GSNの鉄道分野での適用

1) 独立行政法人 産業技術総合研究所, 2)西日本旅客鉄道株式会社
相馬 大輔[1)], 田口 研治[1)], 西原 秀明[1)] , 大岩 寛[1)], 矢田部 俊介[2)], 森 崇[2)]

本発表の目的と関連研究

- **本発表の内容は2012年からの西日本旅客鉄道株式会社様との共同研究で得られた成果の一部である。**

- **本発表は以下を目的としている**
  - GSNで記述することによる理解の難しい規格の記述の整理
    - 目的、要求事項、検証、成果物の対応関係の明確化
    - 参照する事項がコンテキストとして明確化
  - アセスメントのための文書作成支援
    - GSNとセーフティケーステンプレートの連携によるGSNを基にしたセーフティケースの記載内容のチェック
  - 規格適合のアセスメント支援
    - GSNとセーフティケーステンプレートの連携による記載事項の理由の明確化

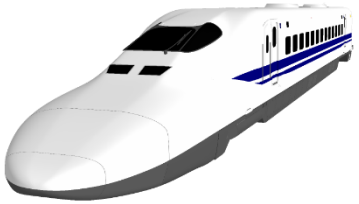
- **関連研究**
  - Parameterised Argument Structure for GSN Patterns, Yutaka Matsuno and Kenji Taguchi
  - A Formal Basis for Safety Case Patterns, Ewen Denney and Ganesh Pai
  - Safety Case Construction and Reuse using Patterns, Tim Kelly, Jhon McDermid

目次

- 鉄道の安全性と規格
- RAMSのGSNによる記述
- セーフティケースとGSNの連携

鉄道の安全性と規格

安全性を求められるシステム規格

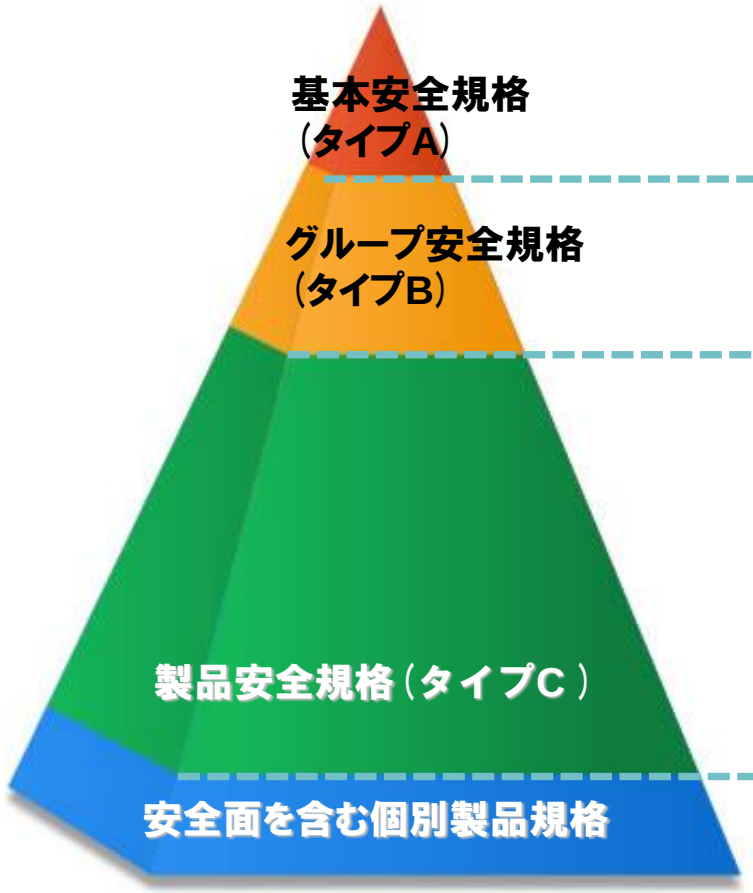



多くのシステムは規模の拡大や多くの機能の実現などにより一層複雑化している
一方で**高い安全性**も求められている

安全性の規格に適合していることで、**システムの安全性**を示す

特にここでは、機能により安全を担保するという**機能安全**を取りあげる

機能安全規格



A 基本安全規格

ISO 12100（基本設計原則）

B グループ安全規格

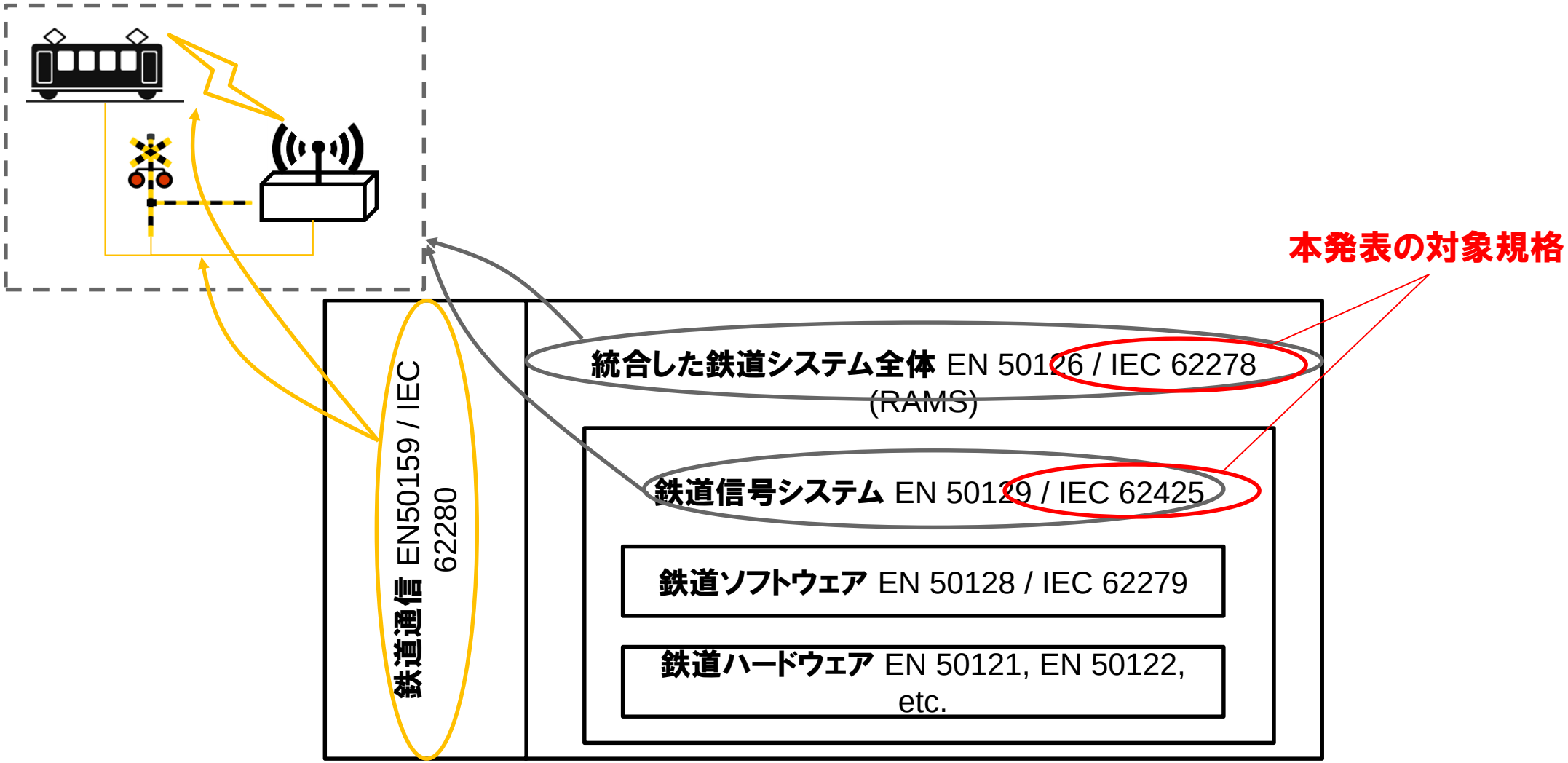
IEC 61508（JIS C 0508）

C 様々な産業分野における製品安全規格

鉄道 (RAMS)	EN 50126 / IEC 62278
自動車	ISO 26262
航空機	DO-178C
医療機器	IEC 62304
原子力	IEC 61513
産業ロボット	ISO 10218

