信頼性設計概論

土屋達弘 (大阪大学)

概要

- 担当教員
  - 土屋達弘
- 内容（予定）
  1. 基礎概念
  2. フォールトトレランス
  3. 分散システムの高信頼化
  4. 分散システムの高信頼化
  5. ソフトウェアの信頼性
  6. ソフトウェアの信頼性, テスト

障害事例

- 東証システム障害 (2005)
- Netflix Christmas Eve outage (2012)
- みずほ銀行 システムMINORI障害 (2021)

基本概念

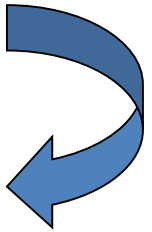
1. ディペンダブルなシステムを学習する
2. ディペンダビリティの関連概念を学習する
3. フォールトツリー解析について学習する
4. 機能安全について学習する

1. ディペンダブルなシステムを学習する

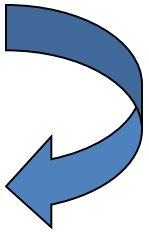
- Dependability
  - 広い意味で，信頼性を表す
  - 障害を避ける能力
- さまざまな属性
  - Reliability, Availability, Serviceability, …
    - 古典的な評価尺度
  - Reliability：時刻tまで正常に動作する確率
    - MTTF：障害までの平均時間

Failure, Fault, Error

- Fault (故障, フォールト)
  - 構成要素の異常. 障害, 誤りの原因.



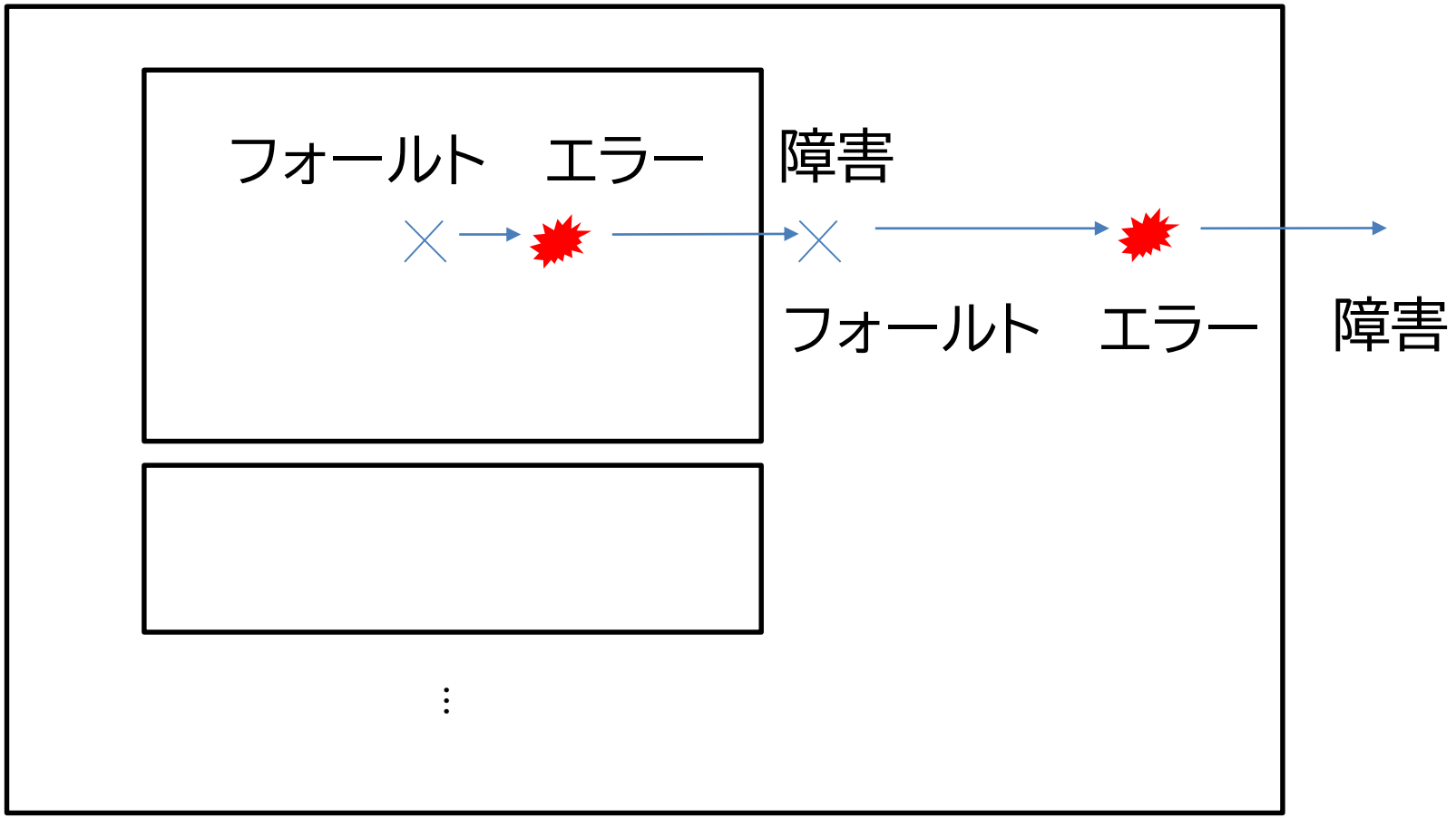
- Error (誤り, エラー)
  - システムの構成要素の異常状態. フォールトが顕在化したもの. 障害の原因.



