

システムに任せる事 項・人間が行う事項 ～システムの役割を決めるには～ (第二段階)

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



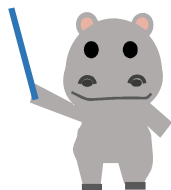
カバ興業 営業 カバお
「怒られてナンボの毎日が生命
の危機です」



カバ鉄道 電気課長
口癖：安くてエエもん持っ
て来い！



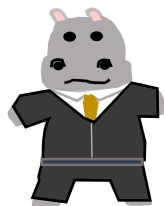
カバ興業 技術 オタかは
「面白くなければ技術じゃな
い」



謎のフリーコンサル
なぞカバ
「知識は力！管理は必然」



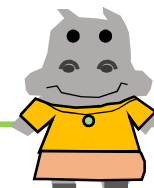
カバ興業 プログラマ
ハッキングカバ
「俺しかできないことをやる」



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」

皆様へのご挨拶

2/1から、交通安全環境研究所の職員になりました。
なお一層業務に精励していきますので、よろしくお
願いいたします。

前回のまとめ

RAMSの第一段階はシステムの範囲や対象、基本的な考え方を関係者と共有します。

取り巻く状況がどのような切り口であるかどうかを網羅的に考えます。

そのうち、潜在的な危険となる事象（ハザード：例えば、信号が赤が出るべきところに青が出る。）の原因（ハザード源：例えば間違った配線）と必要と思われるような管理手法を考えておきます。

前回メールでいただいた質問

危険源になりそうな事項を考えるのは賛成です。
しかし一番の危険源は、
「カバ興業の経営」
ではないでしょうか？

当社にお任せください。

東京都 メーカー勤務



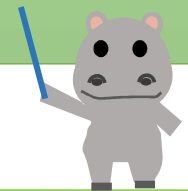
し、失敬な！ 財務は健全に決まっているわ。

次の第2段階は

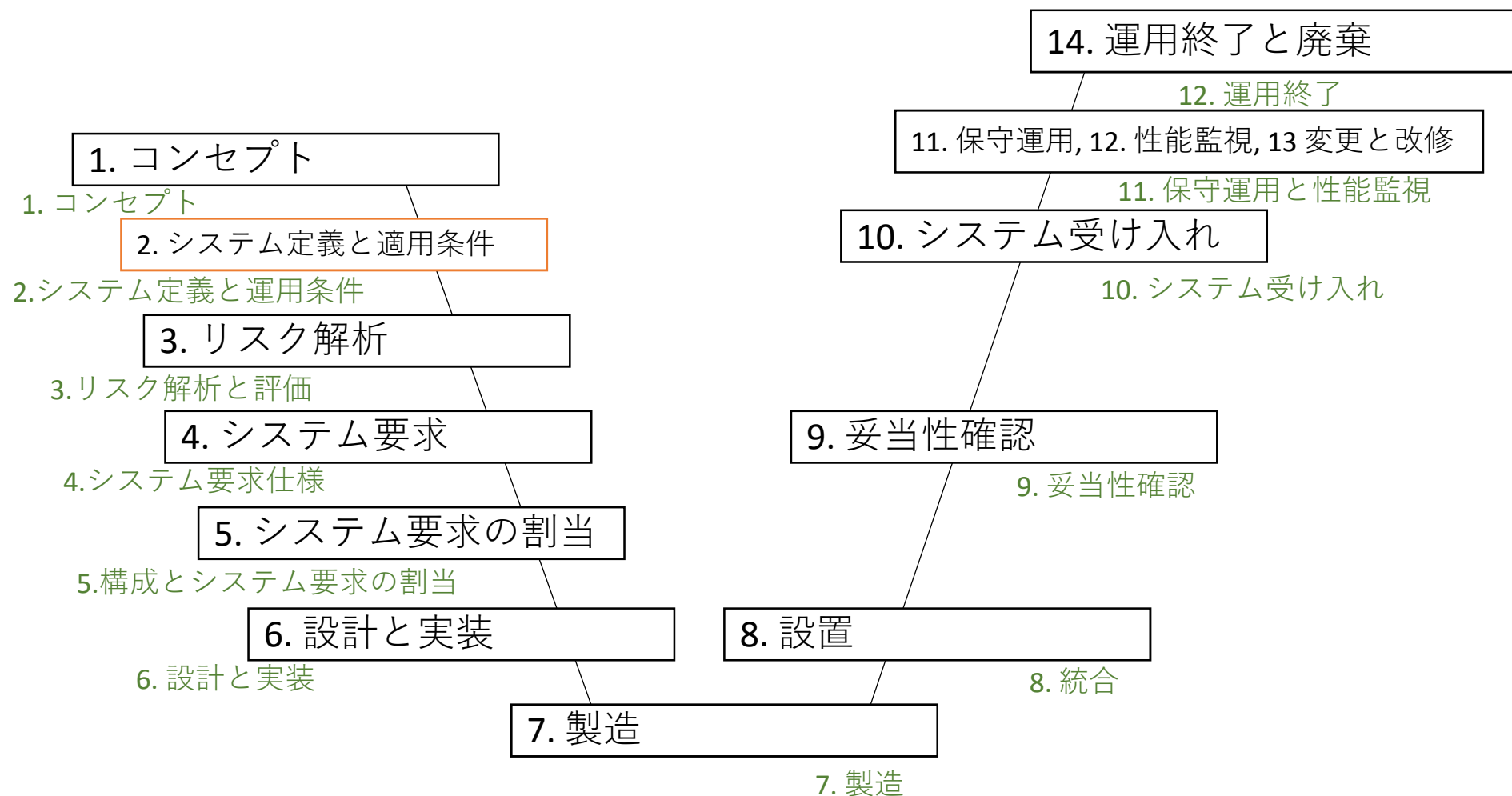
Phase 2: System definition and application conditions
(IEC 62278)

Phase 2: System definition and operational context
(EN 50126-1)

「システムの定義と適用（運用）条件」
と題がついています。

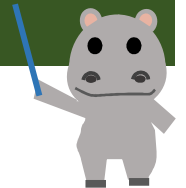


全体のRAMSのライフサイクル



この段階で要求されていること

- 2-1 システムがどんな目的を持つか決める。
- 2-2 数値的目標であるミッションプロファイルを決める。
- 2-3 RAMSの解析をする準備として
 - 2-3-1 システムの境界を決める。
 - 2-3-2 システムに影響する適用要件（運用・保守・外部装置など）の範囲を決める。
 - 2-3-3 ハザード解析の範囲を決める。
- 2-4 RAMに影響を与えそうな事項とその評価をやってみて、感じをつかむ。
- 2-5 ハザードの検出をやってみて、感じをつかむ。
- 2-6 RAMに関する計画をまとめ始める。
- 2-7 安全に関する計画をまとめ始める。



2-1 システムがどんな目的を持つか決める。

2-2 数値的目標であるミッションプロファイルを決める。

2-3 RAMSの解析をする準備として

2-3-1 システムの境界を決める。

2-3-2 システムに影響する適用要件（運用・保守・外部装置など）の範囲を決める。

2-3-3 ハザード解析の範囲を決める。

2-4 RAMに影響を与えそうな事項とその評価をやってみて、感じをつかむ。

2-5 ハザードの検出をやってみて、感じをつかむ。

2-6 RAMと安全に関する計画をまとめ始める。



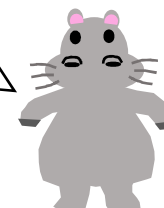
2-1 コンセプトは決めたはず。でもどこまでやるの？

EN 50126-1 7.3.2.1 a)

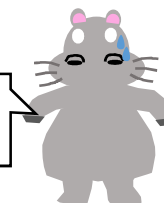
今回の集中連動について、お打ち合わせにきました。どこまでうちがさせてもらったらいいんでしょうか？



フルオートマチックやで！カバ興業に全部任せるから。。



え、それはどういう意味ですか？



だから、システムが壊れても装置が自分で直るとか、連動会議で決まった内容を自動的に試験まで含めてカバ興業が自動装置でやってくれるとか、ダイヤ変更を口で言ったら自動でダイヤやルートが変わるとかそういうようなやつがええな。



え、ええっ、そのようなことは今まで全くお聞きしていないというか、なんというか。。



そなんそらゆうてないわ。だって今考えたことやもん。今までなんも議事録ないよね。。



2-1 目的を決める

EN 50126-1 7.3.2.1 a)

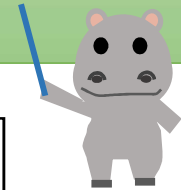
a) the system objective (intended purpose) and its mission profile

システムの目的（意図した目的）とそのミッションプロファイル（を決める）

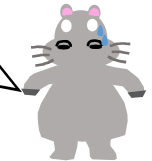
—EN 50126-1 7.3.2.1 a)



システムの意図することを決める。ということは、システムの定義につながるわけやな。



昨日カバ鉄道さんに行ってお伺いしてきたら、何を意図しているかわからなくなってきました。。。



それは、、、はっきりさせないとアカンな。。

2-1 目的を決める

EN 50126-1 7.3.2.1 a)

カバ鉄道殿においては、駅別に継電連動装置の置き換えとして複雑なワイヤーロジック設計が不要な電子連動装置を導入された。

また、電子連動装置は、継電連動装置とは異なり、ロジックの複雑さと大きさが直接は比例しないため、大きな駅の機器室の面積を縮小することができる。

このような特徴をより活用するため、各駅に連動装置を設置するのではなく、拠点となる駅、もしくは指令所などに一括して連動装置の論理部を設け、各機器のインターフェースの部分のみ各駅に設置することにより、保守の重点化、費用の低減を図ることとしている。これを集中連動装置と称する。

想定される可用性については、現行レベルと同一レベルを確保し、ライフサイクルにおいても、現行のシステムと同一のレベルを担保するものとする。

目的：

連動装置の集約を進めることにより、連動機器のスリム化、機器室自体のスリム化、保守の重点化によりライフサイクル費用の低減を目的とする。また、安全性については、現行レベルを維持する。



カバお、お前もスリム化した方がええで。

アイスください。。。



2-1 システムがどんな目的を持つか決める。

2-2 数値的目標であるミッションプロファイルを決める。

2-3 RAMSの解析をする準備として

2-3-1 システムの境界を決める。

2-3-2 システムに影響する運用要求の範囲を決める。

2-3-3 ハザード解析の範囲を決める。

2-4 RAMに影響を与えそうな事項とその評価をやってみて、感じをつかむ。

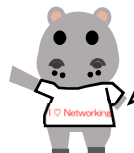
2-5 ハザードの検出をやってみて、感じをつかむ。

2-6 RAMと安全に関する計画をまとめ始める。

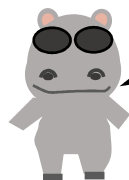


2-2数値目標を決める

IEC 62278 6.2.3.1 a)
EN 50126-1 7.3.2.1 a)



カバ鉄道さんの駅数いくつあるの？
どのくらいの処理周期が必要なの？
ルート数はどれくらいなの？
社長は他の会社にも売り込みたいと思うだろうけど、どのくらいのルート数までOKにするの？



