APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

TABLE OF CONTENTS

SECTION **PAGE**

APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

REVISION RECORD				APPROVAL SIGNATURES	
REV.	DATE	STATUS	REMARKS	INITIATOR	APPROVAL
0	06/28/02	Approved		J. Lane	

APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

1.0 SCOPE

This document provides a list of the potential design deficiencies most often found during detailed hazard analysis (MFEA or fault tree) of the design of facilities and equipment. The existence of one of these configurations in a design does not necessarily constitute an unacceptable hazard. However, such configurations should be scrutinized closely and their worst case effects quantified.

This Checklist is intended to highlight those areas in a facility design most likely to contain equipment configurations which may not safely handle all credible process upsets which can be created by operator error, device malfunctions and errors in locating or sizing control, sensing, alarm, shutdown and pressure relief devices. Some broad aspects of hazard analysis, such as release consequence studies and probabilistic risk assessment, are not addressed by this Checklist. However, thorough application of the Checklist will usually result in identification of weaknesses that exist in a facility design, even though the designers have attempted to follow applicable codes This checklist may be tailored by the Contractor with Government approval.

DEFINITIONS

These definitions apply within the context of this guideline.

- **Abnormal Operating Condition**—A condition which occurs in a process component when an operating variable ranges outside of its normal operating limits.

- **Atmospheric Service**—Refers to operation at gauge pressures between 1/2 ounce per square inch vacuum and 5 pounds per square inch pressure.

- **Backflow—**Fluid flow in a process component opposite to the normal flow direction.

- **Blowdown Valve**—A valve, usually an automatically operated one, used to vent the pressure from a process station on shutdown.

- **Classified Area**—Any area electrically classified Class I, Group D, Division 1 or 2.

- **Containment**—Any method used to collect and direct escaped liquid hydrocarbons to a safe location.

- **Design Pressure**—User specified pressure which is a basis for component design.

- **Design Temperature**—User specified temperature which is a basis for component design.

- **Detectable Abnormal Condition**—An abnormal operating condition which can be automatically detected.

- **Direct Ignition Source**—An exposed surface, flame or spark at sufficient temperature and heat capacity to ignite a combustible mixture.

- **Emergency Shutdown System (ESD)**—A system of manual stations and/or E.S.S. which, when activated, initiates shutdown of the facility.

- **Emergency Support Systems (ESS)**—Systems that perform specific safety functions common to the entire facility, i.e., gas detection, fire loops, containment and ESD systems. Refer to Section 8.0 of this guideline.

- **Excess Temperature**—Temperature in a process component in excess of the rated working temperature.

- **Facility Safety System**—An arrangement of safety devices and Emergency Support Systems to effect facility shutdown. The system may consist of a number of individual process shutdowns and may be actuated by either manual controls or automatic devices sensing detectable abnormal conditions.

- **Facility Shutdown**—The shutting in of all process stations of a facility production process and all support equipment for the process.

- **Fail Closed Valve**—A valve which will shift to the closed position upon loss of the power medium.

- **Fail Open Valve**—A valve which will shift to the open position upon loss of the power medium.

- **Fail Unchanged**—A valve which will remain in its last position upon loss of the power medium.

- **Failure**—Improper performance of a device or equipment item that prevents completion of its design function.

- **Fire Exposure**—The relief valves must be sized to handle the gas evolving from liquid if the equipment is exposed to an external fire.

- **Fired Vessel**—A vessel in which the temperature of a fluid is increased by the addition of heat supplied by a flame within the vessel.

- **Fire Loop**—A control line containing sensing elements [fusible plugs, optical (UV or UV/IR) flame detectors, synthetic tubing, etc.] which, when activated, will initiate shutdown of the facility.

- **FSV**—Flow safety valve(check valve).

- **Gas Detection System**—A control system which monitors the concentration of combustible gases and initiates alarm and/or shutdown functions at predetermined concentrations.

- **High Liquid Level**—Liquid level in a process component above the highest normal operating level.

- **High Pressure**—Pressure in a process component in excess of the maximum operating pressure but less than the maximum allowable working pressure (for pipelines, maximum allowable operating pressure).

- **High Temperature**—Temperature in a process component in excess of the highest normal operating temperature.

- **Indirect Heated Component**—A vessel or heat exchanger used to increase the temperature of a fluid by the transfer of heat from another fluid, such as steam, hot water, hot oil or other heated medium.

- **Leak**—The accidental escape from a process component of liquid and/or gaseous substances to the environment or to another process stream from which it is normally isolated.

- **Liquid Overflow**—The discharge of liquids from a process component through a gas (vapor) outlet.

- **Lower Flammability Limit (L.F.L)**—The lowest concentration by volume of combustible gases in mixture with air that can be ignited at ambient conditions.

- **Low Flow**—Flow in a process component less than the minimum normal operating flow rate.

- **Low Liquid Level**—Liquid level in a process component below the lowest normal operating level.

· **Low Pressure**—Pressure in a process component less than the minimum normal operating pressure.

- **Low Temperature**—Temperature in a process component less than the minimum normal operating temperature.

- **LSH**—Level safety high.

- **LSL**—Level safety low.

- **Malfunction**—Any condition of a device or an equipment item that causes it to operate improperly, but does not prevent the performance of its design function.

- **Maximum Allowable Operating Pressure (MAOP)**—The highest operating pressure allowable at any point in a pipeline system during normal flow or static conditions.

