仕様を決める
～仕様も確認も大事～
（RAMS 第四段階）

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

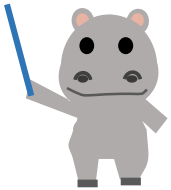
登場人物

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」

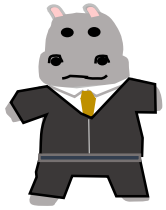
カバ鉄道　電気課長
口癖：安くてエエもん持って来い！

カバ興業　技術　オタかば
「面白くなければ技術じゃない」

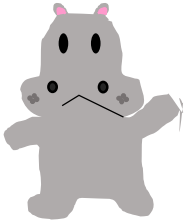


謎のフリーコンサル
なぞカバ
「知識は力！管理は必然」

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！」



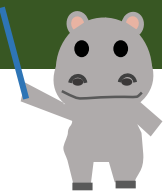
カバ興業の協力会社社員

「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」

この段階で要求されていること

4-1 システムの要求を決める。
4-2 システムの受け入れ基準を決める。

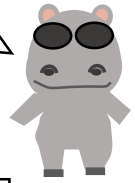


4-1システム要求とは

IEC 62278 6.4.3.1
EN 50126-1 7.5.2

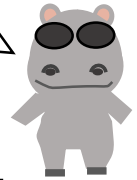
リスク解析も終わったし、次何するんや。

じゃあ聞くけど社長、何のためにリスク解析したんや。



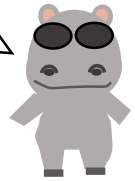
それは。。。。リスクを知って経営に生かすためや！

そんなもん、説明になってへんで。ヤバいとこ分かったら、なにをせなアカンかシステムの要求に生かすんちゃうんか？



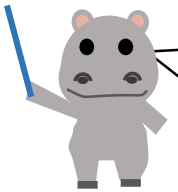
ようわかっとるやないか。それが言いたかったんや！

（ぜったいうそや。嘘をついている眼や。）



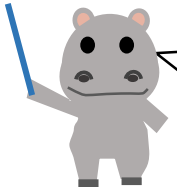
4-1RAMS要求とシステム要求とは

IEC 62278 6.4.3.1
EN 50126-1 7.5.2



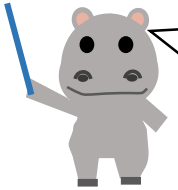
カバ興業の連動装置KABA-X Interlockingのシステム要求って何でしょうか？

そりゃあ、駅長の操作に従い、転てつ機を転換させ、信号を現示して、間違った入力の場合、その命令を無効にするってことや。



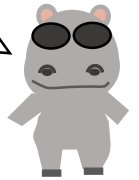
他にありませんかね。それでものは作れますかね。

自分で考え行動する。それがカバ興業や！全部聞いてから仕事するようなヤツはいらん！



自由でいいですね。でもそれで設計は出来るでしょうか。

俺が思うエエもん作るで！社長が自律ってゆうたからには、予算に責任はないオレも、好きなだけお金使って設計するで。



4-1RAMS要求とシステム要求とは

IEC 62278 6.4.3.1
EN 50126-1 7.5.2

周囲環境

周囲環境,
運用条件などの値
Mission Profile

インター
フェース

システムを組む
前からの制約

システム要求
（RAMS REQUIREMENTS)

他で何とか
する事項

要求機能

要求性能

安全
要求機能

安全要求
目標

配送
条件

システムサポート
要求

システムを組む
時の制約

4-1 鉄道事業者の役割

IEC 62278 6.4.3.1
EN 50126-1 7.5.2

システムに求める事項

カバ鉄道さんにはこれだけは決めて頂きたい。

周囲環境

周囲環境,
運用条件などの値
Mission Profile

インター
フェース

システムを組む
前からの制約

システム要求
(RAMS REQUIREMENTS)

