

# Turbine Overspeed Trip Modernization

## Requirements and Implementation Guidance

*Technical Report*

---

Effective December 6, 2006, this report has been made publicly available in accordance with Section 734.3(b)(3) and published in accordance with Section 734.7 of the U.S. Export Administration Regulations. As a result of this publication, this report is subject to only copyright protection and does not require any license agreement from EPRI. This notice supersedes the export control restrictions and any proprietary licensed material notices embedded in the document prior to publication.



# **Turbine Overspeed Trip Modernization**

Requirements and Implementation Guidance

**1013461**

Final Report, November 2006

EPRI Project Manager  
R. Torok

## **DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES**

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

**MPR Associates, Inc.**

## **NOTE**

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail [askepri@epri.com](mailto:askepri@epri.com).

Electric Power Research Institute and EPRI are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2006 Electric Power Research Institute, Inc. All rights reserved.

# CITATIONS

---

This report was prepared by

MPR Associates, Inc.  
320 King Street  
Alexandria, VA 22314

Principal Investigators

D. Mandel  
H. Giesecke  
D. Herrell  
P. Aerts

This report describes research sponsored by the Electric Power Research Institute (EPRI).

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

*Turbine Overspeed Trip Modernization: Requirements and Implementation Guidance*, EPRI, Palo Alto, CA: 2006. 1013461.



# REPORT SUMMARY

---

This report provides guidance for power plant engineers contemplating modernization of their main turbine overspeed trip systems. When a large power plant turbine suddenly loses its output shaft loading due to a generator or power grid problem, the steam flow driving the turbine must be cut off very quickly to prevent an overspeed event. The overspeed trip system protects personnel and plant systems by preventing missiles that can result when turbines disintegrate at higher than normal rotational speeds. It also protects against financial losses of an extended outage and premature turbine replacement. Most power plants still use mechanical systems with moving weights and springs to detect overspeed conditions and initiate steam shutoff. These systems are now obsolete, and updated systems offer significant performance and maintenance improvements. This report explores key technical issues and decisions that should be considered in planning and implementing an updated turbine overspeed trip system.

## Results & Findings

Replacing a mechanical overspeed trip system with a modern digital system can eliminate many operational and maintenance problems associated with mechanical systems and also can improve safety and reduce the risk of damage from overspeed events. Turbine manufacturers and insurers are updating their policies accordingly. To ensure high dependability of the new systems, plants may have to update their processes, procedures, and expertise to properly evaluate and apply the new technology.

## Challenges & Objective(s)

Power plant engineers need to properly manage the aging and obsolescence of turbine instrumentation and control equipment to maintain the safety and operability of the plant. In this case, they need the tools and knowledge to make the transition from obsolete mechanical system technology to updated digital technology in such a way that they realize the benefits and avoid potential pitfalls. Digital technology is relatively new to turbine engineers who maintain mechanical overspeed trip systems, and it can be far more complex in some ways, with potential for new failure modes and unintended functions. Questions also arise in regard to potential insurance implications and manufacturer warranties and recommendations. The objective of this report is to help plant engineers recognize and address pertinent issues and make the important decisions that will arise in planning and implementing a turbine overspeed system upgrade.

## Applications, Values & Use

This report does not attempt to make turbine engineers experts in digital technology, but it will make them aware of key issues and areas where they may need to seek expert help. It also will help them determine important requirements of the new systems, assess merits of various vendor design approaches, and understand utility responsibilities in operating and maintaining the new systems. The report focuses to some extent on nuclear power plant issues, but the guidance can

be applied to any turbine-driven large rotating machinery, including steam-driven feedpumps, safety injection turbines, combustion turbines, and diesel engines. This document also provides guidelines for eliminating the mechanical overspeed trip, thereby reducing the mechanical maintenance burden and the potential for serious damage when testing the overspeed trip system. The guidelines are consistent with the approach taken in current installations by major turbine vendors. This document does not provide all the requirements needed to specify a replacement system; it focuses on those features and capabilities needed to achieve specific improvements and ensure high dependability.

## **EPRI Perspective**

Turbine overspeed trip protection is a clear example of an application where upgrading to digital technology can have clear benefits in improving safety and reliability while reducing maintenance costs. Insurance company data suggest that about half of recent turbine losses occurred during testing of mechanical overspeed trip systems at elevated turbine speeds; digital systems can be tested without overspeeding the turbine, eliminating this risk altogether. Digital systems have better setpoint accuracy as well as hardware fault tolerance and automated diagnostics to increase reliability and reduce the maintenance burden.

Turbine overspeed protection also is a clear example of an application where consequences of a failure can be catastrophic, so users should take great care to properly specify requirements, evaluate products, apply administrative procedures, and maintain configuration control. These are all areas in which power plant engineers will have to be proficient as the industry migrates from obsolete analog technology to modern digital systems. EPRI anticipates that this guideline on modernizing turbine overspeed trip systems will help utilities make the most informed decisions possible as they move forward.

## **Approach**

The project team's goal was to provide practical guidance that will help utilities address specific questions that concern turbine overspeed trip modernization. An EPRI technical advisory group comprised of utility representatives guided the development of the report, and turbine manufacturers and insurers were consulted to ensure that the resulting guidance would be useful and practical.

## **Keywords**

Instrumentation and control  
I&C modernization  
Turbine overspeed trip  
Turbine control



# ABSTRACT

---

The turbine overspeed trip system is designed to stop admitting steam into a turbine when the turbine control system has failed to maintain speed control. While nuclear plants do not classify this system as “safety-related,” the system plays an important role in the plant, protecting both personnel and reactor systems from the missiles that can result when turbines disintegrate at higher than normal rotational speeds. The turbine overspeed trip should prevent loss of turbine speed control from creating significant overspeed events. However, failures of this system have resulted in several damaged or destroyed turbines in the last decade. In addition, insurance data suggests that overspeed system testing caused 50% of the recent turbine losses.

This document explores the technical issues and potential design requirements for modernizing existing mechanical overspeed trip systems. This document also provides guidelines for eliminating the mechanical overspeed trip, thereby reducing the mechanical maintenance burden and the potential for serious damage when testing the overspeed trip system. There is a small increase in electronic maintenance burden, but overall the replacement simplifies testing and provides diagnostics and fault indications. These features reduce the risks inherent with undetected failures and simplify periodic surveillance. The guidelines are consistent with the approach taken in current installations by major turbine vendors.

This report focuses to some extent on nuclear power plants, but the guidance can be applied to any turbine-driven large rotating machinery equipment, including steam driven feedpumps, safety injection turbines, combustion turbines, and diesel engines.

The overspeed trip system guidelines provided in this document are not specific to any particular vendor instrumentation and control or information system architecture. Certain features are easier to implement with a modern software-based monitoring and control system. This document does not provide all the requirements needed to specify a replacement completely, but primarily focuses on those features and capabilities needed to achieve specific improvements to the existing system designs.



# ACKNOWLEDGMENTS

---

A number of utility turbine experts volunteered to participate in a technical advisory group that helped define the industry needs, focus the guideline development effort, and provide comments on drafts:

Randy Bunt	Southern Company
Mitch Burress	TVA
Russell Chetwynd	Southern California Edison Company
Bob Garver	FirstEnergy
Howard Hoffman	Ameren
David Kerr	FirstEnergy
Tom Kordick	Ameren
Kevin Purkey	Southern Company
Philip Schuchter	FirstEnergy
James Wieters	SCANA

The authors also wish to acknowledge the following industry experts who contributed their insights and perspectives on the topic:

Melvyn Cavanagh	Alstom
Terry Cooper	FM Global
Robert Frater	Siemens
Jim Lewis	CMS Energy
Tom McCaskill	Nuclear Electric Insurance Limited (NEIL)
Daniel Rothas	Siemens Westinghouse Power Corporation
Joe Wood	GE Energy



# CONTENTS

---

<b>1 INTRODUCTION .....</b>	<b>1-1</b>
1.1 Turbine Overspeed Danger.....	1-1
1.2 Report Objective.....	1-2
<b>2 TURBINE CONTROL AND PROTECTION SYSTEMS.....</b>	<b>2-1</b>
2.1 Turbine Control System.....	2-1
2.1.1 Speed Sensing .....	2-3
2.1.2 Modulating Valve Control .....	2-3
2.2 Turbine Overspeed Protection Systems.....	2-4
2.2.1 Mechanical Overspeed Protection.....	2-4
2.2.2 Electronic Overspeed Protection .....	2-4
2.2.3 Stop Valve Interface .....	2-5
2.3 Operator Backup .....	2-6
<b>3 ISSUES WITH THE EXISTING SYSTEM.....</b>	<b>3-1</b>
3.1 Issues with Mechanical Overspeed Trips.....	3-1
3.2 Modernizing the Mechanical Trip System .....	3-2
<b>4 MODERNIZING THE MECHANICAL SYSTEM .....</b>	<b>4-1</b>
4.1 System Quality and Dependability .....	4-1
4.1.1 Better Protection by Removal of Hazards .....	4-1
4.1.2 Better Protection by Improved Reliability.....	4-2
4.1.3 Better Protection by Improved Safety.....	4-2
4.1.4 Better Protection by Redundancy.....	4-3
4.1.5 Better Protection through Better Control .....	4-4
4.1.6 Better Protection by Avoiding Part Obsolescence .....	4-4
4.2 FMEA-Based Design.....	4-5