D 安全面を含む個別製品規格

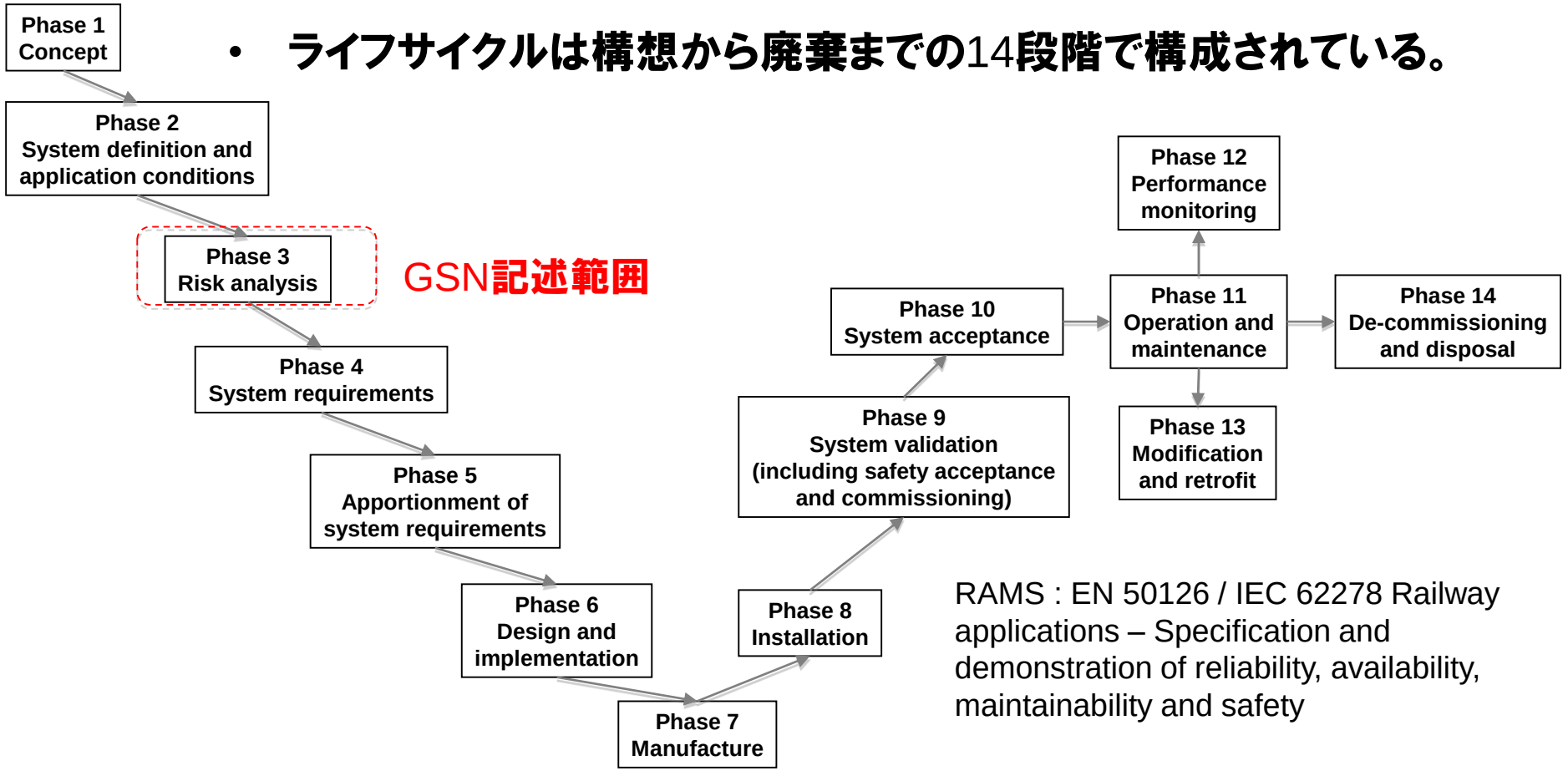
鉄道分野の機能安全規格と関連



IEC 62278 (RAMS)のライフサイクル

- RAMS : **鉄道における機能安全規格の最上位**

- **ライフサイクルは構想から廃棄までの14段階で構成されている。**



RAMS : EN 50126 / IEC 62278 Railway applications – Specification and demonstration of reliability, availability, maintainability and safety

RAMSの各段階での記載事項

RAMSの各段階は5つの項目から成り立っている。

- 目的
  段階で達成するべき目的が記述されている
- インプット
  目的達成のために必要なインプットが挙げられている
- 要求事項
  目的達成のためのタスクや成果物に記載しなくてはならない内容など様々な内容が記述されている
- 成果物
  実施した結果をどのような成果物としてまとめ、提出するかが述べられている
- 検証
  前段階と現段階、または現段階内の成果物の整合性や完全性について検証しなくてはならない事項を挙げている

RAMS Phase 3 Risk Analysisについて

Phase 3 Risk Analysisは

① 当該システムに関わるハザードを特定する
② ハザードの発生につながる事象を特定する
③ ハザードに付帯するリスクを明らかにする
④ リスクを継続的に管理するプロセスを確立する

という4点の達成が目的であり、
①～③の結果はハザードログという成果物にまとめられ、④の基準となる。

リスク分析はライフサイクルの各段階で繰り返し実施される。

セーフティケース(IEC 62425)とは

- システムの安全性を示すための文書
  - システムの受け入れ、安全性評価、規格適合アセスメントに用いる

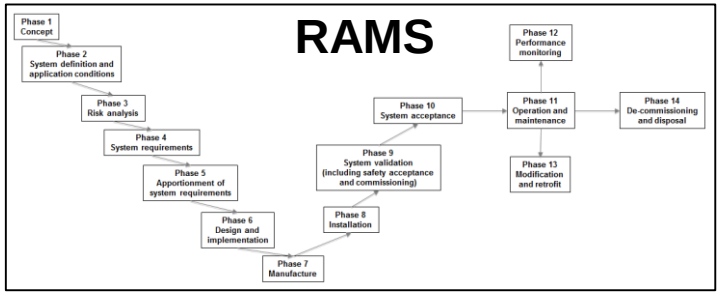
- IEC 62425ではセーフティケースに記載すべき内容が記述されており、以下の6つの章で構成される
  - システムの定義
  - 品質管理レポート
  - 安全管理レポート
  - 技術的な安全性に関わるレポート
  - 関連するセーフティケース
  - 結論

課題1: 機能安全規格RAMS適合のアセスメント

鉄道分野では対象システムの安全性を示す文書(セーフティケース)を作成しアセサーはそれを基に規格適合のアセスメントを実施する

課題 1-1

- RAMSとセーフティケース(IEC 62425)間の関係が不明確であり作成のコストが高い
- 詳細に開発過程で作成された成果物について記述が必要となり漏れ抜けをしやすい



