

システム要求と機能割り当て

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！」

鉄道事業者 カバ鉄道チーム



カバ鉄道 社長
品格の経営、根拠ある経営



カバ鉄道 電気課長
口癖:安くてエエもん持って来い！



カバ鉄道 乗務員 カバどん
いつかは自動化されるかも。ドキドキ

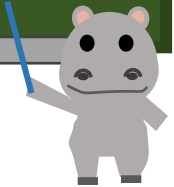


ブタ工業 社長
カバ興業を凌ぐ強い体質づくり

バズバズ

1. はじめに

- 連動装置の機能って何でしょうか？JIS E3013において、連動装置は「信号機、転てつ機などの相互間の連鎖を行う装置の総称」と定義されていますが、それは最低限必要な機能で、一般的にそれ以外の機能を含んでいることがほとんどです。
- 例えば、連鎖以外にも、「信号てこを扱うと、関係する進路を連動図表の定義をもとに開通させるよう関係する端末を制御する機能」は確実にありそうです。
- 機能を定義し、それをどのように実現していくかの初期段階について、少し考えてみたいと思います。



2. システム要求・機能定義の重要性



社長！いつもいつも頼ってばかりでごめん。この前ウチの社長から「連動装置ってなんや」って聞かれたんや。そんなもん、当たり前すぎて答えられへんかったんや。

ええっ、そこからですか。それはまあ、意外に難しい質問かもしれないですね。



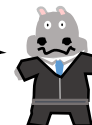
そこやねんな。「お前ら安全投資案件ゆうてくるけど、大体前のと比べて差分しか言わへんけど、まず全体の機能ってなんや。」って言われたわ。

それは誠に遺憾ですな。社長さん  には常識っていうもの知っていただかないと。



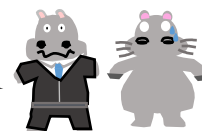
いやー、「投資判断をするときは、機能とそのレベルがしっかりと運行の体系に合っているのか、安全の目指すべきレベルに合っているのか、カネがおうてるかどうかの説明がないと判断のしようがないやろ。ワシのゆうてる事まちごうてるか？」って言われんや。いつもの正論パンチや。

そこについては私も口を酸っぱくして、しっかり機能に見合った値付けをするように、社員に言っており、かつ競争力の高い製品開発に努めておまして。。



いやー、多分社長は、すでにあらかた答え持っとんねん。あれはかなりタヌキやからな。あれは地雷や。間違うと爆発する。ヤバいで。ちゃんと理屈まとめて、報告頼むで。

(ま、丸投げやん。。)



2. システム要求・機能定義の重要性

おい！ハッキングカバ、電子連動ってなんや！

ハァ？なんやそれ。それってオレらがなんであるかを決めることか？ソフト中心にやってるオレが決めてええんか？

そんなんゆうても誰が決めんねん！

ハ〜！それって基本的に客が決めるんちゃうんか。提案営業やったら、「こんなんエエんじゃないですか」って営業を中心にみんなで決めるんちゃうんか。

じゃあ一般的にどうすんねん。

業務要件(Business Requirements)

ユーザー要求(User Requirements)

機能要求(Functional Requirements)

非機能要求(Non-Functional Requirements)

