DUST-EXPERT™

DUST-EXPERT Project Board, (E Fergus, E Hoult, G Lunn, G Norton,
R Santon, A Tyldesley, K Wilson,)
Health and Safety Executive, Quay House, Quay Street, Manchester M3 3JB.

DUST-EXPERT is a consultative expert system developed by HSE to assist designers, users, and others in the field of Dust Explosion prevention and protection. It contains guidance, decision trees, a dust properties data base, a new method of estimating the strength of weak vessels, and vent calculation methods. It has been developed under quality assurance to an appropriate software safety integrity level. The exercise has had many unique features for HSE, and the lessons learnt may assist others contemplating any similar system.

Key Words: dust explosions, expert systems

INTRODUCTION

Many materials are capable of burning explosively if suspended as a dust cloud in air. For an explosion to occur, there has to be sufficient dust in the cloud and an effective ignition source. These conditions are possible in a wide range of industries, including chemical, pharmaceutical, metal powder processing, food and animal feeds, and woodworking. In addition, many industries which use pulverised coal as a fuel may have to address the hazards. Guidance on controlling the risk has long combined advice on avoiding the problem altogether and eliminating sources of ignition, while accepting that in many circumstances the risk cannot entirely be eliminated. It often has to be assumed that a dust explosion may still occur, and systems have to be provided to mitigate the consequences.

The technical aspects of control of the dust explosion hazard have received much scientific attention over the years, not only in the UK but in many other countries as well. Much of this has involved large scale experimentation leading to empirical design recommendations. For the practising engineer, finding a way through a maze of advice, and then applying it as it was intended, has become progressively more difficult. The subject is now mature enough, however, for experts to agree (in most circumstances) what best advice actually is. These characteristics mean that the topic can be developed in expert system form, with conclusions drawn from a coherent set of rules.

In 1988 the concept of artificial intelligence in general and expert systems in particular were relatively poorly understood and applied, but efforts were in progress within HSE to investigate possible applications. A feasibility study was set up into the application of expert systems to relief vent design. The project was awarded to Salford University Business Services (SUBSL); it concluded that

- it was feasible to construct systems for dust explosion, gas explosion, and exothermic reactor vent design,
- there would be a viable market for such systems,
- dust explosions would be the recommended first system.

The last conclusion was made because the technology appeared to be best defined and of the right order of magnitude and complexity. The feasibility study itself included the construction of a preliminary prototype, using CRYSTAL, a proprietary expert system shell.

A subsequent project was set up to develop an expert system for dust explosion relief vent design. This was also awarded to SUBSL. The project was set up in collaboration with the British Materials Handling Board (BMHB), which sought and obtained industrial sponsorship from some 30 companies. BMHB set up a project panel with HSE. The development proceeded over a period of 2 years, with frequent contact between the HSE, BMHB, and SUBSL. It concluded with the production of a relatively completed program, using PROLOG (Ref. 1).

At that time the relevance of Quality Assurance (QA) to safety related software was appreciated but the development of QA standards was immature. HSE specialists and lawyers were not prepared to allow the release of the program because the absence of any formal QA might have consequent liability risks. The program had been written largely without any formal specification, or records, other than the minimum required for technical purposes. An edited version, known as the Research Version, was supplied to specialists within HSE and to the BMHB industrial sponsors for restricted use, and remains in use.

HSE had spent considerable research funds on the work to that time, and a study was set up to consider the options available. These ranged from a cessation of effort to the full repeat of the development under QA. An independent review of the program supported the view that it was not suitable for release without considerable effort. Because of the need to acquire expertise in the field, concurrent with the preparation of software safety integrity standards, and the technical benefits that were seen as probable from the development work, HSE took the decision to proceed with the project.

SAFETY INTEGRITY

A safety-related system should be developed in a systematic way which ensures that all safety requirements are identified and achieved.

A useful concept here is that of "functional safety", which is the ability of the safety-related system to carry out the actions necessary to achieve or to maintain a safe state. These "safety functions" are to be distinguished from any other functions needed to make the system fit for its intended purpose. For example, in the case of the DUST-EXPERT advisory system which must not give unsafe misleading advice, the safety functions would address the integrity of the dust properties database and the observance of calculation constraints, while non-safety functions would include speed of response, interface ergonomics, etc.

Functional safety is addressed by the International Electrotechnical Commission Draft Standard 1508 (Ref. 2). The IEC 1508 approach is fundamentally based on the concept of risk and on the integrity of the precautions which are needed to reduce the initial risk to an acceptable level. It uses a "Safety Lifecycle" (analogous to the well-known software development lifecycle) which systematically carries out hazard and risk analysis, identifies safety functions which must be provided by the system, defines four quantified levels of integrity of the necessary safety functions, and (for software-based systems) recommends specific engineering techniques which are generally acknowledged to achieve the required software safety integrity level (SIL).

