リスク解析

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！」

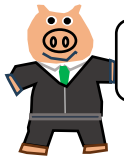
バチバチ

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



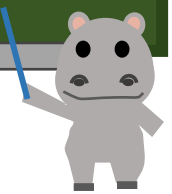
ブタ工業　社長
カバ興業を凌ぐ強い体質づくり

1．はじめに

規格では安全解析やRAM解析が重視されていますが、なぜでしょうか。
これは、計画したことが実際に出来ているかどうかを確認するのは、結局当面推定しかないということだと思います。

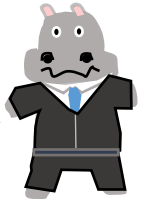
何のために、リスクの解析をするのか、RAMの解析をするのかは、それぞれの商品によって異なると思います。

一般的には、安全に対しては、「必要とされる安全機能は何か？」「その安全機能が許される失敗の頻度はどれくらいか？」「許される失敗の頻度は満たすことができているのか」「頻度で語れないものは、管理で対処するが、管理手法が決められ、そのようにできているか」ということを洗い出すのだろうと思いますが、いかがでしょうか。では、カバ興業ではどんなドタバタが起こっているのでしょうか？今回は、そのうち、どのようにハザードを処理し、確率論的なアプローチで機能を割り振り正当化することを中心に述べたいと思います。



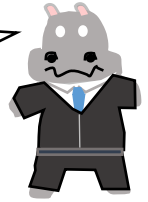
2 わからないなりに何とか。。。

社長、そろそろウチの連動装置替えたいと思っててな。。でもリスクあるよな。だいたいな、何か変える時になんか起こるのが世の常やろ。



いやあ、課長さん！確かにそれはやばいですな。やる前には、しっかり解析して、リスクは作る前にある程度押さえとかないと。。

リスクどうするかって？　いままでカバ興業は失敗ばっかりしてきたから、結構大変やろ。解析ってどうするんや。



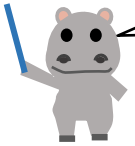
いや、そんな、ウチそんなに信用されてないんですか。。。

そうやで、おたくの技術屋のせいで、カバおくん、いつもペコペコ謝らされてるで。。社長わかってんの？
カバおくん、ストレスでどんどん太っていってるで。かわいそうやん。
そんなんでエエの、おたくら。。

は、はあ、ええっと。。。

2 わからないなりに何とか。。。

またカバ鉄道にかまされたわ。なんであいつらいっつもあんなにかましてくるねん。カバおがかわいそう同情するわって。そう思うんやったらもっと優しくしたれや。



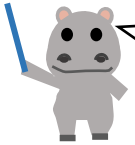
で、なぜリスクアセスメントをするんでしょうか。

そりゃ危ないのをほっとったらアカンからやろ。危なくないように何するか決めるためやろ。

じゃあ、危なくなりそうなモンが現れたら、何とか安全に持っていく機能を作っとくということを社長はゆうてるんか？

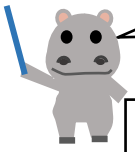
あ、でもそれ、「全部やります」「なんでもやります」って言ってこいってことなんかな？カバ鉄道は喜ぶと思うけど、ほんと大丈夫？

そりゃしょうもないことは、やらんこともあるやろ。ルールで何とかすることもあるかもしれんしな。



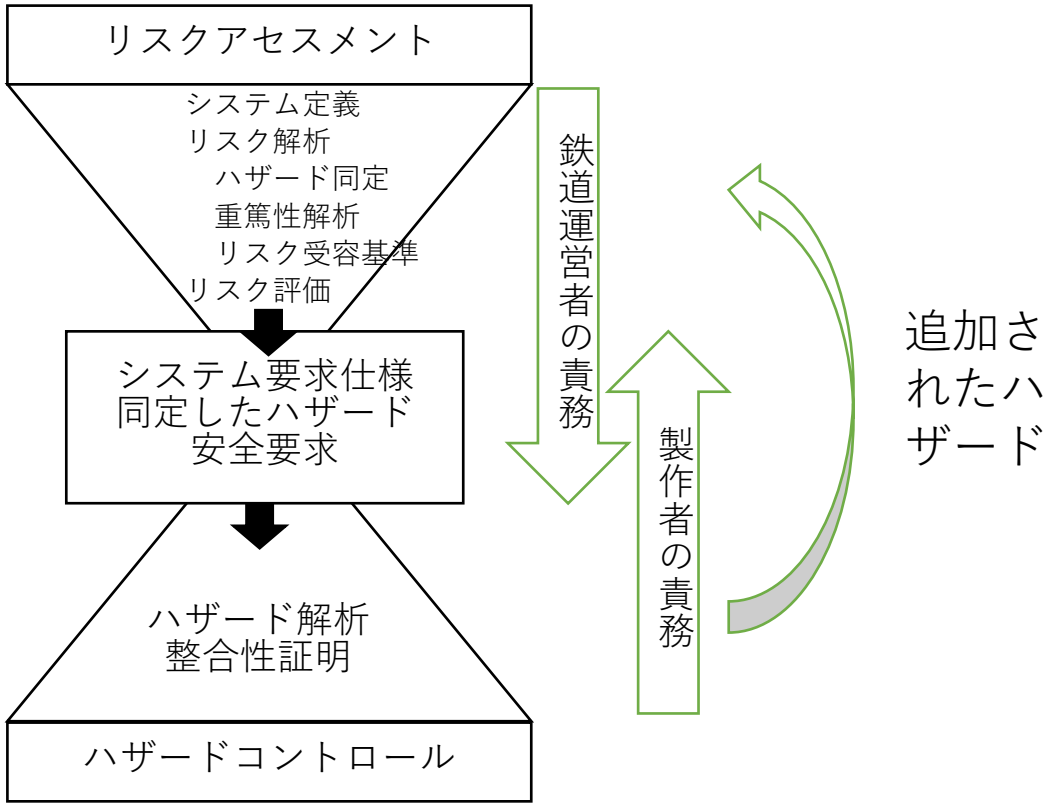
しょうもないこととやらなあかんことの分類、ルールで何とかすることをしっかり決めていけばよさそうですよね。。。

3 よく見る絵



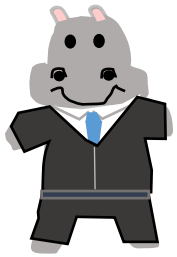
で、この絵です。よく見ますよね。

こういう絵って、わかった気にさせるためのダマシツールなんやて！



4-1 システム定義とは？

安全機能?

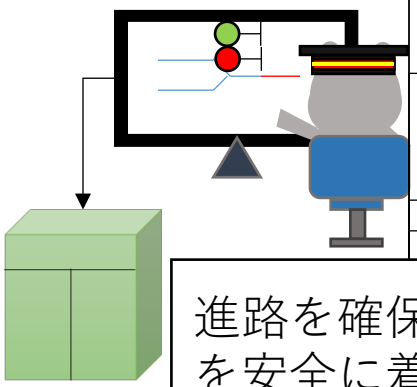


業務執行のトップ
会社を代表する
株主価値を最大化する

⇔

株主総会による監視
取締役による監視
会計士による監査

Function(Subsystem level)



