Verification of Autonomous Systems by Capability Verification Composition (CVC)

Providing methods for assurance in intractably complex systems

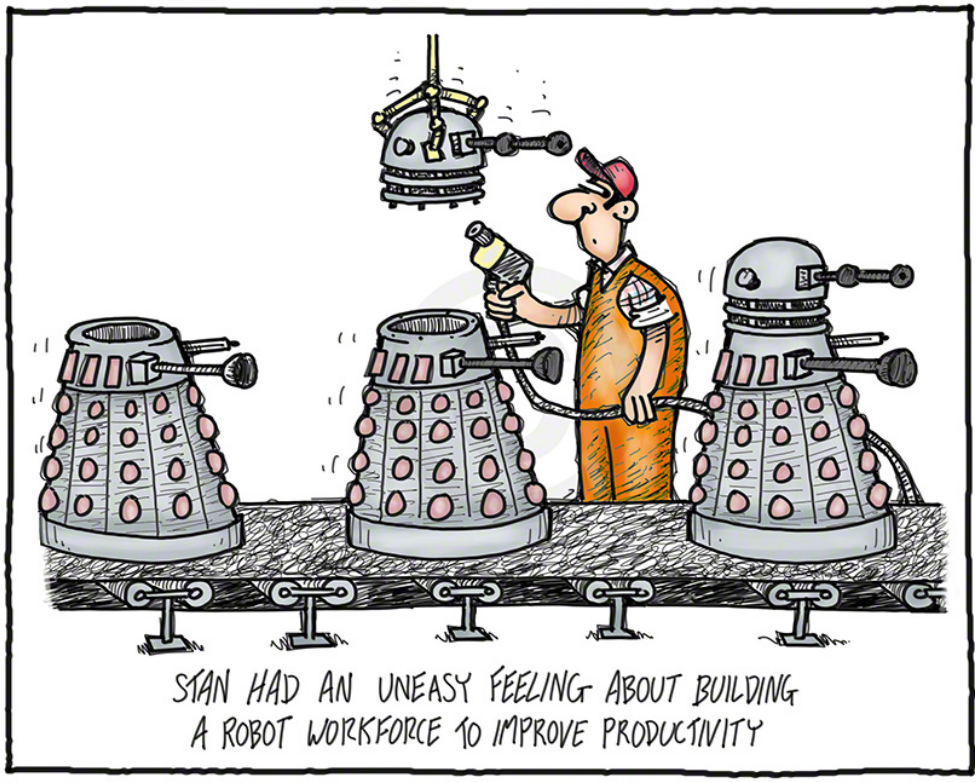
OCEANS 2017 MTS/IEEE
Anchorage, Alaska USA
20 September 2017

