System Engineering
Self-Sustaining Systems

A system that maintains its own health and protects itself from attack, perhaps by monitoring its own status and acting on anomalies.

Robustness in the face of faults—human and otherwise.
Self-Sustaining Systems

- biologically inspired mechanisms
- engineering
- models and/or reasoning
Biology

- diversity
- redundancy
- anti-redundancy
- biological modularity
- spatial compartmentalization
Biology

- gradients
- decay/excitation
- abundance
- randomness (swarms)
Biology

- stigmergy
- apoptosis (programmed cell death)
- evolution/fitness landscapes
- symbiogenesis (Elysia viridis, lichens)
Biology

- growing systems (both with and without programming)
- horticulture
- homeostasis/repair
writing correct programs is hard
writing to correct requirements is impossible
Engineering

- modularity (in the face of changing context)
- encapsulation
- abstraction
- eg, static typing (anti-redundancy)
- eg, aspects (biological modularity)
Engineering

dynamic adaptation (eg, learning what people mean by preferences—what does red mean to you?)

test-driven design—planning how to recognize correct behavior & problems through instrumentation
Engineering

- feedback

- building systems from modules (using self-awareness)
Models & Reasoning

- formal models to check validity—range of acceptable systems behavior
- reasoning about the past and results—and about the future and checking predictions
Models & Reasoning

- construct models down to some level, then generate (grow) the levels below

- parts need to understand their roles & negotiate with other parts

- in some systems, there is no possibility of global control—parts need some autonomy
Attacks

- fault => error => failure
- fault => error => alternative
- hard to detect and diagnose (faulty data)
- attacks might be indistinguishable from bugs
Attacks

defense without diagnosis possible

quick, reactive defense =>
deliberation and retraction/repair

diversity (diverse instruction sets; obfuscation)
Levels

- biological
- engineered
- reflective
Levels

- biological
- totally reactive
- quick
- sublogical
- fight/flight
- error prone
Levels

- engineered
- deliberation
- compositional semantics
- stimulus generalization
- hypotheses about past/future
- long-term perceptions & behaviors
Levels

- reflective
- ability to represent systems of information management
- meta-management
where I’m from...