- Failure (障害, フェイリア)
  - システムが期待されるサービスを提供しなくなること

システムの階層性

System = Systemの集合体



Dependabilityの実現

- Fault Avoidance (フォールトアボイダンス)

  障害の原因となるフォールトが発生しないようにするというアプローチ

- Fault Tolerance (フォールトトレランス, 耐故障性)

  フォールトが発生しても障害に至らないようにするというアプローチ

- 参考

  4つに分けることも多い

  - 前者: fault avoidance + fault elimination
  - 後者: fault tolerance + fault forecasting

Faults (故障, フォールト)

- フォールトが存在する期間による分類
  - Transient fault (過渡フォールト)
    - ◆一時的なfault
  - Permanent fault (永久フォールト)
- その他の分類
  - Physical fault
    - ◆物理的なフォールト
  - Design fault (設計フォールト)
    - ◆例. プログラムのバグ

Fault Tolerance and Redundancy

- フォールトトレラントシステム (Fault-tolerant system)
  = Faultの影響をmaskできるシステム

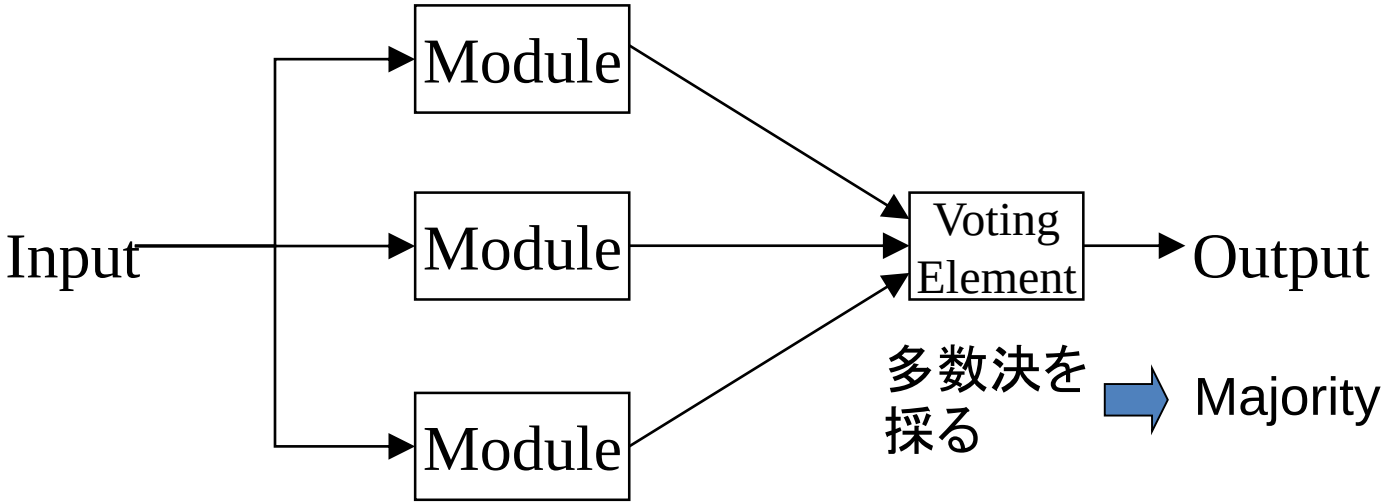
- Redundancy (冗長性)

  Fault toleranceを実現するには, 何らかの形で Redundancy (冗長性, 余分なもの)が必要

  - Space redundancy　(空間冗長性)
  - Time redundancy　(時間冗長性)

代表的なfault tolerance機構 (1)

- Triple Modular Redundancy (TMR)

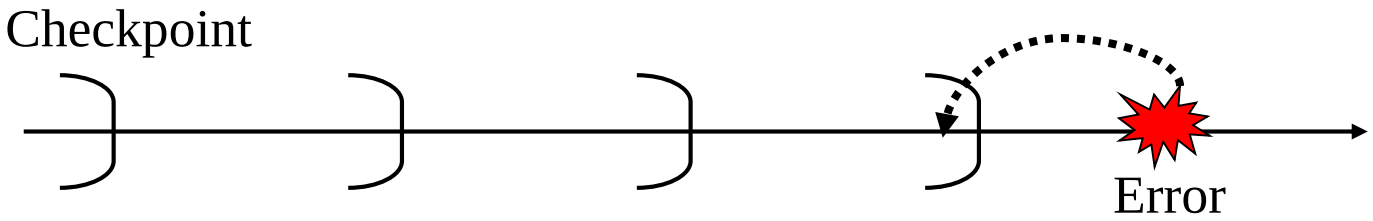


1. 1つのModuleのFaultに耐えられる
2. Faultの発生に対し特別な処理(エラー検出やリカバリー等)を行わない

代表的なfault tolerance機構 (2)

- Checkpoint and Restart (Rollback Recovery)

  チェックポイントでシステムの状態を保存しておき, errorの場合は,
  以前の正常な状態から処理を再開する.



ある特定の条件の下でだけ顕在化する
フォールトに有効(つまり, transient fault)

2. ディペンダビリティの関連概念を学習する

- Reliability
- Availability
- Serviceability
- Integrity
- Security

RAS

RASIS

+Safety

人命，健康，財産や環境に関する影響

ディペンダビリティの主要特性

- RASはIBMによる
- RASISは国外では知られていない
- （伝統的な）ディペンダビリティの主要特性
  - ◆Securityの代わりにSafetyを追加したもの

Reliability/Availability

- Reliability (信頼性, 信頼度)
  - サービスが継続して提供されること
  - 時刻tまでシステムが正しく動き続ける確率
- Availability (可用性, 可用度)
  - サービスが利用できること
  - システムが正しく動いている確率

Serviceability/Integrity/Security

- Serviceability = Maintainability
  - 保守性
    - ◆ヘルプデスク, モニタリング, ソフトウェアアップグレード, 機器交換等
- Integrity
  - データなど情報の不整合, 矛盾がおきないこと
- Security
  - セキュリティ, 機密性

Safety

- 危害 (harm)
  - 人の受ける身体的傷害若しくは健康傷害，又は財産若しくは環境の受ける害
- ハザード (hazard)
  - 危害の潜在的な源
- 危険状態 (hazardous situation)
  - 人，財産又は環境が，1つ又は複数のハザードにさらされる状況
- リスク (risk)
  - 危害の発生確率とその危害の重大さの組合せ
- 安全 (safe)
  - 受容できないリスクがないこと

