EPRI

Development of a Risk Monitor for Assessing Plant Trips

Technical Report

This project was co-sponsored by the U.S. Department of Energy and the Electric Power Research Institute

Development of a Risk Monitor for Assessing Plant Trips

1003117

Final Report, April 2002

Cosponsor
U. S. Department of Energy

EPRI Project Manager
F. Rahn

EPRI • 3412 Hillview Avenue, Palo Alto, California 94304 • PO Box 10412, Palo Alto, California 94303 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

Data Systems and Solutions
ABS Consulting
Scientech

ORDERING INFORMATION

Requests for copies of this report should be directed to EPRI Orders and Conferences, 1355 Willow Way, Suite 278, Concord, CA 94520, (800) 313-3774, press 2 or internally x5379, (925) 609-9169, (925) 609-1310 (fax).

CITATIONS

This report was prepared by

Data Systems and Solutions
4920 El Camino Real
Los Altos, CA 94022

Principal Investigator
K. Canavan

ABS Consulting
300 Commerce Drive, Suite 200
Irving, CA 92602

Principal Investigator
J. Liming

Scientech
11140 Rockville Pike, Suite 500
Rockville, MD 20852

Principal Investigator
T. Morgan

This report describes research sponsored by EPRI and the U. S. Department of Energy under the Nuclear Energy Plant Optimization (NEPO) Program.

The report is a corporate document that should be cited in the literature in the following manner:

Development of a Risk Monitor for Assessing Plant Trips, EPRI, Palo Alto, CA, and U. S. Department of Energy, Washington, D.C.: 2002. 1003117.

REPORT SUMMARY

The probability of losing all off-site power is an important input to many nuclear power plant safety assessments. Reliable off-site power is one key to minimizing the probability of severe accidents. This report describes a tool for reducing effects of off-site power loss during periods when the transmission grid is heavily loaded or unstable due to adverse effects such as weather.

Background

Utilities and the U.S. Department of Energy (DOE) have been concerned about transmission grid security under a deregulated environment, and a joint EPRI/DOE project has been initiated under the Nuclear Energy Plant Optimization (NEPO) program. This project will increase nuclear plant safety and protect the transmission grid from further instabilities—caused when a nuclear unit might be forced off-line due to grid voltage problems—by

- developing a risk monitor tool to help transmission system managers make decisions involving low-reserve margins, shortage of transmission facilities, and technical problems transmitting power over long lines
- providing 'return-to-service' priorities to restore system margins or determine which assets to protect to prevent system margin erosion.

The goal is for nuclear plants to use local grid reliability information to evaluate their safety. In return, grid operators can evaluate the grid's security by obtaining the probability that a nuclear plant will trip off line. A pilot application will be demonstrated at a nuclear unit in a region of the country experiencing grid congestion.

Objective

To provide nuclear utilities with a means of assessing the risk of a plant trip due to equipment configuration or off-site events such as transmission grid instability.

Approach

Essentially, all trip monitor applications are associated with the "when" of performing proposed maintenance activities that can increase the potential for a plant trip or derate. The current generation of risk monitors applies a similar concept associated with when and how maintenance activities are performed. For risk monitors, the risk associated with maintenance activities is evaluated and potentially reduced through control of the maintenance schedule. For trip monitors, the "when" associated with the performance of proposed maintenance activities has both an economic as well as a safety consideration.

Results

The report describes how to use one of two tools—EOOS (a module of the Risk and Reliability Workstation) or Safety Monitor—to develop a trip monitor. Improvements in safety are achieved through averting or lowering the potential for an initiating event. Elements of safety also are improved through better maintenance scheduling. When considering improvements in safety, the trip monitor is used in a fashion similar to the various risk monitors employed throughout the nuclear industry.

EPRI Perspective

This report was requested by NEPO's program advisors. The application or purpose of trip monitors is to reduce the potential for unplanned reactor scrams or derates. Reducing unplanned reactor scrams or derates is important for a variety of reasons, including

- safety improvements
- grid stability
- economic issues.

