SAFETY ISSUES AND THE YEAR 2000

Richard Storey
Allianz Cornhill International, 32 Cornhill, London EC3V 3LJ

Industrial insurers and their clients are increasingly becoming aware of the potential for both property and business interruption losses associated with the millennium bug. This paper is based on the advise which Allianz is currently giving to insured to help minimise exposure to the millennium bug. The paper starts off by describing the nature of the problem along with the types of computer controlled systems which can be affected. Subsequently different loss scenarios are reviewed along with the near disastrous consequences which can follow from a lack of computer based control. The paper aims to provide a framework which allows manufacturers to plan for, and rectify, problems associated with the millennium bug. Ultimately, the advise in the paper aims to reduce the potential for both human and financial loss at manufacturing facilities.

Keywords: millennium bug, Y2K, embedded chips, compliance programme

INTRODUCTION: WHAT IS THE MILLENNIUM BUG

The millennium bug or Y2K problem arises from the potential inability of computer systems, including embedded chips, to recognise correctly the year 2000 as well as other dates both prior and subsequent to the turn of the century. The inability of computer systems to recognise the year 2000 correctly could cause computer systems to malfunction or fail completely resulting in a multitude of serious consequences.

The reason for the possible failure is that until very recently computer programs used computer code which represented year dates as two digits rather than four. For example the year 1963 is encoded as 63 and the year 1901 as 01. The problem occurs when the year 2000 is represented as 00 which may be confused with the year 1900 (or any other century) which is also encoded as 00. Another problematic date is 9th September 1999 which will be encoded as either 99 or 9999 which is often used as a termination sequence within blocks of computer code. Some systems may also not recognise that the year 2000 is a leap year.

Although technically the problem is not difficult to solve, the scale of the problem is enormous due to the reliance of modern society on computer systems. It has been estimated by American computer researchers that the global cost of fixing the problem could be as high as $600 billions US Dollars. Possibly of even more concern is the lack of competent human resources to tackle the problem and the dwindling timeframe available for rectifying any problems.

Allianz Cornhill therefore believes that all companies need to urgently review their year 2000 exposures and take appropriate remedial action to ensure that non-compliant systems are updated. The guidance provided within this paper is aimed at helping companies develop an effective framework for approaching and tackling the year 2000 problem. It is certain that some systems/operations will fail and as such compliance is therefore largely a damage limitation exercise.

What sort of equipment could be potentially affected?

The answer to this is a wide range but in general any equipment containing micro processors will be potentially affected. More specifically a non-exhaustive list would be as follows:-

- Any computer software used within PC and mainframe systems including operating system software
- Security and access control systems
- Alarms including fire alarms
- Process control equipment
- Programmable machinery (including equipment with embedded chip systems)
- Communication systems
- Lifts and other building services equipment
- Bar coding equipment
- Safety critical shutdown systems (major implications for human safety)
- Financial, production scheduling and project planning systems.
- Navigational and satellite positioning systems
- Equipment and machinery testing and monitoring systems

What are the possible consequence of a Year 2000 computer failure?

This is a very difficult question to answer as it will depend on numerous factors including the type of business operations conducted and the degree of reliance of a company on computer systems.

Again a non-exhaustive list of the general consequences is as follows:-

- Computer systems may malfunction or simply shutdown completely
- Production lines may stop or product with an incorrect specification may be produced.
- Alarm systems may fail (both fire and burglary)
- Safety critical systems may fail or malfunction resulting in liability claims
- Financial systems may collapse or malfunction
- Stock control systems may fail
- Building services (heating, cooling, lighting) may malfunction
- Communication systems may fail and associated billing systems crash
- Networked computer systems may not be able to 'talk'
- Supplier and customer chains may breakdown
- Port cargo management systems may fail
- Alignment and navigational systems may cease to operate
- Machinery control may be lost
- Valuable information may be lost

More specifically, with respect to the safety of manufacturing operations such as process plant, possible consequences could be:

Fire

- Failure of computer controlled fire detection systems to recognise fire and raise appropriate alarms. This includes the failure of detection systems to notify remote monitoring stations of alarm conditions

- Failure of computer controlled fire extinguishing systems (such as gaseous or foam systems) to extinguish and control fire

- Fires resulting from process control failures such as overheating of reaction vessels (from loss of coolant), electrical system malfunctions, run-away chemical reaction due to unexpected mixing of reactants, inappropriate handling and processing of flammable liquids

Explosion

- Process control failures resulting in overheating, electrical malfunction, high flammable vapour or dust concentration build-up, failure of monitoring and /or ventilation systems

- Failure of explosion suppression and explosion mitigation systems.

Chemical release

- Release of solid, liquid, or gaseous reactants and/or products into the environment

Nuclear contamination

Release of nuclear material into the environment or reactor meltdown scenario

Equipment start up

- Rotating or other mechanical equipment which starts without warning

- Equipment which is electrically energised without warning

Product spoilage and contamination

- Manufactured with incorrect specification, contaminated or spoiled due to changes in storage conditions.

On a general note, it is clear from the above that there are serious potential consequences to human safety as a result of Year 2000 failures. From a company standpoint there are serious implications with respect to the provision of a safe working environment if a Year 2000 failure occurs. Basically, companies have an obligation to provide a safe working environment under Health and Safety legislation. If a company is shown not to have taken reasonable steps to prevent a Year 2000 injury related incident then it may be culpable under the law.

ADVICE ON TACKLING THE YEAR 2000 PROBLEM

Initial Problem Identification

This is the starting point for ensuring compliance of all computer systems. Companies should consider taking the following action:

- Assess the need to set-up a dedicated year 2000 project team within the company and appoint a competent and proven year 2000 project manager. This individual should hold a senior position within the company to ensure the problem receives exposure at the highest levels of the company so that swift and appropriate action can be taken.

- Generate a detailed inventory of all equipment which is potentially exposed. Where possible try and quantify the effects of the affected systems malfunctioning. Where doubt exists over whether equipment or systems are potentially affected guidance should be sought from equipment manufacturers and suppliers. If in doubt assume the worst and have systems fully evaluated.

- Start a dialogue between yourselves and important customers and suppliers. It is critical to ensure that customers and suppliers are also aware of the problem and taking effective action. Their inability to do so could seriously affect your own business operations. Where a company is either a parent or subsidiary of a large group effective communication lines should be established to ensure that all interested parties are taking action. Particular care is required where computer systems are physically linked within a network as all systems within the network will need to be compliant to ensure that a malfunction or failure does not occur.

- Analyse and allocate sufficient human and financial resources to ensure that the problem can be effectively tackled. Where substantial financial provisions are required these will need to be arranged well in advance.

- Issue clear purchasing instruction to all departments to ensure that all new equipment is year 2000 compliant. Where new equipment and systems are purchased certification should be provided guaranteeing year 2000 compliance and the legal validity of these documents should be assessed.

  Additionally, clear instructions should be issued to all departments who may be responsible for generating new computer code or applications to ensure that these new systems are generated in a year 2000 compliant format.

- The terms and conditions of important contracts including specific wordings should be reviewed to assess whether you are potentially financially or contractually exposed to the year 2000 problem. This should include an assessment of important contracts with suppliers and purchasers.

identical virtual reality view of the problem but within which the results can be displayed.

Thus the initiator of the problem can see his analysis through from the start when he is in control of the definition to the end when he can pick those results which best illustrate his conclusions. Initially, the computations can be handled by experts outside his organisation to ensure that the problem has been handled properly. However, as the user gains experience in the use of the system he can either start to do the calculations on his own machine by installing the CFD package. Or he can run his problems remotely on more powerful computers located elsewhere and maintain tight control of their development. This would be achieved by by initiating a larger proportion of the computational controls from his pre-processor but retaining the greater power of a computational machine run by a consultant organisation possessing better computational facilities.

