ADDING FAILURE EFFECTS TO HAZOP

Colin Feltoe B.Sc(Hons), MIPENZ, C.Eng(UK), P.Eng(Can)
MIChemE (UK), APEGGA (Can), IPENZ (NZ), SCENZ
Safety Solutions Ltd
PO Box 3172
New Plymouth 4341
New Zealand
safety.solutions@xtra.co.nz

ABSTRACT:

What more can be said about HAZOP, a mature subject well developed since the 1960's? Those practitioners who have worked their way through one hundred or more P&ID's, taking several weeks, will understand how difficult it is to keep the team focused and avoid "analysis paralysis".

Starting each line with a failure analysis has several benefits. Most causes generated by the traditional guidewords are captured at this stage, and the team must do some solid analysis from the start improving their understanding of the line dynamics before the classical guidewords are applied. The quality of the finished product, namely the HAZOP report, in the author's opinion, is greatly improved. One disadvantage is that lateral thinking can be inhibited. It is suggested however, that not much lateral thinking goes on in practice, after a few days HAZOP'ing.

The addition of failure effects to the HAZOP process will be demonstrated by example. This will include deviations to be addressed in typical control systems (switches, transmitters, protection devices) and process equipment items. For example, how can a measurement offset (high or low) affect a control system or protection device? Can this lead to a failure on demand and what will be the consequence? The thought process can be interesting, particularly with complex control loops. Those familiar with instrumented protection (IPF) reviews will recognise these questions and the relationship to safety integrity level (SIL) determination which can be incorporated into the review if required.

Introduction:

It is proposed that a list of failures be generated (as causes) and analysed for each line before the application of traditional HAZOP guidewords. This technique has been applied by the author for several years with positive feedback from clients who have suggested the method be shared. There are several benefits including:

i. An initial list of pertinent causes is immediately and easily generated for the HAZOP team to tackle. This reduces the mental effort required for a long study.
ii. An improved understanding by the team of the line dynamics.
iii. Most of the issues raised by the traditional guidewords will have already been raised so **only** additional issues need addressing and documenting.
iv. The likelihood of an omission is reduced, providing confidence that the HAZOP has been rigorously carried out. This is a subjective view supported by client feedback and the author's experience.
v. The overall time required is not increased but may be reduced.

The views presented are those of the author having applied this method to approximately 100 HAZOP studies of varying size and are offered in the hope they will make HAZOPs more effective.

Background:

HAZOP emerged as a diagnostic tool in the late 60's and has remained the preferred method for systematically identifying process plants hazards. It was initially used in the petrochemical/oil and gas industries but now can be found in many others including dairy, pulp and paper, power generation, mineral processing and mining. Some changes to the method have emerged over the years. One example is to batch (or sequential) processes.

Traditionally HAZOP involves the selection of a line on a P&ID. This line is interrogated by the application of guidewords such as more or less flow, pressure, temperature, level etc to generate causes of deviations from the design intent. The consequence associated with each cause is defined assuming any safeguards have failed. These (safeguards) are then identified to determine if the design is sufficiently robust. If not, an action results. Where a large number of action items are expected, a qualitative judgement of risk (assuming existing controls are in place) can be made, possibly using a matrix or even the gut judgement of the team. This enables the actions to be prioritised. Fig 1 shows a typical HAZOP worksheet.

Fig 1 HAZOP WORKSHEET

Diagram:			Line No:1	Design Intent:				
Study No.	Process Dev^{n}	Cause	Consequence	Safeguards	Risk	Act^{n} #	Action	By
Line Comments:								

Authors Definition of HAZOP:

"A systematic study, carried out by a team of persons experienced in aspects of the topic, using the line by line (or step by step) application of guidewords to identify all deviations from the design intent with undesirable effects for safety, operability or the environment." Some "truths" emerge which are not always appreciated.

Truth 1: HAZOP is not a design review.

A design review focuses on whether the design will functionally achieve its goal. It is **success** focused. A HAZOP tries to break the design by exploring failures, such as equipment, control systems and human errors. It is **failure** focussed. HAZOP requires a different mind set to a design review and, in the author's opinion, cannot run concurrently. If the design review has been inadequate then a good HAZOP will find it out. If design issues cannot be tabled the HAZOP will degenerate into a design review.

Truth 2: It is assumed that the protection systems have failed when identifying the "consequences".

To identify the hazard we must assume that the protection system has failed. We then identify the safeguard (for example a high level switch or an operator response) and then decide whether it is adequate to mitigate the hazard.

