改定されたRAMS関係規格の注意点について

－鉄道における国際規格IEC 62425規格の変更とそのポイント－

森　崇　　吉永　純

鉄道認証室

講　演　内　容

１．鉄道保安システムの安全原則
２．機能安全って？
３．規格による安全の考え方
４．IEC 62425規格の変更ポイント

0. 説明の前に：登場するキャラクター

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

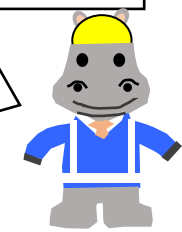
カバ鉄道　社長
品格の経営、根拠ある経営

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

1. 鉄道保安システムの安全原則

あー、今回ご紹介する「列車間隔制御装置KABA-BS02」は、**フェールセーフという安全思想は変えず**ですね、コンパクトかつ省電力としたもので、もちろん**調整なんかも今までと同様**に行って頂けます。もちろん**稼働率**もばっちり。おすすめです。ハイ自信をもっておすすめです。私カバお、**営業一筋これ以上おすすめ**のものはありません！



あーハイハイ、あんたらカバ興業はいつもそうやって、**安全や、稼働率高い、メンテしやすい**とかいうけどな、結局「オレらを信じてください。信頼してください」ってゆうてるだけやないか。そんなんで安全かどうか、安定して運用できるんか、分からへんやないか。で、「**ふぇーるせーふ**」か。そのマジックワード君ないに説明してくれるか？

鉄道に関する技術上の基準を定める省令　第六十三条　「運転保安設備は、電気機器及び回路の特性に応じ、その**機能に障害が発生した場合においても**列車等の安全な運転に**支障を及ぼすおそれのない機能**を有しなければならない。」とあるのでそれがフェールセーフの原則じゃないですか。

要は「カバ興業の製品は、壊れることは特性上しょうがないけど、壊れることを想定してやな、そんで壊れた時には、安全な運転に支障しないような状態、すなわち列車を止める方向で制御する」って言いたいんやな！それがフェールセーフだと。。それってまあ、一見稼働率高いと矛盾しそうやけど、どうすんねん！

い、じ、わ、る。。いえなんでもありません。

1. 鉄道保安システムの安全原則(フェールセーフ)

