FAA Safety Management Systems
Aviation Rulemaking Committee
(SMS-ARC)

Design and Manufacturing
Working Group (D&M) Report
High-Level Recommendations for SMS Requirements

March, 12, 2010

TABLE OF CONTENTS

SECTION 1: Introduction

This report contains the comments and high-level recommendations of the FAA Safety Management Systems Aviation Rulemaking Committee (SMS-ARC) Design & Manufacturing Working Group (D&M) for rulemaking in developing and implementing SMS requirements.

1.1 SMS-ARC Background

The Federal Aviation Administration (FAA) Order 1110.152 effective February 12, 2009 established the charter for a Safety Management Systems Aviation Rulemaking Committee (SMS-ARC) tasked to provide recommendations for rulemaking, processes, policies and guidance to FAA in developing and implementing broadly applicable SMS requirements for aviation service providers such as manufacturers, operators, repair stations, and training organizations. The FAA has appointed association representatives to serve as members of the SMS-ARC and named tri-chairs from a manufacturer, operator, and labor organization to best represent the broad industry that would be affected by an SMS rulemaking proposal. The SMS-ARC established working groups comprised of industry and government subject matter experts (SME) to provide recommendations, advice and guidance to the ARC in the areas of Design & Manufacturing, Operations & Training, and Maintenance. The SMS-ARC held a meeting on September 30 – October 1, 2009 to establish the working group tasking and deliverables.

1.2 Design & Manufacturing Working Group Tasking & Report

The SMS-ARC Design & Manufacturing Working Group (D&M) membership is comprised of a diverse group of individuals with expertise in aviation product safety and related subject matter areas representing organizations regulated under FAR Part 21 for the design and manufacture of type certificated aircraft and engines, approved avionics articles and systems, and association representatives on behalf of general aviation and modification and replacement part manufacturers; and contributors from the Federal Aviation Administration (FAA) Aircraft Certification Service (***Appendix A***).

The D&M was tasked by the SMS-ARC to develop a report which provides comments and high-level recommendations for rulemaking in developing and implementing SMS regulatory requirements (including minority position if required). The tasking statement required the D&M to complete the following:

- **Review Comments to SMS ANPRM** – Review public comments to the SMS ANPRM and develop a high-level summary of industry sector responses to identify key issues, concerns, and any recommendations regarding SMS requirements.
- **Perform Gap Analysis and Exceptions Assessment** – Perform a gap analysis between FAA Order 8000.367, Appendix B SMS requirements for service providers and current regulations and standards for Part 21 design and production approval holders. The analysis should identify the extent to which the intent of each requirement is met and can also identify potential exceptions where they may be impractical or not applicable for each type and/or size of certificate/approval holder organization.

- **Develop a Report on High-Level Recommendations for SMS Requirements** – With consideration of the gap analysis, exceptions assessment and ANPRM comments, develop a report which provides high-level recommendations for SMS requirements that address the following FAA questions:
  - Should the FAA issue regulations on SMS? Why or why not?
  - If so, who should SMS regulations apply to? Why and why not?
  - What should the SMS regulations address? (describe general concepts)
  - What should the guidance material address? (describe general concepts)
  - Explanation of the SMS-ARC working group recommendations
    - Justification (reasoning) for rule change
    - Explanation of benefits
    - Explanation of Costs
    - Harmonization with international standards

Review of Comments to SMS ANPRM

The D&M reviewed the Safety Management System ANPRM Comment Summary prepared by the Regulatory Group (dated November 20, 2009) and developed a high-level summary of the design and manufacturing industry sector responses to identify key issues, concerns, and any recommendations regarding SMS requirements (***Appendix B***).

The majority of commenters in the design and manufacturing community expressed concern over the potential cost and resource burden of SMS regulatory requirements. Many organizations believe they already have robust internal safety programs and that SMS regulations could introduce a significant burden in administration and documentation, without providing a commensurate safety benefit. They suggested many approaches to mitigating this burden including conducting a gap analysis to existing regulations and ensuring that SMS requirements are kept at a high level, non prescriptive, and flexible to allow the use of existing safety systems and company processes in showing compliance. Also, SMS requirements must be scalable to accommodate small to large and simple to complex organizations and various business arrangements. In order to accomplish this, ANPRM commenters recommended pilot SMS implementation programs to develop experience with application of SMS to Design and Manufacturing organizations.

The commenters also expressed concern over protection of safety data, risk assessments and safety decisions from lawsuits and from loss of intellectual property rights and recommended that statutory protection would be required.

Gap Analysis and Exceptions Assessment

The D&M performed a gap analysis between existing regulatory requirements for design and production approval holders and SMS requirements of both the ICAO SMS Framework and FAA Order 8000.367, Appendix B. Current Part 21 and airworthiness regulatory requirements regarding product safety address most SMS elements to various degrees. The greatest gaps between requirements exist with respect to organizational factors and SMS Safety Policy and Safety Promotion elements because FAA does not have organizational requirements for design approval holders like it does with Production approval holders, repair station certificates and air

carrier operating certificates. However, most design/production approval holder organizations have existing mature and effective safety systems and company processes that considerably exceed Part 21 regulatory requirements such as certification processes, quality management systems, internal audit quality assurance programs and continued operational safety programs.

The following appendices provide the D&M's gap analyses documents which includes side-by-side comparision along with comments representing an overall assessment of findings, the extent to which the intent of requirements are met, and exceptions where they may be impractical or not applicable:

Appendix C: Regulatory Gap Analysis – Executive Summary
Appendix D: Gap Analysis: Part 21 Design and Order 8000.367 Appendix B Requirements
Appendix E: Gap Analysis: Part 21 Manufacturing and ICAO SMS Framework Requirements
Appendix F: Gap Analysis: Extent to Which Part 21 D&M Addresses SMS Framework

D&M Report on High-Level Recommendations for SMS Requirements

This report contains the comments and high-level recommendations of the D&M for rulemaking in developing and implementing SMS requirements. It was developed with consideration of the ANPRM comments and gap analyses summarized above. **Section 2 of this report provides the D&M's comments and high-level recommendations in response to the FAA questions**. Section 3 of this report provides a summary list of the high-level recommendations contained within the body of the report along with some additional recommendations on future tasks for the D&M necessary to support future development and implementation of SMS requirements for design and manufacturing organizations.

SECTION 2: Comments in Response to FAA Questions

This section of the report provides the D&M's comments and high-level recommendations for SMS regulatory requirements structured in response to the following FAA questions:

- Should the FAA issue regulations on SMS? Why or why not?
- If so, who should SMS regulations apply to? Why and why not?
- What should the SMS regulations address? (describe general concepts)
- What should the guidance material address? (describe general concepts)
- Explanation of the SMS-ARC working group recommendations (justification, benefits, costs, harmonization with international standards)

2.1 Should the FAA issue regulations on SMS?

FAA is considering new broadly applicable regulation that would require SMS for certain design and production certificate/approval holders and applicants. The SMS-ARC Design and Manufacturing Work Group (D&M) members recognize and endorse the foundational principles and concepts of SMS and consider them generally applicable to all civil aviation product and service providers, and in fact to any organization with safety risk exposure, and thus a need for effective organizational safety risk management. The D&M believes there is potential safety benefit to civil aviation and the air transportation system that could be realized as the result of consistent SMS requirements in the form of a single broadly applicable regulation.

With respect to applicability to Part 21 design and manufacturing organizations, the D&M believes that it is necessary for the FAA to implement SMS requirements that meet the ICAO Annex 8 SMS standard in order to support the global nature of U.S. aviation manufacturer activities and to facilitate reciprocal international acceptance of U.S. state of design and/or manufacturer SMS programs. However, the D&M has identified several key concerns for the design and manufacturing sector that must be addressed in order to achieve success from both a regulator and industry perspective, and to avoid unnecessary administrative burdens without commensurate safety benefit.

The D&M supports consideration of SMS requirements applicable to certain design and manufacturing organizations provided the following key issues are addressed:

- **International Harmonization and Reciprocal Acceptance** – The regulations should be harmonized internationally and there must be reciprocal acceptance of Safety Management Systems
- **Phased Promulgation of SMS regulations** – Promulgation of SMS rulemaking needs to be phased to provide for development of appropriate industry sector-specific requirements and applicability and development of necessary FAA guidance
- **Phased Implementation of SMS Requirements** – Regulations would accommodate phased implementation of SMS elements.
- **Recognize Existing Systems and Processes** – The regulations must provide for acceptance of existing effective safety programs and company processes which are already in place

- **Recognize Certification Procedures and Airworthiness Requirements** - Part 21 certification procedures and airworthiness requirements are prescribed by regulation and can not be changed by SMS requirements and processes
- **Scalability and Flexibility** – The regulations must accommodate a broad range of organizations from small parts manufacturers to large organizations holding multiple types of certificates/approvals and various business arrangements
- **Protection of SMS Safety Information** – There must be protection of safety information from disclosure and use for other purposes
- **FAA Plan for D&M Sector SMS Oversight Activity** – FAA must ensure sufficient planning and workforce training to accommodate efficient and timely assessment and oversight of SMS which is significantly different than current certification compliance activities
- **Alternatives to SMS Implementation Through Regulation** – FAA should consider alternatives to SMS implementation through regulation such as industry consensus standards and voluntary programs which may be more appropriate and effective for certain industry sectors

International Harmonization and Reciprocal Acceptance

Many organizations in the design and manufacturing sector are affected by regulations of multiple State civil aviation authorities. Proliferation of multiple, slightly differing SMS standards could force organizations to accomplish redundant compliance demonstrations and to develop and maintain redundant documentation for compliance, all without benefit to system effectiveness. The D&M recommends that FAA work with ICAO and with other State regulatory authorities to ensure a coordinated and harmonized approach to implementation of SMS requirements to facilitate reciprocal acceptance of SMS programs of the State of design and State of manufacture. FAA should also update bilateral aviation safety agreements to include specific provisions regarding reciprocal acceptance of manufacturer SMS. This is necessary to prevent or minimize any unique, individual State regulatory differences that will drive costly compliance efforts with no measurable improvement in safety.

FAA SMS requirements should be consistent with the ICAO SMS framework to facilitate harmonization and reciprocal acceptance by aviation authorities throughout the world. The preamble of proposed SMS requirements should include discussions on how it meets or is equivalent to the ICAO SMS Framework, particularly where the language may be different.

Phased Promulgation of SMS Regulations

The D&M recommends that new SMS requirements be adopted through phased rulemaking promulgation to build industry sector-specific experience and understanding and provide for the development of appropriate requirements and determination of appropriate applicability and phased implementation. Promulgation of new regulation should start with the basic SMS framework in a single new CFR Part along with appropriate FAR Part industry sector-specific requirements for initial applicability and implementation of SMS. The D&M recognizes that ICAO Annex 6 Part 1 required FAA to implement SMS for certain commercial air carriers by 2009 and that initial applicability would be most appropriate for Part 121 air carriers.

Subsequent rulemaking would include applicability in the other Annex 6 intended CFR Parts, including Parts 91, 135, 145, 142, etc.

ICAO, with technical support from national aviation authorities including FAA, invested several years developing SMS standards including a Safety Management Manual which provides guidance for the development and implementation of SMS requirements upon operating organizations such as air carriers, airports and air traffic providers. In addition, FAA Flight Standards has been working for years on SMS for operators including guidance information introducing SMS to operator organizations (AC 120-92, June 2006) as well as large scale pilot project implementation with several air carriers which have resulted in the development of detailed reference documents on an SMS Framework, SMS Implementation Guide, SMS Assurance Guide, and SMS Gap Analysis Tools for the development and implementation of SMS within an air carrier organization. There is a significant body of knowledge and practical experience regarding the development and implementation of SMS within an air operating organization that is very important in support of developing possible regulatory requirements. The D&M strongly recommends that FAA also work closely with design and manufacturing organizations through a pilot program to collaboratively develop a common understanding of how SMS could best be applied to support the development of appropriate requirements and implementation guidance.

Development of a Part 21 proposed rule requiring SMS applicability to certain design approval holders (DAH) and production approval holders (PAH) can not occur until FAA and industry have a better understanding of how SMS can be implemented within existing organizations and established processes in an effective and efficient manner. FAA Flight Standards pilot programs working with several air carriers and repair stations on voluntary implementation of SMS provided significant experience necessary to refine SMS standards and develop implementation tools and guidance for both industry and FAA. The D&M recommends that development of a proposed rule for applicability of SMS within Part 21 occur only after sufficient implementation experience within the design and manufacturing sector through an FAA sponsored pilot program, as well as development of workable sector-specific industry standards and FAA guidance material.

ICAO Annex 8 currently states that each State of design or manufacture shall require that an organization responsible for the type design or manufacture of aircraft implement a safety management system by November 2013. The need for phased promulgation of SMS requirements as discussed above means that it would not be practical nor even possible for the U.S. to meet this ICAO timeline. Considering the status of SMS requirements and implementation by other regulatory authorities such as EASA, the D&M believes that most ICAO member States will not be able to meet the 2013 date. D&M recommends that FAA work through ICAO to amend Annex 8 standards to establish an appropriate and realistic date for States' to implement SMS requirements for organizations responsible for the type design or manufacture of aircraft.

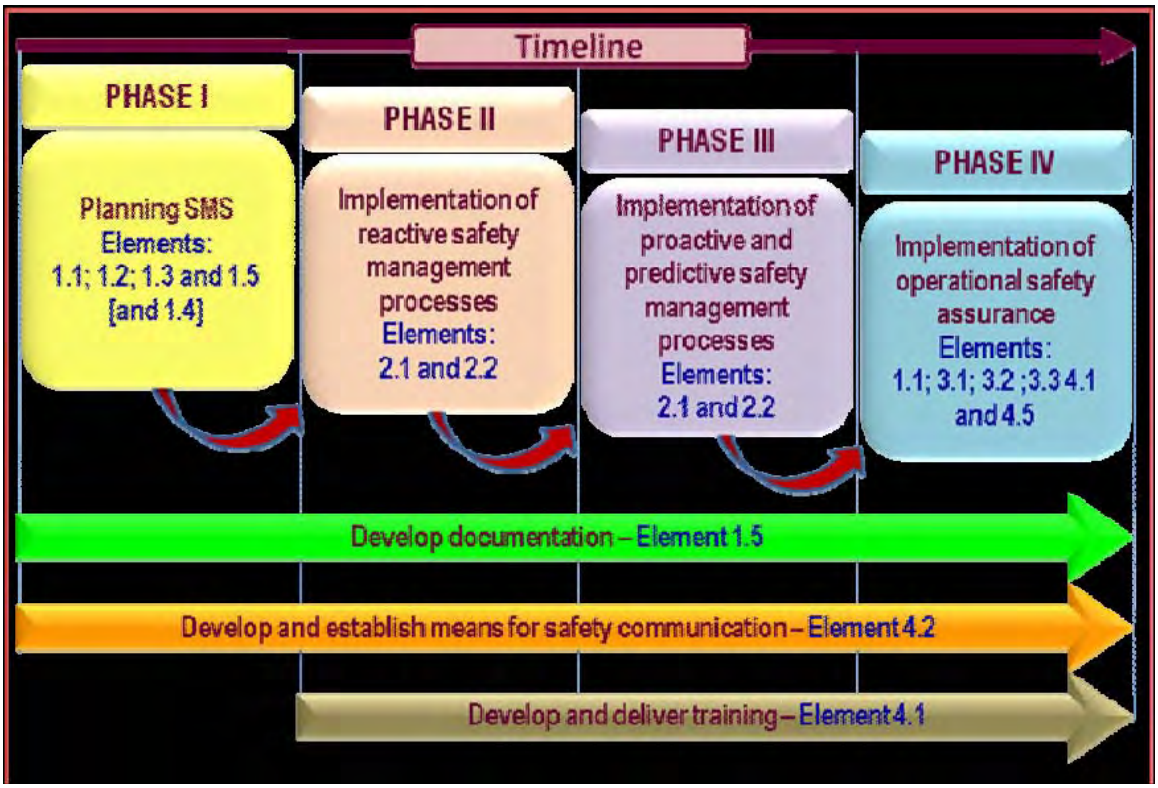
Phased Implementation of SMS Requirements

Regulatory compliance expectations for certificate holders in all sectors should include reasonable time for phased implementation and increasing system maturity. Implementation phasing within design and manufacturing sector organizations should allow sufficient time to

avoid unnecessary resource burdens, and accommodate internal schedule limitations such as type certification programs and documentation revision cycles. System maturation should start with areas with the most potential leverage for safety improvement. For design and manufacturing organizations, the SMS should first address basic processes focused on product performance. For example, a robust continued operational safety process which would mature to include feedback of systemic corrections to the design process. Proactive or predictive efforts to address organizational or contributing factors as hazards in a design or manufacturing environment are more difficult to apply effectively since there is no direct correlation to product attributes, and no industry standard for application. This area requires additional industry study to enable effective, efficient implementation, and therefore should be addressed last.

The ICAO Safety Management System Manual (Chapter 10) provides the rationale and recommendations for implementing Safety Management Systems using a phased-in approach for the variety of SMS program elements. The graphic below summarizes the ICAO recommended phased-in approach. ICAO emphasizes that "the timeline for the implementation of each phase shall be commensurate with the size of the organization and complexity of the services provided." Phased implementation of SMS requirements provides;

- a manageable series of steps to follow in implementing an SMS, including allocation of resources;
- effectively managing the workload associated with SMS implementation; and
- pre-empting a "ticking boxes" exercise.



The ICAO SMS Manual Chapter 10 and two related Appendices provide a detailed phased-implementation plan for SMS. Transport Canada has adopted the phased-in approach to implementing its SMS regulations which is summarized in ***Appendix G***.

Recognize Existing Systems and Processes

Many aviation design and manufacturing organizations have existing, mature and effective safety systems/programs and company processes such as Quality Management System (QMS), internal audit quality assurance programs, continued operational safety programs, and certification processes consistent with existing regulations. Implementation of SMS should complement and enhance those effective systems, and not add unnecessary burden that does not have commensurate safety benefit. The D&M Working Group conducted a gap analysis to assess existing regulations against the ICAO SMS framework and Order 8000.367, Appendix B which determined that existing Part 21 and airworthiness requirements for product safety address most SMS elements to various degrees. The following appendices provide the D&M's gap analyses documents which includes side-by-side comparison along with comments representing an overall assessment of findings, the extent to which the intent of requirements are met, and exceptions where they may be impractical or not applicable:

Appendix C: Regulatory Gap Analysis – Executive Summary
Appendix D: Gap Analysis: Part 21 Design and Order 8000.367 Appendix B Requirements
Appendix E: Gap Analysis: Part 21 Manufacturing and ICAO SMS Framework Requirements
Appendix F: Gap Analysis: Extent to Which Part 21 D&M Addresses SMS Framework

Many design and manufacturing organization's safety systems/programs and company processes considerably exceed the regulatory requirements and thereby provide a very solid foundation for efficient SMS implementation. SMS regulations and guidance for design and manufacturing organizations must be flexible enough to allow for the recognition of existing systems and company processes as acceptable methods of compliance to SMS requirements, to the maximum extent possible.

Recognize Certification Procedures and Airworthiness Requirements

FAA must prescribe minimum standards required in the interest of safety for the design, material, construction, quality of work, and performance of aircraft, aircraft engines, and propellers (49 USC 44701). FAR Part 21 establishes procedural requirements for the issue of type certificates and design approvals (and changes to those certificates/approvals); the issue of production certificates and production approvals and rules governing the holders of these certificates/approvals. Part 21 also prescribes the designation of applicable regulations and minimum airworthiness standards for the issuance of a design approval within each product category (i.e. Parts 23 and 25 for airplanes, 27 and 29 for rotorcraft, 33 for engines, 35 for propellers, etc). This includes regulatory procedures for the establishment of special conditions and continuing airworthiness and safety improvements when the FAA finds that existing regulations do not contain adequate or appropriate safety standards. It would not be appropriate for an SMS to affect the applicability and acceptability of certification procedures and airworthiness requirements for the issuance of a design approval which have been established through public rulemaking and administrative procedures as this would be extremely burdensome, arbitrary and capricious. The D&M recommends that FAA clearly state that SMS can not change applicable regulatory requirements and the level of safety established in the regulations.

Scalability and Flexibility of SMS Requirements

Any FAA regulatory and/or guidance material must be scalable to accommodate a broad range of organizations including small to large, multi-certificated organizations and various business arrangements. In addition, as discussed above on recognizing existing company safety systems/programs and processes, regulatory and guidance material must be flexible enough to allow company processes and "best practices" to support compliance with SMS requirements. To achieve this, the D&M believes the SMS regulatory language must necessarily be simple, efficient, non prescriptive and performance-based with a clear objective.

Protection of SMS Safety Information

To enhance aviation safety by using safety risk management, there must be a free flow of safety ideas and information within certificate holders, between certificate holders and the authorities, and throughout the industry responsible for design, manufacture, maintenance and operation of aircraft.

