機能安全規格ISO 26262の概要と特徴

2012年4月

株式会社レンタコーチ

http://www.rentaco.jp/

概要

◆受講対象者
- 安全設計に関する基本知識を持つソフトウェア技術者
- 同じく、ソフトウェア開発部門のマネージャ

◆習得事項
- ISO 26262の概要と特徴
- 機能安全要求を定義する手順と手法
- 開発フェーズにおいて推奨されている開発手法

◆関連講座
- ソフトウェア安全設計入門

内容

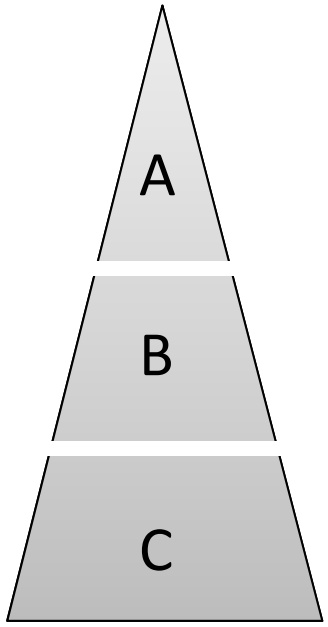
1. ISO 26262の特徴と構成
2. 機能安全マネジメント
3. 主要プロセス
4. 安全要求定義に関するプロセス群
5. 開発フェーズにおける推奨手法
6. 支援プロセス等
7. IEC 61508との比較による特徴

1. ISO 26262の特徴と構成

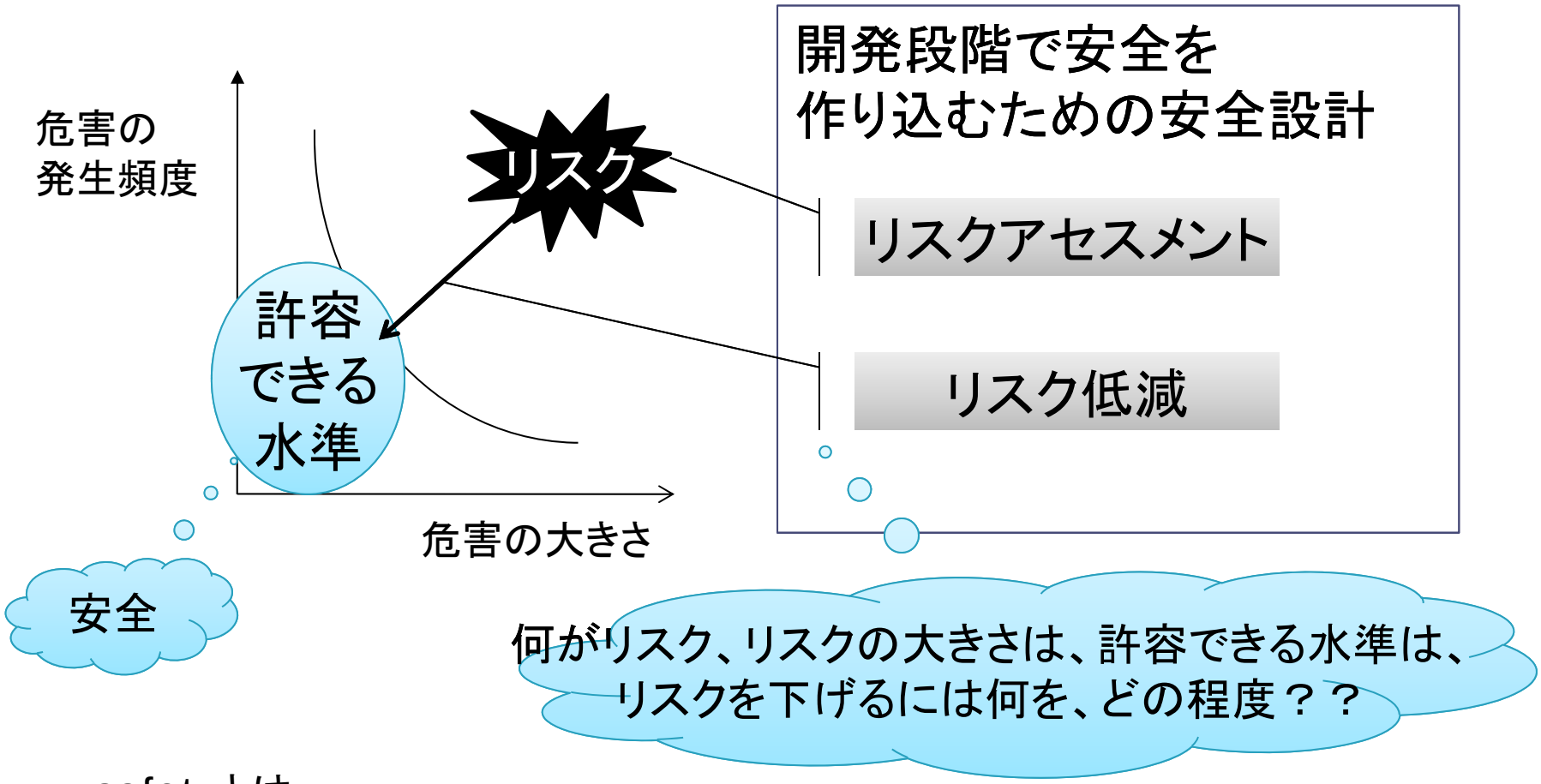
- 特徴
- 規格書の構成

国際安全規格の体系

- ◆ 機械系はISO、電気系はIEC
- ◆ ISO/IECガイド51に準拠
- ◆ A規格：基本安全規格
  - ■ ISO12100：基本概念、設計のための一般原則
  - ■ ISO14121:リスクアセスメント原則
- ◆ B規格：グループ安全規格
  - ■ ISO13849-1:制御システム安全規格
  - ■ IEC61508:機能安全規格
- ◆ C規格：産業別安全規格
  - ■ 航空機：DO-178B
  - ■ 原子力：IEC61513
  - ■ プラント制御：IEC61511
  - ■ 鉄道：IEC62278、IEC62279(ソフトウェア関係)
  - ■ 自動車：ISO26262
  - ■ 医療機器：IEC62304



リスクに基づく安全の定義



safetyとは:

freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment（IEC61508から引用)

ISO 26262とは？

- ◆IEC 61508をベースとし、自動車を対象とする機能安全規格
- ◆2011年11月に発行
  - ■ 2004年から欧州(特に独、伊）中心に議論
  - ■ 議長はBMW、自動車メーカだけ
  - ■ 2008年、CD承認済み
  - ■ 2009年、DISが公開
- ◆安全度としてASILを4段階に定義
  - ■ Severity、Exposure、Controllabilityの組合わせ
  - ■ 冗長系や干渉防止によるASILの低減
- ◆安全要求の実現を保証するために、妥当性確認及び適合確認に対する要求事項を規定

規格書の序文

- ◆自動車分野の安全ライフサイクルを定義し、開発種別に応じた各フェーズのテーラリングを可能にする。
- ◆リスク等級化(ASIL決定)のために、自動車分野固有のリスクベースの手法を提供する。
- ◆残存リスクを許容水準に抑えることを達成するために、安全要求の定義にASILを用いる。
- ◆十分かつ許容できる水準の安全の実現を保証するために、妥当性確認及び適合確認に対する要求事項を提供する。
- ◆サプライヤとの関係に対する要求事項を提供する。

出典:ISO 26262規格書の序文から引用

規格書の構成

1. 用語
2. 機能安全マネジメント
3. 構想フェーズ
4. 製品開発:システムレベル
5. 製品開発:ハードウェアレベル
6. 製品開発:ソフトウェアレベル
7. 生産と運用
8. 支援プロセス
9. ASIL及び安全指向解析
10. ガイドライン(参考)

規格書の章構成

1. 範囲:規格の適用範囲及び各部の適用範囲

2. 規格内参照:他部の参照

3. 用語、定義、略語:第1部(用語)の参照

4. 適合のための要求事項

X. プロセスの解説

X.1 目標

X.2 一般事項

X.3 本節へのインプット

必須条件

追加の支援情報

X.4 要求事項及び推奨事項

X.5 作業成果物

◆ **附属書**:文書フローの概要、及び参考例

2. 機能安全マネジメント

- 要求事項
- 安全ライフサイクル
- 安全計画
- 安全ケース
- 適合確認

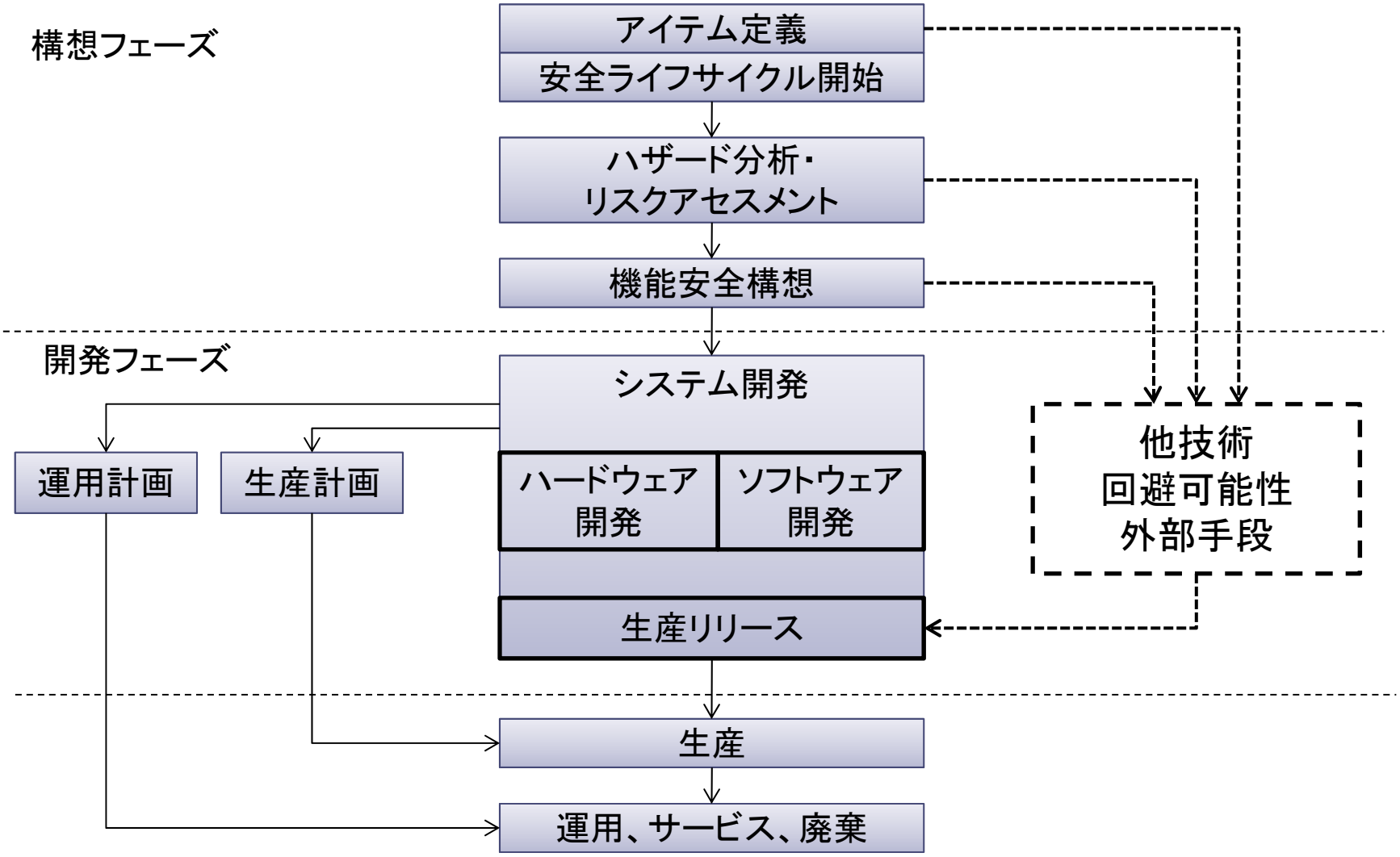
機能安全マネジメントに関する要求事項

◆組織に対する全般的な要求事項
- 機能安全を奨励する安全文化、規格遵守のための規則と手続き等を構築し、維持し、継続的に改善する。
- 要員のスキル、能力、資格を保証する。
- ISO9001等に適合する品質マネジメントシステムを有する。

