ハザード，リスクの分類と
機能安全，SOTIFが対象とする範囲
－自動運転、AIを通して－

2021年 12月 3日（金）

第104回 セーフティーネットワークジャパン定例会

日本信頼性学会　要素技術安全研究会

主査　川島　興

（オリエンタルモーター株式会社）

自己紹介　川島　興　（かわしま　こう）

オリエンタルモーター株式会社
技術開発本部　安全規格部　部長
EMC試験センター所長

- 日本信頼性学会　要素技術安全研究会　主査
  （機能安全規格等の調査研究）

IEC/TC 65/SC 65A/MT 61508 国内委員
IEC/TC 56 Dependability　エキスパート

佐藤吉信先生（元東京海洋大学教授，（公財）医療の質向上研究所・研究員）とともに
ハザード及びリスクの観点から機能安全規格等を調査研究し，
研究成果を国際規格に反映する活動に取組む

日本信頼性学会
RELIABILITY ENGINEERING ASSOCIATION OF JAPAN

要素技術安全研究会

機能安全に関連する規格，法規制及び技術動向を研究し，
適切な機能安全の適用に資する.

研究会：年5回開催

- 機能安全に関連した国際規格，国内の法令等の動向
  および要求事項の調査，国際規格への反映
- 安全に関するトッピックスのディスカッション

ハザード，リスクの分類と，機能安全，SOTIFが対象とする範囲

自動車，ロボットなどの自動運転と，それらへのAI導入は今後の社会に不可欠．

安全な自動運転のために，

- （危険側）故障，危険な機能不全 ･･･ **機能安全**で対応
- 安全関連系が故障せずとも（システムが正常でも）
  意図した安全機能では対処できない事象 ･･･ **SOTIF**で対応

自動運転，AI技術によるハザード及びリスクを
予見性と安全性能限界との関係によって分類することで，

機能安全，SOTIF規格の対象範囲の違いを整理する

本日の内容

1. はじめに （機能安全規格と意図する運用環境）

2. 開いた運用環境のシステムー自動運転車

3.AIを実装したシステムの安全確保

4.安全機能性能の範囲とハザードの予見性によるハザードの分類

5.安全機能性能・ハザード・リスク源の予見性に基づくリスクの分類

5. まとめ　機能安全とSOTIFの適用範囲

6. 事故事例

1. はじめに

機能安全規格

基本安全規格　**IEC 61508**

Functional safety of electrical/electronic/programmable electronic safety-related systems

電気・電子・プログラマブル電子（E/E/PE）安全関連系の機能安全

フレームワーク

①全安全ライフサイクルにわたる機能安全マネジメントシステムに沿った活動

②定量的な安全性能に関する要求事項に適合させる活動

意図する運用環境でのEUC（被制御機器）に起因するハザードを同定，ハザードを制御（抑制）する安全関連系の安全機能を特定、安全機能の遂行に必要な安全度水準（SIL 1～4）を決定し，それに応じた要求事項に適合することで機能安全を確保する.

1. はじめに

機能安全規格

- 自動車分野の機能安全規格

ISO 26262 Road vehicles — Functional safety

IEC 61508を基本安全規格として自動車分野向けに作られた

「機能安全」の定義

IEC 61508-4 3.1.12

EUC 及びEUC 制御系の全体に関する安全のうち，E/E/PE安全関連系及び他リスク軽減措置の正常な機能に依存する部分.

ISO 26262-1 3.67

absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems

多くの機能安全規格が意図する運用環境

もともと機能安全規格は，

安全計装システム，産業機械などが主な対象

IEC 61511　　プロセス産業の安全計装システム
IEC 62061　　機械類の安全関連制御システム

そこから様々な製品規格に展開・引用

ISO 10218　　産業用ロボット
IEC 61800-5-2　モータの可変速駆動システム
IEC 61326-3-1　計測用，制御用及び試験室用の電気装置
IEC 62282-3-100　定置用燃料電池発電システム　　ほか

ISO 13482　　生活支援ロボット
ISO 26262　　自動車

多くの機能安全規格が意図する運用環境

もともと機能安全規格は，

安全計装システム，産業機械などが主な対象

IEC 61511	プロセス産業の安全計装システム
IEC 62061	機械類の安全関連制御システム

そこから様々な製品規格に展開・引用

ISO 10218	産業用ロボット
IEC 61800-5-2	モータの可変速駆動システム
IEC 61326-3-1	計測用，制御用及び試験室用の電気装置
IEC 62282-3-100	定置用燃料電池発電システム　　ほか

ISO 13482	生活支援ロボット
ISO 26262	自動車

あらかじめ定義され，制限された運用環境

・訓練／許可された人だけが入れるエリア：安全柵内

・建屋内／試験室内／筐体内など管理された環境条件下

多くの機能安全規格が意図する運用環境

閉じた運用環境（あらかじめ定義され，制限された運用環境）

ex：・訓練/許可された人だけが立ち入れるエリア内・安全柵内
　　・建屋内/試験室内/筐体内など管理された環境条件下　　など

－ ハザードの大部分が同定でき（想定外のハザードは固有（本質）安全原則等で排除）

－ それらハザードに対して十分な安全性能を持つ安全関連系を構成できる
（安全性能の限界内で運用する）

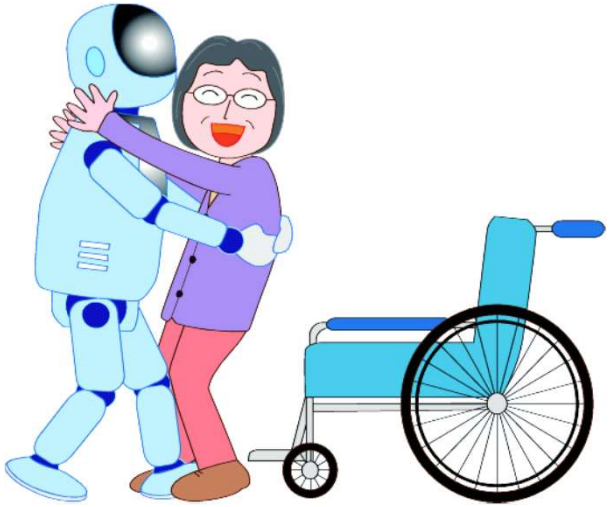
機能安全規格は，

運用環境が閉じたシステムにおける，
安全関連系の安全性能限界内のハザード・リスクへの適用を意図，
といえる．

（IEC 61508を基本安全規格として自動車分野向けに作られたISO 26262も同様）

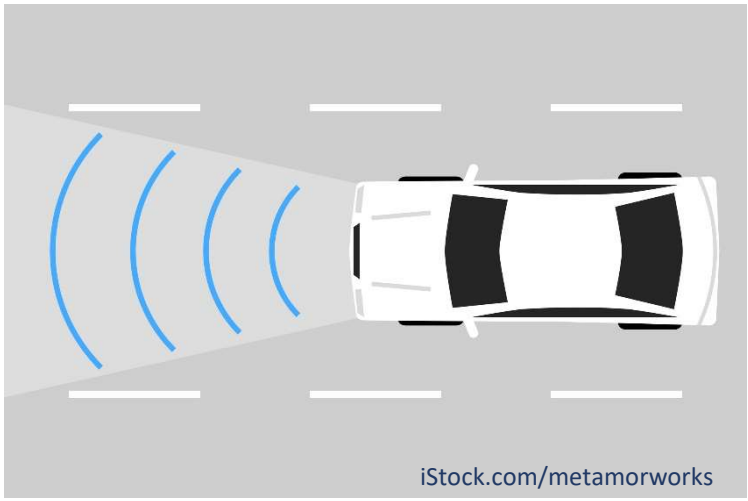
これらの意図する環境は少し違う？

ISO 13482　生活支援ロボット



iStock.com/metamorworks

ISO 26262　自動車



iStock.com/metamorworks

- 訓練，許可された人以外も共存する環境　（子供，高齢者，動物など）
- 一般消費者も使用
- 環境条件が管理された使用場所とは限らない　（雨，雪，霧，砂埃，落下物など）