安全を示す文書を作成

セーフティケース

規格適合性のアセスメント

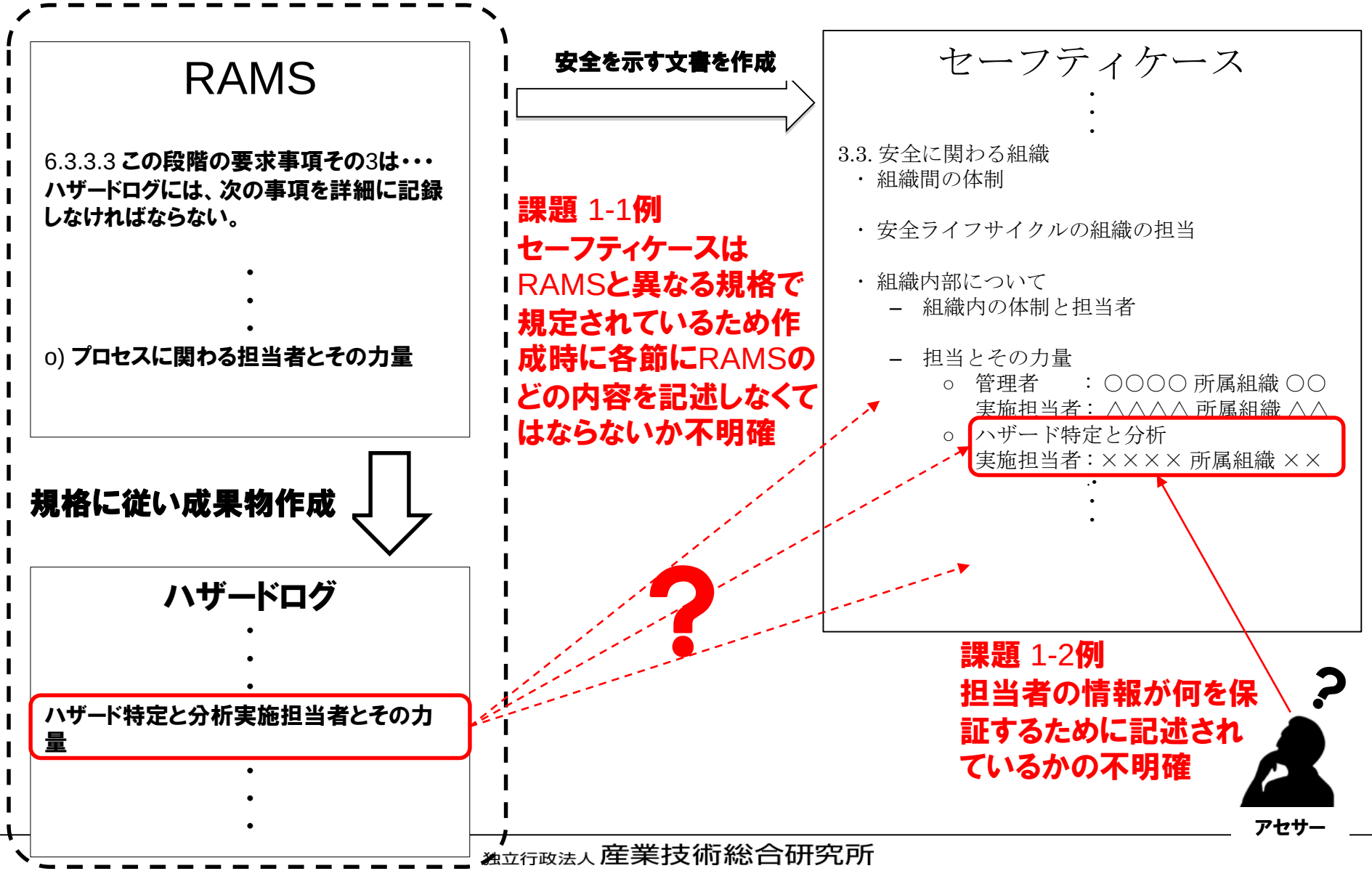
?

アセサー

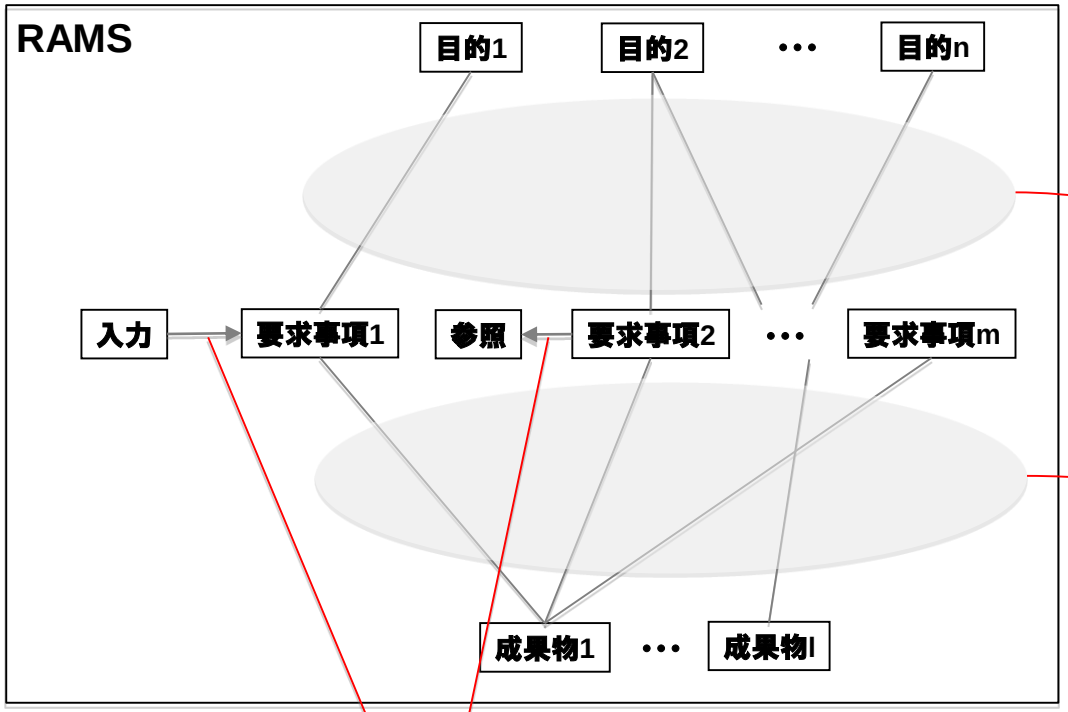
課題 1-2

- セーフティケースの記述内容が規格のどの部分と対応するのか不明確になりやすい
- 記載内容の根拠を理解するのが難しい

課題1の具体例


RAMS
6.3.3.3 この段階の要求事項その3は・・・
ハザードログには、次の事項を詳細に記録しなければならない。
o) プロセスに関わる担当者とその力量
規格に従い成果物作成
ハザードログ
ハザード特定と分析実施担当者とその力量
安全を示す文書を作成
セーフティケース
3.3. 安全に関わる組織
・組織間の体制
・安全ライフサイクルの組織の担当
・組織内部について
– 組織内の体制と担当者
– 担当とその力量
o 管理者 : ○○○○ 所属組織 ○○
実施担当者：△△△△ 所属組織 △△
o ハザード特定と分析
実施担当者：×××× 所属組織 ××
課題 1-1例
セーフティケースはRAMSと異なる規格で規定されているため作成時に各節にRAMSのどの内容を記述しなくてはならないか不明確
課題 1-2例
担当者の情報が何を保証するために記述されているかの不明確
アセサー

課題2：機能安全規格(RAMS)の理解



課題
- 記述されている内容の関係があいまい

課題
- どの情報を入力とするかどの文書や項目を参照するかがあいまい

RAMSのGSNによる記述

Goal Structuring Notation (GSN)

- **保証のための構造化された議論の記述方法**
  - T. Kelly**らにより開発**
  - GSN Community Standard (**入手可能な最新のリファレンス**)

