陸上交通のシステム開発における ライフサイクルとセキュリティ

鉄道認証室　森　崇、吉永　純

はじめに

- セキュリティが注目されています。しかし規格を見ても、いったい何から始めたらいいか困るのではないでしょうか。

- ライフサイクル管理、解析方法、いろいろあります。また、鉄道技術者からすると自動車の動向は大いに気になるところです。

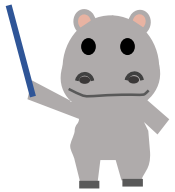
- このため、規格の構成、ライフサイクルにおけるセキュリティ対応の考え方、鉄道と自動車のライフサイクル管理について特徴的な点をご説明したいと思います。
- 時間が限られていますので、マネジメントについてはあまりお話しする時間がありません。網羅的にお話しすべきですが、今回は解析を中心に特徴的な点を重点的にお話しします。

登場人物

鉄道信号保安装置を主業としている「株式会社カバ興業」とその関係のメンバーをご紹介します。どうもカバ興業は、セキュリティ分野についても頑張っていこうとしているようです。しかしなかなか一筋縄ではいかないようです。このカバ興業のドタバタを通して考えていきたいと思います。

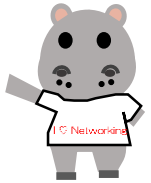
カバ興業　社長
座右の銘：技術と直感

カバ鉄道　電気課長
口癖：安くてエエもん持って来い！

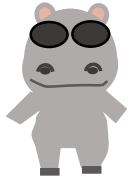


謎のフリーコンサル　なぞカバ
「理屈っぽいのは仕事だからしょうがない。」

カバ興業　営業　カバお
「営業は怒られてナンボ」



カバ興業　技術　オタかば
「面白くなければ技術じゃない」



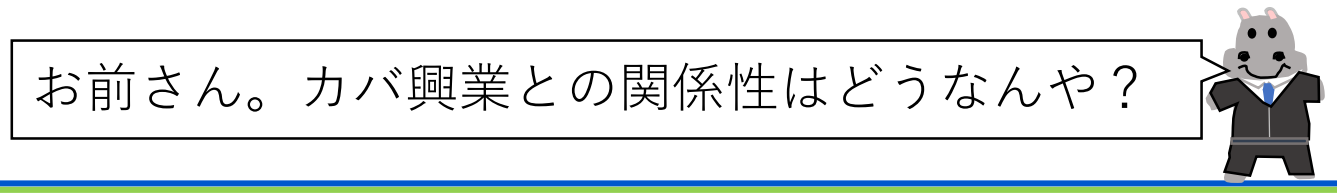
カバ興業　プログラマ
ハッキングカバ
「俺しかできないことをやる」

カバ興業設計課長　カバ実
「みんなで、できるようになりましょう」

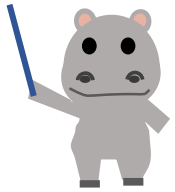
自己紹介

1992年　西日本旅客鉄道株式会社 岡山信号通信区配属
1994年　同社 大阪信号工事所、京都信号工事所で福知山線信号工事担当
1997年　同社技術開発推進部(現イノベーション本部)配属
　2021年までの24年間、IPモビリティ、IPセキュリティ、IPv6の活用、ソフトウェア定義列車無線、無線式列車制御などを担当する。

2019年　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　客員専門調査員委嘱
2021年　同機構　交通安全環境研究所鉄道認証室　任期付主席研究員（現職）
　ソフトウェア、通信の認証を中心に行っている。

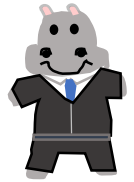


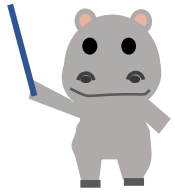
安全とは？セキュリティとは？



つかぬことをお伺いしますが、カバ興業さんの考える「安全」とはなんでしょうか？

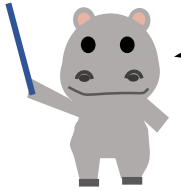
そりゃお前さん。「危険がなく安心なこと」やないか。辞書に書いてるで。





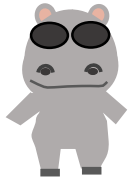
….　では、セキュリティと関係する、セキュアとは何でしょうか?

「安全が保障されていること。」らしいで。辞書によると。



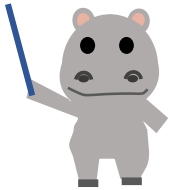
….　ということは安全とセキュアは同じということですか…なんか違うような。

安全：受け入れられないリスクがないこと[ISO/IEC Guide 51:1999, definition 3.1]
情報セキュリティ：偶発的または意図的な不正な情報の流出、転送、変更、破壊に対する情報の保護[IEC 60050 IEV 721-08-57]



安全とは？セキュリティとは？

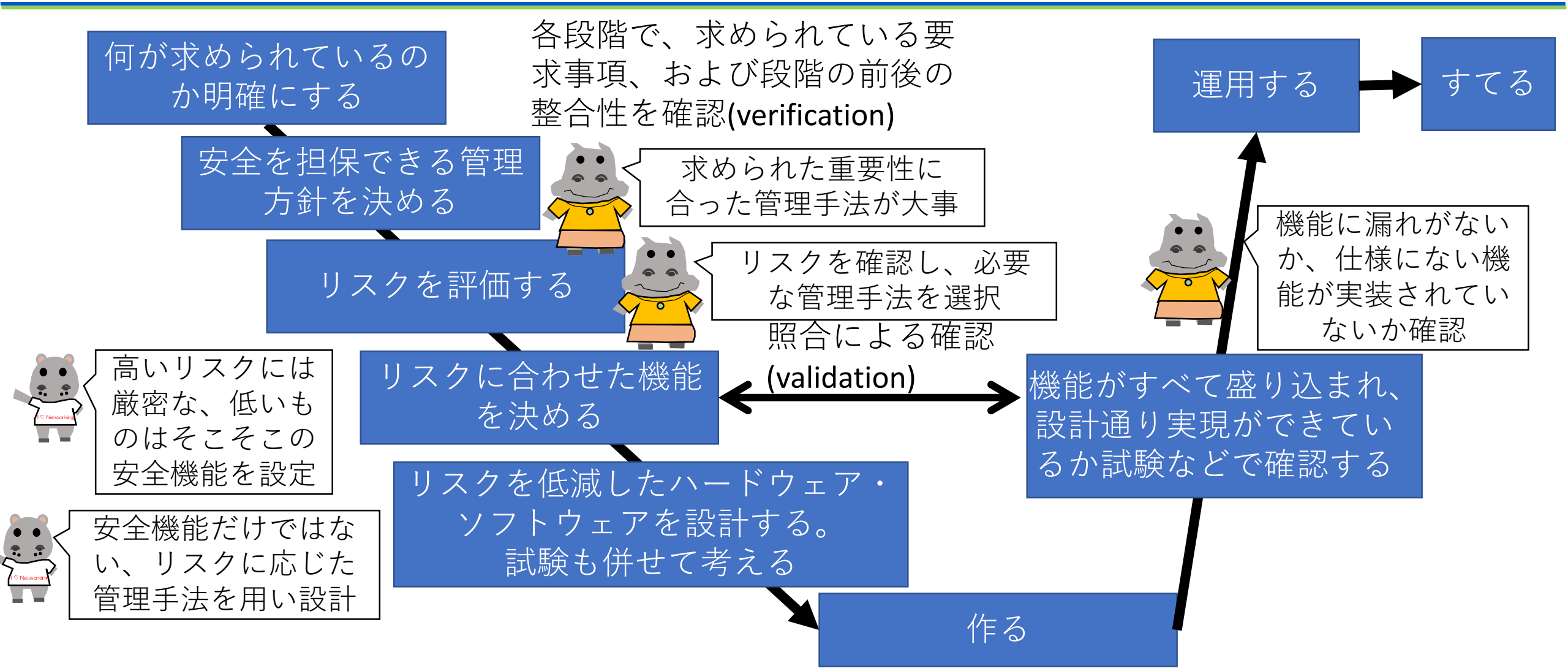
なんかよう分からんな。受け入れられないリスクに、情報セキュリティで対処できるモンもあるんちゃうんか。



