

機能安全とはなにか

独立行政法人自動車技術総合機構
交通安全環境研究所 鉄道認証室
主席鉄道認証研究員

森 崇

目的

- RAMS規格は、一般的に「製品が規格に合っているかどうか認証をとるもの」と思われていますが、どうでしょうか？
- また、規格に合っていれば、安全で信頼性の高いものができると考えているかもしれません。
- RAMS規格はあくまでヒント。いいものを作るための特効薬ではありません。
- これから説明することで、今までよりも「なにかいいかもしれないな。」と思ったことを少しでも取り入れてくだされば、幸いです。

登場人物

鉄道信号メーカー カバ興業チーム



カバ興業 社長
座右の銘：技術と直感



カバ興業 営業 カバお
「怒られてナンボの毎日」



カバ興業 技術 オタかば
「面白くなければ技術じゃない」



カバ興業 プログラマ
ハッキングカバ
「俺しかできないことをやる」



カバ興業設計課長 カバ実
「全体のレベルアップ」

謎な奴



謎のフリーコンサル
なぞカバ
「知識は力！」

鉄道事業者 カバ鉄道チーム



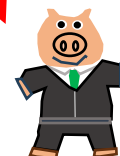
カバ鉄道 社長
品格の経営、根拠ある経営



カバ鉄道 電気課長
口癖：安くてエエもん持って来い！



カバ鉄道 乗務員 カバどん
いつかは自動化されるかも。ドキドキ

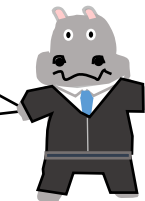


ブタ工業 社長
カバ興業を凌ぐ強い体質づくり

バチバチ

4-1-1 読みが大事

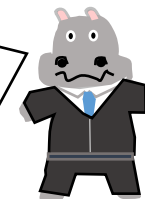
おい、カバお、こっちこい！今期決めるゆうとった、カバ鉄道さんの電子連動どうなってんねん。



は、はい。「高い高い天まで登る高さや、なんでこんな値段になるねんこんなもんいいわけないやろもっと値下げしろ、アカンアカンこんなんいけるわけないやろダメダメダメ」と追い返されました。



あんなあ、買うほうが「安いやないか。これで行こう。」なんて言うわけないやろ。そんなんゆうてくれる会社、あったら見てみたいわ。なんていうか、そんなんアカンかった時のこと、ちゃんと読んでやな、うまいことゆうてやな、ある程度納得してもろて、大体ナンボやったらいけるんか読むのがお前さんの仕事ちゃうんか。お前さんの情報には、相手のホンネまるで入ってないやないか。アカンかった時のこと前もって考えて行動するんちゃうんか。。



うまくいった時のイメージをもって楽観的に行動する方がいいんじゃないですか。ダメだったらその時どうするか考えたらいいでしょ。ポジティブシンキングが大事だってテレビで言っていましたけど。

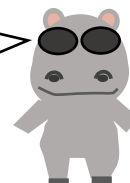


4-1-2 営業もモノづくりも同じ？



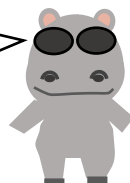
社長に「営業たるもの、怒られること、断られることから情報を得て、次の手を考えるアカンやろ！」と、ドヤされたよ。一度社長もカバ鉄道に行って断られてみるというよ。そんなアイデア急には浮かばないから。。

あんなあ、お前さん。うちの会社のコーポレートアイデンティティー知ってるか？



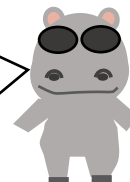
「フェールセーフのカバ興業」でしょ。知ってるよ。

フェールセーフって普通どういう意味で使うか知ってるか？



アカン場合でも安全になるっていうことでしょ。

だ、か、ら、フェールセーフとは違うけどな、お客さんから断られた時にどうするか事前に考えておくのがカバ興業やって、社長ゆうてるのちゃうんか。少なくともオレらはそうやってモノ作ってるで。。そんなん急にアイデアなんか出てくるわけないやんか。。。



