Formal Operability And Hazard Analysis

As Applied To A

Modern Sulfuric Acid Plant

By

Leonard J. Friedman
Acid Engineering & Consulting, Inc.
Lakeland, Florida

I Introduction

Sulfur burning sulfuric acid plants are considered, by many, a mature design, with the contact process evolving to its current form over the past seventy years. Significant changes in plant size, operating pressures and temperatures, and designs that reduce safe operating margins to a fraction of previous levels have occurred in the 1980's. With the changes has been an increase in the number of incidents and catastrophic failures resulting in lost production, equipment damage, environmental releases and injury to personnel.

Formal Hazard and Operability Analysis (Haz-Op) of new and modification projects is the standard route the petroleum, petrochemical and chemical industry has chosen to minimize hazards affecting production, personnel or the environment. In fact, in essentially all of these companies no project (new or modification) can proceed without a formal Haz-Op.

The fertilizer industry traditionally has used a more informal approach, relying on the design engineer and plant engineering, operating and maintenance personnel to perform an individual review based on their extensive operating and/or design experience. This informal procedure has worked to a large degree, however, as plants become more complex and safe operating margins diminish, personnel safety, environmental consequences and financial exposure demand a more formal analysis.

This work will attempt to convince the reader of the advantages of a formal Haz-Op. It will outline the methods used in a formal hazard and operability analysis, and using a number of recent incidents, demonstrate how a Haz-Op may have reduced the damage or prevented the incident.

II Development - Why a Formal Haz-Op?

For many years I believed the informal review by experienced operations, maintenance, and engineering people was sufficient to provide an operable, safe plant. After looking at the experience of the 1980's, and especially the problems with the recently developed acid heat recovery systems, I now believe the only approach to minimize hazards and risks is a **"Formal" Hazard and Operability Analysis.**

My first exposure to a formalized hazard analysis was in the early 1960's when I was working for Nuclear Fuel Services, Inc. during the construction and initial operation of the first pri-

vately owned power reactor fuel reprocessing plant. The plant received spent fuel elements from nuclear reactors and recovered the uranium (low and highly enriched), plutonium, americium, neptunium and other valuable components from highly radioactive fission products using the Purex process.

All privately owned nuclear facilities (power reactors, research reactors and reprocessing plants) required an operating license from the Atomic Energy Commission, "AEC" (now Nuclear Regulatory Commission). One requirement of the operating license procedure was a "Safety Analysis", to prove to the AEC the plant was safe and could be operated without risk to plant personnel, the general public, or the environment. When I arrived on site the plant was under construction and the initial Safety Analysis, consisting of four, 3" thick volumes, was in the hands of the AEC. We received the first set of what seemed like an endless supply of additional questions and concerns. The final Safety Analysis took another six months to complete and filled an additional seven volumes. This Safety Analysis procedure, although cumbersome, uncovered a number of areas of concern making me a believer in the advantages of a formal procedure. Two of the AEC concerns demonstrate this:

1. The nuclear fuel was chopped into small pieces and loaded into baskets that were suspended in a dissolver vessel. Six baskets were put into the dissolver equally spaced around the annulus with concrete separating each basket. The AEC simply asked us to prove the system was critically safe. From a nuclear criticality point of view this was a very complex system, solid fuel (uranium - plutonium), partially dissolved fuel as a slurry, dissolved fuel in solution, interaction of other vessels in the operating cell, various levels of neutron absorbing fission products, with the concrete in the middle of the vessel to absorb sufficient neutrons to maintain the system critically safe. After about three months of manual and computer (remember this is the early 60's) calculations we concluded the system was close to being critical under some operating conditions (loss of agitation) and required additional neutron absorption. Once the problem was identified and considered possible, the group concentrated on a solution. The solution was simple and low cost, involving adding small boron glass pieces (frits) in place of a portion of the fine aggregate in the concrete (and testing the concrete to insure its strength and uniform distribution of frits). If the safety analysis procedure were not required, the potential existed for the dissolver system to go super critical - uncontrolled nuclear reaction - with possible major radioactive contamination and radiation exposure to both in plant personnel and the surrounding population.

2. A number of plant vessels, where phase separations were required contained an expanded vessel diameter, were made critically safe by filling the vessel with boron glass raschig rings to absorb neutrons. The AEC questioners asked us to prove the glass rings would not break, leaving a portion of the vessel without rings. After many hours of thought the technical team devised a plan to separate good rings from rings that could break. Each day for about three weeks the local towns people and AEC representative watched a group of nuclear engineers throw glass rings at a concrete wall. The rings surviving the test were used in the plant.

Although I was fresh from school, the staff was composed of over ten nuclear engineers, each with over twenty years of experience in the design and operation of fuel reprocessing plants (dating back to the Manhattan Project). They came from Oak Ridge National Laboratory, Argone National Laboratory, Hanford Works, and National Reactor Testing Center in Idaho, with an enormous wealth of knowledge and experience. Still the formal safety analysis procedure and questioning (by what I believed to be a group of not so sharp bureaucrats) was instrumental in avoiding a number of potentially disastrous incidents - millions of times more severe than Three Mile Island. From the examples, you can see the questions were not complicated or sophisticated, but of the "what if" type.

In the late 1960's and early 1970's I worked in the central engineering departments of two major chemical companies; Stauffer Chemical Company and Olin Corporation. The Stauffer engineering center provided the design and construction for essentially all Stauffer plants, including insecticide-herbicide, silicones, chlorine-caustic, sulfuric acid, elemental phosphorus, food grade phosphoric acid, chlorinated hydrocarbons, vinylchloride monomer, PVC, etc. With this wide range of processes a formalized procedure was required to review the designs. The reviews included a process department review, a chemical engineering department review, a project review, engineering department review and finally an operating department review.

The process review covered the process design and piping and instrument diagrams. It was aimed at insuring the basic process and equipment sizing was correct, in addition to a line by line review for operation, control, safety, etc. The chemical engineering department review added instrument, mechanical, vessels and electrical personnel to the review team with the aim directed more toward system control, equipment design criteria, design margins, interlocks, start-up and upset conditions. The project and engineering department reviews added less technical project and management people to the team, with their overall experience, for a review of previous meetings conclusions and a look toward cost savings and layout. After the engineering reviews, a final review was made with operating department personnel, to tell them what they were getting. In addition, each capital project required a separate risk analysis to accompany the capital appropriation request to the board of directors. The risk analysis was an independent review of the projects exposure (risks) - environmental, financial, regulatory and general public. The financial exposure included such areas as meeting plant capacity, product specifications, reliability, production interruptions, process and environmental hazards, etc.

