# Chapter 9
# Safety and Security: Managerial Tensions and Synergies


**Paul R. Schulman**

**Abstract** The relationship between organizational safety and security is a conceptual and practical challenge. This paper focuses on the management aspects of this challenge. Its argument is that we have yet to parse out the full range of contradictory and complementary requirements of these two as managerial missions. Considering the requirements for high reliability management can provide a clarifying lens for sorting out the contradictions and complementarities. Some overlapping requirements from a high reliability perspective actually argue for an integration of the two missions within one managerial framework with enhancements for "higher resolution" reliability.

**Keywords** High reliability management · Safety management · Security management · Vulnerability

At a recent conference on safety management organized by a large public utility regulatory agency, the issue of infrastructure security came up for discussion. Addressing the issue, the CEO of a large utility asserted: "If we're doing a good job of safety management that should take care of security too". I took this to be a convenient untruth at the time.

There is a strong debate among scholars and practitioners about whether the same managerial framework within a single organization can accommodate both effective and successful safety and security management [1, 3, 5]. Research on High Reliability Organizations (HROs) has focused on a number of organizations (nuclear power plants, commercial aviation and air traffic control centers, and electrical grid management organizations, for example) with extremely well-developed reliability strategies in both technical design and management systems for protection against failures that can create catastrophic accidents [6, 7, 10, 11]. These organizations notably, as critical infrastructures, are also potentially high-value targets for terrorist assault. But it is not clear from this research that HROs are simultaneously addressing both safety and terrorist security objectives in their reliability strategies.

P. R. Schulman (✉)
Mills College and University of California at Berkeley, Berkeley, USA
e-mail: paul@mills.edu



C. Bieder and K. Pettersen Gould (eds.), *The Coupling of Safety and Security*, SpringerBriefs in Safety Management,
https://doi.org/10.1007/978-3-030-47229-0_9

This essay will consider and compare major variables that have to be addressed and the strategy developed by an organization seeking high reliability management first, with a safety and then, a security mission.

## 9.1 Safety Variables and Strategy

The most prominent feature of HROs is that they are managing technical systems that can fail with catastrophic results—large-scale disruptions of critical services and potentially many deaths. "High Reliability" for an HRO means that there are protections against these failures or accidents in place to preclude them from happening—not just probabilistically, but deterministically. A key managerial feature of this reliability is the protection against errors that could lead to these "precluded events", especially "representational errors"—mis-estimations, mis-specifications, and misunderstanding of the systems being managed that can lead to decisions and actions that invite failure and accidents. In this sense, reliability strategy is simultaneously a commitment to safety because you cannot ensure safety without reliability. But it is system safety, not individualized accidents such as slips, trips, and falls, that is the priority of HROs.

**Robustness of technical systems**. The technical systems under management are well understood in terms of operating principles and the maturity of technical designs. These are not frontier technologies whose operation is experimental in both underlying knowledge and operational experience. Much if not all of operations and maintenance is carefully analyzed, including careful risk analysis, and conducted under elaborate procedures. In the United States, for example, it is against federal law to operate a nuclear power plant "outside of analysis".

Robustness is supported by technical designs that include redundancy of key components, back-up systems to compensate for the loss of primary ones, as well as planned and even automated shut-down protocols to stop operations in safe modes relative to potential major accidents. Non-operation is always a priority to continuing to provide outputs in the face of escalated risk.

The reliability of technical system components is often defined as how well their designs fulfill operational requirements and performance expectations, and within these designs how infrequently they fail. But reliability cannot be fully determined by designs alone. Components must be inspected, operated, and maintained within design specifications. This requires their protection by management from errors that could undermine these processes. Assuring the integrity of management information, decision, and control processes to prevent error is a major feature of managerial reliability.

**HRO managerial strategy**. A classical HRO management strategy for reliability and safety in managing technical systems is founded in the formula that low *input* variance (in external resources, supports, demands, and conditions surrounding the organization) coupled with low *process variance* (operations tied to procedures and careful prior analysis and planning) lead to low output variance (predictable and

reliable performance). Control over input and process variance are key elements in stabilizing performance.

