

機能安全と規格



本日の内容

- 安全とは何か
- 機能安全＝安全？
- RAMSの中の機能安全
- フェールセーフの範囲とフェールセーフティ
- 故障の種別とその対策
- なぜSILを定義するのか、なぜ間違えるのか
- RAMSをやれば安全？
- 皆様をお願いしたいこと

0. 安全とは



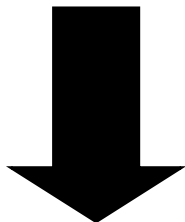
安全とは、人とその共同体への損傷、ならびに人、組織、公共の所有物に損害がないと客観的に判断されることである。と文科省のHPに書いている。しかしこんなことは可能なのか？

Safety
freedom from unacceptable risk
受け入れられないリスクがないこと

-ISO/IEC Guide 51:1999, definition 3.1

受け入れられない

受容できるかの判断



リスクに対する意思決定と
受け入れマトリックスの作成

リスク

Harmの発生確率とHarmの重篤性の組み合わせ

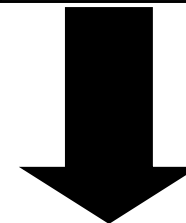
Harmとは

身体的な傷害、または人、財産および家畜に生じる損害・被害



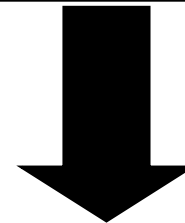
どのようなものが該当するかリストアップ

確率



確率モデルの
策定と推定

重篤性



Harmの
結果推定

1. 安全＝機能安全？

functional safety

part of the overall safety that depends on functional and physical units operating correctly in response to their inputs

機能ユニット及び物理ユニットが、その入力に対して正しく動作することに依存する安全性の一部
とでもなるでしょうか？

あくまで、「一部」です。

本質安全

頑丈に作って壊れにくくする。危険そのものを設計で受容可能まで低減する。

機能安全

安全を阻害する故障を想定して、故障時働く機能を作り、受容可能まで低減。

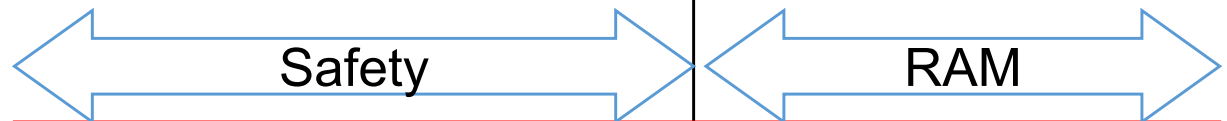


基本的に電子システムにおいて、頑丈に作って壊れにくくするというのはまず難しいため、機能安全以外の選択はとりにくいと思う。

2. RAMS規格と機能安全の関係性

IEC 61508: sets out a generic approach for all safety lifecycle activities for E/E/PE elements that are used to perform safety functions.

機能安全の規格であり、電気/電子/プログラム電子システムの安全機能を働かせるために安全ライフサイクル行為を一般的な方法で決めたもの←どんなことをすればよいのかが決まっている。