◆製品開発における要求事項
- 規格遵守に責任と権限を持つプロジェクトマネージャは、必要なリソースと安全マネージャの任命を確認する。
- 安全計画を作成し、維持し、その進捗を監視する。
- 機能安全の達成を評価できるように、すべての作業成果物を安全ケースに集約する。
- 独立性のある適合確認を計画的に実施する。

◆生産リリース後の要求事項
- 生産リリース後の機能安全を維持する責任者を任命する。
- 機能安全を維持するための手続きを実施する。
- 機能安全に関するフィールドモニタリングを実施する。

安全ライフサイクル



出典:ISO 26262第2部から引用

安全ライフサイクルのテーラリング

◆組織の標準プロセスに対して
- ■ サブフェースや活動の併合、分割
- ■ 作業項目を実施するフェーズやサブフェーズの変更
- ■ フェーズやサブフェーズの繰返し

◆プロジェクト固有のプロセスに対して
- ■ 安全活動の省略、方法変更
  - ●安全計画の一環であり、正当な理由が必要
- ■ 関連要求事項
  - ●既存システムの変更(P3-6)
  - ●使用実績による適合論証(P8-14)
  - ●ASIL分解(P9-5)
  - ●信頼できるツールの利用(P8-11)
  - ●別開発要素（SEooC）

安全計画

計画の対象	関連する作業成果物
安全活動のテーラリング	
ハザード分析・リスクアセスメント	
開発のための活動	
開発インタフェース協定(DIA)	
支援プロセス	
検証と妥当性確認のための活動	アイテム統合テスト計画、ソフトウェア検証計画、妥当性確認計画
適合確認	
従属故障解析と安全解析	
ソフトウェアツールの認定	
使用実績による適合論証	

安全ケース

- ◆目的:　機能安全の実現の評価
  - ■機能安全アセスメントの入力となる
- ◆完全性
  - ■すべての作業成果物が揃っている
  - ■すべての作業成果物に記述漏れはない
- ◆構成管理及び変更管理の対象
- ◆安全計画に従い、文書化の要求事項に従って文書化される

適合確認の種類と独立性

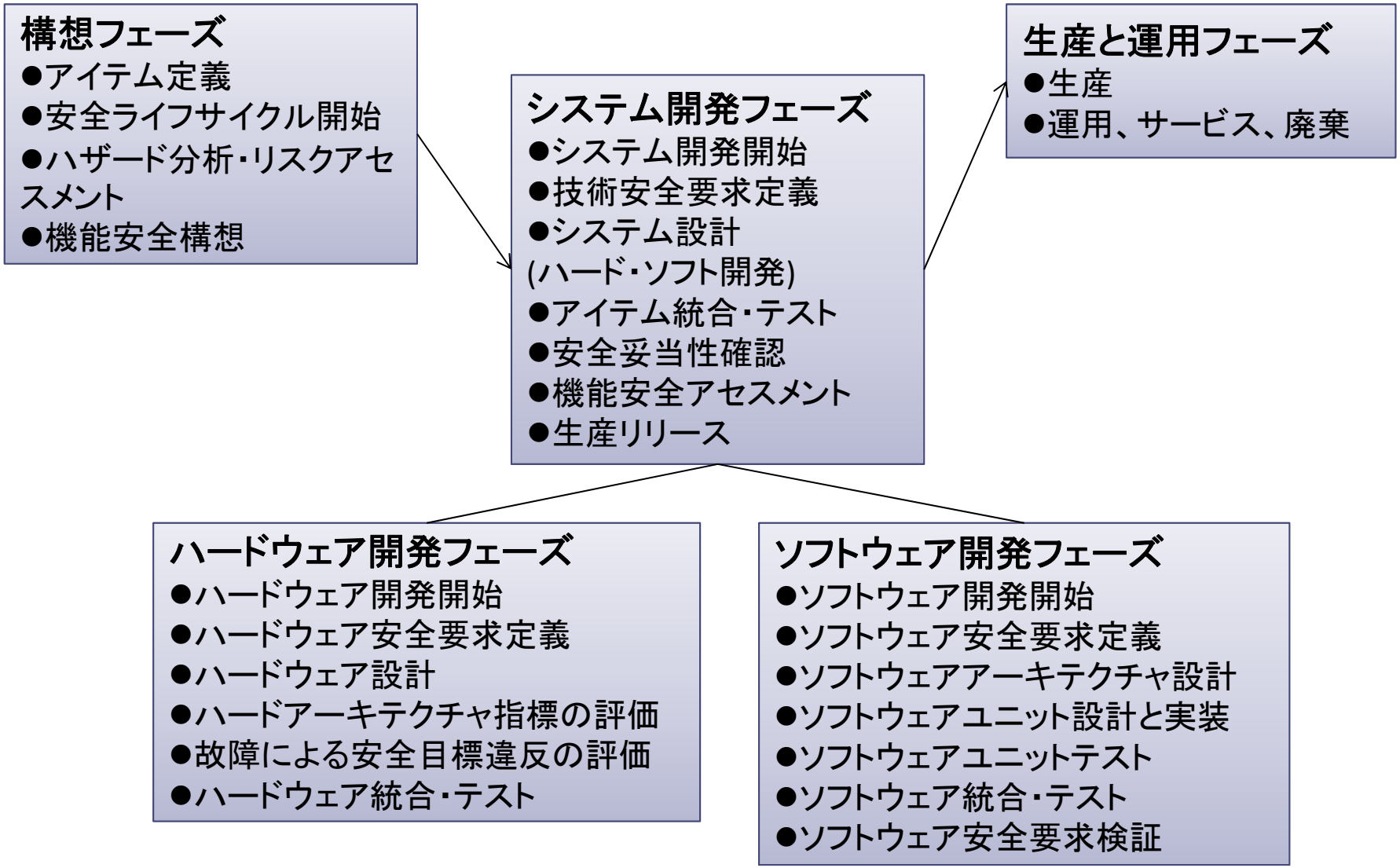
手段	適合確認の対象	独立性の確保		
		他人	他チーム	他部門
作業成果物のレビュー	ハザード分析・リスクアセスメント			全ASIL
	安全計画	ASIL-B	ASIL-C	ASIL-D
	統合テスト計画	(ASIL-A) ASIL-B	ASIL-C,D	
	妥当性確認計画			
	安全解析	ASIL-A,B	ASIL-C	ASIL-D
	ソフトウェアツールの認定	（ASIL-B) ASIL-C,D		
	使用実績による適合論証	（ASIL-A) ASIL-B	ASIL-C	ASIL-D
	安全ケースの完全性			
監査	機能安全に関する開発プロセス	（ASIL-B)		
アセスメント	実現される機能安全			