A *quantified risk assessment* was carried out, taking into account the estimated frequency of explosions in UK dust handling plant, and the known characteristics of practical construction and maintenance of explosion relief equipment. The aims were:

- to assess the risk that a dangerous explosion would arise from a failure of the current manual method of designing explosion relief equipment,
- to set an appropriate safety integrity level for the software-based DUST-EXPERT calculation.

The analysis showed that the influence of a wrong calculation arising from software failure made a relatively small contribution to the overall risk of dangerous explosions. It was concluded that the least demanding IEC 1508 integrity level (i.e. SIL 1, corresponding to a failure probability of between 0.1 and 0.01) was a good standard of safety performance for DUST-EXPERT, given the specific factors of the construction and use of dust explosion protection equipment in the UK. In fact, the software methods which were used to develop DUST-EXPERT correspond to the more demanding SIL 2 level (i.e. failure probability of between 0.01 and 0.001) of IEC 1508. The safety performance of the DUST-EXPERT software therefore significantly exceeds the minimum requirement.

SPECIFICATION

It was appreciated that the preparation of a Software Requirements Specification (SRS) was essential to the envisaged development, and this work was carried out with the assistance of the Applied Information Engineering Department of Lloyd's Register of Shipping. The framework of the specification was based on IEEE 830 (Ref. 3). The availability of the Research Version, (itself based on the earlier CRYSTAL version), and the expertise that had gone into it were significant to the preparation of the SRS. The 400 page document took 2 years to complete under the control of a Project Board. A particular criticism of the earlier work was that its "ownership" was unclear, and HSE have set up and maintained a Board with full responsibility for all aspects of the work, including technical content and contractor management. Project Board members were chosen for their respective expertise, both technical and administrative. This approach has facilitated decision making and enabled a coherent strategy to be evolved and maintained. At different stages some members were more or less heavily involved than others, but all retained their feel for the project; they saw their contributions in relation to the project objectives overall rather than in isolation. At the time this was an innovative approach but its success means that it will be considered for other developments of this type.

DUST-EXPERT has broken new ground in many other ways. It was the first HSE research project to be tendered across Europe under the terms of the EC Public Services Procurement Directive (Ref. 4). This required longer time scales than tendering in the UK alone but it did ensure that the net for a suitable contractor was spread as widely as possible.

KNOWLEDGE BASE

Text Guidance

DUST-EXPERT contains a substantial module of text guidance. This is not limited to advice on explosion venting, but covers comprehensively the prevention of and protection against dust explosions. The user can, for instance, explore the sequence of testing necessary to establish the hazard and level of risk. The range of precautions against dust explosions is also described in detail.

Much of the text has been taken from The Institution of Chemical Engineers' publication, Dust Explosion Prevention and Protection, Part 1 - Venting (Ref. 5). Where new information has become available since 1992, it has been included. This text information is collected under five main headings:

- Explosibility Tests (e.g. 20 l Test Vessel; Modified Hartmann Tests)
- Explosion Violence Factors (e.g. Particle Size; Turbulence)
- Precaution Techniques (e.g. Inerting; Containment)
- Vent Closures (e.g. Explosion Doors; Installation and Maintenance)
- Venting of Specific Plant (e.g. Filters; Spray Dryers)

Each main heading is divided into specific topics. Some of the text is available as context sensitive help screens, while other parts are available through the normal WINDOWS™ hyper-text help system.

Decision trees

Engineering design looks at a range of options before examining a few in great detail. It also makes the necessary calculations for a full costing. The decision trees in DUST-EXPERT take the user systematically through the essential questions that should be addressed at the preliminary stages of plant design. They form a check list that help the user explore all the various approaches to plant safety. Decision trees are provided for control of ignition sources (which will always be relevant) together with the alternative methods of protection of explosion containment, plant venting, explosion suppression and inerting. All the trees in DUST-EXPERT present the user with a series of questions, needing yes/no answers. Extensive additional information is provided in help screens for every question, and the final output of any interrogation of the trees is text advice, appropriate to the answers provided.

Database

Many factors influence the explosion characteristics of individual dusts, such as particle size distribution, moisture content, and any surface coatings or inert contaminants. HSE has long advocated that testing of the actual dust in a plant is the best way to ensure safe design. We cannot realistically, however, expect every small bakery to retest flour or sugar, and neither can we ignore published data from reputable sources. Doubts were expressed at an early stage about advising users to design explosion vents on the basis of published data. The earlier BMHB Board and the current Board felt that it was better to incorporate a data base where the samples were adequately characterised, but which left the user to make a judgement about how well information from the database matched the characteristics of his product.