Although the number of reviews and personnel present at each review were included in a formal procedure, the actual review itself was left to the people assembled. The large number of reviews tended to "cast in stone" the design accepted at the previous review. The Stauffer method was better than an informal procedure, but still left much to be desired, and had the major disadvantage of not involving the operating personnel early in the design, when it was more flexible to change.

NOTE: Essentially all contractors currently have a line by line process department and project review for operability and safety. Some call it a piping and instrument drawing review and some a Haz-Op. However, it is not a Haz-Op in the accepted context, but is similar to the Stauffer procedure - a formal meeting with the review procedure left to the reviewers. The contractors review does not include operating company risk (as defined above), or the possibility of incorrectly sized equipment (covered by vendor guarantees).

After a series of incidents at a number of refineries, petrochemical and chemical plants in the early 1970's causing severe plant damage, injuries and death, the industries moved to adopt methods to prevent future incidents. The method, adopted in one form or another by all, is a **"Formal" Hazard and Operability Analysis.** Today in essentially all chemical companies no capital project or plant modification is approved without a Haz-Op. NOTE: The term Haz-Op as defined here includes both the micro and macro analysis of a project - the formal line by line review, the system review, and the exposure - risk analysis. In addition, engineering societies formed safety sections, offering regular meetings where companies with similar operations could share safety procedures and review design improvements and incidents.

III What is a Hazard & Operability Analysis?

A hazard and operability analysis is a formal technique aimed at stimulating designers and operators in a systematic way so they can identify and develop solutions for the potential hazards, operating problems and risks in a design or plant modification. In the "Examination Session" a multi-disciplinary team uses a formal procedure to examine all parts of a design. The Haz-Op procedure uses "Key or Guide Words" to focus the examiners and help them visualize the ways in which a unit or system can malfunction. Typical "Key Words" are shown in Table 1 and "Key Word Reminder List" in Table 2.

The composition of the Haz-Op team is critical to the success of the analysis procedure. A normal team is composed of design and operating personnel of varying disciplines and experience, a team leader and recorder. The technical team members usually include:

Process Engineer(s)
Research Chemist, Engineer - Development Engineer
Detailed Design Engineers - Instrument, Mechanical, Electrical, Civil
Project Manager and Project Engineer
Production - Operations Manager
Maintenance Manager
Reliability Engineer
Safety Engineer

The team leader directs the analysis and keeps the group under control and focused. The leader should posses the ability to plan and control the Haz-Op based on technical and managerial skills developed from experience in operations and design engineering. The leader should not be closely associated with the subject of study (to maintain objectivity). A recorder is the final member of the team, there to maintain a written record of the analysis, hazards, solutions and outstanding items for further study; freeing the rest of the team to concentrate on the Haz-Op.

The team leader guides the team members in a systematic approach to cover all parts of the plant and all conceivable malfunctions and maloperations. The questioning is focused one by one on each part of the process using the "Key Word" and "Reminder Word" lists to insure all possible deviations will be covered.

The method produces a number of theoretical problems, and each is considered to determine possible causes and results. Some of the causes may be unrealistic and the result is considered not meaningful, some are trivial and excluded from further consideration. However, some have causes which are possible and results that are potentially hazardous or have severe financial exposure, these are noted for corrective action. The procedure continues until all parts and sections of the process are analyzed. Finally a team is selected to study and correct the hazards and/or risks detected, and a second Haz-Op is held to review the modified design. Occasionally a design will include an inherent problem, that after all reasonable efforts, can not be handled by modifying the design. In this case a "Risk" is identified, and highlighted as a part of the appropriation request to management.

IV Haz-Op Analysis of Sulfuric Acid Plant Incidents

This section will review a number of recent sulfuric acid plant incidents and show how a Haz-Op may have reduced or prevented the damage. In addition, we will apply some of the Haz-Op guide words to a relatively new process (acid heat recovery system) and see if there are risks or areas for improvement.

A. Absorption Tower Packing Collapse

The packing support in a sulfuric acid absorption tower failed during plant start-up after a turnaround and the packing collapsed into the bottom of the tower. The plant was down for over four weeks while a new packing support and packing were installed. The incident resulted in a repair cost of about $650,000 and four weeks of lost fertilizer and electric power production. The plant considered itself lucky, since materials and equipment were available on short notice to repair the tower, limiting the financial loss.

An investigation of the incident revealed the following:

1. The plant was in start-up, with sulfur feed to the furnace for about two hours.

2. The main blower low - low discharge pressure, blower surge protection interlock, was in start-up bypass mode.

3. The acid pump tank level dropped more than usual - operators attributed the level drop to normal acid hold-up in the tower packing.

4. The main blower went into surge, and the blower and plant were manually shut-down by the operator.

5. When the acid pump tank reached low level, the operator shut-down the circulating pump.

6. With the plant down it was determined the tower packing support and packing were in the bottom of the tower. The pump tank, pump, and remainder of the system were relatively free of brick or packing pieces.

The investigation concluded the following scenario was the cause of the packing collapse:

1. Some bricks were dislodged from the acid brick arch supporting the Aludur packing support beams. The bricks partially blocked the tower bottom acid outlet, causing acid to build-up in the tower bottom.

2. The acid level increased into the gas inlet nozzle causing waves in the acid and fluctuations in the main blower discharge pressure.

3. The acid level continued to increase, with the waves sufficient to knock over the brick arches, causing the packing support and packing to drop into the bottom of the tower.

4. When the level in the tower increased to block the gas inlet sufficiently to cause the main blower to surge, the plant was manually shut-down. The acid circulating pump was shut-down on low level (alarm) in the pump tank.

The tower sketch (Figure 1) shows the bottom section of the absorption tower. Now let's imagine a portion of the Haz-Op looking at the acid tower. One question from the key word list would ask about "low or no flow" through the tower outlet line. The analysis would conclude that, if the tower acid outlet was blocked or restricted, acid would build up in the tower, blocking the gas inlet, causing acid waves and the main blower to surge. In the start-up condition, the plant would keep running. Is it possible for the outlet to be blocked? Yes, if some bricks come loose. Will the blockage cause a hazard, equipment failure, etc? Yes. There-

fore, a few simple questions from the list would have detected the potential problem. As is the case with most plant problem areas, once they are identified the solution is obvious and low cost. Here, adding a high level alarm to the tower bottom area can detect the problem and shut the plant and circulating pump down - preventing the incident. NOTE: I am only aware of a few acid plants in the world with tower high level alarms or trips. Some would say they have operated acid plants for many years without this problem. The answer to this argument is: Is it possible for this to happen? Yes. Will this problem cause equipment damage and lost production costing over $1 Million? Yes. Can the potential problem be detected to prevent the damage? Yes. Is the cost of prevention reasonable? Yes. Therefore, a protective device should be incorporated in the design.

