安全度水準やパフォーマンスレベルの計算方法

2015/12/24

長岡技術科学大学･システム安全専攻
福田　隆文

- この資料は規格に示されているＰＬあるいはＳＩＬの計算法の大まかな説明であるが、規格の理解のための手引きであったり、実際的な計算法のテキストではない。
- この資料内では、計算の前提などを記載していない。
- したがって、必要に応じて規格や解説書を参照することが必要である。

大まかな手順

- SIL、PLは安全関連系(SRS)･制御システムの安全関連部の作動信頼性(SRP/CS)の指標である
- 表題事項の大まかな手順は次のようになる

1. リスクアセスメント→必要な安全機能の決定
2. 必要な作動信頼性の決定
3. 安全関連系･制御システムの安全関連部の設計
4. 設計したものが2．を満たしていることの検討―SIL, PLの計算

1. リスクアセスメント→必要な安全機能の決定

押しつぶしの危険源	本体	設置されている状態	設置面が傾斜しており何らかの操作中に本体が転倒し、人が下敷きになる	誤使用	Ⅳ	B	Ⅱ	対策済み	仕様で水平に設置することを指示している。 取扱説明書で、設置面の傾斜限度・設置方法及び、運搬中の傾斜限度(15°)を指定する。					
	フタ開閉部、取っ手で引く部分	金材出し入れ	指を挟む	通常	Ⅱ	C	Ⅰ	必要	投入口カバーが所定位置にないと、油圧ポンプに給電されないようにする(※安全機能①, ②')	Ⅳ	C	Ⅱ		自動遮断にする？

どうやって移行するか　**安全機能**

現在の状態
(危険な状態)

どの程度確実に移行できるか　**PL(,SIL)**

安全な状態

リスクアセスメントにより同定

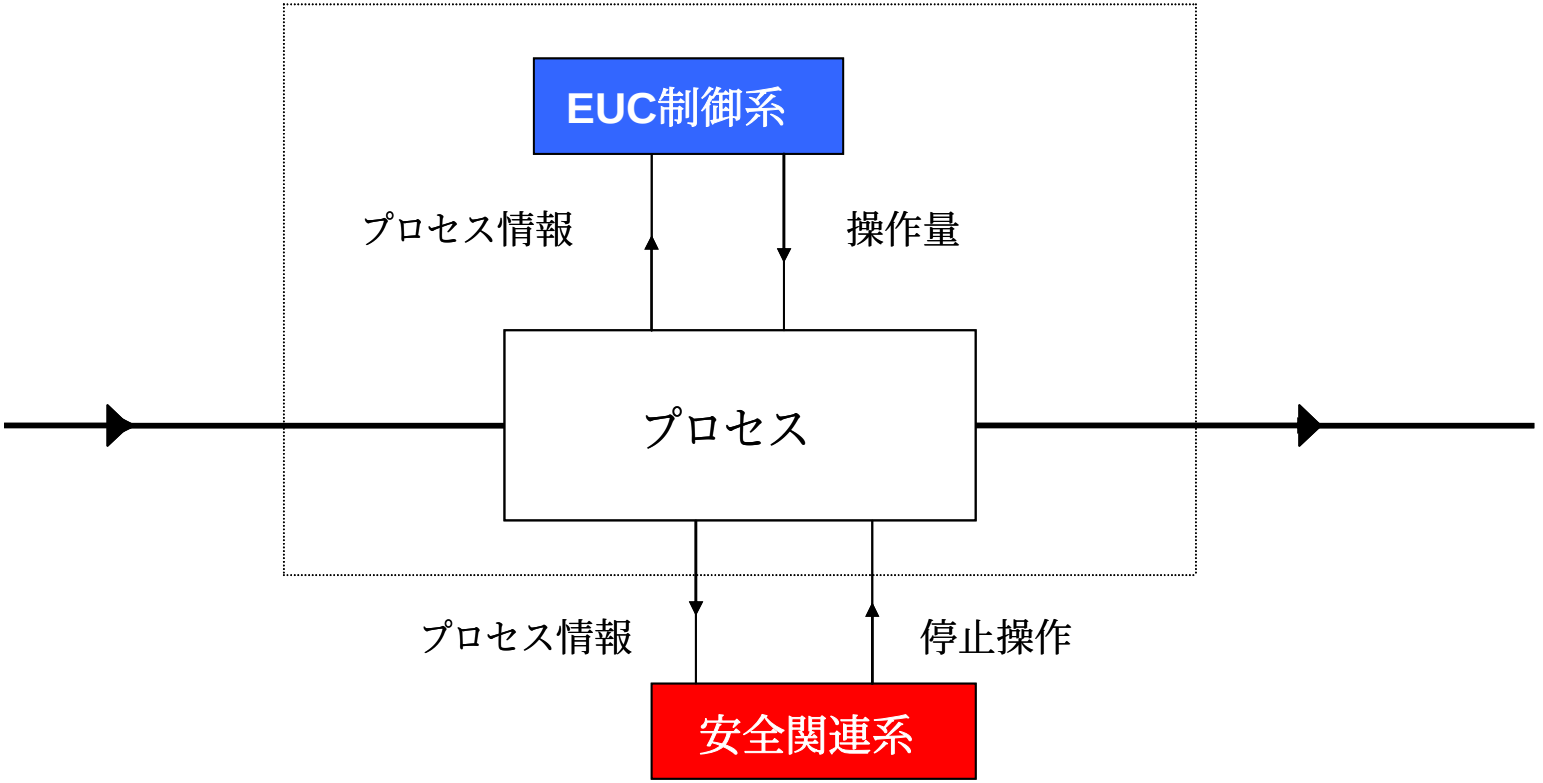
本質的安全設計方策　最小隙間の確保
安全防護　　プレス起動の両手押しボタン

リスクアセスメントにより同定

1.リスクアセスメント→必要な安全機能の決定

2.必要な作動信頼性の決定

- IEC61508　マトリックス法、リスクグラフ法
- IEC62061　マトリックス法
- ISO13849-1　リスクグラフ法



1.リスクアセスメント→必要な安全機能の決定

2.必要な作動信頼性の決定

3.安全関連系･制御システムの安全関連部の設計

4.設計したものが2．を満たしていることの検討―SIL, PLの計算

IEC61508	高頻度モード	故障率	
	低頻度モード	機能失敗確率	
IEC62061	高頻度モード	故障率	機械専用
ISO13849	高頻度モード	故障率	機械専用

SILとPLが比較できるのは共に故障率を使っているから。

- IEC61508のSIL計算は数学的に厳密
- IEC62061は機械に合わせて定型化
- ISO13849は標準構成を使用する前提で簡易化

- ISO13849　Performance Level (PL)

制御システムの安全関連部のPL
Performance Level

3.1.23 パフォーマンスレベル，PL（performance level）

予見可能な条件下で，安全機能を実行するための制御システムの安全関連部の能力を規定するために用いられる区分レベル。

注記 4.5.1 参照

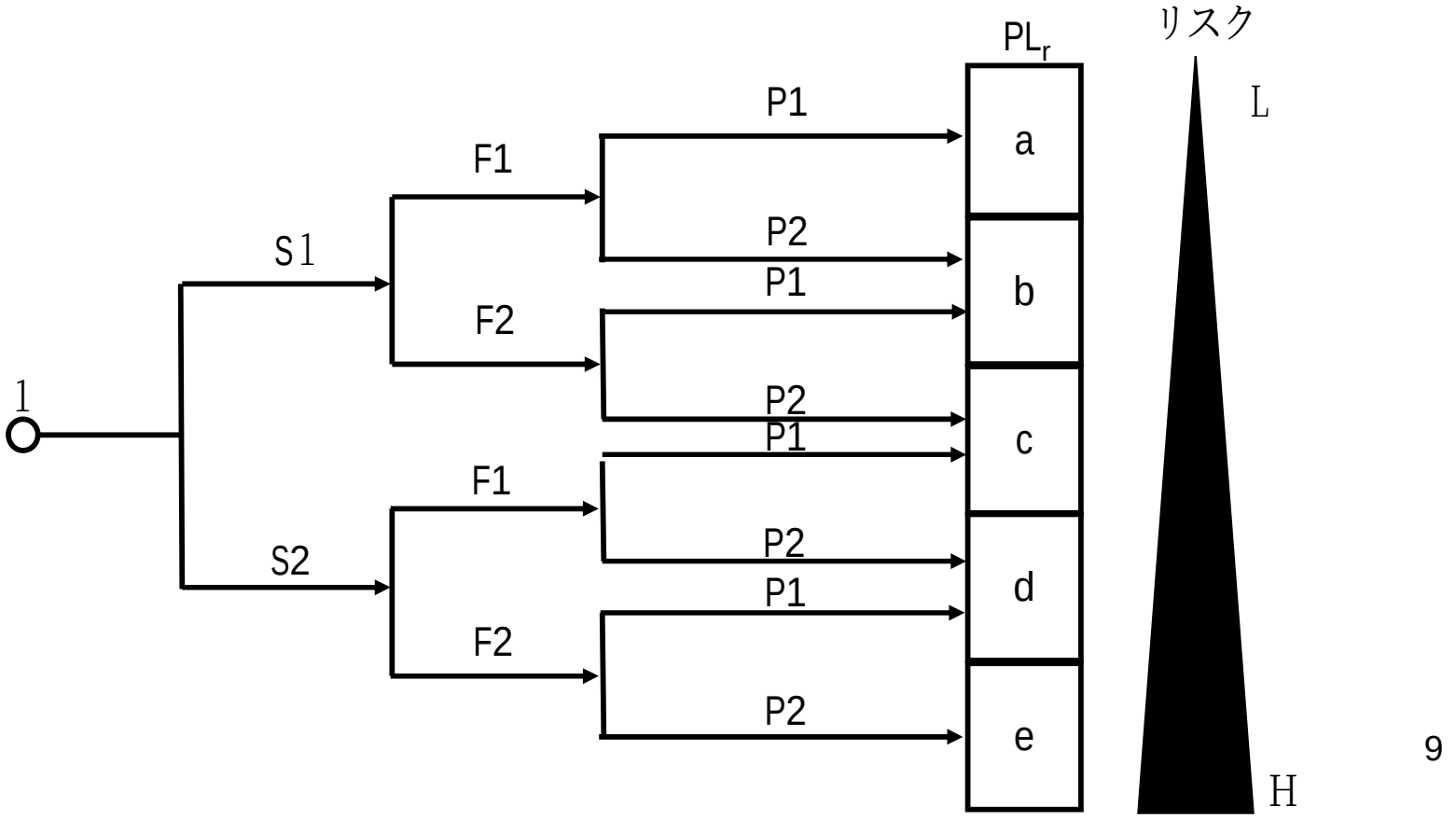
3.1.24 要求パフォーマンスレベル，PLr（required performance level）

