Helix: A Self-Regenerative Architecture for the Incorruptible Enterprise

MURI Review Meeting
08/06/10

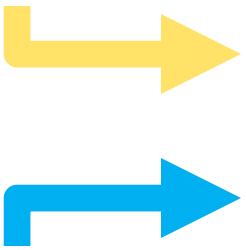
University of California Davis
University of California Santa Barbara
University of New Mexico
University of Virginia

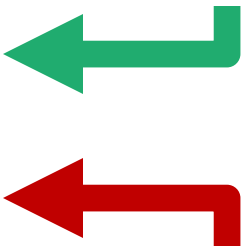
Helix

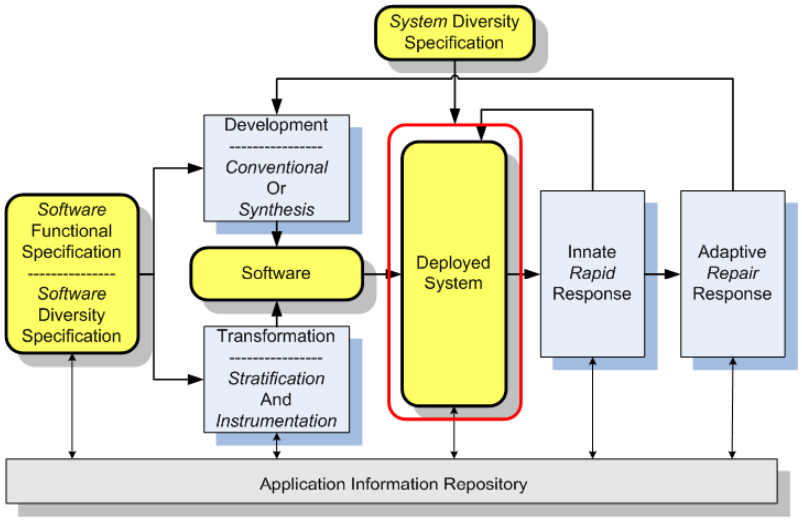
Helix MURI Team

U.C. Davis

U.C. Santa Barbara







HELIX

Univ. New Mexico

Univ. Virginia

Helix Team Members

- University of Virginia:
  - John Knight (PI)
  - Michele Co
  - Jack Davidson
  - David Evans
  - Jason Hiser
  - Anh Nguyen-Tuong
  - Wes Weimer
- University of New Mexico:
  - Stephanie Forrest
  - Jared Saia
- University California Davis:
  - Earl Barr
  - Hao Chen
  - Karl Levitt
  - Jeff Rowe
  - Zhendong Su
  - Felix Wu
- University California Santa: Barbara
  - Fred Chong

Plus lots of students—both graduate and undergraduate

Recent Accomplishments

- Strata-based application control system developed:
  - Flexible sensing and actuation
  - Demonstrated with fine-grain security policy enforcement
  - Changeable remotely and on running app.
- Analyzed and prototyped metamorphic shield
- Program repair technology enhanced and extended to assembly code
- Helix Enterprise control mechanism prototyped:
  - Human in the loop initially
  - To be expanded to automation

Recent Accomplishments

- Attack-resistant distributed algorithms developed based on fast Byzantine agreement algorithms
- Analysis technology for unsafe loading developed
- Approach to cross application information-flow tracking via databases developed
- Hardware design and architecture techniques developed to provide a provably secure foundation for the Helix system
- Begun the development of Helix mock up:
  - Wide range of applications Stratified
  - Windows port of Strata in progress
  - Helix monitoring system prototype
- Can only present certain topics today, see papers or talk to us for more

Show what a Helix system would look like

See annual report for more detail

What And Why?

- What is the MURI project trying to accomplish?

"The objective of this Self Regenerative Incorruptible Enterprise Topic is to develop new algorithms that will enable information systems to **learn**, **regenerate** themselves in response to errors and/or attacks, and **automatically improve** their ability to deliver critical services."

"Biologically inspired diversity may inspire dynamically **immune** components."

- Why is this an important area of research?:

"Existing approaches to information system security and survivability consist of preventing and containing unintentional errors and/or cyber attacks. These systems use **static** means to survive, but are **unable to adapt**, learn, tolerate and/or reconstitute dynamically in response to unforeseen errors and/or unknown cyber attacks."

