STANDARDS APPLICATION – CERTIFICATION OF ADAPTIVE SYSTEMS

Raj Bharadwaj

Oct 19, 2015

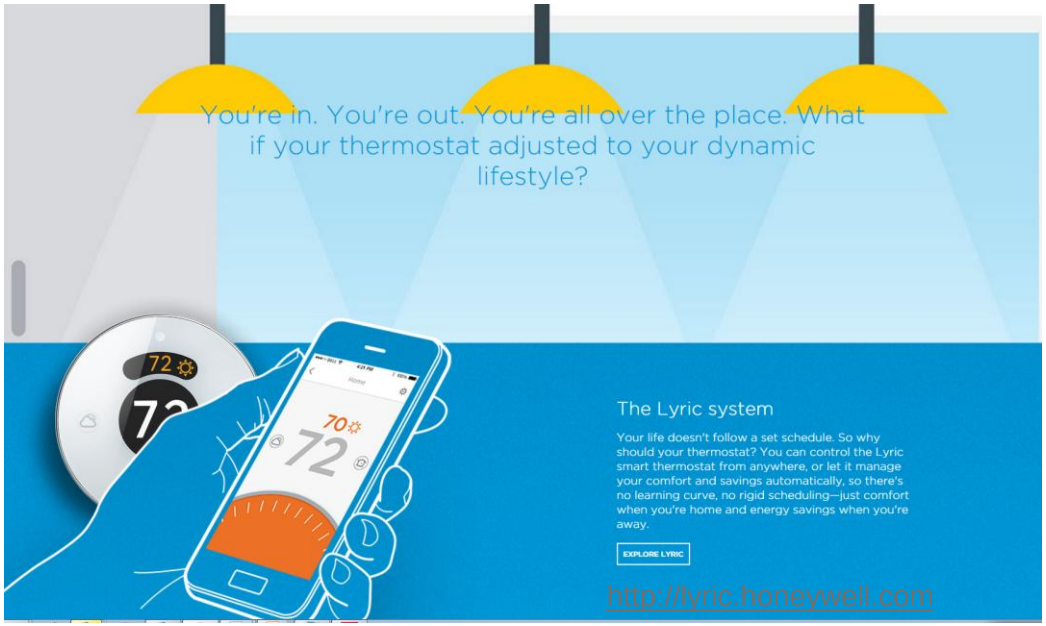
This work was performed under NASA Flight Critical Systems Research Contract NNL06AA05B.
We would like to thank Kelly Hayhurst at NASA for her support and encouragement

Acknowledgements: Chris Wilkinson, Jonathan Lynch (Honeywell)

phmsociety

Honeywell

Adaptive Systems



- Adaptive Systems are all around us
- Search engines and phone make recommendations, thermostat learns, vacuum cleaners move around objects and pets on the floors
- Lot of work has been done on Autonomy in aerospace yet there are no certified Adaptive Systems

Approach for Adaptive System Certification

- Reviewed several types of adaptation and adaptive system
- Focused on a generic and representative adaptive flight control. Excluded gain scheduled AS.
- Defined some basic principles for a system and software design assurance to assure safe use
- Concluded that using only DO-178B would not be adequate – could not meet our principles
- Expanded our investigation to DO-178C and supplements
  - Could those methods address the identified difficulties and follow our principles?
  - Revised our list of objectives to DO-178C Annex A
- Defined what system level functional and safety properties would be needed for example AS– list constraints, convergence, fail safe policies
- Defined what activities and techniques could be used to satisfy the DO-178B/C objectives

http://ntrs.nasa.gov/search.jsp?N=0&DocumentID=20140000469

Conclusions

- Software design assurance alone is inadequate to assure the safe application of adaptive systems
- The safe use of adaptive systems begins at the system level with the constraints on the architecture and permitted adaptation
- The constraints assure that the adaptive system exhibits certain safety properties and assures an acceptable level of safety
- Need to establish and satisfy system safety objectives that are AS-specific
- AS must exhibit certain system level properties to ensure an acceptable level of safety that can be represented mathematical (Model)
- Model should express requirements for functional and safety properties

Encode behavior in mathematical models

Recommendations

- Software design assurance using DO-178C and MBD, FM supplements
- Use DO-330 TQ compliant tools
- Multi-layered verification methods are necessary involving test, analysis/simulation
  - Certification process will need to accept non-traditional means of compliance with certain 178C objectives
    - More reliance on formal analysis/simulation than test
  - Learned state space is too rich to adequately test
- MBD/FM does not obviate testing but can usefully
  - Highlight corner test cases
  - Identify pass/fail criteria, predict expected results
- DO-178C supplements do not need additional or changed content

Existing methods can be used

BACKUP

phmsociety

Honeywell

Focus