安全機能の各々に対し，要求されるリスク低減を達成するために適用されるパフォーマンスレベル。

PL	1時間あたりの危険側故障の平均確率　1/h
a	$\geqq 10^{-5} \sim < 10^{-4}$
b	$\geqq 3\times 10^{-6} \sim < 10^{-5}$
c	$\geqq 10^{-6} \sim < 3\times 10^{-6}$
d	$\geqq 10^{-7} \sim < 10^{-6}$
e	$\geqq 10^{-8} \sim < 10^{-7}$

PLrの決定

- PLr: Required Performance level 要求パフォーマンスレベル　制御システムの安全関連部が有すべきPL
- 危害の大きさと暴露頻度･回避可能性から決定

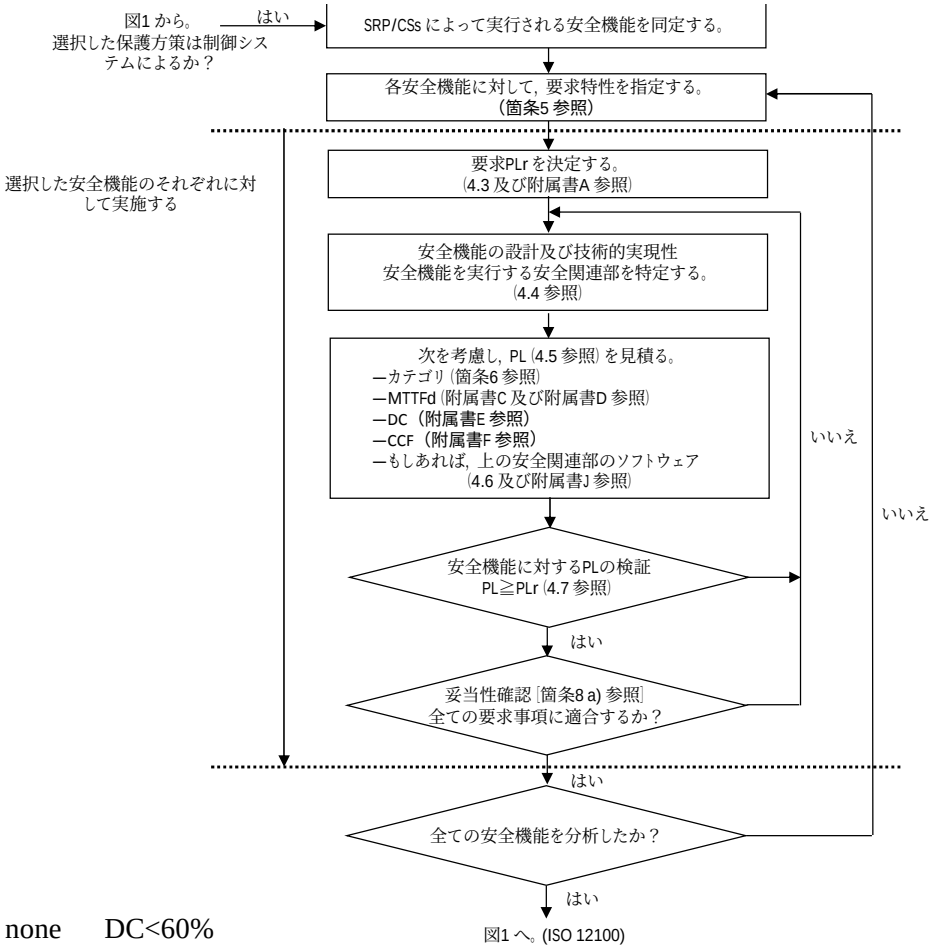


制御システムの安全関連部のPL
Performance Level

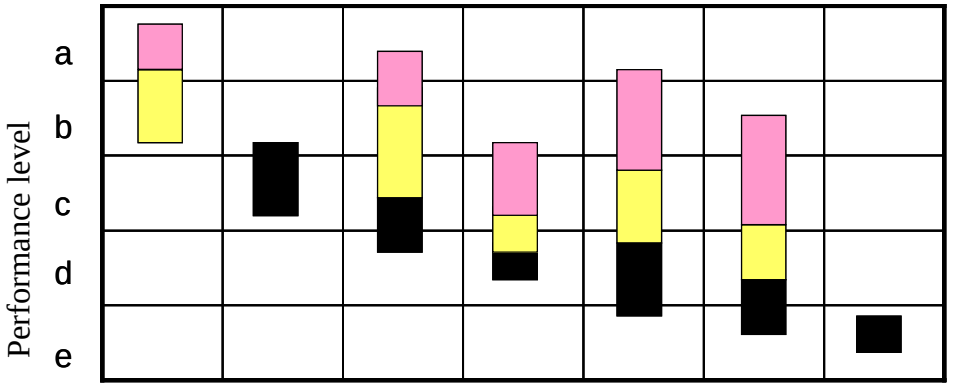
- 定義は故障率に寄る区分であるので、回路などと各要素の故障率等から厳密に求めてもよい。
- しかし、機械の場合、次ページから説明する方法で求めることが多い（。厳密に求めた例を見たことがない。）

PL	1時間あたりの危険側故障の平均確率　1/h
a	$\geqq 10^{-5} \sim < 10^{-4}$
b	$\geqq 3\times 10^{-6} \sim < 10^{-5}$
c	$\geqq 10^{-6} \sim < 3\times 10^{-6}$
d	$\geqq 10^{-7} \sim < 10^{-6}$
e	$\geqq 10^{-8} \sim < 10^{-7}$

PL決定のパラメータ



で，妥当性確認のための追加的支援策が示される。



none DC<60%

low 60%s≦DC<90%

medium 90%≦DC<99%

high 99%≦DC

Cat.	B	1	2	2	3	3	4
DC	none	none	low	medium	low	medium	high

各チャネルの*MTTFd* =low 3years≦*MTTFd* <10years

各チャネルの*MTTFd* =medium 10years ≦*MTTFd* <30years

各チャネルの*MTTFd* ＝high 30years ≦*MTTFd* <100years

指定アークテクチャ

4.5.1

PL の定量化の側面の査定をより容易にするために，この規格は，特定の設計基準及び障害条件下での挙動を満たす5 通りの指定アーキテクチャを定めることによって，単純化した方法を示す（4.5.4 参照）。

指定アーキテクチャから逸脱するSRP/CS に対しては，要求パフォーマンスレベルPLr の達成を証明するための詳細な計算を示さなければならない。

4.5.4

指定アーキテクチャに対しては，次の代表的な仮定がなされる。

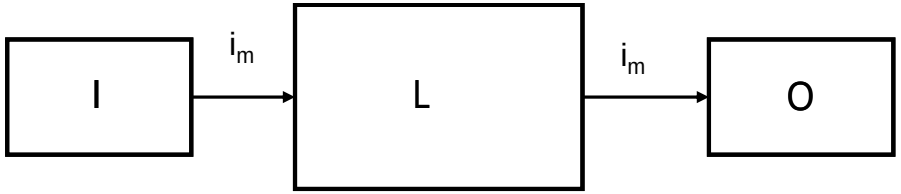
— 使命時間，20 年（箇条10 参照）

— 使命時間内での定故障率

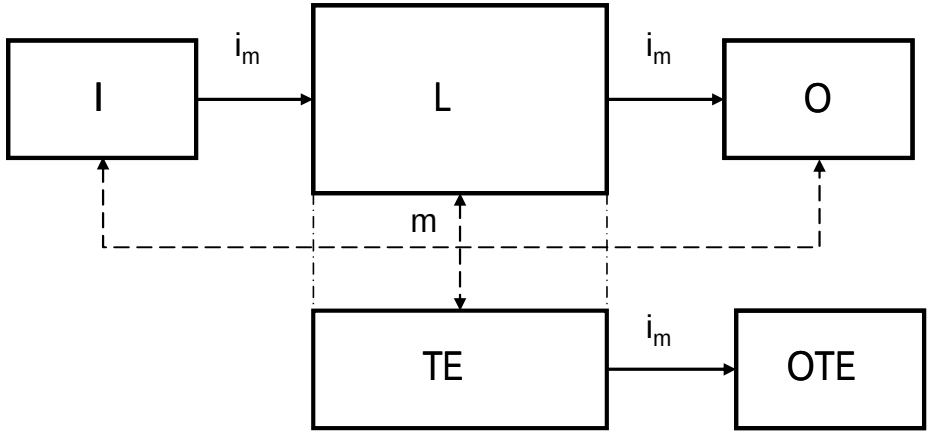
— カテゴリ2，動作要求率≦1/100 の診断試験率（for category 2, demand rate ≦ 1/100 test rate）

