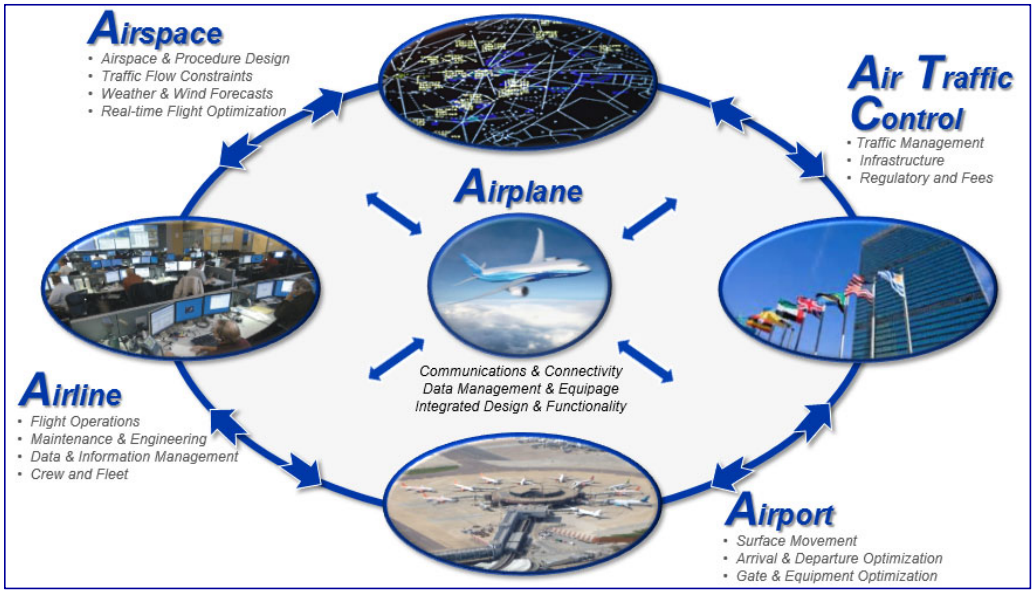
Model Based Systems Engineering and Model Based Safety Analysis

Daniel Fogarty
Boeing Commercial Airplanes

Framework Is Needed to Ensure Air Traffic Safety Goals Met

– Increasingly Autonomous Systems, New System-of-System Risks

- Framework needed to evaluate “system of systems” safety impact due to architecture changes:
  - Reallocation of existing functionality
  - New functionality
  - New interdependencies
- Framework needed to derive and levy failure probability, availability, integrity requirements on systems in air traffic “systems of systems” (i.e. design it in)
- Framework needed to ensure no discrepancies between safety requirements with the air traffic system of systems
- Framework needed to do system of systems validation and verification



“5A” Environment

Air Traffic Safety Framework Helps Evaluate and Ensure Success

ECCN: 9E991

Evolution of Boeing Commercial Airplanes: Major Model First Flights

Airplanes basically look the same.

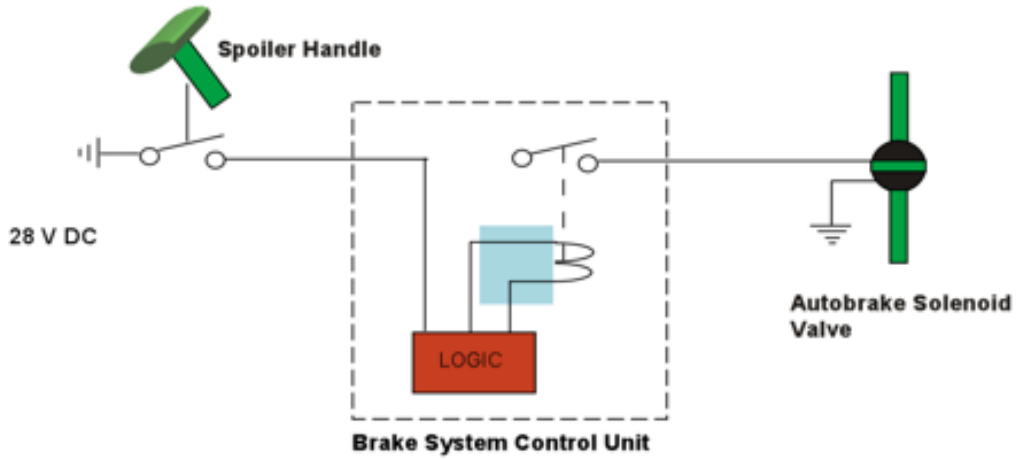
Why have integration challenges increased over time?

