

Introduction



- What I have learned in 45 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)

AGENDA



- What is an SMS?
- Safety culture
- Management Structure
- Risk Management
- Controlling Change
- Safety Information System
- Education and Continual Improvement

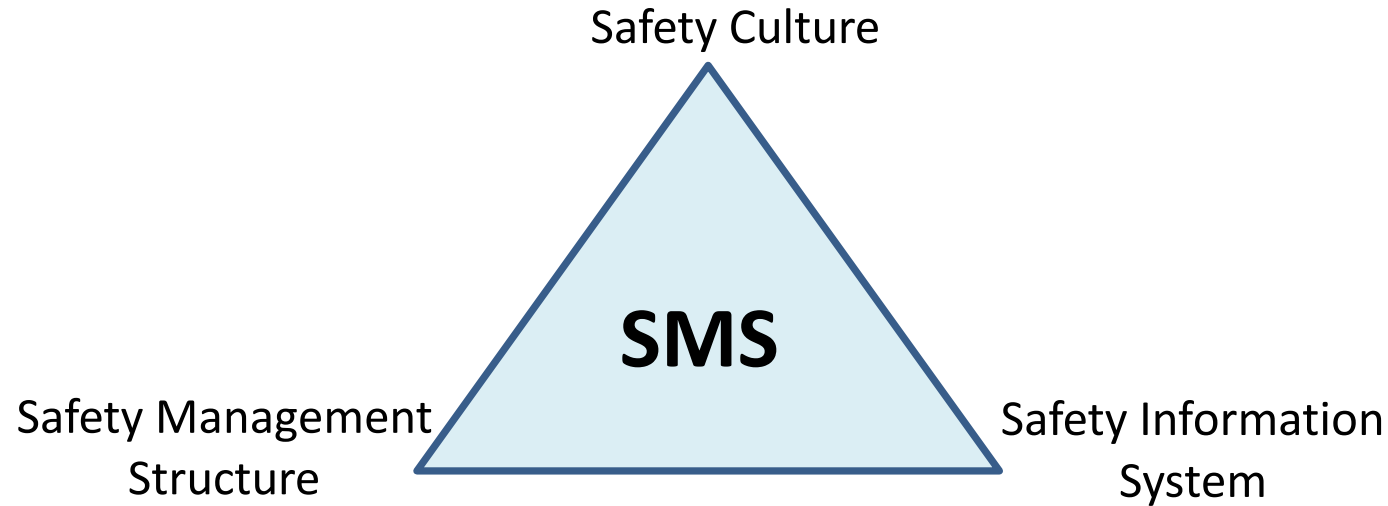
More Information:



- Nancy Leveson, *Engineering a Safer World*, MIT Press, 2012
(Particularly chapters 12-14)
- Nancy Leveson, *Introduction to System Safety Engineering*, MIT Press, 2023, (Particularly Chapters 4 and 14 and Appendices)

