COMPUTERS IN CHEMICAL PLANT - A NEED FOR SAFETY AWARENESS

P G Jones
HSE Technology Division, Bootle, Merseyside.

The paper gives evidence from recent HSE studies of accident/incident reports involving computerised control systems, and then explores the issues which can affect safety. Reference is made to developing trends in control technology and the special problems associated with software.

**KEYWORDS: Safety (computer control)
Computer Control (Safety)**

INTRODUCTION

HSE having three and a half years ago launched guidance on the use of programmable electronic systems (PES) in safety related applications (Ref 1), has continued to take an active interest in developments in the technology. Its professional engineers and scientists have assessed the introduction of upgraded computer systems into industrial processes, but noted that many of the concerns reported earlier (Ref 2) persist. This is somewhat worrying because it would seem that lessons are not being learned, despite wide coverage of the subject in the technical press. It is therefore worth repeating the list of concerns presented previously. These covered:-

(a) Introduction of computer control - poorly thought out and planned

(b) Establishing the requirements - wooly specification, mismatch of understanding

(c) Validation of software - no satisfactory procedures yet

(d) Standard of plant installation - evidence of poor workmanship

(e) What is the plant? - Are the diagrams and specs. up to date?

(f) Protection of system on plant - vulnerability of sensitive instrumentation

(g) Operating and maintenance procedures - are they well documented and followed

(h) Training and personnel - is it suitable for all staff involved?

These problems were detected in a whole range of companies and processes, and indicated that basic discipline in design, installation, operation and maintenance is required across the board.

In the light of these earlier (and continuing) concerns HSE inspectors have been collecting data on accidents and incidents which come to their attention, and an analysis of an early group of these reports has indicated trends which can be noted here.

EVIDENCE FROM ACCIDENT/INCIDENT DATA

Analysis of reports available to HSE showed that there were a range of causes, which could be classified under eight general headings. These are:-

Accident/Incident Causes

Cause	%	Indications from evidence
Poor functional requirement specification	>10	Unrecognised hazards
Poor safety integrity	>30	Lack of back-up, safety devices
Poor design and implement-ation	>10	Inadequately rated components
Poor installation	> 5	Workmanship, protection
Poor operation	> 5	Training, understanding
Poor maintenance	>15	Incorrect re-assembly
Poor modification control	>10	Sloppy management system
Poor decommissioning	> 1	Planning, check-back.

(The detailed analysis is contained in a report which is to be published soon (Ref 3).

It will be noted that many of the causes and indications coincide with the areas of concern identified above. The first four causes in the table suggest a lack of discipline in the introduction of the computer control system, and in this respect the step-wise approach recommended by the HSE Guidelines on PES (Ref 1) had probably not been followed. This involved:-

(a) hazard assessment

(b) identifying the necessary safety requirements to deal with the hazards

(c) deciding on the required level of safety

(d) designing the safety related system to provide (c)

(e) conducting a safety audit via progressive checklist

(f) check back to ensure safety specification is met.

Had these basic steps been rigorously followed, it is likely that a significant number of over 60% of causes would have been identified, and probably dealt with. The same *PES Guidelines* make basic recommendations on operation, maintenance, modification and staff training, which again had they been applied might have dealt with many of the remainder.

It therefore remains a concern of HSE, that relatively straight-forward procedures are not followed in the introduction and use of essentially first generation computer technology in plant and machinery installations. What then are we to make of the use of expert systems, and artificial intelligence protocol developments, particularly where these are appearing in 'on-line' applications? Next we are promised enhanced knowledge based systems and neural computers which supposedly have the capacity to think for themselves!

OTHER TRENDS

Alongside these computer system developments, and perhaps a little more mundane, though still significant in health and safety terms, are optical communications, mains signalling and telecommand methods, all of which have potential applications in plant control. Another technique, which is causing some concern in HSE, is teleservice where suppliers of computerised equipment are able to diagnose and make adjustments from afar. This clearly has legal implications if someone outside the company can make computer coding amendments, or modify operating sequences, especially if this can lead to accident situations. Moreover, it will be recognised that 'afar' can be in another country, where the Health and Safety at Work Act does not apply. HSE would advise potential users of this service to proceed with the utmost caution, particularly if 'on-line' computers are involved.

Despite the various problems or concerns mentioned above, HSE is impressed to see the steady movement towards integrated systems. Clearly, modern thinking is to try and maximise the benefits from investment in computerised equipment. Stand alone techniques of a relatively short time ago, are now becoming linked to provide widely embracing systems from the design office, through provisioning and operations, to final packaging and distribution. Improved sophistication points the way to 'just in time' processing strategies which have already taken root in many manufacturing industries, so saving on materials, time and tied up capital. However, there are likely to be limitations to these techniques in the chemicals sector, owing to the sheer dynamics of many process routes.

The principal driving force for these developments is inevitably economic; better return on capital invested, higher levels of plant availability, reduced labour costs and improved

product quality, are all laudable aims. Applied across wide sectors of industry such trends make good sense for UK Ltd, provided they are applied in a realistic and safe manner. The rewards for getting the process right are great, but the costs of getting them wrong may be greater; computer aided production is attractive, computer aided disaster is abhorrent!