- 列車検知機能
- 連鎖機能
- 連動機能
- マンマシン機能
- 端末制御機能

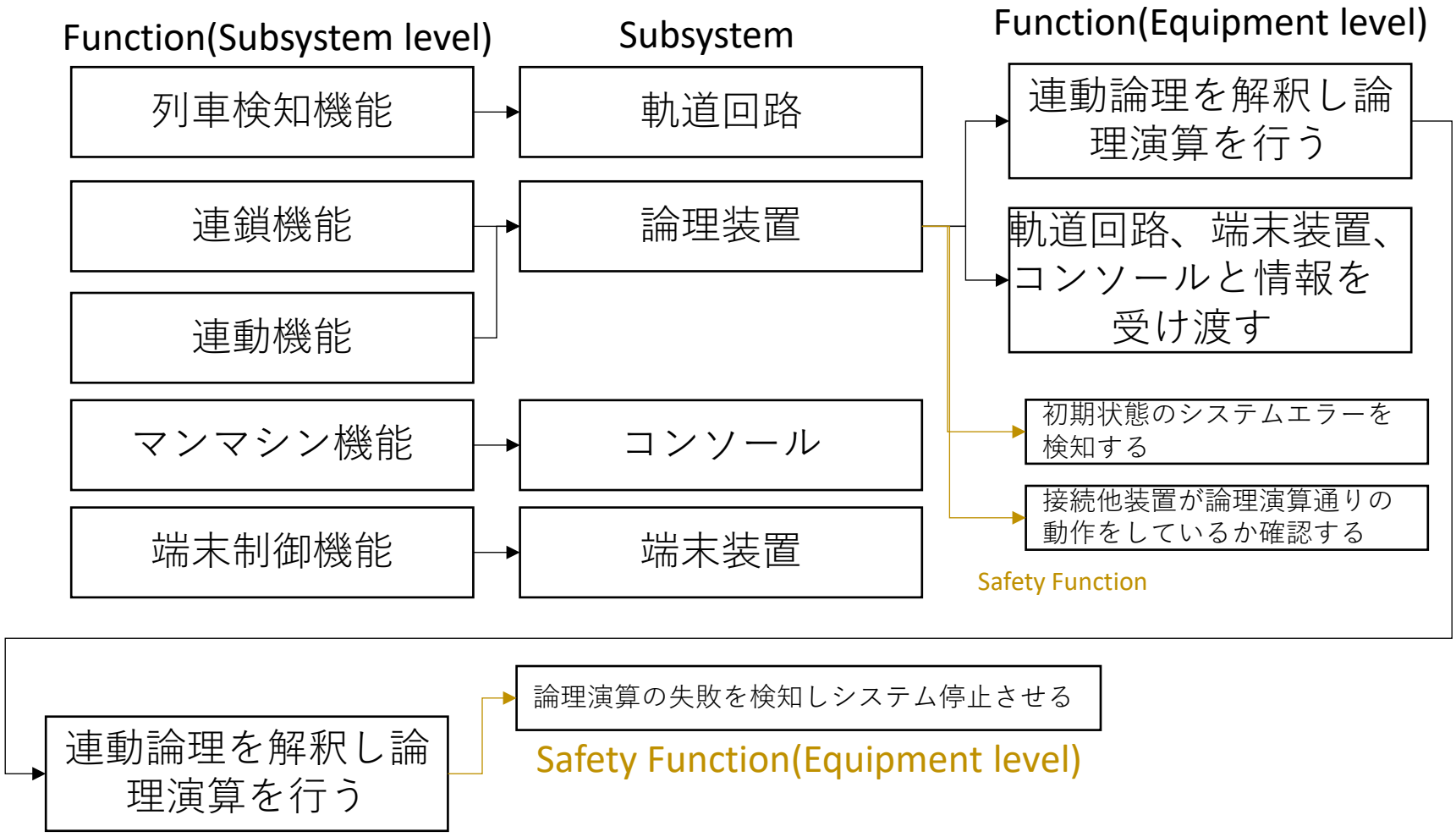
進路を確保し、列車を安全に着発させる

⇨

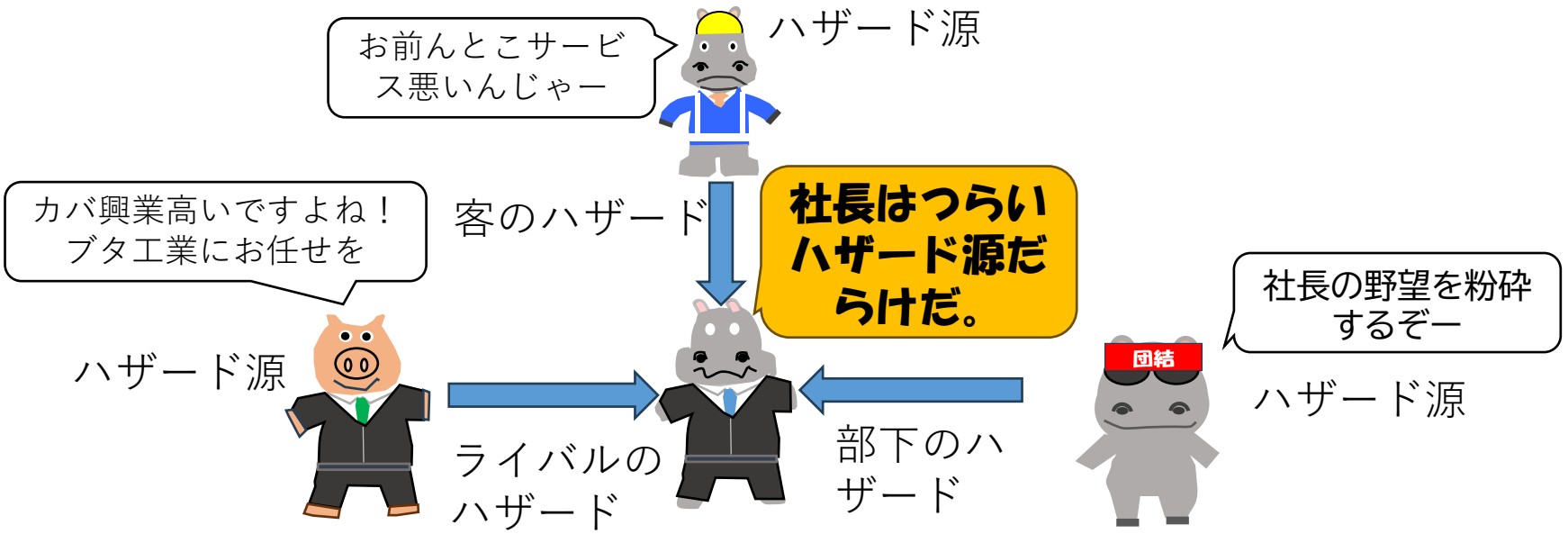
列車が衝突、追突する進路は、設定できないようにする

Safety Function(System level)

4-1 システム定義とは？


Function(Subsystem level)
Subsystem
Function(Equipment level)
列車検知機能
軌道回路
連鎖機能
論理装置
連動機能
マンマシン機能
コンソール
端末制御機能
端末装置
連動論理を解釈し論理演算を行う
軌道回路、端末装置、コンソールと情報を受け渡す
初期状態のシステムエラーを検知する
接続他装置が論理演算通りの動作をしているか確認する
Safety Function
連動論理を解釈し論理演算を行う
論理演算の失敗を検知しシステム停止させる
Safety Function(Equipment level)

4-2 外部からのハザード同定



自分のことは意外にわからんもんやけど
他からの影響はよくわかるモンや。
保守的に考えるんやったら、自分に耐性は全然なし、やられたらすぐギブアップすることを前提に考えるのもエエな。
システムでも同じや。エエもんを前提に考えるのか、なんも対策してないモンを考えるかによって、ハザード対応能力は違ってくる。

4-3 Preliminary hazard analysis

まずヤバいやつ(＝ハザード源)とヤバいこと(＝ハザード)を見つけないかんやろ。

それってPreliminary hazard analysisではないですか?

でもな、意外にPHAってどこにも定義されてないやん。

TASK 202 PRELIMINARY HAZARD ANALYSIS

202.1 Purpose. Task 202 is to perform and document a Preliminary Hazard Analysis (PHA) to identify hazards, assess the initial risks, and identify potential mitigation measures.

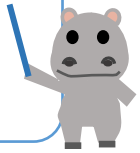
202.2 Task description. The contractor shall perform and document a PHA to determine initial risk assessments of identified hazards. Hazards associated with the proposed design or function shall be evaluated for severity and probability based on the best available data, including mishap data (as accessible) from similar systems, legacy systems, and other lessons learned. Provisions, alternatives, and mitigation measures to eliminate hazards or reduce associated risk shall be included.

