危険を探し･見極める ～リスクの解析とアセスメント～

（RAMS 第三段階）

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 主席研究員

森　崇

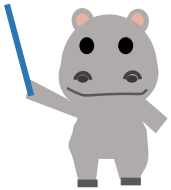
登場人物

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が生命の危機です」

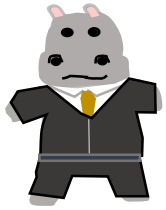
カバ鉄道　電気課長
口癖：安くてエエもん持って来い！

カバ興業　技術　オタかば
「面白くなければ技術じゃない」

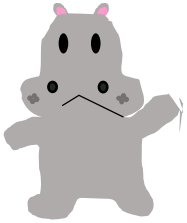


謎のフリーコンサル
なぞカバ
「知識は力！管理は必然」

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」



大蒲教授
「ソフトウェアは作法である！」



カバ興業の協力会社社員

「請負は、請けたら負け」

カバ興業設計課長　カバ実
「みんなできるようになりましょう」

前回のまとめ

RAMSの第二段階はシステムの数値的目標を定め、システムの要求の予備的なハザード分析を行うことにより、システムの実現の見込みをつけます。
そして、安全やRAMの計画を立て、明文化しておきます。

次の第3段階は

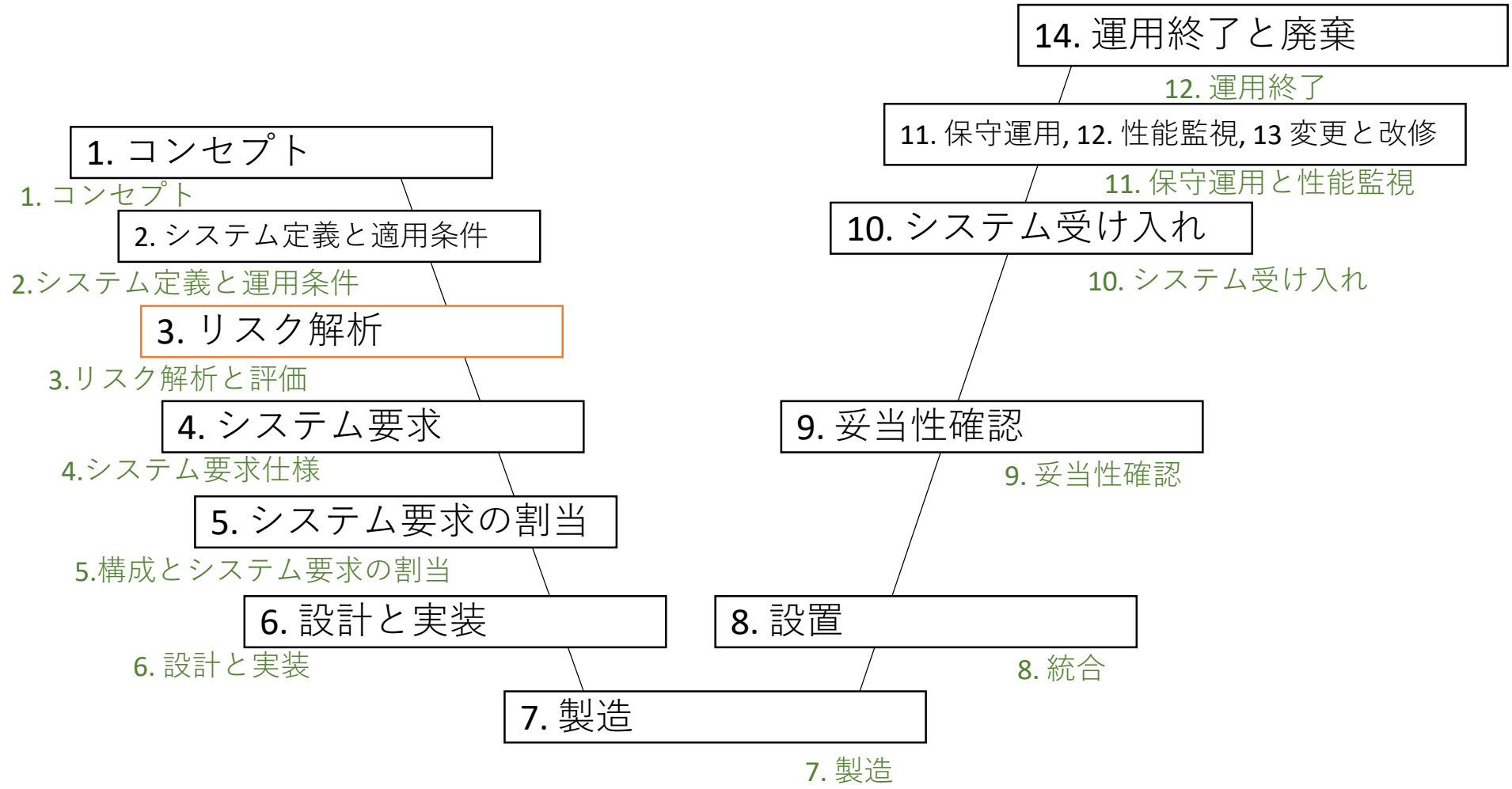
Phase 3 : Risk analysis
(IEC 62278)

Phase 3 : Risk analysis and evaluation
(EN 50126-1)

「リスク解析と（評価）」
と題がついています。

IEC 62278 5.2
EN 50126-1 6.2

全体のRAMSのライフサイクル



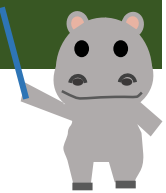
*枠内はIEC 62278, 緑字はEN 50126-1による定義

この段階で要求されていること

3-1 ハザード、RAMへの悪影響がある要因（以下望ましくない要因）を抽出する。
3-2 望ましくない要因のヤバさ加減を把握する。
3-3 望ましくない要因をどうするか決める。
3-4 望ましくない要因を記録に残す。

3-1望ましくない要因の抽出

3-1 ハザード、RAMへの悪影響がある要因（以下望ましくない要因）を抽出する。
3-2 望ましくない要因のヤバさ加減を把握する。
3-3 望ましくない要因をどうするか決める。
3-4 望ましくない要因を記録に残す。



3-1 望ましくない要因の抽出

IEC 62278 6.3.3.1
EN 50126-1 7.4.2.1-1

お前ら、カバ興業に望ましくない要因って何もないやろ。

倒産するかもしれない。給料不払いになるかもしれない。残業代くれないかもしれない。同僚が辞めるかもしれない。休みが取れないかもしれない。必要な本や情報を買ってもらえないかもしれない。開発ツールが古い。ハッキングされるかもしれない。もうアホみたいに望ましくない要因はあるんですけど。。

お、オレらカバ興業一家やないか。

おやつにカバ印アイスをくれない。ケーキもほしい。
というのも足しときます。

はあ、前途多難で透明カバになりそうやな。会社も消えてしまうわ。しかしホンマ、これで全部洗い出せてるんやろか。今はオタカバの意見しか聞いてないし。。カバおは全然仕事と関係ないこと言うし。。。このままやったらブラック企業一直線や。それはもう今のご時世ではアカンしな。。。

