自動車エンジン制御開発における D-Case適用事例

～エンジンストール問題における

D-Case定義及び開発管理 ～

トヨタ自動車 ｴﾝｼﾞﾝ技術開発部
理事　大畠　明
主幹　石崎　直哉
’12/11/16

本日の内容

■背景

■ｴﾝｼﾞﾝ制御開発へのD-Caseの適用

■D-Caseの課題

■OMGへの国際標準化活動

本日の内容

■背景

■ｴﾝｼﾞﾝ制御開発へのD-Caseの適用

■D-Caseの課題

■OMGへの国際標準化活動

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

機能安全規格ISO26262とは

◇機能安全

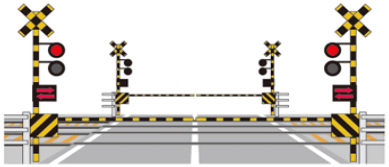
【定義】システムのリスクを**許容できる程度以下に対策**して安全を確保する

⇩

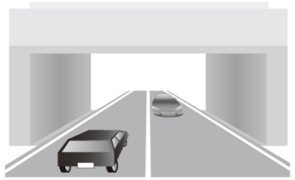
【対義語】本質安全 ⇒対策によってリスクを**なくして**安全を確保する

【例】鉄道の線路横断に対する対策

①鉄道と道路が平面交差
⇒**危険**な状態
（電車との衝突）



②警報機や遮断機を設定
⇒危険な状態（電車との衝突）
が許容できる程度以下
⇒**機能安全**の状態



③立体交差を設定
⇒危険な状態（電車との衝突）
を回避
⇒**本質安全**の状態

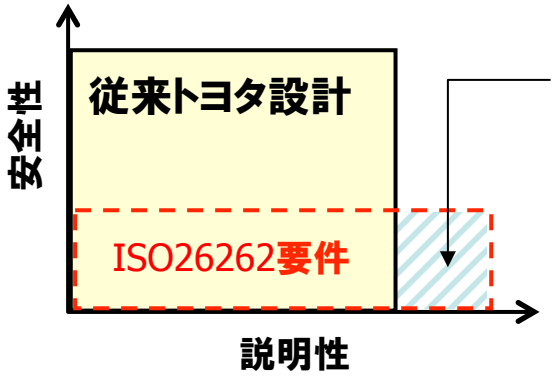
◇ISO26262**規格**

◆**2011年11月に規格制定**

◆対象システム --- 安全に関連する**電気/電子システム（※純粋なメカは対象外）**

◇ISO26262**と従来トヨタ安全設計/品質との関係**

ISO26262はあくまで**ミニマム/必要最低限の安全設計要件**しか規定していない.
例: エンストはISO26262の対象外
⇒ISO26262とは関係なくエンストしないよう**従来トヨタ品質を満たすように作りこむ必要あり.**



第三者への安全性の説明性のために設計エビデンスを残す

ISO26262をﾍﾞｰｽに、ﾄﾖﾀ安全基準を全て証明することが必要。

自動車制御関連の安全に関する課題

◆ ISO26262規格で説明できる安全ﾚﾍﾞﾙとﾄﾖﾀとして証明しなければならない安全ﾚﾍﾞﾙに相違がある。

◆ “想定外“の使われ方も想定外では済まされない。

◆ 近年、情報ｼｽﾃﾑ同士が直接・間接に接続され巨大な情報ｼｽﾃﾑ群を形成し、生活の基本ｲﾝﾌﾗとなっている。自動車と社会ｲﾝﾌﾗ及びそれらの連携による社会ｼｽﾃﾑの安全性と信頼性を保証しなければならない。

