Business Cube & Partners

セーフティクリティカルドメインへのAutomotive SPICEの適用事例とMBD適用の勘所

ビジネスキューブ・アンド・パートナーズ株式会社

Copyright 2019 Buiness Cube & Partners, Inc. All rights reserved.

本日のアジェンダ

Business Cube & Partners

- 会社紹介
- セーフティクリティカルドメインへのAutomotive SPICEの適用事例
  - 自動車分野と航空分野の共通性
  - DO-178Cの概要
  - なぜ、航空分野にAutomotive SPICEを活用？
  - プロセス構築のアプローチ
- モデルベース開発手法を実装する時の勘所
- まとめ

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

本日のアジェンダ

Business Cube & Partners

- 会社紹介
- セーフティクリティカルドメインへのAutomotive SPICEの適用事例
  - 自動車分野と航空分野の共通性
  - DO-178Cの概要
  - なぜ、航空分野にAutomotive SPICEを活用？
  - プロセス構築のアプローチ
- モデルベース開発手法を実装する時の勘所
- まとめ

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

自動車分野と航空分野の共通性

Business Cube & Partners

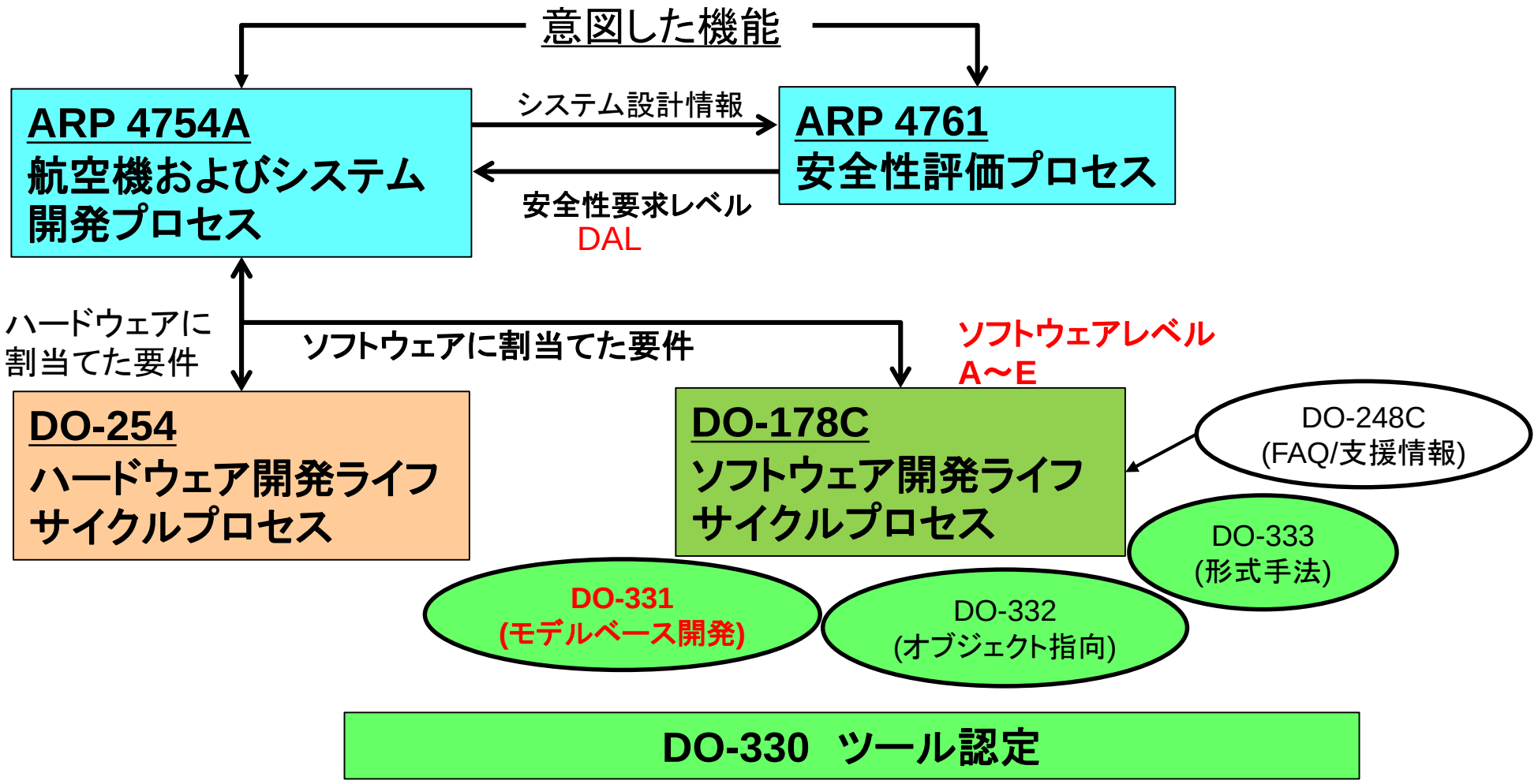
- 自動車業界と航空業界の共通点
  - CO2削減が大きな共通の課題
    - 電動化の流れが加速
      - 車載：HEV/EV
      - 航空：電動エンジン（車と同じコンセプト：電機モータ単独、ジェットエンジン＋電機モータ）
  - 安全規格体系の存在と製品開発への適用
    - 車載：ISO 26262（2010年代～）
    - 航空：ARP4754A、ARP4761、DO-254、DO-178C （1990年代～）
  - モデルベース開発手法の採用
    - システムズエンジニアリング（MBSE）手法
    - ソフトウェア開発領域でのモデルベース手法
  - 今後は、“空飛ぶ車”の開発で、製品技術、開発方法などが、より融合していく
- 狙い：
  - 自動車分野、航空分野の安全規格に準拠したプロセスを構築するためのアプローチを紹介する

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

DO-178Cの概要

Business Cube & Partners

- DO-178Cを含む航空機装備品開発の規格体系



Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

DO-178Cの概要

Business Cube & Partners

DO-178Cとは？

- DO-178Cは、ソフトウェア開発ライフサイクルを定義したガイドライン (Software Considerations in Airborne Systems and Equipment Certification)
  - 1992年：DO-178B
  - 2011年：DO-178Cに改訂