3-1 望ましくない要因の抽出

IEC 62278 6.3.3.1
EN 50126-1 7.4.2.1-1
IEC 62425 A.4.1.1
EN 50129 A.4.2.3

経験的な(empirical)抽出と、
創造的(creative)もしくは演繹的(deductive)な抽出

うちにはカバおが全部今までのハザード等をメモっているので、大丈夫やな。今までの資料見直して、関係するものを洗い出したらええな。

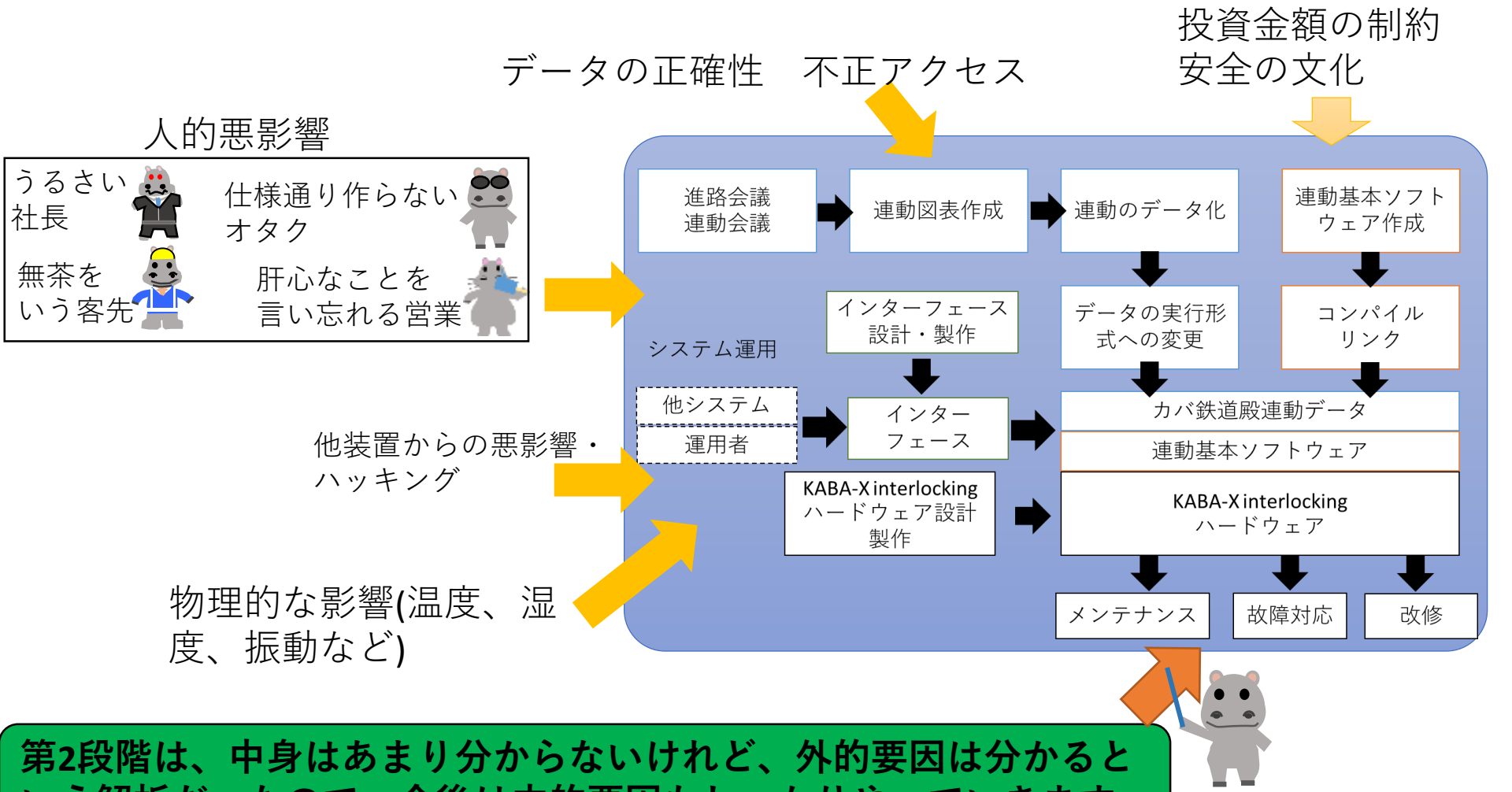
その辺はお任せください。経験的なものはすべてメモってます！～

なかなかよく管理されていますが、今までのハザードではないものは含まれていないですよね。そのために、新しいハザードを抽出する必要がありますよ。brain-storming, structured what-if studies, HAZOP,FMEAが例に挙げられています。これらは創造的手法とか演繹的手法と言います。

皆で発想をつなげていくブレーンストーミングなんかも有効なんやな。

IEC 62278 6.2.3.2 a)

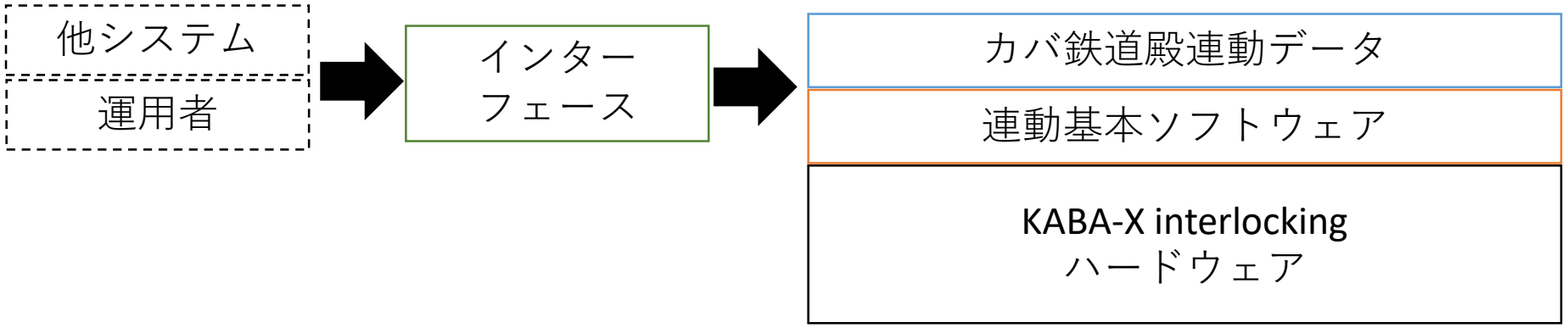
3-1 第二段階との違い

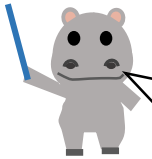


第2段階は、中身はあまり分からないけれど、外的要因は分かるという解析だったので、今後は内的要因もしっかりやっていきます。

3-1故障に着目して望ましくない内容を出す

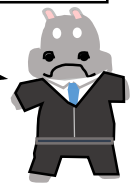
IEC 62278 6.3.3.1
EN 50126-1 7.4.2.1-1
IEC 62425 A.4.1.1
EN 50129 A.4.2.3

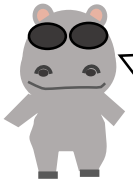




うまく動作しないときどうなるかっていうのは、まあハザード解析の王道ともいえますね。FMEA(Failure Mode and Effective Analysis)です。

うちの装置がうまくいかんやと！そんなことはありエヘンわ！うちの社員が精魂を込めて設計して製作してくれてるねんで！永久不滅や！

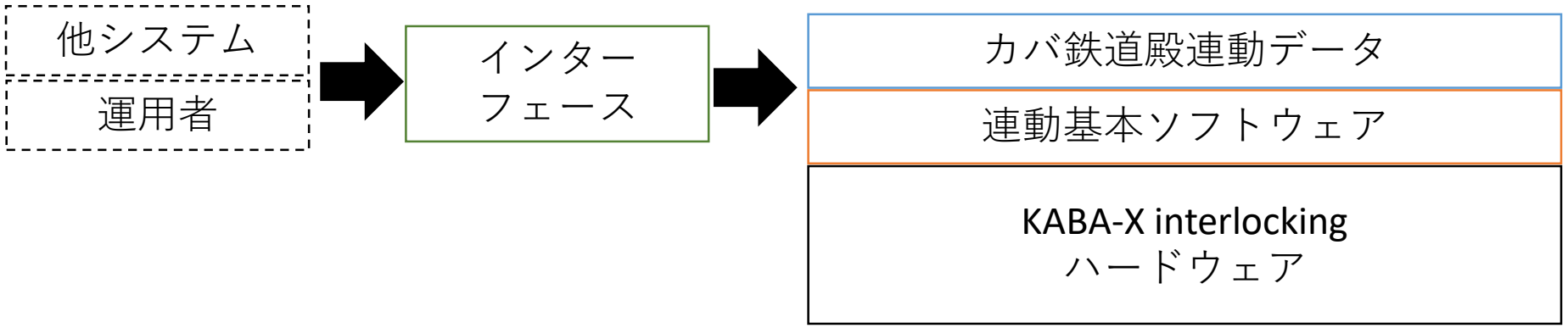


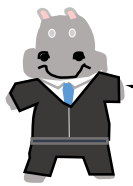


社長。。そういってくれるのはうれしいけどな、カタチあるモンはつぶれるし、だいたいいつまでもツブれんかったらだれも更新してくれんで。ツブれてもお客さん死なしたらいかんで。

3-1故障に着目して望ましくない内容を出す

IEC 62278 6.3.3.1
EN 50126-1 7.4.2.1-1
IEC 62425 A.4.1.1
EN 50129 A.4.2.3





でも、まだ中身の設計終わってないですよ。どんな故障が起こるなんて、分かるはずないじゃないですか！

分らんなりに何とかするのが技術屋ちゃうんか。オレは秘策あるけどな。

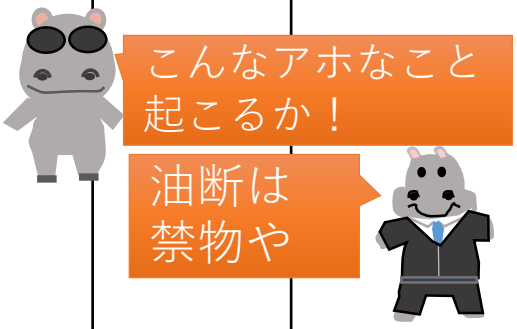
社長の目が濁っているよ。あれは全く何も考えていないときの目だよ。

費用を一番かけずに実現すると、どのような事象が発生するかのモデルで考えて、その対策を打っていくのはどうでしょうか。例えば全部転てつ機も信号もカバ興業のみんなで力合わせて手動でやるとか。。。

3-1 故障に着目した要因の抽出

IEC 62278 6.3.3.1 a)
EN 50126-1 7.4.2.1-1
IEC 62425 A.4.1.1
EN 50129 A.4.2.3

部分	サブシステムレベルの事象	詳細化	上位レベルでの望ましくない事象と重篤性	頻度	対策
連動ハードウェア	処理装置の停止	信号機に進行を指示したままでシステム停止	追突 Catastrophic	考えられる	システム停止した場合、信号機を停止現示にする
		信号機が停止になったままシステム停止	運行不能 Critical	考えられる	所定の稼働率を確保する
		列車検知しない状態てシステム停止	追突 Catastrophic	考えられる	システム停止した場合、信号機を停止現示にする
		列車検知状態になったままシステム停止	運行不能 Critical	考えられる	所定の稼働率を確保する
		転てつ装置転換途中にシステム停止し、信号機進行現示	脱線 Catastrophic	考えられる	システム停止した場合、信号機を停止現示にする
		転てつ装置逆方向鎖錠でシステム停止し、信号機進行現示	追突 Catastrophic	考えられる	システム停止した場合、信号機を停止現示にする
		転てつ装置解錠不能	運行不能 Critical	考えられる	所定の稼働率を確保する

