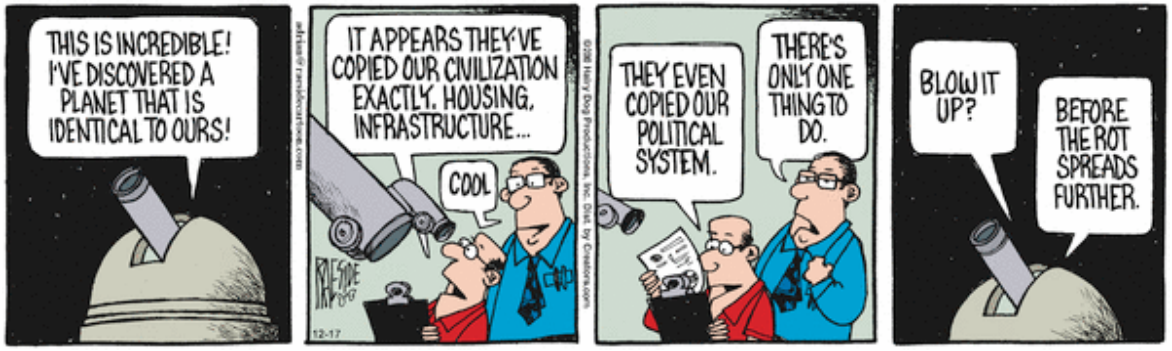
ENGINEERING RESILIENT SPACE SYSTEMS

Questions from the East… (Atkins)

- Reminder of the dictionary definition (the reference for the "common citizen"):
  - **Resilience**: ***an ability to recover from or adjust easily to misfortune or change***
- How do we optimize, not just specify by committee, our meta-level design approach or approaches to resilient spacecraft in terms of complexity, risk, trust, cost, etc.?
- Can we make resilient system design accessible to scientists and mission operators, and will this assist with buy-in?
- ***How can progress or even models/code developed for other domains (cars, planes, Earth-based robots) be translated to resilient spacecraft applications?***
- How does the next generation of student best prepare for the physics-based, logic-based, and systems-based skillsets needed for engineering resilient spacecraft systems?
- ***From my Washington DC locale… What is the risk of resilience for interstellar missions?***



Keck INSTITUTE FOR SPACE STUDIES

GOOD LUCK MSL!!!!!!!!!

ENGINEERING RESILIENT SPACE SYSTEMS

Baumann

1. What are the most interesting ideas you heard at the workshop?
   Gentry Lee's "3D-printer" comments, reconfigurable robots & programmable matter references, and John Doyle's "Universal Architectural Laws" and "constraints that unconstrain" observations
2. What is worth future investigation?
   At some level,everything that was discussed is worthy of further investigation at an appropriate time. However, I strongly suggest that in the next workshop we develop a preliminary time-line and roadmap that links the key technologies and associated capabilities in a phased development roadmap. This should help guide our thinking and provide an aid for conveying our development, test, and application plans to management.
3. What are the biggest hurdles to achieving our vision for resilient sys?
   - Developing a credible and easily understood phased development, test, and deployment strategy with useful technology milestones that is sync'd up with exploration objectives for the next 50 to 100 yrs.
   - Generating a convincing "cost-benefits-analysis" based on life-cycle affordability & quality-of-science benefits for extremely long distance and duration missions in increasingly unknown environments.
   - Simulations of high-fidelity(?) testing scenarios representing a credible set of "alien" environments.
4. Which topics or ideas do you want to champion?
   - Model-based health / fault management system design, analysis, and execution tools and methods
   - Model-based 3-D Printing and/or modular reconfigurable robotic systems in the longer term.
5. What are your takeaway action items?
   - Learn more about all of the topics discussed
   - Generate my own notional "resiliency enabling" technology development and milestone roadmap to stimulate and guide my thinking prior to the next workshop.
6. Are there any other topics that deserve discussion?
   - The nature, identification, and utilization of "dissimilar functional redundancy"
   - The pros and cons of using reconfigurable "swarms" of cubesats to increase resiliency

Keck INSTITUTE FOR SPACE STUDIES

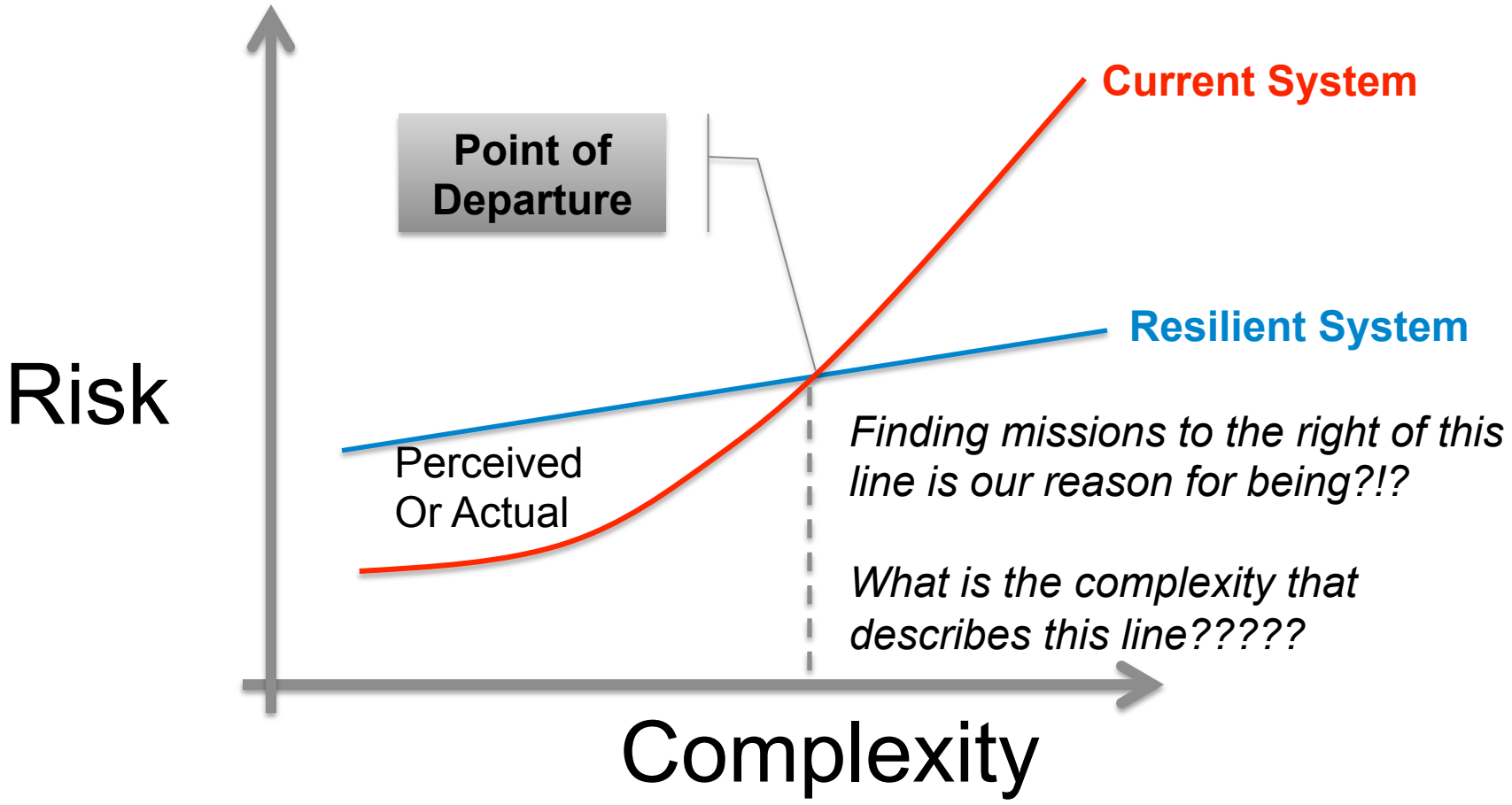
ENGINEERING RESILIENT
SPACE SYSTEMS

Bob's Castle Example

- Rasmussen "Robustness is like siege defense: Strong walls and plenty of supplies but not much freedom"
  - Very profound
  - We define a perimeter and then we defend to the perimeter…not even knowing whether our perimeter is sufficient (can't sufficiently test) and what is outside the walls (we can only validate through strawman scenarios that may not be the real enemy (environment) capability)
- NOW WHAT??
  - No one builds castles anymore…why? (What can we learn from this)
  - Can we move from siege defense to blitzkrieg or maybe guerilla warfare? (What the hell does that mean for us?)