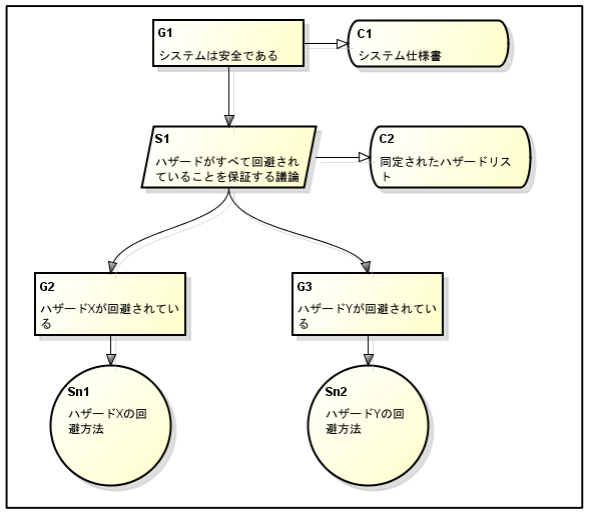
- **システムが満足するべき目標からトップダウンで議論を構造化**

ゴール：**システムが満足するべき目標(部分目標)。**

ストラテジー：**論証の方法。ゴールからサブゴールを導く方針。**

ソリューション：**論証をサポートする具体的な証拠。**

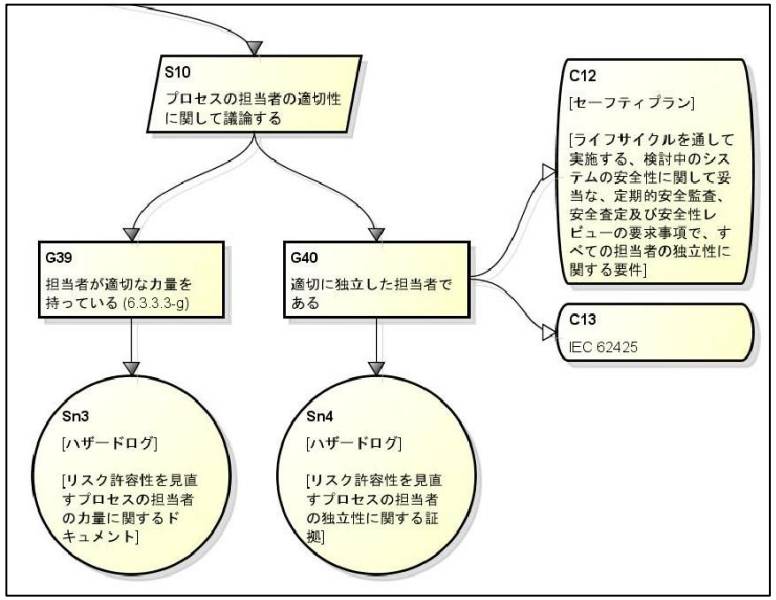
コンテキスト：**議論の背景や文脈。**



RAMSのGSN化について

- **段階ごとにGSNを作成**
  - **ここでは第3段階 リスク分析をGSN化**

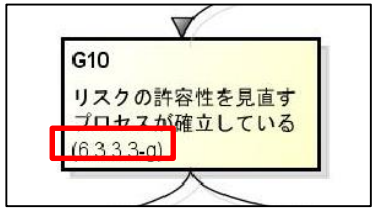
- **規格に記述された内容に沿ってGSNを作成**
  - **安全分析に関する部分と継続的なリスク管理に関する部分を優先的に作成している。**
  - **一部、RAMS認証のための提出ドキュメントテンプレートよりソリューションを作成している。**
  - **ソリューションやコンテキストなどRAMSの成果物が配置される部分は後述する記述方法によりGSNテンプレートとしている。**

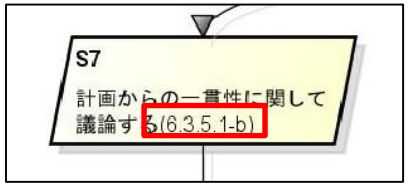


- GSNの作成はastah*/GSN (ChangeVision社製)を使用

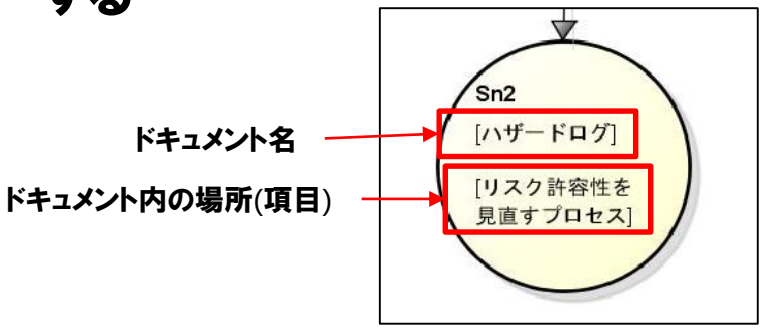
GSNの書き方

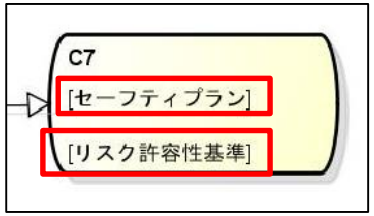
- **要求事項、検証の項目はゴールやストラテジーとして記述される。その際、対応する規格の項目番号を()付で記載する。**

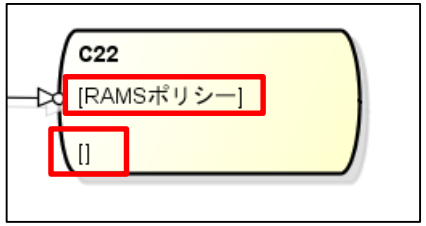




- **ソリューションまたは他段階の成果物をコンテキストとして記述する場合は[ドキュメント名]と[ドキュメント内の場所(項目)]を記述する。ただし、ドキュメント全体が対象の場合はドキュメント内の場所(項目)を空欄として[]のみ記述する**