---

<b>5 SYSTEM SURVEILLANCE AND TESTING</b>	<b>5-1</b>
5.1 Features Required for Surveillance and Test	5-1
5.2 System Test	5-2
5.2.1 Partial System Test	5-2
5.2.2 Periodic Complete Overspeed Test	5-4
5.3 Test Frequency	5-5
<b>6 OTHER PERSPECTIVES</b>	<b>6-1</b>
6.1 Insurer Perspective	6-1
6.2 Turbine OEM Perspective	6-2
<b>7 SUMMARY AND CONCLUSIONS</b>	<b>7-1</b>
7.1 Summary	7-1
7.2 Conclusions	7-3
<b>A REFERENCES</b>	<b>A-1</b>

## LIST OF FIGURES

---

Figure 2-1 Speed Control Loop.....	2-2
Figure 2-2 Overspeed Monitoring Configuration.....	2-5





## LIST OF TABLES

---

Table 4-1 Target Failure Measures for a Continuous Mode of Operation System.....	4-3
Table 7-1 Summary of Turbine Overspeed Issues .....	7-1



# 1

## INTRODUCTION

---

### 1.1 Turbine Overspeed Danger

A steam turbine rotor is designed for the mechanical stresses associated with rotating speeds in a specified operational range. Because centripetal force varies with the square of the rotational speed<sup>1</sup>, stresses increase rapidly with increasing speed. Above the operational speed range, stresses will exceed the strength of the mechanical connection between the turbine blades and the rotor hub. When blades break, centripetal force will often throw the blades through the turbine housing. The resulting missile is a serious safety hazard that can cause significant damage.

In addition to serious damage, the resulting missiles may damage safety systems. General Design Criterion (GDC) 4 of 10 CFR 50 Appendix A requires that “structures, systems and components important to safety shall... [be] appropriately protected against the effects of missiles, pipe whipping, and discharging fluids that may result from equipment failures...” In November 1991, the Salem Unit 2 turbine failure demonstrated that missiles, explosions, fire, and flooding can occur, as documented in NUREG-1275 (Reference 1). The loss of generator seals allowed hydrogen to escape from the generator, and resulted in a hydrogen explosion. The lubrication oil system was breached, resulting in fires that extended deeply into the building. The resulting fire suppression placed large quantities of water throughout the plant. Failure to maintain the turbine overspeed trip system in a fully operable condition resulted in the system being unable to protect the turbine and generator. The NUREG documents how a combination of mechanical component failure, surveillance testing that did not reveal the failures of redundant components, inadequate maintenance, design issues with the solenoid valves and the hydraulic fluids, human error, and poor human interface design led to the overspeed event.

The costs of such a failure can be huge. The associated losses on a large steam turbine, combined with the value of the lost power generation have been estimated at well over \$100 million. Clearly, reducing the likelihood of an uncontrolled and catastrophic overspeed event is essential.

One of the recommendations from NUREG-1275 (Reference 1) is that plant owners not disable any of the redundant overspeed trip systems during testing. If portions of the redundant overspeed system are disabled and the portion under test fails, the probability of an actual overspeed event and loss of the turbine and generator is likely unacceptably high.

---

<sup>1</sup> ( $F_{\text{centripetal}} = m\omega^2 r$ ) where “m” is the mass of the object, “ $\omega$ ” is the rotating speed, and “r” is the radius of its rotational path. As the turbine size increases, the blades increase in length, and thus the centripetal force increases as well, by the square of the rotating speed.

Vendors have developed several systems to regulate, monitor, and limit the speed of the turbine and to reduce the probability of uncontrolled and catastrophic overspeed. These systems rapidly shut down (trip) the turbine by isolating the turbine from all steam sources in the case of uncontrollable or excessive overspeed. The most severe overspeed condition occurs when the generator is disconnected from the grid. This load loss is usually sudden, requiring the overspeed trip system to react rapidly, since the primary force holding the turbine at normal operating speed comes from the electromagnetic fields in the generator, which is providing electricity to the grid. Once the grid is lost, the generator stops holding the turbine at grid frequency and the generator speed increases rapidly. Turbine generators have time constants in the 0.2 to 6 second range.

Two types of overspeed detection and shutdown systems are common: mechanical and electronic. Many facilities rely largely on mechanical overspeed protection systems because electronic systems were unreliable at the time of facility construction. However, mechanical overspeed systems are no longer a necessity as a backup for electronic trip failures. As the digital age has progressed, the quality and reliability of electronic systems have increased significantly thanks to increasingly reliable digital logic, well-written software, and component redundancy. In addition, a significant number of mechanical overspeed trip failures (such as that at the Salem Nuclear Generating Station in November 1991) and the growing maintenance burden for increasingly outdated mechanical systems are causing many utilities to consider modernizing their plant to rely solely on a state-of-the-art digital electronic protection system.

This issue is not only a problem for nuclear power stations, but affects all large high-speed turbine users for which overspeed represents a significant loss of equipment and power production, such as the fossil fuels industries of coal, petroleum and natural gas.

## **1.2 Report Objective**

This report seeks to answer the question: “What can be done about the increasingly antiquated and undesirable mechanical overspeed trip systems?” It first examines why mechanical overspeed trip systems are problematic and potentially hazardous to safe plant operation. A brief discussion of the operation of the turbine control and protection systems sheds light on the systems at issue. Next, the report explores some of the issues and questions that accompany removal of the mechanical overspeed trip, including ways to ensure equivalent or better levels of protection when modernizing overspeed systems through use of improved reliability, redundancy, and test procedures. Finally, this report discusses the recommendations of turbine vendors for current installations, and includes the perspective of companies that insure high-speed turbine operation.

# 2

## TURBINE CONTROL AND PROTECTION SYSTEMS

---

Steam turbines are not only equipped with control systems to govern speed under normal operation, but also with various protection systems that are designed to prevent dangerous events. Included in the protection systems is an overspeed trip protection system that is designed to isolate the turbine steam supply and thus allow the turbine to coast to a halt in the case of overspeed. The design of the protection systems focuses on “single failure criteria,” meaning that in the case of a single failure in the protection system the turbine is still protected and able to shut down safely.

### 2.1 Turbine Control System

The primary function of the control system is to manage normal operation of the steam turbine. The turbine control system, a closed control loop, is the first line of defense against turbine overspeed since a well designed, properly operating turbine control system will accurately maintain the turbine’s speed and prevent it from overspeeding when transients occur, even after the total loss of the generator load.

Most large nuclear power generating plants in the U.S. were built with analog Electro-Hydraulic Control (EHC) systems. With the evolution of modern turbine control systems, some plants have replaced the analog technology with digital versions. Digital EHC systems use microprocessors and software to perform closed loop control.

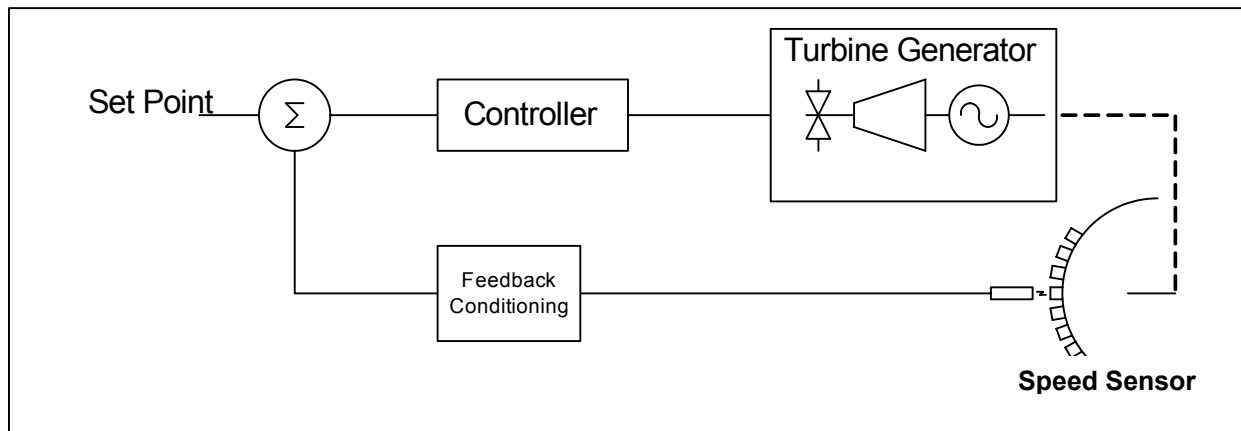
The latest digital EHC systems make use of redundant processors to control the high-pressure hydraulics that drive the valves that regulate steam flow through the turbine. The level of redundancy (double or triple) implemented in the final delivered design is usually dictated by the plant risk avoidance requirements and the choice of vendor.