The development, documentation and availability of safety ideas and information may be inhibited by

- threats of out-of-context exposure through the media
- threats of use of such data as admissions in criminal or administrative litigation
- threats of use of such data in civil litigation

Inhibition on the flow of safety information conflicts with the objectives of a safety management system. Among other things, this may result in warnings not to commit certain thoughts to writing or sharing of certain information, which may mean that important data is lost. This means that certain risks/hazards may not be pursued. In addition, the understanding of risk gained from concatenation of such data may not occur.

Implementation of a safety management system can only be successful if safety information is protected from inappropriate use. There is no SMS without the development, documentation and sharing of safety information. Protection is essential to ensure the availability of such information to enhance safety.

The D&M recommends that FAA seek to have Congress protect Safety Management Systems information from disclosure through discovery and/or FOIA in the United States. ***Appendix H*** provides sample legislative language for protection of aviation safety information which is modeled after 49 USC 1154 on discovery and use of cockpit and surface vehicle recordings and transcripts.

In addition, the D&M recommends that the FAA work through ICAO to expand ICAO Assembly Resolution on protecting safety data (Resolution A 35/17) to specifically include Safety Management Systems information.

FAA Plan for D&M Sector SMS Oversight Activity

The FAA must ensure sufficient planning and capability to accommodate efficient and timely SMS regulatory compliance-finding activities for D&M sector organizations to meet implementation dates while continuing to support ongoing production and product certification activities, and continued operational safety activities. The implementation, assessment and oversight of an SMS for design approval holder organizations will be particularly challenging for both industry and FAA. The type certification process is a series of discreet showings and findings of compliance between the DAH applicant and FAA ACO (and its designees). FAA assessment and oversight of a systems approach to safety management will require a significant change in existing interaction processes between design applicants and FAA Aircraft Certification Offices as well as a cultural shift for the individuals involved.

FAA should develop training and guidance for FAA personnel involved in DAH/PAH SMS assessment and oversight to ensure that eventual SMS regulation, if adopted, does not result in unnecessary and undue regulatory compliance burden, and ensure implementation and oversight activity is efficient and equitable / fair so as not to interfere with competitive business models.

Alternatives to SMS Implementation Through Regulation

The D&M recommends that FAA consider alternatives to SMS implementation through regulation such as industry consensus standards and voluntary programs which may be more appropriate and effective for certain industry sectors. One alternative would be implementation through a combination of (1) recognition of those elements of SMS already existing in the FAA regulations and (2) implementation of those elements missing from the existing regulations through a voluntary compliance system that would be audited under FAA guidelines (These missing elements have been identified by the D&M in the enclosed gap analysis). Such “missing elements” could be published as an industry standard that could be used as the basis for implementation of SMS standards with minimal FAA resource allocation.

The FAA has already relied in the past on accreditation schemes in order to implement programs designed to improve safety beyond existing standards. FAA §21.190 provides for the issue of a special airworthiness certificate for a light-sport category aircraft designed and manufactured to industry consensus standards (published by ASTM). The FAA’s AC 00-56A Voluntary Industry Distributor Accreditation Program is published in an advisory circular and not in the regulations. Compliance with the program is monitored by third party assessments, and is supplemented by popular programs like ASA-100 and ISO 9000 (AS 9100 is a corollary accreditation program for production quality management systems). By utilizing third party auditors who are subject to FAA oversight and industry standards subject to FAA approval, there have been improvements in aviation safety with a minimal implementation and oversight burden on industry and FAA.

There are numerous other examples voluntary programs that are effective without regulatory enforcement which have shown that voluntary guidelines can have a significant effect on an industry in order to promote change. And the benefit of these voluntary guidelines is that it is significantly easier to design a program that is targeted to meeting the program’s goals (like aviation safety improvement through risk-based assessments) when the system is flexible enough to permit the company to develop new ideas with the support of a government agency while minimizing regulatory compliance burden.

2.2 If so, who should SMS regulations apply to?

The FAA, in conjunction with industry, must precisely determine the extent of new SMS requirements applicability in the design and manufacturing sector. In addition, new requirements must also address issues such as transition/grandfathering provisions for existing design certificate/approval holders of 'orphaned' aircraft, civil certificated aircraft in military service, out of production aircraft models, limited in service fleets as well as modifications and component/parts installed thereon. Properly scoped applicability provisions in the rule will significantly reduce the burden of implementation and oversight on both industry and FAA while maximizing the safety benefit of SMS. In addition, several questions were raised regarding FAA's statutory legal authority and regulatory issues regarding imposition of new SMS requirements upon design organizations.

SMS Requirements Should Apply to Certain Design/Production Approval Holders

The design and manufacturing industry sector includes a very broad range of private individuals and organizations that hold the following design and production certificates/approvals:

- Design Approvals
  - Type Certificates (TC) for aircraft, aircraft engines and propellers
  - Supplemental Type Certificates (STC) for changes to TC
  - Parts Manufacturing Approval (PMA) for modification and replacement parts
  - Technical Standard Order Authorization (TSOA) for articles (materials, parts, processes, or appliances) used on civil aircraft
- Production Approvals
  - Production Certificate (PC) for the manufacture TC/STC products and parts installed thereon
  - Parts Manufacturing Approval (PMA) for manufacture of modification and replacement parts
  - Technical Standard Order Authorization (TSOA) for manufacture of articles (materials, parts, processes, or appliances) used on civil aircraft

The D&M believes that SMS requirements should apply to certain design/production approval holders. However, the D&M considers that there are entities upon which imposition of SMS regulations would be ineffective or of limited benefit and overly burdensome. Because SMS implementation in the Design and Manufacturing sector is not yet well understood, and given the limited time available to respond to this initial tasking, the D&M is not able to provide a recommended definition or scope of those entities that SMS requirements should apply. SMS regulations pertaining to design and/or manufacturing organizations should not be promulgated unless and until the following issues related to applicability are resolved in collaboration with industry:

1. What are the criteria to be used for determination of whether an organization should be excluded from SMS requirements? Both industry and FAA must understand whether and how to impose SMS requirements on small organizations, organizations responsible for out-of-production aircraft or small fleet sizes, holders of Restricted Category Type Certificate(s), and aircraft used in commercial vs non-commercial operations.

2. For any organization subject to SMS regulation, how and using what criteria should SMS be scaled?
3. D&M does not recommend that SMS apply to suppliers/vendors that do not independently hold a certificate or approval.
4. Should FAA SMS regulations apply to a holder of a certificate or approval for a product used exclusively in military or other public use service?
5. What does "SMS interoperability" mean? How should SMS interoperability and flow of information be accomplished among organizations (some of which might not be required to have SMS) related to the same product, e.g., the manufacturer, suppliers/vendors to the manufacturer, operators, and maintainers of a product?

Statutory Legal Authority Issues: SMS Requirements Upon Design Organizations

Several questions were raised regarding the FAA's statutory legal authority to issue regulations imposing new SMS requirements upon design organizations that hold a Type Certificate or design approval. With respect to aviation organizations, the Statutes specifically direct FAA to prescribe regulations and minimum standards for the issuance of Production Certificates (PC), Design Organization Certificates (CDO), Air Carrier Operating Certificates, Airport Operating Certificates, and Air Agency Certificates for flight/maintenance schools and repair stations authorizing them with privileges to perform specified functions and to include "terms required in the interest of safety" [49 USC 44702, 44704-44707]. Therefore, FAA clearly has statutory legal authority to issue regulations imposing new requirements upon these certificated production, design, air carrier, and repair station organizations.

However, current statutes do not require the applicant for or holder of a type certificate or design approval to meet any "terms required in the interest of safety" nor any minimum technical or organizational qualification or criteria. As such, FAA regulations state that any interested person may apply for (21.13) and is entitled to (21.21) a type certificate if the product design meets the applicable airworthiness requirements and that it may be transferred to any other person (21.47). Therefore, current holders of type certificates or design approvals include a very broad range of aviation manufacturers as well as non-aviation organizations (i.e. trusts, banks, insurance companies, law firms) and private individual persons who may not be a design organization nor exercise the privileges of the type certificate. Therefore, several questions remain regarding the FAA's statutory legal authority to issue regulations imposing new SMS requirements upon holders of a Type Certificate or design approval that may not be a design organization and whether retroactively imposing new SMS requirements upon such existing holders would be arbitrary and capricious because it would essentially require them to surrender their type certificate or design approval and intellectual property rights.

FAA has not yet promulgated regulations implementing its statutory authority to issue Design Organization Certificates (CDO) which would be applicable to organizations seeking privileges to certify compliance with requirements and minimum standards for the issuance of a TC. The FAA CDO-ARC provided recommendations to FAA for the establishment of CDO which includes SMS as a core requirement.

Regulatory Issues: SMS Requirements Upon Design Organizations

Several questions were raised whether the existing Part 21 regulatory structure allows for the practical implementation of new SMS requirements upon design organizations that hold a Type Certificate or design approval. Current Part 21 regulations allow any person to hold a type certificate, without stipulating management structure or organization requirements. Type certification addresses product definition and compliance with airworthiness standards, but does not establish any minimum requirements for the holder of a type certificate. However, there are examples of current regulations which impose requirements upon the applicant and holder of a type certificate/design approval that could serve as a model for prescribing new SMS requirements. These include §21.3, §21.50, §21.99 and Part 26 requirements which are discussed in the table below.

Another model for application of SMS requirements upon certain design approval holders is for FAA to establish minimum requirements for design organizations and formal recognition and oversight through the issuance of design organization certificate (CDO) or approval. A CDO-ARC has submitted recommendations to FAA for the establishment of a CDO with minimum standards for organizational management systems, capability and documented procedures including a specific requirement for SMS. However, application for CDO would be strictly voluntary for those design organizations that meet the minimum requirements and believe it would provide a benefit commensurate with the additional regulatory burden.

From an international perspective, both EASA and Transport Canada have prescribed regulatory requirements for applicants and holders of type certificates/design approvals establishing minimum standards for the design organization's procedures and capability and that any new SMS requirements would be applicable to these approved design organizations.

The following table provides a summary of different approaches that could be considered for the application of any proposed new SMS requirements upon design and production organizations.

Applicability	Requirement	Pros/Cons
Type Certificate	▪ SMS as an airworthiness requirement and condition for continued eligibility ▪ Part 39Airworthiness Directive ▪ Part 26 retroactive requirements for continued airworthiness and safety improvement	▪ Pro: none ▪ Con: Can not apply management system organizational requirements to a design approval
Holder of a TC	▪ 21.3 reporting of failures, malfunctions and defects ▪ 21.50 make ICA and changes thereto available (only applicable to TC for which application was made after January 1981) ▪ 21.99 required design changes (airworthiness requirement to maintain eligibility of TC required when AD is issued) ▪ Part 26 retroactive requirements for continued airworthiness and safety improvement (airworthiness	▪ Pro: Holders are readily identifiable for each TC ▪ Con: Holders can be any person, no requirements for organization or capability or documented procedures ▪ Con: These are airworthiness applicable to design approvals which the holder must perform in order to maintain the eligibility of the design approval

Applicability	Requirement	Pros/Cons
	requirement to maintain eligibility of TC required when rule is promulgated)	
Certified Design Organization (CDO)	▪ Current statutes authorize FAA to issue CDO ▪ CDO-ARC recommendations include SMS as core requirement	▪ Pro: Defined design organization with minimum standards for organization and capability and documented procedures ▪ Con: CDO not yet established in Part 21 and is voluntary
Approved Design Organization Concept (EASA and TCCA)	▪ Approach used by other international aviation authorities to formally recognize design organizations and prescribe minimum standards and requirements including application of SMS	▪ Pro: Defined design organization with minimum standards for organization and capability and documented procedures ▪ Con: Not specifically authorized in statutes and not yet established in Part 21
Impose requirement indirectly on design approvals through 14 C.F.R. 21.137	▪ Production approval holder's quality system would be required to interface with design approval for SMS purposes ▪ 21.137(a) requires the production approval holder to control the design data and changes ▪ 21.137(m) requires coordination with design approval on in-service feedback, design changes and ICA update	▪ Pro: Production approval holders meet organizational requirements capable of supporting SMS ▪ Pro: PC, PMA, and TSOA will meet 21.137 as the common basis for their production quality systems ▪ Pro: Excepts design approvals that are not associated with an active production approval at the time that the regulation is promulgated (*de jure* grandfathering of inactive TCs) ▪ Con: FAA regulation of design approval holder would be indirect (through the PC/PMA/TSOA) ▪ Con: Would only apply to products still listed on a production certificate ▪ Con: Would not apply to applicants for new design approval

2.3 What should the SMS regulations address?

Initial rulemaking should provide a high-level overarching requirement for SMS, at a similar level of detail to the ICAO SMS framework while ensuring the language is applicable to all industry sectors. Once experience has been gained of the applicability of SMS to the design and manufacturing industry sectors, based on pilot programs, rulemaking should then proceed for Part 21 industry-specific applicability of SMS requirements.

Aviation Safety vs. Workplace Safety

The scope of SMS requirements should be limited to hazards associated with the operation of an aircraft or that could affect the safety of aircraft operations. Such a hazard is a condition that can lead to death or serious injury or substantial damage to an aircraft during aircraft operations with the intention of flight. It is not simply any hazard that can lead to injury, illness or death to people; damage to or loss of a system, equipment, or property; or damage to the environment.

Non-Prescriptive and Performance Based (ICAO SMS Framework Level)

The D&M WG agrees with FAA's vision that the most efficient approach to regulation would be a single new overarching regulatory standard eventually applicable to all intended certificate holders (as addressed below). The single rule approach would promote consistent requirements for multi-certificated organizations, as well as encourage interoperability between SMSs of organizations in the various sectors.

To achieve success with this approach, the regulatory language must necessarily be simple, efficient, non prescriptive and performance-based with a clear objective. The best approach would be to ensure that the proposed new CFR Part be consistent with framework-level language, fully aligned with ICAO Standard(s). The D&M believes that FAA Order 8000.367, Appendix B contains a level of detail that would be inappropriate for an overarching SMS regulation and recommends that the WG be tasked to provide specific comments to FAA.

The D&M Work Group reviewed examples of proposed or published Safety Management System regulatory language from TCCA, EASA, Australia, and Singapore as well as recommendations from the CDO-ARC and a generic sample of regulatory language based on the ICAO SMS Framework as background and reference for development of proposed FAA regulatory language. Each example was evaluated from the perspective of perceived strength and/or weakness as potential candidate language for a proposed single overarching regulation based on the following considerations: alignment with ICAO framework, simplicity efficiency and flexibility non-prescriptive and performance-based, and enforceability (***Appendix I***).

2.4 What should the guidance material address?

The following addresses guidance material specifically intended for application to design and manufacturing organizations, whether published with guidance applicable to other sectors or separately. This discussion should be considered as equally applicable to FAA Orders in terms of findings of compliance and ongoing oversight. Guidance for those responsible for oversight must be consistent with guidance for product and service providers.

Guidance material must clearly describe how compliance might be shown with SMS requirements. Guidance material must be prepared that addresses each SMS requirement. The guidance must be clear enough that the applicant will know whether its implementation will be considered acceptable, and that the same finding of compliance or non-compliance would be provided by any FAA evaluator and any FAA region. It must allow flexibility for applicants to use existing systems and processes to the fullest extent possible. For example, an organization's existing Quality Management System (QMS), Continued Operational Safety Program, or certification processes might already embody all of the SRM processes that might be required by SMS regulations. Such an organization's processes should explicitly be accepted as satisfying some or all, as the case may be, SRM requirements. The following are some specific areas where guidance will be needed. An FAA pilot program implementing SMS within the Design and Manufacturing community is needed to promote an understanding of how SMS would apply and would provide information necessary toward the development of guidance in these areas.

1. SMS introduces organizational and behavior performance concepts as requirements in addition to traditional product oriented safety risk management processes. Those concepts include:
    a. Identification of hazards associated with organizational factors, including human performance within an organization
    b. Qualitative SRM of those hazards
    c. Continuous improvement of SMS processes
    d. Imposition of organizational process requirements related to products, e.g., on the holder of a type certificate

    These concepts must not be embodied as regulatory requirements unless and until FAA and industry together come to a clear understanding of how compliance might be shown, and how enforcement might be accomplished. The guidance material must identify the specific features or characteristics that must be present to constitute an acceptable SMS. However, there is limited experience with application of these concepts to D&M organizations and that guidance will be updated over time to incorporate additional information.

2. Guidance material or the rule itself must enable an organization to determine whether it is required to implement an SMS.

3. Guidance is needed to provide a common understanding and detailed methods of compliance for SRM and SA processes appropriate to the range of DAH organizations and products. AC 39-8 on continued airworthiness assessments of powerplants and auxiliary powerplant installations in transport category airplanes is an existing example of such guidance. The success of AC 39-8 depended upon having a pilot program across the propulsion community, and having a common data-set upon which to base

assessments of new risks. It is recommended that a pilot program (perhaps of some years' duration) be used in the Design and Manufacturing community before SMS rule implementation, to promote understanding of how SMS would apply. Such a pilot program might include compilation of industry safety data (similar to the CAAM reports) to enable the use of common assumptions and hazard classifications. Guidance is also needed for how PAH would accomplish SRM and SA.

4. Guidance material must clearly explain or define the extent to which hazard identification must be accomplished in order to show compliance. FAA evaluation of an SRM process must be limited to its relationship to hazards credibly associated with the operation of an aircraft, or that could affect the safety of aircraft operations.

5. Order 8000.367 Chapter 3 specifies, "AVS must define acceptable and unacceptable levels of safety risk," and Appendix B, section 5 specifies, "The organization must define acceptable and unacceptable levels of safety risk." Guidance material (and/or the rules themselves) must clearly define the meaning of "acceptable and unacceptable levels of safety risk," and explain how an organization might show compliance with a requirement to establish those levels. The guidance material must provide guidance on how to develop procedures and must also provide guidance on the objective standards to which the risks will be compared. The objective standards need to be consistent across the industry and repeatable.

6. Guidance material (and/or the rules themselves) must explain the concept of SMS scalability related to organizational size and complexity, and how an SMS might be appropriately scaled. The material should address such situations as "orphan" type certificates, out-of-production products, or an inactive type certificate held by a single individual.

7. Guidance material (and/or the rules themselves) must identify requirements, criteria, and methods used to establish SMS interoperability (as discussed in Order 8000.367).

8. Guidance material must identify an appropriate SMS implementation schedule, such as phased implementation, that may be used by an organization. Consistent with international implementation schedules in the operations sector, phasing should provide for initial implementation of reactive processes aimed at aircraft-level hazards. Proactive and organization-level processes should not be required until additional understanding of SMS in design and manufacturing organizations is obtained. Examples of phased implementation of SMS requirements which can be evaluated as models for D&M are available from AC 120-92, ICAO SMS Manual and Transport Canada.

9. Guidance material must address acceptable means for holders of multiple certificates (such as a manufacturer holding Type Certificate(s), STC, design approvals, a Production Certificate, and Repair Station Certificate(s)) to allow for integration of a single SMS across the organization that holds those certificates.

10. Guidance material must identify the marking requirements necessary to identify safety information subject to statutory protection from disclosure and misuse, such as records of risk assessments and safety decisions. It would be helpful for the guidance material to identify FAA expectations (type and format of data, who has access, etc.) as well as the

extent of protection afforded. This, of course, presupposes the existence of statutory protection for safety data. It is crucial that such protection be in place; without it, safety data is not likely to be shared.

11. Guidance material on demonstrating the ongoing effectiveness and performance of SMS.

12. Guidance material must identify how a party may demonstrate compliance to certain elements of the SMS requirements through implementation of certain industry consensus standards. Industry Standards like AS 9100 and the MARPA Continued Operational Safety System include elements of SMS. By verifying compliance to those standards in accordance with FAA guidance, the SMS party may demonstrate compliance to the related elements of SMS. FAA guidance should indicate the procedures for acceptance of industry standards, and the process for identifying which elements of SMS are addressed by each industry standard.

2.5 Explanation of the SMS ARC recommendations

- Justification (reasoning) for rule change
- Explanation of benefits
- Explanation of costs
- Harmonization with international standards

Justification (reasoning) for rule change

If ICAO has a standard in Annex 8 requiring organizations responsible for the type design or manufacture of aircraft to have an SMS then it is necessary for the FAA to have SMS regulations that are inline with the ICAO standard to facilitate reciprocal acceptance by other ICAO signatory authorities of the U.S. state of design or manufacturer SMS. Without an FAA recognized SMS, a manufacturer of aircraft might have to demonstrate compliance with potentially conflicting SMS requirements of each non-U.S, authority for which they hold a type certificate which would be burdensome and reduce the overall benefit of SMS. The above provides the primary justification for regulation of SMS for design and manufacturing organizations.