Andrew Bouchard
NSWC PCD Code X22
andrew.bouchard@navy.mil

Dr. Richard Tatum
NSWC PCD X22
richard.d.tatum@navy.mil

Savanna Horan
NSWC PCD X21
savanna.horan@navy.mil

Background

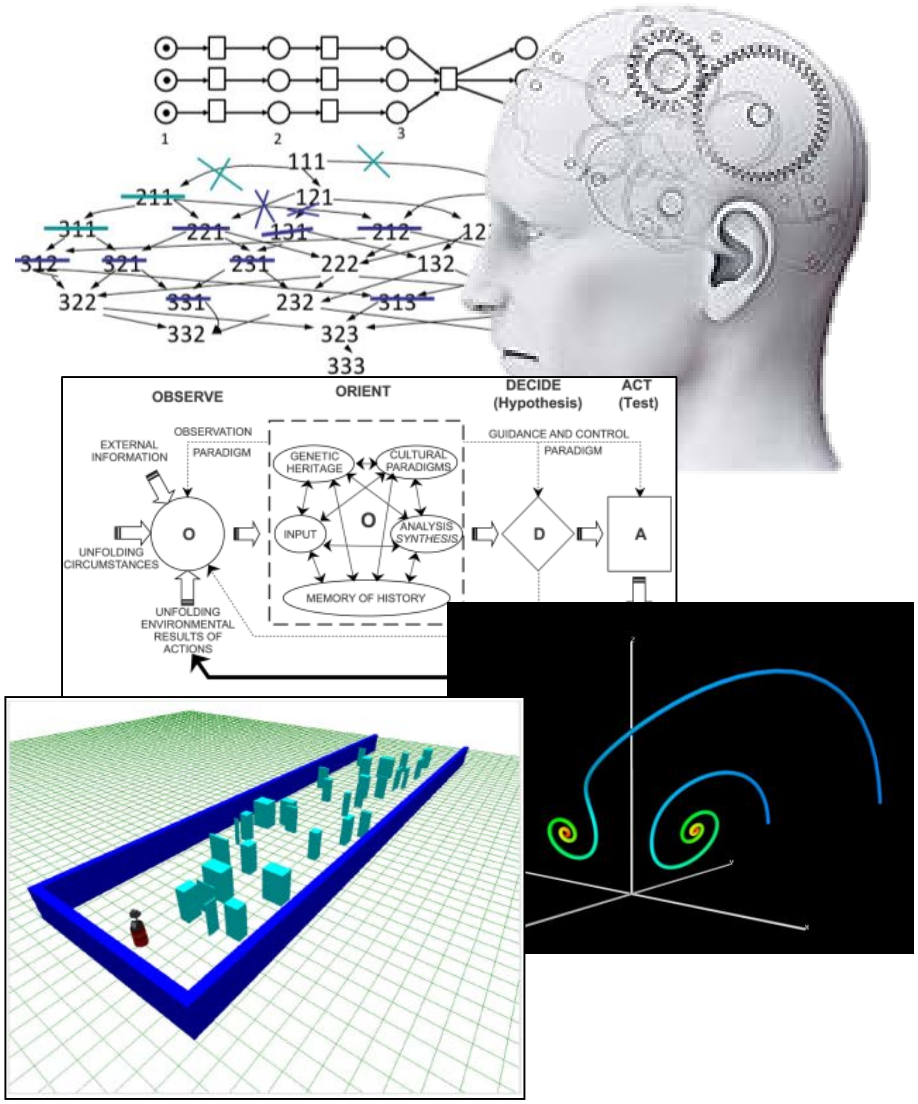


- **Verification** is the process by which we provide assurance that some thing meets the requirements defined for it
- To date, there is no accepted way to
  - Define requirements for autonomous systems
  - Verify autonomous systems
- The problem is one of intractable complexity; systems with
  - unknowably many inputs and
  - unknowably many outputs
  - operating in a stochastic environment

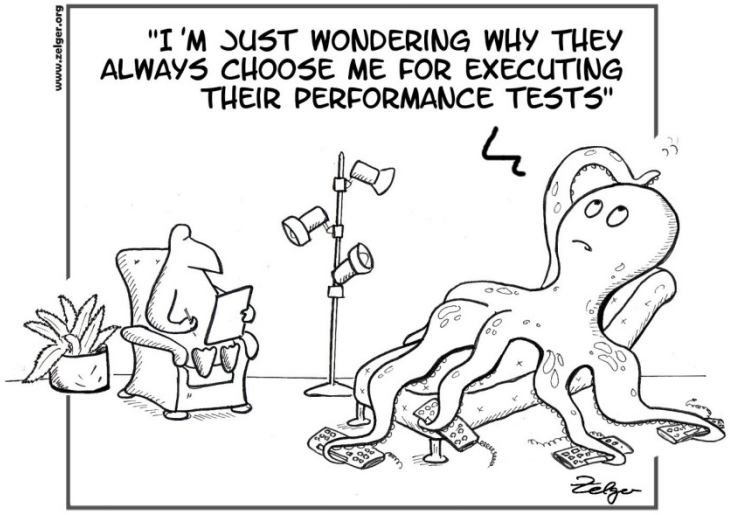
  describe too many states to evaluate them all formally

Initial Efforts

- Literature Survey (OCEANS '15)
  - Ad hoc test cases
  - Subjective expert evaluation
  - Lacking requirements
  - No arguments for generalization
- Analogies
  - Philosophy: Language and meaning are changed and adapted by the communities that use concepts
  - Psychology: Evaluation requires a taxonomy and structure for defining what is being evaluated and based on what parameters
  - Mathematics: Representation of inputs through the use of equivalence classes
  - Statistics: Reduction of dimension of data



Why Do We Verify?

