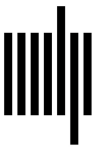
Engineering a Safer World

Systems Thinking Applied to Safety

By: Nancy G. Leveson

Citation:

Engineering a Safer World: Systems Thinking Applied to Safety
By: Nancy G. Leveson
DOI: 10.7551/mitpress/8179.001.0001
ISBN (electronic): 9780262298247
Publisher: The MIT Press
Published: 2016



The MIT Press

13 Managing Safety and the Safety Culture

The key to effectively accomplishing any of the goals described in the previous chapters lies in management. Simply having better tools is not enough if they are not used. Studies have shown that management commitment to the safety goals is the most important factor distinguishing safe from unsafe systems and companies [101]. Poor management decision making can undermine any attempts to improve safety and ensure that accidents continue to occur.

This chapter outlines some of the most important management factors in reducing accidents. The first question is why managers should care about and invest in safety. The answer, in short, is that safety pays and investment in safety provides large returns over the long run.

If managers understand the importance of safety in achieving organizational goals and decide they want to improve safety in their organizations, then three basic organizational requirements are necessary to achieve that goal. The first is an effective safety control structure. Because of the importance of the safety culture in how effectively the safety control structure operates, the second requirement is to implement and sustain a strong safety culture. But even the best of intentions will not suffice without the appropriate information to carry them out, so the last critical factor is the safety information system.

The previous chapters in this book focus on what needs to be done during design and operations to control safety and enforce the safety constraints. This chapter describes the overarching role of management in this process.

13.1 Why Should Managers Care about and Invest in Safety?

Most managers do care about safety. The problems usually arise because of misunderstandings about what is required to achieve high safety levels and what the costs really are if safety is done right. Safety need not entail enormous financial or other costs.

A classic myth is that safety conflicts with achieving other goals and that tradeoffs are necessary to prevent losses. In fact, this belief is totally wrong. Safety is a prerequisite for achieving most organizational goals, including profits and continued existence.

History is replete with examples of major accidents leading to enormous financial losses and the demise of companies as a result. Even the largest global corporations may not be able to withstand the costs associated with such losses, including loss of reputation and customers. After all these examples, it is surprising that few seem to learn from them about their own vulnerabilities. Perhaps it is in the nature of mankind to be optimistic and to assume that disasters cannot happen to us, only to others. In addition, in the simpler societies of the past, holding governments and organizations responsible for safety was less common. But with loss of control over our own environment and its hazards, and with rising wealth and living standards, the public is increasingly expecting higher standards of behavior with respect to safety.

The "conflict" myth arises because of a misunderstanding about how safety is achieved and the long-term consequences of operating under conditions of high risk. Often, with the best of intentions, we simply do the wrong things in our attempts to improve safety. It's not a matter of lack of effort or resources applied, but how they are used that is the problem. Investments in safety need to be funneled to the most effective activities in achieving it.

Sometimes it appears that organizations are playing a sophisticated version of Whack-a-Mole, where symptoms are found and fixed but not the processes that allow these symptoms to occur. Enormous resources may be expended with little return on the investment. So many incidents occur that they cannot all be investigated in depth, so only superficial analysis of a few is attempted. If, instead, a few were investigated in depth and the systemic factors fixed, the number of incidents would decrease by orders of magnitude.

Such groups find themselves in continual firefighting mode and eventually conclude that accidents are inevitable and investments to prevent them are not cost-effective, thus, like Sisyphus, condemning themselves to traverse the same vicious circle in perpetuity. Often they convince themselves that their industry is just more hazardous than others and that accidents in their world are inevitable and are the price of productivity.

This belief that accidents are inevitable and occur because of random chance arises from our own inadequate efforts to prevent them. When accident causes are examined in depth, using the systems approach in this book, it becomes clear that there is nothing random about them. In fact, we seem to have the same accident over and over again, with only the symptoms differing, but the causes remaining fairly constant. Most of these causes could be eliminated, but they are not. The

precipitating immediate factors, like a stuck valve, may have some randomness associated with them, such as which valve actually precipitates a loss. But there is nothing random about systemic factors that have not been corrected and exist over long periods of time, such as flawed valve design and analysis or inadequate maintenance practices.

As described in previous chapters, organizations tend to move inexorably toward states of higher risk under various types of performance pressures until an accident become inevitable. Under external or internal pressures, projects start to violate their own rules: "We'll do it just this once—it's critical that we get this procedure finished today." In the Deepwater Horizon oil platform explosion of 2010, cost pressures led to not following standard safety procedures and, in the end, to enormous financial losses [18]. Similar dynamics occurred, with slightly different pressures, in the *Columbia* Space Shuttle loss where the tensions among goals were created by forces largely external to NASA. What appear to be short-term conflicts of other organizational goals with safety goals, however, may not exist over the long term, as witnessed in both these cases.

When operating at elevated levels of risk, the only question is which of many potential events will trigger the loss. Before the *Columbia* accident, NASA manned space operations was experiencing a slew of problems in the orbiters. The head of the NASA Manned Space Program at the time misinterpreted the fact that they were finding and fixing problems and wrote a report that concluded risk had been reduced by more than a factor of five [74]. The same unrealistic perception of risk led to another report in 1995 recommending that NASA "restructure and reduce overall safety, reliability, and quality assurance elements" [105].

Figure 13.1 shows some of the dynamics at work.[1] The model demonstrates the major sources of the high risk in the Shuttle program at the time of the *Columbia* loss. In order to get the funding needed to build and operate the space shuttle, NASA had made unachievable performance promises. The need to justify expenditures and prove the value of manned space flight has been a major and consistent tension between NASA and other governmental entities: The more missions the Shuttle could fly, the better able the program was to generate funding. Adding to these pressures was a commitment to get the International Space Station construction complete by February 2004 (called "core complete"), which required deliveries of large items that could only be carried by the shuttle. The only way to meet the deadline was to have no launch delays, a level of performance that had never previously been achieved [117]. As just one indication of the pressure, computer screen savers were mailed to managers in NASA's human spaceflight program that depicted a clock counting down (in seconds) to the core complete deadline [74].

