機能安全活用実践マニュアル

別冊１　演習用教材

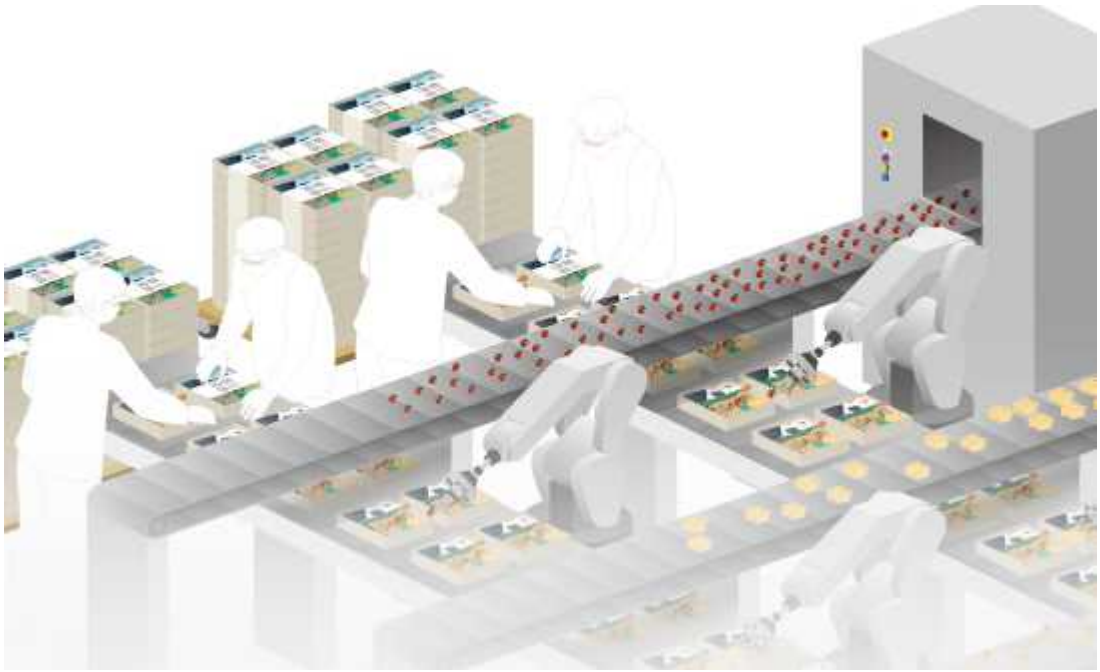
平成 29 年度厚生労働省委託
機能安全を活用した機械設備の安全対策の推進事業

平成 30 年 3 月
中央労働災害防止協会

Ⅰ　産業用ロボットシステムに関する演習教材

１　　演習事例

本章では、協働作業ロボットについてリスクアセスメント、リスク低減対策及び妥当性確認までの演習を行う。



図Ⅰ-1　弁当箱詰めロボット（IDEC ファクトリーソリューションより）

対象とするロボットシステムは図Ⅰ-1 の弁当箱詰めロボットシステムであり、基本構成とタスクは次の通りである。

・ロボット及び人間が協働で弁当具材を弁当箱に詰める作業を行う。
・右側のフライヤー/オーブンから調理された具材が上側のコンベアで運ばれてくる。
・弁当箱は下側のコンベアで右から左奥（作業者側）に運ばれる。ロボットは上側のコンベアの具材を掴んで、弁当箱の所定の位置に詰める＝12 セット/分
・作業者は弁当のパッキング内容を確認し、包装及び台車に載せる。
・弁当に不備（詰め忘れなど）があれば、作業者が該当コンベア（ロボットの近く）に行って具材を詰めなおす＝3 分に 1 回程度
・平均 30 分ごとに弁当メニューが切り替わる。ロボットのハンドは変更なく、プログラムが切り替わる。
・一日の作業終了時に、ロボット、コンベア等の清掃およびメンテナンスを実施する

・清掃作業のし易さのため、可能ならロボットにガードをつけたくない。
・作業者が具材コンベアに近づいても、ロボットを非常停止したくない＝再起動に時間がかかるため。

２　リスクアセスメントとリスク低減方策

表Ⅰ-1　協働作業ロボットの仕様一覧

分類	項目	仕様・制限
工程概要	ロボットを含む各装置類の配置	
	製品・材料の流れ	
	加工・作業内容、加工時の副生物・放出物（フューム、アーク光、熱、音、電磁波、放射性物質）・廃材などの性状・性質・量	
	タクトタイム、サイクルタイム	
	稼働時間（日／月／年）、生産台数（時間／日／年）	
	周辺装置・他の機械や建屋の壁・柱等との距離・空間	
本体	大きさ、形状、機構	
	駆動源・機構	
	質量・重心・モーメント	
	最大可動範囲	
	最大可搬重量	
	最大動作速度	
	設置方法	
エンドエフェクタ	重量、重心	
	駆動源・機構	
周辺装置	大きさ、形状、	
	重量、重心	
	形状	
	駆動源・機構	
動作	軌跡	
	速度	
	待機位置・姿勢	
	起動・停止条件	
製品･材料	製品	
	材料	
	副資材	
	副産物	
使用条件	周辺環境	
	空間的条件	
	関係者	