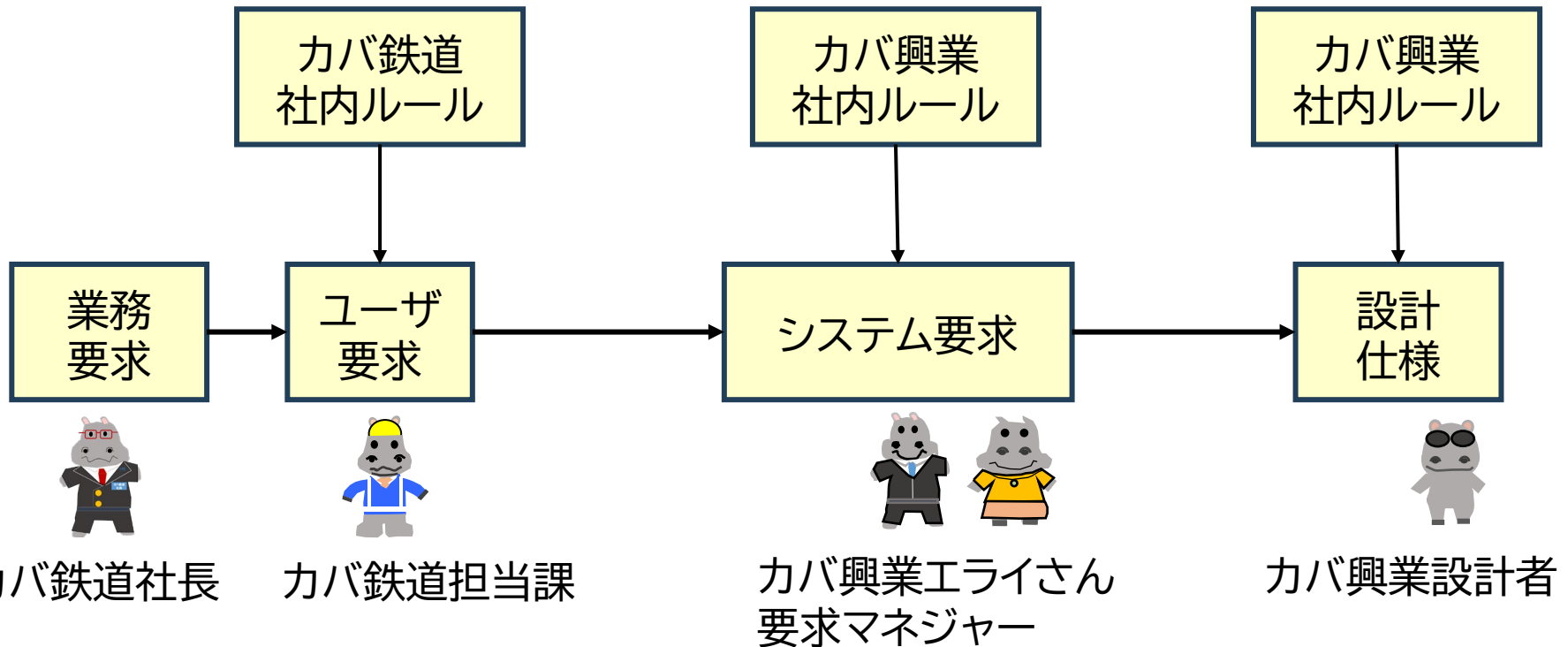
システム、ルール上の
制約など

システム要求として扱う

2. 機能定義の重要性

そんなんゆうても誰が何すんねん。

ハア？なんやそれ。社長のくせにそんなことも分からんのか！また団交したなってきたなー。団交の席で、だれが何をすべきかじっくり議論しようや！なー社長！



2. システム定義の重要性

と、言われても各々の違いが分からない。



業務要件(Business Requirements)

事業を進めていく上で、当該システムを導入して、どうありたいかという要求

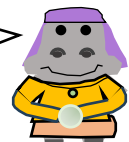
- BR1:駅構内での死傷事故を防ぐために、駅係員の誤った信号操作を無効化したい。
- BR2:併せて、駅係員がスイッチを扱うだけで、列車に対して進路を開通させる作業の効率化を行いたい。
- BR3:機器室の省スペース化を進めて、土地を生み出し、生み出した土地で商売したい。
- BR4:故障があったとき、原因がすぐに絞り込めるようにし、保守の効率化を図りたい。
- BR5:保守要員数を勘案すれば、少なくとも20年はシステム交換を考えていない。
- BR6:当該機器に用意している減価償却費は累計XXXX万円であり、10%超過までは許容したい。
- BR7:各駅とも同一のシステムで共通化したい。

電子連動装置一つにしても、いろいろな思いがありそうやな。で、これは全部公開されるわけではなさそうやから、カバ興業としても、こういうことを考えて予想して開発を行なわなアカンのやろうなあ。占い師連れてくるか。。



ユーザー要求(User Requirements)

見えた見えた
カバ鉄道の方針が！



2. システム定義の重要性

ユーザー要求(User Requirements)

ユーザーの価値の提供のため、どのようにシステムが使用されるか(ユースケース)、どうあればよいか(User stories) を抽出し、ユーザー要求と受け入れられるレベルを決める。

例

- UR1:進路を設定し、保持すること。進路は連動図通りにデータで設定できること。
- UR2:UR1以外の進路設定においては、遠隔でポイントを転換し、駅係員の注意力で進路を開通させること。
- UR3:連動図表通りにデータ設定で連鎖させること。結果を表示すること。
- UR5:単線区間においては、運転方向を決定し、保持すること。
- UR6:関係する進路情報は必要に応じ連動図表通りデータ設定し踏切に渡すこと。
- UR11:一連の動作は5秒以内に完結すること。
- :
- UR21:大きさは最大でも25平方メートルの機器室に収納できること。
- :
- UR31:一連の動作記録は保持し、10年間上書きされないこと。
- :
- UR41:安全に関わる機能の危険側遷移は1時間当たりXXX以下とすること。