The confidence that one can have in published data increases with the number of samples tested. For instance, a value for the explosibility parameter K_{st} based on testing one sample of an obscure synthetic organic chemical may be rather suspect if, for example, the particle size distribution is not the same as that found in the plant in question. On the other hand using a value derived from the results of testing 50 samples of wood dust is probably highly reliable. These are value judgements that cannot conform to all the rules demanded by an expert system; this part of DUST EXPERT requires some intelligent input from the user.

Because taking a wrong value for explosion properties will invalidate all subsequent calculations for explosion venting, great care has been taken to ensure accurate fault free transcription of the data from the original source. The majority of the data comes from a German source (Ref. 6). To improve our confidence in the data, we have queried a several specific results that seemed surprising; we have been assured that they are correct. They serve to highlight the large variation sometimes shown between apparently similar samples.

The data base contains 1200 sets of data relating not only to explosion properties, but also to the ignition temperatures of a cloud or layer, and minimum ignition energy of the dust. All this data is relevant to assessing the hazard in a process plant, but there are no rules to inform a user how the data should be applied. Consequently, the system again requires the user to apply information with understanding. A computer cannot mimic the decisions of an expert. This is particularly important when there is no certainty that a group of experts would reach consensus on their conclusions. Expert system technology is not yet so sophisticated that it can deduce the rules for itself.

The data base contains a section for user's data to be stored. It has conventional search facilities. The full range of data within 17 fields can be viewed if required. The selected dust properties can be automatically stored and transferred for use in subsequent calculations .

Venting Calculations

DUST-EXPERT contains routines which, calculate the area of an explosion vent. Where the mathematics permit, other variables such as reduced explosion pressure can be selected as output. Routines for calculating the effect of a vent duct, the reaction forces produced by a vented dust explosion and the extent of the fireball external to the vent are included. All the calculations are adapted from published guidance. Where the published guidance is in the form of equations, these equations have been used. When the guidance is available only in graphical form, curve fitting routines have been used to generate functions which reproduce the graphical guidance to a satisfactory accuracy.

The vent calculation methods have been divided into Groups, as follows

Compact Vessels

Basic Methods
well validated routines for compact vessels.

Alternative Methods
methods for compact vessels which are little validated or are used in special circumstances.

High Turbulence Methods
methods for circumstances where high turbulence can be expected.

Fluid Bed Dryers
ad hoc methods applicable specifically to some fluid bed driers.

Elongated Vessels

Elongated Vessel Methods
one set allows calculation of the allowable vessel height when the entire roof area is used as a vent; a second set calculates the vent area.

Ducts and Pipelines

Ducts and Pipeline Methods
estimate the spacing along pipelines of vents equal in area to the cross-section of the pipeline.

Buildings

Building Method
a routine which calculates the vent area for buildings containing dust handling equipment or where an extensive dust cloud may develop.

Other calculations

Reaction Force
a method for calculating the reaction force from a vented explosion.

Safe Discharge Area — a method for calculating the extent of the vented flame.

Vent Ducts — a method for estimating the effect of vent ducts on the pressures developed by the vented explosion.

As well as the calculation methods , there is comprehensive help given as screen text. This is in two forms:

- general help which guides the user through the Group and Methods structure.
- help which is applicable to each specific method and gives pertinent information about the application of the method and the limits to its applicability. Each variable has its own help text which can be accessed when the variable is called up by a calculation method.

Each method has a built-in set of constraints applied to each relevant variable, for example vessel volume, or K_{st} value of the dust. These constraints are taken from published guidance and the methods cannot be used outside them. In some methods they also determine which of a number of mutually exclusive options will be used. For instance, for a given design of elongated vessel, the equations for calculation of the vent area alter, depending on the S_t Group of the dust. A screen dump from the module is attached as an example (Fig. 1).

The routine which calculates the effect of vent ducts on the pressure in a vented explosion is the method used in The Institution of Chemical Engineers' publication, Dust Explosion Prevention and Protection, Part 3 (Ref. 7).

Estimation of The Strength of Weak Vessels

While there has been considerable research into dust explosions, very little work has been undertaken to help the designer of plant that must withstand those dust explosions.

However, two different design philosophies have developed:

- explosion pressure resistant equipment which is designed to withstand the expected explosion pressure without being permanently deformed.
- explosion pressure-shock resistant equipment, which is designed to withstand the expected explosion pressure without rupturing, but allowing permanent deformation.

Pressure-shock resistant plant usually has the advantages of being much lighter in weight and cheaper to produce, but because it relies on large deflections and plastic deformation, the analysis of such plant has previously been expensive and time consuming. The strength of weak plant module in DUST-EXPERT goes some way towards making the design of pressure-shock resistant much more practicable.

