独立検証機関による形式手法を用いた第三者検証のコスト評価

実施報告書

２０１３年２月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

はじめに

IPA/SEC では、ソフトウェア品質説明力を強化すべく様々な観点からの検討を実施してきました。その一環として、ソフトウェア品質を説明するための手法等について具体的な実施方法、そのための作業量、実施にあたっての課題等を整理し、実際にソフトウェア品質を説明する際の参考とできるようにするために、公募により、観点ごとに分けられた実験を別々に実施しました。本書は、それらの結果を、実験ごとにまとめた報告書のうちの１つです。

本報告書の実験は、「2011 年度 システムエンジニアリング実践拠点事業」として、株式会社フォーマルテックに委託し実施しました。

「独立検証機関による形式手法を用いた第三者検証のコスト評価」
【報告書】

独立行政法人情報処理推進機構

【目次】

1. まえがき

本実験では、後述する独立検証機関が、形式手法（モデル検査）を用いて、実験対象システムの第三者検証を行った場合に必要なコストを明確にする。株式会社フォーマルテックと独立行政法人産業技術総合研究所が普及活動を行っている、モデル検査を適用する際の標準的な業務プロセス「モデル検査の適用プロセス」の作業フェーズ毎にコストを算出し、それらを合算した総合コストを算出する。モデル検査の適用プロセスには、第三者検証で最初に必要なヒアリングから、別の第三者による検証結果の審査を行う際に必要な検証結果と経緯をまとめたエビデンス作成作業までが含まれている。したがって、本実験で算出した総合コストは、独立検証機関が監査や審査へ参画する際に実際に要する技術的コストに近い値となり、模擬実験でありながら実証実験に近い結果を得ることができる。

実験対象システムは、高電圧の配電線に取り付けられた開閉器を、事業所の親装置より監視／制御する「配電自動化システム」である。

本実験では機能安全の国際規格である IEC61508 をターゲットとして、表 1-1 に示す 2 つの品質レベルを設けて、各レベルごとにコストを計測する。

表 1-1　実験で設定する品質レベル

品質レベル	内容（対応する IEC61508 の安全度水準レベル）
1	機能安全規格の安全度水準レベル 3（SIL3）
2	機能安全規格の安全度水準レベル 4（SIL4）

機能安全規格においては、安全度水準レベル 3 で、形式手法の適用が「推奨」されており、レベル 4 では「強く推奨」されている。そこで、レベル 3 では、モデル記述言語による設計書の形式仕様記述までに要するコストを算出する。レベル 4 では、形式仕様記述によって記述されたモデルの形式検証までに要するコストを算出する。

本章「1 まえがき」の流れを図 1-1 に示す。

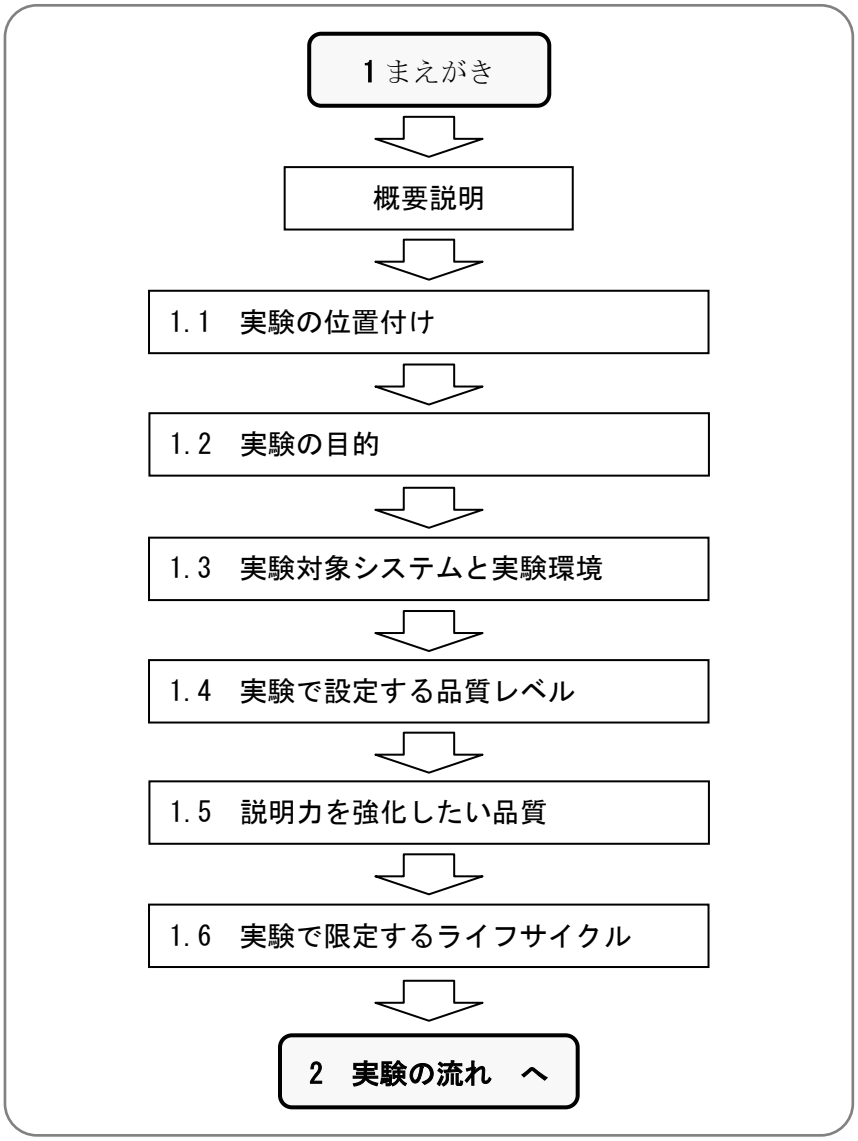


図 1-1　本章の流れ

「1.1」では本実験の、位置付けについて述べる。「1.2」では実験の目的と、なぜ新たに実験をする必要があったのか、その意義について述べる。「1.3」では、実験対象の実製品である配電自動化システムの概要と実験環境を報告する。「1.4」と「1.5」では、品質レベルのターゲットとした機能安全規格（IEC61508）を概説し、ソフトウエア品質説明力の強化という観点において、本模擬実験で検証の対象とする品質について述べる。最後に「1.6」で、本実験で限定するシステムのライフサイクルの範囲を説明する。

1.1. 実験の位置付け

実験の位置付けについて説明する。本実験は、図 1-2 に示すような、独立検証機関（事業者とは独立した立場で品質を検証する組織等）が事業者からの依頼等によって、事業者が有する製品に対して高度で専門的な検証サービスを提供する業務を想定している。

株式会社フォーマルテックが図 1-2 の独立検証機関となり、検証題材の提供企業が同図の事業者で形式手法の適用を希望しているとの想定で実験を行った。したがって、独立検証機関が提供する高度で専門的な検証サービスは形式手法（モデル検査）を用いた設計検証とした。検証サービス提供の仕組みを図 1-2 に示す。

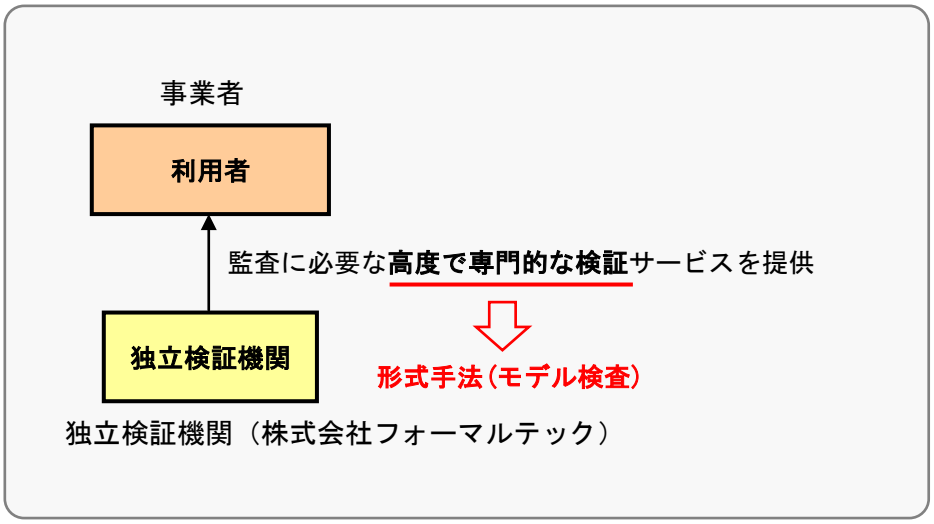


図 1-2　検証サービス提供の仕組み

1.2. 実験の目的

本実験の目的は、民間が主体となる独立検証機関が前述した検証サービス提供の仕組みの下で、検証サービスを提供した場合に必要となるコストを評価することである。

モデル検査をはじめとする形式手法は、ソフトウェアの品質を向上させる新しい検証方法として近年注目されている。シンポジウムやワークショップ、研究会等ではモデル検査というキーワードが頻繁に現れている。産業界における適用事例も、この 10 年で急速に増えており、事例の中には検証に要したコストが公開されているものもある。しかしながら、それらの事例から得られる情報を本実験の目的であるコスト評価に直接用いることはできない。表 1-2 に示すような懸案事項が考えられるからである。

表 1-2　既存の事例から得られる情報の懸案事項

NO	懸案事項	内容
1	第三者検証ではない	システム開発を行った技術者と同一の企業、あるいは同じプロジェクトに所属する担当者が検証を行った事例であり、製品をユーザに提供する事業者とは独立した機関による検証ではない。
2	専門家による検証ではない	適用時に技術習得を始めた初心者や、通常業務では検証作業ではなく開発を行っている技術者による結果である。 モデル検査による検証を事業としている専門家（企業）が実施した事例ではない。
3	試用のコストである	企業内でモデル検査を試運用した結果であり、実製品の品質を確保する検証業務として本格的に適用した結果ではない。
4	検証業務以外のコストが含まれる	技術習得のための時間や、モデル検査ツールの操作方法の習得時間等の純粋な検証業務以外のコストが含まれている。
5	適用プロセスが不明確である	モデル検査を適用する際のプロセス（作業工程）が定義されていない。不明確である。
6	詳細情報が無い	検証の開始から終了までの作業全体のコストのみ公開されており、モデルの作成や検査式の作成など、作業毎の詳細なコスト情報が無い。

上記の表 1-2 に示した、産業界における既存の事例に対する懸案事項を全て解決した上で、検証に要するコストを算出することが本実験の意義となる。懸案事項に対する本実験での解決策を表 1-3 に示す。

表 1-3　既存の事例の懸案事項に対する解決策

NO	懸案事項	解決策
1	第三者検証ではない	実験対象である配電自動化システムの開発を行った企業とは、全く独立した組織が検証を行うことで第三者検証を実現する。
2	専門家による検証ではない	モデル検査を用いた製品の検証を事業として実施している組織が検証を行う。実験で検証を行う株式会社フォーマルテックは、実製品への適用実績を 40 件以上有するモデル検査の専門企業である。
3	試用のコストである	実験対象システムは製品であり試験品ではない。また、検証は製品の品質を向上させるために実施しており、技術の試運用ではなく本格運用である。
4	検証業務以外のコストが含まれる	技術習得や事務手続き等のコストとは明確に区別することで、認証に必要な技術的なコストのみを算出対象とする。
5	適用プロセスが不明確である	モデル検査を適用する際の標準的な業務プロセス「モデル検査の適用プロセス」を定義して、本プロセスに沿ったコストを算出する。
6	詳細情報が無い	標準的な適用プロセスの作業毎にコストを算出し、詳細な内訳を明確にする。

本実験で、算出されたコストによって、独立検証機関による監査や審査への参画の許容の妥当性を評価することができる。

コスト評価の尺度は産業界における作業見積等で一般的に採用されている「人・時」とした。

人・時については、例えば、2.0 人・時は、2 人が 1 時間作業した作業量（コスト）であり、1 人が 2 時間作業した場合、4 人が 0.5 時間作業した場合の作業量でもある。

1.3. 実験対象システムと実験環境

実験対象としたシステムは「配電自動化システム」である。

(1) 実験対象の概要

配電自動化システムの概要図を図 1-3 に示す。

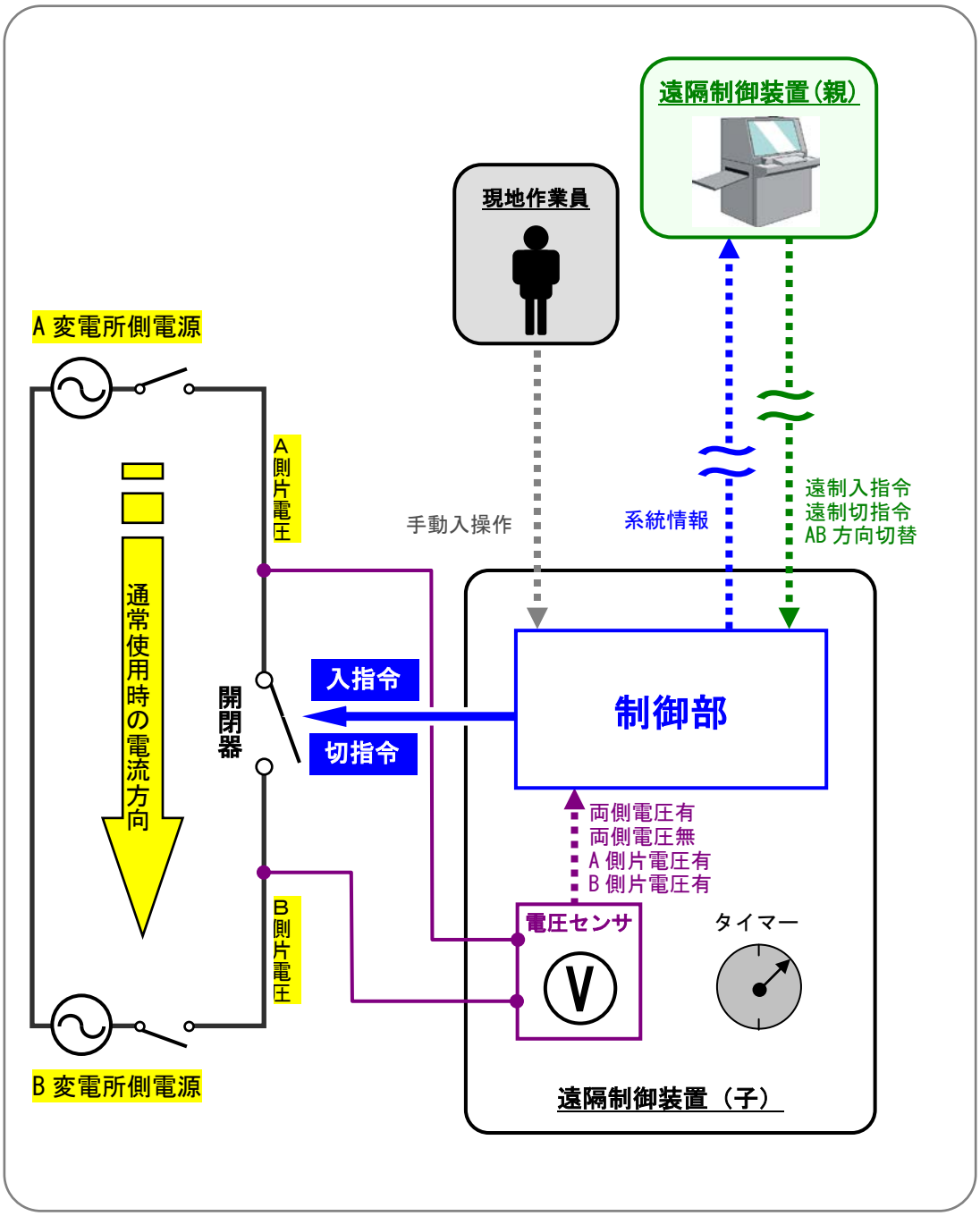


図 1-3　配電自動化システムの概要図

高電圧の配電線に取り付けられた開閉器（スイッチ）を、遠隔制御装置（親）より監視／制御するためのシステムである。開閉器に併設された遠隔制御装置（子）は、通信を用いて開閉器の状態や電線路の状態を監視し、必要に応じて親装置からの遠隔操作によって開閉器を制御する。監視機能は、開閉器が設置された箇所の電力系統情報(電圧等)を親装置に送信する。制御機能では、親装置から出力された命令に応じて開閉器の操作を制御する。

(2) 入手資料

モデル検査による第三者検証を実施するにあたって、入手した資料の一覧を表 1-4 に示す。

表 1-4　入手資料一覧

NO	名称	規模[頁]
1	配電自動化システム　ソフトウェア設計書	52
2	ソフトウェア設計の懸案事項	3

資料 NO.1 の「配電自動化システム　ソフトウェア設計書」は、本システムの開発工程で作成された「配電自動化システム　ソフトウェア機能仕様書」と「配電自動化システム　プログラム詳細仕様書」の基となる設計書である。

資料 NO.2 の「ソフトウェア設計の懸案事項」には、設計段階で継続検討「要」あるいは確認・調査「要」とされた懸案事項が示されている。

(3) 実験環境

実験で用いたモデル検査ツールは「NuSMV Ver2.5.4(Windows 版)」である。モデル検査ツールを実行するために用いた計算機のスペックを表 1-5 に示す。

表 1-5　計算機のスペック

項目	値
機種	DELL 製 INSPIRON
OS	Windows Vista
CPU	3.0[GHz]
メモリ	4.0[GByte]

(4) 実験体制

実験の体制を図 1-4 に示す。

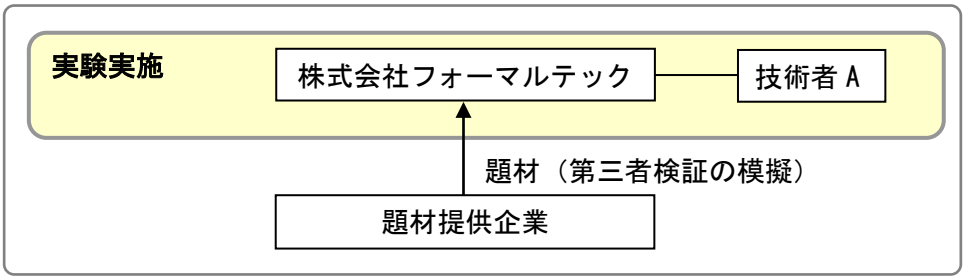


図 1-4　実験の体制

作業は技術者 A が 1 人で実施した。技術者 A のスキル（経験）を表 1-6 に示す。

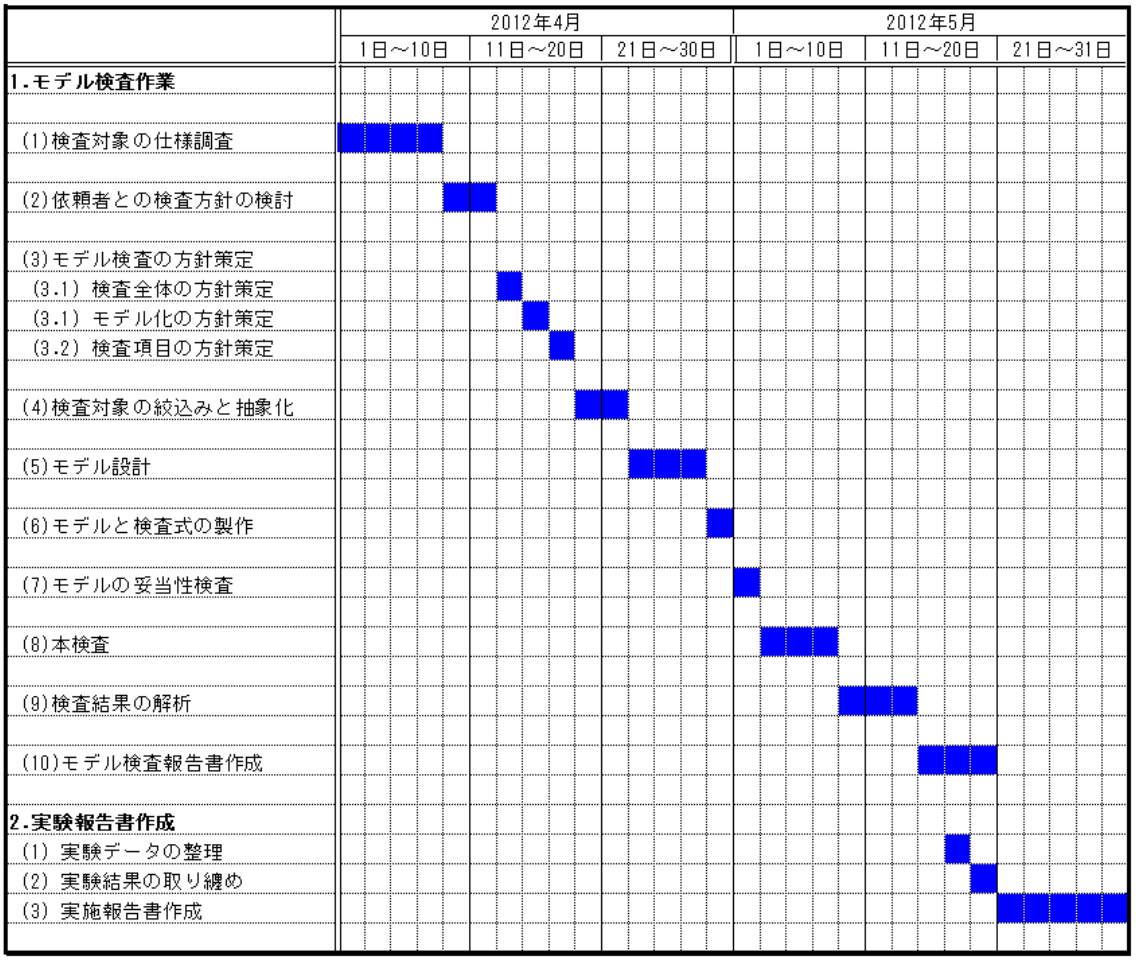
表 1-6　技術者 A のスキル（経験）

項目	スキル（経験）
形式手法（モデル検査）について	
モデル検査の経験年数	10 年
モデル検査の適用実績	40 件以上
実験対象の分野について	
電力設備に関するシステム開発の業務経験	3 年
上記システムへのモデル検査の適用実績	10 件以上
システム開発の工程毎の経験について	
基本計画 ～ 要件定義 ～ 機能設計	7 年
詳細設計 ～ 実装 ～ 単体・総合試験	3 年