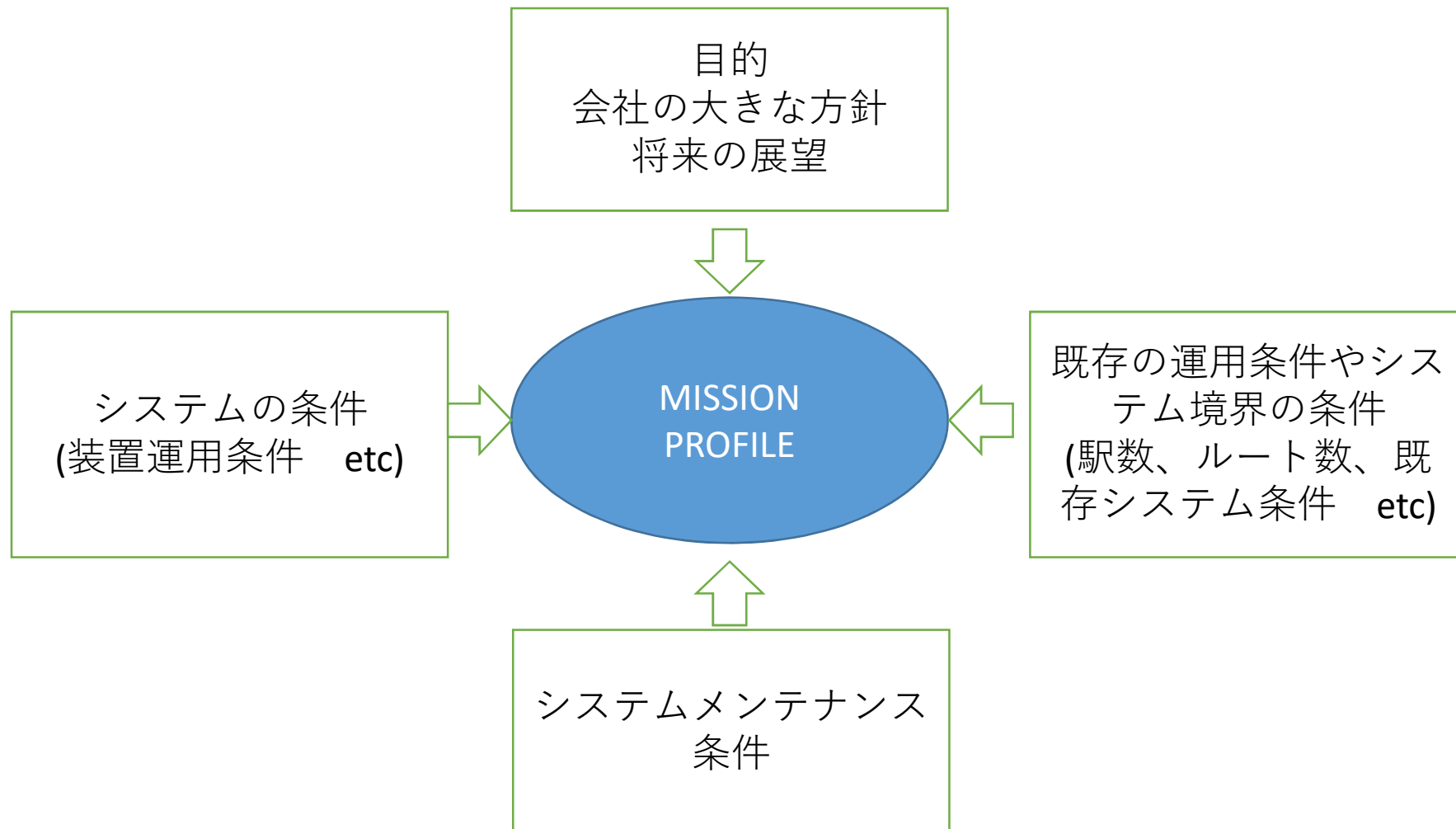
どのくらいの取り替え周期考えてるんや？どのくらいの処理停止時間許容されるねん？故障したときのことをかんがえとかんとあかんやろ。

アイス持ってきたよ。その辺はみんなで考えてよ。ぼくは営業だからそんなん知らないよ。



作れるかボケ！そんなことお前がカバ鉄道と社長に確認してこいや。営業やろ！

2-2 目標を決めるために重要な事項



2-2 目的と数値目標

IEC 62278 6.2.3.1 a),b),c)
EN50126-1 7.3.2.1 a),b),c)

カバ鉄道は、同業他社をしのぐ安全。お客様の命は何よりも優先する。との行動指針がある。



取材してきたよ！

- 基本的には地上装置は機器室収容であり、空調が準備でき、電源も無停電電源が準備できる。
- システムが停止した場合、すべての信号操作が線区全体で不能になる。
- 今まで**15年**間重大なシステム停止は起こっていないため、同等以上の稼働率が必要。

MISSION
PROFILE

- 集約される駅数**20**、ルートは**170**である。
- 各駅の既存連動機、CTCは撤去する。ルート制御装置は残す。
- カバ興業としては他社に売るために、**50駅500ルート**程度までは対応したい。
- カバ興業の電子連動は反応が少し遅いとの評判がある。

- カバ鉄道には保守間合い時間が**3時間**設定されているが、その間合い時間に他の作業が存在すると、信号や転てつ機の操作が発生することもあるため、間合い時間をフルに活用できるわけではない。
- 連動装置を切り離し、手信号で列車を出発到着させる規則があるが、限定的な運用とした位置づけである。

2-2目的と数値目標

IEC 62278 6.2.3.1 a)
EN50126-1 7.3.2.1 a)



カバお、確かにルート数とか、電源とか、そういう数値は決まりそうやな。
おまえさんがいろいろ聞いてくれたおかげさんやで。

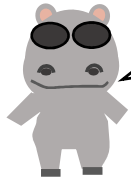
ご褒美にアイスください。。。。



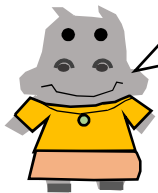
そやけど、安全に対しては、数値化できるんかな。。。。。

2-2安全を例にした目標設定

カバ鉄道は、同業他社をしのぐ安全。お客様の命は何よりも優先する。との行動指針がある。



天の声や！これをどう数値化しようか？



こういう決めるべきパラメータ例の記述があるんですよ。ただどうやって決めるかっていうのは、難しさはありますね。安全に関してはいくつかの決め方があります。

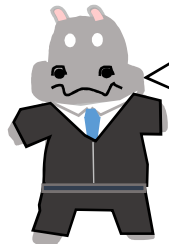
Table C.5 – Examples of safety performance parameters

PARAMETER	SYMBOL	DIMENSION
Mean Time Between Hazardous Failure	MTBF(H)	Time, distance, cycle
Mean Time Between "Safety System Failure"	MTBSF	Time, distance, cycle
Hazard Rate	H(t)	Failures/time, distance, cycle
Safety Related Failure Probability	$F_S(t)$	Dimensionless
Probability of Safe Functionality	$S_S(t)$	Dimensionless
Time to Return to Safety	TTRS	Time

2-2ハザードと数値目標

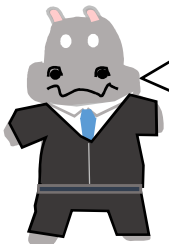
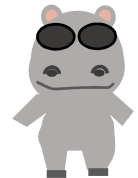
IEC 62278 6.2.3.1 a)
EN50126-1 Annex C

カバが乗った列車が
脱線する



もしおまえらが一人でも死んだら。。。オレはどうすればええんや。。。死なんといてくれ。。。。

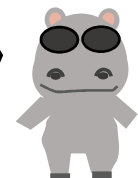
意外に社員思いやな。これはどのくらいの頻度やったら許容できるんや？



あってはない事故や！最大限の防護をせなあかん！

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。



2-2 どんなことが 起こりえるか？

IEC 62278 6.2.3.1 a)
EN50126-1 Annex C

列車が脱線したら、
カバ全滅や。。。

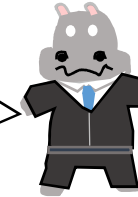


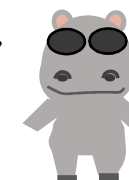
Table C.4 — Severity categories (example 1 related to RAMS).

Severity category	Consequences to persons or environment	Consequences on service/property
Catastrophic	- Affecting a large number of people and resulting in multiple fatalities, and/or - extreme damage to the environment	Any of the below consequences in presence of consequences to persons or environment
Critical	- Affecting a very small number of people and resulting in at least one fatality, and/or - large damage to the environment	Loss of a major system
Marginal	- No possibility of fatality, severe or minor injuries only, and/or - minor damage to the environment	Severe system(s) damage
Insignificant	Possible minor injury	Minor system damage

2-2何をを目指すか？

Frequency of occurrence of an accident (caused by a hazard)	Risk Acceptance Categories			
	Undesirable	Intolerable	Intolerable	Intolerable
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Rare	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Undesirable
Highly improbable	Negligible	Negligible	Negligible	Tolerable
	Insignificant	Marginal	Critical	Catastrophic
	Severity of an accident (caused by a hazard)			複数の人の死亡

社長の思いを表(EN 50126-1 Table C.9)に当てはめると、赤の枠のところくらいやな。これは頻度はHighly improbableということになる。

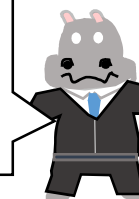


2-2 認められる頻度

Table C.1 — Frequency of occurrence of hazardous events with examples for quantification (time based)

Frequency level	Description	Example of a frequency range based on a single item operating 24 h/day	Example of equivalent occurrence in a 30 year lifetime of a single item operating 5000 h/year
		Expected to happen	
Frequent	Likely to occur frequently. The event will be frequently experienced.	more than once within a period of approximately 6 weeks	more than about 150 times
Probable	Will occur several times. The event can be expected to occur often.	approximately once per 6 weeks to once per year	about 15 to 150 times
Occasional	Likely to occur several times. The event can be expected to occur several times.	approximately once per 1 year to once per 10 years	about 2 to 15 times
Rare	Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur.	approximately once per 10 years to once per 1 000 years	perhaps once at most
Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.	approximately once per 1 000 years to once per 100 000 years	not expected to happen within the lifetime
Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.	once in a period of approximately 100 000 years or more	extremely unlikely to happen within the lifetime

10万年に一回か。
。エエもん設計するで！



2-2ここまでのまとめ

システムの定義、条件



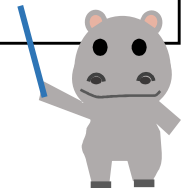
具体的な数値化



難しいものは？



前例やリスクマトリックスを活用



- 2-1 システムがどんな目的を持つか決める。
- 2-2 数値的目標であるミッションプロファイルを決める。
- 2-3 RAMSの解析をする準備として

2-3-1 システムの境界を決める。

2-3-2 システムに影響する運用要求の範囲を決める。

2-3-3 ハザード解析の範囲を決める。

- 2-4 RAMに影響を与えそうな事項とその評価をやってみて、感じをつかむ。
- 2-5 ハザードの検出をやってみて、感じをつかむ。
- 2-6 RAMと安全に関する計画をまとめ始める。

2-3 境界はどのような？

IEC 62278 6.2.3.1b)
EN 50126-1 7.3.2.1 b)

IEC 62278 6.1.3.2 b)

- b) the system boundary, including:
- interfaces with physical environment;
 - interfaces with other technological systems;
 - interfaces with humans;
 - interfaces with other Railway Authorities;

インターフェースと相互作用に変更。
他鉄道事業者から、他鉄道関係者に変更。

EN 50126-1 7.3.2.1 b)

