技術論文

システムズエンジニアリングに基づく機能安全リファレンスアーキテクチャの開発

稲垣　浩之
Hiroyuki Inagaki

概　要

自動車に搭載される制御システムが大規模・複雑化する中で,機能安全設計を効率的に行い,安全論証を効果的に実施できる方法論が求められている.本論文では,限られた開発リソースで安全設計と安全論証を効果的かつ効率的に行うため,以下の特徴を有する機能安全リファレンスアーキテクチャを提案する.このリファレンスアーキテクチャは,ナレッジマネージメント,設計の不雑性回避,相互運用性,設計ミスのリスク回避の4項目の効果を十分に発揮させるための3次元モデルとして構成されている.さらに,システムズエンジニアリングの方法論に基づき,最適なデザインパターンを導出するプロセスを提供し,機能ビューのパターンを基に物理ビューの例も提示する.これにより,異なる抽象度のシステムアーキテクチャ設計への適用をサポートすることで,実設計への適用性をさらに改善することができる.最後に,本提案手法を適用して有効性を検証したケーススタディを紹介する.

1. はじめに

ISO 26262で求められている機能安全において,アーキテクチャ設計は,安全性を論証する上で重要な枠割を果たすため,戦略的に開発されることが必要となる.過去には安全システムアーキテクチャ設計のノウハウの再利用を目的として,セーフティクリティカルなシステムへの適用を前提とした安全設計パターンと安全設計戦術が幾つか提案されている[3][4].また,近年では複雑なシステムを開発する際にリファレンスアーキテクチャが用いられるようになってきている[1][2].しかしながら,実際の開発現場においては,機能安全設計に効果的に活用できているとは言い難い.このことは,以下に示す4項目の効果が十分に発揮できていないことに起因すると考えられる.

ナレッジマネージメント

安全設計の高い知識と過去実績に基づいた良い設計ノウハウを再利用する.

設計の複雑性回避

システマチックフォルトに繋がりやすい設計の複雑化を回避する.

自動車業界内の共通理解

良く信頼されたデザインパターンを採用することで,安全設計の論理的根拠を明示し,自動車業界における共通理解を図る.

リスク低減

良く信頼されたデザインパターンを適用することで,新たなリスク発生を抑制する.

筆者がリーダを務めたJASPAR機能安全ワーキング・デザインパターンチームでは,この問題を自動車業界の共通課題として捉え,2016年～2017年の2年間にわたり本活動が実施された.この活動では,上記4項目を精査し,リファレンスアーキテクチャを適用したシステムズエンジニアリングの観点で体系化するアプローチを採用した.この体系化された機能安全リファレンスアーキテクチャを活用して最適なデザインパターンを選定し,機能安全開発の効率化と安全論証に役立てていくことを業界共通の成果とすることが狙いである.

2. 機能安全リファレンスアーキテクチャ

本論文で提案する機能安全リファレンスアーキテクチャは,以下の3つのレイヤー構成で成り立っている.[1)] Static Layer：冗長設計パターンを用いたアーキテクチャの設計戦略など静的なデザインパターン目標を達成する.[2)] Dynamic Layer :故障検出,安全状態への遷移など動的な設計目標を達成する.[3)] Physical Layer：実装レベルの安全機構のセットからなる.

それぞれのレイヤーでは,再利用可能かつ信頼性が

高いセーフティクリティカルなデザインパターン,及びそれらの要素の相互関係を提供する.同時に,構成要素であるセーフティデザインパターンを品質と設計制約の情報に基づき最適に選択できるように安全設計判断を各レイヤーにてサポートする.これにより,提案するリファレンスアーキテクチャにより示されたシステム設計プロセスは,効果的な機能安全システム設計を可能にする.全体構成を図1に示す.

