SAFETY OVERVIEW OF COMPUTER CONTROL FOR CHEMICAL PLANT

by P G Jones*

The paper identifies the legal requirements, and current status of HSE guidance. Areas of safety concern are then highlighted which may influence HSE's attitude toward future trends. Reference is made to accident and inspection experience, and possible weak spots in existing company regimes are noted.

[Keywords: Safety (computer control), Computer Control (Safety)]

INTRODUCTION

The expanding use of computers for the control of process plant is a trend which is encouraged by the Health and Safety Executive (HSE). It is recognised that the use of computerised equipment can allow an improved sophistication of control, which in turn can lead to optimisation of operating parameters and hence increased plant efficiency and product quality,. However, improved control of process parameters can also, if properly handled, lead to enhanced plant safety by providing much improved knowledge of process status. HSE wishes to see that all potential operating improvements are realised, but is anxious lest the pursuit by industry of improved efficiency and output overshadows the attendant safety considerations.

*HSE Technology Division, Bootle Merseyside

LEGAL POSITION

The provision of computerised equipment for the control of chemical plant would attract the legal duties of Section 6 of the Health and Safety at Work Act 1974, It is therefore worth reminding ourselves what these main duties are (amendments to S6 HSWA introduced by the Consumer Protection Act 1988 are bracketed for ease of reference):-

"S6 (1) It shall be the duty of any person who designs, manufactures, imports or supplies any article for use at work, (or any article of fairground equipment).

(a) to ensure, so far as is reasonably practicable, that the article is so designed and constructed that it will be safe and without risk to health (at all times when it is being set, used, cleaned or maintained by a person at work).

(b) to carry out or arrange for the carrying out of such testing and examination as may be necessary for the performance of the duty imposed on him by the preceding paragraph;

(c) (to take such steps as are necessary to secure that persons supplied by that person with the article are provided with adequate information about the use for which the article is designed or has been tested and about any conditions necessary to ensure that it will be safe and without risks to health at all such times as are mentioned in paragraph (a) above and when it is being dismantled or disposed of: and)

((d) to take such steps as are necessary to secure, so far as is reasonably practicable, that persons so supplied are provided with all such revisions of information provided to them by virtue of the preceding paragraph as are necessary by reason of its becoming known that anything gives rise to a serious risk to health or safety.)

and also

"S6 (3) It shall be the duty of any person who erects or installs any article for use at work in any premises where that article is to be used by persons at work (or who erects or installs any article of fairground equipment) to ensure, so

far as is reasonably practicable, that nothing about the way in which (the article) is erected or installed makes it unsafe or a risk to health (at any such time as is mentioned in paragraph (a) of subsection (1) ----------).

These quotations of duties are not exhaustive, but should be sufficient to show that those who supply and instal computerised plant and ancillary equipment, have legal responsibilities to ensure that it is suitable for the intended purpose.

Similarly, the owners of computerised plant have legal duties under Section 2 of the Act to ensure that it is properly operated:-

"S2 (1) It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees.

(2) Without prejudice to the generality of an employer's duty under the preceding subsection, the matters to which that duty extends includes in particular -

(a) the provision and maintenance of plant and systems of work that are, so far as is reasonably practicable, safe and without risk to health,

and

(b) the provision of such information, instruction, training and supervision as is necessary to ensure, so far as is reasonably practicable, the health and safety at work of his employees."

Again not exhaustive quotations, but enough to show that legal requirements apply to the users of computerised plant. Associated with these general legal duties, there may be more specific requirements, not necessarily applying to the computerised control as such, but rather seeking that the plant is properly designed and safely run. For example, the 'Control of Industrial Major Accident Hazard Regulations 1984 (CIMAH Regs)' place quite stringent requirements on the operators of chemical plant which handle dangerous substances, and in which part of the control regime may well be computerised.

However, we must face up to the reality that computers and ancillary equipment, although powerful tools for the control of plant, are themselves prone to certain difficulties which could lead to failures. Faults built into, or developing in, the hardware or software elements can lead to random or systematic

failures of the computerised equipment. That being so, what, bearing in mind the legal requirements, should be done to ensure, so far as is reasonably practicable, that the plant is operated safely?

GUIDANCE

It was recognised some years ago that there would need to be some guidance on how companies should address these requirements for computerised plant. There is nothing new in the breakdown scenario; let's face it conventional mechanical or electro-mechanical systems are prone to the same difficulties. The only difference is that the failure mechanisms and their manifestation may not be quite so obvious in the case of computerised equipment. However, this failure potential need not give rise to undue concern, if the system has been designed accordingly. Generally speaking the concepts of any strategy for the design, installation, operation and maintenance of such equipment will be applicable to both computerised or conventional control systems.

With these thoughts in mind, HSE staff produced guidelines on the use of computerised equipment in safety related applications (Ref.1). The guidelines present a strategy for dealing with the potential failure problems in a way which will guarantee, so far as reasonably practicable, the safety of the plant under all foreseeable operating conditions. This strategy identifies configuration, reliability and overall quality as the main elements of the safety related system, and takes the user through a step-wise approach to the design comprising:-

(a) hazard assessment
(b) identifying the necessary plant safety requirements,
(c) deciding on the required level of safety
(d) designing the safety related system,
(e) conducting a safety audit via a progressive questionnaire, and
(f) checking back to ensure the safety specification is met.

