MATLAB EXPO 2021

システムレベルからのモデルベースデザインによる機能安全規格対応

大越亮二 / 袁帥

MathWorks®

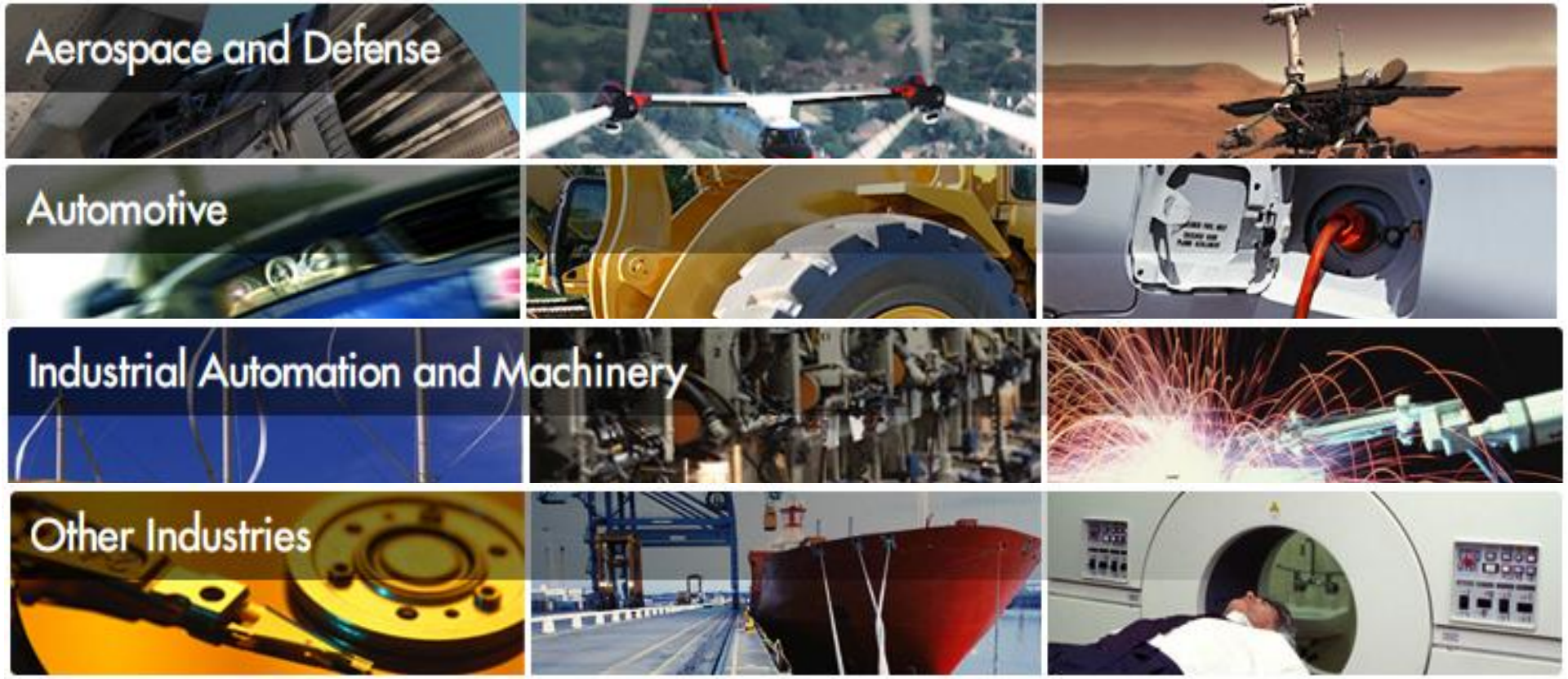
Agenda

1. 高信頼性システム開発のニーズ
   - 機能安全規格の目的
   - 機能安全規格の構成
2. システムレベルにおける製品開発
   - システムズエンジニアリングとは
   - システムズエンジニアリングのプロセス
   - システムズエンジニアリング領域でのMathWorksソリューション活用
3. ソフトウェアレベルにおける製品開発
   - ソフトウェア開発のVプロセスおよび適切な開発ツール
   - 機能安全規格準拠MBDリファレンスワークフロー
   - 静的解析ツールによる自動生成コードとモデルの一致保証

Agenda

1. 高信頼性システム開発のニーズ
   - 機能安全規格の目的
   - 機能安全規格の構成
2. システムレベルにおける製品開発
   - システムズエンジニアリングとは
   - システムズエンジニアリングのプロセス
   - システムズエンジニアリング領域でのMathWorksソリューション活用
3. ソフトウェアレベルにおける製品開発
   - ソフトウェア開発のVプロセスおよび適切な開発ツール
   - 機能安全規格準拠MBDリファレンスワークフロー
   - 静的解析ツールによる自動生成コードとモデルの一致保証

高信頼性システム（High-Integrity Applications)



高信頼性システムは、高い信頼性で、目的とする機能、SILを達成できるように設計され、保守されるような、ソフトウェアが組み込まれたシステムです。

SIL（Safety Integrity Level）：機能安全を達成させるために実施すべき内容の指標

cf. Buncefield Investigation Glossary www.buncefieldinvestigation.gov.uk/glossary.htm

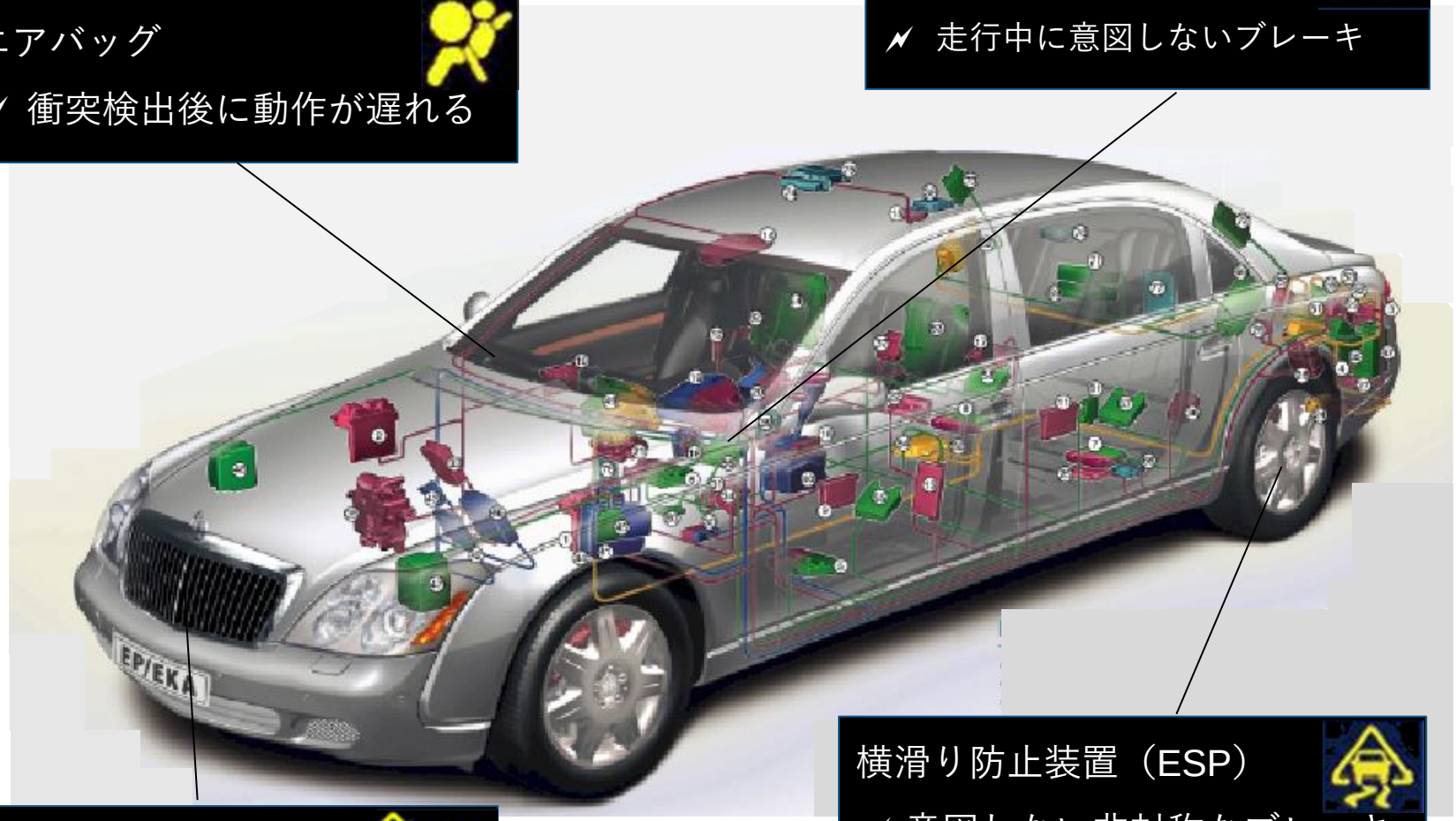
自動車における高信頼性システムの実例

エアバッグ

- 衝突検出後に動作が遅れる

電動パーキングブレーキ（EP

- 走行中に意図しないブレーキ



車間距離制御装置（ACC）

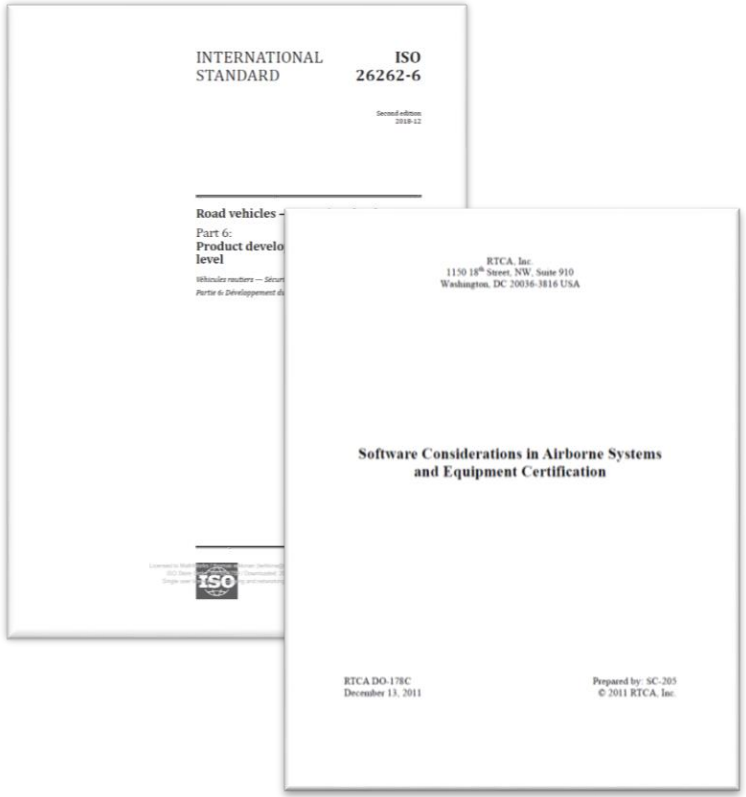
- 要求時間内に減速が足りない

横滑り防止装置（ESP）

- 意図しない非対称なブレーキ

Source: K. Grimm: Software-Technologie in der Automoboilindustrie. 19. STEV-OESTERREICH-FACHTAGUNG IT-/Softwarequalitätsmanagment in der Praxis, Wien, Austria, May 2004

高信頼性システムの開発



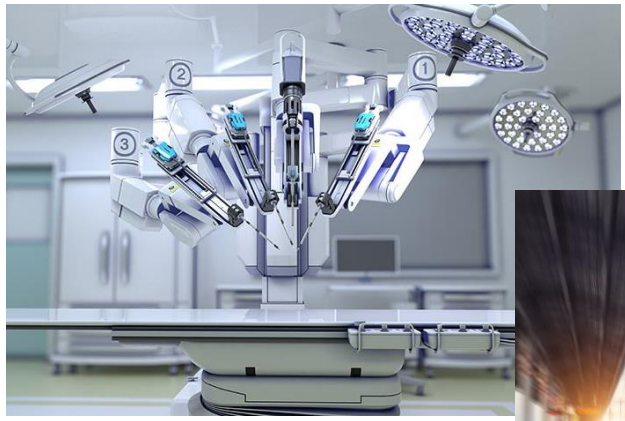
高信頼性システムは、**標準やガイドライン**に沿って開発されます。

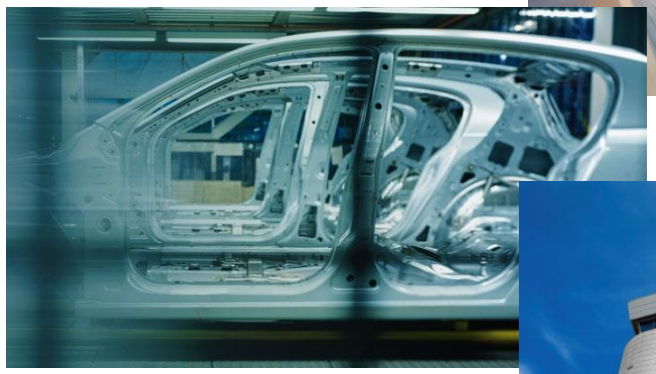
- その開発は、標準規格に従います。
- その開発においては、次の定義が必要となります。
  - 各開発プロセスにおける、**その活動の目的・目標**
  - 開発プロセスの中で使用される**ツールの適格性の検証**の要求
- 開発者は、これらの目的や要求が**標準規格に適合**していることを**証明する必要**があります。

高信頼性システムにおける機能安全の規格

工業分野によって要求される機能安全の規格は異なります

- **IEC 61508** – All industries
- **ISO 26262, SOTIF** – Automotive
- **DO 178C** – Avionics
- **IEC 62304** – Medical
- **EN 50128** – Rail
- **ISO 25119** – Agriculture and Forestry
- And many others…..





機能安全規格の構成（ISO 26262の例）

ISO 26262-1	• 用語集
ISO 26262-2	• 機能安全の管理
ISO 26262-3	• コンセプトフェーズ
ISO 26262-4	**• システムレベルにおける製品開発**
ISO 26262-5	• ハードウェアレベルにおける製品開発
ISO 26262-6	**• ソフトウェアレベルにおける製品開発**
ISO 26262-7	• 生産、運用、サービス及び廃棄
ISO 26262-8	• 支援プロセス
ISO 26262-9	• ASIL指向及び安全性指向の分析
ISO 26262-10	• ガイドライン
ISO 26262-11	• 半導体へのISO26262適用指針

- システムのアーキテクチャ設計
- トレーサビリティ

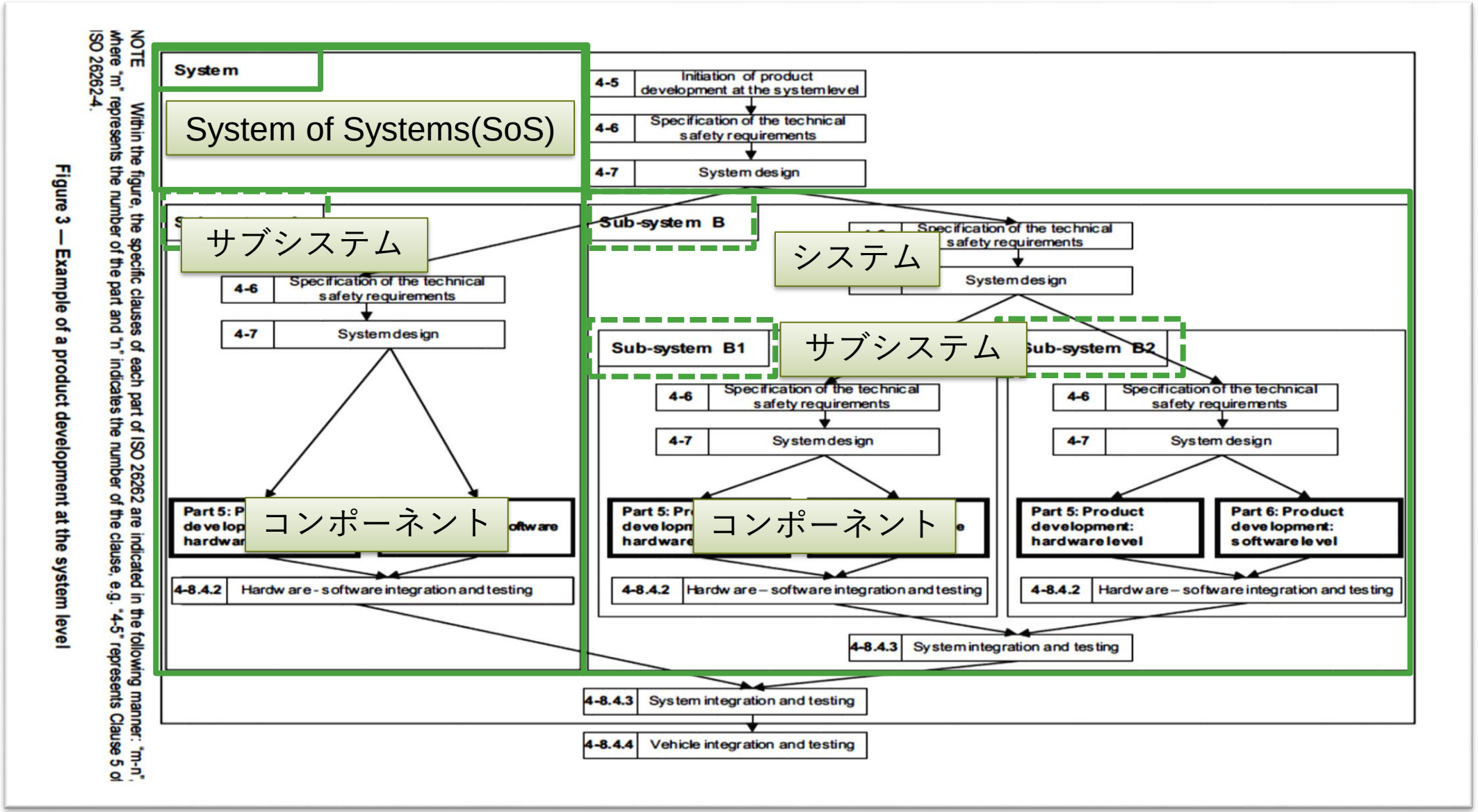
- ソフトウェア開発のVプロセス
- ソフトウェア開発のメソッド
- モデルベースデザイン
- 早期の検証と妥当性確認
- コード生成

