IChemE

www.icheme.org/psep
doi: 10.1205/psep.05184

0957–5820/06/$30.00+0.00
© 2006 Institution of Chemical Engineers
Trans IChemE, Part B, May 2006
Process Safety and Environmental Protection, 84(B3): 174–178

LESSONS FROM HUMAN ERROR INCIDENTS IN PROCESS PLANTS

D. C. HENDERSHOT[*]

Chilworth Technology, Inc., Plainsboro, New Jersey, USA

This paper describes four human error incidents in chemical process plants which I have personally observed, and discusses specific lessons from each of them. As often stated by Trevor Kletz, people respond to stories and examples, and hopefully these incidents will be useful in preventing similar incidents in the future. Fortunately none of the incidents resulted in serious safety consequences, although all cost some money and productivity. And, under other circumstances, similar errors in a more hazardous operation could have had serious safety consequences.

Keywords: case histories; human error; control software errors; construction errors; plant automation.

INTRODUCTION

We often think of human error in terms of plant operations, but it is important to remember that plants are designed and built by human beings, and that errors can occur during design and construction of a plant as well as during operation. The first two incidents occurred in a plant which was highly automated. Extensive automation and computer control creates many new issues in process safety, which have been extensively discussed in the literature, for example, by Leveson (1995), Kletz (1991) and Kletz *et al.* (1995). This particular plant was one of the early applications of extensive automation and recipe driven control to a batch manufacturing plant in the company. During the first couple of years of operation, there were a number of incidents which some people might describe as ‘computer errors’ or ‘automation errors’, but which are in fact human errors on the part of the control software programmers. The third incident is also a construction error—incorrect wiring of field instruments to a computer control system which remained undetected for a long time following construction. The fourth incident is an operating human error, in which I personally played a significant role.

INCIDENT 1: OPERATIONAL DETAILS REALLY MATTER

A specified amount (a couple of thousand gallons) of a dilute aqueous solution of an organic acid was being pumped from a storage tank in a tank farm to a process weigh tank. Because the material was low hazard, a plastic transfer pipe was used for the transfer. Figure 1 shows the system, and the transfer was completely automated, managed by the process control computer. The operator would give the computer an instruction to start a batch of product, and the computer control system would start and stop pumps and agitators, open and close valves, and carry out all of the other operations required to manufacture the product without operator intervention or supervision, as long as the process and equipment performed as specified by the program. Extensive field instrumentation provided feedback to the computer control system to confirm proper operation of the process equipment.

For the specific transfer of concern, the computer program was intended to transfer a specified quantity (say 2000 pounds) of the dilute organic acid from Storage Tank A to Weigh Tank B by starting Pump C and opening the appropriate remote control valves. The quantity of material transferred was measured by a load cell on Weigh Tank B (WIC-B), which would signal the computer to close the valves and stop Pump C when the weight reached the specified value. Storage Tank A also had a level indicator, which was primarily used for inventory management.

On the day of the incident, the control room operator initiated the batch sequence, and then went on to manage other plant activities through the computer control interface. He had to use the same control system operator interface screens for these other activities, so there was no visual display of the dilute acid transfer on the control room display screens. When the computer began to transfer the dilute organic acid from storage to the weigh tank, the plastic transfer line completely ruptured because of a poorly made joint in the piping. The entire flow through the transfer line was spilled to the ground, at a rate of

[*]*Correspondence to*: Dr D. C. Hendershot, Chilworth Technology, Inc., Plainsboro, New Jersey, USA.
E-mail: dchendershot@member.aiche.org

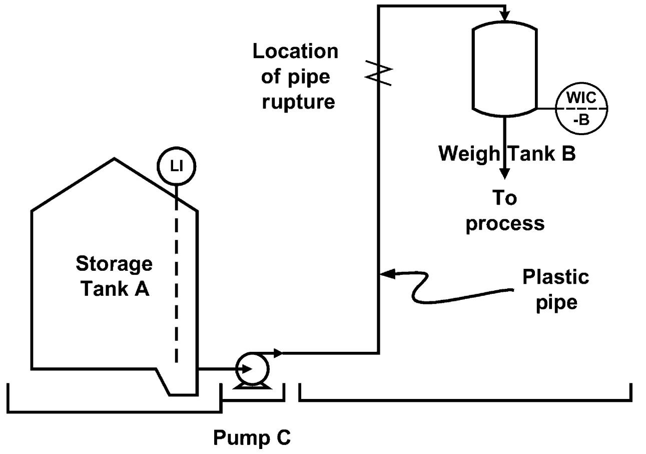

Figure 1. Dilute acid pumping system.

