DEOSプロジェクト
最新動向／SysMLとD-Caseの連携

実用化を目指した組込みシステム用
ディペンダブル・オペレーティングシステム

2013年07月 31日
（独）科学技術振興機構 DEOSセンター　屋代　眞
日本アイ・ビー・エム（株） GBS　豊田　学

独立行政法人
科学技術振興機構
Japan Science and Technology Agency

アジェンダ

1. DEOSプロジェクトの最近の動向 （屋代） 15分
   1. DEOSプロジェクトとは？
   2. 主な成果
   3. 今後の主な予定
   4. D-Caseステンシル（PPT用簡易D-Caseお絵かきツール）ご紹介

2. SysMLとD-Caseの連携 25分
   1. 背景 （屋代）
   2. SysMLとD-Caseの連携による可能性 （豊田）
   3. 開発内容とスケジュール （豊田）

DEOSプロジェクト

- (独)科学技術振興機構の戦略的創造研究推進事業CRESTの研究領域のひとつである「実用化を目指した組込みシステム用デイペンダブル・オペレーティングシステム」における研究開発
- 総括・副総括のもと9つの研究機関が参加
- 変化しつづけるシステムのサービス継続と説明責任の全うを目指したソフトウェア開発・保守のための手法や技術の研究・開発
- 研究・開発の成果を生かして成果の国際標準化を行いコンソーシアム設立を目指す

プロジェクトメンバー　－　研究チーム

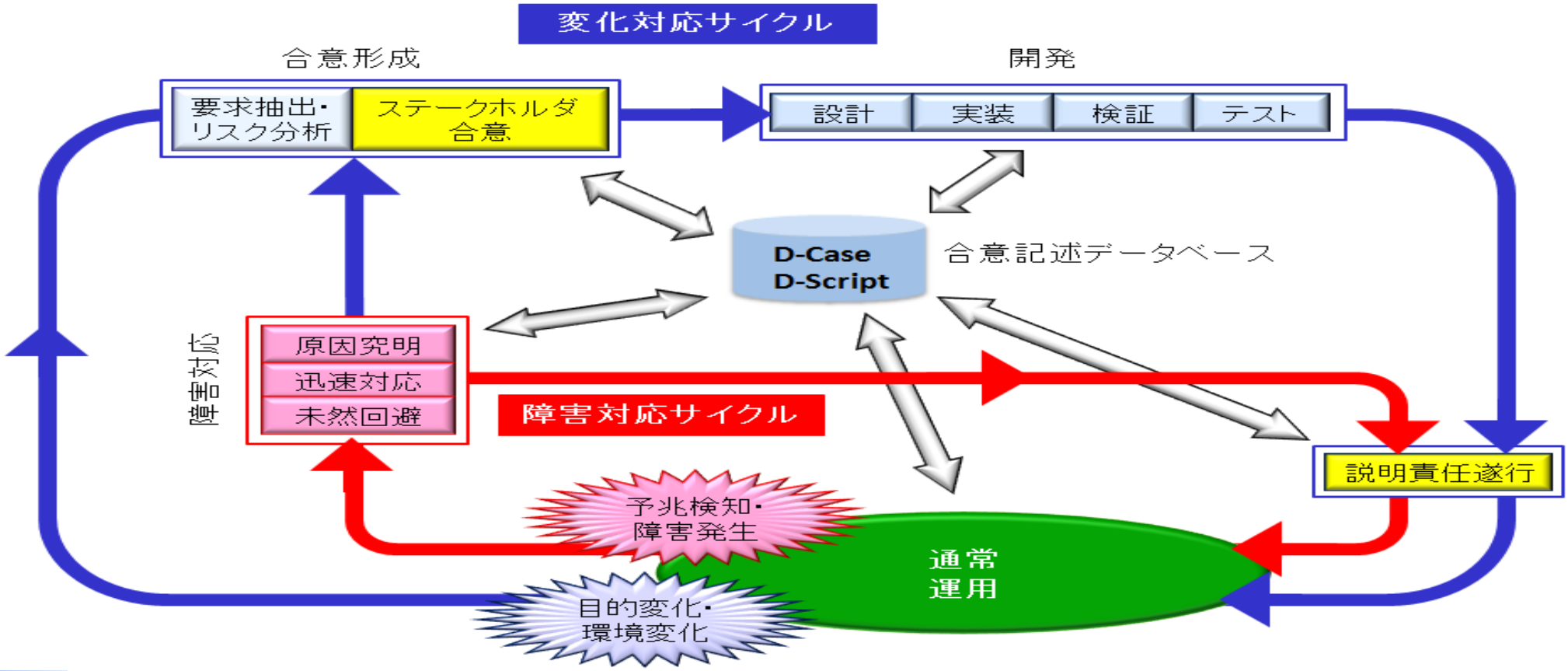
As of 06/01/2013

2006年度採択　研究代表者　（2011年度終了　役職は終了当時）		
石川　裕	東京大学　情報基盤センター　センター長・教授	並列・分散型組込みシステムのためのディペンダブルシングルシステムイメージOS
佐藤　三久	筑波大学　計算科学研究センター センター長・教授	省電力でディペンダブルな組込み並列システム向け計算プラットフォーム
徳田　英幸	慶應義塾大学　環境情報学部　教授	マイクロユビキタスノード用ディペンダブルOS
中島　達夫	早稲田大学　理工学術院　教授	高機能情報家電のためのディペンダブルオペレーティングシステム
前田 俊行	東京大学　大学院情報理工学系研究科　助教	ディペンダブルシステムソフトウェア構築技術に関する研究

2008年度採択　研究代表者・共同研究者		
加賀美　聡	(独)産業技術総合研究所デジタルヒューマン工学研究センター　副センター長	実時間並列ディペンダブルOSとその分散ネットワークの研究
木下　佳樹	神奈川大学　理学部情報科学科　教授	利用者指向ディペンダビリティの研究
倉光　君郎	横浜国立大学　大学院工学研究院　准教授	Security Weaver とPスクリプトによる実行中の継続的な安全確保に関する研究
山本　修一郎	名古屋大学　情報連携統括本部　教授	同上
恩田　昌徳	富士ゼロックス(株)　研究技術開発本部　コミュニケーション技術研究所　グループ長	同上
永山　辰巳	(株)Symphony　代表取締役	同上
松野　裕	電気通信大学　大学院情報システム学研究科　助教	同上
村井　純	慶應義塾大学　環境情報学部　教授	同上
河野　健二	慶應義塾大学　理工学部　准教授	耐攻撃性を強化した高度にセキュアなOSの創出
光来　健一	九州工業大学　大学院情報工学研究科　准教授	同上
山田　浩史	東京農工大学　工学研究院　准教授	同上

