

消費者機械に関する安全規格に対するメタモデリングによるアプローチ

田口研治

Ph.D (Computer Science)

招聘研究員

産業技術総合研究所

オリジナルスライドは以下のセミナーにおいて発表された

*OMG Seminar on Systems Assurance & Safety
For Consumer Devices, 2011 June 22*

本日の話

- **目的**
 - **新たな機能安全規格を作るとしたら、何が出来、何をすべきか？**
- **モデリングの観点から見た国際規格**
 - **形式手法や準形式手法によるアプローチ**
 - **例:WSDL (W3C) の仕様記述言語 Z による記述**
 - **メタモデルを用いるアプローチ**
 - **二つのショーケース**
 - **ISO/IEC 15408 におけるセキュリティの概念**
 - **ISO/FDIS 26262 における安全性の概念**
- **結論**

目的

- **消費者機械に関する機能安全規格の提唱が大畠氏(トヨタ)からされている。**
- **その規格を OMG の System Assurance TF で行おうとしている。**
- **OMG においてはメタモデルを用いた規格化が主である(例: UML)**
- **機能安全の規格を本当に OMG で策定可能であろうか？**
- **その答えの一片を示すのが本講演の目的である。**

規格における準形式手法／形式手法によるモデル化

規格におけるモデリングの観点

- **曖昧性の排除**
 - 準形式手法／形式手法の利用
 - 形式手法が利用されている例
 - **メタモデル (in UML)**
 - **OMG において広く適用**
- **質問**
 - **規格のモデル化が効率的かつ有効に行われるのか？**
 - **予算に釣り合うのか？**
 - **どのような効用があるのか？**

WSDL

- WSDL (Web Services Description Language) by W3C
 - *WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information.*
 - Formally specified in Z and type checked by a tool.
 - *the conceptual model of WSDL 2.0 as a set of components with attached properties, which collectively describe a Web service.*

ComponentModel1

components : \mathbb{P} *Component*

componentIds : \mathbb{P} *ID*

$\forall x, y : \text{components} \bullet$

$\text{Id}(x) = \text{Id}(y) \Rightarrow x = y$

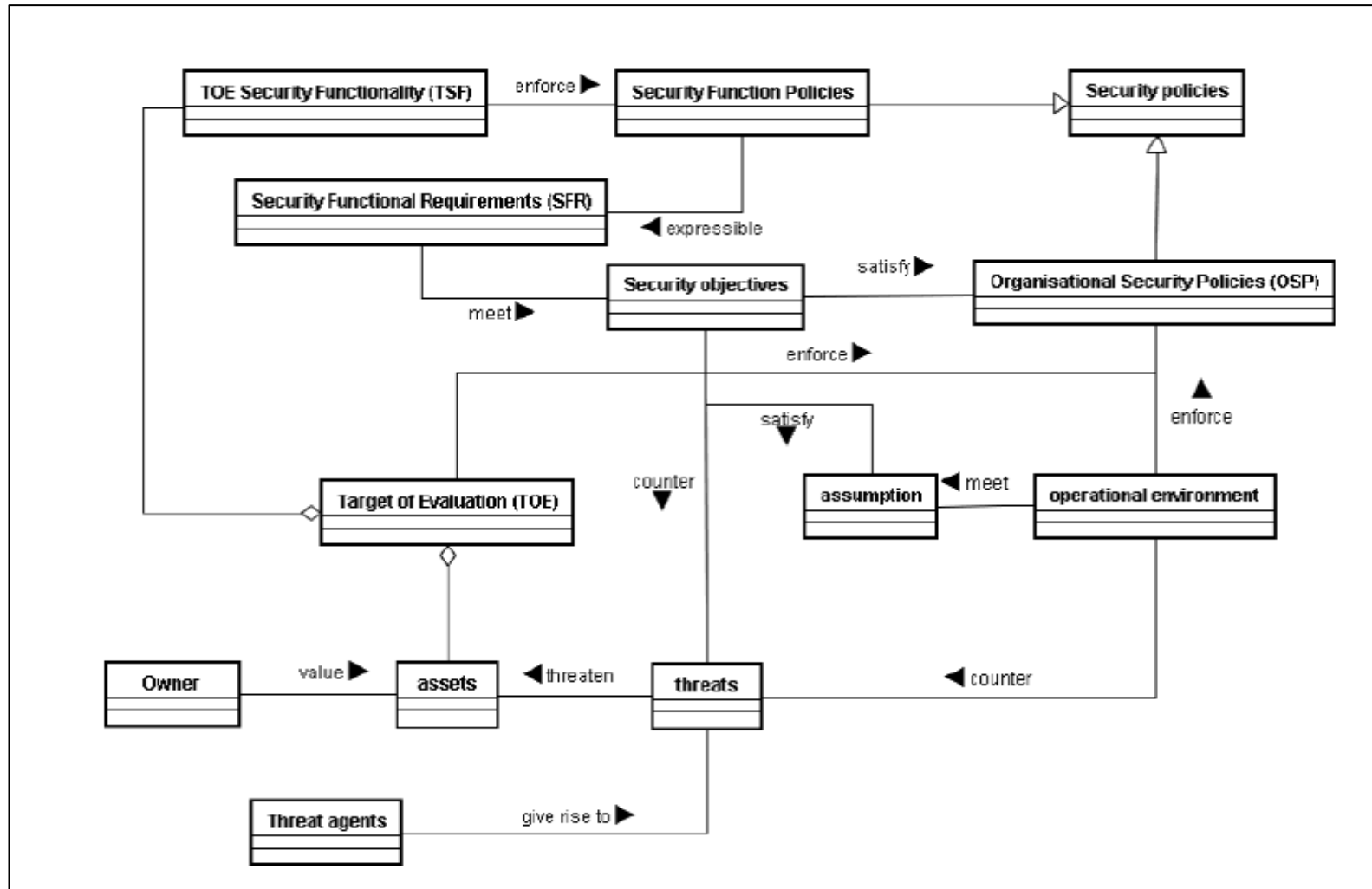
$\text{componentIds} = \{ x : \text{components} \bullet \text{Id}(x) \}$

セキュリティ規格に対するメタモデリングによるアプローチ

Common Criteria (ISO/IEC 15408)

- International standard for security assurance and evaluation for IT products
- A huge number of IT products ranging from OS to smart cards are certified under this standard
- Government agencies and companies mandate the use of IT products certified under the CC (Common Criteria)
- CC consists of Part1 ~ Part3 and CEM (Common Evaluation Methodology),
 - Part 1 (Introduction and general model)
 - Part 2 (Security functional components)
 - Part 3 (Security assurance components)
- A simple diagram is provided to illustrate security concepts used in the standard. **However there is no formal/semi-formal specification as to how underlying concepts are related to each other.**

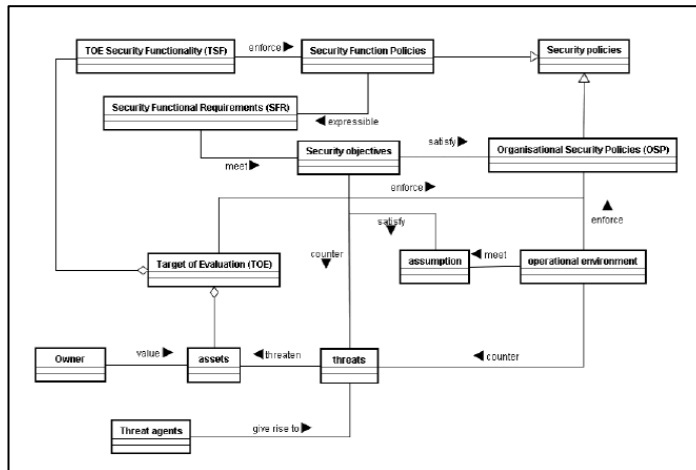
CC におけるセキュリティ概念のメタモデル



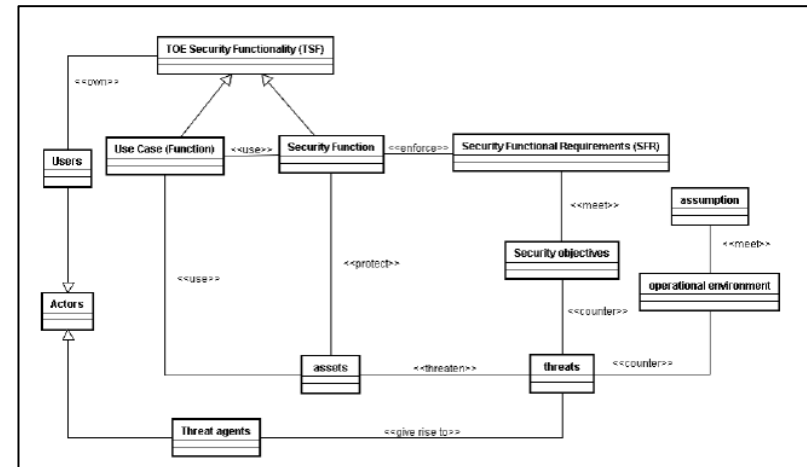
(K. Taguchi, et. al., "Aligning Security Requirements and Security Assurance using the Common Criteria", IEEE SSIRI 2010, pp69-77)

メタモデルに基づいた脅威分析方法論

(1) CC におけるメタモデル記述

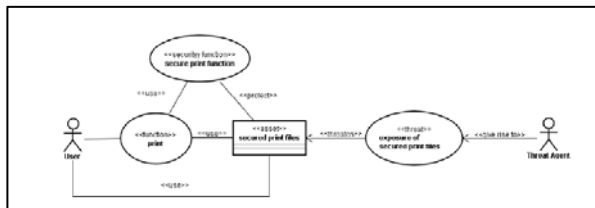


(2) (1) から導出されたモデル化のための枠組み

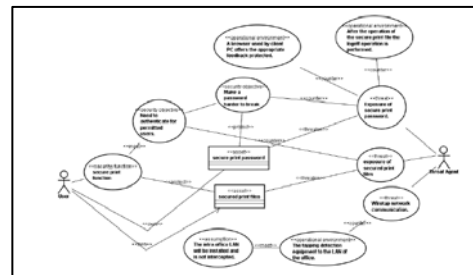


(3) 図式表現と記述のためのプロセス

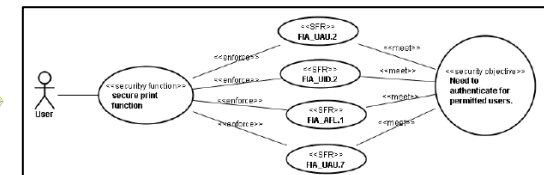
Step 1.



