COMPUTER AIDED HAZARD IDENTIFICATION: FAULT PROPAGATION AND FAULT-CONSEQUENCE SCENARIO FILTERING

S.J.Wakeman, P.W.H.Chung, A.G.Rushton, F.P.Lees, F.D.Larkin and S.A.McCoy

Work at Loughborough University on the development of an automated HAZOP-style hazard identification tool has been in progress for several years. This paper briefly describes the HAZOP procedure and the methodology (fault propagation) upon which Loughborough's system, called AutoHAZID, is based. Problems with a purely fault propagation based approach are illustrated by drawing comparisons between AutoHAZID and conventional HAZOP reports. Four heuristics, used by human teams during HAZOP, are identified as being absent from AutoHAZID's reasoning strategy. The basis of these heuristics, and the impact of using them is then discussed before going on to describe how AutoHAZID has been augmented with a set of filtering rules to mirror the human strategy more closely. A set of examples of AutoHAZID report fragments, based upon an olefin dimerisation plant, is given to illustrate the benefits. An assessment of the improvements in AutoHAZID's performance as a result of the introduction of the filters is given in conclusion.

Introduction

The HAZOP methodology is a widely used and well respected hazard identification technique pioneered at ICI. It has been described in the British Chemical Industry Safety Council publication 'Safety Audits' as:

The application of a formal systematic critical examination to the process and engineering intentions of the new facilities to assess the hazard potential of mal-operation or mal-function of individual items of equipment and the consequential effects on the facility as a whole.

The procedure sets up a framework intended to encourage a hazard study team to consider every possible deviation from intended behaviour of the plant, the potential causes of such a deviation and the consequences resulting from the deviation. A full description of the methodology is given by the Chemical Industry Safety and Health Council of the Chemical Industries Association Limited [CIA, 1977]. In brief the method involves generating a deviation from intent by combining a guideword such as LESS, MORE, NO or OTHER with a process variable such as FLOW, PRESSURE or TEMPERATURE. Each of the guidewords is combined in turn with each of the process variables at agreed locations in the plant being studied. The result is that the team considers possible causes and consequences of every deviation from intent in the plant. The results of the study are generally presented in tabular form as shown in figure 1.

figure 1. A sample HAZOP report fragment

Deviation	Causes	Consequences	Protections
more flow into tank tk101	bypass valve opened in error	potential tank overflow	level alarm on tk101

A prototype AUTOmatic HAZard IDentification (AutoHAZID) system based on the HAZOP approach is currently under development at Loughborough. The work forms part of large scale ESPRIT project being undertaken by a multinational consortium including partners from research institutes, the process industries and software houses. The system is a re-implementation and extension of two previous pieces of work carried out at Loughborough [Chung, 1993; Jefferson et al 1995].

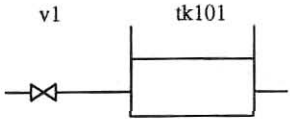
The purpose of the tool is to aid the design process by identifying problems prior to a formal HAZOP meeting. This should result in a significant reduction in the time required for such a meeting and thus reduce the cost of the procedure. AutoHAZID has been applied to many test cases including the plants described in Lawley [1974] and Wells et al [1976]. A slightly simplified version of the Lawley case will be used here for comparison purposes since it is a well known public domain example of the application of the HAZOP technique. The plant diagram is given in fig2.

This paper addresses the methodology upon which AutoHAZID is based, identifies problems inherent in that underlying methodology and describes solutions which have been developed to counter those problems.