他で何とか
する事項

要求機能

要求性能

安全
要求機能

安全要求
目標

配送
条件

システムサポート
要求

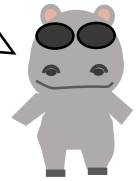
システムを組む
時の制約

カバ鉄道さんと話し合って決めたい。

4-1詳細で網羅的な定義

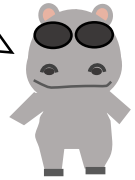
IEC 62278 6.4.3.1
EN 50126-1 7.5.2

俺はエエもん作るで！お客さんが泣いて喜んでくれるもん作るんや。



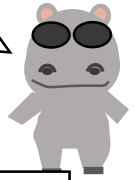
なんか試験をすると、聞いていない機能いっぱいありそうなんだけど。

どうせ客はわがままや。言いそうなモン全部込みでプログラムしといたで！言われんでもやる！それがハッキングカバなんよ！



でも、聞いていない機能の試験はやりようがないよ。試験なしで出荷はできないよ。

オレのソフトにバグはない！試験などイラン！



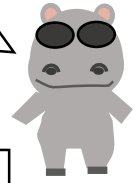
。。。。。

4-1規格ではどうなっているの

IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2

でもねえ、RAMS規格には具体的に、仕様をどう詳細に網羅的に書くかは書いていないんだよね。。。

書いてないことでもやる！それがハッキングカバなんよ！



お前はできても他のモンが困るやろ。。あかんでそんなん。

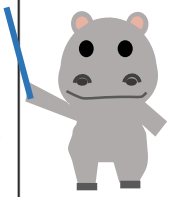
Software Requirement Specification (Table A.2)/ IEC 62279

TECHNIQUE/MEASURE	Ref	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
1. Formal Methods (based on a mathematical approach)	D.28	–	R	R	HR	HR
2. Modelling	Table A.17	R	R	R	HR	HR
3. Structured methodology	D.52	R	R	R	HR	HR
4. Decision Tables	D.13	R	R	R	HR	HR

Requirements:

a) The Software Requirements Specification shall include a description of the problem in natural language and any necessary formal or semiformal notation.

b) The table reflects additional requirements for defining the specification clearly and precisely. One or more of these techniques shall be selected to satisfy the Software Safety Integrity Level being used.



