OPERATORS

Table of Contents

Page

List of Figures

1.0 SCOPE

This document provides an understanding of operational hazards that drive losses and guidance on measures that can be implemented in order to prevent or reduce the severity of the losses. This includes operator training programs, the competence of operators in their day-to-day role, the supporting management structure and organizational culture.

The term “Operators” may include control room operators, field operators and their supervisors.

1.1 Hazard

Operational hazards, if not properly managed, can result in significant property damage and loss of production. For example, operators who lack adequate system knowledge or training can cause failures, while well-trained operators using good procedures and programs can significantly reduce the frequency and impact of failures.

An effective training program supported by the site management team will ensure operators are adequately trained, and reduce the potential for errors to occur.

1.2 Changes

January 2019. Minor editorial changes were made. Sections 2.2.3 ″Management of Change (MOC)″ and 2.2.9 ″Incident Investigations″ are replaced with the reference to Data Sheet 7-43, *Process Safety*.

2.0 LOSS PREVENTION RECOMMENDATIONS

2.1 Introduction

Operator competence (their skill and knowledge) and the actions they take are critical to ensuring the safe operation of facility equipment and processes. In many situations, the actions that operators take can make the difference between a minor event and one that results in major damage to equipment, long term shutdown of operations, and significant business loss.

In addition, influences such as resource management (staffing, training, funding, and equipment maintenance), management support, organizational culture (policies, structure), and operational processes (time pressures, quotas, schedules) can directly affect the safe operation of the facility.

Therefore, management of operational risks is critical to ensuring safe operations and reducing the potential for business losses.

2.2 Human Factor

2.2.1 Management Support

Management should fully support operational staff and there should be an organizational culture that supports this. Demonstrations of the commitment to this culture include the following:

A. Initial and ongoing training for operators

B. Providing operators with the authority to shutdown a process or piece of equipment, without the fear of reprisals, if they think a dangerous/upset condition has developed

C. Including operators in reviews of changes in the design, inspection, and maintenance procedures

D. Providing operators with opportunities to provide feedback

E. Providing clear lines of authority

F. Providing an appropriate budget for training of personnel

G. Management providing written statements of their support

2.2.2 Operator Training Programs

Improper operation can have consequences ranging from inconvenience to significant damage to equipment and property accompanied by long-term unplanned outages. Only qualified operators (i.e., those who are specifically trained) should be permitted to operate a piece of equipment or process. The possibility of improper operation can be minimized by a knowledgeable operator.

Various types of operator training methods and tools are available. Elements of a well-developed operator training program could include some or all the following:

A. Instruction on how the equipment works, identification of equipment hazards, safety systems and their operation, and operating procedures (including those for startup, shutdown, emergency, and lockout)

B. Training manuals that are reviewed and maintained at set intervals, whenever there is a significant change, and when standard operating procedures (SOPs) or emergency operating procedures (EOPs) are updated

C. Understanding of alarms and upset conditions and the corrective actions to be taken when they occur

D. Training records for personnel that are kept up to date

E. Qualified mentors and training personnel who have received appropriate training and have defined roles

F. Defined trainer/mentor qualifications

G. Defined and documented roles, responsibilities, and competencies for all operational positions

H. Practice drills that are conducted for upset/emergency conditions

I. Knowledge checks of operators, which can be accomplished through the use of simulators, on-the-job oral examinations, writing examinations, practical demonstrations, or online assessments

J. A refresher training program that includes such subjects as “what if” scenarios; upset conditions; changes in process, SOPs, or EOPs; and general knowledge checks. The program should be completed at a maximum of every three years but could be more frequent depending on the complexity of the facility and hazards. Practice drills may also be included.

K. A training program that encompasses all areas of the facility in which operators will be responsible

2.2.3 Management of Change (MOC)

Refer to Data Sheet 7-43, *Process Safety*, for relevant recommendations.

