

表目次

表 2-1: フォーマルメソッドの適用レベル	7
表 2-2: 形式検証のアプローチ	8
表 4-1: 導入プロセスの参考としたフォーマルメソッド適用事例	13
表 4-2: 導入プロセスのパターン分類	14
表 5-1: フォーマルメソッド導入の主な効果	26
表 5-2: フォーマルメソッドの主な投資コスト	27
表 5-3: ソフトウェアの不具合に起因する損害リスクの要素	29
表 5-4: 障害発生時の影響度を把握するための主な検討項目(参考例)	33
表 5-5: フォーマルメソッドによる品質の向上に関する主な効果	34
表 5-6: 効果の具体例	35
表 5-7: SPINの技術習得コストの例	42
表 5-8: フォーマルメソッドを用いた設計レベル	42
表 5-9: ケーススタディにおけるフォーマルメソッドの設計付加コスト(時間)	43
表 5-10: 鉄道システムに対するBメソッドの適用プロセスの工数比率	43
表 6-1: ソフトウェアに対する要求	46
表 6-2: ISO/IEC 9126 (ソフトウェアの品質特性)	46
表 6-3: 非機能要求の主な要素とその内容	47
表 6-4: ディペンダビリティの構成要素	48
表 6-5: ディペンダビリティに対する脅威の分類	49
表 6-6: ディペンダビリティに関する対策の分類	49
表 6-7: ディペンダビリティ対策の手法例	49
表 6-8: 検証のレベル	54
表 7-1: 主な形式手法の概要	64
表 8-1: モデリングプロセスの入力情報によるパターン分類	83
表 8-2: モデリングパターンの選択基準	85
表 8-3: 検証性質パターン(モデル検査における時相論理式)	93
表 9-1: 抽象モデルと具体モデルの関係と用途	102
表 9-2: 型と変域の大きさ	107
表 11-1: モード制御ミドルウェアの要求仕様	119
表 11-2: Blu-ray系インタフェースの内部状態	121
表 11-3: Blu-rayミドルウェアモジュールの内部状態	121
表 11-4: 内部状態の対応関係	122
表 11-5: Blu-ray系インタフェースのAPI	123
表 11-6: における各部分のモデリングの方針とその理由	125
表 12-1: 検証対象システムの構成要素	135
表 12-2: ボックス管理システムの要求仕様	137
表 12-3: 待機者リストのデータ型	137
表 12-4: 待合室管理プロセスの受信メッセージと対応するアクション	138
表 12-5: 閲覧室X(X=A or B)管理プロセスが受信するメッセージと対応するアクション	138
表 12-6: 閲覧室Xの扉の解錠条件	140
表 12-7: 検証対象システムのモデリングの前提	143
表 12-8: 待合室管理プロセスの状態遷移表	148
表 12-9: 閲覧室Xプロセスの状態遷移表	150
表 12-10: 各ID端末のID番号割り振り	151
表 12-11: ID端末から送信可能なメッセージ	152
表 12-12: 各管理プロセスの処理と処理対象	154

表 12-13: 本ケーススタディにおける要求仕様と検証性質.....	158
表 13-1: 応用事例情報の整理項目	166
表 14-1: 性質記述パターンライブラリの概要	215
表 15-1: 再利用に対する期待	216
表 15-2: 再利用を行う際の困難 ¹⁵⁸	217
表 15-3: 検証量を減らすための工学的な手法例.....	225

