MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Operator Error or Management Failure? Management's Role in Maintaining Operator Discipline

Marc J Rothschild*, P.E.
Livent Corp.
*Presenter E-mail: marc_rothschild@yahoo.com

Abstract

CCPS defines Operational Discipline as "the execution of operational and management tasks in a deliberate and structured manner." Put more succinctly, operational discipline can be defined as doing the right thing when no one is looking. While Operational Discipline applies to facility personnel across the board, this paper focuses on o*perator* discipline, which this author defines as the requirement to explicitly follow written procedures. The only exception would be if the operator believes that doing so would create harm, in which case the operator should stop all work and only deviate from the procedure with expressed approval from his superiors. This deviation should be processed through the management of change procedures.

Failure to follow procedures has caused incidents and near misses throughout the processing industries. It may be tempting to classify these failures as "operator error" and then reprimand the operator. While this may address the symptom, it most likely would not get to the root of the problem. In order to eliminate these failures, it is important to understand and correct underlying causes. For example, are the procedures accurate and clear? Do the operators have the tools and training necessary to carry out the procedure as specified? Has failure to follow procedures occurred previously and, if so, were actions taken by management in response?

This paper presents a case history of an industrial accident – a refinery hydrocracker explosion – to illustrate how management failure had led to a failure to follow procedures.

Keywords: Operational Discipline, Procedures, Unsafe Practices, Normalization

Introduction

CCPS defines Operational Discipline as "the execution of operational and management tasks in a deliberate and structured manner" [1]. DuPont has offered up this definition for Operational

Discipline: "the deeply rooted dedication and commitment by every member of an organization to carry out each task the right way every time" [2]. While Operational Discipline applies to facility personnel across the board, this paper focuses on o*perator* discipline, which this author defines as the requirement to explicitly follow written procedures. The only exception would be if the operator believes that doing so would create harm, in which case the operator should stop all work and only deviate from the procedure with expressed approval from his superiors. This deviation should be processed through the management of change procedures.

Failure to follow procedures has caused incidents and near misses throughout the processing industries. It may be tempting to classify these failures as "operator error" and then reprimand the operator. While this may address the symptom, it may not get to the root of the problem. In order to eliminate these failures, it is important to understand and correct underlying causes. For example, are the procedures accurate and clear? Do the operators have the tools and training necessary to carry out the procedure as specified? Has failure to follow procedures occurred previously and, if so, were actions taken by management in response?

This paper presents a case history of an industrial accident – a refinery hydrocracker explosion – to illustrate how management failure had led to a failure to follow procedures.

Hydrocracking Process Incident

On January 21, 1997, a refinery hydrocracker unit experienced a runaway reaction, which caused a pipe to fail, resulting in a vapor cloud explosion. One operator was killed, and 46 others were injured. The information given about this accident was obtained from an EPA Chemical Accident Investigation Report [3].

Hydrocracking is a refinery process that breaks apart, or "cracks" larger molecules into smaller ones and saturates the chemical bonds with hydrogen. The process is exothermic, and therefore excess heat must be removed to maintain a constant reaction temperature. The reaction rate increases dramatically with increased temperature, with a 20^{o}F increase resulting in a doubling of the reaction rate. Therefore, it is critical that the temperature be monitored and controlled to prevent a potential runaway reaction.

Figure 1 shows the temperature profile in Reactor Bed 5 at the time of the incident. At 7:34 pm on January 21, 1997, the inlet to Bed 5 showed a rapid increase in temperature, with the temperature exceeding 8008°F. Shortly after this sudden increase, the temperature just as suddenly decreased back to a more normal range. The No. 2 Operator went outside to the temperature panel at the reactor to get confirmation of the temperatures. A few minutes later, the reactor temperatures spiked upwards, dropped to zero and then shot up to nearly 1400°F. This excessive temperature caused a line to fail, resulting in a release and subsequent explosion and fire at the unit. This explosion killed the No. 2 Operator, who was standing at the temperature panel, and injured 46 other personnel. Figure 2 shows this failure point and Figure 3 shows where the No. 2 Operator was located at the time of the incident.