The SMS-ARC Design and Manufacturing Working Group recognizes that not all organizations associated with civil aviation are effectively managing all their safety risks and that SMS regulations can have a positive influence on the overall safety of civil aviation. However, there are many organizations that are effectively managing their contribution to aviation safety and we want to ensure that the implementation of SMS regulations does not diminish or detract from those effective safety program. The SMS-ARC Design and Manufacturing Working Group also recognizes that with proper implementation of SMS regulations even those effective safety programs can also be enhanced.

The SMS-ARC Design and Manufacturing Working Group members believe there would be potential safety benefit to civil aviation and the air transportation system if a consistent set of SMS regulations were promulgated. However, the D&M has identified several key concerns for the design and manufacturing sector that must be addressed in order to achieve success from both a regulator and industry perspective, and to avoid unnecessary administrative burdens without commensurate safety benefit. The D&M supports regulation of SMS for certain design and manufacturing organizations provided the following key issues are addressed:

- **International Harmonization and Reciprocal Acceptance** – The regulations should be harmonized internationally and there must be reciprocal acceptance of Safety Management Systems
- **Phased Promulgation of SMS regulations** – Promulgation of SMS rulemaking needs to be phased to provide for development of appropriate industry sector-specific requirements and applicability and development of necessary FAA guidance
- **Phased Implementation of SMS Requirements** – Regulations would accommodate phased implementation of SMS elements.
- **Recognize Existing Systems and Processes** – The regulations must provide for acceptance of existing effective safety programs and company processes which are already in place

- **Recognize Certification Procedures and Airworthiness Requirements** - Part 21 certification procedures and airworthiness requirements are prescribed by regulation and can not be changed by SMS requirements and processes
- **Scalability and Flexibility** – The regulations must accommodate a broad range of organizations from small parts manufacturers to large organizations holding multiple types of certificates/approvals and various business arrangements
- **Protection of SMS Safety Information** – There must be protection of safety information from disclosure and use for other purposes
- **FAA Plan for D&M Sector SMS Oversight Activity** – FAA must ensure sufficient planning and workforce training to accommodate efficient and timely assessment and oversight of SMS which is significantly different than current certification compliance activities
- **Alternatives to SMS Implementation Through Regulation** – FAA should consider alternatives to SMS implementation through regulation such as industry consensus standards and voluntary programs which may be more appropriate and effective for certain industry sectors

Explanation of Benefits

Potential benefits of an 'ideal' implementation at a D&M organization include the following:

- **International recognition and mutual acceptance**
  - International recognition of an FAA SMS certification would allow mutual acceptance or recognition by non-U.S. regulatory authorities of the U.S. type certificate holder's SMS, assuming the non-U.S. authority required the type certificate holder to have an SMS.

- **Safety data driven rulemaking by FAA and other aviation authorities**
  - With "ideal" implementation comes effective sharing of trusted safety information with regulators. Such sharing likely would tend to promote appropriate regulatory actions, such as airworthiness directives, airworthiness standards, organizational requirements, decisions to add/delete regulations, etc.

- **Streamlined processes and improved process capability**
  - Provided that the implementation does not have the effect of adding layers of compliance
  - SMS adds focus on the assessment and improvement of the organization's capabilities and procedures beyond the current system, which requires FAA to analyze independently the safety implications of new and modified designs.
  - Process enhancements may include:
    - Adopting a data driven approach (similar to system safety) to enhancing safety. This includes the collection and accessibility of data (internal and external) to support better decision-making and proactive identification of safety issues upstream before accidents occur
    - Using a risk based approach so that resources are best allocated to support those activities which will achieve the greatest safety benefit;

  - Better integration of safety processes and end-to-end oversight of safety issues to ensure that safety issues discovered are properly dealt with and "closed" (or completed) regardless of where or by whom they are discovered

- **Improved Organizational Decision-making**
  - An effective safety management system can potentially provide design and/or production organizations with a consistent set of standards to manage continued airworthiness, and to transfer the safety knowledge gained from lessons learned into future designs.
  - For organizations holding multiple certificates, an integrated safety management approach may be an effective way to collect and analyze hazard information and determine the most appropriate way to implement risk controls.
  - Identification of hazards, the analysis and assessment of the associated risk can lead to the development and implementation of appropriate risk controls, improving product safety. If more analytical assessment techniques, similar to AC 39-8, are adopted more appropriate expenditure and timeliness of necessary corrective actions can be made.
  - Understanding what presents the greatest risk and what needs to be addressed
  - With appropriate regulatory guidance, safety management system will ensure a broader focus of potential hazards are considered in an organization when making decisions and hence potentially reduce risk.
  - Providing decision-makers with a solid defense in support of decisions;

- **Proactive Management of Safety**
  - An effective safety management system will ensure the organization continuously evaluates the effectiveness of their risk control measures
  - Early identification and continuous control of safety hazards to prevent accidents from occuring

- **Safety Promotion**
  - Effective promotion of SMS will encourage employees to report and engage in the safety decision making process.

Explanation of Costs

The costs of an SMS regulation are driven by the details of the requirements and implementation, and are difficult to assess until the details are fully understood. If the requirements are prescriptive, do not allow full use of existing safety systems and require an all-encompassing risk analysis process (including comprehensive hazard identification, full human error risk analysis and mitigation, organizational risks and unbounded proactive risk research), then costs will be prohibitively high.

If requirements are kept at a high level, allowing considerable discretion by the organization in how they meet the requirement, and if existing internal safety systems can be used in showing compliance, and if risk analysis activity can be prioritized to address the highest risks, then costs would be very much lower.

As an example, cost estimates for SMS implementation were conducted by one large manufacturer using the high level ICAO requirements, and compared to the estimated costs for a partial implementation of Appendix B. The detailed analysis for partial implementation of Appendix B was submitted to the Docket in response to the ANPRM. The results are shown in the table below. Additional bounding of the requirements could drive costs significantly lower than those shown in the table. In addition, the commenter noted that costs, robustness of analyses and ease of oversight would all be greatly benefited if the industry were to pool data on hazards, as was done by the propulsion industry in the CAAM process.

	Initial (non recurring) cost $MM	**Annual recurring cost $MM**
ICAO SMS Framework	9	25
Appendix B (partial implementation)	107	22

Harmonization with International Standards

Many organizations in the design and manufacturing sector are affected by regulations of multiple State civil aviation authorities. Proliferation of multiple, slightly differing SMS standards could force organizations to accomplish redundant compliance demonstrations and to develop and maintain redundant documentation for compliance, all without benefit to safety. The FAA must work with ICAO and other State civil aviation authorities to establish harmonization of SMS regulation, or reciprocal acceptance of a service provider regulatory compliance finding made by a single authority.

SMS interoperability will also require the flow of information between suppliers and customers in different states, and between organizations and regulators in different states. If a single industry-standard process and format can be used, tailored to comply with all export laws, this will avoid multiple reporting of the same data in several slightly different formats required for different authorities or customers. It is recommended that industry be tasked to develop such a standard in coordination with ICAO.

SECTION 3: Summary of D&M Recommendations

3.1 Recommendations in Response to FAA Questions

The following is a summary list of D&M recommendations which are excerpts taken directly from discussion Section 2 of this report on comments in response to FAA questions and includes a reference to the page number where the recommendation is made:

- The D&M recommends that FAA work with ICAO other State regulatory authorities to ensure a coordinated and harmonized approach to implementation of SMS requirements to facilitate reciprocal acceptance of SMS programs of the State of design and State of manufacture. [6]
- The D&M recommends that new SMS requirements be adopted through phased rulemaking promulgation to build industry sector-specific experience and understanding and provide for the development of appropriate requirements and determination of appropriate applicability and phased implementation. [6]
- The D&M strongly recommends that FAA also work closely with design and manufacturing organizations through a pilot program to collaboratively develop a common understanding of how SMS could best be applied to support the development of appropriate requirements and implementation guidance. [7]
- The D&M recommends that development of a proposed rule for applicability of SMS within Part 21 occur only after sufficient implementation experience within the design and manufacturing sector through an FAA sponsored pilot program, as well as development of workable sector-specific industry standards and FAA guidance material. [7]
- D&M recommends that FAA work through ICAO to amend Annex 8 standards to establish an appropriate and realistic date for States' to implement SMS requirements for organizations responsible for the type design or manufacture of aircraft. [7]
- The D&M recommends that FAA clearly state that SMS can not change applicable regulatory requirements and the level of safety established in the regulations. [9]
- The D&M recommends that FAA seek to have Congress protect Safety Management Systems information from disclosure through discovery and/or FOIA in the United States. [10]
- the D&M recommends that the FAA work through ICAO to expand ICAO Assembly Resolution on protecting safety data (Resolution A 35/17) to specifically include Safety Management Systems information. [10]
- The D&M recommends that FAA consider alternatives to SMS implementation through regulation such as industry consensus standards and voluntary programs which may be more appropriate and effective for certain industry sectors. [11]
- The D&M recommends that the SMS-ARC task the D&M to provide a review of Order 8000.367 Appendix B SMS requirements and to develop an appropriate definition of a "hazard" in order to support FAA pilot program with design and manufacturing organizations. [25]

3.2 Recommendations for Next Steps

The D&M strongly recommended that FAA also work closely with design and manufacturing organizations through a pilot program to collaboratively develop a common understanding of how SMS could best be applied in an effective and efficient manner. This is the only way to develop sufficient implementation experience to support the establishment of appropriate SMS regulatory requirements, applicability scope to certain design and production approval holder organizations, and development of implementation guidance, tools and policy for both industry and FAA. The D&M recommends that the SMS-ARC task the D&M to provide a review of Order 8000.367 Appendix B SMS requirements and to develop an appropriate definition of a "hazard" in order to support FAA pilot program with design and manufacturing organizations.

Review of SMS Requirements in Order 8000.367, Appendix B

The D&M supports a single new overarching SMS regulatory standard which would eventually be applicable to certain design/production approval holders. The single rule approach would promote consistent requirements for multi-certificated organizations, as well as encourage interoperability between SMSs of organizations in the various sectors. To achieve success with this approach, the regulatory language must necessarily be simple, efficient, non prescriptive and performance-based with a clear objective. As stated previously in this report, the D&M believes that FAA Order 8000.367, Appendix B contains a level of detail that would be inappropriate for an overarching SMS regulation and recommends that the WG be tasked to provide specific comments to FAA. The D&M requires additional time to discuss Appendix B requirements in more detail in order to provide FAA with specific comments and justification for this position.

Definition of "Hazard" in Design and Manufacturing Environment

The definition of "Hazard" in the current ICAO guidance as well as in FAA Order 8000.367 may be sufficiently detailed in the context of flight operations and for application in an air carrier's SMS, but requires more specific translation to allow applicability as part of a proposed SMS regulatory mandate for the design and manufacturing sector. The definition from FAA Order 8000.367 is reproduced for reference:

> *"Hazard - Any existing or potential condition that can lead to 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."*

In the areas of aviation product design and continued operational safety, identification of product-related hazards and the effective management of the associated risks are activities that are fundamental and well understood. However, the starting point and necessary prerequisite for accomplishment of a safety risk analysis in terms of likelihood of occurrence and severity of effects is the identification of a specific existent or postulated condition of the product. Under the safety risk management (SRM) component of an SMS, and utilizing the existing hazard definition, a design organization could potentially be expected to evaluate an essentially infinite set of existing or potential conditions involving the organization, personnel, facilities, analytical tools/capabilities and so forth. While these factors could potentially affect the product design, there is no direct correlation any product attribute, and therefore no capability for traditional

evaluation in terms of likelihood of occurrence or severity of effects. It would therefore be impractical or impossible for a design organization to fully comply with the SMS requirements as written in 8000.367 Appendix B. Additional work will be required to develop more specific definitions and guidance for applicability to design and manufacturing activities.

SECTION 4: APPENDICES

Table of Contents

APPENDIX A: SMS-ARC Design & Manufacturing (D&M) Working Group Membership List

Last Name	First Name	Organization	Membership Status
Desrosier	Walter	GAMA	D&M Lead and ARC
Johns	Tom	Boeing	D&M and ARC Tri-Chair
Dickstein	Jason	MARPA & AEA	D&M and ARC
Mahone	Bruce L.	SAE	D&M and ARC
Bartron	Michael	Pratt & Whitney	D&M
Beck	Anthony	Gulfstream Aerospace Corp	D&M
Cummins	Mike	Honeywell Engines & Systems	D&M
Durkin	Chris	Honeywell Avionics	D&M
Jette	Helynne	Bombardier Aerospace	D&M
Kerr	John S.	Bell Helicopter Textron Inc.	D&M
Kihm	Doug	Boeing	D&M
Knife	Sarah	GE Aviation	D&M
Picou	Gary	PS Engineering, Inc.	D&M
Thompson	Dean	Hawker Beechcraft Corp.	D&M
Welch	William (Buck)	Cessna Aircraft Company	D&M
Williams	Rex	Bombardier Learjet	D&M
Reinert	Mike	FAA-AIR	D&M FAA Support
Huber	Chuck	FAA-AIR	D&M FAA Support
Navarro	Linda	FAA-AIR	D&M FAA Support

APPENDIX B: Summary of comments to SMS ANPRM

The D&M reviewed the Safety Management Systems ANPRM Comment Summary prepared by the Regulatory Group (dated November 20, 2009) and developed a high-level summary of the design and manufacturing industry sector responses to identify key issues, concerns, and any recommendations regarding SMS requirements.

Compilation Summary of Comments to SMS ANPRM

The majority of commenters in the Design and Manufacturing community expressed concern over the potential cost and resource burden of SMS. Many believe they already have robust internal safety programs and that SMS regulations would introduce a significant burden in administration and documentation, without providing a commensurate safety benefit. They suggested many approaches to mitigating this burden including:

- conducting a gap analysis to existing regulations or requirements,
- by keeping SMS requirements at a high level and non prescriptive, and
- flexible to allow the use of existing systems in showing compliance,
- scalable to accommodate small to large and simple to complex organizations, and able to
- accommodate various business arrangements.

A phased approach with pilot programs was suggested to develop experience with application of SMS to Design and Manufacturing organizations. The commenters also expressed concern over protection of safety data, risk assessments and safety decisions from lawsuits and from loss of intellectual property rights; statutory protection was requested.

Excerpt Summary of Comments to SMS ANPRM

The following provides a summary of comments to the SMS ANPRM categorized by the Regulatory Group as coming from design, manufacturing and maintenance organizations only (Air Carrier and Training comments are not addressed herein. Some comment attributions may have been omitted by mistake). The reference numbers provided following each set of comments identifies the specific commenter from the docket. This provides a general indication of the number of commenters that support a particular position and traceability in the event a commenter wishes to understand how their response to the ANPRM was considered by the D&M in this report.

DM1 Many companies stated that they already have robust internal safety programs. Many commenters expressed concern over the potential cost and resource burden entailed in showing compliance with SMS requirements. (8.1, 16.1, 20, 21.1, 24.1, 25.1, 26.1, 30.1, 31.1, 32.1, 33.1, 34.1, 39.1, 48.1, 53.1, 57.1, 63.1, 80.1, 88.1, 89.1) . One commenter (a private individual) requested that cost not be considered.

It was pointed out that this cost and resource burden could detract from existing safety systems and processes. (57.1, 80.1, 35.1, 62.1, 25.1, 21.1, 33.1, 49.1, 32.1).
Some commenters said that they had found SMS tools to be helpful in cost savings or reducing quality escapes. (77, 72.1, 63.1)

DM2 Many commenters stated that SMS elements duplicate existing internal processes or existing regulatory requirements, especially existing type certification processes for the design sector and QMS processes and requirements for the manufacturing and maintenance sectors. (57.1, 68.1, 20, 62.1, 25, 72.1, 50.1, 17.1, 19.1, 35.1, 53.1, 58.1, 75.1, 10.1, 25.1, 34.1, 21.1, 24.1, 32.1, 33.1, 36.1, 39.1, 63.1, 77, 44.2, 85.1, 70.1, 49.1, 24.1, 88.1, 19.1)

DM3 SMS was perceived as imposing a significant bureaucratic/documentation burden; doubt was expressed that it would result in a commensurate safety benefit. (24.1, 32.1, 75.1, 10.1, 21.1, 36.1, 39.1, 26.1, 34.1, 8.1, 33.1, 63.1, 25.1, 19.1, 88.1, 16.1, 26.1, 39.1).

DM4 Some commenters, especially the engine community which has a very strong, formalized COS process in place via AC39.8, did not believe that SMS would improve compliance with the CFRs. (17.1, 35.1, 62.1, 88.1, 72.1, 25.1, 75.1, 21.1, 24.1, 63.1). A few airplane-community commenters believed it would be helpful to them in Continued Operational Safety programs (53.1, 49.1)

DM5 The following approaches to mitigating the burden were proposed (in no special order):

- Phased implementation (57.1, 89.1, 79.1, 35.1, 72.1). Commenters noted that the air carrier implementation of SMS is much further ahead than that of Design, Maintenance + Manufacturing sectors, and that developing a common understanding of applicability should precede levying requirements on Design, Maintenance + Manufacturing.
- Gap analysis comparing SMS to existing regulations or requirements (44.2, 51.1, 25, 53.1, 34.1, 8.1, 38.1, 68.1, 62.1, 50.1, 72.1, 25.1, 39.1, 44.2, 70.1, 25.1, 58.1, 77, 19.1). It was suggested that SMS requirements not duplicate existing requirements, or that the MOC for existing requirements be explicitly accepted as also showing compliance with the SMS requirement.
- Many requests to allow use of existing systems in showing compliance (57.1, 58.1, 89.1, 25, 48.1, 68.1, 20, 31.1, 17.1, 35.1, 38.1, 50.1, 10.1, 25.1, 34.1, 24.1, 26.1, 62.1, 72.1, 77, 44.2, 85.1, 70.1, 49.1, 75.1, 24.1). Most commenters who expressed an opinion on the relationship of SMS and QMS proposed that SMS be integrated into existing QMS systems.
- Keeping requirements at a high level/flexible/non-prescriptive (57.1, 89.1, 35.1, 75.1, 50.1, 38.1, 49.1, 50.1, 44.2, 17.1, 30.1, 44.2, 49.1, 58.1)
- Tiered implementation (31.1, 62.1, 72.1, 10.1, 39.1) Some concerns were stated that tiered implementation would not lead to a uniform safety level or would be unfair.
- Limiting the applicability of SMS to some sectors of industry (19.1, 25.1, 50.1, 75.1, 77 etc); there was considerable variation in views on how this should be done. Many small companies said they had not the resources for such a large, complex program (48.1, 80.1, 21, 77, 21.1, 24.1, 26.1, 39.1) and that it would not add value to a simple production process or to a repair station. Equipment suppliers questioned whether their limited scope available for safety improvements justified introduction of SMS. Commenters in the general aviation sector pointed out that their fleets were small and had minimal contribution to system risk. (58.1). Other commenters requested that SMS, if required by regulation, apply to all product and service providers. (57.1, 17.1), or consider immediate application to operators only (16.1,

17.1 , 25.1, 34.1, 50.1, 75.1, 35.1) A cost benefit analysis was requested for each product/service segment.

- Voluntary compliance and guidance, rather than requirements (68.1, 12.1, 87.1, 17.1, 70.1, 33.1, 63.1)
- Accreditation (70.1, 53.1, 49.1, 48.1, 49.1, 38.1 ,16.1)
- Trade group leadership, as opposed to independent efforts (39.1, 16.1)
- Use language of ICAO or of national SMS Standard or of CDO ARC (35.1, 62.1, 38.1, 57.1, 49.1, 19.1, 15.1, 89.1). The AS9100 standard was pointed out as an excellent example to follow. (77, 19.1)
- Use AC39.8 methodology for Safety Risk Assessments (88.1, 62.1 35.1)

DM6 Many comments from the Design, Manufacturing and Maintenance sectors pointed out that the published material has so far dealt with air carrier operations, that the Design, Manufacturing and Maintenance environment is very different in key respects, and that much additional work would be needed to establish if and how SMS requirements should apply to Design, Manufacturing and Maintenance. (89.1, 57.1, 75.1, 50.1, 10.1, 36.1, 63.1, 38.1, 39.1, 88.1, 77, 19.1, 35.1, 25.1, 62.1). Commenters requested sector-specific, size-specific criteria for findings of compliance for an SMS.

DM7 There was considerable disagreement on how SMS should apply to suppliers who do not have design ownership. (19.1, 49.1, 38.1, 35.1, 62.1, 88.1, 10.1) Many felt that SMS should only be levied on certificate-holders. Some proposed a flowdown to suppliers by contractual requirement, others foresaw great difficulties in such a system (16.1, 17.1, 34.1, 58.1, 62.1, 35.1, 48.1). Similarly, repair stations were concerned that they would be required to comply with the conflicting SMS implementations of each of their customers. (8.1)

DM8 There was some confusion over whether SMS should apply to health + safety, or other ancillary disciplines, or only to product safety, clarification was requested (23, 30.1, 75.1, 50.1, 45.1, 19.1, 38.1, 71.1, 72.1, 68.1, 52.1, 26.1, 62.1).