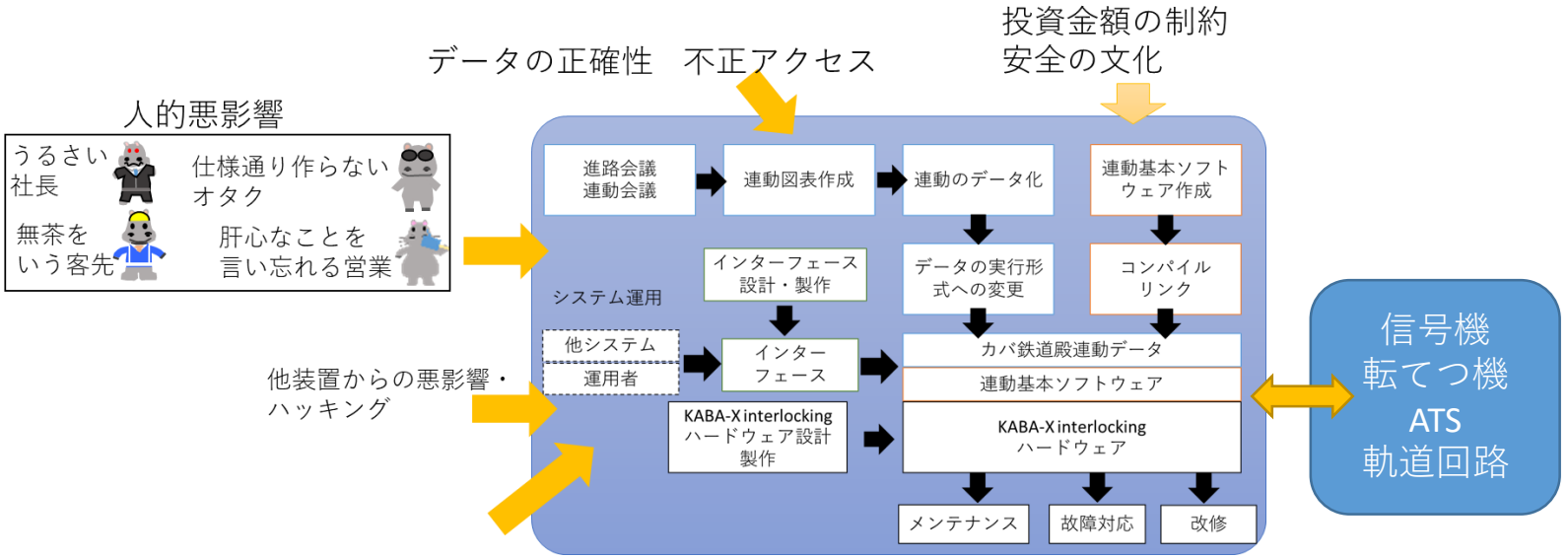


3-1 望ましくない要因の抽出

IEC 62278 6.3.3.1 b)
EN 50126-1 7.4.2.1-1
IEC 62425 A.4.1.1
EN 50129 A.4.2.3

もう少し簡単な方法ないんか。FMEAとか難しそうや。

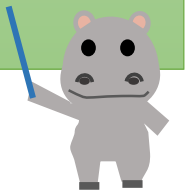
そうですねえ。。HAZOPの考え方使ってみたらどうでしょう。



情報が流れてますけど、この情報が、来なかったり、間違ってたり、順番が逆転してたり、遅かったり、早すぎたりしたらと考えてみればどうでしょう。衝突、脱線や運行不能以外にも何か見えてくるものがあるんじゃないですか？

3-1 ここまでのまとめ

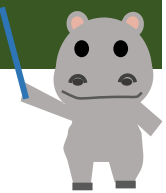
望ましくない事象の洗い出しは
〇経験的手法と
〇創造的または演繹的手法
があります。これは相互補完的で、どちらの方法も採用する方が好ましいです。



3-2 ヤバさ加減を把握

3-1 ハザード、RAMへの悪影響がある要因（以下望ましくない要因）を抽出する。
3-2 望ましくない要因のヤバさ加減を把握する。
3-3 望ましくない要因をどうするか決める。
3-4 望ましくない要因を記録に残す。

ヤバさには、起こる頻度と、結果の重篤性があります。
起こる頻度から先に説明します。



IEC 62278 6.3.3.1　c)
EN 50126-1 7.4.2.1-4

3-2 ヤバいこととは

社長、カバお君の評価、どうしているんですか？

ウチは、野球と同じで3アウト制や。3アウトになったらチェンジや。

この前反省していませんでしたっけ。社員を大事にすると。でもまあ、**同じ失敗を繰り返す**のは困りますよね。

まあ、失敗を繰り返さないための対策っていうのはいるな。

しょうもない失敗はどうですか。例えば机にアイスをこぼしたとか、メモに少し誤字があったとか。

まあ、そんなものは注意すらせんな。それはまあ、**回数が多かっても会社の経営にはほとんど関係ない**わけやしな。。

IEC 62278 6.3.3.1　c)
EN 50126-1 7.4.2.1-4

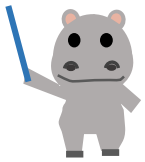
3-2 ヤバいこととは

もしですよ、カバお君が会社のお金を横領したらどうですか？

お、おまえ、なめとるんか！そんなことありえへんやろ。カバおに限ってそれはないぞ！

しゃちょおおお～　一生ついていきますからアイスください！

でもまあ、横領やったら、クビにせなアカンやろうな。ミソギが済んだらまた雇ったるけどな。カバ興業は家族やから。。



やっぱりそうですよね。**<u>一回でもアウトのこともあれば</u>**、**<u>何回やってもセーフ</u>**なこともある。それはまあ、会社経営への影響が違うからでしょうね。

IEC 62278 6.3.3.1 c)
EN 50126-1 7.4.2.1-4

3-2 ヤバいこと度合い

結果の重さ

注：イメージです！

リスクが大きい

ハッキングカバがプログラムで
バグを出して錯誤信号を出す

カバおがプログラムでバグを
出して錯誤信号を出す

どう考えてもだめ

カバおが会社の金
をくすねる

どうしようもなければ仕方ない

条件あるがOK

問題ないんじゃない？

カバおがアイスで
机を汚す

起こる頻度

IEC 62278 6.3.3.1 c)
IEC 62278 4.6.2.2

3-2 ヤバいことの頻度は

頻度	解説
しばしば Frequent	頻繁に起きる。ハザードは連続的に経験する。
ありうる Probable	数回起きる。ハザードは頻繁に起きると仮定できる。
あるかも Occasional	数回起きるかもしれない。ハザードは数回起きると仮定できる。
まずない Rare	システムライフサイクルで起きる可能性がある。ハザードは起きることを仮定できる。
ありえない Improbable	発生するのが困難であるが可能性としてはある。例外的な事象として起きると仮定できる。
かんがえられない Incredible	非常に発生するのが困難。起きることはないと仮定できる。

頻度といっても数字できっちりは出にくいな。。。

EN 50126-1 7.4.2.1-4
EN 50126-1 C.2

3-2 ヤバいことの頻度は

数字でほしい場合もあるな。

頻度	解説	連続稼働の場合	運行時間稼働(5000h/yr) 30年で何回起きるか
しばしば Frequent	頻繁に起きる。ハザードは連続的に経験する。	6週間に一回以上	150回以上
ありうる Probable	数回起きる。ハザードは頻繁に起きると仮定できる。	年1回以上	15回以上
あるかも Occasional	数回起きるかもしれない。ハザードは数回起きると仮定できる。	10年に1回以上	2回以上
まずない Rare	システムライフサイクルで起きる可能性がある。ハザードは起きることを仮定できる。	1000年に1回以上	最大でも1回
ありえない Improbable	発生するのが困難であるが可能性としてはある。例外的な事象として起きると仮定できる。	10万年に1回以上	寿命中起こらないであろう
かんがえられない Highly-improbable	非常に発生するのが困難。起きることはないと仮定できる。	10万年に1回未満	寿命中起こる蓋然性が非常に低い

3-2 ヤバいことの重篤性

IEC 62278 6.3.3.1 d)
IEC 62278 4.6.2.3
EN 50126-1 7.4.2.1-4
EN 50126-1 C.3

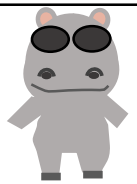
どんなレベルがあるの。

重篤度	人や環境への影響	サービスや財産への影響 (RAMにかかわるもの*)
破滅的 Catastrophic	多くの人への影響とその結果複数の死者またはかつ環境への甚大な被害	下記のいずれかで人や環境に引き続き影響するもの
重篤 Critical	非常に少ない数の人への影響とその結果の死者またはかつ環境への大きな被害	主要システムの損失
境界上 Marginal	死者はないが、重傷または軽傷、またはかつ環境への小さな被害	重大なシステムへの障害
軽微 Insignificant	軽傷の可能性	些少なシステムへの障害