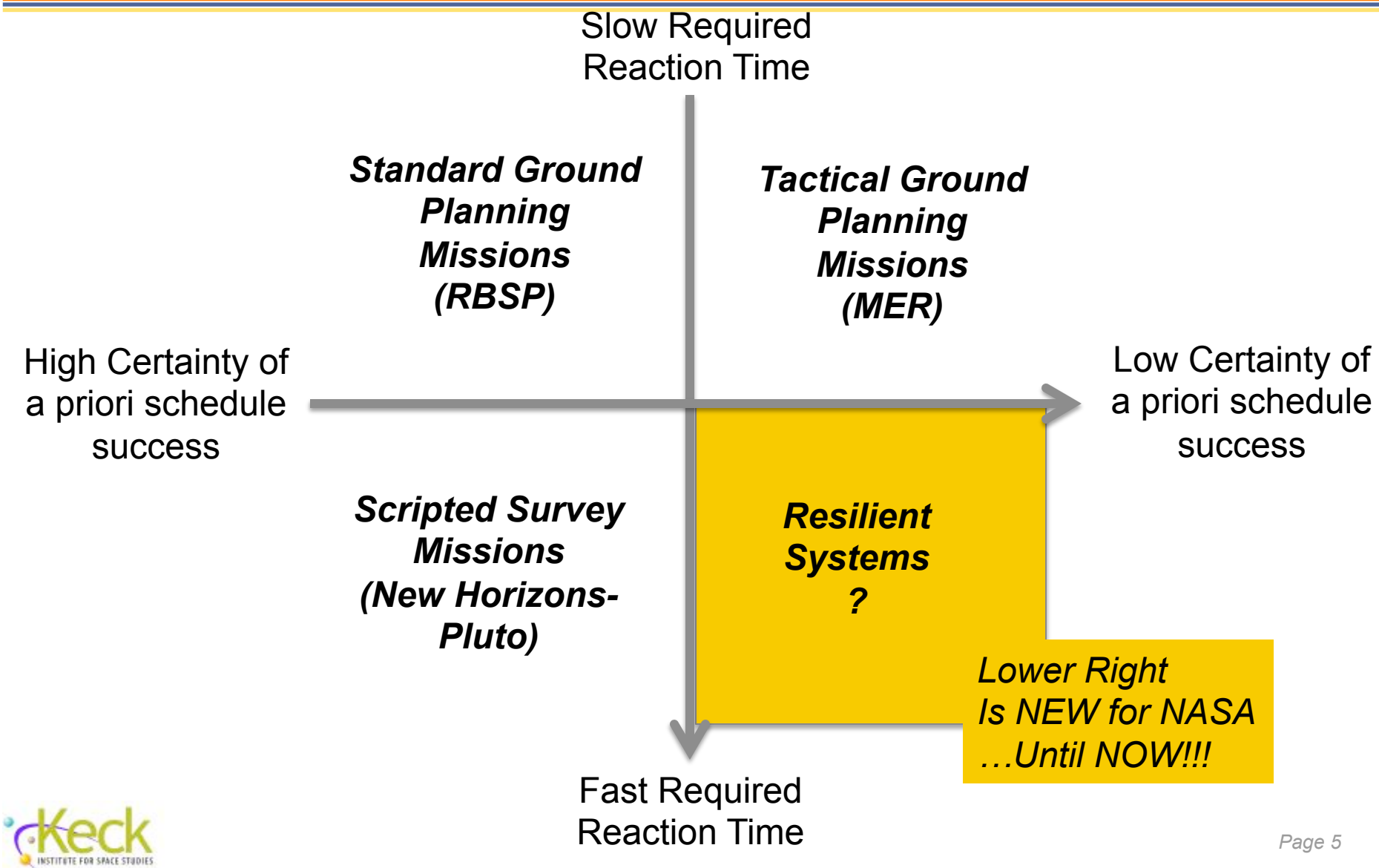
Keck INSTITUTE FOR SPACE STUDIES

Re-Framing The Mitch/John Diagram (Cancro)

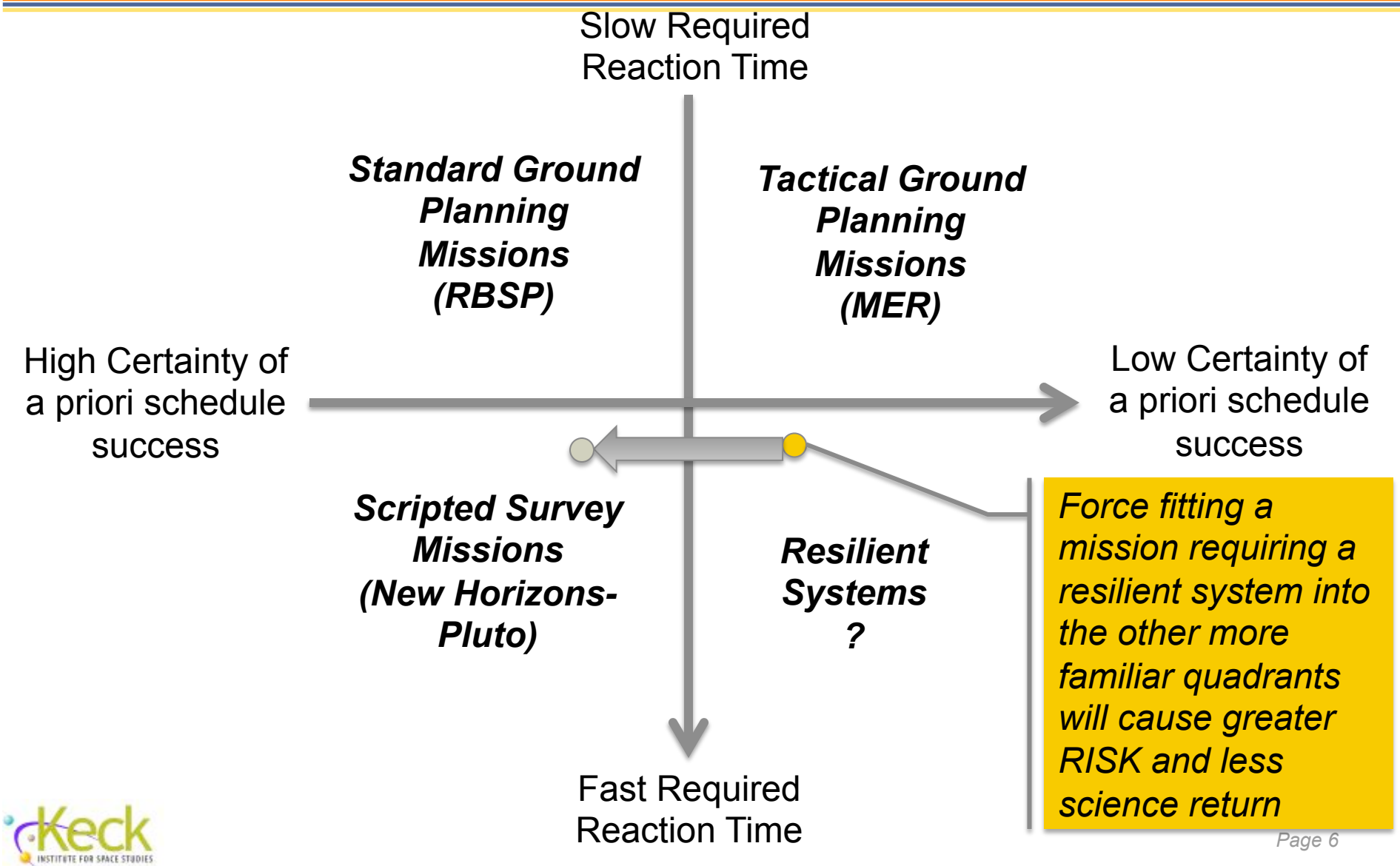


Complexity Branding Quadrant

(stealing from David's Agile Science Ops) (Cancro)



Complexity Branding Quadrant (Broader Market Thru Risk??) (Cancro)



Benchmarking and an Analogy

	"Responsive-ness"	"Resilience"
Performance Goal *(Concise, Quantitative, Concrete)*		
Architectural Principles *(Small List that supports the goal)*		
Architecture Design Features *(Directly Implement the Principles; also maybe what we spend money on to move our principles forward toward goal)*		

Benchmarking and an Analogy

	"Responsive-ness" {Outside Benchmark of AFRL ORS}	"Resilience"
Performance Goal *(Concise, Quantitative, Concrete)*	Build a S/C in 7 Days	?
Architectural Principles *(Small List that supports the goal)*	• Plug-n-Play • Self Discovery • Warehousing/Rapid Assembly	?
Architecture Design Features *(Directly Implement the Principles; also maybe what we spend money on to move our principles forward toward goal)*	• xTEDS (XML description for each component) • ASIM (local ASIC that connects a component into the network) • Pwr/Comm/Structure Backplane • Standards • PnP Software Apps	?

