

確率で言える安全 仕組みで守る安全

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



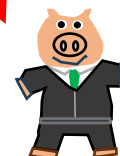
カバ鉄道 社長
品格の経営、根拠ある経営



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

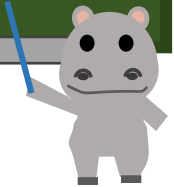


ブタ工業 社長
カバ興業を凌ぐ強い体質づくり

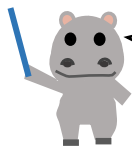
バチバチ

1. はじめに

- IEC 62425は、定量的及び定性的なアプローチで、機能安全を考える規格です。ともすれば、定性的に「この状態遷移は起こりえないであろう」ということで判断してしまうこともあります。少なくとも、定量的な考え方にに基づき、概略の計算を行い、桁が異なるため詳細な計算はしなくても大丈夫というところくらいは、考えておかなければいけません。
- 私は中学生の時、数学の成績は5段階評価で常に「3」でして、高校では、10段階評価で「4」やら「3」やらとっており追試ばかり、大学も電気工学科なのに、社会科学や法学の単位ばかり取っていて、数学を取っておらず落第しそうになりました。
まあもともと文系脳なので、2回目の大学は念願叶い文系に行きましたが。。
- そういう私ですので、数学が苦手な人にもわかるように説明したいと思いますので、よろしくお願いします。

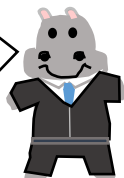


2. 故障ってどんなの。。



カバ社長！このスライド覚えてますか？

なんかおぼろげながら。。



なんかこれ、いろいろありますが、数学の匂いがしませんか？



そんなんワシ専門
ちゃうし、文系やし、
技術屋が知っとる
やろ。経営はヒラメ
キ💡で数字をい
じってナンボやない
で！粉飾はイカ
ン！



4-2-4 Operating Correctly (正しい動作?)

