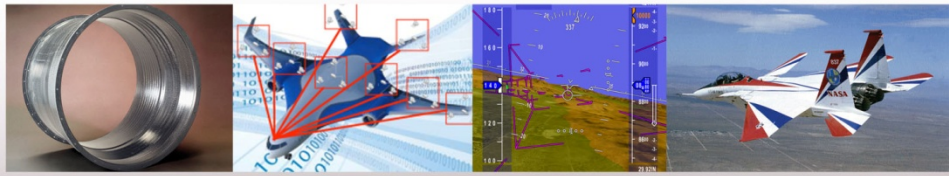
National Aeronautics and Space Administration

NASA Aviation Safety Research
Verification & Validation of Flight Critical Systems (VVFCS) – The Way Ahead



Sharon Graves
NASA Aviation Safety Program
Verification and Validation Summit 2010
October 13-14, 2010

Why VVFCS?

By 2025, U.S. air traffic is predicted to increase 2 to 3 times.

R-1440 Applied Research on Complex Systems Validation and Verification

Applied research on the methods and algorithms to support the validation and verification of complex systems...

EN-3050 Advanced Complex System Validation and Verification Methods

Description: Advanced tools and processes are developed to improve the verification and validation of complex systems and software. Improvements will focus on reducing the time and resources needed to conduct validation and verification as well as improving the quality of the results. ...

INCREASED SAFETY

Our goal is to achieve the lowest possible accident rate and constantly improve safety.

From 2009-2013 FAA Flight Plan

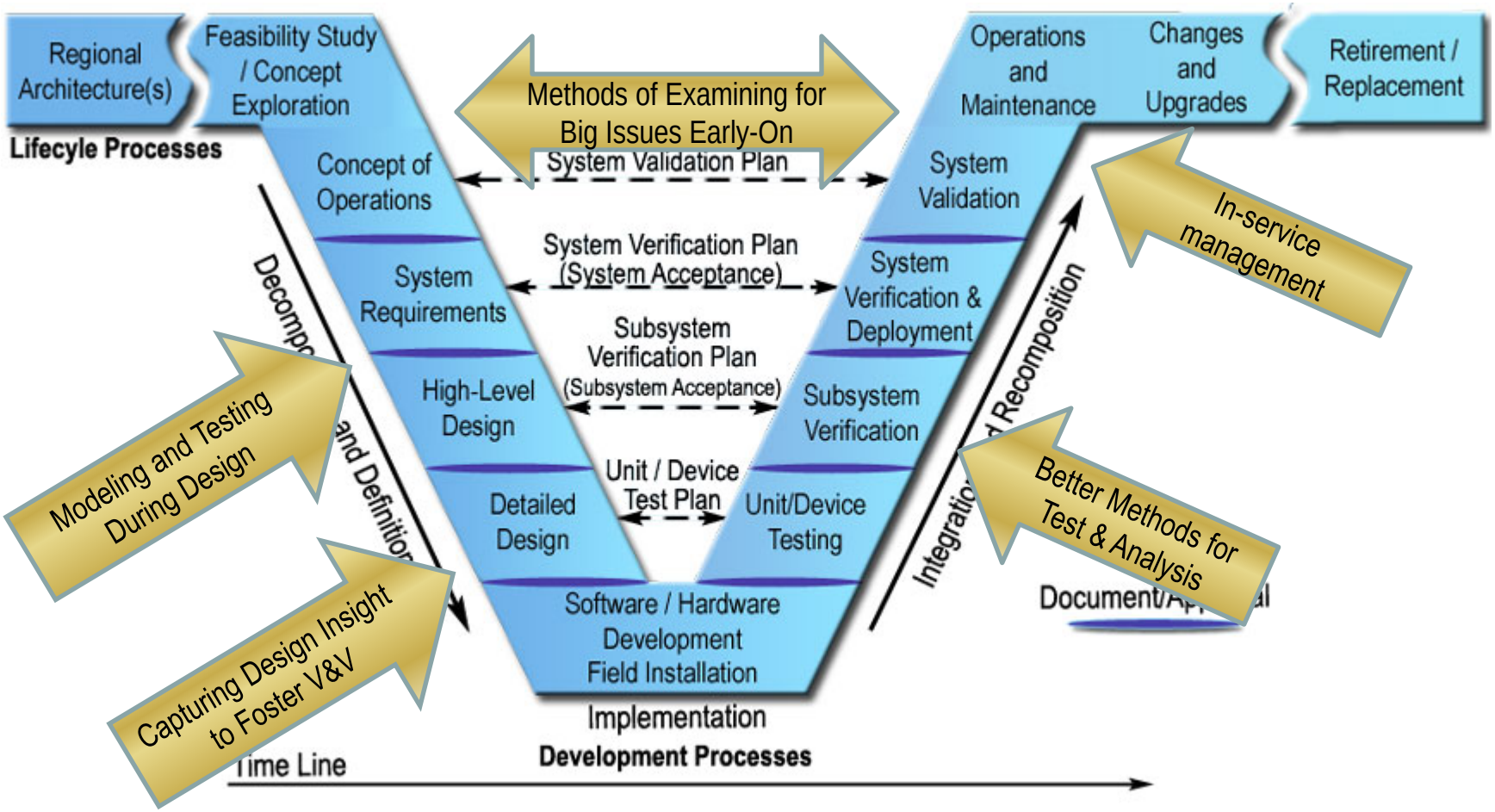
NASA VVFCS Planning Effort to date

- FY10 Planning effort conducted on ARRA funds

  Research plan for transformative, time- and cost-effective , verification and validation tools, methods and techniques that advance safety assurance of complex, networked, distributed flight critical systems operating in the Next Generation Air Transportation System.

