Assurance Evidence for Continuously-Evolving Real-Time Systems Workgroup ASERTW

Dionisio de Niz

https://www.asertw.org

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-1151

Motivation

Improve certification of continuously evolving real-time systems

- Increase the certainty of correct operation
- Reduce the time to achieve certification for each evolution

ASERT Workshop:

- WHO: Government, industry, and academia that
  - Produce evidence (e.g., from real-time analysis)
  - Develop real-time systems
  - Consume evidence for certification
- Topics
  - Re-cetrification
  - Automation
  - Argumentation
  - Transition

Re-Certification

Argument Evolvability

- Argumentation of large-scale systems
  - Incremental argumentation and evidence collection
  - From early stage to final product
- Minimize argument modifications for each evolution

Tool Support

- Streamline argument modification

Design for Evolvability

- Modularization of Functionality and Arguments
  - Minimize impact of change across functionality
  - Minimize impact of change across arguments

Automation

For Evolvability

- Automatic change impact analysis / propagation
- Prevent unintended impact

For Scalability

For Objectivity

- Prevent incorrect input
- Prevent ambiguous argument interpretation

Argumentation

Multiple Appraisal Dimensions

- Different certification communities
  - Security, Safety, Nuclear Surety, Airworthiness
- Different points of view for similar arguments

Argumentation for Evidence Appraisers

- High-level claims derived from low-level arguments and evidence

Argumentation for Evidence Producers

- Low-level arguments and evidence
- Analysis domain experts

Argumentation for Developers

- Low-level connection with “code”
- Low Analysis expertise

Transition / Adoption of Formal Argumentation

Incremental

- Gradual adoption in different aspects

Standards

- Needed to join forces and adoption

Multiple Levels of Rigor

- Apply appropriate rigor to different functionalities

Continuous Evolution

- Should align to continuous evolution efforts (devops / agile)

ASERT Workgroup

Published Report

Defining Agenda

https://www.asertw.org