Safety concerns at Ontario Hydro: The need for safety management through incident analysis and safety assessment

John D. Lee
Battelle Seattle Research Center
4000 NE 41st Street
Seattle, WA
Leejd@battelle.org

Kim J. Vicente
Cognitive Engineering Laboratory
Department of Mechanical & Industrial Engineering
University of Toronto
benfica@mie.utoronto.ca

Safety management and the long-term operation of complex socio-technical systems

Ontario Hydro -- one of the largest electrical utilities in North America -- recently decided to shut down 7 of its 20 nuclear power plants at an estimated cost of $8 billion Canadian. The motivation for this unprecedented step was not technological problems, but rather inadequate management which led to a minimally acceptable level of safety (Andognini, 1997). This paper draws examples from a recent field study conduced at Pickering NGS (Vicente, 1997) to show how system safety can decline if not scrupulously managed.

These plant closures emphasize the variable nature of system safety. System safety cannot be quantified and assessed at the beginning of a system's operation and expected to remain constant after years of operation. Many elements of a complex socio-technical system evolve with time, interacting to affect safety in unknown ways. Changes in instrumentation, number and qualifications of operators, operating conditions, and organizational structure can undermine safety. Expecting that safety remains constant may dangerously underestimate risk.

Safety management

Safety management involves continuous monitoring and intervention to maintain safety as the system evolves. A critical element of this process is monitoring system safety, which requires a reliable means of assessing the level of safety and identifying potential safety problems. This paper focuses on the requirements of monitoring system safety. In particular, this paper describes two complementary approaches that combine to provide an accurate measure of system safety: incident analysis and safety assessments.

Control theory provides a useful framework to examine safety management (Kjellen, 1987;

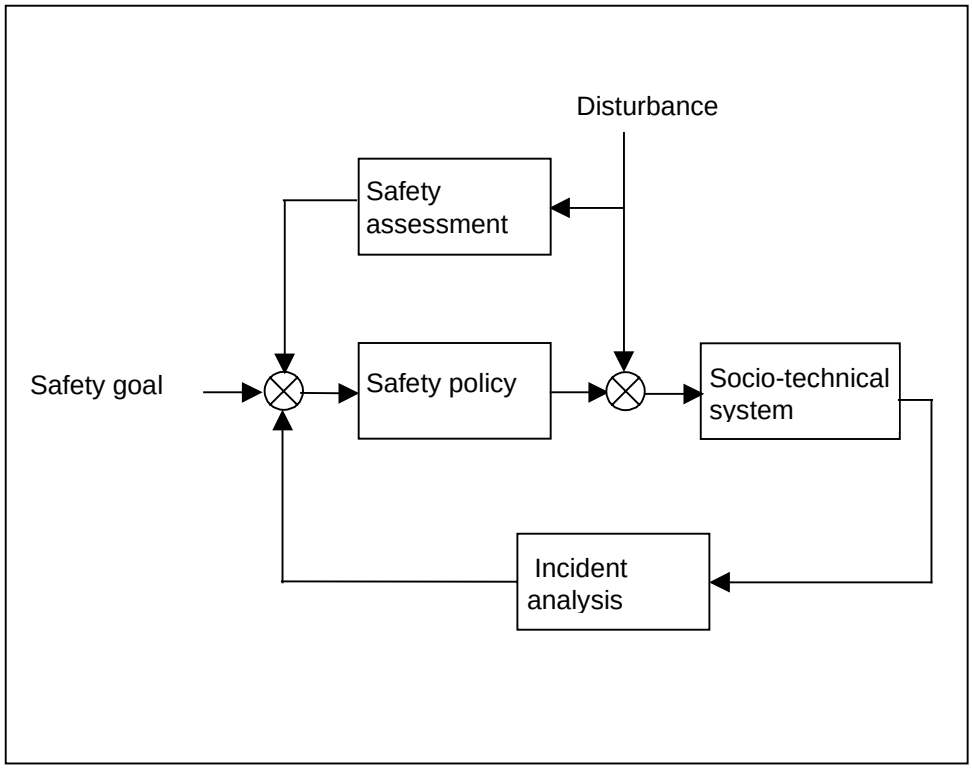

Figure 1. A control-theoretic description of safety assessment and incident analysis in safety management.