— カテゴリ2，MTTFd, TE は，MTTFd, L の1/2 より大きい

B/1

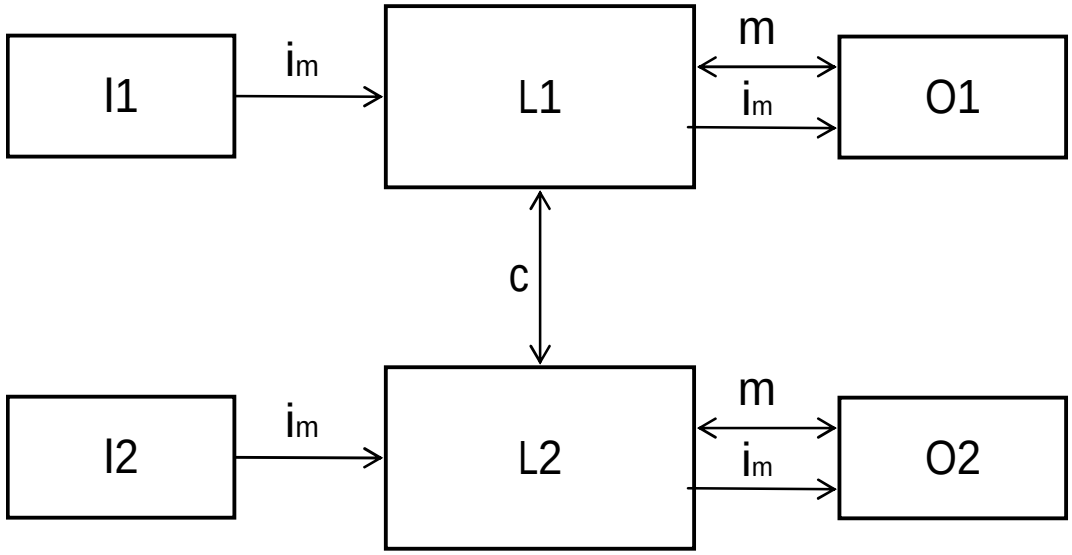


2



3

4



MTTFd	
各チャネルの指定表示	各チャネルの範囲
“低”	3年≦MTTFd＜10 年
“中”	10年≦MTTFd＜30 年
“高”	30年≦MTTFd＜100 年

注記1 各チャネルのMTTFd の範囲選択は，現在の技術水準としてその分野で見られる故障率に基づいており，PL のログスケールに対応して類似のログスケールを形成する。3 年未満の各チャネルのMTTFd 値は，現実のSRP/CSで起こり得るということは予想していない。市場の全てのシステムのうちおよそ30 %が，1 年後に故障し，かつ，取り替えることになるということを意味するからである。100 年を超えるの各チャネルのMTTFd 値は，受け入れ不可能である。理由は，高リスク対応のSRP/CS は，コンポーネントの信頼性だけに依存しないほうがよいからである。システマティック故障及びランダム故障に対してSRP/CS を強化するためには，冗長系，かつ，試験付きのような追加手段を必要とすることが望ましい。実用的には，MTTFd の範囲は，3 通りに制限される。各チャネルにおけるMTTFd 値を最大100 年に制限することは，安全機能を実行する当該SRP/CS の単一チャネルに対して適用される。より高いMTTFd 値は，単一コンポーネントで使用することができる（表D.1 参照）。

注記2 この表の各チャネル間のしきい値は，5 %の誤差範囲内を想定している。

各チャネルのＭＦＦＴｄの推定法

パーツ･カウント･メソッド

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{d_i}}$$

$MTTF_d$ ：1チャネル全体の平均危険側故障率

$MTTF_{d1}, MTTF_{d2}$ ：安全機能に寄与する各コンポーネントのMTTFd

◎　この式は、各要素が直列系をなしていると考えて導出される。規格では、「あるチャネル内のコンポーネントの危険側故障がそのチャネル全体の危険側故障を導くという仮定に基づいている」と記している。

異なるチャネルに対するMTTFd と，各チャネルのMTTFd の対称化

6.2 の指定アーキテクチャは，冗長のSRP/CS における異なるチャネルについて，**各チャネルのMTTFdの値が同じであることを仮定している**。このチャネルごとの値を，図5 の入力データにすることが望ましい。チャネル間のMTTFd が異なる場合には，次の二つの可能性がある。

― 最悪の場合の仮定として，低い方の値を考慮することが望ましい，又は

― MTTFd の代用値の見積りとして，**式(D.2)**を使用する。

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right]$$

DC	
各チャネルの指定表示	各チャネルの範囲
“なし”	DC＜60 %
“低”	60 %≦DC＜90 %
“中”	90 %≦DC＜99 %
“高”	99 %≦DC

注記1 複数の部分で構成されるSRP/CS ではDC に対して，平均のDC（DCavg）を，図5，箇条6 及び附属書E のE.2 に示すように使用する。

注記2 DC の範囲の選択は，60 %，90 %及び99 %のキー値に基づく。これは試験の診断範囲を扱う他の規格（例えば，IEC 61508 規格群）でも設定される。特徴として，DC 自体ではなく（100－DC）%の計測の方が試験の効果に対して有効であるということが，調査によって示される。キー値の60 %，90 %及び99 %に対する（100－DC）%は，PL のログスケール対応の類似のログスケールを形成する。60 %未満のDC 値は，試験のシステムの信頼性に関して僅かな効果しか有しない。したがって，“なし”とする。複雑なシステムに対する99 %以上のDC 値は，達成することが困難である。実用的には，範囲数は，4 通りに制限される。この表の各DC のしきい値は，5 %の誤差内を想定する。

$$DCavg = \frac{\sum_{1}^{n} \frac{DC_i}{MTTF_{di}}}{\sum_{1}^{n} \frac{1}{MTTF_{di}}}$$

CCF

3.1.6　共通原因故障［common cause failure (CCF)］

単一の事象から生じる異なったアイテムの故障であって，これらの故障が互いの結果ではないもの。（IEC 60050-191 Amd. 1 の04-23 参照）

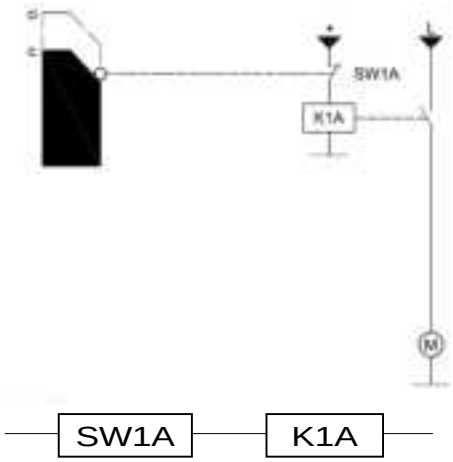
具体的には附属書Fに従い、スコアーを計算する。

No.	CCFに対する方策	Score
1	分離/隔離	
	信号経路間の物理的な分離 配線/配管での分離,プリント基板上での回路間の十分なクリアランス及び沿面距離	15
2	多様性(ダイバーシティ)	
	異なる技術的方式/設計又は物理的原理の使用。 始動の種類,圧力及び温度,距離及び圧力の測定,デジタル及びアナログ,異なる製造業者によるコンポーネント	20
3	設計/適用/経験	
3.1	過電圧,過圧力,過電流などに対する保護	15
3.2	使用のコンポーネントは,”十分に吟味されている”	5
4	査定/分析	
	設計上での共通原因故障を回避するために,故障モード影響解析(FMEA)の結果を考慮しているか。	5
5	適格性(能力)/訓練	
	設計者/保全者は,共通原因故障の原因及び結果を理解できるように訓練されているか。	5
6	環境面	
6.1	適切な規格に従ったCCFに対する汚染防止及び電磁両立性(EMC) 流体システム：圧力媒体のろ過,ほこりの侵入の防止,圧縮空気の水抜き 電気システム：システムは,電磁イミュニティに関してチェックされているか。	25
6.2	他の影響 温度,衝撃,振動,湿度などの環境関連の影響の全てに対してイミュニティの要求事項を考慮しているか。	10
	Total	100

Total score	Measures for avoiding CCF
65 or better	Meets the requirements
Less than 65	Process failed → choose additional measures

MTTFの計算でPLを求める例 ー 附属書I

附属書I I.3 単一チャネルシステム



ー MTTFd

K1A＝50 年　SW1A＝20 年　製造業者提示値

$$\frac{1}{MTTF_d} = \frac{1}{20} + \frac{1}{50} = 0.07$$

→ MTTFd=14.3年 → チャネルのMTTFdは“中”