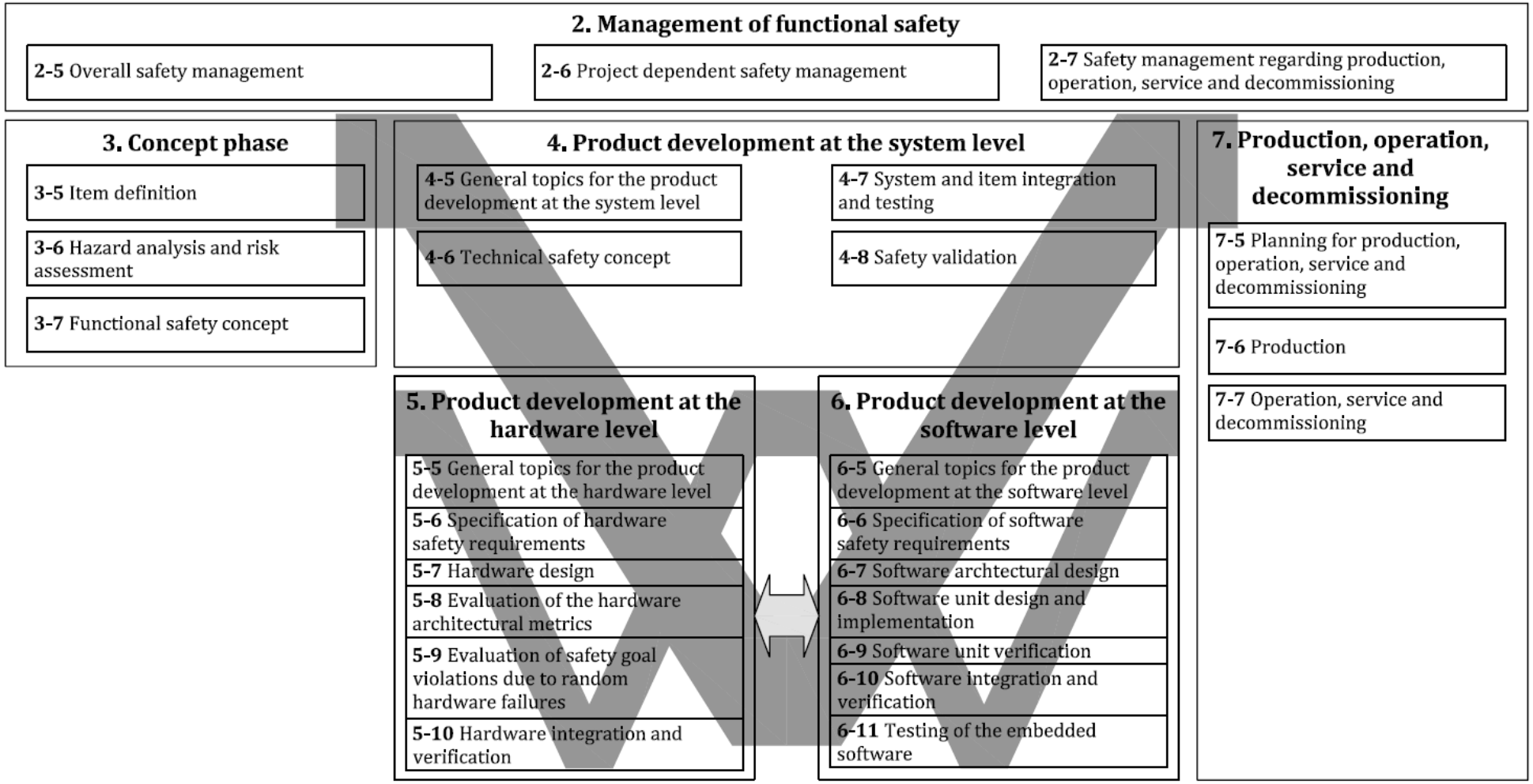
そうですね。一般的に機能安全では、受け入れられないリスクから、セキュリティ関係を除いて考えることが多いですね。しかしこれもケースバイケースなので、今回は除いて考えましょう。

システムが想定した動作とならない要因		
Random Fault	Systematic Fault	Security Vulnerability
安全に関する事項		セキュリティに関する事項
予想以上に部品が壊れた	お客さんの仕様と違う仕様書で作った	セキュリティホールを攻撃された

