# Redundant Governor Control Upgrade for Helms Pumped Storage

By Roger Clarke-Johnson, American Governor Company, Kirkland, WA

## Abstract

As part of a major plant upgrade, Pacific Gas & Electric (PG&E) is replacing the analog governors on three 404MW units at the Helms Pumped Storage plant. Because this is a critical plant, the new governor system features fully redundant PLC controls and feedback sensors, as well as redundant hydraulic control manifolds. This paper provides an overview of redundancy concepts and a description of the redundancy and fail-safe features included in the Helms governor design.

## Introduction

The impressive Helms Pumped Storage Facility is PG&E's largest hydro powerplant and features three 404MW generators. The facility involves two different lakes at different elevations in the Sierra National Forest. Water is pumped to the upper lake during periods of low power demand and used to generate power during peak power demand periods. The powerhouse (shown at right) is embedded more than 1,000 feet within the side of a massive granite mountain. Commissioned in 1984, Helms provides power for about 850,000 homes in California.

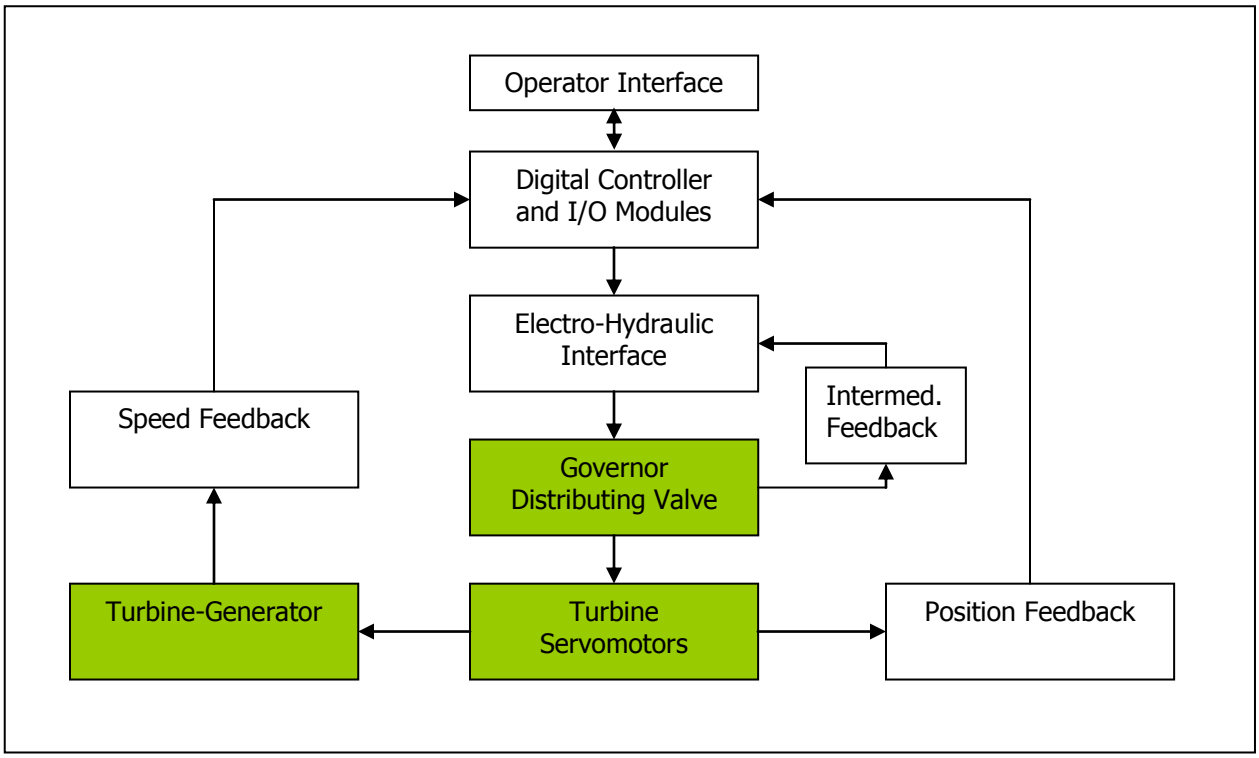
As part of major plant controls, excitation and protection upgrade project begun in 2007, PG&E chose to modernize the original governors and convert them to digital control. The original equipment governors were Woodward Governor Mod II Analog Electronic units that had provided reliable service for over 20 years and were still supported, however; they did not offer the redundancy features PG&E sought. A single point of failure could sideline a unit. With the important role these large units played in satisfying the demands of the California power market, this was unacceptable.