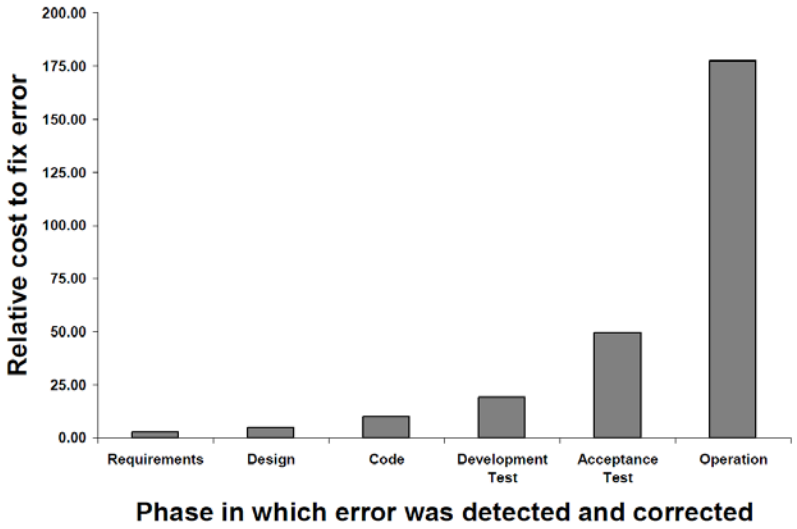
- Objectives
  - Meet the JPDO's needs in V&V research for NextGen transformation
  - Demonstrate advanced methods for relevant issues in the aviation community
  - Reduce barriers to innovation associated with safety V&V
  - Develop V&V methods for safety throughout the entire life cycle

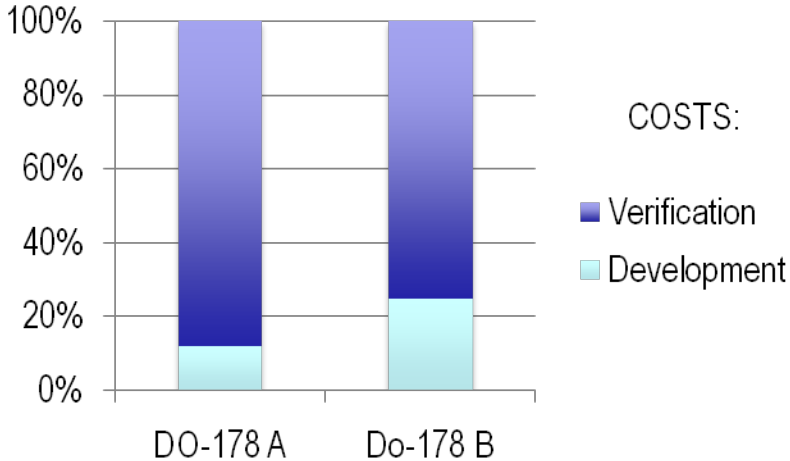
Seeking Lifecycle Model



Impact: Cost, and Constraints on Innovation

System	Lines of Code
Mars Reconnaissance Orbiter	545K
Orion Primary Flight Sys.	1.2M
F-22 Raptor	1.7M
Seawolf Submarine Combat System AN/BSY-2	3.6M
Boeing 777	4M
Boeing 787	6.5M
F-35 Joint Strike Fighter	5.7M
Typical GM car in 2010	100M