B. Sulfur Explosion

In the last ten years there have been a number of sulfur explosions in sulfuric acid plants, all attributed to operator error. Each incident involved an operator accidently closing dampers that restricted or shut off air flow. The following are two examples of sulfur explosions:

The first incident, Figure 2, involves a 1000 STPD sulfuric acid plant. During a restart a sulfur explosion occurred in the rear of the furnace, connecting duct to the boiler, and boiler hot channel. The force of the explosion broke the furnace and boiler loose from their fixed anchors, forcing them apart. Damage included deformed and twisted boiler riser and down comer piping, and furnace, transition and boiler brick damage. Repairs were completed in six weeks at a cost of about $500,000 (not counting lost production). An investigation of the incident found the following:

1. The plant had been experiencing a number of interlock trips during the week prior to the incident.

2. The trips were attributed to a "midnight gremlin" (unknown person reduced the setting on a motor heater, causing the motor to trip at full load). An immediate restart of the plant was possible.

3. The incident occurred shortly after a restart of the plant following a trip. The restart was at full rate with the blower brought to pre-trip discharge pressure and the sulfur value to pre-trip output. During the restart all gas dampers (manually operated) were in the pre-trip position.

4. The No. 1 catalyst bed inlet temperature was increasing. The control room operator instructed his outside operator to close the boiler bypass damper 10%. The No. 1 bed inlet temperature continued to increase and the outside operator was instructed to close the boiler bypass completely.

5. The No. 1 bed temperature increased more rapidly, and the control room operator instructed the outside operator to re-check the boiler damper positions. The operator had erroneously closed the boiler exit damper instead of the bypass damper.

6. In his rush to correct the error, the outside operator closed the boiler bypass damper completely. His intent was to then open the boiler exit damper, less than fifteen feet away.

7. The blower went into surge making a loud noise (blower surge protection system in start-up bypass, so no trip), followed by a "boom" and "screech". The control room operator hit the plant trip button shutting down the plant.

The second incident, Figure 3, involves a somewhat similar scenario. Dampers in sulfuric acid plants tend to stick (build-up of scale and/or sulfates) if not actuated regularly, so many plants move all gas dampers on a regular schedule to insure freedom of movement. A sulfur explosion occurred in the top section of the converter during a scheduled damper movement check. An operator erroneously partially or completely closed both dampers around a steam superheater. The resulting sulfur explosion tore a section of converter roof and inlet duct, tossing them over fifty feet.

In both cases operator error was the stated cause of the incident involving major equipment damage and lost production. I believe that's putting one's head in the sand and taking the easy way out. The operator did make an error resulting in the incident, however, since none of us has been made perfect (never made an error or mistake), the plant design should have considered the possibility of an operator error and a protection system incorporated in the design to prevent the incident.

Here again the Haz-Op analysis would have asked the question concerning air flow - low or none. Low or no air flow (with sulfur on) could cause a sulfur explosion. Is it possible? Yes, if two dampers are partially or completely closed. Therefore, the Haz-Op would have identified the potential hazard and a team directed to develop a solution. One solution used by many plants is a main blower low-low discharge pressure trip - surge protection interlock. This surge protection scenario is: When the air flow is blocked the blower discharge pressure will increase until the blower goes into surge - the air flow will go up and down along with the blower discharge pressure. After one surge the low-low discharge pressure trip will shutdown the plant. This system requires an interlock bypass to allow starting the blower (and plant). NOTE: The first example occurred during start-up with the interlock in bypass, and many plants either do not have a blower surge protection system or operate with it bypassed or jumpered. Also, at low air flow the blower surge protect system may or may not trip the plant. The severe equipment damage, lost production and the potential for personnel injury or death resulting from a sulfur explosion demands a more in depth analysis and improved designs.

C. Acid Pump Tank Explosion

A sulfuric acid plant was down for repair of an acid leak. When the acid circulating pump was started, the roof of the pump tank separated from the tank side walls, breaking the acid piping. About fifteen thousand gallons of strong sulfuric acid was released to the ground in the acid system area of the plant. Investigation of the incident reported the following (Figure 4):

1. The plant was shutdown to repair an acid leak, with some other maintenance items performed during the down time.

2. The acid circulating pump was down to permit work on the acid system.

3. The dilution water control valve was put in manual and set closed. In addition, the interlock system in this plant automatically closed the water valve when the pump was shut-down.

4. When the repairs were completed (after six hours) the acid circulating pump was started. Within seconds of the pump starting the pump tank experienced a rapid release of pressure (explosion), with the tank roof and connecting piping moving in an upward direction. The piping was ruptured and about 15,000 gallons of sulfuric acid was discharged to the ground in the acid area of the plant.

5. A new pump tank and piping was required to make the plant operational again - eight weeks of down-time

Analysis of the incident indicated water was leaking past the closed control valve into the acid pump tank. The acid formed a water layer on top of the denser acid. When the pump was started the acid and water mixed and the heat of dilution of acid raised the temperature producing steam. The steam pressure increased rapidly (explosion) overcoming the open 6" tank vent, and was sufficient to cause the failure of the tank roof and piping.

A formal Haz-Op would have included the key word reminder list question of water flow into the pump tank when the pump was down. Is it possible? Yes, if the valve leaks. Will leakage of water cause a hazard? Yes. Here again the design change to prevent an incident of this type is simple and low cost. One solution is to add a double block and bleed to the dilution valve interlock, so even if both block valves leak, water will flow to the ground instead of the acid pump tank.

NOTE: Very few plants incorporate an interlock to close the dilution water valve on pump shutdown, and I am not aware of any with an interlock double block and bleed system. Most plants rely on the operator to manually close the dilution water control valve and some plants require closing of a manual block valve - reliance on the operator to be perfect.