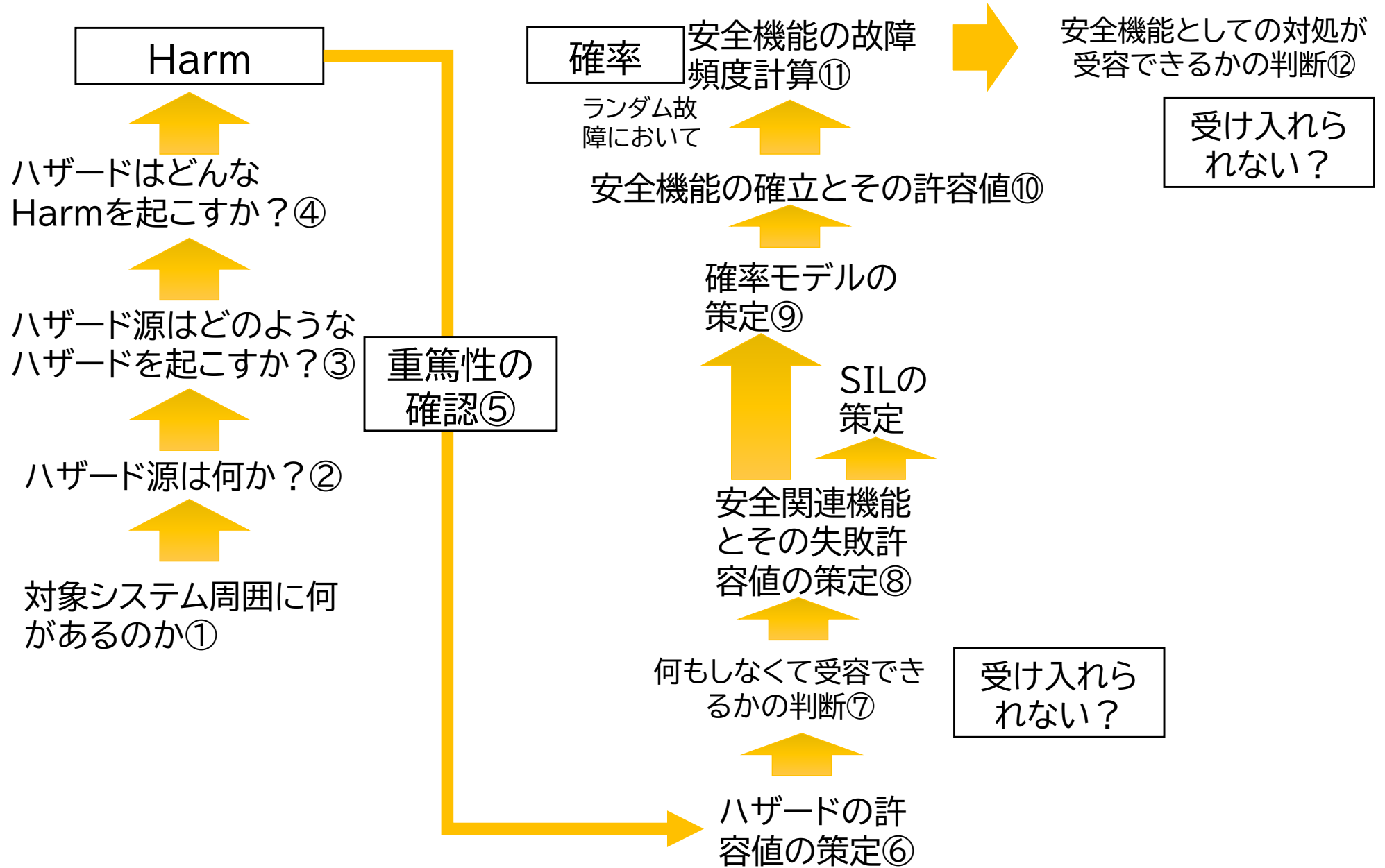
IEC 62278とその関係規格:

IEC 62278シリーズは、IEC 61508の一部の鉄道特化版であり、鉄道においては62278, 62279, 62425はIEC 61508と同等。これらの規格との整合性を示せば、IEC 61508を参照しなくてよい。

ということであるため、これもまた、鉄道において安全及びRAMに対して、ライフサイクルを通してどんなことをすればよいかの考え方の整理がされているということになる。

製品とその機能のSILに応じて、RAMS要求をライフサイクル全体で計画、実現、維持できることが
結局重要

2. 一般的にはどのような流れ？



3. 安全機能の実現

安全機能の確立とその許容値⑩

- ハザードを防ぐ機能(安全機能)と、その機能の目標となる危険側遷移頻度(TFFR: Tolerable Functional Failure Rate)を決める。
- その機能がどのサブシステム・コンポーネント(以降サブシステムなど)に割り当てられるかを定める。安全機能は各々独立である必要がある。独立でない場合は、共倒れするので、それを加味しておく。
- そのサブシステムなどの危険側となる故障頻度を、実際の回路や部品などから推定し、TFFRと矛盾していないかどうかを確認する。
- 推定した方法やその解析の限界を記録しておく。
- TFFRからSILを決める。SILにあった管理手法、技術的実現手法をとる。

3. 安全機能の実現

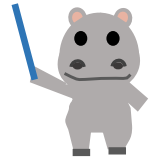
フェールセーフとフェールセーフティ

Fail-safetyの実現



ウチの装置はフェールセーフやねん。

素晴らしいですね。でもIEC 61508には、フェールセーフを必須の概念としていませんし、Introduction以外に出てきていません。社長のフェールセーフとは何でしょうか。



ウチの装置は2つで計算して比較するから安全やねん。一致しなかったら止めるからフェールセーフやねん。

素晴らしいですね。でもそれは、本質的なフェールセーフではなく、故障を検知して止めるまでに、もう一つの系が壊れる蓋然性は非常に少ないから安全という確率的なアプローチではないでしょうか。IEC 62425では、本質的なフェールセーフと、そのようにいくつかの要素を比較して矛盾があれば停止させる概念を含めて、Fail-safetyと称しています。



