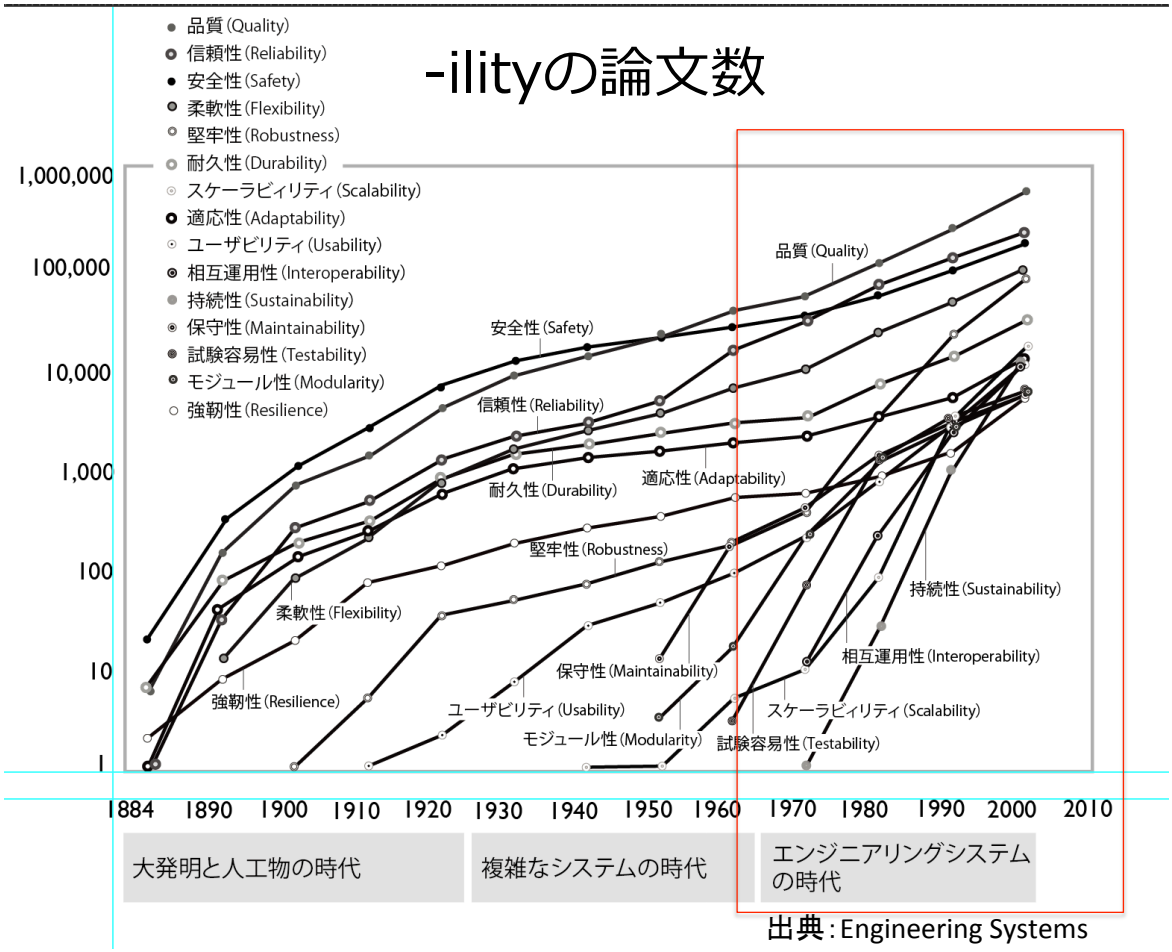
システムズエンジニアリングと ディペンダビリティ

慶應義塾大学大学院システムデザイン・マネジメント研究科
准教授　白坂成功
shirasaka@sdm.keio.ac.jp

-ilityの論文数



出典：Engineering Systems

自己紹介

- 修士：東京大学大学院工学系研究科
- 博士：慶應義塾大学大学院SDM研究科
- 大手電機メーカにて人工衛星開発（１５年間）
  - 「おりひめひこぼし」
  - 「こうのとり」
  - 「みちびき」
  - 2010年4月より慶應大学専任准教授
- INCOSE日本支部設立メンバー
- ISO JTC1/SC7 WG42「アーキテクチャ」
  国内主査
- PMI日本支部 PFM/PGM WG

自己紹介

- 最近の研究テーマ：方法論
  - コンセプトデザイン/
    コンセプトエンジニアリング
  - 大規模システムデザイン
  - 高信頼性システムデザイン
  - イノベーティブデザイン
  - etc