- **Maximum Allowable Working Pressure (MAWP)**—The highest operating pressure allowable at any point in any component other than a pipeline during normal operation or static conditions. MAWP is based on the actual as built component configuration and is always greater than or equal to design pressure.

- **Overpressure**—Pressure in a process component in excess of the maximum allowable working pressure (for pipelines, maximum allowable operating pressure).

- **Pneumatic Power System**—A system which supplies pressure to operate pneumatic actuators.

- **Pressure Control Valve (PCV)**—The PCV is the control valve which regulates the normal operating pressure.

- **Process Component**—A single functional piece of equipment and associated piping, such as a heat exchanger, pump or tank.

- **Process Shutdown**—The isolation of a given process station from the process by closing appropriate SDVs to shut-in flow to the process station or divert flow to another process station. Sometimes referred to as Unit Shutdown (USD).

- **PSH**—Pressure safety high.

- **PSL**—Pressure safety low.

- **Qualified Person**—An individual with characteristics or abilities gained through training or experience or both as measured against established requirements, such as standards or tests that enable the individual to perform a required function.

· **Relief Valves**—Valves that activate automatically to relieve pressure, called "Safety valves", "relief valves", "safety relief valves", or "PSV's" (Pressure Safety Valves).

- **Rupture Discs**—The rupture disc in its simplest form is a metallic membrane that is held between flanges, and is designed and manufactured to burst at a predetermined pressure.

- **Safety Device**—An instrument or control used within the safety system.

- **Sensor**—A device which detects an operating variable and transmits a signal to perform a specific function.

- **Shutdown Valve (SDV)**—An automatically operated valve, usually fail closed, used for isolating a process station.

- **Thermal Expansion**—Blocked-in liquids can expand due to heat to create an overpressure situation.

- **TSH**—Temperature safety high.

- **TSL**—Temperature safety low.

- **Underpressure**—Pressure in a process component less than the design collapse pressure, i.e., that pressure below which mechanical failure can be expected to occur.

- **Undesirable Event**—An adverse occurrence or situation in a process component or process station which poses a threat to safety such as overpressure, underpressure, liquid overflow, etc.

- **Vacuum**—Pressure in a process component less than atmospheric pressure.

- **Vent**—A pipe or hatch on a vessel that opens to the atmosphere. A vent line might contain a pressure and/or vacuum relief device.

- **Vent Valve**—The vent valve is a control valve which regulates pressure in the operating system by diverting flow to the pressure relief system. The setpoint of the vent valve is always higher than the PCV setpoint.

2.0 RISK ASSESSMENT

Where modifications or additions to existing facilities are being evaluated, the risk assessment must include both the existing facility and the modification. Table 2.1 presents a methodology for developing a facility design classification. The user should evaluate each of the eight categories using his or her best judgment based on individual experience. The user should consider the offerings in each category and select the one which best describes the system. In the

event of a tie, select the offering with the highest risk factor. Make only one selection from each category. The Other Factors category is included to allow the user to apply judgment in cases where some facets of the design may not be covered by any other category. Enter the appropriate risk factor in the spaces provided. The total of all risk factors can then be used to assign an appropriate Facility Design Class (see *Section 3.0*).

3.0 FACILITY DESIGN CLASS

The facility design classification is based on the total from Table 2.1.

- **Class 'A' — Total is 11 or more:** Class A facilities are custom designed and require an extensive, highly reliable safety system incorporating levels of safety in addition to those found in a Class B facility.

  With respect to the hazards analysis of Class A facilities, the checklist method presented is usually supplemented with an analysis using a more rigorous method. Acceptable methods include MFEA (Multiple Fault and Error Analysis), HAZOP and fault tree.

- **Class 'B' — Total is 6 to 10, inclusive:** Class B facilities incorporate protective devices IAW Guideline 5.3.

  The hazards analysis of a Class B facility is done using the checklist method presented in some instances a HAZOP is also justified.

- **Class 'C' — Total of 5 or less:** Class C facilities should be evaluated using Guideline 5.3, but need not satisfy all of the requirements. The general intent is that secondary protective devices may not be required. All applicable codes and regulations must be satisfied.

  The hazards analysis of a Class C facility is done using the checklist method presented in Guideline 5.4.

The types of documents required to perform the hazards analysis for each of the facility design classes defined above are shown in the following table. OSHA 1910.119 specifies additional drawing requirements for facilities to which it applies.

Facility Class	Safe Chart	P&ID's	PFD's	Plot Plan
A	X	X	X	X
B	X	X	X	
C	X	X		

Note: A Safe Chart depicts the manner in which undesirable events could result in personnel injury, pollution or facility damage. It also shows where safety devices or procedures should be used to prevent the propagation of undesirable events.

APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

Accidents which occur external to the process in a facility are not self-propagating unless they affect the process or start a fire. If they affect the process, the safety system should shut down the process or affected part of the process. If they result in fire, the safety system should shut down all facility activity except that necessary for firefighting. Such accidents may be caused by actual phenomenon, failure of tools and machinery, or mistakes by personnel. These types of accidents may be prevented or minimized through safe design of tools and machinery, safe operating procedures for personnel and equipment, and personnel training. The Safe Flow Chart indicates the manner in which external accidents may affect the process.

APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

TABLE 2.1 - RISK ASSESSMENT

Select the worst-case offering (as it applies to the entire facility) from each category.