ー DC（診断範囲）

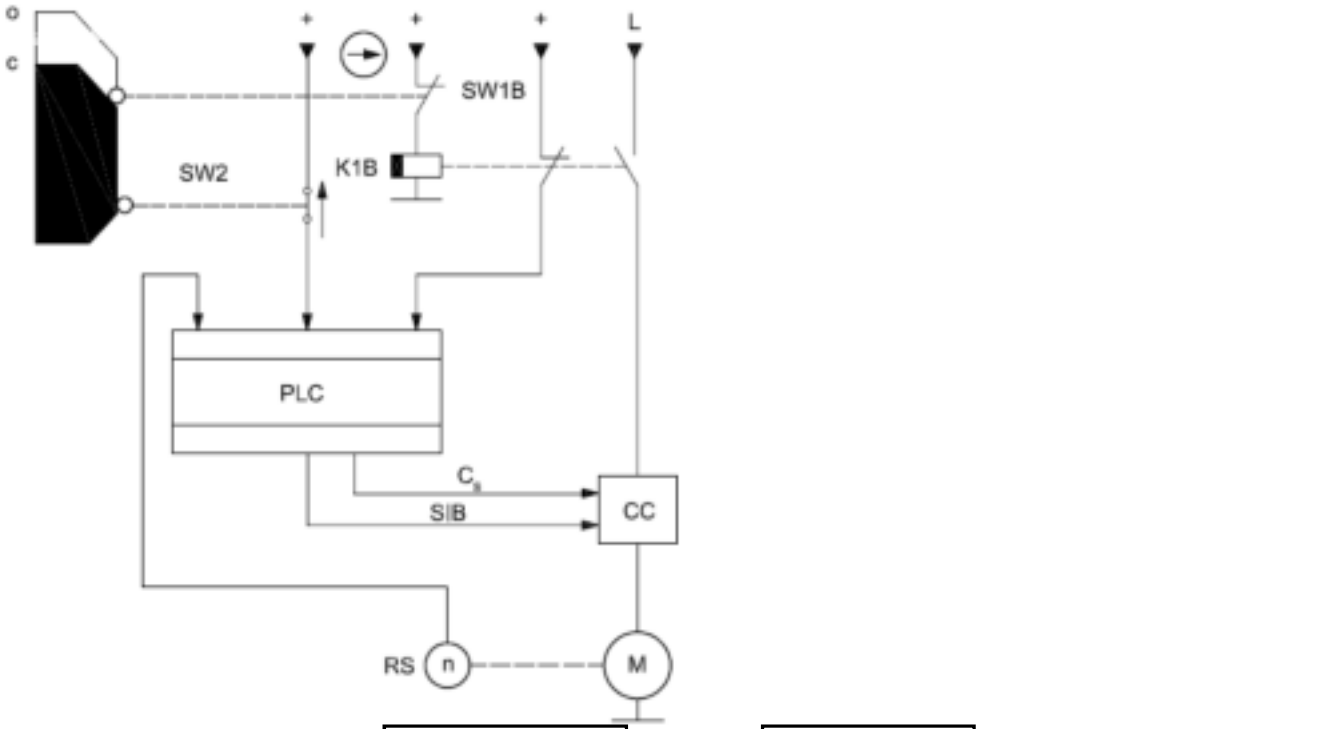
制御回路A では機能試験は不在なので，表6 に従って，DC＝0，又は“なし”となる。

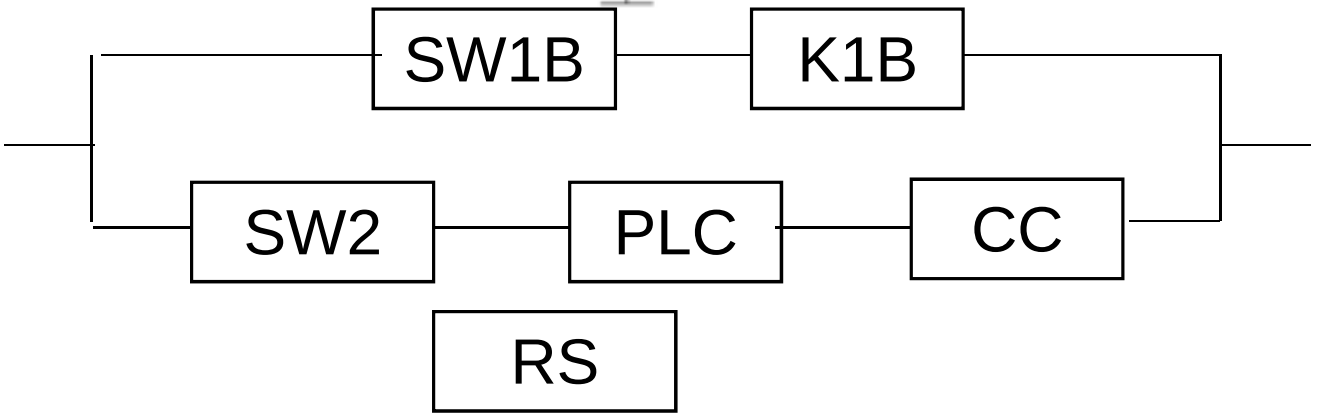
ー カテゴリ

この回路の推奨カテゴリは，カテゴリ1 であるが，チャネルのMTTFd は“中” → **カテゴリB** だけが達成可能 → **PL＝b**

例題

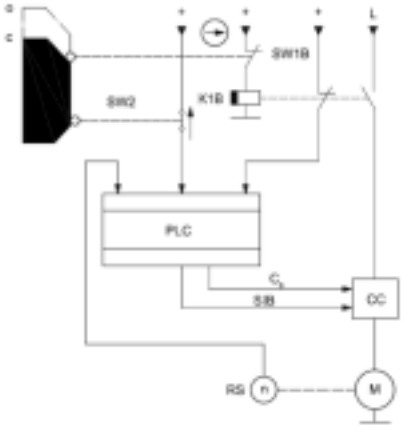
附属書I I.4 冗長システム

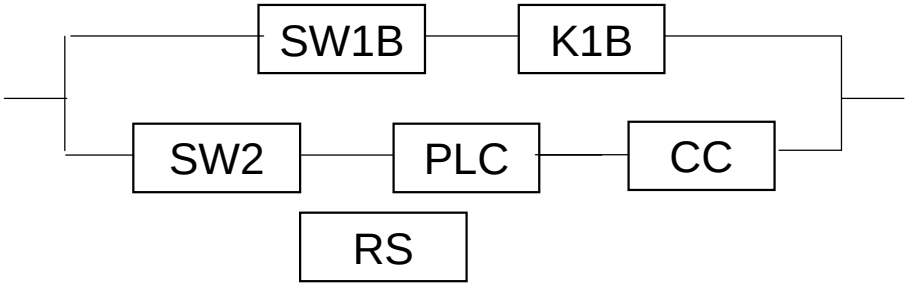




例題

附属書I I.4 冗長システム





ch1 $\frac{1}{MTTF_{dch1}} = \frac{1}{30} \rightarrow MTTF_d = 30$ 年

ch2 $\frac{1}{MTTF_{dch2}} = \frac{1}{20} + \frac{1}{20} + \frac{1}{20} = \frac{1}{6.7} \rightarrow MTTF_d = 6.7$ 年

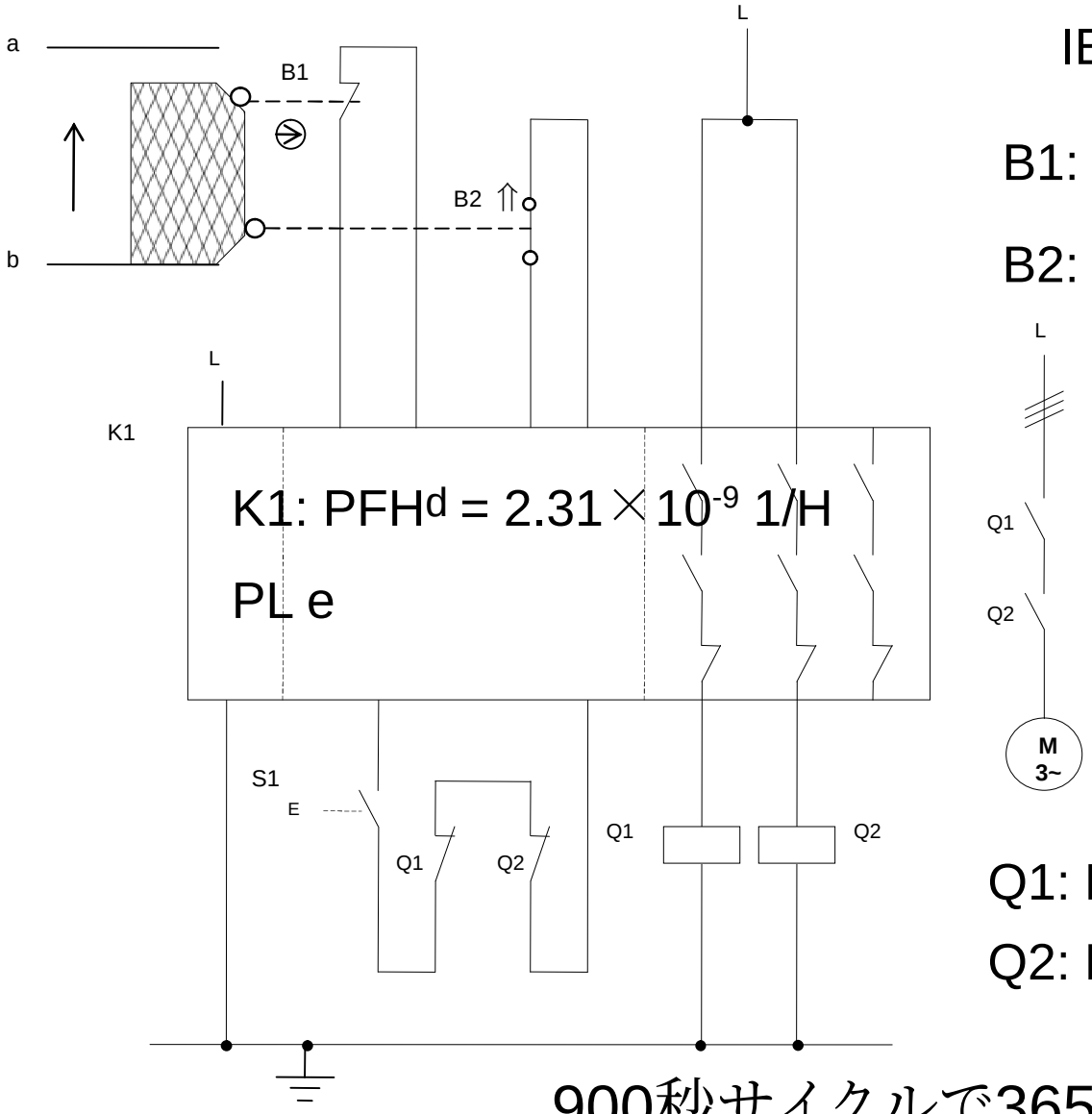
$MTTF_d = \frac{2}{3}\left\{30 + 6.7 - \frac{1}{\frac{1}{30}+\frac{1}{6.7}}\right\} = 20.8$ 年 $\rightarrow MTTF_d =$ 中

