安全のかなめ、故障検知と停止

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

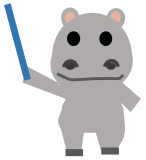
カバ興業　社長
座右の銘：技術と直感

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！」

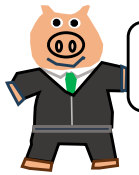
バチバチ

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！

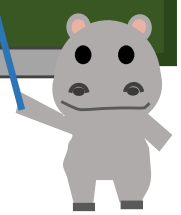
カバ鉄道　乗務員　カバどん
いつかは自動化されるかも。ドキドキ



ブタ工業　社長
カバ興業を凌ぐ強い体質づくり

1．はじめに

- システムの異常があった場合どうしますか。
- これは個人的には難しい質問だと思っています。私は鉄道会社にいる時には、鉄道通信と鉄道信号を同じくらいの期間担当しており、鉄道通信と信号に関して、思想の差の違いに驚きました。
- どのような考え方で異常をとらえ、対処するかを考えていきたいと思います。



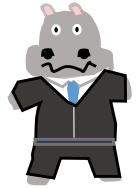
2．壊れたらどうする？！

社長！まあ当たり前の話しするで。カバ興業の装置な、壊れたらどうすんねん。どうなるねん。

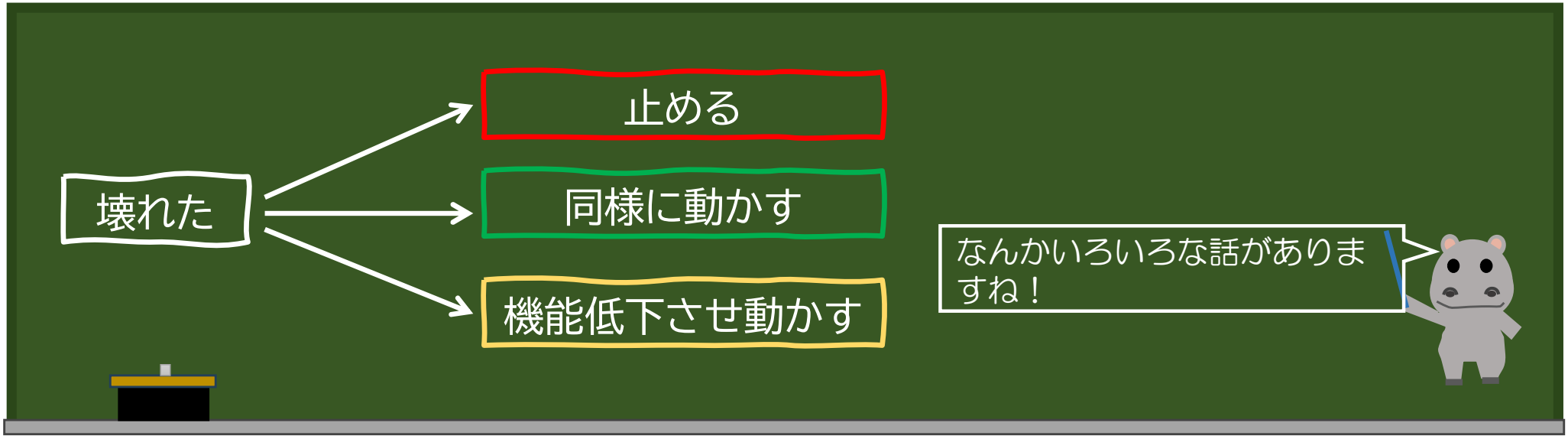
ウチの装置は、そんなん簡単に壊れないようにしていますよ。信頼のカバ興業ですから。壊れませんって。

そんなん聞いてないねん。壊れないように作るのはそもそも機能安全ちゃうやろ。壊れたらどうなるねんって聞いてるねん。

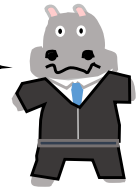
そ、そりゃあ止まりますけど。そういうもんじゃないですか。フェールセーフのカバ興業ですから。お任せください。



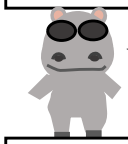
そやけどな、ウチも客商売やねん。止まりました安全です安心してください。ってゆうてもな、続いたら許してもらえへんねん。だから止めたらいいとかそんな簡単やないねん。



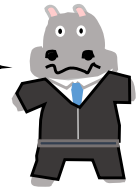
2．壊れたらどうする？！



またカバ鉄道の課長の禅問答にイジメられたで。お前らどう思う！イジメやろ。



いや、意外にエエこと言うているように思えたけどな。。



何やオマエ、その媚の売り方は！カバ鉄道に転職するつもりか？

壊れた場合、その特性に応じてどのような手を打つのかは、リスクアセスメントを実施した後、どうするかをしっかり決めておくこと。また安全性と稼働率の両立を図るためにはどうするかをしっかり考えてくれって言っているんやで。

