17

Routine Operation Phase

An Illustration of the HAZOP Analysis Method for Periodic Review

17.1 Problem Definition

Background

The Anywhere VCM plant has been operating for the past two years without an incident. ABC corporate management believes that the hazard evaluations performed on the plant during its design and after its construction have contributed to this good operating history. To help ensure that this operating record is maintained, ABC management is requiring the Anywhere plant to perform periodic hazard evaluations of all operating units (in fact, ABC has required this of all its facilities).

The Anywhere plant manager will phase in the HE studies over the next three years. The first unit to be reexamined is the plant's incinerator. This unit was selected because it has undergone several minor design changes over the past two years to correct deficiencies discovered during early operations. Specifically, the following changes have been made:

Process Change A — A redundant air supply fan, designed to automatically start upon low air flow (FIC-1), was added.

Process Change B — A redundant flame scanner (UVL-1B) was added to the shutdown system.

Process Change C — A second incinerator temperature indicator (TI-3) was added, as well as a temperature controller that averages TI-2 and TI-3 to regulate fuel gas flow.

Process Change D — A caustic supply connection and a low pH alarm were added to the quench tank to allow pH control.

All of these design changes were made to solve the operability problems discovered during the first two years. Plant engineering and safety personnel reviewed and approved each individual change prior to installation, in accordance with the Anywhere plant's management of change program.

Available Resources

ABC now has a great deal of material describing the VCM incinerator. They also have two years of operating experience with this unit. The following material is available for the HE team to review:

- Piping and instrumentation diagrams (Figure 17.1)
- Process flow diagrams
- Documentation of previous HE studies of the VCM plant (including the HAZOP Analysis of the original incinerator design)
- Operating and emergency procedures
- Maintenance procedures
- Vendor design specifications, including design basis accidents for relief valves
- Incident reports for the incinerator

Selection of Hazard Evaluation Technique

The Anywhere VCM plant manager has designated Mr. Smart to perform the HE study of the incinerator. Mr. Smart is the process engineer responsible for EDC production. However, he has also worked in the incinerator area during construction, start-up, and the first six months of incinerator operation. Also, Mr. Smart has participated in several HE studies (HAZOP Analysis and What-If Analysis) of the Anywhere chlorine units during his five years at the plant.

The incinerator is a well-defined system with detailed documentation. With the information available, almost any technique could be used for the HE study. Mr. Smart's objective, though, is to identify any new hazards that may have been created because of changes in the incinerator design. With such a broad objective, Mr. Smart quickly rules out the selection of HE techniques that are better suited to focusing on a specific problem (e.g., Fault Tree Analysis, Event Tree Analysis, Cause-Consequence Analysis, and Human Reliability Analysis). He also does not choose experience-based methods such as the Checklist Analysis and Safety Review techniques, because audits were performed when each change was made. Thus, he narrows his choice of HE methods to What-If Analysis, What-If/Checklist Analysis, FMEA, HAZOP Analysis, PHA, and Relative Ranking. The PHA and Relative Ranking methods are discarded because they are too general to use at this stage of the process lifetime. Of the remaining methods, Mr. Smart is most experienced with the HAZOP Analysis technique and therefore chooses it.

Study Preparation

Mr. Smart must select appropriately skilled personnel to assist in the HAZOP Analysis. Since all the design changes to the incinerator were engineered at the