	"Responsive-ness" {Outside Benchmark of AFRL ORS}	"Resilience"**
Performance Goal *(Concise, Quantitative, Concrete)*	Build a S/C in 7 Days	Enable Safety in an unknown environment within 5 seconds of any disturbance + Enable discovery in an unknown environment within 1 hour of when a science opportunity is available to system {{WEAK}}
Architectural Principles *(Small List that supports the goal)*	• Plug-n-Play • Self Discovery • Warehousing/ Rapid Assembly	• Formalize Intent • Use current context to detect change and novelty • Accept unknown as normal • Provide both fast+inflexible and slow+inflexible modes
Architecture Design Features *(Directly Implement the Principles; also maybe what we spend money on to move our principles forward toward goal)*	• xTEDS (XML description for each component) • ASIM (local ASIC that connects a component into the network) • Pwr/Comm/ Structure Backplane • Standards • PnP Software	• Understandable and Operator-able manner of describing operator and science team intent • Observation (external and internal) fold into single integrated picture (e.g. SIAP) allowing for sensor changes • Pattern learning as a form of observation understanding (e.g satellite as a sensor) with comparison of current understanding to Intent • Control through adaption of parameters based on external and internal environment (e.g. self-tuning G&C, up-stream data fusion) where control is fast inflexible-loop and adaption of parameters is slow flexible loop.

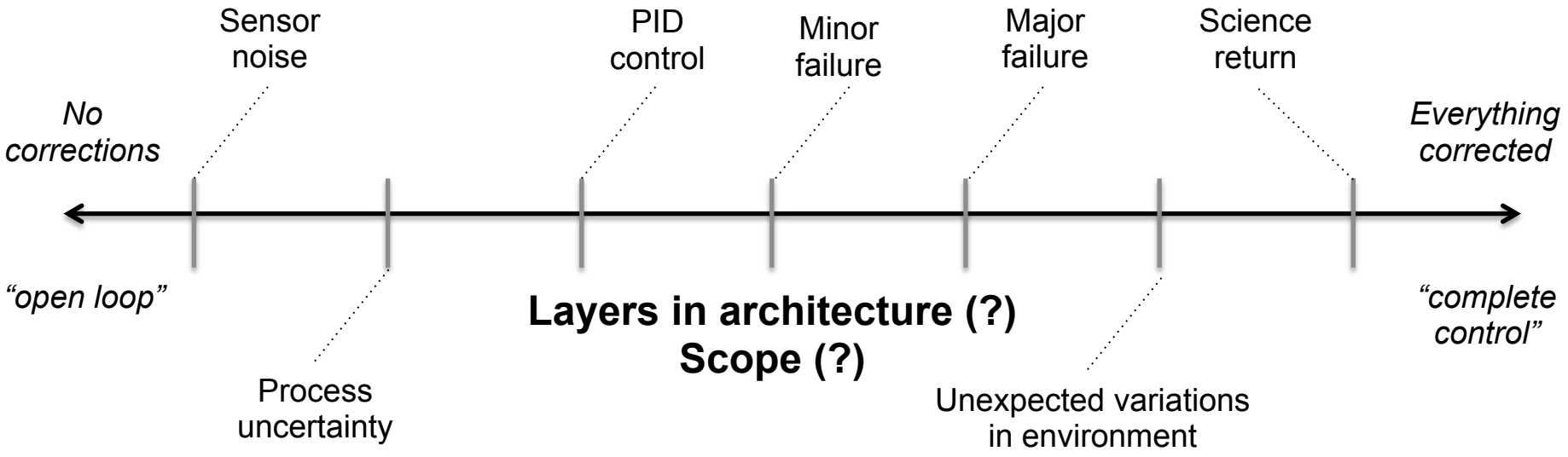
** CONSIDER Planetary Aerobot as Design Reference Mission (or maybe network defense?!?)

	"Responsive-ness" {Outside Benchmark of AFRL ORS}	"Resilience"**
Performance Goal *(Concise, Quantitative, Concrete)*	Build a S/C in 7 Days	Enable Currently Undo-able Missions like Planetary Aerobot or Hydrobot (i.e. mission with low certainty of a priori schedule success and fast reaction time) {{SMALL MARKET}} • Like Tactical ground planning missions (MER) WITHOUT ability to stop the sequence and wait for more direction • Like fast scripted survey missions (Pluto) EXCEPT science is not where you expected to look
Architectural Principles *(Small List that supports the goal)*	• Plug-n-Play • Self Discovery • Warehousing/ Rapid Assembly	• Formalize Intent • Use current context to detect change and novelty • Accept unknown as normal • Provide both fast+inflexible and slow+inflexible modes
Architecture Design Features *(Directly Implement the Principles; also maybe what we spend money on to move our principles forward toward goal)*	• xTEDS (XML description for each component) • ASIM (local ASIC that connects a component into the network) • Pwr/Comm/ Structure Backplane	• Understandable and Operator-able manner of describing operator and science team intent • Observation (external and internal) fold into single integrated picture (e.g. SIAP) allowing for sensor changes • Pattern learning as a form of observation understanding (e.g satellite as a sensor) with comparison of current understanding to Intent • Control through adaption of parameters based on external and internal environment (e.g. self-tuning G&C, up-

ENGINEERING RESILIENT SPACE SYSTEMS

J. Day

- Resilience is simply a measure of the number of states that can be corrected for by a system
  - More states = more resilience
  - Always relative to a particular POV/perspective

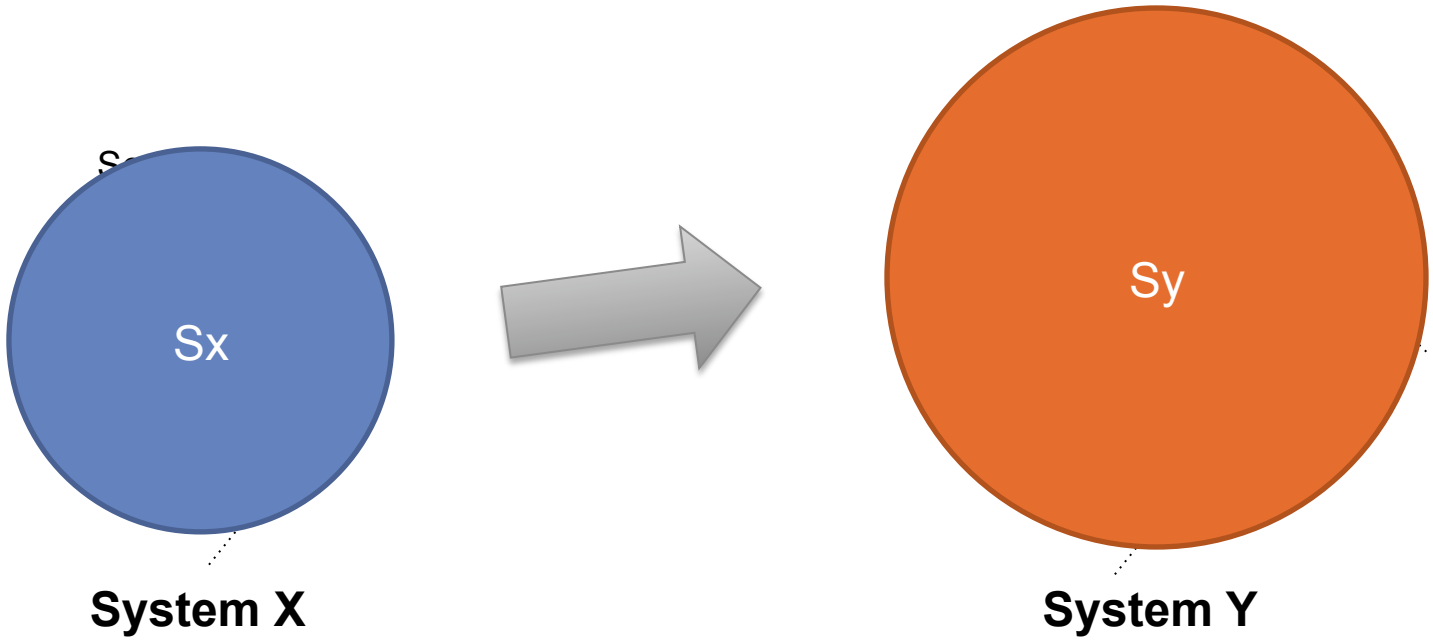


Keck INSTITUTE FOR SPACE STUDIES

ENGINEERING RESILIENT
SPACE SYSTEMS

J. Day

- Resilience is simply a measure of the number of states that can be corrected for by a system
  - More states = more resilience
  - Always relative to a particular POV/perspective