MIL-STD-882E w/CHANGE 1

4-3 Preliminary hazard analysis

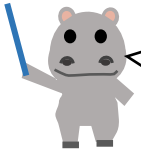
- ハザードを同定する
- 初期リスクを調査する
- 潜在的な対策を同定する

(↑安全の側面では機能安全になりうる)



ほぼ、RAMS Phase2までで行えと言われている事項と同一

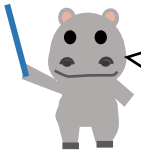
なんに活用できるねん！



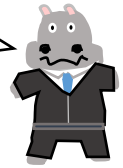
リスク対策とする機能がなんであるか、人手やルールで行う安全対策の概要を決めることができます。

PHAは、IEC 62425でも強く推奨(HR)となっているが、本文中になんであるか、何をすべきか説明がない。何を目的に実施するかをSafety Planにしっかり書いておきましょう。

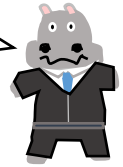
4-3 Preliminary hazard analysis　初期リスク



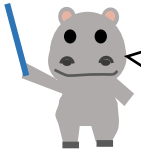
初期リスクゆうても、ウチの機械は、もうある程度できてるし。



そうですね、それをスタートにしてもいいですけど。。



出来てたらあかんのか。



アカンはずないです。でも、その安全を担保する機能、なんでいるんでしょうか。
ありきなら、それは解析の対象から外れちゃうかも。

PHAを行う際は、どのようなシステムを前提にするかによって、危険側に移行する頻度が変わります。どのようなシステムを前提にするかはあらかじめ決めておきましょう。

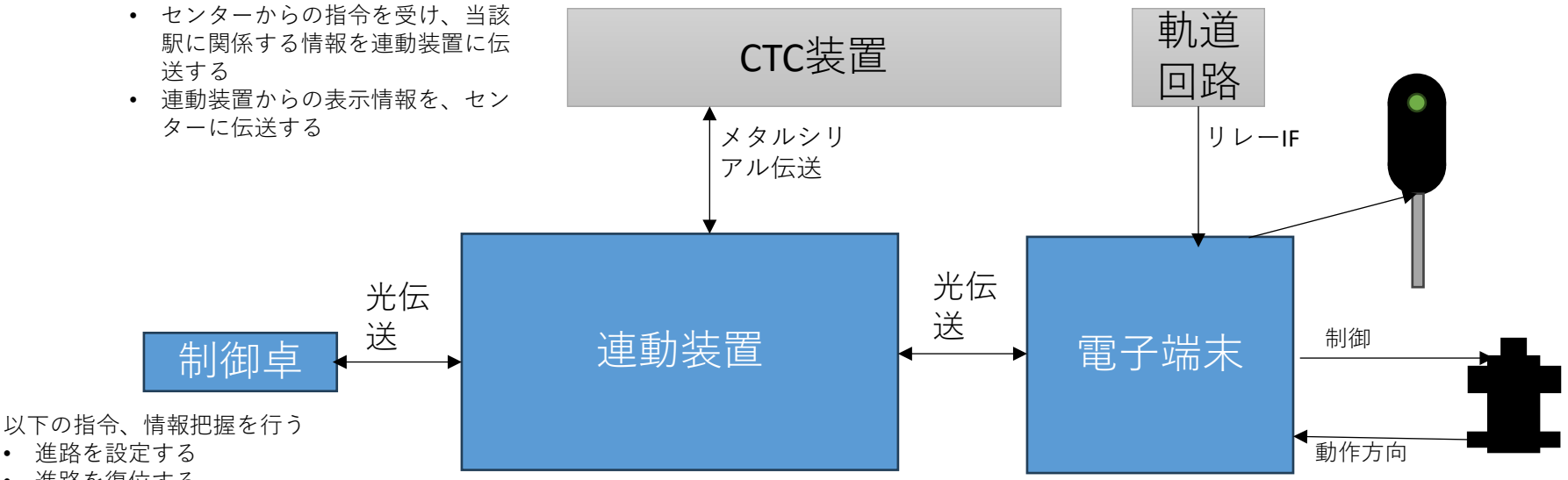
4-3 PHA手法 Interface hazard analysis

ハザードを同定するには、どんな奴がハザード源になるかや！見えるインターフェース、潜在的なインターフェース調べよか。隠れてるヤツのほうが悪質や！。

直流だけで見るな 交流で見ろ！

4-3 PHA手法 Subsystem hazard analysis

機能とサブシステムの関係性がある程度わかっている場合は分かりやすいかも。



- センターからの指令を受け、当該駅に関係する情報を連動装置に伝送する
- 連動装置からの表示情報を、センターに伝送する

以下の指令、情報把握を行う

- 進路を設定する
- 進路を復位する
- 運転方向を設定する
- 照査てこを設定、復位する
- 開通てこを設定、復位する
- 転てつ機を鎖錠する
- 転てつ機を転換する
- 列車運行状況を監視する
- 信号現示を確認する
- 列車接近するとブザーを鳴らす
- ブザーを止める
- 踏切代用てこを設定、復位する
- 解放てこを設定、復位する
- 線路閉鎖てこを設定、復位する
- 駅扱いてこを設定、復位する

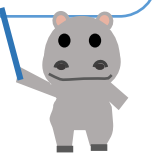
- センター制御、駅制御を選択する
- 制御情報を受ける(制御卓またはCTC)
- 制御卓に表示情報を流す
- CTCに表示情報を流す
- 進路を設定する
- 進路を鎖錠する
- 進路を復位する
- 転てつ機を鎖錠する
- 転てつ機を転換する
- 転てつ機を解放する
- 連鎖関係を計算する
- 端末と制御信号を授受する

- 連動装置からの情報をもとに、リレーをドライブする、信号機、ATS、転てつ機、踏切を制御する
- 列車在線状態を受ける
- 転てつ機、踏切の状態を受ける

これらの機能の、喪失、誤り、反転、遅延などのガイドワードで考えると網羅できそうやな

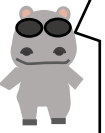
4-3 Preliminary hazard analysis

- ハザードを同定する → その都度あった方法を適用するのはどうか
- 初期リスクを調査する → 機能中心：機能喪失時の結果と重篤性
  ハザード源からの影響：影響結果と重篤性
- 潜在的な対策を同定する



これで概要の対策と必要機能が分かってくるわけやな。
PHAは、例えば「安全機能、SRACの概略を洗い出す」でもいいかもしれん。

4-4 ハザードログを作り、どのような重篤度、頻度なのか、まず考えよう



IHA、SSHAなどの要素をもとに、うまくいかなければ、安全を阻害するどんなアカンことが起こりそうか考えて、重篤度とその頻度を記入してみたらどうや。あ、そうや、前にもゆうたけど、どのようなシステムをもとに考えているかは、明確にしなあかんで。

前提とするシステム：ノンフェールセーフ汎用カバ興業CPUボードとIOポートで構成

ID	ハザード	頻度	重篤度	リスク	対処必要性	対処方法 安全要求または SRAC	対処後頻度	対処後重篤度	対処後リスク	日付及び記入者
023	進路の鎖錠に失敗する	F1	SS1							

重篤度

死亡事故あり	大けがあり	軽いけがあり	けがなし
SS1	SS2	SS3	SS4

頻度

1×10^{-5}/h	5×10^{-5}/h	5×10^{-6}/h	5×10^{-7}/h	5×10^{-8}/h	5×10^{-9}/h
F1	F2	F3	F4	F5	F6

4−5 リスクマトリックス

		死亡事故あり	大けがあり	軽いけがあり	けがなし
		SS1	SS2	SS3	SS4
1×10^{-5}/h	F1				
5×10^{-5}/h	F2				
5×10^{-6}/h	F3				
5×10^{-7}/h	F4				
5×10^{-8}/h	F5				
5×10^{-9}/h	F6				