Energy Level (Normal Operating)		
Gas < 125 psig or liquid	0	
Gas > 125 psig or flashing liquid	1	
Gas > 700 psig	2	
Steam	1	____
Flammability		
Non-flammable	0	
Low Flammability Liquids (Crude Oil, Diesel, Calibrating fluid.)	1	
High Flammability Liquids (NGL/LPG, condensate, gasoline, etc.)	2	
Flammable Gas (Lighter than air)	1	
Flammable Gas (Heavier than air)	2	____
Toxicity/Asphyxiants		
Non-Toxic	0	
Low -Toxicicty	1	
High Toxicity (See Note #1)	2	
Heavier than air gas such as CO_2	2	____
Exposure		
Unmanned and low public exposure	0	
Manned 8-hour day and/or frequent public exposure	2	
Manned 24-hour day and/or constant public exposure	3	____
Environment (See Note #1)		
Fluid Release Non-Damaging (Fresh water, etc.)	0	
Fluid Release Minimal Impact (Release limited by system)	1	
Fluid Release Severe Impact (Release not system limited)	3	____
Economic Consequence		
Low potential loss of capital equipment, production impact and good will at this facility	0	
Medium potential loss of capital equipment, production impact and good will at this facility	1	
High potential loss of capital equipment, production impact and good will at this facility	3	____
Other Factors		
User may enter a value here, ranging from 1 to 3, to account for hazards unique to a particular process or for extreme public exposure		____
TOTAL		
11 or more: Class A, 6 to 10: Class B, 5 or less: Class C		If total is- ____

NOTES: 1. The user may consult Bioengineering and Enviornmental with regard to the relative toxicity and the relative environmental consequence.

APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

4.0 ABBREVIATED SAFETY DESIGN REVIEW CHECKLIST

The following list makes no mention of the many safety design areas in which errors are seldom ever made by design engineers. It is rather a list of the areas in which safety design errors are most likely to occur. Consequently, this list should **not** be taken as a complete Checklist to be used in designing a facility.

The Checklist was written to be a tool for use by persons specifically trained in this method of doing a hazards analysis; consequently, the brevity of this Checklist is intentional. The Checklist described in this section includes some information regarding the background and application of each item; however, thorough and effective use of this Checklist will normally require considerable practice in reviewing facility designs from a critical, safety oriented viewpoint.

Although the Checklist method allows considerable latitude to the individual analyst to decide how the analysis can best be accomplished, one or the other of two basic approaches is usually used. In one approach, the Checklist is taken an item at a time, and each project drawing is in turn scrutinized for instances of the selected item. In the other approach, the project drawings are taken one at a time, and the selected drawing is searched for occurrences of any item on the Checklist.

The choice of approach is subjective. Principal factors involved in the choice include the personal preferences of the analysts and the nature, structure, and size of the project being analyzed. For large projects with a multitude of drawings, the latter approach is more likely to be the choice. If the project is depicted in just a few drawings, the former approach is more often the choice.

Regardless of the approach used, the actual execution of the analysis is a matter of training and experience. There is no step-wise procedure, written or otherwise, that is followed as the analysis is done.

The Checklist has evolved over a period of years. It is a composite listing of design errors which have been found by hazards analyses done using more rigorous methods. While each item in the Checklist will not necessarily be applicable to a given design, the genesis of each item is that of actual experience. At one time or another, and in many cases more than once, the design error alluded to in the Checklist item has been encountered. The material in italics following each item or sub-item gives some information of the background and/or application of that item or sub-item.

1. Potentially inadequate overpressure protection due to:

a) Absence of high pressure shutdowns where needed.

This point primarily looks for failure scenarios which can cause a component to be subjected to unexpectedly high pressures, either because the failures have allowed the usual source pressure to be much higher than normal, or because the component is receiving flow from an unexpected source.

b) PSV's undersized to handle flow rates (both vapor and liquid) or flow restrictions which might be created by the design practices and operating errors referred to in the remainder of this Checklist.

The first part of this item addresses the need to have the relief device sized to handle the flow which results from the worst case failure scenario. For example, could a PSV sized for blocked discharge gas service safely pass two-phase flow if some scenario were to require it? The second part of the item is primarily applicable where a component is protected by a relief device not physically located on the component itself.

c) Questionable PSV and/or pressure sensor settings.

It hardly seems plausible that a professionally executed design could include PSV with set points specified that make it impossible for them to afford the desired protection, or for PSH's to have setpoints which don't allow them to initiate a shutdown in a timely fashion; nevertheless, errors such as these are found from time to time.

d) Fire relief sizing ignored.

This is another example of an error which should never make it to the final design but nevertheless one that is found from time to time.

e) Improper location of PSV's in cases where multiple lines and vessels have only one relief path.

When a relief device is protecting more than one component, the most desirable location is not always chosen. For example, the SAT for Component B might indicate that is protected by the PSV on Component A, and, on the surface, that might appear to be so. However, detailed review may uncover operating modes that provide other sources of input to Component 'B' with 'A' out of service or the path from 'B' to 'A' might be blocked by hydrates, and so on. The solution might be to locate the PSV on 'B' rather than 'A'. Note that this item can be evaluated only after complete piping layout drawings are available.

2. Absence of thermal PSV's on lines, heat exchangers, etc., on which they might be needed after an ESD or normal shutdown.

This is another item where problems are encountered more often than one might expect. Prime candidates for this item are cases where an appreciable delta-T might exist (or develop shortly after shutdown) between the trapped process liquid and its environment because the liquid was colder than normal at shutdown, or because the environment was (or became) warmer than normal at or after shutdown. Of course, the greater the coefficient of expansion of the liquid, the greater the potential pressure increase. Note that the failure of a check valve to hold a tight seat should not be counted as a means of limiting pressure increase from thermal expansion.

