NTT DATA
Global IT Innovator

IEC62853　自動車制御システム開発への応用研究

2018年3月27日

キャッツ株式会社　プロダクト事業本部

CATS Communication Art Technology Systems

INDEX

本資料は，株式会社Symphonyと名古屋大学の共同研究，及び
キャッツ株式会社への委託研究の成果の一部を，自動車応用部会
にて議論，整理したものである。

NTT DATA

IEC62853の概要

01 オープンシステム・ディペンダビリティ

Communication Art Technology Systems

- オープンシステムとは
  - 境界、機能や構造が時とともに変化し、認識のされ方、記述のされ方が視点によって異なるようなシステムのこと。
  - 変化には、要求や環境の変化への適応や、システム自身の自発的な発展による変化が含まれる。
  - オープンシステムでは変化が頻繁に発生するため、その都度不具合が発生しやすい。そのため、不具合を未然に防いだり、早急に対応することによってサービスを継続的に提供できることが求められる。
- オープンシステム・ディペンダビリティ（OSD）
  - システムの目的、目標、環境及び性能の変化に対応し、不断に説明責任を遂行することによって、期待されるサービスを求められた時に求められたように提供する能力。

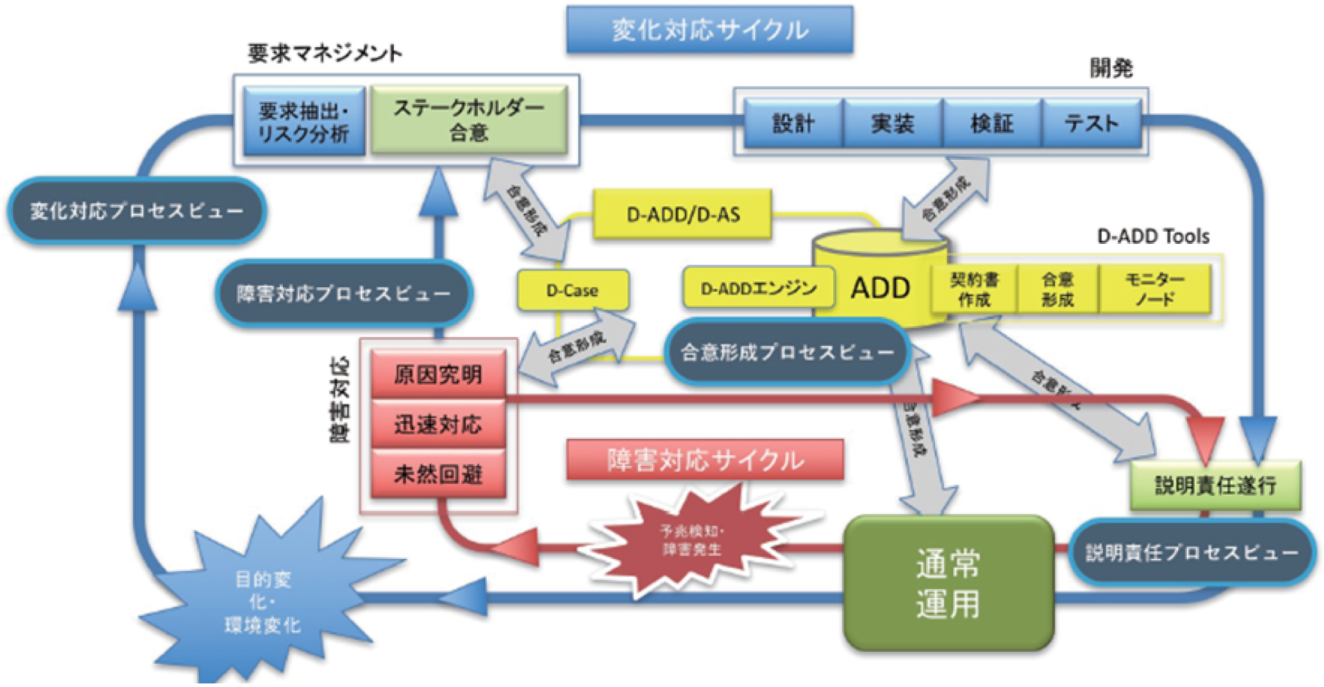
参考：
オープンシステム・ディペンダビリティ達成の要件について～国際標準案IEC62853のアプローチ～
神奈川大学　木下佳樹

NTT DATA

03 IEC62853

Communication Art Technology Systems

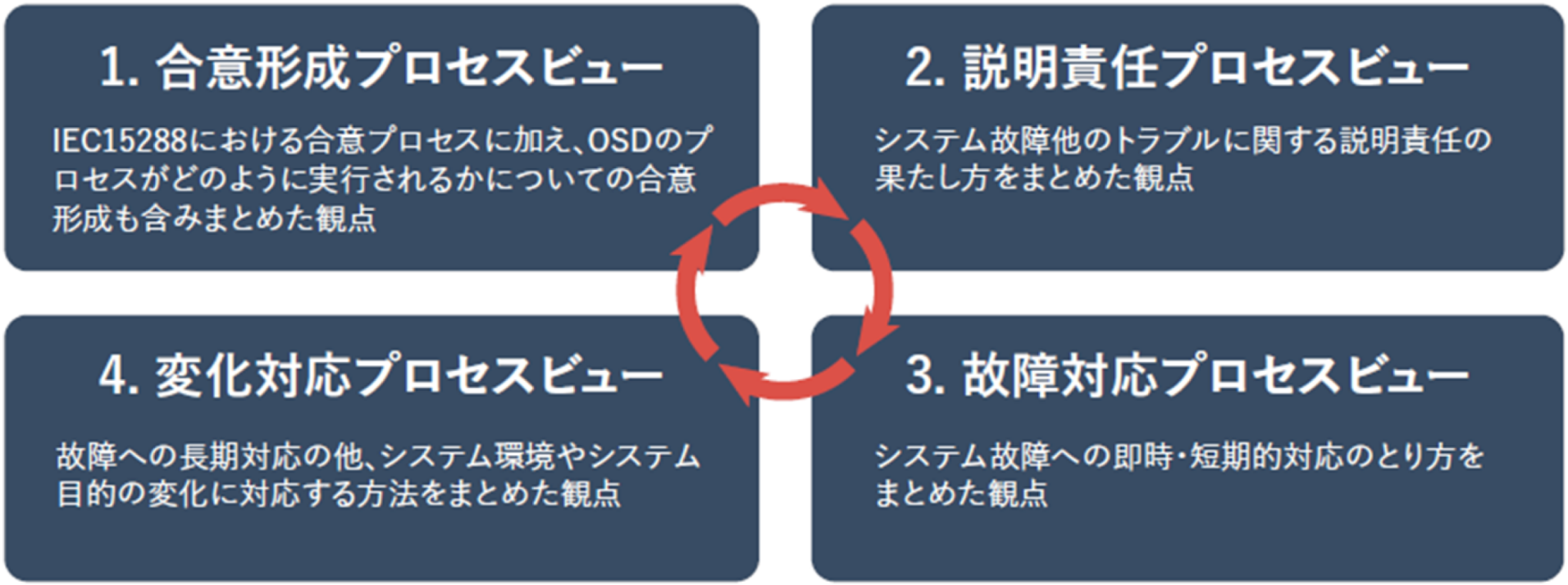
- IEC62853とは
  - 「システムライフサイクルがOSDを達成するため」の要件を規定する標準。
  - IEC62853 Open systems dependabilityとして国際標準の制定が進行中。
  - IEC62853ではOSDの要件として、「合意形成」、「説明責任」、「障害対応」、「変化対応」の4つのプロセスビューを求めている。



