ISO 26262　第2版変化点解説セミナー

Business Cube & Partners

Confidential Information

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

本日のアジェンダ

- 機能安全概論
- ISO 26262 第2版の主要変化点解説
- Biz3　新・機能安全ソリューションのご紹介

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

機能安全概論

Confidential Information

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

国際規格における安全の定義

- ISO/IEC Guide 51 :2014（JIS Z 8051）
  - 許容できないリスクがないこと
  - 原文：”Freedom from risk which is not tolerable”

- ISO 26262
  - 不合理なリスクが存在しないこと
  - 原文：”Absence of unreasonable risk”

上記の定義は共に「リスクゼロの状態」を意味しているのではない
許容できないリスク以外のリスクがあっても安全である」という意味である

つまり・・・

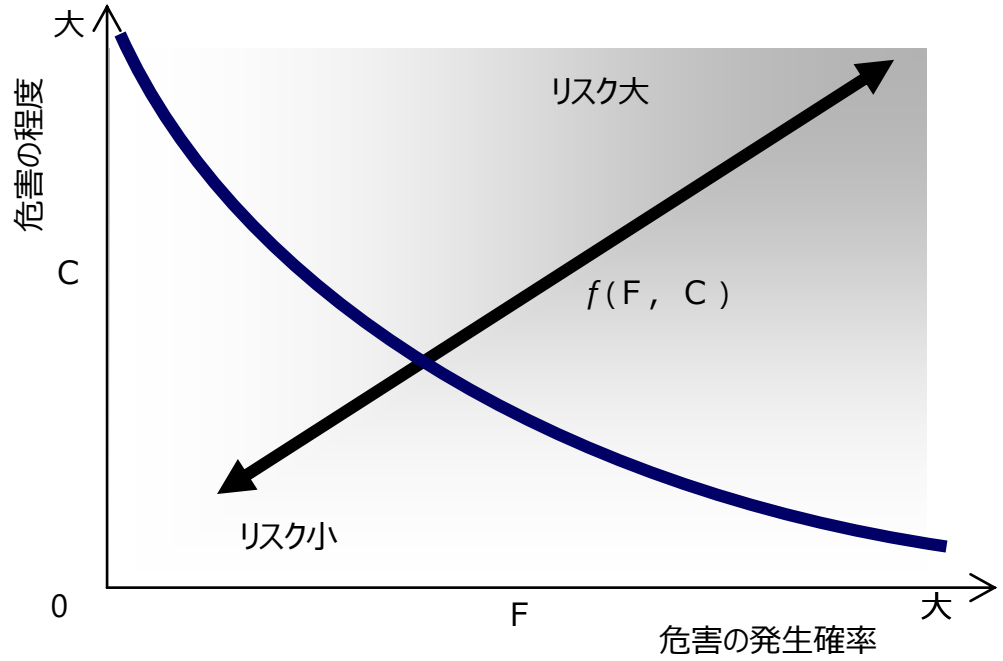
「リスクが許容可能な状態まで抑えられている状態」を安全と定義している
「リスク」については数量的な概念を用いてコントロールしていく

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

リスクの定義

- ISO/IEC Guide 51 （JIS Z 8051）
  - 危害の発生確率及びその危害の程度の組合わせ

- IEC 61508-4:2010 （JIS C 0508-4）
  - 危害の発生頻度及び危害の過酷度の組合せ



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

許容可能なリスク（Tolerable Risk）

Business Cube & Partners

- ISO/IEC Guide 51:2014 （JIS Z 8051）
  - 現在の社会の価値観に基づいて、与えられた状況下で、受け入れられるリスクのレベル

- 2019年4月7日のニュースより

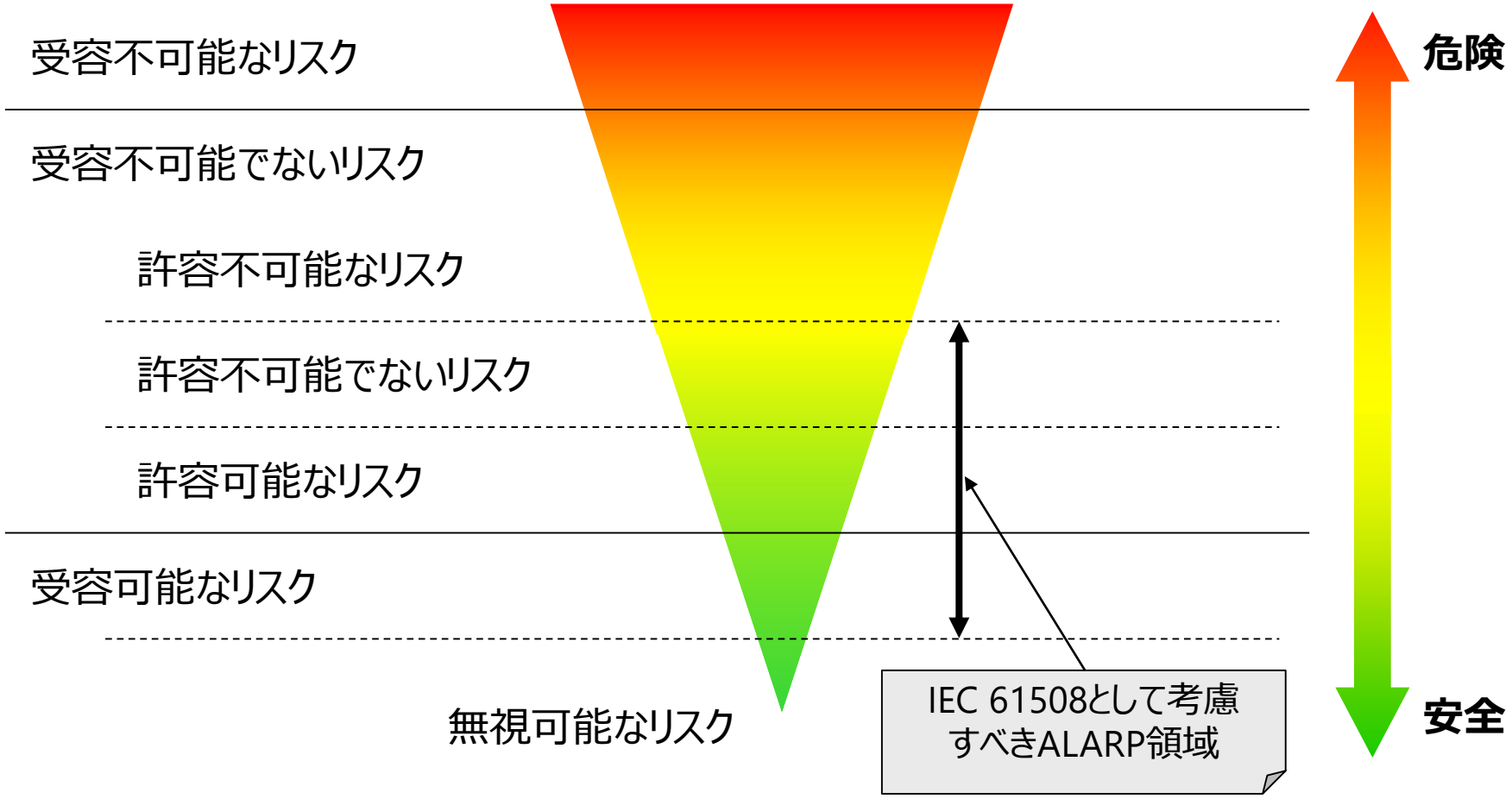
アメリカ人の3分の2が「自動運転車両は購入したくない」　ロイター通信が調査

  - 社会の価値観では自動運転で享受できる利便性と潜在リスクでは、まだ潜在リスクが上回っている(リスクを許容できない)

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

ALARPとは

- ALARP：As Low As Reasonably Practicable
  - 合理的に実施可能な限りリスクを下げる



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

ISO/IEC Guide51に基づく安全の基本アプローチ

1. 存在するリスクを把握する　（リスクアセスメント）
    1. 制限を決定する　（意図する使用、予見可能な誤使用は何か）　→アイテム定義
    2. 危険源を同定する　（危険源分析を行う）　→ハザード分析
    3. リスクを見積る　（危害の頻度、大きさ）　→リスク評価
    4. リスクを評価する　（リスク低減がどの程度必要か）　→ASIL

2. リスクを許容可能な程度まで低減する　（リスクの低減）　→安全コンセプト 安全方策
    1. 本質的な安全設計を行う
    2. 残ったリスクに対して、安全防護や付加保護方策を行う
    3. それでも残ったリスクに対しては、使用者に通知する

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

安全の思想

- 現在の技術水準：State of the arts
  - 機能安全　ISO 26262:2018
  - 品質マネジメント　IATF 16949:2016
  - プロセスモデル　Automotive SPICE, CMMI
- 自動車業界の不正に対する不信感
- 規格準拠型活動が顕在化
  - 規格準拠観点の活動、監査、アセスメントにより本来の目的が達成されない
    - 品質マネジメントシステム導入しても品質があがらない、工数が増える
    - ISO 26262準拠型の開発をしていても安全論証できない
  - より規格目的の達成やプロセス成果の指標評価を重視
- CASEによる利便性向上への期待と潜在リスクへの不安
  - 自動運転システムの安全性
  - サイバーテロへの対策