Rasmussen, in press). Control theory describes the response of a system to external disturbances and shows the effectiveness of various control strategies. In the context of safety management, external disturbances include changes in the environment, personnel, or equipment that influence system safety. Figure 1 uses the concepts of feedback and feedforward control to contrast the capabilities and limits of safety assessments and incident analysis. Safety assessment supports feedforward control and incident analysis supports feedback control. Safety assessment uses a model of the system to specify the adjustments required to compensate for measurable disturbances. As feedforward control, safety assessments enable compensation before the effects of the disturbance are seen in the system safety. In contrast, incident analysis relies on feedback control and so specifies adjustments based on changes in system safety. Because feedback control is based on changes in system safety it provides a means of control for both measurable and unmeasurable disturbances. Feedforward and feedback control have well-known capabilities and limits that can help clarify the requirements of successful safety management.

Incident analysis

Incident analysis provides invaluable data regarding system safety and has been formalized for several domains, such as the nuclear power, maritime and aviation. Incident analysis relies on self-reports of near accident situations to identify specific safety problems. These reports can also provide the basis for identifying more general failure modes. For example, inappropriate use of navigation equipment on ships has led to several incidents (MARS, 1995). These incidents identify specific safety problems associated with the human-machine interface of the navigation instruments. They also reflect the more general problem of potential declines in safety that may accompany advanced technology meant to enhance maritime safety (Lee & Sanquist, 1996; Perrow, 1984). The value of incident analysis lies in the ability to generalize beyond specific, micro-level problems, and specify more general, macro-level solutions. Generalizing from specific problems to general failure modes has been demonstrated in several domains (Kantowitz & Campbell, 1996; Kjellen, 1987).

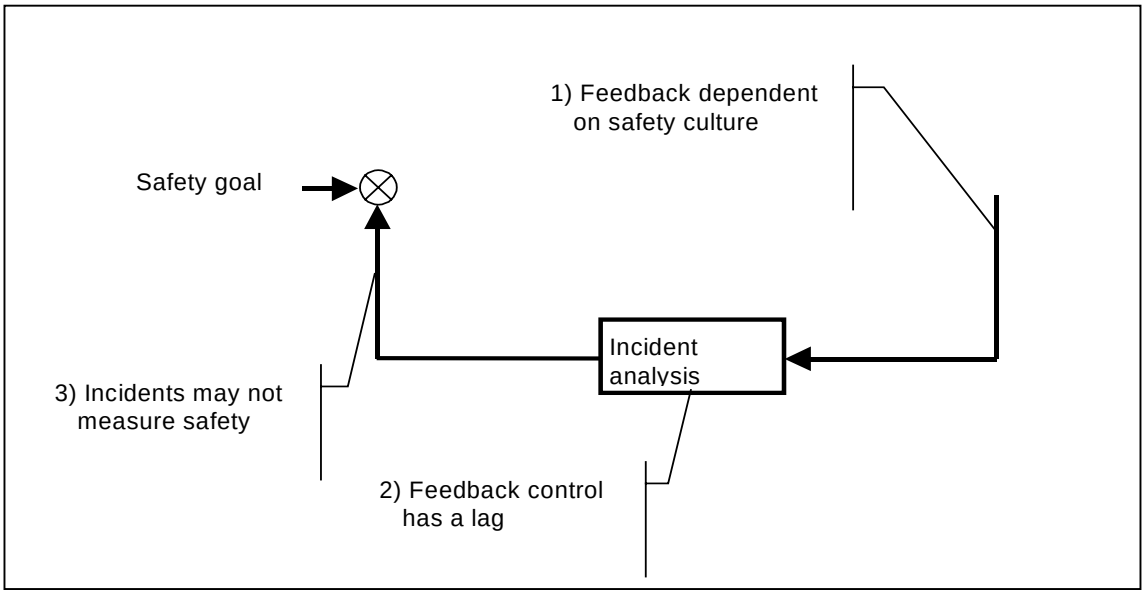

Figure 2. Barriers to safety management through incident analysis.

