NASA Software Assurance's Role in Research and Technology

Oct 26, 2010
TRISMAC
NASA Safety Center
Martha Wetherholt
Discussion

- Software Assurance – what it is to NASA
- Research and Technology Use of Software
- Research of New Software Technologies
- Research for Software Assurance
- The Future
What is Software Assurance?

Software Assurance is an umbrella risk identification and mitigation strategy for safety and mission assurance of all NASA’s software.

- SW Quality
  - Quality Engineering
  - Quality Control
  - Quality Assurance
- Software Safety
- Software Reliability

V&V
  - Process & Product

IV&V
Research and Technology Use of Software

- Software is often used to perform simulations and models to prove out ideas and concepts prior to proceeding to another level.
- Software is used to measure and record results
- Software can be used to control and monitor experiments
- Software used to analyze results and predict
- In this role it is critical that the models and/or simulations accurately depict conditions as well as criteria understudy.
- Focus would be on:
  - SW accuracy and limitation of models and or simulations
  - Ability to add, health monitoring to experiments w/o changing experiment
  - Speed and amount of data to be collected and processed
  - Software programmer’s understanding of needs of researcher
  - Researcher’s understanding of software’s capabilities and limitations
General, Graduated SMA Coverage

**Technology Readiness Levels Summary:**

- TRL 1 Basic Principles observed and Reported
- TRL 2 Technology concept and/or application formulated
- TRL 3 Analytical and experimental critical function and/or characteristic proof-of-concept
- TRL 4 Component and/or breadboard validation in laboratory environment
- TRL 5 Component and/or breadboard validation in relevant environment
- TRL 6 System/subsystem model or prototype demonstration in a operational environment (ground or space)
- TRL 7 System prototype demonstration in an operational environment
- TRL 8 Actual system completed and "Flight qualified" through test and demonstration (ground, airborne or space)
- TRL 9 Actual system "flight proven" through successful mission operations

**Center Institutional Safety Requirements**

- High Risk Test Facilities
- Labs
- OSHA
- Industrial Hygiene
- Fire/Life Safety
- Emergency Preparedness

**Awareness and insight both ways**

**Project dependent,**

*Area targeted for SMA improvements*

**NASA and Center SMA Requirements**

- System Safety
- Quality Assurance
- R&M
- Software Assurance
- Risk Management
Research and Technology Use of Software
TRL Level Discussion

TRLs 1-3: mostly paper concepts/theories, simulations, possibly Facility or bench top

TRLs 4-6: use of Facilities and some experimental build up, proof of concepts, where decision to go to flight demonstration is made

- Software usually written by researcher. SMA may or may not know of any software used in the experiment. If use a NASA Facility to prove out, then must follow facility restrictions and safety requirements.
- Software involvement more extensive and used to monitor and control experiments. Also to analyze results
- As SW becomes more relied on, need to involve SA must be considered to make sure results can be trusted, safety parameters are met and held, possible new software methods are verified.
- SA participates on varied basis based on need/risk which has to be assessed individually
- Project needs to meet flight development requirements for engineering and SMA already in place.

Throughout, SMA should gain insight and prepare for possible advancement of technology.
Research of *NEW* Software Technologies

- Software itself is constantly changing, evolving
- How software development is performed
  - Models to code (e.g. UML), auto code generation,
  - New emphasis on architecture paradigms and schemes for certain kinds of SW systems
  - Autonomy
  - Cloud computing
  - Etc.
- What does software run on, what *will* it run on?
  - Platforms, OS
  - The FPGA, ASIC, CPLD debate and what else?
  - Parallel processing
  - Distributed networks
  - Systems of systems
  - Net and phone based technologies
- So, how does SW Assurance keep up?
Research for Software Assurance

OSMA has its own **Software Assurance Research Program** (SARP)

- Funded and overseen by OSMA
- Run out of NASA’s IV&V Facility
- Yearly Agency-wide survey of SA needs as basis
- Internal and external researchers
  - Center based research
  - Academia
  - Industry
- Peer review of all proposals
- Selection via executive committee
- Selections made and followed up on to assure success (incl. yearly public presentation)
- Most projects are for 3 years
- Technology Transfusion for most promising techniques, processes, etc.
SW Assurance Research Program

OSMA SW Assurance Research

- ~$3M into SARP annually
- 12-20 Center projects in any one year
- Usually fund each for 3 years
- The most promising research gets and additional year or 2 for SW Technology Infusion
- Sometimes we can go outside and have academic projects

Sample Research we fund or have funded:
- Contingency SW in Autonomous Systems
- SW Process Assurance for Complex electronics
- Analyses of defect data and defect detectors
- Model Checking of Artificial Intelligence Planners
- Testing framework for reproducible execution & race condition detection in real-time embedded systems
- Interface Validation for Distributed Software Systems – Phase II
- Test Coverage Analysis – A Tandem Experiment using Available Prototypes
- Research and Development of Deployable IV&V Methods for FPGA Applications
SMA considerations for R&T Projects
(Right tools, right time, right extent)

- Criteria for determining S&MA level of involvement [e.g.]
  Pure "paper studies" or data mining may not need S&MA involvement but awareness may still be needed.
  - Current TRL level
  - Difficulty scale to advance technology ("is it a hard nut to crack?"), complexity
  - Risks & risk tolerance (analyzing/managing uncertainties)
  - $$
  - Verifiable outcome
  - Damage likelihood
  - Impact of failed research (including public opinion)
    - Who cares and how much do they care?
  - Potential for future growth/development
  - Ability to test
  - Path to build with reproducibility
  - "Period of performance" drivers?
SW Assurance considerations for R&T Projects
(Right tools, right time, right extent)

1. **Degree of Control:** The degree of control that the software exercises over safety-critical functions in the system.

2. **Complexity:** The complexity of the software system. Greater complexity increases the chances of errors.

3. **Timing criticality:** The timing criticality of hazardous control actions.

4. **Likelihood** a hazard would occur

5. **Severity** of a potential hazard – always take the worst possible case

6. **Reliance on Software** to determine successful experiment determination or operation of a demo

7. **Need for repeatability**

8. .....
Challenges - Change the Paradigm

- Same as rest of SMA only more so.....
- Each Researcher sees software as their tool to perform or analyze their project
  - Inconsistent approach to how software is written, maintained and used
  - Software not even considered as something that needs to be considered in it's own right
- R&T sees any involvement in SW development itself as potential "road blocks"
  - Expensive and slow
  - Unnecessary
  - Seen as one size fits all
  - We just don't understand their problem... which we may not!
- We need early involvement and awareness to avoid becoming a roadblock if and when the project moves up the TRL scale.
- May be able to point out helpful innovations in SW technologies and methodologies
- Still, We, SA, need to understand the science, technologies, complexities, and risks in order to advise the R&T communities of what SA can do for them.
- Need to shift the paradigm to seeing us as a time and expense savings, not a mindless requirements enforcer ad then live up to that!!
Summary (Cont.)

We need to “Change the Paradigm”:

- Work with the rest of SMA to improve communications & understanding as well as create Training and Awareness Campaigns
- Increase visibility and presence with a questioning interest in what they are trying to achieve
- Make sure Researchers are aware of the benefits of all aspects of S&MA contributions including SA – how do we quickly show them some direct benefits to their project from use of the right software processes for them
- Make sure Software Assurance personnel are aware of the differences in our roles and responsibilities in an R&T environment - keep a light hand in, but keep them safe and help them achieve their goals
- Walk the talk