2.2.4 Standard Operating Procedures (SOPs) and Emergency Operating Procedures (EOPs)

SOPs are in place to provide instruction for operation of processes, systems, or equipment and may include checklists for use by operators to ensure the correct positioning of equipment for the appropriate mode of operation. SOPs may also be provided for other items such as permit to work, quality, and hazard and operability requirements. The procedures should represent a definition of best practice that should be adhered to at all times.

EOPs are address a range of emergency conditions that could have a negative impact on site operations if not addressed appropriately. A methodology should be developed to understand common upset conditions, as well as more critical uncommon emergency events.

SOP and EOP development, review, and training could include using site operations, maintenance, and management staff.

2.2.4.1 SOPs and EOPs should be controlled documents covered under the quality system and therefore, kept up to date. Any changes should be fully controlled, documented, and subjected to management-of-change procedures. Revisions to the procedures will be required periodically. Revisions may also be need when the following occur:

A. There is a major change in the process, such as the introduction of new equipment, chemicals, interlocks, alarms, or personnel.

B. Successful trials are completed that need to be incorporated into the procedures.

2.2.4.2 New and modern control systems will often have a number of parameters that need to be positively achieved and act as a checklist for operators. These should be reviewed periodically with the SOPs to check for consistency and to ensure safe operation is maintained.

2.2.4.3 Upon completion of a new SOP or EOP, or following a revision, the procedure should be reviewed by personnel who are fully familiar with the process it refers to.

2.2.4.4 Final authorization should be provided by management.

2.2.4.5 There should be periodic audits (at a minimum of every three years or as the facility governs) to ensure procedures are implemented in accordance with the relevant SOPs.

2.2.4.6 All SOPs and EOPs should be readily available to operators at all times.

2.2.5 Alarm Management

Operational alarms and annunciators are critical to understanding conditions that are not within normal limits. Alarm set points are typically set at a level that gives operators enough time to react to abnormal conditions and take corrective actions.

Alarm set points should only be adjusted by qualified and authorized personnel. Typically this is managed via security software (i.e., passwords) on the DCS, PLC, or other digital control system. For non-digital systems, this should be managed by preventing access to or locking logic controllers.

If an alarm set point needs to be temporarily or permanently altered, authorized personnel should follow alarm system management-of-change procedures, document all changes, and communicate to operations personnel all changes that may affect system operation.

A method of documenting alarms that have been permanently silenced, (nuisance alarms, false alarms, faulty field devices, or notification alarms) by operations staff should be in place and included in a tracking policy. This also includes forces and jumpers. (A force is a controlled output that is unchanged by input or feedback in a control loop. It is designed to ensure a certain output [control signal, set point signal, or other output] that will not be affected by otherwise related feedback and inputs from the system.)

Alarms should be prioritized so critical alarms (based on the results of hazard analysis of the process) receive the immediate attention of the operator and remain visible and at the top of the alarm list. Ideally, there should only be an audible alarm when there is a change in plant condition that requires the operator to take action. In practice, an assessment is needed if the system is arranged in such a way that allows more alarms to be transmitted than the operator can reasonably respond to.

2.2.6 Equipment Status

2.2.6.1 Management Programs

2.2.6.1.1 Ensure there is a status management program in place in which all plant information is up to date and readily available for operators and their supervisors so they can make routine, accurate, and timely decisions.

2.2.6.1.2 Information may be in various forms and places but it should be easily navigable should information be urgently required. Examples of where information may be available include status boards, computer screens, control panels, printouts or in logs.

2.2.6.1.3 Status information should be maintained, kept current and updated when changes occur.

2.2.6.1.4 Procedures should be in place to quickly notify operators, supervisors and maintenance managers (if applicable) of a deficiency that could affect the safe operation of a system. The deficiency could be due to upset conditions, equipment breakdown or degradation in system performance.

2.2.6.1.5 Procedures should be in place to notify operators and supervisors when there is a planned or ongoing maintenance, or inspection procedure which could affect the operation of the plant.

2.2.6.2 Permit to Work (PTW) Systems

Permit to work systems (including lock out/tag out systems, clearance, and tagging programs) are used primarily in industrial applications to protect personnel but also serve to protect equipment from damage. There should be a policy in place outlining the requirements of the system, and it should be reviewed on a regular basis.