AutoHAZID methodology - fault propagation

The underlying methodology upon which AutoHAZID is based is called fault propagation. This is an established technique which uses qualitative relationships to determine how a disturbance at some point in a network of relationships will affect the rest of the nodes in the network. Early work focused on application of fault propagation to fault tree synthesis [Lees and Kelly, 1986]. In the specific instance of a chemical plant, the nodes in the network can be the process variables such as flow at the outlet of a pump and flow at the inlet of the pump. The relationships declared between these variables define the network. AutoHAZID uses the signed directed graph approach [Iri et al, 1979; Tsuge et al, 1985] to declare these relationships. One relationship in the network may state that the flow at the outlet of a pump is *dependent directly upon the flow at the inlet of that pump. In other words, if the inlet flow* increases then the outlet flow will increase, if the inlet flow drops then the outlet flow will drop also. For any given plant description AutoHAZID can create a network of these relationships based upon relationships that exist within different unit types irrespective of the plant configuration. The configuration independent relationships are combined with connectivity information to generate a connected network of relationships that describe the plant as a whole. The example below shows how a small part of the network is built.

Example : Consider the small plant section below which simply shows an open isolation valve (v1) connected to the inlet of a storage tank (tk101).



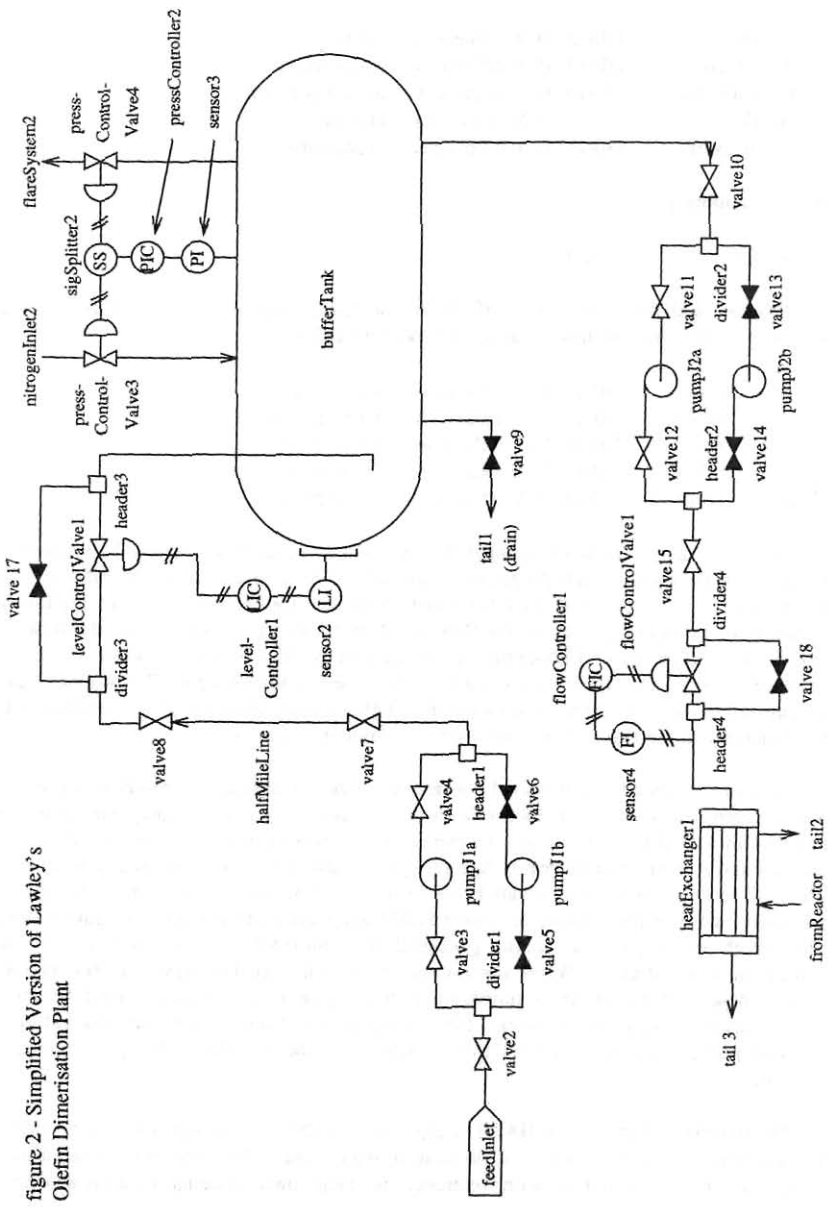


figure 2 - Simplified Version of Lawley's Olefin Dimerisation Plant

First the configuration independent unit information.

