INL/CON-11-22469
PREPRINT

Human Reliability Analysis for Computerized Procedures

Human Factors and Ergonomics Society 55th Annual Meeting

Ronald L. Boring
David I. Gertman
Katya Le Blanc

September 2011

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

HUMAN RELIABILITY ANALYSIS FOR COMPUTERIZED PROCEDURES

Ronald L. Boring, David I. Gertman, and Katya Le Blanc
Idaho National Laboratory, Idaho Falls, ID 83415, USA

This paper provides a characterization of human reliability analysis (HRA) issues for computerized procedures in nuclear power plant control rooms. It is beyond the scope of this paper to propose a new HRA approach or to recommend specific methods or refinements to those methods. Rather, this paper provides a review of HRA as applied to traditional paper-based procedures, followed by a discussion of what specific factors should additionally be considered in HRAs for computerized procedures. Performance shaping factors and failure modes unique to computerized procedures are highlighted. Since there is no definitive guide to HRA for paper-based procedures, this paper also serves to clarify the existing guidance on paper-based procedures before delving into the unique aspects of computerized procedures.

BRIEF INTRODUCTION TO COMPUTERIZED PROCEDURES

Written operating procedures have long been used as a way to support operators in high risk and complex work environments such as aviation, process control, and power generation. In the nuclear power industry, written procedures have been recognized as especially important, because incidents like the Three Mile Island event were made more complex, in part, by inadequate procedures that did not help operators effectively diagnose the situation at the plant. Good written procedures aid operators in many tasks including monitoring, diagnosis, and response planning.

Traditionally, operating procedures are presented in written form on paper. Many challenges have been cited with the use of paper-based procedures (PBPs), including:

- Operators frequently have to manage multiple procedures at one time, potentially leading to navigational difficulties and high cognitive workload associated with keeping track of which procedure the crew is in and where the crew is within the procedure. This situation can be especially challenging for the shift supervisor. (Converse, 1995).
- The sequential presentation of procedures sometimes requires the crew to go through several loops of the procedure before find the correct indications to diagnose the plant status (Fink et al., 2009).
- Keeping place within a procedure has to be done manually, which may increase workload (Fink et al., 2009).
- The information presented in the procedures is static and does not necessarily reflect actual plant conditions (Fink et al., 2009).
- Cautions and warnings may not be applicable to all systems states (Fink et al., 2009; O'Hara et al., 2000).

Advances in digital technology have prompted vendors to consider implementing procedures on computer-based systems, resulting in what is referred to as computerized procedures (CPs). The development of CP systems began in the early 1980s with several simultaneous efforts. Early CP systems include COMPRO (developed by Westinghouse Electric Corporation), COPMA (developed by the Halden Reactor Project), and the computerized procedures for the French N4 reactor design, to name a few.

Depending on the level of CP functionality, a CP system can address the challenges of PBPs in the following ways:

- The CPs can provide navigational links to other necessary procedures, potentially minimizing operator workload when managing multiple procedures.
- CPs can have access to process information, making them sensitive to the context in which they are being used. This can help to ensure that warnings and cautions are always applicable to the current situation.
- The CP can automatically track the path through the procedure, it can automatically mark the current place in the procedure, and it can even alert operators to deviations in the procedure. This reduces the operator's burden associated with place keeping.

In addition to addressing some of the challenges associated with PBPs, CPs can provide enhanced support for operators by:

- Automatically retrieving plant data called out in the procedure.
- Automatically integrating plant information for the operator including automatic processing of procedure step logic.
- Providing links to supplemental information, related procedures, and soft controls.
- Providing embedded process information.
- Automatically executing procedural actions upon operator command.

These enhanced capabilities of CPs, when implemented, are expected to reduce operator workload and improve operator performance when completing procedural tasks in the control room.

Despite these advantages, CPs may fundamentally affect the roles and responsibilities of operators in the control room, which may change the pattern and effectiveness of crew communication and coordination. With PBPs, the unit supervisor typically directs the operators to gather process information specified by the procedure. With CPs, it may be possible for the supervisor to gather that information directly from the CP interface. Eliminating this need may allow the

available operators to perform other important control room functions, but it may also affect the crew's overall awareness of where they are in the procedure.