Biological Metaphor

- Biological populations tend to be able to adapt
  - The magic of diversity
- Why can't computer systems?

- Keep in mind, biological populations do not use diversity to:
  - Protect against overwhelming odds, they use ***skin***
  - Protect against physical trauma, e.g., a gun, they use ***Kevlar***

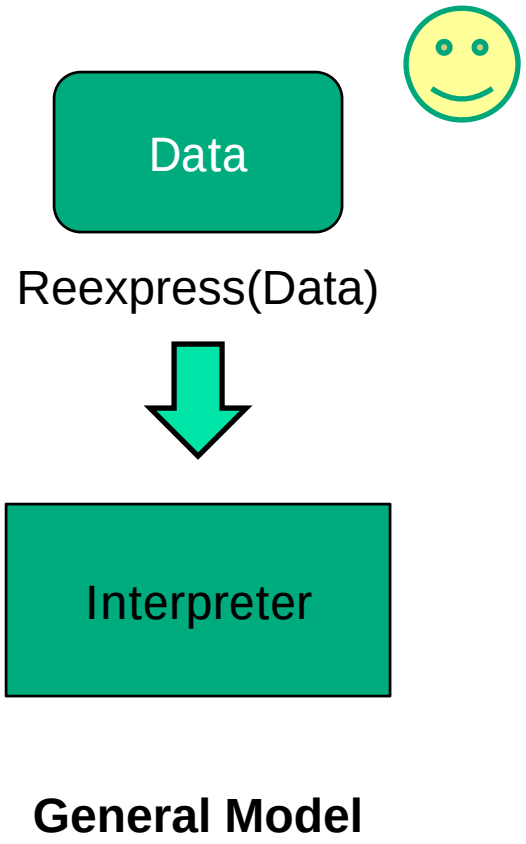
- Let's try **artificial** diversity

What Is Artificial Diversity?

- **Design** diversity:
  - Applied to interpreters
  - Impractical (human created)
- Techniques such as:
  - Address space randomization
  - Instruction set randomization
  - Calling sequence diversity, etc.
- What is being randomized?

Data

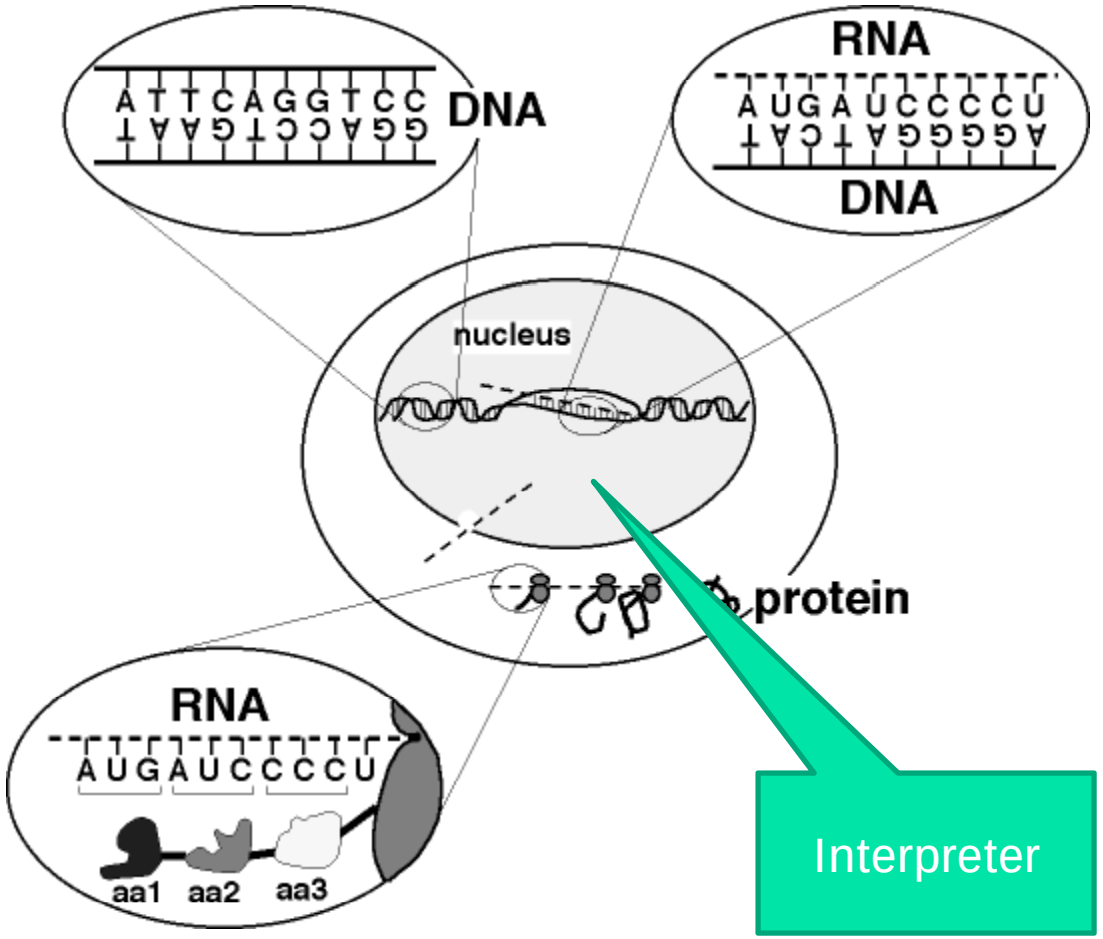
- Artificial diversity is ***data diversity***



