Insight: Steam Turbine Fail-Safe Electronic Overspeed Protection

Essential for the Safe Operation of Steam Turbine Generating Units

Recognizing the Risk

Well configured overspeed protection systems are critical to the safe operation of power generating plants. We have seen this point clearly demonstrated in a serious steam turbine overspeed event that occurred recently. In this particular case the failure of a single UPS (Uninterruptable Power Supply) rendered critical trip commands inoperable, whilst simultaneously tripping the unit by opening the generator circuit breaker. The loss of these protective features meant that the turbine steam valves did not close properly, with the unfortunate result that the unit very quickly overspeed to complete destruction.

This Insight article describes the event, the root cause behind it and highlights best practices to adopt in the design, installation and maintenance of these critically important control systems.

Sequence of Events

The UPS failure resulted in the loss of the critical 230V AC power that furnishes 110V AC and 24 V DC power to the plant control system, including the steam turbine generator controls. The loss of the UPS power source initiated a relay action which removed the generator from the grid by opening the generator circuit breaker. Due to the simultaneous loss of power to the turbine generator controls, the turbine protection and trip systems were no longer functional. A turbine trip signal from the generator breaker trip contacts failed to reach the 220V DC turbine trip solenoid. As the speed increased due to the loss of generator load, the overspeed protection system was unable to monitor the speed or initiate a trip as this protection logic required the 24V DC turbine protection panel power supply which was supplied by the UPS, which had just failed. Speed very quickly increased until the generator retaining rings failed, destroying the generator and initiating a significant lube oil fire. The steam turbine also suffered very serious mechanical damage at this point.

The possibility that an operating steam turbine can be left without overspeed protection is an unacceptable risk. Overspeed protection must be fail-safe and remain functional regardless of any failure to the main power supply.

Deficiencies in the Overspeed Protection

This incident revealed critical flaws in the plant and steam turbine generator controls as the loss of a single UPS rendered the turbine protective and trip commands inoperable. Investigations revealed the following:

- In this particular system, the turbine protective schemes required power from the UPS in order to protect the turbine generator i.e. once power lost:
  - A signal from the generator trip could not trip the turbine.
  - An overspeed trip could not function as the logic required (3) relay actions that relied upon the 24V DC power supplied via the AC UPS system.
- The turbine overspeed protective scheme was incorporated in the turbine controls and not as a separate, independent system. When power was lost to the main control system, so was the overspeed protection.
- The turbine overspeed and other emergency trip schemes were not “fail-safe” such that they would automatically trip upon loss of critical control power. Instead the overspeed trip was designed as “energize to trip”, and was incapable of functioning once power source was lost.

Actual System Design

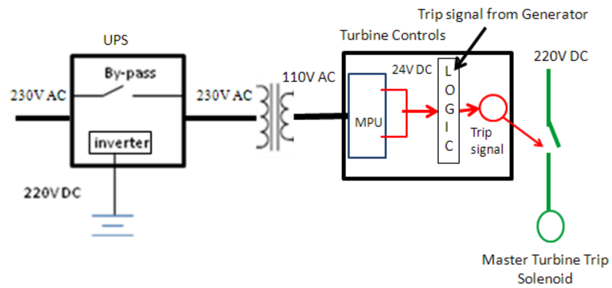

Figure 1 Illustration of the UPS and control system in use at the power plant

In this design the system fails in the following manner: Loss of the single UPS => Loss of 110V AC => Loss of turbine control 24V DC => Loss of turbine protection logic => Loss of the ability for master trip of turbine on the 220V DC supply.