4-1要求機能モデリング例

IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2

カバお、カバ鉄道さんの仕事、利益確保するために何をやっているんや。

ちゃ、ちゃんと営業していますよ。カバ鉄道さんにも毎日訪問してお話ししていますし。。

だから、利益確保するためどうするってゆうてるねん。努力は大事やけど成果は利益やろ。。。利益確保するための要求機能はなんや！

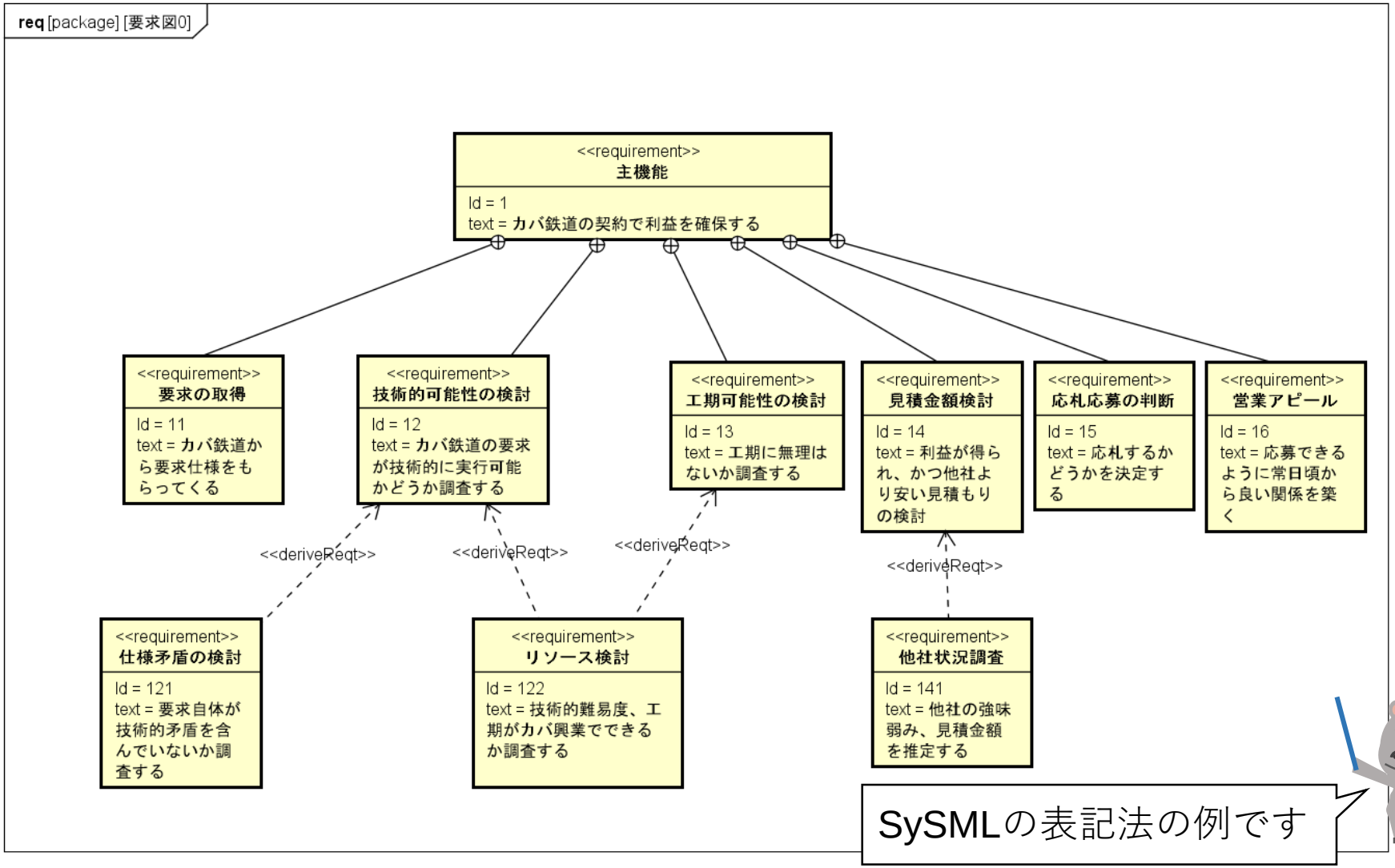
。。。頑張ってます。。。

結局分かってないってことやな！それが問題や！

では利益確保するための要求機能をモデル化してみましょう。

4-1要求機能モデリング例

IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2



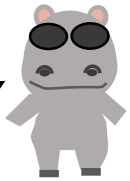
SySMLの表記法の例です

4-1モデリングのメリット

IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2

確かにもれなくかけそうだが、いまいちメリットが分からん。

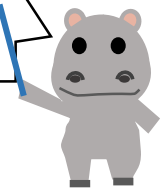
自然文で書くより曖昧さはなく、網羅的ではあるな。
社長知ってるか？こういうモデリングツールは、ある程度表形式や自然文に変換してくれるねんで。



それやったら二度手間やないな。

名前	型	サマリー
Human resource	要求	Technical difficulties, schedules are fitted to Hippo Corp.
Research rivals activities	要求	research rivals' good and bad point, estimate cost of rivals
conformation between the system requirements and techinology	要求	check the coodination between the requirements and technology issues