規格でのフェールセーフの定義は

able to enter or remain in a safe state in the event of a failure

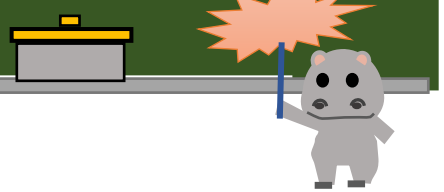
-IEC 60050 821-01-10

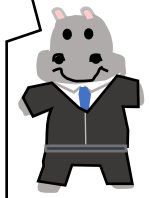
故障した際に安全状態に入るか、とどまることができること

故障を検知し、故障検知後安全状態に遷移しとどめることができる機能を実装するともいえる。

11月21日

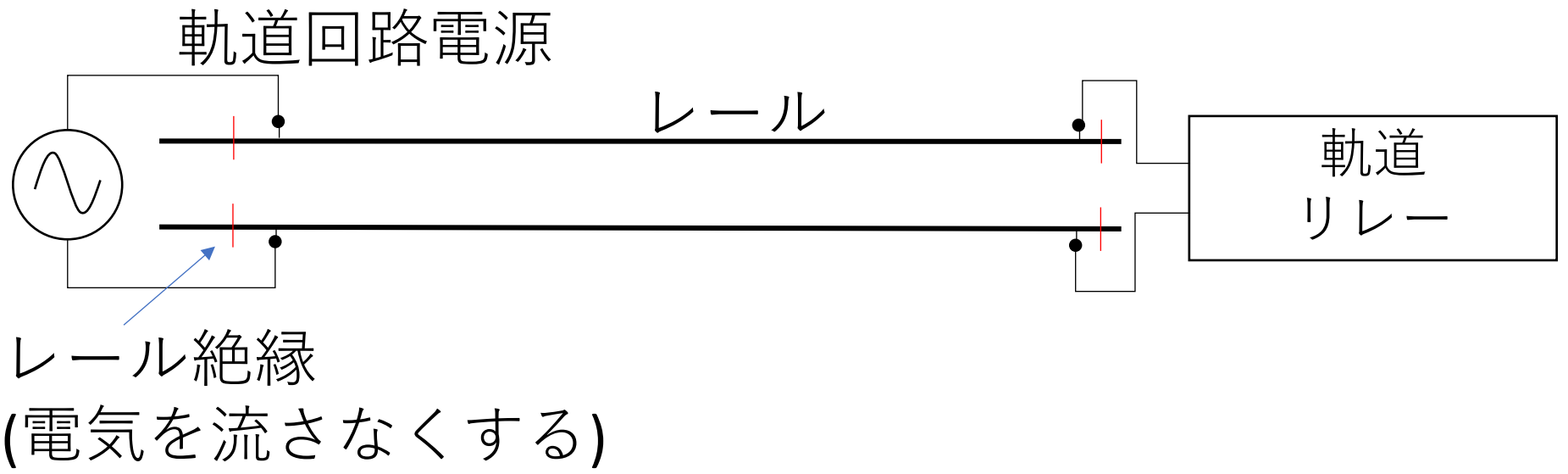
日番カバお

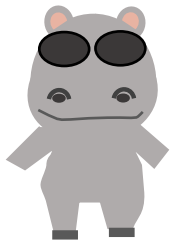




IEC 60050 821-01-10の日本語は「フェールセーフ」、韓国語、中国語は、「故障安全」とかいてるな。故障安全。。そういうことか。

1.鉄道保安システムの安全原則(軌道回路の例)



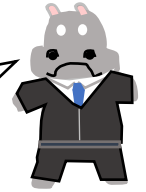


このシステム、故障部位がどこでも「リレーが落下する」という状態遷移になるように工夫されている。これは、どのような状態が起こるか、どこが壊れるかの網羅的解析が必要で、想定なくこの回路が出来上がっているわけではない。すなわち、「できる限り読み切って、故障しても大丈夫な機能」を盛り込んでいることになっているわけや。

2. 機能安全とは

社長！機能安全とは何でしょうか？

え、きのうあんぜん？バカにするな。カバ興業は今日も安全や！
「継続する安全」カバ興業にお任せください！



社長！さすがですね。よっ社長！「継続する安全」が機能安全なのかもしれません。

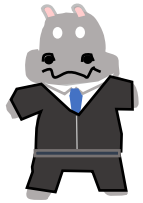
え、ボケたのに、まさかの返し？！「機能による安全」じゃないのん？

3.1.22 functional safety
part of the overall safety that depends on functional and physical units operating correctly in response to their inputs

