Applicability / Compatibility of STPA with FAA Regulations & Guidance

First STAMP/STPA Workshop

Presented by:
Peter Skaves, FAA Chief Scientific and Technical Advisor for Advanced Avionics

Federal Aviation Administration

Briefing Objectives

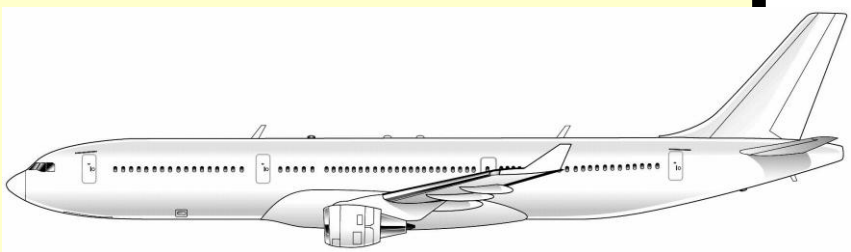
First Stamp/STPA Workshop

- ✓ *Airplane System Design Assurance Process*
- ✓ *Evolving Aircraft Avionics Complexity*
- ✓ *Federated Systems Architecture*
- ✓ *Redundancy & Fault Handling*
- ✓ *Integrated Modular Avionics*
- ✓ *Software Versus Requirements Errors*
- ✓ *STAMP/STPA Discussion Items*
- ✓ *Requirements Allocation*
- ✓ *HW / SW and System Processes*
- ✓ *Guideline Documents*
- ✓ *System Development Lifecycle*
- ✓ *Cyber Security & ARP 4754a*
- ✓ *Applicability / Compatibility of STPA*
- ✓ *Discussion and wrap-up*

Acronyms

AC	Advisory Circular
AEH	Airborne Electronic Hardware
ARP	Aerospace Recommended Practices
ARP 4754a	Guidelines for Development of Civil Aircraft and Systems
BITE	Built-in Test Equipment
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
DO-178	Software Considerations in Airborne Systems and Equipment Certification
DO-254	Design Assurance Guidance for AEH
HW	Hardware
IMA	Integrated Modular Avionics
NextGen	Next Generation Air Transportation System
FAR	Federal Aviation Regulation
RAM	Random Access Memory
STAMP	Systems Theoretic Accident Model and Processes
STPA	System Theoretic Process Analysis
SW	Software

The Airplane System Design Assurance Process



Examples of airplane systems certification rules and guidance

- ✓ **FAR 25.1301** **"General Requirements for Intended Function"**
- ✓ **FAR 25.1309** **"Equipment Systems and Installation"**
- ✓ **AC 20-152** **"Invokes RTCA DO-254 "Design Assurance Guidance for Airborne Electronic Hardware"**
- ✓ **AC 20-115B** **"Invokes RTCA DO-178B Software Guidance"**
- ✓ **AC 20-174** **"Invokes ARP 4754a "Guidelines for Development of Civil Aircraft and Systems"**
- ✓ **ARP 4761** **"Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems"**

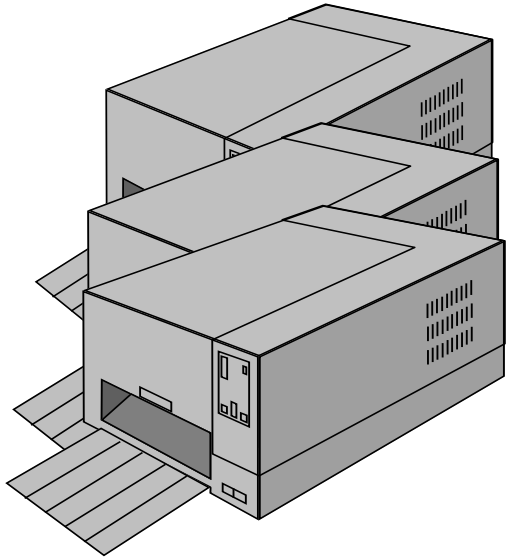
Evolving Aircraft Avionics Complexity & Systems Integration Issues (sheet 1 of 2)

- Aircraft avionics & systems integration issues
  - ✓ Difficulties in analyzing and testing avionics systems requirements due to complexity
  - ✓ Aircraft and systems level requirements validation & verification
  - ✓ Transitioning from federated architectures to Integrated Modular Avionics (IMA) systems
  - ✓ Predicting system and pilot response in the presence of failures
  - ✓ Numerical probability limitations
  - ✓ Software and requirements process error contributions
  - ✓ System development and safety assessment interwoven or separate processes
  - ✓ Aircraft integration with operating environment (e.g., NextGen)

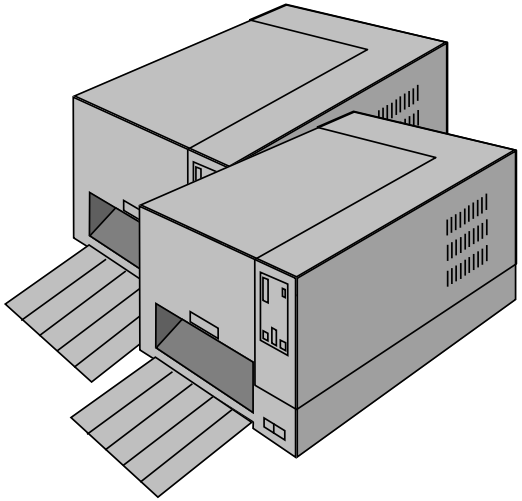
Evolving Aircraft Avionics Complexity & Systems Integration Issues (sheet 2 of 2)