慶應SDMとは？

SYSTEM　　DESIGN

協生社会の実現

MANAGEMENT

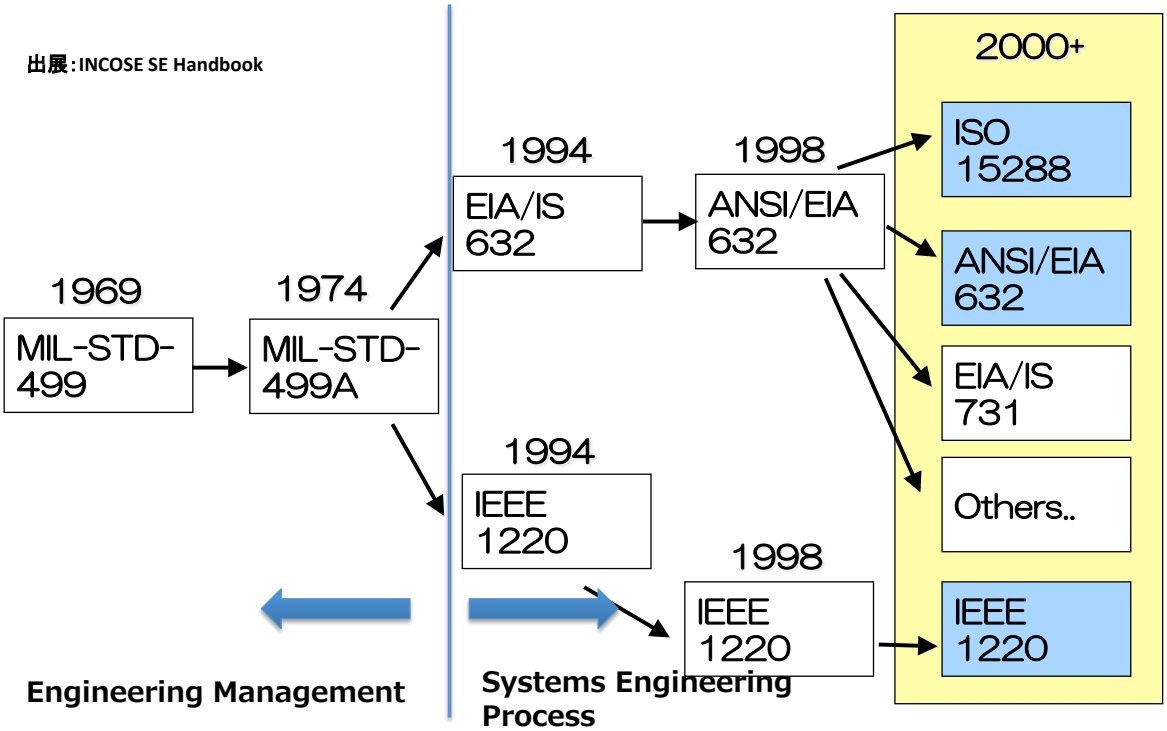
SDM
System Design and Management

慶應義塾大学大学院
システムデザイン・マネジメント研究科

システムズエンジニアリング

システムズエンジニアリング

出展：INCOSE SE Handbook

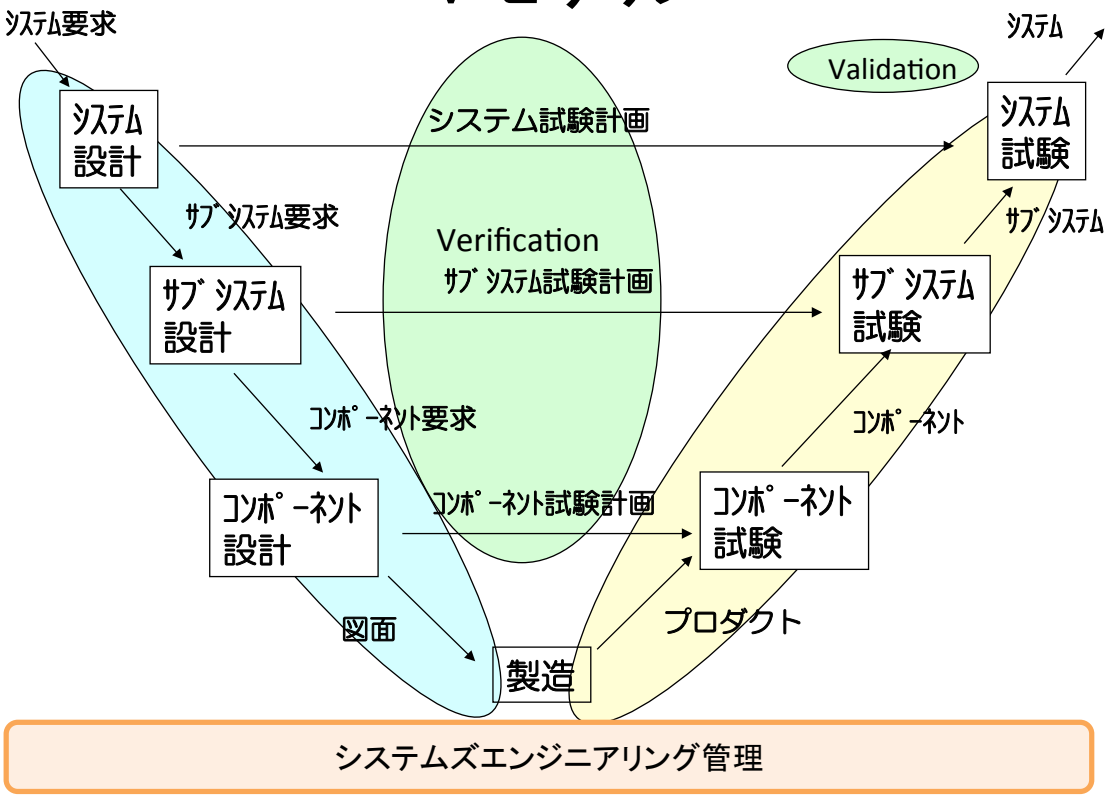


システムズエンジニアリング概要

システムズエンジニアリングを構成する４つの活動

1. システム設計
   - 要件から要求分析、アーキテクチャ設計を実施し、下位への要求を導出する活動
2. インテグレーション
   - 検証の終わったサブシステムを統合する活動
3. 評価・解析
   - エンジニアリング活動における解析および検証(verification)・妥当性確認(validation)等の活動
4. システムズエンジニアリング管理
   - QCDを満たすために、各種活動の計画・実施・評価を行う活動