Step 2.



Step 3.



Step 1.

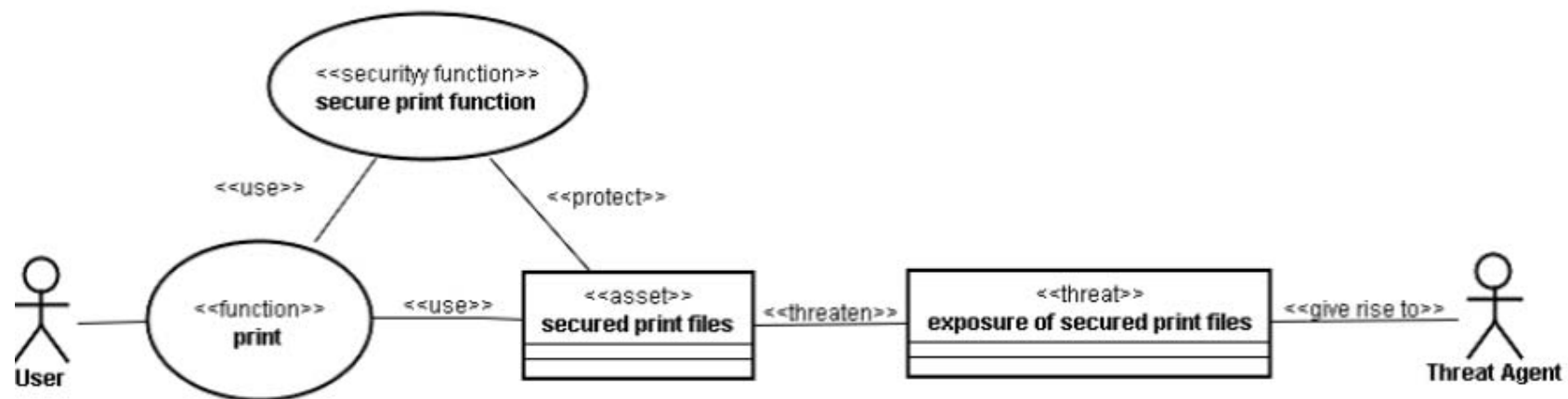


Figure 4. MFP in Phase 1.

- 1: What should be protected is elicited as assets,
- 2: Identify potential threats against assets,
- 3: Identify security function which effectively protect assets from the threats.

機能安全規格に対するメタモデルによるアプローチ

Functional Safety Standards


- **IEC 61508** is a functional safety standard for electric and electronic devices, but there are other standards specifically focused on some particular industrial sectors.
 - Automotive Embedded Systems
 - **ISO/FDIS 26262**, Road Vehicles –Functional safety
 - Control Systems for Railway
 - **CENELEC EN 50128**, Railway Applications: Software for Railway Control and Protection Systems
 - **IEC 62278**, Railway Applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)
 - Avionics Software
 - **DO-178B**, Software Considerations in Airborne Systems and Equipment Certification

ISO/FDIS 26262

ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of E/E systems within road vehicles.

This adaptation applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic, and software elements that provide safety-related functions.

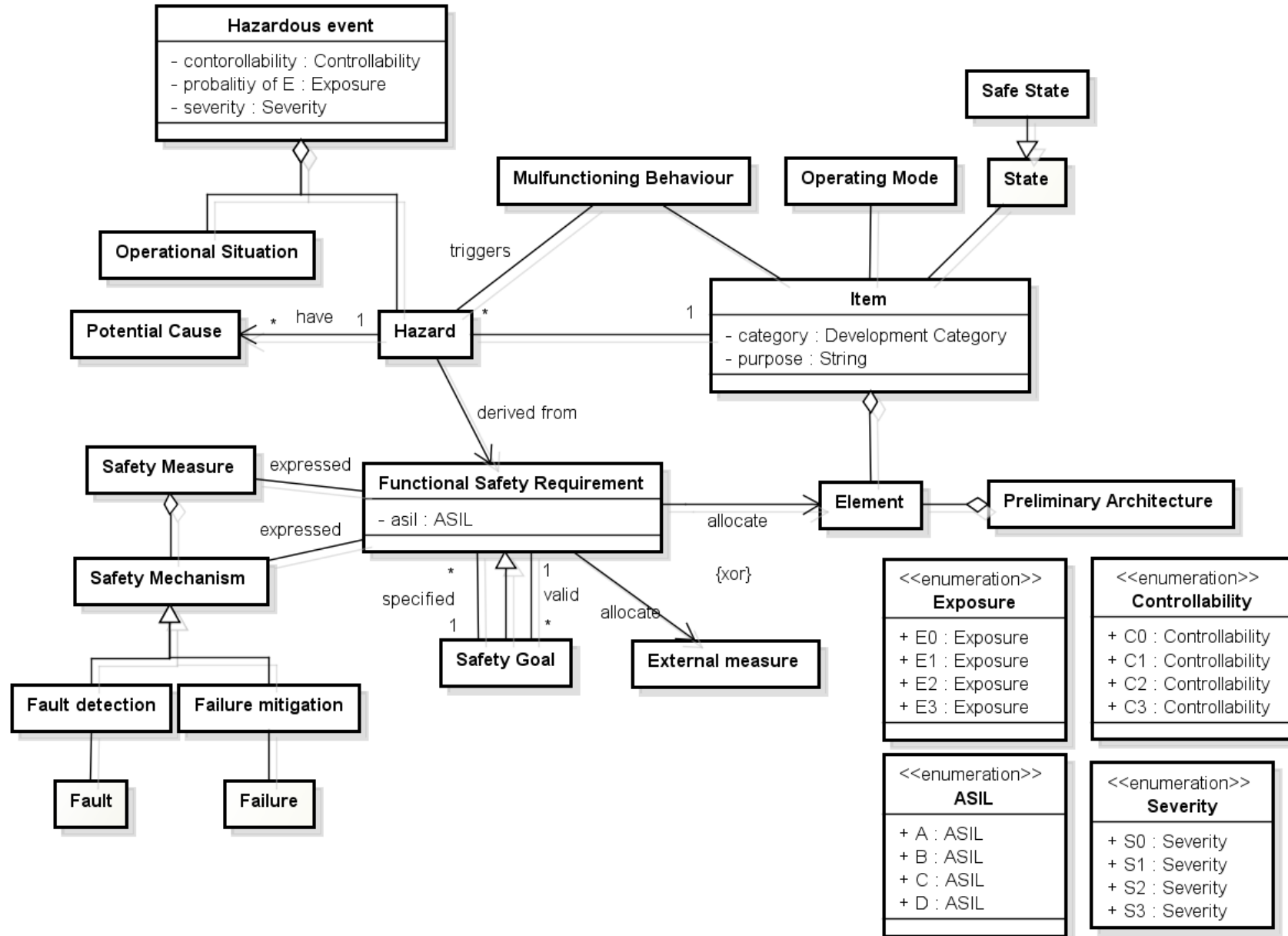
Target of meta-model

- *Part 1: Vocabulary*
- *Part 2: Management of functional safety*
- ***Part 3: Concept phase*** 
- *Part 4: Product development: system level*
- *Part 5: Product development: hardware level*
- *Part 6: Product development: software level*
- *Part 7: Production and operation*
- *Part 8: Supporting processes*
- *Part 9: ASIL-oriented and safety-oriented analyses*
- *Part 10: Guideline on ISO 26262*