$DC_{avg} = \frac{\frac{0.99}{30}+\frac{0.6}{30}+\frac{0.3}{20}+\frac{0.9}{20}}{\frac{1}{30}+\frac{1}{30}+\frac{1}{20}+\frac{1}{20}} = 0.67$ 年 $\rightarrow$ 67% 低

PL=C

附属書Kを使ってPLを求める例 ― IEC/TR 62061-1の8.の例

IEC/TR62061-1:2010より引用



B1: B10d=1 000 000 cycle

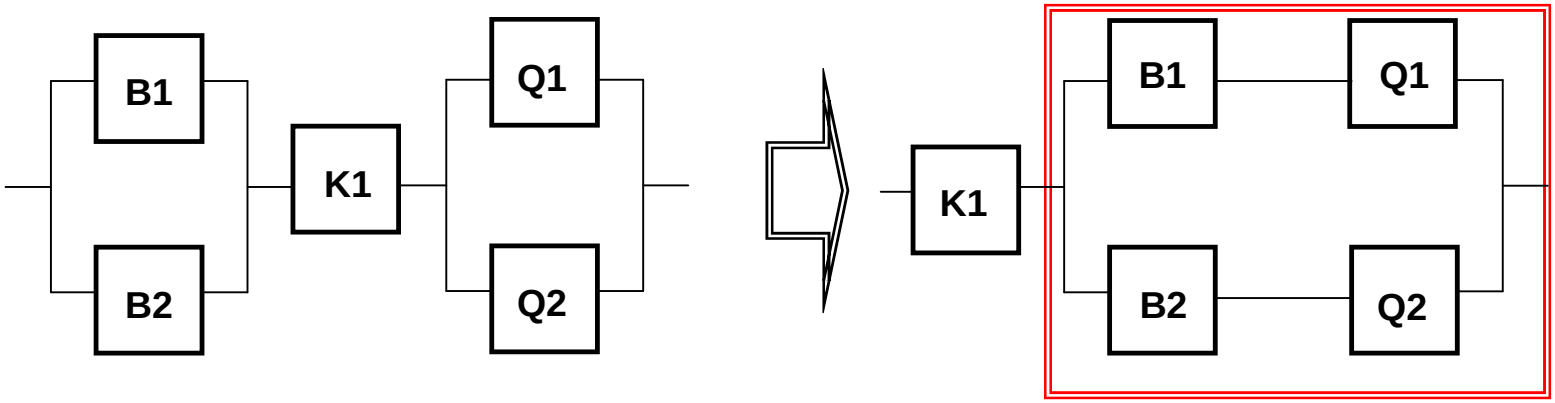
B2: B10d=500 000 cycle

Q1: B10d=2 000 000 cycle

Q2: B10d=2 000 000 cycle

900秒サイクルで365日24時間稼働する →

年間35040回開閉される　nop=35040



電気的な接続　　等価な論理的な接続

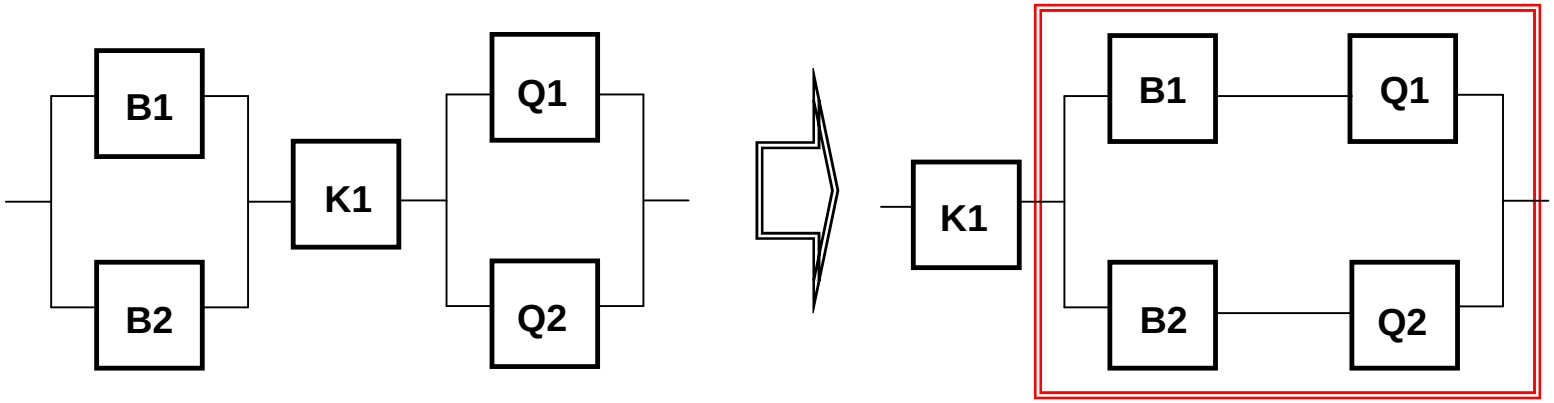
MTTFd B1=1000000/(0.1×35040)=285年

MTTFd B2=500000/(0.1×35040)=143年

MTTFd Q1=2000000/(0.1×35040)=571年

MTTFd Q2=2000000/(0.1×35040)=571年

$$MTTFch1 = \frac{1}{\frac{1}{285}+\frac{1}{571}} = 190 \longrightarrow 100 \qquad MTTFch2 = \frac{1}{\frac{1}{143}+\frac{1}{571}} = 114 \longrightarrow 100$$