4つのプロセスビュー

Communication Art Technology Systems

■ 4つのプロセスビューの概要



NTT DATA

自動車制御システム開発への応用研究

01 背景

Communication Art Technology Systems

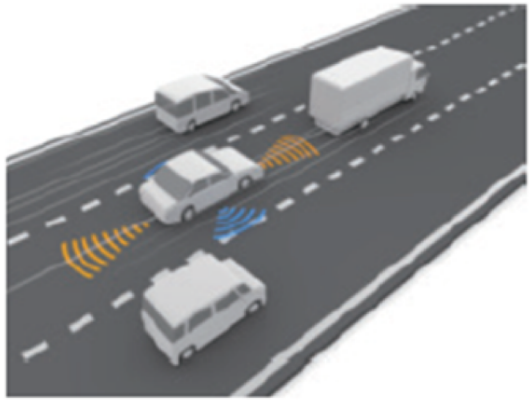
■ 自動車制御システム開発における4つのプロセスビュー

変化対応

法令や規格、交通インフラなど、システムを取り巻く環境が刻々変化する中で、OTAによる車載ソフトウェアのアップデートを柔軟にしていく必要がある。

障害対応

システムの誤作動、HW故障、ハッキングなどによる障害へ迅速に対応し、ユーザに安全性の高い運転支援を持続的に提供できる必要がある。



合意形成

OEM,サプライヤなど、ステークホルダー間の合意形成を確実に行うことにより、不十分な合意形成を原因とする下流工程の後戻りを防ぐ。

説明責任

システムの安全性、規格適合性がどのように実現されているか説明可能にすることにより、ユーザの安心感、さらには社会的信用を獲得する。

■ 自動車開発プロセスにおいてOSDを確保するにはどのようなプロセスを定義すべきか？

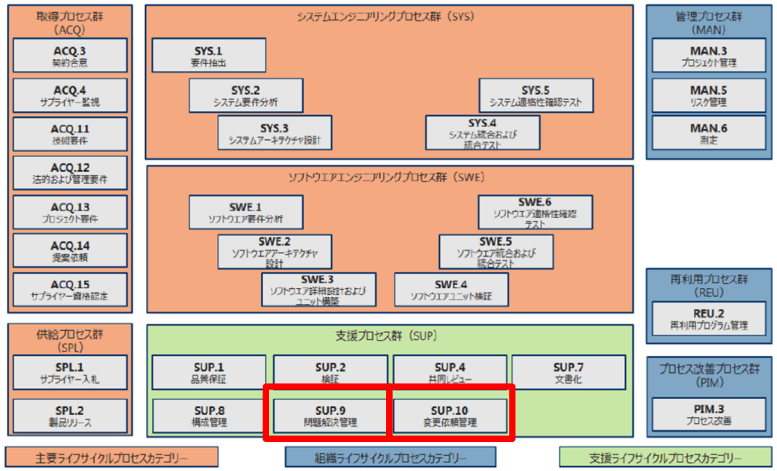
NTT DATA

02 目的

Communication Art Technology Systems

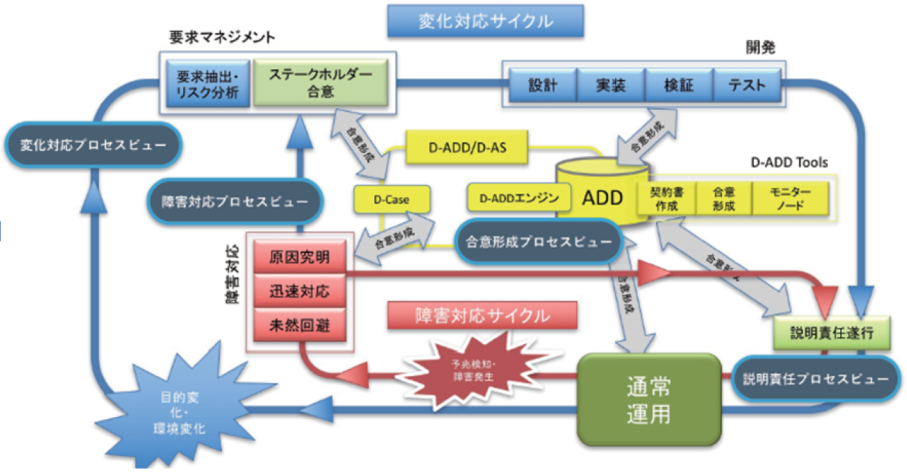
- A-SPICEとIEC62853で構成するディペンダビリティプロセス
  - 自動車分野における開発プロセスであるA-SPICEと、IEC62853を組み合わせてディペンダビリティプロセスを構築する。
  - 4つのプロセスビューとしては、A-SPICEでは障害対応、変化対応がそれぞれ、問題解決管理、変更依頼管理として定義されているので、IEC62853から、合意形成と説明責任を追加する。

A-SPICE



SUP.9：問題解決管理（障害対応）
SUP.10：変更依頼管理（変化対応）

IEC62853



合意形成
説明責任

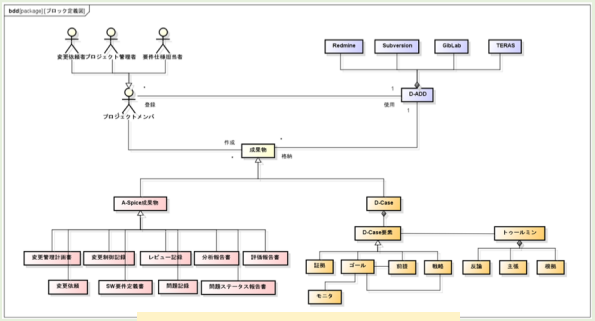
03 アプローチ

Communication Art Technology Systems

- SysMLによるプロセスのモデリング
  - 文章による記述だけではプロセス内容の理解が難しい。そこで、プロセスをモデリング言語により図解し、一般の技術者に理解しやすくする。
  - モデリング言語としては、ソフト、ハード両分野の技術者に浸透しているSysMLを使用する。ブロック定義図で構成、アクティビティ図でプロセスフローをモデル化する。
  - プロセスはそれを適用する組織によって異なるため、一般的に1つのモデルとして定義することは難しい。ここでは、ある組織での1つのユースケースとしてモデル化を行う。