ハザードを限定できない（あらかじめ定義しきれない，制限しきれない）
開いた運用環境

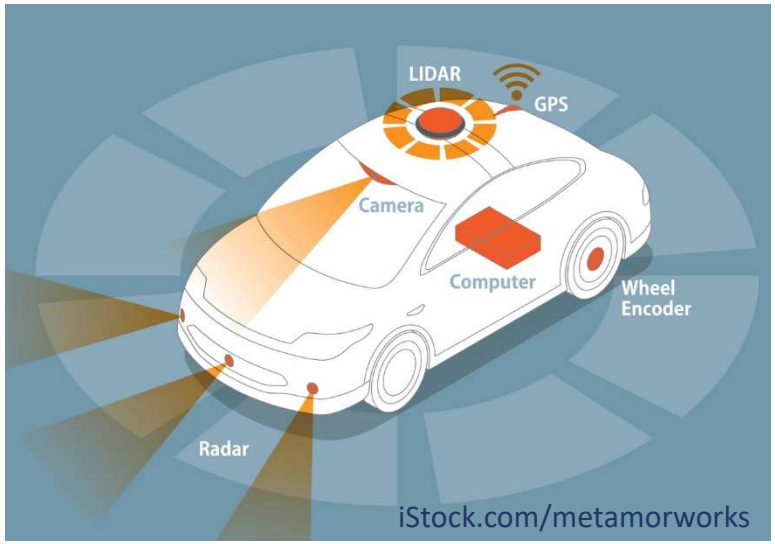
開いた運用環境のシステム

自動運転車

代表的な
センシング機器
- LiDAR，カメラ
- ミリ波レーダー，GPS

＋

これらの情報処理も安全機能となる．



安全性能の限界外の事象

LiDAR，カメラ･･･雪，対向車のライト等により，故障せずとも正常検出できない

曖昧性の大きな入力

信号，標識，道路状況のカメラ画像･･･電圧，温度のような，明確に扱える物理量ではない

AI技術の適用（画像処理など）

人の期待と異なる予見できない判断をする可能性がある

システムの故障ではない

安全性能限界外の事象

LiDAR，カメラ・・・雪，対向車のライト等により，故障せずとも正常検出できない

ミリ波レーダー・・・雪がレーダー部に付着して，故障せずとも正常検出できない

事例　https://dealer.honda.co.jp/hondacars-takaokachuo/blog/detail/?kyoten_cd=02&blog_id=14072

（Honda Cars 高岡中央ホームページ）

曖昧性の大きな入力

信号，標識，道路状況のカメラ画像・・・電圧，温度のような，
決定論的に扱うことができる物理量ではない．
故障せずとも正常検出できない．

下記のようなシーンでは

システムが**正常に作動しない場合**があります。

色あせた
標識

一部が
隠れている
標識

自車の
ヘッドライトの
光が届きにくい
位置にある標識
（夜間）

引用元：標識認識機能 | Hondaの安全技術 | テクノロジー図鑑 | Honda（https://www.honda.co.jp/tech/auto/safety/traffic-sign-recognition.html）

AI技術の適用（画像処理など）

人の期待と異なる予見できない判断をする可能性がある

システムの故障ではない

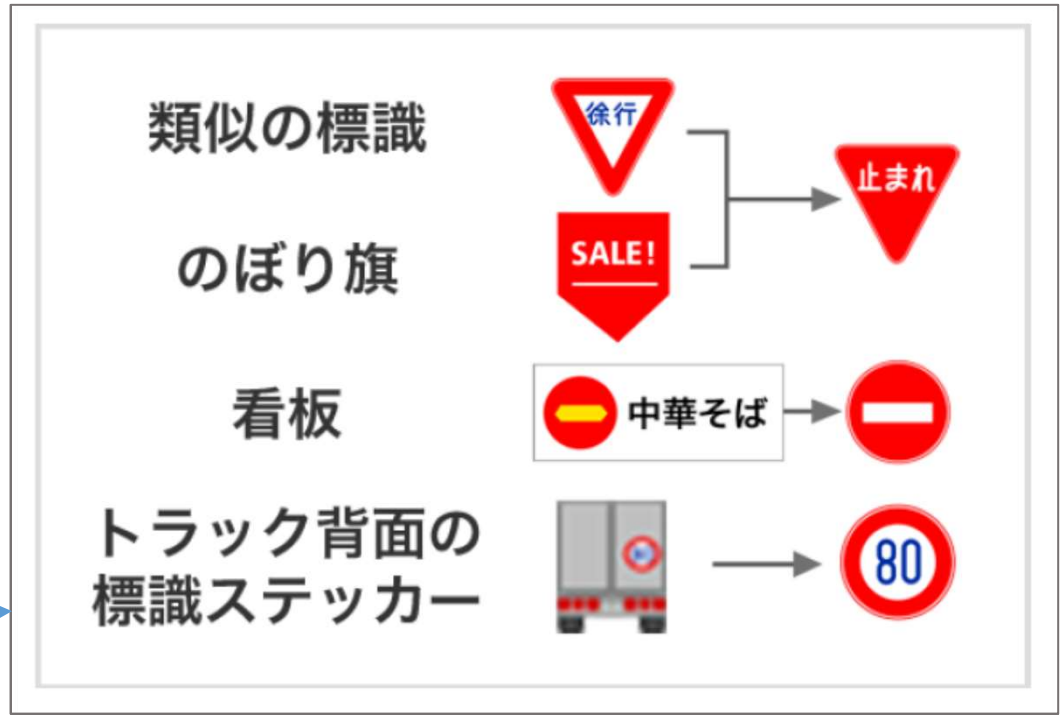
AIを技術を導入したとしても従来システムのこのような現象を皆無にできない

「天下一品を『進入禁止』と誤認？」

引用元：Jcastニュース　2021年2月3日記事　（https://www.j-cast.com/）

どんな誤認の可能性がある？

- 既知の誤認
- まだ未知だが予見可能な誤認
- 未知，かつ予見不能な誤認



引用元：標識認識機能 | Hondaの安全技術 | テクノロジー図鑑 | Honda
（https://www.honda.co.jp/tech/auto/safety/traffic-sign-recognition.html）

AI技術の適用

今後，自動運転車，ロボットなどの基本制御系，安全関連制御系などにAI技術が適用される見込みは高い。

人の期待と異なる予見できない判断をする可能性と，安全性の検証の困難さから，

現行の機能安全規格：SIL 2以上はAI技術の適用を推奨しない.

IEC 61508-3 Ed.2 (2010)

Table A.2 – Software design and development – software architecture design

ソフトウェア設計及び開発－ソフトウェアアーキテクチャ設計

Technique/Measure	SIL 1	SIL 2	SIL 3	SIL 4
Artificial intelligence - fault correction 人工知能－フォールト修正	---	NR	NR	NR

--- : 推奨も反対もしない
NR: 推奨しない

AI を実装したシステムの安全を確保するには[*)]