(5) 実験の日程

実験の作業日程を表 1-7 に示す。表の左上部の「１．モデル検査作業」の詳細については、本書の「4　モデル検査の適用プロセス」で述べる。

表 1-7　実験の作業日程


2012年4月
2012年5月
1日～10日
11日～20日
21日～30日
1日～10日
11日～20日
21日～31日
1.モデル検査作業
(1)検査対象の仕様調査
(2)依頼者との検査方針の検討
(3)モデル検査の方針策定
(3.1) 検査全体の方針策定
(3.1) モデル化の方針策定
(3.2) 検査項目の方針策定
(4)検査対象の絞込みと抽象化
(5)モデル設計
(6)モデルと検査式の製作
(7)モデルの妥当性検査
(8)本検査
(9)検査結果の解析
(10)モデル検査報告書作成
2.実験報告書作成
(1) 実験データの整理
(2) 実験結果の取り纏め
(3) 実施報告書作成

1.4. 実験で設定する品質レベル

本実験では機能安全の国際規格である IEC61508 をターゲットとした。ここでは、機能安全規格を選定した理由と、実験で設定した品質レベルについて報告する。機能安全規格の詳細については一般の参考図書等を参照して頂きたい。

(1) 機能安全規格（IEC61508）を選定した理由

機能安全規格（IEC61508）は国際電気標準会議（International Electrotechnical Commission）が 2000 年に制定した電気・電子関連の機能安全（functional safety）に関する国際規格である。安全性に関係する事項を網羅的に検討／抽出し、安全な製品を開発するために有効な管理手法や技術の適用を定めている。

機能安全とは本質安全と対比して用いられる用語であり、多くの文献で表 1-8 に示すように説明されている。

表 1-8　本質安全と機能安全

用語	説明
本質安全	人間や環境に対して機械や装置、システムが危害を及ぼす原因自体を削減あるいは排除することによって安全を確保すること。 鉄道の例） 線路と道路との交差部から踏切を排除して立体交差とすることで踏切事故をなくす。
機能安全	機能的な工夫を導入することで、危険を許容される目標レベルまで低減することで安全を確保すること。 鉄道の例） 踏切部に遮断機や警報機を設置することで衝突の可能性を低減する。

実験対象とした配電自動化システムは、電力系統上で発生する電気事故等による停電の波及を最小限に抑えると共に、事故復旧後の電力の再供給を迅速かつ確実に進める上で欠かせないシステムである。停電の長期化や電力再供給の失敗等のリスクを低減するためには、本質安全による対策として、復旧作業員の常駐、電線路のハード的な強化が考えられるが現実的ではない。表 1-8 に示すように機能的な工夫を導入することで、それらのリスクを低減することが現実的である。

これらのことから、配電自動化システムは機能安全の考え方によく合致したシステムであるため、本実験は機能安全規格をターゲットとした。

(2) 本実験で設定する品質レベル

機能安全規格では、機器の故障をランダムハードウェア故障とシステム故障とに一旦分類した上で、最終的にシステム全体としての安全度水準(SIL:Safety Integrity Level)を定めている。

前述したように、実験対象とした配電自動化システムは、社会インフラの中枢を成し、我が国の産業、経済、国民生活を維持、発展させる上で必要不可欠なシステムであり、システム全体として非常に高いレベルの安全性が求められる。

本実験では、図 1-4 に示した「検証題材の提供企業」が図 1-2 に示した「事業者」となり、ソフトウェアの品質を向上させる新しい検証方法として注目されている形式手法の適用を希望しているとの想定で実験を行った。機能安全規格では、形式手法と安全度水準との関係を表 1-9 のように定義している。

表 1-9　形式手法と安全度水準

手法	安全度水準			
	SIL1	SIL2	SIL3	SIL4
形式手法	―	R	R	HR

表 1-9 の R は「Recommended (推奨)」であり、HR は「High Recommended (強く推奨)」である。配電自動化システムに求められる安全性のレベルと、形式手法の適用を想定していることから、本実験では表 1-10 に示す 2 つの品質レベルを設定し、それぞれのレベルごとにコストを検証した。

表 1-10　実験で設定する品質レベル

品質レベル	対応する IEC61508 の安全度水準
1	機能安全規格の安全度水準レベル 3 (SIL3)
2	機能安全規格の安全度水準レベル 4 (SIL4)

モデル検査を第三者に依頼する企業には、最終的な形式検証まで外部に委託する企業と、形式仕様記述によるモデル作成まで外部に委託し、形式検証は機密情報保護等の観点から自社内で実施する企業がある。このような背景から、モデル記述言語による設計書の形式仕様記述までを第三者が実施するが、形式検証は実施しない適用レベルを安全度水準レベル 3 とし、形式手法の適用が「強く」推奨されている安全度水準レベル 4 では、形式仕様記述によって記述されたモデルの形式検証まで実施することとした。なお、以降、単にレベルと記した場合は安全度水準レベルを指すものとする。

1.5. 説明力を強化したい品質

本実験が採用する手法によって説明力を強化したい品質は、配電自動化システムの設計品質である。対象システムの開発にあたっては、遠隔制御装置（子）の設置数量の多さや物理的要因（電柱の上に設置）を考慮すると、出荷・設置後の改修は非常に困難であり、システム要件～コンポーネント要件までの設計の上流工程における品質確保が最重要課題となるからである。本実験で説明力を強化したい品質を表 1-11 に示す。

表 1-11　説明力を強化したい品質

品質	内容
安全性 1	ソフトウェアを含めたシステムがフリーズしないこと。
安全性 2	予期せぬ動作により本システム自体が原因となって電気事故が発生し停電とならないこと。

2 つの安全性（安全性 1、安全性 2）は、本システムでは非常に高いレベルで保証されなければならない。安全性 1 では、電気事故が発生した場合に本システムがフリーズしていると広範囲かつ長時間にわたる停電が継続する可能性があり、いかなる操作を行ってもフリーズする危険は最小限に抑える必要がある。さらに、安全性 2 が保証されなければ、安全のために導入した機能自体が人間や環境に危害を及ぼすことになり、絶対にあってはならない事象である。本実験では、システムの取り得る全ての状態空間を網羅的に検査することができるモデル検査を用いて安全性 1 と安全性 2 を保証して品質説明力を強化する。

1.6. 実験で限定するライフサイクル

実験対象とした配電自動化システムでは、製品・サービスの企画は完了しているため、本実験では、「システム要件～コンポーネント要件」を実験対象のライフサイクルとした。

2. 実験の流れ

本実験の流れを図 2-1 に示す。

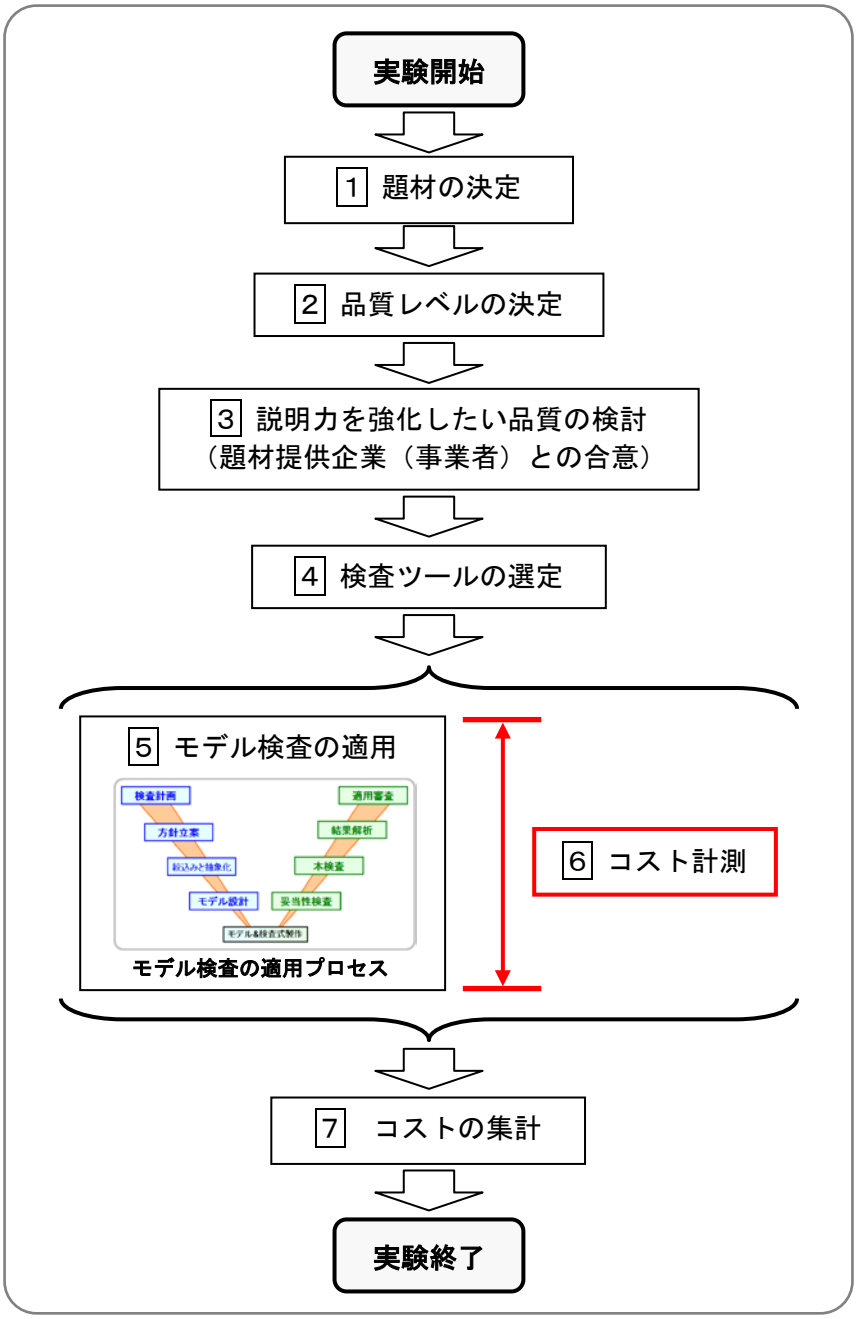


図 2-1　実験の流れ

図 2-1 の流れの中で作業1～3については「1 まえがき」で前述した通りである。また、作業4については「3.3　モデル検査器 NuSMV」で、作業５については「4　モデル検査の適用プロセス」で、それぞれ後述する。以下、作業6と7について述べる。

2.1. コストの計測

ここでは、作業5「モデル検査の適用」と並行して実施した作業6「コスト計測」について説明する。

(1) 計測対象

本実験の目的は、独立検証機関が検証サービスを提供する際のコストを評価することであるため、計測対象は図 2-1 の作業5「モデル検査の適用」を完了するために必要なコストのみとした。これは、モデル検査の適用プロセスの第一の作業工程である「モデル検査の実施計画策定」から最終工程である「モデル検査の適用審査」までに必要なコストである。図 2-1 の作業1～4は実験のための事前作業であり、作業7は実験のための事後処理であるため計測対象からは除外した。また、作業5の範囲内であっても、検証サービスの提供に直接的に資さない作業、例えば、後述する実験データシートの作成作業や、それらのデータの整理作業などについても計測対象から除外した。

(2) 計測方法

モデル検査の適用プロセスで定められた作業を実施する際に、要した時間を計測して実験データシートに記入した。実験データシートのフォーマットを

表 2-2 に示す。

薄黄色のセルは実験データを記入するセルである。灰色のセルは自動計算により合計値が算出され結果が入力されるセルである。

計測及び記入は、モデル検査の適用プロセスの工程毎で、かつ 4 つの作業項目毎に記入する。作業項目の一覧を表 2-1 に示す。

表 2-1　実験データシートの作業項目

作業項目	内容
打合	適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。打合せ用の資料作成時間、メール又は電話による相談時間等も含むものとする。本作業には依頼者の対応が必要である。
検討	独立検証機関内での検討時間又は技術調査の時間、モデル設計時間等を計上する。
作業	コーディング、報告書の記載等の直接的な作業時間を計上する。テストモデルの作成、動作確認等の試行も含むものとする。
実行	モデル検査器 NuSMV の実行と結果出力までの待ち時間を計上する。

時間の計測及び記入は 0.25 時間（15 分）刻みとした。また、当日の工程で、前工程の手戻り作業が発生した場合は、手戻りの作業時間についても当日の作業時間として計上することとした。

表 2-2　実験データシートのフォーマット

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第		[日目]
作業者			

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0
□ 検査の方針立案	0	0	0	0	0
・ 検査全体の方針立案					0
・ モデル化の方針立案					0
・ 検査項目の方針立案					0
□ 検査対象の絞込みと抽象化	0	0	0	0	0
・ 絞込み					0
・ 抽象化					0
□ モデル設計					0
□ モデルと検査式の製作	0	0	0	0	0
・ モデルの製作					0
・ 検査式の製作					0
□ モデルの妥当性検査					0
□ 本検査					0
□ 検査結果の解析					0
□ モデル検査の適用審査					0
合計	0	0	0	0	0

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

本実験で実際に作成・記入した実験データシートを本書末尾の「実験で作成されたデータ等の資料」の「2　実験データシート」に添付する。

2.2. コストの集計方法

ここでは、作業7「コストの集計」を概説する。本実験では、機能安全規格（IEC61508）の安全度水準レベル 3 とレベル 4 を設定し、モデル検査の適用レベルについても品質レベル毎に設定した。品質レベル、それに対応する安全度水準レベル、モデル検査の適用レベルの関係を表 2-3 に示す。

表 2-3　実験で設定した品質レベルとモデル検査の適用レベル

品質レベル	安全度水準レベル（IEC61508）	モデル検査の適用レベル
1	安全度水準レベル 3（SIL3）	モデル記述言語による設計書の形式仕様記述まで。 ただしモデルの妥当性検査は含む。
2	安全度水準レベル 4（SIL4）	形式仕様記述によって記述されたモデルの形式検証まで。

実験データについても、集計・評価しやすいように品質レベル毎に集計した。安全度水準レベル 3 については、モデル検査の適用プロセスの工程の中から必要な工程を抜粋して集計を行った。適用プロセスで安全度水準レベル 3 に必要な工程を表 2-4 に示す。○印を付した工程が必要な工程である。△印は工程の一部が必要である。

表 2-4　適用プロセスでレベル 3 に必要な工程

NO	モデル検査の適用プロセスの工程	要否
1	モデル検査の実施計画策定	○
2	検査の方針立案	○
3	検査対象の絞込みと抽象化	○
4	モデル設計	○
5	モデルと検査式の製作	○（モデルのみ）
6	モデルの妥当性検査	○
7	本検査	×
8	検査結果の解析	×
9	モデル検査の適用審査	△

詳細な集計方法と結果は「5　モデル検査の適用結果とコスト評価」で報告する。

3. モデル検査について

ここでは、実験で用いたモデル検査の技術とモデル検査器 NuSMV について説明する。

3.1. モデル検査とは

モデル検査は形式手法（数理的技法とも呼ばれる）の 1 つである。検査対象となるシステムを有限個の状態を持つモデルとして記述すると、モデルが取り得る全ての状態とパス上で、検査式が成立するか否かを機械的かつ網羅的に検査できる技術である。検査式は、モデルの基となったシステムが満たすべき性質を記述する。ソフトウェアを含むシステムの全数検査を実現することができるため、品質確保と向上のための新しい手法として産業界で注目を集めている。

モデル検査の概要を図 3-1 に示す。

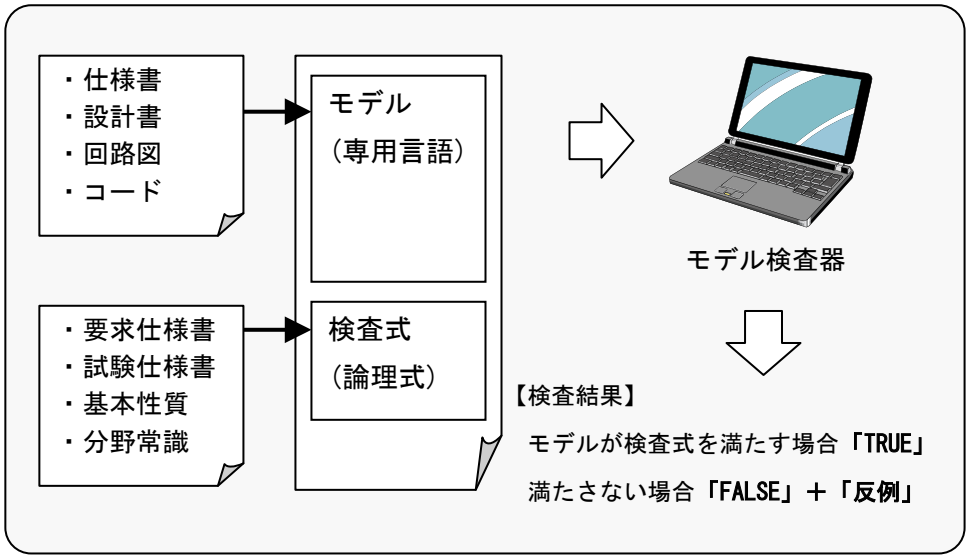


図 3-1　モデル検査の概要

図 3-1 のモデル検査器は、計算機上でモデル検査を行うことができるソフトウェアツールである。図に示したようにノート型の計算機上でも高速に動作するツールが公開されている。

モデル検査器は、モデルが検査式を満たす場合には検査結果として「TRUE」を出力する。反対に、モデルが検査式を満たさない場合には「FALSE」と、その証拠である「反例」を出力する。モデルが取り得る全ての状態とパスを全数探索するため、極めて特別な状態やパスで発生する不具合や予期せぬ動作、漏れや抜け等を発見することができる。一方、「TRUE」が出力された場合には、あくまでモデルに対してであるが、検査した性質が絶対に満たされることを保証することができる。

3.2. モデル検査の利点

これまでの適用事例あるいは導入、運用の経験から、モデル検査には多くの利点があることが分かっている。モデル検査の利点を表 3-1 に示す。

表 3-1　モデル検査の利点

NO	利点
1	全数探索が可能である
2	反例が出力される
3	モデル化の際にも不具合の発見が可能である
4	自動化が進んでいる
5	導入が容易である
6	結果の管理が容易である
7	モデル検査特有の検査が可能である

