制御システムの安全関連部(SRP/CS)

(一財)機械振興協会
技術研究所

目　　次

制御システムの安全関連部(SRP/CS)

制御システムの安全関連部(SRP/CS)

本項においてはISO-18849の内容を解説します。

概要

① 制御システムの安全関連部(SRC/CS)は、安全機能を提供する部分であり、ハードウェアとソフトウェアから構成する。
② 制御システムの安全機能は、パフォーマンスレベル(PL:Performance Level)と定義される5通りのレベル(a、b、c、d、e)のうち一つに振り分けられる。
③ 安全機能の危険側故障発生確率は、ハードウェア並びにソフトウェアの構造、障害検出機構の程[[診断範囲(DC)]、コンポーネントの信頼性[平均危険側故障時間($MTTF_d$)、共通原因故障(CCF)]、設計プロセス、運転ストレス、環境条件と運転手順による。
④ カテゴリとは、達成したPLの査定を容易にするものであり、設計基準と障害条件に従った構造分類であり、5通りのレベル(B,1,2,3,4)に分類できる。
⑤ PLとカテゴリは表1に示す制御システムの安全関連部に適用する。

表1　PLとカテゴリの適合

安全関連制御機能の技術方式		ISO13849(JISB9705)
A	非電気式、例えば液圧式	×
B	電気機械式、例えば、リレー、非複雑電子システム	Pleまでの指定カテゴリ[a)]に適用
C	高複雑電子システム、例えば、プログラム式	Pldまでの指定カテゴリ[a)]に適用
D	AとBとの複合	Pleまでの指定カテゴリ[a)]に適用
E	CとBとの複合	Pldまでの指定カテゴリ[a)]に適用
F	CとA、またはCとA及びBとの複合	X[b)]
X 見出しに示される規格によって取り扱われるアイテム		
注) a) 指定のカテゴリは4.5項に示される。 b) 高複雑電子システムは、この規格に指定されるPLdまでのカテゴリ。		

制御システムの安全関連部(SRP/CS)

設計の流れ

① 安全機能特性を特定し、実現方法を決定
② 安全要求性能レベル(PL_r:Required Performance Level)を決定
③ PL_rと同等以上の安全性能レベル(PL)を構築するために、カテゴリ(システムの構造)、診断範囲などを選択
④ システマチック故障、コンポーネントを考慮してSRC/CSを設計
⑤ ソフトウェアは、V(字)モデルに基づいて設計
⑥ SRC/CSの安全性能レベルの達成度について評価
⑦ 安全性能レベルが、安全性能要求レベルを満足しているかを「分析」と「試験」により検証
⑧ 分析による評価:FMEA、FTAなどの手法
⑨ 試験による評価:通常および異常条件に対しての機能・性能試験