Yet, ironically, this control is grounded in the recognition that a key to high reliability is not a rigid invariance in technical, managerial, and organizational processes but rather the *management of fluctuations* in task performance and conditions to keep them within acceptable bandwidths and outside of dangerous or unstudied conditions [12]. Many organizational processes that support high reliability, including high degrees of attention and care in specific tasks, lateral inter-departmental communication and trust, and shared sensemaking surrounding the execution of plans and decisions, are perishable in the press of day-to-day work and have to be continually monitored and renewed.

Supporting this narrow bandwidth management is the careful identification analysis, and exclusion of precursor conditions that could lead to precluded events. HROs begin with the core set of these unacceptable events, then analyze backward to conditions both physical and organizational that could, along given chains of causation, lead ultimately to significant possibilities of such events. This "precursor zone" typically grows outward to include additional precursor conditions based on more careful analysis and experience. These precursors are in effect leading indicators of potential failures and are given careful attention by operators, supervisors, and higher managers.

Some precursors are in effect "weak signals" to which "receptors" throughout many levels of the organization are attuned and sensitive. Examples of precursors observed in HRO research included: operating equipment nearing the edge of maximum allowable conditions such as temperatures or pressures; too much noise or too many people in a control room; silence or edginess in an individual control operator; backlogs in clearing corrective action reports; a movement into "unstudied conditions" in any operations or maintenance activities. In its effectiveness, this process of precursor management provides a special kind of "precursor resilience" to these organizations. They can identify and move quickly back from the approach to precursor zones while still maintaining a robustness in performance and outputs [10].

Another important element in HRO reliability management is the existence of a great deal of lateral communication. This is important to maintain the system focus of reliability and safety management and prevent localized actions without consideration of their wider effects. There is a lot of inter-departmental collaboration in work planning sessions, incident investigations, procedural reviews and procedure revisions.

Additionally, there is a widely shared culture throughout these organizations that supports the features described above. This culture supports managing to worst-case possibilities and not simply probability, and in many decision-making and planning activities. There is highvalue and indeed much personal esteem accorded to individuals who can offer imaginative examples of potential causal pathways to worst-case possibilities. The culture within HROs also stresses widely dispersed individualized responsibilities associated with detecting error, such as speaking up to correct it, and promoting the identification of precursors and the improvement of procedures. In one HRO, many individuals down to the control room and maintenance shop levels,

for example, actively participated in the procedural revision process. In important respects, these individuals "own" the procedures. In one nuclear power plant personnel at different levels expressed the view that, without continual improvement, existing levels of reliability would likely not be maintained due to the onset of complacency [12].

One important example of the culture of responsibility for safety reaching down to the level of the individuals is the importance of people we termed "reliability professionals" to the successful pursuit of reliability and system safety in HROs [11]. Who are reliability professionals?

These are individuals who have special perspectives on reliability, cognitively and normatively. They mix formal deductive knowledge and experiential knowledge in their understanding of the systems they operate and manage. Their view of the "system" is larger than their formal roles, specializations and job descriptions. They internalize in their identity the reliable and safe operation of their systems. In this, they are "professionals" on behalf of reliability and safety, but are not defined by particular formal degrees or certifications.

We have found reliability professionals distributed in many jobs at many levels in HROs. We find them among control operators, line production or maintenance personnel, engineering and other technical personnel who support operators and maintenance, and among middle-level managers and supervisors, department heads, and CEOs or agency heads. Whatever their formal job, they focus on identifying precursor conditions that degrade safety, including their own performance capabilities. They can also help police their own departmental or unit movements toward a practical drift away from reliability and safety because in their larger system perspective they think about the system risks and consequences of changes they or others make in their own task domain [8].

All of these elements in reliability and safety management in HROs reflect the widely stressed idea that, despite all the prior anticipation and analysis, the elaboration of procedures, the redundancies, and shut-down protections, there is still the potential for surprises in their technical systems and a constant need for vigilance and organizational improvement.

