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?)

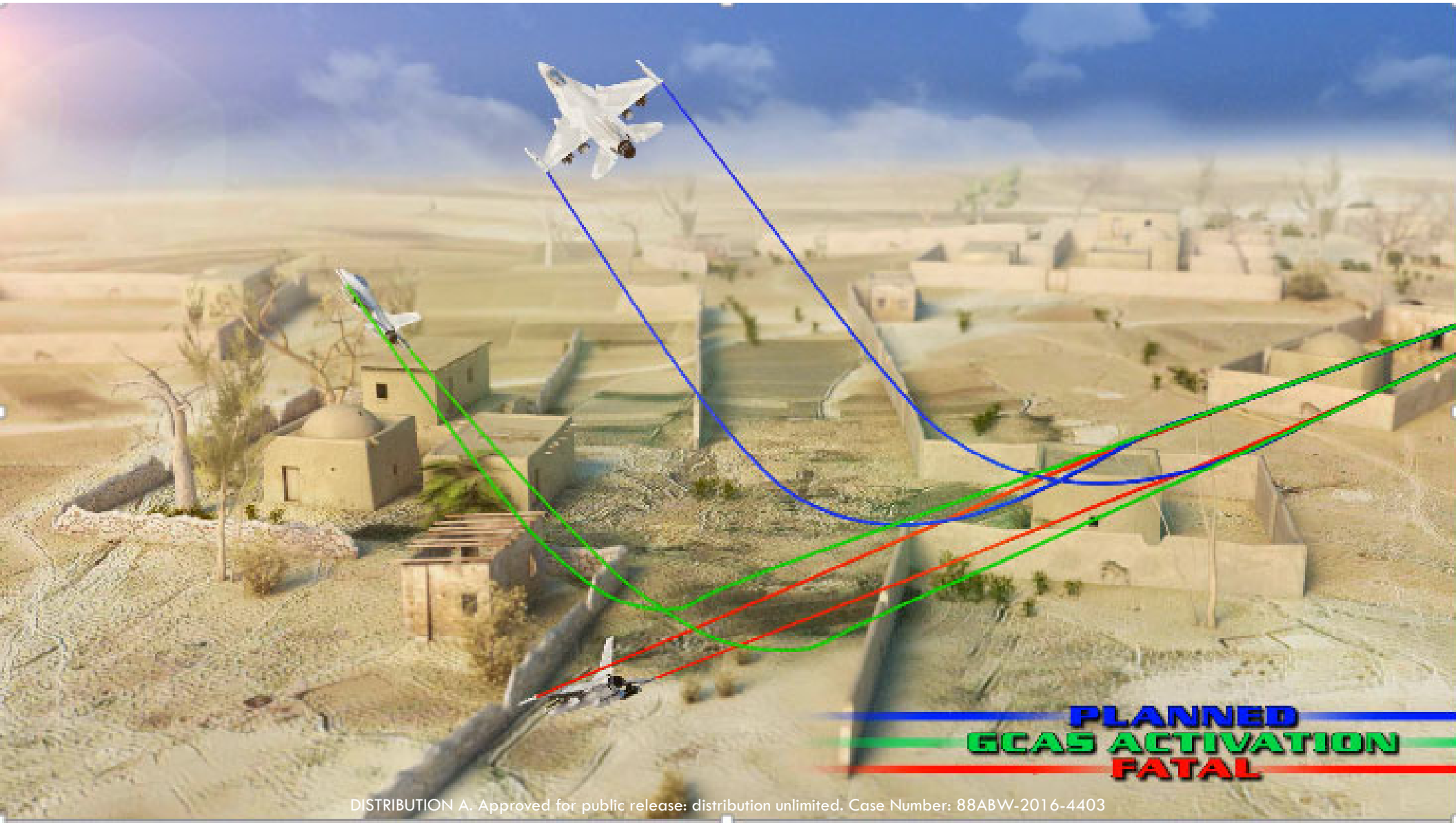
Validation

Did we build the right system?