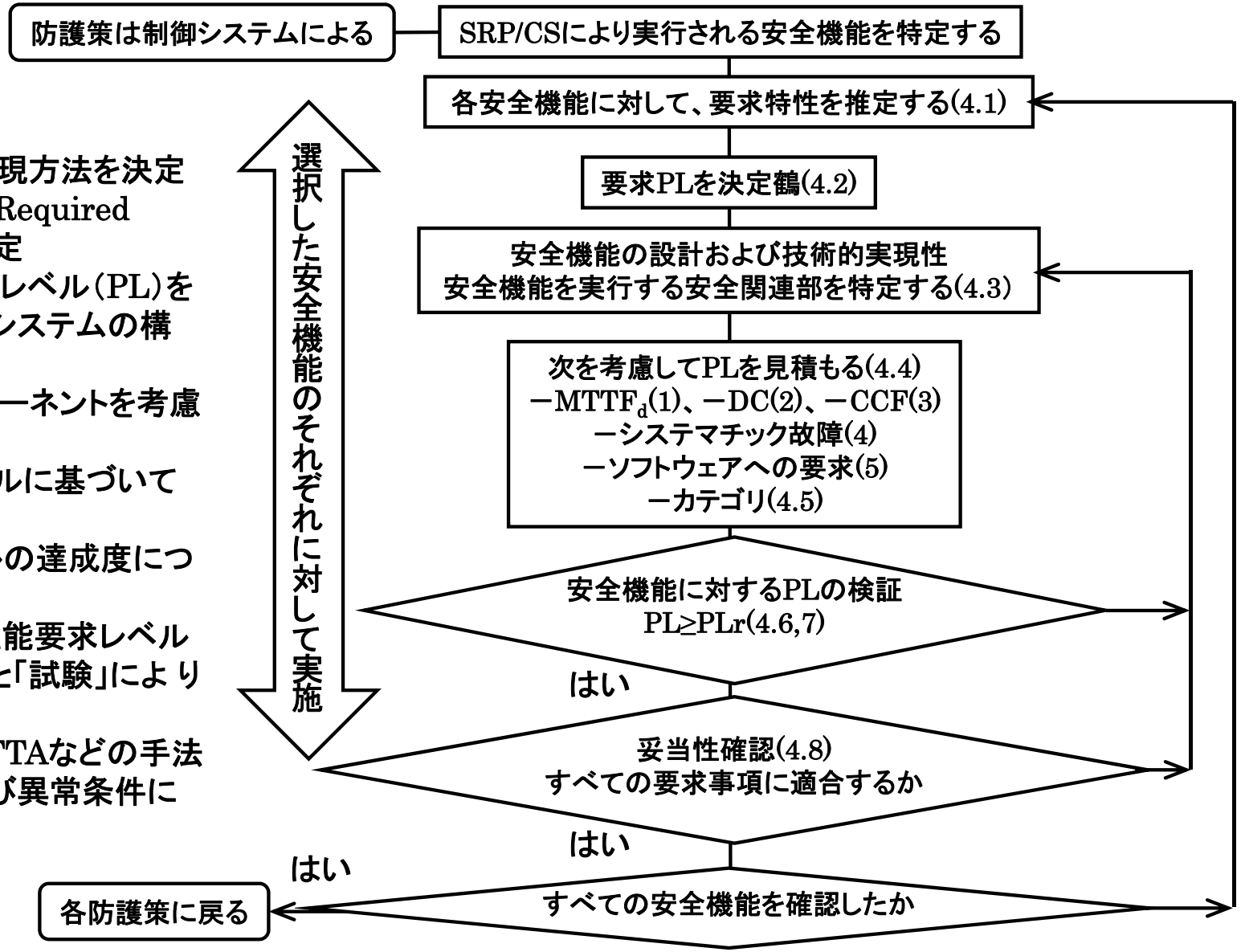


図1　制御システムの安全関連部の設計のフローチャート

1. 安全機能の特性

SRC/CSにより提供される安全機能との概要と要求を表2に示す。設計者は、特定の用途の制御システムで要求される安全方策を達成するために、この表の必要な安全機能を実現しなければならない。.

表2　SRC/CSにより提供される安全機能の概要と要求

安全機能		概要	要求 (ISO13849)
特性	安全関連停止機能	保護装置の停止機能は、作動直後に機械を安全に動作可能な状態にする。この停止は、通常操作の停止機能に優先させる。	5.2.1
	手動リセット機能	安全防護装置により停止の命令が出た後は、再起動のための安全条件が成立するまで停止状態を維持する。	5.2.2
	起動／再起動機能	再起動は、危険状態が存在しない場合のみに自動的実行される。	5.2.3
	ローカルコントロール機能	機械が、たとえば、携帯式制御装置やペンダントにより現場で制御される場合に適用される。	5.2.4
	ミューティング機能	ミューティング機能は、SRP/CSによる安全機能の一時停止を可能とする。	5.2.5
安全関連パラメータ	応答時間	リスクアセスメントで要請される場合、SRP/CSの応答時間を決定しなければならない。	5.2.6
	安全関連パラメータ(速度、圧力など)	あらかじめ設定した制限値を逸脱している場合、制御システムは、適切な方法(たとえば、停止、警報信号、警報音など)で危険を回避する。	5.2.7
	電源の変動、損失、復旧	設計上の範囲逸脱した場合に、他の部分において安全を維持できるように出力信号を生成する。	5.2.8

2. 要求PL_rを決定する

・SRP/CSによるリスク低減方法

設計者は、SRP/CSに備えるべき安全機能特性を前項より選択し、図2の左に示すS(障害のひどさ)、F(危険源への接近頻度)、P(危険源を回避する可能性)からその要求性能レベル(PL_r)を決定する。次に、それに見合うように、カテゴリや診断範囲などを選択し図2の右に示す5段階(a、b、c、d、e)の性能レベルを設定する。表3にPLの性能レベルを示す。

表3　PLの性能レベル

PL	危険側障害発生の平均確立(1/h)
a	10^{-5}≦から<10^{-4}
b	3×10^{-6}≦から<10^{-5}
c	10^{-6}≦から3×<10^{-6}
d	10^{-7}≦から<10^{-6}
e	10^{-8}≦から<10^{-7}

