



High Confidence Software (HCS)

Chuck Howell

703-983-7615 • howell@mitre.org

Jim Moore

703-983-7396 • moorej@mitre.org

MITRE Sponsored Research

**MITRE
Technology
Program**

Problem



- **Software is brittle; assurance cases for critical systems are even more brittle.**
- **Incremental evolution of a system would ideally require incremental revalidation, but we are nowhere near this for critical software-intensive systems.**
 - **Breakage is caused by feature interaction, violation of implicit assumptions, exposure of latent defects, poorly structured assurance cases, ...**
 - **Despite acknowledged problems for current systems, anticipated adoption of new technologies presents even more challenges for assurance.**

Background



Before Software Upgrade



Ariane-5 failure due to software

- Inertial Reference System (IRS) was certified in Ariane-4 program
- Changes were minimized to avoid risk of breakage
- New code was extensively tested

After Software Upgrade



Failure occurred in the certified IRS because Ariane 5 flight envelope was different than the tested envelope - *implicit assumptions of the code were violated*

The failure of the IRS itself was non-consequential - it was the error notification method that caused the catastrophic failure. *This was an unanticipated interface of the IRS.*

Objective



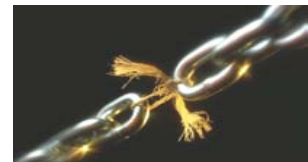
- Series of distinct investigations related to the single concept of incremental revalidation of an evolving critical system and its assurance case
 - Three-year effort
 - Build HCS community of interest in MITRE
 - Establish MITRE as a national resource in HCS
- Rules of engagement:
 - Must reflect MITRE's roles and interests
 - Must be incrementally adoptable

Activities



- **Selected initial notation and tool for assurance case support; applying it to safety and security frameworks; looking at extensions to tools and notation**
 - Exploring application to DOD OT&E evaluation, Navy DDX AGS, NCES, others
- **Investigated engineering basis for software test advisor, documented gaps and state of the practice**
- **New investigation: assurance for adaptive systems**
 - Exploring application to NCES, JTRS, others

Highlight



HCS_CASA.act - ASCE - Adelard Safety Case Editor

File Edit View Format Tools Windows Help

Check network structure

This checks the network for possible errors. The checks will not detect all anomalies.

Double-click on an item to see it in context

Object	Severity	Warning message
CLAIM: \Usage warning	3	Claim with no subclaim, argument or evidence link
ARGUMENT: \Apply recommended safety standards	2	Argument with no subclaim, argument or evidence link
ARGUMENT: \Historically safe	2	Argument with no subclaim, argument or evidence link
CLAIM: \Safety Management activities	1	Claim or evidence with direct evidence link
EVIDENCE: \Safety Review	1	Claim or evidence with direct evidence link
EVIDENCE: \PHA	1	Claim or evidence with direct evidence link
CLAIM: \Is safe now	1	Claim or evidence with direct evidence link