DEOSプロセス

- 反復的アプローチ
  - 目的や環境の変化に対してシステムを継続的に変更して行くためのサイクル
  - 障害に対して迅速に対応するためのサイクル
- D-Caseを含む合意記述データベースにより合意形成および開発・運用フェーズの統合を支援

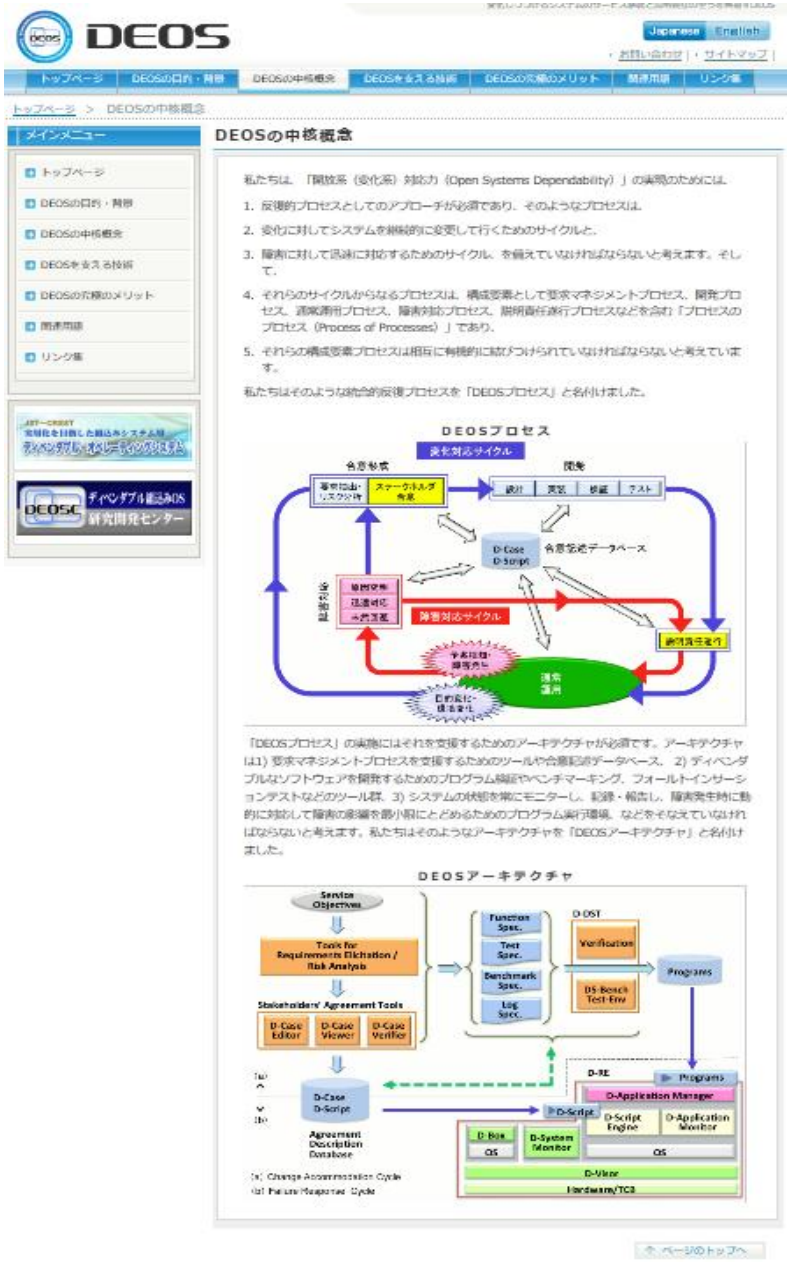


主な要素技術・ツール群

- ステークホルダ合意形成支援ツール
  -> D-Case Editor
- Webブラウザ版 D-Case Editor
  -> D-Case Weaver
- **パワーポイント用 D-Case ステンシル**
  -> D-Case Stencil
- D-Case Verifier （ D-Case/Agda Extension for D-Case Verification ）
  -> 準備中
- D-Script （ D-Caseの記述を基にアプリケーションプログラムを動的に制御）
  -> 準備中
- ソフトウェア検証ツール
  -> モデル検査器
- テスト支援ツール
  -> DS-Bench/Test-Env (DS-Bench/D-Cloud)
- シングルIPアドレスクラスタ
  -> Dependable Single IP Address Cluster (SIAC)
- 仮想マシンモニタとOS監視ツール
  -> D-Visor + D-System Monitor
- DEOSを実現するサービスを提供するための実行環境
  -> DEOS Runtime Environment (D-RE)

DEOS HP DEOSを支える技術:
http://www.dependable-os.net/osddeos/tech.html

DEOS Homepage: http://www.dependable-os.net/



標準化活動 ー IEC, ISO/IEC JTC1, OMG, & The Open Group

- IEC TC56 (Dependability)
  - NWIP提案： Open Systems Dependability 2012年9月提出
  - エキスパートとして改定作業に参加
    - IEC60300-1： Dependability management （最上位規格：Open Systemの概念）
    - IEC 62741: Dependability case
    - IEC 62628: Guidance on software aspect of Dependability
- ISO/IEC JTC1/SC7 (System and software engineering)
  - ISO/IEC15026: System and software assurance (co-editor)
- OMG (SysA: Systems Assurance Task Forceで活動)
  - “Machine Checkable Assurance Language”の提案
    - RFI (Requests for Information: 2012-09-04
    - 審議の後、Requests for Proposals, 投票を経て策定
  - “Dependability Assurance Framework for Safety-Sensitive Consumer Devices”の提案
    - ◆ IPA/SECコンシューマデバイスWG(委員長電通大新誠一教授)、トヨタ大畠氏らが中心となって提出
    - ◆ DEOSチームは標準化に協力
    - RFI (Requests for Information): 2011-12-02
    - White Paper: 2012-9-12
    - RFP(Request for Proposal): 2013.3発行、2013.11 Initial Submission
- The Open Group
  - RTES部会における標準化活動
  - Open Dependability Through Assuredness™(*) 標準V1.0発表 （2013年7月15日）
    - 公開ビデオ http://new.livestream.com/opengroup/allen-philly13/videos/24698802 （9分くらいから）