3. Thermal PSV as the only PSV on the shell of an exchanger with high pressure tubes.

Providing adequate overpressure protection on the shells of such heat exchangers, if they are liquid packed, can be very difficult (see Section A10.3.1). Thermal PSV's are totally inadequate in such cases.

4. PSV's sized and/or check valves located without taking worst case backflow effects into account, assuming a check valve fails to seat due to trash, broken clapper suspension pin, etc.

This item evaluates the isolation of relief paths from pressure sources which are not intended to feed the path. Designs which depend only on a check valve to provide this isolation should be carefully scrutinized, especially if failure of the check valve could significantly increase the total flow to the relief device.

5. Fail open mode of regulators not taken into account in sizing PSV's.

Often, the highest source pressure of any feed to a component is the gas supply. The overpressure protection must be capable of handling the flow from a gas inlet pressure regulator that has failed wide open.

6. Compressor suction PSV not sized to prevent overpressure of suction piping, if the by-pass or anti-surge valve should fail open, or the manual by-pass around such valves should be opened suddenly. Discharge piping volume will, of course, determine whether such overpressure is possible.

This item is straight-forward and is usually a concern only with centrifugal compressors. When calculating the discharge volume, discharge coolers and alternate flow paths must not be overlooked.

7. Lack of vacuum protection for atmospheric vessels which are not designed for full vacuum.

The Checklist concentrates on two things. One, it looks for failure scenarios which could render the safety devices ineffective. Two, it seeks scenarios which could cause a component not normally subject to liquid draw-down or vapor evacuation to be exposed to those actions.

8. Use of fiberglass or other piping not rated for full vacuum in liquid service at locations where vacuum could be created due to elevation change when a column of liquid is drawn down by a pump or by draining the pipe segment involved.

Not all piping is rated for negative pressure differentials; this is a point that is easily overlooked. When such piping is used in a design, areas that must be carefully checked include pump suction

piping and places where elevation decreases downstream of shutdown valves in pipe segments which drain after shutdown.

9. Pressure relief and/or shutdown systems which will not safely respond to general loss of instrument air supply and/or control circuit current.

Shutdown systems have been encountered in which the loss of the control medium did not always result in a complete or safe shutdown sequence. This may be because some of the devices are not fail safe, or it may be because of the way the control medium is distributed. Consider, for example, a pneumatic shutdown system in which a single blockage may deprive a number of shutdown devices of control pressure. As control pressure in the blocked off segment bleeds down, the devices will go to their shutdown position, but because the pressure decay may be very gradual, the individual devices will probably not operate at the same time. Furthermore, it is usually impossible to predict the sequence in which the affected devices will actuate. When evaluating such scenarios, the worst-case sequence should be assumed.

10. Instrument loops in which multiple functions are actuated by a single sensing device.

This item looks for instances where control and shutdown functions are both initiated by the same switch or transmitter, or pass through a common relay or other link in the control loop. In such cases, a single failure could cause loss of both control and shutdown action.

11. Multiple valves, controllers, etc., supplied by the same air supply regulator.

This item is similar to the previous item. It looks for control and associated shutdown instruments which are served by a common instrument air supply regulator.

12. Level sensors to controllers, all alarms, and SD functions are mounted on the same level bridle. Closure of any of the level bridle block valves is a common mode failure for both the level transmitter and level switches. Also apply the same logic to instrument arrangements which are monitoring other parameters (i.e., pressure, etc.).

This item is similar to the two preceding items. In this case, it looks for instances where control and shutdown switches or transmitters are located on a common bridle such that control and shutdown functions could both be rendered ineffective by mispositioned bridle valves. (Note that "common mode failure" is a technical term which means that one failure can affect two or more seemingly separate things. It does not imply that the failure may occur often; in fact, it makes no inference whatsoever with respect to frequency of failure.)

13. Multiple high and low pressure systems/lines tied into the same vent system, without taking worst case back pressure into account.

When a relief or vent system is provided, it must be capable of accommodating the worst-case relieving/venting/blowdown scenario (including rupture disks breaking) from the high pressure components without overpressuring any low pressure or atmospheric components tied to the same system.

14. Absence or improper location of check valves, especially:

a) where lines tie into common headers.

Sneak flow paths may exist if check valves have not been provided or properly located at header connections in shutdown scenarios or in failure scenarios which cause high pressures in some parts of the system.

b) around pump re-cycle valves.

Check valves are sometimes needed in minimum flow recycle loops to prevent reverse flow in shutdown or pump standby situations.

15. In flare/vent system design, provision was not made for:

a) Line and vessel supports insufficient to withstand acceleration/deceleration forces created by high velocity liquid slugs and liquid slug potential not minimized.

Liquid slugs at high velocity can impact a bend with significant levels of kinetic energy to break or crack the line or vessel support if allowances for them have not been made in the design. The verification that such allowances have been made is often as far as the Checklist can go when evaluating this item.

16. LPSD sensors and associated SDV's which have little chance of being effective because of their locations and/or set point (may also apply to low temperature, low level, low flow, etc., sensors).

Aside from low parameter shutdown devices which have not been provided in the design where they should have, an incorrectly specified setpoint or a poorly chosen location are the flaws most often found by this item.

This item is also construed to include high level shutdowns whose location (or setpoint) renders them ineffective. An example would be an LSH whose location (setpoint) is higher than the elevation of the outlet it is trying to protect.