- 特徴：目的指向のアプローチ
  - DO-178Cを適用する場合は、すべての目的を満たす
  - 適用する者は、目的を達成するアクティビティを計画する
  - 計画したアクティビティを実行し、目的が達成されていることを実証する証拠を提供する

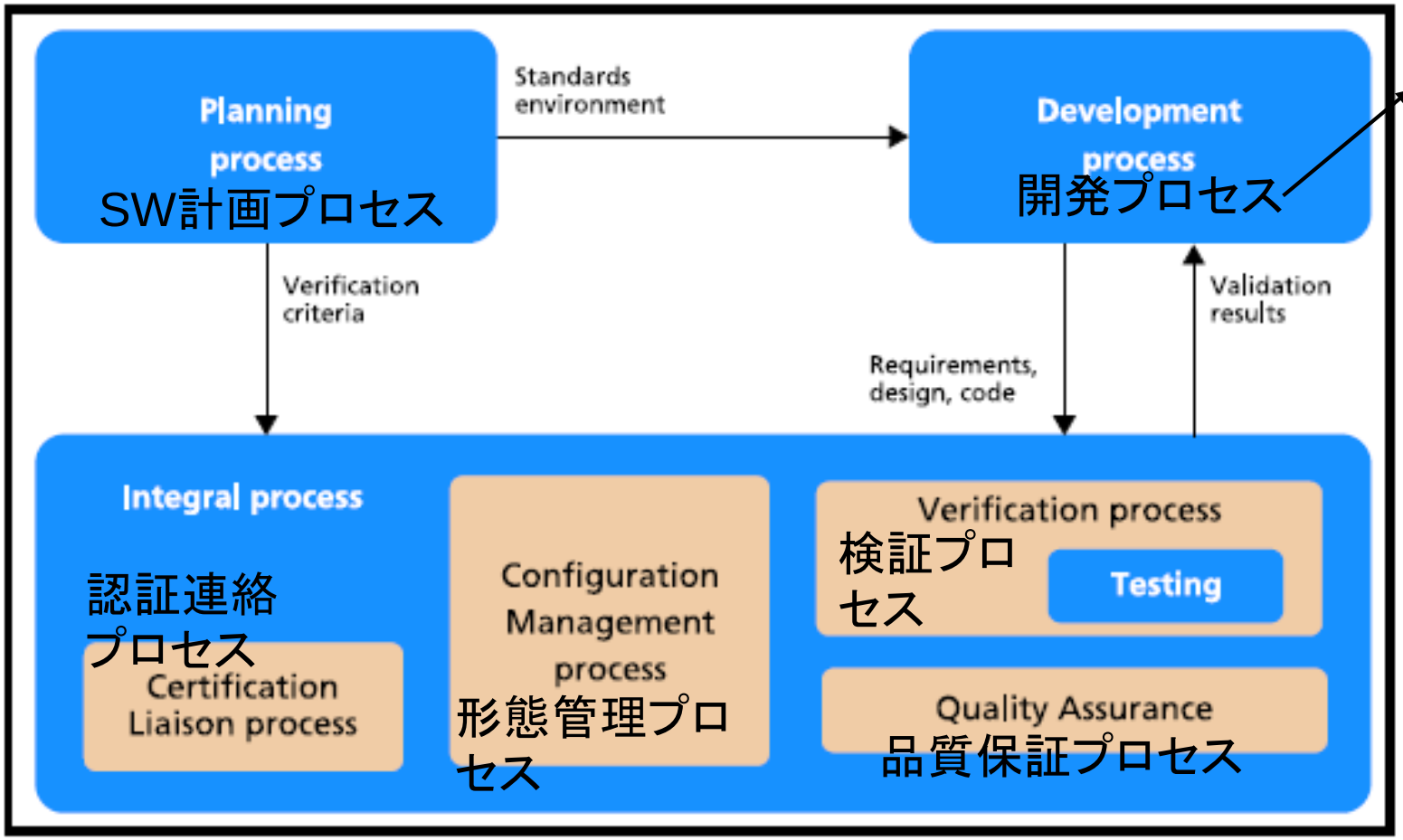
→目的を達成する手段、手法、方法は、自由に定義することができる

  - "shall"、"must"が使用されていない

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

DO-178Cの概要

- DO-178Cで定義されているソフトウェアライフサイクルプロセス
  - プロジェクトごとに、各プロセスの活動を選択、活動の順番、責務を定義する

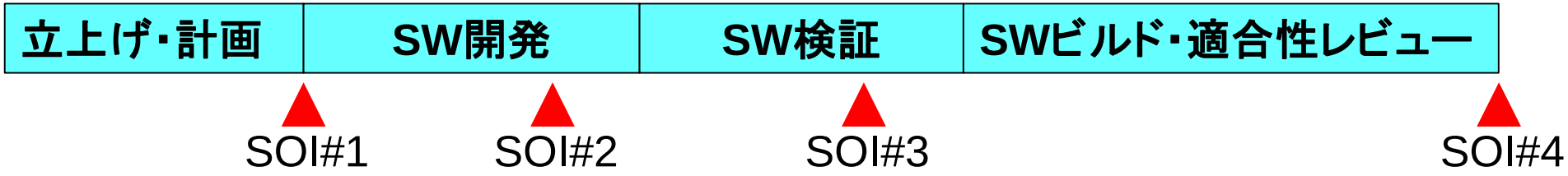


開発プロセスの中
- SW要件プロセス
- SW設計プロセス
- SWコーディングプロセス
- 統合プロセス

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

DO-178Cの概要

- ４つのステージにライフサイクルを分けて、各ステージで、認証機関または、その代理人(DER)による審査を受ける
  - SOI#1(ソフトウェア計画のレビュー)：SW計画書(5種類)と標準書(3種類)及び、開発体制の審査
  - SOI#2(ソフトウェア開発のレビュー)：ソフトウェア要件～ソースコード作成とそれらの検証を審査
  - SOI#3(ソフトウェア検証のレビュー)：検証方法(テストケース作成)及び検証結果(テスト実施)の審査
  - SOI#4(最終ソフトウェア認証レビュー)：最終的に開発プロセス全体として問題ないかの審査



Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

Biz3Template POTX 2.3

なぜ、航空分野にAutomotive SPICEを活用？

Business Cube & Partners

- DO-178C適用時にどのような課題があるか？
  - 安全設計、不具合の検出に目的や活動の観点が多く、管理、組織・体制を含めたプロセスの観点が少ない
    - プロセスは定義されているという前提
  - 各プロセスの章に、“目的”、“活動”、“アウトプット（成果物）”が定義され、“成果物の特性と内容”がLife Cycle Date章に定義されている
    - 活動内容が抽象的なところがあり、成果物の内容との結びつきが弱い
  - SW計画の策定、計画のレビューを完了する(SOI#1)までに時間が掛かる
    - ライフサイクルの定義、各プロセスで使用する手法やツール
    - プロセス間の相互関係、実行順序、フィードバック機構、プロセス移行条件の定義
    - 5種類の計画書、3種類の標準書を策定
      - SW認証計画、SW開発計画、SW検証計画、SW形態管理計画、SQA計画
      - SW要件標準書、SW設計標準書、SWコーディング標準書

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

なぜ、航空分野にAutomotive SPICEを活用？

Business Cube & Partners

- 課題例：5種類の計画書の１つ“ソフトウェア認証計画書”の内容

項目	記載内容
システム概要	システム機能、HW/SWに割当てた機能
ソフトウェア概要	ソフトウェアで実現する機能、安全機能の説明
認証における考慮事項	SWレベルの根拠、準拠の方法
ソフトウェアライフサイクル	**実施する各プロセスの説明(目的、入力、出力、活動、移行基準など)、目的をどのように達成するかを明記する。** 開発プロセス全体の定義
ソフトウェアライフサイクルデータ	成果物の文書名、認証機関に提出するデータ
スケジュール	SW開発スケジュール
追加の考慮事項	認証に影響が出る可能性がある事項(準拠の代替手段、ツール認定、パラメータデータの利用、SWの流用など)を記載
サプライヤ監視	**サプライヤのプロセスと成果物が、SW計画と標準に準拠していることを確認する手段** サプライヤ監視のプロセス定義

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

なぜ、航空分野にAutomotive SPICEを活用？

Business Cube & Partners

- Automotive SPICEは、ISO/IEC 15504に基づいて策定された車載システム開発のためのプロセスモデルである
  - ISO/IEC 15504は、ソフトウェアプロセスモデルの国際規格であり、通称SPICE (Software Process Improvement and Capability dEtermination)と呼ばれる
  - ISO/IEC 15504では、それぞれの業界の特性に合わせた業界特化版SPICEの策定が認められている

- その他の特化版SPICE
  - 航空宇宙：
    - SPICE for SPACE
    - JAXA PAM
  - 医療機器：
    - Medi SPICE
  - エンタープライズ：
    - Enterprise SPICE
  - ソフトウェアテスト
    - Test SPICE

重要：
Automotive SPICEは、プロセスで何を実施すべきか、なぜ実施しなければならないのかといったプロセスの目標や活動によって期待される成果を定義している

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

プロセス構築のアプローチ（全体の流れ）

Business Cube & Partners

Automotive SPICEを適用したプロセス構築のアプローチ： ２段階で実施

- ゴール：Automotive SPICE能力レベル2の達成を目指す（管理されたプロセス）
  - DO-178Cの目的と活動定義をAutomotive SPICEのプロセス成果と比較（プロセスのあるべき姿）
  - DO-178Cの目的を達成するために必要なプロセスの能力レベルは、Automotive SPICEレベル2相当と判断できる

- ステップ1：ギャップ分析とプロセス改善＋安全設計の導入
  - 成果物を作成するまでのプロセス実施内容を成果物でチェックする
  - プロセス実施内容をチェックする
  - ギャップに対する改善計画を立てて、改善を開始する
  - DO-178Cで要求されている安全設計を導入（ツールも検討）
  - ステップ1終了段階で、DO-178C認証は可能なプロセスが準備できる
- ステップ2：モデルベース開発手法を実装した標準プロセスの構築
  - “モデルのユースケース”を考慮したモデルベース実装プロセスを構築する

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

プロセス構築のアプローチ（全体の流れ）

Business Cube & Partners

2段階のアプローチ

- “プロセス成果”とDO-178Cの目的/活動を事前に比較し、不足している活動を抽出する（ギャップ分析時のチェック観点に追加）
- “プロセス成果”が達成できているかを成果物で評価する
- 成果物要件を確認する（テンプレート、チェックリスト、標準書など）
- 各プロセス実施に関する計画、監視、調整、リソース準備、窓口定義

達成

現状分析(レベル2対象)

改善

Automotive SPICEに基づくプロセスの構築
※プロセス内活動と成果物要件の強化

能力レベル2達成

モデルベース手法を実装した標準プロセスを定義

DO-178Cの目的を達成するための設計手法をプロセスに追加
※設計手法、ツール等導入

Automotive SPICE に基づくプロセスの構築
※能力レベル3を目指す(組織レベル)