Agenda

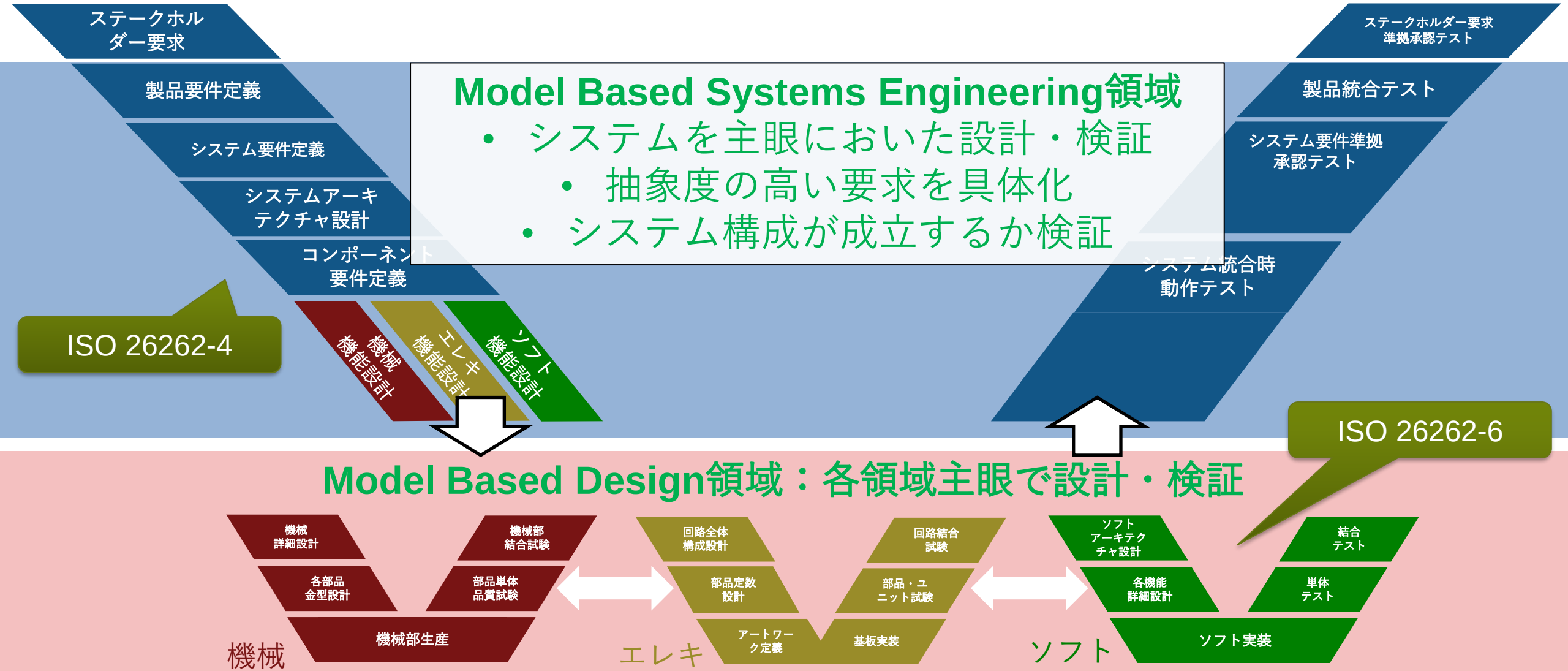
1. 高信頼性システム開発のニーズ
   - 機能安全規格の目的
   - 機能安全規格の構成
2. システムレベルにおける製品開発
   - システムズエンジニアリングとは
   - システムズエンジニアリングのプロセス
   - システムズエンジニアリング領域でのMathWorksソリューション活用
3. ソフトウェアレベルにおける製品開発
   - ソフトウェア開発のVプロセスおよび適切な開発ツール
   - 機能安全規格準拠MBDリファレンスワークフロー
   - 静的解析ツールによる自動生成コードとモデルの一致保証

ISO 26262-4　システムレベルの製品開発

- ISO 26262-4 Figure.3 システムレベルの製品開発例



システムレベルの製品開発



システムズエンジニアリングとは？

- **“システムを成功させるための複数の専門分野にまたがるアプローチと手段”** のことです

言い換えれば

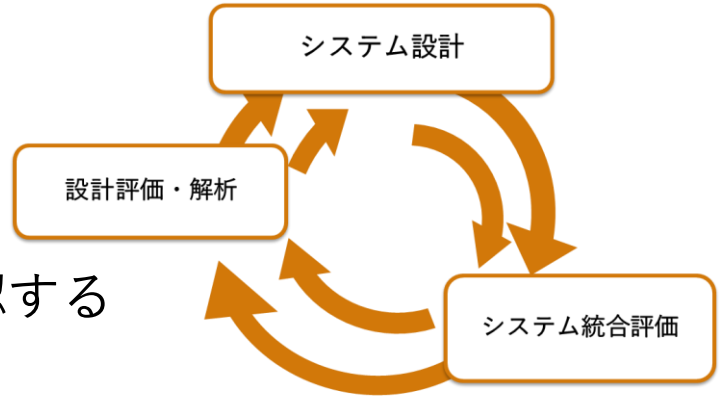
- **“新たなシステムを定義し、開発するためのアクションそのもの”**ともいえます

- システムズエンジニアリングは、必ずしもエンジニアのものとは限りません
  開発環境の外にいる者（仕様を考える企画など）を巻き込む可能性があります

Ref: “Systems Engineering ROI,” 2004 by Eric Honour, PhD. (Former INCOSE President)

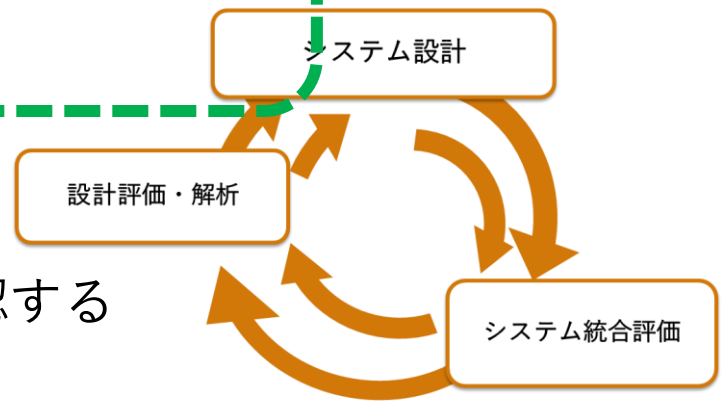
システムズエンジニアリングのプロセス

1. **システム設計**
   - **要求分析**
     - ステークホルダー要求を分析することで要求仕様をつくる
   - **アーキテクチャ設計**
     - 要求仕様を実現するためのシステムの構成（アーキテクチャ）を設計する
     - 各コンポーネントごとの派生要求を作成する
2. **設計評価・解析**
   - アーキテクチャが要求仕様に基づき正しく設計されているか確認する
3. **システム統合評価**
   - 全体の統合評価によってステークホルダ要求を満たすかを確認する



システムズエンジニアリングのプロセス

1. **システム設計**
   - 要求分析
     - ステークホルダー要求を分析することで要求仕様をつくる
   - アーキテクチャ設計
     - 要求仕様を実現するためのシステムの構成（アーキテクチャ）を設計する
     - 各コンポーネントごとの派生要求を作成する
2. **設計評価・解析**
   - アーキテクチャが要求仕様に基づき正しく設計されているか確認する
3. **システム統合評価**
   - 全体の統合評価によってステークホルダ要求を満たすかを確認する



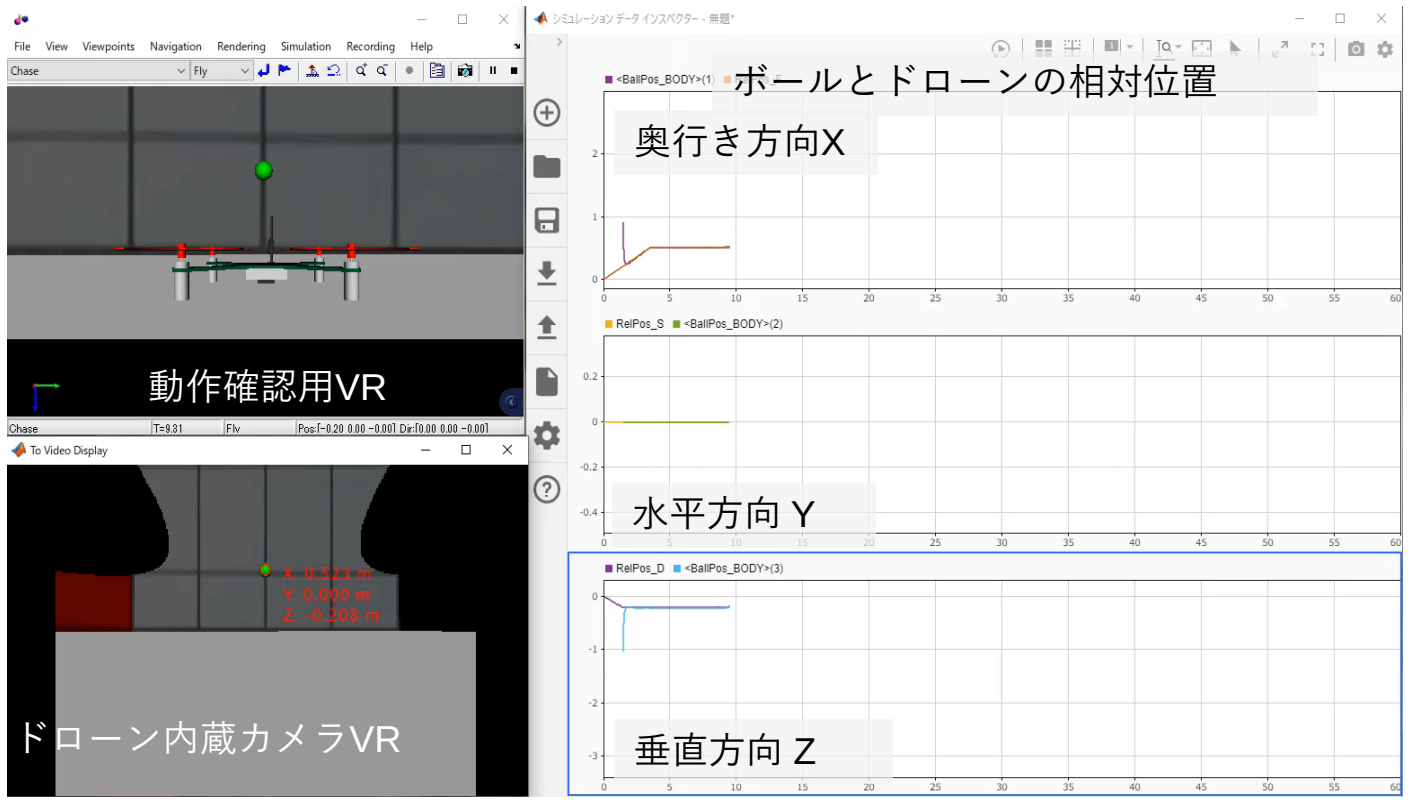
システムズエンジニアリングのプロセス ～ドローン制御開発の例～

ステークホルダ要求
緑のボールを追従するドローン制御を
可能な限り安価に構築すること

要求分析

システム全体の要求仕様

- ドローン制御の開発
  - 緑のボールに追従
  - 対象物との相対距離誤差0.8m以内
- 部材費を$100以下
- 評価用にドローンをVR空間にモデリング



システムズエンジニアリングのプロセス ～ドローン制御開発の例～
システムは複数の小さなシステムやコンポーネントの組み合わせ

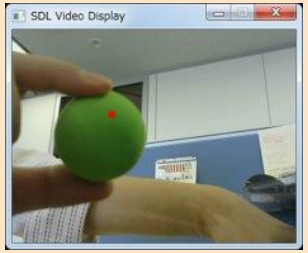
Hardware

カメラ

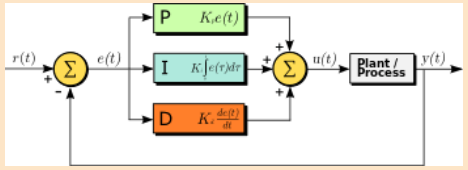
モータ

バッテリー

Software



画像処理



モータ回転制御

システムズエンジニアリングのプロセス ～ドローン制御開発の例～
システムは複数の小さなシステムやコンポーネントの組み合わせ

System of Systems(SoS)
“複数システムの組み合わせで構成されるシステム”

ターゲット
位置推定システム

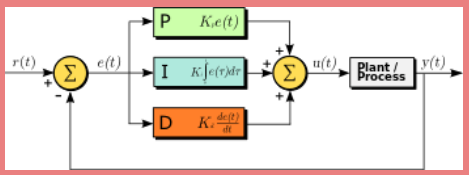
カメラ

画像処理

ドローン
位置制御システム

モータ

バッテリー



モータ回転制御

ドローン制御システム

システムズエンジニアリングのプロセス ～ドローン制御開発の例～
システムは複数の小さなシステムやコンポーネントの組み合わせ

SoS要求仕様

- ドローン制御の開発
  - 緑のボールに追従
  - 対象物との相対距離誤差0.8m以内
- 部材費を$100以下
- 評価用にドローンをVR空間にモデリング

ターゲット
位置推定システム

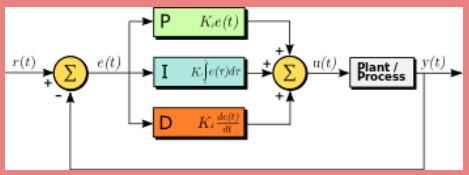
カメラ

画像処理

ドローン
位置制御システム

モータ

バッテリー



モータ回転制御

ドローン制御システム

システムズエンジニアリングのプロセス ～ドローン制御開発の例～
上位要求を具体化させて各システム・コンポーネントの要求仕様へ

SoS要求仕様

- ドローン制御の開発
  - 緑のボールに追従
  - 対象物との相対距離誤差0.8m以内
- 部材費を$100以下
- 評価用にドローンをVR空間にモデリング

ターゲット位置推定システム

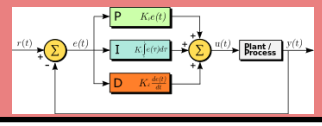
カメラ仕様
- 解像度
- Fps
- コスト
- …

画像処理ソフト仕様
- 位置推定精度
- 位置更新頻度
- …

ドローン位置制御システム

モータ仕様
- 回転数
- トルク
- コスト
- …

バッテリー仕様
- 放電容量
- 電圧
- コスト
- …



制御ソフト仕様
- 応答速度
- オーバーシュート量…

ドローン制御システム

システムズエンジニアリングのプロセス ～ドローン制御開発の例～
上位要求を満たす最適なシステムアーキテクチャ

スペック	値
継続飛行時間	60分
ボール位置推定精度	±0.01m
位置制御の精度	±0.05m
コスト	$400

スペック	値
継続飛行時間	15分
ボール位置推定精度	±0.1m
位置制御の精度	±0.1m
コスト	$90

要求を実現するために最適なアーキテクチャ設計と
各システム・コンポーネントへの詳細要求の落とし込みが必要

システムズエンジニアリング領域に対応する MathWorksソリューション

ステークホルダー要求

製品要件定義

システム要件定義

システムアーキテクチャ設計

コンポーネント要件定義

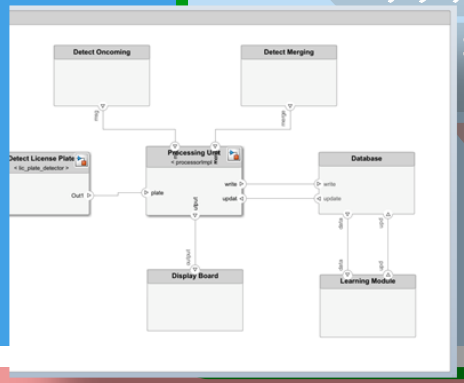
ステークホルダー要求準拠承認テスト

製品統合テスト

システム要件準拠承認テスト

システム統合時動作テスト

Model Based Systems Engineering



System Composer

Simulinkと直接連携できる

システムアーキテクチャ/コンポーネントモデルの記述が可能

機械詳細設計

エレキ機能設計

ソフト機能設計

Model Based Design

機械詳細設計

機械部結合試験

回路全体構成設計

回路結合試験

ソフトアーキテクチャ設計

各機能詳細設計

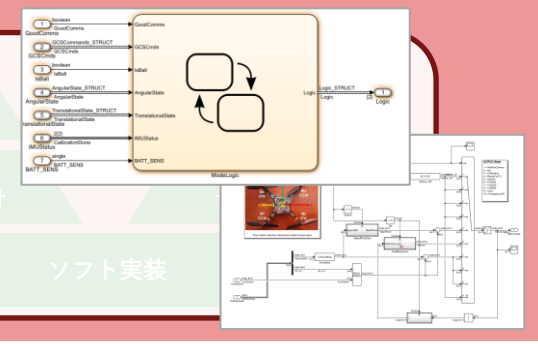
機械部生産

アートワーク定義

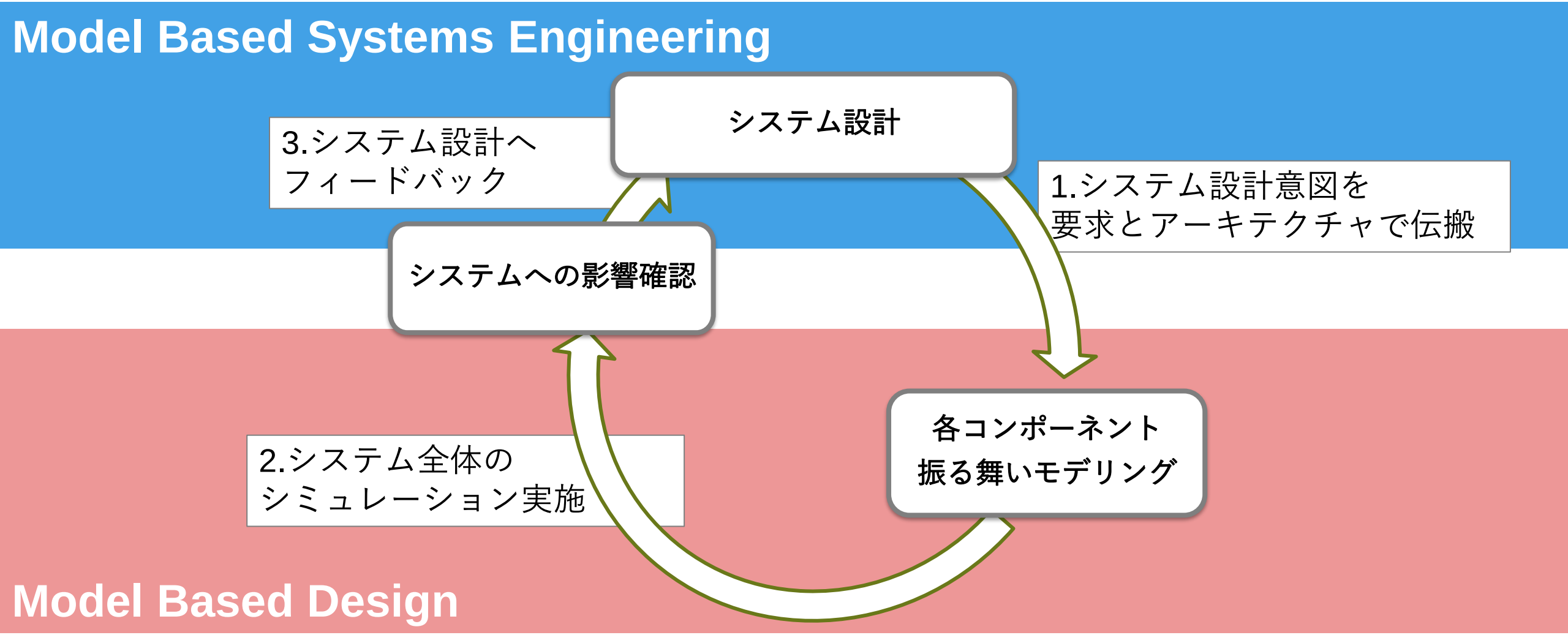
基板実装

ソフト実装

Simulink/Stateflow/Simscape



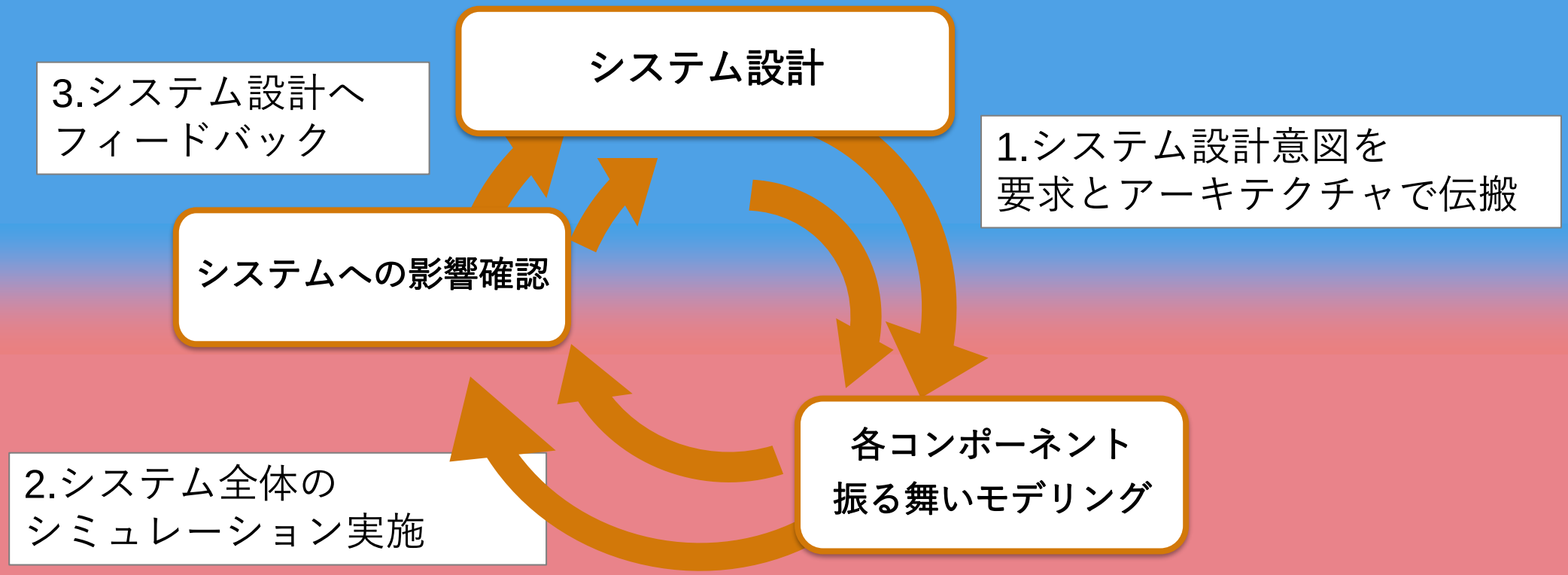
システムズエンジニアリングにおけるツール活用の難しさ
2つの領域で設計の関係性が切れてしまいサイクルが回らない