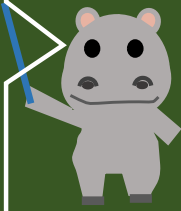
伝送内容によっては少々エラーがあって、誤り訂正で伝送が遅くなっても、それでも良い場合や、完全に止まってしまうより細々でも動いた方がよい場合もあるでしょう。

機能特性の把握とアセスメント

故障した場合の対処策定

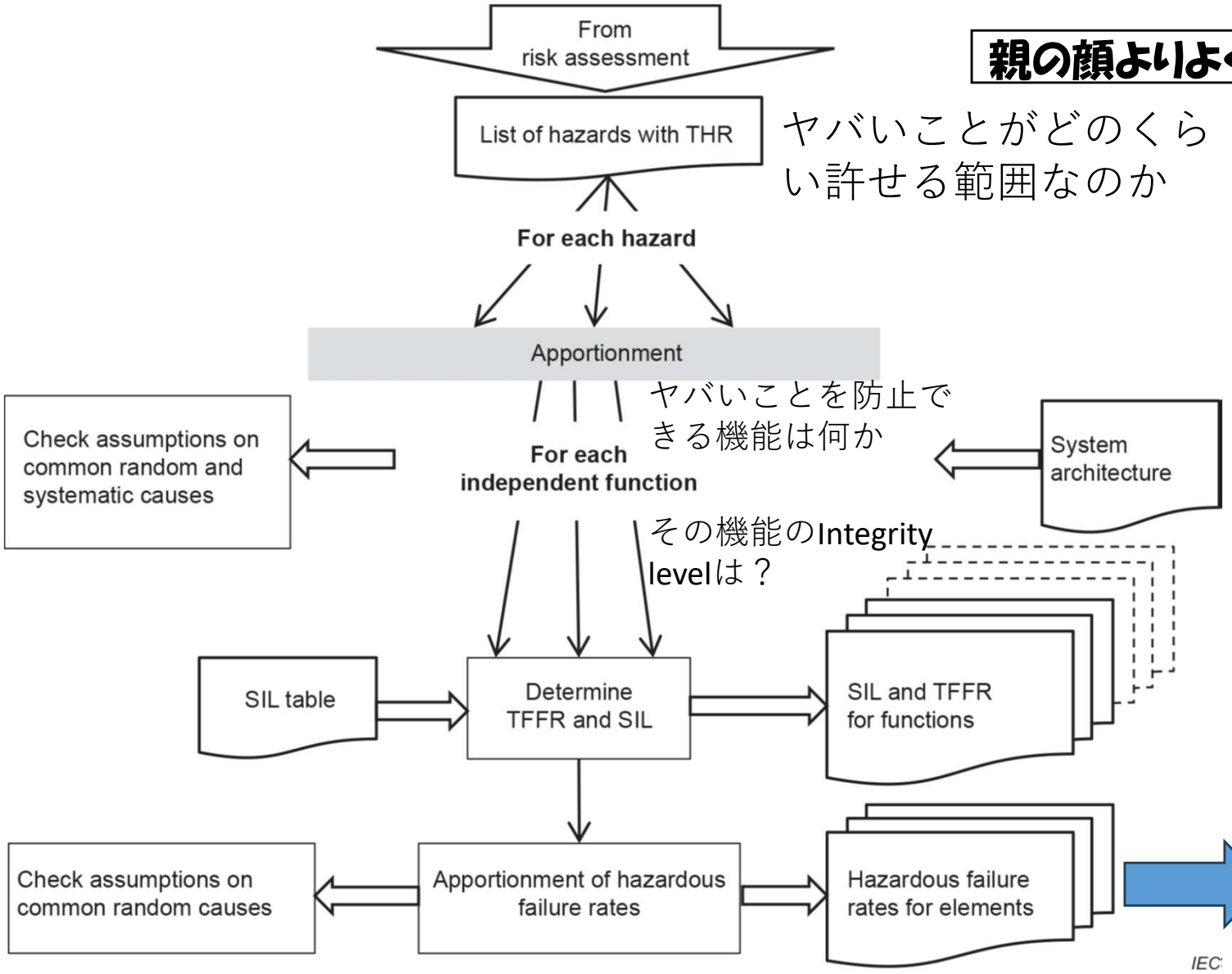
対処のTolerability決定と
その実装の正当性

先ほどの電気課長の質問には、故障した場合、安全関連機能に関するものの場合、該当のユニットは停止させ、他の系に切り替え、ミッションは継続します。が良かったのかな。知らんけど。



