

# DCER 研究会

～ D-Case活用事例 ～

～ エンジン制御開発への適用 ～

トヨタ自動車 エンジン技術開発部

石崎 直哉

'12/9/14

# 自分の使命とは？



エンジン制御の問題が  
ある事件へと発展していく...

# 安全性認識の高まりと制御開発管理上の課題

## 発端：2010年の品質・安全問題

- ・ お客様のトヨタに対する信頼失墜
- ・ クルマに求められる安全・品質の変化
- ・ 電子制御システムの安全も大きな問題に



2010/2月 米国公聴会での証言

## ＜問題を通して痛感したこと＞

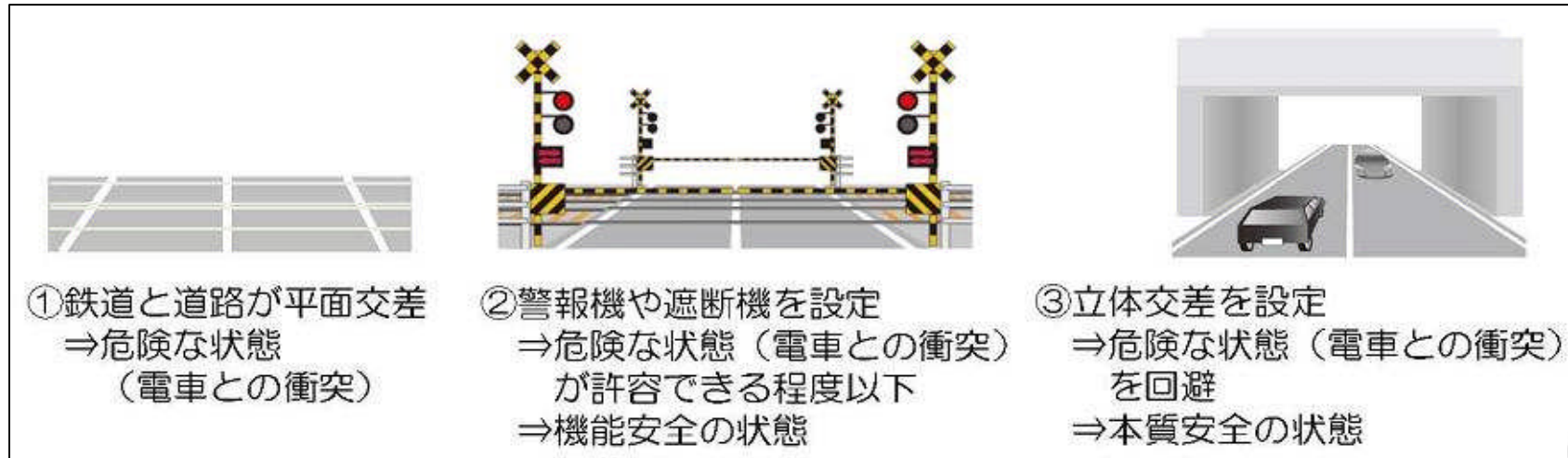
- ・ 現状把握の遅れ ⇒ 意思決定の遅れ
- ・ 問題は北米から一気に全世界へ広がった
- ・ 想定外の使われ方も「想定外」では済まされない  
(フロアマット)
- ・ システム安全への厳しい要求、説明の難しさ  
(BOS、電子スロットル)

ISO26262規格に準拠した製品開発を実施することに決定

# 機能安全規格 (ISO26262)の概要と課題

## 機能安全とは

リスクを許容できる程度以下に対策して安全を確保すること。  
(リスクをゼロにすることは、本質安全。)



## ISO26262のスコープ

◆**対象車両**: 3.5t以下の**量産車**が対象(2輪車、トラックは対象外)  
障害者用などの特別車両は対象外

◆**対象システム**: 安全に関連する**電気・電子システム**

◆**対象の危険事象**: **システム内の部品故障**が原因の危険事象

開発者の**設計ミス**が原因の危険事象

対象部品・対象車両の**製造工程のミス**が原因の危険事象



# ISO26262規格の要求

## 要求1

それぞれの電子制御システムについて、要求される安全レベル(ASIL)を設定し、そのレベルに応じた適切な設計・評価手法を採用すること

## 要求2

構想～実装までの各プロセスの成果物について、安全要求と紐付けすること(トレーサビリティ)

## 要求3

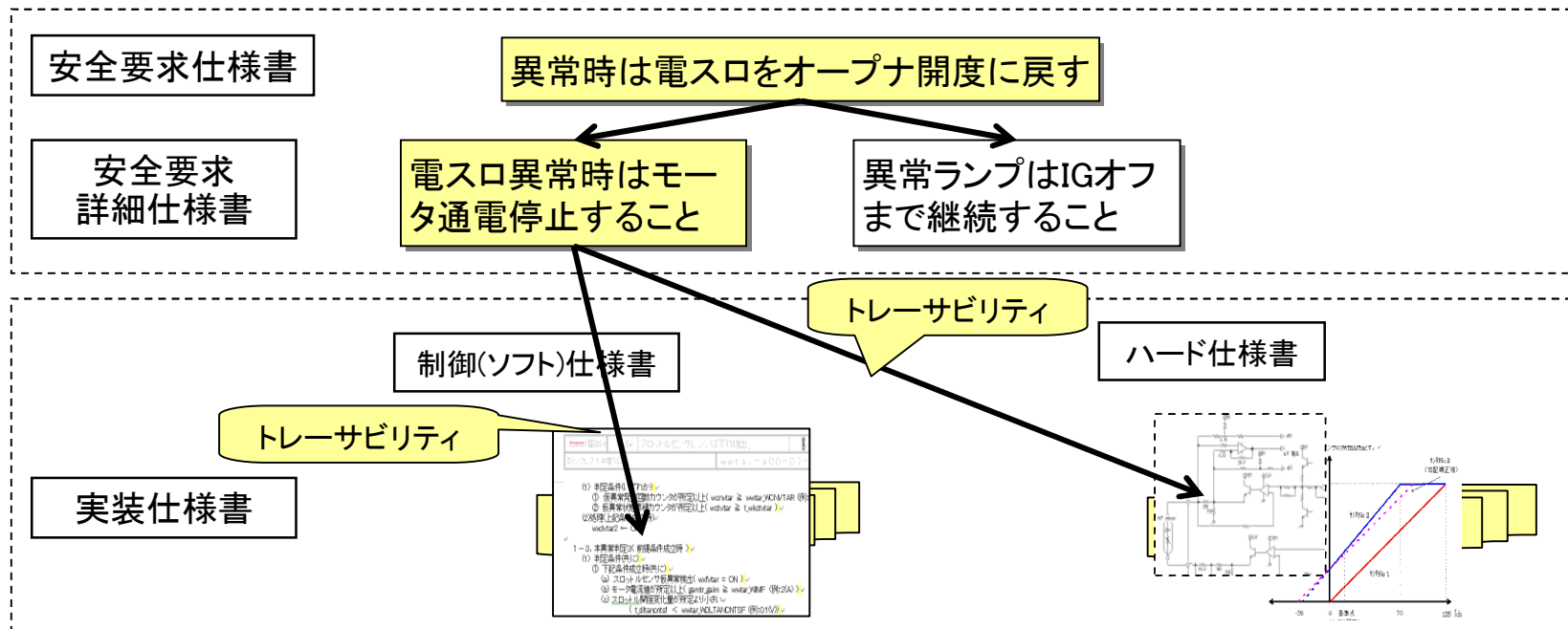
安全を実現するための開発プロセスを定義・実行・管理し、エビデンスを残すこと。



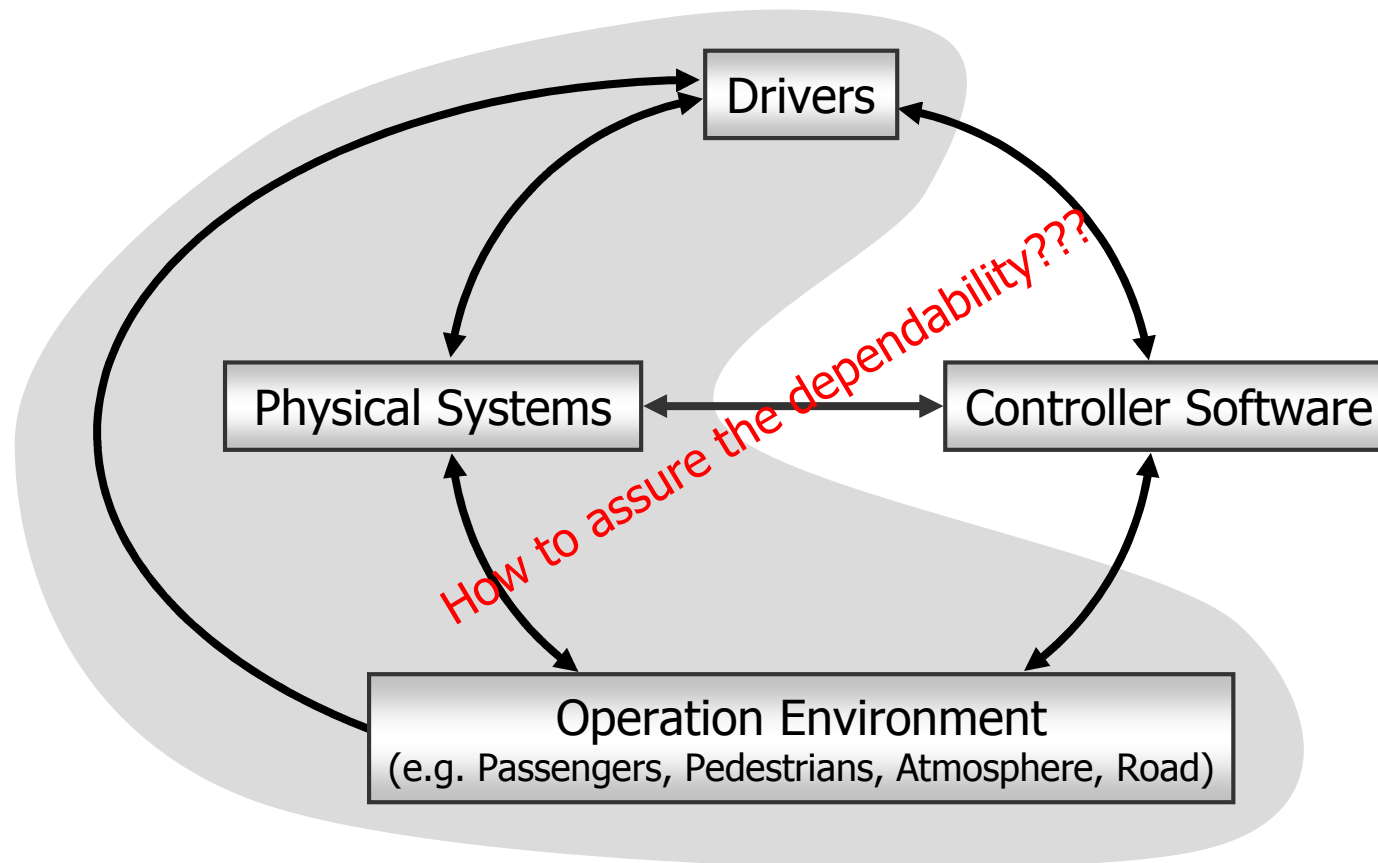
※規格では、上記の共通ルール以外に「システム構想」「システム開発」など工程別のルールも規定される。

