資料3

機能安全とその要求水準の設定

安全度水準とパフォーマンスレベル

厚生労働省安全課

機能安全の導入の背景

- 機能安全とは
  - 電気･電子･プログラム可能電子制御の機能による安全方策
    - 安全関連システムに限定されたリスク低減方策（安全方策）
    - 機械的な安全方策に付加するもの（作動要求状態で必要となる機能）
- 背景
  - 設計仕様規定及び非関税障壁問題
    - 詳細な設計仕様に基づく各国の安全規格の統一が困難
    - 製品の定性的･定量的な安全性能に立脚した性能標準化
  - 事後安全計画の限界
    - 事故･災害の減少に伴い、事故を教訓にして再発防止対策を実施する事後安全対策が困難
  - 製品･システムの複雑化
    - 電子技術の進展による自動制御の複雑化
  - コンピューター制御（PLC)の導入
    - ソフトウエアを含めた安全関連システムに対する安全規格の必要性

危険な状態の多様性と機能安全の必要性

			潜在危険群（潜在危険の多様性）	
			相反潜在危険なし（単純なシステム）	相反潜在危険あり（複雑なシステム）
故障原因の予見性と不確実性	ランダムハードウェア故障	決定論的対応の吟味	アイテムの無秩序状態が安全側の場合、狭義のフェールセーフ技術適用の可能性を吟味する	個別の潜在危険に対しては決定論的対応が可能であっても、全体としては安全度水準（SIL）を基準にした対応が必要
		確率論的対応	アイテムの秩序状態維持が安全側となる場合は、安全度水準（SIL）を基準とした対応が必要	
	決定論的原因故障（想定外故障）		決定論原因故障に対する全安全ライフサイクル要求事項による対応が必要（手順・手続き論的対応）	