*EN 50126は、リスクに安全性のみではなくRAMに対して好ましくない事項も対象としています。

3-2 セキュリティーは頻度分かるんか？

でもなあ、ヤバいってこのごろセキュリティーもあるやろ。うちにもヤバそうなやついるで。

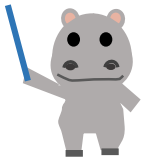


こいつは少なくともやるかやらんかは知らんけど、少なくとも技術は持ってるで。

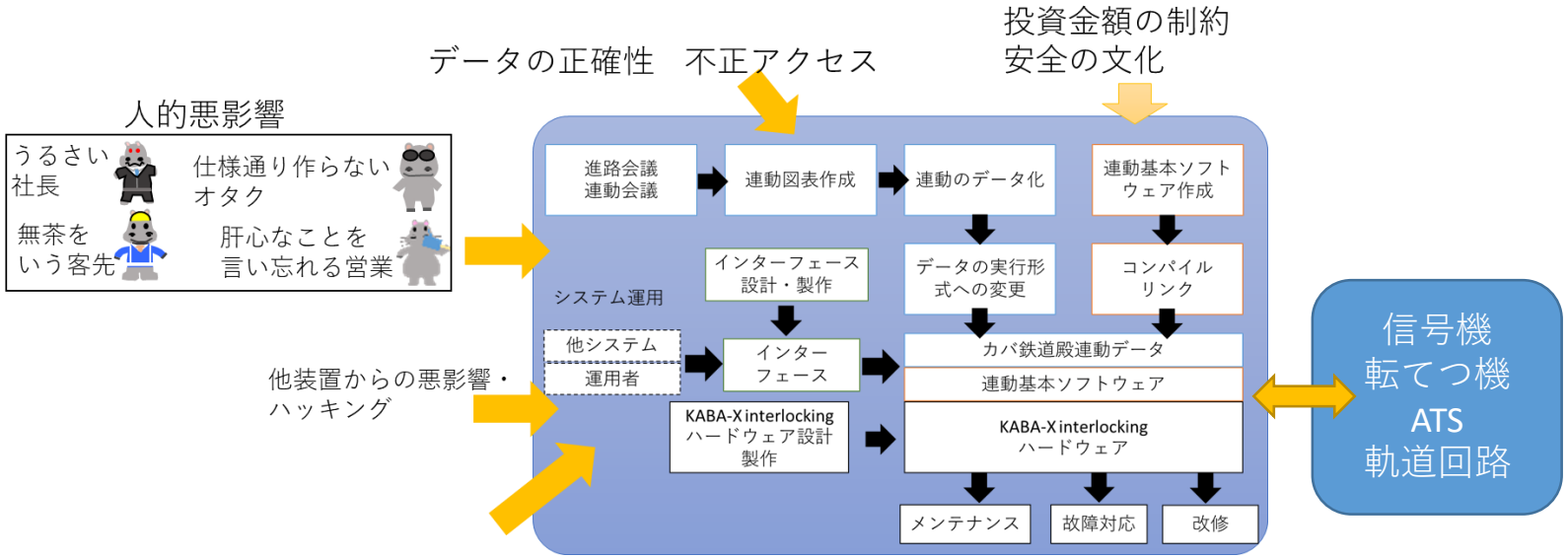
こいつは安全パイや。アイスをやっとけばエエだけや。

セキュリティーの頻度とか、確率とかは、そんなに出るもんじゃありませんよね。攻撃しやすいか、しにくいかで判断するとどうでしょうか。

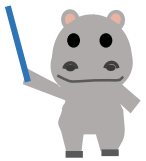
3-2攻撃の対象



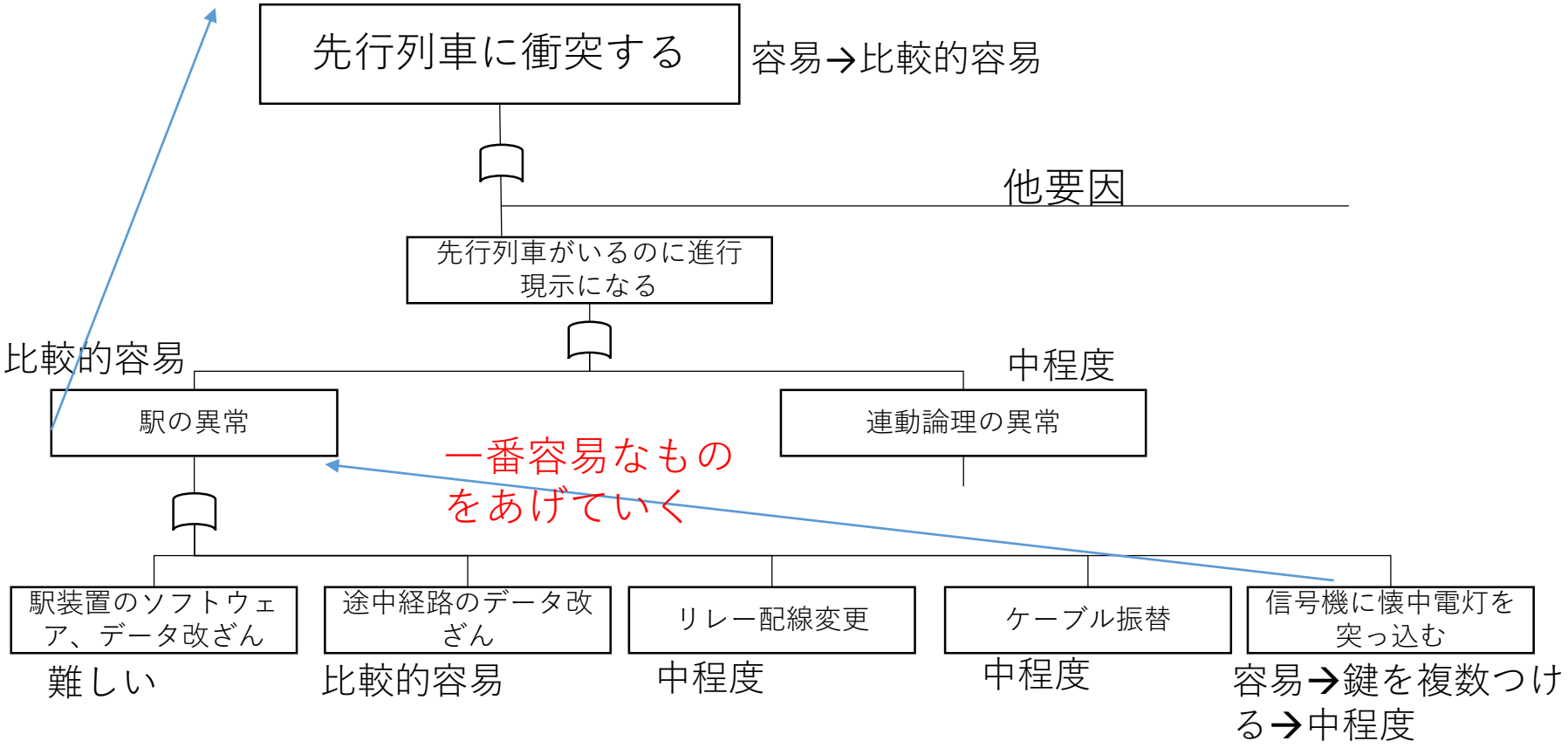
さあ、列車を脱線衝突させるためには、どこを攻めたらいいでしょうかね？当然やりやすいとこですよね。



3-2レベル評価

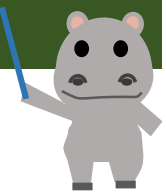


信号機に懐中電灯を突っ込むのは、信号機に鍵がかかってなかったら、技術なんていらないですよね。



3-3 望ましくない要因の対処

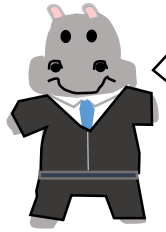
3-1 ハザード、RAMへの悪影響がある要因（以下望ましくない要因）を抽出する。
3-2 望ましくない要因のヤバさ加減を把握する。
3-3 望ましくない要因をどうするか決める。
3-3-1 3つの解析手法　(CoP, 参照装置, 個別解析)
3-3-2 個別解析の例
3-3-3 稼働率解析の例
3-4 望ましくない要因を記録に残す。



IEC 62278 6.3.3.1 c)
EN 50126-1 7.4.2.1-4

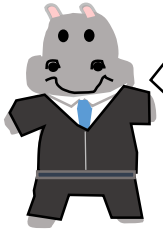
3-3 何でもやります。は何もしないと変わらない？

うちの製品はSIL4です（ホントか？）

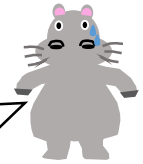


弊社カバ興業の製作する連動装置は、SIL4のフェールセーフコンピュータを使用し、安全に十分に留意してお客様の期待にお応えしますよ！**やれることは全部やる！それがカバ興業なんですよ！**

おお、頼もしいねえ、社長！じゃあカバ興業の製品を使用したら、安全快適な鉄道保安装置が実現できるというわけやな！



当然ですよ課長！ウチはね、SIL4の認証を受けた機械を使ってますからね。だてに「信頼のカバ興業」というキャッチフレーズを使ってませんよ！ウチを信じてくださいよ、ね、課長、今度の機器更新よろしくお願いしますよ。



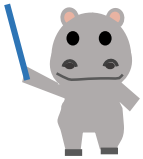
ちょ、調子のいいこと言っちゃってるよ。だいたいSILって機能ごとに設定するのに全部SIL4ってそんなこと言い切っていいの？？

3-3 望ましくない要因はどのように対処するか

IEC 62278 6.3.3.2
EN 50126-1 7.4.2.1

でも、何かの基準で対処するしないを決める必要があるんじゃないでしょうか？

社長のオレが決める！というのはいいすぎやな。。。



ひとつは、Code of practice (CoP)というものです。これはIEC 規格には規定はありません（EN 50126には規定されている)が、暗黙的にはよくつかわれています。

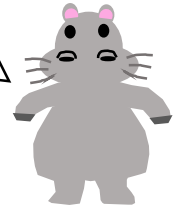
実施の規約ってことやな。社長のオレが規約を作ったんや！っていうことでもええってことか。。

それはダメです。

3-3-1 Code of practice

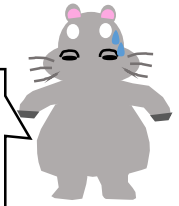
IEC 62278 6.3.3.2
EN 50126-1 7.4.2.1
EN 50126-2 8.3.1

で、データ化けについて、カバ興業ではいったいどうしてるんや？



えっと、うちには優秀なエンジニアがいまして、ハッキングカバっていうんですが、彼が作った「KABA-EDP-1」っていう社内規格で対処しているんですよ。

なにそれ。何か実績あるん？みんなその内容について納得してるん？信用できるかどうかわからんな。。



お客様第一のカバ興業、私カバお、お客様に自信のないものを売るわけにはいきません。技術のカバ興業！絶対に大丈夫です！

だからそれ、ぜんぜん説明になっていないやん。。それで大丈夫って言われても、それ他の人に説明できるわけないやん。

。。。私を信じてください。。。。

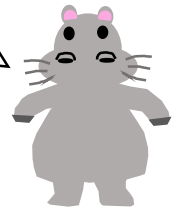
仮にオレが信じても、他人が信じるとは思えんな。宗教ちゃうんやで。宗教は根拠なくていいけど、技術で守る安全てそんなもんか？

