既製システムを ISO26262 に適合させる場合の
セーフティケースの利用とその評価

実施報告書

２０１３年２月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

はじめに

IPA/SEC では、ソフトウェア品質説明力を強化すべく様々な観点からの検討を実施してきました。その一環として、ソフトウェア品質を説明するための手法等について具体的な実施方法、そのための作業量、実施にあたっての課題等を整理し、実際にソフトウェア品質を説明する際の参考とできるようにするために、公募により、観点ごとに分けられた実験を別々に実施しました。本書は、それらの結果を、実験ごとにまとめた報告書のうちの１つです。

本報告書の実験は、「2011 年度 システムエンジニアリング実践拠点事業」として、株式会社ベリサーブに委託し実施しました。

「既製システムを ISO26262 に適合させる場合のセーフティケースの利用とその評価」
【報告書】

独立行政法人情報処理推進機構

目次

1. 背景及び目的

組込みソフトウェアの開発においては、自動車分野をはじめ多くの製品分野で、新規に開発されるソフトウェアは少なく、過去に開発したソフトウェアをベースにした差分開発が大部分を占めると言われている。また、日本の開発現場では、製品の最終品質（絶対品質）が重要視されてきたため、開発成果物（設計企画書や概要設計書など）や、最終成果物のソフトウェアに至った経緯（変更履歴及びその理由など）について、詳細に文書化し管理することが難しいという現状がある。

製品の品質を第三者に説明する際、その 1 つの手段として国際安全規格への適応という手段がある。しかしながら、前述した日本独特の開発状況を背景に、例えば ISO26262（自動車の機能安全規格）などに適応するためには、開発成果物の検討経緯を明示する必要があり、現状の開発の進め方では、適応が難しいという問題がある。

本実験では、既に開発を完了している既製システムについて、自動車メーカーにおける一般的な開発成果物を基に開発経緯をヒアリングで確認することにより、ISO26262 に準拠したエビデンス文書を作成（このことを、以下ではリバーストレースと呼称する）する。これにより、既製システムにおける品質説明力向上に要した工数を測定するとともに、その効果を評価・分析する。

2. 模擬実験の概要

2.1 模擬実験の範囲

本模擬実験は、ソフトウェア品質説明力強化の手段として、国際安全規格への準拠という手段に注目し、既に開発を完了している製品を自動車の機能安全に関する国際規格である ISO26262 に準拠させるために必要な情報を収集する。

実験のためのモデルシステムは、自動車用ドアロックシステム（詳細後述）とし、開発ライフサイクルの概要設計～システム設計（ライフサイクルマネジメントプロセスを除く）の開発成果物に対して、リバーストレースを実施する。（Fig2-1 参照）

自動車用ドアロックシステムは、構造や制御の仕組みが比較的シンプルであり、自動車に対する専門知識が無くても理解し易いシステムであると考えられる。一方で、故障時には安全性に大きな影響を与えるシステムであるため、モデルケースとして妥当と考え選定した。

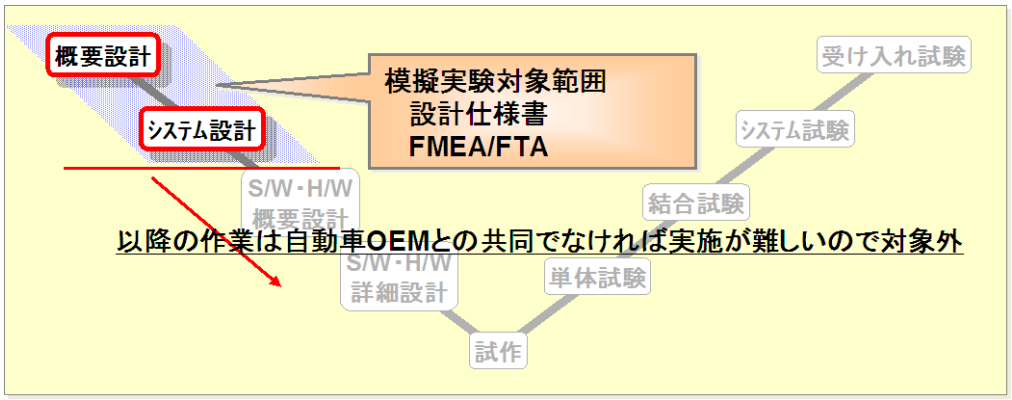


Fig2-1 模擬実験の対象範囲

自動車関連メーカーの従来型開発プロセスにおける「概要設計～システム設計」工程では、ソフトウェア及びハードウェアの具体的なモデルを利用しない場合が多いため、開発成果物に至る検討経緯を詳細にドキュメント化することが難しい領域である。したがって、ISO26262 に準拠する際にも、既存の開発プロセスに対して、ドキュメント化や文書及びトレーサビリティの管理など、新たに追加されるプロセスが多くなる領域と想定される。（Fig2-2 参照）一方で、これ以降の開発プロセスでは、実物の開発が行われるため、自動車関連メーカーなどとの共同作業が必要となることから、本実験の対象範囲外とした。

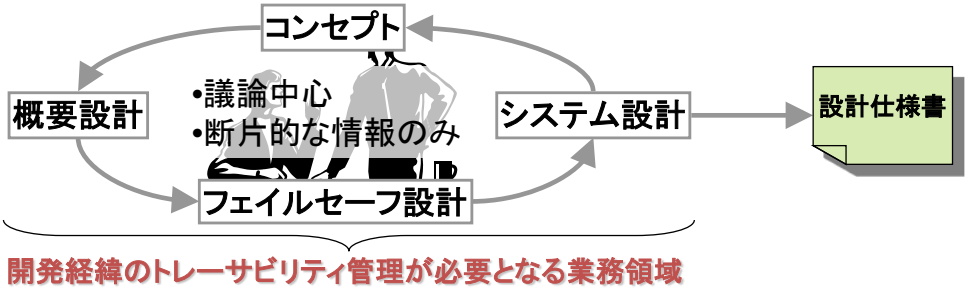


Fig2-2 概要設計～システム設計の業務イメージ

従来型の開発方法（設計仕様書（RFQ*）と FMEA*及び FTA*を開発成果物として、ソフトウェア及びハードウェアを開発する方法）で作成した資料を基に、開発者（ここでは想定される人材要件を持った者）へのヒアリングを行う。得られたヒアリング結果から、開発成果物が作成された経緯が明らかになるように体系化し、ISO26262 に準拠するために必要なエビデンス文書を作成するとともに、その作業工数を計測する。

※RFQ（Request for Quotation）：外注先（候補含む）などへ価格及びその内訳を示す見積もりを作成するように依頼する見積依頼書

※FMEA（Failure Mode and Effects Analysis）：設計段階において、開発するシステムの故障モードを抽出し、発生時におけるシステム全体への影響度合いをレベル分けする手法

※FTA（Fault Tree Analysis）：システムに発生する故障や事故を想定し、その発生原因についてツリー構造で論理展開し、最下層の問題事象の発生頻度から発生確率を算出するとともに、ツリー構造の解析から、発生経路、発生原因を解析する手法

2.2 全体アプローチ

本実験は、リバーストレースのプロセスを想定して実施する。リバーストレースでは、開発成果物が作成された経緯を明らかにするために、経緯の内容を網羅的にかつ構造化された状態でまとめる必要がある。そのために、本実験では GSN（Goal Structuring Notation）* を活用して、ISO26262 に準拠できるように、開発経緯を構造化した文書にまとめる。その上で、ISO26262 の要求事項と対比し適合可否の判定を行うことで、GSN を活用した品質説明力強化の取組みの効果を評価する。また同時に、一連の作業に掛かった工数を計測・算出し、開発プロセスへの業務負荷を評価することにより、リバーストレースにより ISO26262 に準拠する場合の業務負荷を分析する。詳細なアプローチ及びタスクは Fig2-3 の通り。

※GSN（Goal Structuring Notation）：

3 要素の議論文書　①システムの安全性要求（クレーム）、②テストデータなどの根拠（エビデンス）、③クレームに対応するエビデンスの議論（アーギュメント)の関係性をツリー構造やグラフなどにより構造化し、視覚的に表現する手法。この手法を活用することで、システムに不足しているエビデンスを顕在化や議論の明瞭化を図ることができる。(詳細「4.4 本

実験で使用する説明力強化ツール」参照）

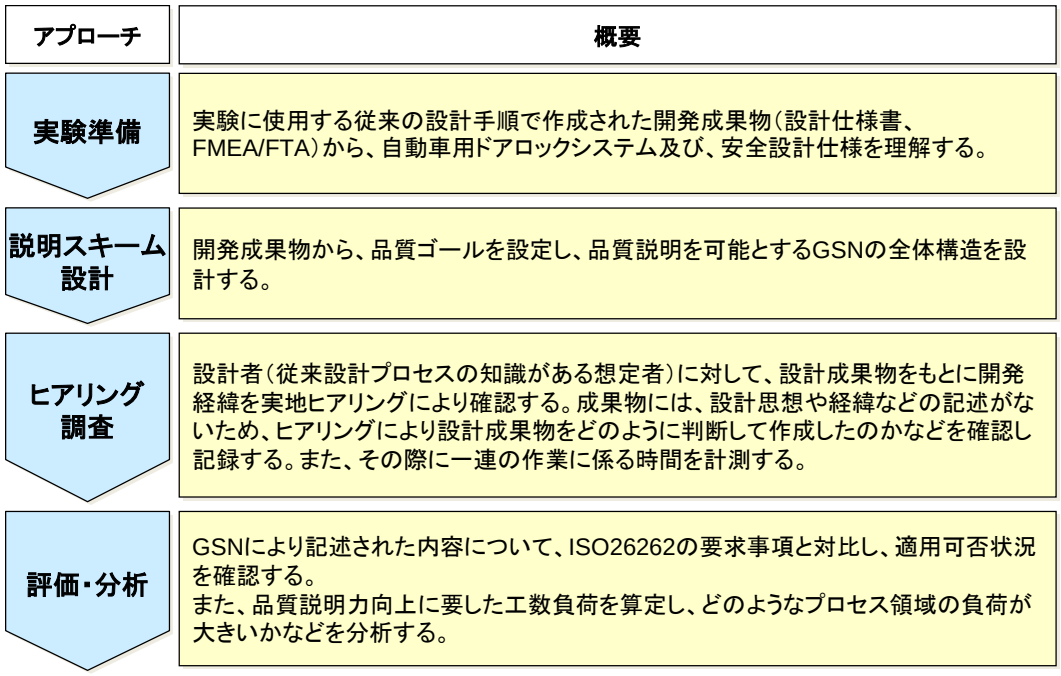


Fig2-3 模擬実験の全体アプローチと主要タスク

2.3 評価方法

本実験では、概要設計～システム設計の開発成果物に対してリバーストレースを実施した場合に、以下 2 点について計測・評価を行う。

・ISO26262 の要求事項への対応可否
・リバーストレースに係る一連の作業工数の計測・算定

2.3.1 ISO26262 の要求事項への対応可否評価

評価指標：適合項目数（単位：個）
適合項目カバレッジ（単位：%）

概要設計～システム設計における ISO26262 の要求事項のうち、リバーストレースによる適合項目数及びカバレッジを計測することにより、GSN を活用したリバーストレースの有効性を評価する。

2.3.2 リバーストレースに要した作業工数評価

評価指標：作業工数（単位：人月）

概要設計～システム設計における開発成果物のリバーストレース作業に要した工数を、実地に計測し、作業工数の大きい業務領域について分析を実施する。

3. 実験対象システムの概要

本実験では、自動車に関する高度な専門知識が無くても理解しやすいことと、不具合発生時に搭乗者の安全に関わる機能であることから、自動車用オートドアロックシステム（以下本システム）を対象として実験を実施した。

3.1　自動車用オートドアロックシステムの主要機能

実験に使用した本システムは、市販車のオートドアロックシステムに近い仕様とするために、基本機能（ドアロック・アンロック機能、車速感応オートロック機能）以外に、トランクリッドのアンロック機能、エアバッグ連動オートアンロック機能、及びチャイルドプルーフのアンロック機能を設定した。エアバッグ連動オートアンロック機能については、当該機能に不具合が発生した場合には、搭乗者の安全に関わる可能性があるため、ISO26262 の適用対象システムになるものと考えられる。

また、当初はフュエルリッドのアンロック機能を設定する予定だったが、当該機能は燃料の盗難防止を目的とした機能であり、安全には影響を及ぼさない機能であることから、本システムからは除外した。

本システムの主要機能をまとめると Fig3-1 の通りである。

機能	仕様
ドアロック･アンロック機能	ドアロックボタン押下により全ドアのロック･アンロック作動
車速感応オートロック機能	車速約30km/h以上で自動ドアロック作動
トランクリッドアンロック機能	車速約10km/h未満でトランクリッドオープナーボタン押下によりトランクリッドアンロック作動
エアバッグ連動オートアンロック機能	エアバッグ作動時にオートアンロック作動
チャイルドプルーフアンロック機能	チャイルドプルーフボタン押下によりチャイルドプルーフアンロック作動
その他の要件	チャイルドプルーフと非干渉にドアロック･アンロックされること 「ドアロック･アンロック機能」不作動時にドアロックレバーにてアンロックできること 「ドアロック･アンロック機能」不作動時に外部よりキー操作にてアンロックできること

Fig3-1 自動車用オートドアロックシステムの主要機能

3.2　アクチュエータ部

本システムのアクチュエータは、電動モーターの動力をモーター軸のウォームギアを介し

てラックアンドピニオンギアに伝達し、ラックギアに連結された調整レバーを稼働させることで、ドアロックの施錠・開錠を行う。(Fig3-2 参照)

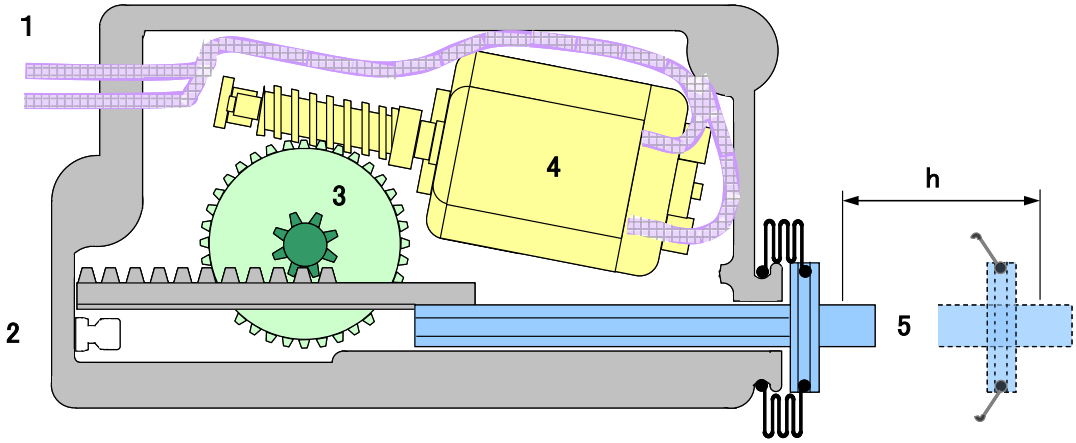


Fig3-2 自動車用オートドアロックシステムのアクチュエータイメージ

3.3 制御部

本実験では、ECU 部分の制御仕様により、周辺デバイスが仕様通りに作動するかどうかについて、シミュレーションにより確認する。(Fig3-3 参照)

本システムにおける制御方法は、各センサーからのアナログ入力(車速センサーなど)、CAN 信号、エアバッグ作動信号(K-Line:車内通信方式の一つ ISO-9141-2、ISO-14230-4 にて規定)、各スイッチ(ドアロック、チャイルドプルーフなど)からの ON/OFF 入力により、所定条件に従った ON/OFF 制御信号を発信することで、制御される。

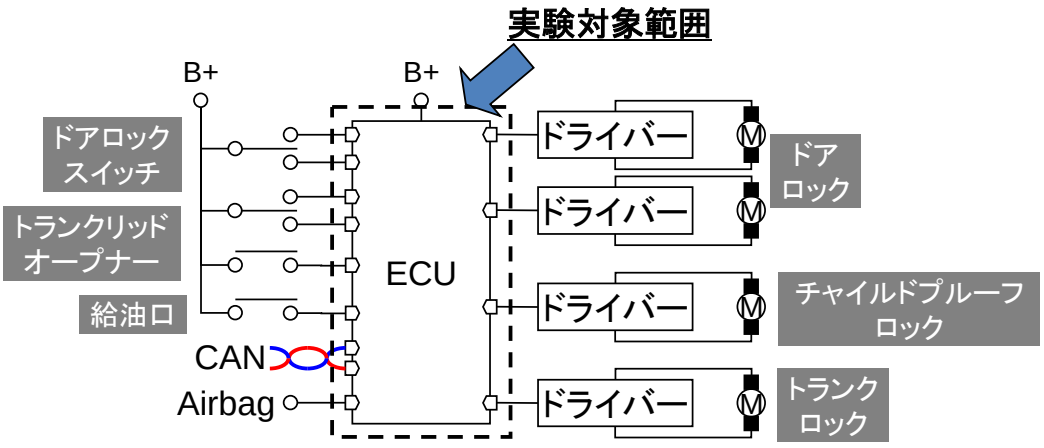


Fig3-3 自動車用オートドアロックシステムにおける実験対象範囲

4. 実験方法

4.1 機能安全レベル

既に述べたように、本実験は対象とするシステムを国際規格であるISO26262 に準拠させることを想定しているため、ISO26262 で規定されている機能安全レベルを設定（選択）した。本システムの開発は、従来型の開発プロセスによって進められたことを想定しており、ASIL[1] Dで要求されるシミュレーションを活用したモデルベース開発の手法を採っていない。したがって本実験では、モデルベース開発が必須とはならないASIL Aを機能安全レベルとして設定し、リバーストレースによるISO26262 への適合可否を評価した。

4.2 本実験で対象とする ISO26262 のセクション

本実験では、前述（詳細は「2.1 模擬実験の範囲」参照）の通り、開発ライフサイクルの「概要設計～システム設計」を対象範囲として、ISO26262 に準拠するような開発プロセスを仮想的に進める。本実験の対象範囲に該当する ISO26262 のパート、及びセクションは Fig4-1 の通りである。以下の項目では、各セクションにおいて ISO26262 が要求するタスクと成果物を説明する。本実験では、成果物と GSN により保証された内容とを対比することで、リバーストレースによる ISO26262 への準拠レベルを評価する。

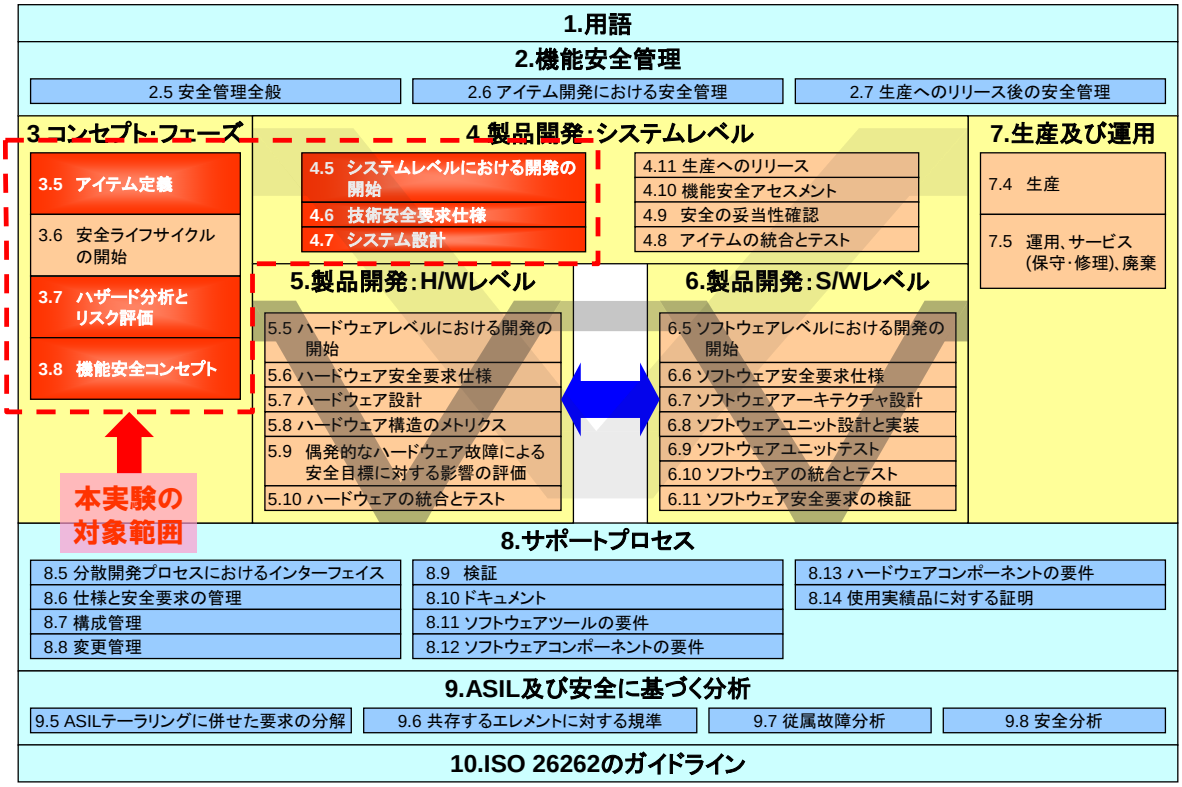


Fig4-1 ISO26262 の対象範囲

[1] ASIL：Automotive Safety Integrity Level
リスクを許容水準に抑えることを達成するための安全性の要求 A(要求レベル低)~D(要求レベル高)までのレベルがある。

4.2.1 「3.5 アイテム定義」

「3.5 アイテム定義」では、関係者間で開発対象についての共通認識を形成するために必要な情報を定義する。要求されるタスクと成果物は以下の通りである。

［要求タスク］

- 開発対象システムと周辺環境の依存関係の明確化
- 開発対象システムとそのインターフェース部分、周辺システムの境界の明確化

［要求成果物］

- アイテム定義書

4.2.2 「3.7 ハザード分析とリスク評価」

「3.7 ハザード分析とリスク評価」では、開発対象システムの故障が原因のリスクを一般に許容される範囲内に収めるために、ASIL レベルとセーフティゴール（最上位レベルの安全要求）を設定する。要求されるタスクと成果物は以下の通りである。

［要求タスク］

- 状況分析とハザードの特定
- 危険事象のレベル分け
- ASIL とセーフティゴールの決定
- ハザード分析･リスク評価結果に対する検証
- セーフティゴールに対する検証

［要求成果物］

- ハザード分析とリスク評価結果
- セーフティゴール
- 検証結果報告書

4.2.3 「3.8 機能安全コンセプト」

「3.8 機能安全コンセプト」では、「3.7 ハザード分析とリスク評価」で設定したセーフティゴールを具体的に落とし込んだ機能安全コンセプトを策定する。機能安全コンセプトには、セーフティゴールから導出された機能安全要求、当該要求を開発対象システムの各要素に割り当てる際の考え方、及び最終的に開発されたシステムの妥当性を確認する際の基準が盛り込まれる。要求されるタスクと成果物は以下の通りである。

［要求タスク］

- 機能安全要求の導出
- システム要素への機能安全要求割り当て
- 妥当性確認基準の設定
- 機能安全コンセプトに対する検証

［要求成果物］

- 機能安全コンセプト
- 機能安全コンセプトに対する検証結果報告書

4.2.4 「4.5 システムレベルにおける開発の開始」

「4.5 システムレベルにおける開発の開始」では、システムレベル開発プロセスにおける機能安全を実現するためのアクティビティを計画する。要求されるタスクと成果物は以下の通りである。

［要求タスク］

- 安全性を考慮した設計、インテグレーションの計画
- 妥当性確認の計画
- 機能安全アセスメントの計画
- システムレベルにおける安全ライフサイクルの開発プロセスへのテーラリング

［要求成果物］

- プロジェクト計画書
- 安全計画書
- インテグレーション計画書
- テスト計画書
- 妥当性確認計画書
- 機能安全アセスメント計画書

4.2.5 「4.6 技術安全要求仕様」

「4.6 技術安全要求仕様」では、機能安全コンセプトを具体的に実現する技術要件を定義する。技術安全要求には、システムが故障した際の検出･表示･制御、及びシステムの安全状態維持などに関する技術要件を盛り込む必要がある。要求されるタスクと成果物は以下の通りである。

［要求タスク］

- 技術安全要求仕様の策定
- 開発システムにおける安全メカニズムの検討
- ASIL のディコンポジション
- 潜在的故障の回避方法検討
- 生産フェーズ以降における該当箇所の特定
- 技術安全要求に対する検証と妥当性確認

［要求成果物］

- 技術安全要求仕様書

- システム検証報告書
- 妥当性確認計画書

4.2.6 「4.7 システム設計」

「4.7 システム設計」では、システムに対する機能要求をハードウェア、及びソフトウェアで実現する方策を開発する。その際に、技術安全要求仕様をハードウェア、及びソフトウェアに割り当てる際の考え方と、これらを統合した際に技術安全要求が実装されていることを確認する方策などを検討する。要求されるタスクと成果物は以下の通りである。

［要求タスク］

- システム設計仕様の検討
- 技術安全コンセプトの検討
- システム構造設計に関する制約条件の考慮
- システム的な故障に対する回避措置の検討
- ハードウェアの偶発的な故障に対する制御措置の検討
- ハードウェアとソフトウェアへの技術安全要求の割り当て
- ハードウェア、ソフトウェアのインターフェース仕様の検討
- 生産フェーズ以降における要求の考慮
- システム設計に対する検証