D. Acid Heat Recovery System

With the increased need for energy recovery, a number of operating companies are considering recovering heat as steam from the acid system. Two acid plant contractors (Monsanto and Lurgi) have developed and installed commercial acid heat recovery systems, producing low pressure steam from absorption tower acid. Lurgi has one unit in operation, and Monsanto has constructed four units at three sites (Korea (2), Norway, Belgium) with two of the units still in operation and one under repair. The systems can be constructed as an add-on unit or integral with the acid absorption tower.

A typical Monsanto type integral acid heat recovery system flow diagram is shown in Figure 5. The heat recovery system uses an austinetic stainless steel (310) for all equipment and piping. Many in the industry have been aware (over twenty years) austinetic stainless steels are resistant to sulfuric acid at elevated temperatures (400^{o}F range) in sulfuric acid above 99%. A number of plants constructed in the late 1960's had stainless steel gas inlet distributors. Until recently designers and operators have not used stainless steels at these temperatures because of the very narrow safe operating range. As you can see in Figure 5, acid temperatures are in the range of 380^{o}F to 430^{o}F with +99% sulfuric acid, and steam produced at 150 psig.

With any new process scheme problems are expected and the acid heat recovery system is no exception. One of the units in Korea and the units in Norway and Belgium have experienced major damage resulting from weak acid in the system.

Korean Plant (Namhae) - In the case of the Korean plant (the first commercial units constructed by Monsanto), the action of the heat recovery system concentration control instrument was set backwards. On start-up the reverse acting concentration controller diluted the acid below 97.5%. It took about two hours to bring the acid strength up to the proper range. Inspection of the plant indicated general corrosion of the system and severe damage to the high velocity acid circulating pump impeller and wear parts. Other problems in the plants included severe vibration and corrosion of the dilution water addition pot and tower acid distributor, and severe acid (carry-over) corrosion of the interstage gas heat exchanger.

Norway (Falconbridge) - The acid heat recovery unit in Norway experienced severe damage after a short operating run as a result of weak acid in the system. The unit has been down since the incident on September 29, 1989. The following facts are available:

1) There was an emergency acid plant shutdown due to a ruptured cooling water line.

2) The final tower acid pump tank dilution water valve remained open, instead of closing to shut off the dilution water flow.

3) Water flowed into the final tower pump tank for about one hour and twenty minutes at an unknown rate, diluting the acid to an unknown concentration.

4) After plant start-up, this weak acid was pumped to the acid heat recovery system.

5) When circulation was started, instrumentation showed a rapid fall in concentration of the acid in the heat recovery system to at least 98%.

6) Due to the temperature effects of conductivity (used to measure acid concentration) the operators were unsure of the acid concentration, but believed it was around 97.5% to 98%. The concentration instrument used has a range of 97.5% to 100%.

7) Back-up instruments to measure corrosion were installed but out of service.

8) The acid steam boiler developed an internal leak, causing further dilution of the acid, increasing the corrosion rate.

9) The plant was shutdown after leaks developed in the acid piping. Draining of the system took many hours. The entire system was severely damaged and is not being repaired.

Belgium (Tersenderlo) - The incident at the acid plant in Belgium occurred in late 1990, and was also due to weak acid. In this case, the heat recovery unit was in its initial start-up with Monsanto start-up personnel on site. A pin hole leak developed in a boiler tube weld, rapidly expanding and diluting the acid causing severe corrosion. The failure was attributed to poor quality control by the boiler vendor (the boiler had passed a code type hydrostatic test before installation). Reconstruction was projected to take six months and cost millions of dollars (not counting lost energy - acid and down-stream plant production).

Are all three of these incidents caused by the boiler vendor, instrument set-up error, or operator error, or are they inherent in the system as designed? I believe these incidents and/or the severity of the equipment damage could have been prevented or mitigated if a proper Haz-Op had been performed. A Haz-Op would have identified the potential problem areas and a design team formed to develop solutions.

E. Haz-Op Comments - Acid Heat Recovery System

If some of the Haz-Op key words are applied to the acid heat recovery system shown on Figure 5, a number of potential hazards and/or risks are easily identified. Then for each hazard or risk a possible solution can be presented.

It is obvious, one of the most significant problems (hazards and risks) in the acid heat recovery system is the result of the acid concentration being less than 99% in the 310 stainless steel used for system piping and equipment. Applying the key word "acid concentration low" to the system as a whole would identify a number of very possible causes of low acid concentration, and the significant hazard and financial risk.

Key Word	Possible Causes	Hazard/Risk
Acid Concentration Low	1. Concentration Instrument Error 2. Boiler Leak 3. Start-up-Conc. Inst. Low Temp. 4. Start-up-98.5% Acid Low Concentration 5. Down-Dilution Water Valve Leaks/Not Closed 6. Water Flow High 7. 98.5% Acid Flow High	a. Severe Corrosion b. Damage To Unit c. Acid Spill d. Long Total Acid Plant Down Time e. High Repair Cost f. Lost Acid and Fertilizer Prod.
Concentration Instrument Incorrect Reading-Low	1. Out of Temperature Compensator Range 2. Out of Instrument Range 3. Pump Down-No Reading 4. Pump Down-Dilution Valve Leaks	a. Low Acid Conc. (See Above)
98.5% Acid Flow - High	1. System Down-Flow Valve Stays Open or Valve Leaks	a. Low Acid Conc. (See Above)
Boiler Tube Leak	1. Tube-Tubesheet Conn. Leak 2. Bad Tube	a. Low Acid Conc. (See Above)

System Modifications To Minimize Hazards Or Risk - Once the possible causes of a hazard or risk are identified, in many cases, alternate materials, equipment or system modifications are easily found. For example, the following system modifications can be proposed to mitigate the hazard, damage and financial exposure from a low acid concentration incident.

1. Catastrophic corrosion failure of the acid heat recovery system installed integral with the acid absorption tower (system shown in Figure 5) will result in acid release to the environment (piping and equipment failure), personnel exposure to hot acid from leaks, and major financial exposure (the cost to repair the unit, lost sulfuric acid, electric power, and fertilizer production). One obvious system modification to limit the financial exposure to the acid heat recovery system and its energy production, is to install the heat recovery system as an add-on unit. Then, when a catastrophic failure occurs, the unit can be bypassed, and the sulfuric acid plant continue to operate at full rate.

2. To reduce the potential damage to the heat recovery system from low acid concentration the system materials of construction can be changed to less acid concentration sensitive materials. For example, an acid brick lined tower and pump tank, Teflon lined piping, etc. will be resistant to all concentrations of sulfuric acid, limiting potential damage to the boiler and circulating pump.

