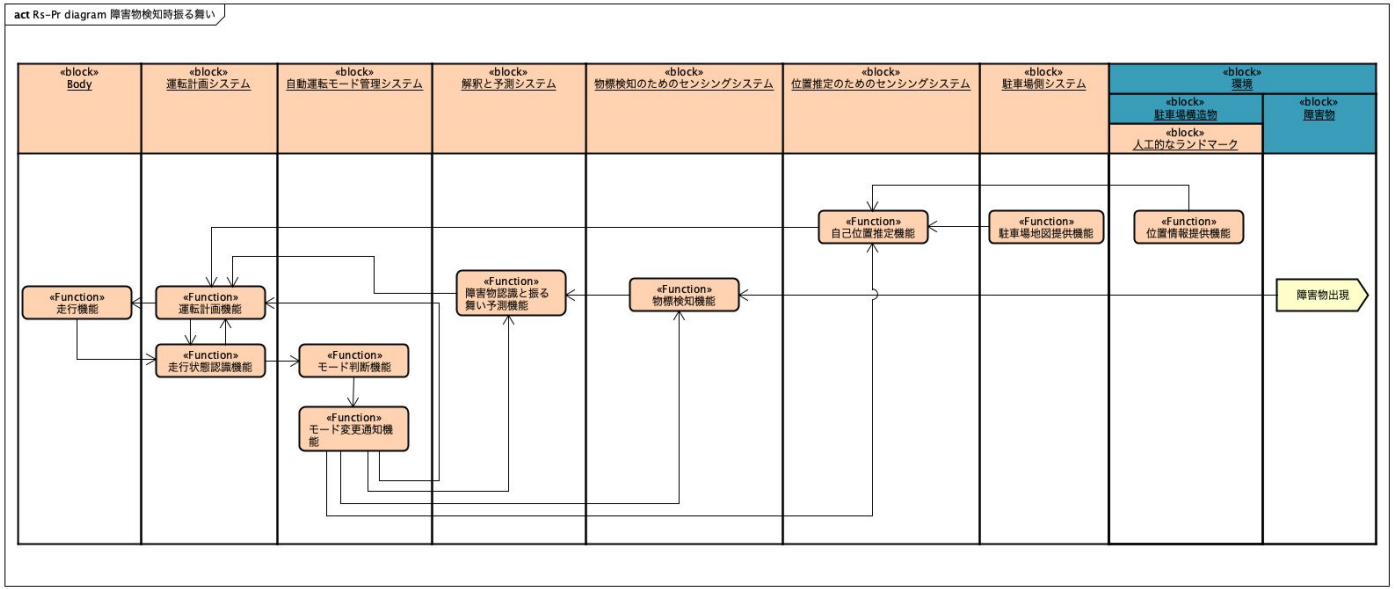
第15回
総合演習2
MBSEによる
アーキテクチャ設計・
アシュアランスケースによる
システム保証

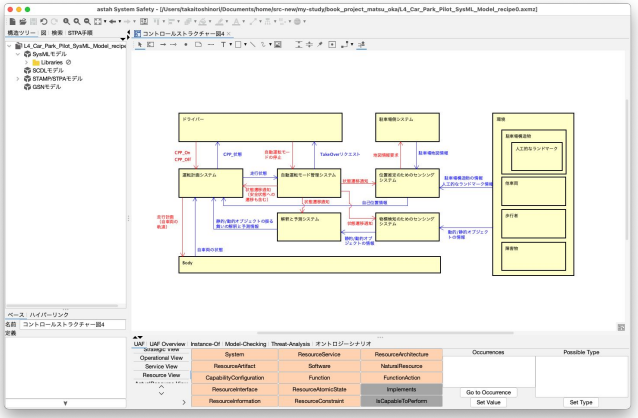
本日のMBSEパートの目標

STAMP/STPAパートで作成したコントロールストラクチャーを利用し
安全なシステムを実現するために必要な機能の抽出を行いましょう



本日の成果物のイメージ

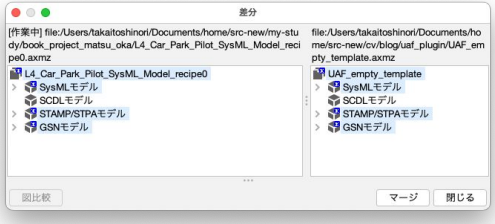
ステップ1: 作成したSTAMP/STPAファイルとUAFテンプレートファイルとのマージ



作成したSTAMP/STPAのファイル

1. メニューの「ファイル」から「プロジェクトの比較とマージ」を選んでください

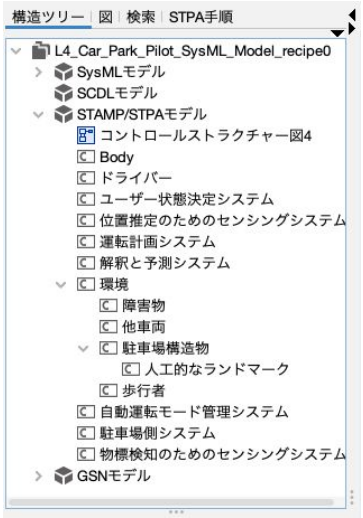
2. 対象ファイルとして「 UAF_empty_template.axmz」を選んでください
3. この画面



