Institution of Chemical Engineers

NORTH WESTERN BRANCH

THE SAFETY AND RELIABILITY OF COMPUTERISED PROCESS CONTROL SYSTEMS

MAIN BUILDING UMIST
MANCHESTER 24th MARCH 1988
SYMPOSIUM PAPERS 1988 NO 2

NORTH WESTERN BRANCH PAPERS 1988 NO.2

INSTITUTION OF CHEMICAL ENGINEERS

THE SAFETY AND RELIABILITY OF COMPUTERISED PROCESS CONTROL SYSTEMS

UNIVERSITY OF MANCHESTER INSTITUTE OF SCIENCE AND TECHNOLOGY

MANCHESTER 24th MARCH 1988

SYMPOSIUM PAPERS 1988 NO.2

NORTH WESTERN BRANCH PAPERS 1988 NO.2

INSTITUTION OF CHEMICAL ENGINEERS

ISBN 0 906636 35 3

Price £25 per copy + postage and packing

Postage and Packing UK £1.00
Europe £2.00
Rest of World (air mail) £3.00

To order, please send cheque or bankers order in sterling payable to 'I.Chem.E. N.W. Branch', to:

Professor J. Garside
Department of Chemical Engineering
U.M.I.S.T.
P.O.Box 88,
Sackville Street,
Manchester, M60 1QD,
ENGLAND.

Telephone: 061 236 3311 ext. 2106

Telex: 666094 UMIST G

NORTH WESTERN BRANCH PAPERS 1988 NO.2

INSTITUTION OF CHEMICAL ENGINEERS

THE SAFETY AND RELIABILITY OF COMPUTERISED PROCESS CONTROL SYSTEMS

C O N T E N T S

I.CHEM.E NORTH WESTERN BRANCH PAPERS 1988 NO.2

FRAMEWORK FOR THE DESIGN AND ASSESSMENT OF SAFETY RELATED CONTROL SYSTEMS

R Bell; M. F. Pantony
Health and Safety Executive,
Technology Division, **Telephone: 051 951 4000**
Magdalen House, Stanley Precinct, **Telex: 628235**
Bootle
Merseyside L20 3QZ, UK

SYNOPSIS

The paper provides an overview of recently issued HSE guidelines on programmable electronic systems (PESs). The guidelines are considered in the context of process plant control and protection systems. The concept of the *'total system environment'* is introduced with a view to developing a model on which to consider the key issues as they relate to plant safety. The objective is to give a design and assessment framework for safety related control systems in a process plant environment. Current and future guidelines and standards developments are also addressed.

1 INTRODUCTION

Computer based systems, generically referred to as programmable electronic systems (PESs) have been used in the process industries for many years - particularly for process control functions. Both centralised and distributed systems have been extensively used. There is no doubt that this trend will continue, and in fact accelerate, due to the many advantages such systems offer the plant operator. The realisation of the advantages will, however, only come about if a disciplined and structured approach to the design is adopted at all project stages. A timely reminder of this is illustrated by a recent failure of a computer system controlling a nylon polymer plant which led to a serious plant incident[1]. It has been

estimated that the cost of the post-incident assessment was 10 times what it would have been had a proper assessment been carried out at the project design stages.

In the past the role that PESs have played have been largely restricted to *process control functions* and have only played a secondary safety role. However, the operational and cost advantages of using PESs are now being exploited in the context of protection systems having a primary safety role. *There is thus an increasing trend to provide both process control functions and protection functions by means of computer systems.* Such systems not only offer the potential to achieve higher levels of safety integrity but also offer the plant user advantages by way of reduced operating and maintenance costs together with the ability to perform complex interlocking and plant monitoring functions. If UK industry is to maintain its competetiveness it is important that the potential financial benefits are fully realised. *Yet this must be done whilst achieving an adequate level of safety.* The potential for improved levels of safety integrity is significant. However, the level of complexity involved means that improvements will only come about if a throughly considered design and assessment methodology is adopted. In order to provide such a methodology, the Health and Safety Executive (HSE) published two documents in June 1987, which are the first in a series whose general title is **"Programmable electronic systems in safety related applications"**. The two documents are:-

1) **"An introductory guide"**[2]. This document (**'PES 1'**) is aimed at the non-specialist and provides and overview of the safety principles.