［要求成果物］

- 技術安全コンセプト
- システム設計仕様書
- ハードウェア、ソフトウェアインターフェース仕様書
- 生産フェーズ以降に対する要求仕様書
- システム検証報告書
- 安全分析報告書

4.3 本実験で使用する開発成果物

本実験では、設計仕様書（RFQ）と FMEA/FTA の実施結果のみが本システムの開発成果物として残されていることを前提している。また、これらの開発成果物が作成された経緯については、議事録及び開発者へのヒアリングを基にして、GSN 展開を実施し、ISO26262 への適合可否について評価した。

以下では、本システムにおける開発成果物の内容について説明する。

4.3.1 設計仕様書（RFQ）

本実験で使用する設計仕様書（RFQ）は、ユースケース、システム概要図、ハードウェアインターフェース仕様、ソフトウェアインターフェース仕様、ハードウェア仕様、ソフトウ

ェア仕様からなる。以下では、設計仕様書（RFQ）を構成するそれぞれの要素について説明する。

概要設計工程で、設計仕様書（RFQ）のユースケース、及びシステム概要図を作成する。後述の FMEA/FTA を実施後に、システム設計工程で詳細の内容を作成した。本実験では、設計仕様書（RFQ）を作成する際の検討経緯を示す議事録についても、設計仕様書（RFQ）の一部と見なして実験を実施した。

4.3.1.1 ユースケース

運転者及び同乗者のユースケース図を作成することによって、本システムに必要な機能を抽出した。ここでは、本システムを運転者及び同乗者が操作するために必要とする情報や、本システムの動作に関わる他システムからの情報についても記載した。

ユースケース図を作成することによって、実現するべき機能をどのシステムで実現するかを決定した。作成したユースケース図は Fig4-2 の通りである。

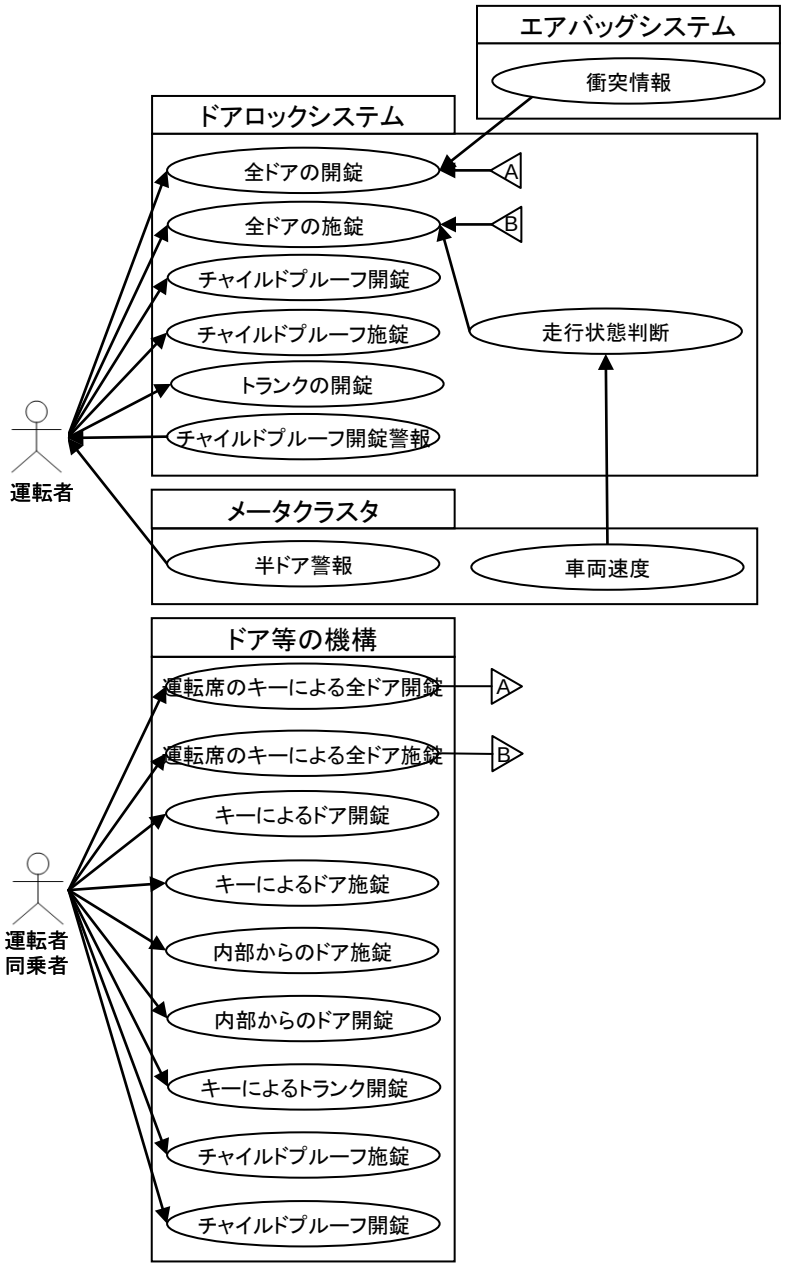


Fig4-2 本システムのユースケース図

4.3.1.2 システム概要図

4.3.1.1 で定義された機能に基づき、システム概要図を作成した。システム概要図では、本システムと外部のシステムとのインターフェース、及び本システムのハードウェアとソフトウェアとのインターフェースを記載している。作成したシステム概要図は Fig4-3 の通りである。

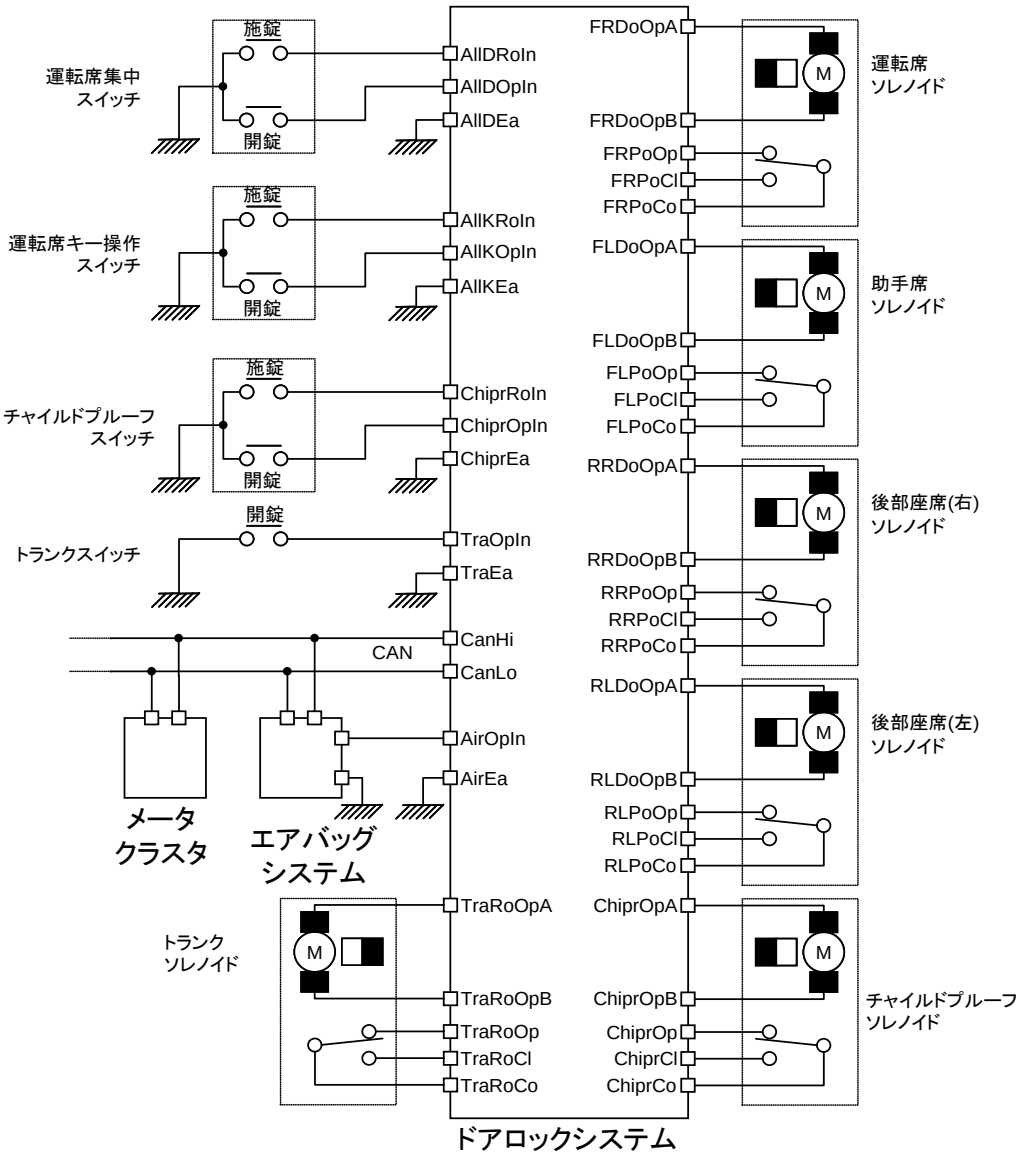


Fig4-3 本システムのシステム概要図

4.3.1.3 ハードウェアインターフェース仕様

本システムを構成するハードウェアごとに、ソフトウェアとのインターフェース部分に関する仕様をハードウェアインターフェース仕様として作成した。作成したハードウェアインターフェース仕様のサンプルは Fig4-4 の通りである。

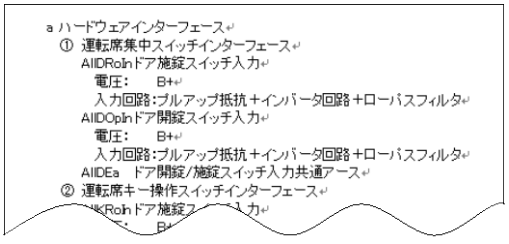


Fig4-4 ハードウェアインターフェース仕様サンプル

4.3.1.4 ソフトウェアインターフェース仕様

本システムを構成するソフトウェアの機能ブロックごとに、ハードウェアとのインターフェース部分に関する仕様をソフトウェアインターフェース仕様として作成した。作成したソフトウェアインターフェース仕様のサンプルは Fig4-5 の通りである。

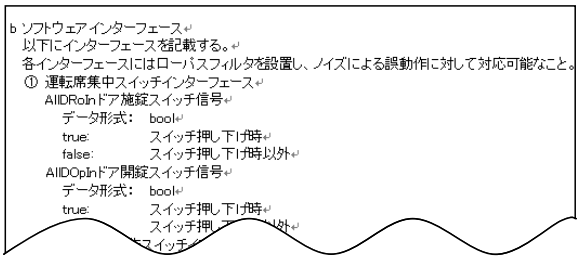


Fig4-5 ソフトウェアインターフェース仕様サンプル

4.3.1.5 ハードウェア仕様

本システムに使用するハードウェアの条件をハードウェア仕様として作成した。作成したハードウェア仕様のサンプルは Fig4-6 の通りである。

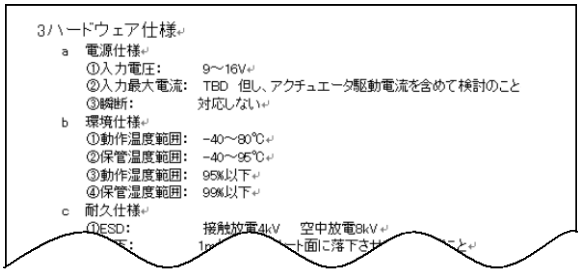


Fig4-6 ハードウェア仕様サンプル

4.3.1.6 ソフトウェア仕様

本システムのソフトウェアを機能ごとに分割して、機能同士のインターフェースを定めたソフトウェア機能ブロック図（Fig4-7）を作成した。また、ソフトウェアの機能間でデータを入出力する関係についてもブロック入出力の一覧（Fig4-8）を作成することで、ソフトウェア仕様として定めた。

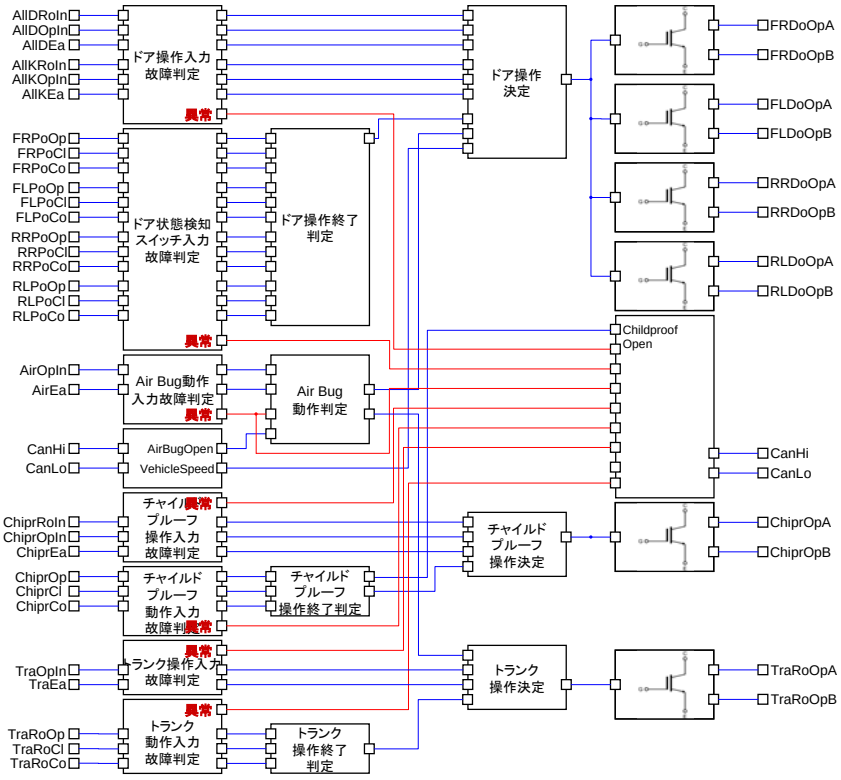


Fig4-7 ソフトウェア機能ブロック図

部	入力		出力		機能
	データ名称	データ形式	データ名称	データ形式	
集中ドア操作入力判定部	AllDRoIn	bool	AllDoorLockOperation	unsignedchar	・スイッチ及びキー操作のデータの入力からドアロックを開錠するか施錠するかを判断 ・開錠/施錠の判断結果を車両速度制御部に出力 ・ドアの状態判定結果から、開錠/施錠の操作信号を終了
	AllDOpIn	bool			
	AllKRoIn	bool			
	AllKOpIn	bool			
	AllDoorLocked	bool			
	AllDoorUnlocked	bool			
ドアロックポジションセンサ入力判定部	FRPoOp	bool	DoorLockStatus	unsignedchar	・各ドアのポジションデータを判断 ・判断結果をドアロック及びトランクリッド施錠判断部に出力
	FRPoCl	bool			
	FLPoOp	bool			
	FLPoCl	bool			
	RRPoOp	bool			
	RRPoCl	bool			
	RLPoOp	bool			
	RLPoCl	bool			
チャイルドプルーフ操作入力判定部	ChiprRoIn	bool	ChildProofOperation	unsignedchar	・スイッチ操作のデータの入力からチャイルドプルーフを設定/解除するかを判断 ・設定/解除データを判断結果を車両速度制御部に出力 ・チャイルドプルーフの状態判定結果から、設定/解除の動作信号を終了
	ChiprOpIn	bool			
	ChildProofLocked	bool			
	ChildProofUnlocked	bool			

Fig4-8 ブロック入出力一覧

4.3.2 FMEA/FTA

設計仕様書（RFQ）に記載されている内容に対して、本システムが安全面における問題点を FMEA/FTA を実施して抽出した。FMEA/FTA によって抽出された問題点については、安全面に問題が無い状態にする必要があるため、そのための方策を推奨是正措置として定めた。

従来型の開発プロセスでは、FMEA/FTA を実施した結果により定められた推奨是正措置

を設計仕様書（RFQ）に反映することによって、本システムが安全面における問題が生じることの無いように開発が進められていく。

FMEA/FTA の実施結果のサンプルは Fig4-9 に示す通りである。

項目	故障モード	故障の影響	状況	故障事象	重大度	故障メカニズム	発生頻度	検出方法	非検出性	制御方法	非制御性	危険優先度	推奨是正措置
運転席集中スイッチ	施錠スイッチ常時 OFF	ドアをロックできない	停車中(乗降中)	ドアをロックできない	4	スイッチ故障	2	無し	10	機械的なロック	1	80	A-a. 機構側でのロックを可能とする
運転席集中スイッチ	施錠スイッチ常時 OFF	ドアをロックできない	停車中(ACC OFF)	ドアをロックできない	4	スイッチ故障	2	無し	10	機械的なロック	1	80	A-a. 機構側でのロックを可能とする
運転席集中スイッチ	施錠スイッチ常時 OFF	ドアをロックできない	停車中(ACC ON)	ドアをロックできない	4	スイッチ故障	2	無し	10	機械的なロック	1	80	A-a. 機構側でのロックを可能とする
運転席集中スイッチ	施錠スイッチ常時 OFF	ドアをロックできない	停車中(IG ON)	ドアをロックできない	4	スイッチ故障	2	無し	10	機械的なロック	1	80	A-a. 機構側でのロックを可能とする
運転席集中スイッチ	施錠スイッチ常時 OFF	ドアをロックできない	走行中	低速走行中にドアが開き、人が落下	9	スイッチ故障	2	無し	10	半ドア警報により運転手に通知	3	540	A-a. 機構側でのロックを可能とする
運転席集中スイッチ	施錠スイッチ常時 OFF	ドアをロックできない	走行中	低速走行中にドアが開き、モノが落下	8	スイッチ故障	2	無し	10	半ドア警報により運転手に通知	3	480	A-a. 機構側でのロックを可能とする
運転席集中			走行中	低速走行中		イッチ故	2	無し				540	A-a. 機構側で を可能

Fig4-9 FMEA/FTA の実施結果サンプル

4.4　本実験で使用する説明力強化ツール

本実験では、システムの安全性を保証するための根拠を示すために、セーフティケースと呼ばれる理論的な枠組みである GSN を使用する。セーフティケースは安全性がいかに保証されるかを、構造化された議論（Structureed argumentation）により示すものである。

本実験において使われる GSN の基本的な記号は Fig4-10 の通りである。

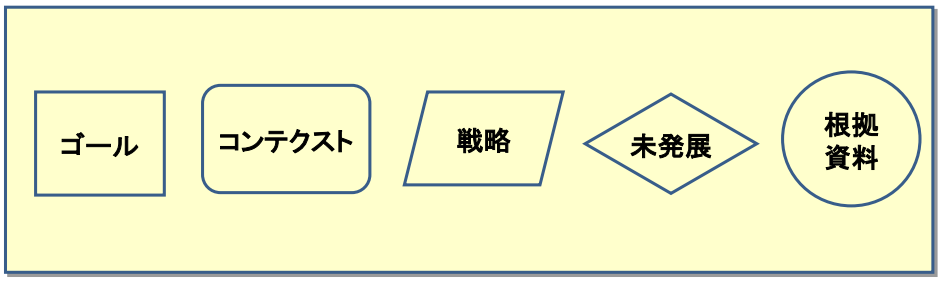


Fig4-10 GSN のモデル要素

・ゴール（Goal）：システムにより満足されるべき要件、制約。ゴールはより詳細な部分ゴールに分解される。

・コンテクスト（Context）：ゴールを具体的に説明する参照項目や資料。

・戦略（Strategy）：ゴールから部分ゴールを導く際の規則や方針。

・未発展（Undeveloped）：関係する議論や資料がなく、より詳細な議論がなされない状態。

・根拠資料（Evidence）：ゴールが成立するための根拠資料。具体的には、ゴールを成立させるための証拠、分析結果、承認者の報告書である。

GSN における機能安全を保証する議論の形式は、Fig4-11 の通りである。

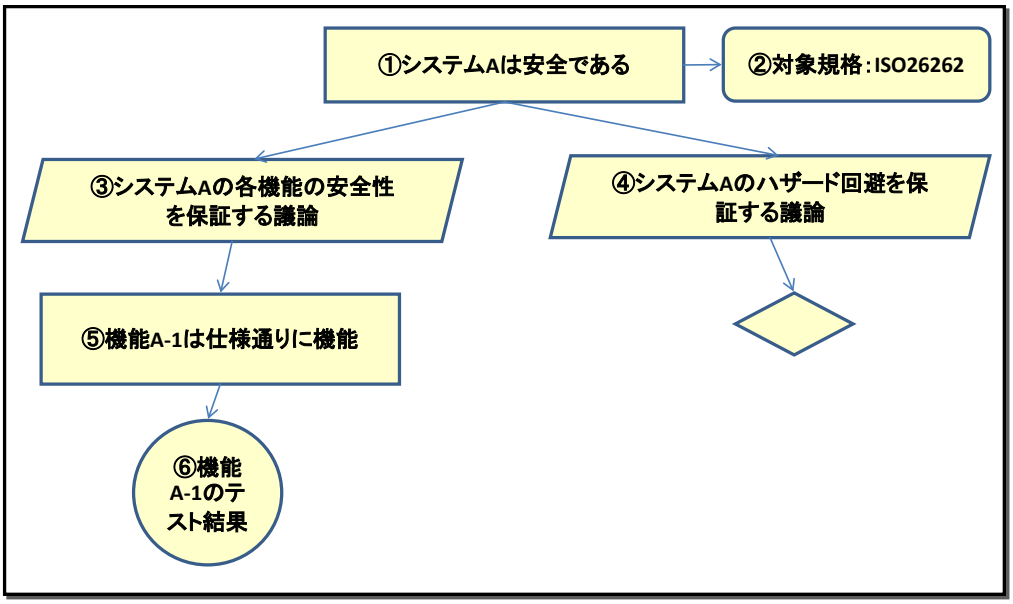


Fig4-11 GSN による議論記述イメージ

ここでは、トップのゴール(①)を設定し、それに対してより詳細な部分ゴール(⑤)を導き出す方策を戦略(③)として記述する。戦略(③)に基づいて部分ゴール(⑤)を導き出し、その部分ゴールがそれ以上詳細化できない場合に、成立するための根拠となる根拠資料(⑥)を記述する。また、戦略(④)については、部分ゴールや根拠資料を設定できない場合には未発展として、十分に保証できないことを示している。

Fig4-11 では、機能 A-1 をテストにより機能検証を行い、その部分ゴール(⑤)の保証が満足されることを示す。

また、GSN図作成には、DEOSプロジェクト[2]で開発されたD-case editor（Eclipseプラグイン）を使用した。本エディターは以下からダウンロード可能であり、無償で利用可能である。

http://www.il.is.s.u-tokyo.ac.jp/deos/dcase/

4.5　新たに必要となるリバーストレースプロセス（想定）の定義

本実験では、既製システムを開発する際に作成した開発成果物を基にして GSN 展開することにより、ISO26262 への適合性に関する論拠を示すまでの一連のプロセスをリバーストレースプロセスとして定義した。

---

2 「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」（DEOS（Dependable Embedded Operating Systems）プロジェクト）は、（独）科学技術振興機構（JST）/CREST の研究領域の 1 つとして、2006 年 10 月に開始された。DEOS は OSD（Open Systems Dependability）を実現するための知識・技術を体系だてたもの。CREST は JST の戦略的創造研究推進事業。

本実験において定義したリバーストレースプロセスは Fig4-12 の通りである。

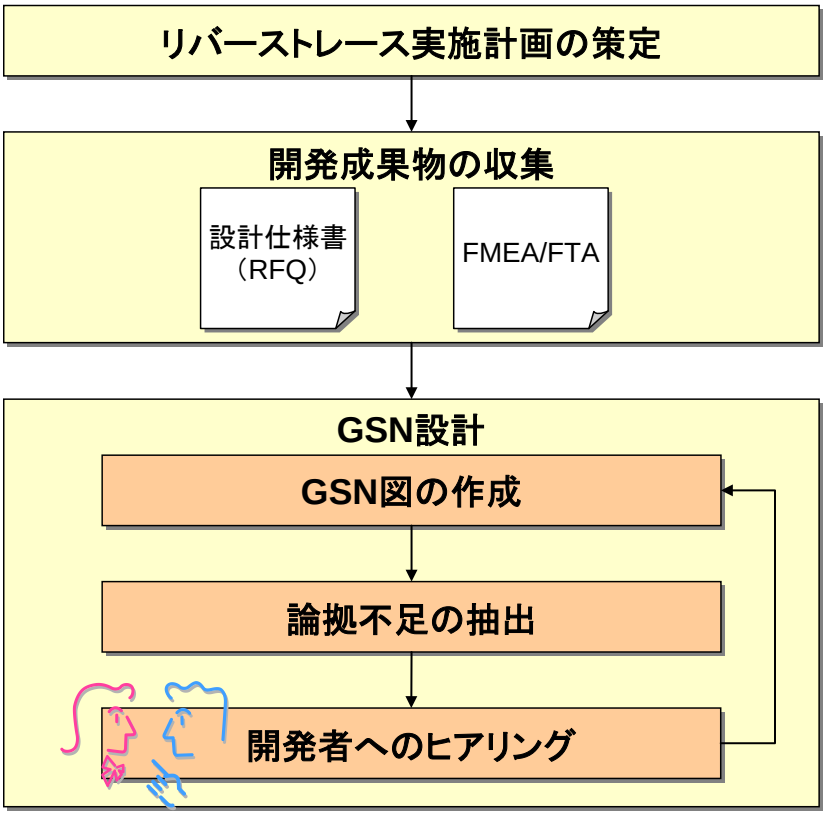


Fig4-12 リバーストレースプロセス

4.5.1 リバーストレース実施計画の策定

GSN を利用したリバーストレースを実施することにより達成したい目標、及びリバーストレース実施の全体計画を GSN 作成者と開発者との間で策定した。本実験では、既製システムに対する ISO26262 への適合可否を評価することを目標としているため、リバーストレース実施の目標を、既製の本システムを ISO26262 へ準拠させることとして設定した。

