

機械の制御システムの設計段階における保護方策

機械装置の危険源は、源流の設計段階において「制御の安全」の考え方によって、それらのリスクを低減して安全なシステムとすることが要求される。これは、設計者が見落としのない危険源のリスクアナリシスを実施して、対象の機械装置が安全に動作するシステムを合理的に構築すると同時に全体システムとして「安全であることの妥当性検証」が必要となる。

[1] 機械装置の制御設計の手順

(1) 設計上の制限条件

・機械の使用者の制限条件を設定して設計前の必要な条件(環境条件・電源条件・要求事項)を確認する。

(2) 一般仕様の確認

・機械の一般仕様(適用法規制・規格、客先安全要求仕様)の確認する。

(3) 機械全体の基本設計

・個別仕様書(設備・機械仕様、制御仕様、システム仕様)を作成と基本設計
・リスクアナリシスの実施(仕様書、及び安全要求使用書により、危険源の同定と評価・査定)

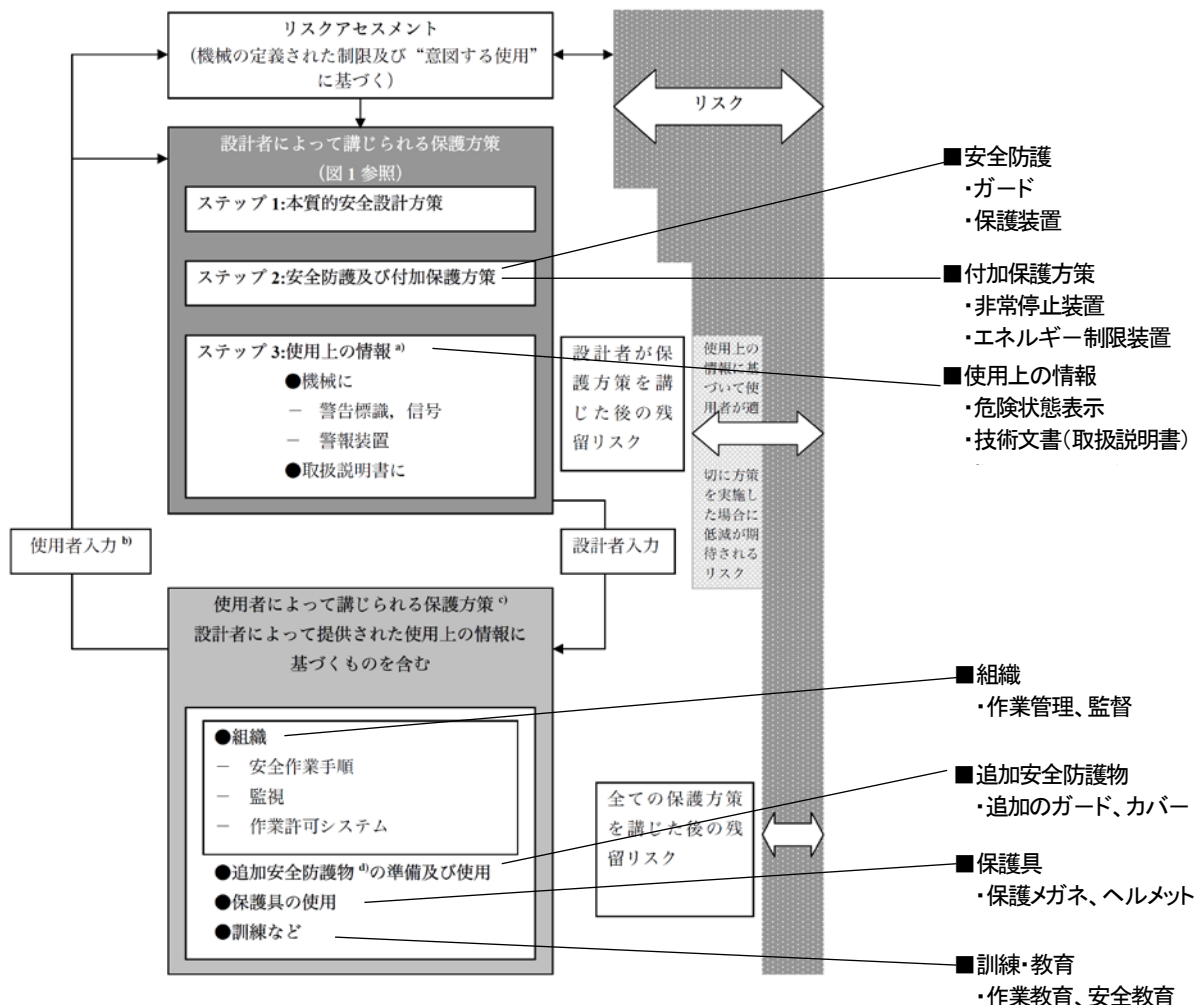
(4) 機械の制御システムのリスク低減・安全の確保

・リスクを低減するための保護方策と安全関連部設計のための安全機能の特定
・安全カテゴリー(B・1・2・3・4)の決定と詳細設計(通常の制御の設計・安全関連部の設計)
・設備・機械の製作・据付工事・エネルギー源の接続方法

(5) 安全立証のための妥当性検証

・妥当性検証(通常の制御部を含めた安全関連部を検証)
・技術書類(据付・操作・保全マニュアル、妥当性検証報告書)の作成

[2] 制御システムの保護方策



■ 制御システム

(1) 本質安全設計 (Step 1)

制御システムにおける安全設計は、機械装置の安全基本仕様として源流設計段階で対応する。

- ・同じ機能を達成するためにより安全な方法を採用する。