安全のフィロソフィー

変化する社会の価値観(許容可能なリスクのレベル)、ALARPの考えに基づき、合理的に可能な限りリスク低減をし続ける継続的改善活動

Confidential Information

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

プロセス構造と改善

Process

安全プロセス
- 基本アプローチ
- 26 Objectives

Method

安全技法・手法
- FMEA/FTA
- VDA・AIAG FMEA
- DFA
- STAMP/STPA
- MBSE/MBD

Tool

ツール
- 要件管理ツール
- 安全分析ツール
- 設計ツール
- 構成管理ツール

基本骨格の部分
安全不履行などがあれば
見直す

時代進化やState of the artsを考慮して常に
見直し、更新される部分

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

ISO 26262 第2版の主要変化点解説

Business Cube & Partners

Confidential Information

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

第2版変化点から見る特徴

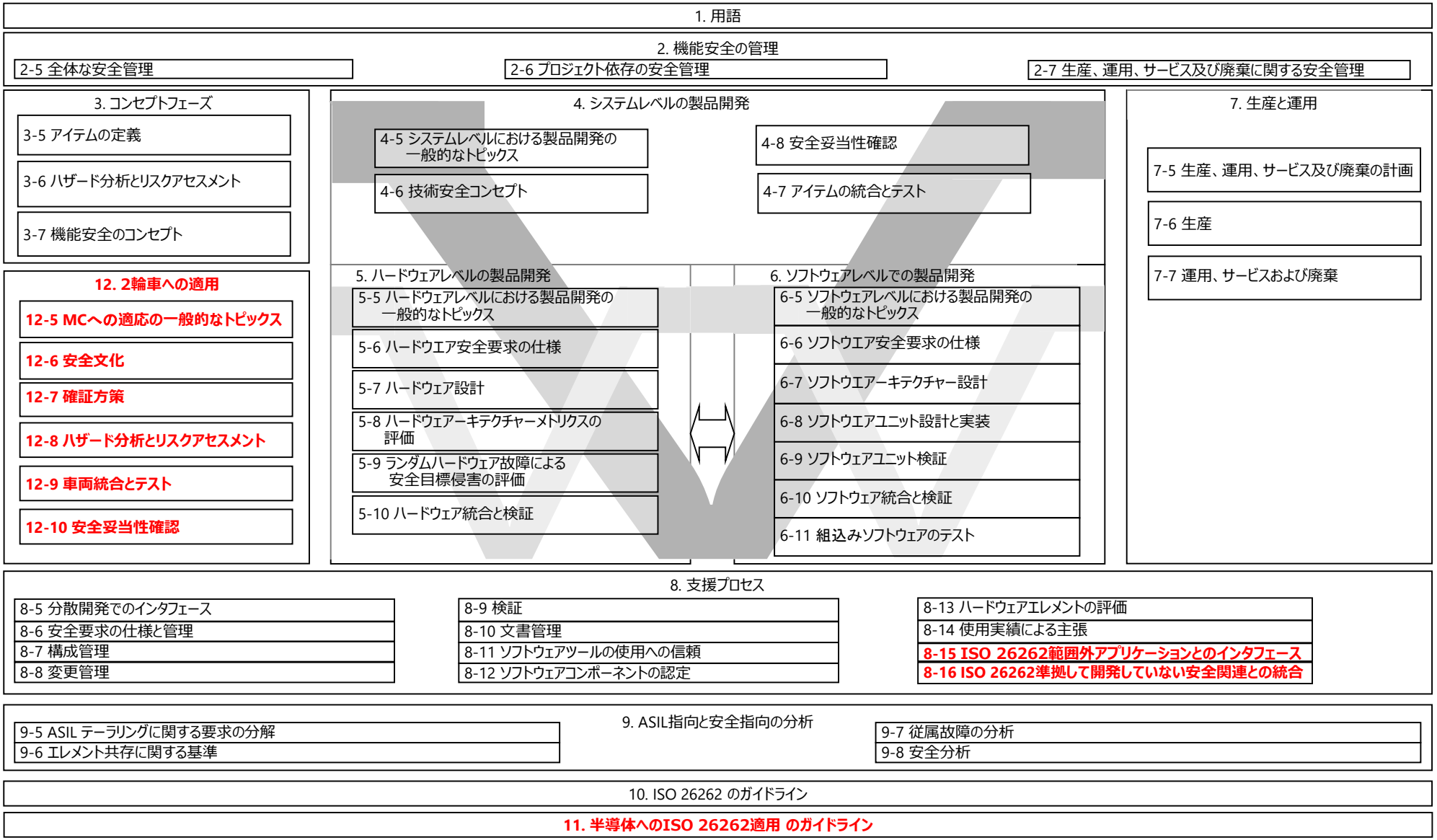
- CASE時代の機能安全規格に進化
  - モペット・特殊車両を除く路面走行車すべてが適用スコープに
    - トラック＆バス(T&B)、モータサイクル
  - 「つながる」に対する配慮
    - サイバーセキュリティとのコミュニケーションチャネル(Part 2)
    - インフラ安全とのインタフェース、コミュニケーションチャネルは、次回の改訂？
  - 「電動化」「自動運転」に対する考慮
    - フォールトトレランス(Part 10)、SOTIF(PAS 21448)
  - 規格の不明瞭な点を改善し、新規参入(電動化システムサプライヤ、COTSやSEooCなどエレメントのサプライヤ)の正しい理解に導く
    - エレメント共存とASILデコンポジション、従属故障分析(ISO 26262-9 Clause 7, Annex C)
    - 既存エレメント、COTS、SEooC利用に対する規格適用
    - ソフトウェア安全分析(ISO 26262-6 Annex E)
- 目的指向の強まり
  - 規格への準拠型指向(規格要件だから、上流からの要件だから、重厚長大なプロセス定義)により、機能安全達成の論証ができないことが問題視された結果として、機能安全の目的を明示し、達成されているかを確証方策で評価
    - 各節の目的の詳細化、目的指向の確証方策

Confidential Information

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

ISO 26262:2018全体像

Business Cube & Partners



※赤太字は第2版で追加

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

変化点トピックス

- スコープ拡大
  - T&B、モータサイクル
  - コミュニケーションチャネル
- 目的指向
  - 目的の詳細化、目的指向の確証方策
  - 機能安全要求の戦略　洗練
- 安全設計と評価
  - 共存とデコンポジション
  - 安全分析(従属故障分析)
  - ハードウェアアーキテクチャメトリクス
  - ソフトウェア安全分析
  - ソフトウェア安全方策
- 既存エレメントの利用
- 安全関連の可用性要求

Confidential Information

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

スコープ拡大

Business Cube & Partners

Confidential Information

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

適用スコープの拡大

- 下記対象物へ適用範囲が拡大し、モペット・特殊車両以外の全ての路上走行車がISO 26262の対象
  - バス
    - 運転席を含んだ座席数9席以上の人、荷物を運ぶことを目的に設計された車両
  - トラック
    - 商品を輸送するように設計された車両、またはシャーシに搭載される設備
  - トレーラー
    - 動力を持たず、けん引車によってけん引されるように設計された車両
  - トラクター
    - セミトレーラーをけん引するように設計された車両
  - モータサイクル
    - 2輪車、または3輪車であって、自重が800kgを超えない車両でモペットは含まない
    - **Part 12**にモータサイクルにISO 26262を適用する場合の要求事項が記載

Confidential Information

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

T&Bに特化した規格要件

- ISO 26262適用範囲外のアプリケーションとのインタフェース　Part 8-15
  - アイテムまたはエレメントのサプライヤ、またはベース車両の製造業者は、アプリケーション側に備える必要がある安全方策を情報として提供する
  - 統合者は適用しなければいけない規格要件に基づいて安全方策を適用

- ISO 26262に準拠して開発されていない安全関連システムの統合　Part8-16
  - 統合者は他の安全規格に対応して開発された安全関連システムが、ISO 26262の要求レベルを満足することを論証
    - 例として
    - パフォーマンスレベル※とASILのマッピング
    - 適用する手法や故障率目標の比較

別の規格(ISO 13849など)が適用されるアプリケーション

ISO 26262が適用されるアプリケーション

※リスクの大きさに基づいて安全関連部に求められる安全性能

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

モータサイクルへの規格適用

- Part12に記述される内容で他規格要件をテーラリング
  - 規模が小さい組織への配慮　確証方策に対する独立性レベルの緩和
  - モータサイクル特有の危険事象におけるコントローラビリティ評価　ー＞ MSIL
  - ISO 26262をモータサイクルに適用　MSIL-ASILマッピング

テーラリング対応マップ

ISO 26262-12:2018		ISO 26262-12:2018
Part2	5.4.2　安全文化	6　安全文化
	6.4.9　確証方策	7　確証方策
Part 3	6　　HARA	8　HARA
	Annex B	Annex B
Part 4	7　　車両統合とテスト	9　車両統合とテスト
	8　　安全妥当性評価	10 安全妥当性評価