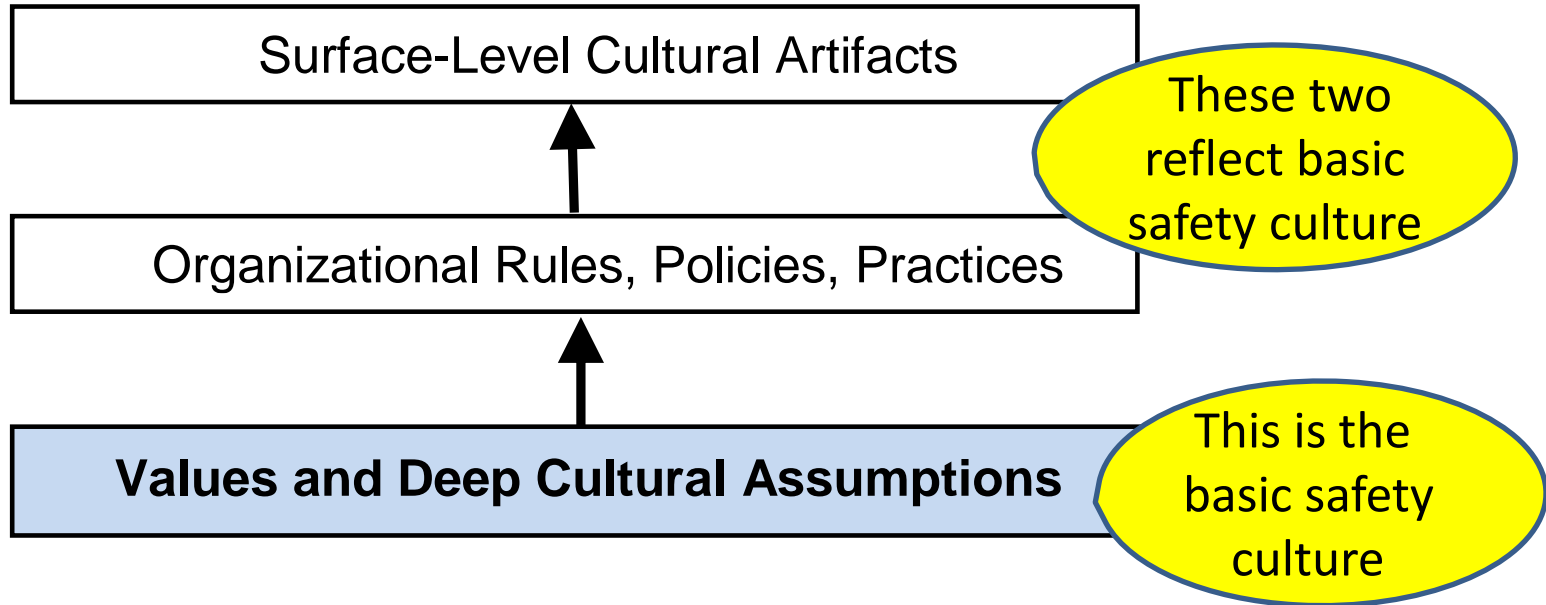
[New book on safety management in preparation, with Capt. Gus Larard]

Three Parts to an SMS



- 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)



- 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

Are these part of the safety culture?

- Guidelines for doing FTA
- FMEA/FMECA results for your product
- Company safety policy
- Belief that safety and productivity conflict

What are some other cultural beliefs and assumptions?

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 regulations 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, increasing profits.
- Safety and productivity go hand in hand.
- Safety commitment, openness and honesty are valued and rewarded in the organization
- Safety concerns must be surfaced without fear. Safety analysis will be conducted without blame.

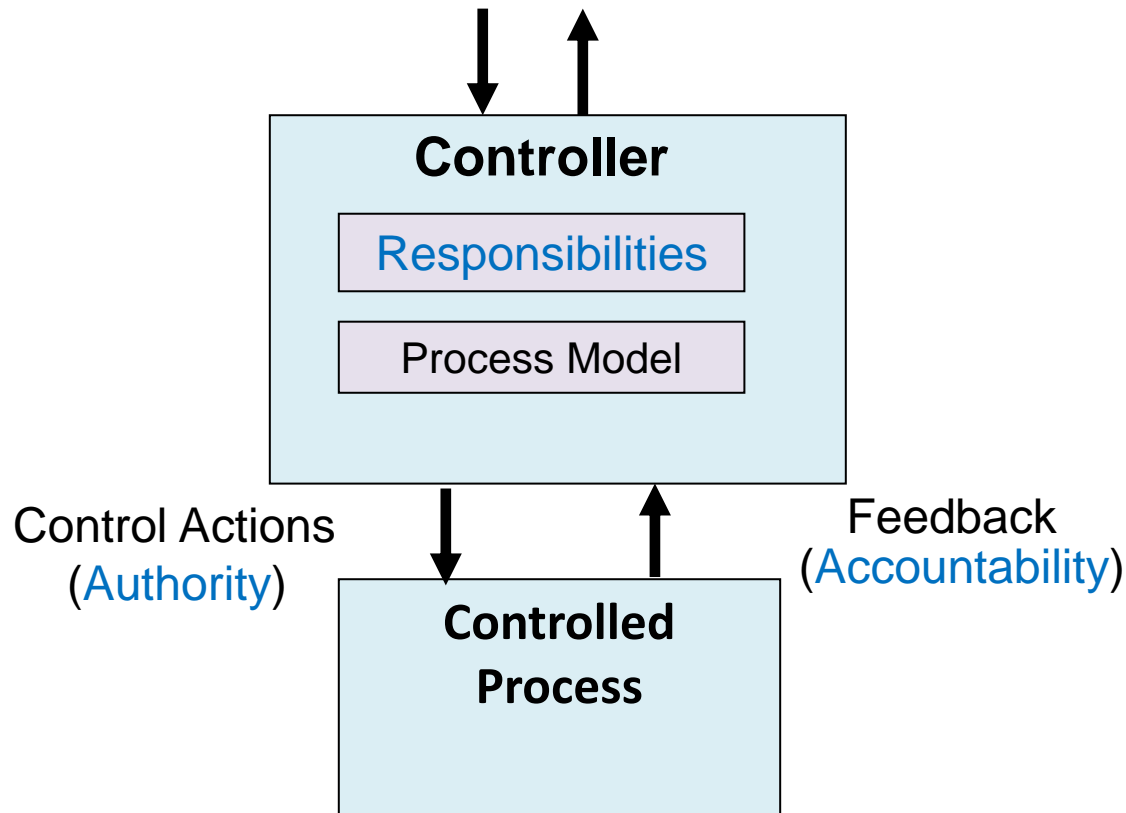
Of course, management commitment is essential

