目次

第 1 章　機能安全の正しいアプローチ 8

1.1　機能安全の目的 9

1.1.1　はじめに 9

1.1.2　機能安全製品開発における問題 9

1.1.3　機能安全規格の目的 11

1.2　機能安全の取り組みのポイント　３ ＋ １ 12

1.2.1　リスクに基づく考え方 13

1.2.2　安全設計 13

1.2.3　プロセスアプローチ 14

1.2.4　安全文化 14

1.3　本ガイドブックの活用方法 15

1.3.1　本ガイドブックの目的 15

第 2 章　リスクに基づく考え方 18

2.1　安全の歴史 19

2.1.1　規格の誕生 19

2.1.2　安全規格の体系 21

2.2　安全とは 22

2.2.1　絶対安全と許容可能なリスク 22

2.3　リスクとは 23

2.3.1　リスクの定義 23

2.3.2　危害の大きさと発生確率 25

2.3.3　危害を引き起こすハザード 26

2.4　リスクアセスメント 27

2.4.1　制約の決定 28

2.4.2　ハザードの特定 28

2.4.3　リスクの見積り 28

2.4.4　リスクの評価 28

2.4.5　残存リスクの評価 29

2.4.6　妥当性評価 29

2.5　リスク低減 31

2.5.1　本質的安全設計 32

2.5.2 付加的保護方策 32
2.5.3 使用上の情報 32
第 3 章 機能安全概論 34
3.1 機能安全 35
3.1.1 コンピュータ技術の発展 35
3.1.2 機能安全の概念 35
3.1.3 自動車産業における機能安全の必要性 36
3.1.4 機能安全を含む安全規格 37
3.2 安全関連系 40
3.2.1 安全機能 40
3.2.2 安全関連系 40
3.3 安全度水準 42
3.3.1 安全度（Safety Integrity） 42
3.3.2 安全度水準（Safety Integrity Level） 42
3.3.3 確率論的安全度水準の達成 45
3.3.4 安全側故障と危険側故障 47
3.3.5 確定論的安全度水準の達成 49
3.4 自動車における機能安全 51
3.4.1 安全方策（Safety Measure） 51
3.4.2 安全度水準（Automotive/Motorcycle Safety Integrity Level） 51
3.4.3 確率論的安全度評価 53
3.4.4 確定論的安全度評価 54
3.5 安全ライフサイクル 55
3.5.1 安全ライフサイクルの外観 55
3.5.2 安全ライフサイクルのサブフェーズ 56
3.6 安全管理 59
3.6.1 安全に関する倫理 59
3.6.2 組織における安全管理 61
3.6.3 プロジェクトにおける安全管理 62
3.7 機能安全の評価 63
3.7.1 確証レビュー 65
3.7.2 機能安全監査 65
3.7.3 機能安全アセスメント 66
第 4 章 安全設計 68

4.1 事故発生メカニズムに関する解説 69
4.1.1 危害の大きさ 69
4.1.2 危害の発生確率 70
4.1.3 事故発生メカニズム 71
4.2 システム 75
4.2.1 システムとシステムの要素 75
4.2.2 要素の相互作用 76
4.2.3 システム境界 77
4.2.4 コンテキスト 77
4.2.5 創発特性 78
4.2.6 まとめ 79
4.3 機能不全の解説 80
4.3.1 ハザードと機能不全 80
4.3.2 危険事象（ハザーダスイベント） 81
4.3.3 EE システムの機能不全 81
4.3.4 安全機能の機能不全 83
4.4 故障とフォールト 85
4.4.1 故障の種類 86
4.4.2 故障率曲線 87
4.4.3 フォールトの種類 88
4.4.4 物理的故障 91
4.4.5 物理的故障の 3 要素 91
4.4.6 ハードウエア部品の故障率 93
4.4.7 従属故障：共通原因故障 94
4.4.8 従属故障：カスケード故障 96
4.5 安全機構の実装 －リスクアセスメント－ 97
4.5.1 アイテム 97
4.5.2 アイテムの定義 99
4.5.3 ハザード分析とリスクアセスメント 100
4.5.4 安全目標の決定 103
4.6 安全機構の実装 －リスクの低減－ 104
4.6.1 安全方策 104
4.6.2 機能安全コンセプト 105
4.6.3 技術安全コンセプト 108
4.6.4 アーキテクチャ設計の評価 111
4.6.5 安全機構の実現 113

4.6.6 ハードウエア開発 114
4.6.7 ソフトウエア開発 118
4.6.8 検証 121
4.6.9 安全妥当性確認 122
第 5 章 安全管理と安全文化 124
5.1 ヒューマンエラーのメカニズム 125
5.1.1 ヒューマンファクター 125
5.1.2 ヒューマンエラーのタイプ 126
5.1.3 ヒューマンエラーの分類 128
5.1.4 ヒューマンエラーの対策 129
5.2 安全管理 132
5.2.1 個人の対応 132
5.2.2 組織の対応 133
5.2.3 プロジェクトの対応 139
5.3 確証方策 145
5.3.1 確証方策の独立性 145
5.3.2 品質保証 147
5.3.3 確証レビュー 147
5.3.4 機能安全監査 148
5.3.5 機能安全アセスメント 149