(1) 全数探索が可能である

モデル検査の最大の利点である。ソフトウェアを含む情報システムの分野で、現実的に困難と言われた全数探索を実現する。モデル検査器の種類と計算機に搭載された物理メモリの量にもよるが、モデル検査で扱える状態数は数兆状態から、場合によっては数京状態に及び、人間では検査することができない規模である。

(2) 反例が出力される

モデル検査器では、モデルが検査式を満たさない場合には「FALSE」と共に、その証拠である「反例」が出力される。反例はモデルの初期状態から始まって、検査式を満たさない状態に至る経路で示されるため、不具合や予期せぬ動作が発生する原因を容易に解析することができる。

(3) モデル化の際にも不具合の発見が可能である

本実験では、機能安全規格の安全度水準レベル 3（SIL3）の認証では、モデル検査の適用レベルをモデル記述言語による設計書の形式仕様記述までとしている。モデル検査では、数理的な仕様記述言語でモデルを作成する際にも、自然言語による記述の漏れや抜け、不確定な動作（不具合等）を発見できる。

(4) 自動化が進んでいる

モデル検査は、形式手法の中でも最も自動化が進んでおり、様々な種類のツールが、有償あるいは無償で公開されている。代表的なモデル検査器としては、「SMV」、「SPIN」、「UPPAAL」、「LTSA」等が挙げられる。

(5) 導入が容易である

形式手法の中では、導入にあたって必要な事前知識が比較的少ない技術である。簡単なプログラミングを行う技術と、論理学の基礎的な知識があればモデル検査器を操作することができる。初心者でも容易に理解できる入門書や、上級者向けに詳細な技術や仕組みを紹介する書籍も販売されている。

(6) 結果の管理が容易である

検査結果として出力されるファイルは小容量であるため、検査のエビデンスの保管が容易である。また反例を含む結果ファイルがあれば、モデル検査器上で不具合現象を再現することができるため、社内やプロジェクトチーム内でシステムの障害情報を共有することや、障害管理に利用することができる。

(7) モデル検査特有の検査が可能である

モデル検査では従来の動作試験では検査できない安全性の検査が可能である。論理学での安全性とは「起こるべきではないことが起こらないこと」である。従来の動作試験ではシステムへの操作や入力に対する応答を見ること、すなわち「起こってほしいことが起こること」だけを検査することができた。モデル検査では、起こらないことを検査できるため「表 1-11　説明力を強化したい品質」で示した安全性 1 と安全性 2 の検査が可能である。

3.3. モデル検査器 NuSMV

モデルの全数探索ができるモデル検査器は、欧米の研究機関を中心に数種類がインターネット上で公開されている。代表的なモデル検査器とその特徴を表 3-2 に示す。詳細は各々のモデル検査器の Web サイトを参照して頂きたい。

表 3-2　代表的なモデル検査器

NO	ツール名称	特徴
1	SMV	SPIN と共に広く利用されているモデル検査器である。モデル記述言語の構文が非常に容易で初心者でも扱いやすい。状態遷移図や状態遷移表のモデル検査に適している。大規模なモデルを高速で検査することができる。複数の種類がありそれらを総称して「SMV 系」と呼ばれることもある。 【URL】 NuSMV　：http://nusmv.irst.itc.it/ CMU-SMV　：http://www.cs.cmu.edu/~modelcheck/
2	UPPAAL	GUI の完成度が高いツールである。状態遷移図を作成するとモデルを自動生成する機能がある。他のモデル検査器にはない特徴として、実時間モデル検査が可能である。 研究用の無償版と商業利用可能な有償版がある。 【URL】http://www.uppaal.com/
3	SPIN	SMV と同様に国内外を問わず利用者が多い。C 言語と類似した Promela と呼ばれるモデル記述言語を採用しているため、プログラミング言語で記述されたソースコードのモデル検査が容易である。 【URL】http://spinroot.com/spin/whatispin.html
4	Alloy	モデルから検査式を満たす遷移系を列挙できるため、モデルの振る舞いや状態を網羅的に確認することができる。集合論に基づいたモデル記述言語を採用しており産業界で普及しているプログラミング言語とは異なるため、論理学や数学の事前知識が必要である。他のモデル検査器と併用することで大きな効果が得られる場合もある。 【URL】http://alloy.mit.edu/community/

実験では、SMV 系のモデル検査器である「NuSMV」を使用した。モデル検査器 NuSMV を選定した理由を表 3-3 に示す。

表 3-3　モデル検査器 NuSMV の選定理由

NO	項目	詳細
1	多くの実績がある	ツール自体の歴史が古く、多くの適用事例があり実績がある。内部のデータ構造として採用しているBDD（Binary Decision Diagram）についても、標準的なパッケージが公開される等、枯れた技術であり実績がある。これらのことから、アプリケーションとしての動作が安定しており、検査結果の信憑性が高い。
2	状態爆発が発生し難い	内部のデータ構造であるBDDはモデルを非常に効率的に構築／計算／管理することができる。他のモデル検査器と比較すると、同一の物理メモリで、より多くの状態を表現できるため状態爆発が発生し難い。
3	検査処理が速い	BDD によって、状態遷移系同士の論理積や論理和を求める演算が高速に行えるため、モデル検査の処理が高速である。 いかなるモデルでも、他のモデル検査器より処理が高速であるとは限らないが、人間が開発するシステムの振る舞いは、BDD と相性が良く、効率的に演算できることが経験的に知られている。
4	オブジェクト指向である	SMV 系のモデル記述言語はオブジェクト指向であるため、状態遷移図や状態遷移表、自然言語で記述された仕様のモデル化が容易である。本実験で検査対象とした配電自動化システムの設計書は、状態遷移図と自然言語で仕様が記述されており、SMV 系のモデル検査器の利用が適している。
5	無償での商用利用が可能	NuSMV は商用利用であっても無償での利用が可能である。OS についても Windows／Linux のどちらにも対応しており企業での利用がしやすい。

3.4. モデル検査器 NuSMV のモデル記述言語

モデル検査器NuSMV のモデル記述言語である「SMV 言語」で記述されたモデルの例を図 3-2 に示す。

```
MODULE main

/* DEFINE 文記述部 */
  FLG := Var_A = nnn & Var_B = mmm;

/* 変数宣言部 */
VAR
  Var_A : 変数 Var_A の型;
  Var_B : 変数 Var_B の型;

/* 状態遷移系記述部 */
ASSIGN
  init(Var_A) := 変数 Var_A の初期値;
  init(Var_B) := 変数 Var_B の初期値;

  next(Var_A) := 変数 Var_A の状態遷移;
  next(Var_B) := 変数 Var_B の状態遷移;
```

図 3-2　NuSMV のモデルの例

SMV 言語の構文は簡単であるため可読性が高く、モデル設計やモデル製作のミスを最小限に抑えることができる。モデルを記述したファイルは SMV ファイルと呼ばれる。SMV ファイルでは、まず変数宣言部で変数を宣言して、次に状態遷移系記述部で、その変数の初期値と状態遷移の様子を記述する。モジュール（MODULE）は main モジュール以外にも、必要に応じてサブモジュールも記述する。個々のモジュールの同期／非同期が設定可能であるため並行システムの記述にも対応している。また、一般的なプログラミング言語と同様、必要であれば DEFINE 文を記述することができる。図 3-2 の例では、「Var_A = nnn & Var_B = mmm」の値を、変数 FLG で DEFINE 定義している。

SMV 言語では、変数毎に振る舞いを記述するため、状態遷移図からの記述に適している。また、変数をオブジェクトと捉えると、オブジェクト指向の記述言語ということができる。

状態遷移図とモデルの簡単な例を図 3-3 に示す。

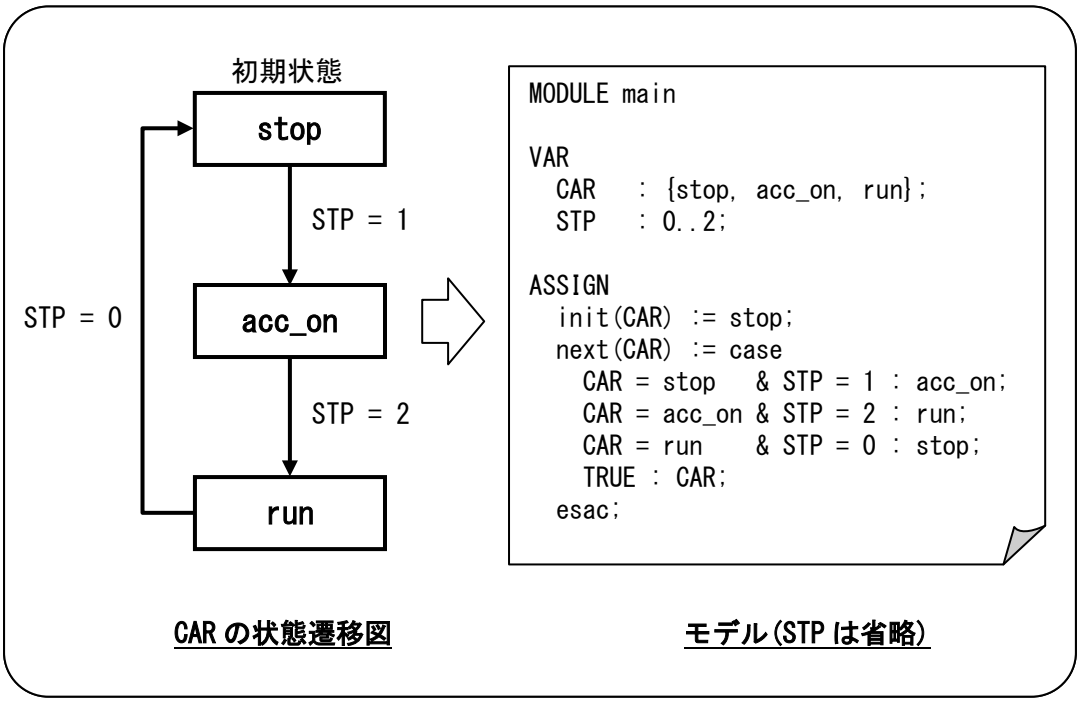


図 3-3　状態遷移図とモデルの例

init 文では変数の初期値を記述する。「init(CAR) := stop」は、変数 CAR の初期値が初期状態 stop（停止）であることを示す。

next 文では、初期状態からの遷移（振る舞い）を記述する。next 文では case 式だけ記述することができる。case 式による条件の場合分けが不要なときは省略可能である。「CAR = acc_on & STP = 2 : run」は「条件 : 遷移先;」の意味である。変数 CAR が acc_on（アクセサリー電源 ON）の状態で変数 STP が 2 となった場合に、変数 CAR は run（走行状態）に遷移する。「TRUE：CAR;」は C 言語における Switch 文の「default」と同様の記述である。case 文の条件が全て不成立の場合に自身の値に遷移する、すなわち前回値を保持することを示している。図では変数 STP のモデルは省略したが、変数 CAR と同様に init 文で初期状態を、next 文で遷移系を記述すれば良い。

変数毎の取り得る状態数を全て掛け合わせた数が理論状態数である。図 3-3 では変数 CAR の状態数 3 × 変数 STP の状態数 3 = 9 となり、理論状態数は 9 状態である。理論状態数から到達可能な状態のみに着目したのが到達可能状態数である。到達可能状態数は次の式で表される。「到達可能状態数 = 理論状態数－到達不可能状態数」

到達可能状態数は全ての変数の状態遷移系を合成したモデル全体の状態遷移系の状態の数である。到達不可能な状態とは、自動車の例では、前輪が右回りに回転中で後輪が左回りに回転中の状態、つまり有り得ない状態である。

3.5. モデル検査器 NuSMV の検査式

NuSMV では検査したい性質（検査式）を CTL（Computation Tree Logic）式あるいは LTL（Liner Tree Logic）式で記述する。両式とも、様々な性質を記述することが可能であり、その記述力には大きな差はない。本実験では検査式として CTL 式を採用した。CTL 式は分岐時相論理式と呼ばれ、状態と状態とを結ぶパスの分岐も考慮した性質を記述することができる。CTL 式の 8 つの基本パターンを表 3-4 に示す。

表 3-4　CTL 式の 8 つの基本パターン

基本パターン	意味
AG(P)	全てのパスにおいて、全ての状態で P が成立する
AX(P)	全てのパスにおいて、次の状態で P が成立する
AF(P)	全てのパスにおいて、将来のある状態で P が成立する
A[P U Q]	全てのパスにおいて、 Q が成立する状態より前の状態まで P が成立する状態が続く
EG(P)	あるパスにおいて、全ての状態で P が成立する
EX(P)	あるパスにおいて、次の状態で P が成立する
EF(P)	あるパスにおいて、将来のある状態で P が成立する
E[P U Q]	あるパスにおいて、 Q が成立する状態より前の状態まで P が成立する状態が続く

上記の基本パターンを組み合わせることで、表 3-5 に示すような性質を記述することができる。表 3-5 は、モデル検査を適用する際によく利用するパターンである。

表 3-5　モデル検査を適用する際によく利用するパターン

パターン	日本語による意訳
AG (AF(P))	常に、将来必ず P になる。 使用例）車は、いつかは必ず停止する。
!EF(P)	将来 P となることはない。 使用例）システムがフリーズすることはない。
AG (P -> AF(Q))	常に、P となるならば将来必ず Q となる。 使用例）A ボタンを押下すると必ず A ランプが点灯する。
!EF(EG(P))	将来 P となり続けることはない。 使用例）A ランプが点灯し続けることはない。

3.6. モデル検査器 NuSMV の反例

反例（CounterExample）は、検査結果が FALSE であった場合のみ出力される。反例は、システムが初期状態から出発して、検査式を満たさない状態に至るまでの経路である。NuSMV では、反例はテキスト形式で標準出力されるため、リダイレクション機能等を利用してファイルに保存することが望ましい。反例の一例を図 3-4 に示す。

```
*** This is NuSMV 2.5.4 (compiled on Fri Oct 28 14:13:29 UTC 2011)
*** Enabled addons are: compass
*** For more information on NuSMV see <http://nusmv.fbk.eu>
*** or email to <nusmv-users@list.fbk.eu>.
*** Please report bugs to <nusmv-users@fbk.eu>

*** Copyright (c) 2010, Fondazione Bruno Kessler

*** This version of NuSMV is linked to the CUDD library version 2.4.1
*** Copyright (c) 1995-2004, Regents of the University of Colorado

*** This version of NuSMV is linked to the MiniSat SAT solver.
*** See http://www.cs.chalmers.se/Cs/Research/FormalMethods/MiniSat
*** Copyright (c) 2003-2005, Niklas Een, Niklas Sorensson

-- specification !(EF (EG ((up = 0 & down = 1) & kasoku = 1)))  is false
-- as demonstrated by the following execution sequence
Trace Description: CTL Counterexample
Trace Type: Counterexample
-> State: 1.1 <-
  up = 0
  down = 0
  kasoku = 0
  up_P = 0
  down_P = 0
  up_flg = 0
  down_flg = 0
  PC = 16
-> State: 1.2 <-
  PC = 10
-> State: 1.3 <-
  PC = 11
-> State: 1.4 <-
  PC = 13
```

図 3-4　NuSMV の反例の一例

反例の「FALSE」は、CTL 検査式「!(EF (EG ((up = 0 & down = 1) & kasoku = 1)))」の検査結果が FALSE であったことを示している。また「State: 1.1 ・・・ State: 1.2 ・・・ State: 1.3 ・・・ State: 1.4・・・」は、状態 1（初期状態） → 状態 2 → 状態 3 → 状態 4・・・のパスと、個々の状態での変数の値を示している。

4. モデル検査の適用プロセス

本実験では、株式会社フォーマルテックと独立行政法人産業技術総合研究所が普及活動を行っている、モデル検査を適用する際の標準的な業務プロセスである「モデル検査の適用プロセス」を採用した。本プロセスはソフトウェア開発の V 字モデルと同様に、モデル検査器 NuSMV を適用する際の作業を、上流工程から下流工程に向かって段階的に管理するためのプロセスである。モデル検査の適用プロセスを図 4-1 に示す。

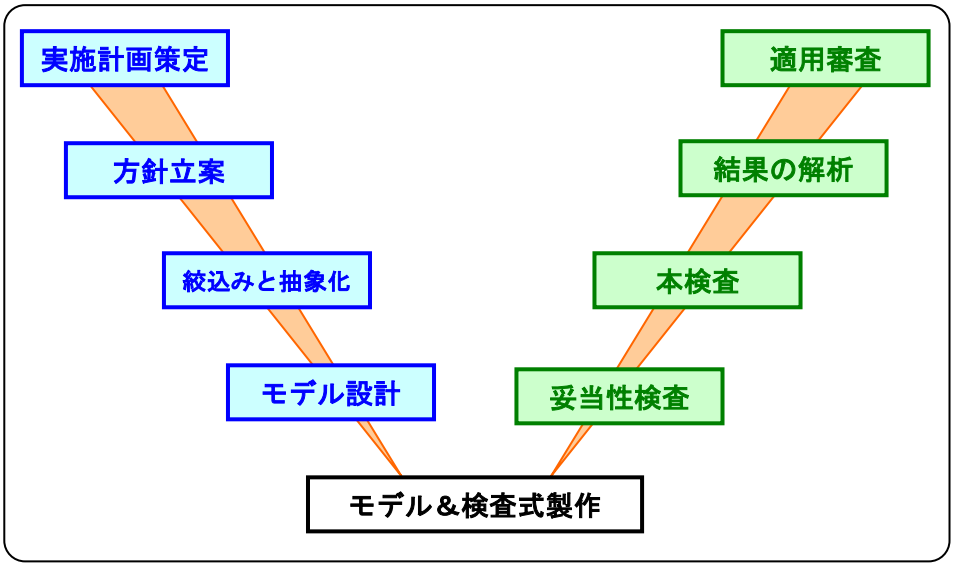


図 4-1　モデル検査の適用プロセス

ソフトウェア開発の作業工程との対応を図 4-2 に示す。

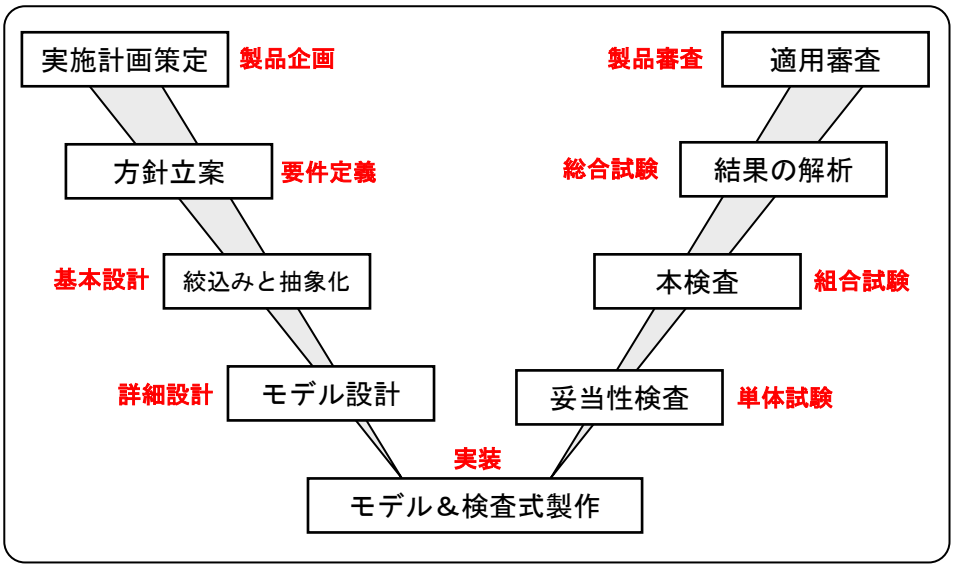


図 4-2　ソフトウェア開発の作業工程との対応

各工程の略称と正式名称を表 4-1 に示す。

表 4-1　各工程の略称と正式名称

NO	略称	正式名称
1	実施計画策定	モデル検査の実施計画策定
2	方針立案	検査の方針立案 □検査全体の方針立案 □モデル化の方針立案 □検査項目の方針立案
3	絞込みと抽象化	検査対象の絞込みと抽象化
4	モデル設計	モデル設計
5	モデル&検査式製作	モデルと検査式の製作
6	妥当性検査	モデルの妥当性検査
7	本検査	本検査
8	結果の解析	検査結果の解析
9	適用審査	モデル検査の適用審査