The EHC system supports power production by controlling the amount of steam admitted to the turbine. The EHC system controls the turbine at each step, from starting and checking the process permissive conditions, through synchronizing the generator to the grid, to delivering the power to the electrical grid. In order to start and synchronize the turbine to the grid, the system controls the initial admission of steam to the turbine to heat the turbine to normal operating temperature. The system then starts (rolls) the turbine spinning, slowly speeds the turbine up to grid frequency, and provides correction signals to adjust the amount of steam to the turbine through the control valves. Once the turbine speed matches the grid frequency and the operator ties the generator to the power grid, grid frequency controls turbine speed. The EHC then manages steam flow to the turbine to maintain the plant generation and power factor set by the operator.

If the generator disconnects unexpectedly from the grid, the steam flow that was generating prime moving power will accelerate the turbine rapidly, since there is no remaining load to balance the turbine's rotating torque. This is known as load rejection, and steam stored in the system will accelerate the turbine above synchronous speed. However, to avoid reaching the overspeed trip setpoint (typically ~110% of rated speed), the turbine control system and control valves need to react rapidly to keep the turbine from accelerating significantly beyond its operational range. The overspeed protection system provides additional safeguards should the normal control system be unable to prevent the sudden speed increase, using a different set of steam stop valves. Failure to control turbine generator speed can result from electronic or software failures in the control system, mechanical failure of any of the control valves, or electronic or mechanical failure in the control valve positioning equipment.

The overspeed protection system is independent of the normal speed control loop. The following sections briefly discuss the normal speed control system. The overspeed protection system is addressed later, in Section 2.2.

Figure 2-1 below illustrates the basic configuration of a speed control loop, specifically an electronic speed control loop.



**Figure 2-1**  
**Speed Control Loop**

The controller, the turbine/generator, and the speed feedback signal make up the main components of a speed control system. The controller computes the difference between the demanded speed value and the actual speed. The difference value, computed and conditioned by the controller, commands the valves to adjust steam flow to the prime mover to increase or decrease the speed of the turbine as necessary to maintain the set point speed.

Sections 2.1.1 and 2.1.2 discuss important components of a speed control system.

### **2.1.1 Speed Sensing**

Speed sensing provides the controller with the actual rotor speed that it needs in order to regulate the speed and correctly control the machine. Typically, a toothed wheel mounted to the rotor and a probe form the basic mechanism for establishing a count. A passive probe of magnetic material will have a constant flux in one medium (e.g. air) and a different flux when exposed to iron. The teeth of the turning wheel are made of iron, and the variation in magnetic flux as the teeth move past the probe induces a voltage in the sensor. The change in depth caused by the shape of the tooth (i.e., the depth of the cuts in the iron) on the wheel determines the shape of the voltage waveform. A conditioning circuit transforms the voltage waveform into a signal that the controller measures. As the rotor spins, the speed sensor uses pulses or counts per unit time to compute revolutions per minute.

A passive speed sensor does not require supporting power. An active probe requires auxiliary power applied to it to emit an electrical signal. The signal can be returned to the control system as either a voltage (using a constant current source to the probe), or a current (using a constant voltage source to the probe). The rest of the processing is similar to that of a passive probe. Generally, passive sensors are preferred because operating without auxiliary power means easier setup and maintenance, as well as a smaller chance of probe failure.

The selection of a speed sensor requires careful examination of different characteristics. The sensor conversion circuit depends on the voltage output and shape of the speed signal. These two factors in turn depend on many factors, including the type of sensor, the mounting distance between sensor and gear, the gear tooth material, the ambient magnetic fields, and the electrical load of the cable and sensor conversion circuit.

An analog electronic controller can convert the raw speed sensor pulse signal into a voltage that is compared to a setpoint to decide whether to trip or not trip the turbine. A digital electronic controller converts the same speed signal into a digital value, representing RPM that is compared to a setpoint to decide whether to trip or not trip the turbine.

Use of multiple sensors and controllers running in parallel and voting on the trip decision can offer increased reliability and availability. The control system can sample more than one speed sensor, and crosscheck to detect failed sensors, or perform various types of calculations, both in analog and digital format.

### **2.1.2 Modulating Valve Control**

Several valves control the flow of steam entering the different pressure stages of a turbine. Usually, each steam inlet has a modulating valve used by the control system to adjust the amount of steam to the turbine. This controls the energy fed into the turbine and effectively controls speed when running free, and power when connected to the grid. Electro-hydraulic servo actuators control the turbine modulating valves. Each actuator positions itself based on the signal received from the EHC. This allows the correct amount of steam to pass through and maintains the turbine speed or power at its desired value.

## **2.2 Turbine Overspeed Protection Systems**

The turbine manufacturer's recommendations are the basis for determining the speed at which a turbine should trip. Plant operating guidelines may provide additional conservatism. Generally, the more power driving the turbine, the less margin exists between normal speed and the overspeed limit. When an overspeed condition occurs, the overspeed protection system rapidly shuts the turbine down by sending a trip signal to close the stop valves (see Section 0 below) and cut the steam to the turbine, removing the rotating force and allowing it to gradually come to a halt. Additionally, valves between the Low Pressure (LP) turbine and the Moisture Separator Reheater (MSR) will also close to remove that steam energy path as well, since there could be sufficient stored energy in the MSR to overspeed the turbine upon loss of load.

The overspeed trip system is one of the protection systems provided for a turbine. In most currently operating nuclear plants, a mechanical overspeed protection system is the final line of defense for overspeed events. The next two sections compare the mechanical and electronic overspeed systems.

### **2.2.1 Mechanical Overspeed Protection**

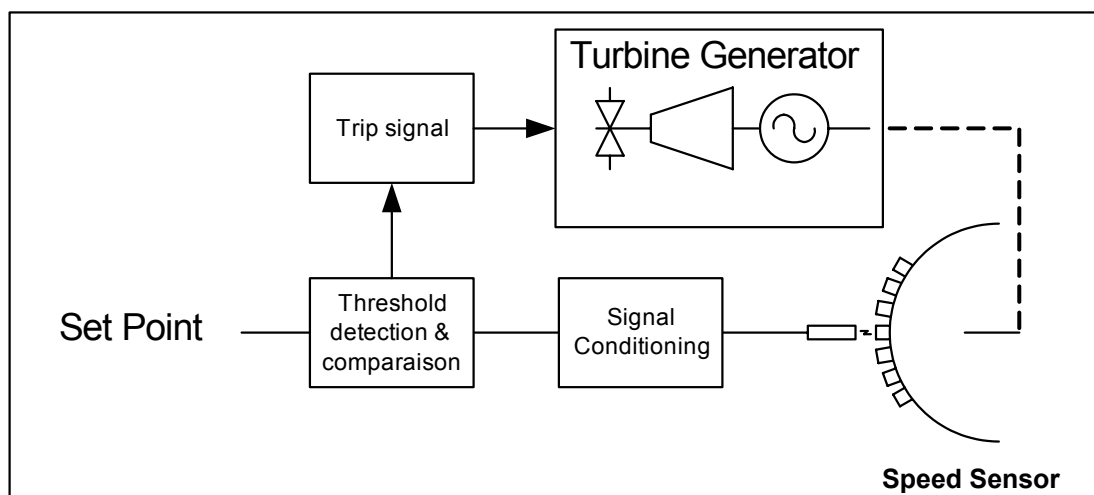
Most plants operating today still protect the main turbine using a mechanical overspeed protection system. The electronic systems available at the time the plants were constructed were not considered sufficiently reliable. As a result, a mechanical overspeed protection system was installed in addition to the electronic overspeed trip. This also provided for a level of redundancy and for diversity. Prior to the Salem event, in the United States, Westinghouse turbines could have the mechanical system set to a higher trip speed than the electronic overspeed protection system, to allow the plant to "ride-through" any brief transients and not trip unnecessarily. After the Salem event, the mechanical and electronic overspeed protection systems were mostly set to the same speed, and testing was enhanced at most plants to identify failures in redundant valves and components, without disabling the other parts of the protection system.

The mechanical system consists of a spring-loaded trip weight mounted in the rotor extension shaft. Under normal speed conditions, the spring opposes the centripetal force of the off-center weight. As the rotor speed increases, the weight's centripetal force overcomes the spring force and the weight moves outward from the rotor's center of revolution, towards a mechanical trigger. When the weight extends far enough, it strikes the trigger and activates the mechanical trip valve for the stop valves' hydraulic header. Upon loss of hydraulic pressure, the actuator drives the stop valves to the closed, or fail-safe position. This cuts off steam to the turbine causing it to coast to a stop.

### **2.2.2 Electronic Overspeed Protection**

Figure 2-2 illustrates the basic configuration of an electronic overspeed protection system.





**Figure 2-2**  
**Overspeed Monitoring Configuration**

As in the speed control loop, a speed sensor provides an electronic signal proportional to the turbine's rotational speed. A sensor and processing electronics detect changes in magnetic fields induced by the teeth on a gear on the turbine's shaft. A detection and comparison circuit, which can be either digital or analog, evaluates the speed signal and compares it to the set point threshold value. While some plants use the same speed pick-ups for the control and the protection systems, others have a completely independent set of pick-ups for redundancy.