MSIL-ASILマッピング

MSIL	ASIL
QM	QM
A	QM
B	A
C	B
D	C

Confidential Information

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

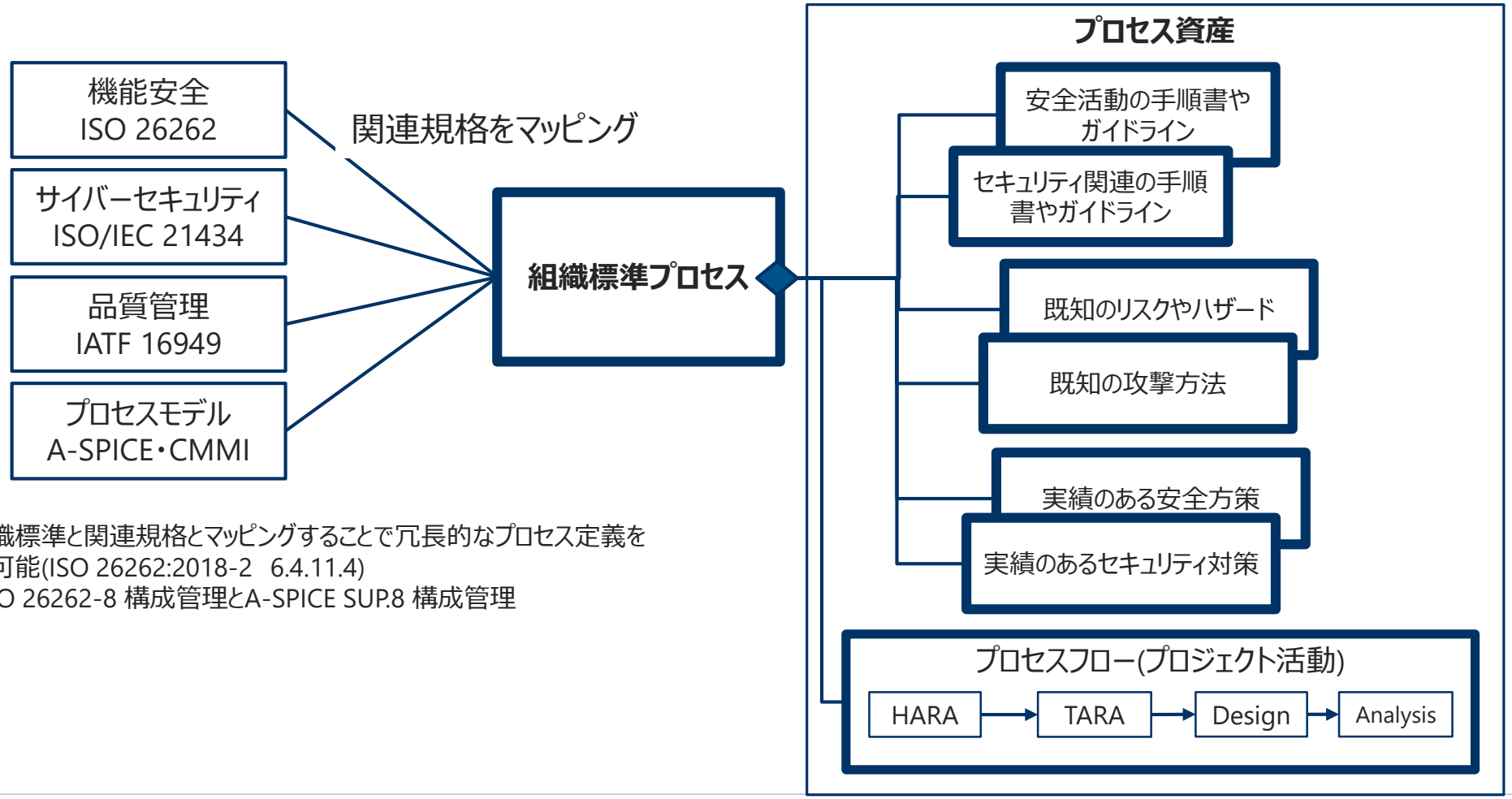
サイバーセキュリティとのコミュニケーションチャネル

- サイバーセキュリティ(ISO 26262-2 Annex E)
  - 安全文化として、組織は機能安全とサイバーセキュリティ対応との間における情報共有手段を考慮しなければならない
    - ハザード分析、リスクアセスメント、脅威分析、脆弱性分析、安全目標、サイバーセキュリティ対策、安全方策
    - セキュリティで保護したい資産　人命(安全)、個人情報、etc.
  - 可能性のある機能安全とサイバーセキュリティ間の関連
    - 共通性のある安全活動とサイバーセキュリティ活動の計画とマイルストーン
    - 市場モニタリングの管理
    - ハザードになりうる脅威の分析
    - 安全目標・コンセプトへの影響判断するため、攻撃が検出された場合の戦略や対策
    - 技術安全要求・安全設計への影響判断するため、サイバーセキュリティ戦略や対策の設計や実装技術
    - ハードウェア、ソフトウェア安全要求達成や設計制約：独立性などへの影響判断するため、サイバーセキュリティソフトウェアやハードウェア設計

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

プロセス定義とコミュニケーションチャネル

- 組織標準プロセス構築時に、関連する規格を踏まえてプロセス定義
- 定義されたプロセスと関連規格要件をマッピングすることで保守性を向上



※組織標準と関連規格とマッピングすることで冗長的なプロセス定義を排除可能(ISO 26262:2018-2　6.4.11.4)
Ex. ISO 26262-8 構成管理とA-SPICE SUP.8 構成管理

Confidential Information

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

目的指向

Business Cube & Partners

Confidential Information

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

機能安全要求に含まれるべき戦略

- 機能安全要求で考慮すべき項目が、ISO/IEC Guide 51のスリーステップメソッドにならって明確化
  - フォールトの回避(1)
    - なるべく失陥や障害が生じないようにすること、完全に回避するのは難しい
    - 多重化、多様設計、安全原則の適用、枯れた技術・部品の適用、State of the artsの適用　など
  - フォールトの検出と制御(2)
  - 安全状態への遷移、安全状態からの遷移(2)
    - 安全原則の一つとして「安全を確認してから使用する」
  - フォールトトレランス(2)
    - 失陥や障害が生じても安全状態が保たれるようにすること
    - 安全関連の可用性要求(Part 10)　など
  - 故障中の機能縮退とドライバー警告との関係性(2)
  - 残存リスク暴露低減のためのドライバー警告(3)
  - 制御性(Controllability)確保のためのドライバー警告(3)
  - 失陥許容時間内におけるエラーハンドリング(2)
  - 制御要求コンフリクト状態における不適切な選択の回避や軽減(2)

リスク低減対策(Guide 51のスリーステップメソッド)
1. 本質的な安全設計を行う
2. 残ったリスクに対して、安全防護や付加保護方策を行う
3. それでも残ったリスクに対しては、使用者に通知する

Confidential Information

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

目的の詳細化

- 5節以降の「*.1 目的」が第1版に比べて明確かつ詳細に
- 規格要件準拠の指向から目的指向(機能安全の達成)へ

- 組織による安全管理の目的(Part2 5.1)
  - 第2版
    - 機能安全達成に有効で、かつ安全に関連する他標準を考慮した安全文化の醸成
    - 機能安全達成に有効な組織標準の確立と運用
    - 安全不履行を解決するためのプロセス確立と運用
    - 安全活動実施に必要な能力管理システムの確立と運用
    - 安全のベースとなる品質管理システムの確立と運用

組織がこの節を実施する目的

  - 第1版
    - 安全ライフサイクルに責任を持つ組織、または安全ライフサイクルの中で安全活動を実行する組織に対する要件を定義する

規格書におけるこの節の目的

Confidential Information

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

目的指向の確証方策

- 確証レビュー、機能安全監査、機能安全アセスメントの実施
  - 目的(Objectives)が達成されているかの観点で確証方策を実施
  - 機能安全監査、アセスメントのスコープや観点が明確化(Part2 6.4.11.4、6.4.12.7)
  - I1以上のドメイン知識を持ったサポートレビュアーの参加が認められる
  - 盲目的な規格準拠型のレビューではなく、目的達成型(規格要件に対して成果物の正確性、完全性、一貫性、十分性、項目)をレビュアーがチェックすることを意図
  - アイテムレベルだけでなく、エレメントレベルでの実施も明記(Part8-5　分散開発も参照)
  - IATF 16949でも同様に目的達成を重視
- アプローチ
  - 各節の目的(Clause x.1 Objectives)およびISO 26262-2 Annex Cを理解
  - 現在の成果物やプロセス、手順で目的が達成できているかを確認
  - 目的達成、機能安全達成が論証できるようなセーフティケースを準備しておく(GSN利用など)
  - 定型チェックリストからオープンクエスチョン型アセスメントへ(A-SPICEアセスメントテクニックも活用)
- セーフティケース
  - **Safety Argumentをサポートするために**作業成果物を一式化　下線が2版で記述追加
  - 安全計画立案を支援するために安全論証を最初に考慮　論証の戦略を計画へ

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

確証方策

確証方策	QM	ASIL A	ASIL B	ASIL C	ASIL D
確証レビュー: アイテムレベルの影響分析	**I3**	I3	I3	I3	I3
確証レビュー:HARA	**I3**	I3	I3	I3	I3
確証レビュー:安全計画	–	**I1**	I1	I2	I3
確証レビュー:FSC	–	I1	I1	I2	I3
確証レビュー:TSC	–	I1	I1	I2	I3
確証レビュー: 統合とテスト戦略	–	I0	I1	I2	I2
確証レビュー: 安全妥当性評価仕様書	–	I0	I1	I2	I2
確証レビュー: 安全分析、従属故障分析結果	–	I1	I1	I2	I3
確証レビュー: セーフティケース	–	**I1**	I1	I2	I3
機能安全監査	–	–	I0	I2	I3
機能安全アセスメント	–	–	I0	I2	I3

ツール認定や使用実績による証明が対象外

Confidential Information

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

ISO 9001・TS 16949対応に見られる企業課題

- ISO 9001認証取得したが、品質、コスト、生産性、顧客満足度などのパフォーマンスが改善しない。経営に役に立っていない。
- 内部監査も適合性の監査から有効性の監査へと言われているが、有効性の監査のために最も効果的なプロセスアプローチ監査が行われていない。
- ”決められたことを行っていない、ルール通りになっていない”といった内部監査指摘が多い。すなわち適合性の監査に終わっており、有効性の監査になっていない。
- 品質マネジメントシステムがプロセスアプローチで適切に運用されておらず、パフォーマンスの改善につながるシステムになっていない。

規格適合を目的とした品質マネジメントシステムの運用の結果、
形骸化が見られ、本来の導入効果が得られない結果となっている

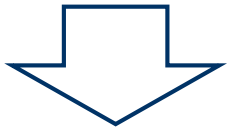
Confidential Information

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

IATF 16949:2016の特徴

- IATFメンバーのOEMが持つ顧客固有要求事項の反映
  - IATF OEMの要求事項が色濃く反映
  - IATF 16949に含まない顧客固有要求事項(APQP、VDA 6.3など)は引き続き考慮

- 運用パフォーマンス、顧客フィードバックをより重視
  - QMSの成果が表れないことを問題視→プロセス評価指標の監視



顧客要求達成、および製品の品質保証を念頭におき、引き続きプロセスアプローチを重視、目的達成型の**魂のこもったプロセス改善活動(＝継続的改善)**が求められる

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

目的達成の例(Part6 Clause7　SWアーキ設計)

Business Cube & Partners

- ソフトウェアアーキテクチャ設計の目的(7.1)
  - ソフトウェア安全要件、および他のソフトウェア要件を準拠するアーキ設計を行うこと
    - システマティックフォールトにより安全要件逸脱が起こる設計であってはいけない
  - アーキテクチャがソフトウェア安全要件の準拠に適していることを検証すること
  - ソフトウェアの実装や検証をサポートすること

何のために

- 要求事項(7.4.1)
  - システマティックフォールトを回避するためのアーキテクチャ特性を扱うために、適切な記法をテーブル1から選択
    - f)抽象化　　大事な特性を取り出す(初期化・終了処理をパッケージにするなど)
    - g)カプセル化　　クリティカルなデータを隠蔽し、不用意にアクセスさせない

何のために

- ソフトウェアアーキテクチャ設計書は、以下の記法から適切な組合せを選択して記述すること
  - 自然言語
  - 準形式記述(UMLやSimulinkなどモデリング言語を使用)

記法選択が目的のようなプロセス定義で、設計品質は現場任せでは目的達成できない
7.4.3で与えられる設計原則を適用、表現・理解しやすい記法を選択するように導くこと
加えてモデルベースアプローチを採用する場合はISO 26262-6:2018 AnnexB.2.3の評価項目も参照のこと

Confidential Information

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

安全設計とその評価(安全分析と従属故障分析)

