

T&E / V&V Role in Safety Management System (SMS)

Presented to: Verification and Validation Summit

By: James Daum

NextGen and Operations Planning Safety Manager

AJP-1900

Date: November 05, 2009



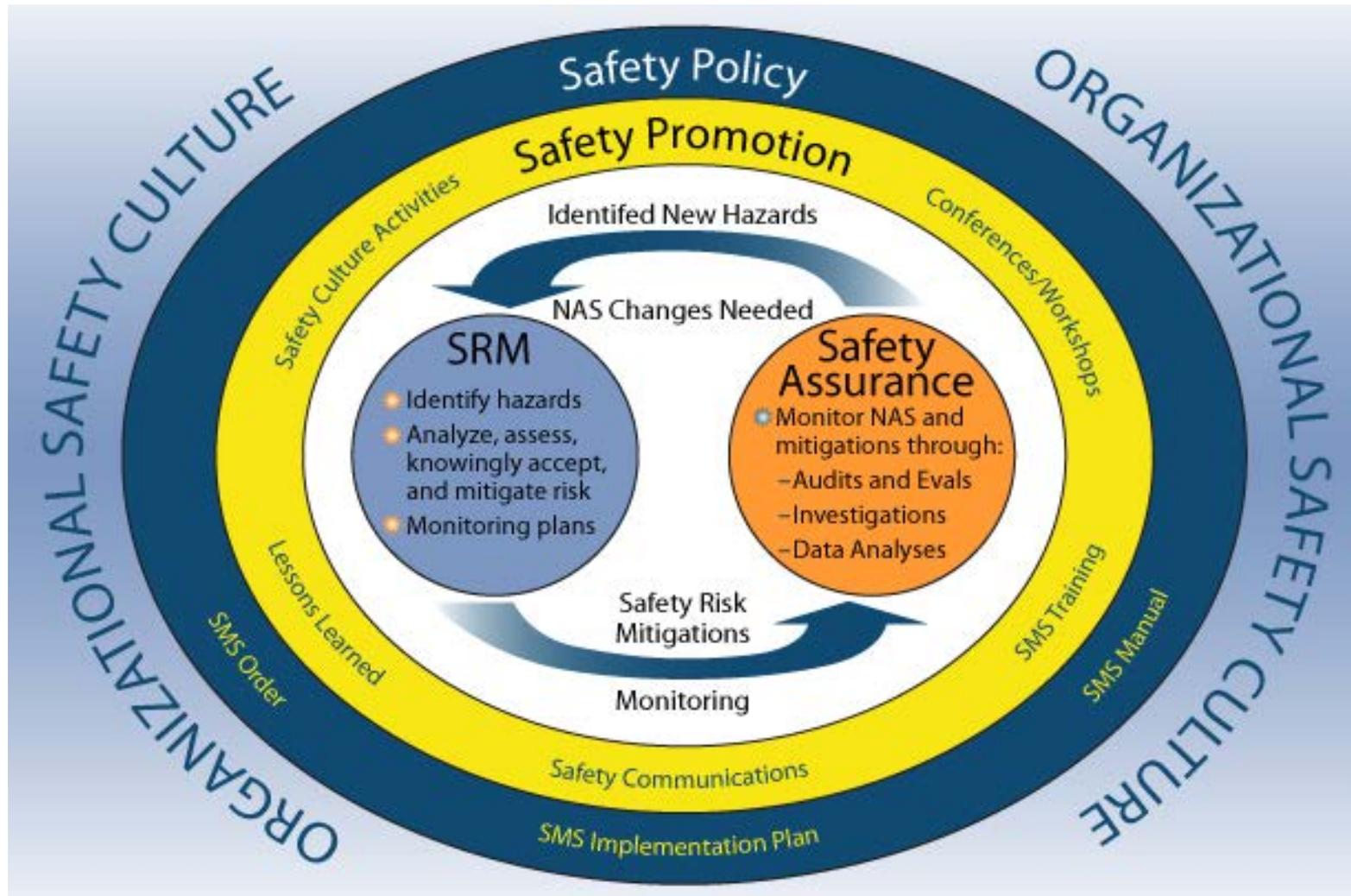
Federal Aviation
Administration



Outline

- **SMS Overview**
- **T&E / V&V in SMS Policy**
- **V&V in Safety Risk Management (SRM)**
 - SRM of Test Activities
- **V&V in Safety Assurance**
- **V&V in Safety Culture**
- **Areas for Improvement**
- **Integrated SRM Concept**
- **Safety Infrastructure Roadmap**

SMS Overview



T&E / V&V in SMS Policy

ATO SMS Manual

- 1.3.3 SMS Products:
 - The SMS builds on, and *must be integrated* into, existing ATO and FAA processes and procedures (e.g., Acquisition Management System (AMS) processes, system safety engineering, *test and evaluation*, facility evaluation and auditing, equipment inspection, and many data collection and analysis programs/systems).
- 3.15.3 Before Implementing a NAS Change
 - Specifically, *the team responsible for the system conducts test and evaluation before implementing a system or a change to the system.* Through verification, the team shows that the system meets its requirements and performs its intended its intended function(s).