Reliability (信頼性, 信頼度)

- 時刻tまでシステムが正しく動き続ける確率
  - 非修理系 (non-repairable system)の評価

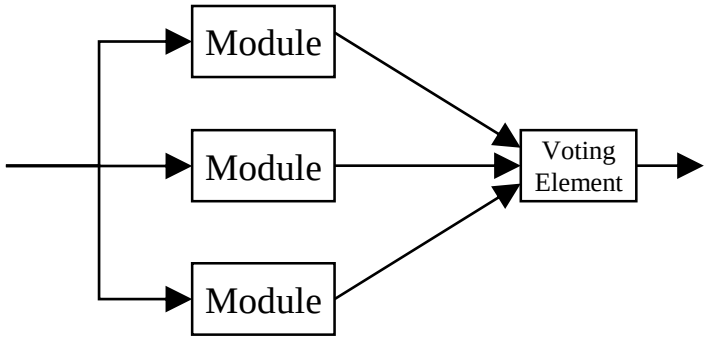
- failure rate (障害率) λ ($\lambda \geq 0$)が一定の場合

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

  - t: 時刻 ($t \geq 0$)
  - e: 自然対数の底

フォールトトレラントシステムの信頼度

- 工夫により$R(t) = \mathrm{e}^{-\lambda t}$を変化
- 例. TMR
  - 仮定
    - ◆モジュールの信頼度：$R_m(t) = \mathrm{e}^{-\lambda t}$
    - ◆Voting element (多数決器, voter)は, 故障しない
    - ◆2台以上のモジュールが故障していなければ, 正常



  - 信頼度 $R(t) =$＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Failure rate (障害率)

- 障害率＝瞬間的に障害が起こる可能性の大きさ

$$\lambda(t) = \lim_{h \to 0} \left(\frac{F(t+h) - F(t)}{h} \right) \frac{1}{R(t)} = \frac{F(t)'}{R(t)}$$

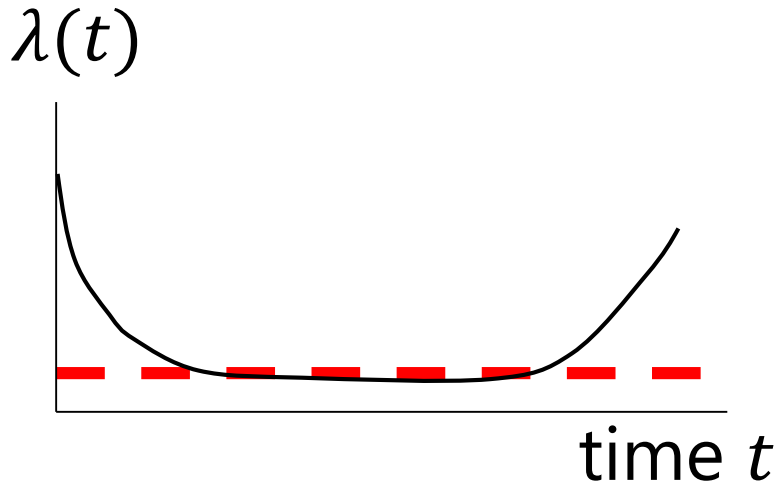
ただし, $F(t) = 1 - R(t)$

  - ◆ 時刻tまでに障害が起る確率
  - ◆ 障害までの時間の累積分布関数

- $\lambda(t)$が定数λ のとき, $F(t) = 1 - e^{\lambda t}$
  - □$F(0) = 0$とする
  - □このとき, 障害までの時間は指数分布

Bathtub Curve (バスタブ曲線)

- 機器の典型的な障害率の推移を表す曲線
- 安定しているときは一定
  - 信頼度を計算するとき, 実用的には一定と仮定してよい



MTTF (Mean Time To Failure, 平均障害時間)

- MTTF (平均障害時間)

$$E[X] = \int_0^\infty t\frac{dF(t)}{dt}dt = -[tR(t)]_0^\infty + \int_0^\infty R(t)dt = \int_0^\infty R(t)dt$$

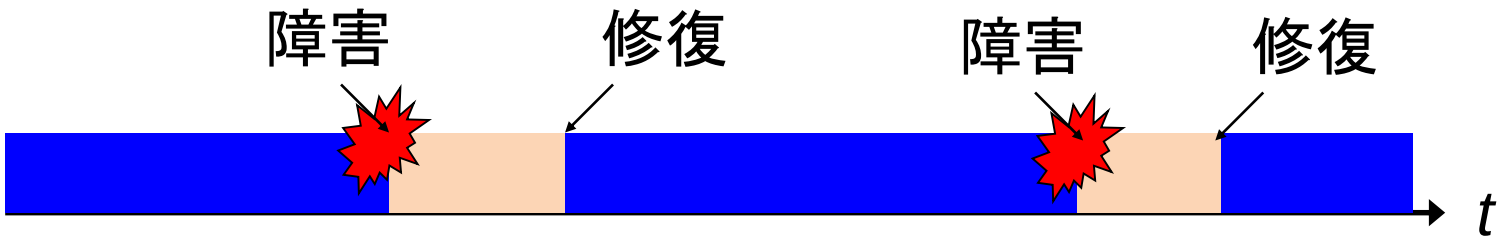
  - Xは障害までの時間をあらわす確率変数

- $\lambda(t) = \lambda$の場合 (Xが指数分布している場合)
  - $R(t) = \mathrm{e}^{-\lambda t}$
  - MTTF $= \frac{1}{\lambda}$

Availability (アベイラビリティ, 可用性, 可用度)

- システムが正しく動いている確率
- Instantaneous availability (瞬時アベイラビリティ)

$A(t)$ = Pr[時刻tでシステムが正常]