(*): Dependability Through Assuredness is a trademark of The Open Group

今後の主なイベント

- ET2013@パシフィコ横浜（ http://www1.jasa.or.jp/et/ET2013/index.html ）
  - **DEOS技術展示： 11月20日（水）ー22日（金）**
  - **DEOSセッション： 11月22日（金） 10:00ー14:00**

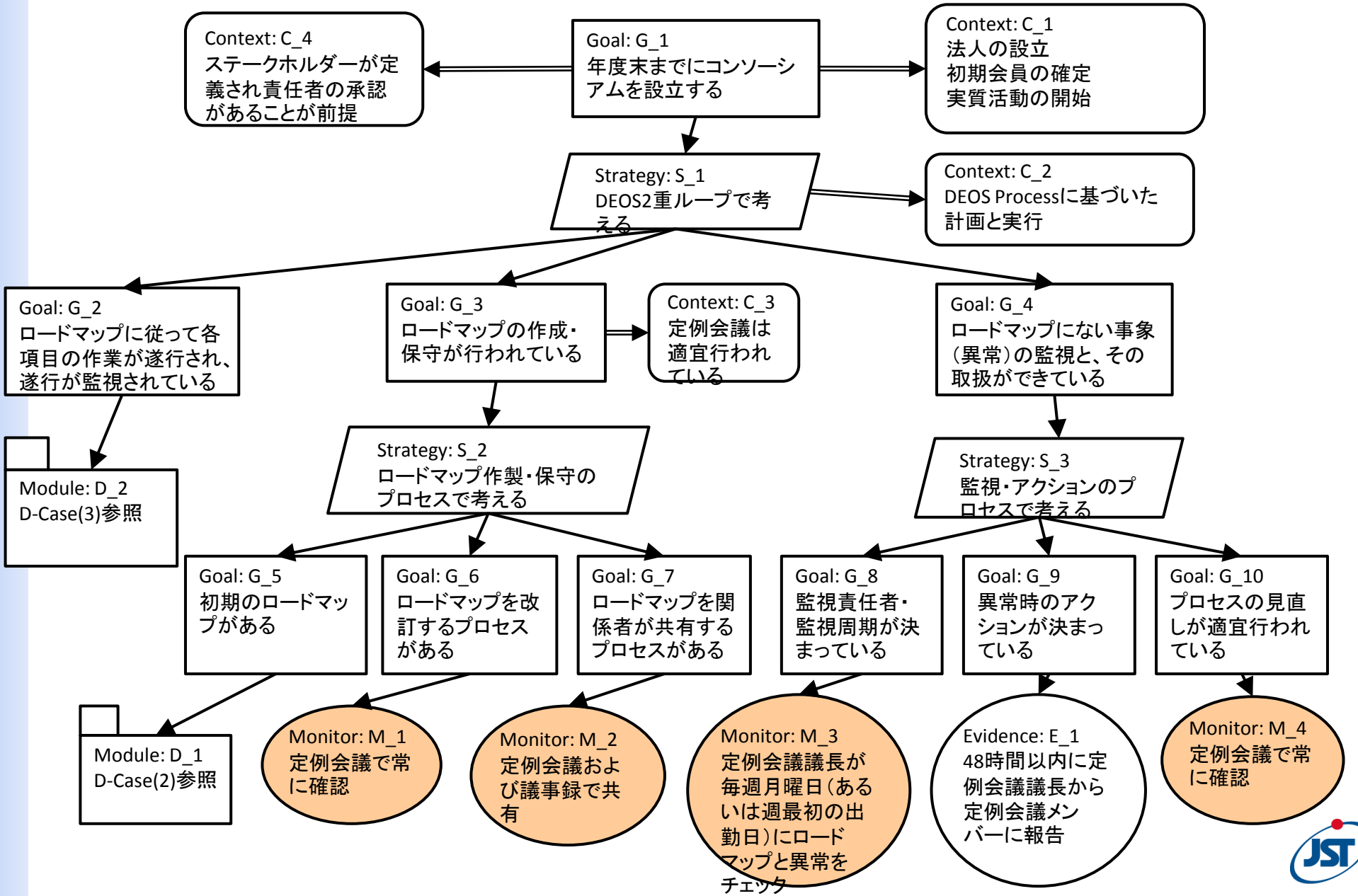
- WOSD2013@Pasadena, CA, USA（ http://www.ubicg.ynu.ac.jp/wosd/wosd2013/ ）
  - **ISSRE2013: 11月4日ー7日**
  - **WOSD2013: 11月4日（予定）**

- OSDコンソーシアム設立（予定）
  - **設立日**
    - **2013年12月01日**
  - **目的**
    - **事業継続・説明責任遂行の手法の確立**
    - **オープンシステムディペンダビリティー技術の標準化**
    - **DEOSに関連した産業の育成**
    - **オープンシステムディペンダビリティー技術の研修**
    - **会員間での非競争領域の共有（情報、事例、基盤プラットフォームの構築、等）**
  - **名称**
    - **一般社団法人 ディペンダビリティ技術推進協会**
    - **英語名： The Association of Dependability Engineering for Open Systems (DEOS Association)**

D-Caseステンシル

- PowerPoint用のAdd-in
  - **PowerPoint2010以降（Windows版）をサポート**
  - **重いツールやサーバーなどが不要で手軽にインストール可能**
  - **機能は限定　ー　D-Caseを手軽に書いてみることが目的**
- プレゼン用・小規模のディスカッションなどに利用可能
  - **簡単にD-Caseを作ってみたい人にお勧め**
  - **開発用のD-CaseはD-Case EditorまたはD-Case Weaver**
- DEOSセンターホームページからダウンロード可能
  - **URL：　http://www.dependable-os.net/tech/D-CaseStencil/**