- The current trend in system design involves increased interaction between aircraft functions and between the digital systems and equipment that implement those functions
- Increased interactions increase the possibilities for errors with functions that are performed jointly across multiple systems
- Traditional methods of demonstrating compliance to federated system architectures, do not adequately support validation & verification of multiple complex systems
- Since many aircraft/system-level decisions are fundamental to the safety aspects of aircraft design and operation, additional methods to mitigate and reduce system errors are needed

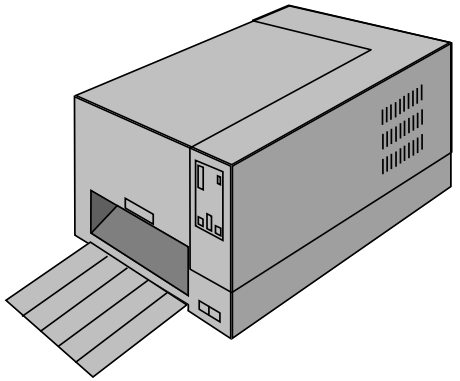
Federated System Architecture



- ✓ Triplex Redundancy
- ✓ Flight Control Systems
- ✓ With independent Backup system



- ✓ Dual Redundancy
- ✓ Flight Management Computers



- ✓ Single Strand
- ✓ ACARS Communication System

Federated Avionics Computer Architecture

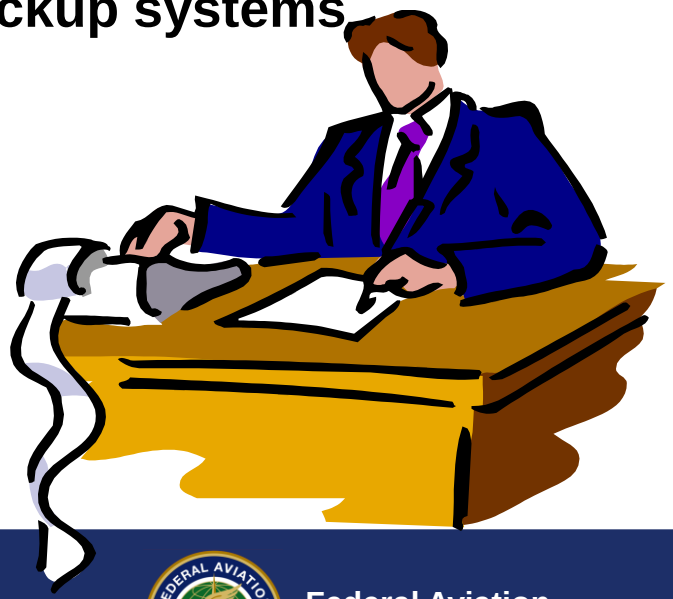
- **Computer Architecture**
  - CPU
  - Program Memory (e.g., Flight Control Software)
  - RAM Memory
  - Digital Busses (e.g., ARINC 429)
  - Discrete I/O
  - Variable Analog
  - Power Supply
  - Chassis

- **Strengths**
  - Isolation of faults
  - Failure analysis and fault detection are enhanced

