安全の目標値とSILの関係

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

森崇

0. 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！」

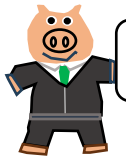
バチバチ

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！

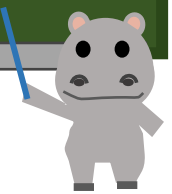
カバ鉄道　乗務員　カバどん
いつかは自動化されるかも。ドキドキ



ブタ工業　社長
カバ興業を凌ぐ強い体質づくり

1．はじめに

- このシステムはSIL4だから！といわれることが多いと思います。
- この摩訶不思議な言葉である、SILは、本来どのように定義され、どのように決めるのか、何に使用していいのかを少し説明させていただきたく存じます。



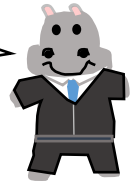
2. SIL4が要求されている

今度の新しい連動装置、カバ興業に発注しようと思ってんねん。勉強してくれるよな。もちろんな、勉強は大事やし安全も大事やで。

もちろん、ブタさんに負けないよう精いっぱいあんじょうやらしてもらいます。で、いつものように、SIL4っていうの、仕様書に書かれるんですか？

まーそらそうやろ。あんさんとこも、「SIL4システムのカバ興業」ゆうてるからな。問題ないやろ。

無論です。認証機関のカバレジストリに「いやあ、これSIL4システムとしてパーフェクトですよ」といわせてみせますよ。



じゃあまあ、カバ興業を本命としとくか。勉強してや頼むで。ブタ工業もこの頃売り込みすごいからな。油断禁物やで。

はい、カバ興業の総力を挙げて、ご期待に沿えるよう頑張らせていただきます！今回はお声がけ、ありがとうございました！

事務所にて

いや社長。SIL4てなんや、SILって。そもそもSILって何に使って、何のためにあるんや。営業トークか。

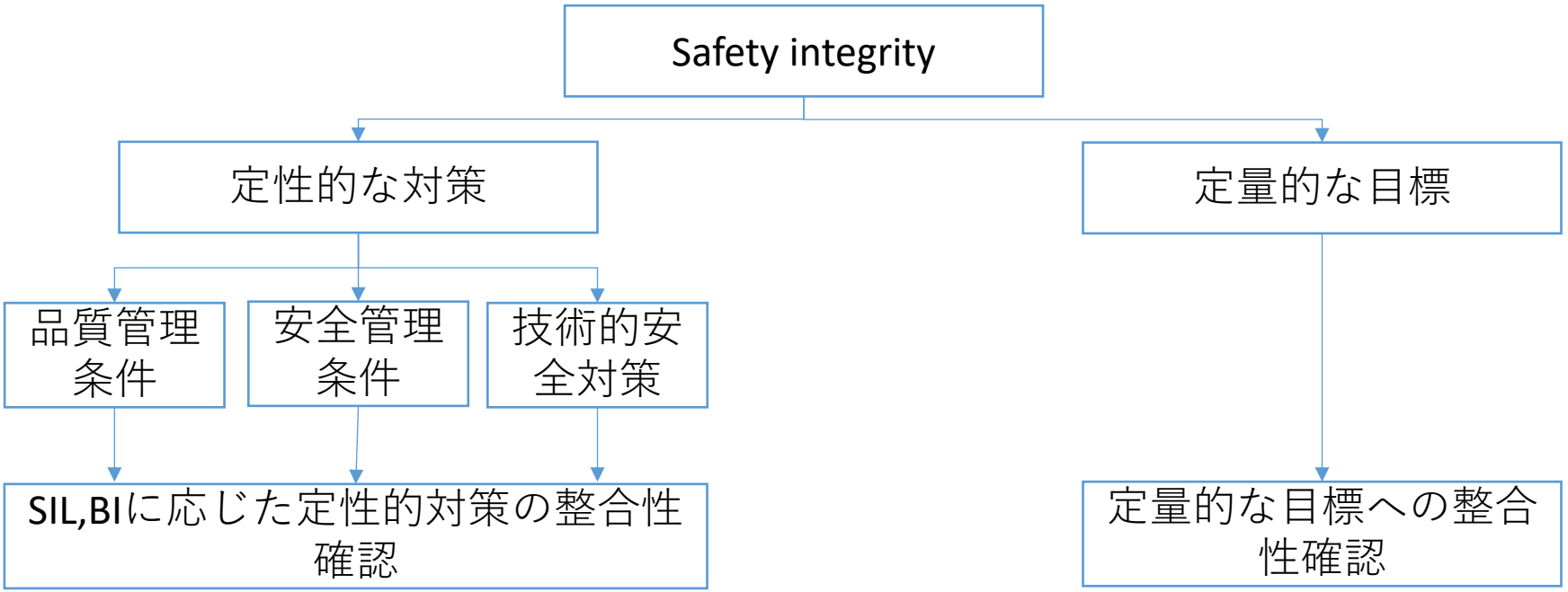
おまえはすぐそうやってな、みんな喜んでるところに水を差すからアカンねん。なんかすごいやつ精一杯やるっていうのは伝わってるやん。。