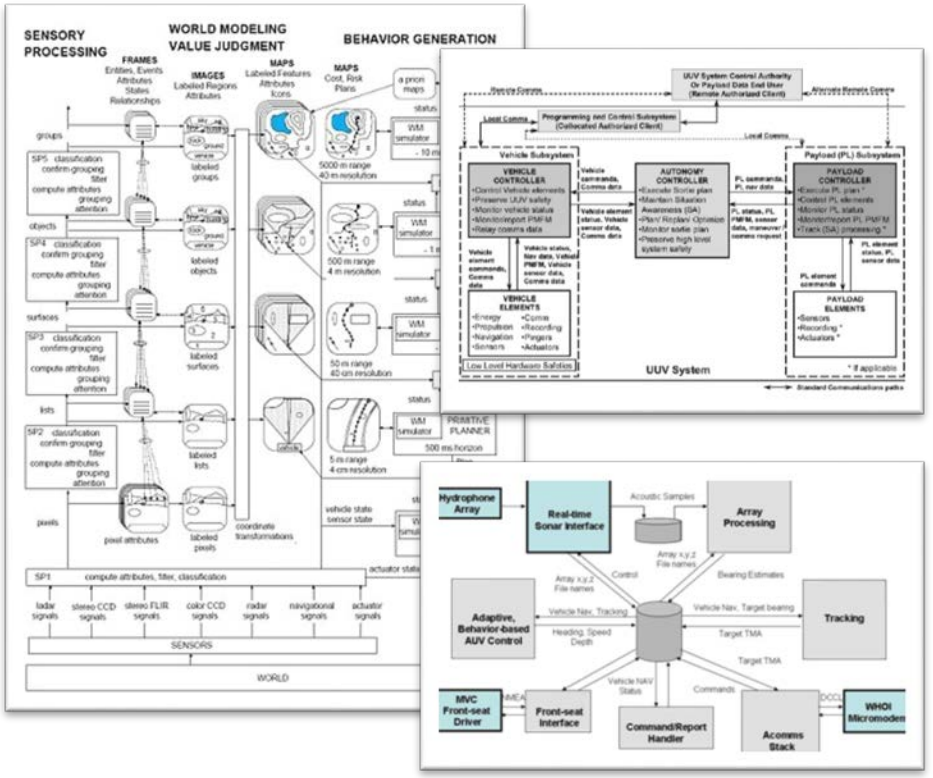


The multi-threaded octopus was looking for a change

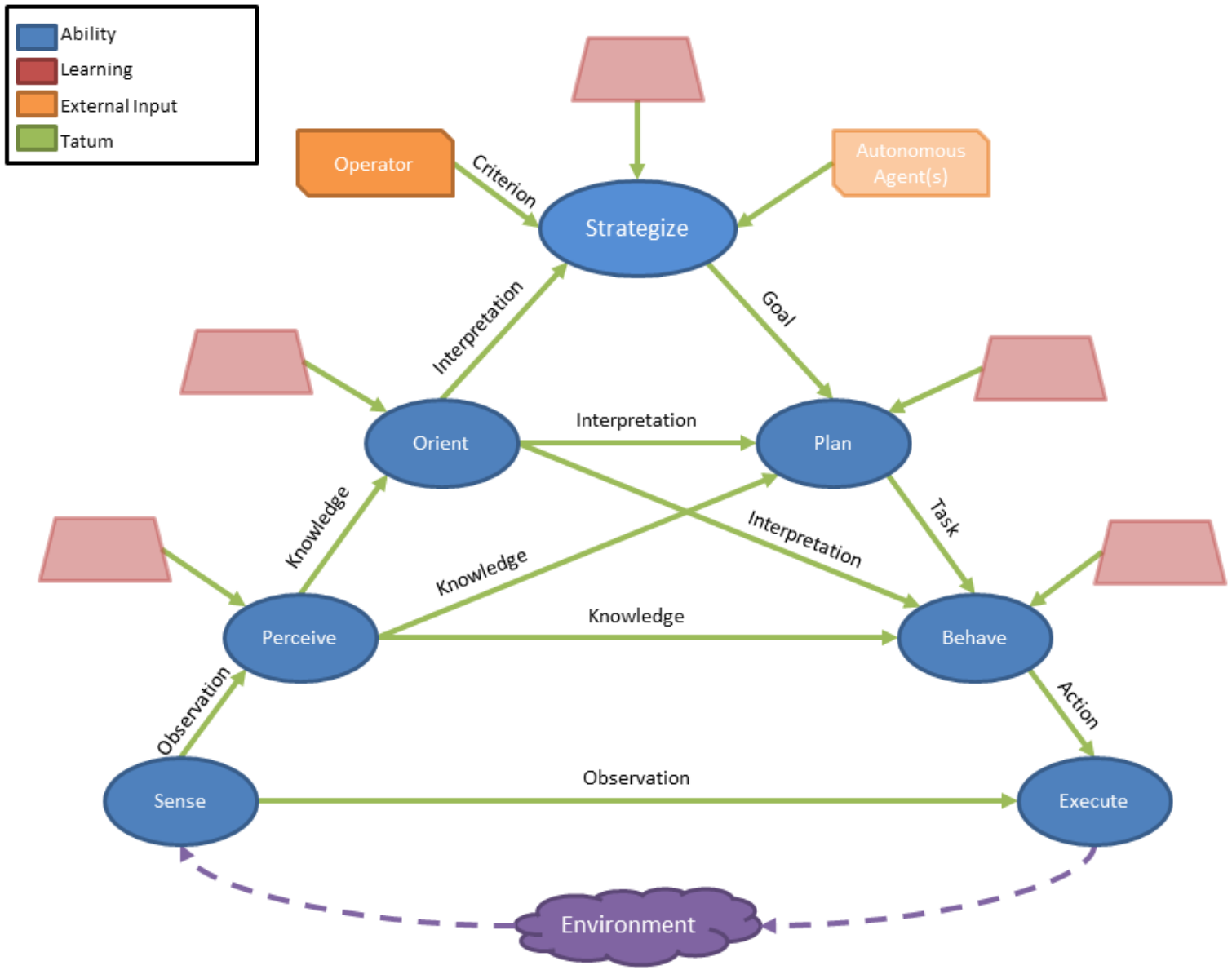
- To provide assurance of performance to who?
- Three key communities
  - Developers: Is my autonomy improving? Where are the needs for development?
  - Evaluators: How to define requirements for autonomy? What makes one better than another?
  - Operators: What can the system do reliably? Under what conditions can I expect the system to succeed?
- We have talked to members of all these communities
  - Sociology Research Methods
  - IDEOU Insights for Innovation
  - Several conferences and meetings
  - Discussions with testing community
  - Multiple military exercises

Divide and Conquer

- Problems:
  - No consistent taxonomy for autonomy
  - Standards are restrictive and divisive
  - Monolithic systems are too complex to evaluate holistically
- Solution
  - Provide an extensible taxonomy that will grow with the community
  - Use an open market model to encourage commonality while permitting innovation
  - Describe autonomous systems using smaller units that are easier to characterize and test