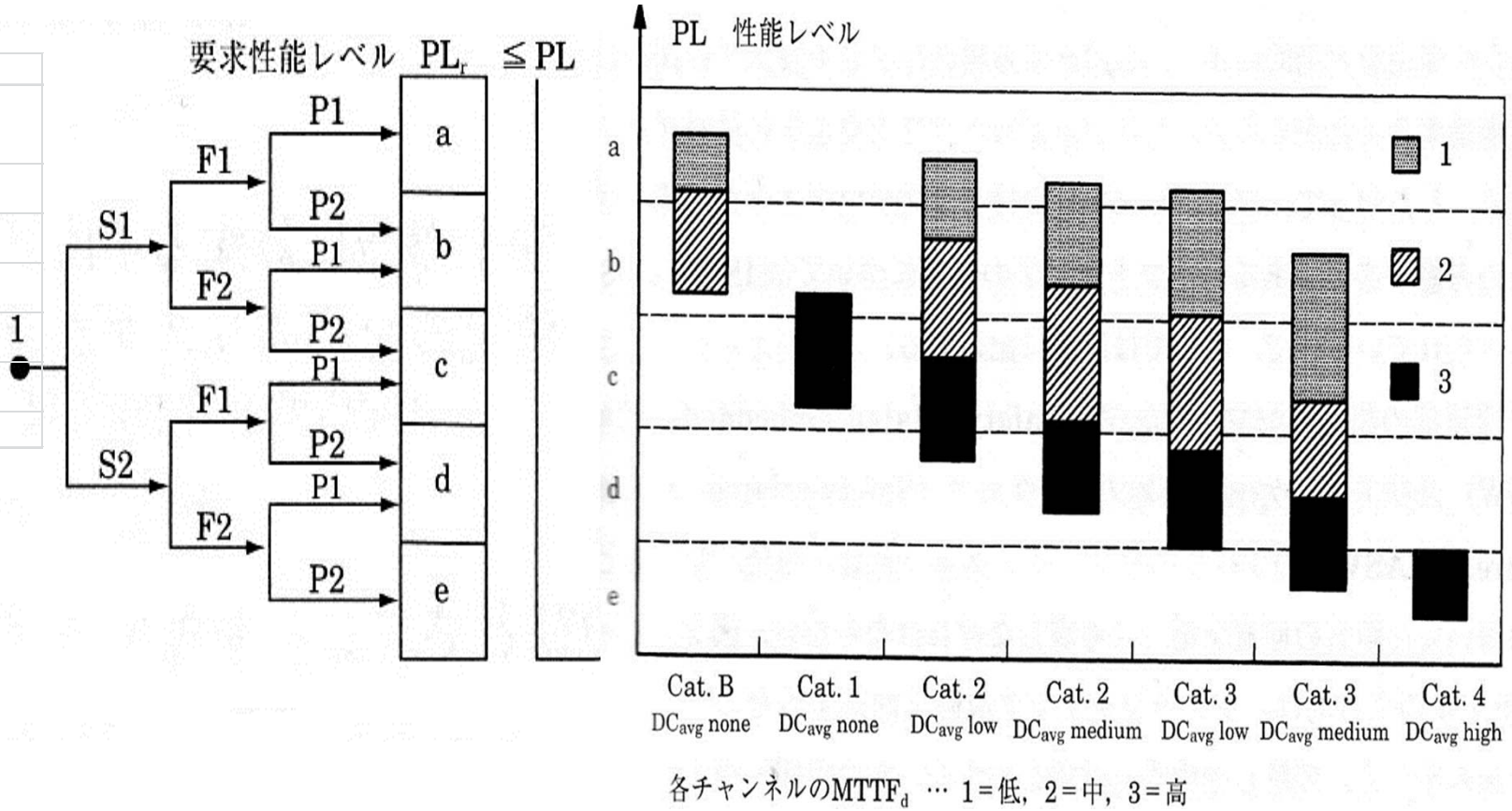
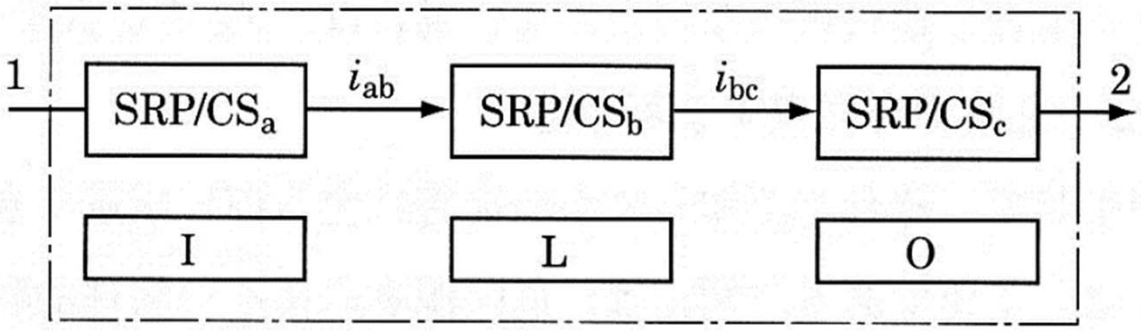


図2　PL_rの設定とPLの見積もり

3. SRC/CSの設計

技術的実現性や用いるべき安全機能を想定して、制御システムの安全設計からSRC/CSを設計する
代表的な安全機能は、図３のダイヤグラムで表現され、SRP/CSは次の組合せによる。

