自動車の運転支援システムを想定したアシュアランスケース(D-Case)記述演習

2014年 12月 19日

柿本 和希
高井利憲

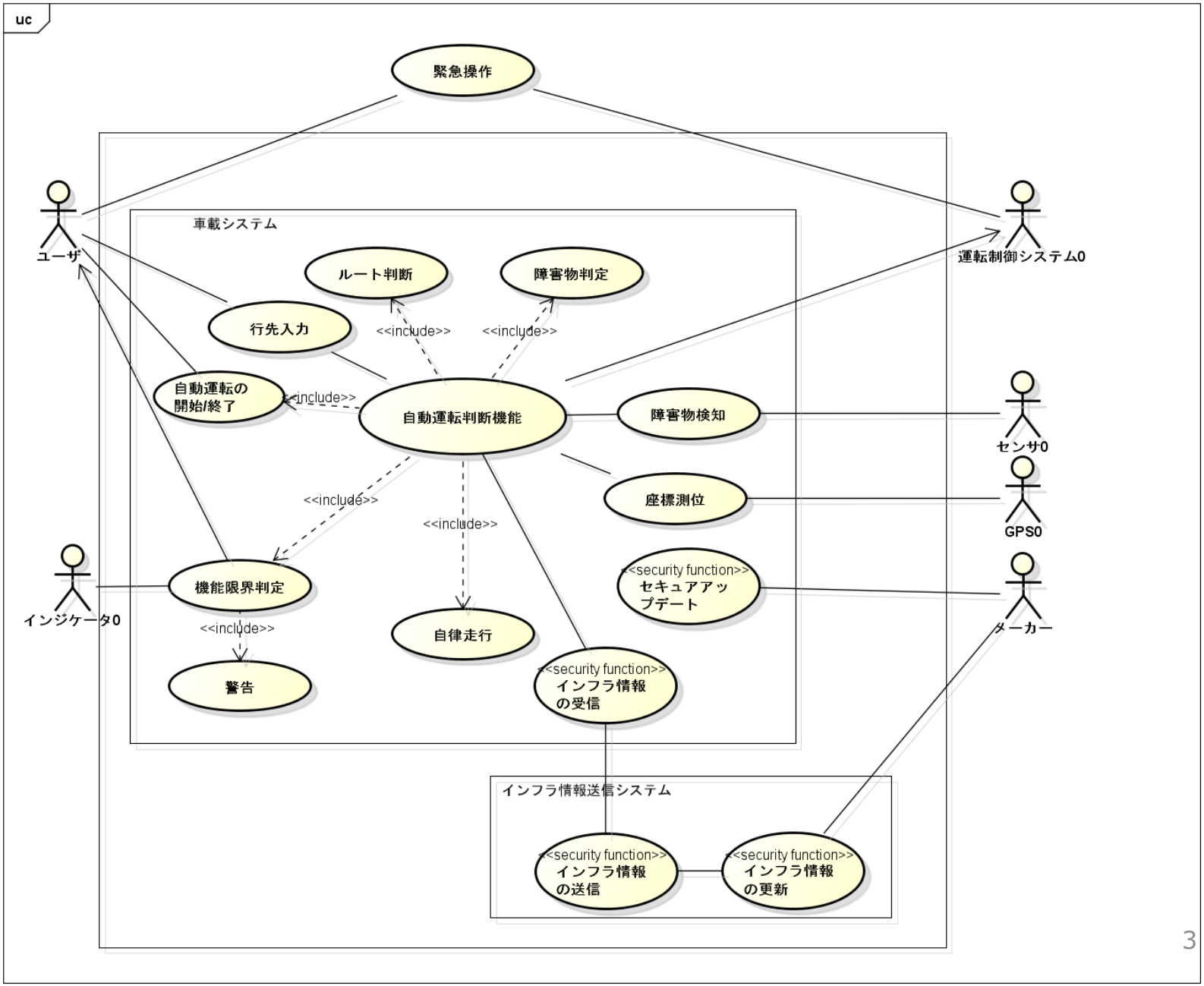
奈良先端科学技術大学院大学 情報科学研究科

対象システムの概要

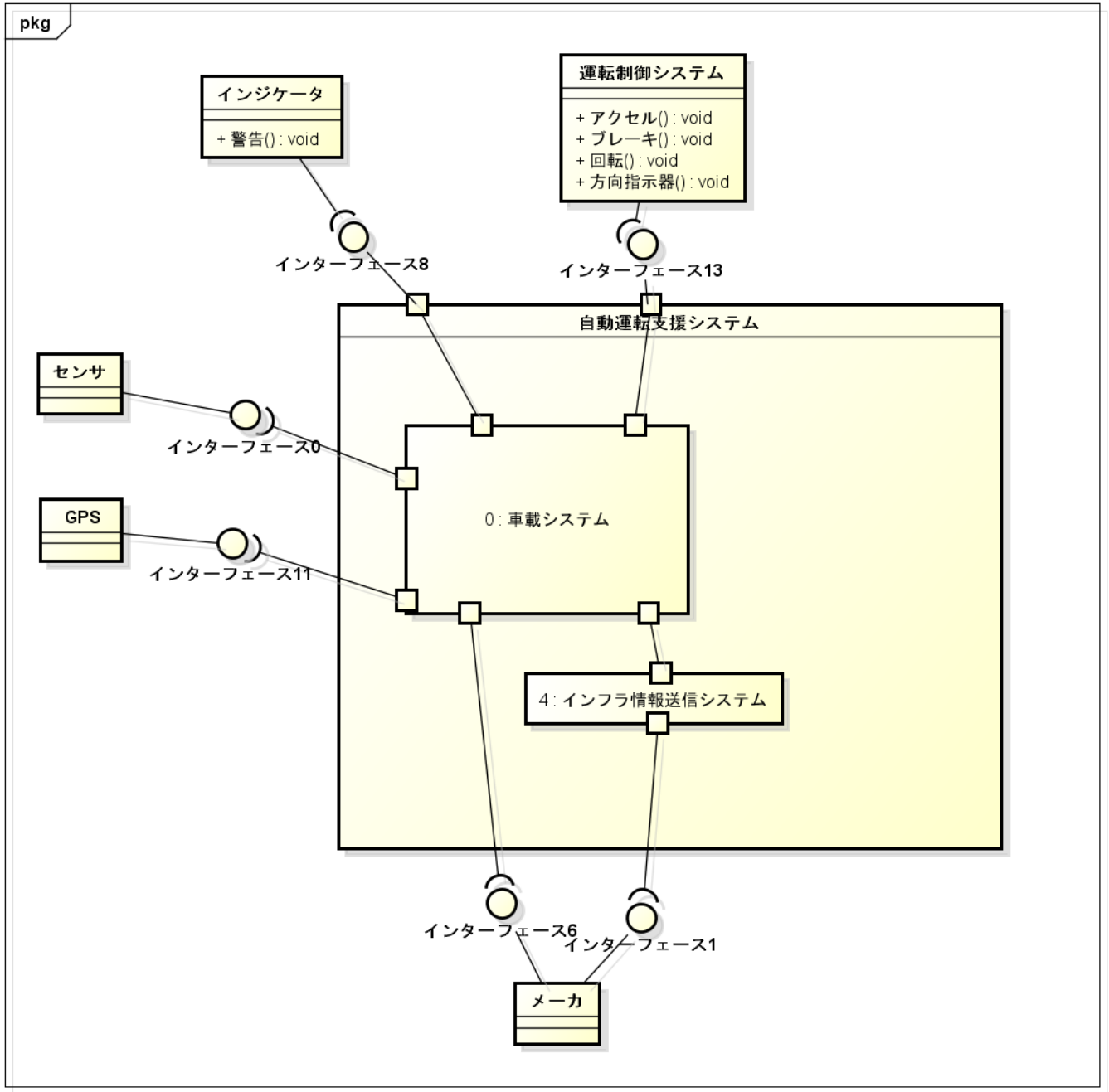
- 高速道路上での、自動運転を支援するシステム
  - 高速道路上に設置されたインフラ情報送信システムから、インフラ情報を受け取る。
  - インフラ情報には、位置情報、道路の角度、事故情報などが含まれる。

- 高速道路入口から、目的の出口まで基本的に自律走行が可能
  - 機能限界に至った場合、それを検知してドライバーへの警告と運転の引継ぎが行われる。
  - 機能限界には、天候などによるセンサの不調や、事故や工事などによる道路状況の変化などを想定している。