PG&E also desired better integration of the governors in their Supervisory Control and Data Acquisition (SCADA) system. In addition to providing local and remote operators a simpler means of dispatching a unit under various Pump or Generate modes of operation, digital governor systems can also communicate status and alarms so that operators and technicians can diagnose and troubleshoot system problems quicker.

In 2008, American Governor Company was selected to provide the first of three digital governor conversions, and worked closely with PG&E and their engineering consultant to design a redundant governor conversion system with no single point of failure.

## Overview of Redundancy Concepts

The diagram below presents a simplified arrangement of a digital governor system:




In a powerplant with a digital governor, the most likely components to fail are the field devices: the electronic position and speed feedback devices connected to the turbine-generator equipment. They are typically the first point of entry for harmful electrical surges and can also be subjected to physical damage or mis-wiring during routine maintenance. Power surges or lightning strikes can also take out the digital controller's power supply. Most of these problems can be avoided by using proper surge control and grounding techniques. The next level of defense is to provide redundant devices and include algorithms in the controller to smartly detect when a feedback signal or power supply has gone bad. In this way the unit can continue operation in the event of a failure of one of these components.

Higher up the food chain are the input/output modules the field devices connect to. Surges can sometimes make their way past the field device and into the module,

causing it to fail. Fail-safe systems in the governor will cause the unit to shutdown in a controlled manner, however, the system is out of service until the module can be replaced. Having redundant input/output modules in conjunction with redundant field devices can prevent a failure in one path from causing a unit shutdown.

So far we have been focusing primarily on feedback devices. There are also control devices that need to be considered. The Electro-Hydraulic Interface (EHI) provides the connection between the digital controller and the existing governor distributing valve, which is typically retained during the conversion. The EHI consists of a proportional control valve, a solenoid valve for emergency shutdown, and shuttle valve manifold assembly. During normal operation, the EHI ports oil via the proportional valve to hydraulically position the distributing valve, which in turn ports larger volumes of oil to the servomotors to move them to the desired position at the desired rate (subject to mechanical rate limits). Intermediate position feedback is required to close this inner control loop.

If the proportional valve or intermediate feedback system fails, position control of the turbine servomotors is lost, which is an emergency condition that triggers unit shutdown. To protect against this failure mode, redundant EHI systems can be specified. This provides two independent paths for controlling servomotor position, and smart algorithms in the controller can detect a failure in either the proportional valve or the intermediate feedback device and switchover to the other EHI.

At the top of the food chain is the digital controller's central processing unit (CPU) module, the brain of a digital governor that also contains the governor program code. Highly reliable and well isolated from field devices, this component is the least likely to fail. This has been proven over decades of use in powerplants. Yet, to prevent any single point of failure, redundant CPUs can be specified. Various interrogation algorithms can be employed to determine whether the Primary or Backup CPU should be in control of the unit. For maximum redundancy, two complete PLC racks (CPU and I/O modules) can be specified.

Finally, a word on the operator interface. A color touchscreen is commonly provided with digital conversions. It communicates with the governor controller and provides a wealth of information for the control and monitoring of the unit locally. However it is not a single point of failure, since the governor operates independently and does not need this device in order to function. In terms of back-up operator controls, local meters and switches can be provided (or retained if they exist) during the conversion. The governor may also be controlled remotely via communication link to a remote supervisory system. If neither is available, a backup touchscreen can be provided.

# Redundancy Approach Taken at Helms

PG&E sought the highest level of reliability for this critical plant, and the redundancy employed reflects this. This section examines the various redundant systems from the ground up.