3-3-1 Code of practiceでよくやってしまうこと

IEC 62278 6.3.3.2
EN 50126-1 7.4.2.1
EN 50126-2 8.3.1

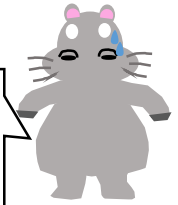
出直してきたんか？で、この前の質問の回答どうやねん。

えっと、うちのハッキングカバが作った「KABA-EDP-1」っていう社内規格は国際規格 IEC 62280を参考に作られています。



そうなんか！しっかりしてるな。でも、規格の考え方きっちり反映して、大丈夫っていう証拠あるんか？

お客様第一のカバ興業、私カバお、お客様に自信のないものを売るわけにはいきません。技術のカバ興業！絶対に大丈夫です！



まだでたよ。。もうおまえだけで来んでエエからエンジニアも来てくれるか？

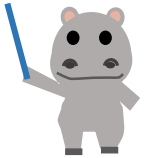
CoPの適用後、その後のリスクアセスメントの必要がなくなるというわけではありません。

3-3-1 Code of practice

IEC 62278 6.3.3.2
EN 50126-1 7.4.2.1
EN 50126-2 8.3.1

「KABA-EDP-1」は、実績ある国際規格IEC 62280に規定する脅威に対応し、使用するネットワークと符号長について、安全性インテグリティーを阻害しない充分な誤り検知能力を備えるよう規定してるで。これは、IEC 62280に書かれている通りや。

要するに世の中のレベルは、満たしているってことやな。それなら分かった。しかしお前んとこの営業は、ホンマ気合しか言わんな！



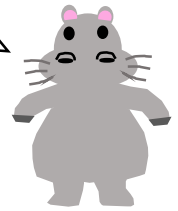
CoPは鉄道界で十分に受け入れられているルールであり、かつ適切な適用でなければなりません。

3-3-1 類似品の調査

IEC 62278 6.3.3.2
EN 50126-1 7.4.2.1
EN 50126-2 8.3.2

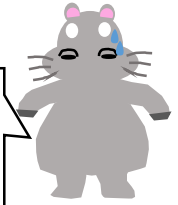
今までの同じような装置では誤り検出符号どうなってるねん？

えっと、同じだと思いますよ。お、な、じ。

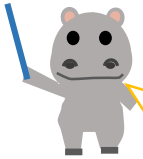


そうなんか！でも、同じような装置の「同じよう」のカバ興業の定義はなんや。

あの、えと、「同じような」は英語でいうところの[similar]だとおもわれます。



そんなんやったら何でも同じようなモンって言えちゃうやろ？



「同じようなモン」がどのような要件を満たしておかなければいけないかは定義があります。

EN 50126-2 8.3.2

3-3-1 類似品の調査

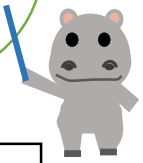
参照システムの条件

- 参照システムは受け入れられるに安全レベルの十分な実績があり、その結果受け入れが適切であること
- 参照システムは対象システムと類似の機能とインターフェースを持つこと
- 参照システムは対象システムと類似の条件でハザードや事故を見るための適切な期間使われていること
- 参照システムは対象システムと類似の環境条件で運用されていること

左が満たされれば

- 参照システムのリスクは対象システムで受け入れ可能とされる
- 参照システムにより包含されるハザードの安全要件は安全解析由来でなければならない。もしくは参照システムの安全記録の評価による。
- 関係するハザードの安全要求として、安全要求がハザード記録に記載されていること

むずかしいな。。



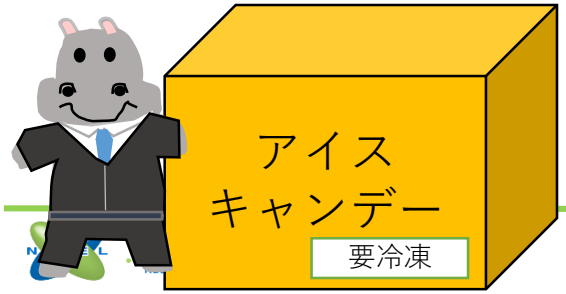
EN 50126-2 8.3.2

3-3-1 類似品の調査

もう少し簡単に言うと、似たもので同じような期間、環境、使い方、インターフェースで、特に安全問題がない場合は、リスクは受け入れられるんや。でも、似たものの安全要求仕様は、リスク解析されていることが必要なんや。またどんなハザードに対する安全要求なのか残ってなかったらダメなんや。

今までと同じ機能です。だからエエんです。はキツイんやな。
オイ、カバお！記録のこっとるやろな！

まあ、いままでの全部ありますけど。アイスと引き換えにお渡しします！

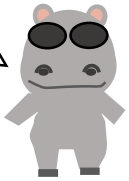


アイスでええんやったら安いもんや！
100本あるで！食え食え！

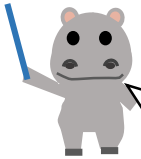
3-3-1 明確なリスク推定

IEC 62278 6.3.3.2
EN 50126-2 8.3.3

今までにないモンや、規格にないモンは、リスク推定をする方法があるわけや。



カバ興業のモンは、リスクがあってはイカンのやで。といってもゼロリスクはないしな。



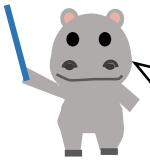
現在のリスクレベルを知り、受け入れ可能なリスクまで下げることになるわけです。

3-3 望ましくない要因の対処

3-1 ハザード、RAMへの悪影響がある要因（以下望ましくない要因）を抽出する。
3-2 望ましくない要因のヤバさ加減を把握する。
3-3 望ましくない要因をどうするか決める。
3-3-1 3つの解析手法　(CoP, 参照装置, 個別解析)
3-3-2 個別解析の例
3-3-3 稼働率解析の例
3-4 望ましくない要因を記録に残す。

3-3-2 明確なリスク推定例

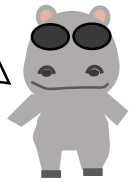
IEC 62278 6.3.3.2
EN 50126-2 8.3.3



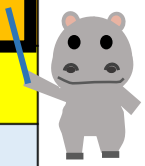
もしカバ興業の保安装置を汎用のCPUボードで作った場合、どれくらい故障するでしょうかね。。

お前なめるなよ。そんなもんは提供しないで。

まあでも、仮にだとしたら、定義された動作通り出力がされるという機能が満たされないのは、おそらく10年に一回くらい起こるやろうな。1.1×10^{-5}/hくらいか。。。



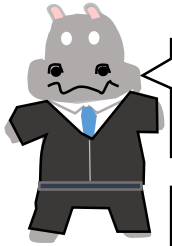
頻度	解説	連続稼働の場合	運行時間稼働(5000h/yr) 30年で何回起きるか
しばしば Frequent	頻繁に起きる。ハザードは連続的に経験する。	6週間に一回以上	150回以上
ありうる Probable	数回起きる。ハザードは頻繁に起きると仮定できる。	年1回以上	15回以上
あるかも Occasional	数回起きるかもしれない。ハザードは数回起きると仮定できる。	10年に1回以上	2回以上
まずない Rare	システムライフサイクルで起きる可能性がある。ハザードは起きることを仮定できる。	1000年に1回以上	最大でも1回
ありえない Improbable	発生するのが困難であるが可能性としてはある。例外的な事象として起きると仮定できる。	10万年に1回以上	寿命中起こらないであろう
かんがえられない Highly-improbable	非常に発生するのが困難。起きることはないと仮定できる。	10万年に1回未満	寿命中起こる蓋然性が非常に低い



IEC 62278 6.3.3.1 e)
EN 50126-1 7.4.2.1-4

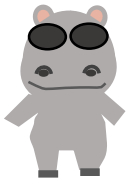
3-3-2まずハザードを考えよう

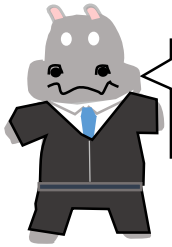
カバが乗った列車が脱線する



もしおまえらが全滅したら。。。オレはどうすればええんや。。死なんといてくれ。。。

意外に社員思いやな。これはどのくらいの頻度やったら許容できるんや？さっきの汎用CPUボードでええんか？

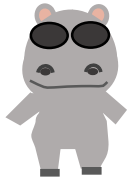




あってはならない事故や！普通のモンはアカン！
最大限の防護をせな！

カバが乗った列車が脱線する

重篤度：複数のカバの死亡
許容頻度 priceless
しかしなんか値を決めな作られへん。



3-3-2認められる頻度と重篤度

IEC 62278 6.3.3.2
EN 50126-2 8.3.3
複数の人の死亡

頻度 ＼ 重篤度→	軽微 1	境界上 2	重篤 3	破滅的 4
しばしば F	望ましくない	不可	不可	不可
ありうる E	受け入れられる	望ましくない	不可	不可
あるかも D	受け入れられる	望ましくない	望ましくない	不可
まずない C	無視できる	受け入れられる	望ましくない	望ましくない
ありえない B	無視できる	無視できる	受け入れられる	受け入れられる
かんがえられない A	無視できる	無視できる	無視できる	無視できる