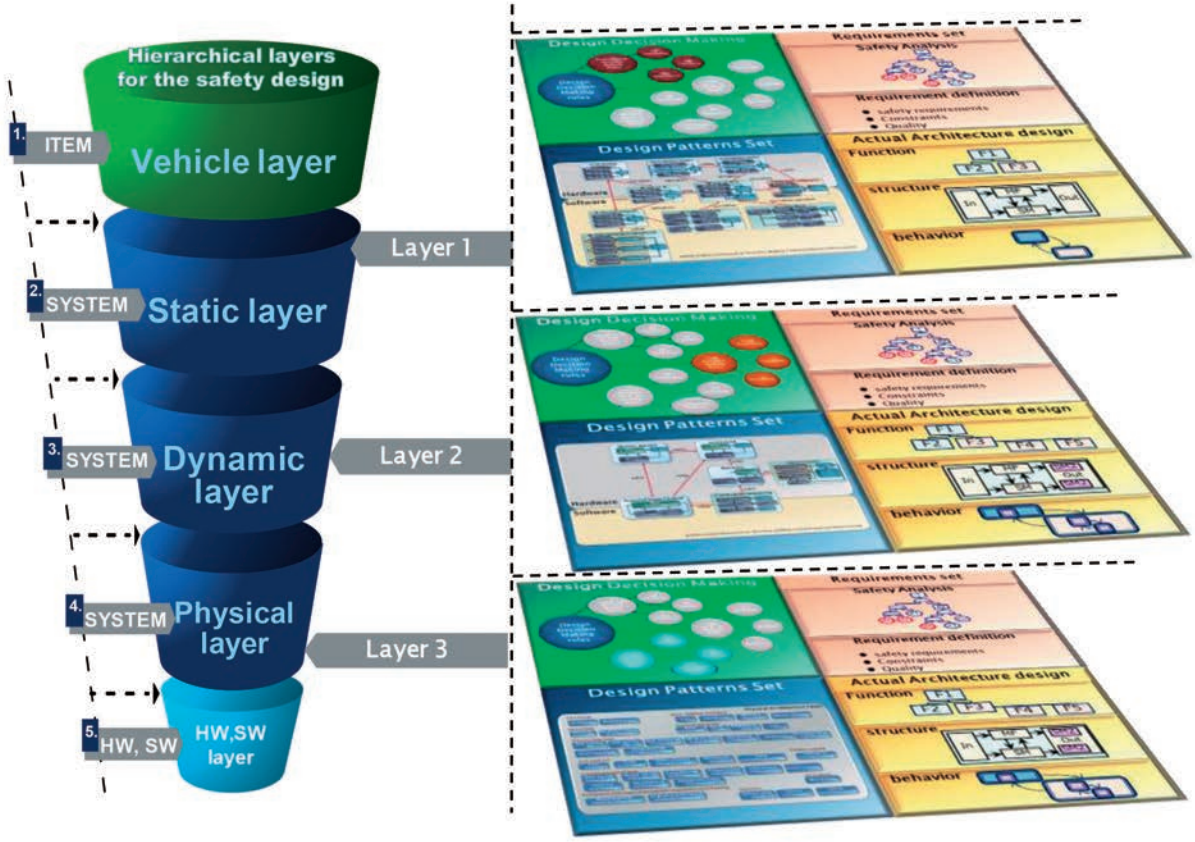

図1　機能安全リファレンスアーキテクチャ

2.1　レイヤー構成

ナレッジマネージメントとはベストプラクティスから得られた設計ノウハウをデザインパターンとしてどのように管理し,設計戦略に基づいて実際の設計に再利用できるかを意味する.図2にセーフティデザインパターンセットの階層構造を示す.システムズエンジニアリングのアプローチにより,抽象度を**静的レイヤー(Static Layer),動的レイヤー(Dynamic Layer),物理レイヤー(Physical Layer)**の3階層に分けている.さらに,それぞれのレイヤーにてFDIR(fault detection, isolation and recovery)に従い分類され,一般的な概念や原則ではなく,具体的な設計課題の解決策としてリファレンスアーキテクチャの中で提示される.