1. Appendix D explains how to read system dynamics models, for those unfamiliar with them.

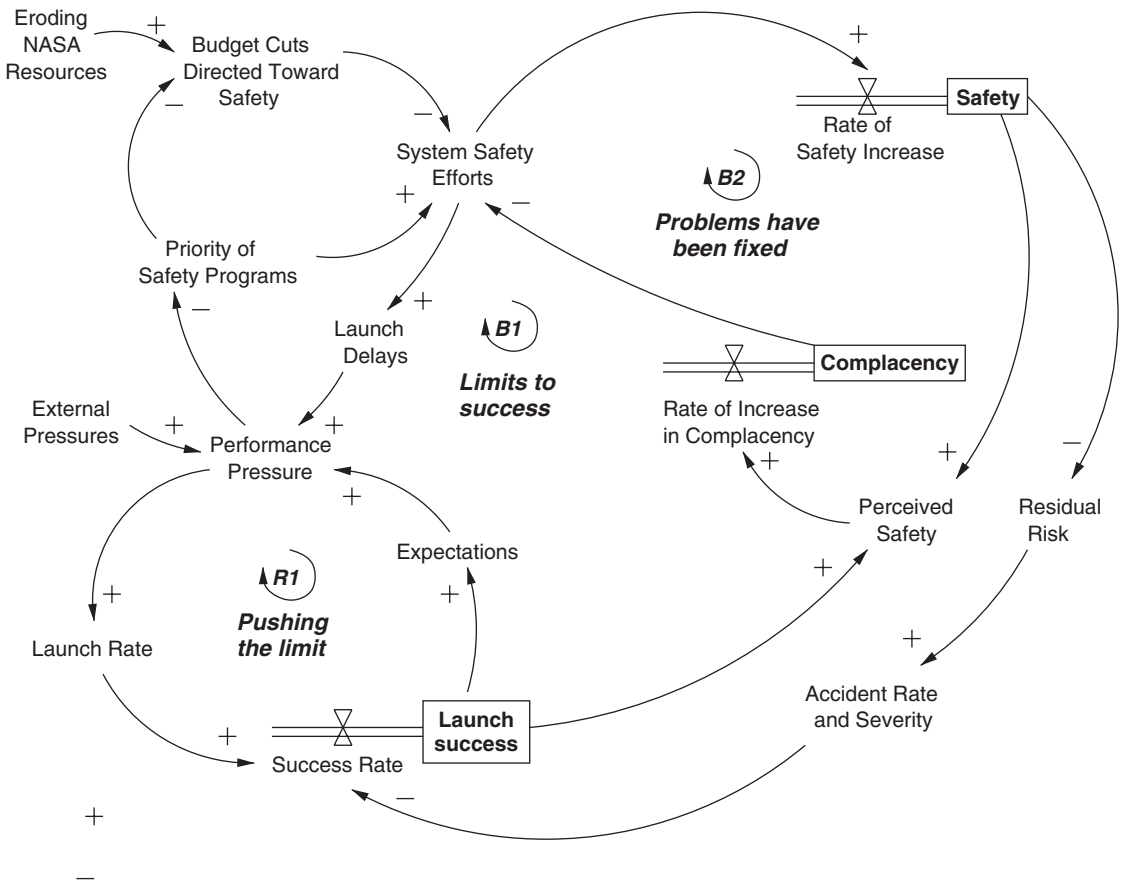


Figure 13.1
A simplified model of the dynamics of safety and performance pressures leading up to the *Columbia* loss. For a complete model, see [125].

The control loop in the lower left corner of figure 13.1, labeled R1 or *Pushing the Limit*, shows how as external pressures increased, performance pressure increased, which led to increased launch rates and thus success in meeting the launch rate expectations, which in turn led to increased expectations and increasing performance pressures. This reinforcing loop represents an unstable system and cannot be maintained indefinitely, but NASA is a "can-do" organization that believes anything can be accomplished with enough effort [136].

The upper left loop represents the Space Shuttle safety program, which when operating effectively is meant to balance the risks associated with loop R1. The external influences of budget cuts and increasing performance pressures, however, reduced the priority of safety procedures and led to a decrease in system safety efforts.

Adding to the problems is the fact that system safety efforts led to launch delays when problems were found, which created another reason for reducing the priority of the safety efforts in the face of increasing launch pressures.

While reduction in safety efforts and lower prioritization of safety concerns may lead to accidents, accidents usually do not occur for a while so false confidence is created that the reductions are having no impact on safety and therefore pressures increase to reduce the efforts and priority even further as the external and internal performance pressures mount.

The combination of the decrease in safety efforts along with loop B2 in which fixing the problems that were being found increased complacency, which also contributed to reduction of system safety efforts, eventually led to a situation of unrecognized high risk.

When working at such elevated levels of risk, the only question is which of many potential events will trigger the loss. The fact that it was the foam and not one of the other serious problems identified both before and after the loss was the only random part of the accident. At the time of the *Columbia* accident, NASA was regularly flying the Shuttle with many uncontrolled hazards; the foam was just one of them.

Often, ironically, our successful efforts to eliminate or reduce accidents contribute to the march toward higher risk. Perception of the risk associated with an activity often decreases over a period of time when no losses occur even though the real risk has not changed at all. This misperception leads to reducing the very factors that are preventing accidents because they are seen as no longer needed and available to trade off with other needs. The result is that risk increases until a major loss occurs. This vicious cycle needs to be broken to prevent accidents. In STAMP terms, the weakening of the safety control structure over time needs to be prevented or detected before the conditions occur that lead to a loss.

System migration toward states of higher risk is potentially controllable and detectable [167]. The migration results from weakening of the safety control structure. To achieve lasting results, strong operational safety efforts are needed that provide protection from and appropriate responses to the continuing environmental influences and pressures that tend to degrade safety over time and that change the safety control structure and the behavior of those in it.

The experience in the nuclear submarine community is a testament to the fact that such dynamics can be overcome. The SUBSAFE program (described in the next chapter) was established after the loss of the *Thresher* in 1963. Since that time, no submarine in the SUBSAFE program, that is, satisfying the SUBSAFE requirements, has been lost, although such losses were common before SUBSAFE was established.

The leaders in SUBSAFE describe other benefits beyond preventing the loss of critical assets. Because those operating the submarines have complete confidence

in their ships, they can focus solely on the completion of their mission. The U.S. nuclear submarine program's experience over the past forty-five years belies the myth that increasing safety necessarily decreases system performance. Over a sustained period, a safer operation is generally more efficient. One reason is that stoppages and delays are eliminated.

Examples can also be found in private industry. As just one example, because of a number of serious accidents, OSHA tried to prohibit the use of power presses where employees had to place one or both hands beneath the ram during the production cycle [96]. After vehement protests that the expense would be too great in terms of reduced productivity, the requirement was dropped: Preliminary motion studies showed that reduced production would result if all loading and unloading were done with the die out from under the ram. Some time after OSHA gave up on the idea, one manufacturer who used power presses decided, purely as a safety and humanitarian measure, to accept the production penalty. Instead of reducing production, however, the effect was to increase production from 5 to 15 percent, even though the machine cycle was longer. Other examples of similar experiences can be found in *Safeware* [115].

The belief that safer systems cost more or that building safety in from the beginning necessarily requires unacceptable compromises with other goals is simply not justified. The costs, like anything else, depend on the methods used to achieve increased safety. In another ironic twist, in the attempt to avoid making tradeoffs with safety, systems are often designed to optimize mission goals and safety devices added grudgingly when the design is complete. This approach, however, is the most expensive and least effective that could be used. The costs are much less and in fact can be eliminated if safety is built into the system design from the beginning rather than added on or retrofitted later, usually in the form of redundancy or elaborate protection systems. Eliminating or reducing hazards early in design often results in a simpler design, which in itself may reduce both risk and costs. The reduced risk makes it more likely that the mission or system goals will be achieved.

Sometimes it takes a disaster to "get religion" but it should not have to. This chapter was written for those managers who are wise enough to know that investment in safety pays dividends, even before this fact is brought home (usually too late) by a tragedy.