・入力(SRP/CS_a)
・論理／処理(SRP/CS_b)
・出力／動作制御要素(SRP/CS_c)
・相互接続手段（i_{ab},i_{bc}）(たとえば、電気的、工学的)



I	入力
L	論理
O	出力
i_{ab}, i_{bc}	内部接続手段
1	起動事象（例えば押しボタンの手動操作，防護柵を開く，AOPD* のビームをさえぎる）
2	機械のアクチュエータ（例えばモータのブレーキ）

* AOPD：能動的光電保護装置（例：ライトバリア）

図3　代表的な安全機能のダイヤグラム

4. 達成されるPLの評価とSILとの関係

ISO13849においては、SRC/CSの安全機能は、性能レベル(PL:Performance Lebel)により明示される。そのため、選択されたそれぞれのSRC/CS(単独または組合せ)について、PLの評価をはじめに行う。PLとSILの関係を表4に示す。SRC/CSのPLは、以下に示すパラメータの評価によって示される。

表4　PLとSILとの関係

PL	SIL
a	対応なし
b	1
c	1
d	2
e	3

(1) 危険側故障の平均時間($MTTF_d$:Mean Time to Dangerous Failure)

個々のチャンネルの$MTTF_d$は表5に示す3つのレベルに分類されており、それぞれのチャンネル(たとえば単独のチャンネル、冗長システムの個々のチャンネル)について考慮しなければならない。

個々のコンポーネントの$MTTF_d$のデータの見積もりは、以下に示す順序でおこなう。

・メーカのデータ
・ISO13849の付属書CおよびDに示される手法
・10年を選択

表5　$MTTF_d$とDC

要素	内容	範囲
$MTTF_d$	各チャンネルの平均危険側故障時間	Low:3～10年 Medium:10～30年 High:30～100年
DC	各チャンネルの自己診断の範囲率	なし:0% Low:60～90% Medium:90～99% High:99%以上

(2) 診断故障(DC:Diagnostic Coverage)

DCは、SRP/CSにおける診断機能の尺度で、表5に示すように四つのレベルで定義される。DCは、SRP/CSの不具合に対する自己診断の範囲または有効度であり、診断の方法と監視の頻度により評価される。

DCは、検出された危険側障害の確立λ_{DD}と全体の危険側障害の確立λ_{total}の分数で表わされる。

$$DC=\Sigma\lambda_{DD}/\Sigma\lambda_{total}$$

(3) 共通原因故障(CCF:Common Cause Failure)

表6　CCF対策と定量化(1/2)

No	CCF対策	スコア
1	分離／隔離 信号経路同士の物理的分離: 配線／配管の分離 プリント回路基板における、十分な空間距離と沿面距離	15
2	多様性 異なる技術／設計や物理気原則が使用される。 例:ファースト・チャンネル・プログラマブル電子機器とセカンドチャンネル・ハードワイヤード 起動の種類 圧力と温度 距離と圧力の測定:デジタルとアナログ 異なる製造者の部品	20
3	設計／アプリケーション／経験	
3.1	過電圧、過圧力、過電流など	15
3.2	十分検討された部品を使用する	5
4	アセスメント分析 故障モード影響分析の結果が、共通原因故障の防止に、設計上考慮されているか。	5
5	能力／訓練 設計者／保守作業車は、共通原因故障の原因と結果を理解するための訓練を受けているか。	5

表6　CCF対策と定量化(2/2)

No	CCF対策	スコア
6	環境	
6.1	CCに対する汚染の防止と電j環境整合性(EMC)は、適切な規格に従う。 流体システム:圧媒体の濾過作用、よごれ吸気の防止、圧縮空気の排出 例:圧媒体清浄に関連する部品製造者の要求に準拠。 電気システム:システムは電磁環境耐性をチェックしたか。 例:CCFに対する関連規格の指定されたとおり化。 流体と電気系システムの組合せは、両方の側面が考慮されなければならない。	25
6.2	その他の影響 温度、衝撃、振動、湿度など(関連する規格で規定)、すべての関連する環境的影響への耐性要求は考慮されているか。	10
	合計	最大100まで

合計点数	CCF対d作
65以上	要求に合致
65未満	プロセスに問題あり→追加手段を選択

(4) システマチック故障
　ある原因により引き起こされる複合的な故障であり、設計や製造プロセスの修正、試験や運用手順の改訂など、すべてを検討することにより除去できる。

(i) システマチック故障を抑制する
システマチック故障は、制御の結果を監視することにより、回避可能である。そのため、監視機能や自動試験機能を組込んでおく。

(ii) システマチック故障の回避
　システマチック故障は、以下の手段により回避できる。
・コンポーネントや材料の選択では、使用条件に対して定格を十分に満たす。また、FMEAが明確になっているか、安全規格に合格しているコンポーネント・モジュールを使用する。
・コンポーネント・モジュールなどの仕様(電圧・電流など)を系統的にシミュレーションして故障を想定する。