Although incident analysis provides significant insight into system safety, it has three important limits. These limits can lead to ineffective safety policies and serious overestimates of system safety. Figure 2 shows part of the control theory description of safety management. This figure highlights three important limits of incident analysis. The first limit reflects an important constraint of most incident analysis approaches: feedback depends on the voluntary support of the workers. Incidents that go unreported for fear of management retribution or lack of safety culture cannot influence safety. The second limit reflects a fundamental limit of feedback control: safety interventions will lag the appearance of safety problems. This means that safety may be seriously compromised before the problem is detected. The third limit concerns the diagnosticity of incident data: incidents may not reflect safety problems associated with catastrophic accidents. These limits must be considered for effective safety management.

Feedback dependent on safety culture

Observations at Ontario Hydro emphasize the importance of safety culture on the effectiveness of incident analysis. Observations suggest that the management does not have a realistic view of human error. When people make mistakes, it seems that management blames them and sometimes scolds them rather than understanding that the errors are actually induced and result from the excessive demands put on operators. Apparently, when people point out these facts, management's response is "How come no one else has the same problem?!" Ironically, the fact that operators are largely able to compensate for the deficiencies that they are faced with actually works against them because it masks the fact that errors can be induced by poor design and poor operating and maintenance practices. Thus, when errors do occur, they are viewed as the fault of an operator rather than what they really are, which is symptoms of a lack of proper systems design and integration (i.e., a lack of fit between the design of training, procedures, displays, controls, alarms, management maintenance policies, and the actual demands of the job).

To be fair, it should be pointed out that some efforts are continually being made to improve the situation but the level of problems which management considers to be "acceptable" is not very ambitious. For example, we were told that there is a work program in place to fix problems related to nuisance alarms and that the target goal for that program is 25 alarms. It seems that technical staff may not have a good appreciation for the implications that (a minimum) of 25 nuisance alarms always appearing

on an alarm summary screen have for effective and reliable monitoring.

Another example of lack of safety culture is that of people coming into the control room, despite the fact that most of these people are supposed to go into a meeting room instead. Because of the large number of people that can be in the control room at any one time, a large amount of noise can be generated. This is very distracting to the operators and can impair their ability to monitor. If the rules for control room traffic were obeyed or enforced, then this problem would not exist.

A final indication of the lack of safety culture on the part of management is the discrepancy between the official message that management tries to communicate (safety is key) and the actions and decisions that management makes. For example, we saw a sign listing the 10 Commandments of Reactor Safety:

1. Operate conservatively
2. Do not relax rules in times of crisis
3. Maintain defense in depth
4. Verify actions affecting reactor safety
5. If in doubt, stop and ask
6. Ensure all actions stand up to critical scrutiny
7. Understand the implications of any change
8. Do not live with problems
9. Determine and correct underlying reasons for problems
10. Keep it simple

Based on the examples presented above, it is clear that management does not obey all of its commandments, especially number 8.

It seems likely that many of these problems arise from the fact that there is no independent, centralized authority responsible for making decisions affecting safety and for setting priorities on maintenance and repair activities. Operators are the end users of the control room instrumentation and are responsible for the unit, so they should have key input into such a process because they know the impact that different problems can have on operations. Leveson (1995) discusses the kinds of steps that should be taken to put in place a process of this type. Unless operators are vested in safety improvement, their participation in an incident reporting scheme will be marginal. Considering only incident reports in an organization with a poor safety culture would reveal nothing about the latent failures that may be accumulating.

