ELSEVIER

Journal of Hazardous Materials 142 (2007) 582–588

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

Tell me why

Dennis C. Hendershot

Chilworth Technology Inc., 250 Plainsboro Road, Building No. 7, Plainsboro, NJ 08536, United States

Available online 6 July 2006

Abstract

Engineers usually do an excellent job of documenting WHAT they build—the plant drawings and specifications record in excruciating detail the materials of construction, temperature and pressure ratings, size of pipes and equipment, equipment layout, piping and equipment interconnections, and all other information required to construct and operate a plant. However, the design basis – the WHY of the plant design – often is not nearly so well documented. Understanding the design basis of the plant, particularly with regard to the safety features, devices, and procedures, is as important, or perhaps more important, than understanding the exact specifications of the equipment for the long term safe operation of the plant. Sometimes the reason for critical safety features, particularly inherently safer design features, may not be apparent to people who were not involved in the original design. These features may be vulnerable to compromise or elimination in future modifications of the plant. The people running the plant at the time the modifications are made no longer remember the original design basis. This can also work in the opposite sense—a plant may continue to accept and manage certain hazards long after the original reason for designing the plant to operate in that way has been eliminated, because it has "always been done that way". This important information about the safety design basis of a plant must be preserved by implementation of a process safety information management system. Several case studies and examples illustrating these points will be discussed.

Keywords: Management of change; Inherently safer design; Process safety management systems; Case histories; Process safety information

1. Introduction

When I was a child in Harrisburg, Pennsylvania, the local newspaper had a regular column called "Tell Me Why". People would submit questions about science and technology to the column, and the author would explain how things worked. The questions might be about natural phenomena (what causes hail?) or artifacts of technology (how does a car engine work?). Maybe I was destined to be an engineer or scientist because the first thing I would always read in the newspaper was the "Tell Me Why" column, even before the comics.

Year later, I have come to recognize that it is just as important to understand why a chemical plant is built and operated in a certain way as it is to know how the plant is built and operated. If people only understand what the plant design is, or what the procedures are, they may or may not preserve that design or activity as time goes by. But if they understand WHY something is built or done in a certain way, they are more likely to maintain the designer's intent in the future. Also, they may identify better ways of accomplishing the same objective as technology and knowledge advance.

Unfortunately, most process and plant design documentation is better for describing WHAT has been built, and WHAT activities are required to operate the equipment. We are not as good at documenting the WHY's—the fundamental design basis for the plant. We need to improve process information and documentation to clearly record the reasons for critical safety design features of a plant so they are not compromised by future modifications by people who are not aware of the intent of the original facility designer. Inherently safer design features may be particularly vulnerable because they may be such a basic part of the plant design that it is not obvious that they represent important process safety features of the design. The following case histories illustrate the importance of understanding why a plant is built in a certain way.

2. Safety features at risk

If the reason for process design features is not clearly documented, the safety of the design might be compromised by future modifications by people who do not understand the intent of the original designer. Also, there may be certain procedures, mea-

E-mail addresses: dhendershot@chilworth.com, dchendershot@comcast.net.

0304-3894/$ – see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2006.06.128

surements, or activities, which require a particular response to maintain a safe operation. But if the people who are doing these things do not understand why they are doing certain things, or what is the required response to certain observations, safe operation will also be compromised. Inherent safety features are most at risk because they are such a fundamental part of the design that their purpose may not be obvious. The reason for a high flow alarm, a high temperature alarm, or a high pressure alarm may be fairly clear, or well documented in the instrumentation and process safety documentation. But if a feed line is designed to be a certain size to limit the flow to a specified maximum rate, is this well documented as a critical safety feature?