13.2 General Requirements for Achieving Safety Goals

Escaping from the Whack-a-Mole trap requires identifying and eliminating the systemic factors behind accidents. Some common reasons why safety efforts are often not cost-effective were identified in chapter 6, including:

- Superficial, isolated, or misdirected safety engineering activities, such as spending most of the effort proving the system is safe rather than making it so
- Starting too late
- Using techniques inappropriate for today's complex systems and new technology
- Focusing only on the technical parts of the system, and
- Assuming systems are static throughout their lifetime and decreasing attention to safety during operations

Safety needs to be managed and appropriate controls established. The major ingredients of effective safety management include:

- Commitment and leadership
- A corporate safety policy
- Risk awareness and communication channels
- Controls on system migration toward higher risk
- A strong corporate safety culture
- A safety control structure with appropriate assignment of responsibility, authority, and accountability
- A safety information system
- Continual improvement and learning
- Education, training, and capability development

Each of these is described in what follows.

13.2.1 Management Commitment and Leadership

Top management concern about safety is the most important factor in discriminating between safe and unsafe companies matched on other variables [100]. This commitment must be genuine, not just a matter of sloganeering. Employees need to feel they will be supported if they show concern for safety. An Air Force study of system safety concluded:

> Air Force top management support of system safety has not gone unnoticed by contractors. They now seem more than willing to include system safety tasks, not as "window dressing" but as a meaningful activity [70, pp. 5–11].

The B1-B program is an example of how this result was achieved. In that development program, the program manager or deputy program manager chaired the meetings of the group where safety decisions were made. "An unmistaken image of

the importance of system safety in the program was conveyed to the contractors" [70, p. 5].

A manager's open and sincere concern for safety in everyday dealings with employees and contractors can have a major impact on the reception given to safety-related activities [157]. Studies have shown that top management's support for and participation in safety efforts is the most effective way to control and reduce accidents [93]. Support for safety is shown by personal involvement, by assigning capable people and giving them appropriate objectives and resources, by establishing comprehensive organizational safety control structures, and by responding to initiatives by others.

13.2.2 Corporate Safety Policy

A policy is a written statement of the wisdom, intentions, philosophy, experience, and belief of an organization's senor managers that states the goals for the organization and guides their attainment [93]. The corporate safety policy provides employees with a clear, shared vision of the organization's safety goals and values and a strategy to achieve them. It documents and shows managerial priorities where safety is involved.

The author has found companies that justify not having a safety policy on the grounds that "everyone knows safety is important in our business." While safety may seem important for a particular business, management remaining mute on their policy conveys the impression that tradeoffs are acceptable when safety seems to conflict with other goals. The safety policy provides a way for management to clearly define the priority between conflicting goals they expect to be used in decision making. The safety policy should define the relationship of safety to other organizational goals and provide the scope for discretion, initiative, and judgment in deciding what should be done in specific situations.

Safety policy should be broken into two parts. The first is a short and concise statement of the safety values of the corporation and what is expected from employees with respect to safety. Details about how the policy will be implemented should be separated into other documents.

A complete safety policy contains such things as the goals of the safety program; a set of criteria for assessing the short- and long-term success of that program with respect to the goals; the values to be used in tradeoff decisions; and a clear statement of responsibilities, authority, accountability, and scope. The policy should be explicit and state in clear and understandable language what is expected, not a set of lofty goals that cannot be operationalized. An example sometimes found (as noted in the previous chapter) is a policy for employees to "be mindful of weak signals": This policy provides no useful guidance on what to do—both "mindful" and "weak signals" are undefined and undefinable. An alternative might be, "If you see

something that you think is unsafe, you are responsible for reporting it immediately." In addition, employees need to be trained on the hazards in the processes they control and what to look for.

Simply having a safety policy is not enough. Employees need to believe the safety policy reflects true commitment by management. The only way this commitment can be effectively communicated is through actions by management that demonstrate that commitment. Employees need to feel that management will support them when they make reasonable decisions in favor of safety over alternative goals. Incentives and reward structures must encourage the proper handling of tradeoffs between safety and other goals. Not only the formal rewards and rules but also the informal rules (social processes) of the organizational culture must support the overall safety policy. A practical test is whether employees believe that company management will support them if they choose safety over the demands of production [128].

To encourage proper decision making, the flexibility to respond to safety problems needs to be built into the organizational procedures. Schedules, for example, should be adaptable to allow for uncertainties and possibilities of delay due to legitimate safety concerns, and production goals must be reasonable.

Finally, not only must a safety policy be defined, it must be disseminated and followed. Management needs to ensure that safety receives appropriate attention in decision making. Feedback channels must be established and progress in achieving the goals should be monitored and improvements identified, prioritized, and implemented.

13.2.3 Communication and Risk Awareness

Awareness of the risk in the controlled process is a major component of safety-related decision making by controllers. The problem is that risk, when defined as the severity of a loss event combined with its likelihood, is not calculable or knowable. It can only be estimated from a set of variables, some of which may be unknown, or the information to evaluate likelihood of these variables may be lacking or incorrect. But decisions need to be made based on this unknowable property.

In the absence of accurate information about the state of the process, risk perception may be reevaluated downward as time passes without an accident. In fact, risk probably has not changed, only our perception of it. In this trap, risk is assumed to be reflected by a lack of accidents or incidents and not by the state of the safety control structure.

When STAMP is used as the foundation of the safety program, safety and risk are *a function of the effectiveness of the controls to enforce safe system behavior*, that is, the safety constraints and the control structure used to enforce those constraints.

Poor safety-related decision making on the part of management, for example, is commonly related to inadequate feedback and inaccurate process models. As such, risk is potentially knowable and not some amorphous property denoted by probability estimates. This new definition of risk can be used to create new risk assessment procedures.

While lack of accidents could reflect a strong safety control structure, it may also simply reflect delays between the relaxation of the controls and negative consequences. The delays encourage relaxation of more controls, which then leads to accidents. The basic problem is inaccurate risk perception and calculating risk using the wrong factors. This process is behind the frequently used but rarely defined label of "complacency." Complacency results from inaccurate process models and risk awareness.

Risk perception is directly related to *communication* and *feedback*. The more and better the information we have about the potential causes of accidents in our system and the state of the controls implemented to prevent them, the more accurate will be our perception of risk. Consider the loss of an aircraft when it took off from the wrong runway in Lexington, Kentucky, in August 2006. One of the factors in the accident was that construction was occurring and the pilots were confused about temporary changes in taxi patterns. Although similar instances of crew confusion had occurred in the week before the accident, there were no effective communication channels to get this information to the proper authorities. After the loss, a small group of aircraft maintenance workers told the investigators that they also had experienced confusion when taxiing to conduct engine tests—they were worried that an accident could happen, but did not know how to effectively notify people who could make a difference [142].

Another communication disconnect in this accident leading to a misperception of risk involved a misunderstanding by management about the staffing of the control tower at the airport. Terminal Services management had ordered the airport air traffic control management to both reduce control tower budgets and to ensure separate staffing of the tower and radar functions. It was impossible to comply with both directives. Because of an ineffective feedback mechanism, management did not know about the impossible and dangerous goal conflicts they had created or that the resolution of the conflict was to reduce the budget and ignore the extra staffing requirements.