2. システム定義の重要性

機能要求(安全関連機能含む)

ある条件下でシステムの動きを定義するために設定

例:立ち上げ時

- FR1-1:ロギングを開始する機能
- FR1-2:メモリ、関係するインタフェース、クロックの健全性を確認し、異常であれば停止状態に遷移する機能
- FR1-3:関係するパラメータ、アプリケーションデータを外部メモリから読み込み、その正当性を確認する機能。異常であれば停止状態に遷移する機能。

例:通常処理時

- FR2-1: 外部装置からデータを読み込む機能
- FR2-2: 制御盤入力を読み込む機能
- FR2-3: 定義された論理演算を行う機能
- FR2-4: 外部装置にデータを出力する機能
- FR2-5: 制御盤に出力する機能
- FR2-6: ロギングをする機能
- FR2-7: 論理演算異常を検知し、異常時停止状態に遷移する機能

例:停止状態

- FR3-1: 遷移した場合、ログ記録後、電源を切断する機能。



カバ実課長！カバ鉄道だけではなくほかにも売れるよう機能を考えてや！



承りました！

2. システム定義の重要性

非機能要求

システムを構築するために必要な
数値的な要件、制約を記載

→ハードウェア、ソフトウェアの製作には機能要求以外にも必要。

例:全般

- 供給電圧 DC 24V 最大電流20A以下
- 寸法、重量はXXXXXXXXとする。
- 動作温度湿度 XXXXX、保管温度湿度XXXXXXXX
- 処理能力として、最大2万論理、処理周期500ms

Etc..