【製品安全の視点】
- 安全設計のために必要な基準・手法を統合する
- 設計に合致した支援ツール導入

DO-178C/DO-331 要求事項のプロセスインフラへの追加
※DO-331の差分を吸収する仕組み

能力レベル3達成

DO-178C認証

MBD適用プロセス
標準プロセス

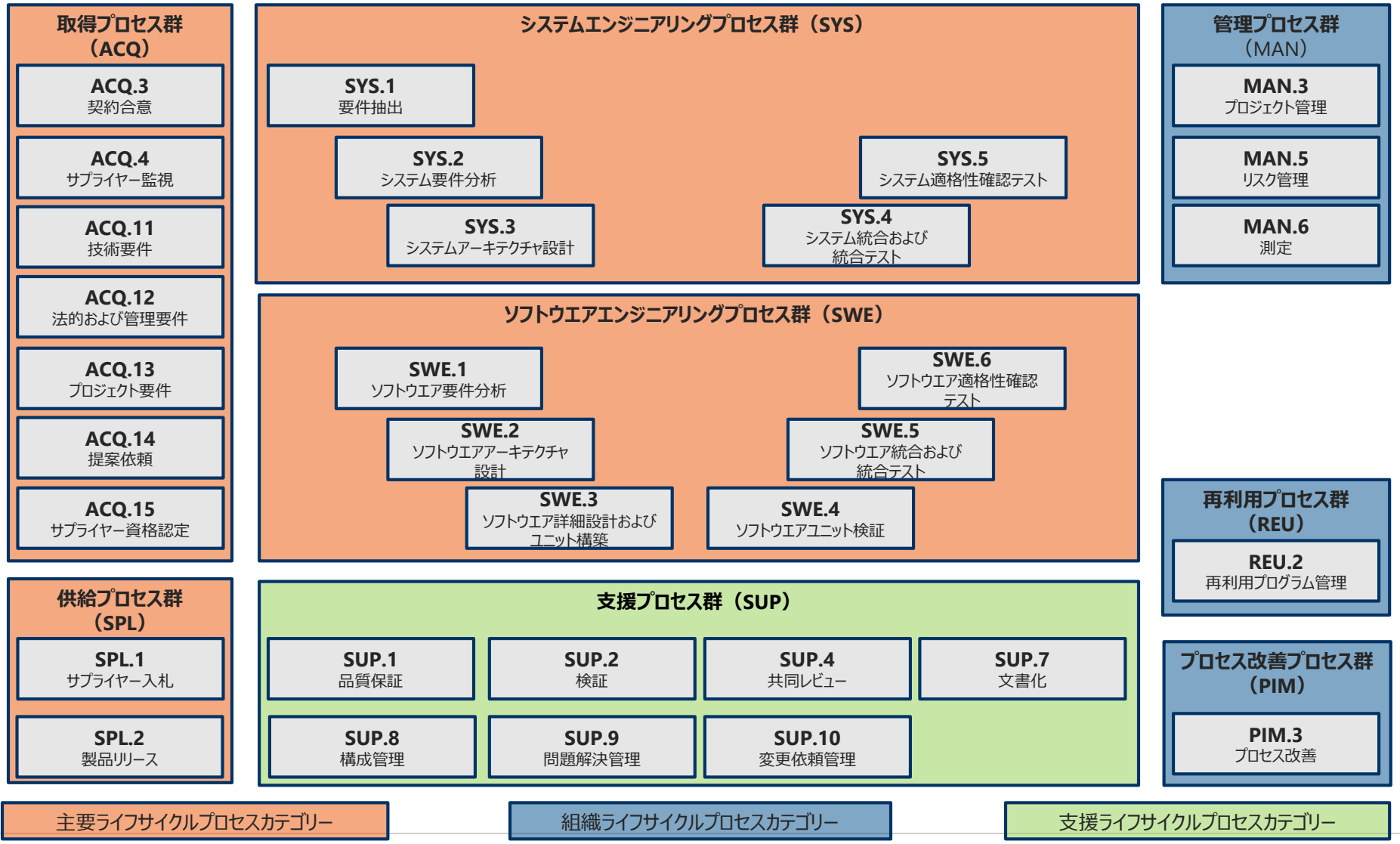
DO-178C認証
（DO-331適用）

人材の育成(プロセス評定、技法、ツール環境構築と運用)