2) **"General technical guidelines"**[3]. This 3 Part document (**'PES 2'**) contains:-

   - general guidance on the problems, and a framework within which they can be approached systematically (Part 1).

   - a method for assessing the safety integrity of PESs - including the hardware and software. (Outlined in Part 1 and described in detail in Part 2).

- a worked example using the method in Part 2 is described in Part 3.

The guidelines are *generically based* and should enable the safety integrity of systems incorporating PESs to be determined irrespective of the application. They have been structured so they do not unreasonably constrain design innovation but allow programmable electronics technology to be safely exploited. A major objective in producing such generically based guidelines was to stimulate industry, and others, to produce their own guidance for specific applications. It is HSEs policy to encourage and give help in the development of this *application specific guidance*.

This paper:

- provides information on guidelines developments taking place - within HSE, industry and national/international standards bodies.

- provides a brief overview of the guidelines. Other recent papers have examined them in more detail or have considered particular facets of them [4,5,6].

- considers, in particular, the application of the guidelines in the context of a process environment - in particular those situations where the control functions and the protection functions are wholly or partly dependent on PESs.

2 SYSTEMS UNDER CONSIDERATION

The guidelines are concerned with those PESs which either acting alone or in combination with non-programmable systems, provide the required level of safety. Such systems, upon which the safety integrity of the plant relies, are referred to as *safety related systems*.

The guidelines do not apply if an *adequate* level of safety is assured by one or more separate non-programmable systems of *conventional safety integrity** or better. Such conventional systems will need to cater for, amongst other things, failures of the controlling PES.

*Note: The term *conventional safety integrity* means the level of safety integrity which has been achieved, in similar situations, by conventional safety related systems which have traditionally been accepted as good engineering practice.

The PES is defined as a system based on a computer connected to sensors and/or actuators on a plant for the purpose of control, protection or monitoring. The term includes all elements in the system extending from plant sensors or other input devices, via data highways or other communication paths, to the plant actuator, or other output devices.

That part of the PES which handles the logic processing is termed the **'programmable electronics'** and refers to those parts of the PES which are not solely dedicated to a particular sensor or actuator on the plant and in which different functions are performed at different times under the control of software. *The term therefore includes both software and hardware elements.* Figure 1 illustrates the basic PES structure. In the context of a safety related system using a Programmable Controller (PC), the programmable electronics would reside within the PC.

3 CONSIDERATIONS UNDERLYING THE GUIDELINES

To ensure safe operation of safety related PESs, it is necessary to recognise the various possible causes of PES failure and to ensure that adequate precautions are taken against each. Two basic types of failure are considered - **Random hardware failures and Systematic failures.**

Random hardware failures are those failures which result from a variety of normal degredation mechanisms in the hardware. Measures of reliability such as the 'mean time between failures' (MTBF) are concerned only with random hardware failures and do not include systematic failures.

Systematic failures are concerned with errors in the design, construction or use of a system which cause it to fail under some particular combination of inputs or under some particular environmental condition. Failures arising from incorrect specification, errors in the software and electrical interference are all examples of **systematic failures.**

4 SAFETY PRINCIPLES

The safety strategy underlying the recommendations made in the guidelines are centred on three system characteristics or *system elements*. The principles which govern the *system elements* underlie the design and assessment strategy for a safety related PES. The three system elements are defined as follows:-

- **Configuration**: The specific arrangement of the programmable electronics within a PES and the combination of PES and non-PES safety related systems.

- **Reliability**: That aspect of the safety integrity relating to random hardware failures in a dangerous mode of failure of the safety related systems.

- **Overall Quality**: The non-quantifiable qualitative aspects of the safety integrity of the safety related systems. This system element is concerned with the precautions taken against systematic failures.