対象システム概要


uc
緊急操作
車載システム
ユーザ
運転制御システム0
ルート判断
障害物判定
行先入力
<<include>>
<<include>>
自動運転の
開始/終了
<<include>>
自動運転判断機能
障害物検知
センサ0
座標測位
GPS0
<<include>>
<<include>>
インジケータ0
機能限界判定
<<security function>>
セキュアアッ
プデート
メーカー
<<include>>
自律走行
警告
<<security function>>
インフラ情報
の受信
インフラ情報送信システム
<<security function>>
インフラ情報
の送信
<<security function>>
インフラ情報
の更新

対象システムの構成


pkg
インジケータ
+ 警告() : void
運転制御システム
+ アクセル() : void
+ ブレーキ() : void
+ 回転() : void
+ 方向指示器() : void
インターフェース8
インターフェース13
自動運転支援システム
センサ
インターフェース0
GPS
インターフェース11
0 : 車載システム
4 : インフラ情報送信システム
インターフェース6
インターフェース1
メーカ

初期ハザード分析

- HAZOP
  - 危険シナリオ分析手法の一つ
  - 設計仕様からの逸脱に対して発生するハザードと、その原因を解析する手法

- 機能ごとにシステムパラメータとガイドワードを用いて分析を行った
  - システムパラメータ（道路状態、加速、減速、開始など16個）
  - ガイドワード（まったく～しない、強く/弱く、ずっと/短くなど14個）

