Title: JST/CREST Project and Modeling Language for Scenario-based Safety Analysis

Abstract:

We are working on practical applications of formal methods to automotive systems. We successfully applied the formal methods to basic software including automotive operating systems such as OSEK/VDX, Classic AUTOSAR, and Adaptive AUTOSAR OSs so far. We would like to extend our target to more modern automotive system platforms, in particular, those for automated driving systems (ADS). The modern automotive system consists of AI for perception and planning, control, and basic software for high-performance computing. Recently, our project titled 'Formal Methods and Verification Tools for Next-generation Automotive System Platforms' which focuses on such modern automotive systems has been accepted by JST/CREST. This project aims at proposing formal methods and verification tools to ensure the safety and reliability of next-generation automotive system platforms. These formal methods and verification tools cover the perception to control functions, and we stick in their practical application to real systems. In the first half of this talk, I would like to introduce the overview of the JST/CREST project.

In the second half of the talk, I would like to focus on our scenario modeling language which is one of techniques being proposed in our project. In practice, the safety of ADS is assessed based on scenarios as shown in ISO 34502. The scenarios represent under-approximation of the whole situation that the system is operated. Thus, it is necessary that the scenarios sufficiently cover important situations; however, it is challenging since the number of the scenarios is huge. We think that one idea to mitigate this problem is to provide the comprehensive and compact representation of the scenarios, which allows us to effectively review it as well as generate scenarios. So far, we proposed a scenario modeling language named CPD (Car Position Diagram) and its scenario generator GCPD based on a SMT solver.

Several standards about scenario-base safety analysis have been proposed recently. JAMA (Japan Automobile Manufactures Association) published Automated Driving Safety Evaluation Framework. In this document, cognitive, traffic, and motion disturbances are systematically analyzed, and their variations are exhaustively defined by matrices. Each of elements of the matrices represents a scenario; however, it contains ambiguity which comes from visual notations used in the document. ISO 34502 which is defined based on JAMA's framework uses zone-graphs to visually describe scenarios (Annex E). The zone-graph is more formal than the visual notation used in JAMA's framework; however, there is still room for improvement from my point of view. We are formalizing scenarios appearing in these standards using our CPD/GCPD now. In this talk, I would like to discuss how we should deal with such scenarios based on our modeling language.