3. 安全関連機能の場合（前回資料）

親の顔よりよく見る絵



ヤバいことがどのくらい許せる範囲なのか

ヤバいことを防止できる機能は何か

その機能のIntegrity levelは？

どの要素(ハードウェア) にどの程度の危険側許容値が割り当てられるか？

IEC 62425 Ed.2 Figure A.4 より引用

4. 対処の基本

なんかハザードに対処する機能とか言ってたけど、具体的にはどうするかゆうてないやん。

故障を検知する機能

検知できなかった場合

検知できた場合

故障したユニットを止める機能

止められなかった場合

止められた場合

安全側に固定する機能

固定できなかった場合

故障状態が、次のメンテナンスまで継続

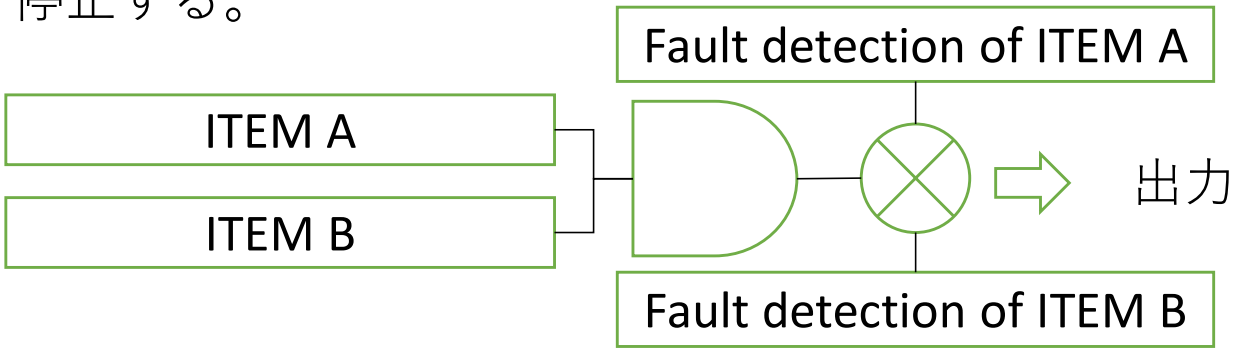
ここに至る危険側故障頻度が、許容できる値を超えるとそもそもダメ

ここで安全！

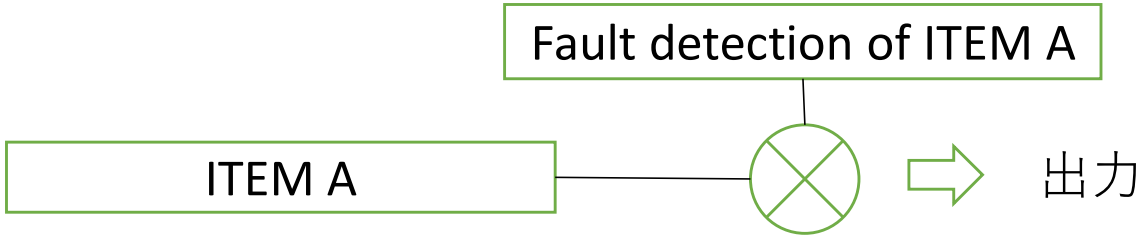
4. 故障を検知する機能

検知する方法によって、検知できる蓋然性が変化する！以下のやつは固い方法！

Composite fail safety : 2つのアイテムを比較し、一致しない場合や故障があれば出力を停止する。



Reactive fail safety : ITEM Aの出力を監視し、故障があれば出力を停止する。



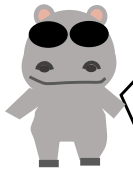
Inherent fail safety : ITEM Aの故障モードはすべて安全側に遷移する。

4. 故障を検知する機能

なぜ固いか説明しよう！

Composite fail safetyの例

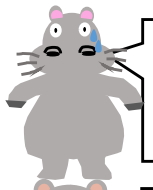
*Item間独立のことをIEC 62425では Primary independenceと言います。



この比較装置の故障状態が読み切れて、物理的現象で故障時安全に遷移することが解析できれば、危険側故障頻度を0と仮定できるボーナスステージがあるんや。。。

IEC 62425 A.3
Safety integrity In the case of components with inherent physical properties (see Annex C) a hazardous failure rate of zero is generally assumed.

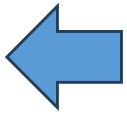
4. 故障を検知する機能



いや、でもお客さんの中で、そんな特殊なものじゃなくて、市販の普通のもので何とかしてくれっていうご要望、すごくあるんですけど。。。

そりゃまあそう言うやろうけど、なんか壊れた場合、大体においてやで、故障検知する機能も無くなるんちゃうか。機能の独立性が大事やで。

なんか売ってるヤツ
（main item）



ウォッチドッグタイマーなど
故障検知のボードを付加

これは、main itemに付加的にチェックデバイスを組み込む方法で、Secondary independenceと言います。前述のPrimary independenceよりも条件が緩いです。
SIL3,4機能を実装する場合、1つの故障で独立性を阻害されないことを前提に、故障検知の方式は、物理的な安全性(inherent fail-safety)は要求されていません。
SIL1,2機能を実装する場合、故障検知の方式は、物理的な安全性(inherent fail-safety)は求められておらず、許容値までの誤り見逃しが認められます。