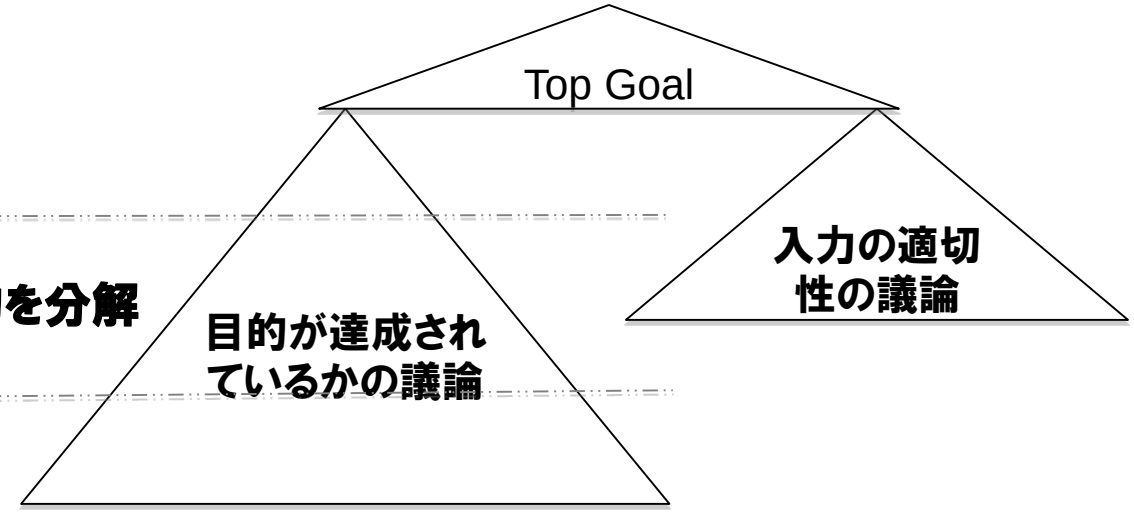


Phase 3 GSNのアーキテクチャ

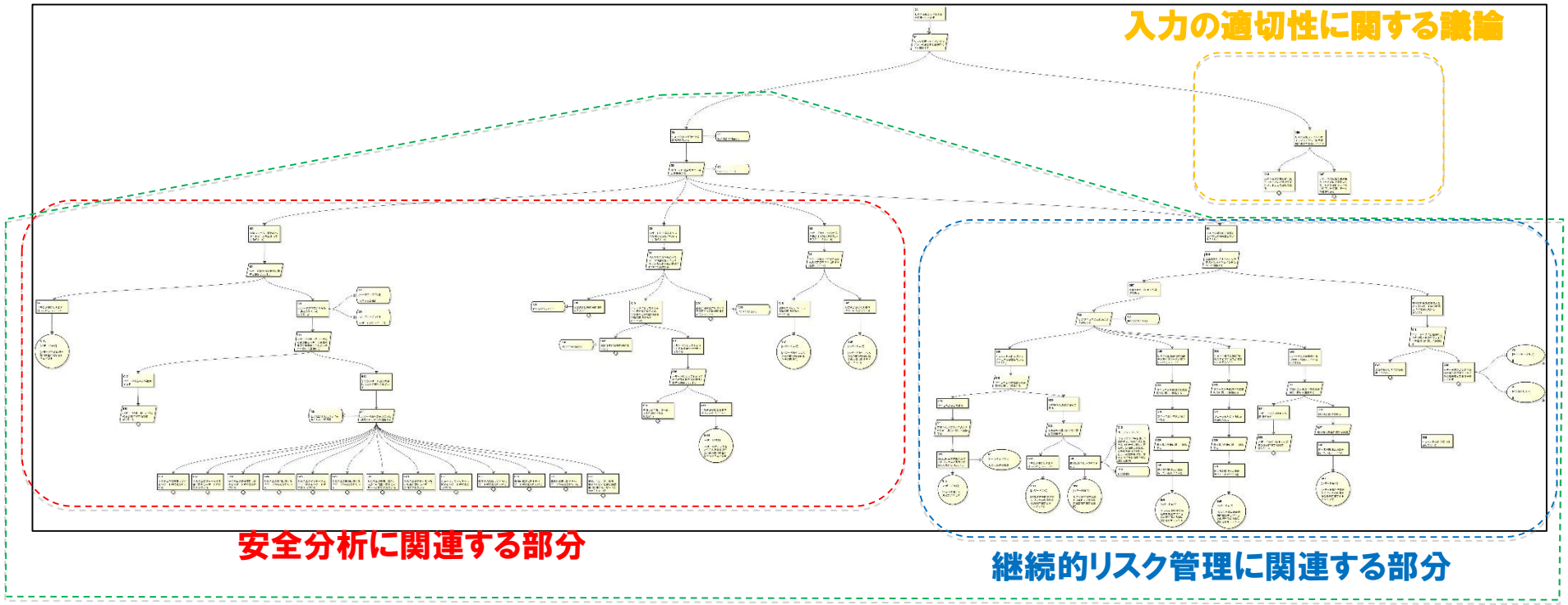
目的ごとにゴールを設定

要求事項、検証などの項目により目的を分解

成果物をソリューションとして配置



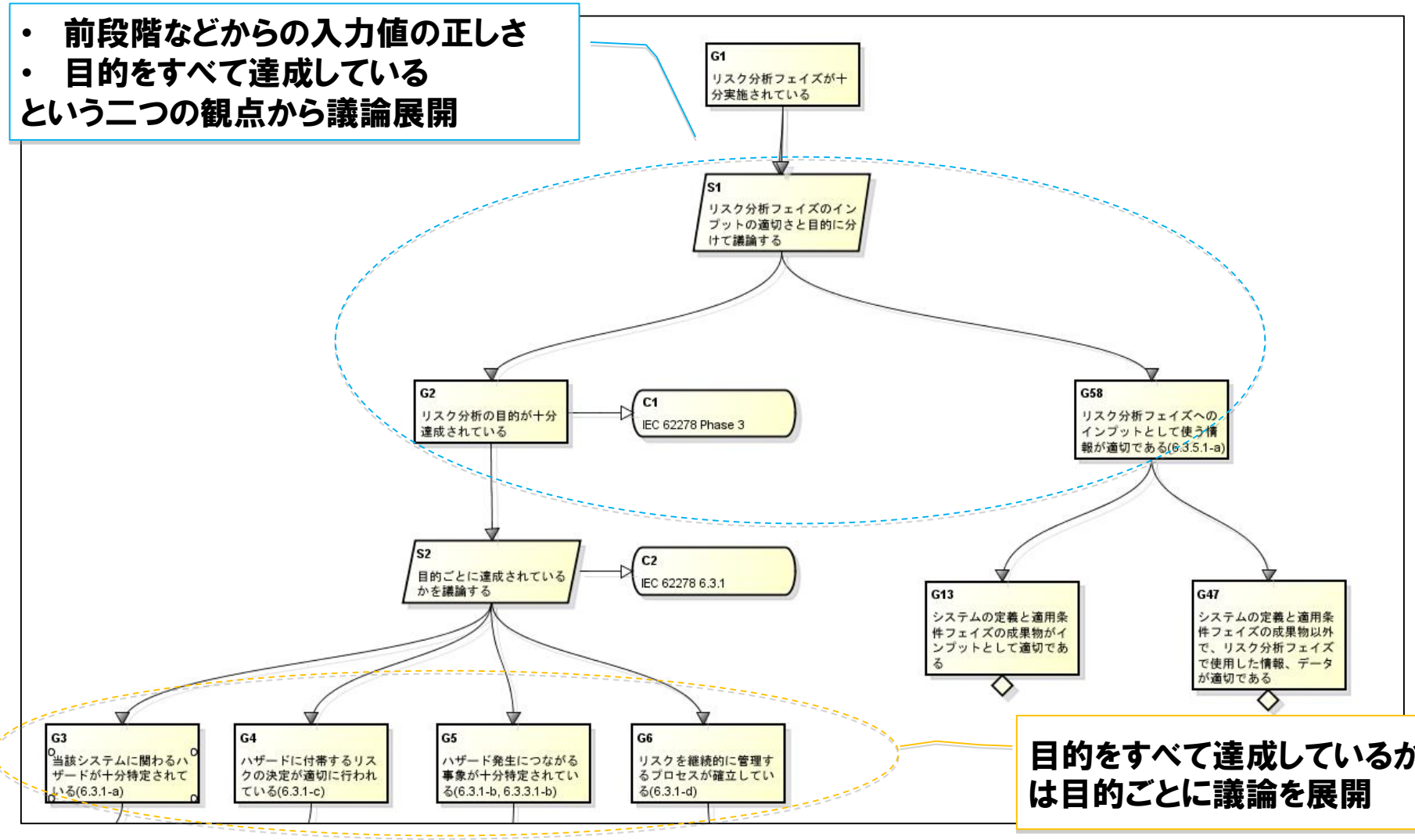
Phase 3 GSNの全体像



GSN上部構造

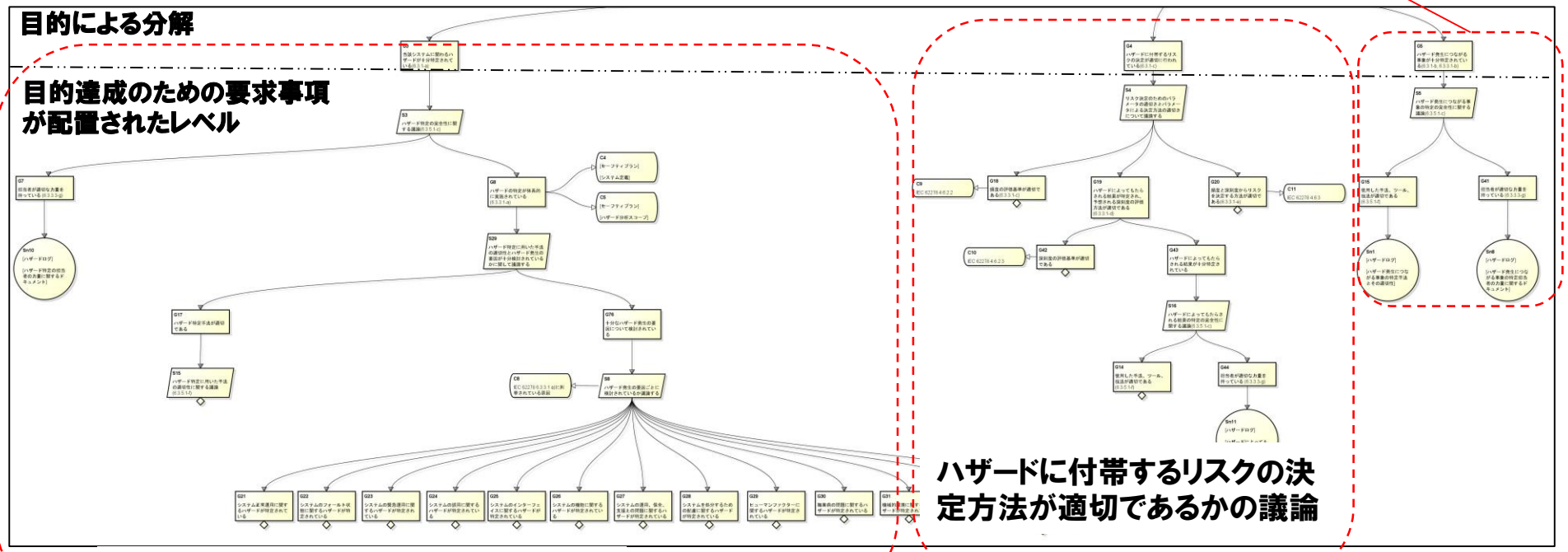
