Engineering Resilient Space Systems: Leveraging Novel System Engineering Techniques and Software Architectures

30 July to 3 August 2012

Mitch Ingham, John Day, Len Reder - JPL

Richard Murray – Caltech

Brian Williams - MIT

ENGINEERING RESILIENT
SPACE SYSTEMS

Attendees

- Ella Atkins – Univ. of Michigan
- Kevin Barltrop – JPL
- Erv Baumann – Northrop-Grumman
- George Cancro – JHU/APL
- John Day – JPL
- Kenneth Donahue – JPL
- John Doyle – Caltech
- Tara Estlin – JPL
- Lorraine Fesq – JPL
- Kim Gostelow – JPL
- Gerard Holzmann – JPL
- Andrew Ingersoll – Caltech
- Mitch Ingham – JPL
- Joseph Kochocki – Draper Lab
- Azad Madni – USC
- Richard Murray – Caltech
- Necmiye Ozay – Caltech
- Robert Rasmussen – JPL
- Leonard Reder – JPL
- Abhinav Saxena – Ames
- Thanos Siapas – Caltech
- Janos Sztipanovits – Vanderbilt U.
- Leslie Tamppari – JPL
- David Thompson – JPL
- Eric Timmons – MIT
- David Wang – MIT
- Brian Williams – MIT
- Huan Xu – Caltech

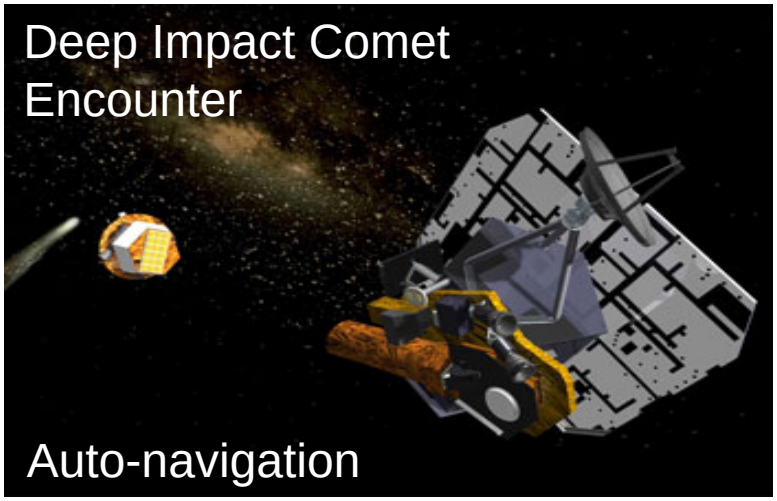
Keck
INSTITUTE FOR SPACE STUDIES

ENGINEERING RESILIENT
SPACE SYSTEMS

ENGINEERING RESILIENT
SPACE SYSTEMS

Setting the Stage

- Future space missions will require the conception, development and operation of spacecraft with unprecedented ***resilience***
  - *ability to achieve science objectives even if spacecraft performance, health or environment are not as expected*.
- Limited examples in systems that have already flown:



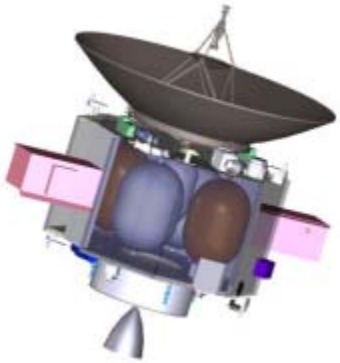
Keck INSTITUTE FOR SPACE STUDIES

ENGINEERING RESILIENT SPACE SYSTEMS

Future (Inter)Planetary Missions

- Venus In-Situ Explorer
  - very short lifetime before extreme atmospheric environment kills spacecraft
  - critical onboard decisions about samples and measurements
  - rapidly-degrading performance of spacecraft and instruments

- Trojan Asteroid Tour and Rendezvous
  - fly by multiple small bodies at very high velocity
  - tiny window for unspecified measurements of asteroids' poorly characterized environments



- Extrasolar planetary probe
  - exceptionally long mission lifetime and distance from Earth
  - completely mysterious environment at its destination
  - full autonomy and unprecedented resilience

NOTE: The Planetary Decadal Survey will be discussed in more detail today by Andy Ingersoll!

