

ILLUSIONS OF SAFETY

Prof. Vicki Bier, Department of Industrial Engineering, University of Wisconsin
bier@engr.wisc.edu

I found the paper by Dowell and Hendershot, "No Good Deed Goes Unpunished: Case Studies of Incidents and Potential Incidents Caused by Protective Systems," to be very thought provoking. As pointed out by the authors of that paper, installing a protective system can provide the *illusion* of safety without the *reality* of safety. In this white paper, I will present several incidents that I have come across in my own work where design errors or latent failures were introduced as a result of plant changes that were intended to be beneficial (mostly from the field of commercial nuclear power), and will give some observations on why such events occur and how they might be prevented.

Along the same lines, I will also give examples of other "illusions of safety" above and beyond the installation of protective devices and similar plant changes. In particular, many organizational programs that are designed to enhance safety may in fact provide the illusion of safety without the reality of safety. Even if such programs do not necessarily lead to increases in risk, they may not always yield significant reductions in risk either.

Due to time constraints, this white paper is somewhat informal, and does not provide documentation for many of the incidents cited. However, it should be possible to provide detailed documentation—e.g., a complete Licensee Event Report (LER)—for all or most of the events discussed here if needed.

Introduction of latent failure modes

In a review of accident precursors at U.S. nuclear power plants from 1984 through 1988 (Bier and Mosleh, unpublished), one category of precursors that emerged as being potentially important (based on the frequency with which such events occurred) was events in which design errors or latent failure modes were introduced as a result of otherwise beneficial plant changes. Five events in this category were identified; they are described briefly below.

1987 (LER No. 244/87-008)--Following modification of the breaker amptector devices, both the 1B residual heat removal pump and the 1B safety injection pump failed to start because of inadequate clearance between the amptector actuator arm and the tripper bar. The stated cause of the event was inadequate design information regarding required clearances from the vendor of the amptector devices. Estimated duration: 15 days.

1987 (LER No. 331/87-009)--Following installation of a new phase differential over-current relay, the B emergency diesel generator automatically shut down on over-current during an automatic actuation test. The stated cause of the event was an inadequate construction acceptance procedure, which contained no

provision for returning the set point of the relay to its specified value following acceptance testing. The relay for the A emergency diesel generator also had an incorrect set point. Estimated duration: 15 days.

1988 (LER No. 251/88-003)--Following a vendor-recommended change-out of 18 gate filter module cards, smoke was observed coming from the 4S battery charger when it was loaded onto its DC bus after preventive maintenance. The 3B and 4A battery chargers were subject to similar problems. The stated cause of the event was an incorrect part selection for the capacitor in the circuit. Duration of latent failure: 8.5 months.

1988 (LER No. 255/88-021)--Following proper back filing of the service water pump impellers to permit the pumps to achieve sufficient flow, five spurious service water pump trips were observed. The stated cause of the events was an incorrect setting on the time over-current relays, which did not account for the pump motor service factor rating. However, prior to the back filing of the pump impellers, service water loads were not sufficient to cause the pump currents to exceed the protective relay set points. Duration of latent failure: approximately 2 years.

1988 (LER No. 280/88-011, Rev. 1)--Inoperable power operated relief valves, due to incorrect torques on bolts and screws. The stated cause of the event was lack of procedural guidance regarding the correct torque values. Duration of latent failure: unknown.

Although these events were not directly related to the installation of protective systems, they clearly demonstrate that "improvements" do not always make things better (or at least not right away). In most cases (LER No's. 244/87-008, 331/87-009, and 280/88-011), the change was simply not implemented correctly; in LER No. 251/88-003, the problem was caused by a design deficiency; in LER No. 255/88-021, the improvement itself revealed a problem that had existed in latent form all along, but had never manifested itself before the plant improvement had been made.