立ち上げ時

- 2秒以内に立ち上がること。

⋮



カバ実課長！カバ鉄道だけではなくほかにも売れるよう機能を考えてや！



承いました！

2. システム定義の重要性

なんかいつも、「安全安全安全」しか言ってこなかったのに、今回は毛色が違うな。ワシの得意な「お客様に寄り添う経営」が来たか！



なんかごちゃごちゃにいろんなこと言われてて、いったいどうなっているのかよくわからないよ。なんか好き放題言われている感じで気分悪いんですけど。。

それを整理するのが「キミ」の仕事やろ。お客様の意見を聞き、また技術者の言うことも整理する。それがデキル営業や。

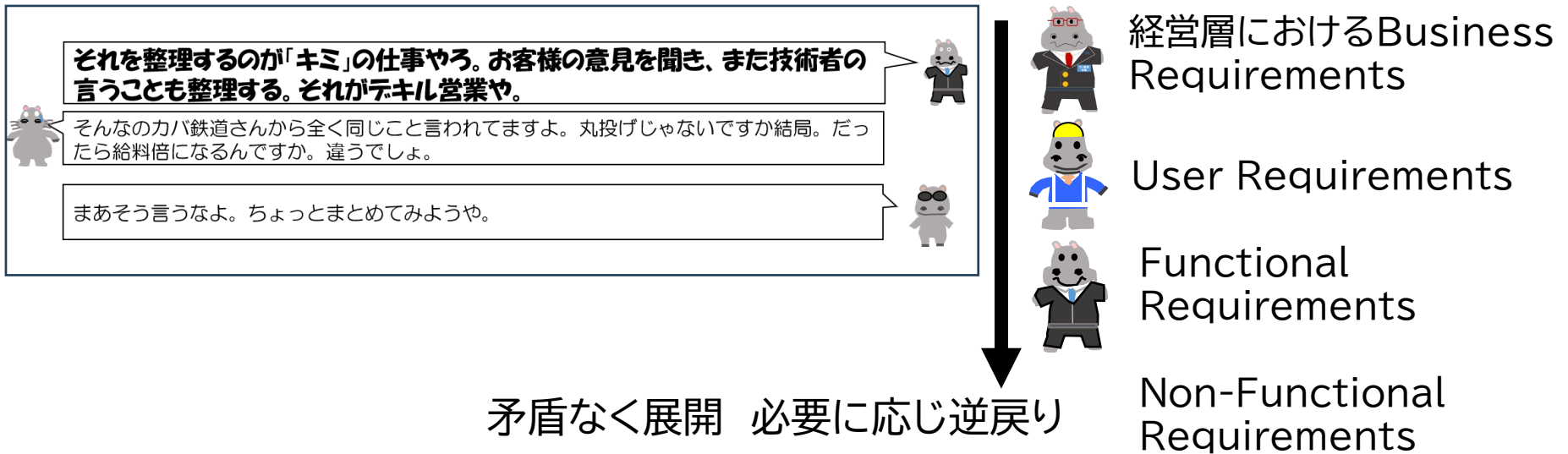


そんなのカバ鉄道さんから全く同じこと言われてますよ。丸投げじゃないですか結局。だったら給料倍になるんですか。違うでしょ。

まあそう言うなよ。ちょっとまとめてみようや。



3.しつこいですがトレースが重要



BR1:駅構内での死傷事故を防ぐために、駅係員の誤った信号操作を無効化したい。

UR3:連動図表通りにデータ設定で連鎖させること。結果を表示すること。
UR5:単線区間においては、運転方向を決定し、保持すること。

FR1-3:アプリケーションデータを外部メモリから読み込み、その正当性を確認する機能
FR2-1: 外部装置からデータを読み込む機能
FR2-2: 制御盤入力を読み込む機能
FR2-3: 定義された論理演算を行う機能
FR2-4: 外部装置にデータを出力する機能
FR2-5: 制御盤に出力する機能