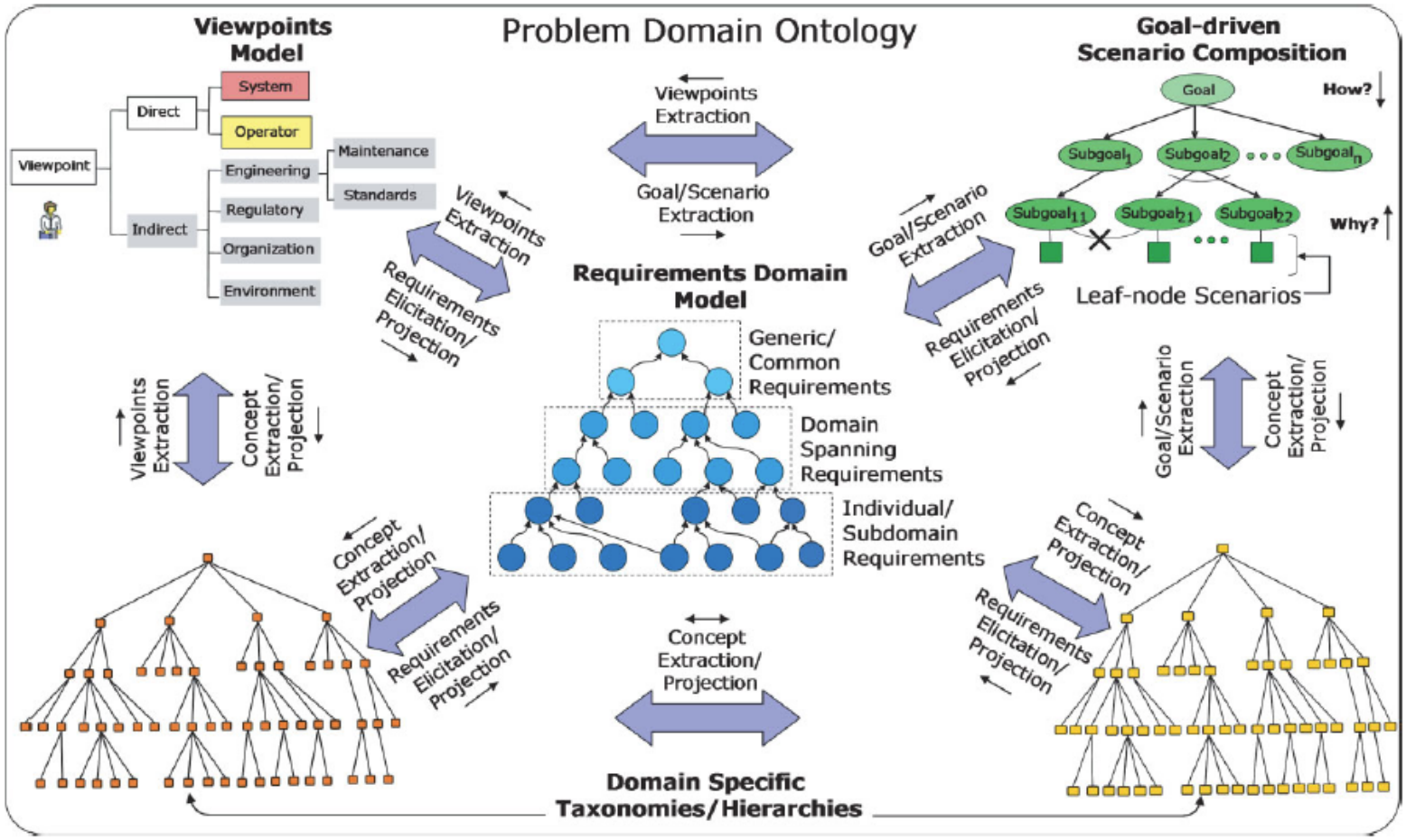
Boehm, B. 1981 *Software Engineering Economics*, as cited in DAA, 2008

Importance of Requirements

- Poor requirements are a primary cause of more than half of all project failures (defined in terms of):
  - Major cost overruns
  - Major schedule overruns
  - Major functionality not delivered
  - Cancelled projects
  - Delivered systems that are never used

From Firesmith “Engineering Safety-Related Requirements for Software Intensive Systems”, SEPG, 2006

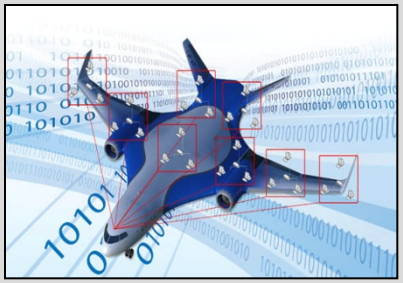
Various dimensions of the Problem Domain



S.-W. Lee, R. A. Gandhi and G.-J. Ahn, Certification Process Artifacts Defined as Measurable Units for Software Assurance, 2007

VVFCS – The way ahead

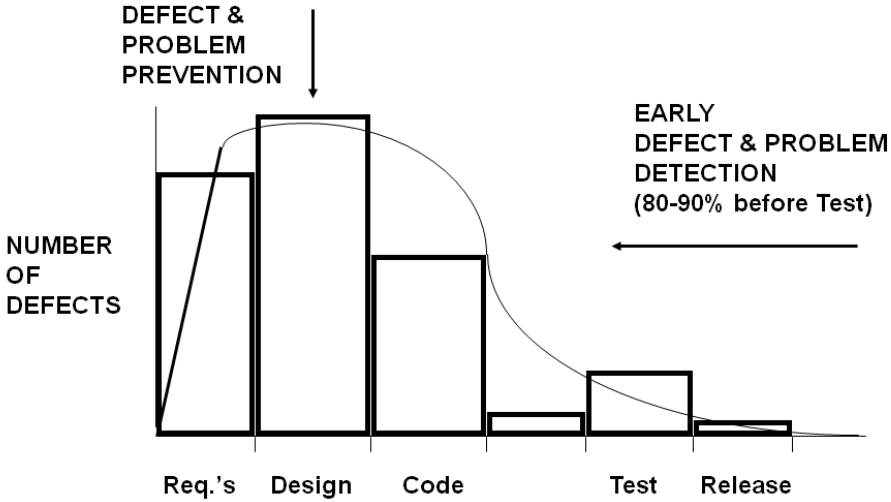
Argument-based Safety Assurance



Software Intensive Systems

Integrated Distributed Systems

Authority and Autonomy



Way ahead

- Products focus on finding faults in requirements-architecture design phase
- Analyze system models early and often (Virtual Integration)
- Evolve components and large scale integrated system