Tips for how management can improve safety culture:

- Set the goals and values to be used in decision-making; establish and communicate what is expected in safety-related decision-making and behavior.
- Support employees who exhibit reasonable concern for safety in their work.
- Create a short, written safety philosophy and more detailed safety policy.
- Ensure safety philosophy and policy have wide buy-in from managers and employees.
- Follow the safety philosophy in your decision-making and expect the same from everyone.
- Emphasize building safety in and not assurance or after-the-fact assessment.
- Perform assessment with the goal of providing evidence that the design is not safe, not providing an argument that it is safe.
- Require objective quality evidence for assurance or certification. Avoid focusing on compliance and paperwork.
- Demonstrate commitment to safety by
 - Personal involvement
 - Setting priorities and following through on them
 - Setting up appropriate organizational structures
 - Appointing high-ranking, respected leaders to safety-related roles and responsibilities
 - Providing adequate resources for safety-efforts to be effective
 - Assigning the best employees to safety-related activities, not just those who are nonessential or expendable
 - Rewarding employees for safety efforts
 - Responding to initiatives by others.
- Minimize blame; focus on “why” not “who”
- Engineer the incentive structure to encourage desirable safety-related behavior
- Listen and be willing to hear bad news. Follow through.

Safety Management Structure

- Make a quick drawing of the safety management structure in your organization.
- Note the assignment of responsibilities



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 components
- 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?

Tips for assigning responsibility:

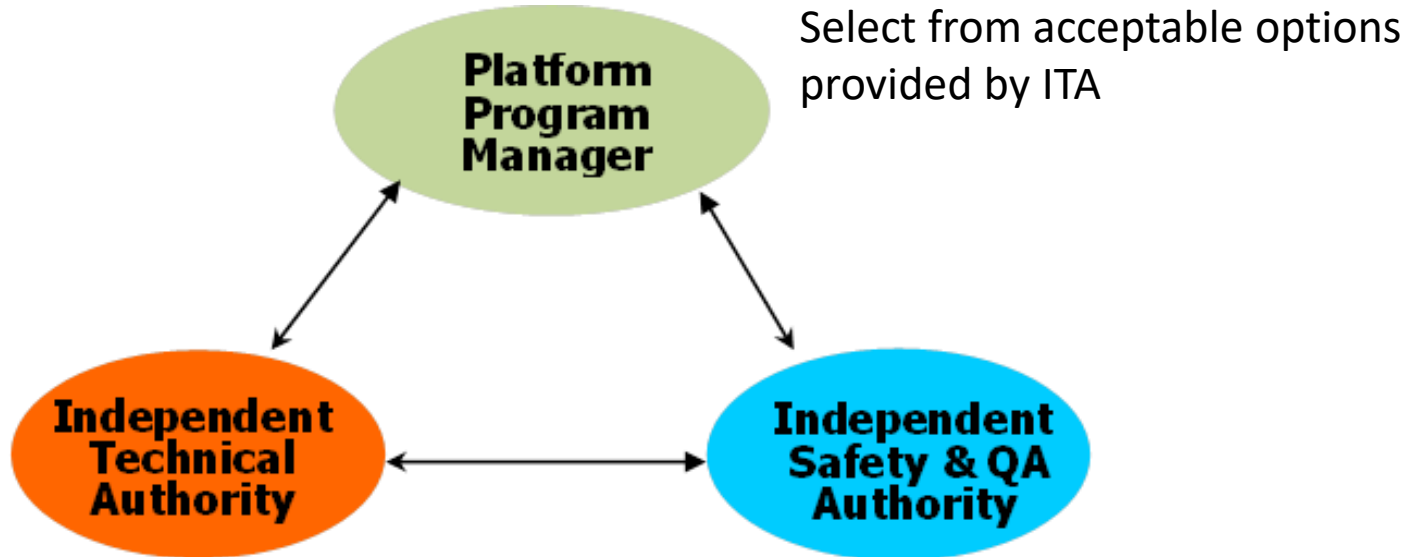
- Appoint leaders who are passionate about safety
- Create career paths for those committed to preventing losses
- Provide a clear definition of expectations, responsibilities, authority and accountability at all levels of the safety control structure
- Do not make everyone responsible for safety and do not push responsibility downward without appropriate decision-making and oversight at the higher levels of the organization.
- Establish appropriate safety responsibilities for contractors and oversee their activities.
- Assign someone to be responsible for ensuring the SMS itself 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



Provide technically acceptable alternatives
Assure adherence to standards

Compliance verification

Tips for where to locate activities in the control structure:

- Create a high-level group with enterprise-level responsibilities, such as ensuring required activities are taking place and are effective and for providing leadership and coordination. This group ensures a common methodology and approach is being used by everyone.
 - They must have a direct path to top management and provide input to management decision-making.
 - They must report to someone with influence and be seen as having the support of senior management.
- Assign responsibilities so that safety is not just a staff function but has direct impact and influence on line operations.
- Integrate the safety function into the system engineering function. Do not separate system safety and system engineering in product development organizations.
- Include system safety expertise in all departments or groups where safety-related decision-making occurs.
- Provide independent oversight in addition to integrated functions.
- Ensure decision makers have direct links to those who can provide safety analysis and information.
- Create direct communication channels between any parts of the organization where there are safety-related activities and safety decisions need to be made.
- Consider implementing the SUBSAFE separation of powers structure. At the least, ensure that technical decisions are independent of programmatic ones.

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
 - A function of the 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



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?

Leading Indicators



- Identify when risk increasing before a major loss occurs
- Risk analysis is 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.

Tips for managing and controlling change:

- Design controls and MOC policy to prevent unsafe changes and detect if they occur.
- Evaluate all planned changes, including temporary ones, for their potential impact on safety.
- Assign responsibility for ensuring that MOC procedures are enforced and are being followed. If they are not, find out why and fix the problems.
- Create documentation and procedures that minimize the cost of performing the MOC procedures.
- Create ways to identify unplanned changes that could be unsafe and to respond to these changes.
 - Create assumption-based leading indicators and a risk management program that effectively monitors and responds when potentially unsafe changes are identified.
 - Record assumptions during design and development of the organizational structure, the SMS, the products, and the workplace.
 - Create shaping and hedging actions and a leading indicator checking program, including audits and performance checking as well as signposts.
 - Implement leading indicators to signal when controls are becoming ineffective.
- Ensure that decision makers have information about the current level of risk and the state of the designed safety controls.
- Assign responsibility to respond when feedback shows that the application of the MOC procedures does not match the true level of risk.
- Remain vigilant against the degradation of the safety control structure and the safety culture over time and any increase in complacency.

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?

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?