本実験で参照した ISO26262 のセクションは「4.2 本実験で対象とする ISO26262 のセクション」で提示した通りであるが、「4.5 システムレベルにおける開発の開始」、及び「4.7 システム設計」については、リバーストレース実施の計画を検討する中で、GSN 図の作成対象から除外している。

「4.5 システムレベルにおける開発の開始」では、既製システムを開発する際に立てた計画の前提として、安全文化を盛り込んだ社内規程が制定されていること、及び ISO26262 の安全ライフサイクルを実際の開発プロセスにテーラリングされていることが重要である。これらの前提については、既に完成しているものとして本実験を進めているため、「4.5 システムレベルにおける開発の開始」を GSN 図の作成対象から除外した。

「4.7 システム設計」については、ISO26262 によって要求される成果物がシステム詳細設計書とシステム設計の検証結果であり、実際の開発成果物を確認したところ、GSN 図を作

成しなくとも要求事項を満足できることが判明したため、対象から除外した。

4.5.2 開発成果物の収集

リバーストレース実施計画の策定を受けて、GSN 図を作成する対象の開発成果物を開発者が収集し、GSN 作成者へと提示した。

本実験では、設計仕様書（RFQ）と FMEA/FTA に加え、これらの開発成果物を作成した経緯が分かるような議事録についても、リバーストレースの対象として収集、提示した。

また、ISO26262 の要求を満足するためには、本システムに対して ASIL を決定しなければならないが、本システムを開発した当時には ISO26262 が存在していなかったという想定のため、ASIL が設定されていない。したがって、FMEA/FTA の実施結果を基にして、追加で ASIL 決定を行うことで代替した。追加部分を検討するために実施した議事録についても、GSN 作成者へと提示した。

4.5.3 GSN 設計

開発者から提示された開発成果物を基にして GSN 図を作成する。「GSN 図の作成」、「不足部分の抽出」、「開発者へのヒアリング」というプロセスを、ISO26262 への準拠を示す論拠に対して不足部分が無くなるまで繰り返し実施する。

一般的に、GSN 図はシステム構造設計から、システムを構成する個々の要素に対して作成される。しかしながら本実験では、比較的シンプルなシステム構成の自動車用オートドアロックシステムを採用したことと、ISO26262 への準拠に主眼を置いたことから、ISO26262 のパート毎に GSN 図を作成して、開発成果物の不足部分を明確にした。

4.5.3.1 GSN 図の作成

開発成果物を基にして、GSN 作成者が D-case editor で GSN 図を作成した。「4.4 本実験で使用する説明力強化ツール」の通り、GSN 図はゴールに対して、論拠を示すための戦略や根拠資料を木構造によって示している。GSN 作成者は、入手した開発成果物からこれらの関係性を分析する。開発成果物を分析するだけでは不明な点については、開発者に質問することによって明確にした。

本実験において GSN 設計を繰り返し実施しているため、GSN 図の作成は複数回実施される。最初の GSN 図作成を GSN 概要設計とし、2 回目以降の GSN 図作成を GSN 詳細設計とした。まず、ISO26262 のパート毎に GSN 図の全体構造を設計することで、GSN 概要設計とした。GSN 詳細設計では、最初の GSN 図作成で不足していた部分の記述や詳細化を行っている。

4.5.3.2 論拠不足の抽出

GSN 図を作成する中で、GSN 作成者が入手した開発成果物のみでは、ゴールの論拠としては不十分な項目が発見される。こういった項目は、最終的な GSN 図においては解消され

る必要があるため、課題として抽出する。

4.5.3.3 開発者へのヒアリング

ゴールに対する論拠が不足している項目を開発者へヒアリングすることによって補強する。ヒアリングした結果については、再度 GSN 設計のプロセスを実施することによって、GSN 図へと反映していく。通常は、論拠不足項目が無くなるまで GSN 設計のプロセスを実施しなければならないが、本実験では既製システムを ISO26262 に準拠させるための検討課題として抽出するに留めている。

4.6　メトリクスの定義及び収集方法

本実験では、「2.3 評価方法」で定義したとおり、「概要設計～システム設計」の開発成果物に対して、リバーストレースを実施した場合の工数、及び導入効果について、以下 2 点の評価指標により計測、評価を行った。

- ISO26262 の要求事項への対応可否
- リバーストレースに係る一連の作業工数の計測

以下では、これらの評価指標を収集するために、本実験で実施した計測方法についての詳細を説明する。

4.6.1 ISO26262 の要求事項への対応可否評価

既製システムを ISO26262 に準拠するための手法として、GSN を活用したリバーストレースが有効であるか否かを評価する。ここでは、リバーストレースによる ISO26262 への適合項目数と、適合項目のカバレッジを測定する。

本実験では、「4.3 本実験で使用する開発成果物」に記載されている開発成果物のみが残されている状況を想定している。これらの開発成果物は ISO26262 を参照せずに作成したものであり、既製システムを ISO26262 に準拠させるためには、ISO26262 の要求事項を満足していることの根拠を示す必要がある。

「4.2 本実験で対象とする ISO26262 のセクション」で示した要求タスクのうち、開発成果物と開発成果物が作成された経緯のみを対象とした GSN を利用したリバーストレースによって、満足することが可能であるという論拠が示された項目数、及びカバレッジの割合を指標として計測した。

本実験により算出された指標を分析することによって、既製システムに対して GSN を利用したリバーストレースを実施することのみで、ISO26262 へ準拠することが可能かどうかの評価を行う。

4.6.2 リバーストレースに要した作業工数評価

既製システムに対して、リバーストレースを実施して ISO26262 の要求事項を満足するための論拠を示した場合に、新たに発生する作業工数を時間単位で測定した。作業工程ごとの測定方法は以下の通りである。

・リバーストレース実施計画策定

GSN を利用したリバーストレースを実施する計画の立案、及び開発者と GSN 作成者の間での計画合意に要した工数を測定した。GSN 作成者と開発者とのミーティング形式による計画策定を行ったため、両者がミーティングに拘束された時間を工数として計測している。

・開発成果物の収集

本システムを開発した際に作成された、既存の開発成果物を収集するのに要した工数を測定した。既存の開発成果物のみでは作成した経緯を説明できない場合、開発時の議論が議事録として残されていないか過去の資料から探索した。資料の探索に要した工数についても、開発資料収集に要した工数として計上した。

・開発成果物の分析

開発者から提示された既存の開発成果物等の資料を、GSN 作成者が読解、分析するのに要した工数を測定した。GSN 作成者が資料を読むだけでは理解できなかった部分については、開発者に対してヒアリングすることに解決する形式を採ったため、ヒアリングに要した工数についても測定して算入している。

・GSN 概要設計

既存の開発成果物、及び ISO26262 の要求事項から GSN 図の概要を作成するのに要した工数を計測した。

また、GSN 図の概要を設計する中で、開発成果物の不明箇所を開発者に対して質問して解決する形式を採ったため、開発者が質問に要した時間についても工数として計上している。さらに、作成された GSN 図の概要設計については、開発者とのレビューミーティングにより承認するという、手続きを採ったため、GSN 作成者と開発者がミーティングに拘束された時間についても当該項目の工数として計上している。

・GSN 詳細設計

既存の開発成果物、及び ISO26262 の要求事項から GSN 図の詳細内容を作成するのに要した工数を計測した。

また、GSN 図の詳細を設計する中で、開発成果物の不明箇所を開発者に対して

質問して解決する形式を採ったため、開発者が質問に要した時間についても工数として計上している。さらに、作成された GSN 図の詳細設計については、開発者とのレビューミーティングにより承認するという、手続きを採ったため、GSN 作成者と開発者がミーティングに拘束された時間についても当該項目の工数として計上している。

4.7　模擬実験の実施

本実験では、客観性を持たせるために、開発者が行う作業と GSN 図を作成する作業を行う担当者をそれぞれ異なる組織に所属する者により実施した。開発者は、リバーストレースの対象となる開発成果物の収集や、GSN 作成者からの質問への回答など、開発者が行う作業を行い、提示された開発成果物を基にした GSN 図の作成などを、GSN 作成者が行った。

GSN 作成者は本システムの開発には携わっていないので、提示された開発成果物の中で不明な点については、開発者に対して質問する形で本実験を進めた。

本実験において実際に実施した詳細な実験の実施手順を以下に示す。

4.7.1 リバーストレース実施計画の策定

本実験におけるリバーストレース実施による目標の立案、及び全体計画を策定した。平成 24 年 4 月 24 日に開発者と GSN 作成者が会議を行うことによって、リバーストレース実施計画を策定した。

4.7.2 開発成果物の収集

リバーストレース実施計画の策定を受けて、開発者が GSN 図の作成に必要な開発成果物を収集し、GSN 作成者に提示した。本システムを開発した際の検討経緯を示す議事録についても、開発者が探索した上で GSN 作成者に提示した。

4.7.3 GSN 図の作成（第 1 回）

開発者から提示された開発成果物を基に、GSN 作成者が GSN 図の概要を作成した。GSN 作成者は、本システムの開発には携わっていないため、最初に、開発成果物の概要把握や内容理解を行った。開発成果物を読むだけでは不明な点については、開発者に対して質問することで GSN 図の作成を行った。

GSN 概要設計では、ISO26262 の要求事項をベースに GSN 図の構造を設計した。

4.7.4 論拠不足の抽出（第 1 回）

GSN 作成者が、自らが作成した GSN 図を基に、ゴールを示す論拠として不足している項目を抽出した。第 1 回の GSN 図作成から論拠不足の抽出までについては、開発成果物の概要把握や内容理解に多くの時間が掛かったため、約 2 週間の期間を要した。

4.7.5 開発者へのヒアリング（第 1 回）

GSN 作成者が作成した GSN 図と、抽出した論拠不足項目を基に、5 月 7 日に第 1 回ヒアリングを実施した。

1 回目のヒアリングでは、GSN 概要設計に対して合意した上で、抽出された不足項目に関して、議事録などの検討経緯を説明した資料が存在しないかを開発者に対して確認した。ヒアリングを実施した結果、新たに提示する必要があることが判明した検討経緯を示した議事録については、開発者が追加で GSN 作成者に対して提示した。

4.7.6 GSN 図の作成（第 2 回）

第 1 回ヒアリングの結果、及び追加で提示された開発成果物を基にして、GSN 作成者が GSN 概要設計の更新と詳細化を実施した。

4.7.7 論拠不足の抽出（第 2 回）

GSN 図を詳細化する際に新たに発見された、ゴールに対して論拠が不足している項目を抽出した。第 2 回の GSN 図作成から論拠不足の抽出に関しては、GSN 図を詳細化する作業に多くの時間が掛かり、1 週間半の期間を要した。

4.7.8 開発者へのヒアリング（第 2 回）

2 回目の GSN 図作成結果及び、抽出した論拠不足項目を基に、5 月 16 日に第 2 回ヒアリングを実施した。

2 回目のヒアリングでは、GSN 詳細設計を作成する中で抽出された論拠不足の項目について、検討経緯に関する議論を行った。

4.7.9 GSN 図の作成（第 3 回）

2 回目のヒアリングで議論した内容を基に、GSN 図を修正した。本来のリバーストレースプロセスでは、ゴールの論拠が不足している項目が無くなるまで、GSN 図作成から開発者へのヒアリングのプロセスを繰り返し実施するが、本実験では、実験期間の制約があるため、3 回目の GSN 図作成までの作業をリバーストレースプロセスとして実施した。

4.7.10　ギャップ分析

本実験では、3 回目の GSN 図作成までで解消することができなかった論拠不足の項目を、ISO26262 に対して既製システムを準拠させるために実施したリバーストレースの残存ギャップとして定義した。ギャップ分析の結果については、5 月 24 日に報告書として GSN 作成者が開発者に対して提出した。

本実験では、ギャップ分析にて報告された項目を、設計仕様書（RFQ）と FMEA/FTA のみでリバーストレースを実施した際に、ISO26262 の要求事項を満足することができなかった項目として定義した。

5. 実験結果

5.1 GSN による説明構成

本実験では、ISO26262 の Part3 及び Part4 の各 Part 毎に、トップゴールが保証できるかどうか GSN 図を作成し、安全性論拠の充不足部分を明確にした。

5.1.1 ISO26262 Part3 における GSN 図

5.1.1.1 全体構造イメージ

GSN の全体構造のイメージを Fig5-1 に示す。

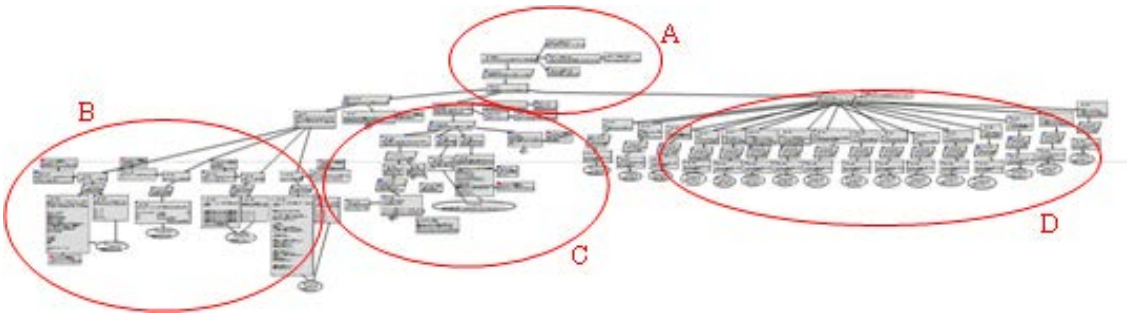


Fig5-1 ISO26262 Part3 GSN 図 全体構造

Fig5-1 は、本システムの安全性を保証する議論が ISO26262 Parts 3 に従って実施されたかどうかについての全体構造イメージを示すものである。

Fig5-1 の各部分構造についての説明を以下に記述する。

要素 A：上部構造

議論の方針を示すトップ構造

要素 B：ASIL 決定基準の妥当性

ASIL の決定に関する基準の妥当性における議論を示す部分構造

要素 C：機能安全概念（Functional safety concept）

機能安全概念が要件通りに定義されていることを保証する部分構造

要素 D：セーフティゴール

定義されたセーフティゴール毎に安全性の議論を行う部分構造

5.1.1.2 上部構造（要素A）

要素 A の全体構造を Fig5-2 に示す。

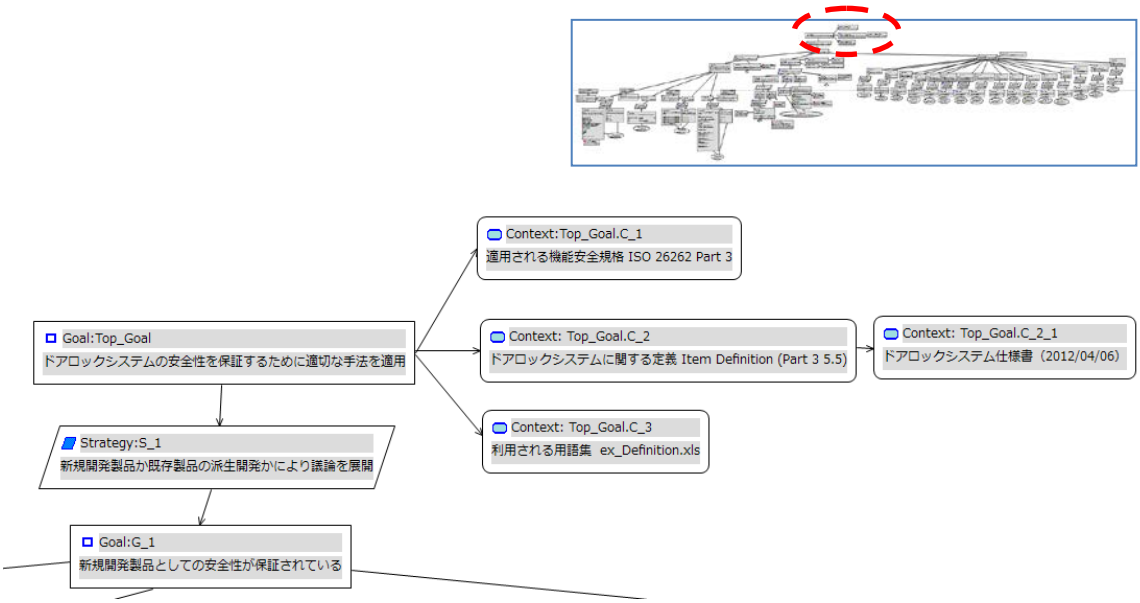


Fig5−2 ISO26262 Part3 要素 A 全体構造

トップゴール（Top_Goal）は本システムの安全性を保証するために適切な手法を適用したかどうかをゴールとして設定した。本ゴールを支援するためのコンテクストとしては、まず、適用される規格に対する参照（Top_Goal.C_1） がある。次に本ゴールが成立するために参照すべき資料として ISO26262 の「3.5 アイテム定義」（Top_Goal.C_2）と 、実際の資料であるシステム設計仕様書（RFQ）が参照されている（Top_Goal.C_2_1）。そして、本議論において利用される用語集があることを資料参照している（Top_Goal.C_3）。

次に、トップゴールを展開するための戦略として、ISO26262 の「3.6 安全ライフサイクルの開始」を参照し、本実験が新規製品開発に当たるのか、それとも派生開発に当たるのかを議論した。本システムは既に開発が終了しており、ISO26262 に準拠するために追加で開発成果物を作成することは想定していない。したがって、部分ゴールとして「新規開発製品としての安全性が保証されている（G_1）」を導出した。

5.1.1.3 ASIL 決定基準の妥当性（要素 B）

G_1 から分岐した部分構造の 1 つが要素 B であり、要素 B は「ASIL の決定に関する基準の妥当性に関する議論」をするためのものである。ここでは、以下の部分ゴールを設定した。

・リスクアセスメントを実施したチームはリスクアセスメントと対象システムに対する十分な知識を持つ（G_11）

・対象部分 item と failure event (hazardous event) の分類とそれに対する S(everity), E(xposure), C(ontrollability) の決定が適切に実施された（G_12）

G_11 は、本実験では対象外としている ISO26262 Part2 の要求事項を参照しているため、未発展（undeveloped）として、これ以上の GSN 展開は実施しなかった。

要素 B の上部構造の例を Fig5-3 に示す。

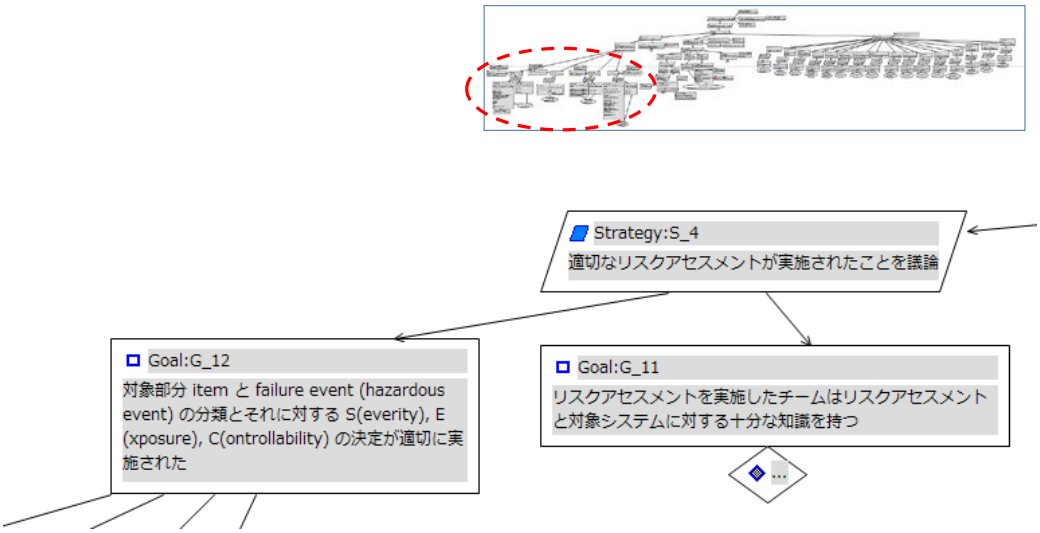


Fig5-3 ISO26262 Part3 要素 B 上部構造（例示）

要素 B の下部構造は、G_12 の部分ゴールである以下の要素から構成されている。

- Severity の設定が適切（G_2）
- Probability の設定が適切（G_3）
- Undetectability の設定が適切（G_4）
- Uncontrollability の設定が適切（G_6）