社長の思いを表に当てはめると、緑の枠のところくらいやな。これは頻度は考えられないくらい少ないということになる。

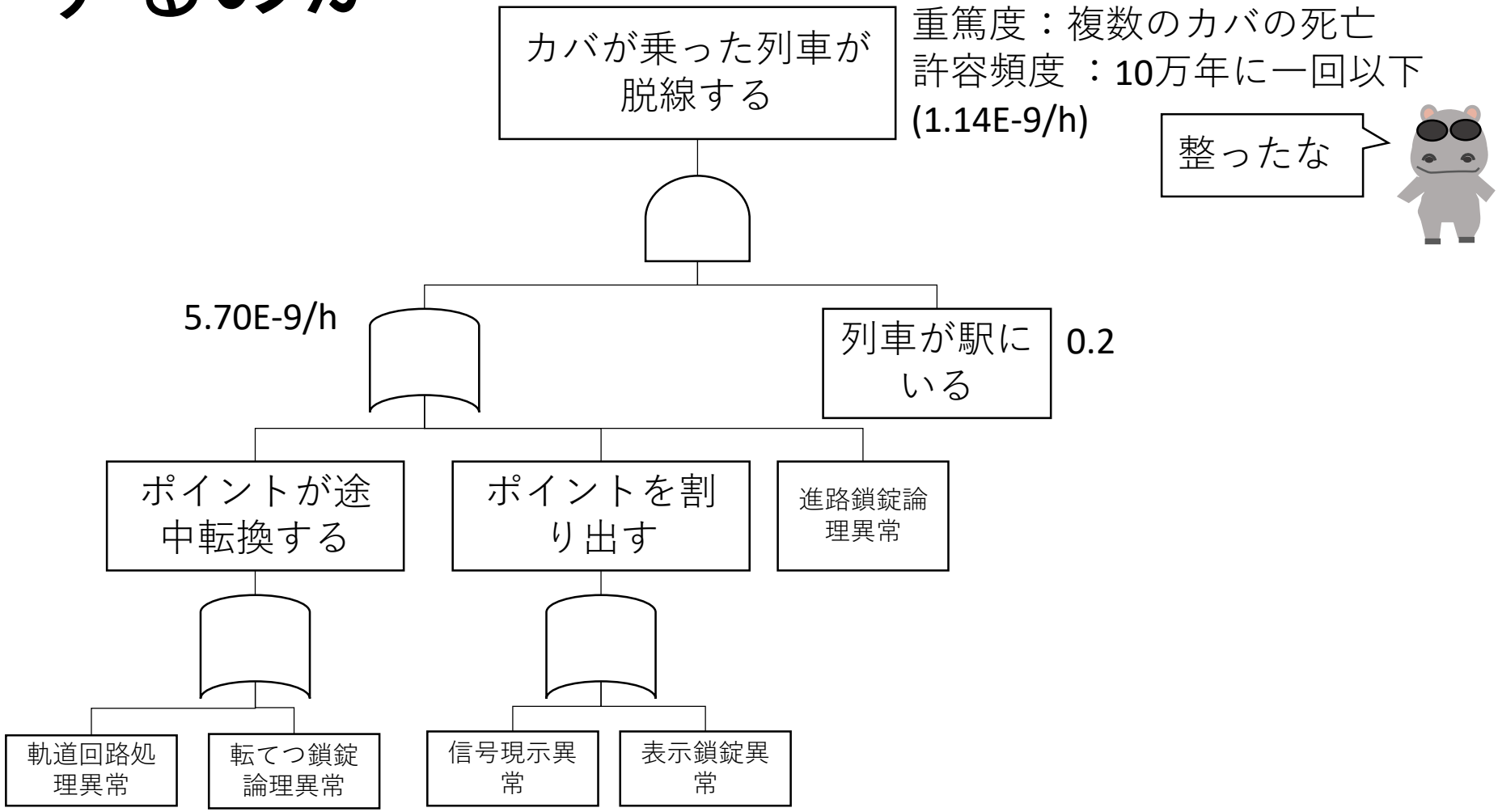
IEC 62278 6.3.3.2
EN 50126-2 8.3.3

3-3-2認められる頻度

頻度	解説	連続稼働の場合	運行時間稼働(5000h/yr) 30年で何回起きるか
しばしば Frequent	頻繁に起きる。ハザードは連続的に経験する。	6週間に一回以上	150回以上
ありうる Probable	数回起きる。ハザードは頻繁に起きると仮定できる。	年1回以上	15回以上
あるかも Occasional	数回起きるかもしれない。ハザードは数回起きると仮定できる。	10年に1回以上	2回以上
まずない Rare	システムライフサイクルで起きる可能性がある。ハザードは起きることを仮定できる。	1000年に1回以上	最大でも1回
ありえない Improbable	発生するのが困難であるが可能性としてはある。例外的な事象として起きると仮定できる。	10万年に1回以上	寿命中起こらないであろう
かんがえられない Highly-improbable	非常に発生するのが困難。起きることはないと仮定できる。	10万年に1回未満	寿命中起こる蓋然性が非常に低い

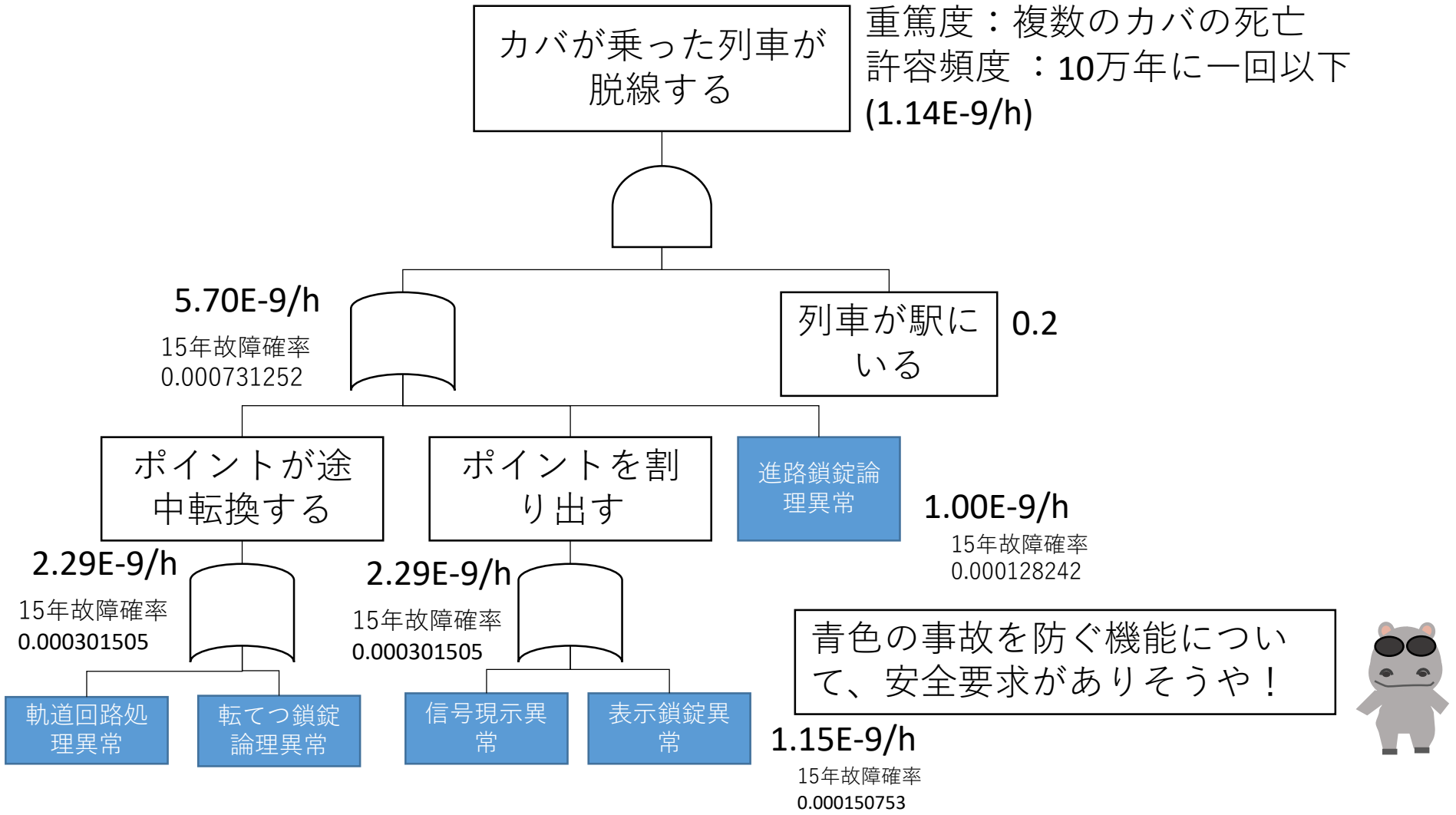
3-3-2 どんな原因で脱線するのか

IEC 62278 6.3.3.2
EN 50126-2 8.3.3



3-3-2 許容度の割り当て

IEC 62278 6.3.3.2
EN 50126-2 8.3.3, 10.2.2

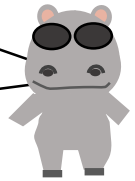


IEC 62278 6.3.3.2
EN 50126-2 8.3.3, 10.2.3

3-3-2 機能ごとのSIL

- 軌道回路処理異常
- 転てつ鎖錠論理異常
- 進路鎖錠論理異常
- 信号現示異常
- 表示鎖錠異常

これらのハザードを防ぐ機能は10^{-9}/hの不安全遷移頻度とすることにしたで



じゃあこの機能はEN 50126-2 Table 2を参考にすると、SIL4ということになるで。

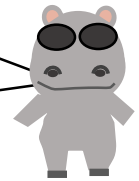
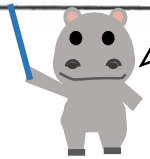


Table 2 — SIL quantitative and qualitative measures

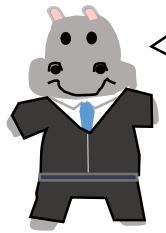
TFFR [h^{-1}]	SIL attribution	SIL qualitative measures
$10^{-9} \leq TFFR < 10^{-8}$	4	Defined in sector-specific standards
$10^{-8} \leq TFFR < 10^{-7}$	3	
$10^{-7} \leq TFFR < 10^{-6}$	2	
$10^{-6} \leq TFFR < 10^{-5}$	1	



ハザードを防ぐ機能を設定した場合の再計算を忘れずに。機能をまたいで同じ対策を打った場合共倒れになる場合もあるので、そういうことが起きる場合はそれを加味して計算してくださいね。
詳しくはCCFで調べて！

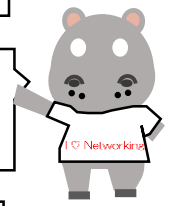
IEC 62278 6.3.3.2
EN 50126-2 8.3.3, 10.2.6

