AdaCore
The GNAT Pro Company

TECHNICAL REPORT

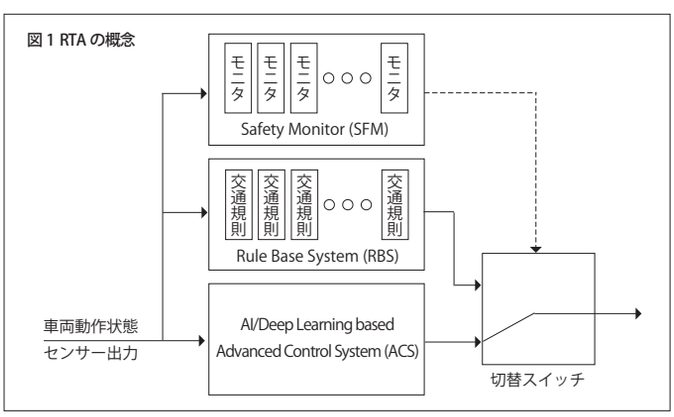
自動運転向け安全制御ならびに監視ソフトウエアの開発に関して

AdaCore 社は、自動運転技術開発向けに形式検証された”Runtime Assurance”（以下 RTA）の開発をご提案します。最初に “Simplex architecture” [注1] で紹介された RTA [注2] は、制御システムの不正な挙動を検出するために、センサーから報告される車両の状態を継続的に監視します。不正な挙動が検出された場合、RTA は、信頼度の高いリカバリーシステム（rule-based system　以下 RBS）へ制御を切り替えます。

AdaCore 社は形式化された法律、条例、道路交通規則に基づいて形式検証された監視システム（Safety Monitor 以下　SFM）、ならびに、形式的に検証された道路交通規則に則った信頼度の高い RBS も開発します。

この 2 つのコンポーネントを応用して、安全性が損なわれない信頼性の高い AI/ ディープラーニングに基づく振舞制御システム（Advance Control System 以下 ACS）の開発、導入が可能となります。

図 1 RTA の概念



このアプローチでは、形式検証された SFM は、形式化された法律、条例、道路交通規則から逸脱する安全基準違反を継続的に監視します。通常運転では、ACS が車両の挙動を積極的に制御します。

安全基準違反が発生することが差し迫った状況が検出された場合、ACS から形式検証された RBS に制御が切り替わります。RBS 動作中も監視は継続され、さらに安全基準違反が発生する場合、最終手段として運転者自身へ操作を戻し、安全回復が図られます。

AdaCore 社は、このアプローチを 2 つの側面から提案します。それは、（1）アプローチを段階的に実施すること（2）車両の安全性を損なうことなく新しい機能を追加することです。

既に、自動運転システムの形式検証に向けての法律、条例、道路交通規則の形式化に着手されていると思われます。この形式化はたいへん重要で、運転中の車両を監視し、安全基準違反が発生することが差し迫った状況かを判断する SFM を速やかに開発することができ、RTA の重要な基盤となります。車両の自立性を実装するために、RBS を開発されていると思います。その際の RBS の要件は形式化された法律、条例、道路交通規則から導くことができます。

開発が完了し検証済であれば、RBS は形式化された法律、規則、道路規則に従っているか運転中の遵守状況を確認する試験が可能です。導入後、RBS は SFM によって監視されているため、運転中に車両の安全性が損なわれることはありません。導入段階では、SFM が安全基準違反を検出した場合、運転者に車両の操作を戻すことがあります。

突き詰めていくと、ACS を開発、導入される場合、形式検証を行うのは困難で、かつ完全にテストすることは不可能と言えます。ただし、ACS は、RBS よりも高性能で、乗客の快適性や燃費の向上等が図られます。そのため、このシステムは実用上最良なものと言えます。

RTA は、ACS のテストが終了し導入が完了するまでの間、継続的に車両の安全性を確保します。SFM は安全基準違反が発生することが差し迫った状況を検出した場合、車両制御を RBS に移行し、回復操作を行います。回復操作が行われたこと、ならびに車両の操作を運転者へ戻す必要があることが警告されます。

AdaCore 社はお客様と、まず初めにサンプルとなる一つの法律、条例、あるいは道路交通規則を選択いただき、形式検証された SFM と車両制御規則を開発することをご提案します。AdaCore 社は SFM 向けに、形式化された要件と SPARK 言語で記述されたモニタを開発し、形式化された要件が例題の法規に合致しているか、モニタの実装がその要件を満たしているのか検証します。また、振舞制御規則のための形式化された要件を作成して、その要件が、例題の法規を満たすかも検証します。

AdaCore 社は自動運転向け RTA の手法を提供できる唯一の企業です。

注 1：Sha, L. et al., “The Simplex Architecture: Analytic Redundancy for Software Fault Tolerance” in Proceedings of the First International Workshop of Responsive Control Systems. 1991

注 2：Lee, I. et al., “Runtime Assurance Based on Formal Specifications.” Departmental Papers (CIS). 1999

お問い合わせ先

IT Access®
アイティアクセス株式会社

本社　〒222-0033 神奈川県横浜市港北区新横浜 3-17-6
TEL: 045-474-9095　FAX: 045-474-8823
E-mail: info@itaccess.co.jp URL: http://www.itaccess.co.jp

2018.9