要素 B の下部構造のうち、Severity（G_2）についての例示記載を Fig5-4 に示す。

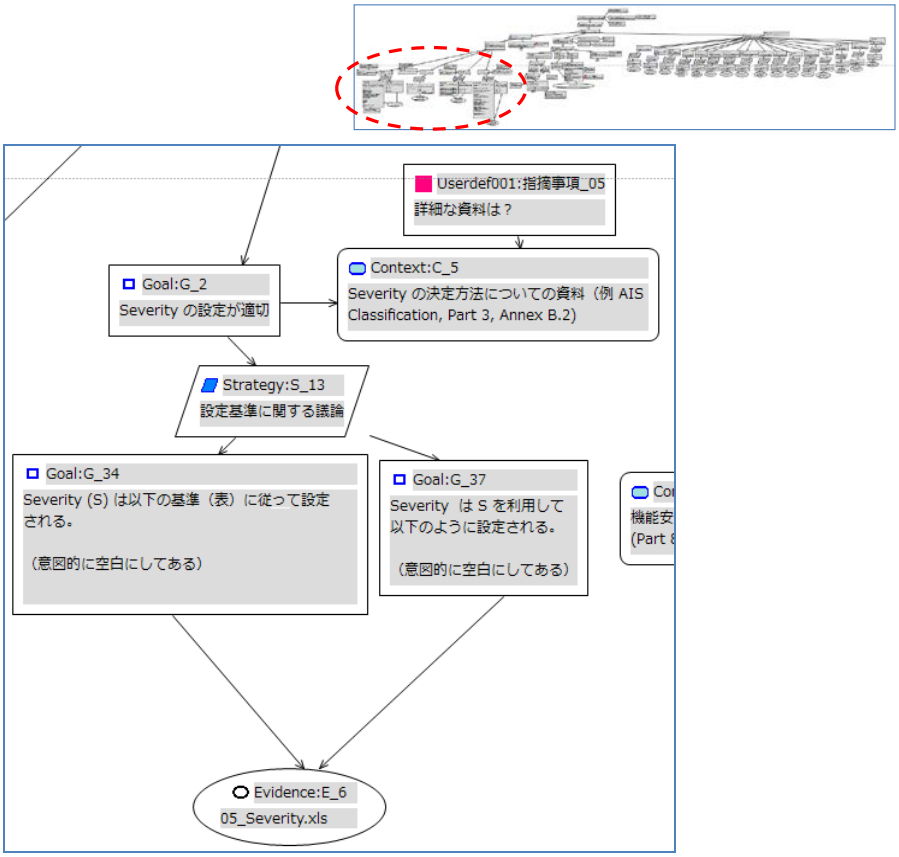


Fig5-4 ISO26262 Part3 要素 B 下部構造- Severity（例示）

要素 B の下部構造のうち、Probability（G_3）についての例示記載を Fig5-5 に示す。

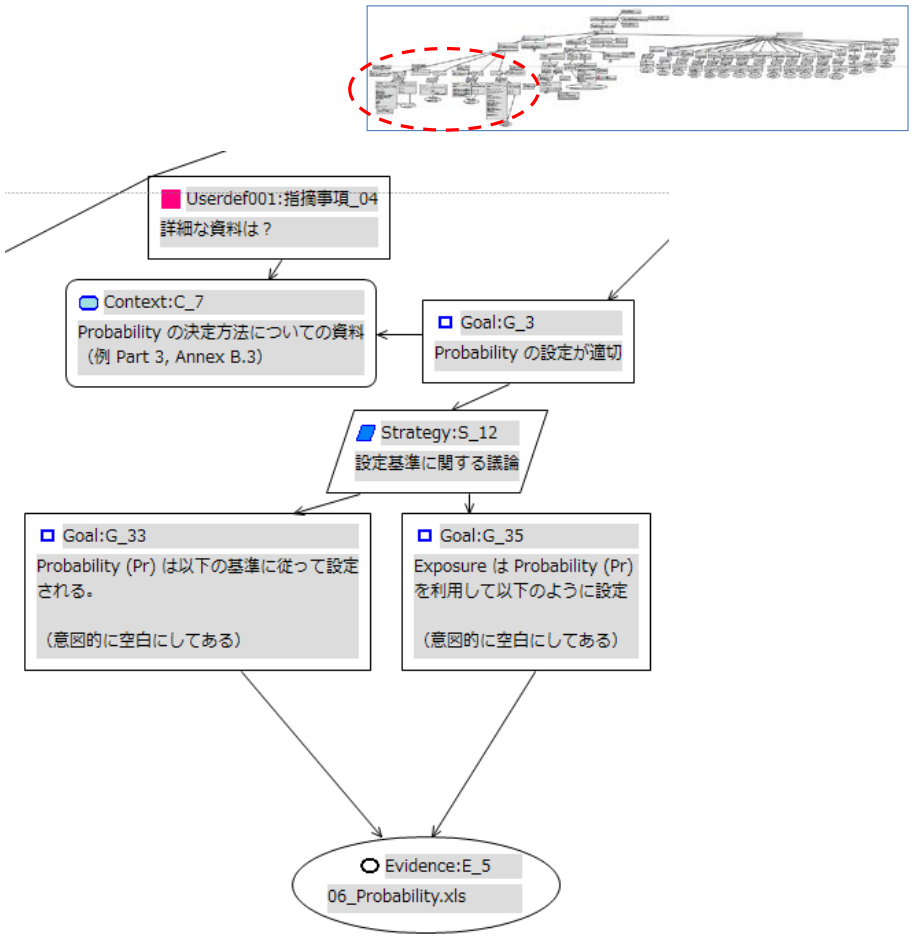


Fig5-5 ISO26262 Part3 要素 B 下部構造- Probability（例示）

要素 B の下部構造のうち、Undetectability (G_4) についての例示記載を Fig5-6 に示す。

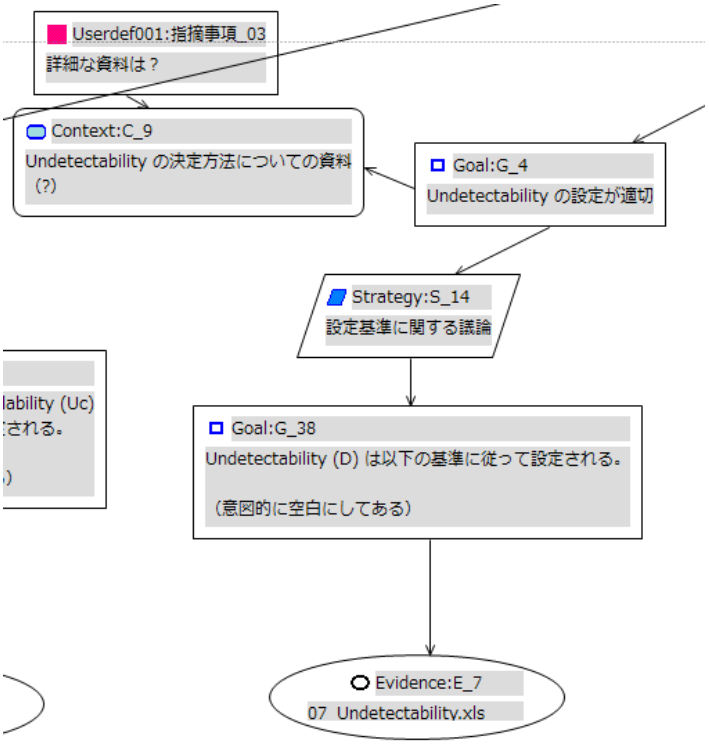


Fig5-6 ISO26262 Part3 要素 B 下部構造- Undetectability（例示）

要素 B の下部構造のうち、Uncontrollability（G_6）についての例示記載を Fig5-7 に示す。

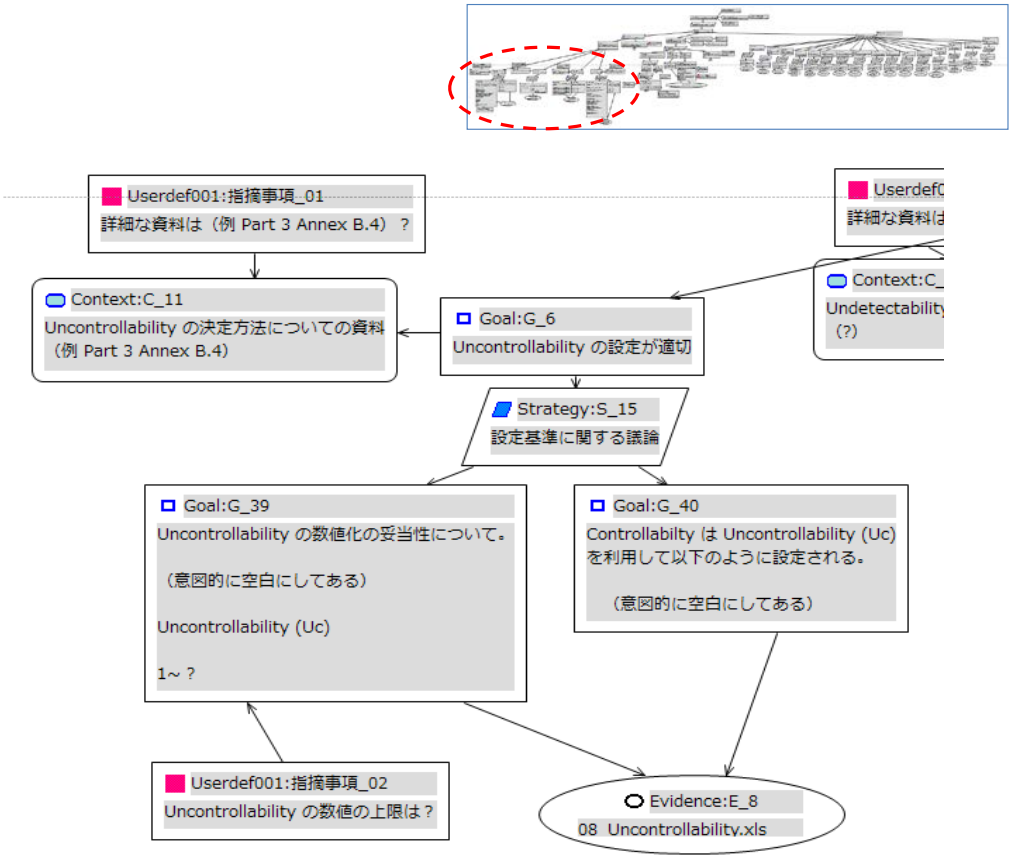


Fig5-7 ISO26262 Part3 要素 B 下部構造- Uncontrollability（例示）

5.1.1.4 機能安全概念（要素 C）

「機能安全概念（Functional safety concept）が規格に準じて定義されている。」（G_41）を要素 C のトップゴールとして、機能安全概念を全般的に議論する構造とした。要素 C の上部構造の例示を Fig5-8 に示す。

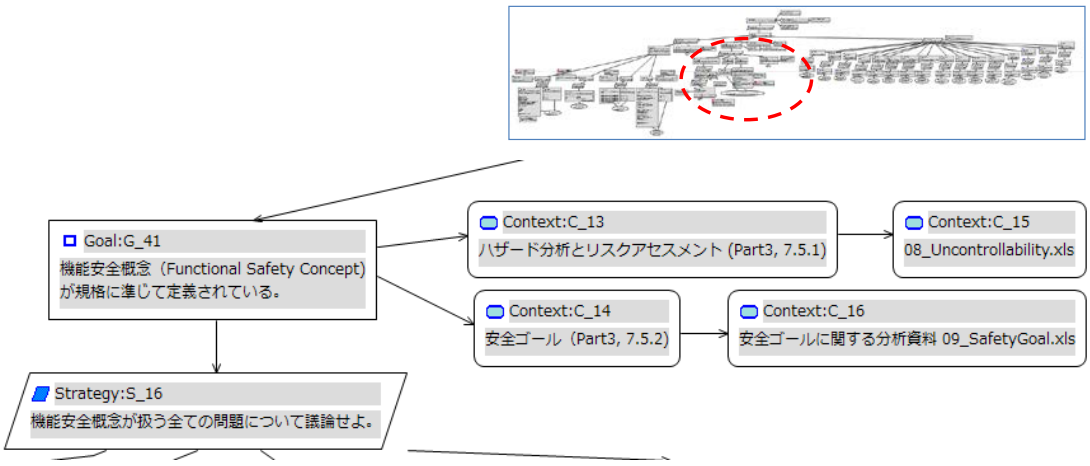


Fig5-8 ISO26262 Part3 要素 C 上部構造（例示）

要素 C の下部構造は、G_41 から分岐した以下の部分ゴールから構成される。

- 機能安全要件（Functional Safety Requirements）は規格に従って仕様記述されている（G_42）
- 機能安全要件の導出は適切に行われている（G_47）
- 機能安全要件の割り当ては適切に実施されている（G_48）
- 妥当性確認の基準（Validation Criteria）は機能安全要件に従って仕様記述されている（G_49）

要素 C の下部構造の例示を Fig5-9 に示す。

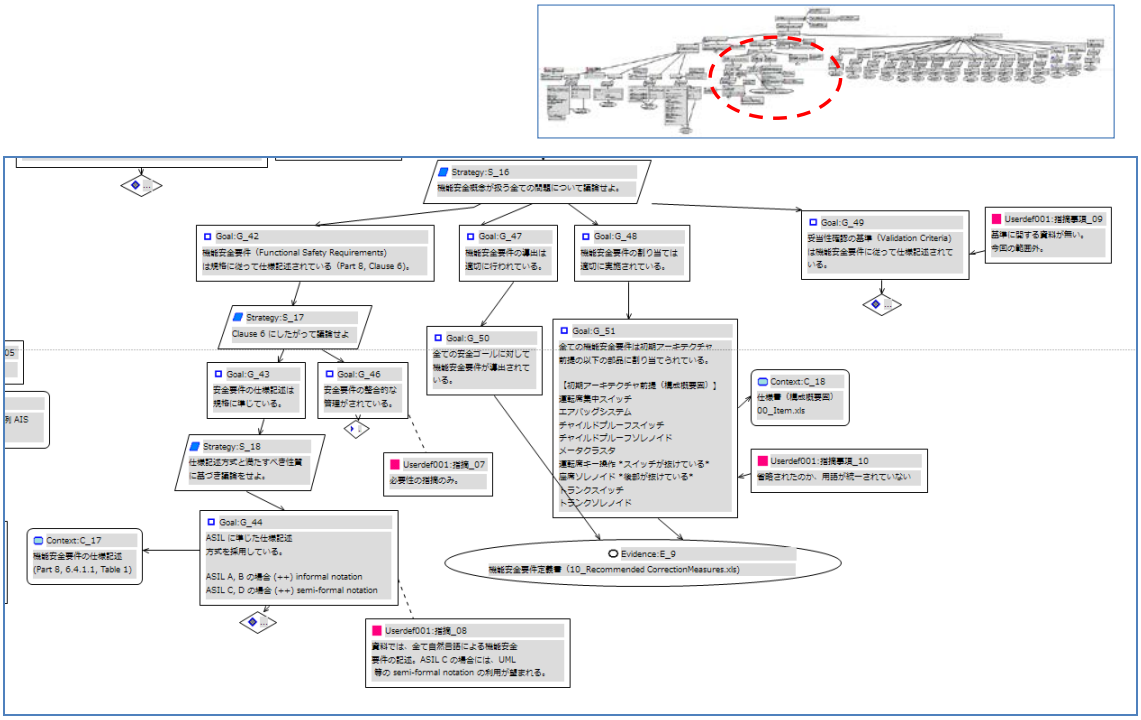


Fig5-9 ISO26262 Part3 要素 C 下部構造（例示）

部分ゴール（G_42）に関しては、さらに仕様記述方法に関する部分ゴール（G_43）と管理方法に関する部分ゴール（G_46）に分かれる。また、部分ゴール（G_47）については、機能安全要件の導出、部分ゴール（G_48）のアーキテクチャに対する機能安全要件の割り当ての適切性について議論展開を行っている。

5.1.1.5 セーフティゴール（要素 D）

要素 D はセーフティゴールについての議論を展開するためのものである。FMEA/FTA により定義されたセーフティゴールは 16 種類あるので、それぞれのハザード分析とリスクアセスメントの結果について議論した。要素 D の全体構造イメージを Fig5-10 に示す。

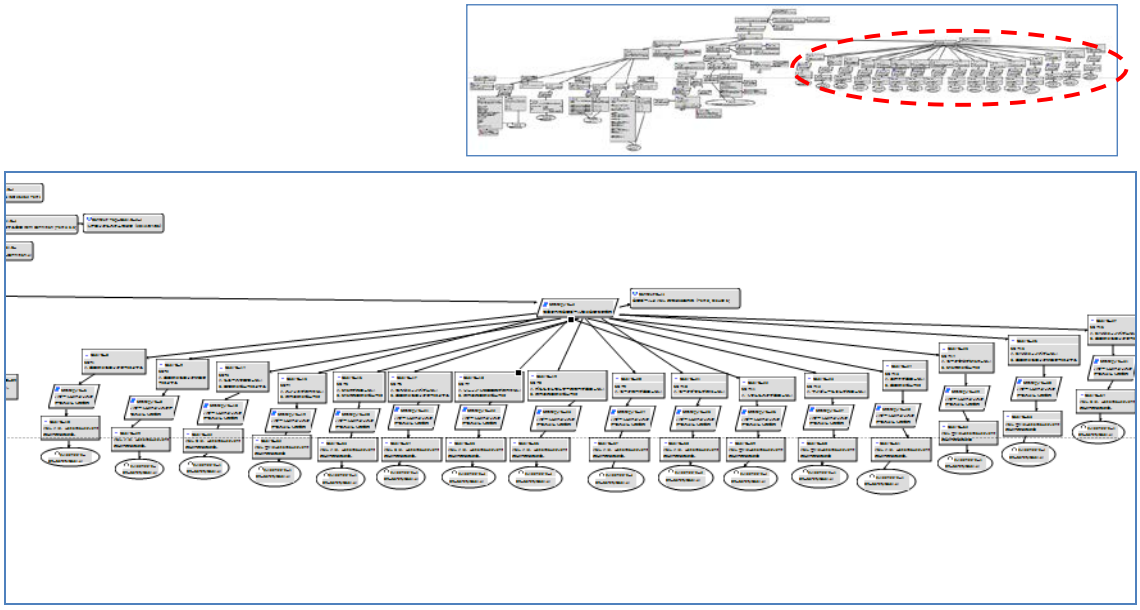


Fig5-10 ISO26262 Part3 要素 D 全体構造イメージ

16 種類のセーフティゴールについて議論を展開し、ASIL 割り当ての妥当性に関する根拠資料を示している。要素 D の部分構造の例示を Fig5-11 に示す。

Fig5-11 ISO26262 Part3 要素 D 部分構造（例示）

5.1.2 ISO26262 Part4 Clause6 における GSN 図

5.1.2.1 全体構造イメージ

GSN の全体構造のイメージを Fig5-12 に示す。本 GSN 図は、対象システムである自動車用オートドアロックシステムの安全性を保証する議論が ISO26262 Part4 Clause6 に従って実施されたかどうかを示すものである。

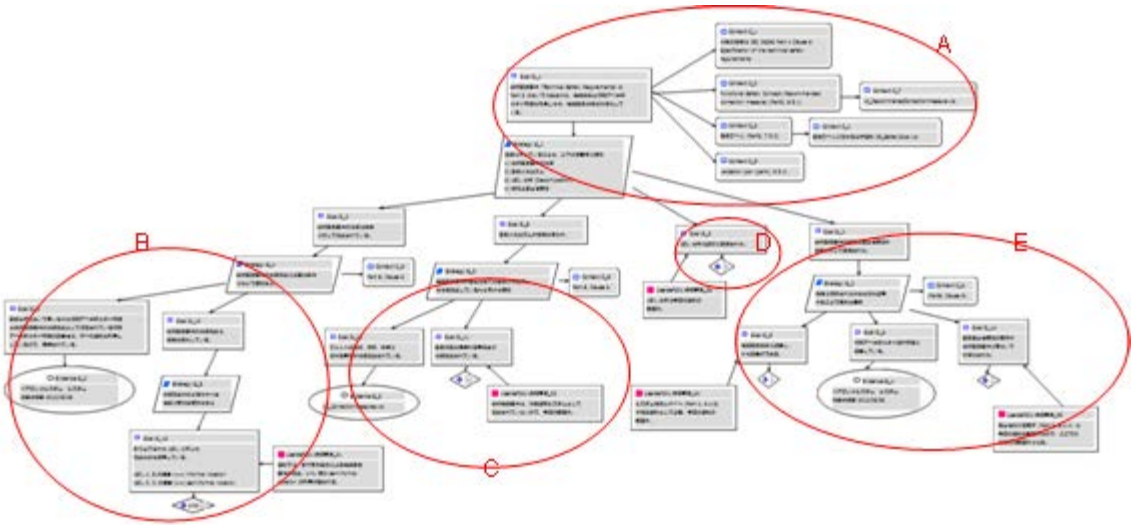


Fig5-12 ISO26262 Part4 Clause6 GSN 図　全体構造イメージ

Fig5-12 は、以下の部分構造から構成される。

要素 A：上部構造

議論の方針を決めるトップ構造

要素 B：技術安全要件（Technical safety requirements）

技術安全要件を満たしているかどうかにおける議論を示す部分構造

要素 C：安全メカニズム（Safety Mechanism）

安全メカニズムの要件を満たしているかどうかの議論を示す部分構造

要素 D：ASIL 分解

ASIL の分解が適切に実施されているかどうかの議論を示す部分構造

要素 E：V&V（検証と妥当性確認）

検証と妥当性確認が適切に実施されているかどうかの議論を示す部分構造

本実験では ASIL 分解は実施しないが、複雑な機能のシステムでは ASIL 分解を実施することによって、開発負荷を軽減できることが想定されるために、参考として記載している。

5.1.2.2 上部構造（要素 A）

要素 A の上部構造を Fig5-13 に示す。

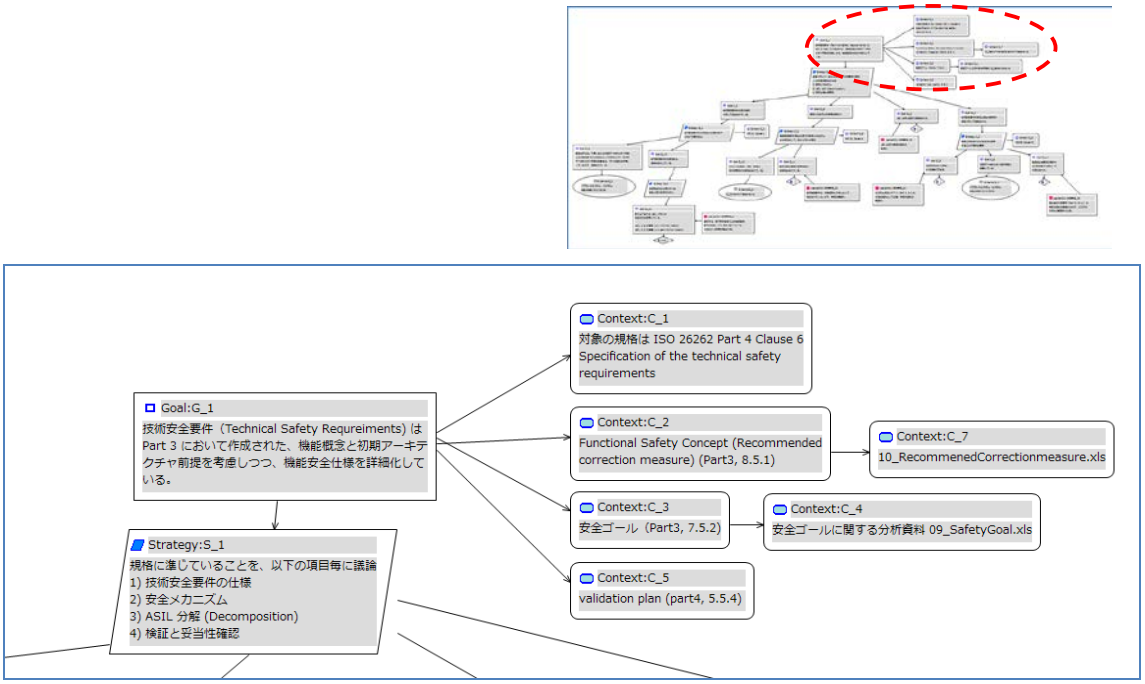


Fig5-13 ISO26262 Part4 Clause6 要素 A 上部構造（例示）

トップゴール（G_1）として、本システムの安全性を保証するために、ISO26262 Part4 Clause6 に従って適切な手法を適用することを設定した。

トップゴールを支援するコンテクストとして、以下の 3 種類を設定した。

- 規格で対象としたセクション（C_1）
- ISO26262 の「4.6　技術安全要求仕様」で要求される入力情報（C_2、C_3、C_5）
- ISO26262 の「4.6　技術安全要求仕様」で要求される入力情報の要件を満たした開発成果物（C_4、C_7）

トップゴールを展開するための戦略として、ISO26262 Part4 Clause6 各セクションの要求事項毎に部分ゴールを設定し、議論することとした。

5.1.2.3 技術安全要件（要素 B）

要素 B の議論構造の例示を Fig5-14 に示す。

技術安全要件を策定する際の制約条件として、ISO26262 の「8.6 仕様と安全要求の管理」が要求されるため、要素 B の議論を支援するコンテクストとして設定した。

また、要素 B のトップゴール（G_2）は、前提条件との整合性（G_9）と仕様の記述方式（G_13）の部分ゴールに分解して議論した。

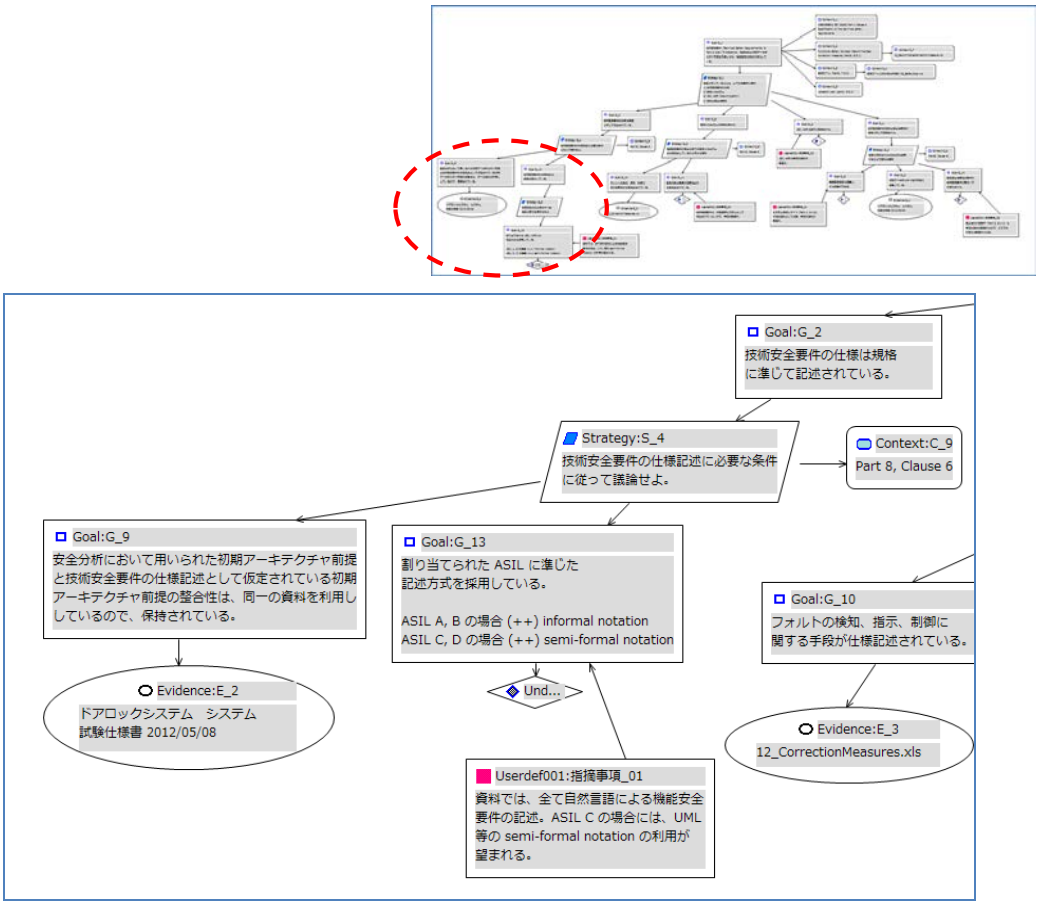


Fig5-14 ISO26262 Part4 Clause6 要素 B の議論構造（例示）

5.1.2.4 安全メカニズム（要素 C）

要素 C の議論構造の例示を Fig5-15 に示す。

安全メカニズムを検討する際の制約条件として、ISO26262 の「8.6 仕様と安全要求の管理」が要求されるため、要素 C の議論を支援するコンテクストとして設定した。

