National Transportation Safety Board

Washington, D.C. 20594

Safety Recommendation

Date: December 23,2005

In reply refer to: P-05-1 through P-05-5

Ms. Stacy Gerard
Acting Assistant Administrator/Chief Safety Officer
Pipeline and Hazardous Materials Safety Administration
400 Seventh Street, SW
Room 2103
Washington, DC 20590

In the pipeline industry, Supervisory Control and Data Acquisition (SCADA) systems are used to collect data from pipeline sensors in real time and display these data to humans who monitor the data from remote sites and remotely operate pipeline control equipment. This study was designed to examine how pipeline companies use SCADA systems to monitor and record operating data and to evaluate the role of SCADA systems in leak detection. The number of hazardous liquid accidents investigated by the National Transportation Safety Board in which leaks went undetected after indications of a leak on the SCADA interface was the impetus for this study. The Safety Board developed a survey to obtain data about the liquid pipeline industry's use of SCADA systems with input from industry. In addition to obtaining survey data, the Safety Board visited 12 pipeline companies that had operating SCADA systems. Based on information from previous accidents investigated by the Board, survey results, and site visit results, the Safety Board's review of SCADA systems in the hazardous liquid pipeline industry uncovered five areas for potential improvement: display graphics, alarm management, controller training, controller fatigue, and leak detection systems.

SCADA Display Graphics

Since its inception in the late 1960s, SCADA has evolved in many areas, but none is as extensive as the use of graphics in the SCADA controller interface. Early displays used monochromatic cathode ray tubes (CRT) with line printers connected to the system. These systems used symbols, such as asterisks, to warn controllers of a potential problem. Early systems represented the pipeline based upon the organization of computing hardware, rather than the configuration of the pipeline itself.

As computer graphics capabilities improved, however, SCADA designs evolved from coded depictions of computer hardware to depictions of pipeline schematics. Current SCADA systems are a mix of tabular and schematic displays. However, one company in the survey presented data in a display that integrated input and output volumes on a pipeline segment into one display, enabling its controllers to identify leaks quickly. The use of such integrated displays has become commonplace in many types of control systems, including those used in the nuclear power and aviation industries.

The Safety Board has advocated graphical standards for computerized control systems since the Brenham storage cavern accident, which occurred in 1992. The Board's recommendation for graphical standards (P-93-22) prompted the API to establish a graphics committee under the cybernetics working group to establish recommended practices for the use of graphics for SCADA interfaces.

The graphics committee began its task in 2001 by reviewing the systems in place at their respective companies. Each company represented on the committee submitted sample SCADA screens. Recognizing the wide diversity among the various systems graphically, the group began looking for acceptable rules for SCADA system graphic design. On July 27, 2005, the committee released a draft of its SCADA Display Recommended Practice 1165 for review.

The use of graphics standards in other industries is widespread. The Nuclear Regulatory Commission published guidelines for the use of human factors in display design in its *Human-System Interface Design Review Guidelines*.[1] The FAA has published human factors guidelines for display design.[2] The power industry has also developed standards in the *Fossil Fuel Power Plant Human-Machine Interface—CRT Displays*.[3] The development of these guidelines has improved the clarity of displays that operators use in control systems. As noted in chapter 4 of the SCADA Safety Study, the Safety Board found many displays in its review that did not follow widely accepted human factors design guidelines for various industry applications. The issues identified included poor contrast between foreground colors and background colors; overuse of colors; displays that were not colorblind friendly; and cluttered displays. The API has released draft guidelines that address the display concerns raised above, including the need for coding of color information for colorblind controllers. Absent the presence of good guidelines, some systems are going to be poorly designed, thereby hindering a controller's ability to detect a leak. Accordingly, the Board concludes that implementation of graphical standards developed for pipeline operations will increase the likelihood that leaks will be detected and that resulting damage from the leaks will be minimized. Therefore, the Safety Board recommends that OPS require operators of hazardous liquid pipelines to follow the American Petroleum Institute's Recommended Practice 1165 for the use of graphics on the SCADA screens.