3. To reduce the potential of a boiler leak causing severe damage to the boiler and entire heat recovery unit, the boiler can be arranged with the acid pressure higher than the water - steam pressure. A leak will then flow from acid to water and can be easily detected for system shut-down with steam vented and water drained. In addition, a leak from acid to water will not cause the leak spot to corrode further increasing the leak, or cause corrosion of the entire heat recovery system.

4. To further reduce the potential for boiler leaks, a double tube-sheet boiler design can be used. It is common engineering practice for processes requiring separation of fluids in a heat exchanger to use a double tube-sheet design with a drain between the two tube-sheets (similar to a double block and bleed arrangement).

5. Other modifications could include: double block and bleed for dilution water and 98.5% acid interlocked to the circulating pump and acid strength; multiple concentration measuring instruments with extended temperature compensation ranges, etc.

This section demonstrates the ease in which the Haz-Op procedure can identify potential hazards and/or financial risks, and once identified, how possible solutions are uncovered. Operating company management must then decide whether to modify the design, with a possible increase in capital cost, or accept the "Risk" based on an informed decision.

V Conclusions

The incidents described above have all occurred more than once in the last ten years. If these incidents are not sufficient to convince the fertilizer industry that something more must be done (incorporate a formal Haz-Op in the project approval process), numerous other incidents are available; furnace explosion during heat-up due to fuel feed without flame safety system (gas-oil pipe with burning rag ignitor); boiler tube melt-down due to operation with low water interlock bypassed; major H_2SO_4 mist release due to bypassed or the lack of an absorber pump shut-down interlock, etc. For those that are still not convinced, and say the incidents described and the resulting hazards and financial loss have not happened to them in ten or twenty years of plant operation; I say "YET". Its like holding a time bomb that's ticking and saying its safe because it hasn't exploded..."YET".

In any design whether new plant, system or modification, there are always a number of choices involving alternate process routes, materials of construction, operating pressures and temperatures, instrumentation and interlock philosophy, etc. The system chosen is a balance of the advantages - disadvantages of the design alternates versus capital and operating cost. I believe an added factor must be included in the design alternate selection process - safety, hazards, environmental exposure, operability, and financial exposure - risk.

The aim of this work was to present a convincing case for the fertilizer industry to adopt **Formal Hazard And Operability Analysis** for all (major and minor) projects - new plants, systems or modifications. In fact, a good starting point for a newly established Haz-Op team would be to analyze existing plant systems. I think many will be surprised at what is uncovered.

References

Chemical Industry Safety and Health Council of the Chemical Industries Association, Ltd., A Guide to Hazard and Operability Studies, 1971.

Falconbridge HRS Problem - Fact Sheet, Letter from J.R. Shafer, Monsanto Enviro-Chem, January 8, 1990.

Farmer, F.R, I. Chem E Symposium Series No. 34, Major Loss Prevention in the Process Industries, 1971.

Kletz, T.A., The Application of Hazard Analysis to Risks to the Public at Large, World Congress, Chemical Engineering, 1976, Amsterdam.

Knowlton, R.E., An Introduction to Hazard and Operability Studies, Chemetics International, Ltd., February 1981.

Lowley, H.G., Operability Studies and Hazard Analysis, Chemical Engineering Progress, April 1974.

U.B. Kim, Y.B. Chin, R.M. Smith, J. Sheputis, Sulfuric Acid Heat Recovery System (HRS) Operations at Namhae Chemical Corporation, Korea, British Sulphur Conference "Sulphur 88", November 1988.

Table 1

Key Word List

Item	Key Words		
Flow	Higher	Lower or None	Reverse
Temperature	Higher	Lower	
Pressure	Higher	Lower	
Concentration	Higher	Lower	
Contaminants (Impurities)	Higher	Lower	
Reactions	Hazardous or Undesirable		
Vessels and Columns			
Level	Higher	Lower	
Agitation (mixing)	More	Less or None	
Sampling			
Spills and Effluents			
Equipment			
Heat Exchangers	Too Large	Too Small	
Towers	High Eff.	Low Eff.	Off-Spec.
Pumps - Blowers	Too Large	Too Small	

Note: The "key Word List" and "Key Word Reminder List" is applied to each item under consideration for: start-up, shut-down, normal operation, emergency condition, etc.

Table 2

Key Word Reminder List

Utility Failure

1. Instrument (air, electrical, mechanical)
2. Electrical
3. Water (freeze-up, break, pump failure, etc.)
4. Steam (failure or full flow)
5. Process Air
6. Cooling Medium (refrigeration)
7. Heating Medium (hot oil, etc.)
8. Vacuum (air leakage, etc.)
9. Inert Gas (N2, CO2, etc.)

Equipment Failure

1. Agitation
2. Leaks, both in and out (exchangers, reactors, etc.)
3. Materials of construction (corrosion, reaction)
4. Relief devices, open vents (failure, plugged, etc.)
5. Valves (fail open, plugged, wrong signal, etc.)
6. Pumps (seal leaks, both in and out, pressure relief)
7. Grounding (static build-up, voltage above ground)