2.1. Case 1—an inherently safer design to prevent scrubber backflow

A batch process used several chemicals which were highly water reactive. Reaction of these materials with water was extremely exothermic, and the reaction generated a large amount of non-condensable gas. The batch process also generated an acid gas by-product, which was removed from the reactor vent stream by a caustic scrubber. The potential hazard of a violent exothermic reaction, which could generate a large amount of pressure in the reactor in case of backflow of water or caustic solution from the scrubber into the reactor, was of great concern to the designers. Because parts of the batch process operated under high vacuum, there was a greatly increased potential for sucking caustic solution from the scrubber back into the reactor at some steps in the process. The designers developed an inherently safer design to make backflow from the scrubber to the reactor highly unlikely, if not quite impossible. The vent line from the reactor to the scrubber followed a circuitous route to the building roof and then back down to the scrubber, reaching an elevation 32 ft above the level of the scrubber overflow. Thus, even if the scrubber plugged and liquid built up until the scrubber was filled, and the valves in the reactor vent were leaking or inadvertently opened during the vacuum steps of the process, it would not be possible for the scrubber solution to flow back to the reactor.

Fig. 1 shows the system as designed. If the scrubber becomes plugged at the bottom, and liquid begins to back up into the scrubber and vent lines, it cannot flow back to the reactor, even if the vent valves are left open or leak while the reactor is in a process step, which requires vacuum (Fig. 2). As long as the plant vent collection header is operating normally, at slightly below atmospheric pressure, any backup from the scrubber will flow into the vent collection system. While this is not desirable, and appropriate monitoring of the scrubber to detect and respond to a backup is still required, it is much better than letting the caustic flow into the reactor where a violent reaction might occur.

In this case, the routing of the vent pipe is an inherent safety feature of the plant. But is this pipe routing documented as a part of the safety basis of the design? The people who originally designed the plant are well aware of the reason for the vent pipe routing. It should be properly documented in the process hazard analysis—for example, as a safeguard for the deviation "Reverse flow from the scrubber to the reactor" in a HAZOP study. But the

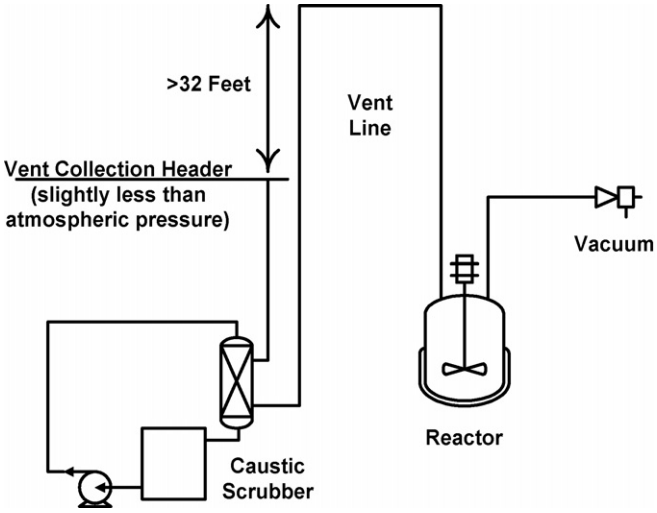

Fig. 1. Scrubber system design.

original designers will move on to other things, and the HAZOP may not be reviewed by new personnel. Perhaps some time in the future it will be necessary to replace the vent line—it may become corroded, for example. It is not hard to envision an engineer in the plant who is not aware of the original design purpose deciding to save a few dollars by routing the vent to the scrubber more directly, as shown in Fig. 3. Now, if there is a backup from the scrubber and the reactor vent valves leak or are not fully closed, it is possible for caustic to flow to the reactor, possibly resulting in a violent reaction and a reactor rupture.

