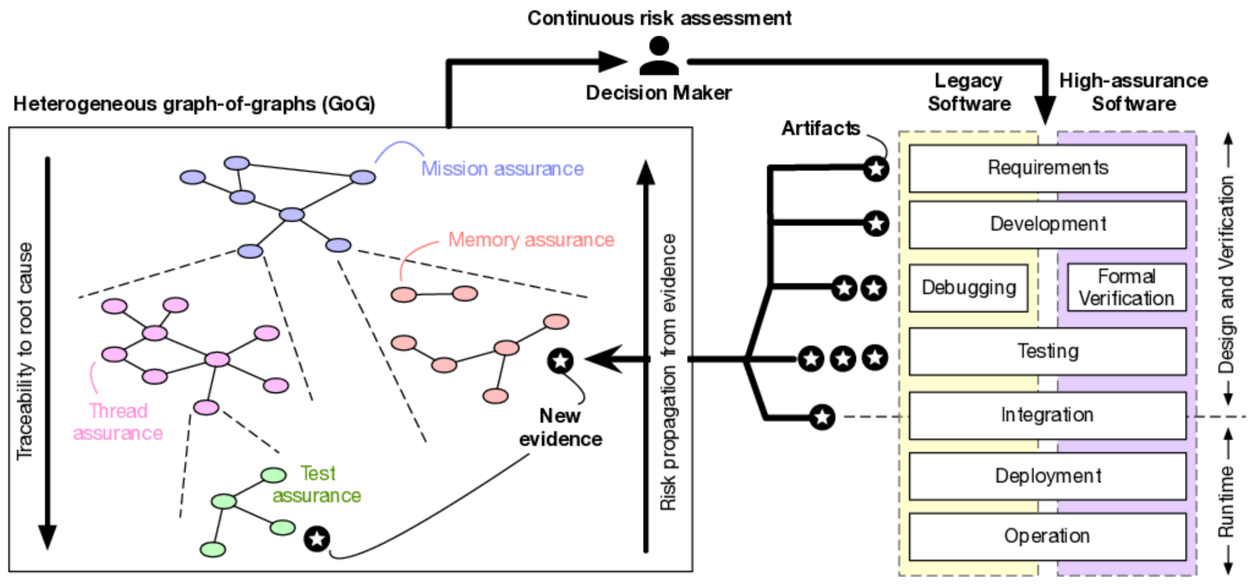
ACE: Assurance, Composed and Explained

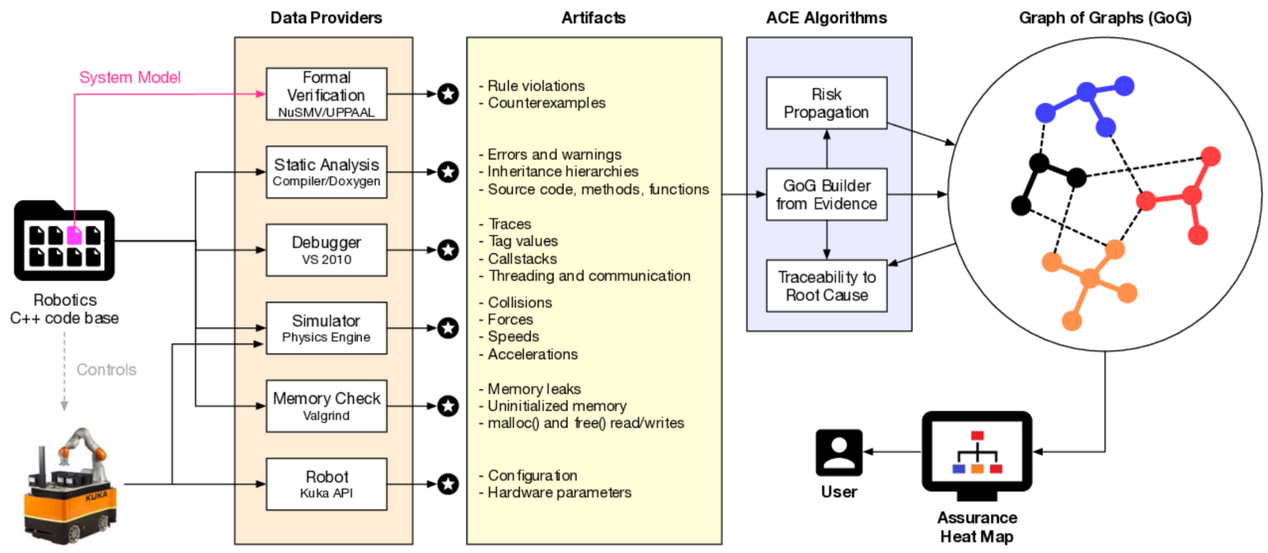
Gustavo Quirós, Arquimedes Canedo, Sanjeev Srivastava, Wei Xia, Pranav Kumar, Amar Kannan
Siemens Corporate Technology, Princeton, NJ
gustavo.quiros@siemens.com