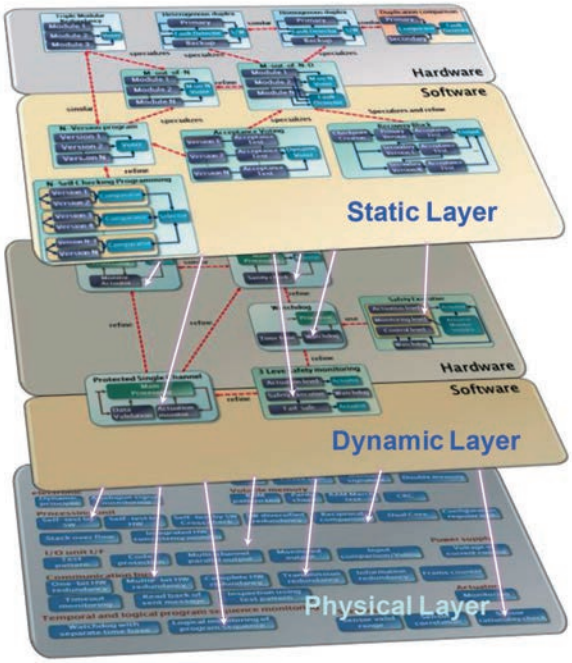

図2　セーフティデザインパターンセットのレイヤー構成

2.2　構成要素

2.2.1　安全設計戦略 (design strategy)

提案するリファレンスアーキテクチャのレイヤー内部構成を図3に示す.機能安全プロセスに適合させるため,安全要件を定義した後に最適なデザインパターンを選定できるようにディシジョンツリーを用いて設計ノウハウを明示的にルール化している.これにより,品質要求と設計制約が設計レベルで考慮され,かつ安全目標が達成できるように,各パターンがリファレンスアーキテクチャの要素として構成されている.これら2つのアクティビティをソリューション空間として定義し,機能安全の設計アクティビティを設計空間として定義する.

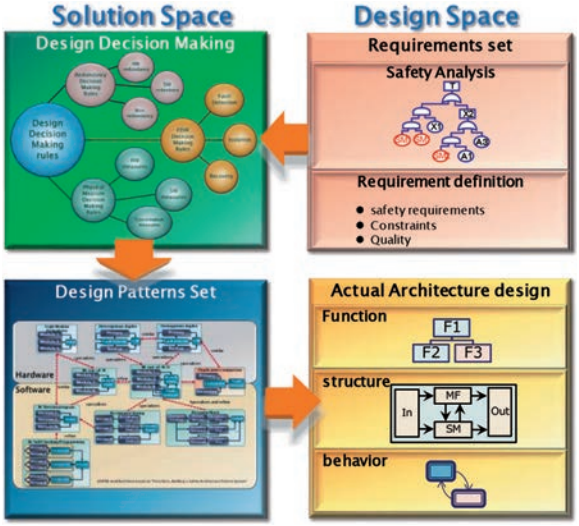

図3　各レイヤーの内部構成

3.　ケーススタディ

3.1　Fail Operationalの機能安全設計

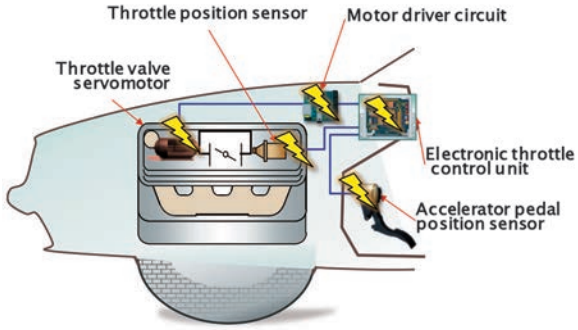

図4　Drive-by-Wire System

ケーススタディとして,Drive-by-Wire システムを対象に本提案手法を検証した結果を紹介する.以下に,構成例と安全アーキテクチャを示す.安全要求として単一故障に対して主機能を継続することを設定し,フェイルオペレーショナルのケーススタディとした.想定faultをセンサ入力系,プロセッサー系,モータ駆動回路系に分けて,それぞれの故障に対してFDIR(fault detection, isolation and recovery)の考えに基づき安全機構を機能要求として定義した.設計制約としては,コスト制約条件,サイズ制約条件,CPUリソース制約を設定し,品質要求としては,ダイアグカバレッジ,演算効率を設定した.機能安全リファレンスアーキテクチャに基づき,セーフティデザインパターンを導出した結果,Triple Modular Redundancy Pattern, Heterogeneous Redundancy Pattern, Actuator Monitor Patternが選択され,アーキテクチャにこれらパターンを組み込んだ.この時,Redundancy Patternを物理レベルで実現するため2台のECUそれぞれに故障自己診断を持たせた2ECU構成としている.これにより,1つのセンサ故障,ECUの故障とモータ駆動回路含めた制御系の故障に対して主機能を継続させるフェイルオペレーショナルの安全アーキテクチャとして確認することができた.このケーススタディを通して,Redundancy のような規模が大きいパターンを実設計に適用する場合は,変更を加えることで実装できる.また,他のパターンを内装するためアーキテクチャが多階層になる傾向がある.今後,より実用性を向上させるため実装時のノウハウをガイダンスへ反映したいと考えている.

