

# 目次

第 1 章	安全ライフサイクルにおけるソフトウェアエンジニアリング	8
1.1	ソフトウェアエンジニアリングの役割	9
1.1.1	ソフトウェアエンジニアリングの目的	9
1.1.2	ソフトウェア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ソフトウェアエンジニアリング	11
1.2.1	ソフトウェアレベルにおける安全活動	11
第 2 章	ソフトウェア安全要求の仕様化	14
2.1	ソフトウェア安全要求の仕様化の概要	15
2.1.1	ソフトウェア安全要求の仕様化の目的	15
2.1.2	ソフトウェア安全要求の仕様化の活動	15
2.2	ソフトウェア安全要求の仕様化の詳細解説	16
2.2.1	ソフトウェア安全要求の定義	16
2.2.2	ハードウェアとソフトウェア間のインタフェース仕様 (HSI) の更新	18
2.2.3	ソフトウェア安全要求の検証	18
2.2.4	HSI の検証	18
	セルフチェックリスト：ソフトウェア安全要求の仕様化	19
第 3 章	ソフトウェアアーキテクチャ設計	20
3.1	ソフトウェアアーキテクチャ設計の概要	21
3.1.1	ソフトウェアアーキテクチャ設計の目的	21
3.1.2	ソフトウェアアーキテクチャ設計の活動	21
3.2	ソフトウェアアーキテクチャ設計の詳細解説	22
3.2.1	ソフトウェアアーキテクチャ設計	22
3.2.2	安全分析	29
3.2.3	ソフトウェアアーキテクチャ設計の検証	31
	セルフチェックリスト：ソフトウェアアーキテクチャ設計	33
第 4 章	ソフトウェアユニット設計及び実装	34
4.1	ソフトウェアユニット設計及び実装の概要	35
4.1.1	ソフトウェアユニット設計及び実装の目的	35
4.1.2	ソフトウェアユニット設計及び実装の活動	35

4.2	ソフトウェアユニット設計及び実装の詳細解説	36
4.2.1	ソフトウェアユニット設計	36
4.2.2	ソフトウェアユニットの実装	37
	セルフチェックリスト：ソフトウェアユニット設計及び実装	38
<b>第5章</b>	<b>ソフトウェアユニット検証</b>	<b>40</b>
5.1	ソフトウェアユニット検証の概要	41
5.1.1	ソフトウェアユニット検証の目的	41
5.1.2	ソフトウェアユニット検証の活動	41
5.2	ソフトウェアユニット検証の詳細解説	42
5.2.1	ソフトウェアユニット検証戦略の立案	42
5.2.2	ソフトウェアユニットの静的検証	42
5.2.3	ソフトウェアユニットテストの設計	44
5.2.4	ソフトウェアユニットテストの実施	48
	セルフチェックリスト：ソフトウェアユニット検証	49
<b>第6章</b>	<b>ソフトウェア統合及び検証</b>	<b>50</b>
6.1	ソフトウェア統合及び検証の概要	51
6.1.1	ソフトウェア統合及び検証の目的	51
6.1.2	ソフトウェア統合及び検証の活動	51
6.2	ソフトウェア統合及び検証の詳細解説	52
6.2.1	ソフトウェア統合戦略の立案	52
6.2.2	ソフトウェア統合テスト戦略の立案	52
6.2.3	ソフトウェア統合テストの設計	52
6.2.4	ソフトウェア統合及び統合テストの実施	56
	セルフチェックリスト：ソフトウェア統合及び検証	57
<b>第7章</b>	<b>組み込みソフトウェアのテスト</b>	<b>58</b>
7.1	組み込みソフトウェアのテストの概要	59
7.1.1	組み込みソフトウェアのテストの目的	59
7.1.2	組み込みソフトウェアのテストの活動	59
7.2	組み込みソフトウェアのテストの詳細解説	60
7.2.1	組み込みソフトウェアテスト戦略の立案	60
7.2.2	組み込みソフトウェアテストの設計	60
7.2.3	組み込みソフトウェアテストの実施	63
	セルフチェックリスト：組み込みソフトウェアのテスト	64

第 8 章	【共通エンジニアリング】安全要件管理 .....	66
8.1	安全要件定義 .....	67
8.1.1	安全要件定義の目的 .....	67
8.1.2	安全要件記述に対する要求事項 .....	67
8.2	安全要件の管理 .....	70
8.2.1	安全要件管理の目的 .....	70
8.2.2	安全要件管理への要求事項 .....	70
第 9 章	【共通エンジニアリング】安全分析 .....	72
9.1	安全分析 .....	73
9.1.1	安全分析の目的 .....	73
9.1.2	安全分析の技法 .....	74
9.2	従属故障分析 .....	80
9.2.1	従属故障分析の目的 .....	80
9.2.2	従属故障分析の手順 .....	80
9.2.3	カップリングファクタ識別の考慮点 .....	83
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 .....	86
10.1	ASIL デコンポジション .....	87
10.1.1	ASIL デコンポジションの目的 .....	87
10.1.2	ASIL デコンポジション適用における考慮点 .....	88
10.2	異なる ASIL エLEMENT の共存 .....	89
10.2.1	異なる ASIL エLEMENT の共存 活動の目的 .....	89
10.2.2	異なる ASIL エLEMENT を共存させるための考慮点 .....	90
第 11 章	【共通エンジニアリング】既存ELEMENT の利用 .....	92
11.1	既存ELEMENT の再利用 .....	93
11.1.1	既存ELEMENT 再利用の目的 .....	93
11.1.2	既存ELEMENT 開発における役割 .....	93
11.2	影響分析 .....	94
11.3	安全関連系への COTS 利用 .....	95
11.3.1	ソフトウェア COTS の利用 .....	95
11.3.2	ハードウェア COTS の利用 .....	96
11.4	安全関連系への SEooC 利用 .....	97
11.4.1	SEooC 開発の流れ .....	97

11.4.2	想定の開発と利用の評価 .....	98
11.4.3	SEooC の統合と評価.....	98