- 7の機能に対して、17のハザードを識別

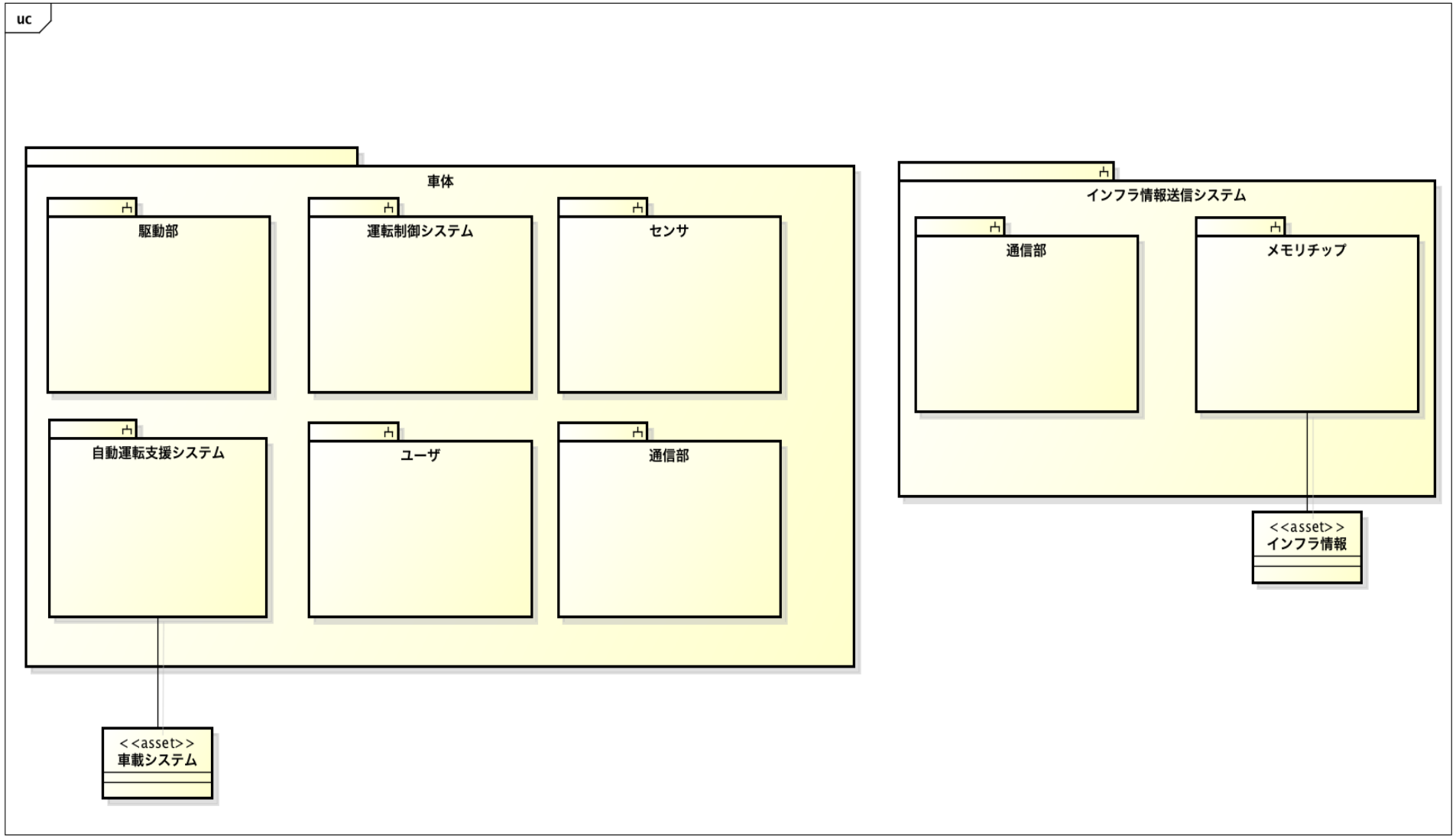
ハザード例

- 不正なインフラ情報を取得する
  - 機能: インフラ情報の受信
  - 影響: 破局的