Keck INSTITUTE FOR SPACE STUDIES

ENGINEERING RESILIENT
SPACE SYSTEMS

J. Day

- Resilience is simply a measure of the number of states that can be corrected for by a system
  - More states = more resilience
  - Always relative to a particular POV/perspective
- Resilience requires presence of options
  - Redundancy in all forms (physical, functional, temporal)
- Complexity is in the eye of the beholder
  - How do we present more capable systems as being no more complex to stakeholders (e.g., project mgr)
  - How do we include resilience in a system without increasing complexity?
- Fundamental barrier to technology adoption is lack of common conceptual foundation
  - Technology solutions use different basis/set of concepts
  - Need to evolve current basis for process/practice to enable technology solutions

Keck INSTITUTE FOR SPACE STUDIES

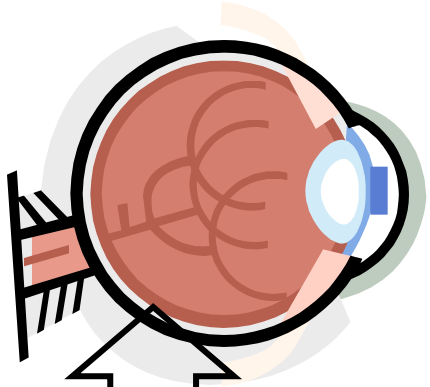
Doyle

Move head

Sense

Fast

Act



Limits on achievable performance and robustness

Same actuator

Delay is limiting

Slow

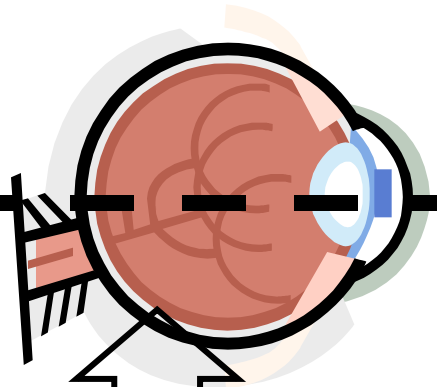
Fast?

Sense

Move hand

Slow

Act



Keck INSTITUTE FOR SPACE STUDIES

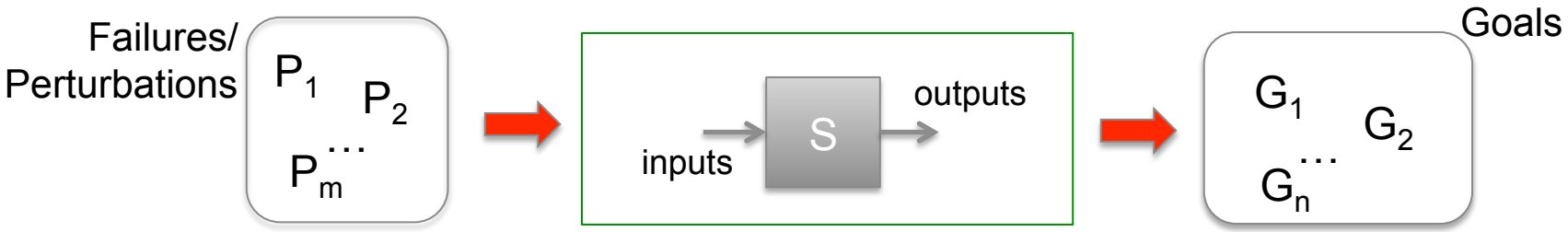
ENGINEERING RESILIENT SPACE SYSTEMS

Attributes Not to Forget (Estlin)

- Scientist is your true customer
  - Involve them early
  - Brief them often
  - You need their support at all phases of system usage
- Spacecraft makes better use of time it has
  - Not just quick or autonomous reaction
  - Could be enabling parallel functionality, better onboard power management, smarter downlink, operation under different environment conditions, etc.
- Lots of great ways to benefit operations team
  - Automate common/mundane activities
  - Help fix problems faster
  - Enable onboard software to be easily adapted when failures occur
  - Ops team wants to support science goals

Keck INSTITUTE FOR SPACE STUDIES

Towards a Measure of Resilience(Gostelow)



Objective function $F = \sum a_i S(G_i)$ where

$S(G_i)$ = degree of success in achieving goal G_i and

a_i = weight for goal G_i

If systems A and B are subjected to the same perturbations and $F_A > F_B$, then system A is *more resilient than* system B.

Parameterize perturbation P_i as $P_i(k)$. Consider $F_A(k)$. The derivitive $\frac{dF_A(k)}{dk}$ is the *sensitivity* of system A to perturbation P_i. System A *is more sensitive* to perturbation P_i than system B if $\left|\frac{dF_A(k)}{dk}\right| > \left|\frac{dF_B(k)}{dk}\right|$

