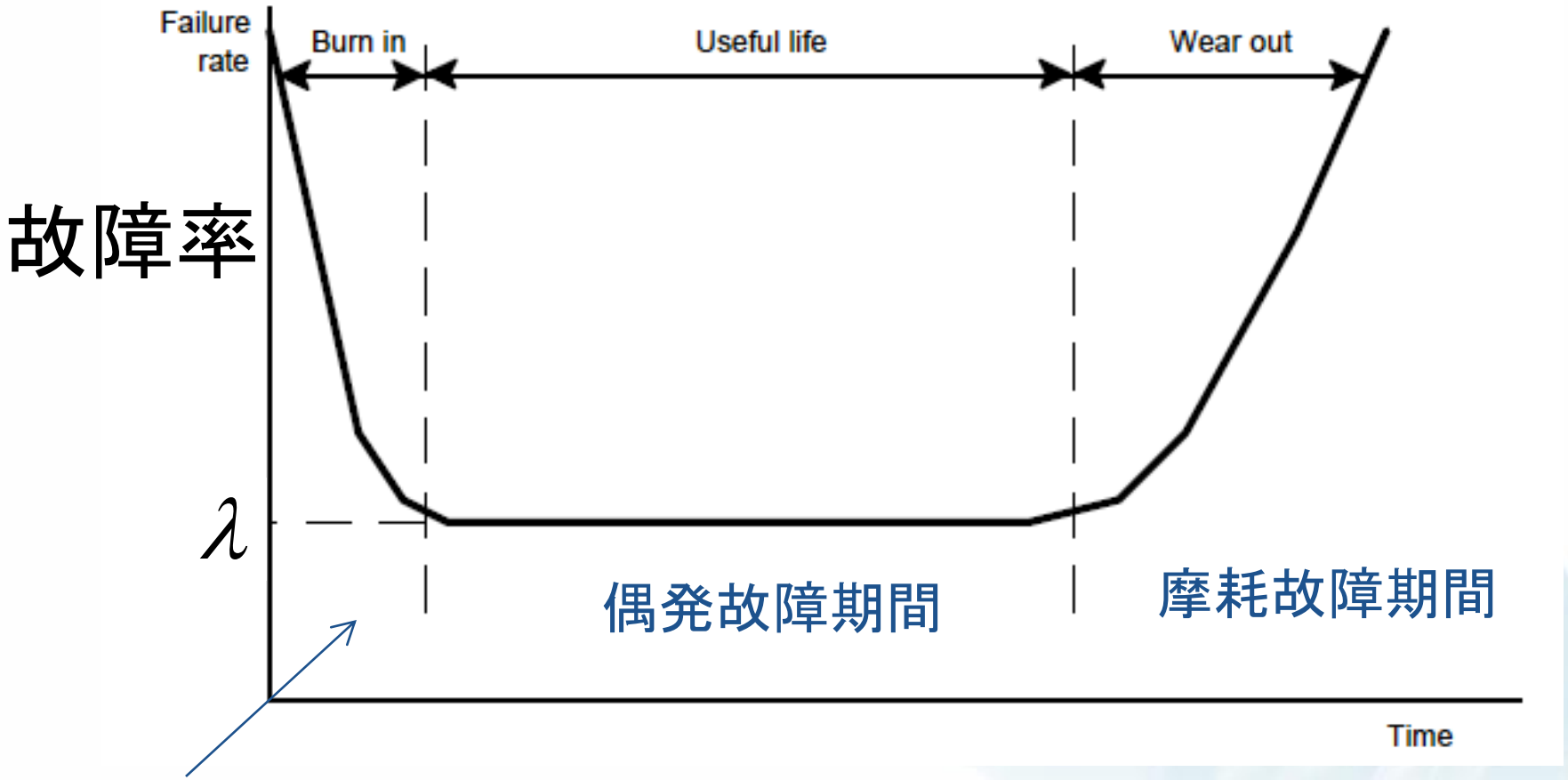
安全信頼性工学

Rafael Batres
豊橋技術科学大学

信頼性の定義

- 信頼性 （JIS Z 8115：信頼性用語）
  - 信頼できる度合(%)
  - "信頼度(信頼性)とはアイテムが与えられた条件で、規定の期間中、要求された機能を果たす確率(性質)である。" (JIS　Z8115-1981)
  - アイテム
    - 部品（part）
    - 構成品（component）
    - 装置（device）
    - 機器（equipment）
    - 機能的ユニット（functional unit）

バスタブ曲線


Failure rate
Burn in
Useful life
Wear out
故障率
λ
偶発故障期間
摩耗故障期間
Time
初期故障期間

信頼性（Reliability）

アイテムが与えられた条件で規定の期間中、要求された機能を果たすことができる性質。

故障確率

$$F(t) = 1 - e^{-\lambda t}$$

$$\lambda > 0$$

故障率

信頼性

λ：

$$R(t) = 1 - F(t) = e^{-\lambda t}$$

関連する概念

確立密度関数

$$f(t)=\begin{cases}\lambda e^{-\lambda t}, & t\geq 0\\ 0, & t<0\end{cases}$$

分布関数

$$F(t)=\int_0^t f(t)=\int_0^t \lambda e^{-\lambda t}=1-e^{\lambda t}$$

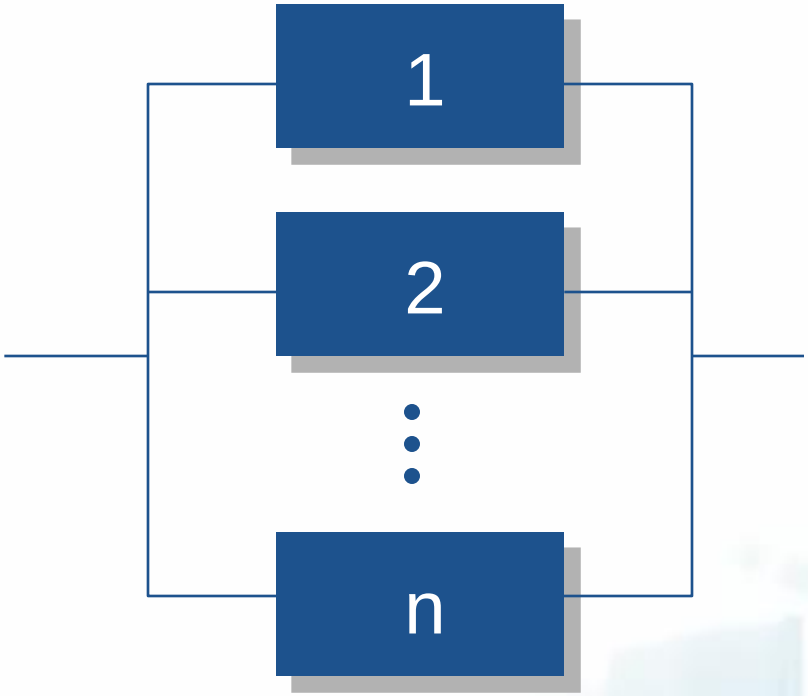
平均故障間隔（Mean time between failures）

$$MTBF=\int_0^\infty tf(t)=t\lambda e^{-\lambda t}=\frac{1}{\lambda}$$

Series Systems

$$F_S = 1 - (1 - F_1)(1 - F_2)\ldots(1 - F_n)$$

Parallel Systems



$$F_S = F_1 F_2 \ldots F_n$$

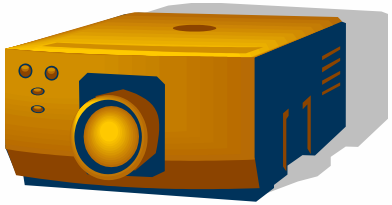
例：本授業の信頼性評価

- プロジェクターの故障率
  - 1ヶ月で1回故障する
- ノートパソコンの故障率
  - 10週間で2回故障する

1週間あたりの授業の故障確率を求めよ

プロジェクターの故障確率

- プロジェクターの故障率
  - 1ヶ月で1回故障する



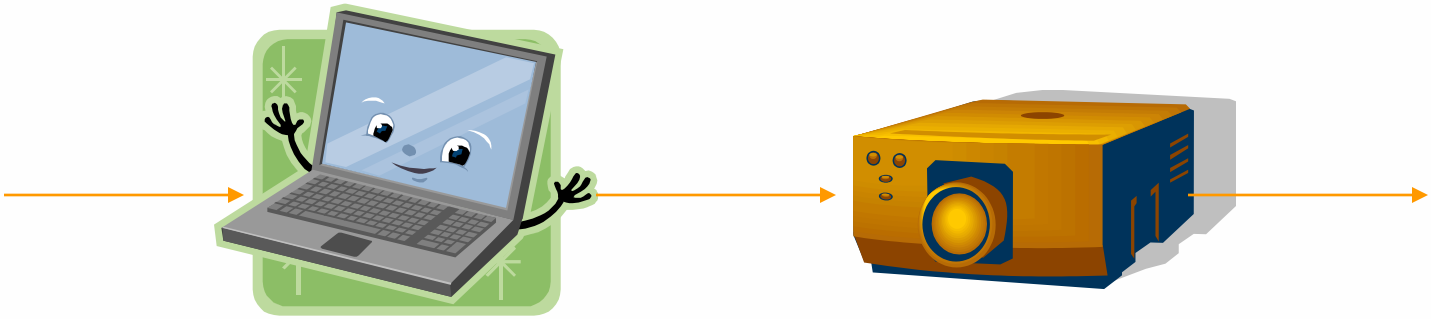
$$F(t) = 1 - e^{-\lambda t} = 1 - e^{-1/4} = 0.22$$