The procedure is therefore, a disciplined approach to the introduction of computer control into any safety regime, and its applicability to the chemical plant situation has been described. (Ref.2).

So how do HSE inspectors use the guidelines in their day-to-day work in dealing with chemical companies? Before answering this question, it must be said that the guidelines are a code of good practice to be used in the light of potential uncertainties (particularly with software integrity) and not the code of good practice. Thus in legal terms they are certainly not an 'approved code of practice' under the HSW Act 1974, but rather a statement of recommended procedure in much the same way as a BS Code of Practice might be. Therefore the

guidelines themselves carry no legal weight, and the way is clear for suppliers and users alike to do things their own way. (ie companies can take and adapt the generic guidelines to suit their own situation).

Having developed the guidelines in conjunction with industry and academia, HSE trained its field inspectors, and their specialist support, in the concepts and application of the recommended procedures. Thus inspectors in talking to companies who use computers in safety related applications, will seek to find out how their systems work compared to the ideas and principles in the guidelines. Should the inspector identify a deficiency in the system which is, or could be, dangerous, he might then suggest a solution based on the recommended procedures. At this stage it would be open to the company to do something else of equal effectiveness to remove the danger. However, should the company not respond enforcement action might then follow, not for non-compliance with the guidelines, but because the danger still exists. In this situation the offence would probably be related to the general duties of the HSW Act mentioned earlier.

The status and use of the HSE guidelines has already aroused a degree of interest, and the position has been discussed in print (Ref.3).

AREAS OF CONCERN

A paper describing some of the areas of HSE concern about the safety of computer controlled systems has been presented previously (Ref.4). However, it is useful to pick out the main worries for brief mention here.

(a) The introduction of computer control - the HSE guidelines mentioned above recommend a systematic approach to the introduction of computer control to chemical plants. In practice there is some doubt as to how far companies go through a disciplined process for the use of such equipment, and this then raises concerns that they may not understand their own system, which hardly inspires HSE confidence especially if said plant happens to be processing dangerous chemicals.

(b) Establishing the requirements - as a corollary to the first point - there is a question of communication between the system supplier and the system user. Large chemical companies are likely to have their own in-house staff who understand both the process and the control electronics; but what about the small to medium size companies? They probably engage a specialist contractor to supply and instal a computer control system for them, giving rise to the concern that the company do not understand the electronics

and the contractor does not understand the action/reaction dynamics of the chemical process.

(c) Validation of software - this is an area where work still needs to be done, especially for relatively non-specialised civil sector systems. Even so-called high integrity software contains faults, some of which may be picked up in plant commissioning or routine running, but others may lie buried until triggered by some 'unusual' combination of circumstances. (In the HSE guidelines the likely existence of software faults is recognised, and design recommendations made accordingly).

(d) Standard of the plant installation - mention was made under the 'legal' section above that plant needs to be properly installed. This means all the plant including the instrumentation and wiring runs etc., and its physical state. In other words, these systems should be of a suitable standard and adequately reliable for the level of risk under their control. On chemical plant, this of course means reliable under the arduous conditions of the process atmosphere which may involve dust, solvent vapour, acid fume, etc.

(e) Do the P&I diagrams reflect what is on plant? - a simple question, but how true in practice? During the life of a plant there may be many reasons why additions, deletions or modifications are made. These should be properly logged, and preferably the reasons for the change noted.

(f) Protection of the control system on the plant - the provision of the control and protection system will probably be vital to the safety of the plant during its operation. But how vulnerable are the instruments and control circuits to damage, either accidental or deliberate? Has provision been made for emergency situations such as fire or flood on this, or adjacent plants? Clearly, HSE inspectors will be concerned if they find that vital instrumentation can be 'knocked-out' with relative ease.

(g) Operating and maintenance procedures - Inspectors would hope to find well-documented procedures for plant operation, and evidence that these were being followed in practice. If properly designed it is likely that the well-intentioned short-cuts which often get introduced by operators will be frustrated by the computerised system. However, this assumes that the system itself cannot be amended by unauthorised tampering. Similarly, concern would be expressed if there were indications that maintenance

was not being done properly, the more so if the procedures countenanced unrecorded modifications to the control hardware or software.

(h) Training and personnel - How much training has been given to the plant operators? What sort of training was it? Did it include the plant managers and maintenance staff? These might be typical questions from an HSE inspector who would hope to find that staff understood their plant and that they had thought through possible emergency scenarios, and practiced their responses to them.

This has been a quick gallop through the menu of HSE concerns about computer controlled plant, and they are as valid now as they were when first presented (Ref 4).

