

ソフトウェア搭載型デバイスに適した高品質ソフトウェア開発プロセス

Development Process which Enables Highly-Reliable Devices Containing Software

安倍 秀二* 水田 恵子*

Shuji Abe

Keiko Mizuta

ソフトウェアを搭載した高信頼デバイスのソフトウェア開発プロセスは、19の標準プロセスから構成されており、多様な開発スタイルに対応するために、プロジェクトの期間を5つのフェーズ（方向づけ、技術確立、機能開発、商品化、資産化）、およびプロジェクトの分割された目的を割り当てたステージに分け、各ステージでは必要な標準プロセスを組み合わせることで開発を進めていくという特徴をもつ。

Software development processes for highly reliable software embedded device consists of 19 processes for dealing with various development styles. A project is divided into 5 phases (Inception, Technological development, Component development, Commercialization, Archiving), allocated the divided objective of the project to the each stage. In each stage, the project is carried out by combining standard processes.

1. デバイス搭載ソフトウェア開発の特徴

一般的に、組み込みソフトウェア開発は、ハードウェアも含めた製品全体の開発の工程にそって、ウォーターフォール型開発（滝の流れのような手戻りのない開発）を想定している場合が多い。そして、製品全体の開発の工程に合わせて要件定義、構想設計、詳細設計、実装、テストといった作業が順次実施される。このような開発では、比較的上流で要件を固める必要があり、下流での変更が困難になる。ウォーターフォール型開発は、試作開発を繰り返しながら段階的に要件を固めるような開発には適用しにくい。開発の上流でのテスト、下流での要件定義、あるいは当初想定外の作業の発生などが起こりうるのが主な理由である。

デバイスはさまざまな用途に利用され、デバイスに搭載されたソフトウェアの市場欠陥は、デバイスが搭載されたすべての製品不良につながり、高い品質の確保が必須となる。また、お客様と共に製品を開発する場合、その開発のスタイルは多様になり、たとえば、お客様に製品や機能を提案するプロトタイプ開発、お客様と技術検討を行うサンプル開発、そして量産品開発など、さまざまな開発がある。さらに、各開発においてソフトウェアのリリース時期は、お客様の開発日程に合わせた設定が必要で、必要な機能・品質レベル（たとえば、異常系のテストは未実施）も異なる。また、要件の確定が開発の終盤になることも多く、段階的な要件確立と品質の作り込みが必要になる。このように、デバイスに搭載されたソフトウェア開発は、望まれる成果を上げ、作業の属人

性を排除するため、作業をプロセスとして定義し、「プロジェクト設計」と独自に呼んでいる開発計画を作成しながら、そのプロセスを確実に実施し、多様な開発スタイルへ対応するとともに、プロセスを実施したという説明責任を果たすことが必要になる。また、ソフトウェア開発の全期間において、すべての作業が定義されたプロセス通りに行われたことを第三者が確実に確認することが大切であり、品質保証部門にSQA担当者（SQA：Software Quality Assurance、ソフトウェア品質保証）、開発部門にPQA担当者（PQA：Project Quality Assurance、プロジェクト品質保証）を設置し、対応している。

2. 高品質ソフトウェア開発プロセス

2.1 プロセスアプローチの採用

多様な開発スタイルに対応するために、本ソフトウェア開発プロセスは、プロセスアプローチの技法を採用している。プロセスアプローチとは、開発に望まれる成果をあげるために、プロセスを定義し、その相互関係を明確にして、運営管理するとともに、一連のプロセスをシステムとして適用することである。ソフトウェア開発に適用した場合、必要な作業をプロセスとして定義し、製品全体の開発の工程内で必要に応じてプロセスを組み合わせることにより、必要な作業をすべて実施し、暗黙の作業がなく、確実な成果物の作成が可能になる。

2.2 プロセスの構成

本ソフトウェア開発プロセスでは、ソフトウェア開発に必要な作業を4つのカテゴリ（システムプロセスカテゴリ、ソフトウェアプロセスカテゴリ、支援プロセスカテゴリ、組織プロセスカテゴリ）と、19の標準プロセスに分割して定義している（第1表参照）。各プロセスの項目は、目的、役割、開始基準、終了基準、テンプレート、ツ

* パナソニック エレクトロニクスデバイス（株）
デバイスソリューション開発センター
Device Solution Development Center,
Panasonic Electronic Devices Co., Ltd.

