MORE EFFECTIVE PERMIT-TO-WORK SYSTEMS

R.E.Iliffe, P.W.H. Chung and T.A. Kletz
Department of Chemical Engineering, Loughborough University, Loughborough, Leicestershire, LE11 3TU. United Kingdom. Email: R.E.Iliffe@lboro.ac.uk

Many incidents in the chemical-industrial workplace are associated with maintenance works, which are typically controlled by permits-to-work (PTWs). Computerised PTWs have advantages of flexibility and informational clarity, and allow closer co-ordination of activities and integration with computer applications. A system has been developed linking computerised PTWs with an incident database: the system examines the nature of the job, equipment and chemicals specified on the PTW and draws users' attention to relevant incident reports without requiring explicit search or further data; unknown or forgotten hazards are thus highlighted when preventative action may still be taken.
Keywords: Permit-to-work, computer integration, accident database.

INTRODUCTION

According to the Health and Safety Executive[1] (HSE) 30% of the accidents which occur in the chemical industries are maintenance-related. A quick check of the Institute of Chemical Engineers accident database reveals that over 700 accidents of the 5000 listed were maintenance-related. Some of these were due to the way in which the maintenance was carried out but most were due to errors in the way the equipment was prepared for maintenance or handed over. Sometimes the permit-to-work (PTW) system was poor, sometimes it was not followed.

Production of PTWs on a computer would have many advantages which could improve permit systems and make it easier to follow them. There would be less tedious form-filling and greater legibility, the permits could then be inspected by supervisors and managers from any location and analysis of the work carried out would be easier. The computer could refuse to issue more than one permit for the same item of equipment and could remind users of other work in progress nearby. However, much greater advantages would follow by linking the computer to a database of accidents and to other information systems. For example:

- The computer could remind the users of any special hazards associated with the equipment to be maintained and its contents, points highlighted during the hazard and operability study and lessons learned during previous maintenance.
- If a vessel is being prepared for entry, the computer could check that the number of slip-plates (blinds) to be fitted (or pipes disconnected) is the same as the number of connections shown on the drawing.
- Suppose a fitter has to replace a gasket during a night shift. On some plants it is easy; only one sort is used and all he has to do is select the right size. On other plants many types are used. The fitter has to get out a diagram, find the line number and then look-up the details in a bulky

equipment list. It should be possible for him to view the line diagram on a computer screen, select the line and have details of it displayed, including the location of the gaskets and any distinguishing marks such as their colour. The line diagram and equipment list will have been prepared on a computer; all that is needed is a link between the design system and the maintenance system. (Of course, we should, if possible, reduce the number of types of gaskets, nut and bolts required even though we may use more expensive types than strictly necessary on some duties.)

- The computer could look at the nature of the job, the type of equipment and the chemicals involved as entered on the permit and then draw attention to any relevant incidents in the accident database. Note that the user would not need to search the database; the computer would do this for him. The computer would be active, the user passive, while in normal information retrieval the opposite usually obtains. This is both the most original and the most fully developed of the proposals discussed in this paper and is presented in more detail from page 8, onwards.

LIMITATIONS OF PERMITS TO WORK

The HSE defines a Permit to Work as:

> A formal written system used to control certain types of non-routine work, usually maintenance, that are identified as hazardous. The terms 'permit-to-work' or 'permit' refer to the certificate or form that is used as part of the overall system of work. The permit is a written document that authorises certain people to carry out specific work at a specific time and which sets out the hazards associated with the work and the precautions to be taken.[2]

Thus a PTW system incorporates both a written document and a series of rules describing and circumscribing safe methods of working. This said, the specific *purposes* which PTWs seek to achieve are more diverse and more complex. One appreciation of PTWs has it that their purpose is first to ensure that proper consideration has been given to the hazards associated with any given proposed operation, second that they should ensure appropriate precautions have been put in place and third that they should facilitate communication between the various parties involved in the works[3]. An alternative view is to say that PTWs perform at least three notionally distinct functions: first they aid the *identification* of potential hazards together with the concomitant precautions which must be taken; second they aid *co-ordination* of the imposition of precautions, the actual carrying out of the maintenance task and the eventual removal of precautions. Third, they *provide a written record* of what was done, by whom, when and how. This may be of use in the event that something does in fact go wrong, as well as to help monitor the procedures which are in place; it would be a mistake to perceive PTW systems as being set in stone; to obtain the best use of them they should be capable of easy modification to meet changing circumstances and individual user needs.