◆ 変化し続ける社会ｲﾝﾌﾗ、年々厳しくなり続ける排気規制・燃費要求へ対応し続けなければならない。

ISO26262をﾍﾞｰｽに、変化し続ける社会ｲﾝﾌﾗ・規制・機能要求に対応可能な安全性議論の方法論が必要である。 ⇒ D-Caseの必要性

本日の内容

■背景

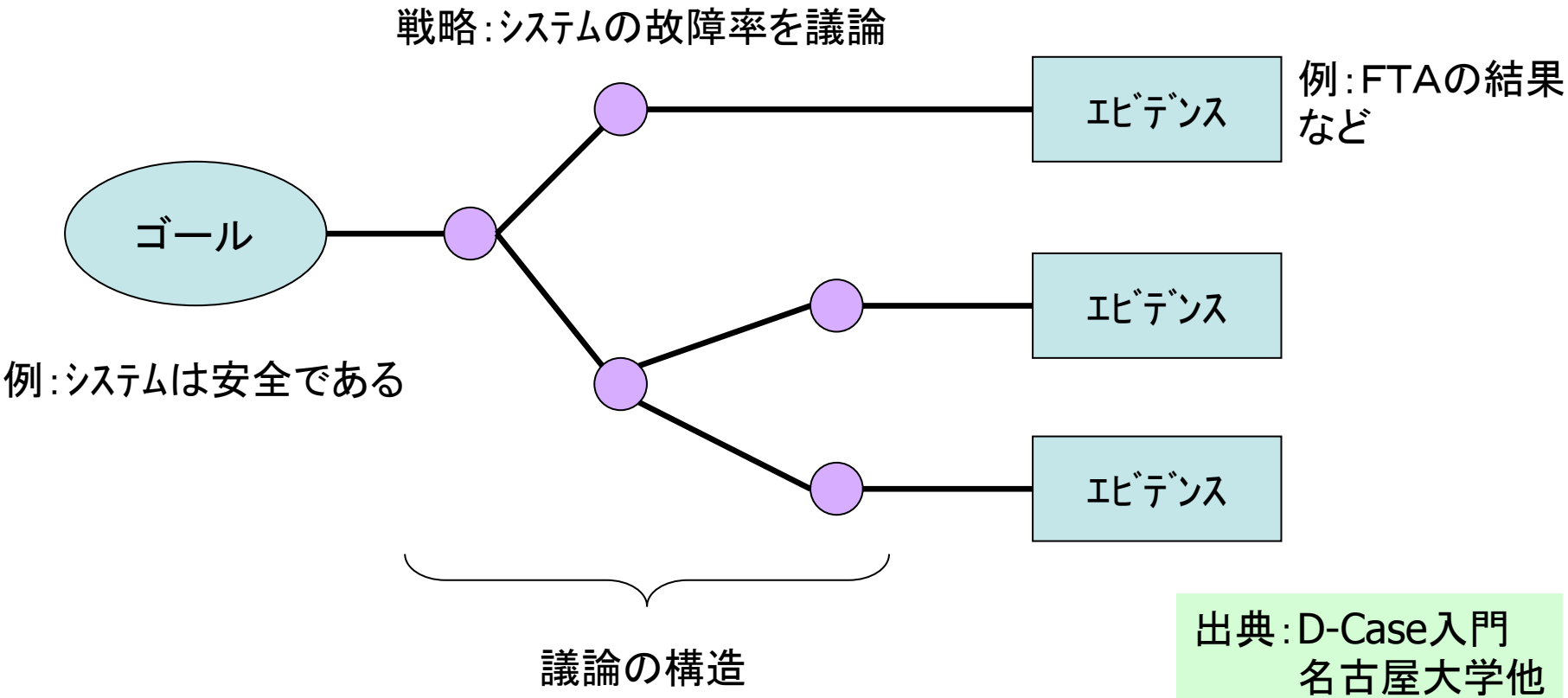
■ｴﾝｼﾞﾝ制御開発へのD-Caseの適用

■D-Caseの課題

■OMGへの国際標準化活動

D-Caseとは

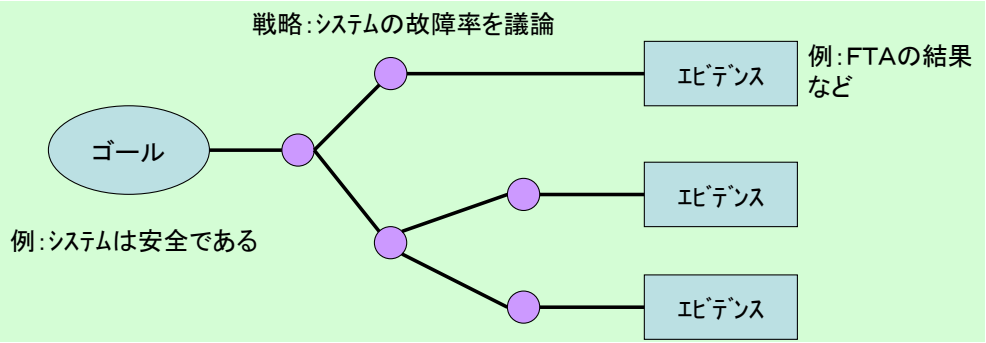
- Assurance Caseの拡張
  - システムのDependabilityを、エビデンスを元に議論するための方法・ツール



出典：D-Case入門
名古屋大学他

D-Caseのメリット

- ❖ 問題全体のスコープの明確化
- ❖ 議論に用いる資料の明示化



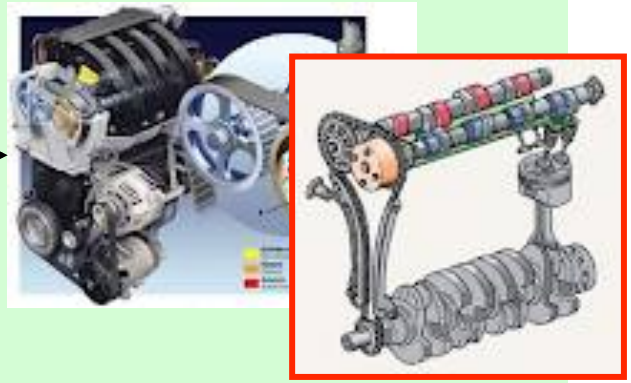
- ❖ 個々のFTA/FMEA等のリスク分析結果の統合
- ❖ 既存の安全や技術規格との適合結果の統合
- ❖ 個々のゴールに対する問題設定と合意条件の議論の明示化
- ❖ 想定する想定外の明示化

自動車制御開発へのD-Case 適用

➢想定：新ﾌﾟﾘｳｽ開発におけるｴﾝｽﾄD-Caseを定義する
- 旧ﾌﾟﾘｳｽをﾍﾞｰｽとして新ﾌﾟﾘｳｽを開発する
- 旧ﾌﾟﾘｳｽｴﾝｼﾞﾝ ⇒ 旧ﾌﾟﾘｳｽｴﾝｼﾞﾝ + VVT