2.2. Case 2—small diameter feed pipe limits reactant flow rate

Fig. 4 shows a design for a semi-batch process for a highly exothermic reaction. The limiting reagent for the reaction (Reactant A) is fed continuously, and the reaction is extremely fast, virtually instantaneous, so there is no buildup of unreacted Reactant A in the reactor. The control system monitors the reaction

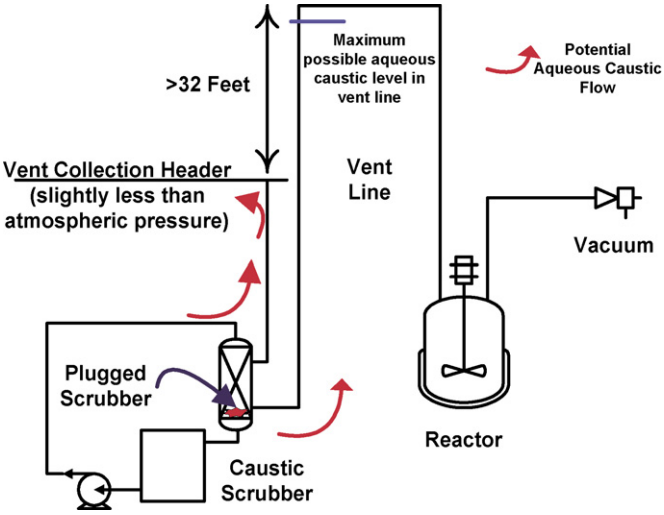

Fig. 2. Aqueous caustic flow with plug at scrubber column bottom.

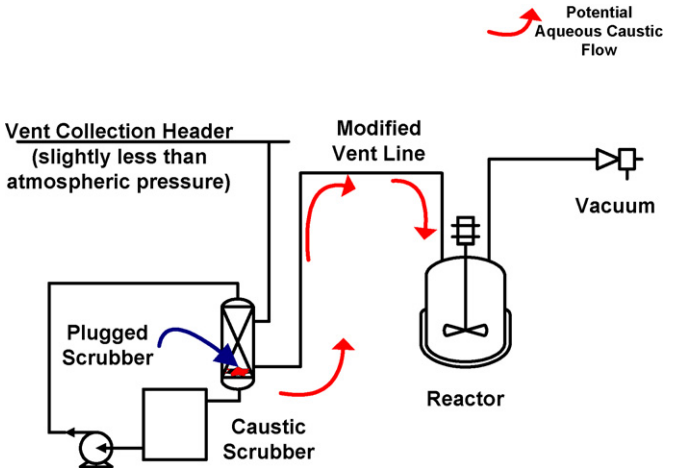

Fig. 3. Aqueous caustic flow with plugged scrubber and modified vent line.

temperature and adjusts the feed rate of Reactant A to maintain the required temperature. There are high temperature and pressure interlocks, which close the Reactant A feed control valve, and an independent shut off valve. The reactor has a large rupture disk to prevent overpressurization in case the Reactant A feed shutdown systems fail to stop the feeds in case of a process upset such as loss of cooling.

The size of the Reactant A feed line is an important part of the safety design for this reactor. The rupture disk design basis is complete loss of cooling to the reactor, and failure to shut down the Reactant A feeds with all Reactant A feed valves completely open. This flow rate is then determined by the size of the Reactant A feed pipe, and the relative elevation of the feed tank and the reactor. It is essential that the process safety information package for this process make this very clear, and that everybody responsible for operation of the plant understand that the feed line size and the elevation of the feed tank above the reactor are critical safety systems for this reactor. It is not enough for plant personnel to know that the Reactant A feed

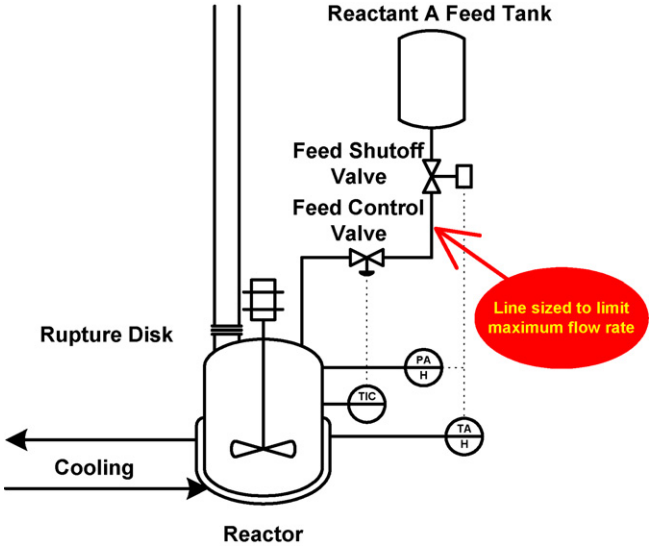

Fig. 4. Semi-batch reactor feed rate limited by pipe size and feed tank location.