- 前段階などからの入力値の正しさ
- 目的をすべて達成している

という二つの観点から議論展開

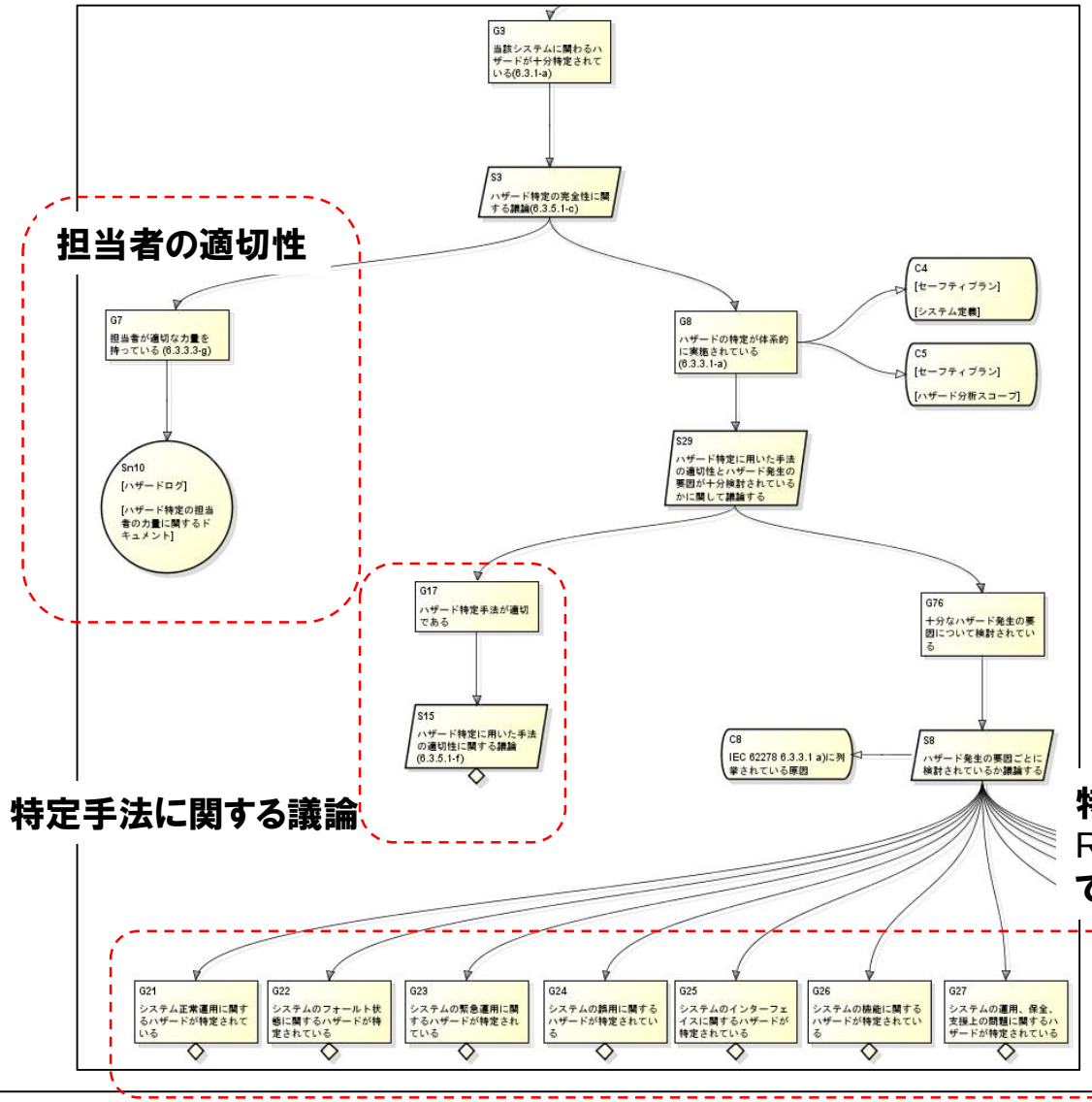


目的をすべて達成しているかは目的ごとに議論を展開

安全分析に関する議論

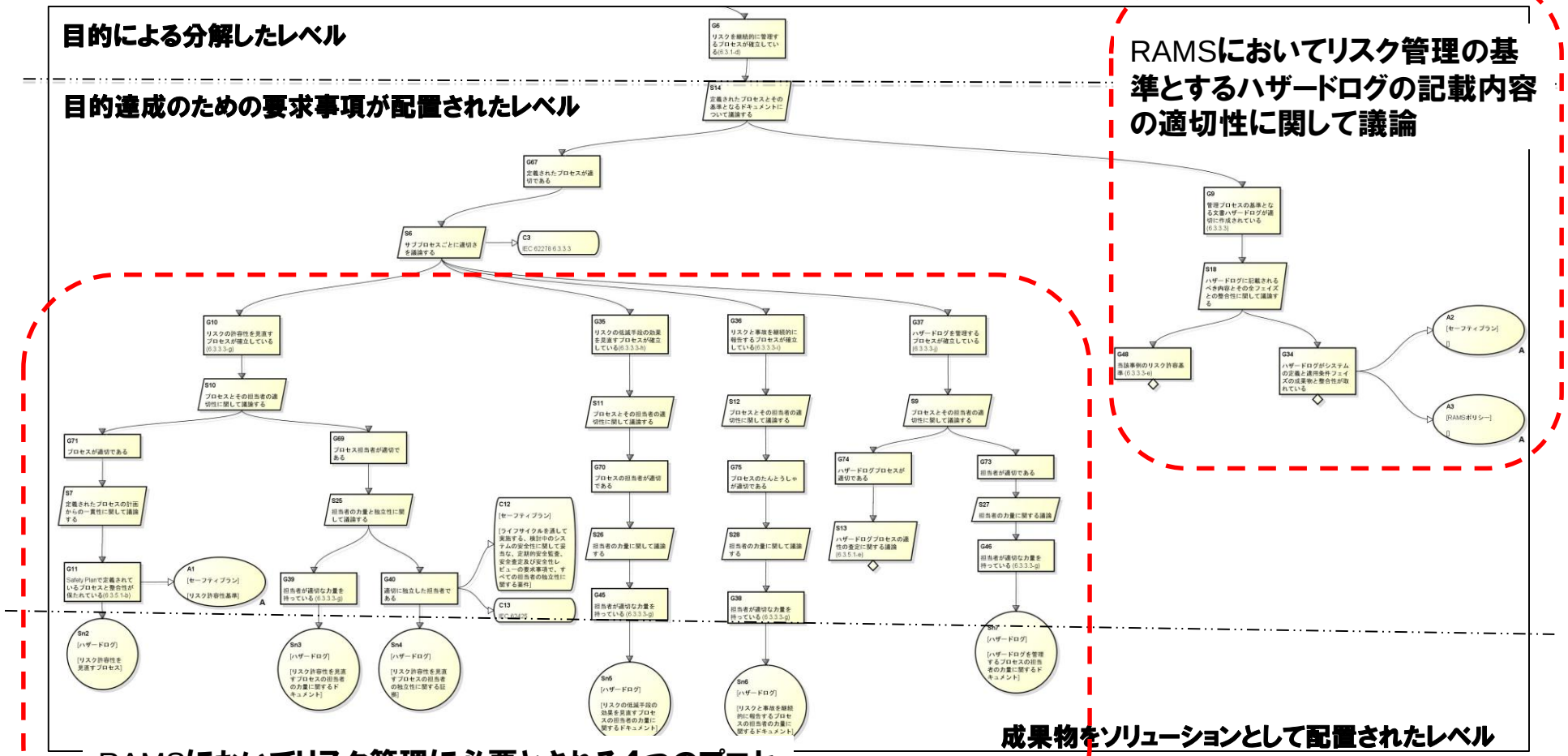

目的による分解
目的達成のための要求事項が配置されたレベル
ハザードの発生につながる事象が十分特定されていることに関する議論
ハザードに付帯するリスクの決定方法が適切であるかの議論
ハザード特定の十分性に関する議論