3. またまた安全に逆戻りすみません

まあそういうなよ。ちょっとまとめてみようや。

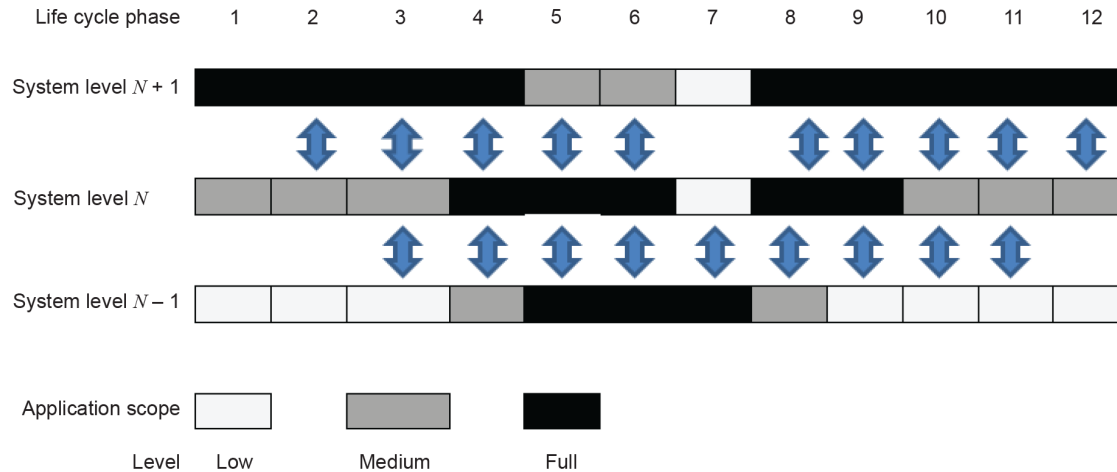


BR1: 駅構内での死傷事故を防ぐために、駅係員の誤った信号操作を無効化したい。

ここには暗黙的なリスクアセスメントがある。



なにそれ。

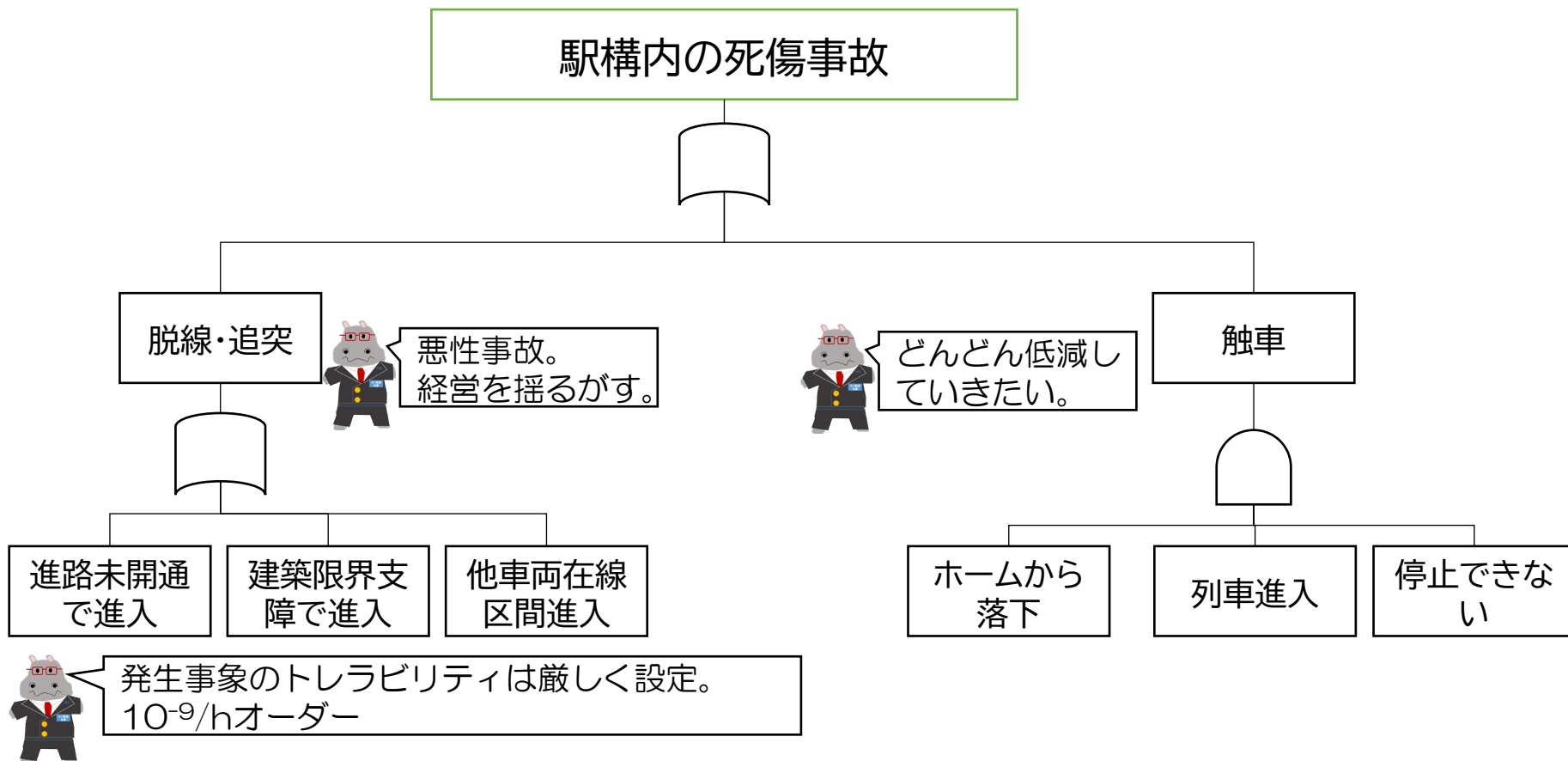


これ見たほうがいい。IEC 62278-1 Figure 10 - Example of life cycles at different hierarchical levels や。対象とするシステムより一つ上のN+1のPhase 3が真っ黒や。それがシステムレベルNに引き継がれるんちゃうか。