The method employed in DUST-EXPERT divides the structure under consideration into a number of commonly found structural features such as flat plates, shells, intersections and different joint types. For each feature DUST-EXPERT calculates a pressure rating. The rating for the whole plant is then taken as the lowest calculated pressure. The method allows the identification of the weakest part of the plant and enables designers to consider the effect of different values of parameters, such as material thickness, on the overall rating.

Considerable research work has gone into developing equations for a number of structural features. A special purpose test rig has been developed which allows features to be subjected to pressure rises typical of vented dust explosions. This has enabled the type of damage sustained by different features to be established. Theoretical analysis and finite element analysis have both been used to develop equations which, wherever possible, have been validated by data from this experimental work (Refs. 8, 9). The essentials of this work were presented at a seminar run by HSE in Sheffield in May 1996.

Currently, DUST-EXPERT contains design equations for the following features,

circular plates
rectangular plates
cylinders
cones
hemispheres

fillet welds
seam welds
butt welds

longitudinal bolted joints in rectangular vessels
longitudinal bolted joints in cylindrical vessels
end plate bolted joints in cylindrical vessels
hoop bolted joints in cylindrical vessels

square duct/square plate intersections
square duct/circular plate intersections
circular duct/square plate intersections
circular duct/circular plate intersections

Many of the feature equations are pressure/strain relationships. The normal elastic limit for engineering materials is of the order of 0.1% strain. However, because pressure-shock resistant design allows permanent deformation, this limit can be extended considerably. The typical limit that DUST-EXPERT uses is 2%, which allows for substantial deformation, but still allows a good margin of safety on rupture.

Input of information is very straight forward; the user identifies which features are present in the piece of plant under consideration and as each is identified a graphic is displayed showing what geometric parameters have to be input. The user is then prompted for the required information. Materials data is obtained from a database of commonly used engineering materials which can be extended by the user. A screen dump from the module is attached as an example (Fig. 2).

The user is required to use engineering judgement to take account of the interdependence of some features, and to allow for features specific to the vessel, such as doors or special strengthening. Values of plant strength can be automatically transferred to the vent calculation module of DUST-EXPERT as reduced explosion pressure (P_{red}).

It is hoped that future work will extend the range of features for which design equations are available, and that the work will receive recognition in a harmonised European Standard.

USER INTERFACE

When drafting the SRS, one of the areas which the Board found most difficult to set out in detail was the user interface. Reference was made to general guidance in ISO 9241, (Ref. 10), but the Board felt that a successful software house was likely to have more appropriate expertise in designing a good interface . This is partly because the bounds of technical feasibility are changing quickly, but also because it was not intended to limit the specification by insisting on a Windows type of display.

The PRINCE rules on management of IT projects stress the need for formal involvement of future users in system design. This was felt to be an area in which potential users could make a particular contribution so the specification included a requirement to develop a dummy interface which would be tested and developed with up to 3 iterations.

The dummy interface, with a fragment of the calculation system and a decision tree, was tested early in the development by a group of HSE users who had not been involved in writing the specification. An improved interface was then created which addressed comments made; this was tested by an engineer from outside HSE who was familiar with the subject matter. After this there was confidence that the user interface was suitable for the target audience - essentially, individuals who are broadly familiar with using modern computing packages, but who would probably use DUST EXPERT relatively infrequently, and certainly not daily.

In addition to the functionality necessary to support the knowledge base described above, the system has conventional file and printing facilities, logging ability, and an explanation function to allow users to determine the reason, for example, that a particular calculation method has failed because of constraints.

SYSTEM DEVELOPMENT METHODS

Specific quantitative and qualitative factors which justify confidence in the safety performance of DUST-EXPERT were documented explicitly as part of the justification of DUST-EXPERT software quality. It is a reflection of the current state of software technology that qualitative factors are significant in this argument. The major factors include:

1. use of verified and peer-reviewed research data on dust combustibility and on weak-vessel strength;
2. detailed software requirements specification, incorporating extensive experience from earlier prototype developments;
3. re-specification of requirements using the formal Vienna Development Method (VDM), machine checking of the self-consistency of the VDM, and hand-proof of software safety properties;
4. software HAZOPs on the VDM;
5. semi-automatic generation of efficient Prolog from the VDM in a clearly-defined manner;
6. white-box testing of Prolog to 100% statement coverage;
7. black-box statistical testing of the integrated system using an executable VDM specification as an oracle;

8. final acceptance testing of integrated system to a pre-specified test plan;
9. technical reviews and audits of quality of deliverables by people independent of the immediate development work;
10. automated tool support for the development process including configuration management;
11. assessment of the impact of off-line development tools on the final system safety integrity;
12. documented competency of development staff.