## 要求2の具体的イメージ

例)

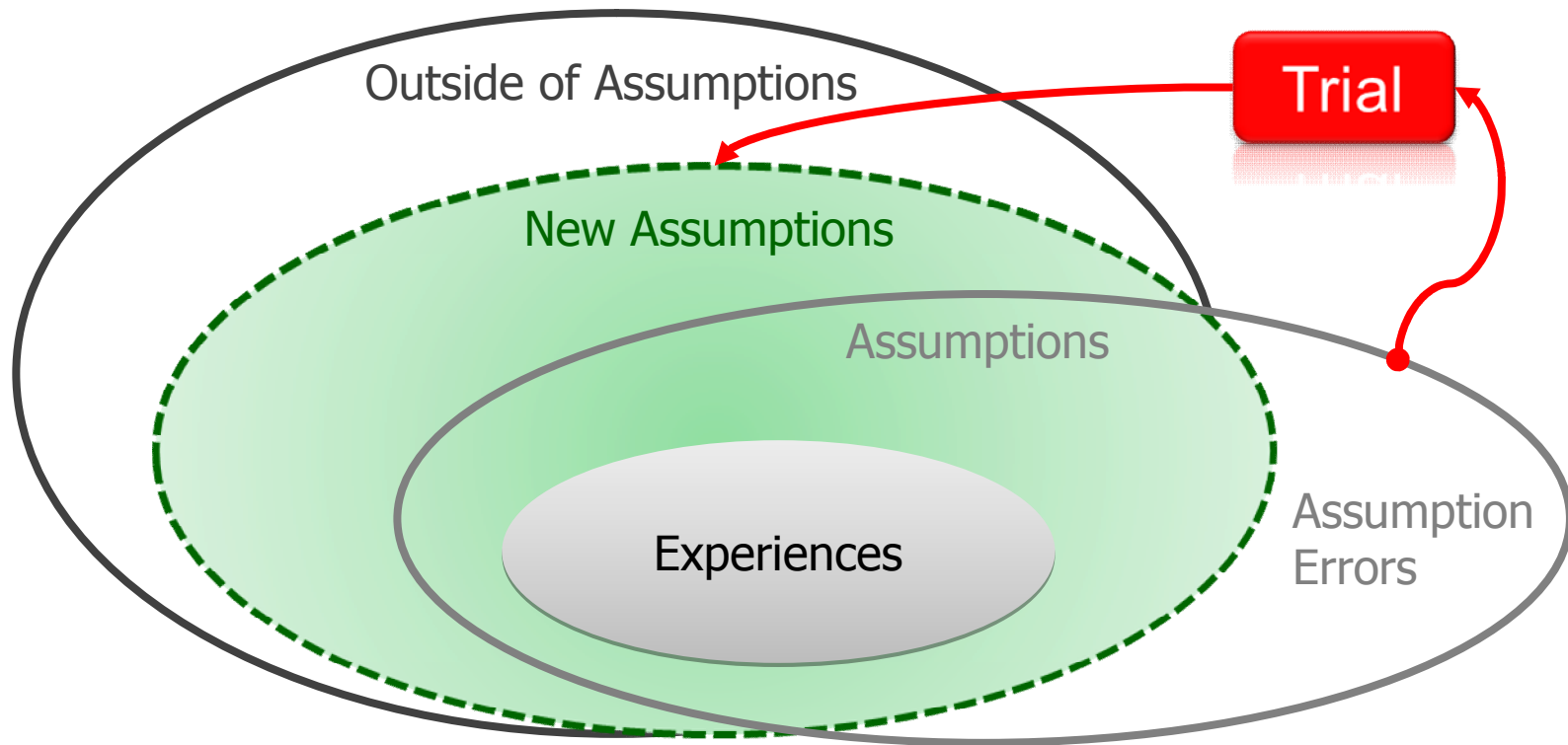


# Characteristics of Consumer Devices



There are frequent interactions between physical system and control software in open, diverse, and dynamic environment.

# Fundamental Approach



Almost all automotive companies well manage the known factors. To ensure the safety and reliability, unknown factors must be well managed.  
➔ Iterations are fundamental approach to manage unknown factors.

# Current Standards and Concerns

- ISO 12100 and ISO 14121, the framework of system assurance, are originally for **industrial machines** and IEC 61508 is originally for functional safety of **industrial plant**.  
(\* Functional safety standards were developed based on IEC 61508 in each industry, such as ISO 26262 for automotive, ISO 13482 for personal robot)
- **Management of unknown factors** is the fundamental issue to ensure the safety and the reliability of consumer devices.

Current standards like ISO 26262 don't state:

- **Rapid iteration** that is a basic way to manage unknown factors
- **Dynamic behavior models** although the term of MBD (Model-Based Development) appears in the part of guideline
- **Connection with physics**





# エンジン制御開発での取組み (MBDの必要性)

※MBD=モデルベース開発

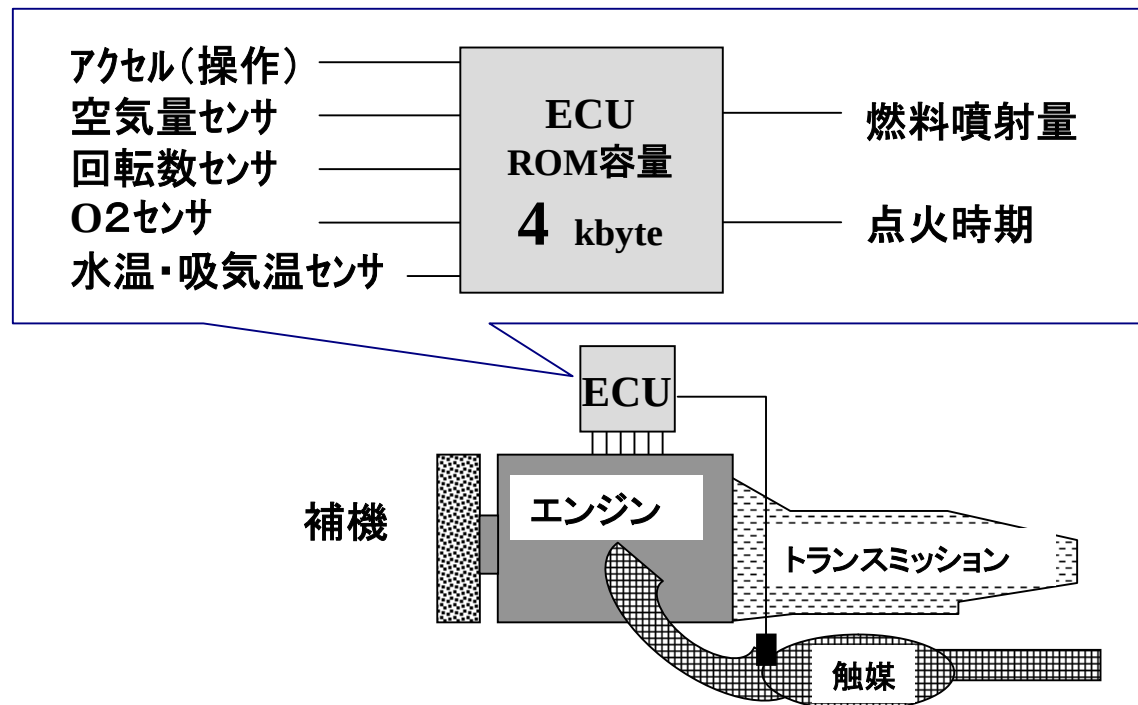
# 過去のエンジン制御開発/適合業務

## ＜EFI当初＞

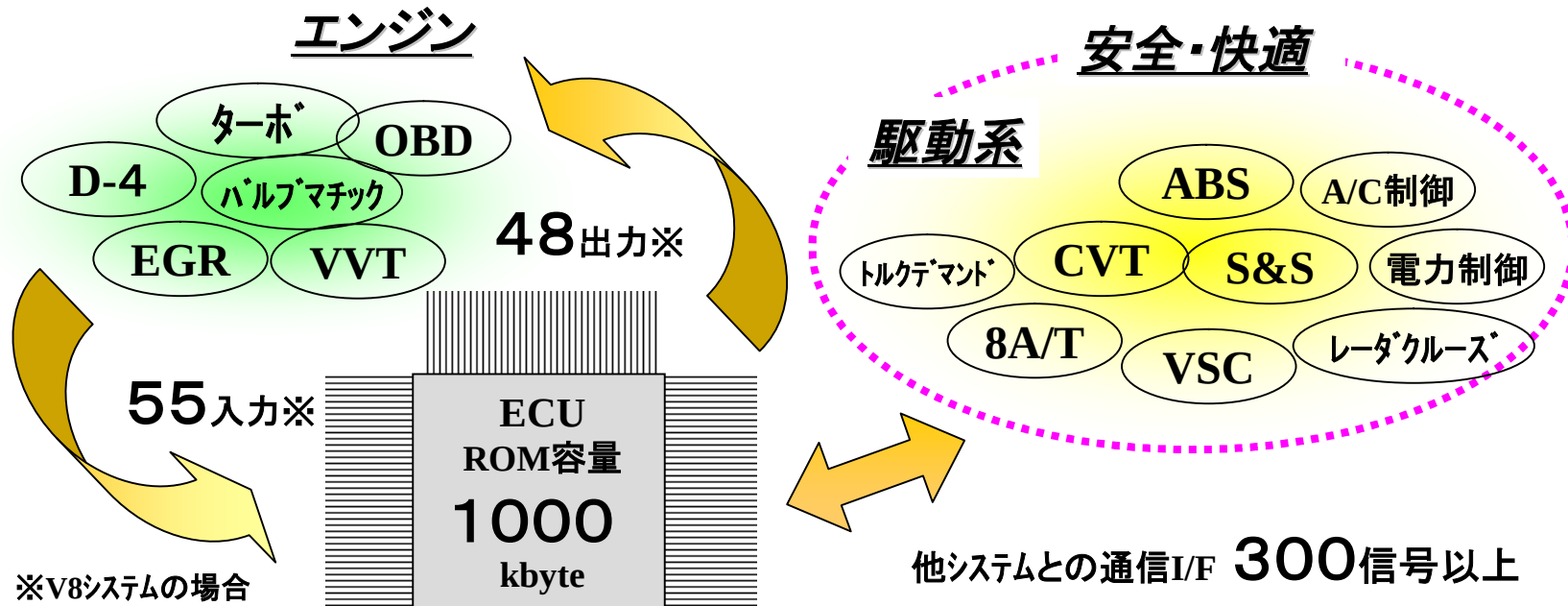
「システム設計」: 組合せる部品が少なく、またエンジンシステムで独立。  
「適合」: 部品の調整代のイメージ、「便利な最終合わせ込み工程」。