Tips for designing communication and coordination:

- Ensure information necessary for decision-making involving safety is available to decision makers.
- Provide communication channels and a way to coordinate activities among those with overlapping safety responsibilities.
- Make sure safety activities are not fragmented and uncoordinated.
- Define required interactions, and ensure that necessary information flow among them is defined and used.
- Identify and document necessary safety-related communication channels among all components of the safety control structure.
- Ensure that feedback and coordination channels exist and are working.
- Consider establishing safety working groups.

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 thus is potentially punitive or is the goal 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)

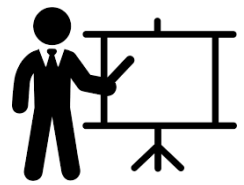


- What types of reporting systems exist in your organization or industry?
- Is it easy to use? Is it encouraged? Is there feedback to the reporter? Is there an anonymous channel for feedback? Is there protection for the reporter?
- How does a potential reporter know when to use reporting channel?
- Do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

Tips for maintaining accurate risk perception:

- Provide information beyond the standard risk matrix including specific existing hazards and ways to manage them.
- Provide ways of updating risk assessment, using at least the original hazard analysis.
- Protect against informal downgrading of risk when accidents do not occur.
- Focus on identifying and implementing ways to fight ignorance, arrogance, and complacency (see SUBSAFE).

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)
- 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?

Tips for training and education:

- Educate; don't just train
- Make sure everyone understands their roles and responsibilities, why the system was designed the way it was, information about hazards and safety constraints enforced by the controls, and the risks they are taking in the decisions they make.
- Include "why" and not just "what."
- Include in everyone's training:
 - The system hazards and the reasons behind safety-critical procedures and operational rules that are related to their jobs.
 - The potential result of removing or overriding controls, changing prescribed procedures, and inattention to safety-critical features and operations.
- Make sure the causes of past accidents in the same or similar systems are well disseminated and understood.
- Give people the opportunity to practice problem-solving involving safety
- Teach general strategies rather than specific responses so that controllers can develop skills for dealing with unanticipated events.
- Teach operators how to test hypotheses in an appropriate way and provide ways for them to learn in this way.
- Include overlearning and continual practice for emergency procedures.
- Review contingency procedures before any safety-critical activity.
- Provide continuous training and not just a one-time event when hired.
- Teach about recent events and trends.
- Consider having managers provide at least part of the safety training.

Learning and Continual Improvement

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



Tips for creating a learning culture:

- Design and ensure the continued efficacy of audits, performance assessments, and reporting systems.
- Audit the safety control structure itself (including all levels) and the effectiveness of the designed controls.
- Design audits so they are constructive learning experiences and not a judgmental process.
 - Include as participants members of the groups that are being audited.
 - Use audits as a way to improve safety and as a learning activity and not to evaluate employees.
- Take advantage of audits to evaluate the effectiveness of training and education activities and use them to provide feedback (knowledge assessment) to be used for improving training activities.
- Create effective system-level accident/incident causal analysis procedures that focus on *why* and not *who*.
- Create incident and investigation procedures that identify systemic factors and not just the symptoms of the deeper problems.
- Embed the investigation procedures in an organizational structure that allows exploitation of the results. Assigning blame or finding a root cause should not be the goal.
- Create an accident investigation process that is managerially and financially independent from those in the immediate management structure involved. Consider using highly trained teams with independent budgets and high-level management. Follow up on recommendations to determine whether they were effective and, if not, then why.
- Ensure that reporting systems are easy to use and available and anonymous reporting channels exist.
 - Encourage reporting and train people to know when it should be used.
 - Provide a written policy.
 - Maximize accessibility, minimize anxiety, and act on information obtained.
 - Provide feedback to those using the reporting channels. Reporters need to feel that their concerns are not being ignored.
- Create a learning culture using feedback loops and the checking during operations of assumptions made in the safety analysis. Make everyone responsible for coming up with solutions and show that their input s matters.
- Assign responsibility to someone in the safety control structure to ensure that learning and improvement is occurring.

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?