  - 属性: 攻撃確率 Enhanced Basic

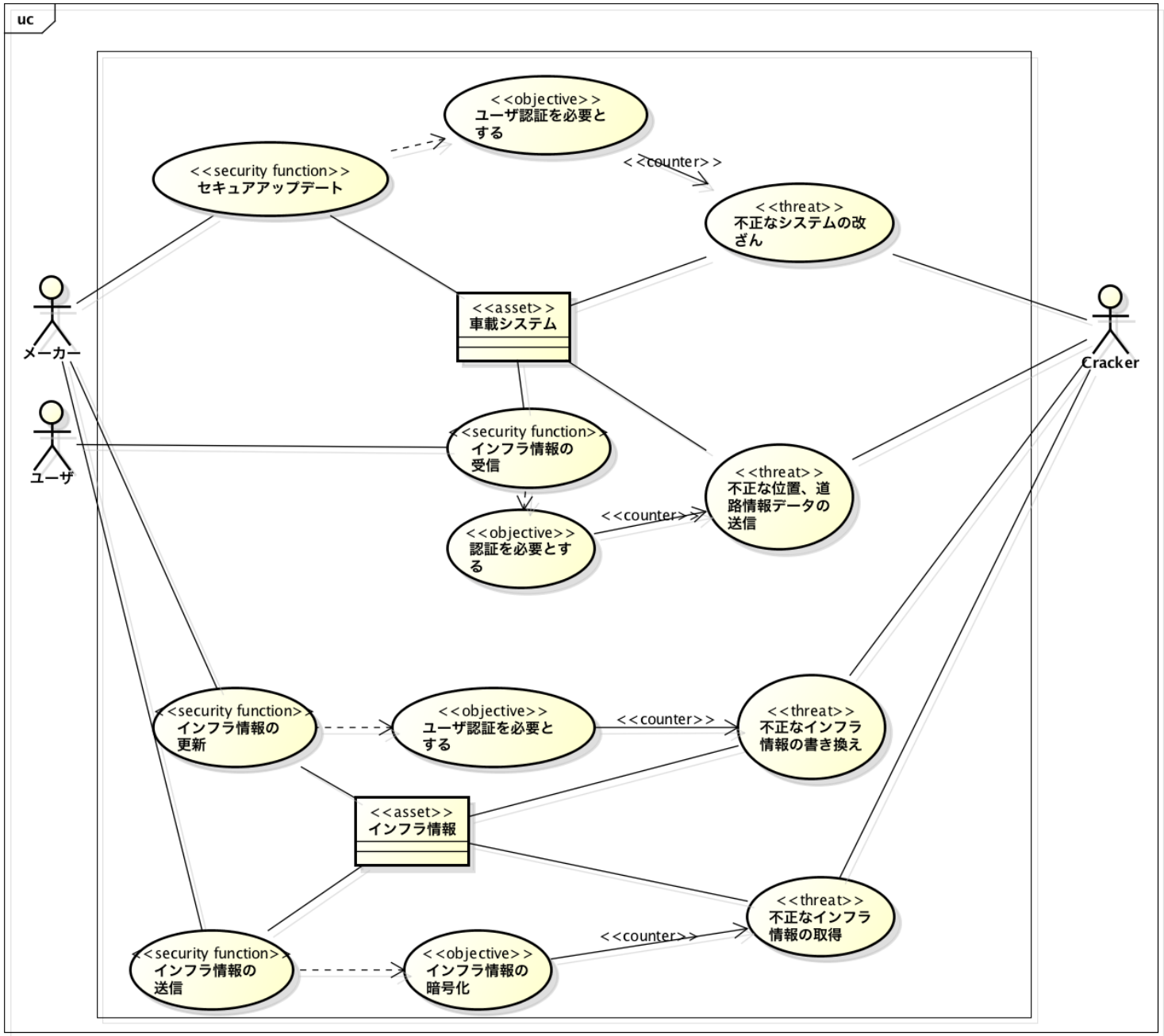
- 意図しない自動運転の開始/終了
  - 機能: 自動運転の開始/終了
  - 影響: 大
  - 属性: C2 通常の方法で制御可能