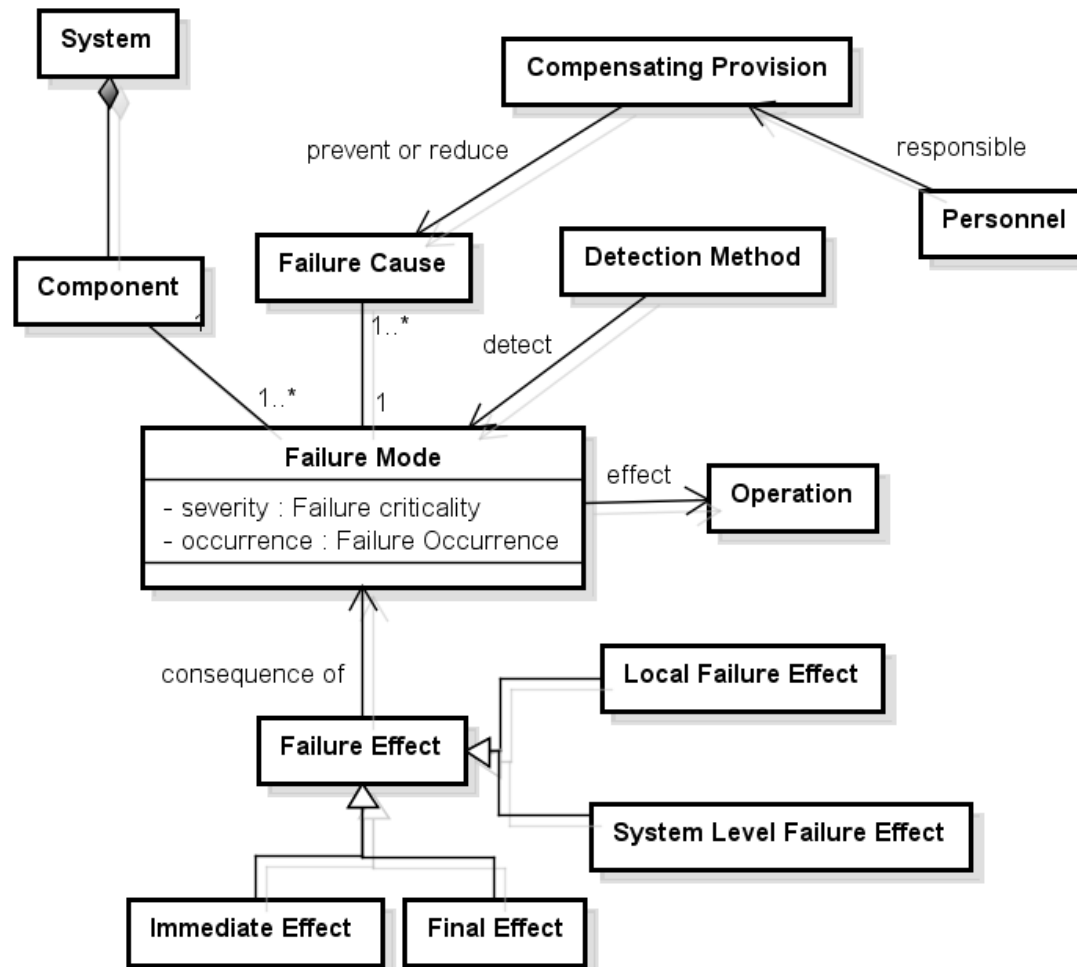
Part 3 ISO/DIS 26262 Process

- Following process is defined in the standard
 - Item Definition
 - Initiation of the safety lifecycle
 - Hazard analysis and risk assessment
 - Functional safety concept
- In addition to the process, the meta-model for the underlying conceptual model is specified in UML.

ISO/FDIS 26262 Safety concept Meta-model

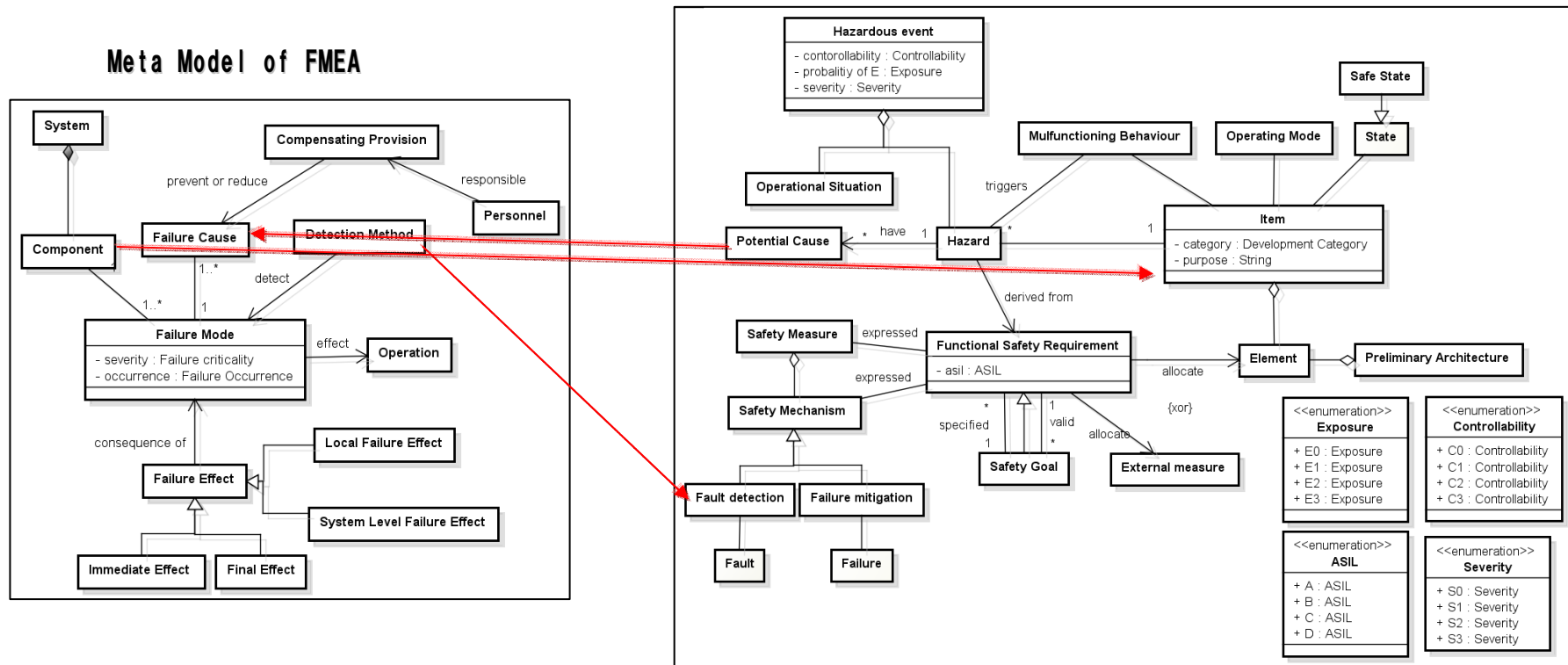


FMEA (Failure Mode and Effects Analysis) Meta-model



IEC 60812, "Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)", edition 2.0, 2006-01 (2006)

Correspondence Between Safety Concepts in ISO 26262 and FMEA



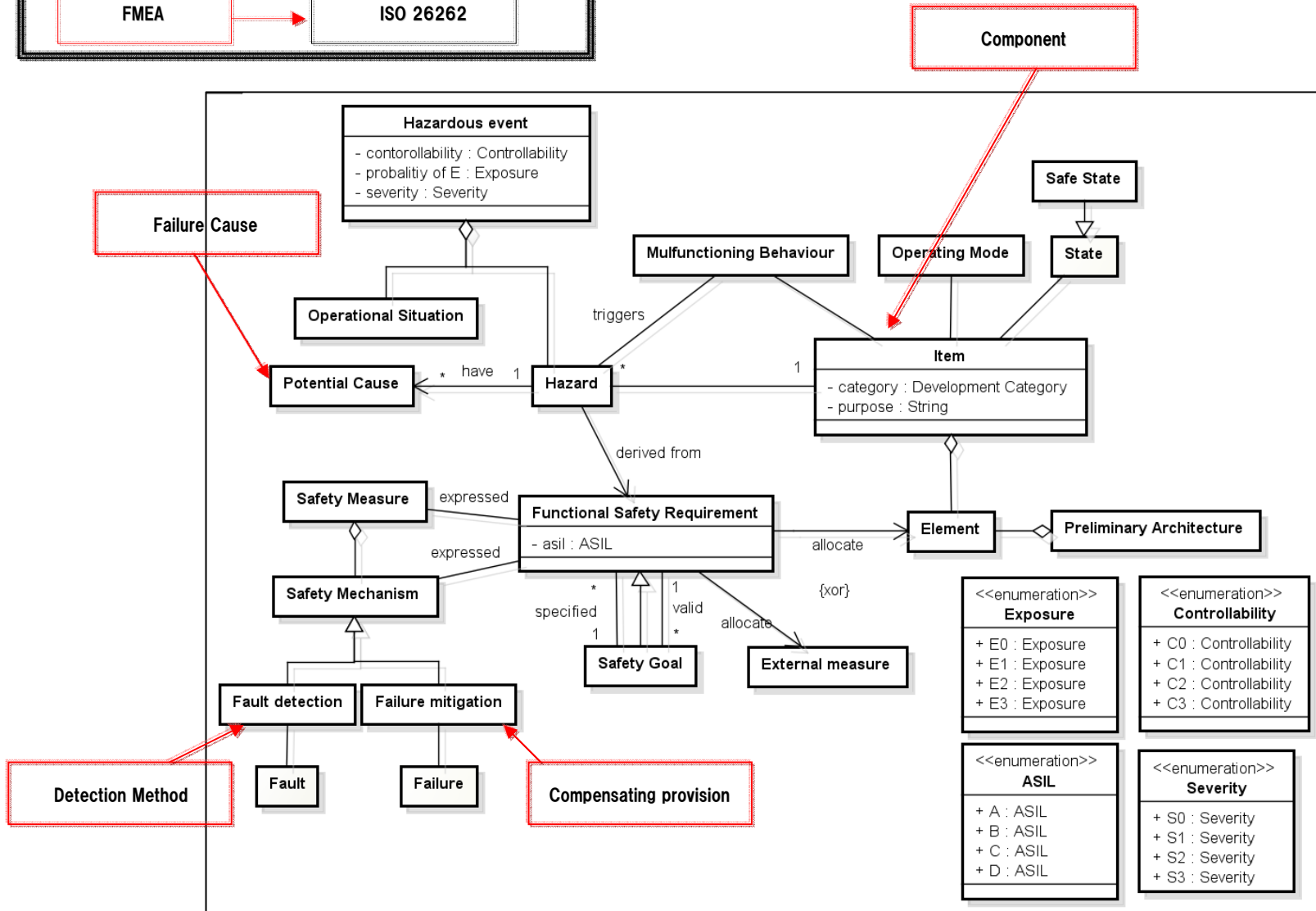
Correspondence between the two meta-model can be determined by the definitions of concepts.