解説図 3－秩序性と安全／危険な状態

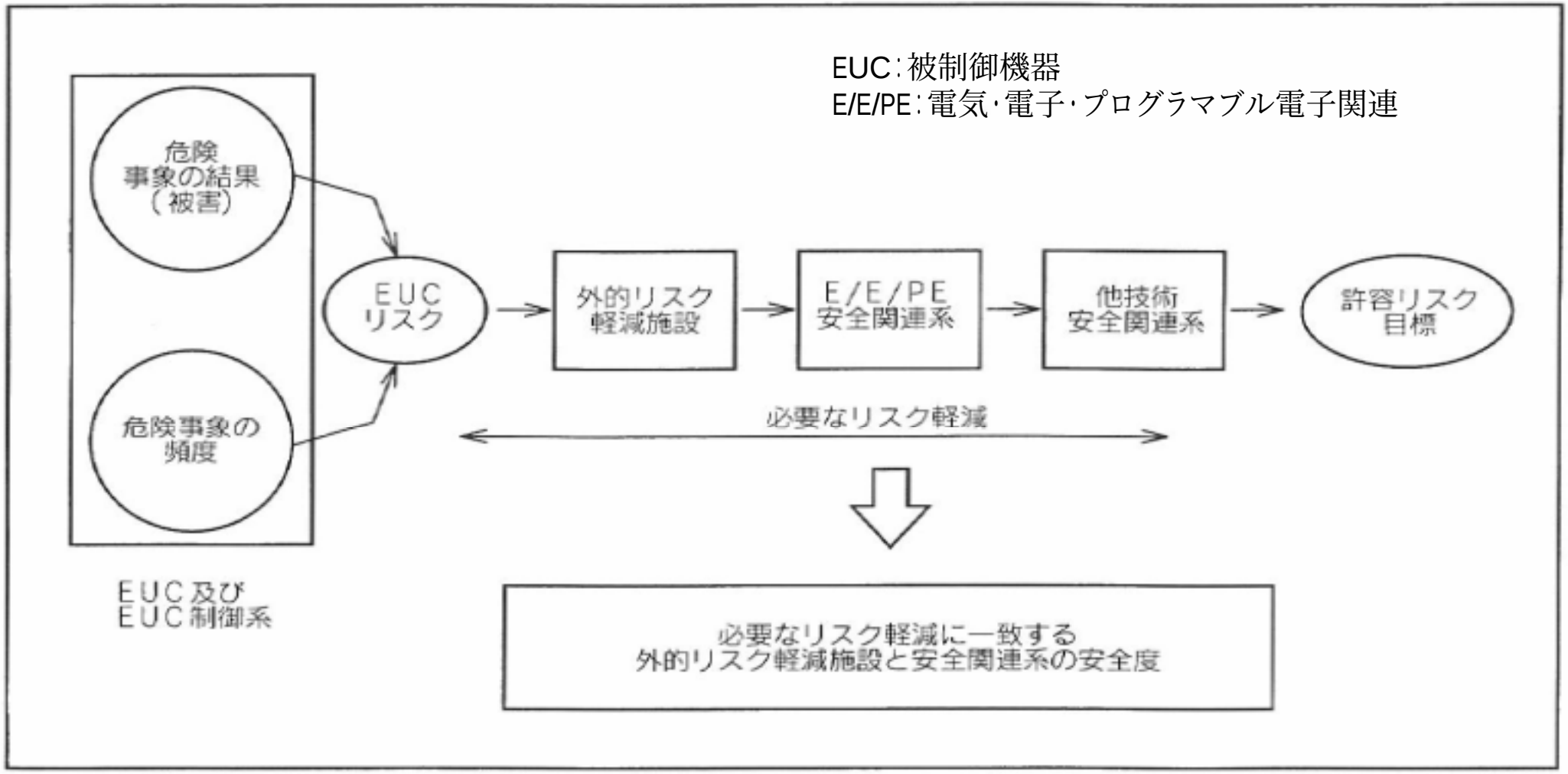
機能安全の導入について

- 国際規格での体系
  - ISO 12100 (基本安全規格)
  - IEC 61508 (グループ安全規格) の制定 (2000年)
    - 電気･電子･ソフトウエア制御による安全関連システムの機能安全の評価
  - IEC62061 (グループ安全規格) の制定 (2005年)
    - 機械類の機能安全の評価
  - ISO 13849-1 (グループ安全規格) の改定 (2006年)
    - 機械類での機能安全の評価
- 基本的考え方
  - ライフサイクルの基本的枠組みの構築
    - ライフサイクルのそれぞれの場面の安全性の尺度として、危害のリスクを用いる。
    - 従来の機械的な安全方策に加え、**安全関連システムの機能**により、リスクを許容可能な水準まで管理抑制
  - 定量的な評価尺度の採用
    - 機能安全によるリスク低減措置は、リスクに対応する確率論的な尺度で表わされる。

全ライフサイクルにおけるリスク低減
全安全ライフサイクル要求事項

- 潜在危険及びリスク解析
  - 合理的に予見される範囲内で、潜在危険、危険状態及び危険事象を明確化する。(HAZOPと呼ばれる場合もある。)
- 全安全要求事項 (要求安全度水準) の設定と割り当て
  - 必要な機能安全を達成するために、安全関連システムや他リスク低減措置の仕様を示し、安全度水準を割り当てる。
- 安全関連システムの安全要求仕様の設定と実現
  - 要求された機能安全が実現されるための仕様を定め、それを実現
- 他リスク低減措置の仕様及び実現
  - 他のリスク低減措置の仕様及びその実現
- 全安全妥当性確認
  - 全安全要求仕様を満たしているかを確認する

全ライフサイクルにおけるリスク低減



附属書A図2　リスク及び安全度の概念

電子・電気・ソフトウエア制御の機能
安全関連システム(safety related system)