ノートパソコンの故障確率

- ノートパソコンの故障率
  - 10週間で2回故障する

$$F(t) = 1 - e^{-\lambda t} = 1 - e^{-2/10} = 1 - e^{-0.2} = 0.18$$

授業の故障確率，信頼性



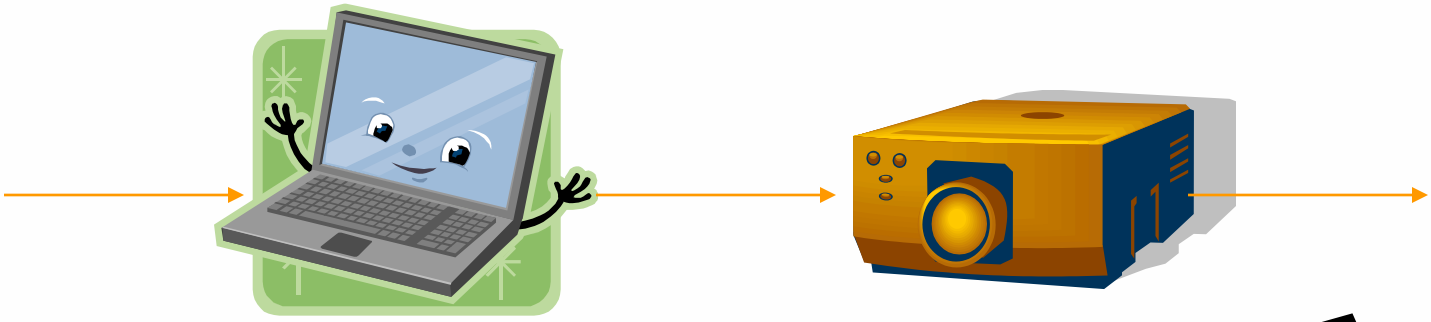
$$F_S = 1 - (1 - F_1)(1 - F_2)\ldots(1 - F_n)$$