In a single trip path system, if the actual speed is greater than the set point, a trip signal commands the stop valves to close. In some redundant systems, each train independently votes and the voting logic determines whether to trip. In other redundant systems, each train provides all the others with their speed values, and each train selects one of the values to generate a trip based on a consensus decision.

The threshold detection and comparison circuit offers different functionalities depending on the manufacturer and options included in the system. Delays, staggered threshold levels, and rate of rise are typical options available. The options selected depend on both the turbine manufacturer's and the plant's requirements. Digital systems usually offer more flexibility than analog systems because of extended computational capabilities. However, overall system and software simplicity is important in safety critical applications such as turbine overspeed protection.

### **2.2.3 Stop Valve Interface**

Both mechanical and electronic overspeed protection systems use the stop valves to trip the turbine. The stop valves are in the steam inlet lines, typically upstream of the modulating control valves. The stop valves quickly isolate steam flow to the turbine. As such, the stop valves are designed to fail-safe to the closed position and to close much faster than the control valves. Typically, a hydraulic actuator opens each valve, and springs force the valves closed when the trip or control system removes hydraulic pressure. Stop valves are also designed so that steam

flow tends to force the valve to the closed position. The stop valve actuator is intentionally completely independent of the modulating valve control system. The turbine overspeed protection system dumps the hydraulic pressure that holds the stop valve actuators open. Then, steam flow and springs force these valves closed. The EHC system also closes the stop valves below a low speed setpoint during turbine shutdown.

The mechanical overspeed detection system triggers a plunger on the mechanical trip valve. The trip valve will drain hydraulic fluid when triggered. Draining the fluid causes a lockout valve to drain the master trip valve. This in turn drains the fluid from the stop valve hydraulic header and causes the stop valves to close, stopping steam flow to the turbine.

In an electronic overspeed protection system, one or more electrically actuated solenoid valves, normally held closed when energized, de-energize to open and relieve hydraulic pressure from the stop valve hydraulic header. The intermediate trip valves are no longer required and are removed to eliminate sources of faults and failures.

## **2.3 Operator Backup**

In addition to the overspeed protection systems, the operator can manually close the stop valves. The control room local stations (such as the EHC panel), and the front standard of the turbine are typical locations with such controls. However, it is extremely unlikely that an operator can intervene in time to stop a turbine from overspeeding unless perhaps he happens to be actively monitoring it at the time. An operator is a not replacement for a working turbine overspeed protection system.

# 3

## ISSUES WITH THE EXISTING SYSTEM

---

### 3.1 Issues with Mechanical Overspeed Trips

There are many issues with mechanical overspeed systems that make them a less than ideal solution. These drawbacks include setpoint imprecision, lack of diagnostics, difficulty of maintenance, difficulty and danger in testing the system, calibration and testing on the critical plant startup path after refueling outage, and a generally antiquated mechanism.

One of the main issues with a mechanical overspeed system is its imprecision. There is no way to pre-set a precise trip point or have the system reliably trip at a given speed. Generally, for mechanical overspeed systems, the weight mechanism will trip the turbine with a variation of up to  $\pm 50$  revolutions per minute (RPM) of the desired set point. This is because the trip is initiated by the centripetal force on a weight overcoming the force of a spring. Over time, factors including spring compressibility and friction from particles in the weight's path can alter the exact RPM at which the trip activates. For an 1800-RPM turbine, a 50 RPM difference is nearly 3%. That means that the trip could occur at a speed up to 3% higher than desired, increasing stresses on the turbine and blades, decreasing the lifetime of the turbine, or at a speed up to 3% lower than the set point, leading to a falsely tripped system. The mechanical system can also completely fail to trip the turbine.

An additional concern with the mechanical overspeed system is its lack of diagnostics. Unlike the electronic overspeed system, which tracks the speed of the rotor, and can provide this information to an operator, the mechanical system gives no such feedback. The mechanical overspeed provides no indication of any problems until it trips the turbine, or fails to trip the turbine. This means that if the trip point is set too low, there is no way to know until it trips and shuts down the entire power production process. If the trip were set too high, it would take an overspeed test or an actual overspeed event to reveal the problem, either of which could lead to destruction of the turbine. Assuming the turbine survives the discovery process, the next steps would be to adjust the mechanism and confirm the setting with an overspeed trip test.

Finally, testing the system is a difficult and even dangerous task. Since there are no diagnostics, there is no way to test the mechanical system other than to force a trip from the mechanical system. If the electronic trip were set at the same or lower speed as the expected mechanical trip, the plant owner would have to disable the electronic trip, and then actually overspeed the turbine to ensure the mechanical trip works. During the time when the plant owner is intentionally overspeeding the turbine, the redundant electronic trip is disabled and the plant owner depends totally on the mechanical trip under test. Even in the best case, where the trip works and shuts down the turbine, the overspeed itself applies unnecessary stress to both the turbine and the generator rotors.

The worst case for this test is catastrophic. If the mechanical trip does not work properly, an actual overspeed event can occur, destroying portions or all of the turbine and generator, and creating missiles. In fact, insurers estimate that 50% of all catastrophic overspeed events at power plants have occurred during failed overspeed tests, in which the mechanical system failed to shut down the turbine as intended (Reference 2). This is an unacceptable risk to both equipment and personnel. In addition, these tests are costly.

Since the generator cannot be on the grid to perform this test, the plant is not creating power during this time, and is therefore losing revenue. Whether testing is done before or after an outage, the rotor must be at operating temperature. It is safer to overspeed a warm rotor, since the material toughness is higher than for a cold rotor. If the testing occurs during startup, the plant owner must heat the turbine to the manufacturer's specifications prior to the overspeed test, which requires time during the startup, extending the total test duration and impact on generation. Testing when coming out of a refueling outage prolongs the time to get the unit back online and producing power. Testing when going into a refueling outage may not have the economic impact, but presupposes that there will be no need for work on the turbine overspeed trip system during the outage. If anything is done during the outage that affects the trip system, then testing must be performed when coming out of the outage, to prove that the overspeed trip system still works.

Because of the imprecision, unpredictability, cost, and even danger inherent in these mechanical overspeed trip systems, plants have begun looking into ways to modernize their overspeed protection systems without creating an increase in overspeed failure probability.

### **3.2 Modernizing the Mechanical Trip System**

When utilities were first constructing nuclear power plants, electronic control systems were analog systems that were limited in capability and especially susceptible to undetected faults and failures. This made the mechanical overspeed system extremely critical. However, as digital electronic systems have become more sophisticated, with vastly improved microprocessor power and reliability, the need for mechanical overspeed systems has lessened to the point that their elimination is cost effective. With the increased reliability of electronic control and overspeed protection systems, and the difficulties and relative unreliability of mechanical systems, many plants are looking to modernize by removing the mechanical systems and going to a purely electronic overspeed system. Keeping the mechanical system requires the plant owner to continue to maintain and test it, including rotor overspeed tests if the mechanical system is to be credited. The mechanical system cannot be abandoned in place, since it still has the potential for unbalancing the rotor by inadvertent extension, and possibly tripping the plant.

# 4

## MODERNIZING THE MECHANICAL SYSTEM

---

Because of the issues with the mechanical overspeed trip system, many facilities are looking into modernizing this protection system. This section describes design features and evaluation processes that can be used to help provide assurance that the replacement system will be highly dependable.

### 4.1 System Quality and Dependability

An overspeed protection trip system should provide an extremely small probability of catastrophic turbine failure. In considering modernizing the mechanical overspeed trip system, the plant owner should ensure that the new protection system is designed properly, to minimize the probability of catastrophic turbine failure. This section defines many of the features that are desirable in an overspeed trip protection system. The plant owners will need to make their own determination as to how well the overspeed trip system vendor does in providing these desired features.

#### ***4.1.1 Better Protection by Removal of Hazards***

Despite the shortcomings of the mechanical system, especially the imprecision of its trip speed, it still provides some level of overspeed protection. If the plant owner were to remove the function completely, this would seem to increase the likelihood of damage due to an overspeed event. However, while a working mechanical trip does provide some level of protection, maintaining proper operation through testing creates the very hazard the system was designed to eliminate. Because most plants have the trip speed of the mechanical system set higher than that of the electronic system, testing proper operation of the mechanical trip system requires the plant owner to disable the lower speed electronic trip.

This means that if the mechanical trip system fails to operate correctly during the test, the only remaining mechanism to stop the turbine is the operator using the manual turbine trip switch. While the operator is certainly minding the manual turbine trip switches more carefully during a mechanical trip test, the operator is by no means failsafe. Insurance data has shown that fully 50% of all overspeed failures occurred during mechanical overspeed trip testing (Reference 2). By eliminating the mechanical trip, the turbine trip system does not need to be tested at speeds above the operational range of the turbine. This removes the condition under which half the turbine failure events occur. It also increases safety during normal operation by avoiding unnecessary blade and generator rotor stress during tests above operational speeds. Where applicable, the plant owner should update the existing Probabilistic Risk Assessment (PRA) to determine how modernizing the mechanical overspeed trip affects total probability of missile generation affecting safety systems. For some plant designs, the orientation of the turbine and

generator when combined with the location of safety systems and systems supporting safety systems makes it impossible for missiles to damage safety systems. For those designs, modernizing the overspeed trip system is driven by reliability considerations and the desire to reduce the costs of maintenance and calibration of the mechanical system.