(1)　機械の使用制限

図Ⅰ-1 の中央のロボットに関して、リスクアセスメントに必要な機械の使用制限を列挙しなさい。機能安全活用実践マニュアルロボットシステム編(以下「ロボットマニュアル」という。)第 3 章 1（1）を参考にして、表Ⅰ-1 の様式にまとめなさい。なお、前頁の説明に書かれていない仕様や制限については、本演習に限り空白でもよい。

(2) リスクアセスメント

図Ⅰ-1 の中央のロボットに関して、リスクアセスメントを実施しなさい。コンベア、フライヤーについてリスクアセスメントする必要はない。添付の表Ⅰ-6 を使用すること。

・ロボットに関する危険源は、ロボットマニュアル第 3 章表 3-8, 表 3-9 を参考にして、表Ⅰ-2 に記入すること。
・ロボットに関する作業は、ロボットマニュアル第 3 章表 3-10 を参考にして、表Ⅰ-3 に記入すること。
・リスクの見積もり・評価は、ロボットマニュアル第 3 章の表 3-15、表 3-16、表 3-17、表 3-18 に基づいて実施すること。
・表Ⅰ-6 の記載方法は、ロボットマニュアル第 3 章の表 3-14、表 3-18 を参考にすること。

表Ⅰ-2 ロボットシステム危険源洗い出しシート例

危険源の種類 / 構成要素	機械的				電気的	熱的	騒音	振動	放射	材料物質		人間工学	環境	組合せ
	動力（挟まれ等）	重量物	滑り・躓き・墜落	その他（切創等）						有害物質	爆発・火災			
ロボット*1														

*1：エンドエフェクタ含む

表Ⅰ-3　ロボットシステム作業洗い出しシート例

フェイズ	作業内容
運搬	
据付	
調整	
生産	
段取り	
保全	
トラブルシューティング	
廃却	
その他	

(3)　リスク低減方策

リスクアセスメントの結果、リスクが 4 の危険源および危険事象に対して、リスク低減方策を考えなさい。ロボットマニュアル第 3 章の表 3-19 を参考に、表Ⅰ-6 のリスク低減方策の列に記載しなさい。

ただし、顧客の要求事項である、「可能であればガードなし」を考慮すること。

ロボットのリスク低減方策は、ロボットマニュアルの第 5 章を参考にすること。

(4)　リスク低減方策の効果－リスクアセスメント

上記のリスク低減方策の効果を評価しなさい。ロボットマニュアル第 3 章表 3-20 に従って、リスク低減方策を実施後の条件下での、リスクを見積もりなさい。表Ⅰ-6 の保護方策後：リスク見積もりの列に記載しなさい。

もし、その結果がリスク 3 以上の場合は、追加のリスク低減方策を検討しなさい。

(5) リスク低減方策の要求安全度水準（PLr）

上記のリスク低減方策のうち、制御システムによる方策について、ロボットマニュアル第 4 章に従って要求安全度水準 (PLr) を求めなさい。同第 4 章図 4-1 に従って求め、表Ⅰ-6 のリスク低減方策の制御方策要求安全度水準（PLr）の欄に求めた PLr のレベルを記載しなさい。

３　リスク低減方策の実現

(1) 安全適合監視速度

図Ⅰ-1 のロボットのリスク低減方策として、作業者がロボットに接近すると、それを検知してロボットを減速させる速度制御（JIS B 8433-1 (ISO 10218-1) 5.6.4 安全適合監視速度）を採用するとする。

・ロボットアームの可動範囲(具材コンベアから弁当コンベアまでの半径 1m)を速度制御の範囲とする→レーザースキャナにより作業者の進入を検知する。
・レーザースキャナはロボット基部、コンベアよりも高い位置に配置する。なお、ロボット後方には人が立ち入らない。ロボットに対して弁当コンベア側から接近する。
・速度制御範囲に作業者が入ると、ロボットのハンドツール部の速度を 200mm/s 以下とする。
・また、ロボットはこの速度を監視し、速度超過時には保護停止する。
・安全適合監視速度の機能を有するロボットを選択する。
・このリスク低減方策は、PLr=d の要求がある。

(2) 安全システム構成

レーザースキャナとロボット安全制御装置のシステム構成図を作成しなさい。

なお、レーザースキャナは、OSSD1/OSSD2 の出力信号を持ち、ロボット安全制御装置は、安全適合速度監視用の SLS1/SLS2 の安全入力端子を持つ。それぞれの信号仕様を表Ⅰ-4 に示す。

表Ⅰ-4　安全機器の信号仕様

安全機器	信号/端子	意味
レーザースキャナ	OSSD1/OSSD2	ON:速度制御範囲に進入なし OFF:速度制御範囲に進入あり
ロボット安全制御装置	SLS1/SLS2	ON:通常運転速度 OFF:減速運転(安全適合監視速度)