TECHNOLOGICAL CONSIDERATIONS

Computerized procedures are a new technology in the control room. The change in technology from PBPs to CPs is analogous to other control room modernization efforts in which analog systems are replaced by digital systems. In some cases, the modernization may represent a like-for-like replacement (e.g., replacing an analog annunciator panel with a digital alarm display). In other cases, an enhanced replacement adds additional functionality that was not possible in the previous technology (e.g., replacing an analog annunciator panel with an intelligent alarm filtering system). Note that this distinction not only applies to upgrades of existing main control rooms but also to new plant designs, which may represent the implementation of newer technologies relative to the existing control rooms in the operating fleet of nuclear power plants.

A central goal for phasing in newer technologies is to ensure that a new system is at least as reliable as the system it is replacing. In terms of human reliability analysis (HRA), the goal is to ensure that operator performance using the newer technology is at least as reliable as performance using the older technology. Such a comparison may be made by estimating the human error probabilities (HEPs) of various human activities, including human failure events (HFEs).

The challenge of new technology is that it, in many cases, is newer than the tools used to evaluate it. Such is clearly the case with CPs and HRA. NUREG-1792, *Good Practices for Human Reliability Analysis* (Kolaczkowsi et al., 2005), outlines a variety of HRA methods. Commonly used HRA methods currently in use in the US nuclear industry include: THERP, ASEP, SPAR-H, ATHEANA, HCR/ORE, CBDT, and the EPRI HRA Calculator (which is actually a collection of methods rather than a single method). It is important to note that none of these HRA methods was explicitly designed to deal with CPs. At the present time, these HRA methods have also not provided supplemental guidance to explain how to use these methods to evaluate operator performance with digital systems, including CPs.

Outside the US, there have been two documented efforts to develop HRA methods that support CPs. The first, Method d'Evaluation de la Realisation des Missions Operateur pour la Surete (MERMOS; Le Bot, Cara & Bieder, 1999), is a method developed by Electricité de France (EDF) to address HRA in support of the CPs used in the N4 class of reactors. Originally, EDF used the ASEP method to model operator performance on pre-initiator events and the THERP method on post-initiator events. However, it was determined that these approaches were very driven by a serial, procedural unfolding of events. The N4 CP system diagnosed situations dynamically, resulting in a less serial event progression. As such, the CPs may be viewed as state-based rather than the more traditional event based or symptom oriented procedures. In order to define HFEs that were more dynamic, the MERMOS approach was developed. The MERMOS method uses selection rules that the operators and CPs follow and that can be reconfigured as required, such as when there is a change to plant state requiring a new response. The primary difference between MERMOS and other methods is its heavy emphasis on the dynamic response of the operator, which is triggered by the rapid reconfiguration of the CPs when the plant state changes.

The second approach to HRA for CPs is still under development by the Korea Advanced Institute of Science and Technology (KAIST; Lee, Ha, and Seong, 2010) and does not yet provide a complete method for review.

Since MERMOS is not currently used in the US for nuclear regulatory and licensing applications and since the KAIST method is still under development, it is important to review the current generation of HRA methods for their treatment of PBPs and consider their suitability for CPs.

HRA FOR PAPER-BASED PROCEDURES

Beginning with the earliest HRA method, the Technique for Human Error Rate Prediction (THERP; Swain and Guttman, 1983), HRA methods have to varying degrees addressed procedures. THERP uses procedures in the determination of the nominal HEP. For example, in the screening phase depicted in THERP Table 20-2, procedures are the primary determiner of the HEP. The "failure to perform rule-based actions correctly when written procedures are available and used" is given an HEP of 0.05 per critical step without recovery factors and 0.025 with recovery factors. However, if written procedures are not available or used, the screening HEP goes up to 1.0. In other words, in a conservative screening analysis using THERP, no credit for operator performance is given in rule-based actions by control room personnel after diagnosis of an abnormal event when procedures are unavailable or aren't used.

Procedures also figure prominently in the detailed (non-screening) analysis of THERP:

- Table 20-5, "Estimated HEP per item (or perceptual unit) in preparation of written material"—omitting a step from a procedure or writing an item incorrectly per a procedure, which is clarified to mean errors in the preparation of written procedures.
- Table 20-6, "Estimated HEP related to failure of administrative control"—use of written procedures during normal vs. abnormal operating conditions or use of calibration and maintenance procedures.
- Table 20-7, "Estimated probabilities of errors of omission per item of instruction when use of written procedures is specified"—essentially the entire table is related to the use of written procedures.