(iii) SRP/CSの開発過程でのシステマチック故障の回避
　SRC/CSの開発過程において機能試験やプロジェクトマネージメントを実施し、その内容を文書化しておくことにより、システマチック故障を回避できる。

4. 達成されるPLの評価とSILとの関係

(5) ソフトウェアへの安全要求

ソフトウェアは、SRP/CSの設計において、特にシステマチック故障の発生を自動的に繰り返し診断するソフトウェアを採用することが必要である。そのために図4に示すV(字)-モデルを採用し、ソフトウェアを読みやすく、理解しやすく、試験しやすく、かつ保守しやすくする。V(字)-モデルの左側は設計活動であり、右側はデバック(試験)である。設計時点で試験方法や期待される結果を明確にしておくことにより、試験による検証が容易になる。

① 安全関連の組込みソフトウェア(SRESW)

PL_rのa～dの場合の対策

・モジュール化や構造化設計、並びにコーディング。

・機能試験、たとえば、ブラックボックス試験。 など

PL_rがcまたはdの場合の対策

・ISO9001と同等のプロジェクト管理と品質管理。

・安全要求事項で構造化された使用と設計。 など

PL_rがeの場合いは、IEC61508-3:1998 7.のSIL3を満足する。

② 安全関連のアプリケーションソフトウェア(SRASW)

PL_rのa～eの場合の対策

・①と同様

PL_rがc～eの場合の追加方策

・ツール、ライブラリ、言語を統一する。

・SRASWと非SRASWのデータの論理的結合があってはならない。

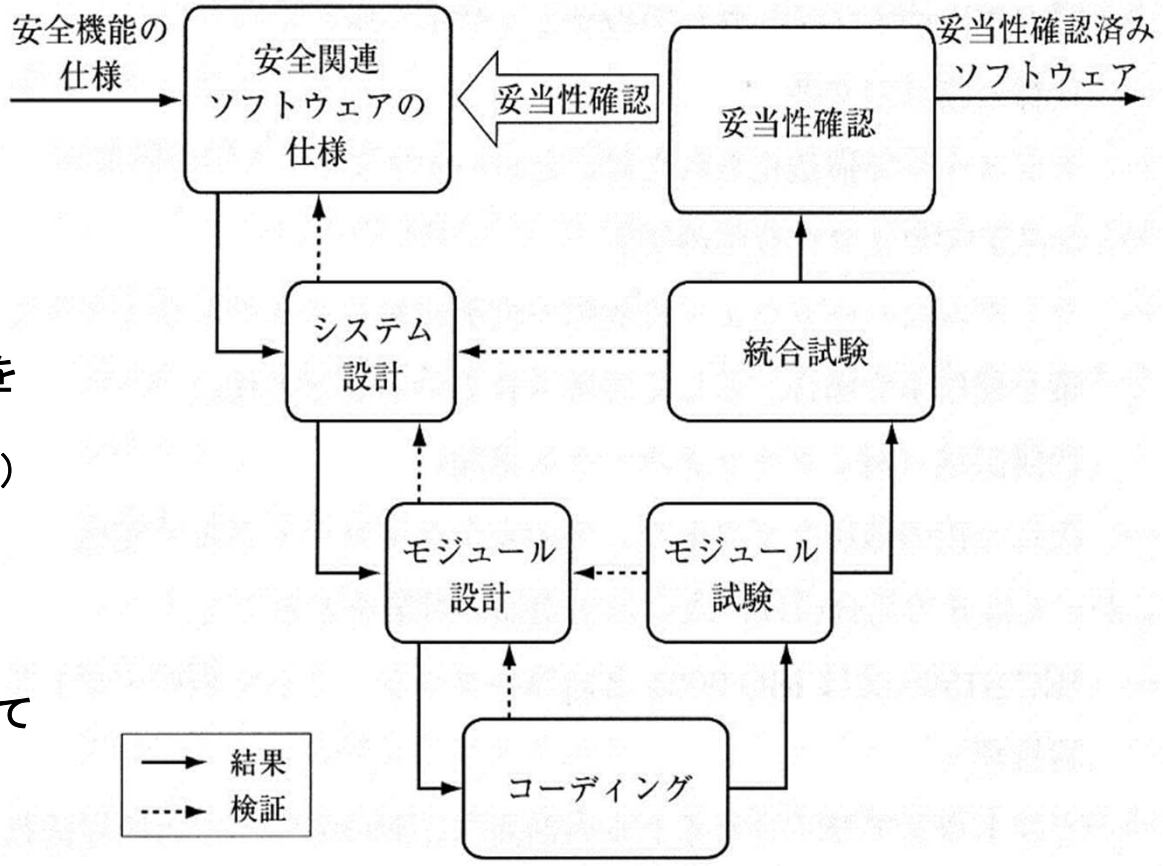


図4 V(字モデル)