第1表 カテゴリー別標準プロセス一覧

Table 1 List of common processes according to category

システムプロセス カテゴリ	ソフトウェアプロセス カテゴリ	支援プロセス カテゴリ	組織プロセス カテゴリ
システム要件開発 (SYRD)	ソフトウェア要件開発 (SWRD)	プロジェクト設計 (PD)	組織マネジメント (OM)
システムアーキテクチャ 設計(SYAD)	ソフトウェア設計 (SWD)	構成管理 (CM)	品質保証 (QA)
システム統合テスト (SYIT)	ソフトウェア構築 (SWC)	問題解決 (PR)	改善 (IMP)
システム適格性テスト (SYQT)	ソフトウェア統合テスト (SWIT)		教育 (TR)
システムプロジェクト マネジメント(SYPM)	ソフトウェア適格性 テスト(SWQQT)		サプライズマネジメント (SM)
	ソフトウェアプロジェクト マネジメント(SWPM)		

ールおよび作業内容からなる。

標準プロセスの目的にそって確実に利用できるように、標準プロセスの要求事項がテンプレートに埋め込まれており、作業者は、テンプレートに記入すれば、標準プロセスの実施やその作業の結果である成果物を作成することができる。また、標準プロセスの解説、具体的な使用方法などを記載し、プロセス教育にも利用できるガイドラインを準備している。

2.3 プロジェクト設計

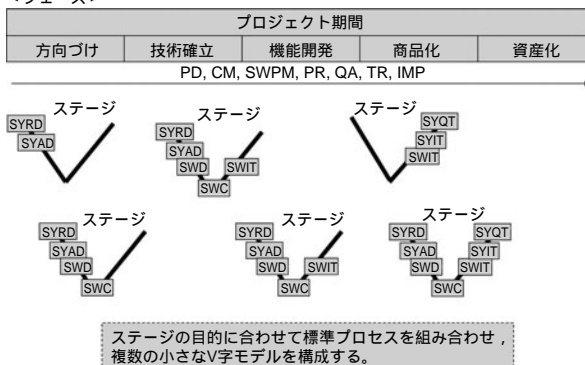
各標準プロセスはソフトウェア開発に必要な作業だけが定義されており、時間の要素はもっていない。実際の開発では、プロジェクトの目的、マイルストーンに合わせて、どの標準プロセスをいつ実施するのかを計画する。すなわち、プロジェクトの達成の目的を、マイルストーンに合わせて、複数の目的に分割し、その分割された目的を実現するためのプロセスを選択して、小さなV字サイクルを設定するようにしている。このような開発計画を策定する作業を「プロジェクト設計」と呼び、フェーズ、ステージ、標準プロセスの3つの粒度で構成される（第1図参照）。

開発者は、以下のステップで開発を進める。

〔1〕ステップ1：ソフトウェアの開発ライフサイクル選択

ソフトウェアの開発ライフサイクルとは、ソフトウェア全体の開発に後述するフェーズの組合せを当てはめたもので、プロジェクトの特徴に合わせて、製品を開発するための「量産品開発」、特定の機能を有する試作品を開発するための「サンプル開発」、新技術を提案するための「プロトタイプ開発」の3種類がある。たとえば、「量産品開発」では、製品開発の全工程の中で、ソフトウェア開発を行う期間を、達成すべき目的およびお客様や内部の

<フェーズ>



第1図 プロジェクト設計

Fig. 1 Project design

マイルストーンに合わせて、5つのフェーズ（P0：方向づけ、P1：技術確立、P2：機能開発、P3：商品化、P4：資産化）に分割する。

〔2〕ステップ2：ステージ設計

各フェーズの目的をさらに分割し、ステージに割り当てる。たとえば、お客様に試作品を納め、要件の妥当性を確認する、あるいはハードウェアの動作確認用のソフトウェアを納めるといった開発などを複数のステージに割り当てる。すなわち、フェーズ内のすべてのステージの目的が達成できれば、フェーズの目的も達成できる。フェーズは2～3箇月、ステージは2週間～1箇月の期間とする。