また、要素 C はフォルトの取り扱いに関する手段（G_10）と安全状態の保持に関する手続き（G_11）の部分ゴールに分解して議論した。

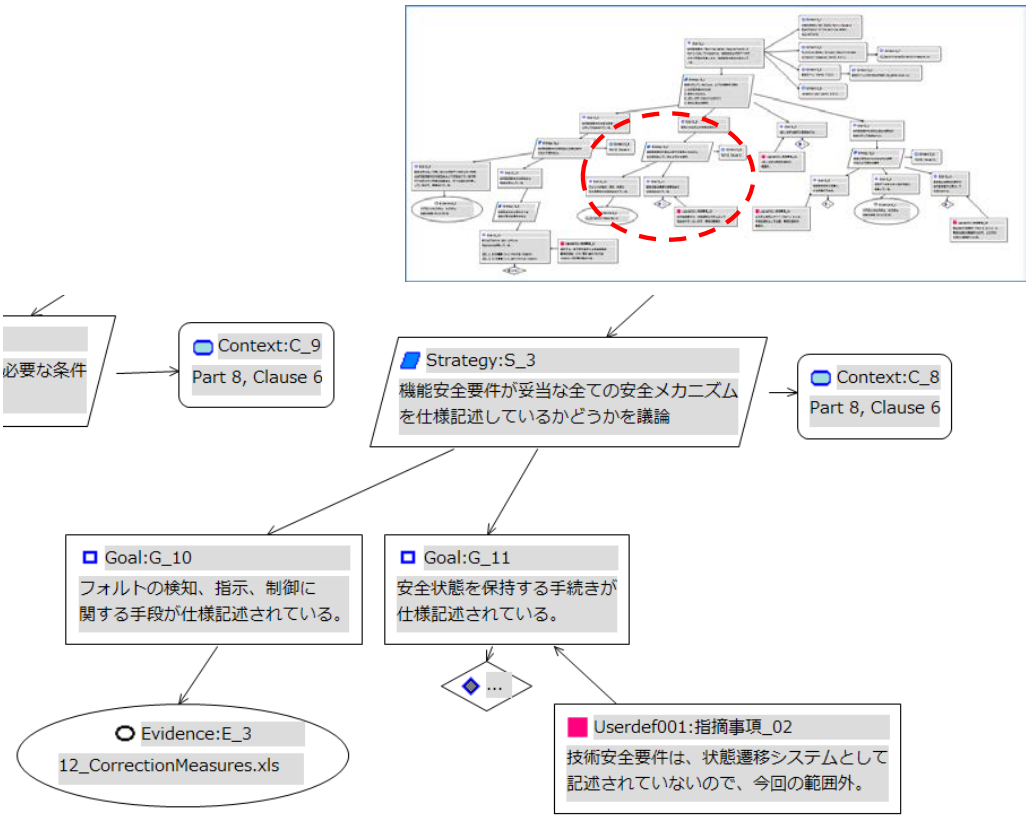


Fig5-15 ISO26262 Part4 Clause6 要素 C 議論構造(例示)

5.1.2.5 ASIL 分解 (要素 D)

本実験では ASIL 分解は実施していないが、複雑な機能のシステムでは、ASIL 分解が必要になるものと想定されるために、要素 D の議論構造の例示を参考として Fig5-16 に示す。

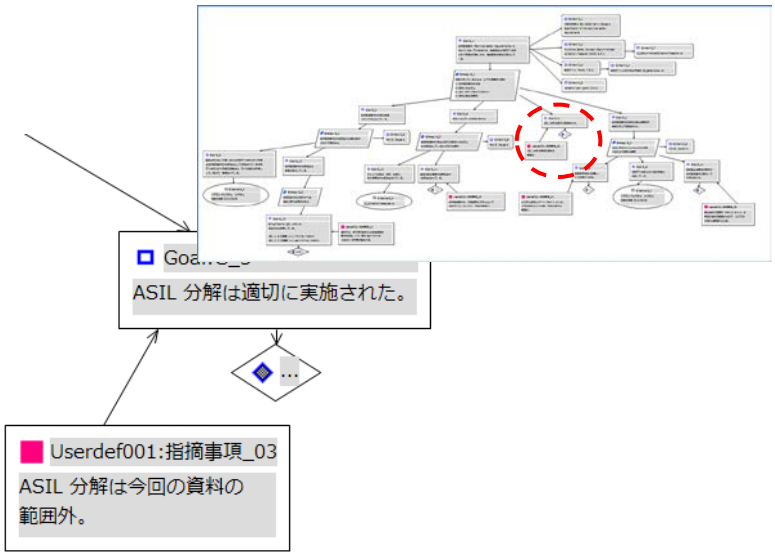


Fig5-16 ISO26262 Part4 Clause6 要素 D 議論構造(例示)

5.1.2.6 V&V（要素 E）

要素 E の議論構造の例示を Fig5-17 に示す。

Verification and Validation（検証と妥当性確認）については、ISO26262 の「8.9 検証」に従って実施することが必要であるため、コンテクストとして設定した。要素 E は以下の 3 つの部分ゴールに分解し、議論を行った。

・機能安全概念に適合し、かつ整合的である（G_5）
・初期アーキテクチャ設計前提に適合している（G_6）
・安全妥当性確認の基準が技術安全要件に基づいて詳細化された（G_14）

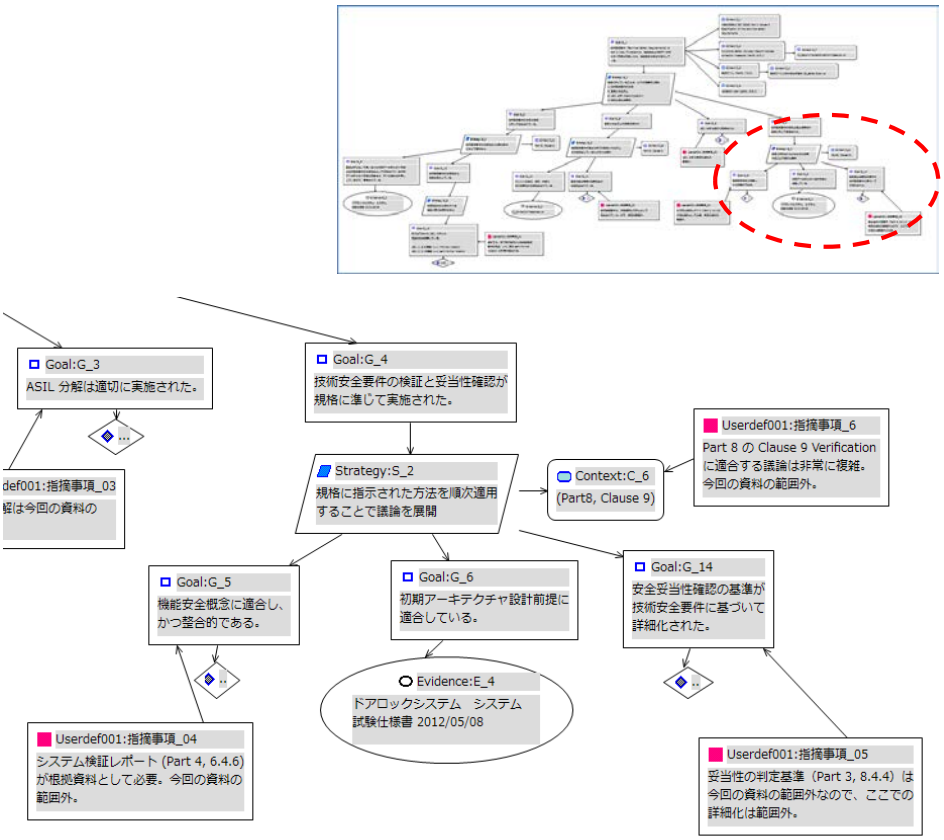


Fig5-17 Part4 Clause6 要素 E 議論構造（例示）

5.2 ISO26262 と GSN により補完された部分との対比

本実験で作成した GSN 図により、ISO26262 Part3 及び Part4 の準拠要件との適合可否を調査した結果は Fig5-18 の通りである。

No.	該当Part	ISO26262要件	適合可否
1	Part.3, 5	アイテム定義	○
2	Part.3, 7	状況分析	○
3	Part.3, 7	ハザード分析	△
4	Part.3, 7	ハザード分析の検証	○
5	Part.3, 7	リスクアセスメント	△
6	Part.3, 7	リスクアセスメントの検証	○
7	Part.3, 7	ASILの決定	○
8	Part.3, 7	セーフティゴールの設定	○
9	Part.3, 7	セーフティゴールの検証	○
10	Part.3, 8	機能安全要件の導出	○
11	Part.3, 8	機能安全要件の割当	○
12	Part.3, 8	妥当性確認の基準を規定	△
13	Part.3, 8	機能安全要件の検証	○
14	Part.4, 5	安全活動の計画	□
15	Part.4, 5	妥当性確認活動の計画	□
16	Part.4, 5	機能安全アセスメント活動の計画	□
17	Part.4, 5	製品開発ライフサイクルのテイラーリング	□
18	Part.4, 6	技術安全要件の規定	対象外
19	Part.4, 6	安全機構の要件	△
20	Part.4, 6	ASIL分解	○
21	Part.4, 6	潜在的障害の回避措置の規定	○
22	Part.4, 6	生産・運用・保守・廃棄に関する技術安全要件の規定	□
23	Part.4, 6	技術安全要件の検証	△
24	Part.4, 6	妥当性確認の基準を追加	△
25	Part.4, 7	システム設計仕様の規定	□
26	Part.4, 7	システム構造設計上の制約	□
27	Part.4, 7	体系的な障害回避措置	□
28	Part.4, 7	運用時のランダムH/W障害の制御措置	□
29	Part.4, 7	ハードウェア・ソフトウェアへの割当	□
30	Part.4, 7	ハードウェア・ソフトウェア・インターフェース仕様	□
31	Part.4, 7	生産・運用・保守・廃棄に関する要件	□
32	Part.4, 7	システム設計の検証	□

Fig5-18 GSN 図により対応した ISO26262 要求項目一覧

○：ISO26262 要件の対応に追加作業が不要（GSN による指摘が無い、または確認して問題がない）

△：ISO26262 要件の対応に不足があるが、既存方法への変更・追加で対応可能なもの

×：ISO26262 要件の対応に不足があり、対応に新規の作業が必要なもの

□：GSN 図を作成しなくとも、ISO26262 要件に対応していることが資料から確認できるもの

Fig5-19 に GSN を利用したリーバストレースによって、ISO26262 に対応することが確認できた項目数、新たに追加する資料が必要など新規対応が必要であることが確認できた項目数、及び既存資料により ISO26262 への対応が確認できた項目数を示す。本システムでは、GSN 図作成のみで、25 項目 80.6%の ISO26262 の要求項目について対応可能であることが確認できた。残り 6 項目 19.4%については、新たに対応が必要となるがそれについては、「5.3 GSN による追加説明に要した工数」にてその工数を見積もった。

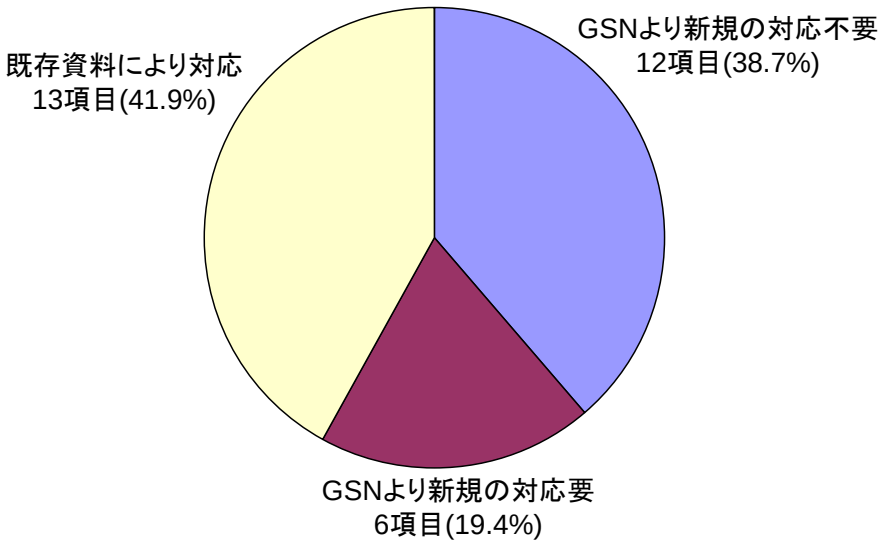


Fig5-19 リバーストレースにより対応した ISO26262 要求項目の割合

5.3　GSN による追加説明に要した工数

既存の設計関連資料のみで、GSN 展開を実施した場合の実測工数について、「4.6.2 リバーストレースに要した作業工数評価」にて定義したタスクごとの実測工数及び割合を Fig5-20 に示す。

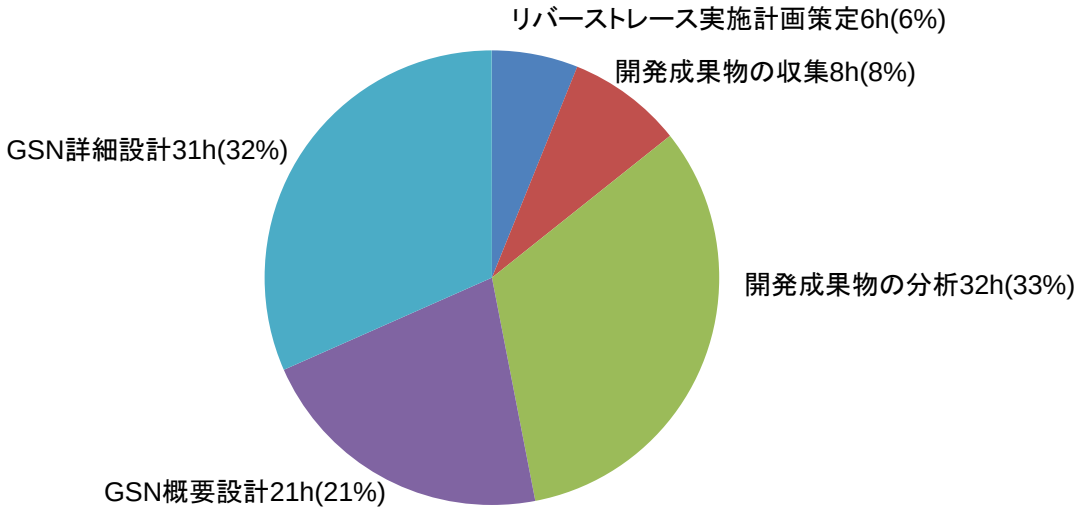


Fig5-20　GSN 図作成に要した工数（実測）

GSN 図作成（ISO26262 の要求事項 12 項目に対応）に要した工数は全体で、98 人時間となった。また、そのうち 47%が GSN 図作成のための準備（「リバーストレース実施計画策定」、「開発成果物の収集」、「開発成果物の分析」）に要する工数となっている。

6. 実験結果の分析・評価

6.1 ISO26262 の要求事項への対応可否評価

本実験で GSN 図を作成したことにより ISO26262 Part3（3.5、3.7、3.8）、及び Part4（4.5、4.6、4.7）の要求事項への対応可否結果は前掲 Fig5-18 の通りで、これにより分析・評価を実施した。（Fig6-1）

Fig6-1 の「C.資料より適合確認したもの」は ISO26262 の要求事項が設計仕様書（RFQ）の記載とほぼ同じ内容になっており、資料の内容を確認することで適合しているものと判断した。

	アイテム数
A.ISO26262要求事項アイテム数	31個
B.既存資料のGSN展開により適合確認したもの	12個
C.資料より適合確認したもの	13個
D.新たに資料作成が必要なもの	6個

Fig6-1 ISO26262 要求事項対応可否アイテム数

既存資料を基にした GSN 展開のみで ISO26262 要求事項へ対応できると想定されるものは、Fig6-1 の B と C のアイテム数の和となり、GSN 展開のみにより対応可能な ISO26262 要求事項への適合項目数及びカバレッジは、80.6%となった。（Fig6-2 参照）

既存資料のGSN展開のみにより対応可能なISO26262要求事項	適合項目数	25個
	適合項目カバレッジ	80.6%

Fig6-2 ISO26262 要求事項適合可否

既存資料を基にした GSN 展開のみでは、カバレッジ 80.6%であるが、Fig6-1「D.新たに資料作成が必要なもの」の 6 項目について、適合事項への対応を保証する資料を作成すれば、カバレッジを 100%とすることができる。「6.2 リバーストレースに要した工数評価」では、この 6 項目への適合を保証するための資料作成に要する工数も含めて試算することとする。

6.2　リバーストレースに要した工数評価

リバーストレースに要した工数は、既存資料の GSN 展開に要した工数と、新たに必要と判明した資料の作成及びその GSN 展開工数に分けて分析・評価する。

6.2.1 既存資料の GSN 展開に要した工数評価

既存の開発関連資料やヒアリングから、GSN 展開して ISO26262 要求事項への適合する際に要する工数は、以下の通りである。

適合作業の作業工数	98時間

参考：上記作業に使用した開発成果物のボリューム：

設計仕様書（RFQ）：Microsoft Word A4 30 ページ程度

FMEA/FTA：Micrsoft Excel A4 1000 ページ程度

6.2.2 説明不足を補完するための資料作成工数の試算

Fig5-18 の通り適合可否が△となり説明不足と判断された各項目及び ISO26262 Part8 に関連する説明不足部分を補完するための資料を作成するに必要なアクティビティを抽出し、工数を試算した。

a. ASIL レベル決定に関連する詳細な資料作成工数（リスクアセスメント(Fig5-18 No.5)を保証）

ASIL を決定するための 3 つの基準である Sevirity / Exposure / Controllability について、社内独自に規定している安全基準と齟齬がないことを保証する根拠が不足しているため、補完する資料作成に要する工数を試算した。

	人	時間	日数	合計
アプローチ検討	1	2	1	2
根拠資料収集	1	8	2	16
根拠調査・分析	1	8	2	16
根拠資料作成	1	1	1	1
レビュー	5	8	1	40
根拠資料修正	1	2	1	2
合計				77

Fig6-3 ASIL レベル決定関連資料作成工数（試算）

b. リスクアセスメントを実施したチーム担当者のスキル説明資料作成工数（ハザード分析(Fig5-18 No.3)及びリスクアセスメント(Fig5-18 No.5)を保証）

ISO26262 Part2 Clause5 にて、適切なスキルを有した担当者のアサインメントが規定さ

れており、アセスメント実行者（1 人）のスキル説明に関する資料（職務経歴書などを想定）作成に要する作業工数を以下のとおり試算した。

	人	時間	日数	合計
資料作成	1	2	1	2

Fig6-4 リスクアセスメント実施者スキルの説明資料作成工数（試算）

c. 機能安全要件検討のプロセス全体における ISO26262 管理方法への適合性説明資料作成工数（ISO26262 Part8 に対応）

全般的な安全要件の議論において ISO26262 Part8 Clause6 へ適合していることを説明する資料作成に要する工数を以下のとおり試算した。

	人	時間	日数	合計
作業項目の過不足確認	1	8	3	24
適合を説明する資料作成	1	4	1	4
レビュー	5	8	1	40
合計				68

Fig6-5 ISO26262 Part8 Clause6 への適合を説明する資料作成工数（試算）

d. 安全メカニズム議論の ISO26262 適合性を補完する説明工数（安全機構の要件(Fig5-18 No.19)を保証）

不具合発生時に、フェールセーフ機能により安全状態（Safe state）へ移行すること、及びフェールセーフ後に安全状態を維持することが ISO26262 Part4 Clause6 に規定されている。GSN 図作成の過程において、今回使用した仕様書に安全状態の維持に関する記述がないことが判明した。仕様書に当該記述を加える場合の工数を下記のとおり試算した。

	人	時間	日数	合計
仕様書理解	1	8	5	40
仕様書修正	1	8	1	8
レビュー	5	8	1	40
合計				88

Fig6-6 安全メカニズムに関する適合性を説明する資料作成工数

e. システム検証レポートの作成（妥当確認の基準を規定(Fig5-18 No.12)、技術安全要件の検証(Fig5-18 No.23)、妥当性確認の基準を追加(Fig5-18 No.24)を保証）

本実験では、Verification and Validation（検証と妥当性確認）を対象としていないため、説明不足項目として挙げられている。実際に Verification and Validation を実施した場合の工数を以下のとおり試算した。（Semi-formal notaiton ではない場合を前提として試算）

	人	時間	日数	合計
設計仕様書/システム仕様書理解	1	8	5	40
テスト仕様書修正	2	8	2	32
レビュー	5	8	1	40
検証実行	1	8	1	8
検証レビュー	5	4	1	20
合計				140

Fig6-7 システム検証レポートの作成に要する工数(試算)

6.2.3 新たに作成した資料の GSN 展開に要する工数試算

GSN 図作成過程において、既存の設計関連資料では説明不足となることが判明した ISO26262 の要求事項に関連して、説明不足を補完する資料を作成して GSN 展開した場合の工数を試算し 55 時間となった。(Fig6-8 参照) ここでは、GSN 展開に要した工数のみを試算している。(説明不足を補完する資料を新たに作成する工数は、「5.3.2 説明不足を補完するための資料作成工数の試算」を参照)

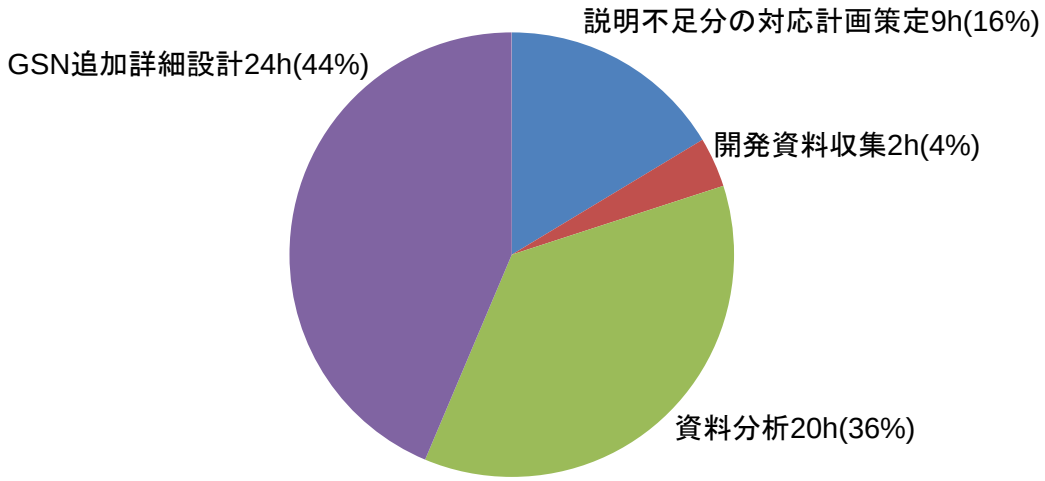


Fig6-8 新たな説明不足補完資料の GSN 展開に要する工数(試算)

また、既存資料の GSN 展開に要した工数を合算すると、GSN 図作成に要する工数の合計は、153 人時間と試算された。

6.2.4 ISO26262 要求事項対応に要する全体作業工数の試算

全作業工数の試算結果を Fig6-9、Fig6-10、及び Fig6-11 に示す。本実験での実測作業工数が 98 人時間、追加作業工数は、430 人時間と試算され、合計の作業工数は、528 人時間となった。本システムに GSN を適用して、ISO26262 Part3 及び Part4 に準拠した場合には、約 3.3 人月(1 か月 20 日、8 時間/日稼働)の作業工数が必要になると試算した。また、6.2.2 の「d. 安全メカニズム議論の ISO26262 適合性を補完する説明工数」は仕様書記述が不足し

ていたものが GSN 展開により偶然発見されたもので、他の資料作成工数とは異質なものではあるが、通常の開発工程でもあり得ることであることと、GSN 展開による成果の 1 つでもあるため、含めて作業工数とし試算した。なお、図中の「設計者」は本文中の「開発者」に対応する。

	担当属性	作業工数(時間)	割合(%)	合計(時間)	合計(%)
実作業	GSN 作成者	82.5	15.6%	98	18.6%
	設計者	15.5	2.9%		
追加作業(試算)	GSN 作成者	48	9.1%	430	81.4%
	設計者	382	72.3%		
合計	GSN 作成者	130.5	24.7%	528	100.0%
	設計者	397.5	75.3%		

