NON SELF ACTING SAFETY SYSTEMS FOR THE PROCESS INDUSTRIES.

W.S.BLACK.(B.P.INTERNATIONAL) presented on behalf of E.E.M.U.A.

Self acting mechanical devices or systems may not be adequate in all cases to prevent hazards on Process plants or may not be economically viable. Under these circumstances non self acting systems may be used as the primary protection against dangers to personnel. The Health and Safety Excutive in 1987 published General Guidelines on Programmable Electronic Systems in Safety Related Applications. This paper describes how some of the principles in the H & SE Guidelines may be applied to the systems used in the Process Industry. The principles applied are those that have been outlined in the EEMUA publication to be published in the near future for use by the Process Industries.

KEY WORDS: SAFETY, PROTECTION, INSTRUMENTATION, CONTROL, CATEGORISATION, MICROPROCESSOR.

INTRODUCTION.

THE EEMUA ORGANISATION.

The Engineering Equipment and Materials Users Association -EEMUA - is an organisation of substantial purchasers and users of engineering products. EEMUA members include leading representatives of both the private and public sectors, from the energy and process industries. EEMUA is concerned with the design, installation, operation and maintenance of the engineering plant used in members' business operations.

The Association aims to reduce members' costs by providing the opportunity for them to share resources and expertise in influencing the environment within which their engineering activities are carried out. EEMUA supports the British Standards Institution, works with other Institutions, Associations, Government departments, regulatory bodies and the Confederation of British Industry. EEMUA is also actively involved with other standards making bodies, both national and international, such as the American Petroleum Institute.

Work which is carried out in-house by members alone, or with the help of other organisations, may lead to the production of Association publications. These are prepared primarily for the use of members, but are sometimes offered for wider circulation. Such publications may also be submitted to the British Standards Institution as the basis for a British Standard.

HISTORY.

The advances in the technology and reduction in the cost and size of

electronic systems have led to the increased use of such systems throughout industry in the last decade. In 1981 EEUA (one of the predecessors of EEMUA) published Handbook 38, 'Guide to the Engineering of Microprocessor based systems for Instrumentation and Control'.(EEMUA Publication No 123). In the same year the HSE published ' OP2 - Microprocessors in Industry', which was aimed at safety, mainly in the context of machinery applications.

In 1983, the members of EEMUA identified a need for a further document concerned with the safety aspects of electronic systems within process plant. It is worth noting the change of emphasis away from the words 'microprocessor' or 'programmable' to the more broad ranging 'electronic'. This is based on the Members' view that many of the problems associated with the hardware of programmable electronics are common to non-programmable electronics and that it is becoming increasingly difficult to define the contents of a particular digital electronic instrument as microprocessor based or not. Hence comparison between programmable and non programmable systems is becoming less valid.

Early in 1984 the H & SE announced that it proposed to publish Guidance on the Safe use of Programmable Electronic Systems. Accordingly EEMUA decided to suspend work in this field until the H & SE Guidance had been published. EEMUA received a draft copy of the H & SE Guidance notes and made comments to the H & SE.

The contact between H & SE and EEMUA was maintained during the development phase of the original H & SE draft and up to the publication of the final document.

The EEMUA/INC Committee and the H & SE believed that, because the coverage of the H & SE Document was so wide,it was necessary to provide more specific guidance for the Process Industry. A sub-committee was set up and a document produced to guide those engaged in the design, operation and maintenance of process plant.

THE PROCESS INDUSTRY.

The process industry has for many years been at the forefront of advances in electronic control. The first digitally controlled plants were in use in 1964. The physical size of process plants has been a continuous spur to the development of electronic control and reporting systems. The financial cost of downtime has meant that control system availability has been a major design criterion. The degree of hazard varies from plant to plant and so do the techniques for minimising the risk. One technique often used has been to separate the control system from the safety system.

In many cases the control system is designed to reduce the number of occurrences that may cause a demand on an ultimate safety system. Hence the safety-related contributions of a control system need to be identified.

The members of EEMUA believe that properly designed, maintained and operated electronic systems can increase the safety and availability of process plant in a cost effective manner. Particular examples of this have been in areas where programmable automation systems have removed operators from work areas with a previously high record of direct injury or long term health exposure risks.

ASSESSMENT OF APPLICATION REQUIREMENTS.