DM9 Commenters asked that any requirements be objective, clear and consistent, to avoid variation in interpretation. (17.1, 57.1, 89.1, 48.1, 49.1, 88.1, 77, 38.1, 36.1). There have been problems with pilot SMS projects due to shifting interpretation/ expectations on the part of regulatory authorities. (44.2).

DM10 Many requests were made for the guidance to accommodate various business models and to be scaleable. (10.1, 15.1, 31.1, 35.1, 38.1, 49.1, 57.1, 62.1, 63.1, 72.1, 89.1)

DM11 There were many requests for harmonization of the US SMS requirements with those of foreign agencies, and bilateral recognition of SMSs, so that international companies need not comply to multiple different sets of SMS requirements. (17.1, 38.1, 57.1, 89.1, 62.1, 72.1, 30.1, 49.1, 44.2, 50.1). One commenter was concerned over potential disharmony between FAA and other US agency requirements (e.g DoD). (19.1)

DM12 There were many comments requesting measures to protect safety data/risk assessments from loss of intellectual property rights, from civil and criminal lawsuits, and to promote protection of personnel with SMS duties from criminal proceedings (8.1, 10.1, 17.1, 19.1, 25.1, 35.1, 30.1, 32.1, 33.1, 36.1, 50.1, 57.1, 53.1, 68.1, 75.1, 77, 89.1, 88.1, 62.1, 63.1, 49.1, 58.1, 28.1, 38.1, 16.1, 8.1, 44.2). The downsides of de-identification and the difference in the nature of reporting for an operational vs a design environment were also raised.

DM13 There is a general desire for concrete metrics and criteria, rather than abstract/academic material ("safety culture" was difficult for many commenters to accept as a requirement basis; commenters from the flight operations area found the "culture" concept more applicable to safety than did those from manufacture and design communities). (28.1, 49.1, 50.1, 62.1, 77, 88.1, 89.1, 35.1).

There was a lot of concern over how acceptable risk levels should be set; who should do it, should it be driven by risk exposure, what metrics would be appropriate, how metrics could have unintended consequences (distort reporting and behavior). (8.1, 10.1, 16.1, 25.1, 30.1, 38.1, 49.1, 50.1, 57.1, 58.1, 62.1, 63.1, 75.1, 77, 88.1)

DM14 There were questions on the requirement for interoperability and how compliance would be shown; the requirement currently appears unbounded. (75.1, 35.1)

DM15 Some commenters questioned the mandate of the FAA to impose such a broad requirement without a specific safety issue to be addressed. (16.1, 48.1, 68.1, 31.1, 33.1, 64.1). The FAA is currently responsible for the safety of the system (except where delegated); how does the FAA give that responsibility to the product or service provider? This concern was also raised over specific elements of SMS (e.g. is the FAA within their charter to require a company to develop a document management program? 44.2).

DM16 It was pointed out that since existing SMS programs vary so widely in performance, elements and outcomes, the ANPRM responses on company's costs benefits and experience will be based on very different understandings of SMS and may not apply to the FAA's implementation. (64.1).

DM17 There was concern that businesses retain internal flexibility to select the tools and processes applicable to the circumstances. (58.1, 63.1).

Concern was expressed over timing of implementation and timing of revisions and updates (short cycle times driving confusion and expense).

DM18 One commenter said the stated requirements went beyond the risk analysis state-of-the-art (quantified risk assessment for operational procedures and substitute risk, 35.1)

DM19 The FAA was requested to consider how ODA would work with SMS (35.1, 57.1)

DM20 One commenter advocated the use of an integrated capability maturity model to measure organizational culture. (28.1)

One commenter suggested that integrated capability maturity models likely will incorporate SMS as a metric set, and if so, equitable SMS requirements should be established. (38.1)

DM21 Two commenters expressed concern over the safety of helicopter tour passengers. (60, 46) *(Recommend this comment be considered outside ARC scope)*

DM22 One commenter offered a proposed architecture for data handling. *(Recommend this comment be considered outside ARC scope)*

APPENDIX C: Regulatory Gap Analysis – Executive Summary

Ground Rules

This analysis addresses regulatory requirements only. Many organizations have process elements in place which they have developed voluntarily or co-operatively with the FAA; such processes are not addressed here.

The analysis was conducted against both the ICAO framework and the Appendix B to Order 8000.367. The current regulatory requirements come much closer to meeting the ICAO framework than they do Appendix B.

The analysis considered the safety of the product separately from the safety of organizational factors.

The referenced appendices show the extent to which existing regulatory requirements mandate process elements of SMS (pink= no requirement in place, yellow= a requirement exists but is not comprehensive; green= the requirement fully addresses the SMS element.)

Appendix D: Gap Analysis: Part 21 Design and Order 8000.367 Appendix B Requirements
Appendix E: Gap Analysis: Part 21 Manufacturing and ICAO SMS Framework Requirements
Appendix F: Gap Analysis: Extent to Which Part 21 D&M Addresses SMS Framework

Safety Policy

There are no current regulatory requirements for design organization safety policy.

CFR 21 already addresses the appointment of key quality personnel for a production certificate holder (this is functionally "the same as" a requirement to appoint key safety personnel, in a production environment). CFR21 also addresses the definition of accountabilities, and documentation of the QMS and production system. No requirements mandate a management commitment to safety, or coordination of emergency response planning (this last was not considered applicable to the design and production environments).

CFR21 addresses only six of the 37 proposed requirements for Appendix B – safety policy.

Safety risk management

The current regulatory requirements already control the product safety of new designs; requiring SMS risk management to the design process is considered redundant. Part 21.99 requires type certificate holders to make design changes to address undsafe conditions as determined by FAA. AC 39-8 defines a propulsion system process meeting the intent of safety risk management, and ETOPS fleets have a defined and required process for initial service as well as continuous monitoring.

CFR 21 has recently been revised; the new requirements address many of the risk management and safety assurance processes of ICAO's SMS framework when applied to a production environment. The notable exception is that CFR21 mandates corrective action by the QMS without a safety risk assessment, so the corrective action might not be prioritized.

Appendix B has 32 requirements under the general subject of safety risk management, ten of which are addressed by current requirements for some products or organization types.

Safety Assurance

CFR 21 already requires QMS performance monitoring and measurement, change management and continuous improvement. This would meet much of the intent of SMS safety assurance, except that monitoring the QMS as a whole might not give a clear metric of SMS performance.

There is no requirement for design organizations in general to perform safety monitoring for new designs or for COS. AC 39-8 defines a propulsion system process meeting the intent of safety monitoring, and so does the ETOPS rule. Only early-ETOPS requires lessons learned from COS to be incorporated into the design process.

Appendix B has 33 requirements under the general subject of safety assurance, a few of which are addressed by current requirements for some products or organization types.

Safety Promotion

There are no current regulatory requirements for safety promotion, either for production or for design organizations.

Appendix B has 14 requirements under the general subject of safety promotion, none of which are addressed by current requirements.

Part 21 Design Organization: SMS Requirements Gap Analysis and Exceptions Assessment

Version: 3/12/2010

Order 8000.367 Appendix B	SUBJECT - TITLE	FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
Preamble	The following requirements are the minimum set of requirements that must be established for constituent product/service provider organizations for which AVS services have oversight responsibility.				
1	**Scope and Applicability** - to be developed by the AVS service/office.				
		§21.1 Applicability	(a) This part prescribes— (1) Procedural requirements for the issue of type certificates and changes to those certificates; the issue of production certificates; the issue of airworthiness certificates; and the issue of export airworthiness approvals. (2) Rules governing the holders of any certificate specified in paragraph (a)(1) of this section; and (3) Procedural requirements for the approval of certain materials, parts, processes, and appliances.	No gap analysis possible since the Order is silent on applicability.	
		§25.1 Applicability	(a) This part prescribes airworthiness standards for the issue of type certificates, and changes to those certificates, for transport category airplanes. (b) Each person who applies under Part 21 for such a certificate or change must show compliance with the applicable requirements in this part.		
		§33.1 Applicability	(a) This part prescribes airworthiness standards for the issue of type certificates and changes to those certificates, for aircraft engines. (b) Each person who applies under part 21 for such a certificate or change must show compliance with the applicable requirements of this part and the applicable requirements of part 34 of this chapter.		
2	**References - to be developed by the AVS service/office**				
			Title 49 USC, 14 CFR, FAA Orders, Advisory Circulars		
3	**DEFINITIONS (Appendix A)**				
	To be developed by the AVS service, but the definitions should be consistent with existing FAA definitions and those in the AVSSMS. **EXCERPTS** of key definitions from Appendix A:				

Order 8000.367 Appendix B	SUBJECT - TITLE	FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
	Safety Management System (SMS) – The formal, top-down business-like approach to managing **safety risk**. It includes systematic procedures, practices, and policies for the management of safety (as described in this document it includes Safety Risk Management, safety policy, safety assurance, and safety promotion).				
	Safety risk – The composite of predicted severity and likelihood of the potential effect of a **hazard**.				
	Hazard – Any existing or potential condition that can lead to 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**.			The proposed definition of hazard is so broad that it includes normal flight (damages environment by noise and emissions) and trivial concerns (spillage of coffee damages property I.e. terminal carpet.	The definition should be revised to focus on product/servise safety and on risk to passengers and crew.
	Accident – An occurrence associated with the operation of an aircraft that takes place between the time any person boards the aircraft with the intention of flight and all such persons have disembarked, and in which any person suffers death or serious injury, or in which the aircraft receives substantial damage.				
	Incident – An occurrence other than an accident that affects or could affect the safety of operations.				" could affect" is too broad. Should say "likely to affect"
4	**Policy [Ref Ch 2 of the Order]**				
4.a.	**General Requirements**				
4.a.(1)	Safety Management must be included in life cycle of the organization's outputs	Title 14 Code of Federal Regulations (14CFR)	Every aspect of civil aviation requires that all products, from design & production and throughout operational life (flight & maintenance), be airworthy, including operating the product in accordance with regulatorily defined airworthiness requirements		Actually, there's no requirement for the product to be airworthy before it's certified. Also, claiming equivalency between airworthiness and safety may get us into difficulties. They are not precisely the same.
4.a.(2)	The organization must promote the growth of a positive safety culture			Propose exception - strike requirement, this will then be consistent with ICAO language	Since no-one knows what a positive safety culture is, or how it can be measured, this requirement should be struck. Need objective requirements.
4.b.	**Safety Policy**				
4.b.(1)	Top management is responsible for the organization's safety policy and its safety performance				
4.b.(2)	The safety policy must:				Comment: the terms “policy” and “procedure” have different meanings in different organizations, which leads to varying interpretation in this section. To some, “policy” is a general statement of organization intent. To others, it is a very specific binding document constituting the internal rules of the organization. E.g. policy abc says you must not discriminate against another employee on the basis of attributes x,y,z, and if you do you will be subject to disciplinary action up to and including dismissal…..

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
4.b.(2)(a)	include commitment to implement and maintain the SMS					
4.b.(2)(b)	include commitment to continual improvement in the level of safety				Propose exception - strike requirement, this will then be consistent with ICAO language	"Risk management" and "objectives" ((g), below) are in conflict with open ended "continual improvement"
4.b.(2)(c)	include a commitment to management of safety risk, defined as The composite of predicted severity and likelihood of the potential effect of a hazard. (Ref App A)					
4.b.(2)(d)	include commitment to comply with applicable legal, regulatory and statutory requirements				Propose exception - strike requirement, this will then be consistent with ICAO language	Not appropriate content for a Safety policy . The field of "legal regulatory and statutory requirements " is extremely broad, and all companies have existing mechanisms and processes to assure compliance. There is no benefit, and significant drawbacks, to including this as part of SMS. If the FAA wants this, they should identify the legal and statutory requirements and cite themm directly, rather than expect each business to do this independently.
4.b.(2)(e)	include an expectation that employees will report safety issues &, where possible, provide proposals for solutions/safety improvements					
4.b.(2)(f)	establish clear standards for acceptable behavior				Propose modification "objective standards for safety-related behavior"	The phrase "acceptable behavior" is so broad that it is impossible for "policy" to establish "clear standards". The work environment inherently has unclear areas - it would be impossible for policy to foresee and rule upon every case in advance. Also, the "behavior" should be bounded to that which could affect safety.
4.b.(2)(g)	provide management guidance for setting safety objectives			Safety objectives are set by regulations, not by "management", in CFR25.1309, CFR25.901c, CFR33.75, AC39-8, etc	Propose modification "or state objectives prescribed by regulatory authorities" Sector -level guidance can then cite 33.75, 25.1309, AC 39.8 etc.	Objectives must be prescribed by FAA regulations and policy, as they currently are for type designs and for propulsion system continued operational safety. It would be very difficult for an organization to set its own safety objectives, from a liability perspective. (and what if the objectives were very low?) There needs to be an external standard set by the authorities, both to provide a common standard of safety, and to limit the exposure of businesses to litigation.

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
			§33.75 Safety analysis	(a) (1) The applicant must analyze the engine, including the control system, to assess the likely consequences of all failures that can reasonably be expected to occur. This analysis will take into account, if applicable: (i) Aircraft-level devices and procedures assumed to be associated with a typical installation. Such assumptions must be stated in the analysis. (ii) Consequential secondary failures and latent failures. (3) The applicant must show that hazardous engine effects are predicted to occur at a rate not in excess of that defined as extremely remote (probability range of 10e(−7) to 10e(−9) [1per 10,000,000 engine flight hours to 1 per 1,000,000,000 flight hours]). Since the estimated probability for individual failures may be insufficiently precise to enable the applicant to assess the total rate for hazardous engine effects, compliance may be shown by demonstrating that the probability of a hazardous engine effect arising from an individual failure can be predicted to be not greater than 10e(−8) [1 per 100,000,000] engine flight hours.		
			§25.1309 Equipment, systems, and instalations	(a) The equipment, systems, and installations whose functioning is required by this subchapter, must be designed to ensure that they perform their intended functions under any foreseeable operating condition. (b) The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that— (1) The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable, and (2) The occurrence of any other failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.		

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
			AC 25.1309-1A System Design and Analysis	10. Quantitative Assessment. B. Quantitative Probability Terms. When using quantitative analyses to help determine compliance with § 25.1309(b), the following descriptions of the probability terms used in this regulation and this AC have become commonly-accepted as aids to engineering judgment. They are usually expressed in terms of acceptable numerical probability ranges for each flight-hour, based on a flight of mean duration for the airplane type. (1) Probable failure conditions are those having a probability greater than on the order of 1 X 10e(-5), [greater than 1 per 100,000 flight-hours}. (2) Improbable failure conditions are those having a probability on the order of 1 X 10e(-5) or less, but greater than on the order of 1 X 10e(-9) [less than 1 per 100,000 flight-hours, but greater than 1 per 1,000,000,000 flight-hours]. (3) Extremely Improbable failure conditions are those having a probability on the order of 1 X 10e(-9) or less [less than 1 per 1,000,000,000 flight-hours].		
			AC39-8	This AC also provides CAAM guidance for estimating the risks associated with identified unsafe conditions; defining, prioritizing, and selecting suitable corrective actions for all identified unsafe conditions; and verifying that the corrective actions were effective. This AC is intended to present a tangible means of logically assessing and responding to the safety risks posed by unsafe conditions.		
4.b.(2)(h)	provide management guidance for reviewing safety objectives					
4.b.(2)(i)	be communicated to all employees & responsible parties				Propose modification to reflect ICAO language - strike "and responsble parties"	Company policy might be restricted to employees and not allowed to be distributed externally to “responsible parties”. Furthermore, there are employees whose behavior cannot affect product safety; there should be no requirement for them to receive this material.
4.b.(2)(j)	be reviewed periodically to ensure it remains relevant & appropriate to the organization					
4.b.(2)(k)	identify responsibility & accountability of management & employees w/respect to safety performance					
4.c.	**Quality policy.**					
4.c.	Top management must ensure that the organization's quality policy is consistent with the SMS.					
4.d.	**Safety Planning.**					
4.d.	The organization must establish and maintain a safety management plan to meet the safety objectives described in its safety policy.					
4.e.	**Organization Structure & Responsibilities**					

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
4.e.(1)	Top management must have the ultimate responsibility for the SMS.					
4.e.(2)	Top management must provide resources essential to implement and maintain the SMS					
4.e.(3)	Top management must designate a management official to implement & maintain the SMS					
4.e.(4)	Responsibilities for aviation safety positions, duties and authorizations must be:			**NOTE:** The term Aviation Safety Position is **not defined** in Order VS 8000.367, nor in any of the FAA literature. The term is also **not defined** in the ICAO Safety Management Manual, Doc 9859.		this should not be required to be in a policy. A policy might define functions rather than position guides. The requirement is unwieldy and not necessary to execution of the functions
4.e.(4)(a)	defined					
4.e.(4)(b)	documented; and					
4.e.(4)(c)	communicated throughout the organization					
4.f.	**Compliance with Legal & Other Requirements**					
4.f.(1)	SMS must include a means of compliance with FAA policy, legal, regulatory & statutory requirements applicable to SMS				Same as 4b2d. Propose exception - strike requirement, this will then be consistent with ICAO language	There are existing means of compliance with legal, regulatory and statutory requirements of many kinds, within each organization. It is not clear why it adds value to uniquely identify those applicable to the SMS and address in safety policy.
4.f.(2)	The organization must establish & maintain a procedure to identify the current FAA policy, legal, regulatory & statutory requirements applicable to SMS				Same as 4b2d. Propose exception - strike requirement, this will then be consistent with ICAO language	There are existing means of compliance with legal, regulatory and statutory requirements of many kinds, within each organization. It is not clear why it adds value to uniquely identify those applicable to the SMS and address in safety policy.
4.g.	**Operational Procedures & Controls**					
4.g.(1)	The organization must establish procedures with measurable criteria to accomplish its safety policy & objectives as defined by the SMS				Further discussion needed to establish intent of requirement.	What is to be measured?
4.g.(2)	The organization must establish & maintain process controls to ensure procedures are followed for operations & activities as defined by the SMS				Further discussion needed to establish intent of requirement.	The intent is unclear. If we publish a policy and require employees to be familiar with it, and have all the systems in place for our SMS, what would be a process control? Not sure how this whole section would apply to design/manufacture.
4.h.	**Emergency Preparedness & Response**					
4.h.(1)	The organization must establish a plan for response to accidents & serious incidents					
4.h.(2)	effectiveness of the plan must be verified at intervals, either by response to real events or as an exercise					
4.i.	**Safety Documentation & Records**					
4.i.(1)	The organization must establish and maintain information, in paper or electronic form, to describe:					
4.i.(1)(a)	safety policies					
4.i.(1)(b)	safety objectives					
4.i.(1)(c)	SMS requirements					
4.i.(1)(d)	safety procedures and processes [Procedure - A specified way to carry out an activity or a process (ref: VS 8000.367 App A Definitions).] [Process - A set of interrelated or interacting activities that transforms inputs into outputs (ref: VS 8000.367 App A Definitions).]					

Order 8000.367 Appendix B	SUBJECT - TITLE	FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
4.i.(1)(e)	responsibilities & authorities for safety procedures & processes				
4.i.(1)(f)	interaction/interfaces between safety procedures & processes			Further discussion needed to establish intent of requirement.	The intent is not clear. What is the distinction between procedures and processes? What constitutes a safety process? Or is this all processes?
4.i.(2)	The organization must document SMS outputs in records.				
4.i.(3)	The organization must maintain docs & records in accordance with document and record managementt policies specified by the oversight organization.				
5	**Safety Risk Management (SRM)**				
5	SRM - A formal process within the SMS composed of describing the system, identifying the hazards, assessing the risk, analyzing the risk, and controlling the risk. The SRM process is embedded in the processes used to provide the product / service; it is not a separate / distinct process. (ref. Order, App A: Definitions)]	§§33.75, 25.571, 25.1309, 25.901c, etc.AC39-8	The regulations cited below define the process, criteria, validation and verification approaches for managing risk for a new type design engine or airplane, and in the case of the propulsion system, the process for managing risk for a product in service.	Design community already complies by requirements in column D, for new design. No further requirement needed for design community - new products	
		§33.75 Safety analysis	(a) (1) The applicant must analyze the engine, including the control system, to assess the likely consequences of all failures that can reasonably be expected to occur. This analysis will take into account, if applicable: (i) Aircraft-level devices and procedures assumed to be associated with a typical installation. Such assumptions must be stated in the analysis. (ii) Consequential secondary failures and latent failures. (3) The applicant must show that hazardous engine effects are predicted to occur at a rate not in excess of that defined as extremely remote (probability range of 10e(−7) to 10e(−9) [1per 10,000,000 engine flight hours to 1 per 1,000,000,000 flight hours]). Since the estimated probability for individual failures may be insufficiently precise to enable the applicant to assess the total rate for hazardous engine effects, compliance may be shown by demonstrating that the probability of a hazardous engine effect arising from an individual failure can be predicted to be not greater than 10e(−8) [1 per 100,000,000] engine flight hours.	Design community already complies for Propulsion COS , by AC39.8 as implemented.No further requirement needed for Propulsion COS.	

