車載組込みシステムの多元的アスペクト指向モデリング･分析方法論

M2004MM007　東　篤子

指導教員　青山　幹雄

1. はじめに

セイフティクリティカルかつリアルタイム分散処理である車載システムでは，機能要求だけではなく安全性や開発コストなどの相反し，かつ多元的に関わる横断的特性(アスペクト) も満たさなければならない．従来のアプローチでは個々のアスペクトを扱っているため，開発ライフサイクルを通じてシステム全体にわたる非機能要求の設計が困難である．本稿では安全性と機能要求との関係と安全性と他のアスペクト間の関係をアスペクト指向で統一的にモデル化，分析する方法論を提案し，機能･非機能要求に柔軟に対応可能な車載システムネットワークアーキテクチャを導く[2].

2. 車載組込みシステムの概要

本稿で対象とする車載組込みシステムの概要として，システムアーキテクチャと開発時の特性について述べる.

2.1. 車載組込みシステムアーキテクチャ

本稿では車載組込みシステムアーキテクチャをコンポーネント/コネクタモデルとして考える．高度な機能を備えた多数の ECU(Electronic Control Unit)をコンポーネントとして，異なる特性をもったネットワーク(コネクタ)を介して連携している．図 1 に，一般的な車載組込みシステムアーキテクチャの例を示す.

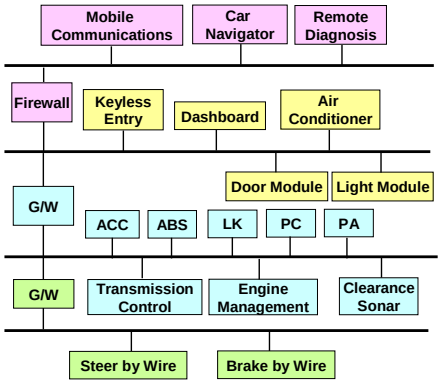

図 1　車載組込みシステムのアーキテクチャの例

2.2. 車載組込みシステム開発時の特性

車載組込みシステムはセイフティクリティカルなリアルタイム分散処理システムであり，複数のコンポーネントから成るサブシステムで構成される．そのため，開発では次の特性も考慮する必要がある.

(1) 開発特性：高い安全性と厳しいコスト制約など相反する多元的な非機能要求
(2) システムアーキテクチャ特性：分散リアルタイム処理を実現するための厳しい時間制約とリソースの制約
(3) ソフトウェアアーキテクチャ特性：異なるトリガ条件(イベントドリブン，タイムドリブン) をもつコンポーネントの混在
(4) プロダクト特性：車種ごとモデルごとに多数のバリエーションをもつマルチプロダクトライン[1]

3. 従来の設計アプローチとその問題点

車載ソフトウェアの安全性に対する従来のアプローチとその問題点を述べる.

3.1. 要求工学のアプローチ

安全性などの非機能要求の重要性が認識されているが，モデル化，分析の方法論は確立されていない.

3.2. アスペクト指向のアプローチ

複数のコンポーネントの横断的特性をアスペクトとしてモデル化する枠組みはあるが，複数のアスペクト間の関連をモデル化する方法論は確立されていない[4].

3.3. ディペンダビリティ，フォールトトレランスのアプローチ

安全性の追及に注目するため，他の非機能要求との関係に基づき，機能要求の重要性に応じた適切な安全性の割り当て方の考慮が不十分である[3].

4. 関連研究

従来のアプローチでは，アスペクトごとに個別の側面から設計するため，システム全体での要素間の関係を把握しづらく，開発ライフサイクルを通した非機能要求の定性的，定量的評価が困難である．しかし，車載組込みシステムでは安全性，性能，コストなど相互に関連し，かつ相反する非機能要求を全体として満たす設計方法論を必要とするため，従来のアプローチだけでは解決が難しい.

本稿では次のアプローチを取り入れたモデル化，分析の方法論を提案する.