The HSE study of incidents in the workplace reveals that a large proportion of the maintenance-related incidents involved failures of the PTW system: in some cases, to a greater or a lesser degree, the PTW system was inadequate; in others it was entirely absent. This is a sobering state of affairs: safety in the chemical-industrial-workplace is achieved primarily by placing physical guards between personnel and known hazards; maintenance, by definition, typically involves the removal of these together with the introduction to the work-site of additional hazards, such as flames, which might not already be present. It is, therefore, not

excessive to regard maintenance itself as an inherently hazardous activity. Largely as a result of the HSE study considerable further work has been done on PTW systems. One report of work carried out by the HSE itself which was published in 1995 was a survey of PTW systems in medium-sized chemical plants[4]. This identified a number of areas where current PTWs are inadequate: the type and format of PTWs varies widely across the spectrum of plants studied; a majority of plants use at least three different forms to cover a variety of jobs, while a significant minority of plants used as many as ten different forms. At the lower end of the scale many firms copy the permits of other companies without paying sufficient regard their appropriateness to their own needs; at the upper end of the scale too great specificity of permit forms may lead to a confusion of paperwork with a consequent loss of efficiency.

This finding was a symptom of a more general confusion on the part of firms over precisely which jobs should be covered by a PTW and which should not. Further, within many companies there was disagreement between management, foremen and fitters over the general applicability of PTWs and the extent to which these had to be followed in every detail. Fitters in particular were unclear about the extent of their freedom to vary their work in light of developing knowledge of the maintenance situation and the extent to which they were bound to follow the plan.

Administrative difficulties exist too: it is frequently difficult to locate authorised issuers when a permit is actually needed, with the result that permits are commonly issued at a specific time in the morning with actual commencement of the work being left till some time later in the day – or in some cases – until several days later. Similarly, confusion frequently exists over which authorisations, additional to that of the issuer, a permit requires – whether it must be signed-off by a fire-marshal, by management or by some specialist fitter. Of course, when additional authorisation *is* required this further exacerbates the problem of locating those whose signature must be obtained. One example serves to illustrate how serious the consequences of these practices may be:

> In 1989 a take-off branch in a polyethylene plant was dismantled to clear a choke. The 8-inch valve isolating it from the reactor loop was open and hot ethylene under pressure came out and exploded killing 23 people, injuring over 130 and causing extensive damage. Debris was thrown six miles and the subsequent fire caused two liquefied petroleum gas tanks to burst. The valve was opened by compressed air and the two air hoses, one to open the valve and one to close it were connected-up the wrong way around. The two connectors should have been of different sizes or design so this could not occur. In addition they were not both disconnected and a lockout device - a mechanical stop - had been removed. It is also bad practice to carry out work on equipment isolated from hot flammable gas under pressure by a single isolation valve. The take-off branch should have been slip-plated and double block-and-bleed valves should have been provided so the slip-plate could be inserted safely. Another factor in the incident was that the equipment had been prepared for repair and had then had to wait for several days until the maintenance team was ready to work on it. During this time the air lines were reconnected, the lockout removed and the isolation valve opened.[5]

Although proper practice would not have directly addressed the issue of bad design, had the permit only been issued *when it was actually needed* there would have been no opportunity for the proper isolations to be improperly removed.

One variant of the problem of administering PTWs which particularly drew the attention of the HSE involves the problem of ensuring that all those people who need to be informed of maintenance work are, in fact, informed. Although this is of particular significance when maintenance carries-over between shifts – the Cullen Report[6] cites the failure to inform a new shift that safety-critical equipment had been disconnected as one of the proximate causes of the Piper Alpha disaster – this problem is not restricted to shift changes. In complex plants, for example, pipework which is disconnected or otherwise isolated prior to maintenance may pass through a number of areas other than that where the work is actually carried out; it is clearly important that the people in charge of those areas be informed of the isolation; sometimes this is not done.

Quite apart from the specific weaknesses identified by the HSE, current PTWs suffer from three *general* weaknesses. First, they are *uninformative.* All current systems assume that issuers are competent to identify hazards and that they merely need to be prompted to remind them of particular dangers. Unfortunately, this assumption is not always wholly valid. The modern workplace is highly and increasingly complex; while it is reasonable to expect issuers to be aware of the more common hazards, such is this complexity that their failure to guard against *every possible* hazard is not culpable.

A second general weakness is that many permits tend to *lack clarity*: the format of most PTWs is some combination of lists, which the issuer checks as appropriate, and boxes which must be physically filled-in. This latter element is essential for adding specificity to the permit and for ensuring that issuers think when completing permits rather than merely operating on autopilot. A drawback, however, is that what seems clear to issuers frequently unclear to anyone else.

A third and final weakness of current systems is that they tend to be *inflexible.* Permits are – or should be – optimised to the specific needs of a given plant. However, to the extent that a PTW system *is* so optimised it tends to be less than optimal should the plant set-up or production requirements change. Given that firms increasingly see flexibility of production as a route to business success an obvious tension can be seen to exist with good PTW practice.

