CONNECTED AVIATION SUMMIT® 2023

Digital Transformation, AI & Innovation

September 6-8, 2023 | Hilton City Center | Denver, CO

# Are We Shifting Left Enough?

*FAA Emerging Strategies to Identify and Resolve Cyber Vulnerabilities Early in the Development Cycle*

Presented by: Hector Morales

Federal Aviation Administration

Enterprise Architecture Manager

FEDERAL AVIATION ADMINISTRATION

ATO Cybersecurity Group

CONNECTED AVIATION SUMMIT® 2023
Digital Transformation, AI & Innovation
September 6-8, 2023 | Hilton City Center | Denver, CO

# The V-Model Verification & Validation (V&V) Process

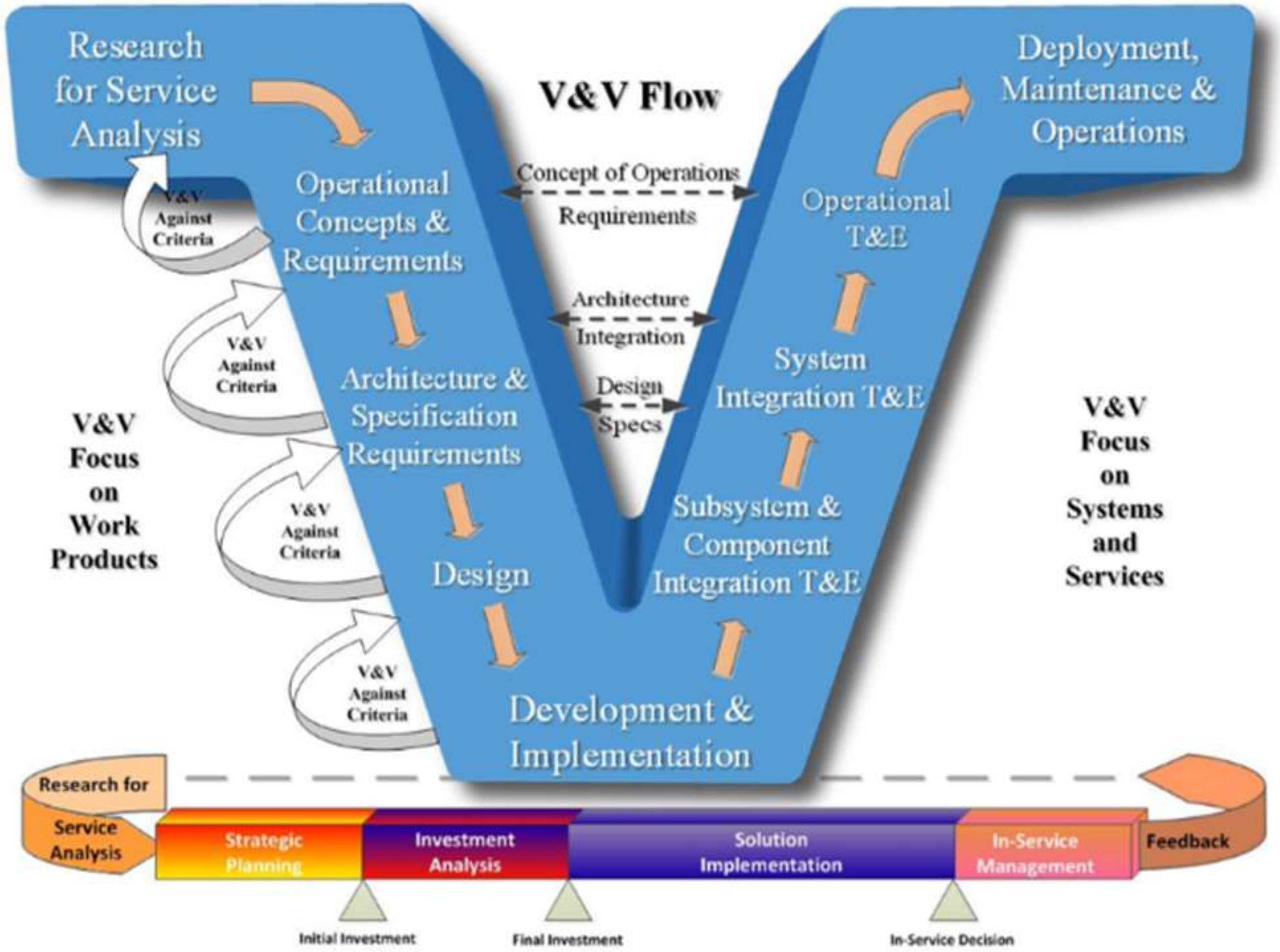
- Traditionally, a V-model approach is used to conduct Verification and Validation (V&V) during a product's Lifecycle Process.

