



VERIFICATION AND VALIDATION OF COMPLEX AND AUTONOMOUS SYSTEMS

11TH ANNUAL V&V SUMMIT
14-15 SEPTEMBER, 2016

KERIANNE GROSS

RESEARCH AEROSPACE ENGINEER

VERIFICATION AND VALIDATION OF COMPLEX AND AUTONOMOUS SYSTEMS TEAM

AEROSPACE SYSTEMS DIRECTORATE

AIR FORCE RESEARCH LABORATORY



How do you prove an autonomous system
will do what you want it to do?



How do you prove an autonomous system
will not do what you don't want it to do?

Verification

Did we build the system right?
(Does it meet specifications?)

Validation

Did we build the right system?
(Does it meet customer's need?)

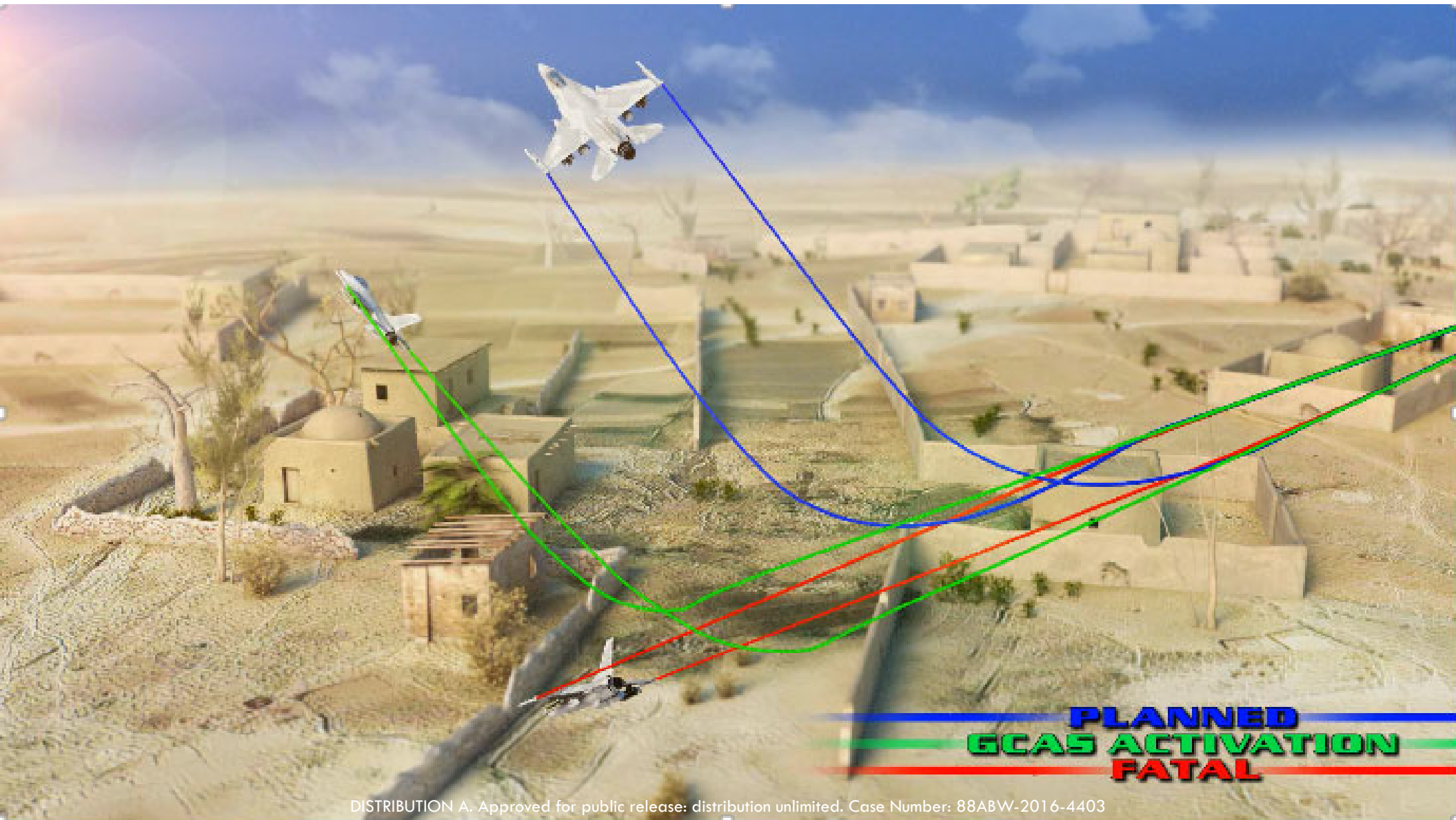
Automation

limited operator involvement
limited to specific actions
well-defined tasks
predetermined responses