The safety dimension must therefore be considered at each stage of an integrated system. Even in computer aided design there may be errors in the programmes which could lead to eventual problems. More and more faith is being put in the infallibility of computerised techniques, but can this always be fully justified? The wise companies and their chemical engineers will be alive to the possibility of problems, and so design and safeguard their systems accordingly.

SAFETY CONSIDERATIONS

The computerised enhancement of many aspects under the control of chemical engineers has much to commend it, provided we do not lose sight of the limitations of the hardware, software and liveware with which we are dealing. Optimisation of process equipment and control methods must give proper recognition to the constraints of safety and reliability, but how much do we really know about these?

For hardware there is in many cases, either from direct plant experience or from manufacturers' data, usually a pool of data on component performance. This can then be converted into meaningful reliability indicators, and hence design strategies to deal with random hardware failures can be devised. Typical amongst these would be the technique of equipment redundancy.

But what about the software? Here we are rapidly into the realms of systematic failures for which little or no meaningful data exists. There may be errors in design, specification or programming of the computer software which can lie buried in the system for considerable periods before becoming apparent. Unfortunately techniques of software verification and validation are still quite limited in their capacity, and short of formal methods for its production, little can be done at this stage, unless of course the design recognises the possibility of failure and provides a fail-safe back up system accordingly.

Then the liveware!. Every system contains an element of the human factor somewhere, whether in the control loop itself or in its design or maintenance. So how reliable are humans? What data is available on the subject, and how meaningful is it? This is a new science which is in its infancy, and HSE along with others is still way down the learning curve. However, what we do know so far is that the performance of an individual, be it as a designer, a programmer or an operator is influenced by a number of factors. These may be associated with the organisation, the job or the individual himself, and any one of them can affect his reliability.

There are then varying degrees of uncertainty, but provided we do not lose sight of this important fact all can be well. This point must be stressed because there is a developing tendency, particularly with knowledge based systems, to assume that the information is always right. However, 'intelligent systems' can only be as good as the information they contain, and systems can make mistakes, for example incorrect knowledge; incorrect inferences; misunderstanding by the user; breakdown of reasoning when faced with unexpected situations; and unacceptable value judgements built into the system.

The use of computerised systems needs to be related to the climate in which they have to operate, and the extent to which their performance is safety related. Clearly there is a spectrum of possibilities here from straight forward economic considerations at one end to processes involving safety critical operation at the other. Hence the demands placed on design integrity may vary and the relevance of safety and reliability to the overall requirement in each case can change accordingly. For example, the design criteria for a machine churning out widgets where the most serious accident is an operator losing a finger, should be somewhat different from that of a weapon system for which a control system malfunction could trigger Armageddon. These may be rather extreme examples, but they should illustrate the point that it is realistic to see a range of design integrities against relevant risk levels in safety related applications.

Another facet which bears on the design problem, is the extent to which systems may be controlled by legislative requirements. For example the Control of Industrial Major Accident Hazards (CIMAH) Regulations, under which companies need to demonstrate to HSE that their process is properly controlled and hence hazardous chemicals are safely contained at all stages. If the control system of such a plant is computerised, the company must convince HSE inspectors that they understand the system and its limitations, and have properly addressed its installation, maintenance and use, as well as ensured that all staff associated with the system have been properly trained. Some may see these requirements as something of a tall order, but they are essential demonstrations of safety assurance. In plants such as these, the consequences of 'getting it wrong' are horrendous; reference Flixborough, Bhopal, Seveso, Mexico City etc! Thus it must be a critical part of any design strategy to ensure that hazards and risks are properly identified, and then safety and reliability provided accordingly.

Until recently there was particular emphasis on just getting the safety right, and it is imperative that this continues to attract attention. However, there is now a wider challenge ie the environment! Whilst it may be possible to separate the safety and environmental controls on a plant, and indeed this may well happen in the short-term, the future will lie in the direction of integrated procedures for safety assurance and pollution limitation. This is clearly a requirement for the

new generation processes and as such provides an objective for plant and control system design.

There is therefore a whole range of applications capable of attracting the use of computerised methods, and there are frequent references to fresh projects or extensions of the technology into new areas. For example, a computer system to log and track permits to work for safer management of process plant is being developed for use on offshore installations. Similarly, in the field of batch plants, tremendous strides have been made in the integration of multi-menu processes. There seems no shortage of opportunity for development, although we need to always be alert not to overlook the important safety dimension in these applications.

There is however another angle we must not lose sight of in all of this work. Most of the computer applications to date have used systems based on quantitative methods for both design and operation. Thus even with all their limitations, one may in theory follow the operation of the programmes via varying degrees of ladder logic. However, recent developments are making increasing use of non-quantitative methods in their structure. These require the injection of value judgements, inferences or route selections based on weighted preferences, all of which have the potential for increasing the level of uncertainty in specific situations. Examples of these trends appear in expert systems, artificial intelligence and knowledge based techniques. At first sight one might think these are robust applications of sound logic, but perhaps it is time to start asking some well known 'what if' type questions, for example:-

- facts as interpreted by who?
- inferences drawn on what basis?
- values assigned by what standard?
- priority selections set by what process?