Due to growing competition in electrical generation and distribution, grid stability is increasingly important to safety as well as plant economics. Understanding and controlling the potential for an unplanned reactor scram or derate can increase grid stability and lower the potential for loss of off-site power or other grid-disturbing events.

Keywords

Trip monitor
Loss of off-site power
Risk analysis
Safety analysis

ABSTRACT

The report describes how to use one of two tools—EOOS (a module of the Risk and Reliability Workstation) or Safety Monitor—to develop a trip monitor. Improvements in safety are achieved through averting or lowering the potential for an initiating event. Elements of safety also are improved through better maintenance scheduling. When considering improvements in safety, a trip monitor is used in a fashion similar to the various risk monitors employed throughout the nuclear industry.

CONTENTS

1 INTRODUCTION

This report presents the lessons learned and experience from the development and use of trip monitors. For the purposes of this paper a trip monitor is defined as a tool used to estimate the likelihood of an unplanned plant scram or significant power derate. In overview, several important lesson have been learned:

- Current model development tools (e.g., EOOS, Safety Monitor, CAFTA, NUPRA, KB3, etc.) are sufficient for the development of a trip monitor. The challenge is the development of site specific model.
- A challenge in building the site specific model is balancing the need for modeling various balance of plant systems against the resources required to develop and maintain the trip monitor. That is, choosing the right level of modeling detail.
- Reliability and failure data traditionally used in the development of Probabilistic Risk Assessments (PRAs) are generally not applicable to trip monitors. Experience has shown that traditional reliability or failure data is conservative when used to evaluate the normally running systems that can impact trip frequency. The traditional data has been shown to produce higher failure or unavailability values than reflected in actual plant experience.
- The rare event approximation used in the development of traditional PRA fault trees may not be applicable in the development of trip monitors. Since trip monitors are actually producing a frequency value, the calculated value can exceed a value of unity (1). While issues with the use of the rare event approximation are particularly relevant when top event *probabilities* are being calculated, the impact of this approximation for top event *frequency* trees needs to be considered. Care needs to be exercised in the techniques used to model and quantify the resulting trip/derate model.
- Trip monitor results are usually dominated by single failures as opposed to the redundant nature of the systems and resulting accident sequences associated with a traditional Level 1 PRA.
- Unlike core damage models, the outcome of a trip/derate model could quite possibly be TRUE when certain plant configurations are input to the trip monitor. The software must accommodate such situations and provide results meaningful to the user.
- The implementation of a trip/derate model at a power plant may require the collection and tracking of data (including system configuration information) that may not be readily available. Because many of the power generation systems are not considered important to safety, maintenance and operations actions on these systems are often not tracked to the same level of detail applied to safety systems. So, a plant planning to implement such a monitoring tool must consider what additional data may need to be obtained and what methods will be used to obtain this data.

- At least one plant has undertaken the development and implementation of a trip monitor to, in part, assess the economics associated with plant scram and derate risk.

The report is divided into several sections. Each section provides important details with regard to the lessons learned and experience.

2 APPLICATION

The application or purpose of the trip monitor is to reduce the potential for unplanned reactor scrams or derates. The reduction in unplanned reactor scrams or derates is important for a variety of reasons. These reasons include:

- Improvements in safety,
- Grid stability,
- Economic issues.

Improvements in safety are achieved through averting or lowering the probability of the potential for an initiating event. Elements of safety are also improved through improved maintenance[1] scheduling. When considering improvements in safety, the trip monitor is employed in a similar fashion as to the various risk monitors employed throughout the nuclear industry.

In an age of increasing competition in the electrical generation and distribution, grid stability is increasingly important to safety as well as plant economics. Understanding and controlling the potential for and unplanned reactor scram or derate, can increase grid stability and lower the potential for loss of offsite power or other grid disturbance events.

Lastly, the control of the potential of an unplanned reactor scram or derate, allows for consideration of the economics associated with electric power production in the planning of maintenance activities. That is, the potential for an unplanned reactor scram or derate can be lowered in periods where production is essential for the reliability of the grid and times of peak electric power prices. It should be noted that for grid stability and economic considerations apply to both the nuclear and fossil generating stations.

