Designing an Effective SMS

Prof. Nancy G. Leveson

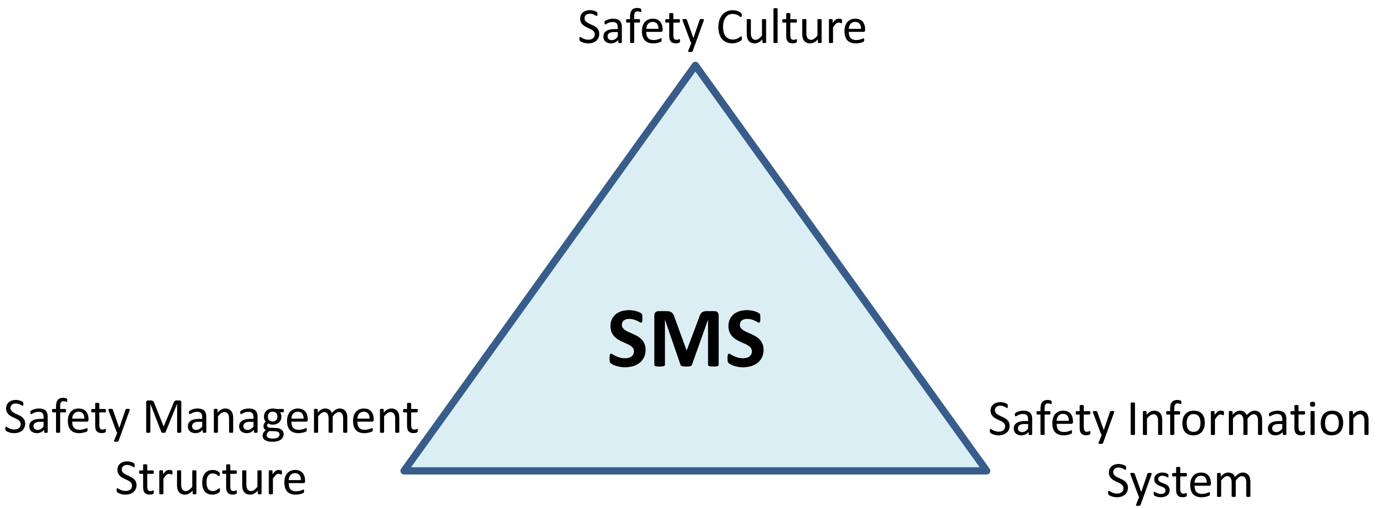
Aeronautics and Astronautics
MIT
(http://psas.scripts.mit.edu/...)

STAMP Virtual Workshop 2020

Introduction

- What I have learned in 40 years in system safety
  - Some orgs have lots of accidents, others few or none
  - Designing an SMS is a system engineering problem
- Lots of “standard” designs, but usually limited in some way
- Instead, design something comprehensive that meets your needs
  - Need to proactively control safety in every aspect of organization
  - Product development vs. services
- General
  - Need effective learning process
  - Need to identify when degrading over time (everything changes over time

