Available online at www.sciencedirect.com
ScienceDirect
Journal of Hazardous Materials 159 (2008) 135–141
Journal of Hazardous Materials
www.elsevier.com/locate/jhazmat

The relationship between automation complexity and operator error

Russell A. Ogle *, Delmar "Trey" Morrison III, Andrew R. Carpenter

Exponent, Inc., 185 Hansen Court, Suite 100, Wood Dale, IL 60134, United States

Received 14 December 2007; accepted 11 January 2008
Available online 31 January 2008

Presented at the 2006 International Symposium, "Beyond Regulatory Compliance: Making Safety Second Nature," Mary Kay O'Connor Process Safety Center, Texas A&M University, College Station, Texas, October 2006.

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. For each case study, we also consider 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.

Keywords: Process automation; Complexity; Operator error; Case studies

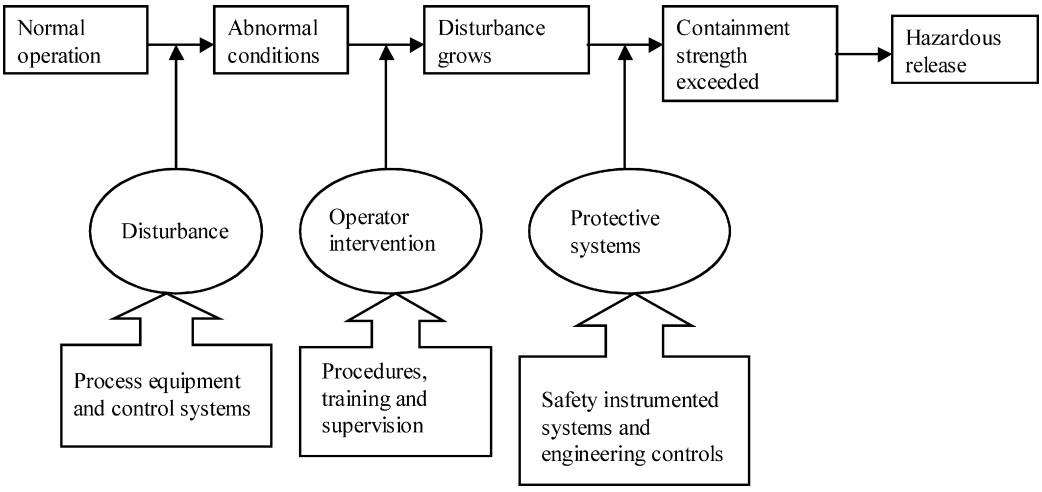
1. Introduction

Several factors are required for the successful operation of chemical process facilities. One of these factors is the control of physical and chemical processes to maintain the desired operational characteristics. The plant operator plays a central role in the control mission. Since the 1960s, there has been a dramatic growth in process automation [1]. This has been stimulated by an interest in both reducing the intensity of manual operation and in increasing the safety of the process by reducing the potential for operator error. But numerous case studies have shown that simply replacing a manual control action with an automated control action does not necessarily reduce the risk of a severe accident [2,3]. Accident prevention requires a balanced analysis of hazards and their control with due consideration of the interactions between the operators, the process equipment, the control systems, and the environment.

A useful accident model for chemical processes is the barrier analysis model [4]. The accident event is a loss of containment of hazardous chemicals or energy. The accident model consists of an initiating event that propagates a disturbance through the system. Operational responses and physical barriers act to reduce (or magnify) the magnitude of the disturbance. The outcome is either success or failure of containment [5,6]. This accident model is illustrated by the figure below.

* Corresponding author.
E-mail address: rogle@exponent.com (R.A. Ogle).

0304-3894/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2008.01.065



Several organizations have published guidelines and standards for safe process automation. For example, the Center for Chemical Process Safety (CCPS), a technical society of the American Institute of Chemical Engineers (AIChE), published a book on safe process automation in 1993 [7]. Following that, the Instrumentation, Systems, and Automation Society (ISA) published a standard for safety instrumented systems (SIS) [8] and the International Electrotechnical Commission (IEC) published their SIS standard in 2003 [9]. These publications address the design, operation, and maintenance requirements for SIS technologies.

AIChE followed these publications with an important contribution to risk assessment involving process automation and safety [6]. This risk assessment methodology, called layer of protection analysis, emphasizes the importance of considering the effectiveness of operator intervention, safety instrumented systems, and engineering controls to prevent or mitigate a hazardous release. Although intended as a semi-quantitative risk assessment methodology, it is also useful as a qualitative accident investigation tool. For a given risk scenario, one must decide how much reliance will be placed on the use of operator intervention, safety instrumented systems, and engineering controls. A qualitative form of layer of protection analysis can assist the accident investigator in evaluating this allocation of safety function.

Too often, facilities rely on operator intervention as their primary line of defense without assessing its potential for success in a given risk scenario. When the risk scenario materializes, the facility may discover that operator intervention may not be successful. When such an accident occurs, it is important to determine if it is the result of simple operator error or if it is indicative of a more systemic deficiency. In this paper we present six case studies of explosions involving operator error in an automated process facility. Taken together, these explosions 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 or safety critical devices (SCD) and explore why they were insufficient to either prevent or mitigate the severity of the explosion.

2. Background

The analysis of the accident case studies relies on three characteristics: layer of protection analysis, automation complexity, and operator error.

The layer of protection analysis (LOPA) methodology introduces an important concept helpful for accident investigation: the independent protection layer. The independent protection layer (IPL) is defined as a device, system, or action that is capable of preventing a risk scenario from proceeding to the undesired consequence. IPLs, listed below, follow a natural hierarchy in the order from initiating event to accident outcome:

1. Basic process design.
2. Basic process control system.
3. Critical alarms and operator intervention.
4. Safety instrumented function.
5. Physical protection devices.
6. Post-release physical protection.
7. Plant emergency response.
8. Community emergency response.

Items 1 and 2 are generally not counted as IPLs. For the purposes of accident investigation, we focus our attention on items 3, 4 and 5 with the intent of identifying means for preventing a loss of containment.

Automation complexity refers to the number and connectivity of the information streams that the operator must monitor and maintain. We use it in this study in a qualitative manner:

- Low automation complexity is defined as a situation where the operator is interacting with a single control loop.
- High automation complexity is defined as a situation where the operator is interacting simultaneously with multiple control loops.