THE COMPUTER VERSUS THE PAPERCLIP

One pedestrian, though still significant, area where a computerised system scores over older systems lies in simple legibility: experience has shown that the rigors of the workplace impact badly on the legibility of permits; issuers' handwriting is frequently illegible; the permit becomes soiled and crumpled; in extreme cases it may disintegrate entirely with the resultant loss of site-specific data such as atmosphere test readings being lost. A computerised system, conversely, at least starts out legible – though individual copies still become stained. However, being automated, additional copies may be printed-out remotely from any convenient printer just as site-readings may be recorded on hand-held units and then downloaded electronically. This minimises delay, protects data and permits the computer to monitor the data so obtained: this last is significant since a number of incidents have occurred due to workers noting *but failing to act upon* instrument readings indicating the development of dangerous situations.

However, it is in the area of *co-ordination* that a computerised PTW system has the greatest comparative advantage over current methods. For example, in order to achieve greater

control over maintenance, the trend has been for maintenance tasks to be broken down into separate stages each of which is subject to a separate permit: typically, in the case of a complex job involving isolation of equipment one permit may be issued to control the application of appropriate isolation and/or the disconnection, a second to control the maintenance task itself and a third to co-ordinate the removal of the isolation and the reconnection of the equipment; traditionally co-ordination between these permits has been by means of a paperclip. However, the system of multiple-paper-permits is not beyond criticism: greater apparent control in such a case is achieved only at an increased cost in bureaucratic complexity; workers may be reluctant to perform 'unnecessary' administration and may not complete the PTWs properly, or may link completed permits improperly; fitters may, as a result of information overload, suffer confusion over what actions the permits actually require them to perform. In such a case redundancy may result in decreased safety.

This problem is compounded when we consider the issue of separate maintenance tasks occurring in close physical proximity. Good practice currently calls for maintenance on neighbouring pieces of equipment to be staggered if this is at all possible: two pieces of neighbouring machinery may require similar but not identical isolations; if one maintenance task is completed before the other the potential for confusion over the removal of isolations is obvious. Alternatively, one job may be fire-sensitive while the other may not: many incidents are on record which occurred due to sparks or flame from one job causing inflammable material from another to ignite.

While computer control of permits cannot eliminate these hazards it does allow much closer control of what goes on: hazards attendant on *each* job can be evaluated *in light of the other*; if problems of common isolation are likely to occur the system can identify potential trouble-spots and require that the isolations, once imposed, are fully labelled and locked to prevent improper removal. Co-ordination of this sort is something that computers are good at dealing with: if the system is properly configured, multiple linked permits may be issued without an unacceptable degradation of safety and also without undue bureaucratic proliferation.

OTHER ISSUES OF INTEGRATION

As was highlighted in the previous section, the imposition of isolations on large and complex plants is frequently difficult and time consuming. Two and three-dimensional plant schematics are in common use as a control tool in process plants. An obvious step would be to integrate a computerised PTW system with such systems: the question of which isolations to impose would be much easier for the permit issuer if such a visual representation were available; further, integration with a plant schematic would allow both the location and the progress of various jobs to be tracked with greater ease: a small refinement might be to have each job flagged and colour-coded to indicate the stage the work has reached; linked jobs might be visibly associated by means of coloured lines.

The visual representation of maintenance tasks would have an additional benefit in achieving greater clarity for the PTW: as has already been noted most PTW systems require a combination of selection-checking and box completion from issuers. While the former permits only a minimum of confusion, the latter is frequently a source of difficulty. A description of a work-site as "all the area to the West of building B" may be clear to the issuer but to no one else. The HSE recommends the imposition of a grid or similar system over a map of the plant area

which should be used as a reference; representing maintenance tasks on a plant schematic permits is a useful elaboration of this basic theme.

Computer integration and personnel co-ordination

As has already been noted, PTW systems tend to suffer from a variety of administrative problems with respect to the issuing process itself: in some plants PTWs must be jointly signed-off by both the actual issuer and a safety officer; in other cases they will additionally require the signature of a fire-safety officer. A computerised system would potentially ease if not wholly eliminate confusion by identifying which authorisations are required for any given permit and in what order, basing this assessment on the entries which are made on the permit by the initial issuer.