Fig6-9 全作業工数一覧

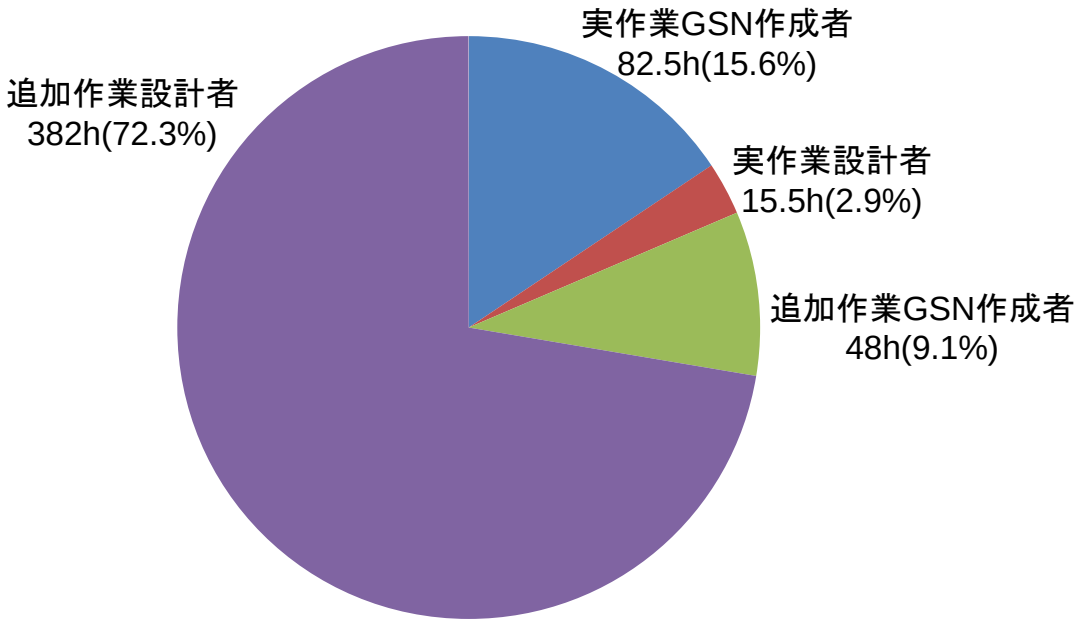


Fig6-10 全作業工数の内訳

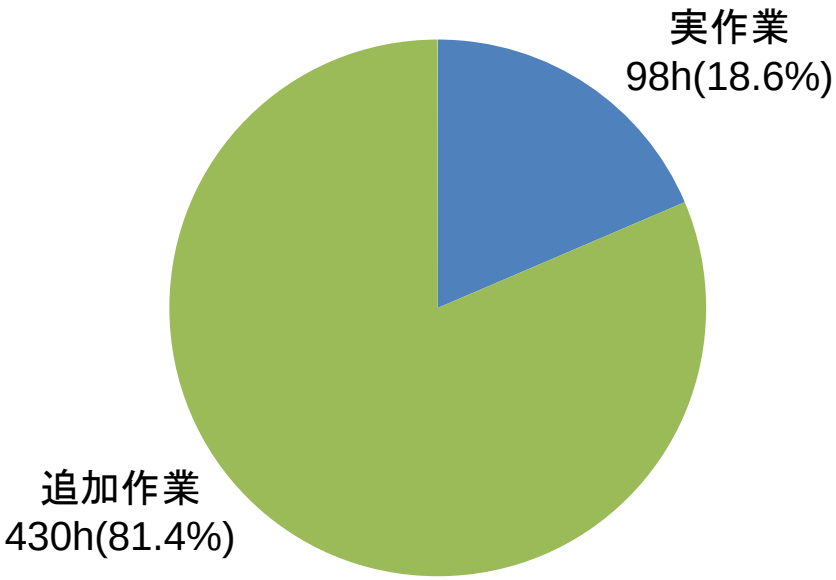


Fig6-11 実作業と試算した追加作業工数

7. 国際規格に準拠させる際に想定される課題と考察

7.1 ISO26262 Part8(Supporting Processes)要求事項対応に関する課題と考察

本実験で対象としたISO26262 Part3及びPart4は、共通要件として、Part8（Supporting Process）の要求事項への対応が必要となる。本実験では設計仕様書、FMEA/FTAのみにより実験を実施したため、Part8の管理プロセス（変更管理、要求管理、構成管理など）の要求事項は対象外とした。しかしながら、日本の開発現場では、このような管理プロセスを組織的に方針を策定して、実施していないところも少なからず存在するものと想定される。または、当然のように意識されて実施されている内容ではあるが、そのプロセスや活動をエビデンスとして書類として残していないところが少なからず存在するものと考える。

このような状況の中で、リーバストレースを実施する場合には、新たな資料を作成する工数が複雑なシステムほど大きく膨らむ可能性があり、コスト面での課題が大きいものと思われる。工数面での検討は、7.4にて実施した。

7.2 ISO26262 Part2(Management of Functional Safety)要求事項対応に関する課題と考察

7.1と同様に、Part2もPart3及びPart4の共通要件である。ISO26262 Part2 Clause5にて､対象とする作業内容と対象システムについて十分な知識を持つことが要求されており、それを保証する資料が必要となる。本実験では7.1と同様の理由で、対象外としているが、この部分も日本の開発現場では、エビデンスとして書類化されていないところは、少なくないものと考えられ、新たな資料作成工数が必要となる。また、Part2の要求事項に対応するためには、現状では暗黙知的な安全設計が行われている場合には、今後「安全文化」やそのエビデンスとなる個々の作業のエビデンスのとり方に留意が必要になると考える。

7.3 技術要件においてSemi-formal notationが要求される場合の課題と考察

本実験では、ASIL Aとして実験を実施したため、ASIL C以上で必須となるSemi-formal notationは対象外とした。仮にSemi-formal notionが必要とされた場合を想定して、追加される工数を参考までに試算した。(Fig7-1) 自然言語で記述された本システムの設計仕様書からモデルベース仕様書を作成したと想定した場合の作成工数を試算した。「6.実験結果の分析・評価」で試算した工数と比較するとレビューの工数が低減しているが、これは自然言語の仕様書の場合、言葉の意味やコンテクストを説明・理解する時間が多いために、工数が大きくなっている。モデルベース仕様書は、Stateflowを理解できる人がレビューすれば、時間を削減できるという利点があるものと考える。

	Part3				Part4				
	人	時間	日数	小計	人	時間	日数	小計	小計
仕様書理解	2	8	2	32	2	8	2	32	64
モデルベース仕様書作成	1	8	2	16	1	8	5	40	56
レビュー	3	4	1	12	3	8	2	48	60
合計				60				120	180

Fig7-1 モデルベース仕様書を新たに作成した場合の工数(試算)

7.4 作業工数増加に関する課題と考察

新たな資料作成に要する工数も含めた、ISO26262 の要求事項に対応するための全体工数について、評価・分析を実施し作業工数削減の可能性について考察した。

7.4.1 評価・分析のための作業項目の一般化

工数を試算した各作業項目について、Fig7-2 の通り標準作業項目を設定することにより、作業項目を一般化して分析することとする。

標準化作業項目	説明
1.計画	対象範囲の選定、アプローチの検討、スケジューリング、必要タスクの抽出など
2.情報収集	必要な資料(議事録などを含む)の探索、印刷、とりまとめ、送付など
3.調査・分析	資料の読み込み、疑問点・問題点抽出、構造分析、論理分析など
4.会議	ヒアリング、レビュー、確認のための打ち合わせなど
5.成果物作成	GSN図の作成、必要資料の作成など
6.その他	標準作業項目1～5に該当しない作業

Fig7-2 標準化作業項目一覧

7.4.2 資料作成工数の標準化作業項目による分析・評価

資料作成工数の中で、最も工数を要すると想定される項目が「会議」である。具体的には、作成する資料の中身の精査及び合意形成に大きな工数が掛かる可能性が高い。「会議」での指摘事項が少なければ、「会議」時間が短縮されるとともに、資料の修正工数も低減されるため、「会議」をいかに効率的に運営するかが工数削減のポイントになると考える。

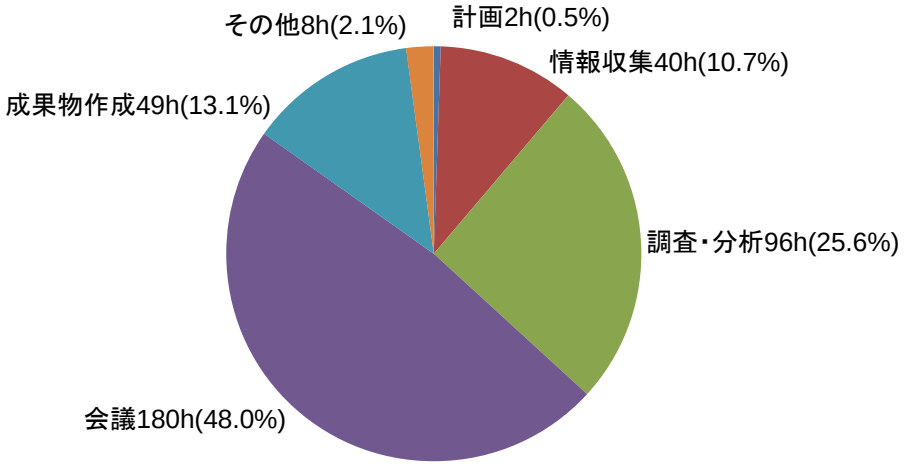


Fig7-3 新たな資料作成に要する標準化項目による工数試算

7.4.3 GSN 展開工数の標準化作業項目による分析・評価

GSN 展開に要する工数では、「会議」と「調査・分析」が大きな工数を占め、合計して 56.1%の工数となっている。本実験では、自動車に関する知識はあまりないものの、GSN 図作成の知見がかなり高い人材により、GSN 展開が実施されている。したがって、実際の開発現場で GSN 展開により、ISO26262 準拠を保証するエビデンスを作成する場合には、「成果物作成」の工数がより膨らむ可能性が高い。一方で、本システムの仕様理解に時間が掛かっているため、「調査・分析」の工数は減少する可能性が高い。

また、GSN 作成者は対象とするシステムの具体的な仕様についての知見が少ない場合が多いと想定されるため、対象システムのスコープ、アプローチ、スケジューリングなどの企画・計画・管理方法を当初にある程度精度高く決定することで、調査分析や会議の進め方など円滑・効率的に進めることができると考える。

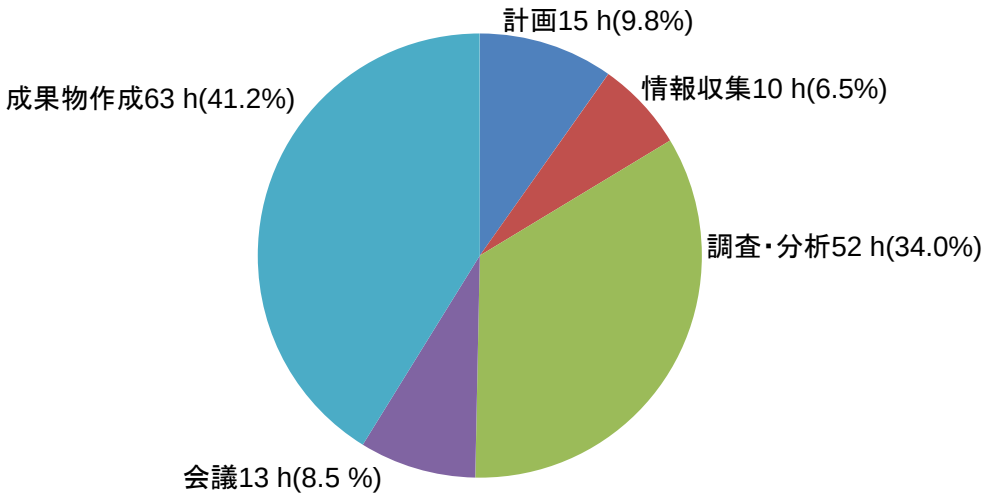


Fig7-4 GSN 展開に要する標準化項目による工数試算

7.4.4 全体作業工数の標準化作業項目による分析・評価

資料作成工数と GSN 展開に要する工数の合算は、Fig7-5 の通りである。全体としては、528 時間（約 3.3 人・月：月 20 日/8 時間稼働、モデルベース仕様書作成を含まず）となり、比較的構造が簡単な ASIL A を想定した自動車用ドアロックシステムの Part3 及び Part4 対応だけにしては、かなり大きな工数が掛かると見込まれる。全体としては、「会議」の工数が 48%と最も大きく、これは前述の通り自然言語仕様書によりレビューや理解のために、言葉やコンテクストの確認・理解に大きな工数が掛かるためである。解決の方向性としては、自然言語仕様書をモデルベース仕様書に変更すれば、会議の時間を大幅に削減することができる。さらに、GSN 展開工数や「調査・分析」に含まれる自然言語仕様書の理解に要する工数も削減することができるものと考える。（モデルベース仕様書への変更工数は Fig7-1 参照）

単位：時間

標準作業項目	資料作成工数	割合（%）	GSN 展開工数	割合（%）	合計	割合（%）
計画	2	0.5%	15	9.8%	17	3.2%
情報収集	40	10.7%	10	6.5%	50	9.5%
調査・分析	96	25.6%	52	34.0%	148	28.0%
会議	180	48.0%	13	8.5%	193	36.6%
成果物作成	49	13.1%	63	41.20%	112	21.2%
その他	8	2.1%			8	1.5%
合計	375	100.0%	153	100.0%	528	100.0%

Fig7-5 標準化作業項目による全体作業工数（試算）

8. まとめ

本実験では、ソフトウェア品質説明力の強化において、国際規格に適合することのフィージビリティを検討するために、自動車メーカーが既製ソフトウェアにおいて、新たに、自動車の機能安全に関する国際規格である ISO26262 に対応する場合に発生する工数を実験により測定・算出した。

本実験は既製システムを対象としているため、既に存在する開発成果物（設計仕様書（RFQ）や FMEA/FTA）を基に GSN 展開することで、ISO26262 の要求事項への対応可否を確認し、掛かる工数を測定した。また、既存資料のみで約 80%のカバレッジとなったため、100%にするために必要となる作業工数を併せて試算した。

本実験の結果として、既製システムに GSN を活用した、ISO26262 に準拠させるためには合計で 528 時間（3.3 人月）という大きな工数が掛かることが判明し、既製システムを国際規格に適合させる場合には、製造事業者にとっては大きな負担になる可能性があることが分かった。

国際規格への準拠は、ソフトウェア品質説明力強化の主要な方法の 1 つであり、この手法の適用をフィージブルなものとするためには、製造事業者と何らかの支援が可能な公的機関との双方での対応策の検討が必要と考える。

本実験で検討した対応策の方向性（仮説）は次の通りである。

1.国際規格への準拠を検討する事業者における検討方策：

① モデルベース開発仕様書の活用

自然言語仕様書からモデルベース開発仕様書へ変更することにより、リバーストレース作業をより効率的に進められる可能性があると考えられる。

② マネジメントプロセスの確立

ISO26262 では、Part2、Part8 のマネジメント及び管理方法などの確立が全プロセスに要求されている。日本の企業は一般的に比較的マネジメントプロセスが弱いと言われていることもあり、マネジメントプロセスの確立が重要と考える。

2.公的機関における検討方策：

③ ガイドラインの作成

製造事業者がある程度円滑に国際規格へ対応できるように、既製システムに配慮した対応ガイドラインを作成することが必要と考える。

本実験では、ISO26262 Part3、Part4 のみを対象として実施したが、開発プロセス全サイクルで実施した場合には、対応のための作業工数が、非常に大きくなることが予想される。本実験での成果や仮説を基に、今後実施が予定されている実証実験では、全サイクルを対象

に、製造事業者なども参画した形で、より実態に近い形で実証実験を実施することにより、現実に近い課題や解決策が検討できるものと考える。

参考文献

[1]「ソフトウェアの品質説明力強化のための制度フレームワークに関する提案」(中間報告)（2011 年 9 月 30 日公開）http://sec.ipa.go.jp/reports/20110930.html

[2] ロバート・ボッシュ Gmbh（2003）『ボッシュ自動車ハンドブック　日本語版第２版』山海堂。

[3] Doug Rosenberg・Kendall Scott（2001）『ユースケース入門　ユーザマニュアルからプログラムを作る』株式会社 テクノロジックアート訳, ピアソン・エデュケーション。

[4] ISO 26262, *Road vehicles –Functional safety–*

[5] Edited by Nicolas Navet and Franoise Simonot-Lion, *Automotive embedded system handbook*, CRC Press

添付資料

認証試験のための GSN 図作成　説明資料

目次

1. 本資料について

本資料は、ドアロックシステムのシステム試験仕様書、FMEA/FTA 結果を基に作成された GSN 図の説明資料である。本資料には以下が含まれる。

1) GSN（Goal Structuring Notation）図の解説
2) GSN 図作成工数の見積もり

1.1. GSN 図とは

GSN (Goal Structuring Notation) は英国ヨーク大学の T. Kelly らが考案した、アシュアランスケース・セーフティケースの分析、記述のための図式表現である。セーフティケースは、アシュアランスケースの 1 つのインスタンスであり、それ以外にも Maintainability Case や Dependability Case、Security Case など様々なシステム特性に基づくケース(Case)が作成されている。基本的には、それぞれのシステム特性に対して「システム特性-Case」を作成することで、そのシステム特性の保証を説明することに繋がる。

【参考文献 (1)】

T. Kelly, “Arguing Safety – A Systematic Approach to Managing Safety Cases”, University of York, Department of Computer Science, 1998

1.2. 作成された GSN 図

本案件においては、ISO 26262 において成果物として指定されているセーフティケースの作成を GSN 図を用いて行った。ISO 26262 の範囲は広いので、協議の結果、以下の箇所に絞って実施した。

【セーフティケースの対象範囲】

1) Part 3: Concept phase
2) Part 4: Product development at the system level, Clause 6 Specification of the technical safety requirements

Part 3:Concept phase は、機能安全の保証のための安全分析（ハザード分析とリスクアセスメント)、機能安全概念（安全ゴール、機能安全要件）を作成するフェーズである。

Part 4:Product development at the system level はハードウェア部分の開発（Part 5 Product development at the hardware level）とソフトウェア部分の開発（Part 6 Product development at the software level）の双方をシステムとして結合、テスト、安全性に関する妥当性確認、アセスメントを実施し、製品として出荷するまでを取り扱う部分である。

本プロジェクトにおいては、Clause 6 Specification of the technical safety requirements（技術安全要件の仕様）に対してセーフティケースを作成した。

【参考文献（2)】

ISO 26262- Part 1 ~ Part 9, Road vehicles – Functional safety, 2011

本案件において作成された GSN 図における注釈は、利用したツール D-case editor において提供されている、ユーザが自由に利用できるノード（Userdef001）を利用した。

1.3. 利用されたツール D-case Editor

GSN図はJST/CRESTによるDEOSプロジェクト[1]で開発されたD-case editor（Eclipseプラグイン）を使用した。本エディターは以下からダウンロード可能であり、無償で利用が可能である。

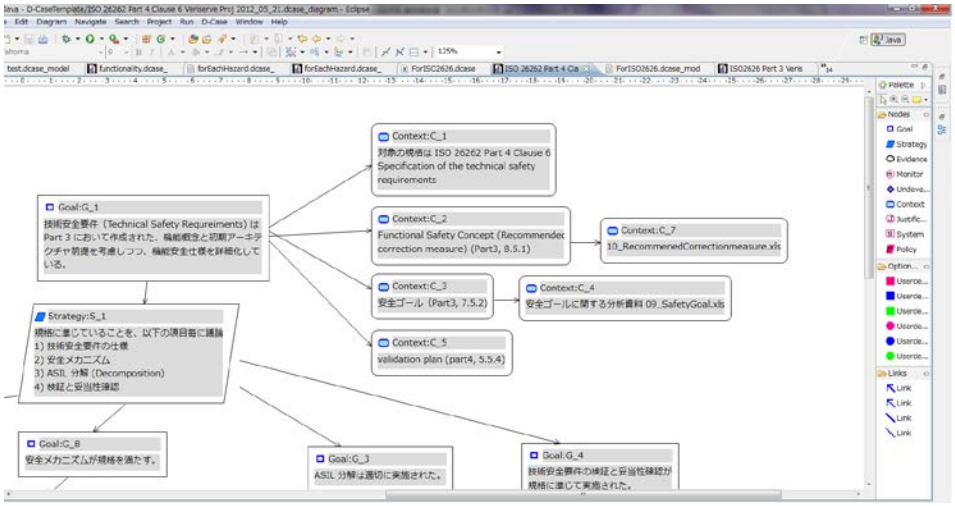


図 1.1. D-case editor のスナップショット

【参考文献（3)】

http://www.il.is.s.u-tokyo.ac.jp/deos/dcase/

[1] 「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」（DEOS（Dependable Embedded Operating Systems）プロジェクト）は、（独）科学技術振興機構（JST）/CREST の研究領域の 1 つとして、2006 年 10 月に開始された。DEOS は OSD（Open Systems Dependability）を実現するための知識・技術を体系だてたもの。CREST は JST の戦略的創造研究推進事業。

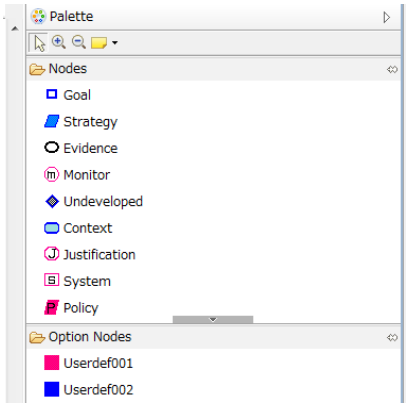


図 1.2. D-case editor で利用可能なノードの種類

本案件においては、通常の GSN で利用されるノードの種類（Goal（ゴール）,Strategy（戦略）,Evidence（根拠資料）,Undeveloped（未発展）,Context（コンテクスト））を利用した。GSN においても提供されている Justification については、今回利用しなかった。Policy, Monitor, System は D-case editor 独自のものであり、今回の目的と合致しなかったので利用をしなかった。System ノードは、GSN におけるモジュールであるが、今回は内容の分析が中心だったので、GSN のアーキテクチャとして利用はしなかった。なお、既に述べたが、図のコメント（指摘事項）としては、Userdef001 を利用した。

1.4. 用語

ISO 26262 における用語（英語）と、本報告書及び GSN 図で利用された用語（日本語）との対応表を以下に示す。ISO 26262 において利用されている用語の日本語訳はまだ統一されていないので、本報告書においてのみ利用されるものと了解されたい。

ISO 26262	本報告書における用語（GSN 図含む）
Safety case	セーフティケース
Preliminary architecture assumptions	初期アーキテクチャ前提
Functional safety concept	機能安全概念
Functional safety requirements	機能安全要件
Safety goals	安全ゴール
Validation criteria	妥当性確認の基準
Technical safety requirements	技術安全要件
Safety mechanism	安全メカニズム

ASIL decomposition	ASIL[2]分解
Validation & Verification	妥当性確認と検証

表 1.1. 用語の日本語訳

2. Part 3 に関するセーフティケース(GSN 図)

本 GSN 図の全体構造は以下に示される。

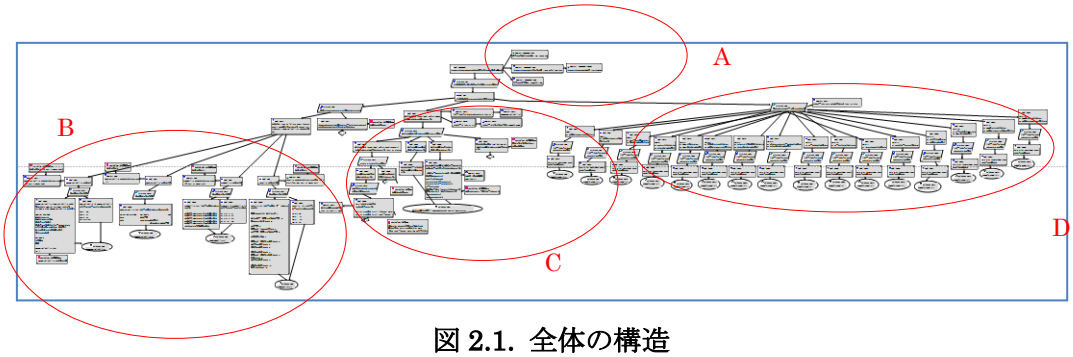


図 2.1. 全体の構造

本 GSN 図は、対象システムである「ドアロックシステム」の安全性を保証する議論が ISO 26262 Part 3 に従って実施されたかどうかを示すものである。

各部分構造について説明をする。

A はトップ構造を示しており、議論の方針を示している。

B は ASIL の決定に関する基準の妥当性に関する議論を示す部分構造である。

C は機能安全概念（Functional safety concept）が規格通りに定義されていることを保証する部分構造である。

D は同定された安全ゴール毎に安全性の議論を行うものである。

以下に各部分構造について説明を行う。

2.1. 上部構造（A）

上部構造は以下の図で示される。

[2] ASIL：Automotive Safety Integrity Level
リスクを許容水準に抑えることを達成するための安全性の要求 A(要求レベル低)~D(要求レベル高)までのレベルがある。

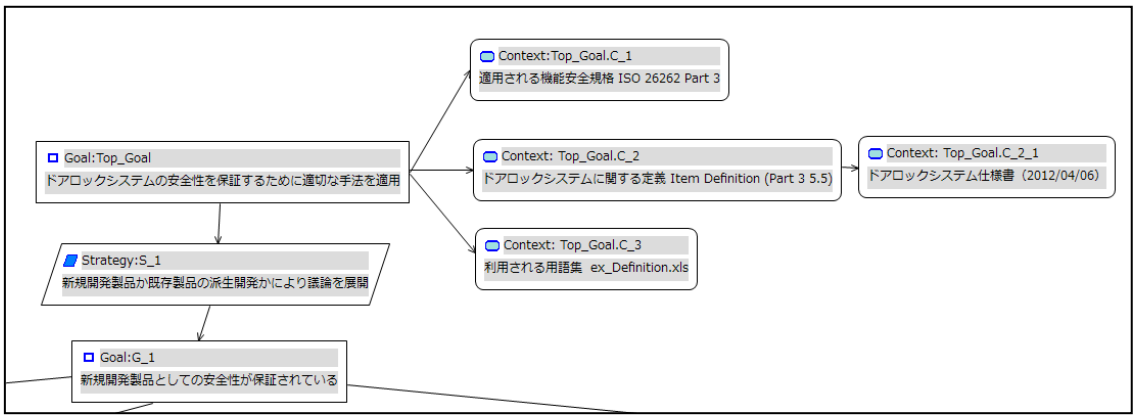


図 2.2. 上部構造（A）

トップゴール（Top_Goal）は対象システム（Item）であるドアロックシステムの安全性を保証するために適切な手法を適用したかどうかを問うものである。本ゴールを支援するためのコンテクストとしては、まず、適用される規格に対する参照（Top_Goal.C_1）がある。次に本ゴールが成立するために参照すべき資料として Item definition と（Top_Goal.C_2）、実際の資料である「ドアロックシステム仕様書（2012/04/06）」が参照されている（Top_Goal.C_2_1）。そして、本議論において利用される用語集を参照している（Top_Goal.C_3）。