Feedback has a lag

Safety culture can also exacerbate the lag between problem detection and safety intervention, another critical limit of incident analysis. Observations at Ontario Hydro suggest that management has set a prioritized list of goals but they have not implemented this scheme in practice. This sends a very salient implicit message to all personnel, namely that safety does not come first. We were told that management has focused on what is easy to fix (e.g., housekeeping), rather than what is important to safety. This attitude seems to have originated with a mission statement that was developed a few years ago, which apparently stated that this plant should be perceived to be a world-class facility. The response to this attitude is best captured by the statement made by the renowned Nobel prize-winning physicist, Richard Feynman, after serving on the Presidential Commission investigating the Challenger space shuttle accident: "For a successful technology, reality must take precedence over public relations, for Nature cannot be fooled" (Feynman, 1988, p. 237). Until management's actions and reward structures are changed to be consistent with their stated priorities, the plant's safety culture will be far from what is desired. Without a firm commitment from upper management, lags in responding to safety problems will grow and undermine the effectiveness of incident analysis.

Incidents may not measure safety

The final limit of incident analysis rests on the fundamental assumption that the same causal factors that govern incidents also govern major accidents. The assumption follows the classic results of Heinrich (1931) who demonstrated that 29 minor injuries and 300 minor incidents occur for every serious injury. The implicit assumption is that the same causal factors that govern incidents and catastrophes. While this may seem to be a trivial limit it, is certainly true that a series of incidents are not always a precursor of major catastrophes.

Relying on incidents to identify major safety problems is not a responsible approach.

Safety assessment

Safety assessment complements incident analysis to provide a reliable measure of system safety. Safety assessment reviews operational procedures, operating conditions, safety culture, and the technical integrity of the system to identify changes in system safety. Safety assessment range from formalized reviews of hazard analyses to informal inspections of critical systems. A thorough assessment provides a comprehensive assessment of latent errors and failure modes. The safety assessment can be viewed as an investigation of an accident before there is an accident to investigate. Specifically, investigators often look back at all the problem signs that were present before an accident but that went unheeded (see Reason, 1990 and Leveson, 1995 for several examples based on the Three Mile Island, Bhopal, and Challenger accidents).

In terms of the control theoretic framework of safety management, safety assessment can compensate for some of the limits of incident analysis. Specifically, safety assessment acts as feedforward control, compensating for disturbances before they affect system safety. This alleviates the problem of lags in responding to safety problems and avoids the assumption that catastrophes stem have the same causes as minor incidents. While safety assessment has many benefits, it suffers from several limits that can be traced to those of feedforward control.

Figure 3 shows part of the control theory description of safety management, highlighting two key challenges for effective safety assessment. First, feedforward control requires a model of how the system will respond to disturbances. Because complex socio-technical systems often defy our ability to model and predict the consequences of many disturbances this can severely limit the benefits of a safety assessment (Wagenaar & Groeneweg, 1987). The second limit reflects the requirement that a feedforward control mechanism requires that disturbances must be measurable if they are to be counteracted. Frequently the complex disturbances that undermine system safety are not easily measured.

One of us (KJV) has conducted field research at one of Ontario Hydro's plants. The goal of that research was not related to safety assessment. Nevertheless, in the course of these field studies, we became aware of several factors that had, to us at least, an obvious connection to plant safety. The symptoms we observed were similar to those that are documented in reports that are produced *after* a large-scale accident occurs and investigators look back at the