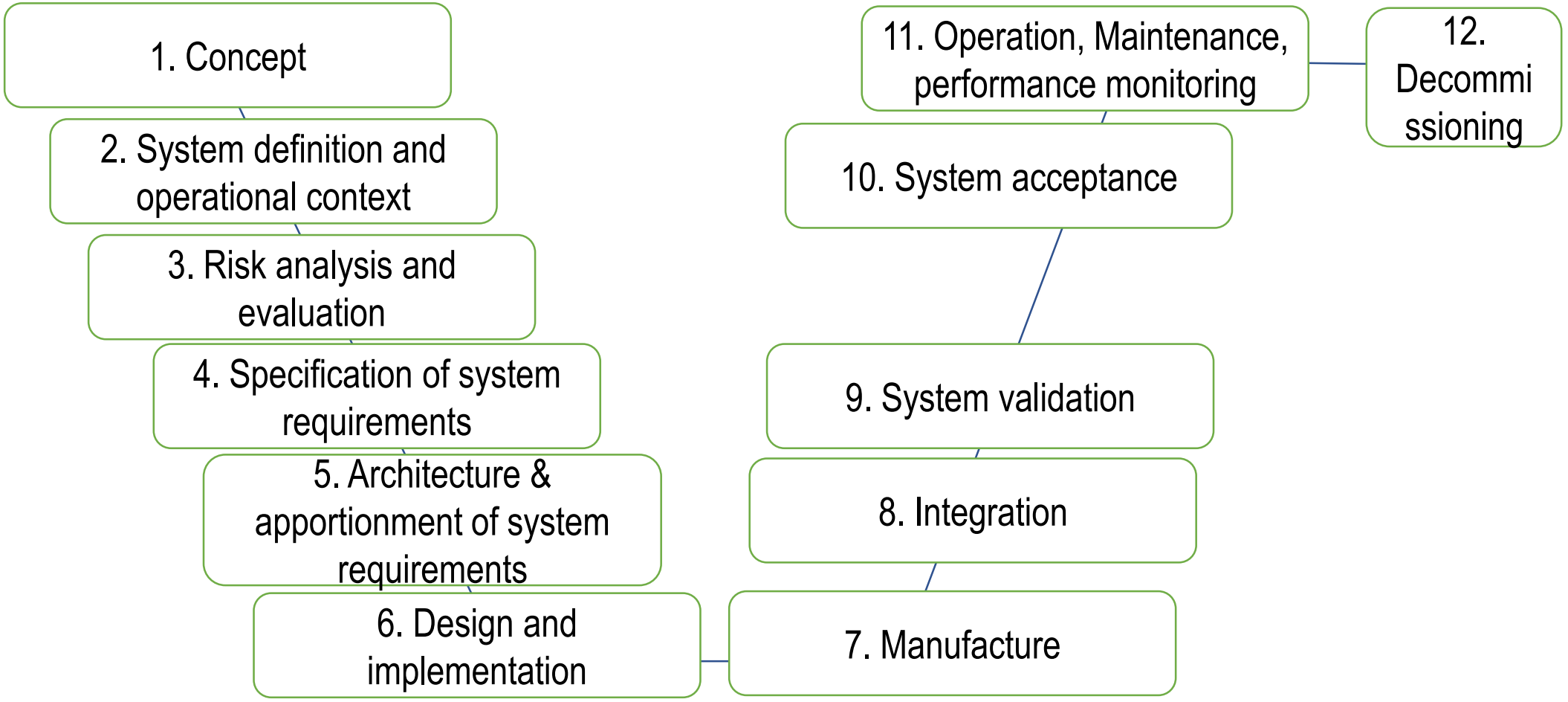
安全とライフサイクルの関係

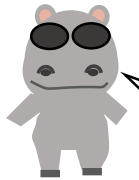


自動車における機能安全システム実現ライフサイクル



鉄道におけるRAMSライフサイクル*





RAMSは国際標準IEC 62278があるが、セキュリティ技術レポートはEN規格しかないので、この絵はEN名称に合わせてある。

*EN50126 Railway applications –Specification and demonstration of reliability, availability, maintainability and safety (RAMS)に規定されるライフサイクル
**Original Equipment Manufacturer 完成車メーカのこと

