A Tool to Support Improved Outage Risk Management

Shawn St. Germain[a*]
Jaques Hugo[a]
[a] Idaho National Laboratory, Idaho Falls, USA

Abstract: During a nuclear power plant outage, the plant configuration is monitored continuously to ensure that it conforms to the approved safety plan. Deviations must be assessed and approved by management committees and, in some cases, the plant operational review committee. In virtually all outage meetings and job briefings, the current nuclear safety status of the plant is communicated, including information on the specific equipment that is being relied on to meet the requirements of the nuclear safety plan. In addition, Operations and the Outage organizations implement several layers of physical and administrative barriers to prevent unintended interaction with the systems and equipment credited for nuclear safety.
In spite of all these efforts, nuclear safety challenges still occur too frequently in outages. While some of these are due to failures of equipment credited for safety, the majority occur because of human error. These typically involve some form of interaction between work activities and plant configuration changes. Some of them are very subtle and are extremely challenging to detect in advance. Nevertheless, they are not acceptable and represent clear opportunities to improve nuclear safety during outages. This project will develop tools and strategies to minimize these interactions.

Keywords: Outage, Requirements Monitor, Configuration Management.

1. INTRODUCTION

Outage risk is currently managed primarily by relying on the scheduling of work within work windows that align with plant conditions that support these windows. There are various requirements that govern what work is allowed to be performed in these work windows.
Ensuring that the plant is continuously compliant with changing requirements while efficiently executing required work continues to challenge outage and operations staff. Better tools for managing the large amount of data associated with maintaining plant conditions within requirements should help reduce errors in configuration management and reduce costs. This paper describes a proposed tool under development at the Idaho National Laboratory (INL) to make key outage parameters and requirements more visible and to automatically detect undesired interactions between upcoming work activities and current requirements.

2. CURRENT OUTAGE RISK MANAGEMENT

Outage risk is currently managed primarily by relying on the scheduling of work within work windows that align with plant conditions that support these windows. There are various requirements that govern what work is allowed to be performed in these work windows.
Ensuring that the plant is continuously compliant with changing requirements while efficiently executing required work continues to challenge outage and operations staff. Better tools for managing the large amount of data associated with maintaining plant conditions within requirements should help reduce errors in configuration management and reduce costs.

To help understand the nature of the challenges facing outage managers and operations supervisors tasked with approving work, a review of Licensee Event Reports (LERs) was conducted [1]. LERs submitted from 2010 through 2015 for events that occurred during shutdown reactor conditions were reviewed. Of these LERs, 248 were identified as being related to an outage execution issue while the other 173 LERs were written during shutdown conditions for issues not related to outage execution

*Shawn.StGermain@INL.Gov

and were ignored. Of the 248 LERs written related to outage execution, 113 were identified as being reasonably preventable and further evaluated. Table 1 lists the most common high level causes identified in these events, the total is more than 113 since some events have more than one identified cause.

Table 1. Shutdown LER Causes.

High Level Cause	Number of LERs noted
Configuration Control	26
Inadequate Procedures/ Procedure Use	66
Mode Change Issues	13
Poor Work Practices	11
Component Verification or Manipulation	6
Clearance Order Issues	5

The primary source of requirements comes from the plant's technical specifications. These technical specifications detail the required safety systems and support systems that must be operable for various plant conditions, known as Limiting Conditions for Operation (LCO). Technical Specifications are required by and are part of the plant's operating license. The LCOs outline the maximum allowed out-of-service time for various plant modes for certain safety equipment.

Another important source of requirements comes from the Shutdown Safety Plan. These Shutdown Safety Plan requirements typically come from a probabilistic risk assessment (PRA). The plant's PRA will calculate a shutdown risk level based on plant conditions and current defense-in-depth. The shutdown PRA model may be able to identify risks involved with work on multiple systems concurrently that may be overlooked if only the plant technical specifications were used. In order to maintain an adequate level of plant safety (low level of plant risk), trains of safety systems or support systems are protected to ensure the desired risk level is maintained. These protected systems are documented in a shutdown safety plan and plants will typically use visual indicators in the plant to alert personnel when they are approaching protected equipment.