受け入れ可能 A

やむを得ない場合受け入れ可能 C

受け入れ不可 N

4-6 対処方針を決める

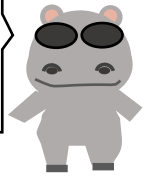
対処必要性はリスクマトリックスで決めるんやけど、どんな対処がエエんか、記入してみよか。とりあえずのアイディアでええけど、定量化しにくいモンはあとで困るで。。

ID	ハザード	頻度	重篤度	リスク	対処必要性	対処方法 安全要求または SRAC	対処後頻度	対処後重篤度	対処後リスク	日付及び記入者　備考
023-1	進路の鎖錠に失敗する(制御装置要因)	F1	SS1	N	Y	論理演算を失敗した場合検知し止める 電子端末との通信エラーを検知し、エラー時安全側制御				2025/10/22 ハッキングカバ
023-2	進路の鎖錠に失敗する(電子端末要因)	F1	SS1	N	Y	論理演算を失敗した場合検知し止める 制御装置との通信エラーを検知し、エラー時安全側制御 フィードバックループを構成する				2025/10/22 ハッキングカバ SRACとして、端末のフィードバックがTFFRに影響を与えないレベルとする

4-7 リスクマトリックスとTHR

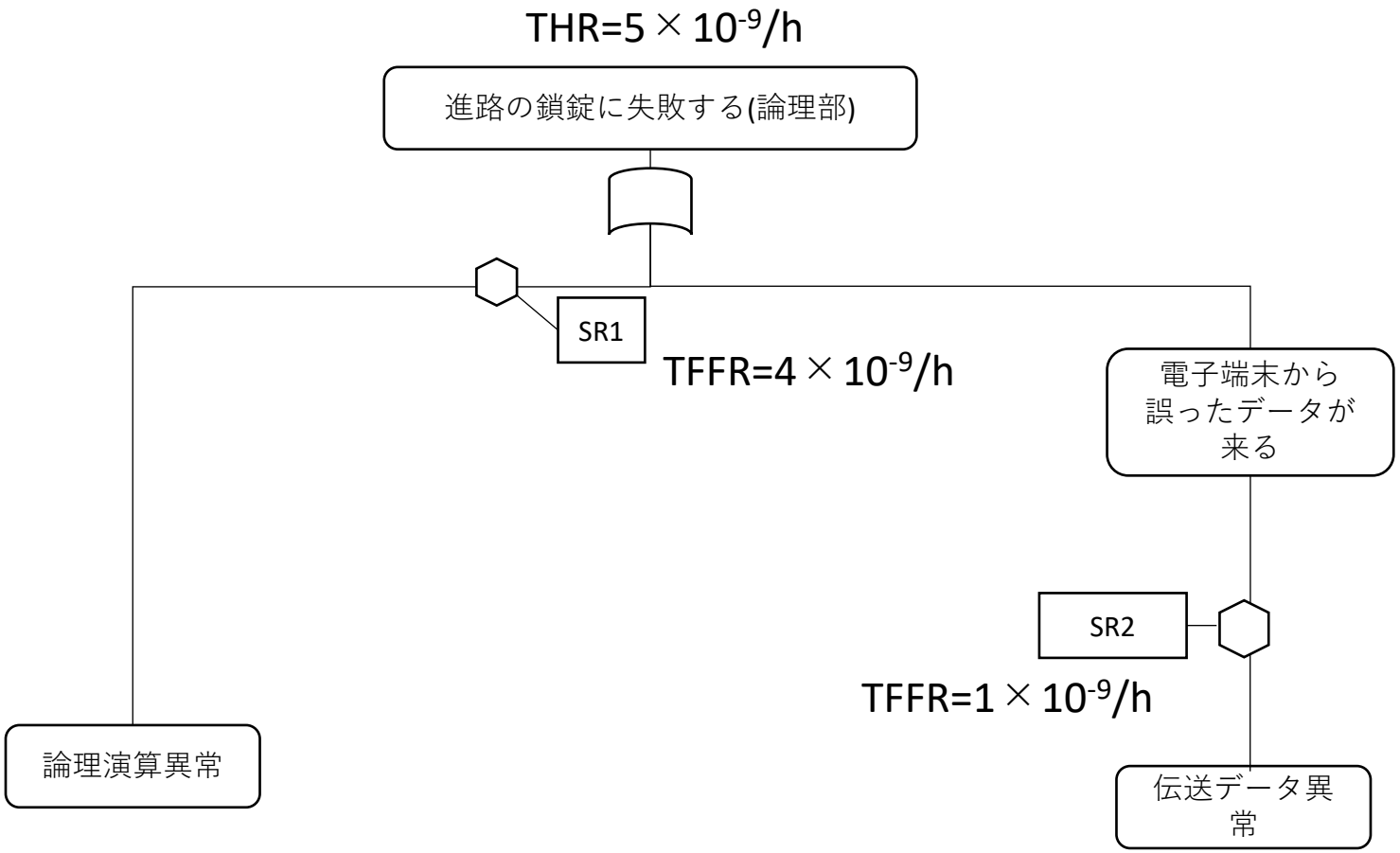
ID	ハザード	頻度	重篤度	リスク	対処必要性	対処方法 安全要求または SRAC	対処後頻度	対処後重篤度	対処後リスク	日付及び記入者　備考
023-1	進路の鎖錠に失敗する(制御装置要因)	F1	SS1	N	Y	論理演算を失敗した場合検知し止める 電子端末との通信エラーを検知し、エラー時安全側制御				2025/10/22 ハッキングカバ

THRはリスクマトリックスから5×10^{-9}/h



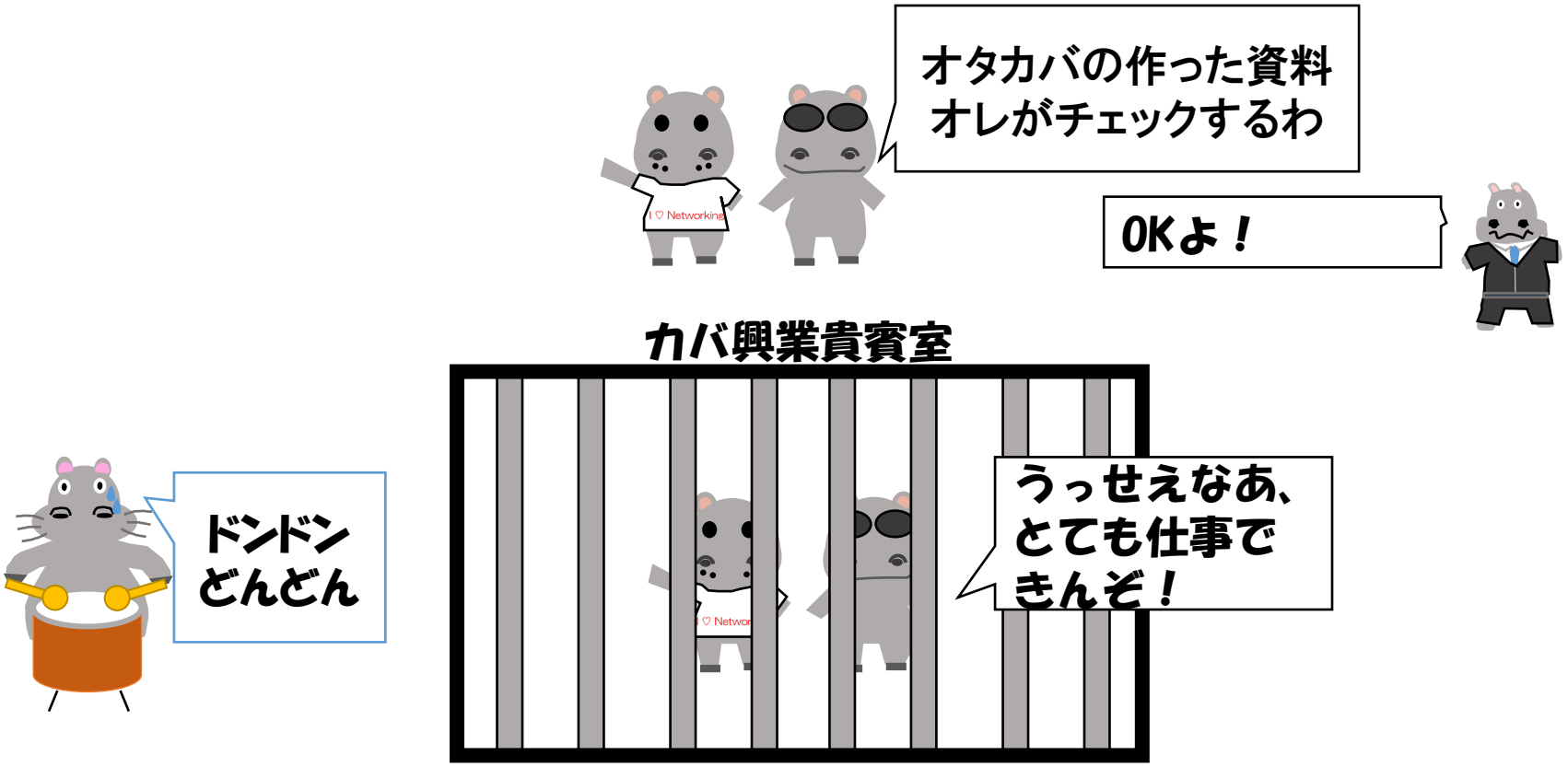
		死亡事故あり	大けがあり	軽いけがあり	けがなし
		SS1	SS2	SS3	SS4
1×10^{-5}/h	F1				
5×10^{-5}/h	F2				
5×10^{-6}/h	F3				
5×10^{-7}/h	F4				
5×10^{-8}/h	F5				
5×10^{-9}/h	F6				