Essentially all the various applications of a trip monitor are associated with the "when" of performing proposed maintenance activities that can result in an increased potential for a plant trip or derate. The current generation of risk monitors apply a similar concept associated with when and how maintenance activities are performed. In the case of risk monitors, the risk associated with the maintenance activities is evaluated, and potentially, reduced through control of the maintenance schedule. In the case of the trip monitor, the "when" associated with the performance of proposed maintenance activities has both an economic as well as a safety consideration.

[1] The term "maintenance" and "maintenance activity" is used throughout this report. This term is meant to apply in broadly and also refers to surveillance and operational activities that can increase the potential for reactor trip or derate.

In summary, the trip monitor assists in answering the question as to when to perform maintenance activities that have an increased potential to result in a plant trip or derate. In addition, as the trip monitor matures in it development and application, the trip monitor also assists in the determination of when maintenance is required on equipment (through evaluation of collected data). That is, maintenance optimization. The trip monitor and maintenance optimization is performed not only for safety considerations but economic considerations as well.

3
TOOLS

A variety of tools are available for the development and maintenance of trip monitors. These tools include the current class of risk monitor software packages such as EOOS and Safety Monitor as well as others. The tools available also impact the methods used in the development of the trip monitor. There are several methods available for the development of trip monitors. These methods include the use of:

- Fault trees
- Event trees
- Reliability block diagrams (RBDs)
- GO models

Combinations of the above can also be employed for the development of trip monitors. Recent experience has used methodology associated with the construction of fault trees. Therefore, this paper presents the lesson learned and experience with regard to this approach. This is not to discourage the use of alternatives or imply that these alternatives are less effective.

4 MODELING REQUIREMENTS

There are several available methods or approaches that can be used in the development of a trip monitor. Each method or approach has a different set of requirements. The most common method used in the development of a trip monitor is phased approach. In the phased approach the complexity and therefore, the modeling requirements, varies with the phase. In a three phase approach:

- The first phase trip monitor is useful in general resource planning and prioritization for addressing plant trip and power reduction issues at a power station, and for prioritizing resource allocation and technical focus of follow-on trip monitor development phases. In this phase, the trip monitor could be primarily based on coarse data from industry generic information sources (i.e., NERC-GADS, INPO EPIX/NPRDS, etc.).
- In the second phase, a reliability logic model such as an event tree, fault tree, or reliability block diagram would be developed for the trip monitor. In this phase, the trip monitor could be used to support broad-based decision-making relative to system-level issues associated with major maintenance or design change management. In this phase, the trip monitor would primarily employ generic data, but could be supplemented with some high-level plant-specific system failure and recovery data.
- In the third and final phase of trip monitor development, the phase 2 system-level logic models would be expanded down to the component (i.e., tag number) level of detail. Also, the trip monitor model input data would be developed at the plant-specific component failure mode level of detail. A Bayesian update process would be employed to develop and continuously update component failure mode failure frequency, exposure, and recovery time data. This phase 3 trip monitor could be employed to address the full spectrum of plant asset management issues.

As with all modeling of complicated processes, the level of modeling is driven by the anticipated needs of the end-user balanced against the available resources. The modeling complexity and requirements are therefore driven by the end-user.

It is important to note that, as the level of modeling complexity increases, the end uses of the model and its accuracy also improve. However, the increasing trip monitor complexity also results in an increase in the resources required to build and maintain the trip monitor.

This report section compares and contrasts the modeling requirements associated with a traditional Level 1 PRA and the modeling requirements of the phase 3 trip monitor. The major differences can be summarized as follows:

- System Analysis Scope

- Modeling Detail
- Data Requirements
- Plant Alignments

The following report sub-sections describe the differences between a traditional PRA and a trip monitor.

a. System Analysis Scope

The differences in system analysis scope arise from the different endstates of the studies. In the case of a traditional Level 1 PRA, the endstate is core damage frequency. In the trip monitor case, the endstate is a reactor scram or derate. The differences in endstate necessitate the modeling of different systems with different success criteria.