Additional requirements may also come from a Mode Change Checklist. Prior to mode change, the new set of requirements that will become active are generally documented in some form of mode change checklist. The most common is the Mode 4 checklist that outlines the required systems that must be operable as well as surveillance tests that must be documented prior to entering mode 4 during plant start-up. Operations personnel typically have lists of equipment that require post maintenance testing that must be completed during the plant start-up before the plant reaches certain operational milestones such at primary coolant temperature or steam pressure.

There are several sources of information that need to be monitored to ensure compliance with the various requirements that may be in place. Work orders are the primary means of controlling the execution of work during an outage. Work orders are created before the outage and include required plant conditions, precautions and limitation and the actual work instructions. Work orders are typically placed in the schedule to match the prerequisites to the expected plant conditions. One finding during the LER review of operating experience was that issues commonly arise when work orders are modified and the impact of the changes are not fully verified against the position of the work in the schedule.

Clearance orders are used to provide protection for workers and equipment during maintenance from high energy fluids, electrical shock, or flooding. The boundaries for a clearance order may extend well beyond the actual area of work to ensure proper protection. There are numerous examples in the operating experience review where a clearance order isolated a system or portion of a system that was needed for decay heat removal at the time it was issued. Other problems arise when still active clearance orders disable a system needed for mode change during start-up.

Surveillance procedures provide guidance for the testing and inspection of plant systems and components. Similar to work orders, surveillance procedures contain prerequisites, precautions and limitations that should be met prior to starting the procedure. Surveillance procedures also need to be carefully scheduled to ensure compliance with requirements. One possible complication that sometimes arises during surveillance testing is the unintended automatic actuation of systems if plant conditions are not consistent with those required by the test or if equipment is not properly aligned to perform the test. Plant operating procedures will also direct the manipulation of components that should be monitored to understand possibly complex system interactions.

The plant computer could also provide useful information for determining the status of key systems requiring monitoring during an outage. The plant computer may have parameter information related to valve position information, pump information or system flow information that could either validate that a particular system in in operation or detect that a system may be out of service.

3. OUTAGE SYSTEM STATUS AND REQUIREMENTS MONITOR (OSSREM)

3.1. Situation Awareness and Information Visualization

As indicated before, a number of requirements govern what work may be performed in the different outage work windows. These requirements include, for example, LCOs that specify the maximum allowed out-of-service time for various plant modes for certain safety equipment, and the shutdown risk level based on plant conditions and current defense in depth. However, as shown in many LERs, nuclear safety challenges still occur during outages. These may be due to failure of safety equipment, but the majority occur because of human error. These typically involve work activities and plant configuration changes. Since plant configuration changes may be subtle and difficult to detect in advance, it is important to develop strategies and information tools to increase situation awareness for all plant personnel.

Situation awareness involves a person's ability to perceive the environment, to comprehend its meaning, and to project that understanding into the future to anticipate what might happen. This applies not only to operational situations, but also to the requirements for optimal outage performance. Optimal situation awareness requires knowledge of, for example, current outage performance parameters and the normal value of those parameters, the difference between current values and normal values, the past state of an activity, and its predicted future state. Situation awareness is maximized by integration of this information, and is thus critical when the Outage Control Center (OCC) team members are confronted by a complex and changing situation. It is directly related to individual worker and joint team performance, and is especially important during abnormal conditions (e.g., emergent conditions such as equipment damage, leaks, releases, etc.) when personnel are required to identify situations and problems not covered by normal procedures, make correct diagnoses of faults, and decide on a path forward.
The need to optimize situation awareness and reduce risk implies that all critical outage performance measures should be designed to support the execution of activities and the

management of associated risks. In addition, this means that any associated information must be accessible in a way that not only supports all three levels of awareness, but also enables personnel to take appropriate action. Failure to communicate this information effectively is likely to undermine outage performance and also increase the risk probability.