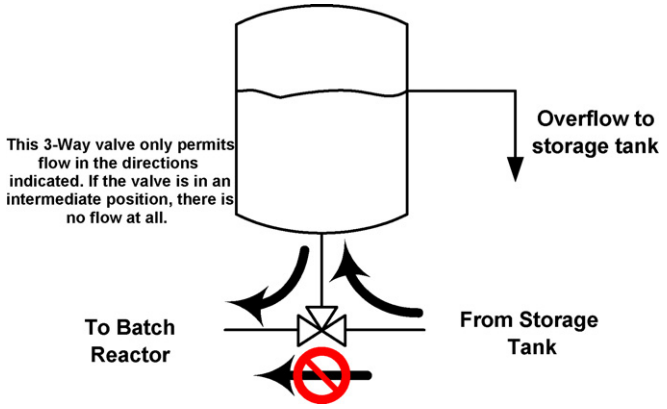

Fig. 5. A feed tank design to hold limit maximum batch charge.

pipe is a particular size—say 1 in. They must know *why* the pipe is that size. Otherwise, a future plant modification might change the feed line size, or something else that impacts the maximum flow rate of Reactant A—for example, relocating the feed tank. This would compromise the design basis of the reactor rupture disk.

2.3. Case 3—using the correct three-way valve

Fig. 5 shows a system for making it extremely difficult to charge an excess of reactant to a batch reactor [1]. The tank holds exactly one batch charge, and the three-way valve will only allow flow from the storage tank to the feed tank or from the feed tank to the reactor. Flow directly from the storage tank to the reactor is not possible. The overflow from the feed tank goes back to the storage tank. The only way that the reactant can be overcharged is to fill the feed tank, empty or partially empty it, re-fill, and repeat the charge to the reactor. While this is not impossible, it is a lot of work, and is unlikely to happen by accident. But it does rely on using the correct type of three-way valve—one which will not allow flow from either side port to the common port, no matter what the position of the valve handle. It will either allow flow from the storage tank to the feed tank, from the feed tank to the reactor, or no flow at all. This is referred to as an "L-Port" three-way valve [2].

There is another type of three-way valve, a "T-Port" three-way valve [2], which will allow flow through various combinations of the valve ports depending on the specific valve configuration. This type of valve can also provide an inherently safer design for some applications. For example, Fig. 6 shows a three-way valve installed on the pressure relief system for a pressurized storage tank. The three-way valve can be set to isolate one of the pressure relief valves from the storage tank for repair or maintenance. If the valve handle is left in an intermediate position, it will allow flow to both relief valves, ensuring that the storage tank has adequate overpressure protection.

The plant documentation should provide the specific valve specification for these applications. However, it may not include the reason for the valve selection—in these cases to make an overcharge of the reactant very difficult, and to ensure the vessel always has an open path to the pressure relief valve, respectively.