＜入力 5＞

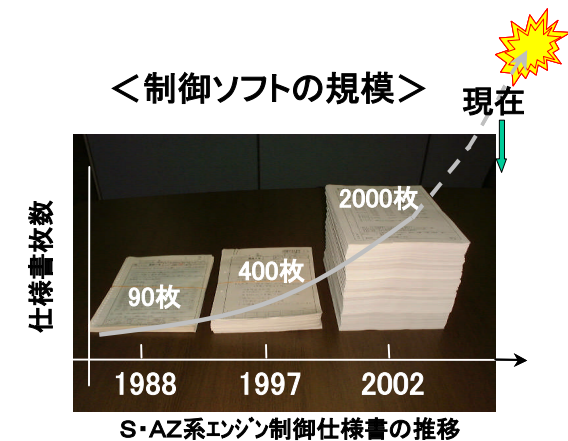
＜出力 2＞



# 巨大化した車両システムと制御開発

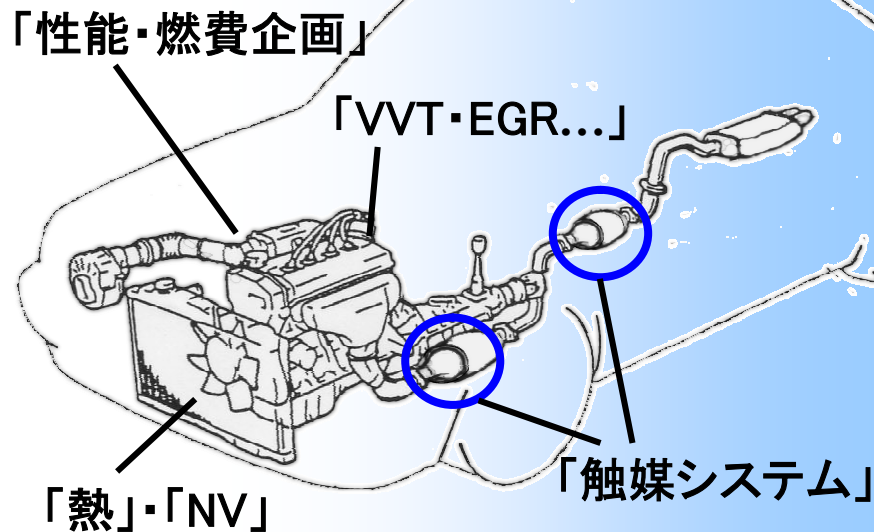


- ①エンジンの機能向上に加え、エンジン以外のシステムとも複雑に絡み合い、「システム設計」に高度なバランス取りが要求されるようになった。
- ②このための制御仕様も肥大化、「適合」項目と「確認」項目も大幅に増加。



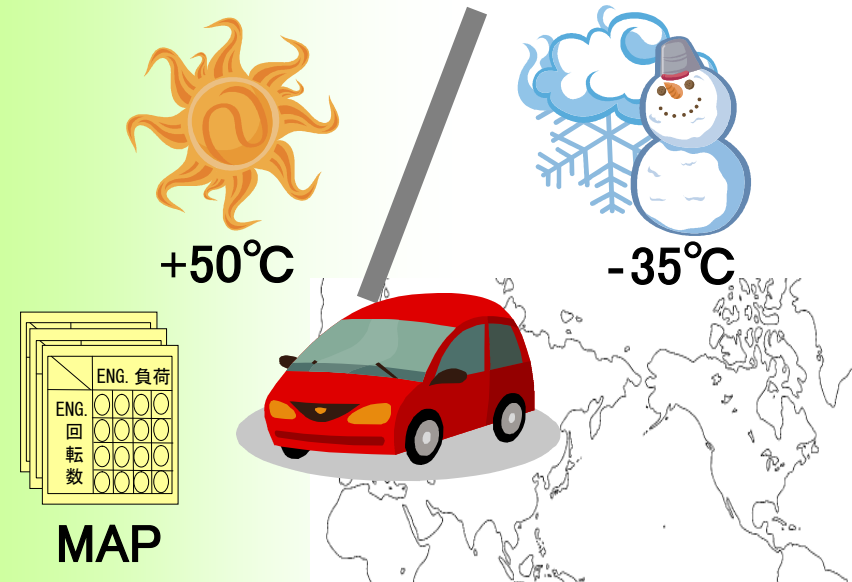
# 制御/適合業務とは

## システム設計



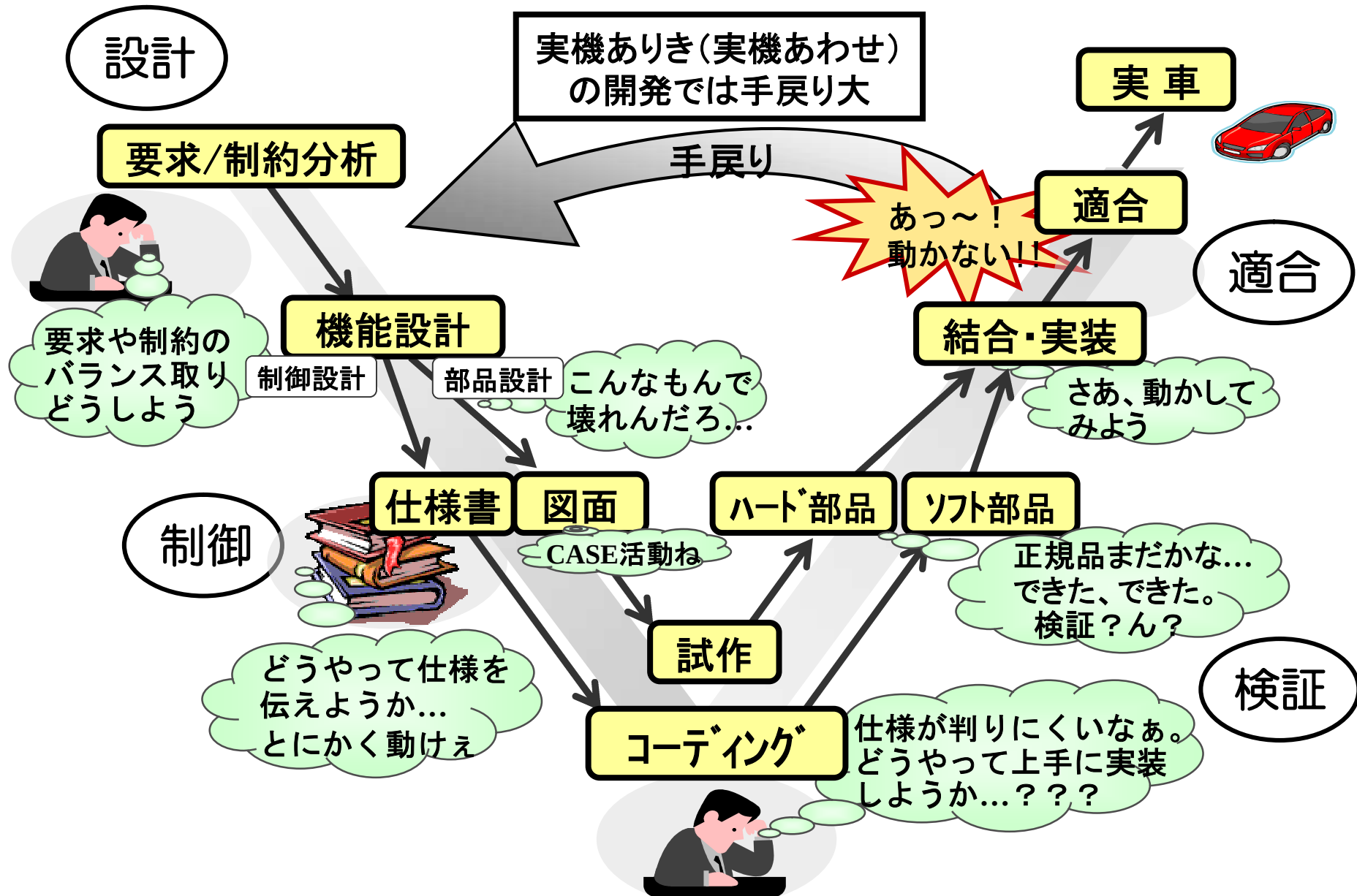
1. エンジンを構成する  
「部品＋制御」(システム)を  
最適に組上げる。  
(システム設計)

## 適合・評価

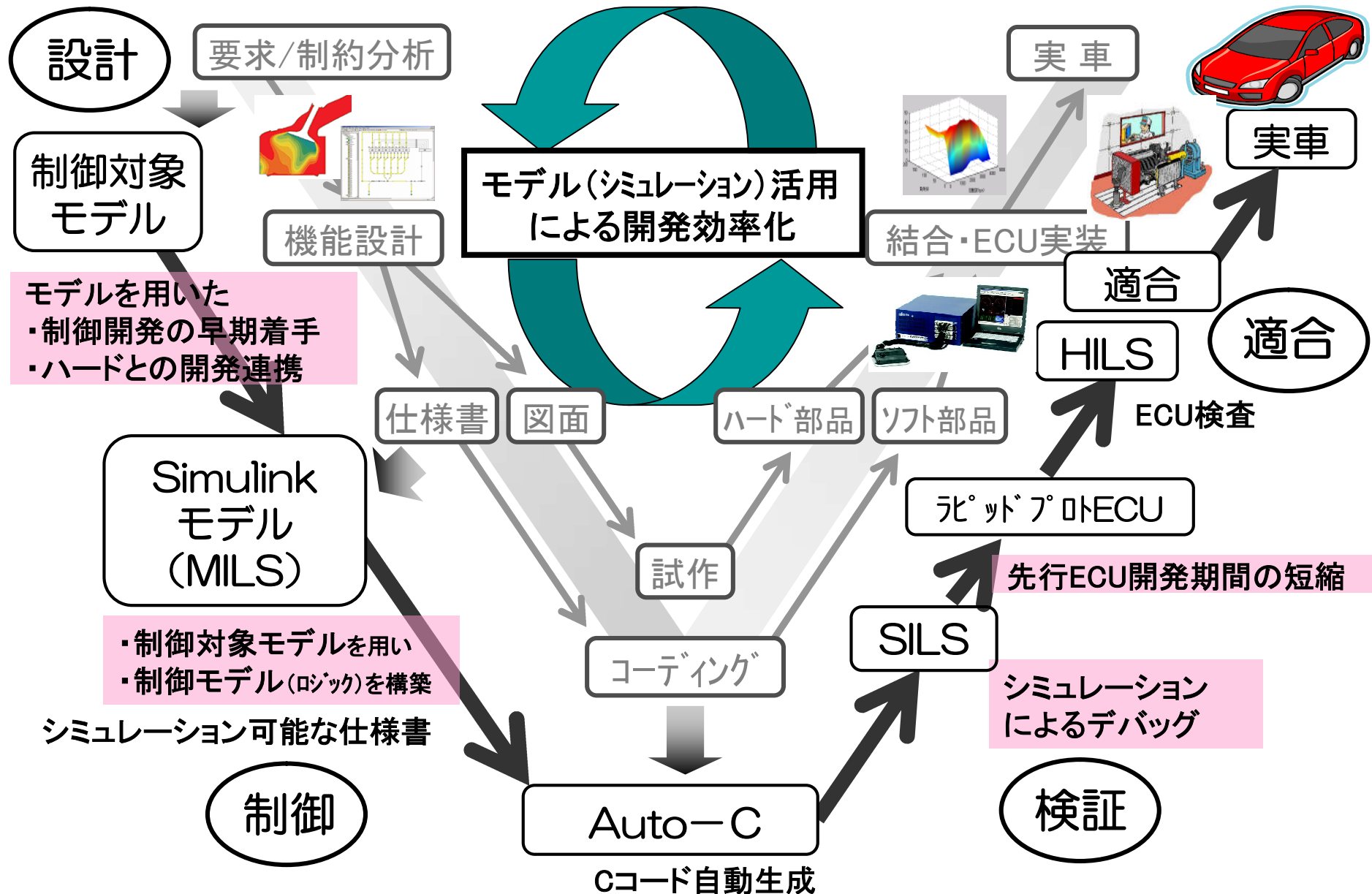


2. 組上げたエンジンシステムが  
最大限に商品力を発揮する様  
プログラムのパラメータを  
調整する。(適合)