Strategy for V&V of Flight Critical Systems

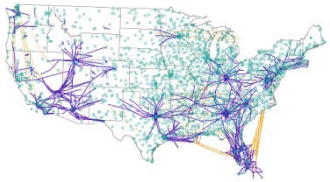
NextGen operational concept | *Common capabilities* | *Technology building blocks*

Mission Analyses

Systems Design

- Net-Centric Operations
- Performance-based services
- Decision-making with weather
- Automation support f/ separation assurance
- Broad-area Precision Navigation
- Trajectory-based Operations
- Super-Density Operations

"Breakthrough Technologies"



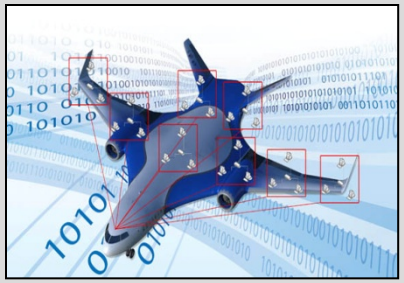
- Validated communications
- Validated architectures
- Compositional V&V
- Formal Methods
- Model-based composition
- Lifecycle V&V Concept Design in V&V Aware Structure

VVFCS Four Research Areas

Argument-based Safety Assurance

Integrated Distributed Systems

Authority and Autonomy



Software Intensive Systems

Verification and Validation for Flight Critical Systems Objectives:

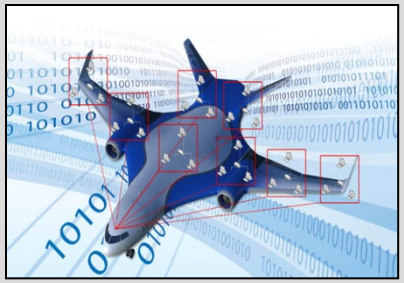
- Develop methods to enable unified safety certification approach joining ground-based systems/procedures with airborne systems/procedures.
- Provide advanced analytical, architectural, and testing capabilities to enable sound assurance of safety-critical properties for distributed systems-of-systems
- Improve the ability to design for safety, and constrain the burdens of dealing with safety in new and more complex systems, i.e., the cost of flight critical software.
- Develop methods that ensure flight-critical systems' assignment of authority and autonomy are comprehensive, lack conflict and ambiguity, and correspond to agents' capabilities and accountability

VVFCS Four Research Areas

Argument-based Safety Assurance

Integrated Distributed Systems

Authority and Autonomy



Software Intensive Systems

Impact of NextGen on Safety Assurance

- A case for safety of a new/modified system is made using standards and guidelines based on experience and community wisdom
- Significant differences exist in *how* the case is made today
  - among organizations responsible for different types of systems
  - using different standards, vocabulary, guidance on acceptability, and degrees of design freedom for automated systems
- These differences and related concerns have implications for safety assessment and assurance for NextGen systems
  - lack of a formal link between the certification or approval of different systems
  - lack of a uniform practice of performing a systems analysis of requirements, including safety
  - insufficient understanding of end-to-end system performance and change impact
  - escalating certification-related costs

[ref. RTCA Task Force 4 Certification, RTCA Certification Task Force, 1999]

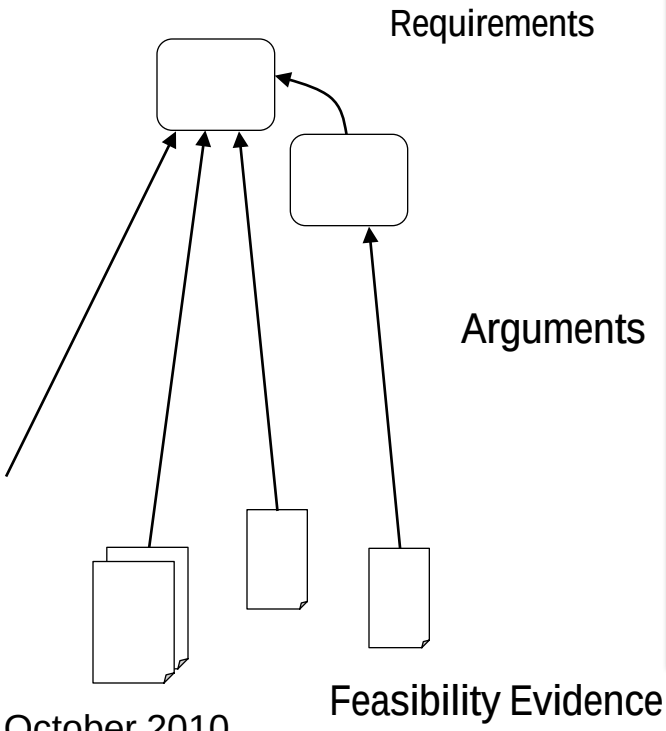
Argument-based Safety Assurance primary objectives

- Consistent and comprehensive safety assessment and assurance methods
  - that cover the system life cycle
  - and work for *all* types of aviation systems and services
- Improved methods, tools, and processes for requirements
  - throughout the system life cycle
  - such that safety requirements can be easily "seen"
  - improving change impact assessment
- Improved methods, tools, and processes for safety-related evidence
  - sources and types of evidence needed to support safety
  - criteria and methods for analyzable arguments about safety

Building a more efficient, effective, and transparent approach for managing and analyzing safety-related data