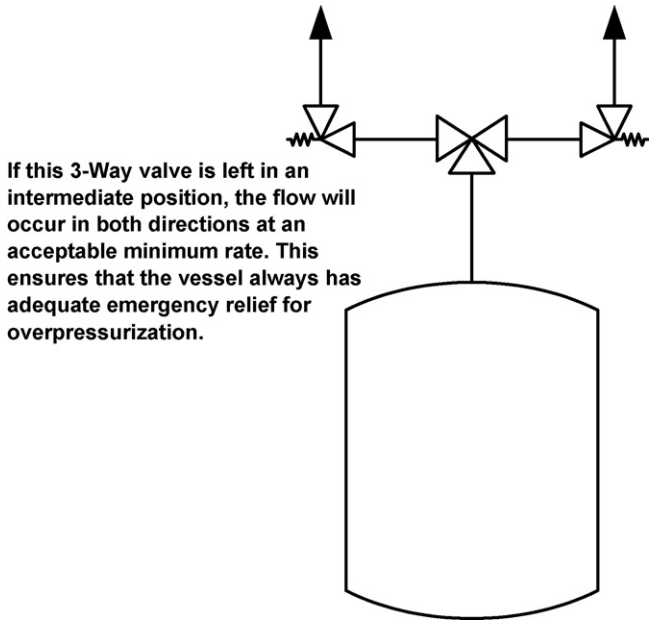

Fig. 6. Three-way valve to allow maintenance on pressure relief valves.

Without this documentation, it is more likely that the reason for the use of a specific type of three-way valve will not be known in a future management of change review, and it is possible that the wrong type of valve will be installed. Or, it is possible that a mechanic will replace the valve with the wrong type, not realizing that the specific valve type is an important safety feature of the plant.

2.4. Case 4—what is that pressure gage for?

Some plant designs include a rupture disk in series with a pressure relief valve for overpressure protection [3], as shown in Fig. 7. There might be a number of reasons for doing this, including, for example:

- Protecting the relief valve from plugging with solids in the process vessel.

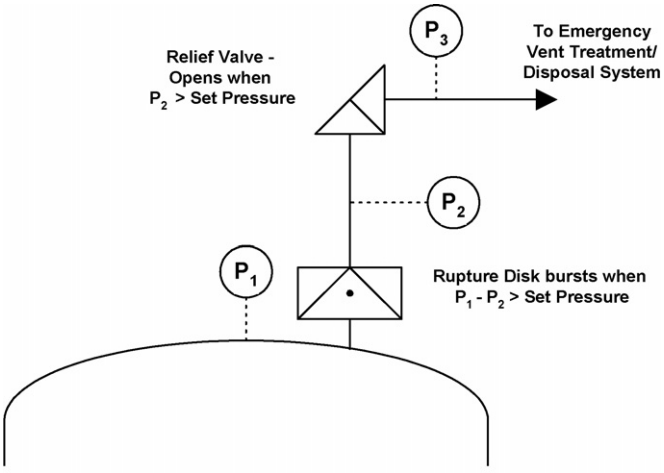

Fig. 7. A rupture disk and relief valve in series.

- Protecting the relief valve from polymer formation if the process vessel contains reactive monomers.
- Protecting a relief valve from a corrosive process stream with a corrosion resistant relief valve, particularly in a situation where a corrosion resistant relief valve is not available.

In these cases, it would be possible to use a rupture disk by itself, without the relief valve, for overpressure protection. However, the addition of a relief valve provides the possibility of limiting the amount of material discharged to the emergency relief treatment system or the outside environment because the relief valve can close when the pressure falls below its set point.

Standards for this type of installation require monitoring of the space between the rupture disk and relief valve for pressure. This is because a small leak in the rupture disk can cause pressure to build up in this space. Since the rupture disk bursts when the differential pressure exceeds its design burst pressure, any pressure on the downstream side of the rupture disk will result in a corresponding increase in the pressure at which the disk bursts. But do the people who read the pressure on the gages, or who receive the alarms from automatic monitoring systems, in this type of installation understand this? In my experience, the answer is often “no”. This applies to operators, mechanics, and many engineers. Often they think that pressure on this gage indicates that there is a small leak in the rupture disk and that it should be replaced at some convenient time. They do not recognize that the pressure compromises the integrity of the pressure relief system without specific training about the consequences of pressure between the rupture disk and relief valve.