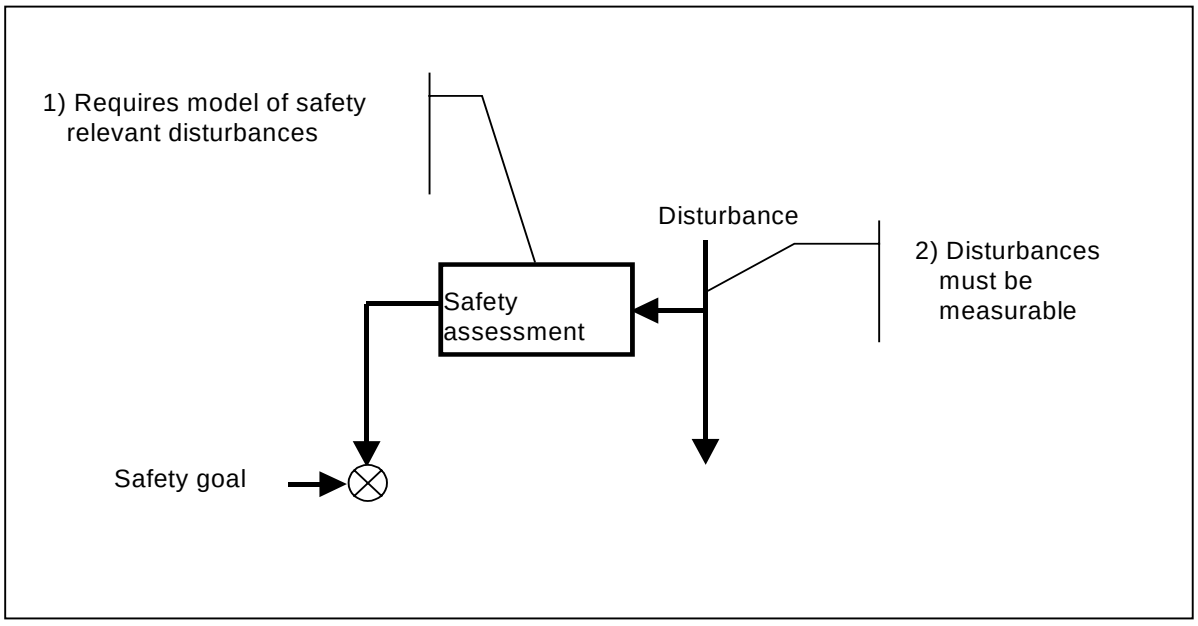

Figure 3. Barriers to safety management through safety assessment.

trail of warning signs to which insufficient attention had been paid (e.g., Perrow, 1984; Reason, 1990; Leveson, 1995). The difference was that, in this case, these symptoms were being observed *before* an accident, yet Ontario Hydro management did not seem to be terribly concerned. The informal safety assessment that resulted from these observations provides examples of how difficulties in measuring safety-relevant disturbances and modeling their effect can undermine safety.

Model of safety-relevant disturbances

The origin of the safety concerns at Ontario Hydro is clearly not technical in nature (Andognini, 1997). On the contrary, there are several reasons indicating that the CANDU reactor is a very advanced design from a technological standpoint. First, the nuclear reaction in a CANDU reactor is inherently unstable, so engineers decided to use digital automation since the 1960s. During this time, the digital technology has proven to be highly reliable compared to the analog technology that has been used in other plants, such as those in the US. Second, the CANDU reactor has been designed in such a way that it can be refueled on-line, while it is producing power to the grid. In contrast, other reactors have to be shut down to be refueled. Thus, the CANDU design has the potential to save a great deal of money by minimizing down time. Third, there is also a great deal of redundancy in the CANDU reactor design. There are multiple safety shutdown systems, and multiple, independent sensor channels are used to monitor key shutdown variables. As a result, the technical reliability of the design is further increased. Finally, CANDU reactors use heavy water as both a coolant and a moderator that keeps the nuclear reaction going. As a result, if there is a loss of coolant, there is also a loss of moderator that automatically slows down the nuclear reaction. This passive safety feature thereby greatly reduces the probability of a core meltdown. In summary, the safety problems at Ontario Hydro are not due to a primitive or deficient technology.

If the problems at Ontario Hydro were not the result of technological deficiencies, then what can they be attributed to? An obvious possibility is the occurrence of a large-scale accident. However, no such accident has ever occurred in the history of the Canadian nuclear industry. To be sure, there had been a number of incidents at Ontario Hydro that had raised concerns about safety with the Atomic Energy Control Board (AECB), the government nuclear regulatory body in Canada (Terry Taylor, personal communication, February, 1998). However, none of these ever threatened the integrity of the plant or the welfare of the public. Thus, the decision to close down the plants cannot be attributed to an aggressive response to a catastrophic accident either. Instead, the root cause of all of the problems was insufficient attention to human and social-organizational factors. Ontario Hydro management seemed to believe that nuclear safety could be maintained by technology alone.