$$F_S = 1 - (1 - 0.18)(1 - 0.22) = 0.36$$

$$P_S = R_S = 1 - 0.36 = 0.64$$

成功確立

授業の故障確率



0.18

0.22

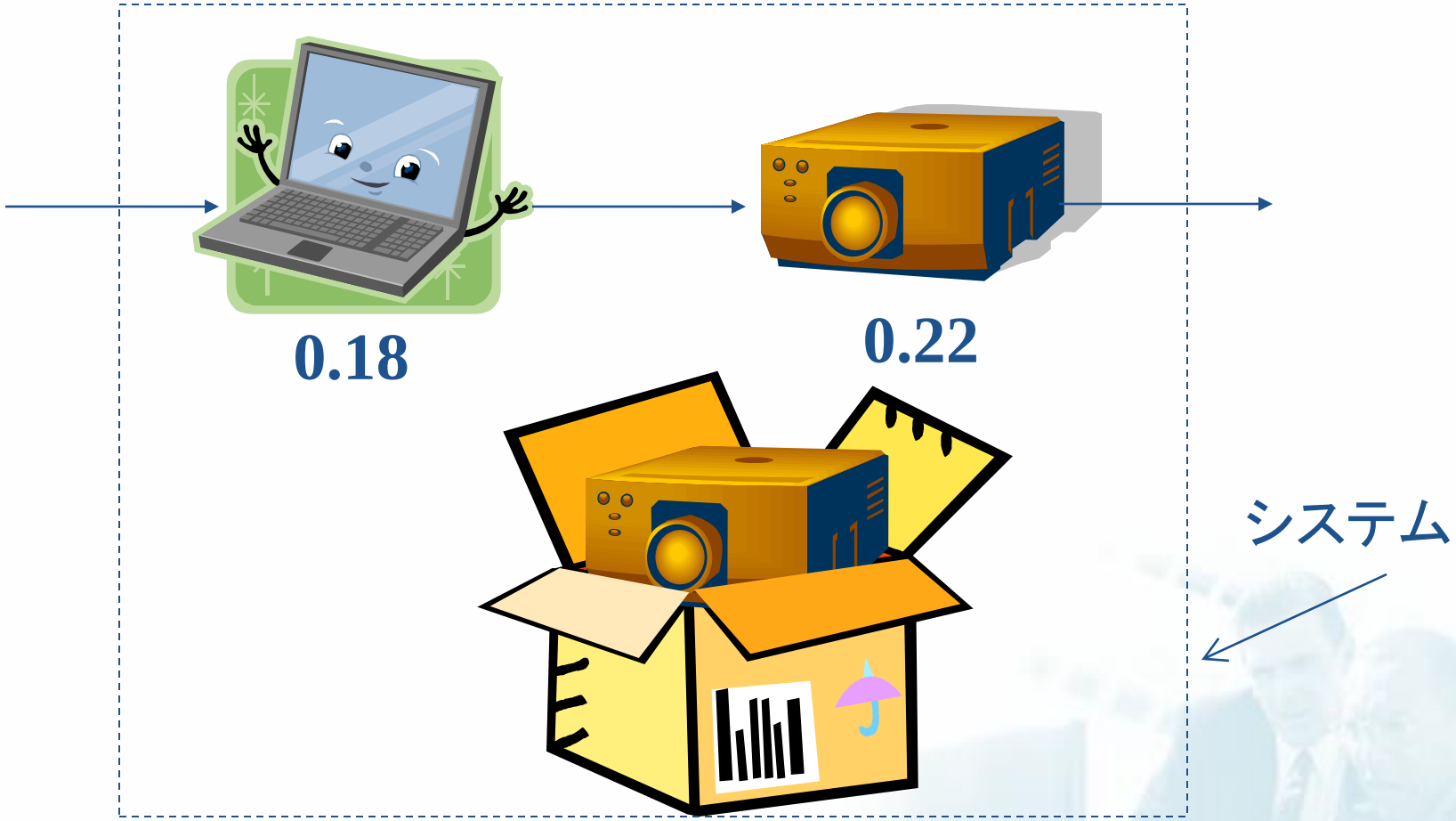
$F_S = ?$

システムの信頼性

P_s = (Aが故障しない場合のシステムの成功確立) * Aの信頼性 +
(Aが故障する場合のシステムの成功確立) * Aの故障確立

$P_s = 1 * R_A + 0 * F_A$

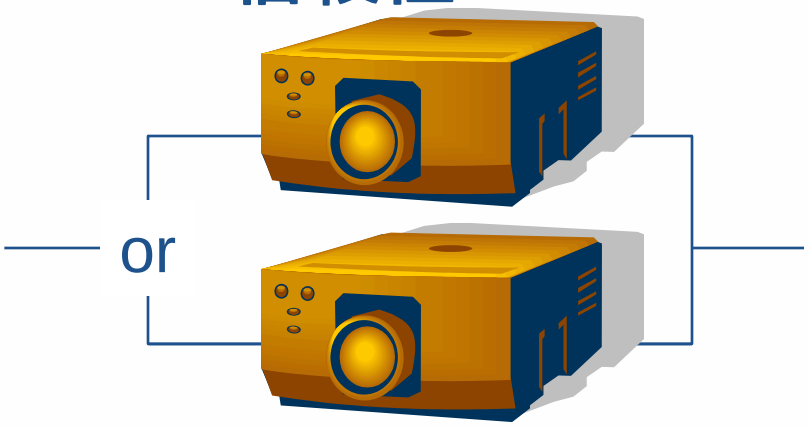
授業の故障確率



$F_S = ?$

プロジェクターの成功確立

信頼性 = 1 - 0.22 = 0.78

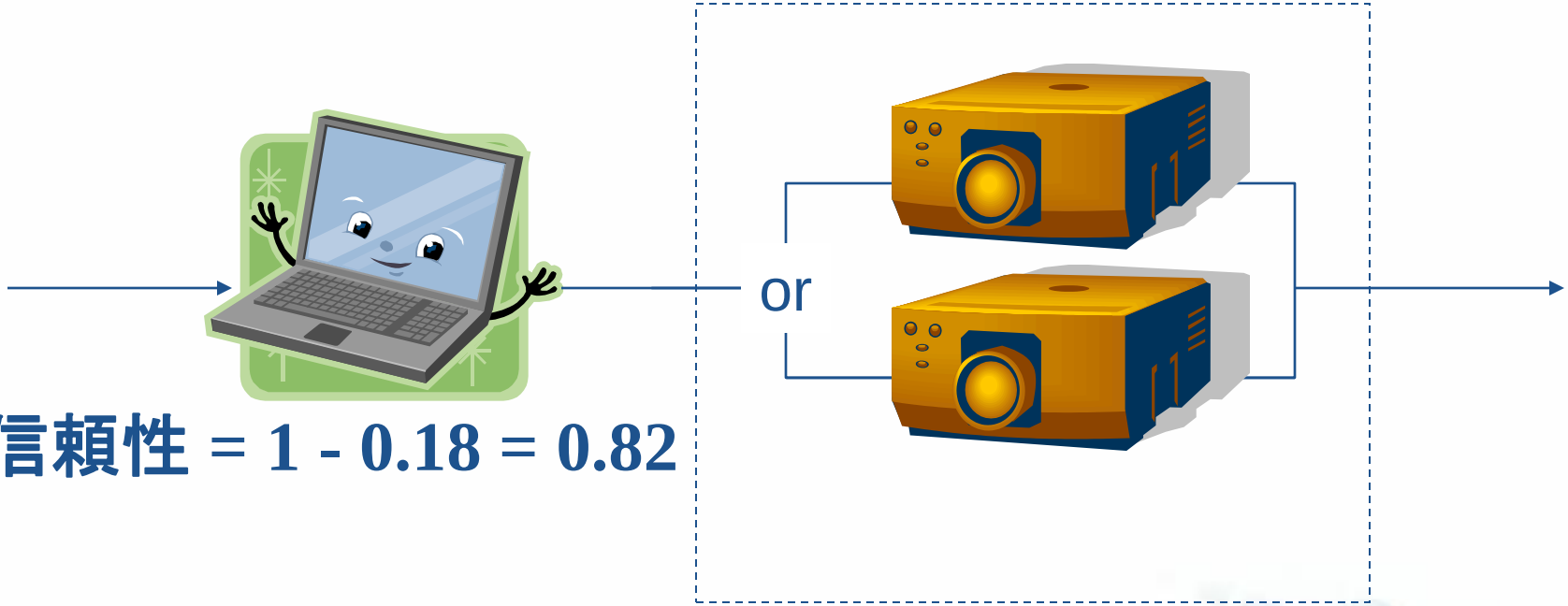


信頼性 = 1 - 0.22 = 0.78

$P_{s,\ proyectors}$ = (プロジェクターが故障しない場合のシステムの成功確立) *
プロジェクターの信頼性 +
(プロジェクターが故障する場合のシステムの成功確立) *
プロジェクターの故障確立

$P_{s,\ proyectors} = (1) * 0.78 + 0.78*(1 - 0.78) = 2*0.78 - (0.78)^2 = 0.96$

プロジェクターの成功確立



信頼性 = 1 - 0.18 = 0.82

信頼性 = 1 - 0.22 = 0.96

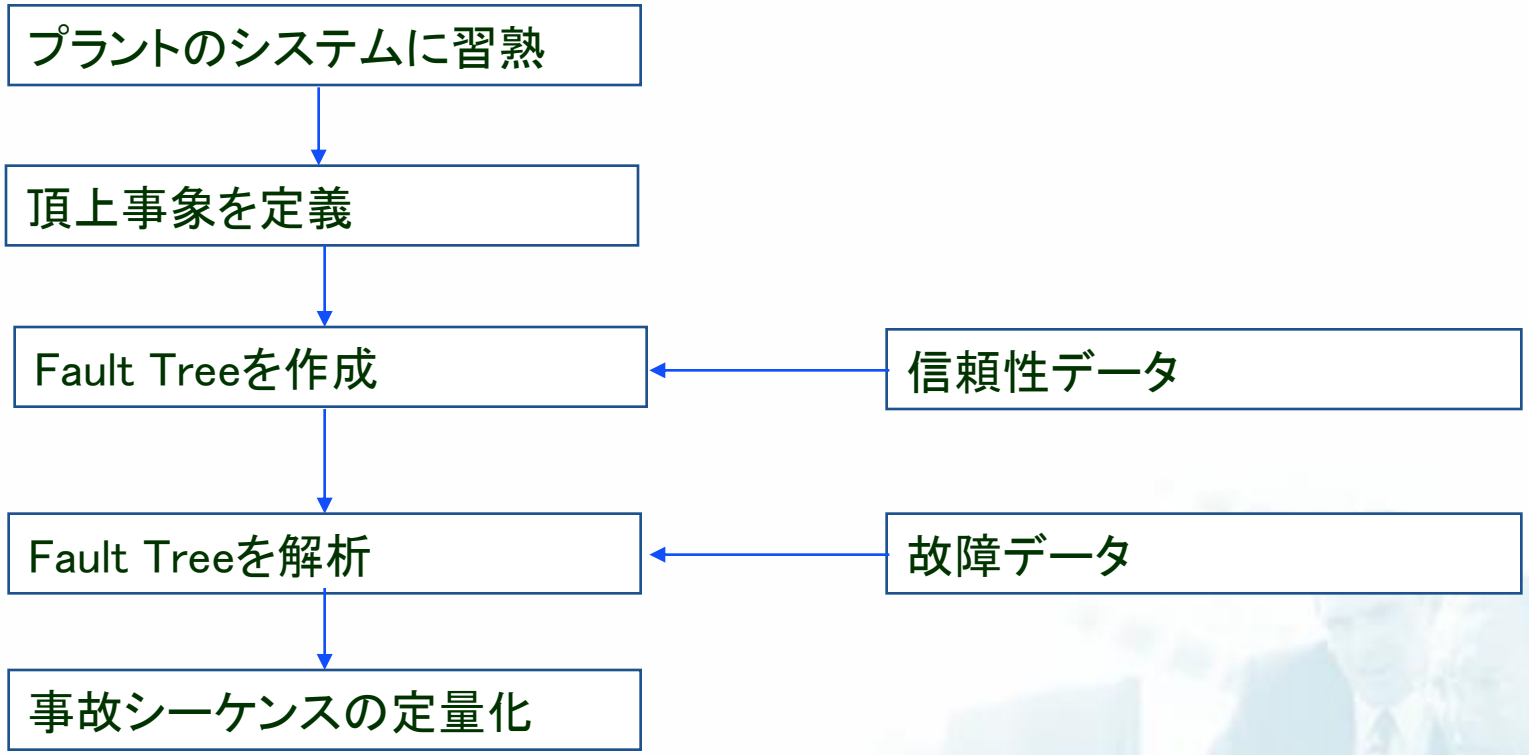
$P_s = 0.82 * 0.96 = 0.78$

$F_s = 1 - 0.78 = 0.22$

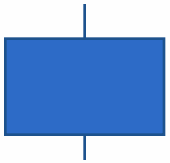
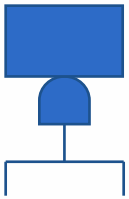
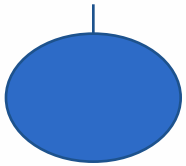
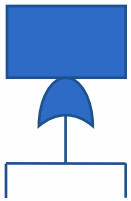
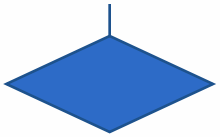
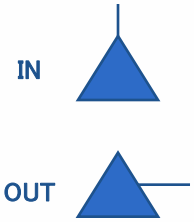
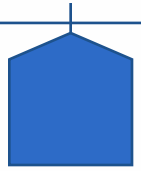
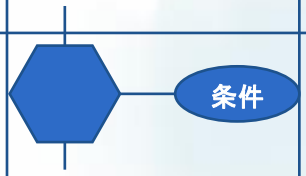
Fault tree Analysis (FTA)

- 故障の木解析法
- 1962年に米国のミサイル製造事故を防止する目的から開発された手法である（Bell Telephone Laboratories）
- トップ事象に災害等の最終結果を置いて、その原因を論理的に解析する
- シナリオを論理的なグラフとしてあらわすことが可能
- 各要素の故障確率、人為的過ちの確率などを推定し、システムの故障率を計算する

FTA　解析の流れ

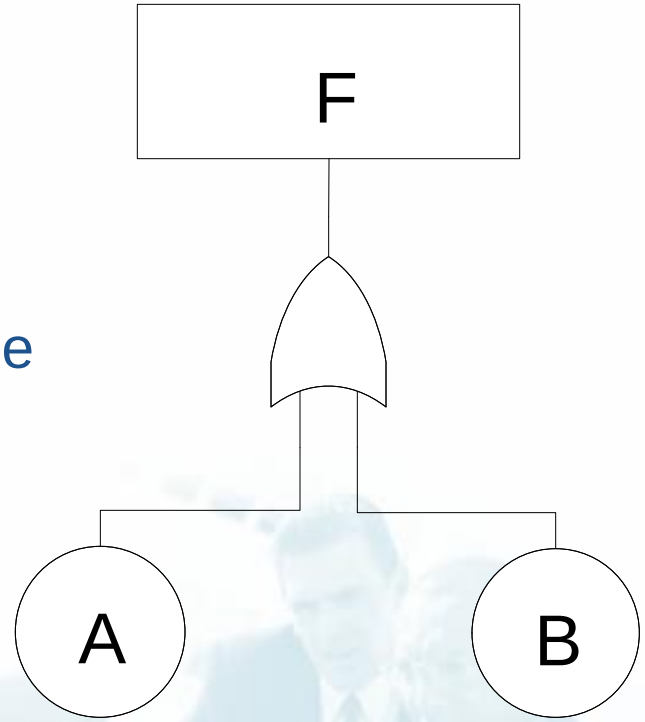

プラントのシステムに習熟
頂上事象を定義
Fault Treeを作成
信頼性データ
Fault Treeを解析
故障データ
事故シーケンスの定量化

FT解析に用いられる記

記号	名称	説明	記号	名称	説明
	事象 event	トップ事象、及び基本事象等の組み合わせにより起る個々の事象(中間事象)		AND ゲート	論理積。
	基本事象 Basic event	これ以上は展開されない、又は発生確率が単独で得られる基本的な事象		OR ゲート	論理和。 冗長系でN out of Mの時は、N/Mゲートとする場合がある。
	否展開 事象 Undeveloped event	情報不足、技術的内容不明のためこれ以上展開できない事象 ダイヤモンド事象と呼ぶ。		移行記号 Transfer gate	FT図上の関連する部分への移行又は連結を示す。
	通常(家型) 事象 Normal (House) event	通常発生すると思われる事象を示す。 火災での「空気の存在」、機器の「保修・試験」等。		制約 ゲート INHIBIT gate	条件付確率。 条件を満足している場合のみ出力事象が発生する。