Confidential Information

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

ASILデコンポジション、エレメント共存の説明強化

- ASILデコンポジション、エレメント共存を適用したアーキテクチャ例がPart9 AnnexBに追記
- 従属故障とASILデコンポジション・エレメント共存の関連記述がPart 9　7.2に追記
- エレメントの共存要件
  - 同一エレメント内に存在するQMもしくは低次ASILサブエレメントが高次ASILエレメントに配置された安全要件を侵害しない(カスケード故障がない)
- ASILデコンポジションの要件
  - 冗長された安全要件はそれぞれ独立でデコンポジション前の安全要件を満たすことができる
  - 冗長化された安全要件間でカスケード故障がない(上記参照)、単一故障により冗長化された安全要件がいずれも満たせなくなることがない(共通原因故障がない)

エレメント共存条件
サブエレメント1.2はサブエレメント1.1の安全要件を侵害しない
(赤矢印がない)

B.1 Example architecture

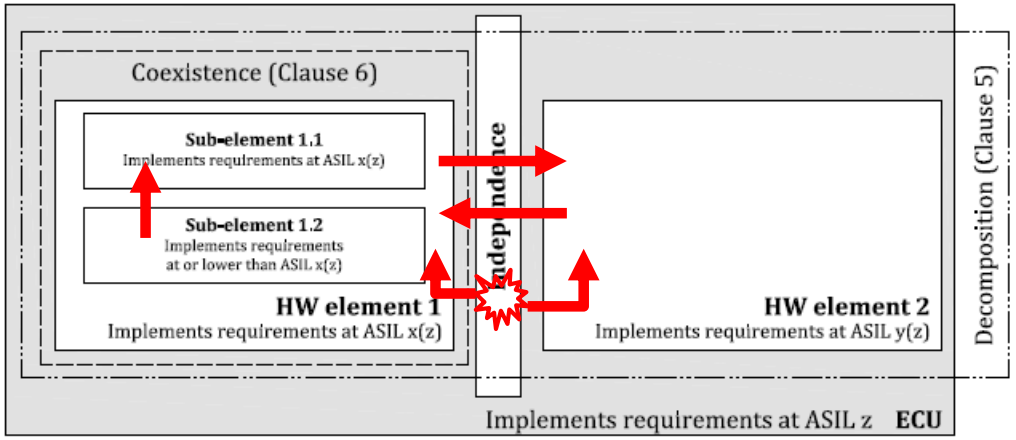


Figure B.1 — Coexistence and decomposition in an example architecture

ASILデコンポジション成立条件
エレメント1、2は干渉しない、共通原因による故障も存在しない
(赤矢印がない)

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

アーキテクチャ設計におけるASILデコンポジション

- ASILデコンポジションに関する記載が移動
  - ISO 26262-4:2011 6.4.3　技術安全要求の仕様化
  - →　ISO 26262-4:2018 6.4.3.6　システムアーキテクチャ設計
  - ハードウェアは第1版からハードウェア設計　7.4.1.3に記載
  - ソフトウェアは第2版でもソフトウェア安全要求の仕様化　6.4.3に記載…

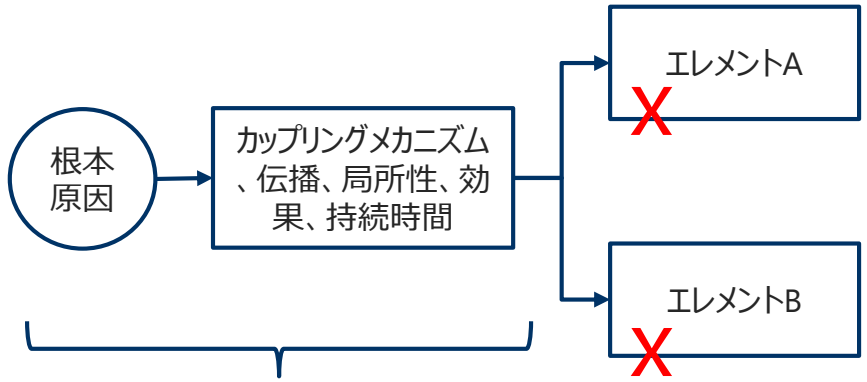
- ASILデコンポジションはアーキテクチャ設計で適用
  - ASILデコンポジションは安全要件を冗長な安全要求にデコンポジションすること・・だが
  - 安全要求を同種・異種冗長化されたアーキテクチャエレメントに分割
  - 独立性の特性(Safety Property)を冗長化されたエレメント間に設定
  - 従属故障分析によりASIL デコンポジション成立を評価

Confidential Information

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

従属故障分析

- 安全分析と従属故障分析の関係(Part 11 4.7.2)
  - 安全分析：SPF,DPF,MPF(脆弱部)を特定、安全機構設計、メトリクス評価を支援
  - 従属故障分析：安全機構の有効性が従属故障イニシエータによって影響されないことを保証することで安全分析を補完する
- Coupling Factorの識別(Part 9 C7、Annex C、Part 11 C4.7に具体例が記載)：従属故障を引き起こす要因となりうるものの識別が従属故障分析の完全性を支援
  - 共有リソース
  - 共通の入力情報
  - 機能間のコミュニケーション
  - 同一型のコンポーネント
  - 環境依存の影響(不十分な耐環境性)
  - 想定外のインタフェース
  - 系統故障による結合

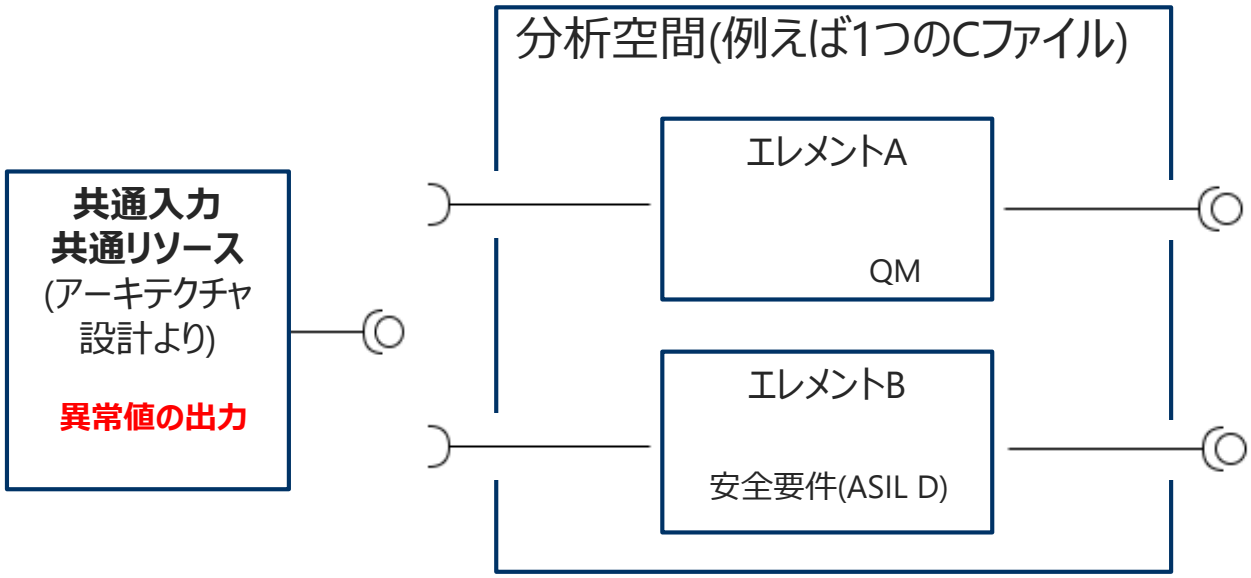


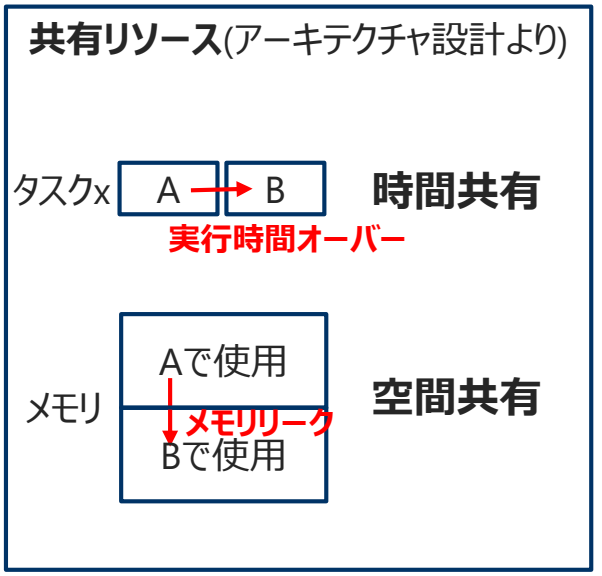
分析対象のエレメントを分析空間においた場合のつながり方(カップリングファクタ)と根本原因(イニシエータ)を特定する

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

ソフトウェアにおける従属故障分析例

- 従属故障分析を行う分析空間を定義し、その領域におけるアーキテクチャからカップリングファクタ(黒太字)、従属故障イニシエータ(赤太字)を同定する
- 従属故障イニシエータの影響が、安全目標・安全要件の侵害に至らないかを分析する





エレメント共存、デコンポジションを成立させたい領域

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

メトリクスによるハードウェアアーキテクチャ評価

- ハードウェアエレメントの故障モード、有効性のある安全機構およびDCの妥当性の主張例
  ISO 26262-5:2018, ISO 26262-11:2018
- 故障率のソース
  - IEC 62380が2017年に廃版、IEC 61709が後継規格
  - 利用時の課題として、基礎故障率λrefを準備しないと故障率が算出できない
  - 半導体の基礎故障率の算出事例はPart 11に詳述
  - λrefに独自データ(フィールドデータ)を使用する場合も70%以上の信頼度が必要？
  - SN29500が追加(≒IEC61709、基準故障率はSiemens社から与えられている)
  - エキスパート判断時はリファレンスとしてSAE J1211(EE部品の信頼性評価ハンドブック)が活用可能
- メトリクスに故障率データが十分な証拠として利用できない場合は、安全機構のダイアグカバレッジで論証の代替が可能
  - 単一フォールトのDC(残存フォールト)がアイテムのSPFM目標値(90%~)以上を達成
  - 多重フォールトのDC(レイテントフォールト)がアイテムのLPF目標値(60%~)以上を達成
- レイテントフォールトの取り扱い例(8.4.8　代替手段b or 代替手段cを適用する事例)がAnnex Hに追加