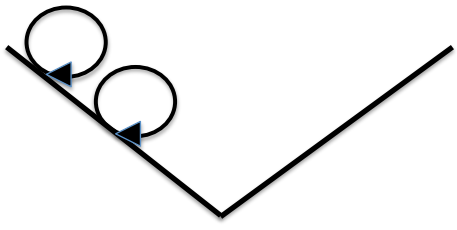
Vモデル



Vモデルに関する間違え

- Vモデルは、時系列的なプロセスとなっている

考え方を表したものである

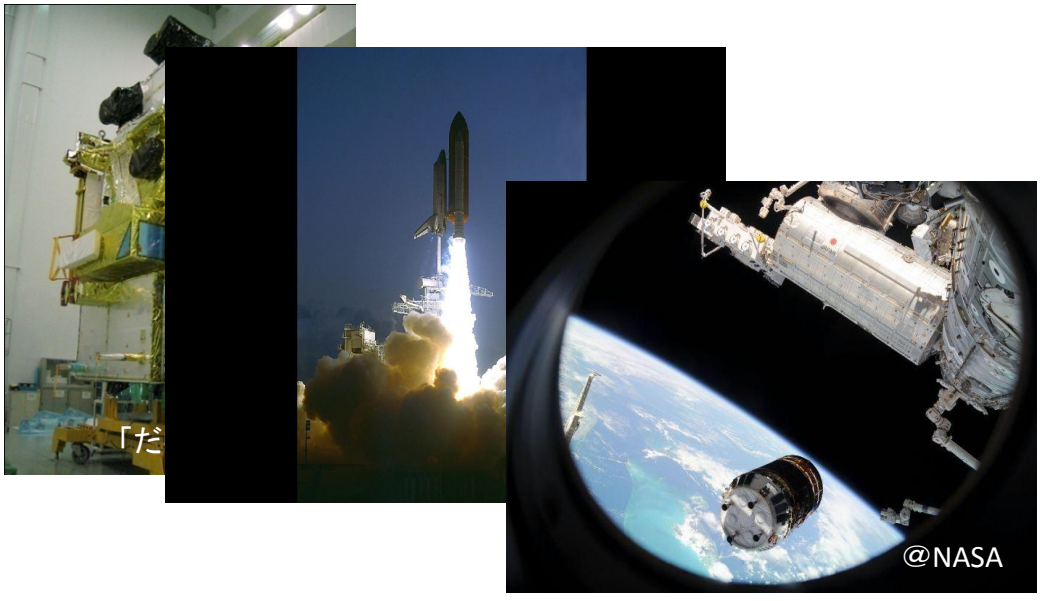


事例:「こうのとり」

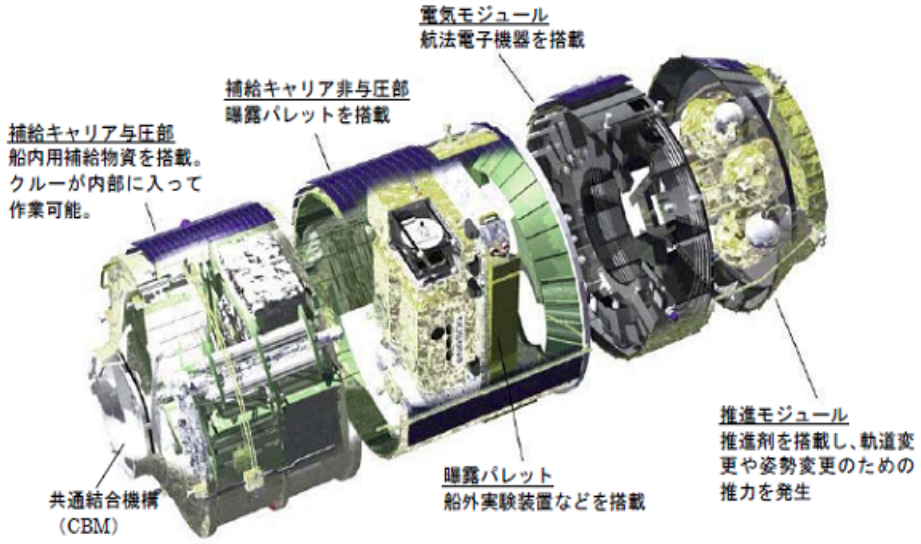
システムズエンジニアリング適用事例におけるディペンダビリティ

背景

宇宙機安全設計の必要性

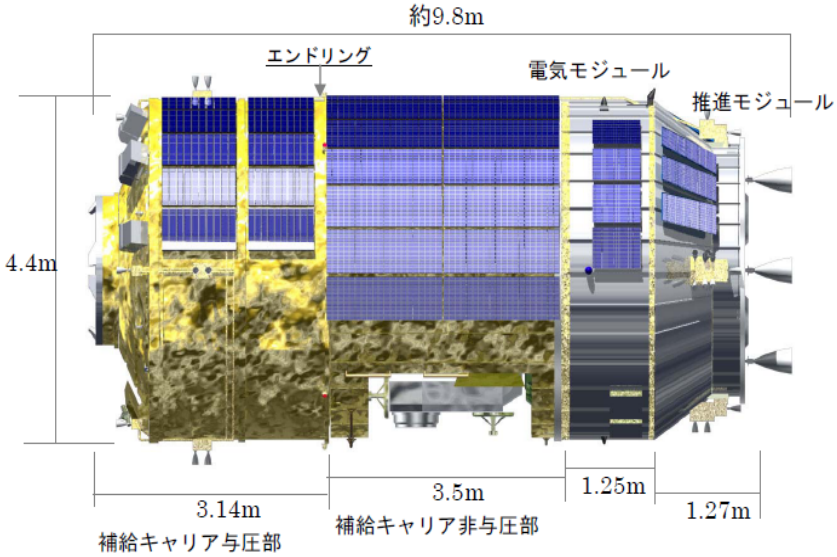


「こうのとり」とは



出典：JAXA (HTV1Press Kit)

「こうのとり」とは



全長：約9.8m
直径：約4.4m
総質量：最大16.5ton
補給能力：最大6ton

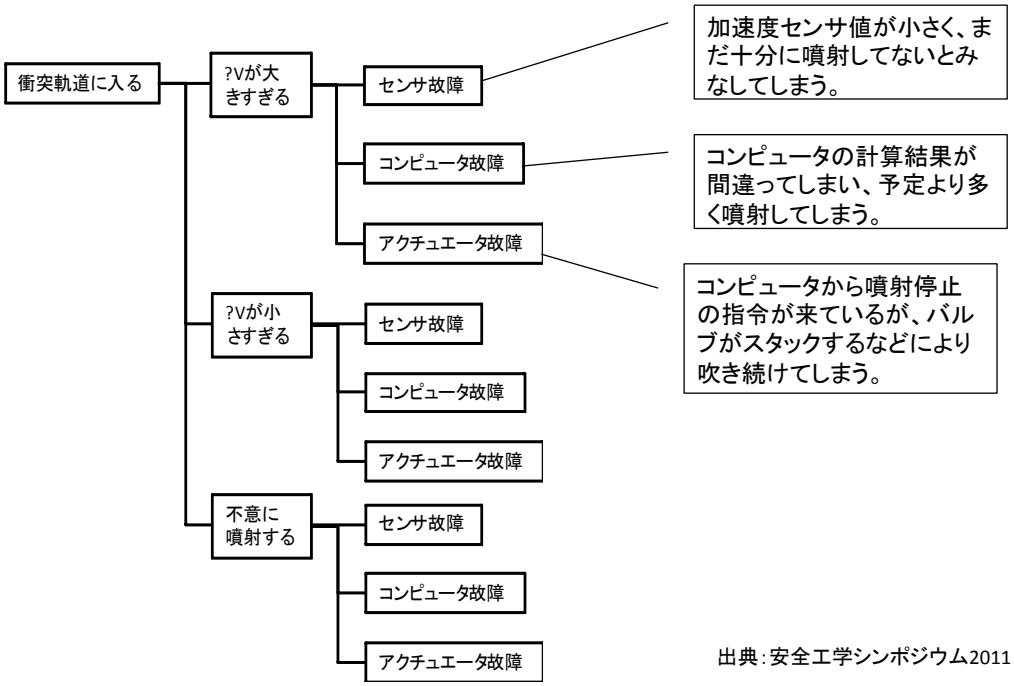
出典：JAXA (HTV1Press Kit)

「こうのとり」における安全設計：コンセプト

- HTVで最もクリティカルなハザード＝衝突＝衝突軌道への投入
  - Catastrophic Hazard＝2 Fail Safeの要求
- FTAによる分析の結果、以下の3つが衝突軌道への投入の主なCause
  - マヌーバ時に予定より大きなΔV（噴射量）を発生する
  - マヌーバ時に予定より小さなΔVを発生する
  - マヌーバが予定されていないときにΔVを発生する

