Preoccupation with the Costs of Preoccupation with Failure

William S. Brown
Brookhaven National Laboratory

Principle

The proposed paper considers practical constraints on a laboratory's response to signals of failure. It is suggested that resource limitations can not only lessen the effort spent looking for weak signals but also can introduce a non-conservative bias in decisions made with respect to the significance of strong signals.

Situation

Regulations require the operators of a national laboratory to report virtually all occurrences that may adversely impact people, programs, or the environment. Thus a basis exists for picking up weak signals of trouble. However, the organization has (of necessity, it could be argued) developed a graded approach to the analysis of these occurrences based on their categorization with respect to specific criteria based on their consequences. Events that involve injuries, substantial harm to the environment or very large dollar losses are thoroughly investigated – others are not.

Analyses of significant events constitute strong signals of underlying trouble. One would expect that full implications of these expensive lessons would be consistently exploited. However, as just as the decisions about which events to investigate is constrained by resource limitations, promulgation of corrective actions is subject to cost-benefit tradeoffs.

Methods of implementation

Encouraged by DOE's endorsement of the approach to human performance developed by the Institute of Nuclear Power Operations, BNL has provided training on human performance fundamentals to its entire operations staff and to the staffs of major operating facilities. Efforts to educate the remaining technical, professional, and scientific personnel are in progress.

In addition, the Laboratory has developed a cadre of employees who have had accident investigation and causal analysis training as well as in-depth training in human performance fundamentals. As a consequence, investigations are much less likely to zero in on the individual failures and more likely to uncover error-likely situation and organization weaknesses.

Results

Last year, a fire in an accelerator facility caused extensive damage (roughly $100,000) and, more importantly, interrupted the research program for over six months. The investigation established that 'trips' were not uncommon occurrences at the facility, and were typically spurious. Owing to the high number of trips and their low diagnostic value, the occurrence of a trip by itself was not investigated beyond the operator pressing the reset button. In other words, a trip became a "well understood problem" and, in some sense, "normal."

The investigation also found that corrective actions, design review recommendations, and improvements developed in response to two previous fires in similar equipment at the Laboratory were not fully adopted at the facility where the fire took place.

Owing to the nature of this event and the findings of other investigations of significant events over the previous several months, the laboratory decided that the development of corrective actions for the event should have a broad scope. Accordingly, development of corrective developed along two lines –

an institution-wide (cross-facility) look at the technology involved in the fires, and an examination how corrective actions are designed and management across the laboratory.

Conclusion

For high-reliability organizations, safety is (in Schulman's words) non-marginalizable property. However, it has been noted by Leveson that "for most organizations… the mission is something other than safety, such as selling products or pursuing scientific knowledge" [emphasis added]. It may be that elements of the way certain organizations are structured, funded, and overseen that will impede their application of the principles of high-reliability organizing.

If tradeoffs are a fact of life, the best course would appear to be to base the necessary decisions on the best possible information. In terms of Heimann's analogy with statistical hypothesis testing, the only way to decrease both types of error (to avoid accepting too much risk and avoid excessive caution) at once is to separate the distributions – by either increasing the sample size or by increasing the sensitivity of the detector. Becoming a *learning* organization may bring about changes that have this effect.