-IEC 62425:2025

何かの（おかしい）入力に対して機能とユニットがうまく働いて実現する安全の概念といえるのではないでしょうか。

2. 機能安全とは



ヤバい状態

なんか壊れる、他の装置から影響(以下異常)を受ける

壊れるな！というのはムリ
影響を受けるな！というのは対処必要

異常を健全な機能で検知

どのような異常かがわからないと、対処の方法がはっきりしない

何らかの形で安全側に遷移させる

壊れたことが分かっても、安全側に遷移させないと、誤った状態のままになる

安全側に固定する

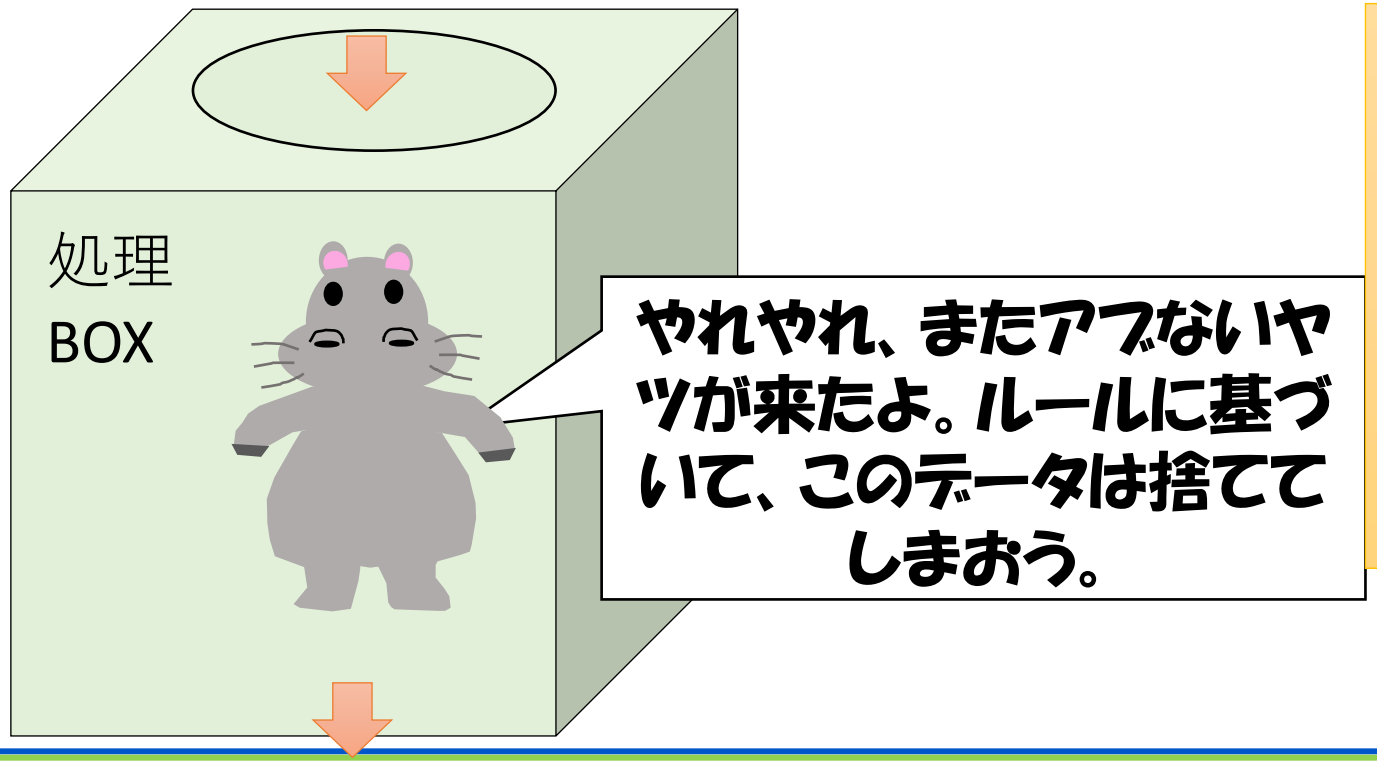
勝手に状態遷移すると、誤った状態に復帰する。

2. 機能安全とは(こんなイメージでは)

機能安全とは

入力に対して、物理的ユニットと機能が正常に働くことにより安全を確保することをいう。

安全を阻害する入力



**システムが健全に作りこまれ、また「危険な場合の動作定義」をする必要がありますよね。
このため、安全を阻害する要因を読み切り、その対処を決めておくという、網羅的なルールと作り込みが必要なんですよね。**

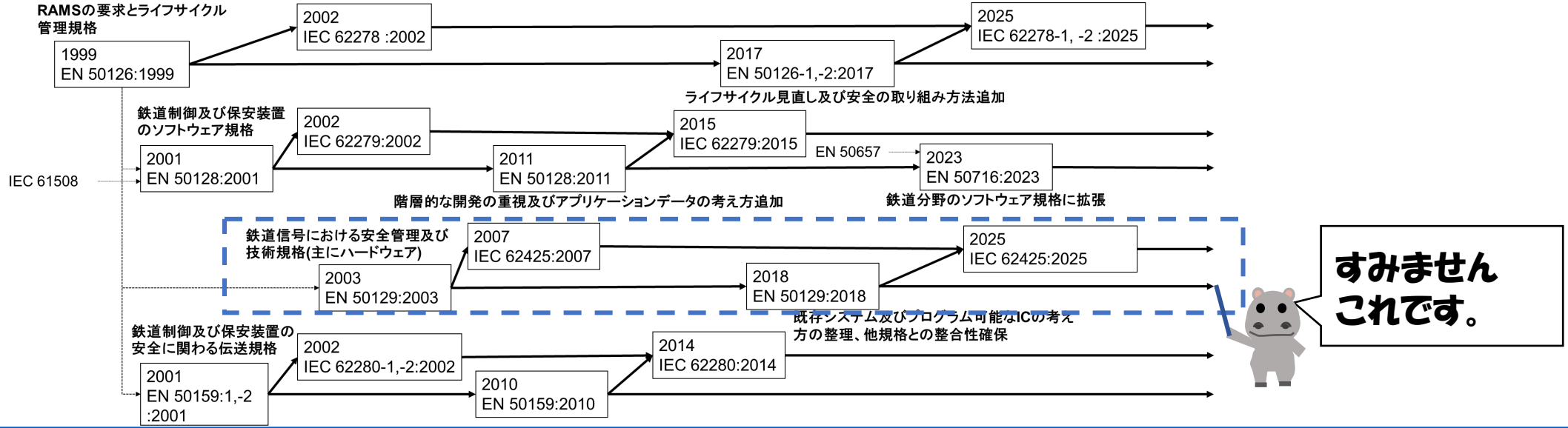
3．規格による安全の考え方

社長！カバ鉄道さんにシステムを受け入れてもらうには、どのような点に注意していますか。

笑顔！じょうだんや。あいつら、「故障は許さへん」とゆうとったが、カバ鉄道の社長さんに一喝されたんか、この頃「Tolerable Functional Failure Rateと故障の関係が大丈夫かどうか説明しろ」といつも言われるわ。