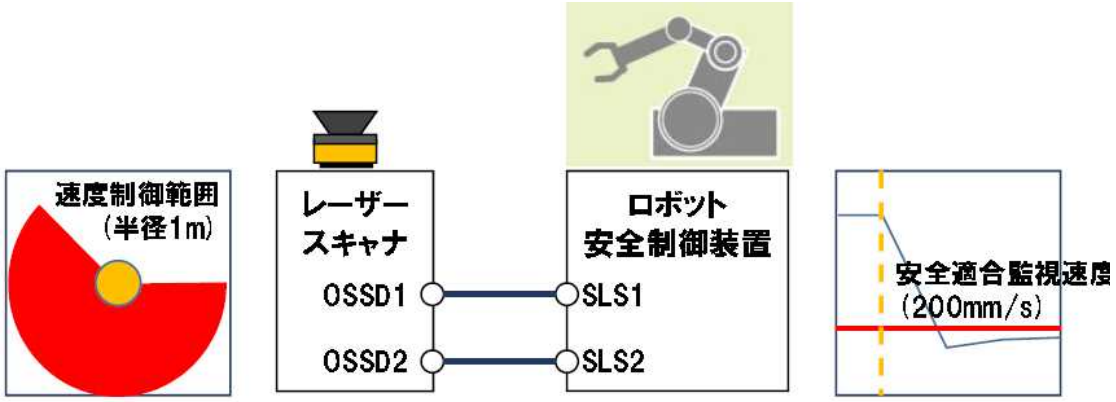
(3)　安全機器の設定パラメータ

レーザースキャナ（速度制御）、ロボット安全制御装置に対して設定する安全関連パラメータを決めなさい。

・レーザースキャナ：速度制御を行う範囲（エリア）

・ロボット安全制御装置：安全適合監視速度（上記エリア内に人が侵入したときの制限速度）

【解答例】



図□-2　安全システム構成図および設定パラメータの設定例

4　妥当性確認

(1)　安全関連システムの PL 評価

前節の安全適合監視速度を実現する安全関連システムについて、PL を求めなさい。図Ⅰ-3 の記入様式に、ロボットマニュアル第 6 章 4 節に従ってパラメータを記入しなさい。

なお、レーザースキャナとロボット安全制御装置の MTTFd および DCavg は表Ⅰ-5 とする。その他のリスク低減方策も含め制御方策に関わる方策の妥当性確認結果を表Ⅰ-6 右端の制御方策妥当性確認（PL）の欄に求めた PL のレベルを記載しなさい。

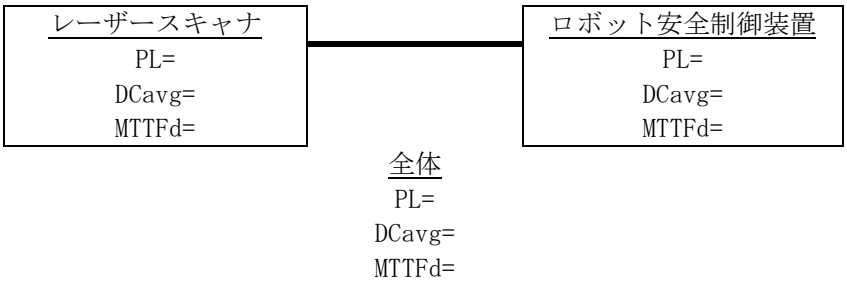
(2)　妥当性確認

上記の結果が、リスク低減方策の安全要求性能を満足したか、確認しなさい。

表Ⅰ-5　安全機器の PL 関連パラメータ

安全機器	DCavg	MTTFd[年]	PFHd[1/時間]	PL
レーザースキャナ	97%	56	1.03×10^{-7}	d
ロボット	92%	47	1.34×10^{-7}	d

【解答】



図□-3　安全関連システムの妥当性確認

表Ⅰ-6 リスクアセスメントシート（弁当箱詰めロボット対象）

No	作業-危険源-危険状態-危険事象	保護方策前：リスク見積				リスク低減方策	制御方策	保護方策後：リスク見積					制御方策
		ひどさ S	頻度 F	回避 P	リスク		要求安全度水準(PLr)	ひどさ S	頻度 F	回避 P	確率 O	リスク	妥当性 (PL)
例	作業者が具材を取るためコンベアに接近時にロボットハンドと衝突、または作業台との間に挟まれる	S2	F2	A2	4	作業者がロボットに接近すると、ロボットを減速制御する（JIS B 8433-1 5.6.4 安全適合監視速度）	d	S2	F2	A2	01	2	d
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													

Ⅱ　ボイラーに関する演習用教材

演習事例

1. リスクアセスメントシート作成

(1) リスク分析、要求安全機能の特定

機能安全活用実践マニュアルボイラー編(以下「ボイラーマニュアル」という。)図 2-6　バーナ空気量不足の FTA 図例に基づき、空気量不足によるバーナ異常失火のリスク分析し、要求安全機能を特定しなさい。結果は、演習シート 1 の要求安全機能(No,キーワード,危険側故障,危険事象,検出方法,要求安全機能、作動要求に関する事項)の欄に記入すること。

なお、仕様、使用条件、保守点検、バーナ系統、燃焼制御系機能ブロック図は、-ボイラーマニュアルの下記の図表を条件とする。不足する情報があれば、各自で条件/仕様などを設定するか、その部分は空白として演習を進めること。