MathWorksソリューションご利用のポイント

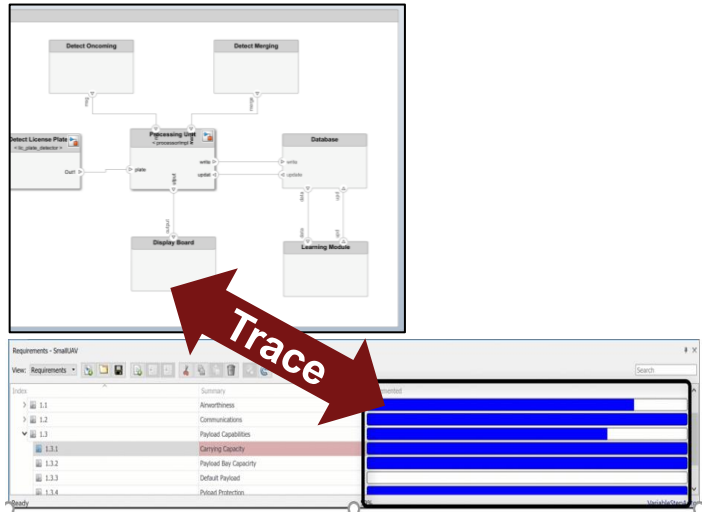
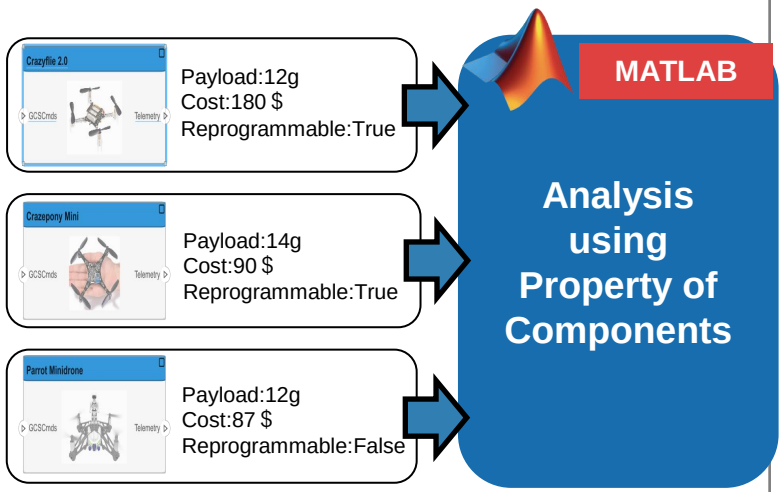
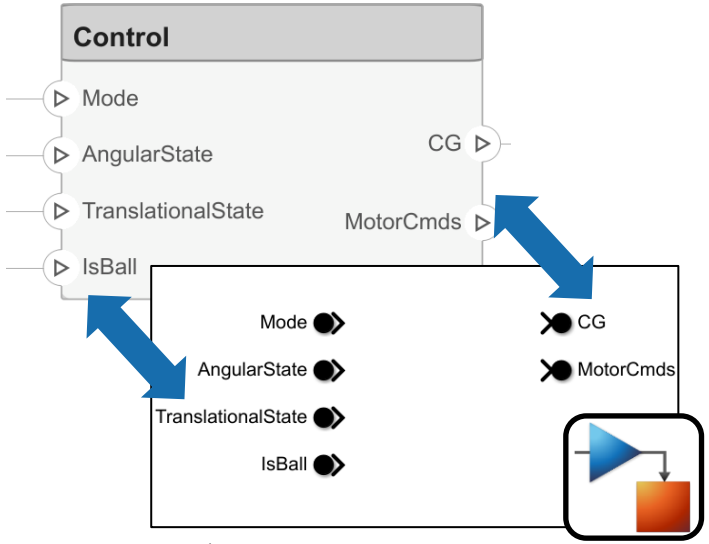
領域間を埋めて開発サイクルを早く回すことで早期に完成度を高める

Model Based Systems Engineering

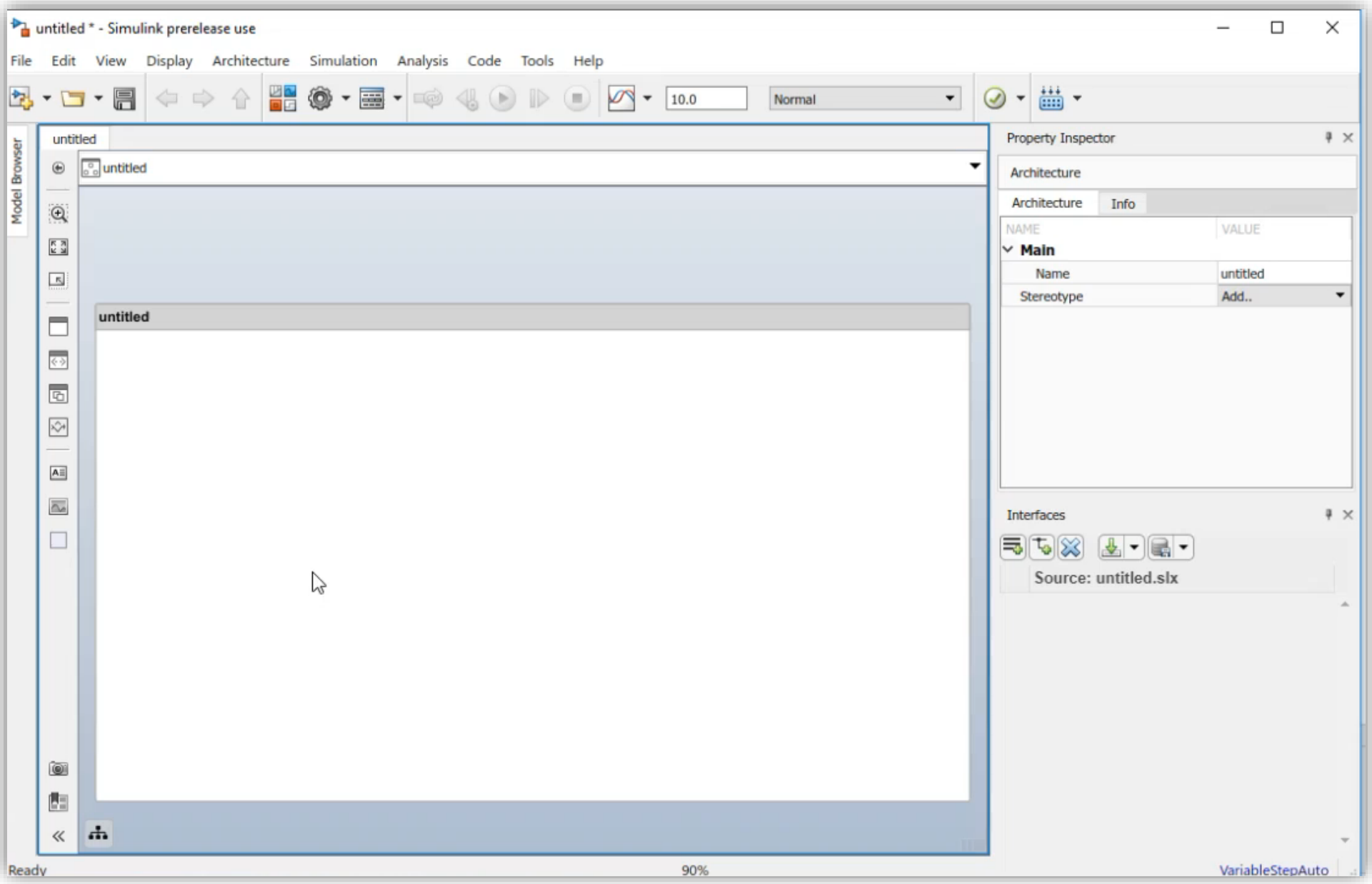


Model Based Design

System Composerはアーキテクチャ設計をサポートします

コンポーネントモデル作成	システムレベルでの解析	インタフェース情報を継承したSimulinkモデルとの連携
システムが持つコンポーネントとインタフェースのモデリングが可能	コンポーネントモデルに定義した属性情報を用いた解析をMATLAB と連携して実施可能	インタフェースを継承したSimulink参照モデルをリンクし、一貫した統合シミュレーション環境を構築
 Simulink Requirements と連携すれば要件トレーサビリティ確保が可能		 Simulinkモデルにコンポーネントの振る舞いを記載することで動的シミュレーションを実施可能

System Composerによるアーキテクチャモデリング（デモ動画）

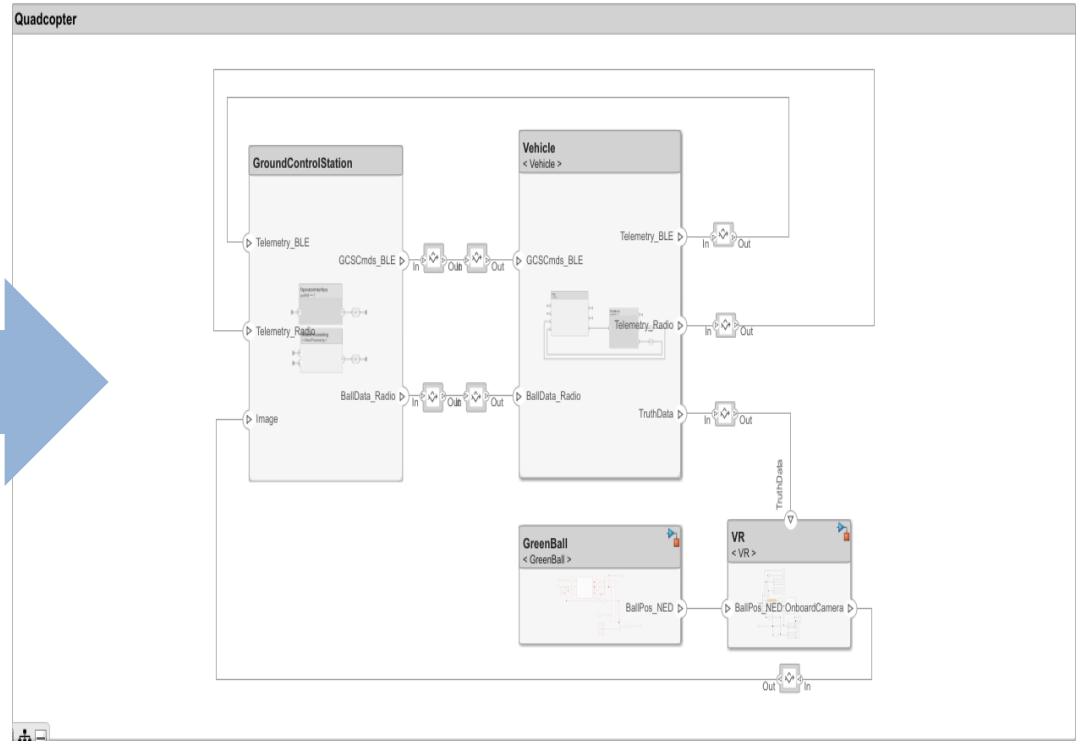


アーキテクチャと要求の紐づけ

アーキテクチャと要求の対応付けをどのように管理すればよい？

- ドローン要求仕様書
  - カメラの性能
    - 画角
    - 解像度
    - フレームレート
  - 姿勢制御部の性能
    - 制御周期
    - 許容誤差範囲
  - ドローンハード性能
    - 重量
    - 最大連続飛行時間
    - ・・・・

?

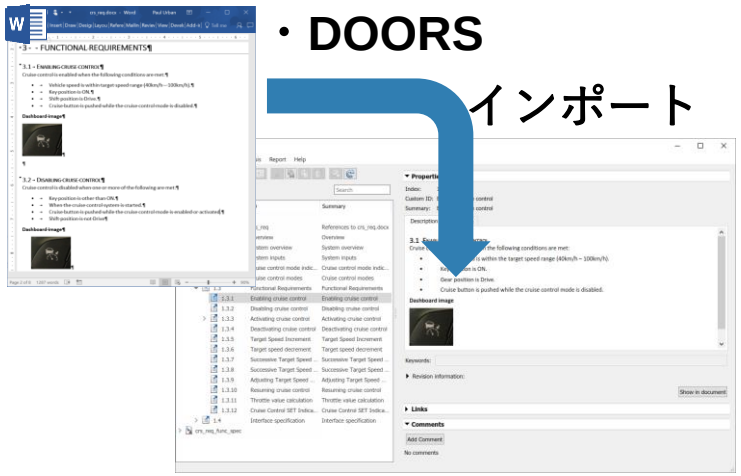
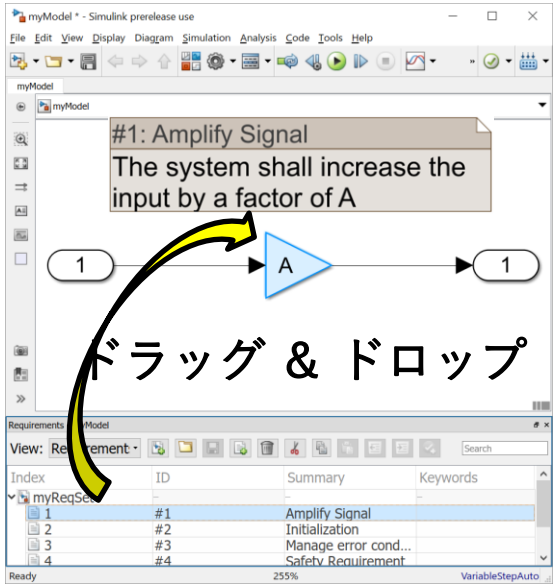
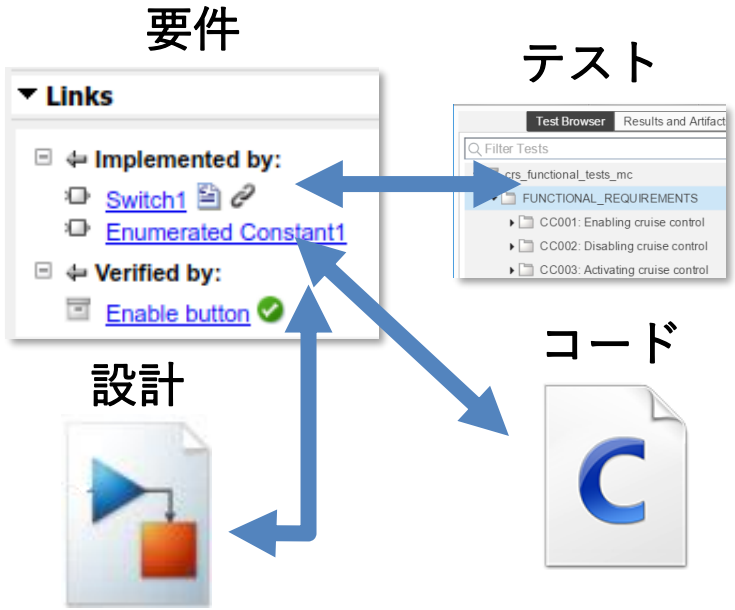