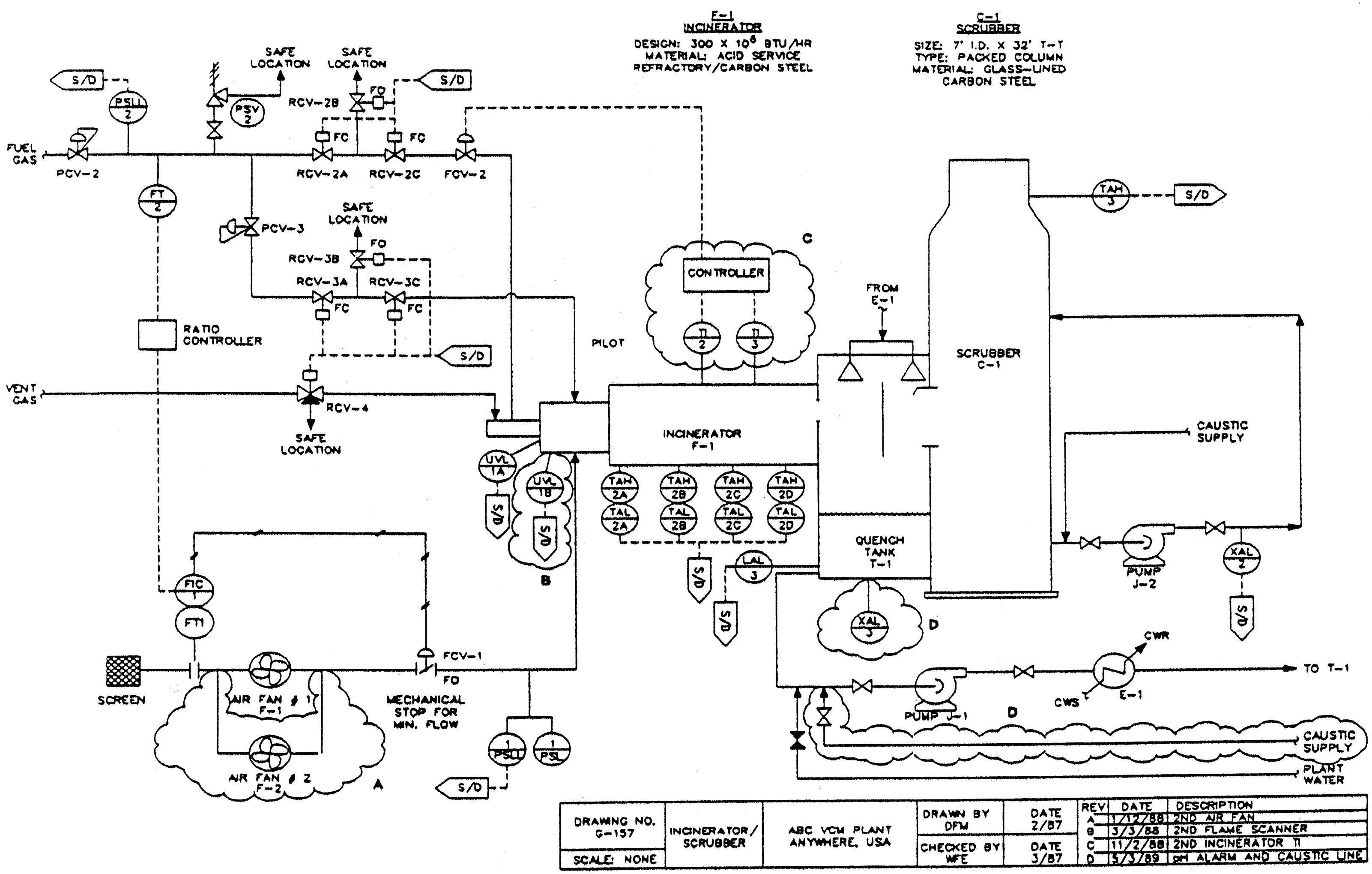

Figure 17.1 Revised incinerator P&ID.

plant, Mr. Smart selects all the HAZOP team members from plant personnel. He selects the following people for this review:

Leader	—	A person experienced in leading HAZOP Analyses. Mr. Smart will be the leader.
Scribe	—	A person who understands technical terms and can record information quickly and accurately. Joe Associate has served as the scribe for ABC HAZOP Analyses before and will fill this position.
Process Engineer	—	A person knowledgeable of the incinerator design and how it responds to process transients. Brenda Piper, a chemical engineer responsible for this unit the last one-and-a-half years, will fill this position.
Operator	—	An experienced person from operations who knows how operators detect and respond to incinerator upsets. David Stedman, an operator for the incinerator since start-up, will fill this position.
Instrumentation and Controls Expert	—	A person familiar with the control and shutdown strategies for the incinerator. Mr. Volt, who designed the instrument changes for the incinerator, will fill this position.

