Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

Science Supporting Security™

Re-envisioning "fault management" to enable resilient operation of modern complex adaptive systems

Fault Management in Complex Adaptive Systems: Applications and Challenges on the Horizon

Dr. Werner J.A. Dahm

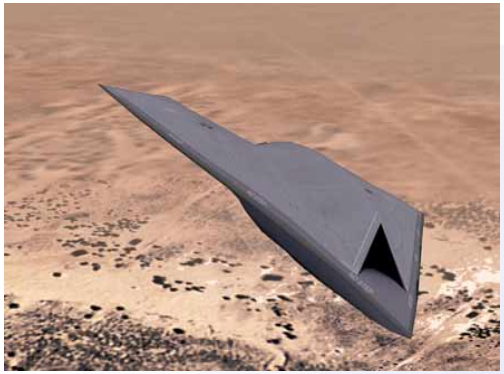
Director, Security & Defense Systems Initiative
Arizona State University

http://sdsi.asu.edu

2012 NASA Spacecraft Fault Management Workshop, New Orleans, LA, 10-12 April 2012

What Does "Fault Management" Mean?

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY



System Resilience

Reliability

Fault Detection

Autonomy

Integrated System Health Management

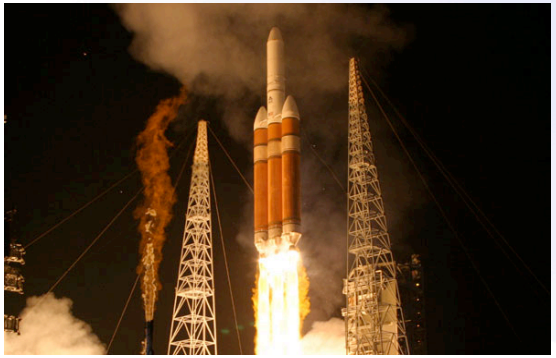
Fault Management

Goal-Based Supervisory Control

Complex Adaptive Systems

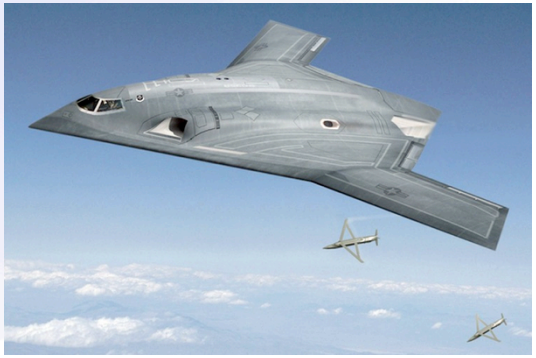
Complex Software Engineering

Fault Tolerance



Verification and Validation

Model-Based Systems Engineering



Key Points in this Presentation

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

1. A transformation is underway in which "complex adaptive systems" are increasingly replacing traditional "simple engineered systems"
2. Complex adaptive systems (CAS) are based on self-awareness and continual autonomous adaptation to maximize achievement of goals
3. Current "fault management" envisions nominal operations punctuated by occasional occurrences of a defined set of anticipatable "faults"
4. As system complexity increases, number of possible faults becomes so large that the tradtional fault management approach is untenable
5. Existing fault management approaches were developed for "simple" engineered systems, and are not suited for complex adaptive systems
6. Applying the current fault management paradigm to complex adaptive systems will result in cost/schedule issues and system failures
7. CAS make no distinction between "nominal" operations and "faults"; in such systems, resilient goal-driven operation is the "norm"
8. Autonomous goal-driven context-aware system adaptation depends on current system state, operating environment, and goal hierarchy

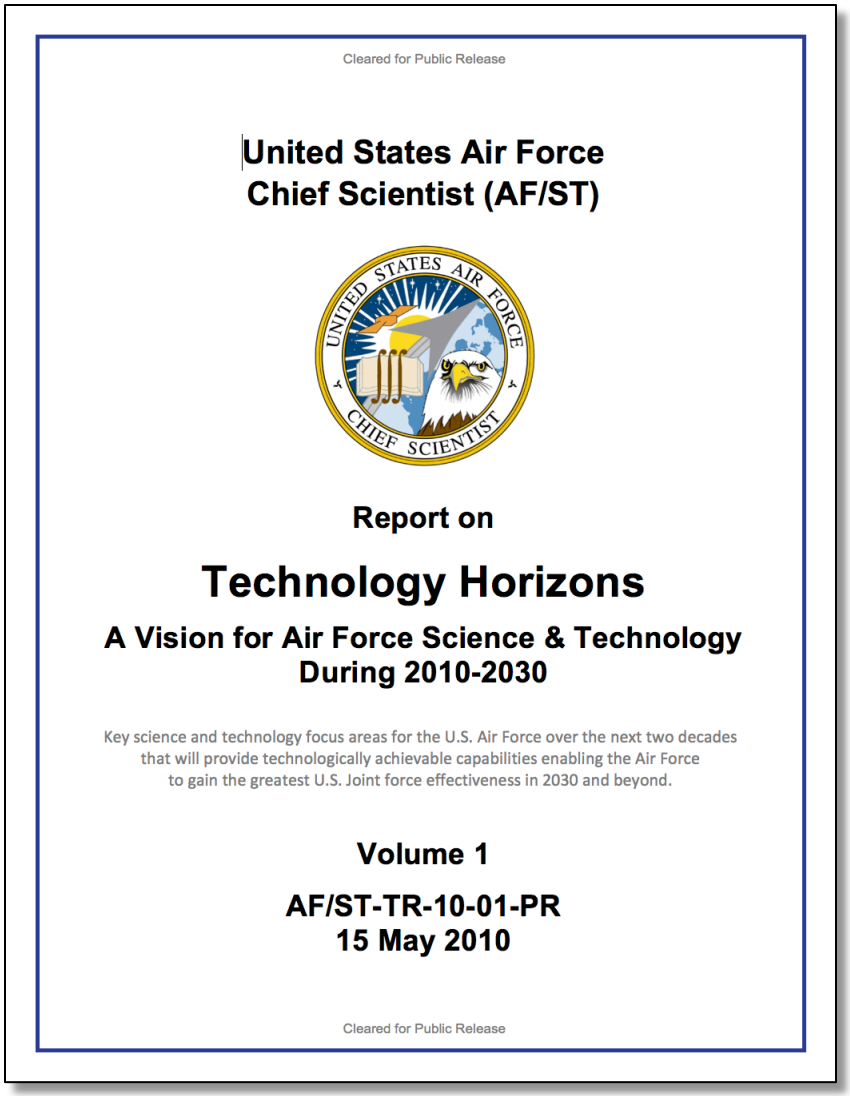
Key Points in this Presentation

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

9. Must establish "certifiable trust" in system performance that cannot be inferred or anticipated from behavior of the individual elements
10. High levels of system adaptation and numbers of inputs make these near-infinite state systems, for which "traditional" V&V is unsuited
11. Neither the intended system performance, nor bounds on acceptable performance, nor limits of actual performance are currently knowable
12. Requires developing new principles for architecting software that can support needed levels of system complexity and adaptability
13. Such adaptable systems can be architected using software systems engineering approaches to make them inherently more V&V-able
14. Adaptive learning with stochastic dither leads to non-deterministic systems that increase the difficulty in establishing certifiable trust
15. Largest uncertainties in certifying that the system will perform within acceptable bounds come from high-dimension small-sample problem
16. What level of confidence in system performance can be considered acceptable to justify the benefits that such systems can provide?

U.S. Air Force "Technology Horizons"

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY



Cleared for Public Release

United States Air Force
Chief Scientist (AF/ST)

Report on

Technology Horizons

A Vision for Air Force Science & Technology During 2010-2030

Key science and technology focus areas for the U.S. Air Force over the next two decades that will provide technologically achievable capabilities enabling the Air Force to gain the greatest U.S. Joint force effectiveness in 2030 and beyond.