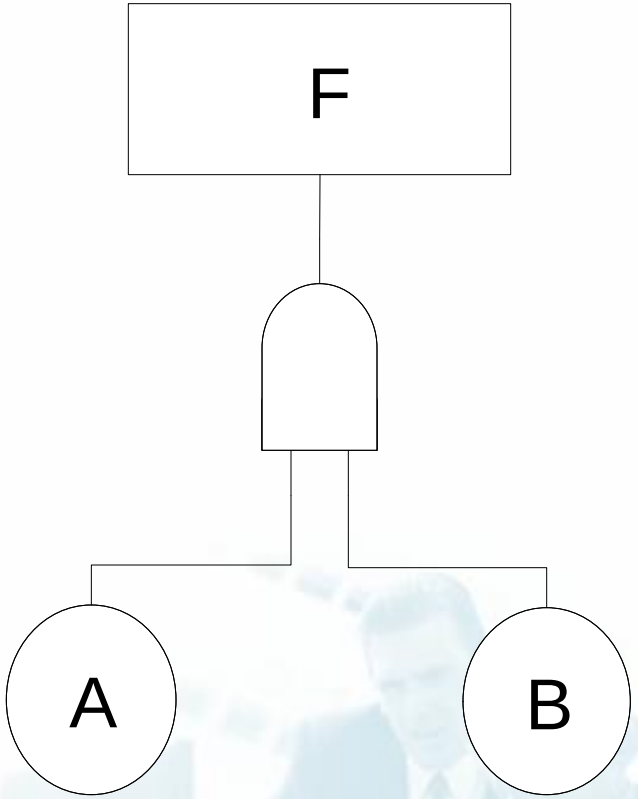
ORゲート

- OR ゲート
  - Any of two events (B, C) can cause a failure event (F)
  - Any of three events (A, B, C) can cause a failure event (F)



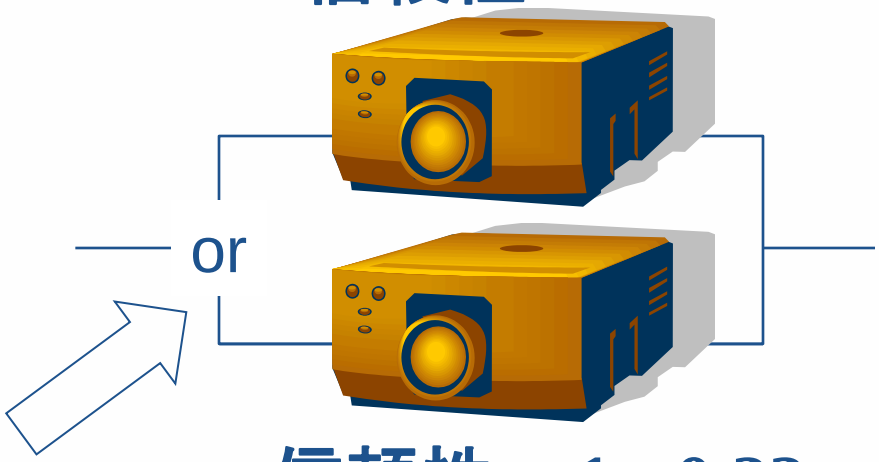
ANDゲート

- ANDゲート
  - All events (A and B) cause a failure event (F)
  - All events (A, B, and C) cause a failure event



プロジェクターの成功確立

信頼性 = 1 - 0.22 = 0.78

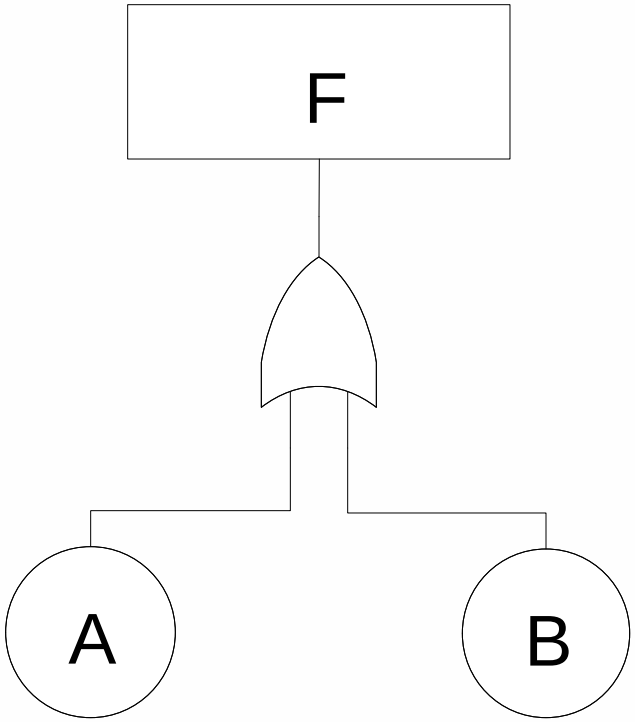


信頼性 = 1 - 0.22 = 0.78

$P_{s,\ proyectors}$ = (プロジェクターが故障しない場合のシステムの成功確立) *
プロジェクターの信頼性 +
(プロジェクターが故障する場合のシステムの成功確立) *
プロジェクターの故障確立