DUST-EXPERT was developed under a formal ISO 9000-3 (Ref. 11) "TickIT" quality management system for software. The use of TickIT addresses those issues which are of particular relevance in software development:

- requirements specification,
- tools and techniques,
- configuration management and change control,
- validation and verification.

For all practical purposes, developing a major software system such as DUST-EXPERT requires the use of off-line support and development tools (e.g. specification tools, language translators, testing tools) and the inclusion of pre-written software packages (e.g. operating system, function library, graphical user interface) in the final system. It is currently impractical to specify the behaviour of such pre-written software components with the same degree of precision as (say) the hardware components of a mechanical system. The software tools and the pre-written software components therefore introduce some uncertainty into the behaviour of the final DUST-EXPERT program. This uncertainty must be taken into account as a quality assurance issue in order to have acceptable confidence in the safety integrity of DUST-EXPERT.

The current state of software quality assurance obliged the Board to rely significantly on qualitative justifications of pre-written software (usually relating to the process by which they were developed) and to have confidence that due care and attention was given by suitably competent people in developing that software. Where practical, this qualitative justification can be complemented by quantitative testing of the observable software behaviour of pre-written software. The effort spent on the overall assessment of pre-written software should be commensurate with the criticality of that software. Thus, faults in the word-processor which is used to write the requirements specification are of little concern, while faults in the VDM tool which checks the internal consistency of the formal requirements specification are of much greater concern.

The major tools and pre-written software packages which are used in DUST-EXPERT were selected to ensure that their impact on the DUST-EXPERT safety integrity can be assessed and justified. This assessment is explicitly recorded in project documentation. Examples include:

1. The IFAD software toolset supports the development of formal specifications in VDM. In DUST-EXPERT the IFAD toolset is used to verify the consistency of the VDM specification. The Institution for Applied Computer Science, Copenhagen, the

suppliers of the IFAD toolset operate a strict system of configuration management. The toolset is very thoroughly checked for correctness before release to customers, resulting in an exceptionally small number (approximately 20) of known bugs considering the size and complexity of IFAD. The suppliers also maintain a list of registered users, who receive a complete IFAD fault history to alert them to possible VDM analysis errors. Finally, experience of IFAD operation gives high confidence that any currently unknown IFAD fault is very unlikely to mask a VDM specification error.

2. DUST-EXPERT is required to run under Microsoft Windows 3.1, which is known to be far from error-free. However, the DUST-EXPERT developers have gained access to the Microsoft problem reporting service (the Microsoft Developers Network) which documents known problems in Windows 3.1. Given the widespread use of Windows 3.1, it is very unlikely that any operating system error which could introduce gross errors into DUST-EXPERT remains unknown to the DUST-EXPERT developers.

3. DUST-EXPERT is implemented in Prolog, using the LPA development toolset which provides a function library suitable for implementing a Windows-based user interface, and for supporting the specialised functions needed for constraint-based logic needed in DUST-EXPERT. LPA Prolog conforms to the ISO standard definition of the language. It is exceptionally well documented, and has been used satisfactorily in a significant number of demanding developments.

Using the above approach, it is very unlikely that there is a significant risk that a fault in any of the support tools or pre-written software components could prevent DUST-EXPERT from achieving its required safety integrity.

The informal software requirements specification for DUST-EXPERT was written after extensive practical experience of earlier prototype developments. The experience and insights resulting from using these prototypes was carefully recorded in the informal software requirements specification of DUST-EXPERT, thus providing a sound basis for both the development and the acceptance testing of the final software.

The informal DUST-EXPERT software requirements specification included dust explosibility data and calculation methods which had been openly published and peer-reviewed, thus justifying a very high confidence in their scientific accuracy. One DUST-EXPERT requirement of particular significance was that the development should produce a system both for the specific calculations of dust explosion relief, and for a reusable shell containing the basic facilities to support a future family of advisory systems analogous to DUST-EXPERT.

The informal specification was rewritten as a formal VDM specification, using a subset of the language constructs which can be executed. The VDM specification was then executed by the IFAD VDM-SL tool, using a suite of test cases which covered the functionality expressed in the original informal requirements specification. This demonstrated that the informal requirement had been correctly captured, and that the specification was logically self-consistent.

A technique specially developed by the DUST-EXPERT developers was that used to automatically translate the executable VDM constructs into corresponding executable Prolog code, making use of the library functions which the LPA Prolog system provides for producing knowledge-based systems to run under Microsoft Windows 3.1. Where the automatic translation resulted in unacceptably inefficient Prolog, the Prolog was hand-tuned. Prototype implementations were made available to trial users, as noted above, as early as possible to enable them to evaluate the interactive user interface. The users' suggestions were taken into account when finalising the interface.