Argument-based safety assurance

- Systematic, structured, connected approach to documenting the relationship of evidence of safety to the requirements
  - including rationale, assumptions, and context



- Contractual requirements for necessary provisions and resources:
  - Explicit definition of feasibility evidence expected as an output of the engineering work

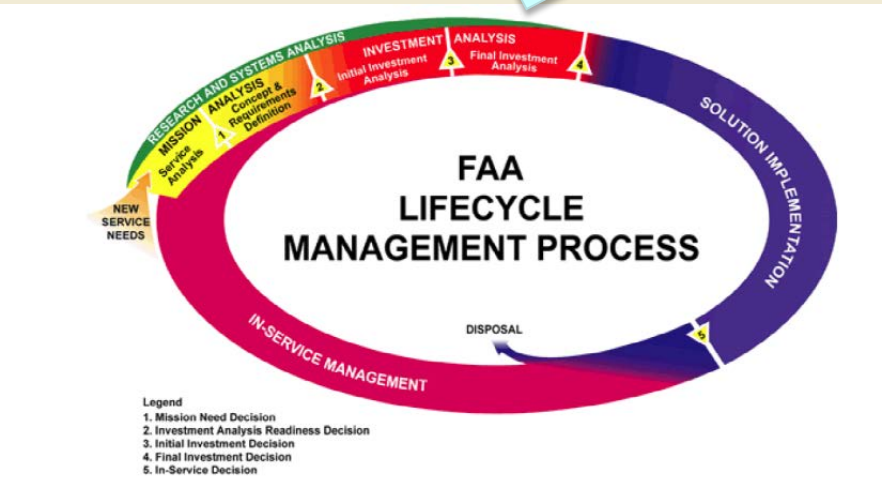


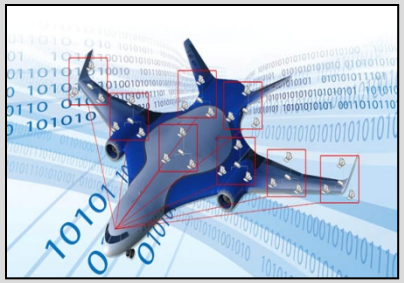
Figure 3.1-1. FAA AMS Lifecycle Management Process

VVFCS Four Research Areas

Argument-based Safety Assurance

Integrated Distributed Systems

Authority and Autonomy



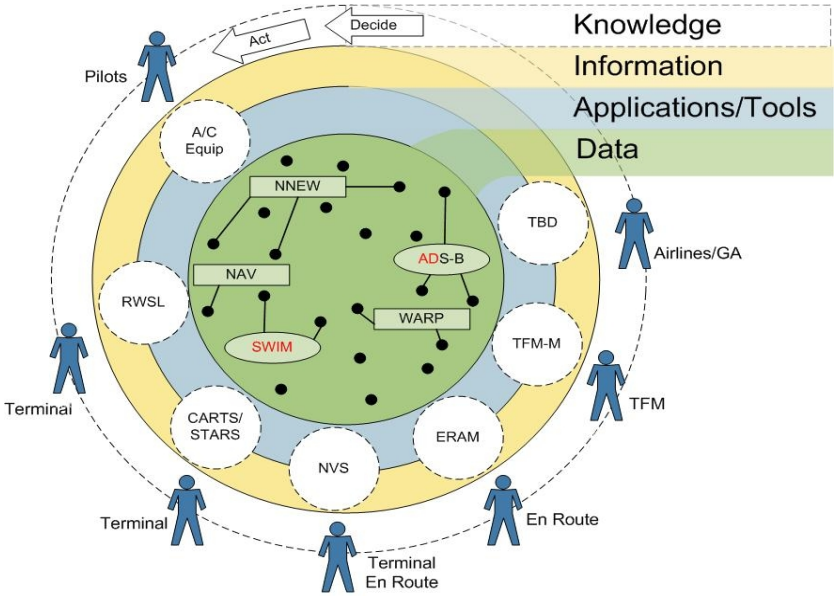
Software Intensive Systems

NextGen as a Complex Systems of Systems

By 2025, all aircraft and airports in U.S. airspace will be connected to the NextGen network and will continually share information in real time to improve efficiency, safety, and absorb the predicted increase in air transportation.

The design of complex distributed systems of systems must pay more attention to fault tolerance to limit how much of the systems behavior is affected by failure.

Conceptual View of Net-Centric NAS: NextGen



Distributed Systems Objective and Approach

Objective: Provide advanced analytical, architectural, and testing capabilities to enable sound assurance of safety-critical properties for distributed systems of systems

Approach:

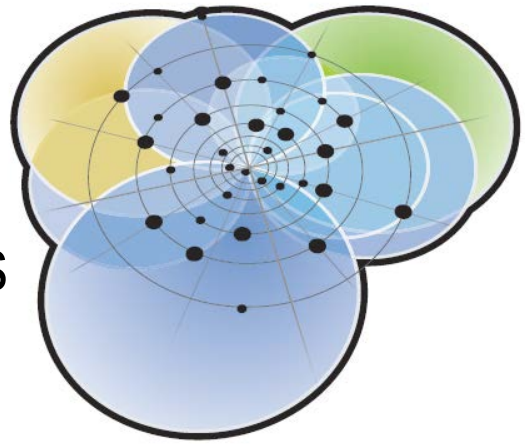
1. Develop validated models of failures, disturbances, & degradations
2. Verify properties of distributed algorithms (e.g. for diagnosis, resource management, aircraft separation, etc.) using various communication topologies and technologies, in presence of disruptions identified in (1)
3. Develop modeling approaches for new system decompositions and functional integration enabled by technological advances
   - Models of coupling and dependencies
   - Non-interference between functions of different criticalities
4. Transition models into practical engineering realizations