D-Caseステンシルデモ （DEOSコンソーシアム設立D-Case）



SysMLとD-Caseの連携

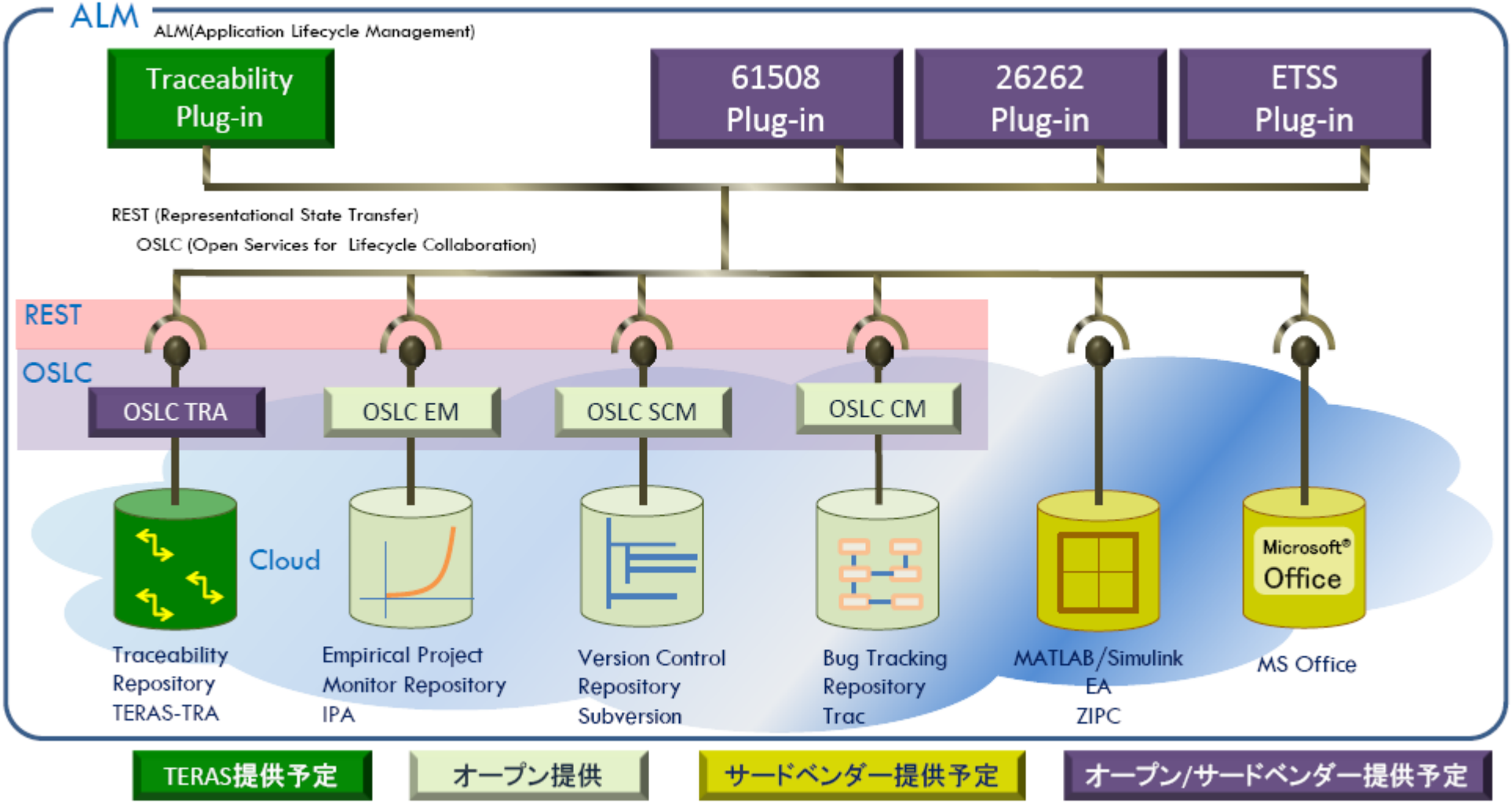
SysMLとD-Caseの連携プロジェクトの背景

- D-Caseは開発・運用を通じてディペンダビリティーに寄与するが、既存の開発・運用プロセスやツールとはどのようにしていくのが良いか？

- 開発・運用で既存の仕組みとの連携が考えられるか？
  - **開発ツールとしてのSysMLとの連携は？**
  - **PLMツールとの連携は？**

- オープンな標準であるOSLC（Open Services for Lifecycle Collaboration）を仲介した連携
  - **D-Caseツール–OSLCインターフェス**
  - **ユースケースとデモ**