Aligning Two Standards

Explanation :

FMEA

ISO 26262



Pros and Cons of Meta-Modeling Approach

- Pros
 - Increase understandability (avoid misunderstanding), which enhance mutual understanding of the underlying concepts/conceptual frameworks,
 - Easy to design supporting tools and build tool chains,
 - as long as everything is defined as meta-models.
 - E.g., EAST-ADL2 (ATTEST Project)
- Cons
 - Still ambiguity remains.

Only structural relationships between concepts are defined.
 - Specifying every detail of a standard in meta-models is costly

Concluding remarks: Moving forward, where?

- Meta-modeling approach is promising and feasible, even effective for a functional safety standard.
 - Provides certain degree of rigor to a standard.
- Some additional remarks
 - Great opportunity to improve/enhance existing functional safety standards,
 - Safety concepts could be refined,
 - Improvement of safety analysis methods
 - Incorporates results of system assurance TF into the standard.
 - Standardization of safety/assurance cases

**ツールP/Fを中心とした新たな
組込み開発環境の構築に関するご紹介**
TERAS
Tool Environment for Reliable and Accountable Software

**キャッツ株式会社
プロダクト事業本部**

一般社団法人TERASとは

- ▶ 設立 2011年4月7日
- ▶ 目的(定款第3条)

当法人は、ソフトウェア開発環境の研究・開発ならびにこれらの標準化及び信頼性・安全性等の評価を含む実用化の促進等を行うことにより、我が国の組込みシステム産業及び組込みシステム産業に係る製造業の振興を図り、もって我が国経済の発展に寄与することを目的とし、その目的に資するため、次の事業を行う。

- ▶ 取組

1. 日本の開発スタイルに適した国産開発ツールを開発
2. 国際標準化活動
3. ツールベンダーの海外進出
4. ユーザのグローバル開発の支援
5. 付加価値の高いソフトウェア業務への転換



参照 経産省「組込みソフトウェア産業活性化プラン」平成21年6月11日

経済産業省 オープンツールプラットフォーム構築事業



経済産業省
Ministry of Economy, Trade and Industry

[本文へ](#) [English](#)



[トップページ](#) | [経済産業省について](#) | [政策別を探す](#) | [組織別を探す](#) | [窓口一覧](#) | [ご意見・お問合せ](#)

[トップページ](#) > [調達・予算執行](#) > [採択結果一覧](#) > 平成23年度「産業技術実用化開発事業費補助金(組込みシステム基盤開発事業(品質説明力向上に向けたオープンツールプラットフォーム構築事業))」に係る交付先の採択結果について

平成23年度「産業技術実用化開発事業費補助金(組込みシステム基盤開発事業(品質説明力向上に向けたオープンツールプラットフォーム構築事業))」に係る交付先の採択結果について

平成23年6月15日
商務情報政策局
情報処理振興課

平成23年度産業技術実用化開発事業費補助金(組込みシステム基盤開発事業(品質説明力向上に向けたオープンツールプラットフォーム構築事業))の交付先について、平成23年4月27日～5月30日の期間をもって公募を行ったところ、期間内に1件の応募がありました。応募のありました提案について、外部の有識者による審査委員会において審査を行った結果、下記の応募者を交付先として決定いたしましたので、お知らせいたします。

採択事業者

一般社団法人 TERAS

問い合わせ先

商務情報政策局情報処理振興課 担当 古川

電話: [03-3501-2646](tel:03-3501-2646)

FAX: 03-3580-6073

[このページの先頭へ](#)

<http://www.meti.go.jp/information/data/c110615bj.html>

背景と課題

日本の組込み開発を取り巻く環境

日本の組込み開発のあり方は、大きな変革の局面を迎えている

日本の組込み産業を取り巻く環境変化

- 品質・安全に関する法規制・規格・世論の厳格化



- ソフト工学技術の進化
- 実装工程の機械化と海外アウトソーシング拡大



- 技術/産業間のコンバージェンス・他システムとの統合化進展



- 開発拠点のグローバル化進行
 - 市場の海外シフトに伴う現地ニーズ対応強化
 - リーマンショック後の円高対応
 - 設計情報の機密管理



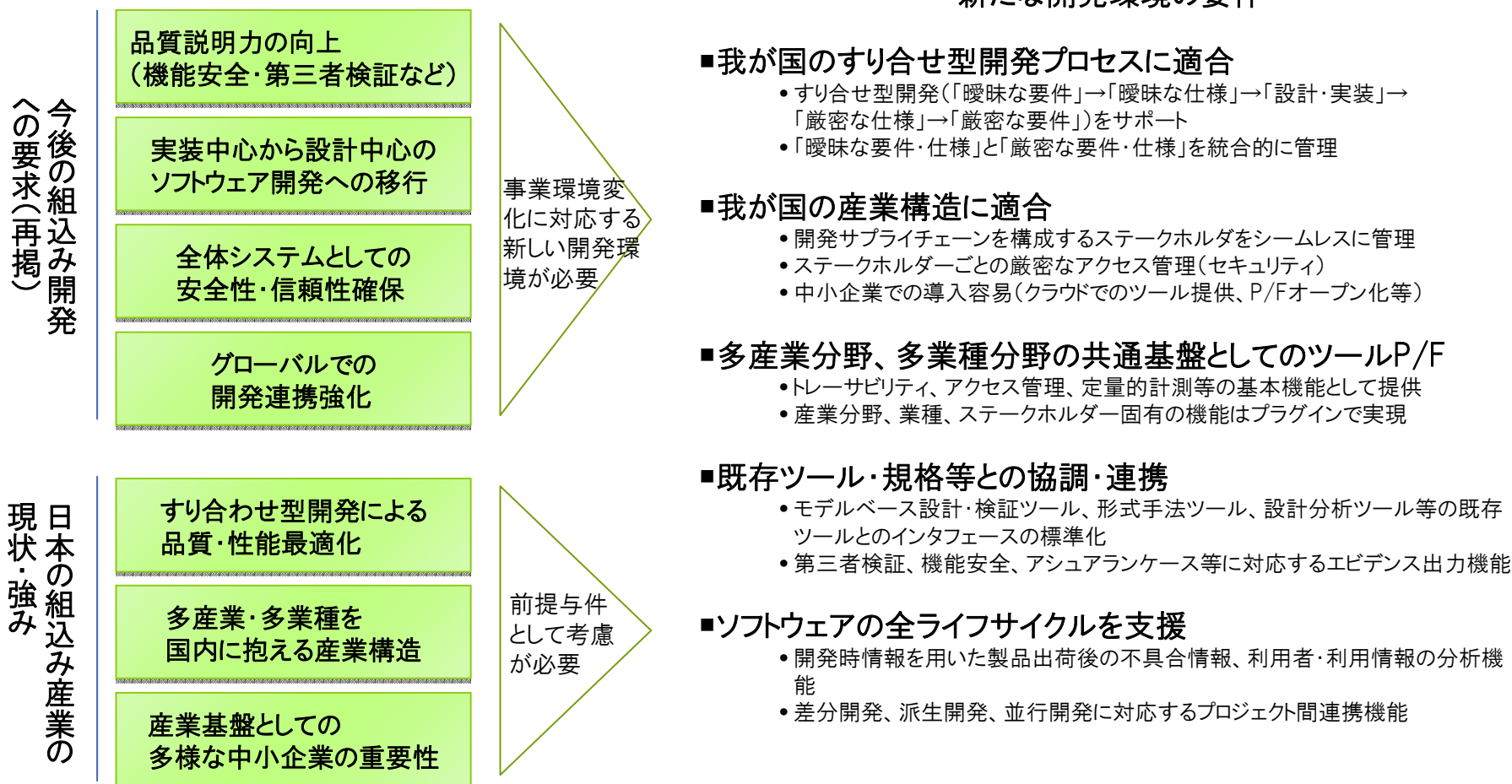
今後の組込み開発への要求

<p>品質説明力の向上 (機能安全・第三者検証など)</p>	<ul style="list-style-type: none"> 製品の“本質的品質”のみならず“説明品質”を果たすためのトレーサビリティ担保が必須の環境に <ul style="list-style-type: none"> - 機能安全、第三者検証に対応した開発情報管理 - 開発に使用する開発ツールの認証取得 - 説明力(証明力)の高い開発技術の適用 など
<p>実装中心から設計中心のソフトウェア開発への移行</p>	<ul style="list-style-type: none"> 国内での開発は上流工程中心にシフト 上流工程の中核技術はモデルベース(モデル駆動)開発技術 開発プロセスのモデルベース開発への適応(上流工程での設計検証など)
<p>全体システムとしての安全性・信頼性確保</p>	<ul style="list-style-type: none"> スマートエネルギー、ITSなど産業をまたぐ統合システムにおける全体システムとしての安全性・信頼性の確保 <ul style="list-style-type: none"> - 共通モデル、相互変換可能なモデルによる上流段階での検証など
<p>グローバルでの開発連携力強化</p>	<ul style="list-style-type: none"> グローバル展開された開発拠点における連携の強化・情報共有化推進による品質確保・生産性向上 開発体制の変化(垂直統合型集中開発→水平分業型分散開発) 今後、国内の開発リソース需要は減少(特にソフトウェア実装・テストの外部委託は海外移転と自動化などにより国内市場は消滅) グローバル開発における設計情報の機密管理体制の強化