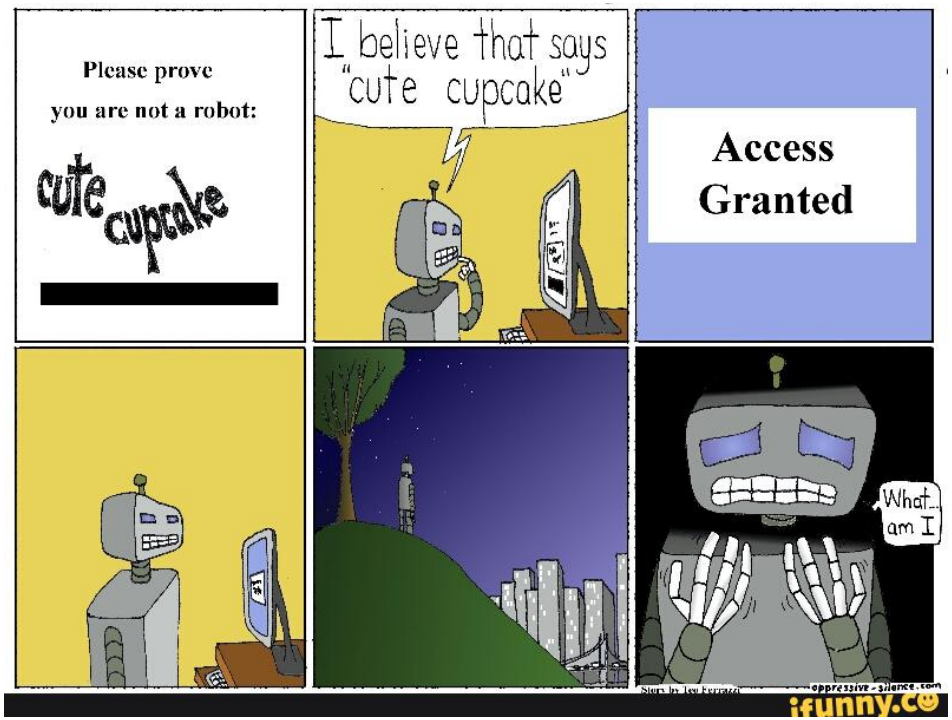
Autonomy Capability Framework



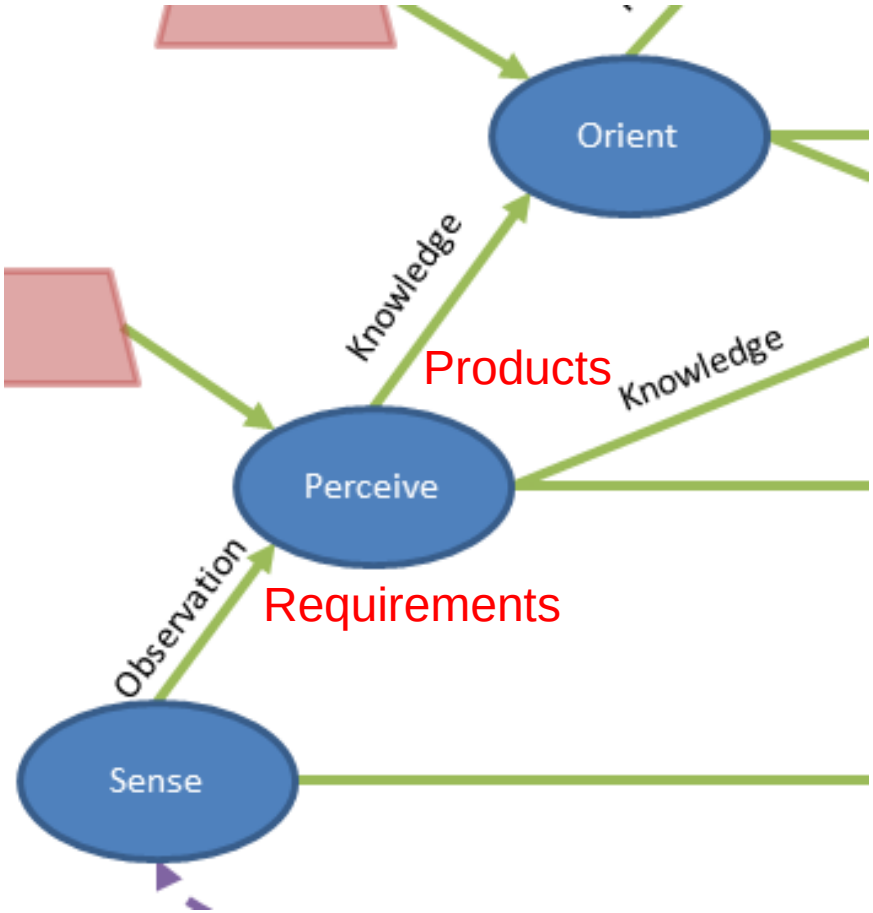
DISTRIBUTION A

Categories

- Ability: the power or skill to do something
  - Abstracted from specific implementation
  - More relevant to what most stakeholders care about
- Tatum: a compound data type consisting of the type of data consumed or produced by an ability and quantitative metrics of that data
  - Example: Sense Sonar ability produces imagery with a resolution, range, rate, and probability
  - Describes and characterizes requirements and products