The cause of the runaway reaction is complex and is not included in this paper but is discussed in the EPA report [3]. This paper focuses on the fact that this runaway reaction could have easily been stopped had the operators activated the emergency depressurization system, as instructed in the emergency procedures. This emergency depressurization system was installed in 1986 to prevent a runaway reaction. The emergency procedures specify that the depressurization is to be activated upon reaching reactor temperatures in excess of 800°F. Nevertheless, the temperature exceeded this threshold two times, yet the operators failed to activate this system. The question is, why did the Board Operator fail to follow the emergency procedure and depressurize the reactor?

Operator Error or Management Failure?

Unreliable Temperature Readings

The first temperature excursion was brief, and the temperature quickly dropped back down to a more normal operating range. The plant had experienced many problems with the temperature recording system, including false readings the previous day. Because of this history, the operators had little confidence that the temperature readings were accurate. The fact that the temperatures returned to normal supported this view. A few minutes later, the temperatures again spiked, this time to 1200°F, but then immediately dropped to zero. In the EPA investigation, it was reported that the operators were not aware that a zero reading indicated an off-the-scale reading, and instead they interpreted a zero as a faulty reading, confirming their suspicions. So, right up to the point of the rupture, the operators did not believe that they had a runaway reaction on their hand.

Although instructed in the procedures to activate this depressurization, the operators are very aware that such action has serious ramifications. The Hydrocracker is a key processing unit and shutting it down would result in significant loss of production, with a corresponding major loss of revenue. Given this consequence of a shutdown, the operators want to be sure that there really is a problem before taking such drastic action.