背景と課題

今後求められる開発環境の考え方

事業環境変化への対応に向けて、日本ならではの強み・特長も十分に考慮した開発環境の整備を進め、日本の組み込み産業基盤強化を支援していくことが必要。



背景と課題

本活動を通じて目指す姿

新たな開発環境の構築を通じ、消費者・産業界共にwin-winとなる状態を目指す。

安心・安全な消費環境の形成

- 品質・安全性が保証された製品を安心して購入できる環境
- 購入後、他製品と連携/混合させた場合も安全性が保証される環境
- 透明性の高い製品情報を容易に掌握できる環境



事業環境変化への対応力強化を通じた国際競争力維持・向上

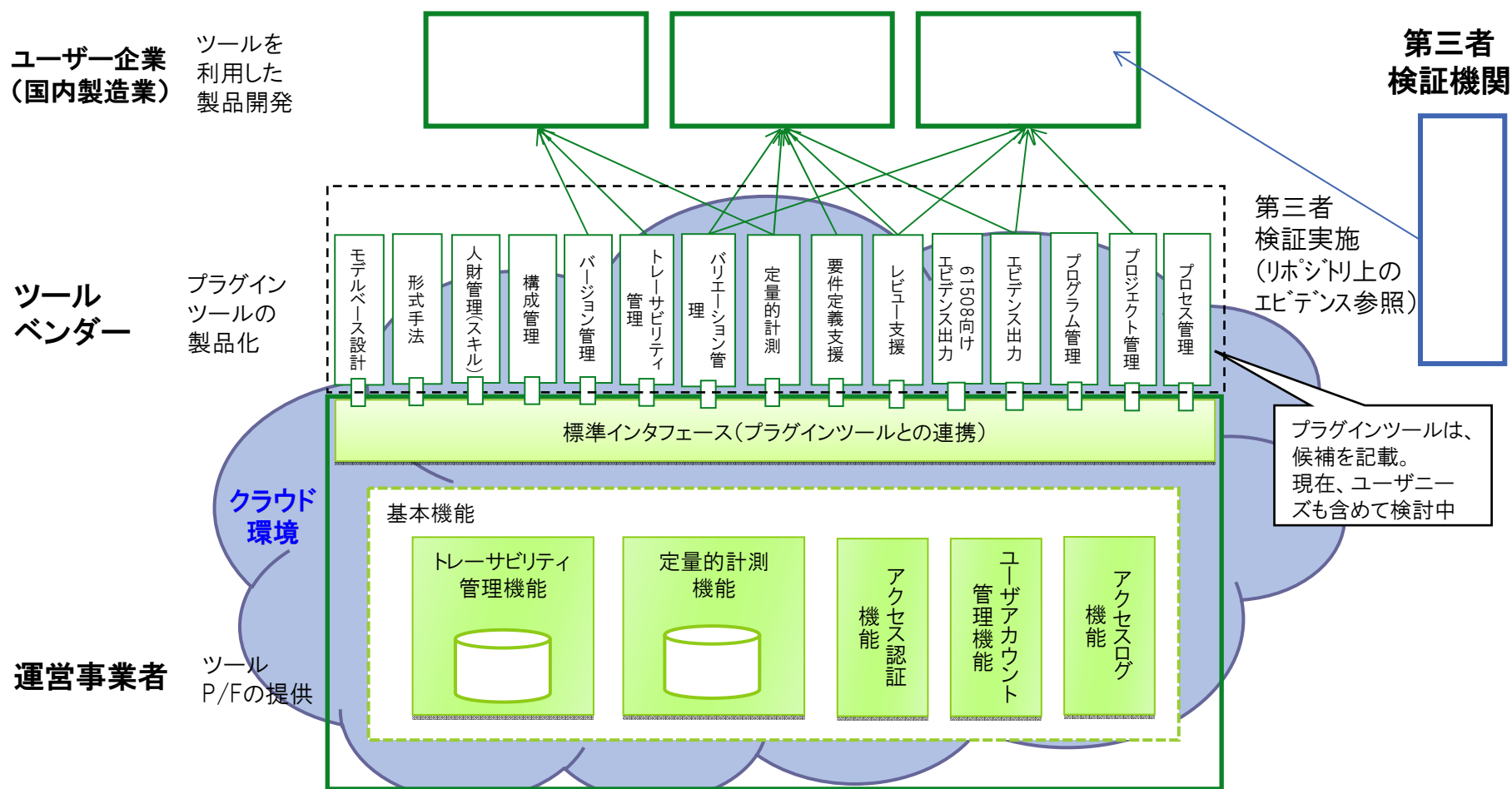
- トレーサビリティ担保による説明品質力強化
- グローバル各開発拠点における均一な開発環境の獲得
- 最先端のツール群を利用した効率的な開発への移行
 - ツール導入負担適正化
 - 必須だが稼働率が低く高価なツールの適用の容易化
- バックグラウンドサービスによるプロジェクト支援
 - リアルタイムなPJ進捗管理(EPM)
 - 認証取得に必要な技術活動記録の自動取得 など
- ソフトウェア資産管理と開発情報管理の厳格化
 - ソフトウェアの不正利用防止
 - 設計情報や評価情報の事故発生後の改竄の防止 など
- 大規模災害に対する安全保障(設計情報の保全)

ツール産業基盤・ビジネス機会の拡大

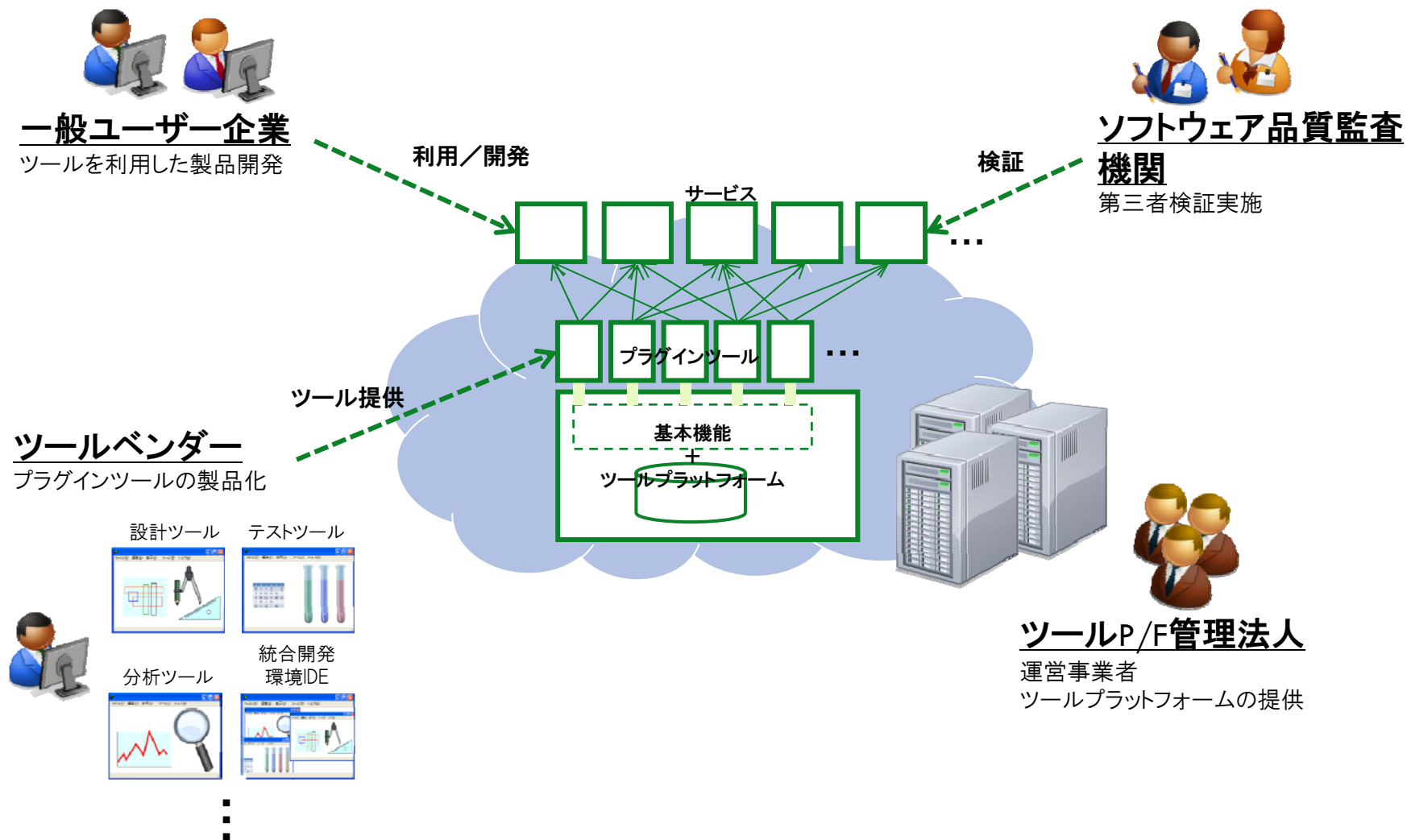
- ツール市場の拡大、新規参入機会の増大
 - 従来顧客と成りえなかった中小企業市場、グローバル市場
 - 教育研修での活用拡大によるツールを取り扱える技術者の増加
- ツール利用状況などのユーザ情報を活用した製品力・事業力の強化
- ツールを活用したサービス事業への展開
- バグ対応など保守業務の効率化、ライセンス管理の厳正化 など

