

System Safety Management Transformation (SSMT) Safety Management System (SSM), Pilot Project Criteria/Requirements Development: MSMS

Alan Stolzer, Ph.D.
May 2011



Background

- CGAR contracted by FAA AIR team to provide SMS subject matter expertise to team developing SMS guidance and advisory circular material to design and manufacturing community – Pilot Project
- Team composition
 - 25 or so FAA people from various offices and directorates, plus contractors (i.e., MITRE, BAH, CGAR)
- Began work in April 2010
 - Telecons
 - Bi-monthly F2F meetings
 - Numerous tasks
- Research support by doctoral student Bill Tuccio

Selected Tasks

Project	Summary Status
System Description and Hazard ID	Accepted March 2011
Data Exchange	Accepted February 2011
AS9100 GAP	Accepted March 2011
Accident Decomposition/Analysis	In Progress May 2011

System Description and Hazard ID

- Throughout AC 120-92a, *system descriptions* are deemed vital:
 - “Hazard analysis begins with system design”
 - “The SA process starts with a System Description which adds structure and helps map organizational responsibilities, functions and interfaces.”
 - “SRM will ... include ... system descriptions and task analysis”
 - System descriptions and task analysis will be developed to the level of detail necessary to: identify hazards, develop operational procedures, and develop and implement risk controls.

No guidance exists on how to do this

System Description and Hazard ID

Interviews with Industry and Literature Review



Initial Draft of System Description and Hazard Identification



Example Execution Scenarios Added to Procedure



Advisory Circular Format Applied to System Description (i.e., not so academic)



Submitted for Use in Pilot Project (with two example execution scenarios)

System Description

Industry Contacts

- Contacted numerous D and/or M entities
- Focus: Do they have a System Description? Further, opinions and knowledge of SMS
- Substantial replies from:
 - Hartzell Propeller (on-site visit, June, 2010 in Dayton)
 - P.S. Engineering
 - Bombardier
 - Hawker Beechcraft
 - Cirrus
- Working report written summarizing interviews and literature review

System Description Procedural Document

- First Draft of Procedural Document
 - Including hypothetical examples of execution
- Feedback on document from industry and FAA
 - Too academic, lengthy, and complex
 - Questions of how to fit with other SMS/DM content, such as the GAP analysis tool

System Description Procedural Document

- Second Draft
 - Original draft used to build a simpler version
 - More of an Advisory Circular format – streamlined, to the point
 - Examples conformed to new approach
 - Shorter, easier to understand
 - Better fit with other SMS/DM material
- Very positive feedback



DESIGN AND MANUFACTURING (D&M) SAFETY MANAGEMENT SYSTEM (SMS) PILOT PROJECT GUIDE

37 pages

APPENDIX D: System Description & Hazard Identification Process

System Description and Analysis Summary

Prior to performing the preliminary gap analysis process, the PMT will assist the company in conducting a System Description and Analysis of the company's operational functions.

- 1) Every system contains inherent potential safety vulnerabilities which are characterized in

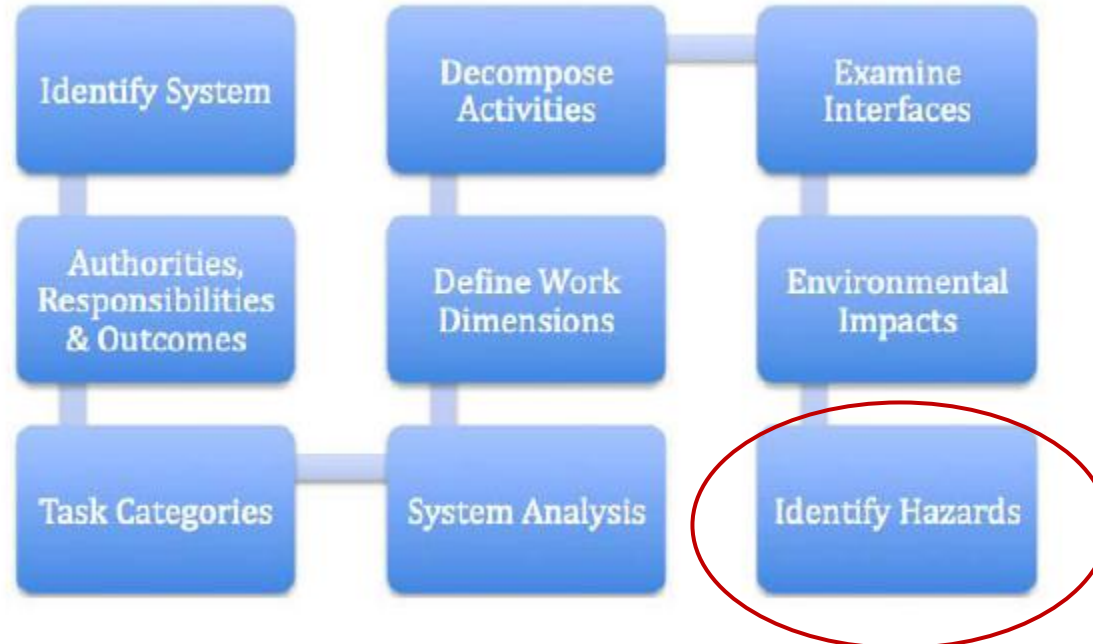
http://www.faa.gov/about/initiatives/sms/pilot_projects/guidance/media/DM_SMS_PilotProjectGuide.pdf