[例] 表示機能として、CRTの代わりにLCD 表示装置とする。
- ・エネルギーを最小限にして制御電源は、安全電圧(SELV)とする。
- ・感電しない電気回路(保護接地)の構築

(2) 安全防護 (Step 2)

機械の安全では、保護方策として隔離の原則に従ったガードを使用するが、
制御の安全では、停止の原則に基づく保護デバイス(動作制限・インターロック)によって安全を確保する。

1) 安全ガード(主に機械的手段による保護方策)

- ・固定式ガード、可動式ガード、調整式ガード
- ・インターロック付ガード、施錠式インターロック付ガード

2) 安全保護デバイス(制御装置による保護方策)

- ・インターロック装置、イネーブル装置、ホールドツーラン制御装置
- ・両手操作制御装置、検知保護装置(セイフティ・ライトカーテン、レーザスキャナ)
- ・能動的電光保護装置、機械的拘束装置、制限装置、動作制限制御装置

3) 安全付加保護方策

- ※緊急時や、予見可能な通常作業・保全作業に必要となる保護方策
- ・非常停止装置(非常停止ボタン、セーフティスイッチ)
- ・動力供給の遮断、及び蓄積エネルギーの開放(又は、封じ込め)に関する方策(ロックアウト)
- ・人の脱出、救助のための方策(脱出・救助用の手動手段や要具)
- ・機械、及び重量構成部品の容易で安全な取扱に関する準備(付属要具の常備)
- ・機械類への安全な接近に関する方策(階段、はしご、プラットフォーム、ガード)

(3) 使用上の情報 (Step 3)

1) 残留リスク

機械の制限事項と意図する使用 (Intended User) を明確にして残留リスクについて、使用者に情報提供する。

- ・表示、標識、絵文字、警告文(PLラベル、注意・警告シール)
- ・安全に関する文書(設置マニュアル・操作マニュアル・保守マニュアル)