Another example occurred in the Deepwater Horizon accident. Reports after the accident indicated that workers felt comfortable raising safety concerns and ideas for safety improvement to managers on the rig, but they felt that they could not raise concerns at the divisional or corporate level without reprisal. In a confidential survey of workers on Deepwater Horizon taken *before* the oil platform exploded, workers expressed concerns about safety:

> "I'm petrified of dropping anything from heights not because I'm afraid of hurting anyone (the area is barriered off), but because I'm afraid of getting fired," one worker wrote. "The company is always using fear tactics," another worker said. "All these games and your mind gets tired." Investigators also said "nearly everyone among the workers they interviewed believed that Transocean's system for tracking health and safety issues on the rig was *counter productive*." Many workers entered fake data to try to circumvent the system, known as See, Think, Act, Reinforce, Track (or START). As a result, the company's perception of safety on the rig was distorted, the report concluded [27, p. A1]

Formal methods of operation and strict hierarchies can limit communication. When information is passed up hierarchies, it may be distorted, depending on the interests of managers and the way they interpret the information. Concerns about safety may even be completely silenced as it passes up the chain of command. Employees may not feel comfortable going around a superior who does not respond to their concerns. The result may be a misperception of risk, leading to inadequate control actions to enforce the safety constraints.

In other accidents, reporting and feedback systems are simply unused for a variety of reasons. In many losses, there was evidence that a problem occurred in time to prevent the loss, but there was either no communication channel established for getting the information to those who could understand it and to those making decisions or, alternatively, the problem-reporting channel was ineffective or simply unused.

Communication is critical in both providing information and executing control actions and in providing feedback to determine whether the control actions were successful and what further actions are required. Decision makers need accurate and timely information. Channels for information dissemination and feedback need to be established that include a means for comparing actual performance with desired performance and ensuring that required action is taken.

In summary, both the design of the communication channels and the communication dynamics must be considered as well as potential feedback delays. As an example of communication dynamics, reliance on face-to-face verbal reports during group meetings is a common method of assessing lower-level operations [189], but, particularly when subordinates are communicating with superiors, there is a tendency for adverse situations to be underemphasized [20].

13.2.4 Controls on System Migration toward Higher Risk

One of the key assumptions underlying the approach to safety described in this book is that systems adapt and change over time. Under various types of pressures, that adaptation often moves in the direction of higher risk. The good news is, as stated earlier, that adaptation is predictable and potentially controllable. The safety control structure must provide protection from and appropriate responses to the continuing influences and pressures that tend to degrade safety over time. More

specifically, the potential reasons for and types of migration toward higher risk need to be identified and controls instituted to prevent it. In addition, audits and performance assessments based on the safety constraints identified during system development can be used to detect migration and the violation of the constraints as described in chapter 12.

One way to prevent such migration is to anchor safety efforts beyond short-term program management pressures. At one time, NASA had a strong agency-wide system safety program with common standards and requirements levied on everyone. Over time, agency-wide standards were eviscerated, and programs were allowed to set their own standards under the control of the program manager. While the manned space program started out with strong safety standards, under budget and performance pressures they were progressively weakened [117].

As one example, a basic requirement for an effective operational safety program is that all potentially hazardous incidents during operations are thoroughly investigated. Debris shedding had been identified as a potential hazard during Shuttle development, but the standard for performing hazard analyses in the Space Shuttle program was changed to specify that hazards would be revisited *only* when there was a new design or the Shuttle design was changed, not after an anomaly (such as foam shedding) occurred [117].

After the *Columbia* accident, safety standards in the Space Shuttle program (and the rest of NASA) were effectively *anchored* and protected from dilution over time by moving responsibility for them outside the projects.

13.2.5 Safety, Culture, and Blame

The high-level goal in managing safety is to create and maintain an effective safety control structure. Because of the importance of safety culture in how the control structure operates, achieving this goal requires implementing and sustaining a strong safety culture.

Proper function of the safety control structure relies on decision making by the controllers in the structure. Decision making always rests upon a set of industry or organizational values and assumptions. A *culture* is a set of shared values and norms, a way of looking at and interpreting the world and events around us and of taking action in a social context. Safety culture is that subset of culture that reflects the general attitude and approaches to safety and risk management.

Shein divides culture into three levels (figure 13.2) [188]. At the top are the surface-level cultural artifacts or routine aspects of everyday practice including hazard analyses and control algorithms and procedures. The second, middle level is the stated organizational rules, values, and practices that are used to create the top-level artifacts, such as safety policy, standards, and guidelines. At the lowest level is the often invisible but pervasive underlying deep cultural operating assumptions

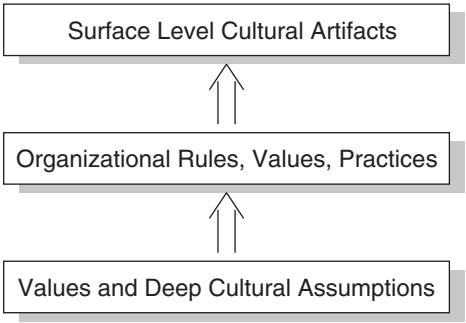


Figure 13.2
The three levels of an organizational culture.

upon which actions are taken and decisions are made and thus upon which the upper levels rest.

Trying to change safety outcomes by simply changing the organizational structures—including policies, goals, missions, job descriptions, and standard operating procedures—may lower risk over the short term, but superficial fixes that do not address the set of shared values and social norms are very likely to be undone over time. Changes are required in the organizational values that underlie people's behavior.

Safety culture is primarily set by the leaders of the organization as they establish the basic values under which decisions will be made. This fact explains why leadership and commitment by leaders is critical in achieving high levels of safety.

To *engineer* a safety culture requires identifying the desired organizational safety principles and values and then establishing a safety control structure to achieve those values and to sustain them over time. Sloganeering or jawboning is not enough: all aspects of the safety control structure must be engineered to be in alignment with the organizational safety principles, and the leaders must be committed to the stated policies and principles related to safety in the organization.

Along with leadership and commitment to safety as a basic value of the organization, achieving safety goals requires open communication. In an interview after the *Columbia* loss, the new center director at Kennedy Space Center suggested that the most important cultural issue the Shuttle program faced was establishing a feeling of openness and honesty with all employees, where everybody's voice was valued. Statements during the *Columbia* accident investigation and messages posted to the NASA Watch website describe a lack of trust of NASA employees to speak up. At the same time, a critical observation in the CAIB report focused on the engineers' claims that the managers did not hear the engineers' concerns [74]. The report concluded that this was in part due to the managers not asking or listening. Managers

created barriers against dissenting opinions by stated preconceived conclusions based on subjective knowledge and experience rather than on solid data. Much of the time they listened to those who told them what they wanted to hear. One indication about the poor communication around safety and the atmosphere at the time were statements in the 1995 Kraft report [105] that dismissed concerns about Space Shuttle safety by accusing those who made them as being partners in an unneeded "safety shield conspiracy."