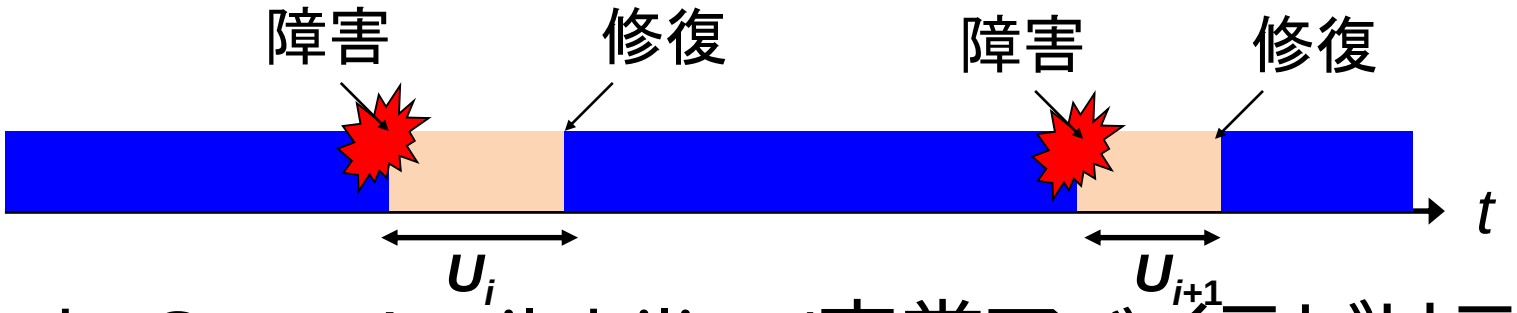
- Steady-State Availability (定常アベイラビリティ)

$$A = \lim_{t \to \infty} A(t)$$

MTTR (Mean Time To Repair)と定常アベイラビリティ

- *MTTR* (Mean Time to Repair, 平均修復時間)

$$MTTR = E[U_i]$$



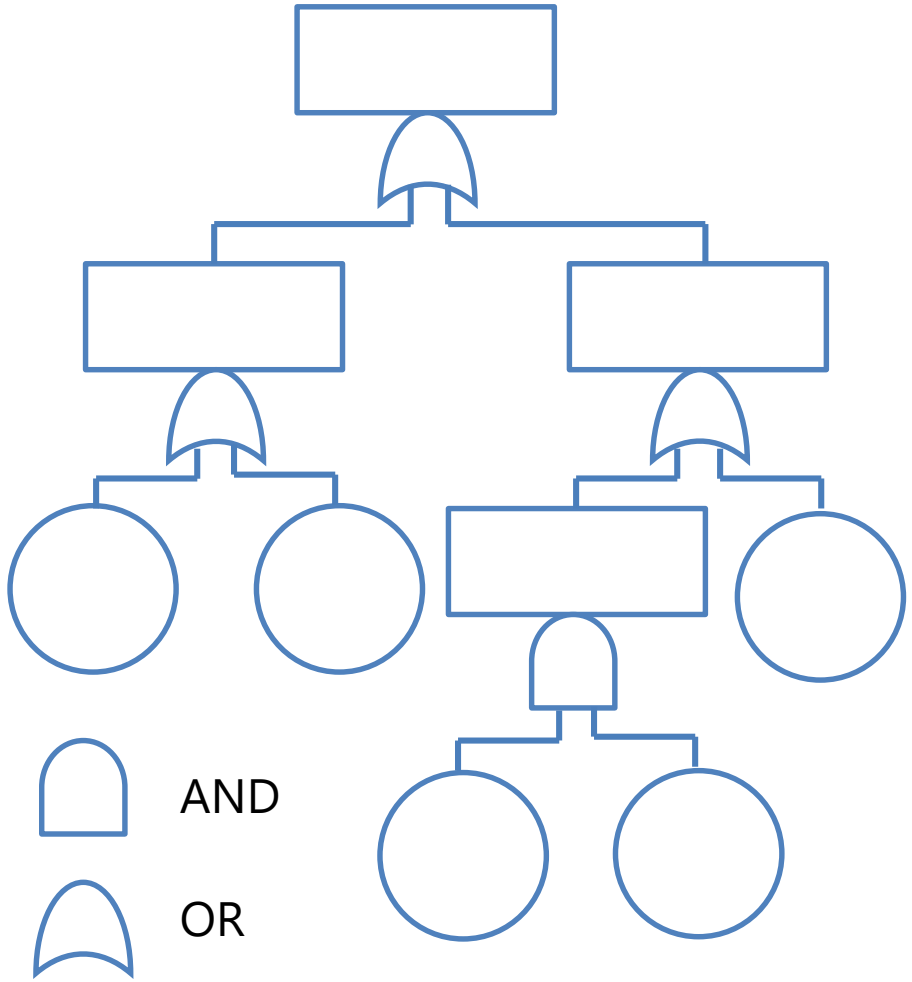
- Steady-State Availability (定常アベイラビリティ)