鉄道におけるRAMSライフサイクル*

ISO 26262の分冊名

2. Management of functional safety

1. Concept

2. System definition and operational context

3. Concept Phase

3. Risk analysis and evaluation

4. Product development at the system level

4. Specification of system requirements

5. Architecture & apportionment of system requirements

5. Product development at the hardware level
6. Product Development at the software level

6. Design and implementation

7. Manufacture

8. Integration

自動車にはなし

9. System validation

4. Product development at the system level

10. System acceptance

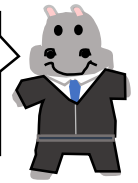
自動車にはなし

11. Operation, Maintenance, performance monitoring

12. Decommissioning

7. Production, Operation, service and decommission

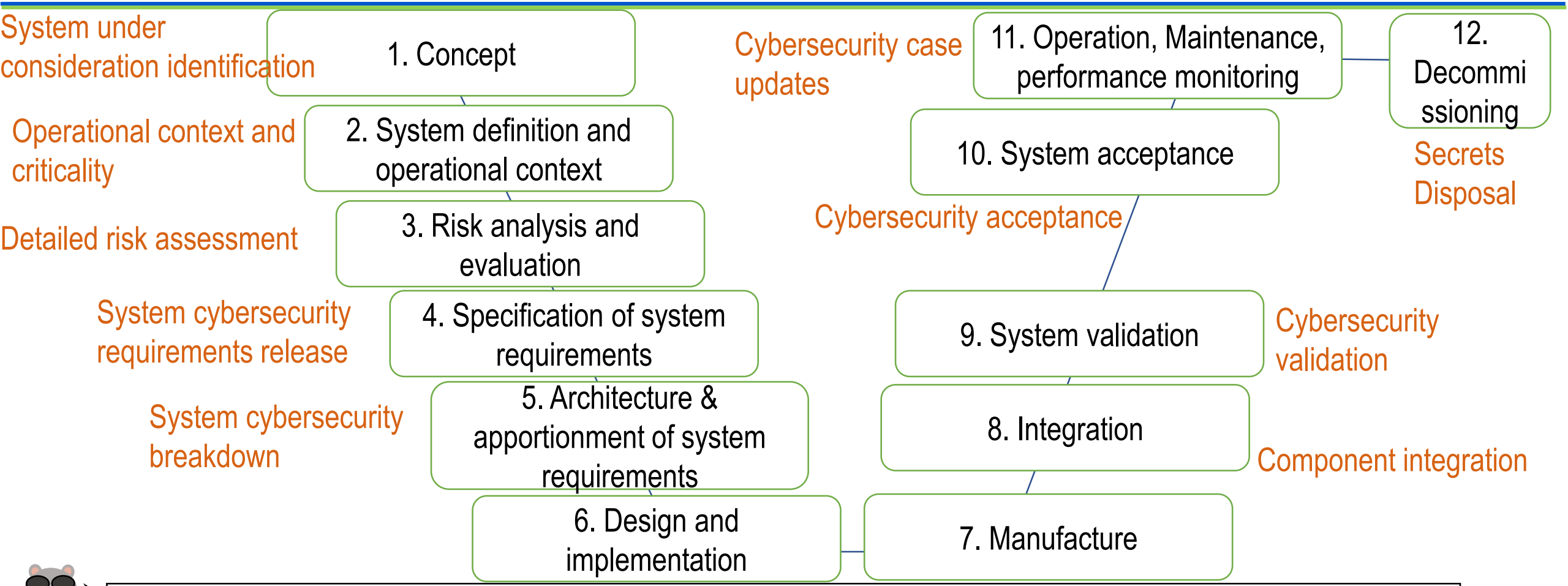
バカな夢を見るな。カバじゃなくてバカになるで。

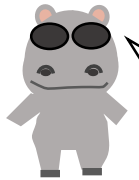


自動車と似てるな。ひょっとしたらカバ興業もOEM**いけるかもな。

*IEC 62278 Railway applications –Specification and demonstration of reliability, availability, maintainability and safety (RAMS)に規定されるライフサイクル
**Original Equipment Manufacturer 完成車メーカのこと

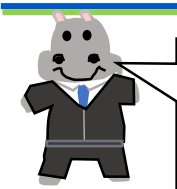
鉄道におけるRAMSライフサイクルとセキュリティ



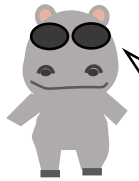


オレンジで、CLC/TS 50701の各段階の成果物を示している。似ているところもあれば違うところもあるな。

鉄道におけるRAMSライフサイクルとセキュリティ

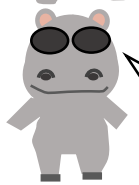


そんなんゆうてもセキュリティとセーフティ、カタカナで書いたらよう似てるやないか。おんなじ方法でやったらエエんちゃうんか。

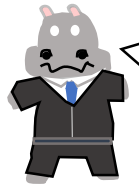


じゃあ大きく違う例をゆうてやるわ。もしな、オレが社長に強烈に恨みをもってカバ興業辞めたら、セーフティは低下するか？

おい、お前辞める気なんか？辞めさせへんぞ。○■하※△마×※흥★◎업◇!은!☆한〆가□※족＋＝×
別にお前辞めても、故障率が上がってセーフティは低下することはないけど、困るやろそれは。。



訳の分からん事はじめにゆうてるな。じゃあセキュリティは？　低下するか？



お、お前まさか、攻撃するんか。■§사¶○이×※버〆◎공△!격!℃금〆지□※다＋＝×
それはセキュリティ上の大きな問題になるかもしれん。要求はなんや。カネか？

鉄道におけるRAMSライフサイクルとセキュリティ 何が違うか？(Phase 1)

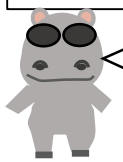
1. Concept

EN 50126 (IEC 62278) RAMS規格

In the context of RAMS performance, the following aspects should be analysed:
a) the scope, context and purpose of the system;
b) the environment of the system, including:
– physical issues;
– system interface issues;
– legislative and economic issues (if they can have impact).
c) previous RAMS requirements and past RAMS performance of similar and/or related systems;
d) current RAMS policy and targets of the relevant railway duty holders;
e) safety legislation.

CLC/TS 50701

— Review of the level of security achieved up to now
— Analysis of the project's security implication and context (incl. generic threats) (see 5.4)
— Alignment with railway operator / asset owner and stakeholder's security goals
— Consideration of security lifecycle aspects (patch management, monitoring, etc.) (see Clause10)
— Plan cybersecurity-related activities

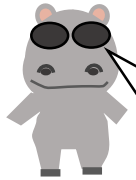


同じような要求は同じ色で書いてみたけど。。なんかセキュリティの方はライフサイクルの問題を早くから気にしてないか？？作りっぱなしではアカンということを暗示してそうや。

鉄道におけるRAMSライフサイクルとセキュリティ何が違うか？(Phase 1)

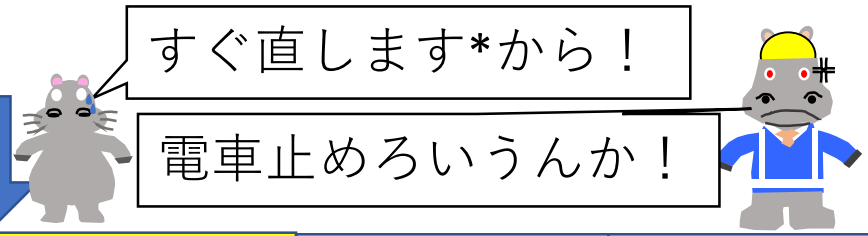
なんか知らんけど脆弱性とかパッチとか、挙句の果てにプランを考えろってか。気が早すぎるんちゃうか。Phase 1なんかなんにも決まってないんやで。

社長の言う通りだよ。お客さんに何も決まってない段階から、セキュリティプランどうしますかなんて聞けるわけないよ。「**お前んとこで考えろ。そんなもん何もないのに分かるわけないやろ。**」で一刀両断だよ。ハッキングカバも一度営業やってみればいいんだよ。



そやけどこの段階で決めとかんと、後で営業のカバおが謝りまくることになるんやで。
それでもエエんか？↓みたいなん容易に予想できるやろ。

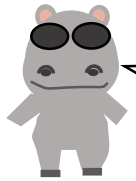
急になんかヤバい脆弱性見つかる



運用中	修正ソフト開発する	試験する	お客さんにOKもらう	運用中

*実際はIEC 62279(鉄道用ソフトウェア)に沿って対処するので、すぐに直るわけではなく、影響解析、仕様策定、試験仕様策定、アーキテクチャデザイン、コンポーネントデザイン、モジュールテスト、統合テストなど多くの段階を踏みます。

鉄道におけるRAMSライフサイクルとセキュリティ 何が違うか？(Phase 1)

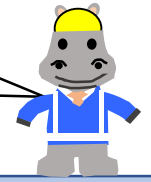


これやったらカバおも怒られんやろ。こんなんコンセプトがないと出てこうへんで。

スクランブルアルゴリズムAに急にヤバい脆弱性見つかる

大丈夫です。予備アルゴリズムがあります。

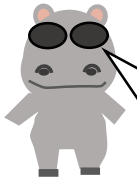
おお、準備がエエな！



1系	スクランブルアルゴリズムAで運用中	アルゴリズムBでスタンバイ	予備スクランブルアルゴリズムC
2系	予備スクランブルアルゴリズムB	アルゴリズムBで運用	
試験系	新アルゴリズム検討	修正ソフト開発する	試験する	お客さんにOKもらう