---

[1] U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Energy Sciences and Technology Department, Brookhaven National Laboratory, *Human-System Interface Design Review Guidelines* NUREG-0700, Rev.2 (Upton, New York: NRC, 2002).

[2] Department of Transportation, Federal Aviation Administration, Human Factors Design Guide for Acquisition of Commercial-Off-The-Shelf Subsystems, Non-Developmental Items, and Developmental Systems, DOT/FAA/CT-96/01 (Atlantic City International Airport, NJ: William J. Hughes Technical Center 1996).

[3] The Instrumentation, Systems, and Automation Society, *Fossil Fuel Power Plant Human-Machine Interface—CRT Displays*, ISA-TR77.60.04-1996 (Research Triangle Park: NC, 1996).

Alarm Philosophy

A key element of the SCADA system display is the alarms that indicate changes along the pipeline. All of the SCADA systems examined in the study use auditory and visual indications to make the alarms more noticeable. During site visits, controllers were asked what they believed to be the most important aspect of the SCADA system for preventing incidents. Most—9 of 12—included alarms in their responses. Nearly all controllers listed the alarm page as one of the screens they used in diagnosing abnormal operating conditions.

Alarms that indicate abnormal conditions along the pipeline must be designed to convey their meaning clearly to the controller. Poorly designed alarms can be difficult to interpret, leading the controller to take actions inappropriate to the actual situation. The importance of alarms in helping controllers understand leaks cannot be overstated. In the Gramercy accident,[4] the line balance alarm indicated that more liquid was entering the pipeline than was being delivered. This alarm occurred 11 seconds after one alarm and 4 seconds before another. In the midst of this quick succession of alarms, the controller failed to read the text of the line balance alarm completely and misinterpreted the alarm. When another line balance alarm occurred 1 hour later, its isolation from other alarms allowed the controller to detect and react to the alarm. In several other accidents, controllers also misunderstood alarms or no alarms were available. In the Winchester accident,[5] for example, the leak detection alarm first alerted the controllers 2 hours before they shut down the line. In the Chalk Point accident, controllers were unable to monitor the pipeline through the SCADA system because the system was not designed to monitor the pipeline during cleaning operations. Had a SCADA system been available, the Chalk Point controllers might have detected the leak more quickly.

Alarms are important for directing a controller's attention; however, alarming potential leak events too often can be distracting. The system designer sets the threshold for an alarm so that virtually no true alarm conditions will fail to set off an alarm. The result is that occasional alarms occur when no true alarm exists (a false alarm). Although SCADA system designers may not view a single false alarm as a problem, multiple false alarms may be. If a controller responds to a false leak alarm, the economic cost of shutting down the line is small compared with the possibility of spilling a large amount of product. However, as the number of false alarms increases, so does the cost of responding to all of them. Controllers may try to differentiate false alarms from true alarms and respond only to the latter. As a result, they may miss a true alarm, increasing the severity of a product leak. In the Gramercy accident, the controller commented that he always saw certain leak alarms when he adjusted the line segment he was working on. In the Kingman accident, the controller stated that, after seeing the rate of change alarm for pipeline pressure, he was waiting for pressure to return to normal as it had in the past.

---

[4] National Transportation Safety Board, *Release of Hazardous Liquid Near Gramercy, Louisiana, May 23, 1996*, Pipeline Accident Brief NTSB/PAB-98/01 (Washington, DC: NTSB, 1998).

[5] National Transportation Safety Board, *Hazardous Liquid Pipe Failure and Leak, Marathon Ashland Pipe Line, LLC Winchester, Kentucky, January 27, 2000,* Pipeline Accident Brief NTSB/PAB-01/02 (Washington, DC: NTSB, 2001).