An appropriate level of management at the site should have overall responsibility for the implementation and ongoing management of the PTW systems.

2.2.6.2.1 A PTW system should be considered whenever it is intended to carry out work that may create a hazardous condition or affect the facility. The system should not be applied to all activities because this may lead to a weakening of its overall effectiveness. The following are examples of when a PTW system may be appropriate:

A. Non-production work (maintenance, repair, inspection, testing, alteration, modification, etc.)

B. Non-routine operations

C. Jobs in which two or more individuals or groups need to coordinate activities to complete the job safely

D. Jobs in which there is a transfer of work and responsibilities from one group to another

2.2.6.2.2 The following are considered to be the minimum features of an effective PTW system:

A. Clear identification of who may authorize particular tasks (along with any limits to their authority) and who is responsible for specifying the necessary mitigation measures

B. Training and instruction in the issue, use, and clearance of permits such as lock-out, tag-out (LOTO)

C. Monitoring and auditing to ensure the program operates as intended

D. A job safety analysis (JSA) or job task analysis (JTA) that includes clear identification of the types of work or tasks that could introduce hazards or risks to equipment

E. For LOTO or line breaking operations, a list of items isolated that is maintained with the permit; this may include provision for personnel to initial and date when items are isolated and also when items are returned to normal operating position

F. Permitted task duration and any supplemental or simultaneous activities along with their mitigation measures

G. Upon completion of the work involving LOTO or line breaks, and prior to any permit being cancelled/completed, there should be a walk down by operations (this should be part of the pre-startup safety review process)

H. Regular auditing of the systems (before, during and after the work) to ensure all relevant processes and procedures have been followed

2.2.7 System Alignments/Configurations

All operators should be aware of the alignment (e.g., equipment such as valves being in the correct position), parameters of the systems, and equipment in their area of responsibility regardless of the mode of operation (e.g., startup, shutdown, normal operation, and maintenance).

2.2.7.1 Routine system alignment checks (which could include visual confirmation for manual systems, and control screens for remote/automated systems) should be completed at a frequency determined by the level of control required and the level of operating activity.

For example, if a system has minimal exposure where an upset condition would lead to minimal impact on the process or production and operates in a steady state mode, then less-frequent checks are warranted. However, if it is a critical system and there could be a significant exposure where an upset condition could threaten facility integrity or production, or where there are frequent changes in operating mode, then more-frequent checks would be needed.

2.2.7.2 When alignment checks are completed, they should be reviewed by the operational staff. These can then be used to verify equipment and operational status, and should be kept available until the next checklist is completed.

2.2.7.3 All changes should be noted on status boards, logs or other readily available locations, and should be communicated at the shift changeover.

2.2.8 Shift Changes

A thorough shift change process should be in place to ensure operators and supervisors obtain good information on facility status. Typically, the shift change process ensures the relieving operator directly discusses all aspects of the facility status as it relates to their duties with the relieved operator. The process may include the following elements:

A. Equipment/unit/facility history and current status

B. Anticipated operating conditions, startups, shutdowns, production changes, etc.

C. Abnormal operating conditions, including current alarms, set point changes, etc.

D. Maintenance outages or de-ratings

E. Planned maintenance activities

F. Where maintenance is required

G. Equipment out of service

H. Temporary restrictions, including any jumpers/bypasses

I. Contractors/outside personnel who are in the operating area

Upon completion of the individual shift changeovers, it may be beneficial to conduct a shift crew meeting to communicate current issues relating to facility status, maintenance activities, and personnel assignments.

2.2.9 Incident Investigations

Refer to Data Sheet 7-43, *Process Safety*, for relevant recommendations.

2.2.10 Asset Integrity

Refer to Data Sheet 9-0, *Asset Integrity,* for relevant recommendations.

3.0 SUPPORT FOR RECOMMENDATIONS

3.1 Illustrative Losses

3.1.1 Operator Error Results in a Thrust Event and Ensuing Jet Fire

An integrated fertilizer complex produced ammonia, urea, granular ammonium nitrate, ammonium phosphate, and urea ammonium nitrate fertilizers. The motor-driven syngas compressor for Plant 2 (Figure 1) was a bottleneck because a failure of this compressor would shut down the plant.