Collaboration with: Honeywell

Validation and Verification of Safety-Critical Integrated Distributed Systems, Kevin Driscoll

Models of failures, …

The research will develop validated models of faults, failures, disturbances, and degradation in:



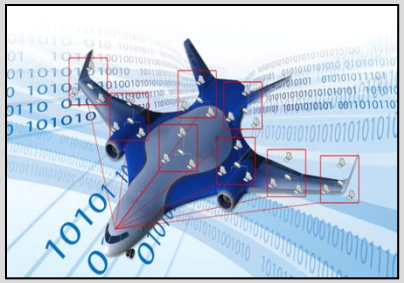
- Large heterogeneous networks
- Mixed synchronous / asynchronous systems
- Multiple time scales
- Integrated functionality sharing distributed resources
- Wireless, wired, human-automation, human-human

VVFCS Four Research Areas

Argument-based Safety Assurance

Integrated Distributed Systems

Authority and Autonomy



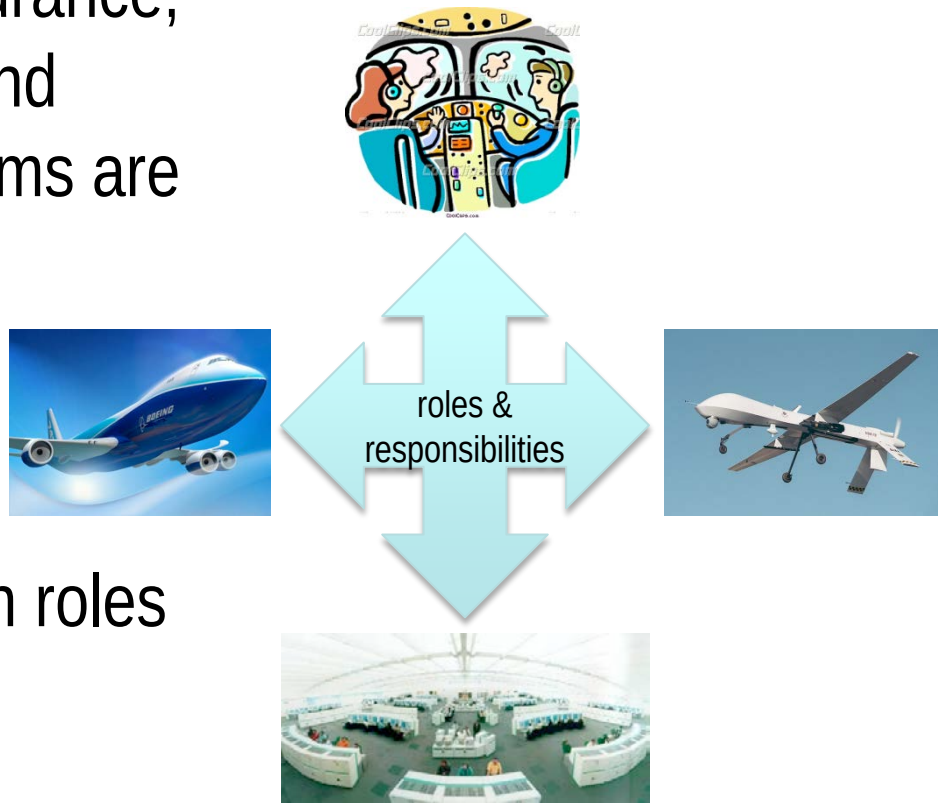
Software Intensive Systems

Allocation of Authority and Autonomy Example: Überlingen Mid-Air Collision

- Bashkirian Airlines Flight 2937 and DHL Flight 611 were level at FL360, under Swiss ATC.
- Both received TCAS advisories that probably would have averted the mid-air collision: Flight 2937 to climb, Flight 611 to descend.
- Due to multiple organizational and technical problems (see notes page), Flight 611 acted on its TCAS advisory, while Flight 2937 acted on ATC direction contrary to its TCAS advisory.
- Unaware of the TCAS advisories, Swiss ATC instructed Flight 2937 to descend from FL360 to FL350 to avoid a conflict with Flight 611.
- A second descent instruction was given by the Swiss controller seconds later, and the Flight 2937 crew acknowledged the instruction.
- Flight 2937 initiated its descent about 25 sec. before the collision.
- The two aircraft collided at FL354 and crashed. There were no survivors.
- Eight managers and employees of the Swiss ATC contractor were prosecuted; four were convicted.

Authority and Autonomy: Primary Objective

- Develop tools that provide assurance, early in design, that authority and autonomy of flight-critical systems are
  - clear,
  - deadlock- and conflict-free,
  - comprehensive, and,
  - consistent with agreed-upon roles and responsibilities.