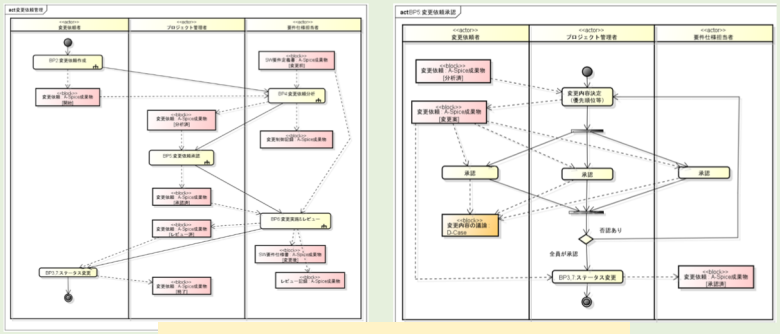
SysMLモデル

ブロック定義図



構成のモデル化

アクティビティ図



プロセスフローのモデル化

NTT DATA

04 SysMLモデル

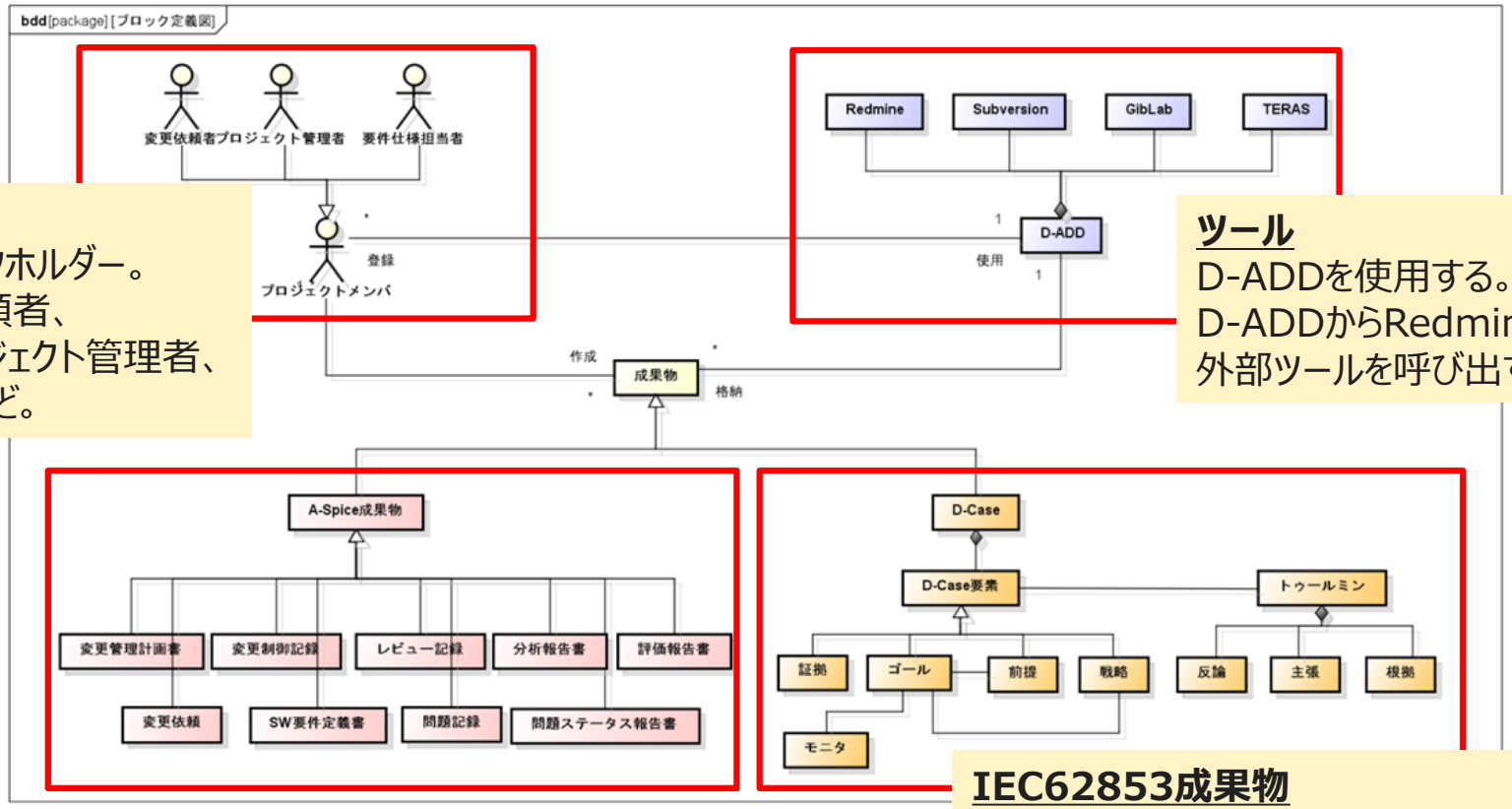
Communication Art Technology Systems

- クラス図
  - プロセスにおける出現要素（アクター、成果物、ツール）を抽出し、それらの関連を定義する。
  - アクターについては、A-SPICEでは定義されていないため、一例を示す。
  - 成果物はA-SPICEの成果物とIEC62853の成果物（D-Case）を想定する。
  - ツールはD-ADDを使用することを想定する。
- アクティビティ図
  - A-SPICEのワークフローにおいてIEC62853の4つのプロセスビューがどのように実行されるかをモデル化する。
  - 具体的に、A-SPICEにおいて成果物に至る過程を合意形成と考え、D-Caseで記述する。
  - A-SPICEプロセス内の各処理の中で、DEOSの合意形成プロセスを回す。

05 ブロック定義図

Communication Art Technology Systems

ブロック定義図



アクター
プロジェクトのステークホルダー。
OEMとして変更依頼者、
サプライヤとしてプロジェクト管理者、
要件仕様担当者など。

ツール
D-ADDを使用する。
D-ADDからRedmine, SVN等の
外部ツールを呼び出す。

A-SPICE成果物
A-SPICEで定義される成果物。
変更管理計画書やレビュー記録など。

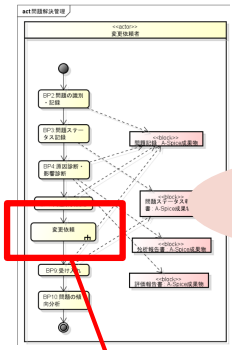
IEC62853成果物
A-SPICE成果物作成過程での議論を
D-Caseとして記述する。
議論の詳細はツールミンモデルで記述。