Preferred System Requirements

The ideal power and control system should be able to maintain integrity in the event of a single UPS failure. Essential trip systems also need be capable of operating independently. Accordingly it is recommended that the following installation requirements be adhered to in the design of turbine electronic overspeed trip systems:

- The trip system must be independent of other control systems.
- Trip system must not be jeopardized by a single failure of any one component or power source.
- Trip solenoids must “de-energize” to trip.
- Trip scheme must be fail-safe and set to operate on the loss of power supply, the speed sensing signal, or power to the trip coil.
- The trip system must be a single action to trip the turbine once the requirement has been met.
- The trip control system must be installed in a keyed & locked cabinet. Only trained personnel should be allowed access.
- Trip system processor function must not rely on a forced ventilation system that could be impaired by fan failure or power outage.
- Signal cables and power supply cables must be installed separately on separate paths. Power supplies must be fed from separate sources.
- The trip system must be pretested prior to operation of the unit to prove it is fully functional before start up.
- System software and configurations must be password protected.
- System software and configurations must only be accessed by trained personnel.
- System must be tested quarterly at a minimum.
- The mean time to repair a system is fixed to 8 hours. (Access to trained personnel within 2 hrs.)
- An exchange module set must be available on site. (sensor, configured channel module, power supply)
- Sufficient training must be provided to all operators.

Preferred System Layout

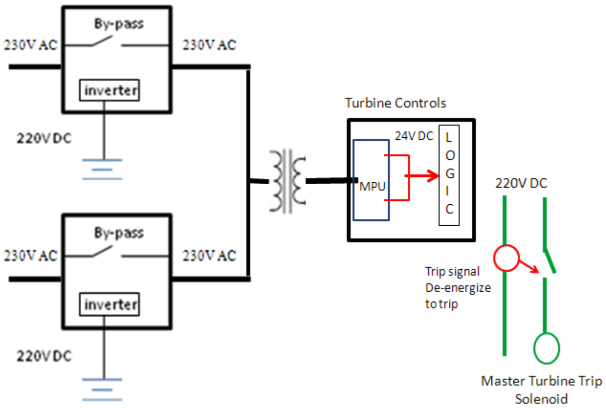

Figure 2 Redundant UPS supplies with separate & “fail safe” turbine protective trips

Recommendations

It is recommended that operators, and / or a competent 3rd party, or the OEM (Original Equipment Manufacturer) review the turbine control & protective schemes to:

- Verify that the overspeed system is not exposed to a single point of failure that interrupts control power to the turbine.
    - Verify that the turbine overspeed protection system has redundant power supplies such that at a single failure will not interrupt critical power.
    - Verify that speed sensing, processor, and trip signal function are triple modular redundant, so no one failure will render the system non-functional.
    - Verify that there are no time delays or other logic requirements that requires power to create a change in state to affect a trip.
- Create a written operations procedure that:
    - Tests the overspeed system functionality on a regular basis.
    - Reviews the operational status of the overspeed system regularly.
    - Requires that if an overspeed protection system trouble alarm occurs, it is addressed within 2 hours and a repair is completed within 8 hours. If this is not possible the unit should be shut down in a controlled fashion until the overspeed system can be corrected.
- Verify that all trip commands will trip the turbine regardless of the operational capability of the UPS power supply to turbine controls (best practice is to send the trip signal directly to main trip solenoid and not through the control panel).
- Verify that the steam turbine generator will safely trip when all control power is lost i.e. fail-safe”.

Conclusions

Electronic overspeed systems are normally reliable. However If the electronic overspeed system is incorrectly specified, designed, installed, or maintained it can leave a client exposed to a large potential loss. It is critical that the overspeed protection system continues to function in the event of a failure of a single UPS (single point failure), or if power is lost to the turbine controls.

It is recommended that owners/operators review their turbine control and protection systems and verify that their overspeed protection system adheres to appropriate International Organization for Standardization (ISO) and American Petroleum

Institute (API) guidance and will function in the case of a single point failure or initiate a turbine trip on loss of the critical power supply.

References & Resources

API 612, 2005 Petroleum, Petrochemical and Natural Gas Industries-Steam Turbines-Special-purpose Applications, Sixth Edition

API 670, R(2010) - 2000 Machinery Protection Systems, Fourth Edition

ISO 10437, 2003 Petroleum, petrochemical and natural gas industries - Steam turbines - Special-purpose applications

AIG Insight, Steam Turbine Mechanical Overspeed Trip Devices - Outdated mechanical trip devices should be replaced with electronic devices

For more information, contact your local AIG Risk Engineer.