(Does it meet customer's need?)

Automation	Autonomy
limited operator involvement	intelligence-based
limited to specific actions	responds in unanticipated situations
well-defined tasks	not pre-programmed
predetermined responses	self-government
	self-directed behavior
	human's proxy for decisions

From AFRL Autonomy S&T Strategy



The New York Times

SCIENCE

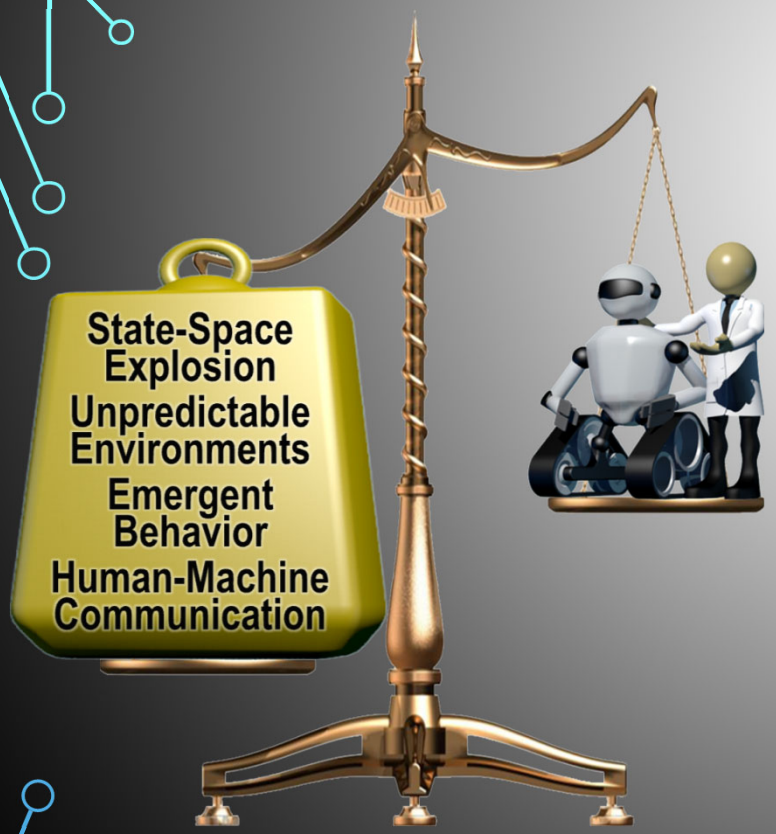
Planes Without Pilots

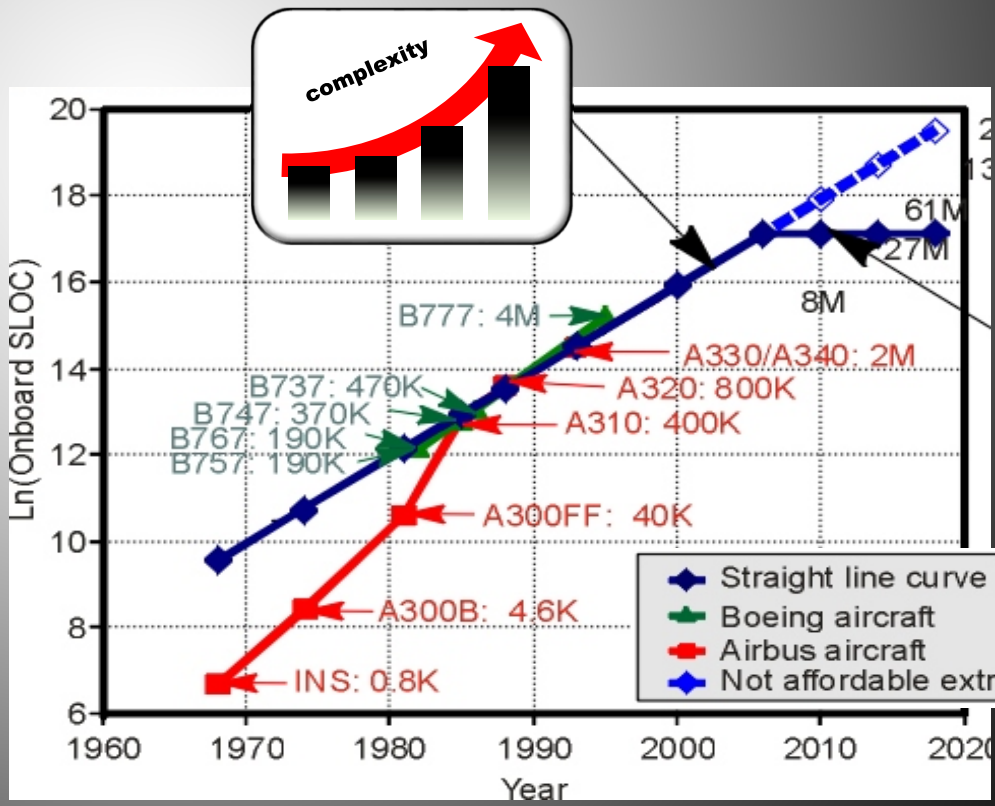
By JOHN MARKOFF APRIL 6, 2015

Harry Campbell

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

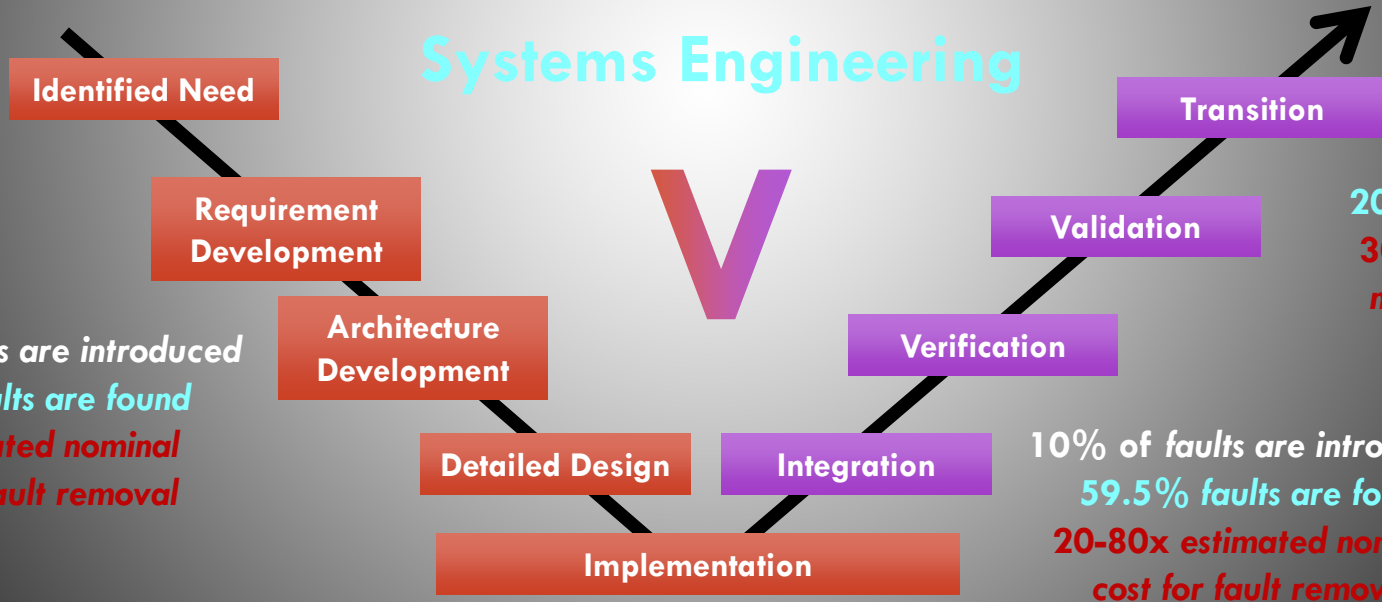
http://www.nytimes.com/2015/04/07/science/planes-without-pilots.html?_r=0