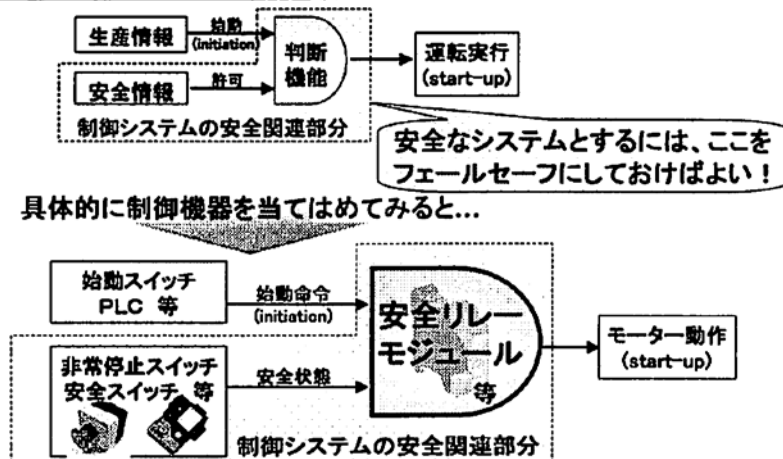
2) 機械の制御システム内の安全関連部の位置付け

安全関連部は機械の制御システムに含まれるが、機能が損なわれることによって安全が損なわれることがあってはならない。

非安全関連部の制御機器の始動命令と保護装置の安全確認信号が揃って、動力制御要素の安全リレー、又は安全リレーユニットから運転起動信号が出力され動力出力機器が作動する。

安全に関わる制御の分離

一般的に制御システムは、安全に関わる制御と生産(非安全)に関わる制御で構成されている



【事例:制御システム】

■課題 1. リスクレベルの決め方 2. 緊急停止スイッチ 3. 外部コントロールによる緊急停止の方法	■管理番号 J-FSS2013-01 Rev.0					
	■分類 ※ ●印:該当する項目					
	【分類1】					
		1. 法規制・規格 (制度・スキーム関連)				
	●	2. 安全規格・技術 (メーカー規格・技術関連)				
■概要 現行の装置は、親機がコントロール(ソフトウェア通信)しているリスクの可能性のある子機に非常停止機能を含めた制御方法となっていたが、規格の要求に適合しているか？		3. 試験規格・方法 (認証機関・試験所関連)				
		4. 全般				
	【分類2】					
		機械安全		EMC	●	RA(リスクアセス)
	●	電気安全		RoHS		環境
	光安全		R&TTE		省エネ	

【1】相談内容

- (1) UV 光照射不停止における紙残存時には、紙焼損のリスクがある。
 現状 ON/OFF は、各 LED ドライバーに RS485 で通信制御している為、照射中に万一通信障害が発生した場合、照射を停止出来ない可能性がある。そこで、正面パネル緊急停止ボタンに、メイン電源ブレーカースイッチを OFF する内部付属装置(電源引きはずし装置)を追加、或いは、緊急停止ボタンを押した場合、制御基板からのコマンドによりドライバー出力を直接遮断 する事を検討中です。いずれの手法が望ましいでしょうか？ ※印刷装置全体の緊急停止ボタンでないで、スイッチの背面は黄色
- (2) 対象機械の規格は、ISO12643-1,2:2009 があります。
 その中では、ISO12643-1 6.6 高接触温度 6.8.2 紫外線放射 ISO1643-2 11.6.5 * * 高温接触温度 付属書 A(「参考」) 機械の危険源で規定されていますが、内容は、紫外線漏れ量と温度対策(カバーや警告ステッカ)しかありません。被害の度合い(ISO13849-1 のリスクフロー)を決めないと PL レベルが決まらないので、回路カテゴリも決まりません。PLb 程度ならドライバ遮断で OK ともなります。
 重度なら PLd ですから、2 重化が必須です。使用者の機械メーカーには、使用時の注意と残留リスクを取説への記載で対応する予定です。

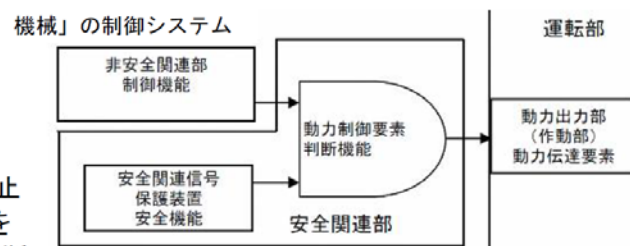
★回答:

まずは、すべての危険を同定してください。『照射不停止における紙残存時には、紙焼損の可能性がある』これは、どの程度のリスクですか？***頻度も重要***です
 色は、“黒色”を“赤色”に変更 ← “赤色”は規格要求(非常停止)有り
 形状は緊急停止と区別出来る形(キノコ型ではなく)緊急時はブレーカー遮断←ブレーカー遮断は緊急不可リスクレベルが決まれば、それに対応した安全制御方式を採用して回路、構造に反映することになります。

【2】提案

本体装置とは別にリレー用電源を駆動させ、非常停止時にリレー接点 ON(リレー電源 OFF)で装置のブレーカーが OFF になる構成にする。(b 接点)にすること。

機能制御系と安全制御系は、独立系統で構成して、機能コントロールが損じても安全は確保される制御方式とすること。



【3】解決方法

親機の機能コントロール信号と安全関連部の緊急停止信号の指令ラインを別(独立)にして、その制御動作を判断させる回路に変更、非常の場合には元電源を遮断しないで UV-LED の照射を停止する構造にする。

■メーカー(業種) ※ ●印:該当する分野		■受付	
検査・計測機器	医療機器	■開始	
情報機器	家電	■終了	
● 産業機器	その他	■作成者 SF(FSS)	

[3] 安全確認型

安全確保の方法には、

- ・安全方策の信頼性の向上による「確率的な安全」と、
- ・安全の立証による「確定的な安全」がある。

信頼性による確率的な安全では、人が危害を受ける可能性が残るが、安全立証による確定的な安全では機械が停止しても人は危害を受けない。

機械の安全確保を確定的な安全で達成するシステムを**安全確認型**という。

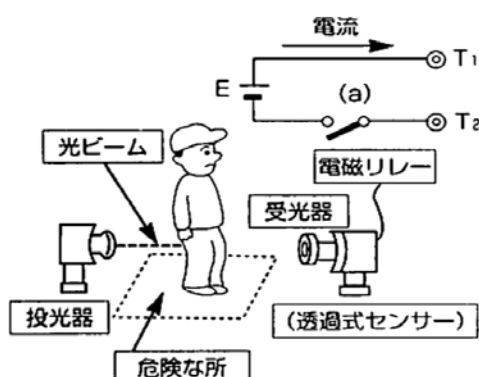
(1) 安全確認型と危険検出型の比較

■ **安全確認型**: 安全が確認されている間だけ機械装置が起動し、安全を確認できなければ起動しない、あるいは運転中であれば停止する制御構成

■ **危険検出型**: 危険検出型とは、危険を検出すれば機械装置は停止するが、危険が検出できなければ危険状態にあっても機械装置は起動し、運転中なら停止しない制御構成

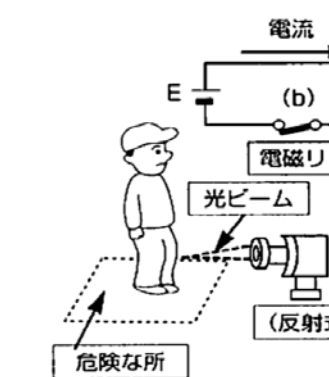
	安全確認型	危険検出型
透過型光電管 (セーフティ・ライト・カーテン) と拡散反射光電管		
光電管 運転方式	ライトオン(正常時オン) 人が光を遮っていない時、 安全確認信号を伝送する。	ライトオン(異常時オン) 人を検知すると、危険検出 信号を伝送する。

(a) 安全確認型システム



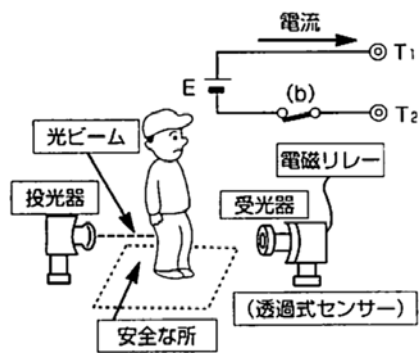
危険な所に人がいないとき、接点(a)がON状態となって、電流が出力される

(b) 危険検出型システム



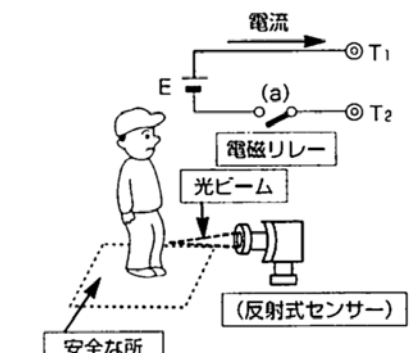
危険な所に人がいるとき、接点(b)になって、電流は出力されない

(c) 危険検出型システム



安全な所に人がいるとき、接点(b)がOFF状態となって、電流は出力されない

(d) 安全確認型システム



安全な所に人がいるとき、接点(a)がON状態となって、電流が出力される

※出典: 安全原則 (SOSTAP)