The problem of physically locating authorised personnel in order to obtain their authorisation would presumably remain even under a computerised system. This might be alleviated to some extent by the integration of the PTW system with a plant intranet: it would clearly be useful to be able to inform personnel of works affecting them electronically and to *view* permits remotely, what is moot is whether the added convenience of being able to *issue* PTWs remotely would be offset by a tendency on the part of issuers to skimp on necessary checks: given that PTWs now *could* be issued from wherever an issuer happened to find himself, might this capability encourage him to be lax in performing necessary checks? Given that a major imperative of any PTW is to encourage issuers to *think* about what they are doing, any development which even *might* encourage one simply to sign-off on permits is to be viewed with extreme caution. Conversely, it is clearly desirable for an issuer to be able to give his authorisation from a work site or safety store having seen that precautions *are* in place and safety equipment *has* been issued. Probably a decision on this point is one which would have to be taken on a case-by-case basis; in any event, integration of a computerised PTW with plant intranets should be accompanied by additional training for both issuers and acceptors to highlight that additional convenience in no way decreases the regulatory force of the permit or obviates the necessity for physical checks by issuers prior to the permit being issued and, by acceptors, prior to work being commenced.

The HSE has identified the problems attendant on work carrying-over between shifts as especially significant. Integration of a computerised PTW system with a plant intranet might reasonably be expected to eliminate or at least reduce the problem which occurs when a whole new set of personnel must be informed of ongoing works. A computerised system should readily be able both to maintain a list of those people who need to be informed of work-in-progress and inform them electronically of what they need to know; further it would be simple matter to have the system log their acknowledgement of receipt of notification.

Clearly the impact of all the possibilities noted so far will be greatest in improving the safety of the system but it should be recognised that the implications go beyond this. For example, it is clearly desirable that decisions relating to maintenance should not conflict unduly with those relating to production; a computerised system controlling both scheduled and unscheduled maintenance will allow management to exercise a greater degree of control over the running of the plant without compromising safety. Improved control over maintenance procedures should result in less 'down-time' for plant which in turn translates into greater production efficiency and, thence, profitability.

Computer integration and personnel evaluation

As has also already been noted one of the basic purposes of a PTW is to provide a permanent record of what has been done, by whom, when and how. This may be of use if an incident actually occurs in order to determine what went wrong but similarly, such records may be used for a variety of other purposes. One of the basic purposes of the Active Database (ADB) under development at Loughborough is to provide the issuers of permits with incident reports relating to their proposed maintenance task even in the absence of a specific request for this information. In order to achieve this the ADB makes its own assessment of potential hazards based upon the information entered on the permit by the issuer. If the user's assessment of risk differs significantly from that of the ADB the system will augment the chances of reports relating to apparently neglected hazards being presented to the user for consideration.

The immediate purpose of this system is, of course, to alert issuers to hazards of which they are unaware or which they have forgotten, but in the longer term the maintenance of *an archive* of permits may be useful as a check on the adequacy of training of issuers: if, for example the issuers of a permit within a plant commonly reveal a blind-spot with respect to a certain class of hazard, this is an indication that the training is inadequate; similarly if a particular issuer commonly neglects a type of hazard, he may need more training, or if he typically fails to note the presence of a variety of hazards this may be an indication of a mismatch of man with job, or indicate an unacceptable slackness on the part of this issuer.

An additional benefit of maintaining a substantial archive of maintenance records is that these may be susceptible to operational analysis which in turn may lead to improvements in the efficiency of the plant: if the records reveal, for example, that a certain type of equipment is off-line for maintenance a disproportionate amount of the time this may be an indication that the equipment in question should be replaced. A further benefit may be to indicate that specific pieces of machinery are breaking down more often than they should: firms could integrate their maintenance logs with a computerised PTW system in order to highlight recurring problems with individual pieces of equipment to issuers at the time a PTW is applied-for.

Further, the maintenance of substantial permanent records is now, in practical terms required by the HSE who include inspection of a selection of PTWs as part of their routine auditing of plant safety procedures. Although it is not yet a legal requirement that firms maintain a permit system, let alone that this be of any specific type, the general requirement that 'reasonable precautions' are taken is such that any firm failing to maintain a PTW system, complete with records, does so at its own risk. In addition to the benefits already noted a computerised system enjoys those generally cited in support of the paperless office: the saving in time, space and expense are substantial.

Computer integration and stock-control

Further efficiencies might be achieved by the integration of PTW and stock-control/warehousing systems: consider, for example, the case of a breakdown requiring the replacement of a component or components. Before this repair can occur someone must first identify what part needs to be replaced, obtain authorisation for its use, locate it and *only then* perform the repair. The situation is complicated still further by the fact that the required part may *not* be held in stock and must therefore be ordered, or, after a part is withdrawn from stock, a

replacement may need to be ordered, or at least a record made of the part's use. All of this is possible but may require an inordinate amount of effort on the part of a number of staff; should the breakdown occur at night, when most staff are absent, the repair may need to be postponed till the next day. While there are clearly issues of control over stock involved here there is no *technical* reason why a PTW system should not be integrated with common stock-control and warehousing systems, so that the part required may be identified and logged out without undue delay. In practical terms too, most decisions authorising the use of components can probably be made at the level of the permit issuer.