TERAS完成予想図



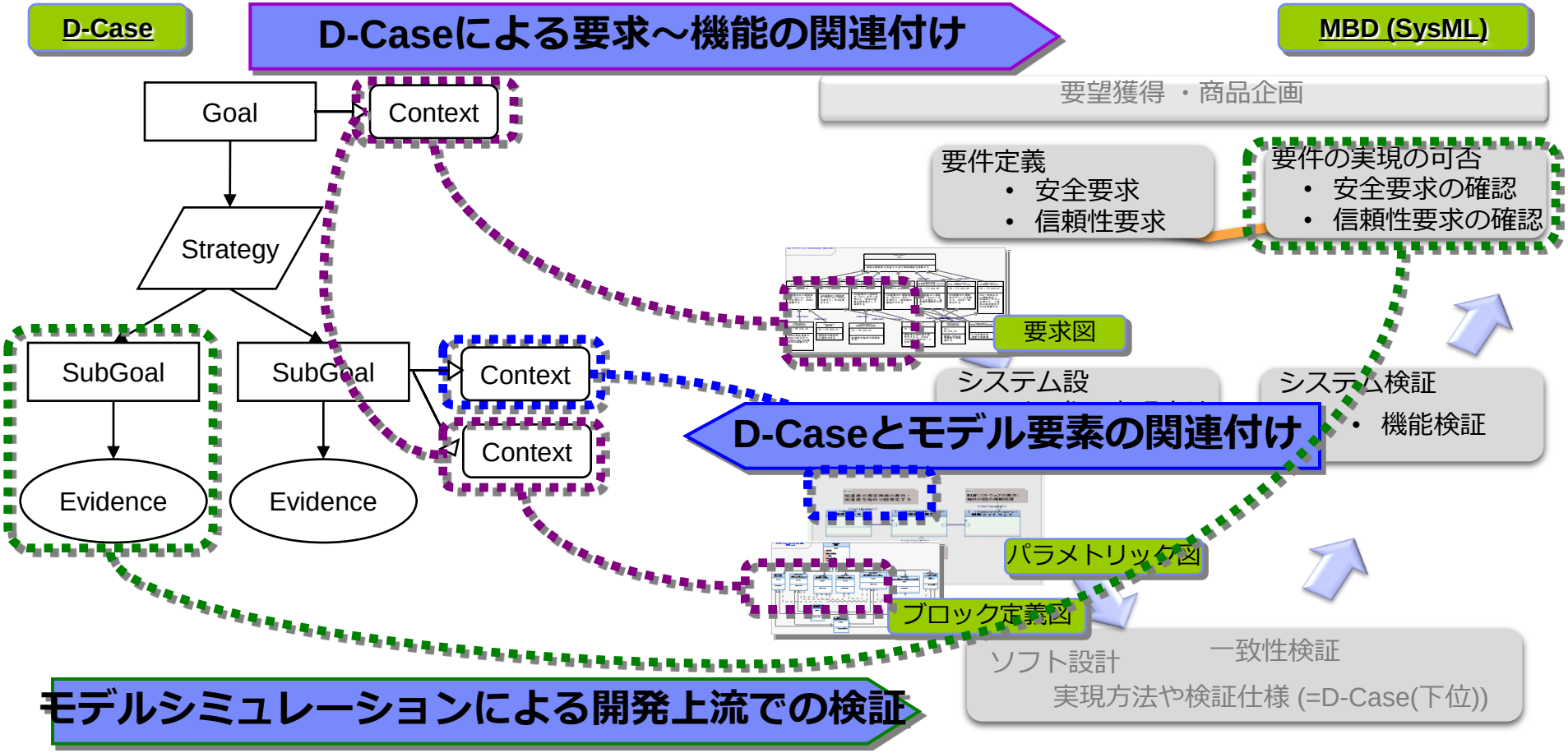
出展： 最新TERAS V2概要とV3構想 2013/3/11

D-CaseとSysML開発環境の連携の技術的概要

D-CaseとSysML開発環境の連携　概要

開発における メリット

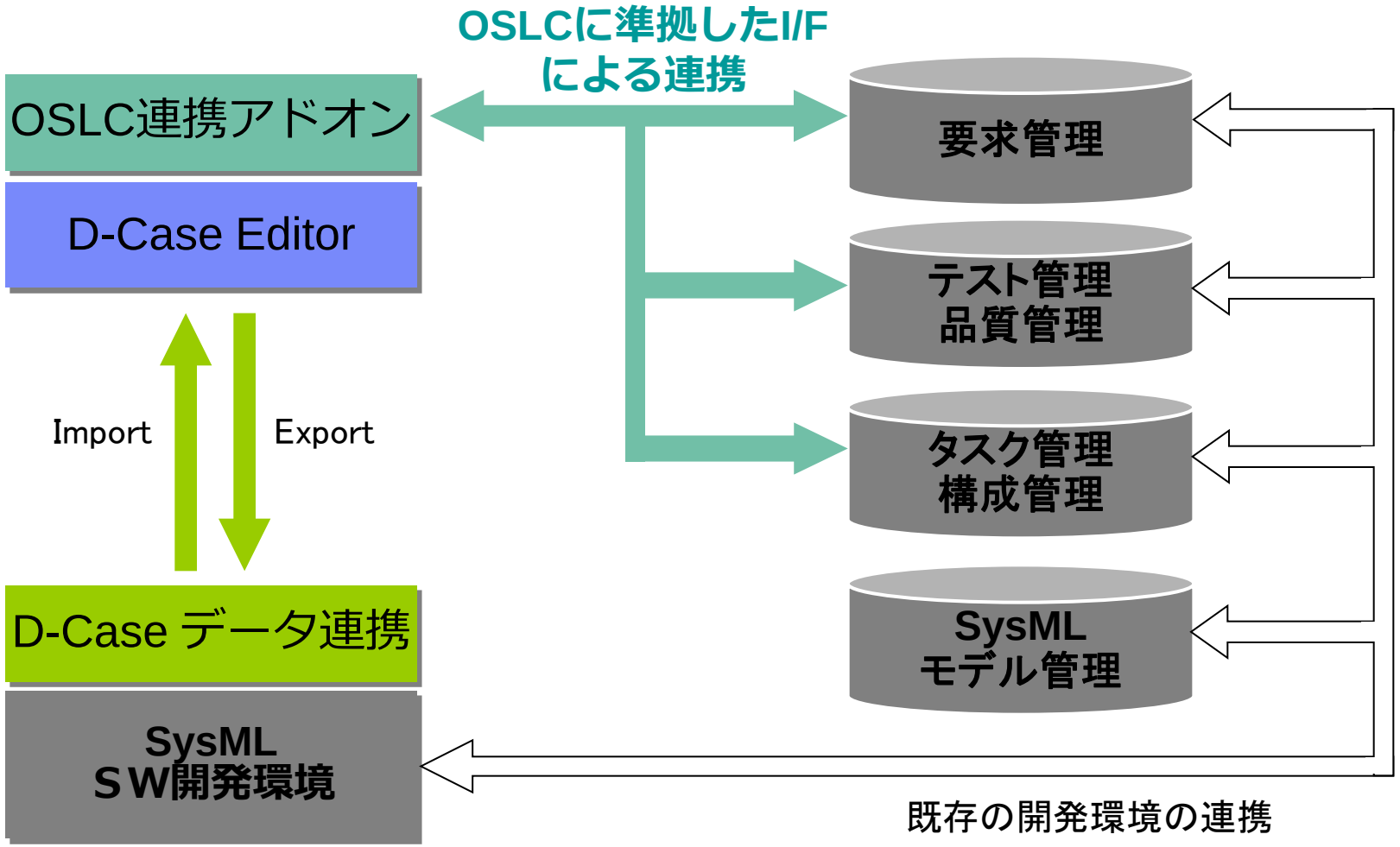
- 開発の上流で要求の妥当性を検証できる
- ゴールの達成に必要な要件・機能の関係を明確化できる