Volume 1

AF/ST-TR-10-01-PR
15 May 2010

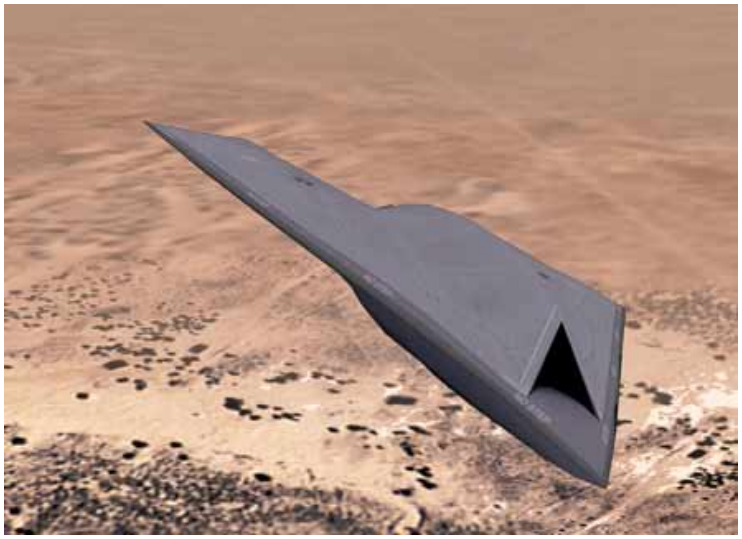
Cleared for Public Release

- Strategic Context
- Enduring Realities
- Overarching Themes
- Potential Capabilities
- Key Technology Areas
- "Grand Challenges"
- Principal Findings
- Implementation Plan

Growth of Complex Adaptive Systems

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

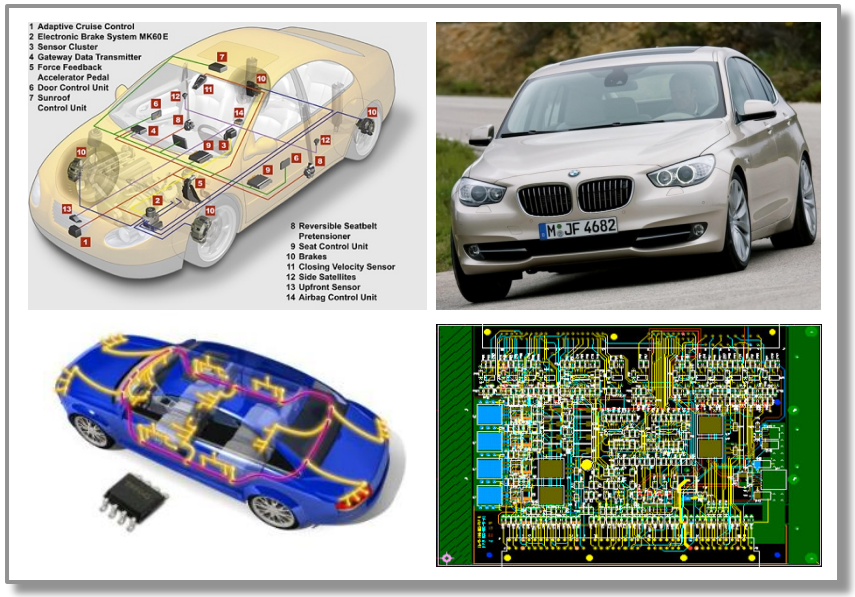
- DoD is in early stages of a transformation to far greater use of autonomous systems and processes; beyond just unmanned vehicles
- Capability increases, workforce efficiencies, and cost reductions are possible through increased use of autonomous systems
- Dramatic increase in range of systems and processes where autonomous reasoning and control can be applied
- Autonomous systems are inherently based on system self-awareness and adaptability to adjust system to maximize its capability
- S&T to establish "certifiable" trust in highly adaptible autonomous systems is a key to enabling this transformation
- Traditional "fault management" approaches must be substantially re-engineered to enable "flexibly autonomous" systems in a wide range of DoD and civil applications



Examples: Complex Adaptive Systems

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

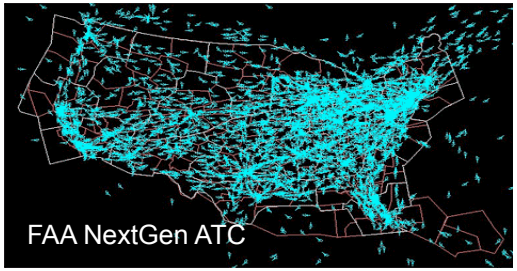
- 5th-generation fighter A/C are deeply integrated software-driven systems
- Overwhelming majority of functions are driven autonomously by software
- Software development and validation account for over 50% of costs
- DoD systems (adaptive radars, UCAVs, etc.) are now increasingly autonomous

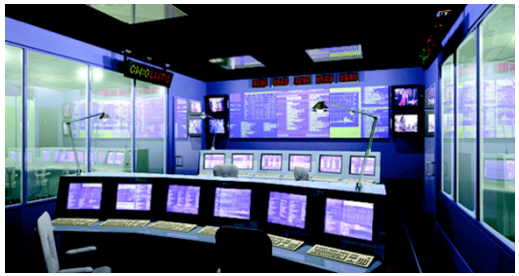


- Premium cars today are controlled by *O*(100) interconnected ECUs
- E.g., autobraking, lane drift warning, autonomous parallel parking, etc.
- 70% of development costs and 40% of production costs are software systems
- Systems today are highly federated but subsystem interactions are increasing

Examples: Complex Adaptive Systems

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

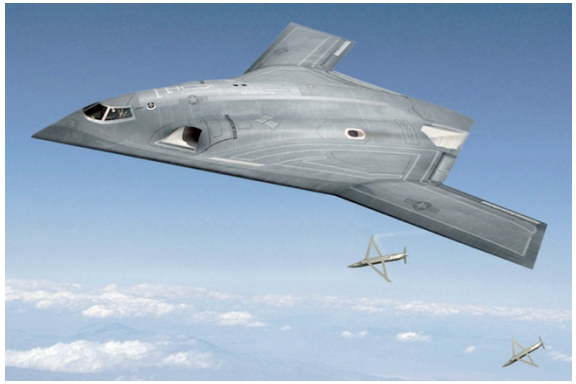


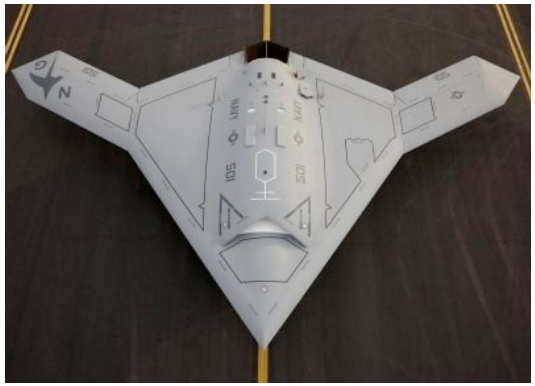


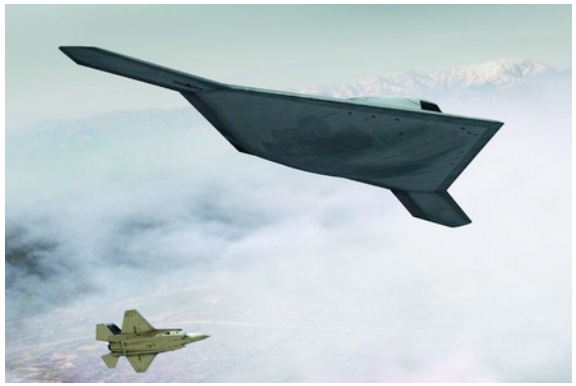
Examples: Complex Adaptive Systems

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- Planned manned and unmanned aircraft systems with high levels of adaptability and autonomy
- Aircraft control system allows self-adaptation to battle damage, component failures, etc.
- Can apply to aircraft structure, control surfaces, avionics, or even to changing threat environment
- On-board real-time reconfiguration of aircraft control system to maximize remaining capability
- Involves adaptive guidance and control (AG&C) system with autonomous high-level reasoner