The plant owner should also consider whether any existing electronic overspeed trip system would be retained as a diverse trip system, or whether maintenance resources are better spent by replacing both the existing obsolete trip systems with a single, redundant system.

#### **4.1.2 Better Protection by Improved Reliability**

A goal for the expected mean time between occurrences of a failure to trip should be at least the life of the plant, and preferably, several times the life of the plant, since the value provided is a statistical measure of probability and not a guaranteed value.

Most of the commercially available overspeed trip systems are based on digital technology, as either firmware running on a microprocessor or microcontroller, or as digital logic running in a programmable logic device. For safety-related applications, the Nuclear Regulatory Commission (NRC) considers complex digital logic running in a programmable logic device as needing a development process comparable to software, with formal design documents, peer review, and testing. Guidance for industrial safety systems does not differ significantly from the NRC guidance. Since digital implementations should be done under formal software quality assurance processes, the normal nuclear issues with high criticality digital equipment apply.

For both nuclear and non-nuclear applications, the consequences of a failure can be severe, so it is prudent for the plant owner to take appropriate steps to ensure that the system is highly dependable. The most expedient approach may be to find a vendor with a highly reliable software and hardware development culture, who has provided turbine overspeed trip systems for a significant period, with high quality software and hardware design processes, and a proven product. This minimizes the probability of latent software design errors, and thus the probability of software common cause failure. Unfortunately, software common cause failure can only be minimized, and cannot be eliminated completely, through these methods.

#### **4.1.3 Better Protection by Improved Safety**

Based on the economic and industrial safety impact of turbine failure, it is recommended that the vendor, an independent certifier, the plant owner, or its proxy evaluate a new digital system to ensure that the design includes adequate features to ensure high dependability. The turbine overspeed protection system is considered a Safety Instrumented System (SIS) or Emergency Shutdown System (ESD) in other industries. As such, it may be possible to purchase a system certified to Safety Integrity Level (SIL) 2 or 3 according to International Electro-technical Commission (IEC) Standard 61508, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems” (Reference 3). This consists of an overspeed trip system with a SIL 2 or SIL 3 rating based on audits from an accredited agency, such as Technischer Überwachungs-Verein (TÜV), the German technical oversight agency. Table 4-1 enunciates the probability of dangerous failure per hour for each SIL level from IEC 61508-1. This table is for

a high demand or continuous mode of operation system, which implements continuous control to maintain functional safety.

**Table 4-1**  
**Target Failure Measures for a Continuous Mode of Operation System**

Safety Integrity Level	High Demand or Continuous Mode of Operation (Probability of a Dangerous Failure Per Hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

If the selected device does not have a SIL rating from an accredited agency, then the plant owner should consider performing or commissioning an evaluation using an approach of the type described in EPRI Report 1011710, “Guideline for Evaluating Critical Digital Equipment and Systems” (Reference 4).

#### **4.1.4 Better Protection by Redundancy**

Redundancy in an electronic overspeed protection system is highly recommended. Redundancy can be built in to the speed sensing circuit with multiple probes, threshold detection and comparison with redundant processors, and trip control and command using redundant voting logic and trip solenoids. There might even be redundancy in the hydraulic circuit, depending on the plant design. Some level of redundancy is already in common use in the large majority of plants, as well as required by nearly every standard. Because it is so crucial, redundancy deserves further mention as a way to improve trip protection in a modern electronic trip system.

In order to minimize the probability of random hardware failures in single trains disabling the protective functions, the system should be designed to be single failure tolerant. The system should include at least two, and preferably three, independent, separately powered sensors, logic solvers, and trip elements.

If only two independent trains are provided, in order for a system of this design to meet SIL 3 requirements, each of the logic solvers typically must have extensive and effective diagnostics, with logic solvers voting in the one-out-of-two diagnostic mode (see several sections of IEC 61508). In order to preclude the trip device from disabling the system, as well as to avoid false trips, the output should vote one-out-of-two taken twice.

If three independent trains are provided, then the requirements for diagnostics are lessened. With three devices, further enhancements to reliability and availability are possible by having the logic solvers share all three input readings, alarm on significant deviations, and initiate trips only when required. The vendor may choose to have each of the logic solvers use only the sensors wired to that logic solver, or have each of the logic solvers choose a representative sample from all logic solvers. The NRC’s current regulatory concerns with safety related data communication

between channels and divisions do not apply to communications between redundant nonsafety related logic solvers. These systems normally use two-out-of-three voting. Diagnostics can further enhance the effective reliability and safety of this system.

With two-out-of-three voting, a single sensor that has a reading significantly different from those of the other two sensors will be voted out of the protection scheme, or will result in only one of the three channels voting to trip. The protection equipment should generate an alarm on this deviation, indicating that troubleshooting and maintenance is required. The protection system would continue to operate, with no loss of power production due to failure of an inexpensive part and no loss of protection on the turbine and generator.

In order to ensure that failure of local power does not result in failure to trip the turbine, the independent trains should fail-safe to the tripped, non-powered condition. Since this requires power to leave the turbine running, the power to the independent trains should be reliable, and output trip devices should be set up to vote on tripping the system. If a two-train system is provided, then the trip devices should also be redundant and designed for single failure tolerance to either energized or de-energized conditions. If a three-train system is provided, then the trip devices should be redundant and require a two-out-of-three vote for failure tolerance.

Finally, valve redundancy is crucial as well. All the redundancy in the speed sensing system and trip triggering logic does no good if the trip valves cannot be shut properly or fast enough. Because of this fact, standards require valve redundancy. The American National Standards Institute/American Petroleum Institute (ANSI/API) Standard 612 requires “the turbine shall be provided with a minimum of two, separate electro-hydraulic solenoid operated valves located in the shutdown system” (Reference 5). While the standard does specify a level of redundancy of two valves, it allows for more by making two the minimum number required. Plants considering removing their mechanical overspeed trip systems (including the mechanically tripped shutoff valves) might want to consider increasing valve redundancy and testability on the electro-hydraulic servo valves, by adding a means of testing each individually, to avoid the masking of faults and failures of redundant valves.

#### ***4.1.5 Better Protection through Better Control***

In conjunction with built in redundancy to the governor and trip systems, alarm systems can add levels of confidence by bringing in the human element. For diagnostics and indication of operability, the overspeed trip system should have sufficient local indication for technicians and engineers and annunciation of faults and failures in the control room for operators. Local indication should also include simultaneous readout of all available turbine speed indications, in common units such as RPM. By annunciating faults and failures in the system, maintenance can be performed before the trip system fails completely.

#### ***4.1.6 Better Protection by Avoiding Part Obsolescence***

Since digital components become obsolete rapidly, the plant owner should discuss parts obsolescence issues with the vendor. The vendor should have a plan for dealing with parts obsolescence, preferably by redesign of the electronics equipment with new components,



maintaining the form, fit, and function compatibility of the new equipment with older equipment. If form, fit, and function compatibility cannot be maintained, then the plant owner may be forced to replace the non-failed, working redundant components with new-design components through the design change process. While the vendor may be willing to commit to keeping the equipment available for the life of the plant, the plant owner should also evaluate the vendor's history and periodically check the vendor's catalog to determine whether a lifetime buy is appropriate before needing replacement equipment. Many vendors evaluate their equipment on a periodic basis, and either make lifetime buys of parts that the manufacturer is about to discontinue, or redesign the equipment with current parts and maintain form, fit, and function compatibility. The plant owner should be familiar, and comfortable, with the chosen vendor's practices.

## **4.2 FMEA-Based Design**

The Failure Modes and Effects Analysis (FMEA) is a systematic procedure for identifying the modes of failure and for evaluating their consequences. The essential function of an FMEA is to consider each major part of the system, how it may fail (the mode of failure), and what the effect of the failure on the system would be (the failure effect).

The FMEA allows the user a structured analysis of a system's failure potential. Application of this analysis activity can ensure that the plant owner and system designers consider all conceivable failure modes and their effects on the operational success of the system. The analysis can also identify the magnitude of failure effects including identifying critical failures that may dictate the frequency of operational test or maintenance, identify "safe" versus "unsafe" failures in the system, and identify the need for design modifications to eliminate unacceptable failure mechanisms.

Failure analyses should be performed for all portions of the turbine overspeed trip system, addressing hardware, software, and all system operations and plant operational modes, to identify plausible failure modes, their estimated frequencies, and effects of the failures on functionality of the system. These analyses should demonstrate that no single failure would cause large-scale loss of the protective function or failure to generate the required alarms. The failure analysis also should demonstrate that the likelihood of common cause failures (including failures caused by errors in software or digital system design) resulting in total loss of the protection features is very low, and that such failures should not be expected to occur well beyond the plant lifetime. Finally, the analysis should address actions by technicians and engineers during configuration, troubleshooting, maintenance, surveillance testing, and any surveillance rounds. The plant owner should request the vendor's failure analysis for the sensors, logic solvers, and trip valves as input to the site's failure analysis. The site's failure analysis will use additional plant-specific information that a vendor is unlikely to have.