(2) 機械装置の運転・停止状態の比較

安全確認型は機械装置の不具合(障害)の発生で安全機能を喪失せず、機械装置を停止状態にして安全の状態にする。
危険検出型は、不具合の発生により安全機能を喪失して、機械装置の運転状態が継続して危険状態になる。

■ **安全確認型**: 不具合(障害)の発生で安全機能を喪失せず、
機械装置を停止状態にして安全を確保

■ **危険検出型**: 不具合(障害)の発生で安全機能を喪失し、
人が遮っても機械装置が危険状態で継続運転

	安全確認信号 (出力接点)	機械状態	危険検出信号 (出力接点)	機械状態
投光器・受光器 故障	オフ(接点開)	停止(安全)	オフ(接点開)	運転(危険)
電源線の切断	オフ(接点開)	停止(安全)	オフ(接点開)	運転(危険)
信号線の切断	オフ(接点開)	停止(安全)	オフ(接点開)	運転(危険)
光軸のずれ	オフ(接点開)	停止(安全)	オフ(接点開)	運転(危険)
レンズの汚れ	オフ(接点開)	停止(安全)	オフ(接点開)	運転(危険)
正常運転時 (人を検知)	オフ(接点開)	停止(安全)	オン(接点閉)	停止(安全)

(3) 安全カテゴリー

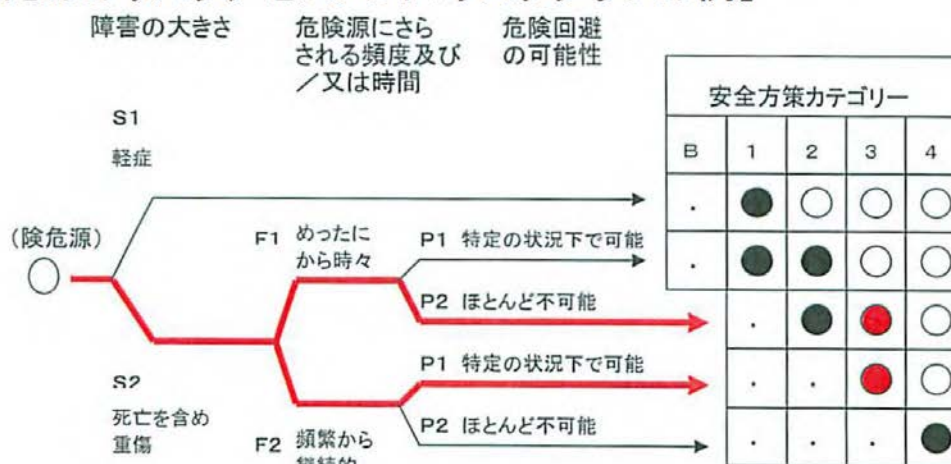
安全カテゴリーとは、制御システムの安全関連部の設計に要求(ISO 13849-1)されている不具合(障害)に対する安全機能の維持能力の分類したもので安全確保のためのリスク低減が制御機能による場合、制御システムで生じる故障に対する安全性の達成レベル(Performance Level)を意味する。

[4] 制御システムにおける安全カテゴリー

リスクアナリシスによって同定された危険(リスク)カテゴリーに対応した制御システムで達成されなければならない安全方策のカテゴリーのことである。

- ・ **制御システムの安全関連部の設計に要求される事項**
- ・ **不具合(障害)に対する安全機能の維持能力の分類**

【安全方策のためのリスクアセスメント: リスクグラフの例】



※出典: 安全方策カテゴリー分類 (SOSTAP)

Example of Risk Analysis

(1) ISO 13849 Analysis

1. Identification of safety function to be performed by the safety related part of the control system

The only safety-related function of the control system which is employed within the FSS controller is the emergency stop circuit. Standard FSS do not require guarding or other interlocks to control access to the machine. The emergency stop system will mainly protect against crushing or trapping hazards.