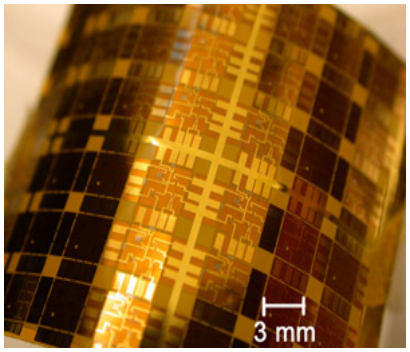


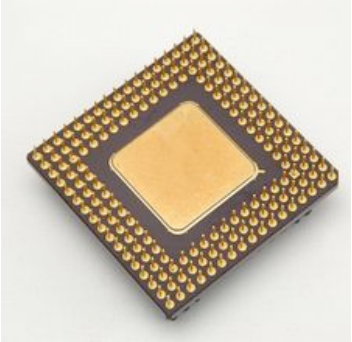
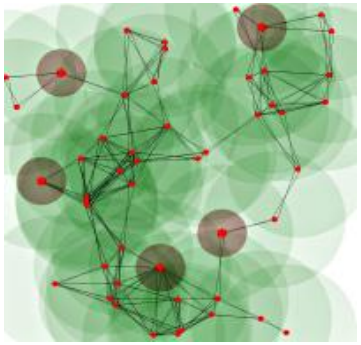


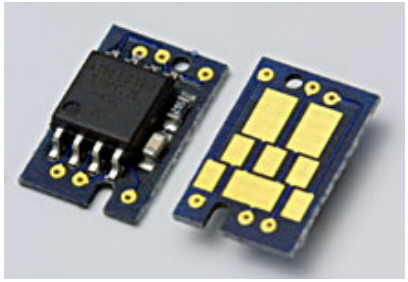
Enablers of Complex Adaptive Systems

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- Miniaturization
  - MEMS fabrication
- Ubiquitous sensing
  - Small, cheap, reliable
  - Multi-modality
- Embedded processing
  - Multi-core, GPGPUs
  - Processing speeds
- Storage
  - Compact terabyte-scale
  - Inexpensive, solid-state
- Software adaptation/learning
  - Expert systems
  - Genetic algorithms
  - Machine learning
  - Stochastic dither





Adaptable Autonomous System Attributes

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

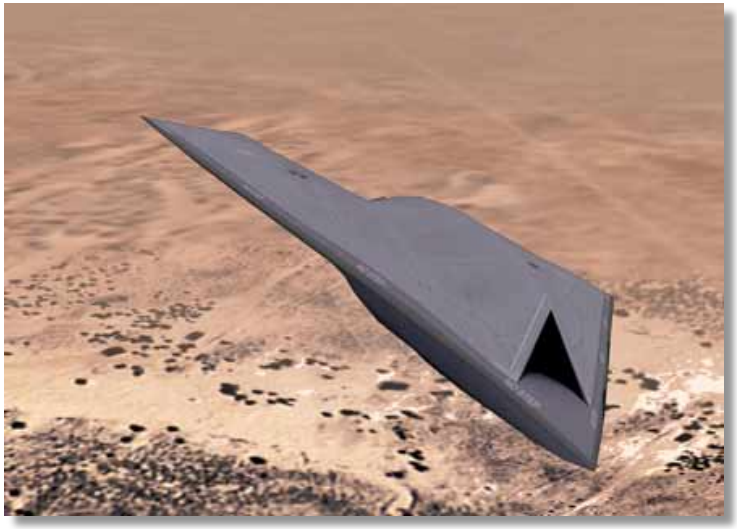
Four Required Attributes of Highly Adaptable Autonomous Systems

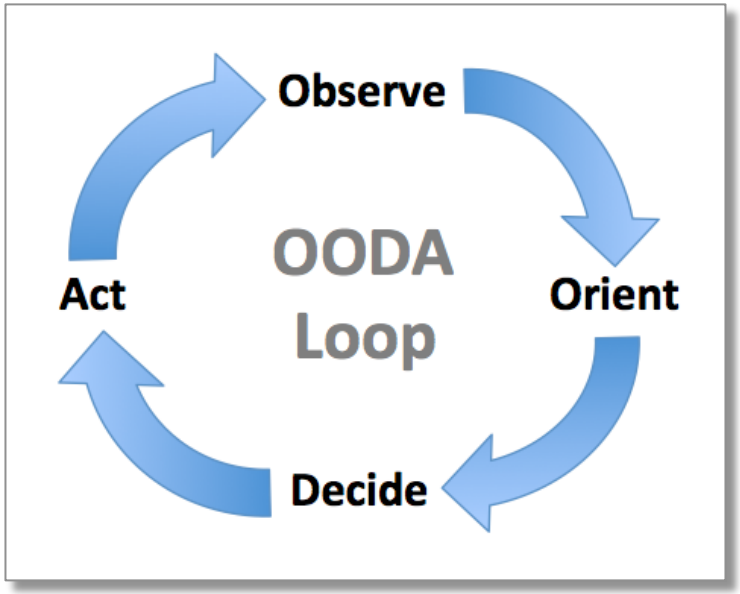
- **Large number of on/off-board inputs (embedded sensors; other platforms)**
- **Large number of <u>interdependent</u> decisions (via fusion of input data)**
- **Large number of system adaptations (may be deterministic or stochastic)**
- **Adaptations evolve continuously based on feedback-driven learning**

As the number of inputs and the number of possible system adaptations increase, these become near-infinite state systems

Mostly driven by number of adaptations

Makes it hugely difficult to prove that such systems will always operate as intended

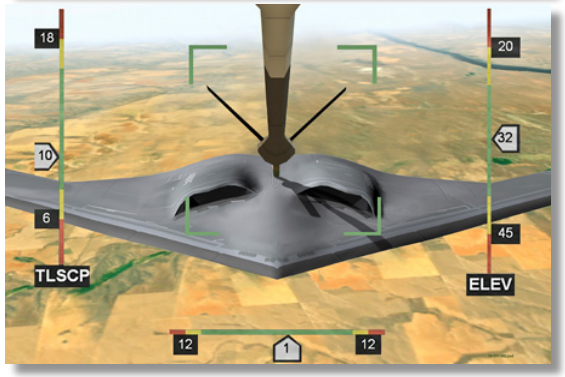


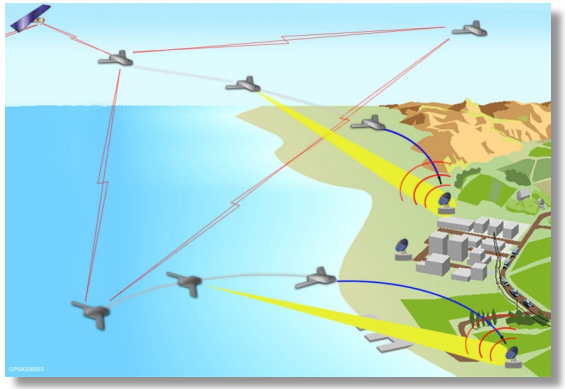


Elements of Complex Adaptive Systems

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- Systems composed of many interacting agents, with system evolving over time via adaptation
  - Agents are at least partly autonomous
  - No agent has full global view of the system
  - Decentralized structure in which no agent has full control of the others
- In some systems all agents may be identical and simple; in others all are different and non-simple
- Resulting complex system behavior is more than 'sum of the parts' – nonlinear dynamics
- Emergent high-level system behavior driven by dynamics of simultaneous interactions of agents
- Typically cannot be fully inferred or anticipated from behaviors of the individual agents
- Number of agents and nature of interactions matter; threshold for emergent behavior

