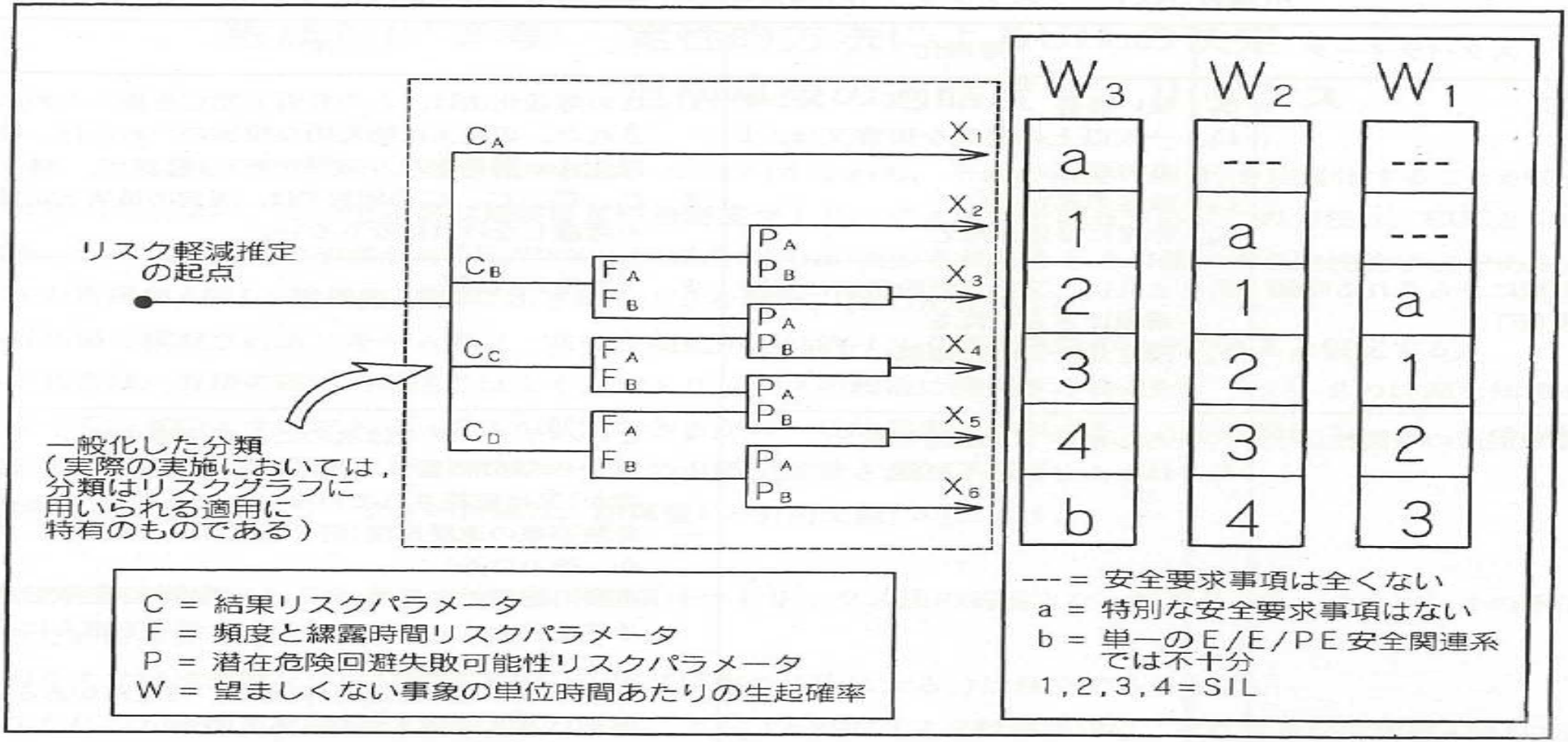
資料3

危険側故障確率の計算方法
IEC 61508-6による方法

厚生労働省安全課

要求安全度水準の決定（定性的評価：リスクグラフ）(IEC 61508-5)