3. 安全を担保するための要素

まずそもそも論やけど、社長としては、「安全」を担保するためにどんな要素あると考えてるのか聞きたいねんけど。

そんなモン、フェールセーフや。フェールセーフが確実に働くよう設計と製作にミスがないようにするにつきてるんや。またなんや、社員株主の文句か。

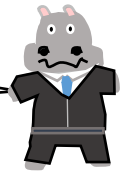
なんかわかったような、それでいて何かもやもやするような。



IEC 62278-2 Fig.11を参考

3. 定性的な対策について

定性的な対策3つあるな。社長としてどういう風に考えてんの。思想が大事なんちゃうの。



そんなモン、カバ実の担当や！ワシは経営で忙しい！

ま、丸投げですか。でもこのように考えられるのでは。

品質管理条件

The purpose of the quality management system is to minimize the incidence of human errors and to improve process performance at each stage of the life cycle, and thus to reduce the risk of systematic faults.
－IEC 62425 Ed.2 5.2
ヒューマンエラーをなくすことにより、systematic faultをなくし、安全性を担保する考え方。
(ISO 9001によるとなっているので、一般的な要求事項を中心に考える。)

安全管理条件

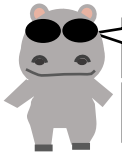
The safety management process aims at minimizing the residual risk of safety-related systematic faults and security threats. The safety management process shall be applied to all safety-related systems. However, the depth of the evidence presented and the extent of the supporting documentation will be appropriate to the degree of safety integrity required to the functions under scrutiny.
－IEC 62425 Ed.2 5.3.1
一般的な品質管理で残ってしまった安全に関するsystematic faultを最小化する。しかし機能に応じてそのレベルは変わる。→安全性インテグリティレベルに依存する。
構造的な文書化、安全ライフサイクル、役割の独立性、リスク解析手法など

技術的安全対策

リスク解析を実施し、安全関連機能の正しい実装及びそのを担保するハードウェア及びソフトウェアの実装、SRACs(safety related application conditions)としたものの担保、SILに応じた技術的要求の実装など

下に行けば行くほど、SILとの関係性が明確になってきますよね。ではSILとは何でしょう。

3. ざっくりとSILとは。。。



結構SILと関係ありそうなモンあるな。ざっくりSILとはなんやろう。

レベル感や！これくらいっていうやつや。だってレベルっていうやろ。

3.68 safety integrity
ability of a safety-related function to perform satisfactorily with respect to safety under all the stated conditions within a stated operational environment and a stated period of time
決められた運用環境及び時間における条件のもとで、当該安全関連機能が十分に機能する能力(≒危険側故障が許容できるレベルに抑えられている。)

3.69 safety integrity level
one of a number of defined discrete levels for specifying the safety integrity requirements for safety-related functions to be allocated to the safety-related systems
安全関連システムに割り当てられる、安全関連機能のためのSafety integrity要求を設定するための離散的なレベルで定義された数値。

こんな文章カバ鉄道さんにもっていったら「全然分からへん帰れ」っていわれるよ。

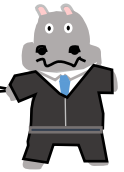
3. ざっくりとSILとは。。。

safety integrity
安全に関係する機能が、アカンようになる場合があるけど、それは影響を考えたときまあ許せる範囲に収まっていること。
そのためには、どんな影響がありそうなのか、許せる範囲がいかほどなのかは決めないとアカンよね。