The final DUST-EXPERT software was subjected to a statistically significant number of numerical test calculations (around 10,000 distinct cases) in order to justify with a confidence of 99% that the required functional Safety Integrity Level (SIL) had indeed been achieved. This extensive numerical testing was made practical by the use of a software "test harness", a tool which takes charge of the user interfaces of DUST-EXPERT, submits numerical test cases, and notes the response from DUST-EXPERT. Often some manual intervention is needed to decide whether the response of the program under test is correct or wrong, but DUST-EXPERT permitted an elegant and very effective alternative. The formal VDM specification was instead symbolically "executed" by the IFAD analyser, and the IFAD result was then compared with the DUST-EXPERT result. This automated IFAD "oracle" both greatly reduced the developers' testing burden, and also gave a very high confidence that the implemented DUST-EXPERT conformed to the logic of its formal specification.

MARKETING AND LEGAL ISSUES

HSE produced DUST-EXPERT primarily for internal use. However, at the early stages, the Board recognised that others would benefit from access to the program. In keeping with broader objectives, the decision was thus taken to look at the possibility of marketing and selling the software. In seeking a route to the market, HSE decided to work with other organisations who had more experience of selling software. The Board approached The Institution of Chemical Engineers as a logical agent because they were already publishers of associated guidance and training material. It is hoped that DUST-EXPERT will, therefore, be available within HSE and also for purchase through the IChemE.

DUST-EXPERT has been a unique exercise for HSE. As a regulatory authority, it has published traditional written guidance but has not been innovative in software development. The exercise has given a practical focus to discussions on liability for safety related software; it continues to be innovative as considerations of international sales, for instance, are explored.

It is essential to ensure that any such product is protected against both criminal and product liability and civil negligence liability charges. This protection is put in place in a number of ways, including: product development to an approriate level of quality assurance in accordance with a conservative estimate of safety integrity level; peer review of the knowledge at all stages; development supervised by an identifiable Board of Management; use of appropriate warnings against mis-use and other hazards, both within the program and in the associated documentation. All these factors have been taken into account in the development of DUST-EXPERT.

The system is designed always to give best technical advice. HSE Inspectors often find that plant has been installed to lesser standards, but in practice only reasonably practicable improvements are required. There is often a difference between legal minimum standards and the best technical advice. DUST-EXPERT gives the latter and no indication of the former.

FUTURE DEVELOPMENTS

One of the advantages of a program such as DUST-EXPERT, (in comparison with conventional written guidance), is the relative ease with which new knowledge can be incorporated. Assuming that there is an accurate user registration base, there is the added assurance that this knowledge can be included in the version held by all users. It is HSE's intention to update the system as and when appropriate new data is available, while maintaining the criteria of peer review and publication acceptability for such data.

As a result of the development of DUST-EXPERT, HSE is in the position of having a *Quality Assured expert system shell which can be populated with knowledge from other* appropriate disciplines. Whilst the resources required for any second or subsequent system to be completed would be reduced by the use of this shell, the resources required to prepare the knowledge base as a software specification alone are significant. Experience over the first years of operation will determine events, but it is hoped and intended that subsequent systems will appear if the experience is satisfactory. As CD technology advances, it is also envisaged that a package that could include video, training, and text as well as an expert system might be viable.

CONCLUSIONS

The project has provided many lessons over the 8 years of its development some of which are summarised below. These may be self evident in retrospect, but they were nevertheless hard learnt and are believed to be worthy of confirmation:

1. The knowledge base to be captured should be large enough to justify the effort involved, but restricted to avoid excessive cost.

2. At least one and more probably two stages of prototyping are required prior to the preparation of an adequate specification.

3. The project must be under the control of a muli-disciplinary group with collective responsibility, and defined individual responsibilities for every aspect of the development.

4. Safety Integrity Level can and should be defined following independent quantified risk assessment.

5. A fully detailed formal software requirements specification must be prepared, and changes to it during software development must be minimised.

DUST-EXPERT has been developed over recent years to these rules and will represent a significant step in the production and presentation of guidance by HSE.

REFERENCES

1. Santon, R. C., 1992, "An expert system for the design of dust explosion relief vents", 7th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Taormina, Italy, 3: 152.

2. Draft International Electrotechnical Commission Standard 1508, 1996 "Functional safety of electrical/electronic/programmable electronic safety related systems", 65A/179-185/CDV, British Standards Institution.

3. IEEE Guide to Software Requirements Specifications, The Institute of Electrical and Electronic Engineers, Inc., 1983. (American National Standard ANSI/IEEE Std 830-1984, Approved July 1984.)