Confidential Information

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

ランダムハードウェア故障の残存リスク評価(PMHF、EEC)

- PMHFの要求事項は基本的に変わらない
  - 単一フォールト、残存フォールトは専用方策が必要　ISO 26262-5:2011　から
  - 単一フォールト、残存フォールトの故障率は専用方策を適用する、または
  - 厳しめのソースを使い、0.01FITの達成(ASIL D)、0.1FITの達成(ASIL C)が必要

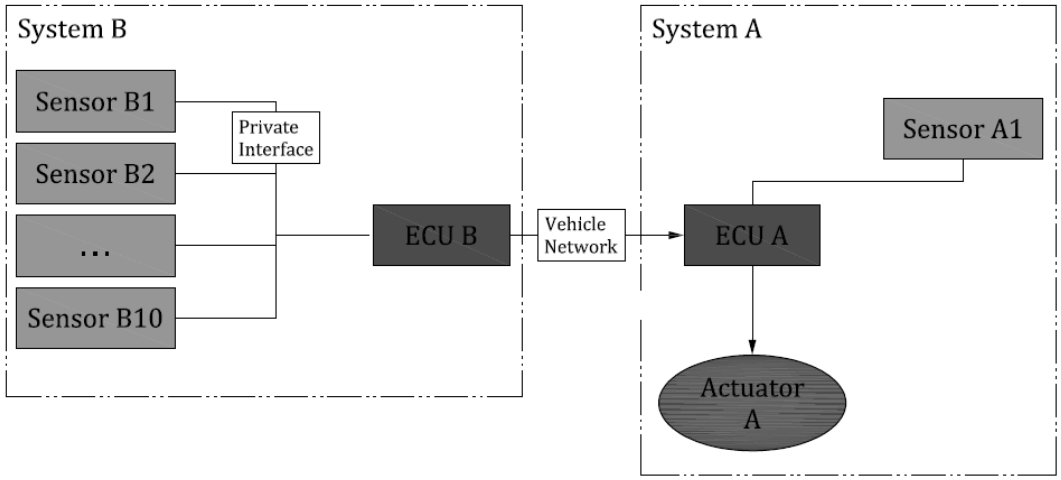
- EECの要求事項は変更あり
  - 従来の要求事項に加えて
  - DPFの故障率は0.01FITの達成(ASIL D)、0.1FITの達成(ASIL C)が必要
  - 単一フォールト、残存フォールトの故障率は専用方策を適用する、または
  - 厳しめのソースを使い、0.01FITの達成(ASIL D)、0.1FITの達成(ASIL C)が必要
  - 下記2項は9.4.1.2、9.4.1.3がPMHFとEEC共通項と解釈できるが、EECの要件と不一致しているため共通理解が必要

Confidential Information

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

複数システムで構成されるアイテムに対するPMHF目標

- 安全目標侵害に至る残存リスク　PMHFに関するガイド(Annex G)
- 第1版での私の理解：PMHF目標値はアイテムとして評価
- 第2版で複数システムで構成されるアイテムの目標値設定が明確化
- 1桁を超えない限りそれぞれのシステムに目標値を割り付けられる
- ＝ASIL Dの場合、最大10システムまではそれぞれ10FITが適用可能



システム構成例(Annex G)

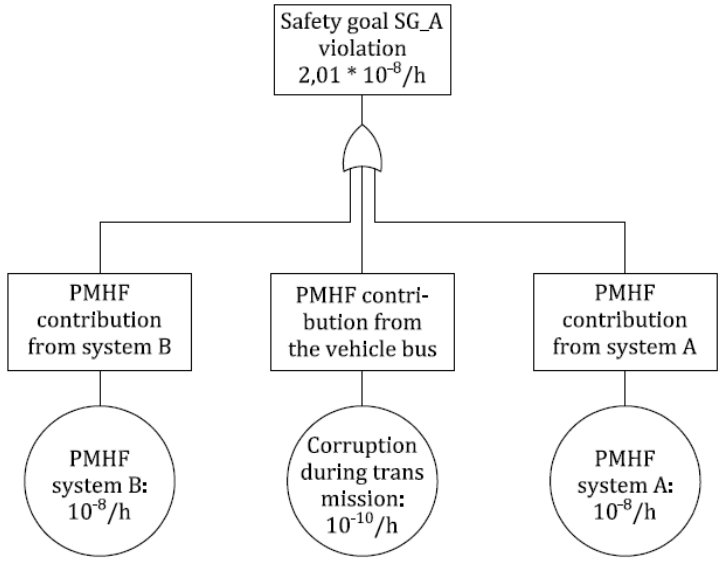


Figure G.3 — PMHF target allocation

PMHF目標値の配置とトータルPMHF

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

ソフトウェア安全分析・従属故障分析の解説強化

- ソフトウェア安全分析と従属故障分析(Annex E)
  - 第1版では手法に関するガイダンスがなかったが、第2版で下記説明やガイダンスが追加
  - Part 6 Annex D、Part 9 Annex Cのカスケード故障要因やカップリングファクタ例やPart 6 Annex E TableE.1、E.2のガイドワード例

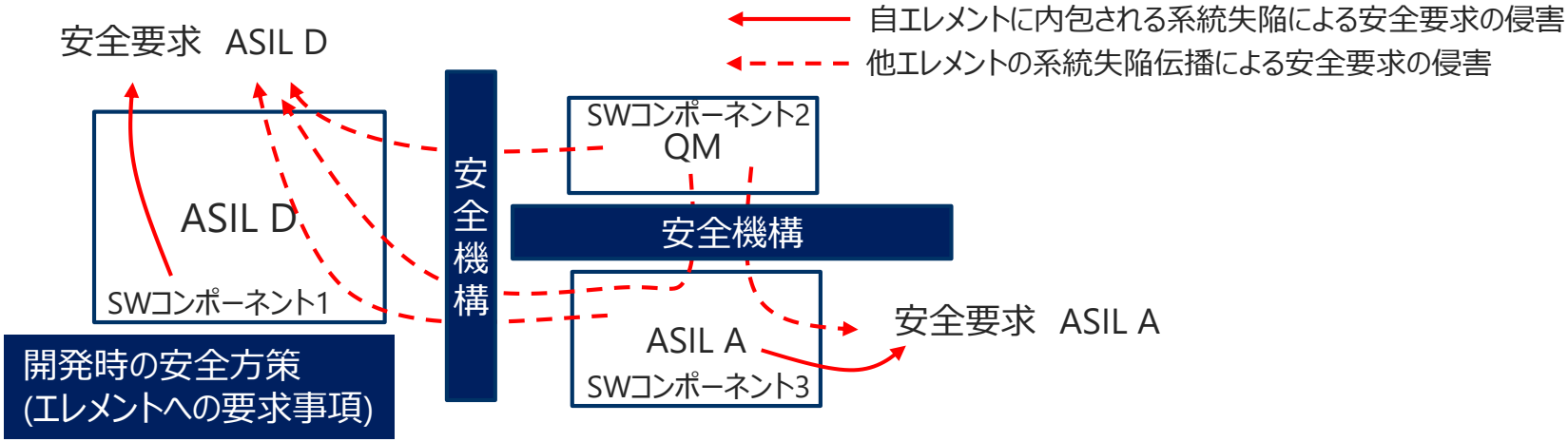
- 実施目的：ソフトウェアに割り付けられる安全要件の機能性、特性の評価
  - エレメントに要求される機能や属性に対する障害、故障の因果分析
  - 安全要件侵害につながる故障ネットや設計の脆弱性の識別
  - エレメント共存とASILデコンポジションの成立性証明

- ソフトウェアアーキテクチャレベルで実施
  - よく聞く質問：なぜソフトウェアに安全分析が必要？バグを見つけたら直せばいい
  - ユニット設計レベルの系統失陥は開発時の安全方策でカバー：ASILがついたエレメントに有効
  - QMエレメントも従属故障がないこと＝＞すべてのエレメントを同一ASILで開発を意味

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

ソフトウェア安全分析と安全機構の必要性

- ソフトウェアアーキテクチャ設計時には上位安全要件の実現に加え、安全要件の侵害に配慮する必要がある
- 系統失陥により安全要件を侵害する可能性がある場合は安全機構を追加、あるいはエレメント共存、ASILデコンポジションを再考することが必要
  - SWコンポーネント1にはASIL Dの安全要求が割り付けられている
  - SWコンポーネント2は安全要件が割りついていない
  - SWコンポーネント3にはASIL Aの安全要求が割り付けられている



- 安全分析の結果、AnnexE.4の安全方策決定戦略の考慮点に基づけば必ずしも安全機構の実装が必要でない(考慮点に関する論拠がしっかりしていればの話)

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

ソフトウェア　安全機構

- 安全分析(従属故障含む)の結果、以下のうち、適切な安全機構の実装が必要
  - エラー検出
    - 入出力データ範囲チェック
    - データの妥当性チェック(信号間の相関チェックなど)
    - データエラー検出(データエラー検出コード、多重領域への記憶)
    - ウォッチドッグ監視
    - プログラムフローモニタリング
    - 多様化設計
    - 安全関連との共有リソースへのアクセス違反アクセス制御
  - エラーハンドリング
    - 安全状態を維持するための機能停止
    - 静的なリカバリー制御
    - 影響最小化のための縮退制御
    - 同種冗長・異種冗長設計

Confidential Information

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

ソフトウェア　安全方策

- 従属故障低減に向けた方策が追加
  - 5.4.3　ガイドラインでカバーされるトピック
    - 並列性指向　追加(全ASILに推奨)
      - 共通リソース利用による従属故障のための並列性と排他制御
  - 7.4.3　アーキテクチャ設計原則
    - コンポーネント間の空間的隔離　追加(ASIL Dに強く推奨)
    - 共有リソースのマネジメント　追加(全ASILに強く推奨)
  - 7.4.14　アーキテクチャの検証
    - スケジューリング分析　追加(ASIL C,Dに強く推奨)
- 系統故障低減(およびアジャイル)に向けた方策追加
  - 9.4.2　ソフトウェアユニットの検証
    - ペアプログラミング　追加(全ASILに推奨)
    - 抽象解釈に基づく静的解析が意味論解析に置き換え(全ASILに推奨)
  - 10.4.2　統合ソフトウェアの検証手法
    - コントロールフローおよびデータフローの検証追加　(ASIL C,Dに強く推奨)
    - 静的コード解析(ガイドラインへの準拠など)　追加(全ASILに強く推奨)
    - 抽象解釈に基づく静的解析　追加(全ASILに推奨)