〔3〕ステップ3：標準プロセスの割り当て

ステージの目的に合わせて必要な作業を抽出し、標準プロセスを割り当てるが、この標準プロセスが作業の最小単位となる。たとえば、要求の分析と要件仕様の確立が目的のステージでは、SYRD、SYADを割り当て、動作ソフトウェアの作成では、SWD、SWC、SWITを割り当てる。ステージの目的に基づき、テストを簡略化したり、ハードウェアの動作確認のため設計を簡略化したりすることも可能になる。

〔4〕ステップ4：段階的な機能の作り込み

プロジェクトの目標に合わせて、反復開発を行いながら、段階的に機能が作り込まれていく。開発のライフサイクルが「量産品開発」の場合は、最終的に、すべての要件が確定し、それに基づいて各種テストが実施され、量産の品質が確保され、リリースされる。

2.4 品質保証

高信頼・高品質のデバイスを開発するためには、前述したようにプロジェクト設計と呼ばれる方法で、作業者の実施すべき作業がすべてプロセスに定義された内容と

して実施できるように計画することと、これらのプロセスが確実に実施されていることを確認する品質保証活動が必要である。プロセス遵守と成果物品質を確保するために、下記の2つの品質保証活動が実施される。

〔1〕SQA担当者によるプロセス監査とPQA担当者によるプロセス指導

プロセスの実施を客観的に確認するために、開発部門とは離れた第三者である品質部門のSQA担当者が、標準プロセスの実施確認の基準を元に、プロジェクトのプロセス実施状況についてのプロセス監査を客観的に実施する。プロセス監査は、各フェーズの移行監査としてプロセス実施の結果を確認する位置づけであり、フェーズ内のプロセスの適切な実施については、プロジェクトごとに割り当てられた開発部門のPQA担当者が確認と指導を行い、SQA担当者を補佐している。

〔2〕成果物のリリース時およびフェーズ移行時に実施するベースライン監査

成果物のリリース時、フェーズ移行時には、要求事項が漏れなく実装されているかを確認するためにベースライン監査がSQA担当者により実施される。ベースライン監査では、プロジェクトが作成してきた成果物の品質目標に応じた品質確保のための活動、すなわち成果物レビューやソースコードの静的解析、各種テストによる欠陥の除去の結果を確認するとともに、要件から設計、ソースコード、テスト仕様の一連の一貫性が確認される。

2.5 導入効果

以上、述べてきたように、本開発プロセスは、ソフトウェアだけでなく、システムプロセスカテゴリーのプロセスを明確に定義し、プロセスアプローチ技法によるプロジェクト設計、プロセス指導やプロセス監査による品質保証活動を確実に実施することによって、高品質で高効率なソフトウェア開発が可能になり、現場の混乱もなく、安定にソフトウェア開発ができるようになった。これらの活動を元に2008年、カーネギーメロン大学のソフトウェア開発組織の成熟度を確認する「CMMI (Capability Maturity Model Integration)」の“レベル3”達成の確認が得られた。また、各お客様の品質監査にも合格している。

3. 動向と展望

現在、自動車用機能安全規格ISO26262の制定が2011年6月を目指して進められている。この規格は、ソフトウェアが搭載された自動車用電子機器の安全を担保するための高信頼の開発プロセスに関するものである。ISO26262では、ソフトウェアとハードウェアのプロセス定義とそれらのシステムとしての協調開発による確実な機能安全要件の実装を担保する技法や手法の定義が含まれている。本開発プロセスは、ソフトウェアだけでなく、システムプロセスカテゴリーのプロセスの明確な定義を行ったが、今後はさらにハードウェア開発プロセスを定義することにより、機能安全規格の要求事項にも対応していく予定である。