システム構成

- D-Case Editor の OSLC連携アドオン
- SW開発環境の D-Case データ連携機能

OSLC (Open Services for Lifecycle Collaboration)
　異なるALMツール間でのデータ連携を可能とする
　仕様を策定



開発の上流で要求の妥当性を検証

•D-Caseによりゴールを達成するために必要な要素を明確にする

•ゴールの達成に満たすべき要求を明示

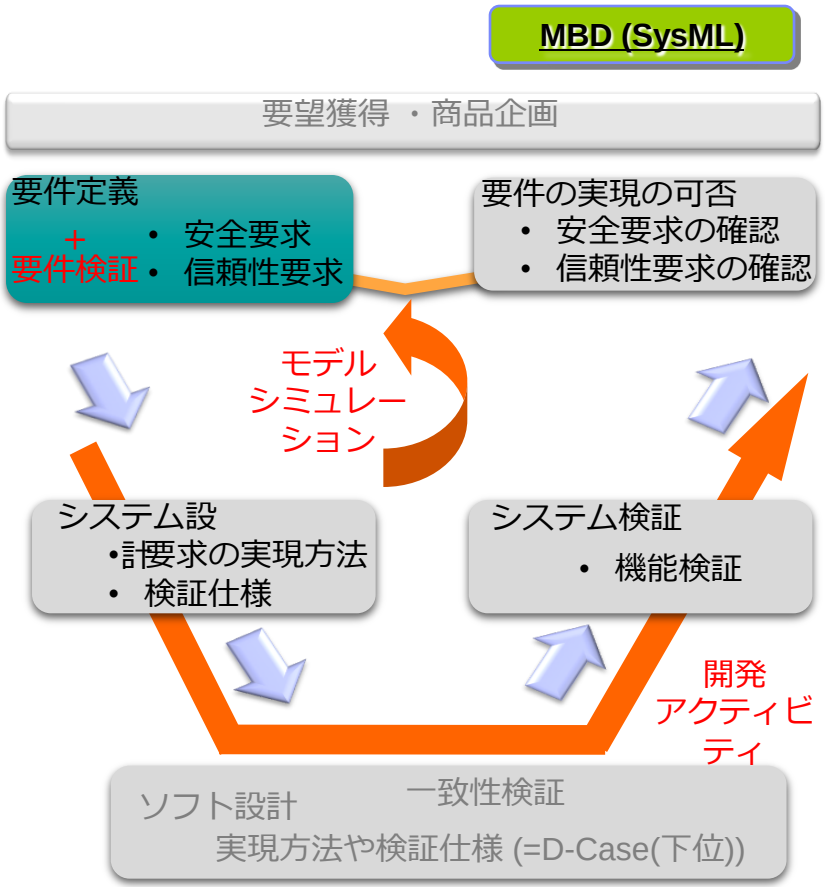
要求をD-Caseに関連付けし参照可能とする

•ゴールの達成に必要な開発アクティビティ
を管理

開発アクティビティをD-Caseに関連付けし参照可能とする

•モデルシミュレーションによる開発上流
での検証

モデルシミュレーション結果をD-Caseに関連付けし妥当性の根拠とする