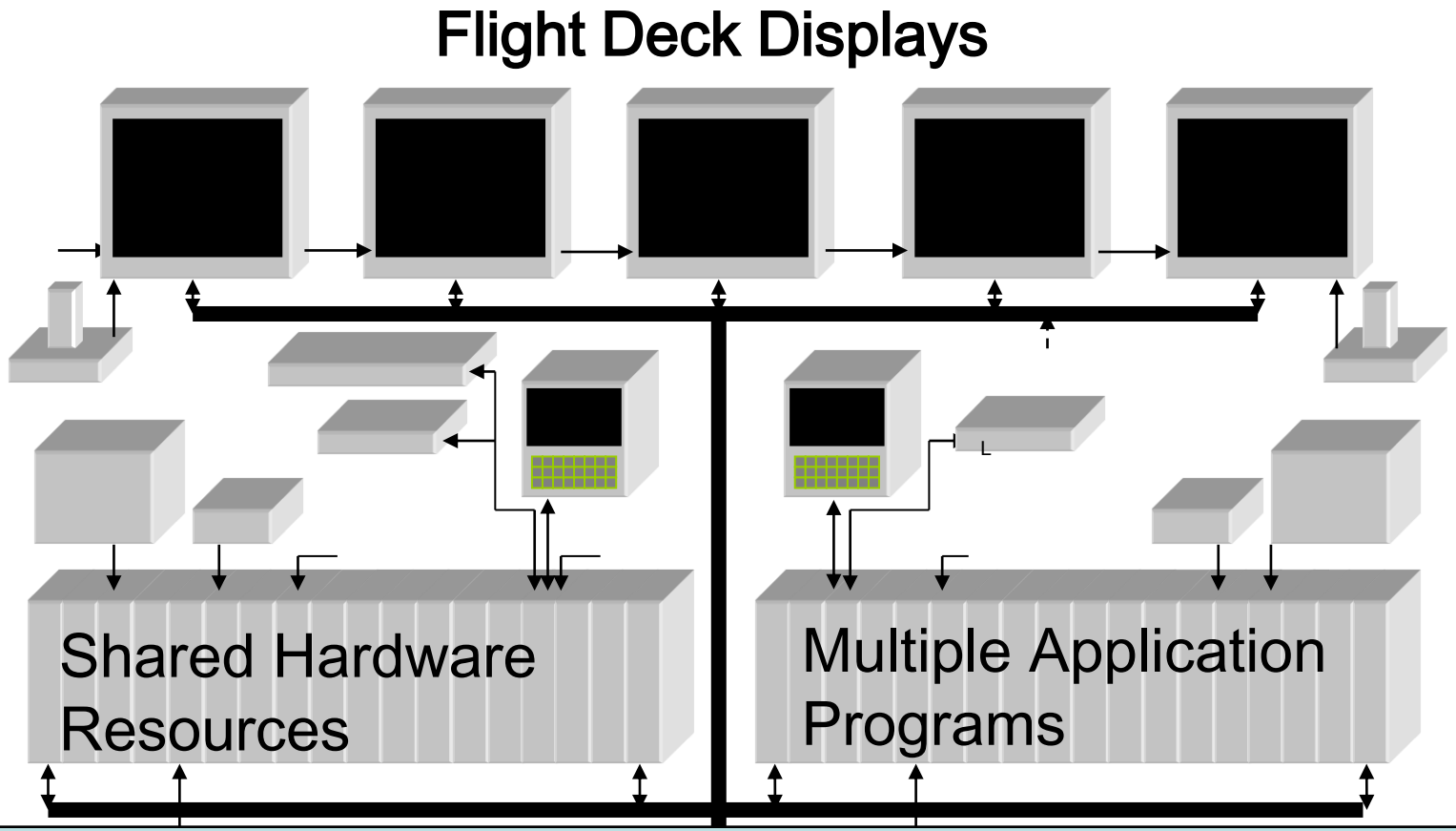
- **Weakness**
  - Duplication of hardware resource
  - Dedicated airborne software program for each avionics computer

Redundancy & Fault Handling

- **Avionics Hardware / Software Redundancy & Fault Handling:**
- ✓ **Typically dual or triple channel**
- ✓ **Voting planes are used to detect and isolate various sensors and aircraft interface inputs**
- ✓ **Built-in Test Equipment (BITE) software are used for internal computer validity checks (e.g, Memory, CPU)**
- ✓ **Common mode failure mitigation may require independent back-up systems**
- ✓ **Examples of independent back-up systems include Standby Flight Instruments or mechanical backup systems**



IMA Notional Diagram



Example: TWO cabinets replace over 100 Federated Systems

Integrated Modular Avionics (IMA) Computer Resource

- **Computer Architecture**
  - CPU
  - Memory Management Units
  - RAM Memory
  - Digital Busses (e.g., ARINC 429)
  - Discrete I/O
  - Variable Analog
  - Power Supply
  - Chassis
- **Strengths**
  - Shared Hardware Resources
  - Software programs are “swapped” and execute concurrently on same computer platform
- **Weakness**
  - Failure analysis, fault detection & isolation of faults are more difficult
  - Common mode fault vulnerability

Common Mode Failure Mitigation

- **Boeing 777 Fly-by-Wire Flight Control architecture**
  - ✓ **Three digital Flight Control Computers**
  - ✓ **Analog electric back-up system to mitigate generic common mode faults**
- **C-17 Cargo Airplane**
  - ✓ **Fly-by-Wire Flight Control System**
  - ✓ **Full Mechanical Back-up**

- **Boeing 737/747/757/767 Series Airplanes**
  - – Do not require electric power for continued safe flight and landing with the exception of the battery backup bus for the Standby Flight Instruments
  - – Full mechanical backup Flight Control System

Boeing 777 Flight Deck

Software Versus Requirements Errors

- Airborne avionics system problems are reported as "*software problems, anomalies, bugs or glitches*"
- Many airborne avionics system problems are not caused during the software development process
- Perfect software does not mean the airborne system requirements are perfect
- Incomplete or incorrect requirements are the root cause of most avionics system failures
- Development processes for Civil Aircraft and Systems are being emphasized
- Robust Integration of highly complex systems at the airplane level is one of the keys to success

Validation vs. Verification

- **VALIDATION: The determination that the requirements for a product are correct and complete.**
  Are we building the right aircraft / system / function / item?

- **VERIFICATION: The evaluation of an implementation of requirements to determine that they have been met.**
  Did we build the aircraft / system / function / item right?