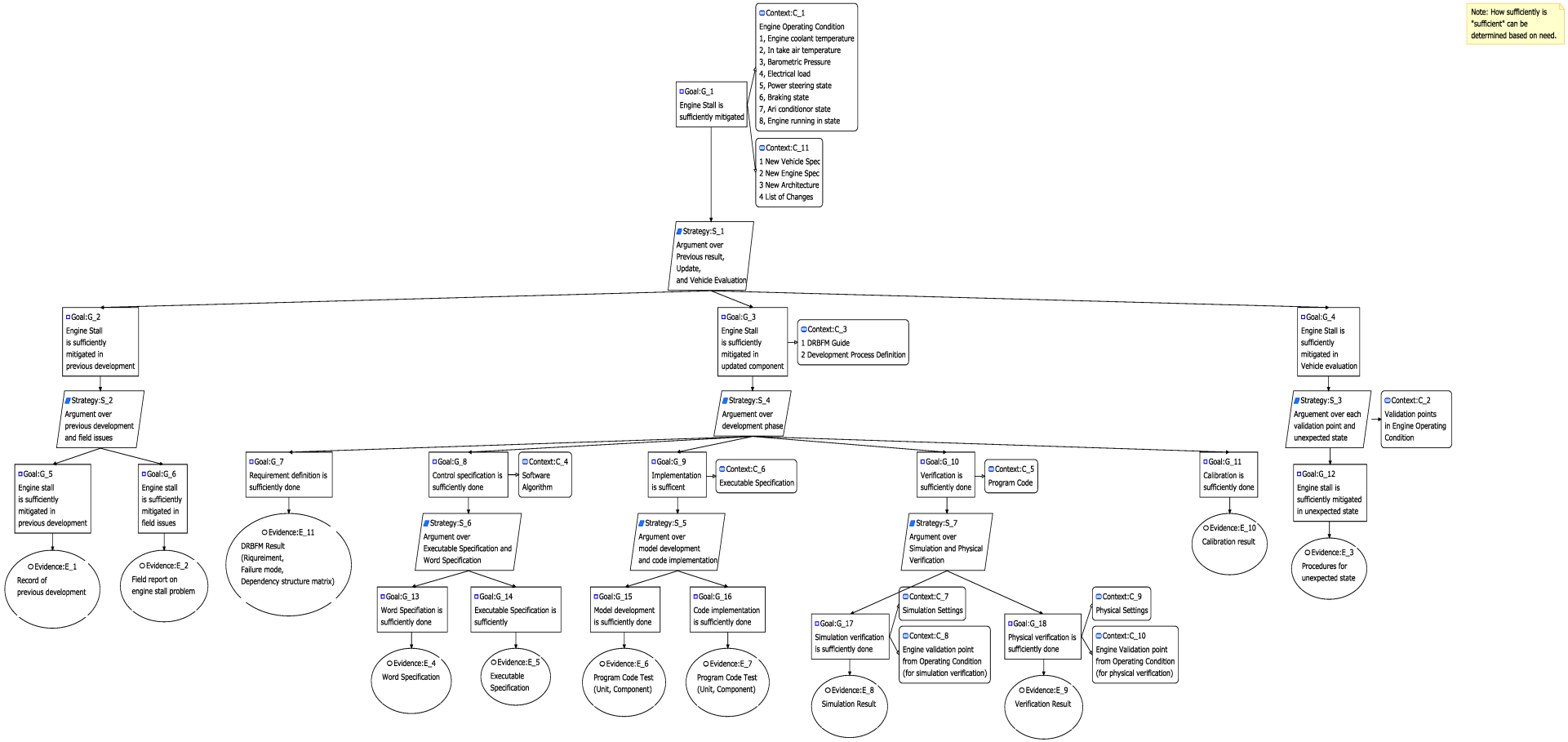
新ﾌﾟﾘｳｽ開発

VVT 機能追加



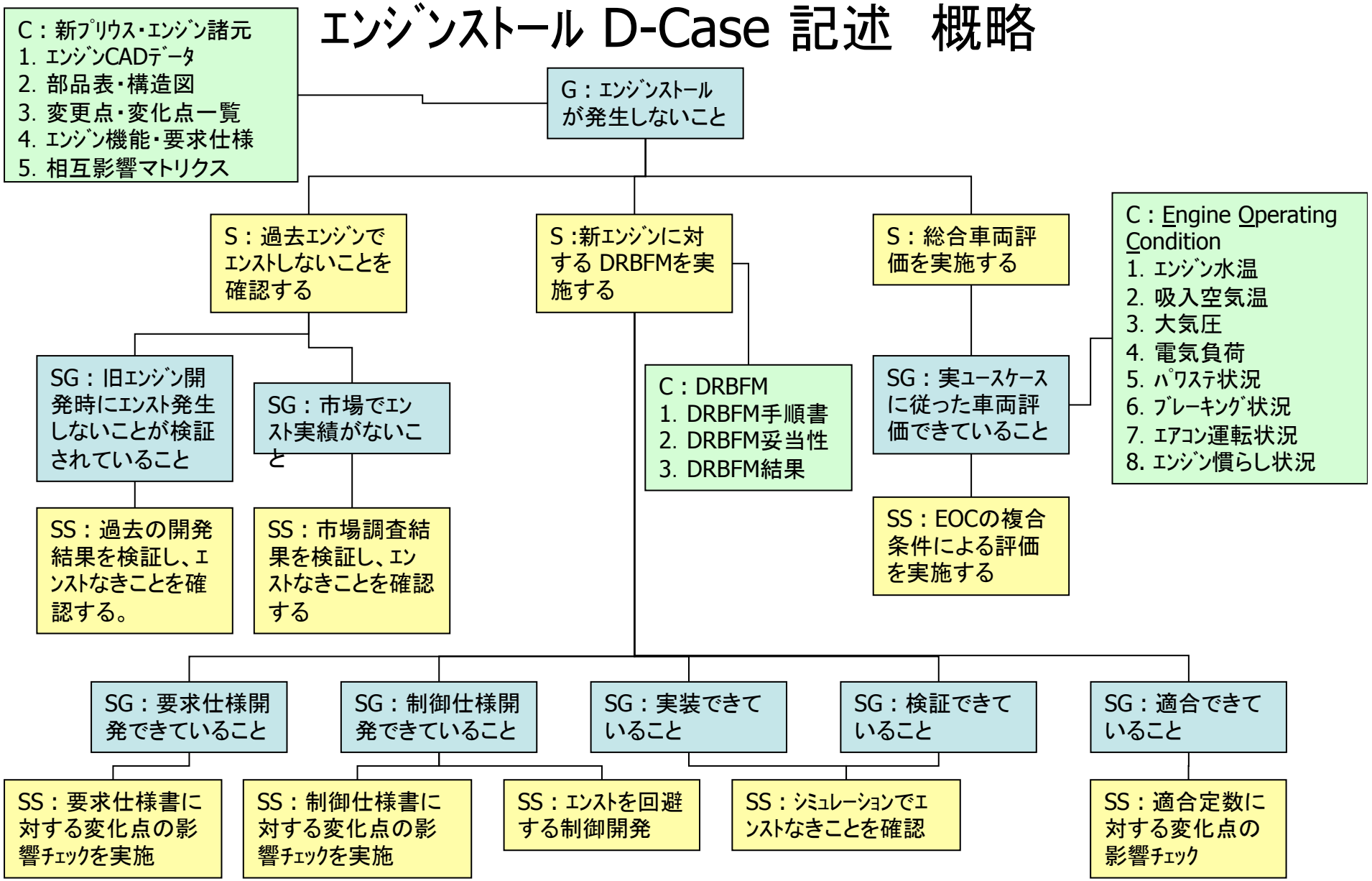
➢トヨタにおけるｴﾝｽﾄ評価・開発のﾌﾟﾛｾｽをD-Caseを適用

エンスト D-Case 例



➢トヨタにおけるエンスト評価・開発のプロセスをD-Caseに実装