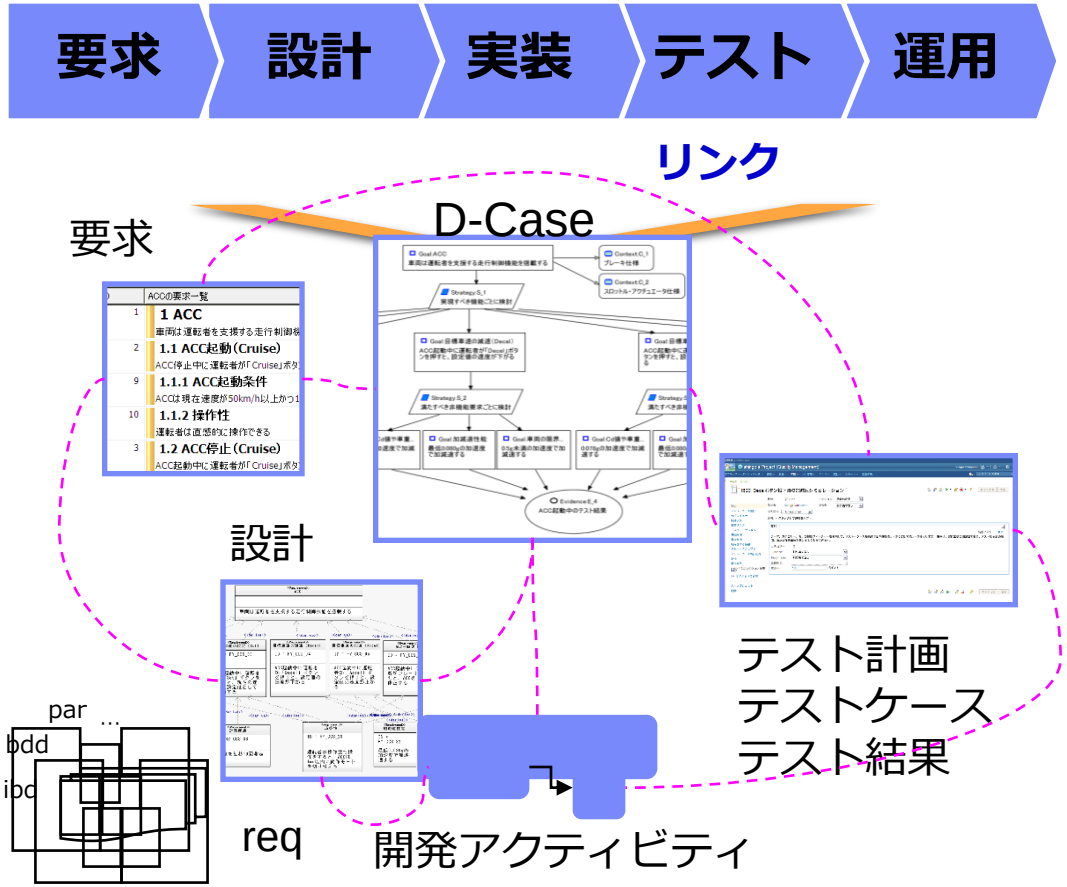
ゴール達成に必要な要件・機能のつながりを明確化

•D-Caseにより開発の意図を継続的に明確化する

•全ライフサイクルで何を実現したいか(=要求）を明確化

•変更に対する影響範囲を特定し修正の妥当性を検証

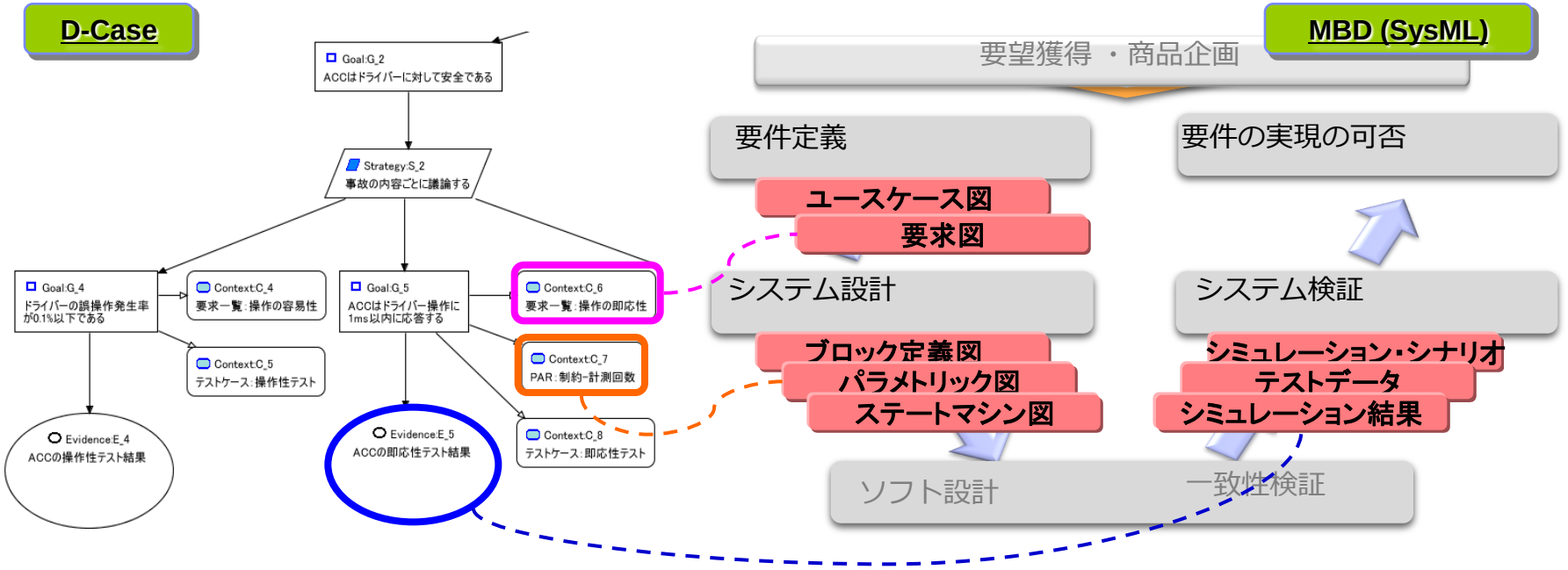
D-Caseとモデル要素の関連付けによりゴール~要求~機能の関係を明確にする



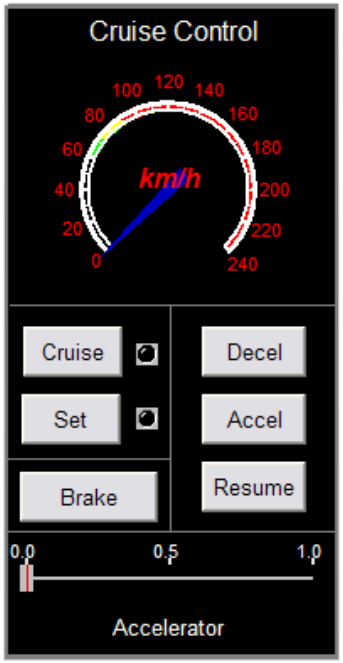
デモ :自動車のクルーズコントロールシステム開発へD-Caseを適用

1. **Dependability合意形成の手法・ツール**
   D-Case
2. **D-Case作成環境**
   D-Case Editor
3. **モデリング言語**
   SysML