各工程の入力と作業内容、作業の結果得られる出力を以下に示す。

4.1. モデル検査の実施計画策定

モデル検査の実施計画策定は、ソフトウェア開発プロセスにおける最初の計画段階である製品企画に該当する。作業プロセスの最上流の工程であり、ソフトウェア開発での企画と同様に重要な工程である。入力と作業内容及び出力の一覧を表 4-2 に示す。

表 4-2　入力と作業内容及び出力の一覧

項目	内容
入力	仕様書／設計書／ソースコード
作業内容	モデル検査適用の企画・提案
出力	実施計画書

(1) 入力

本工程の入力は、上流工程に適用する場合は仕様書や設計書、下流工程に適用する場合はソースコードや詳細設計書である。モデル検査の適用依頼者より入手したドキュメントやソースコードに不明な点が有る場合はヒアリングあるいは文書による調査を行う。ヒアリング結果と調査結果も入力となる。

(2) 作業内容

ソフトウェア開発プロセスにおける製品企画に該当するため、モデル検査を適用するにあたっての目的等を明確にして、適用依頼者に対して企画・提案を行う。また、検査対象のシステムを十分に調査し仕様や仕組みを理解する。第三者検証のサービスとして提供する場合には、実施計画や体制、スケジュールについても検討する。

(3) 出力

出力は、システム概要や目的、体制図、作業工程表、スケジュール等の検査の概要を記載した実施計画書となる。

4.2. 検査の方針立案

ソフトウェア開発プロセスにおける要件定義に該当する。前工程は主として運用面での企画・提案であったが、本工程では技術的な側面も考慮して、モデル検査を適用するにあたっての全体の方針を立案し、さらにモデルと検査項目の方針を立案する。

本工程はさらに表 4-3 に示す 3 つの工程に分類される。

表 4-3　検査の方針立案の作業分類

NO	作業
1	検査全体の方針立案
2	モデル化の方針立案
3	検査項目の方針立案

(1) 検査全体の方針立案

モデル検査全体の方針を立案し、検査にあたっての仮定や前提条件も明確にする。入力と作業内容及び出力の一覧を表 4-4 に示す。

表 4-4　入力と作業内容及び出力の一覧

項目	内容
入力	仕様書／設計書／ソースコード
作業内容	検査の目的の明確化 モデル化の対象と検査項目の導出元の特定
出力	検査対象を個別に特定できる情報 検査にあたっての仮定と前提条件

- 入力

本工程では、前工程と同じく仕様書や設計書、ソースコードが入力となる。入手したドキュメントやソースコードの中からモデル検査を適用する対象物を、1 つあるいは少数に特定する。作業は適用依頼者より適宜合意を取りながら進めることが望ましい。

- 作業内容

まず、検査目的として「何と何を比較して検査するのか」を明確にする。さらに、モデル検査ではモデルが検査式を満たしているか否かを検査するため、「モデル化の対象とするもの」と「検査式を導き出すもの」の 2 つを明確にする必要がある。検査目的とモデル及び検査項目の組合せの例を表 4-5 に示す。

次に、検査にあたっての仮定や前提条件を明確にする。仮定や前提条件の例を表 4-6 に示す。

表 4-5　検査目的とモデル及び検査項目の組合せの例

NO	検査目的	モデル化の対象	検査項目
1	上流／下流間の 整合性の検査	下流側仕様書	上流側仕様書
2	プログラムの動作試験	ソースコード	詳細設計書
3	仕様書の不備の検査 （頁間の矛盾など）	当該仕様書全体	仕様の個々の記載内容
4	不具合解析	仕様書／ソースコード	不具合状態
5	規格類への適合検査	同上	規格／標準

表 4-6　仮定や前提条件の例

NO	仮定や前提条件の例
1	システムの電源状態は常に正常であることを前提とする。
2	通信処理に不具合が潜在する可能性が高いことを仮定する。
3	ハードウェアの異常は発生しないことを前提とする。

- 出力

出力は、ドキュメントの名称や規格番号、ソースコードのファイル名など、検査対象を個別に特定できる情報、検査にあたっての仮定と前提条件である。

仕様書の改版や、それに伴うソースコードの改造があった場合は、ドキュメントの版番号、ソースコートの Ver.NO も一意に特定する。

(2) モデル化の方針立案

「4.2　検査の方針立案」のうち、モデル化を行う際の方針を立案する。対象となるドキュメントやソースコードの中でモデルとして作成する範囲を決定する。入力と作業内容及び出力の一覧を表 4-7 に示す。

表 4-7　入力と作業内容及び出力の一覧

項目	内容
入力	モデル化の対象となる仕様書／ソースコード
作業内容	モデル化の範囲を明確にする
出力	具体的な範囲を特定できる数値や名称

- 入力

  入力は、「4.2(1)検査全体の方針立案」の出力のうちモデル化の対象とする方のドキュメントやソースコードである。検査にあたっての仮定と前提条件によってモデル化の範囲が変わる場合は、それらも入力となる。

- 作業内容

  まず、自然言語からモデル化を行うか、ソースコード、状態遷移図、状態遷移表からモデル化を行うかを明確にする。次に、モデル化の範囲を決定する。範囲を決定する際の例を表 4-8 に示す。

表 4-8　モデル化の範囲の例

モデル化の対象	範囲の例
仕様書	機能仕様書の XX 頁～YY 頁 第 2 章と第 3 章と第 5 章の第 2 節 〇〇機能と□□機能の仕様 〇〇装置と□□装置と△△装置の仕様
ソースコード	〇〇タスク 〇〇関数と□□関数

  範囲を明示するには、第三者でも特定可能な具体的な数値や名称を決定することが重要である。範囲の決定が不十分であると、後の「4.8　検査結果の解析」と「4.9　モデル検査の適用審査」が十分に行えない。

  また、必要に応じてシステムの外部環境のモデル化についても方針を決定する。

- 出力

  出力は、具体的な範囲を特定できる数値や名称と、外部環境のモデル化の方針をまとめたエビデンス（必要な場合のみ）である。

(3) 検査項目の方針立案

検査全体の方針である「4.2　検査の方針立案」のうち、検査項目を検討する際の方針を立案する。どのような性質をどのような検査項目で検査するのかを自然言語のレベルで明確にする。入力と作業内容及び出力の一覧を表 4-9 に示す。

表 4-9　入力と作業内容及び出力の一覧

項目	内容
入力	検査式の導出元
作業内容	検査項目の検討・分類
出力	検査項目一覧

- 入力

  入力は「4.2(1)検査全体の方針立案」の出力のうち検査式を導き出すものと、検査にあたっての仮定と前提条件である。

- 作業内容

  本工程も適用依頼者に大筋の合意を取りながら進めることが望ましい。システムが満たすべき振る舞いや、実現すべき状態を抽出し、検査にあたっての仮定と前提条件を考慮しながら検査項目を検討する。導き出した検査項目は大項目、中項目、小項目等の分類を行う。

  モデル検査特有の検査項目についてもここで検討する。モデル検査の利点である安全性に関する検査項目である。システムの安全性については、仕様書等に記載されていない場合もあり、当該システムが属するドメインの常識や、過去に起きた障害や不具合等からも安全性を見出すことが重要である。

- 出力

  出力は、自然言語で記述された検査項目一覧である。

4.3. 検査対象の絞込みと抽象化

検査対象のシステムの規模が大きく、作成したモデルが大規模になる場合にはモデル検査の技術的課題である状態爆発を回避する必要がある。そこで、「4.2(2)　モデル化の方針立案」で決定した範囲に対して、さらに、絞込みでは仕様書の頁数の削減、ソースコードの範囲縮小を試みる。抽象化では処理の繰り返し回数、装置や入力の数、タイマーの時間等の大きな数量を代表値としたり、公約数とするなどの工夫を行う。

状態爆発が発生する可能性が極めて低い場合は、適用プロセスの中で、本工程のみ省略することができる。入力と作業内容及び出力の一覧を表 4-10 に示す。

表 4-10　入力と作業内容及び出力の一覧

項目	内容
入力	モデル化の範囲
作業内容	モデル化の範囲の更なる絞り込み 数値の抽象化
出力	絞込みと抽象化の作業一覧

(1) 入力

入力は「4.2(2)　モデル化の方針立案」で決定したモデル化の範囲である。

(2) 作業内容

検査対象の絞込みでは「4.2　検査の方針立案」で立案した方針に反しないことを前提にして、モデル化の範囲をさらに絞り込む。絞込みの例を表 4-11 に示す。

表 4-11　絞込みの例

モデル化の対象	絞込みの例
仕様書	機能仕様書の XX 頁は表だけを対象とする 〇〇機能の例外処理は除外する □□装置の故障は考慮しない
ソースコード	Index の並び替えの処理は対象外とする 〇〇関数は戻り値のみモデル化の対象とする

抽象化では主として、大きな数値を小さくすることによって状態数を削減する。同一の振る舞いの繰り返し回数、同種の装置の台数、時間等に関する数値はシステムの性質が変わらないように全ての数値の最小公約数とする等の工夫を行う。また、大量の入力はシステムにとって代表的な値を選択する。

(3) 出力

本工程の作業内容は属人的な要素が大きく、また検査中に状態爆発が発生した場合には再度の絞込みや抽象化が必要となる。したがって、作業の結果や経緯が第三者でも理解できるよう一覧表等にまとめることが重要であり、それが本工程の出力となる。

4.4. モデル設計

モデル設計は、ソフトウェア開発プロセスにおける詳細設計に該当する。抽象的な概念や記述方法を避け、プログラミング言語やモデル記述言語の知識がない第三者でも理解できる形式で表現する。入力と作業内容及び出力の一覧を表 4-12 に示す。

表 4-12　入力と作業内容及び出力の一覧

項目	内容
入力	モデル化の範囲 絞込みと抽象化の作業一覧
作業内容	状態遷移系への変換
出力	モデル設計書

(1) 入力

入力は「4.2(2)　モデル化の方針立案」で決定したモデル化の範囲と、前工程の出力である絞込みと抽象化の一覧である。

(2) 作業内容

モデル検査器 NuSMV のモデル設計で用いられる手法としては、状態遷移図、状態遷移表が挙げられる。モデル検査で扱うモデルは状態遷移系であるため、仕様書が自然言語で記述されている場合は、記載された文章を状態遷移系に変換する。仕様書に状態遷移図や状態遷移表が記載されている場合は、そのまま設計書とすることが可能であり、その場合は、図や表等を識別できる情報を明確にする。

(3) 出力

出力は設計内容を詳細に記載したモデル設計書である。

4.5. モデルと検査式の製作

モデルと検査式の製作は、ソフトウェア開発プロセスにおける実装に該当する。具体的な作業はコーディングとなる。入力と作業内容及び出力の一覧を表 4-13 に示す。

(1) 入力

入力は前工程の出力であるモデル設計書と「4.2(3)　検査項目の方針立案」の出力である検査項目一覧である。

表 4-13　入力と作業内容及び出力の一覧

項目	内容
入力	モデル設計書 検査項目一覧
作業内容	SMV 言語によるコーディング CTL 検査式の作成
出力	モデルと検査式

(2) 作業内容

モデル化ではモデル検査器 NuSMV のモデル記述言語である SMV 言語によりコーディングを行う。ソフトウェア開発の場合と同様に予め「コーディング作法」を決めて、プロジェクト全体で遵守することが重要である。モデルの再利用も考慮して可読性の高いモデルを作成する。

検査式は、検査の目的と個々の検査項目の意味を十分に理解した上で作成する。1 つの式で表現しきれない場合は、複数の式に分割する等の工夫が必要である。モデル検査器 NuSMV では、検査式は CTL 式で記述する。

(3) 出力

出力はモデルと検査式である。

4.6. モデルの妥当性検査

モデルの妥当性検査は、ソフトウェア開発プロセスにおける単体テストに該当する。作成したモデルの単体検査の位置付けである。モデルと実際のシステムとの整合性を検査し、モデルの妥当性を確認する。この後の本検査での手戻りを防ぐ重要な工程である。入力と作業内容及び出力の一覧を表 4-14 に示す。

表 4-14　入力と作業内容及び出力の一覧

項目	内容
入力	モデル
作業内容	予備検査式の作成と検査
出力	妥当性検査済みのモデル 予備検査の結果

(1) 入力

入力は前工程の出力であるモデルである。

(2) 作業内容

予備検査式を作成し、モデル検査器 NuSMV を実行させ検査を行う。予備検査の項目の例を表 4-15 に示す。

表 4-15　予備検査の項目の例

NO	検査項目	内容
1	状態の到達可能性	仕様書で定義された状態は設計の必要性から導き出されたものであり、当該状態に必ず 1 度は到達することを検査する。
2	外部環境の動作確認	外部環境の振る舞いや変化が反例として出力されるような検査式で検査する。
3	変数毎の到達可能性	変数の全ての値に最低 1 度は到達すること。
4	実システムとの整合性	実際のシステムの振る舞いが反例として出力されるような検査式で検査する。

NO.1 の到達可能性の検査では状態爆発が発生することもある。この段階で状態爆発が発生した場合には、次の「4.7　本検査」でも発生する可能性が高い。したがって次工程には進まず「4.2　検査の方針立案」あるいは「4.3　検査対象の絞込みと抽象化」に戻る必要がある。モデルと実際のシステムとの不整合やモデル化のミスを発見した場合は、上流工程である「4.4　モデル設計」あるいは「4.5　モデルと検査式の製作」に戻らなければならない。

(3) 出力

出力は妥当性検査済みのモデルと、その検査結果である。

4.7. 本検査

本検査は、ソフトウェア開発プロセスにおける結合テストに該当する。モデルと検査式との「結合」検査の位置付けである。本来の検証を行う。入力と作業内容及び出力の一覧を表 4-16 に示す。

表 4-16　入力と作業内容及び出力の一覧

項目	内容
入力	モデルと検査式
作業内容	モデル検査器を用いた検査の実行
出力	検査結果 反例

(1) 入力

入力は「4.5　モデルと検査式の製作」の出力であるモデルと検査式である。

(2) 作業内容

モデル検査器 NuSMV を用いて検査を行う。作業にあたっての注意事項を表 4-17 に示す。

表 4-17　本検査での注意事項

NO	項目	内容
1	検査結果の予測	検査前に検査結果の予測を行い、予測と異なる場合は検査式をよく吟味する。
2	到達可能状態数の確認	モデル検査器 NuSMV では、適切なオプションを指定することでモデル（状態遷移系）が到達可能な状態数が出力されるため、状態数が予め想定した範囲内であるか否かを確認する。 特に到達可能状態数が極端に小さい場合は「4.4 モデル設計」のミスが考えられる

(3) 出力

出力は検査結果と反例である。

4.8. 検査結果の解析

検査結果の解析は、ソフトウェア開発プロセスにおける総合試験に該当する。入力と作業内容及び出力の一覧を表 4-18 に示す。

表 4-18　入力と作業内容及び出力の一覧

項目	内容
入力	検査結果 反例
作業内容	第一段階：全工程の作業の妥当性の確認 第二段階：TRUE となった検査項目の確認 第三段階：反例の確認
出力	解析済みの検査結果の一覧

(1) 入力

入力は前工程の出力である検査結果と反例である。

(2) 作業内容

検査結果に対して、以下の状況に応じた確認を行う。

第一段階では、全ての検査結果に対して、これまで実施した全工程の作業の妥当性を確認する。表 4-19 に確認項目を列挙する。

表 4-19　第一段階での確認項目

NO	確認項目
1	「4.2(1)　検査全体の方針立案」の方針と仮定および前提条件の妥当性
2	「4.2(2)　モデル化の方針立案」のモデル化の範囲の妥当性
3	「4.2(3)　検査項目の方針立案」の検査目的の達成度
4	「4.3　検査対象の絞込みと抽象化」の対象と実施内容の妥当性
5	「4.4　モデル設計」で行った設計の妥当性

第二段階では、検査結果が TRUE となった検査項目に着目する。検査式が正しく作成されているかを確認する。また、必要に応じて、当該検査式の否定形（例　EF(P)の場合は!EF(P)）の検査式を検査することによって故意に反例を出力させ TRUE である場合のモデルの振る舞いを確認する。

最後に反例を確認する。反例は、まずモデル上で確認し、次に、モデルの基となった実システム上で実際に起こり得るか否かを調査する。反例を解析する際には初期状態からトレースする方法と、最後の状態から初期状態に向かって遡ってトレースする方法が

ある。前者は振る舞いを理解しやすく偽反例の発見が容易である。後者は不具合解析に適している。反例では不具合の発生する状態が最後の状態として示されるからである。

(3) 出力

出力は解析済みの検査結果の一覧である。さらに、反例が出力された場合、すなわち不具合が発見できた場合は実システムでも発生することの証拠と不具合の原因も出力となる。

4.9. モデル検査の適用審査

モデル検査の適用審査は、ソフトウェア開発プロセスにおける最終段階である製品審査に該当する。製作したモデル、検査式、出力された反例等を含めて、当該案件のモデル検査適用の妥当性を確認する。適用依頼者による受け入れ検査と考えることができる。入力と作業内容及び出力の一覧を表 4-20 に示す。

表 4-20　入力と作業内容及び出力の一覧

項目	内容
入力	全工程の出力
作業内容	モデル検査適用の妥当性の確認
出力	モデル検査報告書

(1) 入力

入力はこれまでの工程の全ての出力である。

(2) 作業内容

全ての出力を簡潔にまとめて「モデル検査報告書」を作成する。本報告書によってモデル検査の適用が有効かつ妥当であったことを確認する。モデル検査報告書は本適用プロセスの工程に沿った形で作成する。

(3) 出力

出力はモデル検査報告書である。報告書の目次の例を図 4-3 に示す。

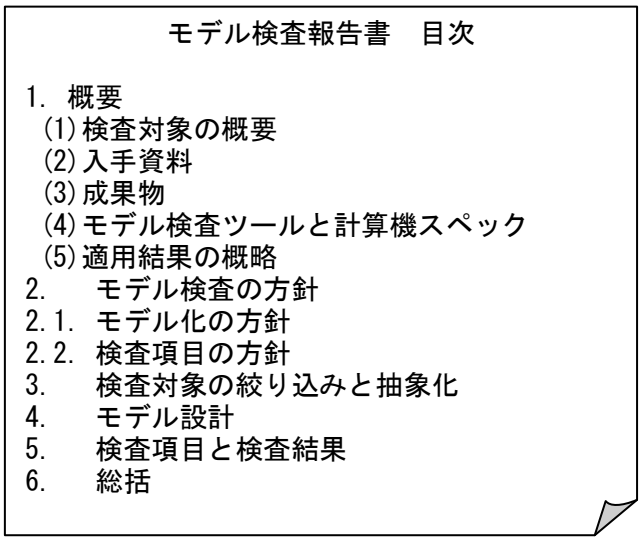


図 4-3　モデル検査報告書の目次の例

本実験で実施したモデル設計の内容と、作成したモデルと CTL 検査式、またモデル検査器 NuSMV より出力された反例を抜粋して、本書末尾の「実験で作成されたデータ等の資料」の「1　モデル検査の適用で作成した資料」に添付する。

5. モデル検査の適用結果とコスト評価

5.1. モデル検査の適用結果

(1) 検査内容

本実験のモデル検査適用では「配電自動化システム　ソフトウェア設計書」を基に、設計者からの仕様のヒアリング内容を考慮してモデルを作成し、CTL 検査式を用いてモデル検査を実施した。作成した CTL 検査式は合計 31 式である。検索項目と CTL 検査式の数を表 5-1 に示す。

表 5-1　検査項目と CTL 検査式の数

NO	検査項目	CTL 式の数
1	設計書で定義された状態への到達可能性の検査	13
2	特定状態からの脱出(他状態への遷移)可能性の検査	13
3	特定機能の検査	1
4	特定状態における電源状態の検査	2
5	通常運用時の停電の有無	1
6	停電状態の継続の有無	1
合計		31