備考: 適合確認=confirmation。 ()は推奨事項。

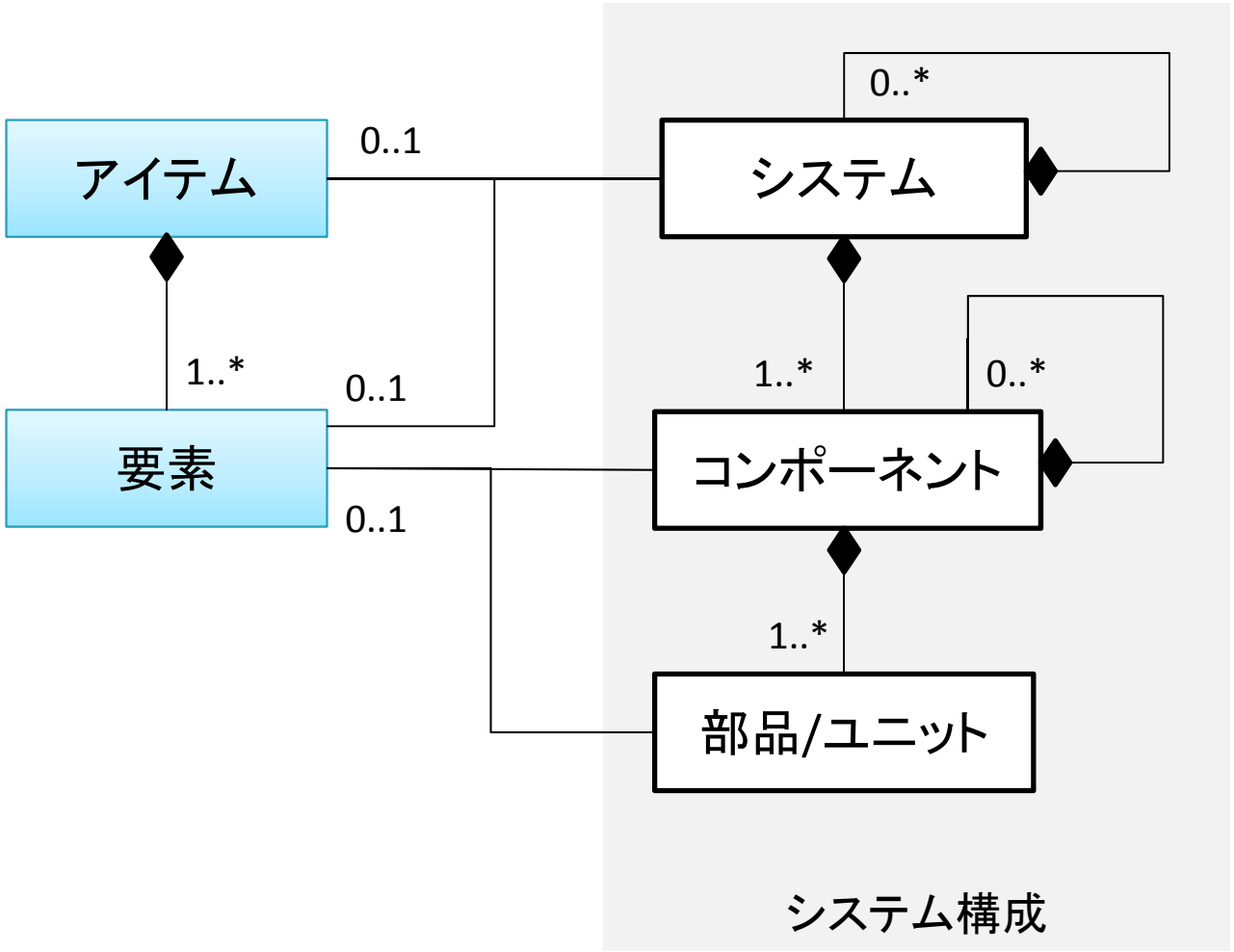
3. 主要プロセス

- 主要プロセスの流れ
- アイテムとシステム構成要素
- 安全ライフサイクル開始
- システム開発開始
- ソフトウェア開発開始
- アイテム統合・テスト

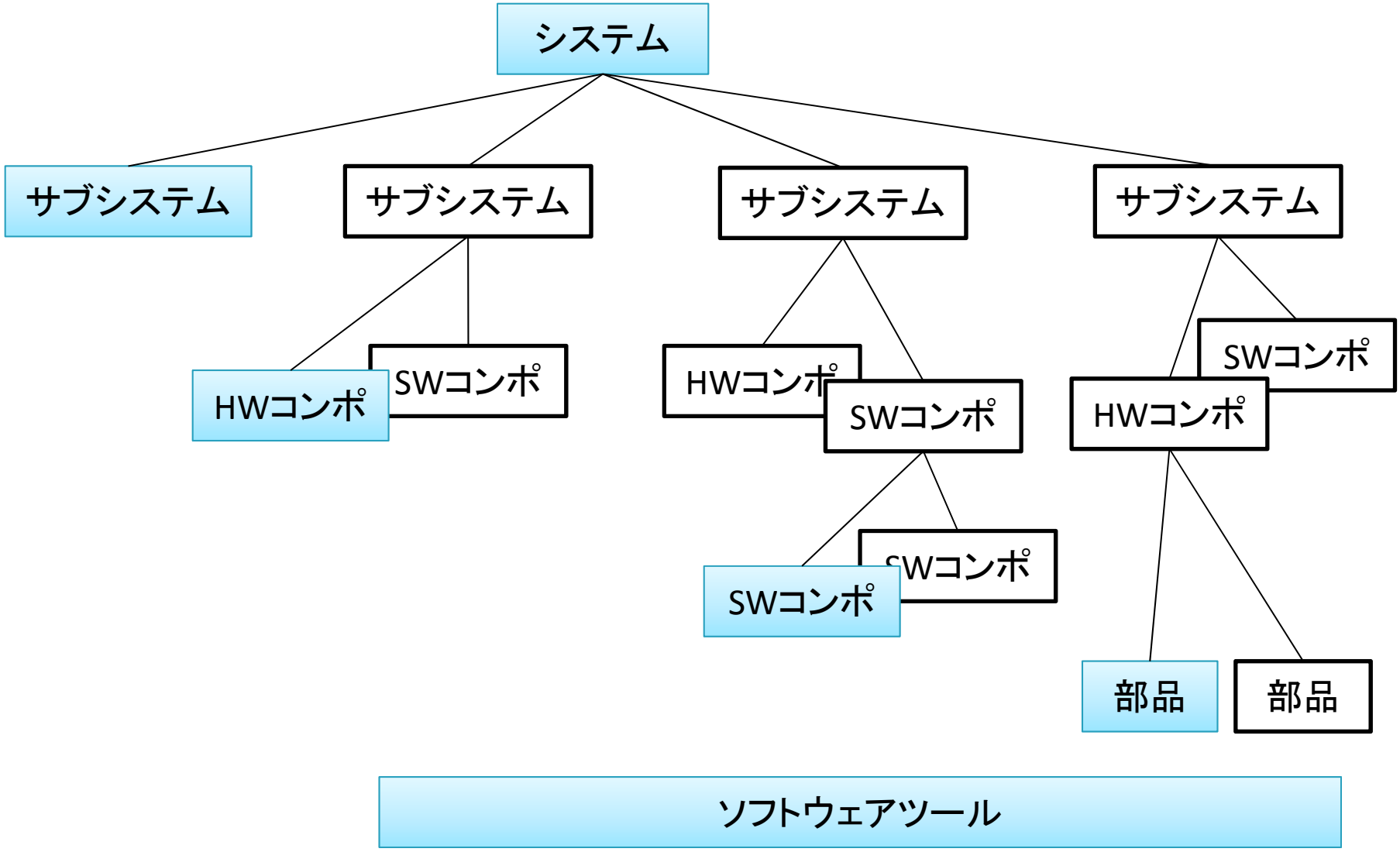
主要プロセスの流れ



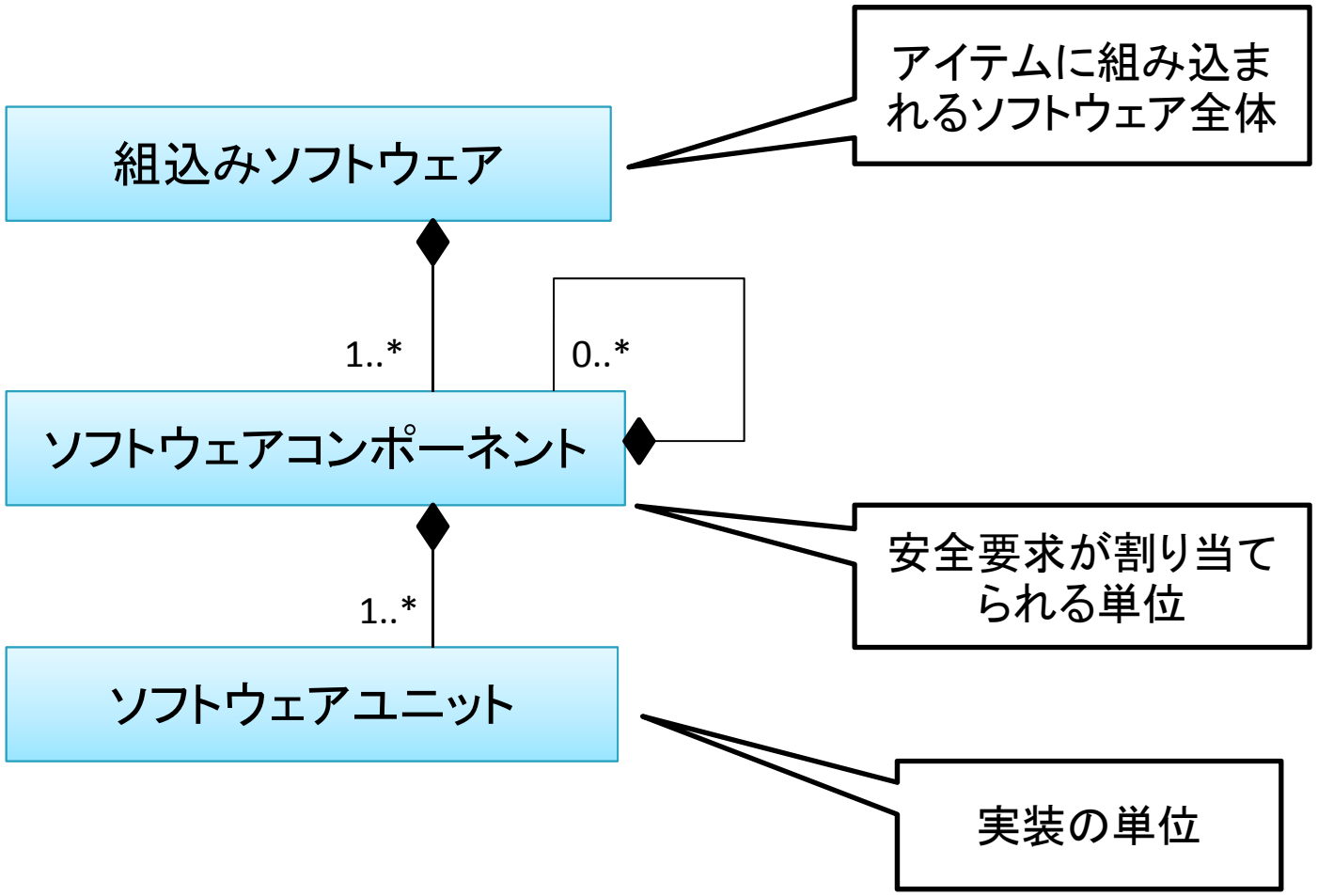
アイテムとシステム構成



システム構成要素と開発対象



ソフトウェア構成要素



安全ライフサイクル開始プロセス

開発種別	影響分析	安全ライフサイクルのテーラリング
新規開発		全安全ライフサイクルを適用する。
既存アイテム又はその環境の修正	アイテム又はその環境に適用される修正を特定し、その影響を分析する。	影響分析に基づいて適用する活動を決め、影響を受ける作業成果物を作り直す。

システム開発開始プロセス

◆システム開発での計画を作成
- ■ 設計や統合で使用する手法
- ■ 安全活動
- ■ 妥当性確認活動
- ■ 機能安全アセスメント活動

◆システム開発のライフサイクルをテーラリング

ハードウェア開発開始プロセス

- ハードウェア開発のための手法と手段を決定
  - ソフトウェア開発の計画と整合するように
- ハードウェア開発のライフサイクルをテーラリング
- ハードウェアコンポーネントの再利用、認定済みのコンポーネントや部品を特定

ソフトウェア開発開始プロセス

- ◆開発フェーズで行われる活動と手法を選定
- ◆ライフサイクルをテーラリング
- ◆構成可能ソフトウェアに関する計画作成
- ◆手法とツールを選定し、適用ガイドラインを作成
- ◆モデリング又はプログラミング言語を選定
  - ■あいまいさがない、
  - ■組込み実時間処理に向いている等の基準に従う
- ◆設計・コーディングガイドラインを作成

設計・コーディングガイドライン

計画段階で規定しなければならない項目	ASIL-B	ASIL-C	ASIL-D
低複雑度の強制	HR	HR	HR
言語サブセットの使用	HR	HR	HR
強い型付けの強制	HR	HR	HR
防御的プログラミング技巧の使用	R	HR	HR
確立している設計原則の使用	R	R	HR
曖昧さのないグラフィカル表現の使用	HR	HR	HR
スタイルガイドの使用	HR	HR	HR
命名規則の使用	HR	HR	HR