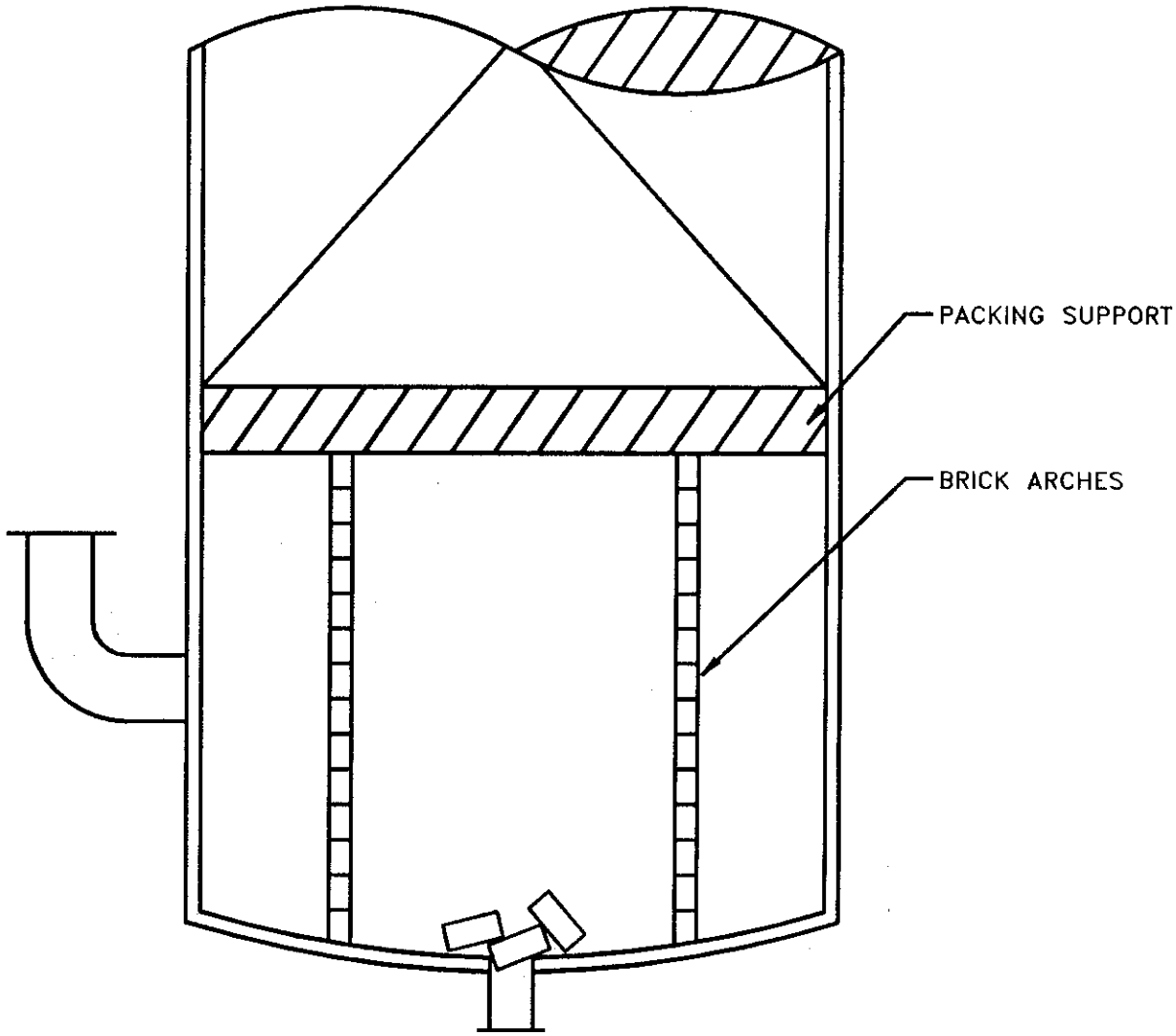
Special Situations

1. Areas potentially impacting on neighbors or public - disaster plan
2. Potential for fire within plant
3. Potential for toxic exposures in plant (gas, liquid)
4. Spills (exposure in sewers, in waste treatment)
5. Maintenance, layouts for access and removal
6. Winterizing, freeze-up, crystallization
7. Sampling (accessibility, plugging)
8. Vessel entry (24" manways, air supply, blinding)
9. Decontamination (purging, including pumps and sampling)
10. Government regulations - EPA/OSHA impact; air, water
11. Solid waste disposal - eliminate/define disposal
12. Noise, odors

Special Upsets

1. High Pressure - relief location, discharge points, reaction forces, emergency venting (fire, explosion, toxic)
2. High Temperature - runaway or explosion, burns, sun heat, external heat from fire, etc.
3. Reactants - wrong material, added at wrong stage
4. Thunderstorms - lightning, flooding
5. Tornado, hurricane, earthquake - wind loads, flooding
6. Airplane crash, large crane mishaps, runaway truck
7. Extreme continued low temperature, deep snows
8. Momentary power loss - what will and won't restart
9. Fire in cable trays (fire stops, route away from flammables)