出典：安全工学シンポジウム2011

「こうのとり」における安全設計：コンセプト



出典：安全工学シンポジウム2011

「こうのとり」における安全設計:安全要求

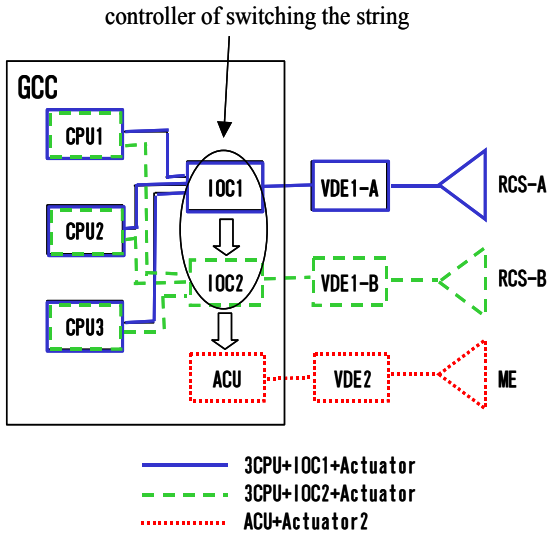
- システム安全要求
  - 2 Fail Safe for Catastrophic Hazard, 1 Fail Safe for Critical Hazard
- コンピュータシステム安全設計要求 (CBCS:Computer Based Control System Safety Requirements)
  - Must Work Function (MWF) 要求
    - 機能が失われるとハザードになる場合
    - フォールトトレランスによる制御
  - Must Not Work Function (MNWF)要求
    - 不適切なタイミングで機能が動作するとハザードになる場合
    - インヒビットによる制御
  - 一般要求
    - ハザード制御に使われるコンピュータ及びソフトウェアに対する要求

例えば、温度センスする機能が失われると、沸騰させるときに加熱しすぎてしまう
→センサを複数持たせる

例えば、手が口の下にあるときに、間違ってお湯がでると火傷をしてしまう
→ロック機構を持たせる

出典:「こうのとり」(H-IITransferVehicle:HTV)におけるコンピュータシステム安全設計(2011)

「こうのとり」における安全設計



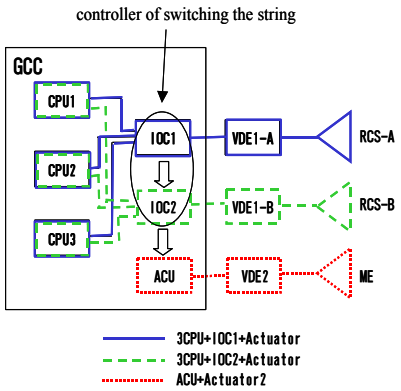
ミッションを継続できる機能
＝正しくΔVを制御
＝安全

ミッションは継続できないが、安全なレベルでΔVを制御する機能

現在制御に使っているアクチュエータ:マヌーバ自体を禁止できないため、ΔVあるいは加速度量をモニタしながら、異常があった場合にはアクチュエータを切り替えることで対応

出典:安全工学シンポジウム2011

「こうのとり」における安全設計



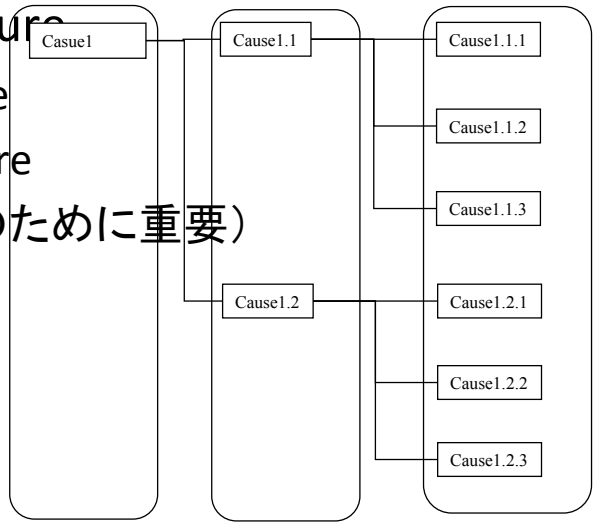
3系あるため、1系のみのときよりも信頼性の低い部品を利用が可能

コモンモード故障対応
- ソフトウェアは3種類
- コンピュータも3種類
- センサ類は、多種センサ

出典：安全工学シンポジウム2011

「こうのとり」における安全設計：設計（階層化FDIR）

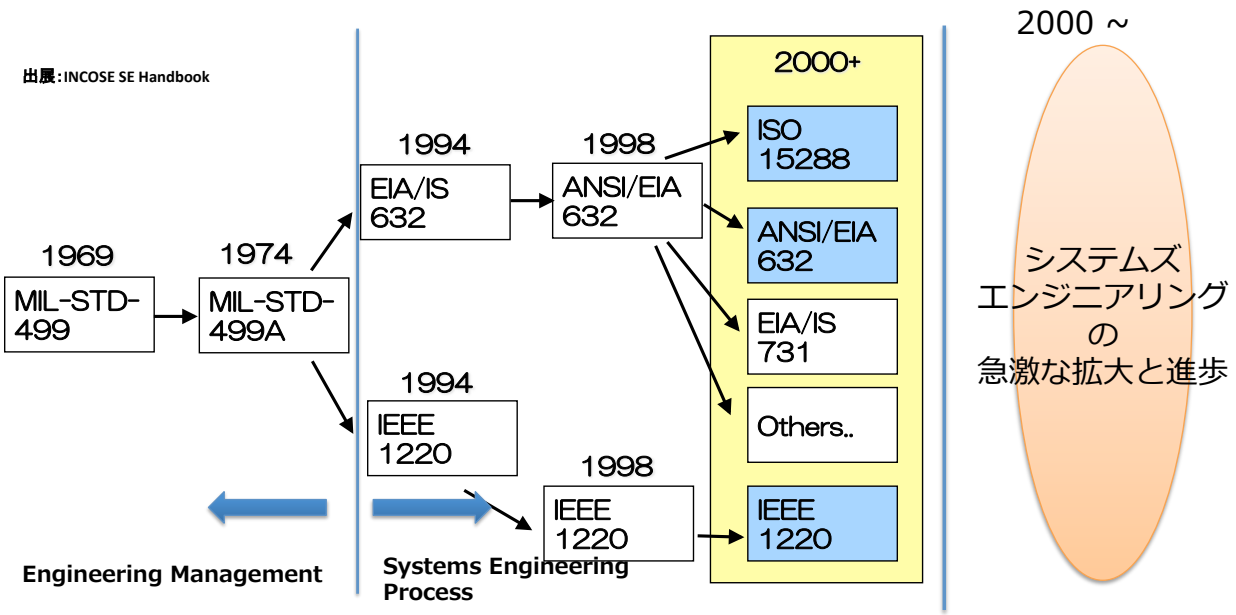
- FDIR (Fault Detection, Isolation and Recovery)
- Layered FDIR architecture
  - Wide coverage of cause
  - Quick response to failure
    （ミッション継続性のために重要）