備考:HR:強く推奨、R:推奨、NR:非推奨。

アイテム統合・テストプロセス

◆統合の計画を立て、テスト仕様を定義

◆テスト目標

- ■ システマテック障害の検出
- ■ 機能安全及び技術安全要求
- ■ 安全メカニズム
- ■ 内部及び外部インタフェース
- ■ ランダムハードウェア障害の診断率
- ■ 頑強性

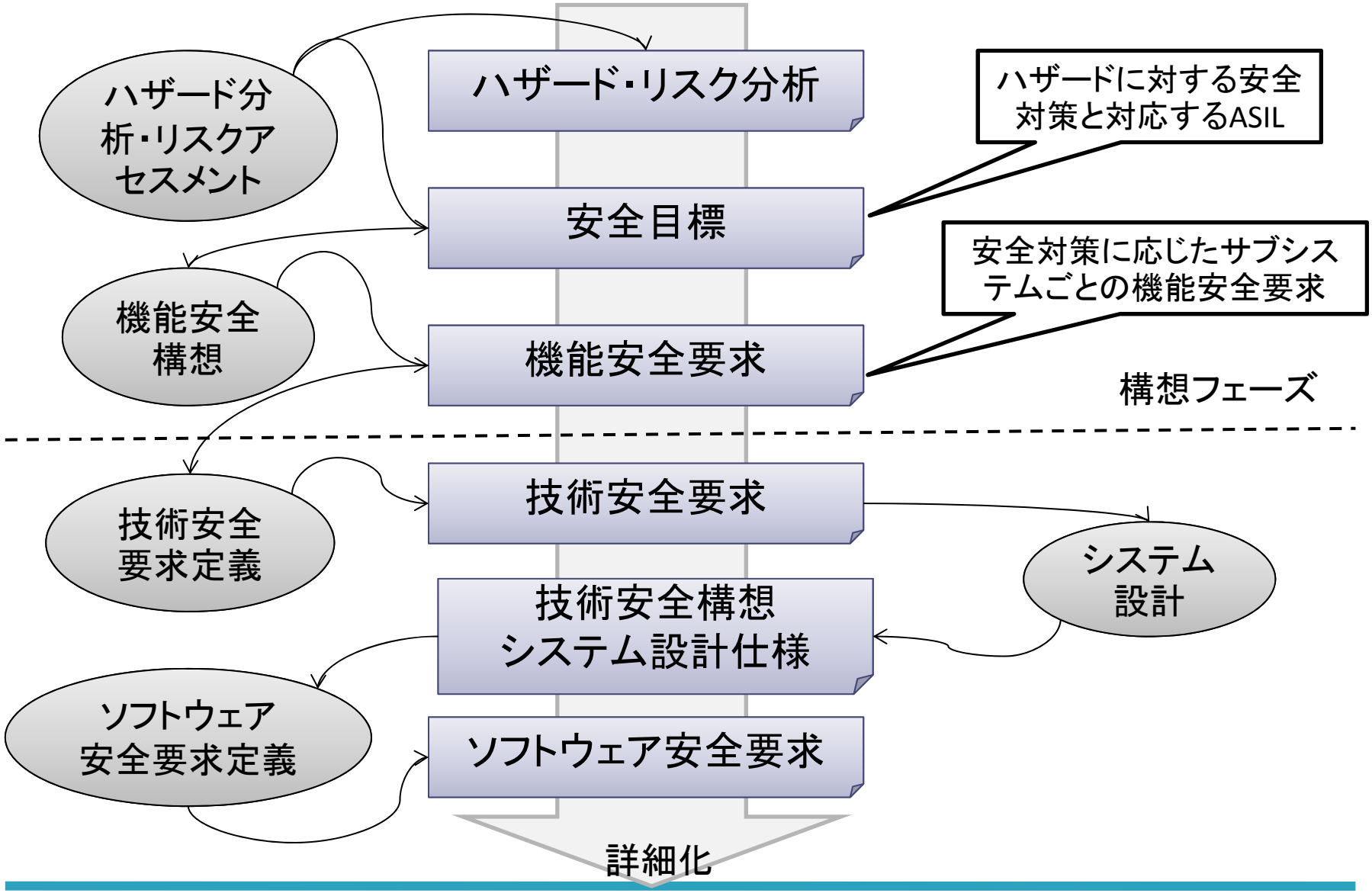
◆統合手順

1. ハードウェアとソフトウェアを統合
2. 要素を統合
3. アイテムを車両に統合

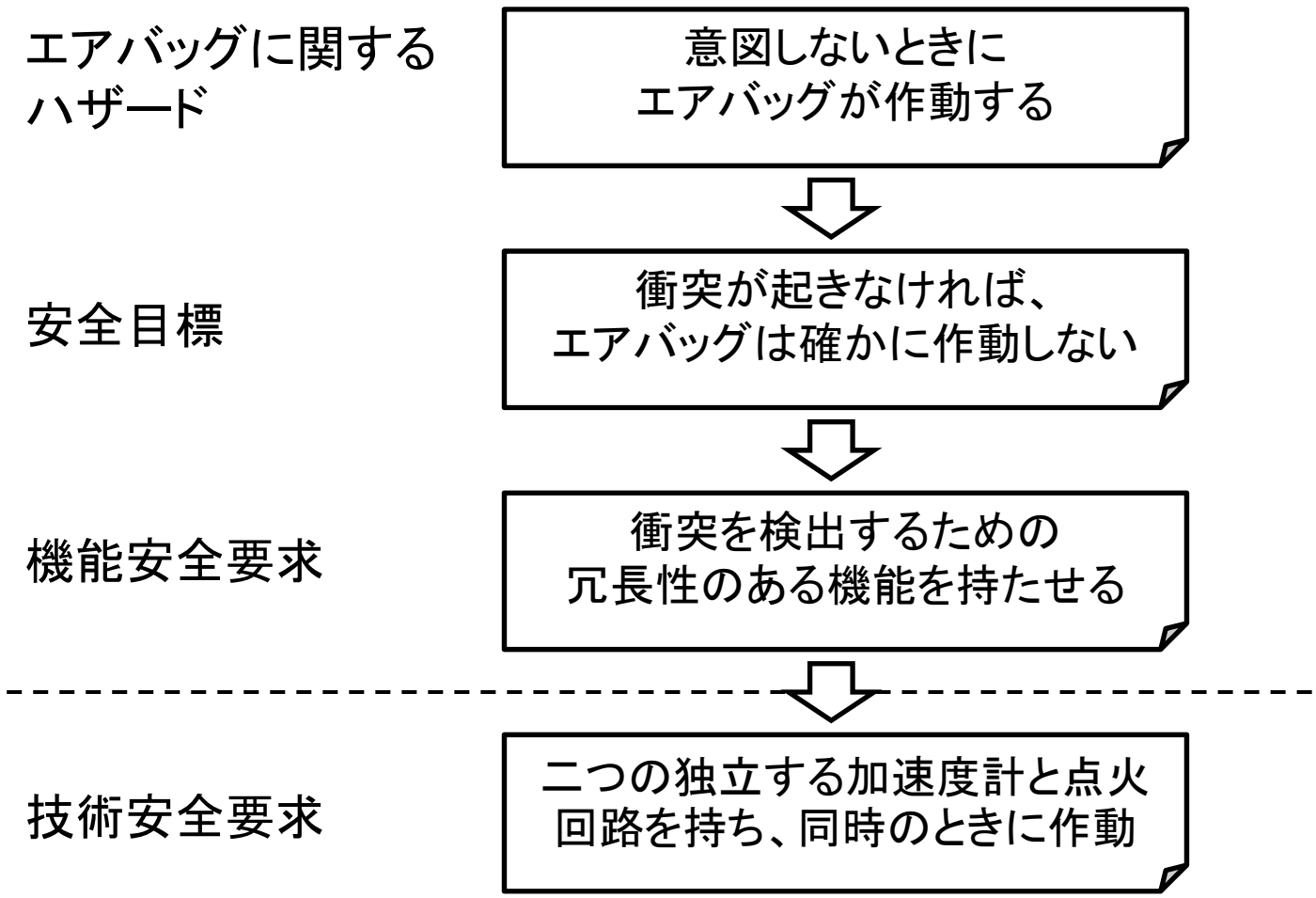
4. 安全要求定義に関するプロセス群

- ハザード分析・リスクアセスメントプロセス
- 機能安全構想プロセス
- 技術安全要求定義プロセス
- システム設計プロセス
- ソフトウェア安全要求定義プロセス
- 安全要求の定義と管理に関する要求事項

安全要求詳細化の流れ



安全要求の例



出典: 規格書第10部から引用

関連用語

和訳	原語	説明
安全活動	safety activity	安全ライフサイクルで行われる活動
安全措置	safety measure	故障を検出、制御、緩和するための活動や技術解
安全メカニズム	safety mechanism	安全状態を達成又は維持する目的で、障害を検出又は故障を制御するために、要素によって実現される技術解
安全目標	safety goal	最上位の安全要求
機能安全要求	functional safety requirement	実装から独立した、安全関連の属性を含む、安全動作や安全措置
機能安全構想	functional safety concept	機能安全要求と、その構成要素への割当て、要素間の相互作用

ハザード分析・リスクアセスメントプロセス

◆ハザードを特定する
- ■運転状況をもとにしてハザードを系統的に洗い出す。
- ■運転状況とハザードから危険事象を定義する。

◆危険事象を分類する
- ■Severity:被害の大きさ、3段階
- ■Exposure:暴露確率、4段階
- ■Controllability:回避可能性、3段階

◆危険事象に対するASILを決める
- ■分類結果に基づき、4段階(A、B、C、D)