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

Systems Engineering



70% of *faults are introduced*
3.5% *faults are found*
1x *estimated nominal cost for fault removal*

20% of *faults are introduced*
16% *faults are found*
5x *estimated nominal cost for fault removal*

10% of *faults are introduced*
59.5% *faults are found*
20-80x *estimated nominal cost for fault removal*

20.5% *faults are found*
300-1000x *estimated nominal cost for fault removal*

From:

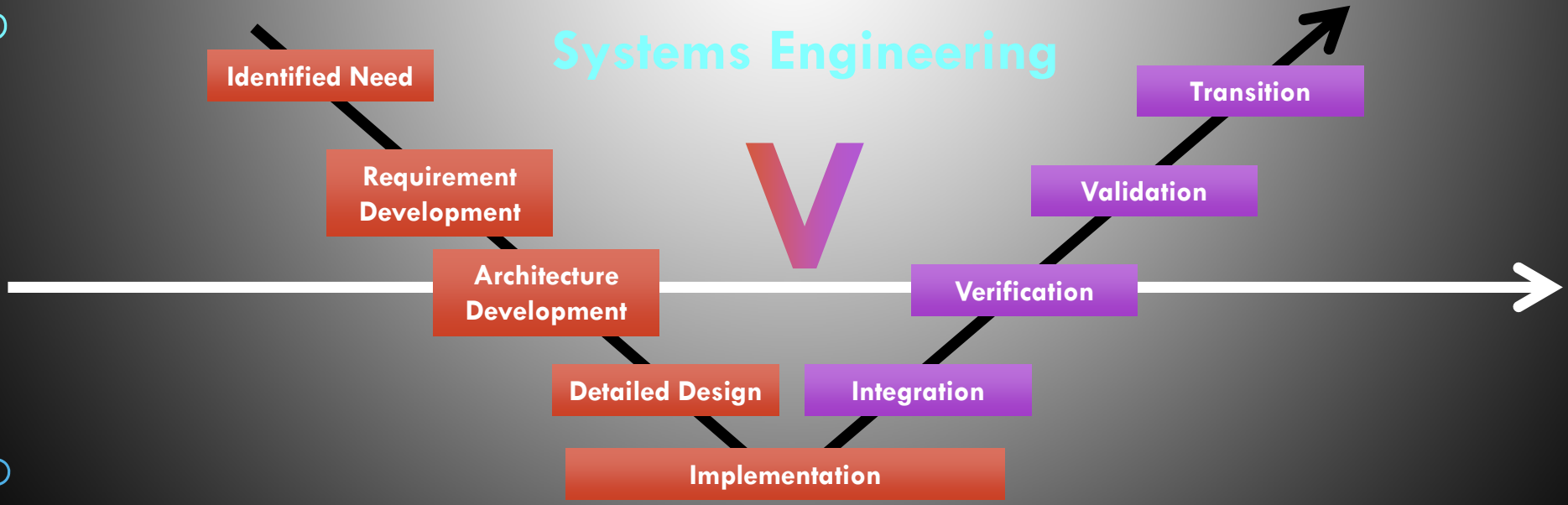
NIST Planning report 02-3, *The Economic Impacts of Inadequate Infrastructure for Software Testing*, May 2002.