The 'qualitative' results described in the earlier section were obtained using a complete PHOENICS system which included the VR-Editor and the VR-Viewer as well as the CFD package. A computer running on a Pentium 130 with 32 MBytes of memory performed quite adequately without excessive run times when the simple models with a fairly coarse mesh size was employed. The results for a 50 000 cell simulation show similar trends to the smaller models, however, grid independence may not have been reached and a 500 000 cell model is presently being constructed. This model will be used to explore the effects of a number of factors which have been identified in this paper as having an important bearing on the validity of a 'quantitative' analysis. The results of these calculations will be reported at the meeting.

CONCLUSIONS

The dangers associated with spills of oils which can produce gases has been identified as presenting a real risk to the safe operation of process equipment in enclosed buildings which possess void spaces below floors formed from gratings. The problem has been examined employing Computational Fluid Dynamic (CFD) methods and the authors of the paper have concluded that this approach is useful for preliminary studies but must be used with care when realistic quantitative results are desired.

REFERENCES

(1) PHOENICS Version 3.1 user manuals (1998), CHAM Ltd, Bakery House, Wimbledon, SW19 5AU

- Where possible automatic conversion methods should be applied. Experience has shown that these are quicker, save on resources and convert in a uniform manner. However, on a cautionary note they will not be suitable for all systems.

- Develop contingencies as part of the conversion process. For business critical systems, contingencies are vital to ensure that operations can continue should problems arise.

CONTINGENCY PLANNING

As previously described, contingency planning forms an important part of the year 2000 compliance process. Contingency plans should be developed to cope with unforseen failures of microprocessor controlled systems or for situations where the failure can be foreseen but the consequences of failure are either unknown or unclear.

Due to the potential for a large number of systems to fail in an unforeseen way (particularly where large numbers of embedded chips are involved), it will not generally be possible to develop contingencies to cover all eventualities. The first task with respect to contingency planning should therefore be to identify and prioritise those systems which are most critical to the continuation of business activity so that contingencies can be developed for these.

Contingency planning in the context of the year 2000 problem will normally involve preparing in advance to either **replace** or **repair** malfunctioning systems or components. This should involve the purchase and stockpiling of substitute components and the development of remedial action plans. Remedial action plans will normally involve assessing the following elements and then documenting the outcome:

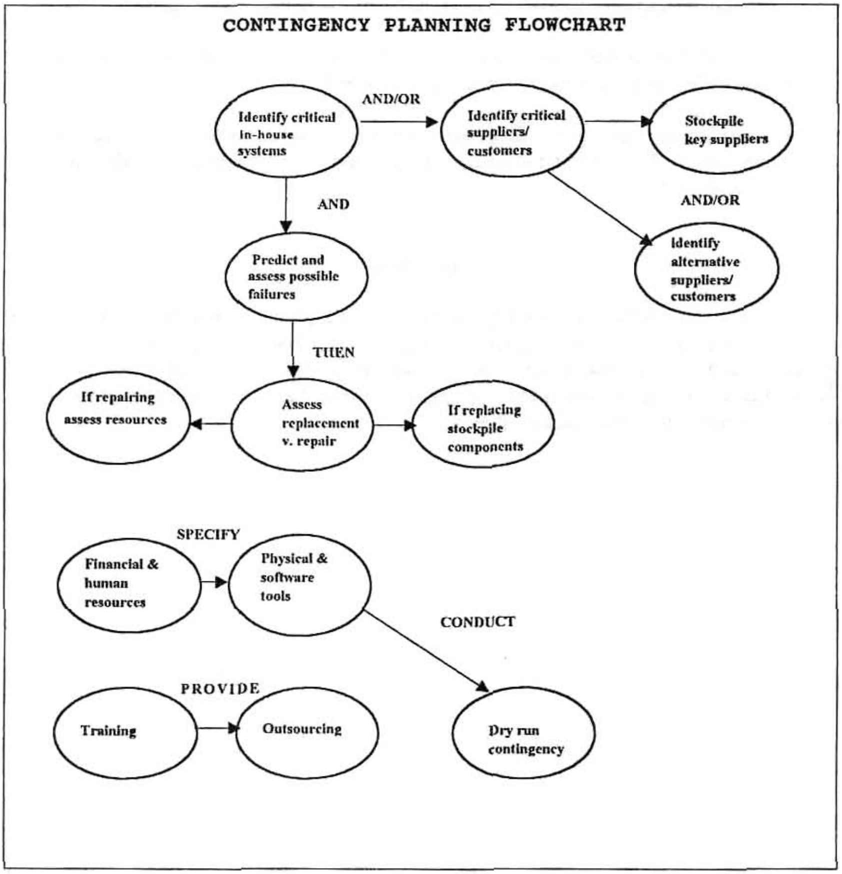
- Assessing what probable financial and human resources will be required and ensuring that these will be available. Where outside expertise, usually in the form of IT consultants, may be required, availability should be assessed and contractual arrangements made well in advance. The logistical side of available resources should be carefully analysed to ensure that assistance is available on a twenty four hour continuous basis.