複数の要求仕様書・派生要求仕様書

システムアーキテクチャモデル

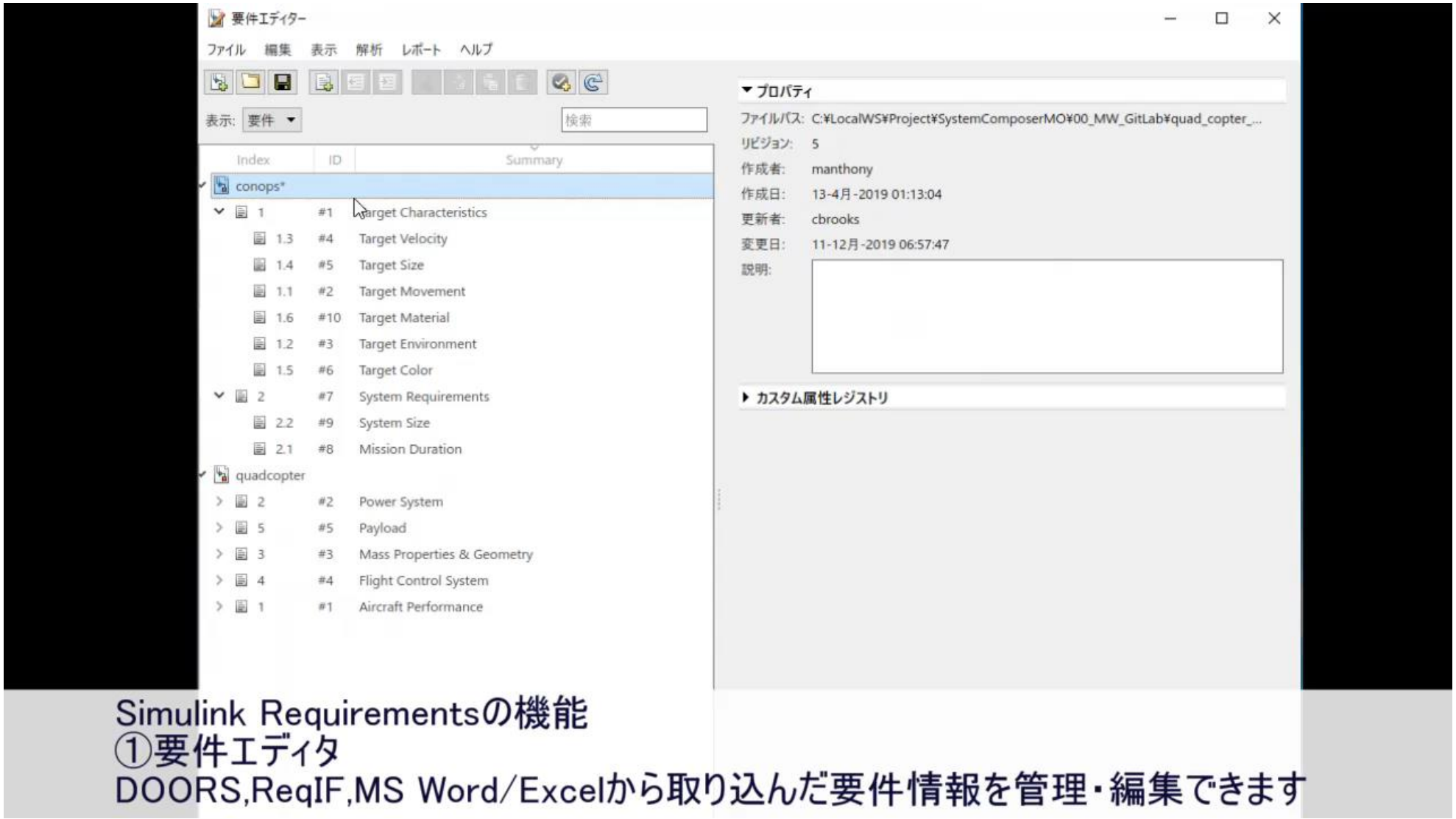
アーキテクチャと要求の紐づけ

Simulink Requirementsで要件の作成、管理、トレースを実現

要件エディタ	要件パースペクティブ	要件トレーサビリティ
Simulink上で外部要件と内部要件の管理と分析	要件をドラッグ＆ドロップしてリンクを作成	要件と設計、コード、テスト間で双方向にトレーサビリティを確保
外部要件 ・Word ・Excel ・DOORS インポート 		

アーキテクチャと要求の紐づけ（デモ動画）

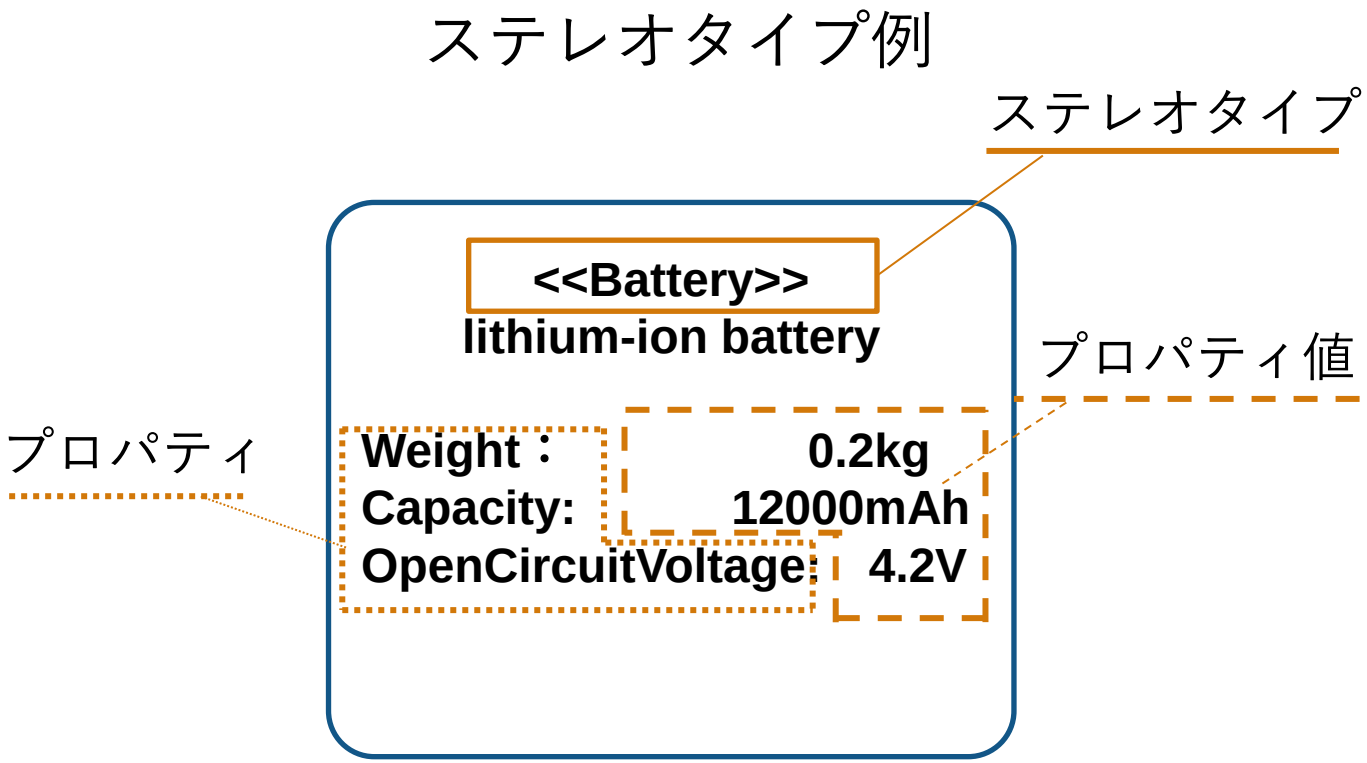
Simulink Requirementsで要求の管理、トレースを実現



システムレベルのアーキテクチャ解析
ステレオタイプ・プロパティとは？

- ステレオタイプ
  - 特定用途のために拡張して定義したモデル要素・情報をまとめたもの

- プロパティ
  - ステレオタイプに付随するモデル情報のこと
  - プロパティに割り当てられた具体的な値をプロパティ値・プロパティ情報と呼ぶ



システムレベルのアーキテクチャ解析

どのような場合にシステムレベル解析を用いるのか？

- 本システムで使用するドローンのアーキテクチャ候補が３つあります

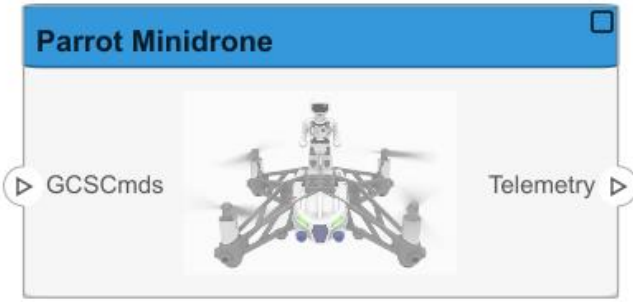
<<QuadCopterPhisicalProperties>>

Payload:12g
Cost:$180
Reprogrammable: True

<<QuadCopterPhisicalProperties>>

Payload:14g
Cost:$90
Reprogrammable: True

<<QuadCopterPhisicalProperties>>

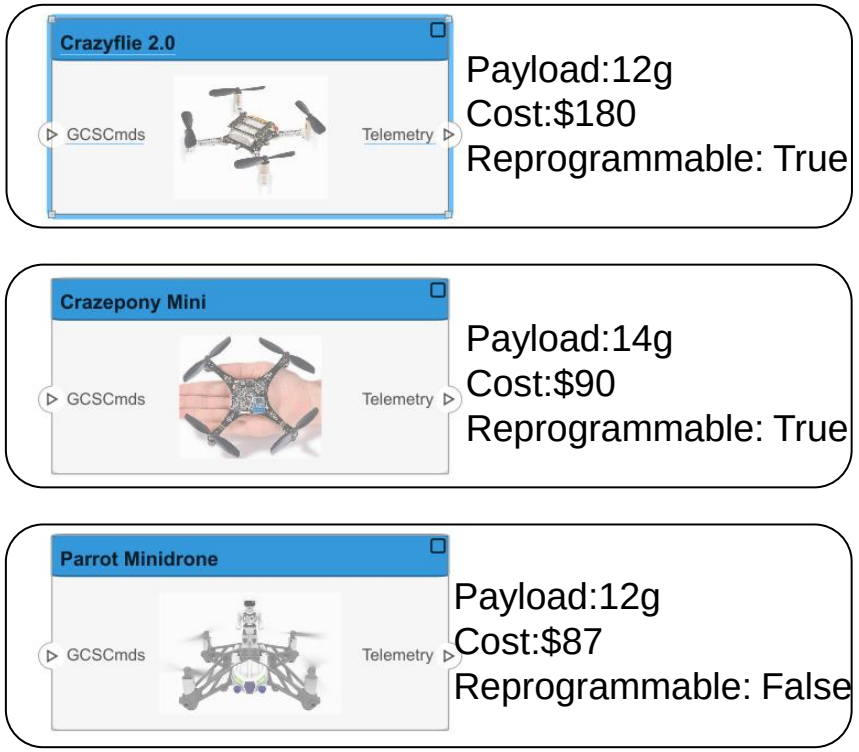


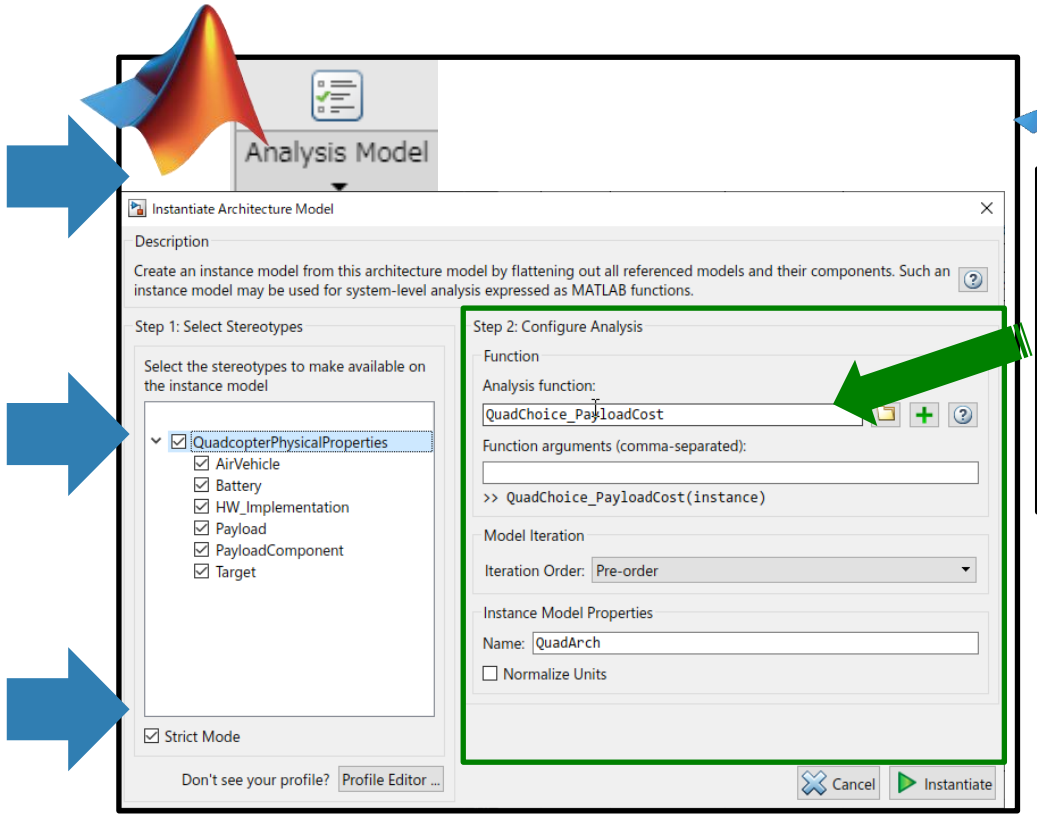
Payload:12g
Cost:$87
Reprogrammable: False

選定基準：リプログラミング可能 ∩ ペイロード量/コスト比最大

システムレベルのアーキテクチャ解析

選定基準をMATLAB言語で数式として定義
各種Toolboxを活用し様々な演算をプロパティ値をベースに実施も可能





QuadChoce_PayloadCost.m

PayloadCost =
PayloadCapacity / Cost
***Reprogrammable**

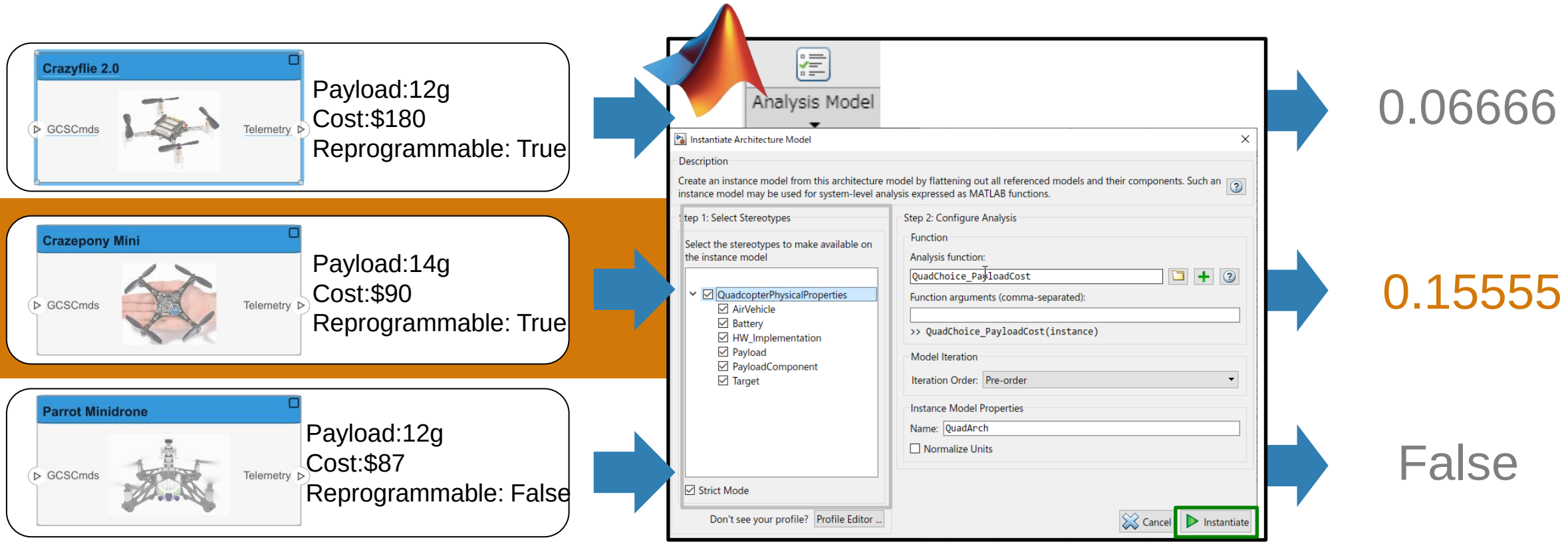
数学および最適化

Curve Fitting Toolbox
Optimization Toolbox
Global Optimization Toolbox
Symbolic Math Toolbox
Mapping Toolbox
Partial Differential Equation Toolbox

AI、データサイエンス、統計

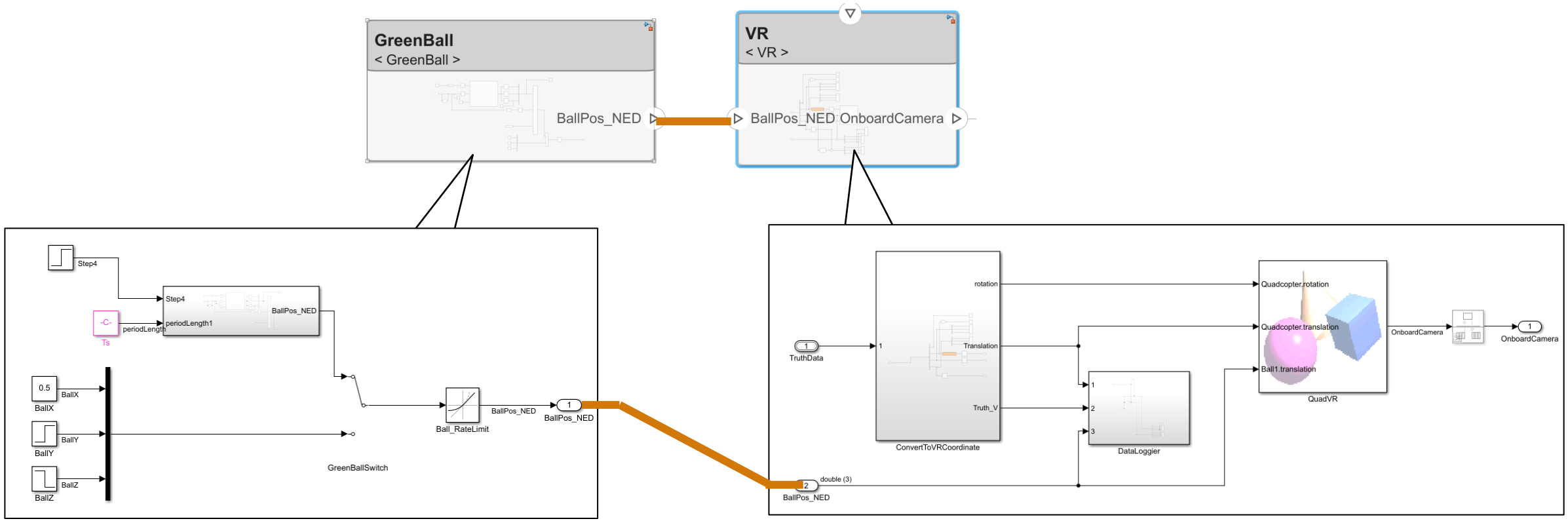
Statistics and Machine Learning Toolbox
Deep Learning Toolbox
Reinforcement Learning Toolbox
Deep Learning HDL Toolbox
Text Analytics Toolbox
Predictive Maintenance Toolbox