17. Line and vessel packing times not taken into account in selecting locations and/or closing time of ESD valves and their ability to respond effectively to a potential overpressure.

The shutdown valve which is being counted on to isolate a component from a pressure source must be able to achieve tight shutoff before the pressure in the component exceeds its rating.

18. Situations in which operators may not have time to make the desired response where a shutdown or emergency action is intended to be manually initiated in response to an alarm.

Certain actions in response to emergency situations are intended to take place only when initiated manually (i.e., by the operator). This item attempts to make sure that the operator will have enough time to initiate the action.

19. Absence of multiple seals and inner seal failure sensors on high pressure liquid hydrocarbon pumps.

Seal leaks at high pressure pumps moving volatile hydrocarbon liquids can cause fires. This item attempts to make sure that suitable protection has been provided where needed.

20. Series regulators:

a) Pressure let down valves (regulators, Joule-Thompson valves, etc.) installed in series, without taking into account the fail open mode (leak, trash, high upstream pressure) of the

upstream valves, when selecting the valve top works, piping and PSV setting for downstream components.

When a component is being fed by two pressure let down valves in series, the component must be protected against the inlet pressure to the first let down device, not the second. If the upstream device fails open and applies the higher pressure to the downstream device, that pressure might force the downstream device open. The source pressure is thus passed along to the using component with just the one failure.

b) Working pressure of body inadequate on downstream regulator, when no PSV exists between regulators. This is most often overlooked when P&ID's show no spec break between regulators.

The pressure ratings of regulator bodies are often the weak points in a system and are often overlooked when pressures are stepped down by a series of regulators.

21. Configurations (considering line size, length, and WP) which may allow full opening blowdown or drain valves, rupture disks, etc., to overpressure their downstream piping, as a result of pressure gradients created when open.

Spec breaks are typically found on the downstream side of such devices. The spec break may be a significant distance from the next pressure protection device, creating the potential for overpressure of the line itself, especially in chain lines where a liquid slug may be followed by high pressure gas, if the drain valve is left open too long.

22. Absence of appropriate flashback prevention mechanism and/or flame management package on fired heaters.

Flashback protection must not be overlooked on fired components.

23. Drain system common line block valves located downstream of multiple, high pressure drain block valves.

A blocking device in a low pressure drain system connected to high pressure components can be a leading candidate to be the first failure in a severe overpressure scenario.

24. Low pressure block valves installed as the first valve downstream of higher WP operated valves (dump valves, etc.). The next (second) lower WP block valve downstream of a higher pressure operated valve should also be examined to check for cases in which a motive may exist (during shutdown, maintenance, etc.) for closure of this LP valve without first closing the upstream block valves and depressing the intervening line segment.

Spec breaks are frequently found just downstream of level control valves or pressure let down valves. Overpressure protection must be provided before the next downstream point of potential blockage.

25. Any configuration in which only one of the following failures (including valve leaks) or errors can result in overpressure, overflow, or gas release:

This item attempts to seek out places where single failures or errors can result in significant overpressure scenarios.

a) A manual block valve switched to or left in the wrong position.

Likely candidates are valves or blinds which must be closed for maintenance purposes from time to time.

b) Mispositioning of pairs of block valves which are normally operated at the same time.

When a set or group of valves must all be operated to accomplish an action (i.e., switching a component from Header B to Header C), the mispositioning of all the valves in the set or group is counted as one error.

c) Minor leakage of a check valve in either the operating or shutdown mode.

A check valve, by itself, should never be depended on to completely isolate a part of the system from another part that remains under pressure after a shutdown. Examples of the latter include injection headers.

26. Failure to minimize risk of minor leaks, spills, and venting in facilities handling highly toxic materials.

Even minor (very low quantity) leaks can be very dangerous if highly toxic materials are involved.

27. Lines, vessels, packing, gaskets, etc. which may be exposed to temperatures well below or above design specifications.

Failure scenarios can sometimes allow high or low temperatures to appear in components normally well isolated by distance from where the temperature extremes usually occur.

28. PSV's whose discharge is not piped to a safe area. (thermal PSV's are common culprits.)

This point can be very difficult to assess if the analysis is being done before the facility is built. In such cases, some effort should be made to determine what criteria will be used to determine what a safe place or area is.

29. Drains from pressurized process lines and vessels piped directly into atmospheric (open) hydrocarbon drains or sewer systems.

Such arrangements could allow hydrocarbon liquids or vapors to migrate into areas where ignition sources may be present because no hydrocarbons are expected in the area.

30. Recycle loops (control valves or PSV's) which bypass coolers, and pump recycle loops not piped back to suction surge vessel.

In recycle situations, the heat added by the work being done is not removed. This can lead to equipment failure and possibly a fire hazard.

31. Maximum liquid head pressure not accounted for when selecting maximum elevation of vapor vent and/or liquid overflow lines on atmospheric tanks.

32. Shutdown system pneumatic or electrical logic in which failure or improper setting of a single component can negate the shutdown system without actuating any warning device.

Although this point is aimed primarily at shutdown bypass switches or devices, it applies to any device associated with the shutdown system whose failure or incorrect setting could defeat all or a significant part of the shutdown system.

33. Likelihood of repeated spurious shutdowns due to inadequate spread between control, alarm, and/or shutdown setpoints for process parameters.

If an alarm has been provided for the purpose of giving the operator time to prevent a shutdown by taking an action, the spread between the alarm and shutdown setpoints should be such that the operator can be expected to have time to take the action.