As an example, the differences in system analysis scope include the requirement to develop of detailed models associated with balance of plant (BOP) systems. These additional systems analyses are generally limited to balance of plant systems and can include system such as the main condenser, steam jet air ejector, turbine trip and bypass and other similar systems. In general, these BOP systems are modeled in varying detail based on their project contributions to the plant trip frequency or megawatts lost.

In addition to the additional systems analyses that must be developed, may of the Level 1 PRA systems that can be used require significant changes to the success criteria for their successful use in the trip monitor. The changes to success criteria include changes such as requiring all feedwater and condensate pumps as opposed to a single pump post trip. In addition, other changes such as requirements for feedwater heating also changing in success criteria and importance.

b. System Model Detail

The system modeling detail of a trip monitor versus a traditional PRA also differs. Attention to the level of detail in the trip monitor must be considered with respect to availability of data as well as considerations with regard to the maintenance that can or might be performed during normal power operations.

If a phased approach is adopted in the development of the trip monitor, the initial system models of the trip monitor may be relatively simple. However, these simple initial models will also reduce the applications and insights available from the trip monitor.

In later phases of the trip monitor development, the system model level of detail will increase. Phase 3 trip monitor models are developed relatively consistent with the level of detail found in the typical Level 1 PRA.

c. Data Requirements

As in the case with the system analysis scope and the system analysis detail, the data requirements will vary depending on the anticipated uses of the trip monitor. If a phased approach is taken to the development of the trip monitor, phase 1 will use relatively generic data from sources such as NERC-GADS, INPO EPIX and/ or INPO NPRDS as well as others.

In the phase 2 models some generic data would be replaced by plant specific experience. The plant specific experience would generally be limited to those pieces of equipment that have experienced or are experiencing operational issues or those that have been shown to significantly impact the trip or derate frequency.

In phase 3 of the trip monitor development, extensive use of plant experience is required. New methods or processes for the collection of data are generally required since only primitive means are generally currently available for the collection of data on many balance of plant systems and components.

d. Plant Alignments

During normal plant operation, the plant alignments can vary significantly. These plant alignments vary from power source arrangements to support system cooling water sources. Even simple plant alignment changes can significantly affect the reactor trip or derate frequency as well as the core damage frequency.

In the early phases of the trip monitor development only the most significant plant alignments or configurations are modeled. Generally, these plant configurations are determined using the Level 1 PRA model to determine those plant configurations that are risk significant.

In phase 2 of the trip monitor developed, additional plant alignments are added based on judgment as to which alignments could significantly impact the trip or derate frequency.

In phase 3, the trip monitor adds additional plant alignments and configurations to ensure that most of the normal plant operational alignments are available within the trip monitor.

5
REQUIRED RESOURCES

For a power plant to implement a trip monitor, various resources must be available to support the project. These resources must consider both the model development as well as implementation of the completed model in the plant. The resources to be considered are discussed in this section.

a. Model Development Phase

Depending upon the approach used to develop the trip monitor (i.e., develop a model in a phased approach, develop a model completely as one project, etc.), the level of effort from the plant's PSA group and any consulting support could range from 4 to 6 man-months of effort up to several man-years for a complete detailed model with a detailed basic event mapping database. In addition to the base level of support from the PSA organization and consultant, the needs for resources from other plant organizations are discussed below.

As noted above, the first step of the process is the determination of the objectives of the planned trip monitor. The determination of those objectives should include input from plant management, as well as representatives of operations, maintenance, and perhaps, system engineering. The overall amount of time required from each group is relatively small, but it is important that a consensus on expectations be reached early in the project. Also, the need for support from groups outside the PSA & Reliability groups should be clearly understood by the decision makers, so that access to the required resources will be available when needed.

If plant trip history is to be reviewed, then access to historical records (including possibly NERC GADS data) will be needed. Limited support from plant staff familiar with those records may be required to extract the required information in an efficient manner.

In order to develop the necessary system models, access to system design and operations information will be needed. This will include drawings, systems descriptions, procedures, etc. Note that for systems outside the power block (e.g., the switchyard), some additional effort might be required to obtain this information beyond that normally assumed for a modeling project.

