
SOTIF
AI時代の安全性概念
について

SOTIF

Safety Of The Intended Function
意図された機能の安全性

ISO/PAS 21448:2019

意図された機能の安全性とは？

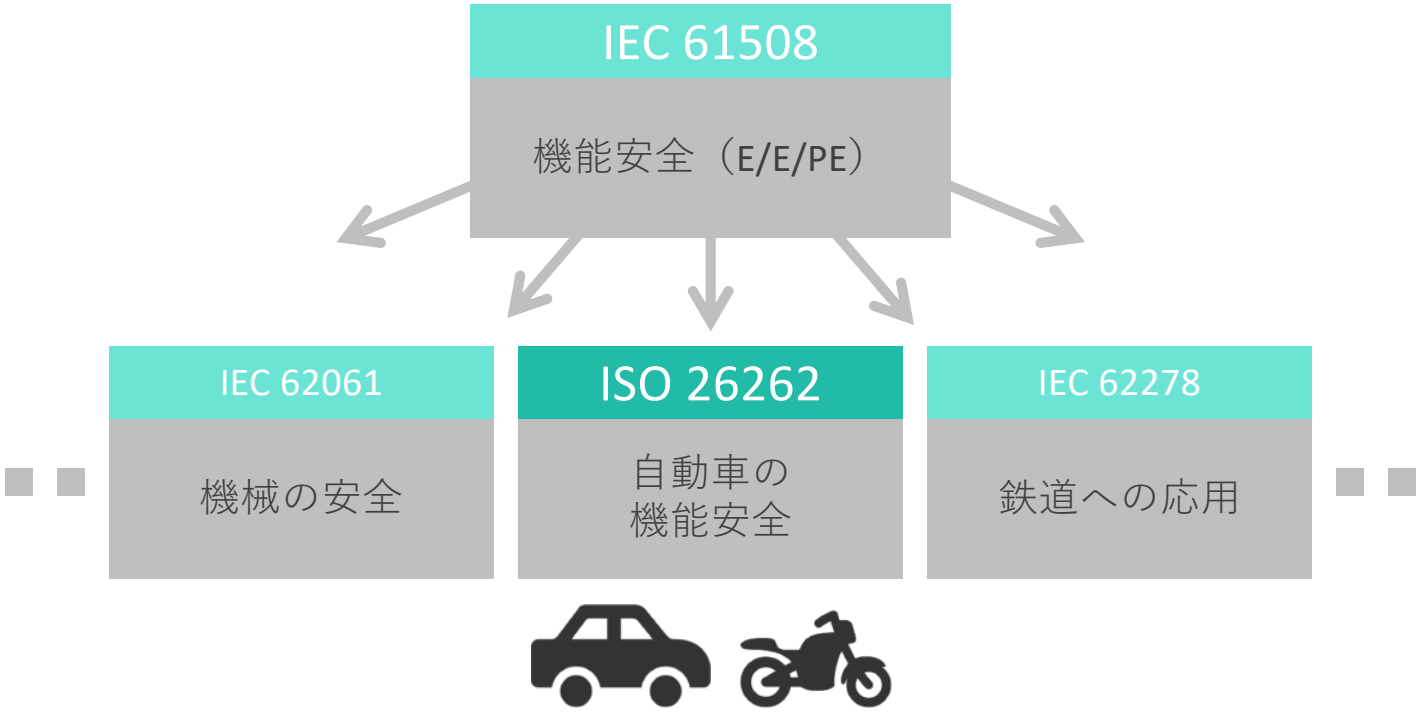
機能安全とは？

機能：E/Eシステム（コンピュータ等の電子機器を含んだ装置）で実装される機能（例：自動緊急ブレーキ）

機能安全：機能が機能不全のふるまいをすることにより引き起こされるハザードが原因となる，不合理なリスクの不在

コンピュータで実装する機能が
故障しないことで保たれる安全のこと

機能安全とは？



自動車分野の機能安全は
ISO 26262で規定されている


自動車はたくさんの
E/Eシステムで制御されている

ADAS（先進運転支援システム）

ACC（Adaptive Cruise Control System:アダプティブクルーズコントロール）

FCW（Forward Collision Warning:前方衝突警告）

AEBS（Advanced Emergency Braking System：衝突被害軽減制動制御装置）

TSR（Traffic Sign Recognition：交通標識認識）

LDW（Lane Departure Warning：車線逸脱警報）

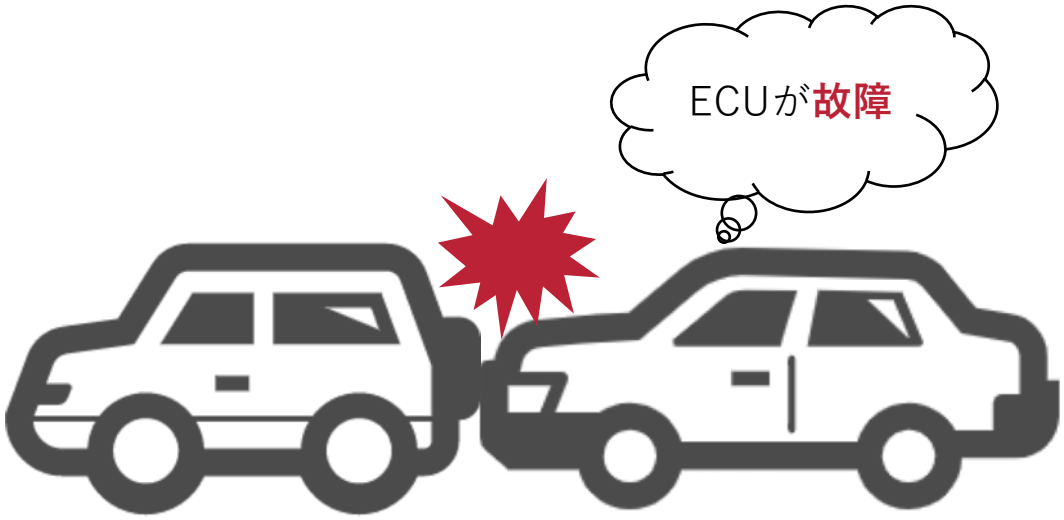