v1 relationships

in flow	DIRECTLY influences	out flow
in pressure	DIRECTLY influences	out pressure
in temperature	DIRECTLY influences	out temperature
out flow	DIRECTLY influences	in flow
out pressure	DIRECTLY influences	in pressure *etc*

tk101 relationships

in flow	DIRECTLY influences	level *etc*

Now we add the connectivity information which is plant dependent. This information serves to connect the two independent networks declared above.

v1 out flow	DIRECTLY influences	tk101 in flow
v1 out pressure	DIRECTLY influences	tk101 in pressure
v1 out temp.	DIRECTLY influences	tk101 in temp.
tk101 in flow	DIRECTLY influences	v1 out flow
tk101 in pressure	DIRECTLY influences	v1 out pressure *etc*

Now we have a network defined which declares local relationships between process variables in the plant. Fault propagation can now be used to determine the effects of some disturbance in the network on the other nodes. Consider, for example, the fault 'high pressure upstream of v1' occuring causing the flow at (v1 in) to increase. We see that the flow at (v1 out) would also increase. Furthermore an increase in the flow at (v1 out) would cause a flow increase at (tk101 in), this in turn causing an increase in (tk101 level). The original fault has propagated through the network showing that 'high pressure upstream of v1' would result in a level increase in the tank. This is the essence of fault propagation.

Fault propagation is the method by which AutoHAZID emulates the HAZOP procedure. It is also believed to echo the method subconsciously used by humans to carry out the reasoning required in a HAZOP. There are differences in the results of the reasoning carried out by humans and AutoHAZID however, even though the same low level reasoning strategy is used. These differences occur for a variety of reasons. The most fundamental though is the *exhaustive and repetitive nature of AutoHAZID's application of the fault propagation strategy.* The length of propagation chains generated by AutoHAZID is not bound by time or concentration constraints. When humans reason about the relationships in a network such as the one described the length of propagation chains generated is often curtailed by applying some heuristic to save time or work - partial propagation chains are remembered and the start and end points used like local influences rather than the full chains being regenerated for example.

The rigorous nature of AutoHAZID's application of the fault propagation process generates a larger result set than would a human team in many cases. This observation has also been made by other researchers with reference to their own systems [Vaidhyanathan and

Venkatasubramanian, 1996]. The amount of information, often redundant, can however be too great for easy consumption. The fault propagation methodology needs to be augmented by heuristics such as those used by humans to curtail the amount of redundant information generated. The following sections highlight in more detail the nature of the differences between the results produced by a human and an early version of AutoHAZID caused by HAZID's rigorous fault propagation system and a method is presented, termed filtering, which has been used to overcome some of the problems.

Comparison of human and early AutoHAZID reports

Before beginning it will be useful to clarify some terms that will be used frequently.

fault: An equipment failure which leads to some process deviation or hazard.
consequence: A hazard or operability problem produced by a process deviation or fault.
scenario: A fault and consequence pair identified under some deviation.

In order to benchmark the behaviour of AutoHAZID it was applied to the feed section of an olefin dimerisation plant as given by Lawley[1974]. The AutoHAZID result set was compared to the result set given by Lawley. The most immediate observation was the difference in the size of the reports generated. The report produced by AutoHAZID was many times the length of that given by Lawley. It seemed unlikely that the automated system had actually produced so much more interesting and correct information than the human one so work began to identify the differences in reports.