－AIの機能安全能力による　（方策1）
－AI以外の手段による　（方策2）
－方策1及び2による　（方策3）

AIは、学習を重ねることで判断の正確性が高まるが、
判断ミスを完全になくすことはできない。

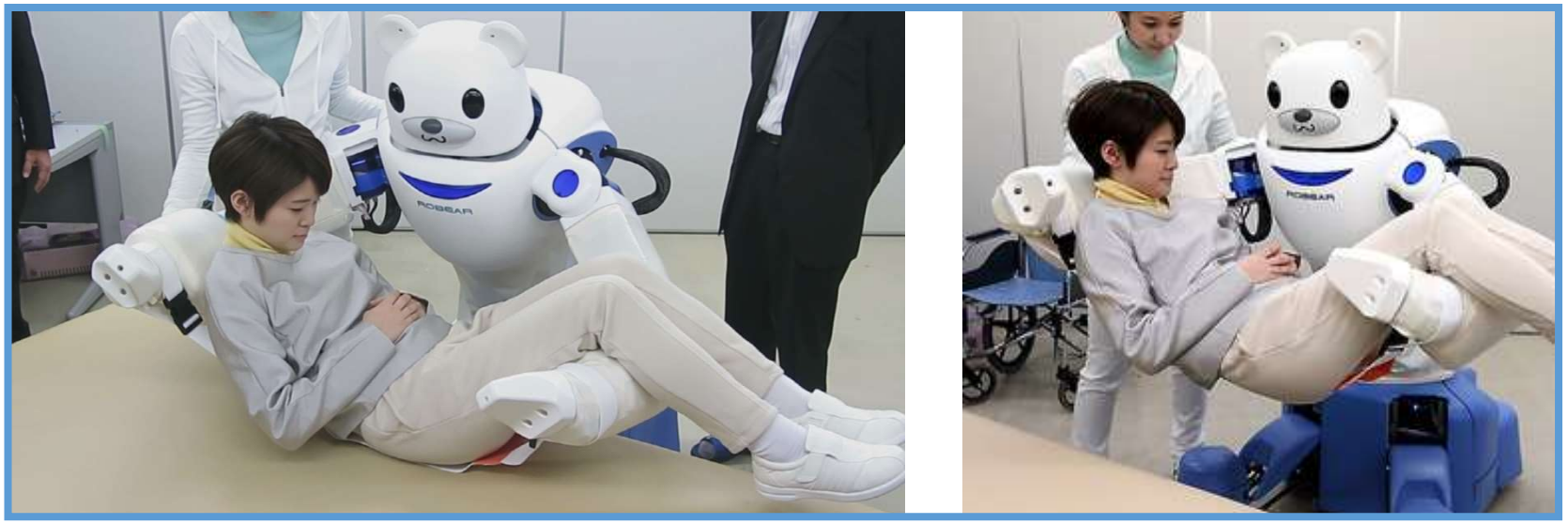
AIだけで固有安全/本質安全を達成するのは現時点で困難

多重防護層の構築により安全を確保　＝方策3

*) 人工知能(AI)と安全 (soumu.go.jp)：人工知能(AI)と安全，佐藤吉信，2019年2月5日

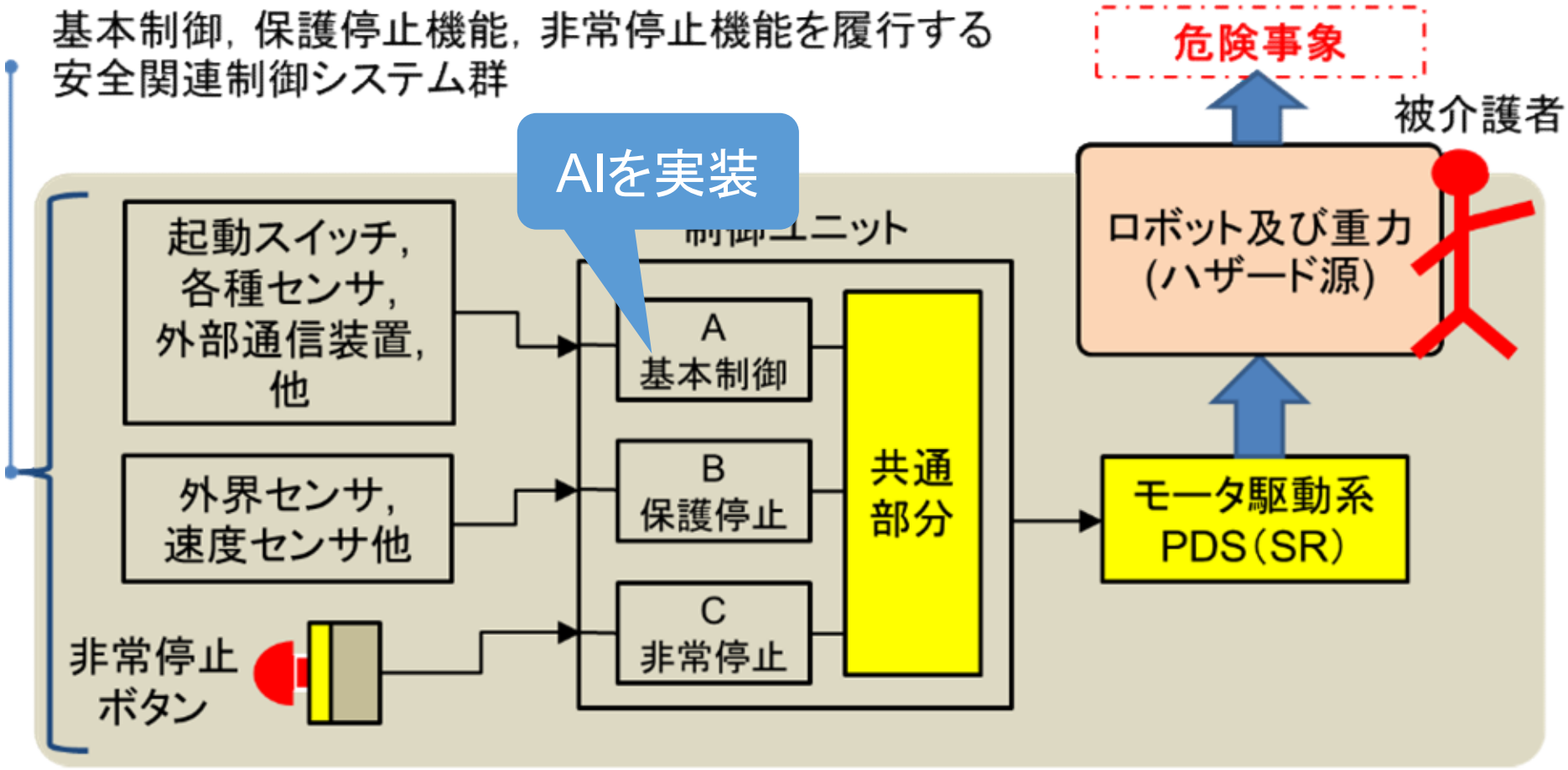
多重防護層による安全確保

介護ロボットのデモ



出典：理化学研究所　RIBAⅡ　2015.2.24　Kyodo News（共同通信社）

例：衝突ハザード及び転倒ハザード等を有する介護ロボットの安全関連制御システム群（多重防護層）



佐藤吉信，人工知能（AI）技術と安全性，平成30年度電子部品信頼性調査研究委員会研究成果報告書，RCJ，pp.4−10，March 2019

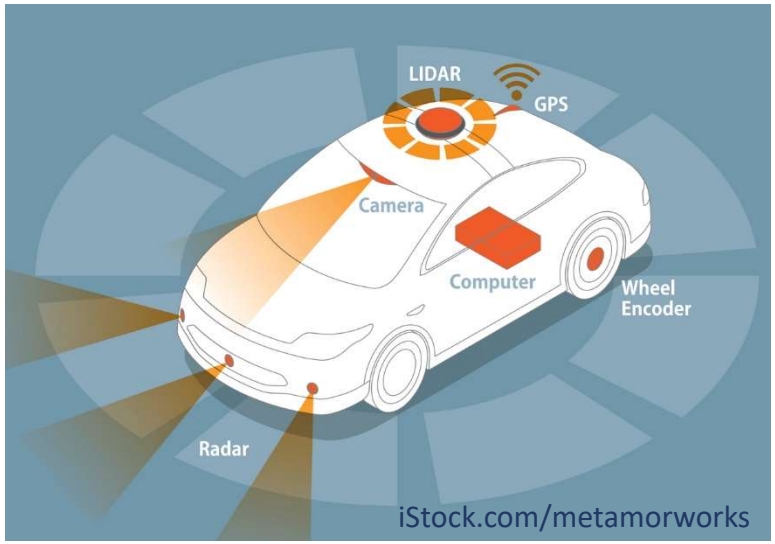
開いた運用環境のシステム

自動運転車

代表的な
センシング機器
- LiDAR，カメラ
- ミリ波レーダー，GPS

＋

これらの情報処理も安全機能となる．



安全性能限界外の事象

LiDAR，カメラ･･･雪，対向車のライト等により，故障せずとも正常検出できない

曖昧性の大きな入力

信号，標識，道路状況のカメラ画像･･･電圧，温度のような，明確に扱える物理量ではない

AI技術の適用（画像処理など）

人の期待と異なる予見できない判断をする可能性がある

システムの故障ではない．
機能安全では対処できない．

安全関連系の故障に加え，

安全性能限界外，予見不能のハザード，リスクの想定が必要

合理的に予見可能な誤使用

故障せずとも,

人による取り扱い方によっては危険が生じる

Intended use（意図する使用）:

製品若しくはシステムとともに提供される情報に従った使用,
又はそのような情報がない場合には一般的に理解されている方法による使用.
（ISO/IEC Guide 51 :2014　3.6）

misuse（誤使用）:

製造者が意図しない方法でユーザーがそのシステムを使用すること
（ISO/PAS 21448 :2019　3.7）

reasonably foreseeable misuse（合理的に予見可能な誤使用）:

容易に予測できる人間の行動によって引き起こされる使用であるが,
供給者が意図しない方法による製品又はシステムの使用.
（ISO/IEC Guide 51 :2014　3.7）

システムの故障ではない.
機能安全では対処できない.

新しい概念　SOTIF

安全な自動運転のために，

- （危険側）故障，危険な機能不全 ･･･ **機能安全**で対応
- 安全関連系が故障せずとも（システムが正常でも）
  意図した安全機能では対応できない事象 ･･･ **SOTIF**で対応

ISO/PAS 21448 :2019
Road vehicles – **S**afety **o**f **t**he **i**ntended **f**unctionality
（自動車 ― 意図した機能の安全性）

PAS: Publicly Available Specification（公開仕様書）
緊急の市場ニーズに対応するための文書

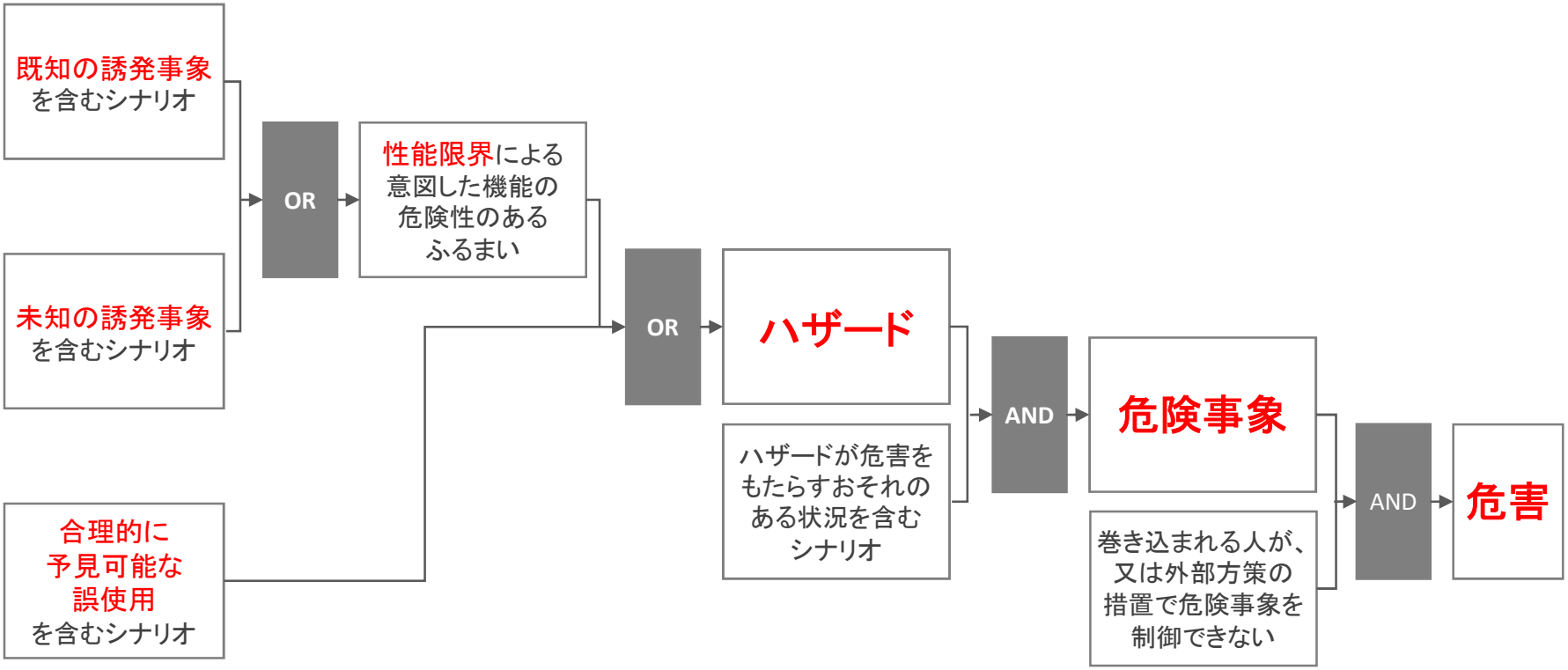
- 安全機能，安全性能の不完全性
- 合理的に予見可能な誤使用

によって生じるハザードによるリスクを十分に小さくする考え方，手順を示す．

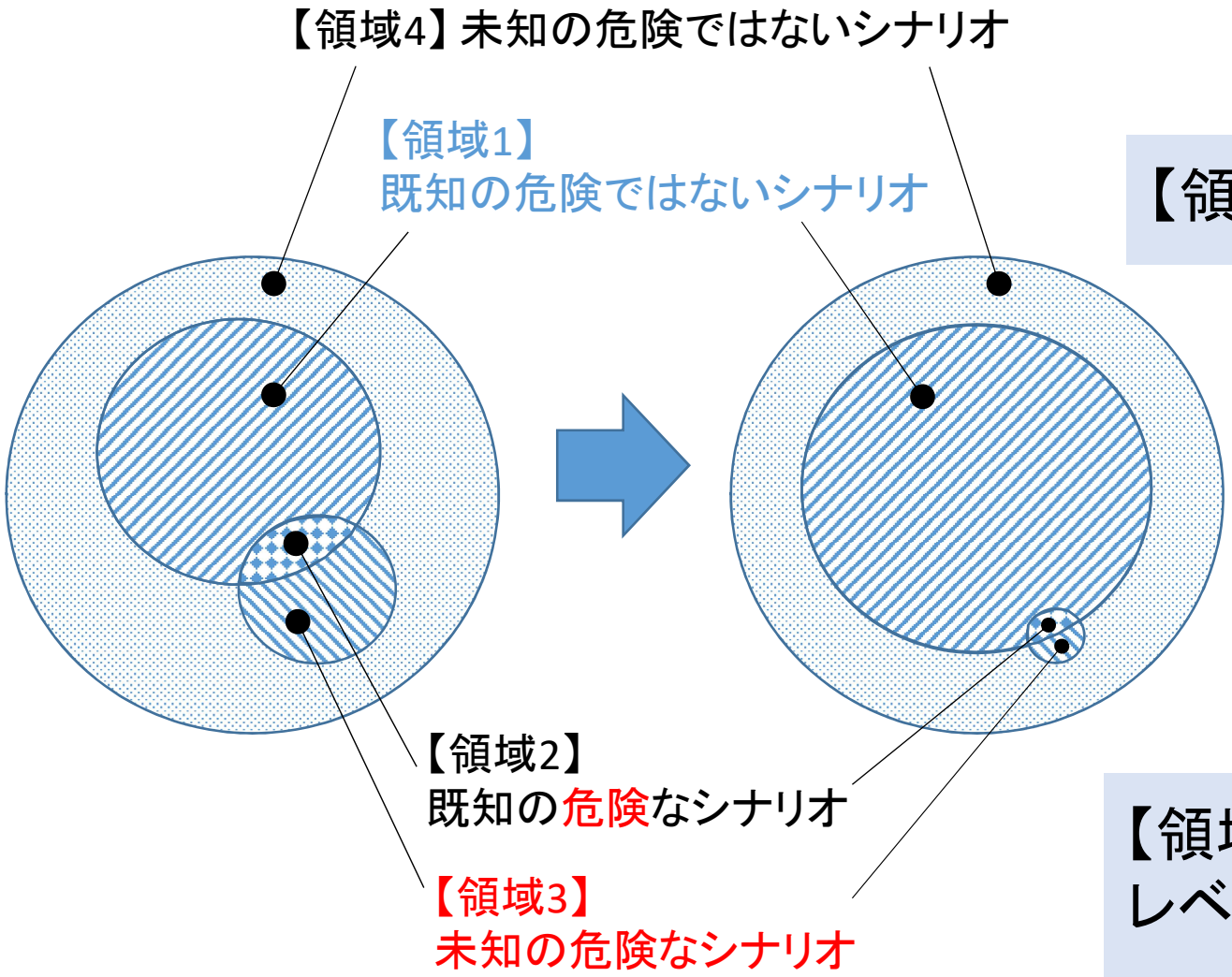
開いた運用環境を対象とする安全関連制御系全般に応用できる

SOTIFに関連するハザードと危害の発生

ISO/PAS 21448 11.2 Table 6