4.1. アスペクト指向分析

システムやコンポーネントに横断的に関わるコンサーンを分離したのち，対象システムまたはコンポーネント群でキーとなるコンサーンを特定する．また，システムまたはコンポーネントに対する各アスペクトを定量的に割り当てる.

なお，本稿では，コンサーンもアスペクトとして統一して扱う．

4.2. アスペクトの定量的評価方法

組込みシステムの安全性を確保するための規格である IEC61508 SIL(Safety Integrity Level)により安全度を定量的に評価する[3]．SIL ではシステムのトリガ条件(イベントドリブン，タイムドリブン)ごとに安全度を扱えるため，本稿では安全性アスペクトの尺度として使用する．

また，コネクタであるネットワークプロトコルを伝送速度に応じてレベル分けするために，SAE(Society of Automotive Engineers)のクラス分類方法を採用する．

4.3. ソフトウェアプロダクトライン

プロダクトラインのコンセプトに基づき，コンポーネントをドメインレベルの再利用資産として開発し，そのドメイン資産を使用してアプリケーションを開発する． 本稿では，図 1 に示したコンポーネントとネットワークプロトコル，各アスペクトをドメイン資産と考え，プロダクトライン毎にネットワークアーキテクチャを導く．

5. 多元的アスペクト指向プロダクトライン開発方法論

5.1. 多元的アスペクト指向プロダクトライン開発プロセス

モデリング･分析のアプローチにはトップダウンとボトムアップのアプローチがある．本稿では，図 1 に示すコンポーネント/コネクタが満たすべき非機能要求が存在すると考え，ボトムアップアプローチをとる．図 2 に示すように，機能要求，非機能要求からコンポーネント/コネクタとアスペクトの関係を示すアスペクト指向モデルを導出する．さらに，アスペクトトレース/ドメインのコンセプトに基づき多元的アスペクトを分析し，分析結果を再利用資産として組合せることでプロダクトラインアーキテクチャを導出する．

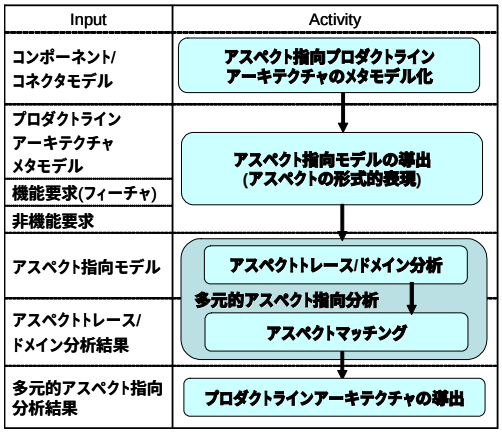

図 2 多元的アスペクト指向プロダクトライン開発プロセス

5.2. アスペクト指向プロダクトラインアーキテクチャのメタモデル

図 1 に示す車載組込みシステムを 2 つの視点，アーキテクチャを軸にしたフィーチャの視点と非機能要求を軸にしたアスペクトの視点でモデル化する．

図 3 にモデルの要素を定義するメタモデルを示す．ここで，Concern とは設計時に考慮すべき点であり，アスペクトとは Concern を実装したものである．

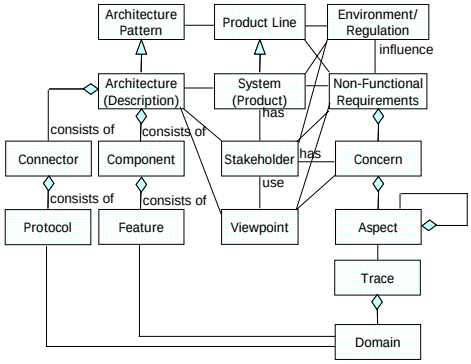

図 3 アスペクト指向プロダクトラインアーキテクチャのメタモデル

5.3. アスペクト指向モデルのアスペクト表現

本稿ではアスペクトをフィーチャ/プロトコルと同様に重要な設計要素と位置づけ，コンポーネントとコネクトを，フィーチャ/プロトコルとアスペクトの対として次のように定義する．

Component = F (Features, Aspects)