表 5-1 の NO.3 と NO.4 は「1.3　実験対象システムと実験環境」の表 1-4 で示した「ソフトウェア設計の懸案事項」より導出した検査項目である。

黄色で網掛けした NO.1 と NO.2 の検査項目は「1.5　説明力を強化したい品質」の表 1-11 で示した「安全性 1」に該当する。さらに、水色で網掛けした NO.5 と NO.6 の検査項目は「安全性 2」に該当する。対応を表 5-2 に示す。

表 5-2　説明力を強化したい品質と検査項目の対応

説明力を強化したい品質	内容	検査項目
安全性 1	ソフトウェアを含めたシステムがフリーズしないこと。	NO.1 と NO.2
安全性 2	予期せぬ動作により本システム自体が原因となって電気事故が発生し停電とならないこと。	NO.5 と NO.6

NO.1 は設計書で定義された状態への到達可能性の有無を検査する検査項目である。全ての状態は設計上の必要性から定義されたものであり、到達可能性は「有」でなければならない。したがって、検査結果は全て「TRUE」のはずであり、検査結果が「FALSE」の場合にはシステムのフリーズ（デッドロック等）の問題がある可能性が高い。NO.2 は上記 NO.1 と対を成す検査項目である。NO.1 と同様に設計書で定義された各状態からの脱出可能性の有無を検査する検査項目である。システムが、定義された任意の状態に到達後、当該状態から別の状態に遷移できることを検査するものであり、本検査項目についても検査結果は全て「TRUE」でなければならない。検査結果が「FALSE」の場合には、同じくフリーズ（ライブロック等）の問題がある可能性が高い。

NO.1 と NO.2 については、モデル検査の適用プロセスの「モデルの妥当性検査」の工程で検査を行った。

NO.5 では外部で事故が発生していないにもかかわらず、本システムの振る舞いによって、すなわち本システム自体が原因となって停電が発生する可能性を検査する。システムの根幹を成すものであり必ず「TRUE」でなければならない。NO.6 についても本システムの根幹を問う検査項目である。事故からの復旧を目的とする本システムが、停電発生の直接的な原因にならないだけでなく、停電継続の原因にならないことを検査した。

(2) 検査結果

本適用では、指摘事項が発見されたため「初期モデル」とモデル上の改良事項を反映した「改良モデル」の 2 つのモデルを作成した。モデルと到達可能状態数の一覧を表 5-3 に示す。

表 5-3　モデルと到達可能状態数

NO	モデル	到達可能状態数
1	初期モデル	79,360
2	改良モデル	102,400

モデル毎の検査結果を表 5-4 に示す。「検査項目 NO」は表 5-1 の「NO」である。検査項目 NO.1 と NO.2 では検査結果が全て「TRUE」となり、説明力を強化したい品質の「安全性 1：ソフトウェアを含めたシステムがフリーズしないこと」を証明することができた。

検査項目 NO.5 と NO.6 でも検査結果が共に「TRUE」となり、「安全性 2：予期せぬ動作により本システム自体が原因となって電気事故が発生し停電とならないこと」を証明することができた。

表 5-4　モデル毎の検査結果

検査項目 NO	初期モデル	改良モデル
1	全て TRUE	全て TRUE
2	全て TRUE	全て TRUE
3	FALSE	
4	① FALSE ② FALSE	① TRUE ② TRUE
5		TRUE
6		TRUE

検査項目 NO.3 と NO.4 では、初期モデルで検査結果が「FALSE」となり、合計 3 件の指摘事項を発見した。NO.4 の検査項目で発見された 2 件の指摘事項については、モデル上の改良を行い、改良したモデルで再検査を行ったところ、検査結果が全て「TRUE」となることを確認した。

5.2. 安全度水準レベル 3（SIL3）の場合のコスト評価

表 5-5 に示す 5 つの観点からコストの評価（集計／算出）を行った。

表 5-5　コストの評価（集計／算出）の観点（SIL3）

NO	観点
1	総作業コスト
2	設計書の頁当たりの作業コスト
3	モデルの 1 行当たりの作業コスト
4	モデル検査の適用プロセスの工程毎の作業コスト
5	作業項目の割合

集計・算出のために作成した実験データの集計シートを本書末尾の「実験で作成されたデータ等の資料」の「3　実験データの集計シート（SIL3)」に添付する。

(1) 総作業コストの集計

モデル検査の適用プロセスの第一の作業工程である「モデル検査の実施計画策定」から、モデル記述言語による設計書の形式仕様記述を行う「モデルと検査式の製作」及び「モデルの妥当性検査」までに必要な作業時間を集計した。ただし、本レベルではモデル化までがコスト評価の対象であるため、本検査の際に必要な CTL 検査式の製作時間は除外した。また、「モデル検査の適用審査」の工程で作成するモデル検査報告書についても、報告書の約 1/3 を占める検査結果の報告が不要であるため、レベル 4 における報告書作成時間の 2/3（1 － 1/3）を加算することとした。

結果を表 5-6 に示す。総作業コストは「147.75 人・時」であった。

表 5-6　総作業コスト（SIL3）

項目	結果[人・時]
総作業コスト	147.75

安全度水準レベル 3（SIL3）での作業対象の資料を表 5-7 に示す。

表 5-7　安全度水準レベル 3（SIL3）での作業対象の資料

NO	名称	規模[頁]
1	配電自動化システム　ソフトウェア設計書	52

(2) 設計書の頁当たりの作業コストの算出

モデル記述言語による設計書の形式仕様記述までの作業で、設計書 1 頁当たりに必要な時間を算出した。計算式を図 5-1 に示す。

$$\text{設計書の頁当たりの作業コスト} = \frac{\text{上記(1)の総作業時間}}{\text{配電自動化システム　ソフトウェア設計書の頁数}}$$

図 5-1　設計書の頁当たりの作業コスト（SIL3）

自然言語で記述された設計書には、論理的かつ緻密に記述されているもの、曖昧な表現が含まれているもの、派生開発等の理由で既存のシステムからの差分だけが正確に記述されているもの等、様々な記述レベルがあり、そのレベルによって形式仕様記述に必要な時間が大きく異なる。したがって、本項目で算出した数値は他の事例と単純には比較できないことに注意が必要である。

結果を表 5-8 に示す。

表 5-8　設計書の頁当たりの作業コストの算出（SIL3）

項目	値	単位
総作業時間(A)	147.75	[人・時]
配電自動化システム　ソフトウェア設計書の頁数(B)	52	[頁]
設計書の頁当たりの作業コスト(A/B)	2.84	[人・時／頁]

設計書の頁当たりの作業コストは「2.84 人・時／頁」であった。

(3) モデルの 1 行当たりの作業コストの算出

モデル記述言語による設計書の形式仕様記述の最終結果であるモデルの 1 行当たりの作業時間を算出した。計算式を図 5-2 に示す。なお、モデルの行数には、コメント行、空白行も含むものとする。

$$\text{モデルの 1 行当たりの作業コスト} = \frac{\text{上記(1)の総作業時間}}{\text{作成したモデルの行数}}$$

図 5-2　モデルの 1 行当たりの作業コスト

本項目についても、他の事例と単純には比較できないことに注意が必要である。なぜなら、モデルの行数は、当該事例で採用した絞込みと抽象化の手法や範囲、度合いによって大きく変化するためである。

結果を表 5-9 に示す。本実験では初期モデルと改良モデルの 2 つのモデルを作成したが、SIL3 での作業である形式仕様記述までに作成したのは初期モデルであるため、モデルの行数は初期モデルのものを採用した。

表 5-9　モデルの 1 行当たりの作業コストの算出

項目	値	単位
総作業時間(A)	147.75	[人・時]
初期モデルの行数(B)	276	[行]
モデルの 1 行当たりの作業コスト(A/B)	0.54	[人・時／行]

設計書の頁当たりの作業コストは「0.54 人・時／行」であった。

(4) モデル検査の適用プロセスの工程毎の作業コストの集計

モデル検査の適用プロセスの工程毎の作業時間を集計した。本レベルで必要な工程と作業時間は上記総作業時間と同じである。

工程毎の作業時間を表 5-10 に示す。

表 5-10　工程毎の作業時間（SIL3）

工程	合計[人・時]
実施計画策定	32.25
方針立案	44.25
絞込みと抽象化	14.50
モデル設計	19.00
モデル&検査式製作	10.50
妥当性検査	6.75
適用審査	20.50
合計	147.75

工程毎の作業時間の割合を円グラフで図 5-3 に示す。

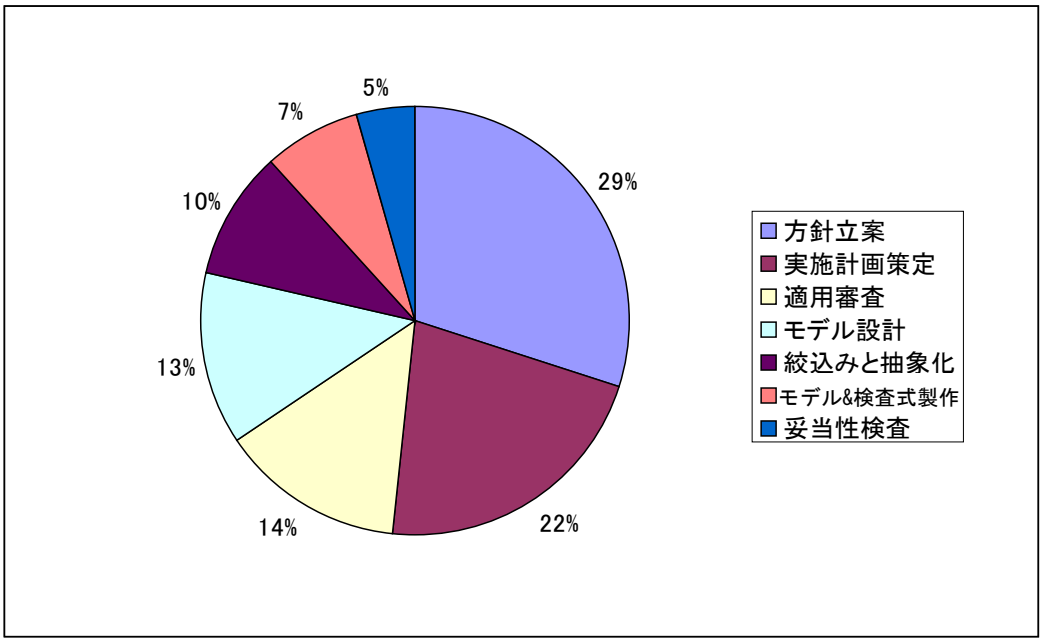


図 5-3　工程毎の作業時間の割合（SIL3）

図 5-3 の円グラフは割合の降順に並び替えを行った。

(5) 作業項目の割合の算出

「2.1　コストの計測」の表 2-1 に示した打合、検討、作業、実行の 4 つの作業項目の割合を 2 種類算出した。総作業時間内での割合と、モデル検査の適用プロセスの工程毎での割合である。

作業項目毎の作業時間を表 5-11 に示す。

表 5-11　作業項目毎の作業時間（SIL3）

作業項目	合計[人・時]
打合	39.25
検討	52.00
作業	54.00
実行	2.50
合計	147.75

総作業時間に占める 4 つの作業項目の割合を円グラフで図 5-4 に示す。

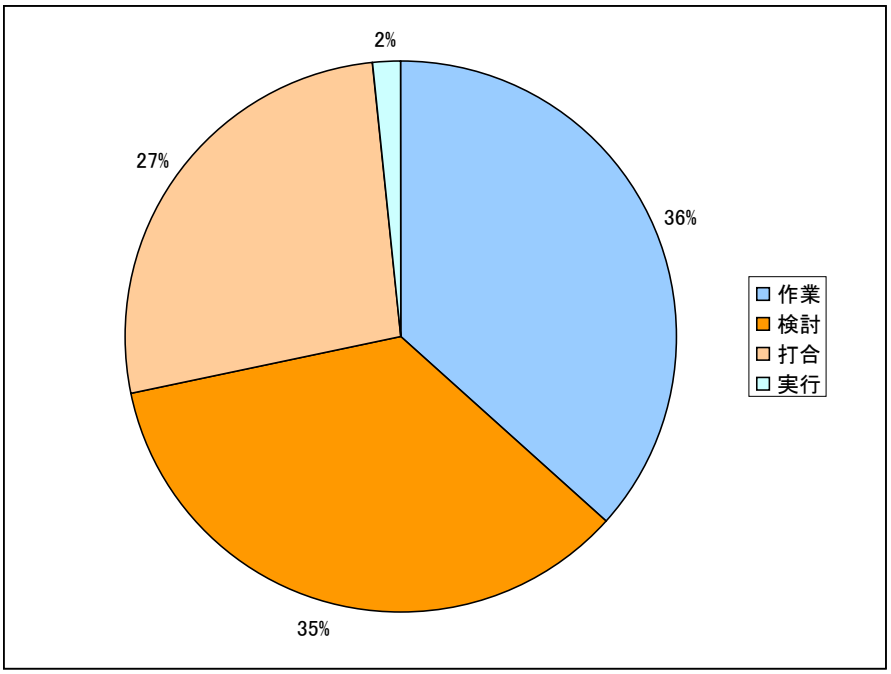


図 5-4　総作業時間に占める 4 つの作業項目の割合（SIL3）

図 5-4 の円グラフは割合の降順に並び替えを行った。

作業項目毎かつ適用プロセスの工程毎の作業割合を表 5-12 に示す。

表 5-12　作業項目毎かつ適用プロセスの工程毎の作業割合（SIL3）

工程	打合	検討	作業	実行	合計[%]
適用審査	19.5	9.8	70.7	0.0	100
妥当性検査	0.0	14.8	55.6	29.6	100
モデル&検査式製作	0.0	9.5	85.7	4.8	100
モデル設計	5.3	32.9	61.8	0.0	100
絞込みと抽象化	10.3	74.1	15.5	0.0	100
方針立案	44.6	39.5	15.8	0.0	100
実施計画策定	40.3	41.9	17.8	0.0	100

適用プロセスの工程毎に占める 4 つの作業項目の割合を 100%積み上げ方式の棒グラフで図 5-5 に示す。

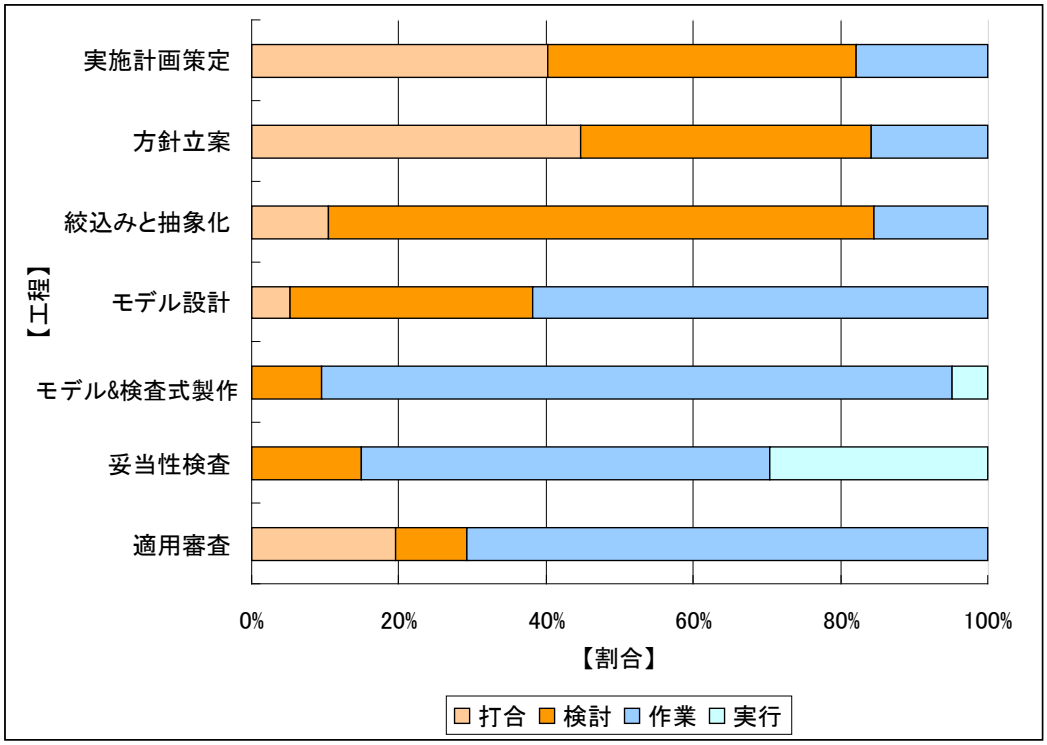


図 5-5　適用プロセスの工程毎に占める 4 つの作業項目の割合（SIL3）

5.3. 安全度水準レベル 4（SIL4）の場合のコスト評価

表 5-13 に示す 6 つの観点からコストの評価（集計／算出）を行った。

表 5-13　コストの評価（集計／算出）の観点（SIL4）

NO	観点
1	総作業コスト
2	設計書の頁当たりの作業コスト
3	1 人・時で検査可能な到達可能状態数
4	モデル検査の適用プロセスの工程毎の作業コスト
5	作業項目の割合
6	指摘事項 1 件当たりの作業コスト

集計・算出のために作成した実験データの集計シートを本書末尾の「実験で作成されたデータ等の資料」の「4　実験データの集計シート（SIL4)」に添付する。

(1) 総作業コストの集計

モデル検査の適用プロセスの第一の作業工程である「モデル検査の実施計画策定」から最終工程である「モデル検査の適用審査」までに必要な作業時間を集計した。

結果を表 5-14 に示す。総作業コストは「200.50 人・時」であった。

表 5-14　総作業コスト（SIL4）

項目	結果[人・時]
総作業コスト	200.50

安全度水準レベル 4（SIL4）での作業対象の資料を表 5-7 に示す。

表 5-15　安全度水準レベル 4（SIL4）での作業対象の資料

NO	名称	規模[頁]
1	配電自動化システム　ソフトウェア設計書	52
2	ソフトウェア設計の懸案事項	3
合計		55

(2) 適用に必要な資料の頁当たりの作業コストの算出

形式検証を含むモデル検査の適用に必要な資料 1 頁当たりの時間を算出した。レベル 4 では形式検証で用いる検査式を作成するために、入手資料（表 1-4）の NO.2「ソフトウェア設計の懸案事項」も用いたため、分母にその頁数を加算した。計算式を図 5-6 に示す。

適用に必要な資料の頁当たりの作業コスト　=

$$\frac{\text{上記(1)の総作業時間}}{\text{配電自動化システム　ソフトウェア設計書の頁数} + \text{ソフトウェア設計の懸案事項の頁数}}$$

図 5-6　適用に必要な資料の頁当たりの作業コスト（SIL4）

自然言語で記述された設計書には、論理的かつ緻密に記述されているもの、曖昧な表現が含まれているもの、派生開発等の理由で既存のシステムからの差分だけが正確に記述されているもの等、様々な記述レベルがあり、そのレベルによって形式仕様記述に必要な時間が大きく異なる。したがって、本項目で算出した数値は他の事例と単純には比較できないことに注意が必要である。

結果を表 5-16 に示す。

表 5-16　適用に必要な資料の頁当たりの作業コストの算出（SIL4）

項目	値	単位
総作業時間(A)	200.50	[人・時]
配電自動化システム　ソフトウェア設計書の頁数(B)	52	[頁]
ソフトウェア設計の懸案事項(C)	3	[頁]
設計書の頁当たりの作業コスト(A/(B+C))	3.65	[人・時／頁]

形式検証を含む適用に必要な資料の頁当たりの作業コストは「3.65 人・時／頁」であった。

(3) 1 人・時で検査可能な到達可能状態数の算出

モデル検査を適用したシステムの規模は、モデルの到達可能状態数によって、ある程度知ることができる。モデル検査の最大の利点は全数探索であり、どれだけの状態数のモデルをどれだけの作業時間で全数探索できたのかが大きな焦点となる。モデル検査器 NuSMV では CTL 検査式を検査する際にモデルの到達可能状態数を出力させることができるため、レベル 4 では、1 人・時で検査可能な到達可能状態数を算出した。計算式を図 5-7 に示す。