  Where in-house human resources are critical it will be necessary to ensure that adequate and appropriate training has been provided. Where possible dry runs of the contingency scenarios should be performed to assess the adequacy of responses.

- An assessment should be made of what tools will be potentially required to alter or repair systems. Where specific tools and systems are required these should be purchased in advance and tested using dummy systems. Tools with respect to the year 2000 problem can have a multitude of definitions including physical tools required to alter machinery and equipment and software tools required to modify computer code.

In addition to an assessment of in-house systems, contingencies may also need to be developed for coping with problems which stem directly from the non-compliance of key customers and suppliers. Generally, these problems can be addressed in advance in a number of ways. Firstly, critical raw materials, components and services can be purchased in advance and stockpiled on site. Secondly, where single sourcing exists an alternative supplier can be sought in advance and preliminary arrangements made to supply materials, components or services in the event that the usual supplier has major problems. Finally, where neither of the above options is seen as being viable, key suppliers and customers should be contacted well in advance and assurances of year 2000 compliance sought.

Obviously, the development of contingency plans will be specific to the operations conducted and the overall company philosophy. A general framework can however be developed and is summarised within the following flowchart:


CONTINGENCY PLANNING FLOWCHART
Identify critical in-house systems
AND/OR
Identify critical suppliers/ customers
Stockpile key suppliers
AND/OR
Identify alternative suppliers/ customers
AND
Predict and assess possible failures
THEN
If repairing assess resources
Assess replacement v. repair
If replacing stockpile components
SPECIFY
Financial & human resources
Physical & software tools
CONDUCT
PROVIDE
Training
Outsourcing
Dry run contingency

PROCESS VALIDATION

Once equipment has been converted a testing strategy will need to be developed. While it will often not be possible to test all eventualities, the testing regime should be designed to be as rigorous as possible. With respect to testing you should consider the following:-

- Use a separate testing environment from the normal production and/or operational environment. This should ensure that problems can be identified and fixed without putting on-going operations in jeopardy.

- Check that computer licences will not expire and extend or re-new where necessary.

- Monitor all systems and report progress. Problems may not be immediately apparent during testing so that on-going checks will need to be performed.

- Once equipment and/or systems have been successfully monitored certification of equipment can be performed. This would act to benchmark equipment as being compliant and allow progress to be monitored.

CONCLUSION

The year 2000 problem is likely to have major ramifications with potential effects to all aspects of our professional and personal lives. Companies both large and small have an obligation to protect their employees as well as the companies and consumers with whom they interact. Only those companies who can identify the potential for loss and take steps to minimise these potential losses will be able to confidently operate up to and beyond the millennium.