3. 安全機能の実現

フェールセーフとフェールセーフティ

Fail-safetyの実現

物理現象

- 電流が断たれる
- 発振が止まる
- 周波数がずれて、パッシブフィルタの出力が停止する
- などなど

正当性の確認

- 複数のハードウェアで比較して一致しているか確認し、一致していなければ止める
- 逆関数を計算して元に戻るかを別ハードウェアで行い、元に戻らなければ止める
- 計算結果を別ハードウェアで検算して不一致判定すれば止める
- などなど

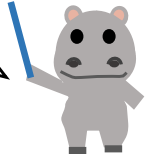
じつはこれ、双方を使っていることが多く、計算は複数で行い、停止するのはリレーの電源を切るなど物理現象を使っていることなど、組み合わせで安全担保していることが多くあります。

4. どのように受容可能とするのか



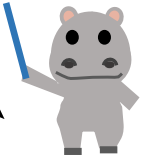
カバ興業の保安装置は、SIL4。だから $10^{-9}/h$ 。

その言い方はダメな例として、IEC 62278-2
10.2.12 Prevention of misuse of SILsにあげられています。



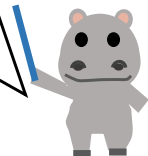
なんでだめなんや。常識的にSIL 4やろ。

リスクアセスメントする前に、決めても意味ないとされていること、また、SILは「この装置はSIL 4」というようなシステム特性には割り当てないこととされているのです。