The most immediate observation made during the comparison was the difference in number of causes given for each set of consequences. Lawley cites on average around two causes per consequence. AutoHAZID on the other hand averaged in the region of ten causes per consequence. The extra causes were found to fall into a variety of classes. In a local context, ie. within a list of causes for some consequence, it was found that some causes were incorrect due to process fluid dependency and others were uninteresting because they were too similar to other causes listed. A clear example of the latter arose under the guideword NO FLOW in the line to the buffertank. Lawley cites isolation valve closed in error as a possible cause. AutoHAZID, since it decomposed the plant to the unit level, cited every individual isolation valve on the feed side of the buffertank. In a global context, ie. within the report as a whole it was seen that small lists of faults often appeared together in clusters scattered throughout the report. The pair of faults 'LCV bypass opened in error' and 'LCV fails open' in the feed section to the buffertank for example were given as potential causes of MORE FLOW into the buffertank and MORE LEVEL in the buffertank. The two faults would usually not be repeated for the second deviation by a human team, rather a reference to the cause list in the earlier MORE FLOW deviation occurrence would be given.

A further observation arising from the comparison was that hazardous scenarios tended to appear many times in the report as they could be identified under a variety of guidewords. In Lawley's example it would be possible to identify the overflow of the settling tank caused by the LCV failing open under either high flow into the settling tank or under high level in the tank itself. The mechanistic approach taken by AutoHAZID would find both cases, but unlike the human team would not realise that listing the scenario a second time would be redundant.

The comparison also showed that AutoHAZID was frequently identifying consequences which were incorrect in the context of the process being considered. Hazards are very often dependent upon the process fluids and conditions in the plant. In a high pressure system containing a flammable fluid a leak leading to loss of containment would usually be more interesting than in a low pressure system containing cooling water. AutoHAZID was incapable of distinguishing such subtleties - it could only be made to report either a generic 'fluid release' or a list of different types such as 'flammable release', 'toxic release' and 'corrosive release' as the consequences of the leak.

Applying AutoHAZID to other test cases confirmed the initial findings from the Lawley comparison. Are all of these differences undesirable though? Clearly the process dependent nature of the causes and consequences was a major shortcoming. In the loss of containment example cited above it is important that the system should be able to draw attention to the different categories of release. The effect of listing many faults which are essentially the same due to their degree of similarity in terms of unit type and plant location is to clutter the report with uninteresting information. This could also lead to important information being overlooked when the report is studied. The repeated clustering of small faults sets, which would be referenced rather than repeated by a human team, has the same effect. The final difference, the repeating of scenarios under different deviations, also makes the report more verbose without adding any novel information.

Classifying and addressing the undesirable features

The previous discussion highlights two areas of interest, those of correctness and conciseness. Into the former camp fall the problems with the process dependent nature of faults and consequences. Into the latter the issues of fault similarity, fault clustering and repeat scenarios. After much discussion with industrial partners it became clear that even if the system could deal with the process dependency the sheer volume of information generated by AutoHAZID would still prove prohibitive to its usefulness. The report must consist of a very high percentage of interesting and novel information. Somehow the information must be filtered before reporting in a way that preserves the interesting and important whilst at the same time greatly reducing the volume. Essentially the number of scenarios reported is not the key to success, rather it is the fraction of those reported which are of interest. If every scenario listed was different and interesting then even if some problems were not identified by AutoHAZID the burden upon the human hazard study team would still be greatly eased. If on the other hand only one in every twenty scenarios was different and interesting the effort required to sieve through the report would probably outweigh the benefit. The moral seems to be: 'be correct but be concise'.

So, how can these issues of correctness and conciseness be addressed? In the latter case we are in a good position since we have too much information. If we put ourselves in the same position with the process dependent faults and consequences we would be able to make progress along the same lines. The use of heuristics such as those mentioned earlier - combining similar faults, commuting fault clusters to references and discarding repeat scenarios - should enhance the usefulness of the system. These three together with a method for filtering process dependent faults and consequences give us four heuristics that should reduce the size of the report generated by AutoHAZID without losing anything of interest. These rules have been termed filtering methods.

Addressing the problem areas by use of filtering methods

The four filtering methods mentioned above have been implemented. The following discussion outlines the heuristics employed giving a flavour of the impact of the filters when used both in combination and individually. The report fragments given as examples once more pertain to the Lawley case study. The fragments are intended to be illustrative rather than exhaustive and focus upon the deviations NO FLOW into buffertank and LESS LEVEL in the buffertank. For clarity, protective devices have been omitted from the results since they have no bearing on the filters discussed here.