2.5. Case 5—why take this sample?

An exothermic batch reaction process required a sample of the reaction mixture immediately prior to the gradual addition feed of the limiting reactant. This sample was analyzed for composition before the feed was started. The sampling step was included in the process because one of the components of the reaction mixture reacted readily with water, an almost ubiquitous potential contaminant in a chemical plant. While this reaction was not highly exothermic or hazardous, it changed the composition of the reaction mixture. The result was that the reaction was much slower during the gradual addition feed and the reactant would not be consumed as rapidly as expected. The buildup of unreacted material in the reactor could result in a runaway reaction if there was a loss of temperature control during the gradual addition reactant feed. Unfortunately, this was not clearly documented in the process safety information package for the process.

Some years later, it was proposed to eliminate this sample. The people operating the plant at the time were no longer aware of the reason for the sample—they thought that it was being taken for quality control purposes. On the few occasions that the batch sample had not met its specifications, charge adjustments were made and so there was no safety incident. The plant was willing to accept the possibility of quality issues caused by an occasional incorrect composition, but was not aware of the potential safety hazard. Fortunately, the management of change review included

an engineer who had been involved in the original design. That engineer remembered the original purpose for the sample, and it was retained as a part of the process. Documentation was also upgraded to make it clear WHY the sample was an important safety feature of the process.

This is an example of a process safeguard being its own worst enemy. If the safeguard is effective, the incidents which the safeguard prevents do not occur. People may forget these hazards, or discount the potential for occurrence because of their experience. They may question the need for the safeguard. "We never have this kind of incident, so why do we need this safeguard?" They do not recognize that these kinds of incidents do not occur because the safeguard, and others, are present. If the safeguards are good, nothing happens! So, people react by questioning the need for the safeguard. It is essential to clearly document the reason for process safeguards, and also document historical incidents and near misses, which demonstrate the need for the safeguard.

3. Unnecessary hazards accepted

In the cases discussed so far, the failure to understand the reason why a process or procedure was designed in a particular way resulted in a potential for changing the system to remove a process safety feature. But there is another potential consequence of not understanding why a plant was designed and operated in a particular way. It is possible that a plant is designed a certain way for reasons that make good sense at the time of the design. This might include accepting the presence of a hazard, and including systems to manage the risk associated with that hazard. But things change, and the reasons for accepting the hazard and managing the risk may no longer apply at some time in the future. But by that time, the process and procedures have become second nature, and nobody questions them. Alternative designs, which might be inherently safer may not be considered.

3.1. Case 6—the Fisher barn effect, an everyday example

Gifford Pinchot (Fig. 8) was governor of Pennsylvania for two terms (1923–1927, and 1931–1935). In 1931, during the Great Depression, he began an extensive rural highway program intended to "get the farmer out of the mud". Twenty thousand miles of paved "Pinchot Roads" were built in Pennsylvania, improving the transportation infrastructure and providing badly needed jobs. One of those roads was built in rural western Pennsylvania, through Mr. Fisher's farm. Fig. 9 shows the original proposed routing of the new road through the farm, going right through Mr. Fisher's barn, which would have to be demolished. Mr. Fisher had a lot of local political influence, and, although he would be compensated, he did not want to go through the aggravation of building a new barn in a different location. He was able to exert his influence to have the route of the road through his farm changed to the route shown in Fig. 10. This introduced a sharp curve near the farmhouse, but driving speeds were slow and this was considered acceptable at the time.

Fig. 8. Pennsylvania Governor Gifford Pinchot (standing on earth mover) on the construction site for a "Pinchot Road".

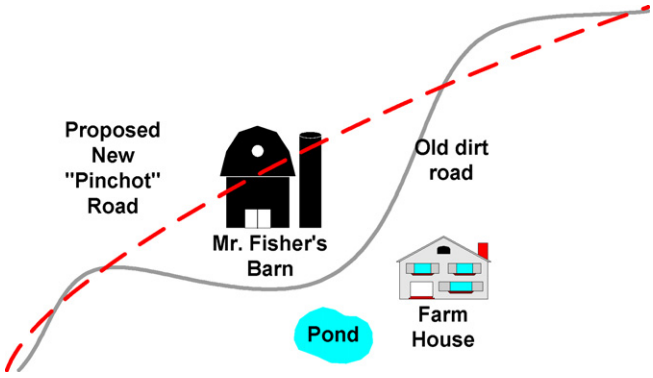

Fig. 9. Original proposed road alignment.