鉄道におけるRAMSライフサイクルとセキュリティ何が違うか？(Phase 1)

でもよお分からん。じゃあなんで安全に対しては、ヤバいときコンセプトいらんのや？



じゃあもう一度シナリオ見てみよか？基本的に安全の場合、経年で不安全になるのではなく、システムのアベイラビリティに問題が出てくる。このため、人に危害を与えるリスクは増えへんのや。

そろそろお取り替えを。

安全に問題あるんか？

いえ、故障したら安全には止まりますが。

ホンならおんなじモンで取り替えてくれ。

故障増えてくる

運用中

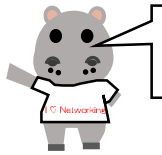
取り替えシステムで運用中

製作する

試験する

お客さんにOKもらう

安全解析vs セキュリティ解析の手順

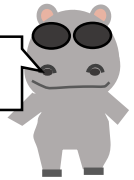


安全やセキュリティどんな手順で解析するんだろうか。

	Phase1	Phase2		Phase3	Phase4,5
安全の側面*	システム定義	ハザード***の同定	重要性解析	リスクの推定と受け入れ可能レベル設定	機能要求と機能の割り当て
セキュリティの側面**	対象システムを同定	初期リスクアセスメント	対象システムの分離	詳細なリスクアセスメント	サイバーセキュリティ要求と詳細化

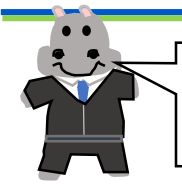
やること一緒みたいやな。

各々の特性に応じて解析する！



*IEC 62425 Figure A.3 – Example risk analysis process
**CLC/TS 60701 Figure 1 – Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk
***a condition that could lead to an accident (事故を導くかもしれない状態) IEC 62425 3.2.10

安全解析vs セキュリティ解析(危険要因の同定の差異)



こういったモンを解析するには、どんなヤバいことがあるかもれなく出すことが大事や。経営もリスクの想像と対処が大事や。直感経営者のワシは、直感で勝負や！

安全のハザード同定は、IEC 62425によると

Systematic identification of hazards generally involves two phases: (系統的なハザード同定は2つの段階)

– an empirical phase (exploiting past experience, e. g. checklists); (経験的なもの→社長のやり方ですね)

– a creative phase (proactive forecasting, e. g. brain-storming, structured what-if studies). (創造的なもの (×想像))

セキュリティの脅威の情勢の導出はCLC/TS 50701によると

The threat landscape should be based on recognized and accepted threat library or reports and built with a high-level approach providing an overview of the threats applicable to the railway sector

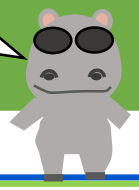
Threat libraries and reports like the following should be taken as inputs:. (脅威の情勢検討は鉄道に適用できる有名どころの参考書使う必要がある。以下のものが例。)

— ENISA Threat Landscape Yearly report

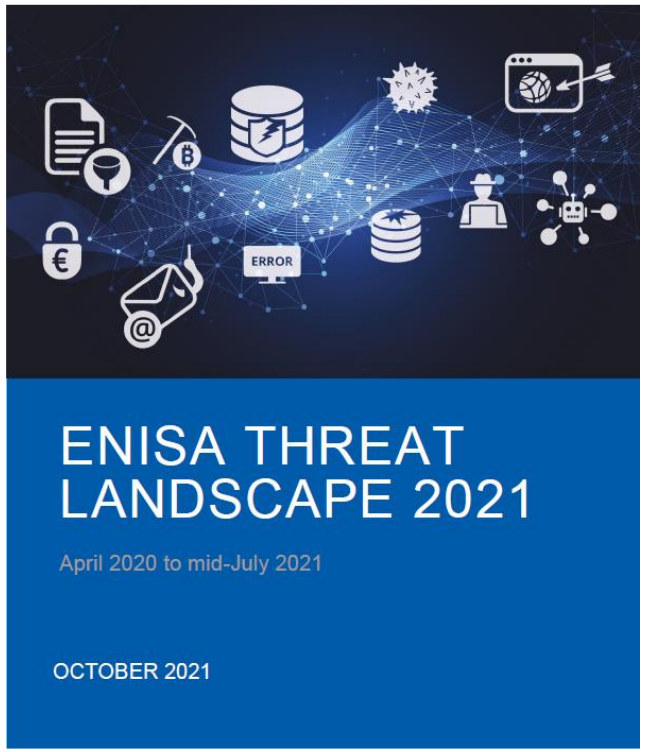
— ISO/IEC 27005

— NIST SP 800-30.

特にセキュリティは直感はアカンぞ！



安全解析vs セキュリティ解析(危険要因の同定：参考文献の例)

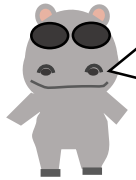


単に読んでみても非常の面白い本。
無料なのでぜひ読んでもらいたい。
巻末に典型的な攻撃リストがあり、参考になる。

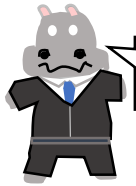
https://www.enisa.europa.eu/publications

安全解析vs セキュリティ解析(要素の差異)

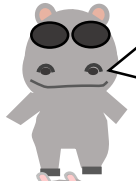
安全第一、安全第一、カバ興業は安全優先や。



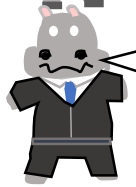
じゃあもしオレが、社長に不満をもって会社辞めてサイバー攻撃したら、カバ興業の信号装置が誤動作して列車が脱線するかもな。オレの給料不当に安いと思うで。安全の第一歩。それは賃上げや。



おい、お前俺を脅してるんか。脅迫やぞ脅迫。お巡りさーん、ここに悪いカバがいます。

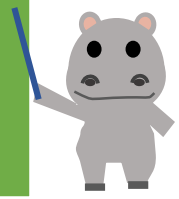


仮定や仮定。もしオレが給料安いからと言って、カバ興業のオンラインバンキング不正使用して、オレの口座に振り込んだらどうする。それもセキュリティ事故やろ。



お巡りさーん、ここに詐欺師*がいます！悪いカバがいます。

安全に関しては、けがをしない、人命が失われないという観点ですが、どうやらセキュリティは、おカネの面、人命の面、稼働率の面などいろいろありそうですね。解析も多面的にわたりそうです。



*電子計算機使用詐欺罪及び不正アクセス禁止法に抵触する可能性が高い。
ただしカバは自然人ではないため刑事罰は与えられない可能性が高い。

安全解析vs セキュリティ解析(要素の差異)