エンジンストール D-Case 記述　概略



➢トヨタにおけるエンスト評価・開発のプロセスを概ね実装可能

本日の内容

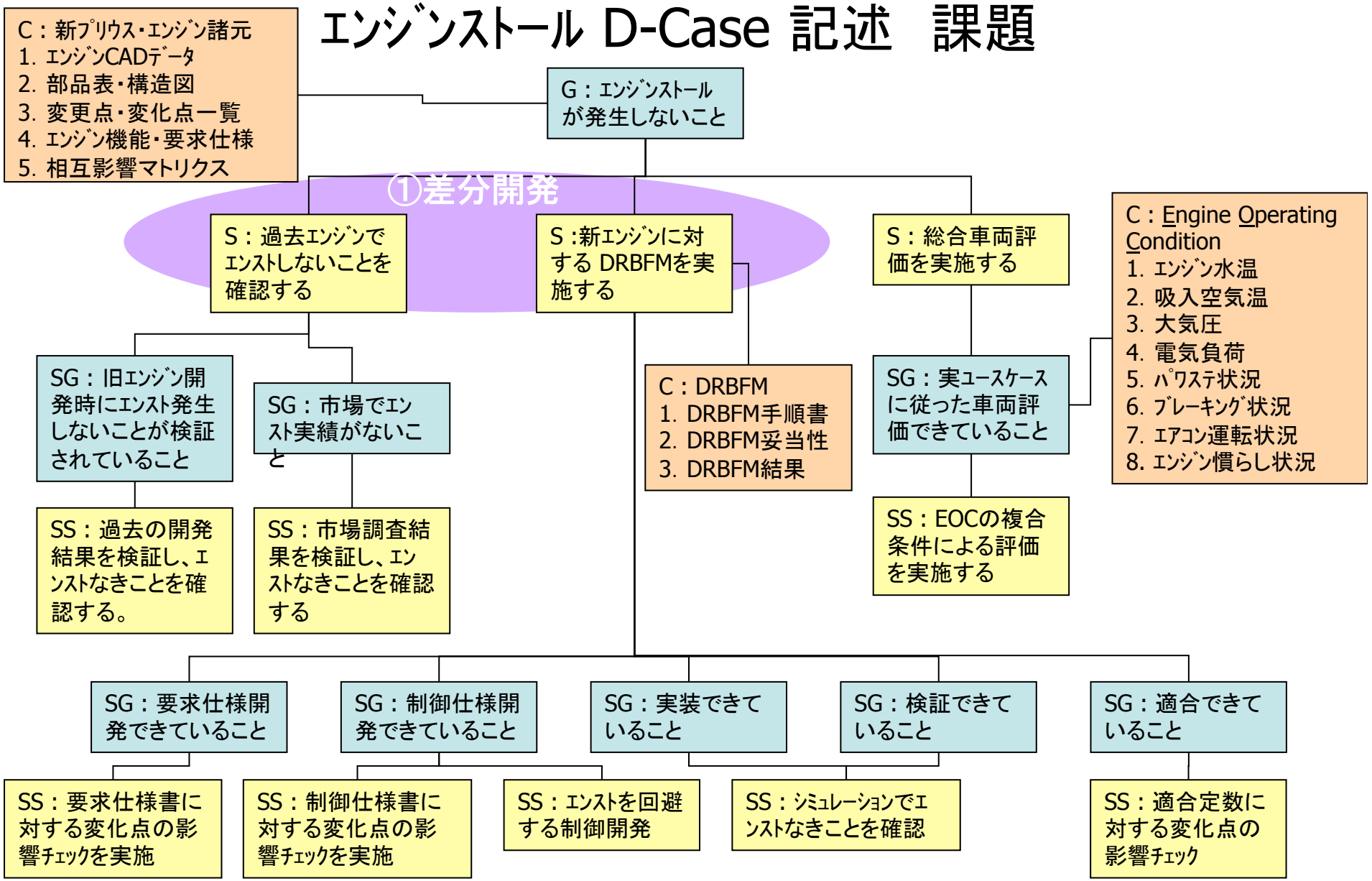
■背景

■ｴﾝｼﾞﾝ制御開発へのD-Caseの適用

■D-Caseの課題

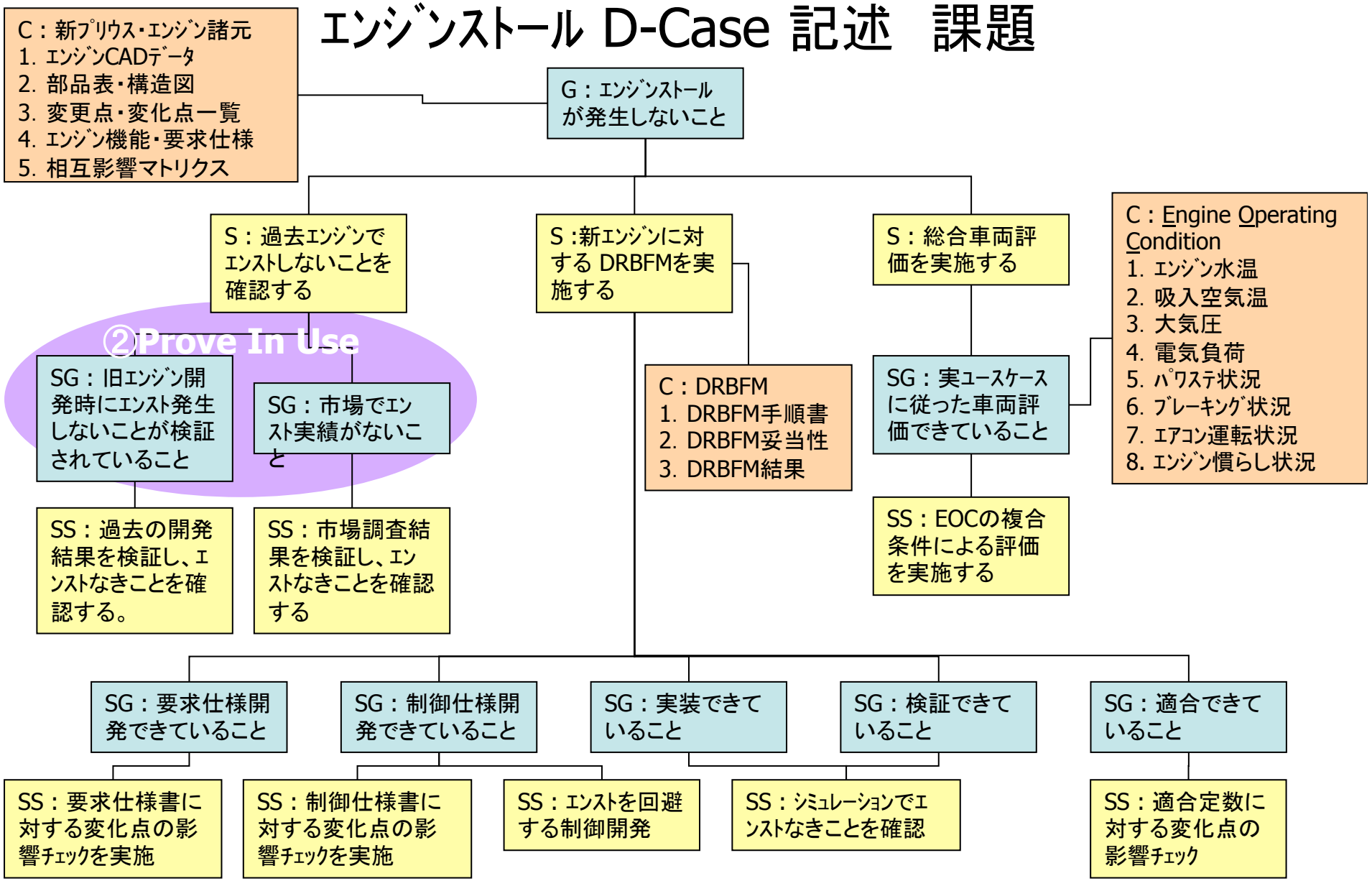