Keck INSTITUTE FOR SPACE STUDIES

ENGINEERING RESILIENT
SPACE SYSTEMS

What We Have Today

- "Brute force" – preserve spacecraft in known environments and in response to internal faults
  - hardware redundancy
  - shielding
  - hundreds of pre-programmed 'reflexes'
  - large technical margins
- Significant costs across multiple dimensions, e.g., power, weight, complexity
- Limited effectiveness in addressing environmental uncertainty
- Limits classes of missions we are capable of pursuing, and increases risk

Keck INSTITUTE FOR SPACE STUDIES

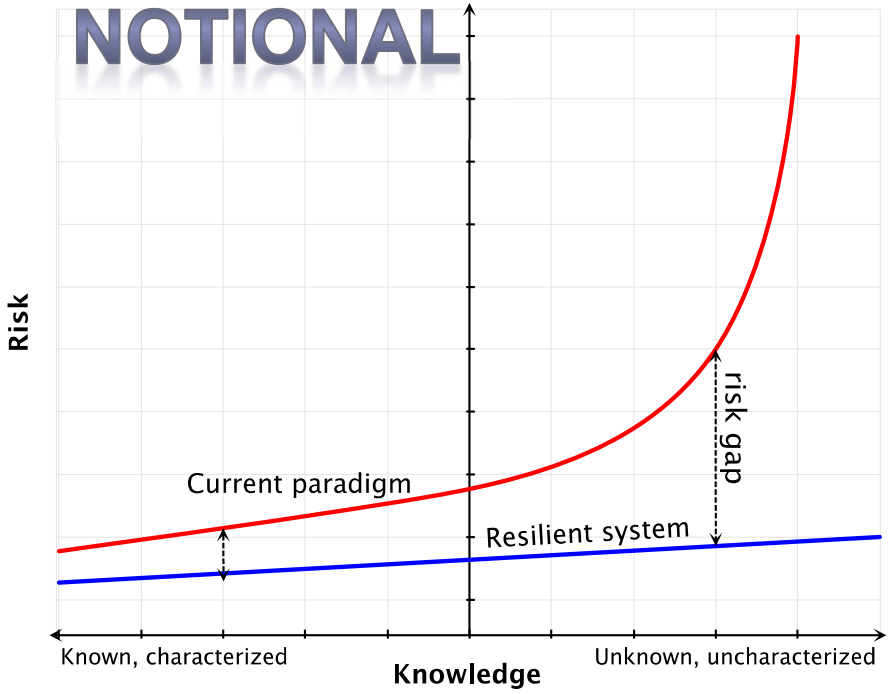
ENGINEERING RESILIENT SPACE SYSTEMS

What We Need

Our Claim:

- Resilience for missions like those described on slide 5 ***cannot be achieved by incrementally building on*** current state of practice
- Requires a ***fundamental paradigm shift*** in the way we conceptualize, design, implement, validate, and operate our systems

- Need a proper balance of:
  - reflex-oriented behavior, and
  - ability to comprehensively reason about current state of system and environment
- The challenge: effectively develop and deploy such capabilities in order to enable new classes of missions



Keck INSTITUTE FOR SPACE STUDIES

ENGINEERING RESILIENT
SPACE SYSTEMS

Study Goal

Determine a set of:

- System capabilities,
- System architectures and patterns,
- Software architectures,
- Autonomy technologies, and
- Systems engineering and Software processes

that have the best chance of realizing the needed resilience in future missions.

Keck INSTITUTE FOR SPACE STUDIES

Study Scope

Engineering Resilient Space Systems STUDY

Workshop #1 – July 2012

- Develop a Vision
- Characterize Problem – Discuss Needs
- Define Reference Missions
- Develop list of capabilities
- Select Themes for Exploration in the Study Period
- Plan Study Period

Study Period

- Explore Themes
- Develop Strategies
- Plan Workshop #2

Workshop #2 – Jan 2013

- Characterize solution space
- Refine study period results
- Develop proposal concepts

ENGINEERING RESILIENT
SPACE SYSTEMS

Envisioned Study Products

- ✓ Clear Vision Statement
- ✓ Slide package describing science needs and reference missions
- ✓ Description of the desired system capabilities
- ✓ Description of functions required for the new system capabilities
- ✓ Specification of unique architectural patterns and attributes to support these systems
- ✓ List of enabling software and autonomy technologies (e.g., middleware, languages, frameworks, algorithms, etc.)
- ✓ List of key processes for the agile and verifiable development of these systems and enabling the management of complexity
- ✓ List of recommended future capability and technology investments
  - Roadmap for future research and development programs
  - Which ideas need to be matured to enable truly resilient missions?