$P_{s,\ proyectors} = (1) * 0.78 + 0.78*(1 - 0.78) = 2*0.78 - (0.78)^2 = 0.96$

ORゲート



$$R_S = R_1 R_2$$

$$F_S = 1 - R_S$$

$$F_S = 1 - R_1 R_2$$

$$F_S = 1 - (1 - F_1)(1 - F_2)$$

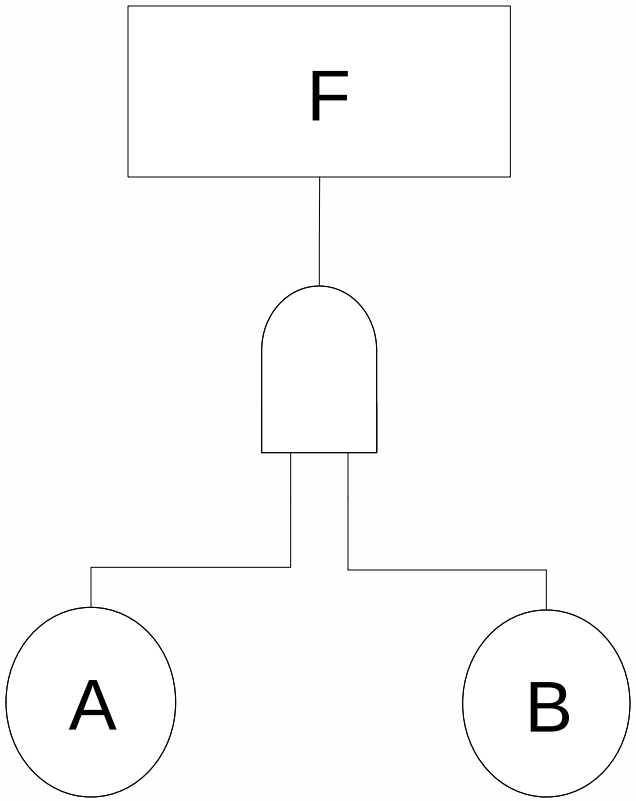
$$F_S = F_1 + F_2 - F_1 F_2$$

入力が3の場合：

$R_i < 0.2$ の場合 $F_S \approx F_1 + F_2$

$$F_S = F_1 + F_2 + F_3 - F_1F_2 - F_1F_3 - F_2F_3 + F_1F_2F_3$$

ANDゲート



$$R_S = R_1 + R_2 - R_1R_2$$

$$F_S = 1-R_S$$

$$F_S = 1-(R_1 + R_2 - R_1R_2)$$

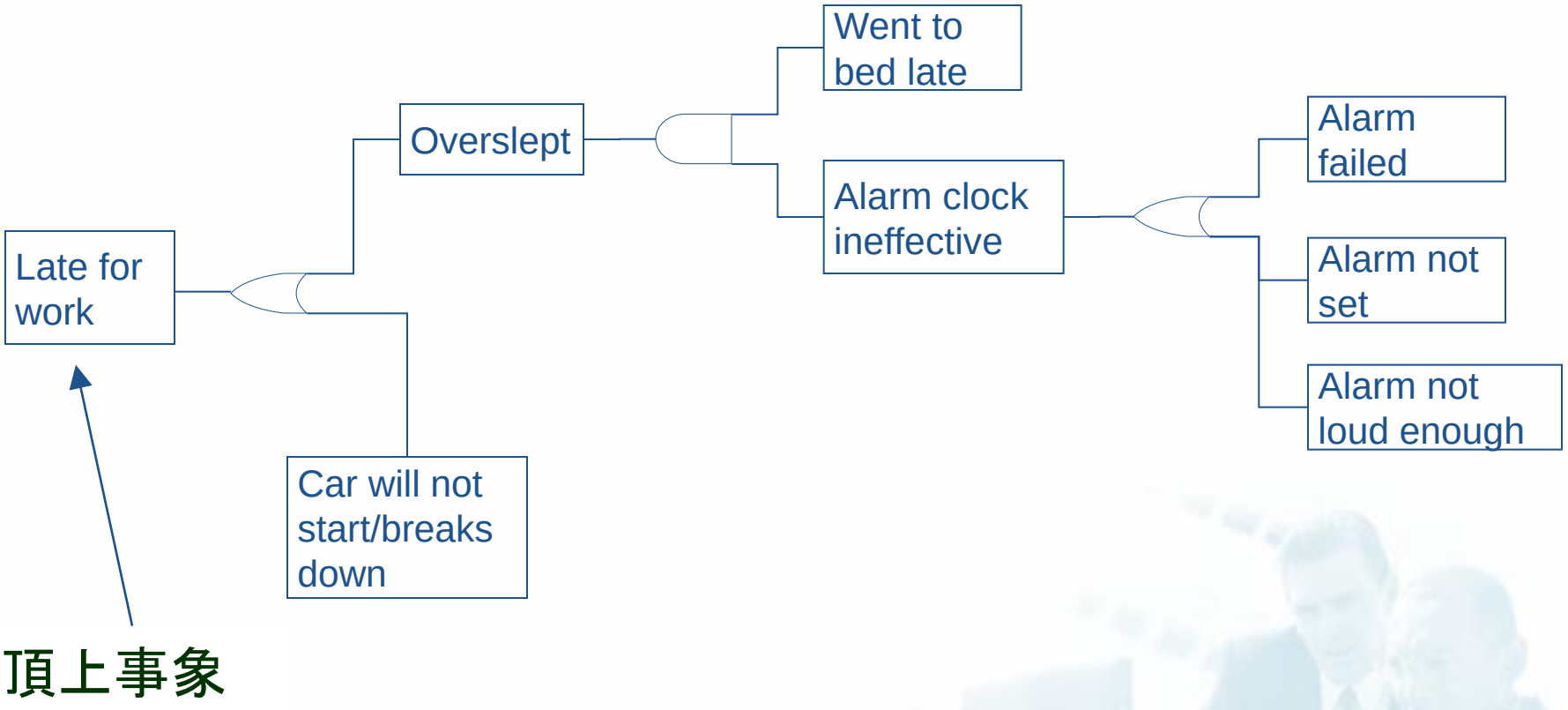
$$F_S = 1- [(1 - F_1) + (1 - F_2) - (1 - F_1)(1 - F_2)]$$