Design of any process plant or piece of equipment proceeds in a number of well defined steps. Initially the concept of the plant is studied to assess the way it will function and the safety, environmental and economic effects on the existing plant site. This initial broad brush review identifies the salient points of the working and operation of the plant. Among the most important items to be identified at this stage are the dangers to personnel, to the environment, and to plant and equipment arising from the new plant in both normal and abnormal operational modes.

Where possible dangers are identified, the next stage is to design the plant and its control systems to eliminate these possible hazards or to reduce them to acceptable levels. The safety systems and the modes of operation of the plant are studied by multi-disciplinary teams and, depending on the degree of hazard, the types of protection and control systems are selected and designed.

The degree of assessment of the designs will depend on the nature of the hazard and the size and complexity of the plant. The general advice in the EEMUA document is to separate safety protective systems from control systems, this substantially reduces the assessment work needed.

On small items of plant such as packaging machines, burner systems etc, there will be a tendency to use a combined system. These plants may be only updates of existing designs that have been in use for many years, and these systems need to be critically examined by a competent engineer to ensure that there are no safety aspects concerned before a decision is made that an assessment in line with the H & SE Guidance Note PES 2
(Ref 1) is unnecessary.

To decide the most appropriate design and the extent of the assessment needed it is helpful to divide the instrument and safety systems into categories according to application.

CATEGORY DEFINITIONS.

When designing process plant it is necessary to incorporate devices to ensure that the plant remains safe even under conditions of equipment failure or maloperation. In the majority of cases the required level of safety can be achieved by installing mechanical devices such as relief systems or direct acting electrical switches. In certain cases it may not be practicable to use mechanical devices or such devices may not be adequate alone to ensure safety, in which case additional protective systems may be required.

Systems required for the safe and reliable operation of the process plant may be divided into the following categories:

Category 0 System. A self acting mechanical device or system which is a protection against dangers to personnel. Examples include relief valves, bursting discs or containment.

Category 1 System. A non self acting system which requires an outside source of energy and which is a protection against dangers to personnel. Such a system may be necessary where self acting mechanical devices are not used or are not adequate acting alone. Examples include electronic, hydraulic, pneumatic and relay systems.

Category 2 System. A system which protects against the damage to the environment, damage to the process plant, loss of product or production.

Category 3 System. A control system which ensures reliable production and maintains the plant operation within operational limits.

The requirement for, and consequences of failure of the above categories are detailed in Table 1.

CATEGORISATION PROCESS.

A systematic review of the process is necessary to identify those instrument systems where failure to act or spurious trip would result in a hazard.

This review will involve process and operational engineers, system specialists and those engineers responsible for the mechanical integrity of the plant.

The review may be included with the normal Hazard and Operability studies such as recommended by the Chemical Industries Association.

Alternatively, it may be appropriate to have a separate review, the results of which are considered during the Hazard and Operability study. The latter is preferred since calculation to check mechanical integrity and relief valve capacity etc may need to be made and the full results should be available before the Hazard and Operability study takes place.
The review to establish Categorisation may involve rethinking or redesign of the ultimate protection system and these activities are inconsistent with the role of the formal Hazard and Operability study team.

Recommended steps in the review process are as follows:-

1. A line by line review of the process should be carried out. The normal variables of pressure, temperature, flow and level etc should be considered in turn to establish the abnormal conditions that occur under fault conditions.

2. A schedule should be prepared of all failures which may result in plant conditions beyond design limits. At this stage no credit should be taken or recognition given to any particular system of instrumentation. It is assumed at this stage that self acting devices (as defined in BS 5500 Appendix J) function according to design requirements.

3. The process conditions after failure should be determined.

4. Engineers responsible for the process and mechanical integrity of the plant should identify where conditions would be unacceptable for safety reasons.

5. Where the instrument systems prevent unacceptable conditions arising, designers should then consider if modifications can be made to the mechanical or process design that would make equipment design safe for the failure conditions. It should be stressed that the number of Category 1 systems should always be minimised. In deciding whether to use Category 0 or Category 1 devices for ultimate protection, designers should take into consideration the necessary detailed assessment required during the design and the subsequent procedures during maintenance if Category 1 devices are

used.

6. Any instrument systems necessary to prevent any unacceptable conditions arising should be listed together with the potential hazard. All aspects of the systems should be listed including sensors, logic and final element. A typical form which may be used for schedule purposes is attached.

CATEGORISATION EXAMPLES.

The categorisation principles may be best illustrated by considering the following examples.

Further examples of where Category 1 systems may arise in process plant are listed in Appendix 1. of the EEMUA document. Only examples frequently encountered are listed, and the list should not be considered as complete.