In preparation for the HAZOP meeting, Mr. Smart divides the incinerator into process sections. The incinerator was completely analyzed using the HAZOP Analysis technique prior to construction. To expedite this review, Mr. Smart chooses to analyze only the design changes; therefore, he sections only those portions of the incinerator that had design changes. In particular, the sections Mr. Smart decides to review in this HAZOP Analysis are:

- The air supply line to the incinerator (since a second fan was added to this line)
- The fuel gas supply line to the incinerator (since the FCV-2 control strategy was changed)
- The quench tank water recirculation line (since a caustic supply was connected to this line)

The UVL-1B and XAL-3 instruments provide additional safeguards for the incinerator and quench tank, respectively. Thus, Mr. Smart decides he will review the previous HAZOP Analysis of the incinerator system and insert these new safeguards where appropriate. Even though Mr. Smart will include these instruments as safeguards, he does not plan to consider how these items might fail in the current HAZOP Analysis, since they were analyzed in the previous study.

Next, Mr. Smart sends a memo to all the HAZOP team members informing them of the time and place of the HAZOP meetings. Mr. Smart has scheduled a one-day HAZOP Analysis of the incinerator changes to be held in the plant's training building. Included in the memo is an updated drawing of the incinerator, a list of sections to be examined, the design intention of each section, and a brief description of the HAZOP Analysis method. Mr. Smart asks the team members to bring pertinent information on the incinerator (e.g., operating procedures, incident reports, interlock loop sheets) for reference.

As a last preparation step, Mr. Smart prepares a blank HAZOP table to use in the review. He also prepares a preliminary list of deviations to use. This list will be supplemented with other deviations that the HAZOP team identifies during the review.

17.2 Analysis Description

The HAZOP Analysis begins at 8:00 a.m. on Wednesday when the team tours the unit. Afterwards, they gather in the plant conference room and Mr. Smart starts the meeting by reviewing ABC's corporate policy regarding periodic HE studies of operating units. He also notes that the incinerator was the first unit chosen for reevaluation at the VCM plant, not because of any specific safety concerns, but because it had been modified several times over the past two years. Mr. Smart reviews the schedule for the day and the ground rules for the HAZOP Analysis. (He dispenses with introductions since everyone knows each other.) He then briefly reviews how the technique will work and how Mr. Associate will record the results of the review. Mr. Smart also describes the sections of equipment (or nodes) the team will analyze, the design intent of each section, and the order in which they will review these sections.

To start the review, Mr. Smart asks Mr. Stedman to describe (1) the operation of the air supply line to the incinerator and (2) the reason the second air fan was added. (Note: Mr. Smart purposely wanted to involve the operator, who is normally a quiet person, in the discussions; thus, he asks Mr. Stedman to speak first on a familiar subject.) Mr. Smart then begins the HAZOP Analysis meeting, starting with the deviation "No Flow of air."

Mr. Smart — Okay, let's begin the HAZOP. The first deviation is No Flow of air to the incinerator. What is the consequence of this deviation?

Mr. Stedman — We won't lose air to the incinerator unless we have a plant power outage. If the one fan goes down, the second fan we just added will autostart and make up the supply.

Mr. Smart — Whoa!!! Slow down! I see your point and those are good comments. However, remember that I said we would assume the safety features don't work while we examine consequences. Later we will go back and add the safeguards. Now, David, what happens if you lose air to the incinerator?

Mr. Stedman — Well, the incinerator temperature will drop, you'll get poor combustion, and shortly thereafter the incinerator should shut down on low temperature or possibly loss of flame.

Mr. Smart — What about equipment damage or a flammable/toxic release?

Ms. Piper — The incinerator is hot enough that, if it continues to receive fuel gas or vent gas, we may get an explosion. If not, we definitely would have a flammable gas release out the stack.

Mr. Smart — Okay, so a loss of air could potentially cause a flammable gas release and maybe an explosion. Got that Joe? [*Nods yes.*] What are some causes of low air flow?

Ms. Piper — The obvious ones are the air fan fails off and the air flow control valve (*FCV-1*) fails closed.

