Dynamic Operations Wayfinding System (DOWS) for Nuclear Power Plants

Ronald L. Boring(✉), Thomas A. Ulrich, and Roger T. Lew

Idaho National Laboratory, Idaho Falls, ID, USA
{ronald.boring, thomas.ulrich, roger.lew}@inl.gov

Abstract. A novel software tool is proposed to aid reactor operators in responding to upset plant conditions. The purpose of the Dynamic Operations Wayfinding System (DOWS) is to diagnose faults, prioritize those faults, identify paths to resolve those faults, and deconflict the optimal path for the operator to follow. The objective of DOWS is to take the guesswork out of the best way to combine procedures to resolve compound faults, mitigate low threshold events, or respond to severe accidents. DOWS represents a uniquely flexible and dynamic computer-based procedure system for operators.

Keywords: Nuclear power plant · Computer-based procedures · Wayfinding · Severe accident

1 Introduction

1.1 Background

We propose a novel software tool to aid reactor operators in responding to upset plant conditions. The proposed Dynamic Operations Wayfinding System (DOWS) effectively serves as a global positioning system (GPS) navigator for the reactor operator to maintain safe plant operations despite emerging or unanticipated plant conditions. Current paper-based procedures are static, and they offer minimal flexibility in responding to plant upsets that occur: (1) below a certain setpoint (e.g., slow leaks), (2) beyond the design basis of the plant (e.g., severe accidents), or (3) in an unanticipated or unexampled manner (e.g., compound events). The operating procedures for all three are underspecified—in the first case, abnormal or emergency operating procedures are not warranted, but the condition falls outside normal operations; in the second case, the severe accident management guidelines are typically very broad and do not offer the operator useful step-by-step guidance in the face of failed systems; in the final case, compound events may force the operator down a procedure path that fails to resolve the most risk significant fault.

1.2 Existing Procedures in Nuclear Power Plants

A crew of nuclear power plant operators follow detailed procedures to cover a variety of plant contexts. These context-dependent procedures include: standard (or normal)

C. Stephanidis (Ed.): HCII 2015 Posters, Part II, CCIS 529, pp. 497–502, 2015.
DOI: 10.1007/978-3-319-21383-5_83

operating procedures (SOPs), abnormal operating procedures (AOPs), emergency operating procedures (EOPs), and severe accident management guidelines (SAMGs). The use of these procedures ranks from frequent for SOPs to extremely rare for SAMGs. The current regulatory framework in the United States means that existing plants exclusively maintain the use of paper-based procedures, while new builds are adopting various forms of computer-based procedures. These computer-based procedures follow a continuum specified in IEEE-Std-1786 [1]:

- *Type 1* procedures simply feature digitized, static versions of the paper-based procedures.
- *Type 2* procedures feature embedded indicators that are displayed as part of the procedures on a screen. Without the embedded procedures, reactor operators have to find indicators across the control boards [2].
- *Type 3* procedures combine the features of Type I and Type II procedures with soft controls. Rather than carry out actions on the plant using physical knobs, switches, and dials on the control boards, the operators can perform those activities with the press of an on-screen button in the procedures.

These three types of computer-based procedures offer significant advances over existing plant operations (while introducing some new types of failure opportunities [3]). However, they tend to follow the same format as the paper-based procedures they replace. In other words, with few exceptions [4], they do not respond or change the procedural path depending on the plant state or emerging circumstances. Perhaps it is appropriate to add a *Type 4* procedure to the existing taxonomy. We posit that a Type 4 procedure is one that adapts in response to changing conditions at the plant. Adaptation without optimization is fruitless. This is the main advantage of DOWS—it optimizes the procedure to allow the operator to respond in the safest and most efficient manner to emerging plant upsets.

2 DOWS Conceptual Overview

2.1 Purpose

The purpose of DOWS is to diagnose faults, prioritize those faults, identify paths to resolve those faults, and deconflict the optimal path for the operator to follow. The objective of DOWS is to take the guesswork out of the best way to combine procedures to resolve the compound faults. Further, the proposed DOWS is dynamic in that it adapts to changing conditions, thus becoming a uniquely flexible yet useful resource for operators. It is hypothesized that DOWS will reduce variability in operational outcomes when responding to changing or inadequately proceduralized events. Such variability has been a cause for considerable concern in prior operator studies (e.g., [5]). Minimizing operator performance variability while maintaining a dynamic response to complex and changing conditions are keys to ensuring DOWS is part of a fault-tolerant and resilient system.