附属書D図1　リスクグラフ：一般的スキーム

ISO 13849のリスクグラフには、Wがない。（高頻度モードを前提）

機能安全の評価尺度：
安全度水準（Safety Integrity level: SIL) (IEC 61508-1)

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

低頻度作動要求モード：安全機能が作動要求だけによって動作し、作動要求の頻度が１年当たり１回以下の場合
高頻度作動要求モード：安全機能が作動要求だけによって動作し、作動要求の頻度が１年当たり１回より大きい場合
連続モード：安全機能が通常運転の一環として被制御機器（EUC)を安全状態に保持する場合

（IEC 61508-4 3.5.16）

危険側故障確率（低頻度モード）(IEC 61508-6)

- 基本式
- $\mathrm{PFD}_{\mathrm{avg}} = \lambda_{\mathrm{DU}} \times \left(\frac{T_1}{2} + MTTR\right) + \lambda_{\mathrm{DD}} \times MTTR$
  - $\mathrm{PFD}_{\mathrm{avg}}$：作動要求当たりの機能失敗平均確率
  - λ_{DU}：検知できない危険側故障確率
  - λ_{DD}：検知できる故障側確率
    - 故障側確率は、平均故障時間の逆数
  - T_1：検査インターバル（proof test interval)
  - $MTTR$：平均修理時間（mean time to repare）
- 考え方
  - PFDというのは、安全関連システムが「**機能していない時間**」を「**運転時間（≈機能している時間）**」で除したもの。（安全関連システムが機能しない割合）
  - **検知できない危険側故障が発生した場合**、検査するまで機能しないので、**平均すると検査インターバルの半分の時間は機能しない**。それに、修理時間を加えたもの。
  - **検知できる故障が発生した場合**は、直ちに修理するので、修理時間だけが機能しない時間となる。

危険側故障確率：多重化した場合の計算例
(IEC 61508-6)