正しい動作って。正しい動作だったら、壊れてないやろ。これどういう意味や。

まあ普通そう考えるわな。でも、壊れた時に対応する機能が正しく動くと考えたらどうや。。

なんかおかしいぞ！

correct functional operation

入ってきたデータが
間違っとる

当該装置は壊れてい
るわけではないが異常

物理的に故障してい
ない装置で正しく動
作させればよい

ノイズでデータが化
けとる

当該装置は物理的に
故障しているわけ
ではないが、一時的に
一部の機能は喪失し
ている可能性あり

Effects of faults

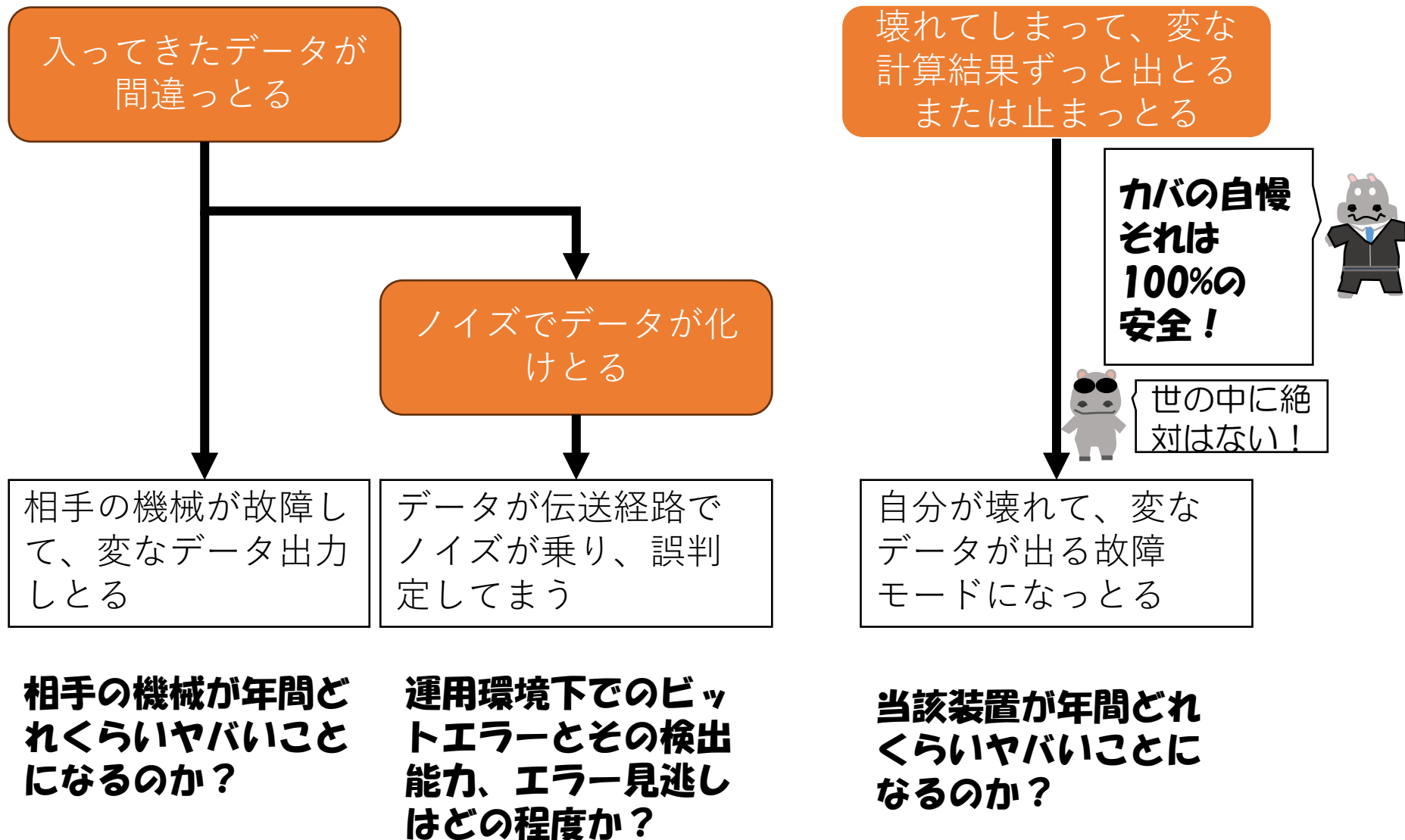
壊れてしまって、変な
計算結果ずっと出とる
または止まっとる

当該装置は物理的に
故障し、一部の機能
は喪失している

機能喪失していない部分で、安全動作を適切に実施すればよい



2. 故障ってどんなの。。



3. 確率の安全、そうでない安全。。

自分が壊れて、変なデータが出る故障モードになっとなる

いろいろな対策を組み合わせ、
上記のような故障が起こり、シ
ステムを止められない確からし
さが低いからよしとする。

組み合わせによる確率
論的アプローチ



世の中に絶対はない！

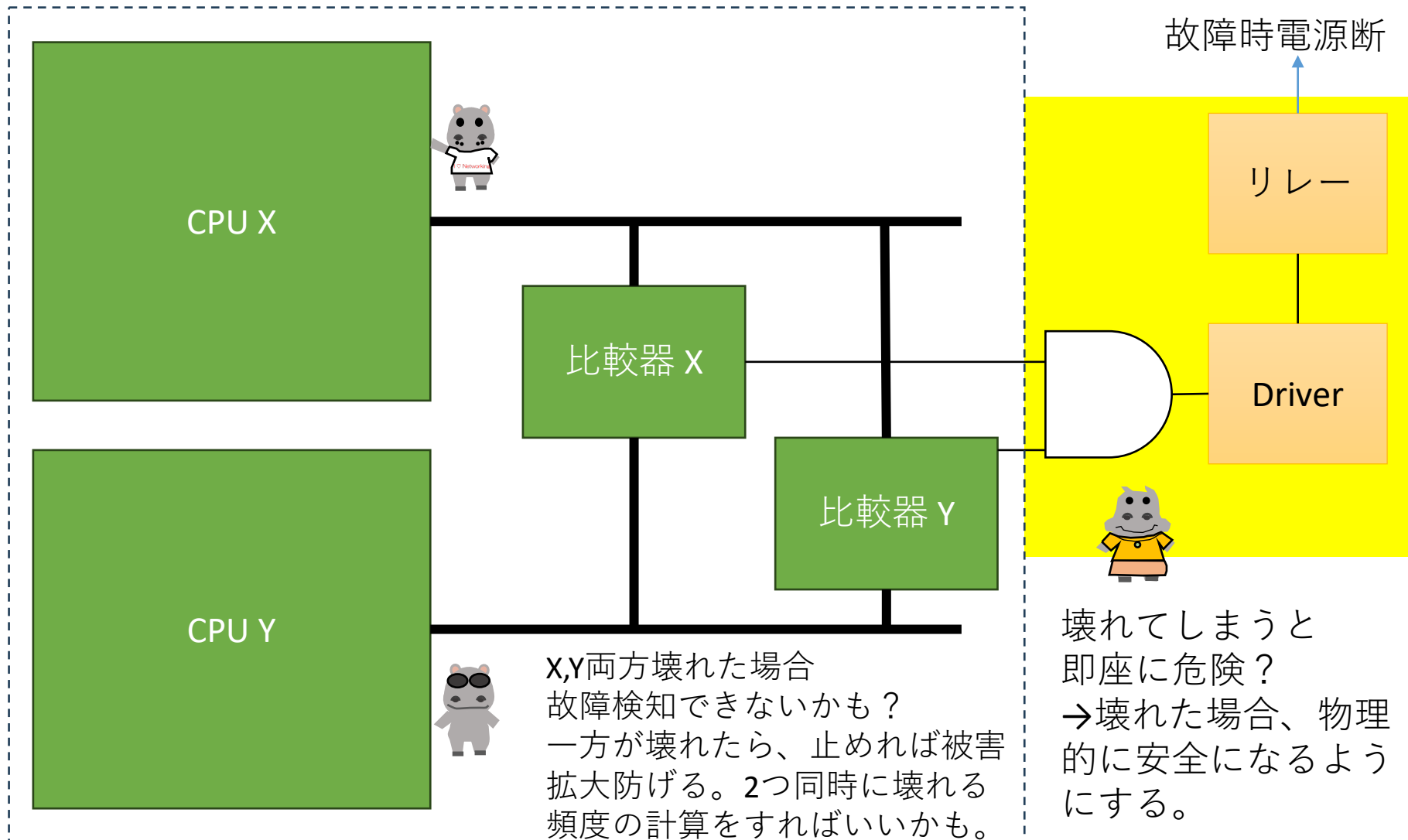
物理的にそのような危険側遷移
故障が起こらない仕組みで、シ
ステムを止める仕組みである。

本質的なFail-safe
(Inherent fail-safety)