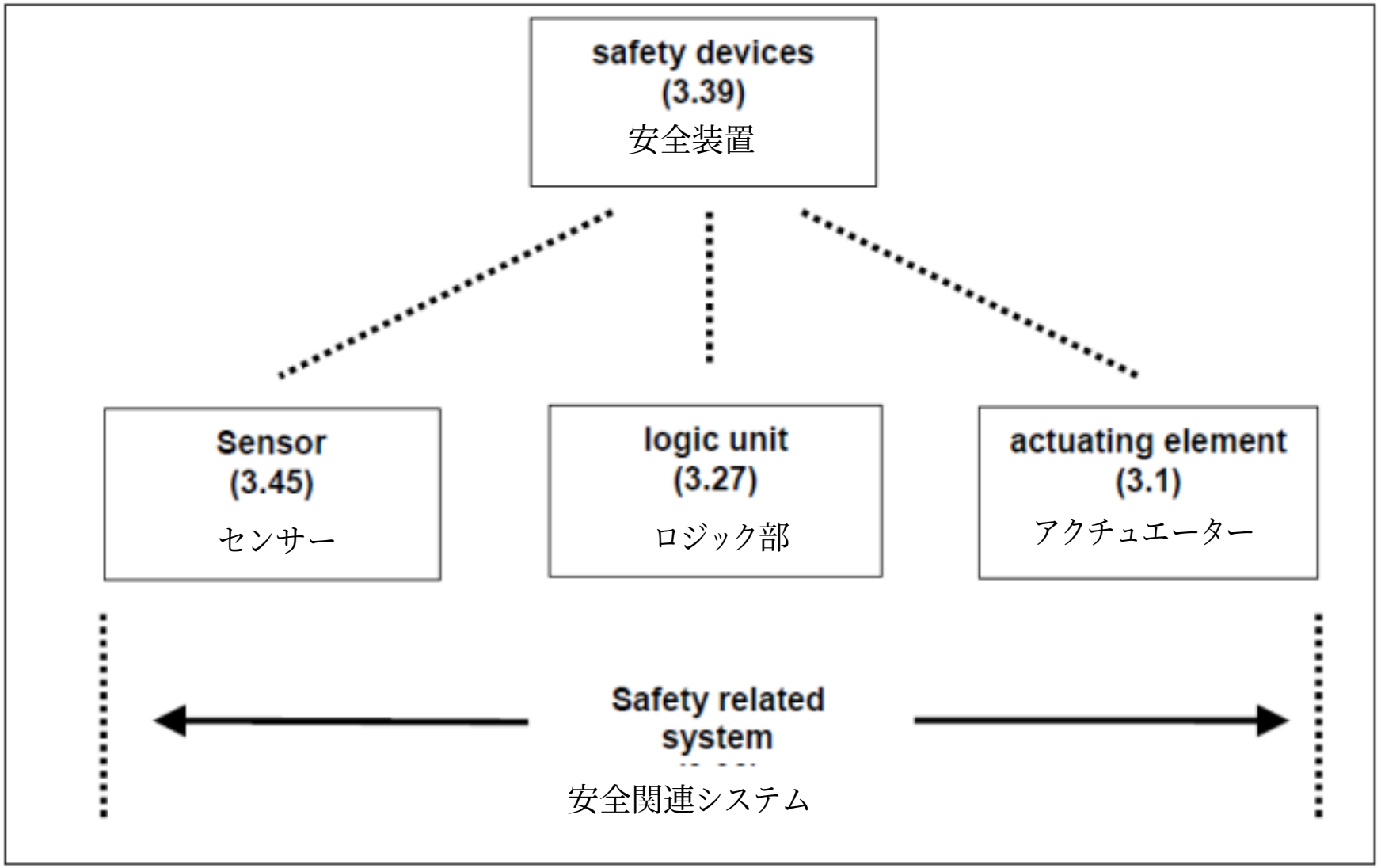


Figure 4 – Definition and components of a safety-related system

定量的な評価尺度

- 定量的な安全性能標準
  - 安全関連システムの機能によるリスク管理抑制の性能は、確率論的な尺度である**安全度水準** (safety integrity level: SIL) 又は**パフォーマンスレベル** (Performance level)によって表される。
- 安全度水準とは
  - IEC 61508 (グループ安全規格) の制定 (2000年)
  - 電気･電子･ソフトウエア制御による安全関連システムの機能安全の評価
- パフォーマンスレベルとは
  - ISO 13849-1 (グループ安全規格) の改定 (2006年)
  - 機械類での機能安全の評価