THERP also considers procedures as a modifier (essentially a performance shaping factor or PSF). For example, the differential effects of procedures on stress for

skilled and novice operators are accounted for in THERP Table 20-16. Having routine, procedurally guided tasks results in lower overall multipliers applied to the nominal HEP than does performing tasks without procedures in terms of stress.

Many HRA methods that have come after THERP have treated procedures as a type of PSF. These PSFs serve as multipliers to the nominal HEP, typically to increase the HEP when procedures are inadequate. There is considerable variability in how procedures are treated as PSFs across methods. Generally, the quality of the procedures is considered in HRA, although in some methods the procedural adherence by the crew is also considered. A perfectly written procedure will not be effective if it is not followed by the crew. Although crews are heavily trained on procedure following, recent research (Lois et al., 2009) suggests that for any given scenario, there are multiple procedural paths that may be taken by crews in response to a plant upset. Moreover, some responses may not be procedurally driven, especially when there are complex, multiple plant conditions that may make diagnosis difficult.

Generally speaking, current HRA methods address procedures through three broad PSFs:

- Procedural quality,
- Procedural adherence or use (which may fall under work processes in some methods), and/or
- Experience and training to the procedures.

It can be assumed that for most main control room applications, the procedural quality represents a high level of quality. By the time written procedures are implemented across plants, there is a high level of vetting and standardization. In addition, operators are trained on any modifications to procedures, minimizing the adverse effects of procedure versioning. It can also generally be assumed that crews are highly trained on and experienced with written procedures, since regular training is a requirement for reactor operator licensing. Some unusual plant conditions may, however, fall outside the realm of regular training.

The greatest source of performance uncertainty comes not from the procedural quality or the experience and training of the crew but rather in procedural adherence. Issues in procedural adherence may be either intentional or unintentional. Intentional deviation from the procedures is typically not malicious (with the intent to hurt the plant), but rather a case of well-intentioned operator workarounds (such as when skipping ahead in a procedure to resolve an understood plant condition). An unintentional deviation from the procedures is likely a case of a slip or lapse. A slip or lapse is often recovered, such as when the shift supervisor catches a reactor operator's skipped step. Threeway communication serves to help ensure that inadvertent skips are caught immediately. Even so, procedure steps are sometimes skipped, especially when the crew is confronted with multiple simultaneous control room actions and their corresponding procedures.

Based on an expert consensus by the authors, the following list describes the most likely operator errors when using paper-based procedures:

- Skipping a step,
- Misreading or misinterpreting a step,
- Performing steps or substeps in the wrong order,
- Performing steps too early or too late for the plant (timing issues), and
- Going to the wrong procedure.

The likelihood of each of these activities can be accounted for by any of the current quantitative HRA methods. In most cases, these failure modes are not risk significant in isolation. In addition to second checking by fellow crew members, written operating procedures feature some degree of redundancy such as loop-backs. The consequence of a missed procedural step is most likely a delay in diagnosing or correcting the plant upset. For a time-sensitive response, such a delay can significantly impact the ability of the crew to deal with the upset. In the case of intentionally skipping ahead or branching to a different procedure, the danger is that important preparatory steps in responding to the plant may be omitted, which has the potential to make the situation much more complex, especially if the crew has misdiagnosed the upset condition or if there are multiple faults.

HRA FOR COMPUTERIZED PROCEDURES

Performance Shaping Factors

In terms of PSFs, CPs maintain the three fundamental PSFs associated with PBPs: procedural quality, procedural adherence or use, and/or experience and training to the procedures. As with PBPs, in CPs procedural quality is deemed a factor largely negated by the extensive development efforts behind nuclear power plant procedures. Also, as with PBPs, in CPs, experience and training are deemed adequate for all but the most improbable plant upset conditions. Of course, the transition to CPs from PBPs will require additional training to ensure operator fluency with the CP interface. Such training is assumed to have been adequately carried out prior to operator engagement with the CP system in the main control room.

A more challenging issue may be maintaining operator proficiency for backup procedures, especially if those happen to be PBPs. The optimal level and interval of training required by the operator to use PBPs when otherwise accustomed to CPs has not been determined.