Unhealthy work atmospheres with respect to safety and communication are not limited to NASA. Carroll documents a similarly dysfunctional safety culture at the Millstone nuclear power plant [33]. An NRC review in 1996 concluded the safety culture at the plant was dangerously flawed: it did not tolerate dissenting views and stifled questioning attitudes among employees.

Changing such interaction patterns is not easy. Management style can be addressed through training, mentoring, and proper selection of people to fill management positions, but trust is hard to gain and easy to lose. Employees need to feel psychologically safe about reporting concerns and to believe that managers can be trusted to hear their concerns and to take appropriate action, while managers have to believe that employees are worth listening to and worthy of respect.

The difficulty is in getting people to change their view of reality. Gareth Morgan, a social anthropologist, defines culture as an ongoing, proactive process of reality construction. According to this view, organizations are socially constructed realities that rest as much in the heads and minds of their members as they do in concrete sets of rules and regulations. Morgan assets that organizations are "sustained by belief systems that emphasize the importance of rationality" [139]. This myth of rationality "helps us to see certain patterns of action as legitimate, credible, and normal, and hence to avoid the wrangling and debate that would arise if we were to recognize the basic uncertainty and ambiguity underlying many of our values and actions" [139].

For both the *Challenger* and *Columbia* accidents, as well as most other major accidents where decision making was flawed, the decision makers saw their actions as rational. Understanding and preventing poor decision making under conditions of uncertainty requires providing environments and tools that help to stretch our belief systems and to see patterns that we do not necessarily want to see.

Some common types of dysfunctional safety cultures can be identified that are common to industries or organizations. Hopkins coined the term "culture of denial" after investigating accidents in the mining industry, but mining is not the only industry in which denial is pervasive. In such cultures, risk assessment is unrealistic and credible warnings are dismissed without appropriate action. Management only wants to hear good news and may ensure that is what they hear by punishing bad news, sometimes in a subtle way and other times not so subtly. Often arguments are

made in these industries that the conditions are inherently more dangerous than others and therefore little can be done about improving safety or that accidents are the price of productivity and cannot be eliminated. Of course, this rationale is untrue but it is convenient.

A second type of dysfunctional safety culture might be termed a "paperwork culture." In these organizations, employees spend all their time proving the system is safe but little time actually doing the things necessary to make it so. After the Nimrod aircraft loss in Afghanistan in 2006, the accident report noted a "culture of paper safety" at the expense of real safety [78].

So what are the aspects of a good safety culture, that is, the core values and norms that allow us to make better decisions around safety?

- Safety commitment is valued.
- Safety information is surfaced without fear and incident analysis is conducted without blame.
- Incidents and accidents are valued as an important window into systems that are not functioning as they should—triggering in-depth and uncircumscribed causal analysis and improvement actions.
- There is a feeling of openness and honesty, where everyone's voice is respected. Employees feel that managers are listening.
  - There is trust among all parties.
  - Employees feel psychologically safe about reporting concerns.
  - Employees believe that managers can be trusted to hear their concerns and will take appropriate action.
  - Managers believe that employees are worth listening to and are worthy of respect.

Common ingredients of a safety culture based on these values include management commitment to safety and the safety values, management involvement in achieving the safety goals, employee empowerment, and appropriate and effective incentive structures and reporting systems.

When these ingredients form the basis of the safety culture, the organization has the following characteristics:

- Safety is integrated into the dominant culture; it is not a separate subculture.
- Safety is integrated into both development and operations. Safety activities employ a mixture of top-down engineering or reengineering and bottom-up process improvement.
- Individuals have required knowledge, skills, and ability.

- Early warning systems for migration toward states of high risk are established and effective.
- The organization has a clearly articulated safety vision, values and procedures, shared among the stakeholders.
- Tensions between safety priorities and other system priorities are addressed through a constructive, negotiated process.
- Key stakeholders (including all employees and groups such as unions) have full partnership roles and responsibilities regarding safety.
- Passionate, effective leadership exists at all levels of the organization (particularly the top), and all parts of the safety control structure are committed to safety as a high priority for the organization.
- Effective communication channels exist for disseminating safety information.
- High levels of visibility of the state of safety (i.e., risk awareness) exist at all levels of the safety control structure through appropriate and effective feedback.
- The results of operating experience, process hazard analyses, audits, near misses, or accident investigations are used to improve operations and the safety control structure.
- Deficiencies found during assessments, audits, inspections, and incident investigation are addressed promptly and tracked to completion.

The Just Culture Movement

The Just Culture movement is an attempt to avoid the type of unsafe cultural values and professional interactions that have been implicated in so many accidents. Its origins are in aviation although some in the medical community, particularly hospitals, have also taken steps down this road. Much has been written on Just Culture—only a summary is provided here. The reader is directed in particular to Dekker's book *Just Culture* [51], which is the source of much of what follows in this section.

A foundational principle of Just Culture is that the difference between a safe and unsafe organization is how it deals with reported incidents. This principle stems from the belief that an organization can benefit more by learning from mistakes than by punishing people who make them.

In an organization that promotes such a Just Culture [51]:

- Reporting errors and suggesting changes is normal, expected, and without jeopardy for anyone involved.
- A mistake or incident is not seen as a failure but as a free lesson, an opportunity to focus attention and to learn.

- Rather than making people afraid, the system makes people participants in change and improvement.
- Information provided in good faith is not used against those who report it.

Most people have a genuine concern for the safety and quality of their work. If through reporting problems they contribute to visible improvements, few other motivations or exhortations to report are necessary. In general, empowering people to affect their work conditions and making the reporters of safety problems part of the change process promotes their willingness to shoulder their responsibilities and to share information about safety problems.

Beyond the obvious safety implications, a Just Culture may improve morale, commitment to the organization, job satisfaction, and willingness to do extra, to step outside their role. It encourages people to participate in improvement efforts and gets them actively involved in creating a safer system and workplace.

There are several reasons why people may not report safety problems, which were covered in chapter 12. To summarize, the reporting channels may be difficult or time consuming to use, they may feel there is no point in reporting because the organization will not do anything anyway or they may fear negative consequences in reporting. Each of these reasons must be and can be mitigated through better system design. Reporting should be easy and not require excessive time or effort that takes away from direct job responsibilities. There must be responses made both to the initial report that indicates it was received and read and later information should be provided about the resolution of the reported problem.

Promoting a Just Culture requires getting away from blame and punishment as a solution to safety problems. One of the new assumptions in chapter 2 for an accident model and underlying STAMP was:

> Blame is the enemy of safety. Focus should instead be on understanding how the entire system behavior led to the loss and not on who or what to blame.

Blame and punishment discourage reporting problems and mistakes so improvements can be made to the system. As has been argued throughout this book, changing the system is the best way to achieve safety, not trying to change people.

When blame is a primary component of the safety culture, people stop reporting incidents. This basic understanding underlies the Aviation Safety Reporting System (ASRS) where pilots and others are given protection from punishment if they report mistakes (see chapter 12). A decision was made in establishing the ASRS and other aviation reporting systems that organizational and industry learning from mistakes was more important than punishing people for them. If most errors stem from the design of the system or can be prevented by changing the design of the system, then blaming the person who made the mistake is misplaced anyway.