Goals

- Quantify and expose the assurance and risk of safety-critical systems across their components using information from multiple sources of evidence.
- Close the gap between traditional engineering and formal methods to better assess the cost/risk trade-off of system assurance.
- Help to concentrate verification and validation efforts by guiding design and implementation improvement while supporting the isolation and solution of errors.
- Combine reasoning with uncertainty and static analysis techniques for quantified and supported metrics for assurance and risk for system components with or without formally verifiable models while considering multiple assurance aspects.



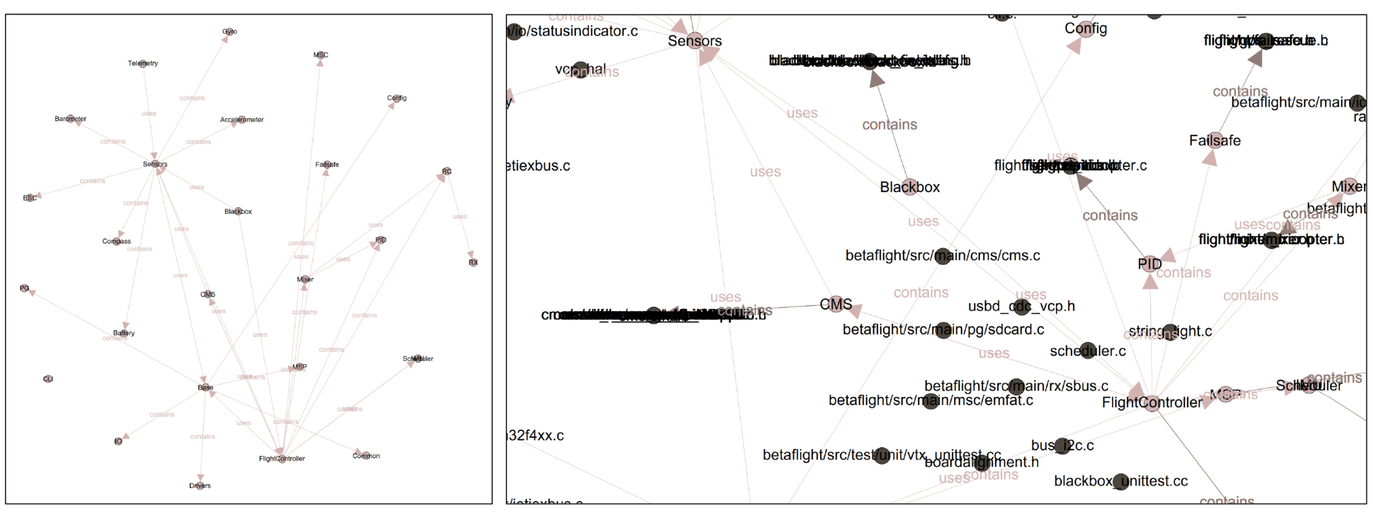
Approach



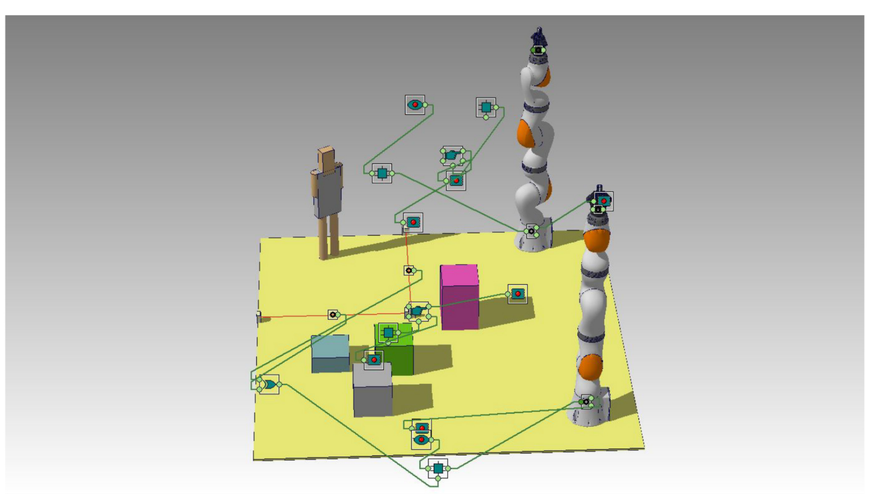
- Continuously integrate data from multiple artifacts from the design and verification phase into a heterogeneous graph-of-graphs (GoG).
- Implement a collection of data providers (e.g. static analysis, code management/repository, C/C++/C# parsers, architecture UML model)
- Define the ACE ontology as the underlying data model of the GoG.
- Compute assurance and risk quantities based on Evidence Theory to provide a continuous risk assessment capability.