Three Parts to an SMS



Safety Culture

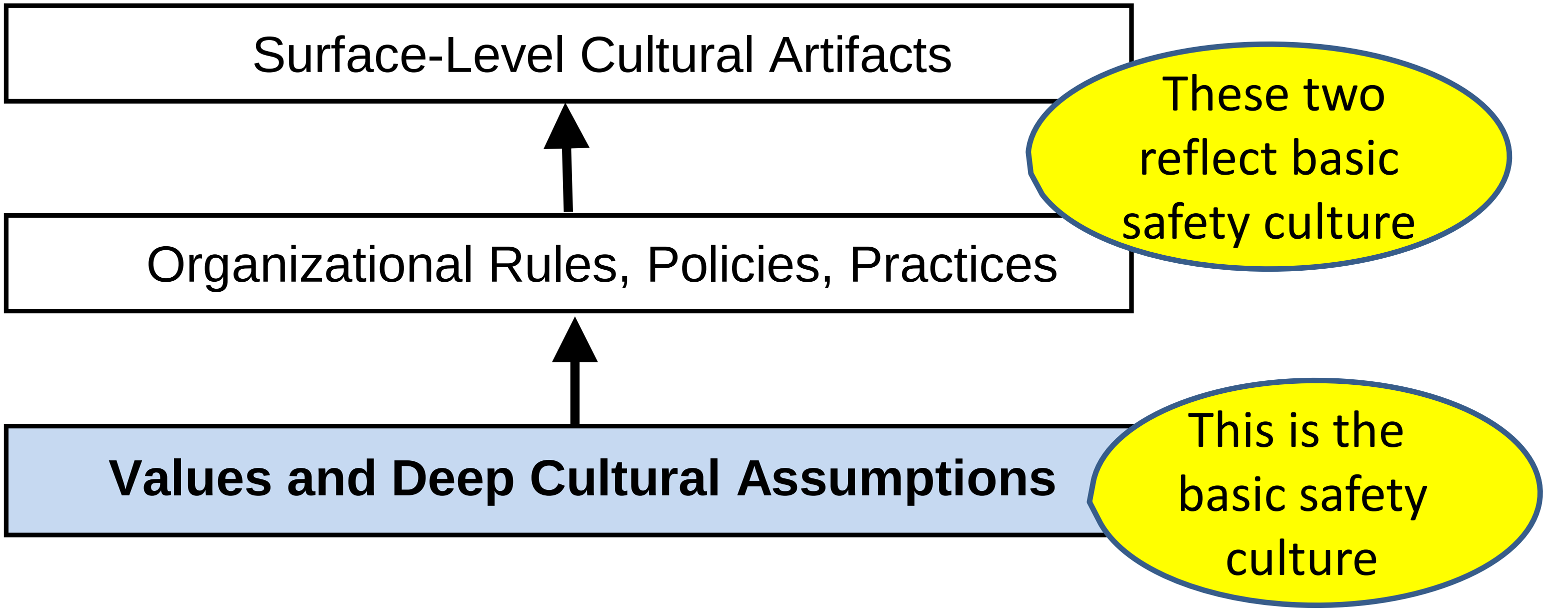
SMS

Safety Management Structure

Safety Information System

- Culture defines desirable and effective behavior
- Safety management structure determines how cultural goals will be implemented
- Safety Information System provides information to make management structure successful

Safety Culture (Shein)


Surface-Level Cultural Artifacts
Organizational Rules, Policies, Practices
Values and Deep Cultural Assumptions
These two reflect basic safety culture
This is the basic safety culture

- Changing only top two will have little lasting impact
- Trying to change culture without changing environment it is embedded within also doomed to failure
- Effective or not, there is ALWAYS some kind of safety culture

Types of High Accident Safety Cultures

Do any of these reflect your organization or industry?

- Culture of risk acceptance:
  - Accidents are inevitable; accidents considered the price of productivity
  - Everyone should be responsible for safety (their own and others)
  - Accidents result from lack of responsible behavior by individuals; if everyone acted responsibly and safely, accidents would be reduced.
- Culture of denial
  - Reliance on risk assessment, usually unrealistically low
  - Warnings dismissed without appropriate investigation
  - Management wants to hear good news so that is what they are told
  - Focus on showing system acceptably safe, not on identifying ways it might be unsafe

Types of High Accident Safety Cultures (2)

- Culture of compliance
  - Focus on complying with government regulations
  - Belief that compliance with gov’t regs will lead to acceptable results
  - After the fact assurance is emphasized with extensive “safety case” arguments with little impact on actual product or process
- Culture of paperwork
  - Assumption that producing lots of documentation and analysis paperwork leads to safe products and services.
  - Most paperwork produced by group independent of and with little interaction with those designing and operating products, implementing processes, or providing services (so little impact on design and operations)
- Culture of “swagger”
  - Safety is for sissies; real men thrive on risk

Features of an Effective Safety Culture

Which of these are true for your organization?

- Management understands safety and productivity go together
  - Openness about safety and safety goals
  - Willingness to hear bad news
- Emphasis on doing what is necessary and not just complying with government regs or producing a lot of paperwork
- Employees believe managers want to hear their safety concerns and will take action
- Managers believe employees worth listening to and worthy of respect
- Employees feel safe reporting concerns and feel their voice valued
- Safety is shared responsibility but responsibility not just placed on workforce to keep themselves and others safe.

Improving Safety Culture

1. Safety culture is established by top management
   - Set goals and requirements for achieving those goals
   - Establish what is expected in safety-related decision making and behavior
2. Communicate basic values you want people to follow
   - Create a safety philosophy statement for organization or industry
   - Examples in paper that accompanies this tutorial
   - Ensure wide buy-in and make sure being followed
   - Demonstrate commitment to philosophy, e.g.,
     - Personal involvement
     - Setting priorities, provided resources
     - Rewarding employees for safety efforts
     - Responding to initiatives by others

Example of Philosophy Statement

- Preventing accidents is good business. Increasing quality and safety lead to decreasing cost and schedule and, in the long term, increase profits.
- Safety and productivity go hand in hand.
- Safety commitment, openness and honesty are valued and rewarded in the organization
- Safety analysis must be surfaced without fear. Safety analysis will be conducted without blame.