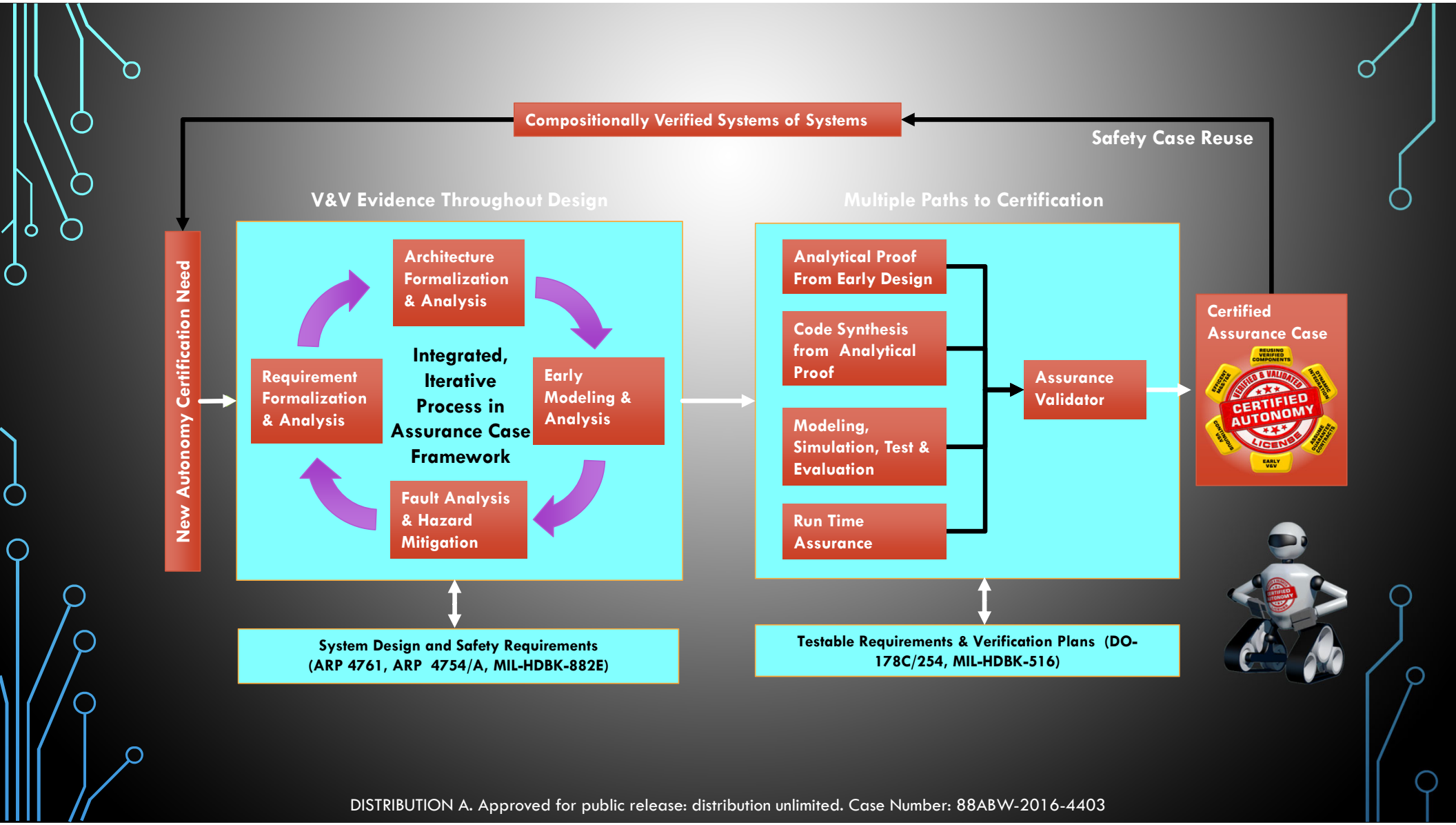
D. Galin, *Software Quality Assurance: From Theory to Implementation*, Pearson/Addison-Wesley (2004)