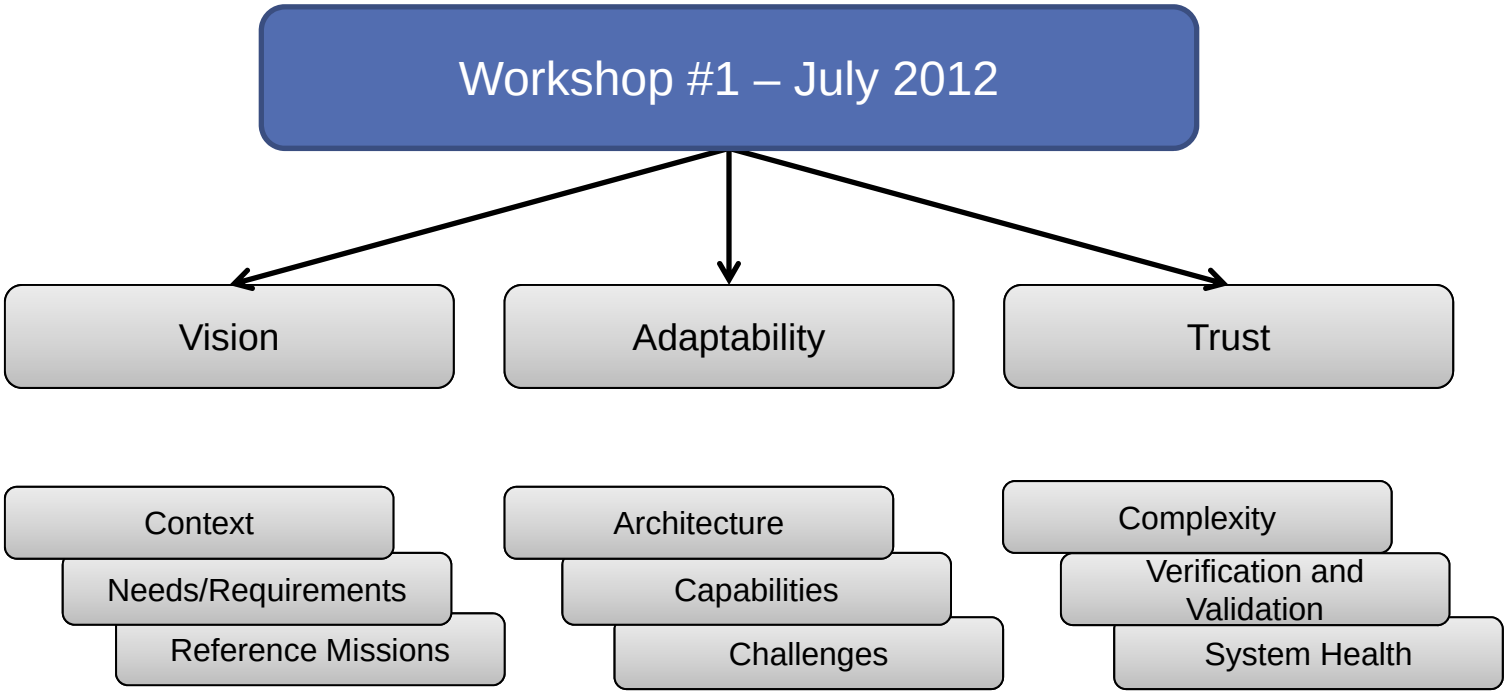
ENGINEERING RESILIENT SPACE SYSTEMS

Workshop #1 Goals

- Day 1: Vision
  - Establish a *vision* and conceptual basis for resilience in engineered systems
  - Document *science motivation* for resilience
  - Capture a set of driving *Reference Missions*
- Day 2: Adaptability
  - Establish key *architectural attributes* for adaptability
  - Document key *capabilities* for resilient systems
  - Determine *challenges* to realizing envisioned systems
- Day 3: Trust
  - Establish key *architectural attributes* for trustworthy resilience
  - Document *development-time and run-time* approaches for achieving trust in future resilient systems
- Day 4: Planning for Study Period and Workshop #2