4. EC Public Services Procurement Directive, (The EC Services Directive) (92/50/EEC).

5. Lunn, G. A., 1992, Dust Explosion Prevention and Protection, Part 1, Venting (2nd Edition), The Institution of Chemical Engineers.

6. Brenn-und Explosions-Kenngrößen von Stäuben, BIA/BVS, Erich Schmidt Verlag, August 1987, HSE Translation No. 145131.

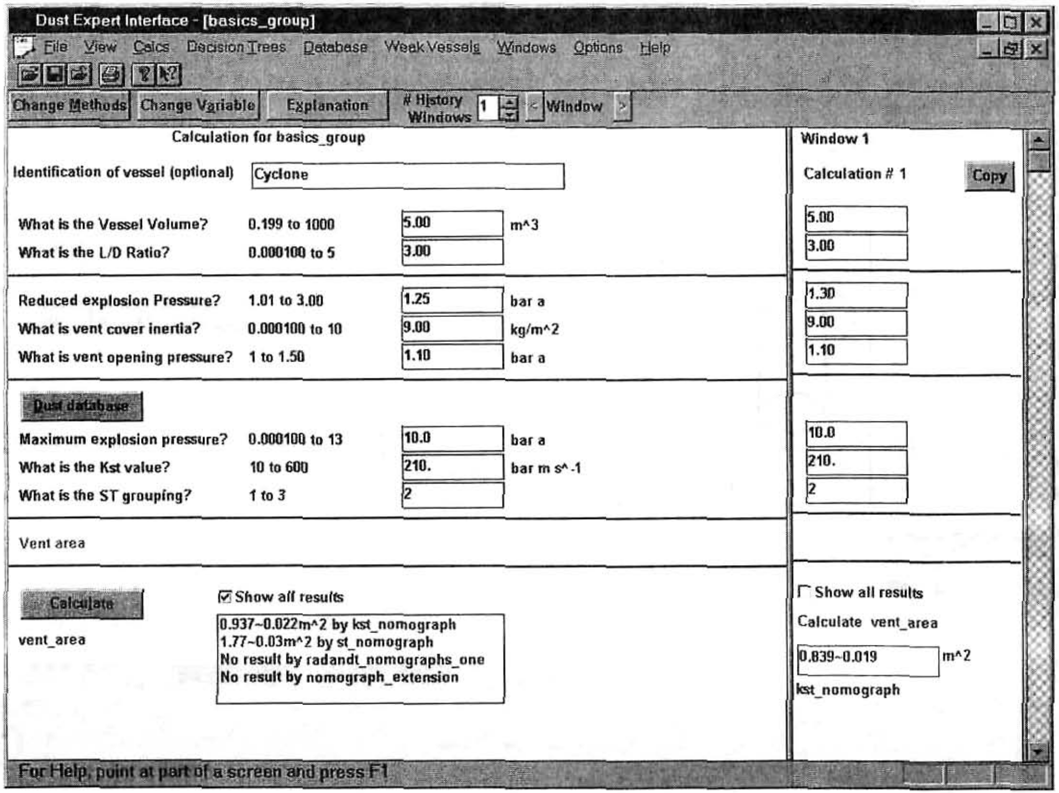
7. Lunn, G. A., 1988, Dust Explosion Prevention and Protection, Part 3, Venting of Weak Explosions and the Effect of Vent Ducts, The Institution of Chemical Engineers.

8. Pilkington, D.F., Platt, G., and Norton, G., 1994, "Design and development of a rig for the pressure testing of weak vessels and subsequent work relating to the strength of flat plates", Hazards XII, European Advances in Process Safety, 57-74.

9. Norton, G. Pilkington, D.F., and Carr, J.B., "The strength and mode of failure of a square duct entering a square plate under internal pressure, by experiment, classical and non-linear finite element analysis", Hazards XII, European Advances in Process Safety, 75-90.

10. ISO 9241: 1992 (BS EN 29241: 1993), "Ergonomic requirements for office work with visual display terminals", British Standards Institution.

11. ISO 9000-3: 1991 (BS 5750 Part 13: 1991), "Guidelines for the application of ISO 9001 to the development, supply and maintenance of software", British Standards Institution.