Truth 3: HAZOP will not extract knowledge which is not there:

HAZOP is a systematic way of extracting knowledge, but it can't extract what's not there. Some very interesting questions may still arise, but have the right questions been asked? Having the right knowledge in the team is essential. It helps to have a leader with a good engineering background, but independent of the project. His or her skill is in the application of the HAZOP technique. Process knowledge lies within the team.

Truth 4: HAZOP does not challenge the accuracy of the design.

The starting assumption is that all calculations and design decisions have been made correctly so a design error, such as wrongly sizing a valve or a pump, is not raised as a failure. These issues are covered by the design checks and balances.

Truth 5: The plant will be operated in accordance with the design philosophy.

While this is a HAZOP assumption, human error and human nature should not be ignored. In the fullness of time, knowledge of the design philosophy will be diluted and possibly forgotten. The design should be sufficiently robust to take account of this.

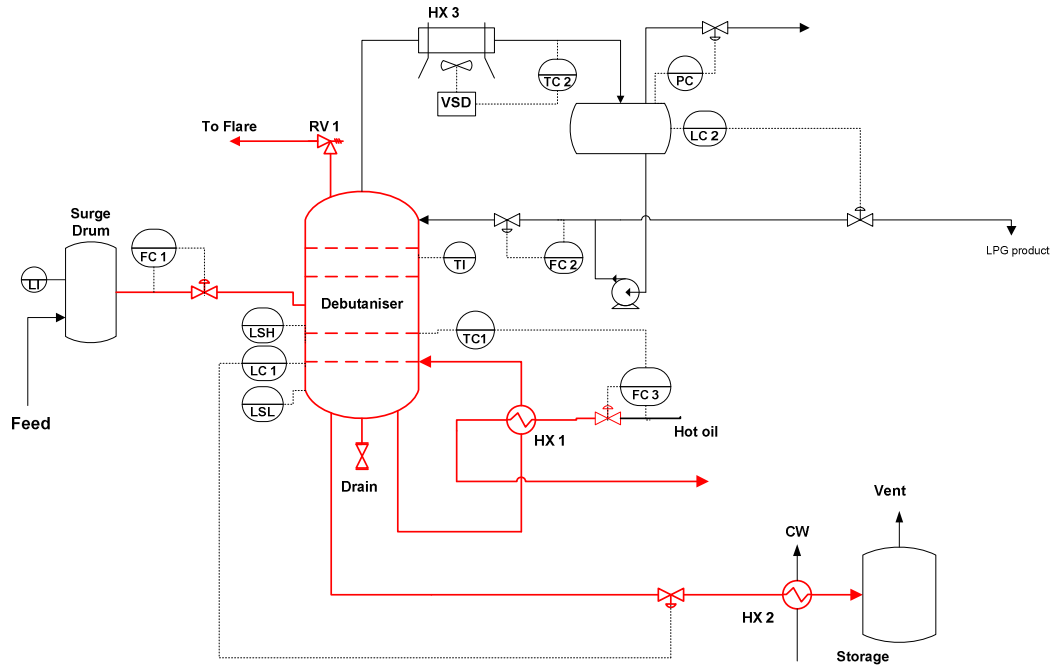
Application of Failure Effects

Individual effects have been discussed above. The following is an example of the failure causes generated before the application of the traditional guidewords of “High Flow” etc. This list can be generated quickly then all causes analysed before moving to the traditional HAZOP guidewords. While the causes may be repetitive, particularly for control systems, the analyses rarely are.

Process Description (Fig 3)

Feed, consisting of un-stabilised condensate, is fed into a column on flow control. The column re-boiler is heated with hot oil. Butane and light ends are driven off the top of the column, the light ends being vented to a low pressure fuel system and the condensed butane going to LPG storage. The column bottoms product (condensate) is mainly C5+ with some C4 (butane). The butane content must be controlled to prevent the RVP (Reid Vapour Pressure) exceeding 69kPa which is a transport specification. This is controlled by the temperature controller on tray 3 (TC1). The column tops temperature is manually controlled by adjusting the reflux flow (FC-2). Light ends are vented from the reflux drum via a pressure controller and the product is cooled to ambient temperature (not shown) and sent to storage.