Both validation and verification apply to every requirement

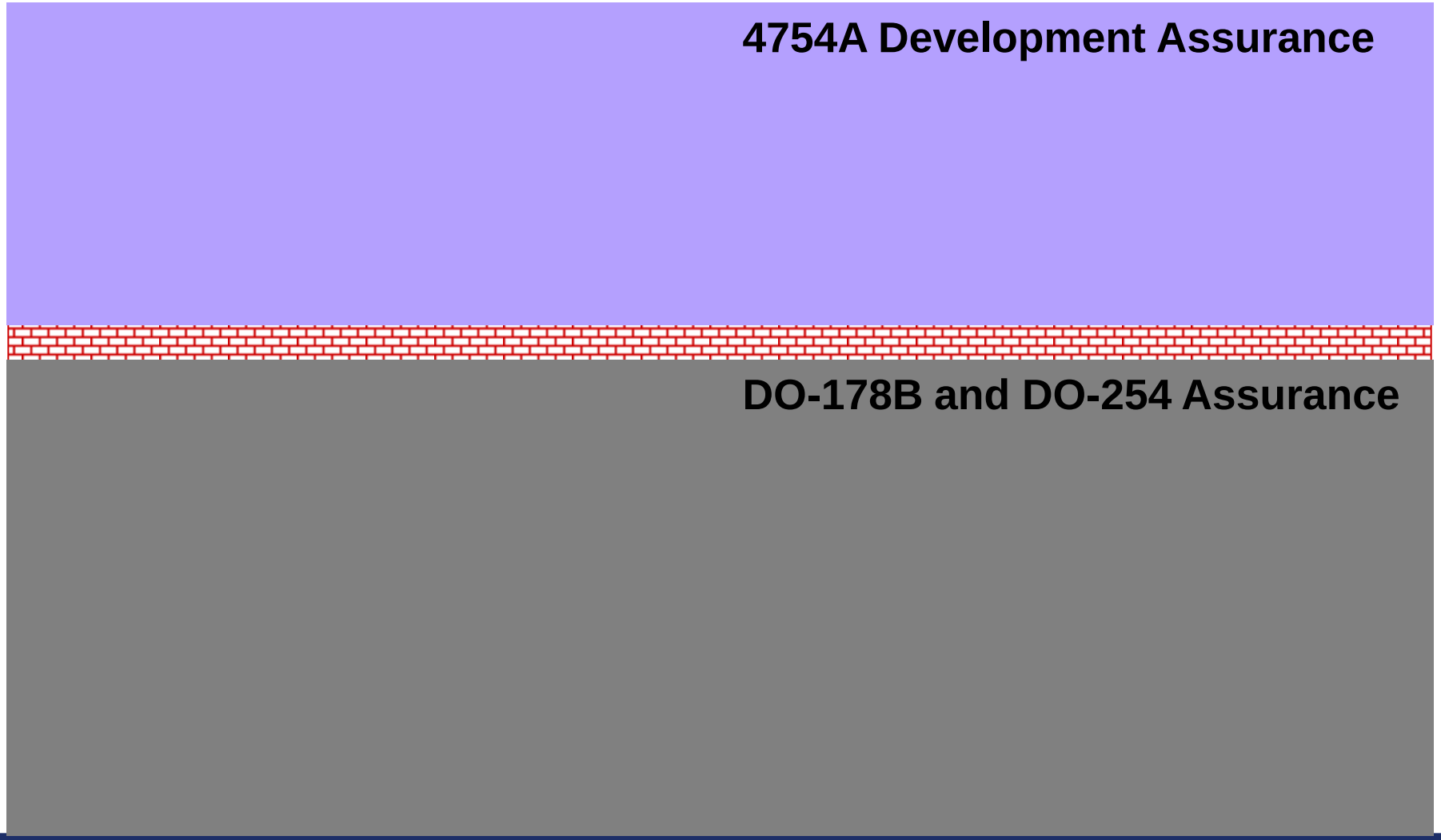
STAMP / STPA Discussion Items (sheet 1 of 2)

- Proposes an alternative process to current FAA safety assessment methods
- States that traditional approaches to safety analysis assume that accidents are caused by component failures
  - ✓ Worked well with legacy aircraft that had simple conservative designs
  - ✓ Does not work as well with very complex systems that are highly integrated with other systems
  - ✓ Extensive use of software allows very complex systems to be constructed, resulting in an increased potential for accidents from unsafe interactions among non-failed components
  - ✓ Failures resulting from unplanned behavior of software dependent systems may occur

STAMP / STPA Discussion Items (sheet 2 of 2)

- STAMP (and STPA) extends the safety analysis to include non-linear, indirect, and feedback relationships among events
- Extends the traditional approach to consider new accidents caused by component interactions, human mistakes, management and organizational errors and software errors (particularly requirements errors)
- STPA recognizes that accidents result not only from system component failures but also from interactions among system components that violate system safety constraints
- System Safety is reformulated as a system control problem rather than a component reliability problem