ハザード特定の十分性に関する議論



特定されたハザードの網羅性に関して、RAMSで考慮すべき発生要因がすべて網羅されているかにより議論

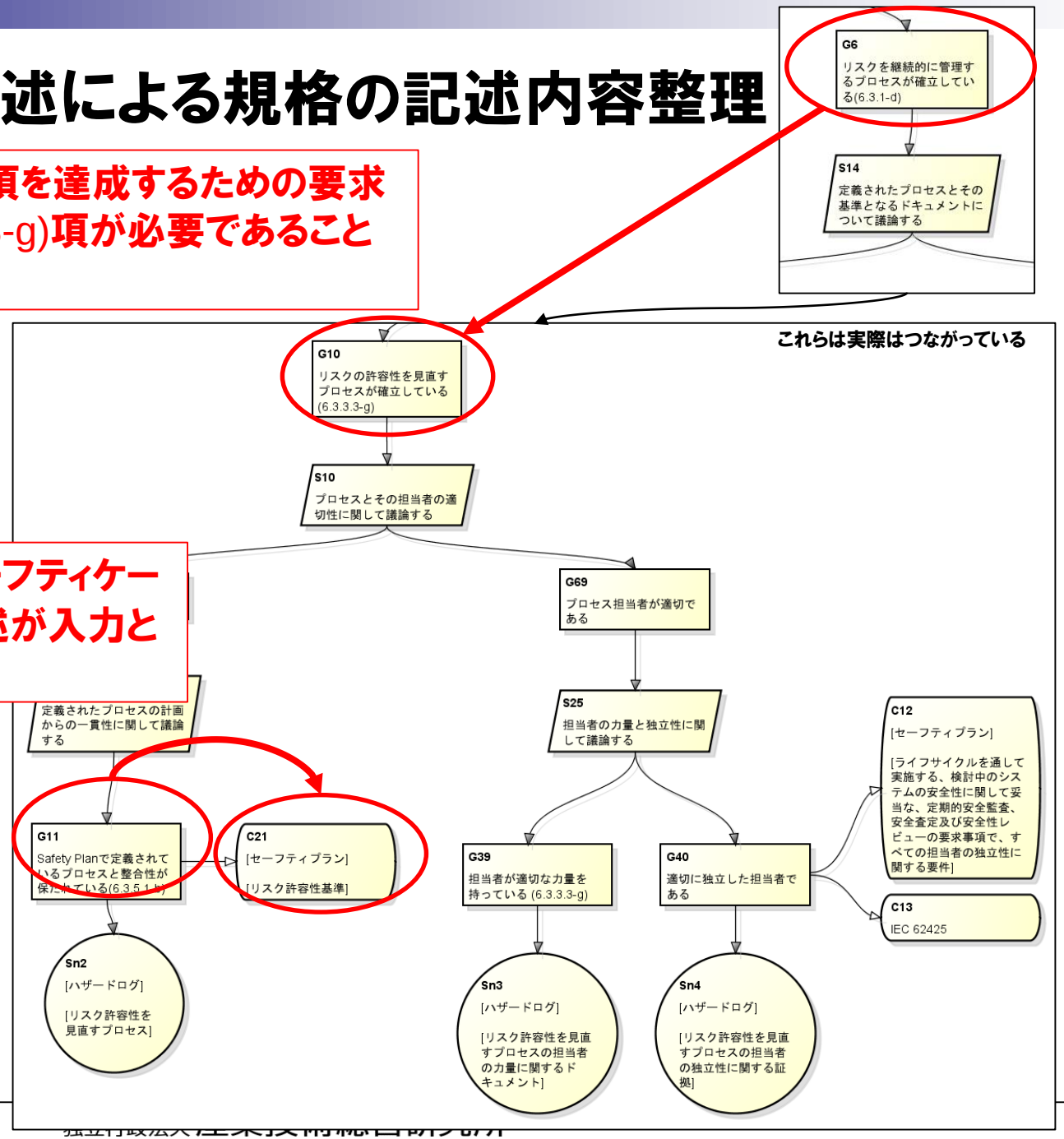
継続的なリスク管理に関する議論



GSN記述による規格の記述内容整理

目的6.3.1-d)項を達成するための要求事項に6.3.3.3-g)項が必要であることが明確化

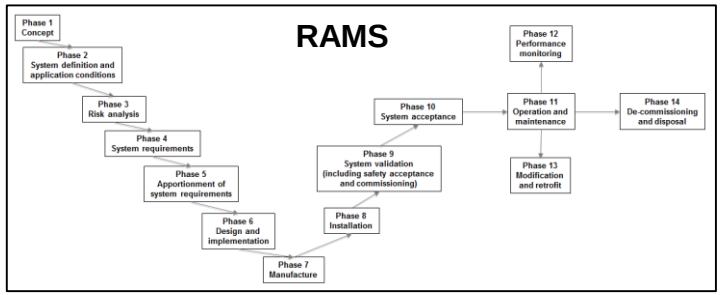
要求事項6.3.5.1-b)項にセーフティケースのリスク許容性基準の記述が入力として必要であることがわかる



セーフティケースとGSNの連携

機能安全規格RAMS適合のアセスメント支援

現状



セーフティケースを作成

セーフティケース

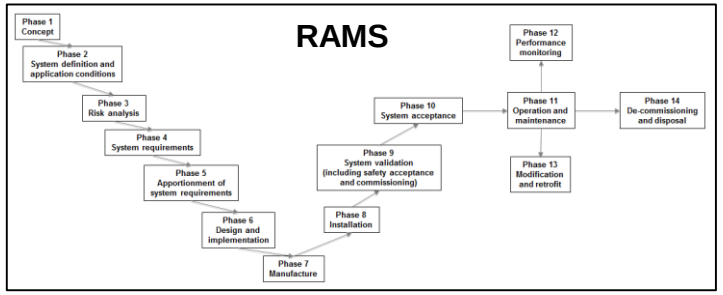
アセスメント

アセサー

セーフティケースの作成支援
GSNに成果物を登録することで、セーフティケースの対応する部分に成果物が登録される。GSNはRAMSに沿って作成されているため、ギャップが小さい。

アセスメント支援
セーフティケースの記述内容をGSNの対応する議論構造を見ることで理解が容易になる

アセスメント



GSNテンプレートに成果物を登録

GSNテンプレート

[ドキュメントA] [項目A]

[ドキュメントB]

連携

セーフティケーステンプレート

○○について△△
- [ドキュメントA] [項目A]
- [ドキュメントB]

本発表での方法

セーフティケースのテンプレート

セーフティケース

⋮

3.3. 安全に関わる組織
- 組織間の体制

- 安全ライフサイクルの組織の担当

- 組織内部について
  - 組織内の体制と担当者

  - 担当とその力量
    - リスク許容性を見直すプロセス
      管理者　　：[ハザードログ：リスク許容性を見直すプロセス管理責任者とその所属]
      実施担当者：[ハザードログ：リスク許容性を見直すプロセス実施担当者とその所属]
    - ハザード特定と分析
      実施担当者：[ハザードログ：ハザード特定と分析実施担当者とその所属]