4-8 FTA解析とTFFR



SR1:フェールセーフプラットフォームにて、演算異常検知、停止をする機能
SR2: 安全コードを付加して、不正常な符号を除去する機能(これは論理部が正常な前提)

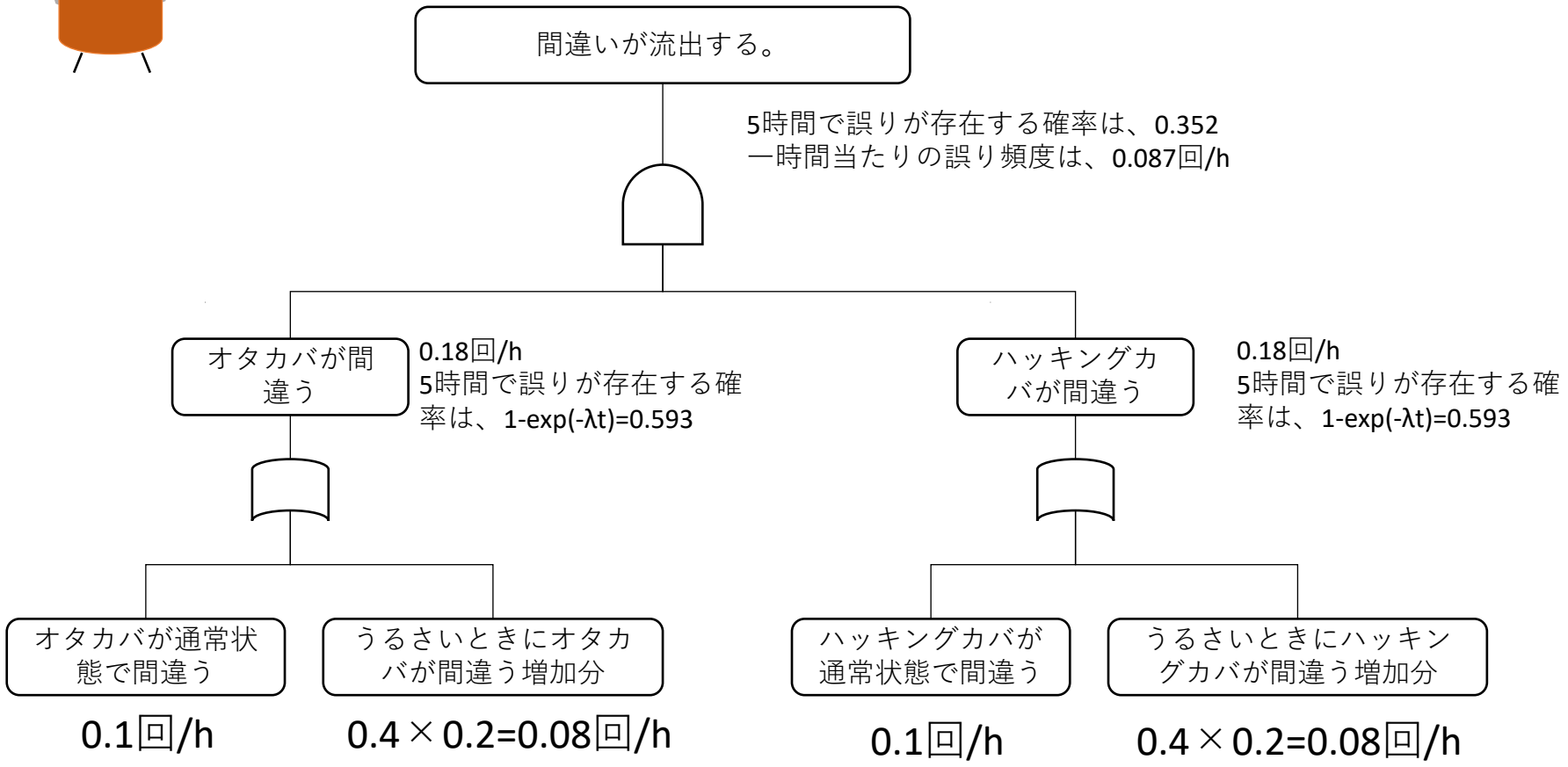
4-9 共通原因故障に注意



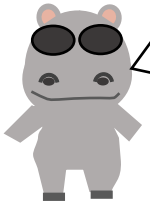
仕事は5時間。カバおの太鼓はランダムに全時間の20%が響き渡りました。
太鼓がなっている間は、間違いが0.4回/h追加されます！
オタカバの通常の誤り頻度は、0.1回/h、ハッキングカバの通常の誤り頻度は、0.1回/hとします。