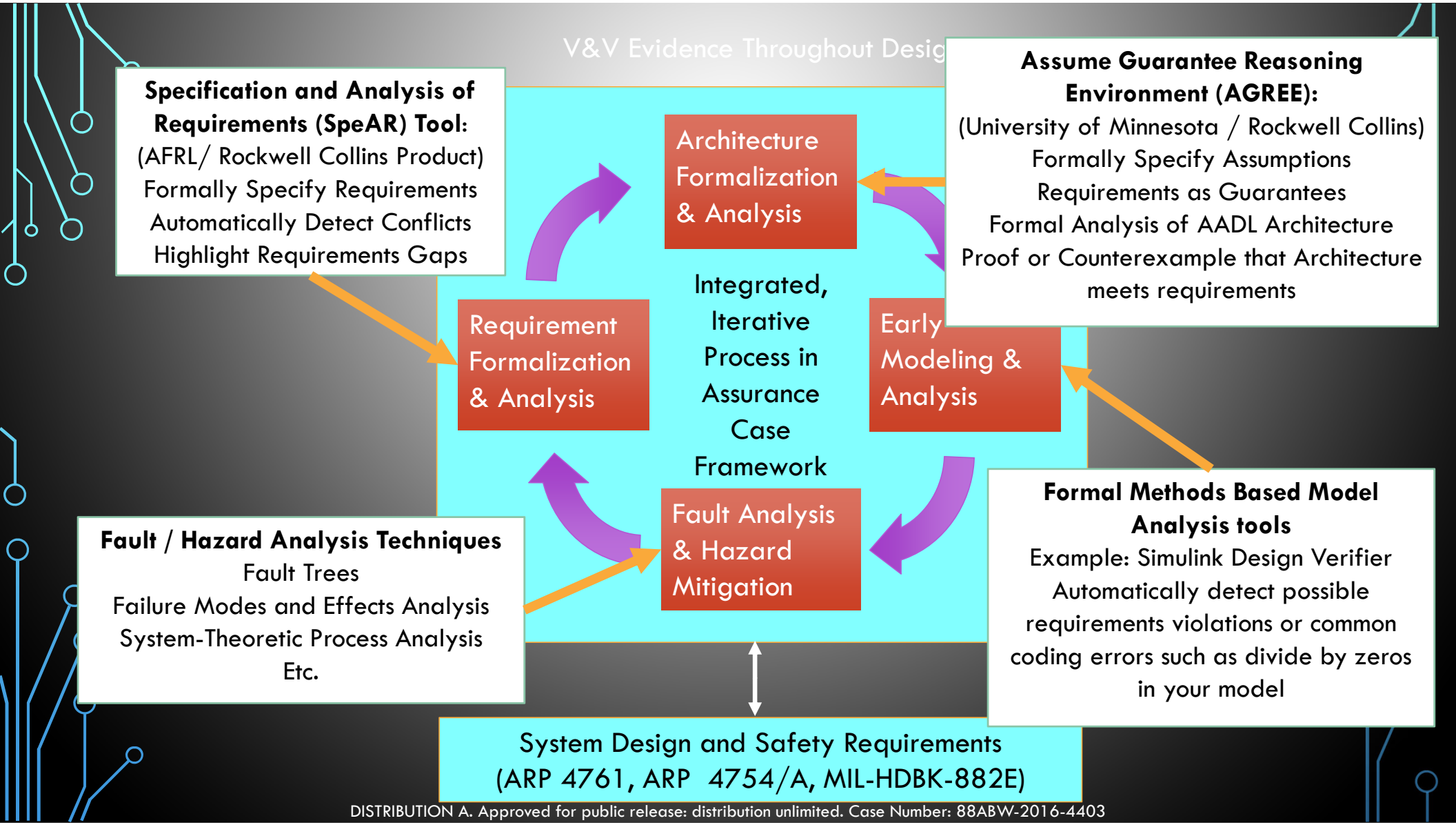
B.W. Boehm, *Software Engineering Economics*, Prentice Hall (1981)

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

Systems Engineering







Multiple Paths to Certification

Evidence from Early Analysis Phases
Requirements
Architecture
Models
Fault/Hazards

Correct by Construction Design
Automatically construct logically correct, verifiable designs
"Play Calling"