オープンツールプラットフォームイメージ

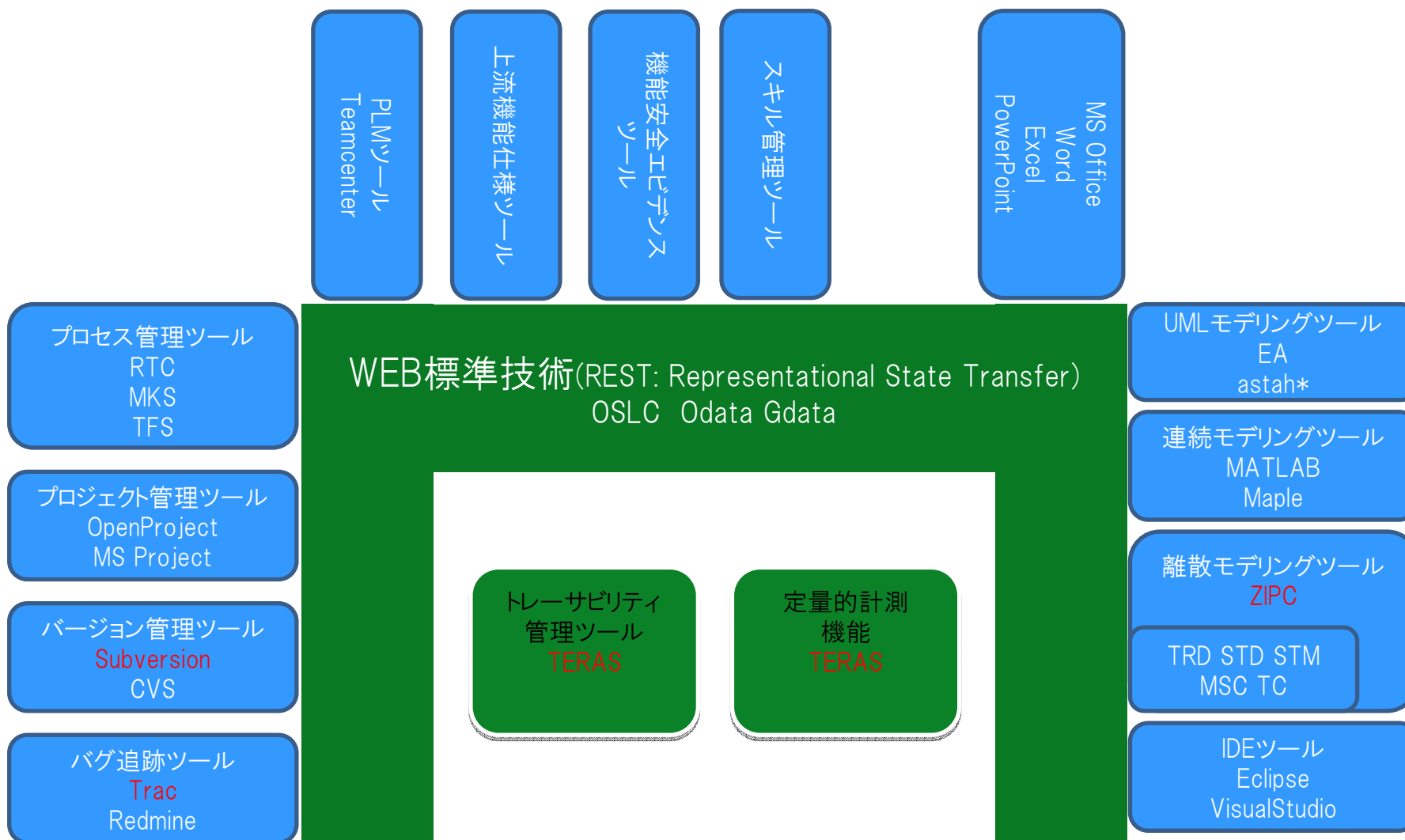
クラウド上でツールチェーンP/Fならびにプラグインツールが提供される環境を形成することで、ユーザー企業においては、説明品質の向上と最新ツール機能利用促進の効果を期待すると共にツール産業の活性化にも寄与する事業環境を形成する。