Connector =P (Protocols, Aspects)

この関係を UML のクラス表記を拡張して図 4 のように表現する．

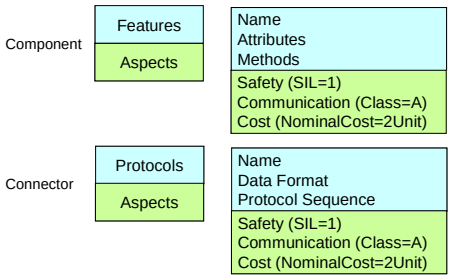

図 4 コンポーネント/コネクタのアスペクトの形式的表現

5.4. アスペクト指向モデルの多元的アスペクト分析

リアルタイム分散処理組込みシステムではコネクタを介してコンポーネントを組合せてシステムを構築する．設計時にはシステムの横断的特性であるアスペクトのマッチングを取る必要があるが，このアスペクトマッチングが設計時の困難さの要因である．本稿では分散システム上でアスペクトやアスペクト群ごとのアスペクトマッチングを設計，検証するため，図 5 に示すアスペクトトレースとアスペクトドメインの概念を提案する．

(1) アスペクトトレース：コネクタを介して接続されるコンポーネント(群)のアスペクトを制御の流れに沿って順位付けたアスペクトの集合である．i番目のコンポーネント/コネクタの n 個のアスペクトはベクトルとして式(1)で定義できる．j 個のコンポーネント/コネクタにわたるアスペクトとレースを式(2)で表現できる．

$$\boldsymbol{Ai}=(\mathrm{Ai}(1), \mathrm{Ai}(2), \ldots, \mathrm{Ai}(n)) \quad (1)$$

$$\boldsymbol{Tj}=\cup_j \boldsymbol{Aj}=(\cup_j \mathrm{Aj}(1), \cup_j \mathrm{Aj}(2), ..., \cup_j \mathrm{Aj}(n)) \quad (2)$$

図 5 では，Component1 から Component2, 3, 4, へと制御の流れがあり，Component4 ではさらに Component5 への流れがあることを示す．したがって，3 つの制御の流れに沿って 3 つのアスペクトトレースを定義できる．

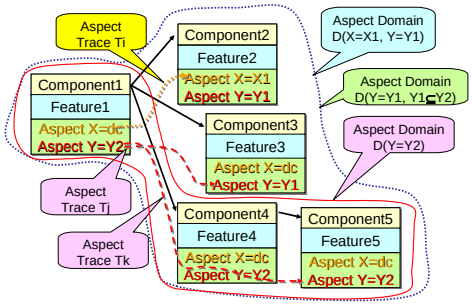

図 5　アスペクトトレースとアスペクトドメイン

(2) アスペクトドメイン：アスペクトトレースの共通集合は同一アスペクトの範囲を示す．つまり，アスペクトがマッチングしているコンポーネント/コネクタの範囲である．この範囲をアスペクトドメインと呼び，式(3)で定義する．ただし，$\boldsymbol{Ck(n)}$は n 個のアスペクトが k 個のドメイン(Dk)で満たすべき条件を表す．

$$\boldsymbol{Dk}=\cup_k(\boldsymbol{Tk} \mid \boldsymbol{Ck}) \quad (3)$$

すなわち，アスペクトドメインとは，条件 $\boldsymbol{Ck}$=(Ck(1), Ck(2), …, Ck(n))を満たすトレースの和集合である．

(3) アスペクトマッチング：アスペクトマッチングには 2 種類のマッチングを定義できる．

(a) 強いマッチング：システム全体にわたり全てのアスペクトトレースが所与の条件を満たす．

(b) 弱いマッチング：システムの所定の範囲(サブシステムなど)であるアスペクトトレースが所与の条件を満たす．

(4) アスペクトの優先順位付け：アスペクトを，必須アスペクト(必達すべきアスペクト)と選択アスペクト(必達ではないが，達成が望ましいアスペクト) の 2 つのレベルに分けて優先度をつけて分類する．