なかなかいいですね。IEC 62425規格では、それだけではないんですよね。

オマエそれでもコンサルか！急に規格の名前なんかゆっても、お客さんら目を白黒させるだけやろ。まあオレも急にTFFRとか言ってしまったけどな。要は「安全に関係する機能が失敗するのはこれくらいやったら堪忍するで。ということや。

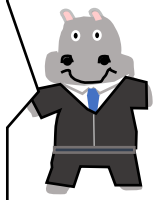


すみません
これです。

3．規格による安全の考え方

カバ社長のご意見

故障はアカン。言われてないことでもこっそりやっとくのが、KABA Qualityや。
言われてることだけやるなんて、信頼は得られへんで！計画に書いている以上のことをやる！それがカバの誠意や！
一人一人の技術力がスゴイカバ興業に死角なしや！技術屋を大事にして、爆発的な開発能力で業界をリードする！それがカバ興業や！



研究開発型企業？

カバ実課長の忠告

やり方をしっかり計画して、その計画に基づいて開発、設計を実施します。第三者の目で実施を確認し、もし計画からの差異が発生したら、計画に定められた通りの行為で変更するか、計画を改め、その影響調査を行い、適切にやり直します。

規格に合った企業？

3．規格による安全の考え方

Random fault

パーツなどがある一定の確率で壊れることによる故障

確率論的なアプローチ

Systematic fault

inherent fault in the specification, design, construction, installation, operation or maintenance of a system, subsystem or equipment
仕様や設計などの間違いからくる故障

Quality management

Life cycle process管理によるヒューマンエラー防止による安全
(IEC 62425 Ed.2 5.2 The quality management process)

どのような管理手法を各RAMSライフサイクルにおいて、安全のために適切なルールを準備するかが中心の議論となる。

The first prerequisite for safety acceptance is that the quality of the system, subsystem or equipment has been, and continues to be, controlled by an effective quality management system throughout its life cycle.

Safety management

Systematic fault残存リスク管理およびセキュリティの脅威によるヒューマンエラー防止による安全
(IEC 62425 Ed.2 5.3 The safety management process)

残存リスク管理の要素は、structured documentation, safety life cycle, safety organization, safety plan, hazard log, safety requirement specification, system design for safety, safety operation and maintenance plan, safety verification, safety validation, safety qualification test, management of SRACs, safety justificationを行うことに対処。

4. IEC 62425規格の変更ポイント

機能安全を網羅的に考える

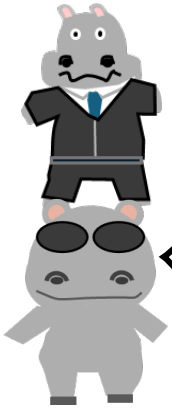
↓

今までの規格で、詳細に決めたほうが良い事項を追加する

- **今まで使用していて、システムとして活用したい、または組み込みたい場合の対処**
- **安全関連機能と車の両輪をなす、制約事項の明確化 Safety Related Application Conditions**
- **ユーザーが動作を定義できるICである、User Programmable Integrated Circuitの要求**

4. IEC 62425規格の変更ポイント

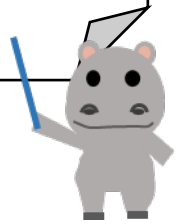
既存装置の活用と規格適合性について



ウチの今までの開発資産どうなる?

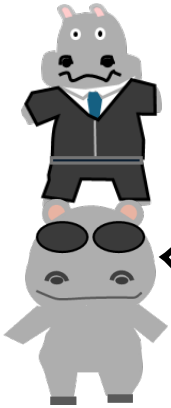
今までは、「対象外」とされていたが、これからは要求を守れば「規格適合対象」にできるんや。

会社は過去の資産を抜きに開発を行うことは少ないでしょう。
これらの資産を抜きにして開発を進めると大変非効率ですので、過去は「IEC 62425適合性対象外」としてきましたが、対象システムの中で対象の部分と対象外の部分が混載してしまいます。これを避けるため、一定の条件を付けて「規格適合」とすることができるようになりました。機能やインターフェースの明確化、故障モードとその故障の起きる頻度、試験とそのverificationがなされていることが大まかな条件となります。(他に条件あり)