The ammonia plant was being restarted after an outage. As part of the startup of the syngas compressor, a “balance,” or equalization valve was opened between the discharge of the syngas compressor second stage and the inlet to the recycle stage (Figure 2). Once the compressor was started, this valve was left open until the process loop was stable.

Fig. 1. Syngas compressor train

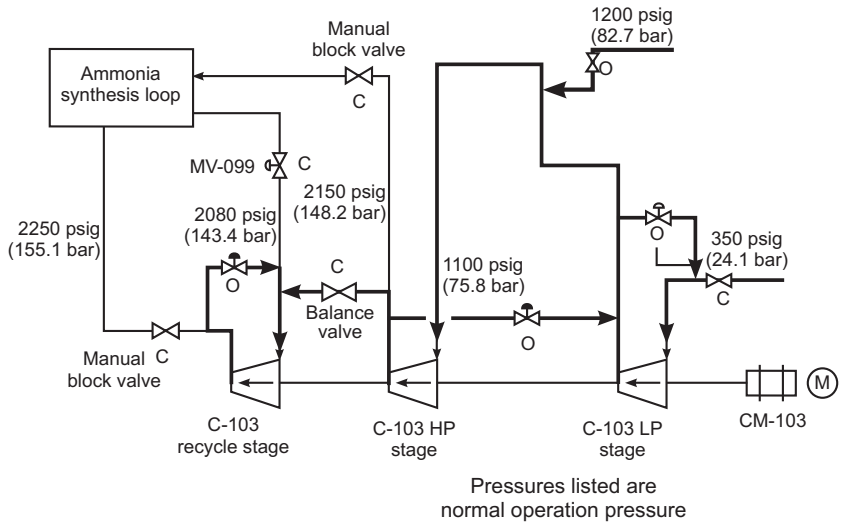

Fig. 2. Simplified schematic of syngas compressor at startup

Although the operators had been recently trained, checklists were used, and field operations were directed by control room operators, the field operators closed the balance valve after the compressor was started and before the process was stable. The valve closure resulted in unbalanced loads on the compressor with damage to rotating and stationary elements due to the sudden axial thrust. The axial thrust caused a syngas piping flange failure, resulting in a jet fire, shutting down production.

The compressor and motor sustained significant mechanical damage. The ensuing jet fire damaged the building structure. A 30-week production interruption occurred while building repairs were made and the compressor and motor were replaced.

The incident investigation revealed that a complacent culture was in place. This, combined with an inadequate communication protocol, failure to follow operating procedures, and lack of adequate safety devices, were contributing factors.

3.1.2 Plant Trip Results in a Reformer Failure Due to Operator Error

An integrated fertilizer complex produced ammonia, urea, granular ammonium nitrate, ammonium phosphate, and urea ammonium nitrate fertilizers. Nitrogen operations for ammonia production consisted of two ammonia plants (Plants 1 and 2). The primary reformers were bottlenecks.

During normal operations, the site had three package boilers for plant medium pressure steam demand, one of which provided redundant (N+1) steam capacity. At the time of the incident, this boiler was offline for maintenance. The two other boilers were maintaining plant steam demand until one of the boilers tripped off line due to loss of the forced draft fan and could not be restarted. This resulted in reduced plant steam supply and a site-wide shutdown. The automatic interlocks on the Plant 1 reformer successfully tripped that unit off line due to low steam flow through the reformer tubes without incident. However, operators continued to try to keep the Plant 2 reformer on line manually. This resulted in overheating of all 160 tubes and the inlet and outlet headers (Figure 3).

Fig. 3. Damaged reformer tubes

The lack of adequate interlocks placed increased reliance on the operators to act appropriately during normal and upset conditions. When the steam upset occurred, the flood of alarms and resulting miscommunication on the operation of Plant 2 contributed to the incident.