表 1-2 ボイラーの仕様例
表 1-3 ボイラーの使用条件、保守点検
表 1-4 部品点検・交換リスト例
図 2-3 ガスバーナ制御系統の例
図 2-4 燃焼制御系機能ブロック図例

(2) 要求安全度水準の決定、使用者への情報

(1)で特定した要求安全機能の要求安全度水準、使用者への情報を決定しなさい。結果は、(1)で作成した演習シート 1 に記入すること。
要求安全度水準の決定にあたって評価した各パラメータ(C,F,P,W)の評価理由を欄外に記載すること。
不足する情報があれば、各自で条件/仕様などを設定するか、その部分は空白として演習を進めてください。

2. SIL の評価

図Ⅱ-1 は、ボイラーマニュアル３．２．４ 低水位/燃焼系遮断の構成例（３）にエア圧スイッチ、エア圧スイッチ入力/RY1 リレー駆動部を追加したものである。
図Ⅱ-2 は、その追加したエア圧スイッチ入力/RY1 リレー駆動部の回路例である。

(1) 信頼性ブロック図

図Ⅱ-1 に基づき、エア圧スイッチ接点開により遮断弁で燃料を遮断する安全機能の信頼性ブロック図を作成しなさい。(演習シート 2-①)

(2) FMEDA 評価

FMEDA シートを使用して、図Ⅱ-2 エア圧スイッチ入力/RY1 リレー駆動部の FMEDA を実施しなさい。(演習シート 3)

●各部品のデータについて

故障率/故障モードのデータは、付録 1 を使用すること、その際にリレーコイルの故障率は 50(FIT)とすること。また診断率は付録 2 を使用し、リレー接点の監視が実施されている条件での診断率を使用すること。

(3) 構成要素の危険側故障率

(1)の信頼性ブロック図で示した各構成要素とその危険側故障率を表で示しなさい。(演習シート 2-②)

なお、リレー接点の危険側故障率は 500(FIT)、エア圧スイッチの危険側故障率は 100(FIT)、遮断弁の危険側故障率は 5000(FIT)とする。

(4) 各構成要素(サブシステム)の PFDavg 算出

各構成要素(サブシステム)の PFDavg を計算し、各構成要素(サブシステム)の SIL(相当値)を示しなさい。(演習シート 2-③)

なお、プルーフテスト間隔などの条件は、1 項の演習内容を参考に設定して、その内容を明記すること。

(5) システムの SIL 値の結論

PFDavg の合計からシステムの SIL 値を算出し、アーキテクチャ制約からの SIL 値を確認し、システムの SIL 値の結論を示しなさい。(演習シート 2-④,⑤,⑥)