LKAS（Lane Keeping Assist System：車線逸脱防止支援システム）

ECUは自動車1台あたり数十個

AEBS（緊急ブレーキ）

危害（Harm）なし

AEBS（緊急ブレーキ）



機能の故障（意図しない機能）による危害

AEBS（緊急ブレーキ）

性能の限界（意図された機能＝故障なし）による危害

AEBS（緊急ブレーキ）

AEBSシステム

トリガーとなる事象：	ハザードの可能性となる動作：	ハザード：	危害：
空き缶が落ちている	誤認識によるブレーキ指示	急ブレーキ	後続車の追突

性能の限界（意図された機能＝故障なし）による危害

テスラ社による死亡事故（2016年5月）

著作権に関わるため図は非掲載

性能の限界（意図された機能＝故障なし）による危害

出典｜小林雅一，AIが人間を殺す日，集英社，2017

SOTIF

Safety Of The Intended Function
意図された機能の安全性

ISO/PAS 21448:2019

意図された機能の安全性とは？

SOTIF（ISO/PAS 21448:2019）とは？

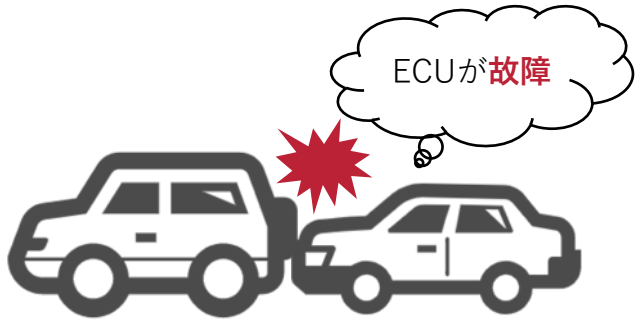
The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is referred to as the Safety Of The Intended Functionality (SOTIF).