NTT DATA

06 アクティビティ図

Communication Art Technology Systems

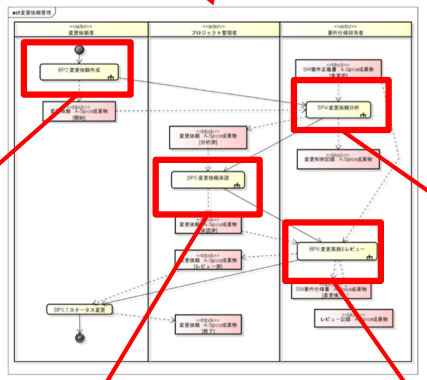
アクティビティ図の階層構造



問題解決管理

障害対応

問題解決管理のサブプロセスとして
変更依頼管理を呼び出す。



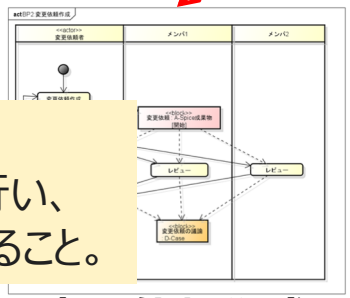
変更依頼管理

変化対応

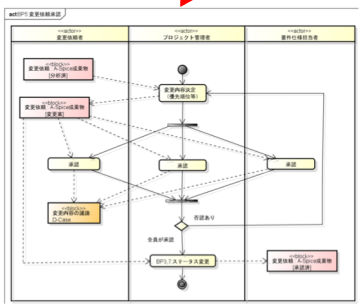
変更依頼管理プロセス内の各処理の中で
合意形成プロセスを回す。

合意形成

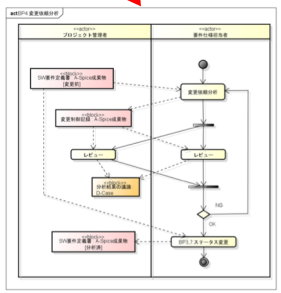
成果物に対して
関係者がレビューを行い、
内容について合意すること。



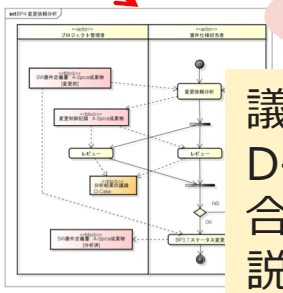
変更依頼作成



変更依頼承認



SW要件仕様書変更&レビュー



変更依頼分析

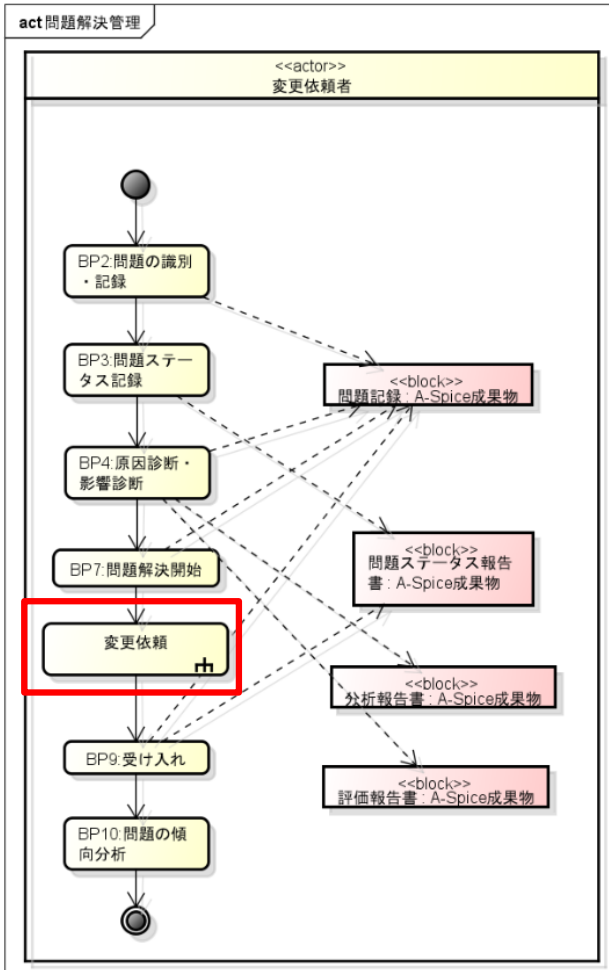
説明責任

議論の証跡を
D-Caseとして残し、
合意に至った過程を
説明できること。

06 アクティビティ図

Communication Art Technology Systems

問題解決管理



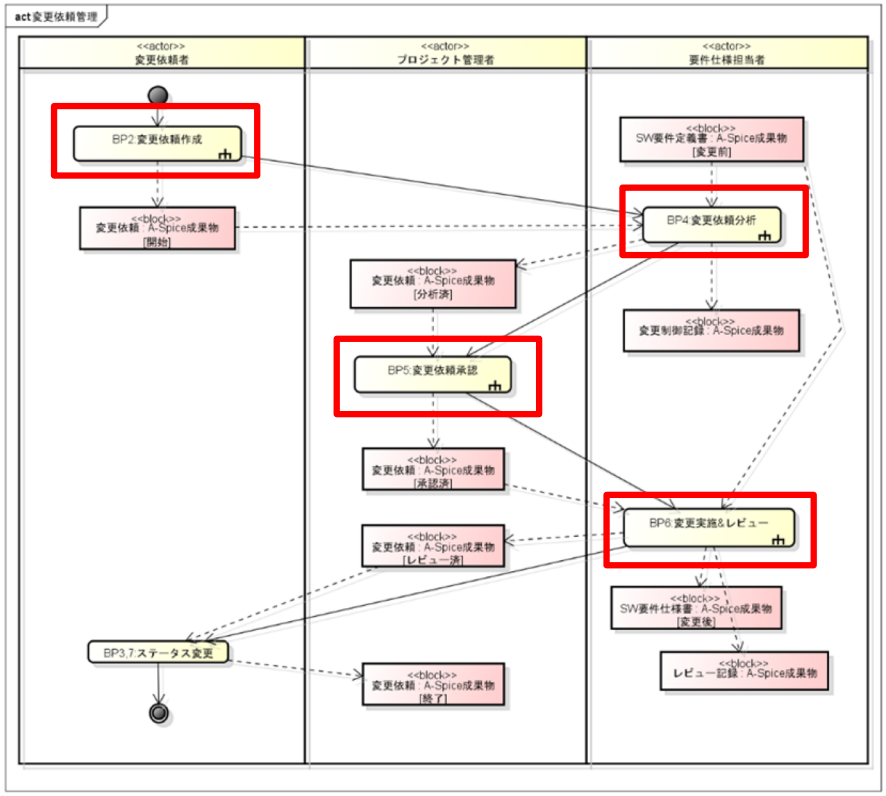
アクティビティ	問題解決管理
アクター	OEM：変更依頼者
内容	・障害発生時、OEMにおいて問題の識別、原因分析を行い、サプライヤに変更依頼を出す。 ・「変更依頼」処理から変更依頼管理プロセスを呼び出す。
A-SPICE成果物	問題記録、問題ステータス報告書、分析報告書、評価報告書

NTT DATA

06 アクティビティ図

Communication Art Technology Systems

変更依頼管理



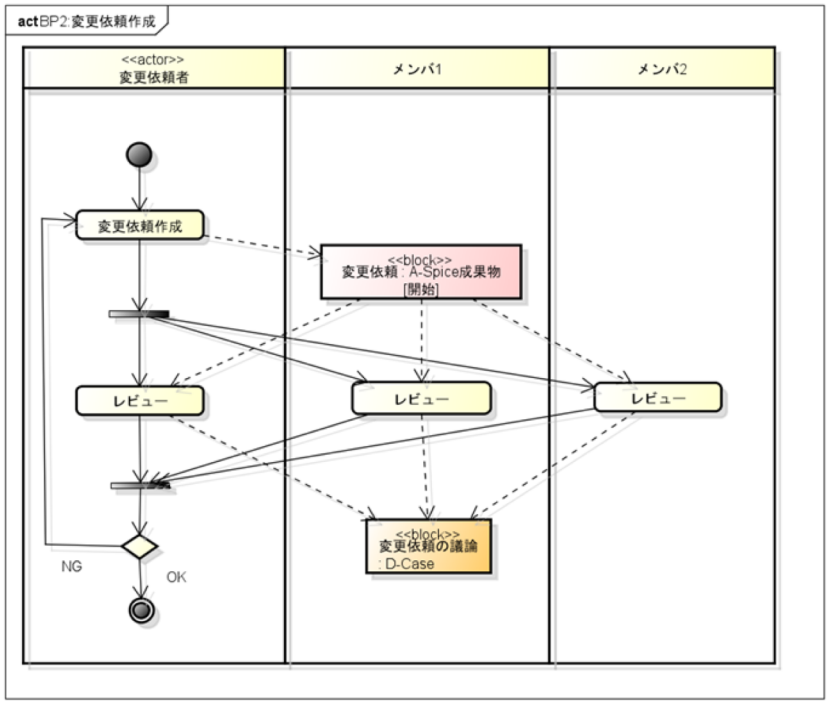
アクティビティ	変更依頼管理
アクター	OEM：変更依頼者 サプライヤ：プロジェクト管理者、要件仕様担当者
内容	・変更依頼者が変更依頼を作成する。 ・サプライヤにおいて、変更依頼内容の分析、変更依頼内容承認、変更実施、変更レビューを行う。 ・各処理の中で合意形成サイクルを回す。
A-SPICE成果物	変更依頼、変更制御記録、SW要件定義書