システムレベルのアーキテクチャ解析
ステレオタイプを用いた演算結果を基にコンポーネントを選定



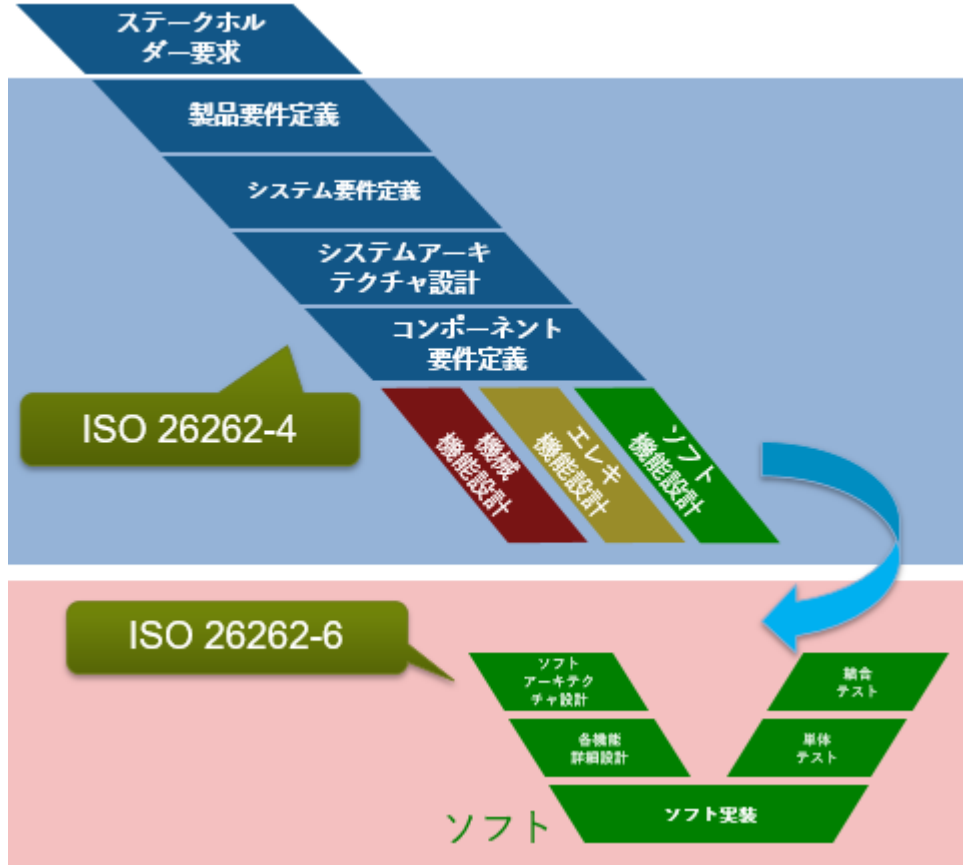
システム振る舞いの妥当性確認

モデル間で信号が接続されるため、システム全体をシミュレーション可能



システム設計の成果物例（ソフトウェア設計に渡す情報）

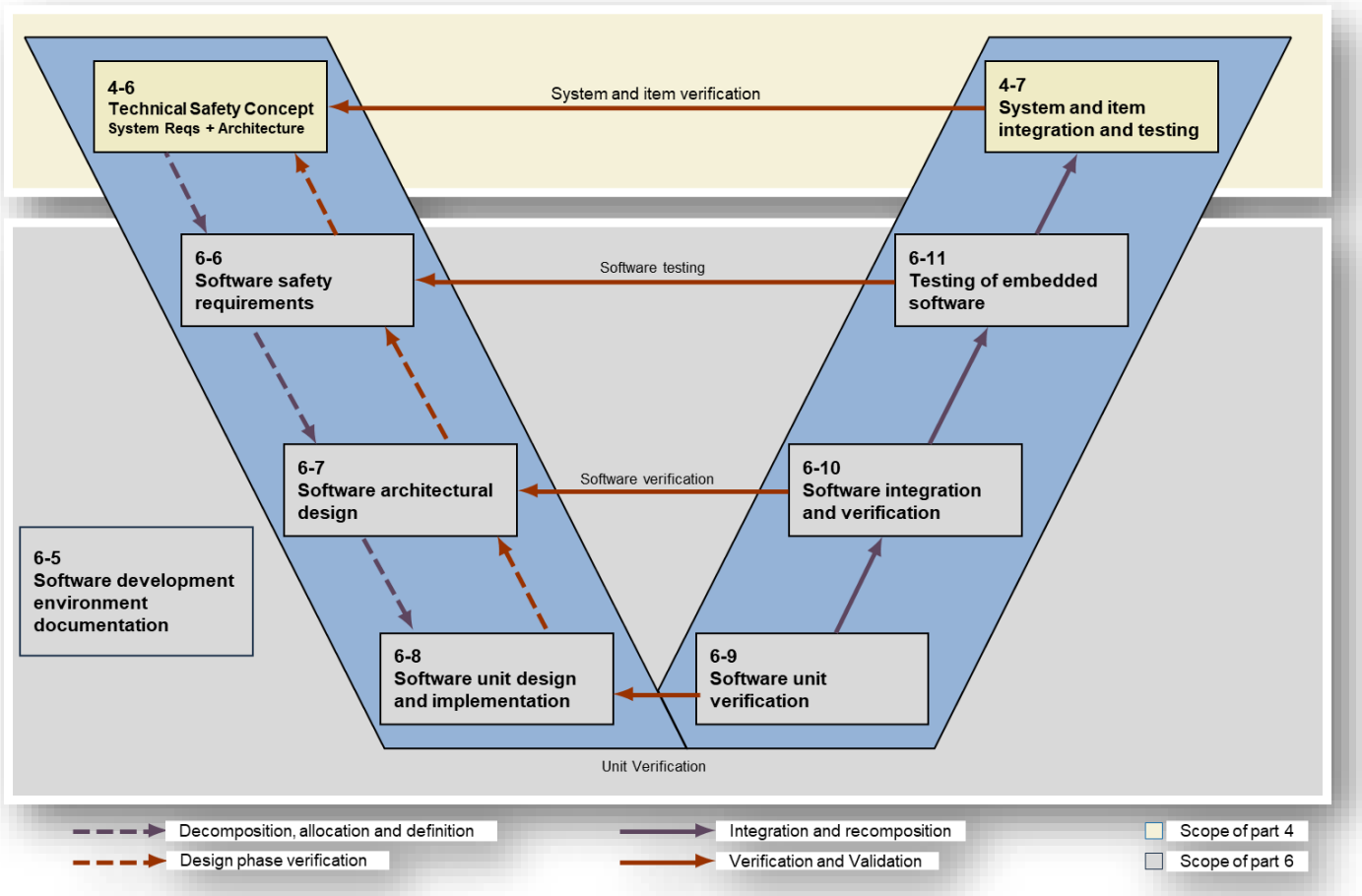
1. ソフトウェアと関連するシステムの要求
2. システムの安全のためのオブジェクティブ
3. ソフトウェアに要求される機能安全のレベル
4. システムの説明とハードウェア部分定義の情報
5. ソフトウェア設計における制約
6. ソフトウェアのプロセスで行うシステム関連の検証活動
7. システムのプロセスで行ったソフトウェア関連検証活動の説明とエビデンス
8. システムのプロセスで確認したソフトウェアに関連するデータの受容性に関するエビデンス



Agenda

1. 高信頼性システム開発のニーズ
   - 機能安全規格の目的
   - 機能安全規格の構成
2. システムレベルにおける製品開発
   - システムズエンジニアリングとは
   - システムズエンジニアリングのプロセス
   - システムズエンジニアリング領域でのMathWorksソリューション活用
3. ソフトウェアレベルにおける製品開発
   - ソフトウェア開発のVプロセスおよび適切な開発ツール
   - 機能安全規格準拠MBDリファレンスワークフロー
   - 静的解析ツールによる自動生成コードとモデルの一致保証

機能安全規格のソフトウェア開発Vプロセス



自動車用 ISO 26262 Part-6: 2018

規格プロセス準拠のための成果物例

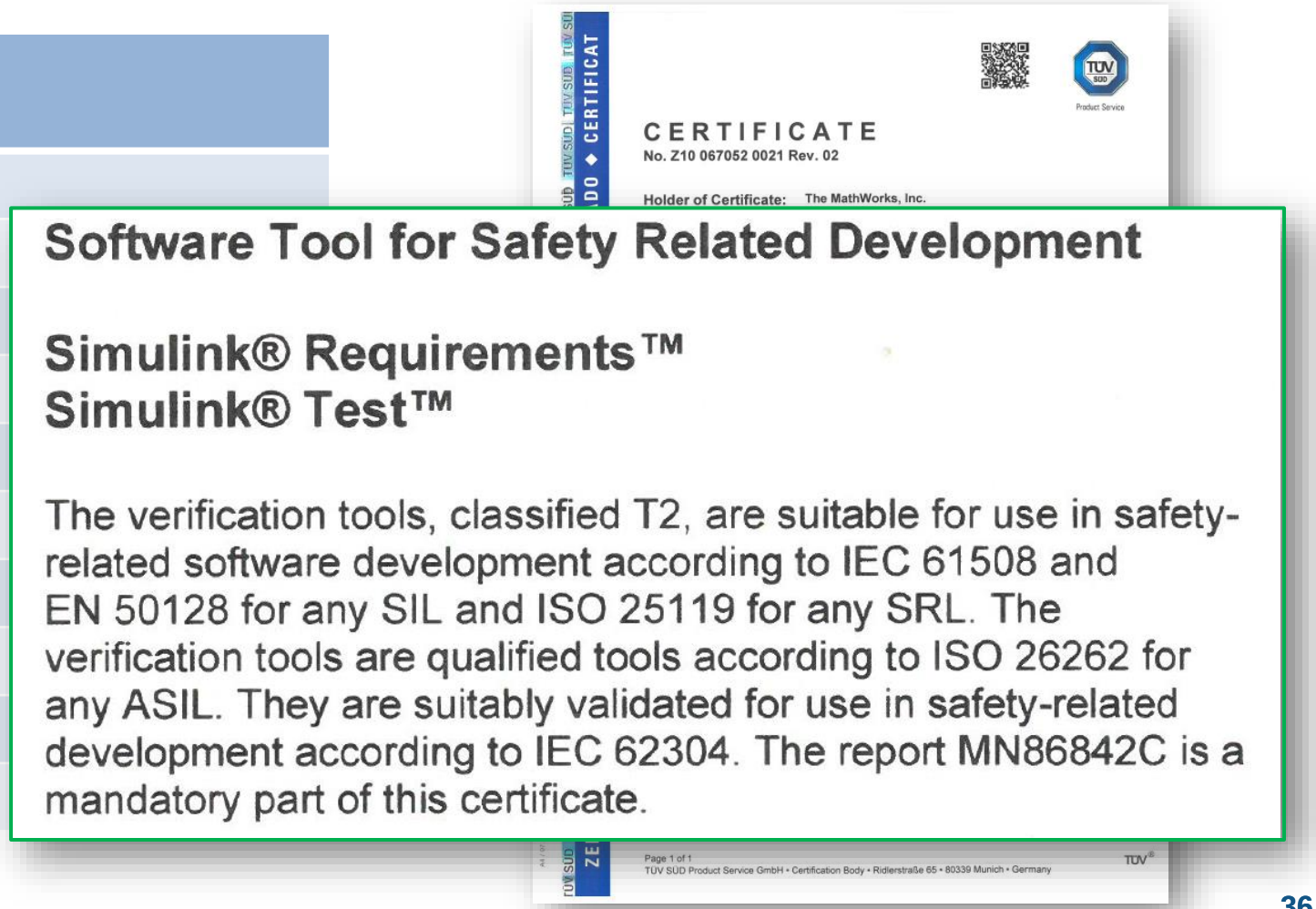
- 要求仕様書
- 検証仕様書
- 検証計画書
- アーキテクチャ設計レポート
- 詳細設計レポート
- 実装用コード
- トレーサビリティ記録
- レビュー結果記録
- スタイルガイドライン準拠レポート
- 要求ベーステストレポート
- カバレッジ分析レポート
- 開発ツールの適格性証明レポート
- ・・

プロセスの成果物例

ソフトウェア開発における適切な開発ツール

- 自動車、鉄道、医療機器などの規格における全ての安全レベルに対して適切なソフトウェア開発ツールとして、 MathWorksのツールは認証機関TÜV SÜDによる事前認定を取得しています

認証機関TÜV SÜDによって事前認定されたMathWorksツールの一覧	
モデル検証ツール	Simulink Requirements
	Simulink Test
	Simulink Check
	Simulink Coverage
	Simulink Design Verifier
コード生成ツール	Embedded Coder
	AUTOSAR Blockset
	Simulink PLC Coder
コード検証ツール	Polyspace Bug Finder
	Polyspace Code Prover



ソフトウェア開発における適切な開発ツール

- 自動車用機能安全規格のISO 26262-Part6 : 2018では、MathWorksのSimulinkとStateflowが適切な開発ツールとして取り上げられています

Table 5 — Notations for software unit design

	Notations	ASIL A	ASIL B	ASIL C	ASIL D
1a	Natural language[a]	++	++	++	++
1b	Informal notations				
1c	Semi-formal notations[b]				
1d	Formal notations				

[a] Natural language can complement the use of notat
natural language or provide an explanation and rationa

EXAMPLE To avoid possible ambiguity of natural langu
diagram with natural language can be used.

[b] Semi-formal notations can include pseudocode or n

NOTE UML®, SysML®, Simulink® and Stateflow®
information is given for the convenience of users of this
products.

Table 2 — Notations for software architectural design

	Notations	ASIL A	ASIL B	ASIL C	ASIL D
1a	Natural language[a]	++	++	++	++
1b	Informal notations	++	++	+	+
1c	Semi-formal notations[b]	+	+	++	++
1d	Formal notations	+	+	+	+

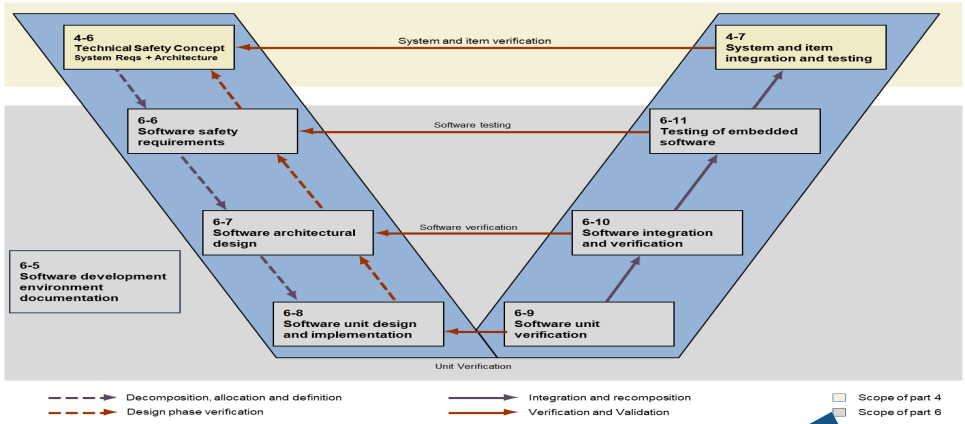
[a] Natural language can complement the use of notations for example where some topics are more readily expressed in natural language or providing explanation and rationale for decisions captured in the notation.

[b] Semi-formal notations can include pseudocode or modelling with UML®, SysML®, Simulink® or Stateflow®.

NOTE UML®, SysML®, Simulink® and Stateflow® are examples of suitable products available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of these products.

機能安全規格準拠MBDリファレンスワークフロー

- 第三者認証機関である TÜV SÜD 社より審査され承認されています
- MBDリファレンスワークフローの活用により、ソフトウェア開発プロセス一部の自動化が可能です

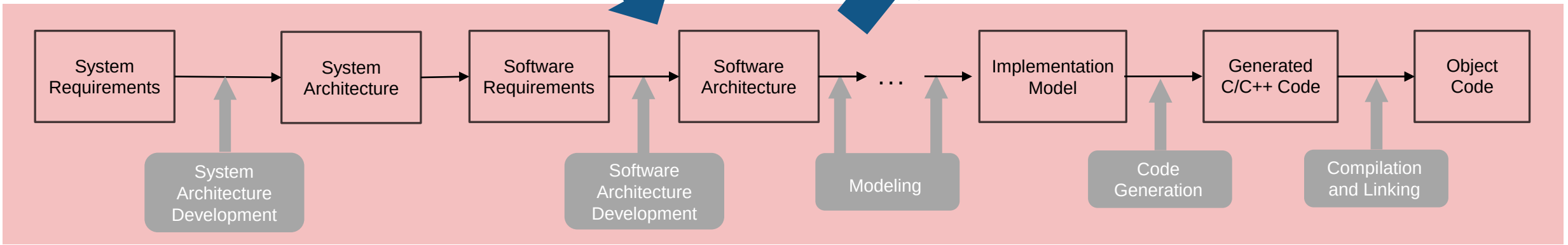


機能安全規格のVプロセス

規格プロセス準拠のための成果物例

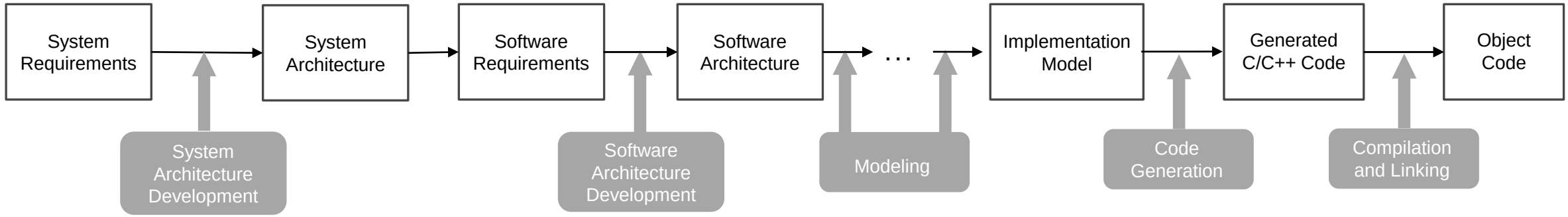
- 要求仕様書
- 検証仕様書
- 検証計画書
- アーキテクチャ設計レポート
- 詳細設計レポート
- 実装用コード
- トレーサビリティ記録
- レビュー結果記録
- スタイルガイドライン準拠レポート
- 要求ベーステストレポート
- カバレッジ分析レポート
- 開発ツールの適格性証明レポート
- ・・