Figure 1 Temperature Profile in Hydrocracker Reactor

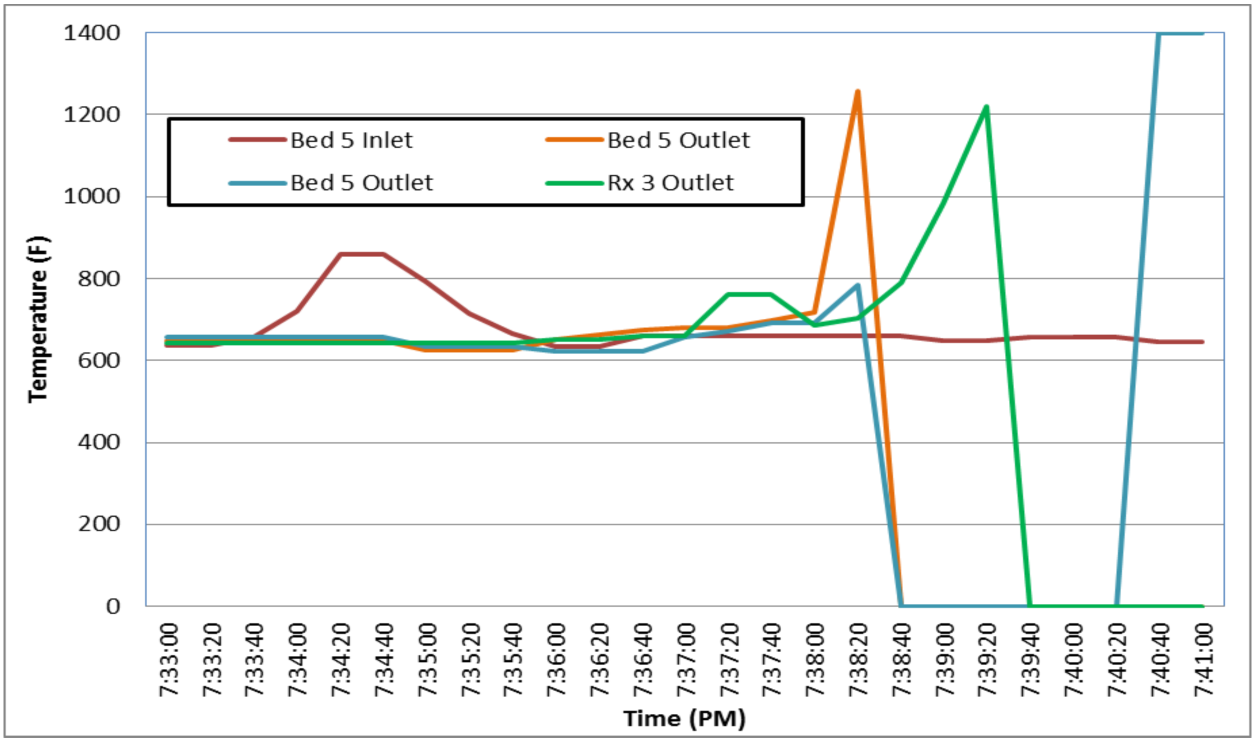
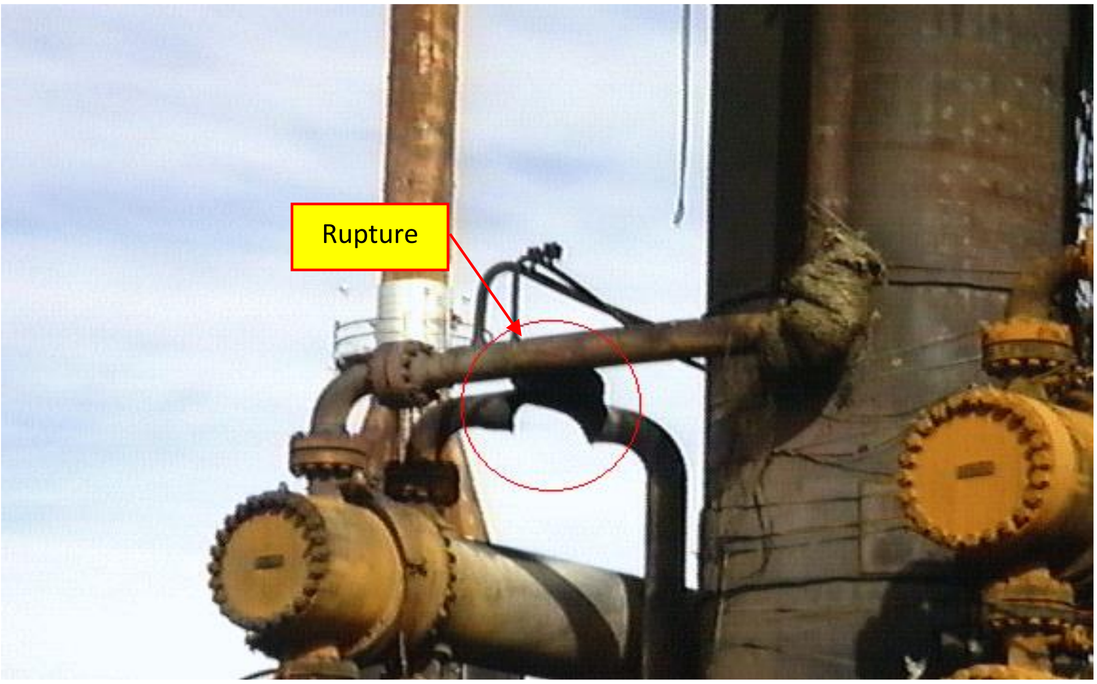
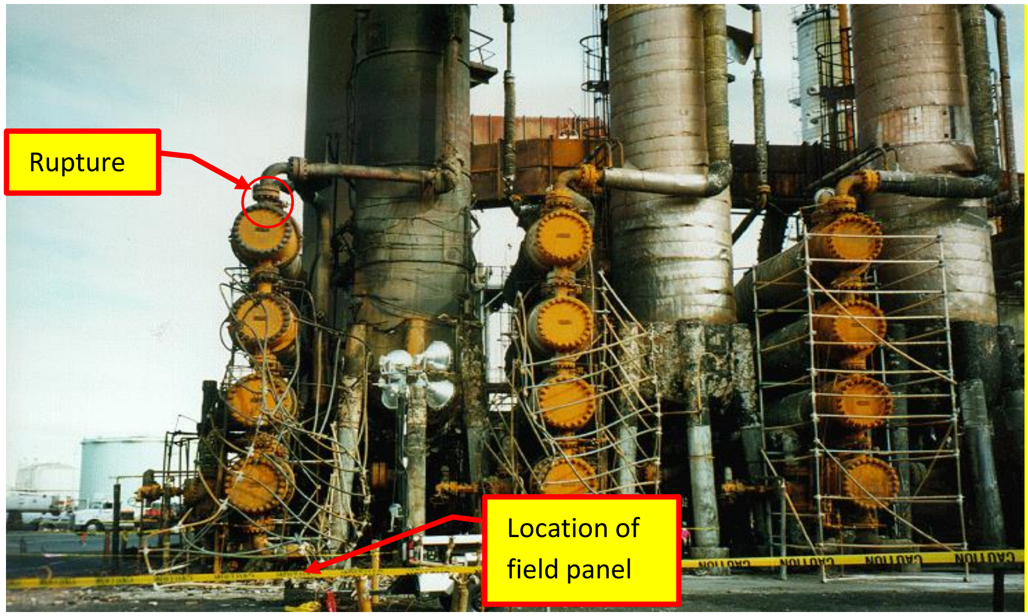