機能不全，人の誤使用によるリスクが対象

ハザードとなる動作

危害なし

危害あり



ハザードの可能性となる動作が危害を招く


システムがハザードとなる動作をするとき
機能には何が起きているのか？

機能安全とSOTIF

故障あり

- **故障**
  - ランダムハードウェア
  - システマティック

機能安全
（ISO 26262）

機　能

E/Eシステム
ハードウェア
ソフトウェア

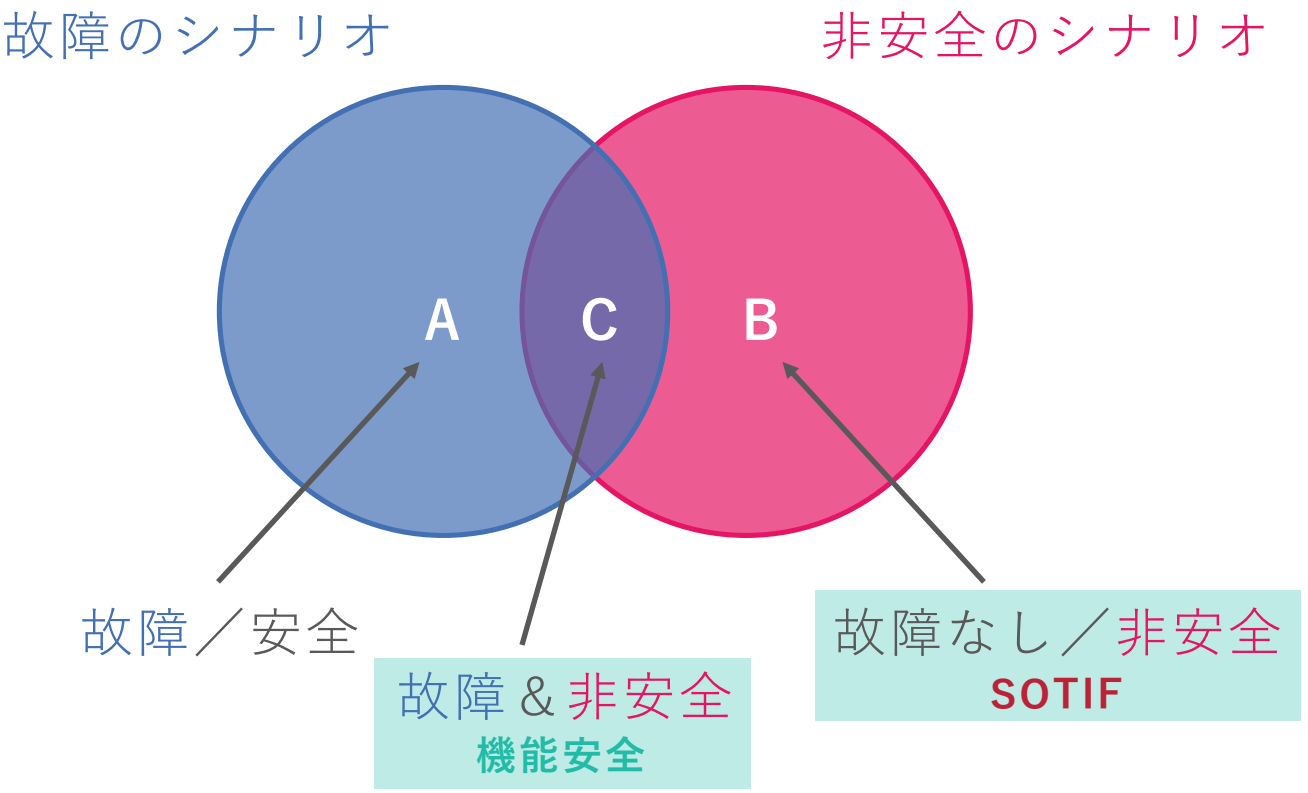
故障なし

- **性能の限界**
  - **多数のセンサ**や多様な環境条件による頑強性の不足
  - **複雑なアルゴリズム**（機械学習など）による正しい状況認識の不足
- **人の誤使用**
  - ドライバーの注意欠如