About a year after the new road was built, Mr. Fisher's barn burned down—very likely, like many barn fires, due to spontaneous combustion of moist hay or straw (Fig. 11). Mr. Fisher decided to build a new barn on the same side of the road as his house and the pond where his cattle could get water. Now, more than 70 years later, the road still follows the original "Pinchot road" alignment, with the sharp curve (Fig. 12). With higher highway speeds, once every couple of years a car leaves the road on the curve and winds up in the farmhouse yard, or, if going in the other direction, perhaps in the pond! The road has been rebuilt many times over the years, but nobody ever questioned the alignment of the road or changed it to eliminate the

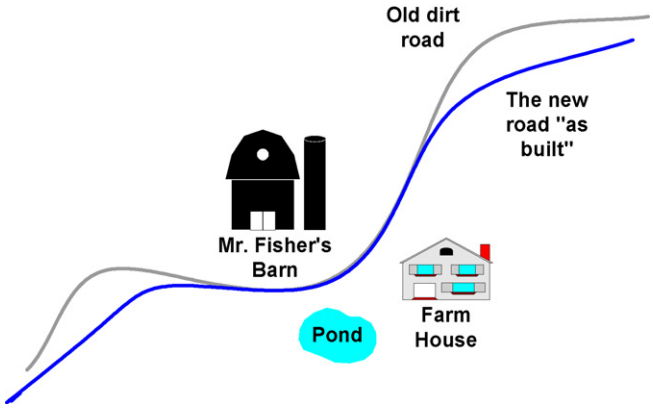

Fig. 10. "As built" road.

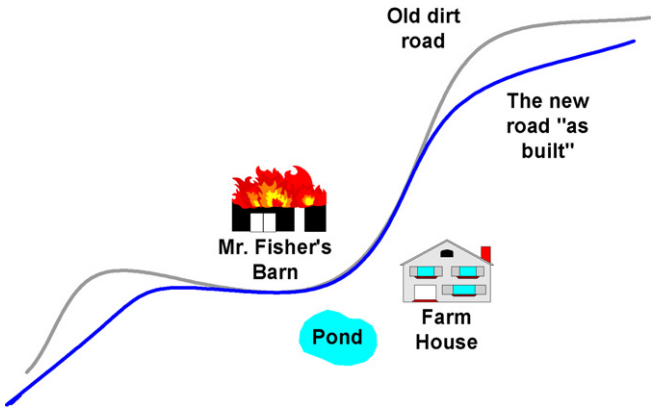

Fig. 11. After the road was built.

sharp curve. The hazard, the sharp curve, has been accepted as "the way things are" long after the reason for accepting it (the original barn) had disappeared. Over the years, nobody (except for a few people in the Fisher family) remembered the original proposal for the road alignment, and the reason it had changed. The hazard remains, and risk is managed through warning signs and driver procedures (reduced speed limit for the curve). These fail periodically and there is an accident.

3.2. *Case 7—the Fisher barn effect in the chemical industry*

The "Fisher Barn Effect" is an interesting story, but what does it have to do with the chemical industry? Well, we can also accept and manage hazards which are present for a reason which made sense at the time a plant was built, but no longer makes sense. For example, in 1996 a paper describing inherently safer design applications in existing plants [4] discussed the substitution of aqueous ammonia for anhydrous ammonia, significantly reducing hazard distance in case of a leak or spill.