出典：計測自動制御学会産業論文誌

システムズエンジニアリングの最新動向

システムズエンジニアリング



Systems Engineering 世界動向

【適用ドメインの拡大】

- 防衛/航空/宇宙→他の産業へ
  - Transportation
  - Healthcare、Biomedical
  - Automotive（防衛/航空/宇宙から幹部を受入。もちろん逆も）
  - Consumer Product
- 自産業へのカスタマイズ（ex. P&Gのパンパース）

【Systems Engineeringの進化】

- 方法論の進化：MBSE
- 適用領域の拡大：俯瞰化

方法論の進化

モデルベースド・システムズエンジニアリング

記事コピー・転載の問い合わせは
日刊工業新聞社著作権管理センター
TEL 03-5644-7101
http://www.nikkan.co.jp
日刊工業 検索

2013年 9月23日 月曜日

日刊工業新聞

16

理工学書・専門書は…
Nikkan BookStore
日刊工業 本 検索
日刊工業新聞社出版局のホームページ
http://pub.nikkan.co.jp/

システム工学国際協議会（INCOSE）フェロー
サンフォード・フリーデンタール氏

複雑化やリスク管理に対応

異業種横断、学習プロセス重要

モデルベースド・システムズ・エンジニアリングに注目

試作減らし開発期間短縮

深層断面

設計・開発手法の比較

車業界相次ぎ導入

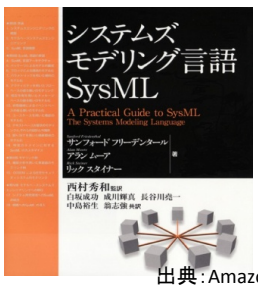
次世代電力網・鉄道にも波及

出典：日刊工業新聞

25

SysMLによるシステム表現

- SysMLで何ができるのか？
- 構造／振る舞い／要求／パラメトリック制約
- 協働作業
- コンカレントエンジニアリング



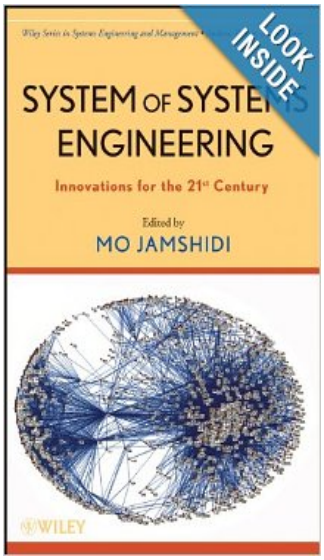
出典：Amazon

書籍のご紹介（Practical Guide to SysMLの翻訳本）

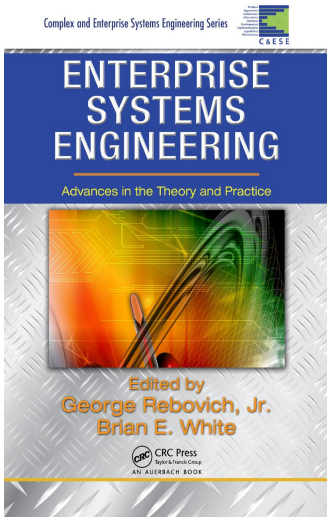
- **システムズモデリング言語 SysML**
- 西村 秀和（監訳），白坂成功，成川輝真，長谷川堯一，中島裕生，翁志強
- **著者：Sanford Friedenthal, Alan Moore, Rick Steiner**
- 出版社：東京電機大学出版局
- 発売日：2012年5月10日

適応領域の拡大：俯瞰化

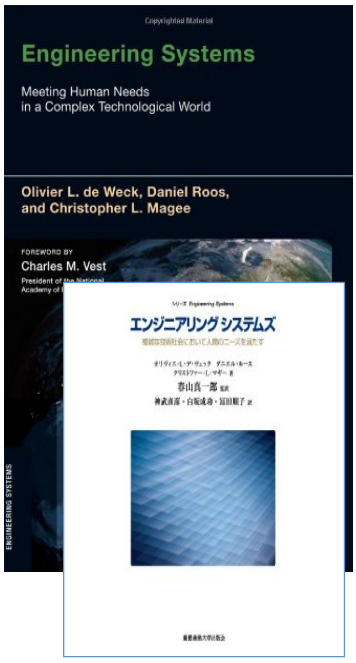
System of Systems Engineering (2008)



Enterprise Systems Engineering (2010)

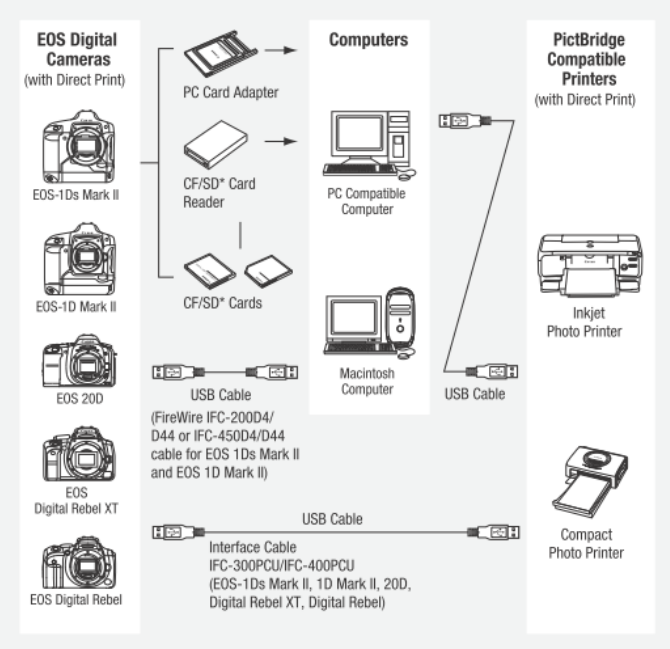


Engineering Systems (2011)