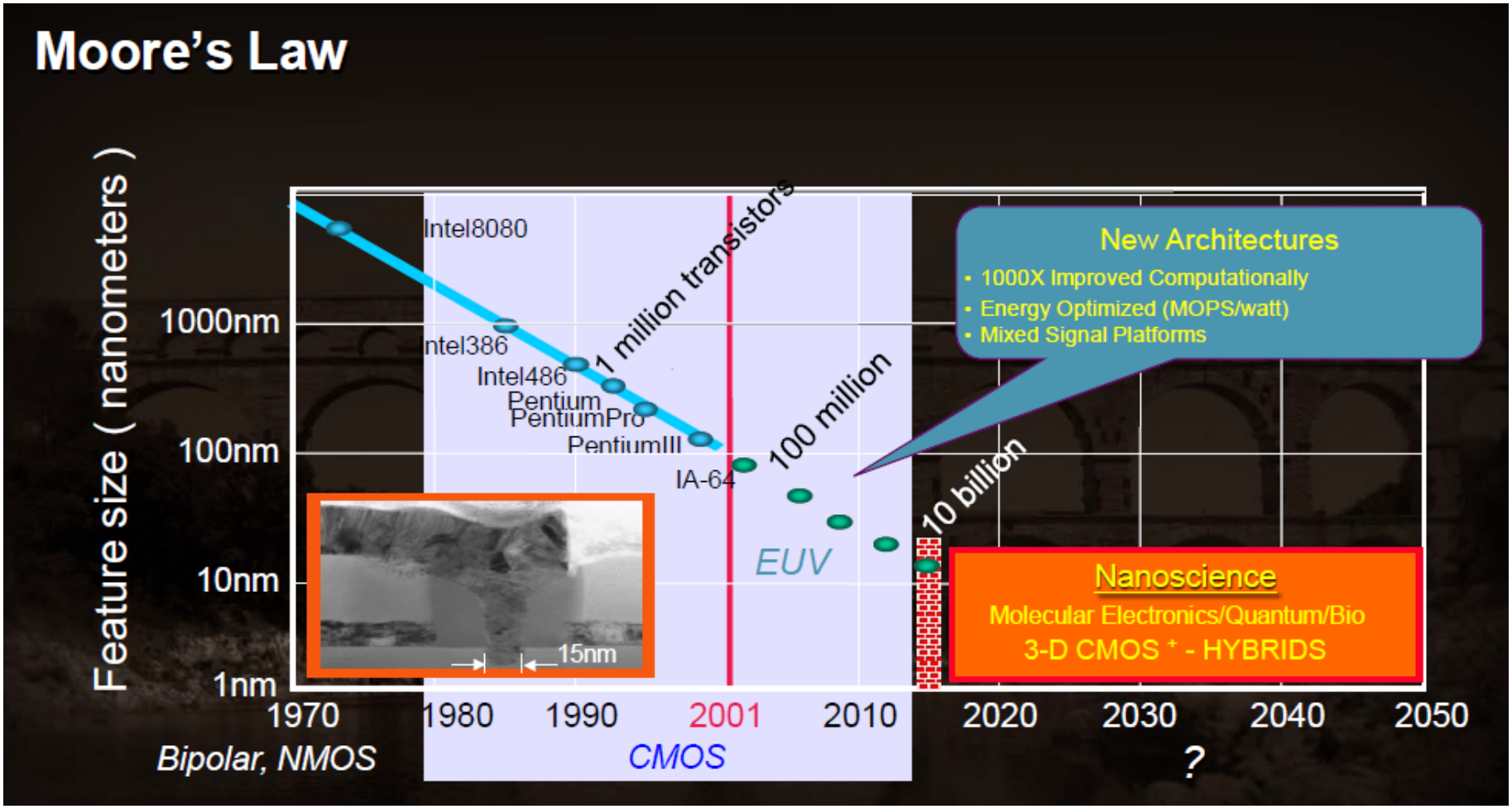
Ingham – W/S #1 takeaways

- Stakeholder concerns and priorities
  - Key Metric: value to customer (scientist) vs cost [performance/risk/cost]
  - Got good input from one important stakeholder set (scientists) – though more perspectives are probably needed
  - Need perspectives from other stakeholders (Programs/Projects) – to-do for Study Period and Workshop #2
- Required system attributes (specifically for RESILIENCE)
  - System Reconfigurability
  - Survivability/Self-preservation
  - Responsiveness/Reactivity
  - Creativity/Problem-solving

Are these right? Are there others?

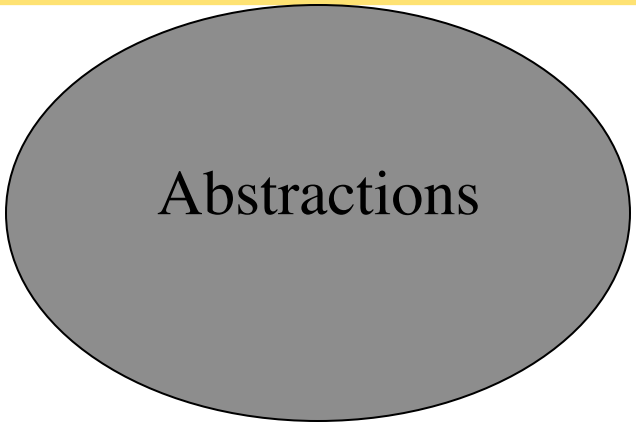
- Required(?) capabilities
  - Design-time:
    - Architecture specification, (meta-)modeling and analysis (prove "nice" properties about architectures)
    - Tools are being worked in programs like AVM/META
    - Need investment in methodology (e.g., methods for MBSE)
  - Run-time:
    - Fail-operational behavior ("function preservation") and graceful degradation
    - Onboard adaptation/reconfiguration to new/modified objectives and changes in component health/functionality
- Challenges
  - Technical: lack of *architecting* rigor and knowledge; integration of technologies into system-level capabilities (with adequate performance, and trustworthiness)
  - Cultural: incremental advancement vs. fundamental/architectural advancement; maybe bootstrap from other domains (Smart Grid, UAVs, etc.); "bend over backward" approach (demo at no cost to project)

Managing Complexity - Moore's Law (Kochocki)

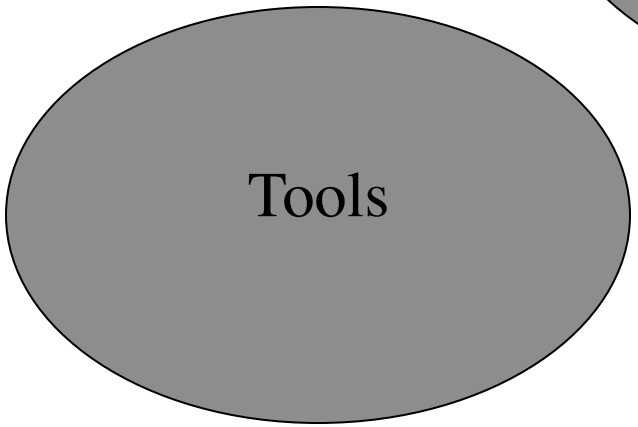


Alberto Sangiovanni Vincentelli, 2009 DARPA/NSF Complexity Workshop

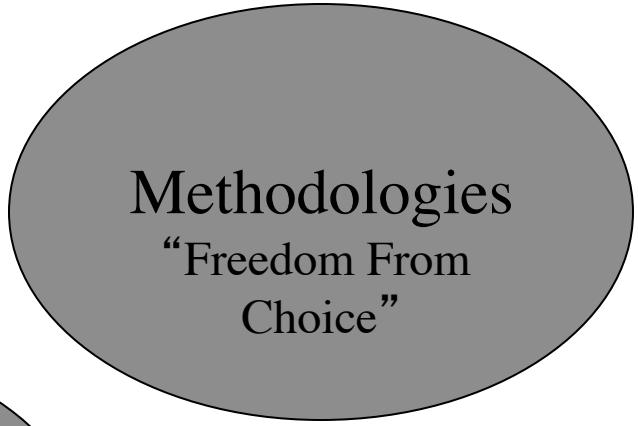
Coping with Complexity – How (Kochocki)



Cells = Building Blocks
Cells Built in Roads = Wiring Paths
Synchronous
for Verification

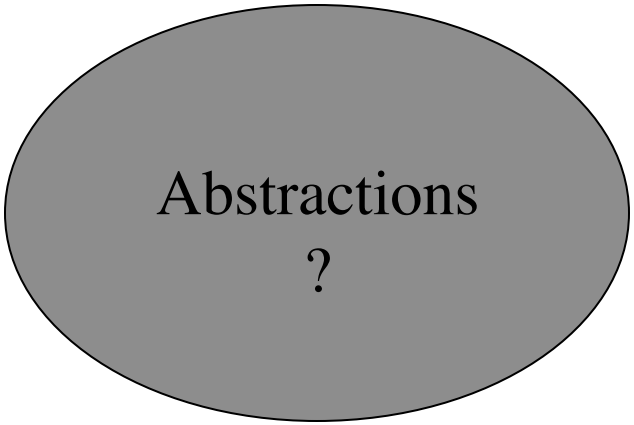


Logic Synthesis
Placement
Routing

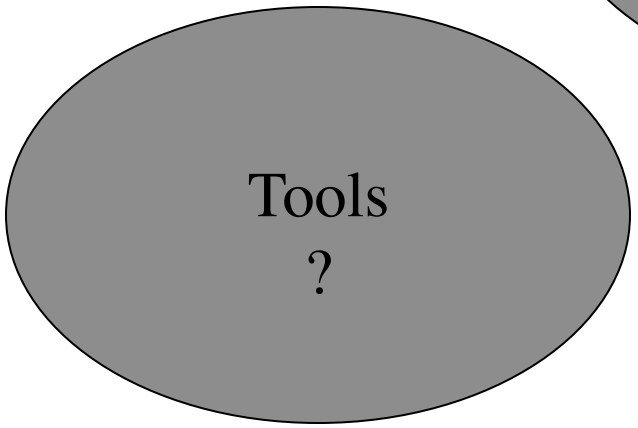


Restricted design allows for automation

Resilient System Engineering (Kochocki)



Raw Materials
3D Plant
Programs

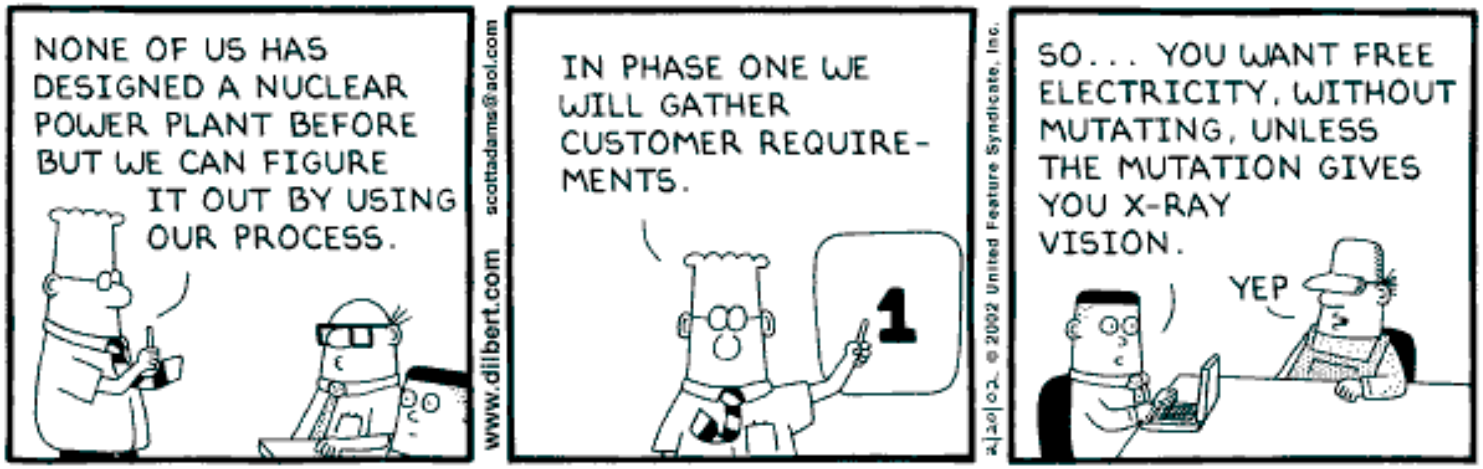


Resiliency
Architecture Analysis
Design Space Analysis
V&V

META?
ISO2070?
CMMI-RES?