The report fragment from AutoHAZID, with all filters, as applied to the guidewords NO FLOW into buffertank and LESS LEVEL in the buffertank is shown in fig3. The report fragment without filters employed is given in fig4.

The difference in clarity and conciseness is immediately apparent. Although only a small report fragment has been shown, the benefits on larger studies are even more dramatic. When scaling up the study to larger plants and more deviations the performance of the filters actually improve, especially those which filter repeat scenarios and handle the cluster referencing. The following discussion describes how each of the filters contribute to the final effect. As each filter is added the cumulative effect can be seen.

figure 3. Report fragment from AutoHAZID with all filters applied.

Deviation	Causes	Consequences
bufferTank noFlow in	levelControlValve1 closed, valve8 etc closed, pumpJ1a no flow out.	bufferTank loss of level, gas breakthrough to downstream units.
bufferTank lessLevel liquid	levelControlValve1 part closed, valve8 etc part closed, pumpJ2a overspeed, pumpJ1a less pressure out.	bufferTank loss of level, gas breakthrough to downstream units.
	valve8 etc leak, halfMileLine leak, valve17 leak.	bufferTank loss of level, gas breakthrough to downstream units, toxic release, flammable release.

figure 4. Report fragment from AutoHAZID without filters.

Deviation	Causes	Consequences
bufferTank noFlow in	levelControlValve1 closed, valve8 closed, valve7 closed, valve4 closed, halfMileLine blocked, valve8 blocked, valve7 blocked, valve4 blocked.	bufferTank loss of level, gas breakthrough to downstream units.

	valve2 closed, valve3 closed, valve2 blocked, valve3 blocked, feedInlet no flow upstream.	bufferTank loss of level, gas breakthrough to downstream units, pumpJ1a cavitation.
bufferTank lessLevel liquid	levelControlValve1 closed, levelControlValve1 part closed, valve8 closed, valve8 part closed, valve8 blocked, valve7 closed, valve7 part closed, valve7 blocked, valve4 closed, valve4 part closed, valve4 blocked, halfMileLine blocked, pumpJ2a overspeed.	bufferTank loss of level, gas breakthrough to downstream units.
	valve2 closed, valve2 blocked, valve3 closed, valve3 blocked, feedInlet no flow upstream.	bufferTank loss of level, gas breakthrough to downstream units, pumpJ1a cavitation.
	valve8 leak, valve7 leak, valve4 leak, valve17 leak, halfMileLine leak, pumpJ1a leak, valve3 leak, valve2 leak, valve6 leak, valve5 leak.	bufferTank loss of level, gas breakthrough to downstream units, toxic release, flammable release.

1. Process dependent faults and consequences

This filter allows a wide variety of similar but subtly different faults and consequences to be defined in the models used by AutoHAZID. Each variant being conditional upon some process information means that, although AutoHAZID will initially identify them all, the filter can selectively reject those which are not relevant in the context of the plant being analysed. The results of applying only this filter are given as fig 5. The fault 'blocked' has been declared as being dependent upon the fluid freezing or containing solids. A spontaneous blockage by a clean fluid above its freezing point is considered unlikely to occur. AutoHAZID has identified that there is no obvious source of solids and that the fluid will not freeze under the process conditions.

figure 5. Report fragment with process dependency filter only.