2.2 Navigating a Physical World Map vs. a Procedure

DOWS builds on wayfinding algorithms to calculate dynamically the optimal route for the operator to complete a task. Just as a GPS navigator can accommodate wrong turns and road obstructions to lead the driver to the desired destination, DOWS treats plant conditions and states as constraints, plant risk as the criterion for preferred route selection, and operational goals as destinations. The objective is to craft a route for the operator to complete specific tasks, even if the plant conditions create unique scenarios not anticipated by procedure writers.

The task space for operators following procedures can easily be mapped to the types of environmental primitives used in contemporary wayfinding algorithms in computerized navigation aids. The primitives used in map-based navigation can be cross-walked to procedures as follows:

- *Starting Point → Current Operational Context:* In the physical world, the starting point represents the geographic coordinates where the person is currently. When following procedures, the context is usually an initiating event that triggers a particular procedure. For example, an alarm would trigger a particular AOP. This AOP determines the destination.
- *Destination → Desired End State:* The destination is, of course, the location to which the individual wishes to go. Likewise, any procedural action is designed to build toward a desired end state, typically a restoration of the steady state condition characteristic of the plant's normal operating mode.
- *Path → Procedure:* In the cartographic world, the path marks a route between two points. In nuclear operations, such a path is marked by a procedure that the operators follow in order to change the current state of the plant. A literal path moves through a fixed terrain; a procedure changes the terrain to map the process to the physical characteristics of the plant. Both path and procedure include several attributes.
- *Path Difficulty → Task Complexity:* A navigational algorithm may take attributes of the path into account (e.g., paved vs. unpaved roadway). In an operational context, this can be equated with task complexity—how easy or difficult it is to complete the task specified in the procedure. It is generally desirable to take the easiest procedural path, but other factors may dictate different priorities.
- *Path Length → Procedure Steps:* A short road may take longer than a long road simply due to speed limits. In operational terms, the number of steps of a procedure equates to the path length. Note that the number of steps is not always a good measure of duration, because steps are rarely of equal duration.
- *Path Duration → Time Required:* An important metric for navigational aids is how long it will take to reach the destination. For operations, where critical time windows may factor into the safety of the plant, one of the key measures is the time required to complete the procedure steps.
- *Intersection → Branching Point:* An intersection represents a waypoint along the path, after which an additional navigation route must be considered. For each alternate route, the factors under consideration such as path duration must be calculated to determine the optimal path among alternate routes. For procedure

following, a branching point represents the point at which the operator jumps to a different point in the current procedure or to a different procedure entirely. Rarely are such branching points optional—they are invariably followed if the conditions are met. For the purposes of procedure wayfinding, branching points may represent alternate priorities when confronting compoud faults and can help operators to prioritize optimal routes to follow through multiple, concurrent procedures.

- *Obstruction → System Fault:* An obstruction is an emerging condition (e.g., a traffic jam or detour) that prevents travel along the desired route. An equivalent situation during procedure following would be a sudden system fault that prevents the operator from activating required plant functions or even diagnosing current plant states. Obstructions and system faults require dynamic recalculation to find a new route.

This list is not exhaustive, but it provides a sample of how mapping can occur for both physical environments and procedural paths in reactor operations. It is not necessary to invent new algorithms (although it may be desirable to adopt different wayfinding strategies like simplest rather than shortest path [6]). Rather, it is necessary to translate these characteristics from the plant and the procedures into primitives that can be used to build maps through tasks. A particular facet of mapping these primitives becomes parsing procedural blocks of activities. Rather than take an entire 23-step EOP, for example, as a single path, that EOP should be divided into logical subpaths that can be combined to form an entire procedure. The parsing allows flexibility in the implementation of DOWS.

2.3 DOWS Implementation

The DOWS algorithm queries a variety of data (e.g., existing alarms, state of systems, plant mode, etc.) when predetermined parameters are met and analyzes this information. The output of the system includes the conclusion(s) of the analysis on a display that may include a system overview given at the appropriate level of detail. A context-based procedure with visual aids if needed will be displayed to assist the operator in taking the right action based on the system diagnosed faults. A level of confidence could be provided to the operator based on the algorithm's output. This could be based on data quality and quantity as well as risk significance of the faults. The operator is given the option to take other actions if merited.

DOWS builds on best practices for computer-based procedures (e.g., [1]), including the display of plant states and the use of soft controls. Required data are available to the operator within DOWS to aid in decision-making. Additionally, best features of GPS navigator displays will be incorporated, including the quick selection of goals (destinations), the overview of different paths, the display of information relevant to immediate task and situation awareness, warnings about impending obstacles toward goal completion, and the zoomable view to different levels of information.