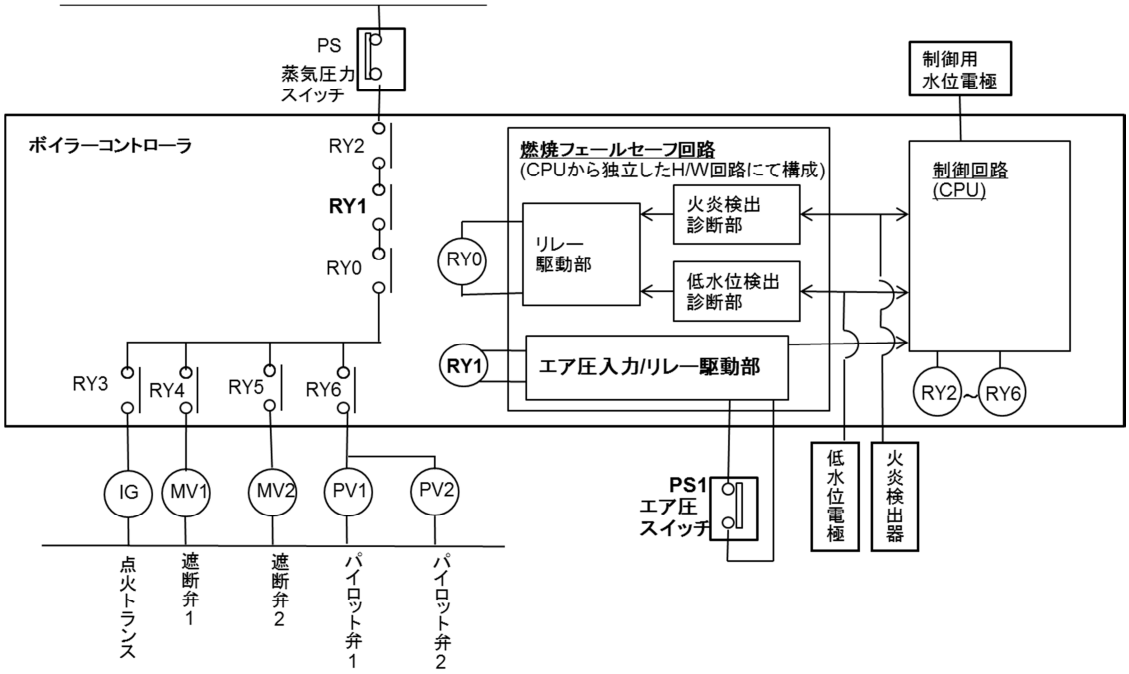


図 Ⅱ-1 演習-構成例

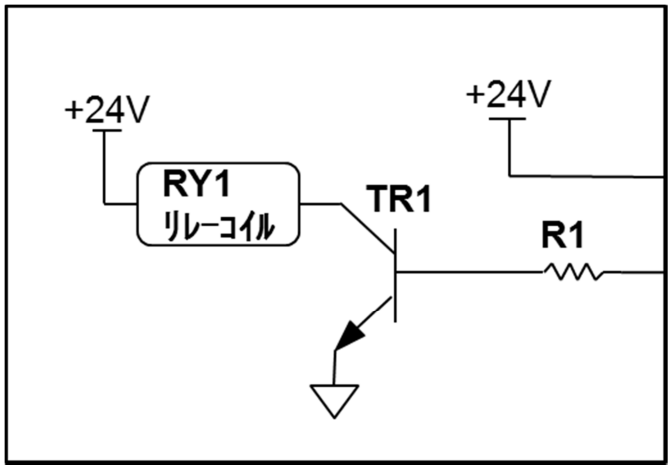


図 Ⅱ-2　演習-エア圧入力/リレー駆動回路

【演習シート１】

要求安全機能の特定							安全度水準決定					取扱説明書記載事項、点検内容など	
No	キーワード	危険側故障	危険事象	検出方法	要求安全機能	作動要求に関する事項 (構造/機械式安全装置)	C	F	P	W	SIL	製造者追加対策	使用者追加対策
各パラメータ(C,F,P,W)の評価理由													

要求安全機能の特定							安全度水準決定					取扱説明書記載事項、点検内容など	
No	キー ワード	危険側故障	危険事象	検出方法	要求安全機能	作動要求に関する事項 (構造/機械式安全装置)	C	F	P	W	SIL	製造者追加対策	使用者追加対策

【演習シート 2】

①信頼性ブロック図

②構成要素の危険側故障率

記号	構成要素	危険側故障率 λD(FIT)

③サブシステムの計算条件と結果

プルーフテスト間隔の設定に対する説明：

項目				
構成(1oo1、1oo2、、)				
PFDavg の計算式(63 ページ参照)				
危険側故障率 λD(FIT)				
DC				
検知不可危険側故障率(FIT)				
検知可能危険側故障率(FIT)				
プルーフテスト間隔 T1(年)				
平均修理時間 MRT(時間)				
平均修復時間 MTTR(時間)				
tCE(時間)				
tGE(時間)				
βD(%)				
β(%)				
PFDavg				
SIL				

④ランダムハードウエア故障確率　PFDavg 合計からの SIL 値

⑤アーキテクチュアの制約からの SIL 値

⑥システムの SIL 値の結論

演習シート 3（FMEDA 評価シート）

番号	部品名称	全故障率(FIT)	故障モード	分配率(%)	故障率(FIT)	安全側/危険側	診断率(%)	λ_{SD}(FIT)	λ_{SU}(FIT)	λ_{DD}(FIT)	λ_{DU}(FIT)	$\lambda_{\text{No Effect Failure}}$(FIT)	$\lambda_{\text{No Part Failure}}$(FIT)

付録１　故障率・故障モード（EN 13611:2007）

EN 13611:2007の故障率データを示す。この故障率はSN 29500をもとにして雰囲気温度60℃、ディレーティングが67%の場合において評価している。また、周囲条件及び(又は)負荷条件が規定値と異なる場合、故障率が再計算されなければならない。
表J.3に含まれるもの以外のコンポーネントの個々の故障率はメーカーによって提供される故障率を使用して決定されなければならない。これは、特にリレー、火炎検出部などに適用することがある。
B10d値を使用したリレーの故障率を決定する方法は、J.5.4.4.3の中で与えられる。

注１　簡単に計算するため、故障率は故障モードの数を考えて同じ割合で分割される。
例えば、ダイオード用の基礎故障率λBは、フォールト・モード「オープン」と「ショート」に分割されて、λopen = λshort = λB/2となる。
注２　表J.3で与えられる故障率と周囲及び負荷条件を計算する方法は、SN 29500シリーズのデータベースから得られた。

故障率・故障モードの使用にあたっては、規格の他の注意事項も参照すること。

表J.3 故障率と故障モード

コンポーネントタイプ	故障モード							故障率	
	ショート	オープン	ドリフト 1/2x	ドリフト 2x	その他	ピン数	フォールト数	コンポーネント故障率 λ (FIT) a	フォールトあたりの故障率 λ (FIT)
列	1	2	2a	2b	2c	3	4	5	6
抵抗									
カーボンフィルム		1				2	1	1.6	1.6
金属フィルム		1				2	1	0.3	0.3
金属酸化膜		1				2	1	8.0	8.0
巻き線型	1	1				2	2	8.0	4.0
抵抗体素子のネットワーク	1	1				2	2	0.2	0.1
可変抵抗器									
巻き線型(一層)		1				3	3	48.0	16.0
その他	1	1				3	6	48.0	8.0
バリスタ	1	1				2	2	1.0	0.5