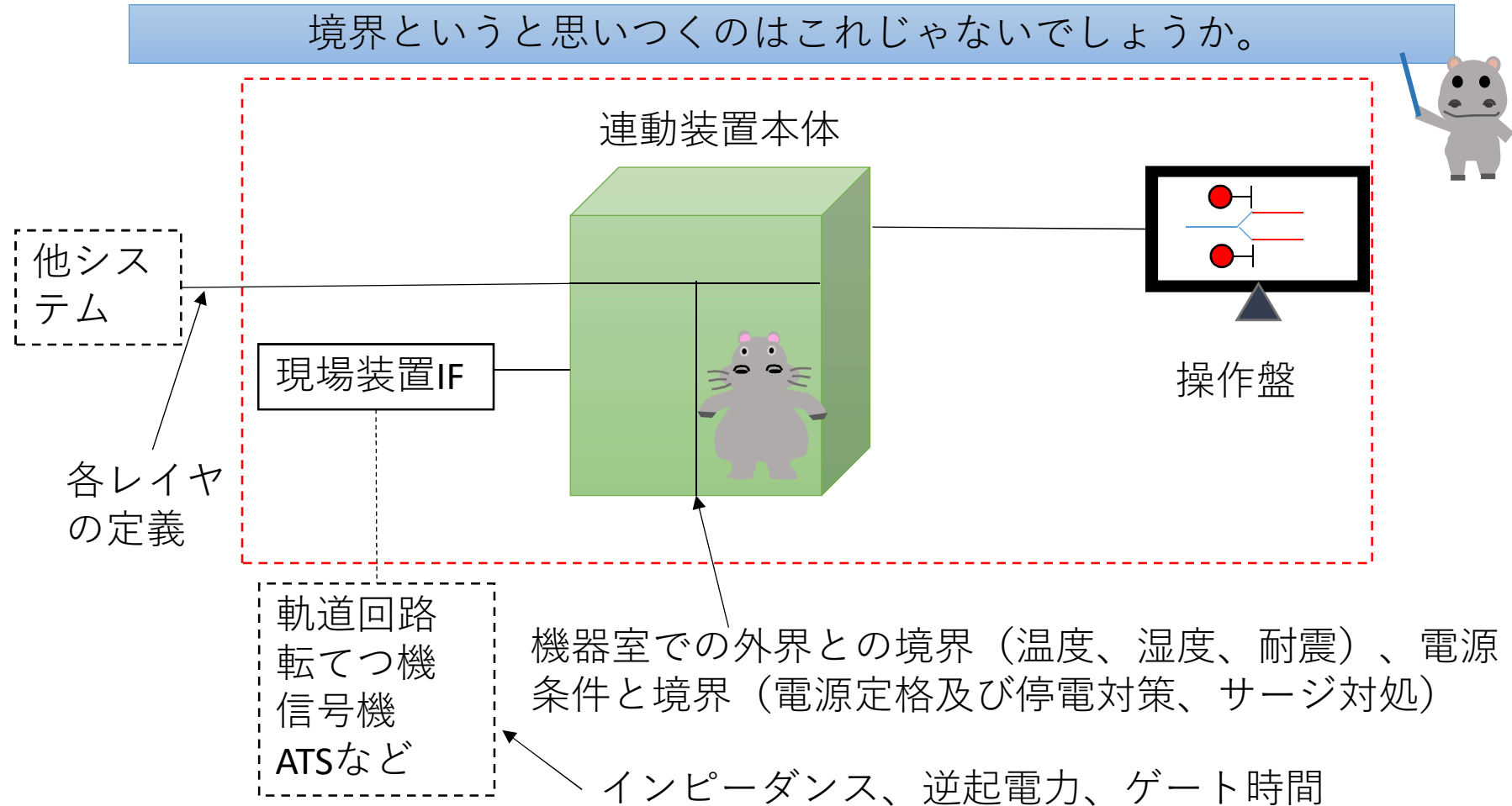
- b) the system boundary, including:
- interfaces and interactions with physical environment (e.g. climatic conditions, mechanical conditions, altitude) and with other systems;
 - interfaces and interactions with other technological systems;
 - interfaces and interactions with humans;
 - interfaces and interactions with other railway duty holders;



よくわからんが、下の方がなんか増えとるな。。カバおに訳させよう。。

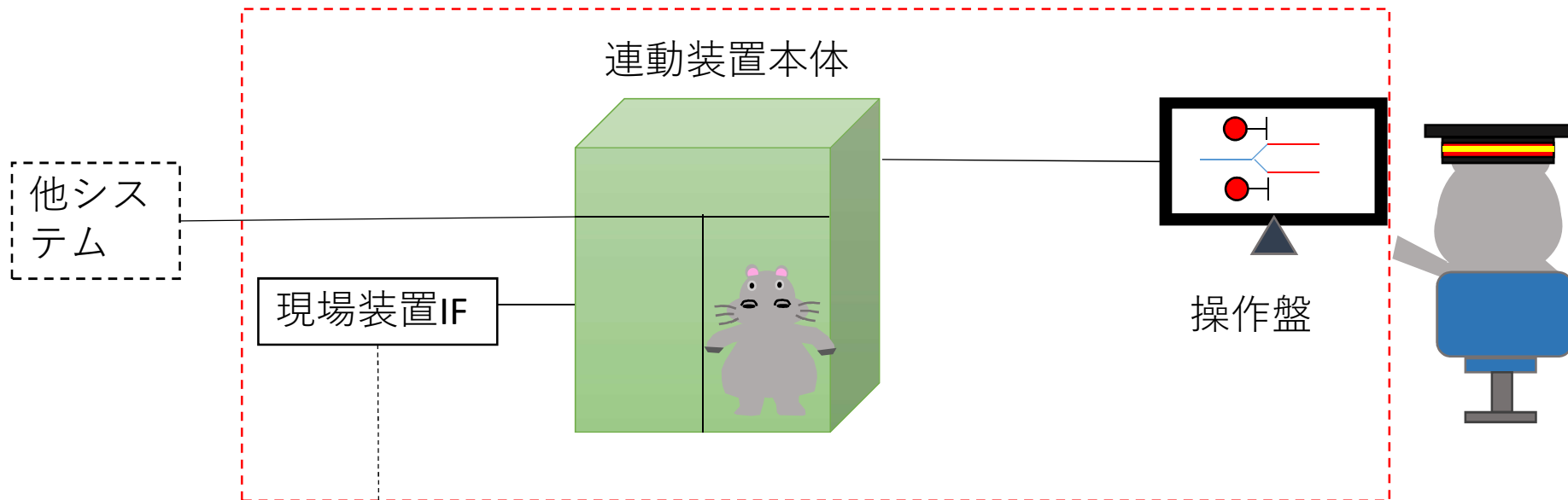
2-3境界とは？

IEC 62278 6.2.3.1b)
EN 50126-1 7.3.2.1 b)

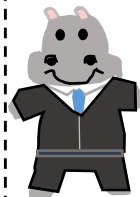


2-3 境界はどのような？

IEC 62278 6.2.3.1b)
EN 50126-1 7.3.2.1 b)



軌道回路
転てつ機
信号機
ATSなど



うちがデータ作成を担当しても
境界は赤い点線で、あまり変わ
らんような感じるけどな。。

社長、直感ですけど、営業としての感覚は全然違いますよ。
非常に危険な香りが。そこをあいまいにすると、大モメし
て赤字一直線じゃないですか。。

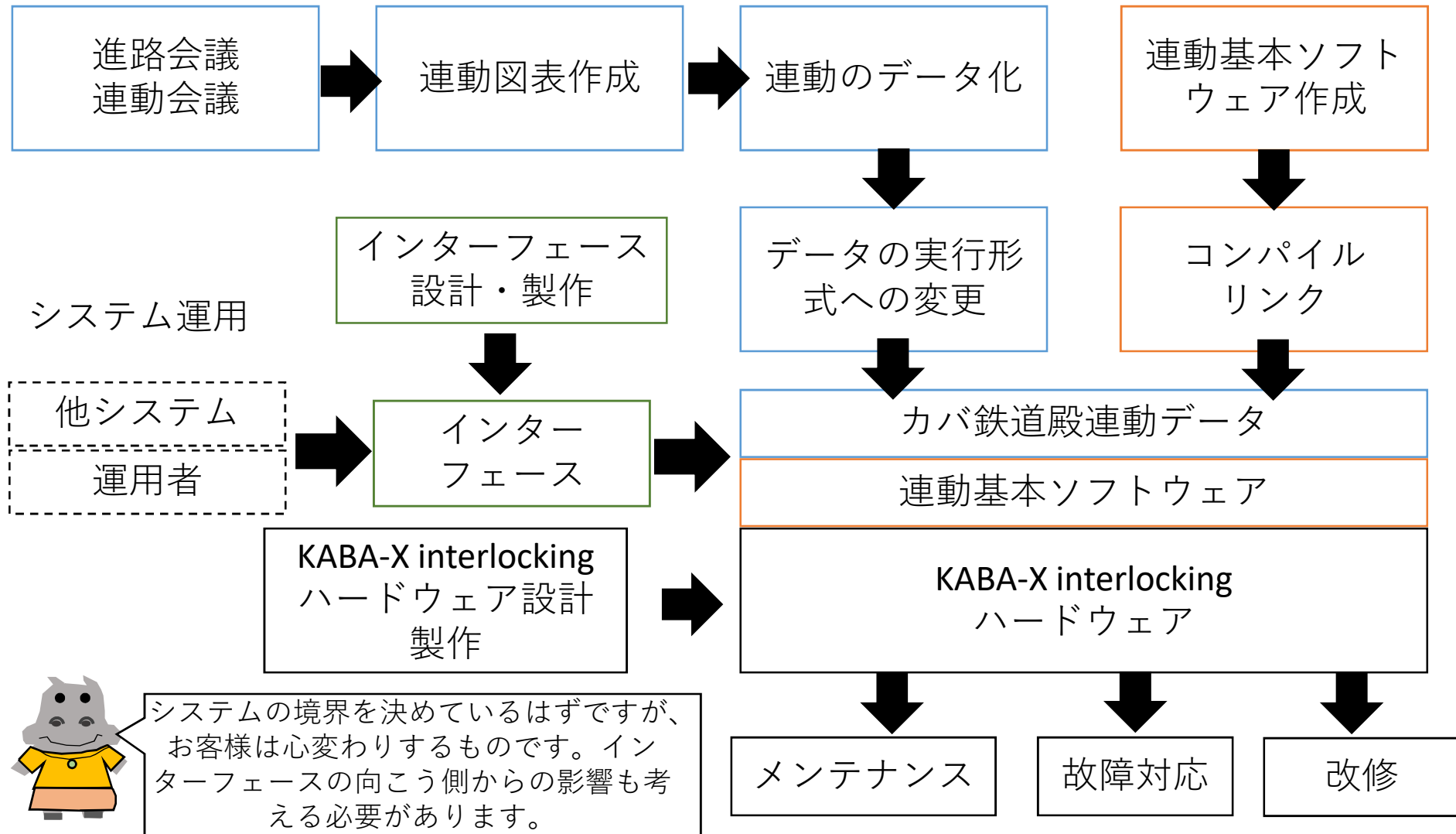


境界というのはシステム境界だけなのでしょうか？



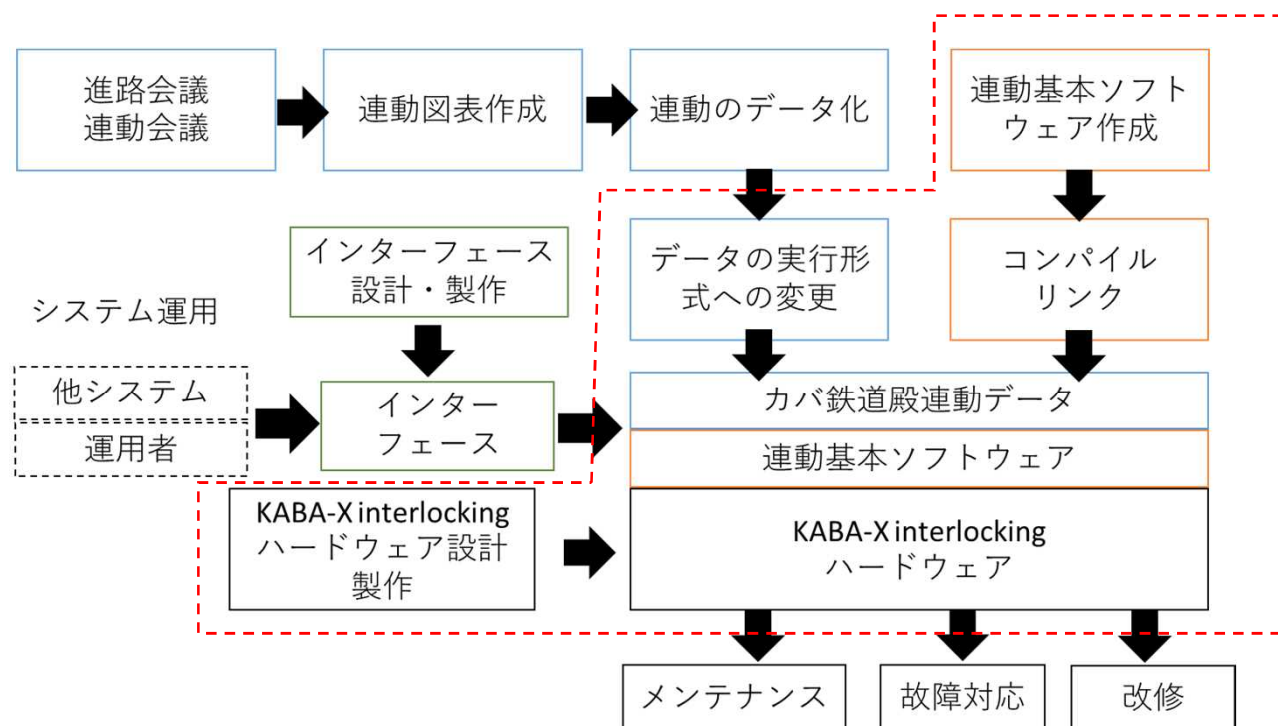
2-3いろいろな境界

IEC 62278 6.2.3.1b)
EN 50126-1 7.3.2.1 b)