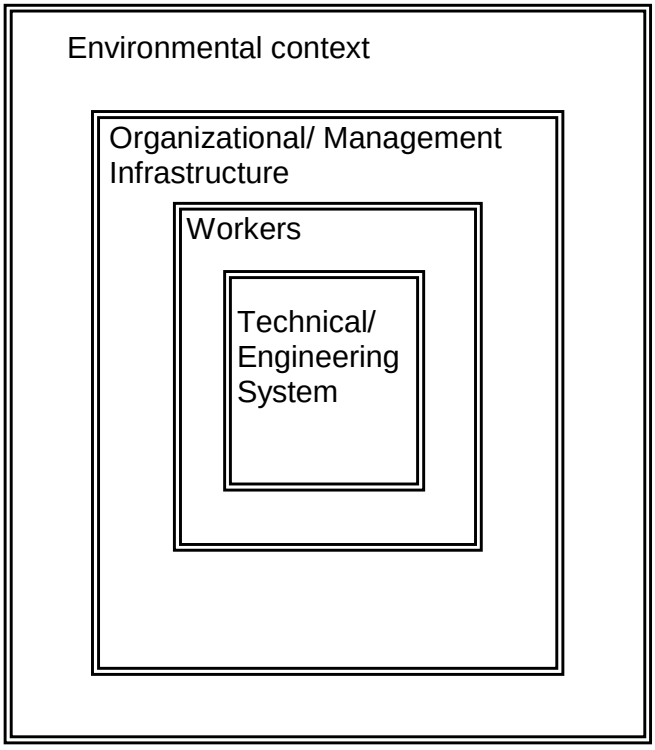

Figure 5: Levels of the socio-technical system that must be included in a safety assessment

The unjustified satisfaction of the Ontario Hydro management concerning system safety stems from a failure to consider the full range of factors affecting safety. Their implicit model of system safety seems to have focussed on the technical/engineering system in the center of Figure 5. A more in-depth safety analysis shows that overall system safety is highly dependent of the workers and the organizational and management infrastructure. Focusing on one part of the complex system provides a misleading estimate of system safety. Unfortunately focusing on a quantitative analysis of the technical engineering system is not uncommon, possibly reflecting the inherent difficulties of modeling the outer levels of the system.

Disturbances must be measurable

Another limit of safety assessments is that the disturbances that affect safety must be measurable. Often disturbances are unanticipated and not easily measurable from a technology-centered perspective. Because workers adapt to accommodate disturbances their effects may not be immediately apparent. Thus, a safety analysis must be sensitive to the full range of factors affecting system safety.

As an example, many of the factors that make monitoring difficult stem from the fact that the plant is no longer operated in the way that was originally intended. The problem is that the instrumentation has not been updated (especially the alarm system) to reflect the reality of how the plant is currently operated. Several examples were identified. On at least one unit, the heaters on the deaerator system were originally designed to be normally run on automatic. However, it was found that this would put too great a load on the electrical bus. Thus, the current practice is to normally have the heaters off rather than on automatic. The problem lies in the fact that there is a light at the top of the panel which lights up when any handswitch is not in its "normal" position. The logic for this indication is still based on the outdated assumption that the heaters are supposed to be run in the automatic mode. As a result, this "warning" light is always on, even when the unit is running properly, thereby making it worse

than useless because it distracts operators' attention from noticing indications that are truly meaningful.

Other signs that operators are being forced to live with problems because management has not given sufficient priority to updating or maintaining instrumentation and equipment were also observed. For example, the long term status binder of one reactor unit documents the fact that there is a component that has been reported as being deficient and has been waiting for parts to repair it since 1990! The severity of this delayed response in terms of safety degradation was not established.