- The V-model establishes an association between each phase of Development and Testing.
  - Development = Verification Phase
  - Testing = Validation Phase

- Generally, the physical infrastructure is replicated in a Development Service Verification test bed prior to going into the Operational environment
  - Each are self-contained and have to be informally or formally tested.
  - These tests are generally performed manually by an independent QA/QC program.

Verification Phases

Validation Phases

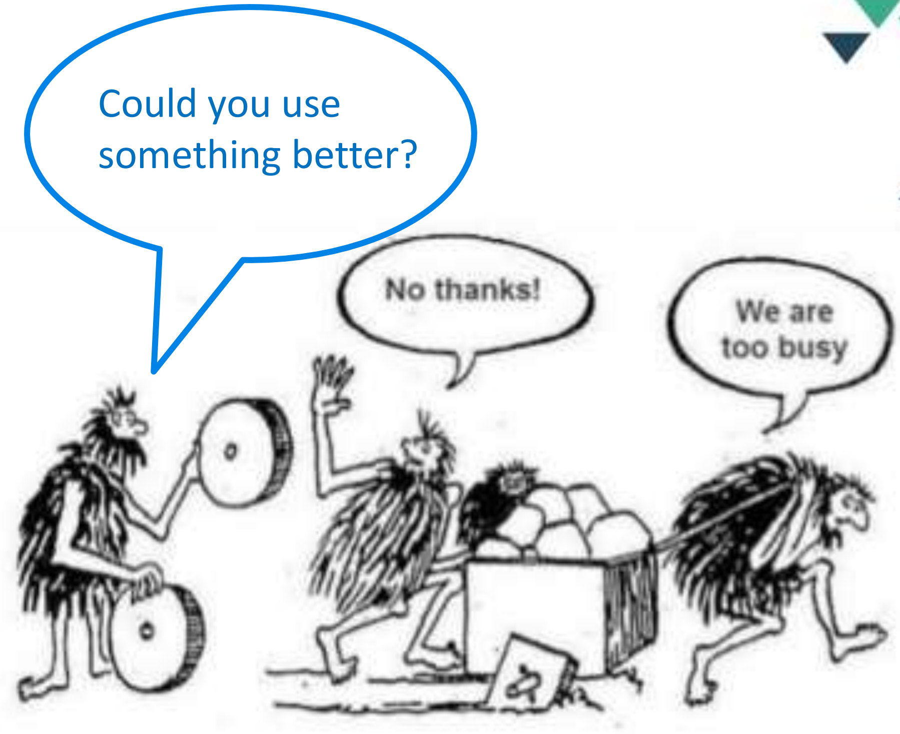


# Challenges of the Status Quo

- Traditionally, code is subjected to security as the *last phase before release* which often creates a time crunch.
  - Developers are usually working till the last minute, leaving the security team little time to ensure the code is secure.

- When vulnerabilities are exposed, either the release is *delayed* or the development team has to scramble to correct each security issue while the security team has to scramble to check the revisions.

- This creates *a great deal of expense* and slows down application release and launches
  - If iterations are released in haste, the chances of overlooking or under-prioritizing a vulnerability are significant.