4-9 共通原因故障に注意

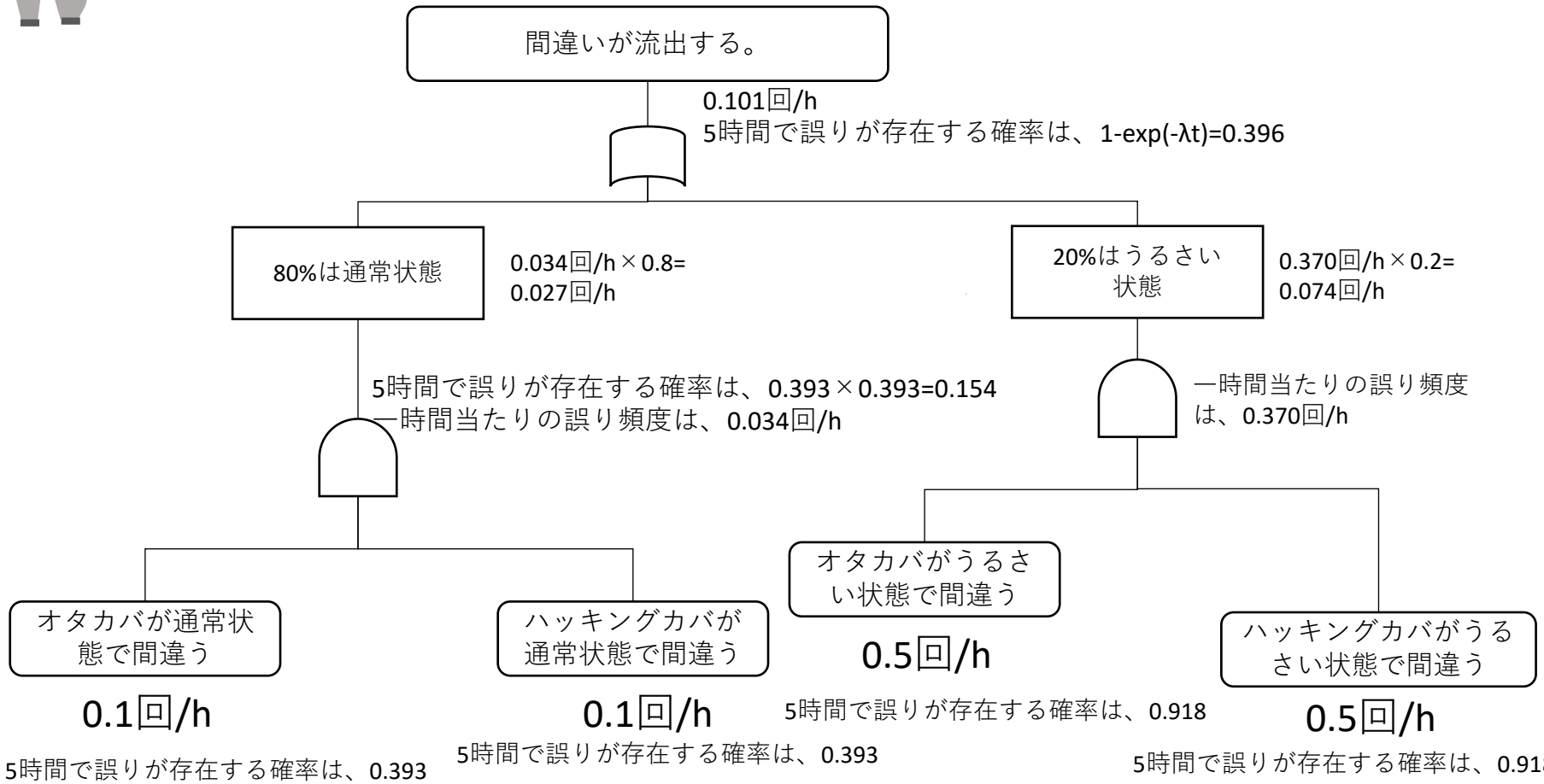
ハッキングカバとオタカバが両方間違えるとダメなんだよね。だからANDが成立するとOUTじゃないの。
間違えは、通常とうるさいときに違うから、それを配分してるよ。



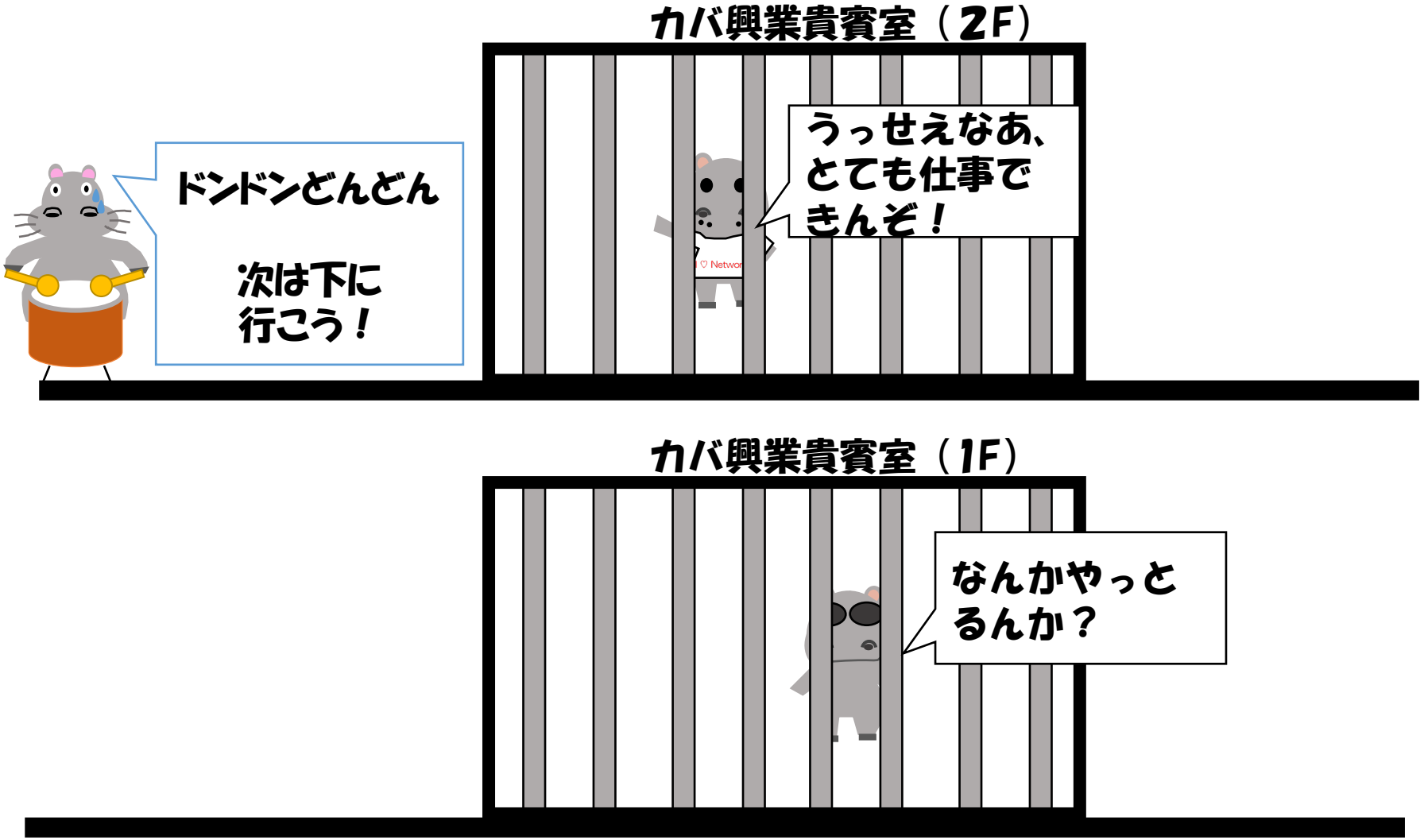
4-9 共通原因故障に注意



なんかさっきの合ってそうやけど、あれはあかんのちゃうか。
だってうるさいときは、俺もオタカバも同時にヘタるんやで。だから共通原因故障や。
共通に壊れてるときとそうでないときは場合分けして合計すべきや。