1 人・時で検査可能な到達可能状態数 =

$$\frac{\text{作成したモデルの到達可能状態数}}{\text{上記(1)の総作業時間}}$$

図 5-7 1 人・時で検査可能な到達可能状態数

到達可能状態数については、SPIN 等の他のモデル検査器でも出力する機能を有しており、本項目で算出した数値は、他の事例との比較はできないが、同一の事例で、絞込みと抽象化の手法や範囲、度合いを合わせた上で他のモデル検査器を用いた場合であれば、比較対象とすることができる。

結果を表 5-17 に示す。本実験では初期モデルと改良モデルの 2 つのモデルを作成したが、SIL4 での作業で、説明力を強化したい品質を最終的に確認したのは改良モデルであるため、モデルの到達可能状態数は改良モデルのものを採用した。改良モデルの到達可能状態数は「5.1 モデル検査の適用結果」の表 5-3 を参照。

表 5-17 1 人・時で検査可能な到達可能状態数の算出

項目	値	単位
改良モデルの到達可能状態数(A)	102400	[状態]
総作業時間(B)	200.50	[人・時]
1 人・時で検査可能な到達可能状態数(A/B)	511	[状態／人・時]

1 人・時で検査可能な到達可能状態数は「511 状態／人・時」であった。

(4) モデル検査の適用プロセスの工程毎の作業コストの集計

モデル検査の適用プロセスの工程毎の作業時間を集計した。

工程毎の作業時間を表 5-18 に示す。

表 5-18　工程毎の作業時間（SIL4）

工程	合計[人・時]
実施計画策定	32.25
方針立案	44.25
絞込みと抽象化	14.50
モデル設計	19.00
モデル&検査式製作	20.25
妥当性検査	6.75
本検査	10.50
結果の解析	22.25
モデル検査の適用審査	30.75
合計	200.50

工程毎の作業時間の割合を円グラフで図 5-8 に示す。

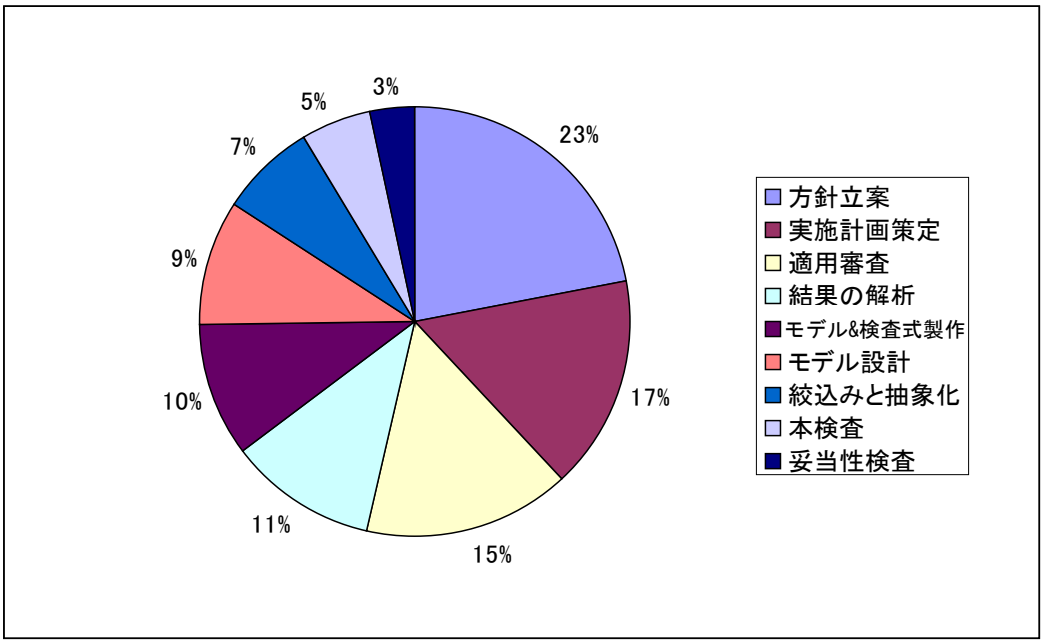


図 5-8　工程毎の作業時間の割合（SIL4）

図 5-8 の円グラフは割合の降順に並び替えを行った。

(5) 作業項目の割合の算出

「2.1　コストの計測」の表 2-1 に示した打合、検討、作業、実行の 4 つの作業項目の割合を 2 種類算出した。総作業時間内での割合と、モデル検査の適用プロセスの工程毎での割合である。

作業項目毎の作業時間を表 5-19 に示す。

表 5-19　作業項目毎の作業時間（SIL4）

作業項目	合計[人・時]
打合	44.50
検討	80.25
作業	70.00
実行	5.75
合計	200.50

総作業時間に占める 4 つの作業項目の割合を円グラフで図 5-9 に示す。

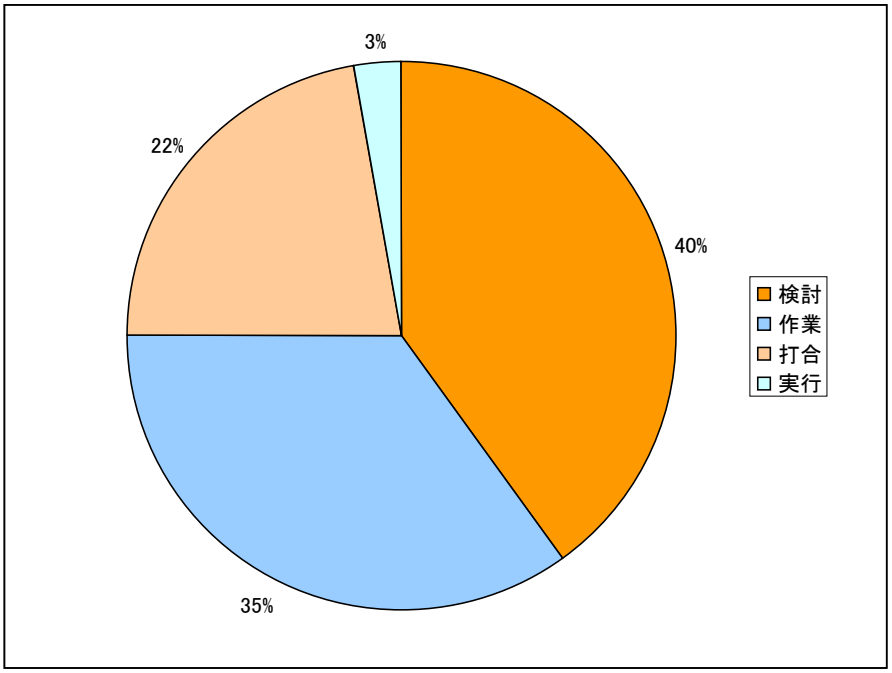


図 5-9　総作業時間に占める 4 つの作業項目の割合（SIL4）

図 5-9 の円グラフは割合の降順に並び替えを行った。

作業項目毎かつ適用プロセスの工程毎の作業割合を表 5-20 に示す。

表 5-20　作業項目毎かつ適用プロセスの工程毎の作業割合（SIL4）

工程	打合	検討	作業	実行	合計[%]
適用審査	19.5	9.8	70.7	0.0	100.0
結果の解析	0.0	93.3	4.5	2.2	100.0
本検査	4.8	33.3	40.5	21.4	100.0
妥当性検査	0.0	14.8	55.6	29.6	100.0
モデル&検査式製作	13.6	19.8	61.7	4.9	100.0
モデル設計	5.3	32.9	61.8	0.0	100.0
絞込みと抽象化	10.3	74.1	15.5	0.0	100.0
方針立案	44.6	39.5	15.8	0.0	100.0
実施計画策定	40.3	41.9	17.8	0.0	100.0

適用プロセスの工程毎に占める 4 つの作業項目の割合を 100%積み上げ方式の棒グラフで図 5-10 に示す。

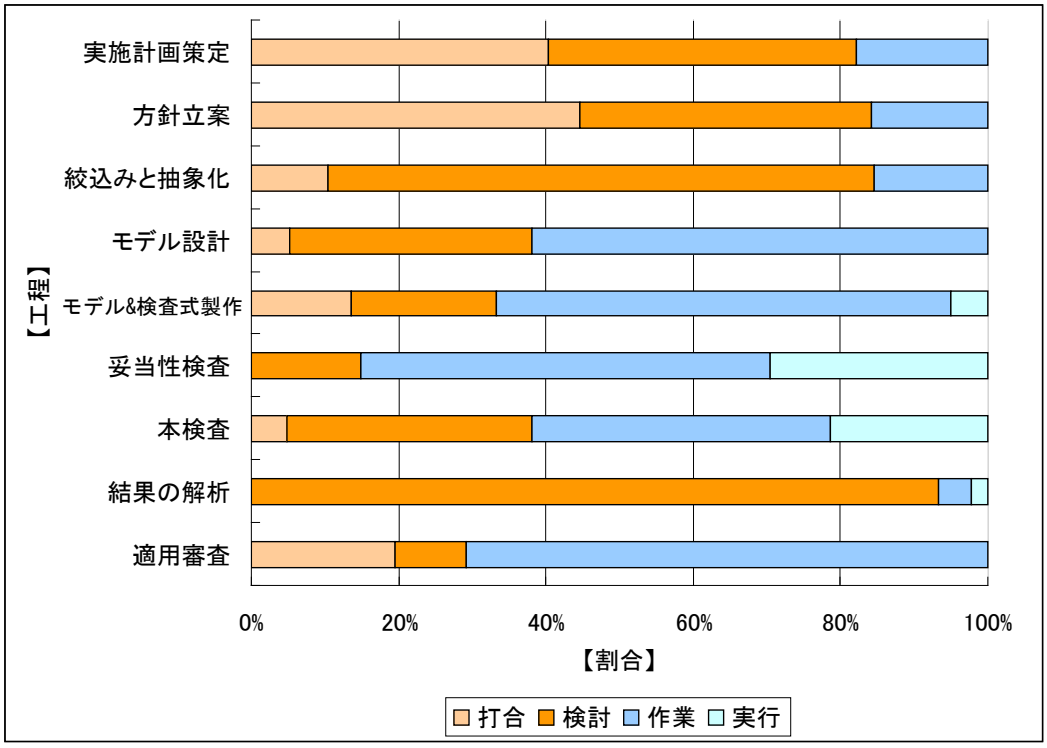


図 5-10　適用プロセスの工程毎に占める 4 つの作業項目の割合（SIL4）

(6) 指摘事項の 1 件当たりの作業コストの算出

モデル検査の適用によって発見した指摘事項の 1 件当たりの作業時間を算出した。計算式を図 5-11 に示す。

$$\text{指摘事項 1 件当たりの作業コスト} = \frac{\text{上記(1)の総作業時間}}{\text{発見した指摘事項の件数}}$$

図 5-11　指摘事項の 1 件当たりの作業コスト

結果を表 5-21 に示す。

表 5-21　指摘事項の 1 件当たりの作業コストの算出

項目	値	単位
総作業時間(A)	200.50	[人・時]
指摘事項の件数(B)	3	[件]
1 人・時で検査可能な到達可能状態数(A/B)	67	[人・時／件]

指摘事項の 1 件当たりの作業コストは「67 人・時／件」であった。

5.4. 実験に対する考察

本模擬実験で得られたモデル検査の結果と種々のコストに対して、模擬的な独立検証機関として実験を実施した立場から考察する。

(1) 総作業コストと設計書の頁当たりの作業コスト

安全度水準レベル 3（SIL3）における総作業コストは「147.75 人・時」であり、設計書の頁当たりの作業コストは「2.84 人・時／頁」であった。また、安全度水準レベル 4（SIL4）における総作業コストは「200.50 人・時」であり、適用に必要な資料の頁当たりの作業コストは「3.65 人・時／頁」であった。

本実験で検査対象とした「配電自動化システム」は、我が国の生活基盤である電力を安定供給するシステムであり、社会インフラの中枢を成すものである。それ故に、機能安全規格のレベル 3 あるいはレベル 4 といった高いレベルの安全度水準が求められている。

また、大規模かつ長期的な設備投資を必要とする配電システムの開発期間は、数ヶ月から規模によっては数年に及ぶこともある。これらのことを考慮すると、総作業コストについては、同システムの開発期間内（開発総コスト）で検証にかけるコストとしては妥当性があると考えられる。

また、発電システムや配電システム等の社会インフラ系のシステムでは、発注者や一次受け企業、二次受け企業、三次受け企業、場合によっては官公庁の立場など、多くのステークホルダー、技術者がシステム開発に関与し、仕様書のレビューや、システムの検証には多大な人員が必要とされる。特に上位仕様書の場合は、高々1 頁の記載に対して数人～十数人の技術者が一日分の作業コストをかけることも珍しくない。したがって、頁当たりの作業コストについても、2.84 人・時／頁と 3.65 人・時／頁という数値は充分に妥当である。

(2) モデルの 1 行当たりの作業コスト（SIL3）

作成したモデルの 1 行当たりの作業コストは「0.54 人・時／行」であった。

モデル記述言語を用いた形式仕様記述では自然言語による仕様書に潜む「曖昧さ」や「場違いな詳細過ぎる記述」等を排除して、当該仕様書に適切な抽象度で極力小さなモデルで仕様を表現することが望ましい。本実験で作成したモデルの行数は「276 行」であり、安全度水準レベル 4（SIL4）に対応した形式検証では、同じモデルで安全性の保証、指摘事項の発見ができている。したがって、本実験の安全度水準レベル 3（SIL3）に対応した形式仕様記述作業で作成したモデルは、抽象度と規模の面において適切であったと考えられる。

(3) 1 人・時で検査可能な到達可能状態数（SIL4）

1 人・時で検査可能な到達可能状態数は「511 状態／人・時」であった。これは到達可能状態数を総作業時間で除した理論的な数値である。モデル検査では個々の CTL 検査式に対して、それぞれ全数探索を行うため、本実験で検査した延べ状態数は以下の式で表される。

検査した延べ状態数 = モデルの到達可能状態数 102400×検査式の数 31 = 3174400

1 人・時で検査可能な「延べ」到達可能状態数は、15841（511*31）状態／人・時ということができる。モデル検査による全数探索と人間の視認による網羅的な検査との比較には賛否両論あるが、ここであえて比較すると、300 万を超える状態を 200 時間以上（総作業時間）にわたって継続的に視認することは作業者の集中力の持続可能性の点で非現実的であり、たとえ 1 時間だけであっても 15000 以上もの状態を人間が視認することは非常に難しいと考えられる。

本事例は、モデル作成の際の絞込みと抽象化が効果的に作用し、比較的小さなモデルを作成することができた。過去の事例の中には、モデルの到達可能状態数が数億状態、数十億状態となったものもある。

以上のことから、システムの検査方法としてモデル検査を採用することは、数多くある検査手法の 1 つの選択肢として妥当性があると言える。

(4) モデル検査の適用プロセスの工程毎の作業コスト

ここでは「5.2　安全度水準レベル 3（SIL3）の場合のコスト評価」の図 5-3 と、「5.3 安全度水準レベル 4（SIL4）の場合のコスト評価」の図 5-8 より考察する。図 5-3 と図 5-8 において、モデル検査の適用プロセスの工程のうち、V 字のそれぞれの頂点（上流側）の 2 つの工程に着目する。着目する工程は実施計画策定、方針立案、結果の解析（SIL4 のみ）、適用審査である。これらの工程の作業コストが全体に占める割合を表 5-22 と表 5-23 に示す。

表より、安全度水準レベル 3（SIL3）では全体の 65%、安全度水準レベル 4（SIL4）では全体の 66%を、適用プロセスの上流工程に要していることがわかる。システムの品質を確保・向上するための取組みとして、ソフトウェアの開発プロセスでは上流工程に重点を置いて、そこでの作業を確実かつ充分に実施することが重要である。このことは、システムの品質に大きな影響を与える検証プロセスでも同様である。

モデル検査の適用にあたっても、実施計画と検査方針の立案、その妥当性を確認する結果の解析と適用審査が重要なプロセスであり、独立検証機関には、これを確実かつ充分に実施できる技術と経験、知識とノウハウが求められる。

表 5-22　上流工程の作業コストが全体に占める割合（SIL3）

工程	割合[%]
モデル検査の実施計画策定	22
検査の方針立案	29
モデル検査の適用審査	14
合計	65

表 5-23　上流工程の作業コストが全体に占める割合（SIL4）

工程	割合[%]
モデル検査の実施計画策定	17
検査の方針立案	23
検査結果の解析	11
モデル検査の適用審査	15
合計	66

(5) 作業項目の割合

ここでは「5.2　安全度水準レベル 3 (SIL3) の場合のコスト評価」の図 5-4 及び図 5-5 と、「5.3　安全度水準レベル 4（SIL4）の場合のコスト評価」の図 5-9 及び図 5-10 より考察する。

上記(4)で、モデル検査の適用にあたっては適用プロセスの上流工程の作業が重要であることがわかった。一般に、ソフトウェアの開発プロセスや検証プロセスの上流工程においては依頼者からの要求獲得や、合議による合意形成、そのための社内検討が主たる作業となる。この点に着目して、図 5-4 と図 5-9 より、本実験で分類した 4 つの作業項目のうち、適用依頼者との打合せと、独立検証機関内での検討作業が全体に占める割合をまとめると、表 5-24 と表 5-25 のようになる。同じく、図 5-5 と図 5-10 より、モデル検査の適用プロセスの上流工程の作業における打合と検討の割合をまとめて表 5-26 と表 5-27 に示す。

表 5-24 と表 5-25 より、打合と検討の作業全体に占める割合は、安全度水準レベル 3（SIL3）とレベル 4（SIL4）共に 62%である。また、表 5-26 と表 5-27 より、適用プロセスの上流工程の作業における打合と検討の割合は両レベルとも、適用審査以外では 80%を超えていることがわかる。なお、適用審査では依頼者による審査を受けるための報告書の作成作業の割合が高いため、打合と検討の割合が 20%代となっている。

これらのことから、独立検証機関には、モデル検査の適用にあたって依頼者からの要求獲得や合意形成、社内での充分な調査・検討を実施する能力が求められる。

表 5-24　打合と検討が全体に占める割合（SIL3）

作業項目	割合[%]
打合	27
検討	35
合計	62

表 5-25　打合と検討が全体に占める割合（SIL4）

作業項目	割合[%]
打合	22
検討	40
合計	62

表 5-26　上流工程の作業における打合と検討の割合（SIL3）

工程	打合と検討の割合[%]
モデル検査の実施計画策定	82.2
検査の方針立案	84.1
モデル検査の適用審査	29.3

表 5-27　上流工程の作業における打合と検討の割合（SIL4）

工程	打合と検討の割合[%]
モデル検査の実施計画策定	82.2
検査の方針立案	84.1
検査結果の解析	93.3
モデル検査の適用審査	29.3

(6) 指摘事項の 1 件当たりの作業コスト（SIL4）

指摘事項の 1 件当たりの作業コストは「67 人・時／件」であった。本数値については、数値自体を他の事例や他の手法と比較して、その大小を議論することは有意義ではないと考えられる。ソフトウェアの不具合やシステム全体の障害に関わる指摘事項は、その「量」だけでなく「質」も考慮することが重要だからである。

モデル検査では、システムが取り得る全ての状態とパスを網羅的に検査するため、極めて特別な状態や状況で発生する不具合や予期せぬ動作を発見することができる。本実験では題材を提供して頂いた企業内で充分に設計とレビューを実施した設計書にモデル検査を適用したが、設計者とレビューアが予期できなかった指摘事項を 3 件発見することができた。

検証対象の配電自動化システムでは、機能安全規格のレベル 3 あるいはレベル 4 の非常に高いレベルの安全度水準が求められるシステムであり、単位時間あたりの危険側故障確率（1/hour）は、SIL3 で「10^{-8}以上 10^{-7}未満」、SIL4 で「10^{-9}以上 10^{-8}未満」が求められている。その故障確率を達成するためには、稀な状況で発生する危険側故障であっても、発見・対策を行うことが重要である。

67 人・時／件は非現実的な数値ではなく、実現可能な妥当な値であると考えられ、モデル検査の適用は、システム全体の危険側故障確率の削減に大きく寄与したものと考えられる。

(7) 説明力を強化したい品質

本実験で説明力を強化したい品質を表 5-28 に示す。安全性 1 と安全性 2 に関するモデル検査による検査結果は「5.1　モデル検査の適用結果」を参照。

表 5-28　説明力を強化したい品質

品質	内容
安全性 1	ソフトウェアを含めたシステムがフリーズしないこと。
安全性 2	予期せぬ動作により本システム自体が原因となって電気事故が発生し停電とならないこと。