出典：Amazon.com

System of Systems



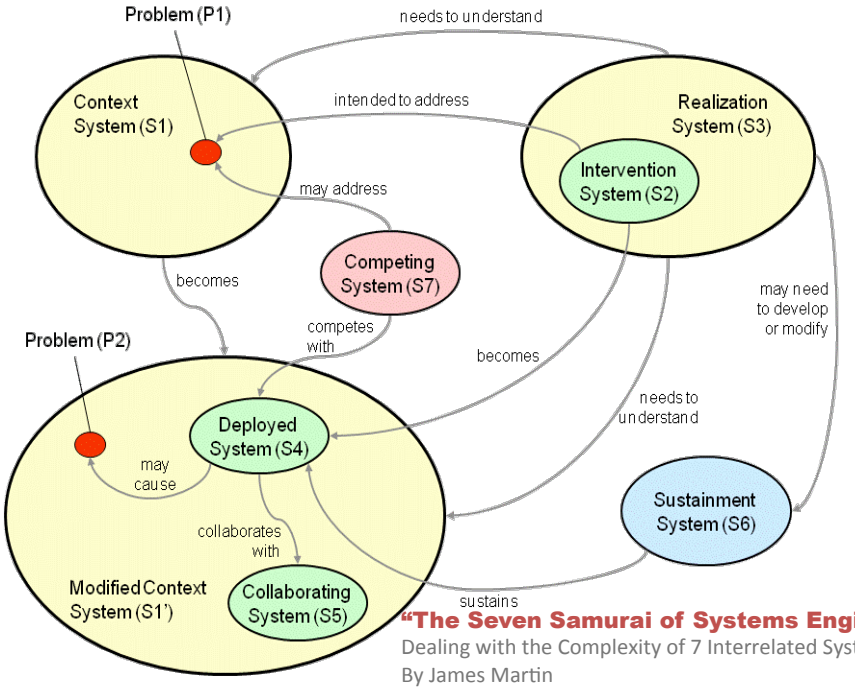
出典：INCOSE Systems Engineering Handbook

The Seven Samurai
of
Systems Engineering

Dealing with the Complexity
of 7 Interrelated Systems

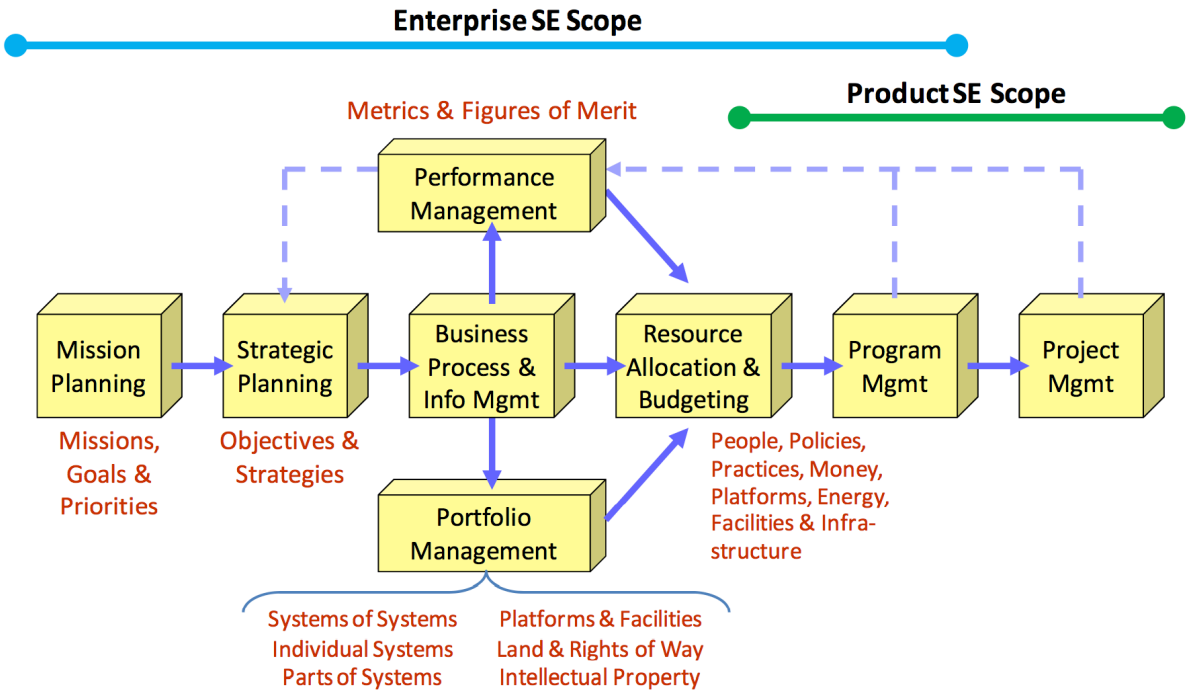
"The Seven Samurai of Systems Engineering
Dealing with the Complexity of 7 Interrelated Systems"
By James Martin

Enterprise Systems Engineering: Seven Samurai



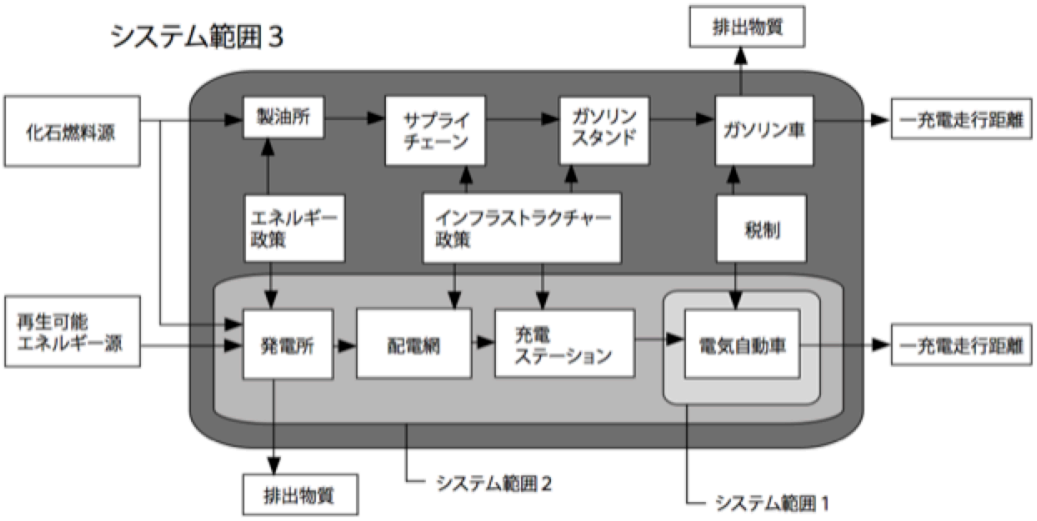
"The Seven Samurai of Systems Engineering
Dealing with the Complexity of 7 Interrelated Systems"
By James Martin