Mr. Volt — A low signal from the fuel gas flow indicator (*FT-2*) or a high signal from the air flow transmitter (*FT-1*) will also close the air flow control valve (*FCV-1*).

Mr. Stedman — A plugged air screen will choke the air flow.

Mr. Smart — Joe, are you keeping up? [*Joe shakes head no.*] Okay, the causes so far are: a plugged air screen, an air fan failure, a false high signal from FT-1, a false low signal from FT-2, and air flow control valve FCV-1 failing closed. Any more? [*No answer. Joe breathes a sigh of relief.*] What about a loss of power?

Mr. Stedman — That will stop the fan, but it should also cause the incinerator to shut down because the RCVs on the fuel lines (*RCV-2A/B and RCV-3A/B*) should close and the incinerator is interlocked to trip on a power loss. If it's only a local power loss, then the spare fan should make up the air flow.

Mr. Smart — Okay, that's a safeguard for partial loss of air. Are there any other causes? [*Quiet.*] Okay, what other safeguards are in place to protect against no air flow?

Ms. Piper — The air flow control valve (*FCV-1*) has a mechanical stop to prevent it from fully closing, we have redundant fans with one on autostart, the air screen is cleaned weekly, there is a low-low air pressure (*PSLL-1*) shutdown interlock, there are numerous interlocks on the incinerator, and a loss of power will automatically shut down the incinerator.

Mr. Smart — How often is the autostart fan tested?

Ms. Piper — Well, we put the spare fan in because we occasionally had vibration problems with fan #1 and we can't run the plant without the incinerator up. We've actually used fan #2 three times in the last 18 months. I don't know if it is on a test schedule, though.

Mr. Smart — Do I hear a recommendation here?

Mr. Volt — Yes, we should routinely test the autostart for the fan.

Mr. Smart — What about the fuel/air ratio controller and the fuel/air flow transmitter arrangement.

Ms. Piper — I think the safeguards we have are more than adequate. [*Others nod agreement.*]

Mr. Smart — The next deviation is Low (*Less*) Flow of air. Consequences?

Mr. Stedman — What is low?

Mr. Smart — Outside the normal operating limits. Say the air flow control valve (*FCV-1*) is closed down to the mechanical stop.

Mr. Stedman — You probably have the same consequences as before. Perhaps less severe.

Ms. Piper — I agree. The safeguards are still the same and the causes are the same.

Mr. Smart — Joe, read back the causes and safeguards you just wrote down. [*Joe reads list.*] Are these okay?

Mr. Stedman — Everything but loss of power and the fan failing off are okay for causes. The safeguards are fine.

Mr. Smart — Everyone agree? [*Nods yes.*] Any recommendations? [*None suggested.*] The next deviation is High Flow. Consequences?

Ms. Piper — If the fuel/air ratio is too lean, you again have poor combustion. Since the air flow is high, you probably will sweep unburned flammable gas out the stack. If the flow is high enough you may blow out the flame and cause an incinerator shutdown.

Mr. Smart — Any other damage?

Mr. Stedman — Hopefully, the air will sweep any fuel gas or vent gas out the stack. However, we always worry about a potential explosion whenever we lose the flame in the incinerator.

Mr. Smart — What are some causes for high air flow?

Ms. Piper — Well for starters, the opposite causes of low flow. Air flow control valve FCV-1 failing open, fuel flow transmitter FT-2 outputting a false high signal, or air flow transmitter FT-1 outputting a low signal will do the trick.

Mr. Stedman — How about both fans running at full speed. Can that cause the problem?

