

例外状態における非機能要求の明確化

三瀬 敏朗^{†1}

我々の生活を取り巻く家電製品には、多くのソフトウェアが組込まれている。これらの製品は不特定多数の人々により様々な環境において長期間利用される。製品の利用期間には、様々な不具合や故障が発生することが予想される。利用者を障害から救うために、製品は、使用開始から寿命末期に至るまで、高い品質基準と安全を保持することが必要である。そのために、正常でも異常でもない状況における非機能要求を明確にする必要がある。

Clarifying Non-Functional Requirements in Anomalous States

TOSHIRO MISE^{†1}

Systems embedded in household electric appliances are used for long periods of time by various kinds of people. These environments sometimes cause unexpected failures. To save users from the appliances failures, every product is required to retain a high standard of quality and safety until their terminal period. Therefore it is necessary to make clear Non-Functional Requirements in Anomalous States.

1. 背景

家電製品等のソフトウェア組込み製品（以後、製品という）は、我々の日常生活において様々な環境の下で使われている。そのため、その製品の開発者は、製品が想定使用期間を越えて使用されても、また想定していない方法で使用されても、故障による障害から利用者を守らなければならない。これらの製品では、頻度が高い状況において必要なハードウェアが装備されている。このため、カタログに記載された機能を実現できる状況から逸脱した環境や使われ方において、完全な機能や非機能は要求されない。ただし、製品は利用者の生活に密着しており、安易な停止は許されない。そのため、利用者に支障の少ない軽微な故障であれば、安全性を確保しつつ、製品機能や利便性などの非機能の継続性についても配慮する必要がある。

製品は、どのような事態に陥っても機能を失わないようにするフォールトトレランスを要求されていない。製品の利用価値は、価格に対して最大の価値を提供することである。したがって、製品は、可能な範囲で稼働させるフェールソフト、システムが誤動作をしたり部品が故障したりしても、安全側に制御するフェールセーフ、操作や手順を間違えても、危険を招かないよ

うに設計するフルブーフにより、利用者に安全性と高い可用性を提供する必要がある。しかし、製品が正常な振る舞いから逸脱状況において使われ続けるため、逸脱要因が複合することによる設計者の想定していない障害リスクも増加する。

このような、すべての機能やすべての非機能を部分的にしか満足できない状況において、使用者に最大の利用価値を与えるという要求も非機能要求である。つまり、利用者は、正常なカタログに記載された振る舞いだけではなく、これらから逸脱した製品の振る舞いに対しても製品の品質と見なす。

製品が使用される環境と製品に要求される要件について図 1 に示す。カタログに記載された使用環境において、製品は機能要求と非機能要求を満足されなければならない（領域 A）。また、製品が重大な故障や製品の環境に重大な問題があった場合は、直ちに安全に停止しなければならない（領域 C）。これらに属さない領域として、製品の環境や製品自体に軽微な問題があるが、重大な問題ではないという領域がある（領域 B）。この領域では、カタログに記載されたすべての機能を要求されてはいないが、できる限りの機能や非機能を継続し、最大価値を提供することが要求される。また、製品の環境や製品自体の問題がなくなった場合には、速やかに前の状態に復帰することが期待される。

^{†1} パナソニック株式会社
Panasonic Corporation

このような非機能要求を明確にするためには、以下のプロセスが必要となる。図2に非機能要求から非機能要求を保証するための機能要求に変換するプロセスを示す。はじめに、機能要求から製品の振る舞いに変換する。次に、その振る舞いに対して、製品が使われる悪環境や誤操作などの逸脱要因を想定し、障害分析を行う。障害分析は、システムの振る舞いが逸脱した結果として起こりうる障害に至る例外的な振る舞いを抽出する。さらに、例外的な振る舞いが、非機能要求の視点から許される範囲かの妥当性を検証する。その逸脱が許容できない場合は、障害と見なされる。そのため、障害に対する回避対策を検討し、それらを非機能要求を保証するためのための障害回避機能として機能要求に組み込み、様々な逸脱に耐えうるかの検証をもう一度行う。この理由は、非機能要求の項目間に相互関係があるため、他の非機能要求に影響がないことを確認する必要があるためである。