電気的な接続　　等価な論理的な接続

チャネル1,2共に100年　－－＞　系としても100年

B1,B2のDCは99%　　もっともらしさチェック

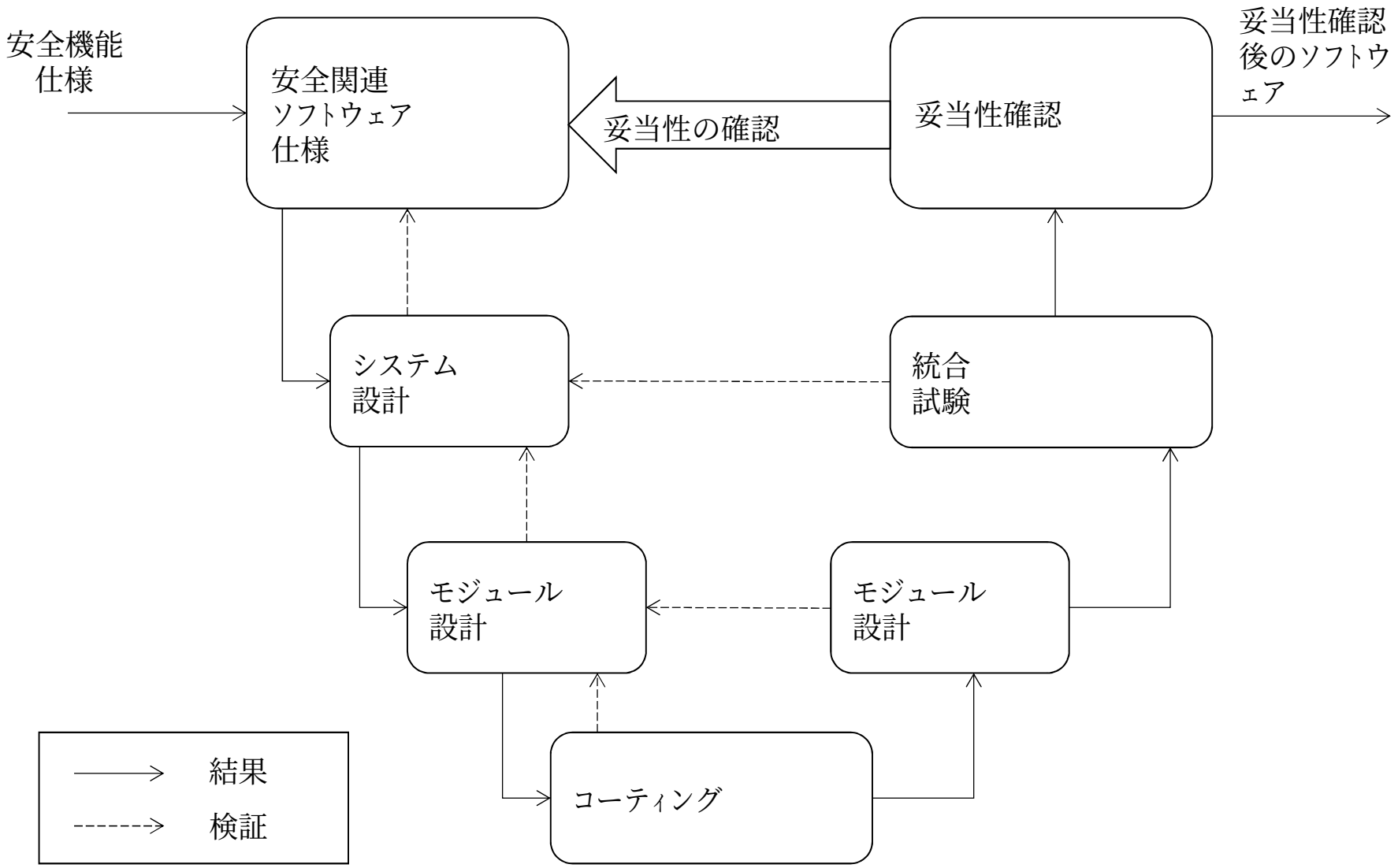
Q1,Q2のDCは99%　　バック接点による監視

DCavg=99%

PL e　－－＞　PFHd=2.47×10^{-8} 1/H

PFHd = 2.47×10^{-8}＋ 2.31×10^{-9} =　2.70×10^{-8}　1/H　　PL e

ソフトの開発



注記　附属書Jに、ライフサイクル活動に対してより詳細な推奨事項を示す。

図6－ソフトウェア安全ライフサイクルの単純化Vモデル

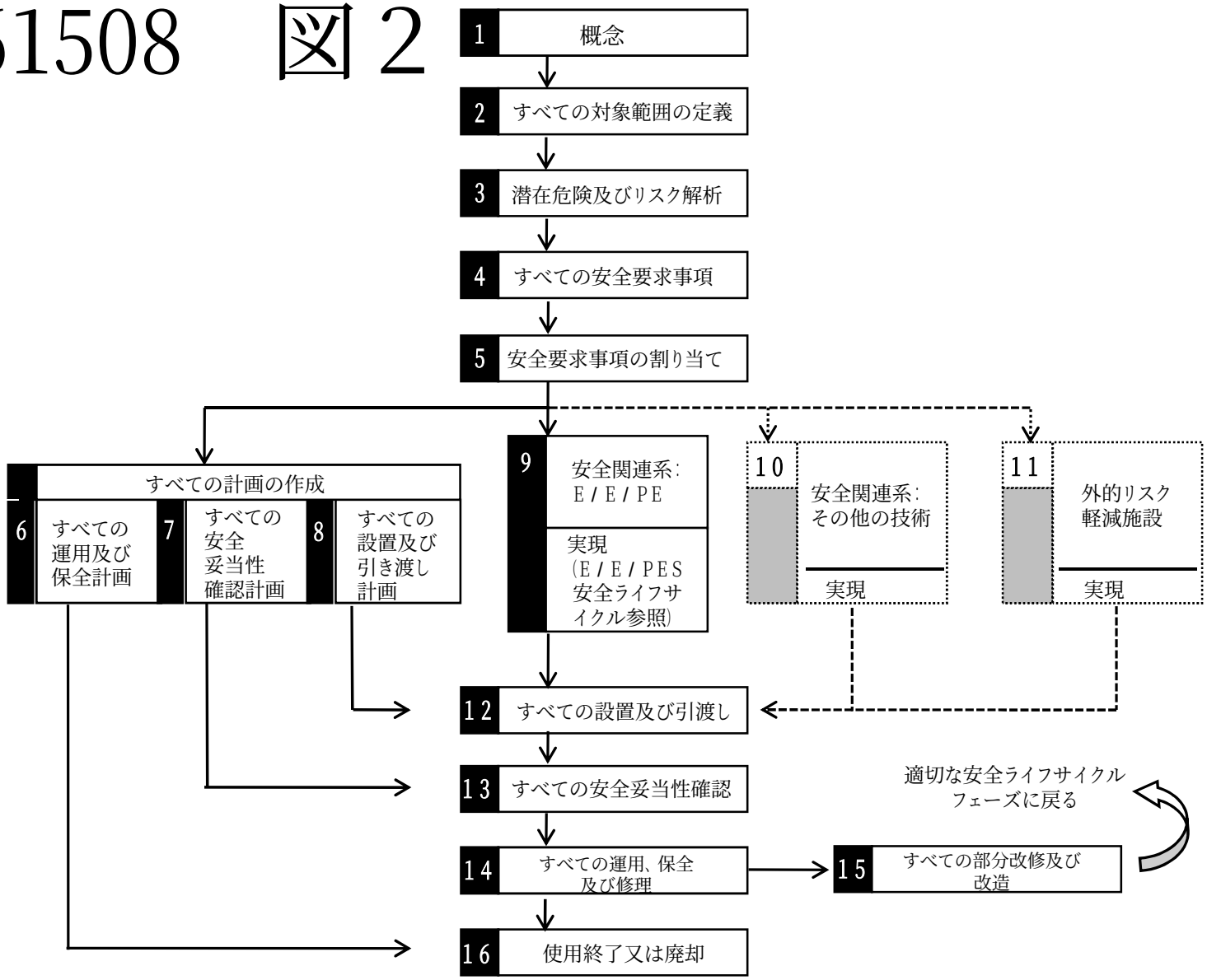
- IEC 61508 Safety Integrity Level (SIL)

➢ランダム故障 信頼性工学的手法で規定
➢系統的故障 管理手法を規定

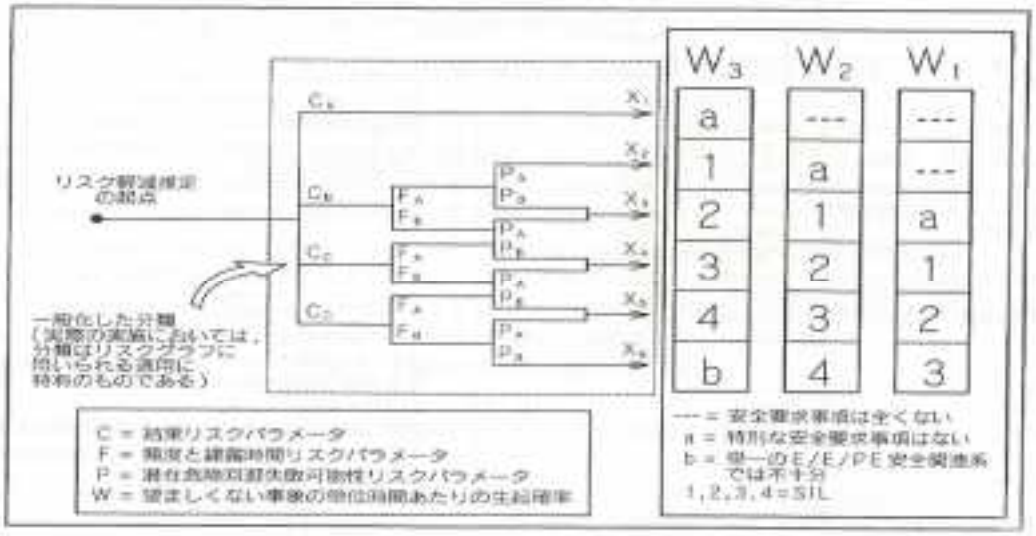
- IEC 62061 機能安全の機械への応用版

➢IEC61508に比して簡便化されている

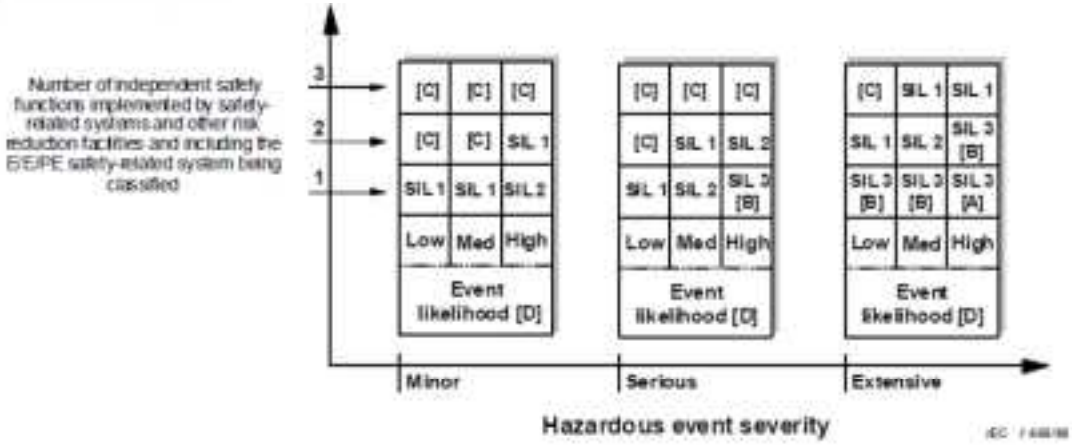
IEC61508　図２


1 概念
2 すべての対象範囲の定義
3 潜在危険及びリスク解析
4 すべての安全要求事項
5 安全要求事項の割り当て
すべての計画の作成
6 すべての運用及び保全計画
7 すべての安全妥当性確認計画
8 すべての設置及び引き渡し計画
9 安全関連系：E/E/PE
実現（E/E/PES安全ライフサイクル参照）
10 安全関連系：その他の技術
実現
11 外的リスク軽減施設
実現
12 すべての設置及び引渡し
13 すべての安全妥当性確認
14 すべての運用、保全及び修理
15 すべての部分改修及び改造
適切な安全ライフサイクルフェーズに戻る
16 使用終了又は廃却

必要なSILを求める方法－IEC61508



附属書D図1　リスクグラフ：一般的スキーム



[A] One SIL 3 E/E/PE safety function does not provide sufficient risk reduction at this risk level. Additional risk reduction measures are required.

[B] One SIL 3 E/E/PE safety function may not provide sufficient risk reduction at this risk level. Hazard and risk analysis is required to determine whether additional risk reduction measures are necessary.

[C] An independent E/E/PE safety function is probably not required.

[D] Event likelihood is the likelihood that the hazardous event occurs without any safety function or other risk reduction measure.

[E] Event likelihood and the total number of independent protection layers are defined in relation to the specific application.

