形式手法の産業応用の観点からCPSを考える

青木利晃[†1] 片山卓也[†2,†3]

Thinking about CPS from the view point of Industrialization of Formal Methods

Toshiaki Aoki [†1] and Takuya Katayama[†2,†3]

1. 形式手法の産業応用

我々の研究室では，形式手法の実践手法について研究を行っている．我々が，現在，最も力を入れているのは，車載システムへの形式手法の実践的適用手法に関してである．車載システムの安全性や信頼性に関する問題は，社会において非常に大きな関心となりつつある．車は，従来は機械的に制御されてきたが，近年，コンピュータ制御技術の発展と利便性や性能の追求により，多くの部品の電子化が進んできている．これにより，車載システムの規模の急速な増大と複雑化がもたらされ，主に，電子制御部分の安全性と信頼性に関する問題が取り上げられつつある．世界標準においては，機能安全に関する標準が一般の電子システムだけでなく，車載システムに特化されたものが策定されている．また，実社会においては， 2010 年に発生したトヨタ車の急加速問題において，電子スロットル制御システムの検証が NHTSA と NASA により実施された．我々は，このような車載システムの安全性や信頼性の問題を背景に，車載システムへの形式手法の実践を試みている．現在，主に，車載オペレーティングシステムの検証手法[1)–3)]，ISO26262 における安全要求の形式化と検証手法[5)]，車載ネットワークで結合されたシステムの検証手法[4)] について研究を行っている．これらについて詳細は説明しないが，興味がある方は，参考文献などを参照いただきたい．

現在の自動車には，100 個以上の ECU(Electronic Control Unit) が使われていることもある．それらの ECU は，ネットワークにより接続され，通信している．ここで，通信プロトコルとしては，CAN, LIN, MOST など複数のプロトコルが混在して用いられている．さらに，複数の電源系統が使用されており，ある ECU が，その ECU が接続されている電源系統とは，別の電源系統の ON/OFF を制御している．また，年々，ECU の性能が向上しており，マルチコア化もなされている．AUTOSAR OS の標準仕様には，1 つの ECU 上に複数のアプリケーションを割り当てるための保護機能や，マルチコアに関する機能も盛り込まれている．まさに，ヘテロジニアスな構成となっている．

2. CPS の課題

CPS には色々な見方が存在する（と聞いている）．私の立場から見ると，比較的「まっとう」なバズワードであると考えている．現在，実際に使われてるシステムを，CPS という観点から，よく考えてみましょう，と言っているような気がするからである．先を見据えて新しい何かを創出するというよりは，現状をなんとかしなければならない，というメッセージに思える．私自身，形式手法の実践に関する研究を行っているが，その動機と一致する．以下では，その観点から，私が重要だと考えている問題点を２つほど，紹介したい．

１つ目は，モデル化の問題と計算の問題の切り分けである．モデル化の問題とは，CPS で起きている現象を明らかにして，何らかの形式で表現することである．表現されたものの上で計算ができるかどうかは別問題である．計算の問題とは，CPS で起きている現象が，どこまで計算により解決できるかということである．つまり，モデル化したものに対して，’計算ができるかどうか’，ということに関する追求である．現在，車

†1 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology
†2 中央大学研究開発機構
Chuo University
†3 JAIST シニアプロフェッサー
Senior Professor, JAIST

載関連の PS(Physical System) に関する技術として，形式手法の分野ではハイブリッドシステム，実践では MATLAB/Simulink が注目されている．ハイブリッドシステムにおいては，主に，自動的に解ける問題に関する追求が行われている．しかしながら，自動的に解ける問題は限られており，CPS で起きている問題の多くを解決できる，とは言いがたいと考えている．MATLAB/Simulink では，フィードバック制御の部分のモデルを記述，シミュレーション行い，プログラムを自動生成できる．ハードウェアや，電気回路，物理環境のシミュレーションを行うツールとも連携ができる．これらは，実際に必要とされることを実現しているが，詳細にシミュレーションしたり計算することは困難な状況である．このような状況から，モデル化の問題と計算の問題の切り分けが重要であると考えている．