$$A = \lim_{t \to \infty} A(t) = \frac{MTTF}{MTTF+MTTR}$$

  - 修理系の場合 MTTFをMTBFと呼ぶことが多い
    - ◆Mean Time between Failures

3.フォールトツリー解析について学習する

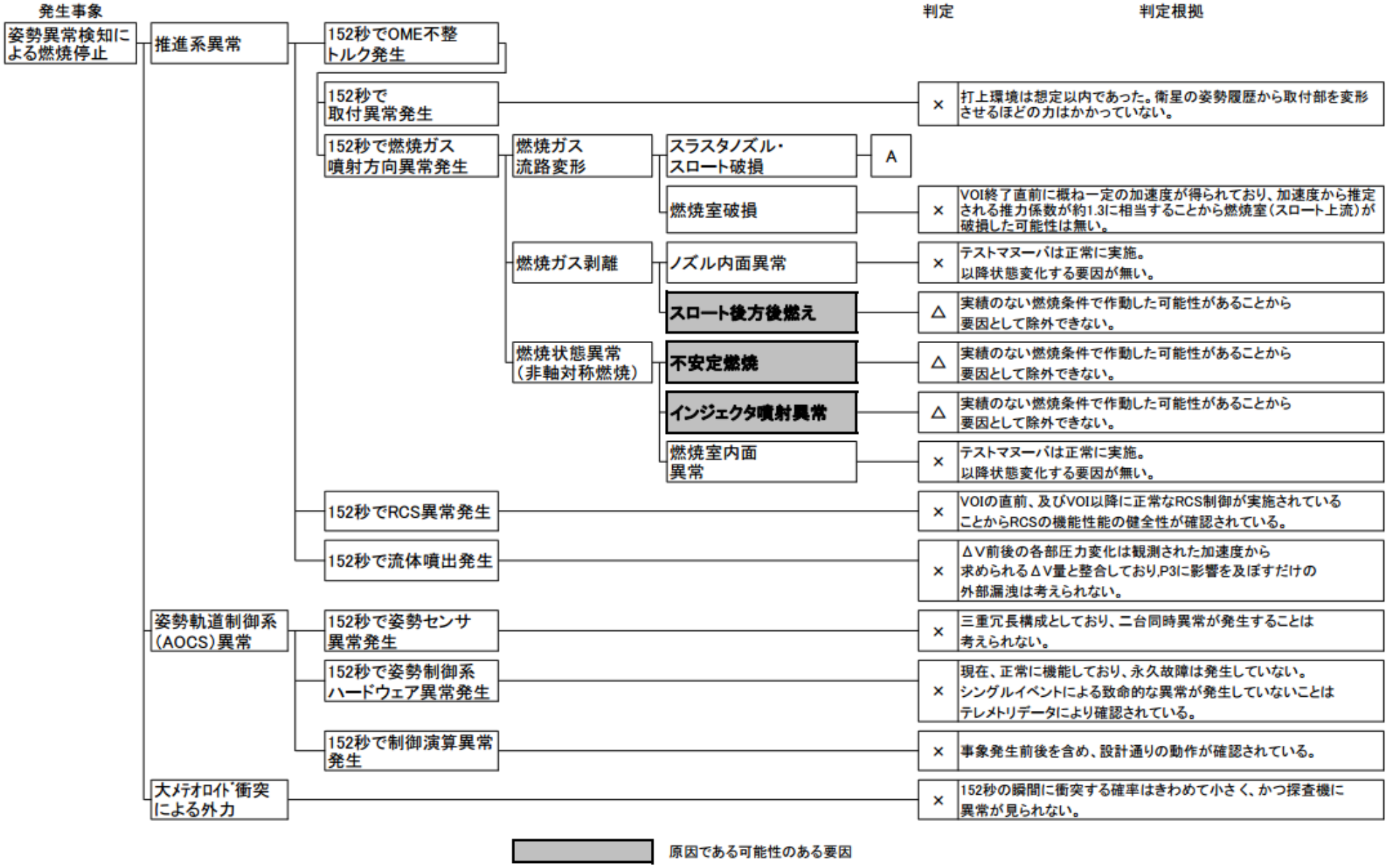
- フォールトツリー (Fault Tree)
  - 根が表す事象をハザードや障害とする
  - 葉を基本事象とする
  - 葉以外の頂点
    - ◆原因となる事象を表す頂点を，子とする
    - ◆原因と元の事象との関係を，論理ゲートで表す



フォールトツリー解析

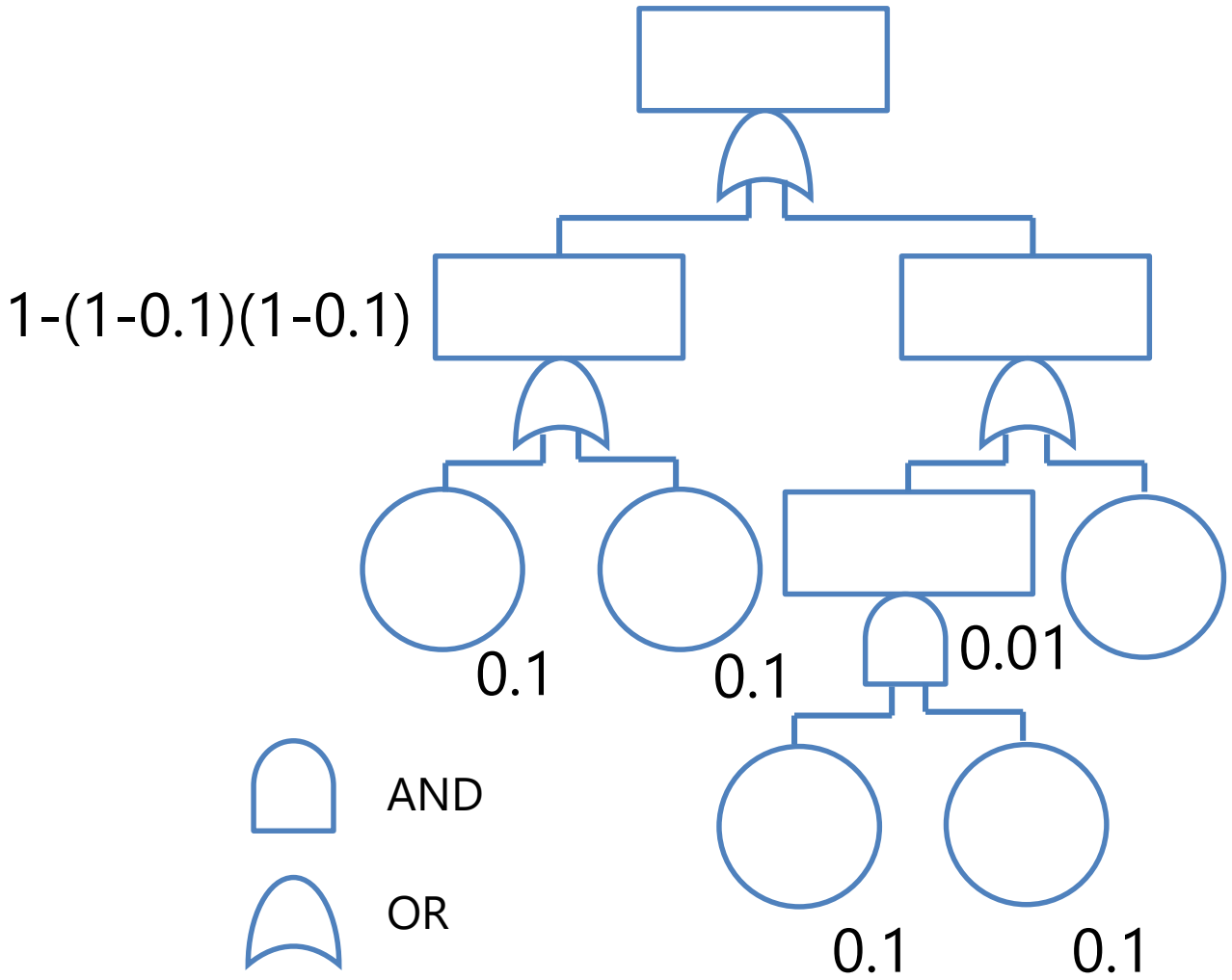
- FTA (Fault tree analysis)の目的
  - どのようなハザードがあるかを解析
  - どのように障害が生じるかを解析
  - 起こった事象の解析
  - 危害や障害の発生確率の解析
    - 確率的FTA