We therefore need to be mindful of present generation problems, and proceed with caution towards computerised systems having greater integration or more comprehensive control strategies.

SYSTEMS AND SOFTWARE

The development of computerised plant in the process industries and elsewhere has focussed attention on the need for a disciplined 'systems' approach to projects. In order to ensure that the full benefits of computerisation are enjoyed, it is essential that the total control regime is considered as a complete system, so that various forms of sensors, controllers and actuators, be they electronic or mechanical, can properly support one another as an integrated whole. This is particularly important for safety related systems, where different types of safeguards may supplement one another in the

overall configuration for safety (Ref 4). A recent study (Ref 5) shows that there is a large measure of recognition for this requirement, and it is encouraging to see that the control systems community are developing an international standard on safety related systems (Ref 6).

Also under development is an international standard for the software (Ref 7). This will be particularly welcome since the whole subject of computer software reliability has been attracting increasing attention. Both the technical and popular media have been focussing on the difficulty of verifying and validating software (Refs 8, 9, 10) since no guarantees can be given for its correct functioning under all conditions. In properly designed and engineered systems this uncertainty can be largely overcome by double, triple or quadruple redundancy provisions in safety critical areas. However, such provisions are expensive and inevitably there are strong commercial pressures to limit the back-up systems to reduce costs. This has led to a spate of examples where software errors have led to system failure or dangerous operation (Refs 9, 10).

Whilst actively supporting the development of the IEC Standard on software, UK government has also been encouraging the introduction of formalised regimes for the use of computerised systems. DTI and HSE recently launched a campaign on SafeIT (Ref 11), which alerts industry to the current status of computerisation techniques, and maps out a strategy for responsible advance in this area. In addition DTI has also sponsored a healthy research programme for work on safety critical system projects (Ref 12). All this is good news indeed, but clearly these activities are geared towards future improvements and answers, so what of today?

The best advice at this stage is to be aware of the limitations of software and to design systems accordingly. The PES Guidelines referred to at the beginning (Ref 1) establish a basic framework in which to operate, and this may be supplemented by other guidance to handle the more sophisticated systems (Refs 13, 14).

SUMMARY

The use of computerised equipment can allow an improved regime of control, which in turn can lead to optimisation of operating parameters and hence plant efficiency and product quality. Improved control has the potential, if properly integrated, for enhanced safety by providing much greater knowledge of plant status. However, there are already a range of problems with the current generation of equipment and these should be solved before increasing sophistication is introduced into safety related applications and particularly safety critical systems. The question of software integrity is especially relevant to the need for caution at this time.

-ooo-

REFERENCES

1. Programmable electronic systems in safety related applications:

   Pt. 1 An introductory guide ISBN 011 8839136 HMSO
   Pt. 2 General technical guidance ISBN 011 8839063 HMSO

2. Safety overview of computer control for chemical plant. P Jones paper to IChemE Hazard X Conference: Symposium Series No. 115.

3. "Out of control" - internal HSE report for the Control Systems Technical Committee - to be published in Spring 1991.

4. Specification, Design and Testing of Safety Critical Systems - Dr P A Bennett paper given to F.Eng conference on "Warnings of preventable disasters", QEII Conference Centre 6.9.90.

5. A study of the computer based systems safety practices in the UK, European and US industry - report prepared by Centre for Software Engineering, Inst. Electrical Engineers, and Dept. of Trade and Industry (Dec 89) - published by IEE. ISBN 0 86341 700 0 - HMSO.

6. IEC draft standard "Functional safety of programmable electronic systems: generic aspects" (IEC reference "65A Secretariat 96).

7. IEC draft standard "Software for computers in the application of industrial safety related systems" (IEC reference "65A Secretariat 94).

8. Software Safety Notebook - Microsystem Design - April 1990

9. Computer unreliability and Social vulnerability - T Forester, P Morrison - FUTURES June 1990.

10. BBC2 Antenna Programme - Wednesday 24 October 1990.

11 SafeIT - A Government Consultation Document on the safety of computer controlled systems - May 1990 - issued by Dept. of Trade and Industry.

    Pt. 1 Overall approach
    Pt. 2 Standards framework.

    Available from ICSE Secretariat, DTI/ITD7a - Room 840 Kingsgate House, 66/74 Victoria Street, London.

12. Information Engineering Advanced Technology Programme - Systems Engineering - Research Workplan for Safety Critical Systems Projects - available from DTI/ITD4 - 420/30/004 - Kingsgate House, 66/74 Victoria Street, London.

13. Rationale for the development of the UK defence standards for safety critical computer software - Air Vice Marshall M J D Brown - Compass 7 - 11 June 90 - Strategic Electronic Systems MOD/PE, 98 High Holborn, London.

14. Evaluation of Safety Critical Software - D L Parnas, Juan Schouwen, S P Kwan - Communications of the American Computer Manufacturers - June 1990 Vol. 33 No. 6.

-oOo-