カバの自慢 それは
100%の安全！

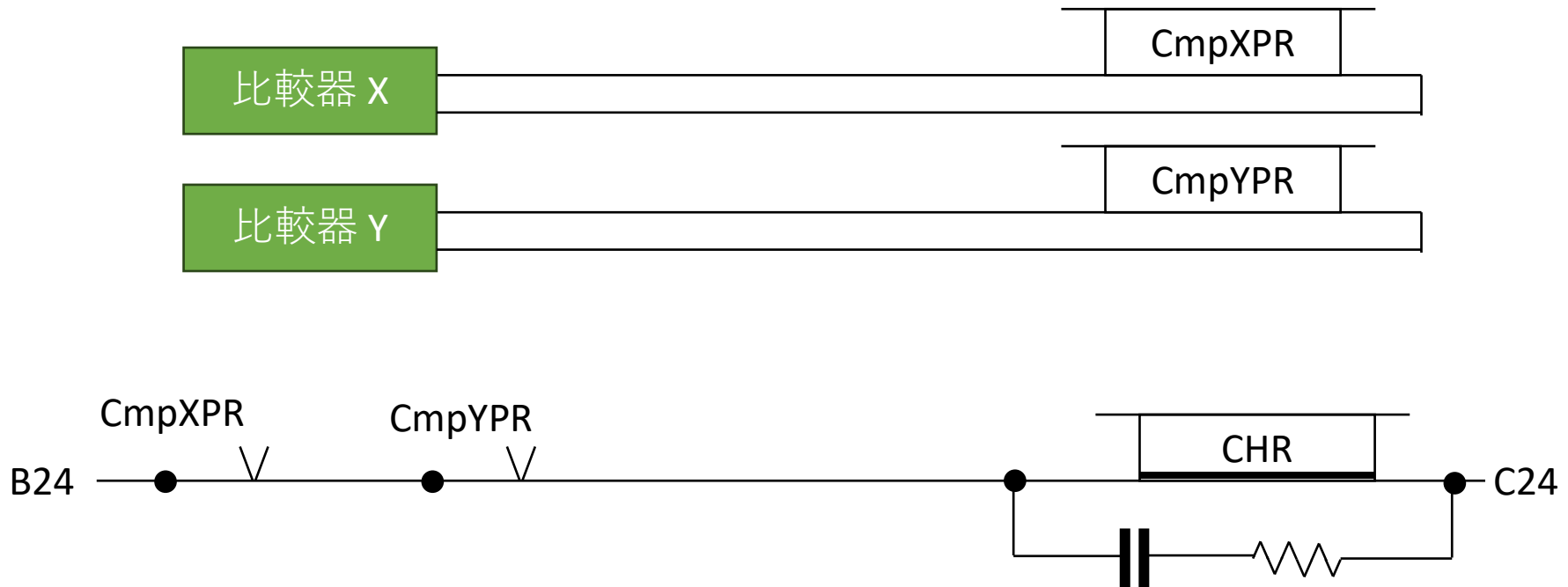


4. CPUボードの例



4. CPUボードの例

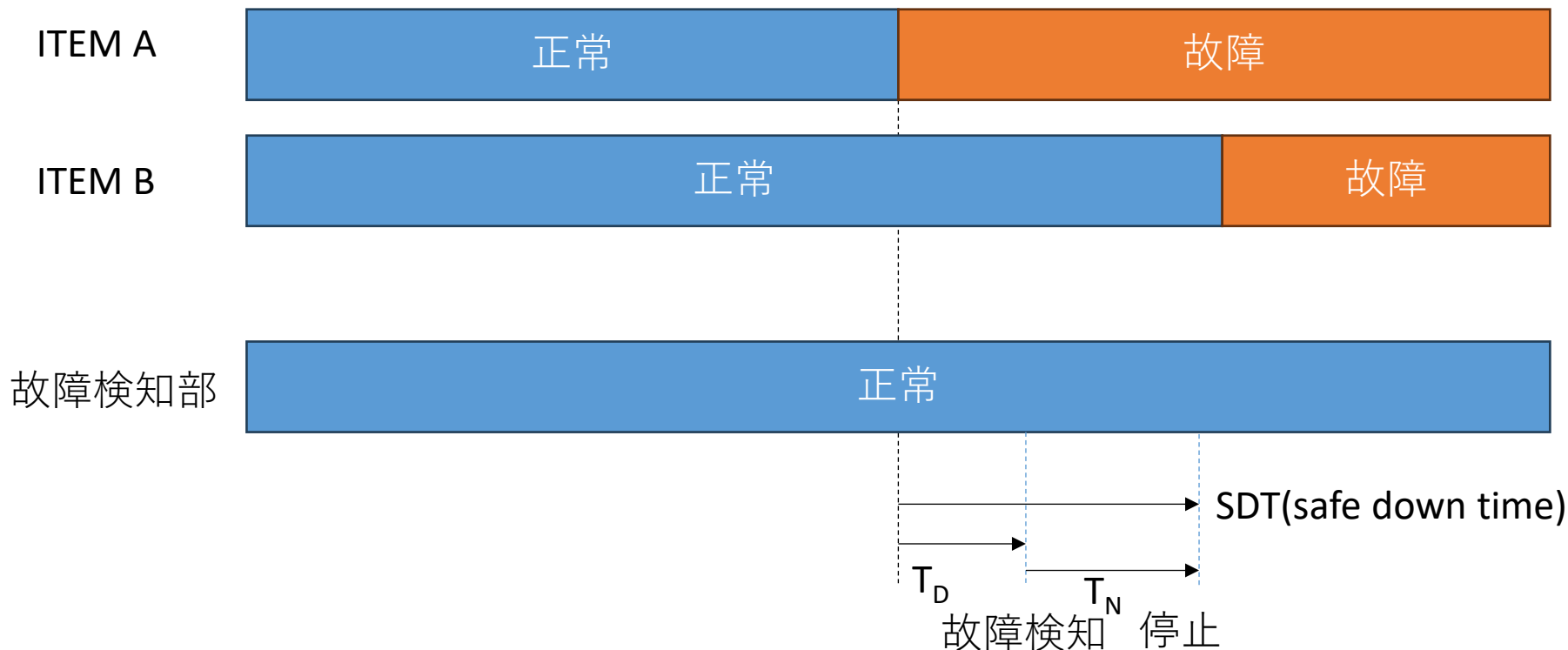
4. 1. 「物理的に安全」の例



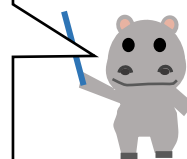
各リレーにおける故障モードの確認
コンデンサ、抵抗の故障モード確認

4. CPUボードの例

4. 2. 多重故障を防ぐ

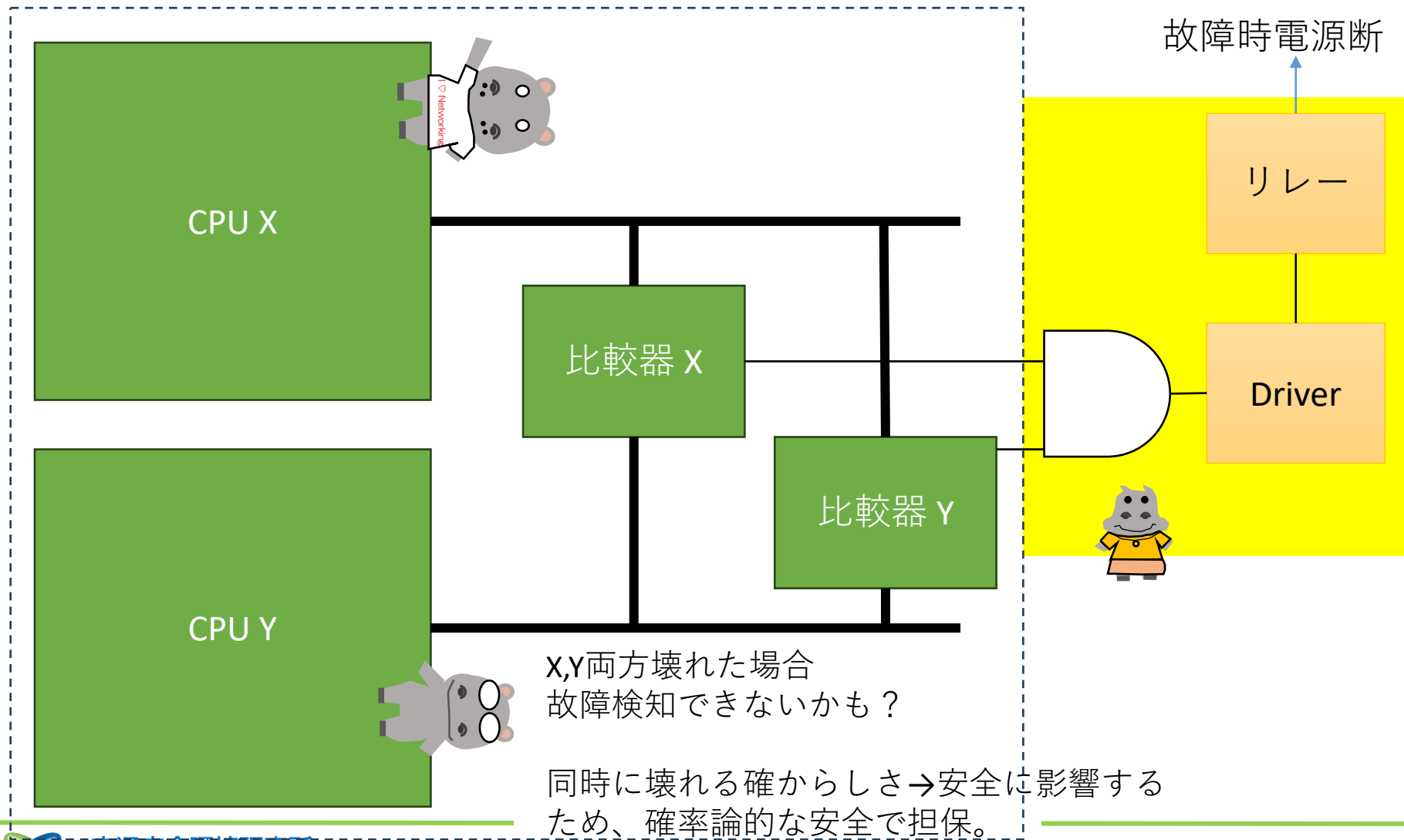


ITEM Aが故障した際に、ITEM Bの故障がSDTの間に起こると多重故障で、検知が難しくなることがあります。SDTに至るまでに、次のアイテムが壊れる確率を計算し、危険側故障頻度を求めます。