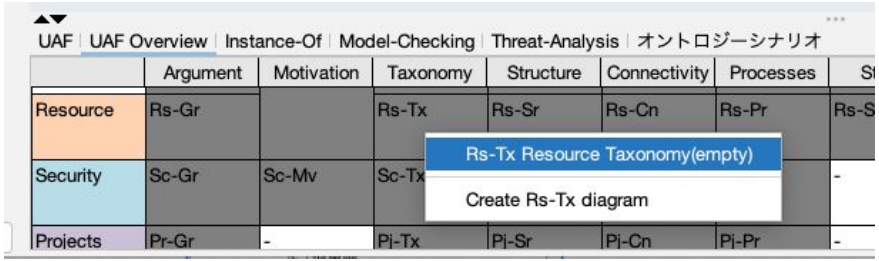
がでたら「マージ」を押してください（次に聞かれる優先順位はそのままで構いません）

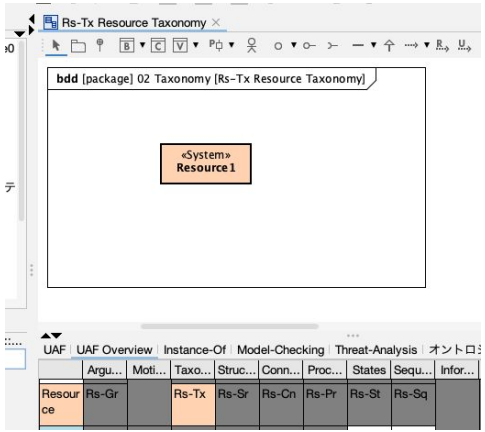
ステップ2：STAMP/STPAモデルの再利用（準備1）

1. 構造ツリーからコントロールストラクチャーのコンポーネントを表示してください（入れ子のものもぜんぶ展開してください）



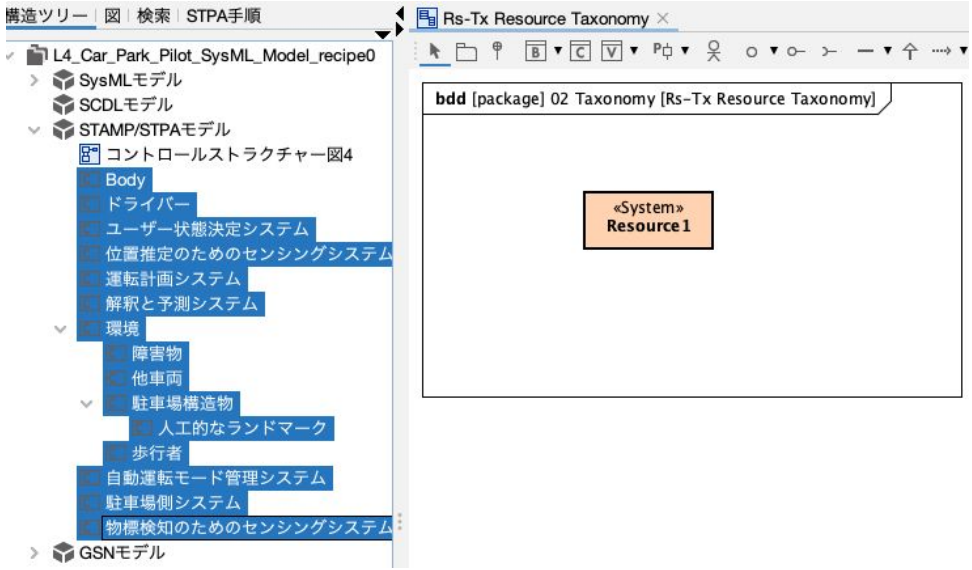
2. Rs-Tx Resource Taxonomy(empty)を開いて図の名前をRs-Tx Resource Taxonomyに変更してください