コンポーネントタイプ	故障モード							故障率	
	ショート	オープン	ドリフト 1/2x	ドリフト 2x	その他	ピン数	フォールト数	コンポーネント故障率 λ (FIT) [a]	フォールトあたりの故障率 λ (FIT)
列	1	2	2a	2b	2c	3	4	5	6
PTC サーミスタ	1	1	1	1		2	4	5.0	1.25
NTC サーミスタ	1	1	1	1		2	4	3.0	0.75
コンデンサ									
EN 60384-16 に従う金属化フィルム:MKT、MKP、MKU		1				2	1	4.3	4.3
EN 60384-16 に従う金属化フィルム:MKC		1				2	1	7.3	7.3
金属箔:KC		1				2	1	20.9	20.9
金属箔:KS、KP、KT		1				2	1	7.4	7.4
金属化紙(フィルム):MP、MKV)	1	1				2	2	12.4	6.2
セラミック:NDK/ LDC, COG, NPO	1	1				2	2	4.8	2.4
セラミック:HDK/MDC、X7R、X5R	1	1				2	2	9.7	4.8
セラミック:HDK/HDC、Z5U、Y5V、Y4T	1	1				2	2	24.2	12.1
アルミニウム電解質(固体電解質)	1	1	1			2	3	2.2	0.75
タンタル電解質(固体電解質)	1	1	1			2	3	51.8	17.3
可変	1	1				2	2	14.0	7.0
インダクタ、変圧器									
LF インダクタ、変圧器	1	1				2	2	7.0	3.5
emc 抑制用インダクタ	1	1				2	2	2.1	1.05
スイッチモード電源の主変圧器および変圧器[b]	1	1			-4	4	6	48.0	8.0
スイッチモード電源の主変圧器および変圧器	1	1				4	10	48.0	4.8
ダイオード等									
ユニバーサル、ショットキーダイオード	1	1				2	2	2.3	1.15
サプレッサーダイオード	1	1				2	2	16.8	8.4
Z ダイオード<1W	1	1				2	2	2.4	1.2
Z ダイオード>1W	1	1				2	2	47.5	23.8
定電圧ダイオード	1	1	1	1		2	4	16.1	4.0

コンポーネントタイプ	故障モード							故障率	
	ショート	オープン	ドリフト 1/2x	ドリフト 2x	その他	ピン数	フォールト数	コンポーネント故障率 λ (FIT) a	フォールトあたりの故障率 λ (FIT)
列	1	2	2a	2b	2c	3	4	5	6
整流ダイオード	1	1				2	2	4.0	2.0
整流器ブリッジ	1	1				4	10	20.0	2.0
ディアック[c]	1	1			2	2	4	150.0	37.5
トランジスタ等									
バイポーラ、ユニバーサル、例えばTO18、TO92、SOT23	1	1				3	6	7.6	1.3
バイポーラ低消費電力､例えばTO5、TO39	1	1				3	6	52.8	8.8
トランジスターのトランジスターアレイ	1	1				3	6	38.0	6.3
バイポーラパワー、例えばTO3、TO220	1	1				3	6	132.0	22.0
FET 接合、MOS	1	1				3	6	12.7	2.1
MOS、パワー、例　TO3、TO220	1	1				3	6	264.0	44.0
サイリスタ[c]	1	1			2	3	8	100.0	12.5
トライアック[c]	1	1			2	3	8	150.0	18.5
集積回路[d e]									
μC/ASIC/PLD≦32pin[CORE]								50.0	
[IC]	1	1				16	57	194.2	3.41
μC/ASIC/PLD＞32pin[CORE]								100.0	
[IC]	1	1				40	153	487.1	3.18
EEPROM	1	1				28	105	310.0	2.95
OpAmp バイポーラ	1	1				8	25	13.8	0.55
OpAmpCMOS、基準要素	1	1				8	25	8.8	0.35
コントローラ（スイッチングレ	1	1				6	1	23.0	1.35

コンポーネントタイプ	故障モード							故障率	
	ショート	オープン	ドリフト 1/2x	ドリフト 2x	その他	ピン数	フォールト数	コンポーネント故障率 λ (FIT) [a]	フォールトあたりの故障率 λ (FIT)
列	1	2	2a	2b	2c	3	4	5	6
ギュレータ)							7		
トランズミッタ/レシーバ/ADC	1	1				8	25	23.0	0.9
CMOS/TTL 論理ゲート	1	1				16	57	11.5	0.2
光電子コンポーネント									
フォトカップラー、バイポーラ出力	1	1				4	10	42.0	4.2
フォトカップラー、FET 出力	1	1				4	10	104.0	10.4
Si フォトダイオード/Si PIN フォトダイオード	1	1				2	2	5.7	2.9
Ge フォトダイオード	1	1				2	2	185.0	92.5
Si フォトトランジスタ	1	1				3	6	6.3	1.05
フォトエレメント	1	1				2	2	6.0	3.0
フレームセンサー（光レジスター等）[f]	1	1				2	2		
UV 管	1	1				2	2	50000	25000
リレー[g]									
コイル	1	1				2	2		
接点	1	1				2	2		
クリスタル、水晶発振子[h]	1	1				2	2	15.0	7.5
セラミック共振子[h]	1	1				2	2	5.0	2.5
ヒューズ		1				2	1	25.0	25.0
避雷器（ガス充てん）	1	1				2	2	1.0	0.5
スイッチ									
DIP スイッチ、接点あたり	1	1				2	2	0.3	0.15
パワースイッチ、接点あたり	1	1				2	2	80.0	40.0
ジャンパー		1				2	1	1.0	1.0