Table 3 – Hazard severity level　　IEC 62278 Table 3による

Severity level	Consequence to persons or environment	Consequence to service
Catastrophic	Fatalities and/or multiple severe injuries and/or major damage to the environment	
Critical	Single fatality and/or severe injury and/or significant damage to the environment	Loss of a major system
Marginal	Minor injury and/or significant threat to the environment	Severe system(s) damage
Insignificant	Possible minor injury	Minor system damage

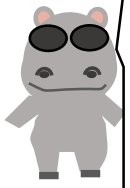
安全の面　　サービス提供の面

安全解析vs セキュリティ解析(要素の差異)

Table 3 — Qualitative Impact Assessment example EN 50701 Table 3による

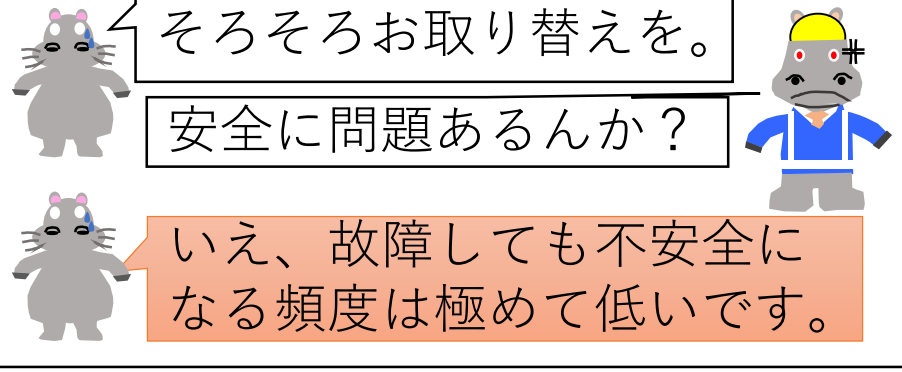
Impact	Human health and safety	Operational availability	Financial impact
A	One or several fatalities	Most of operations disturbed during more than 1 week	Could lead to organization bankrupt
B	Several severe or critical injuries	Most of operation disturbed between 1 day and 1 week. Important operation disturbed during more than 1 week	Impact in a significant way the organization annual budget (>10 % of revenue)
C	One severe injury or several injuries requiring hospitalization	Most of operation disturbed between 1 h and 1 day Important operation disturbed between 1 day and 1 week	Impact in a significant way the organization annual benefits.
D	One injury requiring hospitalization or several light injuries (not requiring any hospitalization)	Important operation disturbed less than 1 day.	Impact not visible on annual basis

In the initial risk assessment, the worst-case consequence shall be used to determine the considered impact for each asset property.



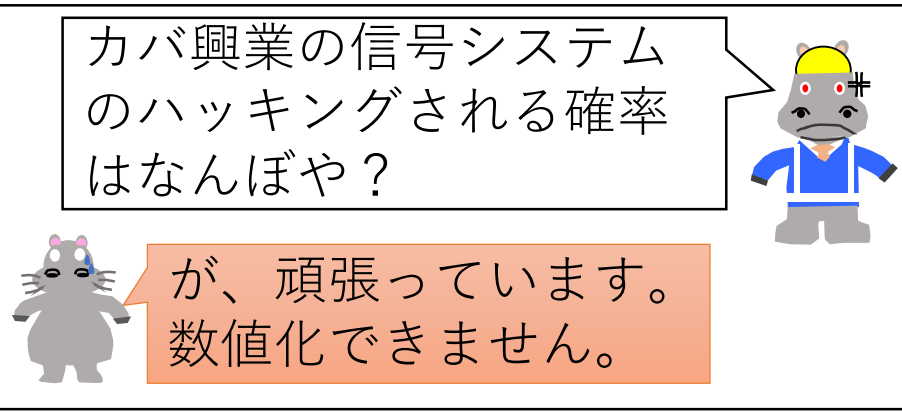
事前解析の場合は、この中で一番重篤なものを選ばなあかんで。

安全解析vs セキュリティ解析(解析方法の差異)



安全機能の失われる頻度が重篤度を加味して受け入れられるレベルであればよい。
仕様やソフトウェアの誤りなどは、許容頻度に相当する(いわゆるSafety Integrity Level)品質管理と技術的手法であればよい。

確率論的解析アプローチから、使用する技術的手法や品質基準を決める



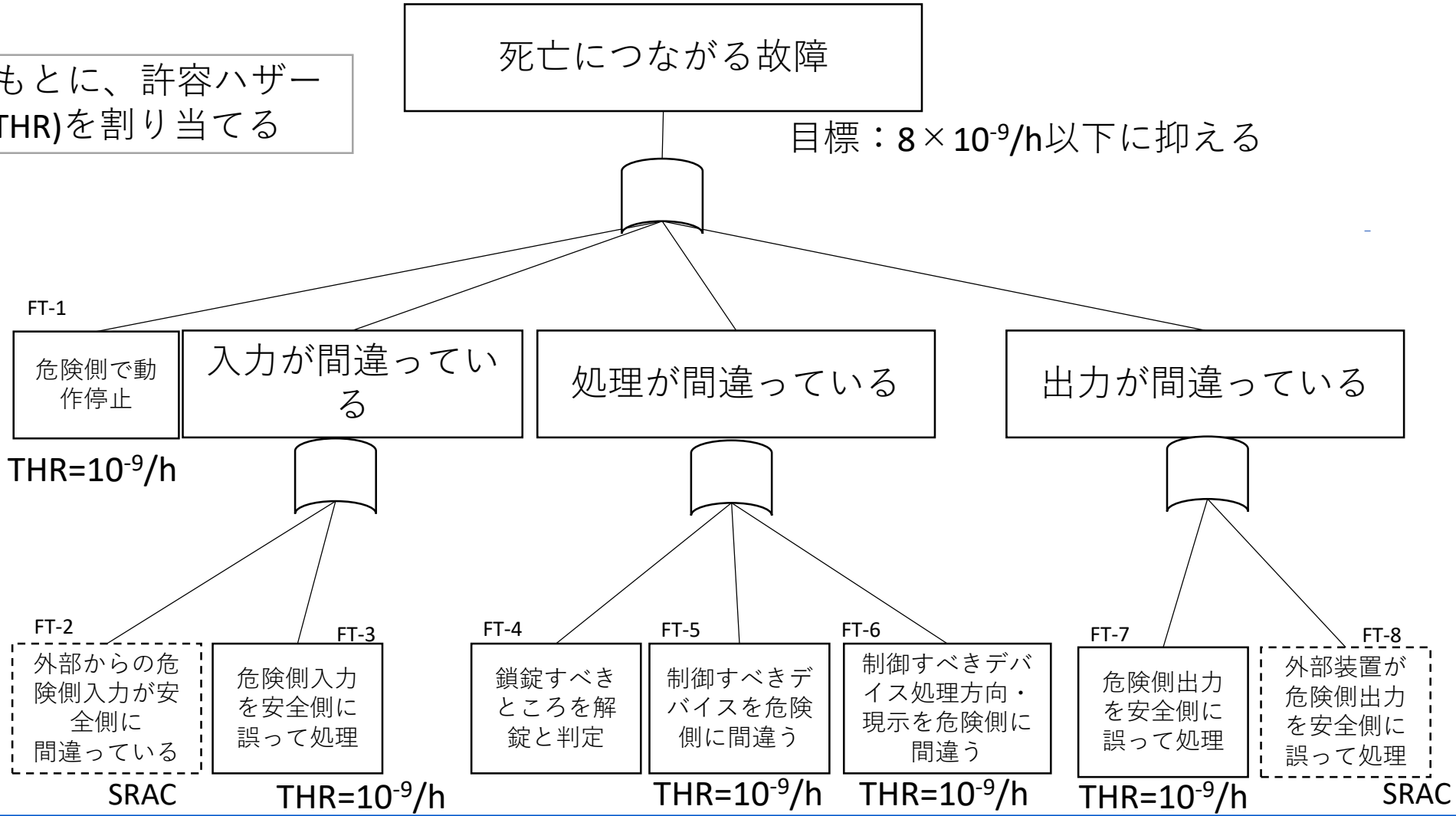
悪意のある目的を達成できる容易さ・困難さが重篤度を加味して受け入れられるレベルであればよい。
ハッキング容易さと重篤度を加味した技術的手法であればよい。

