Synthesis and Verification of Dynamic Assurance Cases for Self-Adaptive Systems

Radu Calinescu and Ibrahim Habli
Department of Computer Science
University of York

This PhD project will develop a suite of tool-supported techniques for the continual run-time synthesis and verification of dynamic assurance cases for self-adaptive systems used in safety-critical applications.

Self-adaptive systems can dynamically adjust their architecture and parameters in response to events such as workload changes and component failures. This capability is in great demand in autonomous systems, and has potential applications in safety-critical domains ranging from manufacturing and healthcare to transportation and finance. However, this potential is currently underachieved because of challenges associated with the development of assurance cases for self-adaptive systems. In particular, the traditional method of devising assurance cases prior to system deployment is not applicable to self-adaptive systems, for which some of the required assurance evidence is unavailable until run time.

The project will develop techniques and tools for automating the dynamic generation of assurance cases conforming to the OMG Structured Assurance Case Metamodel (SACM) standard[1] through the integration of both design-time and run-time evidence about the safe operation of the self-adaptive system. The project will extend our recent research on engineering trustworthy self-adaptive software using dynamic assurance cases[2] with: (a) techniques for generating and continually updating machine-readable SACM assurance arguments; and (b) techniques for verifying the correctness of the generated dynamic assurance cases.

[1] Object Management Group. Structured Assurance Case Metamodel™ (SACM™) v2.0 - Beta, July 2017.

[2] R. Calinescu, S. Gerasimou, M.U. Iftikhar, I. Habli, T. Kelly, D. Weyns. Engineering Trustworthy Self-Adaptive Software with Dynamic Assurance Cases. *IEEE Transactions on Software Engineering* **PP**(99):1-31, 2017.