安全性 1 については、モデル検査の適用プロセスの「モデルの妥当性検査」によって確認が可能であり、実験では安全性 1 に関する全ての CTL 検査式で検査結果が「TRUE」となったため、安全度水準レベル 3（SIL3）とレベル 4（SIL4）共に全数探索によって保証することができた。

安全性 2 については、適用プロセスの「本検査」すなわち形式検証によって確認が可能である。したがって、形式検証を実施していない安全度水準レベル 3（SIL3）では、

全数探索による保証はできないが、形式仕様記述によって仕様を「formal」に記述することで、安全性を確保でき得る充分な設計が実施されたことを保証することができる。

一方、安全度水準レベル 4（SIL4）では、安全性 2 に関する全ての CTL 検査式で検査結果が「TRUE」となったため、全数探索によって当該安全性を保証することができた。

6. まとめ

本実験では配電自動化システムにモデル検査を適用し、「実験の位置付け」で説明したような検証業務を想定した場合、独立検証機関の参画の許容性についてコスト評価を行った。

実験結果からの考察によって以下の 5 つのコストについて妥当性を確認した。

・「総作業コスト」
・「頁当たりの作業コスト」
・「モデルの 1 行当たりの作業コスト」
・「1 人・時で検査可能な到達可能状態数」
・「指摘事項の 1 件当たりの作業コスト」

「モデル検査の適用プロセスの工程毎の作業コスト」を評価した結果、モデル検査の適用にあたっては適用プロセスの上流工程である以下の 4 つ工程が重要であることがわかった。

・モデル検査の実施計画策定
・検査の方針立案
・検査結果の解析
・モデル検査の適用審査

独立検証機関には、これらの工程を確実かつ充分に実施できる技術と経験、知識とノウハウが求められる。

「作業項目の割合」の評価では、モデル検査の適用プロセスの上流工程においては、適用依頼者との打合せと独立検証機関内での検討作業が 80%以上を占めることがわかった。したがって独立検証機関には、モデル検査の適用にあたって依頼者からの要求獲得や合意形成、社内での充分な調査・検討を実施する能力が求められる。

「説明力を強化したい品質」の保証度の評価では、安全性 1 は、安全度水準レベル 3（SIL3）とレベル 4（SIL4）共に全数探索によって保証することができた。安全性 2 は、安全度水準レベル 3（SIL3）では形式仕様記述による充分な設計で保証できることがわかった。安全度水準レベル 4（SIL4）では、全数探索によって当該安全性を保証することができた。

本実験によって形式手法を用いた第三者検証は、産業界がソフトウエア品質説明力を強化する上で、「独立検証機関の監査や審査への参画の許容性」の範囲内であり、充分に実現可能性があることがわかった。

7. 用語集

用語	用語意味
安全性（モデル検査）	起こるべきではないことが起こらないこと。
入／切指令	開閉器の状態を入あるいは切の状態にするための指令
遠制	遠隔制御の略である。
片電圧有	開閉器を挟んで片側だけに電圧が有る状態
偽反例	元のシステムでは存在しない状態やパスを含む反例。モデルの間違いによって出力される場合が多く、システムの不具合ではない。
時相論理式	いつかPになる、ずっとPである等の時間に関する問題を表現する論理式である。多くのモデル検査器で検査式として用いられる。
状態爆発	モデル検査の課題である。モデルの取り得る状態数が大きくなり過ぎて、計算機のメモリ不足に陥ること、あるいは現実的な時間で検査結果が得られなくなること。
電気事故	電気に関するシステム（設備や機器）の故障や不具合あるいは誤操作によって発生する事故。
到達可能状態数	モデル検査で、モデル全体の状態遷移系の状態のうち、初期状態から到達可能な状態の数。
配電（事業）	発電所で発電した電力を送電網、変電所を経由して需要家（一般家庭、工場等）に供給するため、配電網システムの構築とその運用を行うこと。
反例	モデル検査器で検査結果がFALSEの場合の証拠。状態遷移系の初期状態から検査式を満たさない状態までのパス。 CounterExample。
パス	状態遷移図において、状態と状態とを結ぶ経路。
モデル検査	初期状態がsのモデルMと時相論理式pがあるとき、M, s |= pが成り立つか否かを、モデルMが取り得る全状態空間を探索することによって検査すること。
モデル検査器	計算機上でモデル検査を全自動で実行するソフトウェアツール。 検査結果がFALSEの場合は反例(counter example)を出力する。
理論状態数	モデル検査で、モデルの変数毎の取り得る状態数を全て掛け合わせた数。

用語	用語意味
Alloy	モデル検査器の一種。米 MIT（マサチューセッツ工科大学）で開発された。複数の反例を状態遷移系の形式で視覚的に出力可能である。
BDD	Binary Decision Diagram の略。二分決定グラフと呼ばれる。状態遷移系を効率的に実装／演算／管理することができるデータ構造。
CadenceSMV	SMV 系のモデル検査器。米 Cadence 社（ケーデンス社）によって開発された。研究と教育でのみ利用可能で企業での商用利用は禁止されている。
CMU-SMV	SMV 系のモデル検査器。米 CMU（カーネギーメロン大学）によって開発された。SMV 系の中では最も古い。
CTL	Computation Tree Logic の略。分岐時相論理。モデル検査器 SMV で主として使われる検査式。
LTL	Linear Temporal Logic の略。線形時相論理。
NuSMV	SMV 系のモデル検査器。イタリアの大学と研究機関によって CMU-SMV を拡張して開発された。オープンソフトウェアである。
Promela	Protocol meta languageの略。モデル検査器SPINのモデル記述言語。 一般に「プロメラ」と呼ばれている。
SMV	Symbolic Model Verifier の略。モデル検査器の一種。 一般に「エス・エム・ブイ」と呼ばれている。
SMV 言語	モデル検査器 SMV におけるモデル記述言語。公式な名称ではなく一般的な呼称である。
SMV ファイル	SMV 言語で記述したモデルと、CTL 式で記述した検査式を１つにまとめたファイル。公式な名称ではなく一般的な呼称である。
SPIN	Simple Promela INterpreterの略。モデル検査器の一種。 一般に「スピン」と呼ばれている。
UPPAAL	モデル検査器の一種。スウェーデンのUppsala(ウプサラ)大学とデンマークのAalborg(オルボー)大学とが開発した。一般に「ウパール」と呼ばれている。

添付資料

実験で作成されたデータ等の資料

【目次】

1. モデル検査の適用で作成した資料

(1) モデルの詳細設計

本実験では、モデル検査の適用にあたって、モデルの詳細設計として図 1-1 と図 1-2 に示すような状態遷移図を作成した。

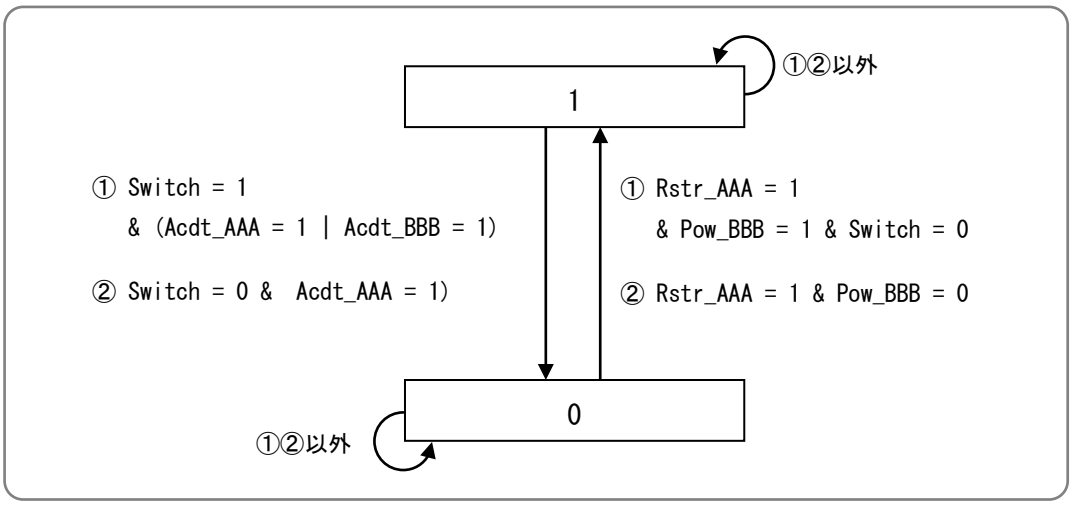


図 1-1　A 変電所側電源の状態遷移図

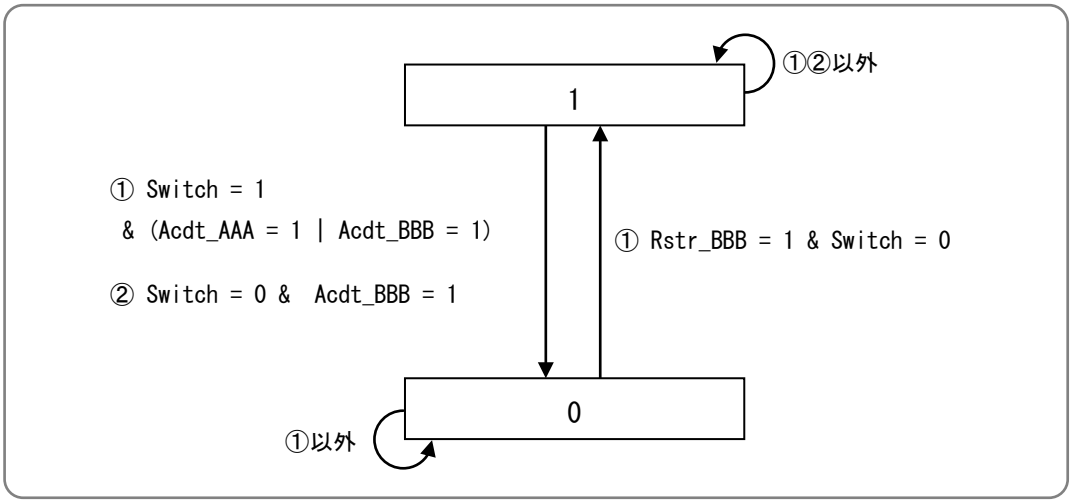


図 1-2　B 変電所側電源の状態遷移図

(2) 作成したモデル

実験で作成したモデルの一部を図 1-3 と図 1-4 に示す。図 1-1 と図 1-2 の状態遷移図から作成したモデルである。

```
--/*****************************************************************************/
--/**                                                                         **/
--/** ----------------------------------------------------------------------- **/
--/**     モデル名      : 配電自動化システム設計書解析モデル                  **/
--/**     検査概要      : 詳細設計の精度向上                                  **/
--/**     改訂          : 初版                                                **/
--/** ----------------------------------------------------------------------- **/
--/**     検査対象言語  : 自然言語(日本語)＋状態遷移図                        **/
--/**     ファイル名    : Pow_dac_Sys1.smv                                    **/
--/**     担当          : **********************************                **/
--/** ----------------------------------------------------------------------- **/
--/**                                                                         **/
--/*****************************************************************************/

--/*****************************************************************************/
--/*                                                                           */
--/*      MODULE「main」                                                       */
--/*                                                                           */
--/*****************************************************************************/

MODULE main

--/*****************************************************************************/
--/*      DEFINE 定義 | 書式  AAA := XXX; |                                   */
--/*****************************************************************************/

DEFINE

--/*****************************************************************************/
--/*      変数宣言(VAR) | 書式  AAA : 変数の型; |                             */
--/*****************************************************************************/

  -- A 変電所側電源 --
  Pow_AAA : 0..1;                                    -- 1:入   0:切 --

  -- B 変電所側電源 --
  Pow_BBB : 0..1;                                    -- 1:入   0:切 --

   ●
   ●
   ●
   ●
   ●
   ●
```

図 1-3　実験で作成したモデル（抜粋）(1/2)

```
--/*************************************************************************/
--/*      状態遷移記述(ASSIGN)                                              */
--/*************************************************************************/

ASSIGN

--/*********************************************************************/
--/*      初期化(init) | 書式  init(AAA) := 値; |                      */
--/*********************************************************************/

  -- A 変電所側電源(初期値 = 1:入) --
  init(Pow_AAA) := 1;

  -- B 変電所側電源(初期値 = 0:切) --
  init(Pow_BBB) := 0;

      ●
      ●
      ●
      ●
      ●
      ●

--/*********************************************************************/
--/*      状態遷移(next) | 書式  next(AAA) := case |                   */
--/*                     |         条件 : 値;      |                   */
--/*                     |         TRUE : 値;      |                   */
--/*                     |       esac;             |                   */
--/*********************************************************************/

  -- A 変電所側電源 --
  next(Pow_AAA) := case
    Pow_AAA = 0 & Switch = 0 & Rstr_AAA = 1 & Pow_BBB = 1    : 1;
    Pow_AAA = 0              & Rstr_AAA = 1 & Pow_BBB = 0    : 1;
    Pow_AAA = 1 & Switch = 1 & (Acdt_AAA = 1 | Acdt_BBB = 1) : 0;
    Pow_AAA = 1 & Switch = 0 & Acdt_AAA = 1                  : 0;
    TRUE : Pow_AAA;
  esac;

  -- B 変電所側電源 --
  next(Pow_BBB) := case
    Pow_BBB = 0 & Switch = 0 & Rstr_BBB = 1                  : 1;
    Pow_BBB = 1 & Switch = 1 & (Acdt_AAA = 1 | Acdt_BBB = 1) : 0;
    Pow_BBB = 1 & Switch = 0 & Acdt_BBB = 1                  : 0;
    TRUE : Pow_BBB;
  esac;

      ●
      ●
      ●
      ●
      ●
      ●
```

図 1-4　実験で作成したモデル（抜粋）(2/2)

(3) 作成した CTL 検査式

実験で作成した CTL 検査式の一部を図 1-5 に示す。

```
--/*****************************************************************************/
--/**                                                                         **/
--/** ----------------------------------------------------------------------- **/
--/**     名称 : 配電自動化システム設計書解析モデルの検査(CTL)式一覧          **/
--/** ----------------------------------------------------------------------- **/
--/**     ファイル名    : Pow_dac_Sys.ctl                                     **/
--/**     担当          : **********************************                **/
--/** ----------------------------------------------------------------------- **/
--/**                                                                         **/
--/*****************************************************************************/

        ●
        ●
        ●
        ●
        ●
        ●

--/*****************************************************************************/
--/**  モデル検査報告書「各状態からの脱出(他状態への遷移)可能性の検査」      **/
--/*****************************************************************************/

-- 状態 01 --
   -- 公平性制約 --
   FAIRNESS Rstr_AAA = 1
   FAIRNESS Rstr_BBB = 1
   -- 検査式 --
   SPEC !EF(EG(CTRL =  1))

-- 状態 02 --
   -- 公平性制約 --
   FAIRNESS ((Oprt = Rmt_Off                & On_Tmr = 0)
          | ((Oprt = Rmt_On | Oprt = Man_On) & On_Tmr = 0)
          | ( Oprt = AB_Chg                 & On_Tmr = 0))
   -- 検査式 --
   SPEC !EF(EG(CTRL =  2))

-- 状態 03 --
   -- 公平性制約 --
   FAIRNESS (Oprt = Rmt_Off & Both_Tmr = 0)
   -- 検査式 --
   SPEC !EF(EG(CTRL =  3))

        ●
        ●
        ●
        ●
        ●
        ●
```

図 1-5　実験で作成した CTL 検査式（抜粋）

(4) 反例

実験においてモデル検査器 NuSMV から出力された反例を図 1-6～図 1-9 に示す。図 1-6 は検査結果が「TRUE」の場合である。図 1-7～図 1-9 は検査結果が「FALSE」の場合である。「specification」は、検査した CTL 検査式である。

```
*** This is NuSMV 2.5.4 (compiled on Fri Oct 28 14:13:29 UTC 2011)
*** Enabled addons are: compass
*** For more information on NuSMV see <http://nusmv.fbk.eu>
*** or email to <nusmv-users@list.fbk.eu>.
*** Please report bugs to <nusmv-users@fbk.eu>

*** Copyright (c) 2010, Fondazione Bruno Kessler

*** This version of NuSMV is linked to the CUDD library version 2.4.1
*** Copyright (c) 1995-2004, Regents of the University of Colorado

*** This version of NuSMV is linked to the MiniSat SAT solver.
*** See http://www.cs.chalmers.se/Cs/Research/FormalMethods/MiniSat
*** Copyright (c) 2003-2005, Niklas Een, Niklas Sorensson

-- specification EF CTRL = 1  is true
-- specification EF CTRL = 2  is true
-- specification EF CTRL = 3  is true
-- specification EF CTRL = 4  is true
-- specification EF CTRL = 5  is true
-- specification EF CTRL = 6  is true
-- specification EF CTRL = 7  is true
-- specification EF CTRL = 8  is true
-- specification EF CTRL = 9  is true
-- specification EF CTRL = 10  is true
-- specification EF CTRL = 11  is true
-- specification EF CTRL = 12  is true
-- specification EF CTRL = 13  is true
```

図 1-6　NuSMV より出力された反例（抜粋）(1/4)

```
        ⋮

-- specification !E [ !(CTRL = 12) U ((Pow_AAA = 1 & Pow_BBB = 1) & Switch = 1) ]   is false
-- as demonstrated by the following execution sequence
Trace Description: CTL Counterexample
Trace Type: Counterexample
-> State: 1.1 <-
  CTRL = 1
  Switch = 0
  Pow_AAA = 1
  Pow_BBB = 0
  Oprt = Emp
  AB_Flg = 0
  Acdt_AAA = 0
  Acdt_BBB = 0
  Rstr_AAA = 1
  Rstr_BBB = 0
  Emp_Tmr = 0
  On_Tmr = 0
  Both_Tmr = 0
  PT_Emp = FALSE
  PT_BBB = FALSE
  PT_AAA = TRUE
  PT_Both = FALSE
-> State: 1.2 <-
  CTRL = 2
  Oprt = Rmt_On
  Rstr_AAA = 0
  Rstr_BBB = 1
-> State: 1.3 <-
  CTRL = 3
  Switch = 1
  Pow_BBB = 1
  Oprt = Emp
  Rstr_BBB = 0
  PT_AAA = FALSE
  PT_Both = TRUE
```

図 1-7　NuSMV より出力された反例（抜粋）(2/4)

```
-- specification !(EF (CTRL = 12 & PT_AAA = TRUE))  is false
-- as demonstrated by the following execution sequence
Trace Description: CTL Counterexample
Trace Type: Counterexample
-> State: 1.1 <-
  CTRL = 1
  Switch = 0
  Pow_AAA = 1
  Pow_BBB = 0
  Oprt = Emp
  AB_Flg = 0
  Acdt_AAA = 0
  Acdt_BBB = 0
  Rstr_AAA = 1
  Rstr_BBB = 0
  Emp_Tmr = 0
  On_Tmr = 0
  Both_Tmr = 0
  PT_Emp = FALSE
  PT_BBB = FALSE
  PT_AAA = TRUE
  PT_Both = FALSE
-> State: 1.2 <-
  CTRL = 2
  Oprt = AB_Chg
  Rstr_AAA = 0
  Rstr_BBB = 1
-> State: 1.3 <-
  CTRL = 11
  Pow_BBB = 1
  AB_Flg = 1
  Acdt_BBB = 1
  Rstr_BBB = 0
  PT_AAA = FALSE
  PT_Both = TRUE
-> State: 1.4 <-
  CTRL = 12
  Pow_BBB = 0
  Oprt = Emp
  AB_Flg = 0
  Acdt_BBB = 0
  PT_AAA = TRUE
  PT_Both = FALSE
```

