Safety Alert

Date of Event: 16 May 2018

Binary Plant Safety System Compromised

What happened?

In investigating concerns raised by one of Contact's Generation Controllers it was observed that a Level 1 vaporiser high pressure trip had been activated at the end of March 2018 during a cold start up of G16 at the Wairakei Binary Plant. The trip activation did not immediately result in the plant being shut down by the hard wired Emergency Shutdown System (ESD; referred to as the Turbine Control Backup Relay or TCBR in the Ormat documentation). The plant did trip 4 minutes later through the PLC on low pentane temperature.

Investigation revealed a wiring fault which solidly earthed the 24V DC control supply 0V common on the switched side of the shutdown relay K3 in one of the field junction boxes. As the design of the ESD relies on K3 to break the common 0V leg of the control supply and thus force all of the pneumatic solenoid valves to assume their fail-safe state and the fact that the 0V leg of the control supply is earthed, K3 was defeated and activation of overspeed or high pressure trips would not result in an immediate shutdown as intended.

Wairakei Binary G15 was shut down and the same fault found on this unit. The two Te Huka Binary units were shut down and the ESDs on these units were confirmed to function correctly.

How did it happen?

As the wiring in the field junction box has not been disturbed since hand-over, it is probable that this fault has been present since construction. Examination of commissioning records show that the ESD was tested by activation of one of the E-Stop push buttons. The all of the initiating elements in the ESD chain are monitored by the plant PLC which controls the +24V DC supply to the pneumatic solenoid valves. As far as we have been able to establish at the time of writing, all of the ESD signals except the E-Stop push buttons only raise alarms; the E-Stops however do cause the PLC outputs to switch off thus deenergising the pneumatic solenoids to their fail safe state. Unless high speed monitoring was in place, the time difference between K3 being de-energised and the PLC turning off the supply to the solenoids would be indiscernible.

Following an apparently successful Emergency Shutdown test, the commissioning and subsequent return to service testing has assumed relay K3 being deenergised and un-latched demonstrates each element in the ESD to be working correctly.

What did we learn?

Effective end-to-end testing of all functions in an ESD is essential.

The design of the ESD is such that it is vulnerable to a common mode failure.

How can we improve?

Contact Energy is in the process of re-designing the Safety Functions on its Binary Plants and will be replacing the system with a dedicated Safety Controller and SIL rated components with enhanced diagnostic capabilities. Until this is completed, a full functional test of the ESD is mandated before restart of Binary Units.

Safety Alert

Get in touch...

Peter Moffat | Peter.Moffat@contactenergy.co.nz | 07 376-1974
or
Mathew Staddon | Mathew.Staddon@contactenergy.co.nz | 07 376-1919