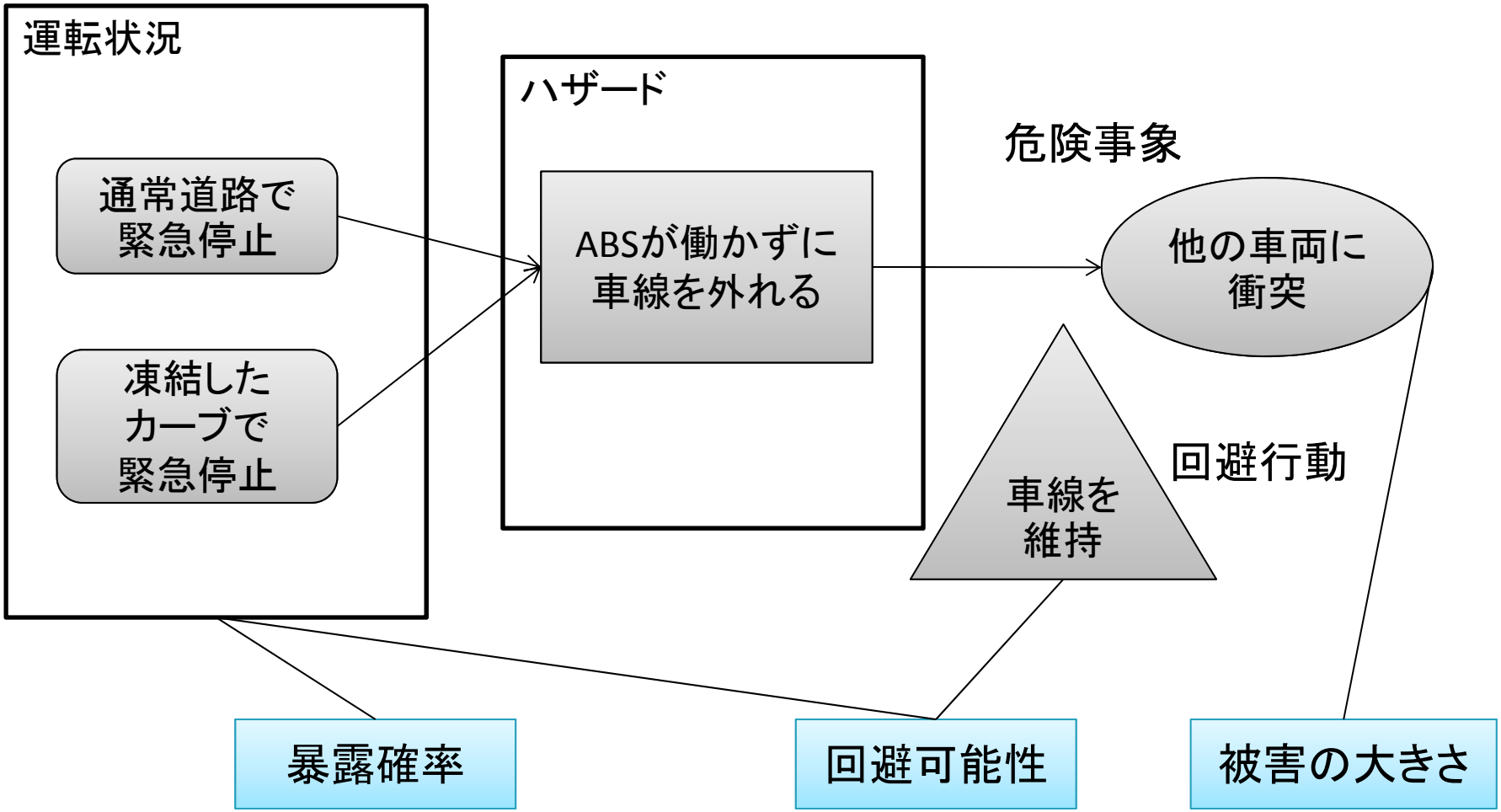
◆危険事象に対する安全目標を定義する
- ■技術解ではなく、安全状態への遷移等の機能目標

◆安全目標等を検証する

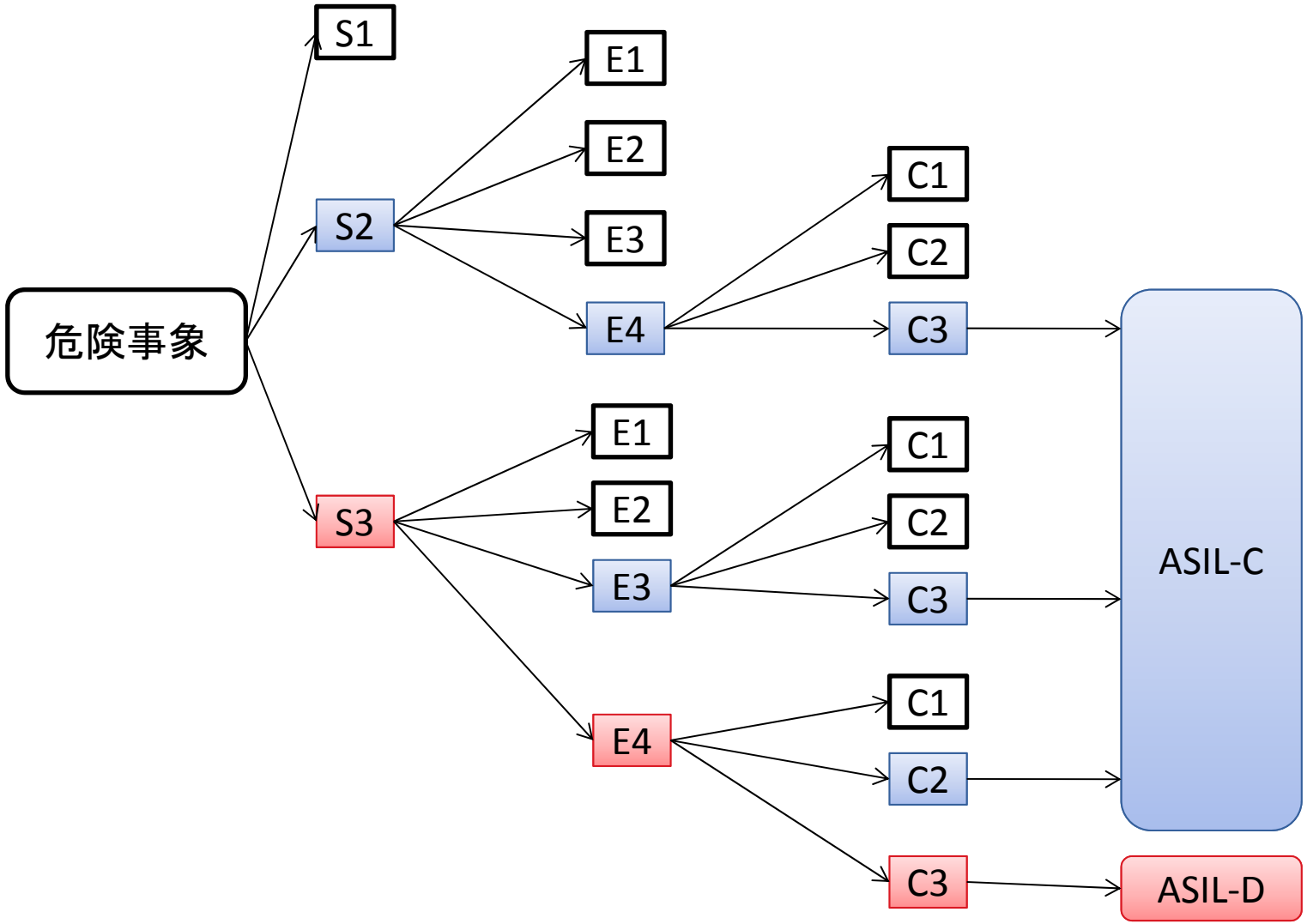
危険事象分類のための因子

因子	水準	説明
被害の大きさ	S1	軽傷
	S2	重傷で生命に危険を与えるが、生存が確かな傷害
	S3	生命に危険を与え、生存が不確かな重大傷害
暴露確率	E1	極めて低い
	E2	低い
	E3	中間
	E4	高い
回避可能性	C1	簡単に回避できる(たとえば、99%以上の人が回避可能)
	C2	通常は回避できる(90%以上)
	C3	回避は難しいか不可能(90%未満)

ハザード分析の例



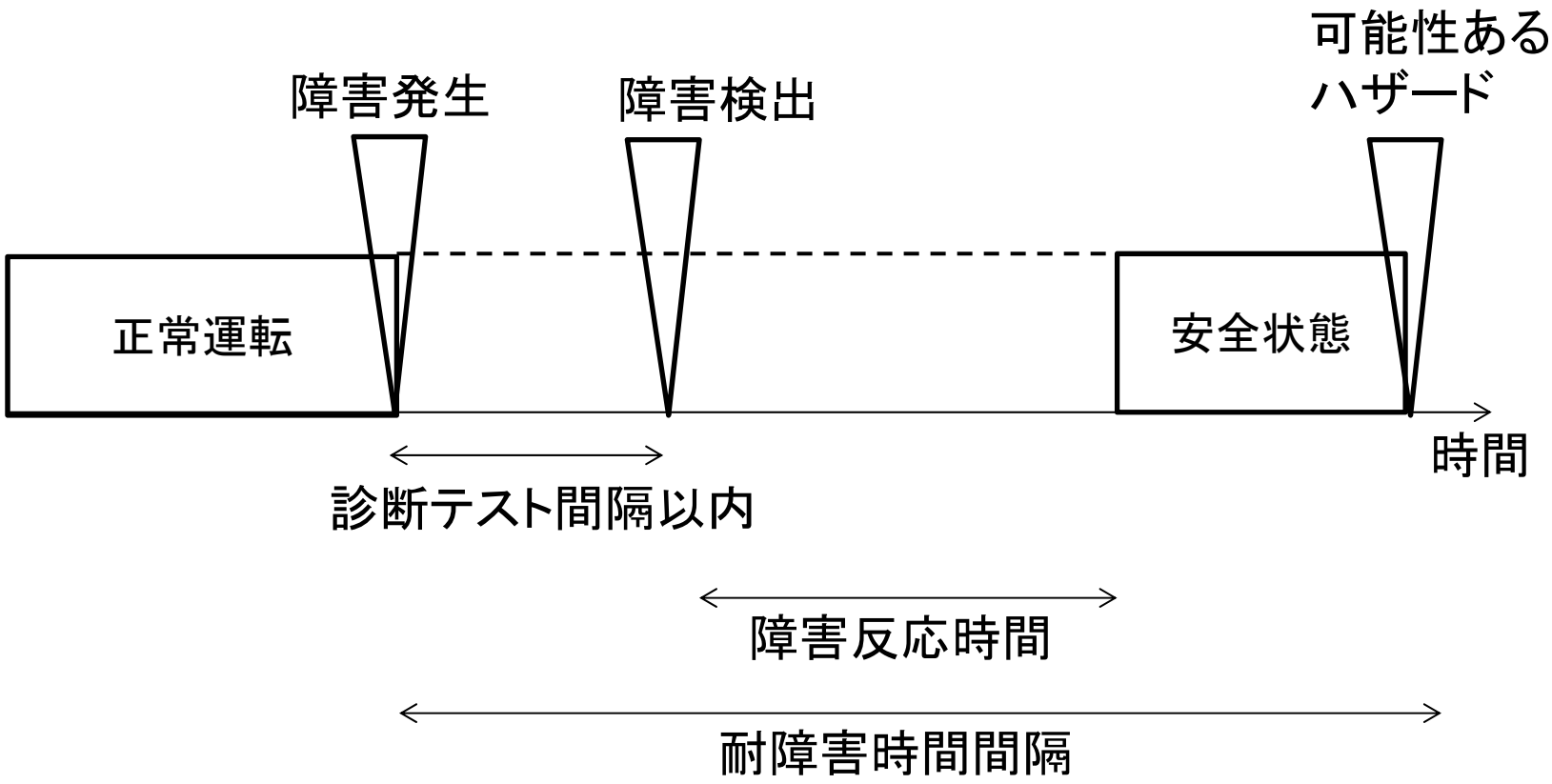
ASIL-C/D決定のためのリスクグラフ



機能安全構想プロセス

- ◆ 各安全目標に少なくても1件の機能安全要求を定義
  - ■ 考慮事項
    - ● 暫定アーキテクチャ
    - ● 動作モード、耐障害間隔、安全状態、非常運転間隔、機能冗長性
    - ● 安全解析の活用
  - ■ 規定事項
    - ● 運転者への警告や機能縮退
    - ● 安全状態へ移行できないときの非常運転
    - ● 想定している運転者の行動、手段、回避操作
- ◆ 機能安全要求を割当てる
  - ■ 暫定アーキテクチャに基づく要素、
  - ■ 他技術で実現される要素、又は、外部手段
- ◆ 安全妥当性確認の受入れ基準を定義する
- ◆ 機能安全構想を検証する
  - ■ 安全目標との整合性と適合性
  - ■ 危険事象を緩和又は回避する能力