しかし、一般的に推奨されているFTAやFMEAなどの手法を含めて、複雑な動作を行うソフトウェア組込み製品に適した障害分析手法は確立されていない。

そこで、我々は、ソフトウェア組込み製品に対して、分析対象を製品利用環境を含んだ状態遷移モデルとし、簡略化した状態遷移表である非正常系分析マトリクスと、それを適用した障害シナリオ抽出手法ESIM(Embedded System Improving Method)を研究している。そのポイントは、下記である。

- ・障害に至る時間変化に対する影響を陽に含むシナリオ過程を分析
- ・複合的な要因が相互に影響する障害の分析
- ・アーキテクチャ設計段階で予見できない障害の抽出
- ・部品故障や誤操作など広く影響要因を捉えた分析

2. 議論したい課題

社会インフラとなるシステムも利用者の生活に密着し、安易にシステム停止をさせることができない。また、組込みシステムと同様に、システムの機能が家庭の中に入り込み、一般利用者による使用が多くなっていく。今後、社会インフラとなるシステムは、組込みシステムとの共通性が増してくると考えられる。

社会インフラとなるシステムでは、基盤となるシステムが稼働してから新たな用途が開拓されいく。これにより、後に接続されるシステムは、最初の意図とは変化している。しかし、最初に施工したシステムの基本的な設計の基盤は、容易に変更できない。

このような状況の中で、システムの安全性と可用性などを維持するための要求定義について、以下の項目

製品の振る舞い	正常な振る舞い	逸脱した振る舞い	停止
動作条件	カタログに記載された動作環境	カタログに記載された動作環境からの逸脱 過負荷、施工不良、イタズラなど異常操作 異常環境、設定不良、ハード誤動作、 経年劣化、故障など	
製品への期待	製品に期待された要件をすべて確保	安全性を確保しつつ、可能な機能を活かし、早く正常に復帰	安全な停止
機能要求と非機能要求の充足性	100%	0%	
領域	領域A	領域B	領域C

図1 障害分析の領域

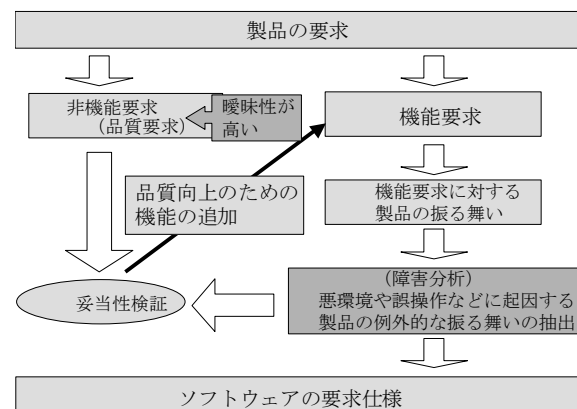


図2 正常な動作からの逸脱の分析

などを議論したい。

- ・組込みシステムから社会インフラへの適用をさせる
とき違いはなにか。
- ・止まらないシステムを構築するために、どのような
要求を定義すべきか。
- ・要求定義におけるアーキテクチャと非機能要求の関
係をどのように配慮すべきか。

参 考 文 献

- 1) 三瀬 敏朗, 新屋敷 泰史, 橋本 正明, 中谷 多哉子, 片峯 恵一, 鶴林 尚靖, 吉田 隆一: 非正常系分析マトリクスによるソフトウェア組込み製品の障害シナリオ抽出手法, 電子情報通信学会 和文論文誌 Vol.J95-D, No.11, pp.1897-1908(2012)
- 2) 三瀬 敏朗, 新屋敷 泰史, 中谷 多哉子, 片峯 恵一, 鶴林 尚靖, 橋本 正明: 高品質組込みソフトウェア設計における非機能要求に着目したプロジェクトマネジメント, プロジェクトマネジメント学会, 2008 年度春季研究発表大会 pp.221-216(2008)