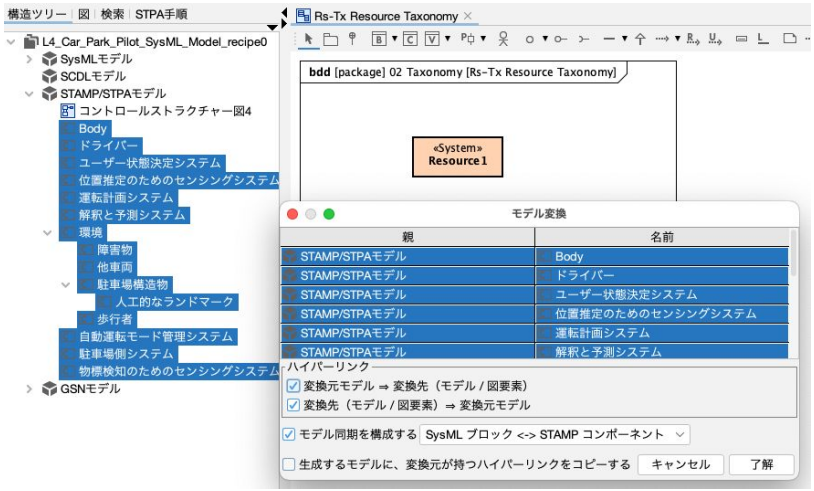


ステップ3：STAMP/STPAモデルの再利用（準備2）

1. 構造ツリーからSTAMP/STPAモデル内のコンポーネントを全部選択してください

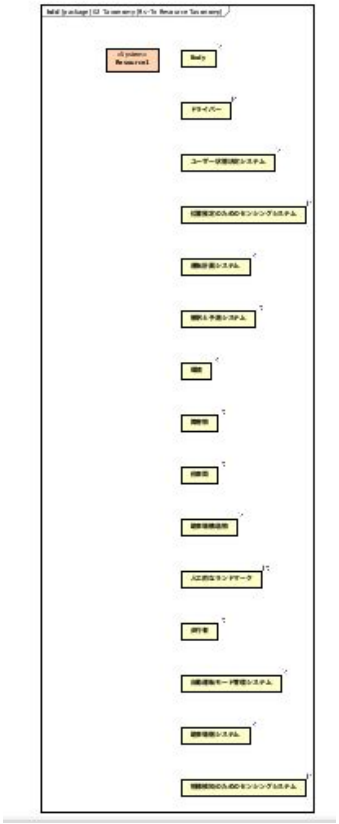


1. そのままマウスでRs-Tx Resource Taxonomyの図上へドラッグ＆ドロップしてください



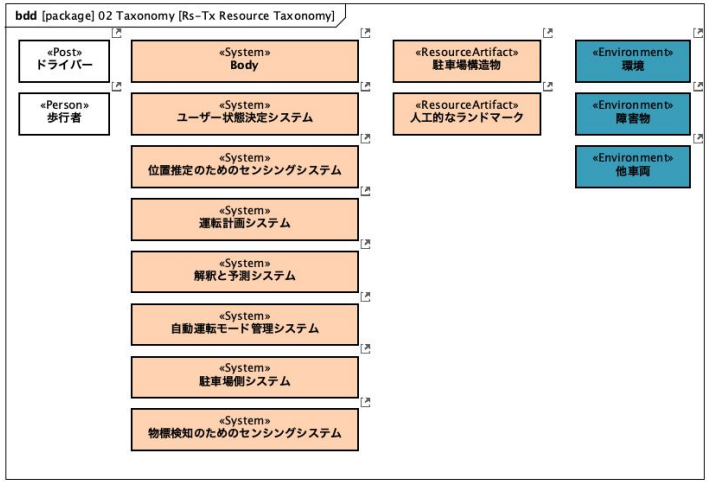
ここで、オプションは上記の通りとして、了解を押してください

ステップ4：STAMP/STPAモデルの再利用（準備3）



このような図が得られていると思います

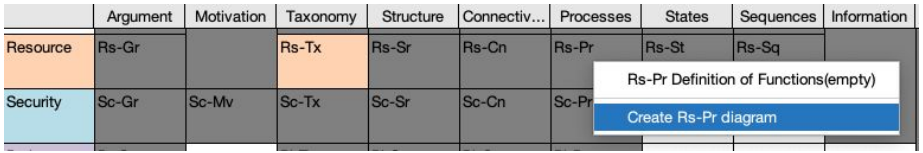
UAFで用意されている概念を用いて
整理してください



Post, Person ← Personnel Viewにあります
System, Resource Artifact ← Resource Viewにあります
Environment ← Parametersにあります