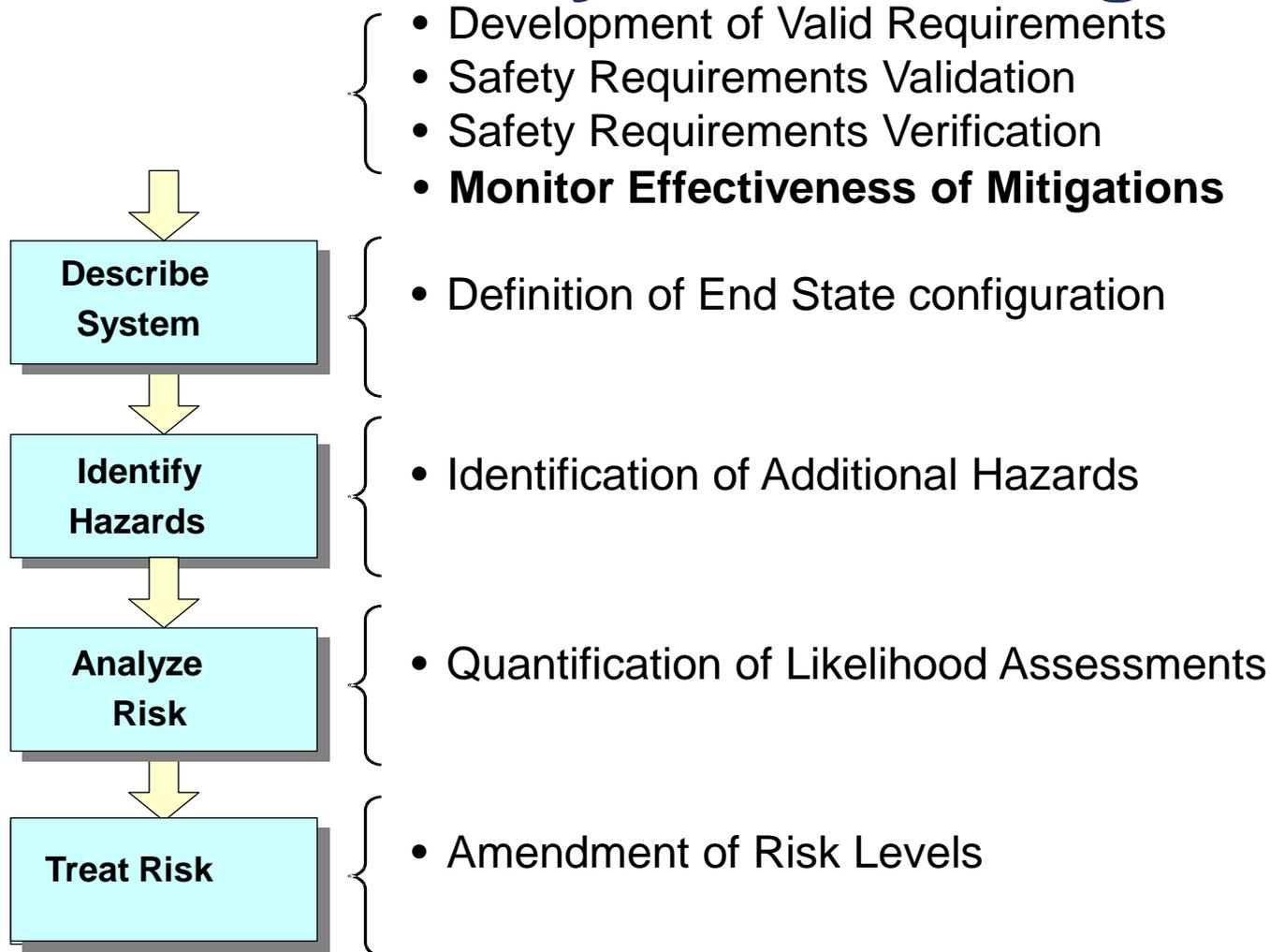
V&V in SMS Policy

Control. Anything that mitigates the risk of a hazard's effects. A control is the same as a safety requirement. All controls are written in requirement language. There are three types of controls:

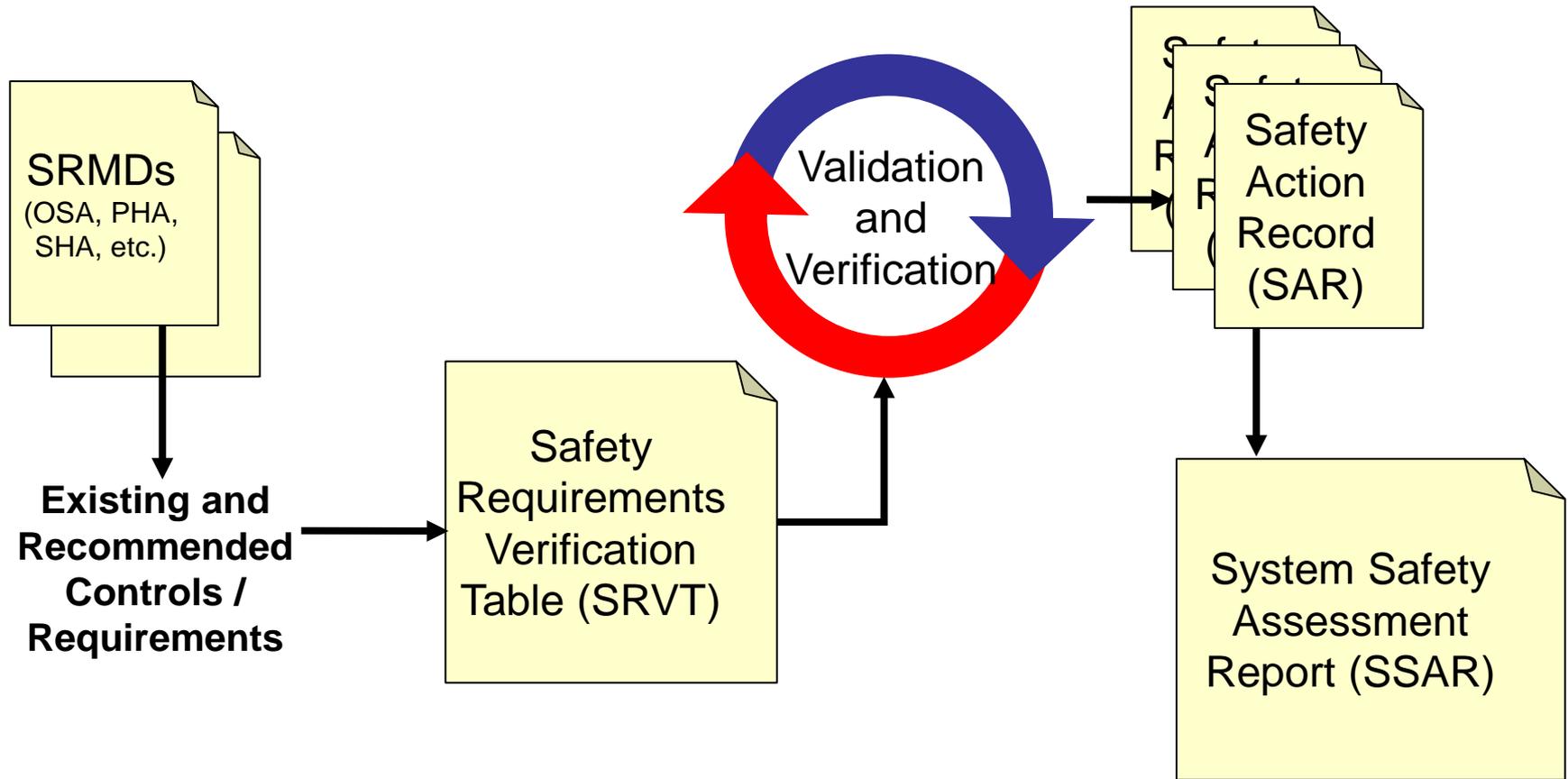
- (1) Validated - Those controls and requirements that are unambiguous, correct, complete, and verifiable.**
- (2) Verified - Those controls and requirements that are objectively determined to have been met by the design solution.**
- (3) Recommended - Those controls that have the potential to mitigate a hazard or risk, but have not yet been validated as part of the system or its requirements.**



V&V in Safety Risk Management (SRM)



V&V in SRM Documentation



Initial Risk

Predicted Risk

Residual Risk

SRM of Test Activities

- **Time is not a determining factor when implementing NAS changes**
- **SRM must be conducted and documented on all tests, demos, and prototypes that touch the NAS**
- **Potential Hazards**
 - Transition issues (where do the barriers exist old vs. new)
 - Mitigations not fully implemented for test or demo
 - Initial Operating Capability (IOC) vs. Initial Service Decision (ISD)
 - Deviations from test plans “What if we....”
 - Leave behinds
- **SRMDMs: Low Safety Effect is not No Safety Effect**

V&V in Safety Assurance

“Audits and evaluations support the essential function of the SMS by ensuring that safety objectives have been met.”



V&V in Safety Culture

Positive Safety Culture Attributes in a V&V Organization

- Employees at all levels understand the hazards and risk inherent in their operations and those with whom they interface.
- V&V activities and procedures are free from program schedule and cost pressures
- Management defines and supports programs aimed at identifying and reporting hazards
- Employees identify gaps in safety process and work to identify revised practices to assure NAS safety

Areas for Improvement

- **Updating SRMDs with information learned from T&E activities “SRMD = SRM Done”**
- **Identification of additional hazards during T&E**
- **Feedback of data from T&E to SRMP and Safety Engineers**
- **Monitoring of controls for effectiveness by organizations other than operational entities**
- **Coordination of V&V with integrated SRM concepts**

Integrated SRM Concept