Another example (identified during a risk assessment of a nuclear power plant) involved the reactor trip system, which is responsible for shutting down the reactor in case of an emergency. The proper design of this system is rather complex and counterintuitive, in order to ensure (a) that any one of the two trains of reactor trip breakers is sufficient to trip the reactor in case of an actual emergency, but (b) that a single train of reactor trip breakers can be tested without tripping the reactor. (In fact, when I first reviewed the design of this system, it took me several hours to figure out why it looked the way it did.) In any case, during the course of the risk analysis, a colleague of mine realized that the design of the system at this one power plant had been altered to a simpler and more "intuitive" design (Rao, personal communication). Presumably, someone had thought that the more complicated and unintuitive system design had been a "mistake,"

and changed the design. However, the result was that the reactor would have tripped every time the system was tested. This is admittedly much less serious than a design flaw in which the reactor would not have tripped at all, but is still dangerous, since *any* reactor trip disturbs the plant from its steady-state operation and requires the successful operation of safety systems to prevent an accident.

Hence, the frequent practice of giving full credit for risk reductions due to plant design or operation changes, before the effectiveness of those changes has been empirically demonstrated, may not adequately reflect the potential for risk increases immediately after the implementation of plant changes. Major changes in system configuration may reliably eliminate certain failure modes; for example, removal of an unnecessary check valve would eliminate the possibility of that valve failing to open. However, the effects of more subtle changes may be difficult to predict.

For example, replacement of one component by a similar component may not lead to improved performance even if the new item is more reliable, since the new component may not be fully suited to the intended application. This was the case in LER No. 251/88-003, where a replacement capacitor met all published specifications of the original component but was nonetheless not suitable for the application at hand. Similarly, maintenance changes (e.g., improved cleanliness) may not be sufficient to address the root cause of the original problem, and in fact may not even have the intended effect. For example, more frequent testing may cause increased wear-out rather than reduced failure rates. Due to the possibility of such unanticipated failure modes, care should be taken in assigning risk reduction credit to design and maintenance changes.

Perhaps LER No. 255/88-021 provides the best illustration of this. In this event, the improper back filing of the service water pump impellers was corrected, allowing the pumps to achieve the rated flows for the first time. Due to this modification, the original problem (i.e., marginally insufficient flow at high service water loads, which would probably have been adequate for virtually all system functions) was replaced by a potentially much more severe problem (namely, spurious pump trips at high loads, resulting in zero flow rates). Although eventually corrected, this problem persisted for approximately 2 years.

In particular, LER No. 255/88-021 involved an improvement intended to increase service water pump flow rates to their rated values; the pumps had previously achieved slightly less than rated flow. This "improvement" did succeed in increasing the pump flow rates. However, the pump over-current relays had been set improperly, with the result that the pumps would trip whenever they reached their rated flow. Thus, the supposed "improvement" actually made things significantly worse for a period of about two years. Instead of achieving almost their rated flow (which would probably have been sufficient for virtually all conditions), there was now a risk that the pumps would not be available at all, which created a much more dangerous situation.

It is also important to note that, while all the latent failures we observed were transitory and were eventually detected and repaired, their durations were by no means always negligible. If the latent failure modes introduced by plant modifications tended to be short-lived, they would not necessarily be a major concern. However, of the five events identified above, two were found during monthly surveillance testing, and could have existed as latent failures for periods of up to one month; durations of 15 days were estimated for these events. For failure modes not typically revealed by routine testing, durations can be even longer. LER No. 251/88-003 involved a latent failure of more than 8 months; the failure mode was found not during routine testing, but after preventive maintenance. The latent failure in LER No. 255/88-021 persisted for a period of approximately 2 years, during which time several spurious pump trips resulted; while the first trip occurred only a couple of months after the introduction of the latent failure mode, the root cause was not successfully identified until much later. Finally, the duration of LER No. 280/88-011 could not be estimated, but might well have been substantial, since the improper torque of the actuator diaphragm hold-down screws and bolts might have occurred as early as the previous plant outage.

Further research on the effectiveness of plant design changes might provide more insight into the frequency with which latent failures are introduced, and the severity of such failure modes when they exist. For example, a comprehensive review of all design changes at one or two sample plants over a period of several years might provide a basis for this assessment; such a review would need to be essentially prospective in nature, focused on identifying problems occurring subsequent to each design change. The results of such research could help in determining how much credit to take for plant changes.