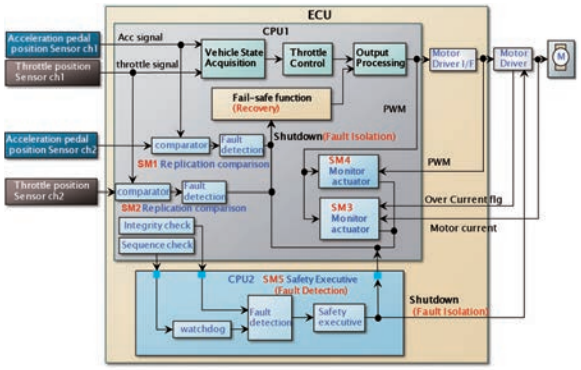

図5　デザインパターン適用結果

4.　まとめ

本アプローチは,システムズエンジニアリングに基づく機能安全リファレンスアーキテクチャの開発と,その構成要素とその関連を定義することである.提案する機能安全リファレンスアーキテクチャは,機能安全システム設計を行う上で,安全性と,そのトレードオフとなる品質特性と制約条件をシステマティックに関連付けることで,実設計への適用性の向上に有効であることが確認できた.また,JASPARのワーキング活動を通して自動車業界内でノウハウを共有し有効活用する目的に対しても,機能安全リファレンスアーキテクチャは効果的な手段であると言える.さらに対処する問題領域として,今後の自動運転開発での安全設計を見越し,フェイルオペレーショナルに焦点をあて,FDIR (Fault-

Detection,Fault-Isolation and Recovery Techniques)の概念を導入していることも特徴である.最後に,提案手法は,ケーススタディを実施して,実用性と有効性を確認することができた.今後,提案する機能安全リファレンスアーキテクチャは,JASPARにおける業界協調活動を通じて,各社の機能安全対応製品の開発,および,さまざまな組織による活用が期待できる.

5. おわりに

JASPAR機能安全WGでは,本活動成果として「機能安全デザインパターン活用ガイド」と,SysMLで記述したデザインパターンセットを公開することができた.この活動では,慶應義塾大学大学院 システムデザイン・マネジメント研究科 白坂成功教授から,丁寧かつ貴重なご助言を賜りました.ここに感謝の意を表します.また,WG活動を通じて多くの知識や示唆を頂いた,2016年度と2017年度のJASPAR機能安全WGの皆様に感謝します.

参考文献

1) Robert Cloutier, Gerrit Muller, Dinesh Verma, Roshanak Nilchiani, Eirik Hole, and Mary Bone., “The Concept of Reference Architectures”, Journal Systems Engineering archive Volume 13 Issue 1, February 2010 Pages 14-27
2) Preschem, C., Kajtazovic, N. and Kreiner, C. 2015. “Building a Safety Architecture Pattern System”., EuroPLoP ’13: Proceedings of the 18th European Conference on Pattern Language of Program, Article 17 (July 2013), 55 pages.
3) Ashraf Armoush, “Design Patterns for Safety-critical Embedded Systems”, EuroPLoP '13 Proceedings of the 18th European Conference on Pattern Languages of Program Article No. 17, 2010
4) Weihang Wu & Tim Kelly., “Safety Tactics for Software Architecture Design”, COMPSAC '04 Proceedings of the 28th Annual International Computer Software and Applications Conference - Volume 01 Pages 368-375, 2004

筆 者

稲垣 浩之
ソフトウェア技術部
安全・セキュリティの企画,開発