# システム設計の実態



# システム設計の革新～ MBDによる制御開発 ～



# モデルベース開発(MBD)の取組みイメージ

設計

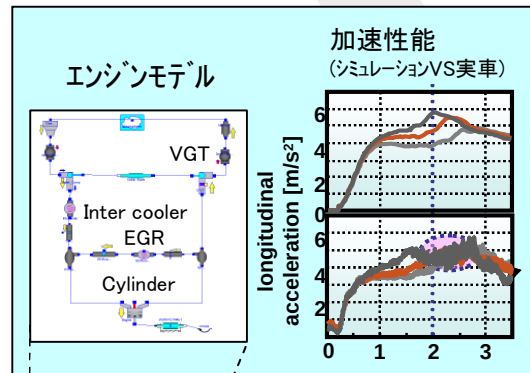
モデルを用いた  
・制御開発の早期着手  
・ハードとの開発連携

開発プロセスと  
ツール・DBの紐付け

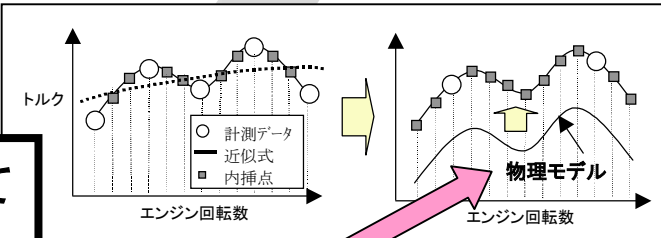
MBDフレームワーク

適合

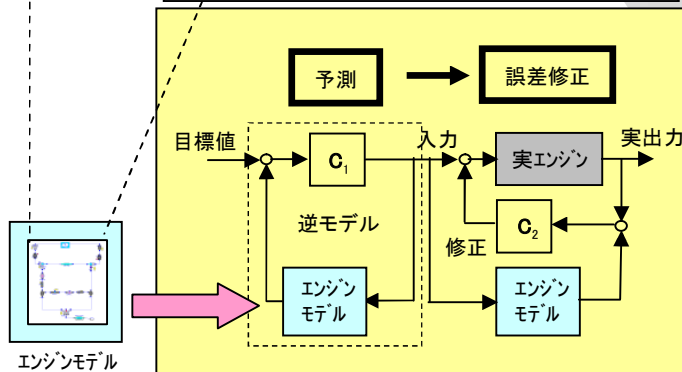
モデルベース適合



モデル(シミュレーション)を軸として  
エンジンの制御開発を行う  
⇒品質向上+開発効率化



モデルベース制御 (Simulink仕様書)



制御

制御対象モデルを用い  
制御モデル(ロジック)を構築

制御ロジック  
(Simulink仕様書)

シミュレーションによる  
制御開発・検証・デバッグ

Auto-C

R/Dtype

先行ECU開発期間の短縮

検証

HILS

SILS

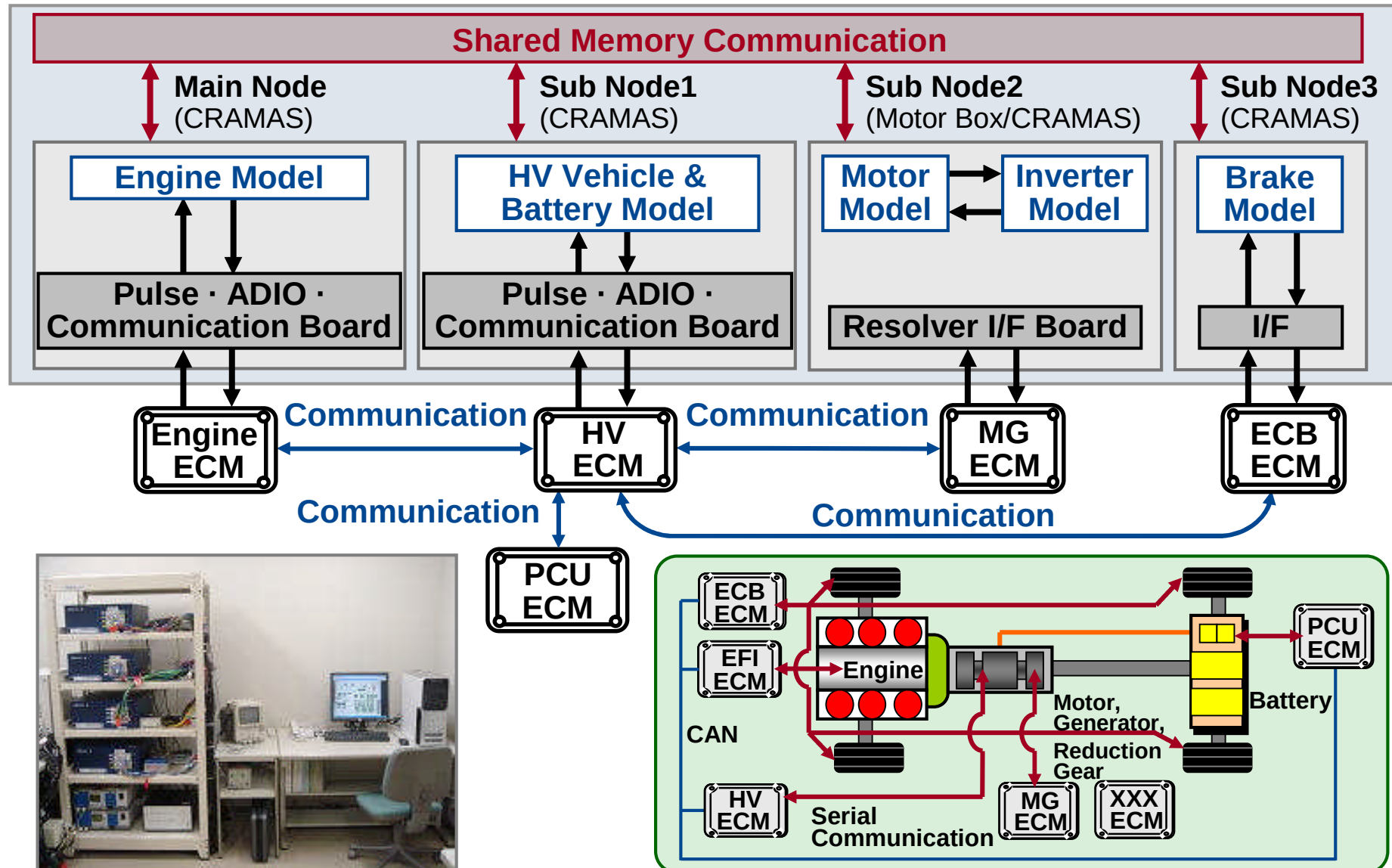
ECU検査

制御ロジック  
(Simulink仕様書)