Research has shown that the way in which information about the dynamic environment is represented in a person's mental model plays a significant role in anticipation of certain events, and thus also affects a conscious attention and search for information. There is also common agreement that the work situation in complex industrial environments is characterized by high information content, which, if not managed properly, may contribute to excessive mental workload, and hence worker error. Because of the unique cognitive and perceptual requirements posed by the complex information generated during outages, the design of effective information displays requires an understanding of human factors in general, and visual communication in particular. This involves an analysis of the nature, role, and composition of the discrete components of the visual elements of displays. This is a necessary element in the analysis of situation awareness, due to the very nature of the processes of representation, communication and interpretation of information in all work domains. In fact, the semantic content of information artifacts in the OCC is so high that it should be treated as a complex, hierarchical architecture of meanings, expectations, targets, values, and measures.

Well-designed visual displays of information are generally beneficial to situation awareness and therefore to communication and overall outage performance [2]. However, the entire weight of responsibility for the success or failure of information displays does not fall on display technology alone. Designers of the information and the communication medium must thoroughly understand the work domain. They should understand that workers have already constructed a mental model of the domain into which the available information will be rapidly integrated. This implies that they possess a level of knowledge and expertise that often allows them to infer intended meaning from incomplete information. However, incomplete and inaccurate information introduces a level of uncertainty and risk, because workers' expertise cannot compensate for the failure of a display to present information in a way that matches their individual or collective mental model.

Previous analyses of communication patterns in OCCs have demonstrated that more information is not necessarily better for optimal performance [3]. Too much information can cause "cognitive clutter" and may interfere with effective response and appropriate mitigation. Methods of providing information to OCC team members are still very simplistic because they rely primarily on presenting raw data that does not exploit the potential of effective visual communication. Additionally, there is much more data available that is not typically evaluated, because methods have not yet been developed to process and integrate this information into something meaningful.

We need to understand how the display of OCC information is related to the total context of the outage and associated activities and emergent risks, that is, how does the individual worker and the team as a whole decide where to focus their attention, whether regarding the external world (the plant) or regarding their own interior world (mental model)? We also need to know what contributes to the perceptual salience of the information in various contexts. How does displayed information modify the worker's internal mental organization and subsequent action? Measures of optimal situation awareness therefore need to include an analysis of the actual information that the OCC members deal with: location, type, duration (transience), frequency (repetition), structure, format, accuracy, origin, etc. [4].

Ultimately, a visual analytic approach to the design of outage risk management information will support the cognitive-semantic aspects of the analysis and design of information displays. A coherent taxonomy or framework of structured representations would provide a practical way to ensure consistency and coherence in the display architecture. It should thus be possible to ascertain with a greater degree of accuracy and confidence why, how and when certain display configurations promote and others inhibit situation awareness, and thus awareness of risks.

It can thus be concluded that, rather than relying on computer systems alone to alert plant staff to undesired interactions, humans will remain the primary means of controlling work within existing requirements. However, visualization tools like outage risk information dashboards can assist staff in maintaining awareness of ever-changing conditions and requirements, for example, the status of critical plant equipment, including reactor protection system, equipment cooling systems, residual heat removal, emergency diesel generators, etc.

3.2. Text Mining

A large amount of power plant operational information resides in a relatively unstructured textual form in diverse types of documents. This information is typically impenetrable to automated processing. Operating procedures typically contain sections documenting precautions and limitations for procedure use and initial conditions. However, there may be additional equipment impacts that are not obvious by simply reading the front matter of the procedures. Supervisors approving work rely heavily on the schedule and the description of the work to ensure that the procedure would be authorized at a particular time.

Computational techniques that include text mining and text analytics have been developed in recent years to discover and present knowledge – facts, business rules, and relationships – embedded in a variety of written sources. A specialized area of text mining called natural language processing may be useful for extracting information from sources that have a nearly regular structure.

Revealing information from procedures and other documents through text mining may provide another layer of protection from undesired interactions by automatically detecting component manipulations that may not be in alignment with requirements at that moment.