Autonomy

intelligence-based
responds in unanticipated situations
not pre-programmed
self-government
self-directed behavior
human's proxy for decisions

From AFRL Autonomy S&T Strategy



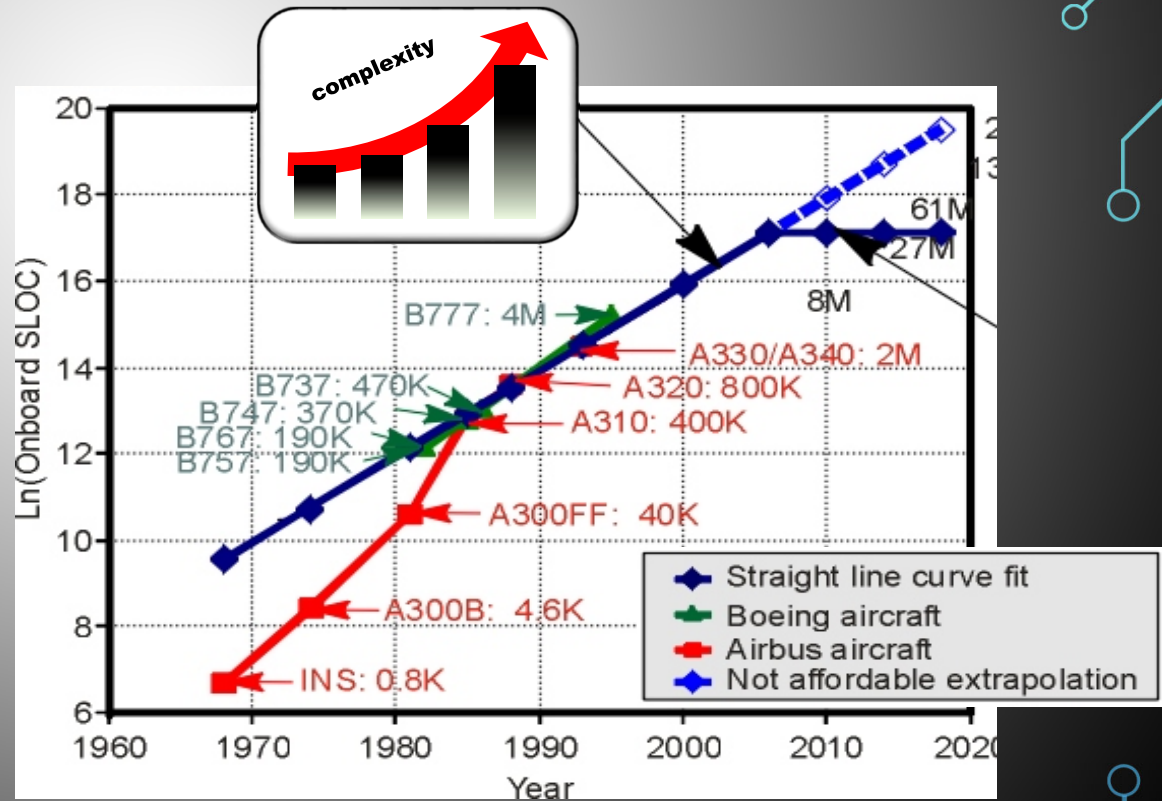
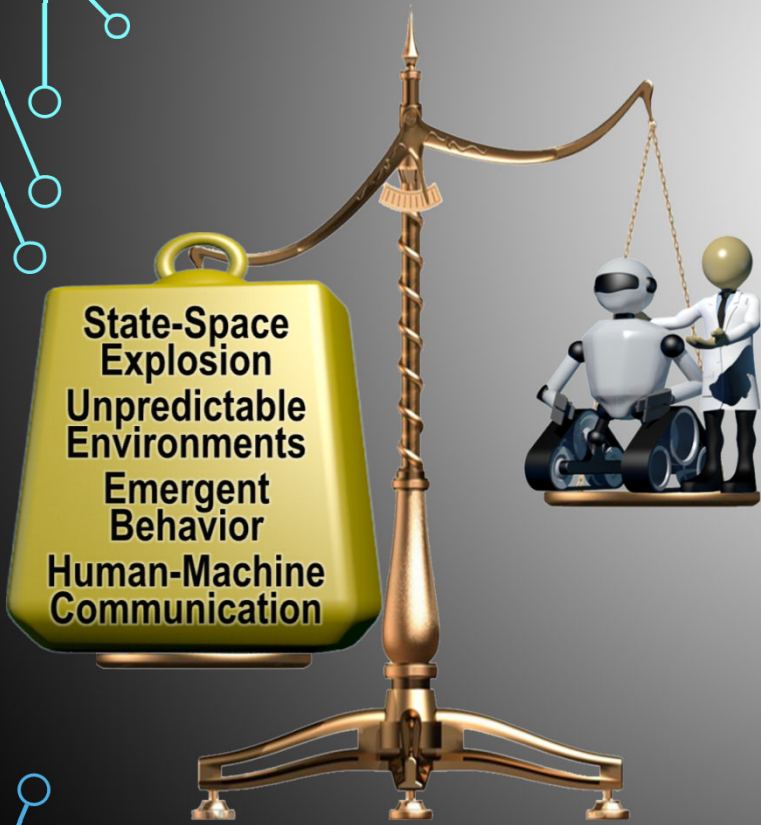
**PLANNED
GCAS ACTIVATION
FATAL**