But it is important to appreciate that in this recognition of the *potential* for surprises and their strategy of precursor resilience, HROs are hardly confronted with major uncertainty in day-to-day operations and performance. In their settled technology, elaborate planning, anticipation, and analysis, it is not "managing the unexpected" HROs are engaging in. Instead, in managing to possibility, and adding a worst-case slant to planning and analysis, they are *enlarging* expectancies—formalizing an approach to avoid complacency and add to the possible scenarios that are part of their prior analysis and anticipation.

Now let's consider management challenges with respect to a *security* mission and what "high reliability" might mean in this context.

## 9.2 Security Management Variables and Reliability Strategy

**Failure versus Vulnerability**. One obvious difference between safety and security management is in the primacy of hostile intent. For example, while they may have been "hardened" to resist an external assault, and while their management systems were well organized to guard against unintended errors in operations and maintenance, HROs were not well prepared to protect against willful and strategic *internal* sabotage through actions of destructive intent.

This is a special challenge in "managing the unexpected". It is one thing to identify and manage operational risks of failure, it is another to identify and manage vulnerability to destructive intent. There are always more ways that a complex system can fail than there are for it to operate correctly as designed. But hostile strategy, both external and internal, can add additional possibilities for disaster because of the treatment of vulnerabilities as strategic targets. Further, if attacks on these vulnerabilities do not have to include the survival of the attackers, the possibilities get even larger still. An example of this is the strategy adopted by airlines after 9/ll to harden the cockpit door of airplanes to resist external intrusion from potential terrorists among the passengers. Ironically and tragically, addressing this problem led to a reciprocal vulnerability: a saboteur already inside the cockpit. In fact, a suicidal co-pilot of Germanwings Flight 9525, with the pilot momentarily out of the cockpit, locked the door, thus making himself impregnable, and flew the plane into a mountain-side. Protecting the cockpit against external intrusion actually created a new vulnerability and an opportunity for a different form of assault. Achieving reliability and safety against nature or inadvertent human actions is hard enough. It becomes a different challenge when failure itself is part of a learning system with the ability to develop *counter-strategy* for its promotion.

**A special problem in "design-based" vulnerability**. Vulnerability itself can come in a variety of forms, giving many options to saboteurs. Vulnerability means risk exposure, but vulnerability also pertains to an *innate ability to be harmed*. One form of vulnerability is by willful design strategy plus by potential victims toward harm itself. In way, victims move to make an assault more likely and/or more consequential with respect to harm. An example is when housing developments are built in flood plains, increasing their vulnerability to floods or when tall buildings or roads are constructed on earthquake faults or individuals build homes in forest areas with increased exposure to wildfire. A spectacular example of design-based vulnerability lies in the internet and its vulnerability to cyberattack.

It has been argued that the internet can now be attacked from any location, at any scale, and across a wide range of precision [4]. No natural system on earth could survive to evolve such an extreme degree of vulnerability. But the internet is not a natural system. We have allowed, encouraged, and designed it to evolves to this high degree of vulnerability. Currently, the internet is certainly one of the most important critical infrastructures with simultaneously the most extensive social dependency and the highest vulnerability of any system humans have ever created.

Every new element we add to internet connectivity, or the extension of its functions and capacity, introduces additional vulnerabilities—often across multiple dimensions. This design perversity, in which each new design element adds an increased number of vulnerabilities, to viruses, hacking or fraud, is an enlarging challenge to our processes of forecasting and understanding. It is hard to see how, under these current challenges, internet security can be successfully managed by individual organizational strategy or effectively addressed in local or regional public policy. By extension, it would seem that controlling design-based vulnerability implies the need for larger-scale social regulation than organizational self-interest or even an industry-wide self regulation would fully address.

In addition, for a terrorist, not every target has to be of high value in terms of disruption and death. Terror is designed to induce public fear and uncertainty, as well as policy reactions in anger that may lead to the sacrifice of other values held by a society. In this way, targets can have symbolic value well beyond any physical destruction. Even attacks on targets of marginal significance, or attacks that fail, can induce fear and a sense of vulnerability within a population. Security management can hardly be the management of everything. As two analysts conclude, "Most sensible people would […] agree that it is impossible to thwart each conspiracy and detect each and every lone individual or group harbouring evil intentions" [2]. So high reliability security management cannot realistically rise to the level of the precluded event standard sought for safety in HROs, nor is it likely to be pursued effectively by single organizations.