FIGURE 1



ACID TOWER

FIGURE 2

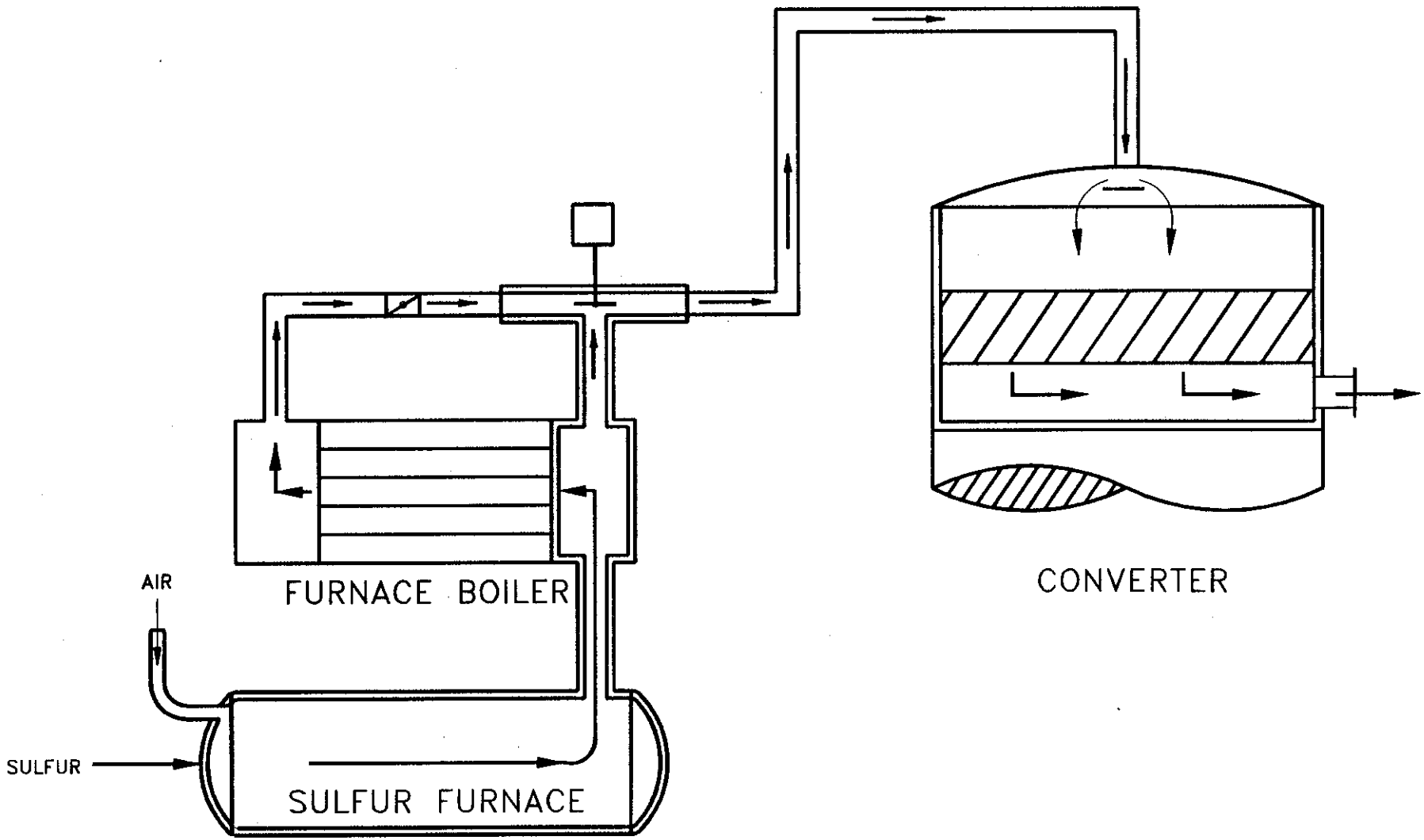


FIGURE 3

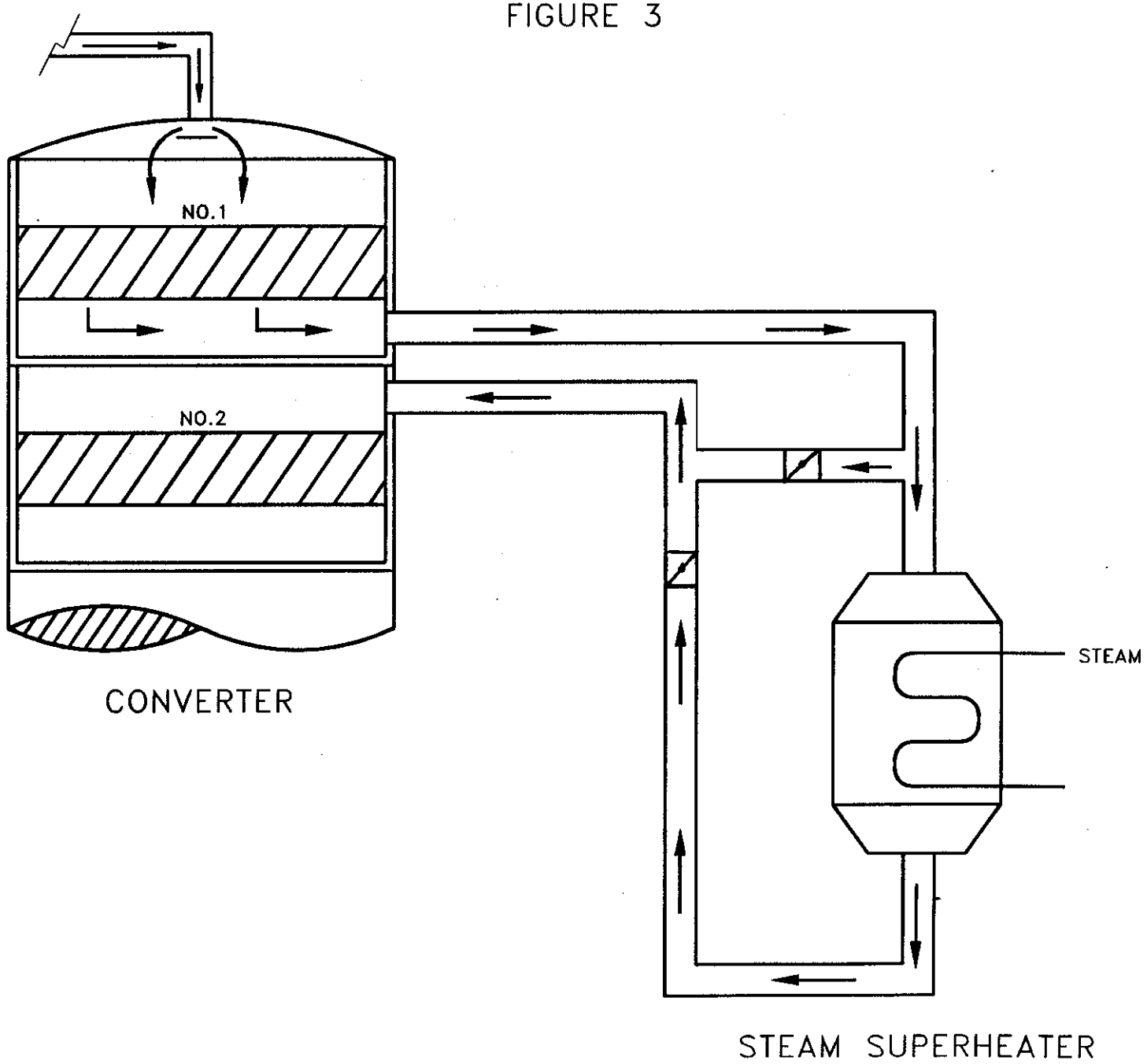
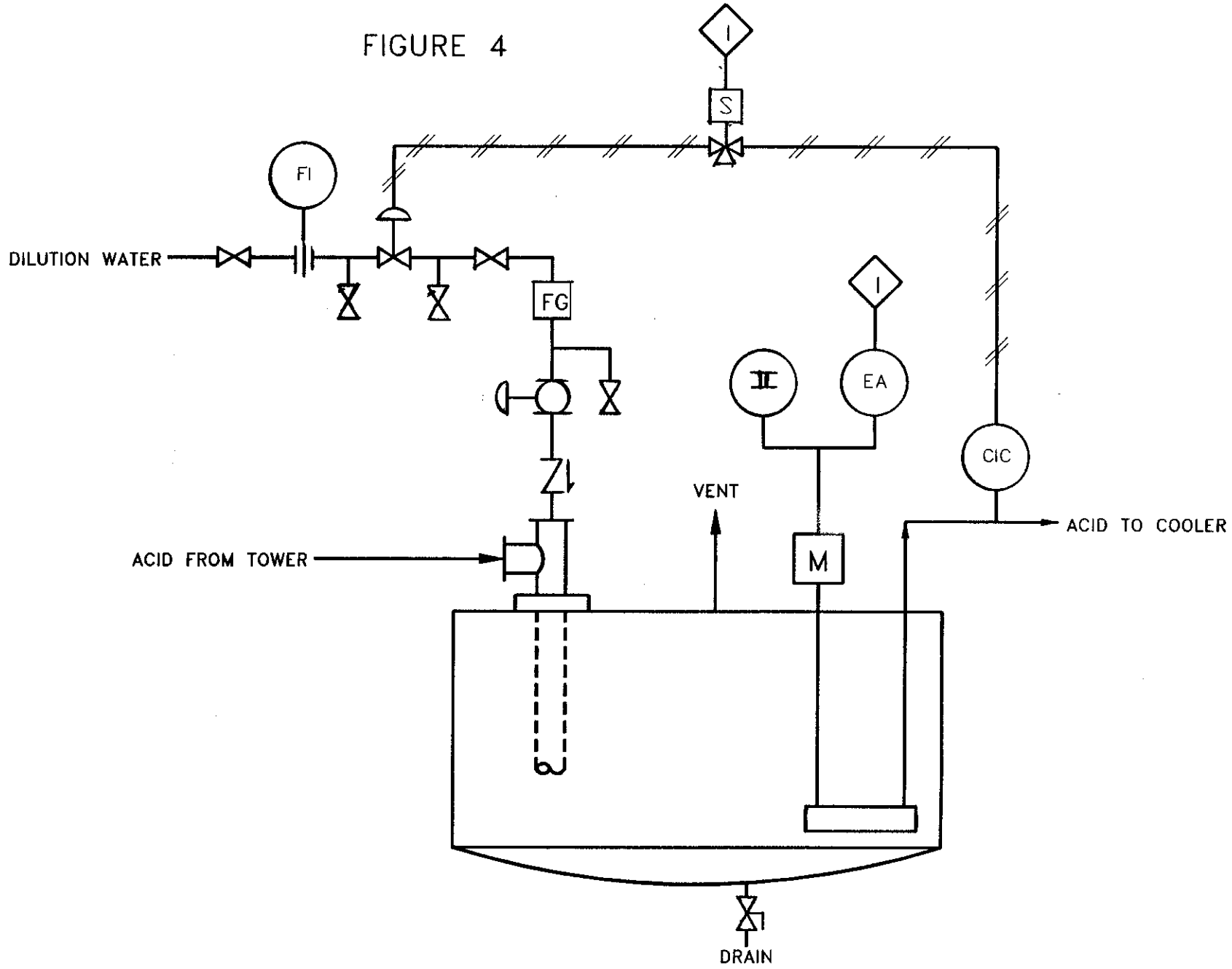