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

プロセス構築のアプローチ　Automotive SPICE プロセス参照モデル

Business Cube & Partners

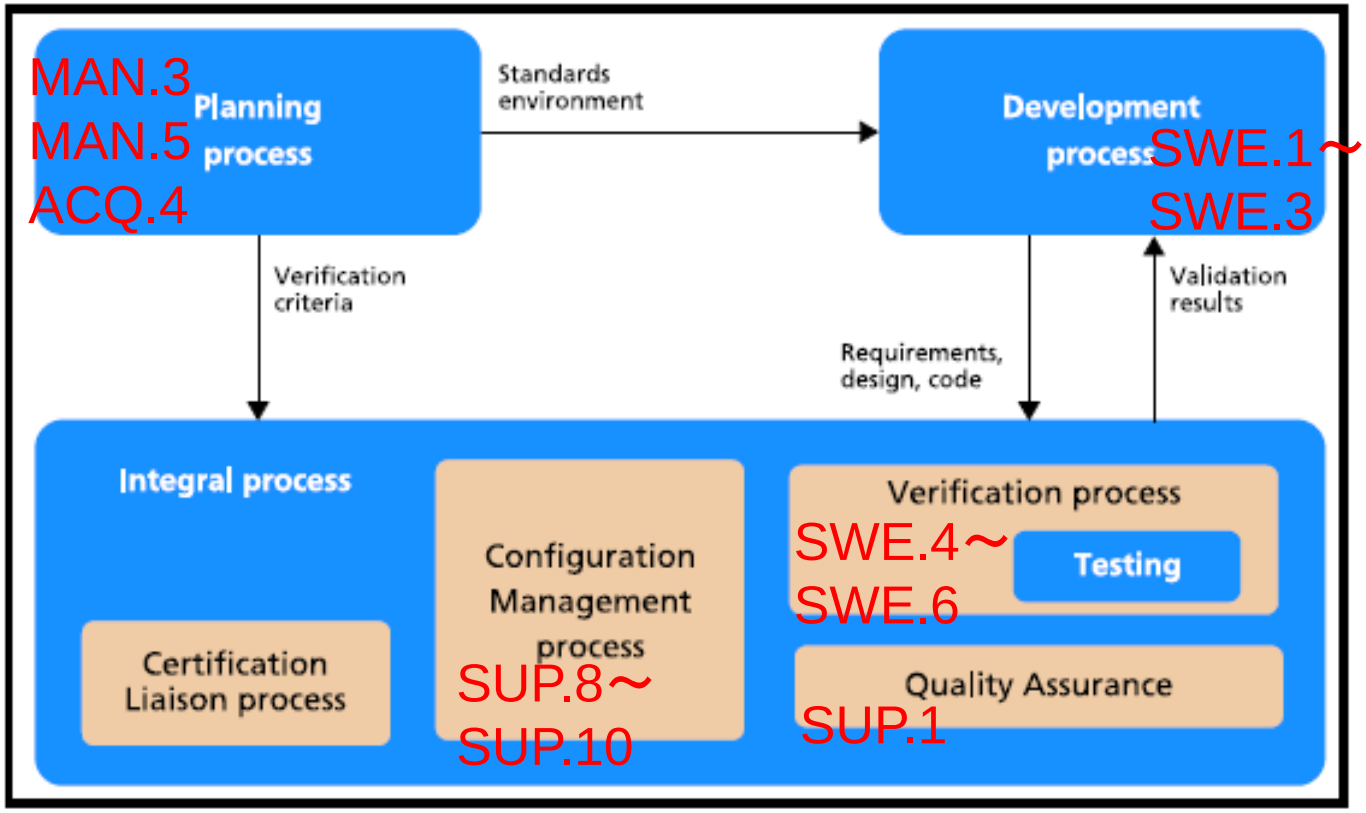


Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

プロセス構築のアプローチ：現状分析

Business Cube & Partners

- “プロセス成果”とDO-178Cの目的/活動を事前に比較し、不足している活動を抽出する
  - DO-178CのプロセスをAutomotive SPICEのプロセスエリアにマッピングする



Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

プロセス構築のアプローチ：現状分析

Business Cube & Partners

- 例：DO-178CのSW要件分析プロセス

1)安全設計/安全要求とそれら以外に分類
2)PDCA観点で、分類する

活動内容

a. The system functional and interface requirements that are allocated to software should be analyzed for ambiguities, inconsistencies, and undefined conditions. SW要件の分析
b. Inputs to the software requirements process detected as inadequate or incorrect should be reported as feedback to the inputs source processes for clarification or correction. フィードバック機構
c. Each system requirement that is allocated to software should be specified in the high-level requirements. SW要件の仕様化
d. High-level requirements that address system requirements allocated to software to preclude system hazards should be defined. 安全設計
e. The high-level requirements should conform to the Software Requirements Standards, and be verifiable and consistent. SW要件の評価
f. The high-level requirements should be stated in quantitative terms with tolerances where applicable. SW要件の分析
g. The high-level requirements should not describe design or verification detail except for specified and justified design constraints. SW要件の評価
h. Derived high-requirements and the reason for their existence should be defined. SW要件の分析
i. Derived high-level requirements should be provided to the system processes, including the system safety assessment process. フィードバック機構
j. If parameter data items are planned, the high-level requirements should describe how any parameters data items is used by the software. The high-level requirements should also specify their structure, the attributes for each of their data elements, and, when applicable, the value of each element. The values of the parameter data item elements should be consistent with the structure of the parameter data item and the attributes of its data elements. SW要件の仕様化

引用元：DO-178C, “Software Considerations in Airborne Systems and Equipment Certification”

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

プロセス構築のアプローチ：現状分析

- Automotive SPICEのSW要件プロセス（SWE.1）の“プロセス成果”とDO-178CのSW要件プロセスの目的、活動）を比較する
  - 不足分をギャップ分析の観点として加える

Automotive SPICEのSW要件分析プロセス

Process ID	SWE.1
Process name	Software Requirements Analysis
Process purpose	The purpose of the Software Requirements Analysis Process is to transform the software related parts of the system requirements into a set of software requirements.
Process outcomes	As a result of successful implementation of this process: 1) the software requirements to be allocated to the software elements of the system and their interfaces are defined; 2) software requirements are categorized and analyzed for correctness and verifiability; 3) the impact of software requirements on the operating environment is analyzed; 4) prioritization for implementing the software requirements is defined; 5) the software requirements are updated as needed; 6) consistency and bidirectional traceability are established between system requirements and software requirements; and consistency and bidirectional traceability are established between system architectural design and software requirements; 7) the software requirements are evaluated for cost, schedule and technical impact; and 8) the software requirements are agreed and communicated to all affected parties.

SW要件の仕様化の観点に追加

SW要件の評価の観点に追加

ここまでの作業を他のプロセスでも実施する

引用元：Automotive SPICE Process Assessment / Reference Model V3.1

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

プロセス構築のアプローチ：現状分析

Business Cube & Partners

- 実際の成果物と既存のプロセス定義を見て、評価する
  - これからプロセスを構築する場合：Automotive SPICEをフルに適用してギャップ抽出
  - 既存のプロセスがある場合：前ページのギャップ分析の観点を中心に評価する

- 成果物の要件と成果物管理に関する評価
  - DO-178Cのライフサイクルデータの特性とAutomotive SPICEの成果物特性を参照して、その内容に沿って定義されているかをチェックする→**各標準書の内容**
  - 構成管理ツールの利用範囲、運用方法の確認と対応（成果物の保管、テンプレート管理）

- プロセス実施に関する評価
  - プロセス実施目標、計画、監視、調整、リソース準備
    - プロセス実施に関する計画を立てて、実施や調整（スケジュール変更）に必要なリソースを割り当てているかをチェックする
    - プロセスの実施に関与する個人やグループ、窓口が決定されているかをチェックする

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

プロセス構築のアプローチ：安全設計の導入

Business Cube & Partners

- 安全設計技法・手法の実装
  - 要求されている安全設計、観点を各標準書(SW要件、SW設計、コーディング)に組み込む
- 設計や解析を支援するツールを決める
  - 成果物要件を満たすように、データ書式を決める
  - ツールクォリフィケーションデータの準備