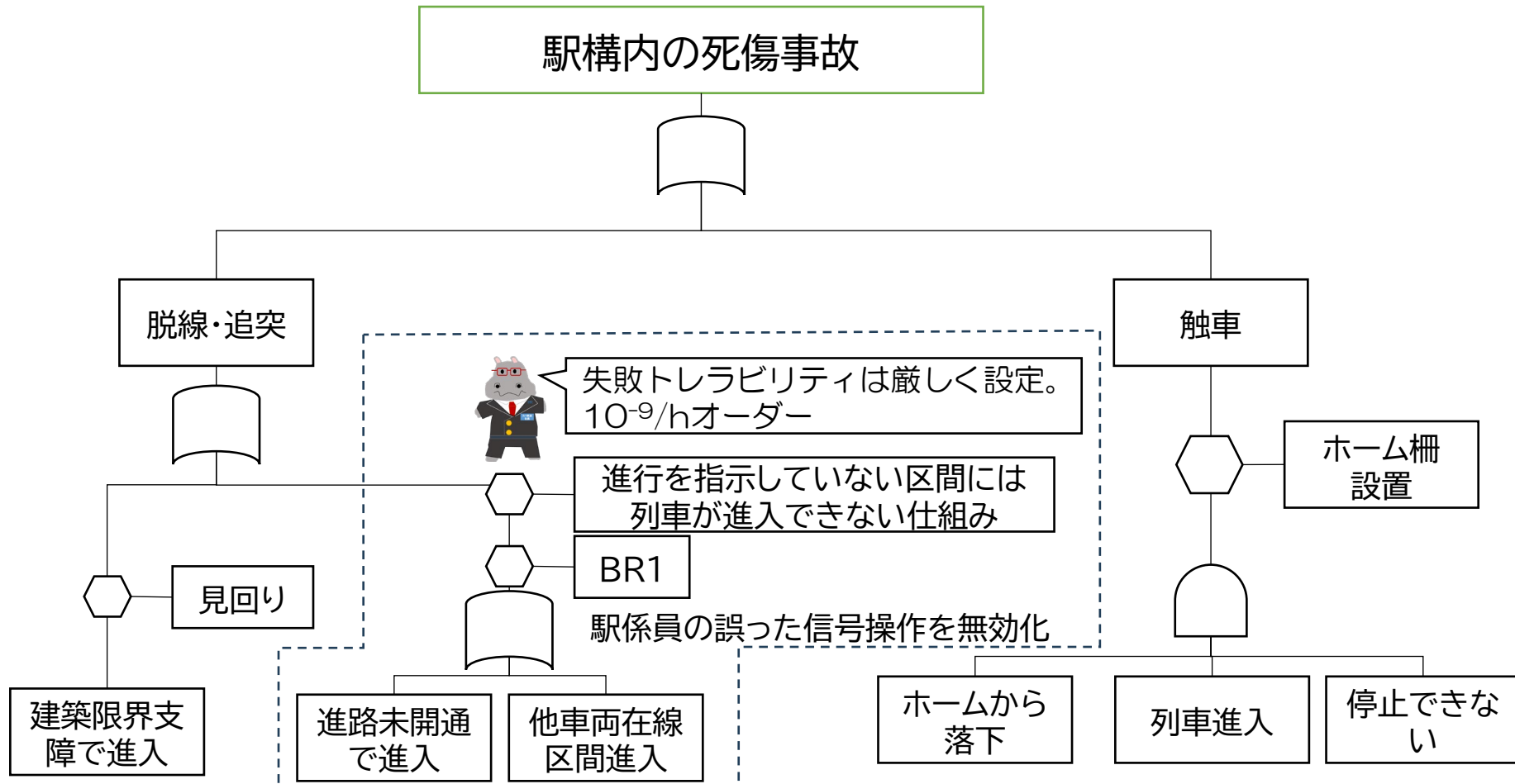
3. またまた安全に逆戻りすみません

おそらくカバ鉄道が考えているのは社長レベルではざっくりこういうヤツや。



3. またまた安全に逆戻りすみません

で、カバ鉄道は対策を考えるわけや。おそらく頭の中はこうや。



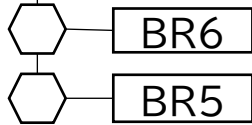
3.でも安全だけでもない

で、カバ鉄道は企業や。こういう解析もしているはずや。

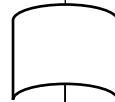


利潤の確保

投資活動キャッシュ
フロー最適化



機会損失の最小化



土地アセットの有
効活用

年間300万
円増収見込み

BR3



閉そく割の最適化

BR2

列車間隔最
適化

列車に対して進路を開
通させる作業の効率化

編成最適化

速度向上

BR7

構内改良

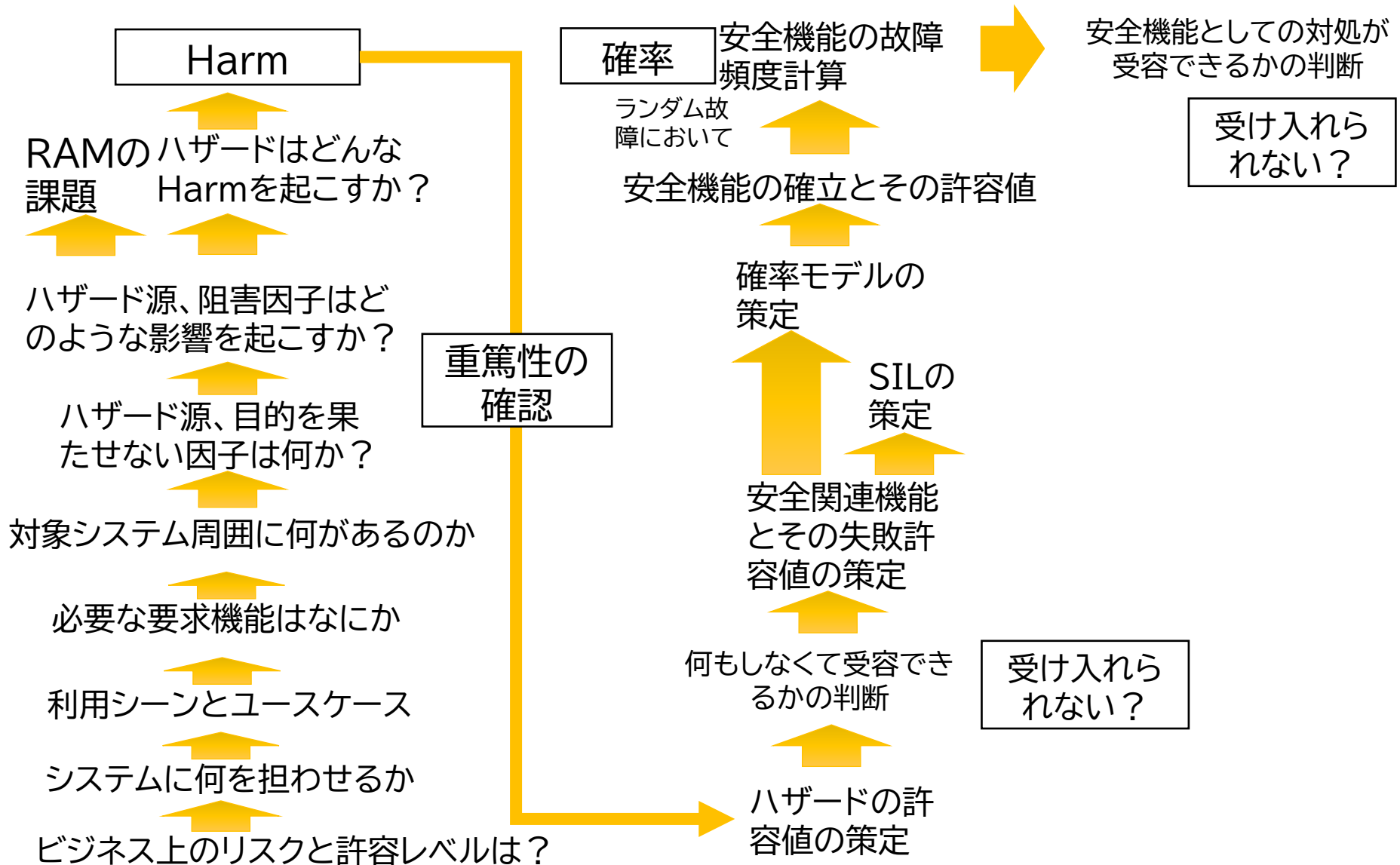
連動装置アプリケーショ
ンデータ作成の共通化

BR4

故障があったとき、
原因特定の迅速化

保守効率化

4. 安全を中心にした流れ



5. 今日の議題：忘れてませんか機能の割り当て

お客様の思いを受け止めた機能を定義するのは分かった。これでモノができるんちゃうか。



まあこれなら、お客さんからすれば「ゆうてることやってくれるやんか」って言われそうですね。あーよかった。後は技術屋の仕事だから頑張るね！

