



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

Dionisio de Niz

<https://www.asertw.org>



Copyright 2022 Carnegie Mellon University.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

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-certification
 - 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>