Text mining may thus be an important tool for identifying plant impacts from procedures or work orders that need to be performed during an outage. The underlying principle is that computational techniques will be used to comb through procedures and work orders to identify equipment manipulations that will affect shutdown risk. The basic process will be to process procedures and work orders to create correlations between action verbs and equipment part numbers (EPNs) associated with plant equipment that is to be monitored by the system. The system could either process a procedure or work order on demand by the work approver or setup to automatically process work orders based on the outage schedule of upcoming work. Table 2 lists some example action verbs that may be relevant for detecting component manipulations.

Table 2: Action Verbs for Automated Document Evaluation

Affected Item/SSC	Related Action Verbs	
Valves	Open	Close
	Ensure Open	Ensure Closed
	Check position	Throttle
	Stroke	Inspect
Pumps	Stop	Start

	Check	Inspect
Motor	Stop Check	Start Inspect
Instrument/Display	Calibrate Monitor	Read Inspect
Control	Actuate Align Maneuver Manipulate Press Rotate	Adjust Close Move Open Release Turn
Tools	Use Inset Turn	Select Remove Move
Procedure	Calculate Close Complete Direct Enter Inspect Manipulate Measure Move Obtain Perform Read Release Review Shift Stop	Check Compare Declare Ensure Initiate Install Mark Monitor Notify Open Press Record Remove Rotate Start Write

3.3. System Status Monitor

Current risk monitors do not typically provide real-time information on actual plant configuration and system status during outages. A preliminary investigation has identified a number of key parameters that could contribute significantly to the ability to understand the risks associated with changing conditions during an outage. Making these parameters and requirements visible in real-time would enable all personnel involved to anticipate and prepare for the configuration changes and requirements during plant evolutions.

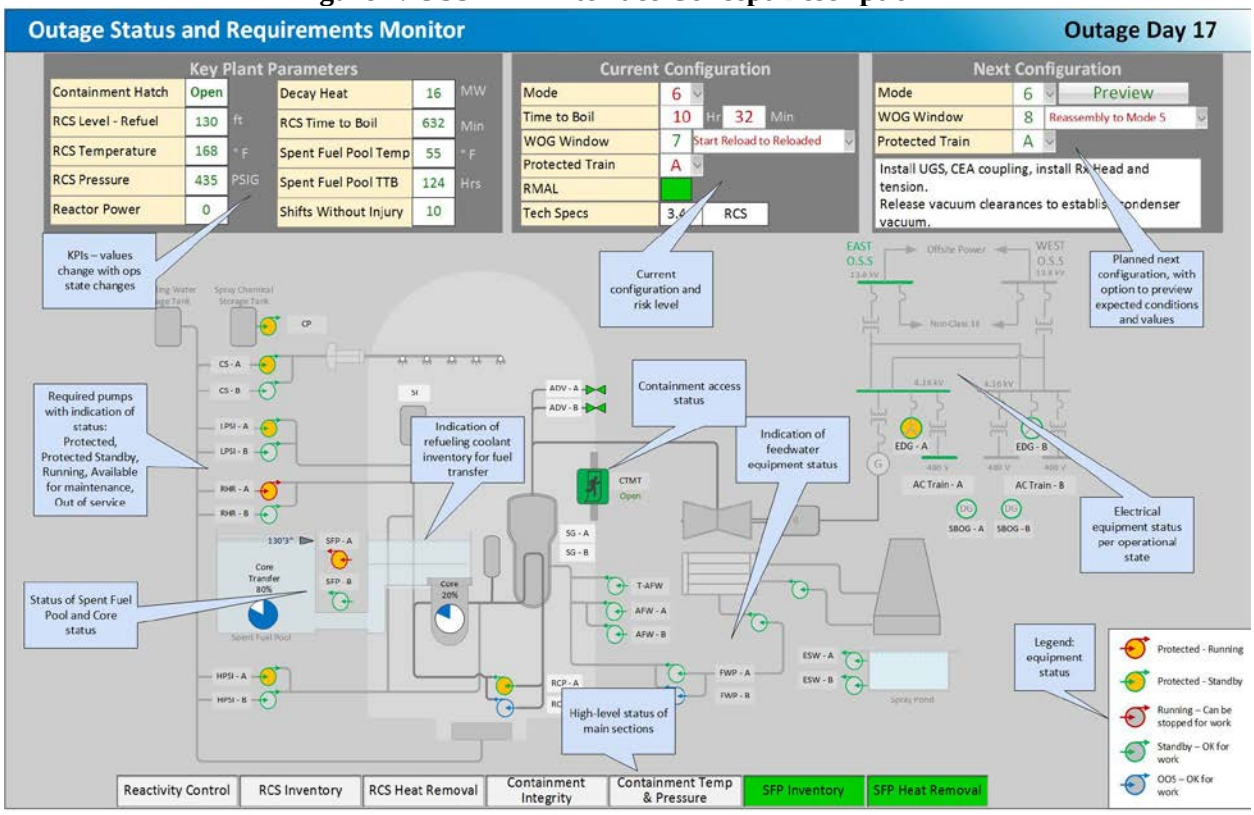
The Outage System Status and Requirements Monitor (OSSREM) contains the following information sections:

1. Key Plant Parameters. This includes the status of key systems and the overall plant condition during Modes 1 through 6, for example, reactor power, containment status, reactor coolant system, decay heat, spent fuel pool temperature and level, etc.

2. Current plant configuration. Critical parameters displayed in this section include the current mode, Risk Management Action Level (RMAL), bulk coolant Time to Boil, Protected Train, outage work window, etc.
3. Next Configuration. This section of the display provides a prospective indication of the requirements for the next phase of the evolution, or work window.
4. Finally, the display includes a simplified plant mimic diagram that indicates the status of the key systems during the outage, specific modes, and specific work windows. System status is indicated by means of symbols for systems and trains that are in the following conditions:
    - Protected and running
    - Protected and in standby
    - Running but not protected, which means systems that can be stopped for maintenance
    - Standby and available for maintenance
    - Out of service

Figure 1 shows the design layout of the Outage Status and Requirements Monitor (OSSREM). The annotations provide a brief explanation of the content and intention of portions of the display. The software also includes a database to track current actual status, current required status and the future required status of monitored components and systems. The display will light up similar to an alarm display to alert staff when requirements are not or would not be met for future configurations. The software will be able to consolidate data from numerous sources related to plant configuration including the plant computer, clearance order database, work management system and procedures.

Figure 1: OSSREM Interface Concept Description



4. CONCLUSION

While current methods of outage risk management have so far prevented any serious outage related accident, a review of LERs and industry events suggests there is still room for improvement. Looking at the causes of these outage related events, is appears that plants still struggle with maintaining plant conditions within technical specification requirements. Some of the weaknesses are related to configuration management and issues with procedures, particularly following procedure revisions. It appears that recent advances in data processing and analytics may provide a technology solution to provide a backup to plant operators in ensuring plant work is in compliance with requirements. A combination of data visualization, natural language text mining and logic models could be employed to develop an advanced requirements monitor to support outage operations. Future work will involve further developing a prototype requirements monitor to test various technological aspects to determine the suitability and real time accuracy of such a system.

References

[1] S. St. Germain, J. Hugo, M. Manic and K. Amarasinghe. "*Technologies for Detecting Interactions between Current Plant Configurations States and Component Manipulations Directed by In-Use Procedures*", INL/EXT-17-43234, Idaho National Laboratory: Idaho Falls, ID (2017).

[2] S. St. Germain and J. Hugo. "*Development of an Overview Display to Allow Advanced Outage Control Center Management to Quickly Evaluate Outage Status"*, INL/EXT-16-39622, Idaho National Laboratory: Idaho Falls, ID (2016.

[3] S. St. Germain, R. Farris, A. Whaley, H. Medema and D. Gertman. "*Guidelines for Implementation of an Advanced Outage Control Center to Improve Outage Coordination, Problem Resolution, and Outage Risk Management"*, INL/EXT-14-33182, Idaho National Laboratory: Idaho Falls, ID (2014).

[4] J. Hugo "*The Semiotics of Control Room Situation Awareness"*, In *Thatcher, A., J. James, & A. Todd (Eds.), CybErg 2005* (pp. 1–14). Johannesburg, South Africa: International Ergonomics Association Press. (2005)