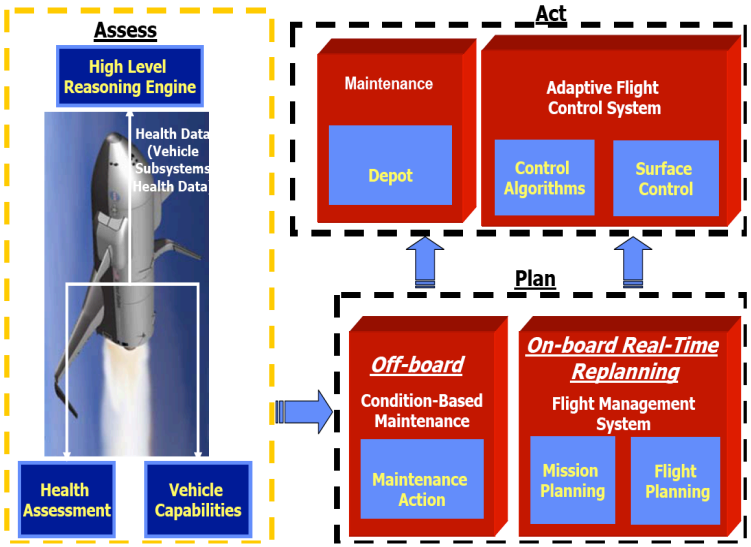




State Awareness and System Adaptation

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- Distributed sensing allows systems to have high levels of "state awareness"
- System "state awareness" can include:
  - Self-awareness (system health)
  - Operating environment awareness
- May include system self-experimentation to assess current state and capabilities
- State assessment and current goals are inputs to a high-level reasoning engine
- Seeks context-aware goal-driven system adaptation to best meet operator's intent
- System adaptation may be autonomous or with human supervisory control
- Eliminates preplanned responses to a discrete set of anticipated faults
- Allows resilient system performance even for unanticipatable fault scenarios



From Deriso (2005)

Autonomy and System Adaptation

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- Adaptation may range from human-driven to fully-autonomous … "flexible autonomy"
- Adaptation decisions can span from slow inputs for scheduling to real-time control
- Real-time adaptation seeks best course of action without relying on preplanned options
- Autonomous reasoning engine uses a goal hierarchy that allows less-than-full solutions
- Operator interacts with system at goal-level; task-level control is derived autonomously
- Involves elements of machine intelligence, high-level reasoning, self-learning algorithms
- Could involve stochastic experimentation; e.g., continually self-adaptive coefficients
- Autonomous system adaptation provides the basis for "complex adaptive systems"

“Traditional” Fault Management

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- Traditional “fault management” is based on detection, isolation, identification and response to a discrete set of anticipated faults
- Envisions the system operating in a “nominal state” punctuated by occasional occurrences of anticipatable pre-defined “faults”
- Fault management involves anticipating the set of faults and then developing an appropriate set of responses for each
- Works well if system is sufficiently simple; i.e., a low degree of adaptability and limited interdependences between subsystems
- As system complexity increases, number of possible faults can grow so large that this approach becomes increasingly difficult
- Not all faults are properly anticipated, and greater likelihood of multiple-fault interactions can lead to fault management failures
- Becomes increasingly important to address fault management early in system development; as system complexity grows, fault management consumes substantial share of development cost

Fault Management in Adaptive Systems

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- As systems become increasingly complex and adaptive, number of system states and failure modes becomes uncountable
- Classical separation between “nominal operation” and “faults” becomes untenable; system is continually operating under faults
- Continued application of traditional fault management paradigm to such systems will lead to schedule and cost issues, and failures
- Traditional “fault management” must be replaced by continuous system adaptation to achieve a defined goal hierarchy;
- No longer makes a distinction between “nominal operation” and “pre-defined faults”; resilient operation under faults is the “norm”
- A “fault” is now “anything that causes the system to adapt”; may not be due to component failures, and traceability is irrelevant
- Replaces “fault management” challenge with the need to develop flexibly autonomous control architecture with sufficient high-level goal-driven adaptability to enable operation under all conditions

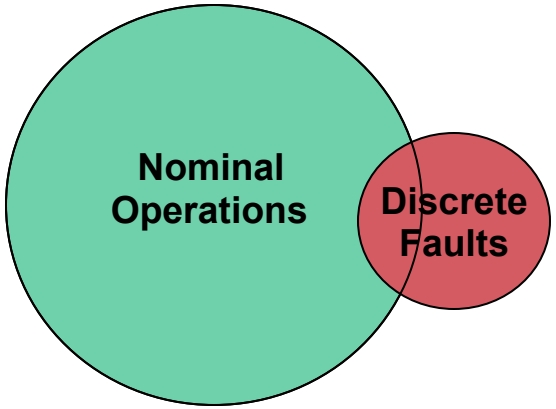
Fault Management in Adaptive Systems

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

Traditional "Simple" Engineered Systems

- **Involve a relatively small number of discrete fault modes that can be anticipated**
- **Appropriate system response for each fault can be determined beforehand**
- **Fault management involves process to find and classify faults and develop responses**
- **Fault detection, localization, identification characterization, and pre-scripted response**

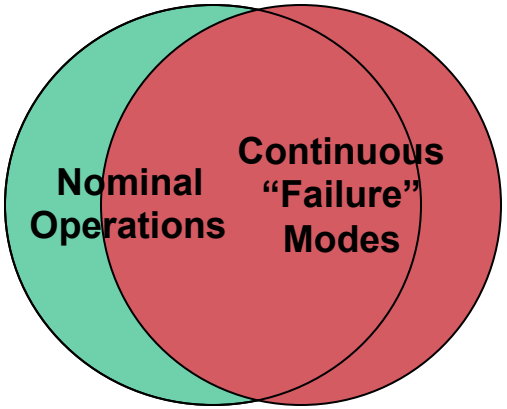
Simple systems involve preplanned responses to a discrete set of anticipatable fault modes



Emerging "Complex Adaptive Systems"

- **System complexity and adaptability creates near-infinite, continuous set of fault modes**
- **Concept of "nominal" operation punctuated by occasional "faults" no longer applies**
- **System is always operating in failure modes and continually developing best responses**
- **Appropriate goal-level response depends on system state, environment, and goal network**

Involves continuous goal-driven adaptation to an uncountable number of "failure" modes



Fault Management in Adaptive Systems

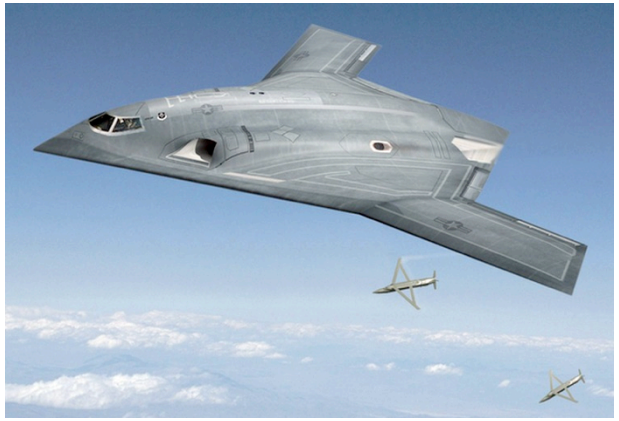
Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

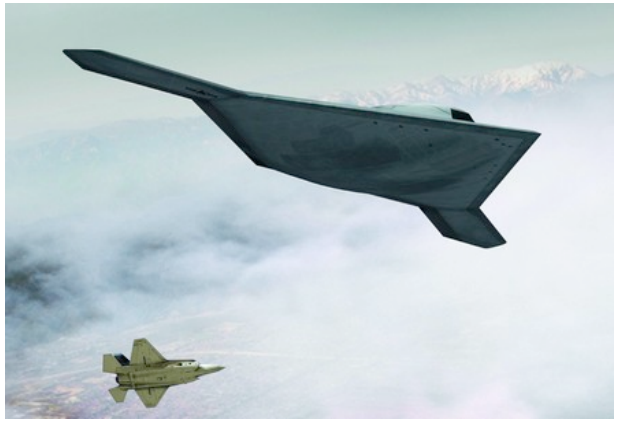
- Near-infinite set of possible "faults" in complex adaptive systems makes traditional fault identification largely impossible
- However, goal-based autonomous reasoning and control makes fault identification non-essential, and possibly counter-productive
- Notion of discrete fault management is replaced by presumption of continually evolving fault environment to which system adapts
- Requires developing new principles for architecting software that can support needed levels of system complexity and adaptability
- Extends well beyond traditional software engineering challenges for large software; high levels of system adaptability create major challenges for software testing and certification
- Complex adaptive system software becomes increasingly less deterministic due to goal-driven context-aware adaptability
- Verification and validation of complex adaptive control software becomes a major challenge; these are near-infinite state systems