機能安全の評価尺度：
安全度水準（Safety Integrity level: SIL)

表 2－安全度水準（SIL）：低頻度作動要求モードで運用する E/E/PE 安全関連系に割り当てられる安全機能に対する目標機能失敗尺度

安全度水準	低頻度作動要求モード運用 （作動要求当たりの設計上の機能失敗平均確率） （PFDavg）
4	10^{-5} 以上 10^{-4} 未満
3	10^{-4} 以上 10^{-3} 未満
2	10^{-3} 以上 10^{-2} 未満
1	10^{-2} 以上 10^{-1} 未満

表 3－安全度水準（SIL）：高頻度作動要求又は連続モードで運用する E/E/PE 安全関連系に割り当てられる安全機能に対する目標機能失敗尺度

安全度水準	高頻度作動要求又は連続モード運用 安全機能の危険側失敗の平均頻度（PFH）［1/h］
4	10^{-9} 以上 10^{-8} 未満
3	10^{-8} 以上 10^{-7} 未満
2	10^{-7} 以上 10^{-6} 未満
1	10^{-6} 以上 10^{-5} 未満

機能安全の評価尺度：
パフォーマンスレベル（Performance level)

- 機械安全（ISO13849）による機能安全の尺度
- 安全度水準と同じく、確率で評価。（相互互換）

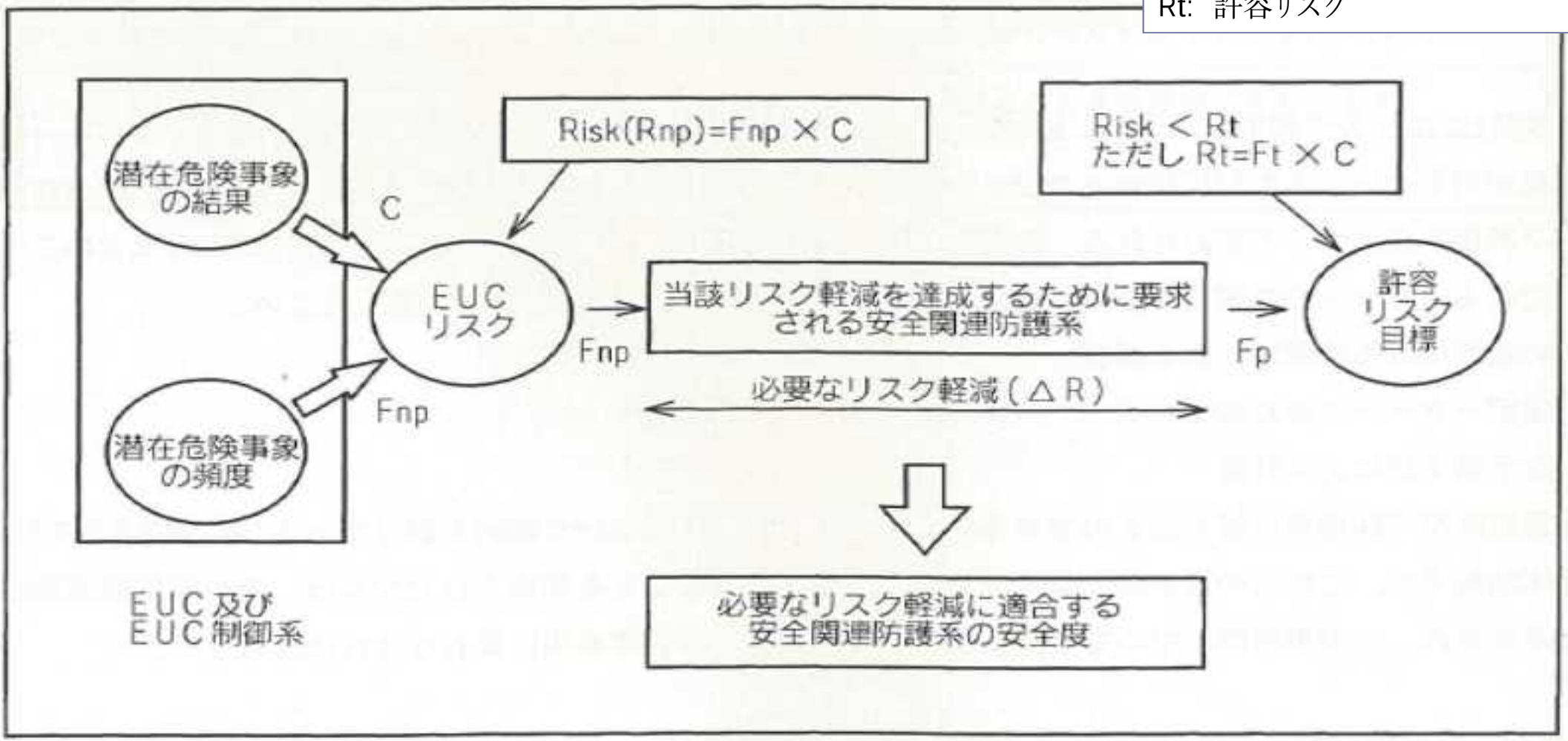
パフォーマンスレベル（PL)	安全度水準（SIL) 高／連続作動
a	-
b	1
c	2
d	3
e	4