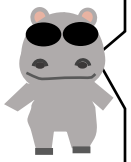
これやったらイメージできる。

safety integrity level
安全に関係する機能がアカンようになる許せる範囲は、多分年1回とか、100年に一回やったら堪忍できるというような感じだと思うんやけど、まあざっくり段階に分けたほうが便利やから、何段階かにまとめてしまおうということ。

やっぱりレベルやんけ。



3. ざっくりとSILとは。。。

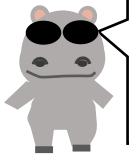


ほら見てみ。なんでレベル感が先に出てくんねん。普通に考えたら、あくまでSafety Integrityありきちゃうんか。これくらいやったら許せる、だから段階分けしたら、SILいくつっていうんちゃうんか。

社長がゆうてるの、通知簿で「５」やから、試験は100点って言ってるのと変わらへんで。試験が100点やから、通知簿「５」なんやろ。

す、推定100点。。。

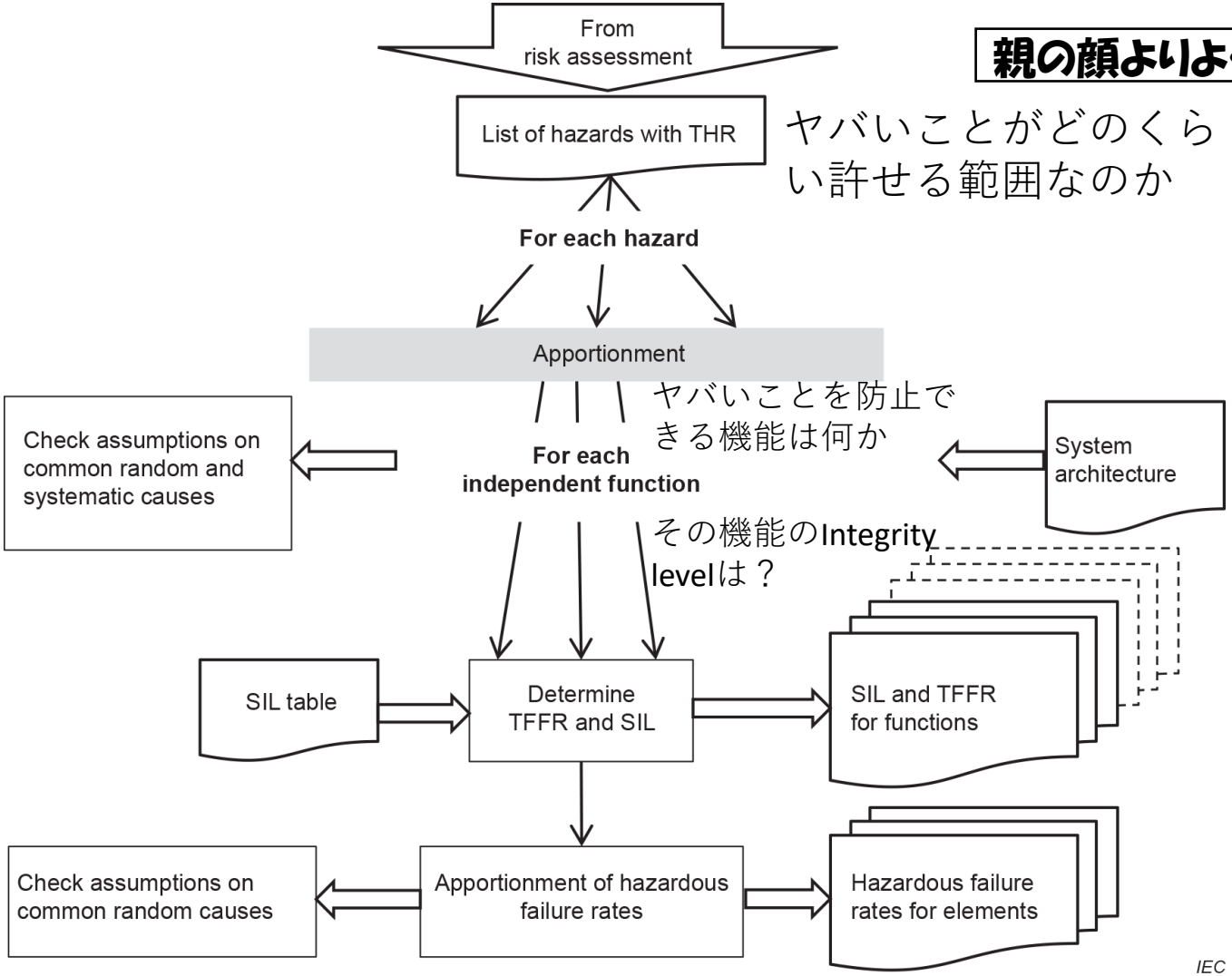
そやけどな、世の中そんなんばっかりちゃうねん。
お前さんな、目標たてる時、「82.5点取ります。」って言わへんやろ。
「通知簿で5とってきたら、ゲーム機買ったる」とかいうやろ。
やっぱりレベル感って大事やねん。
それを完全に無視するっていうのは、それはそれでピンとこーへんねん。