Confidential Information

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

まとめ：基本的な安全設計活動

- 安全要件の仕様化
  - 上位要件、コンセプトを受けて、開発レベル(システム・HW・SW)の安全要件仕様化
- 安全アーキテクチャ設計
  - (必要に応じてフォールト、ハザード要因識別のための安全分析)
  - 安全機構の設計、安全方策の適用
  - ASILデコンポジション、エレメント共存の戦略化と適用
  - 安全特性(無干渉、独立性)を考慮したアーキテクチャ設計
- アーキテクチャ評価
  - 安全分析によるアーキテクチャ評価(ハザード要因の識別、安全機構の有効性)
  - 従属故障分析によるASILデコンポジション、エレメント共存の成立性評価
  - メトリクスによる定量的アーキテクチャ評価と残存リスクの定量評価
- 検証
  - 安全機構の有効性、安全要求の準拠性に関する根拠の提供

Confidential Information

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

既存エレメントの利用

Confidential Information

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

安全活動における役割階層化

- 完成車メーカー
  - システムインテグレータ＝アイテムとしての統合
- システム
  - システムインテグレータ
- ソフトウェア
  - ソフトウェアインテグレータ
  - ソフトウェアエレメントプロバイダ(既存のソフトウェアエレメント)
- ハードウェア
  - ハードウェアインテグレータ
  - ハードウェアエレメントプロバイダ(既存のハードウェアエレメント)
  - 半導体IPプロバイダ

Confidential Information

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

ハードウェアの評価(ISO 26262-8:2018 Clause13)

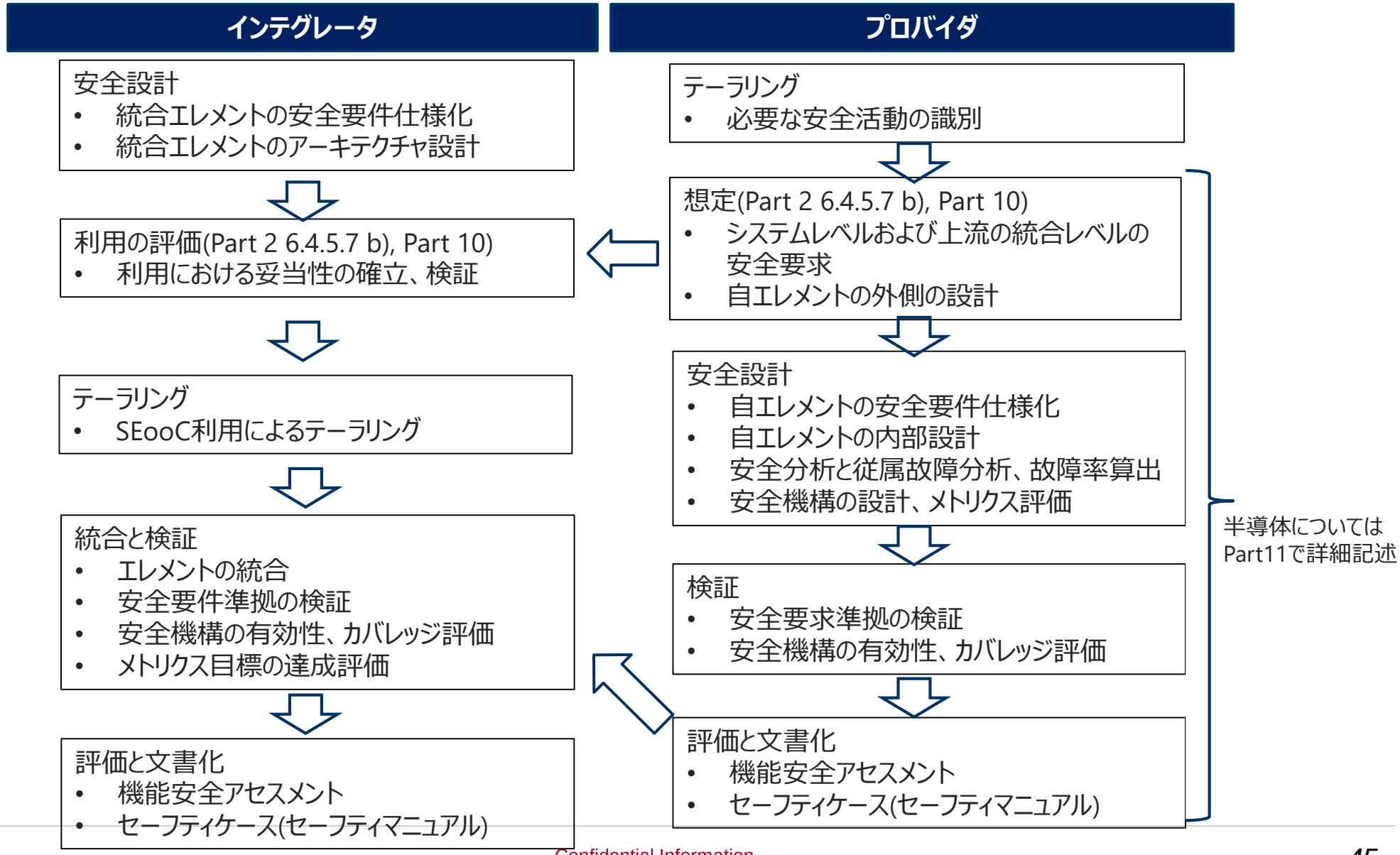
- 安全関連製品に組み込まれる汎用ハードウェア製品(以下2種)に対してPart5適用の代わりとなりうる評価方法を提供
  - COTSのハードウェアコンポーネントや部品
  - ISO 26262準拠で開発されていないカスタムハードウェアコンポーネントや部品

Class I	Class II	Class III
安全機構を持たない、内部の実装詳細が分からなくても安全関連故障モードが特定できる部品 • 抵抗 • キャパシタ • トランジスタ • ダイオード　など	安全機構を持たない、いくつかの動作モードやパラメータを持ち、内部の実装詳細が分からなくても系統故障がドキュメントから想定可能な部品 ・燃料圧力センサ ・温度センサ ・スタンドアロンADC　など	安全機構を持つ、複数の動作モードやパラメータをもち、内部詳細が分からないと安全分析できない複雑な部品 ・MCU ・MPU ・DSP　など
部品単体での評価は不要 Integratorが、Class I部品が組み込まれたハードウェアをISO 26262-5に準拠して開発すればよい	分析とテストからSPEC通りの性能であること、意図通りに使用できることを評価して、使用可能 評価方法は第1版と変わらず	Class IIの評価に追加して、追加方策により残存リスクが低いことの論証が必要 ※次世代製品ではISO 26262準拠の開発が求められる

Confidential Information

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

SEooC開発フロー



Confidential Information

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

半導体へのISO 26262適用(Part 11)

- 半導体開発時に適用しなければいけないPart(Part5など)はあるものの、半導体サプライヤの方はまずPart 11を読むとおおよその安全活動が理解できる規格
- コンテキストによらない安全関連の半導体に対する安全指向の説明
  - 基礎故障率の計算方法
  - 従属故障分析の解説と事例
  - 半導体IPの取り扱い
    - SEooCとしてのIP　Part 10、COTSとしてのIP、コンテキストの中で開発されるIP
- 安全関連の半導体の開発フローをモデル化
  - 半導体内部のフォールトモデルの識別
  - 故障モードの識別、故障モードへの故障率分配
  - 定性的、定量的な安全分析、従属故障分析
  - 安全機構の設計、実装
  - 系統失陥回避のための安全方策
  - 検証
  - 文書化(セーフティケース・セーフティマニュアル)
- 主要半導体のユースケース記述

Confidential Information

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

安全関連の可用性要求

フェールオペレーションを目指して

Confidential Information

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

安全関連の可用性要求

- フォールトトレランス
  - 障害に対する耐性
  - 指定されたフォールトの存在下で指定した機能を提供する能力(ISO 26262-1:2018)
- 例として、電動化された機能の停止時の残存リスク
  - 電動機構(モータ＋ギア)で倍力して操作アシストする機能が停止、倍力失陥した状態でドライバーによる残存リスク低減が困難であればフォールトトレランスを考える
    - 油圧パワステー＞電動パワステ
    - 油圧ブレーキー＞電動ブレーキ
  - 電源失陥時の機能可用性、走行シチュエーションと安全状態維持に必要な性能を考慮して選択。これらの方策はASIL対応能力が求められる
    - メカニカルバックアップ？　－＞　アザーテクノロジー
    - サブ電源？　－＞　残存リスク(ASIL)に応じた安全方策
    - 別システムによる代替制御？　－＞　同上
    - 車両動作状態の制限(車速制限はS,Eが下がりリスク低減)　－＞　同上