SOTIFによる安全性向上のイメージ



【領域1】を大きくする.

【領域3】を許容可能なレベルまで小さくする.

領域3をどのようにして小さくするか

未知のシナリオは，システムが車両に統合されてから現実の状況の中で遭遇.

各種テスト，系統的な分析などの産業分野でのベストプラクティスで小さくする.

ISO/PAS 21448 11.2 Table 9　残存リスクの評価

	方法
A	SN比の低下に対するロバスト性の妥当性確認（例えば，ノイズ注入テストによる）
B	独立性が該当するのであれば，それを求めて，アーキテクチャ特性の検証
C	ランダムテストケースでのループ内テスト（技術分析又はエラー推測から導き出す）
D	ランダム入力テスト
E	選択したテストケースでの車両レベルテスト（技術分析又はエラー推測から導き出す）
F	長期車両テスト
G	フリートテスト
H	現場の経験から導き出されるテスト
I	コーナーケース及び合理的に予見可能な誤使用のテスト
J	既存のシステムとの比較
K	選択したシナリオのシミュレーション
L	ワーストケースシナリオの分析

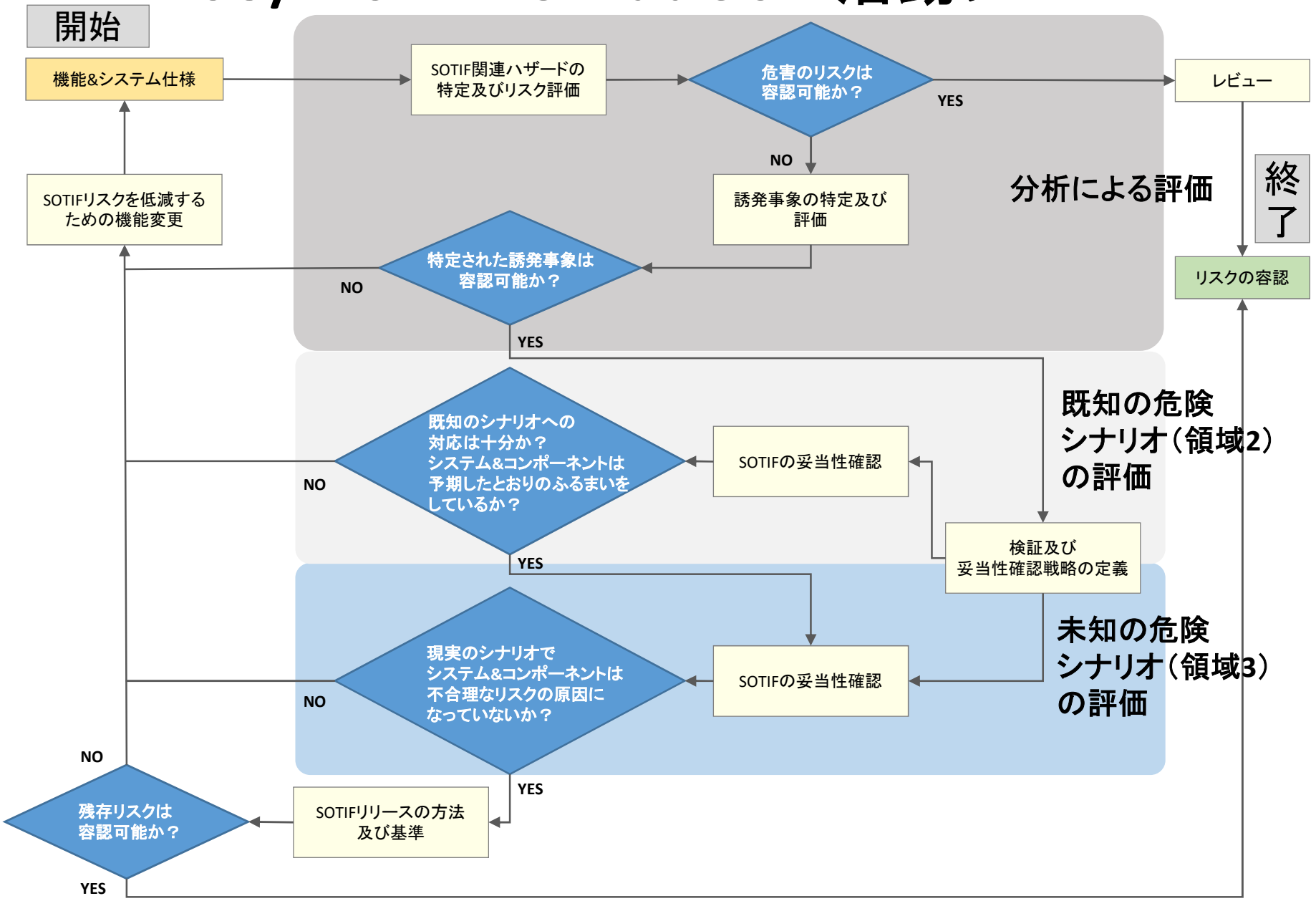
ISO/PAS 21448　A～L　**12種類**

ISO/DIS 21448　A～P　**16種類**

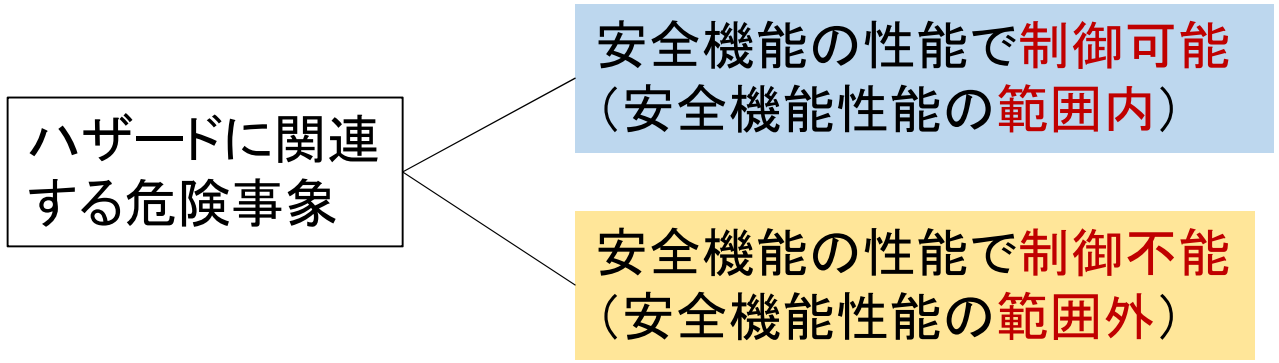
（国際規格原案）

合理的に予見可能な誤使用のテストほか追加

ISO/PAS 21448　Table 9　活動フロー



安全機能性能の範囲及び限界



【例】 衝突被害軽減ブレーキで横断者を検知し衝突を回避

	検知	衝突回避	安全機能性能の限界	安全機能性能の範囲
70m前方を横断	可能	間に合う（制御可能）	限界内	範囲内
30m前方を横断	可能	間に合わない（制御不能）	限界外	範囲外
衝突被害軽減ブレーキ なし	できない	できない（制御不能）	対象外	