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
			§25.1309 Equipment, systems, and instalations	(a) The equipment, systems, and installations whose functioning is required by this subchapter, must be designed to ensure that they perform their intended functions under any foreseeable operating condition. (b) The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that— (1) The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable, and (2) The occurrence of any other failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.		
			AC 25.1309-1A System Design and Analysis	10. Quantitative Assessment. B. Quantitative Probability Terms. When using quantitative analyses to help determine compliance with § 25.1309(b), the following descriptions of the probability terms used in this regulation and this AC have become commonly-accepted as aids to engineering judgment. They are usually expressed in terms of acceptable numerical probability ranges for each flight-hour, based on a flight of mean duration for the airplane type. (1) Probable failure conditions are those having a probability greater than on the order of 1 X 10e(-5), [greater than 1 per 100,000 flight-hours}. (2) Improbable failure conditions are those having a probability on the order of 1 X 10e(-5) or less, but greater than on the order of 1 X 10e(-9) [less than 1 per 100,000 flight-hours, but greater than 1 per 1,000,000,000 flight-hours]. (3) Extremely Improbable failure conditions are those having a probability on the order of 1 X 10e(-9) or less [less than 1 per 1,000,000,000 flight-hours].		
			AC39-8	This AC also provides CAAM guidance for estimating the risks associated with identified unsafe conditions; defining, prioritizing, and selecting suitable corrective actions for all identified unsafe conditions; and verifying that the corrective actions were effective. This AC is intended to present a tangible means of logically assessing and responding to the safety risks posed by unsafe conditions.		
5.a.	**SRM must, at a minimum, include the following processes:**					

Order 8000.367 Appendix B	SUBJECT - TITLE	FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
5.a.(1)	describe system; [SYSTEM - An integrated set of constituent elements that are combined in an operational or support environment to accomplish a defined objective. These elements include people, hardware, software, firmware, information, procedures, facilities, services and other support facets. (ref. Order, App. A: Definitions)]		AC33.75 System refers to a combination of inter-related items arranged to perform a specific function(s).	Propose definition be revised to be more closely bounded.	The definition of 33.75 is far more applicable. The definition from the order is so broad, the task is unbounded and beyond today's analytical capabilities.
				Design community already complies by requirements in column D, for new design. No further requirement needed for design community - new products	
5.a.(2)	identify hazards; [Hazard - Any existing or potential condition that can lead to 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. (ref. Order, App. A: Definitions)]	§§33.75, 25.571, 25.1309, etc.AC39-8		Design community already complies by requirements in column D, for new design. No further requirement needed for design community - new products	
5.a.(3)	analyze safety risk; [Safety risk - The composite of predicted severity and likelihood of the potential effect o a hazard. (ref. Order, App. A: Definitions)]	§§33.75, 25.571, 25.1309, etc. AC39-8		Design community already complies by requirements in column D, for new design. No further requirement needed for design community - new products	
5.a.(4)	assess safety risk; and	§§33.75, 25.571, 25.1309, etc.AC39-8		Design community already complies by requirements in column D, for new design. No further requirement needed for design community - new products	
5.a.(5)	control/mitigate safety risk	§21.50 Instructions for continued airworthiness	ICA includes Airworthiness Limitations section, an element of the type design per §21.31(c), and servicing information, scheduling information which provides recommended periods for cleaning, inspecting, adjusting, testing, lubricating, wear tolerances, troubleshooting, and list of tools and equipment.	Design community already complies by requirements in column D, for new design. No further requirement needed for design community - new products	
		AC39-8	Contains criteria for determining, for the propulsion system, whether an unsafe condition exists; acceptable probability/severity criteria, time limits for mitigation of the condition, guidance on validation of any statistical model of the risk condition, and verification of the effectiveness of the mitigating action. AC39-8 completely meets the intent of the safety risk management and safety assurance aspects of SMS, once the propulsion system has entered service.	Design community already complies for Propulsion COS , by AC39.8 as implemented.No further requirement needed for Propulsion COS.	

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
5.b.	**The elements of the SRM process must be applied, either qualitatively, or quantitatively, to:**					
5.b.(1)	initial designs of systems, organizations & products; [System - An integrated set of constituent elements that are combined in an operational or support environment to accomplish a defined objective. These elements include people, hardware, software, firmware, information, procedures, facilities, services and other support facets) *.			**SYSTEMS:** The foundation of civil aviation in the U.S. is **airworthiness;** conformance to type certificate for products and conformance to type design for component parts of products, and in condition for safe operation. Products (type certificated aircraft, aircraft engines, and propellers and all parts comprising those products) are designed according to the appropriate **Airworthiness** Standards: 14CFR Part 23 for Normal, Utility, Acrobatic, and Commuter Category Airplanes; Part 25 for Transport Category Airplanes; Part 27 for Normal Category Rotorcraft, Part 29 for Transport Category Rotorcraft; and, Part 33 for Aircraft Engines. The products are type certificated according to the stringent requirements contained in 14CFR Part 21 - Certification Procedures for Products and Parts.	Design community already complies by requirements in column D, for new design. No further requirement needed for design community - new products	
				Specifically, safety analyses are conducted on engines (33.75), propulsion systems (25.901c), and all airplane systems (25.1309) to ensure that they meet acceptable hazard probability/severity criteria before the product can be certified.		
				AC33.75 System refers to a combination of inter-related items arranged to perform a specific function(s).		The definition of 33.75 is far more applicable. The definition from the order is so broad, the task is unbounded and beyond today's analytical capabilities.
				ORGANIZATIONS:		
						There is no mandate for the FAA to approve the "design of organizations"

Order 8000.367 Appendix B	SUBJECT - TITLE	FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
			PRODUCTS: A newly manufactured aircraft is issued its original **airworthiness** certificate when it is found to conform to its type design and to be in condition for safe operation. At that time, it meets the safety criteria defined in the regulations. (ref. §21.183(a) & (b)) When it enters service, maintaining its **airworthiness**, i.e. maintaining conformance to its type certificate (and for all installed component parts, maintaining their conformance to their respective type designs), and its condition for safe operation, lies in the realm of the maintenance provider. The primary means of continuing the **airworthiness** of in-service aircraft is by using "the methods, techniques, and practices prescribed in the current manufacturer's maintenance manual or **Instructions for Continued Airworthiness** (required by §21.50) prepared by its manufacturer." (ref. §43.13(a))		
			Type certificate holders may have Continued Operational Safety Processes agreed with the FAA, such as those defined in AC39-8.		
5.b.(2)	the development of safety operational procedures;			Propose requirement be struck, for Design and manufacturing sectors	: it is not possible to apply the full SRM process to development of operational procedures. If "operational procedures" means the customer's use of the product, the data to quantify risk does not exist; instead operational procedures are developed using precedent, pilot's experienced judgment and knowledge of past Lessons Learned. If "operational procedures" means design company internal processes, it is truly impossible to quantify risk associated with a change. (e.g what is the change in risk by having a design review conducted by phone/Webex, rather than with physical presence?) Similarly, what is the risk in manufacturing of using grinding machine A vs B?
5.b.(3)	hazards [Hazard – Any existing or potential condition that can lead to 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.(ref App A Definitions, Order VS 8000.367)] that are identified in the safety assurance functions - described in Chapter 6.	§21.3 Reporting of failures, malfunctions, and defects	(a) Except as provided in paragraph (d) of this section, the holder of a Type Certificate (including a Supplemental Type Certificate), a Parts Manufacturer Approval (PMA), or a TSO authorization, or the licensee of a Type Certificate shall report any failure, malfunction, or defect in any product, part, process, or article manufactured by it that it determines has resulted in any of the occurrences listed in paragraph (c) of this section.	Already complies for the design sector by the type certification safety analysis. Already complies for the manufacturing sector via the QMS processes in place (corrective action taken for non-conformances)	
		§145.221 Service difficulty reports			

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
5.b.(4)	planned changes to the productional/operational system, including introduction of new products & procedures, to identify hazards associated with those changes			Introduction of new products is controlled by type certification or by the design change system.?8110 form?	Already complies for the manufacturing sector, via part 21 QMS requirements. Already complies for the design sector, via type certification and by design change system.	Changes to the production system are already addressed by the quality system. Design changes are validated and certified by CCMM. These processes provide assurance that unintended effects will not result. Addition of a SRM element would not be practicable (the data do not exist to support analyses) or added value.
5.c.						
5.c.	The organization must establish feedback loops between assurance functions (described in Ch 6) to evaluate the effectiveness of safety risk controls [ref Fig B-1]					
5.d.	**The organization must define a process for risk acceptance**					
5.d.(1)	The organization must define acceptable and unacceptable levels of safety risk			The only risk acceptance in all of 14CFR is related to certain flight test certification items, and when issuing a Special Flight Permit (§21.197), or special flight authorization i/a/w §91.715. At all other times, all civil aircraft must be airworthy (conform to type certificate/type design and be in condition for safe operation (ref. §91.7). That is to say, there is no decision to accept or reject a risk or hazard; type certificated products, and all components, appliances and parts installed thereon MUST be airworthy.	Propose modification - "….acceptable levels of safety risk (may be set by regulation)" Already complies for Design, via type design safety analysis. Already complies for manufacturing, via QMS process	Acceptable levels of risk must be provided by the oversight organization, to ensure a consistent level of safety throughout the system and to provide legal protection to the organization.
				Acceptable risk levels for product certification are defined in CFR33.75, 25.1309; acceptable risk levels for continued airworthiness are defined in AC39-8.		
5.d.(2)	The organization must define levels of management able to make safety risk acceptance decisions				Propose modification "able to review safety risk against defined acceptable levels"	Internal policy defines levels of management to review risk, but the FAA has final authority on whether risk level is acceptable. For instance, the FAA has not given manufacturers the authority to decide whether or not Airworthiness Directives should be written.

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
5.d.(3)	The organization must define level of safety risk that is acceptable in the short-term, while long-term safety risk control/mitigation plans are developed and implemented.			Safety risk (The composite of predicted severity and likelihood of the potential effect of a hazard. (ref. Order VS 8000.367, App. A: Definitions)) is **NOT** an element of continuing airworthiness / maintenance. **Airworthiness** Standards, including Parts 23, 25, and 33, contain quantitative design requirements to ensure safe flight and landing in the event that any failure condition occurs. Those requirements are contained in a product's type certificate, an element of airworthiness. The **Instructions for Continued Airworthiness** (also part of the type certificate, and required by §21.50(b)), through the exhaustive Maintenance Review Board process (for transport category aircraft) are developed to ensure realization of the inherent safety and reliability levels of the equipment (as designed, certificated, and manufactured); and to restore safety and reliability to their inherent levels when deterioration has occurred.	Propose modification - "….(acceptable levels may be set by regulation)"	
				Acceptable short-term risk levels for continued airworthiness are defined in AC39-8, as are parameters for the introduction /implementation of mitigation plans.	Already complies for propulsion, via AC39.8 as implemented.	
5.e.						
5.e.	If applicable, the organization must establish procedures to obtain oversight organization approval for those planned changes that require oversight approval prior to implementation (in accordance with Chapter 4, Section f).			Procedures already exist for obtaining oversight approval to design changes (8110).	Already complies for manufacturing via QMS process. Already complies for design, via design change process.	
5.f.						
5.f.	The safety risk of identified hazards must be deemed acceptable prior to implementation of the following items in the production/operational system: [SYSTEM - An integrated set of constituent elements that are combined in an operational or support environment to accomplish a defined objective. These elements include people, hardware, software, firmware, information, procedures, facilities, services and other support facets. (ref. Order, App. A: Definitions)]					
5.f.(1)	new system designs;			Compliance with the risk levels defined in 25.1309, 25.901c and 33.75,as applicable, is already a certification requirement.	Already complies for design via the type certification process	already addressed for design organizations by the certification process
5.f.(2)	changes to existing system designs;			?the 8110 process already ensures that changes to existing designs do not increase the level of risk beyond that required for initial certification.	Already complies for design, via the design change process.	

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
5.f.(3)	new operations/procedures; and				The concept of operations/procedures is not clear in the context of a design organization's SMS. Provided that the design is safe, the organizations procedures do not involve risk. The term "operations " is not understood in this context. Manufacturing already complies via the QMS process	the intent is unclear. Risk assessment is not practicable for operations/procedures, as discussed above.
5.f.(4)	modified operations/procedures				The concept of operations/procedures is not clear in the context of a design organization's SMS. Provided that the design is safe, the organizations procedures do not involve risk. The term "operations " is not understood in this context. Manufacturing already complies via the QMS process	
5.g.						
5.g.	The SRM process may allow AVS or AVS services/offices to take interim immediate action to mitigate existing safety risk.		§39.5 When does FAA issue airworthiness directives?	FAA issues an airworthiness directive addressing a product when we (FAA) find that: (a) An unsafe condition exists in the product; and (b) The condition is likely to exist or develop in other products of the same type design.	This provision allows action by the FAA, it is not a requirement placed upon the design organization. It should not appear in this document.	
			§21.99 Required design changes	(a) When an Airworthiness Directive is issued under Part 39 the holder of the type certificate for the product concerned must— (1) If the Administrator finds that design changes are necessary to correct the unsafe condition of the product, and upon his request, submit appropriate design changes for approval; and (2) Upon approval of the design changes, make available the descriptive data covering the changes to all operators of products previously certificated under the type certificate. (b) In a case where there are no current unsafe conditions, but the Administrator or the holder of the type certificate finds through service experience that changes in type design will contribute to the safety of the product, the holder of the type certificate may submit appropriate design changes for approval. Upon approval of the changes, the manufacturer shall make information on the design changes available to all operators of the same type of product.	21.99 already empowers the FAA to do this.	
5.h.						

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
5.h.	Describe System. The system description must be completed to the level necessary to identify hazards. [Hazard – Any existing or potential condition that can lead to 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. (ref. Order, App. A; Definitions)]			5h,i, j, k, only repeat the provisions of 5a. The responses and existing regulations for 5a apply.		
5.i.						
5.i.	Identify Hazards. Hazards must be identified within the system as described in Section h (above).			As indicated immediately above, hazards are identified and analyzed, and their effects are considered in the design and certification of engines. When risks exceed the acceptable levels defined in part 33 and 25 regulations, their effects are mitigated , as required for product certification.		
5.j.	Analyze Safety Risk. The process must include analyses of:			As indicated immediately above, hazards are identified and analyzed, and their effects are considered in the design and certification of engines. When risks exceed the acceptable levels defined in part 33 and 25 regulations, their effects are mitigated , as required for product certification.		
5.j.(1)	existing safety risk controls [Safety risk control – A characteristic of a system that reduces safety risk. Controls may include process design, equipment modification, work procedures, training or protective device.(ref. App A Definitions, Order VS 800.367)];					
5.j.(2)	contributing factors; and					
5.j.(3)	the safety risk of reasonably likely outcomes from the existence of a hazard, to include estimation of the:					
5.j.(3)(a)	likelihood and					
5.j.(3)(b)	severity					
5.k	Assess Safety Risk. [Safety risk – The composite of predicted severity and likelihood of the potential effect o a hazard.(ref. App A Definitions, Order VS 8000.367)]			As indicated immediately above, hazards are identified and analyzed, and their effects are considered in the design and certification of engines. When risks exceed the acceptable levels defined in part 33 and 25 regulations, their effects are mitigated , as required for product certification.		
5.l.	Control/Mitigate Safety Risk.			As indicated immediately above, hazards are identified and analyzed, and their effects are considered in the design and certification of engines. When risks exceed the acceptable levels defined in part 33 and 25 regulations, their effects are mitigated , as required for product certification.		
5.l.(1)	Safety risk control/mitigation plans must be defined for hazards identified with unacceptable risk.					

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
5.l.(2)	Substitute risk [Substitute risk – Risk unintentionally created as a consequence of safety risk control(s) [Safety risk control – A characteristic of a system that reduces safety risk. Controls may include process design, equipment modification, work procedures, training or protective device.].(ref App A Definitions, Order VS 8000.367)] must be evaluated in the creation of safety risk controls/mitigations				Propose requirement be struck.	The evaluation of substitute risk is beyond the state of the art. There is no means to fully comply with this requirement
5.l.(3)	Safety risk control/mitigation must be evaluated to ensure that safety rqmts have been met					
5.l.(4)	when safety risk control/mitigation plans are implemented, they must be monitored to ensure that safety risk controls have the desired effect.					
6.00	**Safety Assurance [Ref Ch 4 of the Order]**					
6.a.	**General Requirements. The organization must monitor its systems, operations and products/services to:**					
6.a.(1)	Identify new hazards;		§21.3 Reporting of failures, mallfunctions, and defects	(a) Except as provided in paragraph (d) of this section, the holder of a Type Certificate (including a Supplemental Type Certificate), a Parts Manufacturer Approval (PMA), or a TSO authorization, or the licensee of a Type Certificate shall report any failure, malfunction, or defect in any product, part, process, or article manufactured by it that it determines has resulted in any of the occurrences listed in paragraph (c) of this section.	Already addressed by 21.3 for Design and manufacturing sectors.	There is no requirement for organizations to be aware of product failures in service. In many cases, there is no mechanism for them to become informed of such events. Operators are not required to report to the manufacturer or design organization
			§21.99 Required design changes	(a) When an Airworthiness Directive is issued under Part 39 the holder of the type certificate for the product concerned must— (1) If the Administrator finds that design changes are necessary to correct the unsafe condition of the product, and upon his request, submit appropriate design changes for approval; and (2) Upon approval of the design changes, make available the descriptive data covering the changes to all operators of products previously certificated under the type certificate.		
6.a.(2)	Measure the effectiveness of safety risk controls [Safety risk control – A characteristic of a system that reduces safety risk. Controls may include process design, equipment modification, work procedures, training or protective device. (ref. App A Definitions, Order VS 8000.367)];			The process defined in AC39-8 includes verification that safety risk controls are effective in mitigating the risk being addressed.	Already addressed for Propulsion by AC 39.8 as implemented.	
6.a.(3)	Assess compliance with legal, regulatory & statutory requirements applicable to the SMS; and				See4b2d. Propose exception - strike requirement, this will then be consistent with ICAO language	

Order 8000.367 Appendix B	SUBJECT - TITLE	FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
6.a.(4)	Assess conformity with organizational safety policies & procedures				
6.b.	**Information Acquisition**				
6.b.(1)	The organization must collect data/information necessary to demonstrate the effectiveness of the SMS			This is a new requirement and potentially very burdensome, especially to the sectors of general aviation and business/air-taxi.	
6.b.(2)	The organization must monitor operational data/information.				
6.b.(3)	The organization must monitor products & services received from contractors			Already required for manufacturing by QMS requirements. Already required for Design by type certification safety analysis.	
6.c.	**Employee Reporting System**				
6.c.(1)	The organization must establish & maintain an employee reporting system in which employees can report hazards, issues, concerns, occurrences, occurrences, incidents, etc., as well as propose solutions/safety improvements				
6.c.(2)	Employees must be encouraged to use the employee reporting system without reprisal (footnote 6: This does not restrict management from taking action in cases of gross negligence or willful operation outside the organization's safety requirements)				
6.d.	**Investigation**				
6.d.(1)	The organization must establish criteria for which accidents & incidents will be investigated.		In both federal law and in Order VS 8000.367, accidents and incidents pertain to aircraft flight operation only, not to maintenance, or administrative, operations. See 4.h.(1), above.		
6.d.(2)	The organization must establish procedures to:				
6.d.(2)(a)	investigate accidents				
6.d.(2)(b)	investigate incidents; and				
6.d.(2)(c)	investigate instances of suspected non-compliance with safety regulations.			Propose exception; this is not appropriate to Design and Manufacturing environment.	This requirement is directed at carrier operations and is not appropriate for design/manufacture/repair. Strong corrective processes already exist for production and repair services. For design and continued airworthiness, the FAA makes a compliance finding, not the manufacturer.
6.e.	**Auditing of the Production/Operational System**				

