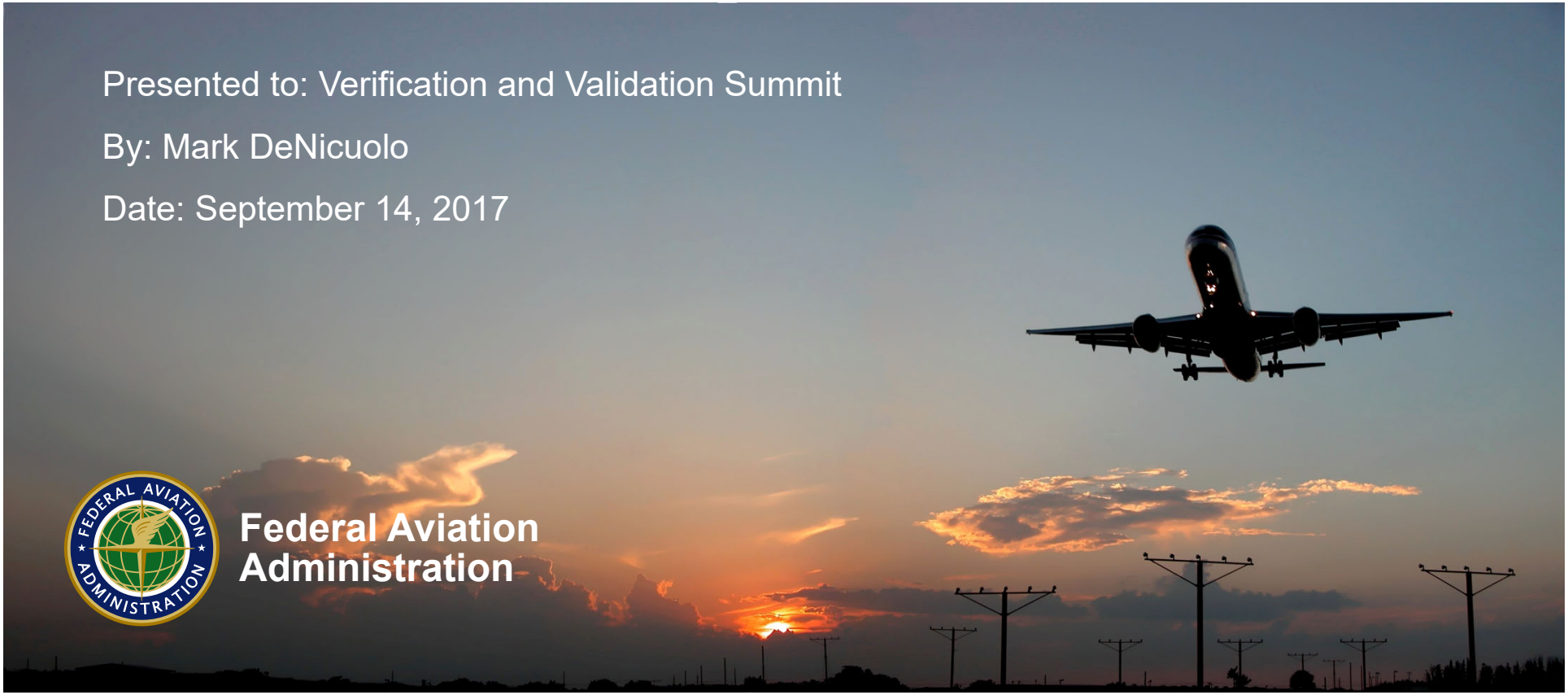
Safety in the ATO

Integrating Safety with Verification and Validation



Presented to: Verification and Validation Summit

By: Mark DeNicuolo

Date: September 14, 2017

Federal Aviation Administration

When safety isn't a priority…

Safety of the National Airspace System (NAS)

- **Safety programs help us understand:**
  - What is happening in the NAS
  - Where the hazards exist
  - How to mitigate the hazards
- **Examples of safety programs:**
  - Risk Analysis Process (Airborne, Surface, System Integrity)
  - Voluntary reporting programs
  - Partnership for Safety
  - Runway Safety
  - Quality Assurance and Quality Control
  - Safety audits and assessments

How the ATO Manages Safety

The ATO's safety management system is made up of four basic components:

V&V directly supports these areas.