5. システムを安全側に遷移させる

故障を検知する機能

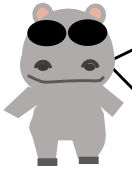
検知できた場合

故障したユニットを止める機能

検知してもほっとくのは、アカンですよね。

腐ったミカンは。。。

なんかゆうたか？その発言は見過ごせんな！



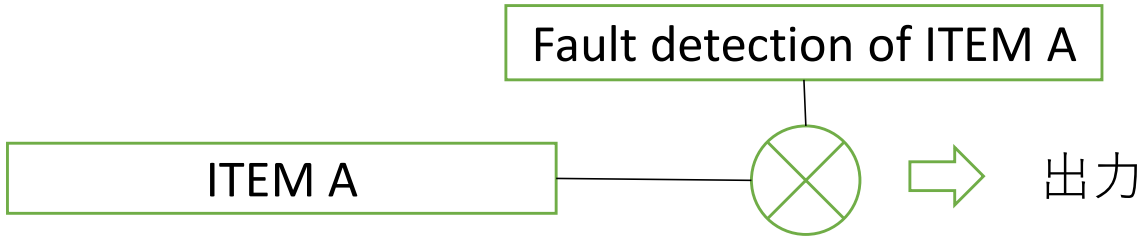
真面目な話、止める機能は、SIL3,4機能を実装するモンは自動で、
SIL1,2を実装するモンは、人手でも構わないことになっている。
(IEC 62425 Table E.4 注釈a).2)

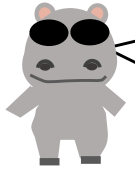
5. システムを安全側に遷移させる

よかった！これで安心だね。カバ興業の製品は絶対事故は起こしません。だって物理的に絶対にないとお墨付きがあるからね。今すぐ営業行きたくなったよ。

いや待て待て。落ち着けよ。装置は急に止まれない！

Reactive fail safety : ITEM Aの出力を監視し、故障があれば出力を停止する。

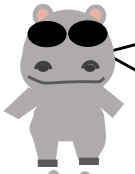




この場合、故障検知するまでは、誤ったデータが出る可能性があるんや。

ヤバいじゃない。間違い流出。確実にただじゃすまない未来しか見えないけど、こんな方式規格で認められているの。ヤバいじゃない！

5. システムを安全側に遷移させる



実はまだあるんや。。

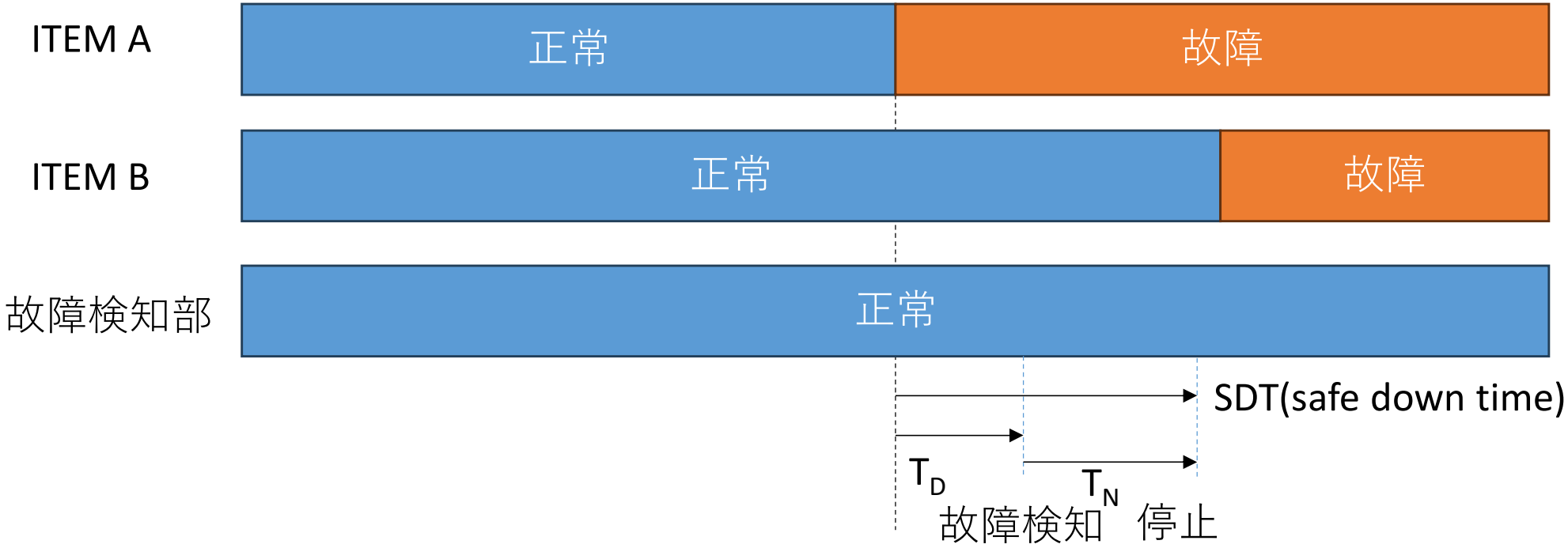
もう技術屋はうそつきだということが十分にわかったよ。
聞かなかったら素直な気持ちで売り込みに行けるのに、もう聞きたくないよ。