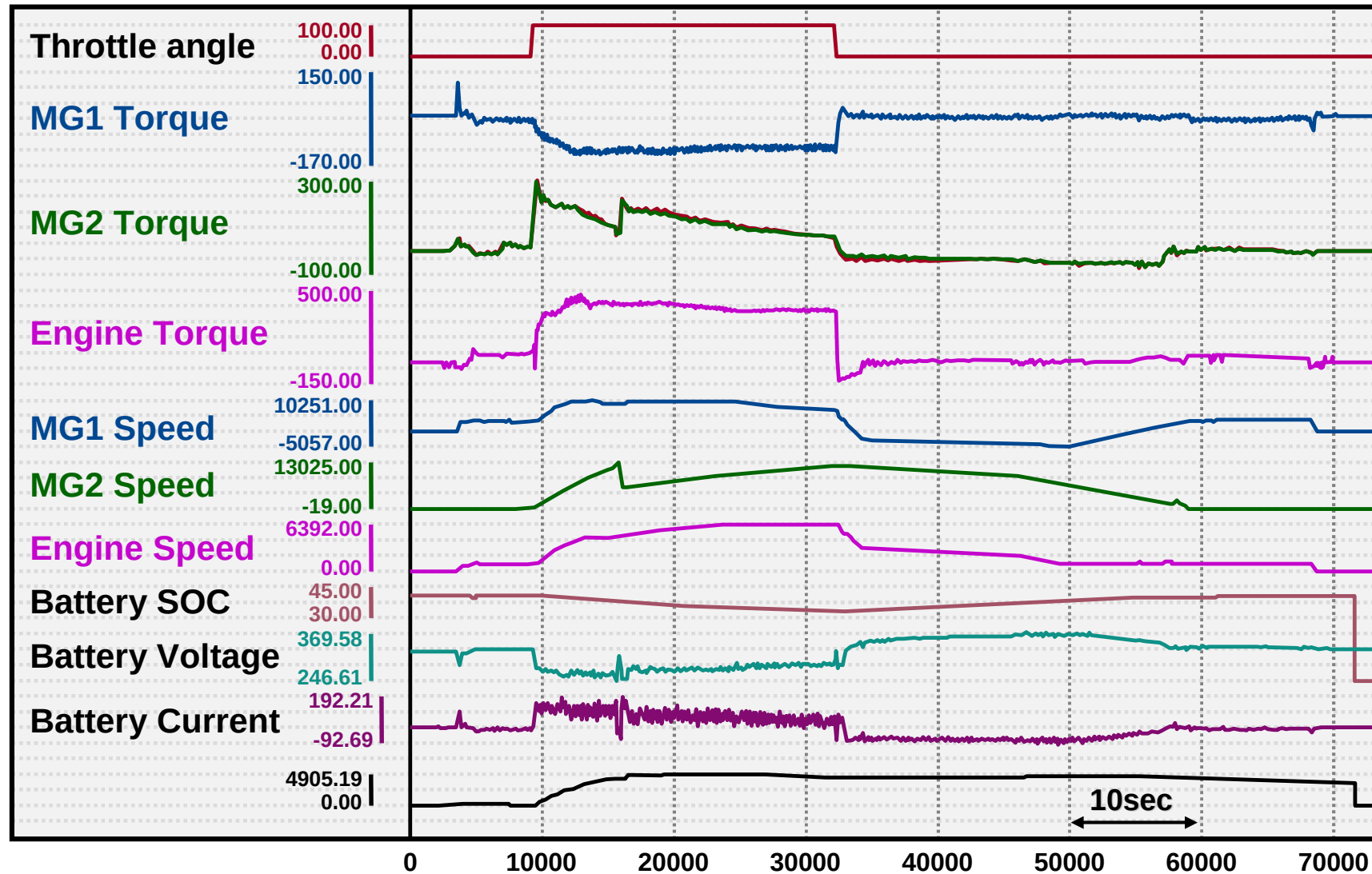
# MBDの取組み例

# HV-HIL System

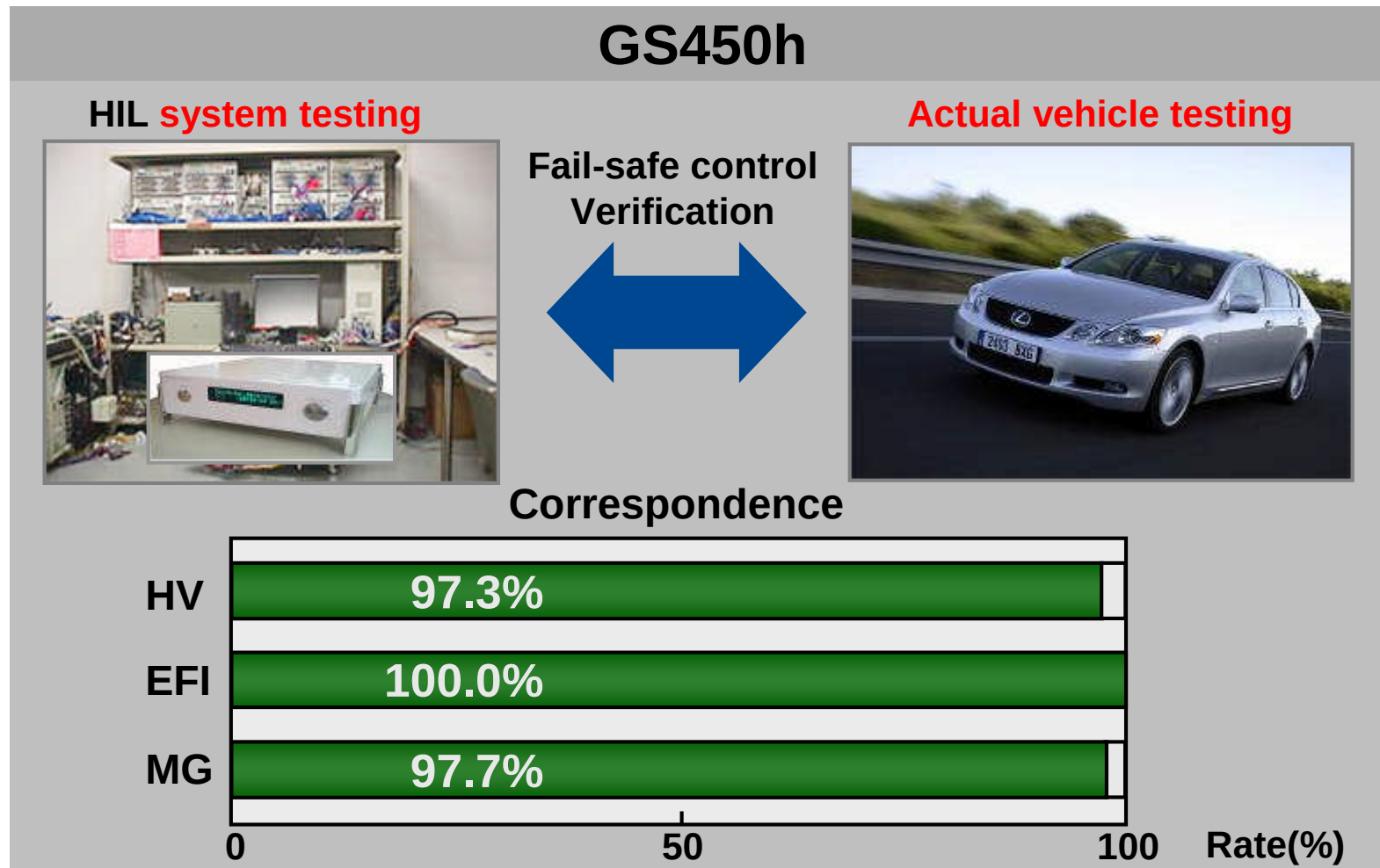


(the source) Aachen colloquium 2006

# HV-HIL Simulation Result Example



# HV-HILS Application Results

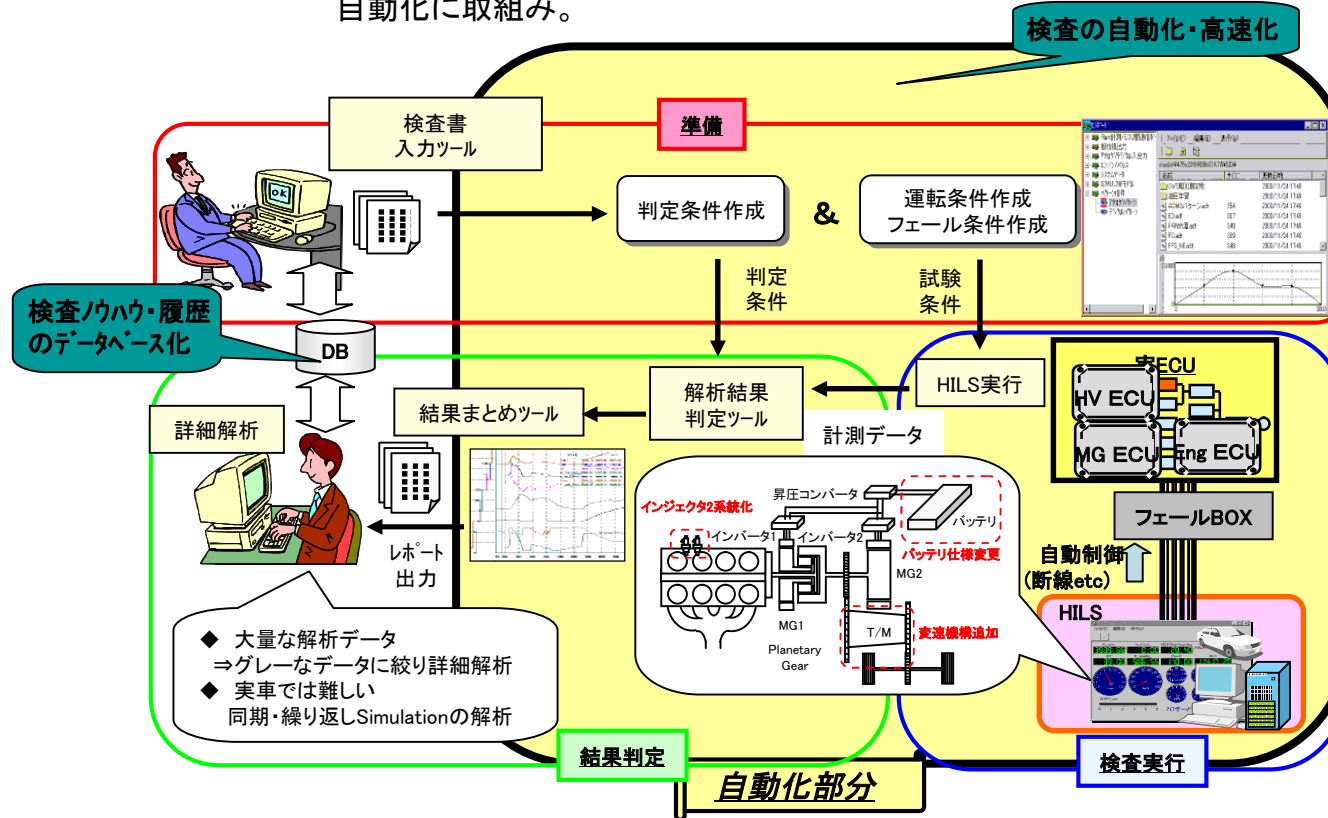


HIL system has been applied for hybrid fail-safe control verification.

- 97% agreement with actual vehicle test results.
- 30 times faster than conventional vehicle tests.

# HV-HILSの検査自動化システム構築

**構成** 制御用ECU 検査自動化への取り組みを実施  
HV車(EFI, MG, HV)のダイアグ・フェールセーフ検討評価の  
自動化に取組み。



## 結果(進捗状況)

- ・Fail-Box+検査管理ツールを利用した検査自動化を構築し、各車種に展開済み。
- ・検査ノウハウや検査履歴のデータベース化も可能になった。

## 結論

- ・検査の50倍高速化を実現⇒検査拡大or徹底した検査が可能に。

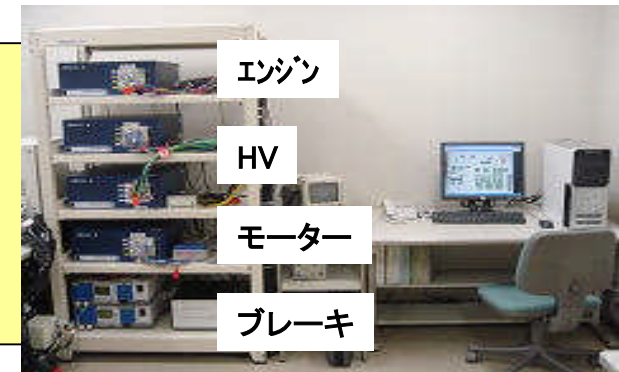
# HV-HILS運用での課題・問題点

## 経緯

- ・HV-HILSはシステムとして確立し、技術部門内に14台導入したが低稼働率
- ・ノウハウが各部署、各担当者に蓄積／共有化できない。

## 問題点

- ・ある部署でHILSを立ち上げた時の資産、経験が他部署で生かされていない。
- ・情報収集からHILS構築までが人海戦術。  
(情報は電話交渉、連メモの嵐)



熟練HILS構築者



仕様書入手

HILS構築



各担当が、今までの  
ノウハウで収集

横展すると...