Access to systems engineers and operations staff will be required, on a consulting basis, during model construction. This support should require less than a man-week each from these two groups, unless extensive review sessions are to be performed.

Plant personnel that are experienced with plant operation (but not necessarily having a detailed knowledge of PSA) can perform the review of plant maintenance and operating procedures. The effort to perform such a review will depend upon how the procedures are stored and categorized, and whether the procedures already contain some guidance as to the trip potential of the operations that are performed. This effort can require anywhere from several man-weeks to several man-months, depending upon the above factors.

A final review of the trip model should be conducted with key operations staff members (and possibly, members of system engineering and maintenance planning). This review session might require one or two days and involve several plant personnel (i.e., one to two man-weeks of total personnel effort).

b. Trip Monitor Implementation Phase

The extent of additional effort, if any, to implement a trip/power reduction model will be somewhat plant-dependent. If the same software interface is used for both the core damage and trip models (e.g., by using EOOS or Safety Monitor), then most of the input required for the trip model would be obtained in a similar manner as is required the existing core damage model. If a separate software package is used for the trip model, then some inputs may have to be duplicated to support both the safety and generation risk monitoring functions.

The addition of system models for various primary and secondary systems might introduce the need for additional system alignments to be modeled. If any such alignment options are added, then additional information must be tracked by the plant staff (and included in automated input files from scheduling programs and control room log software) in order to properly reflect the impacts of alignment changes in the calculated risk.

If the impacts of performing trip-sensitive actions near plant equipment is to be included (e.g., as an environmental/testing factor), then a process may need to be developed to track and input this information to the trip monitor. The trip-sensitive items may include operating procedures, which are performed on an as-needed basis, rather than according to a fixed schedule (as is usually true of maintenance and testing procedures). The performance of these procedures might not be currently recorded (e.g., in a control room log) on a consistent basis. Also, it may not be possible to evaluate the impacts of those operating procedures on a proposed future work schedule.

In summary, the resources required to implement the trip monitor are not expected to be large, but proper implementation may require the cooperation of several plant groups, and may require some changes in the way that information is collected and stored.

6 CASE STUDIES

Two case studies on the development of trip monitors are presented in the following report sub-sections. The purpose of these report sub-section is to present an overview of the issues associated with the development of trip monitors at specific sites. These issues may not be experienced by an utility developing a trip monitor and are presented for information only.

a. San Onofre Trip Monitor

San Onofre has implemented an initial version of a trip monitor, using a modified version of the Safety Monitor™ software. The initial model is currently in trial use by plant staff, and additional model/data enhancements are being considered for implementation in early 2002.

In developing its trip monitor, plant staff particularly wanted a tool that would help them to identify how day-to-day plant activities might affect trip or power reduction risk. As such, the model was intended to focus on intersystem dependencies, human actions, and possible system alignments that affect risk. Component hardware failures were included in the model. However, it was recognized that the risk posed by many of these failures, particularly single component failures, was "constant" from a day-to-day perspective and relatively unaffected by ongoing plant operations. For example, the plant must reduce power if one of the four circulating water pumps fails to operate. So, this risk is present at all times and will not increase or decrease over time. However, the presence of maintenance or operations staff performing work near the pumps could contribute to an inadvertent trip of a pump, even if the work being performed was not directly expected to cause an impact on the pump(s).

The existing master fault tree (top logic) model was expanded to include an additional consequence (trip/derate) and the Safety Monitor™ software was modified to process and display the additional information, including features such as important operable components, restoration advice, schedule evaluation, etc. It was decided to define the top event of the trip model as those events that would result in a plant trip or a power reduction of greater than 10% within three minutes of the event occurrence. Hence, failures that could either not be averted by human action, or would require extremely rapid human response were selected for initial evaluation.

Project activities proceeded in parallel in three main areas:

1. Identification of those systems whose failures could result in the top event, and subsequent modeling of those systems.

2. Review of plant trip/power reduction history (as well as the history of sister plants) to determine historical frequencies. Also, an initial component failure database and HEP library were also determined.

3. Screening of relevant plant operating and maintenance procedures to determine those with trip-critical impacts. This list of procedures was then reviewed with operations staff.