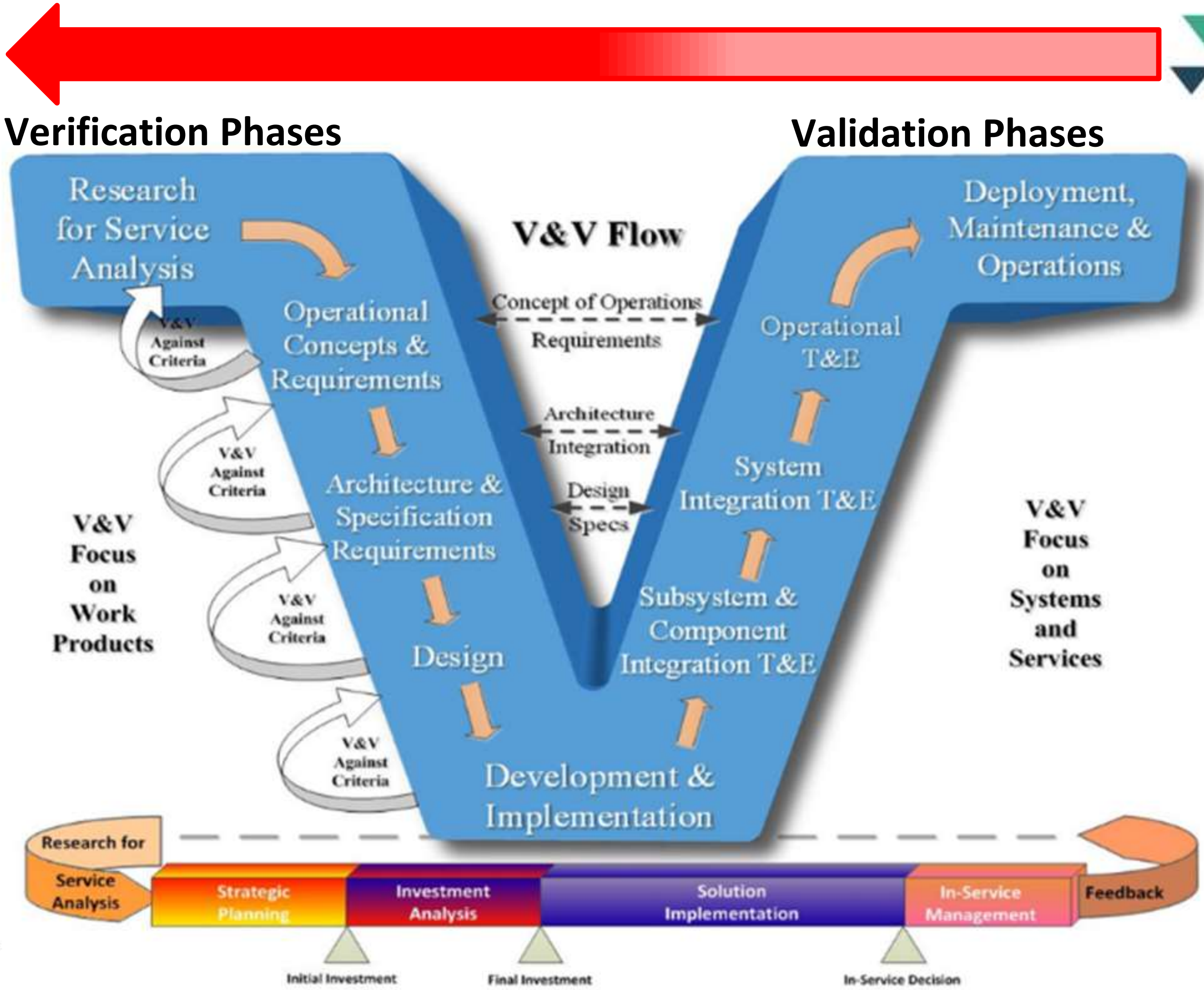


*To fully implement a Shift Left Approach, a change in culture is necessary*

CONNECTED AVIATION SUMMIT® 2023
Digital Transformation, AI & Innovation
September 6-8, 2023 | Hilton City Center | Denver, CO

# Shifting Left, Secure by Design

- The complexity of the NAS and the ever-evolving cyber threats are driving the need for security involvement earlier in the software development life cycle
- Shift Left = SecDevOps versus DevSecOps
- Objective is to introduce Cyber requirements, V&V and Test & Evaluation (T&E) activities earlier in the Development Cycle
  - Identifies and Mitigates Risk Earlier
  - Lowers long-term cybersecurity costs
  - Assures an on-time schedule



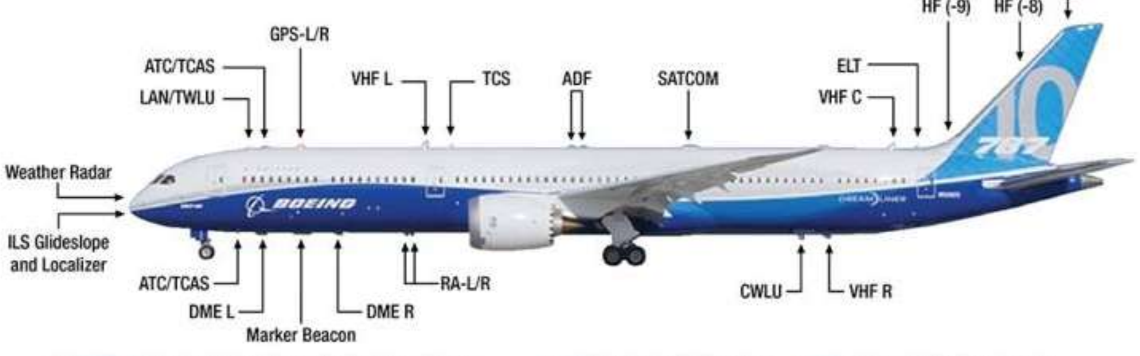
# Evolving Mitigation Activities

*The FAA is using mitigation activities to minimize risk in Development and Operational Environments*