A culture of blame creates a climate of fear that makes people reluctant to share information. It also hampers the potential to learn from incidents; people may even tamper with safety recording devices, turning them off, for example. A culture of blame interferes with regulatory work and the investigation of accidents because people and organizations are less willing to cooperate. The role of lawyers can impede safety efforts and actually make accidents more likely: Organizations may focus on creating paper trails instead of utilizing good safety engineering practices. Some companies avoid standard safety practices under the advice of their lawyers that this will protect them in legal proceedings, thus almost guaranteeing that accidents and legal proceedings will occur.

Blame and the overuse of punishment as a way to change behavior can directly lead to accidents that might not have otherwise occurred. As an example, a train accident in Japan—the 2005 Fukuchiyama line derailment— occurred when a train driver was on the phone trying to ensure that he would not be reported for a minor infraction. Because of this distraction, he did not slow down for a curve, resulting in the deaths of 106 passengers and the train driver along with injury of 562 passengers [150]. Blame and punishment for mistakes causes stress and isolation and makes people perform less well.

The alternative is to see mistakes as an indication of an organizational, operational, educational, or political problem. The question then becomes what should be done about the problem and who should bear responsibility for implementing the changes. The mistake and any harm from it should be acknowledged, but the response should be to lay out the opportunities for reducing such mistakes by everyone (not just this particular person), and the responsibilities for making changes so that the probability of it happening again is reduced. This approach allows people and organizations to move forward to prevent mistakes in the future and not just focus on punishing past behavior [51]. Punishment is usually not a long-term deterrent for mistakes if the system in which the person operates has not changed the reason for the mistake. Just Culture principles allow us to learn from minor incidents instead of waiting until tragedies occur.

A common misunderstanding is that a Just Culture means a lack of accountability. But, in reality, it is just the opposite. Accountability is increased in a Just Culture by not simply assigning responsibility and accountability to the person at the bottom of the safety control structure who made the direct action involved in the mistake. All components of the safety control structure involved are held accountable including (1) those in operations who contribute to mistakes by creating operational pressures and providing inadequate oversight to ensure safe procedures are being followed, and (2) those in development who create a system design that contributes to mistakes.

The difference in a Just Culture is not in the accountability for safety problems but how accountability is implemented. Punishment is an appropriate response to

gross negligence and disregard for other people's safety, which, of course, applies to everyone in the safety control structure, including higher-level management and developers as well as the lower level controllers. But if mistakes were made or inadequate controls over safety provided because of flaws in the design of the controlled system or the safety control structure, then punishment is not the appropriate response—fixing the system or the safety control structure is. Dekker has suggested that accountability be defined in terms of responsibility for finding solutions to the system design problems from which the mistakes arose [51].

Overcoming our cultural bias to punish people for their mistakes and the common belief that punishment is the only way to change behavior can be very difficult. But the payoff is enormous if we want to significantly reduce accident rates. Trust is a critical requirement for encouraging people to share their mistakes and safety problems with others so something can be done before major losses occur.

13.2.6 Creating an Effective Safety Control Structure

In some industries, the safety control structure is called the safety management system (SMS). In civil aviation, ICAO (International Civil Aviation Authority) has created standards and recommended practices for safety management systems and individual countries have strongly recommended or required certified air carriers to establish such systems in order to control organizational factors that contribute to accidents.

There is no right or wrong design of a safety control structure or SMS. Most of the principles for design of safe control loops in chapter 9 also apply here. The culture of the industry and the organization will play a role in what is practical and effective. There are some general rules of thumb, however, that have been found to be important in practice.

General Safety Control Structure Design Principles

Making everyone responsible for safety is a well-meaning misunderstanding of what is required. While, of course, everyone should try to behave safely and to achieve safety goals, someone has to be assigned responsibility for ensuring that the goals are being achieved. This lesson was learned long ago in the U.S. Intercontinental Ballistic Missile System (ICBM). Because safety was such an important consideration in building the early 1950s missile systems, safety was not assigned as a specific responsibility, but was instead considered to be everyone's responsibility. The large number of resulting incidents, particularly those involving the interfaces between subsystems, led to the understanding that safety requires leadership and focus.

There needs to be assignment of responsibility for ensuring that hazardous behaviors are eliminated or, if not possible, mitigated in design and operations. Almost all attention during development is focused on what the system and its

components are supposed to do. System safety engineering is responsible for ensuring that adequate attention is also paid to what the system is *not* supposed to do and verifying that hazardous behavior will not occur. It is this unique focus that has made the difference in systems where safety engineering successfully identified problems that were not found by the other engineering processes.

At the other extreme, safety efforts may be assigned to a separate group that is isolated from critical decision making. During system development, responsibility for safety may be concentrated in a separate quality assurance group rather than in the system engineering organization. During operations, safety may be the responsibility of a staff position with little real power or impact on line operations.

The danger inherent in this isolation of the safety efforts is argued repeatedly throughout this book. To be effective, the safety efforts must have impact, and they must be integrated into mainstream system engineering and operations.

Putting safety into the quality assurance organization is the worst place for it. For one thing, it sets up the expectation that safety is an after-the-fact or auditing activity only: safety must be intimately integrated into design and decision-making activities. Safety permeates every part of development and operations. While there may be staff positions performing safety functions that affect everyone at their level of the organization and below, safety must be integrated into all of engineering development and line operations. Important safety functions will be performed by most everyone, but someone needs the responsibility to ensure that they are being carried out effectively.

At the same time, independence is also important. The CAIB report addresses this issue:

> Organizations that successfully operate high-risk technologies have a major characteristic in common: they place a premium on safety and reliability by structuring their programs so that technical and safety engineering organizations own the process of determining, maintaining, and waiving technical requirements with a voice that is equal to yet independent of Program Managers, who are governed by cost, schedule, and mission-accomplishment goals [74, p. 184].

Besides associating safety with after-the-fact assurance and isolating it from system engineering, placing it in an assurance group can have a negative impact on its stature, and thus its influence. Assurance groups often do not have the prestige necessary to have the influence on decision making that safety requires. A case can be made that the centralization of system safety in quality assurance at NASA, matrixed to other parts of the organization, was a major factor in the decline of the safety culture preceding the *Columbia* loss. Safety was neither fully independent nor sufficiently influential to prevent the loss events [117].

Safety responsibilities should be assigned at every level of the organization, although they will differ from level to level. At the corporate level, system safety responsibilities may include defining and enforcing corporate safety policy, and establishing and monitoring the safety control structure. In some organizations that build extremely hazardous systems, a group at the corporate or headquarters level certify these systems as safe for use. For example, the U.S. Navy has a Weapons Systems Explosives Safety Review Board that assures the incorporation of explosive safety criteria in all weapon systems by reviews conducted throughout all the system's life cycle phases. For some companies, it may be reasonable to have such a review process at more than just the highest level.

Communication is important because safety motivated changes in one subsystem may affect other subsystems and the system as a whole. In military procurement groups, oversight and communication is enhanced through the use of *safety working groups*. In establishing any oversight process, two extremes must be avoided: "getting into bed" with the project and losing objectivity or backing off too far and losing insight. Working groups are an effective way of avoiding these extremes. They assure comprehensive and unified planning and action while allowing for independent review and reporting channels.