Analytical Proof From Early Design

Code Synthesis from Analytical Proof

Assurance Validator

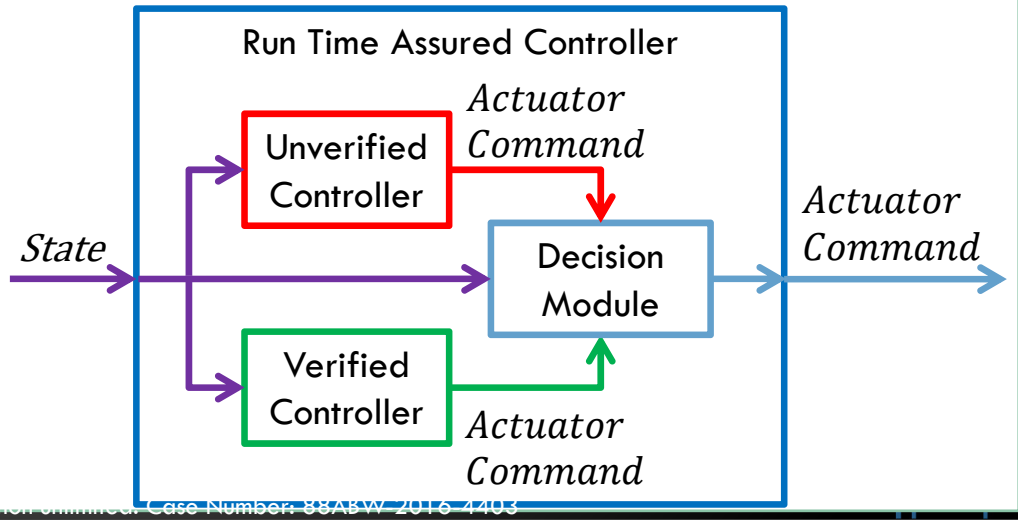
Certifier
Inspect evidence

Traditional V&V Efforts
Hardware in the Loop Simulation
Pilot in the Loop Simulation
Environmental Testing
Flight Test