### *Gate Position Sensing*

Redundant magnetostrictive linear displacement transducers (MLDTs) are provided in the turbine pit and are wired to separate analog input modules in each controller. They provide direct, electronic feedback of turbine servomotor position. A typical redundant MLDT installation is shown at right. Algorithms in the Governor detect failure of either transducer, trigger the Governor Trouble alarm, and specifically indicate the alarm on the HMI. In the event both transducers fail, an emergency shutdown is initiated.

### *Speed Sensing*

Primary speed sensing is performed by an American Governor PT Interface Module connected to a generator Potential Transformer (PT). PT speed sensing provides a better speed signal for on-line governing than shaft-mounted pick-ups because the PT speed signal is much less affected by generator shaft runout. The PT interface module transforms the AC signal to a 24 volt square wave. The processed signal is routed into the Allen-Bradley Configurable Flow Meter (1756-CFM) module. The module is configured for high resolution frequency mode, with a module accuracy of 0.00045HZ. The speed data is transferred to the CPU via the backplane.

This configuration yields two PT speed signal values because the 24 volt square wave is routed into both the A and B channels on the CFM module. This provides a limited amount of module redundancy because the customer's PT system and the PT interface module are common to both signals.

PT speed sensing is compliant with IEEE 125 "IEEE Recommended Practice for Preparation of Equipment Specifications for Speed-Governing of Hydraulic Turbines Intended to Drive Electric Generators." Algorithms in the Governor detect failure of the Primary speed signal, trigger the Governor Trouble alarm and automatically switch to the back-up speed sensing.

Back-up speed sensing utilizes two active proximity probes (also called Zero Velocity Pickups or ZVPUs) that are brought in directly to an Allen-Bradley High Speed Counter (1756-HSC) module. The probes are mounted on the existing Woodward SSG and

monitor the main drive gear teeth. As the teeth pass the probes a square wave signal is generated. While the speed signals generated by the proximity probes are not as accurate as the PT method, the ZVPUs can reliably detect rotational speed down to 0.0 rpm and are thus ideally suited for brake actuation and creep detection. The ZVPU speed signals are also preferred during starting and stopping sequences.

Algorithms in the Governor detect failure of the Backup speed signals, trigger the Governor Trouble alarm, and specifically indicate the alarm on the HMI. In the event all speed signals fail (PTs and Proximity probes), an emergency shutdown is initiated.

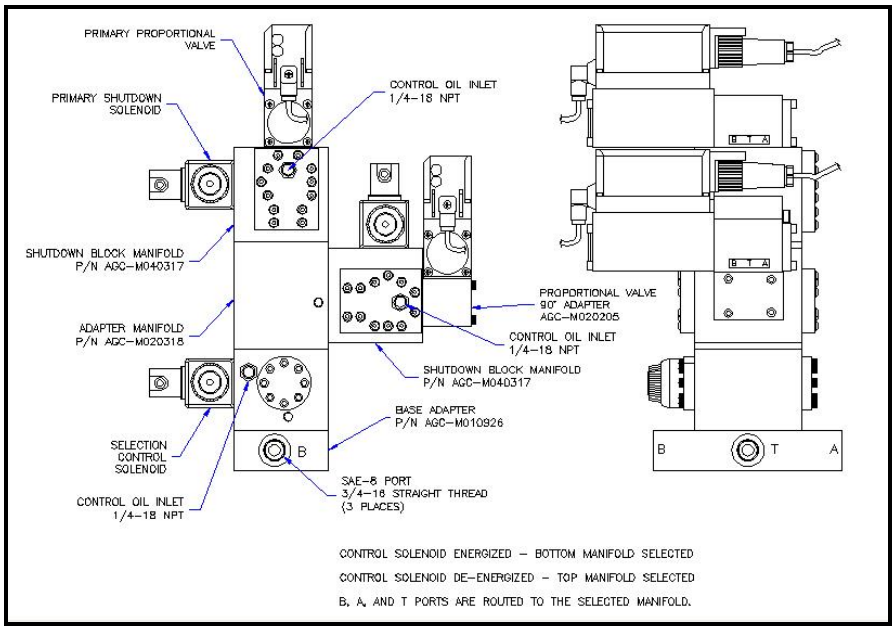
Both the Primary and Back-up speed signals are monitored continuously for an overspeed condition. The overspeed trip logic has an operator configurable trip level. In addition, the existing mechanical overspeed in the Woodward SSG is retained to provide an overspeed trip that is independent of the governor control system.