確率論的なアプローチは困難、目的達成容易性の解析になる

安全解析vs セキュリティ解析(解析方法の差異)

トップダウンの安全解析例

FTA解析をもとに、許容ハザード頻度(THR)を割り当てる

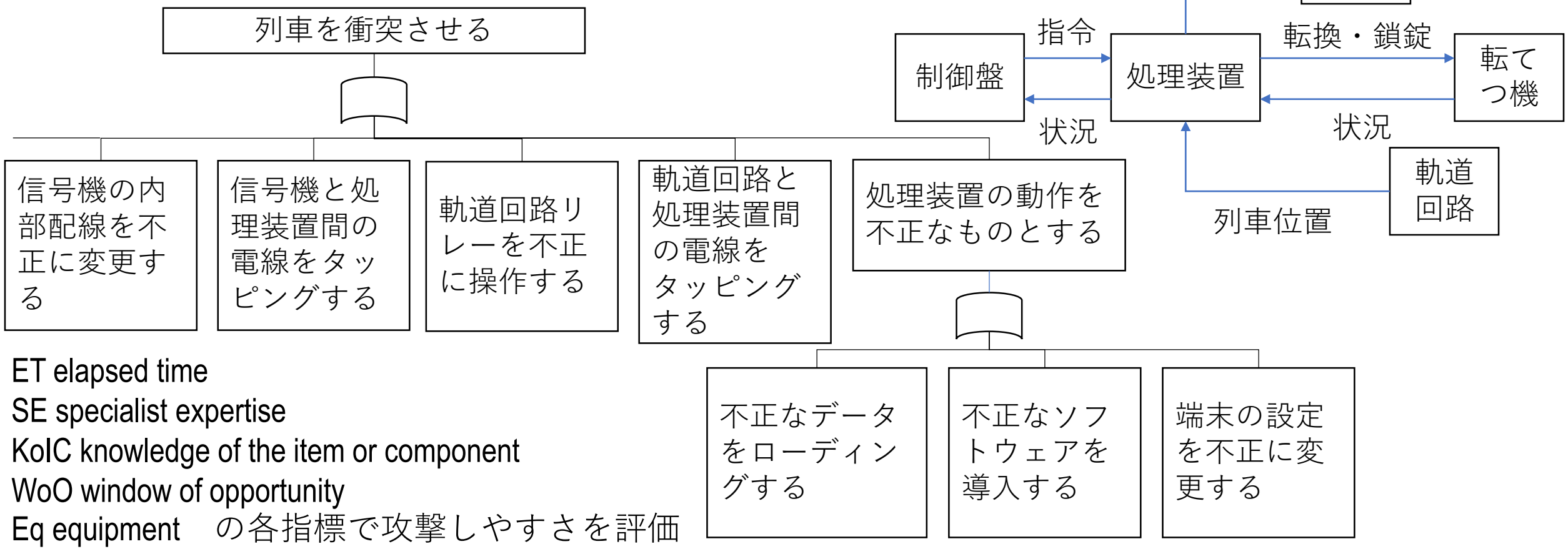


THR：Tolerable Hazard Rate
SRAC: Safety Related Application Conditions

安全解析vs セキュリティ解析(解析方法の差異)

トップダウンのセキュリティ解析例

アタックツリー解析：ISO SAE 21434
H.2.5 Attack path analysis



モデル

ET elapsed time
SE specialist expertise
KoIC knowledge of the item or component
WoO window of opportunity
Eq equipment　の各指標で攻撃しやすさを評価

自動車の場合はどうか(リスクアセスメントと要求)