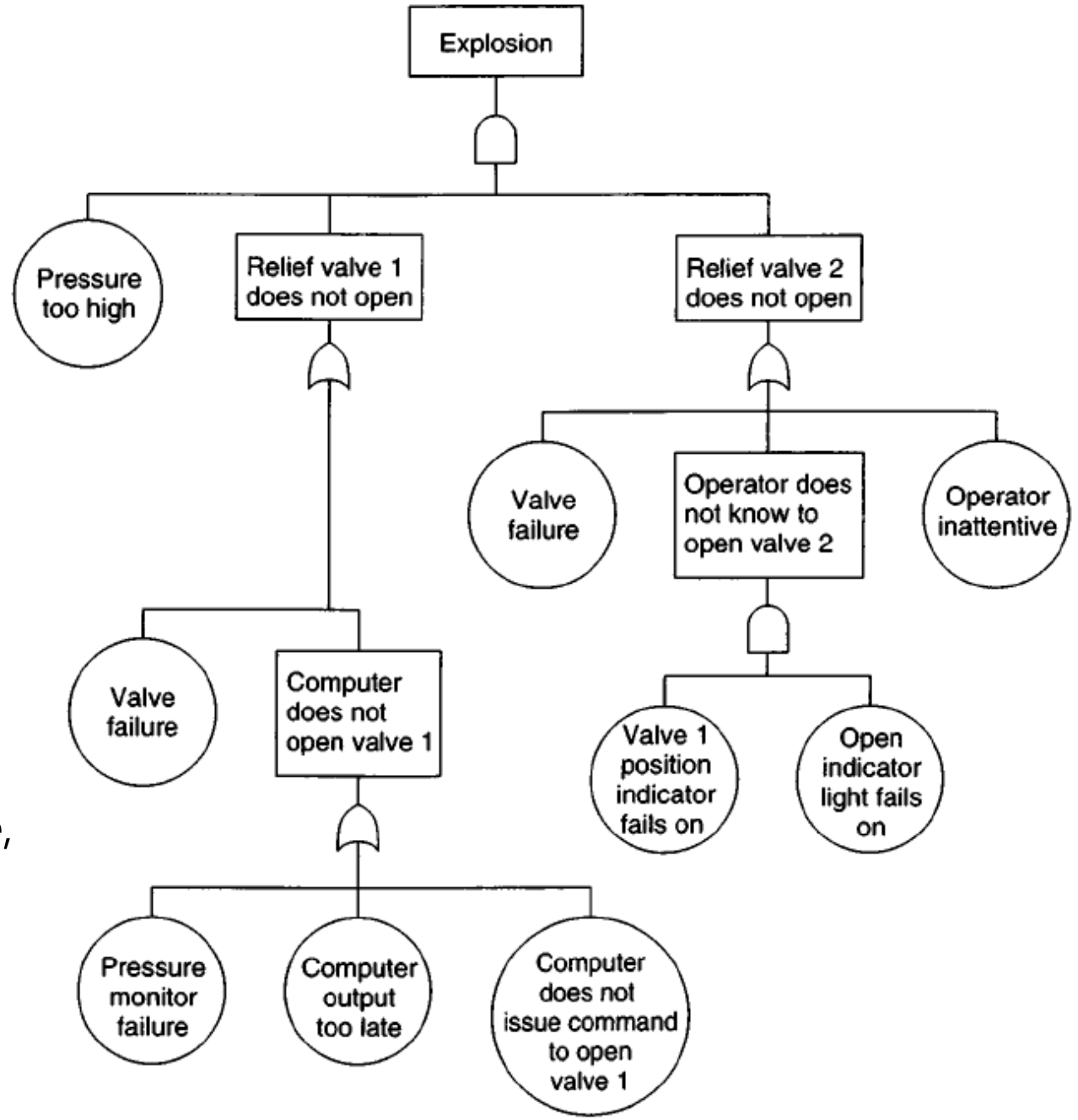
あかつきの金星周回軌道への投入失敗に対するFT (引用 JAXA「あかつき」の金星周回軌道投入失敗 に係る原因究明と対策について)