about 50 US gallons per minute. Because the computer control system was programmed to continue the transfer until the weight in Weigh Tank B reached the specified value (about 2000 lb), the computer continued to pump material. The transfer should normally have taken about 5 min, but it continued for a much longer time. Finally, a field operator observed the spilling material from the ruptured pipe and reported it to the control room. The control room operator manually stopped the transfer and isolated the ruptured line. The spill of about 10 000 lb of material was contained in the plant containment area, and there was no uncontained release or ground contamination. The material was not flammable or highly toxic, so the cleanup was accomplished without problem. But, this incident could have been much more serious if a more hazardous material had been involved.

Why did this incident occur? Clearly the initial spill occurred because of a fault in the joint of the plastic pipe used for material transfer. But, why was the spill so large? The computer control system was programmed to pump the dilute acid until the weight in Weigh Tank B reached 2000 lb. Of course, the weight would never reach 2000 lb because no material was actually reaching Weigh Tank B because the transfer line had ruptured. The computer had not been programmed to check that the weight in Weigh Tank B was actually increasing once the valves had been opened and the pump started. And it was not programmed to expect that the transfer would be complete in about 5 min—when the weight of material in Weigh Tank B had not reached 2000 lb in about 15 min, the computer continued to pump, and would have continued until the storage tank was empty. The only reason the spill was stopped was that a field operator observed the leak and it was manually stopped. This spill would have been much smaller nearly all of the time if done manually by a reasonably competent operator. Not all of the time, operators also do make mistakes and fail to observe things in the plant. But, nearly any qualified chemical plant operator would know to check that material is actually arriving in the destination tank when initiating a transfer, and the instrumentation was readily available to do this. Also, he would get very suspicious if the transfer operation, which normally takes about 5 min, was not complete after 15 min or more. He would shut down the operation and try and figure out what was wrong.

Of course, the computer could also be programmed to do these things (and it was, in response to the incident), but in this case, it was not. This represents a human error on the part of the programmer, and more likely, the engineers who wrote the detailed specification of what the program was expected to do. This error was not detected by the protocols to test the plant and software during startup. It is actually easy to understand how this kind of an error can be made. There are a virtually infinite number of small details involved in the safe and correct operation of a chemical plant. When well trained people operate the plant, they do most of these things automatically, often without being specifically told to do them. Most operating instructions for transferring material from one tank to another probably do not specifically tell the operator to check that the material is arriving where it is supposed to (although perhaps they should). But, most well trained operators will do this most of the time. Not always, of course—even well trained operators will forget details like this some of the time, but most of the time a good operator would have stopped this spill long before 10 000 lb of material had been released. But the computer never would have stopped the transfer because the checks had not been built into the program.

Lessons

- It is essential to analyse all operations in great detail when specifying the requirements for the computer control programs. Make sure that you understand everything that a person would do in conducting the operation, and recognize that many of these activities represent common sense to a well trained operator and that they may not be written down. A computer has no common sense, it only knows what the programmer tells it. Any activity left out of the program will never occur.
- Errors in the specification of requirements for computer safety systems, or errors in implementation of those specifications in the actual computer code, may remain hidden until the process challenges the system. For each challenge to an operator, there is a probability that he will fail to respond correctly and in time to prevent or mitigate the incident. But the computer would never have prevented this incident as it was programmed.

INCIDENT 2: IMPORTANCE OF TRAINING IN AN AUTOMATED PLANT

A batch process included a batch distillation step to remove a light material from the process. The distillation was done through a packed column connected to the reactor overhead system (Figure 2). The distillation was controlled by the vapour temperature at the top of the column (T-V in Figure 2). As the distillation proceeded, the amount of reflux to the column would be increased to concentrate the light material at the top of the column. The distillation was considered complete when it was no longer possible to control the vapour temperature (T-V) below the specified value at

Download English Version:

https://daneshyari.com/en/article/588909

Download Persian Version:

https://daneshyari.com/article/588909

Daneshyari.com