34. The following items apply to the hydrocarbon atmospheric storage. Reservoir/tank not designed to prevent static charge accumulation and discharge during refill or during normal operation.

If the flow path of liquid into the reservoir is not properly designed, static electrical charges can build up and be an ignition source. This is a particular concern in environments conducive to the generation of static electrical charges, namely, cold, dry climates.

APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

5.0 SAFETY SYSTEMS REVIEW DOCUMENTATION EXAMPLES AND RISK MATRICES

By:	Drawing:
Date:	Drawing:

Abbreviated Safety Design Review Checklist Item		"X" if No Prob.	See Note #	See PPR #
1(a)	Potentially inadequate overpressure protection due to absence of PSH where needed.			
1(b)	Potentially inadequate overpressure protection due to PSV undersized for vapor and liquid flow or presence of flow restriction.			
1(c)	Potentially inadequate overpressure protection due to questionable PSV and/or PSH settings.			
1(d)	Potentially inadequate overpressure protection due to fire relief sizing ignored.			
1(e)	Potentially inadequate overpressure protection due to improper location of PSV's where multiple lines, vessels share relief path.			
2	Absence of thermal PSV's on lines or heat exchangers on which they might be needed after ESD or normal shutdown.			
3	Thermal PSV is the only PSV on the shell of an exchanger with high pressure tubes.			
4	PSV's sized and/or check valves located without taking worst case backflow into account.			
5	Fail-open mode of regulators not taken into account when sizing PSV's			
6	Compressor suction PSV not sized to protect suction side on settle-out or if recycle/anti-surge/bypass valve fails open.			
7	Lack of vacuum protection of atmospheric or other vessels not designed to withstand vacuum.			
8	Fiberglass piping not rated for vacuum used in liquid service at locations where vacuum is possible on draw-down of liquid column.			
9	Pressure relief or shutdown systems does not safely respond to general loss of instrument air or control electrical power.			
10	Instrument loops in which multiple functions (e.g., control and shutdown) are actuated by a single sensing device.			
11	Multiple valves, controllers, etc., supplied by the same air supply regulator.			
12	Sensors for control, alarm, and/or shutdown function on a bridle which can be isolated from vessel by one pair of bridle valves.			
13	Multiple high and low pressure vessels tied to same vent system without considering worst-case back pressure.			
14(a)	Absence or improper location of check valves where lines tie into common headers.			
14(b)	Absence or improper location of check valves around pump recycle valves.			
15(a)	In vent system design, no provision for line and vessel supports to withstand forces created by high velocity liquid slugs.			
16	Absence of low pressure shutdowns; or any shutdown whose location or setpoint make it ineffective.			
17	Line/vessel packing times not considered when selecting ESD valve locations and/or closure times.			
18	Situations where operator may not have time to react where design requires manual response to alarm or shutdown signal.			
19	Absence of multiple seals and seal failure sensors on high pressure liquid hydrocarbon pumps.			
20(a)	For series pressure regulators: Fail-open mode of upstream regulator not considered when designing downstream components.			
20(b)	For series pressure regulators: Working pressure of downstream regulator inadequate if no PSV between regulators.			
21	Configurations where fully open drain or blowdown valves or rupture disks overpessure downstream piping.			
22	Absence of flashback protection and/or flame management package on fired heaters.			
23	Drain system block valves located downstream of multiple high-pressure drain block valves.			
24	Low pressure block valves downstream of higher working pressure operated (control) valves.			
25(a)	Overpressure, overflow, or gas release caused by manual valve switched to or left in wrong position.			
25(b)	Overpressure, overflow, or gas release caused by mis-positioning of pairs of valves normally operated at the same time.			
25(c)	Minor leakage of a check valve in either the operating or the shutdown mode.			
26	Failure to minimize risk of leaks, spills, venting in facilities with highly toxic materials.			
27	Lines or vessels which may be exposed to temperatures well below or above design specs.			
28	PSV's whose discharges are not piped to a safe area. (Thermal PSV's are common culprits.)			
29	Drains from pressurized process lines/vessels piped directly to atmospheric or open drains or sewer systems.			
30	Recycle loops or PSV discharge paths which bypass coolers; pump recycle piped to suction rather than to surge vessel.			
31	Maximum liquid head not considered when designing vents or overflow lines for atmospheric tanks.			
32	Shutdown system logic in which a failure or improper setting can negate all or part of the system without an alarm.			
33	Likelihood of repeated shutdowns due to small spread between control, alarm, and shutdown setpoints.			
34	Storage not designed to prevent static charge accumulation and discharge during refill or normal operation.			

APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

Start Date, This Element: 9/15/97

HAZOP ELEMENT WORKSHEET

Element Number	Description	Drawing Number(s)/Revision(s)
1	Glycol Vent Knock-Out Drum, Pumps, and Vent Cooler	REB-SY-DW-1236-3, Issue 1A, Rev. 0