A Simple Example.(1).

A pressure relief valve is provided on a vessel containing a non-hazardous fluid under pressure to protect against rupture of the vessel.

Control and protection systems may be employed to start or stop the associated compressor to ensure that pressure is maintained at a level, within the design limits of the vessel, but below the pressure relief valve setting.

Whether or not the control or protection systems contain a PES, the document PES 2 does not apply provided the relief valve is adequate acting alone to assure the safety of the plant.

In the same category are mechanical overspeed bolts fitted on steam turbines and switches which directly remove primary power.

A Simple Example.(2).

A machine uses a Category 1 system to coordinate a large number of sequential processes at high speed.

The machine is equipped with a guard to protect the operator from the moving parts.

If a switch on the guard directly removes primary power from the machine immediately the guard is moved, then this is Category 0 protection, and PES 2 does not apply. It is important in this application to ensure that the Category 1 system does not interfere with the integrity of the ultimate protective device.

If, in order to reduce to reduce downtime, the direct removal of primary power by a switch is replaced by an ordered sequential stop controlled by a Category 1 system, then it has two functions :-

- The prevention of hazard to personnel by an instrumentation safety system. (Category 1)

- The prevention of unnecessary production losses by a protection system.(Category 2)

The relevant parts of the PES 2 and EEMUA guidance documents will apply in this case since a Category 1 application is involved.

A PES based example.

In this application, a vessel is being used in which a potentially dangerous exothermic reaction takes place.The vessel is equipped with pressure relief valve which is capable of protecting against some of the normally foreseen dangers but not against the abnormal high temperature situation. To deal with this abnormal incident, a PES system monitoring temperature and acting on the system to prevent danger is installed. (Cat 1 application).

This PES system would be subject to the procedures laid out in the PES 2 document, for in this case the relief valve is not adequate acting alone to ensure the safety of the plant.

SYSTEM SELECTION.

The systems required can be selected after considering the whole process control and protection facilities required for the plant and categorising the elements.

Selecting the most appropriate system will require close co-operation between engineers representing process, operations, maintenance, process control and instrumentation.

In selecting suitable systems for Category 1 consideration will need to be given to both EEMUA and H & SE Guidance documents.

When selecting the type of system to be used for Category 1, 2, and 3, consideration should be given to whether the systems should be programmable or non-programmable and if programmable, the degree to which software can be changed by the user. (i.e. variability).

The IEE 'Guidelines for the documentation of software in industrial computer systems' classifies programmable systems into three types:

Fixed Program System. This type is typical of the proprietary single function system usually available 'off the shelf'. An example of this type could be a three term controller which emulates, and in some cases is interchangeable with it's analogue equivalent.

Limited Variability System. This type of system is packaged typically as a Programmable Logic Controller, Distributed System or multivariable controller.

The user is usually provided with the capability of configuring the system to his specific requirements without the need of the specialist skills of computer programmers.

Full Variability System. This is the type of system which will be, typically, minicomputer based with an operating system which provides system resource allocation and a real-time multi-programming environment. The system is tailored for a specific application using high level languages or an assembler by a professional specialist.

For any application the choice of system will depend on the facilities for

present use and future development. The aim should be the use of a system of minimum variability for the following reasons:

a) Programming effort will be minimised.
b) The need for specialist resource will be minimised.
c) Maintenance staff will need less training.
d) Less risk of system faults and systematic errors.
e) Testing is minimised.

Table 2 shows how the functionality typically required for the different types of application can be efficiently achieved with systems of differing variability. Users with a high level of skill and experience in programmable systems may be able to implement systems with higher degrees of variability. Users with little or no experience in programmable systems are advised to reduce to a minimum the variability of the systems used.

REVIEW METHOD.

After categorising the applications and defining the control and instrumentation to be used, the arrangements should be subjected to some form of review process. Specialist knowledge will be needed for this review and an appropriate group should be established for this purpose.

The group should comprise operations staff and process engineers familiar with the process requirements and control specialists familiar with the failure modes of control equipment. To ensure some independance, at least one of the control specialists should not have been involved with the design of the safety related systems. The examination may take place in stages coinciding with the normal process reviews. An early review will be necessary to confirm the overall design philosophy. A later review will normally be needed after the vendors have been selected and the design is at an advanced stage to establish that the initial philosophy has been implemented sucessfully. Continuity with the normal process review is essential and may be provided by a process or operations member attending both reviews.