4-1-3 どっちがいいと思いますか？



怒られないように、はじめっから壊れないように作っておけばいいんじゃないかな。壊れないなら、ちゃんと目的を果たすことができるから、安全も信頼性も両立するし、ぼくも怒られないよね。

アホかオマエ、カタチあるもんは壊れるねん。経営者としてやな、壊れんようにするためにナンボカネ掛けてもエエなんて言えるわけないやろ。壊れても最低限、被害が広がらんように、アカンようになったら、安全に止める機能を付けるのが筋なんちゃうんか。でも確かに怒られたくはないわな。。



ライフサイクル全体で壊れなく働く

VS

壊れることを予想して対処する

どっちを選びますか？



4-2 機能安全とは？

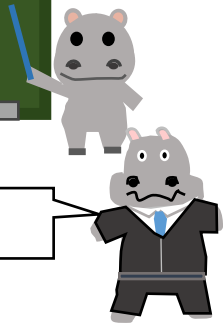
3.1.22 functional safety

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

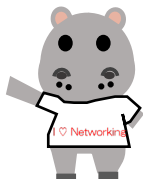
-IEC 62425 Ed.2

当該入力に対して、機能と物理的なユニットにより適切に動作することによる総合的な安全の一部

オマエこの翻訳、全然よくないんちゃうか。。まるで意味が分からんぞ。



4-2-1 入力とは



検査するときは、入力の網羅性試験が大事ですよ。その入力が異常値であれば、安全にシステムを止めるなど、安全動作をすることが機能安全と言えるのでしょうか。事前に入力の異常値を動作を加味した機能を作りこんでおくかが大事ですよ。



そうとも言えますが、それだけでいいのでしょうか。

	Intentional connection	Unintentional connection
Physical	指定ポートから電磁的ノイズ、過電圧や物理的なストレスが入ったらどうするの？ それが一時的故障？恒久的故障？	基板の内部配線や接地など、本来つなぐとされていないところから電磁的ノイズ、物理的なストレスが入ったらどうするの？ それが一時的故障？恒久的故障？
Functional	指定ポートから入力されたデータが間違ったらどうするの？	多分考えなくてよい。

4-2-2 機能と物理的ユニット

IEC 62425

A.2 Safety requirements



網羅的な安全対応機能を重視したいぞ！

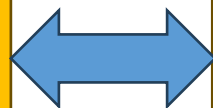


課長、私教育はしっかり受けているので、乗務員として危険対応能力は網羅しています！でも力バなので、ひょっとしたら失敗する頻度は結構あるかも。。

そもそも危険に対応する機能として定義されているか

使用する物理ユニットが、その機能の実現に対して、十分な能力を持っているか

どのようなハザードに対して対応できるかという
機能の定義



その機能のTolerable
Functional Failure Rate
(TFFR)と実際の物理ユニッ
トのFailure Rateとの整合性、
異常検出時間など