コンポーネントタイプ	故障モード							故障率	
	ショート	オープン	ドリフト 1/2x	ドリフト 2x	その他	ピン数	フォールト数	コンポーネント故障率 λ (FIT) a	フォールトあたりの故障率 λ (FIT)
列	1	2	2a	2b	2c	3	4	5	6
ケーブル		1				2	1	1.0	1.0

注　列の説明:

1;2　EN 13611 からの故障モード

2a、2b　故障モード「公称値の半分のドリフト」、「公称値の 2 倍までのドリフト」、

2c　特別な故障モード(脚注を参照)

3　コンポーネントあたりの接続ピンの数

4　1、2、2a、2b、2c 及び 3 に起因するフォールト数

5　コンポーネントあたりの故障率(脚注 a を参照)

6　フォールトあたりの故障率

a 故障率は、基礎故障率、EN 13611 の最大周囲温度条件(+60℃)に基く温度依存ファクター π_T、$U/U_{max} = 0.7$(EN 61508-2:2010,7.4.2.13 による 67%のディレーティング)で計算された電圧依存ファクター π_U 及び負荷依存ファクター π_L に対して計算される。

b 故障モード排除「短絡回路 1 次/2 次」("-4 は次を意味する:フォールト総数は排除された短絡の数によって減少する」)。

c 2c 列の故障モード「半波モード A/K」、「半波モード K/A」。

d 3 列にピン数の入力(n =ピンの数)。

e 故障率$_{[IC]}$=故障率$_{[CORE]}$+(n *故障率$_{[バイポーラトランジスター]}$/3)　→4 列

$N_{[IC]}$＝故障モード数= $N_{[短絡]}$＋$N_{[断線]}$

$N_{[短絡]}$=(n-1)+(n - 2)+(n - 4);

隣接ピンの短絡、およびピンと+V_{CC} 間の短絡及びピンと V_{CC}(GND)間の短絡。

$N_{[断線]}$= n

f 個々に決定されること;J.5.4.4.2 を参照

g 故障率は個々のコンポーネントに対して決定されなければならない;J.5.4.4.3 を参照。故障率は各接点に適用される。

h 低調波/高調波は、EN 13611 によってカバーされる。

付録２　診断率（EN 13611:2007）

表 J.1 と表 J.2 は関連する診断率（DC)のレベルを達成するランダムハードウェア故障を検知・制御する診断テストの技術と方策を提供する。
診断テストが下表の「参照」の要求事項に適合する場合に、その診断率(DC)を計算に使用してもよい。他の方策および技術は、主張された診断率を支援する証拠がある場合に使用できる。

表 J.1- 診断技術

診断技術	参照	DC	備考
オン・ライン監視による故障検出	EN 61508-2:2010、A.2、A.3	90 %	故障検出の診断率に依存する。
アイドル電流原理	EN 61508-2:2010, A.2, A.15	60 %	電気機械システム、アクチュエータ
リレー接点の監視	EN 61508-2:2010、A.2、A.15	99%	電気機械システム、アクチュエータ
コンパレータ	EN 61508-2:2010、A.2、A.3	99%	主として故障モードが安全側にある場合、高
多数決投票	EN 61508-2:2010、A.2、A.3	99%	投票の質に依存する。
冗長ハードウェアによるテスト	EN 61508-2:2010、A.3	90%	故障検出の診断率に依存する。
動的な原理	EN 61508-2:2010、A.3	90%	故障検出の診断率に依存する。
監視冗長	EN 61508-2:2010、A.3	90%	故障検出の診断率に依存する。
タイムウィンドウのない分離したタイムベースのあるウォッチドッグ	EN 61508-2:2010、A.10、A.12	60%	プログラムシーケンス、クロック
タイムウィンドウのある分離したタイムベースのあるウォッチドッグ	EN 61508-2:2010, A.10, A.12	90%	プログラムシーケンス、クロック
プログラムシーケンスの一時的・論理的な監視の組合せ	EN 61508-2:2010、A.10、A.12	99%	プログラムシーケンス、クロック
安全シャット・オフのある過電圧保護	EN 61508-2:2010、A.9	60%	電源
安全シャット・オフのある二次電圧制御および防護	EN 61508-2:2010、A.9	99%	電源