図面が  
足りないよ！



この図面は  
いらない！

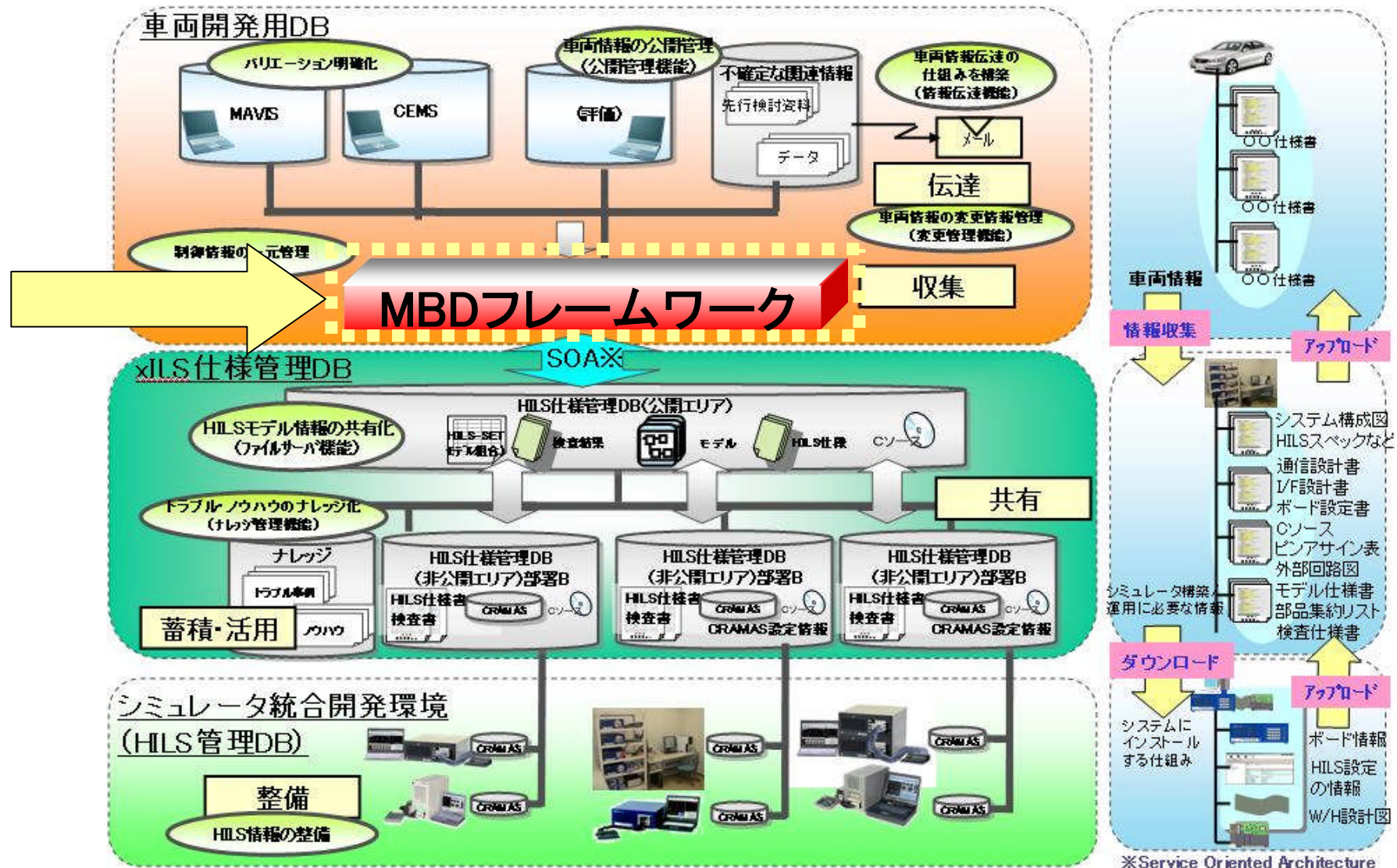


必要な情報が間違いなく集約できない



# MBDフレームワーク開発

- ・制御開発環境の統一
- ・制御開発者の情報共有基盤

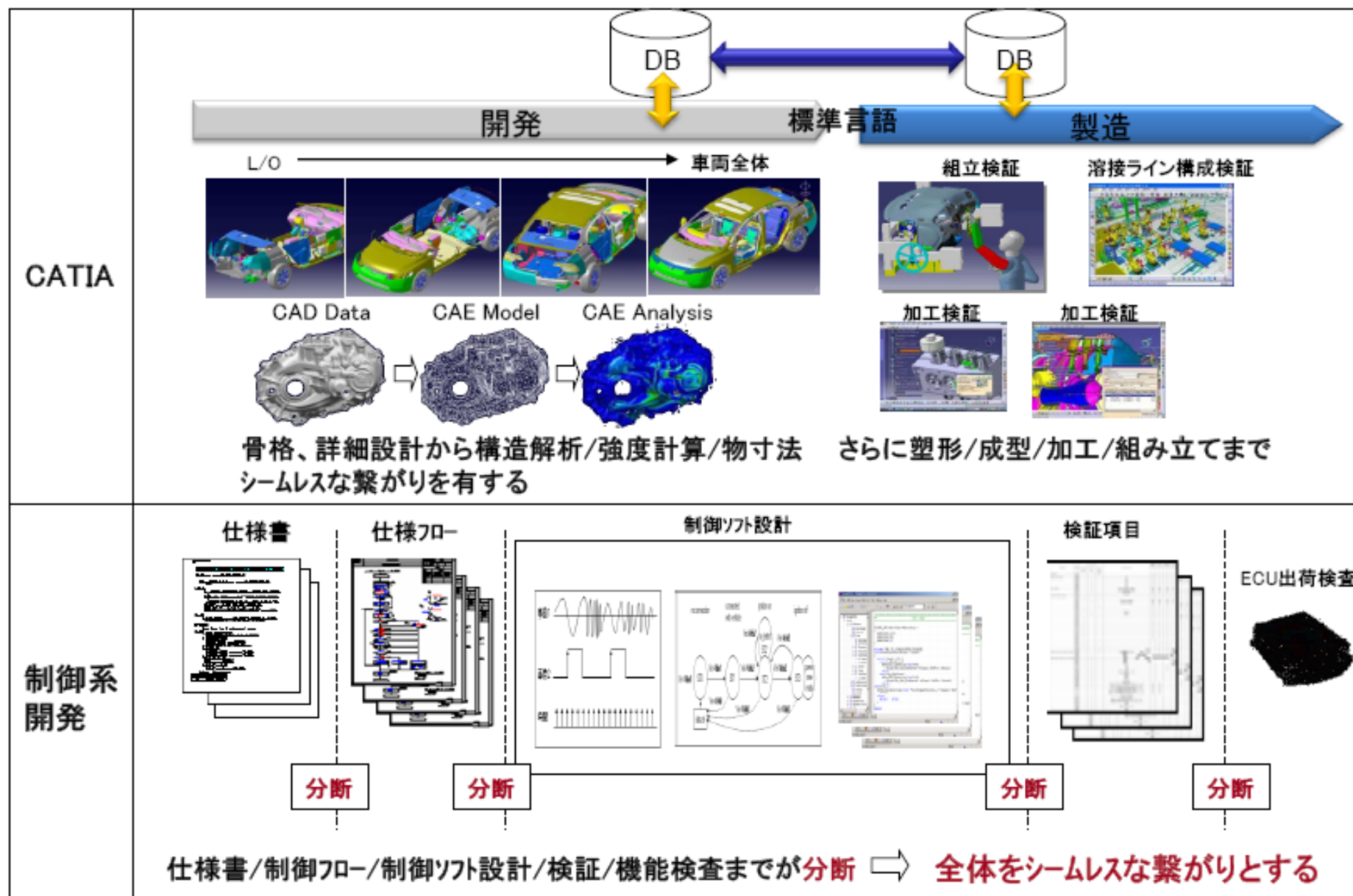


# MBDF(MBDフレームワーク)のご説明



# 背景① 分断された環境

25



分断されら環境を設計ツールと同等の制御系開発ツールに進化させたい

# MBDFの実施例

MBDF：技術者の情報基盤となるDB

⇒ 技術者は作業に必要な全ての情報をMBDFから入手

xxxF 11月 スケジュール  
1. 冷間試験：11/01 ~ 11/10  
2. E80試験：11/14 ~ 18  
3. KCS試験：11/21 ~ 24  
4. DR会議：11/25

1. スケジュール確認

2. やるべきタスク確認

タスクリスト  
1. 低温連続試験：11/20  
2. Thw95付着量確認：11/30  
3. Aby学習値確認：12/10  
4. Pセンサー校正：12/15

• 最終リリースデータ承認  
• チーム議論

成果物  
1. xxxF技術速報：石崎  
2. 技術速報添付データ：石崎  
3. xxxF新FWM適合：瀬尾  
4. E100報告まとめ：渡邊

6. 適合データリリース

MBDフレームワーク  
MBDF

3. SIL/HILSで実機前評価

• Cソース入手  
• SWビルド

xxxF Cソースリスト  
• eafqinj\_c\_mat.c  
• easyidl.c  
• eegrmc\_c\_mat.c  
• entcal\_c\_mat.c

4. 評価・試験

5. エンジンベンチで自動適合

ツール  
1. 統計処理.xls  
2. データ処理.m  
3. Excel2Matlab.xls

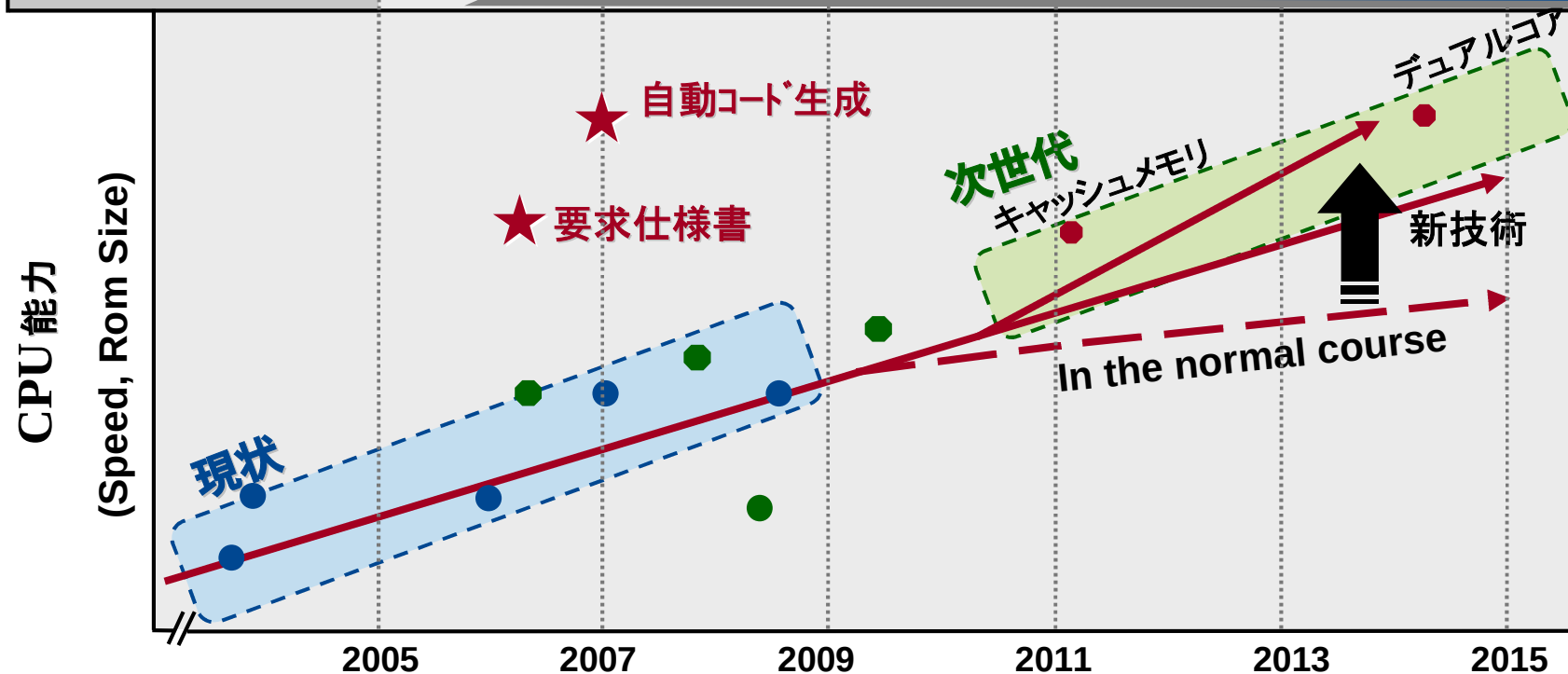
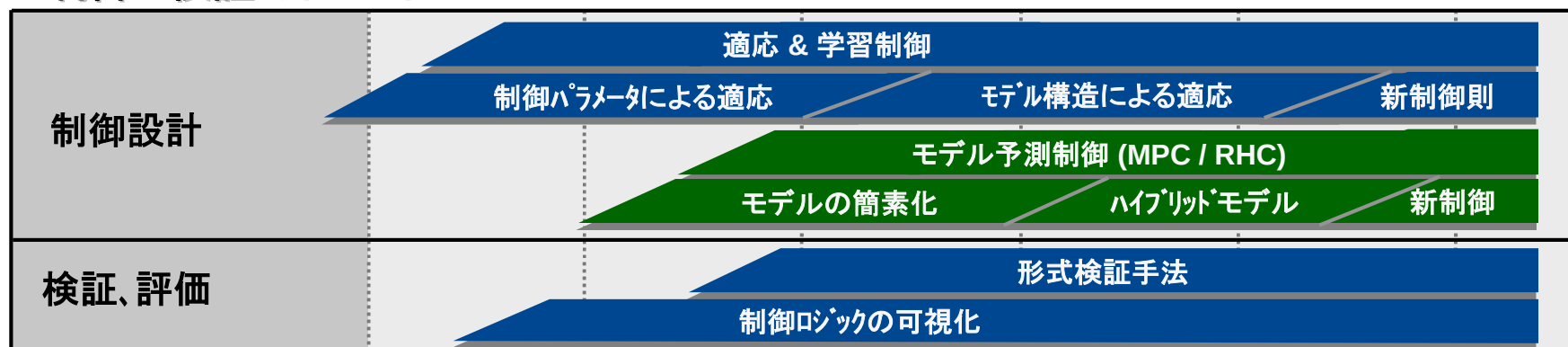
学習値確認タスク  
• 確認手順書  
1. thw20.xls  
2. thw80.xls  
3. 斜流角比較.xls  
• テスト手順書入手  
• 実験データ登録