5. カテゴリと各チャンネルの$MTTF_d$、DC_{avg}、CCFの関係

(1) 概要

カテゴリは、PL_rを満足するシステムを構築するための基本的な要素であり、故障に対する耐性に関して、2，3項で述べた設計上の考慮（例えば、コンポーネントの不具合、共通原因故障を検知するための診断範囲など）に基づきSRP/CSに要求される内容を示したものである。

・カテゴリB：基本的カテゴリである。故障の発生は、安全機能の喪失つながる。
・カテゴリ1：このカテゴリにおいては、故障に対する改善は、主としてコンポーネントの選択と適用により達成される。
・カテゴリ2～4：これらのカテゴリにおいては、特定の安全機能に関し、性能上の改善は、主としてSRP/CSの対応により達成される。
・カテゴリ2：このカテゴリにおいては、特定の安全機能が実行されていることを定期的にチェックすることにより安全機能の有効性が確認される。
・カテゴリ3と4：これらのカテゴリにおいては、単一の故障が安全機能の喪失にならないことにより高い安全性が達成される。
・カテゴリ（3と）4：カテゴリ4において（とカテゴリ3において合理的に実施可能な場合）、SRP/CSの故障は検出される。カテゴリ4では、故障の蓄積に対する耐性をもつ。

表7　障害が発生した場合のSRO/CSからカテゴリへの要求事項(1/2)

カテゴリ	要求のまとめ	システム動作	安全実現のための原則	各チャンネルの$MTTF_d$	DC_{avg}	CCF
B	SRO/CSとその保護装置は、その部品と同じく、予想される影響に耐えられるよう、関連企画に従い、設計、構築選択、組立てられていること。基本の安原則が使用される。	故障が発生すると安全機能の喪失を招くことがある。	主に製品の選択によって特徴づけられる。	低～中	なし	関連なし
1	Bの要素が適用される。十分検討された部品と安全原則が使用っされる。	故障発生確率はカテゴリBより低いが故障時は安全機能の喪失を招くことがある。	主に製品の選択によって特徴づけられる。	高	なし	付属書F
2	Bの要求と十分検討された安全原則が適用される。安全機能は機械の制御システムにより適切な感覚で点検される。	故障が起きると点検と点検の間で安全機能の喪失を招くことがある。安全機能の喪失は点検により検出される。	主に製品の選択によって特徴づけられる。	低～高	低～中	付属書F

表7　障害が発生した場合のSRO/CSからカテゴリへの要求事項(2/2)

カテゴリ	要求のまとめ	システム動作	安全実現のための原則	各チャンネルの$MTTF_d$	DC_{avg}	CCF
3	Bの要求と十分検討された安全原則が適用される。 安全関連部品は以下のように設計される。 ①単一故障が安全機能の喪失を招かないこと。 ②実行可能な限り単一故障は検出される。	単一故障発生時、安全機能は動作する。 すべてではないが故障を検出できる。 検出されない故障が累積した場合、安全機能の喪失を招くことがある。	主に構造によって特徴づけられる。	低～高	低～中	付属書F
4	Bの要求と十分検討された安全原則が適用される。 安全関連部品は以下のように設計される。 ①単一故障が安全機能の喪失を招かないこと。 ②単一故障は、次の安全機能が働く前に検出されること。検出が不可能でも、故障の累積が安全機能の喪失を招かないこと。	単一故障発生時、安全機能は動作する。 累積故障の検出により安全機能の喪失率は減少する。(高いDC) 安全機能喪失を防止するため、故障はすぐに検出される。	主に構造よって特徴づけられる。	高	高(故障の累積を含む)	付属書F

(2) カテゴリの仕様

各SRP/CSは、関連するカテゴリの要求事項に適合しなければならない。重要なことは、図5で示されるPLは、カテゴリ、各チャンネルの$MTTF_d$とDC_{avg}によって、指定アーキテクチャに基づいているということである。

① カテゴリB

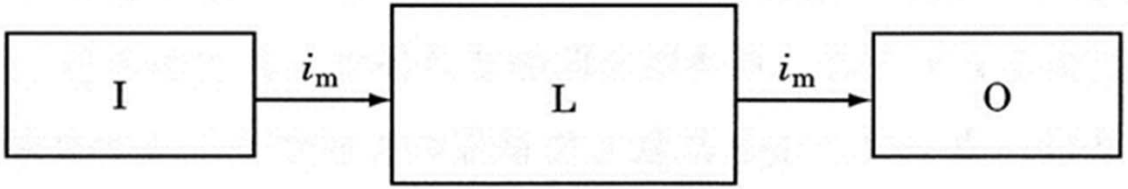
カテゴリBには「基本安全原則」が適用される。

カテゴリBでは、単一故障が発生すると、安全機能の損失を招くことがある。

カテゴリBのシステム内では、診断範囲がなく(DC_{avg}=0%)、かつ、各チャンネルの$MTTF_d$は低～中までとなる。

カテゴリBによって達成可能なPLは、bである。

カテゴリBの指定アーキテクチャを図5に示す。



i_m 内部接続
I 入力装置，例：センサ
L 論理
O 出力装置，例：主継電器

図5 カテゴリBと1の指定アーキテクチャ

② カテゴリ1

カテゴリBの要求が適用される。カテゴリBと1の指定アーキテクチャは同じであり、どちらも、基本安全規格が適用される。そのうえで「十分に吟味されたコンポーネント」の使用が要求される。