2-3責任分担を決める

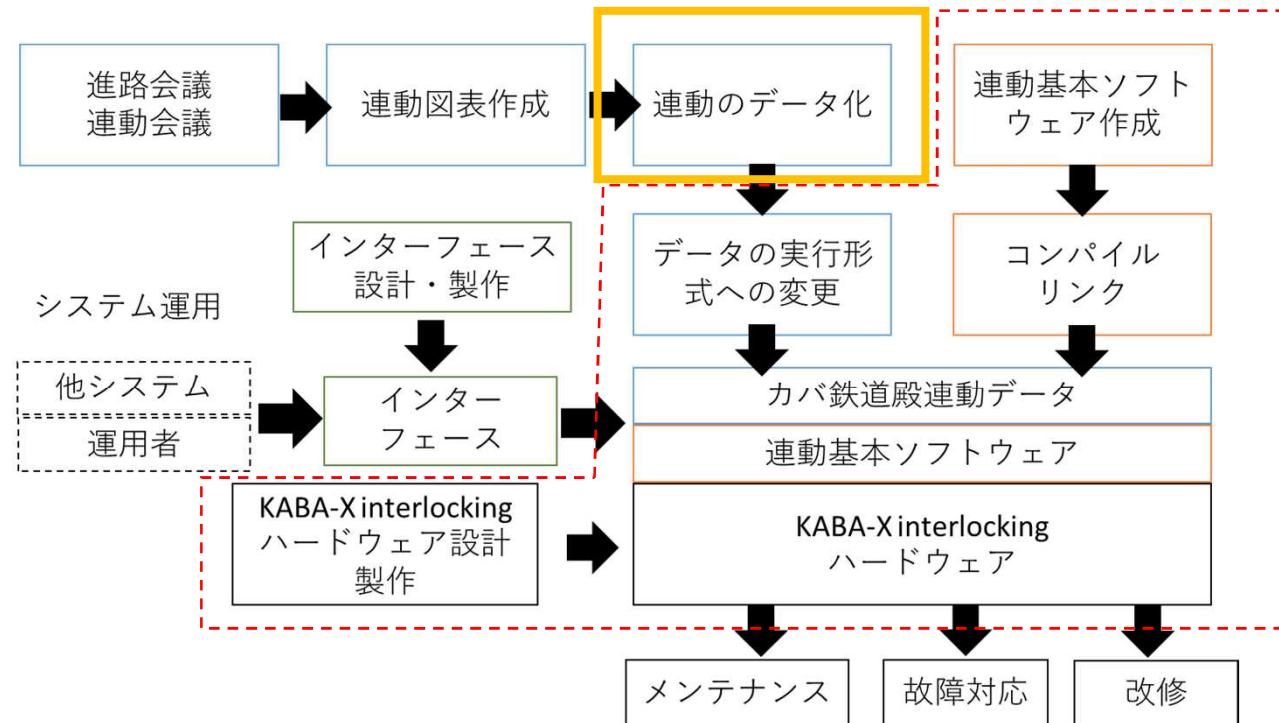
IEC 62278 6.2.3.1b)
EN 50126-1 7.3.2.1 b)



明らかに赤点線内はうちの担当だが、他はどうするねん。メンテナンス、故障対応、改修以外は担当外と思っているが、明確なものはないかもしれん。インターフェースはケースバイケースやな。ほかのシステムでやるかもしれん。システム運用は、そりゃあカバ鉄道やろうけどな。また、どこまで人手でやるか、機械でやるかも明確やないな。

2-3責任分担を決める

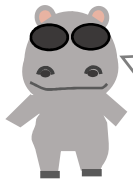
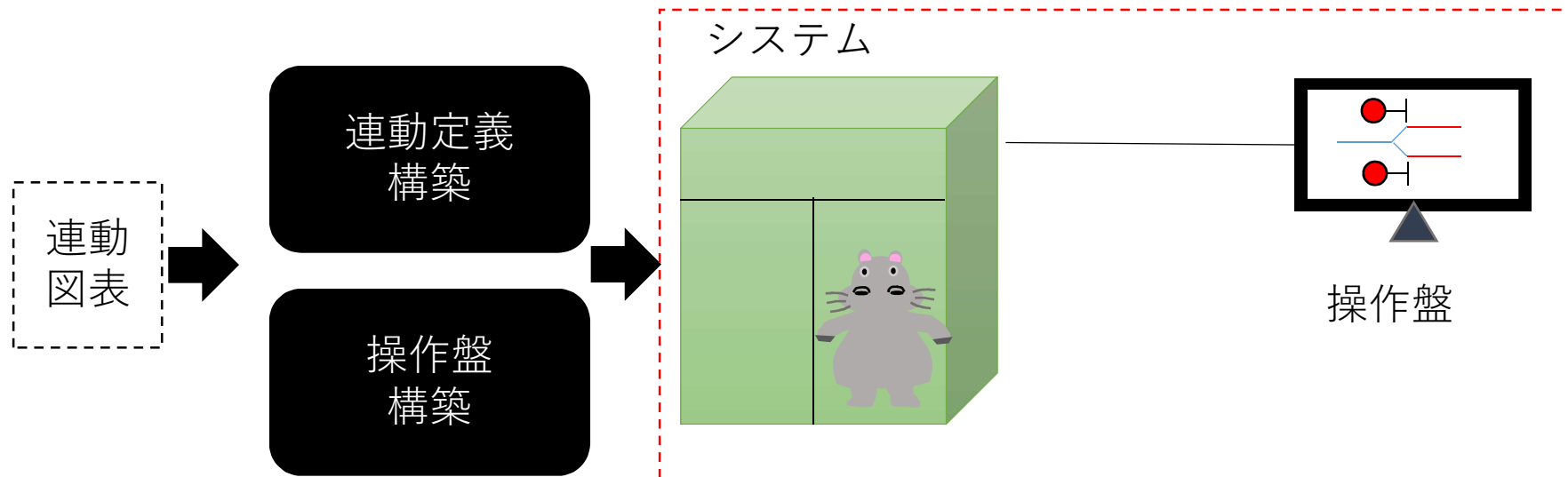
IEC 62278 6.2.3.1b)
EN 50126-1 7.3.2.1 b)



仮にカバ興業が連動のデータ化まで引き受ける場合、何かインターフェースが変わるんやろうか？装置自体のインターフェースは変わらんような。でもなんか役割が変わるような。人手でやるんか？機械でやるんか？

2-3 こういう境界も考慮

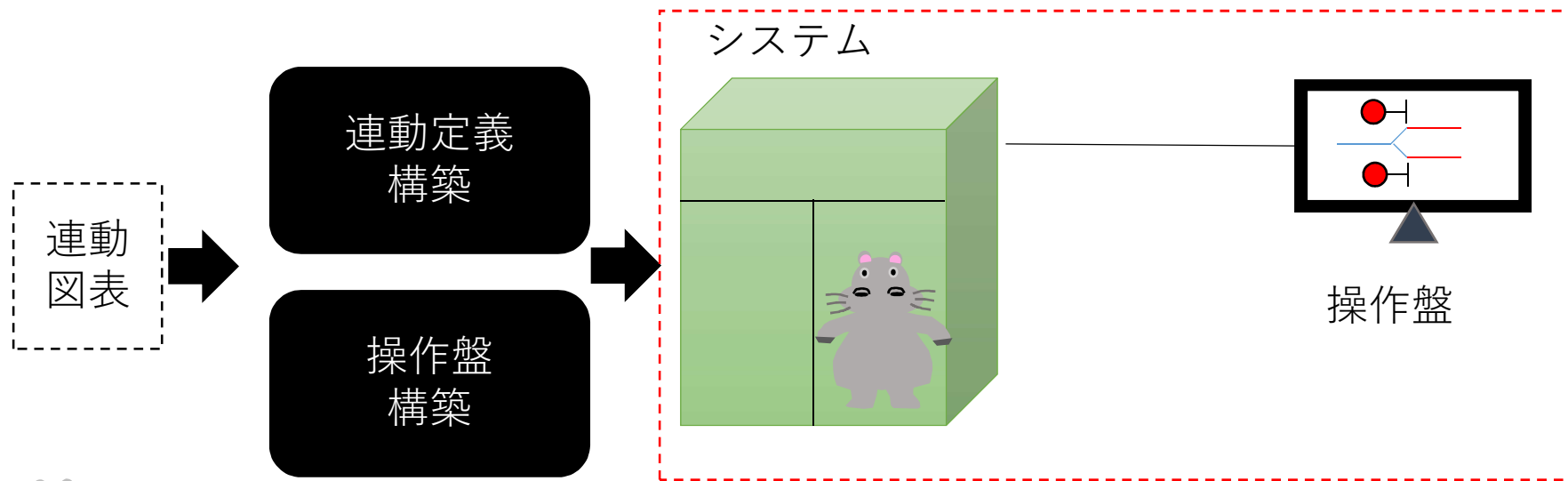
IEC 62278 6.2.3.1b)
EN 50126-1 7.3.2.1 b)



この構成を手で行うか、自動化するか、カバ興業とするのか、他社発注になるのか、相互影響から言ってどんな安全要求レベルが必要なのか、システムの境界と要求はめっちゃ重要なんか分かったで。

2-3 こういう境界も考慮

IEC 62278 6.2.3.1b)
EN 50126-1 7.3.2.1 b)

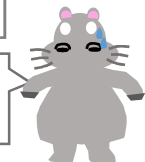
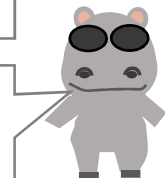


これもしエエ加減な連動定義構築されとったらどうなるんや。ヤバそうな感じしかせんで。。



確実に社長のクビが飛ぶ事態やろうな。。。もし連動定義構築をエエ加減なブタ工業が請けたら、ウチがとばっちりを受けるかもしれんな。。

なんとかせえ、カバお！

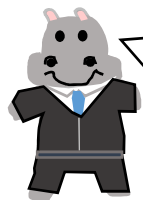
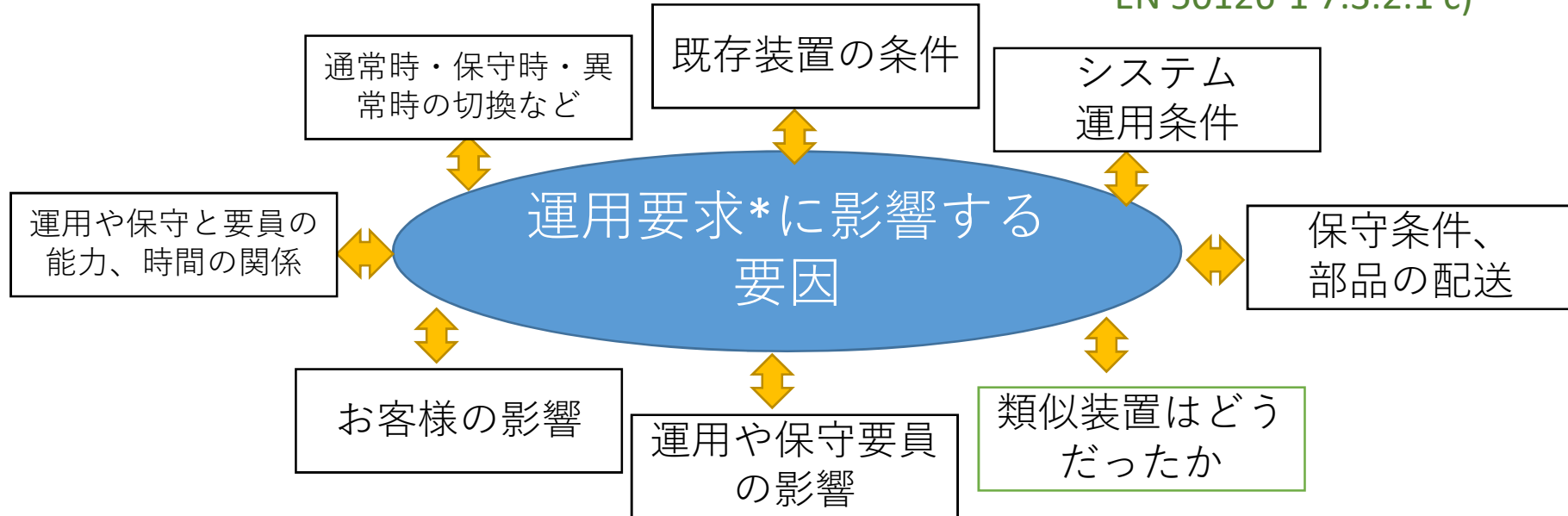


.....

