



Mary Kay O'Connor Process
Safety Center
2006 International Symposium

<http://process-safety.tamu.edu>

The Relationship Between Automation Complexity and Operator Error

Russell A. Ogle, Delmar “Trey” Morrison and Andrew R. Carpenter

Exponent, Inc.

185 Hansen Court, Suite 100

Wood Dale, IL 60134

[*rogle@exponent.com*](mailto:rogle@exponent.com)

Abstract

One of the objectives of process automation is to improve the safety of plant operations. Manual operation, it is often argued, provides too many opportunities for operator error. By this argument, process automation should decrease the risk of accidents caused by operator error. However, some accident theorists have argued that while automation may eliminate some types of operator error, it may create new varieties of error.

In this paper we present six case studies of explosions involving operator error in an automated process facility. Taken together, these accidents resulted in six fatalities, 30 injuries and hundreds of millions of dollars in property damage. The case studies are divided into two categories: low and high automation complexity (three case studies each). The nature of the operator error was dependent on the level of automation complexity. We also consider for each case study the contribution of the existing engineering controls such as safety instrumented systems (SIS) or safety critical devices (SCD) and explore why they were insufficient to prevent, or mitigate, the severity of the explosion.

In the low automation complexity environments the operator errors tended to be simple lapses (unintentional action). The response time for error identification, diagnosis and correction was typically less than two minutes. This places an enormous time pressure on successful operator intervention. In each of these three cases, the operator was aware that there was a problem but was unable to successfully intervene.

In the high automation complexity environments, the operator errors were intentional but mistaken actions. The response time for error identification, diagnosis and

correction ranged from 30 minutes to six hours. In these cases it would seem that operator intervention could have been successful if the necessary data and alarms had been available. In each of these three cases the operator failed to detect the abnormal condition.