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
6.e.(1)	The organization must ensure that regular audits of production/operational system's safety functions are conducted with priority on the areas of highest safety risk. This obligation must extend to any contractors the organization may use to accomplish those functions. (Footnote 8: The organization can choose to conduct audits of its contractors or require that contractors conduct their own audits and provide the resultant data/information to the organization.)			~~Safety risk (The composite of predicted severity and likelihood of the potential effect of a hazard. (ref. Order VS 8000.367, App. A: Definitions)) is~~ **~~NOT~~** ~~an element of continuing~~**~~airworthiness~~** ~~/ maintenance. Airworthiness Standards, including Parts 23, 25, and 33, contain quantitative design requirements to ensure safe flight and landing in the event that any failure condition occurs. Those requirements are contained in a product's type certificate, an element of airworthiness. The~~ **~~Instructions for Continued Airworthiness~~** ~~(also part of the type certificate, and required by §21.50(b)), through the elaborate Maintenance Review Board process (for transport category aircraft) are developed to ensure realization of the inherent safety and reliability levels of the equipment (as designed, certificated, and manufactured); and to restore safety and reliability to their inherent levels when deterioration has occurred.~~	Need discussion in order to understand intent of requirement.	the term “audit” may not be appropriate.
						It is not clear what is meant by “safety function”. Organizational branches tagged as “safety”? They do not introduce safety risk, their job is to reduce risk, so why audit them? Or organizations whose activities result in a safe product? That would be almost the entire business…
					The intent of the phrase "safety function" is not clear with respect to a design organization. The design organization produces safe products by ensuring that the products work, meet the design intent, and are certified. In that sense, every engineer performs a "safety function". The safety organization typically performs oversight. It does not introduce "safety risk". Auditing the bsafety organization does not appear to directly support the overall intent of designing safe products.	Comment: The extent of applicability of an SMS is not clear, but any organization with an SMS should be “audited” by itself or by the FAA. TC holders should not be tasked with policing the internal processes of other companies, nor is it practicable to require this – subcontractors would then be audited multiple times by different customers, to subtly different requirements.
6.e.(2)	The organization must ensure regular audits are conducted to:					

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
6.e.(2)(a)	determine conformity with safety risk controls; and [Safety risk control – A characteristic of a system that reduces safety risk. Controls may include process design, equipment modification, work procedures, training or protective device. (ref App A Definitions, Order VS8000.367)]			Safety risk (The composite of predicted severity and likelihood of the potential effect of a hazard. (ref. Order VS 8000.367, App. A: Definitions)) is **NOT** an element of continuing airworthiness / maintenance. Airworthiness Standards, including Parts 23, 25, and 33, contain quantitative design requirements to ensure safe flight and landing in the event that any failure condition occurs. Those requirements are contained in a product's type certificate, an element of airworthiness. The Instructions for Continued Airworthiness (also part of the type certificate, and required by §21.50(b)), through the elaborate Maintenance Review Board process (for transport category aircraft) are developed to ensure realization of the inherent safety and reliability levels of the equipment (as designed, certificated, and manufactured); and to restore safety and reliability to their inherent levels when deterioration has occurred.	Need discussion in order to understand intent of requirement.	The requirement could not be interpreted in the context of a design organization.
					The intent of the phrase "safety risk control" is not clear with respect to a design organization. The design organization produces safe products by ensuring that the products work, meet the design intent, and are certified. Provided this is done, there is no need for "safety risk controls", they are frozen into the design.	
				For continued operational safety - if an unsafe condition is identified in the design - AC39-8 clearly defines the process for introducing mitigating action and ensuring that it is effective.		
6.e.(2)(b)	assess performance of safety risk controls			For continued operational safety - if an unsafe condition is identified in the design - AC39-8 clearly defines the process for introducing mitigating action and ensuring that it is effective.	Propulsion already complies by AC 39.8 as implemented.	
6.e.(3)	Auditing may be done at planned intervals or as a continuing process					
6.f.	**Evaluation of the SMS** [(SMS) – The formal, top-down business-like approach to managing safety risk. It includes systematic procedures, practices, and policies for the management of safety (as described in this document it includes Safety Risk Management, safety policy, safety assurance, and safety promotion). (ref App A Definitions, Order VS8000.367)]					

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
6.f.(1)	The organization must conduct evaluations of the SMS to determine if the SMS conforms to requirements.					
6.f.(2)	Evaluations may be done at planned intervals or as a continuing process.					if the SMS meets requirements during an initial evaluation, why are further evaluations required? What would have changed?
6.g.						
6.g.	Audits by Oversight Organization. If applicable, the organization must include the results of oversight organization audits in the data/information analyses conducted as described in Section h.					
6.h.						
6.h.	Analysis of Data/Information The organization must analyze the data/information described in Section b.				Analysis of Propulsion operational data is already required in AC39.8 as implemented	some of this data may require analysis, but not necessarily all of it.
6.i.	**System Assessment**					
6.i.(1)	The organization must assess the performance of:				Compliance not possible until SMS is in place	
6.i.(1)(a)	the production/operational system's safety functions against its safety requirement(s) as defined by the SMS and				Compliance not possible until SMS is in place	
6.i.(1)(b)	the SMS against its requirements				Compliance not possible until SMS is in place	
6.i.(2)	System assessments must result in the documentation of:					
6.i.(2)(a)	conformity with existing safety risk control(s)/SMS requirement(s) (including legal, regulatory, & statutory requirements applicable to the SMS);					
6.i.(2)(b)	nonconformity with existing safety risk control(s)/SMS requirement(s) (including legal, regulatory & statutory requirements applicable to the SMS);					
6.i.(2)(c)	potential ineffective control(s); and					
6.i.(2)(d)	potential hazard(s) found.					
6.i.(3)	The SRM process must be utilized if the assessment identifies:					
6.i.(3)(a)	potential hazards or					
6.i.(3)(b)	the need for production/operational system changes					
6.j.						
6.j.	Corrective Action. When nonconformities are identified, the organization must prioritize and implement corrective actions				Manufacturing already complies via QMS requirements. Design already complies via disclosure on non-compliance process.	
6.k.	**Management Reviews**					
6.k.(1)	Top management must conduct regular reviews of SMS effectiveness				Compliance not possible until SMS is in place	
6.k.(2)	Management reviews must assess the need for changes to the SMS				Compliance not possible until SMS is in place	
7	**Safety Promotion [Ref Ch 6 of the Order]**					

Order 8000.367 Appendix B	SUBJECT - TITLE		FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
7.a.	**Safety Culture.**					
7.a.	Safety Culture. Top management must promote the growth of a positive safety culture demonstrated by, but not limited to:					
7.a.(1)	publication to all employees of sr. mgt's stated commitment to safety;					
7.a.(2)	communication of safety responsibilities with the organization's personnel to make each employee part of the safety process;					
7.a.(3)	Clear & regular communications of safety policy, goals, objectives, standards & performance to all employees of the organization;				Propose discussion of how this is effective and appropriate in design and manufacturing communities, before levying a requirement.	before setting requirements for safety promotion, it should be clear how the requirement will support the objective. It is not clear how this requirement will change employee behavior in the design/manufacture/repair sector. Manufacturing employees know, and take very seriously, the requirement to produce parts to print. Communicating safety policy, goals and objectives will not affect this in any way.
7.a.(4)	an effective employee reporting system that provides confidentiality and de-identification as appropriate (as described in Chapter 6, Section c);					
			§193.1 What does this part cover?	This part describes when and how the FAA protects from disclosure safety and security information that you submit voluntarily to the FAA. This part carries out 49 U.S.C. 40123, protection of voluntarily submitted information.		
			§193.9 Will the FAA ever disclose information that is designated as protected under this part?	The FAA discloses information that is designated as protected under this part when withholding it would not be consistent with the FAA's safety and security responsibilities, as follows: (a) Disclosure in all programs. (1) The FAA may disclose de-identified, summarized information submitted under this part to explain the need for changes in policies and regulations. An example is the FAA publishing a notice of proposed rulemaking based on your information, and including a de-identified, summarized version of your information (and the information from other persons, if applicable) to explain the need for the notice of proposed rulemaking.		
7.a.(5)	use of safety information system that provides accessible, efficient means to retreive information; and					
7.a.(6)	allocation of resources to implement & maintain the SMS					
7.b.	**Communication and Awareness**					

Order 8000.367 Appendix B	SUBJECT - TITLE	FAR Part 21 & as indicated	SUBJECT - TITLE	Exceptions Assessment (i.e. limits of applicability)	Comments/Notes
7.b.(1)	The organization must communicate SMS outputs to employees as appropriate [SMS Output - The result or product of an SMS process. In this context, the result of a process, which is intended to meet a requirement described in this Standard (e.g., results of safety risk analyses, safety audits, and safety investigations) Order VS 8000.367, Appendix A: Definitions]			Compliance not possible until SMS is in place	
7.b.(2)	If applicable, the organization must provide access to the SMS outputs to its oversight organization, in accordance with established agreements & disclosure programs			Compliance not possible until SMS is in place	
7.b.(3)	The organization must ensure that affected employees & external stakeholders (including its oversight organization, if applicable) are aware of the short-term safety risk of hazards that may exist in the production/operational system while safety risk control/mitigation plans are developed & implemented (as described in Chapter 5, Section d3)		The only possible meaning of hazard is with respect to any existing or potential condition that could lead to injury, illness or death to people during the operation of a civil aircraft. The damage to or loss of a system, equipment, or property likewise is with respect to the operation of civil aircraft. Flying on civil aircraft is not part of the normal duties of a design engineer; employees of design organizations are no more exposed to short term safety risks while hazards are being mitigated than is the general public. It is not clear whether this requirement directs that short-term safety risks be communicated to the general public, nor what means would be used to do so.	Interpretation required.	
7.c.	**Personnel Competency**				
7.c.(1)	The organization must document competency requirements for those positions identified in (App B) Ch 4, Sect. e4. [Aviation Safety Positions]		**NOTE:** The term Aviation Safety Position is **not defined** in Order VS 8000.367, nor in any of the FAA literature. The term is also **not defined** in the ICAO Safety Management Manual, Doc 9859. It is assumed that it refers to those whose primary duties are focused specifically on aviation safety, rather than normal design.		It is not clear that documenting competency requirements is an appropriate approach. It is not clear who, in the organization, is able to assess competency in the specialized area of safety engineering, and how their competency to do so is to be assessed. The phrase "key competencies" might be more applicable than competency requirements.
7.c.(2)	The organization must ensure that individuals in the positions identified in (App B) Ch 4, Sect. e4 meet the documented competency requirements.				
7.d.	**Safety Knowledge Management.**				
7.d.	Safety Knowledge Management. The SMS must include a process to capture knowledge of safety and incorporate it into future products, services and practices as appropriate.				
8	**Interoperability**				
8	Interoperability [Ref Ch 7 of the Order] The organization's SMS must be able to interoperate with other organizations' SMSs to manage cooperatively issues of mutual concern.			Interpretation required.	It is not clear how compliance to this requirement can be shown by any one organization, since it depends on the interaction of multiple organizations.

ganization: (ICAO) SMS Requirements Gap Analysis and Exceptions Assessment
2009

ICAO Requirements	Regulatory References	Text	Comments/Notes
1.1 Management commitment and responsibility	21.135	Each applicant for or holder of a production certificate must provide the FAA with a document describing how its organization will ensure compliance with the provisions of this subpart. At a minimum, the document must describe assigned responsibilities and delegated authority, and the functional relationship of those responsible for quality to management and other organizational components	The ICAO checklist for this element suggests a number of other items that could be addressed, but that are not addressed by US regulations, such as (1) A clear statement about the provision of the necessary resources for the implementation of the safety policy, (2) Safety reporting procedures, (3) Signature of the Accountable Executive, (4) Communication throughout the entire Organization, (5) Periodic review to ensure the policy remains relevant and appropriate, (6) A formal process for developing a coherent set of safety objectives, (7) A link between the safety objectives and the safety performance indicators, safety performance targets and action plans
1.2 Safety accountabilities	21.135	Each applicant for or holder of a production certificate must provide the FAA with a document describing how its organization will ensure compliance with the provisions of this subpart. At a minimum, the document must describe assigned responsibilities and delegated authority, and the functional relationship of those responsible for quality to management and other organizational components.	Although there is a requirement to specify in writing the assigned responsibilities, there is no requirement to specify an accountable executive; however it does appear that there is a requirement to document safety responsibilities, accountabilities and authorities
1.3 Appointment of key safety personnel	21.135	Each applicant for or holder of a production certificate must provide the FAA with a document describing how its organization will ensure compliance with the provisions of this subpart. At a minimum, the document must describe assigned responsibilities and delegated authority, and the functional relationship of those responsible for quality to management and other organizational components.	ICAO describes this as a requirement that the safety authorities, responsibilities and accountabilities of personnel at all levels of the organization be defined and documented
	21.137(h)(1)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (h)(1) Procedures to ensure that only products or articles that conform to their approved design are installed on a type-certificated product. These procedures must provide for the identification, documentation, evaluation, segregation, and disposition of nonconforming products and articles. Only authorized individuals may make disposition determinations.	
1.4 Coordination of emergency response planning		THERE IS NO PART 21 REQUIREMENT FOR EMERGENCY RESPONSE PLANNING BY A PRODUCTION APPROVAL HOLDER	ICAO describes this as a requirement for an emergency response contingency plan

ICAO Requirements	Regulatory References	Text	Comments/Notes
1.5 SMS documentation	21.135	Each applicant for or holder of a production certificate must provide the FAA with a document describing how its organization will ensure compliance with the provisions of this subpart. At a minimum, the document must describe assigned responsibilities and delegated authority, and the functional relationship of those responsible for quality to management and other organizational components.	The existing regulations do not require the specific SMS elements, like risk analysis, to be described in the context of their SMS identifiers, but the elements of SMS exist in the written production system.
	21.137	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: ETC.	
2.1 Hazard identification	21.137(n)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (n) Quality escapes. Procedures for identifying, analyzing, and initiating appropriate corrective action for products or articles that have been released from the quality system and that do not conform to the applicable design data or quality system requirements.	ICAO anticipates that companies will have a formal safety data collection and processing system for actively seeking and effectively collecting information about hazards. 21.137(g) provides the foundation for collecting internal data that would support hazard identification, but there is no affirmative obligation to engage in hazard identification. 21.137(n) is reactive to quality escapes. 21.137(m) responds to data from in-service operations, but it could be accused of being inadequately proactive.
	21.137(g)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (g) *Inspection and test status.* Procedures for documenting the inspection and test status of products and articles supplied or manufactured to the approved design.	
	21.137(m)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (m) *In-service feedback.* Procedures for receiving and processing feedback on in-service failures, malfunctions, and defects. These procedures must include a process for assisting the design approval holder to— (1) Address any in-service problem involving design changes; and (2) Determine if any changes to the Instructions for Continued Airworthiness are necessary.	

ICAO Requirements	Regulatory References	Text	Comments/Notes
2.2 Safety risk assessment and mitigation	21.3(f)	(f) If an accident investigation or service difficulty report shows that a product or article manufactured under this part is unsafe because of a manufacturing or design data defect, the holder of the production approval for that product or article must, upon request of the FAA, report to the FAA the results of its investigation and any action taken or proposed by the holder of that production approval to correct that defect. If action is required to correct the defect in an existing product or article, the holder of that production approval must send the data necessary for issuing an appropriate airworthiness directive to the appropriate aircraft certification office.	Safety risk assessment is required under 21.137(h) and 21.137(n), as well as under 21.137(m) which requires proceduresfor "processing feedback." 21.137(h) addresses procedures for preventing non-conformities (an example of safety risk mitigation) and it also requires the identification evaluation, etc of nonconformities. 21.3 implies an additional obligation to make an investigation and report it to the FAA, but only upon the request of the FAA.
	21.137(h)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (h) *Nonconforming product and article control.* (1) Procedures to ensure that only products or articles that conform to their approved design are installed on a type-certificated product. These procedures must provide for the identification, documentation, evaluation, segregation, and disposition of nonconforming products and articles. Only authorized individuals may make disposition determinations.	
	21.137(i)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (i) *Corrective and preventive actions.* Procedures for implementing corrective and preventive actions to eliminate the causes of an actual or potential nonconformity to the approved design or noncompliance with the approved quality system.	
	21.137(m)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (m) *In-service feedback.* Procedures for receiving and processing feedback on in-service failures, malfunctions, and defects. These procedures must include a process for assisting the design approval holder to— (1) Address any in-service problem involving design changes; and (2) Determine if any changes to the Instructions for Continued Airworthiness are necessary.	
	21.137(n)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (n) Quality escapes. Procedures for identifying, analyzing, and initiating appropriate corrective action for products or articles that have been released from the quality system and that do not conform to the applicable design data or quality system requirements.	

ICAO Requirements	Regulatory References	Text	Comments/Notes
3.1 Safety performance monitoring and measurement	21.137(g)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (g) *Inspection and test status.* Procedures for documenting the inspection and test status of products and articles supplied or manufactured to the approved design.	ICAO is looking for the organization to verify its safety performance in reference to the safety performance indicators and safety performance targets of the SMS. This should include auditting, ongoing analysis of data, and monitoring the efectiveness of solutions. 21.137(g) provides the internal data collection to support this function. 21.137(l) provides internal auditing to maintain compliance to the identified safety goals of the production system
	21.137(l)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (l) *Internal audits.* Procedures for planning, conducting, and documenting internal audits to ensure compliance with the approved quality system. The procedures must include reporting results of internal audits to the manager responsible for implementing corrective and preventive actions.	
3.2 The management of change	21.137(a-b)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (a) Design data control. Procedures for controlling design data and subsequent changes to ensure that only current, correct, and approved data is used. (b) Document control. Procedures for controlling quality system documents and data and subsequent changes to ensure that only current, correct, and approved documents and data are used.	ICAO anticipate sthat there will be a process for analyzing proposed changes to the system, to make sure that the safety elements of the system will not be compromised by the change. 21.137(a) and 21.137(b) anticipate change mangement sufficient to ensure that data is FAA-approved and documents are current
3.3 Continuous improvement of the SMS	21.137(i)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (i) *Corrective and preventive actions.* Procedures for implementing corrective and preventive actions to eliminate the causes of an actual or potential nonconformity to the approved design or noncompliance with the approved quality system.	There are two halves to this. First, ICAO anticipates that the organization will implement a system to identify and mitigate substandard performance of the SMS (continuous improvement until SMS standards are met). The second half is about continuous improvement beyond established standards. The first half is addressed in 21.137(i) and 21.137(l), which require auditing and corrective/preventative action, but there is no regulatory element requiring continuous improvement beyond the standards of compliance. There is no regulatory element requiring continuous improvement beyond the standards of compliance. Such an element would be diffficult to measure as an objective standard, and would run the risk of failing to set an objective standard for regulation, andmay be considered unenforceable under the "void for vagueness" doctrine. Thus such an element may need to be omitted from the US regulations.
	21.137(l)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (l) *Internal audits.* Procedures for planning, conducting, and documenting internal audits to ensure compliance with the approved quality system. The procedures must include reporting results of internal audits to the manager responsible for implementing corrective and preventive actions.	

ICAO Requirements	Regulatory References	Text	Comments/Notes
4.1 Training and education		THERE IS NO PART 21 REQUIREMENT FOR TRAINING AND EDUCATION BY A PRODUCTION APPROVAL HOLDER	ICAO anticipates identification of training needs, implementation of training (including SMS training), and assesment of effectiveness of training. Perhaps there should be a requirement that PAHs train their personnel in operation under the Hazard Identification and Risk Assesment elements of the system.
4.2 Safety communication.	21.137(c)	Each applicant for or holder of a production certificate must establish and describe in writing a quality system that ensures that each product and article conforms to its approved design and is in a condition for safe operation. This quality system must include: (c) *Supplier control*. Procedures that— (1) Ensure that each supplier furnished product or article conforms to its approved design; and (2) Require each supplier to report to the production approval holder if a product or article has been released from that supplier and subsequently found not to conform to the applicable design data.	ICAO anticipates communication processes within the organization that permit the safety management system to function effectively. 21.137(c)(1) helps to ensure flow-down of information to suppliers and 21.137(c)(2) helps to ensure flow-up of hazard data from suppliers. 21.137(d) helps to ensure flow of information within the organization

Extent of Regulatory Gap Analysis between Part 21 Productino and Design Requirements and ICAO SMS Framework

Version: February 16, 2010			Production	Production	Design	Design
ICAO Elements	**ICAO Requirements**		**Summary (Product Safety SMS)**	**Summary (Organizational factors SMS)**	**Summary (Product Safety SMS)**	**Summary (Organizational factors SMS)**
1. Safety Policy						
			Premise: in a production system, making a conforming product implies making a safe product. Therefore, requirements addressing the quality management system are also effective in addressing product safety.			
	1.1 Management commitment and responsibility		No existing requirement	There is no existing requirement for a stated commitment to safety by management.	No existing requirement	No existing requirement
	1.2 Safety accountabilities		No existing requirement	21.135 requires a description of assigned responsibilities and delegated authority, and of functional relationships between those responsible for quality and management.	No existing requirement	No existing requirement
	1.3 Appointment of key safety personnel		No existing requirement	Appointment of key Quality personnel meets the intent of the requirement, in context.	No existing requirement	No existing requirement
	1.4 Coordination of emergency response planning		No existing requirement	No existing requirement	No existing requirement	No existing requirement
	1.5 SMS documentation		No existing requirement	The elements of SMS are captured in the written production system documentation, although they are not explicitly identified as such.	No existing requirement	No existing requirement
2. Safety risk management						
	2.1 Hazard identification 2.2 Safety risk assessment and mitigation		Existing quality system requirements (21.137i, n) address identification, analysis and instigating corrective action for non-conforming products, and eliminating the actual and potential causes o non-conforming products or non-compliance with the quality system (equate this to SRM in the production context). The regulatory requirements do not require risk management, although individual organizations may have that process in place (MRB) There is no general regulatory requirement for prioritizing quality system response to non-conformance based on safety risk.(Special requirements apply to critical parts in CFR33).	Existing quality system requirements (21.137i) address eliminating the actual and potential causes of non-conforming products or non-compliance with the quality system (equate this to SRM in the production context). This could include organizational, human error and environmental factors.	**New type design complies**. Existing airworthiness standards require comprehensive safety analysis as part of product certification; additional SRM activities are not needed.	No existing requirement
					COS of engines and propulsion systems complies. AC 39-8 lists well-known hazards and defines a process for assessing in-service events to establish hazard level and mitigating actions.	