Figure 2 Line Rupture



Picture from EPA report

Figure 3 Location of Temperature Panel



Picture from EPA report

Procedural Issues

The operating procedures for this unit had several deficiencies:

- There were inconsistencies regarding the stated upper safe operation temperature, ranging from 690°F in one procedure to 1,000°F in another.
- The procedures were found to be inconsistent on the safe temperature differentials across and between the reactor beds.
- The procedures were out of date. For example, in February of 1996, the catalyst in all top beds of Stage 2 was replaced with a more reactive catalyst. However, no changes were made to the written operating procedures to reflect the catalyst change and the increased risk of temperature excursions due to increased reactivity.
- Some of the procedures were contradictory and could not be followed. For example, the SOP stated that the quench valves should not be opened more than 50%, while this same procedure also specified that the operators are to maintain a flat temperature profile across the beds, which required additional quench flow beyond a 50% valve position.
- The procedures specified that the outlet bed temperatures were to be the same, but that often was not possible at the desired high throughput due to the limiting capacity of the trim furnaces.

Considering these deficiencies in the procedures, it is possible that the operators did not have confidence in them and therefore did not directly refer to them when operating the unit.

Culture of Production over Safety

Perhaps the biggest reason that the operator did not activate the emergency depressurization is that, as reported in the findings of the EPA report: "*An operating environment existed that caused operators to take risks while operating and to continue production despite serious hazardous operating conditions.*" The Production Area Supervisor stated that failure to use the emergency depressurizing system for a temperature exceeding 800°F would be considered a serious matter and could be subject to disciplinary action. Despite these words, there had been several occurrences over the past several years where the reactor temperature exceeded 800°F and the emergency depressurization system was not activated, yet no disciplinary action was ever taken. Moreover, management never even investigated why the operators failed to depressure the unit, as required. In those situations, rather than depressurizing the reactor, which would shut down the unit, the operators instead brought the reactor under control by adjusting operating parameters. This failure to take corrective action by management to enforce the compliance with the procedures gives a clear message to the operators that they acted appropriately in maintaining operations.

The failure of management to recognize the seriousness of the failure of the operators to shut down the unit may be attributed to what is known as "normalization of unsafe practices." Unsafe practices can become part of the normal and accepted way of accomplishing tasks if nothing bad happens as a result of these practices. The space shuttle Columbia disaster is a well-known example of this phenomenon. NASA's original specification for the space shuttle had zero allowance for any foam loss as any loose debris could seriously impact the very delicate thermal protection system. However, despite this very tight specification, nearly every space shuttle flight prior to and including the Columbia disaster experienced some foam loss. As reported by the Columbia Accident Investigation Board: "With each successful landing, it appears that NASA engineers and managers increasingly regarded the foam-shedding as inevitable, and as either unlikely to jeopardize safety or simply an acceptable risk." [4]

The root of normalization of unsafe practices can be found in the relationship between safety and operations. While it is often stated that process safety and operations are on the same side, the truth is that these two elements are almost always in conflict with each other. That is because the benefit of unsafe behavior is immediate and tangible, whereas the potential benefit of safe behaviors is long term and results in an intangible non-event. Had the operators shut down the hydrocracker unit, as instructed, the refinery would have taken a significant financial hit. Consequently, the operators would likely have faced second guessing as to why they didn't try to keep the unit online, especially when considering that they were previously able to keep the unit online under similar circumstances.