FMEA techniques are defined in Military Standard 1629A (Reference 6), which, while obsoleted by the Department of Defense, is still an excellent process standard for FMEA techniques.

In addition to FMEA, Fault Tree Analysis (FTA) will be performed as part of the PRA. Building the fault tree should be part of the failure analysis activities for this modernization.

Performing failure analysis is only useful if the results of the analyses are considered in the system design. The plant owner should ensure that the FMEA results are incorporated into procedures, design, implementation, and testing. The plant owner should ensure that FMEA techniques were used during design activities for the logic solver as well as for the modernized plant protection system design.

While the logic solver is not nuclear safety related, it should still be treated as high criticality software. The software that the vendor has written to run the logic solver, along with any tuning or adaptation necessary to apply the logic solver to the plant owner's turbine generator, should have design documentation, records of peer review and testing, and have been generated and maintained under a software quality assurance process. As an Emergency Shutdown system, industry practice outside the nuclear industry is to require software processes similar, or sometimes more rigorous, than applied to nuclear safety systems. EPRI report 1011710 (Reference 4) provides current guidance for evaluation of software-based systems for nuclear safety related and other critical applications.

# 5

## SYSTEM SURVEILLANCE AND TESTING

---

An upgraded redundant electronic overspeed system does not require the repeated calibration and testing needed for mechanical overspeed systems. However, an electronic system does not eliminate the need for testing. In addition, an electronic system can support enhanced surveillance tests, to ensure continued correct operation during standard use, as well as providing the operator with warnings about system faults and failures that do not require a total system trip. This section discusses issues the plant owner should address in modifying the existing surveillance testing and the types of alarms that should be present.

### 5.1 Features Required for Surveillance and Test

A mechanical overspeed trip system does not provide any means for detecting faults and failures. The result is that the system can suffer from undetected failures that may not become apparent until the overspeed system should fail to trip.

The replacement system should provide the operations and maintenance staff with significantly better indication of operability, and with significantly better means of troubleshooting and testing the overall turbine system.

For normal periodic surveillance of the speed sensing and processing electronics, the electronic overspeed trip system should provide external indication that each of the redundant trip sections is operable, of any faults or failures in the system, and of the current voting status. The electronic system should provide dry contact<sup>2</sup> outputs to annunciate electronics faults and failures to the control room, including speed mismatch between the redundant trains. The electronic trip system could also send digitized data to an external system for display to the plant operations staff. For local maintenance and troubleshooting, the system should provide a local human-system interface (HSI). If an interface to a remote system is used, the trip system should protect itself from modification by the remote system. The trip system's local display should protect itself from unintended or malicious change in setpoint values and function, by providing cyber security features, to the level desired by the plant owner.

For testing the hydraulic portions of the system, the device should provide some means of injecting electronic signals into the speed sensor and tripping one of the redundant trains. This should not result in tripping the turbine, but should demonstrate that the trip functions up to the stop valves' hydraulic header. Periodic surveillance tests of the whole system will still be

---

<sup>2</sup> Dry contacts are potential free and normally implemented by relays. Opening or closing the contacts results in a change in state that the plant annunciator, or plant process computer detects, and aural and visual notification of the change in state to the control room operations staff.

needed to demonstrate that the stop valves function, but the goal should be that these tests are less frequent compared to the requirements under the mechanical systems.

## **5.2 System Test**

Most utilities test the complete trip system every outage. Whether the plant owner tests at shutdown or during startup, the total system should be tested, starting at the speed sensors, through the trip logic, through the output voting and the hydraulic stop valve header, all the way through the closure of the stop valves. While testing during plant shutdown into outage is attractive, the plant owner should also test the system after any turbine or trip system disassembly, modification, or assembly and prior to operation.

There are two ways to test any system. The site can test the entire system as a whole by causing it to perform its designed function, or it can test each component in logical groups, with sufficient overlap, and deduce whether they will work appropriately as a system. For a system as complicated as a steam turbine generator overspeed trip with such critical demand on correct functionality, both of these methods should be employed at varying frequencies.

The modernization of the mechanical overspeed trip does not eliminate the requirement for full system testing. However, the replacement electronic trip system does allow for testing individual portions of the system, demonstrating that most of the system works, without tripping the turbine. This section discusses testing for both the partial system test as well as the full overspeed assessment. The section concludes with a brief discussion of elements to evaluate in setting the test frequency.

### **5.2.1 Partial System Test**

Because of the high cost of shutting down the plant to perform a complete system test, the plant owner should consider testing components from time to time to validate continued proper operation of the overspeed trip system between complete system tests. These tests should be on each section of the trip system from speed sensing mechanisms to shut off steam valves. Ideally, with proper system design, the plant owner can complete these tests without interrupting power generation. By simply taking the component being tested offline, the component can be assessed without tripping the entire system, and there is still sufficient redundancy so that if the turbine were to overspeed during the subcomponent test, the redundant subcomponents would trigger the turbine trip. Since the overspeed protection system is designed to be operational even with a failure at one point in the system, it can also be operational if one component is intentionally removed for test.

The first place to perform a partial system test would be at the speed sensing mechanism. As suggested in Section 4, consider a system with three redundant speed sensors and two-out-of-three trip voting. In this configuration, removing one pickup for test is essentially the same as a failure in one of the speed pickups. The pickup is no longer a reliable source of rotor speed information and the voting logic adjusts by reverting automatically to one-out-of-two voting while the third pickup is offline. The offline speed pickup can now be tested for proper operation, to see if an injected overspeed signal will provide correct data and trigger a trip signal

to the voting logic. By sequentially performing this test on each speed pickup while the others are online, the entire speed sensing and most of the logic solver mechanism will be verified without ever halting power generation or losing the ability to trip the turbine during an overspeed event. Some of the triple redundant systems perform this testing automatically, and alarm when the system detects internal faults and failures.

According to ANSI/API Standard 670 (Reference 7), speed-sensing pickups should be tested to ensure they react properly with a reading of  $\pm 1\%$  of the set trip speed. The authors note that the plant owner likely should consider this the minimum acceptable accuracy. The plant owner could also consider that sensing the current rotor speed indicates that the speed sensors are operating correctly, since there are no known failure modes in the sensor itself where the speed would freeze at a given level. However, there are failure modes where the electronics or the microprocessor in the logic solver can freeze at a given limit. Therefore, disconnecting the speed sensor and verifying that the speed goes immediately to zero proves that the speed sensing electronics are operating correctly.

If injecting electronic signals at the input speed sensors is impractical, the system should provide a means of injecting speed signals where the speed sensors feed into the logic solvers, providing sufficient overlap to demonstrate that the speed sensing inputs are operable. This could be done by displaying the current turbine RPM for each train, and then verifying that the correct signals exist on each of the train inputs, and that the injected signal results in appropriate changes for the affected train.

If signal injection testing is performed, the speed pickup should be tested in two ways. First, check that an injected speed just over (but still within) the stated accuracy of the trip speed generates a trip signal. Second, testing should also ensure that a signal injected below the trip point does not trigger a trip signal. This will keep the system from tripping falsely.

These on-line surveillance tests should also support testing all of the discrete outputs used to annunciate faults and failures and display engineering unit and status values in the control room.

Another goal of a partial system test is to verify performance of the stop valves that are responsible for isolating steam to the turbine in the event of an overspeed. If the hydraulic system holding the stop valves open can reopen the valves against rated steam pressure, then it is possible to test each of the control valves individually, verifying their complete closure. Current stop valve tests require reducing the plant generated power by some acceptable amount, and then verifying that each of the stop valves will close and then reopen. Literature and evaluations of Emergency Shut Down and Safety Instrumented Systems in industry state that the most probable failure is the failure of the stop valve to move or to seat and close completely. The literature also suggests that similar design stop valves become less likely to close as time passes since their last successful test (see Section 0, 5.3 Test Frequency, below). EPRI Report 1008740 (Reference 8) uses data from INPO that demonstrates that the valves are the least reliable part of the overspeed protection system.

If testing can demonstrate that stop valves at least move from their full open position, then there is a greater probability that they will close when needed. Several of the ESD and SIS standards state that some, but not all, of the probability of correct stop valve operation can be assured by just moving the valve from the full open position. Currently, there is no capability to perform

these partial stroke tests on the existing hydraulic stop valves. If partial stroke testing capability were to be installed, several design precautions would need to be observed. These include making sure the partial stroke test capabilities would not prevent the full closure capability. EPRI Report 1004960 (Reference 9) provides additional information on monitoring turbine valves during stroke testing to provide early detection of degrading conditions.

### **5.2.2 Periodic Complete Overspeed Test**

Periodically, it is wise for the plant owner to verify that the complete overspeed trip system works and can actually trip the turbine. For most commercial US nuclear plants, this periodic test has to be performed when the nuclear reactor is not producing full power. This test is typically performed after the turbine has been maintained and at every scheduled refueling outage. The tests are performed with the generator not attached to the grid, so the amount of steam required to generate an overspeed condition is very small, and there is very little resistance to rapid increases in rotor speed. It is important that this test exercise the system software and hardware in their normal operating modes.