					COS: Other products do not have an existing requiremen for product-specific hazards identified after entry into service, although non-regulatory systems are already agreed between FAA and many TC holders, and implemented.	
					COS of all certificated products complies, in part, by 21.3	
					COS for ETOPS complies for some hazards(first 1/4 million hours service), as required by (21.4)	
3. Safety assurance						
	3.1 Safety performance monitoring and measurement		Existing quality system requirements (21.137m) address defining a quality system to assure product safety and conformance, inspecting product (21.137g, measures the quality system capability), identifying quality escapes and removing them from the system or otherwise controlling their risk (21.137n),conducting interna audits to assure compliance with the QMS(21.137l) receiving and processing feedback on in-service failures, malfunctions, and defects and supporting the design approval holder in developing corrective action . (These activities equate to monitoring and measurement of the system performance - both for detected non-conformances and undetected non conformances- in the production context). There is no regulatory requirement for a means to discriminate between the safety performance of the quality system and the overall performance o the quality sustem.		**New Design: Complies for early-ETOPs fleet. For other fleets/products, does not comply.** There is no regulatory requirement (outside ETOPs) to apply the knowledge gained in monitoring safety performance back to the development of new designs.	No existing requirement, although individual organizations may have measures in place.
					COS of engines and propulsion systems complies. AC 39-8 requires verifying that corrective actions are effective	
					COS for ETOPS complies. ETOPS rule requires monitoring and measurement of fleet performance.	
					COS for non-ETOPs, non-propulsion does not comply by an existing requirement, although many organizations have measures in place to maintain their product reputation..	

	3.2 The management of change		Existing quality system requirements address design data control and change management(21.137a), production process change management (21.137d), quality system document control and change management (21.137b). Production process control change management is controlled by the quality system as a whole (maintains conformity with drawing and monitors for process degradation, identifies, addresses root cause.) There is no regulatory requirement for change management to focus on the safety effect of a change rather than the overall quality effects. There is no regulatory requirement to ensure that changes to the production process maintain compliance to the airworthiness requirements.	There are no existing requirements regarding change management for organizational factors.	**New Design complies:** FAA applies issue papers or Special Conditions where they perceive novel design features. New rules are developed to manage changes in technology, operational expectations or new understanding of risks..	No requirement.
					Certification of design changes: Existing regulations adequately address product changes that would affect safety (21.93, 21.101)	
	3.3 Continuous improvement of the SMS		21.137 i and l address continuous process improvement. This may include organizational	21.137 i and l address continuous process improvement. This may include organizational and environmental root	No requirement.	No requirement.
4. Safety promotion						
	4.1 Training and education		Not applicable	There is no existing requirement for training and education in the QMS. Individual organizations may such commitments in place voluntarily.	No requirement.	No requirement.
	4.2 Safety communication.		Not applicable	21.137c requires communication with suppliers; 21.137m requires communication with the design approval holder. There are no existing requirements regarding internal communication.	No existing requirement	No requirement.
						Note: The above analysis applies to general requirements. Organizational delegation may require additional process elements similar to SMS elements, for parts of the delegated process.

APPENDIX G. Transport Canada's Phased-In Approach to SMS Implementation

The implementation of SMS involves a progressive development. Transport Canada is taking a phased-in approach to implementation. The four phases extend over 3 years.

Regulation In force Date	+ 90 Days	+ 1 Year	+ 2 Years	+ 3 Years
	Initial Certification	1 Year Follow up	2 Year Follow up	3 Year Follow up

Phase 1: Initial Certification

Within 3 months of the publication of the SMS regulation, initial certification requires that applicants provide Transport Canada:

- The name of the accountable executive;
- The name of the person responsible for implementing the SMS;
- A statement of commitment to the implementation of SMS (signed by the accountable executive);
- Documentation of a gap analysis between the organization's existing system and the SMS regulatory requirements; and
- The organization's implementation project plan, based on the requirements of the exemption and the certificate holders internal gap analysis.

Phase 2: One-Year Follow-up

At one-year, certificate holders will demonstrate that their system includes the following components:

- Documented safety management plan;
- Documented policies and procedures relating to the required SMS components; and
- A process for occurrence reporting with the associated supportive elements such as training, a method of collecting, storing and distributing data, and a risk management process.

Phase 3: Two-Year Follow-up

Two years after initial certification, the certificate holder will demonstrate that, in addition to the components already demonstrated during Phase 2, they also have a process for the proactive identification of hazards and associated methods of collecting, storing and distributing data and a risk management process.

Required components:

- Documented safety management plan;
- Documented policies and procedures;
- Process for reactive occurrence reporting and training; and

- Process for proactive identification of hazards.

Phase 4: Three-Year Follow-up

One year following phase 3, certificate holders will demonstrate that, in addition to the components already demonstrated during phases two and three, they have also addressed:

- Training;
- Quality Assurance; and
- Emergency preparedness.

Transport Canada's Implementation Schedule for all Civil Aviation Organizations

Transport Canada's vision is that SMS will be implemented in all regulated civil aviation organizations by 2015. However, SMS implementation depends on the date regulations come into force and following which will be phased in over three years. Design and Manufacturing Organizations must comply with TCCA's SMS requirements by January 2013

CAR Part	Planned In-Force
Part I	**In-Force: May 31, 2005** **Published: June 15, 2005**
Part III	
Airports (Group I)	**In Force: January 1, 2008** **Published: December 26, 2007**
Airports (Group II)	**In Force: January 1, 2009** **Published: December 26, 2007**
Water Airports	January 2014
Part IV	
Aeroplane and Helicopter Flight Training Units	January 2012
Part V	
Approved Manufacturers (561)	**January 2013**
Approved Maintenance Organization (AMO) (705)	**In-Force: May 31, 2005** **Published: June 15, 2005**
Approved Maintenance Organization (AMO) (703, 704)	January 2011
Approved Maintenance Organization (AMO) (702)	January 2012
Approved Maintenance Organizations*	January 2013

(AMO) (573)	
Aircraft Certification	January 2014
Part VII	
702	January 2012
703, 704	January 2011
705	**In-Force: May 31, 2005 Published: June 15, 2005**
Part VIII	**In Force: January 1, 2008 Published: December 26, 2007**
	Updated: December 22, 2009

* All remaining AMOs.

Legend

Areas highlighted in blue, in the left column, are those parts of the *Canadian Aviation Regulations* (CARs) that have completed the consultation process for the SMS Notices of Proposed Amendments (NPAs).

Areas highlighted in grey, in the left column, indicate that the consultation process has not yet started or has not yet been completed for those parts of the CARs.

Areas highlighted in yellow, indicate dates that are currently forecasted for the specified activity. The planned in-force dates are predicated on:

- The timely acceptance of NPAs by *CARAC* Technical Committees; and
- Meeting the *Canada Gazette* Part I and II timings.

In addition:

- Delays in acceptance of NPAs by the CARAC Technical Committee or delays in the *Canada Gazette* Part I or II activities may require that the in-force dates for specific CARs Part regulations be revised to a later date;
- A number of NPAs have not as yet been submitted to the *CARAC* process and none of the NPAs have completed the *Canada Gazette* Part I or II process; and
- All in-force dates are subject to change.

SEC. xxx. PROTECTION OF AVIATION SAFETY INFORMATION.

(a) Limitation on Disclosure and Use of Information-

(1) IN GENERAL- Except as provided by this section, no person party may use discovery or subpoena to obtain--

(A) data used solely to support risk analysis or risk management performed under a Safety Management System;

(B) any report or data produced as a consequence of or in support of the risk assessment deliberations under a Safety Management System;

(C) any report created as part of a Safety Management System; or

(D) the results of any hazard identification or risk assessment performed as part of a Safety Management System.

(2) FOIA NOT APPLICABLE- Section 522 of title 5, United States Code, shall not apply to reports or data described in paragraph (1).

(3) EXCEPTIONS- Nothing in paragraph (1) or (2) prohibits the FAA from disclosing information contained in reports or data described in paragraph (1) if withholding the information would not be consistent with the FAA's safety responsibilities, including--

(A) a summary of information, with identifying information redacted, to explain the need for changes in policies or regulations;

(B) information provided to correct a condition that compromises safety, if that condition continues uncorrected; or

(C) information provided to carry out a criminal investigation or prosecution.

(b) PERMISSIBLE DISCOVERY - Except as provided in subsection (c), a court may allow discovery by a party of reports or data described in paragraph (1) only if, after an in camera review of the information, the court determines that the information was not necessary to the Safety Management System and was associated with the Safety Management System for no other purpose than protection of the information from disclosure.

(c) PROTECTIVE ORDER- When a court allows discovery, in a judicial proceeding, of reports or data described in paragraph (1), the court shall issue a protective order--

(1) to limit the use of the information contained in the report or data to the judicial proceeding;

(2) to prohibit dissemination of the report or data to any person that does not need access to the report for the proceeding; and

(3) to limit the use of the report or data in the proceeding to the uses permitted for privileged self-analysis information as defined under the Federal Rules of Evidence.

(d) SEALED INFORMATION- A court may allow reports or data described in paragraph (1) to be admitted into evidence in a judicial proceeding only if the court places the report or data under seal to prevent the use of the report or data for purposes other than for the proceeding.

(e) SAFETY RECOMMENDATIONS- This section does not prevent the National Transportation Safety Board from referring at any time to information contained in a Safety Management System report in making safety recommendations.

(f) WAIVER- Any waiver of the privilege for self-analysis information by a protected party, unless occasioned by the party's own use of the information in presenting a claim or defense, must be in writing.

Appendix I: Examples of SMS Regulatory Language and D&M Comments

The D&M Work Group reviewed examples of proposed or published Safety Management System regulatory language, including existing regulation from various State civil aviation authorities, as a background and reference for development of proposed regulatory language. (Note: This is not intended as a comprehensive review of international regulation). Each example was evaluated from the perspective of perceived strength and/or weakness as potential candidate language for a proposed single overarching regulation based on the following considerations: alignment with ICAO framework, simplicity efficiency and flexibility non-prescriptive and performance-based, and enforceability.

Contents:

Example 1:
Transport Canada - General SMS Regulation (107.03) and specific example regulation for Airline Operations (705.152)

D&M WG comments:

- Alignment with ICAO Framework
TC CAR 705.152 does not directly align with the ICAO Framework. The regulation includes seven required components which can be reasonably interpreted to address safety policy, hazard identification, risk management and performance monitoring, but there is not a direct correspondence to the ICAO components and elements.

- Simplicity, efficiency, flexibility
The TC CAR is reasonably brief but is specifically geared to an airline operator (as the regulation is specifically applicable), and as written would not be practical as a single broadly applicable regulation

- Non-prescriptive, performance-based
The CAR is primarily performance based but includes some prescriptive elements (for example, the internal hazard reporting policy must include "the conditions under which immunity from disciplinary action will be granted"

- Enforceability
The CAR is existing regulation and was written in the form of enforceable regulatory language. It would be instructive to review the experiences of Canadian operators and TC as regards to regulatory compliance efforts.

Regulatory Language:

107.03 A safety management system shall include

(a) a safety policy on which the system is based;

(b) a process for setting goals for the improvement of aviation safety and for measuring the attainment of those goals;

(c) a process for identifying hazards to aviation safety and for evaluating and managing the associated risks;

(d) a process for ensuring that personnel are trained and competent to perform their duties;

(e) a process for the internal reporting and analyzing of hazards, incidents and accidents and for taking corrective actions to prevent their recurrence;

(f) a document containing all safety management system processes and a process for making personnel aware of their responsibilities with respect to them;

(g) a quality assurance program;

(h) a process for conducting periodic reviews or audits of the safety management system and reviews or audits, for cause, of the safety management system; and

(i) any additional requirements for the safety management system that are prescribed under these Regulations.

……

705.152 - *Components of the Safety Management System*
(amended 2005/05/31; no previous version)

(1) The safety management system shall include, among others, the following components:

(a) a safety management plan that includes

(i) a safety policy that the accountable executive has approved and communicated to all employees,

(ii) the roles and responsibilities of personnel assigned duties under the quality assurance program established under section 706.07 or the safety management system,

(iii) performance goals and a means of measuring the attainment of those goals,

(iv) a policy for the internal reporting of a hazard, an incident or an accident, including the conditions under which immunity from disciplinary action will be granted, and

(v) a review of the safety management system to determine its effectiveness;

(b) procedures for reporting a hazard, an incident or an accident to the appropriate manager;

(c) procedures for the collection of data relating to hazards, incidents and accidents;

(d) procedures for analysing data obtained under paragraph (c) and during an audit conducted under subsection 706.07(3) and for taking corrective actions;

(e) an audit system referred to in subsection 706.07(3);

(f) training requirements for the operations manager, the maintenance manager and personnel assigned duties under the safety management system; and

(g) procedures for making progress reports to the accountable executive at intervals determined by the accountable executive and other reports as needed in urgent cases.

(2) The components specified in subsection (1) shall be set out in the air operator's company operations manual and maintenance control manual (MCM).

Example 2: EASA Proposed Amendment on SMS

D&M WG comments:

- Alignment with ICAO Framework
The proposed regulatory language in OR.GEN.200 does not fully align with the ICAO Framework outline. Item (1) safety policy does not include any subordinate elements. Item (2) reasonably addresses hazard identification and safety risk management. The remaining components (safety assurance and promotion) are not directly addressed.

- Simplicity, efficiency, flexibility
The language of OR.GEN.200 is very brief, high-level, and reasonably satisfies the necessity for simple, efficient and flexible regulation.

- Non-prescriptive, performance-based
The language is non-prescriptive and performance based, with the exception of the specific requirement for an "organization manual" and its associated contents.

- Enforceability
The language is written in a style that could reasonably be proposed as regulation.

EASA Proposed Regulatory Language:

EASA NOTICE OF PROPOSED AMENDMENT (NPA) NO 2008-22C

... establishing the implementing rules for the competent authorities, including general requirements, approved training organisations, aeromedical centres, licensing and medical certification of flight crew.

Section 2 –Management
OR.GEN.200 Management system

(a) An organisation shall establish and maintain a management system that includes:

(1) a safety policy;

(2) a process for identifying safety hazards and for evaluating and managing the associated risks;

(3) clearly defined lines of safety accountability throughout the organisation, including a direct accountability for safety on the part of senior management;

(4) personnel trained and competent to perform their tasks;

(5) a process for reporting and analysing hazards, incidents and accidents and for taking corrective actions to prevent their recurrence;

(6) an organisation manual containing all management system processes, including a process for making personnel aware of their responsibilities and an amendment procedure;.

(7) a function to monitor compliance of the management system with the relevant requirements and adequacy of the procedures. Compliance monitoring shall include a feedback system of findings to the accountable manager to ensure corrective action as necessary; and

(8) any additional requirements that are prescribed in this Part.

(b) The management system shall correspond to the size, nature and complexity of the activities, and the hazards and associated risks inherent in these activities.

Web address:
http://www.easa.eu.int/ws_prod/r/doc/NPA/NPA%202008-22c%20-%20Part-OR.pdf

Example 3:
Australian Government Civil Aviation Authority (CASA) SMS Requirements for Air Operators

D&M WG comments:

- Alignment with ICAO Framework
The CASA Civil Aviation Order aligns directly with the ICAO Framework outline, except for the following deviations:

- Under the Policy component, there is no reference to documentation and records, and there is reference to "relevant third party relationships and interactions"
- For operators of large aircraft, a flight data analysis program (FDAP) is required as a fifth component of the SMS

- Simplicity, efficiency, flexibility
With the exception of the additional required component (FDAP) for operators of large aircraft, the CASA Order remains at the ICAO Framework outline level, affording the greatest simplicity and flexibility.

- Non-prescriptive, performance-based
The CASA Order is non prescriptive and performance based, with the exception of the added prescriptive requirement for FDAP.

- Enforceability
The CASA order has basically converted the ICAO Framework outline language to enforceable regulatory language. It would be instructive to review the experiences of Australian operators and CASA as regards to regulatory compliance efforts.

CASA Regulatory Language:
Civil Aviation Order 82.3 Amendment Order (No. 3) 2009.
Section 82.3 (Conditions on Air Operators' Certificates authorising regular public transport operations in other than high capacity aircraft)
…
2A Safety management system

2A.1 For this Order, a ***safety management system*** or ***SMS*** is a systematic approach to managing safety that must:

(a) include the organisational structures, accountabilities, policies and procedures necessary to manage safety in a systematic way; and
(b) comply with paragraph 2A.2.

2A.2 An SMS must, as a minimum, include the following:

(a) a statement of the operator's safety policy and objectives, including documented details of the following:

(i) the management commitment to, and responsibility for, safety risk management;
(ii) the safety accountabilities of managers;
(iii) the appointment of key safety personnel;
(iv) the SMS implementation plan;
(v) the relevant third party relationships and interactions;
(vi) the coordination of the emergency response plan;

(b) a safety risk management plan, including documented details of the following:
(i) hazard identification processes;
(ii) risk assessment and mitigation processes;

(c) a safety assurance system, including documented details of the following:
(i) safety performance monitoring and measurement;
(ii) management of change;
(iii) continuous improvement of the SMS;

(d) a safety promotion system, including documented details of the following:
(i) training and education;
(ii) safety communication;

(e) for an operator who operates an aircraft with a maximum take-off weight exceeding 27 000 kg — a flight data analysis program (***FDAP***) in accordance with paragraph 2A.3.

2A.3 For subparagraph 2A.2 (e), a FDAP must:

(a) regularly record and analyse the operational flight data of individual and aggregated operations to improve the safety of flight operations; and

(b) be integrated into the safety assurance system mentioned in subparagraph 2A.2 (c); and

(c) be supplied by:
(i) the operator; or
(ii) without in any way compromising the operator's responsibility for the existence and effectiveness of the FDAP — another appropriate person; and

(d) ensure that:
(i) except with the person's written consent or by a court order — the identity of a person who reports data to the program is protected from disclosure to anyone other than a person whose duty requires him or her to analyse operational flight data and who, therefore, has access to identity information solely for that purpose; and

(ii) no punitive action may be taken by the operator against a person who reports data.

Example 4:
Civil Aviation Authority of Singapore (CAAS) - SMS Regulation for Maintenance Organizations

D&M WG comments:

- Alignment with ICAO Framework
The CAAS SMS regulations for maintenance organizations are in alignment with the ICAO Framework. The regulatory language contained in SAR 145.64 requires establishment of an SMS acceptable to the authority, that:

(1) Identifies safety hazards and assesses, controls and mitigates risks;
(2) Ensures that remedial actions necessary to maintain an acceptable level of safety is implemented
(3) Provides for continuous monitoring and regular assessment of the safety level achieved; and
(4) Aims to make continuous improvement to the overall level of safety.

The regulation further specifies that the "…framework for the implementation and maintenance of a safety management system must include, as a minimum, the elements as listed in Appendix 6." The referenced appendix reproduces identically the ICAO Framework outline.

- Simplicity, efficiency, flexibility
The minimalist approach of utilizing the ICAO Framework outline provides the simplest and most flexible language.

- Non-prescriptive, performance-based
The SAR 145.64 language is sufficiently non-prescriptive and performance-based, and could reasonably serve as an example for a single overarching regulation intended to eventually apply to service providers across all sectors.

- Enforceability
The ICAO Framework Outline is written as a set of statements defining the envisioned components and elements, and is not written as enforceable regulatory language. The Singapore regulation provides enforceability by requiring an SMS acceptable to the Authority, including basic SRM and SA functions, and further requiring that the service provider's SMS "include, as a minimum, the elements as listed [in the ICAO Framework outline]…"

CAAS Regulatory Language:

…

SAR-145.64 Safety Management System

(a) The SAR-145 approved maintenance organization (except Sub-part D organisations) must establish a safety management system acceptable to the Authority that:

(1) Identifies safety hazards and assesses, controls and mitigates risks;
(2) Ensures that remedial actions necessary to maintain an acceptable level of safety is implemented
(3) Provides for continuous monitoring and regular assessment of the safety level achieved; and
(4) Aims to make continuous improvement to the overall level of safety.