Requirements Allocation



Requirements Allocation

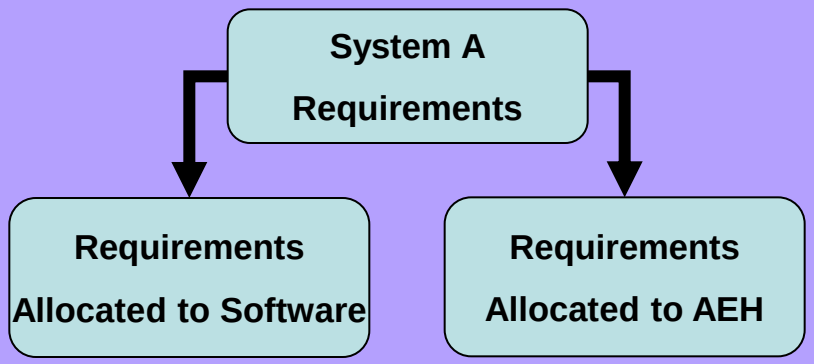
System A Requirements

4754A Development Assurance

Validates that the requirements are **correct** and **complete**

DO-178B and DO-254 Assurance

Requirements Allocation



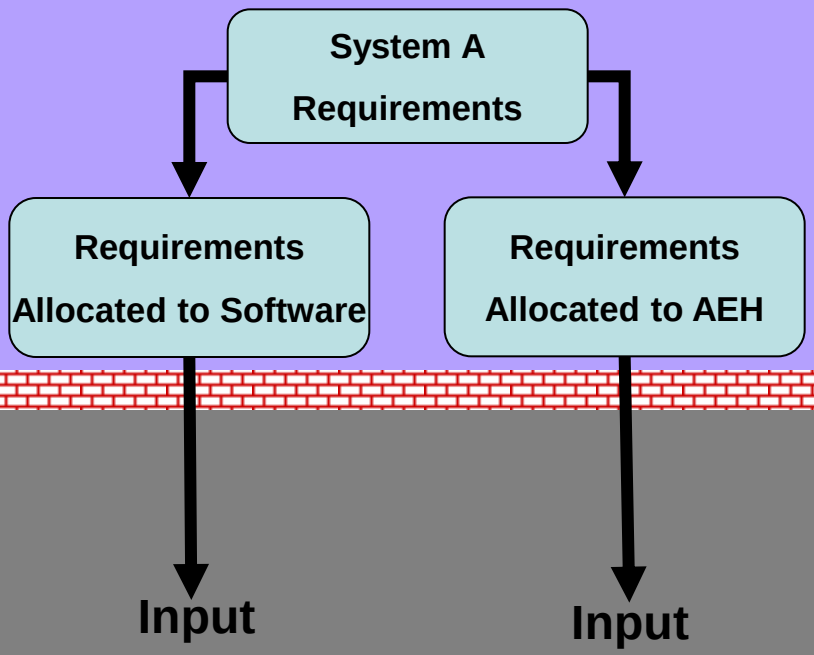
4754A Development Assurance

Validates that the requirements are **correct** and **complete**

Allocates requirements to software and AEH Items

DO-178B and DO-254 Assurance

Requirements Allocation



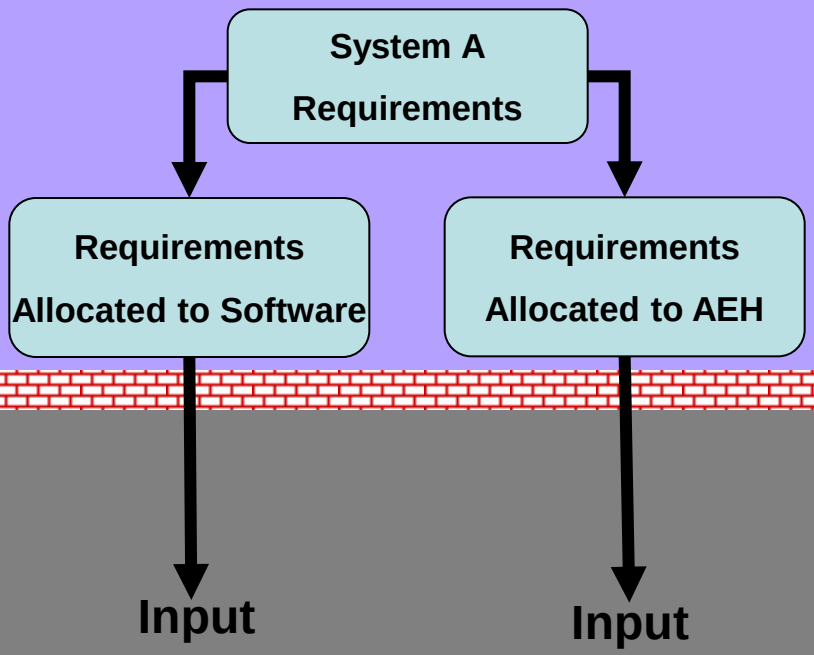
4754A Development Assurance

Validates that the requirements are **correct** and **complete**

Allocates requirements to software and AEH Items

DO-178B and DO-254 Assurance

Requirements Allocation



4754A Development Assurance

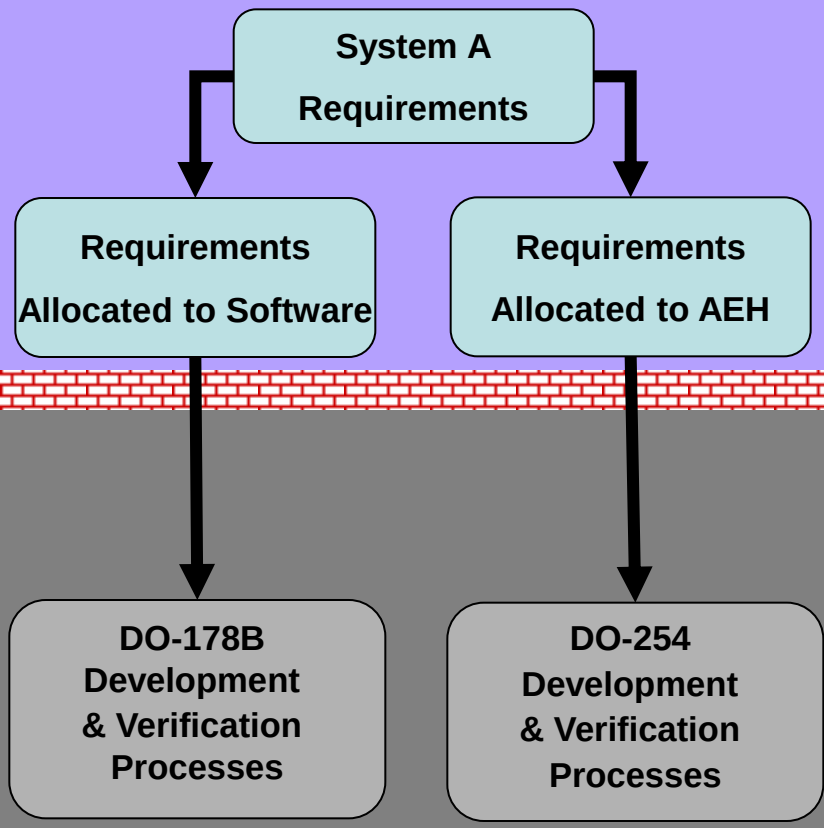
Validates that the requirements are **correct** and **complete**