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number: 88ABW-2016-4403



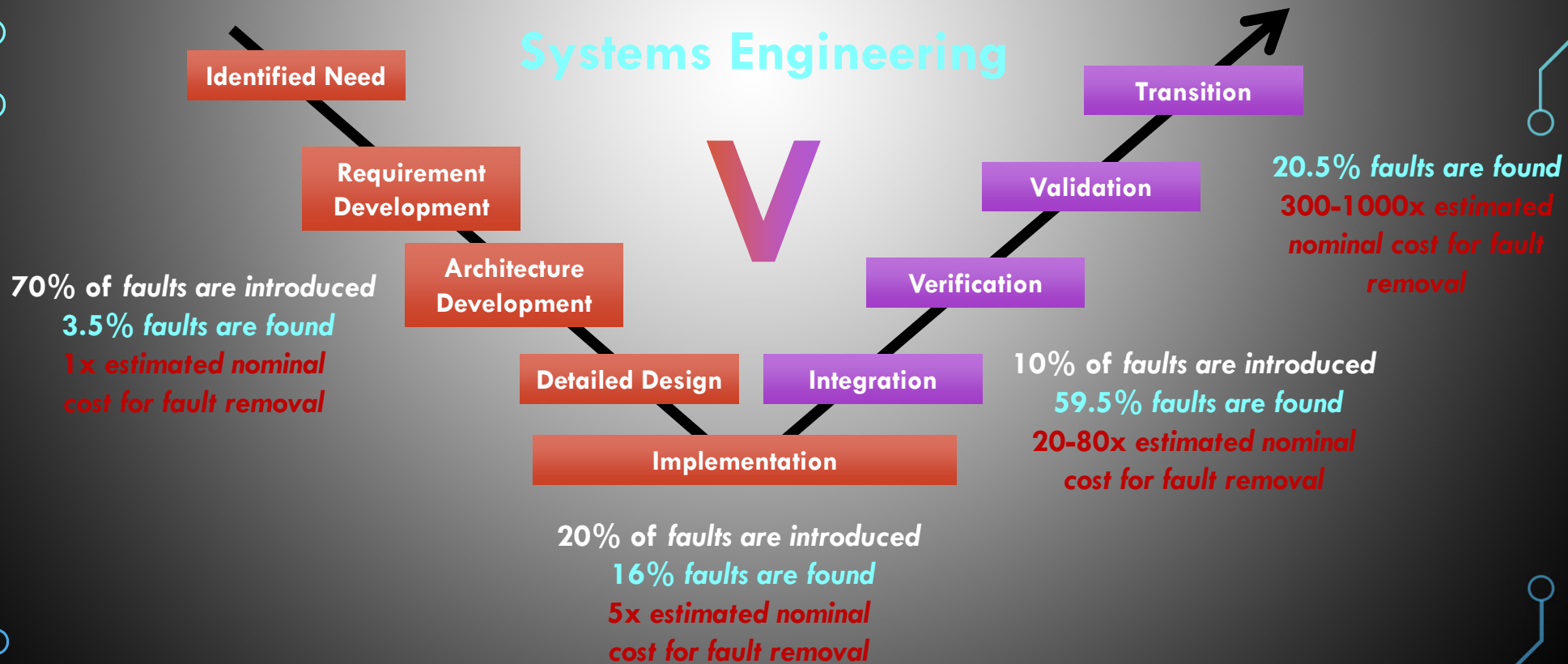
“In a recent survey of airline pilots, those operating **Boeing 777s** reported that they spent just **seven minutes manually piloting** their planes in a typical flight. Pilots operating **Airbus** planes **spent half that time.**”