General Model

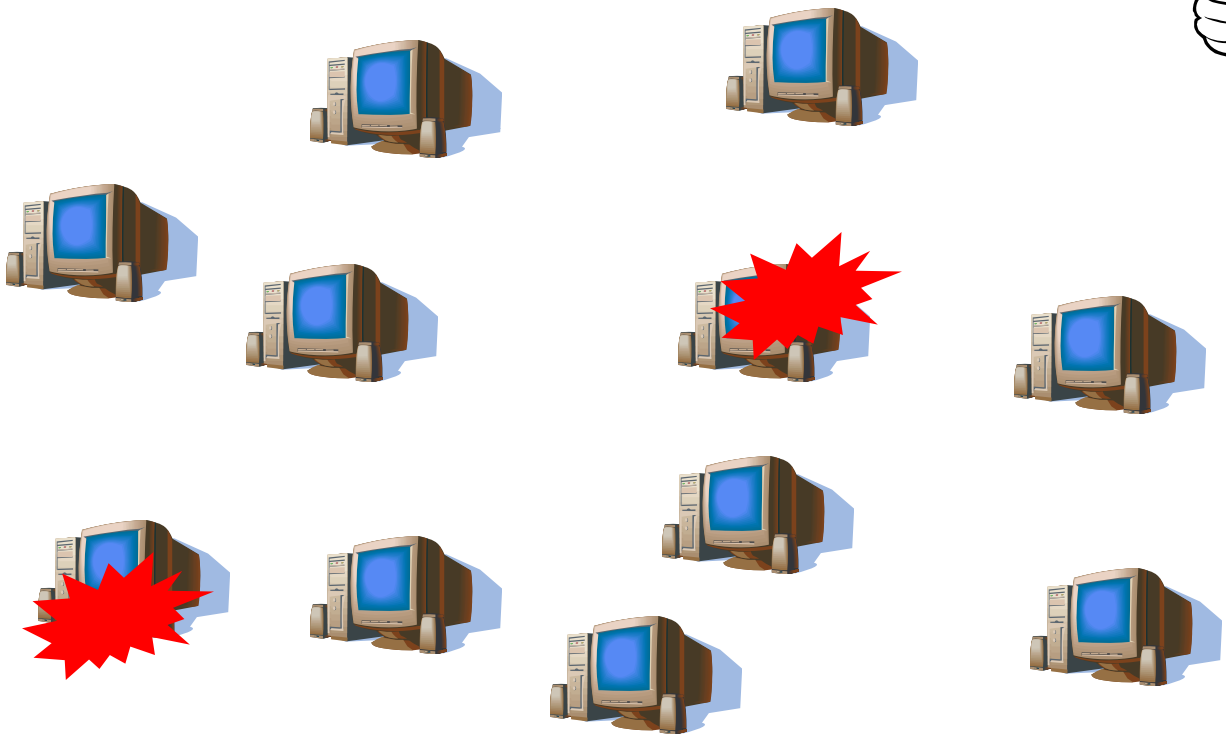
Data Diversity in Nature

- DNA is ***data***
- Data diversity appears to be random in Nature
- Survival by natural selection implies better genes

