Insight: Standby DC Supply System Criticality

Recognizing the Risk

Well configured UPS (Uninterruptable Power Supplies) systems are critical to the safe operation of power generating plants. We have seen this point clearly demonstrated in a serious steam turbine over-speed event that occurred recently. In this particular case the failure of a single UPS 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 over-sped 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

When the UPS failed there was a loss of the critical 230V AC power that furnishes the 110V AC and 24 V DC supply to the steam turbine generator controls. A fundamental consequence of losing the UPS system was a simultaneous initiation of a relay system removing the generator from the grid by opening the generator circuit breaker. Without the UPS, turbine protective and trip systems became completely inactive and a turbine trip signal from the generator breaker controls failed to reach the 220V DC trip solenoid. As turbine speed increased with the sudden and dramatic loss of generator load, the over-speed protection system was unable to monitor the speed or initiate a trip, since this system required the 24V DC power to function. Speed very quickly increased until the generator retaining rings failed, destroying the generator and initiating a significant fire as lube oil escaped from ruptured pipes, igniting on the hot steam lines. The steam turbine also suffered very serious mechanical damage at this point.

The incident investigation revealed that for several months prior to the event the plant had problems with frequent UPS warning alarms and some operational issues with the UPS and static bypass switch. The static bypass switch was inoperative at the time of the failure.

Deficiencies in Plant Control Systems

This incident revealed critical flaws in the plant and in the design of the steam turbine generator controls. In this example critical controls were powered from a single UPS without a back-up source. The loss of this single UPS therefore rendered turbine protective and trip commands inoperable. Key observations highlighted by the incident investigation are as follows:

- The UPS was the only source of power for turbine protective tripping scheme actuation. Its failure meant that there were no active controls to protect the turbine generator from destruction.
- There was no fail-safe shut down procedure for the turbine generator upon loss of critical power from the UPS. In fact, with the control scheme in place, the loss of the UPS was designed to trip the generator breaker but would not trip the turbine. This was certain to result in the over-speed and destruction of the turbo generator unit.
- The UPS had a history of alarms and minor failures that were not adequately addressed by operations or maintenance groups at the plant.
- Plant operations and maintenance departments did not fully understand the critical importance of the UPS.

Design of UPS at Power Plant

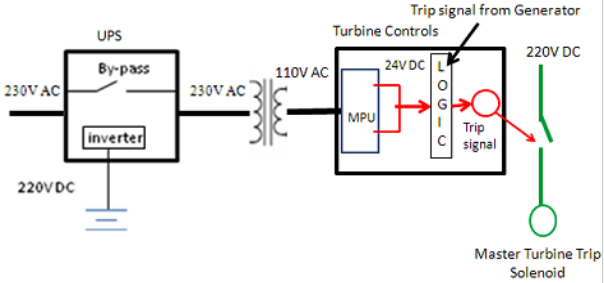

Figure 1 Illustration of the UPS and control system in use at the power plant

With 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.

Recommended Design Requirements for UPS Schemes

The following installation guidelines indicate the ideal requirements for UPS systems.

- Critical turbine control circuits must be provided with redundant power sources such that one single failure of a UPS or other component will not result in loss of protection. (THESE POWER SUPPLIES MUST BE CONSIDERED CRITICAL EMERGENCY POWER TO BE MAINTAINED DURING LOSS OF GRID.)
- The preferred arrangement is to have protective circuits and relays separate from other controls and powered from a secure DC supply.
- The main and alternate power sources are required to be sized to supply all emergency loads simultaneously. If a battery is to be considered an alternative source it must be capable of supplying power even if the UPS is lost.
- Transfer between power sources must be sufficiently fast to maintain function of protective schemes during transfer between either grid or battery.
- UPS/emergency systems must be tested periodically on a schedule acceptable to the authority having jurisdiction to ensure the systems are maintained in proper operating condition. A written record must be kept of these tests. This includes regular testing of the batteries, including periodic load testing. The authority having jurisdiction must conduct or witness a test of the complete system periodically.
- Battery systems that are part of the UPS/ emergency system must be periodically maintained to ensure serviceability.
- Periodic power source interruption tests should be carried out to insure transfer switches are functional and that the back-up system has sufficient load carrying capability.
- Audible and visual signal devices must be provided for the following:
    - Indicate loss of the emergency source
    - That the battery is carrying load
    - That the battery is not functioning
    - Indicate a ground fault in solidly-grounded wye systems. The sensor indicating ground-fault must be located at or ahead of the main system disconnecting from the emergency source.
- All boxes and enclosures for critical/emergency circuits must be permanently marked so that they will be readily identified as a component of a critical circuit or system.

- Wiring from a critical /emergency power source or emergency source distribution over current protection to emergency loads must be kept entirely independent of all other wiring and equipment. Exceptions apply where load equipment must have wiring from two sources
- The UPS should be installed in spaces or areas that are fully protected by an approved automatic fire suppression system.

Preferred Arrangement

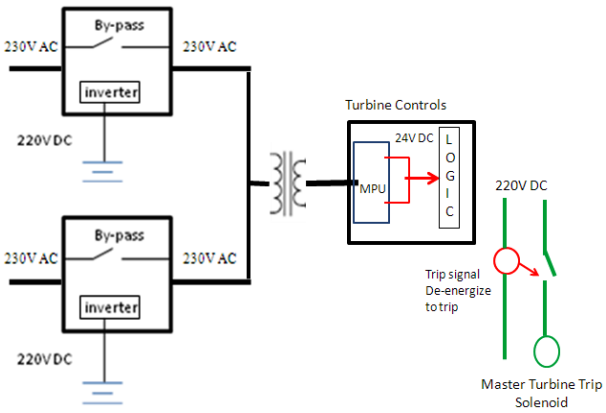

Figure 2 Preferred – redundant USP supplies with separate & fail safe turbine protective trips

Recommendations

It is recommended that operators, and / or competent 3rd party, or the original equipment manufacturer (OEM) review the UPS configuration and turbine control & protective schemes to:

- Verify that the turbine protection system has redundant power supplies such that at a single UPS failure will not interrupt critical power. IF THE TURBINE CONTROL AND PROTECTION SYSTEMS RELY ON A SINGLE UPS EXTRA DILIGENCE AND EXTREME CAUTION IS REQUIRED.
- Create a written operations procedure that:
    - Identifies and labels the critical UPS power source(s) that provides power to plant controls and protection schemes.
    - Requires regular checks and periodic operational tests of the UPS operating characteristics, system voltages and the back battery health. All checks to be documented.
    - Requires that if a UPS 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 UPS can be corrected.
    - Identifies what critical UPS system spares are maintained
- Verify that a generator trip command will trip the turbine regardless of the operational state of the UPS power supply to turbine control system. 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 trip when all critical power is lost i.e. “Fail Safe”

Conclusions

The critical nature of UPS systems is not always well appreciated. A control system relying on a single UPS source to power critical turbine protection systems can leave generation facilities exposed to catastrophic failure should this single source

UPS fail. Owners and Operators should review their plant's UPS/ critical power arrangements to ensure that protective circuits are not vulnerable to a single point UPS failure.

Referenced & Resources

National Fire Protection Association (NFPA) 70 National Electrical Code

Institute of Electrical and Electronics Engineers (IEEE) Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications, IEEE Std. 446-1995

National Electrical Contractors Association (NECA) 411 Standard for installing and maintaining Uninterruptible Power Supplies (UPS), National Electrical Contractors Association (2006)

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

International Organization for Standardization (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

*While NFPA documents are the global standard used by AIG, international equivalents may be acceptable.

For more information, contact your local AIG Risk Engineer.