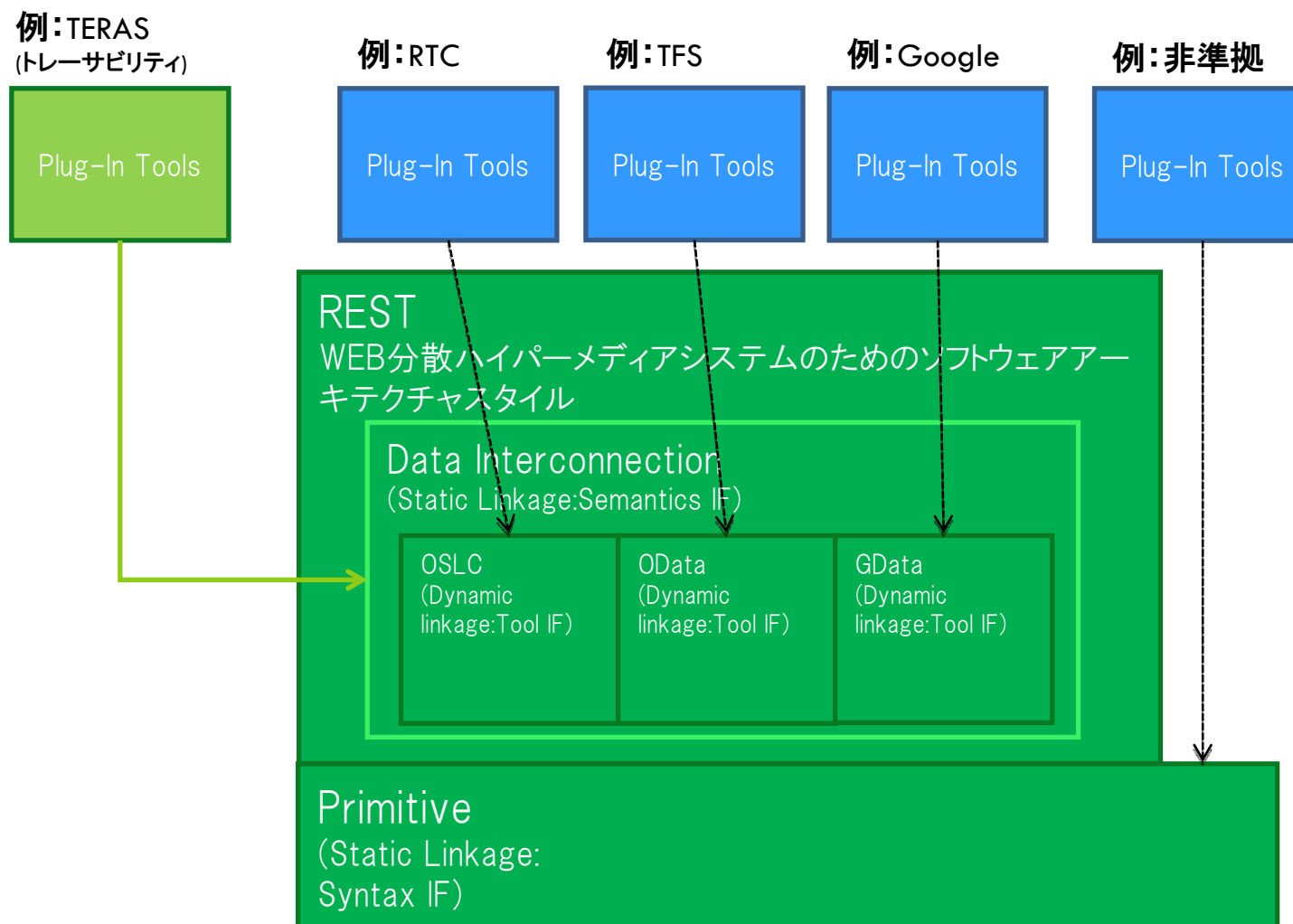
オープンツールプラットフォームのクラウドサービス



オープンツールプラットフォーム関連図

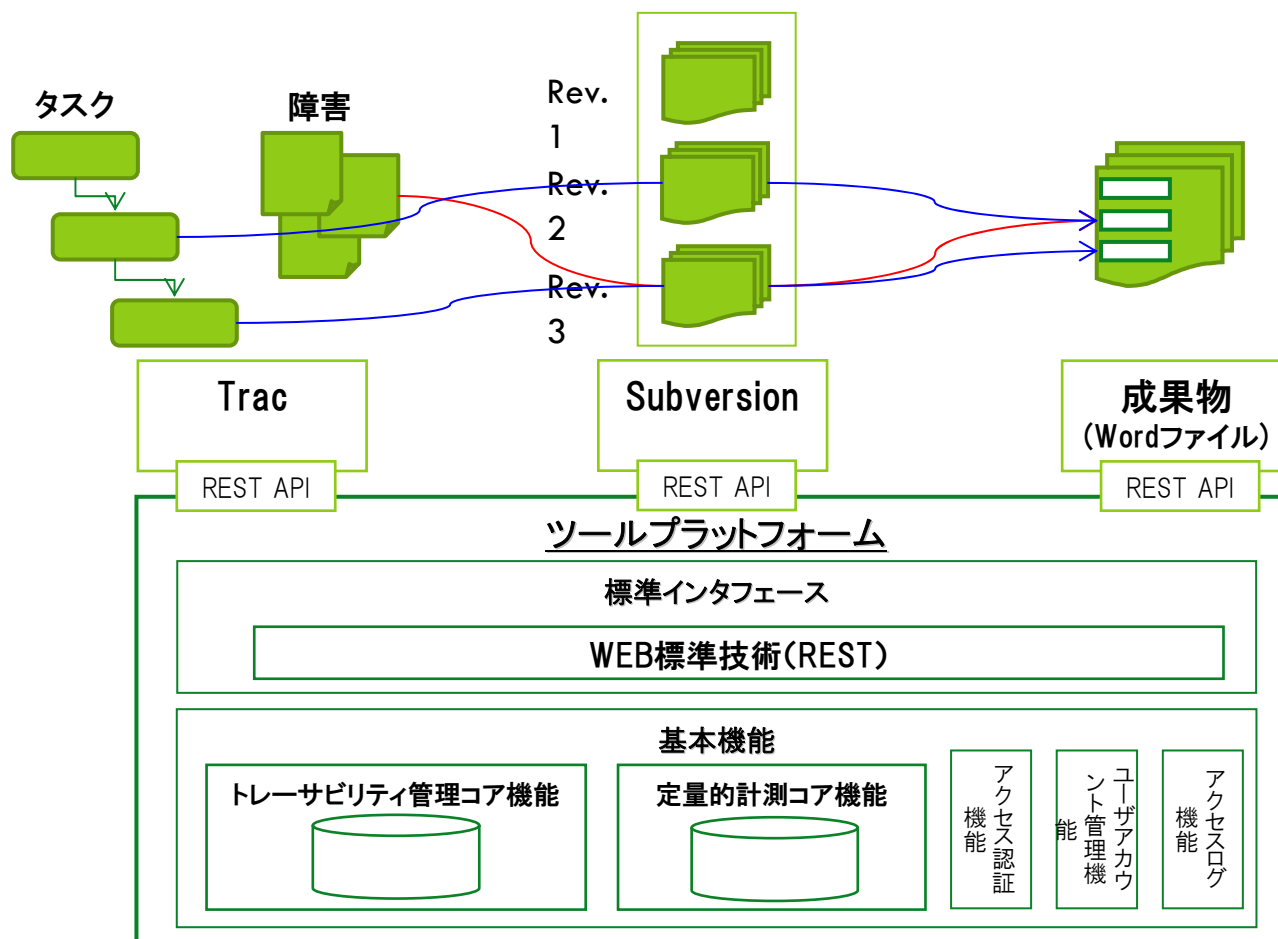


オープンツールプラットフォームによる標準化



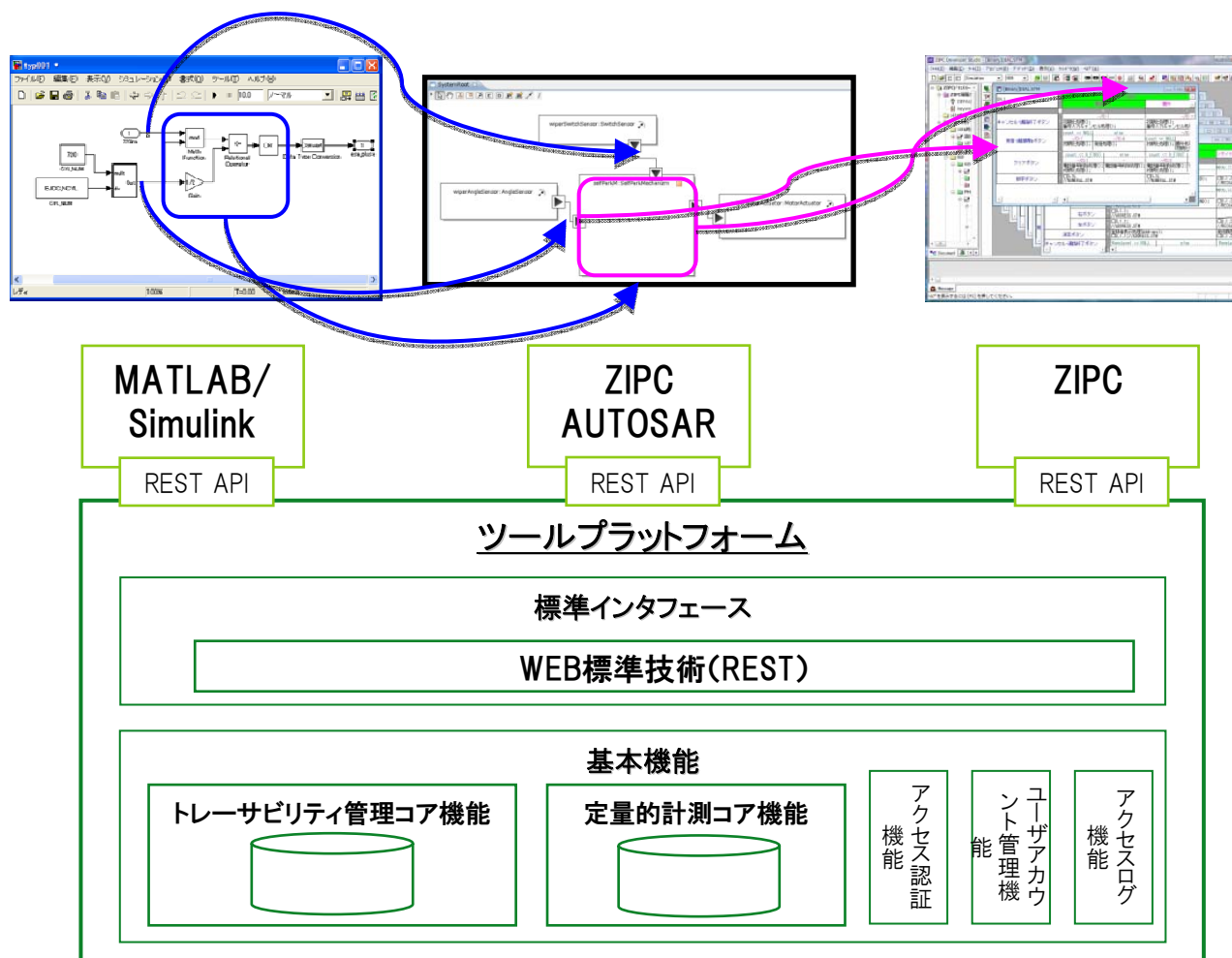
ツール連携の構想例(管理ツール)

- ▶ Trac、Subversion、成果物の異なる設計間の対応関係を管理
 - ▶ Trac、Subversion連携ではコミットログを活用した紐付けまでしかできない (タスクとファイル単位(リビジョン指定))



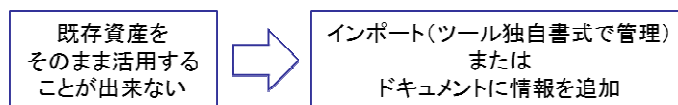
ツール連携の構想例(設計ツール)

- ▶ MATLAB/Simulink、ZIPC AUTOSAR、ZIPCの異なる設計間の対応関係を管理



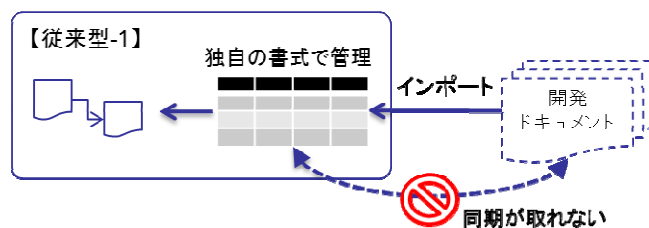
オープンツールプラットフォームの強み

- ▶ ツールプラットフォームの基本機能として、トレーサビリティ管理機能を搭載している
 - ▶ ALM全般にわたる要件トレーサビリティを提供
- ▶ 日本の開発形態にマッチした機能
 - ▶ すり合わせ開発での使いやすさにフォーカス
(フィードバックを考慮したトレーサビリティ確保)
- ▶ 既存資産への適合
 - ▶ 既存文書ファイルに手を加えずにトレーサビリティ情報を追加可能