ELEM	ITEM	P'RAM	GW'RD	DEVIATION	CONSEQUENCE	CAUSE	EXISTING PROTECTION	RECOMMENDATION	COMMENT/ACTION BY	RANK
General Comments for this Element: The review of this element is a combined tech review and HAZOP. The feed is mostly water vapor with a small amount of benzene and other aromatics. Total liquid is 413-445 lb/hr, with 22 lb/hr aromatics. V2509 is 3 1/2′ by 10′ and is sized to have a residence time of 4-8 hours. Vent connects to warm gas flare, which has a maximum back pressure of about 5 psig. The dead-head pressure capability of the pumps is not enough to overpressure the outlet nozzle or the discharge piping.										
1	1.1	Flow	None	Slugs accumulate in inlet line to the coolers.	High back pressure is reflected to the glycol condenser.	The line into the coolers in not designated to have no pockets.	None.	Designate line 6″-VL-1246-A1 to have no pockets.		TRC
1	1.2	Flow	None	Non-condensable gases are trapped in the cooler.	Cooler efficiency is seriously reduced.	Cooler is vapor-locked.	None.	Provide a means, such as a balance line, that will allow non-condensable to flow to the drum without blocking flow of liquids through the cooler.		TRC
1	2	Flow	More	NSDF						
1	3	Flow	Less	NSDF						

APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

Start Date, This Element: 9/15/97

HAZOP ELEMENT WORKSHEET

Element Number	Description	Drawing Number(s)/Revision(s)
1	Glycol Vent Knock-Out Drum, Pumps, and Vent Cooler	REB-SY-DW-1236-3, Issue 1A, Rev. 0

ELEM	ITEM	P'RAM	GW'RD	DEVIATION	CONSEQUENCE	CAUSE	EXISTING PROTECTION	RECOMMENDATION	COMMENT/ACTION BY	RANK
1	4	Flow	Back	Back flow takes place to V2509 via a recirculation line.	V2509 fills, and, as worst case, could carry over to the flare.	A block valve in a recirculation line fails open.	None.	Relocate the recirculation lines so they are between the pump and the discharge check valve.		TRC
1	5	Flow	Also	NSDF						
1	6	Flow	Lieu	NSDF						
1	7	Flow	Slug	NSDF						

APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

Start Date, This Element: 9/15/97

HAZOP ELEMENT WORKSHEET

Element Number	Description	Drawing Number(s)/Revision(s)
1	Glycol Vent Knock-Out Drum, Pumps, and Vent Cooler	REB-SY-DW-1236-3, Issue 1A, Rev. 0

ELEM	ITEM	P'RAM	GW'RD	DEVIATION	CONSEQUENCE	CAUSE	EXISTING PROTECTION	RECOMMENDATION	COMMENT/ACTION BY	RANK
1	8	Press	More	High pressure reflected from the existing flare header.	In the worst case, V2509, E2509A/B, and the glycol still could be subjected to pressure above their design.	The flare header is filled with liquid from another source or scenario. The header could be pressurized by gas from the glycol flash separator (80 psig) or to a higher pressure by a relieving scenario at V1532 or some other vessel tied into the header.	None.	Change the vent connection to the new flare header when that header is installed. In the interim, consider connecting to the flare header at a location downstream of the flare header liquid drums or vent V2509 to the atmosphere. Also see 1-11.		2
1	9	Press	Less	NSDF						
1	10	Press	None	NSDF						

APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

Start Date, This Element: 9/15/97

HAZOP ELEMENT WORKSHEET

Element Number	Description	Drawing Number(s)/Revision(s)
1	Glycol Vent Knock-Out Drum, Pumps, and Vent Cooler	REB-SY-DW-1236-3, Issue 1A, Rev. 0

ELEM	ITEM	P'RAM	GW'RD	DEVIATION	CONSEQUENCE	CAUSE	EXISTING PROTECTION	RECOMMENDATION	COMMENT/ACTION BY	RANK
1	11	Temp	More	Wet vapor sent to the warm gas flare (existing flare).	Liquids will condense in the flare system, resulting in slugs for which the system is not designed to handle without excessive back pressure resulting from a venting or blowdown situation.	The glycol vent coolers failed, or a relief valve at the condenser has operated prematurely, sending flow to the drum which bypasses the coolers.	Temperature signal and fan motor run signals are present in the DCS and there is a TAH in the control room panel.	Change the drum vapor outlet to the new flare header when it is installed. In the interim, have the fan motors alarm in the control room when the fan is not running and have administrative procedures require frequent monitoring of the liquid levels in the existing flare header liquid boots. Also see 1-8.	This is seen as a hazard (Rank 2) as well as a tech review comment.	TRC
1	12	Temp	Less	NSDF						

APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

Start Date, This Element: 9/15/97

HAZOP ELEMENT WORKSHEET

Element Number	Description	Drawing Number(s)/Revision(s)
1	Glycol Vent Knock-Out Drum, Pumps, and Vent Cooler	REB-SY-DW-1236-3, Issue 1A, Rev. 0

ELEM	ITEM	P'RAM	GW'RD	DEVIATION	CONSEQUENCE	CAUSE	EXISTING PROTECTION	RECOMMENDATION	COMMENT/ACTION BY	RANK
1	13	Level	More	Carryover occurs from the drum.	Liquids carryover to the existing flare.	The level controller, high level alarms, and the high level shutdowns are all driven by the same controller, thus one failure can defeat control and protection functions.	None.	Provide a separate bridle (and hence separate controllers) so that the high (and low) level alarm and shutdown functions are completely separate from the control functions. The re-design should be consistent with the design at the flare/vent KO drums in the Team B scope.		TRC
1	14	Level	Less	NSDF						
1	15	Comp	More	Drum not adequately ventilated prior to entry for maintenance.	Personnel hazard may exist when necessary to enter the drum for maintenance.	The vent valve, presently shown as 1″, may not by large enough to properly vent the drum.	Maintenance personnel would have to wear breathing apparatus.	Evaluate the size requirements for the manual vent valve on V2509 and re-size if necessary.		TRC

