IIS-090
Embedded Computing Safety: Architectures and Design Tactics

Philip Koopman
Associate Professor, Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA

Priya Narasimhan
Assistant Professor, Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA

Abstract

Designing to achieve acceptable extra-functional qualities such as performance, dependability, and safety is a difficult task, especially for cost-constrained embedded systems such as those found in automobiles. A model of safety quality attributes would enable making progress in automating the evaluation and eventual synthesis of systems that achieve safety design goals as an intrinsic property of the design. But to do this, several issues must be addressed, such as how we formulate safety requirements, what measures we use to evaluate those requirements in an architecture, how we derive a model from the architecture, and how we specify architectural decisions that may improve safety in a software system. This first effort in this direction will identify safety quality scenarios and safety architecture design tactics used or plausible for use in existing automotive product designs. A second year effort is anticipated that will use these results to create a safety model amenable to automated analysis.