<http://www.nytimes.com/2015/04/07/science/planes-without-pilots.html? r=0>



Highly complex systems and increasing autonomous systems face many of the same Verification and Validation challenges

Systems Engineering



From:

NIST Planning report 02-3, *The Economic Impacts of Inadequate Infrastructure for Software Testing*, May 2002.

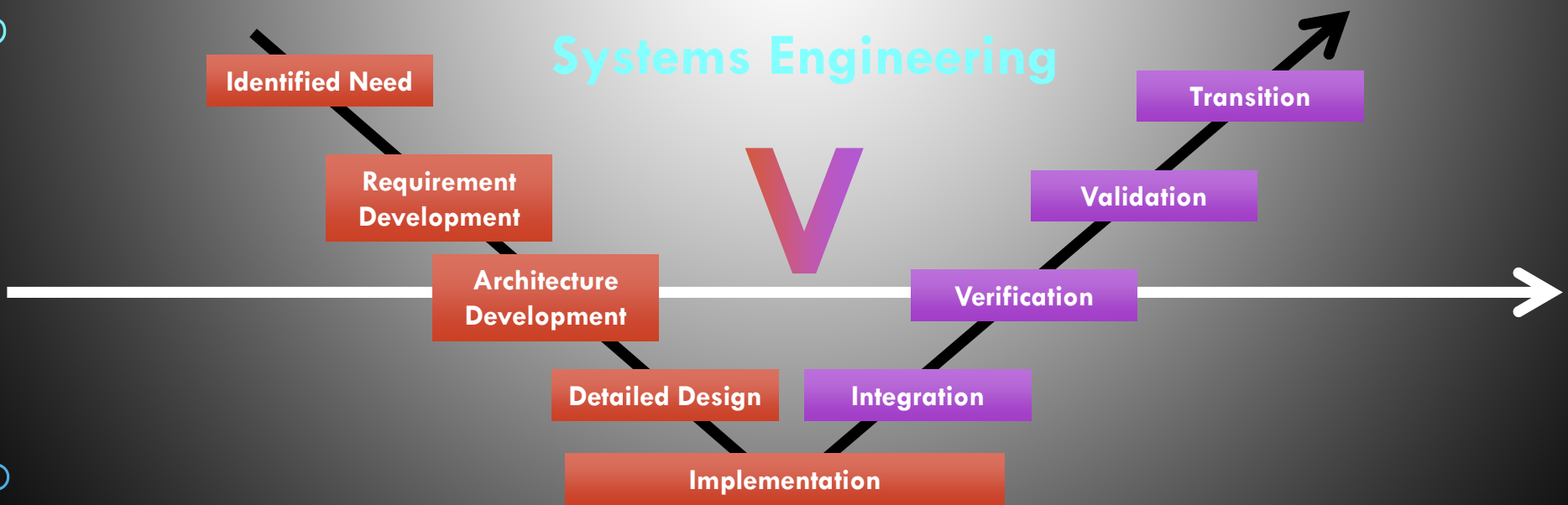
D. Galin, *Software Quality Assurance: From Theory to Implementation*, Pearson/Addison-Wesley (2004)