The overall philosophy of control and instrumentation should be considered to establish the equipment used satisfies the basic elements defined in PES 2, viz:

Configuration. The aim is to ensure the arrangement of systems is appropriate to the process and that deviation from Codes of Practice and industry guides are acceptable.

Reliability. The aim is to ensure that reliability analyses have been carried out appropriate to the requirements of the system.

Quality. The aim is to ensure that quality consistent with the necessary reliability is achieved at all stages of design, manufacture, installation and test.

Before commencing work the review team should gain a reasonable understanding of the dangers associated with the process and the control and instrument systems used.

Clear terms of reference and reporting requirements should be made known to the team before work commences.

From knowledge or the risks and the systems used, the team should agree the extent of the examination at each stage and the relevant questions which need to be considered. The questions listed below are typical and should be used to stimulate further enquiry. The style should be open such that further matters can be considered when relevant.

The check lists in the PES 2 document should also be consulted and formal check lists may need to be completed for some applications.

Actions and recommendations from each review should be considered at subsequent stages and plant start-up should not take place until the team consider the systems to be in a suitable stste to ensure safe commissioning and operation.

General.

1. What categories of systems are required for the process applications. ?

2. What procedure has been used for categorisation.?

3. Is the variability of all systems proposed appropriate to their application.?

Category 1 Applications.

4. What are the consequences of failure of the Category 1 systems.?

5. What configuration of systems are used for Category 1 applications.? On what basis has the configuration been decided and is it consistent with the consequences of failure.?

6. Is the reliability of the Category 1 systems appropriate for the application.?

7. What Quality Assurance procedures are to be applied to the Category 1 systems during design, manufacture, software development, installation, testing and maintenance.?

8. What failures of the Category 1 systems are reasonable foreseeable and how are they detected.?

9. Are the Category 0 and 1 systems adequately designed for all reasonably foreseeable failure modes of the Category 2 and 3 systems and the plant.? Are they adequate for the demand rate arising from failure of the Category 2 and 3 systems.?

Category 2 and 3 Applications.

10. What are the reasonably foreseeable failure modes of the Category 2 and 3 systems and how have they been determined.?

11. What features of the Category 2 and 3 systems are redundant.? The review team should consider the following:

12. What loop allocation philosophy has been used.?

13. What evaluation work has been carried out to establish that the hardware and system software are fit for their purpose.?

14. What Quality Assurance procedures have been used for the Category 2 and 3 systems during design, manufacture, software development, installation, testing and maintenance.?

15. What success/failure criteria have been used in calculating the reliability of the Category 2 and 3 systems.?

16. What reliability has been predicted for the Category 2 and 3 systems.?

Operation.

17. How is information on normal and abnormal plant conditions presented to the operator.?

18. How is information on fault/failure conditions presented to the operator.?

19. What procedures are defined for the operator in the event of system failure.?

20. What training has the operator received on the system that will enable him to respond to normal and fault conditions on the plant and the systems.?

21. What defeat facilities are available to the operator and how is defeat status indicated/logged and what procedures are used.?

Maintenance.

22. What maintenance procedures have been defined as necessary during routine periodic operation and for failure conditions.?

23. What training has been given to maintenance engineers.?

24. What spares are necessary to ensure the mean time to repair of equipment is acceptable and how are the spares controlled.?

25. What maintenance assistance is available to the operations staff during the day, night and weekends.?

26. What facilities are available for testing.?

27. What test intervals have been defined for each system and what testing procedures have been defined.?

28. What test equipment is necessary and what procedures are defined for routine calibration of the test equipment.?

29. What is the effect of hand held radios and what restrictions are placed on their use.?

Modifications.

30. Have modification procedures been defined for the Category 1, 2 & 3

systems.?

31. What levels of authority are necessary for modifications to each Category of the system.?

32. How is it to be assured that modifications to the systems do not invalidate the data upon which the design of the safety system has been basewd.?

33. How is access to the system for making changes in the software and configuration controlled and how is access by unauthorised personnel prevented.?

Environmental.

34. Is the equipment suitable for the environmentwithin which it is to be placed.? The following should be considered.

Temperature.
Humidity.
Vibration.
Area Classification.

35. Is the environment suitable for operations and maintenance staff.? The following should be considered.

Temperature.
Humidity.
Ventilation.
Lighting.
Noise.
Hazardous or toxic gases.

IMPLEMENTING CATEGORY 1 SYSTEMS.