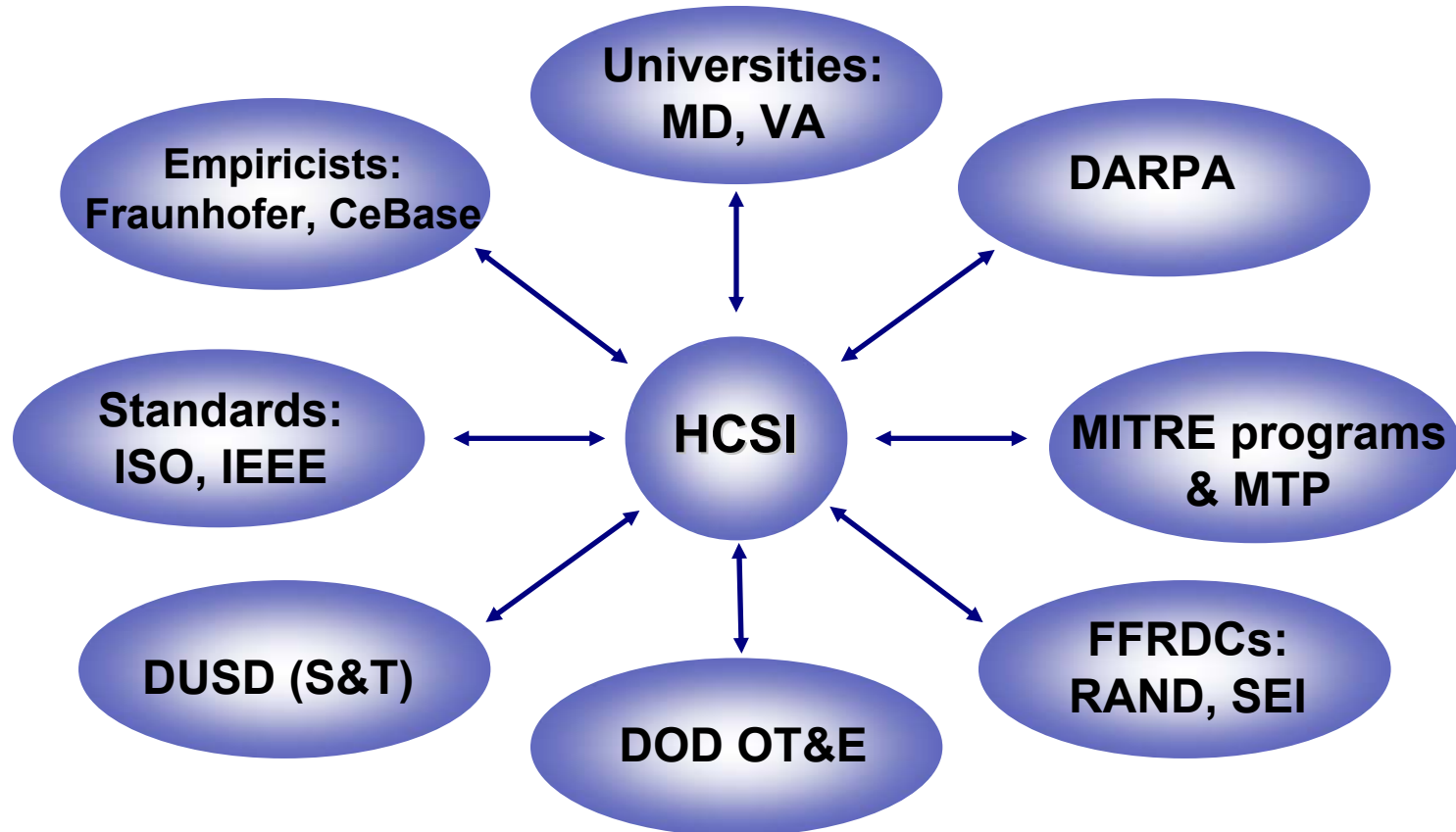
ASCE

The network check rules identify the following anomalies:

- Network circularities should not exist
- Claim with no subclaim, argument or evidence link
- Argument with no subclaim, argument or evidence link
- Claim or evidence with direct evidence link
- Floating claim
- Evidence with claim or argument as input

start | HCS_CASA.act - ASC... | Check network struct... | ME_CASA.txt - XEmacs | 11:29 AM

Highlight



Interaction with Other Organizations

Impacts



■ On our sponsors

- Enable them to develop and acquire critical software systems with greater predictability and reduced risk
- Allow them to adopt the technology in an incremental manner since they will never scrap everything and start over

■ On MITRE

- Leverage MITRE's engagement across a broad range of sponsors and systems to make a sustained contribution

■ On the software development community

- Contribute to the technology base
- Contribute to standards
- Encourage development of implementing products and tools

Future Plans



- **Research investigations**
 - **Assurance case management**
 - **Develop generic assurance case templates for safety and security frameworks, extend notations and tools for improved support**
 - **Adaptive systems**
 - **Investigate assurance techniques for one aspect of general adaptive systems: management of updates within large configuration space**
- **Internal engagement**
 - **“Adopt” (shadow) sponsor projects**
- **External engagement**
 - **Public workshop on assurance cases**
 - **Additional university and FFRDC collaboration**