Autonomy Capability Framework

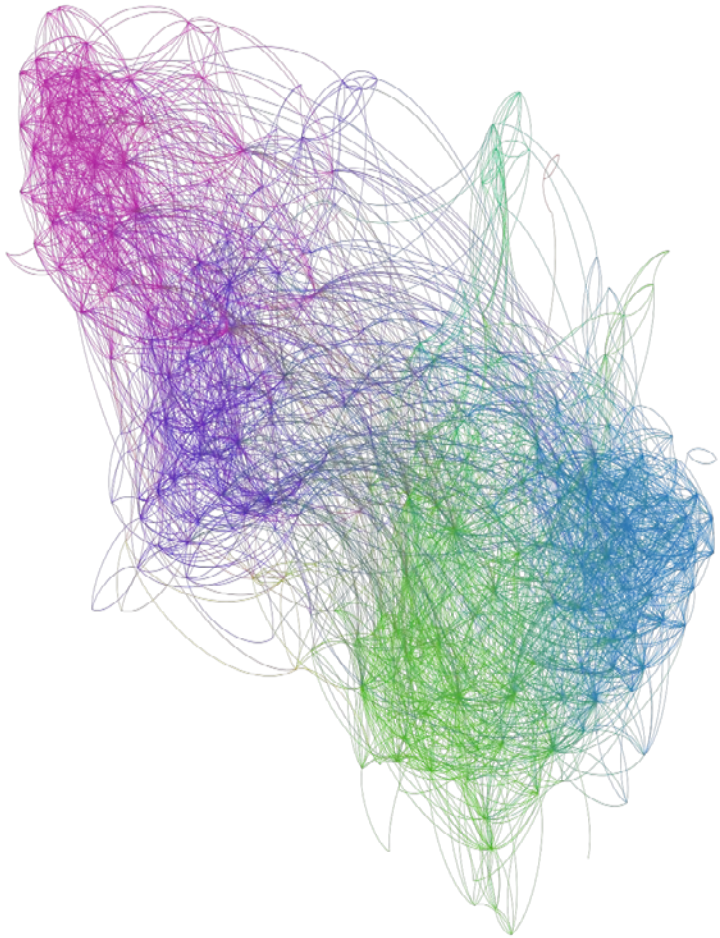


- We define general autonomy abilities based on common classes of inputs and outputs
- Each ability and tatum is backed by a clear definition
- Specific systems and modules can be evaluated according to the abilities they implement
- Better implementations will:
  - Reduce requirements
  - Increase performance
- By decomposing systems into the abilities that comprise them, we reduce the complexity of evaluation
- Ability owners can define their own requirements and products, but the connections incentivize convergence
- Note: Tatum connections are not restrictive

Summarize Results

- Problems:
  - Need is driven by system performance
  - The performance of one capability will affect another
- Solution
  - Develop compositional algorithms that predict overall performance from capability metrics
  - Create methods for describing products that depend on requirements
  - Also use an open market model for compositional algorithms

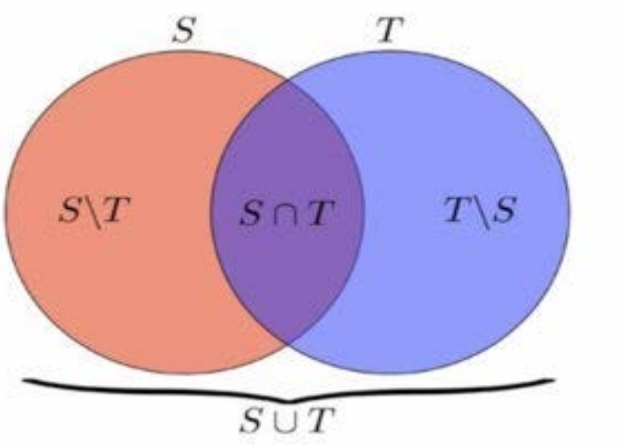
Mathematical Framework

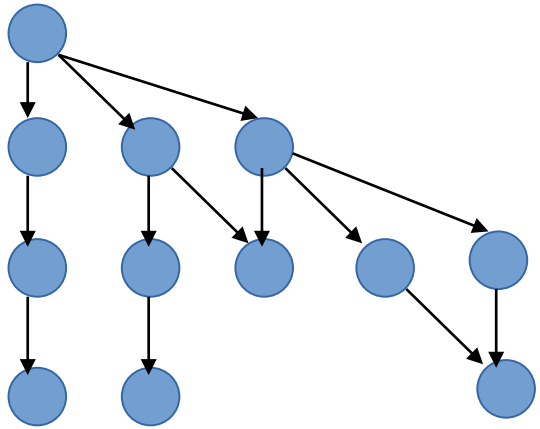


- Consider the capability framework describing a given system as a directed graph in which the abilities are the vertices and tatums are the edges
- Edges connect vertices and describe the flow of information between abilities
- We can define functions to describe relevant sets within this system
  - The tatums (requirements and products) associated with a given ability
  - The attributes of a given set of tatums
  - The range associated with a given tatum
  - Dependability with respect to environment