Safety Management Structure

- Need clear definition of expectations, responsibilities, authority, accountability at all levels
- Higher levels control interactions among lower components
- Feedback and coordination among entities
- Leading indicators and ways to identify when losing effectiveness

Questions about assigning responsibility:

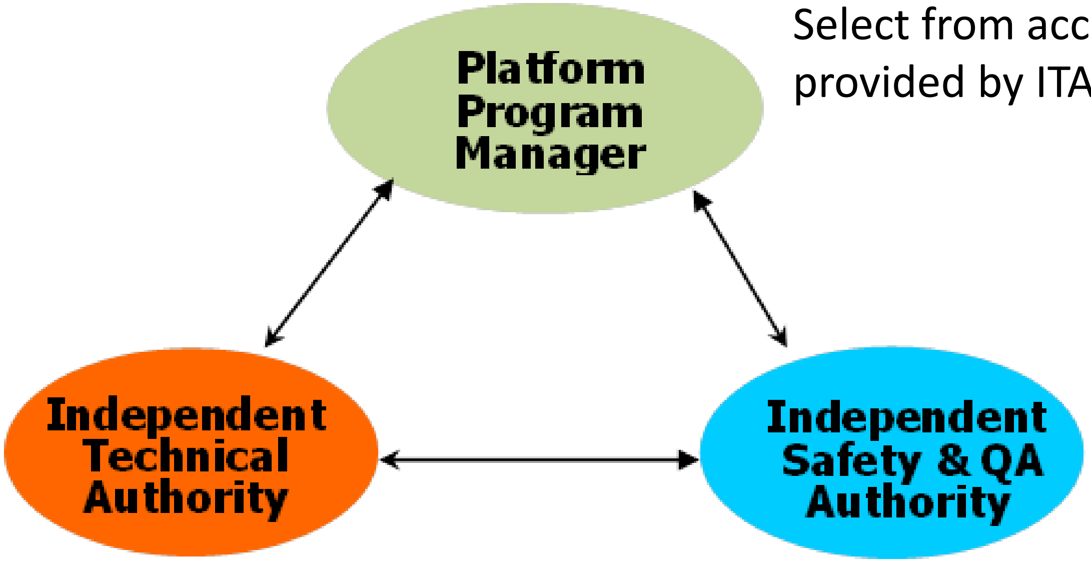
1. Is this a rotational assignment or a choice by those passionate about safety?
2. Is there a career path within safety?
3. Is everyone responsible for safety? Are specific responsibilities, etc., assigned at all levels of management structure?
4. Is someone assigned to be responsible for ensuring SMS is designed and working properly?

Place in the Organization

Questions to ask:

- Is there an enterprise-level group with direct access to top management?
  - Coordination
  - Make sure activities are being implemented and effective
  - Ensure management decisions are informed
- Is safety a staff-level function? If so does it have impact on line operations? Are there responsibilities at each level?
- Is system/engineering safety separate from workplace safety (EHS)?
- Is system safety separate from system engineering? (e.g., in QA?)
- Do decision makers have direct access to information needed to make safety-related decisions when they need it?

SUBSAFE Independent Technical Authority



Platform Program Manager

Independent Technical Authority

Independent Safety & QA Authority

Select from acceptable options provided by ITA

Provide technically acceptable alternatives
Assure adherence to standards

Compliance verification

Communication and Coordination

- Are there people with overlapping responsibilities? If so, are there means for coordination?
  - When changes made?
  - Working groups? (reducing uncoordinated and fragmented activities)
- What communication exists between development and operations?
- Is there a way of determining whether information flow is actually occurring?

Managing and Controlling Change

- Are management of change procedures documented? Being followed? Effective? Practical (too expensive? time consuming? difficult?)?
- Who is responsible to ensure that MOC procedures are being followed? Feedback channels?
- What about unplanned changes?
  - How detect that critical, unplanned changes have occurred? (e.g, leading indicators?)
  - Who is responsible to respond?
  - How ensure that risk is not being informally re-evaluated downward?

Designing and Encouraging Feedback

- Are appropriate feedback channels defined and working?
- What kinds of audits and performance assessments are performed? Are they based on the identified hazards and safety constraints? Is there an audit of whether safety control structure itself is working as designed?
- How is audit information gathered? Used? Is the goal to find deviations and potentially punitive or to identify improvements?
- Are knowledge of safety and training part of the assessments?