### *Governor Control Power*

Redundant 125/24VDC cabinet power supplies with alarm contacts and diode switching systems for bumpless transfer are provided to power field devices and output relay coils. Also, each governor PLC control rack has its own 125VDC power supply module.

### *Electro-Hydraulic Interface (EHI)*

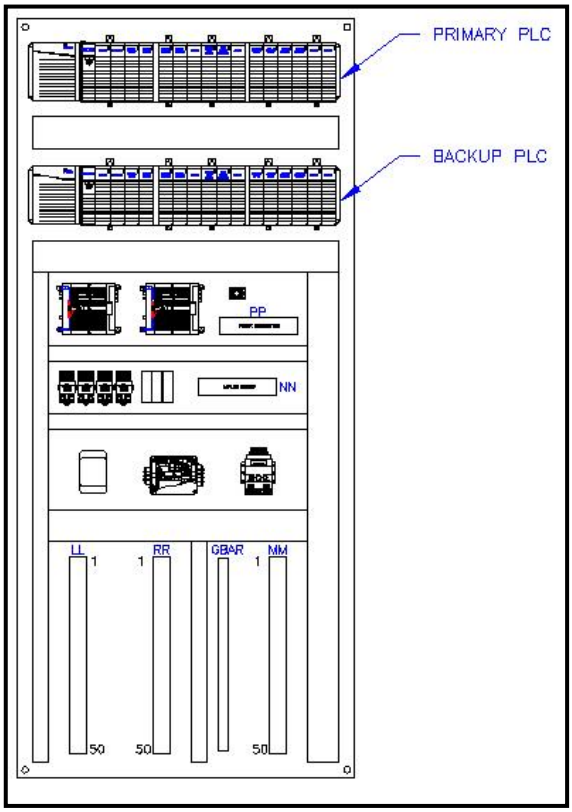
Redundant EHI manifold assemblies are provided, each with a proportional control valve and solenoid shutdown valve. Each EHI also has its own electronic LVDT feedback device for distributing valve spool position to close the intermediate feedback loop. Each EHI system is thus completely independent. The two EHIs are mounted on a solenoid-controlled switchover manifold that enables the switchover from the Primary EHI to the Backup EHI in the event of a component failure in the Primary.




*Arrangement diagram of redundant EHI manifold assembly*

*Side and rear views of installed redundant EHI manifold assembly and LVDT feedback devices*

## *Governor PLC Control System*




Redundant Allen-Bradley Control Logix™ programmable logic controller (PLC) racks are provided in a Primary / Back-up configuration. CPU, memory and I/O modules are all redundant, and the redundant feedback signals are shared between the controllers to further enhance reliability of the system. Each PLC rack has its own power supply, and redundant cabinet power supplies are provided with diode switching to power the interposing relays and field devices. PLC status and alarms are communicated to the local operator interface touchscreen as well as the SCADA system.

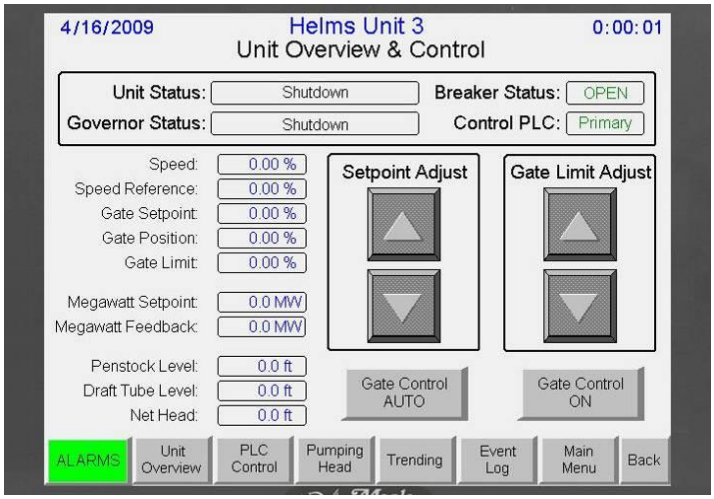
The PLC arrangement is shown at left. The rear panel (not shown) of the dual-access governor control cabinet contains the interposing relays and field terminal blocks. The dual-access cabinet was specified to save space.