Figure G.1 – Hazardous event severity matrix – example (illustrates general principles only)

必要なSILを求める方法－IEC62061

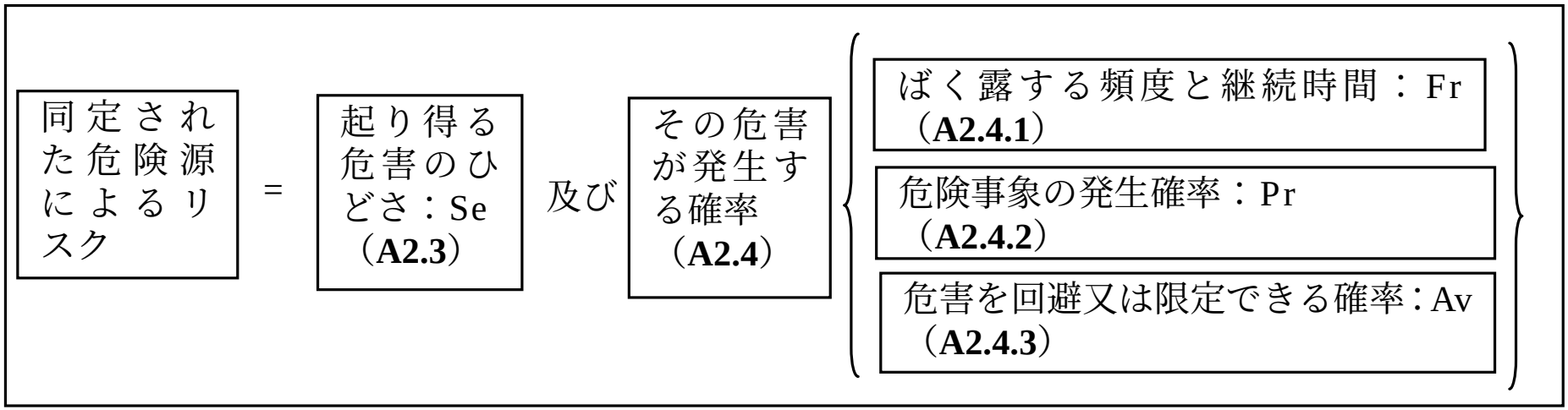


図 A.2－リスク見積りに用いるパラメータ

IS014121と同じ

表A.1－危害のひどさ（Se）の分類

危害のひどさ	危害のひどさレベル（Se）
回復不可能：死亡，目･腕の喪失	**4**
回復不可能：手足骨折，指の喪失	**3**
回復可能：医師の手当てを必要	**2**
回復可能：応急処置を必要	**1**

表A.2－ばく露の頻度と継続時間（Fr）の分類

ばく露の頻度と継続時間（Fr）	
ばく露の頻度	**継続時間>10分の場合のばく露レベル値**
Fr ≤ 1時間	5
1時間 ＜ Fr ≤ 1日	5
1日 ＜ Fr ≤ 2週	4
2週 ＜ Fr ≤ 1年	3
1年 ＜ Fr	2

- すべての運転モード（正規運転、保全など）、危険区域のアクセスの必要性、アクセスの性質（材料の供給、設定など）を考慮する
- 暴露継続時間が１０分未満ならばく露のレベルを一つ下げて良い。

表A.3－発生確率（Pr）の分類

発生確率	発生確率の指標（Pr）
とても高い	5
起こりやすい	4
時々起こる	3
まれには起こる	2
無視できる	1

Frは次のことを考慮して見積る。

－異なる運転モード（正規運転、保全、不具合探求など）における危険源に関する機械部分の動きを予測できるか

－危険源に関連する機械部分への介入に関して、規定又は予見できる人の行動特性ストレス、危険な兆候への不注意

表A.4－危害を回避又は限定できる確率（Av）の分類

危害を回避又は限定できる確率（Av）	
不可能	5
まれには可能	3
かなり可能	1

Avは次のことを考慮して見積る。
－突然の、高スピード、又は低スピードでの危険事象の現れ
－危険源から逃れるための空間の有無
－コンポーネント又はシステムの性質
－危険源を認識できる可能性

表A.6－SIL割付けマトリクス

危害のひどさ（Se）	クラス（Cl）				
	3～4	5～7	8～10	11～13	14～15
4	SIL2	SIL2	SIL2	SIL3	SIL3
3		（OM）	SIL1	SIL2	SIL3
2			（OM）	SIL1	SIL2
1				（OM）	SIL1

$$Cl = Fr + Pr + Av$$

OM: Other method　SRECS以外の方策を推奨

SILの基準　IEC61508

Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 3 – Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

SILの基準：
1時間当たりの危険側故障の確率（PFH_D）

1時間当たりの危険側故障の確率（PFH_D）**[probability of dangerous failure per hour]**

SRECS又はそのサブシステムが，1時間の間に危険側故障を起こす平均確率。

注記　PFH_D 1)を作動要求毎の失敗確率*PFD* 2)と混同してはならない。

注**1)**　この規格は，連続モード及び高頻度作動要求モードのSILを定義するためにPFH_Dを用いる。この規格では，PFH_D は無次元数である。無次元にするために，“1/時間”の次元をもつ危険側故障率λ_D にわざわざ1時間を乗じている。**6.7.8.2**の式(A)，(B)，(C)，(D1)，(D2)を参照。

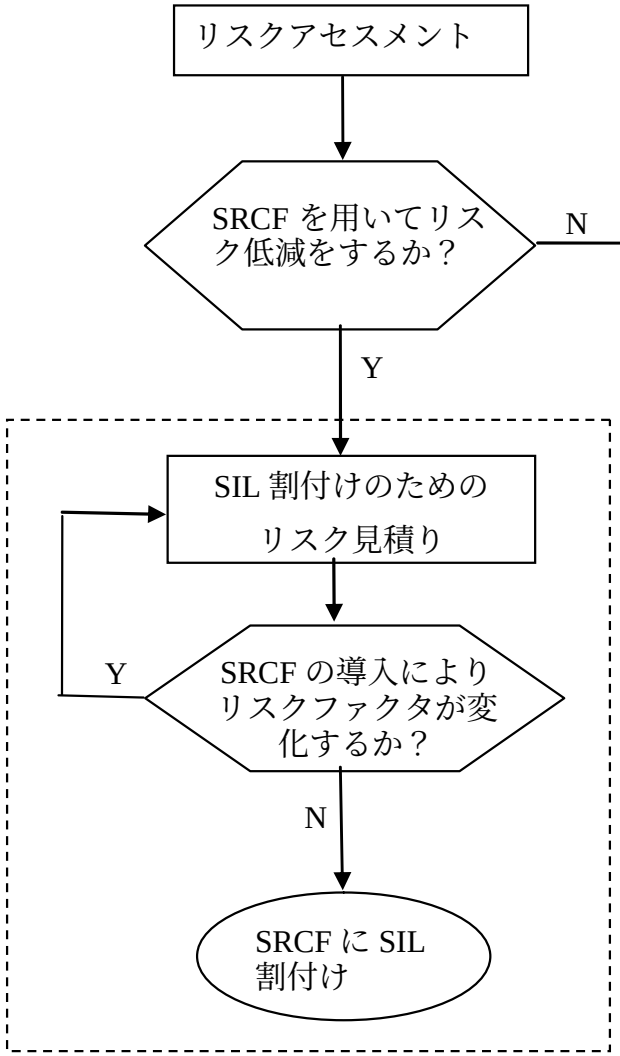
注**2)**　*PFD*は，**IEC 61508**で低頻度作動要求モードのSILを決定するために用いられるが，この規格は，低頻度作動要求モードを扱わないので，SILの定義には*PFD*を用いない。

安全インテグリティレベル

安全インテグリティレベル	１時間当たりの危険側ランダム故障確率　（PFH_D）
SIL 3	$10^{-8} \leqq PFH_D < 10^{-7}$
SIL 2	$10^{-7} \leqq PFH_D < 10^{-6}$
SIL 1	$10^{-6} \leqq PFH_D < 10^{-5}$

安全インテグリティレベル：SRCFの目標故障率

規格で示されたSILの割付け手順



SRCF: Safety-Related Control Function
安全関連制御機能

SIL付与の制約

表 5—サブシステムのアーキテクチャによる SIL 付与の制約：
用いるサブシステムアーキテクチャの違いに応じて SRCF に付与できる SIL の上限

安全側故障比率（SFF）	ハードウェアフォールトトレランス（表内の**注記 1** 参照）		
	0（表内の**注記 3** 参照）	1	2
SFF ＜ 60%	許されない	SIL 1	SIL 2
60% ≤ SFF ＜ 90%	SIL 1	SIL 2	SIL 3
90% ≤ SFF ＜ 99%	SIL 2	SIL 3	SIL 3（表内の**注記 2** 参照）
99% ≤ SFF	SIL 3	SIL 3（表内の**注記 2** 参照）	SIL 3（表内の**注記 2** 参照）

注記 1 ハードウェアフォールトトレランス N は，N+1 個のフォールトが安全機能の失敗を起こし得ることを意味する。
注記 2 SIL 4 付与限界は，この規格では考慮しない。SIL 4 に関しては **IEC61508-1** を参照。
注記 3 例外については **6.7.7** を参照。

- 付与できる最高のSILを左表のように定めている。

安全側故障比率（safe failure fraction）：サブシステムの全故障のうち，サブシステムが危険側故障にならない故障の割合。

$SFF = (\Sigma \lambda S + \Sigma \lambda DD) / (\Sigma \lambda S + \Sigma \lambda D) = (\Sigma \lambda S + DC \times \Sigma \lambda D) / (\Sigma \lambda S + \Sigma \lambda D)$

λS：安全側故障の発生確率，λDD：診断機能によって検出される危険側故障の発生確率

λD：危険側故障の発生確率，DC：診断率

アーキテクチャーによる制約

表 6－アーキテクチャによる制約：カテゴリに関連付けた SILCL

カテゴリ	左欄のカテゴリをもつサブシステムは，下欄に示す特性をもつものとみなす。		アーキテクチャによる制約に基づく SIL 付与限界
	ハードウェアフォールトトレランス	SFF	
1	0	＜ 60%	表内の**注記 1** 参照
2	0	60%～90%	SIL 1
3	1	＜ 60%	SIL 1
	1	60%～90%	SIL 2
4	2 以上	60%～90%	SIL3（表内の**注記 3** 参照）
	1	＞90%	SIL3（表内の**注記 4** 参照）

注記 1　SFF＜60%の場合のカテゴリ 1 及びカテゴリ 2 のケースは，**JIS B 9705-1** の格付けには該当しないため，**JIS B 9705-1** に従って設計されるサブシステムは，実際には 60%以上の SFF を達成すると考えられる。