それは、多重故障や。。。

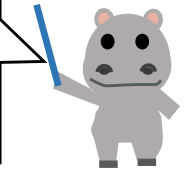
頼むから壊れない安心できるもの作ってよ。怒られるの誰だと思っているんだよ！！！もうカバ鉄道の鉄格子のあるゲストルーム行きたくないよ。

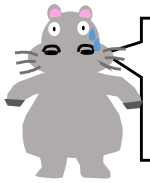
5. システムを安全側に遷移させる

多重故障を防ぐ



ITEM Aが故障した際に、ITEM Bの故障がSDTの間に起こると多重故障で、検知が難しくなることがあります。SDTに至るまでに、次のアイテムが壊れる確率を計算し、危険側故障頻度を求めます。

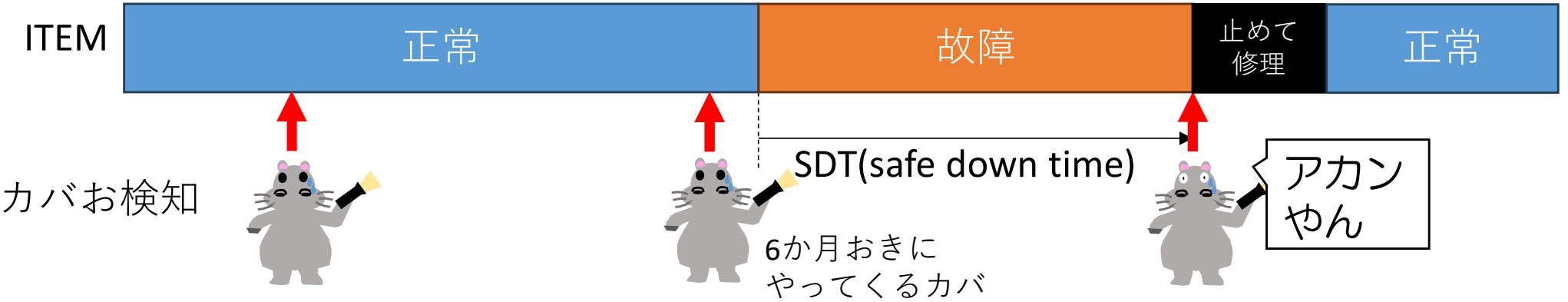




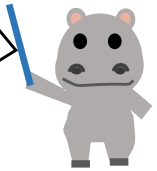
なーんだよ。こんなのSDTまで超短いから、起こるわけないじゃない。技術屋はすぐ脅すんだから。こんなん「絶対起こりません」って言っておけばいいんだよ。

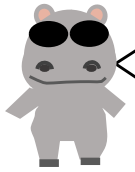
5. システムを安全側に遷移させる

SIL1,2では、止めるのは「カバ」でもいい！



このような場合は、SDTが結構長くなります。一つ目の故障は事故につながらなくても、二つ目の故障が重なった場合、状態遷移が読み切れず、機能安全が働かない場合があります。



