Safe Composition through Dynamic Feature Interaction Resolution

Submitted by Eunsuk Kang on Tue, 04/20/2021 - 4:12pm. Contributor:
Eunsuk Kang

ABSTRACT

The *feature interaction* problem occurs when two or more independently developed components interact with each other in unexpected ways, causing undesirable effect on the system performance and safety. For instance, a pair of safety features in a vehicle may attempt to send conflicting acceleration commands to the engine controller, potentially violating a safety requirement that would have been satisfied if each feature had existed in isolation. Feature interactions are major obstacles to building large, complex systems out of heterogenous components, and pose new challenges in emerging cyber-physical systems (CPS), such as intelligent vehicles, unmanned aerial vehicles (UAVs), and the Internet-of-Things (IoT).

In this talk, I will describe our on-going work on techniques for safely managing and resolving undesirable interactions between CPS components [1, 2]. I will first introduce the state-of-the-art methods for managing feature interactions and argue that the existing approaches are not sufficient to deal with the highly dynamic, evolving nature of modern CPS domains. I will then describe a new type of approach called *context-driven resolution* that leverages techniques in runtime verification and synthesis to dynamically detect and resolve undesirable interactions. I will describe how our approach is capable of resolving interactions even when (1) the system evolves over time with newly added or modified features, and (2) none of the conflicting features may be satisfactory with respect to the overall system safety. I will demonstrate our approach using case studies on safety features in autonomous drones and intelligent vehicles. I will also present some of the remaining challenges and future directions towards enabling safe, seamless composition of heterogenous CPS.

[1] Gafford, B., Durschmid, T., Moreno, G.A., Kang, E.: Synthesis-based resolution of feature interactions in cyber-physical systems. In: IEEE/ACM International Conference on Automated Software Engineering (ASE) (2020)

[2] Raghavan, S.G., Watanabe, K., Kang, E., Lin, C., Jiang, Z., Shiraishi, S.: Property-driven runtime resolution of feature interactions. In: International Conference on Runtime Verification (RV) (2018)

Eunsuk Kang is an Assistant Professor in the Institute for Software Research, School of Computer Science at Carnegie Mellon University. His research interests include software engineering and formal methods, with applications to system safety and security. His expertise is in leveraging formal modeling techniques, design methodologies, and automated verification to construct secure and reliable software and cyber-physical systems (CPS), and he has applied his work to a diverse range of systems, including intelligent vehicles, unmanned aerial vehicles (UAVs), medical devices, water treatment plants, and mobile applications. For his work, he has received two ACM Distinguished Paper Awards (FSE 2016, ICSE 2015) and a Best Paper Award (at IEEE/ACM Internet of Things Design and Implementation Conference, 2017).

Other available formats:

Safe Composition through Dynamic Feature Interaction Resolution

Switch to normal viewerSwitch to experimental viewer

Presentation HCSS 2021