

Sharing is Caring

ExxonMobil Rotterdam refinery fire Lessons from a complex restart



Description

On 21 August 2017, a major fire occurred in the Powerformer unit at the ExxonMobil refinery in Rotterdam, the Netherlands.

At approximately 19:35, an electrical short circuit tripped a compressor and caused a voltage dip that stopped the waste heat boiler fan. When exhaust gases from the unit's six furnaces were redirected to the boiler, pressure increased and the high-pressure protection shut down all six furnaces.

Although the cause of the disturbance had not been established, a hot restart was initiated to avoid excessive cooling and possible damage to the catalyst.

During the restart, operators were required to restart and stabilise six furnaces while receiving approximately 250 alarms every ten minutes. Several furnace protection systems also had to be temporarily bypassed.

A thermal-overload alarm activated for a circulation pump, which later stopped. Its failure was not recognised. The standby pump was under maintenance, but the panel operator did not know it was unavailable.

Loss of circulation caused the associated furnace to trip on low flow. However, the trip was not connected to the pump failure. The low-flow protection was manually bypassed and the furnace was restarted without confirming that liquid was circulating through its coil.

The coil overheated and ruptured. Hydrocarbons entered the furnace and ignited, while the contents of the connected distillation tower continued to feed the fire. Approximately 110 tonnes of liquid, mainly toluene and xylenes, were released.

There were no fatalities or injuries. However, the furnace was destroyed and the Powerformer unit remained out of operation for approximately one year.

Key findings

- The plant was restarted before the cause of the initial disturbance was understood.
- The low-flow trip worked as intended, but the protection was bypassed and the furnace was restarted.
- Manual bypassing had become normal practice because the approved five-minute automatic bypass was considered too short.
- The design allowed safety-critical protection to be bypassed, enabling the burners to operate without flow through the coil.
- The simultaneous restart of six furnaces and approximately 250 alarms every ten minutes contributed to the pump failure being missed.
- The standby pump was under maintenance, but the panel operator did not know it was unavailable.

Why does it concern me?

A restart is not simply the reversal of a shutdown. Plant conditions may have changed, equipment may be unavailable and the original disturbance may have affected other parts of the process.

A safety trip indicates that the conditions required for safe operation are no longer present. Bypassing the trip does not restore those conditions. It removes the protection that responded to them.

Ask the following questions:

- Do we understand why the plant or equipment tripped before authorising a restart?
- Can safety-critical protection be bypassed, and how are bypasses controlled and removed?
- Do operators know when standby or safety-critical equipment is unavailable?
- Could alarm flooding, workload or insufficient staffing prevent recognition of a developing hazardous condition?