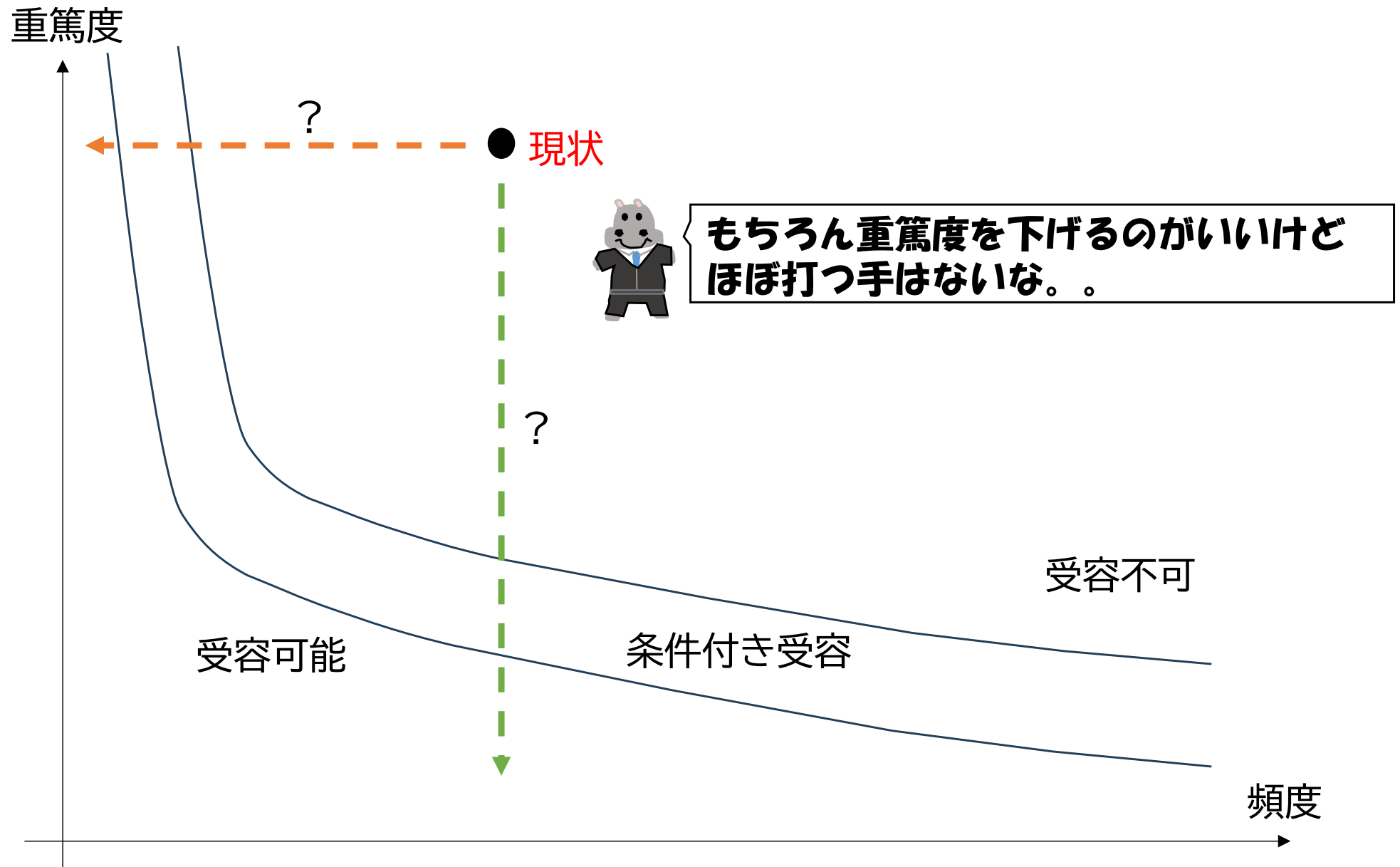


そんなもんミッション変わらんのやったら同じやろ前と。

IEC 62278-1やIEC 62425において、詳細なリスク想定 (Explicit Risk Estimation) でなくても、既存の解析の差分でもよいことになっているので、同じ機能には同じ受け入れ基準を設けても構いません。



4. どのように受容可能とするのか



4. 頻度が低い→実績ではだめ？

重篤度

求められるレベルはどうでしょうか。
信頼区間はいかほどで検討でしょうか？



受容可能 条件付き受容 受容不可

● 現状？



ウチの製品は、今まで危険側故障をしたことがない。だから大丈夫！

頻度

4. 頻度が低い→実績ではだめ？



ウチの製品は、10年間危険側故障をしたことがない。だから大丈夫！

社長、10年って、87660時間ですよ。これで一時間当たり $10^{-9}/h$ の危険側故障頻度って。。。言えます？



これは、、、これじゃあアカン。
100台ならどうや。。

そもそもまだモノができていないですよ。御社の費用で100台10年動かしてから出荷するんですか？それでも $10^{-7}/h$ レベルですが。



5. SILは何のために割り当ててるのか



SILはなんで割り当ててるんや。

安全関連機能の危険側遷移は、許容値以下としておきたい



信頼性ダイアグラムで、機能安全を担保する機能の失敗が許容値以下となることを確認

Random fault

しかしながら

そもそも仕様が間違っている？
計算が間違っている？
ソフトウェアにバグがたくさん残っている？
試験がいい加減？

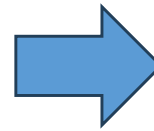
Systematic fault



しっかり管理すること、適切な技術を選択することでしか対処できない人間的なエラーがある。

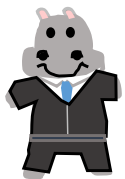
5. SILは何のために割り当ててるのか

機能安全を担保するための安全機能
の危険側遷移許容値
(Tolerable Functional Failure
Rate : TFFR)



SILに合ったルールと管理、技術的な
制約と選択

TFFRに応じ、
BI, SIL1,2,3,4の
5段階を割り当てる



**SILはRandom faultとSystematic faultをつなぐ架け橋ということ
かもしれんな。**

5. SILはモノ？機能？



でもなんで保安装置SIL 4っていうのはおかしいねん？

システムの構成する機能は、安全に関わるもの、そうでないものがあります。十把一絡げにSIL 4というと、すべての機能及び装置に対して均一に管理することになり、メリハリが付きません。また現実問題として、無理なこともあります。



でも安全に関わる部分はSIL 4ちゃうんか。

安全に関わる機能は、やはり安全に関わる機能を動作させるのにふさわしいハードウェアに割り当て、その機能の危険側故障許容値にふさわしいハードウェアにするのですね。
必要な安全機能のレベルを担保するために、ハードウェアがあるということになるわけです。だって必要がないのにオーバースペックのハードウェア作るほど御社が甘い会社とは思えないですもんね。



6. RAMSをやれば安全？



IEC 62278に適合させれば、IEC 61508をやる必要ないっていったやん。

IEC 61508: sets out a generic approach for all safety lifecycle activities for E/E/PE elements that are used to perform safety functions.

機能安全の規格であり、電気/電子/プログラム電子システムの安全機能を働かせるために安全ライフサイクル行為を一般的な方法で決めたもの←どんなことをすればよいのかが決まっている。



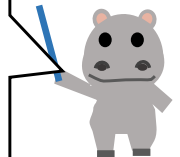
IEC 62278とその関係規格:

IEC 62278シリーズは、IEC 61508の一部の鉄道特化版であり、鉄道においては62278、62279、62425はIEC 61508と同等。これらの規格との整合性を示せば、IEC 61508を参照しなくてよい。