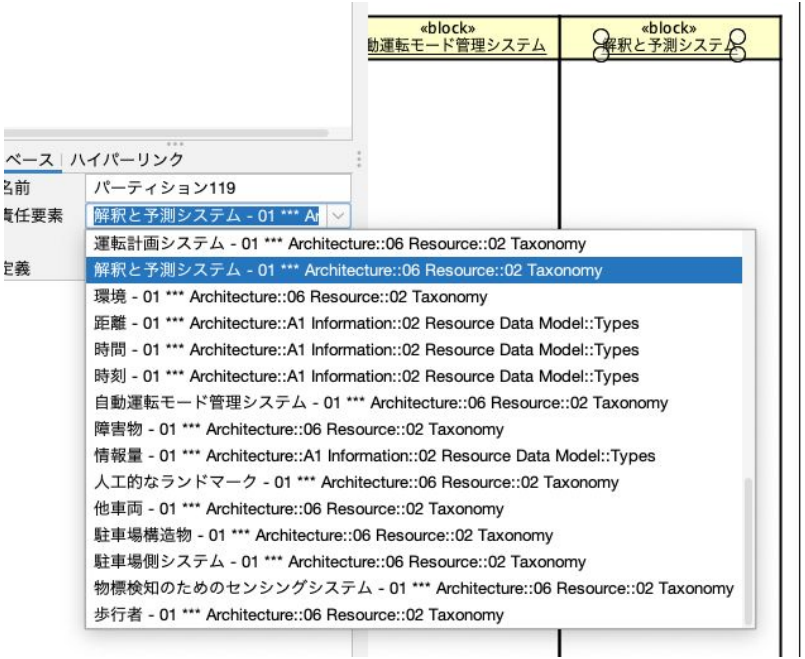
ステップ5：振る舞いモデルの作成を通じた機能の抽出（1）

1. Rs-Prのセルから「Create Rs-Pr diagram」を選んでください



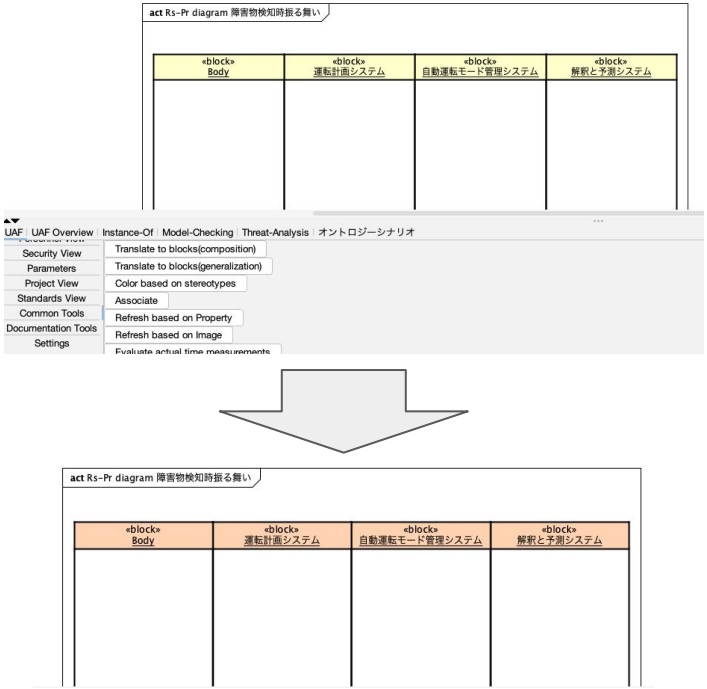
2. 「Rs-Pr 障害物発見時の振る舞い」など、STAMP/STPAで分析したシナリオの名前などを付けてください

パーティションを準備します。パーティションの型を設定してください

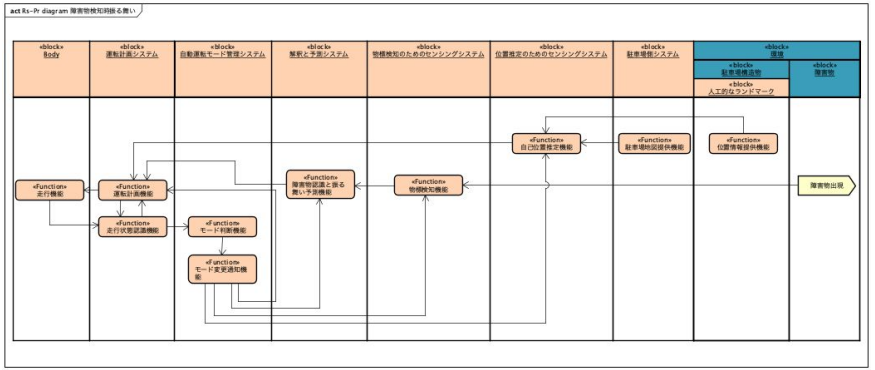


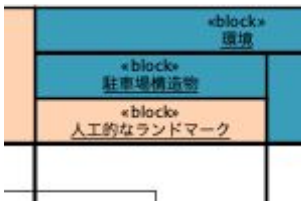
ステップ5：振る舞いモデルの作成を通じた機能の抽出（2）

1. 型を設定されたパーティションは、Common ToolsタブのColor based on stereotypesボタンを押すと型に応じた色を付けてくれます。