ACTIVE DATABASE SYSTEM DEVELOPMENT

The focus of this half of the paper shifts from the general applicability of computers to the problems of PTW systems to a specific active database of incident reports drawn from the process industries which is currently under development by the Plant Engineering Group at Loughborough University. A particular feature of note is that where possible generic software already in wide distribution has been utilised: the system generates the queries it makes of the database in standard-format Structured Query Language (SQL) while interconnectivity with any standard database package is achieved by using Microsoft ODBC software. The present version of the incident database has been implemented using Microsoft Access; an earlier version was implemented in PARADOX. The use of popular commercial systems enables easy integration of the ADB by users with varying installed system configuartions.

Database Structure and Report Retrieval

As has been noted, a basic problem of current PTWs is that they tend to be uninformative: if an issuer is actually unfamiliar with a hazard no amount of prompting by a permit will serve to remind him; if he is aware of a hazard but does not think to apply his knowledge to a new situation the system will similarly fail. The fundamental goal of the ADB system is to tell workers about hazards of which they may previously have been unaware, or have forgotten, or have otherwise failed to consider, at a time when they can still do something about it.

What allows the ADB to function is the novel arrangement of data according to number of loosely related classification hierarchies rather than by a more traditional single alphabetical list of keywords. These hierarchies, respectively relating to Equipment, Operation, Chemicals, Cause and Consequence together provide a description of the key elements of an industrial incident and together represent a domain description of the chemical-industrial workplace. The significance of this is that it is less necessary to formulate an exact query in order to retrieve information than is required by conventional databases; data is 'loosely' sorted according to the information that appears in the accident report and thematically related information is then stored 'together' at an appropriate level of the various classification hierarchies. An exact query about a particular case will achieve an exact response; a less precise query, however, will still retrieve *appropriate* information, albeit along with some additional information which may not be *precisely* that which is required. In the context of PTW systems, however, a slightly 'fuzzy' view of the problem is actually required: the variety of *notionally distinct* hazards is actually quite limited; what is a matter of almost limitless variation is the way in which these basic hazards may occur in new situations[7].

Let us consider the organisation of data in the ADB. In figure 1 a section of the Causes hierarchy is displayed with the number of reports primarily indexed according to each node being shown in brackets. In this representation *Electrical equipment cause* is shown as a daughter of *Equipment cause* and a parent of both *Short circuit* and *Lack of earthing*. Reports are indexed according to the specificity of information appearing in the text: if an incident occurred due to equipment failure, but no specifics of what type of equipment, or which sort of failure are

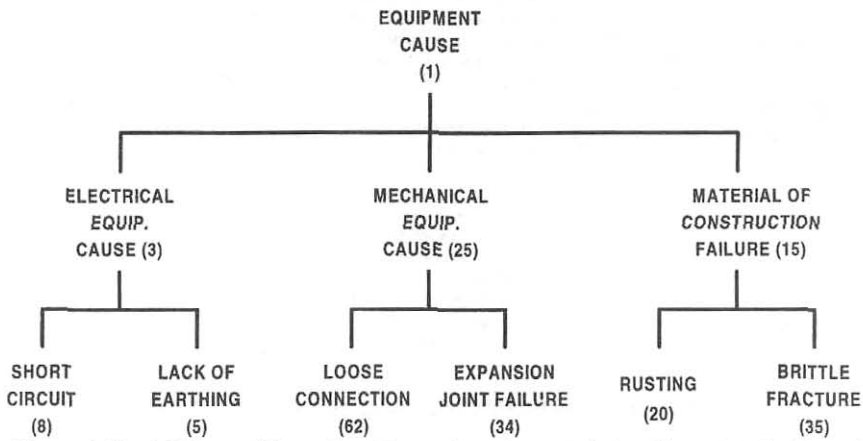

Figure 1: Partial Causes Hierarchy with number of reports indexed/associated with each node.

provided, the report is indexed at a high level of abstraction – further up the hierarchy. If more information is available and it is known, for example, that it was electrical equipment which failed, or that the cause for this failure was a short circuit, the report is indexed at a lower, more specific level. However, since a parent/child link is defined between *Electrical equipment cause* and *Short circuit*, retrieval of related-but-not-identical reports is simplified: if one is interested in cases involving electrical equipment failure then all the children of that node are of potential interest also. To a lesser – but calculable – extent the opposite is also true: interest in failures involving short circuits may make the more general electrical equipment failure of interest also[8].