$$F_S = F_1 F_2$$

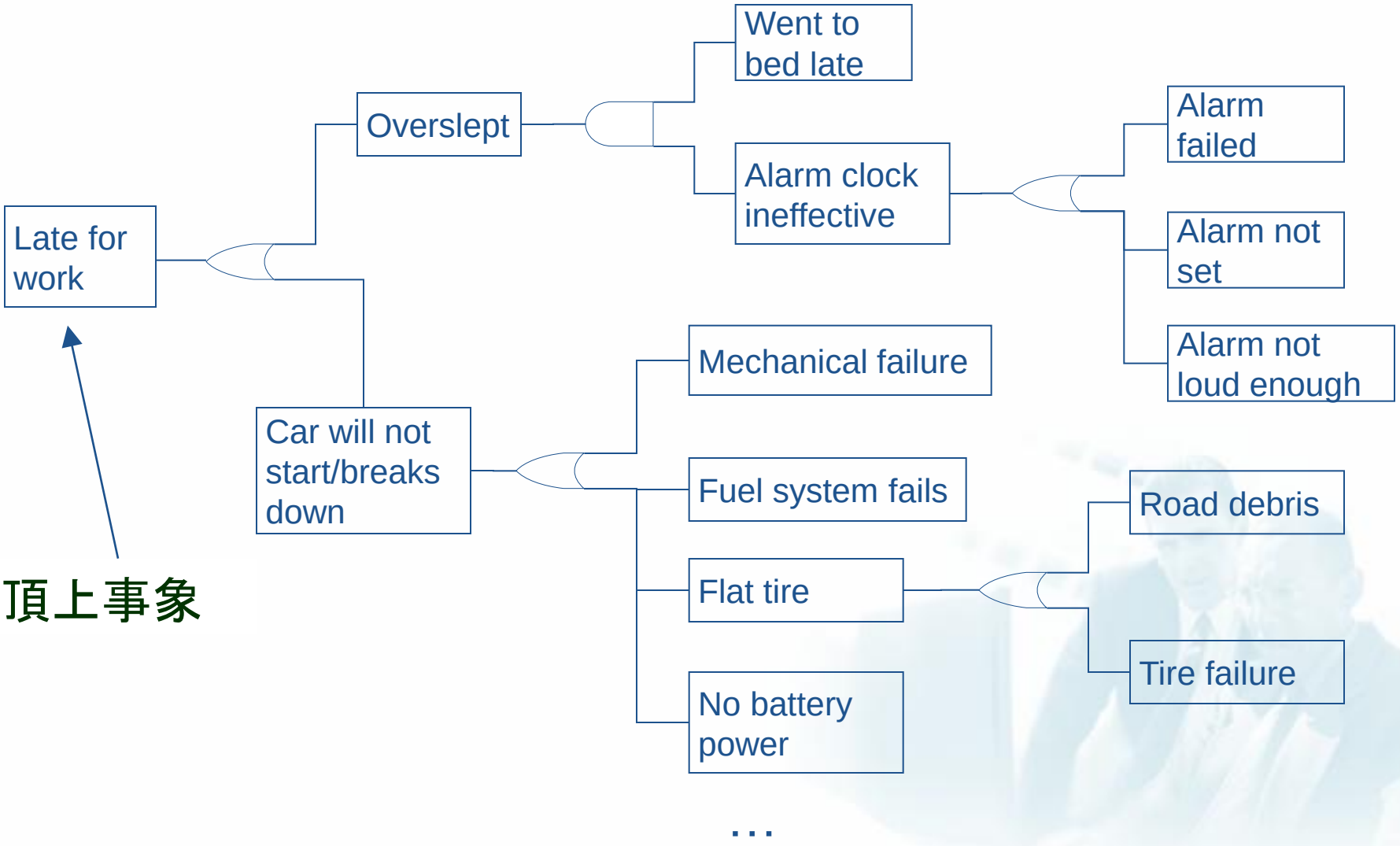
入力が3の場合：

$$F_S = F_1F_2F_3$$

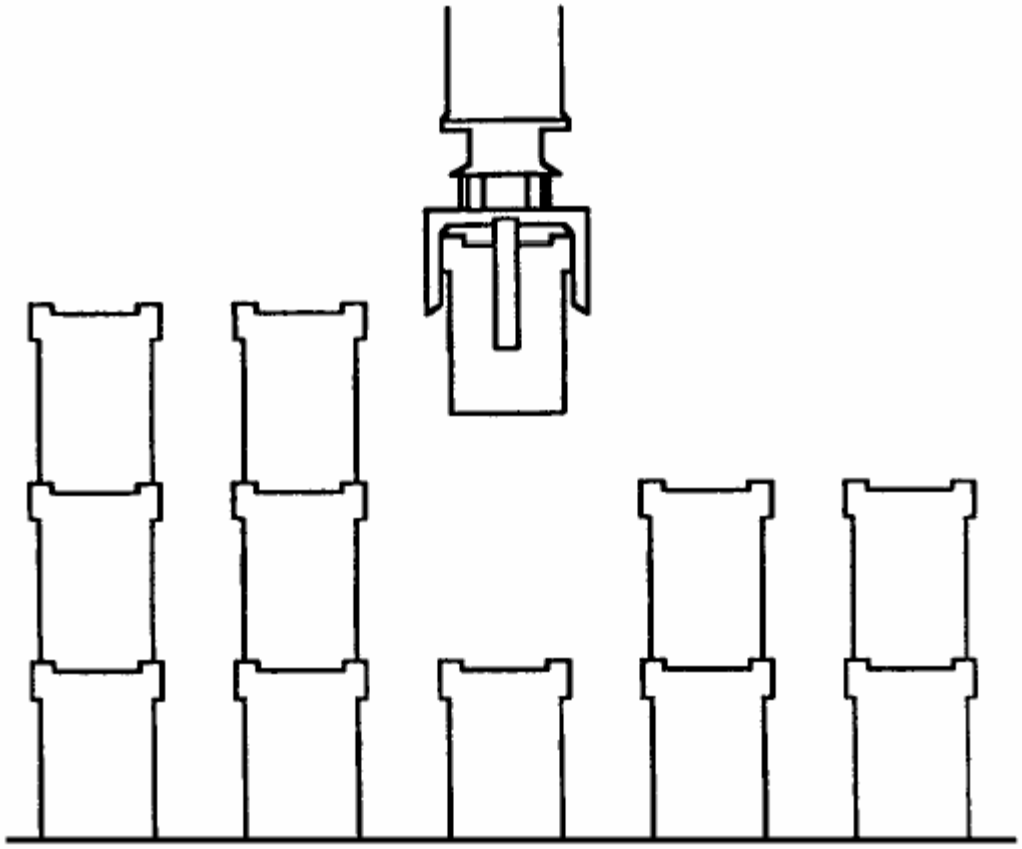
FTAの例

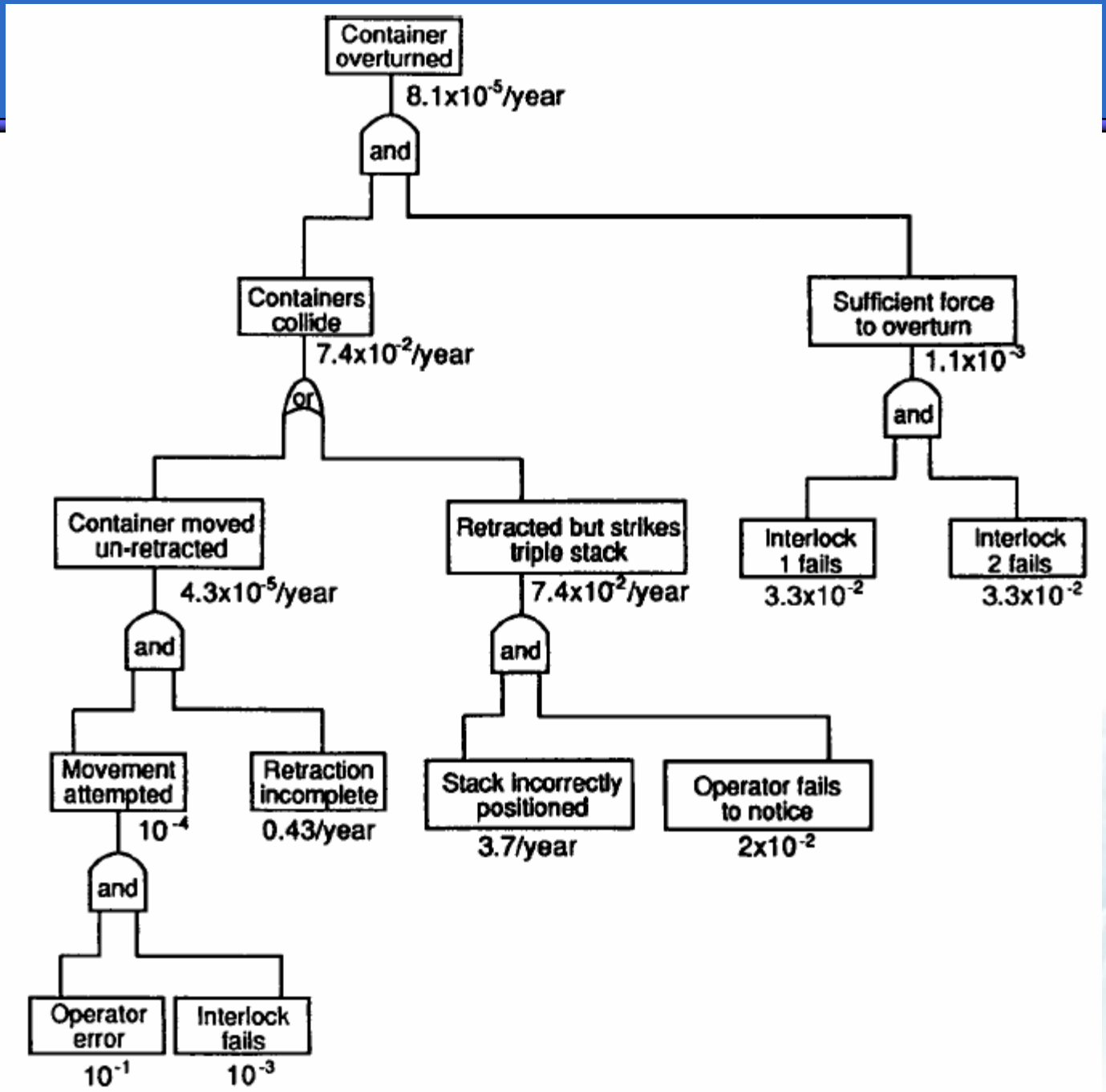

Late for work
Overslept
Went to bed late
Alarm clock ineffective
Alarm failed
Alarm not set
Alarm not loud enough
Car will not start/breaks down
頂上事象

FTAの例

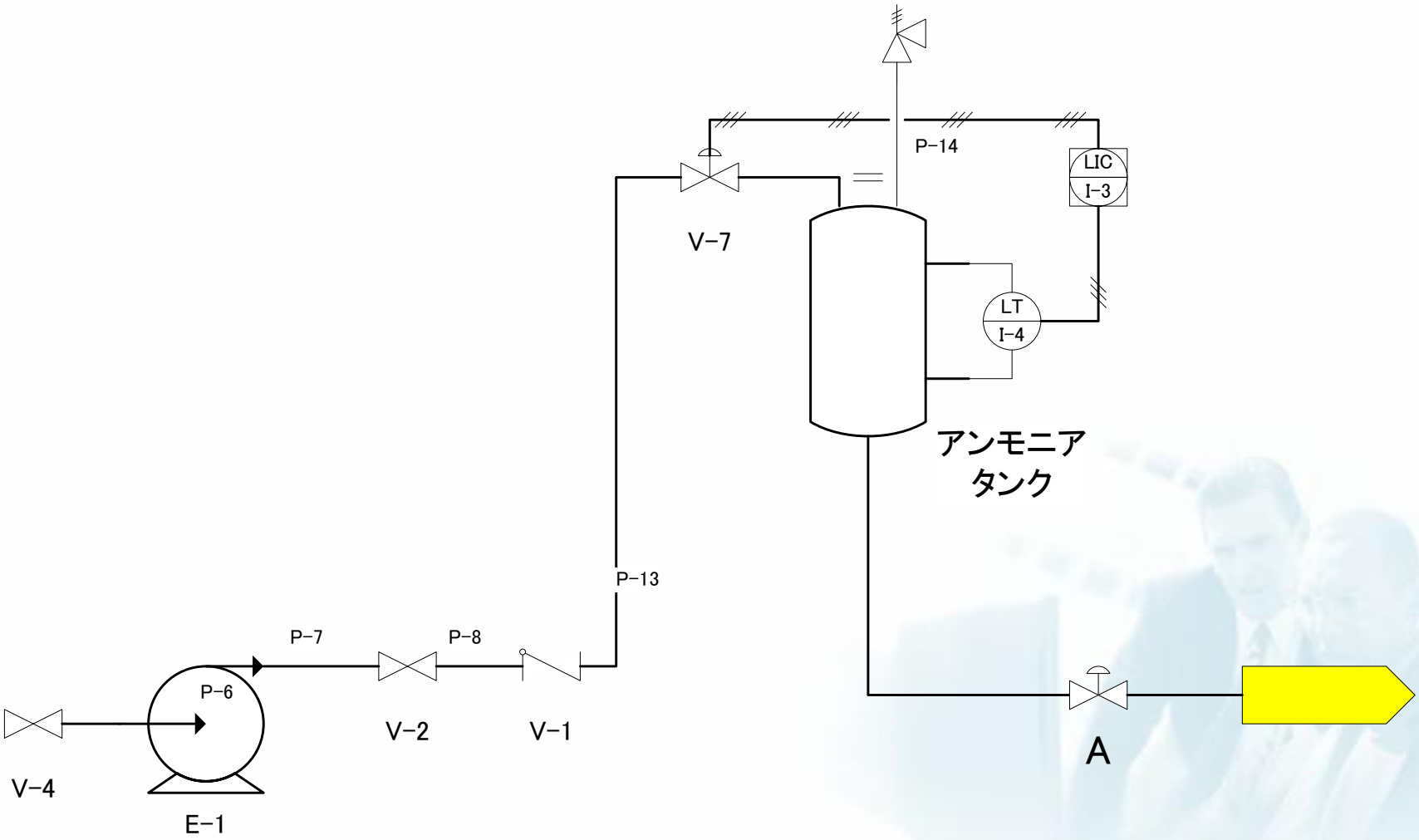

Late for work
Overslept
Went to bed late
Alarm clock ineffective
Alarm failed
Alarm not set
Alarm not loud enough
Car will not start/breaks down
Mechanical failure
Fuel system fails
Flat tire
Road debris
Tire failure
No battery power
...
頂上事象