The ATO's Approach to Safety:

Collect, Find, Fix

Collect, Find, Fix in Action: The Top 5

IFR/VFR
Close encounters between IFR and VFR aircraft

NOTAM Issuance/Cancelation
Lack of, untimely, or outdated NOTAMs in the system

NOTAM Prioritization
Inability of ATC or pilots to distinguish between applicable or pertinent NOTAMs

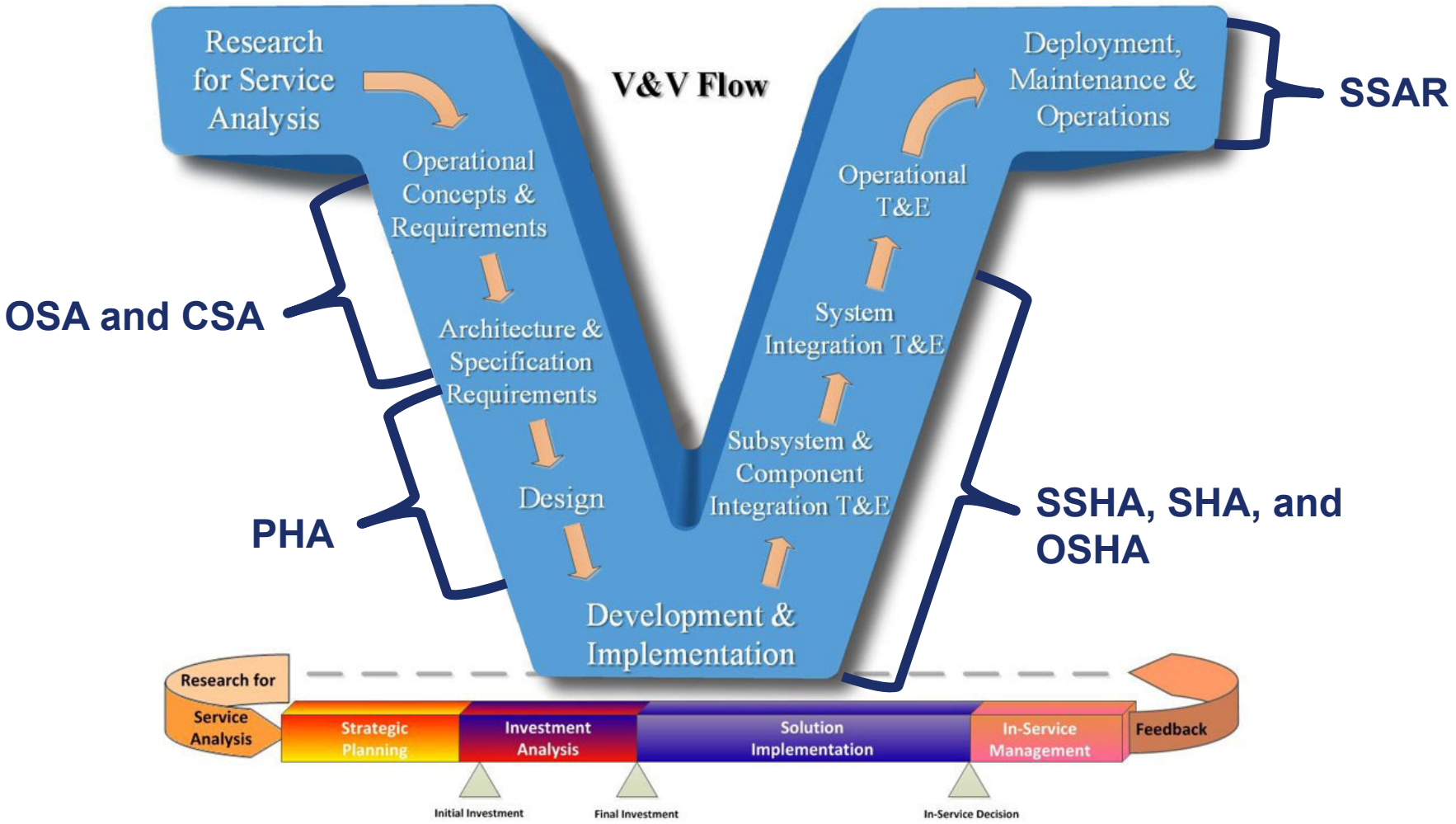
Runway Flyovers
Unexpected aircraft/vehicle on the runway with another aircraft cleared to takeoff/land, resulting in flyover

Wrong Surface Landing
Aircraft lands on wrong runway or taxiway, or at wrong airport

Safety Risk Management (SRM)

- **Any change to the NAS that affects operations requires a safety analysis.**
- **Safety analyses serve to:**
  - Understand the planned change (Collect)
  - Identify the potential safety risk of the change (Find)
  - Mitigate and monitor the risk (Fix)
- **For acquisition programs, this is an iterative process that matures with the program.**