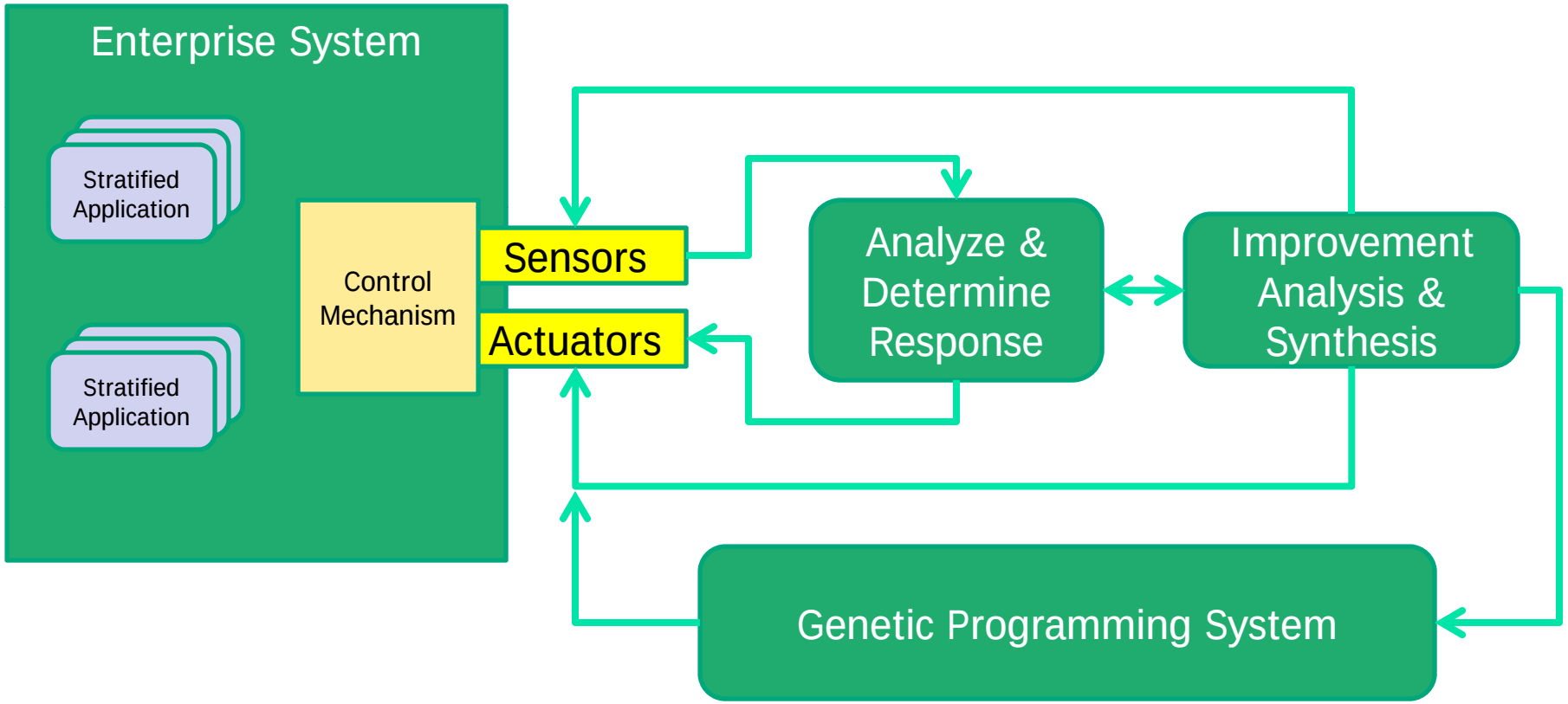


Diverse Population

Threat



Regeneration & Improvement



Genetic Disease

- Suppose DNA is defective in some way
- Result is a genetic disease
- Solution:

Genetic engineering

- Computer “genetic disease”:

Security vulnerability

- Solution:

Program repair via genetic programming

Summary

Helix provides:

- Diverse population of system
- Enterprise-wide flexible sensing, actuation and protection mechanism via application virtualization
- Incorruptibility:
  - Extensive and evolvable enterprise protection
- Diversity ensures population will survive attack
- Regeneration by:
  - Reproduction – new population members
  - Surgical repair of damaged population members
- Treatment of vulnerabilities (genetic disease) by repair

Questions?

Further details:

http://helix.cs.virginia.edu