必須アスペクトは単一である．複数のアスペクトが必須アスペクトに相当する場合には，まず最重要アスペクトを必須アスペクトとする．これが満たされた場合にのみ，満足する条件の範囲で，次に重要なアスペクトを必須アスペクトとして順次分析する．

6. 車載組込みシステムの例題への適用

図 1 のアーキテクチャをもつ車載組込みシステムを例として，アスペクト指向モデリングの効果を示す．

6.1. 例題におけるアスペクトとアスペクトの評価尺度

非機能要求として，安全性，性能，コストを取り上げる．車載組込みシステムでは，安全性を重視するため，必須アスペクトは安全性である．一般に安全性を高めるためには，開発コストも増大するため，安全性とコストは相反するアスペクトである．また，安全性を保証するためにコネクタの通信プロトコルや性能には一定の条件が課されるため，安全性と性能は関連するアスペクトである．この 3 種類のアスペクトを表 1 に示す尺度と基準値で定義する．

表 1　アスペクトの定義

アスペクト	尺度	基準値
安全性	IEC 61508 の SIL	1(Low)~4(High)
通信性能	SAE Class	A(Low)~D(High)
コスト	Unit Cost	1, 5, 10, >10

6.2. 車載組込みシステムのアスペクト指向モデル

図 1 のコンポーネントに 3 種類のアスペクトを割り当て，コンポーネント間の関係を加えたモデルを図6に示す．

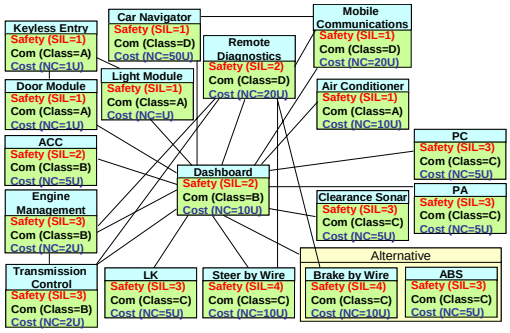

図 6　車載組込みシステムのアスペクトネットワーク

6.3. 車載組込みシステムのアスペクト指向モデルの多元的アスペクト分析

図6に基づき，必須アスペクトである安全性に対し，コスト，性能それぞれについて各コンポーネントの位置づけを分析した結果(アスペクトマトリクス)を重ねたマトリクスを図7に示す．

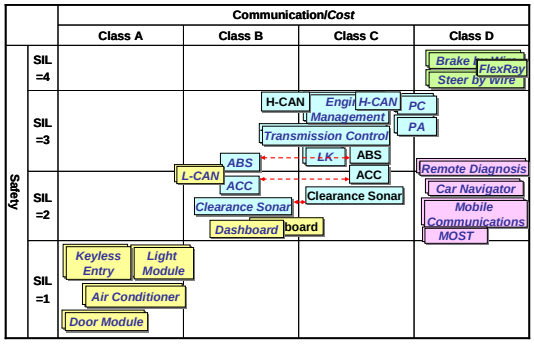

図 7　アスペクトマトリクスのオーバレイ

図7を見ると，位置にズレが生じるコンポーネントが存在することから，設計時に注意すべきコンポーネントとアスペクトであること，また選択アスペクトの中から2番目に必須のアスペクトの決定を検討する必要もあることがわかる．

6.4. プロダクトラインアーキテクチャの導出

前項までの分析結果を再利用資産としてプロダクトラインアーキテクチャを導出する．各アスペクトレベルの計算結果から図 8 に示すようにプロダクトラインごとにアスペクトが満たすべき範囲がわかる．この範囲を満たしながら，プロダクトラインアーキテクチャを構築できる．

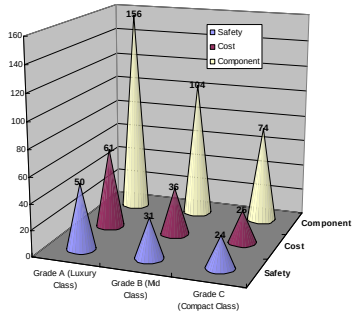

図 8　3 つのプロダクトラインのアスペクトレンジ

図6, 図7から安全性アスペクトのマッチングを取り，各コネクタ(MOST, Low-Speed CAN, High-Speed CAN, FlexRay)を介して，4つのサブシステムすべてを接続すると図9に示す Grade A(Luxury Class)のアーキテクチャを構成できる．