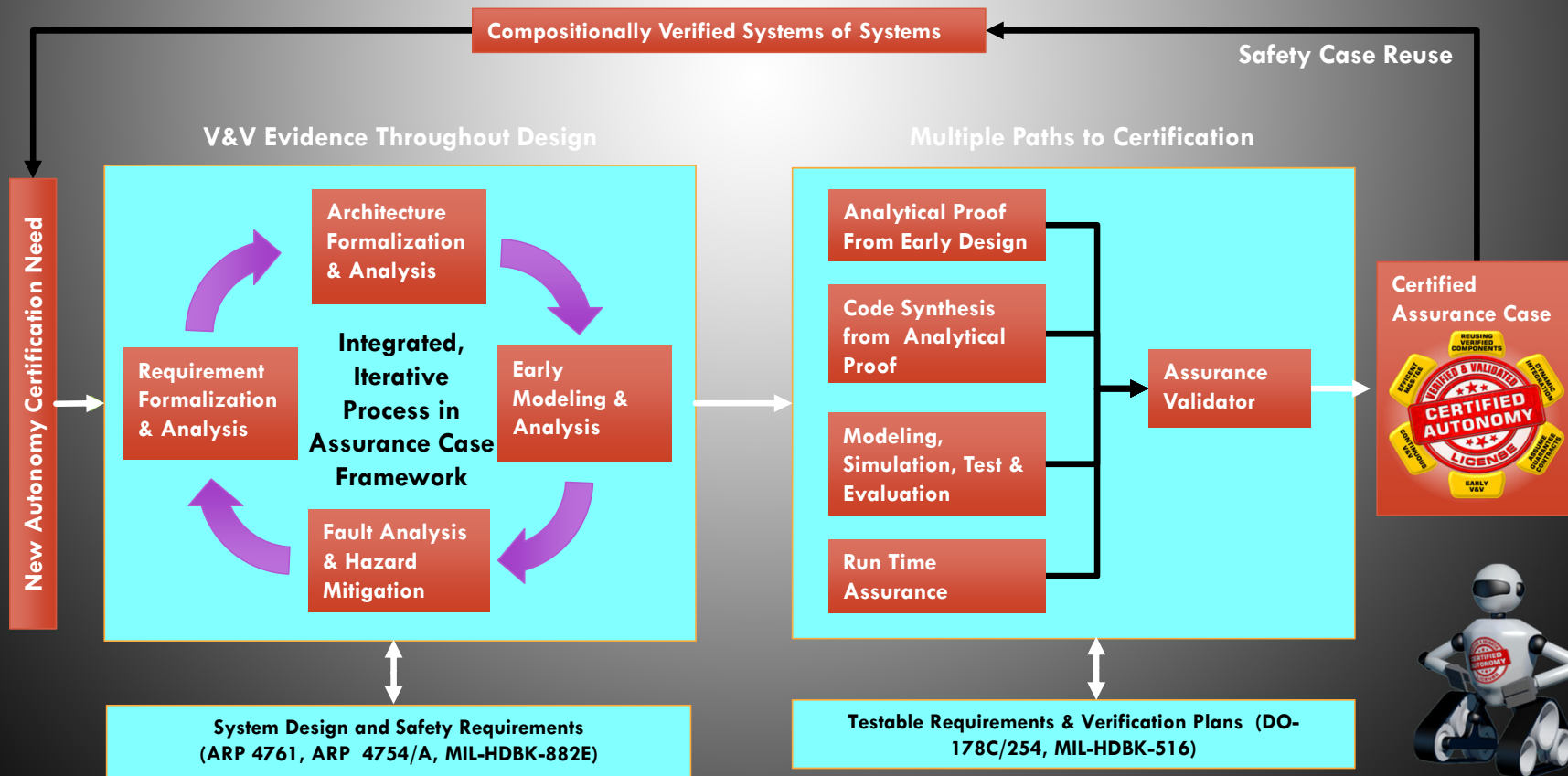
B.W. Boehm, *Software Engineering Economics*, Prentice Hall (1981)

P. H. Feiler, "Supporting the ARP4761 Safety Assessment Process with AADL," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 6 February 2014. Accessed 5/27/15 from: <https://wiki.sei.cmu.edu/aadl/images/1/13/ERTSEMV2-Feb2014.pdf>

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number: 88ABW-2016-4403

Systems Engineering





V&V Evidence Throughout Design

Specification and Analysis of Requirements (SpeAR) Tool:
(AFRL/ Rockwell Collins Product)
Formally Specify Requirements
Automatically Detect Conflicts
Highlight Requirements Gaps

Assume Guarantee Reasoning Environment (AGREE):
(University of Minnesota / Rockwell Collins)
Formally Specify Assumptions
Requirements as Guarantees
Formal Analysis of AADL Architecture
Proof or Counterexample that Architecture meets requirements

Requirement Formalization & Analysis

Architecture Formalization & Analysis

Early Modeling & Analysis

Integrated, Iterative Process in Assurance Case Framework

Fault Analysis & Hazard Mitigation

Formal Methods Based Model Analysis tools
Example: Simulink Design Verifier
Automatically detect possible requirements violations or common coding errors such as divide by zeros in your model

Fault / Hazard Analysis Techniques
Fault Trees
Failure Modes and Effects Analysis
System-Theoretic Process Analysis
Etc.