自動車
ISO SAE
21434

アイテム定義 ⇨ サイバーセキュリティゴール*

*一つ以上の脅威シナリオに対するコンセプトレベルのサイバーセキュリティ要求

⇨ サイバーセキュリティコンセプト

鉄道
CLC/TS
50701

対象システムを同定 ⇨ 初期リスクアセスメント ⇨ 対象システムの分離 ⇨ 詳細なリスクアセスメント ⇨ サイバーセキュリティ要求と詳細化

えらい自動車はあっさりしてるな。

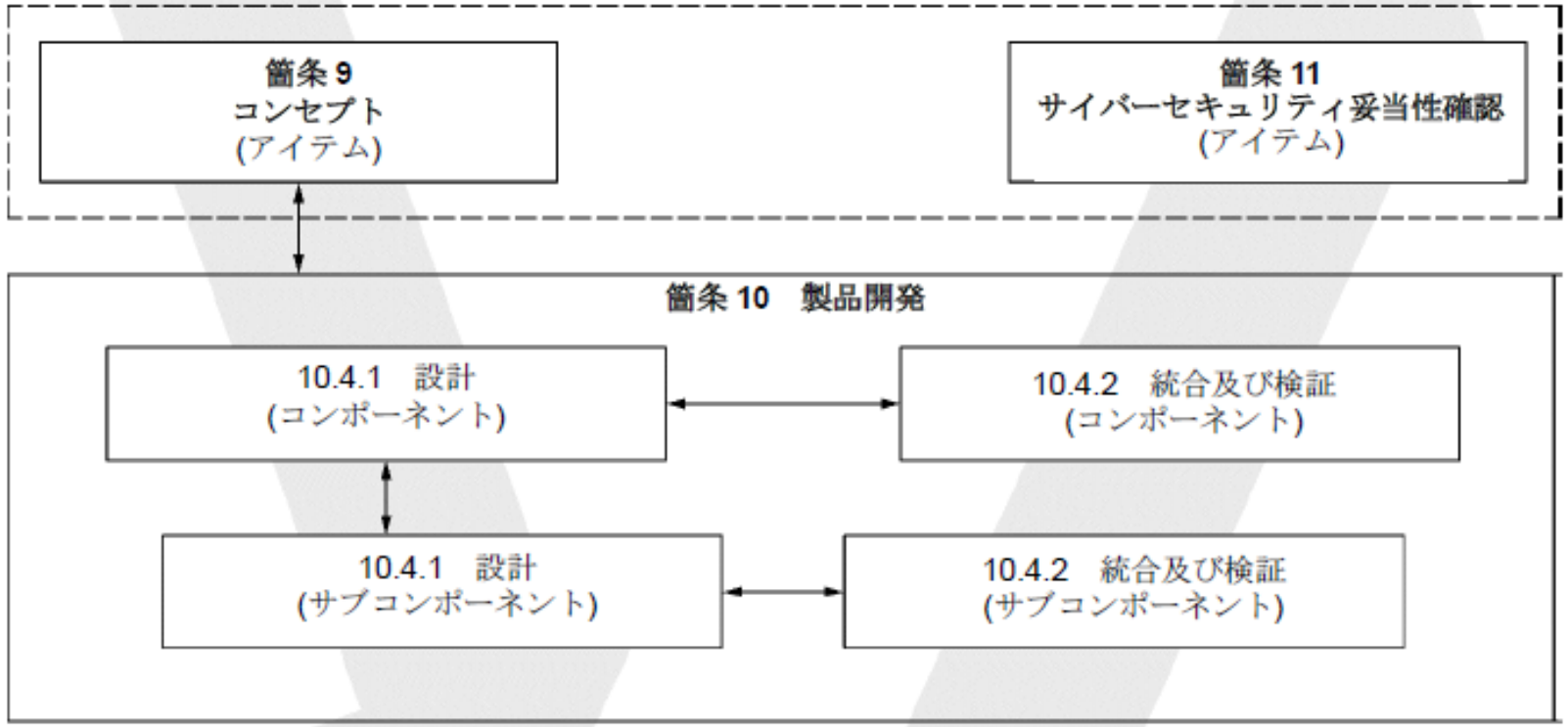
甘いな社長。サイバーセキュリティゴールを成立させるには、ISO SAE 21434の15章の以下全部やる必要があるんやで。

ISO SAE 21434 Chapter 15の内容

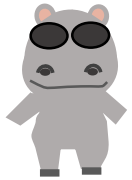
- 資産識別
- 脅威シナリオ作成
- インパクト評価
- 攻撃経路分析
- 攻撃実現可能性の評価
- リスク値の決定
- リスク対応の決定

自動車の場合はどうか(製作)

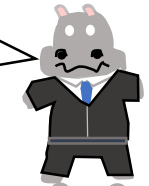
自動車
ISO SAE 21434



セキュリティ対策はソフトウェアの製作に近いから、鉄道のソフトウェア規格IEC 62279の設計と試験に近いことが書いてある。



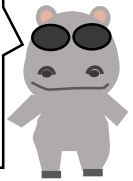
で、鉄道は!セキュリティ規格はどうや？



ISO SAE 21434 10.4.1,2に相当する部分はない！

なんでや！

ハナから鉄道ではサブコンポーネントなんて作る気ないからや。（と思う）



自動車の場合はどうか(作った後)

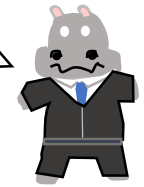
ISO SAE 21434 13.3.2 Requirements and recommendations
[RQ-13-01] For each cybersecurity incident, a cybersecurity incident response plan shall be created that includes:
a) remedial actions;
b) a communication plan;
c) assigned responsibilities for the remedial actions;
d) a procedure for recording new cybersecurity information relevant to the cybersecurity incident;
e) a method for determining progress;
f) criteria for closure of the cybersecurity incident response; and
g) actions for the closure.
[RQ-13-02] The cybersecurity incident response plan shall be implemented.

CLC/TS 50701 10 Operational, maintenance and disposal requirements
10.1 Introduction
For this version of this Technical Specification, specific advices are provided for vulnerability management and patch management activities. In a later versions, security monitoring, Incident management, business continuity and crisis management will be also addressed.

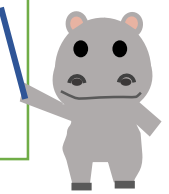
自動車の場合はどうか(作った後)

うーん。鉄道の方は、相手がプロやから、運用に入ったら個別に決めるということで、脆弱性のマネージメントと、パッチあてしか決めてないのか。。　こんなお客さんばっかりだから、期限が来たらサポート終わりですよなんて言えるわけないよ。。。

自動車はやっぱりエンドユーザーがどんな状況か全くわからんからな。ウチの規模では対処できる相手じゃないかも、やっぱりOEMは無理か。。。



しかしながら、自動車の
「サイバーセキュリティ監視は，サイバーセキュリティ情報を収集し，定義されたトリガーに基づくトリアージのためにサイバーセキュリティ情報を分析する。」
という内容が鉄道にないとすれば、脆弱性が残ってしまうかもしれませんよね。。



まとめ

- 安全におけるライフサイクルと、セキュリティにおけるライフサイクルの異なる点をご説明しました。
- ✓ 安全については、設計段階の検討が重要ですが、セキュリティはライフサイクル全体の検討が必要です。

- 安全とセキュリティの解析方法をご説明しました。
- ✓ 安全解析は基本は確率的なアプローチ、セキュリティは攻撃容易性について着目します。

- 鉄道と自動車のライフサイクル管理について特徴的な点をご説明しました。
- ✓ どちらも基本となる規格のライフサイクルをベースに、どのような行為をセキュリティ対策で行うべきかを述べていますが、特性により少し異なる点もあります。良い点を相互に参照してはいかがでしょうか。