大規模複雑化した組込みシステムための障害診断における形式手法の適用事例報告

岡野浩三
信州大学工学部情報工学科
okano@cs.shinshu-u.ac.jp

北道淳司
会津大学コンピュータ理工学部
kitamiti@u-aizu.ac.jp

要旨

IPA/SEC ソフトウェア高信頼化推進委員会 障害原因診断 WG では，大規模・複雑化した組込みシステムで発生した障害に対する初動調査から障害原因診断分析，整理に至るまでのプラットフォームとして事後 Verification & Validation(V&V)を提案している(発表時には参照先を示す)．本稿では，事後 V&V において，形式手法による障害原因診断の例を述べる．

1. はじめに

大規模・複雑化した組込みシステムでの障害は社会への影響が大きく，多くの設計技法や国際規格が提案されているがそれでも障害が発生する．本稿では，形式手法を用いて障害診断を行った例を述べる．形式手法は，数学的な意味定義が行われた言語および手続きによりシステムのモデリングおよびモデルに対する議論(ある性質が成り立つかどうかなど)が行える．形式手法の一つであるモデル検査手法を化学プラントに適用し，プラントに内在する障害を検出し，モデルを修正するまでを述べる(詳細はスライド参照)．

2. 形式手法を用いた障害診断例

対象は図 1 に示す化学プラントである．2 つの水槽があり，センサ，操作員による操作を入力として，水槽があふれないように制御する．このプラントでは，ある条件において水槽があふれるという障害が発生した．プラントの制御部に着目し，形式手法の 1 つである UPPAAL[1]を用いて文献[2]を参考にモデル化した(図 2)．

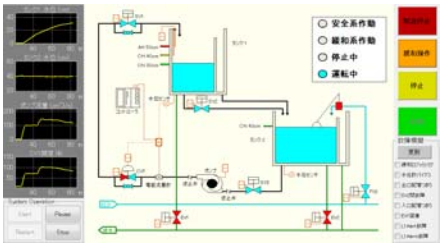

図 1対象とした化学プラント

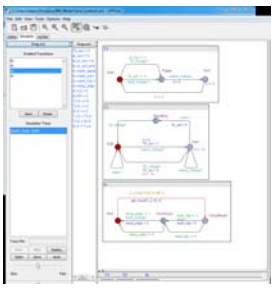

図 2 UPPAAL を用いたモデル

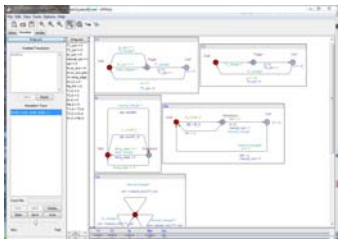

図 3 修正して得られたモデル

一般に，事後 V&V では事故などが発生したあとシステムの資料などからシステムモデルを作成し，そのモデルを解析して事故の原因を究明する．このケーススタディでは図1のシステムの要求記述をもとに図 2 のモデルを作成した．「水槽はあふれない」ことを時相論理式で表し，モデル検査を行った結果，性質が成り立たないことと反例が示された．反例を解析した結果，モデル(すなわち，当初の制御部の設計)にバグがあることが分かり，それを修正したモデル(設計)を作成し，性質が成り立つことを示した．

3. まとめ

組込みシステムの障害に形式手法を適用し，その障害を検出し，取り除いた事例を述べた．形式手法のこのような利用に関する質問，ご意見を伺いたい．

[1] Gerd Behrmann, Alexandre David and Kim G. Larsen,” A Tutorial on Uppaal,” LNCS Vol. 3185, pp 200-236, 2004.
[2] Kim Björkman, Juho Frits, Janne Valkonen, Jussi Lahtinen, et al., “Verification Of Safety Logic Designs By Model Checking,” Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC&HMIT 2009.