障害からハザードに至る時間間隔



技術安全要求定義プロセス

- ◆システム特性を規定する
  - ■ 通信、ユーザインタフェース、制約、構成上の要求
- ◆安全メカニズムを規定する
  - ■ 障害を検出、表示、制御するするための手段
  - ■ 安全状態を達成し、維持するための手段
    - ●耐故障時間間隔、非常運転間隔を決める
    - ●安全状態への遷移、その維持手段を決める
  - ■ 警告と機能縮退を実現するための手段
  - ■ 潜在障害を回避するための手段
    - ●多点障害検出間隔を決める
    - ●2点障害が潜在しないための手段を決める
- ◆妥当性確認の基準を決める
- ◆新しいハザードを検出したら、変更管理に従ってハザード分析・リスクアセスメントをやり直す

ランダムハードウェア故障に関する用語

和訳	原語	説明
一点故障	single-point failure	一点障害によって起き、直ちに安全目標違反を引き起こす故障
一点障害	single-point fault	安全メカニズムが対処しない障害
多点故障	multiple-point failure	複数の独立した障害の組合せによって起き、直ちに安全目標違反を引き起こす故障
多点障害	multiple-point fault	他の独立した障害と組合わせて、多点故障を引き起こす障害
多点障害検出間隔	multiple-point fault detection interval	多点障害を、多点故障となる前に、検出するための時間間隔
残存障害	residual fault	単独で安全目標違反を引き起こす障害の一部で、安全メカニズムが対処しない範囲の障害
潜在障害	latent fault	多点障害検出間隔以内に安全メカニズムで検出されず、ドライバに知覚されない多点障害
故障率	failure rate	故障の確率密度 / 要素の生存確率
診断率	diagnostic coverage	ハードウェア要素の故障率の一部で、安全メカニズムで検出される範囲

システム設計プロセス

- ◆技術安全要求をシステム構成要素に割当てる
- ◆システマテック故障の回避
  - ■ 演繹的又は帰納的故障解析を実施する
  - ■ 故障の源は回避されるか、その影響は軽減される
  - ■ 複雑さに起因する故障を回避するため、モジュラー設計技法を適用する
- ◆ランダムハードウェア故障の制御
  - ■ 故障を検出し制御する手段を規定する
  - ■ 故障率と診断率を構成要素レベルで規定すべき
- ◆ハードウェアとソフトウェアへの割当て
  - ■ 技術安全要求はハードとソフトに割当てられる
- ◆ハードウェアとソフトウェアのインタフェース
  - ■ 相互依存性、動作モード、資源利用法、診断機能、干渉防止機能等

ハードウェア安全要求定義プロセス

- ◆技術安全要求からハードウェア安全要求を定義
  - ■ 耐故障のための安全メカニズムのハードウェア安全要求と関連属性
  - ■ 安全メカニズム以外に関する要求
- ◆ハードウェア設計の検証基準を定義
- ◆ハードウェア/ソフトウェアインタフェースを詳細化し、ソフトウェアとの依存性を明確にする
- ◆ハードウェア安全要求を検証

ソフトウェア安全要求定義プロセス

- ◆技術安全要求を実現するソフトウェア機能を定義
- ◆技術安全構想とシステム設計に基づき、次の点を考慮する:
  - ■システムとハードウェアの構成
  - ■ハードウェア/ソフトウェアインタフェース
  - ■ハードウェア設計仕様に対する要求
  - ■タイミングに関する制約
  - ■外部インタフェース
  - ■車両等の動作モード
- ◆ハードウェアとのインタフェースを詳細化し、ハードウェアとの依存性を明確にする
- ◆検証には推奨手法を適用する

安全要求の定義と管理に関する要求事項

対象分野	要求事項
表記法	特徴の実現のため、自然言語と別表の手法を組み合わせる
特徴	曖昧さを避けるため、安全要求は分離されている
	安全要求は、曖昧でなく、理解しやすく、不可分で、矛盾せず、実現可能で、検証可能である
属性	識別番号、状態、ASIL
管理	安全要求は階層構造をとり、組織的に体系づけられ、完全性を持ち、外部一貫性を保ち、重複なく、保守容易である
	安全要求は上下方向に追跡可能であり、設計、検証とも追跡可能
	安全要求は構成管理に従う

表記法	ASIL-B	ASIL-C	ASIL-D
形式的でない表記法	HR	R	R
半形式手法	R	HR	HR
形式手法	R	R	R

表記法の比較

	規則		特徴
	シンタックス (書き方、構文規則)	セマンテックス (読み方、解釈)	
自然語	×	×	自由に表現できるが、意図は正しく伝わらない。
非形式手法	△	△	規則が共有されず、意図は正しく伝わらない。
半形式手法	○	△	書くものは統一されるが、その解釈に差が出る。
形式手法	○	○	書かれている内容を機械で解釈できる。

備考: ○は、統一された規則があり、共有されていることを示す。△と×は、そうでないことを示す。

5. 開発フェーズにおける推奨手法

- 設計表記法
- 設計原則
- 障害や故障を制御するための技法
- 設計の検証
- テストによる検証

主要な開発手法一覧

分野	手法	補足説明
表記法	半形式手法	UML、SADT、SysML
設計原則	設計・コーディングガイドライン	
故障制御	安全解析	FTA、ETA、FMEA、HAZOP
	エラー検出	防御的プログラミング
	エラー制御	回復処理、機能縮退
設計検証	インスペクション	
	シミュレーション	
	プロトタイピング	
	安全解析	安全解析手法を検証に活用
	半形式手法	半形式手法による表記を活用
	静的解析	制御フロー分析、データフロー分析
テスト	テスト手法	欠陥注入テスト、B2Bテスト
	テスト設計技法	同値分割、境界値分析
	構造網羅度	分岐網羅度、MC/DC、関数網羅度

システム設計における手法

適用分野	手法	推奨度	IEC 61508との相違
故障回避	演繹的解析(FTA,信頼性ブロック図)	HR	システム設計というフェーズは対象外(第2版ではこのフェーズが追加された)
	帰納的解析(FMEA、ETA、マルコフモデル)	HR	
検証	インスペクション	HR	
	ウォークスルー	NR	
	シミュレーション	HR	
	プロトタイピング	HR	
	安全解析(FMEA、FTA、ETA等)	HR	

備考1:推奨度はASIL-Dにおける推奨度。HR:強く推奨、R:推奨、NR:非推奨。
備考2:ウォークスルーは非公式だという理由で、排除している。

ソフトウェアアーキテクチャ設計における手法(1/2)

適用分野	手法	推奨度	IEC 61508との相違
表記法	形式的でない表記法	R	規定せず
	半形式手法	HR	同じ
	形式手法	R	
エラー検出	もっともらしさのチェック	HR	異常表明プログラミング/R
	データエラー検出	R	同じ
	外部監視装置	HR	プログラムシーケンス監視/HR
	制御フロー監視	HR	実行履歴の記録/R
	多様化ソフトウェア設計	HR	多様化プログラミング/R
エラー制御	静的回復処理	R	後方回復、前方回復等/R
	機能縮退	HR	同じ
	独立した並行冗長性	HR	多様化プログラミング/R
	エラー訂正符号	R	同じ

備考1:推奨度はASIL-Dにおける推奨度。HR:強く推奨、R:推奨、NR:非推奨。

ソフトウェアアーキテクチャ設計における手法(2/2)

適用分野	手法	推奨度	IEC 61508との相違
検証	ウォークスルー	NR	両者を区別せず、ウォークスルー/HR
	インスペクション	HR	
	シミュレーション(実行可能モデル)	HR	シミュレーション/モデリング/HR
	プロトタイピング	HR	
	形式手法	R	同じ
	制御フロー分析	HR	静的解析/HR
	データフロー分析	HR	

備考1:推奨度はASIL-Dにおける推奨度。HR:強く推奨、R:推奨、NR:非推奨。

ソフトウェアユニット設計・実装における手法(1/2)

適用分野	手法	推奨度	IEC 61508との相違
表記法	自然言語による文書化	HR	規定せず
	形式的でない表記法	R	規定せず
	半形式手法	HR	同じ
	形式手法	R	同じ
検証	ウォークスルー	NR	両者を区別せず、ウォークスルー/HR
	インスペクション	HR	
	半形式手法	HR	同じ
	形式手法	R	同じ
	制御フロー分析	HR	静的解析/HR
	データフロー分析	HR	
	静的コード解析	HR	
	意味的コード解析	R	

備考1:推奨度はASIL-Dにおける推奨度。HR:強く推奨、R:推奨、NR:非推奨。
備考2:インスペクション対象は、設計、モデル、ソースコード。

ソフトウェアユニット設計・実装における手法(2/2)

適用分野	手法	推奨度	IEC 61508との相違
設計原則	単一入口単一出口	HR	モジュラーアプローチ/HR
	動的オブジェクトと変数の禁止	HR	多少の違いはあるが、設計及びコーディング規約/HR
	変数の初期化	HR	
	変数名の多重使用の禁止	HR	
	大域変数の回避	HR	
	ポインタの限定使用	HR	
	暗黙の型変換の禁止	HR	
	隠れたデータフローと制御フローの禁止	HR	
	無条件ジャンプの禁止	HR	
	再帰呼出の禁止	HR	

備考1:推奨度はASIL-Dにおける推奨度。
備考2:これらの設計原則は、MISRA Cの適用で解決できる。

ソフトウェアユニットテストにおける手法

適用分野	手法	推奨度	IEC 61508との相違
テスト	要求に基づくテスト	HR	機能及びブラックボックス試験/HR
	インタフェーステスト	HR	インタフェース試験/HR
	欠陥注入テスト	HR	動的解析及び試験/HR
	資源使用テスト	HR	性能試験/HR
	バックツーバックテスト	HR	規定せず
テスト設計	同値分析	HR	動的解析及び試験/HR
	境界値分析	HR	
	エラー推測	R	
網羅度	分岐網羅度	HR	
	MC/DC	HR	規定せず