Collaboration with:

UNIVERSITY of VIRGINIA

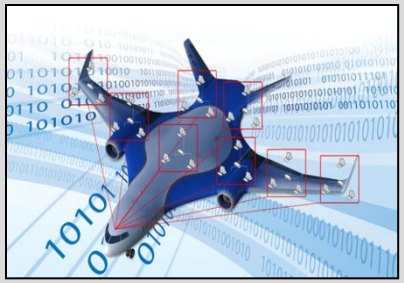
SRI International

VVFCS Four Research Areas

Argument-based Safety Assurance

Integrated Distributed Systems

Authority and Autonomy



Software Intensive Systems

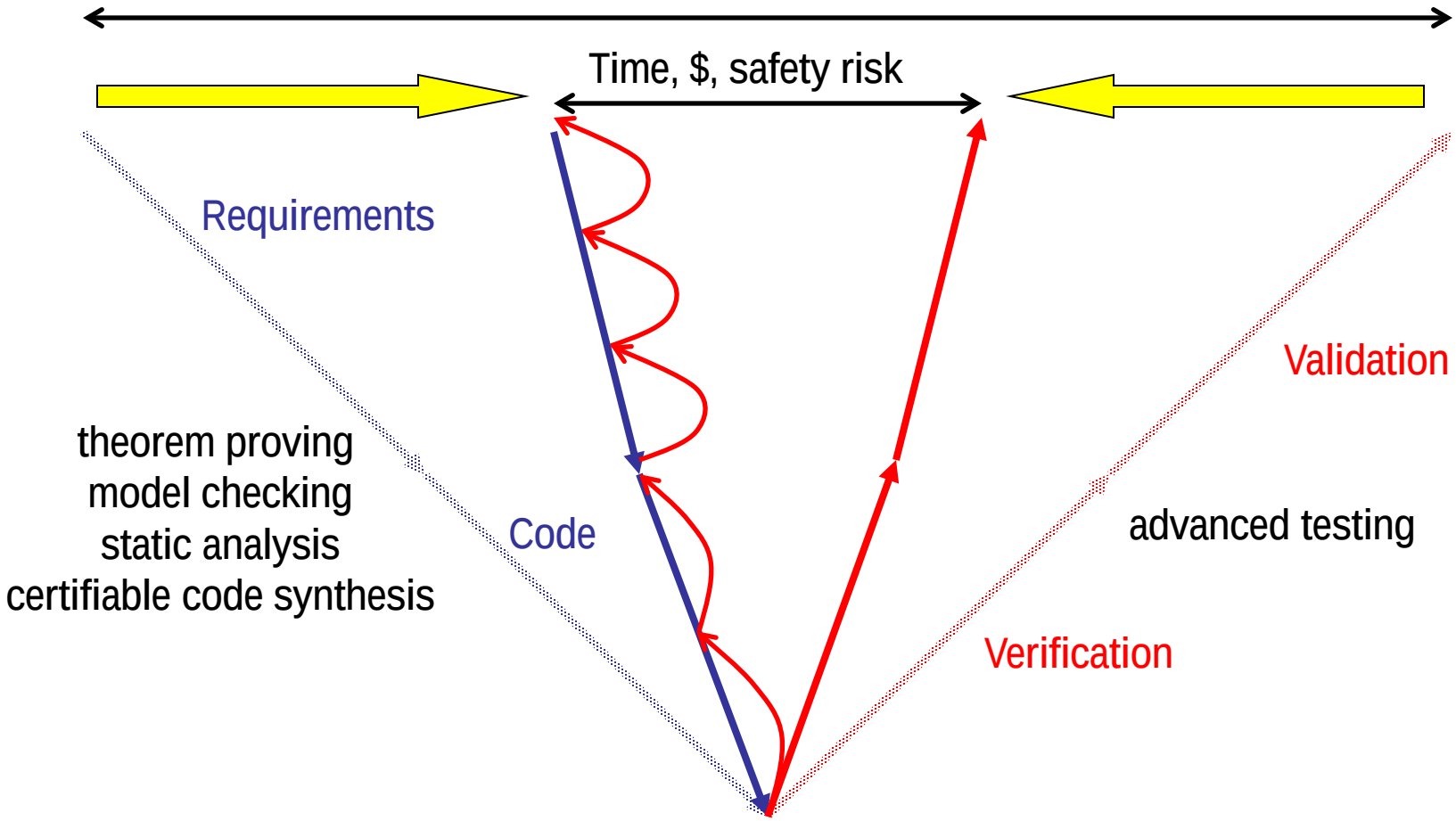
Software Intensive Systems primary objectives

- Widespread use of formal methods
- Compositional verification,
- Design for verification and early application of V&V in the life-cycle
- Combination of testing with formal methods and learning techniques
- Certifiable code generation
- Development of foundational libraries
- Support for safety cases

New V&V techniques that can significantly reduce cost and increase software assurance and dependability.

- Collaboration with: Carnegie Mellon, Honeywell, SRI International

S/W Lifecycle Perspective



Summary

- Four focal research areas
- Partnerships and collaboration with industry, FAA, JPDO, military and academia for coordinated and integrated research & development activities are essential
- Technology transfer at all levels
- Maintain relevancy by on-going communication with key players in community

Thank You!

Questions?