確率的FTA

- 例. 基本事象が独立で,
  生起確率 0.1 の場合

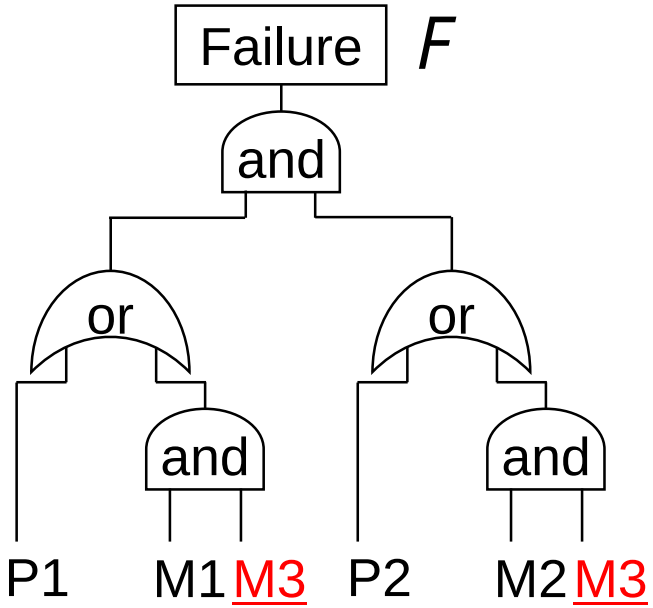




N.Leveson, Safeware, Addison-Wesley, 1995

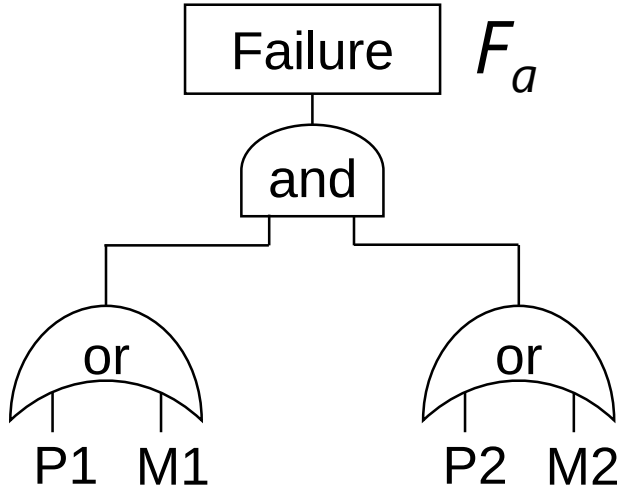
Factoring

- 同じ基本事象が複数の葉に現れる場合，状況を分解して解析すること

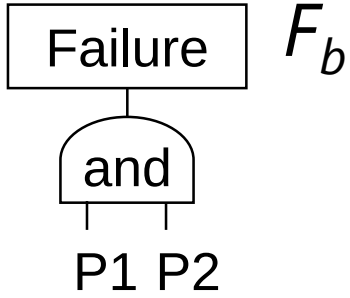


$$F = F_{M3}F_a + (1\text{-}F_{M3})F_b$$

M3が障害



M3が正常



FTA以外のハザード分析手法

- HAZOP (Hazards and Operability Analysis)
  - ガイドワードから，逸脱(異常)，原因，結果を導出
    - ガイドワード (guide words)の例：無，逆，大，小，...

松野，山本,「実践D-Case」の例を改変

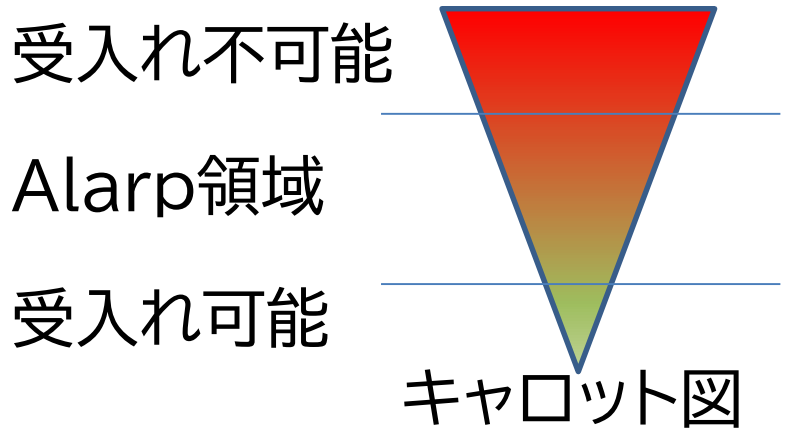
ガイドワード	逸脱	原因	結果
大	危険な現場での速度超過	安全教育不足	脱線事故
無	危険な現場へのATS設置漏れ	安全意識不足 予算不足	脱線事故

⋮

- FMEA (Fault Mode Effect Analysis)
- STPA (System-Theoretic Process Analysis)