*We are building segmented Operating Environments (OEs) to protect our Mission Critical (MC) and Mission Essential (ME) Systems/Services with Enterprise Cybersecurity Capabilities*

- **Managed Enterprise Security Monitoring**:
  - Integrate different monitoring and detection tools
  - Automate tasks for simpler, more effective security operations
- **Security Enterprise Asset Management:**
  - Centralized capability
  - Support collection of specific NAS assets for each environment
- **Centralized NAS Software Security Management:**
  - Improves cyber security posture of the NAS
  - Provides centralized capability for security patch & protection updates
- **Managed Enterprise Security Protections (Shared Telco):**
  - Implemented via a Network Edge Protection capability
  - Support secure NAS operations when running in a Zero-Trust environment

**Boeing 787 Antennas**



- LAN/TWLU Terminal wireless local area network (LAN) unit
- ATC/TCAS Air traffic control/traffic collision and avoidance system
- DME Distance measuring equipment
- RA Radio altimeter
- GPS Global positioning system
- TCS Terminal cellular system
- ADF Automatic direction finder
- CWLU Crew wireless LAN unit
- ELT Emergency locator transmitter
- HF High-frequency radio
- VOR VHF omni-directional ranging

*Source: Boeing*

*Like the NAS, Aircraft Systems are comprised of many supporting systems and services. In both, Segmentation is broadly used as a Defense-in-Depth Strategy*

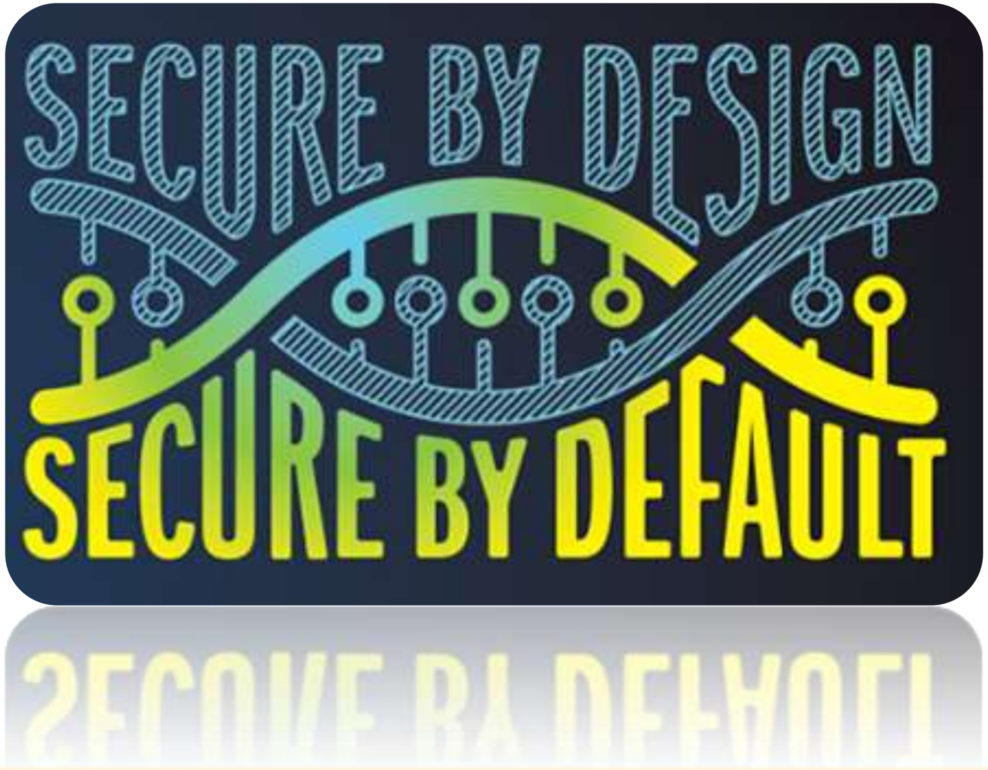
# Benefits

### Secure by Design

- Security issues are anticipated and remediated early
  - Relationships between developers, testers, security teams, and operations staff are streamlined

### Increased Delivery Speed & Reduced Cost

- Testing is one of the top reasons for release delays.
  - Shift Left cybersecurity supports faster application delivery because there is *no pause* in coding while cybersecurity teams perform their V&V and T&E reviews.
- Continuous testing means *security flaws are caught sooner*, so fixes are easier and less costly to make.
- Shift Left security *reduces the time* between releases by enabling DevOps and security to work in parallel thereby *reducing overall product cost*.



# Questions