Enterprise Systems Engineering



出典：Enterprise Systems Engineering

Engineering Systems



出典：Engineering Systems

事例：俯瞰化されたシステム

システムズエンジニアリング

事例１：DARPA F6プロジェクト

出典：DARPA F6プロジェクト

事例２：ほどよしプロジェクト

ほどよしプロジェクト：４つの目標

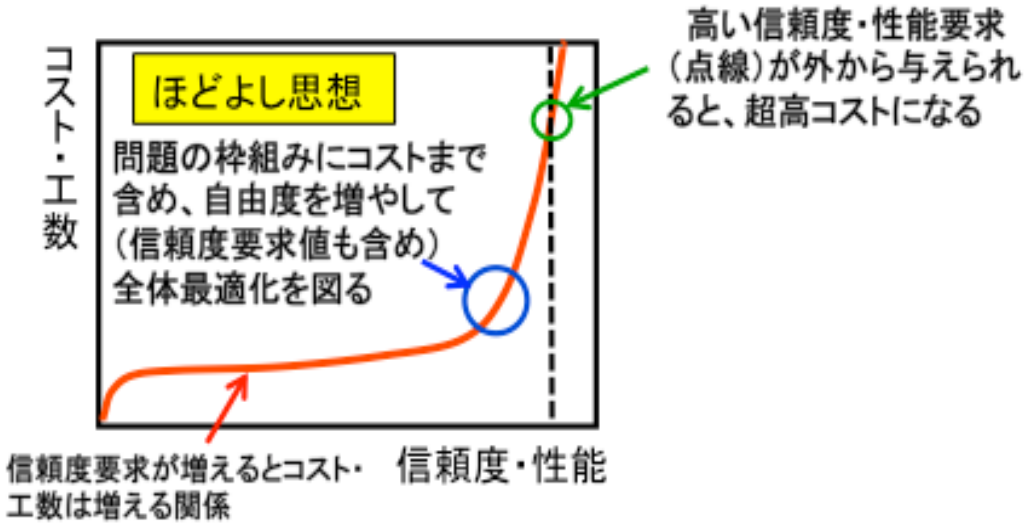
- 2010～2014　最先端研究開発支援プログラム -

世界トップ水準の超小型衛星（50kgクラス）を低コスト（3億円以下）、短期間（2年以内）で開発・運用できる土台を構築し、世界に先駆けてその効果的な利用を開拓すること

1. 超小型衛星に適した「ほどよし信頼性工学」や試験手法を含めた開発プロセスの構築
2. 開発を支える国内のサプライチェーンネットワークの構築と人材育成
3. サイズ比の性能が世界レベルの要素機器や先進的地上局の研究開発
4. 従来にない新しい宇宙利用法と利用コミュニティを開拓し、衛星開発・利用産業につなげる

出典：2013年宇宙科学技術連合講演会発表資料

ほどよし信頼性工学とは



出典：2013年宇宙科学技術連合講演会発表資料

ほどよし信頼性工学：基本方針

- 3つの柱
  1) 衛星の信頼性に「真に」影響を与えるファクタを見極め、そのモデル化を行うこと
  2) その観点のもと、真のシステム信頼度を高められる設計手法の探究
  3) 開発プロセスにおける無駄なく信頼性を維持する手法（プロセスアプローチ）の探究

共通コンセプト

従来の問題設定の枠にとらわれず、それを一段階外側に広げ、その中で増えた自由度も利用して全体最適を目指すアプローチ

出典：2013年宇宙科学技術連合講演会発表資料

信頼度に真に影響を与えるファクターの導出

システム信頼度＝設計信頼度
× 設計通りに動作する信頼度　（1）

設計通りに動作する信頼度＝$f(\pi_1, \pi_2, \pi_3) \times \pi_4$　（2）

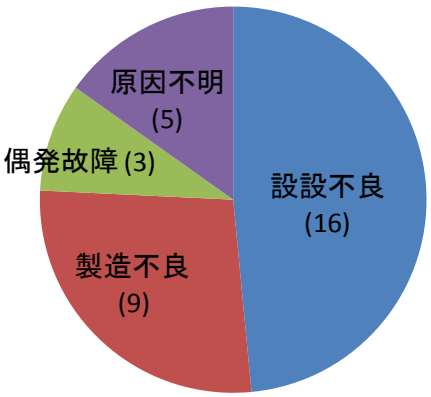
π_1：ロジックミスや設計ミス等のヒューマンファクターを考慮した 設計信頼度

π_2：設計通りに作られたかの製造信頼度

π_3：試験や軌道上実証による動作確認が確実にできているかの実証信頼度

π_4：運用が衛星設計時に予期された通りに確実に行われるかの運用信頼度

出典：2013年宇宙科学技術連合講演会発表資料



2002～2006，11衛星，全33件
(by 宇宙研　斉藤先生の調査)

複雑度の指標

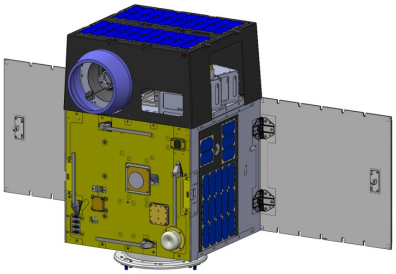
- **設計通りに動作する信頼度低下の要因＝複雑度**
- **「コンテクスト（文脈）数」の概念**：
  「異なる地上試験を必要とし、人間がそれぞれの状況での機器の動作の健全性を考えないといけないコンテクスト（文脈）の数」という概念を提案し、その組み合わせ的爆発が信頼度の低下と工数（開発の労力）の増大につながる。

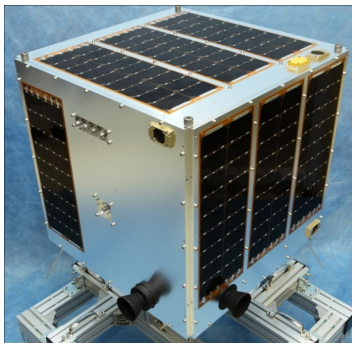
  信頼度の向上は、「コンテクスト数を如何に少なくするか」、また、「コンテクストの場合の数の爆発の連鎖を如何に切るか」という視点でアイデアを追求

出典：2013年宇宙科学技術連合講演会発表資料

どんな姿勢でも太陽電力確保できる設計

- 太陽電池パドル方式 vs. ボディーマウント方式





- 姿勢制御能力に衛星の生き死にが依存する（コンテクストの伝播あり）
- 太陽電池のない面があっても「衛星姿勢が静止することはない」を保障することで対応

・発生電力量は制限されるが、生き残れる・時間余裕がある。

「姿勢というコンテクストに衛星の電力が依存しなくなる」

出典：2013年宇宙科学技術連合講演会発表資料

ほどよし信頼性工学：基本方針

- 3つの柱
  1) 衛星の信頼性に「真に」影響を与えるファクタを見極め、そのモデル化を行うこと
  2) その観点のもと、真のシステム信頼度を高められる設計手法の探究
  3) 開発プロセスにおける無駄なく信頼性を維持する手法（プロセスアプローチ）の探究