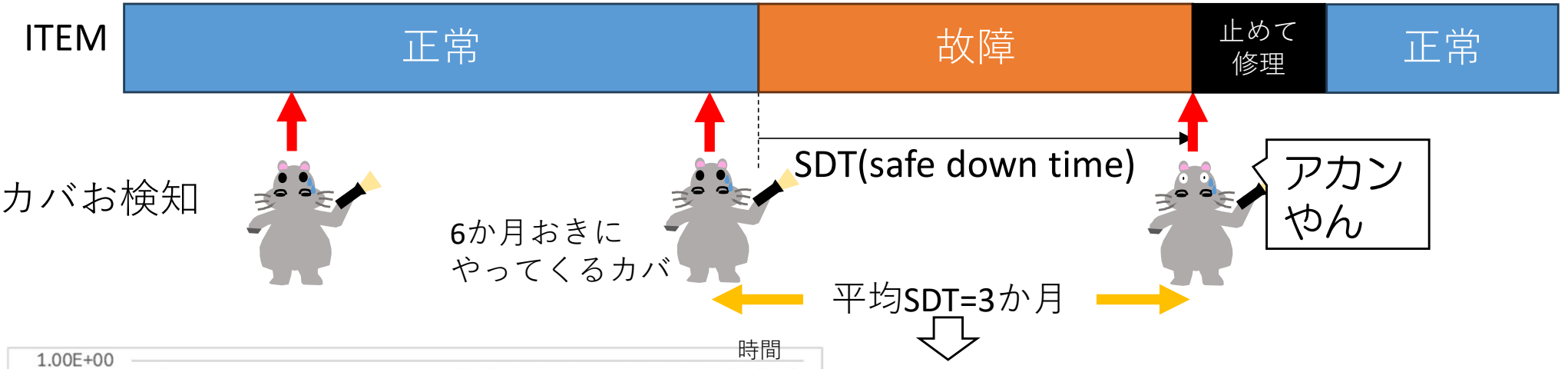


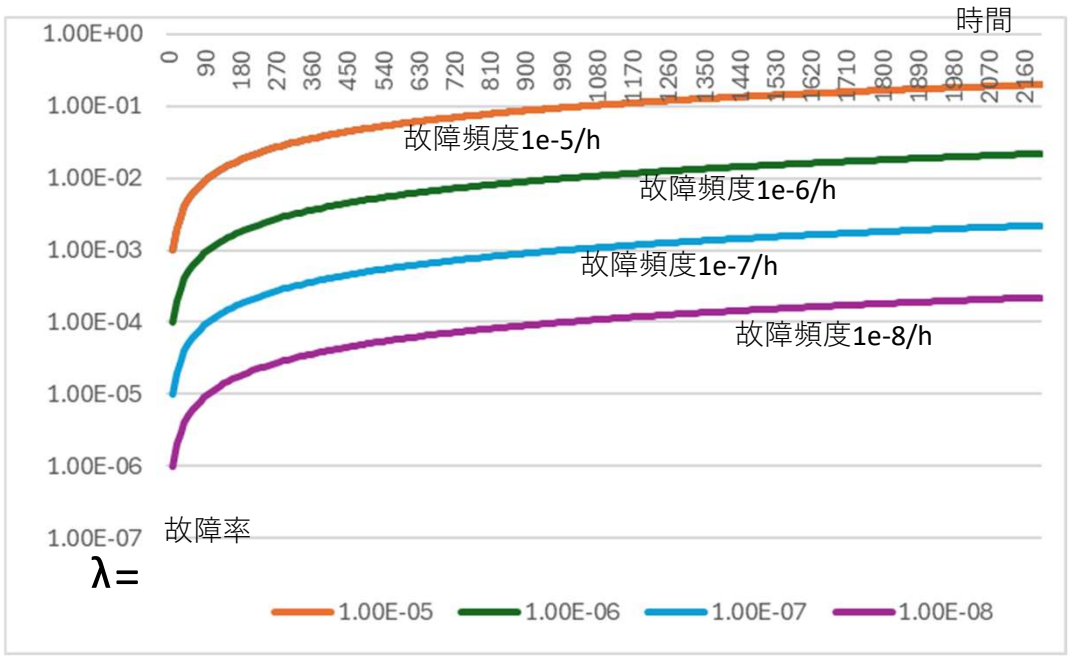
機能安全は、ツブれた時どうするかを決めておいて、その通り動いたら大丈夫という考え方や。どうなるか分からへんけど多分OKというのは、震える事象や。。

多重故障が起こる前に、止めるというのは状態遷移を複雑にしないためにも大事ですよね。

5. システムを安全側に遷移させる

SIL1,2では、止めるのは「カバ」でもいい！

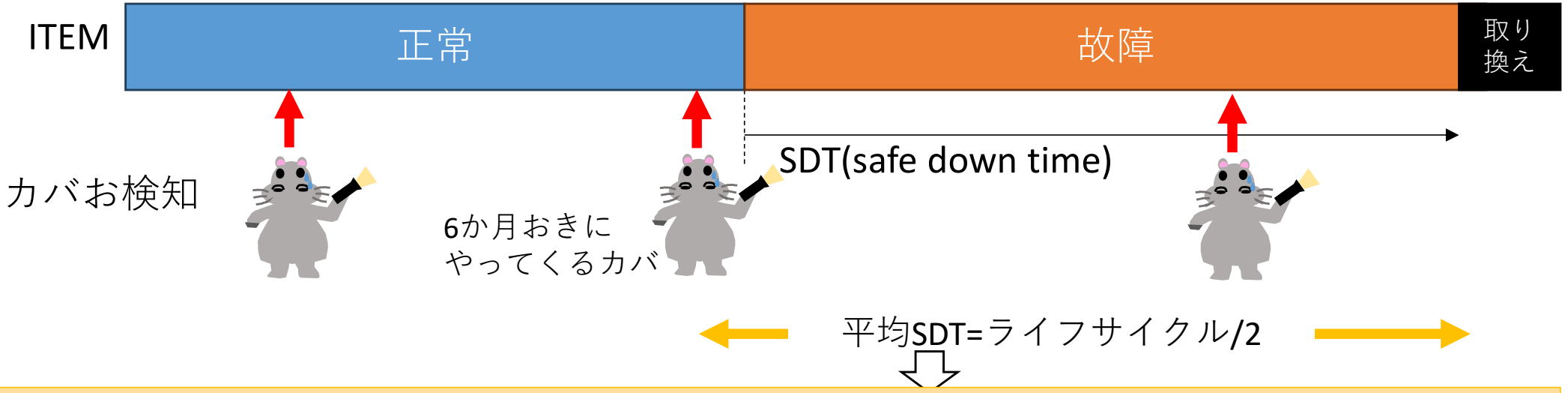




ITEMの故障頻度が一時間当たりλ、3か月を2200時間とすると、故障回数は2200×λ
指数分布に従うとすると、故障率は、$1-e^{-2200\lambda}$