2. Required characteristics

The required characteristics of the emergency stop system have been determined as follows.
(the reference numbers relate to the clause numbers of ISO 13849-1)

1) Relevant standards

- ISO13850: emergency stop function
- ISO14118 prevention of unexpected start-up

2) Safety related stop function

Activating the emergency stop will immediately put the machine into a safe state

3) Manual reset function

Stop condition will only be cancelled by a manual reset operation.

4) Start/Restart function

Start/restart can only be activated manually.

5) Local Control function

Selection of local control, ie hand-box is achieved automatically by the pc system which is located outside the danger zone, selecting local control does not create a hazardous situation.

6) Muting function

No muting capability.

7) Response time

The response time will be fast enough to provide stopping of the machine motion within a suitable distance.

8) Safety related parameters

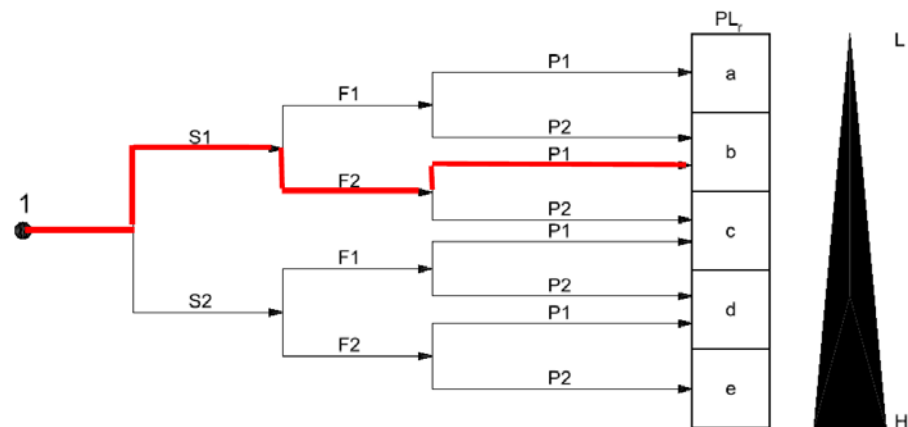
No requirement, as the system is not programmable.

9) Fluctuations, loss & restoration of power sources

The system, being contactor-based, will be insensitive to power fluctuation, and will fail-safe if power is lost. It will require re-setting when power is restored.

(2) Risk Estimation and the determination of the required Performance Level [PLr] of emergency stop circuit

This analysis is based on the methods and risk graph outlined in ISO 13849-1



Key

- 1** Starting point for evaluation of safety function's contribution to risk reduction
- L** low contribution to risk reduction
- H** high contribution to risk reduction
- PL_r** required performance level

Risk parameters:

- S** severity of injury
 - S1 slight (normally reversible injury)
 - S2 serious (normally irreversible injury or death)
- F** frequency and/or exposure to hazard
 - F1 seldom-to-less-often and/or exposure time is short
 - F2 frequent-to-continuous and/or exposure time is long
- P** possibility of avoiding hazard or limiting harm
 - P1 possible under specific conditions
 - P2 scarcely possible

Risk Graph for Determining Required Performance [PLr] Level for Safety Function

The emergency stop circuit is the main safety related part of the control system. The rationale for determining the required performance level PL_r is as follows:

Severity of injury

S1 Slight injury

The mechanical 'friction' drive mechanism is such that it will slip if it meets resistance.

Frequency of exposure to the hazard

F2 Frequent exposure

Depending on how the FSS is utilised and its design, the exposure could be frequent. If the machine is being used for part-program development or manual inspection, and it is a large bridge or horizontal arm style where the operator can move into the working volume, then the exposure could be frequent.