NTT DATA

06 アクティビティ図

Communication Art Technology Systems

変更依頼作成



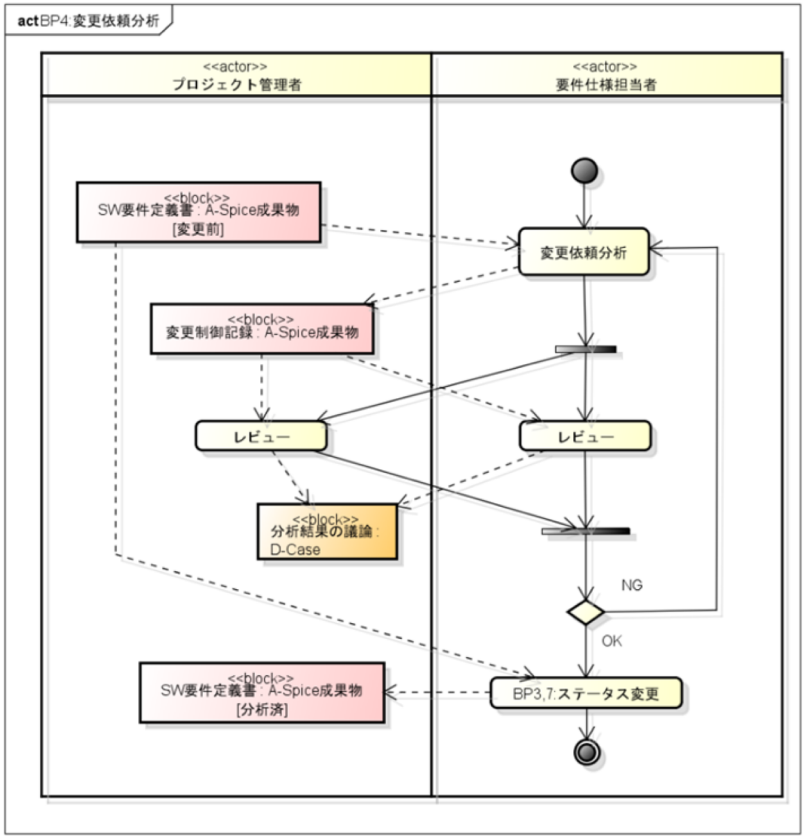
アクティビティ	変更依頼管理
アクター	OEM：変更依頼者、メンバ1、メンバ2
内容	・OEMにおいて、変更依頼者が変更依頼を作成する。 ・変更依頼の内容をOEM内の他メンバとともにレビューする。 ・レビュー内容はD-Case「変更依頼の議論」として記録する。
A-SPICE成果物	変更依頼
62853成果物	変更依頼の議論

NTT DATA

06 アクティビティ図

Communication Art Technology Systems

変更依頼分析



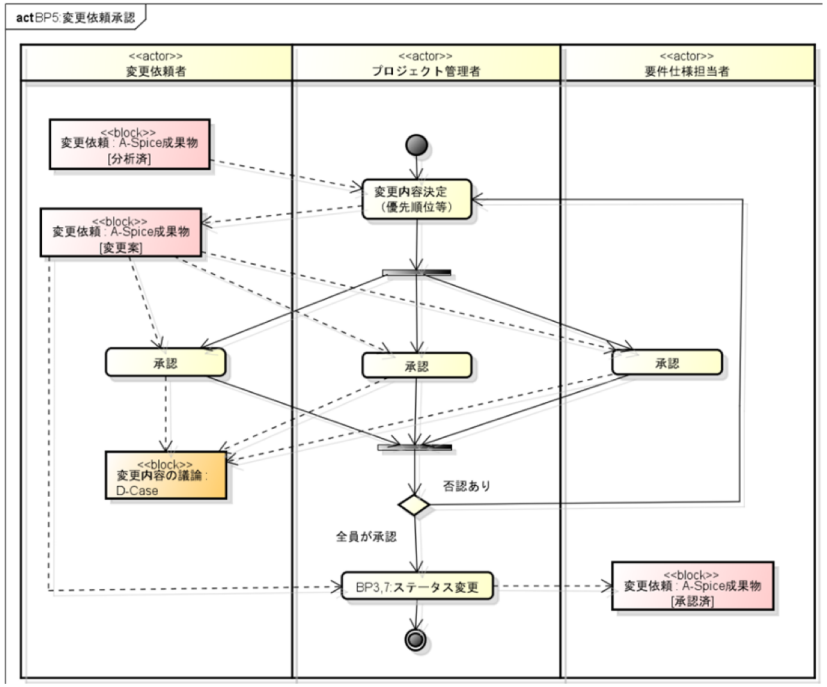
アクティビティ	変更依頼分析
アクター	サプライヤ：プロジェクト管理者、要件仕様担当者
内容	・サプライヤにおいて、要件仕様担当者が、変更依頼内容を分析し、変更の影響範囲や修正コストを算出する。 ・分析内容をサプライヤ内でレビューする。 ・レビュー内容はD-Case「分析結果の議論」として記録する。
A-SPICE成果物	SW要件定義書、変更制御記録
62853成果物	分析結果の議論

NTT DATA

06 アクティビティ図

Communication Art Technology Systems

変更依頼承認



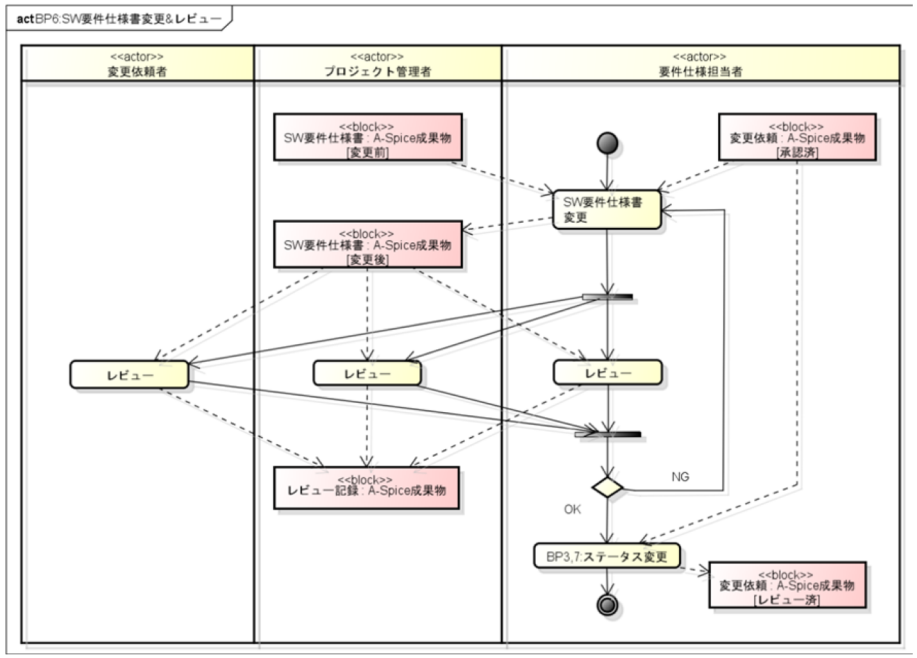
アクティビティ	変更依頼承認
アクター	OEM：変更依頼者 サプライヤ：プロジェクト管理者、要件仕様担当者
内容	・サプライヤにおいて、プロジェクト管理者分析内容に基づいて変更案を作成する。 ・変更案について、OEM、サプライヤでレビューを行い、承認する。 ・レビュー内容はD-Case「変更内容の議論」として記録する。 ・なお、この承認プロセスはA-SPICEにもともと存在するものである。
A-SPICE成果物	変更依頼
62853成果物	変更内容の議論