こういう出力も出ますね。さらにいろいろなUML図を追加していくと、ソースコードの骨格も自動生成されますね。



4-1Formal method

IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2

カバ興業では、お客様を歓迎するため、ご訪問者様の会社名を会社の玄関に掲示する。

こういうことにしたからな！
これが仕様やで。

今日はカバ鉄道さんが打ち合わせにお越しになるからな。

わかりました！

今電話があって、先にブタ鉄道さんが来られるそうだ。

分かりました！

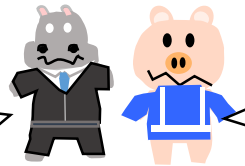
歓迎
ブタ鉄道ご一行様

あれ、今日はカバ鉄道なのに、ブタ鉄道の看板が出ているよ。変えておこう。

歓迎
カバ鉄道ご一行様

歓迎
カバ鉄道ご一行様

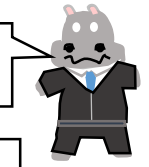
いえ、当社は御社第一に考えて。嘘じゃないです。



今日はうちのライバル、カバさんトコも来られるんですなあ。御社は商売繁盛ですなあ。

4-1Formal method

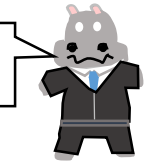
IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2



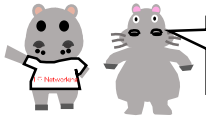
こらっ！おまえら！心臓が止まりそうになったやないか！

ちゃんと仕様通りやりましたよ。

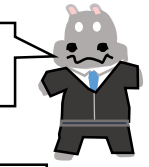
カバ興業では、お客様を歓迎するため、ご訪問者様の会社名を会社の玄関に掲示する。



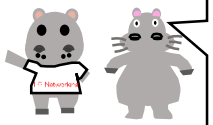
んなもん、順番間違えたらアカンやろ。



それは申し訳ないですけど、仕様には書いていないですよね。。



アホかいちいち書けるかそんなもん。常識で考えなアカンやろ。



まあそうですけど、プログラムは言われたとおりしか動きませんから、仕様がいい加減なカバ興業なんてことになったら倒産ですよ。

4-1Formal method

IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2

Formal method：
曖昧でない言語で仕様を厳密に定義し、テストケースを定め試験を行うことにより正確な仕様定義が出来る。また、ソフトウェアのコードの一部自動生成も出来、生産性が向上するかもしれない。

```
active proctype otakaba()
        {
        printf ("Pig Railway¥n")
        }
active proctype kabao()
        {
        printf ("Hippo Railway¥n")
        }
```

オタカバはブタ鉄道を、カバおはカバ鉄道の看板をあげるというPromela定義の例。

これを形式チェックツールSPINで解析すると、全ての場合がリストアップされる。（この例では、まずオタカバがブタ鉄道を選択し、次にカバおがカバ鉄道を選択する場合と、その逆の場合。動作が一意に決まらないことが分かる。）