Introduction of latent failure modes is also a potential candidate for prevention through plant operational improvements. Since these latent failures can be temporarily risk-significant, it might be worthwhile to attempt to reduce the likelihood of such events through appropriate modifications in the procedures for plant change control. At first, preventing the introduction of latent failure modes would appear to be difficult if not impossible, since their very occurrence shows that plant modifications can have unanticipated consequences; how can we prevent consequences that we cannot anticipate? However, structured procedures have been developed to aid in identifying possible failure modes. For example, HAZOPS procedures are essentially inductive in nature (as opposed to the deductive processes involved in failure modes and effects analysis). Therefore, one possible strategy for reducing the introduction of latent failure modes might be some type of customized HAZOPS procedure for change control.

Given the number of plant changes typically made in any given year, it would not be realistic to enforce the use of such a procedure on each and every design change; among other things, this would turn the HAZOPS review into a rote exercise, rather than the creative thought process that is intended. However, such a review procedure might nonetheless be beneficial when applied to plant changes with the potential to affect risk-

significant systems, particularly systems in which latent failures are unlikely to be discovered during routine plant testing. Research on the effectiveness of design changes and the typical severity of latent failures could provide insight into the potential value of adopting preventive measures of this sort.

Required corrective action reports

Many organizations require corrective action reports for every significant incident, as a part of their overall safety program. For example, the requirement for such corrective action reports (and the corrective actions they described) formed a substantial part of the National Aeronautics and Space Administration (NASA) safety program for the space shuttle. In some cases, when an incident reveals an obvious design flaw that can reasonably be remedied by installing a protective system or making some other plant design change, such corrective actions may genuinely contribute to improved safety. For example, adding check valves to a compressed air system would genuinely help to reduce the risk that a leak in one part of the system would result in a loss of pressure throughout the entire system. Even in this case, of course, there is the potential for the corrective action itself to cause further incidents, as noted above; for example, the check valves may fail to open when needed, although the probability of this failure mode is likely to be low.

In other cases, however, there may either be no obvious design change that would eliminate the problem that was observed in the incident, or the relevant design changes may simply be too expensive to implement. In this case, the requirement to identify a corrective action for each incident tends to result in corrective action reports that are long on "motherhood-and-apple-pie" actions, such as promises to maintain improved cleanliness or implement better housekeeping procedures; in fact, such motherhood-and-apple-pie corrective action reports are frequently found in NASA's incident data bases.

The point is not that improved cleanliness or better housekeeping might contribute to an increased risk of accidents, but rather that *promises* of improved cleanliness or better housekeeping do not ensure a *reduced* risk. Such promises are almost impossible to enforce, and are often observed only in the breach; in any case, organizational commitments to efforts such as improved cleanliness or better housekeeping are notorious for being extremely short-lived.

Furthermore, even if one could have confidence that the promised corrective action would be successfully implemented, it is often unclear whether such actions would actually reduce the risk of the particular failure mode or incident that was observed. Improved cleanliness may reduce the frequency of filter plugging, and better housekeeping may reduce the frequency with which tools are dropped into reactor vessels, but such corrective actions may not reduce the risk of problems such as pump failures, if the failure was due to factors such as wear-out or misalignment rather than debris or corrosion. Thus, without a definitive root cause analysis, it is often difficult to

determine whether the promised corrective action is even relevant to the problem at hand.

Another similar example of a motherhood-and-apple-pie corrective action that I have often seen in Licensee Event Reports for U.S. nuclear power plants deals with incidents that were due (in whole or in part) to human error. Here, corrective action reports frequently say simply that the particular employee involved in the incident was "counseled," which presumably means that the employee was instructed not to make the same mistake in future! Once again, this type of corrective action is unlikely to be very effective in practice.