備考1:推奨度はASIL-Dにおける推奨度。
備考2:バックツーバックテストでは、モデルとコードで同じテストを実施し、結果を確認。

ソフトウェア統合テストにおける手法

適用分野	手法	推奨度	IEC 61508との相違
テスト	要求に基づくテスト	HR	ユニットテストに同じ
	インタフェーステスト	HR	
	欠陥注入テスト	HR	
	資源使用テスト	HR	
	バックツーバックテスト	HR	
テスト設計	同値分析	HR	
	境界値分析	HR	
	エラー推測	R	
網羅度	関数網羅度	HR	規定せず
	呼出網羅度	HR	規定せず

備考1:推奨度はASIL-Dにおける推奨度。
備考2:バックツーバックテストでは、モデルとコードで同じテストを実施し、結果を確認。

ソフトウェア安全要求検証における手法

適用分野	手法	推奨度	IEC 61508との相違
テスト環境	Hardware-in-the-loop	HR	個別応用分野向きは対象外
	ECUネットワーク環境	HR	
	実車	HR	

備考1:推奨度はASIL-Dにおける推奨度。HR:強く推奨、R:推奨、NR:非推奨。

6. 支援プロセス等

- 分散開発に関する要求事項
- 検証に関する要求事項
- ソフトウェアツールの分類と認定方法
- ソフトウェアコンポーネントの認定条件
- ASIL分解
- ASIL共存
- 従属故障
- 安全解析

支援プロセス(第8部)の構成

- ◆分散開発におけるインタフェース
- ◆安全要求の定義と管理
- ◆構成管理
- ◆変更管理
- ◆検証
- ◆文書化
- ◆ソフトウェアツールの使用における信頼性
- ◆ソフトウェアコンポーネントの認定
- ◆ハードウェアコンポーネントの認定
- ◆使用実績による適合論証

分散開発に関する要求事項

- ◆分散開発の範囲
  - ■ 車メーカとサプライヤ、サプライヤとサブサプライヤ、等々
- ◆サプライヤ選定
  - ■ 同等のASILに対応する開発を実施できる能力を評価する
  - ■ RFQで規格への適合を要求する
- ◆分散開発の計画
  - ■ 双方の安全マネージャを任命する
  - ■ 双方の担当プロセス・活動、実施責任者を決める
  - ■ 支援プロセスとツールを合意する
- ◆分散開発の実行(省略)
- ◆安全アセスメント
  - ■ サプライヤ拠点で車メーカが実施する(ASIL-C/D)
  - ■ その他の適合確認をASILに応じて実施する

検証に関する要求事項

- ◆目的
  - ■作業成果物が要求事項を満たすことを確認
- ◆検証計画
  - ■安全ライフサイクルのフェーズ及びサブフェーズを対象
  - ■検証する作業成果物、検証手法、合格基準、是正処置及び回帰テスト方針を決める
  - ■使用するツールを決める(ツール認定が必要となる)
- ◆検証仕様
  - ■レビュー、シミュレーション、又はテストを選択
  - ■テストケースは事前条件、入力データ、期待結果を含む
  - ■テスト方法はテスト環境、依存性、資源を規定
- ◆検証の評価
  - ■検証結果が期待結果を満たす度合
  - ■合否判定と、不合格の場合の理由

検証の対象

作業成果物	ASIL-A	ASIL-B	ASIL-C	ASIL-D
ハザード分析・リスクアセスメント	○	○	○	○
安全目標	○	○	○	○
機能安全構想	○	○	○	○
技術安全要求	○	○	○	○
システム設計	○	○	○	○
ハードウェア安全要求	○	○	○	○
ハードウェア設計	○	○	○	○
ハードウェア故障に関する手法と分析	×	△	○	○
ソフトウェア安全要求とHSI要求	○	○	○	○
ソフトウェアアーキテクチャ設計	○	○	○	○
ソフトウェアユニット設計と実装	○	○	○	○
ソフトウェアとハードウェアコンポーネント認定	○	○	○	○
安全解析	○	○	○	○

ソフトウェアツールの分類と認定手法

ソフトウェアツールの分類

	TD1	TD2	TD3
TI1	TCL1		
TI2	TCL1	TCL2	TCL3

TI: Tool Impact
TI1:ツールが誤動作しても安全要求に違反しない
TI2:違反する恐れあり

TD: Tool error Detection
TD1:検出度高い
TD2:検出度中
TD3:検出度低い

TCL: Tool Confidence Level

ASIL-Dにおけるツールの認定手法

手法	TCL2	TCL3
使用実績による信頼度	R	R
開発プロセスの評価	R	R
ツールの妥当性確認	HR	HR
安全規格に準拠する開発	HR	HR

備考:TCL1に対しては認定不要。

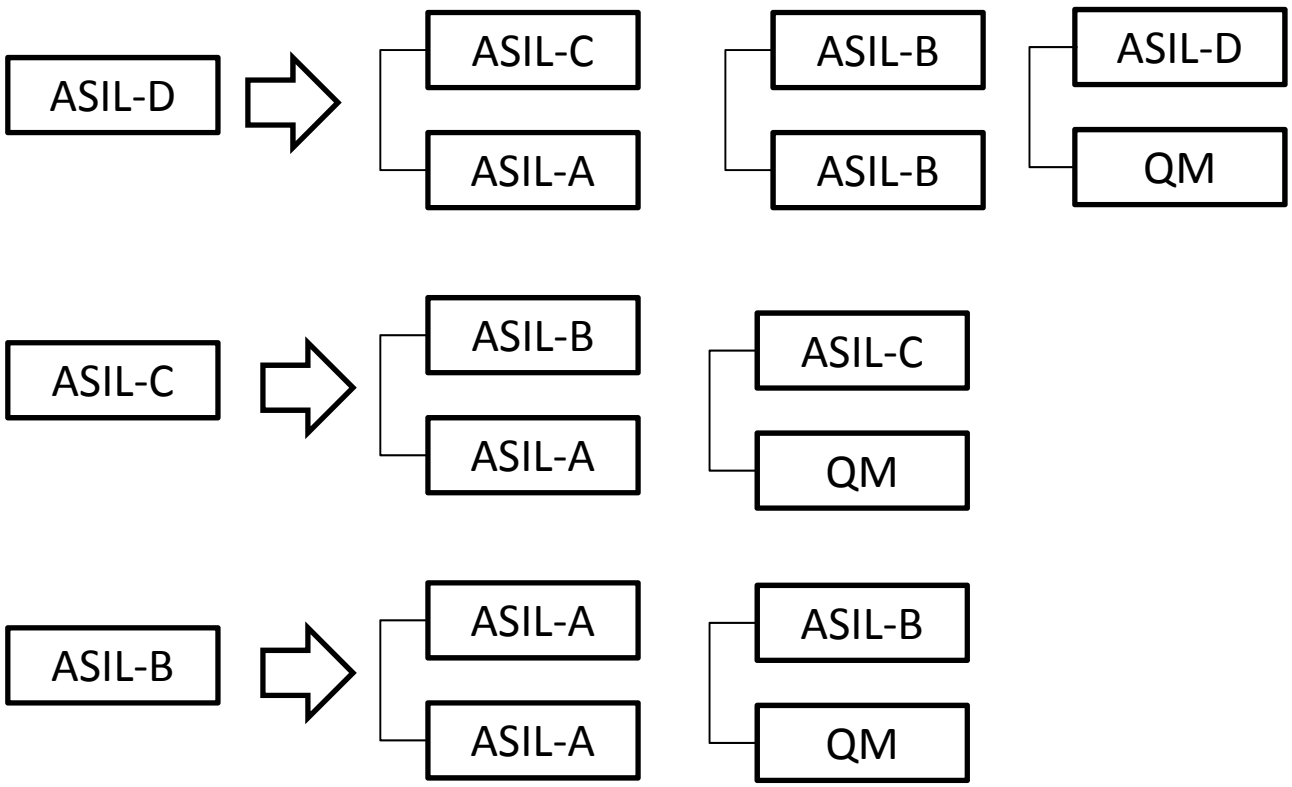
ソフトウェアコンポーネントの認定条件

- ◆仕様書の記載事項
  - ■ 要求、構成、インタフェース、結合方法、適用マニュアル
  - ■ 異常条件に対する応答、他コンポとの依存性
  - ■ 既知の異常とその回避策
- ◆検証に関する基準
  - ■ 要求網羅度、構造網羅度(ASIL-Dのみ)を測定
  - ■ 正常処理と故障時の動作をカバー
  - ■ 安全要求違反につながる既知エラーがない
- ◆意図する用途に対する妥当性の検証
  - ■ 意図する用途に関する要求を満足する
- ◆認定作業の文書化
  - ■ 認定者、認定環境、検証結果
  - ■ コンポーネントの識別、構成、最高ASIL

ASIL及び安全指向解析(第9部)の構成

- ASILテーラリングに関する要求分解
- 要素共存のための基準
- 従属故障解析
- 安全解析

ASIL分解



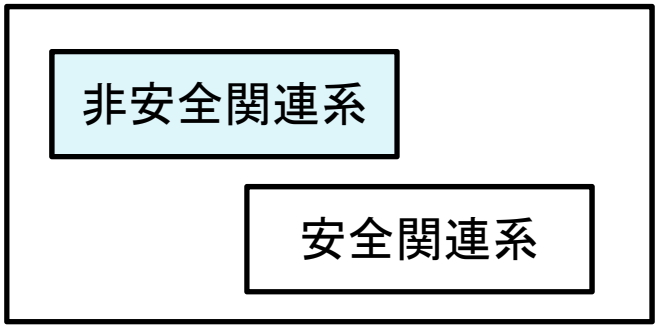
要求事項

- 適合確認をもとのASILに従って実施。
- 独立性の分析が必要。
- ランダムハードウェア故障に対するASILは不変。
- 統合とそれ以降の活動も元のASILで。