V字プロセスでSysMLモデルとD-Caseを作成してシミュレーションで検証する



【参考】　クルーズコントロールシステムの動き



◆クルーズコントロールを起動 / 終了する

Cruise を押す　※ PCS（プリクラッシュ・セーフティ）から停止要求があれば終了する

◆現在速度で定速走行を開始する　※30km/h以上100km/h以下での走行時に限定

クルーズコントロール起動後に Set を押す

◆目標速度を設定し定速走行を開始する　※30km/h以上100km/h以下で設定可

◆目標速度より遅い速度で走行している場合

クルーズコントロール起動後に Accel を押して任意の速度を設定して Set を押す

※ Accel は1プッシュあたり、3km/h設定速度が上がる

◆目標速度より速い速度で走行している場合

クルーズコントロール起動後に Decel を押して任意の速度を設定して Set を押す

※ Decel は1プッシュあたり 3km/h設定速度が下がる

◆クルーズコントロールを中断(休止)する

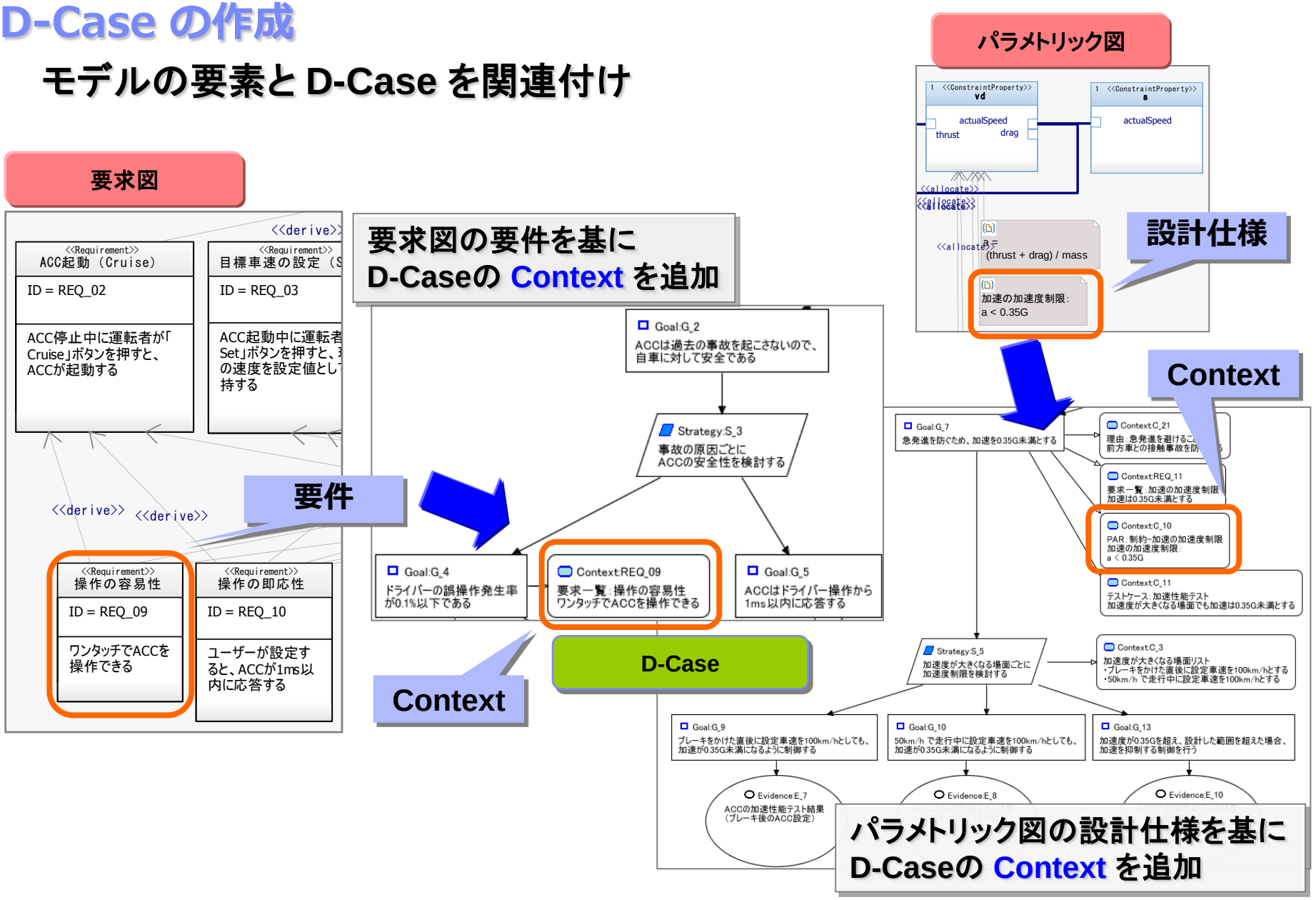
クルーズコントロール起動時に Brake を踏む

◆クルーズコントロールを再開する　※休止時の目標速度で定速走行を開始する

クルーズコントロール休止時に Resume を押す

D-Case の作成

モデルの要素と D-Case を関連付け



モデルシミューレションによる検証

ボディタイプ セダンとワゴンに対して加速度要求を満たすことの検証

テストデータ

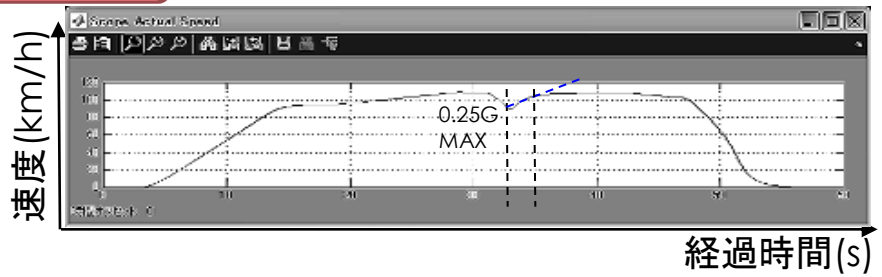
要求 ： 急発進を防ぐため加速度の制限を 0.35G 未満とする

ボディタイプ	セダン	ワゴン
車重 (kg)	1,700	2,500
空気抵抗 Cd値	0.44	0.50
前面投影面積 (m^2)	1.8	2.0
加速度要求	0.35G 未満	0.35G 未満

シミュレーション結果

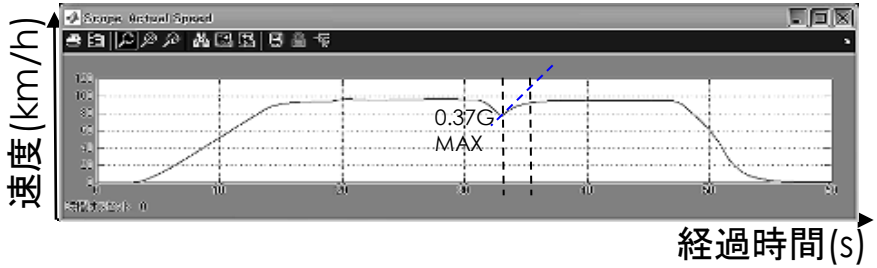
テストデータをモデルに反映しシミュレーションを実行

ワゴン



加速度要求：0.35G未満
最大加速度：0.25G
クリア！

セダン



加速度要求：0.35G未満
最大加速度：0.37G
クリアせず！

D-CaseとSysML開発環境の連携　まとめ

D-CaseとSysML開発環境の連携のメリット

- 開発の上流で要求の妥当性を検証できる
- ゴールの達成に必要な要件・機能の関係を明確化できる

デモ

- クルーズコントロールシステム開発へD-Caseを適用

連携機能の開発

- D-Case Editor の OSLC連携アドオンの開発
- SW開発環境の D-Case データ連携機能の開発

2013年8月中旬
開発完了を予定