4. CPUボードの例

4. 3. 同時に壊れるとどうしようもない



4. CPUボードの例

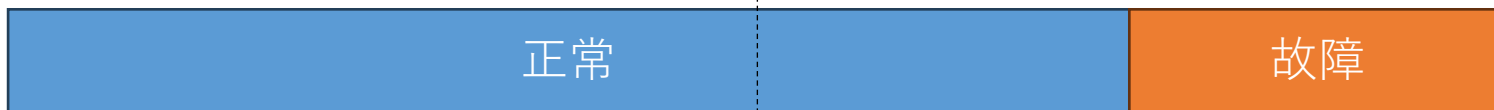
4. 4. とりあえず一人で走る方法も。。

故障修理せずに放置する場合

ITEM A



ITEM B



Bに処理系切替動作継続

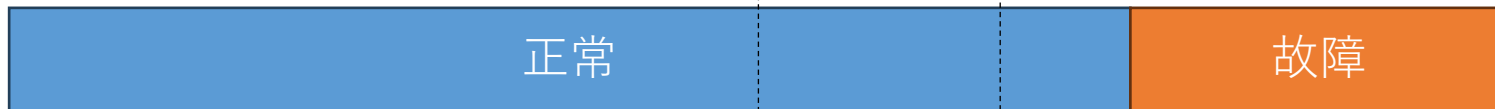


故障検知不能の場合、危険になる

ITEM A



ITEM B



Bに処理系切替動作継続



故障修理完了
Aに処理系切替

このように、故障した場合系を切り替えるような仕組みの場合、修繕を行うまでの時間と安全性が密接に絡みます。平均故障間隔の間に故障が起こると危険になる蓋然性があり、これも確率論的な安全です。