Why do Model Based Systems Engineering (MBSE) and Model Based Safety Analysis (MBSA)?

Evolution of Systems Architectures Has Impacted Required Integration and Safety Activities

Architectural styles

B-767 - Simple components with simple interfaces



The system designer defines the interface.

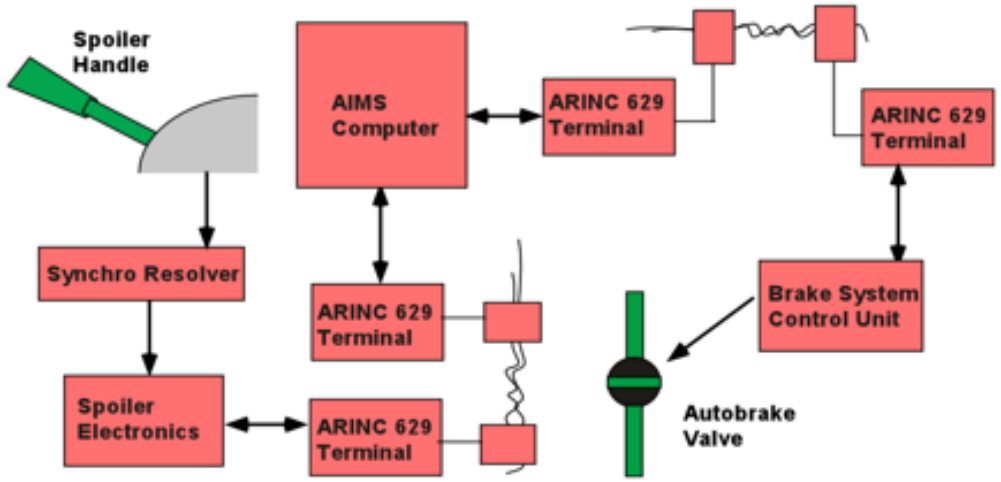
The connectivity and context are easily depicted by the ATA system schematic.

The integration effort is correspondingly simple.

Evolution of Systems Architectures Has Impacted Required Integration and Safety Activities

Architectural styles

B-777 - Simple components with complex interfaces



The interface is defined by others.

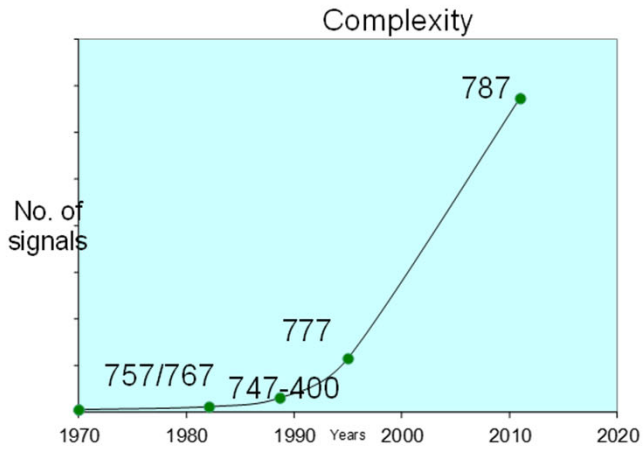
The system designer has to absorb and produce a large amount of detail.