4-2 要求を受け入れるには？

4-1 システムの要求を決める。
4-2 システムの受け入れ基準を決める。

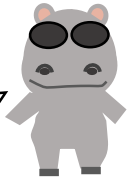
4-2 要求を受け入れるには？

IEC 62278 6.4.3.2
EN 50126-1 7.5.4

要求の受け入れ？！そんなもんオレがOKやったらOKやないか。オレがルールブックや！

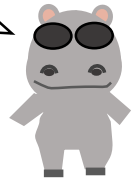
その強気さを  (カバ鉄道電気課長)さんの前で一回ゆうてみ。

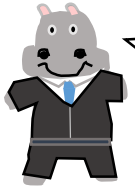
二度と買ってもらえないと思うで。



カバ鉄道様のおっしゃることが、絶対や。間違いないで。

（ぜったいうそや。嘘をついている眼や。）





カバお、カバ鉄道の課長さんのところに、野球のチケット持って行っとけよ！黄色のやつやぞ。オレンジ持って行ったらアカンで。

あの人ね、ト〇キチだけど、そういうの絶対受け取らないよ。
持って行くとメチャクチャ叱られるんですけど。。。システムも受け取ってくれなくなるよ。。。

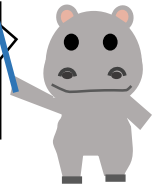
4-2 要求を受け入れるには？

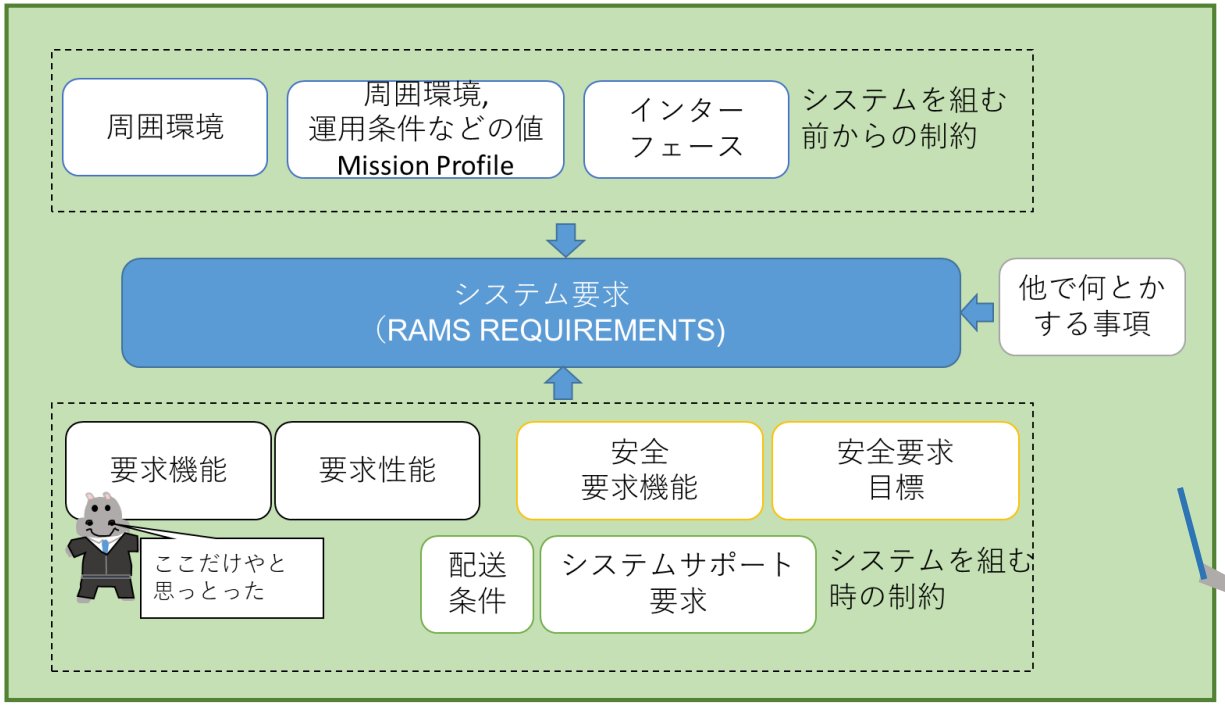
IEC 62278 6.4.3.2
EN 50126-1 7.5.4

具体的に規格では、受け入れってどうなっているんかな？

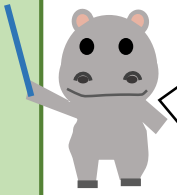
Overall requirement → RAMS requirements

整合性があるかどうかのチェック





ここだけやと思っとった



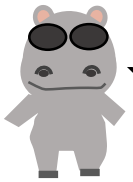
こういうことがちゃんと考慮されているかどうかですよね。

4-2 要求を受け入れるには？

IEC 62278 6.4.3.2
EN 50126-1 7.5.4

受け入れ条件を決める

受け入れの手順の方針、手順を決めるRAMS validation planを構築する
- 前提とするシステムの記述
- 要求仕様を含めたRAMS validation(≒試験)方針
- validationを進めるための試験と解析方法
- validationを進めるための管理手法
- 進める順番とスケジュール
- 不適合だった場合のプロセス