十分に吟味されたとしての能力は、そのアプリケーションに依存する。たとえば、ポジティブの接点を備えた位置スイッチであり、これを確実にするために以下の対策を講じる必要がある。

・調整後にスイッチの固定を確実にするための手段。カムの固定を確実にするための手段
・位置スイッチのオーバトラベル回避のための手段

発生確率はカテゴリBより低いが、故障時に安全機能の喪失を招くことがある。

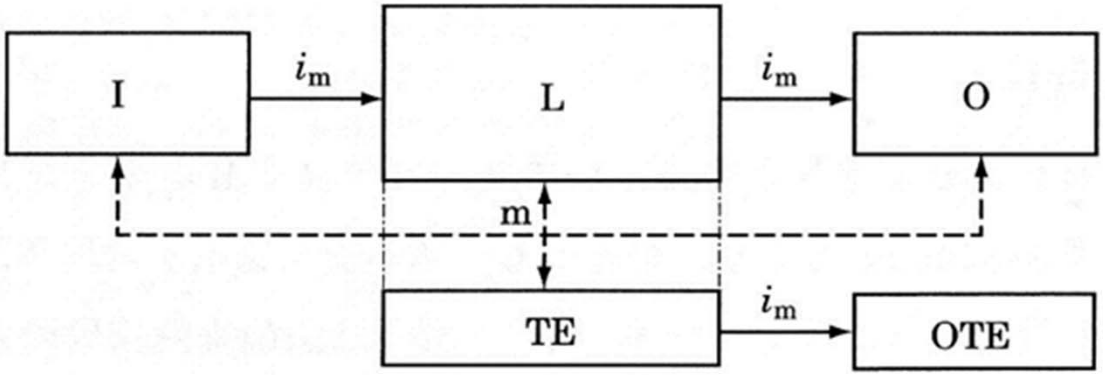
カテゴリ1の指定アーキテクチャは、カテゴリBと同じである。

③ カテゴリ2

カテゴリBの要求と「十分吟味にされた安全原則」が適用される。安全機能は、制御システムにより適切な間隔で点検する必要がある。

カテゴリ2は、カテゴリ1に機能の監視が追加されたことが特徴である。ただし、故障が起きると、点検と点検の間で安全機能の喪失を招くことがある。このような安全機能の喪失も、点検により検出される必要がある。