（安全設計・解析支援について、IDAJ様の講演を参照ください）

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

本日のアジェンダ

Business Cube & Partners

- 会社紹介
- セーフティクリティカルドメインへのAutomotive SPICEの適用事例
  - 自動車分野と航空分野の共通性
  - DO-178Cの概要
  - なぜ、航空分野にAutomotive SPICEを活用？
  - プロセス構築のアプローチ
- **モデルベース開発手法を実装する時の勘所**
- まとめ

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

モデルベース開発を実装する時の勘所

Business Cube & Partners

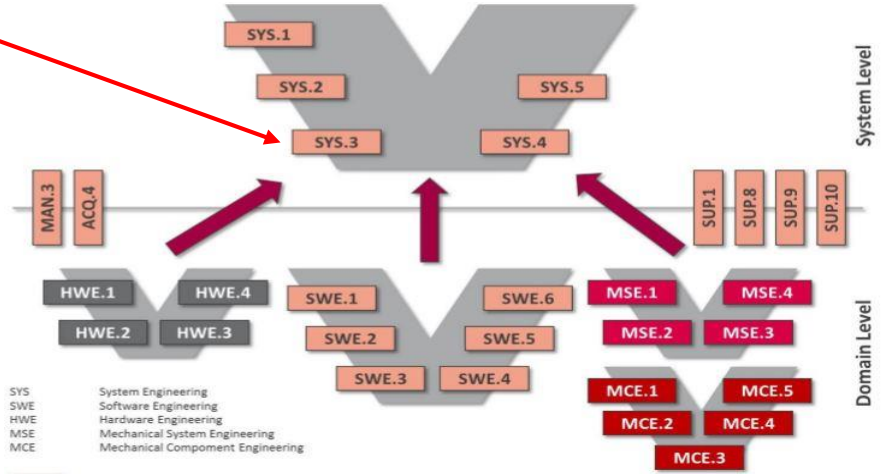
- モデルベース開発手法を実装する狙いは？
  - 安全な製品を効率よく開発する
  - 手戻りを減らすためのフロントローディング（設計と検証の同時進行）
  - プロセスや活動の自動化（ドキュメント自動生成、コード自動生成、検証など）
- モデルベース開発手法の扱い
  - 車載：ISO 26262では、モデルベースを適用した場合の要求が組み込まれている
  - 航空：DO-178Cでは、補足規格DO-331としてサポート
- どのプロセス領域にモデルを導入してプロセスを構築するかを考えていますか？
  - モデル言語の構文や意味づけが、導入するプロセス領域で表現すべきことに適しているか？
  - モデルは成果物の一部、それとも、補足情報（絵として貼り付ける）？

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

モデルベース開発を実装する時の勘所

Business Cube & Partners

- 「Automotive SPICEガイドライン」と「DO-331 」で共通で、重要な観点
  - モデルのユースケースを定義すること
    - “**<u>システムアーキテクチャ設計</u>**は、SysMLを使用する”



  - 表記の構文や意味付けを定義する（形式/準形式/非形式）
    - 準形式：SysML、UML、Simulinkなど
    - 形式：VDM、B、SCADEなど

→認証機関も同様の分類認識

  - モデルだけでは表現できないことは、自然言語で補足を付ける
    - 設計根拠などをモデルのそばに、テキストで記述しておく
    - モデルが成果物の一部であるなら、後工程では重要な入力になる