カバはゲームせーへんから。。そういう問題じゃないか。まあ社長の言わんとすることもわかる。

4. SILの割り当て

親の顔よりよく見る絵



IEC 62425 Ed.2 Figure A.4 より引用

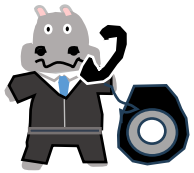
4. SILの割り当て

リスクアセスメント

いやあ、電子連動いろいろハザードあるな。どれくらいやったら許してもらえるかな。

Tolerable Hazard Rateの設定

カバ保険さん。一応今回の新製品、衝突事故や脱線事故の保険、お願いしますわ。え、利率？そりゃあその事故システム当たり10万年に一回に抑えますから保険料は。。。



Apportionment

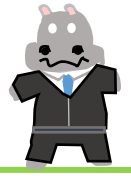
おいオマエら、各サブシステムに危険側故障許容値割り振るから。保険屋ともうねごったから。

Independent function

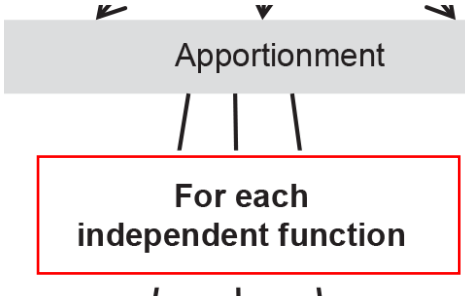
じゃあ、転てつ機の転換にXX、信号現示のにXXにしようか。だからどちらもSIL4か