Allocates requirements to software and AEH Items

DO-178B and DO-254 Assurance

Assume the requirements are **correct** and **complete**

Requirements Allocation



4754A Development Assurance

Validates that the requirements are **correct** and **complete**

Allocates requirements to software and AEH Items

DO-178B and DO-254 Assurance

Assume the requirements are **correct** and **complete**

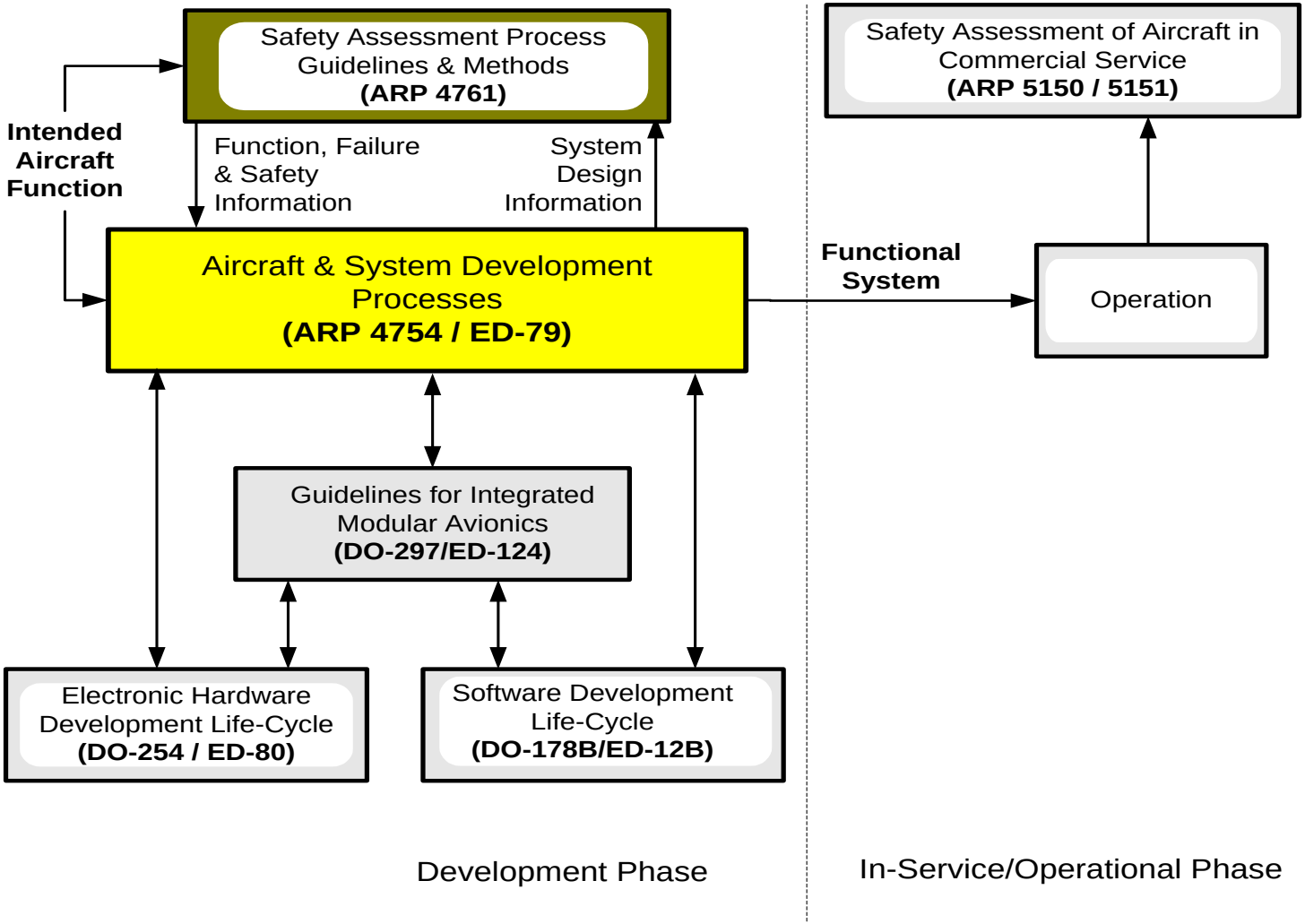
Develop the software and AEH

Verify that the software and AEH meets their requirements

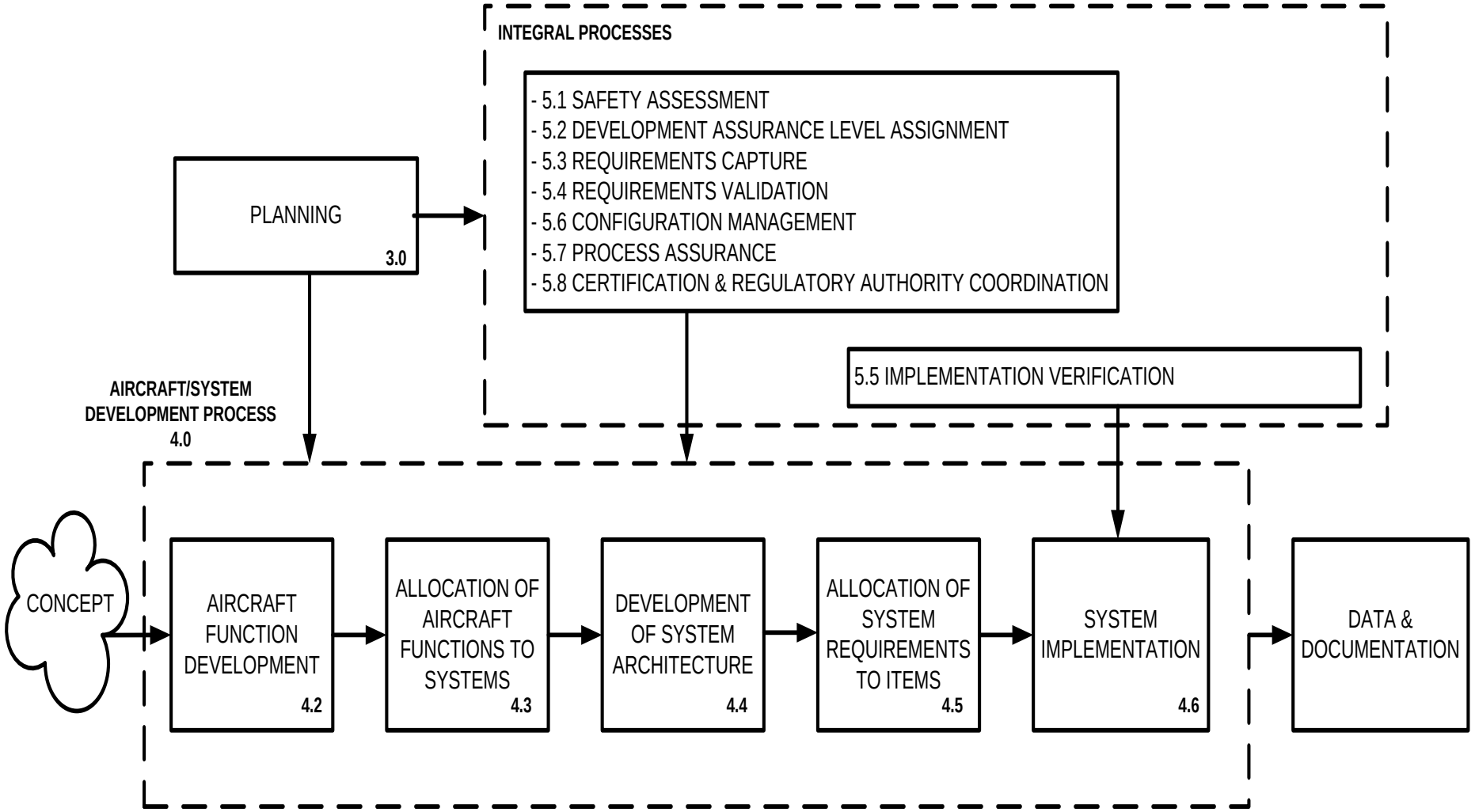
HW / SW and System Processes

- **DO-254 (HW), DO-178 (SW) and ARP 4754A (System), are all assurance processes**
  - ✓ Invoked formally by FAA advisory circulars
  - ✓ Harmonized with International Civil Aviation Authorities
  - ✓ Establishes confidence that the development has been accomplished in a sufficiently disciplined manner to limit the likelihood of development and requirements errors that could impact aircraft safety
  - ✓ Assurance level establishes the level of process rigor which is commensurate with the functional failure condition
  - ✓ They are all dependent on each other