Where Category 1 systems are identified, then such systems should be engineered in accordance with the EEMUA Guidance document and PES 2. Where the system used is non programmable then certain aspects of the EEMUA document and PES 2 will not be relevant, such as the requirements for software quality. Other requirements in the document relating to hardware, quality and reliability will apply equally to both programmable and non programmable systems.

It is important that any Category 0 or 1 system should:-

1. be of sufficient reliability to deal with the number of demands for operation arising from the Category 2 or 3 system or from the plant itself:

and

2. adequately cater for all reasonably forseeable failure modes of the Category 2 or 3 systems together with all reasonably forseeable failure modes of the plant itself.

The requirements relating to the design, specification, procurement, of

Category 1 systems are complex. It would be impossible in a paper of this length to describe these requirements without simplifying them to a misleading extent.

The reader is referred to the EEMUA and HSE publications for the full requirements.

IMPLEMENTING CATEGORY 2 & 3 SYSTEMS.

Where Category 2 & 3 systems are used which are programmable their failure rate and mode can have an important effect on the safety that can be achieved by Category 0 or 1 systems.

the Category 0 or 1 system must be adequate to deal with the demand rate and all reasonably foreseeable failure modes of the Category 2 and 3 system or the plant itself.

The frequency of failure in the dangerous direction of the Category 2 or 3 systems should be no higher than that of an equivalent conventional system. The factors which need to be considered and the procedures by which this can be established are discussed below.

Failures of Conventional Systems.

The majority of component failures result in low or zero signal levels. Normally control, protection and safety systems are designed such that a low output state drives the plant to a safe state. The safe state is thus assured when common mode failures occur such as power supply or air supply failures.

Where conventional analogue control systems are used, failures are generally assumed to be single and random to the higher condition or multiple and low caused by common mode failure of power. The way in which process engineers size relief capacity is often based on this assumption.

Failures of Programmable Systems.

With programmable systems, failures of a single output to the unsafe direction may be caused by failure of input or output electronics of individual channels. The failure rate of individual outputs needs to be evaluated but is unlikely to be higher than conventional systems.

In programmable systems, failure to the unsafe direction of more than one output may be caused by either random hardware faults or systematic failures in system or application software.

Random Hardware Failures.

Prior to application, control systems should be assessed to ensure that simultaneous failures to the high state will be infrequent.

In some programmable systems, the design of input or output modules or power supplies may be such that a single failure may cause more than one output to fail to the high condition at the same time. Often redundancy techniques are used such that multiple failures are prevented by switching to standby devices. Even where this is the case, the probability of simultaneous failure to the high condition of more than one output is finite and needs to be considered.

The assessment to ensure that failures do not lead to unacceptable demand rates on the ultimate protection may be qualitative. Failures within the control system should be reviewed to establish what warning messages are given and what action taken on system failures.

Where the consequences of failure are severe a more quantitative approach may be appropriate as detailed below.

The procedure below is recommended at an early stage in the design of the control system.

1. Ascertain system failures which may lead to more than one output failing to the unsafe condition simultaneously.

2. Define the redundancy or standby arrangements considered necessary for reliable and safe operation.

3. Determine the probability of simultaneous failure to the unsafe direction of more than one output. Probability may be expressed in a number of ways, mean time between the event occuring expressed in years enables comparison with other hazards such as vessel failure.

4. With the failure rates calculated, consider with process engineers the strategy for allocating loops to the system. A grouped or distributed strategy may be adopted and this is considered below.

5. With the Process engineers agree the allocation of control equipment to the process. Even where the probability of failure is low, it is often good practice to ensure that critical combinations are not within the same control device or subsystem.

Faults in Application or System Software.

The probability of a software fault simultaneously affecting more than one output is difficult to predict. Conventional reliability analysis cannot be used since the problems which occur relate to the design of the software and are systematic by nature. In assessing the suitability of a process control system, the following points should be taken into consideration:

1) System Software.

In using programmable electronic systems for a process control application, different types of system software may be used depending on the control system selected.

The IEE publication 'Guidelines for the documentation of software in industrial computer systems.' defines three types of programmable systems as follows:

Fixed Program System. This type is typical of the proprietary single function system usually available 'off the shelf'. An example of this type could be a three term controller which emulates, and in some cases is interchangeable with it's analogue equivalent.

Limited Variability System. This type of system is packaged typically as a Programmable Logic Controller, Distributed system or multivariable controller.

The user is usually provided with the capability of configuring the system to his specific requirements without the need of the specialist skills of computer programmers.