備考1: 分解後のそれぞれの要求はそれ自体で元の要求を満たす(冗長性)。
備考2: ASIL-Dの分解には、追加的要求事項がある。

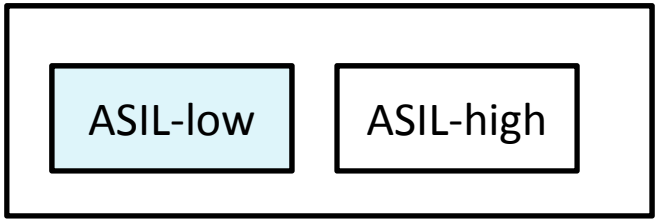
ASIL共存

構成要素



非安全関連副要素にASILを割当てなくてよい条件:
●安全関連副要素に干渉しない

構成要素

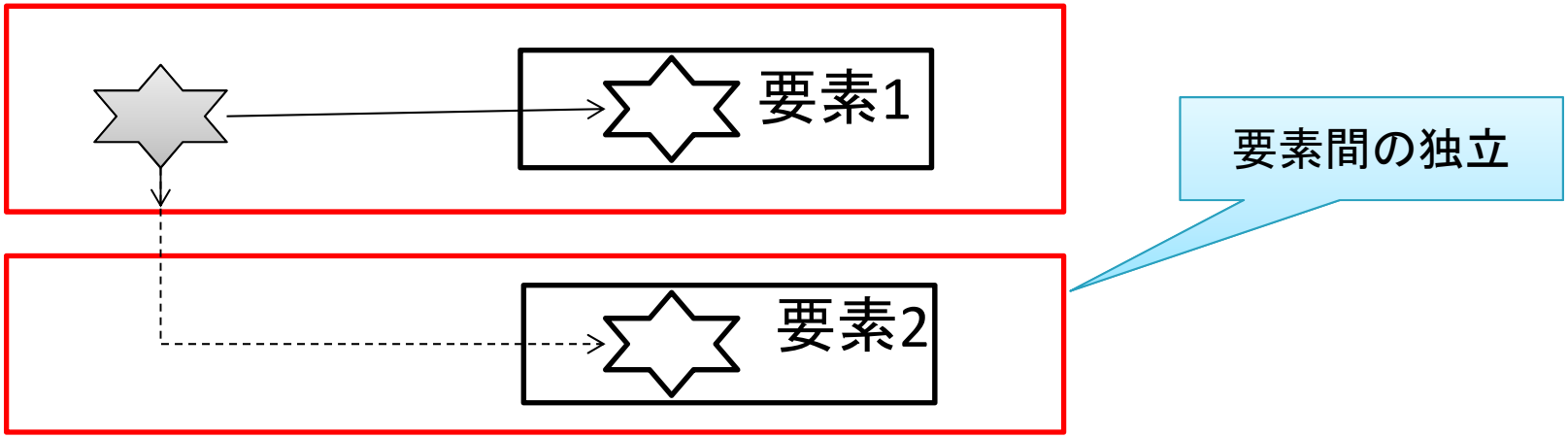


低いASILを割当ててよい条件:
●高ASILを持つ副要素に干渉しない

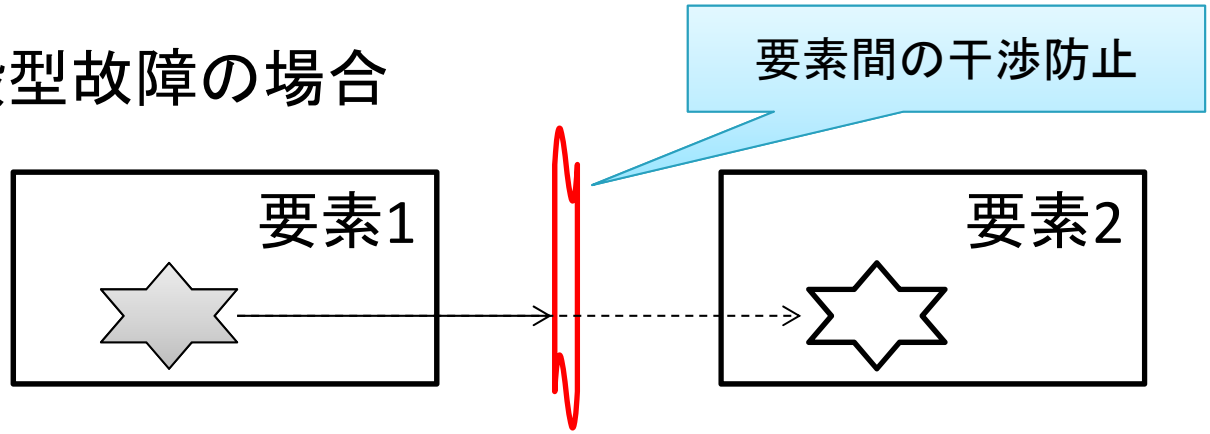
原則:すべての副要素に最高ASILを適用する。

従属故障

共通原因故障の場合



伝搬型故障の場合



従属故障:　二つの故障が同時に起きる確率が、それぞれの故障の起きる確率の積にならない。

安全解析

- ◆目的は、安全目標や安全要求が満たされなくなる条件や原因を探り、対策を開発に反映すること
- ◆標準やガイドラインに従って、構想フェーズ、開発フェーズで適宜実施
- ◆結果は、適合確認の対象となる
- ◆定性的解析
  - ■安全要求違反につながる障害や故障の系統的な識別
  - ■結果の評価、原因の特定
  - ■安全メカニズムや安全構想の弱点を識別
  - ■手法として、FMEA、ETA、HAZOP
- ◆可能であれば、定量的解析を実施
  - ■手法として、FTA、マルコフモデル、信頼性ブロック図

7. IEC 61508との比較による特徴

- 開発プロセス
- 安全度
- 開発管理等

備考: IEC 61508規格書としてはJIS C 0508を参照している。

IEC 61508との比較一覧

	ISO 26262	IEC 61508
開発プロセス	開発フェーズをシステム、ハードウェア、ソフトウェアに分割。	第2版において、システムとハードウェアが分離。
	フェーズ分けがA-SPICEに類似。	一般的なVモデルを想定。
安全度	運転状況に基づく定性的な手法を示し、ハザードごとにASIL設定。	●故障率に基づく定量的な手法でSILを計算する。 ●ソフトウェアに関しては具体的な手法を提示していない。
	冗長系や異ASIL共存におけるASIL低減が可能。	記述無し。
開発手法	自動車分野の実態に合わせて、開発サブフェーズごとに具体的に手法を提示。	特定の応用に合わせて手法を推奨してはいない。
開発管理	ソフトウェアツールや再利用コンポーネントの認定手法を規定。	第2版で、ツール認定が規定された。
	車メーカとそのサプライヤとの分散開発に関する手続きを規定。	記述無し。

開発プロセスに関する特徴

- ◆開発プロセスをシステム、ソフトウェア、ハードウェアとレベルを分けたとき、ISO 26262は明確に区分しているが、IEC 61508ではシステムレベルの作業項目が不明確である。
- ◆ISO 26262における開発フェーズ分けは、自動車分野の開発プロセスモデルAutomotive-SPICEとの対応が取りやすい。
- ◆ISO 26262における開発フェーズは、IEC 61508に比べて定型的にプロセス定義されていてる。
  - ■目的、概要、入力、要求事項、出力

開発フェーズの対応関係

Automotive-SPICE	ISO 26262	IEC 61508
要件抽出	アイテム定義	概念
		全対象範囲の定義
	ハザード分析・リスクアセスメント	潜在危険及びリスク解析
	機能安全構想	全安全要求事項
		安全要求事項の割当て
システム要件分析	技術安全要求定義	
システムアーキテクチャ設計	システム設計	
ソフトウェア要件分析	ソフトウェア安全要求定義	ソフトウェア安全要求仕様
ソフトウェア設計	ソフトウェアアーキテクチャ設計	ソフトウェア設計及び開発
ソフトウェア構築	ユニット設計・実装	
	ソフトウェアユニットテスト	
ソフトウェア統合テスト	ソフトウェア統合・テスト	
		PE統合
ソフトウェアテスト	ソフトウェア安全要求検証	ソフトウェア安全妥当性確認
システム統合テスト	アイテム統合・テスト	
システムテスト	安全妥当性確認	全安全妥当性確認

安全度に関する特徴

- ISO 26262は、運転状況の分析に基づく、定性的なASILの算出法を規定している。
- ASIL低減を可能にするために、
  - 冗長構成において、各要素のASILの決め方、適合確認等に関する要求事項を規定している。
  - 異なるASILを持つ副要素から構成される要素において、各副要素のASILを決めるための基準を示している。

開発管理等に関する特徴

- ◆ソフトウェアツールの使用について、ISO 26262は、誤動作・誤出力の検出度合いに応じて認定手法を規定している。
  - ■ IEC 61508も第2版でツール認定規定を追加。
- ◆ソフトウェアコンポーネントの再利用について、ISO 26262は同様に認定の条件を規定している。
- ◆車メーカがサプライヤと分散開発する場合において、サプライヤの選定、契約、開発計画、開発実施、安全アセスメント等に関する手続きを規定している。

参考:ソフトウェア支援ツールの分類

カテゴリ	クラス	定義	例
オンラインツール		実行時に安全関連系に直接影響を与えるツール	
オフラインツール		ソフトウェア開発を支援するツール	
	T1	実行可能コードやデータを生成しないツール	テキストエディタ 設計支援ツール 構成管理ツール
	T2	テストや検証を支援するツールで、誤動作すると欠陥を見落とす可能性があるが、実行可能ソフトウェアに誤りを作り出さないツール	テスト道具 カバレッジ測定 静的解析
	T3	実行可能コードに貢献することができる出力を生成するツール	コンパイラ

出典: IEC 61508第2版　第4部

参考:T2ツールに対する要求事項(一部)

◆仕様又は製品資料

- ツールの動作、及び
- 使用方法又は制約事項を記述している必要がある。

◆アセスメント

- ツールに対する信頼度、及び
- 実行可能ソフトウェアに影響を与えるかもしれない、ツールの故障メカニズムを確定する。
  - 手法の例として、ソフトウェアHAZOP
- 故障メカニズムに対する緩和策が適切かを判断する。
  - 緩和策の例として、既知バグの回避、ツール機能の使用制限、ツール出力の確認、別ツールの重複利用

出典:IEC 61508第2版　第3部　7.4.4節

参考:T3ツールに対する要求事項(一部)

- ◆T2ツールに対する要求事項に加えて、
- ◆仕様やマニュアル通りに動く証拠を用意する。
  - ■ 使用実績
  - ■ 妥当性確認
- ◆証拠を用意できなければ、ツールの欠陥に起因する故障を制御できる有効な手段が必要。
  - ■ 例として、多様化コードの生成

出典:IEC 61508第2版　第3部　7.4.4節

参考資料

◆ISO 26262:2011規格書、ISO

◆JIS C 0508規格書、日本規格協会

◆ソフトウェア安全設計入門、株式会社レンタコーチ

まとめ

- ISO 26262は自動車用の安全ライフサイクルを定義し、開発種別に応じたテーラリングを可能とする。
- 機能安全をマネジメントするため、製品開発プロジェクトだけでなく、組織全体も要求事項を満たさなければならない。
- 規格への適合を確認するため、成果物のレビュー、開発プロセスの監査、機能安全実現のアセスメントを、ASILに応じた独立性で実施しなければならない。
- 作業成果物は安全ケースとして保持しなければならない。
- ハザード識別からソフトウェア安全要求までの手順と作業項目が示されている。
- 妥当性確認と検証を重視し、そのための手法を開発フェースに沿ってASILに応じて推奨している。
- ツールの使用、コンポーネントの再利用には、その認定作業が必要となる。
- 車メーカとサプライヤの分散開発では、共同で規格に適合する責任がある。

ご清聴ありがとうございました

作成者:
株式会社レンタコーチ
http://www.rentaco.jp/

問合せ先:
中村　洋
nakamura@rentaco.jp