- 運転の引継ぎに対してドライバーが応じない
  - 機能: 機能限界判定
  - 影響: 中
  - 属性: C1 簡単に制御可能

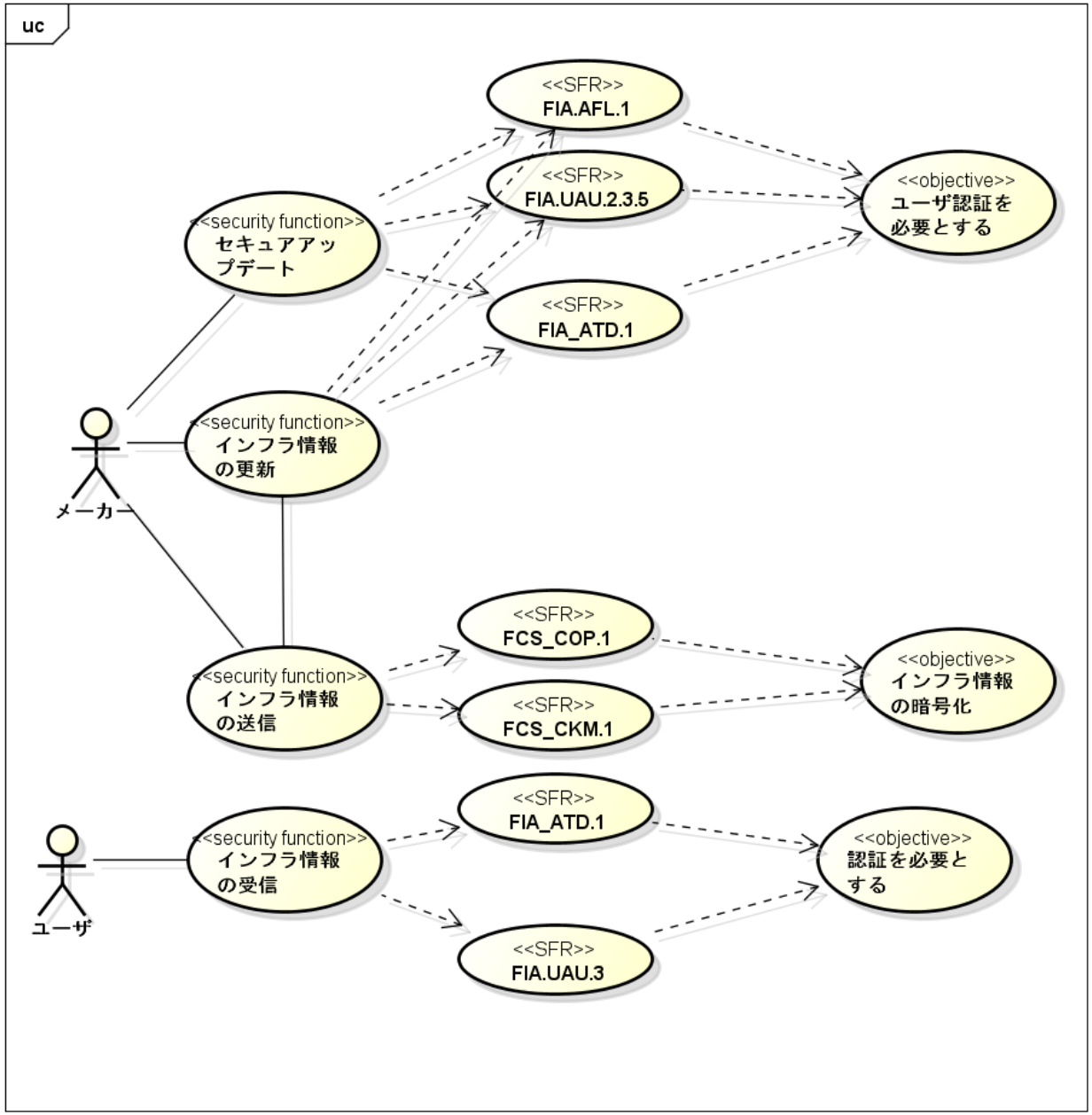
配置図


uc
車体
駆動部
運転制御システム
センサ
自動運転支援システム
ユーザ
通信部
<<asset>>
車載システム
インフラ情報送信システム
通信部
メモリチップ
<<asset>>
インフラ情報

ミスユースケース


uc
<<objective>>
ユーザ認証を必要とする
<<security function>>
セキュアアップデート
<<counter>>
<<threat>>
不正なシステムの改ざん
メーカー
<<asset>>
車載システム
Cracker
ユーザ
<<security function>>
インフラ情報の受信
<<threat>>
不正な位置、道路情報データの送信
<<objective>>
認証を必要とする
<<counter>>
<<security function>>
インフラ情報の更新
<<objective>>
ユーザ認証を必要とする
<<counter>>
<<threat>>
不正なインフラ情報の書き換え
<<asset>>
インフラ情報
<<threat>>
不正なインフラ情報の取得
<<security function>>
インフラ情報の送信
<<objective>>
インフラ情報の暗号化
<<counter>>