First, it is not at all clear that future instances of the same type of error are likely to involve the same employee in any case (unless that employee was particularly ill-trained, for example, in which case "counseling" or re-training may actually be helpful). If the problem is important, it should presumably be brought to the attention of *all* workers who could potentially end up in similar situations, not only the particular person involved in the incident at hand.

Moreover, this type of "corrective action" again begs the question of the root cause(s) of the incident. For example, a frequent type of human error in practice is performing the right action on the wrong component; e.g., disabling the wrong pump in preparation for maintenance. If this is done purely as a result of inattention, then counseling employees to pay closer attention could conceivably be effective (although we don't really know very much about how to reliably motivate people or influence their behavior). However, if the correct circuit breaker was one of several dozen identical breakers on an ill-labeled control panel, it is unclear that most employees will reliably be able to select the correct breaker even given superb motivation and training. In this case, providing better labeling and color-coding for the breakers is likely to be much more effective than counseling the employees to pay closer attention to their work.

To summarize, requiring corrective action reports gives management the feeling that they are doing something about every identified problem. Perhaps more importantly, in bureaucratic and regulated organizations, required corrective action reports can provide protective cover for future incidents; a manager can point to the fact that procedures were followed and "appropriate" corrective actions taken on all previous occasions when similar incidents had occurred. However, if perusal of the actual corrective actions cited in these reports indicates a high frequency of motherhood-and-apple-pie corrective actions, the *impression* of safety may in fact be an *illusion* of safety.

The effectiveness of corrective actions (particularly vague actions such as improved cleanliness or counseling of employees) can only be judged *after the fact* (from a reduced rate of similar incidents in the future), not from the existence of a corrective action report. Moreover, I will argue in the next section that it may not be appropriate to require corrective actions for all incidents.

Root cause analysis

Just as many organizations require a corrective action report for every significant incident, so too is root cause analysis routinely required (e.g., in Licensee Event Reports for nuclear power plants). However, this can again give the illusion of safety instead of the reality.

In particular, a review of outage reports for one particular nuclear power plant identified a series of similar repeated problems in the first year or two after commercial operation. Each of these problems triggered a root cause analysis, followed by a corresponding corrective action. However, as the problem continued to recur, it became clear in retrospect that the supposed "root cause analyses" had not in fact been successful at finding the actual root cause of the problem. Eventually, after yet another recurrence of the same problem, the root cause *was* apparently identified, as evidenced by the fact that the problem suddenly ceased to be observed.

The point of this example is not to argue that root cause analysis is undesirable or counterproductive, but simply to point out that the act of performing a root cause analysis does not ensure that the root causes are actually found. One can mandate that the desired *effort* be undertaken, but not that the desired *result* be achieved. Thus, the effectiveness of root cause analyses (like corrective actions) can only be judged *in retrospect* (from the absence of similar incidents in the future), not from the existence of a root cause analysis.

Despite this limitation, it may well be appropriate to require a root cause analysis for each significant incident that occurs, to ensure that such events are treated with appropriate seriousness. However, in cases where the analyst does not have much confidence that the correct root cause has in fact been found, it may not be appropriate to require that a corrective action be performed. If organizational constraints create pressures to find a so-called "root cause" in each root cause investigation, and implement a corrective action for each identified "root cause," this may waste resources and reduce opportunities for future learning (by creating a pretense that the root cause of each incident has already been found), while again providing only an illusion of safety.

Observations

The incidents discussed in this paper provide evidence (a) that supposedly beneficial plant changes can in fact make things worse, and (b) that organizational measures intended to ensure safety, such as requiring root cause analyses and corrective action reports for each significant incident, may in some instances be wholly ineffective even when they do *not* make things worse. The intent is not to discourage root cause analyses, corrective actions, and other beneficial plant changes, but rather to point out how elusive the goal of maximizing safety is. Therefore, the effectiveness of safety programs and improvements should whenever possible be judged based on actual data, since the presumption of effectiveness can frequently be misleading.

References

Bier, V. M., and A. Mosleh, "Insights Gained from Precursor Studies," unpublished.

Rao, S. B., personal communication.