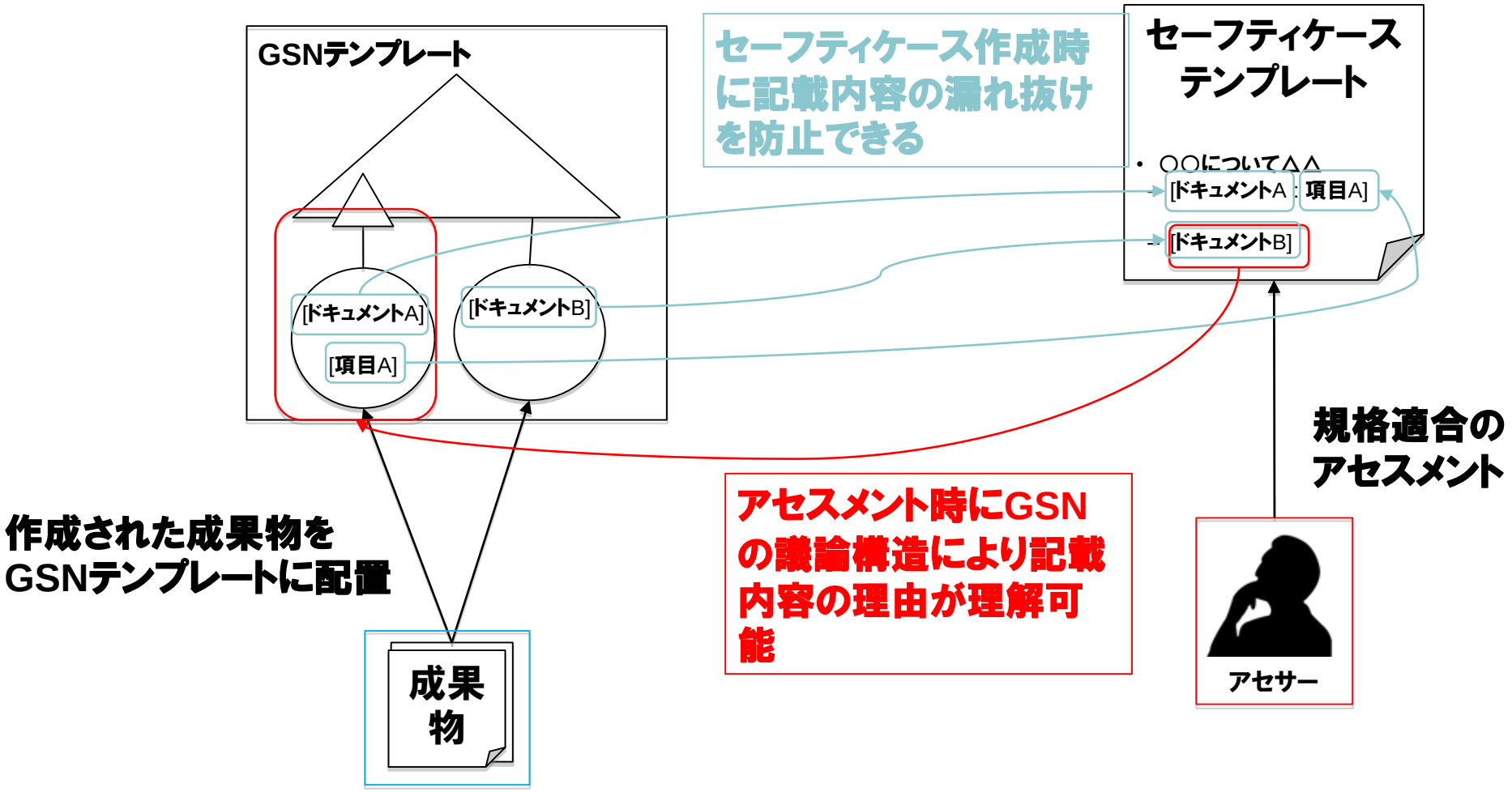
成果物を記述する部分をパラメータとする。
ドキュメントのある部分を示す場合 → [ドキュメント名：記載箇所]
ドキュメント全体をさす場合 → [ドキュメント名：]

3.5[ハザードログ：ハザード管理票]

ID	ハザード	構成部品	ハザードを導くイベント	発生頻度	ハザード発生の結果	深刻度	リスク	リスク許容基準	対応策

⋮

セーフティケースとGSNの連携



GSNとセーフティケースの関連具体例

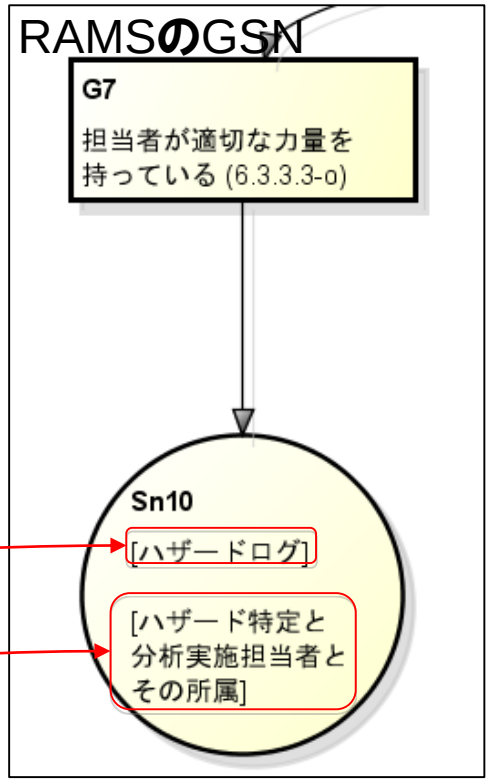
セーフティケース

3.3. 安全に関わる組織
- 組織間の体制

- 安全ライフサイクルの組織の担当

- 組織内部について
  - 組織内の体制と担当者

  - 担当とその力量
    - 管理者　　：[ハザードログ：リスク許容性を見直すプロセス管理責任者]
      実施担当者：[ハザードログ：リスク許容性を見直すプロセス実施担当者]
    - ハザード特定と分析
      実施担当者：[ハザードログ]：[ハザード特定と分析実施担当者とその所属]



セーフティケースを基に評価する際、記載内容がどのような理由(根拠)により記載されているかが明確になる。
GSNテンプレートのソリューションに対応するドキュメント(ドキュメントの一部)を入力することによりセーフティケースの記載内容の漏れ抜けを防ぐことができる

まとめと今後の課題

- **まとめ**
  - GSNで記述することで理解の難しい規格の記述が整理される
    - 目的、要求事項、検証、成果物の対応関係の明確化
    - 参照する事項がコンテキストとして明確化
  - アセスメントのための文書作成支援
    - GSNとセーフティケーステンプレートの連携によるGSNを基にしたセーフティケースの記載内容のチェック
  - 規格適合のアセスメント支援
    - GSNとセーフティケーステンプレートの連携による記載事項の理由の明確化

- **今後の課題**
  - GSNによるトレーサビリティ確保の支援
  - GSNパターンの意味論的枠組み

参考文献

- IEC 62278 / EN 50126(**鉄道アプリケーション- 信頼性・可用性・保安性・安全性の仕様と実証(**RAMS**)**)
Railway applications - The specification and demonstration of Reliability, Availability Maintainability and Safety (RAMS)

- IEC 62279 / EN 50128(**鉄道アプリケーション- 鉄道制御・保安システムのソフトウェア**)
Railway applications - Communications, signaling and processing systems - Software for railway control and protection systems

- IEC 62425 / EN 50129(**鉄道アプリケーション- 保安装置用安全関連電子システム**)
Railway applications - Communications, signaling and processing systems - Safety related electronic systems for signaling

- IEC 62280-1 / EN 50159-1(**鉄道アプリケーション- 通信・保安装置・処理システム- クローズド伝送システムによる安全関連通信**)
Railway applications: Requirements for Safety-Related Communication in Closed Transmission Systems

- IEC 62280-2 / EN 50159-2(**鉄道アプリケーション- 通信・保安装置・処理システム- オープン伝送システムによる安全関連通信**)
Railway applications: Requirements for Safety-Related Communication in Open Transmission Systems

- GSN Community Standard Version 1.0, 2011.