

機械安全に係る設計技術者コース  
「機械安全に係る高度な設計技術者カリキュラム」Aコース

# 機械安全エンジニア A MSE A

講習会テキスト

制御安全（上級）  
(ISO 13849-1 および IEC 62061)

2019年2月

一般社団法人 安全技術普及会

## はじめに

本書は初版として 2004 年 12 月に発行した「制御安全技術」を国際規格の改定内容に照合し、より詳細な設計者が利用できるものとして新規に作成した。

機械システムにおいて機械可動部（機械アクチュエータ）の駆動には制御が盛んに用いられる。したがって、制御に基づく安全性の確保は国際規格で最も重要視される。

例えば、すべての機械は少なくとも起動と停止の機能をもつ。機械の起動と停止は最も重要な安全機能（安全確保の機能）であって、このほとんどが制御機能によって実現される。基本安全規格 ISO 12100 は制御を含む機械システム全般を扱う規格であるが、制御についても基本技術として準拠すべき要求事項を示している。

本書は制御システムに求められる安全関連部に要求される安全要求仕様について基本安全規格を含み ISO 13849-1 に述べられている詳細な技術を説明、解説した教科書である。

また、第 2 版に伴い IEC 62061 についても概要の解説を記載した。

なお、本文で十分説明できない補足的事項については付録として添付し、さらに、理解度を深めて頂くために提供しているので利用してほしい。

第 2 版 2019 年 2 月 1 日

編集 教育企画委員会  
委員長 今枝幸博  
委員 大西正紀

# 目次

第Ⅰ章 制御安全/機能安全 .....	1
Ⅰ.1 機械における制御システム .....	1
Ⅰ.2 一般的な機械の構成 .....	1
Ⅰ.3 機械の運転状態における制御の役割 .....	2
Ⅰ.4 制御システムの安全関連部と非安全関連部 .....	3
Ⅰ.5 制御システムの安全関連部の歴史 .....	4
第Ⅱ章 制御システムの安全関連部 .....	6
Ⅱ.1 制御システムの安全関連部の反復プロセス .....	6
Ⅱ.2 ISO 13849-1 におけるリスクアセスメント .....	8
Ⅱ.3 PL パラメータの概要 .....	9
Ⅱ.3.1 カテゴリ (Category) .....	9
Ⅱ.3.2 平均危険側故障時間 $MTTF_D$ (mean time to dangerous failure) .....	10
Ⅱ.3.3 診断範囲 DC (diagnostic coverage) .....	16
Ⅱ.3.4 共通原因故障 CCF (common cause failure) .....	22
Ⅱ.3.5 PL パラメータの関係 .....	24
Ⅱ.4 PL 見積もりの単純化 .....	25
Ⅱ.5 安全関連部のブロックダイアグラム .....	26
第Ⅲ章 ISO 13849-1 での妥当性確認 .....	31
Ⅲ.1 Table K.1 による $MTTF_D$ の決定と $PFH_D$ .....	31
Ⅲ.2 障害の考慮、障害の除外 .....	33
Ⅲ.3 カテゴリによる安全関連制御部出力の解説 .....	35
Ⅲ.4 確認事例 .....	38
Ⅲ.4.1 印刷機械におけるシリンダの清掃時手動操作の安全関連部に関する検証 .....	38
Ⅲ.4.2 可動式ガードの位置監視 - カテゴリ 4 - PL e に関する検証 .....	46
Ⅲ.4.3 ガード施錠付きインタロックガード - カテゴリ 3 - PL d .....	50
Ⅲ.4.4 安全モジュールによる保護装置のカスケード接続 (非常停止機能、STO) - カテゴリ 3 - PL d .....	56
第Ⅳ章 ソフトウェア .....	61
Ⅳ.1 ソフトウェア設計 .....	61
Ⅳ.2 ソフトウェア設計簡易 V-model .....	63
第Ⅴ章 技術文書 .....	65
Ⅴ.1 技術文書 .....	65
第Ⅵ章 IEC 62061 .....	67
Ⅵ.1 概要 .....	67
Ⅵ.2 用語 .....	67
Ⅵ.3 機械に用いる電気・電子・プログラマブル電子制御システム (SRECS) 設計のための手順	70
Ⅵ.3 SIL の割付け .....	73
Ⅵ.3.1 リスクアセスメント .....	73
Ⅵ.3.2 制御機能の安全インテグリティ要素 .....	76
Ⅵ.3.3 SRCF の安全インテグリティ要求仕様 .....	76
Ⅵ.3.4 $PFH_D$ の推定 .....	76

VI. 3.5	SFF の推定.....	77
VI. 3.6	フォールトトレランス.....	78
VI. 3.7	カテゴリを持つサブシステムの PFH <sub>0</sub> の限界値 .....	79
VI. 3.8	$\beta$ 値の推定 .....	79
VI. 3.9	自己診断、プルーフテスト .....	81
VI. 3.10	アーキテクチャ .....	81
VI. 3.11	系統的故障の回避 .....	83
VI. 4	SRECS の設計事例.....	84
VI.4.1	SRECS の設計例.....	85
附録 表 K.1	データ (ISO 13849-1:2015 より) .....	90
参考文献	.....	94