機能安全要求の導出方法
－ 初期アーキテクチャと時間間隔を中心に －

伊藤　昌夫[†]

A Method for Derivation of Functional Safety Requirements
- Focusing on Preliminary Architecture and Time Interval -

Masao Ito

ねらい　本論では，概念段階に作成する機能安全要求の導出について記述する．記述内容は，乗用車用機能安全規格 ISO 26262 Part 3 に従う．特に，初期アーキテクチャへの安全機構の埋込，および故障耐性時間間隔の記述について手順を示している．

キーワード　機能安全要求，ISO 26262，概念段階，初期アーキテクチャ，時間間隔

Target: In this paper, we provide the approach for deriving the functional safety requirement in the concept phase. It conforms the standard ISO 26262. Especially, we focus on the design of preliminary architecture and the calculation of time interval.

Keywrds:　Functional Safety Requirements, ISO 26262, Concept Phase, Preliminary Architecture, Time Interval

１．背景

機能安全要求（仕様）は，概念段階におけるアイテムに関する成果物である．後続する個別システム開発の入力となる．実際のシステムは，機能安全要求に従うため，乗用車のような一般に広く利用されているシステムにおいては，重要な位置づけを持つ要求である．

本論では，機能安全要求の記述項目は，乗用車の機能安全規格である ISO 26262 Part 3 に従う．先行するタスクは，ハザード分析とリスク評定であり，そこで定めた Automotive Safety Integrity Level (ASIL)やセーフティゴールを利用する．

機能安全要求では，故障耐性時間間隔といった時間間隔を含む記述が必要になるにも関わらず，適切なガイドが少なく，経験的に記述が難しい仕様である．

これまで筆者はハザード分析やリスク評定に必要な制御可能性の計算方法について示しており[1][2][3]，本論は，その結果を受けて，如何に機能安全要求を記述するかを示す．

2．課題：機能安全要求

機能安全要求とは，定義に従えば，「実装から独立した安全に関わる振る舞い，または安全手段であり，安全に関わる特性を含む」である（1-1.53，以降，括弧内は規格関連番号，但し最初の数字は，Part の番号である）．

機能安全要求が含むべき項目は以下である（3-8.4.2.3）

- 動作モード
- 故障耐性時間間隔
- 安全状態
- 緊急動作間隔
- 機能的冗長性

動作モードと安全状態は，それぞれハザード分析およびリスク評定中で検討されるので，その詳細化によって得ることができる．しかし，他の項目については，機能安全概念タスク中で検討する必要がある．

3．これまでに示した手法

これまでに示した手法について，本論と関係する範囲に限定して，簡単に示す．

概念段階の最初に，アイテム定義を行う．ここでは静的／動的アイテムスケッチを用いる．アイテム定義と並行して，そのトップゴールを詳細化したゴールモデルを作成する．ノードにガイドワードを適用することで，ハザード候補を識別する．この候補は障害ノードとする．この解決策，即ちセーフティゴールを解決ノードとして表現する．ここでのゴール–障害ノード–解決ノード関係は，Goal Structure Notation（GSN）を用いたセーフティケースとして示すことができる．本論で示す機能安全要求を，仕様ノードとして表現することで，全体が統一的にゴールモデルを中心に表現できる．本論では，このうち，解決ノードから，仕様ノードの関係を詳細に記述する．

[†]株式会社ニルソフトウェア
Nil Software Corp. 2-17-7, Kinuta, Setayga, Tokyo 157-0073, Japan,
E-mail: nil@nil.co.jp

4. 導出の方法

本論では，機能安全要求のうち，特に初期アーキテクチャと時間間隔を中心とする．

4.1 初期アーキテクチャ

ベースとなるのは，前章におけるアイテムスケッチである．ASIL に基づき，必要な安全機構を加える（機能的冗長性検討の一部である）．安全機構の中身は，ハザードとその影響により異なるが，概念段階における構造としてはパターン化することができる．下図に幾つかのパターンを示す．