Working groups usually operate at different levels of the organization. As an example, the Navy Aegis[2] system development, a very large and complex system, included a System Safety Working Group at the top level chaired by the Navy Principal for Safety, with the permanent members being the prime contractor's system safety lead and representatives from various Navy offices. Contractor representatives attended meetings as required. Members of the group were responsible for coordinating safety efforts within their respective organizations, for reporting the status of outstanding safety issues to the group, and for providing information to the Navy Weapons Systems Explosives Safety Review Board. Working groups also functioned at lower levels, providing the necessary coordination and communication for that level and to the levels above and below.

A surprisingly large percentage of the reports on recent aerospace accidents have implicated improper transition from an oversight to an insight process (for example, see [193, 215, 153]). This transition implies the use of different levels of feedback control and a change from prescriptive management control to management by objectives, where the objectives are interpreted and satisfied according to the local context. For these accidents, the change in management role from oversight to insight seems to have been implemented simply as a reduction in personnel and budgets without assuring that anyone was responsible for specific critical tasks.

2. The Aegis Combat System is an advanced command and control and weapon control system that uses powerful computers and radars to track and guide weapons to destroy enemy targets.

Assigning Responsibilities

An important question is what responsibilities should be assigned to the control structure components. The list below is derived from the author's experience on a large number and variety of projects. Many also appear in accident report recommendations, particularly those generated using CAST.

The list is meant only to be a starting point for those establishing a comprehensive safety control structure and a checklist for those who already have sophisticated safety management systems. It should be supplemented using other sources and experiences.

The list does not imply that each responsibility will be assigned to a single person or group. The responsibilities will probably need to be separated into multiple individual responsibilities and assigned throughout the safety control structure, with one group actually implementing the responsibilities and others above them supervising, leading (directing), or overseeing the activity. Of course, each responsibility assumes the need for associated authority and accountability plus the controls, feedback, and communication channels necessary to implement the responsibility. The list may also be useful in accident and incident analysis to identify inadequate controls and control structures.

Management and General Responsibilities

- Provide leadership, oversight, and management of safety at all levels of the organization.
- Create a corporate or organizational safety policy. Establish criteria for evaluating safety-critical decisions and implementing safety controls. Establish distribution channels for the policy. Establish feedback channels to determine whether employees understand it, are following it, and whether it is effective. Update the policy as needed.
- Establish corporate or organizational safety standards and then implement, update, and enforce them. Set minimum requirements for safety engineering in development and operations and oversee the implementation of those requirements. Set minimum physical and operational standards for hazardous operations.
- Establish incident and accident investigation standards and ensure recommendations are implemented and effective. Use feedback to improve the standards.
- Establish management of change requirements for evaluating all changes for their impact on safety, including changes in the safety control structure. Audit the safety control structure for unplanned changes and migration toward states of higher risk.

- Create and monitor the organizational safety control structure. Assign responsibility, authority, and accountability for safety.
- Establish working groups.
- Establish robust and reliable communication channels to ensure accurate management risk awareness of the development system design and the state of the operating process.
- Provide physical and personnel resources for safety-related activities. Ensure that those performing safety-critical activities have the appropriate skills, knowledge, and physical resources.
- Create an easy-to-use problem reporting system and then monitor it for needed changes and improvements.
- Establish safety education and training for all employees and establish feedback channels to determine whether it is effective along with processes for continual improvement. The education should include reminders of past accidents and causes and input from lessons learned and trouble reports. Assessment of effectiveness may include information obtained from knowledge assessments during audits.
- Establish organizational and management structures to ensure that safety-related technical decision making is independent from programmatic considerations, including cost and schedule.
- Establish defined, transparent, and explicit resolution procedures for conflicts between safety-related technical decisions and programmatic considerations. Ensure that the conflict resolution procedures are being used and are effective.
- Ensure that those who are making safety-related decisions are fully informed and skilled. Establish mechanisms to allow and encourage all employees and contractors to contribute to safety-related decision making.
- Establish an assessment and improvement process for safety-related decision making.
- Create and update the organizational safety information system.
- Create and update safety management plans.
- Establish communication channels, resolution processes, and adjudication procedures for employees and contractors to surface complaints and concerns about the safety of the system or parts of the safety control structure that are not functioning appropriately. Evaluate the need for anonymity in reporting concerns.

Development

- Implement special training for developers and development managers in safety-guided design and other necessary skills. Update this training as events occur and more is learned from experience. Create feedback, assessment, and improvement processes for the training.
- Create and maintain the hazard log.
- Establish working groups.
- Design safety into the system using system hazards and safety constraints. Iterate and refine the design and the safety constraints as the design process proceeds. Ensure the system design includes consideration of how to reduce human error.
- Document operational assumptions, safety constraints, safety-related design features, operating assumptions, safety-related operational limitations, training and operating instructions, audits and performance assessment requirements, operational procedures, and safety verification and analysis results. Document both what and why, including tracing between safety constraints and the design features to enforce them.
- Perform high-quality and comprehensive hazard analyses to be available and usable when safety-related decisions need to be made, starting with early decision making and continuing through the system's life. Ensure that the hazard analysis results are communicated in a timely manner to those who need them. Establish a communication structure that allows communication downward, upward, and sideways (i.e., among those building subsystems). Ensure that hazard analyses are updated as the design evolves and test experience is acquired.
- Train engineers and managers to use the results of hazard analyses in their decision making.
- Maintain and use hazard logs and hazard analyses as experience with the system is acquired. Ensure communication of safety-related requirements and constraints to everyone involved in development.
- Gather lessons learned in operations (including accident and incident reports) and use them to improve the development processes. Use operating experience to identify flaws in the development safety controls and implement improvements.

Operations

- Develop special training for operators and operations management to create needed skills and update this training as events occur and more is learned from

experience. Create feedback, assessment, and improvement processes for this training. Train employees to perform their jobs safely, understand proper use of safety equipment, and respond appropriately in an emergency.

- Establish working groups.
- Maintain and use hazard logs and hazard analyses during operations as experience is acquired.
- Ensure all emergency equipment and safety devices are operable at all times during hazardous operations. Before safety-critical, nonroutine, potentially hazardous operations are started, inspect all safety equipment to ensure it is operational, including the testing of alarms.
- Perform an in-depth investigation of any operational anomalies, including hazardous conditions (such as water in a tank that will contain chemicals that react to water) or events. Determine why they occurred before any potentially dangerous operations are started or restarted. Provide the training necessary to do this type of investigation and proper feedback channels to management.
- Create management of change procedures and ensure they are being followed. These procedures should include hazard analyses on all proposed changes and approval of all changes related to safety-critical operations. Create and enforce policies about disabling safety-critical equipment.
- Perform safety audits, performance assessments, and inspections using the hazard analysis results as the preconditions for operations and maintenance. Collect data to ensure safety policies and procedures are being followed and that education and training about safety is effective. Establish feedback channels for leading indicators of increasing risk.
- Use the hazard analysis and documentation created during development and passed to operations to identify leading indicators of migration toward states of higher risk. Establish feedback channels to detect the leading indicators and respond appropriately.
- Establish communication channels from operations to development to pass back information about operational experience.
- Perform in-depth incident and accident investigations, including all systemic factors. Assign responsibility for implementing all recommendations. Follow up to determine whether recommendations were fully implemented and effective.
- Perform independent checks of safety-critical activities to ensure they have been done properly.