■OMGへの国際標準化活動

エンジンストール D-Case 記述　課題



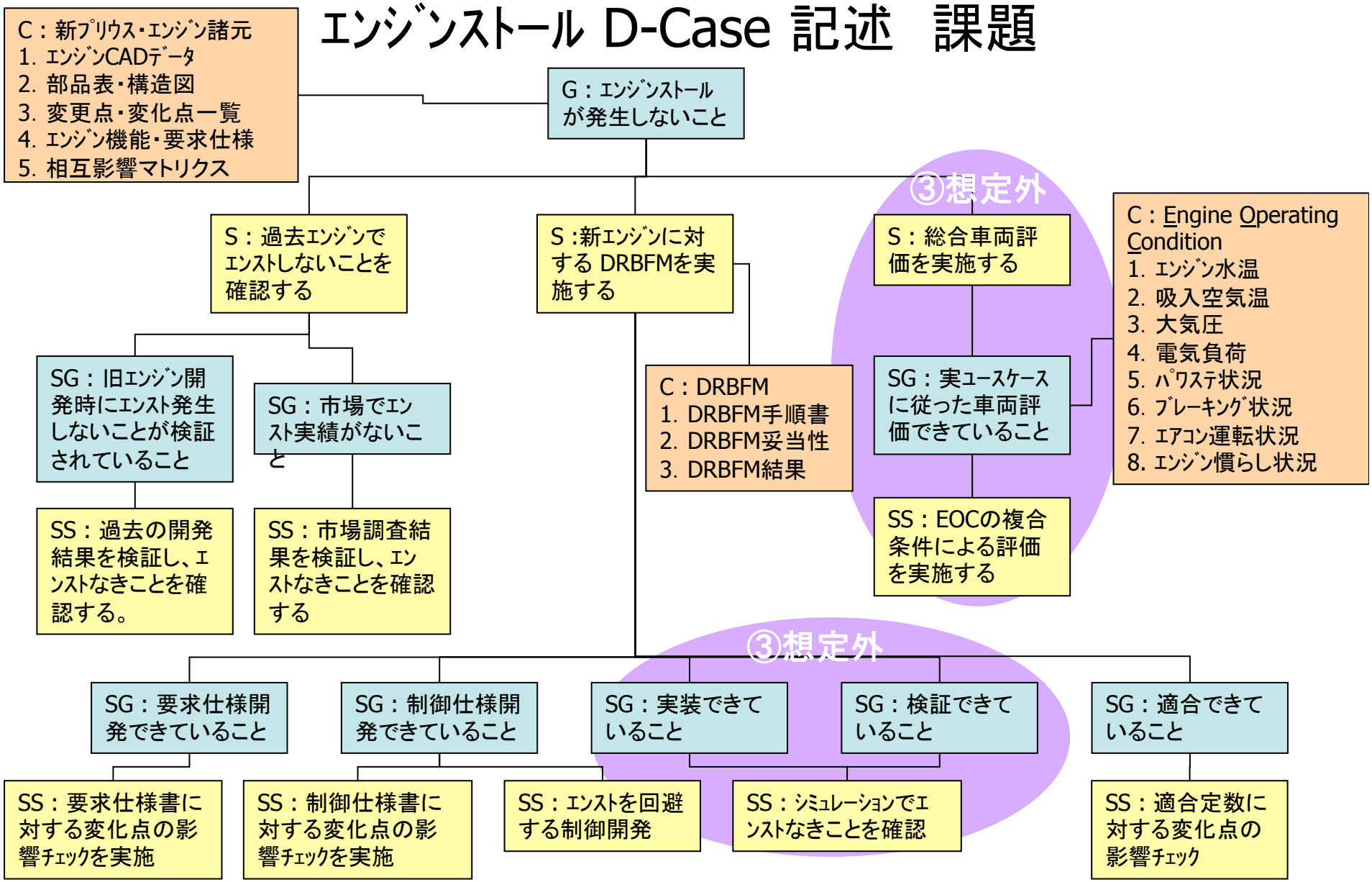
➢抜け漏れなく適切な保証の議論ができているか不明確

エンジンストール D-Case 記述　課題



➢抜け漏れなく適切な保証の議論ができているか不明確

エンジンストール D-Case 記述　課題



➢抜け漏れなく適切な保証の議論ができているか不明確

D-Case適用上の課題

- 差分開発
  - 制御の70~80%は再利用. 新規開発部分と再利用部分の個別議論は適切か？
- Prove In Use
  - 再利用部分に関して、市場実績の評価の扱い方は適切か？
- 想定外 ⇒ Iteration
  - 不明確或いは変化し続ける規制・要求に対してどのように評価するか？

