SIS-TECH
12621 FEATHERWOOD, STE 120
HOUSTON, TX 77034
713-909-2100

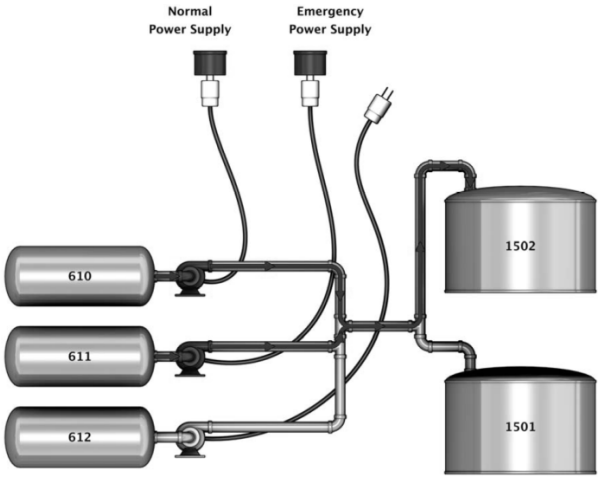
Case Study: Petrolia, Pennsylvania (October, 2008)

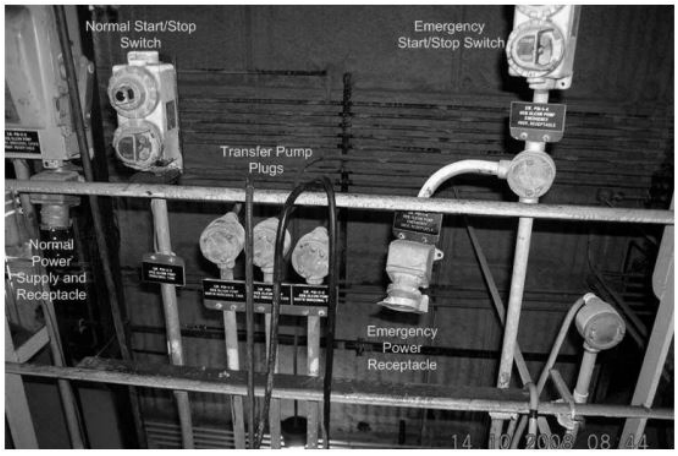
In the following example, inadequate management of a "temporary" automation change leads to a toxic gas release with community-wide impact.

Impact: Oleum release; 1 injured, plant and 2500 in local towns evacuated; roads closed.

Power Configuration Diagram

CSB Report Figures 5 and 4





Summary:

Twenty-eight years prior to the event, a “temporary emergency” power supply was installed at the oleum transfer pumps. The intention was to use this new power supply only during outages of the primary power circuit under closely monitored conditions. A management decision was made to use an operator response to alarm safeguard to protect the downstream tanks from overflowing instead of wiring the existing high level interlocks into the new power circuit.

This “temporary” automation change and the associated operating limitations were never incorporated into the facility’s PHA, operating procedures, other process safety information documents, or the control computer operating interface.

On weekends, this particular part of the facility was lightly staffed for only a few hours. One task during this time was to transfer as much oleum into the feed tanks as possible, to support production at the start of the week. Over the intervening years, the weekend operators developed a common practice to use the backup power source to run a second pump, speeding up the transfer of this critical raw material.

On the day of the incident, an operator was pumping oleum from vessel 611 using the primary power source and from vessel 612 using the backup power source. Status of the pump using backup power was not indicated on the DCS, and the pump could only be stopped locally while on backup power.

When the operator stopped pumping from vessel 611 via the DCS at end of the weekend shift, he inadvertently left the pump on backup power running.

When the feed tank eventually became full, a local high level alarm beacon activated on run tank 1502, but the operator had already left the control building.

Less than an hour later, sulfuric acid mist flowed out via the tank conservation vent. The mist was seen leaving the building. The release escalated when operators blew air through the transfer line, incorrectly suspecting a leak. An emergency was declared and the facility was evacuated, along with three nearby towns. About two hours later, the pump was stopped by cutting power to the oleum storage building.

Instrumentation and Controls Gaps:

- Second “temporary” power supply added 28 years prior to event, with decision to not use the same automated interlocks used on the primary supply and to rely only on operator response to alarm as a safeguard against overfill
- Change not incorporated into plant documentation or logic solver operator displays.
- Operator practice evolved to use the “temporary” power supply to run a second pump on weekends, without the close monitoring initially intended at the time of the installation of the “temporary” power supply
- Result was that high high tank level trip was effectively bypassed for the pump run on backup power
- High level alarm used as normal fill level; horn not working and no one present

Key Automation Learning Points:

Forces, jumpers, and temporary fixes can unintentionally become permanent if MOC is not robustly followed and key plant documentation is not updated. Hazard analysis and safeguard implementation are just as important for a facility change intended to be relatively short term as for a significant capital project. In this incident a "temporary" automation change became a 28-year undocumented latent failure.

Sources:

CSB. 2009. *INDSPEC Oleum Release Case Study*. Case study 2009-01-I-PA. Washington, D.C.: U.S. Chemical Safety Board..