ハザードへの対応（セキュリティ）

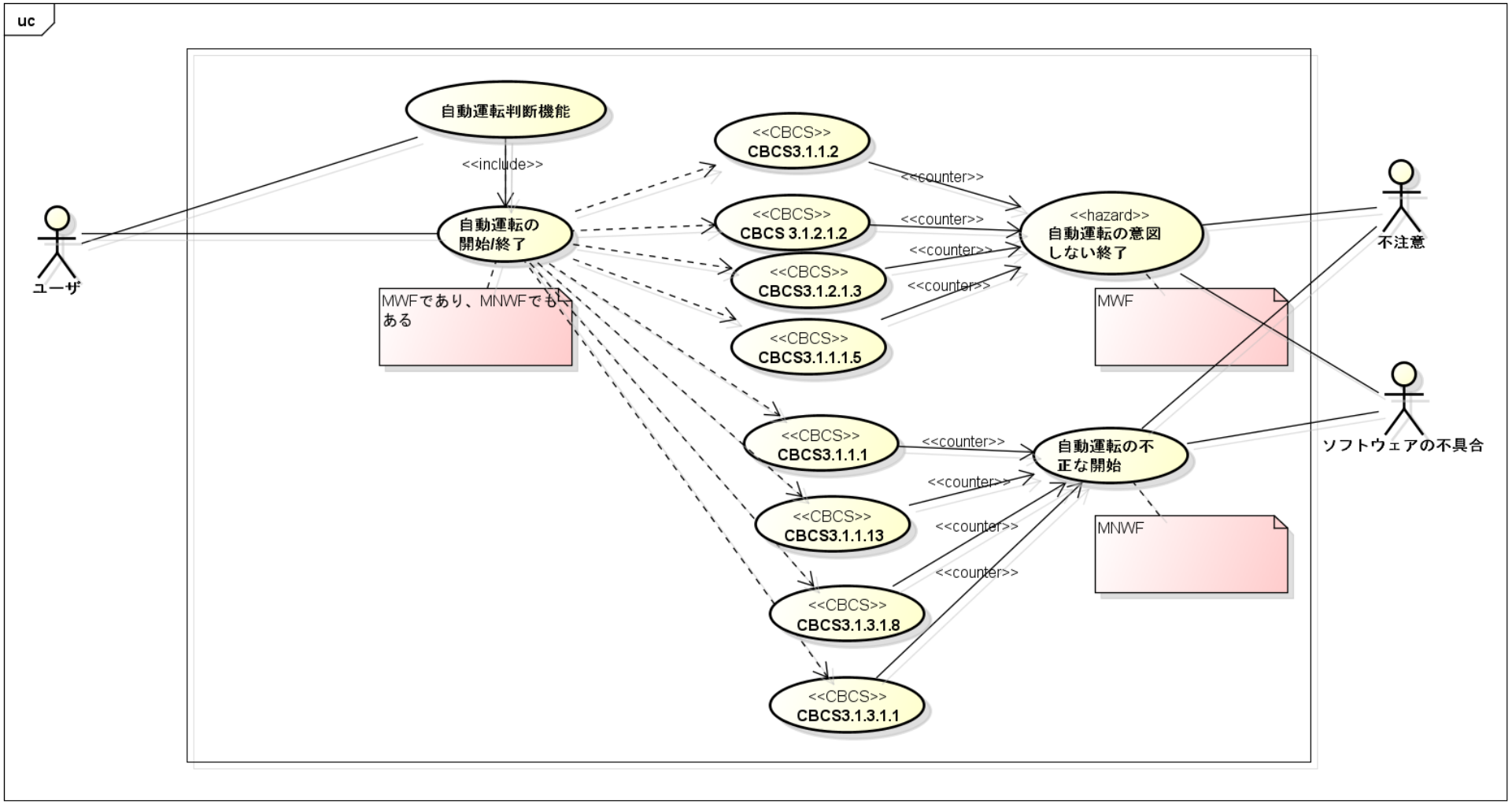


CBCS安全要求

- Computer based control system 安全要求
  - ISS建造にあたり、NASA が定めた安全要求の一つ
  - コンピュータによってハザードを制御するシステムにおいて、安全設計を行うための要求

- 一般要求（全てのCBCS設計で満たされるべき要求）
- MWF要求
  - MWF: 安全を確保するため、その機能が動作し続けなければならない機能
- MNWF要求
  - MNWF：安全を確保するため、その機能が動作してはいけない機能