MBDリファレンスワークフローで成果物の自動作成ができる部分は多い



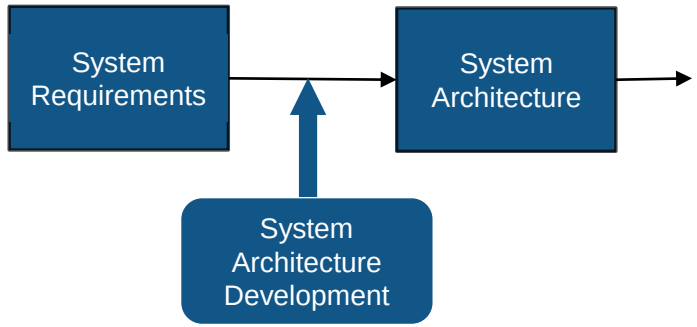
機能安全規格を準拠するためのMBDリファレンスワークフロー

機能安全規格準拠MBDリファレンスワークフロー



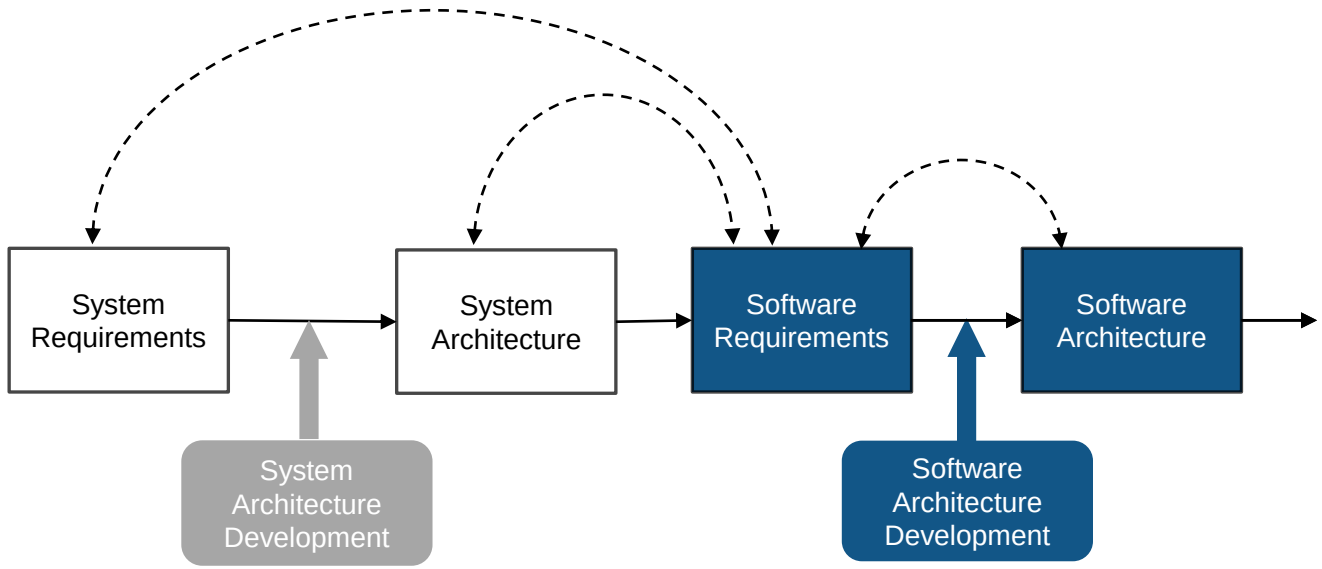
System Level | **Software Level**

機能安全規格準拠MBDリファレンスワークフロー：
System Requirements and Architecture



System Level

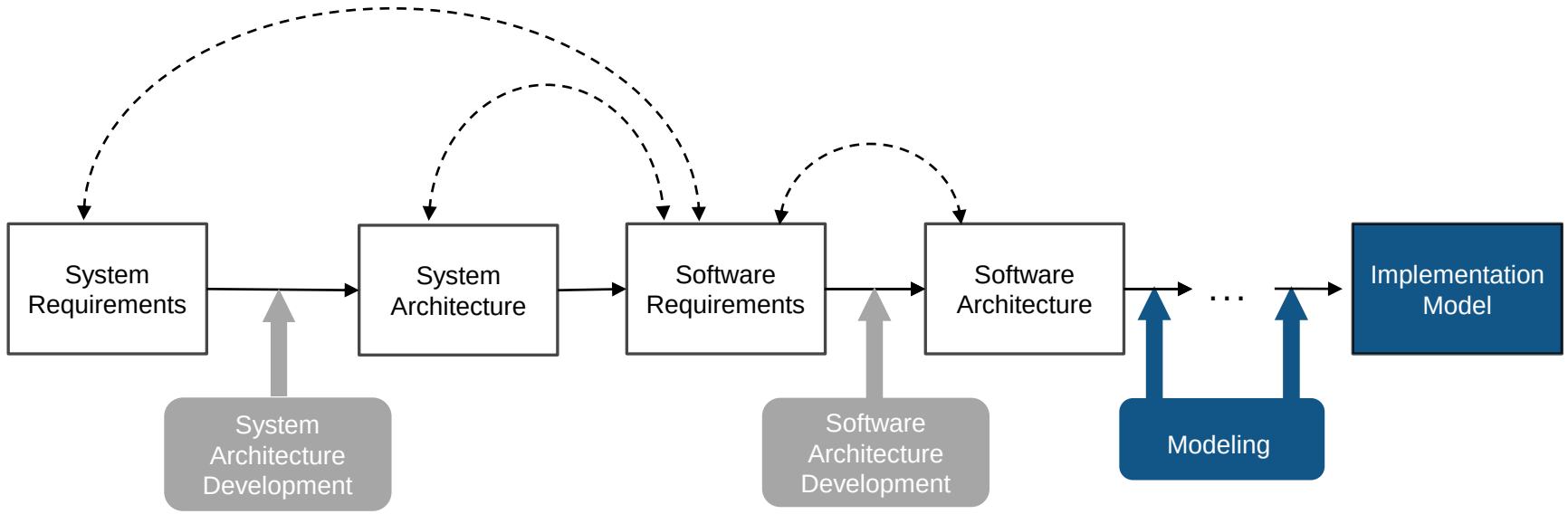
機能安全規格準拠MBDリファレンスワークフロー：Software Requirements and Architecture



System Level

Software Level

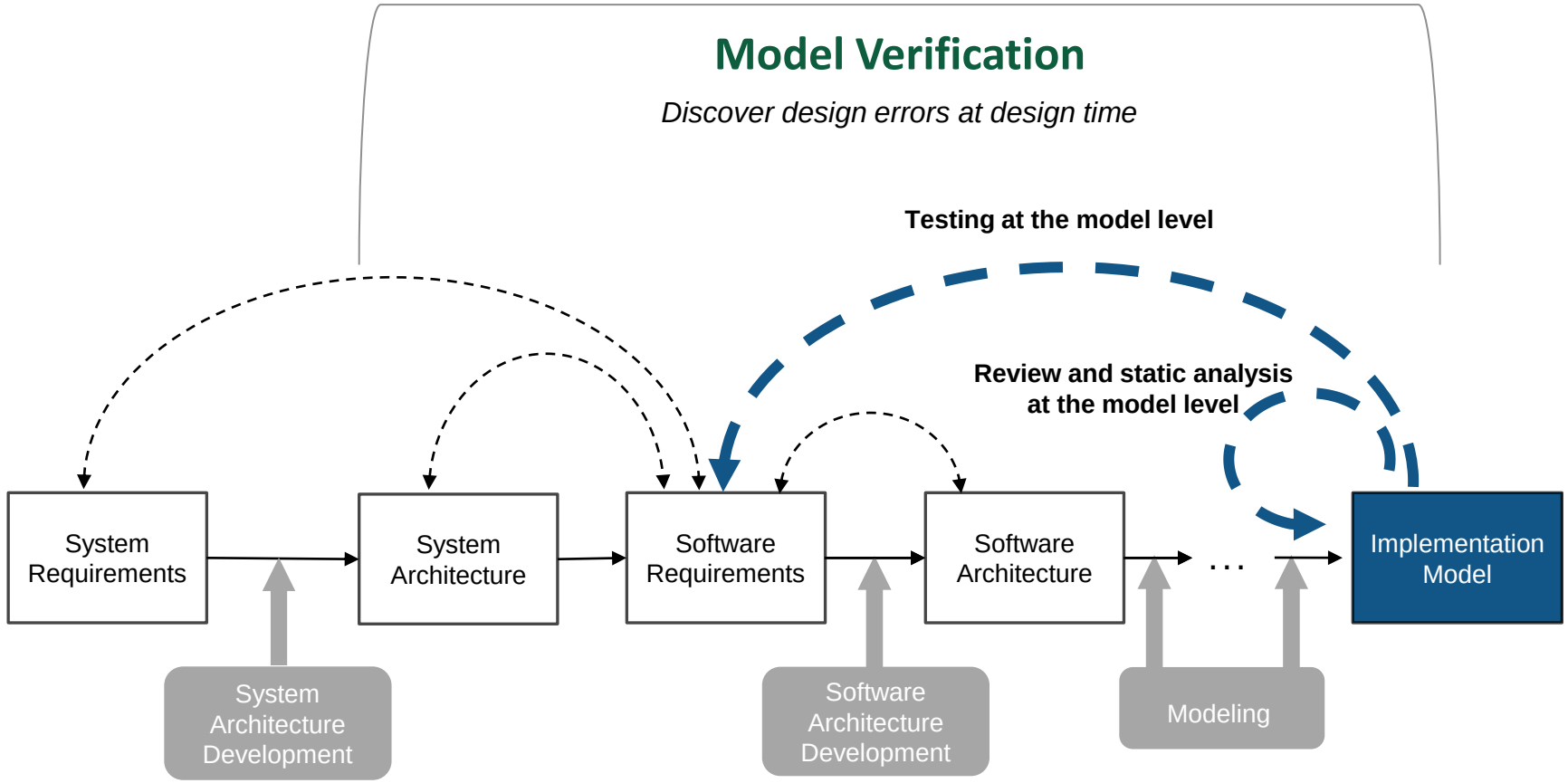
機能安全規格準拠MBDリファレンスワークフロー：Detailed Design



System Level

Software Level

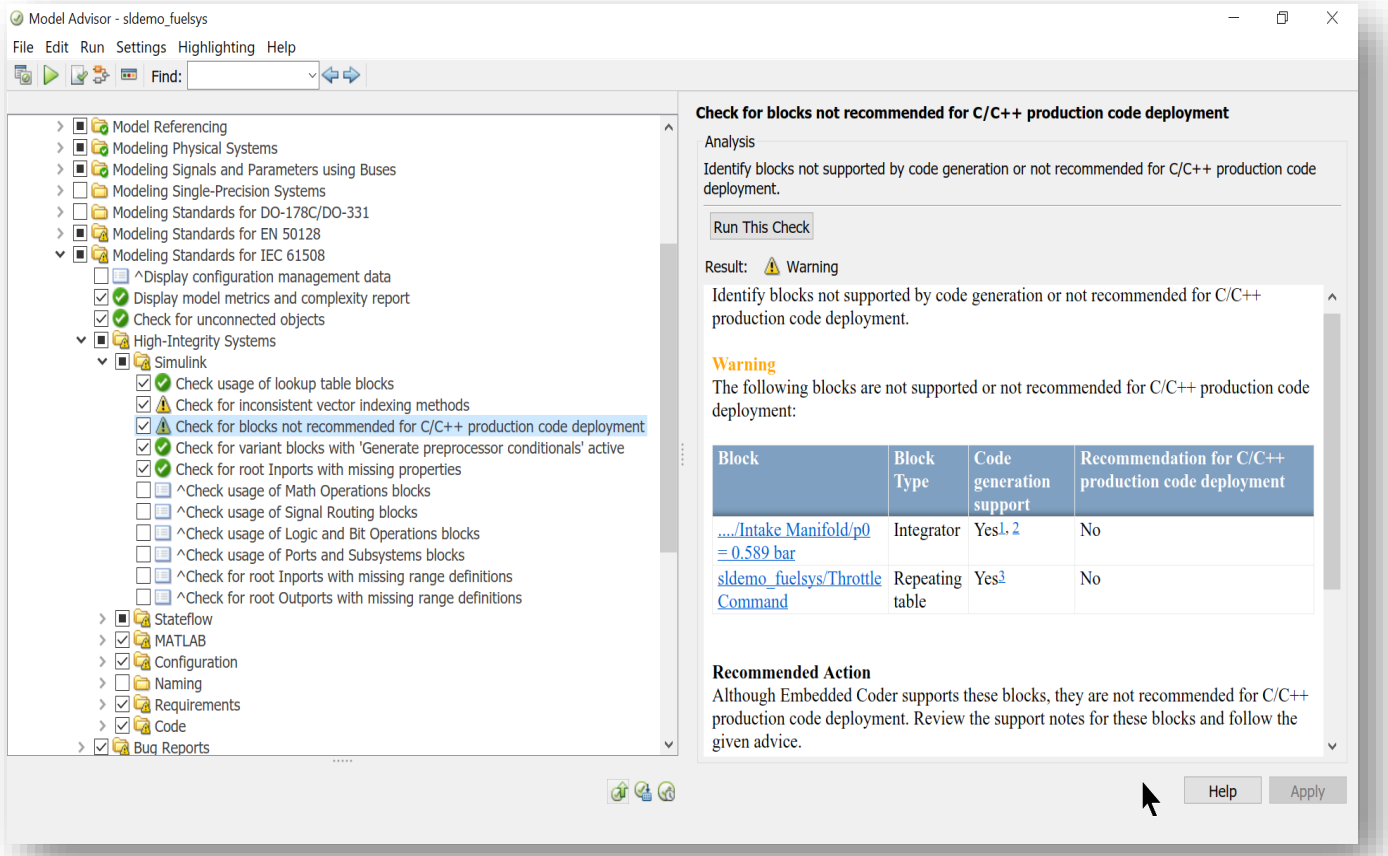
機能安全規格準拠MBDリファレンスワークフロー：Model Verification



System Level | Software Level

モデリングスタイルガイドラインのチェック

Model Advisor Analysis

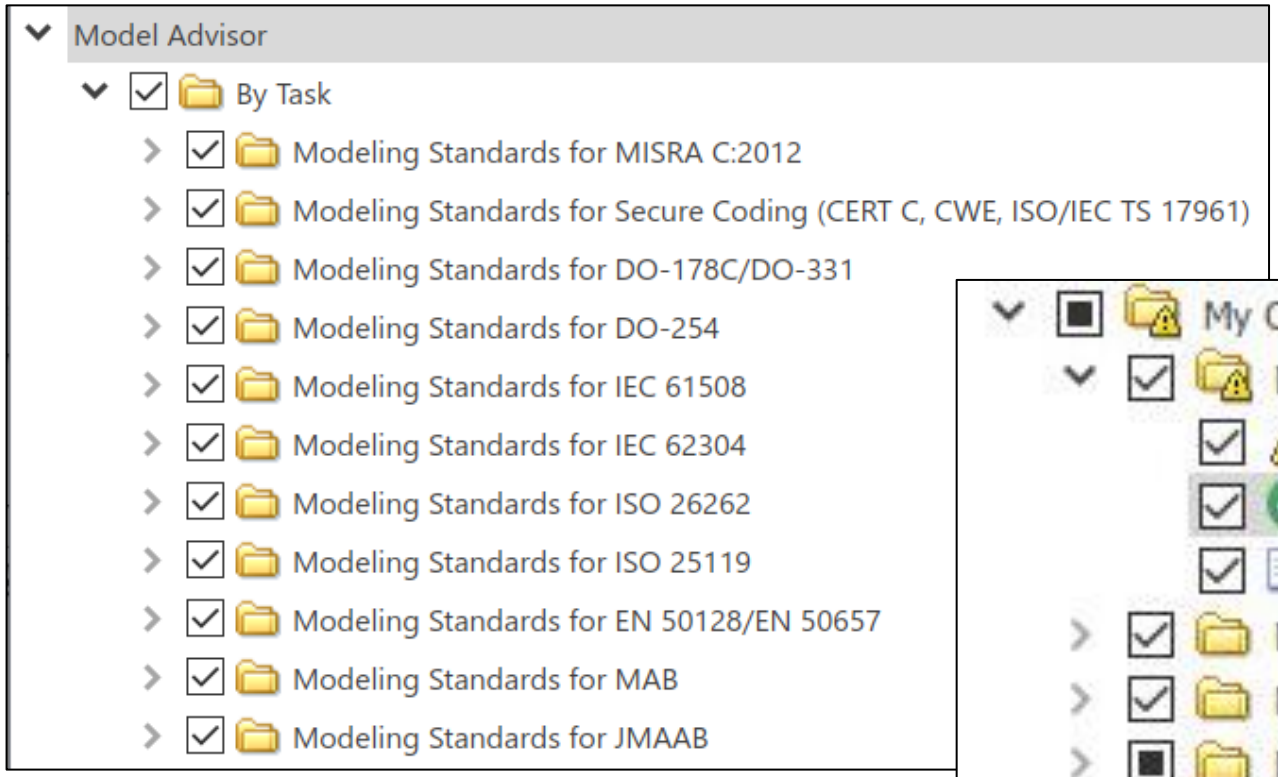


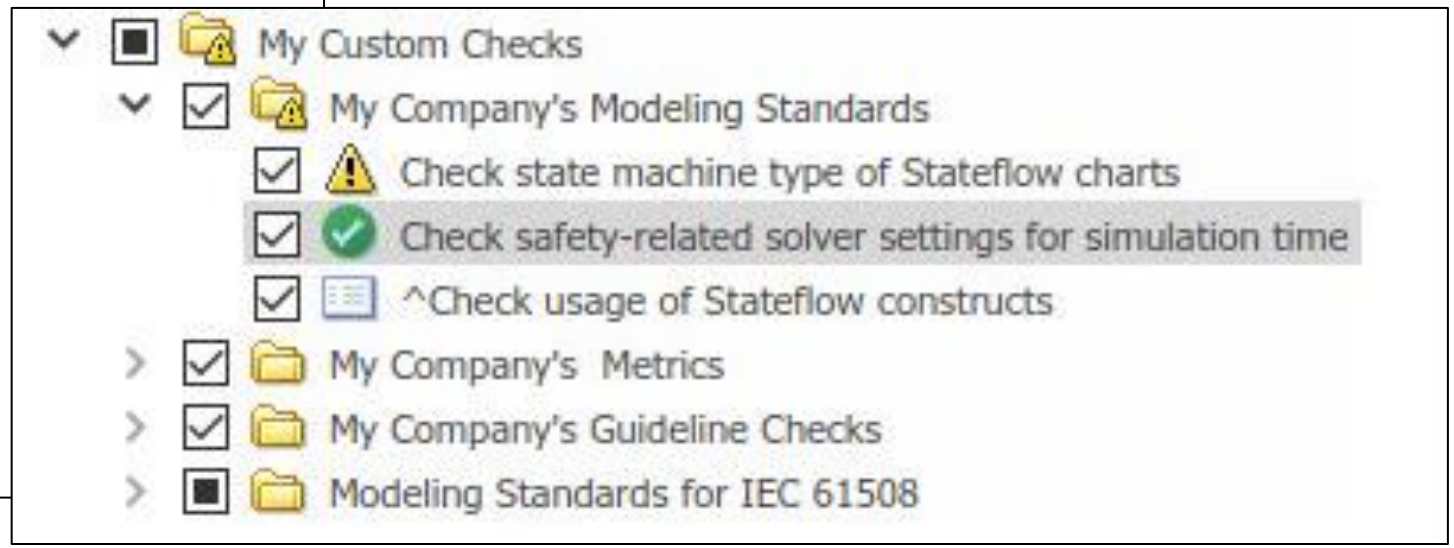
スタイルガイドラインチェックの目的

- 可読性
- セマンティクス
- パフォーマンスと効率性
- 再利用性
- ……

機能安全規格準拠用のモデリングスタイルガイドライン

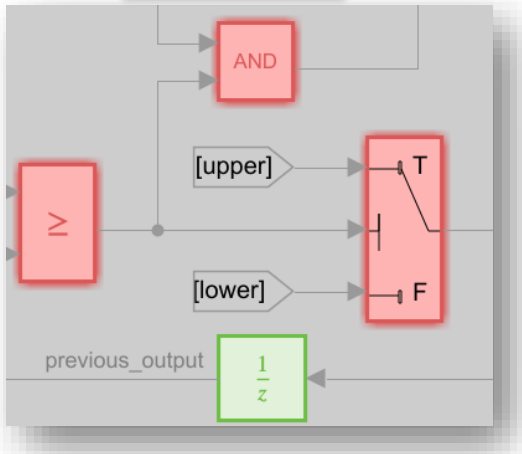
- Simulink Check は、様々な機能安全規格に対応するモデリングスタイルガイドラインを事前に用意して、ユーザー様にご提供しています
- 必要に応じて、スタイルガイドラインのカスタマイズや追加なども可能です