- 2-1 システムがどんな目的を持つか決める。
- 2-2 数値的目標であるミッションプロファイルを決める。
- 2-3 RAMSの解析をする準備として
 - 2-3-1 システムの境界を決める。
 - 2-3-2 システムに影響する運用要求の範囲を決める。
 - 2-3-3 ハザード解析の範囲を決める。
- 2-4 RAMに影響を与えそうな事項とその評価をやってみて、感じをつかむ。
- 2-5 ハザードの検出をやってみて、感じをつかむ。
- 2-6 RAMと安全に関する計画をまとめ始める。

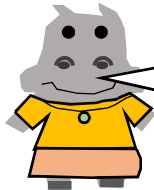
2-3システムに影響する運用要求要因

IEC 62278 6.2.3.1c)
EN 50126-1 7.3.2.1 c)



会社経営の検討範囲と似てるな！
カバおの能力は今後に期待やけど、拘束時間を倍にして埋め合わせたら今の経営規模は2倍にできるな！

やせる思いです。辞めます！



これらの条項を明らかにしていけば、運用要求が決まり、現在考えているシステムとの差分が分かりますよね。

2-3システムに影響する運用要求要因

IEC 62278 6.2.3.1c)
EN 50126-1 7.3.2.1 c)



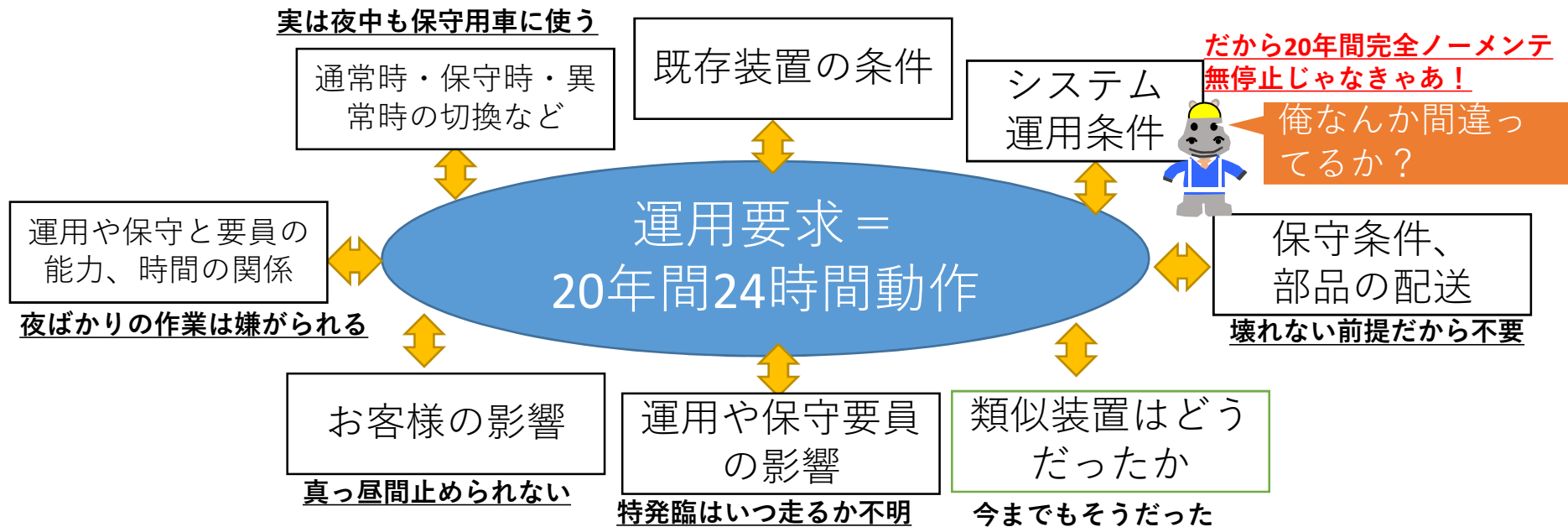
連動装置って基本的に取り替えまで連続稼働やんな。

ま、まあそうですね。（絶対悪いことが起こる。。。）



ということは、ウチが取り替えるというまでに故障したら、カバ興業は責任をとってくれることになるな。

そ、それは保証できませんよ。（おっさん何いってんねん。。。）



2-3システムに影響する運用要求要因

IEC 62278 6.2.3.1c)
EN 50126-1 7.3.2.1 c)

分かりました！カバお、清水の舞台から飛び降りた気持ちで技術にやらせます！



さすがやねえ、カバおくん。営業の鏡やで！



ウチも^{あきな}商いをやっております。エライ申し訳ないですが、追加費用200%いただいてもよろしいでしょうか？



なんやそれ！もうええわ。今まで通り3年ごとの検査やった方が安いんやろ！



さすが課長さん！関西人の鏡ですなあ！よく分かっていただきまして、ありがとうございます！



システムに影響する運用要求は、結局機械の要求に多く割り振るか、人手の方に多く割り振るかによってコストや手間、安全性など総合的に判断して今までも決めていきますよね。

RAMSでは、このようなことを記録しておくことになります。後で何でこんな判断したのかよく分かるように、見直しをするときに役立つようにです。

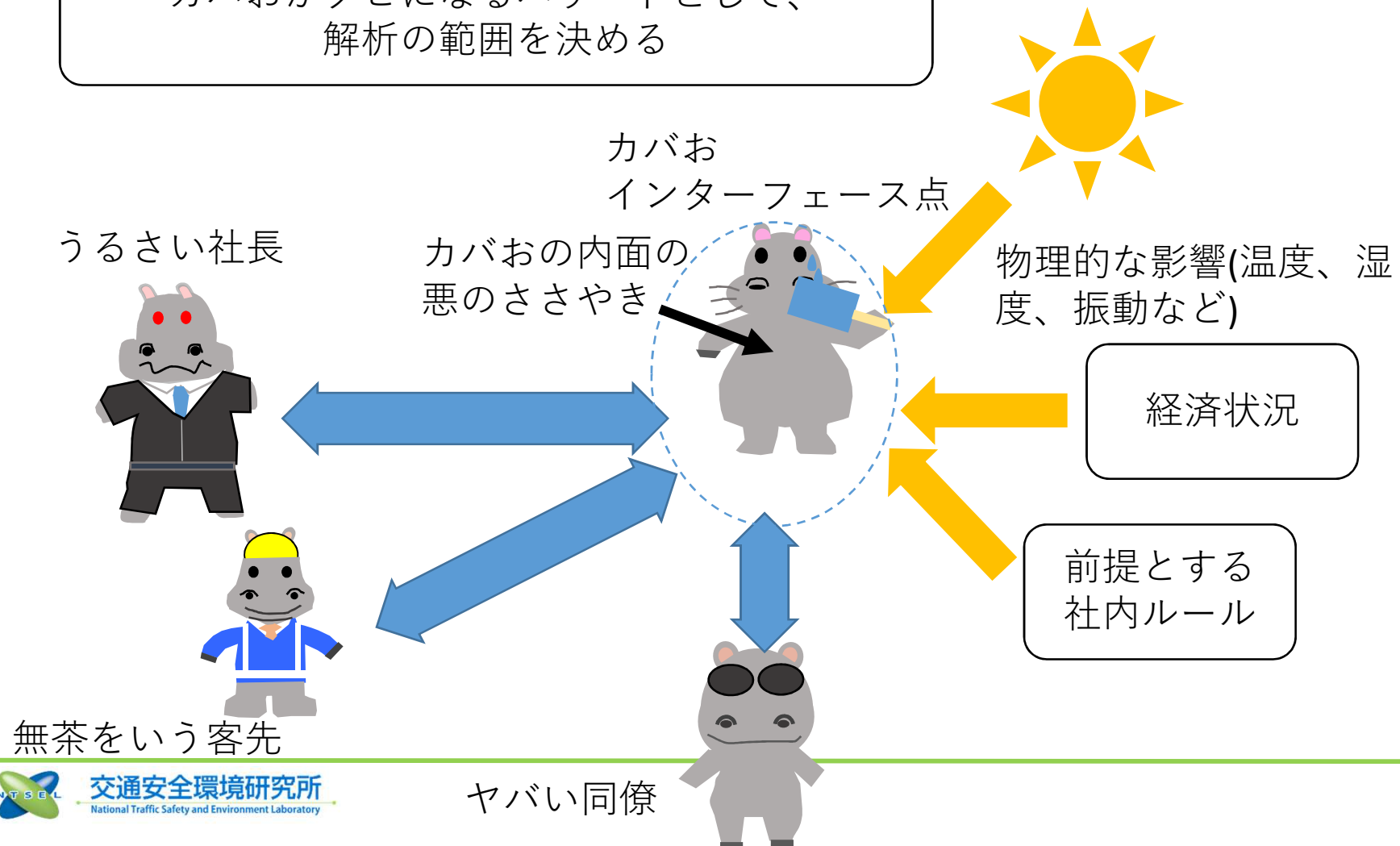


- 2-1 システムがどんな目的を持つか決める。
- 2-2 数値的目標であるミッションプロファイルを決める。
- 2-3 RAMSの解析をする準備として
 - 2-3-1 システムの境界を決める。
 - 2-3-2 システムに影響する運用要求の範囲を決める。
 - 2-3-3 ハザード解析の範囲を決める。
- 2-4 RAMに影響を与えそうな事項とその評価をやってみて、感じをつかむ。
- 2-5 ハザードの検出をやってみて、感じをつかむ。
- 2-6 RAMと安全に関する計画をまとめ始める。

2-3ハザード/リスク 解析の範囲を決める

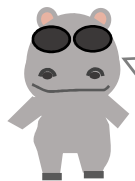
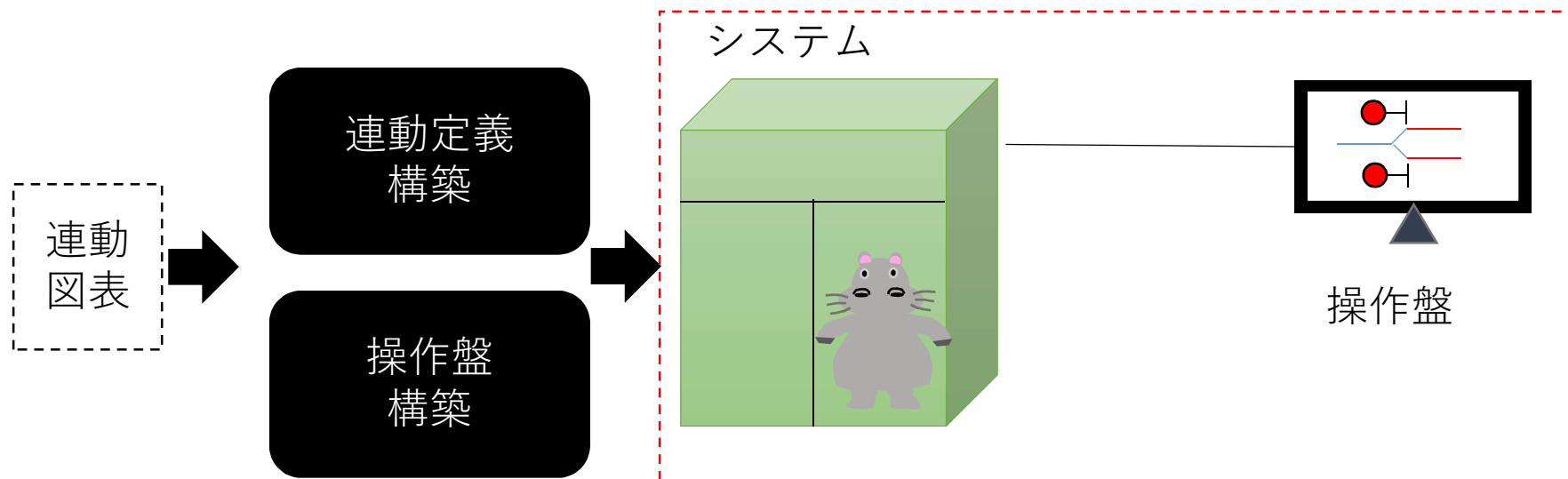
IEC 62278 6.2.3.1 d)