Possibility of avoiding the hazard

P1 Possible to avoid hazard

FSS accelerate and move relatively slowly so it should be possible to avoid the hazard. The machine is normally operated by a trained operator.

Severity of Injury	Frequency of exposure	Possibility of avoiding hazard	Performance level PL _r
S1 Slight	F2 Frequent to continuous	P1 Possible	b

■ 安全カテゴリーの分類

制御システム内で構築される安全関連部の安全機能の要求事項と維持能力は、カテゴリー(B,1,2,3,4)別に分類される。

表 I.1 制御システムの危険事象発生確率低減の要求事項 (ISO13849-1)

保護方策 カテゴリー	要求事項	安全機能の維持能力 (不具合*発生時の挙動)	入/出力 関係
B	・機械制御システム安全関連部の目的機能を実現すること。	・不具合発生時安全機能を損う場合が十分起こり得る。	$A_i = B_o$ $A_i: 2$ 値 入力 $B_o: 2$ 値 出力
1	・カテゴリーBの要件を満たすこと。 ・十分に吟味された高信頼性のコンポーネントの使用および安全原則に従うこと。	・カテゴリーBと同様であるが、安全関連部の安全確保機能の信頼性は高い。	
2	・カテゴリーBの要件を満たすこと。 ・安全の確保は十分に吟味された安全原則に従うこと。 ・安全機能は適当な間隔でチェックされること。	・安全機能の消失はチェックによって検出されるが、チェック間隔時間の間では安全機能を損なう。	$A_i \geq^{2)} B_o$
3	・カテゴリーBの要件を満たすこと。 ・安全の確保は十分に吟味された安全原則に従うこと。 ・設計要件：単一不具合で安全機能を損わない。単一不具合はできる限り検出されること。	・単一不具合で安全機能が損われない。 ・すべてではないが、不具合の検出ができる。未検出の不具合の蓄積で安全機能を損う場合がある。	$A_i \geq^{3)} B_o$
4	・カテゴリーBの要件を満たすこと。 ・安全の確保は十分に吟味された安全原則に従うこと。 ・設計要件：単一不具合は安全機能実行時、若しくはその前に検出されること。それを実施できない場合不具合の蓄積で安全機能を損わないこと。	・不具合が生じた場合、常に安全機能は損われない。 ・不具合は安全機能実施の前の段階で必ず間に合うように、予防措置として検出される。	$A_i \geq^{4)} B_o$
* リスクアセスメント上での危険事象：安全確保の保護方策の不具合の結果として生じる			

表 I.2 保護方策カテゴリーの技術的方法と危険事象の発生モード

カテゴリー	保護方策	安全原則	危険事象*モード
B	制御機能実現	基本安全原則	不具合発生時危険
1	高信頼化	“十分に吟味された”安全原則	不具合発生時危険（確率小）
2	チェックによる機能確認		チェック間隔間で危険
3	機能確認付二重系		不具合の蓄積で危険
4	連続的機能確認、ダイバーシティ**		不具合の蓄積配慮
*危険事象：安全方策の不具合の結果として生じる		**異種技術の適用	

※出典：基本安全規格 ISO13849-1の安全原則 (SOSTAP)

■ 安全関連用語

(1) 基本安全原則

制御システムの安全関連部の設計・製作・選択・編成・組立に関する安全原則で、以下を考慮すること。

- ・予想される負荷状態(遮断容量、及び頻度に対する信頼性)
- ・作業過程に用いられる材料の影響
- ・外部の電磁界、エネルギー供給の中断、又は停止

(2) 十分に吟味された安全原則

- ・特定の障害の回避(間隔による回路短絡の回避)
- ・障害の発生確率を低減(マージン設計)
- ・安全状態での故障(不具合発生時の動力遮断)
- ・障害の早期検出(地絡検出回路)
- ・障害の影響の抑制(機械設備の接地)

(3) 十分に吟味されたコンポーネント

- ・過去の安全実績のある、又は類似コンポーネント
(ヒューズ、ブレーカ、電磁接触器 等)
- ・安全関連適用例で立証検証されたコンポーネント
(非常停止スイッチ、イネーブルスイッチ 等)