表 J.2 診断方策

診断方策	参照	DC	備考
テストパターン	EN 61508-2:2010, A.7	99 %	I/O 装置
アナログ信号監視	EN 61508-2:2010, A.3, A.14	60 %	I/O 装置、センサー
リファランスセンサー	EN 61508-2:2010, A.14	90 %	センサー
修正チェックサム	EN 61508-2:2010, A.5	60 %	不変メモリ(ROM)
シングルワード（8 ビット）の署名（CRC）	EN 61508-2:2010, A.5	90 %	不変メモリ(ROM) 署名の有効性は、保護される情報のブロック長に関係する署名の幅に依存する。
ダブルワード（16 ビット）の署名（CRC）	EN 61508-2:2010, A.5	99 %	不変メモリ(ROM) 署名の有効性は、保護される情報のブロック長に関係する署名の幅に依存する。
RAM テスト「チェッカーボード」又は「マーチ」	EN 61508-2:2010, A.6	60 %	可変メモリ(RAM)
RAM テスト「ウォークパス」	EN 61508-2:2010, A.6	90 %	可変メモリ(RAM)
RAM テスト「ガルパット」又は「透明ガルパット」又は「アブラハム」	EN 61508-2:2010, A.6	99 %	可変メモリ(RAM)
ハードウェア又はソフトウェア比較、および読み書きテストのあるダブル RAM	EN 61508-2:2010, A.6	99 %	可変メモリ(RAM)
ソフトウェアによるシングルチャンネルの自己テスト（ウォーキングビット）	EN 61508-2:2010, A.4	90 %	演算処理装置(CPU)
ソフトウェアによる相互の比較	EN 61508-2:2010, A.4	99 %	演算処理装置(CPU);比較の質に依存する。
情報の冗長	EN 61508-2:2010, A.8	99 %	内部通信

付録３　共通原因故障モデル（EN 13611:2007）

ここで述べる手法は、EN 61508-6, 2010 付属書 D を修正したものである。
複雑なシステムの場合で表 J. 4 のいずれの項目もあてはまらない場合は、β = 2%の共通原因ファクターを使用しなければならないとしている。また。表 J. 4 の項目の少なくとも 1 つがあてはまる場合は、J. 4 を使用して X 及び Y を集計して β を決定するとしている。

表 J.4 — 電子又はセンサー/アクチュエータのスコア

項目	電子制御		センサー/アクチュエータ	
	X	Y	X	Y
冗長チャネルが検出部に異なる電気的技術(例えば、一方がプログラマブル、他方がリレー)、アクチュエータに異なる物理的な原理を使用する。	7		7.5	
冗長チャネルがセンサーに異なる電子技術(例えば、一方が電子、他方がプログラマブル電子)、又は異なる電気的な原理/設計(例えばディジタル、アナログ)、アクチュエータ(例えば異なるメーカー又は技術)を採用する。	5		5.5	
多様性中、例えば異なる技術を使用するハードウェア診断テストの使用	3	1.5		
チャネル間の交差結線は、診断テスト又は投票目的に使用された以外の情報の交換を妨げる。	0.5	0.5	0.5	0.5
同じハードウェアで同様の環境の中で5年以上の使用経験がある。	1.0	1.5	1.5	1.5
すべてのフィールド故障が、設計に充分にフィードバックされて分析析されているか。(手順の証拠書類が必要である。)	0.5	3.5	0.5	3.5
全てのコンポーネント故障(又は劣化)が検知されること、根本的原因が確証されたこと、及び同様なアイテムが故障の同様の潜在的な原因について調査されたことを保証する作業の書面によるシステムがあるか?		1.5	0.5	1.5
システムは診断率中(> 90%…<99 %)を有している。	1.5	1.0		
システムには診断率高(> 99 %)である。	2.5	1.5		
設計者は、共通原因故障の原因及び結果を理解するように(教育資料で)訓練されたか。	2.0	3.0	2.0	3.0
システムは外部環境を制御することなく常に温度、湿度、腐食、ダスト、振動などの範囲(テストされた範囲)内で動作するか。	3.0	1.0	3.0	1.0

表 J.5 から β の値を得るためにスコア値 S =X+Y+40 を計算する(注を参照)。

表 J.5 — β の計算

スコア (S)	β	
	電子制御	センサー/アクチュエータ
100 or above	0,5 %	1 %
60 to 100	1 %	2 %
40 to 60	2 %	5 %

注 1、EN 61508-6:2010 表 D.1 の次の側面が EN 13611 や適用可能な製品規格において原理的に適用可能であり、Xmin = 17 および Ymin = 23(Smin = Xmin+Ymin = 40)が与えられる:

**多様性低(例えば同じ技術を持ったハードウェア診断テスト)の使用。
**機器で使用された技術に基づいた設計は、>5 年間、フィールドで成功裡に使用されている。
**簡単なシステム(低 I/O 複雑さ)。
**過電圧/過電流に対して保護された I/O(義務としての emc、及び電気的強度試験による妥当性確認)。
**共通原因故障の源が FMEA によって検知され、設計によって除去される。
**共通原因故障が設計レビューで検討され、結果が設計にフィード・バックされる。
**システムには少なくとも低い診断率(> 60%…<90%）がある。
**ユーザアクセスが技術的及び、または組織的な方策によって制限される。
**信号及び供給配線が十分に分離される。(義務的な em、及び電気的な強度試験による妥当性確認)
**システムが安全面を考慮した包括的な環境試験の主題である。

注 2 それらの測面は、全体像を良く示すために表 J.4 から除外された。

中央労働災害防止協会　技術支援部　2018.3