カバおがクビになるハザードとして、
解析の範囲を決める



2-3ハザード/リスク 解析の範囲を決める

IEC 62278 6.2.3.1 d)



この黒の部分、やるべきかどうか、どうしようか。。。

2-3ハザード/リスク解析の範囲を決め、 システムの対象とするか考える

IEC 62278 6.1.3.1d)
IEC 62278 6.1.3.2b)



社長としては、まず設計をする前に、どこから安全に対して悪影響を受けるかざっくり考えておいて、どこまでやるかを判断せなアカンわな。以下がプランA,B,Cや。



データ作成はうちの担当じゃないので、正しくないと、連動の動作は正常に行われず、人命の影響がある可能性があるため、データ誤りの動作異常についてカバ興業は一切の責任を負いません。

これをカバおに言わせようか。。なんかこう、失注しそうやな。。

このような安全使用条件を Safety related application conditions(SRAC)といいます。



うちにデータの作成も任せてください。連動図表から自動で変換する装置を作りますから。

変換装置の安全性について、かなり検討が必要そうやな。できるかな。



データ作成体制を強化し、人手（カバ手？）でデータ作成します。

カバ鉄道に付け込まれるだけの気がする。悩ましいな。。

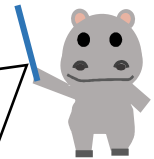
2-3 差分を知る



正直言うと、システムって一から作るってことは少ないんや。
今までのものを活かして、差分だけミッションプロファイルや解析の範囲決めたいな。

e) identification of the system and related documents, including assumptions made about particular functions or subsystems that are different from an existing reference version, explicitly stating and justifying the deviations.

システムの同定、関係する資料をはっきりさせる中で、既存のものからどのように違うかを含むことに EN 50126はなっているんですよ。
(IEC規格は明記されていません)



「違いがわかる男。」が大事なんやで。やっぱり。。

そんなコーヒーのテレビコマーシャルとっくに封印されて知っている人いませんよ。。



- 2-1 システムがどんな目的を持つか決める。
- 2-2 数値的目標であるミッションプロファイルを決める。
- 2-3 RAMSの解析をする準備として
 - 2-3-1 システムの境界を決める。
 - 2-3-2 システムに影響する適用要件（運用・保守・外部装置など）の範囲を決める。
 - 2-3-3 ハザード解析の範囲を決める。
- 2-4 RAMに影響を与えそうな事項とその評価をやってみて、感じをつかむ。**
- 2-5 ハザードの検出をやってみて、感じをつかむ。**
- 2-6 RAMと安全に関する計画をまとめ始める。

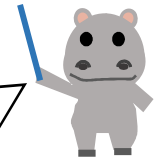


2-4,5 RAMSにおけるシステムのヤバいところをつかんでおきたい



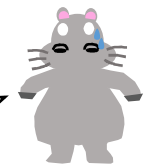
社長として、やっぱりその装置がどれくらい失敗するとヤバいかは事前につかんでおいて、見積もりとか、工期とか、人の配置とか、安全性を考えたいとは思うわな。

そりゃあ、経営に責任を持つものとしては、そうですね。ヤバい件名はお金をかけて時間もかけてやらないといけないですよ。これをPreliminary RAM Analysis、安全に関してはPreliminary Hazard Analysisっていうんですよ。大事ですよ。



おい、カバお、わかったか。危険予知やぞ危険予知。カバ鉄道さんにお金ようけもらっとけよ！

「ヤバいからお金ください」でお金くれるような激アマな会社ないですよ。ちゃんと理由を言わんとアカンに決まってるじゃないですか。



2-4,5この状況下でカバおがどんな好ましくない行動に出るか考えてみよう



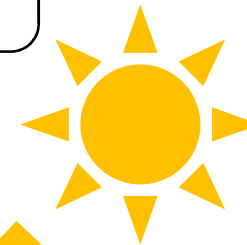
大変だ何とかしなきゃ！

やる気がなくなり、仕事の品質が下がる

会社に反感を持ち、お金をくすねる

etc...

納期をごまかし、会社の信頼が失墜する



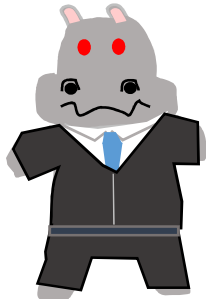
カバお
インターフェース点

物理的な影響(温度、湿度、振動など)

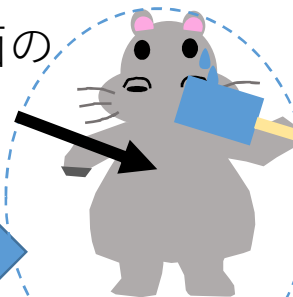
経済状況

前提とする
社内ルール

うるさい社長

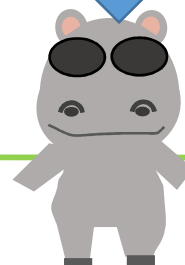


カバおの内面の
悪のささやき



無茶をいう客先

ヤバい同僚



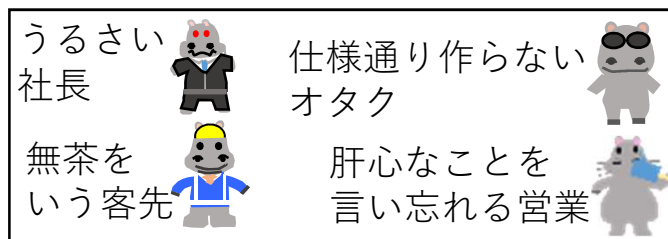
2-4,5 RAMSに影響を与える事象を考えてみよう

IEC 62278 6.2.3.2 a)b)

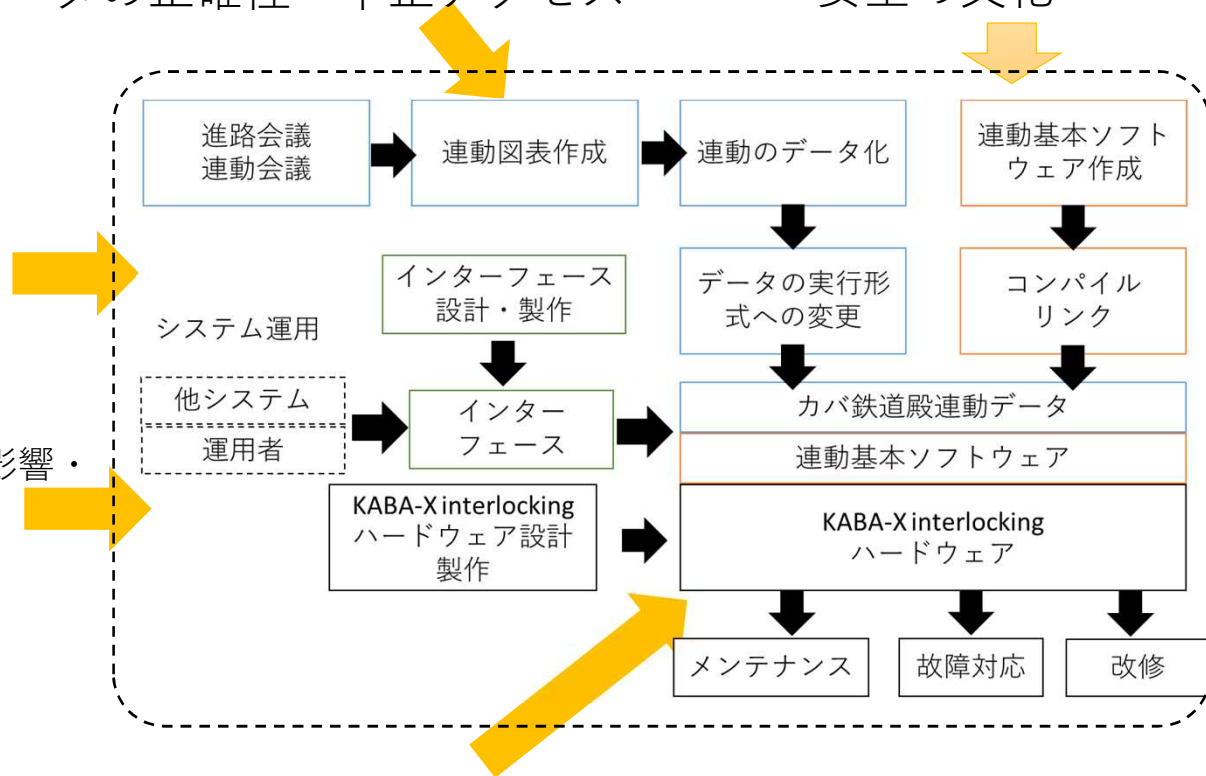
データの正確性 不正アクセス

投資金額の制約
安全の文化

人的悪影響



他装置からの悪影響・ハッキング



物理的な影響(温度、湿度、振動など)

2-4,5中身も決まっていらない のにどうやって解析するの？

IEC 62278 6.2.3.2 a)



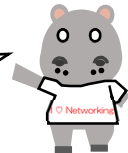
社長として、いろいろなヤバそうなことはつかんでおきたいのはあたりまえやわな。

でもまだシステムの中身全然決まってないですよ。どうやって解析するんですか？リスク解析は第3段階じゃないですか？



やる気になったら何でもできる！1.2.3.ダー！

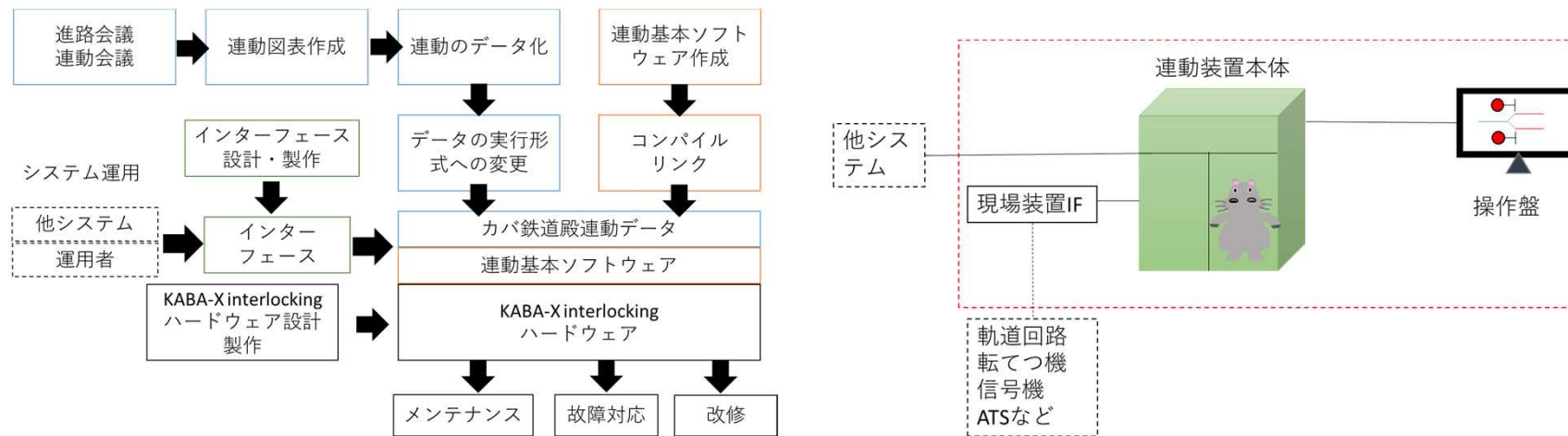
無茶苦茶や。。。。



で、本当のところどうすればいいのでしょうか？

2-4,5 こう考えたら いかがでしょうか？

分かっている範囲で業務や装置をモデル化



業務のモデル化

システムのモデル化

その情報の流れが間違ったり、来なかったり、遅れたり、順序が違ったりしたらどうなるかイメージ



2-4,5影響を与える事象と結果、 対処の必要性をまとめる

IEC 62278 6.2.3.2 a)