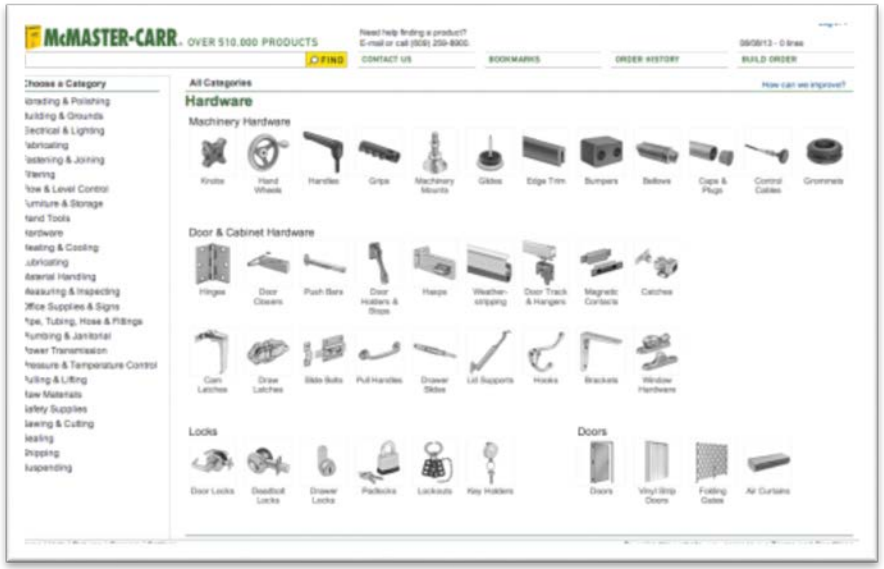
Mathematical Application Examples

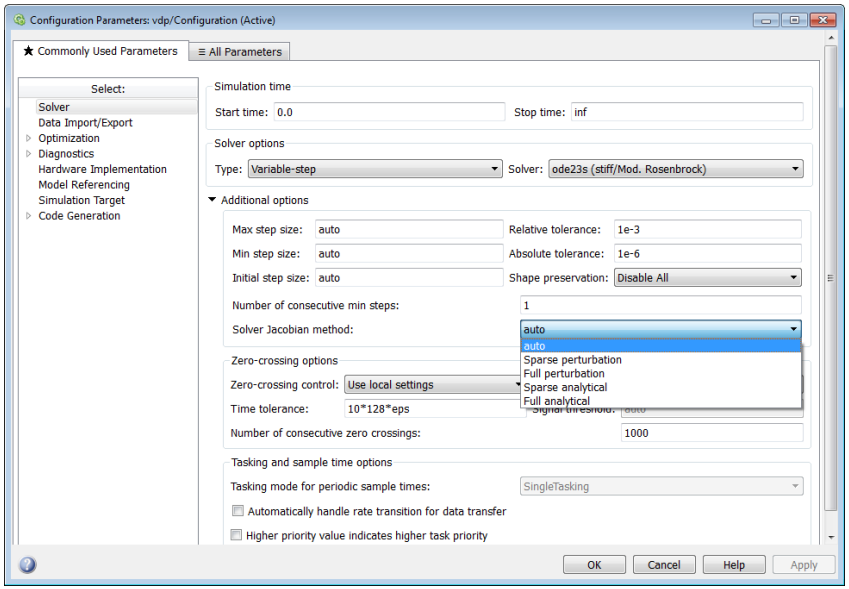
- Comparing Individual Nodes
  - Jaccard similarity coefficient
  - Similarity between tatums and attributes of those tatums
  - Useful in determining whether requirements are met and identifying gaps
- System Dependability
  - Assume that dependability requirement tatum has been defined for all abilities
  - The performance of each ability can be considered independently
  - For each path through the system, compute the probability of the ability functioning in a given environment
- Note that different analyses/assumptions will require different algorithms





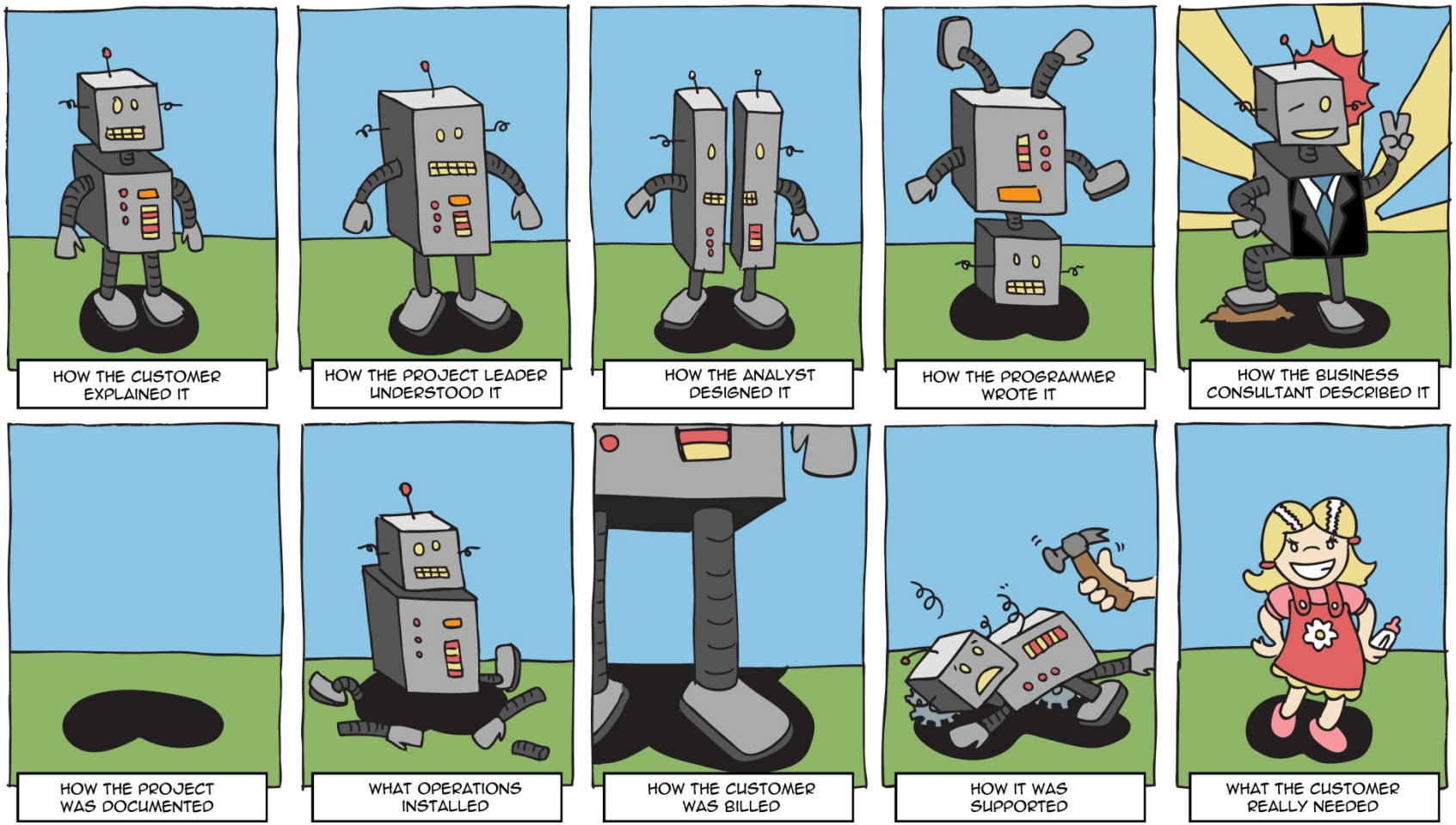
Future Work





- Formal establishment of framework with community for feedback and support
  - Feedback already solicited from multiple organizations
  - All input welcome
- Creation of an online tool for the “marketplace” of abilities and tatums
  - Begin the development of community-based standards
  - Improve awareness of available capabilities
- Tatums that are general properties versus situational
  - Example: Maximum rpm versus maximum speed over ground

Questions?