ENGINEERING RESILIENT
SPACE SYSTEMS

It Takes Everything(Kochocki)



ENGINEERING RESILIENT SPACE SYSTEMS

Topics to Consider

Azad Madni

- Resilience needs proaction, reaction and learning and adaptation
- Resilience needs to be interpreted based on context/domain
- Resilience needs to explicitly monitor risks and correct drift towards brittleness
- Resilience is a characteristic of a well-designed autonomous system that needs to operate in uncertain environments
- The specific dimensions where resilience is needed, needs to be identified (e.g., payload, schedule, network

- Adaptability and Trust
  - Closed loop concept engineering is key to building trust between engineers and operators especially with regard to adaptability considerations

Azad Madni

ENGINEERING RESILIENT SPACE SYSTEMS

Murray

- Insights on architectures for resilient space systems
  - Architecture = organizing principles and constraints; elegance
  - Resilience requires performance measure + uncertainty set
  - Principles: horizontal transfer and speed/performance tradeoff
- Provocative assertions
  - *Basic* technologies to implement resilience in space systems already exist in other domains (eg AUTOSAR, ROS, IMA, UAVs)
  - If we have to demonstrate resilience via space flights, we will fail
    - Programs will always be risk averse & financially constrained => can't overcome the TRL valley of death
    - Not convinced that resilience can "buy its way" onto space vehicle
    - Possible alternatives: land or sea vehicles (joint with DoD?), robonaut?
  - Need a formal & analyzable specification language for (discrete) mission performance (conops) and system/environ uncertainty
    - Likely to require set-based notations (partial orders, lattices, etc)
    - Should allow reasoning at difference stages of design process (arch)

Keck INSTITUTE FOR SPACE STUDIES

ENGINEERING RESILIENT SPACE SYSTEMS

Lightning Talk - Ozay

- Still not clear to me:
  - Metrics?
  - Unexpected behavior/environment? Can we boil it down to uncertainty (which sounds more quantifiable and can be refined online via “learning”)?
- Interesting Idea:
  - Defining and closing the loops (Bob Rasmussen) - including human operators?
- Possible action items:
  - Understand/pose a concrete problem (or some of the loops therein) related to a reference mission
  - Given a sample problem, think about how synthesis tools can help

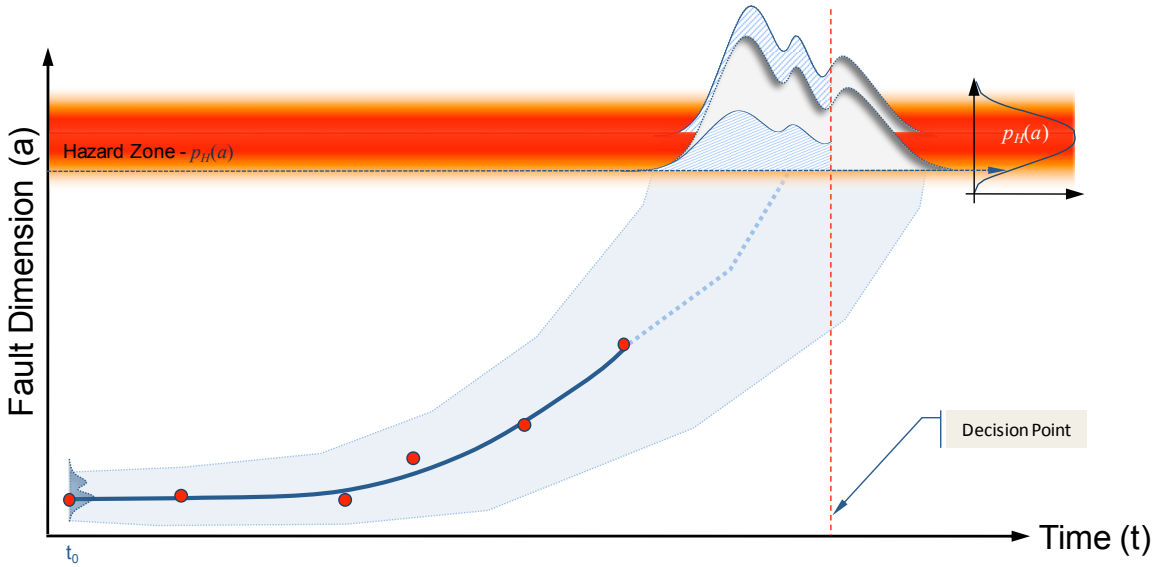
Resilient Space System Wrap-Up (Reder)

- Our vision and associated reference missions
  - We have a nice list of reference missions
  - No clear vision statement - we need one! Maybe Friday??
- Resilience
  - A bit confused about the scope
  - Resilience Space System: (1.) ability to *anticipate* (a priori) need for change and effect it, (2.) ability to *grow* new functionality, (3.) *tolerate internal flaws* and/or self correcting them (***self-healing***)
- Horizontal Transfer & Layering - Skeptical! Perhaps I don't get it
  - Layering often violated within software architectures
  - No discussion of ***encapsulation*** **– Components & Connectors**
  - **Interactions are a problem**
- Bacterial Biosphere - Interesting, but I don't really understand it yet
  - Perhaps an approach for self-correcting software architectures
    - Can defective components be constantly replaced with **fixed** ones?
    - Should we be looking toward systolic array topologies?

ENGINEERING RESILIENT
SPACE SYSTEMS

Prognostics for Resilience (Saxena)

Prognostics: Predicting remaining useful life of a component/system before it stops performing its intended function within specifications



Message:

Prognostics (if done right) ***can be a very powerful enabler of resilience, esp. for remote and inaccessible missions***