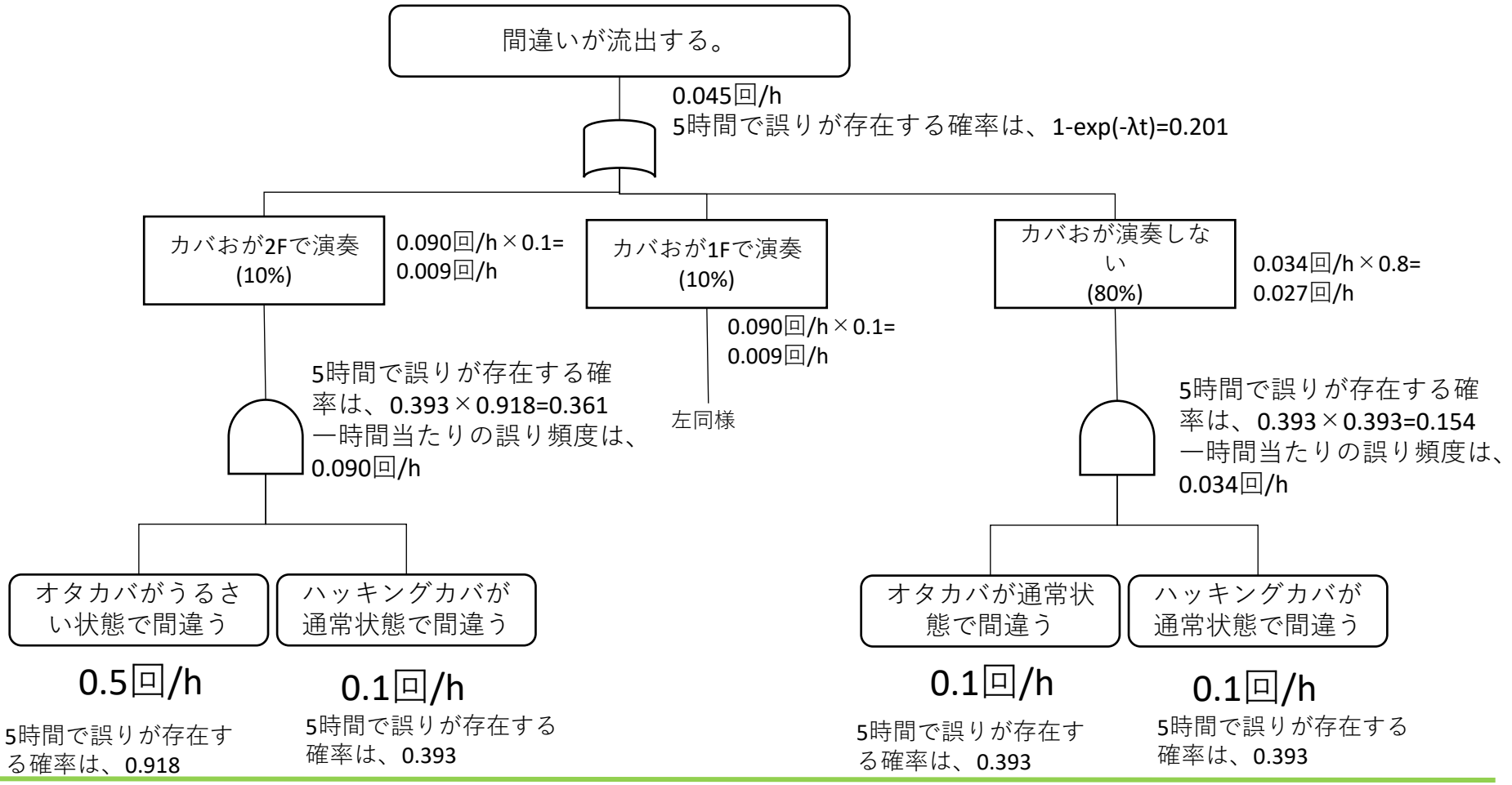


4-9 共通原因故障に注意(独立性の担保)



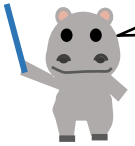
4-9 共通原因故障に注意

だいぶんよくはなるな。でももともとあいつらの間違い率は通常でも高いからな。。投資効果は微妙や。もっと注意深いカバ雇わないかんな。



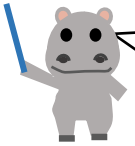
4-10 TFFRから、実際のサブシステムなどへの割り当て

機能機能って、そりゃお前さん、ある機能がちゃんと動く蓋然性とレベルを定義しろっていうのは、そりゃ大事だわさ。でもな、オレらモノづくりしてんねん。実際のモノはどう作ったらエエかっていうのがキモやねん。



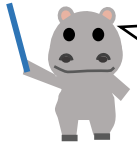
それは、その機能が動く装置の安全レベルを決めたらいいんですよね。

まあそうや、結局どのボードをどのレベルで作らなあかんかを知りたいねん。それを言えや！



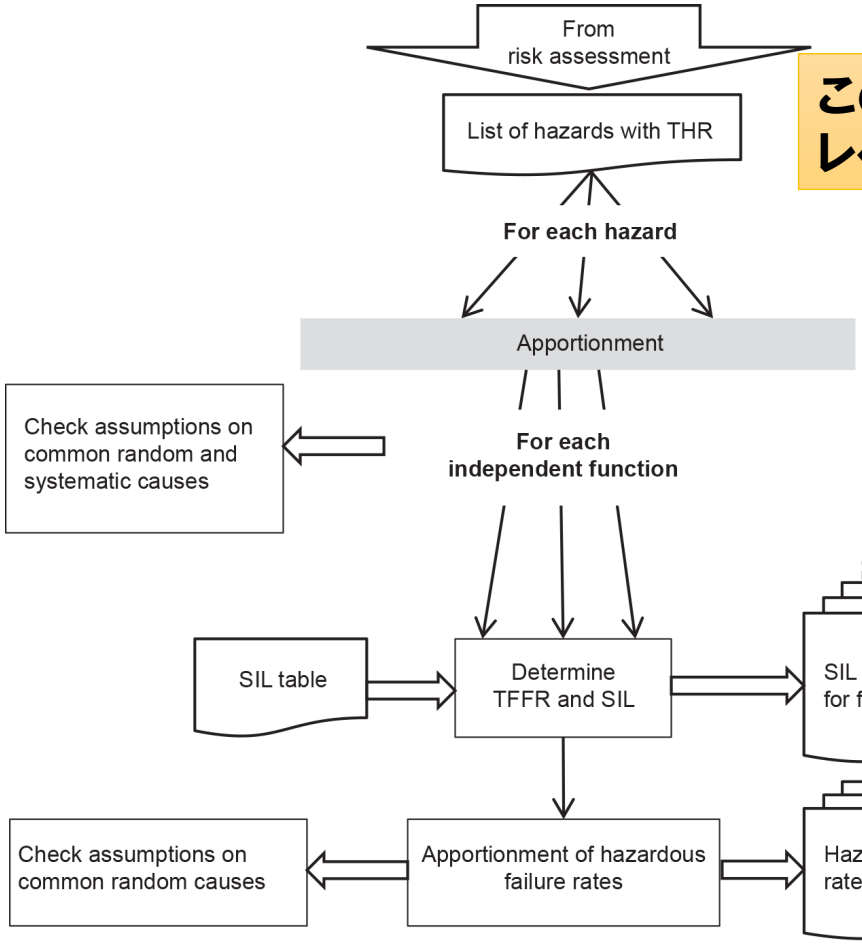
ですからですね、その機能をサブシステムに割り当てるから、その装置の危険側Failure rateと割り当てられた機能の整合性問題なので。。

だからやな、お前らの話、めんどくさいから、大事な機能はSIL4や、だからボードはSIL4やとか、乱暴な話になってお前らに怒られるねん。ちゃんと順番を追って教えろや。そういうなんかフワっとした話、もういらんねん。そんな話しは、オレら求めてないねん。