“Trust” in Complex Adaptive Systems

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- DoD must establish “certifiable trust” in any system before it can be fielded
- Key driver is V&V of the complex software in highly adaptable autonomous system
- Drives current development costs and limits degree of autonomy that can be fielded
- Law/policy restrictions as well as cultural resistance to field “uncertifiable autonomy”
- Highly adaptable autonomous systems are far simpler to build than to adequately V&V
- Creates potential asymmetric advantage for adversaries who field uncertified systems
- Maintain supervisory control via “flexible autonomy” driven by “human in the loop”
- Methods to achieve “certifiable trust” in autonomous systems is a key DoD need





Software Growth & Error Rates/Types

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

Equivalent Software Lines of Code

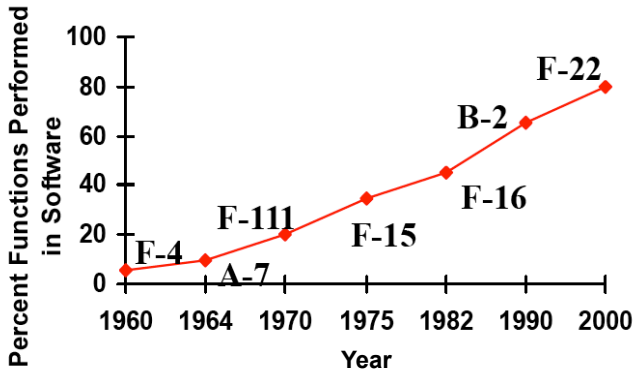
System	ESLOC
F-4A	1,000
F-15A	50,000
F-16C	300,000
F-22	2,500,000
Android OS	12,000,000
F-35A	18,000,000
2011 BMW 535i	>80,000,000

Growth in Adaptability and Factors Driving System Certifiability

	Simple			CAS
Adaptability	None	User Adaptive	Competitor Adaptive	Full Scope Adaptation
Control	Central	Disaggregated	Distributed	Virtual
ESLOC	10,000	100,000	1,000,000	>10,000,000
Structure	Discrete Product	Multiple Products	Loosely Integrated	Integrated Assemblage
Certifiability	Validated	Semi-Validated	Weakly Validated	???????

Percent of Functions Performed in Software

Adapted from Nidiffer (2008) CMU Software Engineering Institute

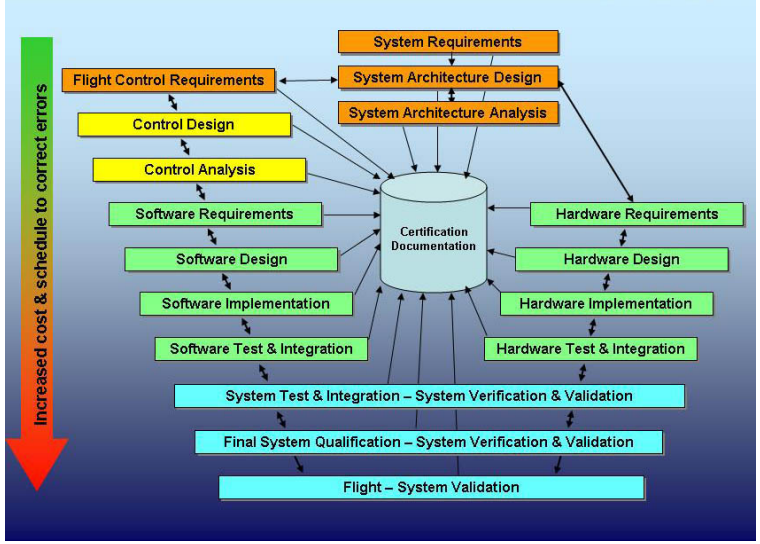


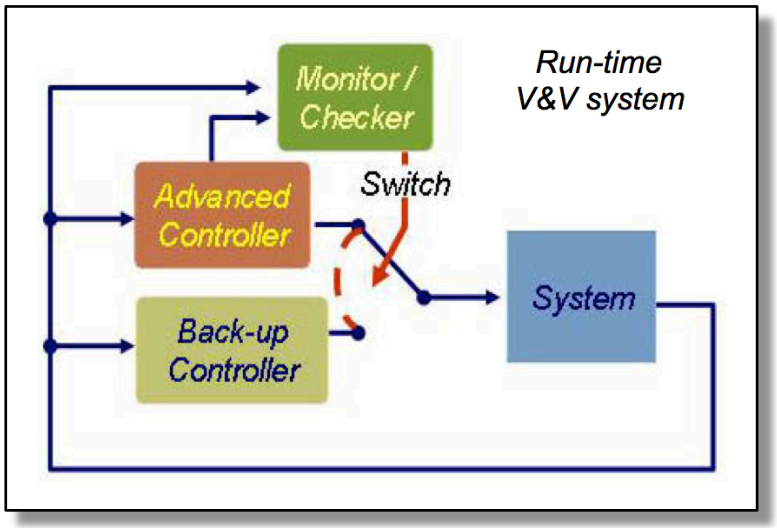
- **4-6 errors/KSLOC rate for average suppliers; critical code has 0.1-1.0 errors/KSLOC**
- **E.g., F-35A can expect to have *O*(1800) errors in its operational flight program (OFP)**
- **F-35 is "tested to exhaustion" … of budget; over half of development cost is software**
- **Most errors are not from code complexity, but from logic complexity due to adaptivity**

Formal Methods vs "Run-Time V&V"

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- Formal methods for finite-state systems based on abstraction and model-based checking do not extend to such systems
- Probabilistic or statistical tests do not provide the needed levels of assurance; set of possible inputs/states far too large
- Classical problem of "proving that failure will not occur" is the central challenge
- Run-time approach circumvents usual limitation by inserting monitor/checker and simpler verifiable back-up controller
- Monitor system state during run-time and check against acceptable limits
- Switch to simpler back-up controller if state exceeds limits
- Simple back-up controller is verifiable by traditional finite-state methods



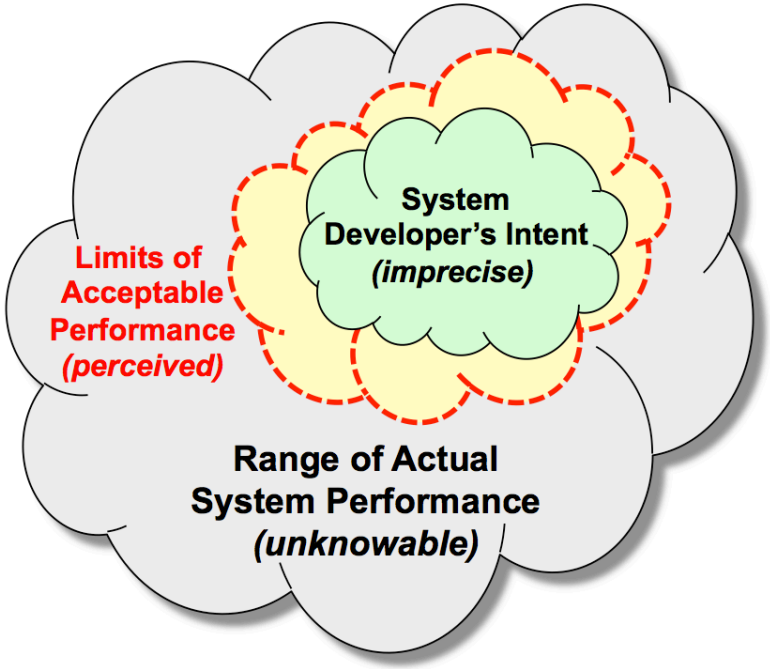


No "Truth Data" for Adaptive Systems

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- Larger uncertainties in V&V of such systems are from lack of "truth data"
- For near-infinite state systems, range of actual performance is unknowable
- Even developer's intent for range of system performance is imprecise
- Cannot anticipate all situations that the system may need to perform in
- Instead define situation-independent limits of acceptable performance
- Replaces intent (positive) with bounds on performance (non-negative)
- Even these bounds can only be based on perceived acceptability
- Not based on comparisons with truth data or uncertainty quantification
- Acceptability of performance based on unknown or ill-defined criteria