➢実際の自動車制御開発への適用事例を増やし、さらなる深彫り議論が必要
➢社会ｲﾝﾌﾗとの関係もあり、自動車だけでなく産業界全体での議論が必要

本日の内容

■背景

■ｴﾝｼﾞﾝ制御開発へのD-Caseの適用

■D-Caseの課題

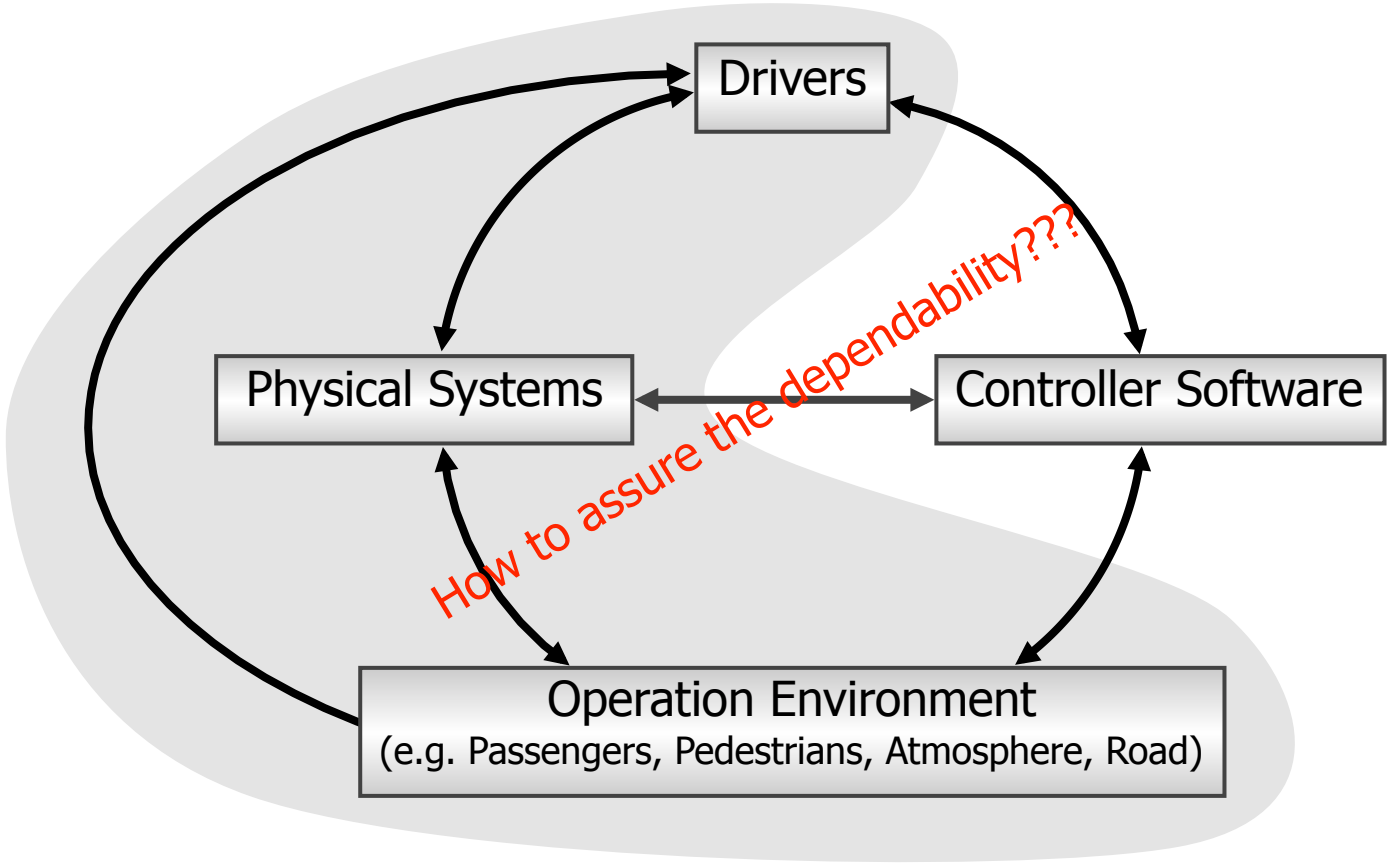
■OMGへの国際標準化活動

What are Consumer Devices?

	Factory machineries	Consumer devices
The number of the production	A few to Many	A huge number
Users	Experts	General users
Cost	High	Sufficiently low
Maintenance	Real field (strongly managed)	Users, Service stations (weekly managed)
Environment	Factory environment (almost stable)	Factory environment User environment (Open, dynamic and diverse)