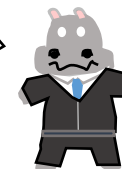


5. しょうがない、 確率論の話するか！

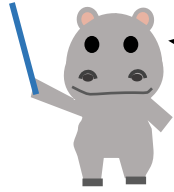


世の中に絶対はない！

**カバの自慢 それは
100%の安全！**

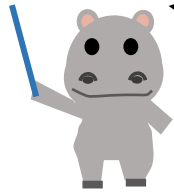


5. 1. 確率と言えばサイコロじゃないか！



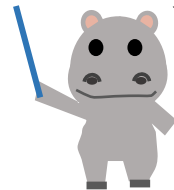
カバ社長！さいころがありますね。1の出る確率はどうですか？

チンチロリンか！カバ興業はグリーンな会社や！サイコロなんか絶対禁止や。で、そんなもん1/6にきまっとるやろうが？



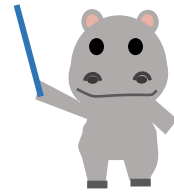
では、1.0から6.9まで、0.1刻みでランダムに出てくる謎ボックスがあるとしましょう。1の位が1になる確率はどうでしょうか。

そなんんするか。と言いたいとこやけど、60通りのうち1.0から1.9までの10通りがあてはまるから1/6にきまっとるやないか。



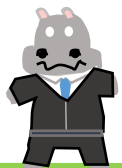
では、1.0から6.99まで、0.01刻みでランダムに出てくる謎ボックスがあるとしましょう。1の位が1になる確率も同じですよ。

もうお前の言いたいことは想像ついとんねん。ドンドンどんどんどんどん細かくしていってもおんなじやと言いたいんやろう。



ということで、どんどん細かくしていったら、任意の値の任意の半径内に必ず値が存在するということになり、それを連続と。。。大学一年で習うはずですが。イプシロンデルタっていう。。。

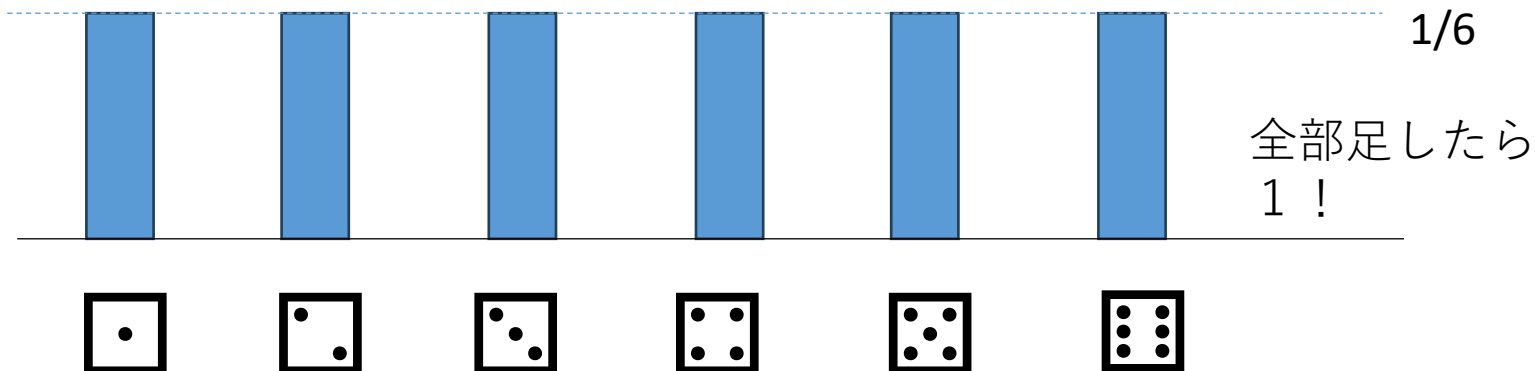
ワシは文系やそなんん知らん。聞いたことない。



5. 2. 離散的な確率と確率密度



サイコロは、1から6までの値が均等に出るモンと仮定しよう。ということは、1,2,3,4,5,6の出目の出る確率を足せば1になるはずや。1から6まで均等に出るから、それぞれの出目の確率は6で割って1/6や。



1以上7未満の実数がランダムに出るボックスがあるとする。1以上7未満の整数が出る確率はもちろん1や。指定された範囲の数がでる確率を面積で表したのが下の図や。



1以上3未満が出る確率は1/3のような気がするわ。確かに面積が1/3になっとるわ。



5. 2. なんで確率が密度なんや

1以上7未満の整数がランダムに出るボックスがあるとする。出た数の1万倍がもらえるとすると、5が出る確率はどうやという質問はどうや。

そいゃあ、おまえさん、50000円になることもあるだろうさ。よくテレビでもやっとなるわな。食事の値段当てたらゴチになりますってやつやで。

ナンボカネくれるねん。ってというのは、ピタリ賞もあるやろうけど、実数がランダムに出るピタリ賞はどうや。

そいゃあ、おまえさん、小数点あるから結構難しいわな。でも0ではないんやないか。。

でもそんなうまくいくか？ピタリ賞やで。小数点以下無限に桁があるで。。それって0に極限するんやないか。0とみなしてもいいと。。。

じゃあ聞くけどな、5を引く確率は0、5.001を引く確率も0、じゃあ全部足しても0で全部空くじイカサマちゃうんか！

いや社長待て。5以上5.001未満を引く可能性と言えは、それは0ではないぞ。ピンポイントはムリでも、ある範囲に入る実数は確実に存在する。だから連続値の場合は、ある範囲における確率の議論をしないと意味がない。範囲になるので、密度×範囲で確率が計算できるよう、確率密度関数を定義しておくんや。