Confidential Information

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

ISO 26262運用上の提案

機能安全実装支援の一例

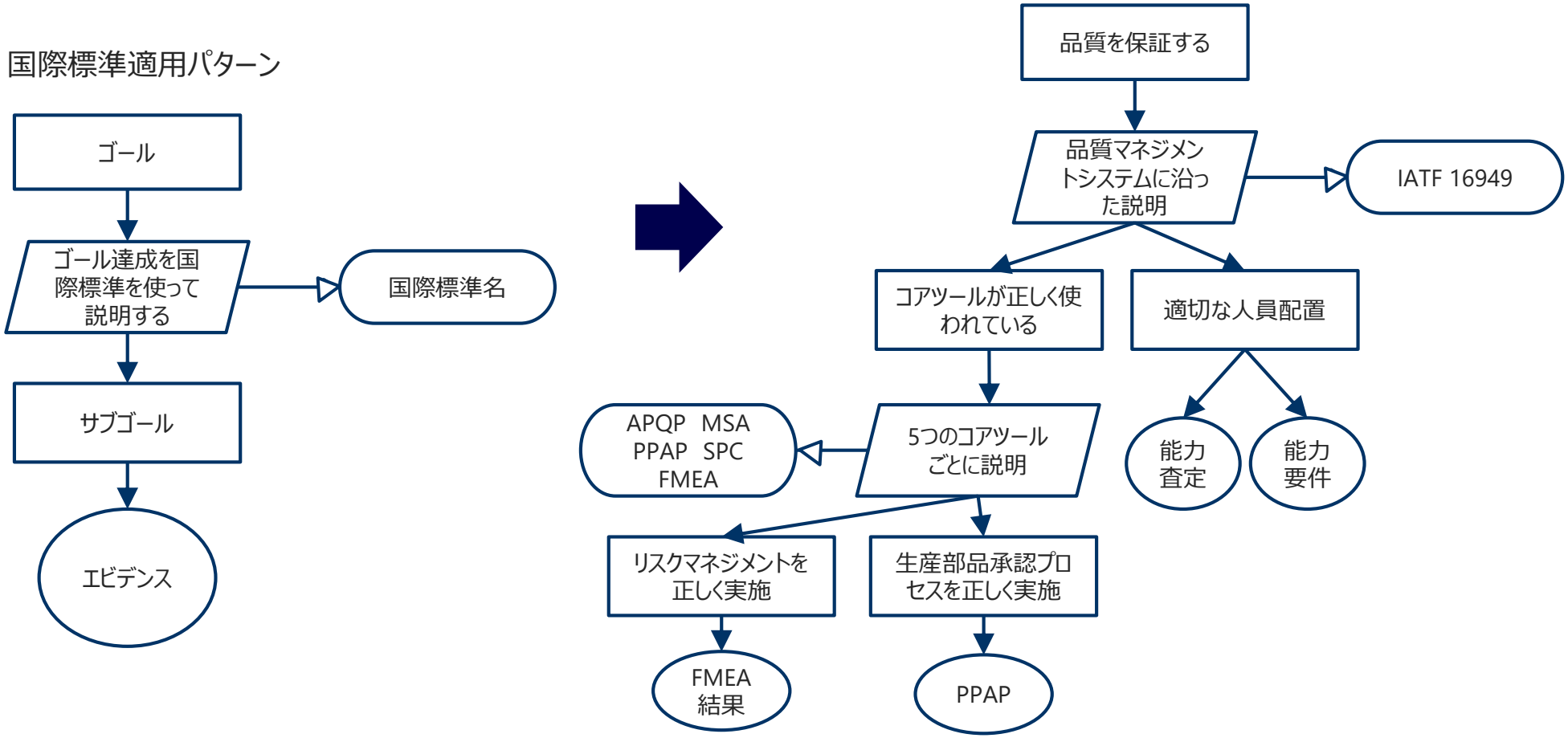
Business Cube & Partners

Confidential Information

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

GSNを用いた論証テクニック

- パターン化
  - ある論証構造を汎化・標準化して論証をパターン化＝論証の体系化

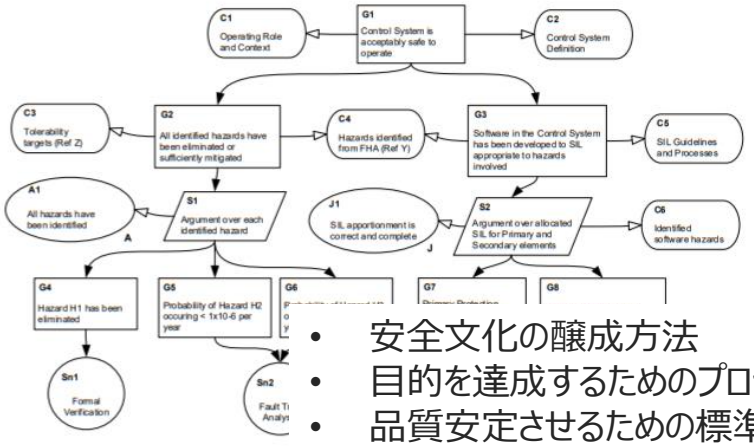


Confidential Information

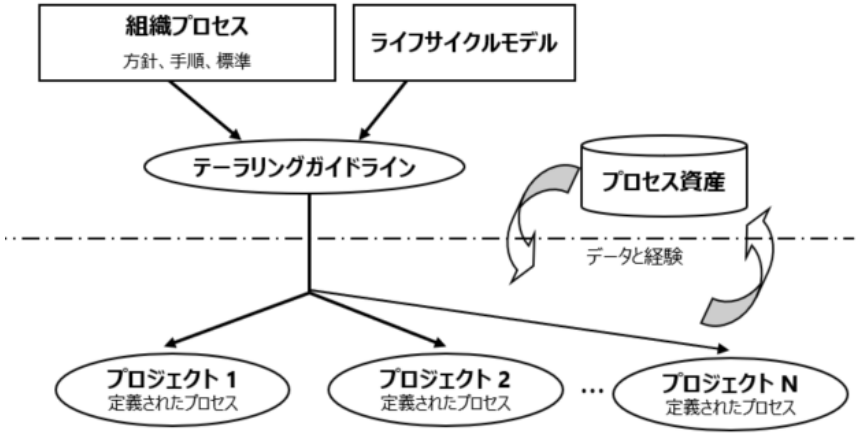
Copyright 2019 Business Cube & Partners, Inc. All rights reserved.

安全論証スキームの活用

論証ゴール: ISO 26262の目的が達成できる

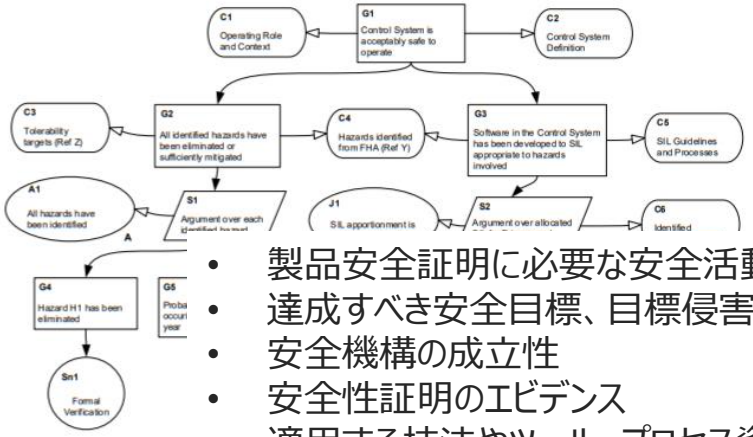


- 安全文化の醸成方法
- 目的を達成するためのプロセス定義
- 品質安定させるための標準や手順の提供
- 能力査定やトレーニングに関する仕組み



スキームをベースに組織標準を策定

論証ゴール: 製品の残存リスクは許容レベルに低減されている



- 製品安全証明に必要な安全活動
- 達成すべき安全目標、目標侵害に至る要因
- 安全機構の成立性
- 安全性証明のエビデンス
- 適用する技法やツール、プロセス資産

スキームをベースに安全計画を策定

Confidential Information

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

体系的FMEAの活用

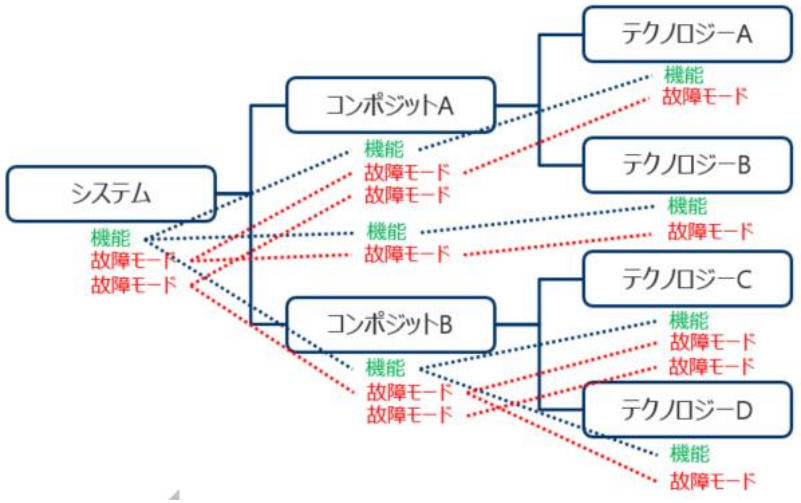
- 特徴
  - FTAの要素(故障ツリー)をもった体系的FMEA
  - エレメントのFaultが上流のFailureへ至る故障連鎖をツリーで可視化、分析・論証しやすい
  - デザインFMEAと工程FMEAのシームレスな分析が可能
  - 統合者と供給者で共同作業、整合が容易

AIAG and VDA FMEAの6Step(リリース版は7Stepになる予定)

System Analysis			Failure Analysis and Risk Mitigation		
1st Step 分析対象の定義	2nd Step 構造の分析	3rd Step 機能の分析	4th Step 故障の分析	5th Step リスク評価	6th Step 最適化
Project identification	System structure for a product or elements of a process	Overview of the functionality of the product or process	Establishment of the failure chain (potential Failure Effects, Failure Modes, Failure Causes) for each product or process function (step)	Assignment of Prevention Controls (existing and/or planned) to the Failure Causes and Failure Modes	Identification of the actions necessary to reduce risks
Project plan	Visualization of the analysis scope using a structure tree or equivalent: block diagram, boundary diagram, digital model, physical parts, or process flow diagram	Visualization of product or process functions using a function tree (function net), function matrix parameter diagram or process flow diagram	Visualization of product or process failure relationships (failure nets and/or the FMEA worksheet)	Assignment of detection controls (existing and/or planned) to the Failure Causes and Failure Modes	Assignment of responsibilities and deadlines for action implementation
Analysis boundaries: What is included and excluded from the analysis	Identification of design interfaces, interactions, close clearances, or process steps	Association of requirements or characteristics to functions and functions to system or process elements	Creation of failure structures by linking the failures in the failure chain	Rating of Severity, Occurrence and Detection for each failure chain	Implementation and documentation of actions taken
Identification of baseline FMEA with lessons learned		Cascade of customer (external and internal) functions with associated requirements	Identification of product noise factors or process sources of variation (4M) using a fishbone diagram, parameter diagram, or failure network Collaboration between customer and supplier (Failure Effects)	Collaboration between customer and supplier (Severity) Action Priority (AP)	Confirmation of the effectiveness of the implemented actions Assessment of risk after actions taken Continuous Improvement of the product and process
Basis for the Structure Analysis step	Basis for the Function Analysis step	Basis for the Failure Analysis step	Basis for the record of failures in the FMEA form and the Risk Analysis step	Basis for the product or process Optimization step	Basis for refinement of the product and/or process requirements and prevention / detection controls