The most serious problem that we uncovered is the status of the Emergency Core Injection (ECI) flowmeters. We were told that these meters have not functioned properly since the plant was first constructed. Their deficiency is not a subtle one; they indicate flow when there is none! Attempts have been made over the years to remedy this problem but without success. There are several reasons why this may be an important threat to safety. First, on at least some of the units, these meters have not been reported as deficient or disabled. Thus, they are showing faulty readings. Second, the emergency operating procedures refer to these meters as a way of verifying ECI activation. Thus, in an emergency, it is possible that operators would follow the procedure and forget that the meters are not providing accurate readings. If for some reason, the ECI system were not to activate properly, the meters would still indicate flow, and operators would incorrectly infer that there was flow when there was none. Operators have been told to use other meters to confirm if there is in fact any flow from the ECI system. However, we do not know if this amended practice is documented anywhere. Moreover, if it is the case that these meters work properly in the simulator (we do not know if this is the case, but it seems likely), then operators would be trained to use the meters which are faulty in the control room, thereby making it more likely that they would use them in an emergency, rather than remembering to follow the amended practice. This problem seems to be an accident waiting to happen.

A similar problem surrounds the pressure sensor test circuit for the heat transport system. The problem is an important one because this pressure sensor is one of the parameters that can trigger a safety system. There are two sets of valves surrounding this pressure sensor, one pair which is manually operated from the field only, and the other pair which are isolation valves operated from the control room. The testing is intended to be controlled with the isolation valves, not the manual valves. We were told that the isolation valves have parts missing, and so the manual valves must be used instead. The potential problem in this case results from the fact that there are two manual valves leading to the pressure sensor, one that is part of the test circuit and the other which leads to the heat transport system itself. Under normal operations, the path that leads to the heat transport system should be open (so that the sensor can measure the state of the system), whereas the path that leads to the test circuit should be closed (so that the test circuit does not interfere with the accurate measurement of pressure). During the test, the inverse true, since the idea is to connect the pressure sensor to the test circuit, temporarily isolating it from the heat transport system. The danger is that the manual valve connecting the sensor to the heat transport system may be mistakenly left closed after a test. This is not an unheard of error in maintenance tasks conducted out in the field (Rasmussen, 1978). The error would be much less likely to occur if the isolation valves that can be controlled from the control room were used for the test, as they are supposed to be. Should this error occur, then the pressure sensor, which is a safety system sensor, would be nullified because it would become isolated from the heat transport system whose pressure it is supposed to be measuring. Clearly, this is a very serious problem. Moreover, it does not have any visible symptoms, and as a result, it can go unnoticed for a long time. Like the previous example, this is an accident waiting to happen, needing only an unlikely but possible set of events to occur to trigger it. This is the classic pattern of large-scale accidents (Reason, 1990).

The limitations of the alarm system in particular were vividly pointed out to us at the beginning of one shift, when the operator took an alarm summary

from the printer and reviewed with us the reasons why each alarm was in. On this particular occasion, there were 8 analog alarms in. All of these were nuisance alarms: 3 were caused by equipment that had been DRed, 2 were jumpered out, and 3 resulted from work permits. Thus, despite the fact that there was no problem, 8 analog alarms were still active. The situation was even worse for contact indicator alarms. There were a total of 27 such alarms at the start of the shift. The causes for these alarms were as follows: 15 resulted from equipment that had been reported as being deficient, 4 from work permits (one of these since 17/7/95!), 1 from equipment that was temporarily missing, 2 from systems that were not in service, 3 from other units, and only 2 that were veridical indications of problems that required attention. Clearly, monitoring is made much more difficult when only 2 out of 35 alarms actually signify a problem.

Updating is also relevant to procedures as well. The operating manuals describe the original standard practice. Operating memos describe changes to these original practices. While the operating memos refer to the operating manuals, the reverse is not true. As a result, if an operator looks in the manuals to look up a procedure, it is easy to make a mistake if they do not remember that there is an operating memo modifying that procedure. This problem is aggravated by the fact that on at least some units, there is a whole binder full of operating memos, some going back to at least 1993. Thus, the sheer number and the dated nature of some of the memos make a mistake more likely to occur.

It is very interesting to observe that the same situation does not occur with the emergency operating procedures (AIMS). In this case, a photocopy of any relevant operating memo is included in the procedure manual itself. It would be a simple thing to do the same thing for the operating manuals (e.g., a colored photocopy could even be inserted to signify to the operator that there is an operating memo pertinent to that procedure). It seems that management does not think that the effort is worthwhile for operating memos that do not refer to emergency operating procedures. While it is certainly true that the AIMS have a higher impact on safety in terms of magnitude, it must be pointed out that the operating manuals are consulted much more frequently than the AIMS. Not using the same cross-referencing practice for both will tend to induce errors much more frequently although of less severity.