例

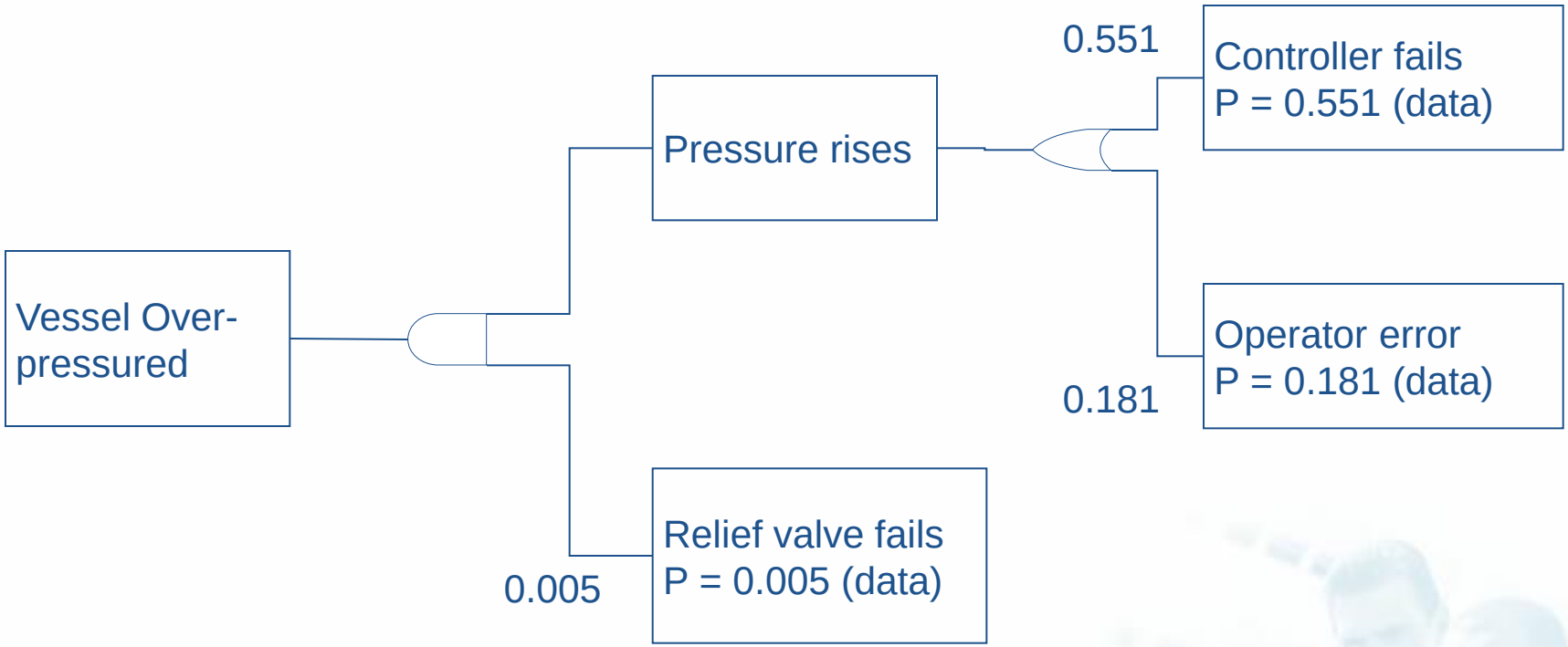



Container overturned
8.1x10-5/year
and
Containers collide
7.4x10-2/year
Sufficient force to overturn
1.1x10-3
or
and
Container moved un-retracted
4.3x10-5/year
Retracted but strikes triple stack
7.4x10-2/year
Interlock 1 fails
3.3x10-2
Interlock 2 fails
3.3x10-2
and
and
Movement attempted
10-4
Retraction incomplete
0.43/year
Stack incorrectly positioned
3.7/year
Operator fails to notice
2x10-2
and
Operator error
10-1
Interlock fails
10-3

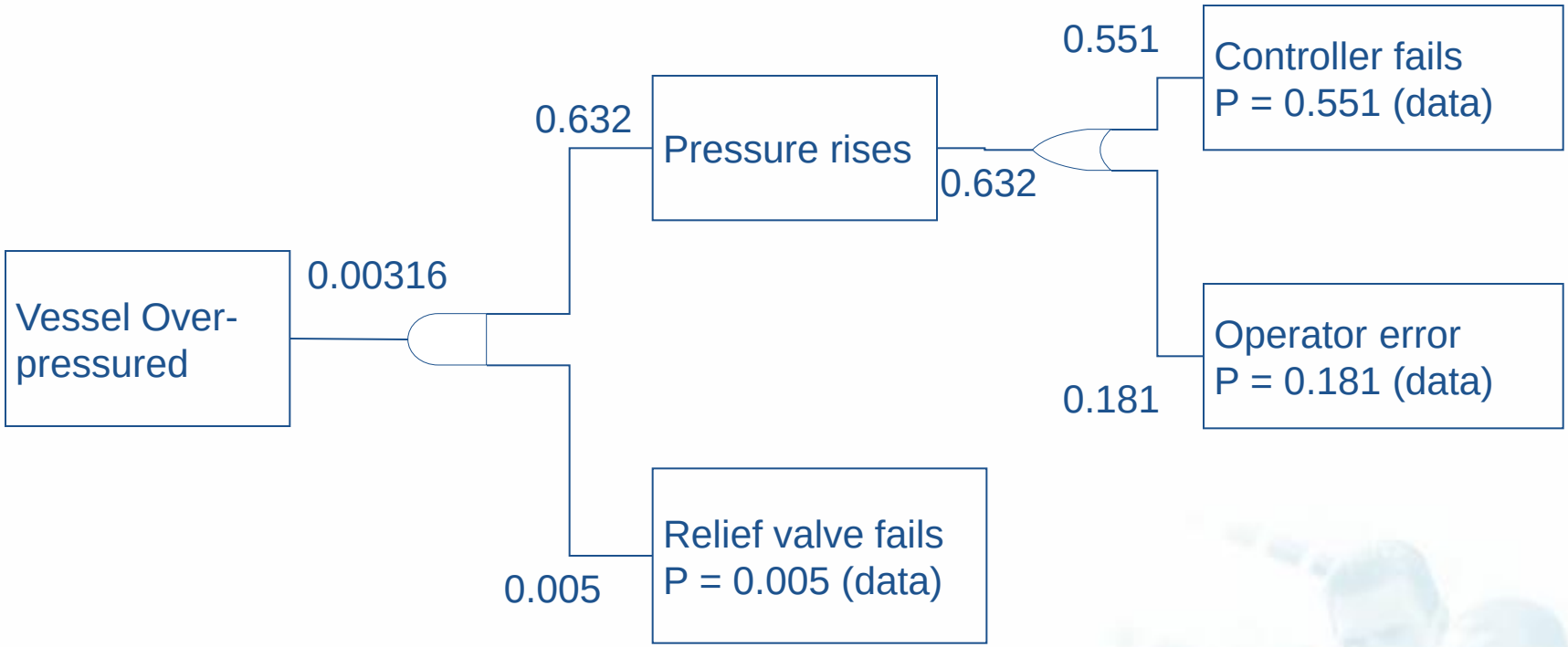
例



Level Controller LIC I-3 fails



Controller fails



Pressure rises: P= 0.551 + 0.181 – (0.551)(0.181) = 0.632

Vessel overpressured P= (0.632)(0.005) = 0.00316

リスク解析はどんな時でつかうか？

“Perform an analysis only to reach a decision. Do not perform an analysis if that decision can be reached without it. It is not effective to do so. It is a waste of resources.”

Dr. V.L. Grose
George Washington University

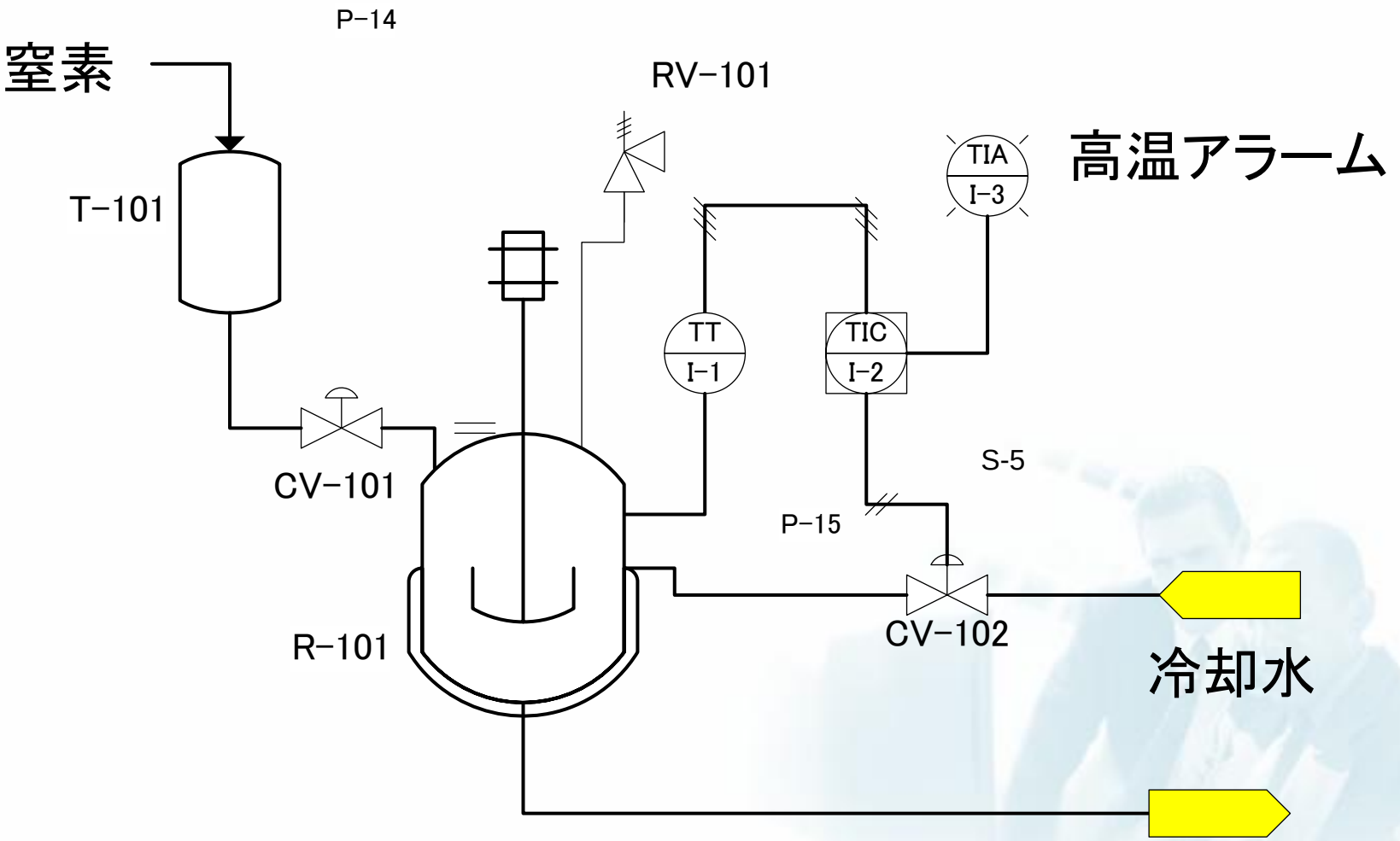
ETA(事象の木解析，event tree analysis)