Central Problem of V&V in Highly Adaptable Autonomous Systems



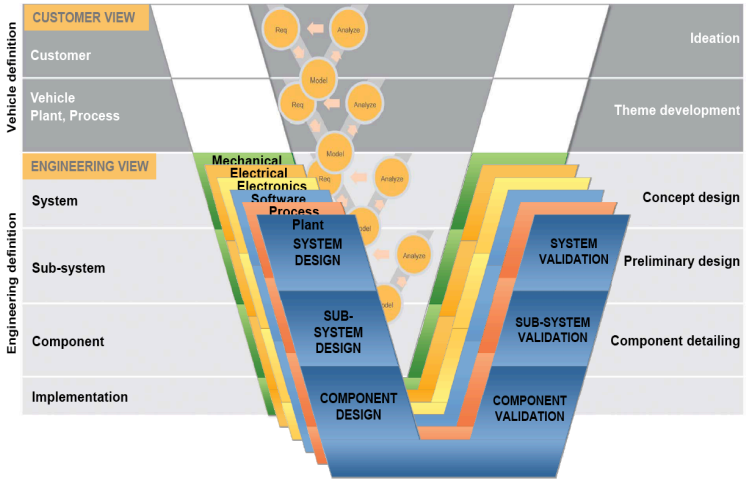
System validation is based on assessing the acceptability of performance based on unknown or ill-defined criteria

V&V for Complex Adaptive Systems

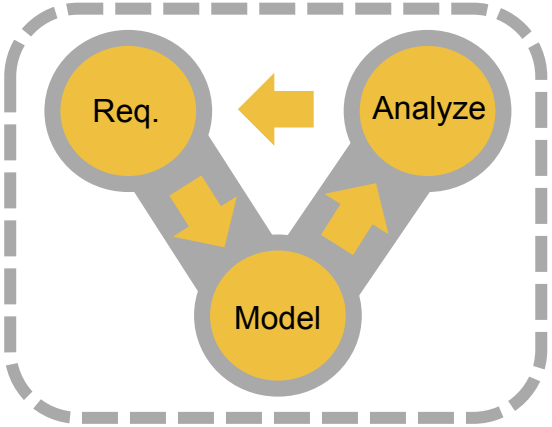
Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- In CAS, developer's intent is typically not in form of governing equations
- V&V instead centers on assessing if system performs as was intended
- Intended range of inputs states must be tested for each system adaptation
- But near-infinite state systems make such "direct V&V" impossible
- Requires a different concept for how V&V can be achieved for CAS
- One possibility is based on a software systems engineering approach
- Decompose system into lower-level elements with requirements for each
- Aggregated model for each element at each level is simple enough to V&V
- Do these simpler models suffice to V&V the system?

Systems engineering V-model for V&V of CAS



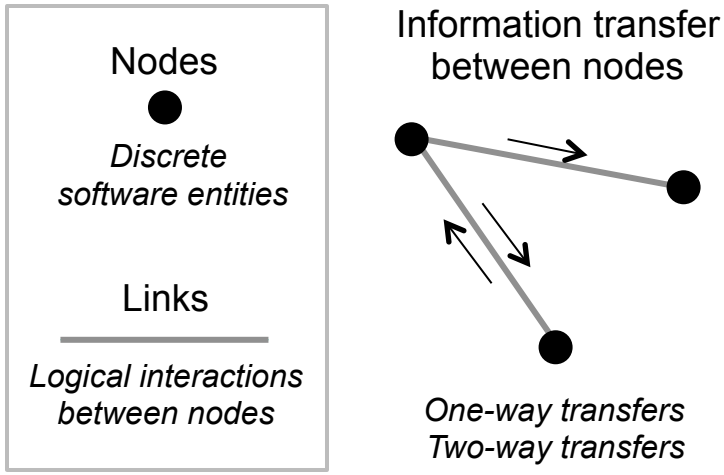
"Unit cell" V&V process at each level of V-model

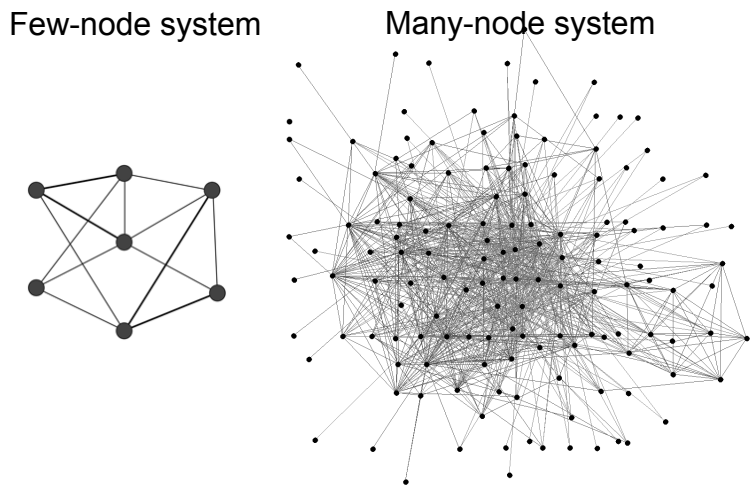


V&V for Complex Adaptive Systems

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- **Interactions among software agents represented by network diagram**
- **Information transfer between entities via data- or state-sharing alters nodes**
- **Adaptation within the system occurs as node-states change by interactions**
- **"Few-node systems" have dynamics that are driven by node models**
- **"Many-node system" dynamics largely result from interactions among nodes**
- **Model fidelity of individual nodes is less important than fidelity of links**
- **Simple V&V-able nodes can still lead to complex non-V&V-able system**
- **As the number of possible system adaptations increases, the logic of all possible interactions exceeds what can be understood or analyzed**