カテゴリ2の指定アーキテクチャを図6に示す。



点線は適切に実施可能な不具合検出

i_m	内部接続
I	入力装置，例：センサ
L	論理
m	監視
O	出力装置，例：主継電器
TE	試験機器
OTE	試験機器の出力

図6　カテゴリ2の指定アーキテクチャ

5. カテゴリと各チャンネルの$MTTF_d$、DC_{avg}、CCFの関係

④ カテゴリ3

カテゴリBの要求と「十分吟味にされた安全原則」が適用される。

カテゴリ3のSRP/CSは、以下のように設計される。

・単一の故障が安全機能の喪失を招かないこと。

・二つの論理装置により単一の故障を確実に検出する。

なお、検出されない故障が累積した場合には、安全機能の喪失を招くことがある。

カテゴリ3と4は、L1、L2という別々の論理装置を装備し、相互に比較することを要求している。(多様性:ダイバーシティ)。

カテゴリ3の指定アーキテクチャを図7に示す。

⑤ カテゴリ4

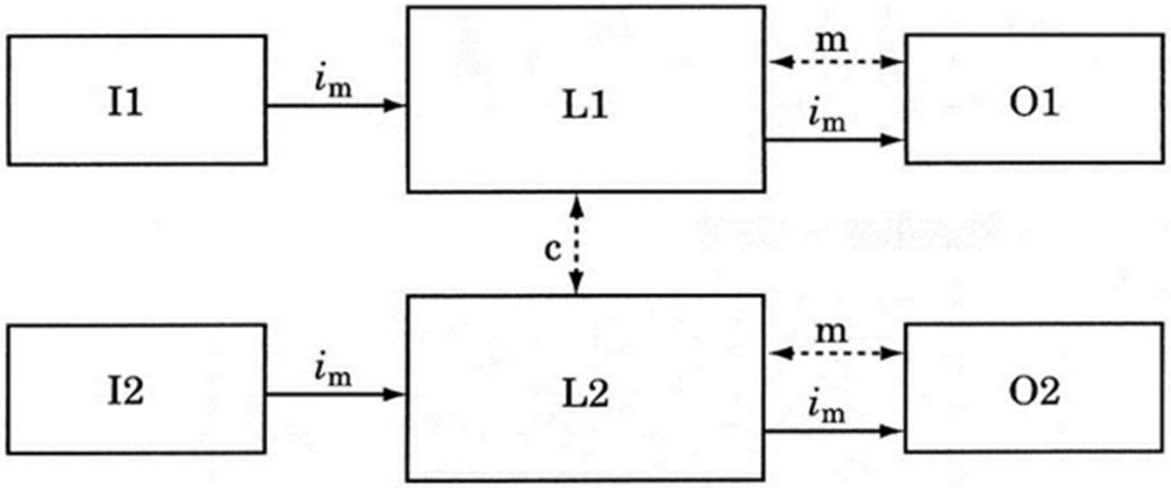
カテゴリBの要求と「十分吟味にされた安全原則」が適用される。カテゴリ3は、単一故障を検知するだけであるが、カテゴリ4は累積故障(二つ以上の故障)を防ぐ設計とする。

カテゴリ4のSRP/CSは、以下のように設計される。

・単一故障が安全機能の喪失を招かないこと。

・単一故障は、次の安全装機能が働く前に検出されること。検出が不可能でも、累積故障による安全機能の損失を招かないこと。

カテゴリ4の指定アーキテクチャは、カテゴリ3と同じである。



点線は適切に実施可能な不具合検出

i_m	内部接続
c	相互監視
I1, I2	入力装置, 例:センサ
L1, L2	論理
m	監視
O1, O2	出力装置, 例:主継電器

図7 カテゴリ3と4の指定アーキテクチャ

(3) 異なるカテゴリに対するSRP/CSの選択と組合せ

安全機能は、入力システム、信号のプロセスユニット、出力システムなどいくつかのSRP/CSを組合せることによって実現できる。これらのSRP/CSには、いくつかの異なったカテゴリが含まれる場合があるので、SRP/CSのカテゴリ選定は、前述の五つのカテゴリを参考に選択する必要がある。

SRP/CSを組合せたもののPLは表8を参考にして決めるが、全体を監視機能（例えば、入出力、もしくは、入力と動力からのフィードバック信号を監視するなど）を設けることにより安全を確保すべきである。

表8　SRP/CSを組合わせたPLの例

PL_{low}	N_{low}	⇒	PL
a	>3	⇒	なし、許可していない
	≦3	⇒	a
b	>2	⇒	a
	≦2	⇒	b
c	>2	⇒	b
	≦2	⇒	c
d	>3	⇒	c
	≦3	⇒	d
e	>3	⇒	d
	≦3	⇒	e

6. 達成したPLと要求PL_rの適合性検証

構築されたSRO/CSのPLを計算し、要求性能PL_rと同等以上であることを確認し文書化する。必要に応じて根拠となる計算式も記述しておくこと。

ここで確認された妥当性は、使用上の情報の漏れの確認を含み、提供される使用上の情報による設置後の危機対策にも活用される。

妥当性の確認の結果、PL_rが達成されていない場合には、設計変更が必要となる。

オペレータとSRP/CSとのインタフェースは、機械のすべての使用条件と誤使用において危険が発生しないように設計されなければならない。

人間工学の利用により、SRC/CSを含む機械と制御システムが操作しやすくなり、危険な作業を誘導しにくくなる。

7. 妥当性の確認

妥当性の確認とは、「SRP/CSの安全機能について特別の要求事項に適合することを審査する」ことである。妥当性確認では、要求された安全機能(PL_r)とSRP/CSによる安全機能(PL)がISO13849を満足していることを明らかにすることでもある。

妥当性の確認は、以下の２項目について実施する。

・分析：トップダウン技法として、FTAやETAを用いる。

・適合試験：分析では十分に確認ができなかった場合、試験を実施して確認する。予想される環境条件下(振動、温度、湿度、EMCなど)で装置が機能することを確認する。

8. 技術資料

SRP/CSを設計するにあたって、以下に示す情報を資料化しておく。

- SRP/CSの安全機能
- それぞれの安全機能の特徴
- SRP/CSの機能の正確な開始時点と終了時点
- 使用環境条件
- 性能レベル(PL)
- 選択したカテゴリ
- 信頼性($MTTF_d$、DC、CCF、寿命時間)に関するパラメータ
- システマチック故障に対する対策
- 対策として採用した技術
- 考えられた故障
- 除外された故障
- ソフトウェアの資料
- 合理的に予見可能なご使用に対する対策