(b) The framework for the implementation and maintenance of a safety management system must include, as a minimum, the elements as listed in Appendix 6.
(c) A safety management system shall clearly define lines of safety accountability throughout the organization, including a direct accountability for safety on the part of the accountable manager and SAR-145.30 senior persons.

SINGAPORE AIRWORTHINESS REQUIREMENTS
PART 145
SECTION 2 APPENDIX 6
SAFETY MANAGEMENT SYSTEM FRAMEWORK ELEMENTS

The framework for the implementation and maintenance of a safety management system should include, as a minimum, the following 4 components and 12 elements:

Safety Policy and Objectives

a) Management commitment and responsibility
b) Safety accountabilities of managers
c) Appointment of key safety personnel
d) Emergency response planning
e) Documentation and records

Safety Risk Management

f) Hazard identification processes
g) Risk assessment and mitigation processes

Safety Assurance

h) Safety performance monitoring and measurement
i) Management of change
j) Continuous improvement and audit

Safety Promotion

k) Training and education
l) Safety Communication

Note: Refer to AC 1-3 for CAAS SMS guidance materials. Reference may also be made to ICAO SMM Document 9859 for any supplementary guidance where appropriate.

Example 5:
CDO-ARC Proposal
(Proposed regulatory language extracted from Certified Design Organization Aviation Rulemaking Committee Report to the FAA - May 2008; Page 185-186)

D&M WG comments:

- Alignment with ICAO Framework
The proposed regulatory language contained in the CDO-ARC report aligns with the four ICAO Framework components (or 'pillars'), but deviates at the element level

- Simplicity, efficiency, flexibility
The CDO-ARC language is reasonably brief, however some of the specific citations at the element level are unique to the design and manufacturing sector. The language would require some modification to be considered as a candidate for general applicability

- Non-prescriptive, performance-based
To the extent that the language follows the ICAO Framework, the proposed regulation is reasonably non-prescriptive

- Enforceability
The CDO-ARC draft SMS requirements for a CDO certificate holder are written in a manner that could reasonably be proposed as regulatory language.

CDO-ARC Proposed Regulatory Language:

…

§21.729 Safety management system required of a CDO certificate holder

A certificate holder must maintain a safety management system (SMS) that incorporates the following:

(a) *Safety Policy* that –

(1) Defines the SMS goals and objectives,
(2) Defines how the organization will implement the SMS to attain the goals and objectives of (a)(1),
(3) Establishes senior company management's commitment to safety management and an expectation of high safety performance, and
(4) Commits to a process-based approach to safety promotion within the company.

(b) *Safety Risk Management* processes applied to safety systems; compliance processes; product, part, and appliance designs; and production or in-service events, that are performed as follows:

(1) Describe the system of interest;

(2) Define the hazards associated with the system defined in (b)(1);
(3) Analyze the safety risk of identified hazards, characterizing the likelihood and severity of each hazard;
(4) Assess the safety risk and incorporate that assessment into its decision-making processes; and
(5) Control, mitigate, or eliminate that safety risk consistent within established FAA airworthiness standards through the implementation of programs, processes, or product redesign.

(c) ***Safety Assurance*** processes that –
(1) Monitor the implementation of the safety policy;
(2) Assess safety systems; compliance processes; product, part, and appliance designs; and production or in-service events, to identify new or potential hazards;
(3) Analyze those assessments as part of its risk management program; and
(4) Continually ensure appropriate safety risk controls are effective for those hazards, based on their safety consequence and likelihood of occurrence.

(d) ***Safety Promotion*** processes that –
Implement the actions necessary to create an environment within the CDO where safety objectives can be achieved and maintained. Those actions must include –
(1) A program to ensure people are appropriately qualified to perform the necessary safety analysis and use the SMS principles when making safety decisions,
(2) A clear definition of what actions are acceptable and unacceptable in the workplace with respect to the reporting of safety issues,
(3) A program for safety information sharing within the organization to ensure lessons learned are available to others doing the same or similar tasks, and
(4) A periodic review of the safety management program to ensure that the defined processes are achieving their desired outcomes.

Example 6:
8000.367 - Appendix B
(FAA Order VS 8000.367 - AVS Safety Management Requirements - 05-14-2008; Appendix B - Product/Service Provider SMS Requirements)

D&M WG comments:

- Alignment with ICAO Framework
Appendix B of FAA Order 8000.367 includes the four components from the ICAO Framework outline (Policy, SRM, SA, and Promotion), but also includes far more than the twelve elements of the framework.

- Simplicity, efficiency, flexibility
The extensive language of the Appendix significantly exceeds the Framework outline level, preventing the necessary flexibility for application as a single overarching regulation.

- Non-prescriptive, performance-based
Some of the language in the Appendix is overly and unnecessarily prescriptive. For example the following citation could be interpreted to mean that the certificate management office must dictate the nature and type of documentation and records:

> "The organization must maintain documents and records in accordance with document and record management policies specified by the oversight organization."

- Enforceability
The appendix is written with the appropriate character and phraseology for draft proposed requirements, however the amount and detail of the language would likely create an unreasonably large burden for regulatory compliance, and would inherently result in enforceability issues.

8000.367 Appendix B Proposed Requirements:

(Format changed from original)

Appendix B: Product/Service Provider SMS Requirements
The following requirements are the minimum set of requirements that must be established for constituent product/service provider organizations for which AVS services have oversight responsibility.
1. Scope and Applicability. To be developed by the AVS service/office.
2. References. To be developed by the AVS service/office.
3. Definitions. To be developed by the AVS service, but the definitions should be consistent with existing FAA definitions and those in the AVSSMS.
4. Policy.
a. General Requirements.
(1) Safety management must be included in the entire life cycle of the organization's outputs.
(2) The organization must promote the growth of a positive safety culture (described in Chapter 4, Section b and Chapter 7, Section a).

b. Safety Policy.
(1) Top management is responsible for the organization's safety policy and its safety performance.
(2) The safety policy must:
(a) include a commitment to implement and maintain the SMS;
(b) include a commitment to continual improvement in the level of safety;
(c) include a commitment to the management of safety risk;
(d) include a commitment to comply with applicable legal, regulatory and statutory requirements;
(e) include an expectation that employees will report safety issues and, where possible, provide proposals for solutions/safety improvements;
(f) establish clear standards for acceptable behavior;
(g) provide management guidance for setting safety objectives;
(h) provide management guidance for reviewing safety objectives;
(i) be communicated to all employees and responsible parties;
(j) be reviewed periodically to ensure it remains relevant and appropriate to the organization; and
(k) identify responsibility and accountability of management and employees with respect to safety performance.

c. Quality Policy. Top management must ensure that the organization's quality policy is consistent with the SMS.

d. Safety Planning. The organization must establish and maintain a safety management plan to meet the safety objectives described in its safety policy. [1]

e. Organizational Structure and Responsibilities.
(1) Top management must have the ultimate responsibility for the SMS.
(2) Top management must provide resources essential to implement and maintain the SMS.
(3) Top management must designate a management official to implement and maintain the SMS.
(4) Responsibilities for aviation safety positions, duties and authorizations must be:
(a) defined;
(b) documented; and
(c) communicated throughout the organization.

f. Compliance with Legal and Other Requirements.
(1) The SMS must incorporate a means of compliance with FAA policy, legal, regulatory and statutory requirements applicable to the SMS.
(2) The organization must establish and maintain a procedure to identify the current FAA policy, legal, regulatory and statutory requirements applicable to the SMS.

g. Operational Procedures and Controls.
(1) The organization must establish procedures with measurable criteria to accomplish its safety policy and objectives as defined by the SMS. [2]
(2) The organization must establish and maintain process controls to ensure procedures are followed for operations and activities as defined by the SMS.

h. Emergency Preparedness and Response.
(1) The organization must establish a plan for response to accidents and serious incidents.
(2) The effectiveness of the plan must be verified at intervals, either by response to real events or as an exercise.

i. Safety Documentation and Records.

(1) The organization must establish and maintain information, in paper or electronic form, to describe:
(a) safety policies;
(b) safety objectives;
(c) SMS requirements;
(d) safety procedures and processes;
(e) responsibilities and authorities for safety procedures and processes; and
(f) interaction/interfaces between safety procedures and processes.
(2) The organization must document SMS outputs in records.
(3) The organization must maintain documents and records in accordance with document and record management policies specified by the oversight organization.

5. Safety Risk Management .3
a. SRM must, at a minimum, include the following processes:
(1) describe system;
(2) identify hazards;
(3) analyze safety risk;
(4) assess safety risk; and
(5) control/mitigate safety risk
b. The elements of the SRM process must be applied, either quantitatively or qualitatively, to:
(1) initial designs of systems, organizations, and products;
(2) the development of safety operational procedures;
(3) hazards that are identified in the safety assurance functions (described in Chapter 6); and
(4) planned changes to the production/operational system, including introduction of new products and procedures, to identify hazards associated with those changes.
c. The organization must establish feedback loops between assurance functions (described in Chapter 6) to evaluate the effectiveness of safety risk controls.
d. The organization must define a process for risk acceptance.
(1) The organization must define acceptable and unacceptable levels of safety risk. Descriptions must be established for severity levels and likelihood levels.
(2) The organization must define levels of management that can make safety risk acceptance decisions.
(3) The organization must define the level of safety risk that is acceptable in the short-term, while long-term safety risk control/mitigation plans are developed and implemented.
e. If applicable, the organization must establish procedures to obtain oversight organization approval for those planned changes that require oversight approval prior to implementation (in accordance with Chapter 4, Section f).
f. The safety risk of identified hazards must be deemed acceptable, prior to implementation of the following items in the production/operational system:
(1) new system designs;
(2) changes to existing system designs;
(3) new operations/procedures; and
(4) modified operations/procedures.
g. The SRM process may allow AVS or AVS services/offices to take interim immediate action to mitigate existing safety risk.

Figure B-1 illustrates the SRM process (described in this Chapter) and links it to safety assurance functions (described in Chapter 6). Note that this diagram is a functional depiction of the processes, not an organizational illustration. Therefore, these processes are not necessarily separate or distinct from the production/operational system; rather, the SRM process is embedded in the production/operational system. In addition, the process flow depicted can be entered at any point as circumstances require and it is not intended to suggest that the processes are necessarily linear. While the diagram and numbering system may imply that the functions are sequential; this is not necessarily the case.

(Figure B-1 – Safety Risk Management and Safety Assurance - deleted from copy)

h. Describe System. The system description must be completed to the level necessary to identify hazards. 4
i. Identify Hazards. Hazards must be identified within the system as described in Section h.
j. Analyze Safety Risk. The safety risk analysis process must include analyses of:
(1) existing safety risk controls;
(2) contributing factors; and
(3) the safety risk of reasonably likely outcomes from the existence of a hazard, to include estimation of the:
(a) likelihood and
(b) severity. 5
k. Assess Safety Risk. Each identified hazard must be assessed for its safety risk acceptability (as defined per requirements listed in Section d).
l. Control/Mitigate Safety Risk.
(1) Safety risk control/mitigation plans must be defined for hazards identified with unacceptable risk.
(2) Substitute risk must be evaluated in the creation of safety risk controls/mitigations.
(3) The safety risk control/mitigation must be evaluated to ensure that safety requirements have been met.
(4) Once safety risk control/mitigation plans are implemented, they must be monitored to ensure that safety risk controls have the desired effect.

6. Safety Assurance. Figure B-1 illustrates how Safety Assurance functions (described in Sections b-k) are linked to the SRM process (described in Chapter 5).
a. General Requirements. The organization must monitor its systems, operations and products/services to:
(1) Identify new hazards;
(2) Measure the effectiveness of safety risk controls;
(3) Assess compliance with legal, regulatory and statutory requirements applicable to the SMS; and
(4) Assess conformity with organizational safety policies and procedures.
b. Information Acquisition
(1) The organization must collect the data/information necessary to demonstrate the effectiveness of the SMS.
(2) The organization must monitor operational data/information.
(3) The organization must monitor products and services received from contractors.
c. Employee Reporting System
(1) The organization must establish and maintain an employee reporting system in which

employees can report hazards, issues, concerns, occurrences, incidents, etc., as well as propose solutions/safety improvements
(2) Employees must be encouraged to use the employee reporting system without reprisal.[6]

d. Investigation [7]

(1) The organization must establish criteria for which accidents and incidents will be investigated.
(2) The organization must establish procedures to:
(a) investigate accidents;
(b) investigate incidents; and
(c) investigate instances of suspected non-compliance with safety regulations.

e. Auditing of the Production/Operational System

(1) The organization must ensure that regular audits of the production/operational system's safety functions are conducted with priority placed on the areas of highest safety risk. This obligation must extend to any contractors that the organization may use to accomplish those functions.[8]
(2) The organization must ensure that regular audits are conducted to:
(a) determine conformity with safety risk controls; and
(b) assess performance of safety risk controls.
(3) Auditing may be done at planned intervals or as a continuing process.

f. Evaluation of the SMS

(1) The organization must conduct evaluations of the SMS to determine if the SMS conforms to requirements.
(2) Evaluations may be done at planned intervals or as a continuing process.

g. Audits by Oversight Organization. If applicable, the organization must include the results of oversight organization audits in the data/information analyses conducted as described in Section h.

h. Analysis of Data/Information

The organization must analyze the data/information described in Section b.

i. System Assessment

(1) The organization must assess the performance of:
(a) the production/operational system's safety functions against its safety requirements as defined by the SMS and
(b) the SMS against its requirements.
(2) System assessments must result in the documentation of:
(a) conformity with existing safety risk control(s)/SMS requirement(s) (including legal, regulatory and statutory requirements applicable to the SMS);
(b) nonconformity with existing safety risk control(s)/SMS requirement(s) (including legal, regulatory and statutory requirements applicable to the SMS);
(c) potentially ineffective control(s); and
(d) potential hazard(s) found.
(3) The SRM process must be utilized if the assessment identifies:
(a) potential hazards or
(b) the need for production/operational system changes.

j. Corrective Action. When nonconformities are identified, the organization must prioritize and implement corrective actions.

k. Management Reviews.

(1) Top management must conduct regular reviews of SMS effectiveness.

(2) Management reviews must assess the need for changes to the SMS.

7. Safety Promotion.

a. Safety Culture. Top management must promote the growth of a positive safety culture demonstrated by, but not limited to:

(1) publication to all employees of senior management's stated commitment to safety;

(2) communication of safety responsibilities with the organization's personnel to make each employee part of the safety process;

(3) clear and regular communications of safety policy, goals, objectives, standards and performance to all employees of the organization;

(4) an effective employee reporting system that provides confidentiality and de-identification as appropriate (as described in Chapter 6, Section c);

(5) use of a safety information system that provides an accessible, efficient means to retrieve information; and

(6) allocation of resources to implement and maintain the SMS.

b. Communication and Awareness

(1) The organization must communicate SMS outputs to its employees as appropriate.

(2) If applicable, the organization must provide access to the SMS outputs to its oversight organization, in accordance with established agreements and disclosure programs.

(3) The organization must ensure that affected employees and external stakeholders (including its oversight organization, if applicable) are aware of the short-term safety risk of hazards that may exist in the production/operational system while safety risk control/mitigation plans are developed and implemented (as described in Chapter 5, Section d3).

c. Personnel Competency

(1) The organization must document competency requirements for those positions identified in Chapter 4, Section e4.

(2) The organization must ensure that individuals in the positions identified in Chapter 4, Section e4 meet the documented competency requirements.

d. Safety Knowledge Management. The SMS must include a process to capture knowledge of safety issues and incorporate it into future products, services and practices as appropriate.

8. Interoperability. The organization's SMS must be able to interoperate with other organizations' SMSs to manage cooperatively issues of mutual concern.

Footnotes:

[1] Safety planning is a component of safety management that is focused on setting safety objectives and specifying necessary operational processes and related resource requirements to fulfill those objectives.

[2] Measures are not expected for each procedural step. However, measures and criteria should be of sufficient depth and level of detail to ascertain and track the accomplishment of objectives. Criteria and measures can be expressed in either quantitative or qualitative terms.

[3] In general, the extent and structure of safety risk assessment that is necessary will be greater when the item/issue to be assessed is more complex and effects of the hazards are more severe. The intent of the SRM process is to focus on the areas of greatest concern from a safety perspective, taking into account safety risk, complexity, operational scope (impact to the air transportation system), etc.

[4] While it is recognized that identification of every conceivable hazard is impractical, organizations are expected to exercise diligence in identifying and controlling significant and reasonably foreseeable hazards related to their operations. Describing the system involves the act of bounding the system (i.e., defining what the system actually is). The definition process is a purely subjective one. Defining a system requires a definition of its boundary and its components.

[5] Severity and likelihood may be expressed in qualitative or quantitative terms.

[6] This does not restrict management from taking action in cases of gross negligence or willful operation outside the organization's safety requirements.
[7] It is understood that not all organizations have the ability to directly investigate accidents and incidents for relevance to their products/services (e.g., organizations that provide air traffic management systems or subsystems). Therefore, in this case the organization should use the results of investigations conducted by other entities.
[8] The organization can choose to conduct audits of its contractors or require that contractors conduct their own audits and provide the resultant data/information to the organization.

Example 7: Sample U.S. Regulatory Language Based on ICAO SMS Framework

- Alignment with ICAO Framework
The draft language (identified as new proposed Part 195) aligns with the four ICAO Framework outline components. It aligns with the twelve outline elements except under Safety Policy where there is slight deviation in that the element regarding documentation and records is not explicitly included, and a requirement for internal reporting procedures is added.

- Simplicity, efficiency, flexibility
The proposed language generally remains at the framework outline level. The component and element descriptive statements are converted to the form of requirements language, thereby approaching the simplest practical concept for proposed regulation, and allowing the greatest flexibility.

- Non-prescriptive, performance-based
The language is generally non-prescriptive, simply requiring the regulated entity to have a procedure to address the required elements.

- Enforceability
The draft provides an example of reasonably enforceable language based directly on the ICAO Framework outline.

DRAFT Sample U.S. SMS Regulatory Language Based on ICAO Framework

Title 14
Chapter 1
Subchapter L [new]
Part 195

195.1 Safety Management System

(a) This Part applies to any person that is required, under this Chapter, to have a safety management system.

(b) The procedures described in this Part shall be known, collectively, as a safety management system.

(c) A person required by this Chapter to have a safety management system may incorporate some, none or all of its procedures in any other manual or collection of procedures maintained by the person.

(d) Where the procedures required under this part are substantially similar to procedures required by other regulations, a single procedure may meet the requirements of two or more requirements.

(e) The procedures required by this part will reflect the size, culture, special operating requirements and business practices of the party implementing the safety management system, and therefore may differ among similarly situated persons based on the differing practices of each person.

195.3 Definitions

(a) Regulated Party, for purposes of this Part, means a person who is required by this Chapter to have a safety management system.

195.5 Safety Policy

The Regulated Party shall have the following Safety Policy data and procedures:

(a) An internal procedures for reporting safety issues;

(b) A procedure for periodic review of the safety policy and objectives, to ensure that they remain relevant and appropriate to the organization

(c) An organizational chart that identifies, the title, duties and responsibilities of
(1) the Accountable Manager who is responsible for the implementation and maintenance of the SMS;
(2) each management person who has authority to make decisions regarding safety risk tolerability;
(3) each management person who is accountable for implementing safety policy
(4) each management person who is accountable for ensuring that safety policy is implemented

(d) A procedure for appointing the Accountable Manager;

(e) Where emergency response procedures are necessary, procedures for

(1) transitioning from normal to emergency operations, and returning to normal operations,;

(2) coordination of emergency response planning;

(f) A description of the safety policy, safety objectives, safety performance indicators and safety performance targets of the Regulated Party;

195.7. Safety risk management

The Regulated Party shall have the following Safety Risk Management procedures:

(a) A procedure for collecting safety data and identifying aviation safety hazards associated with the Regulated Party's operations

(b) A procedure for reviewing aviation safety hazards associated with the Regulated Party's operations and identifying appropriate controls of the aviation safety risks posed by each aviation safety hazard.

195.9 Safety assurance

The Regulated Party shall have the following Safety Assurance procedures:

(a) A procedure for verifying the safety performance of the organization and validating the effectiveness of the safety risk controls in reference to the safety performance indicators and safety performance targets of the Safety Policy.

(a) A procedure for managing change within the organization to assure that change does not adversely affect safety performance

(b) A procedure for using safety data to improve the Regulated Party's Safety Management System

195.11 Safety promotion

The Regulated Party shall have the following Safety Promotion procedures:

(a) A procedure for training the Regulated Party's safety-related personnel to assure that they are competent to perform their SMS duties.

(b) A procedure for safety communication that ensures
(1) that all safety-related personnel are fully aware of the Regulated Party's safety management system, and
(2) that the Regulated Party's safety information is conveyed to appropriate personnel.