モデルカバレッジの測定と分析

Simulink

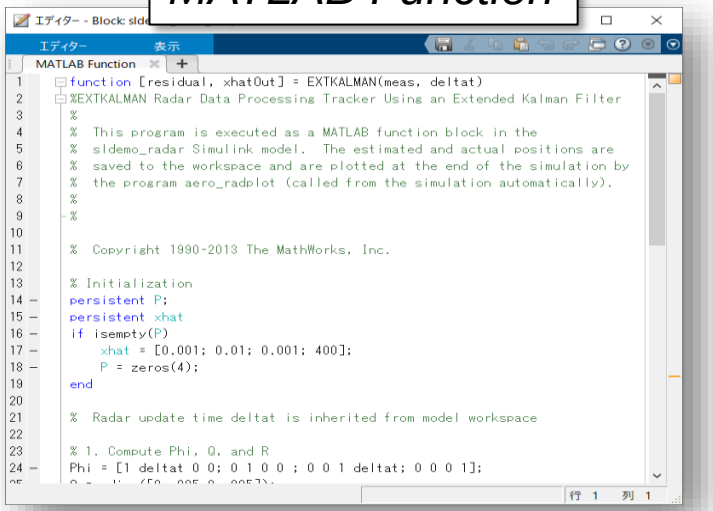


Stateflow

カバレッジ計測と分析の目的

- テスト不足箇所の特定
- 要求抜け漏れ有無の確認
- 意図しない機能有無の確認

MATLAB Function

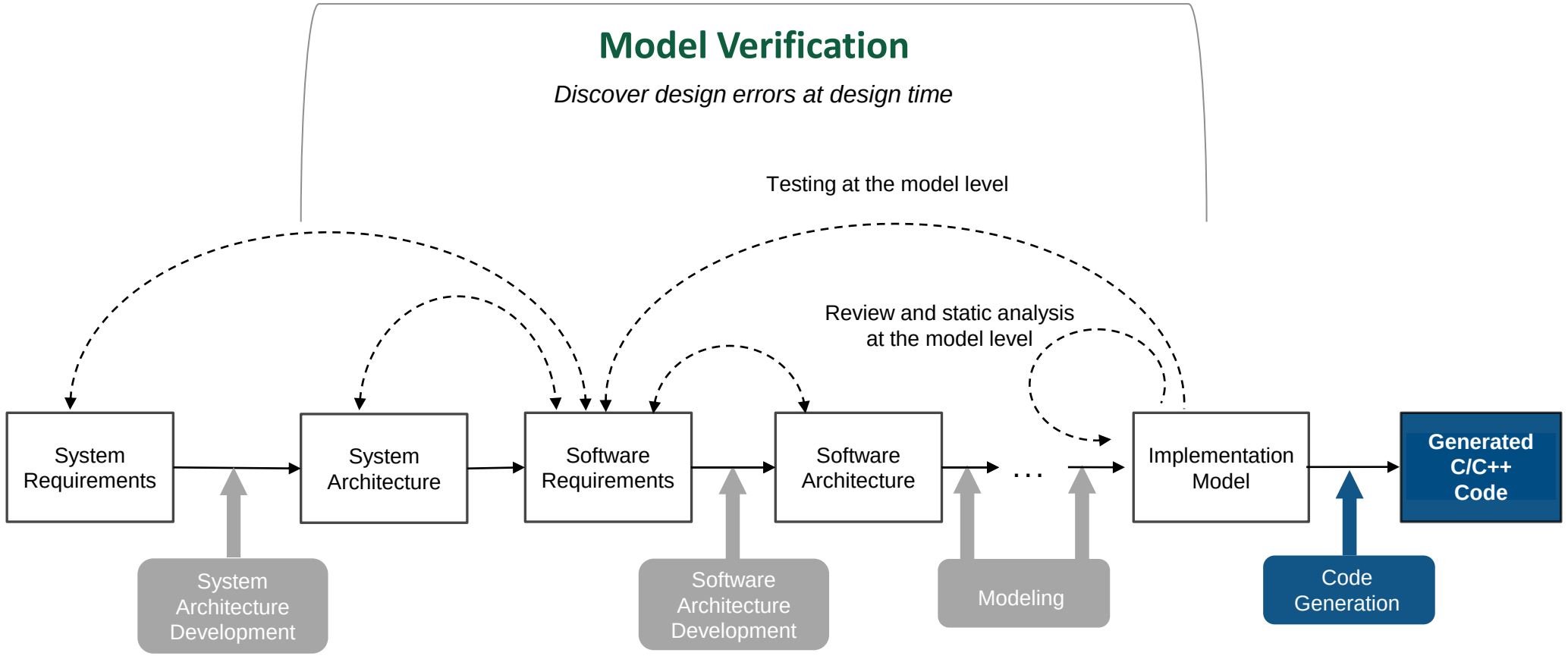


Simulink Coverage のレポート

Summary

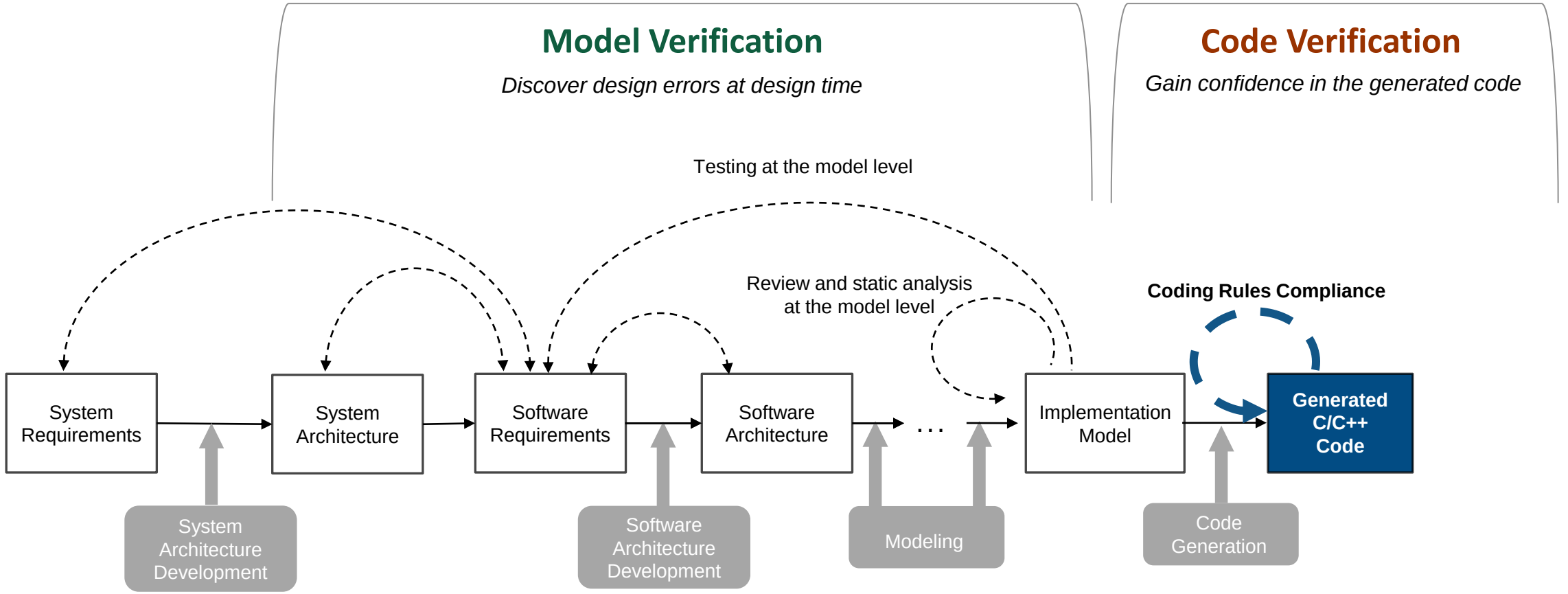
Model Hierarchy/Complexity	Test 1									
		Decision		Condition		MCDC		Execution	Relational Boundary	Saturation on integer overflow
1. sldemo_fuelsys	80	34%		34%		7%		90%	10%	50%
2. Engine Gas Dynamics	13	71%		NA		NA		100%	50%	50%
3. Mixing & Combustion	3	67%		NA		NA		100%	NA	50%
4. EGO Sensor	2	100%		NA		NA		NA	NA	NA
5. System Lag		NA		NA		NA		100%	NA	NA
6. Throttle & Manifold	10	73%		NA		NA		100%	50%	50%
7. Intake Manifold	2	100%		NA		NA		100%	NA	50%
8. MATLAB Function	2	100%		NA		NA		NA	NA	NA
9. Throttle	6	83%		NA		NA		100%	100%	50%

機能安全規格準拠MBDリファレンスワークフロー：Code Generation



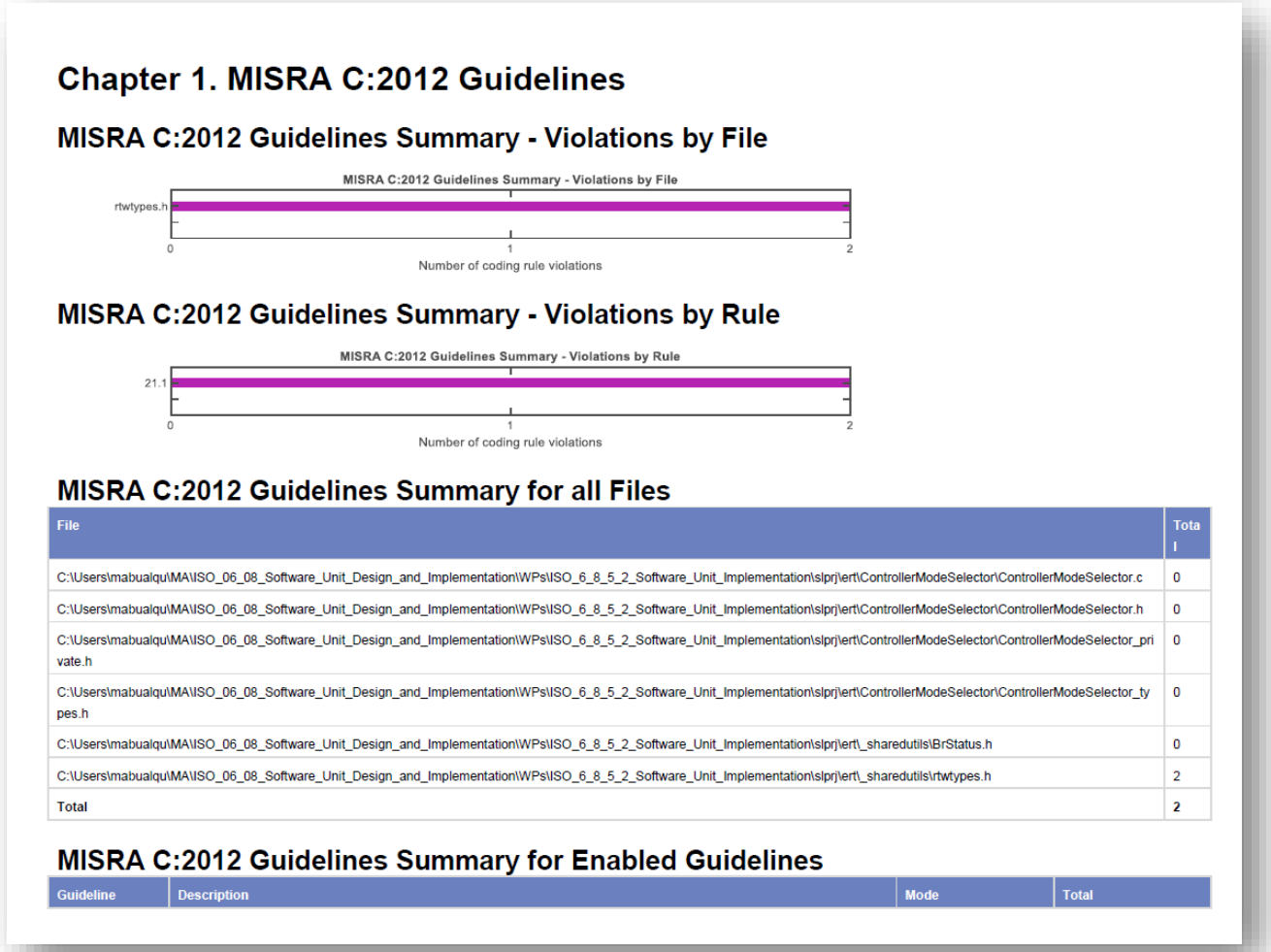
System Level | Software Level

機能安全規格準拠MBDリファレンスワークフロー：Code Verification



System Level | **Software Level**

MISRA-C / CERT-C などコーディングルール準拠の確認



Chapter 1. MISRA C:2012 Guidelines

MISRA C:2012 Guidelines Summary - Violations by File

MISRA C:2012 Guidelines Summary - Violations by Rule

MISRA C:2012 Guidelines Summary for all Files

File	Total
C:\Users\mabualqu\MA\ISO_06_08_Software_Unit_Design_and_Implementation\WPs\ISO_6_8_5_2_Software_Unit_Implementation\slprj\ert\ControllerModeSelector\ControllerModeSelector.c	0
C:\Users\mabualqu\MA\ISO_06_08_Software_Unit_Design_and_Implementation\WPs\ISO_6_8_5_2_Software_Unit_Implementation\slprj\ert\ControllerModeSelector\ControllerModeSelector.h	0
C:\Users\mabualqu\MA\ISO_06_08_Software_Unit_Design_and_Implementation\WPs\ISO_6_8_5_2_Software_Unit_Implementation\slprj\ert\ControllerModeSelector\ControllerModeSelector_private.h	0
C:\Users\mabualqu\MA\ISO_06_08_Software_Unit_Design_and_Implementation\WPs\ISO_6_8_5_2_Software_Unit_Implementation\slprj\ert\ControllerModeSelector\ControllerModeSelector_types.h	0
C:\Users\mabualqu\MA\ISO_06_08_Software_Unit_Design_and_Implementation\WPs\ISO_6_8_5_2_Software_Unit_Implementation\slprj\ert_sharedutils\BrStatus.h	0
C:\Users\mabualqu\MA\ISO_06_08_Software_Unit_Design_and_Implementation\WPs\ISO_6_8_5_2_Software_Unit_Implementation\slprj\ert_sharedutils\rtwtypes.h	2
Total	2

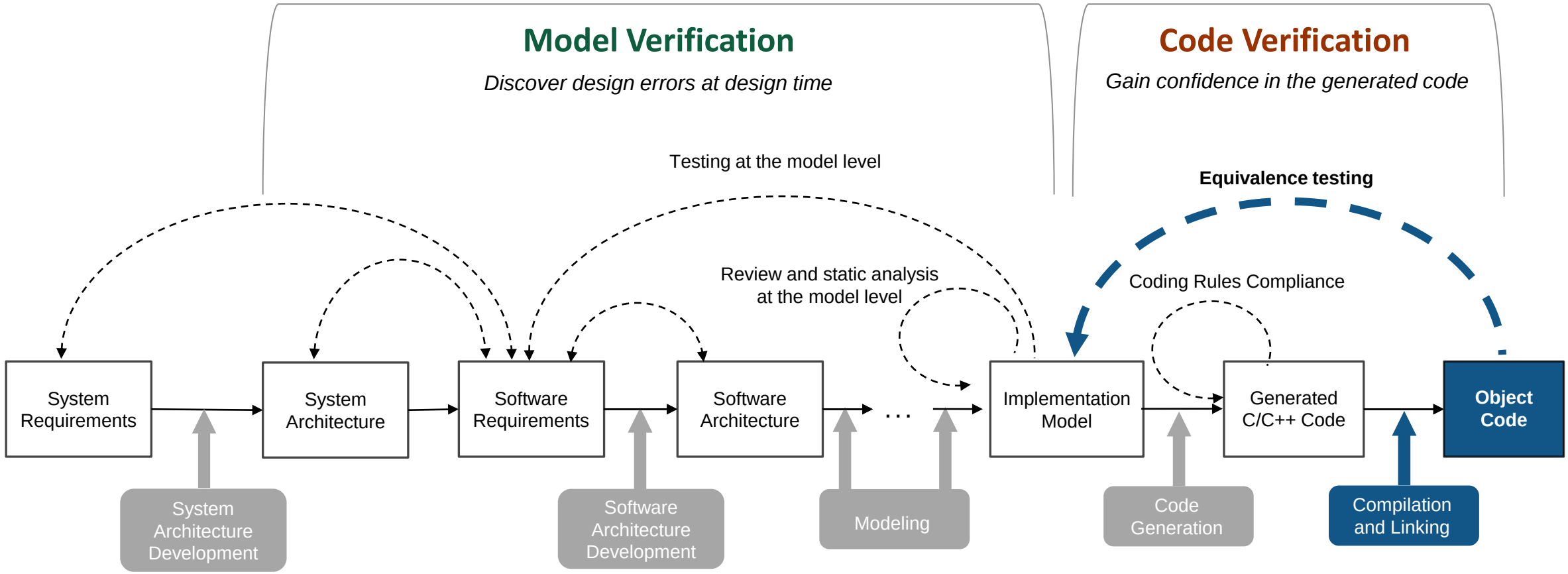
MISRA C:2012 Guidelines Summary for Enabled Guidelines

Guideline	Description	Mode	Total

Polyspaceを用いるコーディングルール準拠の確認

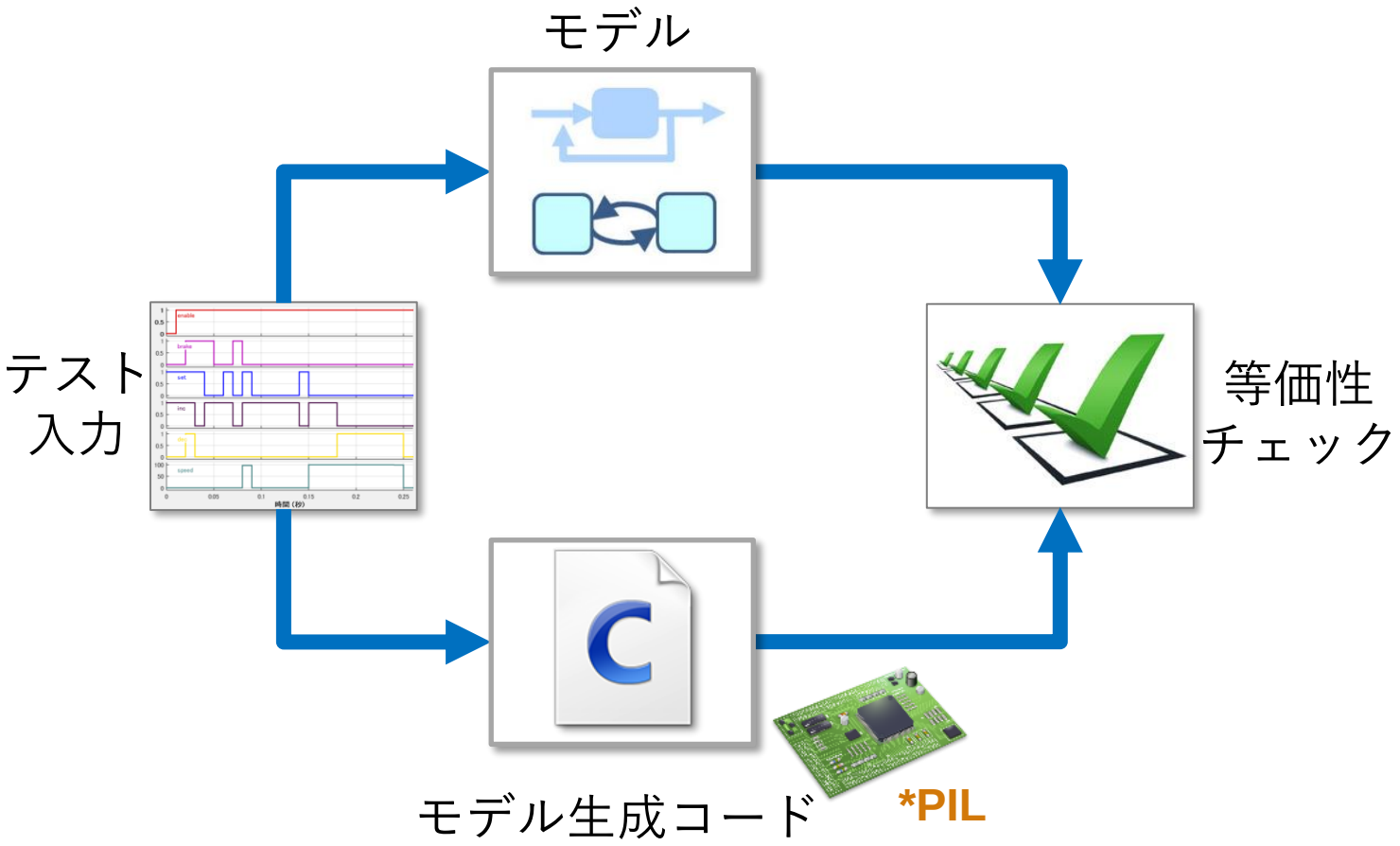
- MISRAコーディングルールチェック
  - MISRA C®：2004 チェッカー
  - MISRA C®：2004 AC AGC チェッカー
  - MISRA C®：2012 チェッカー
  - MISRA® C++ チェッカー
- セキュリティコーディングルールチェック
  - CERT-all：セキュアルール/推奨
    - CERT Cルール、および、推奨に対応するバグ項目
  - ISO 17961：Cセキュアコーディングルール