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

モデルベース開発を実装する時の勘所

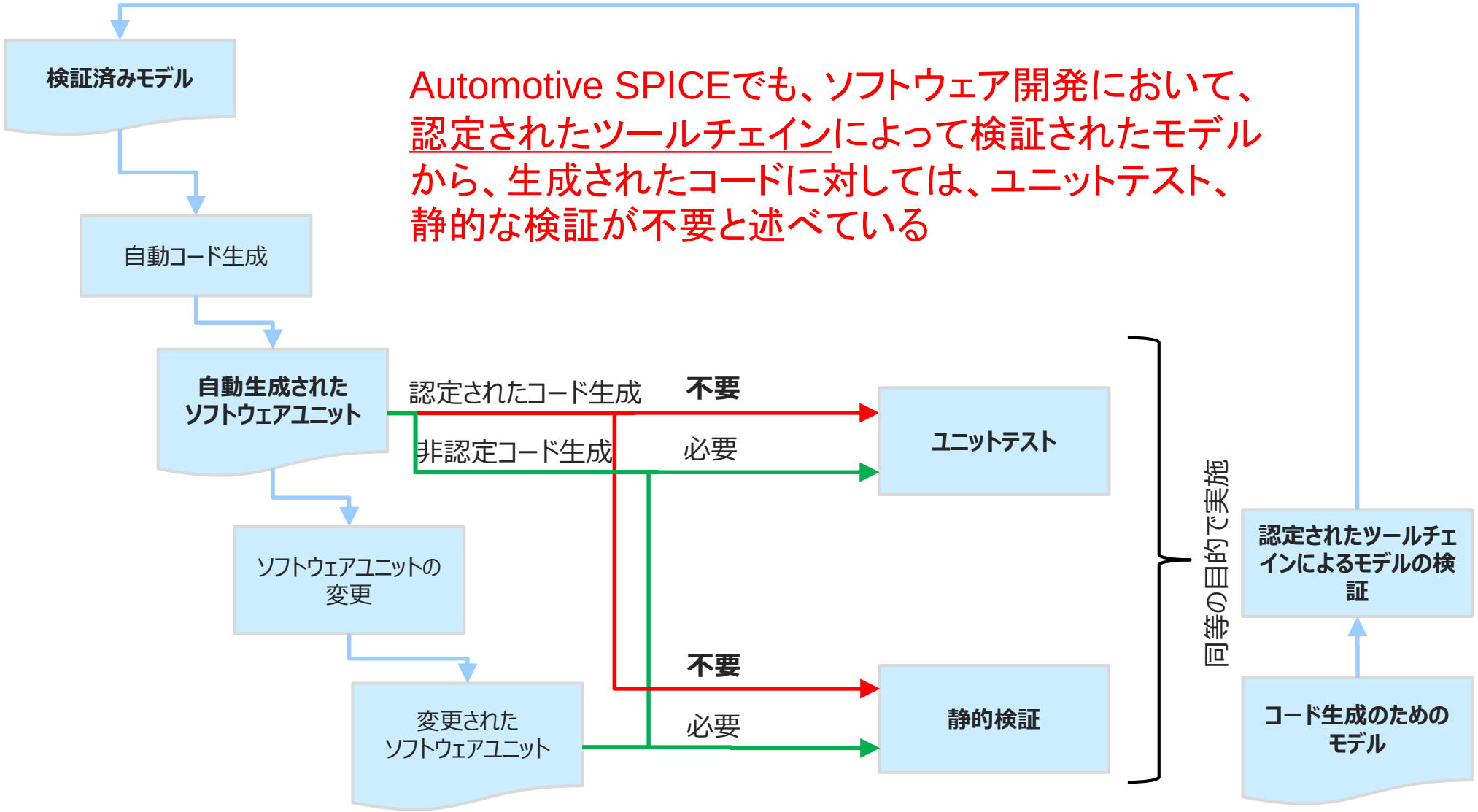
Business Cube & Partners

- モデルからコードを自動生成する場合（ソフトウェア設計に適用）
  - 位置づけ：
    - コード生成はすでに設計の一部
    - 設計から導出したもの（モデルと設計書の間のトレーサビリティが必要）
  - ソフトウェア設計において、ソフトウェアを理解するためには重要な情報を付加する
    - 例：モデルに追加するテキストでの注釈（設計の決定根拠など）→自動コード生成には影響ないが、レビューの際には必要
  - モデルに対して行うユニット検証では、ソフトウェアユニットがソフトウェア詳細設計およびソフトウェアの非機能要件と整合性を持っていることを示す→**要件ベースシミュレーション、トレーサビリティ、モデルカバレッジ解析**
  - トレーサビリティと一貫性の確認によってモデルとソースコードの整合性を保つ
  - モデルに対する付加情報とモデル、ソースコードとの整合性は一般的にレビューで確認する→**モデルから生成された設計ドキュメントでレビューする**

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

モデルベース開発を実装する時の勘所

Business Cube & Partners



Automotive SPICEでも、ソフトウェア開発において、認定されたツールチェインによって検証されたモデルから、生成されたコードに対しては、ユニットテスト、静的な検証が不要と述べている

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

モデルベース開発を実装する時の勘所

Business Cube & Partners

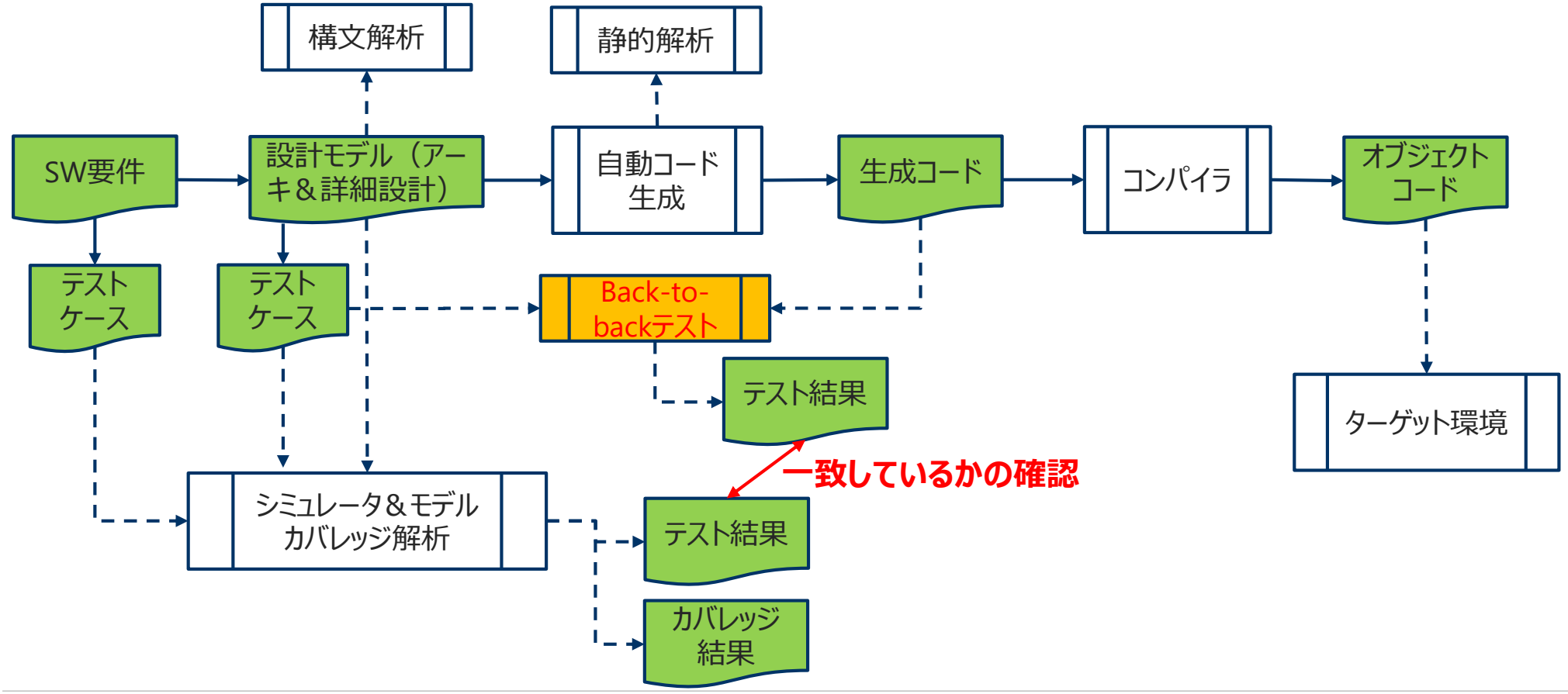
- “コード生成のための認定されたツールチェイン”とは？
  - 生成されたコードが、設計モデルに対して正しく、一貫性があるという証拠がある
- どのようにして、“生成されたコードが、設計モデルに対して正しく、一貫性がある”ことを示すか？
  - モデルベースツールの機能または、モデル言語の性質によって方法が変わる
  - ケース1：“Back-to-back”テストの実施、モデルと生成コード間のトレーサビリティによって、成立する
    - 車載系は、このアプローチが多い
  - ケース2：“コード生成”、“モデル検証手段”に関する認定の信頼性で成立する
    - 航空系は、このアプローチが多い（ツール認定の信頼度を活用）