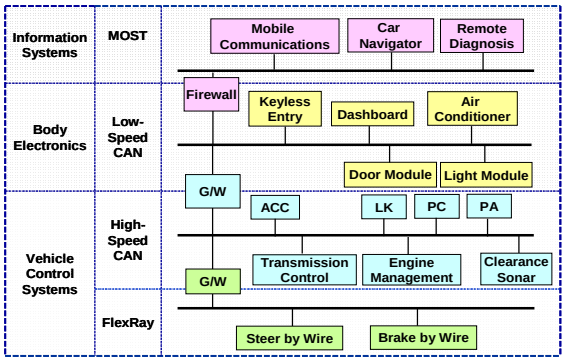

図 9　プロダクトラインパターン(Luxury Class)

アスペクトマッチングを維持しながら，Luxury Class のパターンからサブシステムを取り外すまたはサブシステム内のコンポーネントを交換/取り外すと，より廉価なプロダクトライン，Mid Class や Compact Class のネットワークアーキテクチャも構成できる．詳細は修士論文に示す．

7. プロダクトラインアーキテクチャ設計支援ツール

本稿で提案するアスペクト指向モデリング，分析の結果をもとに，プロダクトラインアーキテクチャ設計のコンピュータ支援を提案する．本ツールは，アーキテクチャパターンとコンポーネント/コネクタの組合せ方，あるいはアスペクトの制約によって多数存在するアーキテクチャのバリエーションをシミュレーションし，設計者による最適なアーキテクチャの選択を支援する．図 10 にツール概要を示す．

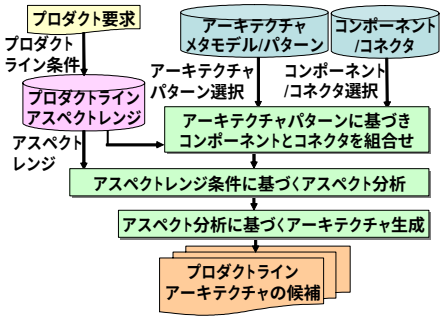

図 10　プロダクトラインアーキテクチャ設計支援ツール

8. 今後の課題

現代の自動車では，車種によっては 50 を超える ECU が連携しており，多くの非機能要求を扱う必要があるため，アスペクトトレースの組合せは増大する．今後，実システムに適用するためには，アスペクトとコンポーネント/コネクタの一層複雑な関係をモデル化でき，モデルの正当性を検証できる方法を検討する必要がある．

9. まとめ

セイフティクリティカルかつリアルタイム分散処理である車載システムにおいて，安全性や開発コストなどのような相反し多元的に関わる横断的特性(アスペクト) に対し，安全性と機能との関係と安全性と他のアスペクト間の関係をアスペクト指向で統一的にモデル化，分析する方法を提案した．また，プロダクトライン開発アプローチに基づき，アスペクトモデリング，分析結果を再利用可能なドメインの資産として組合せ，機能とアスペクトを最適なレベルで満たす車載組込みシステムのプロダクトラインモデルを導出できた．

参考文献

[1] P. Clements, et al., Software Product Lines: Practices and Patterns, Addison Wesley, 2001.

[2] 東 篤子ほか，車載組込みシステムの多元的アスペクト指向モデリング試論，ウィンターワークショップ 2006･イン･鴨川 論文集，Jan. 2006, pp. 9-10.

[3] MISRA, *Development Guideline for Vehicle Based Software*, V. 1.1, 2001.

[4] R. Reddy, et al., An Aspect-Oriented Approach to Analyzing Dependability Features, *Proc. AOM '05*, Mar. 2005, http://dawis.informatik.uni-essen.de/events/AOM_AOSD2005/.