One way to ensure controller attention to critical alarms is to prioritize them. The Human Factors Design Standard (HFDS)[6] produced by the Federal Aviation Administration states that "alarms should be automatically organized and presented to the users in a prioritized manner." Alarms that would indicate an immediate action, such as indicators of potential product loss, should override all alarms and require immediate action by a controller. Prioritized alarms would help controllers recognize which alarms can wait and which require immediate attention and action. More than 25 percent of the companies surveyed currently do not prioritize alarms. As a result, controllers may be receiving unnecessary alarms that result in lower vigilance to all alarms.

In addition to being prioritized, alarms can be suppressed when a controller knows the information that the alarm provides, such as an alarm that indicates an increase in flow following a pipeline startup. Controllers then have fewer alarms to read but can later check for alarms that were suppressed in the alarm log. Alarms that could be suppressed include repetitive alarms and alarms that signal situations of which the controller is aware, alarms that are the result of equipment being out of service, or multiple alarms that are related to one fault.[7]

An oil company presented its strategy for alarm management at the *2002 Pipeline and Cybernetics Conference* sponsored by the API.[8] The company reported performing periodic reviews to remove unnecessary alarms and properly define all alarm settings. They also reported training its controllers to deal with a burst of alarms that can occur with a system leak. The company reported dividing its alarms into three categories: priority three alarms, which signify notices of normal operations that may not require any action on the part of the controller; priority two alarms, which signify a device in trouble or a significant critical operation alert and for which the response would be based upon the controller's training; and priority one alarms, which protect against product containment or and for regulatory compliance. For priority one alarms, controller action is required as is documentation of the action.

In addition to prioritizing and suppressing alarms, SCADA managers need to work with controllers to ensure that the meaning of each alarm is unambiguous.[9] For example, in one site visit the controller noted that alarms were labeled with codes that were more for the SCADA manager to use in diagnosing SCADA software than for controllers to use to understand a problem on the pipeline. Designing alarms to be more meaningful would assist controllers in making accurate decisions.

Ensuring that alarms do not occur too frequently and are understood by controllers requires the company to have an effective alarms audit system. "It is important to continuously audit, maintain and improve the alarm system through analysis and review with the operators on

---

[6] Department of Transportation, Federal Aviation Administration, *Human Factors Design Standard*, DOT/FAA/HF-STD-001 (Atlantic City International Airport, NJ: William J. Hughes Technical Center, 2003).

[7] D. Bailey and E. Wright, *Practical SCADA for Industry* (London, England: IDC Technologies Inc., 2003).

[8] *2002 Pipeline and Cybernetics Conference*, American Petroleum Institute, Houston, Texas, April 21-23, 2002.

[9] C.E. Billings, *Human-Centered Aviation Automation: Principles and Guidelines* (Moffett Field, CA: National Aeronautics and Space Administration, Ames Research Center, 1996).

the performance of the system."[10] Following the Gramercy accident, the Safety Board recommended that the company:

> Evaluate the effectiveness of alternative display formats and frequencies of alarming critical information for your supervisory control and data acquisition system and modify the system as necessary to ensure that controllers are specifically prompted to consider the possibility of leaks during system deviations that are consistent with a loss of product from a pipeline. (P-98-22)

As a result of their review of leak alarms, the company was able to reduce the number of leak alarms from 150 to 200 a day down to 60 per day. The Safety Board classified recommendation P-98-22 as "Closed—Acceptable-Action."

In the Safety Board's survey, 26 of the 78 control centers that responded to the survey reported having no plan in place for reviewing/auditing alarms. Each control center should have a review/audit policy with regular review intervals to ensure that controllers are appropriately responsive to each alarm they receive. The Safety Board concludes that an effective alarm review/audit system will increase the likelihood of controllers appropriately responding to alarms associated with pipeline leaks. Therefore, the Safety Board recommends that the Office of Pipeline Safety require pipeline companies to have a policy for the review/audit of alarms.