NTT DATA

06 アクティビティ図

Communication Art Technology Systems

SW要件仕様書変更&レビュー



アクティビティ	SW要件仕様書変更＆レビュー
アクター	OEM：変更依頼者 サプライヤ：プロジェクト管理者、要件仕様担当者
内容	・決定した変更内容に基づいて、サプライヤにおいて、変更を実施する。 ・実施した変更についてサプライヤ内でレビューを行う。 ・レビュー内容はA-SPICE成果物「レビュー記録」に記録する。
A-SPICE成果物	変更依頼、SW要件仕様書、レビュー記録

NTT DATA

07 課題

Communication Art Technology Systems

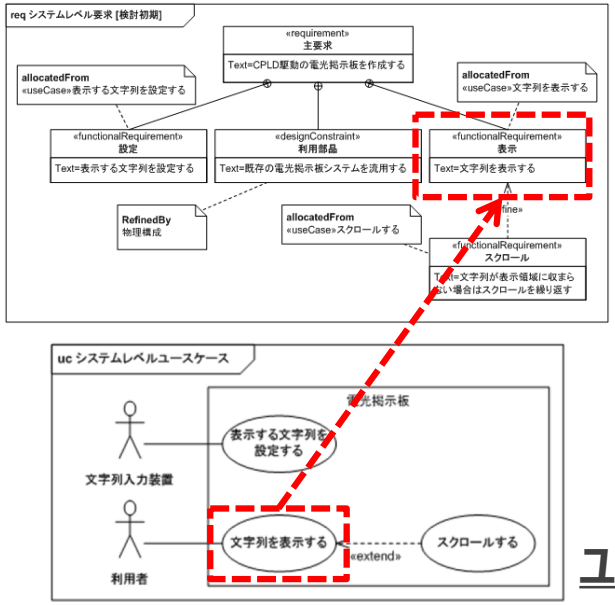
- アクターについて
  - アクターの役割と権限はクロスする関係にあり、単純な継承関係で表せない。
  - アクセスコントロールモデルとして体系化が必要。
- 成果物について
  - 成果物をGSNで表現することが考えらえれる。
  - 成果物とそれに至る過程の議論を統合してトレサビ管理しやすくする。
- D-Caseについて
  - ワークフローの中には意思決定や議論すべき個所が多数存在する。それらすべてをD-Caseで記述していると作業量が膨大となってしまう。D-Caseを記述する基準があるとよい。例）成果物内の各項目について1つのD-Caseを対応付けるなど。
  - また、D-Caseを記述する際、どの詳細度まで記述すればよいかも課題である。（議論を掘り下げすぎるとソースコードレベルの話になってしまう。）

NTT DATA

07 課題

- 現状、UMLで書いたモデルと変わらない。SysMLを生かした図が書けないか？
  - 要求図
    - IEC62853の要求を要求図で整理する。
    - ブロック定義図やアクティビティ図の要素との関係を定義する。(allocation)
  - コンポーネント図
    - D-ADDは System of Sytemsとみなせる。
    - ４つのプロセスを実現するシステムのインターフェースをコンポーネント図で表し、それらの呼び出し関係をアクティビティ図やシーケンス図で表す。

要求図



ユースケース図

コンポーネント図

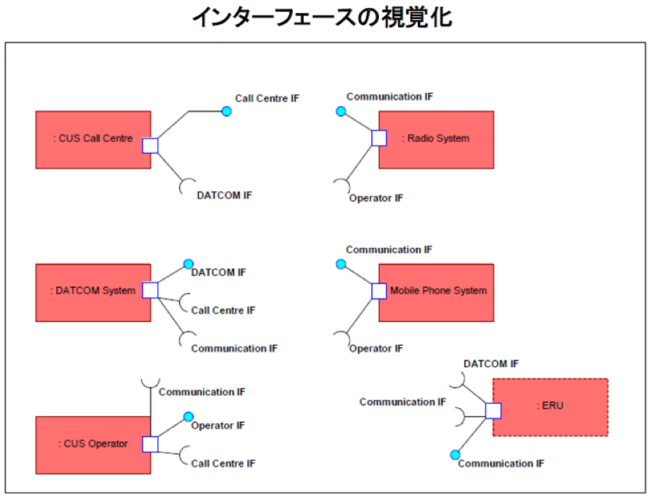
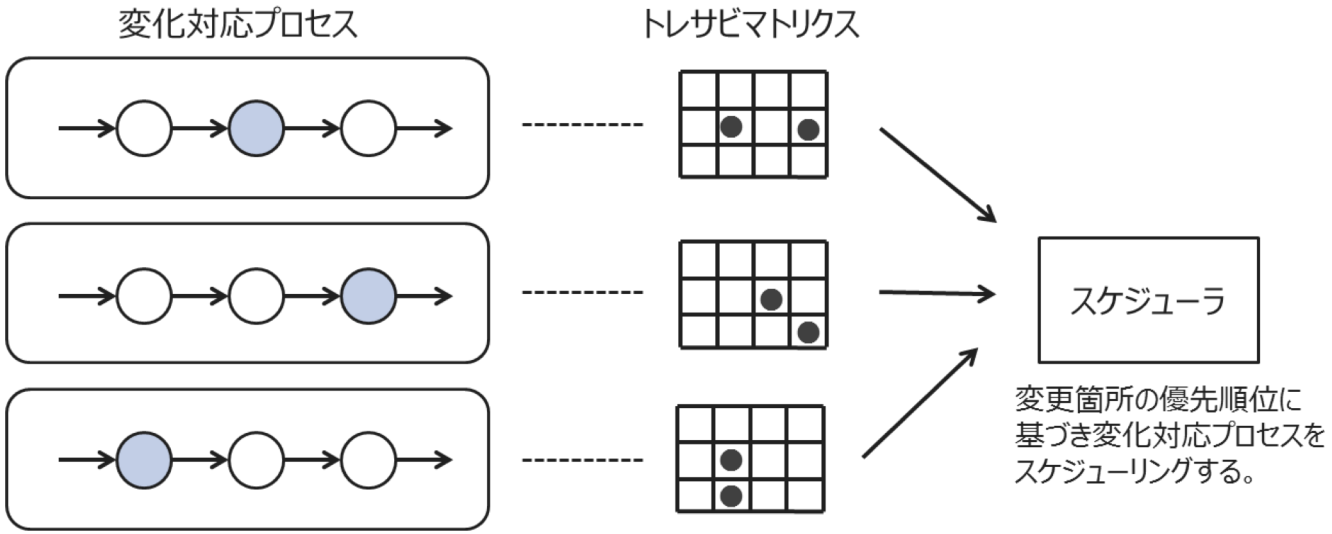


図 15-B-1-2　SOS 緊急応答システムの視覚化（インターフェースの視覚化）の例

07 課題

Communication Art Technology Systems

- 変化対応プロセスの並列実行
  - 複数の変更が同時に起こる場合、変化対応プロセスを並列実行する必要がある。
  - 変更箇所が干渉する場合、各プロセスが無計画に実行させると整合性がとれなくなる可能性。
  - トレサビマトリクスなどに基づいて適切にスケジューリングする必要がある。
  - ➔ ペトリネットでモデル化（神奈川大 木下様、武山様）