The traditional overspeed tests verify that the overspeed trip system provides the protective function when the rotor achieves the overspeed RPM. At least one of the turbine Original Equipment Manufacturers (OEMs) still recommends that the surveillance tests be performed at the actual overspeed RPM, although the technical basis for this is unclear. This report concludes that with software based trip systems, there is no reason to stress the rotor by testing at the overspeed trip point. Overspeed trip testing should test the overspeed trip system, not the mechanical integrity of the turbine. To the extent possible, it should avoid stressing the turbine by running it above the normal operating speed.

As an alternative that is accepted by at least one of the insurance vendors, the software could be configured to allow substitution of a lower RPM test point in the software. This capability could be used to test each of the redundant portions at some lower speed. This capability could also be used to test online, if some means are provided to detect servo valve operation in the dump valves without actually closing or moving the stop valves.

If this approach is followed, then there should be a clearly and well-designed means of setting the system into this test mode, which cannot be inadvertently entered during normal plant operation. The test mode should be clearly annunciated or indicated in the control room, and should be initiated by key lock switches or other physical controls. The lower test setpoint values should not be entered manually, to preclude a technician from setting the wrong values into the operating plant and thus inadvertently and silently defeating the protective function. If setpoint value changes are performed manually, the plant owner must independently verify that the setpoint values have been restored correctly after testing is complete. If the setpoint value changes are performed under software control, the plant owner must verify and validate that the setpoint changes operate correctly during factory acceptance testing.

### **5.3 Test Frequency**

During the period after a test proves the trip system's proper operation, the probability of dangerous faults increases with time, until the plant owner performs the next set of tests. This issue is documented in EPRI Report 1008740 (Reference 8). The goal of these proof tests is to ensure detection of dangerous faults that diagnostics or other less comprehensive testing do not detect. These proof tests are critical to achieving the system reliability expected in most plant PRA analyses. Part of the replacement activities and the on-going operation and maintenance of the equipment is to ensure that the testing frequency is correct, sufficient, and appropriate for the target hardware safety integrity level requirements, ensuring that the trip system will likely function correctly when needed.

The sensing and logic solvers should have diagnostic coverage in the logic solver software. For the sensors, the logic solvers should compare the redundant values and generate alarms on significant deviations. The plant owner should take credit for periodic rounds, verifying that the displayed values for RPM are reasonable and consistent with the plant's state, as well as evaluating any other diagnostic error messages that are displayed. The annunciation and indication of such data in the control room is also part of the periodic surveillance, especially if the logic solvers are protected with appropriately designed watchdog timer circuits that do not depend on correct software operation to indicate errors (see EPRI TR-107339, Revision 0, Appendix A, pages A-36 and A-37, Reference 10). The plant owner should evaluate the degree to which the diagnostics cover the possible faults and failures in the sensors and logic solvers, as these are the most likely means of uncovering random hardware failures. Diagnostics may not detect some classes of software or hardware design flaws.

The actuated stop valves and the electronic-to-hydraulic interface are the primary concerns for undetected faults and failures. The plant owner can manually test the sensors and logic solvers. The logic solvers can self-detect and annunciate faults and failures. With careful design, the vendor and plant owner can design a testable electronic-to-hydraulic interface. However, the stop valves themselves remain an issue.

The stop valves remain in the open position continuously. Two failure modes are common in such applications: stuck in the open position and failure to seat completely to stop steam flow. The only way to be sure that the stop valves are not stuck is to move them periodically. The only way to be sure that the stop valves will seat completely is to close them periodically. In many nuclear plants, utilities only perform complete valve closure tests during complete overspeed trip system proof testing during refueling. In 1997, the process industry reported on a population of 552 valves in emergency shutdown systems with 127 critical failures. Of these, the stop valve leaked 75 times and failed to move 46 times (Reference 11).

The probability that a valve will fail is a linear expression involving the probability of failure per hour times the proof test interval divided by two (Reference 9). The longer the proof test interval, the greater the likelihood that one or more stop valves will fail when needed. Reliability analysis for systems like the turbine overspeed trip system show that the electronic-to-hydraulic interface and valves contributes most to the probability of failure. The interfaces and valves contribute more since the sensors and logic solvers are tested automatically, whereas the interfaces and valves are not (Reference 12). Additional testing, including partial stroking of

each stop valve, may be necessary to achieve the probability of failure assumed in the plant PRA. Partial stroke testing can detect stuck valves, but cannot detect failures that result in leaks.

The plant owner should also consider the implications of their current procedures for testing the turbine stop valves. On-line testing of one or more valves individually may be necessary to maintain acceptable assurance that the stop valves will operate when needed. This may require additional valves and electronics if automated testing is necessary.



# 6

## OTHER PERSPECTIVES

---

In making recommendations about a system as critical as the overspeed trip system, it is appropriate to get other perspectives. This includes the companies who insure the power plants as well as the turbine and overspeed system manufacturers, who all clearly have a very large financial stake in ensuring that overspeed protection is sufficient.

### 6.1 Insurer Perspective

Those who insure power plants against turbine overspeed events have a very large financial stake in overspeed protection. Thus, their opinion about the modernization of the mechanical overspeed trip is a valid one and an important one to get. The authors contacted two of the largest power plant insurance companies in the world and found that they were in agreement. The electronic overspeed protection system is preferred to the mechanical type. The representatives said they recommend an electronic system that is redundant, reliable, has fault tolerance such as 2-out-of-3 voting, performs self-diagnostics, and has an alarm system. One insurer even said that in these situations, the plants could remove the mechanical system completely.

The question was posed to the insurers about acceptable testing techniques. The response was that the plant owner needed to have a formal, documented overspeed trip test procedure consistent with turbine manufacturer guidelines; direct owner, engineer, and supervisor oversight; and the system should record the results to allow for resolution of any difficulties. The non-nuclear insurer wanted to see that DC systems were tested and maintained for systems using batteries. Both wanted to see complete testing, including the operation of the emergency stop valves. They also commented that while testing during shutdown was acceptable, if any work was done while the turbine was offline, the system should be tested again on start up to verify the work was done correctly. Opinions on overspeed trip test speed, however, differed. While the NEIL standard (see more below) currently only allows for an overspeed trip test at or above operational speed, companies who insure non-nuclear turbines have begun to allow utilities to perform overspeed trip tests below operational speed. The non-nuclear insurer was very clear to point out that as long as the test proved out the operation of the entire system (or as much as is possible), the trip could be performed at any turbine speed, and thus verify system operation with much safer conditions. The nuclear insurer stated that his company's next technical advisory meeting would consider performing these tests at speeds lower than operational speed.

The authors reviewed the Nuclear Electric Insurance Limited (NEIL) 2004 Loss Control Standard (Reference 13). It states that a plant will receive additional credit within the scope of their insurance if they have independent overspeed protection. This is described as “an

independent system beyond the normal systems to provide additional assurance against excessive overspeed.” The insurer does not differentiate between mechanical and electronic trips, allowing either one to receive the insurance credit. The NEIL insurance currently allows a small credit for redundant overspeed trip systems. The NEIL insurance also allows the backup system credit to be taken within a dual or triple redundant overspeed trip system. The backup system must be tested periodically for operability.

The testing portion of the document describes how often components of the plant should be tested, with one key requirement. The document explains that if the plant owner has performed maintenance work on the overspeed system that could affect the operation of the overspeed system, a full overspeed test should be done. For mechanical systems, this test is an “actual overspeed test” at speeds above the normal operational speed of the turbine. However, for electronic overspeed systems, though a full system trip is required, the plant owner can perform the test “at or above normal running speed.” This means insurance companies will give equal credit to plants for performing a full overspeed trip at normal running speed as they would for an above normal operation speed trip with a mechanical trip. As discussed earlier, the excess speeds are much more dangerous in that the stresses on the turbine rotor and blades and generator rotor are higher, as well as the probability of mechanical failure during test. The insurance company accepts that electronic overspeed trip systems provide equivalent protection without endangering the rotating equipment, by giving them equal value for testing at much safer speeds. For NEIL insurance, full system testing must be performed at every refueling outage, with quarterly simulated testing between refueling outages.

## **6.2 Turbine OEM Perspective**

Turbine original equipment manufacturers were also contacted about removal of the mechanical overspeed system. The OEMs were asked about their current philosophy, issues associated with removing the mechanical overspeed trip, and concerns the plant owner should address to ensure appropriate overspeed protection.

The authors contacted three of the largest manufacturers of turbines and overspeed protection systems and asked if they are still installing mechanical overspeed trip systems in their turbine installations. Each OEM independently indicated that not only are they no longer installing mechanical overspeed trip devices on their new installations, they are also modernizing older turbines by replacing the mechanical system with an electronic one, although plants are not required to do so.

The systems being installed vary in the details of their methods for reducing overspeed likelihood. However, every OEM consulted explained that in removing the mechanical trip, to ensure equal or better overspeed protection, they were installing or upgrading the electronic overspeed trip.