Procedural adherence as a PSF may represent an area of improved operator performance, especially if the system maintains a check mechanism to remind the operator when steps have been skipped. CP systems have been developed that color-code procedural steps, such that procedural steps which have been skipped will be highlighted differently than successfully completed steps. This visual reminder of a skipped step can nearly eliminate skipped procedural steps unless the operator reaches an overload condition of having to juggle multiple procedures simultaneously. CPs do not

eliminate the possibility of intentionally skipping ahead. It is possible in most CP systems, for example, for the operator to navigate ahead in the procedures or to force a step out of sequence.

In addition to the PSFs for PBPs, CPs add a number of PSFs, including:

- Communications,
- Workload and situation awareness factors introduced by CPs, and
- Human-System Interface (HSI) quality and usability.

Communications

Anecdotal evidence from CP system developers has suggested that digital control rooms can feature breakdowns in communications due to the so-called keyhole effect. Because information relevant to procedures may be provided to an operator on a local display, the operator may focus attention on individually completing tasks, without using traditional threeway communication with other crew members. Some control room vendors are using large overview displays as a way to enhance operator communication by drawing the center of focus away from the local display to a common point shared by all crew members. In one vendor's control room, operators have been instructed to use a laser pointer to point at the area of the overview display being referenced, in order to ensure a common focal point during threeway communications. Formal studies to understand the effects of CPs on communication patterns and the effectiveness of mitigation strategies have not been published to date.

Workload

Ideally, CPs should decrease operator workload compared to PBPs. This decrease in workload is accomplished by simplifying the process of tracking procedures, by providing relevant information to a particular procedural step embedded in the CP system or on nearby displays, and by automating some basic processes that the operator would otherwise have to carry out manually. Some CP systems may also provide diagnostic aids to the operator, eliminating the complexity of decision making associated with manual calculations, trending, or synthesis of disparate data sources.

CPs may, however, increase operator workload in cases of malfunction. For example, if an indicator connected with the CP gives a wrong reading, the operator may over-rely on that indicator, making recovery more difficult. Similarly, if the CP is misaligned with the current plant state (e.g., a CP system that misdiagnoses the plant upset condition), the operator workload may increase dramatically if the operator is forced to second-guess the system. Such increased workload can be accounted for through information foraging theory (Pirolli, 2009). In a main control room equipped with CPs, the operator may grow used to having relevant plant information pushed to him or her. If the flow of information fails, the operator must transition to an information pull mode, in which he or she must find the relevant indicators amid a myriad of system status indicators. The operator may even need to navigate nested or windowed information displays to find relevant information that would otherwise be buried. The consequence of the transition from information push by the system to operator pull of the information results in dramatically increased workload for the operator. A similar workload transition may occur when resorting to paper-based backup procedures.

Human-System Interface

The ultimate successful use of a CP system depends on the extent to which it has a well-designed HSI that is usable by the operator. Factors to consider in good HSI design are explicated in sources such as NUREG-0700 (US Nuclear Regulatory Commission, 2002). Usability, which goes beyond hardware and software requirements, may be facilitated through an iterative user-centered design process, including human-in-the-loop testing during the CP system development.

In many ways, computerized procedures are a specialized case of advanced HSIs. As such, many of the system and human-system failure modes can be expected to be similar. It is nonetheless incumbent on the human reliability analyst reviewing scenarios involving operator interaction with CPs to include in their review the human performance features for the advanced control room environment of which the CPs are an integral part.

As noted earlier in this paper, special care should be taken regarding the features associated with the HSI for CPs and the ways that the crews communicate. For example, the crew may share overall plant process and status information via a series of centrally located large overview displays. This may comprise one mode of presentation that facilitates communication and active collaboration. Alternatively, smaller displays distributed within the control room may be daisy chained together to support crew communication but may or may not contribute to the same type of situation awareness and collaborative workspace associated with the larger display presentation of plant status information.

Failure Modes

In addition to consideration of CP-specific PSFs, it is necessary to look at the failure modes that are unique to CPs. Four failure modes are of particular interest and generally should be part of the underlying HRA analysis for CPs:

- *Operator failure to transfer to backup procedures.* If there is a catastrophic failure of the CP system (i.e., a system crash), does the operator effectively transfer to backup PBPs or a secondary, redundant CP system? Especially in the case of transition to PBPs, the underlying concept of operation changes, and there may be adverse performance effects.
- *Operator failure under degraded CP functionality.* The CP system may under some circumstances not perform well (e.g., if there are multiple competing faults that require prioritization or when faulty sensor data require additional manual diagnosis of system status). The

operator's ability to step in and use his or her expertise is critical to the successful outcome of such a scenario.