5. 2. 離散的な確率と確率密度

$$1 = \sum_{k=1}^n p_k$$

要素がnこあって、k番目の要素の確率を p_k とした場合、それらを全部足すと100%、すなわち1になるわけですね。

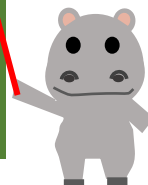


また技術屋は式でごまかそうとする。なんでこんな説明するねん。
現れるサイコロの出目を全部集めたら100%になるってゆうてるだけやん。
これやから技術屋のこういうやり方キライやねん。



$$1 = \int_a^b p(x) dx$$

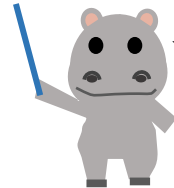
連続の場合、とりうる区間aからbの確率の密度を積分したら、100%になるわけですね。ある区間に入る確率はその区間の積分をしたらいいわけです。



なんでそんな説明するねん。密度ってある決まった大きさ(面積や体積)の中にどれ位入ってるかってことやんか。
例えば1つのオリに3匹のカバがいる。密や密。密密や！オリに3匹ずついるんや。
密密オリにいる3匹に、オリ数掛けたらカバの数がでるやろ。オリ3つなら9匹や。
じゃ、「確率密度」の場合、密度に範囲掛けたらエエだけやん。それで確率なるやん。
おまえ、それでもコンサルか！ワシの方がましな説明できるで！ワシ文系や文系！

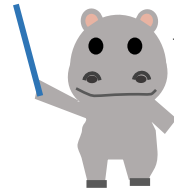
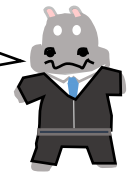


5. 3. 頻度と確率



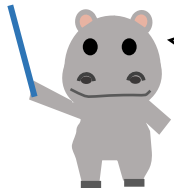
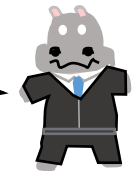
カバ社長！さいころがありますね。3つのサイコロのゾロ目の出る確率はどうですか？

チンチロリンは禁止やゆうとるやろ。1/36やけどな。1万円で36万円か。お、結構エエな。いやいやそんなんやるヤツ辞めてもらうで。。



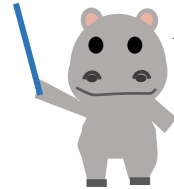
では、一年で1回コワれるカバ興業の製品があります。一年でコワれる確率はどうでしょうか。