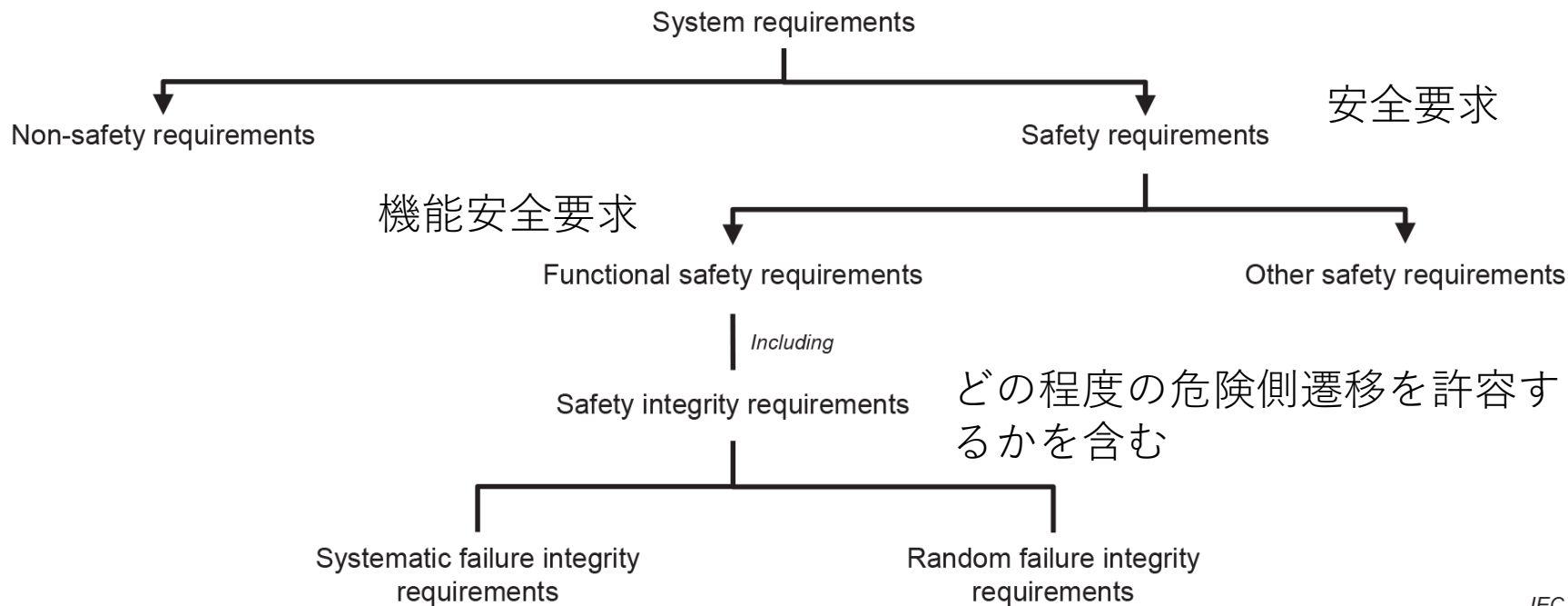


両方いりますよね。。

4-2-3 機能と安全性のレベル要求

IEC 62425

A.2 Safety requirements

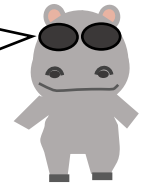
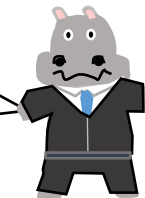


4-2-4 Operating Correctly (正しい動作?)

正しい動作って。正しい動作だったら、壊れてないやろ。これどういう意味や。

まあ普通そう考えるわな。でも、壊れた時に対応する機能が正しく動くって考えたらどうや。。

なんかおかしいぞ！



correct functional operation

入ってきたデータが
間違っとる

当該装置は壊れてい
るわけではないが異常

物理的に故障してい
ない装置で正しく動
作させればよい

ノイズでデータが化
けとる

当該装置は物理的に
故障しているわけ
ではないが、一時的に
一部の機能は喪失し
ている可能性あり

Effects of faults

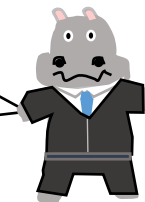
壊れてしまって、変な
計算結果ずっと出とる
または止まっとる

当該装置は物理的に
故障し、一部の機能
は喪失している

機能喪失していない部分で、安全動作を適切に実施すればよい

4-3 機能安全を実現する方式

壊れた時にも何とかしろって。。。ダイイングメッセージみたいやな。。



故障したら、ある一定方向に状態が遷移するという物理的特性が使用できる場合は、実現できることもあるな。例えば、リレーなんかで、電気が切れたら特定の接点が構成されとかな。でもダイイングメッセージは、死んだら自動的に書くものでもないから、機能安全ではないだろう。