# エンジン制御の将来予測

## 今後のエンジン開発革新 - 環境に適応する・自ら学習する制御 -

### - 制御 / 検証のトレンド -



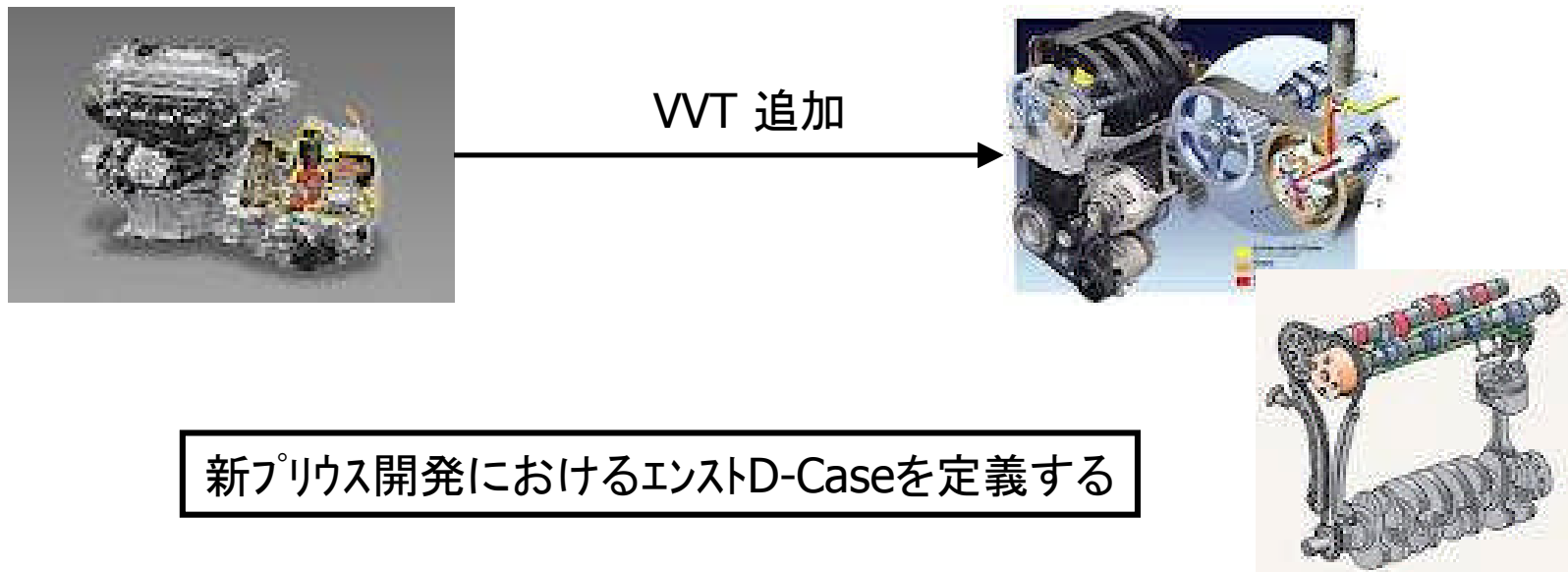
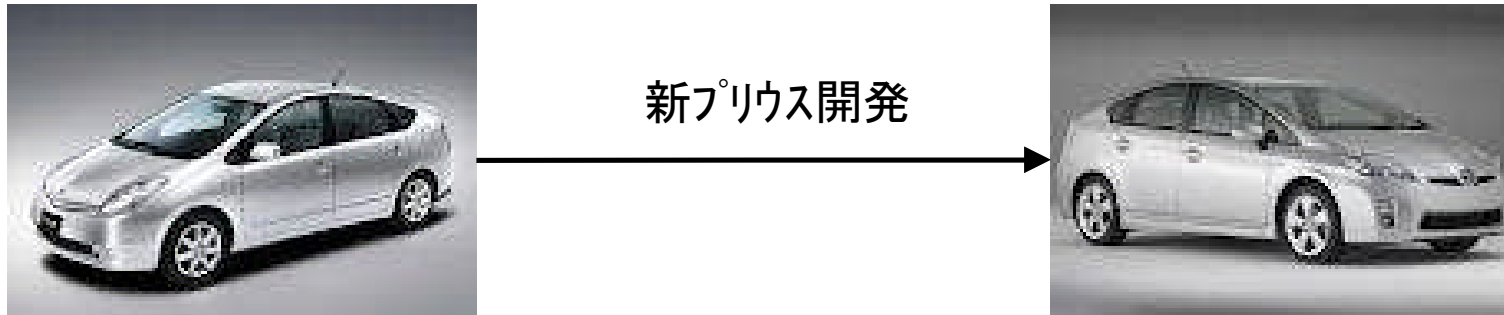
# 自動車制御におけるD-Case適用