Fig3



HAZOP Worksheet

Diagram: DB 723-P- 11 rev D			Line No:23 (red)	Design Intent: Debutaniser feed to column bottoms, re-boil and product to storage.				
Study No.	Process Deviation	Cause	Consequence	Safeguards	Risk	Act^{n} #	Action	By
Line Comments: 1. TC 1 to control RVP below 69 kPa 2. Zero water assumed in feed other than under process upset.								
23.1	Control/Eq Failure *(Lo Flow)**	FC-1 Fails Hi	Reduced throughput – not significant	Operator observation of low tops temp	L			
23.2	" *(Hi Flow)*	FC-1 Fails Lo	Hi feed to tower, potential flooding, Off spec products. Significant reprocessing cost.	Product lab analysis (too late) Operator observation of temperatures.	H	1	Configure TAH on TI and TAL on TC1.	AB
23.3	" *(Hi Level)*	LC-1 Fails Lo	Hi level, in tower, tray damage.	LSH	L			
23.4	" *(Lo Level)*	LC-1 Fails Hi	Lo Level , re-boiler tubes exposed, tube failure, C4 in hot oil. Vapour by pass to storage, storage overpressure.	LSL. Vent sized for LCV fail open.	H	2 3	Confirm if tubes designed to run dry, if not revisit metallurgy Consider relocation of FCV-3 downstream of re-boiler.	CD BC
23.5	" *(Hi level)*	LSH Fails on demand	As Study23. 3	NA		4	Feed into IPF** review	BC
23.6	" (*Lo Level*)	LSL Fails on demand	As study 23.4	NA		5	Feed into IPF* review	BC
23.7	" *(Hii Flow)*	RV-1 Spring Failure	Rapid tower depressuring. Significant process upset. Equipment damage unlikely.	Low likelihood CCTV on flare with operator observation. Numerous alarms	L			
23.8	" *(Hi Flow)*	RV-1 Passes	Loss of product to flare	CCTV on flare	L			
23.9	" *(Lo Temp)*	TC-1 Fails Hi	Lo bottoms temperature, condensate RVP high Loss of C4 product. C4 venting from storage.	Product lab analysis. Operator observation of storage vent (unlikely).	M	6	Provide independent TI on tray 3	BC
23.10	" *(Hi Temp)*	TC-1 Fails Lo						
23.11	" *(Lo Flow)*	FC-3 Fails Hi						
23.12	" *(Hi Flow)*	FC-3 Fails Lo						
23.13	" *(Impuities)*	HX-1 Leaks						
23.14	" *(Impurities)*	HX-2 Leaks						

* *(xxx)* – Equivalent traditional guideword

* * IPF – Instrumented Protection Function review leading to SIL determination

Once all the above causes have been addressed then the traditional guidewords can be applied.

23.15	Hi Flow	Operator set point error						
23.16	Misdirected Flow	Drain open or passing						
23.17	Lo Flow	Loss of Feed						

.

Developing Failure Effects.

There are several questions which can be asked (and answered) for control system and equipment failures. The following represents some of them. The consequences, safeguards and actions below are arbitrary.

Control Systems:

The following example refers to a level control system however the same questions can be asked about flow, pressure and temperature control systems.
Figure 2a shows a knock out vessel separating liquid from gas. It is equipped with a level control linked to a variable speed pump which removes the liquid. In addition there are independent high and low level switches, that alarm and trip the pump, and an overhead compressor (not shown).

Fig 2a – Level Control + Level Switches

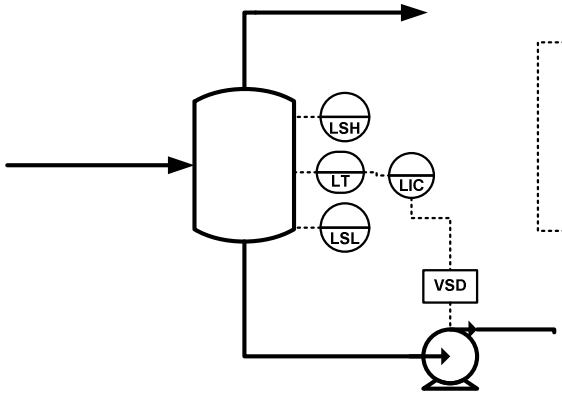
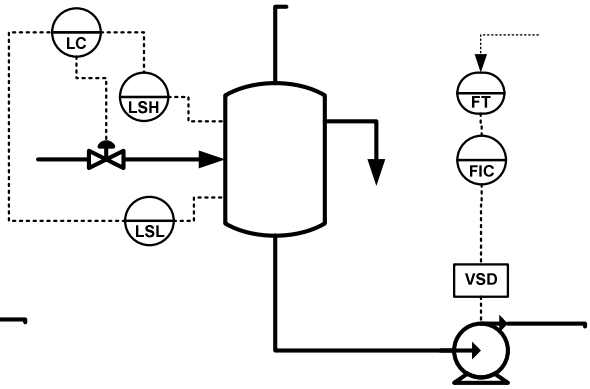