お前バカにしとるんか。うちの装置は20年は持つぞ。でも一年に一回か、100パーセントかな。



では、半年でコワれる確率はどうでしょうか。

50パーか。。



では、2年でコワれる確率はどうでしょうか。

200パー！なわけないか。。



5. 3. 頻度と確率

なんか変ですよ。200パー壊れるって。。

でもなんか、20000%やらないといった人いたよな。これと比べたら1/100やで。

それは言葉のあやでしょう。。

判定期間1年

4台導入

故障修理

故障率 25%
故障頻度 0.25台/年

4台導入

故障修理

故障修理

故障修理

故障修理

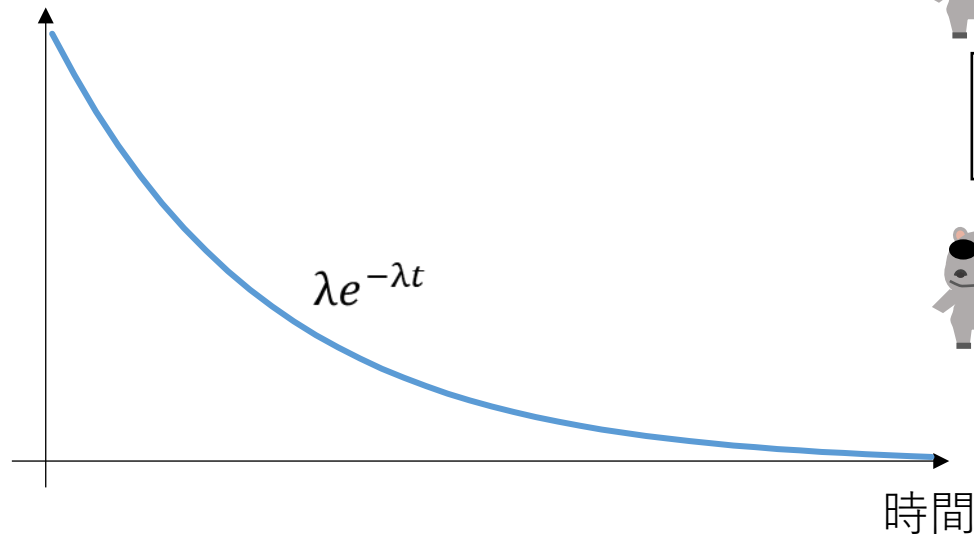
故障率 50%
故障頻度 1台/年

故障しないという実力をどちらが適切に表しているでしょうか？

ウチがフタさんトコに負けるはずがないわ。

5. 4. 確率モデル

壊れる確率密度



コワれる数って、だんだん下がるわな。

え、時間がたつとコワれる可能性が高まるんじゃないの？

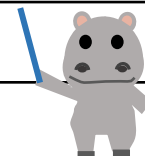


それはそうや。でもそれは累積故障確率や。コワれてしもたら数が減るやろ。だから、生き残っとるヤツが減ってくるから、確率密度関数は、下がってくるんや。



イメージ的に、なんかこんなふうに故障の確率ってあらわされるような気がせーへんか？

$\lambda e^{-\lambda t}$ がこの曲線になるんですよ。

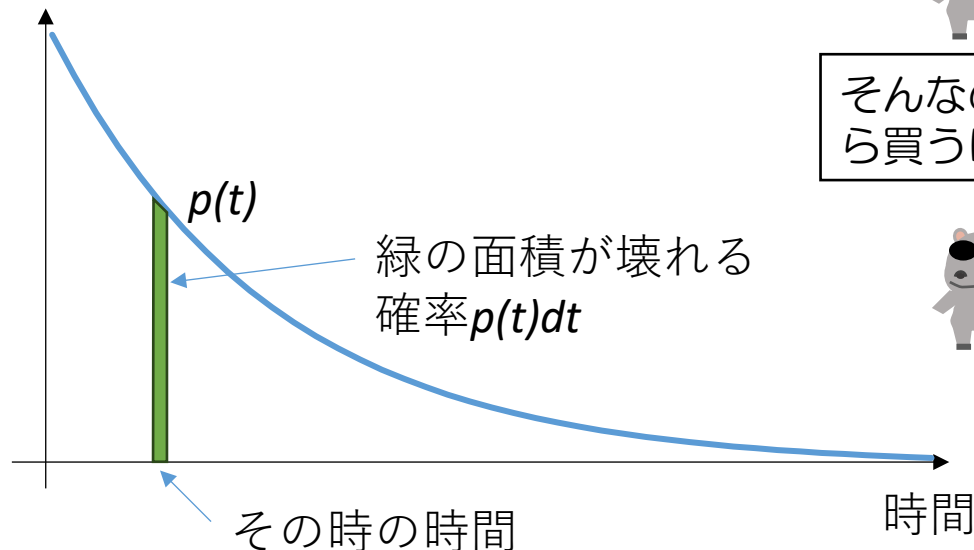


また数式か。お前らコンサルはそうやってオレらをいじめる。。



確率モデルと平均 (参考)

壊れる確率密度



じゃあこのグラフの場合、どのくらいの時間で平均的に壊れるんやろうか。

そんなの知らないよ。確率というなら宝くじなら買うけどね。1等5000万円。夢があるよね。



じゃあ一等5000万円は、100万分の1出るとしたら、期待できるのは50円やな。二等100万円は10万分の1で10円。三等500円は10分の一で50円。合わせて期待できるのは、110円や。カバおは500円出して110円をこうてるわけや。とんだ負け戦やで。。

そんなの知らないよ。夢を買っているんだよ。現実は関係ないよ。でも、確率にその時のもらえる値を掛けて、全部足すと期待値になるんだね。まあそうなんだろうね。



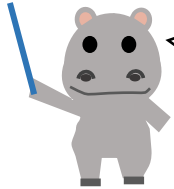
そういうことや。このグラフでは、壊れる確率に時間をかけて、全部のエリア足し合わせると、壊れるまでの時間の期待値、すなわち平均故障間隔になるんや。

$$\int_0^{\infty} t \lambda e^{-\lambda t} dt = [-te^{-\lambda t}]_0^{\infty} + \int_0^{\infty} \lambda e^{-\lambda t} dt = 0 - \left[\frac{1}{\lambda} e^{-\lambda t} \right]_0^{\infty} = \frac{1}{\lambda}$$



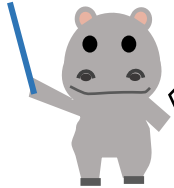
平均故障間隔の逆数は、時間当たりの故障回数になるので、 λ は故障頻度と言えます。

5. 5. 頻度と確率の変換



故障する頻度はλらしいですね。こういうモデルの場合。これを指数分布と言います。

要は何でもエエけど、お客さんの壊れるなという要求は大事や。



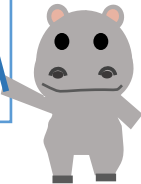
故障のモデルについて、IEC 62425は、一般的には指数分布に沿うものとして扱います。

さっき確率密度関数 $\lambda e^{-\lambda t}$

と言いましたね。 a から b までの発生確率は $\int_a^b p(t)dt$ で、 $p(t)$ を $\lambda e^{-\lambda t}$ としたものが指数分布の確率になります。 λ は頻度です。

$$\int_0^{\infty} \lambda e^{-\lambda t} dt = [-e^{-\lambda t}]_0^{\infty} = 1$$

確率密度関数を0～∞まで全部足したら1！



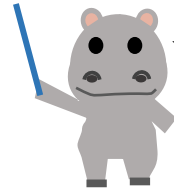
故障頻度 λ の時、時間 a までに故障が発生する確率

$$P(a) = \int_0^a \lambda e^{-\lambda t} dt = 1 - e^{-\lambda a}$$

時間 a までの故障確率から頻度を導出

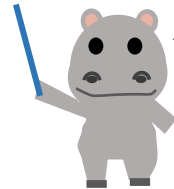
$$\lambda = -\frac{\log_e(1-P(a))}{a}$$

5. 5. 頻度と確率の変換



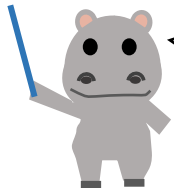
カバ社長！さいころがありますね。1の出る確率はどうですか？

チンチロリンか！そんなもん1/6にきまっとるやろうが？さっきゆうたやろ。



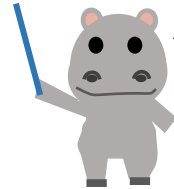
では、一年で1回コワれるカバ興業の製品があります。一年でコワれる確率はどうでしょうか。

