目次

第 1 章　安全ライフサイクルにおけるシステムエンジニアリング.....8

1.1　システムエンジニアリングの役割.....9

1.1.1　システムエンジニアリングの目的.....9

1.1.2　システムエンジニアリングの活動.....10

1.2　安全ライフサイクルにおけるシステムエンジニアリング.....11

1.2.1　階層的なシステムエンジニアリング.....11

1.2.2　車両レベルのシステムエンジニアリングにおける安全活動.....11

1.2.3　システムレベルのシステムエンジニアリングにおける安全活動.....13

第 2 章　アイテム定義.....14

2.1　アイテム定義の概要.....15

2.1.1　アイテム定義の目的.....15

2.1.2　アイテム定義の活動.....16

2.2　アイテム定義の詳細解説.....17

2.2.1　車両機能の定義.....17

2.2.2　ユースケース分析.....17

2.2.3　システムコンテキスト分析.....20

2.2.4　文書化（製品の要件定義）.....23

2.2.5　検証レビュー.....23

セルフチェックリスト：アイテム定義.....24

第 3 章　ハザード分析とリスクアセスメント.....26

3.1　ハザード分析とリスクアセスメント　概要.....27

3.1.1　ハザード分析とリスクアセスメントの目的.....27

3.1.2　ハザード分析とリスクアセスメントの活動.....27

3.2　ハザード分析とリスクアセスメント　詳細解説.....28

3.2.1　ハザードの識別.....28

3.2.2　運用状況の分析.....30

3.2.3　危険事象の決定.....31

3.2.4　事故シナリオの特定.....31

3.2.5　危害の大きさの見積もり.....31

3.2.6　制御可能性の見積もり.....32

3.2.7 リスクの評価 34
3.2.8 安全目標 35
3.2.9 ハザード分析及びリスクアセスメントの検証レビュー 36
セルフチェックリスト：ハザード分析とリスクアセスメント 37

第 4 章 機能安全コンセプト 40

4.1 機能安全コンセプトの概要 41
4.1.1 機能安全コンセプト開発の目的 41
4.1.2 機能安全コンセプト開発の活動 41
4.2 機能安全コンセプトの詳細解説 42
4.2.1 安全状態の定義 42
4.2.2 安全構想設計 44
4.2.3 機能安全要件定義 47
4.2.4 車両レベルのアーキテクチャ設計 49
4.2.5 機能安全要件の割り当て 53
4.2.6 妥当性確認の基準定義 53
4.2.7 リスクアセスメント結果及び機能安全コンセプトの検証レビュー 55
セルフチェックリスト：機能安全コンセプト 56

第 5 章 技術安全コンセプト 58

5.1 技術安全コンセプトの概要 59
5.1.1 技術安全コンセプト開発の目的 59
5.1.2 技術安全コンセプト開発の活動 59
5.2 技術安全コンセプトの詳細解説 60
5.2.1 技術安全要件定義 60
5.2.2 安全機構設計 62
5.2.3 システムアーキテクチャ設計 65
5.2.4 システムアーキテクチャの評価 72
5.2.5 技術安全コンセプトの検証レビュー 75
セルフチェックリスト：技術安全コンセプト 76

第 6 章 システム・アイテム統合とテスト 78

6.1 システム・アイテム統合とテストの概要 79
6.1.1 システム・アイテム統合とテストの目的 79
6.1.2 システム・アイテム統合とテストの活動 79
6.2 システム・アイテム統合とテストの詳細解説 80

6.2.1 統合戦略の立案 80
6.2.2 テスト戦略の立案 80
6.2.3 テスト設計 81
6.2.4 統合及び統合テストの実施 89
セルフチェックリスト：システム・アイテム統合とテスト 90
第 7 章 安全妥当性確認 92
7.1 安全妥当性確認の概要 93
7.1.1 安全妥当性確認の目的 93
7.1.2 安全妥当性確認の活動 93
7.2 安全妥当性確認の詳細解説 94
7.2.1 安全妥当性確認戦略の立案 94
7.2.2 安全妥当性確認テスト設計 94
7.2.3 安全妥当性確認の実施 95
7.2.4 安全妥当性確認結果の評価 95
セルフチェックリスト：安全妥当性確認 96
第 8 章 【共通エンジニアリング】安全要件管理 98
8.1 安全要件定義 99
8.1.1 安全要件定義の目的 99
8.1.2 安全要件記述に対する要求事項 99
8.2 安全要件の管理 102
8.2.1 安全要件管理の目的 102
8.2.2 安全要件管理への要求事項 102
第 9 章 【共通エンジニアリング】安全分析 104
9.1 安全分析 105
9.1.1 安全分析の目的 105
9.1.2 安全分析の技法 106
9.2 従属故障分析 112
9.2.1 従属故障分析の目的 112
9.2.2 従属故障分析の手順 112
9.2.3 カップリングファクタ識別の考慮点 115
第 10 章 【共通エンジニアリング】ASIL 依存のエンジニアリング 118
10.1 ASIL デコンポジション 119

10.1.1 ASIL デコンポジションの目的 119
10.1.2 ASIL デコンポジション適用における考慮点 120
10.2 異なる ASIL エレメントの共存 121
10.2.1 異なる ASIL エレメントの共存　活動の目的 121
10.2.2 異なる ASIL エレメントを共存させるための考慮点 122
第 11 章 【共通エンジニアリング】既存エレメントの利用 124
11.1 既存エレメントの再利用 125
11.1.1 既存エレメント再利用の目的 125
11.1.2 既存エレメント開発における役割 125
11.2 影響分析 126
11.3 安全関連系への COTS 利用 127
11.3.1 ソフトウエア COTS の利用 127
11.3.2 ハードウエア COTS の利用 128
11.4 安全関連系への SEooC 利用 129
11.4.1 SEooC 開発の流れ 129
11.4.2 想定の開発と利用の評価 130
11.4.3 SEooC の統合と評価 130