Deviation	Causes	Consequences
bufferTank noFlow in	*levelControlValve1 closed,* valve8 closed, valve7 closed, valve4 closed.	*bufferTank loss of level,* gas breakthrough to downstream units.
	valve2 closed, valve3 closed, feedInlet no flow upstream.	bufferTank loss of level, gas breakthrough to downstream units, pumpJ1a cavitation.
bufferTank lessLevel liquid	levelControlValve1 closed, levelControlValve1 part closed, valve8 closed, valve8 part closed, valve7 closed, valve7 part closed, valve4 closed, valve4 part closed, *pumpJ2a overspeed.*	bufferTank loss of level, gas breakthrough to downstream units.
	valve2 closed, valve3 closed, feedInlet no flow upstream.	bufferTank loss of level, gas breakthrough to downstream units, pumpJ1a cavitation.
	valve8 leak, valve7 leak, valve4 leak, valve17 leak, halfMileLine leak, pumpJ1a leak, valve3 leak, valve2 leak, valve6 leak, valve5 leak.	bufferTank loss of level, gas breakthrough to downstream units, toxic release, flammable release.

2. *Combining similar faults*

This filter is used to combine similar faults in similar units in the same process line to a single fault. Lawley quotes an isolation valve blockage as being a cause of NO FLOW in the feed line to the buffertank rather than state a possible valve blockage for each isolation valve in the feed line. AutoHAZID, with this filter applied, achieves a similar result as can be seen in fig6. If the same fault is found in many instances of the same unit type in the same line as being the cause of some deviation then only one of them is retained. The *etc* qualifier is added to the fault description to show that many similar faults could occur.

figure 6. Report fragment with process dependency and similar fault filters.

Deviation	Causes	Consequences
bufferTank noFlow in	levelControlValve1 closed, valve8 etc closed.	bufferTank loss of level, gas breakthrough to downstream units.
	valve2 etc closed, feedInlet no flow upstream.	bufferTank loss of level, gas breakthrough to downstream units, pumpJ1a cavitation.
bufferTank lessLevel liquid	levelControlValve1 closed, levelControlValve1 part closed, valve8 etc closed, valve8 etc part closed, pumpJ2a overspeed.	bufferTank loss of level, gas breakthrough to downstream units.
	valve2 etc closed, feedInlet no flow upstream.	bufferTank loss of level, gas breakthrough to downstream units, pumpJ1a cavitation.
	valve8 etc leak, valve17 leak, halfMileLine leak, pumpJ1a leak, valve3 etc leak, valve6 etc leak.	bufferTank loss of level, gas breakthrough to downstream units, toxic release, flammable release.

It is noticeable that AutoHAZID quotes 'valve8 etc...', 'valve3 etc...' and 'valve6 etc...' as possible causes of lessLevel. This is because the faults do not appear in the same line. AutoHAZID recognises this difference in location as being important, the pressure difference across the pump for example may make one of the leak locations a more worrying prospect.

3. Removing repeat scenarios

This is a filter which works at the level of the whole HAZOP report. If some fault-consequence scenario is found under some deviation and AutoHAZID has already found the same fault-consequence scenario under an earlier deviation then the latter find will be omitted. The entire second block of scenarios identified under lessLevel has been eliminated by the repeat scenario filter. The report fragment is shown in fig7.

figure 7. Report fragment with process dependency, similar fault and repeat scenario filters.

Deviation	Causes	Consequences
bufferTank noFlow in	levelControlValve1 closed, valve8 etc closed.	bufferTank loss of level, gas breakthrough to downstream units.
	valve2 etc closed, feedInlet no flow upstream.	bufferTank loss of level, gas breakthrough to downstream units, pumpJ1a cavitation.

bufferTank lessLevel liquid	levelControlValve1 part closed, valve8 etc part closed, pumpJ2a overspeed.	bufferTank loss of level, gas breakthrough to downstream units.
	valve8 etc leak, valve17 leak, halfMileLine leak, pumpJ1a leak, valve3 etc leak, valve6 etc leak.	bufferTank loss of level, gas breakthrough to downstream units, toxic release, flammable release.

4. Referencing fault clusters

Often a set of faults appeared together as a cluster in the early AutoHAZID system as possible causes of several different deviations. AutoHAZID now uses a filter to determine whether some cluster of faults leads to the deviation being considered via a propagation sequence involving a deviation already reported. If so a reference is given to the earlier deviation. The results of adding this filter are shown in fig8 (cf. fig3, repeated here for the reader's convenience).

figure 8. Report fragment with all filters operating.