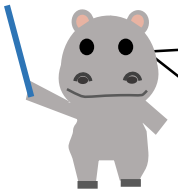


オレのコードに間違いはない。カバおの営業は間違いだらけ。

ひどいよ。。。

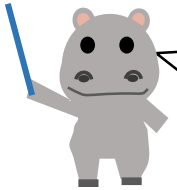
4-2 試験はどうするの？

IEC 62278 6.4.3.2
EN 50126-1 7.5.4



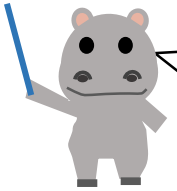
Validationには試験が非常に大事ですけど、カバ興業連動装置-"KABA-X Interlocking"の試験はどうしているのですか。

そんなもん、網羅性がだいじやな。全ての進路の鎖錠条件を総当たりに全部試験をしてるで。



素晴らしいですね。ブラックボックステストですね。で、一部改修があったときはどうするのですか？

改修していないところもしたところも、全ての進路の鎖錠条件を総当たりでまた試験するで。それが品質のカバ興業や！



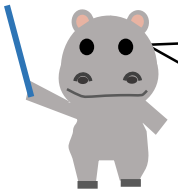
素晴らしいですね。しかしお金がかかりませんか？かなり時間がかかると思いますが。

時間より安全やで。なあカバお！

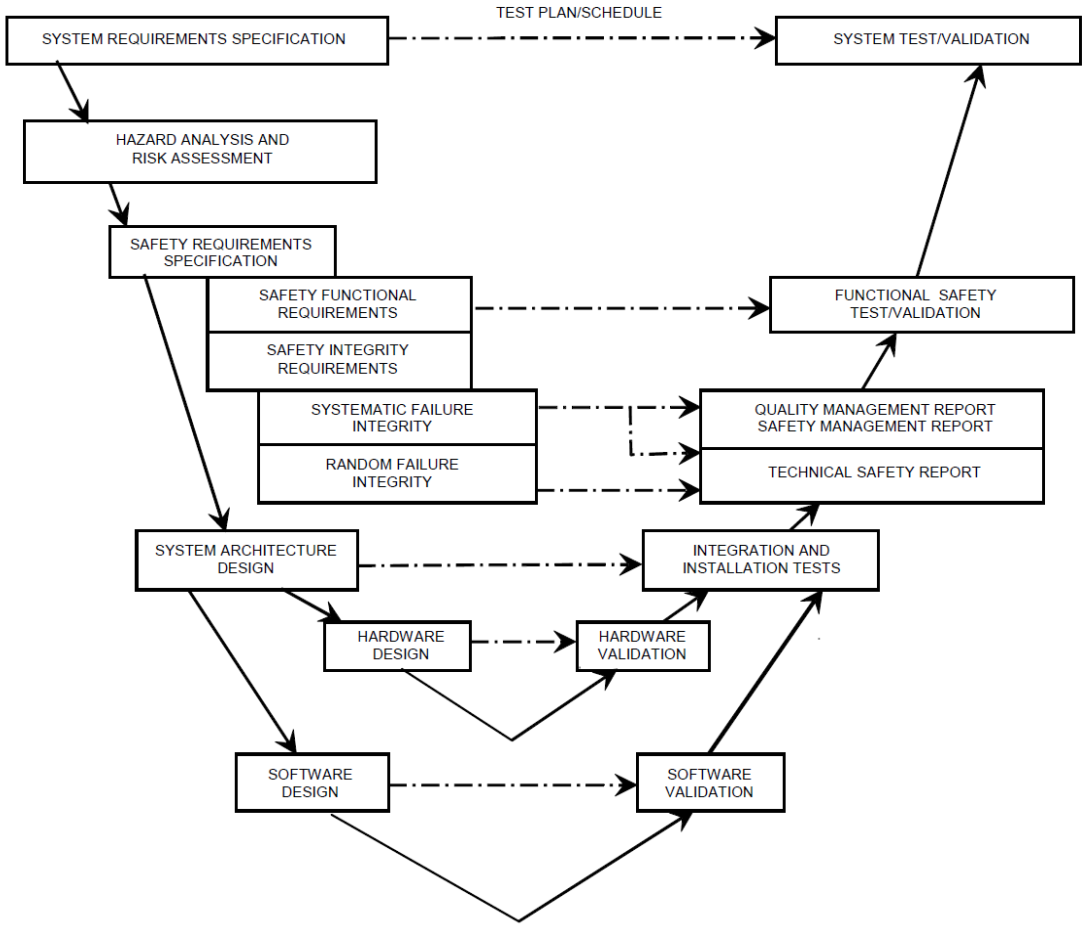
でもカバ興業の改修は高いってカバ鉄道からいわれてるんだよね。。

4-2階層的試験

IEC 62278 6.4.3.2
IEC 62425 5.3.2
IEC 62279 5.3.2.1
EN 50126-1 7.5.4

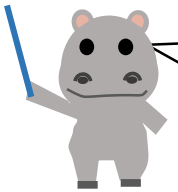


階層的な試験で試験内容を決めるのはどうでしょうか。

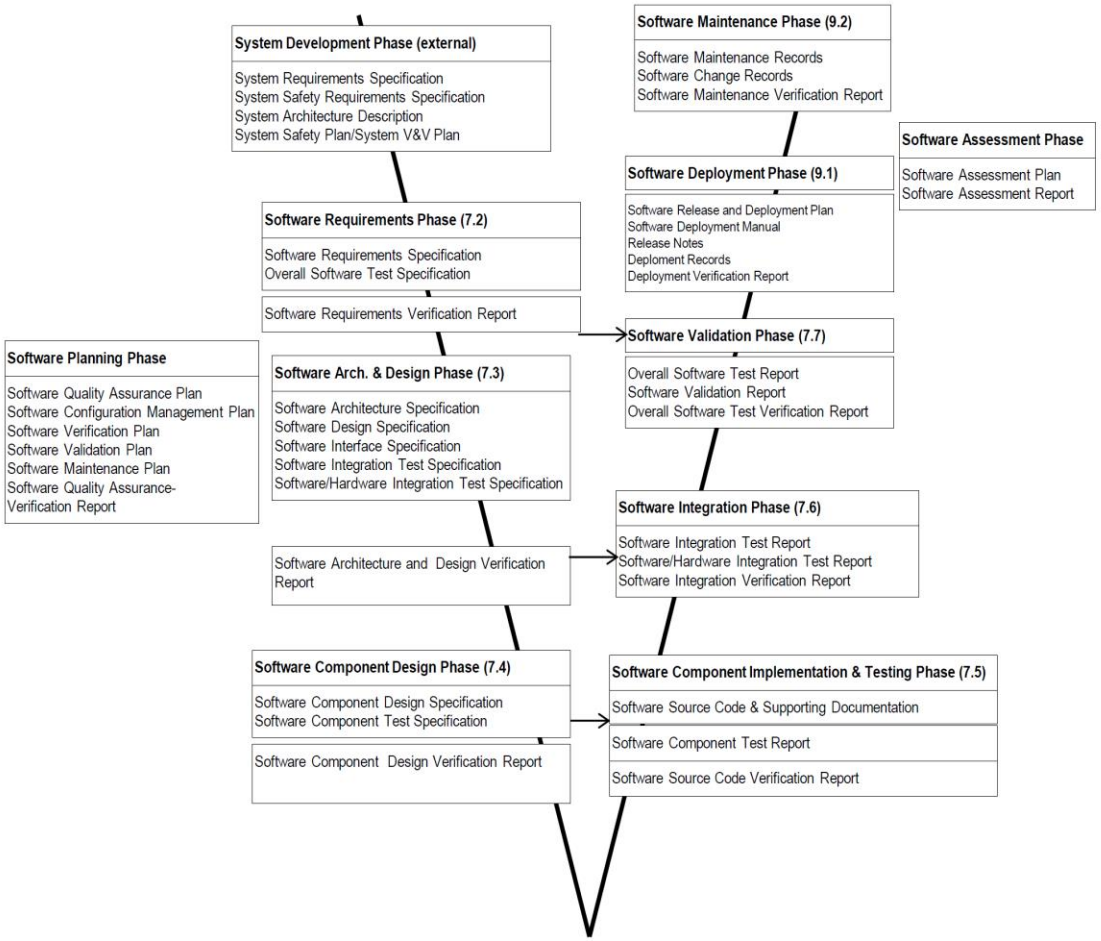


4-2階層的試験

IEC 62278 6.4.3.2
IEC 62425 5.3.2
IEC 62279 5.3.2.1
EN 50126-1 7.5.4



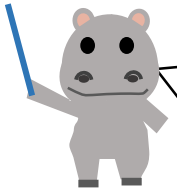
ソフトウェアの部分に限定するとこうです。



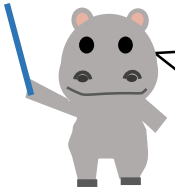
4-2 全体の試験だけすればいい？？

IEC 62278 6.4.3.2
EN 50126-1 7.5.4