**Managerial control variables**. Strategic vulnerability adds additional challenges to reliable security management. Targets can be both external and internal. While an organization may have a set of controls it can use in internal operations (hierarchical authority, procedural requirements, training, hiring and firing, surveillance, etc.), it may have few control variables to cover the vulnerability of external infrastructures, or the loss of goods or service outputs from other organizations upon which it depends for operation. Further, those attacks that are not prevented may well require coordinated emergency response and recovery operations under conditions difficult for any single organization or set of organizations to manage effectively:

> Plans for crisis and disaster management tend to have a highly symbolic character, and often provide little guidance for those who must respond to unforeseen and unimagined events. In addition, plans are only useful if they are tested and refined and the people who work within the plan are familiar with their roles, responsibilities and interactions with others [2].

Also, consider the risks of risk assessments themselves applied to vulnerability. The purpose of risk analysis and assessment is to identify risks, rank them in terms of their importance and likelihood, and prioritize attention and resources devoted to them on the basis of this priority. Yet security vulnerability assessments, if known, might well undermine their own accuracy through counter strategy they might generate on the part of hostile strategists. They could in fact attract potential terrorists and add to the risk surrounding what are identified as vulnerable targets, or instead increase risk to low risk -assessed targets. Why not direct hostile action to what appear to be the *least* likely and possibly least defended targets?

The role of precursor management and the search for leading indicators and weak signals may also be limited in security management because perpetrators of attacks will make every effort to keep potential precursor actions and information secret or even disguise their intentions with false signals.

**Contradictions between security and safety management strategy**. Given the challenges associated with security management, it is not surprising that some of the approaches taken toward managing vulnerability might conflict with those dominant in safety management. The stress on anticipation and prior analysis appropriate to reliable safety management of settled technical systems may introduce rigidity and undermine the resilience and adaptability necessary for rapid responses to unexpected assaults. The need to contain the spread of information, about key plans, decisions, and priorities, within an organization to prevent counter learning on the part of internal or external enemies, may conflict with the system-level perspective, supported by extensive lateral communication, relied upon by HROs. Even the effort to harden targets against attack through guns, gates, and guards, as in the Germanwings example, may cause security protocols to conflict with the ease of access necessary for collaborative operations and decision-making [9]. The frameworks for physical and information security may also interfere with rapid inter-organizational coordination of emergency response operations after an attack.

## 9.3 A High Reliability Perspective on Both Safety and Security

**A case for overlapping management**. Even given the differences and potential contradictions between safety and security management, it could still be argued that there can be constructive overlap or "synergies" in the effort to achieve high reliability management of both missions. As noted in the workshop prospectus, failures in either can lead to "similar ultimate consequences" which may require similar emergency and crisis management approaches (although in terror attacks, first responders may also be part of the intended targets).

A major foundation for an overlap of high reliability management of both safety and security is the common need in both missions to identify and minimize error. Managerial reliability is founded on the management of error—including the errors of misperception, misidentification, and misunderstanding. The constant search for these forms of representational error, the continual questioning of assumptions, and accepting the possibility of surprise are underlying strategic and cultural features of high reliability management for safety. They are useful in warding off complacency and hubris, states of mind that could undermine the flexibility and imagination useful in foreseeing and preparing for terror attacks. The pattern recognition skills of reliability professionals are likewise useful for identifying quickly both unfolding system failures and progressing terrorist assaults.

The focus on precursor conditions and precursor indicators is also important to both missions. Learning to recognize potential precursors to terror attacks is already an important part of security management. Here again, the support given to reliability professionals in high reliability management is important. These individuals are often ones who look for and detect weak signals. In organizations with high reliability management, there is generally a receptivity to spokespersons for a neglected perspective. Terms such as "I find myself in uncharted territory" or "I'm not comfortable taking this action" are taken seriously, especially when those using them also have the ability to stop work or veto actions as part of their job authority.