ENGINEERING RESILIENT SPACE SYSTEMS

Workshop #1 Scope



Topics of Discussion

- Results of Planetary Decadal Survey
- Definitions of resilience
- Science needs
- Agile science ops
- Attributes of resilience
- Measures of resilience
- Biological analogues
- Uncertainty
- Self-preservation
- State awareness
- Dimensions of trust
- Measures of trust
- Development-time vs. run-time approaches
- Agile verification
- ISHM

Keck INSTITUTE FOR SPACE STUDIES

Workshop #1 Products

- ✓ Documentation of a clear *Vision statement*, compelling *science case* and set of *Reference Missions*
- ✓ Key *architectural attributes, principles, and patterns* for trustworthy resilience
- ✓ List of *challenges* to achieving trustworthy resilience
- ✓ Documentation of a core set of *capabilities* required to achieve trustworthy resilience
- ✓ Initial list of systems and software *engineering processes/approaches* that enable *development and operation* of trustworthy resilient systems
- ✓ Identified sub-teams to further refine these concepts
- ✓ Defined topics for the Study Period and Workshop #2, and a tentative schedule
- ✓ Final report outline and content ideas

Structure of Workshop

- Discussion sessions are structured to have a lead-in talk, followed by a moderated discussion
  - Provocative talks (45 to 60 min.) intended to stimulate a great deal of discussion
  - Context talks (15 min. or so) intended to keep a theme moving along
- We have volunteers (*thank you!*) to take notes in each discussion session
  - However, more help is certainly welcome – please contribute notes
- We have room to make adjustments in our agenda, expand or change discussion topics
  - Each day has a separate co-lead moderating
  - Moderator for the day will make the final decision on changes

ENGINEERING RESILIENT
SPACE SYSTEMS

Guidelines/Suggestions

- Productive discussion is key to our success
- Please share what you know
  - Don't fear to speak up and express yourself
  - If you don't know or understand something, ask a question
- Help us formulate provocative questions
  - Help us guide discussion topics with them
- Please do not be dismissive; every idea merits at least a few minutes of discussion
  - But the moderator reserves the right to move discussion along!
- Postdocs/students: you are part of our core group; ask questions, participate in discussions
- Think about your concluding lightning talks throughout the workshop days

Keck INSTITUTE FOR SPACE STUDIES

ENGINEERING RESILIENT
SPACE SYSTEMS

Example Provocative Questions

1. What are fundamental requirements that drive us to resilient space systems?
2. How much resilience is enough? Are there quantitative metrics to access this?
3. What are the challenges to realizing a resilient space system? Are they purely technological?
4. Can resilience be architected? Should it?
5. Does resilience require some form of redundancy?
6. Does resilience imply some level of “intelligence”?
7. Does resilience imply (additional) complexity?
8. How does the concept of resilience relate to dependability and adaptability?
9. What is the overhead for designing for resilience? Can it be measured? Can it be optimized?
10. Can we envision a long-lived (50+ year duration) resilient system that evolves using unsupervised learning and changes in its environment?

Keck
INSTITUTE FOR SPACE STUDIES

Engineering Resilient
Space Systems

ENGINEERING RESILIENT
SPACE SYSTEMS

More Provocative Questions

1. What is the sweet spot in the spectrum between reactive and deliberative (for resilience)? How much does the nature of the mission impact this balance?
2. Does designing for minimal function result in dramatically different architectures than designing for resilience?
3. What are the necessary properties for a resilient system to maintain stability? Is this purely a classical control theory requirement to keep poles on the left hand side of the S-plane or within the unit circle of the Z-plane or are there more?
4. Are there certain architectural topologies applied to resilient systems that can minimize the effect of failed interfaces and protocols within the system?
5. What is the definition of “state aware”? Is it a certain cognitive awareness of system health and an external sensing of operation environments? What are the attributes of the system state to be aware of?
6. Can we leverage low-cost spacecraft platforms like CubeSats to prove out resilience capabilities and technologies? What would be some relevant CubeSat Reference Missions?