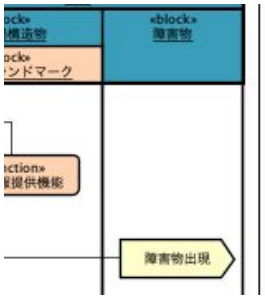


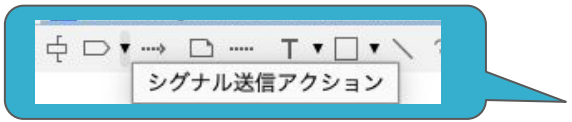
2. 記述したいシナリオに必要な機能を定義していく





パーティションは階層化できます





機能ではない、環境からの情報発信などは、シグナル送信アクションが使えます

MBSEパート補足

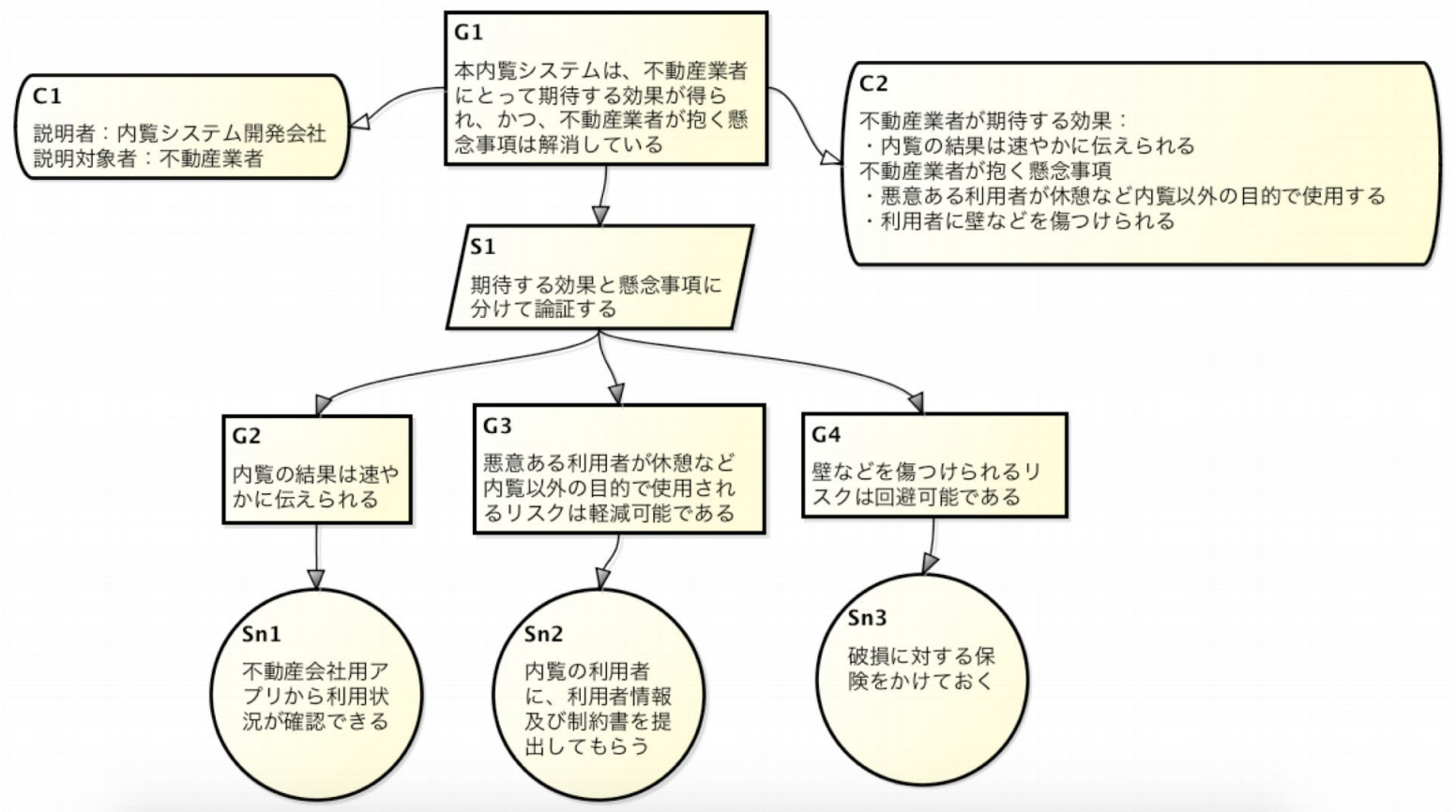
今回は、安全なシステムを実現するために必要な機能の抽出という目的のためにモデルを記述しました

- 機能の抽出は、今回記述したプロセスのモデルだけでなく、状態のモデルややりとりされる情報のモデルなどを記述したり、それらに基づいてシミュレーションしたりしながら妥当性を確認する必要があります
- さらには、安全性という観点だけでなく、戦略やオペレーションなど他の様々な観点もモデル化しながら最終的な機能を確定していきます
- MBSEでは、それら多くの観点から見て検討したソリューションが満足するものであることを客観的に説明するためのエビデンスを提供します