おいおいアカンやないか。会社において担当分けが大事なように、システム要求をどうやって実現するか考えていく必要があるんちゃうんか。。



安くするには、全部の機能を一つのハードに入れればいいんじゃない。技術屋はなんか知らないけど分けたがるんだよね。なんで連動機能とログ装置を分けるのかさっぱりわからないよ。

カバおエエこというやないか。ハードを少なくしたら安くなってフタ工業にも勝てるんちゃうか。おいハッキングカバ、そうしてみろ。



断る！絶対お断りや。かえって高くなる。多分課長も同意見やと思うけどな。



出来なくはないですが、ライフサイクルコストを考えた時、あまりいい選択には思えないですけどね。検討はしますが。



なんでそうなんねん。オマエらちゃんと理由言うてないやん。。



5. こういうのはどうでしょう

SIL4の機能にSIL2機能を前提とした基盤はどう？

連動における不正解錠のトレラビリティは $10^{-9}/h$ とする。

動作ログは10年分保持できるようにする。



機能の重要性を考慮して準備されたカバ興業謹製連動データ	普通の管理で作ったログ設定データ
カバ興業ご自慢のSIL4の管理手法で作られたアプリケーションソフトウェア	SIL2の管理手法で作られたログソフトウェアと設定データ
SIL2の管理手法で作成された処理装置付属の基本ソフトウェア	
処理を誤り、検知もできない頻度が $2 \times 10^{-7}/h$ である処理装置	