4. IEC 62425規格の変更ポイント

SRACsについて



安全を担保するのはなんや？安全のための機能か？

使う時の制約や前提を守ってもらうためのSRACs(Safety Related Application Conditions)もいるで。

- いままで、SRACsについては、その管理に関して明確な規定があったわけではありませんが、使い方を誤ると、せっかくの装置も台無しなので、規格上も重視されるようになりました。
- SRACsについては、「できないことを前提にするな」 など「べからず」が明記されるとともに、事故を引き起こす要因である「ハザード」と必ず対応させることが求められます。「なんとなく危なそうだから制約をつけておこう!」というのは避けなければなりません。

4. IEC 62425規格の変更ポイント

ユーザがプログラムできるLSIについて

なんか焼き込んで動作定義できるLSIこの頃よく使うらしいな。

FPGAとかPLDとかいうやつやな。ロジックゲートを記述言語でプログラムできる。ハードとロジックの設計双方の技術が必要や。

- システムの高密度化を進めるため、FPGA,PLDなどのLSIにロジック回路をプログラムする手法が安全関連システムにも導入されるようになってきました。
これは、ロジック回路設計をSystem Verilogなどの HDL(Hardware Description Language)を用い記述します。このため、LSIのハードウェアのランダム故障だけではなく、システマティック故障も考えなければなりません。
また、ソフトウェアの規格　IEC 62279では手薄な、ロジック回路が同時並行的に動くことによる、タイミングの問題(Clock domain crossingやMeta stability)などが発生する可能性があるので、こういったことも注意する必要があります。

4. IEC 62425規格の変更ポイント

その他の事項について：TFFRについて

ハザードがどれくらいガマンできるかのTHR(Tolerable Hazard Rate)とハザードをトップ事象とした安全解析から、ハザードをストップさせる安全機能とその安全機能の失敗許容度TFFR,(Tolerable Functional Failure Rate)とその SILを決めます。

ヤバい原因であるハザードとどれくらい許容できるかのTHRを決める。

ヤバい原因であるハザードを防ぐ機能である安全機能と、THRと矛盾しない失敗許容度TFFRを決める。

安全機能が実装されるサブシステムなどを決め、割り当てられた機能のTFFRと矛盾しないサブシステムなどの許容故障頻度を決める。

実際の回路設計、構成設計などで、許容故障頻度を満たすような実装を行う。

4. IEC 62425規格の変更ポイント

その他の事項について：BIについて

機能が失われたら危険側に遷移する許容度(TFFR : Tolerable Functional Failure Rate)がSIL1未満の10^{-5}/hレベルのものはどうなんですか？

それは、SIL0や。

SIL0てなんですか？TFFRが規定されているので、安全にかかわるのではないですか？社長は数値が低ければ安全に関係ないと割り切っていいとおっしゃるのですか？

なんやおまえ！神聖カバ興業にケンカを売ってるんか！安全は正義！絶対や！安全に関係する奴はSIL4、いや5や。確率は関係ない！

いきなり格上げですか。今までの規格はここは抜け目だったんですよね。
これらは安全に関わるけれど、でもリスクは少ないものとしてBasic Integrityとして扱うことになります。
安全に関係ないものもBIとして扱いますが、IEC　62425の対象外となります。

4. IEC 62425規格の変更ポイント

その他の事項について：階層的な考え方

SASC (Specific Application Safety Case)

GASC (Generic Application Safety Case)

Application data and configurations

Subsystem #1

Subsystem Safety Case

Subsystem #2

Subsystem Safety Case

Equipment#1

GPSC (Generic Product Safety Case)

Equipment#2

GPSC (Generic Product Safety Case)

Equipment#3

GPSC (Generic Product Safety Case)

下から上まで全方位で安全の証拠が必要なんですね。乗務員から社長まで安全はしっかりと

5.まとめ

- 機能安全とは「危険を解析しておき、異常な入力があった場合、安全となるように状態遷移させる」ことによる安全です。
- IEC 62425は、鉄道保安装置の機能安全での安全を実現するための規格です。
- この機能安全を実現するため、「補強したらよりよくわかりやすくなる」という点を改定で補強しています。
- 安全に関わる機能を定義するのと、制約条件であるSRACsは車の両輪です。この部分が個人的には一番大事と思っています。

11月21日

日番カバお