FIGURE 4



ACID PUMP TANK

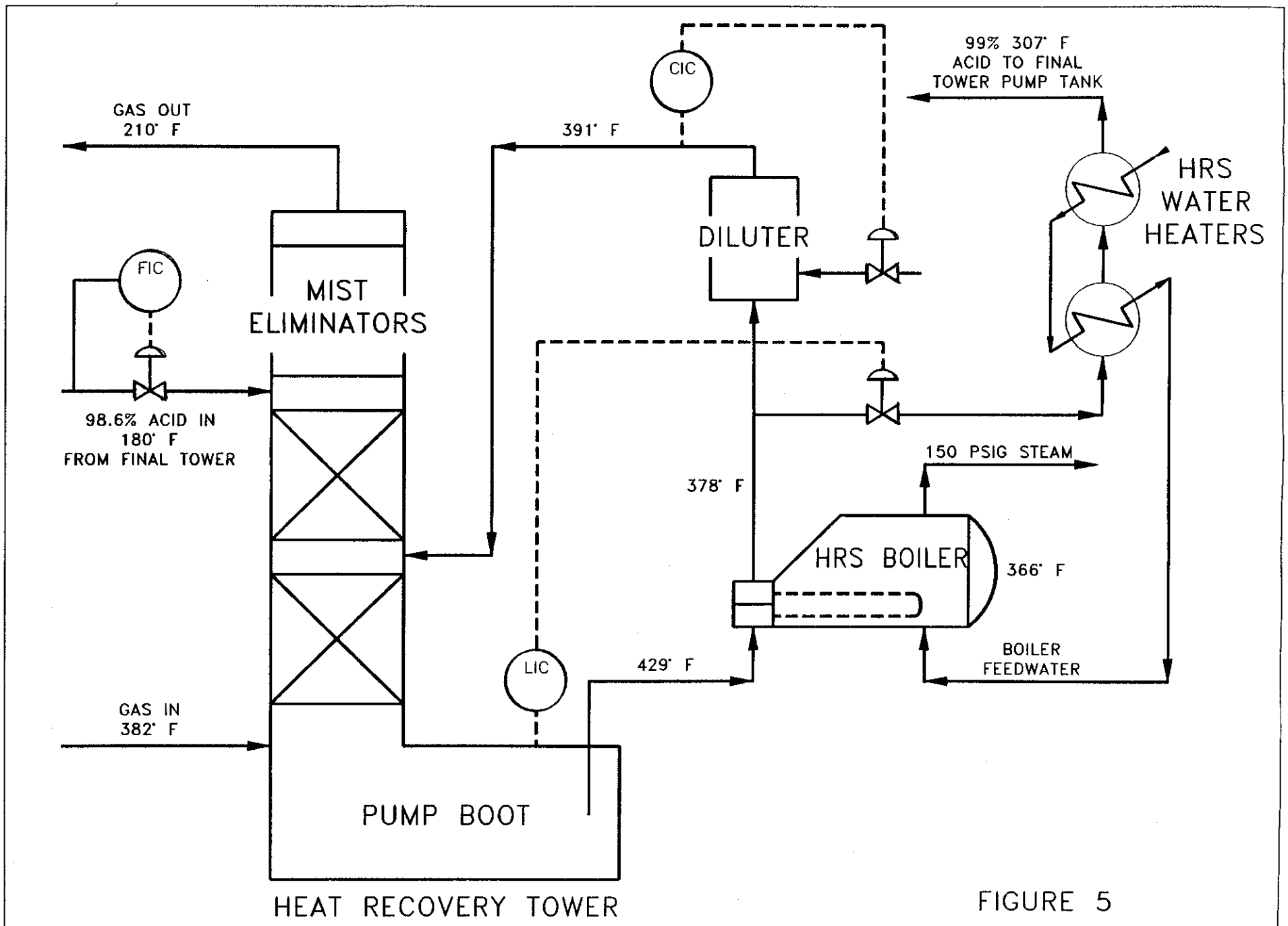


FIGURE 5

HEAT RECOVERY SYSTEM