あれでも、それって、論理部の演算って共通の機能ありません？

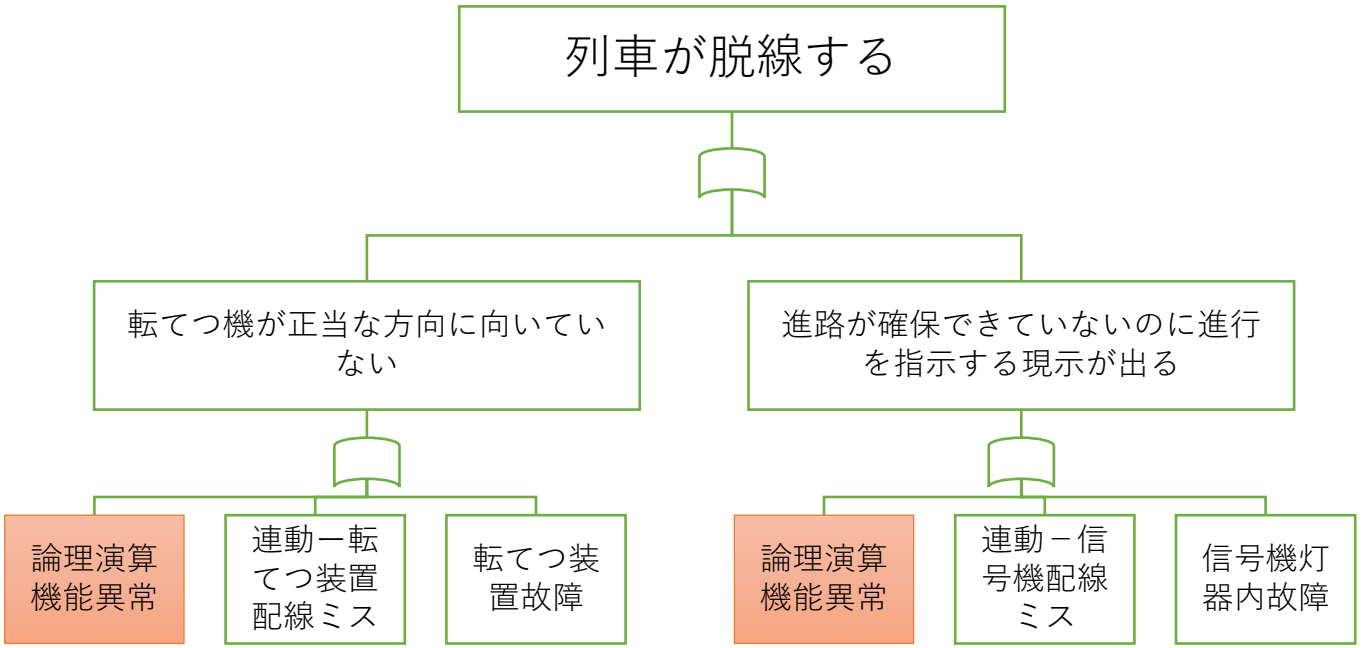
！！！！

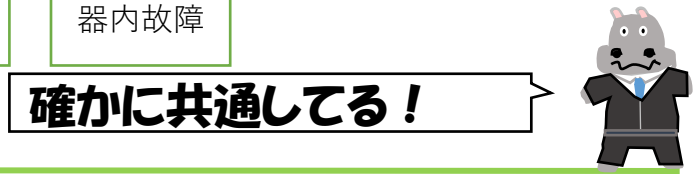


4. SILの割り当てと機能独立性



独立した機能にSILは割り当てられることに注意！





4. SILの割り当てと機能独立性

Apportionment

For each independent function

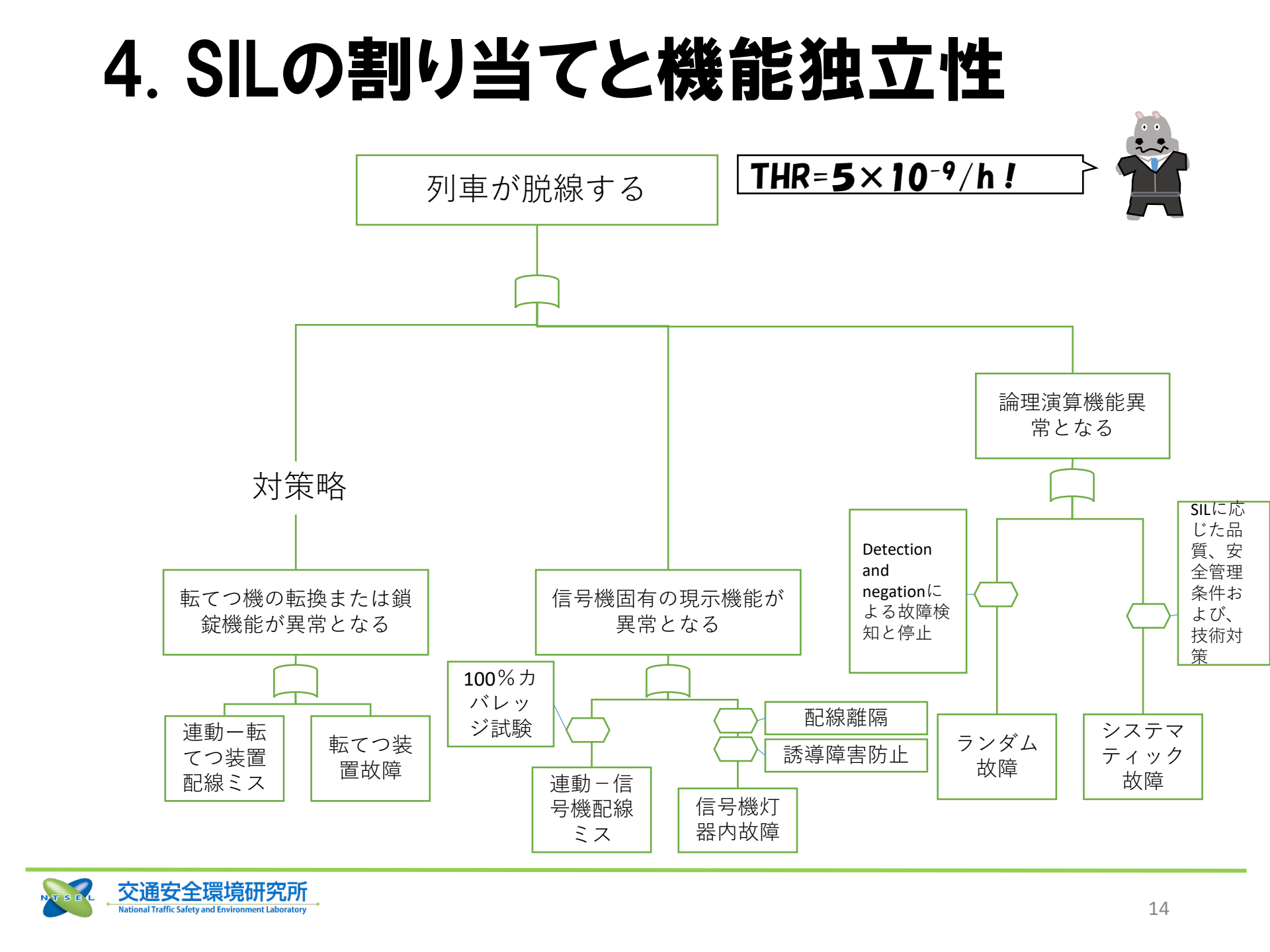
独立した機能にSILは割り当てられることに注意！

THR=5×10⁻⁹/h！

列車が脱線する

- 転てつ機の転換または鎖錠機能が異常となる
  - 連動ー転てつ装置配線ミス
  - 転てつ装置故障
- 信号機固有の現示機能が異常となる
  - 連動－信号機配線ミス
  - 信号機灯器内故障
- 論理演算機能異常となる
  - ランダム故障
  - システマティック故障

4. SILの割り当てと機能独立性



4. SILの割り当て対象

なんかなあ、これ全部割り当てんの？直観的にやけど、配線離隔のSILなんて意味あるの？実施はもちろん大事だけどねえ。。。

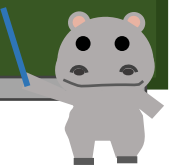
IEC 62278-2 10 Apportionment of functional safety integrity requirementsに内容がありまして、