そんなもん、連動装置としてちゃんと動けばいいから、A駅の連動機能全体の試験を完全にやったらええんちゃうんか？



でも社長、A駅は、ソフトウェアモジュールの一部の機能しか使っていないかもしれないですよね。A駅で使っていない機能の試験は漏れますよね。



ハードウェアだって、A駅よりも大きな駅の場合は、ボードを追加するかもしれないですよね。そういう試験は？

おい、オタカバ！ちゃんと試験してるやろうな！いろいろなこと考えて！

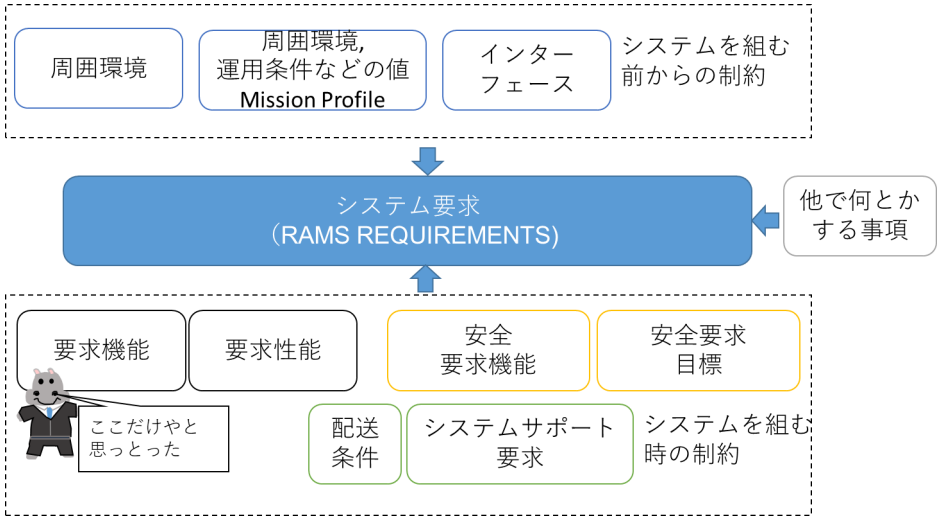
……..そんなこというと思ったからやってましたよ。。。

だから階層的な試験がいるのです。

まとめ

- システム要求は機能要求だけではありません。
- 要求を決めるには、網羅的な手法が好ましいです。モデル化などを行うとどうでしょうか。Formal methodも将来的には必要かもしれません。

- システムの受け入れは、最終試験だけではありません。各段階での確認で、最終的に受け入れ試験を行います。



Next

2021/10/21にお会いしましょう。

SEE you on Oct. 21,2021.