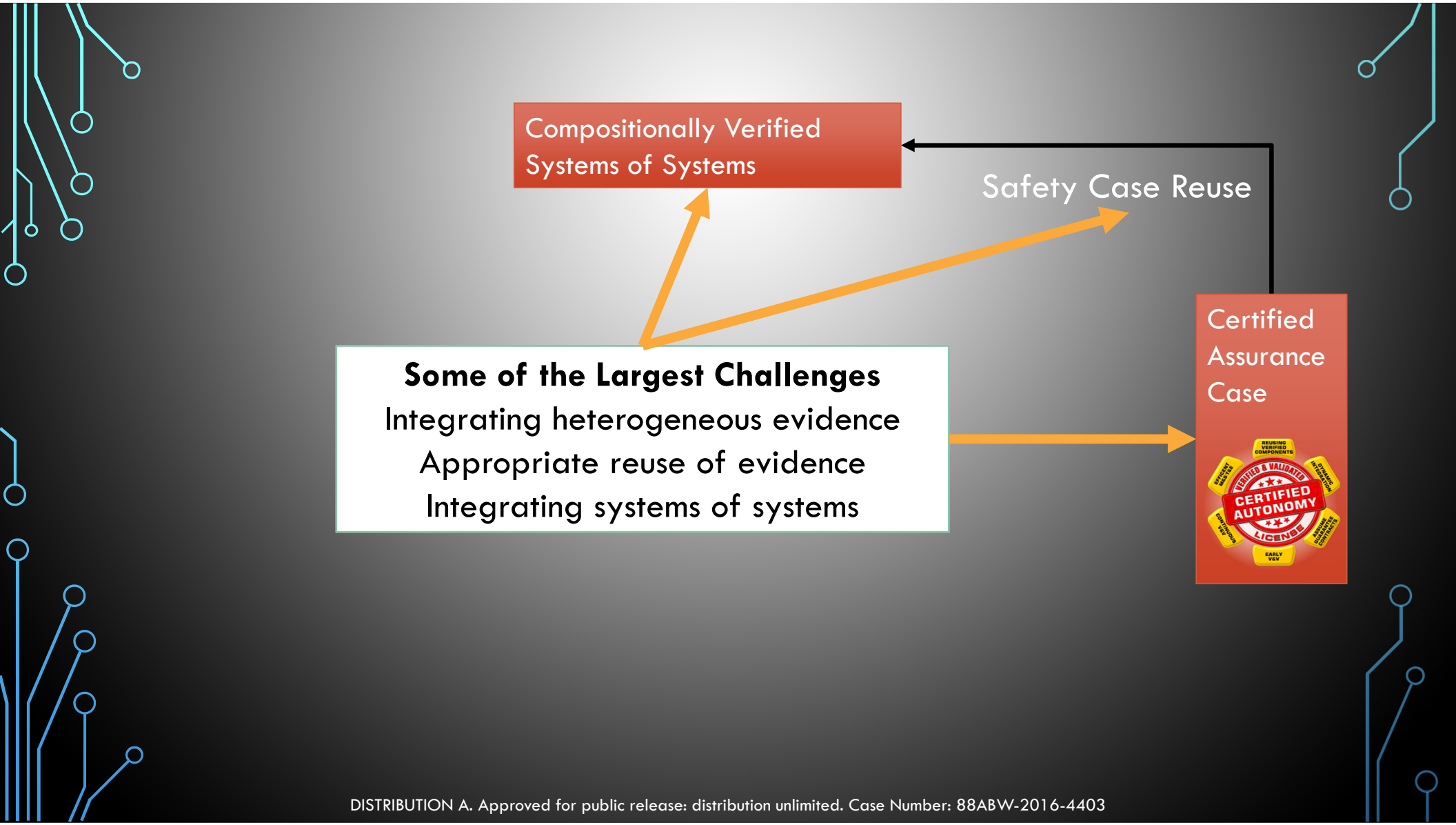
Modeling, Simulation, Test & Evaluation

Run Time Assurance

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



Testable Requirements & 178C/254, M



QUESTIONS?

Kerianne Gross

Kerianne.Gross@us.af.mil

937.713.7025

BACKUP SLIDES

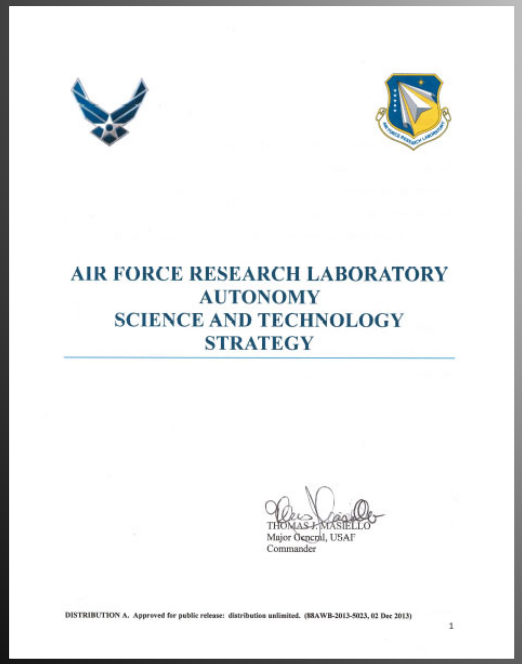
Verification and Validation Research Strategy

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*
- **Evidence based Design and Implementation**
  - *Assurance of appropriate decisions with traceable evidence at every level of design to reduce the current T&E burden*
- **Cumulative Evidence through RDT&E, DT & OT**
  - *Progressive sequential modeling, simulation, test and evaluation*
- **Run time behavior prediction and recovery**
  - *Real time monitoring, just-in-time prediction, and mitigation of undesired decisions and behaviors*
- **Assurance Arguments for Autonomous Systems**
  - *Reusable Assurance Case based on previously evidence building blocks*

AFRL V&V Research Areas

AFRL AUTONOMY S&T STRATEGY



AIR FORCE RESEARCH LABORATORY
AUTONOMY
SCIENCE AND TECHNOLOGY
STRATEGY

THOMAS J. MASIELLO
Major General, USAF
Commander

DISTRIBUTION A. Approved for public release: distribution unlimited. (88AWB-2013-5023, 02 Dec 2013)

1

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