Methods include installing a new digital EHC using proven technology with enhanced decision logic, redundancy, and improved software. Others use full triple modular redundancy. This includes three independent speed pickups with their own trains and controllers. The logic uses two-out-of-three voting to decide if a trip is required, and if so sends a signal to triple redundant

solenoids to trip the stop valves. Some even extend the two-out-of-three voting scheme to the hydraulic dump valves for the stop valve header allowing for even further fault tolerance.



# 7

## SUMMARY AND CONCLUSIONS

---

### 7.1 Summary

This report describes a range of issues that should be understood and addressed in planning and implementing a modern turbine overspeed protection system. Considerations range from weakness of the old mechanical overspeed trip systems to insurer requirements for new digital systems. Table 7-1 briefly summarizes the issues discussed in the report and provides pointers to the report sections where more details can be found.

**Table 7-1**  
**Summary of Turbine Overspeed Issues**

<b>Issue/Consideration</b>	<b>Decision Criteria – Pros</b>	<b>Decision Criteria – Cons</b>
<i>Maintain Existing Technology – Mechanical Overspeed Trip Systems (3.1)</i>	Plants are familiar with equipment and procedures	Obsolescence of hardware, vendor support, and expertise  Limited accuracy and reliability  No on-line diagnostics or surveillance available  Difficult to set, maintain, and calibrate  Maintenance tasks are critical path during outages  Requires high risk test procedures
<i>Install Modern Technology - Electronic Overspeed Trip Systems</i>	Addresses existing obsolescence problem (4.1.6)  Improved accuracy, safety, and reliability (4.1.2, 4.1.3)  Automated calibration, diagnostics, and alarms (4.1.5)  Eliminates need for high risk tests (5.1)  Insurers prefer electronic overspeed trips (6.1)	New technology, equipment, processes, and procedures  Digital systems can be more complex  Rapid obsolescence possible (4.1.6)  Mechanical system cannot be abandoned in place (3.2)

**Table 7-1 (continued)**  
**Summary of Turbine Overspeed Issues**

<b>Issue/Consideration</b>	<b>Decision Criteria – Pros</b>	<b>Decision Criteria – Cons</b>
<i>Removal of Mechanical Trip System (3.1)</i>	<p>Eliminates mechanical system disadvantages (listed above)</p> <p>Turbine insurers and OEMs favor this approach (6.1, 6.2)</p>	<p>Mechanical system cannot be abandoned in place (3.2)</p> <p>Replacement system needs a backup (but fault tolerance in digital systems effectively provides built-in back up)</p> <p>Creates need for high confidence in replacement system (1.1)</p>
<i>Availability of Proven Digital Overspeed Trip Systems</i>	<p>Several vendors supply equipment and can tailor a system to user needs (6.2)</p> <p>Significant operating experience exists (6.1, 6.2)</p> <p>Insurers are familiar with new products (6.1)</p> <p>Digital systems meet insurer requirements (6.1)</p>	<p>May be difficult to verify quality, dependability</p> <p>Range of design approaches to select from may add confusion</p>
<i>Design Features for New Overspeed Trip Systems (4.1)</i>	<p>Hardware (double or triple) redundancy of speed detectors, power supplies, etc. provides fault tolerance (4.1.4)</p> <p>Diagnostics and alarms detect faults before system function is degraded (4.1.5)</p> <p>Data validation and voting logic reduce inadvertent trips</p> <p>Fail-safe features should be used as appropriate</p> <p>Vendor can tailor a system to specific user requirements (6.2)</p>	<p>Unnecessary complexity is a possible pitfall</p>

**Table 7-1 (continued)**  
**Summary of Turbine Overspeed Issues**

Issue/Consideration	Decision Criteria – Pros	Decision Criteria – Cons
<i>Evaluation of Quality and Dependability (4.1)</i>	<p>Insurers may credit certifications by independent agencies (6.1)</p> <p>EPRI guidance available on performing evaluations (Appendix A)</p> <p>FMEA-based design treats potential failure modes (4.2)</p> <p>May consider tradeoffs between diagnostics and hardware fault tolerance</p>	<p>Evaluation is recommended because of safety/cost consequences of system failure (1.1, 4.2)</p> <p>Should check system importance in plant PRA (4.1.1)</p> <p>Evaluations require vendor cooperation, as well as specialized digital design and software expertise</p> <p>Vendor literature does not provide sufficient information for the evaluation (6.2)</p> <p>Vendor may not be willing to support evaluation</p>
<i>System Surveillance and Testing of Digital Systems (5.1)</i>	<p>Automated diagnostics and alarms reduce scope of testing (4.1.5)</p> <p>Partial system testing can be performed with system on-line (5.2.1)</p> <p>Full system test possible at or below normal operating speed (based on insurer requirements) (5.2.2, 6.1)</p>	<p>Full system tests still required (5.2.2, 6.1)</p> <p>Test intervals will need reevaluation (5.3)</p>

## 7.2 Conclusions

Modernization of the overspeed protection system with updated technology can eliminate or mitigate many of the problems associated with mechanical turbine protection systems. However, the new digital systems come with a different set of potential problems, issues, and failure modes that should be addressed in design, maintenance, and periodic testing to ensure that they will perform at the desired levels of dependability and reliability. More specific, detailed conclusions include the following:

- When updating to a digital turbine overspeed protection system, the old mechanical overspeed system can be removed to eliminate the need for maintenance and high-risk overspeed trip tests. Turbine OEMs and insurers agree.
- Digital overspeed protection systems should be highly fault tolerant with respect to hardware failures. Various design approaches have been used successfully to accomplish this.
- The vendor, an independent certifier, the plant owner, or its proxy should evaluate a new digital system to ensure that the design includes adequate features to ensure high

dependability. An FMEA-type evaluation should be part of this, and the plant's PRA may need to be updated.

- Human error is the most likely path to catastrophic failure when allowing the trip setpoint to be changed by the user. Because of this, procedures and administrative controls for setting trip set points on the digital systems should be strictly controlled to minimize the possibility that human error leads to a lack of overspeed protection.



# A

## REFERENCES

---

1. Ornstein, H.L., Nuclear Regulatory Commission, NUREG 1275, Vol. 11, “Operating Experience Feedback—Turbine-Generator Overspeed Protection Systems,” May 1995
2. *Orbit*, “Electronic Overspeed Detection Systems,” by Jeff Rudd, Second/Third Quarters 1999, pg 44
3. International Electrotechnical Commission, IEC 61508, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems,” May 2000
4. Electric Power Research Institute, EPRI Report 1011710, “Guideline for Evaluating Critical Digital Equipment and Systems,” December 2005
5. American National Standards Institute/American Petroleum Institute, ANSI/API 612, “Steam Turbines - Special-Purpose Applications,” February 2003
6. United States Military Standard 1629A, “Procedures for Performing a Failure Modes and Effects and Criticality Analysis,” November 1980 and Subsequent Notices
7. American National Standards Institute/American Petroleum Institute, ANSI/API 670, “Machinery Protection Systems,” December 2000
8. Electric Power Research Institute EPRI Report TR-1008740, “Risk Evaluation of Nuclear Steam Turbine Destructive Overspeed,” July 2003
9. Electric Power Research Institute EPRI Report TR-1004960, “Turbine Steam Valve Diagnostic Testing,” December 2004
10. Electric Power Research Institute, EPRI Report TR-107339, “Evaluating Commercial Digital Equipment for High Integrity Applications, A Supplement to EPRI Report TR-106439,” December 1997
11. *PROCESSWest*, “Partial Stroke Testing of Emergency Shutdown Valves,” by Ken Bingham, Summer 2005
12. Exida, “The Effects of Partial Valve Stroke Testing on SIL Level,” by Iwan van Beurden and Rachel Amkreutz, October 2001
13. Nuclear Electric Insurance Limited, “Loss Control Standards,” September 2004






## Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

© 2006 Electric Power Research Institute (EPRI), Inc. All rights reserved.  
Electric Power Research Institute and EPRI are registered service marks of the Electric Power Research Institute, Inc.

 Printed on recycled paper in the United States of America

## The Electric Power Research Institute (EPRI)

The Electric Power Research Institute (EPRI), with major locations in Palo Alto, California, and Charlotte, North Carolina, was established in 1973 as an independent, nonprofit center for public interest energy and environmental research. EPRI brings together members, participants, the Institute's scientists and engineers, and other leading experts to work collaboratively on solutions to the challenges of electric power. These solutions span nearly every area of electricity generation, delivery, and use, including health, safety, and environment. EPRI's members represent over 90% of the electricity generated in the United States. International participation represents nearly 15% of EPRI's total research, development, and demonstration program.

Together...Shaping the Future of Electricity

### *Programs:*

Nuclear Steam Turbine Generator Initiative  
Steam Turbines, Generators, and Balance-of-Plant

1013461

---

## ELECTRIC POWER RESEARCH INSTITUTE

3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA  
800.313.3774 • 650.855.2121 • [askepri@epri.com](mailto:askepri@epri.com) • [www.epri.com](http://www.epri.com)