注記 2　SFF＞90%でカテゴリ 2 のケースは，**JIS B 9705-1** の設計要求事項によって達成されないと考えられる。

注記 3　ハードウェアフォールトトレランスが 2 以上（複数のフォールト蓄積を許容）のカテゴリ 4 サブシステムの場合，診断率は 90%以下であると考える。

注記 4　ハードウェアフォールトトレランスが 1 である場合は，カテゴリ 4 には 90%超（ただし 99%未満）の SFF を必要とする。

注記 5　**JIS B** 9705-**1**:1996 のカテゴリ B は，SIL 1 を達成するのに十分とは考えられない。

危険側故障率の限界値

表 7－危険側故障確率の限度値

カテゴリ	左欄のカテゴリをもつサブシステムは下欄の特性をもつと想定される。		サブシステムに付与できる PFH_D 限度値 （*MTTFsubsystem*,*Ttest*，*DC* を考慮） (表内の**注記 1** 参照）
	ハードウェアフォールトトレランス	*DC*	
1	0	0%	製造者データ又は一般的なデータ（**附属書 D** 参照）を使う。
2	0	60 ～ 90%	$PFH_D \geq 10^{-6}$
3	1	60 ～ 90%	$PFH_D \geq 2\times10^{-7}$
4	2 以上	60 ～ 90%	$PFH_D \geq 3\times10^{-8}$
	1	> 90%	$PFH_D \geq 3\times10^{-8}$

注記 1　PFH_D 付与の限度値は，サブシステムの MTTF（サブシステム製造業者又は関連データ便覧から得る。），SRS に規定されるテスト又はチェックのサイクルタイム（この情報は **ISO 13849-2，3.5** によるサブシステム妥当性確認のためにも必要とされる），及びこの表に規定する診断率（これらの値は **JIS B 9705-1** に記述されるカテゴリの要求事項に基づいている。）の関数である。

注記 2　**JIS B 9705-1** の*カテゴリ* B は，SIL 1 を達成するのに十分であるとは考えられない。

ランダムハードウェアー故障率推定－PFDの計算

単一の場合

プルーフテストのない場合の信頼度関数，故障率は前出の通りです。

ＰＦＤは，$\frac{\text{診断テスト間での平均休止時間}}{\text{診断テスト間隔}}$で，プルーフテスト間隔を$T_P$，その間のある時刻$t$で故障が発生した（但し，検出されていない）とします。

$$PFD=\frac{\int_0^{T_P}(T_P-t)\,f(t)\mathrm{d}t}{T_P}=\frac{1}{T_P}\int_0^{T_P}F(t)\mathrm{d}t=\frac{1}{T_P}\int_0^{T_P}(1-R(t))\mathrm{d}t=\frac{1}{T_P}\int_0^{T_P}(1-\mathrm{e}^{-\lambda t})\mathrm{d}t=\frac{1}{T_P}\int_0^{T_P}\lambda t\mathrm{d}t=$$

(17）

低頻度作動要求モードのPFD

必要なユニット数	冗長ユニット数			
	1	2	3	4
1	$\frac{\lambda T_p}{2}$ (1oo1)	$\frac{(\lambda T_p)^2}{3}$ (1oo2)	$\frac{(\lambda T_p)^3}{4}$ (1oo3)	$\frac{(\lambda T_p)^4}{5}$ (1oo4)
2	—	λT_p (2oo2)	$(\lambda T_p)^2$ (2oo3)	$(\lambda T_p)^3$ (2oo4)
3	—	—	$\frac{3\lambda T_p}{2}$ (3oo3)	$2(\lambda T_p)^2$ (3oo4)
4	—	—	—	$2\lambda T_p$ (4oo4)

高頻度／連続作動要求モードの故障率

必要なユニット数	冗長ユニット数			
	1	2	3	4
1	λ (1oo1)	$\lambda^2 T_p$ (1oo2)	$\lambda^3 {T_p}^2$ (1oo3)	$\lambda^4 {T_p}^3$ (1oo4)
2	—	2λ (2oo2)	$3\lambda^2 T_p$ (2oo3)	$4\lambda^3 {T_p}^2$ (2oo4)
3	—	—	3λ (3oo3)	$6\lambda^2 T_p$ (3oo4)
4	—	—	—	44 4λ (4oo4)

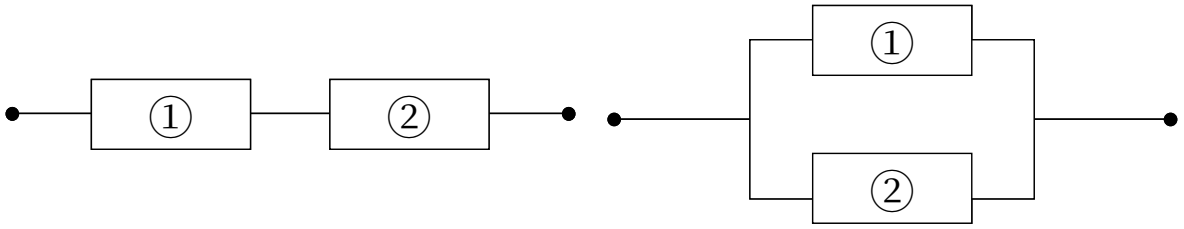
直列の場合

$$PFD = \frac{\lambda_1 T_P}{2} + \frac{\lambda_2 T_P}{2} = PFD_1 + PFD_2 \qquad (22)$$

並列系の場合

$$MTTF = MTTF_1 + MTTF_2 - \frac{1}{\frac{1}{MTTF_1} + \frac{1}{MTTF_2}} \qquad (26)$$

$$PFD = \frac{\lambda_1 \lambda_2 T_P^2}{3} \qquad (27)$$



(a) 直列系　　(b) 並列系

図7 直列系／並列系

ランダムハードウェアー故障率推定の単純化アプローチ　IEC62061

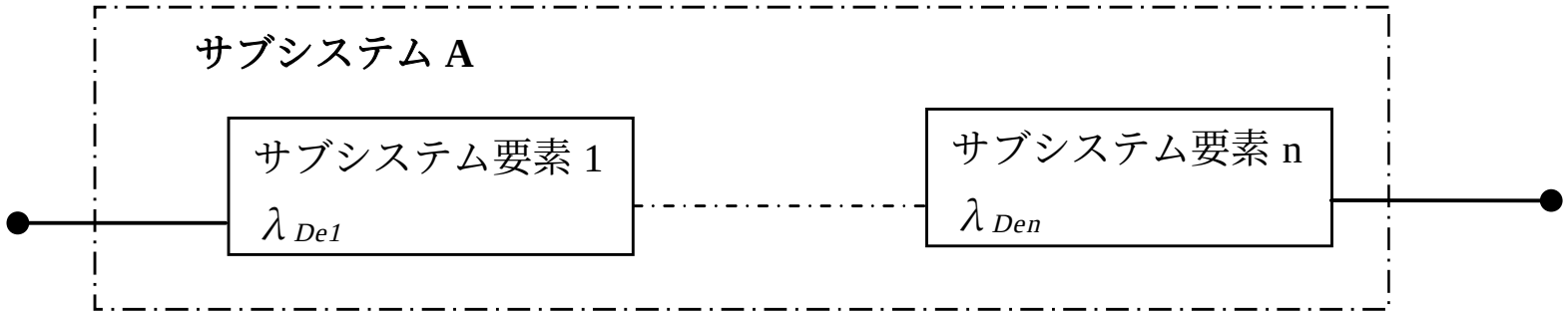


図 6ーサブシステム A の論理的表現

$$\lambda_{DssA} = \lambda_{De1} + \ldots + \lambda_{Den} \qquad (A)$$

$$PFH_{DssA} = \lambda_{DssA} \times 1h$$

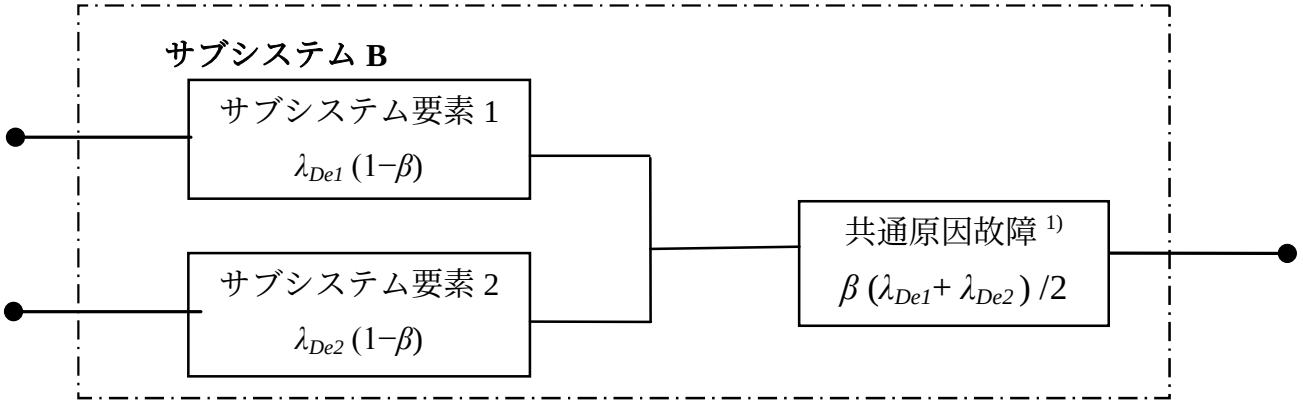


図 7ーサブシステム B の論理的表現

$$\lambda_{DssB} = (1-\beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta(\lambda_{De1} + \lambda_{De2})/2 \qquad (B)$$

$$PFH_{DssB} = \lambda_{DssB} \times 1h$$