Fig 2b – Two Level Switches giving gap control



Cause 1	Level Transmitter Fails High: This means there is an offset such that the instrument is reading higher than the actual level. The controller will still be controlling to the set point so the operator will be unaware of the fault.
Consequence	Low level in the vessel, pump cavitation, possible seal failure and fire. Eventual backflow if pump trips.
Safeguards	Low level switch alarms and trips pump, operator observation of cavitation (not considered likely).
Risk	Medium
Action	Quantify risk and consider backflow protection.

Cause 2	Level Transmitter Fails Low: The offset is now lower than the actual level
Consequence	High Level with liquid carryover. Compressor damage – significant cost.
Safeguards	High level switch alarms and trips compressor.
Risk	High (Considered likely within life of plant)
Action	Feed into IPF (Instrument Protection) review and provide protection with appropriate SIL (Safety Integrity Level).

The next "cause" to be considered is the "failure on demand" of each level switch. The consequence will be the same as for the transmitter failures. The required SIL level can now be determined (or tabled for a separate meeting) and the system designed to provide the required probability of failure on demand (fractional dead time/unavailability, whichever terminology you care to use).
It is now common to have two level transmitters (one for control and the other for independent safeguarding actions) rather than a level transmitter and two switches. The total cost is similar once cabling etc has been included and a comparison between transmitters is provided reducing the need for periodic calibration. Full function testing is still required to verify the status of other elements in the system. While the use of a second transmitter is an improvement, additional failures are introduced as follows.
"Fail Low" of the trip transmitter could result in a failure to trip on demand for a high level or a spurious low level trip.
"Fail High" will be the reverse. Failure to trip on a low level or a spurious high level trip.

Fig 2b is an atmospheric feed vessel with a constant flow out and on/off make up based upon the level switches. (A silly arrangement, but one which can be found. This guarantees an incident every time a switch fails in service).

Cause 1	Level Switch Low (LSL) fails on demand: A demand is placed upon it every time it is asked to operate.
Consequence	The pump will cavitate eventually running dry. Worst case - pump replacement. (Quick evaluation by leader: Cost ~ $3000 for each switch failure. Failure rate ~ every 4 years for payback time of two years worth spending ~$1500 to eliminate)
Safeguards	None
Risk	Low
Action	Assess test frequency for switch and monitor performance.

Cause 2	Level Switch High fails on demand.
Consequence	Overflow vessel into bund. The bund will hold the capacity of the tank. If the feed is not stopped within 20 minutes the bund will overflow. The material is both expensive, difficult to recover and toxic to marine life.
Safeguards	Operator observation (not considered likely)
Risk	High
Action	Provide valve position feed back on inlet with "time out" which shuts off the feed (based upon the expected frequency of operation).

Typical Equipment Failures:

Heat Exchangers:

E.g. Tube failure or cracked plate, fan trip (fin fan exchangers), weather extremes (e.g sudden deluge on fin fan exchanger), fouling (external or internal, hydrates, wax, bugs).
The first question to ask for tube or plate failure is which way the leak will go. In many cases it could be either, depending on the position of an upstream control valve. Overpressure protection should be built into the design either by the provision of a safety valve or by the equipment design pressure. This leaves contamination and its downstream effects as the issue to be addressed, particularly in the food industry. Leaks between streams of similar phase and composition can be difficult to detect and can have significant consequences. For example, a leak on a gas to gas exchanger around a methanator feeding an ammonia synthesis loop can introduce carbon oxides to the synthesis loop and poison the ammonia converter catalyst. Aqueous to aqueous leaks can be difficult to detect so it is always worth checking whether steam or chilled water systems in the food industry have only food grade additives.

Pumps:

E.g. Seal failures: Single mechanical seals will require an external method of leak detection, if this can be justified. Where double mechanical seals are used, leak detection (at least of the inner seal) is usually provided.
Electrical failure: A trip causing the motor contactors to open is apparent to the operator.
Mechanical Failure: A coupling or impeller failure can go undetected unless there is some secondary indication of operation such as flow.

Block Valves:

E.g. Stuck in wrong position or seat passing ("Misdirected Flow"): Feedback on automated block valves covers the "stuck" situation. A passing seat is insidious and if the consequence is significant, a double block and bleed should be considered. The dairy industry makes extensive use of valve feedback which is not the case in the oil or petrochemical industry.