The controllers have identical operational software installed. After the programs are downloaded, bits are selected in each controller that allows them to be identified as either the Primary or Backup.

Under normal operation, the Primary controller is operating to control the unit and the Backup controller is in a following mode.

The Primary and Backup communicate in two ways. An Ethernet link connects the two systems together and data is exchanged at 10ms intervals. The shared data is monitored to verify such things as operational mode, faults, alarms, setpoints, I/O values, and heartbeats.

Each controller also has a relay output that drives a discrete input to the other controller. When the relay is energized it tells the other controller that it is functioning and ready to assume control of the wicket gates if required. This hardware link has been made available to reduce the absolute reliance on the Ethernet link.




A color touchscreen Human Machine Interface (HMI) is provided at the unit for local operator control, monitoring and diagnostic capabilities.

The Unit Overview screen is shown at left. Multiple other screens are easily accessible via navigation buttons at the bottom of each screen.

**Managing Inputs and Outputs**

The PLCs both need to have access to the system inputs and outputs. While the inputs are relatively easy to manage, the outputs require a bit more attention.

The Discrete Inputs are directly routed to both the Primary and Backup systems. This has little or no impact on the external system because of the high impedance of the discrete inputs.

The analog inputs have been routed to both the Primary and Backup systems, but the implementation is different between the Primary and Backup. Because of the nature of the Allen-Bradley input modules in use, a 4-20mA signal cannot be daisy chained through two modules. The RTN (DC common) input to the module are not isolated, thus the current exiting the module is not guaranteed to be the same as the current entering; there is an alternate path available internal to the module through other analog signals. A solution to this concern was found through special configuration of the Primary and Backup analog input modules.

The discrete outputs from the Primary and the Backup drive the same set of interposing relays. Because of this sharing, the behavior of the discrete outputs must be tightly controlled depending upon the situation. Control algorithms coordinate the outputs from both PLCs. This insures a bumpless transfer, coordination between signals and failsafe operation.

The analog outputs from the Primary and the Backup drive the same external devices. The exception to this is the valve drivers: the Primary and Backup each drive their own proportional valves.

Special considerations were taken to prevent signal cross-feeding and to insure accurate signal sourcing.

All the other analog outputs are routed through diodes to prevent one PLC from back feeding the other. Because the currents would otherwise sum together, when a PLC is not in control, its analog outputs are forced to zero milliamps.

## Automatic Switching Operation

The system has been designed such that the Primary PLC is controlling the unit under normal operations. It is only when a severe fault occurs that the Primary will transfer control to the Backup.

Faults that will initiate a transfer to Backup include all Major PLC faults and gate driver failure. Major PLC faults include module failures, loss of communication with an I/O module, CPU RAM failure, loss of executable program, stack overflow, watchdog timer expired, and variable out of its designated range. If the Primary PLC loses power or the power supply fails, the transfer will be initiated as the "status relay" de-energizes and the Backup assumes control of the redundant EHI.

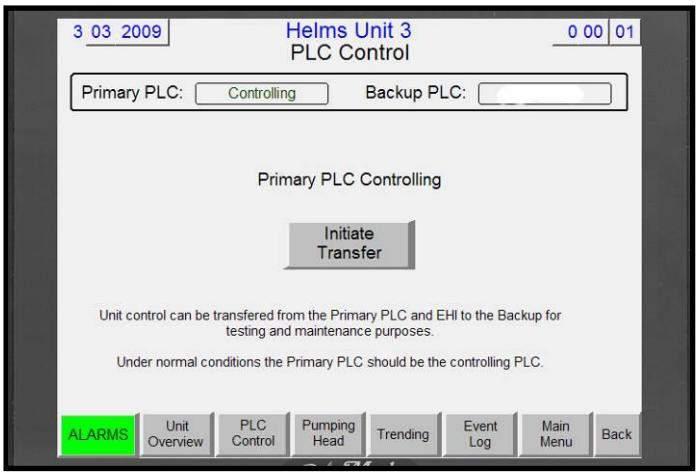
The automatic switch from Primary to Backup is a one way process. The Backup will NOT automatically transfer back to Primary even after the faults have been cleared. This has been done to prevent any scenarios where the system control is repeatedly bounced back and forth because both controllers are experiencing the same problem and they cannot communicate the situation properly.