電子モンか否か

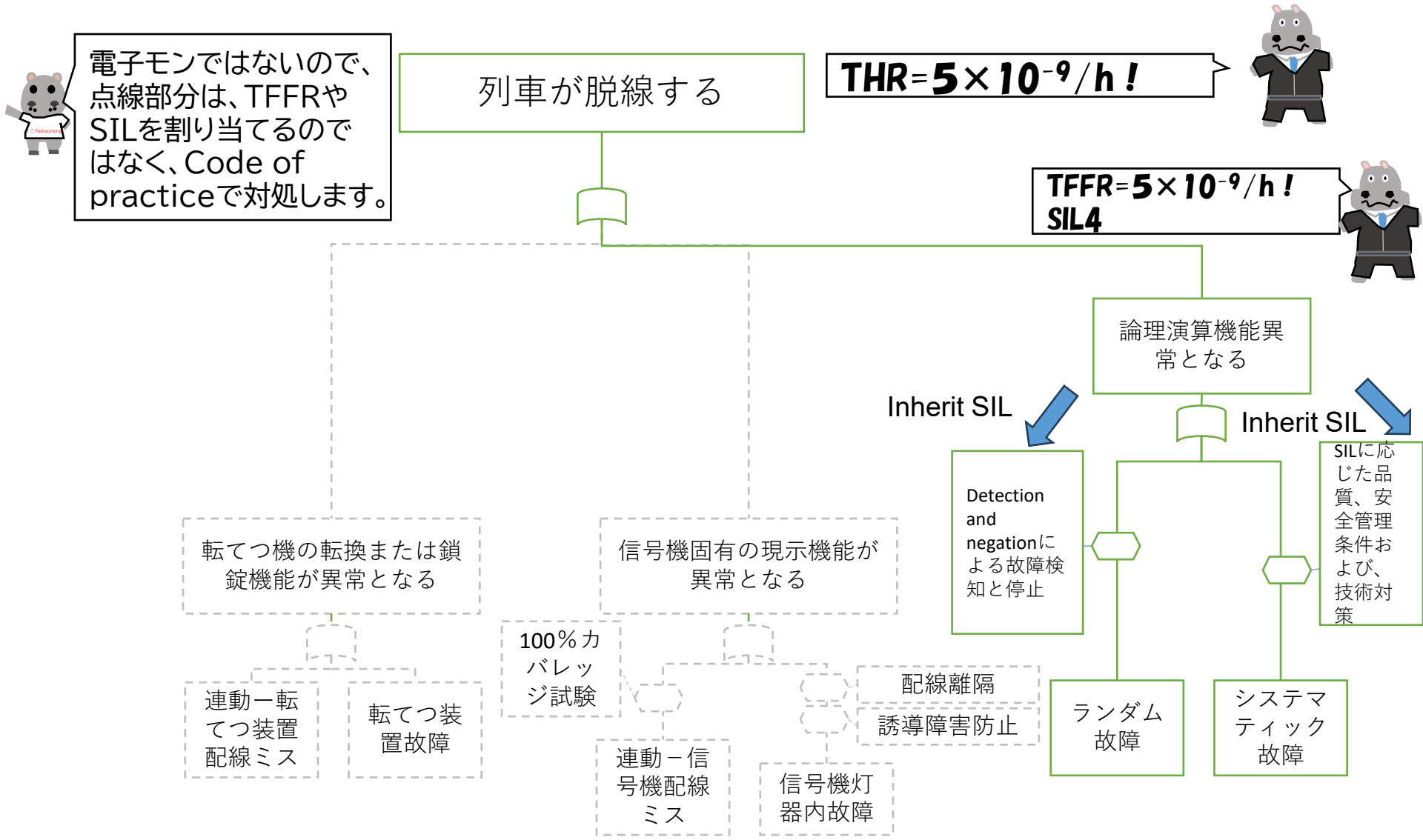
電子モンは10.2参照

それ以外は10.3参照
SIL割り当て対象外

SIL shall not be used for non-functional safety. SIL assigned to mechanical or electro-mechanical equipment shall be considered not applicable and in the demonstration process this shall be stated, as this document introduces only measures and techniques for electronic systems.