From this starting point, specific information may be reached by a variety of routes: since every report is indexed under at least four distinct hierarchical heads (primarily these are *Equipment, Operation, Cause and Consequence* with *Chemicals* and *Chemical Properties* possible secondary heads) any report may be accessed by a number of routes. It should be noted, however, that each descriptive acts as a constraint upon the 'hits' achievable by reference to the hierarchy. For example, in Figure 2 each of the various nodes with the exception of *Toxic by skin contact* will result in the retrieval of the report shown; although toxicity by skin contact is a property of Benzene recognised by the system, this characteristic played no part in this incident and hence is excluded from being retrieved. Any combination of the *other* nodes shown in figure 2 would result in this report's retrieval, albeit *some* combinations of nodes might *also* result in the retrieval of a variable number of other more-or-less appropriate reports.

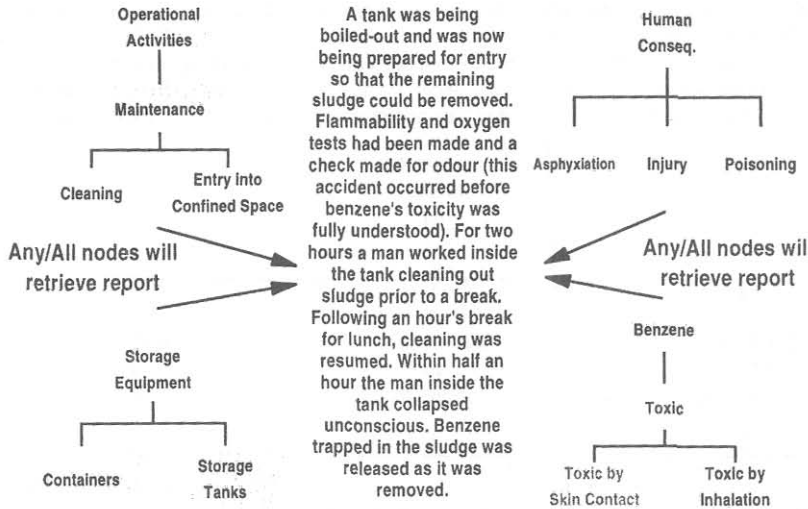

Figure 2: Diagram indicating various routes to retrieve a particular incident report.

Active Database Integration and Permits to Work.

In order for the ADB to function as desired it was necessary to develop a computer front-end in the form of a PTW. In format this is closely based on many existing PTW systems: it was felt that the existing paradigm, despite its various drawbacks, has achieved a fair degree of efficiency overall; in part also it was hoped a familiar format would reassure potential users of the system and minimise the time required for them to familiarise themselves with its use. A specific design goal was that the computerised PTW should be at least as quick and as easy to complete as existing systems. The intent is that the user should complete the permit in a conventional manner and the ADB should then make its determination of the relevance of particular incident reports based on the information so gained without any further action on the part of the user.

Figure 3 shows the first of a number of 'panels' which make up the PTW; the format throughout is the familiar one combining checklists and boxes requiring active completion. In addition to the design principles mentioned above, a 'modular' approach to form design was taken as a result of the HSE finding that firms use different PTW forms for different maintenance tasks. The division of the PTW into a number of panels is intended to improve the logical flow from section to section and facilitate PTW customisation: the choices made by users on the earlier, more general, panels determine which, if any of the later specific panels are presented for completion. Firms may thus enjoy the advantages of permits tailored to individual and current needs without the drawbacks of bureaucratic proliferation.

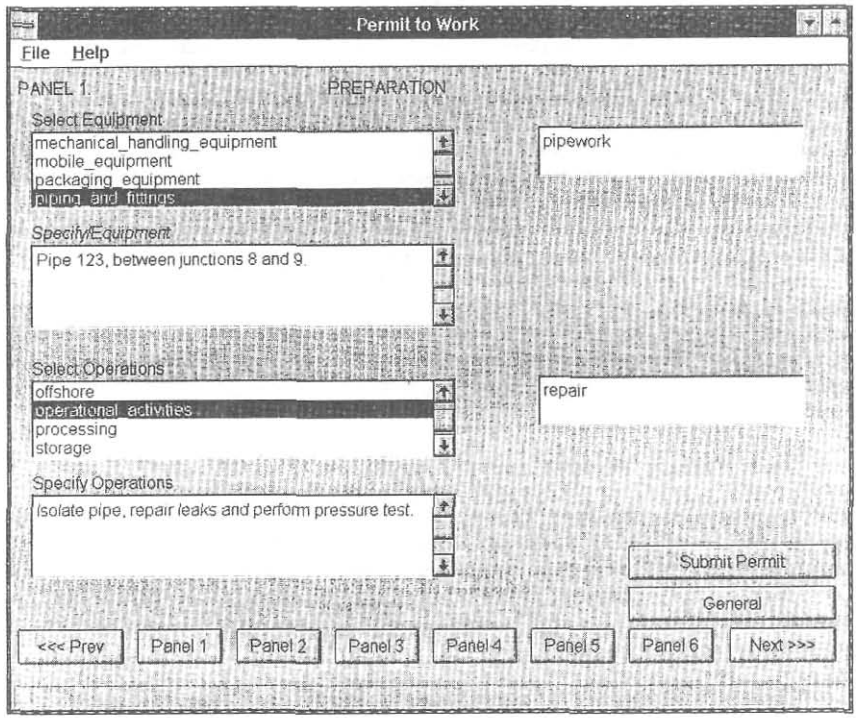

Figure 3: Screen dump of part of Computerised Permit-to-Work: 'Preparation for work: Equipment type and Operations type'.