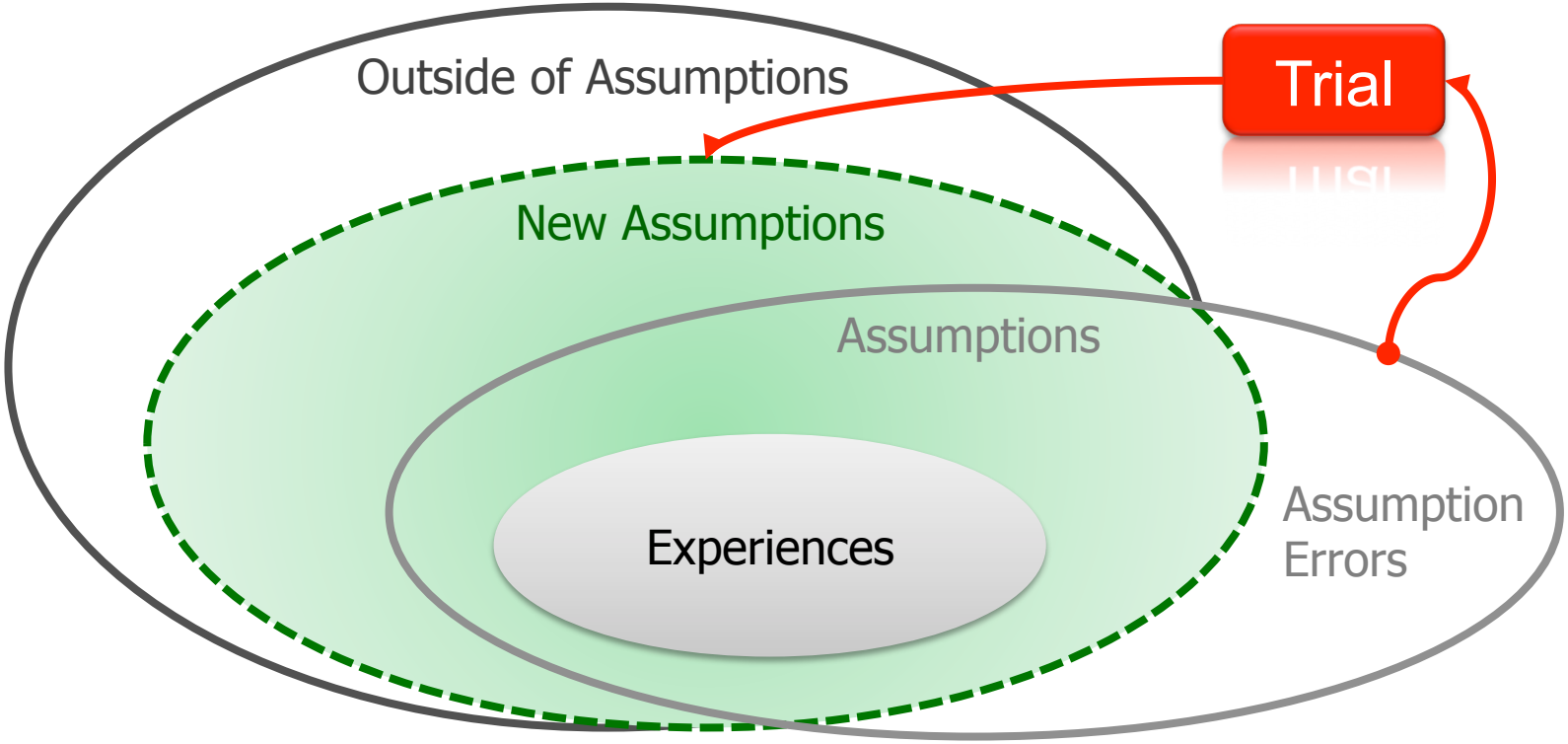
Consumer devices are industrial products used by general end users such as automobiles, service robots, consumer electronics, smart houses and so on.

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.

国際標準化提言 骨子

1. 巨大ｼｽﾃﾑの不完全さ・不確実さから生ずる“想定外”を減らすには、素早い繰り返しの開発ﾌﾟﾛｾｽが必要

2. 自動車業界における制御ｼｽﾃﾑ開発で実践してきた“素早い繰り返し”の開発ﾌﾟﾛｾｽを標準化へ

3. MBDによる制御開発で、Simulationを繰り返しながら“想定外”へも対処可能な開発方法論を織り込む

4. ISO26262体系を元に保証の全体像をﾒﾀﾓﾃﾞﾙ化し、議論項目を明文化する

5. 開発者に負担をかけず、保証議論のTraceabilityが自然にとれるﾂｰﾙﾁｪｰﾝが必要

消費者機械に対するDependability保証の方法論を規格化したい

OMG 団体概要

◆Object Management Group（OMG)は、ｿﾌﾄｳｪｱ開発の標準化に関する国際的･オープンな非営利団体で、1989年に発足。

◆企業･大学･官庁･ｴﾝﾄﾞﾕｰｻﾞｰがOMGに加入し、共同で様々な観点のｿﾌﾄｳｪｱ開発･統合に関する標準を開発する。

◆OMGはISOへの強力な標準化仕様提案団体となっており、OMGへの標準化提案はISO標準化へのFast-Trackｱﾌﾟﾛｰﾁとなる可能性あり。

OMGを通じてｿﾌﾄｳｪｱ開発の観点から
Dependability保証の方法論を規格化する

OMG規格化方針

- **規格化目的**
  - “Dependable”システムを効果的に開発/保証する標準（方法論）を提供する
  - 他規格（ISOxxxxxx)などを補完する

- **規格内容**
  - Consumer Device及び用語の定義
  - 消費者機械のDependabilityの保証に関する議論構造を規格化する
  - 他のツールへのデータフォーマット（インターフェース）を決める

- **条件**
  - 議論構造の利用方法・条件・更新方法などを付帯する
  - 特定プロセスを規定しない(プロセスの例をAppendixに付帯する）

- **ターゲット**
  - Consumer Device Provider (OMG規格に基づいたツールをベンダーにより供給を受け、ISO規格などを補完することができる）
  - ツールベンダー

消費者機械に対するD-Caseを規格化

まとめ

- ✓自動車制御安全性認識の高まり
- ✓D-Caseによる自動車制御開発
- ✓D-Caseの課題
- ✓消費者機械Dependability保証の国際標準化活動