Ms. Piper	—	No, the autostart will not turn on fan #2 until fan #1's power is interrupted. Also, air flow transmitter FT-1 would close the damper.
Mr. Volt	—	I don't think that's correct. According to the instrument loop sheets, the autostart for fan #2 is triggered by a low flow signal from FT-1. And besides, an operator could put fan #2 on manual and start it with fan #1 running.
Mr. Smart	—	So air flow transmitter FT-1 outputting a false low signal will start fan #2 and open air flow control valve FCV-1?
Mr. Volt	—	Yes, I believe that's right. I recommend we trigger the autostart from low pressure switch PSL-1. We will need to make sure the second fan gets up to speed before we get a low-low trip.
Mr. Smart	—	Joe, are you keeping up? [*Joe asks the group to wait a minute.*] We jumped ahead to recommendations. Let's back up and discuss the safeguards.
Mr. Stedman	—	The fans are fixed-speed. Also, you have all the interlocks on the incinerator as before.
Mr. Smart	—	Any others?
Mr. Stedman	—	We monitor the air flow as part of our board checks. A good operator would note a faulty air flow reading and correct the problem.
Mr. Smart	—	Would it be caught before the incinerator shuts down?
Mr. Stedman	—	Maybe. Depends on how much time it takes until an incinerator interlock is reached.
Ms. Piper	—	If you blow the flames off the burners, just seconds.
Mr. Smart	—	Any recommendations?
Ms. Piper	—	I agree with Mr. Volt that we should trigger the autostart off pressure switch PSL-1. We should also consider installing a high flow alarm to alert the operator to possible FT-1/FCV-1 failures. By the way, we should use a separate flow transmitter for this alarm.
Mr. Smart	—	Okay, but let's not design the solution. I've got your ideas noted and we'll leave the design work to engineering and instrumentation and controls. Other recommendations? [*Pause.*] The next deviation is Low Air Temperature. Consequences?
Ms. Piper	—	We use ambient air. Even on the coldest day, I don't believe the incinerator would see any impact other than using slightly more fuel.

Mr. Smart — Okay, so there is no significant consequence. Let's move on to the deviation High Air Temperature?

Ms. Piper — Again, I don't think it would do anything.

The HAZOP questioning continues throughout the day until all the deviations postulated by the team are examined for the three process sections (air line, fuel line, and quench tank water recirculation line). At this point Mr. Smart is ready to close the meeting by reviewing the recommendations made. However, Ms. Piper raises an additional issue.

Ms. Piper — Before we stop, I think we should examine the added flame detector. We've discussed all the equipment and instrument changes except this one.

(Note: The team discussed the new pH monitor [XAL-3] when they examined the new caustic line.)

Mr. Smart — I didn't include the UVL instrument change as a separate item in the HAZOP Analysis because it is solely an added safety feature. I didn't see any safety implications with this change.

Ms. Piper — I see your point. But I would have said the same thing about the second air fan before we examined it.

Mr. Smart — You're right. However, rather than HAZOP the entire incinerator or shutdown system, why don't we just perform a failure modes and effects analysis on this change? [*The others agree after Mr. Smart explains what an FMEA is.*] Okay, how can the UVL detector fail?

Mr. Volt — It can fail to detect loss of flame and it can inadvertently initiate a shutdown signal when no problem exists.

Mr. Smart — Any other failure modes? [*No answer.*] What is the effect of the UVL failing to detect loss of flame?

Ms. Piper — If the incinerator is operating normally, none. If there is a flameout, then you only have one detector to protect you. You may get an explosive mixture in the incinerator.

Mr. Smart — Safeguards?

Ms. Piper — We have a second flame detector. Also, we have the temperature interlocks on the incinerator.

Mr. Smart — Recommendations? [*None suggested.*] What is the effect of a false flameout signal?

Mr. Volt	—	A false signal from either UVL will cause an incinerator shutdown. As long as the fuel is shut off, there's no danger.
Mr. Smart	—	And if fuel isn't shut off, do you have an explosion potential?
Ms. Piper	—	Yes! The incinerator will become fuel-rich for a period of time. But operators will eventually shut off the fuel supply. We may then reach a point as air leaks into the incinerator where the fuel/air mix is flammable.
Mr. Smart	—	What safeguards exist?
Mr. Stedman	—	The UVLs haven't given us any problem thus far. I think the second UVL was put in just to give us a better scan of the fire.
Mr. Smart	—	Okay, we'll note that the UVLs have been reliable. Any other safeguards? [*None suggested.*] Any recommendations?
Mr. Volt	—	We might want to consider a voting system for the UVLs like we have for the incinerator thermocouples.
Mr. Smart	—	Why don't we suggest that the reliability of the UVLs be examined to determine if a voting system is needed? Does that sound okay? [*Others agree.*]

Mr. Smart then closes the meeting by reviewing the recommendations made during the course of the day. He also asks that the team members review the report he will prepare for management when it is ready. Finally, he thanks the team for their participation and compliments them on the excellent review.