Designing and Encouraging Feedback (2)

- How are incidents and accidents investigated?
  - Are systemic factors identified or just symptoms?
  - Is the goal to identify a root cause or someone to blame?
  - Is the whole safety management structure investigated for its role?
  - Are managers responsible for investigating accidents in their chain of command? Or is there a financially and managerially independent investigation group?
  - Is responsibility assigned for ensuring fixes implemented?
  - Is there a check that the fixes have been implemented?
  - Is there any check that the fixes are effective?

Designing and Encouraging Feedback (3)

- What types of reporting systems exist in your organization or industry?
- Is it easy to use? Is it encouraged? Is there feedback to the reporter? Is there an anonymous channel for feedback? Is there protection for the reporter?
- How does a potential reporter know when to use reporting channel?
- Do you have a “just culture”?

Risk Management

- Activities associated with identifying hazards, identifying their potential causes, and using info to reduce risk through design of products, processes, services, and workplaces.
- Embedded somewhere in SMS (where is yours?)
- Risk (vs. severity and likelihood):
  - Effectiveness of the controls used to enforce safe system behavior
  - Design and operation of the safety management structure
  - Note: Does not require determination of likelihood of events but rather an evaluation of the controls being used to prevent them.
- Need to:
  - Design procedures for performing technical risk management activities
  - Assign responsibility for implementing these procedures to components of the safety control structure
  - Create leading indicators to identify when risk increasing

Leading Indicators

- Identify when risk increasing before a major loss occurs

- Based on assumptions made about:
  - How products and processes will behave
  - How components of safety control structure will behave
  - Environment in which they operate

- Violation of assumptions undermine original risk identification and management assumptions.

- Leading indicators are characteristics of a system, organization, or organization's operation indicating that not operating as assumed when designed.

- Surprisingly, violations of probabilistic risk calculations usually are ignored and not re-evaluated after concrete evidence that actual use of system violating assumptions made in calculation.

Risk Management (2)

- Who designs hazard analysis activities?
- Who is responsible for performing them? How does the information produced get to those who need to use it?
- What types of leading indicators are used? What happens if they signal a potential problem?
- Who is responsible for gathering/evaluating evidence about the truth of the probabilistic risk assessments?
- Who is responsible for determining that SMS (including personal behavior) is not degrading over time? How is this done?
- What feedback and evidence is used to keep mental models of decision makers consistent with actual level of risk at any time?
- Virtually always precursors before a major loss. Part of “noise/signal” problem. Does your organization have a way of identifying the difference?

Education and Training

- Is there education for everyone with safety responsibilities?
- Does it include the safety philosophy statement? Hazards and how to recognize them? Safety constraints? Priorities and how to make decisions?
- Does training include “why” and not just “what”? (education vs. training). Does it include previous accidents and what changes made to prevent a reoccurrence?
- What types of special, in-depth training about hazards for people interacting with complex systems (e.g., automation, robots)
- [List of what need to know in accompanying paper]
- Is training one-time or continual?
- Is there an assessment process for training effectiveness?
- What types of learning is done from incidents and accidents?
- Are managers involved in safety training?

Learning and Continual Improvement

- What process is in place to ensure continual learning and improvement?

Safety Information System (1)

- Key to success of SMS; info may be collected per company or industry
- After accidents, often discovered the information needed to prevent loss existed but was not used or not available to those who needed it.
- Has anyone done an evaluation of your SIS lately?
- Is information collected primarily because needed for government reports?
- Is an evaluation done periodically to see if people getting the information they need? Has a study of what each person needs for their responsibilities been done?
- Is “data” turned into “information”?

Safety Information System (2)

- Is data collected but never analyzed? (e.g., no time)
- Is data presented in a form people can learn from? Apply to daily jobs? Use throughout product life cycle?
- Is SIS integrated into environment in which safety-related decisions are made?
- Do you get the information you need? Do you know where to find it?
  - Find out what information people need. Make sure can get it when needed and in a usable form.
- Is collected information filtered (e.g., accidents and incidents blamed on operators)? Suppressed? Unreliable? Are checklists used for collection? Do lawyers influence what is collected and recorded?

Summary: Effective SMS requires

- Commitment and leadership at all levels
- A strong corporate safety culture
- A clearly articulated safety vision, values, and procedures, shared among stakeholders
- Appropriate assignment of responsibility, authority, accountability
- Feedback channels that provide accurate view of state of safety at all levels of the SMS
- Integration of safety into development and operations (not a separate and independent group or separate subculture)
- Individuals with appropriate knowledge, skills, and ability

- Designated process for resolving tensions between safety priorities and other priorities
- Risk awareness and communication channels for disseminating safety information
- Controls on system migration toward higher risk
- Effective and usable safety information system
- Continual improvement and learning
- Education, training, and capability development.