The detailed requirements of the three system elements are, together, intended to tackle both random hardware failures and systematic failures. (Figure 2). The safety integrity level for the safety related systems is specified in terms of the three systems elements - the exact package of which will depend upon the application in question and therefore the level of safety to be achieved. This package constitutes the *safety integrity criteria* for the application. For a specific application the three system elements will be specified as follows:-

- The **configuration** will be specified in terms of the number of safety related systems together with the requirements relating to the programmable electronics (both hardware and software).

- The **reliability** will be specified either *qualitatively* or *quantitatively*.

- The **overall quality** will be specified in terms of the precautions that need to be built into the design, operation, use etc, against systematic failure causes. For those applications that demand a high level of safety integrity the guidelines use a series of checklists which are organised such that each checklist relates to one of the 16 life-cycle phases - see Figure 3. *The purpose of the checklists is to provide a stimulus to critical appraisal of all aspects of the safety related systems rather than lay down specific requirements.*

The safety principles relate to the *total configuration of safety related systems* required to achieve an adequate level of safety integrity for the hazard in question. The total configuration will comprise, in many cases, both PES and non-PES safety related systems - which may be automatic or manual in operation.

It is recognised that an adequate level of safety integrity may be achieved other than by the strategy put forward in the HSE guidelines. HSE believe, however, that the strategy recommended represents a practical foundation on which to base the design, taking into account all potential causes of failure including software faults and electromagnetic interference.

5 DESIGN AND ASSESSMENT GENERAL FRAMEWORK

The overall framework, including the key steps, for design and assessment of safety related PESs is shown in Figure 4.
From Figure 4, it can be seen that:-

- the required level of safety integrity is specified in terms of the three system elements - *configuration, reliability and overall quality. This specification for the safety integrity in terms of the system elements constitutes the safety integrity criteria for the application.*

- the *safety integrity criteria* relates to the total configuration of safety related systems (both PES and non-PES).

- the *safety integrity criteria* are used as the basis of design and analysis of the safety related systems.

It is intended that future guidance documents will specify the *safety integrity criteria* for specific applications. Where no such criteria has been developed for the particular application, the overall objective should be to ensure that the safty integrity of the total configuration of PES and non-PES safety related systems should not be inferior to *conventional safety integrity*.

In determining *conventional safety integrity* for a particular application, guidance may be obtained from consideration of conventional systems which have been or would be accepted in similar circumstances. In some cases, it will be possible to make a direct comparison with existing or replaced plant. A direct comparison will not always be easy since PESs are used in many new fields of technology and applied in many new ways; in such cases, accepted good practice in other similar situations will provide important guidance.

The design and assessment framework (Figure 4) has been discussed in terms of the total configuration of safty related systems one or more of which was a PES. However, the framework and much of the guidance contained in 'PES 1' and 'PES 2' is applicable to non-PES systems. *For example, in the context of Steps 1 - 6; all steps are relevant to situations where there are no PESs in the total configuration of safety related systems.*

6 APPLICATION OF THE SAFETY PRINCIPLES

Publication 'PES 2' provides a number of examples of how the safety principles apply in various general cases for those situations in which no safety integrity criteria, specified in terms of the system elements, have been developed. Examples are given for *protection systems; separate control and protection systems; combined control and protection systems; and continuous control for safety.* The examples are not intended to cover all situations or all means by which the safety principles may be satisfied. They are intended merely to illustrate how the safety principles apply in practice. It is intended that there will be further documents to show how they apply in specific circumstances.

7 TOTAL SYSTEM ENVIRONMENT

The application of the PES guidelines to the process industry needs to be considered in the context of the **'total system environment'** as it relates to the hazard(s) in question. All those systems which play a part,

to a greater or lesser degree, in preventing the hazard(s), or mitigating the consequence of the hazardous event(s) need to be considered. The *total configuration of safety related systems* is a part of this **'total system environment'**.