出典元：VDA QMC　FMEA Alignment VDA and AIAG

アイテムー＞システムー＞エレメントー＞工程とシームレスな故障連鎖分析が可能

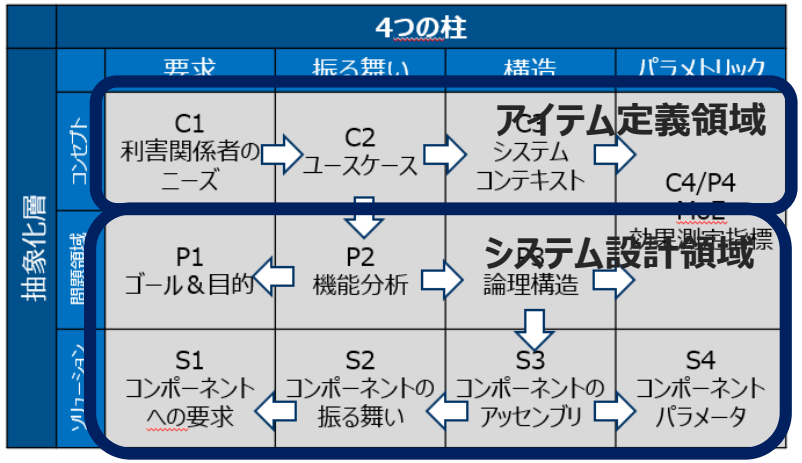


※IATFで参照しているAIAGのFMEAマニュアル ver.4は、2019年5月にAIAG and VDA FMEA Handbookとして上記内容をベースに改定が予定されています。AIAGのHPより本件に関するホワイトペーパーが入手可能

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

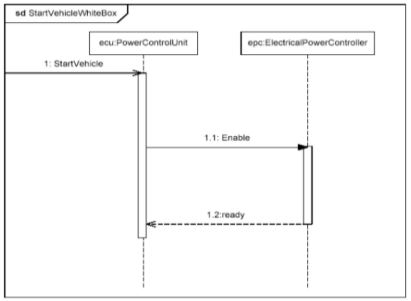
システムモデルの活用

Business Cube & Partners

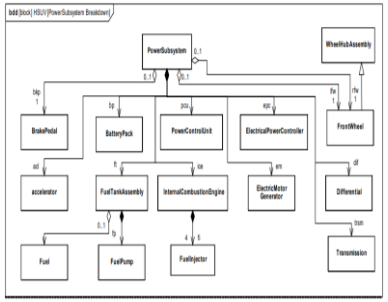


※Dassault Systems社様(No Magic)のModel Based Systems Engineering with MagicGridより出典

【アーキテクチャ設計】
モデルによるシステム分析・設計



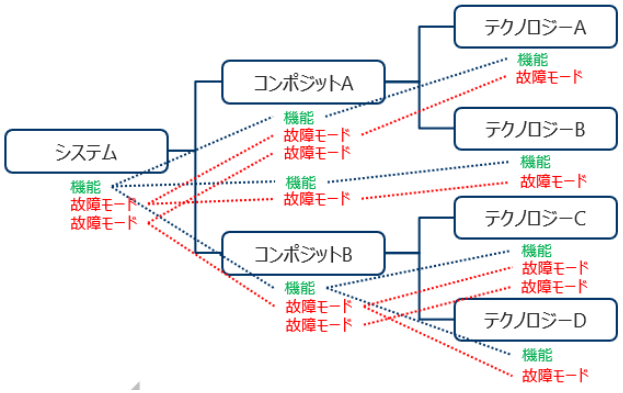
振る舞い図による機能分析



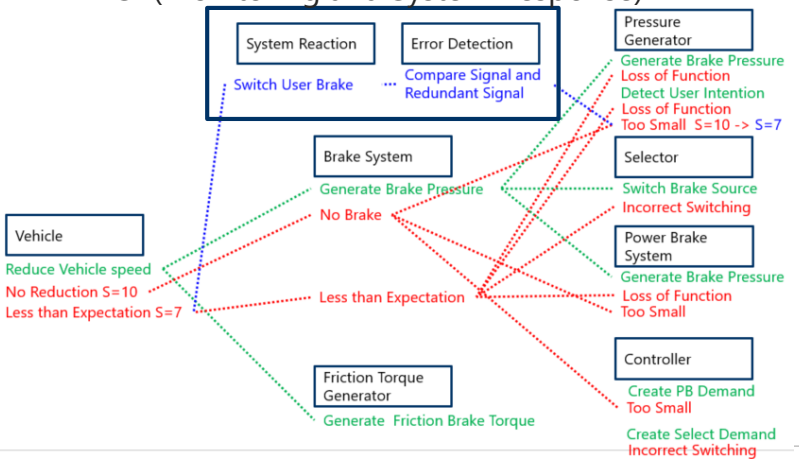
構造図による構造分析

設計モデル要素を安全分析モデルに反映

【アーキテクチャ評価】
VDA FMEAによる安全分析と対策効果の確認



MSR(Monitoring and System Response)



Confidential Information

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

Biz3　新・機能安全ソリューションのご紹介

Business Cube & Partners

Confidential Information

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

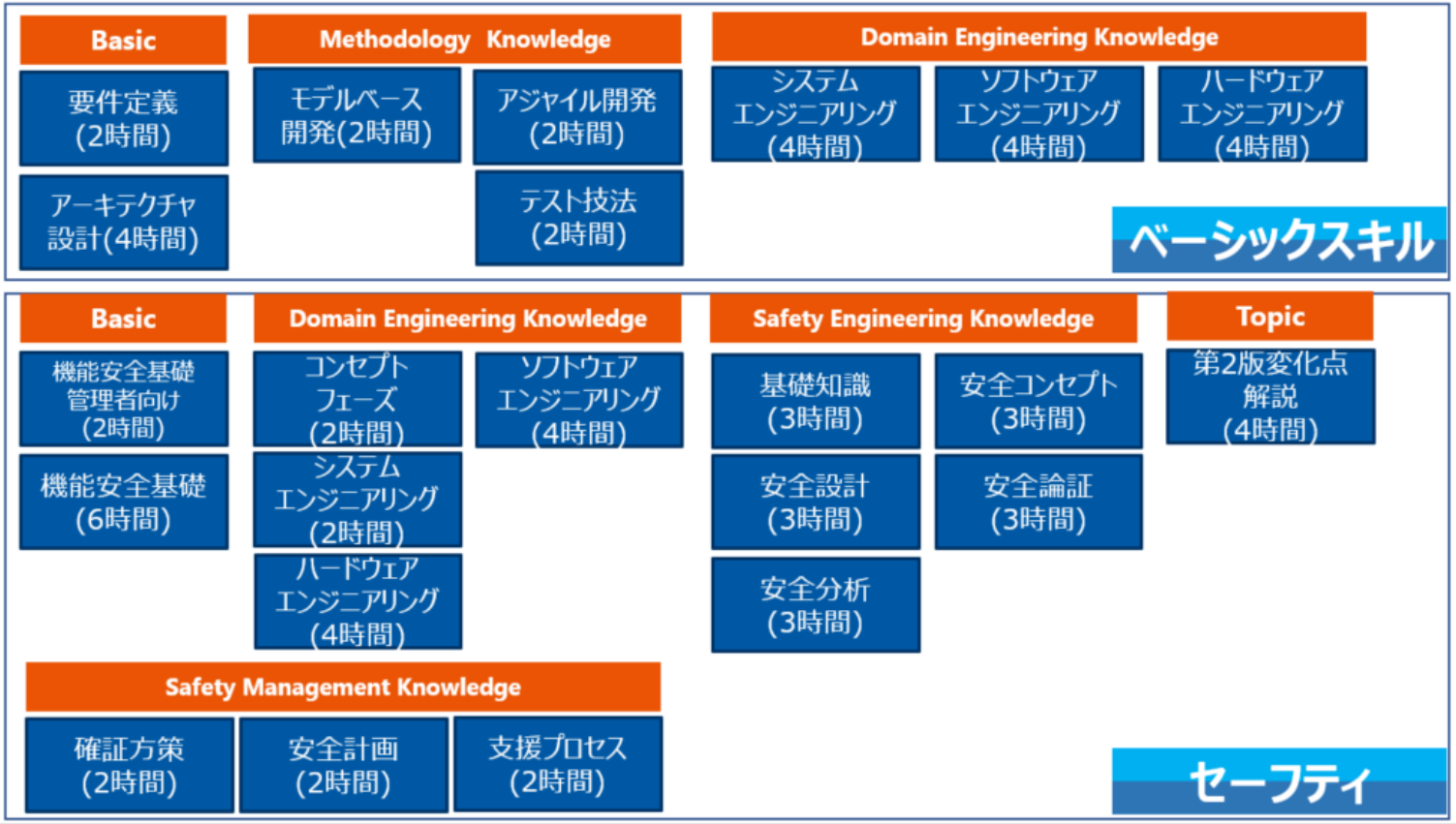
新・機能安全ソリューションのご案内

- 新・ISO 26262　機能安全実装支援コース
- 新・ISO 26262実践ガイドブック

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

新・ISO 26262　機能安全実装支援コース

- トレーニングのモジュール化
  - 規格理解から、実践するための技法解説など、お客様のニーズに合わせてモジュールを組み合わせたトレーニングパッケージをご提供
  - 目的に合わせてエンジニアリングのベーシックスキルとセーフティのスキルを組合わせ可能



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

新・ISO 26262　機能安全実装支援コース

Business Cube & Partners

トレーニングコース

マネジメント層向け ショートコース	機能安全基礎 管理者向け (2h)				
初級・新人教育向け 1日コース	機能安全基礎 (6h)				
セーフティエンジニア育成 2.5日コース	基礎知識 (3h)	安全設計 (3h)	安全分析 (3h)	安全 コンセプト (3h)	安全論証 (3h)
システムエンジニア育成 2日コース	【ベーシック】 要件分析 (2h)	【ベーシック】 アーキテクチャ 設計(4h)	【ベーシック】 システム エンジニアリング (4h)	【セーフティ】 システム エンジニアリング (2h)	
安全管理者育成 1日コース	基礎知識 (3h)	安全論証 (3h)	安全計画 (2h)	確証方策 (2h)	支援プロセス (2h)

Confidential Information

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

新・ISO 26262実践ガイドブック

- 第2版対応
- トレーニングモジュールと連動した章構成

ISO 26262 実践ガイドブック シリーズ

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

Business Cube & Partners

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

Confidential Information

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