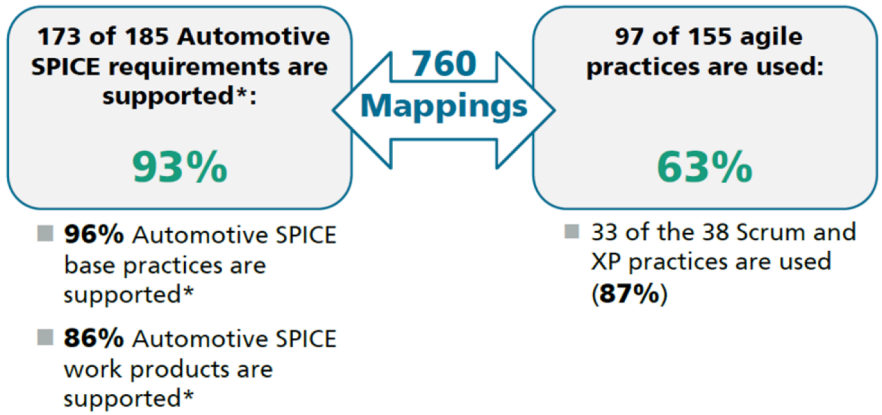
NTT DATA

08 関連研究

Communication Art Technology Systems

- 本研究の応用としてIEC62853をA-SPICEやISO26262にマッピングさせることが考えられる。
- 国際規格とアジャイルのマッピングに関する資料
  - “CMMI or Agile Why Not Embrace Both!”, H. Glazer, 2008.
    - アジャイルとCMMIの共存により開発効率を大幅に改善できる。
  - “How Do Agile Practices Support Automotive Spice Compliance?”, P. Diebold, 2017.
    - A-SPICEとアジャイル（Scrum,XP）の対応関係を調査。
  - “Agile in Automotive Pocket Guide”, Kugler Maag, 2017.
    - A-SPICEにおいてアジャイルを導入するためのガイド。

Name	Agile Method	Processes (BPs)															WPs	BP & WP
		ACQ.4	SYS.1	SYS.2	SYS.3	SYS.4	SYS.5	SWE.1	SWE.2	SWE.3	SWE.4	SWE.5	SWE.6	SUP.1	SUP.8	SUP.9	SUP.10	MAN.3	Total	Total	Total
Backlog	SCRUM																		47	14	61
Burn Chart	SCRUM																		9	2	11
Code and Test	XP																		4	2	6
Collective Ownership	XP																		7		7
Continuous Deployment	XP																		6	2	8
Continuous Integration	XP																		12	4	16
Daily Meeting	SCRUM																		12	5	17
Definition of Done	SCRUM																		17	8	25
Impediments	SCRUM																		11	8	19
Incremental Design	XP																		4	3	7
Iterative development	SCRUM																		1	4	5
Metaphor	XP																		3	1	4
Negotiated Scope	XP																		2		2
On-site customer	XP																		13	1	14
Open Workspace	XP																		9		9
Pair Programming	XP																		5	1	6
Pay-per-Use	XP																				
Planning Game	XP																		5		5
Planning meeting	SCRUM																		17	8	25
Product Owner	SCRUM																		28	2	30



NTT DATA

09 まとめ

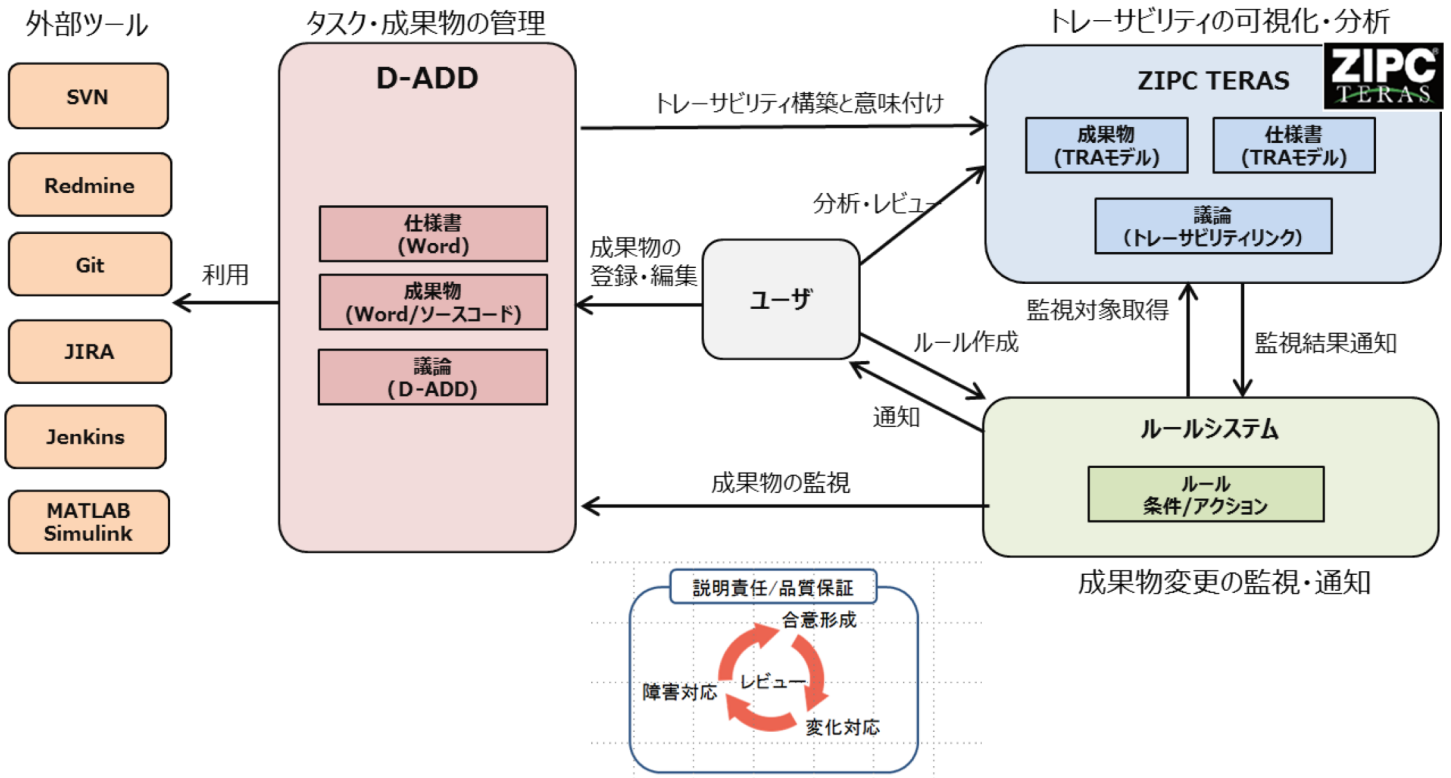
Communication Art Technology Systems

- A-SPICEとIEC62853による自動車制御システム開発のためのディペンダビリティプロセスの構築。
  - プロセスの理解容易化のため、SysMLのブロック定義図とアクティビティ図によりモデル化を行った。
- 今後の課題
  - ワークフロー内の各処理がどのようにツールで実現できるかを検討し、D-ADDのツール要件を明らかにする。