In the context of a chemical plant the key features of this **'total system environment'** are shown in Figure 5 and include:-

- The main process control system which is designed to keep the plant within its designed operational envelope.
- The operator and his role in the overall scheme of things.
- The alarm system and its role in the overall scheme of things.
- Those systems that have primarily been designed to provide the requisite level of safety (ie, dedicated protection systems).

Only when the above features have been identified and the design philosophy worked out is it possible to make soundly based judgements about a number of issues as they effect the overall safety integrity. For example, the importance of the following:-

- The control system contribution to the overall safety. For example, what is the role of the control system in achieving the required level of safety? If other systems are primarily responsible for safety, has a failure rate been ascribed to the control system? How was it formulated?
- Functional specification of the protection systems. How was this formulated? Does it take into account the total configuration of safety related systems? Does it consider all reasonably forseeable events with regard to control system and plant failure causes?
- The demand rate used as a basis for the protection system design. How was this demand rate formulated?

- The role of the operator. Has the operator's performance been taken into account in any estimated control system failure rate?

- Alarm management systems. How have these been taken into account in estimating the control system failure rate? Where they taken into account in estimating the demand rate on the protection systems?

- Software change procedures. The highest degree of formality should be applied to the safety related systems. It may be possible to relax the procedures for other systems - but only after consideration of their function in the overall scheme. For example, for non-safety related systems (as per definition in 'PES 2') it should be possible to have less rigourous software change procedures. This is one of the benefits of using the concept of the *safety related system*.

- Maintenance priorities. How have they been determined between those systems which are safety related and others?

The adoption of a structured design and assessment framework should enable the above questions, and other to be answered and enable decisions which affect safety, and which could have important economic implications, to be made on a rational basis. It is important that the '**total system environment**' is developed in the future so that individual elements in this '*environment*' can be considered together with the interaction between each element.

8 PROTECTION SYSTEMS

8.1 Terminology

The two terms - **SAFETY-RELATED SYSTEM** and **TOTAL CONFIGURATION OF SAFETY-RELATED SYSTEMS** - are fundamental to the guidelines and are considered below in the context of *separate control and protection systems*.

Consider a plant which is controlled by a *main process controller* and *two separate protection systems*. The main controller provides the full range of control functions for the plant but should this controller fail in some way, or conditions on the plant deviate to the extent that it cannot be controlled by the controller, then protection is provided by the *two separate protection systems*.

Failure of the main process controller to keep the plant within its operational envelope puts **DEMANDS** on the two protection systems. For the particular application, the two protection systems provide an adequate level of safety, taking into account the hazard in question and the number of **DEMANDS** made upon the protection systems. Each protection system is a **SAFETY-RELATED SYSTEM** and the two protection systems together constitute the **TOTAL CONFIGURATION OF SAFETY-RELATED SYSTEMS**.

In many cases the *main process controller* will have safety functions, but what is of importance is that the two protection systems provide, in their own right, the requisite level of safety. *The very fact that the main process controller has safety functions does not of itself make it a safety-related system.*

The concept of the **SAFETY RELATED SYSTEM** has been developed to separate the complexity of the main process control computer from the dedicated protection systems. This has important economic and safety benefits. It is essential however in doing this that an appropriate demand rate is used as a basis for the protection systems. Control system failure will be only one source of demands for protection and overall demand rate on the protection systems may not be sensitive to control system failure. It may not therefore be necessary to carry out a quantitative assessment of the control system in order to determine its failure rate.

The demand rate is used in the design of the protection systems, in the first instance, to meet the requirements of the **reliability** system element. The requirements relating to **configuration and overall quantity** are applicable only to the protection systems and not to the main

process controller (providing the main process controller does not constitute a safety related system). This has important advantages with regard to maintaining the initial design safety integrity.

8.2 Process plant example

Considering the process shown in Figure 6 the vessel contains a liquid in which there would be serious safety implications if the level rose beyond a critical point. The basic system is as follows:-

1) On the lower part of the vessel is a level transmitter feeding into the process computer. The signal from the level transmitter provides:-

- Control of the valve which itself controls the liquid in the vessel
- Level indication for the process operator
- An alarm set at a prescribed value, eg, 80% level. This alarm operates through the process computer software (ie it is 'software-based').