ENGINEERING RESILIENT SPACE SYSTEMS

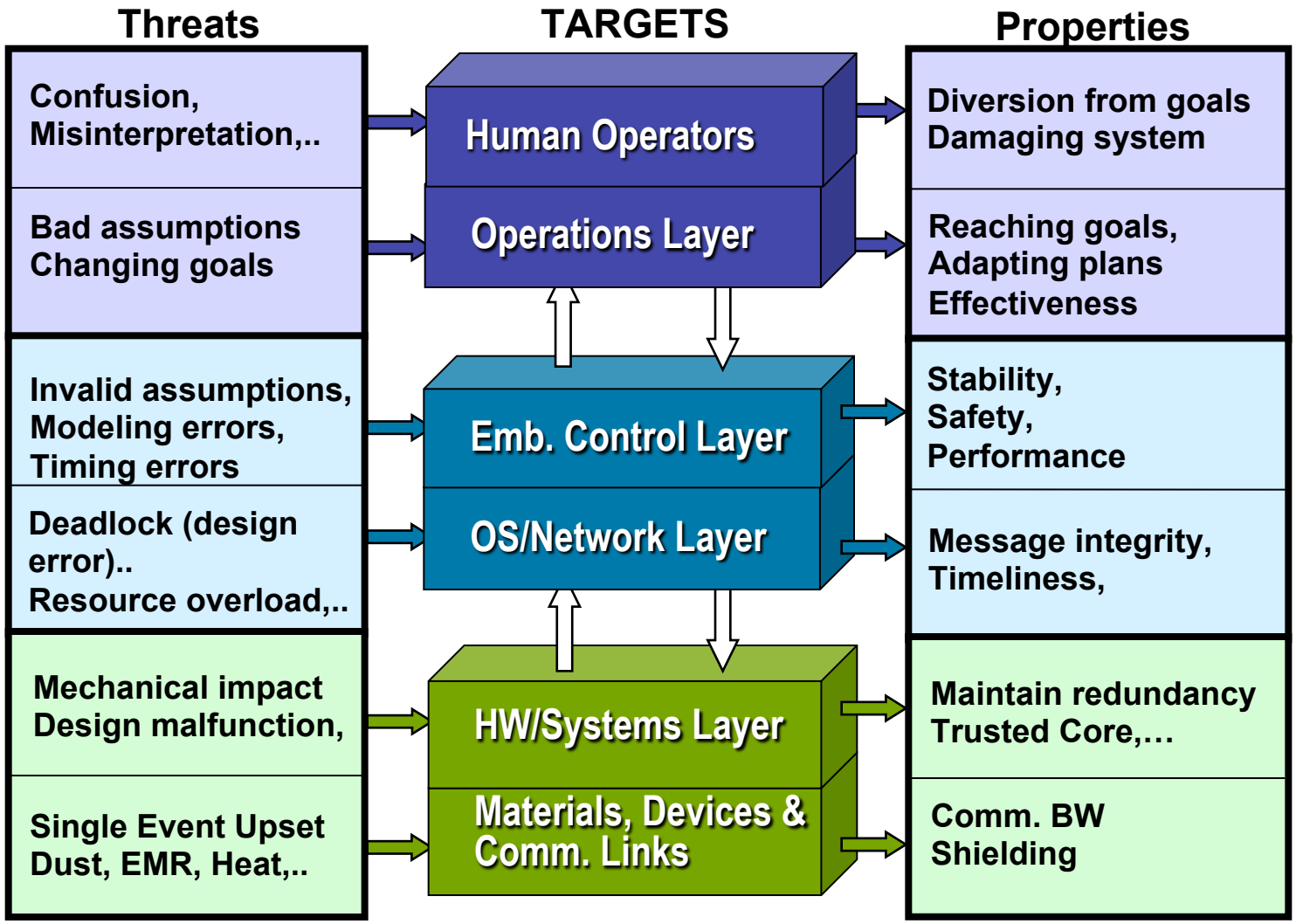
Prognostics for Resilience (Saxena)

- **What can prognostics do**
  - Advanced warning before a failure actually occurs
  - Continued tracking of health state evaluation – proactive monitoring
  - Provide an estimate of time left – to aid in appropriate decision making
    - Plan a strategy and fix it before it fails
    - If not fixable
      - Extend life while you figure out – less aggressive maneuvers
      - Reconfigure (if redundancy exists), re-plan
      - Plan a graceful degradation path
      - Prioritize objectives given inevitable

- **Challenges**
  - Validation and verification
    - How to test and guarantee performance under uncertainty – analytical proofs
    - Access to "real(istic)" test systems (often fleet size of ONE)
  - Uncertainty characterization and handling for DM
  - Real-time and onboard computational requirements
    - Scoping – identifying and anticipating eventualities – which target systems?
  - Cost-benefit justifications – fly-away costs vs. lifetime costs
  - Integration from inception vs. as an after thought

ENGINEERING RESILIENT
SPACE SYSTEMS

Resilience/Janos

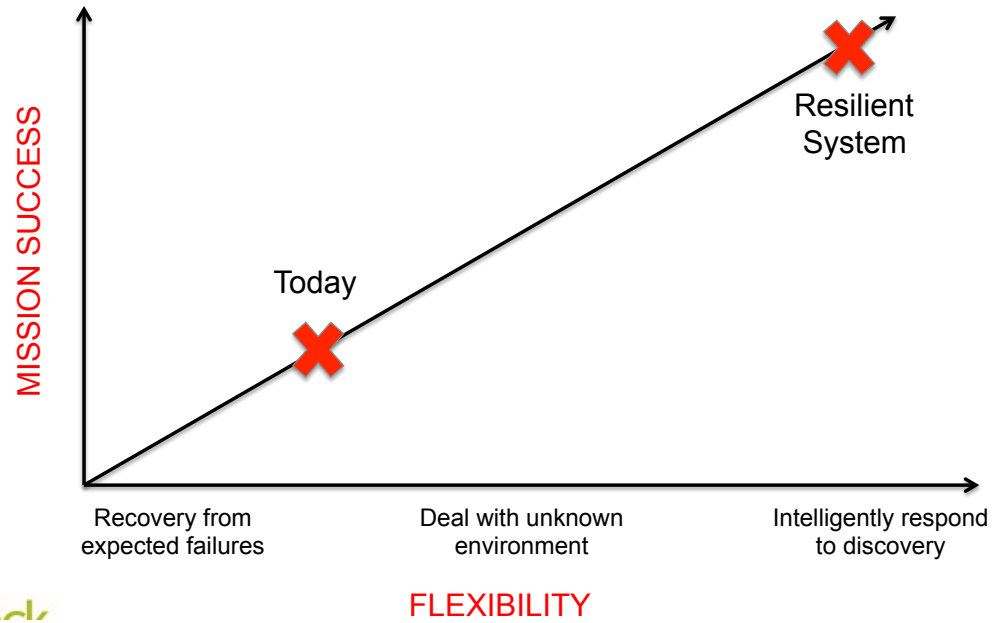


Keck INSTITUTE FOR SPACE STUDIES

Tamppari thoughts

- Need an agreed upon vision (more specific?) and primary objective

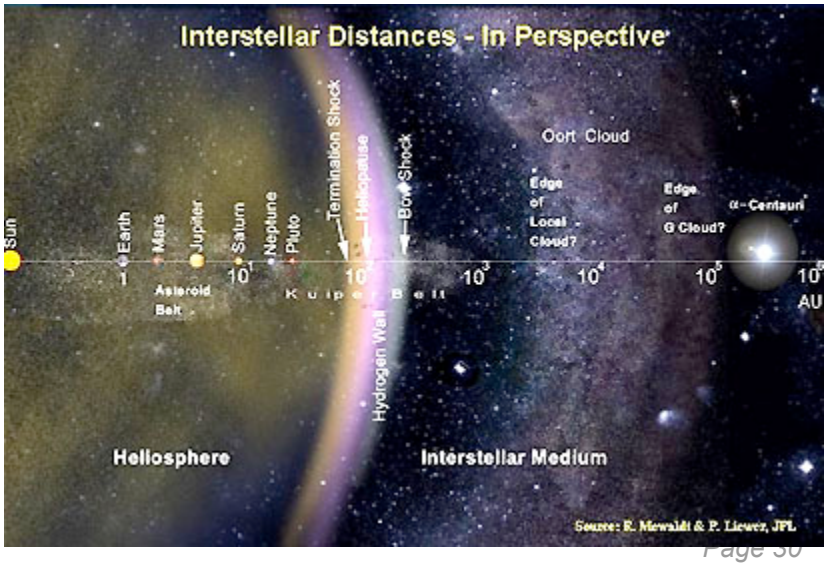
- Don't just prepare for failure, but also prepare for success
- Discovery is on the continuum of fault/failure recovery and environmental uncertainty resilience
- Flexibility parable – flexibility in VML sequencing, but could not test - led to *less science*