- *Operator failure to recover from operator-induced input errors.* If the operator takes a wrong action in the CP, the operator must have the ability to backtrack. In the case of automated actions, the operator decision may set in place a chain of plant actions. The operator must be able to reverse these effects and resume on the correct path in the CP system.
- *Operator failure to follow CPs*. As with PBPs, it is possible for the operator to perform steps not specified in the procedure or, inadvertently, to skip a step. Unique to CPs is the shared frame of reference for operators sharing CPs. A skipped step can affect the displays of all operators working together on the CP, as the CP system may deliver context displays specific to each step. The result would be missed information and a failure of the CP system to track operator actions properly.

CONCLUSIONS

While CPs solve some of the inherent limitations of traditional PBPs, they introduce new issues that must be carefully considered in HRAs. For safety critical domains like nuclear power plant operations, it is necessary to review the performance of operators using the various systems and tools required for operation. Since its inception, HRA has taken written operating procedures into account. With the advent of computerized procedures, it is necessary to review the assumptions of HRA for procedures and to determine to what extent unique elements must be modeled. This paper has demonstrated how existing HRA methods can be used to perform or review HRAs for CPs.

It must be noted that existing HRA methods used in the US are not designed specifically for CP considerations. The present paper provides insights that enable the analyst or HRA reviewer to generalize existing HRA approaches to CPs. Nonetheless, the differences between CPs and PBPs and, especially, the differences between CPs and other HSI systems, warrant a reconsideration of the methods. Future work will address gaps in the current coverage of HRA methods with respect to CPs and identify future research and development needs for HRA to be optimized to CP applications.

ACKNOWLEDGEMENT AND DISCLAIMERS

The authors wish to thank Dr. Jing Xing of the U.S. Nuclear Regulatory Commission for sponsoring this research. The opinions expressed in this paper are those of the authors and not those of the authors' sponsoring organization. This work of authorship was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately-owned rights.

Idaho National Laboratory is a multi-program laboratory operated by Battelle Energy Alliance LLC, for the United States Department of Energy under Contract DE-AC07-05ID14517.

REFERENCES

Converse, S. (1995). *Evaluation of the Computerized Procedure Manual II (COPMA II), NUREG/CR-6398.* Washington, DC: US Nuclear Regulatory Commission.

Fink, R., Killian, C., Hanes, L., & Naser, J. (2009). Guidelines for the design and implementation of computerized procedures. *Nuclear News, 52*(3), 85-88, 90.

Kolaczkowski, A., Forester, J., Lois, E., & Cooper, S. (2005). *Good Practices for Implementing Human Reliability Analysis (HRA), NUREG-1792.* Washington, DC: US Nuclear Regulatory Commission.

Le Bot, P., Cara, F. & Bieder, C. (1999). A second generation HRA method: What it does and doesn't do. *Proceedings of the American Nuclear Society*, *II*, 852-860.

Lois, E., Dang, V.N., Forester, J., Broberg, H., Massaiu, S., Hildebrandt, M., Braarud, P.Ø., Parry, G., Julius, J., Boring, R., Männistö, I, & Bye, A. (2009). *International HRA Empirical study—Phase 1 Report, Description of Overall Approach and Pilot Phase Results from Comparing HRA methods to Simulator Performance Data, NUREG/IA-0216, Vol. 1.* Washington, DC: US Nuclear Regulatory Commission.

O'Hara, J., Higgins, J. C., Stubler, W. F., & Kramer, J. (2000). *Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance, NUREG/CR-6634.* Washington, DC: US Nuclear Regulatory Commission.

Pirolli, P.L. (2009). *Information Foraging Theory: Adaptive Interaction with Information.* Oxford, UK: Oxford University Press.

Seung, W.L., Ha, J.S., & Seong, P.H. (2010). Development of an HRA Method based on Human Factor Issues for Advanced NPP. In *Proceedings of the Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2010)*.

Swain, A.D., & Guttman, H.E. (1983). *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278*. Washington, DC: US Nuclear Regulatory Commission.

US Nuclear Regulatory Commission. (2002). *Human-System Interface Design Guidelines, NUREG-0700.* Washington, DC: US Nuclear Regulatory Commission.