- ET
  - 要素の状態(故障，正常) によって分岐し，最後にシステムの破損状態に到達します
- ETA
  - (ET)を作成して解析する手法

FTA: 頂上事象（結果）→　複数の基本事象（原因）

ETA: 1つの基本事象（原因）→　頂上事象（結果）

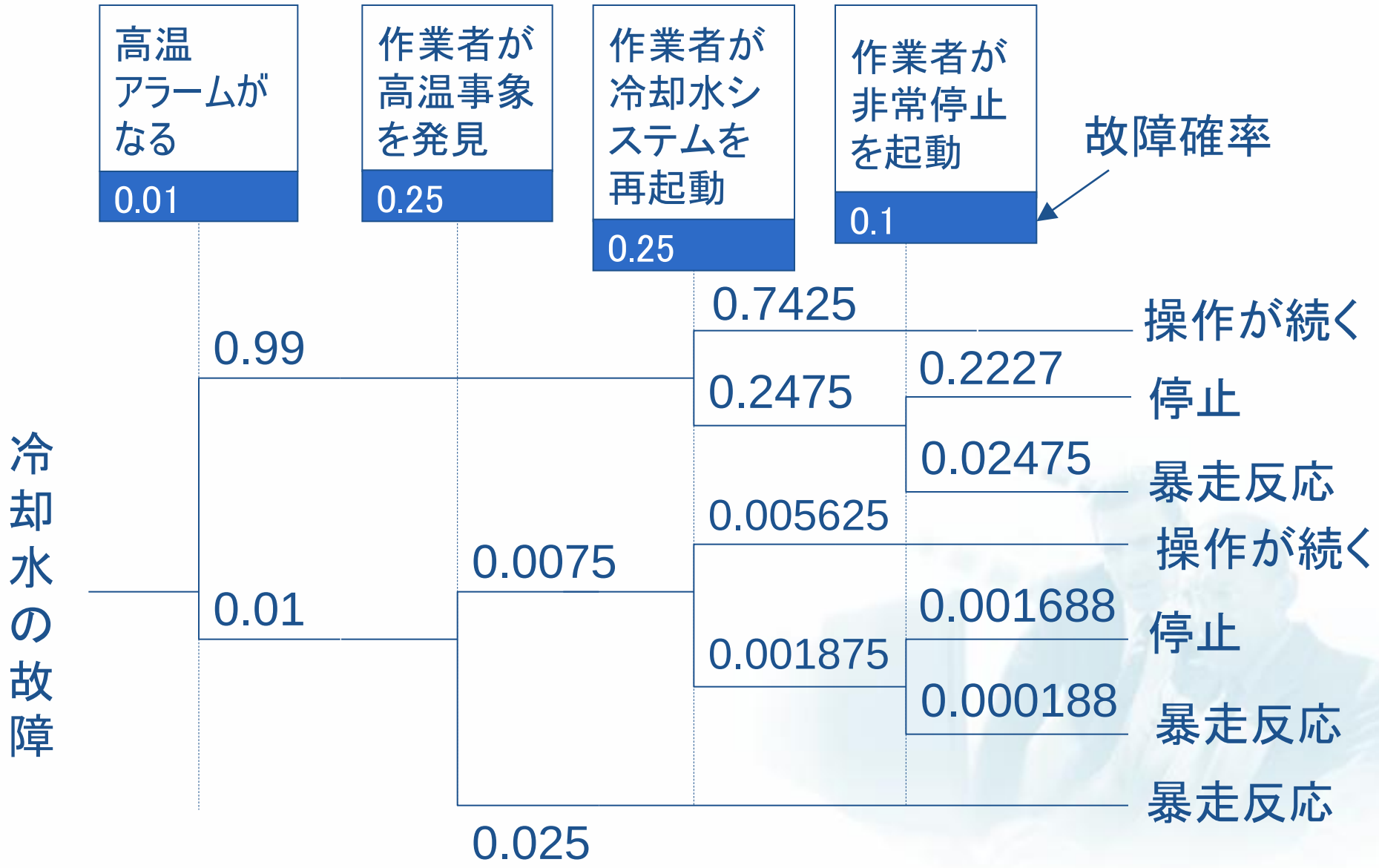
バッチ反応器


P−14
窒素
RV−101
T−101
TIA
I−3
高温アラーム
TT
I−1
TIC
I−2
S-5
CV−101
P−15
R−101
CV−102
冷却水

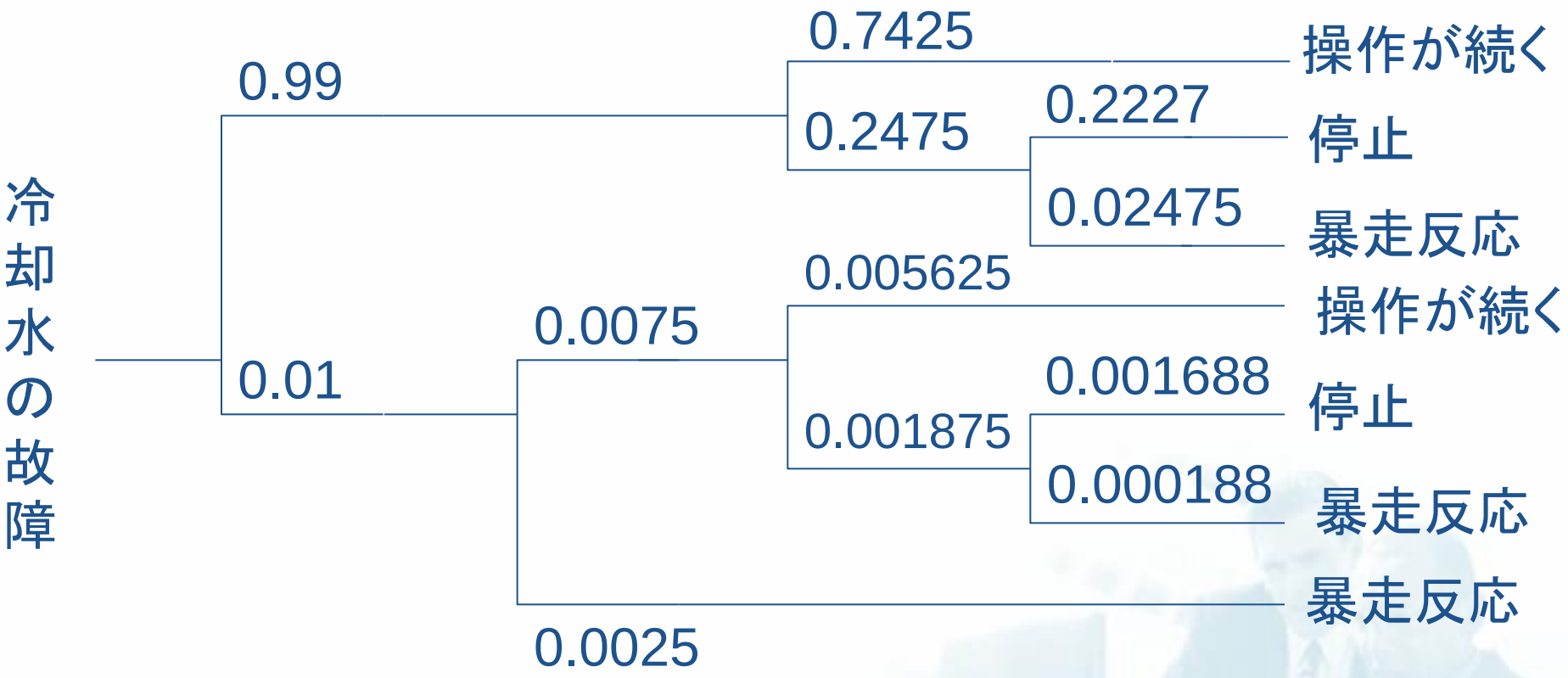
データ

安全機能	成功確立	故障確率
高温アラームがなる	0.99	0.01
作業者が高温事象を発見	3 out of 4 times	0.25
作業者が冷却水システムを再起動	3 out of 4 times	0.25
作業者が非常シャットダウンを起動	9 out of 10 times	0.10

冷却水の故障のET


高温アラームがなる
0.01
作業者が高温事象を発見
0.25
作業者が冷却水システムを再起動
0.25
作業者が非常停止を起動
0.1
故障確率
冷却水の故障
0.99
0.01
0.7425
0.2475
0.0075
0.025
0.2227
0.02475
0.005625
0.001875
0.001688
0.000188
操作が続く
停止
暴走反応
操作が続く
停止
暴走反応
暴走反応

冷却水の故障のET



暴走反応の総合確率 = 0.02475 + 0.000188 + 0.0025 = 0.02744

= 1/36 years