System Description and Hazard Identification: A Process for Design and Manufacturing Organizations

Alan J. Stolzer, Ph.D.

Embry-Riddle Aeronautical University

FIGURE 1. SYSTEM DESCRIPTION PROCEDURE OVERVIEW



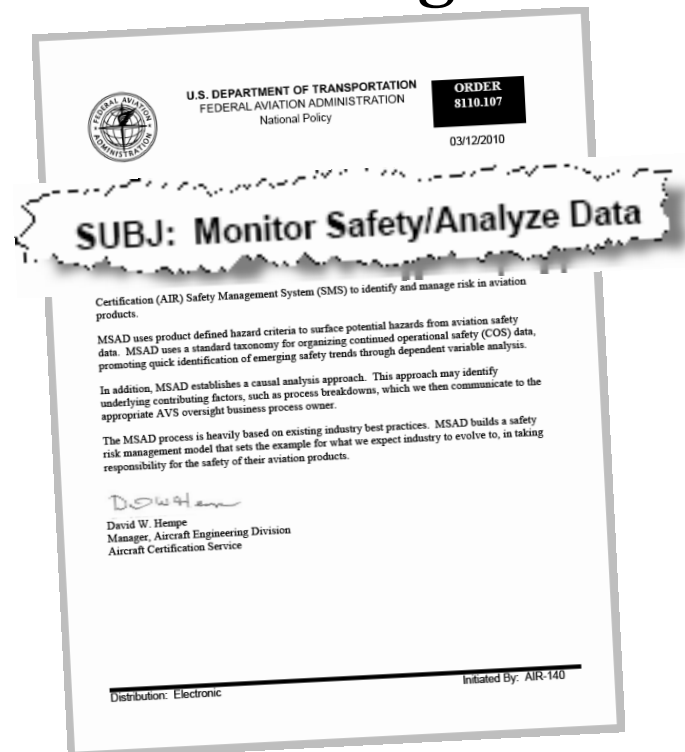
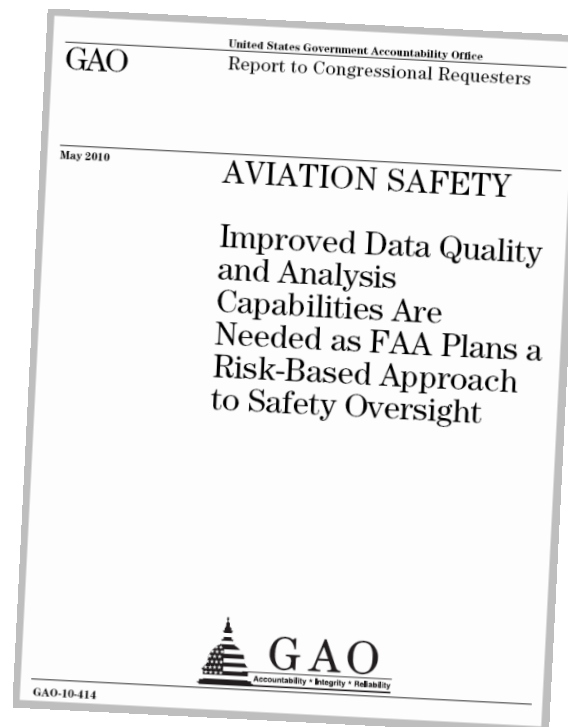
Data Exchange

FAA requested an examination of issues surrounding data exchanged between industry and the FAA as a result of SMS

- D&M Company Interviews
- Literature Review
 - Social & Cognitive Networks
 - Rules pertaining to D&Ms (Parts 21, 23, 25, 26, 35)
 - Relevant government, incl. GAO, reports
 - DOT RITA
 - BTS
 - numerous other industries, sources, even international
- Presented for Review

Data Exchange Approach

- Literature Review and industry interviews
- Two key sources – both significantly impact future decisions on how FAA should manage SMS data



Data Exchange Discussion

- Much of today's FAA data exchange in D&M world is email based, with little feedback to providers of data
- SharePoint is offered to providers of data as a submission technique, but with little elaboration, causing confusion and poor adoption
- Proprietary data concerns within D&M community

Data Exchange Discussion

- Industry will need technology to collect SMS metrics as industry and FAA mature
 - Implies software and/or software standards to manage SMS metric data
 - Market already has some software vendors for SMS data management
 - Should the FAA create software standards?
- Data Supply Chain
 - Protect proprietary information, interface with other systems, such as MSAD.