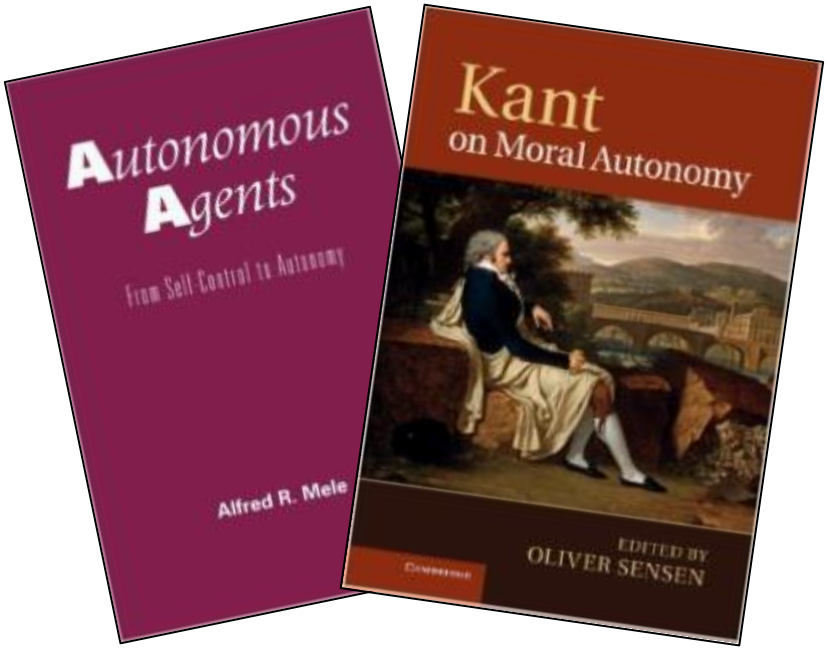
Andrew Bouchard
NSWC PCD Code X22
andrew.bouchard@navy.mil
850-636-6467

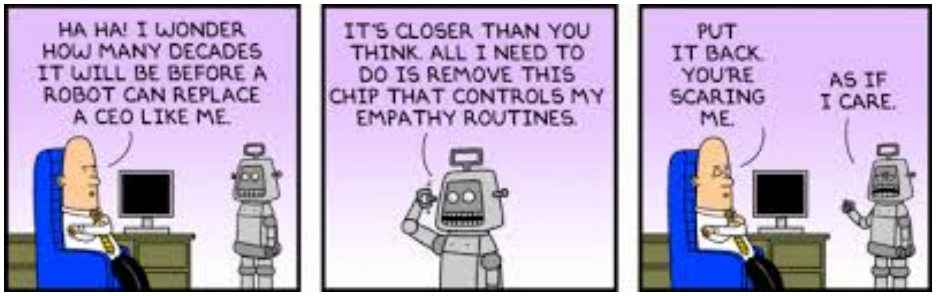
Dr. Richard Tatum
NSWC PCD X22
richard.d.tatum@navy.mil
850-230-7486