How Safety Integrates with V&V



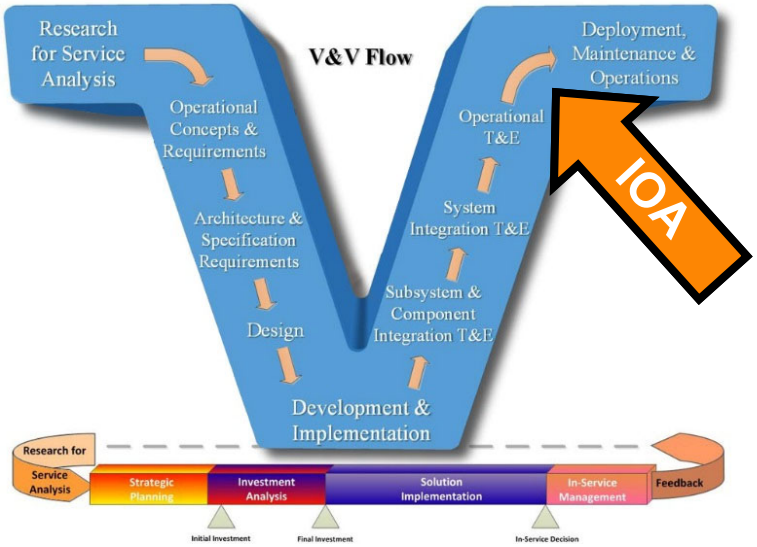
Safety Hazards

- **The Hazard Analysis Worksheet (HAW) is the basis of every safety analysis.**
- **For each hazard, the HAW includes:**
  - Cause
  - System state
  - Controls (already implemented)
  - Effects
  - Risk (severity and likelihood)
  - Performance targets
  - Safety requirements

Safety Requirements

- **Safety requirements are program requirements designed to mitigate the hazards in the HAW.**
- **All safety requirements must be verified and validated.**
  - This is typically done through the test program.
  - Verification and validation should consider the system state, causes, and controls from the HAW.
  - This is documented in the Safety Requirements Verification Table (SRVT).

Example: IOA Supports Safety and V&V

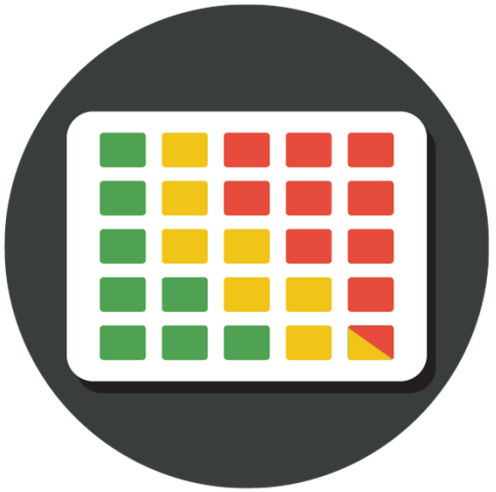


- ✓ IS IT **SUITABLE?**
- ✓ IS IT **EFFECTIVE?**
- ✓ IS IT **SAFE?**

- **Independent Operational Assessment (IOA) is conducted before full deployment of a system.**
- **IOA is a safety assessment and a V&V activity.**
- **IOA provides a readiness determination in support of the In-Service Decision.**

How IOA Integrates Safety

- **IOA incorporates SRM into its processes.**
- **IOA planning and conduct incorporates SRM documentation and answers the following questions:**
  - Are the identified hazards occurring?
  - Are there new hazards?
- **IOA reports findings that have any potential safety risks.**



V&V Supports Safety

- **Many new systems provide important safety benefits.** Watch the video ▶
- **V&V can support safety by ensuring that safety benefits are realized with minimal new risk.**
  - **Verification** of the safety requirements to reduce new risk
  - **Validation** that the design achieves the intended safety benefits

Event: San Francisco International Airport (SFO) *July 7, 2017, at 11:56 pm PDT*

- **Runway 28L was closed, but Runway 28R remained open. Taxiway C runs parallel to Runway 28R.**
- **ACA759 (Air Canada) was on an approximate 0.6 mile final when the pilot asked the controller to verify that they were still cleared to land on Runway 28R because they saw lights.**
  - The controller confirmed and re-cleared ACA759 to land on Runway 28R.
- **ACA759 instead lined up with Taxiway C and overflew the following four aircraft:**
  - UAL1 and PAL115 by 100 feet
  - UAL863 by 200 feet
  - UAL1118 by 300 feet

Watch the video ▶

What You Can Do

Know how your program benefits/impacts safety.

Understand how your program impacts the overall safety of the NAS.

Learn about the hazards and safety requirements associated with your program.

Verify safety requirements in the context of the hazard.

Report potential safety issues.

Determine if your V&V findings impact safety.