- Formulate algorithms for propagating the risk quantities across the GoG based on Canonical Belief Propagation by message passing.
- Provide an assurance heat map of the system where risk hotspots can be identified interactively by the user.
- Provide automatic tracing of assurance issues to their root causes.
- Demonstrate the capabilities of ACE on two use cases: industrial robot control with human safety, and reliable flying drone control (Betaflight).

Evaluation

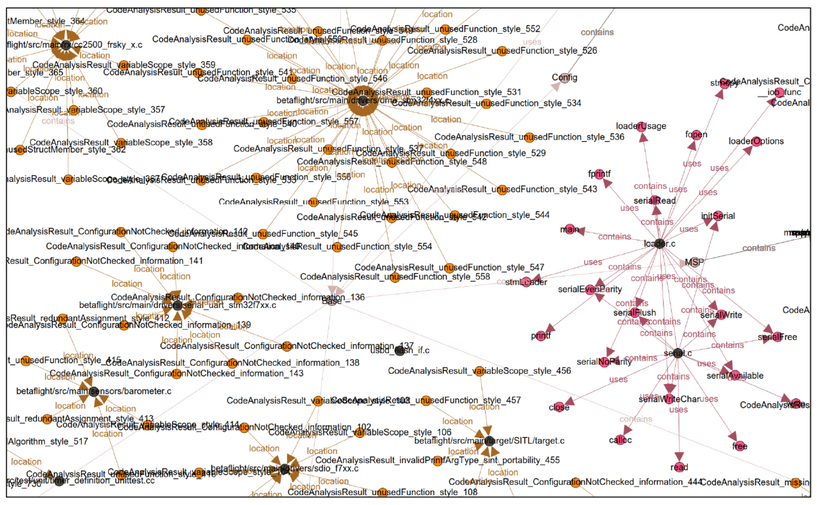
Composed Graph Data from Betaflight Use Case (21107 nodes, 15442 edges)



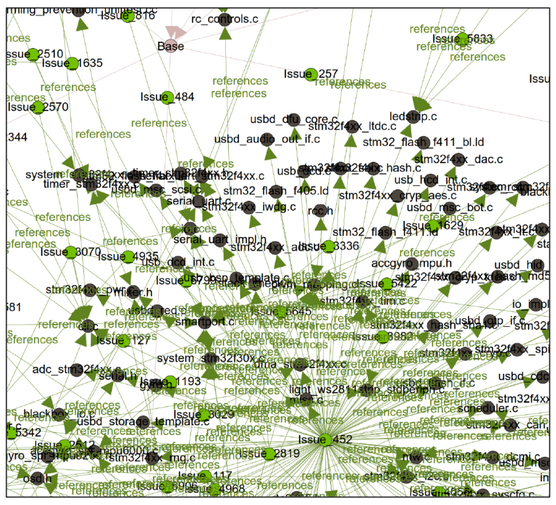
Simulation of Shared Environment for Robots and Humans



Architecture



Architecture + Source Files



Architecture + Source Files + Code + Static Analysis

Architecture + Source Files + Code Management Issues

Web-Based UI with Interactive Assurance Heat Map

This material is based upon work supported by the Defense Advanced Research Projects Agency (DARPA) and Space and Naval Warfare Systems Center, Pacific (SSC Pacific) under Contract No. N66001-18-C-4059. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and not necessarily reflect the views of DARPA or SSC Pacific.

SIEMENS
Ingenuity for life