内容	影響	悪影響	対策の必要性	ID
連動図表の情報が間違っている	安全	錯誤信号現示 異なった転てつ装置の転換	人命を失うため必要	XXX-001
	信頼性	信号機が現示されない	輸送影響が大きく必要	XXX-002
連動データが作成できない	信頼性	稼働不能	工事日程への影響のため、 対処必要	XXX-003
連動データが遅れる	信頼性	納期遅延	工事日程への影響のため、 対処必要	XXX-004
連動データが誤る	安全	錯誤信号現示 異なった転てつ装置の転換	人命を失うため必要	XXX-005
連動図表と連動データの作成順序が違う	安全	異なるバージョンによる錯誤信号現示など	人命を失うため必要	XXX-006
:				

システムの故障による不安全側遷移だけ注目してたけど、そういう問題だけじゃなさそうですね。。。。



- 2-1 システムがどんな目的を持つか決める。
- 2-2 数値的目標であるミッションプロファイルを決める。
- 2-3 RAMSの解析をする準備として
 - 2-3-1 システムの境界を決める。
 - 2-3-2 システムに影響する適用要件（運用・保守・外部装置など）の範囲を決める。
 - 2-3-3 ハザード解析の範囲を決める。
- 2-4 RAMに影響を与えそうな事項とその評価をやってみて、感じをつかむ。
- 2-5 ハザードの検出をやってみて、感じをつかむ。
- 2-6 RAMと安全に関する計画をまとめ始める。**



RAM Planについてご説明します！

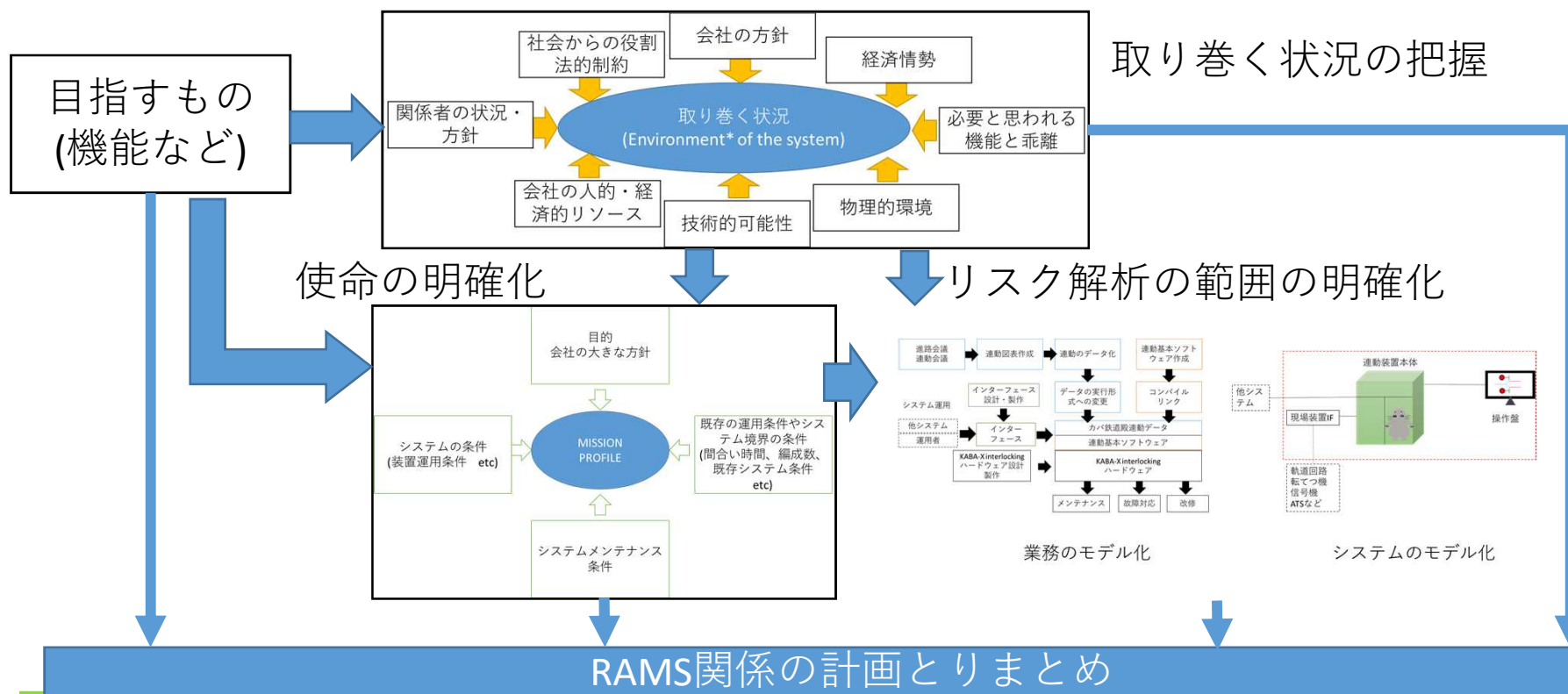
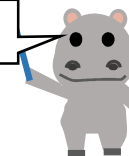
2-6 今までの議論の整理



おい、おまえら！いろいろ議論したけど、そろそろ整理しないと、オレの頭がパンクしそうやで。どういう方針で行くかそろそろ決められるんちゃうか！ おまえら、イヤそうやな。



この段階で、RAMSに関する計画をひとまとめすることになっているんですよ。

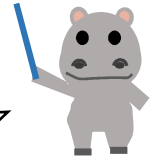


2-6 RAM Plan*とは



社長にやれと言われたけど、いったい何書けばいいの？

マネジメントの計画、信頼性、アベイラビリティ、保守性についての解析と計画について書くんですよ。



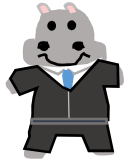
どうせあの社長は、「俺の言うことすなわちマネジメント」と言うに決まってるし、本当に大丈夫か。。



おれが最終決定者だ！オレがCEOだ！おれが決める！カバにはボスは一人しか必要ないんやで！

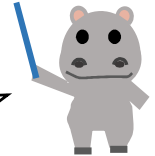
*IEC 62278においては、RAM Planは定義されておらず、RAM Programmeとして第4段階で定義されています。しかしながら、安全に関する計画であるSafety Planを第2段階で策定している以上、RAM Planを同じように策定する方が自然と思われるので、EN 50126に対応して、ここに持ってきています。IEC 62278では、RAM Programmeを後に策定することから、Safety Planと矛盾しないようにするためのRAMS policy (6.2.3.3)を先に作ることにしています。

2-6 Safety Planとは

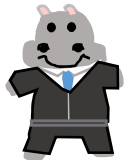
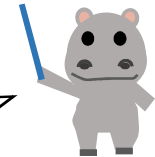


おれはカンが鋭いねん。Safety PlanはRAM Planの安全版やろ。当たりやろ！

(そんなん当たらないほうがおかしいと思うけど)
あたりです！やっぱり社長はすごいですね！

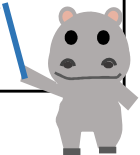


で、カバ興業は、どのような安全に対する計画をお持ちですか？



いろいろカバ鉄道さんに言われてその都度作っているんやけど、なかなか
收拾がつかへんねん。そろそろ「これや！これこそカバ興業の安全や！」
というのを作りたいねん。何書くかわからへんねん。

documented set of time scheduled activities, resources and events serving to implement the organisational structure, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given safety requirements relevant to a given contract or projectと IEC 62278にはSafety Planについて書かれていますね。



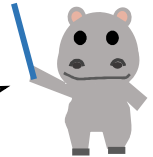
2-6 具体的にはどんなこと書くの

EN 0126-1 Annex A.3



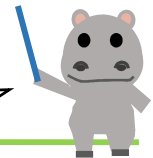
CEOとして、部下に指示するとき、具体性がほしい！なんかないのか？

あまりいいたくないけど、あります。EN 50126-1 Table A.1にあります。



1. 受注前
導入対象のRAMS目標の評価
2. 事前検証
RAMS要求の評価
類似システムなどのRAMS評価
導入対象による安全の影響の同定
3. 入札
最悪ケースの事前RAMS解析
RAMS要求のシステムへの割り当て
リスク解析の実施
RAMに関する好ましくない事象の解析
RAMSに関するデータのアセスメント準備
入札各章ごとのRAMSに関する懸念の評価 (以下略)

と計画しなければならないことが列記されています。

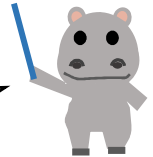


2-6 鉄道事業者の留意点



鉄道事業者が書くとなると、どういう点に注目すればいいかな。。

さっきの資料の裏返しを考えればいいのではないのでしょうか？



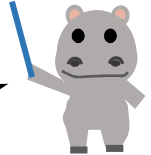
1. 受注前 → 鉄道事業者におけるコンセプト段階
導入対象のRAMS目標の評価 → 導入対象装置のRAMS目標の決定方法
2. 事前検証 → システムの定義と使用条件
RAMS要求の評価 → RAMSの観点のMission Profileの妥当性の検討
類似システムなどのRAMS評価 → 類似システムの調査対象抽出と調査内容
導入対象による安全の影響の同定 → 既存システムの調査対象抽出と調査内容
3. 入札
製作者評価方法
4. 契約後
製作者のマネジメント体制の評価方法
安全解析方法と評価方法
保全方法
受け入れと試験体制
改修と取り替え計画

2-6 体制や図書は？



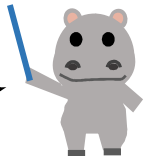
計画というと、体制やら、つくらなアカン書類とか、いろいろ考えなあかな。RAMS規格にのってるんやろ。