2) Above the level transmitter is a single level switch which is hardwired into an alarm.

3) Above the single level switch are three level switches feeding into two programmable controllers (PC 1 and PC 2). Within each PC '2 out of 3' voting takes place. The output of each PC goes to the trip valve and also to a trip alarm.

4) A trip valve can also be operated by direct means from a stop button which is hard-wired.

8.3 Determination of safety related systems

In the context of the process plant indicated in Figure 6; the way in which the **SAFETY-RELATED SYSTEMS** are determined is described below (see Figure 7).

From a *control and protection* viewpoint, there are essentially four systems.

1) As the level of liquid in the vessel rises, (to, say, the 80% level), *Alarm 1* is raised. The plant has been so designed that the operator can, on receipt of *Alarm 1*, take corrective action to prevent the liquid level from rising any further and, in fact, to reduce the level. *This is system 1.*

2) If, however, the operator cannot control the liquid level or, the process computer is incapable of taking the corrective action, even though the operator has performed correctly, the liquid level may rise until the hardwired *Alarm 2* is raised. Even at this point, the operator should still be able to take corrective action to stop the liquid level rising any further. *This is system 2.*

3) If the operator cannot control the liquid level and the liquid continues rising, it will then activate, via the three level switches and PC 1 and PC 2, the trip valve to automatically bring the plant to a safe state. *This is system 3.*

4) Should system 3 fail, then the operator can bring the plant to a safe state by operating a hardwired system activated by a shut-down button. *This is system 4.*

In this particular case, the *safety-related systems are systems 3 and 4.* These two systems provide the requisite level of safety, taking into account factors such as the level of hazard involved and the number of demands made upon *systems 3 and 4 by failure of systems 1 and 2.*

It can be seen that whether a system is **SAFETY-RELATED** is determined by the particular circumstances and many factors need to be considered. The role of the operator in *systems 1 and 2* is very important, since efficient and correct operator action will minimise the **DEMANDS** on the two protection systems (*systems 3 and 4*). This has an important bearing on the level of integrity required of *systems 3 and 4* in order to achieve an acceptable **HAZARD RATE**.

As indicated previously, the guidelines apply to the **TOTAL CONFIGURATION OF SAFETY RELATED SYSTEMS** - in this case *systems 3 and 4*.

The identification of the *safety related systems* is Step 2 in the design and assessment framework (see Figure 4). Steps 4-6 then need to be carried out. Step 3, the determination of the required level of safety integrity, is a vital step prior to any assessment. The HSE guidelines provide guidance on how this can be obtained if no established safety integrity criteria *for the application* exists. The process plant control and protection systems indicated in Figures 6 and 7 is an example of *separate control and protection systems*.

9 SAFETY CASES FOR CIMAH

The **Control of Industrial Major Accidents Hazards (CIMAH) Regulations** requires under Regulation 7,[8] that certain manufacturers (defined in Regulation 6) prepare a written report - commonly called the *'safety case'* and to submit it to HSE. Schedule 6 of the Regulations specifies the information to be included in the safety case. In essence, the safety case is a demonstration that the manufacturers activity is being carried out safely.

The HSE guidelines on PESs, provide a design and assessment framework for the systematic examination of equipment in which a PES plays a role in the achievement of the required safety level. The guidelines address all aspects relevant to both random hardware and systematic failure causes. The method of approach adopted in the guidelines to both design and assessment (in particular the use of **Steps 1-6** and the **checklists** (see Figures 3 and 4) could very usefully form the basis of the preparation of safety cases required by CIMAH. The adoption of a common framework, including the use of the checklists would be of benefit to both manufacturer and HSE. It should, for example, greatly facilitate communication between HSE and the manufacturer.

10 FUTURE DEVELOPMENT: GENERAL

Guidelines development will need to take place on both a generic and