Appropriateness and 'User Modelling'

One potential problem of the system as it has been presented so far is that it will tend to return too much information rather than too little. The reasons for this are several: as we have seen, the hierarchical organisation of data means that all associated reports will be returned in response to any given query; any which are not desired must explicitly be excluded in one fashion or another. This tendency is exacerbated by a feature of structured taxonomies which has been discovered by experience: the main advantage enjoyed by a hierarchical taxonomy over traditional alphabetical organisations is that proper data placement can quickly be determined from the structure of the taxonomy itself; the drawback is that some data falls outside the pattern prescribed by the taxonomy. Take, for example, an incident involving a solenoid-operated isolation valve which operated too slowly: is this a case involving electrical equipment failure, mechanical equipment failure or safety equipment failure? To what extent can slowness to operate be said to be a 'failure to operate'?

A response to this problem has been to permit incident reports to be indexed by means of multiple descriptives. This makes indexing of data much easier but only does so at the cost of greatly increasing the potential number of 'hits' – with a corresponding degradation of appropriateness of system response. In order to offset this difficulty and re-enhance appropriateness of information retrieval, the system has been developed to accommodate differing needs by different classes of system user, as well as individual needs of individual users. The initial logic guiding this development was the recognition that that plant operators will have different informational needs from those of maintenance personnel and that both will have different needs from those of plant designers. While the former categories of user are likely to require an 'active' database with incident reports being presented without any explicit request being made for them, the latter category probably does not. Further, plant designers are likely to need as detailed as possible an account of an incident to allow them to 'design-out' the possibility of recurrence; conversely, maintenance workers' requirements are accommodated better by a more abbreviated statement of what went wrong together with a statement of what lessons should have been learned. Similarly, plant operators are likely to require a *still more* compressed version of events since their acquaintance with an incident is likely to be made under time pressure as incidents develop.

The necessity for the system to respond differently to different classes of user was further developed by a desire to respond individually to individual users: to prevent information overload, it was decided that a 'cap' should be placed on the number of reports presented to any user at any given time. This cap would vary according to circumstances, and, most notably, in response to what individual users might be expected to know about their own particular situation. If, for example, the job to which the permit pertained was one which is very familiar then less information relating to its hazards need be retrieved; if the job is an unfamiliar one, the need for information is correspondingly greater.

These ends are achieved by maintaining a system-record of the details of past jobs undertaken by each user: if no record exists of a user having undertaken a particular job in the past, then, upon submission of a permit, the system will return the maximum number of appropriate reports, subject only to the arbitrarily imposed 'cap'. If, conversely, the system determines *this* user has performed *that* task several times recently, a much smaller selection of reports – or possibly none at all – will be returned. The intention is that the user not be overloaded with extraneous information and that he should not be bored by seeing again reports that are possibly wearily familiar. Between these extremes, where the system determines *some* degree of familiarity with a job, a less-than-maximum number of reports will be returned. Where possible those reports which are returned will be ones which have not been seen by this user before, or, if this is not possible, are at least those which were reviewed least recently. Figure 4, shows a typical system printout summarising the details entered on a PTW together with report details which were automatically generated.

PERMIT-TO-WORK SECTION A – GENERAL INFORMATION:

A1 - Enter Plant Name: Anytown Chemical Process Plant
A2 - Permit Valid From: 09.00 hrs 11/05/1998 **A3 - Permit Valid Till**: 17.00 hrs, 11/05/1998
A4 - Permit Number: 560 **A5 - Issuer Name**: John Smith **A6 - Acceptor Name**: Joe Bloggs

SECTION B – PREPARATION

B1 - Equipment Selected: Pipework
B2 - Equipment Specified: Pipe 123, between junctions 8 and 9.
B3 - Operations Selected: Maintenance
B4 - Operations Specified: Isolate pipe, repair leaks and perform pressure test.
B5 - Hazards Identified: Fire and Explosion; Gas or Fumes; Heat; Trapped Pressure.
B6 - Chemicals Present: Liquefied Petroleum Gas (LPG)
B7 - Physical Isolation: Physical Isolation IS appropriate
B8 - Method of Isolation Used: Single/double isolation valve closed off and locked.
B9 - Fire Permit: A fire permit IS necessary.
B10 - Precautions Taken: Pipe 123 isolated by valve; valves locked and marked; protective hoods issued; foreman for area informed of work in progress.
B11 - Factories Act/ Chemical Works Regulations: DO NOT APPLY
B12 - Installed Radioactive Source: No installed radioactive source.
B13 - Electrical Isolation: Electrical Isolation NOT APPROPRIATE
B14 - Master Control Sheet: Master control sheet DOES NOT apply