Control valves:

Control valve failures are covered by the transmitter failures discussed above. The issues generated by the failure of the transmitter provide the loop's worst case since the operator will have no idea it has happened. Treating the valve separately is unnecessary repetition.

Relief Valves:

E.g. Failure to reseat (common): How will you know? What contingency is in place?
Spring failure causing RV to open: Not common but not incredible
Fouled seat: A bursting disk backed up by an RV can be used but beware of hidden pitfalls.

Bursting Discs:

E.g. Pinhole or fatigue leading to in service failure, incorrect installation

Non Return Valves:

E.g. Stuck open: If the operation of a non return valve cannot be verified in service then it's use should only be considered for process rather than safety reasons.

Maintenance/Engineering Errors Post Start Up:

Control Valve Trim Change:

Check this does not compromise the sizing basis for a downstream relief valve.

XSV (emergency shutdown valve) Solenoid Change:

This can affect the speed the valve opens or closes. The sequence of closing may be important, for example an outlet XSV closing before and inlet XSV can create the high pressure situation it is intended to prevent.

Pump / Impeller replacement:

An almost identical pump is used as a spare with no hazardous area rating on the motor.

Pump Wiring (Centrifugal):

Rotation checks should pick up reverse wiring otherwise reduced performance will be the only indication.

Trimmed Impeller Replaced with Full Sized Impeller.

In most of the above cases the solution is to have a management system, such as control of change, in place.

Benefits:

The suggestion, to commence the study of each line by addressing the failure effects as individual causes, does not change the principles upon which HAZOP is based. The classical HAZOP guidewords are still applied after the failures have been analysed but **only** additional issues are considered. It should be noted that a conscientious application of the traditional guidewords alone should bring out all of the issues raised by the failure effects application. But why wait? The HAZOP worksheet completed for fig 3 identifies all the failure effect process deviations as "equipment or control system failure". Study item "23.1" could just as easily have been labelled "Low Flow".

The quality of the review is of paramount importance and many factors can compromise this. A large study can involve many P&ID's and requires stamina from both the leader and the team. After a few sessions, the sight of "High Flow" for the 57th time can induce an attention deficit known as "analysis paralysis". The number of visits to this guideword do not change, but the mental burden is reduced. In addition, some team members find the classical guidewords abstract, making the generation of "causes" hard work. It is easier to generate a list of equipment and control system failures at the outset. By progressing along a line, identifying all the failures associated with equipment and control systems, a list of "causes" is immediately generated for the team to get stuck into. Having worked through these, they will have a very good understanding of the line and it's dynamics. The classical guidewords are then applied. Only issues not already raised in the study of failure effects are addressed and documented. It could be argued that time is saved in the generation of "causes" but time saving is not the objective. HAZOP quality is the main issue.

The benefit of working in this way did not come as a blinding flash of inspiration for the author. It resulted from undertaking many batch/sequential process HAZOPs where one method of generating deviations is to assume each item is not in it's desired state at each stage in the process. The power of this simple approach slowly became apparent. Applying the same principle to continuous processes was a logical step.

Why only failure effects and not failure modes?

So long as a failure is credible, it can be considered. Any failure having serious consequences and thought to be sufficiently likely can then have its failure modes analysed as a HAZOP action item. Note: Low likelihood is not the same as not credible. It may, however, be a reason to accept risk.

An Additional Burden?

The author does not see the application of failure effects as an additional burden but rather an enhancement to the existing methodology. If it is accepted that all the issues raised by a review of the failure effects are necessary then there is no additional burden in review time or documentation.

Conclusion:

Starting each line with a failure analysis has several benefits. Most causes that would be generated by the traditional guidewords are captured at this stage, and the team must do some solid analysis from the start improving their understanding of the line dynamics before the classical guidewords are applied. The quality and completeness of the finished product, namely the HAZOP report, in the author's opinion, is greatly improved as is the efficiency of the review.

Biography:

Colin has more than 35 years industrial experience including the oil& gas, petrochemical, dairy and other associated industries. He established Safety Solutions Ltd in 1993 and now, together with his son Paul, offers Process Safety, Training and Advanced Process Control consultancy services. He has extensive experience in HAZOP and other process hazard review techniques and has trained over 1000 HAZOP leaders and participants over the last 15 years. A qualified chemical engineer, Colin has professional registration in the UK, Canada and New Zealand, where he is now based. In his spare time he moonlights as a Test Certifier under New Zealand's Hazardous Substances and New Organisms legislation and as a New Zealand Qualifications Authority assessor.