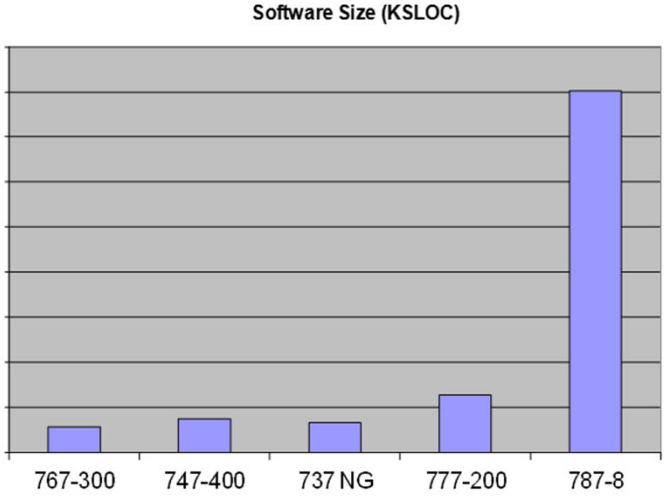
The ATA schematic must be augmented by ICDs, protocol definitions, system descriptions, and etcetera.

Integration becomes very difficult.

Evolution to Software Intensive & Integrated Architectures
Improved Performance and Increased Integration Challenges

- Increased systems interfaces increase validation and verification challenges
- Change impact analysis becomes more critical for highly integrated systems
- Same airplane trends will impact 5A System of Systems, where airplane is just a node in the system



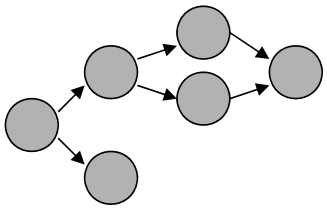


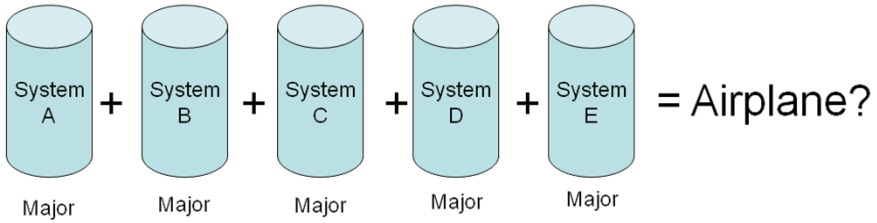
Increased systems complexity/integration drives need for modeling and analyses

ECCN: 9E991

Important Consideration: Assessing Cumulative Failure Effects of Highly Integrated Systems

- **Ensure that interdisciplinary approach considers both nominal and failure conditions**
- **Interdisciplinary approach needs to validate that the system is going to work with no anomalous behavior, and will function as expected in given failure conditions**