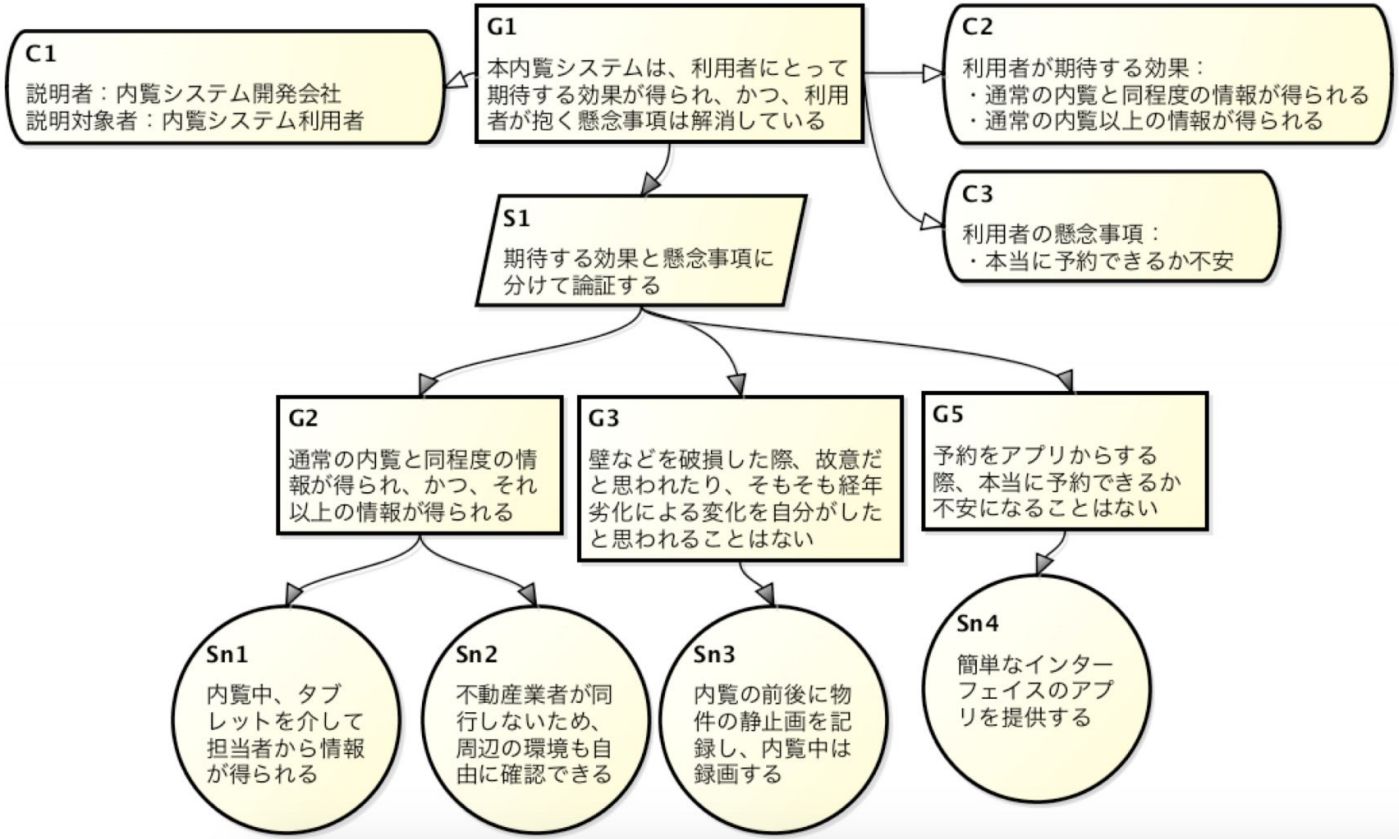
アシュアランスケースによるシステム保証

- 演習1ステークホルダーの分析
  - このシステムにどのようなステークホルダがいるか、挙げてみよう
- 演習2　前提とトップゴールの設定
  - 今回は、開発企業とシステムの安全性認証者（アセッサー）間の合意形成にする
  - 安全性に関するトップゴールにする
  - 必要十分な前提をトップゴールにつけよう
- 演習3　サブゴールへの分割
  - トップゴールの分割が最も大事
  - 分割の例
    - システムの構造による分割
    - システムのプロセスによる分割
    - システムの要求による分割
    - システムのハザードによる分割