カバしゃちゅ〜
ばんざい



そんな物理的特性特にCPUなんかでは無理やろ。壊れ方なんか分からんし。



健全性を
お互いが確認



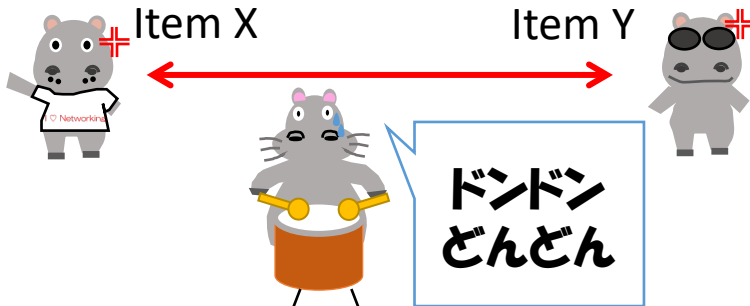
どちらかが、異常と判断すると、制御を止める。

4-3-1 共通原因故障を防ぐ

独立性が不十分な場合

健全性をお互いが確認
どちらかが、異常と判断すると、制御を止める。
でも両方同時に間違えたらオワリ。。

うるせー
間違えるやないか



うるせー
間違えるやないか

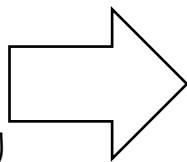
ハザードに対して独立している場合

Item X



うるせー
間違えるやないか

演算結果
相互にやり取り



Item XでItem Yの計算結果比較
Item YでItem Xの計算結果比較

Item Y



なんかやってるん
か？

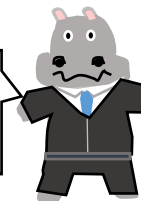
どちらかが不一致なら止める！
オリが離されており、共通原因故障
が防止されている。

4-4 機能安全だけが安全？



怒られないように、はじめっから壊れないように作っておけばいいんじゃないかな。

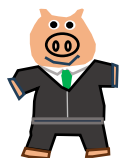
壊れても、安全に止める機能を付けるのが筋なんちゃうんか。



3.1.22 functional safety

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

- ハザード自体をなくす。
 - 列車と車の衝突を防ぐため、カバ興業の踏切制御装置をやめて、ブタ工業施工の高架工事を行う。→本質安全。
- 発生する蓋然性を0に近くする。
 - 列車の脱線を防ぐため、ガチガチの枕木とガチガチのレール、スーパーロングレールを採用する。



高架工事、軌道工事もブタ工業にお任せを！小手先のカバ興業の対策ではなく、元から原因を断ちましょう！

いや、分かる、分かるんだけど、何年かかるか分からんし、金銭的にも簡単ではない！株主に説明できんかもしれん。やはり投下資金と見あう安全性は、機能安全も含めて考えるのが企業経営者としては必要であることは分かっしてほしい。。



4-5まとめ

- 機能安全は、安全を担保するため、入力に対して適切に対処する機能を定義しておく安全の実現手法の一つです。
- 入力は明示的に入力されたものに限られません。ノイズ、雷、物理的ストレス、誤ったデータ等、明示的または非明示的なものが入力されます。このためハザード源の抽出は非常に重要です。
- 機能安全は、入力された事柄に対する適切な対応の機能定義のみではありません。装置などが、その機能の数値的なレベル、例えば機能がうまく働かない頻度、処理時間なども定義する必要があります。
- 機能安全を実現する方法はいろいろありますが、一般的には、物理的現象で故障した際、特定の状態に遷移する特性を活用する場合、複数のアイテムを比較して、不一致の場合、故障で機能喪失していない機能を使用し、安全側に遷移させます。
- 複数のアイテムを使用する場合は、同時に壊れると、残っている機能がないかもしれません。共通原因故障に注意しましょう。