## ～ エンジンストール問題への適用 ～

- ISO26262の弱点を克服できる安全要求開発が合理的にできないか
- 製品のライフサイクル及び開発の進化と共に持続的に成長する管理ができないか

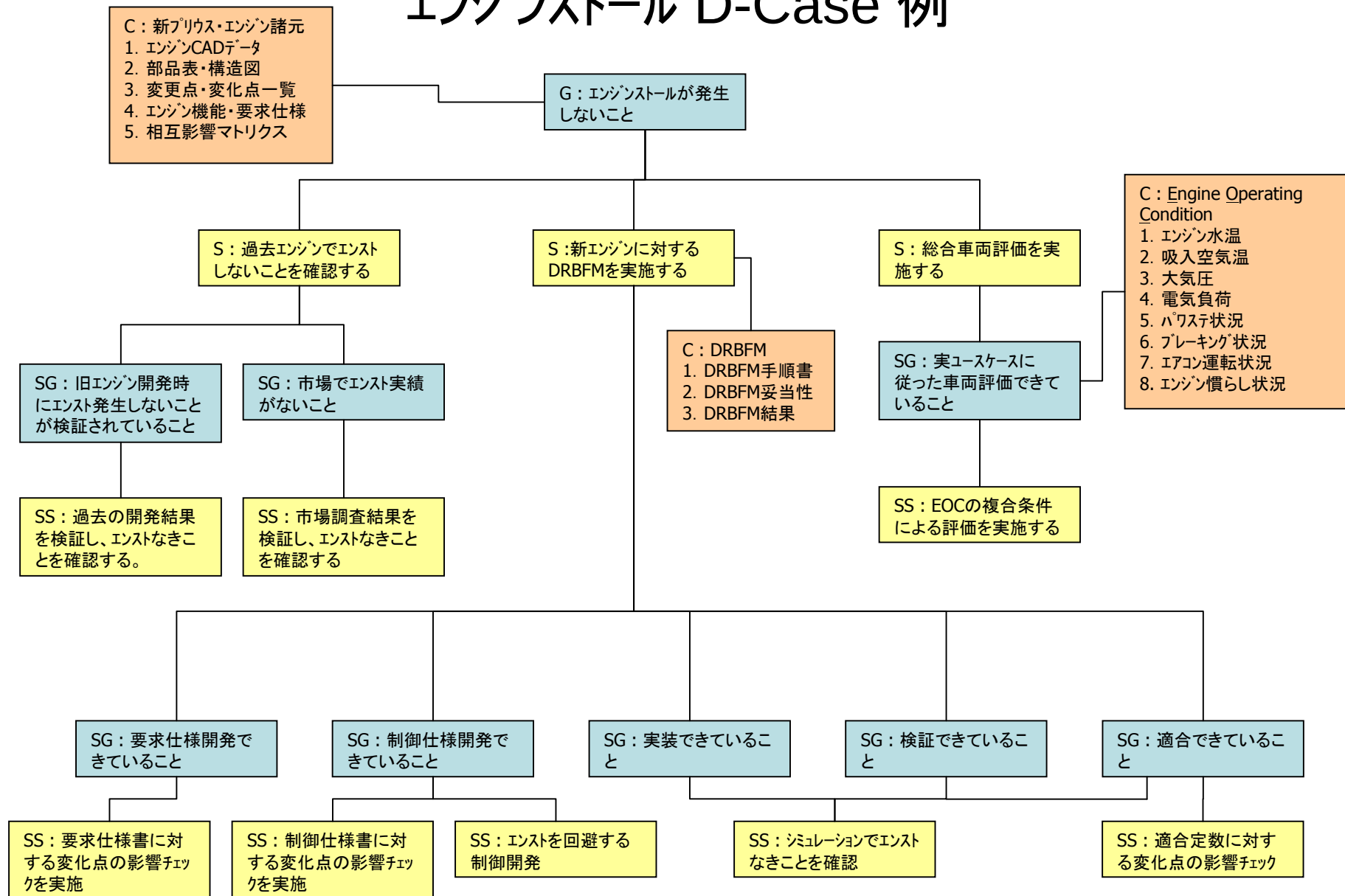
# インスタ D-Case 例

- 旧プリウスをベースとして新プリウスを開発する
- 旧プリウスエンジン ⇒ 旧プリウスエンジン + VVT



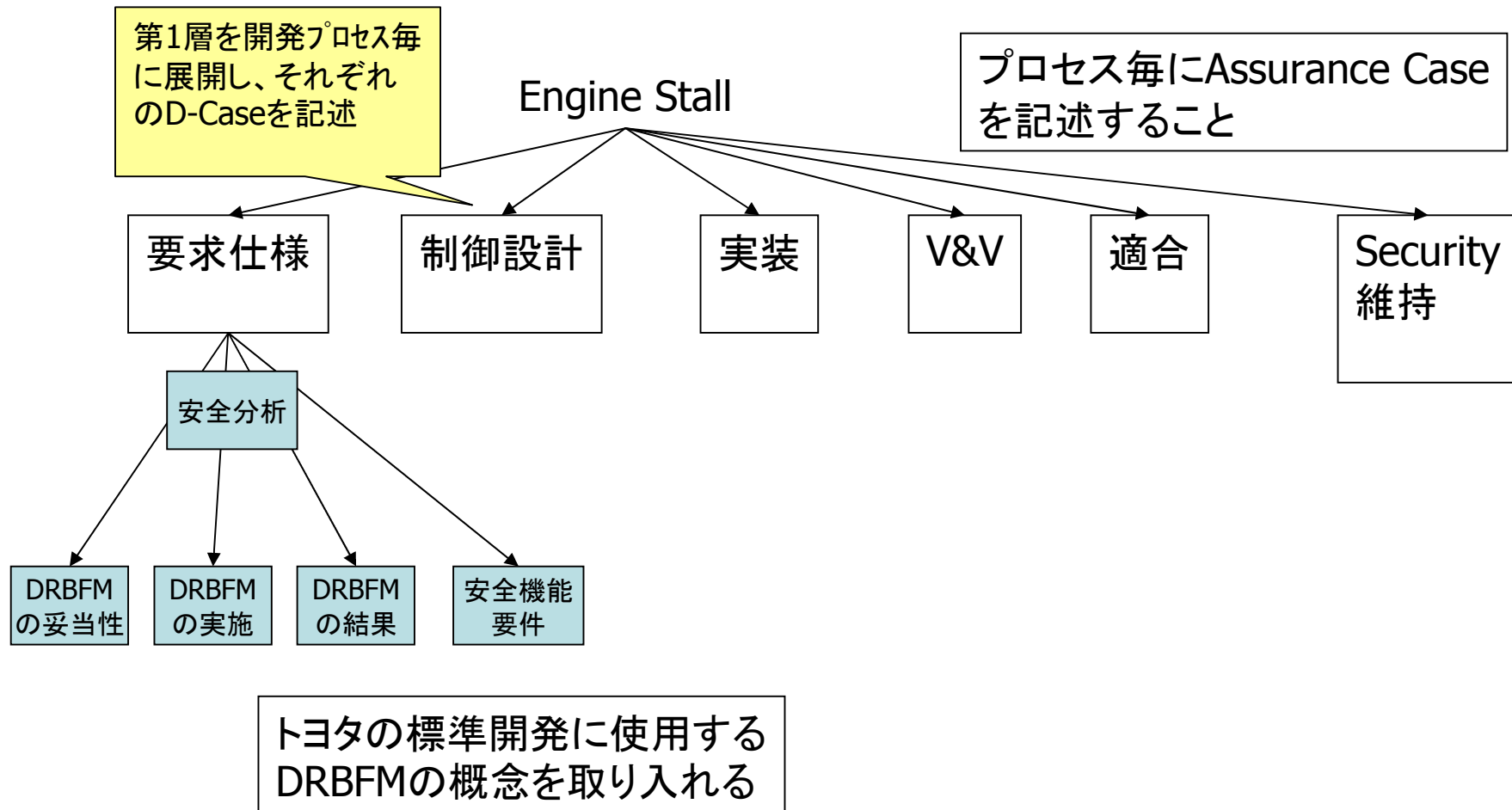
新プリウス開発におけるインスタD-Caseを定義する

# エンジンストール D-Case 例

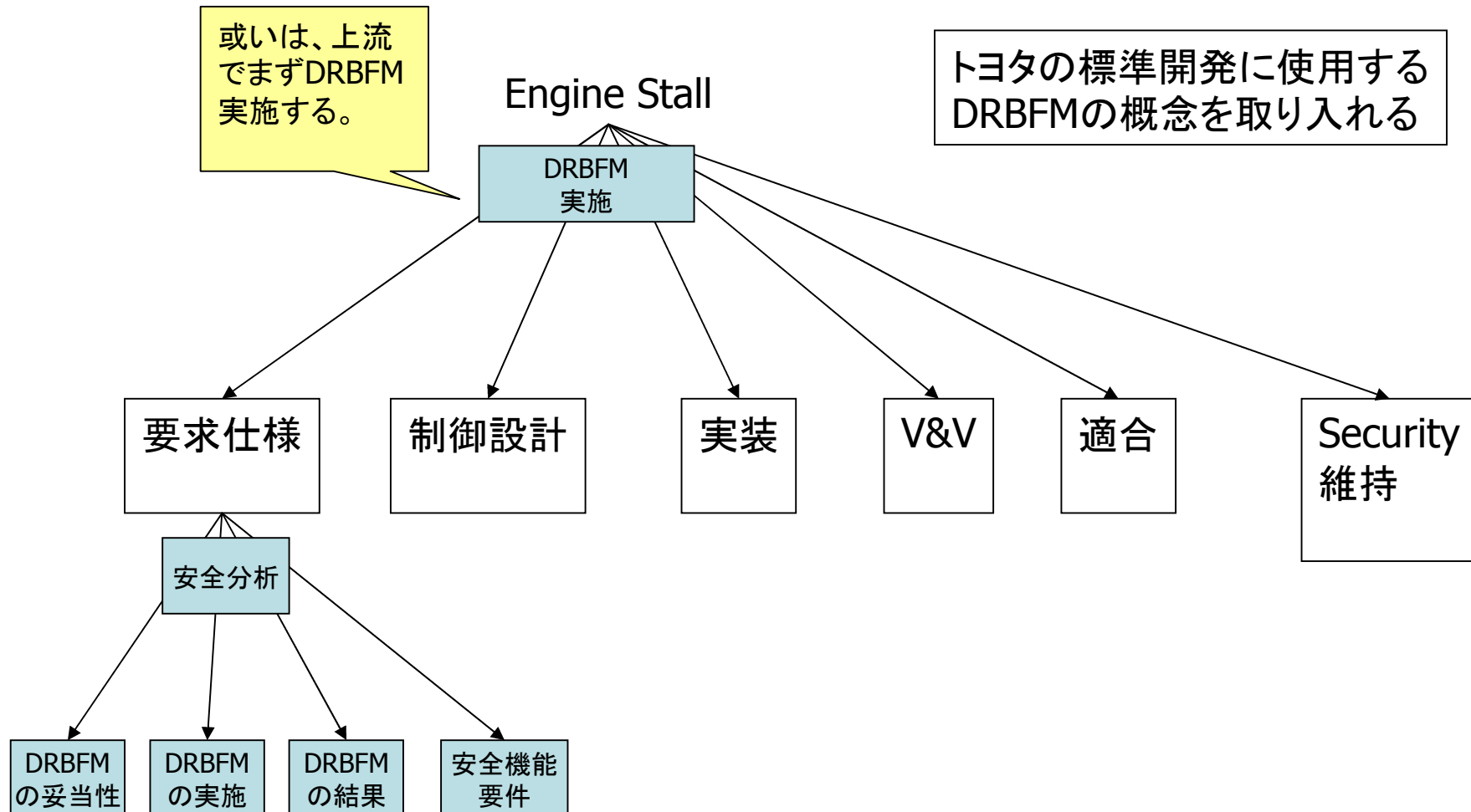




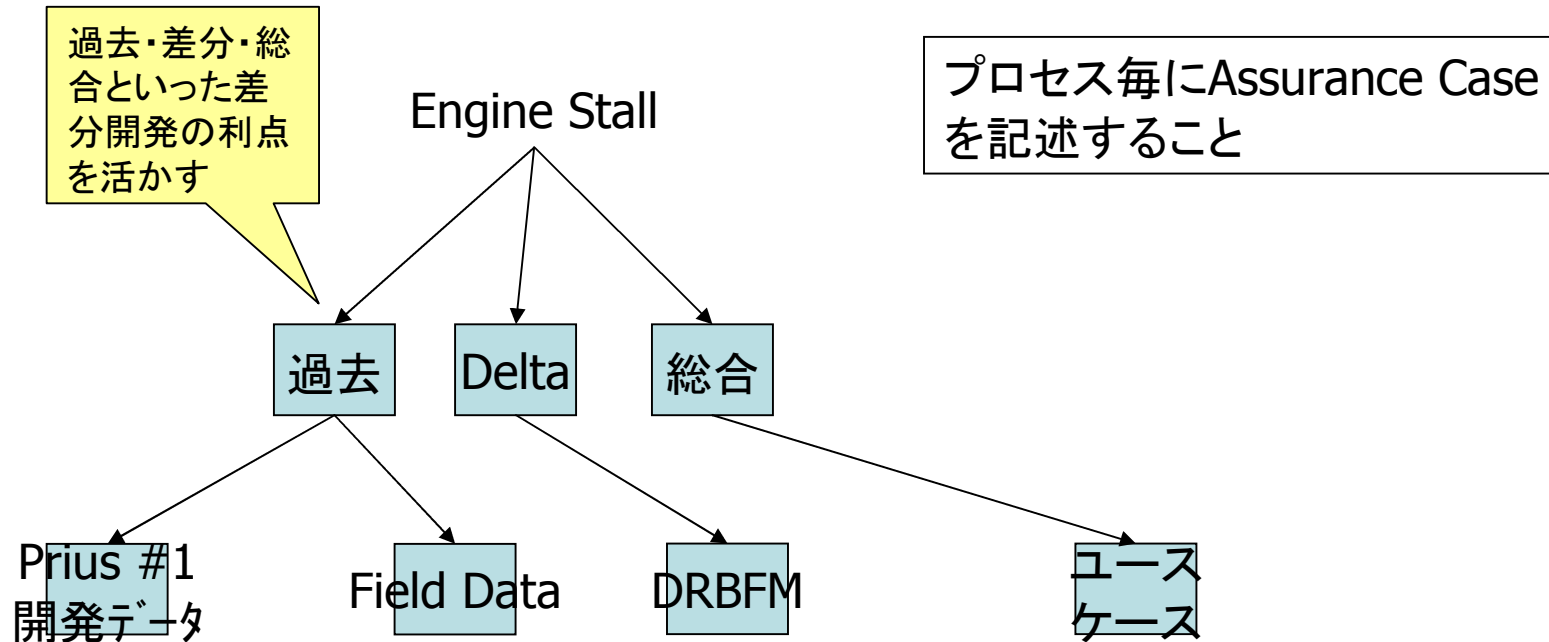
# D-Case記述方法 案#1



# D-Case記述方法 案#2



# D-Case記述方法 案#3



1. 自動車制御開発においてD-Caseを記述する場合は、差分開発の特長を利用して記述するのが良い。
2. 第1層を過去・差分・総合の3レッグに分けてそれぞれのD-Caseを検討すると考えやすい。

# 自分の使命とは？



- 自動車を凶器にさせない
- 安全な自動車制御の飽くなき探求

# Thank you