安全機能性能の範囲とハザードの予見性による ハザードの分類*)

安全機能性能	ハザード (予見可能)	メタハザード (予見不能)
範囲内[1] (制御可能)	限界内ハザード	限界内メタハザード
範囲外[2] (制御不能)	限界外ハザード 対象外ハザード	限界外メタハザード 対象外メタハザード

1 対象範囲内でまれに安全機能の失敗(不全)などのリスク源(risk sources)が発現し，不確実性すなわちリスクを生じさせる要因となる.

2 対象範囲外には安全機能の不設置(不備)も含む.

ハザードを予見できるかは，ハザードを同定する分析者の知識，技術及び注意力等に依存する.

*)川島 興，佐藤吉信，ハザード・リスクの分類法と機能安全・SOTIF・人工知能(AI)の対象範囲，REAJ第34回秋季信頼性シンポジウム報文集，日本信頼性学会，Session 3-1，Nov. 2020

安全機能性能の範囲とハザードの予見性による ハザードの分類*)

安全機能性能	ハザード (予見可能)	メタハザード (予見不能)
範囲内[1] (制御可能)	限界内ハザード	限界内メタハザード
範囲外[2] (制御不能)	限界外ハザード 対象外ハザード	限界外メタハザード 対象外メタハザード

1 対象範囲内でまれに安全機能の失敗(不全)などのリスク源(risk sources)が発現し，不確実性すなわちリスクを生じさせる要因となる.

2 対象範囲外には安全機能の不設置(不備)も含む.

制御不能な限界外/対象外メタハザードをできるだけ減らし，既知の限界内ハザードにしていくことで安全性が高まる.

*)川島 興，佐藤吉信，ハザード・リスクの分類法と機能安全・SOTIF・人工知能(AI)の対象範囲，REAJ第34回秋季信頼性シンポジウム報文集，日本信頼性学会，Session 3-1，Nov. 2020

安全機能性能・ハザード・リスク源の予見性によるリスクの分類*)

安全機能性能の範囲とハザードの予見性によって分類した諸ハザードによって生じるリスク

安全機能性能	リスク（予見可能）	メタリスク（予見不能）
範囲内（制御可能）	限界内ハザード（に対する安全機能の）不具合リスク	限界内ハザード不具合メタリスク 限界内メタハザード不具合メタリスク
範囲外（制御不能）	限界外ハザードリスク 対象外ハザードリスク	限界外ハザードメタリスク 限界外メタハザードメタリスク 対象外ハザードメタリスク 対象外メタハザードメタリスク

*)川島 興，佐藤吉信，ハザード・リスクの分類法と機能安全・SOTIF・人工知能(AI)の対象範囲，REAJ第34回秋季信頼性シンポジウム報文集，日本信頼性学会，Session 3-1，Nov. 2020

機能安全の諸リスクへの適用範囲*)

機能安全　運用環境が閉じたシステムにおける，安全関連系の安全性能限界内のハザード，リスクへの適用を意図

“安全機能性能の範囲外の外乱によるリスクは無視又は許容できる”

外部からのテロ攻撃，航空機の落下，
洪水・地震・津波・火山の噴火など自然環境の影響，ほか

安全機能性能	リスク（予見可能）	メタリスク（予見不能）
範囲内（制御可能）	限界内ハザード（に対する安全機能の）不具合リスク	限界内ハザード不具合メタリスク 限界内メタハザード不具合メタリスク
範囲外（制御不能）	限界外ハザードリスク	限界外ハザードメタリスク 限界外メタハザードメタリスク
	対象外ハザードリスク	対象外ハザードメタリスク 対象外メタハザードメタリスク

*)川島 興，佐藤吉信，ハザード・リスクの分類法と機能安全・SOTIF・人工知能(AI)の対象範囲，REAJ第34回秋季信頼性シンポジウム報文集，日本信頼性学会，Session 3-1，Nov. 2020

自動運転車に想定されるリスクの範囲*)

自動運転

活動範囲の自由度が高く，運用環境は閉じたシステムであると想定することは難しい．

従って，機能安全が対象とする安全機能性能の範囲内のリスクの他に，範囲外の諸リスクを考慮する必要がある．

安全機能性能	リスク（予見可能）	メタリスク（予見不能）
範囲内（制御可能）	限界内ハザード（に対する安全機能の）不具合リスク	限界内ハザード不具合メタリスク 限界内メタハザード不具合メタリスク
範囲外（制御不能）	限界外ハザードリスク 対象外ハザードリスク	限界外ハザードメタリスク 限界外メタハザードメタリスク 対象外ハザードメタリスク 対象外メタハザードメタリスク

*)川島 興，佐藤吉信，ハザード・リスクの分類法と機能安全・SOTIF・人工知能(AI)の対象範囲，REAJ第34回秋季信頼性シンポジウム報文集，日本信頼性学会，Session 3-1，Nov. 2020

自動運転車に想定されるリスクの範囲*)

自動運転

活動範囲の自由度が高く，運用環境は閉じたシステムであると想定することは難しい．

従って，機能安全が対象とする安全機能性能の範囲内のリスクの他に，範囲外の諸リスクを考慮する必要がある．

安全機能性能	リスク（予見可能）	メタリスク（予見不能）
範囲内（制御可能）	限界内ハザード（に対する安全機能の）不具合リスク	限界内ハザード不具合メタリスク 限界内メタハザード不具合メタリスク
範囲外（制御不能）	限界外ハザードリスク 対象外ハザードリスク	限界外ハザードメタリスク 限界外メタハザードメタリスク 対象外ハザードメタリスク 対象外メタハザードメタリスク

機能安全では対応できない

*)川島 興，佐藤吉信，ハザード・リスクの分類法と機能安全・SOTIF・人工知能(AI)の対象範囲，REAJ第34回秋季信頼性シンポジウム報文集，日本信頼性学会，Session 3-1，Nov. 2020

安全関連系へのAI技術実装で想定されるリスクの範囲 *)

AI

- 判断結果は学習によって変化する （向上すれば有用）.
- 判断結果の理由の検証が困難 （リスク源になり得る）.
- 人の期待と異なる想定外の判断をする可能性がある.
  （有用な方向又は危険な方向へ）

システムへのAIの実装は，安全機能性能の範囲外の諸リスクに対して，
ポジティブにもネガティブにもリスク源として作用し得る.