5. システムを安全側に遷移させる

気づかない故障もある！

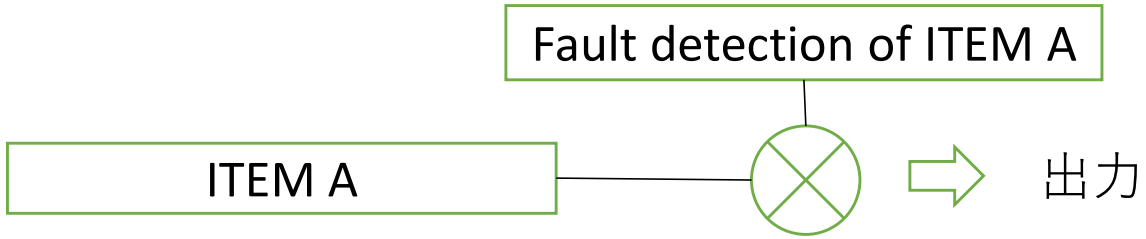


故障検知のカバレッジ率と安全は大きな相関関係にある！

Caution!危険! Caution!危険!
このため、IEC 61508においては、検知できない危険側故障はいかほどか、というところに配慮されている。IEC 62425についてはここは数学的なアプローチはなく（定性的な表現はあり）、出てくる数式は故障検知は100%できるものとして扱っていることに注意。（もし故障検知が100%ではないシステムの場合、配慮が必要。）