Sharon.S.Graves@nasa.gov

- BACKUP

V&V Products List

- Criteria/standards of certification/ methods of compliance
- Web based activities to bring V&V activities to table
- Run-time verification
  - Non-linear arithmethic; analyzing numerical instabilities
- Math models for survivability or resilience
  - Systems need to keep running when faced with hazards (stochastic or accidental, non-stochastic)
- Trusted platform models; fault tolerance measures
- Manned & unmanned vehicles interoperability
- Rapid prototyping
- Formal Methods
  - Finite-state formal methods, infinite state formal methods
- Control design and validation
- Design Guides, simulations, requirements (Dependability/Safety cases, central models, autocode generation, model-based V&V, V&V aware systems – test points that are embedded into model)
- System level automated V&V environment
- Architecture definition, Control system integration,
- Provide generic IMA test bench

NRA Details

Organization	PI	Sub-org	Title	Description
MIT	Leveson, Nancy	Honeywell	Assuring Safety using System Theoretic Concepts	The research proposes an innovative systems and controls theory approach to hazard analysis and safety with a demo, eval. and comparison to traditional approaches. Application: flight control systems including NextGen and IMA. Designs safety into early design and describes the effort here as a re-engineering problem for NextGen; problem is seen where changes are proposed and analysis must be used to ensure changes will not degrade current level of safety.
SGT, INC.	Denney, Ewen	none	Automating the Generation of Heterogeneous Aviation Safety Cases	Development of a tool which supports the automated creation of evidence-based arguments. Extend and adapt the AutoCert code verification tool to demonstrate the use of formal verification for the automated construction of safety cases. inherently recognizes assurance and cert. as human activities. Since humans design, build, verify and certify software, analysis tools need to support their activities by explaining reasoning in a comprehensible and usable way. The proposal plan is to extend and adapt the AutoCert code verification tool to demonstrate the use of formal verification for the automated construction of safety cases.
KESTREL TECHNOLOGY LLC	Barry, Matthew	none	A Safety Case Workbench	Extend and adapt the AutoCert code verification tool to demonstrate the use of formal verification for the automated construction of safety cases. Phase 1 consists of development of a safety case work bench that will support argument-claim-evidence approach. In Phase 2 put work bench to use in preparing 3 safety cases.
RECTOR & VISITORS OF THE UNIVERSITY OF VIRGINIA	Bass, Ellen	U of Ill, Urbanna Georgia Tech Rsrch Corp	NextGenAA: Integrated model checking and simulation of NextGen authority and autonomy	Create an integrated suite of simulation, formal verification, and trace analysis tools that use an agent modeling language description for examining A&A safety issues. Create openly available and re-usable models and verification approaches applicable to assessing A&A safety issues beyond scenarios tested.
HONEYWELL INTERNATIONAL INC	Driscoll, Kevin	SRI International WW Technology	Validation and Verification of Safety-Critical Integrated Distributed Systems	Proposed work will bridge gap betw/ theory and practice of fault-tolerant DS – puts analysis tools in hands of engrs and delivering reusable, validated models of fault-tolerant frameworks such as TTEthernet. Will demo new modeling approaches and verification techniques. Research proposes creating models, methods, tool extensions and an integration infrastructure that design engineers can easily use for V&V of safety-critical integrated distributed systems.
CARNEGIE MELLON UNIVERSITY	Giannakopoulou, Dimitra	SGT	Compositional Verification for Flight Critical Systems	Compositional verification technology with component verification
SRI INTERNATIONAL	Shankar, Natarajan	Honeywell	An Evidential Tool Bus for Flight Critical Software Systems	Research proposes robust model-based assurance of fcs centered around SRIs evidential toolbus (ETB) and PVS specification/verification framework. Builds on Honeywells suite of MATLAB based tools for capturing and analyzing rqmts, models and designs; Approach is validated thru case studies covering flight control and management as well as air-traffic control. Their goal is to bring about an order-of-magnitude improvement in the efficiency and effectiveness of software certification through the integration and distribution of robust formal verification/validation tools. Development of a suite of modeling and analysis tools that manage the task of designing, building, validating, verifying and certifying software-intensive systems.

Formal Methods

- Designs
  - Prototyping
  - Functional verification
- Formal Methods
  - * Theorem proving
    * Model checking
    * Real-time, hybrid, stochastic systems
    * SAT and SMT solvers
    * Symbolic execution
    * Abstraction
    * Compositional verification
    * Program refinement
    * Static analysis
    * Dynamic analysis
    * Automated testing
    * Model-based testing
    * Model-based development
    * Fault protection
    * Security and intrusion detection
    * Application experiences
    * Modeling and specification formalisms
    * Requirements specification and analysis

VVFCS Definitions

- *Validation*: Confirmation that proposed system requirements, and/ or operational systems, meet the expectations of the customer and other stakeholders, accomplishing the intended purpose in the intended environment(s), throughout the system's life cycle
- *Verification*: Confirmation that proposed or operational systems comply with requirements throughout the system's life cycle
- *System*: The hardware, software, people, facilities, and procedures organized to accomplish common objectives
- *Flight-critical System*: Any system required to ensure the safe conduct of an aircraft flight. This definition incorporates the definition for system, given above; includes air, ground, and space systems; and recognizes that human performance is central to flight-critical system performance.
- *Life cycle*: The series of stages spanning system conceptualization, development, implementation, and retirement