The resulting model included seventeen plant systems (both BOP and various primary systems such as RCS, CCW, ESFAS, RPS, etc.). In those cases where existing fault tree models existed from the core damage PSA, these models were expanded to support the trip/derate function. All other systems had new fault trees developed, but in a modularized format.

About 120 plant procedures were identified as being trip-sensitive, and environmental/testing factors were developed for each new procedure. An initial mapping of the model's basic events to major plant components was also developed. (More detailed mapping will be conducted in 2002.)

The resulting model was then quantified in the Safety Monitor™ under various plant configurations and the component failure rates and HEPs were adjusted empirically to "calibrate" the model to match historical trip/derate data. (More formal data analysis is planned for 2002.)

The resulting trip monitor package has been in trial use at San Onofre since the fall of 2001, and initial feedback from plant staff has been positive. The initial model is being used in an advisory capacity, recognizing that the model will undergo continued enhancement over the coming months. In the meantime, feedback from plant staff (both concerning model assumptions/data, and suggestions for additional features) is being collected to address in the next phase of model/software development.

Enhancements to the models/data expected to be performed in 2002 include:

- Additional modeling of several systems, including the switchyard.
- Sub-division of a number of the trip-sensitive procedure steps to reflect the specific actions being taken during certain evolutions, particularly for the operating procedures.
- Additional review of model assumptions and success criteria with cognizant system engineers.
- More comprehensive mapping of the model to plant equipment, particularly for support equipment for the major components.
- Additional work in the areas of component failure data and human reliability data.

b. South Texas Project

The STP Nuclear Operating Company (STPNOC) has developed a "balance-of-plant" (BOP) availability model for its South Texas Project Electric Generating Station (STPEGS).

This model consists of a detailed fault tree model coded in the SAPHIRE computer program, and Balance-of-Plant Performance Predictor (BOPPP). The BOPPP software is designed to perform component failure mode level input data (i.e., frequency, exposure, and recovery time) Bayesian updating, and to produce unit, system, and component-level availability performance measure predictions (i.e., for unit trip frequency, MWH loss, and other key availability parameters). The BOPPP software is based on common, simple relational database and spreadsheet analysis tools. The projected trip frequency is categorized by probabilistic safety assessment (PSA) initiating event category code, so that BOP model results can be applied within the PSA.

Also, STPNOC has developed spreadsheet-based BOP Risk Assessment Calculator (RAsCal) software to support BOP configuration risk management at STPEGS. This software, similar to its reactor safety RAsCal software for safety configuration risk management at STPEGS, tracks projected reactor trip and MWH loss profiles based on actual historical and planned equipment configurations at the plant resulting from planned and unplanned maintenance, testing, inspection, etc.

The BOP RAsCal tool is applied by station operators to assist in planning and managing upcoming equipment maintenance and other key plant evolutions, based on maintaining projected reactor trip and MWH loss levels within specified instantaneous and cumulative limits. The overall goal is to optimize plant safety, reliability, efficiency, and costs to support maximizing long-term profitability.

To better support long-term profitability decision-making at STPEGS, STPNOC is currently developing a risk-informed asset management (RIAM) software tool for the station. This software accepts PSA, BOPPP, and other station evaluation output data as its input data, and then calculates projected station financial performance measures and investment option evaluation metrics to support and promote prudent change management processes at STPEGS, all with the ultimate goal of maximizing long-term profitability.

Target:
Nuclear Power

About EPRI

EPRI creates science and technology solutions for the global energy and energy services industry. U.S. electric utilities established the Electric Power Research Institute in 1973 as a nonprofit research consortium for the benefit of utility members, their customers, and society. Now known simply as EPRI, the company provides a wide range of innovative products and services to more than 1000 energy-related organizations in 40 countries. EPRI's multidisciplinary team of scientists and engineers draws on a worldwide network of technical and business expertise to help solve today's toughest energy and environmental problems.

EPRI. Electrify the World

Printed on recycled paper in the United States of America

1003117

EPRI • 3412 Hillview Avenue, Palo Alto, California 94304 • PO Box 10412, Palo Alto, California 94303 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com