3.1.3 Loss of DC Power Supply and Lubrication Oil System Failure on a Gas Turbine Generator due to Operator Error

An aluminum smelter operated five potlines. Electrical power was generated onsite in the four separate power stations capable of meeting plant electrical demand of approximately 1500 MW for aluminum production. Power Station 4 consisted of four gas turbines (GT) rated at 164 MW and heat recovery steam generators (HRSGs) each supplying a single 130 MW condensing steam turbine.

The VRLA batteries for Power Station 4 required replacement based on test results. The new battery bank was installed but remained isolated from the dc emergency bus while the batteries were exchanged. During this operation a lock-out tag-out procedure was used, but after placing the new batteries in service the lock-out tag was removed without closing the isolating switch.

The dc emergency and control systems were now without power. A trip occurred on the GT, but the generator circuit breaker was still in the closed position because the relays did not function with the batteries isolated due to lack of tripping current. An operator corrected the battery isolation condition, opening the generator breaker and starting the lube oil pumps. However the loss of lube oil to the bearings resulted in shaft journal rubbing/scoring (Figure 4).

Fig. 4. Rotor journal scoring

Generator motoring and rotor thrust also occurred as the generator stayed connected to the grid while the generator breaker was closed. This resulted in blade and stationary vane contact and casing rubbing in the GT compressor section (Figure 5).

The initial cause of this incident was incorrect switching of the emergency and control dc batteries due to failure to follow operating procedures. Contributing causes included deficiencies in the lock-out tag-out system and failure of operators to initially realize the cause of the incident due to inadequate training.

3.1.4 Turbine Mechanical Breakdown Due to Bypassing of Control Valves

A power generation plant was comprised of three municipal waste incineration lines. The plant produced approximately 30 MW electric power, 85 tons/hour of steam and hot water. After a shutdown and overhaul, the steam turbine was in the process of being placed back into service when the unit tripped off line. Two further attempts were made to restart the turbine, with no result. Testing was conducted on the steam admission valves that required manually bypassing the ESV, but no bypass lock-out tag-out procedures were followed. In addition, the bypassing was not communicated among the operators involved, nor was the open position of the manual valves properly communicated.

This situation allowed high-pressure steam to be admitted directly into an out-of-service and non-rotating steam turbine, which immediately resulted in significant overpressure of the LP turbine and a violent axial movement of the rotor relative to the casing. Lifting the casing to investigate the damage revealed labyrinth seal, shaft, bearing, gear box, and casing damage (Figure 6).

Fig. 5. Rubbing damage to compressor blades

Fig. 6. HP upper casing damage seal

Contributing factors were lack of communication, poor management of safety device bypasses, and inadequate operator training on startup, lock-out tag-out, and valve testing procedures.

3.1.5 Loss of Lubrication on a Steam Turbine Generator Due to Locked Out DC Lube Oil Pumps Results in Mechanical Damage

A four-unit electric generating station had a total capacity of 430 MW. Operators were bringing down Unit 3 due to a boiler tube leak. During the shutdown process, an alarm indicating loss of 480 V and UPS power came in. The operator did not immediately recognize that ac power to the lubrication and seal-oil pumps were also interrupted. While the dc seal-oil pump did detect the loss of ac power and started, the dc emergency oil pump motor did not start. The dc controls had been locked out by operators as part of the restart to prevent automatic starting of the pump.

The shaft-driven oil pump was able to supply lubrication to the unit until approximately 2200 rpm. Once lubrication was lost, the rotor quickly came to a stop. Dropping of the shaft allowed the generator inboard bearing hydrogen seal oil to leak hydrogen into the turbine hall. The hydrogen and the lube oil ignited, resulting in a fire, but the deluge sprinkler functioned. Bearings, seals, and the turbine rotor were damaged due to loss of lubrication. Inadequate startup procedures and operator training were contributing factors.

3.1.6 High Vibration Due to Improper Feedwater Treatment by Operators

A 1957 GE steam turbine (17,750 kW) matched with a 1981 generator (16,800 kW) had a catastrophic breakdown. Over the course of two days, plant operators were aware of boiler feedwater quality issues (low pH). Attempts to correct this situation were seemingly on track when the overnight shift foreman took the unauthorized action of adding a 50% caustic solution (NaOH) to a demineralized water storage tank. This increased the feedwater pH to over 12 and significantly increased the sodium level.