2 つ目は，規模と複雑さの問題への真摯な取り組み，である．ソフトウェア工学の分野では，規模と複雑さの問題は，長年，研究者の間で共有されて来た．実際，論文の評価の節を見ると，規模 (scalability) は代表的な評価軸となっている．しかしながら，実際のシステムに適用するくらいのパフォーマンスが獲られているものは少ない．また，ケーススタディの論文を見ていても，システム全体に適用しようとしているものは稀である．高々，システムの一部に関して，要求される性質のごく一部について取り扱っているだけである．実際の開発で使うためには，その一部への手法を，全体に適用する必要があるが，そのためには，規模や複雑さを管理するための別の手法が必要となるはずである．しかしながら，規模や複雑さの問題は，ないがしろにされがちである．特に，CPS のような，規模と複雑さの高度な問題を抱えている対象には，最初から，白旗を上げているように思えるのである．

3. 真摯な産学連携体制の構築

以上で述べたように，CPS という言葉で改めて感じるのは，現状のシステムの問題を直視して，解決しなければならないということである．そのためには，真摯な産学連携体制の構築が不可欠であると考えている[6]．ソフトウェア工学/科学分野における産学連携の必要性については，長年，言われ続けてきた．しかしながら，十分に連携できていないのが現状である．企業においては，現場対応の技術的方法で問題を解決しているように見える．また，大学においては，単純化された問題設定のもとでの研究を行っており，その有効性については現実的評価が行われないものが多い．

連携の障壁には様々なものが考えられるが，以下で，いくらか指摘しておきたい．まず，産業界における，企業秘密の問題がある．重要なノウハウのみならず，顧客と関係する情報を過度に守秘する傾向があり，十分に研究コミュニティに開示できていない．次に，これも産業界のものであるが，経営者への見せ方，および，経営者の認識の問題である．企業の経営は，技術だけではないとはわかっているが，それでも技術の重要性をないがしろにしすぎているように思える．経営者への説明方法など工夫が必要であろう．研究コミュニティにおいては，論文中心の業績評価も問題であると思われる．大学などにおける業績評価においては，論文数などが客観的な指標として使われがちである．さらに，論文のための研究は，比較的，容易に学会で評価されやすく，実践のための研究は，非常に労力がかかるが，それに見合う評価がされていないように見える．産業界にとって本質的な問題に挑戦したかどうかで評価する必要があるのではないか．

4. ま と め

このポジションペーパでは，現在，我々のグループが主に取り組んでいる車載システムの状況を紹介し，我々の経験から，CPS で重要と思われる課題，および，解決のための重要な方策として，産学連携体制の構築について述べた．経験に基づいたものなので，根拠は無いが，議論のたたき台となれば幸いである．

参 考 文 献

1) Kenro Yatake, Toshiaki Aoki: Model Checking of OSEK/VDX OS Design Model Based on Environment Modeling, pp.183-197, 2012.
2) Jiang Chen and Toshiaki Aoki: Conformance Testing for OSEK/VDX Operating System Using Model Checking, APSEC, pp.274-281, 2011.
3) 青木利晃, 佐藤信, 谷充弘, 矢竹健朗: モデル検査とテストによる車載オペレーティングシステムのシームレスな検証, 組込みシステムシンポジウム, pp.178-187, 2012.
4) Xiaoyun Guo, Hsin-Hung Lin, Kenro Yatake and Toshiaki Aoki An UPPAAL Framework for Model Checking Automotive Systems with FlexRay Protocol, FTSCS, pp.36-53, 2013.
5) 青木利晃，千葉勇輝，松原正裕，西昌能，成沢文雄: ISO26262 における安全仕様のゴール木を用いた浅い形式化, FOSE, ポスター発表, 2014.
6) 片山卓也:先進的ソフトウェア技術の実践と創造, SEC journal 創刊 10 周年特別号, p.2, 2014.