ENGINEERING RESILIENT SPACE SYSTEMS

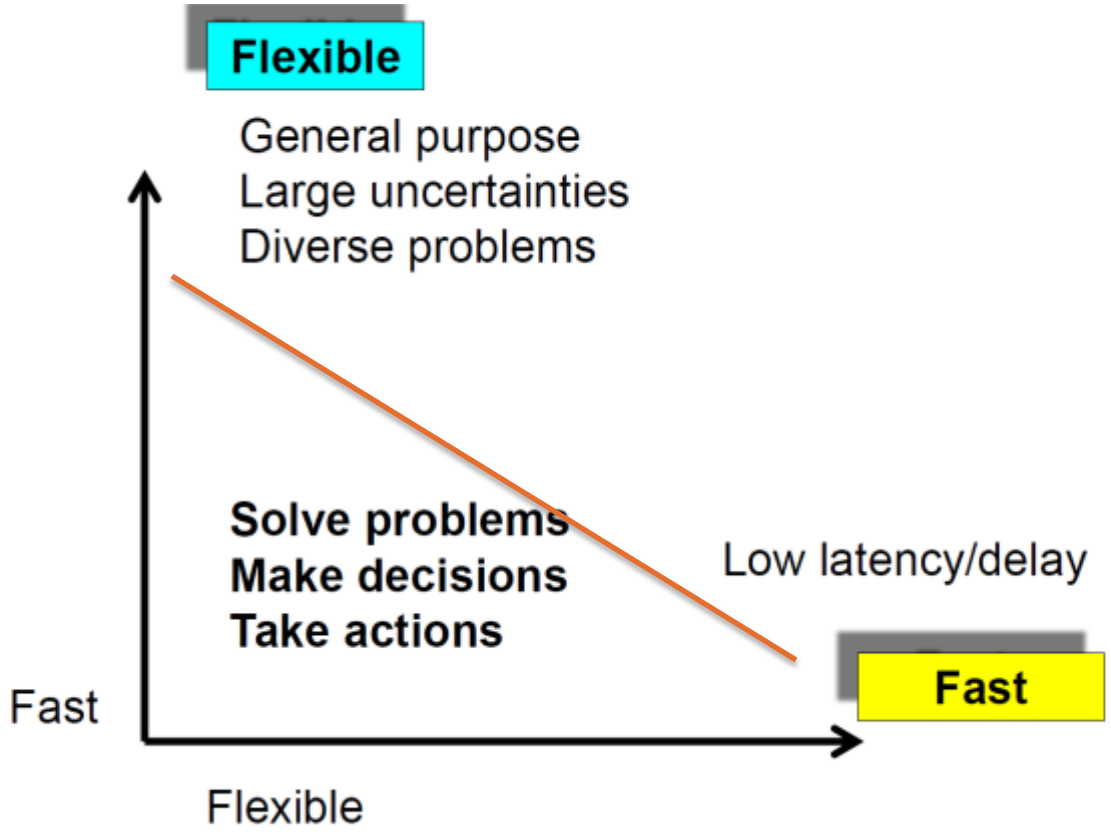
The Oort Cloud Century Mission (Thomson)

- **Spacecraft:** A big optical telescope + RTG + ion drive
- **Science themes**
  - Extreme parallax observations (up to 600AU baseline) reveal local universe in 3D dimensions
  - Upon arrival, locate and investigate the Oort cloud objects
- **Resilience themes**
  - **Discovery**
    - **Long light time delay** requires autonomous flyby responses
    - Most targets not known in advance
  - **Anomalies**
    - **Long duration mission** (50+ years) is a stepping stone to interstellar spacecraft
    - Requires redundant components with **horizontal transfer of capability**
    - An international effort, must preserve mission continuity for 50-100 years



ENGINEERING RESILIENT
SPACE SYSTEMS

Timmons



- AI vs. Architecture
- ROS
- Demos Critical

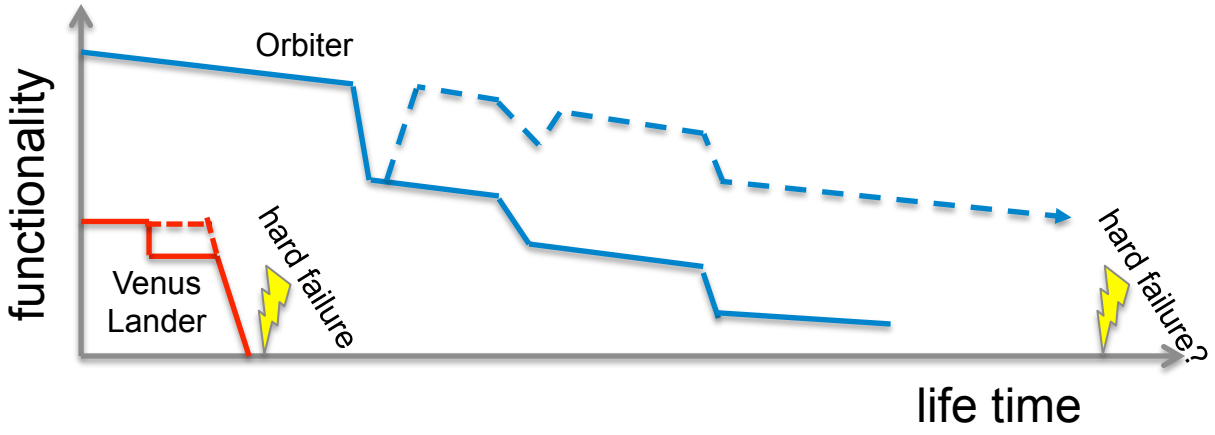
Keck INSTITUTE FOR SPACE STUDIES

ENGINEERING RESILIENT SPACE SYSTEMS

Functional Redundancy (Wang)

- Functional Redundancy *with respect to a set of objectives*
  - Not Hardening
  - Not necessarily multiple-to-1 replacement
- Decision Making (on-board)
  - ***When*** to enable?
  - ***Which*** to enable?
- Redundancy with respect to what environment envelope?
  - Humans can learn and have abundant resources.
  - This is a luxury not afforded in space, so we must try to predict the unexpected… or 3D print it.
- Which missions are best suited for resilience?

(more area below the curve = better)



Keck INSTITUTE FOR SPACE STUDIES

ENGINEERING RESILIENT
SPACE SYSTEMS

Risk-directed Human-Machine Interaction (Williams)

- *Operators and designers explicitly declare requirements on risk.*
- *RS probabilistically validate and revise their models on line.*
- *RS assess risk against mission risk specifications.*
- *RS actively probe and explore to improve risk assessments.*
- *RS adjust actions to meet risk specifications.*
- *RS continuously diagnose barriers to acceptable mission risk, and*
  - *adjust actions and plan contingencies,*
  - *Inform designers and operators of barriers, causes, and contingencies.*
  - *Transition authority to humans as needed.*

1. **Continually replan paths for the rescue vehicles given current knowledge of risk in the environment.**

2. **Deploy sensing assets to minimize uncertainty in mission risk.**

3. **Continuously re-evaluate the risk of the rescue vehicle plan.**

4. **Engage the operator when the risk tolerance is breached.**

ENGINEERING RESILIENT
SPACE SYSTEMS

Storytelling (Xu)

- What is the story, who is your audience, and how do you tell it?

- Reference Missions
  - Take what you have, turn it into what you need, to get what you want
  - Take what you need, turn it into what others want, and make it what you will have

ENGINEERING RESILIENT
SPACE SYSTEMS

Themes from Lightning Talks

- Day after lightning talk summary slides

ENGINEERING RESILIENT SPACE SYSTEMS

Themes from Lightning Talks

- **Where is the vision?**
  - What is the story, who is your audience, and how do you tell it?
  - Need an agreed upon vision (more specific?) and primary objective
  - We need to narrow scope

- **What are the metrics?**
  - Towards a Measure of Resilience (Gostelow)
    - Perhaps apply to current missions showing brittleness
  - Other metrics – John Doyle is a smart guy – figure it out?
  - Any proposal will have to show quantitative value so this is needed for technology program

ENGINEERING RESILIENT SPACE SYSTEMS

Themes from Lightning Talks

- **Barrow technologies from other domains**
  - How can progress and/or even models/code developed for other domains (cars, planes, Earth-based robots) be translated to resilient spacecraft applications?
  - Basic technologies to implement resilience in space systems already exist in other domains (e.g. AUTOSAR, ROS, IMA, UAVs)
  - Stay focused on Spacecraft domain
    - NASA may not fund it but KISS might!

ENGINEERING RESILIENT SPACE SYSTEMS

Themes from Lightning Talks

- **Technologies**
  - Fundamental barrier to technology adoption is lack of common conceptual foundation
    - Tools are being worked in programs like AVM/META
    - ***Need investment in methodology*** (e.g., methods for MBSE)
  - Architectural analysis and ***metrics*** tools
  - Need a formal & analyzable ***domain specification language*** for (discrete) mission performance (conops) and system/environ uncertainty
    - Likely to require set-based notations (partial orders, lattices, etc)
    - Should allow reasoning at difference stages of design process (arch)
    - Given a sample problem, think about how synthesis tools can help
  - ***Spacecraft could makes better use of time if:***
    - we enable rapid autonomous reaction
    - we could enable parallel functionality, better onboard power management, smarter downlink, operation under different environment conditions, etc.
  - ***Bacterial Biosphere inspired*** approach for self-correcting, evolving software architectures

Keck INSTITUTE FOR SPACE STUDIES

ENGINEERING RESILIENT
SPACE SYSTEMS

Keep in mind

- Where is the innovation and revolutionary idea?

The Keck Institute for Space Studies is a "think and do tank"

"…studies must concentrate on ideas that have the capability for **revolutionary advances** in space mission capability."

"…fund the initial steps towards making progress on that key ***innovation/challenge***."

Keck INSTITUTE FOR SPACE STUDIES