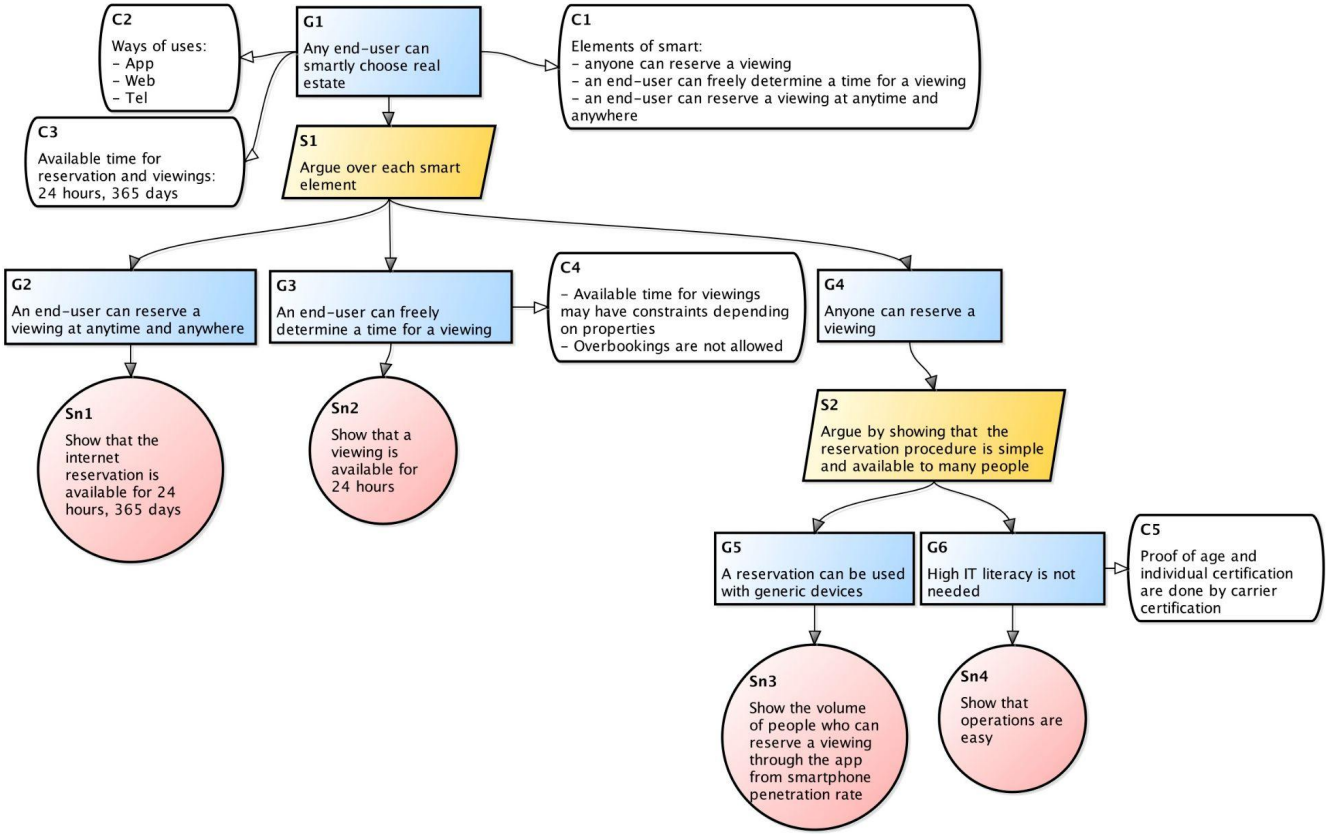
13回目の演習解答例1



13回目の演習解答例 2

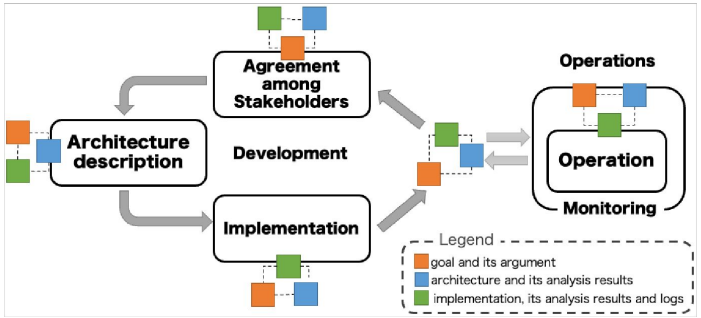


13回目の演習の解答例

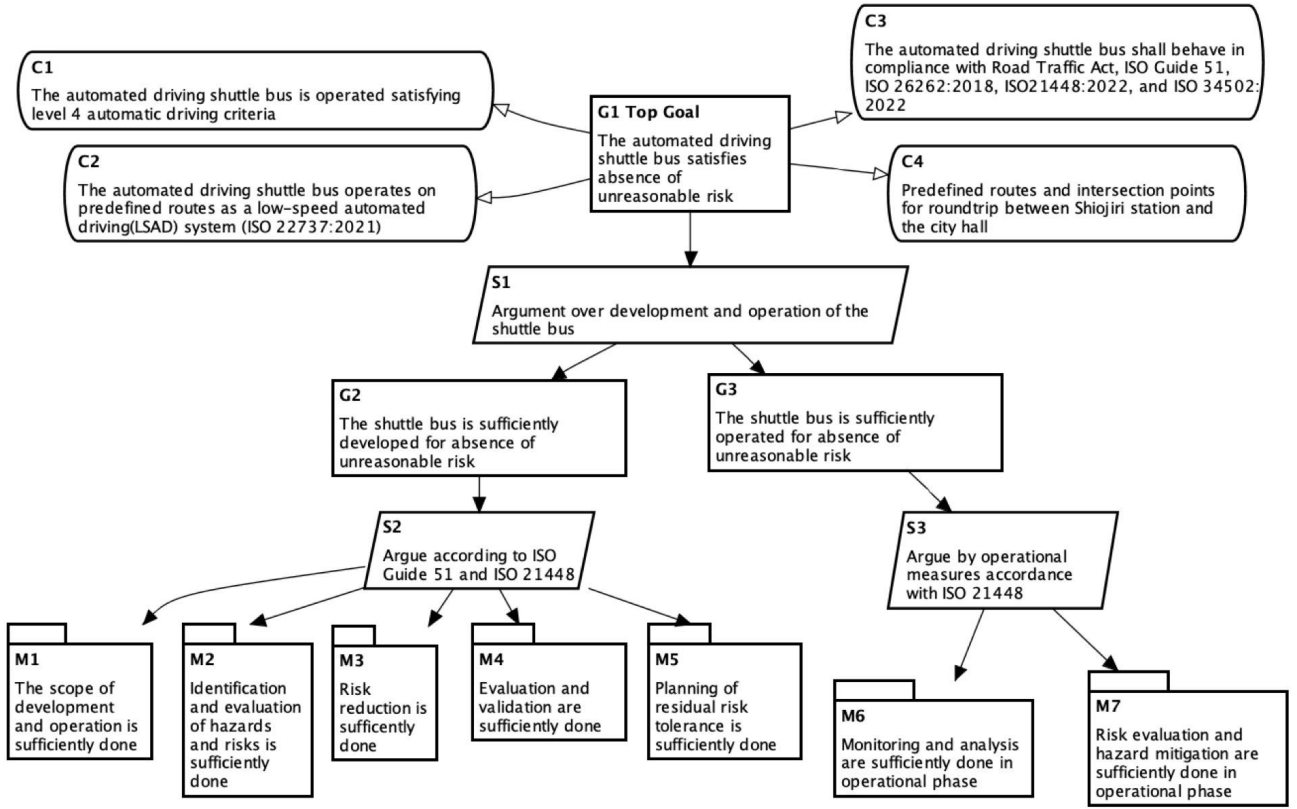


A Case Study of Continuous Assurance Argument for Level 4 Automatic Driving

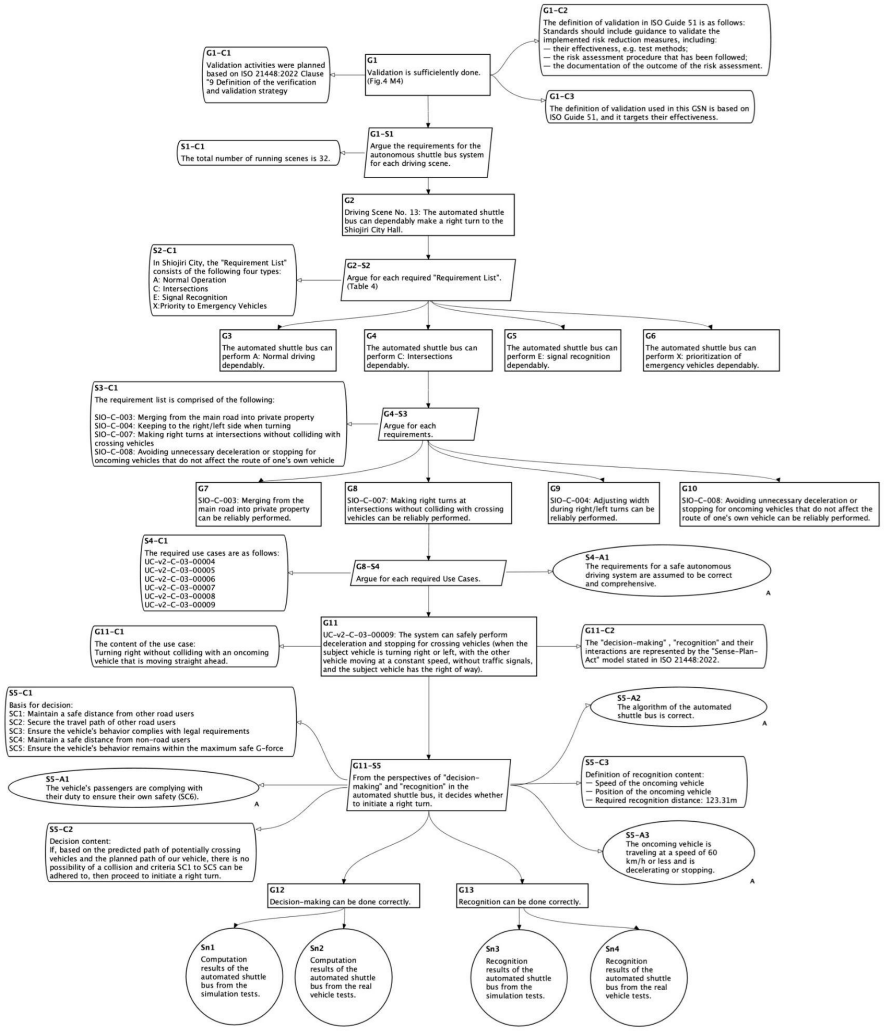
- レベル4自動運転システムをオープンシステムととらえ、ディペンダビリティを継続的に保証するための枠組みを提案
- 塩尻駅から塩尻市庁舎の周回コース(2km)の、特に市役所へ入るための右折にフォーカスし、STAMP/STPAの分析結果などをもとにD-Caseを記述試行
- 市庁舎の屋上に設置されたモニタリングシステムから対向車の速度をモニタリングし、D-Caseで前提として記述されている対向車速度を超えていないかチェックできるようなプロトタイプのツール連携を実装



自動運転システムのGSN: トップレベル



自動運転システムのGSN:
市庁舎へ入る右折に
関する議論



本授業の内容のまとめ

- 信頼性の概念
  - ディペンダビリティ、安全性、セキュリティ、 …
- 安全性、セキュリティ分析手法
  - FTA, FMEAなどの従来の安全分析手法
  - STAMP/STPAによる安全、セキュリティ分析
- モデルベースシステムズエンジニアリング(MBSE)
- アシュアランスケースによるシステム保証
  - Goal Structuring Notation (GSN)
  - D-Case手法