CBCS対応ミスユースケース



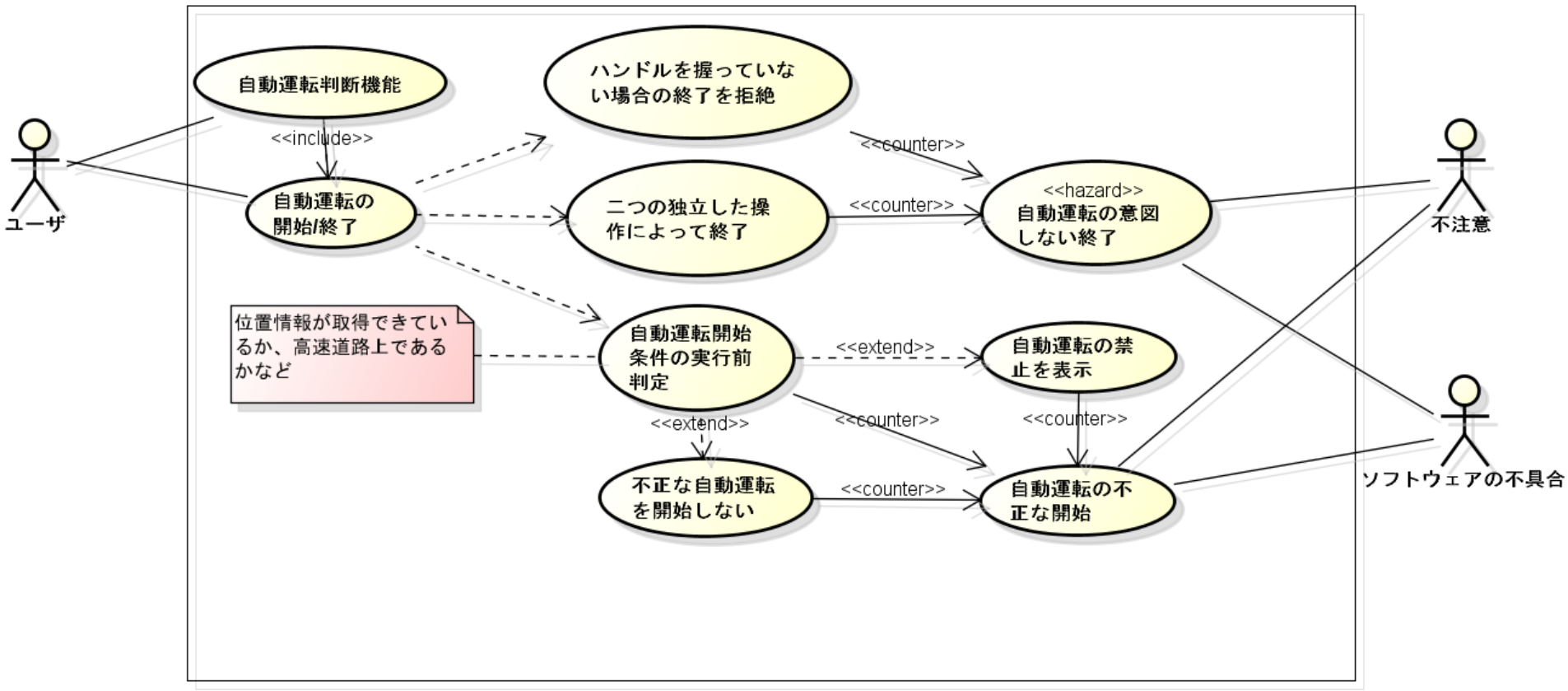
CBCS: 自動運転の意図しない終了

- CBCS3.1.1.2
  - The CBCS shall perform an orderly shut down of a function to a known, safe state upon receipt of a termination command or detection of a termination condition.
- CBCS3.1.2.1.2
  - Where loss of a capability could result in a critical hazard the CBCS shall provide two independent and unique command messages to deactivate the capability.
- CBCS3.1.2.1.3
  - At least one independent operator action shall be required for each operator initiated command messages used in the shutdown of a capability or function that could lead to a hazard.
- CBCS3.1.2.1.5
  - Alternate or redundant functional paths shall be separate or protected such that any single credible event which causes the loss of one functional path will not result in the loss of the redundant functional path.

CBCS: 自動運転の不正な開始

- CBCS3.1.1.1
  - The CBCS shall safely initialize to a known, safe state.
- CBCS3.1.1.13
  - The CBCS shall reject hazardous commands which do not meet prerequisite checks for execution.
- CBCS3.1.3.1.1
  - The CBCS shall perform prerequisite checks for the safe execution of hazardous commands.
- CBCS3.1.3.1.8
  - A CBCS shall make available to the crew or ground operators the status of software inhibits used to disable the execution of hazardous commands.

ハザードへの対応


自動運転判断機能
ハンドルを握っていない場合の終了を拒絶
<<include>>
<<counter>>
ユーザ
自動運転の開始/終了
二つの独立した操作によって終了
<<counter>>
<<hazard>>
自動運転の意図しない終了
不注意
位置情報が取得できているか、高速道路上であるかなど
自動運転開始条件の実行前判定
<<extend>>
自動運転の禁止を表示
<<extend>>
<<counter>>
<<counter>>
不正な自動運転を開始しない
<<counter>>
自動運転の不正な開始
ソフトウェアの不具合

アシュアランスケース概要

- トップゴール
  - 自動運転中における、開発側の責任となるような事件・事故のリスクは許容範囲内である
- トップゴールのコンテキスト
  - 具体的な法整備が進んでいない
  - 高速道路での支援を想定する
  - システムは現在、設計段階である
- ノード数
  - 40～
  - 最終的には50前後の見込み

アシュアランスケース: 戦略の例

- ハザード分析において作成した、図や表に沿った戦略
  - コンテキストとして、作成した図へのリンクを作成

- セキュリティに関するゴールと、セーフティに関するゴールに分ける
  - セキュリティに関するハザードを CC を用いて、
    それ以外はCBCSを用いて保証したため
- 車体搭載部分とインフラ部分にわける
  - 配置図から
- 機能ごとにわける
  - HAZOP
- ハザード、または脅威ごとに分ける
  - ミスユースケース

今後の展開予定

- まだ分析していないハザード（セーフティ）への対応
  - CBCS安全要求への対応付け
  - 設計の詳細化