ACTUAL EXPERIENCE

The aforementioned areas of concern were not only identified by HSE whilst developing the PES Guidelines (Ref 1), but also reflect the experiences from field inspection work and accident reports. Whilst it is fair to say that the feedback from HSE staff is not all doom and gloom in the area of computerised control, it must be recorded that a remarkable number of companies do not adequately understand the system they are using on plant. Often the 'black-box' syndrome is encountered (ie no problems now because the computer is running the plant), or the 'if it's working, leave it alone' approach to maintenance requirements. These attitudes hardly inspire confidence, especially if found on plants processing hazardous chemicals! Are HSE being unreasonable in expecting companies to understand their own plant control systems? We think not, since clearly there is a responsibility under Section 2(2) HSW Act, to operate the plant safely at all times.

When inspection reports refer to poor standards of installation, inaccurate documentation, vulnerability to damage of essential control items or substandard maintenance, then it is wholly proper for HSE to be concerned, and for this concern to be expressed loud and often. HSE takes this line, not because it is against the use of computerised control equipment, but to ensure that this powerful tool for improving plant output and product quality is properly and safely exploited.

In order to keep the safety position in perspective, HSE is now logging the detail of reported accidents and incidents which involve failure of a computerised system, or its human operators. Unfortunately our past records often failed to include enough data on the control system malfunction, to be useful to us now in identifying trends or problem areas etc, so that our list only covers the last few months. However, from the fifty or so reports we have to hand, some observations are possible:-

(a) about half involved software problems. (eg inadequate specification for the job, improper programming due to failure to understand the process dynamics, unauthorised modifications to the control programme).

(b) about one third were 'man/machine' interface problems (eg computer giving ambiguous information, operators making wrong assumptions based on read-out information).

(c) only ten percent were traceable to computer hardware faults. (eg circuit board errors).

(d) about one third were associated with maintenance operations (eg attempts to defeat interlocks, not replacing faulty instrumentation, disconnecting control circuitry).

Once HSE has an adequate databank on accidents and incidents involving computerised plant, it will publish it in suitably anonymised form. It would be helpful if industry also drew attention to its experience (eg via the IChemE Loss Prevention Bulletin), and especially any lessons from 'near-misses' which often do not get reported to HSE.

AREAS REQUIRING ATTENTION

Clearly, it would be useful for companies to give attention to the list of concerns noted above. Whilst it is not claimed this list is exhaustive, it is nevertheless based on evidence of real problems which have occurred in UK or elsewhere.

Associated with these concerns, HSE would suggest three areas which require particular attention. Firstly, careful thought needs to be given to the design and installation of the system for use on chemical plant. This includes setting the original specification, and ensuring that the control hardware and software address this specification. In doing this, it is essential for there to be a good understanding of the interface between the process dynamics and the control functions. Particular care will be needed in the introduction of 'off-the-peg' systems to different processes.

Secondly, should be a requirement that personnel are properly trained in the use of the computerised plant. This should cover all those who may be responsible for, or involved in, its operation and maintenance, and training schedules should recognise emergency shut down situations, covering both 'expected' and 'unexpected' events. It must be recognised that despite the sophistication of computerised control systems, the 'human factor' is inevitably involved somewhere, and should therefore be addressed accordingly.

Thirdly, the computer industry still needs to do more to ensure the validation of software both in the as supplied form, and for on site testing purposes. Until significant improvements are readily available for civil sector use in this area, it is wise to assume that the software will contain faults, and hence that the total system is designed accordingly (see Guidelines in Ref 1).

Computerised control systems are powerful tools which can bring many benefits, but they are not perfect and the shortcomings (eg software validation, the human factor, etc) should be recognised.

FUTURE TRENDS

The development of computers and their associated technologies are proceeding apace, and seem to offer us more and more glittering prizes in on-line and off-line applications. Whilst one cannot help but be impressed by the ever-expanding potential, we must not lose sight of the problem areas, particularly where these can involve safety. Indeed it has already been suggested (Ref 5) that we may be storing up trouble for the future via the use of unreliable micro-chips, and this ".....will inevitably lead to computer-aided disasters".

HSE is trying to keep in touch with those developments which impinge on system safety, and to offer comment or guidance as appropriate. Under study at the moment are optical communications, mains signalling, telecommand techniques and expert systems, all of which have potential for use in control technology. However, it must be remembered that although HSE seeks to keep pace with these and similar developments, the legal duties fall to the manufacturers (S6 HSWA) and the owners (S2 HSWA) of control systems, to ensure that they are supplied, installed and operated safely. In doing this, it is appropriate that adequate attention is paid to previous experiences, and particularly those which may cause concern over plant safety.

-o0o-

REFERENCES

1. *Programmable Electronic Systems in safety related* applications - General Technical Guidance.

HMSO publication (ISBN 0 11 8839063).

2. Safety considerations in the use of programmable electronic systems for the control of chemical plant.

P G Jones, HSE Technology Division, Bootle.

(Paper based on an invited lecture given to the Loss Prevention session at the 9th World Congress of Chemical Engineering and Chemical Plant Design - CHISA 87 - Prague, Czechoslovakia Sept 87: copy available via HSE Library, Bootle).

3. PES Guidelines - Ally or Adversary? - The Chemical Engineer Aug 88 - No 451 p16-20.

4. IChemE North Western Branch, Symposium Papers 1988 No 2, Section 7.

5. The Engineer, 4 February 1988, p14.