安全機能性能	リスク （予見可能）	メタリスク （予見不能）
範囲内 （制御可能）	限界内ハザード（に対する安全機能の）不具合リスク	限界内ハザード不具合メタリスク 限界内メタハザード不具合メタリスク
範囲外 （制御不能）	限界外ハザードリスク 対象外ハザードリスク	限界外ハザードメタリスク 限界外メタハザードメタリスク 対象外ハザードメタリスク 対象外メタハザードメタリスク

機能安全では対応できない

*)川島 興，佐藤吉信，ハザード・リスクの分類法と機能安全・SOTIF・人工知能(AI)の対象範囲，REAJ第34回秋季信頼性シンポジウム報文集，日本信頼性学会，Session 3-1，Nov. 2020

機能安全，SOTIFの適用範囲*)

機能安全　運用環境が閉じたシステムにおける，安全関連系の安全性能限界内のハザード，リスクへの適用を意図

SOTIF　機能安全が対象としない限界外のハザード，リスクを可能な限り同定・分析し，除去又は許容リスクレベルに低減

安全機能性能	リスク（予見可能）	メタリスク（予見不能）	
範囲内（制御可能）	限界内ハザード（に対する安全機能の）不具合リスク	限界内ハザード不具合メタリスク 限界内メタハザード不具合メタリスク	
範囲外（制御不能）	限界外ハザードリスク	限界外ハザードメタリスク 限界外メタハザードメタリスク	機能安全では対応できない
	対象外ハザードリスク	対象外ハザードメタリスク 対象外メタハザードメタリスク	

*)川島 興，佐藤吉信，ハザード・リスクの分類法と機能安全・SOTIF・人工知能(AI)の対象範囲，REAJ第34回秋季信頼性シンポジウム報文集，日本信頼性学会，Session 3-1，Nov. 2020

まとめ　機能安全，SOTIFの適用範囲*）

安全機能性能	リスク （予見可能）	メタリスク （予見不能）
範囲内 （制御可能）	限界内ハザード（に対する安全機能の）不具合リスク [1]	限界内ハザード不具合メタリスク [2] 限界内メタハザード不具合メタリスク [2]
範囲外 （制御不能）	限界外ハザードリスク [3]	限界外ハザードメタリスク [3] 限界外メタハザードメタリスク [3]
	対象外ハザードリスク [4]	対象外ハザードメタリスク [5] 対象外メタハザードメタリスク [6]

1 機能安全規格のランダムハードウェア故障の性能指標（SIL）を適用
2 機能安全規格の決定論的対応能力の性能指標(SC)を適用
3 SOTIF規格を適用
4 安全機能の対象外としたときにリスクレベルは許容可能か，リスクアセスメントで判定
（残留・残存リスク）
5, 6 リスクアセスメントの品質向上でメタリスクを予見可能にしてリスク許容可否の判定

*）川島 興，佐藤吉信，ハザード・リスクの分類法と機能安全・SOTIF・人工知能(AI)の対象範囲，REAJ第34回秋季信頼性シンポジウム報文集，日本信頼性学会，Session 3-1，Nov. 2020

自動運転車の事故事例

ここでは，SOTIFによってできるだけ多くのハザード・リスクを予見し，安全機能性能の限界内ハザード・リスクとして明示的に対応できるようにすることの重要性を共有する.

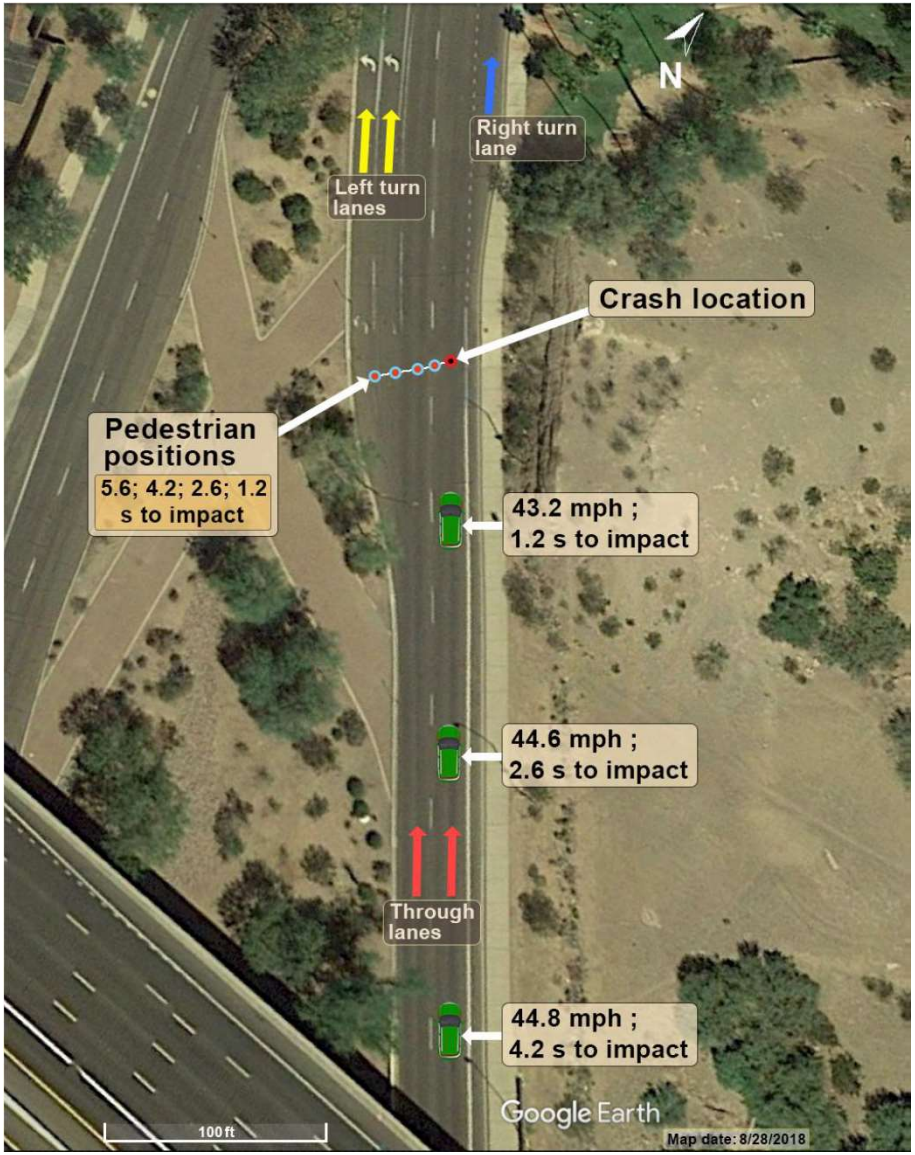
＜事例＞2018年9月，米国アリゾナ州で発生.
夜間に自転車を押しながら高速道路を横断中の歩行者が試験走行中の自動運転車にはねられ死亡.

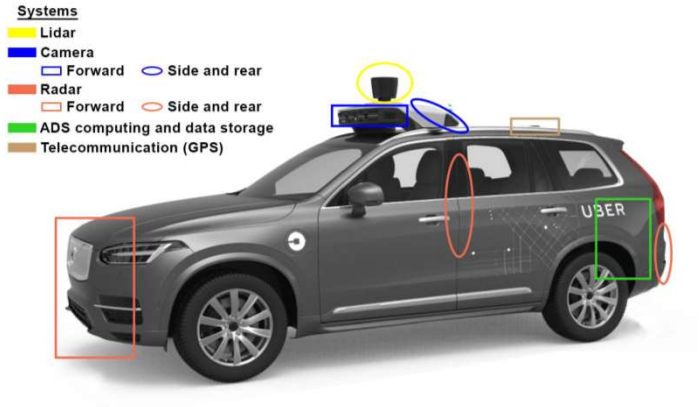
衝突1.2秒前	約70km/hで走行中，進路上に歩行者を検知. 回避できない（安全性能限界を超えている） ことをEUC制御システムが認識.
衝突0.2秒前	減速制御を開始すると同時に運転者に音響で警告.