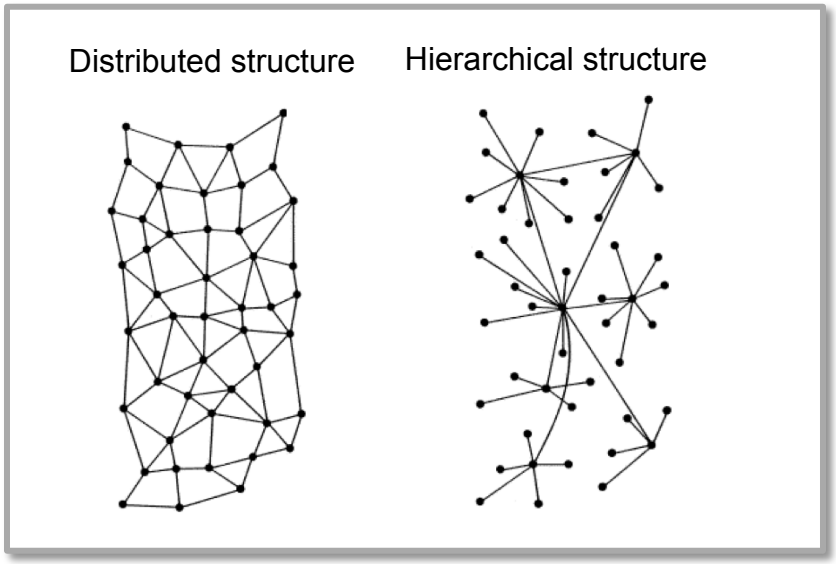


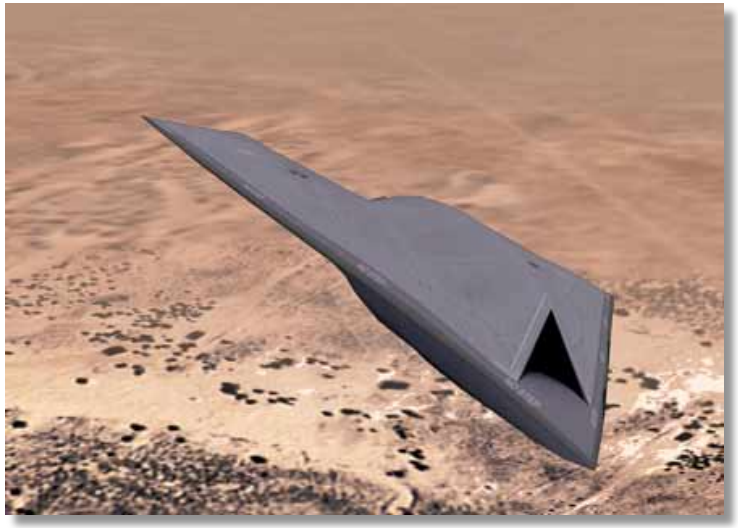


Architecting Software to Enable V&V

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- Complex adaptive systems will have many-node network structures
- Can the network structure underlying a CAS be architected to enable V&V?
- Use hierarchical approach to do V&V at each level of system aggregation
- Highly distributed structures cannot be effectively aggregated to allow V&V
- System must be designed from outset to achieve needed hierarchical form
- "Design for V&V-ability" is not done today; it may be a key for future CAS
- Granularity at each level must be fine enough to permit clustered modeling
- Limits of clustered model fidelity will introduce uncertainty in V&V results
- Not the largest source of uncertainty



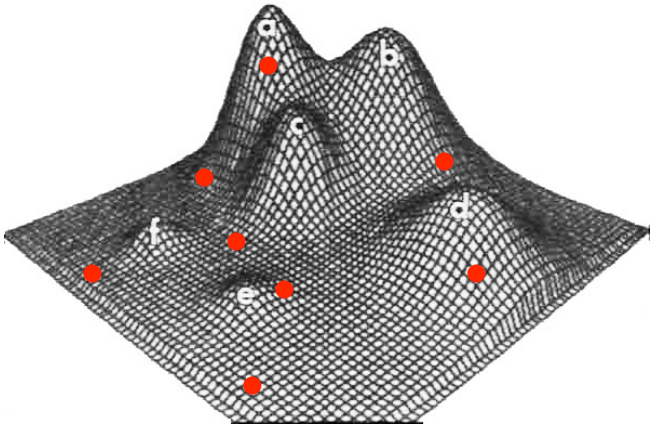


“Near-Infinite State System” Problem

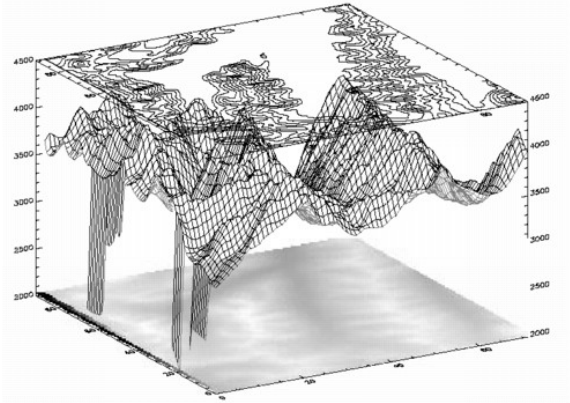
Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

- The current system state and inputs define the sample space for V&V
- Near-infinite state systems will have exceedingly high dimensionality
- It is only possible to test a vanishingly small fraction of the sample space
- Classic high-dimension small-sample problem; how do we maximize utility?
- High-dimensional response surface approaches will be effective here
- Factorial methods and outlier cases
- Response surfaces may be poorly behaved due to strong nonlinearity
- Leads to high level of uncertainty that system will stay in acceptable bounds
- Clustered model fidelity and unknown acceptability criteria add uncertainty

V&V in CAS becomes an increasingly high-dimension small sample-size problem as system adaptability increases



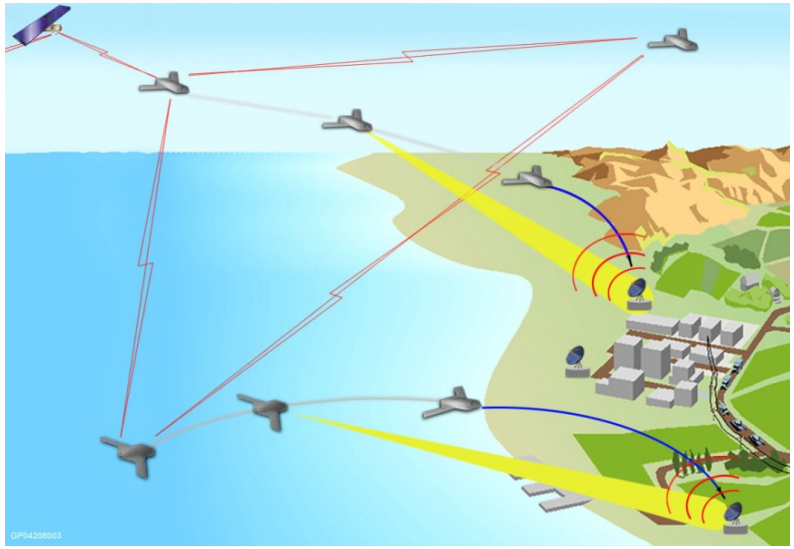
Near-infinite state systems may have very poorly behaved response surfaces that prevent needed validation confidence