Savanna Horan
NSWC PCD X21
savanna.horan@navy.mil
850-230-4708

DISTRIBUTION A

Analogies: Philosophy

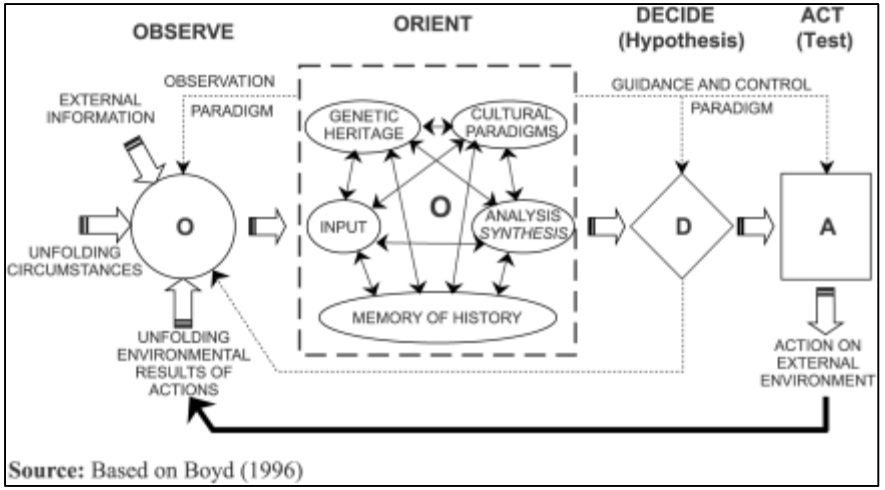




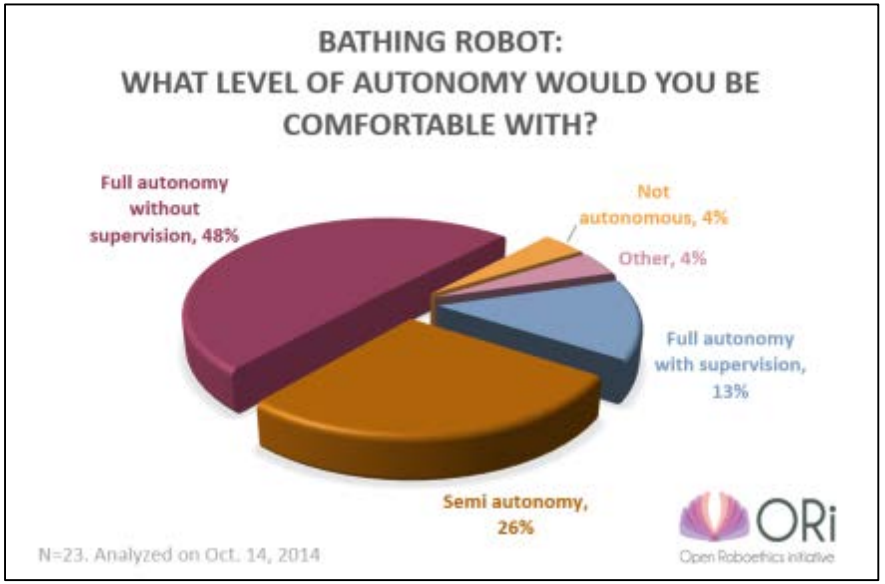
- Why philosophy?
  - "The task of philosophy… is to extricate and bring to light the hidden categories and models in terms of which human being think" *Isaiah Berlin*
  - History of formal sciences began with philosophy
- Autonomous agent
  - Self-rule or self-government
  - A set of competencies - capacities to choose rationally and objectively
- Free will and political autonomy
  - Internal capacity to act
  - Freedom from manipulation
- Autonomy as the requirement for moral responsibility

Analogies: Psychology

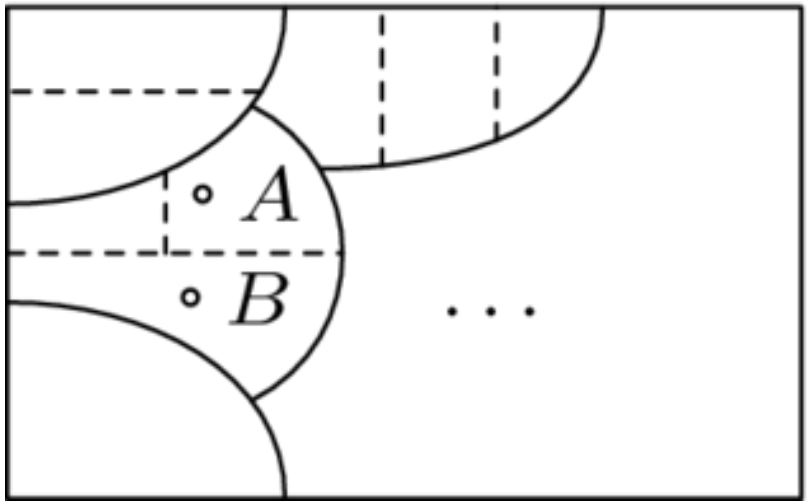
- Why psychology?
  - Cognitive psychology: the study of "how people acquire, perceive, process, and store information" (APA)
  - Autonomy mimics human capability
- Goal-Setting
  - Analogy to human goal-setting
    - Framework for black-box evaluation
    - Assumes human psychology (desires, motivation, etc.)
  - Goal type, difficulty, complexity
  - Requires a taxonomy of goals
- Expert Evaluation
  - No consensus on general measurement
  - Expert evaluation is task-specific
  - Requires taxonomy of capabilities
- Trust
  - Key attributes of trust
  - Dynamics of trust when violated

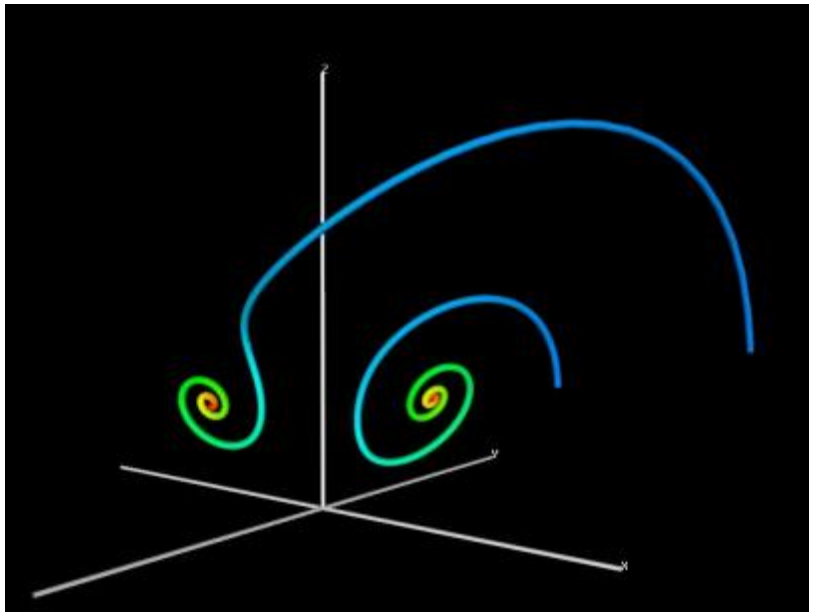


Source: Based on Boyd (1996)



Analogies: Mathematics





- Why mathematics?
  - Proofs and theorems
  - Techniques for complexity reduction
- Equivalence Classes
  - Define equivalence classes
  - Divide inputs into subsets based on equivalence
  - Test a few samples from each subset
- Edge Case Identification
  - Find input cases where behavior changes
  - Characterize gross behaviors based on these transitions

- Why statistics?
  - How to analyze data scientifically
  - What is important?
- Variable Identification
  - Dependent versus independent
  - Principal component analysis
- Reduce Input Space to Relevant Variables