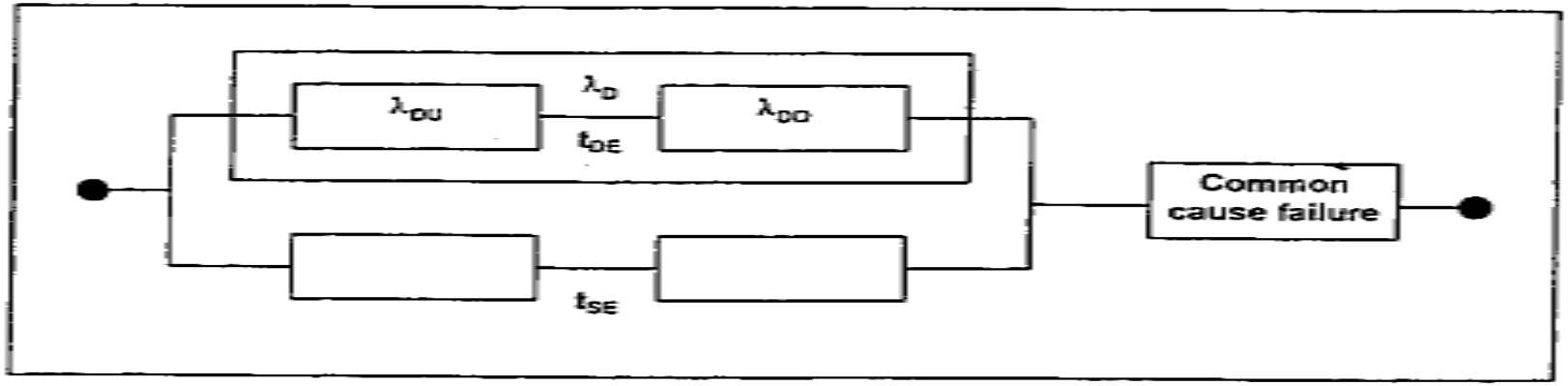


Figure B.7 — 1oo2 reliability block diagram

- $\mathrm{PFD}_{\mathrm{avg}} = 2[(1-\beta)\lambda_{\mathrm{DD}} + (1-2\beta)\lambda_{\mathrm{DU}}]^2 t_{DE} t_{SE} + 2\beta\lambda_{\mathrm{DU}}\left(\frac{T_1}{2} + MTTR\right) + \beta\lambda_{\mathrm{DD}} MTTR$
  - β ：危険側故障確率に占める共通原因故障(CCF)の割合
- PFDを下げる方策（安全方策）は、
  - PFDに占める割合が大きいのは、$2\beta\lambda_{\mathrm{DU}}\left(\frac{T_1}{2} + MTTR\right)$の部分。
  - 低減効果の大きいのは、①設計上の工夫により「共通原因故障の割合（β）」を減らす、②自己診断(self test)等によって、「検知できない故障確率（λ_{DU}）」を減らす③検査インターバル(T_I)を短くする、のいずれか
  - IECは、この手法を検討を設計者に全面的に委ね、数値計算により、安全度水準を決定する。
  - 一方、ISOはメニュー方式で、あらかじめ定められた選択肢の中から対策を選び、その組み合わせで、パフォーマンスレベルを決定する。

機械式安全装置と安全関連システムの関係（ボイラーの例）

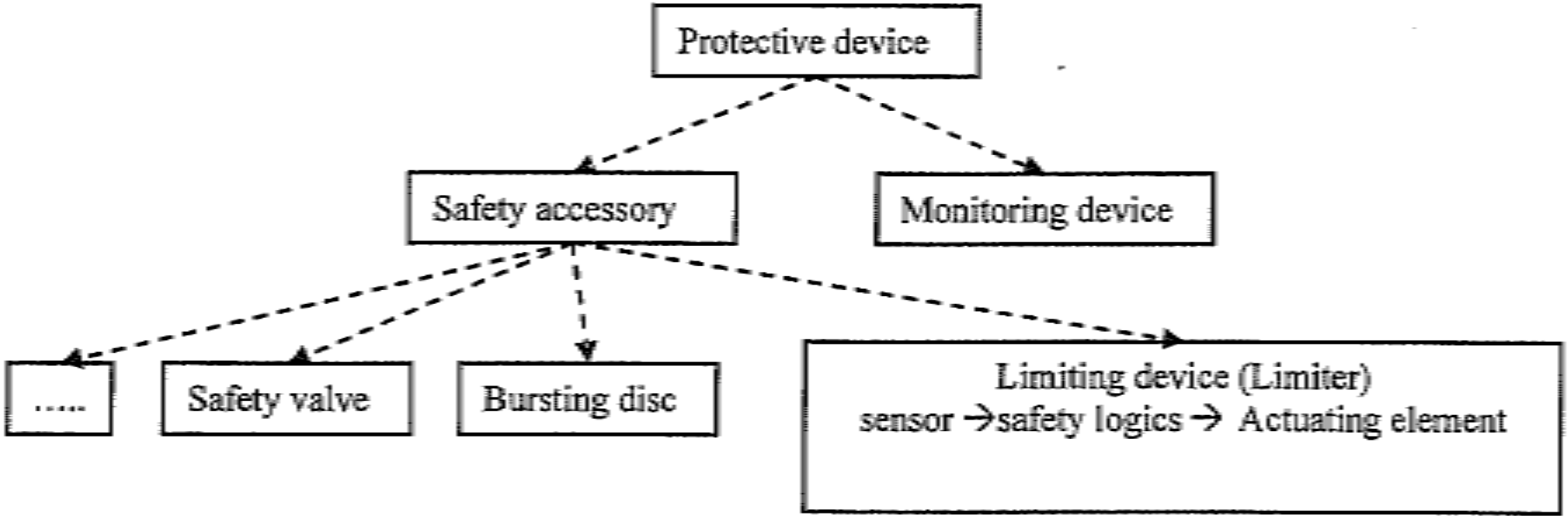


Figure 1 — Protective devices and safety accessories according to Directive 97/23/EC (PED)

- 電気・電子式の安全関連システムであるリミッターと、機械式安全装置である安全弁（safety valve)や破裂板（bursting disc)は並列になっており、省略は認められていない。
  - (EN 12953-11)