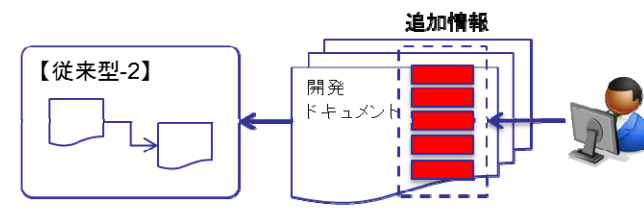


従来型の要件管理ツール

開発ドキュメントをインポートする必要がある



または 開発ドキュメントに対して開発者がトレース情報を追加する必要がある

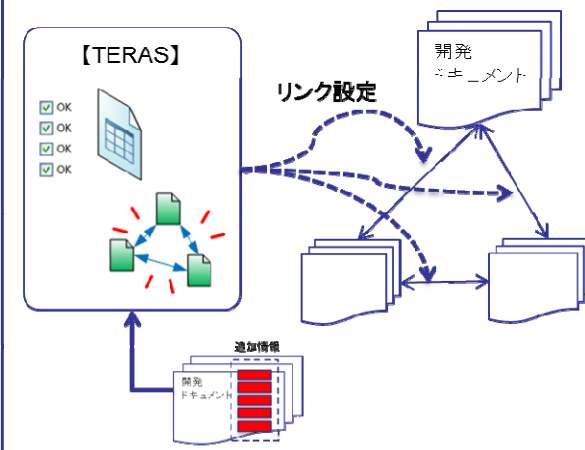


既存資産をそのまま有効活用

新世代

インポートもドキュメントの修正も不要

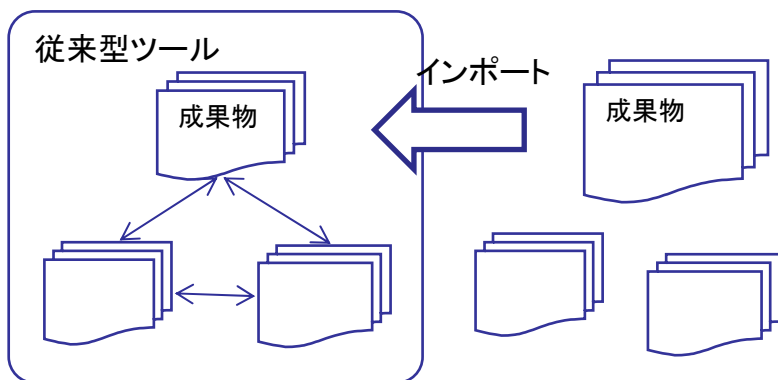
- ▶ ドキュメント内の要素単位でのリンクが可能
- ▶ ドキュメント修正時には、差分によるリンクが可能
- ▶ 追加情報を設定することで自動リンクも可能



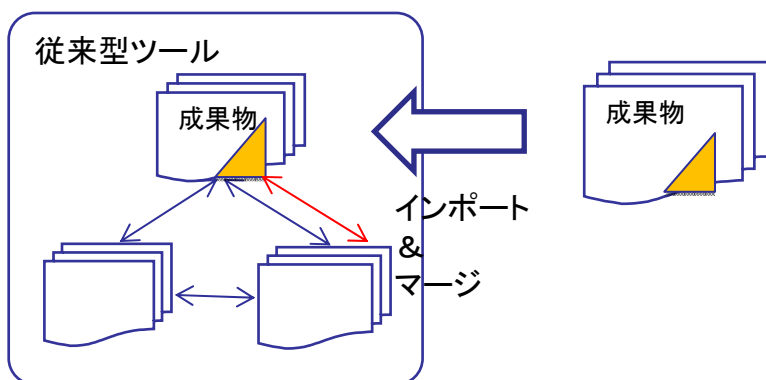
すり合わせ型開発の支援

従来型のトレーサビリティ管理ツール

ア) 成果物をインポートしてツール上で管理



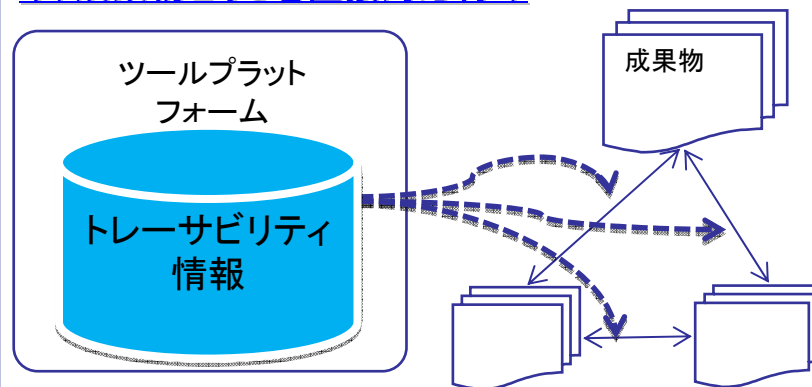
イ) 修正時



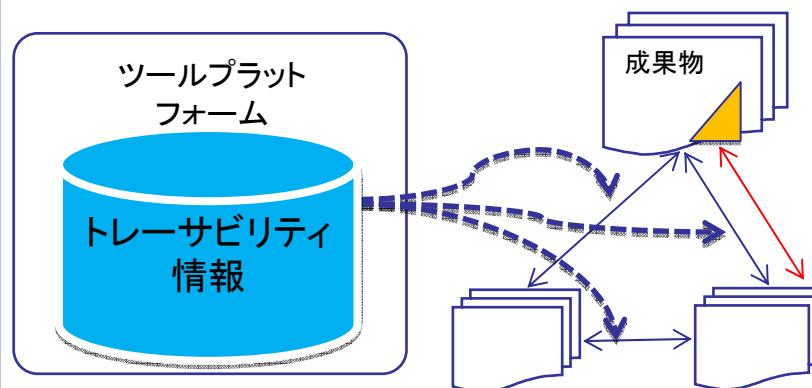
- トレーサビリティはツール上の要素間で管理
- ドキュメント修正時には再度インポート

ツールプラットフォーム

ウ) 成果物どうしを直接対応付け



エ) 修正時



- 成果物本体どうしのトレーサビリティを直接管理
- ドキュメント修正時には、差分のみをリンク

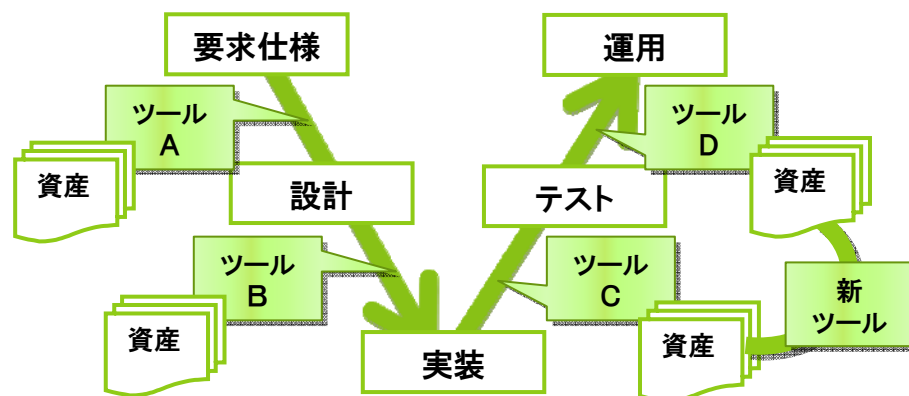
OSLCと協調

▶ OSLC ⇒ Open Services for Lifecycle Collaboration

▶ 疎結合によるツール統合の標準化

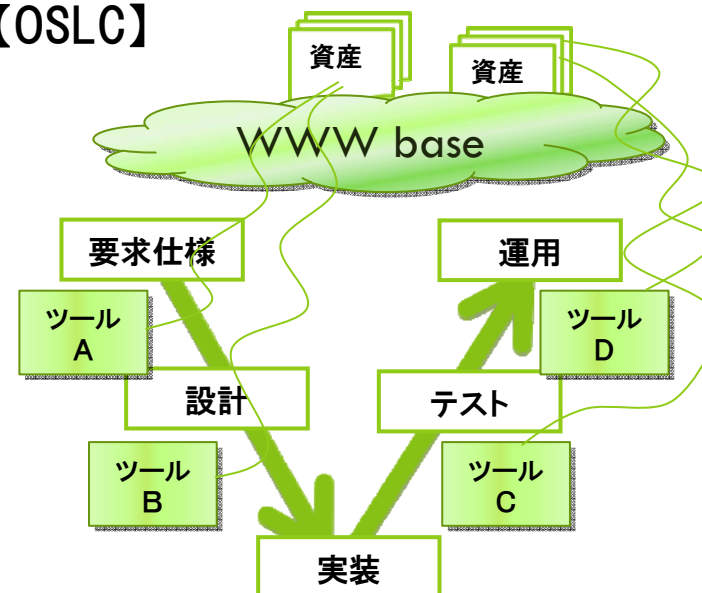
- ▶ 構成管理・見積り/要求管理・アセット管理・アーキテクチャ管理・品質管理を含む
- ▶ ALM(Application Life-cycle Management) とPLM (Product Life-cycle Management)の統合

【これまで】



- ✓ 各ツールはライフサイクル内の特定のプロセスに特化
- ✓ 他ツールからのアクセスにはAPIやベンダー独自の言語が必要
- ✓ 異なるツール間の連携を図る新たなツールによる堅固な結合
- ✓ ⇒アップグレードやリビジョンアップに弱い

【OSLC】



- ✓ 一様なアーキテクチャと一連のプロトコル
- ✓ 緩く結び付いたツールを着実な方法で統合 (インテグレート)する
- ✓ ⇒単独のベンダーで行えることではない

OSLCの特性とは

- ▶ インターネット的統合性(Internet-style integration)をサポートする“OSLCアーキテクチャ”の特性:
 - ▶ 規模拡張性(Scalable)
 - ▶ 無数のユーザ・リソースをサポートする
 - ▶ 分配性(Distributed)
 - ▶ 世界に散らばったユーザ・リソースをサポートする
 - ▶ 信頼性(Reliable)
 - ▶ あらゆる種類の接続環境に対しても上手く対応する
 - ▶ 拡張性(Extensible)
 - ▶ 操作上のプロトコル・サービスは開かれていて制約がない
 - ▶ 簡易性(Simple)
 - ▶ 使いやすく・学びやすい(ベンダー間連携や閉じた世界に依存しない)
 - ▶ 公平(Equitable)
 - ▶ 全ての参加者に等しく使える(個人から大企業まで、オープンソース・内製・商用でも、参加に障壁をつくらない)