図目次

図 2-1: フォーマルメソッドの位置付け(設計検証の場合)	6
図 2-2: フォーマルメソッドの具体的イメージ(モデル検査SPINの場合)	7
図 4-1: 導入プロセスの概略(共通部分)	14
図 5-1: 発生可能性と障害発生時の影響度とリスクの関係	30
図 5-2: 不具合が発生したことによる対策費の総合計(2008 会計年度)	32
図 5-3: 開発現場が抱える問題点とフォーマルメソッドの適用で期待される効果の例	37
図 5-4: 欠陥の混入工程、発見工程、除去コスト	38
図 5-5: 開発プロセスのフロントローディングと許容負荷(文献EASISを元に作成)	40
図 6-1: ディペンダビリティ確保の対策分類と利用される技術の関係	51
図 6-2: 信頼性・安全性・セキュリティの関係	52
図 6-3: フォーマルメソッドの主な適用箇所と用途	54
図 6-4: 開発V字モデルにおける各種手法の適用箇所	55
図 6-5: 障害の区別と評価対策アプローチ	57
図 7-1: 主な形式手法の用途例の俯瞰	62
図 7-2: 成功事例に基づく目的と対象(レベル)による適用手法の典型例	63
図 7-3: SPINの開発プロセスにおける位置づけ	69
図 7-4: NuSMVの開発プロセスにおける位置づけ	71
図 7-5: UPPAALの開発プロセスにおける位置づけ	73
図 7-6: SCADEの開発プロセスにおける位置づけ	74
図 7-7: 過去 25 年の形式手法の変遷	75
図 7-8: Bの開発プロセスにおける位置づけ	77
図 7-9: Event-Bの開発プロセスにおける位置づけ	78
図 7-10: VDM++の開発プロセスにおける位置づけ	80
図 8-1: コンポーネント駆動パターンの概要	86
図 8-2: システムの構成要素と相互作用の例	88
図 8-3: 状態遷移表に基づくPromela記述テンプレート(例)	92
図 8-4: アルゴリズム駆動プロセスの概要	94
図 8-5: 要求性質駆動プロセスの概要	95
図 9-1: 2つの並行プロセスの状態遷移図(例)	98
図 9-2: 非同期並行実行による状態遷移図	98
図 9-3: 交通信号モデルの抽象化(例)	100
図 9-4: 抽象化の健全性の条件(言葉による説明)	101
図 9-5: モデルの抽象化と状態回避策に関する全体像	103
図 9-6: 実質的に逐次的な処理のシーケンス図	105
図 9-7: 冗長な中間状態s1 がある場合	111
図 9-8: 状態s1 を省いて、a;b を 1 ステップにした場合	111
図 9-9: スタックの利用前部分の不定値	113
図 11-1: 検証対象システムの構成	116
図 11-2: 検証対象システムの構成	118
図 11-3: プロセスの構成図	120
図 11-4: 実際のシステムのプロセス構成とモデリングを行う単位	125
図 11-5: 実際のシステム構成とモデルのプロセス構成	126
図 11-6: モードモジュールの状態遷移表	128
図 11-7: ミドルモジュールの状態遷移表	130
図 12-1: ボックス管理システム全体像	135

図 12-2: 表示装置の更新タイミング	142
図 12-3: 実際に近いモデル(全体像)	145
図 12-4: 単純化した検証対象システムのモデル(全体像)	146
図 12-5: 閲覧者の動線(システム設計時)	147
図 12-6: parsonData型の定義	148
図 12-7: BoothRoomParsonData型の定義	150
図 12-8: チャンネルpciの定義	151
図 12-9: 扉脇ID端末認証装置のモデル化	152
図 12-10: 在室センサのモデリング	153
図 12-11: データベース(DB)と表示装置のモデル化	154
図 12-12: 表示装置のモデリング	156
図 12-13: 閲覧者のオートマトン(大枠)	157
図 12-14: 待合室における閲覧者のオートマトン	157
図 12-15: 検証内容S01 のLTL式	159
図 12-16: 検証内容S02 の基本となるLTL式	160
図 12-17: 検証内容S02 のLTL式	160
図 12-18: 待合室のPromela記述	161
図 12-19: assert文を追記した待合室のPromela記述	162
図 12-20: S03 の検証結果	163
図 12-21: 対処を行った待合室のPromela記述	165
図 13-1: ソフトウェアアーキテクチャ設計	167
図 13-2: SCADEにより作成されたスケジューリングとコミュニケーションモデル	169
図 13-3: UPPAALによるシーケンス制御モデル図	170
図 13-4: 入退室管理システムの全体像	172
図 13-5: プラットフォームドアの構成	173
図 13-6: 列車制御システムの構成	176
図 13-7: MULTOSの概要	183
図 13-8: 実践した形式モデリングの流れ	185
図 13-9: OpenComRTOSのアプリケーション概要	186
図 13-10: TSEアーキテクチャの概要	189
図 13-11: OpenNANDフラッシュメモリのためのストレージプラットフォーム	190
図 13-12: 意思決定システム(BOS)の全体像	192
図 13-13: X線CTスキャンのアーキテクチャの概要	195
図 13-14: 無人シャトル制御システムにおける抽象モデルと具体モデルとの関係	197
図 13-15: 開発されたプラットフォームドア	198
図 13-16: ディスプレイアーキテクチャ(オレンジ色はディスプレイアプリケーション、緑色はウインドウマネージャ)	200
図 13-17: TradeOneシステムの構成	202
図 13-18: IECSソフトウェアの構成図	204
図 13-19: 開発された自動販売機の構成図	205
図 13-20: Static Driver Verifier toolの解析エンジンアーキテクチャ	207
図 13-21: 鉄道制御システムの主要なStatemateモデル	208
図 14-1: LTLとCTLの簡約な表現	213
図 14-2: LTLによる表現	214
図 14-3: CTLによる表現	214
図 15-1: 再利用の基本構造	216
図 15-2: 再利用における検証一般の課題	218
図 15-3: フィーチャモデルの例	220

図 15-4: 再利用におけるモデル検査技術の適用の概観	221
図 15-5: 再利用資産のモデル検査の例	222
図 15-6: フィーチャモデルを用いた検証状況の明確化例	223
図 15-7: 再利用可能な検証資産の例	224
図 16-1: 信頼度成長曲線	230
図 16-2: 信頼度成長曲線の傾きとテストに発生している問題の例	231
図 16-3: 欠陥の摘出工程分布と品質評価	231
図 16-4: W字モデル開発	233