17.3 Discussion of Results

The results of the HAZOP Analysis and the FMEA were handwritten on the blank table prepared by Mr. Smart. After the meeting, Mr. Smart and Mr. Associate transcribe these notes into a formal, typewritten table. This table describes, on a cause-by-cause basis, the results of the HAZOP Analysis. Word processing software was used to facilitate this effort. Tables 17.1, 17.2, and 17.3 list a portion of the team's findings.

Some of the important findings from this review are the following:

- Ensure the redundant air fan autostart will not be triggered by FT-1 malfunctions.

- Verify the UVL reliability, and consider a UVL voting system if the reliability is not acceptable.

Table 17.1 Sample HAZOP Analysis Results for the Routine Operation Phase

P&ID No: E-250
Revision: D
Meeting Date: 9/5/90
Team: Mr. Smart, Mr. Associate, Ms. Piper, Mr. Stedman, Mr. Volt (all from the ABC Anywhere Plant)

Item Number	Deviation	Causes[a]	Consequences	Safeguards	Actions
1.0 LINE — AIR SUPPLY LINE TO INCINERATOR (INTENTION: SUPPLY 15,000 SCFM OF AIR TO INCINERATOR AT AMBIENT TEMPERATURE AND 3 IN. WC)					
1.1	No flow	1 — Air fan #1 fails off 2 — FCV-1 fails closed 3 — FT-1 fails — high signal 4 — FT-2 fails — low signal 5 — Loss of electric power 6 — Plugged air screen	A — Incinerator shuts down. Possible release out the scrubber stack. Potential incinerator explosion if shutdown interlocks fail	1 — Redundant fan on standby with autostart A — Low-low air pressure (PSLL-1) shutdown interlock 1,2,3,4,6 — Multiple incinerator shutdown interlocks (temperature, flame) 1,5 — Automatic shutdown upon loss of electric power 6 — Air screen cleaned weekly 5 — FCV-1 fails open on loss of electric power 2,3,4 — Mechanical stop on FCV-1	1 2
1.2	Low flow	1 — FCV-1 fails — partially	A — Inc[illegible]ator shuts down.	1,2,3 — Mechanical stop on	

				2,3,4 — Mechanical stop on FCV-1	
1.2	Low flow	1 — FCV-1 fails — partially closed 2 — FT-1 fails — high signal 3 — FT-2 fails — low signal 4 — Plugged air screen	A — Incinerator shuts down. Possible release out the scrubber stack. Potential incinerator explosion if shutdown interlocks fail	1,2,3 — Mechanical stop on FCV-1 4 — Air screen cleaned weekly A — Low-low air pressure (PSLL-1) shutdown interlock A — Multiple incinerator shutdown interlocks (temperature, flame)	
1.3	High flow	1 — FCV-1 fails open 2 — FT-2 fails — high signal 3 — FT-1 fails — low signal 4 — Operator inadvertently starts fan #2 (fan #1 still running)	A — Poor combustion, with potential release of flammable gas out the scrubber stack. Excessively high air flow may blow flame out causing a shutdown	A — Multiple incinerator shutdown interlocks (temperature, flame) 4 — FT-1 closing to reduce air flow	2 3
1.4	Low temperature		No consequences of interest		
1.5	High temperature		No consequences of interest		

[a]The consequences and safeguard numbers correspond to the numbered causes. The letter "A" indicates that the respective consequences and safeguards apply to all of the listed causes.