自動運転車の事故事例

米国アリゾナ州テンペ警察署によって公開された動画

事故の詳細





- **衝突5.6秒前**　進行方向の左前方で自転車を押す歩行者を「自動車」として検知した．その後，**5.2秒前**に「その他」として検知，**4.2秒前**には再び「自動車」として検知した．
- 検知した対象物の種別が変化すると，別の対象物を検知したものとして扱い，対象物の位置の履歴が引き継がれない仕様であった．
- 衝突5.2秒前に「その他」として検知された歩行者は横断を始めていたが，4.2秒前に再び「自動車」として検知されたため，5.2秒前からの歩行者位置の履歴は引き継がれず，対象物は4.2秒前の位置に移動なく静止していると認識した．
- その後も検知結果が「自動車」，「自転車」，「その他」の間で幾度も変化したため，歩行者の移動経路が正確に予測できず，自車との衝突の危険を認識できなかった．
- **衝突1.2秒前**　自動運転車の進路上に歩行者が「自転車」として検知された．自動操舵で回避できないと判断し，ここで初めて自動運転システムが衝突の危険を認識した．
- 緊急事態に対応するため運転者が搭乗していたが携帯電話で動画を見るなどして，前方を十分注視していなかった．
- **衝突0.2秒前**　音響で運転者に警告し，同時に減速制御を開始した．
- **衝突0.02秒前**　運転者がハンドル操作を開始し，自動運転システムが解除された．
- **衝突0.7秒後**　運転者がブレーキを掛けた．

米国国家安全運輸委員会 事故報告書 HAR-19/03 PB2019- 101402

川島 興，自動運転による事故事例とその考察，日本信頼性学会誌 Vol.42, №1（通巻251号），日本信頼性学会, pp.32-37, Jan.2020

限界外ハザードが突然発生？

衝突1.2秒前　　約70km/hで走行中，数十m先の進路上に歩行者を検知.

回避できない（安全性能限界を超えている）ことを
EUC制御システムが認識.

衝突0.2秒前　　減速制御を開始すると同時に運転者に音響で警告.

この事故のSOTIFに関連する二つの要素

安全機能，安全性能の不完全性

・自転車を押している人間の検知結果が「自動車」，「自転車」，「その他」の間で幾度も変化．

・検知した対象物の種別が変化すると，別の対象物を検知したものとして扱い対象物の位置の履歴を引き継がないことから移動経路が推測されなかった．
このような場合、正確な衝突予測ができない。

合理的に予見できる誤使用

・運転者は携帯電話で動画を見ていて前方を注視していなかった．

・機械が主になり人が従になるときの人間工学的問題は以前から知られており，この誤使用は容易に予想できた．

安全機能の不完全性　＋　合理的に予見できる誤使用

回避能力を超えた限界外ハザードが発生

人間工学的側面

ISO/TR 22100-3 :2016
機械類の安全性 ーISO 12100との関係ー
第3部：安全規格への人間工学的原則の導入

5.3.2.5 ヒューマンエラー

・機械の設計者が，注意及び集中に影響する人間工学的要因を考慮に入れない場合，作業者の意図しない行動によるリスク，又は合理的に予見可能な誤使用によるリスクが生じる.

・まだその時点で存在していない情報に重要な注意を払うための管理時間が長くなるほど警戒心は低下する.（開始30分を過ぎると低下が顕著になる.）

この事故のSOTIFに関連する二つの要素

安全機能，安全性能の不完全性

・自転車を押している人間の検知結果が「自動車」，「自転車」，「その他」の間で幾度も変化．

・検知した対象物の種別が変化すると，別の対象物を検知したものとして扱い対象物の位置の履歴を引き継がないことから移動経路が推測されなかった．
このような場合、正確な衝突予測ができない。

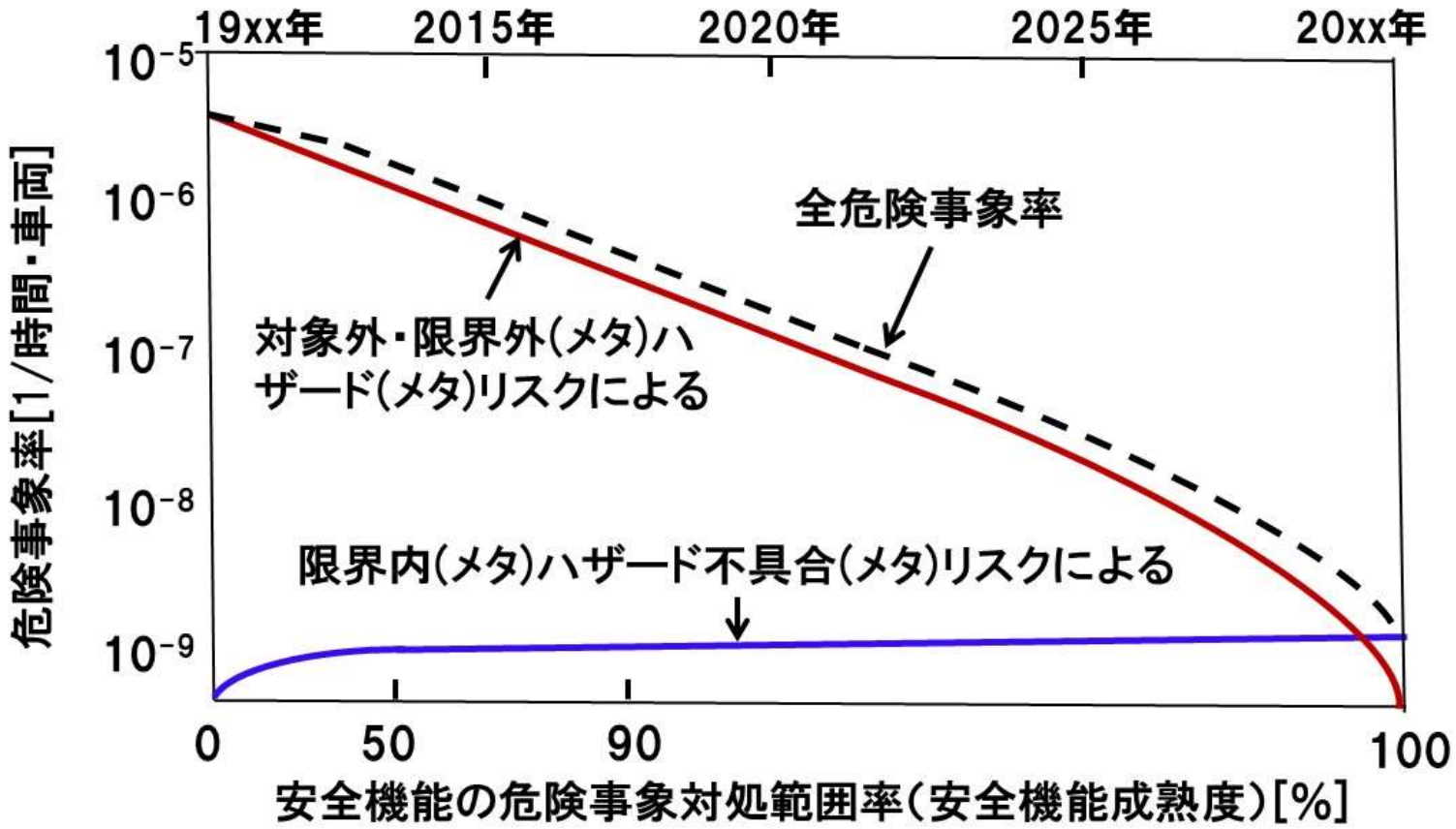
合理的に予見できる誤使用

・運転者は携帯電話で動画を見ていて前方を注視していなかった．

・機械が主になり人が従になるときの人間工学的問題は以前から知られており，この誤使用は容易に予想できた．

この事故はSOTIF規格を適用することで防げた可能性が高い

機能安全，SOTIFによる自動車安全機能の成熟と危険事象率の減少*)



ハザードリスクの分類よって対象外・限界外（メタ）ハザード（メタ）リスクの同定が体系的に実施可能になり，自動運転やAIを実装した安全関連系などにおいても安全機能の成熟が進むことで，危険事象率を下げていくことが期待できる.
自動運転だけでなく，開いた環境で運用される安全関連系全般に有効であろう.

*）川島 興，佐藤吉信，ハザード・リスクの分類法と機能安全・SOTIF・人工知能(AI)の対象範囲，REAJ第34回秋季信頼性シンポジウム報文集，日本信頼性学会，Session 3-1，Nov. 2020

ご静聴ありがとうございました