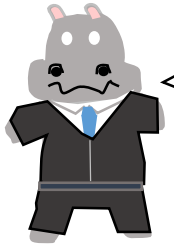
3-3-2 何のためにSILを決めるのか？



SILって。別に不安全側遷移頻度を10^{-9}/h以下にすればええんちゃうか？

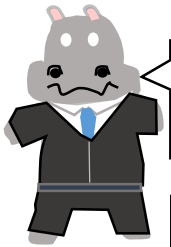
確かにハードウェアなど故障率が計算できるものはそうですが、じゃあソフトはカバおに作らせましょうか？





アカン絶対！バグだらけになる。しっかり管理しないとアカンで。

安全のレベルを決めると、管理レベルや、標準的に使用されている技術レベルを決めることができますね。



そうか。。オレのカバの一声で何とかなるもんではないのか。。。

確かにソフトは自信ないけど。ひどいなあみんな。。。

3-3-2 何のためにSILを決めるのか？

IEC 62278 6.3.3.2
EN 50126-2 8.3.3, 10.2.6
IEC 62425 Table E.1

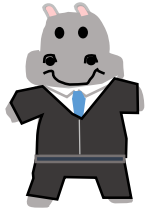
Table E.1 – Safety planning and quality assurance activities (referred to in 5.2 and 5.3.4)

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Checklists	R: checklist of activities and items to be produced		R: checklist of activities and items to be produced	
2 Audit of tasks	R		HR	
3 Inspection of issues of documentation	HR: documents agreed between railway/safety authority and industry		HR: all documents	
4 Review after change in the safety plan	HR			
5 Review of the safety plan after each safety life-cycle phase	HR			

このように安全性に応じてのチェックレベルが決められているので、あまり安全性に関係ない部分はチェックを省略できたりします。

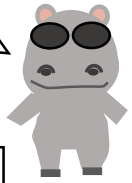
3-3モデルからのリスク推定

IEC 62278 6.3.3.2
EN 50126-2 8.3.3
IEC 62425 B.3.1
EN 50129 B.3.1



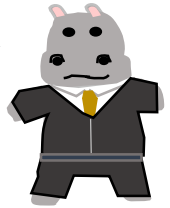
連動装置の機能の必要な安全性はどのくらいのレベルか個別にどうかわかったな。

CoPでもIEC 62425ではこれはfail safetyの枠の中やし、このような仕組みの安全装置は結構前例もあるやろ。安全性の度合いもわかったな。

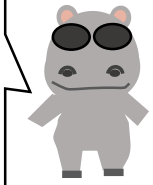


でも、故障を検知して止めるという機能が大事なのはわかったけど、その機能を実現するソフトウェアはどうすんねん。
数なんかソフトででるんか？

ソフトウェアに対しては、機能のSILレベルに応じて、その機能を実現する手法について、SSIL(software safety integrity level)を決め、管理手法の厳密さの調整を行います。



でたな大蒲教授。要は大事な機能は重点的に管理を行い、あまり安全に関係ないものは、それに応じて管理を調整することにより全体のコストと安全性のバランスをとるんや。



3-3-3システムの稼働率は上がっているのか？

EN 50126-2 8.3.3

これって止まりまくり？！

出力

一時間当たり危険側故障回数
1×10^{-9}/h
30年故障率 0.00026

危険側故障検知して
止める機能を実現する装置

一時間当たり危険側故障回数
1.07×10^{-9}/h
30年故障率 0.00028

正常信号

制御装置

一時間当たり故障回数 10^{-5}/h
30年故障率は0.928

EN 50126-2 8.3.3

3-3-3 稼働率はどうか

おまえんとこのやつ、安全性が高いかもしれんけど、こんなもん使いモンになるか！うちは機械が動いてこそお客さんからお金もらえるねんで！

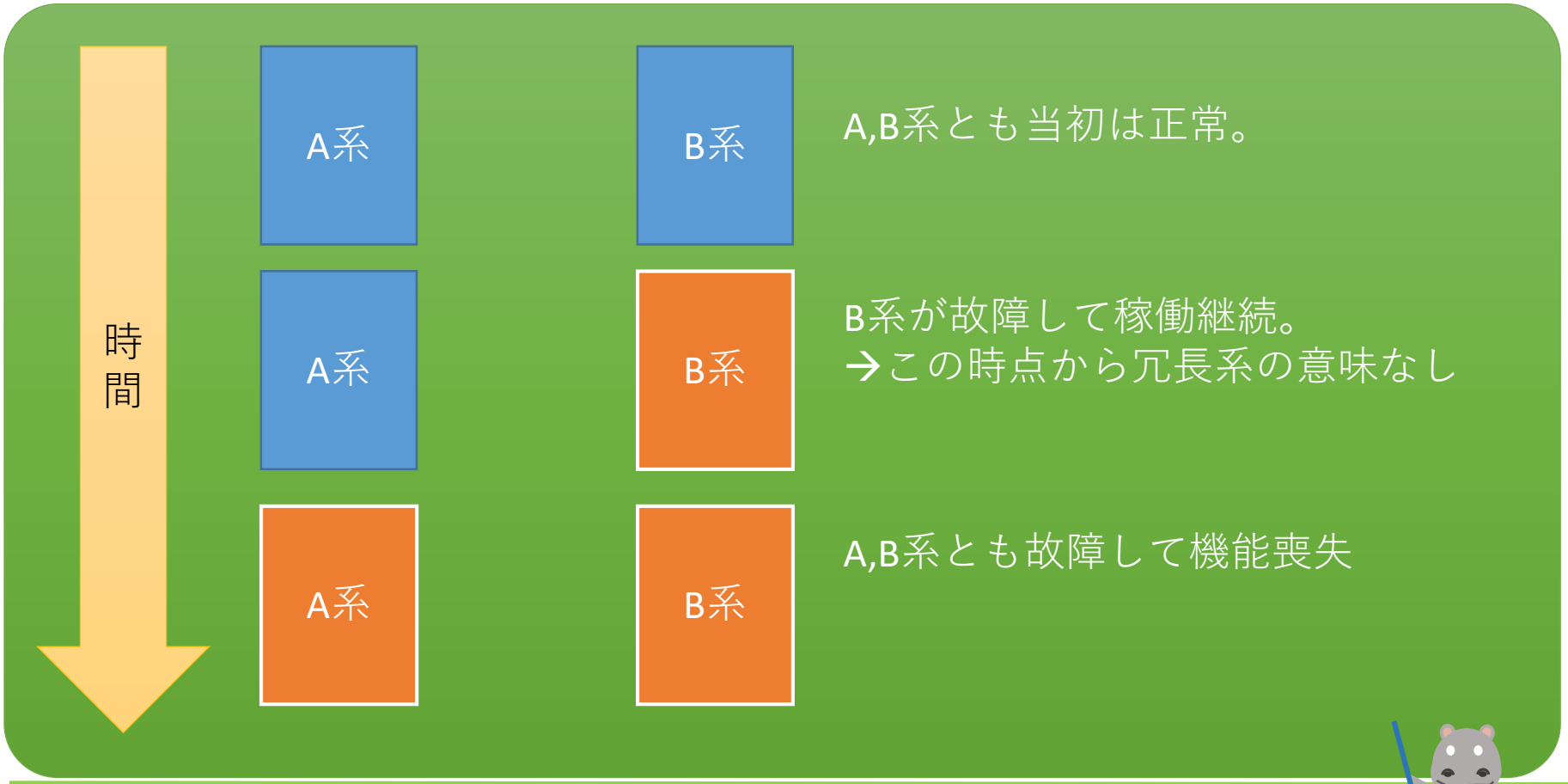
安全第一のカバ興業、私カバお、お客様に自信のないものを売るわけにはいきません。技術のカバ興業！絶対に大丈夫です！

それは安全の話やろ。全然かみ合ってないわ。おまえんとこの機械、30年で無傷なの7%しかないんやろ。そんなもんおまえ、ダメに決まっとるやろ。

あの、二重系にしていただければ、問題はないかと。。。

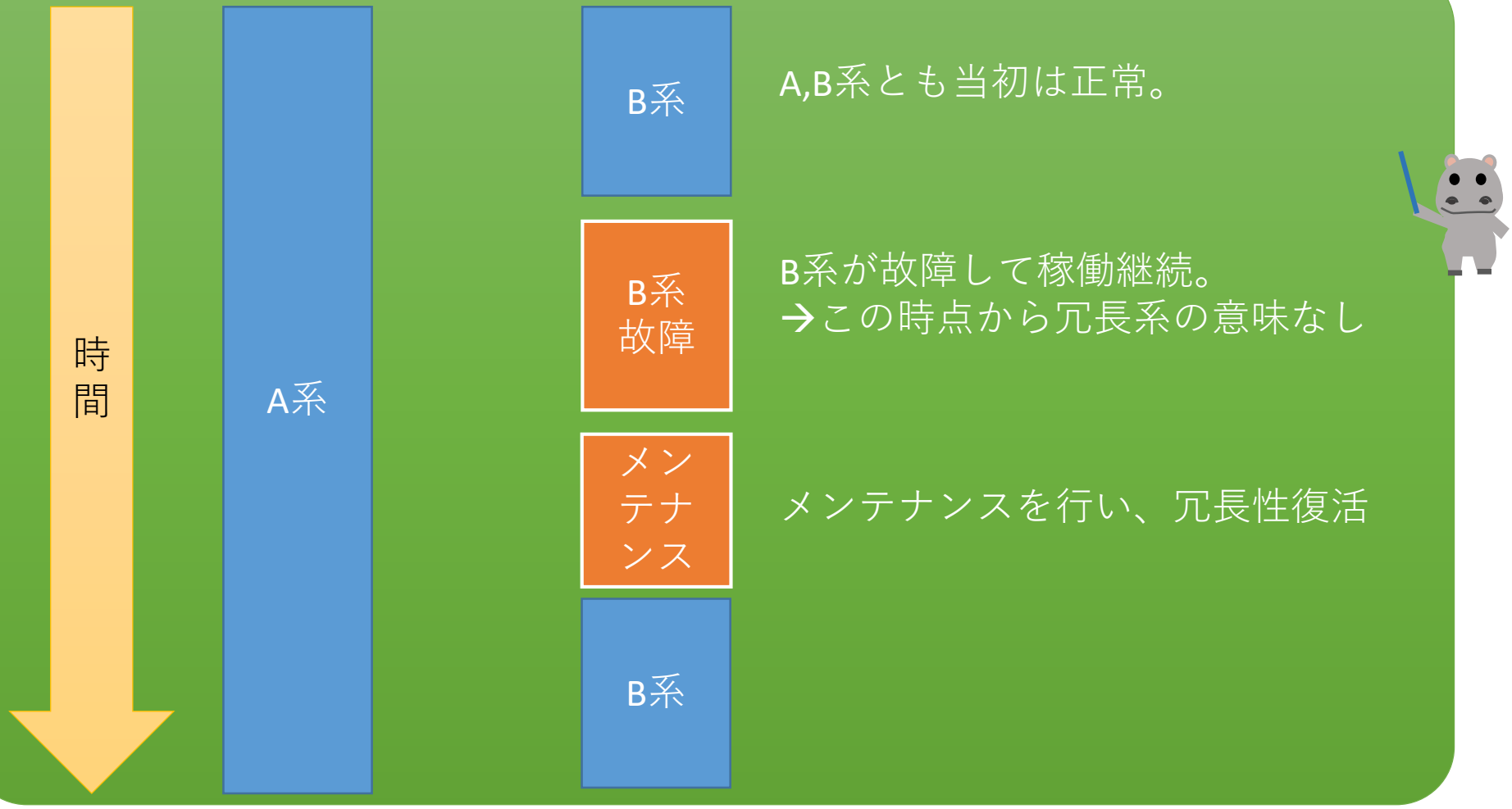
でまかせばっかり言いやがって。もう来んでええカバお！大体二重系にしても、保全せず壊れたままだったら何にも役に立たんで。保全の間隔なんかも関係あるんちゃうんか。