Guideline Documents



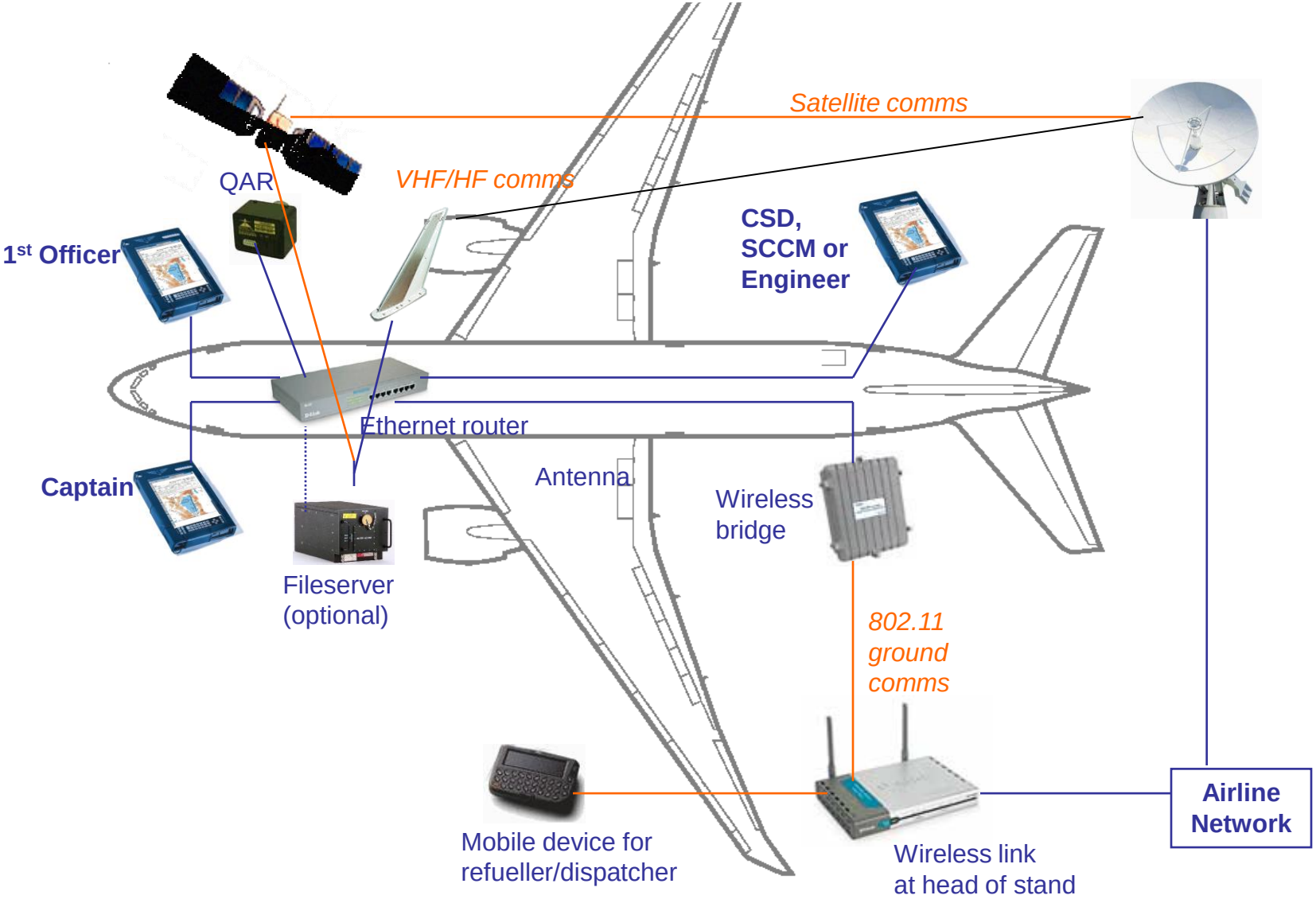
Aircraft or System Development Lifecycle



Aeronautical Systems Security & ARP 4754a

- The existing Code of Federal Regulations does not specifically address cyber security vulnerabilities
  - ✓ Special Conditions have been Issued for certain Boeing and Airbus Airplanes
  - ✓ Ground based Information Technology (IT) networks are able to read/write information to aircraft avionics systems
  - ✓ RTCA SC-216 Aeronautical Systems Security is developing industry Standards
  - ✓ Current proposals include adding cyber security requirements to the ARP 4754a development process

Possible Architecture & Infrastructure



Applicability / Compatibility of STPA

- Need to identify gaps in existing FAA guidance material that STPA would address (would require review of the new ARP 4754a and proposed ARP 4761 standards)
- FAA needs to better understand the STPA model with respect to accident causes, tool analysis and safety constraints
- Need to determine how the STPA process could be used in combination with other FAA guidance material
- Would need to obtain consensus with industry and international Civil Aviation Authorities in the use of STPA
- Recommendations include implementation of STPA on a pilot certification project for fact finding purposes

Questions & Wrap-Up

- **Send your questions to me at:**
  - peter.skaves@faa.gov
  - Telephone (425) 917-6700
- **Thank you for your assistance !!!**