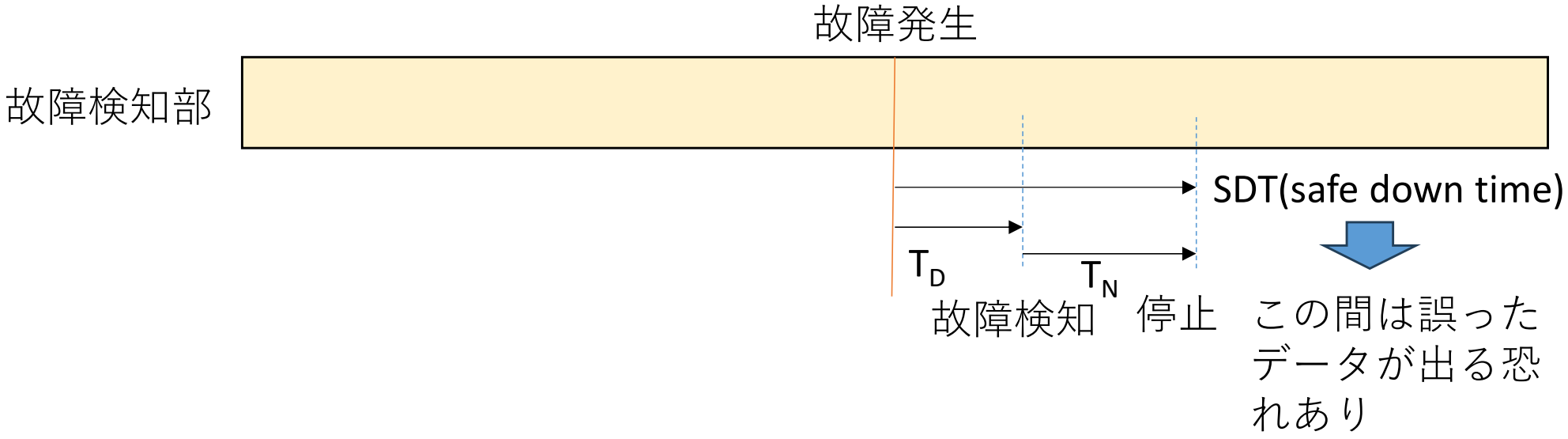
5. システムを安全側に遷移させる

Reactive fail safety : ITEM Aの出力を監視し、故障があれば出力を停止する。

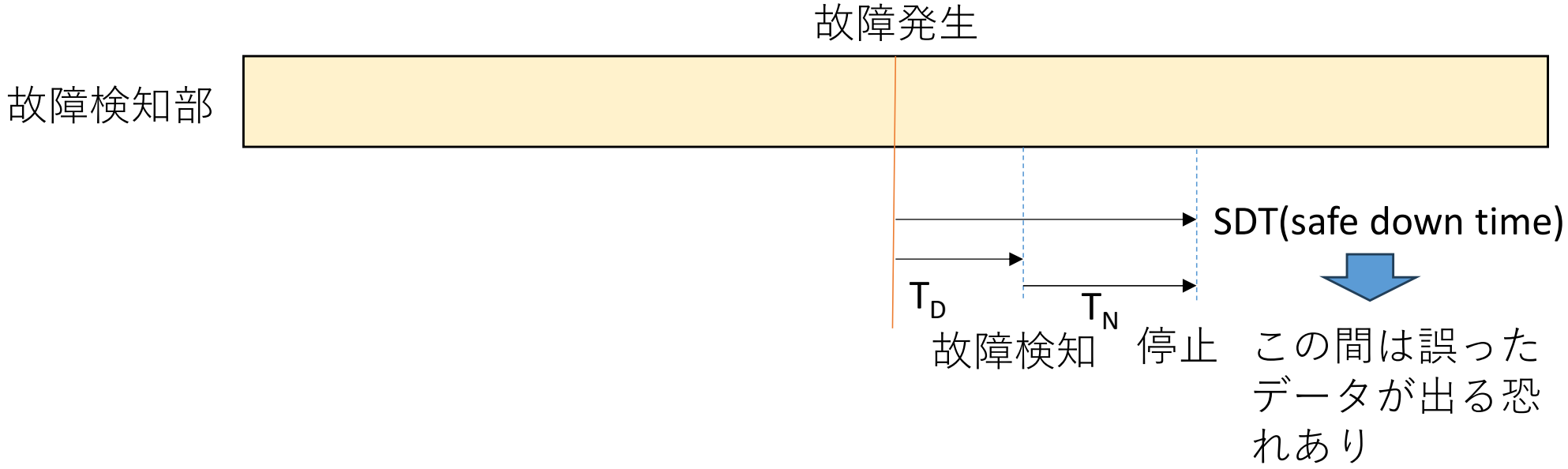


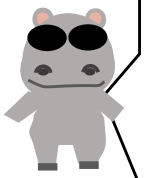
この場合、故障検知するまでは、誤ったデータが出る可能性があるんや。

ヤバいじゃない。間違い流出。確実にただじゃすまない未来しか見えないけど、こんな方式規格で認められているの。ヤバいじゃない！



5. システムを安全側に遷移させる



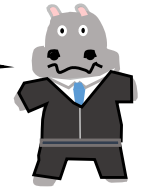


SDTの時間は誤ったデータが出るもんやとおもってやな、ソフトとか設計する必要があるな。またはハード屋！オマエらがこの時間短こうせいや！
あ、カバ興業は零細やから、オレが全部やることになるんか。。。
例えば：
継続した情報（リレーはXXms以上電源が入らないとONにならない。2回同じ情報が来ないとそのデータは使わない。とか）のみを採用するとか、ある程度の制御に余裕を持たせて、短時間の誤情報は事故につながらないとか。。。

6. 通信システムの場合は？

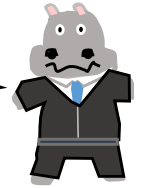
なんかこの頃、速い5Gとかいって、「KTTコドモ」には期待していたんだよ。
でも、全然速くなくて、むしろなんか詰まっちゃって遅くなってるよ。

またコドモか。おれはコドモに期待しとるから、投資したんや！どうしてくれる！



でも全くつながらないよりましだよね。。ベストエフォートだし。しょうがないよね。。

なにゆうてんねん！カバおは優しすぎねん。カバ興業はな、「確実に制御する。」ややってみて、アカンかったなんてゆうてみい、もう二度と出入り禁止になるで。



通信は、特に無線通信は、もとよりある程度のビットエラーや、伝送遅延、リソースの共用による輻輳は避けられないなかで、符号の処理、遅延時間を見越したアプリケーションソフトウェアなどで対応することが必要やで。

6. 通信システムの場合は？

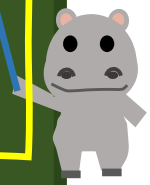
でも、5Gはなんか低遅延で伝送品質もいいって聞いたけどそれはどうなんや？

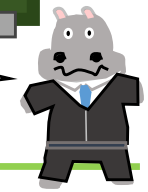
eMBB:（enhanced Mobile BroadBand）みんなが知ってる5G
伝送速度が速く、一般用途に向く。

mMTC:（massive Machine Type Communication）IoT機器を接続する。今のところ通信事業者からの提供はなし？

URLLC:（Ultra-Reliable and Low Latency Communications）32bytesのパケット送信時に1ms以下の無線区間遅延かつ99.999%以上の パケット受信成功確率の達成、遠隔制御や交通システム制御目的。今のところ通信事業者からの提供はなし？

この1システムで3つ同時には実現できず、選択。





ワシKTTコドモの株買い占めてURLLCやらせるで、新社名はカバコドモや！

7. まとめ

機能安全を実現する重要なポイントは、
「故障を見つける」
ことです。そして「安全な状態に持っていく」ことも重要です。

見つけて止めるまでの間、多重故障が起こるかもしれません。
多重故障は解析が厄介です。このため、多重故障が起こる前に、止めることが非常に大事になります。

止めるまでの間、誤ったデータが出てくる場合があります。それは制御方法で工夫することになります。

通信においても、ある一定の遅延量、誤りレートに抑える動きがあります。このようなものの活用が期待されます。