Dust Expert Interface - [basics_group]
File View Calcs Decision Trees Database Weak Vessels Windows Options Help
Change Methods
Change Variable
Explanation
# History Windows
Window
Dust database
Calculate
Copy
For Help, point at part of a screen and press F1

Calculation for basics_group

Identification of vessel (optional) Cyclone

What is the Vessel Volume?	0.199 to 1000	5.00	m^3	5.00
What is the L/D Ratio?	0.000100 to 5	3.00		3.00
Reduced explosion Pressure?	1.01 to 3.00	1.25	bar a	1.30
What is vent cover inertia?	0.000100 to 10	9.00	kg/m^2	9.00
What is vent opening pressure?	1 to 1.50	1.10	bar a	1.10
Maximum explosion pressure?	0.000100 to 13	10.0	bar a	10.0
What is the Kst value?	10 to 600	210.	bar m s^-1	210.
What is the ST grouping?	1 to 3	2		2

Vent area

vent_area

☑ Show all results

0.937~0.022m^2 by kst_nomograph
1.77~0.03m^2 by st_nomograph
No result by radandt_nomographs_one
No result by nomograph_extension

Window 1

Calculation # 1

□ Show all results

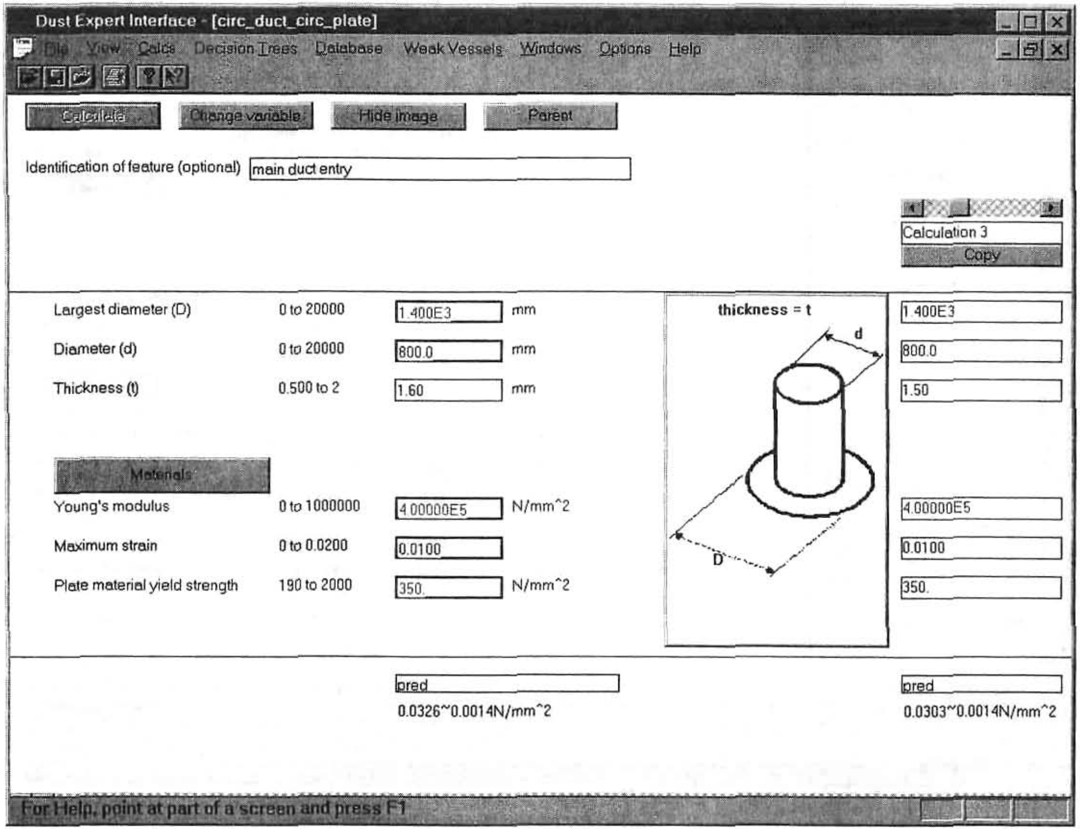
Calculate vent_area

0.839~0.019 m^2

kst_nomograph

FIG 1

DUST-EXPERT SCREEN , VENT CALCULATION



Dust Expert Interface - [circ_duct_circ_plate]
File View Calcs Decision Trees Database Weak Vessels Windows Options Help
Calculate
Change variable
Hide image
Parent
Copy
Materials
thickness = t
d
D
For Help, point at part of a screen and press F1

Identification of feature (optional) main duct entry

Calculation 3

Largest diameter (D)	0 to 20000	1.400E3	mm	1.400E3
Diameter (d)	0 to 20000	800.0	mm	800.0
Thickness (t)	0.500 to 2	1.60	mm	1.50
Young's modulus	0 to 1000000	4.00000E5	N/mm^2	4.00000E5
Maximum strain	0 to 0.0200	0.0100		0.0100
Plate material yield strength	190 to 2000	350.	N/mm^2	350.
		pred 0.0326~0.0014N/mm^2		pred 0.0303~0.0014N/mm^2

FIG 2

DUST-EXPERT SCREEN , STRENGTH ESTIMATION