次に、トップゴールの展開のための戦略として、Part 3 6. Initiation of the safety lifecycle に従った戦略によりトップゴールを展開する。ただし、本 item は新規開発なので、派生開発の際に必要な impact analysis 等を実施する必要は無く、ゴールとして「新規開発製品としての安全性が保証されている（G_1）」に至る。

2.2. Bの構造

G_1 からの分岐の 1 つが B であり、この部分構造は「ASIL の決定に関する基準の妥当性に関する議論」するためのものである。ここでは、以下の部分ゴールを設定した。

「対象部分 item と failure event (hazardous event)の分類とそれに対する S(severity), E(exposure), C(controllability)の決定が適切に実施された（G_12）」

「リスクアセスメントを実施したチームはリスクアセスメントと対象システムに対する十分な知識を持つ（G_11）」

G_11 に対しては、今回は作成の対象外ということで、ゴール自身は未発展（undeveloped）である。それに対して、G_12 はさらに展開される。

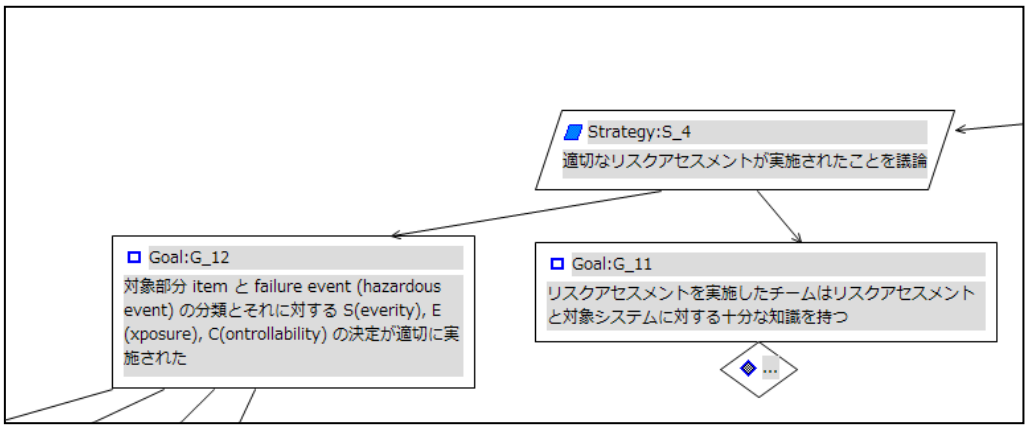


図 2.3. B の上部構造

B の下部構造としては、

「Uncontrollability の設定が適切（G_6）」
「Undetectability の設定が適切（G_4）」
「Probability の設定が適切（G_3）」
「Severity の設定が適切（G_2）」

がサブゴールとして展開されている。提供された資料においては、controllabilityをuncontrollabilityという基準から導出点や、undetectabilityを利用する点など、独自の手法を用いている点からしても、その手法の妥当性を主張する必要があると考え、このような構造を取った。各サブゴールは、参照すべき資料として、05_Severity.xls、06_Probability.xls、07_Undetectability.xls、08_Uncontrollability.xlsを参照している。

Uncontrollability に関する議論の構造は以下に示される。

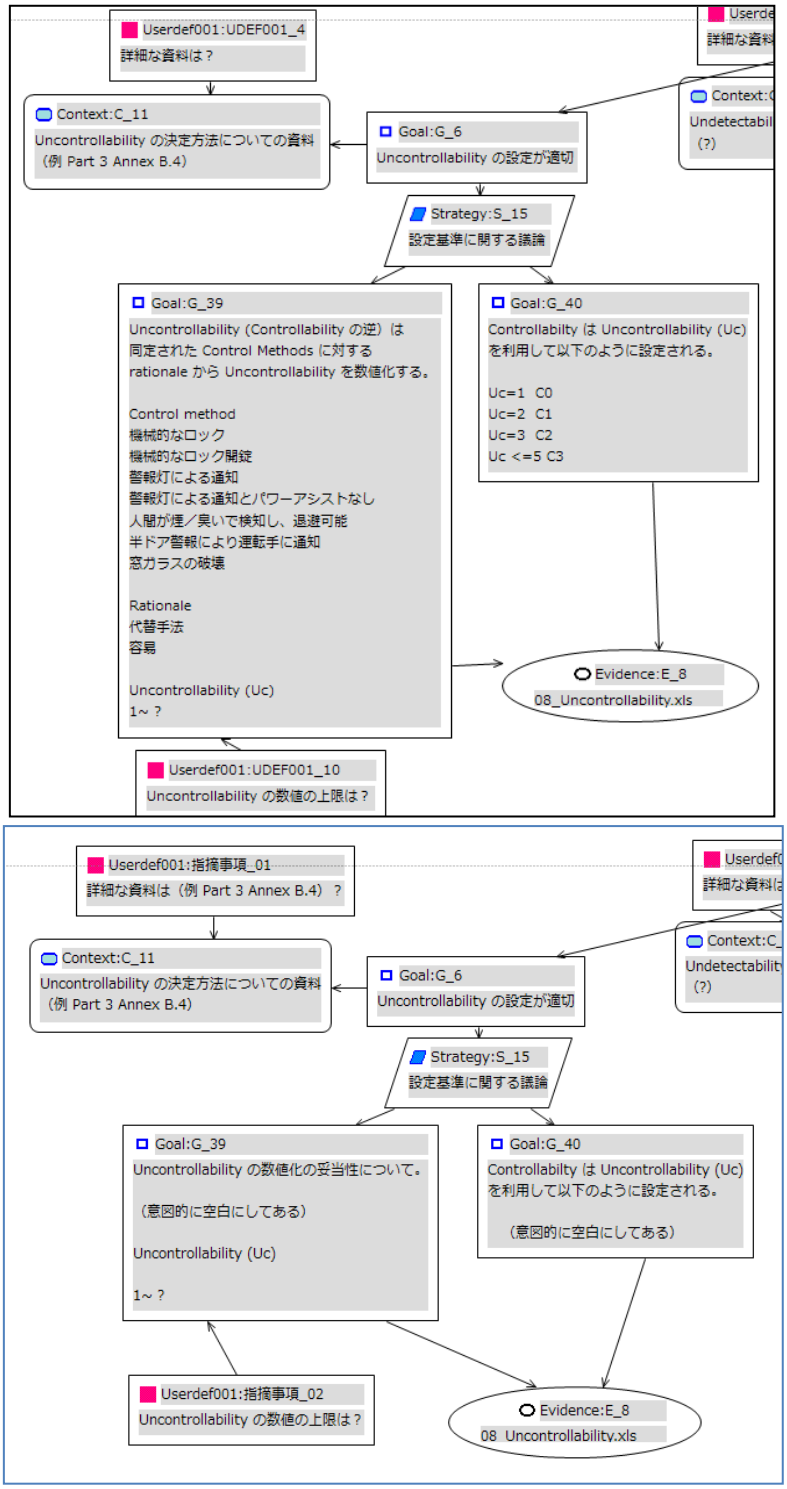


図 2.4. Uncontrollability について

ここでの uncontrollability の基準については、資料から読み取った。

何故、このような基準を設定したかについては、分析資料以外の説明資料の提示が必要であると思われる。

議論の根拠としては、08_uncontrollability.xls を提示した。

他の undetectability、severity、probability についても同様である。ただし、undetectabilityについては、その必要性、妥当性、他との関連について、議論を提示する必要がある。

以下に他の構造についても示す。

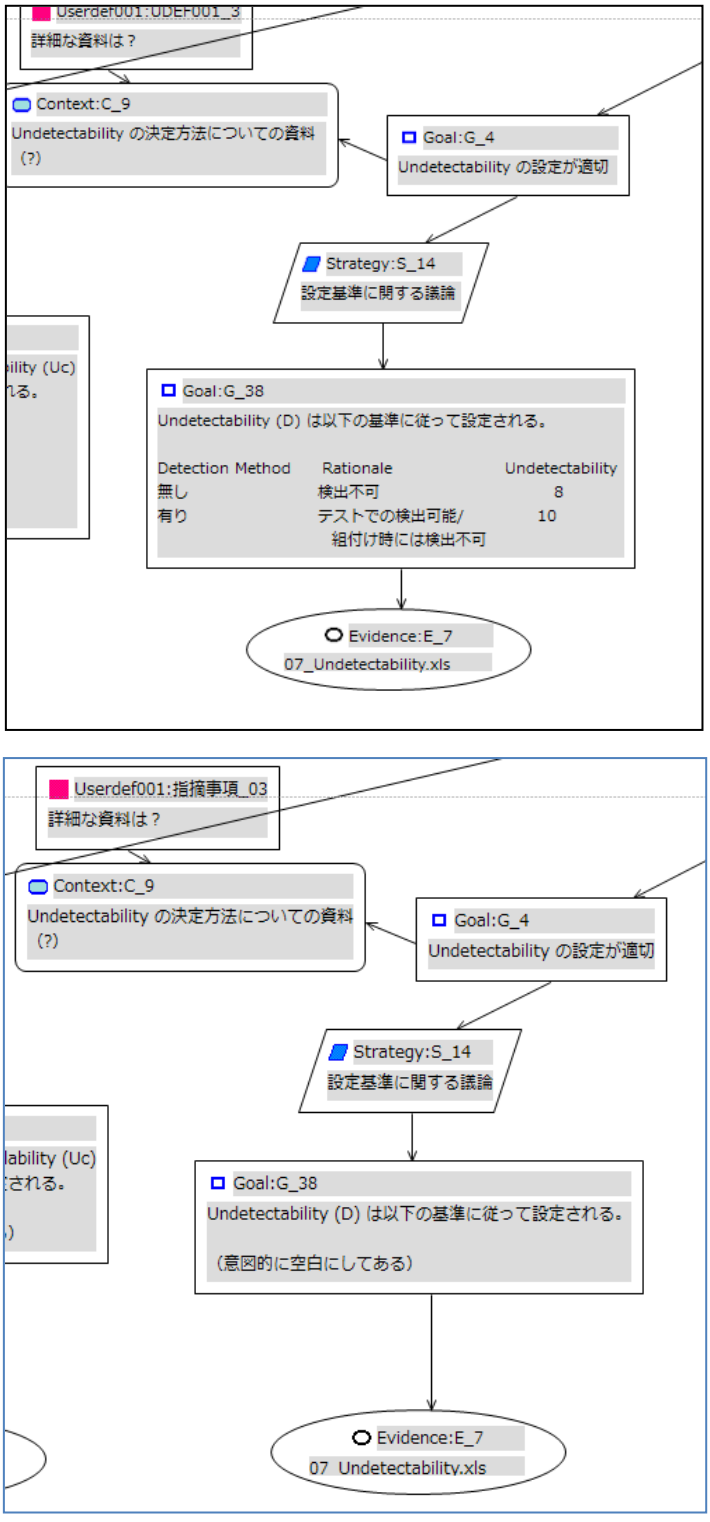
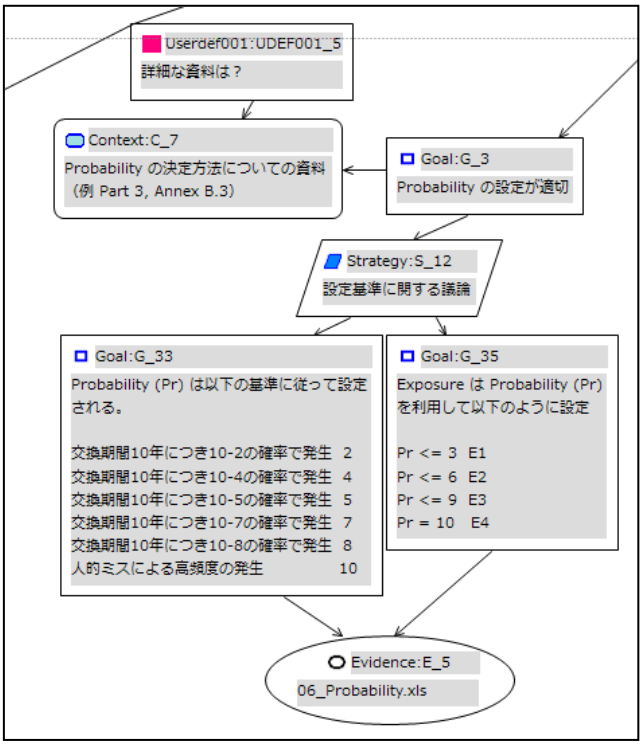


図 2.5. Undetectability について



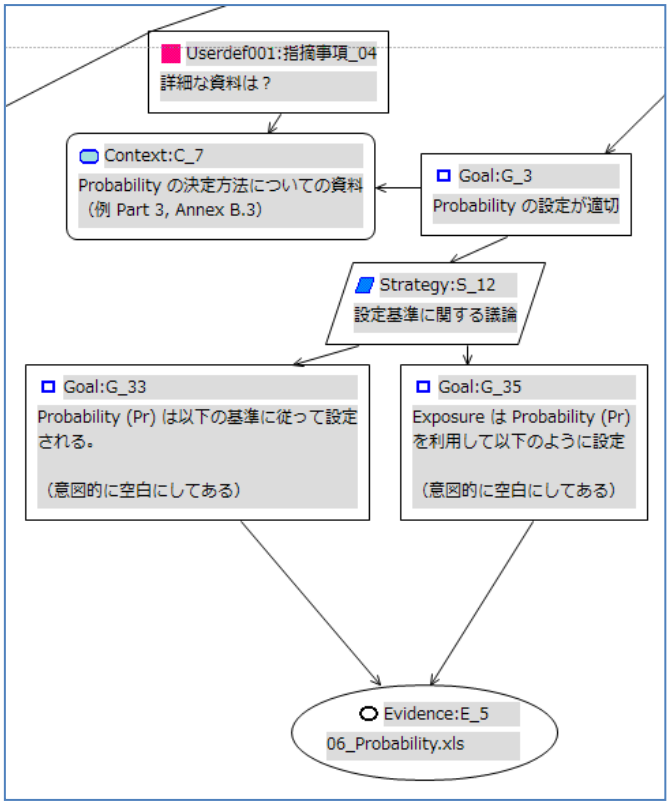


図 2.6. probability について

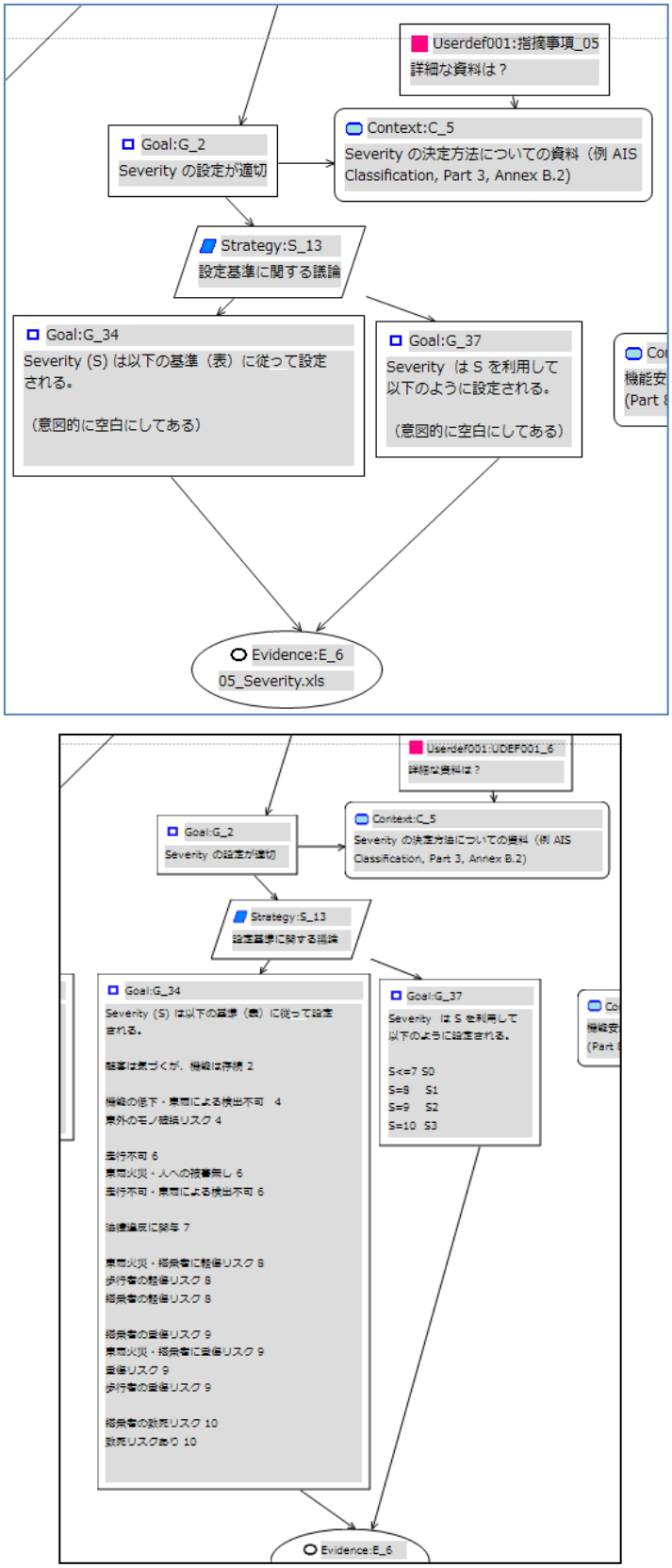


図 2.7. severity について

2.3. Cの構造

C においては、「機能安全概念（Functional safety concept）が規格に準じて定義されている」をトップゴールとして、機能安全概念が取り扱う、全ての問題について議論する構造とした。

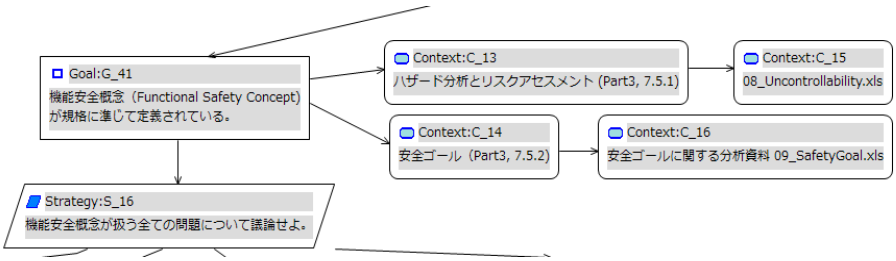


図 2.8. C の上部構造

この下に、「機能安全要件（Functional Safety Requirements）は規格に従って仕様記述されている」、「機能安全要件の導出は適切に行われている」、「機能安全要件の割り当ては適切に実施されている」、「妥当性確認の基準（Validation Criteria）は機能安全要件に従って仕様記述されている」という部分ゴールを導出した。

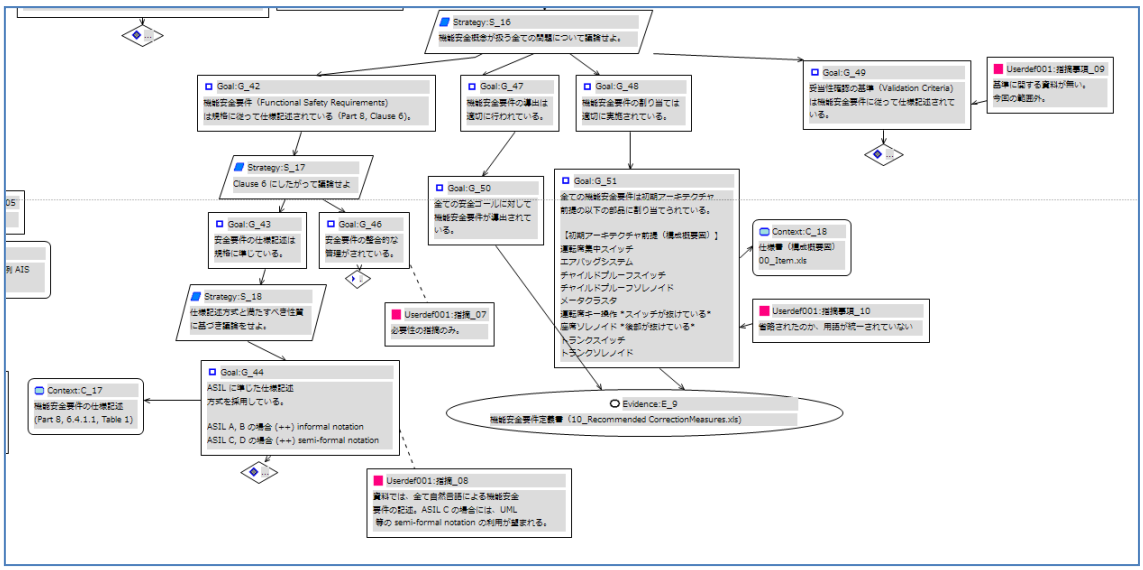


図 2.9. C の下部構造

最初の部分ゴールに関しては、さらに仕様記述方法と管理方法について分かれる。

次の部分ゴールについては、機能安全要件の導出と割り当ての適切性について議論を行っている。そしてその根拠資料は「機能安全要件定義書」である。

妥当性確認の基準については、展開が行われていない。

2.4. Dの構造

D は安全ゴールについての議論を展開するためのものである。現在同定された安全ゴールは 16 種類あるので、それらについて、そのハザード分析とリスクアセスメントの結果について、議論した。

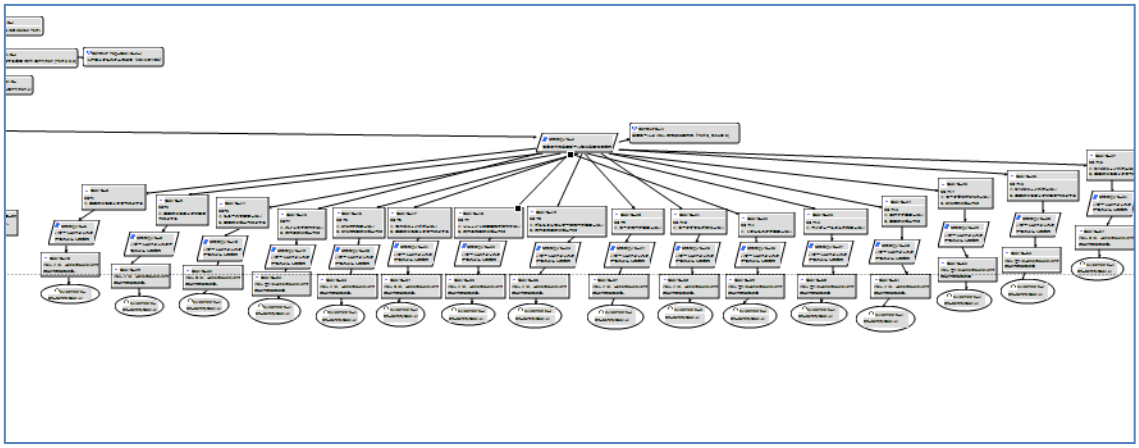


図 2.10. D の構造

16 の安全ゴールについて全て議論を展開している。現在、展開の方法は同一であり、ASIL の割り当ての妥当性について根拠資料を示している。

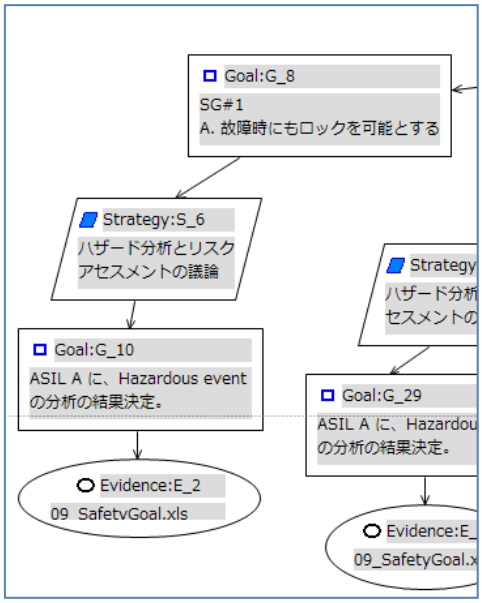


図 2.11. 安全ゴール

3. Part 4 Clause 6 に関するセーフティケース（GSN 図）

GSN 図としては、議論の構造を決める「上部構造」、「技術安全要件（Technical safety requirements）」の仕様記述に関する部分、「安全メカニズム（Safety mechanism）」、「ASIL 分解」、機能安全要件に関する「V&V（妥当性確認と検証）」から構成される。