The 1996 paper did not discuss the history of the facility—why was the plant using anhydrous ammonia, and going to the trouble of managing the risk if aqueous ammonia could be used in all of the manufacturing processes? The history

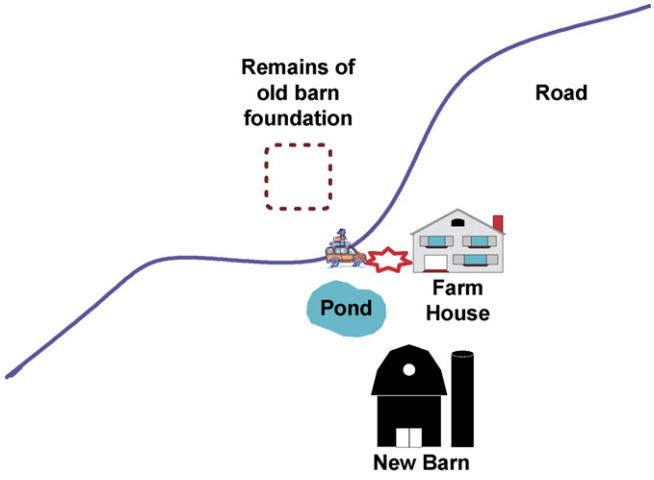

Fig. 12. More than 70 years later.

reveals that this is a clear example of the "Fisher Barn Effect" in the chemical industry. Many years ago, this plant operated a process which required the use of anhydrous ammonia. Because it was necessary to have anhydrous ammonia on site, and manage the risk properly, it made sense to use this ammonia supply for all ammonia consuming processes on the site rather than installing a separate aqueous ammonia supply system. When the process which required the use of anhydrous ammonia shut down, nobody thought to question if this change would offer opportunities to reduce hazards in other processes. The other ammonia consuming processes simply continued to operate the same way they always had, using anhydrous ammonia. Some years later, in a process safety review, the question was brought up, and the processes were changed to use aqueous ammonia. Just as for the Fisher barn, a hazard was accepted and managed even though the original reason for the design was no longer relevant.

4. Summary

The examples described illustrate the importance of good documentation of the reasons for a plant design and plant operating procedures. Traditional plant design information is good at describing what the plant is, but may not be very good at describing why the plant was built that way. Process hazard analysis studies such as HAZOP studies offer a good opportunity to document which features of a plant design are important to safety, and why they have been designed in a certain way. It is important for people involved in the operation and modification of a plant to be familiar with this documentation, and use it when making changes in design or operation. In particular, they should pay attention to plant design features which appear "odd"—do not change them unless you fully understand why they were constructed in that "odd" way. This critical information about the design basis of the plant must be preserved in the plant's process safety information management system.

The great physicist Niels Bohr said "The opposite of a great truth is also true". Unusual design features in a chemical plant are examples. They may represent a creative way to eliminate a hazard, or more reliably manage risk. But they may also be a response to conditions which were relevant at the time of the plant design, but which are no longer relevant to current operations—like the Fisher barn. This can lead to continued acceptance of hazards when the reasons for accepting and managing those hazards no longer exist. These issues can be avoided by a complete understanding of the design basis, the "Why", of the plant design and operation.

References

[1] D.C. Hendershot, Safety considerations in the design of batch processing plants, in: J.L. Woodward (Ed.), Proceedings of the International Symposium on Preventing Major Chemical Accidents, Washington, DC, February 3–5, American Institute of Chemical Engineers, New York, 1987, pp. 3.2–3.16.

[2] Marwin 3-Way Ball Valve Side Entry Port Configurations, Marwin Valve, Division of Richards Industries, 3170 Wasson Road Cincinnati,

OH 45209, Exhibit 198, issued: April 1, 2003; revised: June 29, 2004 (http://www.marwinvalve.com/threeway.html).

[3] A.M. Dowell, D.C. Hendershot, No good deed goes unpunished: case studies of incidents and potential incidents caused by protective systems, Process Safety Prog. 16 (3) (1997) 132–139.

[4] G.W. Carrithers, A.M. Dowell, D.C. Hendershot, It's never too late for inherent safety, in: Proceedings of the International Conference and Workshop on Process Safety Management and Inherently Safer Processes, Orlando, FL, New York, October 8–11, American Institute of Chemical Engineers, 1996, pp. 227–241.