Deviation	Causes	Consequences
bufferTank noFlow in	levelControlValve1 closed, valve8 etc closed, pumpJ1a no flow out.	bufferTank loss of level, gas breakthrough to downstream units.
bufferTank lessLevel liquid	levelControlValve1 part closed, valve8 etc part closed, pumpJ2a overspeed, pumpJ1a less pressure out.	bufferTank loss of level, gas breakthrough to downstream units.
	valve8 etc leak, halfMileLine leak, valve17 leak.	bufferTank loss of level, gas breakthrough to downstream units, toxic release, flammable release.

The three faults 'valve3 etc leak...', 'valve6 etc leak...' and 'pumpJ1a leak...' have been changed to a reference to pumpJ1a less pressure out, which would appear earlier in the report.

Conclusion

Comparison of the early AutoHAZID system with the filter-augmented version yields similar observations to the comparison of the Lawley result set with the early AutoHAZID result set. The effect of including the various filters has been to shift AutoHAZID's behaviour toward that demonstrated by a human team. The result set produced now is far more concise but the change has been achieved without losing any valuable information. The response of industrial partners to the developments has been highly favourable. Gaining acceptance for automated systems, which are intended to emulate a manual procedure, is often difficult. This is even more so if the results of the two approaches can be easily compared and there are significant

differences. In order for a system to be accepted it must first demonstrate that it can delivery a similar type of result, the use of filters goes a long way towards achieving this.

Looking at the examples above, particularly the comparison of the early AutoHAZID report fragment with the fragment from the filter augmented version, the benefits of applying the methods are clear. All of the correct hazards are identified with the filtering methods applied but in a much more succinct report. Returning to the earlier moral elicited from our industrial partners the filters manage to successfully improve on correctness and conciseness.

The use of the filters described here does not solve all of the problems associated with AutoHAZID's rigorous fault propagation system. Many other types of problem exist which are yet to be addressed by means of filters or otherwise. Progress is encouraging however.

Acknowledgements

The authors would like to thank all in the STOPHAZ project and the Commission of the European Community who have provided finance for the project. P.W.H.Chung is supported by a British Gas/Royal Academy of Engineering senior research fellowship.

References

Chung, P.W.H. (1993). Qualitative Analysis of Process Plant Behaviour. Proc. 6th Int. Conf. on Ind. and Eng. Applications of Artificial Intelligence and Expert Systems. p277.

C.I.A. (1977). A Guide to Hazard and Operability Studies.

Iri, M., Aoki, K., O'Shima, E and Matsuyama, H. (1979). An Algorithm for Diagnosis of System Failures in Chemical Process. Computers in Chem. Eng. Vol 3, p489.

Jefferson, M., Chung, P.W.H. and Rushton, A. (1995). Automated Hazard Identification for Emulation of Hazard and Operability Studies. Proc. 8th Int. Conf. on Ind. and Eng. Applications of Artificial Intelligence and Expert Systems. p765.

Lawley, H.G. (1974). Operability Studies and Hazard Analysis. (1974). Chemical Engineering Progress Vol 70, No 4.

Lees, F.P. and Kelly, B.E. (1986). The Propagation of Faults in Process Plants: Parts 1-4. Reliability Engineering Vol 16, No1.

Tsuge, Y., Shiozaki, J., Matsuyama, H. and O'Shima, E. (1985). Fault Diagnosis Algorithms Based on the Signed Directed Graph and its Modifications. Ind. Chem. Eng. Symposium No 92, p133.

Vaidhyanathan, R. and Venkatasubramanian, V. (1996). Experience with an Expert System for Automated HAZOP Analysis. Computers in Chem. Eng. Vol 20, Suppl., ppS1589-S1594.

Wells, G.L., Seagrave, C.J. and Whiteway, R.M.C. (1976). Flowsheeting for Safety. Instn. Chem. Engrs.