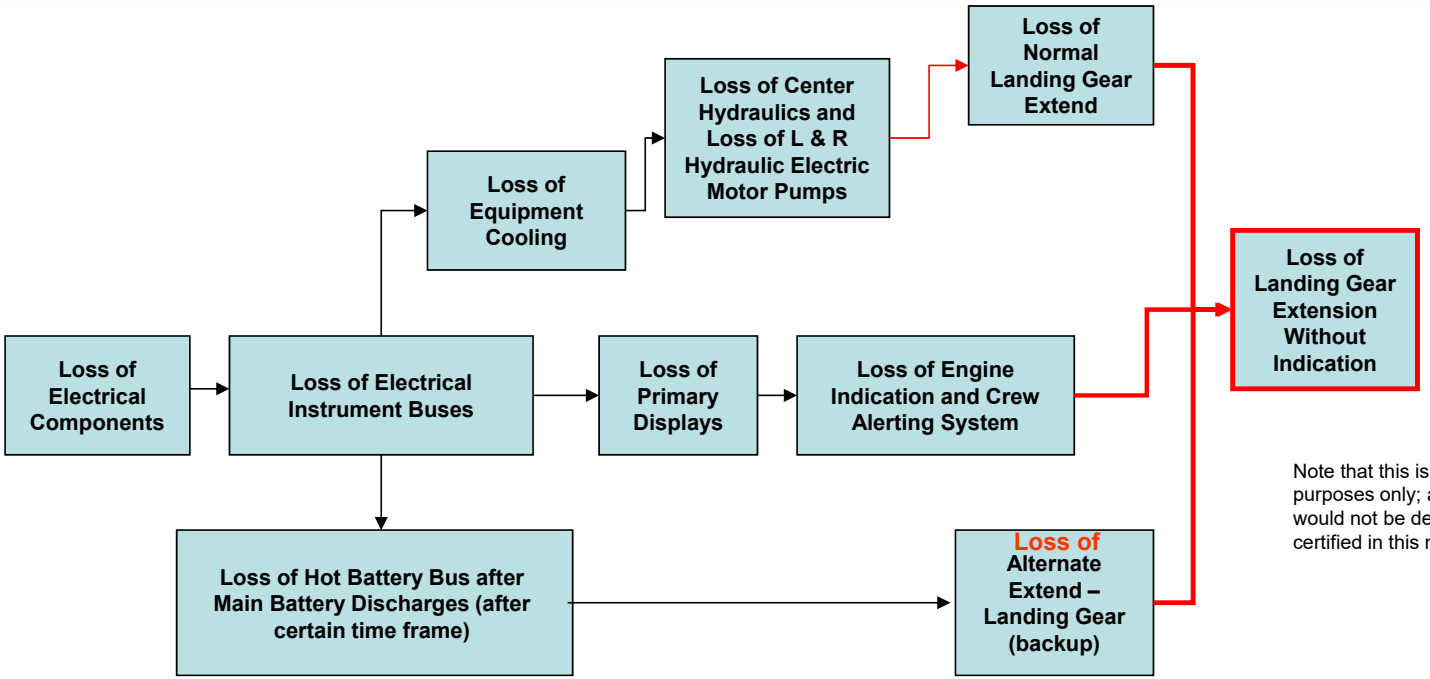




Single Failure Example and Cascading Effects

- **If there is an acceptable system level of degradation for each system, does this mean that the cumulative effect will be acceptable?**

Important Consideration: Assessing Cumulative Failure Effects of Highly Integrated Systems



Simplified Diagram

Note that this is for illustrative purposes only; aircraft systems would not be designed and certified in this manner.

- Effects of complex systems interfaces with other complex systems not always immediately transparent.
  - At each point, all of the failures are acceptable from a systems perspective (acceptable loss of redundancy or functionality).
  - However, the cumulative effect of acceptable systems-level effects is catastrophic at the airplane level.

Model Based Safety Analysis Can Help Identify System Architecture Deficiencies

Evolution to Software Intensive & Integrated Architectures
Improved Performance and Increased Integration Challenges

- Benefits of software intensive and integrated architectures are often better understood than the technical challenges

- Need to ensure “system of systems” of validated and verified

Boeing 377 Stratocruiser

Boeing 787 Dreamliner

- New functionality
- Reallocation of functionality
- New interdependencies

Boeing has developed processes and tools to address “system of systems” validation and verification

ECCN: 9E991

High Level of System Complexity and Integration Drove Need for Integration Rich Data Modeling

787 Systems Architecture and Interfaces Modeled in an Integrated, Object-Oriented Database

- ~5,300 equipment installations with data interfaces
- ~6,000 messages
- ~10,000 electrical connections
- ~1,000,000 data parameters
- ~60,000,000 objects in database

Systems Architectures Created, Analyzed and Validated at Different Levels:

- Horizontal and vertical integration at all levels:
  - Airplane
  - System
  - Subsystem
  - LRU/Component
  - Message
  - Parameter

Extensive Integration Analyses Conducted:

- Intra-System Analyses
- Inter-System Analyses
- Airplane Level Analyses
- Single and Multiple Failure Case Analyses
- Cascading Failure Effects Analyzed
- End-to-End Timing Analyses (Latency, etc.)
- Bandwidth and Throughput Analyses
- Redundancy, Separation and Control

ICD and Analyses Coordinated and Integrated with Other Groups:

- Safety
- Certification
- Labs
- Flight Operations / MMEL
- Gauntlet / Flight Test
- Reliability, Maintainability & Testability
- ETOPS
- EME
- Wiring

BCA Firsts:

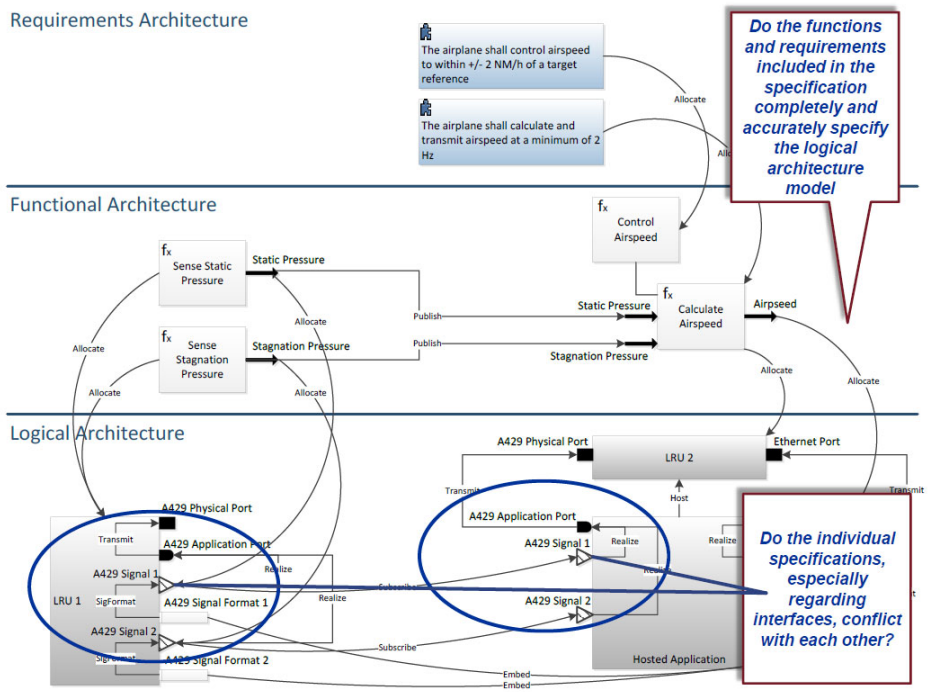
- Suppliers and Boeing working and integrating in the same, single source database (authoritative source for logical architecture)
- Depth and breadth of systems' interface modeling
- Discrepancies identified and resolved in an integrated manner Depth and breadth of functional integration analyses
- Single and multiple failure analyses conducted prior to first flight and results used for predicted flight test effects

Validation of Systems Architecture Prior to Testing Enabled by Model Based Systems Engineering, From Both Depth and Breadth Perspective

Model Based Systems Engineering (MBSE)

Need integrated framework/tools to manage interfaces across 5-A SoS

- MBSE has allowed Boeing to meet the following challenges:
  - Bounding increased data management effort due to increased systems integration
  - Coordination of development, design and data management activities within a globally distributed supplier base
- Boeing has reduced specification errors that result in costly rework
- Boeing has acquired some insights into what is required to effectively develop, deploy and manage an MBSE environment



Large scale highly integrated systems result in large and highly integrated models

Boeing Has Expertise in "System of Systems" Safety Analyses and Meeting Regulatory Requirements

- Airplane is a "system of systems"

- Boeing conducts safety analyses to ensure:
  - No single failure catastrophic and multiple failures <1E-9
  - Safety impacts of functional re-allocations understood and acceptable
  - Airplane and system safety assessments acceptable
  - Etc.

- Requirements identified and levied on systems (i.e. designed in)

	Classification of Failure Conditions				
	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants (excluding Flight Crew)	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Probability			~ 1E-05 or less	~ 1E-07 or less	~ 1E-09 or less