機能安全規格準拠MBDリファレンスワークフロー：Code Verification



System Level | **Software Level**

Back-to-Backテストによる自動生成コードとモデルの一致保証

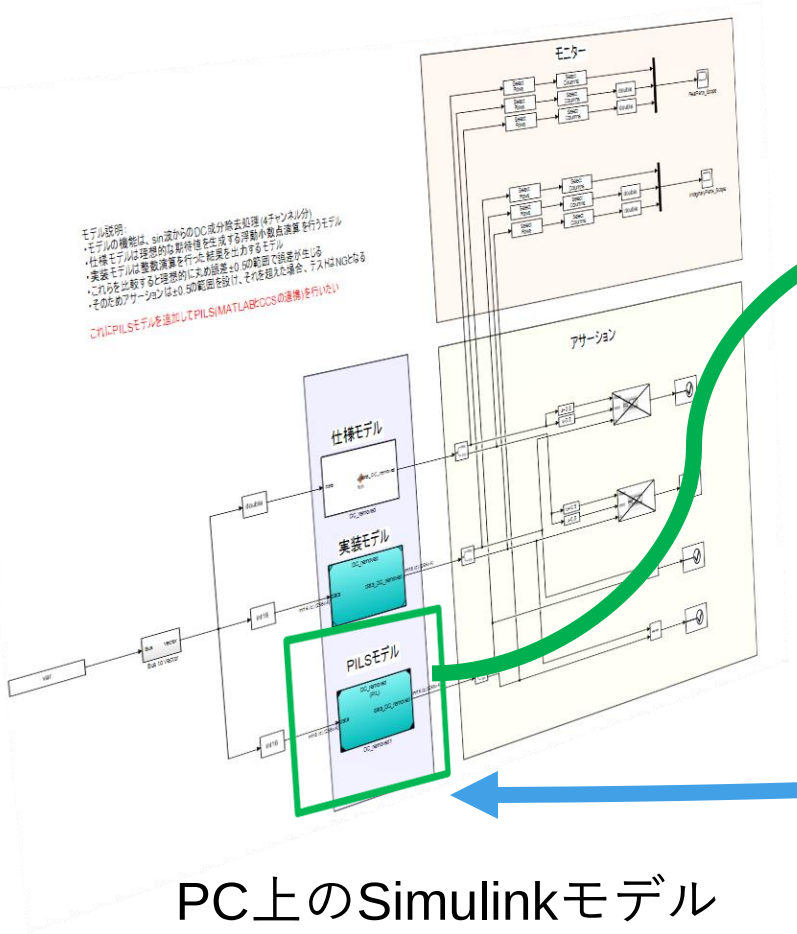


Back-to-Backテストの目的

- モデル＆生成コード動作の等価性
- コード生成ツール設定ミス
- コード生成ツール不具合
- コンパイラ不具合
- 処理系依存動作
- メモリ消費量評価
- 実行速度評価

*PIL（Processor In the Loop）：MCU/シミュレータ・エミュレータ上でコード実行

PILを用いるBack-to-Backテストの動作イメージ



PC上のSimulinkモデル

コード生成

コンパイル
／リンク

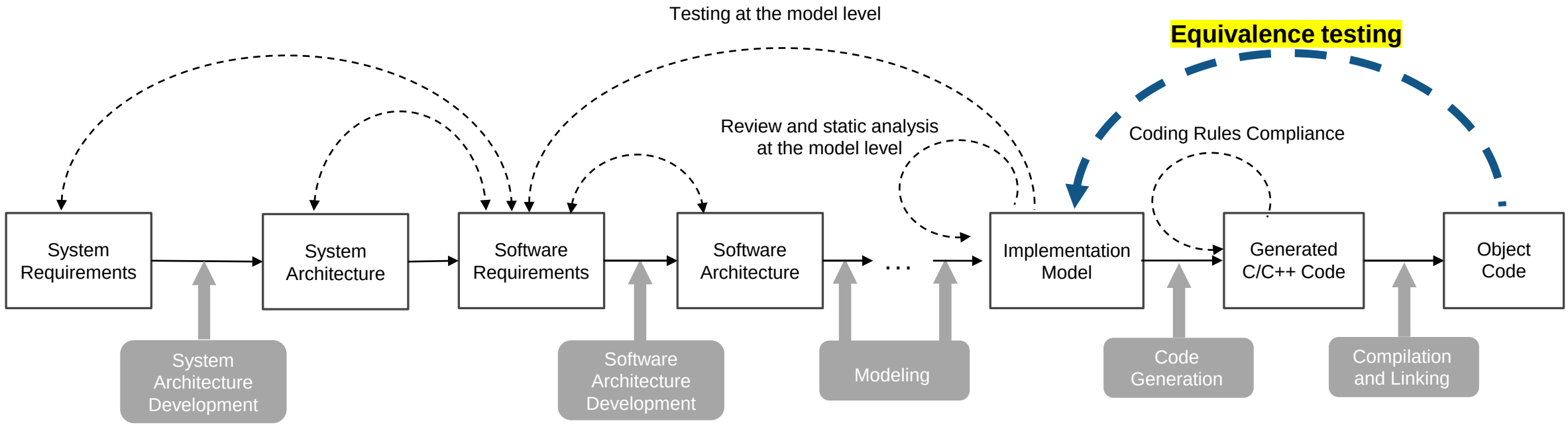
ダウンロード

評価ボード

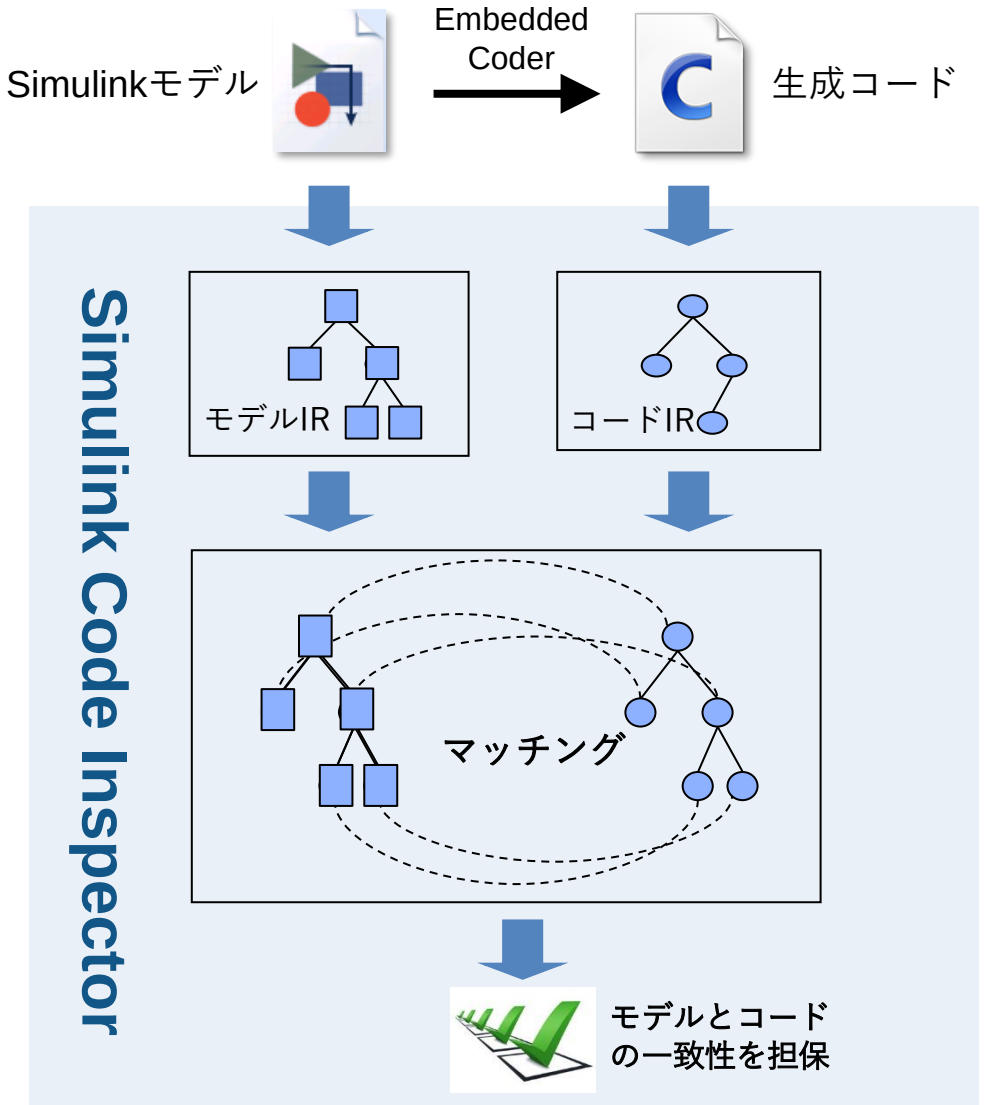
シミュレーション中の通信

静的解析ツールによる自動生成コードとモデルの一致保証：Simulink Code Inspector の活用

一致保証の方法	手法・ツール	特徴
動的テスト	Back-to-Backテスト	モデリングのスタイルにおける制約が少ないため、設計効率が高い
静的解析	**Simulink Code Inspector**	**モデルとコードの一致性を確認するためのBack-to-Backテストが省略可能**



Simulink Code Inspector の仕組みとメリット



仕組み

- モデルとモデル生成コードをIRレベルで1対1に解析し、両者の一致性を検証します
  - Back-to-Backテストによる数値計算の結果比較ではなく、両者が同じ構造・内容となっているかを確認して、一致性を担保します

メリット

- 目視のコードレビューやBack-to-Backテストによる等価確認の省略ができます
- Simulink Code Inspector解析に必要な制約をモデルに課すことで、量産モデルに求められる標準化や生成コード品質・信頼性を確保することができます

IR (Intermediate Representation)：構文解析された計算用内部表現

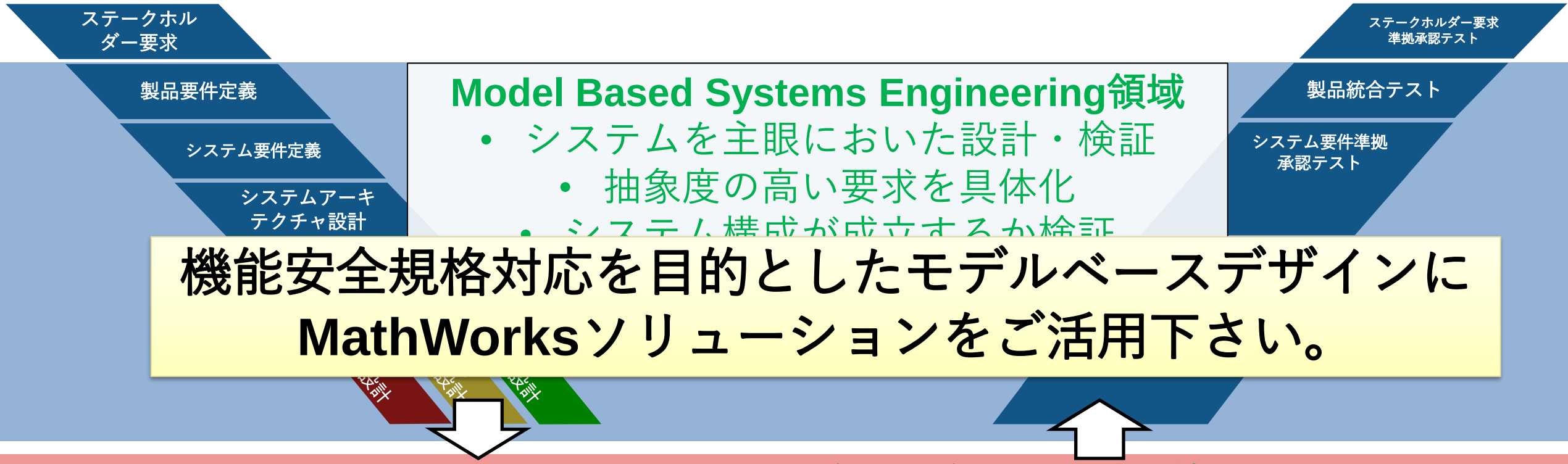
機能安全規格準拠MBDリファレンスワークフロー
検証作業項目のまとめ

モデル検証	検証項目	ツール
Review and static analysis at the model level （モデルレベルのレビューと静的解析）	モデルレベルの設計レビュー	Simulink Report Generator
	モデリングスタイルガイドラインのチェック	Simulink Check
	モデル設計エラーの検出	Simulink Design Verifier
Testing at the model level （モデルレベルのテスト）	トレーサビリティチェック	Simulink Requirements
	モデルシミュレーション結果と期待値との比較	Simulink Test
	モデルカバレッジの測定と分析	Simulink Coverage / Simulink Design Verifier

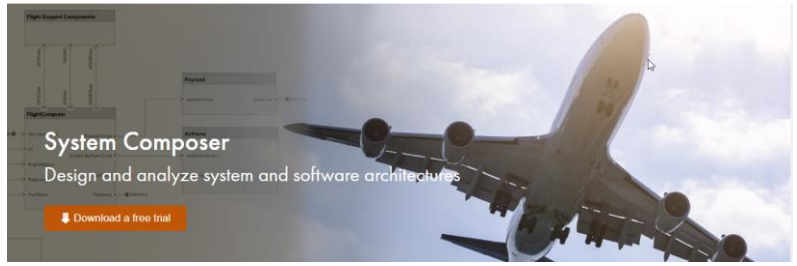
コード検証	検証項目	ツール
Equivalence testing （モデルとコードの等価確認）	トレーサビリティチェック	Simulink Requirements / IEC Certification Kit
	コードカバレッジの測定と分析	Simulink Coverage
	生成コードとモデルとのBack-to-Backテスト	Embedded Coder / Simulink Test
	＊静的解析による生成コードとモデルの一致保証	**Simulink Code Inspector**
Coding Rules Compliance （コーディングルール準拠の確認）	MISRA-C/CERT-Cなどへの準拠確認	Polyspace Bug Finder

＊Simulink Code Inspector による実装コードとモデルの一致保証がされる場合は、Back-to-Backテストによる一致性の確認が省略可能です

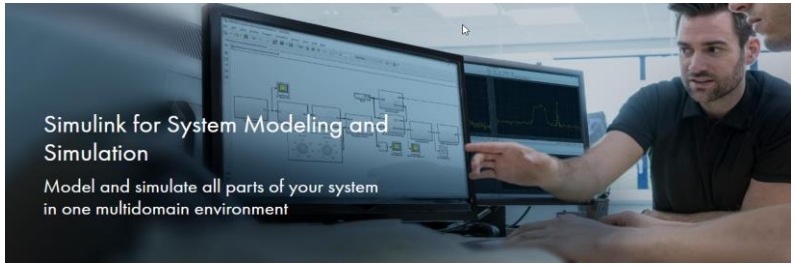
まとめ


ステークホルダー要求
製品要件定義
システム要件定義
システムアーキテクチャ設計
ステークホルダー要求準拠承認テスト
製品統合テスト
システム要件準拠承認テスト
Model Based Systems Engineering領域
• システムを主眼においた設計・検証
• 抽象度の高い要求を具体化
• システム構成が成立するか検証
機能安全規格対応を目的としたモデルベースデザインに
MathWorksソリューションをご活用下さい。
Model Based Design領域：各領域主眼で設計・検証
機械詳細設計
各部品金型設計
機械部生産
機械部結合試験
部品単体品質試験
機械
回路全体構成設計
部品定数設計
アートワーク定義
回路結合試験
部品・ユニット試験
基板実装
エレキ
ソフトアーキテクチャ設計
各機能詳細設計
ソフト実装
結合テスト
単体テスト
ソフト

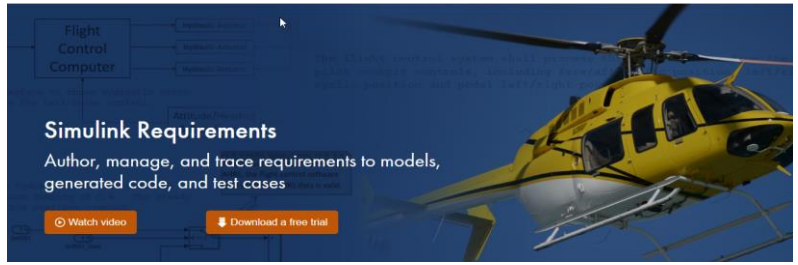
Learn More



[System Composer]

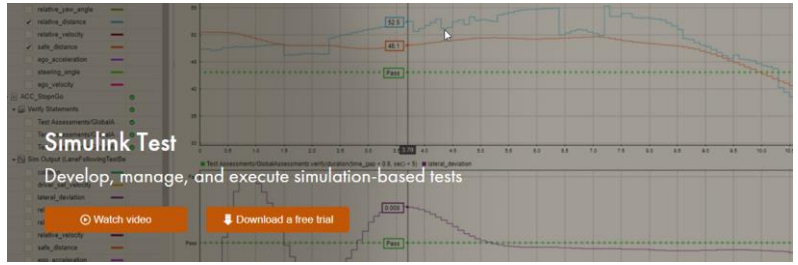


[Model-Based Systems Engineering]



[Simulink Requirements]

[System Modeling and Simulation]



[Simulink Test]

[ISO 26262 Advisory Service]

MATLAB EXPO 2021

Thank you