Data Exchange Discussion

- Safety Analyses of Data
 - Interrelationships between D&Ms may be able to be explored
 - Trend analysis
- Industry Data Usage
 - Support adhoc reporting
 - Support targeted alerts
 - Support mashups of data
 - Support social tagging
 - FAA should monitor usage statistics of features

Recommendations

- MSAD
 - FAA D&M SMS team should meet with MSAD program leaders, create roadmap for the future
- SMS Software Standards
 - An FAA/Industry group should create SMS software standards
- Workflow over email for data exchanges
 - Start move away from email for data exchanges towards a workflow based submission scheme

Recommendations, cont'd

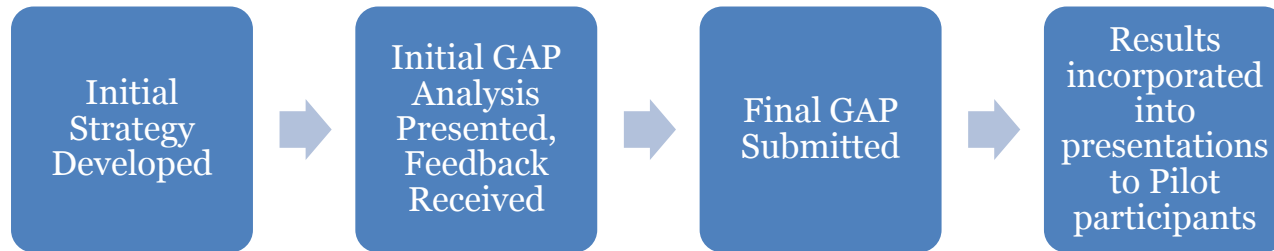
- Consider SMS Data Warehouse/Business Intelligence system development at FAA
- Identify typical measures a D&M can make and submit to FAA as part of SMS
- Identify industry intellectual property rights concerns
- Determine where and how D&M companies can make anonymous reports similar to ASRS

Recommendations, cont'd

- Semantically enable future data sharing efforts
 - i.e., make unstructured data queryable
- Embrace social networking in data sharing
- Meet with existing organizations engaging in data sharing to learn best practices

AS9100 vs. SMS

FAA requested that we put together a document explaining the difference between quality (AS9100B) and SMS (D&M Framework)



AS9100 vs. SMS

- Created a document suggesting an approach to compare AS9100B and SMS/DM.
 - Modeled after AC 120-92A, *Safety Management Systems for Aviation Service Providers, Appendix 2, Comparison of Safety Management System Framework with Other Standards.*

AS9100 vs. SMS

- Tabulated comparison in Microsoft Access database
- Had 259 AS9100B total “nodes” vs. 197 for SMS/DM
- The 197 SMS/DM areas resulted in 83 rows of GAP comparisons*
 - 44 of 83 SMS/DM areas had no AS9100B equivalent
 - 39 of 83 SMS/DM areas had some AS9100B equivalent

*Many SMS nodes were combined due to similarities.

AS9100 vs. SMS Conclusions

- Safety Policy is well covered by AS9100B
 - ...however, requires mapping from quality focus to quality *and* safety focus
- Safety Risk Management is lacking/absent
- Safety Assurance is lacking/absent
- Safety Promotion is weakly covered
 - Does promote the quality management system
 - Silent to data sharing

GAP - Rating Rubric

Rating	Rating Scale	Description
5	----- -----5	AS9100B has large omissions in both scope of safety and scale compared to SMS. While AS9100B may mention the area covered by SMS, it is nearly an empty comparison or complete gap.
4	----- ----4-	AS9100B is lacking both in scope of safety and scale compared to SMS.
3	----- --3--	SMS and AS9100B have equivalent scope of safety concepts. SMS scale exceeds that of AS9100B.

(continued)

GAP - Rating Rubric

2	----- -2----	SMS and AS9100B have equivalent scale of concepts. SMS scope exceeds that of AS9100B in the area of safety or as otherwise stipulated in comparison comments.
1	----- 1-----	SMS and AS9100B safety scope and scale identical; SMS linguistic expression requires AS9100B linguistic adjustment.
0	-----0-----	SMS and AS9100B equivalent both in safety scope and scale.

Accident Decomposition

- Use a well-documented accident to illustrate SMS/DM “in-action”
 - Decompose an accident, i.e., work backwards, from accident causes to hazards, pointing out SRM and SA connections, to help show Pilot participant **value of SMS**
- Accident selected (Pensacola, Delta Airlines 1288 MD-88, Uncontained Engine Failure, 1996)
- Initial SMS/D&M Analysis Applied – currently under review