Training and Selection

Pipeline controllers are primarily trained on the job. As such, controllers become very proficient at handling the day-to-day operations of a pipeline system. However, the training of infrequent events, such as leak detection and mitigation, must be learned from methods other than on-the-job training. In addition, although it is optimal to have controllers shut down a pipeline as soon as a leak occurs, oftentimes the evidence of a leak is ambiguous. This ambiguity leads controllers to call in others to help decide if a leak has occurred.

The issues of controller training, selection, and qualification have been noted in six of the SCADA-related accidents the Safety Board investigated. For example, in the Fork Shoals accident,[11] the Board noted that the "training provided by the operator to its pipeline controllers and shift supervisors before the accident was inadequate to prepare them to respond properly and in a timely fashion to abnormal conditions and pipeline emergencies." Likewise, in the Gramercy accident, the Board recommended that the operator use recurrent pipeline controller training to increase controller proficiency in interpreting and responding to control system data that may indicate a system leak.[12] In both accidents, controllers misunderstood SCADA indications of a leak and failed to respond quickly.

[10] Bailey and Wright, *Practical SCADA for Industry*.

[11] National Transportation Safety Board, *Pipeline Rupture and Release of Fuel Oil in the Reedy River at Fork Shoals, South Carolina*, Pipeline Accident Report NTSB/PAR-98/01 (Washington, DC: NTSB, 1998).

[12] The Gramercy recommendation on training, P-98-21, was classified "Closed—Unacceptable Action" on April 28, 1999.

Following the Winchester, Kentucky, accident, the operator indicated that the company was in the process of incorporating a training simulator into its training program so that controllers could experience simulated leaks on the pipeline. In a similar manner, the pipeline operator in the Knoxville, Tennessee, accident[13] planned to incorporate data from the accident into its simulator to better train controllers in leak recognition and response.

In 1987, following two gas pipeline accidents, the Safety Board issued Safety Recommendation P-87-2, asking the Research and Special Programs Administration (RSPA) to require that operators of pipelines develop and conduct selection, training, and testing programs to annually qualify employees. In 1998, the Safety Board classified the recommendation "Closed—Unacceptable Action" because RSPA had failed to conduct the required rulemaking. In 1997, following an accident in San Juan, Puerto Rico,[14] the Safety Board issued Safety Recommendation P-97-7, asking RSPA to complete a final rule on employee qualification training and testing standards within 1 year, to require operators to test employees on the safety procedures they are expected to follow, and to demonstrate that employees can correctly perform the work.

RSPA issued a Notice of Proposed Rulemaking in October 1998, and in January 1999, the Safety Board commented on it, noting that the proposed rule failed to adequately address qualification requirements or include requirements for training and testing. The final rule, issued in April 2001, allowed controllers to be evaluated by written or oral examinations, observation during on-the-job performance, or work history. After October 28, 2002, operators were not allowed to use work history as an evaluation measure and were required to use another method at the next evaluation, such as a written test. However, the rule allowed operators to determine the interval between evaluations. It was therefore conceivable that a pipeline employee might indefinitely continue to perform safety-related tasks based solely on work history. Accordingly, the Board closed Safety Recommendation P-97-7, unacceptable action, noting that the rule failed to address the importance of testing the controller at regular intervals.

On March 3, 2005, in response to the *Pipeline Safety Improvement Act of 2002*, OPS promulgated additional regulations for qualification of pipeline controllers. These regulations restricted operators from using observation of on-the-job performance as the sole method of evaluation and required operators to provide appropriate training to ensure that individuals performing covered tasks had the necessary knowledge and skills to perform the tasks.

On April 15, 2005, in response to the *Pipeline Safety Improvement Act of 2002*, OPS also published a request for control centers to participate in their pilot program on controller certification. The three centers for the study have been selected and the OPS study team has

---

[13] National Transportation Safety Board, *Hazardous Liquid Petroleum Products Pipeline Rupture, Colonial Pipeline Company, Knoxville, Tennessee, February 9, 1999,* Pipeline Accident Brief NTSB/PAB-01/01 (Washington, DC: NTSB, 2001).