共通コンセプト

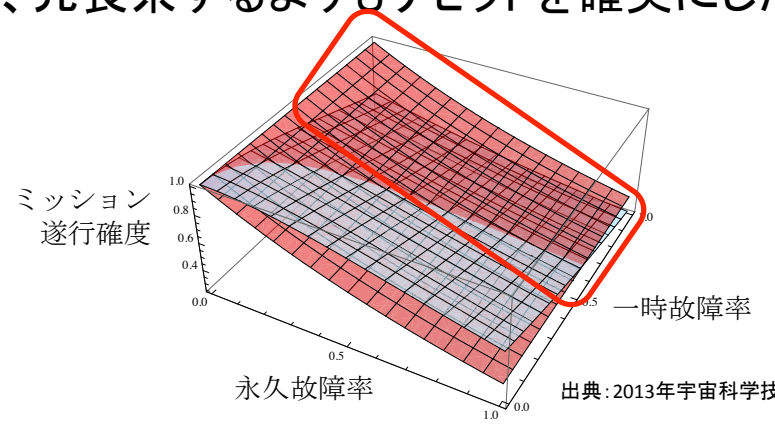
従来の問題設定の枠にとらわれず、それを一段階外側に広げ、その中で増えた自由度も利用して全体最適を目指すアプローチ

42

出典：2013年宇宙科学技術連合講演会発表資料

設計論への反映：リセットの利用

- PCにおけるリセットでの復帰：ある意味で万能
  - 状況にかかわらず同じ手で済む（コンテクスト数１）
- リセットは「継続オペレーションをあきらめる」と引替え
- 「リセットで復帰する」ことが確実だという前提に立てば、冗長系するよりもリセットを確実にした方が効果的



出典：2013年宇宙科学技術連合講演会発表資料

設計論への反映：軌道上システム再構成能力

- レベル１：軌道上でソフトウェアを容易に再構成できる設計
  - 軌道上でより最適なパラメタにチューニング（打ち上げ時は地球補足まで出来ればよい。）
  - 想定外の状況に対しても対応
  - 顧客の要望変化へも柔軟に対応

- レベル２：コーディングをしないソフトウェア開発
  - パラメタ設定によるSDKライブラリからソフトウェアを実現
  - 単体モジュールの設計検証と製造検証が不要
  - ソフトウェア全体の検証は打ち上げまでに必要なところを検証

出典：2013年宇宙科学技術連合講演会発表資料

ほどよし信頼性工学：基本方針

- 3つの柱
  1) 衛星の信頼性に「真に」影響を与えるファクタを見極め、そのモデル化を行うこと
  2) その観点のもと、真のシステム信頼度を高められる設計手法の探究
  3) 開発プロセスにおける無駄なく信頼性を維持する手法（プロセスアプローチ）の探究

共通コンセプト

従来の問題設定の枠にとらわれず、それを一段階外側に広げ、その中で増えた自由度も利用して全体最適を目指すアプローチ

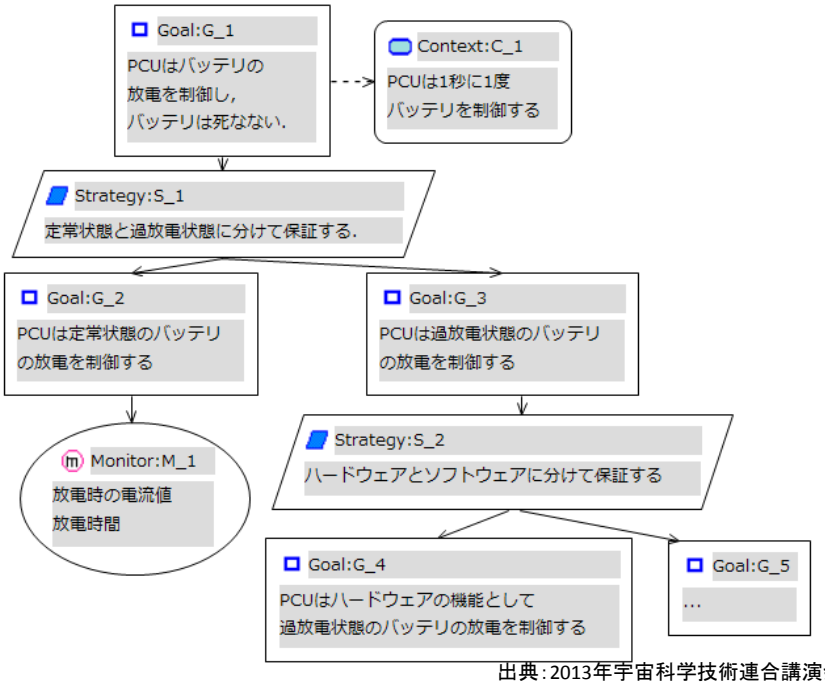
出典：2013年宇宙科学技術連合講演会発表資料

開発プロセスにおける無駄なく信頼性を維持する手法（プロセスアプローチ）の探究

- 開発資源（人的含む）全体を見ての最適配分の検討：目的を明確化（メタプロセス化）
  －デザインレビュー会　－文書管理　－試験の最少化
- 外部企業とインターフェースを切っての契約は自由度を妨げてしまう
  －同一の開発チームとして協働　（SSTL, SpaceX等の成功例）
  －顧客とも共同で目標性能・信頼度設定（自由度が増える）
- 個々のプロジェクトではなく継続したプログラムレベルでの信頼性管理
  －メインCPUの裏で次世代CPUの試験　－標準化で実績数を稼ぐ

出典：2013年宇宙科学技術連合講演会発表資料

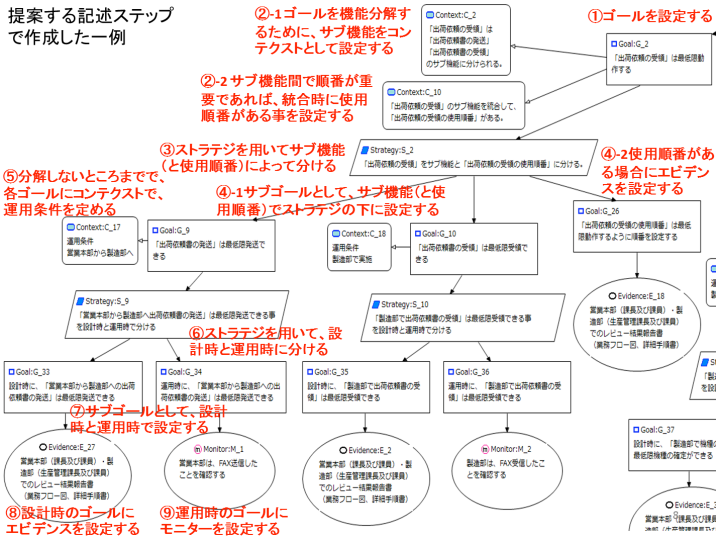
見える化→アシュアランスケースの導入
D-CASEによるほどよし3号機電源系設計



出典：2013年宇宙科学技術連合講演会発表資料

事例３：業務プロセスデザインと品質保証

株式会社加藤製作所における業務プロセスの品質保証と海外展開への活用



出典：2013年日本経営システム学会発表資料

まとめ

- システムズエンジニアリングとディペンダビリティの親和性は高い
- システムズエンジニアリングの適用範囲拡大にあわせて、適用範囲の拡大