



U.S. Department
of Transportation
**Federal Aviation
Administration**

SOC

Safety Oversight Circular

SOC **08-06**
DATE: October 1, 2007

Air Traffic Safety
Oversight Service (AOV)

Subject: ATO Safety Management System (SMS) Definitions

ISSUE: SMS definitions across the FAA are not consistent. This inconsistency demonstrates a lack of coordination within the agency and may cause confusion for the users of the Safety Management System (SMS).

OBJECTIVE: Obtain concurrence from the plenary crosscutting group on the definition of certain frequently used SMS terms.

DISCUSSION: The SMS Crosscutting Working Group established a team to gain concurrence on SMS definitions. The group considered and reviewed terms and definitions listed in the following:

- SRMGSA
- ATO SMS Manual
- AOV SMS Order
- ATO SMS Order
- JPDO SAFETY Standard
- AVS SMS Order
- SEM

The use of each term and its definition was discussed among the group and discrepancies were noted. The discrepancies were then vetted among the group and a common definition was established where possible and a consensus was made when divergent definitions were required to meet specific needs of each organization.

RECOMMENDATIONS: It was agreed that henceforth this list will be used by both ATO and AOV when documenting SMS policy and procedures. ATO and AOV will accept the attached master list of definitions and make changes to the above policy and guidance documents to incorporate them as applicable when each document is next revised or updated. AOV will hold this master list, publish it as a Safety Oversight Circular (SOC), and post the list and SOC on the AOV KSN site.

ATO/AOV Standard SMS Definitions: The following master list is the set of terms that were deemed to be crosscutting by the Definitions Working Group. The group agreed upon the shown Crosscutting Definitions for those terms. Most original

definitions for terms were very similar to each other: changes were made to have unified ATO/AOV definitions.

Term	Crosscutting Definition
Acceptance	The process whereby the regulating organization has delegated the authority to the service provider to make changes within the confines of approved standards and only requires the service provider to notify the regulator of those changes within 30 days. Changes made by the service provider in accordance with their delegated authority can be made without prior approval by the regulator.
Accident	An unplanned event that results in a harmful outcome; e.g., death, injury, occupational illness, or major damage to or loss of property.
Approval	The formal act of responding favorably to a change submitted by a requesting organization. This action is required prior to the proposed change being implemented.
Assumptions	Characteristics or requirements of a system or system state that are neither validated nor verified.
Cause	Events that result in a hazard or failure. Causes can occur by themselves or in combinations.
Configuration Management	A management process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.
Control	Anything that mitigates the risk of a hazard's effects. A control is the same as a safety requirement. All controls must be written in requirement language. There are three types of controls:
Validated Control	Those controls and requirements that are unambiguous, correct, complete, and verifiable.
Verified Control	Those controls and requirements that are objectively determined to have been met by the design solution.
Recommended Control	Those controls that have the potential to mitigate a hazard or risk, but have not yet been verified as part of the system or its requirements.
Effect	Effect. The effect is a description of the potential outcome or harm of the hazard if it occurs in the defined system state.
Hazard	Any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a condition that is a prerequisite to an accident or incident.
Incident	A near miss episode, malfunction, or failure with minor consequences that could have resulted in greater loss. An unplanned event that could have resulted in an accident, or did result in minor damage, and indicates the existence of, though may not define, a hazard or hazardous condition.
Maintenance	Any repair, adaptation, upgrade, or modification of National Airspace System (NAS) equipment or facilities. This includes preventive maintenance.
National Airspace System	National Airspace System: Is comprised of airspace; airports; aircraft; pilots; air navigation facilities; air traffic control (ATC) facilities; communication, surveillance, navigation, and supporting technologies and systems; operating rules, regulations, policies, and procedures; and the people who implement, sustain, or operate the system components.
Oversight	To validate the development of a defined system and verify compliance to a pre-defined set of standards; Regulatory Supervision.

Process	A set of interrelated or interacting activities which transforms inputs into outputs.
Requirement	An essential attribute or characteristic of a system. It is a condition or capability that must be met or passed by a system to satisfy a contract, standard, specification, or other formally imposed document or need.
Risk	The composite of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state.
Initial Risk	The composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the risk at the preliminary or beginning stage of a proposed change, program or assessment
Current Risk	The predicted severity and likelihood of a hazard at the current time. When determining current risk, both validated controls and verified controls may be used in the risk assessment. Current risk may change based on the actions taken by the decision-maker that relate to the validation and/or verification of the controls associated with a hazard.
Residual Risk	The risk that remains after all control techniques have been implemented or exhausted and all controls have been verified. Only verified controls can be used to assess residual risk.
Safety Council	A forum for top management officials from AOV and the ATO Safety Service to meet and discuss noncompliance and other safety issues in an attempt to resolve those issues.
Safety Culture	Safety Culture: The product of individual and group values, attitudes, competencies, and patterns of behavior that determine commitment to, and the style and proficiency of, an organization's Health and safety management. In addition, the four key components of a safety culture are reporting culture (encourage employees to divulge information about all hazards that they encounter), just culture (employees are held accountable for deliberate violations of the rules but are encouraged and rewarded for providing essential safety-related information), flexible culture (to adapt effectively to changing demands and allow quicker, smoother reactions to off-nominal events), and learning culture (willing to change based on safety indicators and hazards uncovered through assessments, data, and incidents).
Safety Directive	A mandate from AOV to ATO to take immediate corrective action to address a noncompliance issue that creates a significant unsafe condition.
Safety Requirement	A control written in requirements language.
System	An integrated set of constituent pieces that are combined in an operational or support environment to accomplish a defined objective. These pieces include people, equipment, information, procedures, facilities, services, and other support services.
System State	An expression of the various conditions, characterized by quantities or qualities, in which a system can exist.
Verification	The process that ensures that the system requirements have been met by the design solution and the system is ready to be used in the operational environment for which it is intended.

The following list is a set of definitions that were deemed to be cross-cutting by the Definitions Working Group. However, the group agreed that the current definitions, while different, were similar enough not to cause issues.

Term	ATO Definition	AOV Definition
Safety Management System	An integrated collection of processes, procedures, policies, and programs that are used to assess, define, and manage the safety risk in the provision of ATC and navigation services.	An integrated collection of processes, procedures, and programs that ensures a formalized and proactive approach to system safety through risk management. Risk analysis and assessment are required for all changes to identify safety impacts. The SMS is a closed-loop system ensuring all changes are documented and all problems or issues are tracked to conclusion. When properly implemented, an SMS establishes a safety philosophy or culture that permeates the entire organization in the monitoring and continuous improvement of safety of the operation.
Safety Risk Management	A formalized, proactive approach to system safety. SRM is a methodology applied to all NAS changes that ensures that hazards are identified and unacceptable risk is mitigated prior to the change being made. It provides a framework to ensure that once a change is made, it continues to be tracked throughout its lifecycle.	A process within the SMS composed of describing the system, identifying hazards, and analyzing, assessing, and controlling the risk.
Validation	The process of proving that the right system is being built, i.e., that the system requirements are unambiguous, correct, complete, and verifiable.	The process of proving that the functions, procedures, controls, and safety standards are correct and the right system is being built (i.e., the requirements are unambiguous, correct, complete, and verifiable).



Anthony S. Ferrante
Director, Air Traffic Safety Oversight Service