SOTIF
（ISO/PAS 21448:2019）

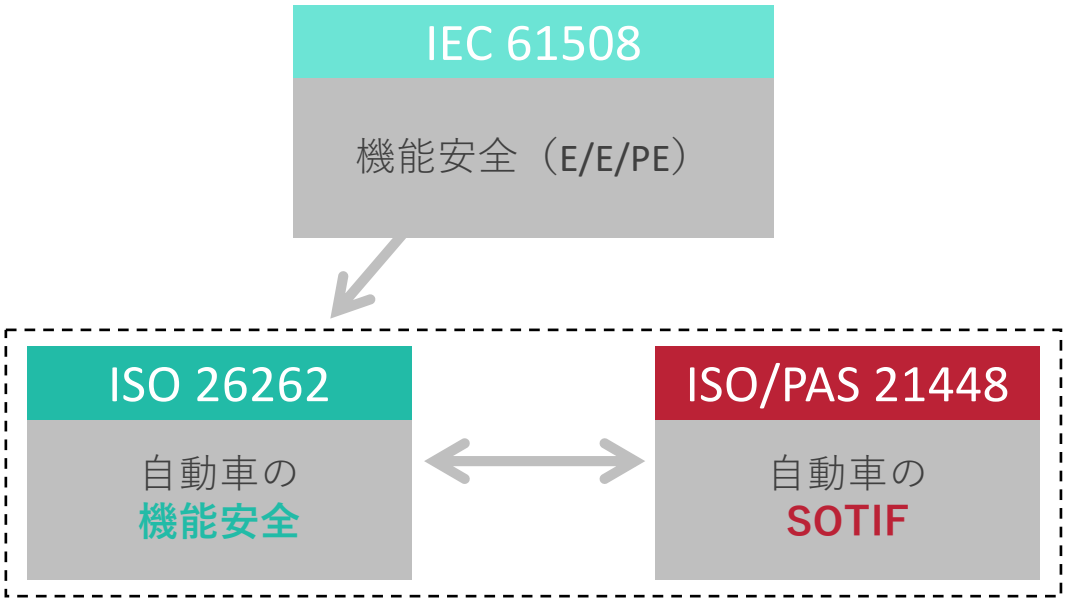
故障あり／なし
ハザードの可能性となる動作の原因となる

STAMPの対象



SOTIFは故障なし／非安全が対象

機能安全とSOTIF



機能安全とSOTIFは相補的

SOTIF（ISO/PAS 21448:2019）の構成

1	Scope
2	Normative references
3	Terms and definitions
4	Overview of this document’s activities in the development process
5	Functional and system specification (intended functionality content)
6	Identification and Evaluation of hazards caused by the intended functionality
7	Identification and Evaluation of triggering events
8	Functional modifications to reduce SOTIF related risks
9	Definition of the verification and validation strategy
10	Verification of the SOTIF (Area 2)
11	Validation of the SOTIF (Area 3)
12	Methodology and criteria for SOTIF release

Annex　A – G

シナリオの4つのエリア

著作権に関わるため図は非掲載

非安全を無くしたい

出典｜ISO/PAS 21448:2019, Figure 7, p. 7

4つのエリアの進展

著作権に関わるため図は非掲載

エリア2 → エリア1
エリア3 → エリア2

出典｜ISO/PAS 21448:2019, Figure 8, p.8

SOTIF（ISO/PAS 21448:2019）の構成

規格実施の流れ

1	Scope
2	Normative references
3	Terms and definitions
4	Overview of this document's activities in the development process
5	Functional and system specification (intended functionality content)
6	Identification and Evaluation of hazards caused by the intended functionality
7	Identification and Evaluation of triggering events
8	Functional modifications to reduce SOTIF related risks
9	Definition of the verification and validation strategy
10	Verification of the SOTIF (Area 2)
11	Validation of the SOTIF (Area 3)
12	Methodology and criteria for SOTIF release
Annex	A – G

著作権に関わるため図は非掲載

出典｜ISO/PAS 21448:2019, Figure 9, p. 9

まとめ

- **SOTIF**（ISO/PAS 21448）：意図された機能の安全性
- **機能**：E/Eシステムで実装される機能
- **機能安全**（ISO 26262）：E/Eシステムに**故障がある**場合
- **SOTIF**：E/Eシステムに**故障がない**場合
  - 性能の限界（機能不十分）
  - 人の誤使用（合理的に予見できる）


ありがとうございました