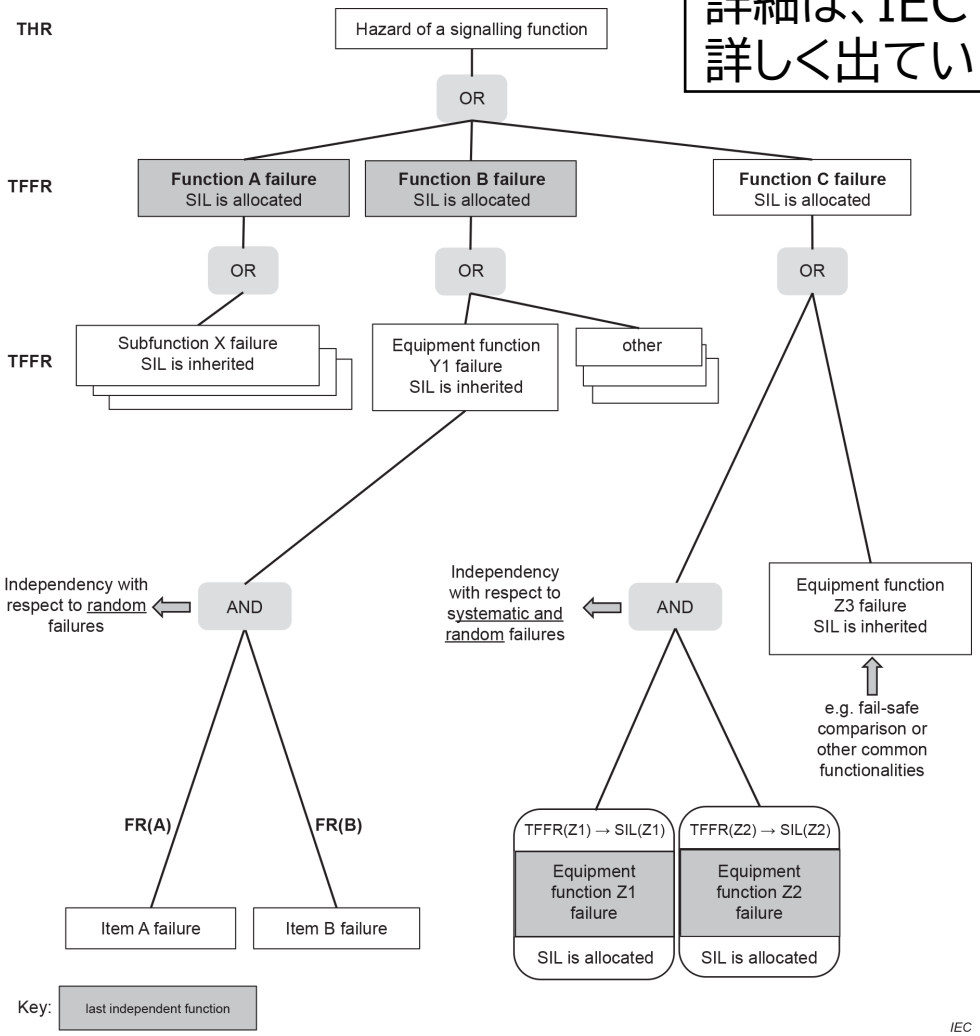


4. SILの割り当てと対象



4. SILの割り当ての詳細

詳細は、IEC 62425 Ed.2 Annex Dに詳しく出ています。

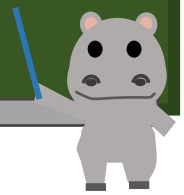


5. まとめ(アカンやつ)

最後に、こういう使い方は間違いというのが、IEC 62278-2 10.2.12にあります。
-SILは適切なライフサイクル段階でのリスク解析後に最終の独立機能に対して割り当てるものです。はじめからSIL4とか言ってもあまり意味がないです。
例： 脱線を防ぐ機能がSIL4→解析していくにつれ、独立でない機能があちこちに交じっているかもしれません。気持ちはわかりますが、どうせもう少し解析しない限り具体的な方法は出てきませんし、共通原因故障もわからないと思います。

-SILは機能安全以外、また10.2にあるように電子システム以外に使用するべきではないです。
-インテグリティ要求(=これくらいなら許容できる)を定量的、定性的に満たしても、それは関連する機能を正しく定義しているかどうかは分かりません。
-SILはシステムの特性を述べるために使うべきではありません。SIL4処理装置という表現は間違いです。すべての安全の前提条件を満足したうえで、SIL4の機能を処理するのに適した処理装置である。というのが正確です。
まあ、なかなか難しいですが、心にとめておいていただけると幸いです。

– SILs should be assigned at the level of the last independent function only after a risk analysis in the appropriate life cycle phases according to one of the risk acceptance principles or equivalent derivation. It is meaningless to assign SILs prior to completing such an analysis.
– SILs should not be used for non-functional safety, e.g. applying SILs to safety against slips, trips and falls. (10.2.1ではshall-notになっているので、強めにすべきではないと言っている。)
– Fulfilling all quantitative and qualitative integrity requirements does not guarantee that the related function is correctly defined.
– SILs should not be used for describing systems attributes, e.g. "this is a SIL 4 computer". The correct wording would be: "this is a computer capable of performing the specified SIL 4 safety related functions, provided that all SRAC associated with this computer are applied".



5. まとめ（SILとTFFRを満たせばいいのか）

SIL2の機能を実装するシステムでよく聞くのですが、TFFRが定義されており、それが満たすことが安全の証拠という議論が多くあります。

IEC 62278-2にそのヒントがあります。

あくまでSILは機能安全に関わるレベルです。壊れないから許容できるというのとは違います。
機能安全に関係する機能に定量的、定性的な要求と、そのTFFRの充足は必要ですが、安全機能はTFFRの充足だけでは十分とは言えません。

危険側故障が存在するのか、故障を検知するのか、安全側遷移の考え方など下記を参考にしていただくようお願いします。

10.2.4 Functional safety integrity and random failures
When a tolerable functional unsafe failure rate (TFFR) is defined, all the other relevant quantitative and qualitative requirements for each function shall be set, in order to fulfil the THR target defined at the hazard level.
In fact, the TFFR is not sufficient to characterize a safety-related function. The necessary functional failure model and the architectural design shall address:
– the functional unsafe failures;
– how the system is able to detect the fault if required;
– the safety design principles that assure a safe reaction;
– the safe down time (SDT, see D.3.1) if needed in the model;
– how the function exits the fault state, e.g. by restoration or entering a safe state;
– how the system contains the fault effects (system recovery, emergency procedures);
– the procedural and maintenance actions to be implemented and what is the periodicity of those actions to be implemented.
Auxiliary functions (diagnostics) and preventive maintenance should also be taken in account.