We are not able to make decisions based on hindsight, but we are able to evaluate the risks of an adverse event and make informed decisions based on those risks. This was done by the refinery. In 1986 the refinery identified the risk of a runaway reaction and, in response, installed a means to immediately depressurize the unit and established conditions where the operators were to activate it. While the risk of the event remained unchanged, the *perception* of the risk did change.

One factor that influences risk perception is known as "melioration bias," which is the tendency to assign greater weight to short term results, and to underestimate the potential for the occurrence of a negative event. If the unsafe behavior does not result in an incident or accident, and if the unsafe behavior results in positive outcomes, then positive reinforcement increases the strength of the bias. Other factors that affect the perception of risk include rare event and optimism bias. Rare event bias is the tendency to under evaluate or minimize the likelihood of being adversely affected by a negative event that is known to occur only on rare occasions. Optimism bias results in the perception that one is less likely to experience a negative event compared to others in a similar situation.

These shifts in risk perception are revealed in a press release produced by the refinery, following this accident. In their statement, the refinery reported that they "found the incident to be highly unprecedented in the 34-year history of the hydrocracker unit, outside the realm of its experience in the refining industry, and that of the qualified operators on duty the night of Jan. 21" [5]. The implication of this statement is that this was a freak event and that they could not reasonably have prepared for its occurrence. Of course, this is difficult to accept, as the refinery did acknowledge the potential for this event, installed a safety system specifically to address it, and provided instructions to the operators to activate the safety system upon reaching specific operating parameters. From a mathematical perspective, 34 years is not statistically significant compared to the "expected" frequency of a line rupture – which is on the order of once every 10,000 – 100,000 years. However, if the statement accurately reflects the sentiment of the refinery management, it can only be concluded that the management's perception of risk has been reduced due to 34 years of success at being able to maintain unit operations despite occasional temperature excursions.

Management's Responsibility in Maintaining Operator Discipline

As shown in this case study, management needs to make sure that the operating procedures are clear and accurate and that the instrumentation and controls are reliable. In addition, management needs to be unambiguous regarding the importance of safety and that their actions are consistent with this message.

Specific measures that management can take to bolster safety include the following:

- Ensure that employees are aware of the hazards of the process and are aware of the consequences of failure to follow safe operating practices;
- Give operators written authority to stop or shut down the process if they believe that harm may occur;
- Enforce a policy of not allowing deviations from established safety standards without first conducting a Management of Change;
- Implement a policy of zero tolerance for willful violations of process safety policies, procedures and rules;
- Investigate all abnormalities as "near-misses";
- Share findings of incident investigations, including similar incidents in other industries.

Conclusion

In this case study, the runaway reaction could have been stopped had the operator activated the emergency depressurization system, as specified in the emergency procedure. However, in the EPA report, it was concluded that an operating environment existed that encouraged operators to take risks while operating and to continue production despite potentially serious hazards. Management is responsible to ensure that the operators have procedures and instrumentation that they can trust, and Management must give a clear and consistent message regarding the importance of process safety in operations.

References

1. Center for Chemical Process Safety, “Guidelines for Risk Based Process Safety,” 2007.
2. Rains, Brian D., “Operational Discipline – Does Your Organization Do the Job Right Every Time?” Mary Kay O’Connor Process Safety Center International Symposium, College Station, TX, 2011.
3. U.S. Environmental Protection Agency, “EPA Chemical Accident Investigation Report - Tosco Avon Refinery - Martinez, California,” 1998.
4. Columbia Accident Investigation Board, Report Volume 1, Chapter 6, page 122, August 2003.
5. Business Wire Report, “Tosco releases report on Jan. 21, 1997 accident investigation,” May 29, 1997.