During the next 17 hours, feedwater test results were drastically out of range and a series of other operational and equipment problems surfaced. Operating procedures were not followed and the steam turbine-generators continued to be operated as if feedwater and steam conditions were normal. Eventually the unit tripped on high vibration. The turbine main stop valve did not close properly and the turbine over-sped to destruction. After further investigation, it was determined the stop valve was stuck in the open position due to a buildup of sodium on the valve stem.

3.1.7 Tall Oil Fire due to Operator Error

A fire occurred outside a distillation column at a tall oil refinery plant. The loss was caused by an operator error when a blank flange on a pipe connected to a distillation column was removed while the distillation column was in operation. This lead to a failure of the vacuum in the column, which caused material in the column to condense and fall down the column. The product in the column was at a temperature above its autoignition point and this lead to the fire. There was damage to pumps, motors, wiring, and instrumentation in the immediate area of the fire.

3.1.8 Explosion at a Chemical Plant

Multiple deficiencies occurred during a lengthy startup process that resulted in a runaway chemical reaction inside a residue treater pressure vessel. The vessel ultimately over-pressurized and exploded.

The incident occurred during startup, following a lengthy period of maintenance. It was found that the startup was begun prematurely (a result of pressure to resume production) and took place before valve alignments, equipment checkouts, a pre-startup safety review, and computer calibration were complete. Additionally, it was found that there was no thorough process hazard analysis (PHA).

There were numerous critical omissions, including an overly complex standard operating procedure (SOP) that was not reviewed and approved, incomplete operator training on a new computer control system, and inadequate control of process safeguards. A principal cause of the incident was the intentional overriding of an interlock system that was designed to prevent an explosive atmosphere from occurring within the vessel.

It was found that critical operating equipment and instruments were not installed before the restart, and were discovered to be missing after the startup began. A gas-monitoring system was not in service as the startup ensued.

4.0 REFERENCES

4.1 FM Global

Data Sheet 7-43, *Process Safety*

Data Sheet 9-0, *Asset Integrity*

APPENDIX A GLOSSARY OF TERMS

Alarm: Provides an audible, visual, or other form of signal about a problem or condition.

Annunciator: A signaling apparatus, usually used in conjunction with a buzzer that displays a visual indication.

Consequence: The outcome of an event.

Culture: An organization's system of commonly held values and beliefs that influences the attitudes, choices, and behaviors of the individuals in the organization.

Error: An action that unintentionally departs from an expected behavior; an act of commission or omission that leads to an undesirable outcome or significant potential for such an outcome.

Event: An unwanted or undesirable change in the state of a system, structure, or component. It can also manifest itself as an unwanted or undesirable change in a worker or an organization (such as industrial safety, environmental health, behavior, or administrative control).

Mistake: A failure during intentional behavior or an incorrect choice; an error of reasoning, such as making a bad choice or failing to think through the full implications of an action.

Risk: The combination of (1) the frequency or probability of occurrence, and (2) the consequence of a specified event. The concept of risk always has two elements: the frequency of event occurrence and the consequences of the event.

Safety culture: The product of individual and group values, attitudes, competencies, and patterns of behavior that determines the commitment to and the style and proficiency of an organization's health and safety programs. Organizations with a positive safety culture are characterized by communication founded on mutual trust, by shared perceptions of the importance of safety, and by confidence in the efficacy of preventive measures.

Violation: A deliberate, intentional act to evade or deviate from a known policy or procedure for personal advantage (such as comfort, expedience, or convenience). Violations are not errors and should not be tolerated.

APPENDIX B DOCUMENT REVISION HISTORY

January 2019. Minor editorial changes were made. Sections 2.2.3 ″Management of Change (MOC)″ and 2.2.9 ″Incident Investigations″ are replaced with the reference to Data Sheet 7-43, *Process Safety*.

April 2016. This is the first publication of this document.