**Challenges in safety and security management integration**. It will not be easy to bring both safety and security missions under a larger framework of high reliability management. This will require developing both a wider scope and longer time frame of anticipation and at the same time, a more distributed participation in error detection and precursor resilience. A higher resolution anticipation entails gathering a wider range of information and applying more imagination to the analysis of both external and internal threats over a range of scales, scope, and time.

Enlarged time horizons for anticipation and planning could uncover both slow motion safety and vulnerability issues, such as the design-based vulnerability described earlier, or even climate change, that are likely to grow over time. Enhanced anticipation will likely need to be matched by a wider range in the *scale* of reliability management to include recognizing inter-organizational and even international precursors of accidents or assaults and the ability to manage defenses and responses on these international scales.

Teams also can be important to enlarging the range of organizational *resilience* in the face of failure or attack. In many cases, reliability professionals in teams function effectively as first responders after failure or attack, bringing their experience and effectiveness at pattern recognition quickly to bear in guiding action to limit damage or speed recovery. The role of U.S. air traffic controllers in clearing the skies of all aircraft quickly after the onset of the 9/11 terror attacks is a good example of this emergency response role at the service of both safety and security. Organizations can train and support their reliability professionals to use their skills as a means to improve both the anticipation of vulnerability and the capacity for resilience to back-up reliability in the promotion of both safety and security.

## 9.4 Conclusion

It is possible, based on the argument above, that applying an overlapping high reliability management framework to both safety and security missions cannot only enhance both but will also actually protect *against their undermining one another*. The error sensitivity at the foundation of high reliability management can also apply to the identification of and reaction to leading precursor indicators of one mission undermining the other. It is important to think carefully about this enhanced reliability and how it might be lost to both safety and security objectives if these objectives were

to be treated as separate processes and managed in separate management domains alone.

## References


1. M.F.H. Abulamddi, A survey of approaches reconciling between safety and security requirements engineering for cyber-physical systems. J. Comput. Commun. **5**, 94–100 (2017)
2. A. Boin, D. Smith, Terrorism and critical infrastructures: implications for public-private crisis management. Publ. Money Manag. **26**(5), 295–304 (2006)
3. S. Coursen, Safety vs. security: understanding the difference may soon save lives. *Linkedin* (2014). https://www.linkedin.com/pulse/20140831152519-11537006-understanding-the-difference-may-soon-save-lives-safety-vs-security
4. P. Dombrowski, C. Demchak, Thinking systemically about security and resilience in an era of cybered conflict, in *Cybersecurity Policies and Strategies for Cyberwarfare Prevention*, ed. by J. Richet (ISI Global, Hershey, PA, 2015), pp. 367–382
5. S.H. Jore, The conceptual and scientific demarcation of security in contrast to safety. Eur. J. Secur. Res. (2017). https://doi.org/10.1007/s41125-017-0021-9
6. T. LaPorte, P. Consolini, Working in practice but not in theory: theoretical challenges of high reliability organizations. Publ. Adm. Res. Theory **1**(1), 19–47 (1991)
7. T. LaPorte, High reliability organizations: unlikely, demanding and at risk. J. Conting. Crisis Manag. **4**(2), 60–71 (1996)
8. K.A. Pettersen, P. Schulman, Drift, adaptation, resilience and reliability: an empirical clarification. Saf. Sci. **117** (2016). https://doi.org/10.1016/j.ssci.2016.03.004
9. K.A. Pettersen, T. Bjørnskau, Organizational contradictions between safety and security–perceived challenges and ways of integrating critical infrastructure protection in civil aviation. Saf. Sci. **71**, 167–177 (2015)
10. E. Roe, P. Schulman, *Reliability and Risk: The Challenge of Managing Interconnected Critical Infrastructures* (Stanford University Press, Stanford, 2016)
11. E. Roe, P. Schulman, *High Reliability Management* (Stanford University Press, Stanford, 2008)
12. P. Schulman, The negotiated order of organizational reliability. Adm. Soc. **25**(3) (1993), 353–372