System Design and Safety Requirements
(ARP 4761, ARP 4754/A, MIL-HDBK-882E)

Multiple Paths to Certification

Evidence from Early Analysis Phases

Requirements
Architecture
Models
Fault/Hazards

Analytical Proof
From Early Design

Code Synthesis
from Analytical
Proof

Modeling,
Simulation, Test &
Evaluation

Run Time Assurance

Correct by Construction Design

Automatically construct logically correct,
verifiable designs
“Play Calling”

Certifier

Inspect evidence

Assurance
Validator

Traditional V&V Efforts

Hardware in the Loop Simulation
Pilot in the Loop Simulation
Environmental Testing
Flight Test

Active monitoring, bounding and online verification based on
the Simplex Architecture

Run Time Assured Controller

Unverified
Controller

Actuator
Command

Verified
Controller

Actuator
Command

Decision
Module

Actuator
Command

State

Testable Requirements &
178C/254, M

Compositionally Verified
Systems of Systems

Safety Case Reuse

Some of the Largest Challenges
Integrating heterogeneous evidence
Appropriate reuse of evidence
Integrating systems of systems

Certified
Assurance
Case



A decorative graphic of a circuit board with various lines and nodes, rendered in a light blue color, is positioned on the left side of the slide. It features several vertical lines of varying heights, some with small circles at their ends, and some horizontal lines connecting them, creating a stylized representation of a printed circuit board (PCB).

QUESTIONS?

Kerianne Gross

Kerianne.Gross@us.af.mil

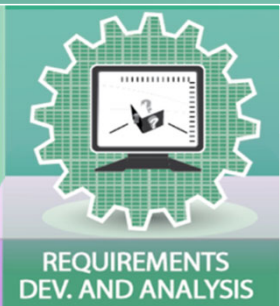
937.713.7025

The slide features a dark gray background with a subtle gradient. In the four corners, there are decorative elements consisting of light blue lines that resemble circuit traces or fiber optic paths, ending in small circles. These elements are positioned in the top-left, top-right, bottom-left, and bottom-right corners.

BACKUP SLIDES

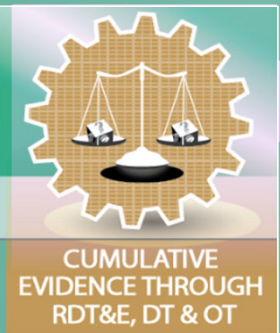
Verification and Validation Research Strategy

DOD AUTONOMY V&V RESEARCH AREAS



Methods & Tools for Requirements Development and Analysis

- *Precise, structured standards to automate requirement evaluation for testability, traceability, and de-confliction*



Cumulative Evidence through RDT&E, DT & OT

- *Progressive sequential modeling, simulation, test and evaluation*

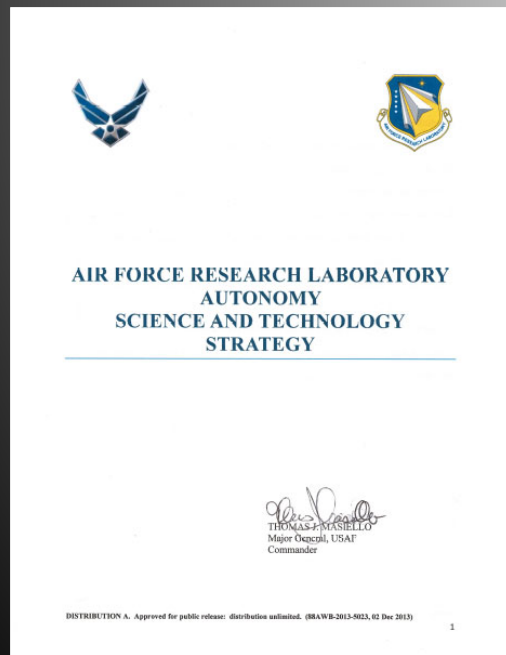


Assurance Arguments for Autonomous Systems

- *Reusable Assurance Case based on previously evidence building blocks*



AFRL AUTONOMY S&T STRATEGY



Goal #1: Deliver flexible autonomy systems with highly effective human-machine teaming

Goal #2: Create actively coordinated teams of multiple machines to achieve mission goals

Goal #3: Ensure operations in complex, contested environments

Goal #4: Ensure safe and effective systems in unanticipated and dynamic environments

Verification and Validation of Complex and Autonomous Systems Team in AFRL/RQQA is leading work under to address Goal #4