図 1-8　NuSMV より出力された反例（抜粋）(3/4)

```
  ⋮

-- specification !(EF (CTRL = 12 & PT_BBB = TRUE))  is false
-- as demonstrated by the following execution sequence
Trace Description: CTL Counterexample
Trace Type: Counterexample
-> State: 1.1 <-
  CTRL = 1
  Switch = 0
  Pow_AAA = 1
  Pow_BBB = 0
  Oprt = Emp
  AB_Flg = 0
  Acdt_AAA = 0
  Acdt_BBB = 0
  Rstr_AAA = 1
  Rstr_BBB = 0
  Emp_Tmr = 0
  On_Tmr = 0
  Both_Tmr = 0
  PT_Emp = FALSE
  PT_BBB = FALSE
  PT_AAA = TRUE
  PT_Both = FALSE
-> State: 1.2 <-
  CTRL = 2
  Oprt = AB_Chg
  Rstr_AAA = 0
  Rstr_BBB = 1
-> State: 1.3 <-
  CTRL = 11
  Pow_BBB = 1
  Oprt = Rmt_On
  AB_Flg = 1
  Acdt_BBB = 1
  Rstr_BBB = 0
  PT_AAA = FALSE
  PT_Both = TRUE
-> State: 1.4 <-
  CTRL = 12
  Pow_BBB = 0
  Oprt = Emp
  Acdt_BBB = 0
  PT_BBB = TRUE
  PT_Both = FALSE
```

図 1-9　NuSMV より出力された反例（抜粋）(4/4)

2. 実験データシート

ここでは、本実験でモデル検査の適用プロセスの工程毎かつ作業項目毎に作業時間を記入した実験データシートを添付する。

図 2-1 は実験データシートのフォーマットである。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第		[日目]
作業者			

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
☐ モデル検査の実施計画策定					0
☐ 検査の方針立案	0	0	0	0	0
・ 検査全体の方針立案					0
・ モデル化の方針立案					0
・ 検査項目の方針立案					0
☐ 検査対象の絞込みと抽象化	0	0	0	0	0
・ 絞込み					0
・ 抽象化					0
☐ モデル設計					0
☐ モデルと検査式の製作	0	0	0	0	0
・ モデルの製作					0
・ 検査式の製作					0
☐ モデルの妥当性検査					0
☐ 本検査					0
☐ 検査結果の解析					0
☐ モデル検査の適用審査					0
合計	0	0	0	0	0

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

図 2-1　実験データシートのフォーマット

薄黄色のセルは実験データを記入するセルである。灰色のセルは自動計算により合計値が算出され結果が入力されるセルである。

モデル検査器の適用プロセスを図 2-2 に示す。

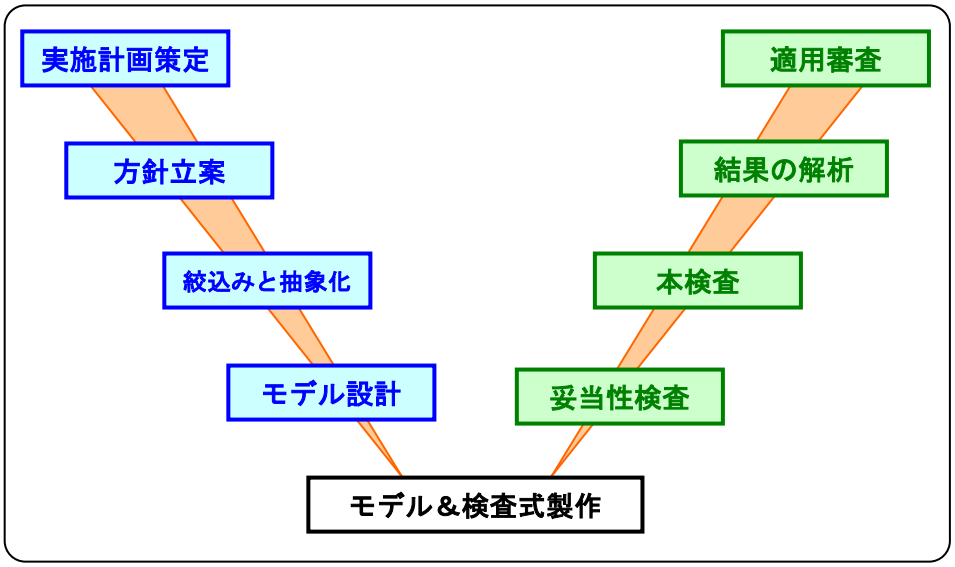


図 2-2　モデル検査器の適用プロセス

モデル検査の適用プロセスの各工程の略称と正式名称を表 2-1 に示す。

表 2-1　各工程の略称と正式名称

NO	略称	正式名称
1	実施計画策定	モデル検査の実施計画策定
2	方針立案	検査の方針立案 □検査全体の方針立案 □モデル化の方針立案 □検査項目の方針立案
3	絞込みと抽象化	検査対象の絞込みと抽象化
4	モデル設計	モデル設計
5	モデル&検査式製作	モデルと検査式の製作
6	妥当性検査	モデルの妥当性検査
7	本検査	本検査
8	結果の解析	検査結果の解析
9	適用審査	モデル検査の適用審査

モデル検査の適用プロセスの詳細は、「模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価　実験報告書」の「4．モデル検査の適用プロセス」を参照頂きたい。

また、実験データシートの作業項目の一覧を表 2-2 に示す。

表 2-2　実験データシートの作業項目

作業項目	内容
打合	適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。 打合せ用の資料作成時間、メール又は電話による相談時間等も含むものとする。
検討	独立検証機関内での検討時間又は技術調査の時間、モデル設計時間等を計上する。
作業	コーディング、報告書の記載等の直接的な作業時間を計上する。 テストモデルの作成、動作確認も含むものとする。
実行	モデル検査器 NuSMV の実行と結果出力までの待ち時間を計上する。

時間の計測及び記入は 0.25 時間（15 分）刻みとした。また、当日の工程で、前工程の手戻り作業が発生した場合は、手戻りの作業時間についても当日の作業時間として計上することとした。

以下、実験で記入したシートを添付する。シートは実験を開始した第 1 日目から第 45 日目までの 45 シートである。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	1	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定	4.25				4.25
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	4.25	0.00	0.00	0.00	4.25

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	2	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
☐ モデル検査の実施計画策定	4.25				4.25
☐ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
☐ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
☐ モデル設計					0.00
☐ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
☐ モデルの妥当性検査					0.00
☐ 本検査					0.00
☐ 検査結果の解析					0.00
☐ モデル検査の適用審査					0.00
合計	4.25	0.00	0.00	0.00	4.25

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	3	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定		5.00			5.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	5.00	0.00	0.00	5.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	4	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
☐ モデル検査の実施計画策定	1.00	2.75	0.75		4.50
☐ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
☐ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
☐ モデル設計					0.00
☐ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
☐ モデルの妥当性検査					0.00
☐ 本検査					0.00
☐ 検査結果の解析					0.00
☐ モデル検査の適用審査					0.00
合計	1.00	2.75	0.75	0.00	4.50

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	5	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定		2.00	2.00		4.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	2.00	2.00	0.00	4.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	6	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
☐ モデル検査の実施計画策定	3.50	1.25	1.00		5.75
☐ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
☐ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
☐ モデル設計					0.00
☐ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
☐ モデルの妥当性検査					0.00
☐ 本検査					0.00
☐ 検査結果の解析					0.00
☐ モデル検査の適用審査					0.00
合計	3.50	1.25	1.00	0.00	5.75

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	7	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
☐ モデル検査の実施計画策定		2.50	2.00		4.50
☐ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
☐ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
☐ モデル設計					0.00
☐ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
☐ モデルの妥当性検査					0.00
☐ 本検査					0.00
☐ 検査結果の解析					0.00
☐ モデル検査の適用審査					0.00
合計	0.00	2.50	2.00	0.00	4.50

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	8	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	2.00	0.00	0.00	2.00
・ 検査全体の方針立案		2.00			2.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	2.00	0.00	0.00	2.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	9	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	1.50	3.00	1.00	0.00	5.50
・ 検査全体の方針立案	1.50	3.00	1.00		5.50
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	1.50	3.00	1.00	0.00	5.50

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	10	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	4.50	0.00	2.25	0.00	6.75
・ 検査全体の方針立案	4.50		2.25		6.75
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	4.50	0.00	2.25	0.00	6.75

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	11	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	7.50	1.00	0.00	8.50
・ 検査全体の方針立案					0.00
・ モデル化の方針立案		7.50	1.00		8.50
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	7.50	1.00	0.00	8.50

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	12	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	1.75	0.50	1.50	0.00	3.75
・ 検査全体の方針立案					0.00
・ モデル化の方針立案	1.75	0.50	1.50		3.75
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	1.75	0.50	1.50	0.00	3.75

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	13	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	1.00	0.00	0.00	0.00	1.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案	1.00				1.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	1.00	0.00	0.00	0.00	1.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	14	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	1.50	0.00	0.00	0.00	1.50
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案	1.50				1.50
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	1.50	0.00	0.00	0.00	1.50

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	15	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.50	2.00	0.00	0.00	2.50
・ 検査全体の方針立案	0.50	1.00			1.50
・ モデル化の方針立案					0.00
・ 検査項目の方針立案		1.00			1.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.50	2.00	0.00	0.00	2.50

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	16	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.50	2.00	1.25	0.00	3.75
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案	0.50	2.00	1.25		3.75
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.50	2.00	1.25	0.00	3.75

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	17	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	2.00	0.75	0.00	2.75
・ 絞込み		1.00	0.50		1.50
・ 抽象化		1.00	0.25		1.25
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	2.00	0.75	0.00	2.75

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	18	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	1.50	6.50	0.00	0.00	8.00
・ 絞込み	1.00	2.25			3.25
・ 抽象化	0.50	4.25			4.75
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	1.50	6.50	0.00	0.00	8.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	19	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
☐ モデル検査の実施計画策定					0.00
☐ 検査の方針立案	4.75	0.00	0.00	0.00	4.75
・ 検査全体の方針立案	2.75				2.75
・ モデル化の方針立案	0.50				0.50
・ 検査項目の方針立案	1.50				1.50
☐ 検査対象の絞込みと抽象化	0.00	2.25	0.50	0.00	2.75
・ 絞込み		2.25	0.50		2.75
・ 抽象化					0.00
☐ モデル設計					0.00
☐ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
☐ モデルの妥当性検査					0.00
☐ 本検査					0.00
☐ 検査結果の解析					0.00
☐ モデル検査の適用審査					0.00
合計	4.75	2.25	0.50	0.00	7.50

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	20	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	1.00	0.00	1.00
・ 絞込み			0.50		0.50
・ 抽象化			0.50		0.50
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	0.00	1.00	0.00	1.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	21	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計		2.00	3.25		5.25
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	2.00	3.25	0.00	5.25

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	22	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計	1.00	2.25	1.00		4.25
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	1.00	2.25	1.00	0.00	4.25

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	23	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
☐ モデル検査の実施計画策定					0.00
☐ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
☐ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
☐ モデル設計			6.00		6.00
☐ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
☐ モデルの妥当性検査					0.00
☐ 本検査					0.00
☐ 検査結果の解析					0.00
☐ モデル検査の適用審査					0.00
合計	0.00	0.00	6.00	0.00	6.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	24	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	4.50	0.00	4.50
・ モデルの製作			4.50		4.50
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	0.00	4.50	0.00	4.50

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	25	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	3.50	0.50	4.00
・ モデルの製作			3.50	0.50	4.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	0.00	3.50	0.50	4.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	26	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	1.75	1.50	1.00	0.00	4.25
・ モデルの製作					0.00
・ 検査式の製作	1.75	1.50	1.00		4.25
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	1.75	1.50	1.00	0.00	4.25

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	27	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.75	0.00	0.00	0.00	0.75
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案	0.75				0.75
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	1.00	0.50	0.00	0.00	1.50
・ モデルの製作					0.00
・ 検査式の製作	1.00	0.50			1.50
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	1.75	0.50	0.00	0.00	2.25

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	28	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	3.00	0.00	0.00	0.00	3.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案	3.00				3.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	2.00	0.00	2.00
・ モデルの製作					0.00
・ 検査式の製作			2.00		2.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	3.00	0.00	2.00	0.00	5.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	29	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査		1.00	2.75	1.00	4.75
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	1.00	2.75	1.00	4.75

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	30	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.50	0.00	0.00	0.50
・ 検査全体の方針立案					0.00
・ モデル化の方針立案		0.50			0.50
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計		1.50	1.00		2.50
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	2.00	1.00	0.00	3.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	31	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査			1.00	1.00	2.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	0.00	1.00	1.00	2.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	32	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査		0.50	2.25	0.50	3.25
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	0.50	2.25	0.50	3.25

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	33	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査		2.00	0.50	0.25	2.75
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	2.00	0.50	0.25	2.75

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	34	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	1.00	0.50	0.50	2.00
・ モデルの製作					0.00
・ 検査式の製作		1.00	0.50	0.50	2.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	1.00	0.50	0.50	2.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	35	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析		3.00	1.00	0.25	4.25
□ モデル検査の適用審査					0.00
合計	0.00	3.00	1.00	0.25	4.25

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	36	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析		5.00			5.00
□ モデル検査の適用審査					0.00
合計	0.00	5.00	0.00	0.00	5.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	37	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
☐ モデル検査の実施計画策定					0.00
☐ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
☐ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
☐ モデル設計		0.50	0.50		1.00
☐ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
☐ モデルの妥当性検査					0.00
☐ 本検査	0.50	1.00	0.50	0.25	2.25
☐ 検査結果の解析					0.00
☐ モデル検査の適用審査					0.00
合計	0.50	1.50	1.00	0.25	3.25

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	38	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	1.00	1.00	0.00	2.00
・ モデルの製作		1.00	1.00		2.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査			1.00	1.25	2.25
□ 検査結果の解析					0.00
□ モデル検査の適用審査					0.00
合計	0.00	1.00	2.00	1.25	4.25

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	39	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析		7.75		0.25	8.00
□ モデル検査の適用審査					0.00
合計	0.00	7.75	0.00	0.25	8.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	40	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析		5.00			5.00
□ モデル検査の適用審査					0.00
合計	0.00	5.00	0.00	0.00	5.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	41	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査			4.00		4.00
合計	0.00	0.00	4.00	0.00	4.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	42	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査			5.50		5.50
合計	0.00	0.00	5.50	0.00	5.50

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	43	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査	0.50	0.50	8.00		9.00
合計	0.50	0.50	8.00	0.00	9.00

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	44	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査	4.00	1.50			5.50
合計	4.00	1.50	0.00	0.00	5.50

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

作業日	第	45	[日目]
作業者	**********		

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					0.00
□ 検査の方針立案	0.00	0.00	0.00	0.00	0.00
・ 検査全体の方針立案					0.00
・ モデル化の方針立案					0.00
・ 検査項目の方針立案					0.00
□ 検査対象の絞込みと抽象化	0.00	0.00	0.00	0.00	0.00
・ 絞込み					0.00
・ 抽象化					0.00
□ モデル設計					0.00
□ モデルと検査式の製作	0.00	0.00	0.00	0.00	0.00
・ モデルの製作					0.00
・ 検査式の製作					0.00
□ モデルの妥当性検査					0.00
□ 本検査					0.00
□ 検査結果の解析					0.00
□ モデル検査の適用審査	1.50	1.00	4.25		6.75
合計	1.50	1.00	4.25	0.00	6.75

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

3. 実験データの集計シート（SIL3）

監査レベルの SIL3 のコスト評価に用いた実験データの集計シートを以下に添付する。

(1) 総作業コスト

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					32.25
□ 検査の方針立案					44.25
・ 検査全体の方針立案					
・ モデル化の方針立案					
・ 検査項目の方針立案					
□ 検査対象の絞込みと抽象化					14.50
・ 絞込み					
・ 抽象化					
□ モデル設計					19.00
□ モデルと検査式の製作					10.50
・ モデルの製作					10.50
・ 検査式の製作					
□ モデルの妥当性検査					6.75
□ 本検査					
□ 検査結果の解析					
□ モデル検査の適用審査					20.50
合計					147.75

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

(2) モデル検査の適用プロセスの工程毎の作業コスト

モデル検査の適用プロセスの工程毎の作業時間[時間]	
工程	合計
方針立案	44.25
実施計画策定	32.25
適用審査	20.50
モデル設計	19.00
絞込みと抽象化	14.50
モデル&検査式製作	10.50
妥当性検査	6.75
合計	147.75

(3) 作業項目の割合の算出

工程	作業	検討	打合	実行	合計
合計	54.00	52.00	39.25	2.50	147.75

工程	打合	検討	作業	実行	合計[h]
適用審査	4.00	2.00	14.50	0.00	20.50
妥当性検査	0.00	1.00	3.75	2.00	6.75
モデル&検査式製作	0.00	1.00	9.00	0.50	10.50
モデル設計	1.00	6.25	11.75	0.00	19.00
絞込みと抽象化	1.50	10.75	2.25	0.00	14.50
方針立案	19.75	17.50	7.00	0.00	44.25
実施計画策定	13.00	13.50	5.75	0.00	32.25
合計	39.25	52.00	54.00	2.50	147.75

工程	打合	検討	作業	実行	合計[%]
適用審査	19.5	9.8	70.7	0.0	100
妥当性検査	0.0	14.8	55.6	29.6	100
モデル&検査式製作	0.0	9.5	85.7	4.8	100
モデル設計	5.3	32.9	61.8	0.0	100
絞込みと抽象化	10.3	74.1	15.5	0.0	100
方針立案	44.6	39.5	15.8	0.0	100
実施計画策定	40.3	41.9	17.8	0.0	100

4. 実験データの集計シート（SIL4）

監査レベルの SIL4 のコスト評価に用いた実験データの集計シートを以下に添付する。

(1) 総作業コスト

【実験データシート】

模擬実験：独立検証機関による形式手法を用いた第三者検証のコスト評価

モデル検査の適用プロセスの工程毎の作業時間[時間]

工程	打合	検討	作業	実行	合計
□ モデル検査の実施計画策定					32.25
□ 検査の方針立案					44.25
・ 検査全体の方針立案					
・ モデル化の方針立案					
・ 検査項目の方針立案					
□ 検査対象の絞込みと抽象化					14.50
・ 絞込み					
・ 抽象化					
□ モデル設計					19.00
□ モデルと検査式の製作					20.25
・ モデルの製作					
・ 検査式の製作					
□ モデルの妥当性検査					6.75
□ 本検査					10.50
□ 検査結果の解析					22.25
□ モデル検査の適用審査					30.75
合計					200.50

打合：適用依頼者との打合せ時間、仕様のヒアリング時間等を計上する。
検討：独立検証機関内での検討時間、モデルの設計時間等を計上する。
作業：コーディング、報告書の記載等の直接的な作業時間を計上する。
実行：モデル検査器NuSMVの実行と結果出力までの待ち時間を計上する。

計測及び記入は0.25時間刻みとする。

(2) モデル検査の適用プロセスの工程毎の作業コスト

モデル検査の適用プロセスの工程毎の作業時間[時間]	
工程	合計
方針立案	44.25
実施計画策定	32.25
適用審査	30.75
結果の解析	22.25
モデル&検査式製作	20.25
モデル設計	19.00
絞込みと抽象化	14.50
本検査	10.50
妥当性検査	6.75
合計	200.50

(3) 作業項目の割合の算出

工程	検討	作業	打合	実行	合計
合計	80.25	70.00	44.50	5.75	200.50

工程	打合	検討	作業	実行	合計[h]
適用審査	6.00	3.00	21.75	0.00	30.75
結果の解析	0.00	20.75	1.00	0.50	22.25
本検査	0.50	3.50	4.25	2.25	10.50
妥当性検査	0.00	1.00	3.75	2.00	6.75
モデル&検査式製作	2.75	4.00	12.50	1.00	20.25
モデル設計	1.00	6.25	11.75	0.00	19.00
絞込みと抽象化	1.50	10.75	2.25	0.00	14.50
方針立案	19.75	17.50	7.00	0.00	44.25
実施計画策定	13.00	13.50	5.75	0.00	32.25
合計	44.50	80.25	70.00	5.75	200.50

工程	打合	検討	作業	実行	合計[%]
適用審査	19.5	9.8	70.7	0.0	100.0
結果の解析	0.0	93.3	4.5	2.2	100.0
本検査	4.8	33.3	40.5	21.4	100.0
妥当性検査	0.0	14.8	55.6	29.6	100.0
モデル&検査式製作	13.6	19.8	61.7	4.9	100.0
モデル設計	5.3	32.9	61.8	0.0	100.0
絞込みと抽象化	10.3	74.1	15.5	0.0	100.0
方針立案	44.6	39.5	15.8	0.0	100.0
実施計画策定	40.3	41.9	17.8	0.0	100.0