In the event of a severe fault, the Primary will relinquish control to the Backup if the Backup is in good health. If the Backup is not ready, the unit will trip and shutdown safely. If the Backup assumes control and then encounters a serious fault, it will NOT try to transfer back to the Primary. It will trip the unit and shutdown safely.

Control can only be switched back to the Primary by operator intervention. It is recommended that this be done after the fault has been fully explored and the unit is shutdown.

## Manual Switching Operation

The system control can be manually swapped from the Primary to the Backup through the HMI control screens. A sample of the HMI screen is shown below. In order for the swap to be possible, both controllers must be in good operating condition. The communications link must also be active.




When voluntarily transferred, the non-controlling unit has a 1 second overlap to power up its dedicated EHI (proportional valve and shutdown valve) and start controlling the distributing valve. The overlap minimizes any disturbances in the control system.

The Primary and Backup can be switched back and forth as many times as desired.

It is recommended that the manual switching operation be performed bi-annually to exercise the backup system. The switching should be done in Generate mode with the unit at synchronous (100%) speed with the breaker open. No disruptions are expected during the switching process, but prudence is always the best course of action. The unit may be put on-line after the swap has been initiated.

**Interface to Hydraulic Control Assemblies**

The Primary PLC is wired to the (top) Primary EHI assembly while the Backup PLC is wired to the (side) Backup EHI assembly. The Backup's proportional valve and shutdown valve are not energized when the Primary is in control. By keeping the hardware in its shelf state, it will not be subjected to premature and undetected failure.

A switching solenoid controls which manifold actually controls the distributing valve and therefore the wicket gate position. The Backup controller is responsible for energizing the switching solenoid and taking control of the wicket gates when the Primary fails or faults.

During normal operations, the switching solenoid at the base of the assembly is de-energized and the Primary (top) EHI assembly is in control of the distributing valve hydraulics. If the associated shutdown solenoid is energized, the proportional valve is free to accept milliamp commands from the Primary PLC and move the distributing valve and therefore, the wicket gates. The status of the Backup shutdown block manifold assembly does not affect the operation of the Primary assembly.

If the system control transfers to the Backup PLC, the switching solenoid at the base of the assembly is energized and the Backup (side) EHI assembly is in control of the distributing valve hydraulics. The Backup PLC controls the relay that energizes the switching solenoid. Once again, if the associated shutdown solenoid is energized, the

proportional valve is free to accept milliamp commands from the Backup PLC and move the distributing valve, and therefore, the wicket gates. The status of the Primary shutdown block manifold assembly does not affect the operation of the Backup assembly.

The Primary PLC and Backup PLC are directly wired to their respective shutdown block manifold assemblies. Each PLC can only drive the shutdown block manifold that it has been connected to.

## Operator Interface and SCADA Communication

At Helms the unit governors will normally be controlled from either the Control Room or from a remote Dispatch Center. Both methods utilize a ModBus communication link from the SCADA system directly to the digital governor. Under normal operation, control commands, alarms, and status information are passed back and forth over the Modbus communication link.

A local operator touchscreen is provided at the unit to provide local control in the event of a SCADA failure, as well as for routine maintenance and testing. Both governor PLC systems communicate with the touchscreen, so operators and technicians can see alarms from both systems and can take control of the unit locally.

## Conclusion

The first fully redundant digital governor system for Helms successfully passed a thorough Factory Acceptance Test in 2008 and was being installed in the powerhouse as this paper was being written. Site start-up and acceptance testing is expected to occur in May 2009 and the results will be presented orally.

## Author

Roger Clarke-Johnson is the Western Region Manager for American Governor Company. He has over 20 years of experience with hydro governor systems and technology, ranging from mechanical to analog to digital governors. Prior hydro experience includes similar positions at GE, Woodward and Digitek.