4. 機能安全について学習する

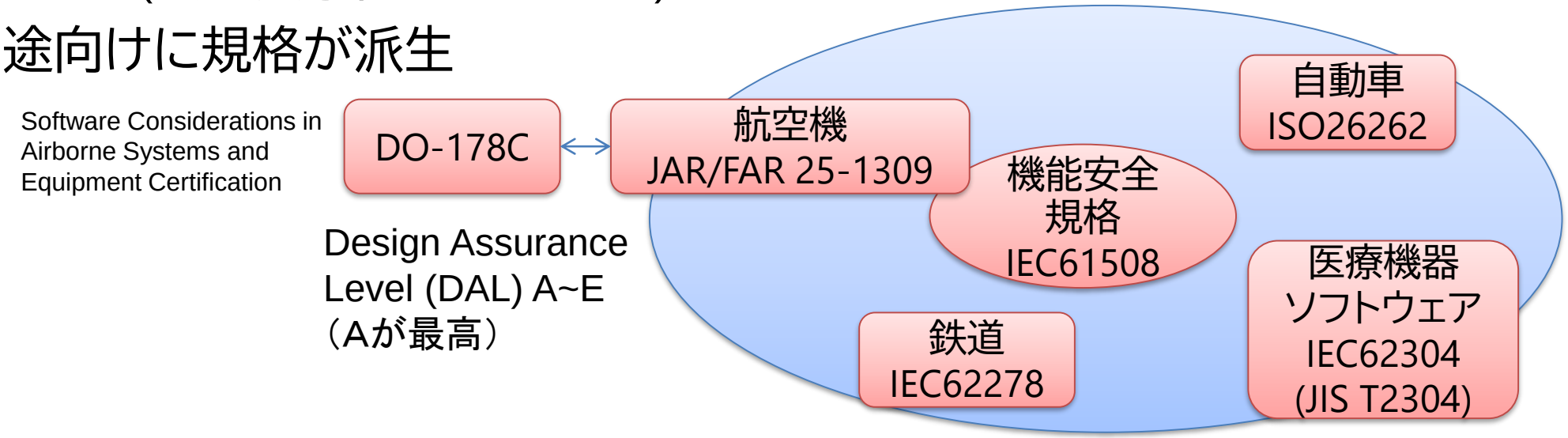
- 機能安全 (Functional safety)
  - 機能的な工夫により, 許容できるレベルの安全を確保すること
    - ◆対比: 本質安全：危害を及ぼす原因そのものを低減, 除去
- ALARP (As low as reasonably practicable)
  - リスクは合理的に実行可能な限り, できるだけ低くしなければならないという考え方

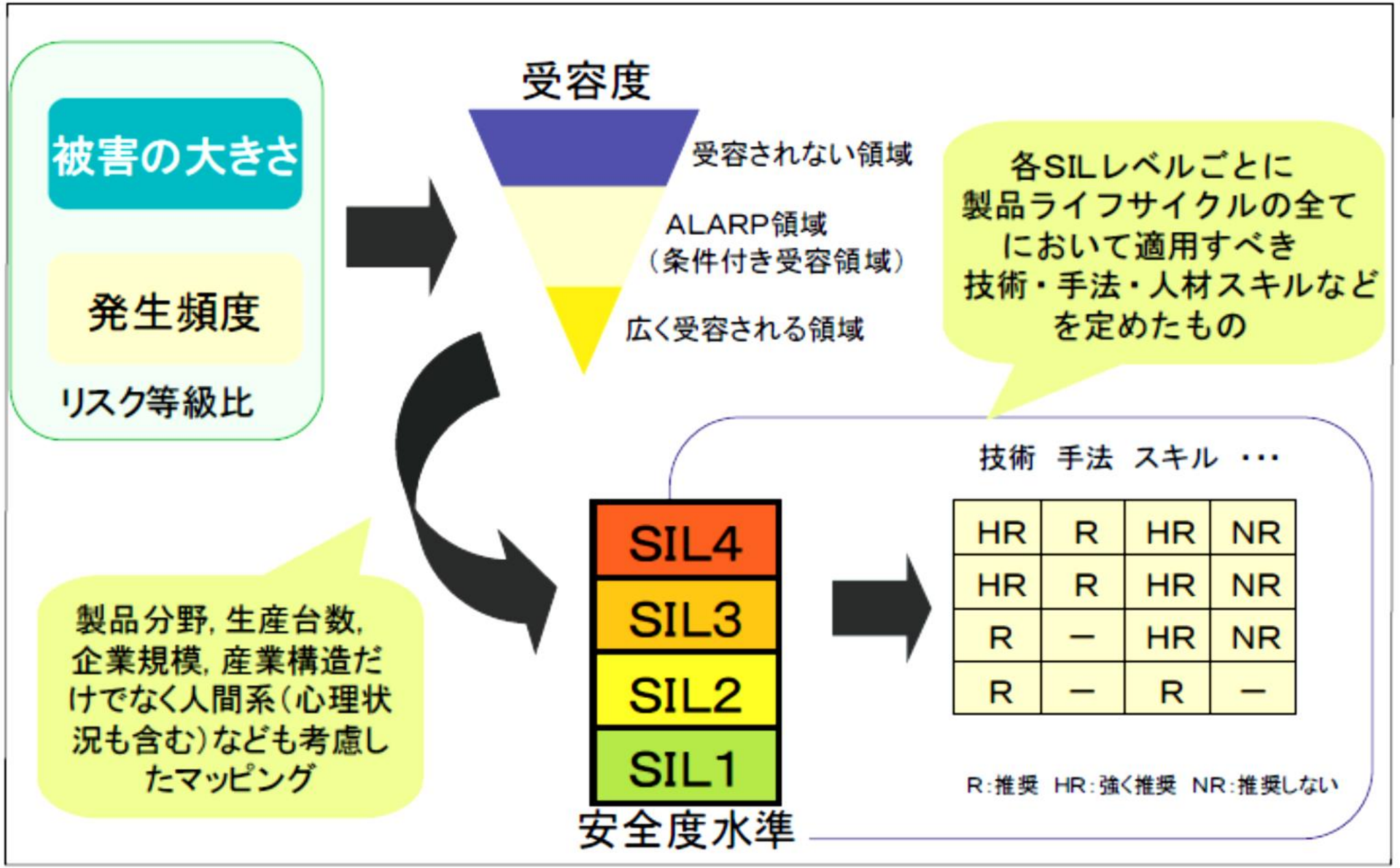


キャロット図

機能安全規格

- 安全を実現するための規格
- 例. IEC61508
  - 電気・電子・プログラマブル電子安全関連系の機能安全規格
  - 許容リスクを安全度水準 (SIL: Safety Integrity Level)として定義
    - ◆SIL 1 (安全要求低:単位時間障害確率10^{-5}～10^{-6})
      ～SIL 4 (安全要求高: 10^{-8}～10^{-9})
  - 各用途向けに規格が派生





引用：IPA, 組込みシステムの安全性向上の勧め, オーム社, 2006