[14] National Transportation Safety Board, *San Juan Gas Company, Inc./ENRON Corp., Propane Gas Explosion in San Juan, Puerto Rico, on November 21, 1996*, Pipeline Accident Report NTSB/PAR-97/01 (Washington, DC: NTSB, 1997).

begun regular meetings with these participants. The team is on schedule to deliver a report to Congress by December 2006.

In addition to the rulemaking actions described above, industry has taken steps to improve controller training and qualification. For example, the American Society of Mechanical Engineers (ASME) is creating a standard for qualifying pipeline personnel. The ASME B31Q committee, which is charged with developing the new pipeline operator qualification standard, is currently reviewing comments on the draft version, which was available for public comment on February 2, 2005. The committee identified nine tasks for ensuring that pipeline controllers are qualified. Training tasks related to leak detection are to "monitor system operation including monitoring for pipeline leaks" and to "recognize and react to abnormal situations."

As of November 30, 2004, RSPA responsibilities regarding the implementation of pipeline controller training were transferred to the Pipeline and Hazardous Materials Safety Administration (PHMSA). Changes currently being implemented by PHMSA and ASME to shape the qualification and training of controllers have been suggested by the Safety Board for 20 years. The Safety Board recognizes that, although overdue, these actions are a positive step toward achieving pipeline safety objectives.

Several training coordinators interviewed during the study also highlighted ongoing activities at their companies to improve controller training, including the use of simulators. Two trainers commented on their efforts to incorporate simulators into their training. At the time of the Safety Board's survey, only 23 of the 91 control centers reported having simulators. Training coordinators also mentioned that using leak detection tools and trend screens are an aspect of training that controllers have the most difficulty understanding.

During the course of the study, the Safety Board found that lessons learned in other industries could be applied to SCADA systems in the pipeline industry, particularly in regard to the development of more realistic training. Following the power outage of August 14, 2003, for example, the North American Electrical Reliability Council[15] found that operators using SCADA systems to monitor the status of the electric grid were not adequately prepared to deal with the abnormal operations that occurred on that day. The SCADA controllers on the electric grid were trained on the job, just as pipeline controllers were often trained. The Council concluded that controllers need improved training for abnormal operations, including simulations of abnormal operation either on computer or as tabletop drills.

Pipeline training coordinators who used simulators for training reported that the simulators were invaluable for leak detection training. In contrast, they found on-the-job training for leak detection to be difficult because such events are rare and may not occur during training. Coordinators stated further that oral or written tests might not be the most effective means of training controllers to recognize leak events. The Safety Board concludes that requiring controllers to train for leak detection tasks using simulators or non-computerized simulations will improve the probability of controllers finding and mitigating pipeline leaks. Therefore, the Safety Board recommends that the Office of Pipeline Safety require controller training to include

---

[15] U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 5, 2004.

simulator or non-computerized simulations for controller recognition of abnormal operating conditions, in particular, leak events.

Fatigue Management

Of the 18 controllers interviewed in the study, 8 reported their work schedules as the general thing they most disliked about their jobs. When all 18 controllers were asked if there was anything they disliked about their work schedules, 10 indicated working the night shift or not getting enough sleep, particularly when their shifts changed from day to night or night to day. Eleven of the twelve companies visited by the Safety Board used rotating 12-hour shifts to control and monitor pipelines. At one company, a controller monitored the pipeline during business hours, and the SCADA system alerted a receptionist or answering service, who informed the on call controller when an alarm occurred.