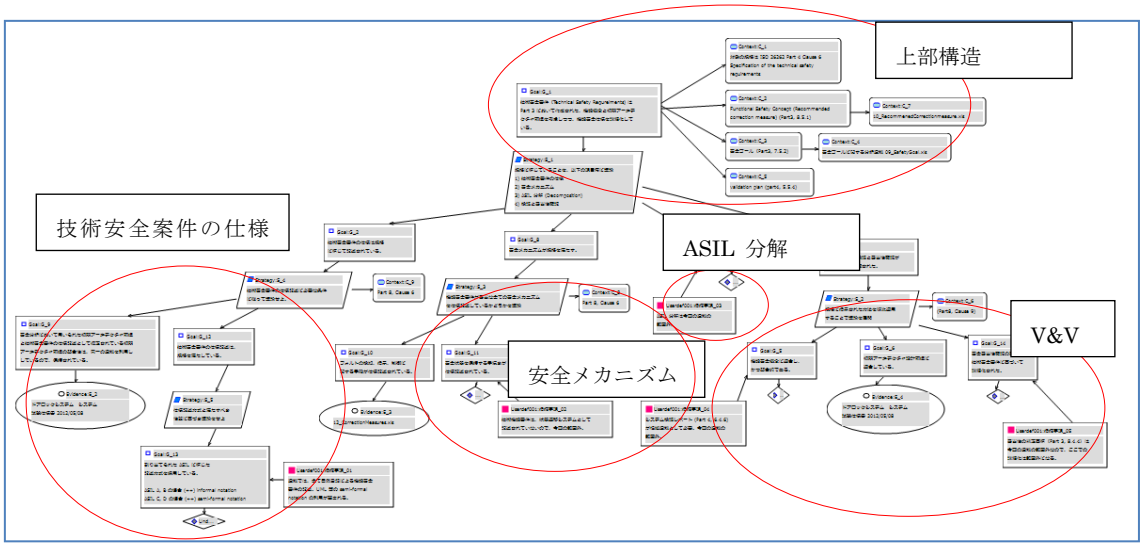


図 3.1. Part 4 に関する GSN 図

ASIL 分解は今回の資料には含まれないが、対象領域のセーフティケースとしての完全性を考慮し含め、注意事項として指摘を行った。

3.1. 上部構造

上部構造は、以下に示される。

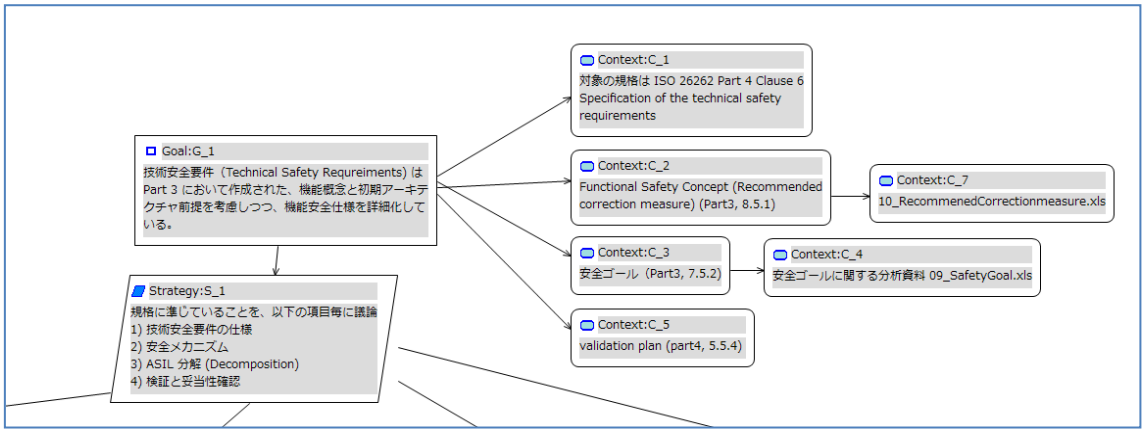


図 3.2. 上部構造

コンテクストとしては、どの規格を対象としているか（ISO 26262, Part 4, Clause 6,

Specification of the technical safety requirements)、Part 3 の成果物である機能安全概念、安全ゴールと Part 4 において作成された妥当性確認計画（Part 4, 5.5.4）である。特に最後の成果物は対象範囲外なので、参照資料としては何も与えられていない。

分解の戦略としては、各部分構造の特徴毎に議論をせよ、という形となっている。

3.2. 技術安全要件

技術安全要件についての議論であるが、Part 3 における機能安全要件と同様な制約がある。それが Part 8, Clause 6 Specification and management of safety requirements である。

最初のサブゴールは、part 3 において利用された初期アーキテクチャ前提（Preliminary architecture assumptions）と、本技術安全要件で利用されたものとの整合性が保持されていることであるが、それは同一の仕様書を用いているので、保証されている、というものである。

次のゴールは技術安全要件の仕様記述が割り当てられた ASIL のレベルにおいて、適切に利用されていることである。今回の資料は、全て UML のような semi-formal notation を利用していないので、本ゴールを満たしていない。ここでは、満たしていないことを指摘したまま残しておく。

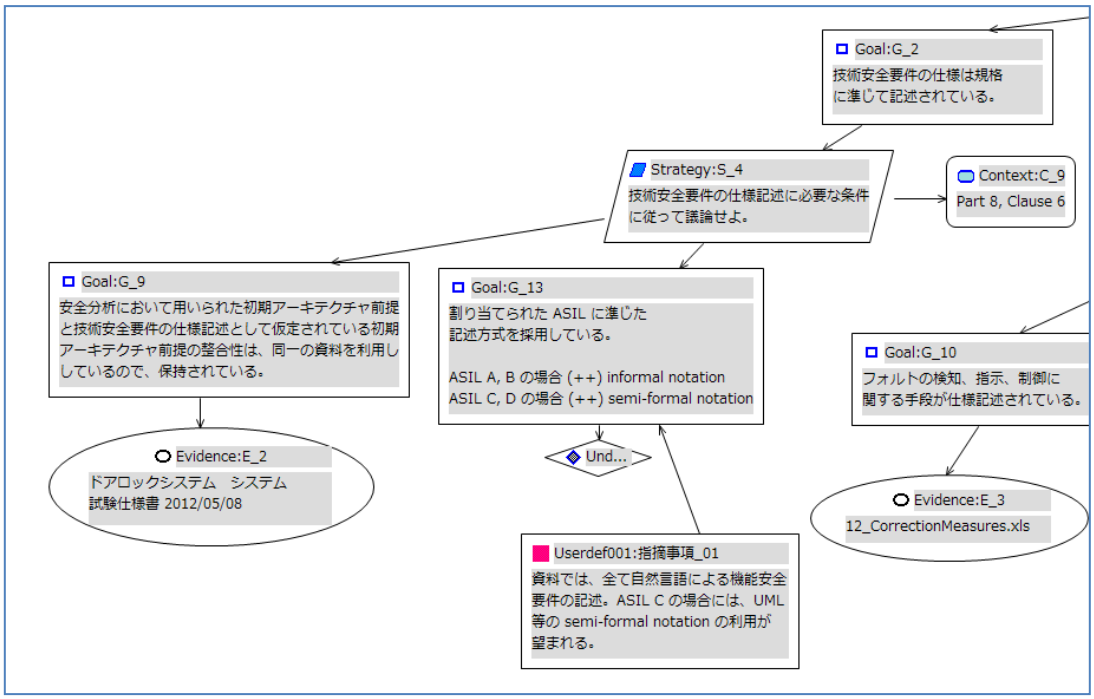


図 3.3. 技術安全要件の構造

3.3. 安全メカニズム

安全メカニズムに関しては、モデルとしての充足条件が満たされているかを議論する必要がある。そして、その内容の詳細は Part 8 の Clause 6 に依存している。ここでは、フォルトの検知、指示、制御に関する記述が行われているかについて、条件を満たしていることを根拠資料とともに示した。状態遷移システムとしての仕様記述も必要であるが、今回はモデルとしてそこまで記述されておらず、安全状態を保持する手続きの仕様記述については、資料として提供されていなかったが、その点については指摘にとどめている。

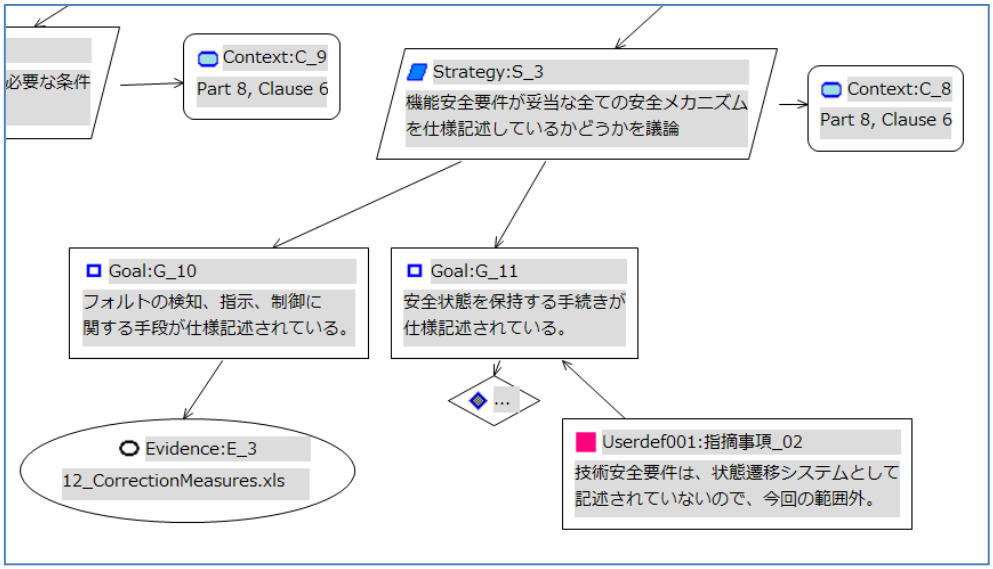


図 3.4. 安全メカニズムに関する構造

3.4. ＡＳＩＬ分解

ASIL 分解は今回の対象範囲外ということであったが、構造の中には残してある。

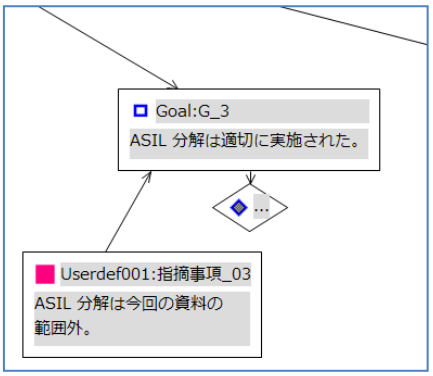


図 3.5. ASIL 分解

3.5. V & V

Verification and Validation（検証と妥当性確認）については、Part 8 の Clause 9 に従って検証が必要である。ここでは、Part 3 の「機能安全概念に適合し、かつ整合的である」というゴールに対しては、システム検証レポート（Part 4, 6.4.6）が必要になるが、今回の資料の対象外だったので、ゴールは未発展のままにしてある。それに対して、「初期アーキテクチャ設計前提（Preliminary architecture design assumption）に適合している」という適合性については、仕様書を根拠資料として満たしているとした。最後に、item に対する安全妥当性の基準の詳細化は、Part 3 における Validation criteria と関連するが、基準に対する根拠資料がないので、未発展のままにしてある。

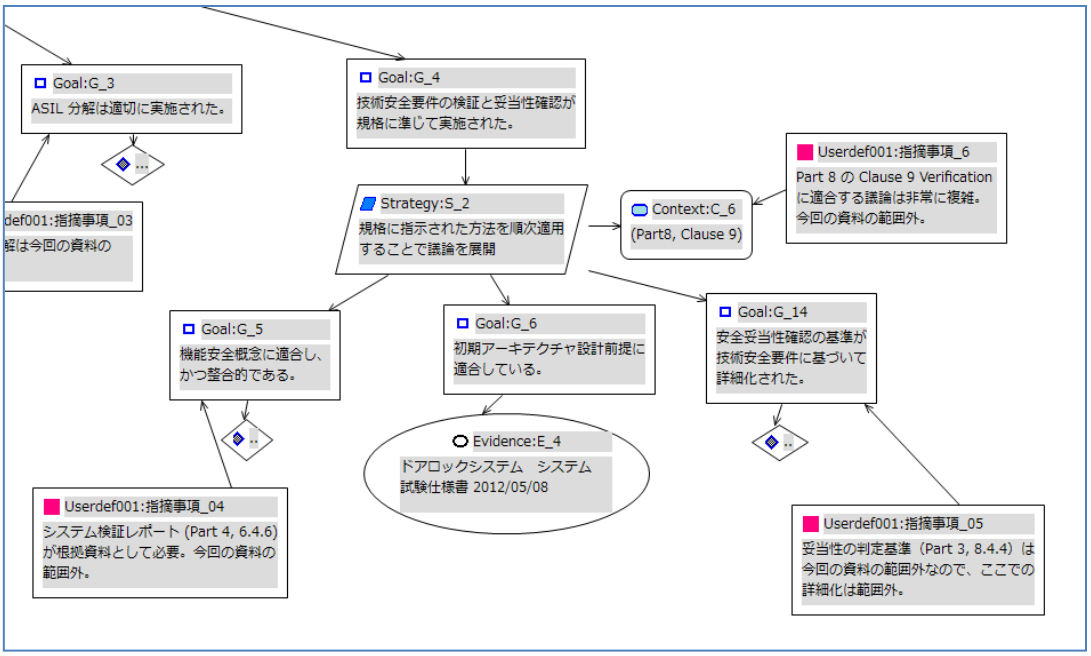


図 3.6. V&V

4. 工数

本章においては、各 GSN 図における指摘事項とその内容、指摘事項について作成する際の工数の根拠、指摘事項について今後作成する場合の見積もりを実施したので、その内容を記す。

様々な工業分野において作業見積もりの方法の確立が望まれているが、GSN図作成については研究論文のサーベイを実施したが、関連論文は発見出来なかった。本報告書における見積もりは、実作業ベースで推定されたものである。精密な見積もり方法を確立するためには、知見と経験が欠けているのが現状である。分析に必要な項目としては、主に以下が挙げられる。

- 開発者のセーフティケース作成経験（年数）
- 対象分野（規格、対象システム）に対する知識・経験（年数）
- 議論の抽象度（議論構造の深さと広さ。モジュラリティ）
- ケース作成の事前条件（スクラッチから作成か、既存のものの改訂。パターン利用の有無）

GSN 図作成を実際に行ったのは 1 名であり、他 1 名がレビューに加わった。実際に作成を担当した者の経験歴は以下の通りである。セーフティケース作成については、約 2 年のセーフティケース、アシュアランスケースの研究経歴（論文発表 1 本）と、OMG（Object Management Group）における Assurance case の規格化に携わった経歴を持っている。作成実績としては、ISO 26262 に関連するテンプレート作成（Part 3 と Part 4 の Clause 10 Functional safety assessment）の経験を有する。ここで言うテンプレートとは、GSN におけるパターンであり、実際のセーフティケースを作成する前に、特定の対象に対する議論の構造を定義するか、作成されたセーフティケースを再利用するために、スケルトンだけが抽出されたものである。GSN にはそのためのパターン言語があるが、上記の場合は D-case editor によるものなので、GSN のパターン言語は利用していない。

対象になった機能安全規格 ISO 26262 については、その内容について理解しているが、認証作業に実際に携わった経験は無い。対象システムであるドアロックシステムについては、概要的な知識を保有している。

本案件で対象になった Part 3 に関しては、Habli らの論文があり、全く白紙からの作成では無かったことはここに明記する必要がある。

【参考文献】

I. Habli, et. al., “Model-Based Assurance for Justifying Automotive Functional Safety”, in the proceedings of the 2010 SAE World Congress, Detroit, Michigan, USA, April 2010

レビューの内容は、議論の構造、適切な資料がコンテクストで参照されているか、適切な資料が根拠資料として利用されているかについて確認したものである。したがって、資料の妥当性確認とは異なることを明記する。

4.1. 作業の工数

以下に作業工数を示す。資料の分析は、GSN 図作成のために提供された資料の内容を分析するのに掛かった工数である。

作業項目	工数
1. 資料の分析	32 h
2. GSN 図作成（アーキテクチャ設計、作図、レビュー）	46 h

表 4.1. 作業工数

4.2. 作業の工数見積り（Part 3 部分）

GSN 図上に、GSN 作成時に作成した指摘事項を基に、GSN 作成の工数見積もりを行った。指摘番号は、GSN 図における Userdef001 ノードにおいて番号付けられたものである。指摘内容は、ノード内で省略された記述を正確に記述している。作業内容は、GSN 図に追加作業をする内容について記してある。作業時間は、作業の見積もり（最大時間）が記されている。

指摘番号	指摘内容	GSN 作成（作業内容）	見積もり作業時間（最大時間）
指摘事項_01	Controllability の決定に際する詳細な資料の必要性。例 Part 3 Annex B.4。****注意 1****	資料の分析とコンテクストの追加（最小時間：単なるコンテクストの追加。最長時間：資料の分析と確認）。****注意 2****	1h
指摘事項_02	Controllability を決定する際に利用される Uncontrollability の値の上限（提供資料にデータが無かった）。	資料の確認が必要なだけで、GSN 上での変更・追加は必要なし。	なし。
指摘事項_03	undetectability に関する資料の必要性。	資料の分析とコンテクストの追加（最小時間：単なるコンテクストの追加。最長時間：資料の分析と確認）****注意 2****	1h
指摘事項_04	Probability の決定に際する詳細な資料の必要性。例 Part 3 Annex B.3。****注意 1****	資料の分析とコンテクストの追加（最小時間：単なるコンテクストの追加。最長時間：資料の分析と確認）****注意 2****	1h
指摘事項_05	Severity の決定に際する詳細な資料の必要性。例 Part 3 Annex B.2。	資料の分析とコンテクストの追加（最小時間：単なるコンテクストの追加。最長時間：資料の分析と確認）****注意 2****	1h
指摘事項_06	リスクアセスメントを実施したチ	資料の分析と根拠資料の追加。	1h

	ームはリスクアセスメントと対象システムに対する十分な知識を持つかどうか。資料の関連で、指摘のみ。		
指摘事項_07	資料の関連で、指摘のみ。	資料の分析と根拠資料の追加。	1h
指摘事項_08	指摘のみ。資料は、全て自然言語による機能安全要件の記述が行われている。割り当てられた ASIL のレベルに従って、UML 等の semi-formal notation の利用が望まれる（例：ASIL C の割り当てがある）。	資料の分析と根拠の追加（ASIL 毎の記述の確認を根拠資料に対して実施し、GSN の根拠として付け加える）	2h
指摘事項_09	指摘のみ。妥当性確認の評価資料は提供されたが、基準に関する書類が欠如している。	妥当性評価のためには、Part 4, 6.4.6 Verification and Validation と 9.4.3 Execution of Validation を参照しながら、議論の展開が必要になるので、単に、根拠資料を追加すれば良い訳ではない。本 GSN 図と同等の抽象度と考え見積もった。	4h
指摘事項_10	用語の不統一（用語が省略されて利用）。	必要なし。	なし。

表 4.2. Part 3 の未作成部分の工数見積もり

注意１：

ASIL の決定のためには、Severity (S), Exposure (probability) (E), Controllability (C) をどのように決定したかが重要である。ISO 26262 では Annex B の B.2 Examples of severity, B.3 Examples and explanations of the probability of exposure、 B. 4 Examples of controllability (chances to avoid them)が例示されている。例えば、Severity については Abbreviated injury scale (AIS)や、Baker らによる The injury severity score などが参照されており、妥当性のある基準に基づく必要がある。今回、提供された資料には、独自の計算方式と根拠資料が利用されているが、その妥当性を示す資料が欠けていたので指摘したものである。

注意２：

これらの作業は、資料のアセスメントに必要な妥当性確認では無いことを注意されたい。

セーフティケースの妥当性確認においては、参照した資料の妥当性確認等が実施されるが、本作業は、セーフティケースを作成する際に、内容を確認するためだけであり、GSN 上で参照されていることが、すなわち、資料としての妥当性の確認が済んでいる、というものでは無いことを注意されたい。

4.3. 作業の工数見積り（Part 4 部分）

指摘番号	指摘内容	GSN 作成（作業内容）	見積もり作業時間（最大時間）
指摘事項_01	資料では、全て自然言語による機能安全要件の記述。ASIL C の場合には、UML 等の semi-formal notation の利用が望まれる。	資料の分析と根拠の追加（ASIL 毎の記述の確認を根拠資料に対して実施し、GSN の根拠として付け加える）	2 h
指摘事項_02	技術機能要件は、状態遷移システムとして記述されていないので、今回の範囲外。	資料の分析と根拠の追加（各技術安全要件に対して、状態遷移システムとしての記述を確認し、GSN の根拠として付け加える）	2 h
指摘事項_03	ASIL 分解は今回の資料の範囲外。	ASIL 分解については、分解の妥当性の検証が難しく、また事例としては、ケースバイケースで実施される。であるので、どの程度の規模の GSN 図になるかどうかは現時点で判断するのは困難。	不明。
指摘事項_04	システム検証レポート（Part 4, 6.4.6)が根拠資料として必要。今回の資料の範囲外。	対象となる技術安全要件と Part 3 において作成された機能安全概念とが適合しているかについての議論が必要になる。どの程度の規模の GSN 図になるかは現時点で判断するのは困難。	不明。
指摘事項_05	妥当性の判定基準（Part 3, 8.4.4）は今回の資料の範囲外なので、ここでの詳細化は範囲外。	資料の分析と根拠資料の追加（詳細化された適合性確認計画 Part 4 6.5.3（基準はその一部）を根拠資料として追加)。	2 h
指摘事項_06	Part 8 の Clause 9 Verification に適合する議論は非常に複雑。今回の資料の範囲外。	システム検証レポートの妥当性に関する、Part 8 Clause 9 は、Part 4 Clause 6 と同様の分量を持ってい	22h

		る。Part 4 の工数と同等なものとして、作業工数の見積もりを行った。	

表 4.3. Part 4 の未作成部分の工数見積もり

5. まとめ

本案件においては、GSN 図を用いて ISO 26262 のセーフティケースの作成を行った。ISO 26262 の規格通りに行う部分と若干ずれる部分については、より詳細に議論を構築する必要があるので、その点については注意を払った。ISO 26262 におけるセーフティケースの書き方はまだ確立していないので、このようなトライアルをより実践的な環境において実施する必要があると思われる。

見積もりについては、どれだけの議論を展開すれば良い、という基準が無いので、見積もる方法論が確立していないのが現状である。今後、厳密な方法論を確立する必要がある。

6. 付録

最初に、本案件の対象である ISO 26262 のセーフティケースについて説明を行う。セーフティケースの定義は多々あり、共通の理解のものに本案件を進めるためにも、説明が必要であると考えられる。

6.1. ISO 26262 において定義されているセーフティケース とは

本案件の対象規格である ISO 26262 では、セーフティケース の記述は、Part 1、Part 2、そして Part 10 において述べられている。Part 1 のセーフティケースの定義では、以下のように記述されている。

> *1.106*
> *safety case*
> *argument that the safety requirements for an item (1.69) are complete and satisfied by evidence compiled from work products of the safety activities during development*
>
> *NOTE Safety case can be extended to cover safety (1.103) issues beyond the scope of ISO 26262.*

（ISO 26262 Part 1, page 14）

セーフティケース の定義として特別な意味を付与している形ではないが、item というシステム（もしくはサブシステム）を表す ISO 26262 独自の用語については注意が必要である。

注意として記されているが、セーフティケースは ISO 26262 のスコープを超えて利用することも可能である。その場合には、規格に規定された内容とは異なる議論を、独自に構築する必要がある。

ISO 26262 におけるセーフティケース の記述に関しては、以下のように規定されている。

> ***6.4.6 Safety case***
> ***6.4.6.1*** *This requirement shall be complied with for items that have at least one safety goal with an ASIL (A), B, C or D: a safety case shall be developed in accordance with the safety plan.*
> ***6.4.6.2*** *The safety case should progressively compile the work products that are generated during the safety lifecycle.*

(ISO 26262, Part 3, page 13)

すなわち、本要件（セーフティケース）は、ASIL（Automotive Safety Integrity Level）A、B、C、D が割り振られた少なくとも一つの安全ゴールを持つ item のために作成され、セーフティケースは規格で規定された safety plan に従って開発されなければならない、という点と、安全ライフサイクルの間に生成された work product（規格で規定された提出すべき成果物）を、漸次的に集めなければならない、ということが示されている。

ここで、分かるのは、Part 3（Concept Phase）で作成される、ASIL が割り当てられた安全ゴールに関する議論に対して利用され、根拠資料として利用されるのは work product である、ということである。

6.1.1. セーフティケースのライフサイクル

セーフティケースも他の産業製品と同様に、作成から破棄されるまでのライフサイクルを持つ。セーフティケースは作成された後、レビューを受け、その完全性についての検証が行われる（Part 2, Table 1, page 15）。その後、受理され、改訂が必要になれば保守が行われ、最後に必要が無くなると放棄される。

1） 作成
2） レビュー
3） 受理
4） 保守
5） 放棄

本ライフサイクルで本案件に関連するのは、１）～２）である。

6.1.2. セーフティケースのレビュー

セーフティケースのレビューには様々な条件があるが、ここでは ISO 26262 で規定されたレビューの方法を示す。

C.2 Review of the completeness of the safety case (see 6.5.3)

C.2.1 *Confirmation that the work products referenced in the safety case are available and sufficiently complete, so that the item's achievement of functional safety can be adequately evaluated.*

NOTE The referenced work products can be the work products that are identified as relevant to support the safety case.

C.2.2 *Confirmation that the work products referenced in the safety case:*

- *are traceable from one to another,*
- *have no contradictions within or between work products, and*
- *either have no open issues that can lead to the violation of a safety goal, or have only open issues that are controlled and have a plan for closure.*

(ISO 26262, Part 2, page 21)

ISO 26262 においては、セーフティケース の中で work product（提出すべき成果物）が根拠資料として参照され、レビューにおいては、それらが利用可能であり十分に完全であるか確認することで、item の機能安全の達成が、適切に評価されること、さらに、 セーフティケースにおいて参照される work product については、互いにトレーサブルであり、相互に矛盾が無く、安全ゴールを侵害するようなオープンイシューが無いことを確認する必要があることと記されている。