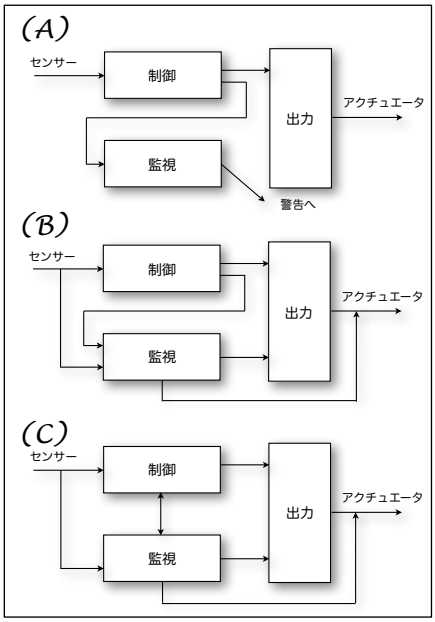

図 1　冗長性のための機能安全機構の埋込

Fig.1 Embedding the Safety Mechanism for Redundancy

制御とあるノードは，対象となる機能を実現するコンポーネントであり，監視とあるノードは，安全機構の一部を構成する．(A)は，単純な警告のみを送出するパターンであり，(B)では，センサーからの入力及び制御出力を監視し，要すれば出力をオーバライドする．(C)(B)に加えて相互に監視し，要すれば出力をオーバライドするパターンである．安全ゴールおよび，次節で示す時間間隔の情報を用いて，最終的なパターンを選択し，機能的冗長性とする．

4.2 時間間隔の算出

2 章で示したように，機能安全要求では，時間間隔として，故障耐性時間間隔および緊急動作間隔の算出が必要になる．故障耐性時間間隔は，アイテムないしはエレメントに故障が発生してから，ハザード事象が生じるまでの時間間隔である．この間に故障を検知し，安全状態に縮退するが，最初の故障から縮退が完了するまでの時間間隔が，緊急動作間隔である（診断間隔に起因する故障検知できない時間間隔を含んでいる）．

さまざまな種類の時間間隔が存在している．例えば，故障検知は一定間隔で，（監視ノード中で）動作している．故障発生後，直ちに検知処理があれば，故障耐性時間間隔および緊急動作間隔ともに短くなる．監視だけではなく，故障時に縮退するために何らかの計算を行う場合，計算量によって実行時間は変動する．或いは，監視ノードの独立性を高めるために，異なる ECU で動作する必要があるかもしれず，その場合は，実行時間に更に差が生じる．

本手法では， AADL[4]を用いて，各ノード（およびその構成要素）と，そこでの処理に要する時間を定義する．AADL は記述のための必要な要素を持っている．

```
processor PRC_750
properties
  SEI::cycle_time => 12 ps;
end PRC_750;

process SafetyMech
  features
    ...
end SafetyMech;

process implementation SafetyMech.Impl
  subcomponents
    CM_TASK : thread detect_fault_QZ013.i
    ...
  connections
    ...
end SafetyMech.Impl;

thread detect_fault_QZ013
  feature
    sensor_data: in data port;
    actuator_data: out data port;
  properties
    Disptach_protocol -> Periodic;
    Period => 50ms;
end detect_fault_QZ013;
```

図 2　時間記述を含んだ故障検知モジュールの記述例

Fig.2 Sample of Detection Module with Time Interval

図 2 が記述例である．概念段階では，これら数値はあくまで推定値である．しかし，判断の根拠を残すことに意味がある．最終的にこれら時間間隔定義から，故障耐性時間間隔および緊急動作間隔を算出する．

5. まとめ

本論では，機能安全要求のうち，初期アーキテクチャと時間間隔を中心に記述した．これらはドライバの制御可能性とも関係する重要な記述である．それにも関わらず具体的な手段が示されることが少なく，その点で貢献できると考えている．

文　　献

[1] 伊藤，「概念段階におけるハザード・脅威の識別手法」，SEC Jounarl，第 10 巻，第 6 号，2015 年

[2] 伊藤，「CARDION: 概念段階における ハザード・脅威の抽出手法」, www.ipa.go.jp/files/000036233.pdf, 2014

[3] 伊藤，「制御可能性算出のためのドライバモデルおよび環境モデルの構築」, http://www.ipa.go.jp/files/000043912.pdf, 2015

[4] SAE, "Architecture Analysis and Design Language (AADL), AS5506A," ed: SAE, 2009.