3 The Need for DOWS

There is considerable cost in terms of resources to amend existing paper-based procedures to become computer-based procedures. The benefits may not be apparent, especially with the additional complexity of adding primitives to allow the system to navigate optimal paths. We conclude this paper with three distinct examples where the overhead to adapt procedures is quickly outweighed by the advantages afforded by DOWS:

- Idaho National Laboratory has developed a computerized operator support system (COSS) prototype [7] that is capable of early fault diagnosis. The challenge with such diagnosis is that the fault detection is often sufficiently sensitive to anticipate the issue before it has reached the threshold for an alarm. Early diagnosis can mitigate faults before they have an actual consequence on plant operations; yet, currently, the procedures are not written at this level. DOWS enables the system to provide relevant procedural guidance to operators to allow them to respond to the COSS and realize its potential.
- The SAMGs developed for severe accidents are not at the same level of detail as AOPs and EOPs, forcing operators to make many on-the-fly decisions without clear procedural guidance [8]. While severe accidents are extremely rare, operators responding to such an event must overcome severe psychological and physical stress, which do not make ideal companions to complex decision making. DOWS, when properly configured, can serve as an aid to allow operators to navigate the difficulties of severe accidents, prioritize responses, and work step-by-step toward achieving desired end states.
- In compound faults, there is often symptom masking, which makes it difficult for operators to diagnose the root cause of particular faults. For example, a steam line break may mask the symptoms of a co-occurring steam generator tube rupture [5]. Moreover, there may be conflicting indications that result in ambiguity when the operator needs to select the most appropriate procedure. Because procedures must be followed linearly, the operator potentially loses considerable time and minimizes the safety margin when he or she steps through an incorrect procedure. As such, resolving conflicting procedural paths becomes difficult and time-consuming in the prescribed linear process. DOWS can prevent false paths by shortening the number of potentially irrelevant prescripted steps in a procedure and by dynamically recalculating new procedure paths when warranted.

4 Conclusions

This paper has presented initial concepts related to DOWS. DOWS will initially be prototyped on a select number of scenarios and procedures (e.g., steam generator tube rupture masked by a steam line break) in order to establish a proof of concept for the design approach and to optimize the algorithm. A series of operator tests will be conducted to determine the efficacy of the wayfinding algorithm and the quality of the information presentation. An iterative design approach will be employed, refining the interface and algorithm over successive scenarios of increased complexity. The final design should as a result be scalable to other plant systems and will represent a significant, original technological advance to operator performance and overall plant resilience.

5 Disclaimer

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

1. Institute of Electrical and Electronics Engineers: IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities. IEEE Std 1786-2011, New York (2011)
2. Boring, R.L.: Information foraging in nuclear power plant control rooms. In: Proceedings of 2011 European Safety and Reliability (ESREL) Conference: Advances in Safety, Reliability, and Risk Management, pp. 654–660 (2011)
3. Boring, R.L., Gertman, D.I.: Current human reliability analysis methods applied to computerized procedures. In: Joint Probabilistic Safety Assessment and Management and European Safety and Reliability Conference, 16B-Th4-3 (2012)
4. Doutre, J.L., Pirus, D., Ratti, L., Audet, G.: N4 NPP's operation: preliminary tendencies. In: Enlarged Halden Programme Group Meeting, Lillehammer (1998)
5. Forester, J., Dang, V.N., Bye, A., Lois, E., Massaiu, S., Broberg, H., Braarud, P.Ø., Boring, R., Männistö, Liao, H., Julius, J., Parry, G., Nelson, P.: The International HRA Empirical Study: Lessons Learned from Comparing HRA Methods Predictions to HAMMLAB Simulator Data, NUREG-2127, U.S. Nuclear Regulatory Commission (2014)
6. Duckham, M., Kulik, L.: "Simplest" paths: automated route selection for navigation. In: Kuhn, W., Worboys, M.F., Timpf, S. (eds.) COSIT 2003. LNCS, vol. 2825, pp. 169–185. Springer, Heidelberg (2003)
7. Thomas, K., Boring, R., Lew, R., Ulrich, T., Vilim, R.: A computerized operator support system prototype. INL/EXT-13–29651, Idaho National Laboratory (2013)
8. Vayssier, G.: Present day EOPS and SAMG—Where do we go from here? Nuclear Eng. Technol. **44**, 225–236 (2012)