Table 17.2 Sample Action Items from the Routine Operation Phase

List Number	Action to be Considered	Responsibility	Status
1	Establish a periodic program for testing the autostart fan (Item 1.1)	Ms. Piper	To be completed within 50 days
2	Consider using PSL-1 to autostart the standby fan (Item 1.1 and 1.2)	Mr. Volt	To be completed within 60 days
3	Consider installing a high flow alarm on the air supply line (independent of FT-1) (Item 1.3)	Mr. Volt	To be completed within 30 days

Table 17.3 **Sample FMEA Results for the Routine Operation Phase**

P&ID No: E-250
Revision: D
Meeting Date: 9/5/90
Team: Mr. Smart, Mr. Associate, Ms. Piper, Mr. Stedman, Mr. Volt (Anywhere VCM Plant)

Item Number	Component	Failure Mode	Effects	Safeguards	Actions
1	Flame scanner UVL-1B	No signal change	Loss of capability to initiate an incinerator shutdown upon loss of flame. Potential incinerator fire or explosion if flame extinguished	Redundant UVL Multiple incinerator interlocks (temperature, fuel, and air)	
		False flameout signal	Inadvertent incinerator shutdown. Potential incinerator explosion if incinerator fuel not shut off	Shutdown is alarmed. Operators verify shutdown actions Double block and bleed valves in fuel lines Three-way shutoff valve in vent line	Verify the reliability of the UVLs

- Program the controller associated with TI-2 and TI-3 to ignore an out-of-bounds temperature signal.

- Verify that the design and construction materials of circulation pump J-1 and heat exchanger E-1 can withstand high pH service.

Next, Mr. Smart prepares a report of the HAZOP Analysis and the FMEA. This brief report contains a list of the team members, a list of information used, a summary of the team's recommendations, and detailed HAZOP and FMEA tables. Also included in this report is a description of the review's scope and a copy of the updated P&ID used in the study. After the team members review this report, Mr. Smart sends it to plant management.

17.4 Follow-Up

All of the questions raised during the HAZOP Analysis were eventually resolved. Also, the team found no problems that needed immediate attention by management. After completing and transmitting the report to the plant managers, the HAZOP team was finished. Plant management reviewed the recommendations made, accepted them, and assigned the incinerator area supervisor the responsibility of resolving each recommendation. The supervisor assigned the recommendations to appropriate personnel. He checked on the status of implementation monthly until all recommendations were resolved. The HAZOP report and resolutions of each recommendation (documented by the supervisor) were placed in the engineering files for the incinerator.

17.5 Conclusions and Observations

The HAZOP Analysis (and FMEA) went well because Mr. Smart was prepared, the right team of skilled personnel was assembled, and Mr. Smart involved everyone in the review. The HAZOP Analysis took only six hours. To expedite the review, Mr. Smart examined consequences of deviations before inquiring about causes and safeguards. If the consequence was of no concern, he quickly moved on to other deviations. Mr. Smart also kept the team focused, quickly curtailing unproductive side discussions and avoiding excessive time spent on designing solutions to problems.

Mr. Smart also expedited the review by not arbitrarily sticking with one HE method. Upon realizing that the flame scanner must also be reviewed, he chose the FMEA technique to examine this one piece of hardware. The FMEA method is well suited to examining the impacts of hardware failures. Table 17.4 summarizes the time required to perform the HAZOP Analysis.

One of the pitfalls Mr. Smart avoided was using the previous incinerator HAZOP Analysis as the basis for the current HAZOP Analysis. The previous HAZOP Analysis results were shared with the current HAZOP Analysis team members before they began the second review, but these results were not used as a "checklist" for the current HAZOP Analysis. Although using the results of an earlier study as a checklist appears to be an effective way to review a system,

Table 17.4 HAZOP Analysis Staff Requirements for the Routine Operation Phase

Personnel	Preparation (hr)	Evaluation (hr)	Documentation (hr)
Leader	4	6	12
Scribe	2	6	16
Team Member[a]	1	6	1

[a]Average per team member.

Mr. Smart attended some HAZOP Analyses in the chlorine plant where this approach proved to be a mistake. More often than not, the team tended to analyze only whether the changes could cause process upsets rather than thinking of other ways such upsets could occur.

One final observation is that the team did develop a few recommendations with respect to the changes made. ABC had modified the incinerator slightly over the past two years to remedy some operability problems. The modifications improved the availability of the incinerator and apparently enhanced its safety. However, the HAZOP Analysis identified some failures related to these changes that could create safety problems — even after the modifications had been through the usual plant engineering reviews.