Fatigue related to rotating 12-hour shifts has been examined in numerous studies. In a 1999 study,[16] researchers examined workers at a petrochemical plant and measured their alertness at three intervals (second, sixth, and tenth hour). They found that, according to subjective ratings, controllers working the night shifts were less alert in their tenth shift hour than during their second hour (a decrease from 8.1 to 5.1 on a 10-point scale). This decrease in alertness persisted through their three-night schedule. Conversely, their daytime counterparts were able to maintain alertness over their whole shift. In another study,[17] researchers found that decreased performance (187 percent more errors) and increased sleepiness (66 percent) for workers of a 12-hour shift during their last 4 hours on shift. Also, workers on the 12-hour work schedule reported reductions in the amount of sleep and its quality. When the same workers were retested 3.5 years later,[18] subjects working the 12-hour shift still showed decreased performance on a number of cognitive tasks and less quality sleep than their 8-hour shift counterparts.

Among the companies visited, the Safety Board found that the rotation between night and day shifts varied widely. One company used a monthly rotation with controllers on day shifts for a month followed by night shifts for a month. Another company used 4 day shifts followed by 4 night shifts.

Rotating controllers from day to night shifts was discussed in the Safety Board's Fork Shoals accident report.[19] That controller had worked during the day on his last shift and had just moved to the night shift. Such inversions of schedule can increase fatigue. In addition, the controller had been awake for 17 hours when the accident occurred. Following the Fork Shoals accident, the Safety Board recommended that RSPA assess the potential safety risks associated

[16] F.M. Fischer, C.R.C. Moreno, F.N.S. Borges, and F.M. Louzada, "Alertness and Sleep after 12 Hour Shifts: Differences Between Day and Night Shift Work," *Proceedings, XIV International Symposium on Night and Shiftwork*, September 13-17, 1999.

[17] R.R. Rosa, M.J. Colligan, and P. Lewis, "Extended Workdays: Effects of 8-Hour and 12-Hour Rotating Shift Schedules on Performance, Subjective Alertness, Sleep Patterns, and Psychosocial Variables," *Work and Stress* 3(1) (1989), pp. 21-32.

[18] R.R. Rosa, "Performance, Alertness, and Sleep After 3.5 Years of 12 Hour Shifts: A Follow-Up Study," *Work and Stress* 5(2) (1991), pp. 106-116.

[19] NTSB/PAR-98/01

with rotating pipeline controller shifts and provide guidelines for controller work schedules that reduce the likelihood of accidents attributable to controller fatigue (P-98-30).[20]

The Safety Board also issued Safety Recommendation P-99-12[21] to RSPA as a result of its safety report, *Evaluation of U.S. Department of Transportation Efforts in the 1990s to Address Operator Fatigue*.[22] The recommendation asked RSPA, within 2 years, to establish scientifically based hours-of-service regulations that set limits on hours of service, provided predictable work and rest schedules, and considered circadian rhythms and human sleep and rest requirements. Both pipeline fatigue recommendations are on the Safety Board's Federal Most Wanted List.

In response to both recommendations, RSPA stated in 2000 that it was trying to determine the role of fatigue in pipeline accidents and that it was considering an advisory bulletin on the issue of controller fatigue. RSPA stated that it had also examined its accident database for the prevalence of controller fatigue in pipeline accident reports. After analyzing the database, RSPA stated that fatigue was not a factor in pipeline accidents although it should be noted that items related to fatigue, such as controller work schedules, were not available in the dataset.

PHMSA, which has assumed responsibility for Safety Recommendation P-98-30, has initiated another study on fatigue to address the recommendations.[23] In 2004, Batelle Memorial Institute was awarded a contract to conduct research on human factors in the pipeline control room. The research plan includes an examination of fatigue in the control room and will examine multiple pipeline companies.