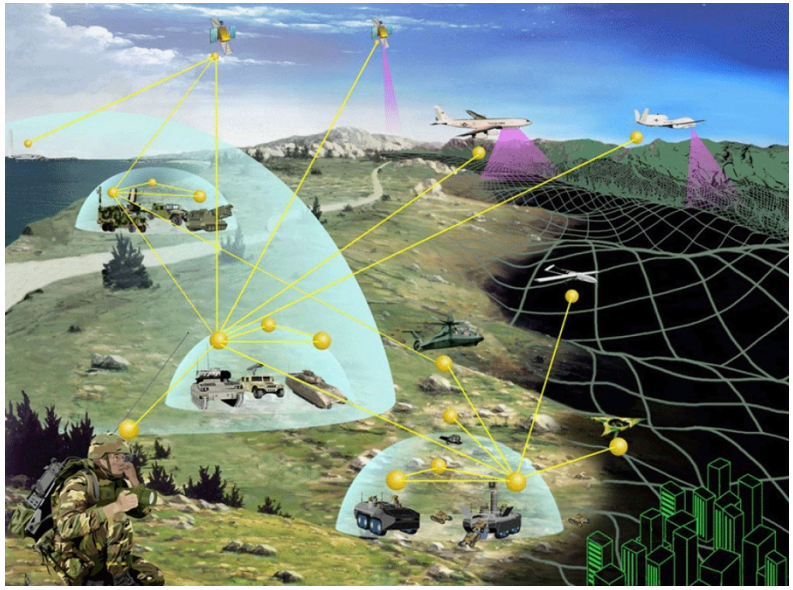


V&V of Non-Deterministic Systems

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

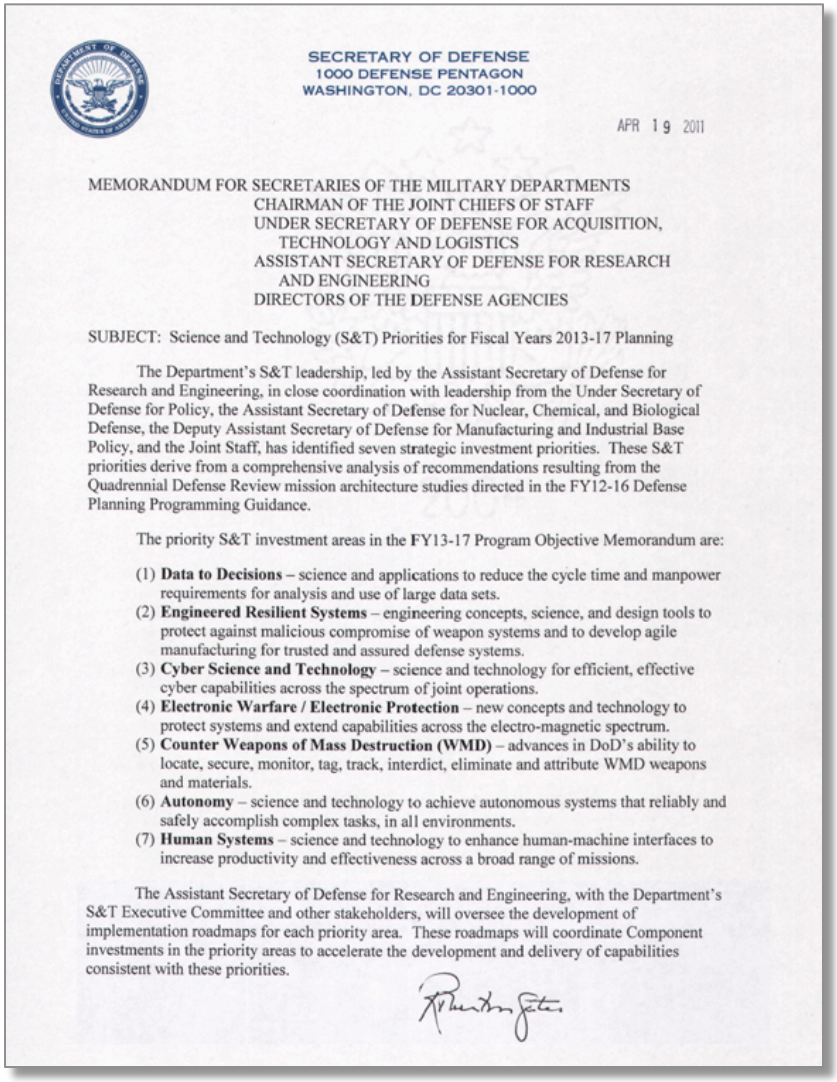
- Adaptive learning with dither will lead to non-deterministic systems
- Given initial state and inputs produce different system-level performance
- Creates additional statistical element that further complicates V&V for CAS
- However larger uncertainies in system performance come from other sources
- What confidence level must be shown to establish "certifiable trust" in CAS?
- "Apollo-era" low-dimensional finite state systems set demand near 100%
- Subsequent higher-dimensional finite state systems still use >99% criteria
- CAS will need far more relaxed criteria
- 'Not one life lost' mentality misses the human cost of lost opportunities





DoD's Stated S&T Priorities for FY13-17

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

APR 19 2011

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY AND LOGISTICS
ASSISTANT SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Science and Technology (S&T) Priorities for Fiscal Years 2013-17 Planning

The Department's S&T leadership, led by the Assistant Secretary of Defense for Research and Engineering, in close coordination with leadership from the Under Secretary of Defense for Policy, the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense, the Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy, and the Joint Staff, has identified seven strategic investment priorities. These S&T priorities derive from a comprehensive analysis of recommendations resulting from the Quadrennial Defense Review mission architecture studies directed in the FY12-16 Defense Planning Programming Guidance.

The priority S&T investment areas in the FY13-17 Program Objective Memorandum are:

(1) **Data to Decisions** – science and applications to reduce the cycle time and manpower requirements for analysis and use of large data sets.
(2) **Engineered Resilient Systems** – engineering concepts, science, and design tools to protect against malicious compromise of weapon systems and to develop agile manufacturing for trusted and assured defense systems.
(3) **Cyber Science and Technology** – science and technology for efficient, effective cyber capabilities across the spectrum of joint operations.
(4) **Electronic Warfare / Electronic Protection** – new concepts and technology to protect systems and extend capabilities across the electro-magnetic spectrum.
(5) **Counter Weapons of Mass Destruction (WMD)** – advances in DoD's ability to locate, secure, monitor, tag, track, interdict, eliminate and attribute WMD weapons and materials.
(6) **Autonomy** – science and technology to achieve autonomous systems that reliably and safely accomplish complex tasks, in all environments.
(7) **Human Systems** – science and technology to enhance human-machine interfaces to increase productivity and effectiveness across a broad range of missions.

The Assistant Secretary of Defense for Research and Engineering, with the Department's S&T Executive Committee and other stakeholders, will oversee the development of implementation roadmaps for each priority area. These roadmaps will coordinate Component investments in the priority areas to accelerate the development and delivery of capabilities consistent with these priorities.

1. Data to Decisions
2. Engineered Resilient Systems
3. Cyber Science and Technology
4. Electronic Warfare / Electronic Protection
5. Counter Weapons of Mass Destruction
6. Autonomy
7. Human Systems

ASD(R&E) Systems 2020 Initiative

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

Systems 2020 is an Initiative from the Assistant Secretary of Defense (Research & Engineering)

$100M over 5 years (FY12 – 16)

UNCLASSIFIED

SYSTEMS ENGINEERING
Research Center

Systems 2020
Strategic Initiative

Final Technical Report SERC-2010-TR-009

August 29, 2010

Principal Investigator: Dr. Barry Boehm,
University of Southern California

Contributors: Jennifer Bayuk, Abhi Desmukh, Robert Graybill, JoAnn Lane, Alan Levin, Azad Madni, Mike McGrath, Art Pyster, Stas Tarchalski, Richard Turner, and Jon Wade

Contract Number: H98230-08-D-0171 , DO 002, TO 0002, RT 0020

Report No. SERC-2010-TR-009
FINAL August 29, 2010
UNCLASSIFIED

Systems 2020 Research Areas

1. Model-Based Systems Engineering

- M&S throughout the development process
- More effective concept engineering
- Concurrent design, develop, deploy, and evolve

2. Platform-Based Engineering

3. Capability on Demand

- Embedded organic adaptation capabilities
- On-demand adaptability
- Self-adaptive systems
- Field-adaptive systems

4. Trusted Systems Design

Basic Science Issues are identified for each of these areas

This is a Community-Wide Challenge!

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

Today's Main "Take Away" Points

Security and Defense Systems Initiative
ARIZONA STATE UNIVERSITY

1. Complex adaptive systems (CAS) are based on self-awareness and continual autonomous adaptation to maximize achievement of goals
2. Existing fault management approaches were developed for "simple" engineered systems, and are not suited for complex adaptive systems
3. Applying the current fault management paradigm to complex adaptive systems will result in cost/schedule issues and system failures
4. CAS make no distinction between "nominal" operations and "faults"; in such systems, resilient goal-driven operation is the "norm"
5. Autonomous goal-driven context-aware system adaptation depends on current system state, operating environment, and goal hierarchy
6. High levels of system adaptation and numbers of inputs make these near-infinite state systems, for which "traditional" V&V is unsuited
7. Such adaptable systems can be architected using software systems engineering approaches to make them inherently more V&V-able
8. Largest uncertainties in certifying that the system will perform within acceptable bounds come from high-dimension small-sample problem

Security and Defense Systems Initiative

ARIZONA STATE UNIVERSITY

Science Supporting **Security**™

For additional information, please contact:

Dr. Werner J.A. Dahm

Director, Security & Defense Systems Initiative
Arizona State University

Werner.Dahm@asu.edu
480-727-8598

32