SECTION C – OPERATIONS

C1 - Type of Job: Job is in NO SMOKING area and involves welding/and/or grinding
C2 - Physical Limits of Fire Permit: Area A sections 3 and 4
C3 - Duration of Fire Permit: 09.00 hrs 11/05/1998 till 17.00 hrs 11/05/1998
C4 - Factories Act/Chemical Works Declaration: Not entered/not appropriate
C5 - Precautions Declaration: All the precautions stated in section B have been put in place and checked by me personally.

SECTION D – SIGNING-OFF

D1 - Status of Permit: Permit current

1 of 3 relevant accident report(s) retrieved as follows: **REPORT NUMBER**: 11
CHEMICAL: LPG **EQUIPMENT**: PIPELINE **OPERATION**: HOT WORK
CAUSE: TESTING INADEQUATE **CONSEQUENCE**: NEAR MISS
DESCRIPTION: Welding was being carried out – during shutdown – on a relief valve tailpipe. It was disconnected at both ends. Four hours later the atmosphere at the end furthest from the relief valve was tested with a combustible gas detector. The head of the detector was pushed as far down the tailpipe as it would go; no gas was detected and a work permit was issued. While the relief valve discharge flange was being ground a flash and a bang occurred at the other end of the tailpipe. Gas in the tailpipe 20m long and containing a number of bends had not been dispersed and had not been detected at the other end of the pipe. **LESSONS**: Before allowing welding or similar operations on a pipeline which has or could have contained flammable gas or liquid (1) sweep out the line with steam or nitrogen from end to end; (2) test at the point at which welding will be carried out. If necessary, a hole may have to be drilled into the pipeline.

Figure 4: Summary printout of Permit with associated incident report

CONCLUSION

To conclude, it is clear that the application of computers to the problems of PTW systems promises a variety of benefits ranging from added legibility to the proactive retrieval of information appropriate to the user's situation but which he has not actually asked for. Collectively, these enhancements promise to make PTWs far more effective; hopefully this should go a long way towards improving plant safety – as well as improving business efficiency – in the chemical-industrial workplace. It is unlikely, however, that any system will be able to render maintenance actually *safe*: the HSE has noted that in many cases workers have failed to do what their permits – correctly – told them they should, either considering the completion of a permit as an end in itself unrelated to actual work practice, or for some other reason. Computerising the process is unlikely to change this singularly human pattern of behaviour.

FURTHER WORK

Further work is also under way to improve the appropriateness of information retrieval from the database by applying case-based reasoning techniques to aid the data recovery across the domain hierarchies as well as up and down. Further work is planned to improve co-ordination between related permits as discussed above as well as in the area of automatically informing workers of the status of current maintenance jobs. The authors would welcome an approach from anyone who might be willing to try-out the system described in an operating plant.

ACKNOWLEDGEMENTS

This work is being carried out with the financial assistance of EPSRC grant (GR/K67502) and with the support of ICI and British Gas. P.W.H. Chung is supported by a British Gas-Royal Academy of Engineering Senior Research Fellowship.

REFERENCES

1. Health and Safety Executive – *Dangerous Maintenance*, p. 2, HMSO, London, (1987).
2. Health and Safety Executive – *Setting up and Running a Permit-to-Work System: How to do it,* p. 1, HMSO, London, (1996).
3. Scott S.J. – *Management of safety - Permit to Work Systems*, Major Hazards Onshore and Offshore, p. 171, IChemE, Rugby, (1992).
4. Riley D.B & Weyman A.K. – *A Survey of Permit-to-Work Systems and Forms in Small to Medium Sized Chemical Plant*, Major Hazards Onshore and Offshore II, p. 369, IChemE, Rugby, (1995).
5. Kletz T.A. – *What Went Wrong: Case Histories of Process Plant Disasters*, p. 2, Gulf Publishing Company, London, (1998), 4th Edition.
6. Cullen W.D. – *The Public Inquiry into the Piper Alpha Disaster,* HMSO, London, (1990).
7. P.W.H. Chung, R.E. Iliffe and M. Jefferson – *Integration of an Incident Database with Computer Tools*, Proceedings of IChemE Research Event 1998, 12148 - 12203.
8. P.W.H. Chung & M. Jefferson – *A Fuzzy Approach to Accessing Incident Databases.* To appear in International Journal of Applied Intelligence.