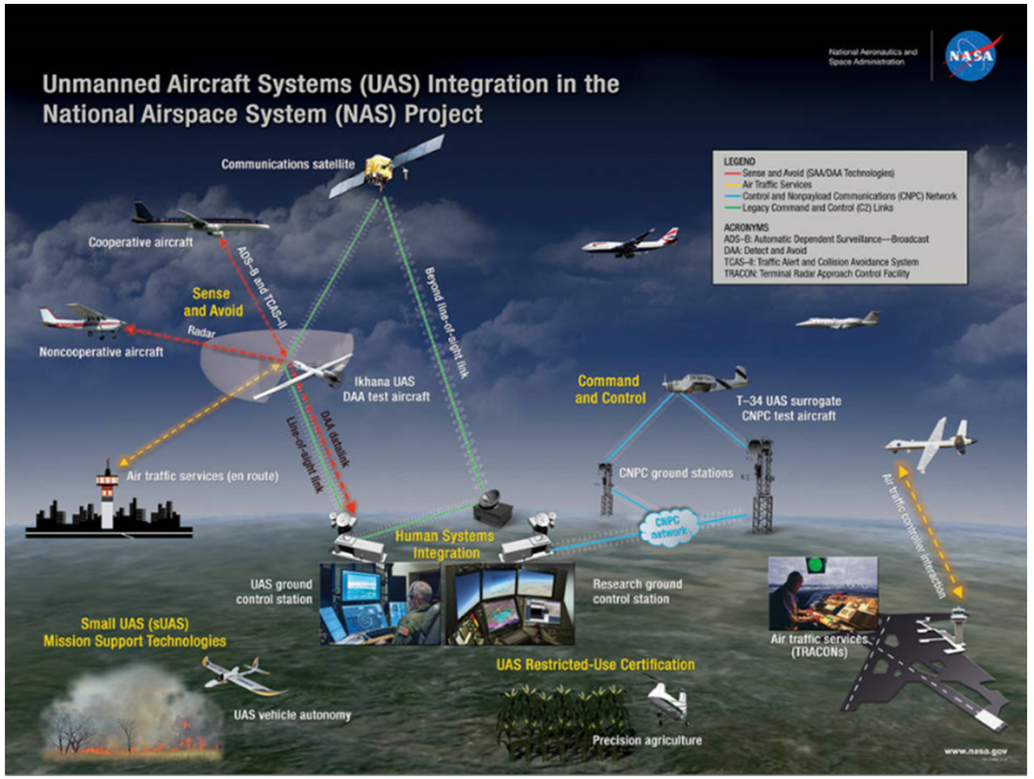
Existing Framework to Evaluate Airplane Safety ("Skin and In")

ECCN: 9E991

National Airspace System Evolution

- Air traffic "system of systems" is changing:
  - New functionality
  - Reallocation of existing functionality (including autonomous systems)
  - New interdependencies
  - Increased air vehicles

- Need framework to be able to evaluate system of systems safety ("skin and out")

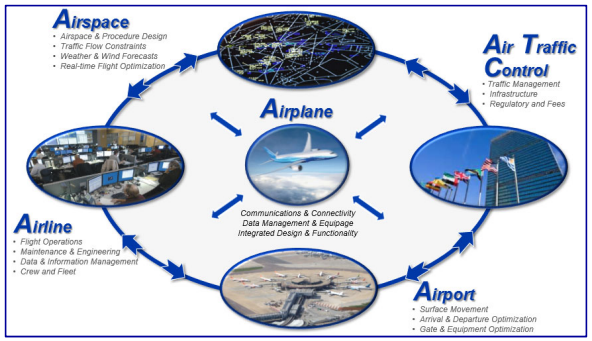


Same Airplane Architecture Trends Occurring in 5A System of Systems (SoS), Where Airplane Is Just a Node in the System

Framework Is Needed to Ensure Air Traffic Safety Goals Met

– Increasingly Autonomous Systems, New System-of-System Risks

- A framework needs to be developed to be able to evaluate the potential impact to safety as the ATM system changes (reallocation of existing functionality, new functionality, new interdependencies, etc.)
- Same architecture trends and integration challenges facing the 5A air traffic management environment occurred within airplanes and other Boeing products
- Boeing developed MBSE and MBSA processes and tools to address these challenges
- These processes and tools could potentially be extended to help with validation and verification in the 5A environment



Boeing Developed Processes/Tools Could Potentially Help Create And Validate the "5A" Safety Framework

Questions

ECCN: 9E991