要求安全度水準の設定

- 定量的評価
  - 許容リスクから、必要な低減リスクを計算する方法
    - 許容リスク（何分の１までリスクを低減すれば良いのか）を特定する必要がある。（実際は困難。）
- 定性的評価
  - リスクグラフ法
    - 事故の結果、頻度・曝露期間、危険回避可能性、望ましくない事象の発生頻度をパラメータとし、枝分かれ法により、要求安全度水準を決定
    - 最も広く行われている方法
  - 過酷度マトリクス法
    - 施設の数と苛酷度をパラメータとし、表形式で要求安全度水準を決定
    - 複数の機械等を設置する場合に使用される方法

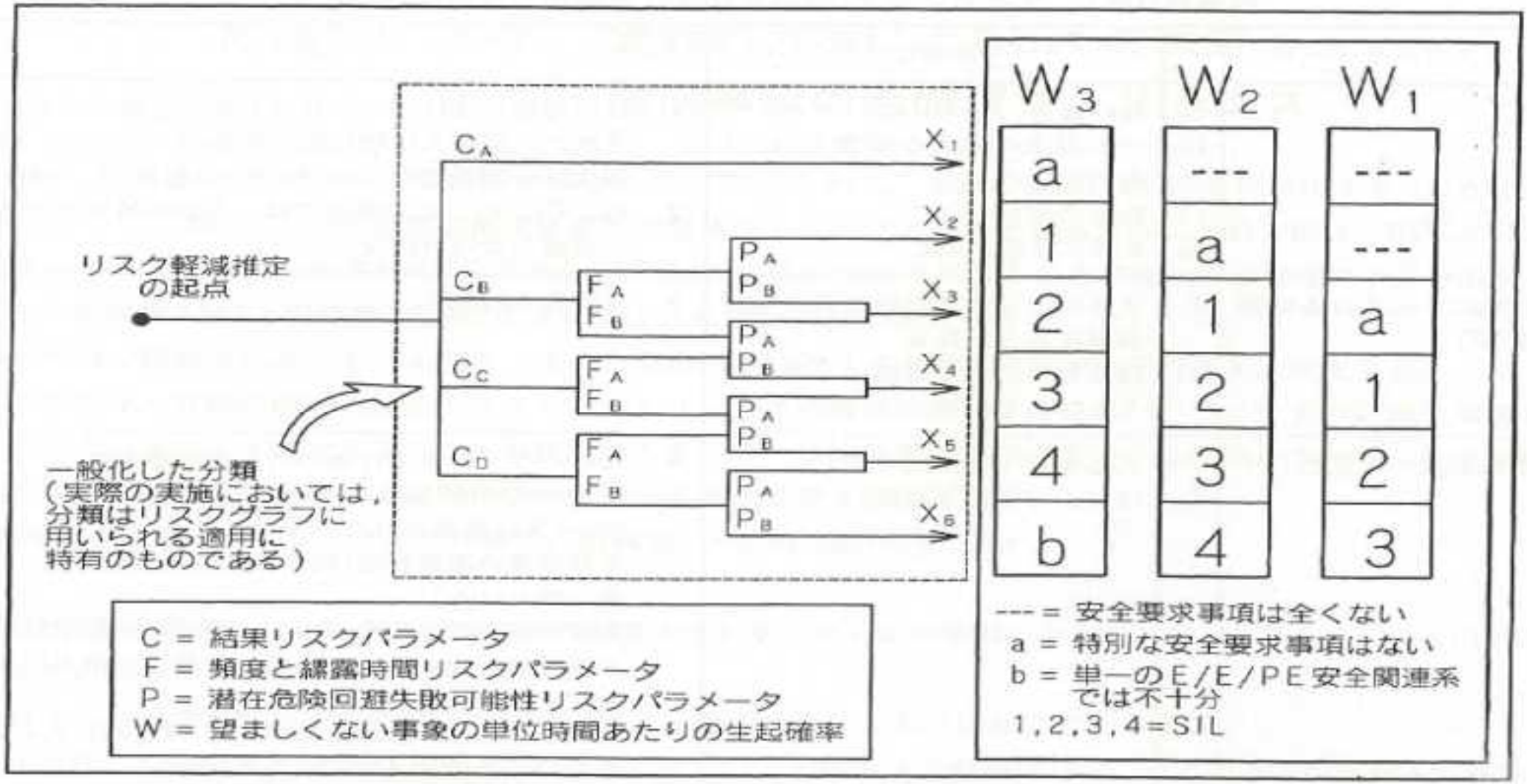
要求安全度水準の決定(定量的評価)

C: 危険事象の結果
EUC: 被制御機器
Fnp: 安全関連系の作動頻度
Fp: 防護策実行後のリスク頻度
Ft: 許容リスク頻度
Rt: 許容リスク



附属書C図1　安全度の割り当て：安全関連防護系の例

要求安全度水準の決定
（定性的評価①：リスクグラフ）



附属書D図1　リスクグラフ：一般的スキーム

リスク解析(HAZOP)・要求安全度水準決定（具体例）

キーワード	原因	結果/リスク	検知方法	ハザード防止対策	防止不能なハザード対策	C	F	P	W	SIL	製造者追加対策	設置者追加対策
蒸気圧力	消費側での蒸気排出の停止	熱交換器での圧力上昇	熱交換器圧力リミッター	リミッターによる熱源のシャットダウン	機械式安全弁	Cc	FA	-	W1	SIL2		
ボイラー水の水位	給水停止	過熱/空焚き	水位計	水位制御系による熱源シャットダウン	シャットダウン後の水位低下に対する設計余裕	Cc	FA	-	W1	SIL2	水位計に最低水位を明示	水位計の日常点検

結果(C)		曝露頻度(F)		回避可能性(P)		事象発生確率(W)	
CA	軽傷	FA	1日12時間以下	PA	一定程度可能	W1	非常に低い
CB	後遺障害	FB	1日12時間超	PB	困難	W2	低い
CC	死亡					W3	比較的高い
CD	複数死亡						