The wide range of changes that occur across time make safety assessments conducted at the beginning of the system lifecycle quite inaccurate. Because workers are extremely adaptive the effect of these changes can be masked making it difficult to assess their safety consequences. The difficulty in measuring these changes and anticipating their effect undermines a feedforward control strategy, such as safety assessment.

Conclusions

Combining incident analysis and safety assessments provides an effective gauge of system safety. Each approach has limits that can generate a distorted view of system safety. Combining the two approaches provides a reliable measure of safety. Safety management is a requirement for complex systems due to changing level of safety as system evolves. Risk assessments completed when the system was first developed may have little relevance to system safety after several years of operation because systems evolve and change in ways that cannot be anticipated. These changes can seriously undermine system safety. Safety management can address this problem with a continual assessment of system safety using incident analysis and safety assessments.

Control theory provides a useful framework to compare the complementary contributions of incident analysis and safety assessment. Incident analysis supports feedback control of safety and the limits of feedback control bound the benefits of incident analysis. Specifically, incident analysis is limited because:

- Feedback depends on safety culture.
- Feedback control has a lag.
- Incidents may not measure safety.

Safety assessment supports feedforward control and is bounded by the requirements of feedforward control. Some specific limits include:

- Interventions requires model of safety-relevant disturbances

- Disturbances must be measurable and recognizable.

The complex socio-technical nature of many systems makes safety management difficult. This is illustrated by the case of Ontario Hydro, where a technology-centered focus ignored safety issues and engendered "an inadequate respect for radiation" (Andognini, 1997, p. 62).

References

Andognini, G. C. (1997). *Report to management: IIPA/SSFI evaluation findings and recommendations*. Toronto: Ontario Hydro.

Feynman, R. P. (1988). *"What do you care what other people think?": Further adventures of a curious character*. New York: Norton.

Heinrich, H.W. (1931). *Industrial Accident Prevention: A Scientific Approach.* New York, NY: McGraw-Hill.

Kjellen, U. (1987). Deviations and the feedback control of accidents. In J. Rasmussen, K. Duncan, and J. Leplat (Eds.), *New technology and human error.* New York: Wiley.

Kantowitz, B. H. & Campbell, J. C. (1996). Pilot workload and flightdeck automation. In R. Parasuraman and Mustapha Mouloua (Eds.), *Automation and human performance: Theory and applications*. Mahwah, New Jersey: Lawrence Erlbaum.

Lee, J. D. & Sanquist, T. F. (1996). In R. Parasuraman and Mustapha Mouloua (Eds.), *Automation and human performance: Theory and applications*. Mahwah, New Jersey: Lawrence Erlbaum.

Leveson, N. G. (1995). *Safeware: System safety and computers*. Reading, MA: Addison-Wesley.

Moray, N. & Huey, B.M. (Eds.) (1988). *Human factors research and nuclear safety.* Washington, D.C.: National Academy Press.

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. New York: Basic Books.

Rasmussen, J. (1978). *Operator/technician errors in calibration, setting, and testing nuclear power plant equipment* (N-17-78). Roskilde, Denmark: Risø National Laboratory, Electronics Department.

Rasmussen, J. (in press). Risk management in a dynamic society: A modelling problem. *Safety Science*.

Reason, J. (1990). *Human error*. Cambridge, England: Cambridge University Press.

Vicente, K. J., Burns, C. M., Mumaw, R. J., & Roth, E. M. (1996). How do operators monitor a nuclear power plant? A field study. In *Proceedings of the 1996 American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies* (pp. 1127-1134). La Grange Park, IL: American Nuclear Society.

Wagenaar, W.A. & Groeneweg, J. (1987). Accidents at sea: Multiple causes and impossible consequences. *International Journal of Man-Machine Studies.* (27) 587-598.