OPS developed an advisory bulletin, *Pipeline Safety: Countermeasures to Prevent Human Fatigue in the Control Room* (FR Doc. 05–15956), on rotating schedules for the pipeline industry. The bulletin suggests that companies achieve the following: develop shift rotation practices that minimize fatigue, limit controllers to 12-hour shifts unless extraordinary or emergency situations are involved, document cases where controllers have to work longer than 12 hours in a shift, ensure that controllers get 10 hours of rest between shifts, and develop guidelines for scheduling controllers that consider the effects of fatigue. In addition, the bulletin includes suggestions for training controllers and supervisors about fatigue and ensuring that the control room environment does not induce fatigue. To ensure that companies do not take advantage of extraordinary or emergency situations, the Safety Board expects that OPS will examine documentation of these circumstances to determine if the situations are truly extraordinary. Giving companies information about the risks of fatigue will benefit controllers who already report issues with fatigue. The issuance of this bulletin on August 11, 2005, is a positive step toward reducing fatigue in pipeline controllers. However, the Board is concerned that, despite the issuance of an advisory bulletin, some operators will continue to operate shifts conducive to fatiguing controllers.

[20] The status of this recommendation is Open—Acceptable Response.

[21] The status of this recommendation is Open—Acceptable Response.

[22] National Transportation Safety Board, *Evaluation of U.S. Department of Transportation Efforts in the 1990s to Address Operator Fatigue*, Safety Report NTSB/SR-99/01 (Washington, DC: NTSB, 1999).

[23] RSPA had previously begun a study with Volpe to address fatigue in pipeline operations; however, the Volpe study was discontinued early in the research.

The Safety Board also found that most controllers interviewed expressed concern about the length and rotation of work schedules including their difficulties in getting enough sleep or the fatigue they felt while working night shifts. Despite the large percentage of controllers expressing fatigue issues related to shift work, the effect of this fatigue cannot be ascertained from currently collected accident data. The Safety Board concludes that because the report form used by the Office of Pipeline Safety for companies to report liquid pipeline accidents (PHMSA F 7000-1) does not require operators to provide information about fatigue, such as controller work schedules, it is not possible to empirically determine the contribution of fatigue to pipeline accidents using the Office of Pipeline Safety accident database. Therefore, the Safety Board recommends that the Office of Pipeline Safety change the liquid accident reporting form (PHMSA F 7000-1) and require operators to provide data related to controller fatigue. Possible items to be added to the accident report form could include the time a controller had been on duty, the time a controller had been awake prior to the accident, the detection time of the accident, the time the leak is estimated to have begun, and whether the controller changed from day to night shift (or night to day) in the previous 2 days.

The collection of data about fatigue on a revised hazardous liquid reporting form combined with the research underway to understand human fatigue in pipeline operations being funded by OPS and industry will provide a good estimate of the effects of the fatigue controllers report on the performance of their duties. The issuance of the fatigue bulletin is a good first step to mitigating the effects of fatigue on controllers. The Safety Board will monitor the outcomes of the OPS-funded fatigue research and the outcome the research produces.

Computational Pipeline Monitoring

Improving leak detection was a primary focus of the Safety Board's public hearing on pipeline safety. In the regulations for pipeline integrity management, the OPS requires pipeline operators to take steps to prevent and mitigate the consequences of a pipeline failure that can affect a high consequence area. Operators are required to conduct a risk analysis of pipeline segments to identify additional actions that would enhance public safety or environmental protection. Operators are also required to have a means to detect leaks, evaluate the capability of the leak detection system, and modify it as necessary to protect any high consequence areas. However, the regulations stop short of mandating computer-based leak detection systems[24] in high consequence areas. In the *Pipeline Safety Improvement Act of 2002*, Congress required OPS to conduct research on leak detection systems, emphasizing the detection of small leaks.

Twelve of the twenty-eight pipeline systems that had leaks above 50,000 gallons had no computer-based leak detection in place. For the 16 systems that did have leak detection in place, 6 leaks were first detected by the leak detection system. Third parties detected two leaks on pipelines with leak detection systems and five leaks on pipelines without leak detection.

---

[24] Computer-based leak detection systems include CPM systems and systems that detect the presence of a leak using a sensor that detects a product release and then sends an alarm to the operator.