Tips for designing a safety information system:

- Accurate and timely feedback and data are important.
- The SIS should provide the information necessary to detect trends, changes, and other precursors to an accident; to evaluate the effectiveness of the safety controls; to compare models and risk assessments with actual behavior; and to learn from events and improve the SMS.
- Use the defined responsibilities of those in the safety control structure to identify the information they need to keep their process models accurate enough for good decision-making.
- Understand the limitations of your collected data.
- To be most useful, information must be accurate and timely, and it must be disseminated to the appropriate people in a useful form.
- Find ways to collect data that minimize distortion of the data (filtering, suppression, and unreliability).
- Keep detailed information on actual safety-related incidents, and ensure that information gets to the people who need it.
- Create ways to improve the comprehension and reliability of data collection.
- Try to include statistical significance on numeric data if possible.
- Use STPA to identify what data needs to be collected, and provide guidance on the importance of the events that are occurring.
- Collect data to validate the hazard analysis results and to identify factors that were thought to be eliminated or mitigated.
- Ensure that data is analyzed and not just collected.
- Present data in a way that people can learn from it and apply it to their daily jobs.
- Keep data up to date.
- Document design rationale and intent, and provide traceability to assist in the change management process.
- Tailor the information provided and the presentation format to the needs of those receiving it.
- Providing too much data, particularly raw data, can be as dangerous as providing too little.
- Adapt the presentation of information to the cognitive styles of the users, and integrate it into the environment in which safety-related decisions are made.
- Use the hazard analysis and safety management system design processes to determine what information is needed, when it is needed, and how it will be used.

Other SMS topics: Managing Safety During

- Development
- Operations and designing/updating operational procedures
- Maintenance

Tips for managing safety-critical development:

- Start safety efforts early.
- Spend time on planning up front. It will save much more in time and resources than trying to fix problems identified later.
- Design safety into the system; do not wait to add it to a completed design.
- Do not focus on generating a lot of paperwork and documentation. It does not make a system safer; it simply wastes resources.
- Do not rely on compliance with standards to prevent accidents. More than compliance is required.
- Document and validate assumptions and design rationale. Establish traceability between safety requirements and constraints, hazard analysis, identified causal scenarios, and design features to eliminate or control hazards.
- Minimize unnecessary complexity and features that increase complexity.
- Use system engineering processes that integrate the design of hardware, software, and human factors.
- Place high priority on communication about safety in large development projects. Use working groups and other communication channels and ensure they are effective.
- Integrate safety engineers and activities into the main engineering design process.

Tips for creating and updating operational procedures:

- Explain the rationale behind the procedures.
- Keep procedures up to date by periodically revisiting them and monitoring when changes in the system or environment make updating necessary.
- Monitor whether procedures are being followed. If not, identify why people feel the need to change them. Evaluate the gap between specified procedures and actual behavior. Encourage input from those deviating from procedures to explain why and participation in any evaluation and correction activities.
- Create procedures through a partnership between operators, system designers, system safety engineers, and human factors experts. Perform an independent review of the resulting procedures along with testing or other types of evaluation.

Tips for maintenance:

- Identify safety-critical equipment.
- Provide proper resources and training.
- Ensure that failure and maintenance information is being recorded accurately.
- Assign oversight responsibilities to ensure that proper maintenance is being performed and that an accurate view of the state of the equipment is provided to decision makers.
- Use preventative maintenance rather than run critical equipment until failure.
- Before returning to potentially dangerous operation:
 - Test the alarms and other equipment to ensure it has been reactivated,
 - Ensure the maintained equipment is operating correctly.
- Provide independent maintenance of redundant components when relying on redundancy for safety.
- Perform trend analysis to warn when risk may be increasing and about any changes in maintenance procedures that are increasing risk.
- Do not startup or perform any safety-related activities when safety-critical equipment is not operational.
- Create ways to ensure that safety-interlocks are reset after maintenance activities.
- Create a maintenance information system that contains up-to-date information about maintenance activities—including instructions and maintenance activities along with any relevant trend analysis. This information should be easy to retrieve and should provide an accurate view of the current state of the plant equipment.

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

SUMMARY



Effective SMS requires

- 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 (including leading indicators to detect increases in risk)
- Effective and usable safety information system
- Continual improvement and learning
- Education, training, and capability development.