D-ADDによるツール支援

01 D-ADDによるツール支援

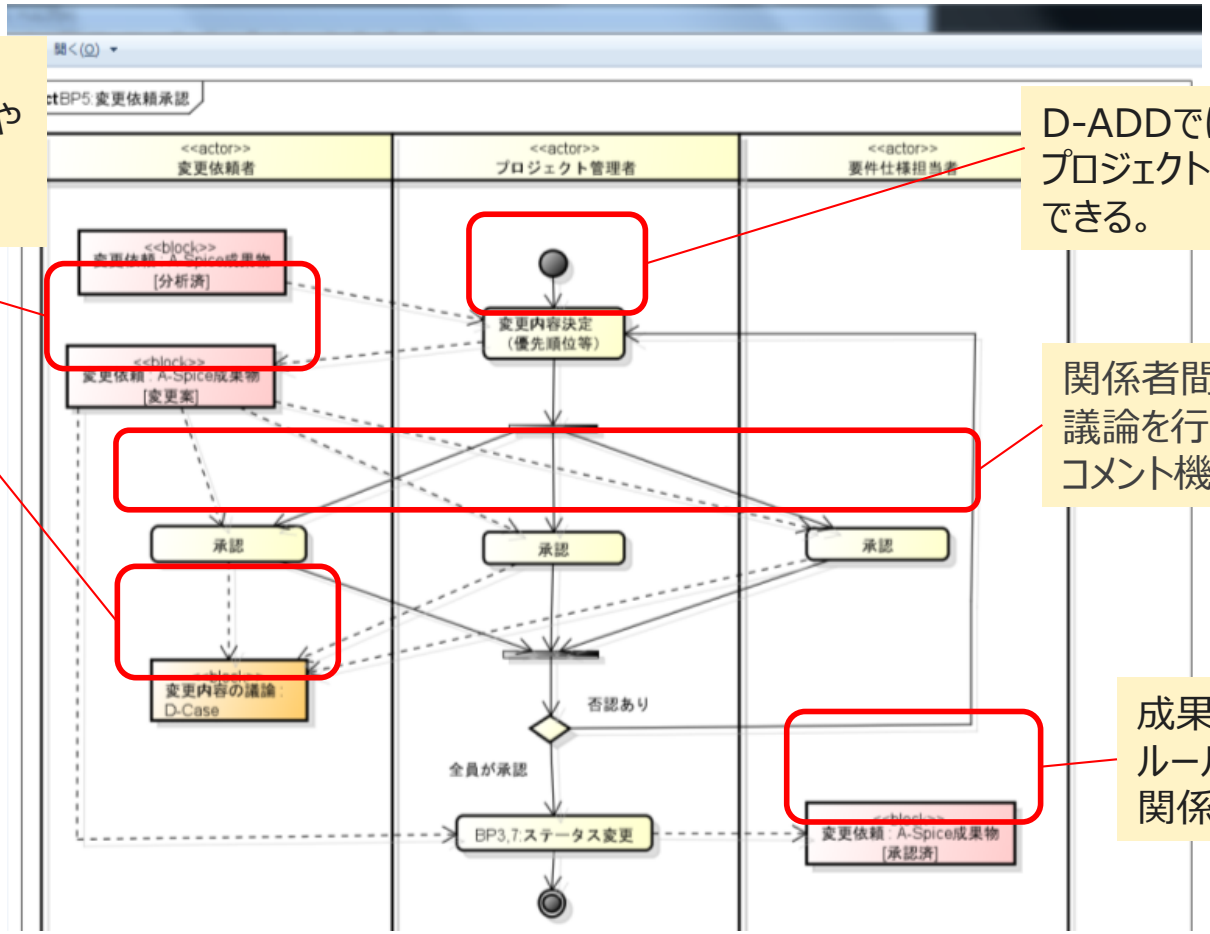
- IEC62853プロセス実行に対するツール支援として、D-ADDとZIPC TERASによる支援環境を構築・検討している。
  - D-ADD：合意記述データベース（Symphony）
  - ZIPC TERAS：トレーサビリティ管理ツール（CATS）
- D-ADDとZIPC TERAS連携では、レビュー駆動を提唱し、品質保証の観点からレビューとトレーサビリティの観点を突き詰める。



02 アクティビティ図との関連

- アクティビティ図で定義したディペンダビリティプロセス内の各処理をD-ADD、ZIPC TERASで支援することができる。
  - プロジェクト・タスク管理、コメント機能、トレサビ管理、変更通知など。

ZIPC TERASでは、
成果物間のトレサビ構築や
レビュー進捗の可視化を
行うことが可能である。



D-ADDでは、プロセス内の各処理を
プロジェクトやタスクとして管理することが
できる。

関係者間で成果物のレビューや
議論を行う際には、D-ADDの
コメント機能を利用することができる。

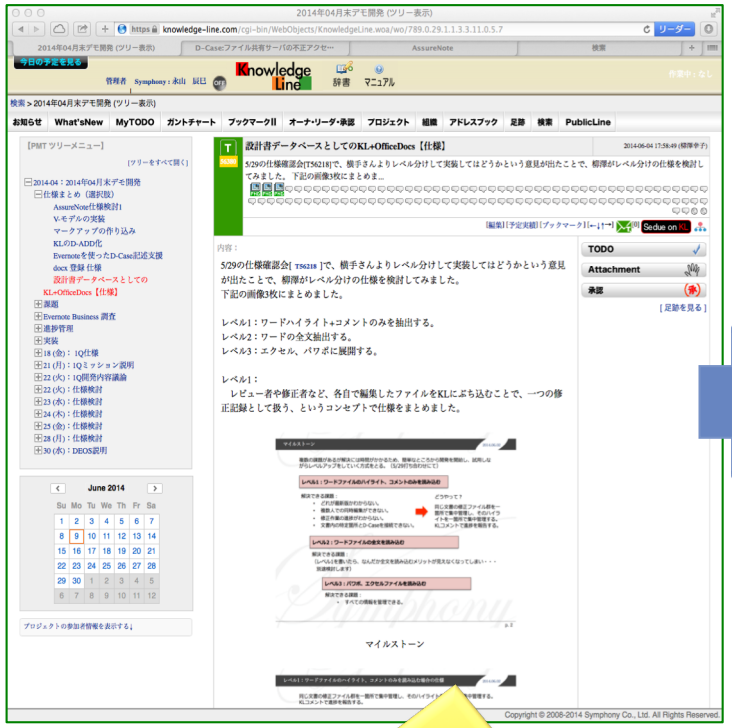
成果物に変更があった際には、
ルールシステムがそれを検知し、
関係者に通知する。

03 D-ADDのコメント機能

Communication Art Technology Systems

- D-ADDでは、コメント欄で議論を行い、議論の構図をグラフ表示することが可能。

タスク管理画面

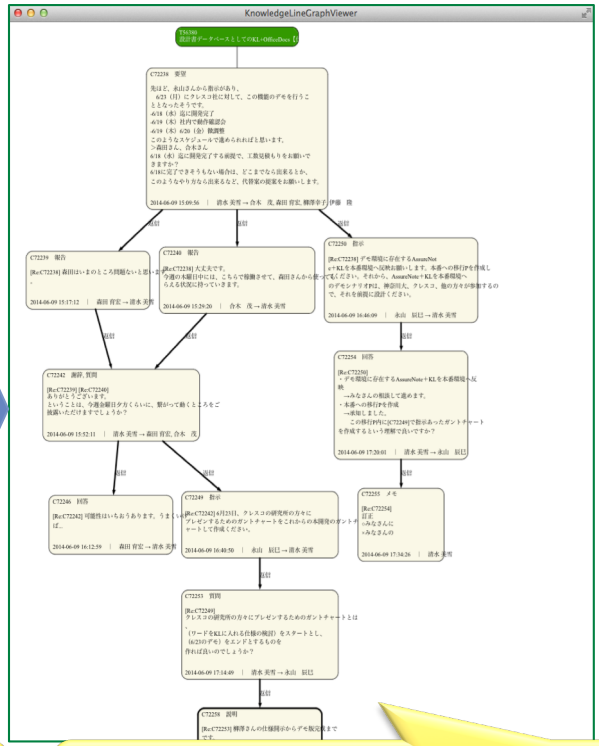


合意すべき内容のコンテンツ

コメント欄

コメント欄による合意記述
（主張、反論、証拠、関連、裏付け）

合意グラフ



コメント履歴から合意グラフの生成
（ツールミンモデル）

Communication
Art
Technology
Systems

NTT DATA
Global IT Innovator