あまりいいたくないけど、IEC 62278には、あまりあるとはいえないです。

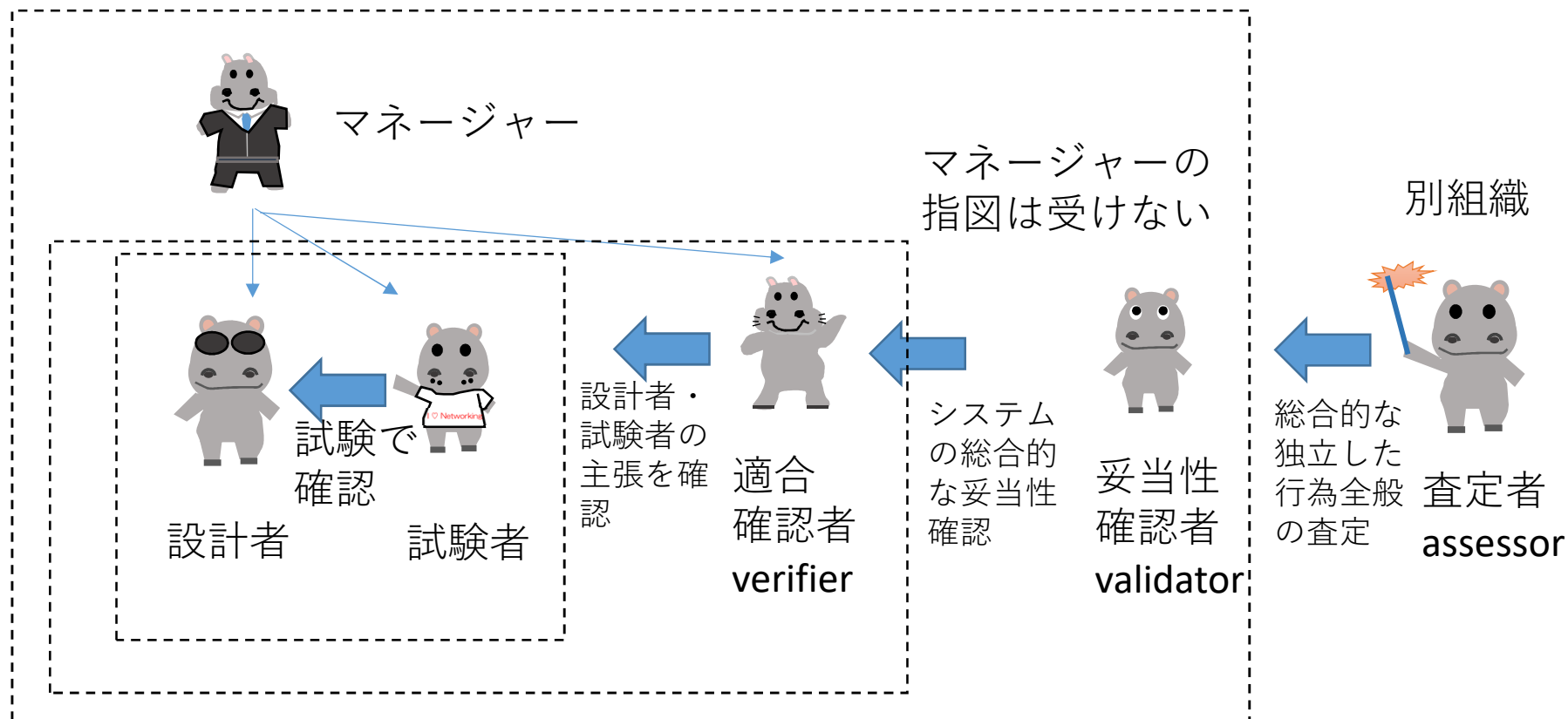


と、いうことは、ハッキングカバとか、カバ実課長に考えさせるってことやな。「おい、おまえら、やれ！」

それは、各々の技術的な規格に載っているので参照してください。



2-6 体制の例



適正な態勢・必要な能力・教育を安全性レベル、品質管理規定及び規格に合った形で定める。IEC 62278には体制の例がなく、他の規格を参照して定めることが多い。

2-6 準備する図書の例

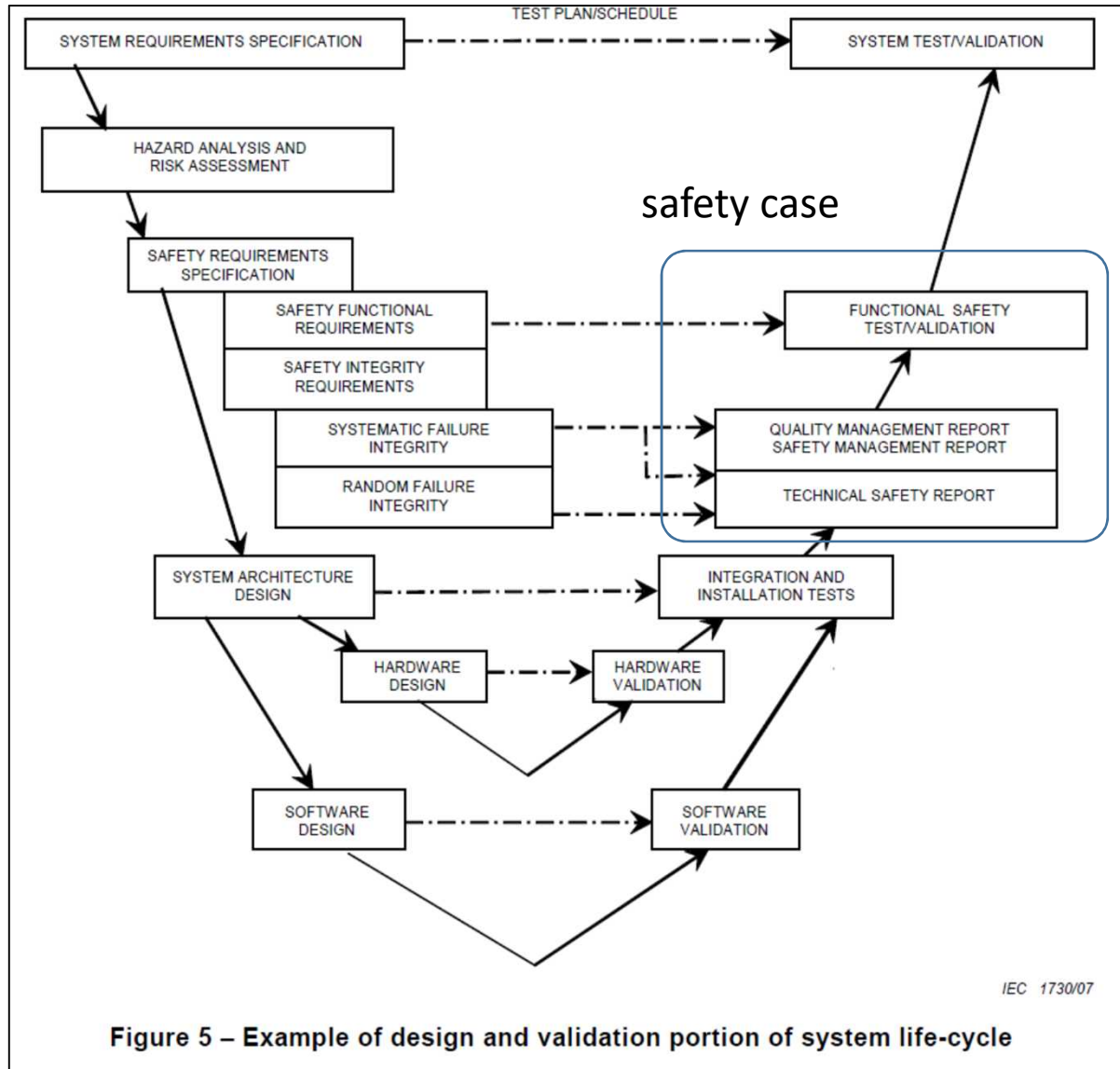
(主にハードウェア安全面)

IEC 62278 6.2.3.4 e),g)

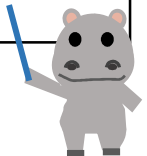
EN 50126-1 7.3.2.3 e)

IEC 62425 5.3.2

IEC 62279 Ed.2 5.3



IEC 62425における、システム要求仕様から総合テストまでの行う事項を示したものです。各段階で要求・その要求のverification、試験計画、試験計画のverification、試験の実施とそのverificationや、安全に対するまとめであるsafety caseを作成することが述べられています。



2-6 準備する図書の例

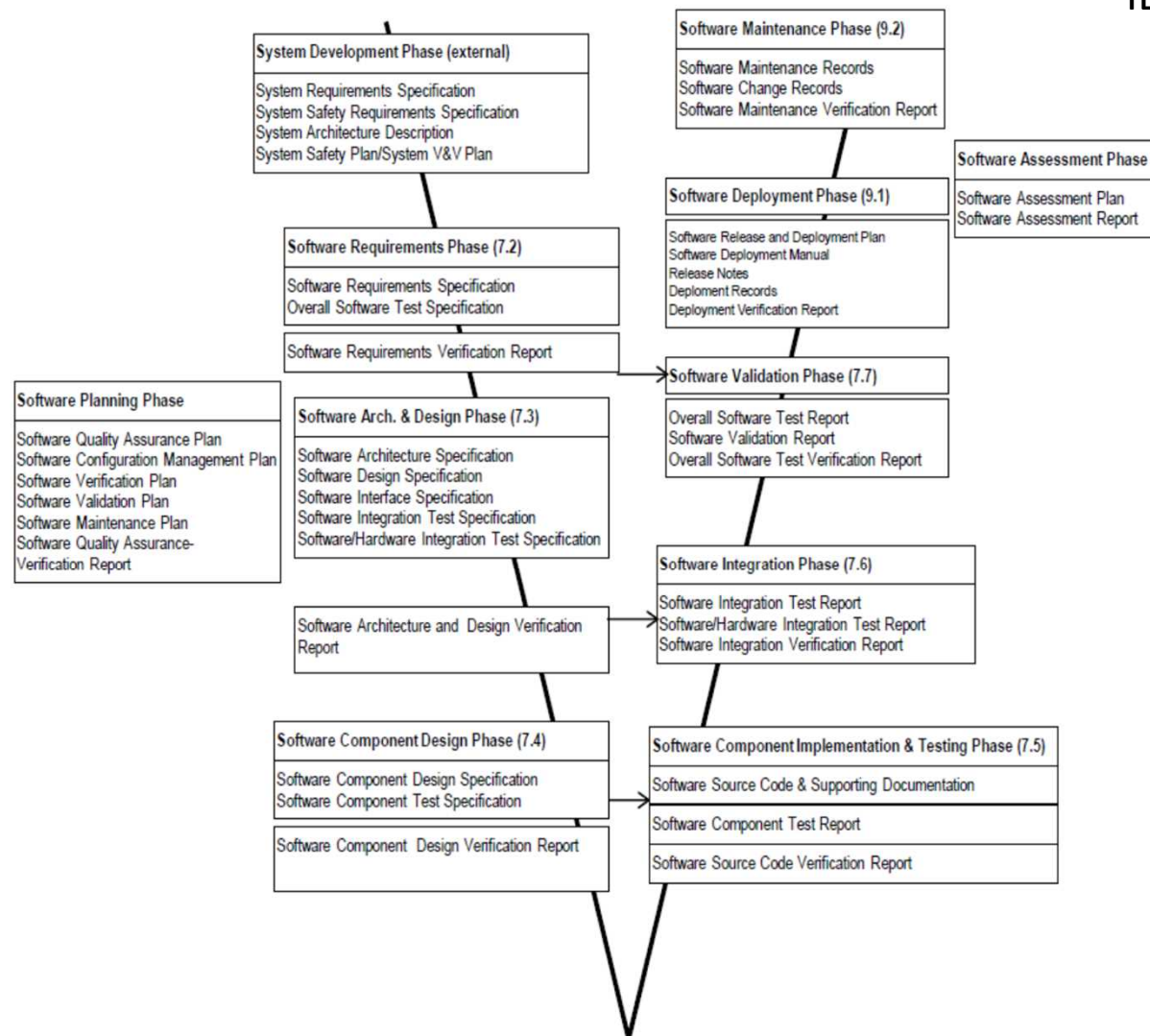
(主にソフトウェア安全面)

IEC 62278 6.2.3.4 e),g)

EN 50126-1 7.3.2.3 e)

IEC 62425 5.3.2

IEC 62279 Ed.2 5.3



IEC 62279における、ソフトウェアの観点で、システム要求仕様からメンテナンスまでの行う事項を示したものです。各段階でどのような文書が必要か述べられています。

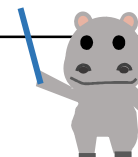


Figure 4 – Illustrative Development Life cycle 2

まとめ

2-1 システムがどんな目的を持つか決める。

規格には今一つはっきり書いていませんが、システムの目的を決めましょう。

2-2 数値的目標であるミッションプロファイルを決める。

目的を達成する数値がないと作れませんし、解析評価もできません。

2-3 RAMSの解析をする準備として

2-3-1 システムの境界を決める。

2-3-2 システムに影響する適用要件（運用・保守・外部装置など）の範囲を決める。

2-3-3 ハザード解析の範囲を決める。

どこまでがシステムとして担当する範囲か決めないと、解析評価もできません。

2-4 RAMに影響を与えそうな事項とその評価をやってみて、感じをつかむ。

2-5 ハザードの検出をやってみて、感じをつかむ。

システムを構築していく際の、重点を把握しましょう。また、安全機能を大まかに把握しましょう。

2-6 RAMと安全に関する計画をまとめ始める。

計画がなければ何もできません。システムの目的・数値的目標・取り巻く背景・担当範囲・安全機能などから必要な計画を策定しましょう。