ということであるため、これもまた、鉄道において安全及びRAMに対して、ライフサイクルを通してどんなことをすればよいかの考え方の整理がされているということになる。

社長の意思次第です。

目標となるトレナビリティ(=我慢できる範囲)をどのように実現するかの方法論ですから。目標をどう置くか経営のトップマターですよ。



厳しければ厳しいなりにお金もかかるし、甘ければ信用を失うし、経営者はつらい。

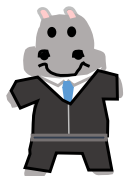
7. 最後に みなさんにおねがいしたいこと

IEC 61508にも、IEC 62278にも書かれていることですが、これらの規格はライフサイクルを通した機能安全の実現の一般的なアプローチが示されています。

「ライフサイクルを通して」なので、「今なら出来る」「書くだけなら出来る」では規格に合わない別の管理手法となってしまいます。

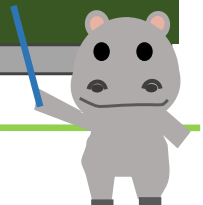
規格に書いていることに関しては、実はそれほど難しいことは書かれていません。しかし、「多岐にわたる」ことは否定しません。

「多岐にわたる」ことを個人で実施するのは大変です。「大変である」ということはよく聞きますが、みんなで得意分野を出し合って、ドキュメント化し、次世代の皆さんに残していくことを心掛けていただければ、「RAMSを通した次世代育成」ができるのではないかと考えています。



RAMSセミナー Webで開催中

回数	実施	内容	関係する規格
第1回	2025/4	初回説明とシステムを構築する前に調べる事項	IEC 62278 Phase I
第2回	2025/5	まず関係する状況を知ろう	IEC 62278 Phase2
第3回	2025/7	機能安全とは何か	IEC 62425
第4回	2025/9	確率で言える安全、仕組みで守る安全	IEC 62425/62279
第5回	2025/11	リスク解析	IEC 62278 Phase3
第6回	2026/1	安全の目標値とSILの関係	IEC 62278 Annex A
第7回	2026/3	安全のかなめ、故障検知と停止	IEC 62425
第8回	2026/5	ソフトウェアと安全関連システム	IEC 62279
第9回	2026/7	ソフトウェアの階層的開発	IEC62279
第10回	2026/9	システム要求と機能割り当て	IEC 62278 Phase 4,5
第11回	2026/10/28	トレーサビリティの重要性	IEC 62425/62279
第12回	2027/1	汎用製品の場合、特定の製品の場合の考え方	IEC 62425
第13回	2027/3	駅別データ等アプリケーションデータの重要性	IEC 62279
第14回		試験の網羅性の検討	IEC 62279
第15回		伝送における安全性と安全コード	IEC 62280
第16回		伝送線路のエラーと安全性の関係	IEC 62280
第17回		セキュリティ規格の動向	
第18回		VerificationおよびValidation	IEC 62425/62279/62278



第11回 RAMSセミナー トレーサビリティの重要性

2026年10月28日(水)15:00～ WEBにて

- トレーサビリティって、一番認証機関が鬼の首を取ったみたい、「できてないやないか」とうるさく言うものと相場は決まっています。
- でもよく見ると、結構皆さんやっている、重要性も認識されているけれど、規格がどうこうといわれると、ええっそんなんイヤ、となってしまうのではないのでしょうか。
- 以下の内容で説明します。ぜひお越してください。

- オレが一番、だからトレースなんて必要ない！について 
- でも、普通の会社は、会議で決まってことはやっているはず 
- 規格ではどんなこと言われているの？ 実は項目は多くないトレースの秘密
- 形式的にはOK、でも役に立たない事例

以上お話しします。

(独)自動車技術総合機構 交通安全環境研究所 鉄道認証室



交通研フォーラム

日時 2026年11月18日(水) 13:00~17:10 19日(木) 10:00~16:40
場所 東京大学 伊藤国際学術研究センター及びオンライン配信

- 交通安全環境研究所では、日頃の研究活動等について多くの皆様にご理解いただくため、「交通安全環境研究所フォーラム2026」を開催いたします。本年のフォーラムも引き続き、対面形式とオンライン形式を組み合わせたハイブリッド形式で開催させていただきます。
- フォーラムへの参加につきましては、事前登録制(無料)とさせていただきます。事前登録は、10月中旬から開始の予定です。

- 鉄道認証室は、

講演4. 仮想化する計算能力と鉄道信号保安装置

ー専用ハードウェアから仮想化基盤へ、その規格適合性を考えるー

として、18日の一番最後に、仮想化基盤における

IEC 62425, 62280, CLC/TS 50701, IEC 62443-3-2など、安全、伝送とサイバーセキュリティに関して、関連規格上の留意点と実現方法を考察します。