ハッキングカバによると、 $1 - \exp(-1 \times 1) = 0.63$ らしい。



では、半年でコワれる確率はどうでしょうか。

ハッキングカバによると、 $1 - \exp(-0.5 \times 1) = 0.39$ らしい。

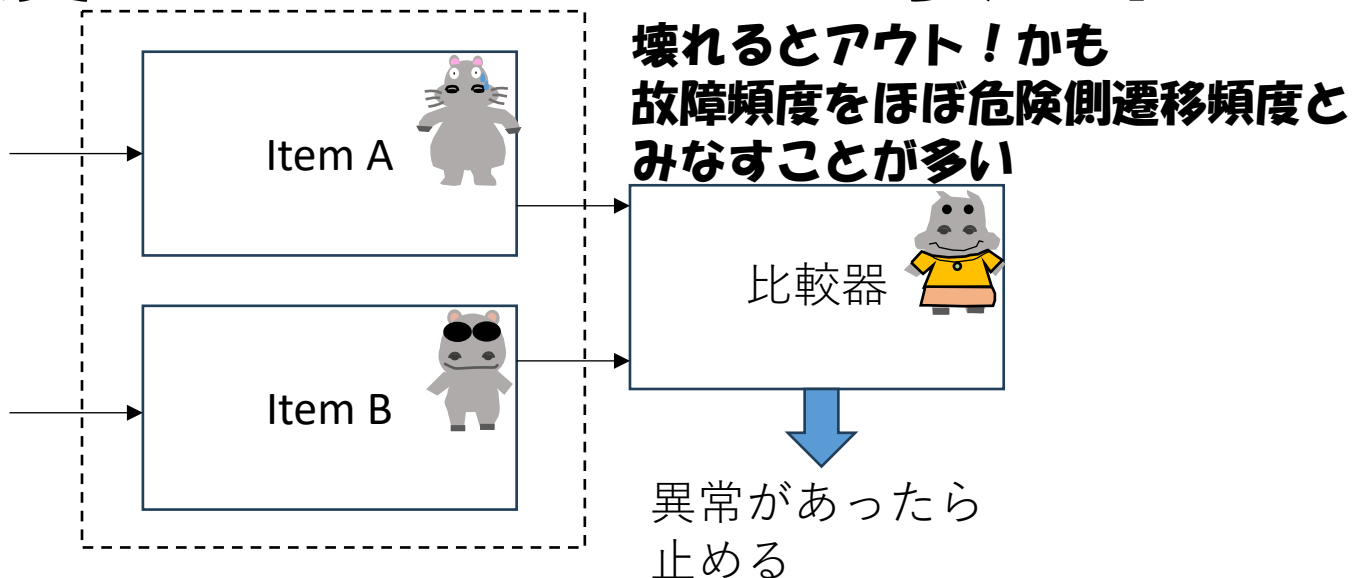


では、2年でコワれる確率はどうでしょうか。

0.86くらいらしいわ。

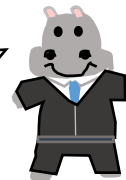


故障頻度と2002システムの安全性



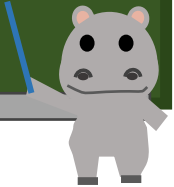
両方壊れないと危険側に遷移しない
→システムを止める前にA,B両方壊れる頻度が危険側遷移頻度となる。

まあ両方壊れることはめったなことではないやろう。
要は、Aが壊れて、止める前にBも壊れてしまったら、比べようがないから、それを防がなあかん。
比較器は、これ、壊れたらえらいこっちゃ。カバ実がなんでもOKにしてしまうと最悪や。。。こいつがしっかりすることは決定的に大事やないか！



6. まとめ

- システムは故障することを前提に構築するのが機能安全ですが、安全側に遷移することがほぼ確実、だれが見ても大丈夫という方法と、確率的なアプローチで、まあ大丈夫受け入れ可能でしょうという方法があります。
- 2つのアイテムを組み合わせて、同時に故障することは非常に少ないので大丈夫という考え方を取ることがあります。このような場合、片方のアイテムが故障した場合システムを速く停止し、安全側に遷移させることで危険側に遷移する頻度を下げます。
- また、2つのアイテムがあり、故障時系切り替えをしてミッションを継続するようなシステムの場合、平均故障間隔と故障頻度の関係が重要になってきます。このようなシステムの場合、メンテナンスと安全性の関係が深くなります。
- 確率、頻度は少し違う概念です。区別しておくとう理解が深まります。



多重故障を防ぐ(参考)

ITEM A



ITEM B



→ SDT(safe down time)

○ITEM Aが故障した際、SDTの時間内に、ITEM Bが故障する頻度またその逆の合計が、その装置に実装されている機能のTFFRを下回れば、比較器の故障を無視すればOKとなります。

このため、SDTの間に故障する頻度を計算します。

ITEM Bの一時間当たりの危険側故障頻度を FR_B 、ITEM Aの危険側故障頻度を FR_A とします。

SDTの時間内にITEM Bが危険側故障する確率は、

$$P_{fb}(SDT) = \int_0^{SDT} FR_B e^{-FR_B t} dt = 1 - e^{-FR_B SDT} \text{ となります。}$$

これは、マクローリン級数展開 $e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} \dots$ を近似で使用すると、

$$P_{fb}(SDT) \approx FR_B SDT \text{ となります。}(FR_B SDT \ll 1 \text{ の場合})$$

この時、ITEM Aが危険側に壊れる頻度と、この $P_{fb}(SDT)$ を掛けると、Aが危険側に壊れ、次にBが危険側に壊れる一時間当たりの頻度 FFR_A を導出することができます。

すなわち、

$FFR_A(SDT_A) = FR_A \cdot FR_B \cdot SDT_A$ となります。その逆、Bが危険側に壊れ、次にAが危険側に壊れる一時間当たりの頻度

FFR_B は $FFR_B(SDT_B) = FR_A \cdot FR_B \cdot SDT_B$ となり、この2つの合計

$FFR = FR_A \cdot FR_B \cdot (SDT_A + SDT_B)$ が、ITEMに実装する機能のTFFRを下回れば、比較器に関する事項以外は満たすことになります。