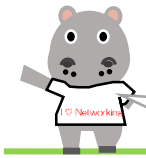
3-3-3 稼働率はどうか


時間
A系
B系
A系
B系
A系
B系
A,B系とも当初は正常。
B系が故障して稼働継続。
→この時点から冗長系の意味なし
A,B系とも故障して機能喪失

3-3 稼働率はどうか

EN 50126-2 8.3.3





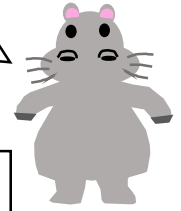
片系が故障・メンテナンス中にもう一方が故障しない限りミッションは実施できるわけですね。故障検知と修理の素早さが命です。

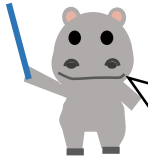
EN 50126-2 8.3.3

3-3-3 稼働率の検討

RAMSによく”logistics support”という言葉が出てくるのはこういう理由やな。要はせっかく2重系にしても、故障した後タイムリーに交換しないと、稼働率は大幅に下がる可能性があると。。。

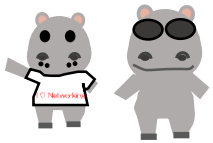
社長お願いしますよ。予備品は不足しないようにホント十分確保しといてくださいね。怒られるのはぼくなんだから。。





しかしやみくもに予備品を確保するのは、コストアップにつながりますよね。また技術者がカバ鉄道に急行できるかもカギになります。

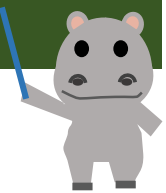
うーん。これが経営っていう難しさか。。カバお！しっかりカバ鉄道さんに稼働率を確保したいなら予備品がいるって言ってこなアカンで。オタかば！ハッキングカバ！お前らも明日から24時間携帯電話出れるようにしとけ！



給料と待遇の悪いカバ興業、退社させていただきます！
あとはよろしくお願いします！　ブタ工業に転職します！

3-4 記録に残していこう

3-1 ハザード、RAMへの悪影響がある要因（以下望ましくない要因）を抽出する。
3-2 望ましくない要因のヤバさ加減を把握する。
3-3 望ましくない要因をどうするか決める。
3-3-1 3つの解析手法　(CoP, 参照装置, 個別解析)
3-3-2 個別解析の例
3-3-3 稼働率解析の例
3-4 望ましくない要因を記録に残す。



3-4 困ったことを記録する

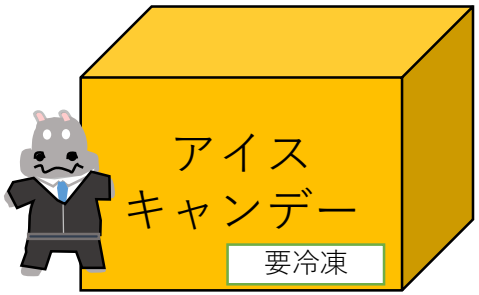
IEC 62278 6.3.3.3
EN 50126-1 7.4.2.2

カバおはなんか知らんけど、記録は得意やからな！　カバお！記録のこっとるやろな！

社長の暴言や勘違いのすべての記録をとっていますよ。これさえあれば。。。ふふふふふ。。

おい、おまえオレを脅すんか。。俺らカバ興業一家、家族やないか。

何も脅していませんよ。記録があるって言っただけです。社長が脅しと思うなら、それは社長にウシロメタイことがあるからですよね。。。



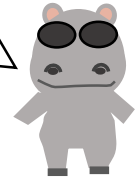
アイス食うか。200本あるで！食え食え！

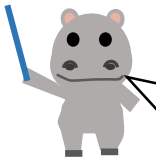
カバ興業がいい会社になるためには、記録して改善することは必要ですよね社長。脅しと思うなんて心外ですよね。アイスは頂きます！

3-4 困ったこととは何か

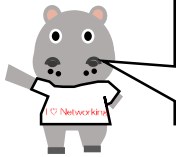
IEC 62278 6.3.3.3
EN 50126-1 7.4.2.2

カバおはどんなことを記録しているか知らんが、普通はイヤなことは書きたくないわな。でも書かんとアカンというのも分かる。

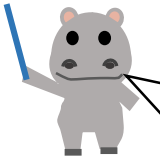




じゃあ記載することを少し整理してみましょう。



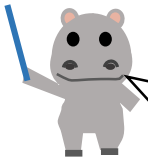
困ったことを書く「ハザードログ」は、困りごと、重篤性と頻度を書いて、対処方針を書くみたいなイメージあるけどね。



まあそれでもいい線いっていますが、どのようなことを書くべきかを調べていきましょう。

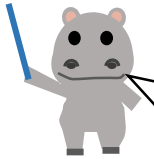
3-4まとめる目的

IEC 62278 6.3.3.3
EN 50126-1 7.4.2.2



ハザードログを作る目的は何でしょう。

困ったことを今解決できなくても、しかるべき段階になったとき解決できるようメモっておく機能ですよね。



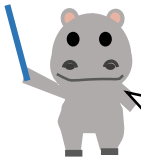
まあそれでもいい線いっていますが、それは「カバおメモ」とあまり変わらないと思いますよ。

ハザードについて既知の前提をもとに、対処すべきかどうかの判断、対処方針、決められた手順で実施されたかどうかを記録し、問題がないか確認する記録資料

じゃないでしょうか。
また、将来の設計の見直しや次のプロジェクトにも役立つかもしれません。

3-4 メモるだけではダメ

IEC 62278 6.3.3.3a)l)
EN 50126-1 7.4.2.2



きっちり対処したことを記録しましょう。

まず対処方針を決めておかないときっちり対処したかどうかも分かりませんよね。

ハザードログの目的

ハザードについて既知の前提をもとに、対処すべきかどうかの判断、対処方針、決められた手順で実施されたかどうかを記録し、問題がないか確認し、安全と品質、将来の次のプロジェクトに役立てることを目的とする。

リスク解析の条件

(例1)本システムは導入先が決定しているため、2020年現在の導入先の運行条件および設備を前提としてリスク解析を行う。
(例2)本システムはカバ興業が標準システムとして構築するものであるため、企画書に記載した最大容量の設備と運行条件を基に解析を行う。

3-4ハザードログの例

IEC 62278 6.3.3.3k)l)m)n)o)
EN 50126-1 7.4.2.2

IEC 62278は細かすぎる規定があるので、EN 50126-1に基づいて例を作ってみました。

ハザードログの目的　　対応装置　　前提　　.

番号	ハザード(気になる事項)	起こりそうな危険事象	リスク評価			対処法	対処後リスク評価			各種条件(他システム、管理によるもの)
			重篤度	頻度	リスク		重篤度	頻度	リスク	

EN 50126-1 7.4.2.2. Hazard Log
a) the purpose of the hazard log;
b) each hazard, entities responsible for managing the hazard, and the contributing functions or components;
c) likely consequences and frequencies of the sequence of events associated with each hazard, when applicable;
d) the risk arising from each hazard (in quantitative or qualitative terms), where appropriate;
e) risk acceptance principles selected and in case of explicit risk estimation also the risk acceptance criteria to demonstrate the acceptability of the risk control related to the hazards;
f) for each hazard: the measures taken to reduce risks to a tolerable level or to remove the risks;
g) exported safety constraints.

まとめ

3-1 ハザード、RAMへの悪影響がある要因（以下望ましくない要因）を抽出する。
　経験的な方法、システマティックに抽出する方法を併用することが望ましい。

3-2 望ましくない要因のヤバさ加減を把握する。
　頻度と重篤度が大事

3-3 望ましくない要因をどうするか決める。
　COP、前例、解析による方法がある。
　SILは装置ではなく、機能に依存。

3-4 望ましくない要因を記録に残す。
　単に記録ではなく、ハザードについて既知の前提をもとに、対処すべきかどうかの判断、対処方針、決められた手順で実施されたかどうかを記録し、問題がないか確認する記録資料として考えるといいのでは。