- Prioritize maintenance for identified safety-critical items. Enforce maintenance schedules.
- Create and enforce policies about disabling safety-critical equipment and making changes to the physical system.
- Create and execute special procedures for the startup of operations in a previously shutdown unit or after maintenance activities.
- Investigate and reduce the frequency of spurious alarms.
- Clearly mark malfunctioning alarms and gauges. In general, establish procedures for communicating information about all current malfunctioning equipment to operators and ensure the procedures are being followed. Eliminate all barriers to reporting malfunctioning equipment.
- Define and communicate safe operating limits for all safety-critical equipment and alarm procedures. Ensure that operators are aware of these limits. Assure that operators are rewarded for following the limits and emergency procedures, even when it turns out no emergency existed. Provide for tuning the operating limits and alarm procedures over time as required.
- Ensure that spare safety-critical items are in stock or can be acquired quickly.
- Establish communication channels to plant management about all events and activities that are safety-related. Ensure management has the information and risk awareness they need to make safe decisions about operations.
- Ensure emergency equipment and response is available and operable to treat injured workers.
- Establish communication channels to the community to provide information about hazards and necessary contingency actions and emergency response requirements.

13.2.7 The Safety Information System

The safety information system is a critical component in managing safety. It acts as a source of information about the state of safety in the controlled system so that controllers' process models can be kept accurate and coordinated, resulting in better decision making. Because it in essence acts as a shared process model or a source for updating individual process models, accurate and timely feedback and data are important. After studying organizations and accidents, Kjellan concluded that an effective safety information system ranked second only to top management concern about safety in discriminating between safe and unsafe companies matched on other variables [101].

Setting up a long-term information system can be costly and time consuming, but the savings in terms of losses prevented will more than make up for the effort. As

an example, a Lessons Learned Information System was created at Boeing for commercial jet transport structural design and analysis. The time constants are large in this industry, but they finally were able to validate the system after using it in the design of the 757 and 767 [87]. A tenfold reduction in maintenance costs due to corrosion and fatigue were attributed to the use of recorded lessons learned from past designs. All the problems experienced in the introduction of new carbon-fiber aircraft structures like the B787 show how valuable such learning from the past can be and the problems that result when it does not exist.

Lessons learned information systems in general are often inadequate to meet the requirements for improving safety: collected data may be improperly filtered and thus inaccurate, methods may be lacking for the analysis and summarization of causal data, information may not be available to decision makers in a form that is meaningful to them, and such long-term information system efforts may fail to survive after the original champions and initiators move on to different projects and management does not provide the resources and leadership to continue the efforts. Often, lots of information is collected about occupational safety because it is required for government reports but less for engineering safety.

Setting up a safety information system for a single project or product may be easier. The effort starts in the development process and then is passed on for use in operations. The information accumulated during the safety-driven design process provides the baseline for operations, as described in chapter 12. For example, the identification of critical items in the hazard analysis can be used as input to the maintenance process for prioritization. Another example is the use of the assumptions underlying the hazard analysis to guide the audit and performance assessment process. But first the information needs to be recorded and easily located and used by operations personnel.

In general, the safety information system includes

- A safety management plan (for both development and operations)
- The status of all safety-related activities
- The safety constraints and assumptions underlying the design, including operational limitations
- The results of the hazard analyses (hazard logs) and performance audits and assessments
- Tracking and status information on all known hazards
- Incident and accident investigation reports and corrective actions taken
- Lessons learned and historical information
- Trend analysis

One of the first components of the safety information system for a particular project or product is a safety program plan. This plan describes the objectives of the program and how they will be achieved. In addition to other things, the plan provides a baseline to evaluate compliance and progress. While the organization may have a general format and documented expectations for safety management plans, this template may need to be tailored for specific project requirements. The plan should include review procedures for the plan itself as well as how the plan will be updated and improved through feedback from experience.

All of the information in the safety information system will probably not be in one document, but there should be a central location containing pointers to where all the information can be found. Chapter 12 contains a list of what should be in an operations safety management plan. The overall safety management plan will contain similar information with some additions for development.

When safety information is being shared among companies or with regulatory agencies, there needs to be protection from disclosure and use of proprietary data for purposes other than safety improvement.

13.2.8 Continual Improvement and Learning

Processes and structures need to be established to allow continual improvement and learning. Experimentation is an important part of the learning process, and trying new ideas and approaches to improving safety needs to be allowed and even encouraged.

In addition, accidents and incidents should be treated as opportunities for learning and investigated thoroughly, as described in chapter 11. Learning will be inhibited if a thorough understanding of the systemic factors involved is not sought.

Simply identifying the causal factors is not enough: recommendations to eliminate or control these factors must be created along with concrete plans for implementing the recommendations. Feedback loops are necessary to ensure that the recommendations are implemented in a timely manner and that controls are established to detect and react to reappearance of those same causal factors in the future.

13.2.9 Education, Training, and Capability Development

If employees understand the intent of the safety program and commit to it, they are more likely to comply with that intention rather than simply follow rules when it is convenient to do so.

Some properties of effective training programs are presented in chapter 12. Everyone involved in controlling a potentially dangerous process needs to have safety training, not just the low-level controllers or operators. The training must include not only information about the hazards and safety constraints to be

implemented in the control structure and the safety controls, but also about priorities and how decisions about safety are to be made.

One interesting option is to have managers serve as teachers [46]. In this education program design, training experts help manage group dynamics and curriculum development, but the training itself is delivered by the project leaders. Ford Motor Company used this approach as part of what they term their Business Leadership Initiative and have since extended it as part of the Safety Leadership Initiative. They found that employees pay more attention to a message delivered by their boss than by a trainer or safety official. By learning to teach the materials, supervisors and managers are also more likely to absorb and practice the key principles [46].

13.3 Final Thoughts

Management is key to safety. Top-level management sets the culture, creates the safety policy, and establishes the safety control structure. Middle management enforces safe behavior through the designed controls.

Most people want to run safe organizations, but they may misunderstand the tradeoffs required and how to accomplish the goals. This chapter and the book as a whole have tried to correct misperceptions and provide advice on how to create safer products and organizations. The next chapter provides a real-life example of a successful systems approach to safety.

For information about special quantity discounts, please email special_sales@mitpress.mit.edu

This book was set in Syntax and Times Roman by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Leveson, Nancy.
Engineering a safer world : systems thinking applied to safety / Nancy G. Leveson.
p. cm.—(Engineering systems)
Includes bibliographical references and index.
ISBN 978-0-262-01662-9 (hardcover : alk. paper)
1. Industrial safety. 2. System safety. I. Title.
T55.L466 2012
620.8′6—dc23
2011014046

10 9 8 7 6 5 4 3 2 1