前向きな話として受け止めます。。。

4-10 ハザードから、実際のサブシステムなどへの割り当て



このようなハザードは、これくらいのレベルにしておきたいという思い

システム構成を見ながら、ハザードを防ぐ機能を割り当てる

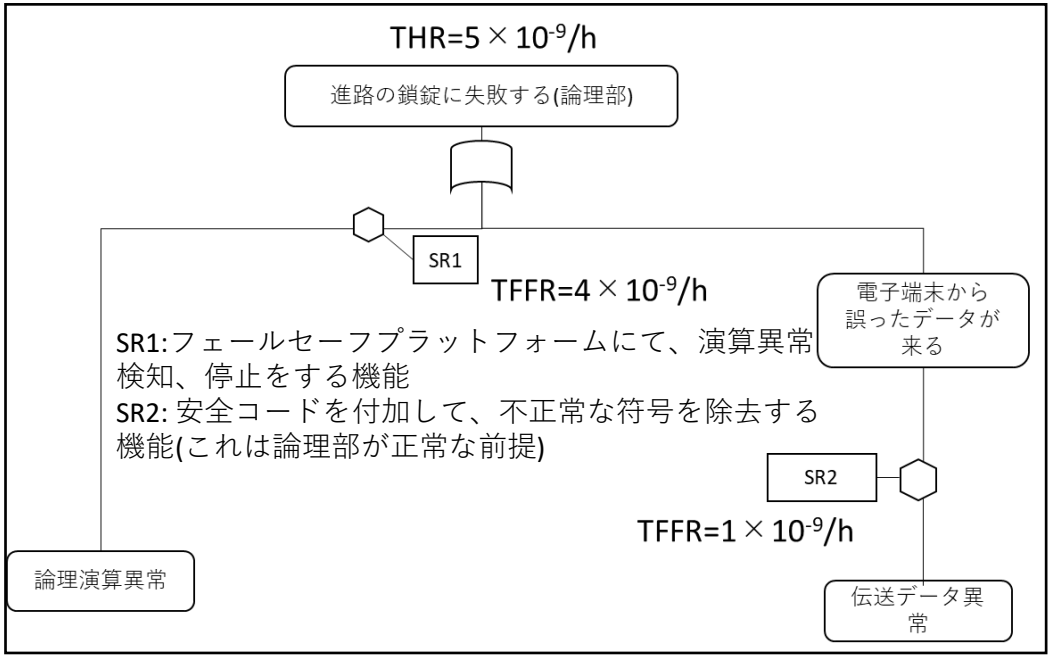
ハザードを防ぐ機能とTHRを比べて、矛盾がないようにする

ハザードを防ぐ機能と、実際に割り当てられたサブシステムの危険側故障頻度を整合させる

THR : Tolerable Hazard Rate

TFFR : Tolerable Functional Failure Rate

4-11 FTA解析とTFFR



論理部に実装される安全機能のうち、故障検知停止にかかわるもの

SR1 4×10^{-9}/h　SRx 5×10^{-9}/h　SRy 3×10^{-9}/h

論理部ボードの危険側故障頻度許容値

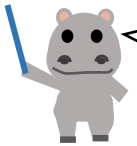
一番厳しい3×10^{-9}/hを許容値とする

論理部に実装される安全機能のうち、論理部が正常に動作することが前提になるもの

SR2:符号誤り検知 ⇨ 符号誤り見逃し率1×10^{-9}/hとなるよう安全符号長設計

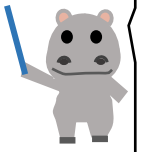
SRz:xxサブシステム故障検知 ⇨ 不安全側故障見逃し頻度をSRzと整合するよう設計

参考　前出したスライドです



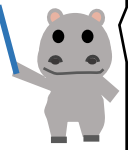
カバ社長！このスライド覚えてますか？

なんかおぼろげながら。。。



なんかこれ、今回に関係しそうな点ありますか。

ははーん。Correct functional operationとEffect of faultsのかき分けが怪しいぞ！



コワれた場合と、正しく動いて異常を見分けるのは分けて考えましょう

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。。

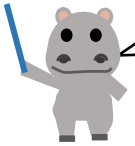
なんかおかしいぞ！

correct functional operation		Effects of faults
入ってきたデータが間違っとる	ノイズでデータが化けとる	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	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	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

4-12 TFFRとSIL

オレは今までさんざんSILSILSILSILとカバ鉄道さんから言われてきた！
しかしやな、ここまでSILって出てないやないか！TFFRという機能故障頻度しか言ってへんし、これだけでエエんちゃうんか。もうSILはイヤや。

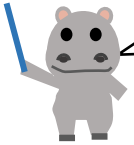


それは、まあ必要だから言っているんですよね。カバ興業のソフトウェアのバグが出る頻度は出せますか。TFFRと整合するような。。

アホかオマエ。そんなモン、各々の能力や、むずかしさ、納期によるから一概に言えるわけないやろ。

ですからですね、そこなんですよ。確率論で言いにくい故障原因は、管理レベルで何とかしなければならない。その安全レベルがSILなんですよ。その機能の実現にどのくらいの安全レベルでなければならないかということはいるでしょう。高いレベルの安全には、しっかりした管理と能力が必要ですよね。

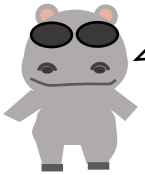
誠実なカバ興業！そんなもんすべてにおいてベストを尽くすのがカバ興業や！お客様や機能によって差別はしない！



マジで言ってるんですか。お金いくらあっても足りませんよ。メリハリは安全に必要ですよ。リソースは有限ですし。。

4-12 TFFRとSIL

SIL決めてから、TFFR決める？



逆や逆やで社長！
目標とする許容故障レートに合ったSILを決めて、そしてそのSILに合った管理するんや。

Table A.1 – The SIL table

TFFR per hour and per function	Safety integrity level
$10^{-9} \leq TFFR < 10^{-8}$	4
$10^{-8} \leq TFFR < 10^{-7}$	3
$10^{-7} \leq TFFR < 10^{-6}$	2
$10^{-6} \leq TFFR < 10^{-5}$	1

5 リスクアセスメントとハザードコントロールの実施例

①必要な機能を満たすアイテムを準備し、物理的な接続や機能的な接続をイメージする。

②発生する事象と頻度を勘案したリスクマトリックスを準備する。

③アイテムの機能が満たされなかった場合、遅れた場合、誤った場合などガイドワードに基づいて、発生する事象と頻度をイメージし、解析を行う。(FMECAなど)この際リスクマトリックスを適用する。発生する事象がハザードになりうるか検討しハザードログにまとめる。

ここまでがPHAレベルとしてよいかも

④提示した解決法は、機能としてどのように表現できるかを検討する。安全を守るための機能は「安全要求機能」となり、RAMを確保するための機能は「RAM要求」となる。SRACとなる要求は、その旨整理する。これらをハザードログに整理する。

⑤受け入れられない事象のTHR(Tolerable Hazard Rate)を決める。RAM要求についても同様。

⑥受け入れられない事象をトップ事象として、FTA解析を行う。歯止めとする安全要求機能に漏れがないかチェックする。トップ事象のTHRと矛盾しないようTFFR(Tolerable Functional Failure Rate)を決める。RAM要求についても同様。

5 リスクアセスメントとハザードコントロール

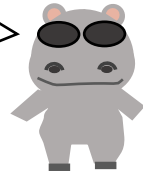
⑦割り当てられたTFFRをもとに、SILを決定する。また、この機能が実装されるサブシステム又はアイテムごとにFR(Failure Rate)を決め、実装する機能のうちSILが一番大きいものの技術的手法や管理手法を使用することを宣言する。

⑧方針が定まったのち、FTA、FMECAについて見直す。特にCCFがないかどうかを確認する。

⑨安全要求機能、RAM要求機能をTFFRやSILから勘案して具体的な解決案を決定する。

⑩サブシステムがある場合、再度サブシステムごとに①からの事項を繰り返す。

カバ興業リスクアセスメントシステム文書にこう書いてるんちゃうんか？
よう読んだ方がエエで。



6. まとめ

- ハザードの同定は、まず周囲から！周囲を知ると影響が分かります。
- PHAは何でしょうか？まず概略のリスクを判定し、対策方針を決めます。
- ハザードログは、PHAで同定したリスクを記載し、判定結果を述べ、対策方法を記載した後、リスク解析を行いその対策方法で問題がないかを記載していきます。常にアップデートが必要な図書です。
- 安全は機能だけでは守れません。そのレベルを同定する必要があります。もちろん機能で何とかする場合と、ルールで何とかする場合があります。
- レベルの同定は一般的にTHRを決め、それに対応するTFFRを決めていき、その機能がどのサブシステムに割り当てられるかで、TFFRと矛盾しないサブシステムの危険側故障頻度を決めます。
- サブシステム以降についても同様の解析が必要です。