土台がしっかりしてへんのに、
そんなもんアカンに決まってるやんけ！
フタ工業から処理装置買って来たんか！
基礎が大事や！基礎が！



5. これはどうでしょう

SIL4、SIL2の機能にSIL4機能を前提とした基盤のみ使用するのはどう？

連動における不正解錠のトレ 動作ログは10年分保
ラビリティは $10^{-9}/h$ とする。 持できるようにする。



とにかく試験を尽くして頑張ったカ
バ興業謹製アプリデータ

カバ興業ご自慢のSIL4の管理手法
で作られ試験されたガチガチ
アプリケーションソフトウェア

SIL4の管理手法で作成された処理
装置付属の基本ソフトウェア

処理を誤り、検知もできない頻度が
 $2 \times 10^{-10}/h$ である
Fail-safety処理装置

しっかりしとるやないか。これは自信もっ
ていい！



カバ鉄道さんにログ機能の見てくれ悪いって言われたよ。分かりにくいって。で、IPネットワークにつなぎたいってさ。

ムリに一つにさせたのは社長とオマエやで。IPプロトコルスタックなんかSIL4の手法で作ってるもんなぞ知らんからイチから作るんか？それにGUIをSIL4の手法で作るんか？カネかかるで。



そんなのいいから早くしてよ。これじゃあ売れないよ。

まず謝ってくれ。話はそれからや。ハードソフトもメモリハリが大事や。。



5. 大は小を、兼ねる？！

当該機能AのSILよりも、高いSIL割り当てがされているの機能Bの管理手法、ハードウェアを活用したほうがよい例

- Bの機能を実現するために使用しているソフトウェアモジュールをAの機能実現に再利用。但しAの機能をBで使用しないように分離*
- Bの機能のログを送信するなど、Bの機能を実現するためのハードウェアやソフトウェアをフックしているが、Aの機能のSILはBより高くない場合。
- Bの機能と密接に関係する機能Aを実装する場合

混ぜない方がいいんじゃない と思う例

- 安全に関わらないが、既存のOSの機能を活用したほうがコストも工数も低く、ハードウェア追加費用を十分に賄える場合。
- 関係する機能ではあるが、しばしば調整が必要な安全に関わらない機能と安全に関わる機能
- 決定論的に決まる安全機能と、確率論的に決定される機能やAIで判断する機能

*Where the software consists of components of different software safety integrity levels then all of the software components shall be treated as belonging to the highest of these levels unless there is evidence of independence between the higher software safety integrity level components and the lower software safety integrity level components. This evidence shall be recorded in the Software Architecture Specification. (IEC 62279 7.3.4.9)

5. これはどうでしょう

うまく分ける！

連動における不正解錠のトレ
ラビリティは $10^{-9}/h$ とする。



安全に関係するカバ興業謹製アプリ
データは、SIL4の管理手法

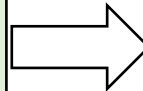
カバ興業ご自慢のSIL4の管理手法
で作られ試験された
アプリケーションソフトウェア

SIL4の管理手法で作成された処理
装置付属の基本ソフトウェア

処理を誤り、検知もできない頻度が
 $2 \times 10^{-10}/h$ である
Fail-safety処理装置

ログ
出力
機能

データ
を送信



動作ログは10年分保
持できるようにする。



GUI、設定ファイルなどは、お客様に
合わせてカバ興業が開発

Syslogサーバーなど汎用の動作ロ
グソフトウェアを活用

LINUXなど汎用OSを活用

普通のPCを活用

5. 基本的な割り当て考え方

機能要求、非機能要求、スケーラビリティから、サブシステムの構成を考える

機能要求、非機能要求(安全要求、安全要求のレベルを含む)をサブシステムに割り当てる

システム全体、他サブシステム、外部からくるハザード解析、信頼性解析を行い、割り当てられた機能要求、非機能要求の阻害要因の対策を検討する

具体的なハードウェア、ソフトウェア設計

SRACs

割り当てられた機能のTFFRとの整合性確保



6. まとめ

- 今回は機能の階層的な構造と、その役割分担についてお話ししました。
- 要求工学は、一つの学問として確立しています。私は、Microsoft Press のSoftware Requirement 3rd Editionを参考にしましたが、おそらく良い本はたくさんあると思われます。
- 要求を実現するためには、いろいろ考えなければいけないことがあると思いますが、適切なサブシステムへの機能割り当てを常に考えていただければ幸いです。