In the Safety Board's survey of pipeline control centers, 58.5 percent of the companies reported that their SCADA systems included leak detection functions. Of all companies reporting, 37.2 percent had leak detection software embedded in their SCADA systems and 24.4 percent reported that they used a separate leak detection computer program. More than half of these companies reported that they had in the past detected a leak with their leak detection systems.

Although computer-based leak detection systems are not required for all liquid pipelines in the United States, some regulatory agencies have taken that step. In Washington State, following the Bellingham accident,[25] companies were required by State regulation to be able to locate leaks of 8 percent maximum flow within 15 minutes or less. In addition, Canada requires companies to develop and implement pipeline control systems that include "a leak detection system that, for oil pipelines, meets the requirements of CSA Z662[26] and reflects the level of complexity of the pipeline, the pipeline operation and the products transported." Germany also currently requires computerized leak detection on its hazardous liquids pipelines.

One concern with CPM is that the systems are unable to detect small leaks with great accuracy. However, the technology is improving and the ability of current leak detection systems to detect small leaks is currently being studied in congressionally mandated research funded by OPS. Further, CPM systems can be effective in rapidly detecting major pipeline ruptures that require controllers to act quickly to limit the consequences of these spills. The data from the accidents from 2002–2004 show that leak detection systems can be effective in large spills. The Safety Board has also documented accidents in which CPM systems detected spills quickly: Cohasset (3 minutes),[27] Gramercy (3 minutes),[28] Winchester (1 minute),[29] and Bellingham (13 minutes).[30]

The Safety Board also recognizes that "one size fits all" does not work for all pipelines. However, the many CPM methods that exist each have their strengths and weaknesses. The Safety Board concludes that ensuring constant monitoring of an entire pipeline using a computer-based leak detection technology would enhance the controller's ability to detect large spills, increase the likelihood of spill detection, and reduce the response time to large spills. Therefore, the Safety Board recommends that the Office of Pipeline Safety require operators to install computer-based leak detection systems on all lines unless engineering analysis determines that such a system is not necessary.

Therefore, as a result of its study on supervisory control and data acquisition systems used on hazardous liquid pipelines, the National Transportation Safety Board recommends that the Pipeline and Hazardous Materials Safety Administration:

---

[25] National Transportation Safety Board, *Pipeline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999,* Pipeline Accident Report NTSB/PAR-02/02 (Washington, DC: NTSB, 2002).

[26] The regulation appears in Onshore Pipeline Regulations 37(c) 1999. The Canadian Standard Association Z662 addresses oil and gas pipeline regulations in Canada.

[27] National Transportation Safety Board, *Rupture of Enbridge Pipeline and Release of Crude Oil near Cohasset, Minnesota, July 4, 2002,* Pipeline Accident Report NTSB/PAR-04/01 (Washington, DC: NTSB, 2004).

[28] NTSB/PAB-98/01

[29] NTSB/PAB-01/02

[30] NTSB/PAR-02/02

> Require operators of hazardous liquid pipelines to follow the American Petroleum Institute's Recommended Practice 1165 for the use of graphics on the SCADA screens. (P-05-1)
>
> Require pipeline companies to have a policy for the review/audit of alarms. (P-05-2)
>
> Require controller training to include simulator or non-computerized simulations for controller recognition of abnormal operating conditions, in particular, leak events. (P-05-3)
>
> Change the liquid accident reporting form (PHMSA F 7000-1) and require operators to provide data related to controller fatigue. (P-05-4)
>
> Require operators to install computer-based leak detection systems on all lines unless engineering analysis determines that such a system is not necessary. (P-05-5)

Please refer to Safety Recommendations P-05-1 through P-05-5 in your reply. If you need additional information, you may call (202) 314-6177.

Acting Chairman ROSENKER and Members ENGLEMAN CONNERS and HERSMAN concurred in this recommendation.

[Original Signed]

By: Mark V. Rosenker
Acting Chairman