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

モデルベース開発を実装する時の勘所

Business Cube & Partners

- ケース1：Back-to-backテストによって、モデルと生成コードの一致性を確保する

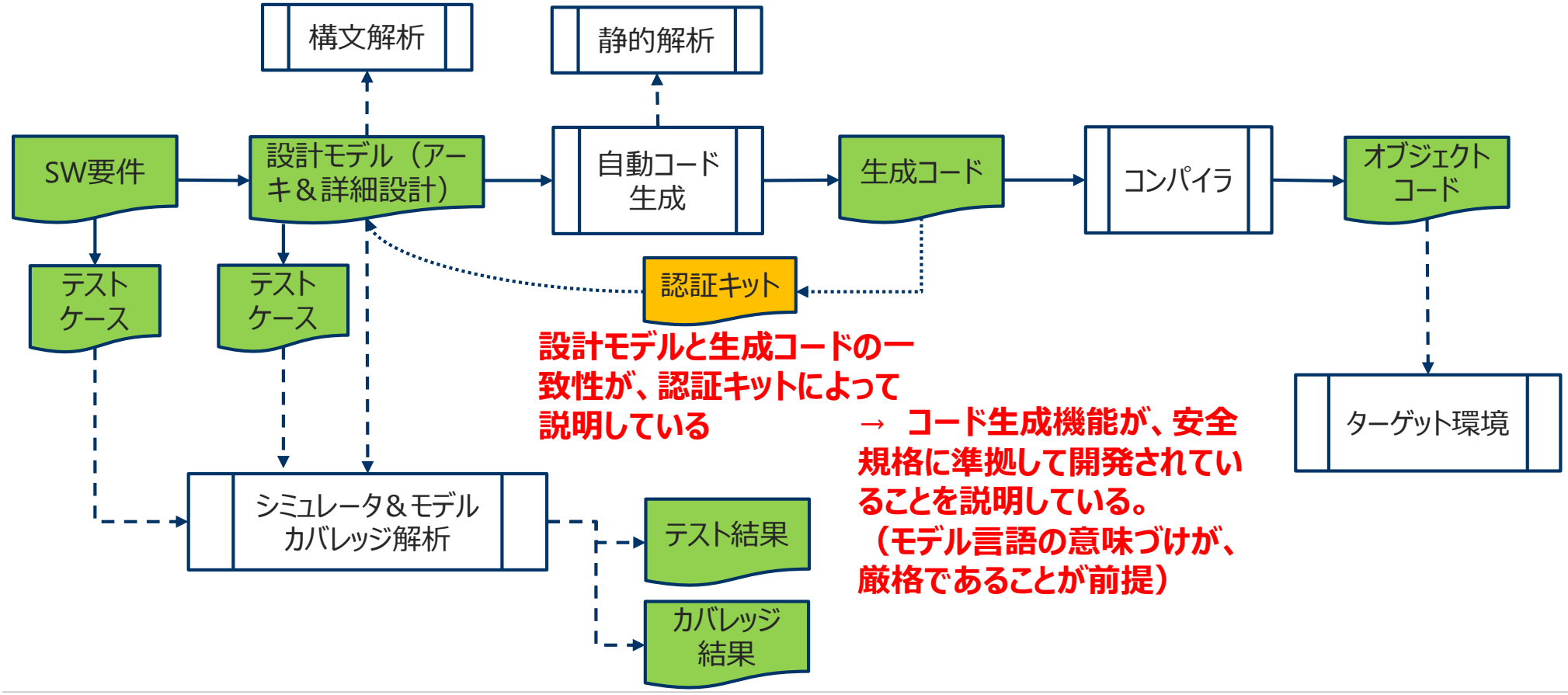


Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

モデルベース開発を実装する時の勘所

Business Cube & Partners

- ケース2：認定されたツールチェイン(構文解析、自動コード生成、モデルテスト等)によって、モデルと生成コードの一致性が担保される



Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

本日のアジェンダ

Business Cube & Partners

- 会社紹介
- セーフティクリティカルドメインへのAutomotive SPICEの適用事例
  - 自動車分野と航空分野の共通性
  - DO-178Cの概要
  - なぜ、航空分野にAutomotive SPICEを活用？
  - プロセス構築のアプローチ
- モデルベース開発手法を実装する時の勘所
- まとめ

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

まとめ

Business Cube & Partners

本セッションで、お話したこと：

- DO-178Cに準拠したソフトウェア開発を構築する場合に、現状の分析を行う道具として“Automotive SPICE”をするアプローチを紹介した
  - DO-178Cの目的、活動を理解して、プロセス視点で不足している活動を補うために、Automotive SPICEでギャップを抽出する
  - DO-178Cの目的を達成するプロセスは、Automotive SPICE能力レベル2を達成できれば良い
  - さらに、能力レベル3達成を目指し、「組織標準プロセス」を構築し、各プロジェクトに適用することで、計画の審査に掛かるまでの時間を削減する
- Automotive SPICEガイドラインとDO-331 で共通で、重要な観点について説明した
  - モデルのユースケースを明確にし、適用するプロセスの後工程への影響を考慮する
    - SW開発の場合、設計モデルのデザイン根拠などの付加情報
  - 認定されたツールチェインにおけるモデルと生成コードの一致性確保のアプローチを説明した

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

お問合せは下記までお気軽にご連絡ください。

ビジネスキューブ・アンド・パートナーズ株式会社
コンサルティング事業部
consulting@biz3.co.jp
http://biz3.co.jp

Copyright 2019 Business Cube & Partners, Inc. All rights reserved.