APPENDIX I
DESIGN GUIDELINE 450

OC-ALC	DESIGN GUIDELINE 450
Section **DESIGN REVIEW**	Subject **SAFETY SYSTEMS REVIEW**

Start Date, This Element: 9/15/97

HAZOP ELEMENT WORKSHEET

Element Number	Description	Drawing Number(s)/Revision(s)
1	Glycol Vent Knock-Out Drum, Pumps, and Vent Cooler	REB-SY-DW-1236-3, Issue 1A, Rev. 0

ELEM	ITEM	P'RAM	GW'RD	DEVIATION	CONSEQUENCE	CAUSE	EXISTING PROTECTION	RECOMMENDATION	COMMENT/ACTION BY	RANK
1	16	Comp	Less	Maintenance work on V2509 is unnecessarily difficult.	Maintenance work is excessively complicated.	Blindable points have not been provided at the drum.	None.	Provide blindable points as appropriate at all connections to the drum.		TRC
1	17	Power	More	NSDF						
1	18	Power	Less	NSDF						
1	19	Other	Fire	NSDF						

PROJECT NAME

POTENTIAL PROBLEM REPORT

Date:

PPR No. _____
Area _____
Equipment Affected _____
Drawing and Zone _____ Rev. No. _____
Problem or Hazard _____
SDRCL Item Reference _____ Number of Simultaneous Failures Required _____
First Failure _____
Severity _____ Frequency ____ Risk Rank _____ Per Risk Rank Matrix dated 3/31/93

Description of Potential Problem:

Recommended Corrective Action:

Response:

The following tables provide a guideline for assessing the qualitative risk of items identified during the systems safety engineering review and for providing a matrix to determine the appropriate corrective action.

Hazard Severity

Category	Descriptive Word	Expected Event Consequence
I	Catastrophic	Multiple Fatalities Multiple hospitalization of ten or more workers and/or members of public Extensive facility property/equipment damage, major business interruption; or Catastrophic environmental impact.
II	Critical	Fatality Multiple hospitalization of less than ten workers and/or injury to members of the public Major equipment damage, moderate business interruption Severe environmental impact; or Large public disruption.
III	Significant	Release of large or moderate quantities of flammable or toxic material (minimal impact) Less severe medical treatment injury of a worker(s) Moderate equipment damage, minor business interruption Moderate environmental impact; or Small public disruption.
IV	Minor	Release of minor quantities of flammable or toxic material First aid injury of worker Minor equipment damage, negligible business interruption; or Minor environmental impact.

Individual Event Frequency Level

Level	Descriptive Word	Definition
A	Frequent	Repeated events could be expected in life of facility.
B	Probable	Several events could be expected in the life of facility.
C	Possible	Single event could reasonably be expected to occur in life of facility.
D	Improbable	Occurrence of a single event not expected during the lifetime of a particular facility, but could be expected over the lifetimes of several similar facilities.
E	Highly Improbable	Event occurrence during lifetimes of several similar facilities would not be expected.

Risk Assessment Matrix

Hazard Severity Category	Frequency Level (Probability)				
	A	B	C	D	E
I	1	1	2	3	4
II	1	2	3	4	5
III	2	3	4	5	5
IV	3	4	5	5	5

Risk Assessment Ranking		
Risk Rank	**Descriptive Word**	**Definition**
1	Very High	Immediate corrective action required Engineered remedial action required
2	High	High priority corrective action required Engineered remedial action preferred
3	Moderate	Reduced priority corrective action required Engineered or procedural remedial action
4	Low	Significant corrective action to further reduce risk not required Minor adjustments or changes should be implemented, where possible
5	Very Low	Corrective action to further reduce risk not necessary

Matrix Notes

Hazard Severity:

OSHA reportable events (report within 8 hrs) fall under the Critical or Catastrophic Severity Categories. The minimum OSHA reportable event (fatality; or 3 or more workers hospitalized) falls under the Critical Hazard Severity.
Public disruption includes evacuation, blockage of highways, etc. Negative publicity for the company may also be implicitly included, as appropriate, in public disruption and/or business impact.
Financial criteria for equipment damage and/or business interruption may be established for a particular project to better define the degree of loss corresponding to each Hazard Severity Category.

Individual Event Frequency Level:

Descriptive Word in Individual Event frequency Level are intended to approximately correspond to the numerical frequencies below.

Level	Descriptive Word	Numerical Frequency	Definition
A	Frequent	10^{0} to 10^{-1}/yr	Repeated events could be expected in life of facility.
B	Probable	10^{-1} to 10^{-2}/yr	Several events could be expected in the life of facility.
C	Possible	10^{-2} to 10^{-4}/yr	Single event could reasonably be expected to occur in life of facility.
D	Improbable	10^{-4} to 10^{-6}/yr	Occurrence of a single event not expected during the lifetime of a particular facility, but could be expected over the lifetimes of several similar facilities.
E	Highly Improbable	$<10^{-6}$	Event occurrence during lifetimes of several similar facilities would not be expected.

Risk Assessment Ranking:

A Risk Rank of 4 is the As low as reasonably practical level (i.e. cost effective corrective actions should be implemented).

SAFETY ANALYSIS
FUNCTION EVALUATION (SAFE) CHART

FUNCTION PERFORMED

SHUTDOWN OR CONTROL DEVICE IDENTIFICATION

PROCESS COMPONENT		DEVICE	ALTERNATE PROTECTION	
IDENTIFICATION	SERVICE	TAG NUMBER	TAG NUMBER	COMPONENT IDENTIFICATION