Full Variability System. This is the type of system which will be, typically, minicomputer based with an operating system which provides system resource allocation and a real-time multi-programming environment. The system is tailored for a specific application using high level languages or an assembler by a professional specialist.

For any application the choice of system will depend on the facilities for present use and future development. The aim should be the use of a system of minimum variability for the following reasons:

a) *Programming effort will be minimised.*

b) The need for specialist resource will be minimised.

c) Maintenance staff will need less training.

d) Less risk of system faults and systematic errors.

e) Testing is minimised.

An indication ofthe most appropriate system to use for different applications is indicated in Table 2.

In general for regulatory control of process control software, systems with limited or fixed variability will be used. The extent to which full variability software system is used is generally minimised since this reduces the potential for systematic errors in the application programs.

Distributed system and PLCs are available with a wide range of control algorithms which can be configured and conventional programming is not required. The need to use full variability software can often be eliminated.

With normal methods of system software development new systems are unlikely to have fault free software. Faults range from significant to trivial and may occur frequently or seldom. With a more mature software system, remaining faults are likely to be trivial and infrequent. It is rare for any system with complex algorithms to be fault free.

Before using any control system on potentially hazardous plant the system software needs to evaluated. Alternative means are as follows:

a) Formal evaluation.

The proposed system may be installed connected to some form of simulator. The simulator could be generic but may be designed to simulate an important process function which will be required for the particular application. The performance of the system should be checked against all common failures expected in the system and the process.

Facilities for such testing are available at SIRA who have considerable experience of evaluating control systems.

Where systems have been evaluated it is important to ascertain the test

method and specification used. Limited evaluations are often performed which test a system against the manufacturer's specification only.

b) User experience.

Vendors can normally arrange visits to users who have had the proposed system in operation for a period of time. Discussions should take place with the users' operations and maintenance staff. Care is needed before accepting another user's view that the system performs well. If his application is monitoring only, or batch or on a small plant, then some problems may not be significant in his application which may be unacceptable in the proposed application. The version of systemsoftware used and the developments since the system was installed need to be established.

2) Application Software.

Errors in application programming leading to simultaneous failures of more than one output to the unsafe condition can be avoided providing the following principles are applied:

The best system software for the application should be selected. System software which will demand the development of new algorithms should be avoided. Systems which have a wide range of proven algorithms at the configuration level are preferred.

Well defined procedures should be used during the design and implementation of the application software. The general principles laid down in Section 5 and 6 of the EEMUA document apply equally to the development of application software for control purposes.

Where set-points are downloaded from supervisory or operating programmes, then the set-point values or rates of change should be limited to minimise disturbance to the plant.

Change and modification procedures should be used during design implementation and use. The general principles laid down in Section 7 of the EEMUA document apply equally to application software for control purposes.
The application software should be subject to comprehensive testing to ensure it fulfils the functions required. The general principles laid down in Section 9 of the EEMUA document should be applied.

LOOP ALLOCATION STRATEGIES.

At an early stage the way in which equipment is allocated to process areas needs to be decided. Process engineers and operations management need to appreciate the failure modes of the system and the predicted reliability before considering the strategy to be used.

Alternative strategies which can be applied are as follows:

Outputs Distributed.

In this strategy loops which may fail simultaneously are not allocated to the same process unit. Where this is the case, relief systems for the separate process units may be designed assuming failures are single and

random.

Where the relief systems are common to more than one process unit, then the failure modes need to be considered when the facilities are designed. Examples include common flare or treatment facilities.

Where outputs are distributed, a single failure can cause process problems in more than one area and can lead to a high demand on the operator.

Faults may be difficult to diagnose and due to their widespread nature may be more more difficult for an operator to deal with.

Outputs Grouped.

In this strategy outputs which may fail simultaneously are allocated to the same process unit. In designing the relief systems the failure rate and mode needs to be considered.

Where the outputs are grouped, a single failure is likely to cause direct problems in one process unit only. The operator is more able to handle problems which are restricted to a single process unit. Often all failed loops are presented on the same graphic or group display. Faults are easier to diagnose and are less likely to lead to general disruption of the whole plant.

The strategy adopted will depend on the following:

a) The probability of simultaneous failure. With well designed systems with redundant features, the probability may be small compared with the process risk from conventional failures. When set against generally accepted safety levels the risk may be low enough to be acceptable.

b) The characteristics of the process. The distributed strategy may be the most suitable for processes which are simple and slow acting. Effective operator action in the event of a failure may allow production to continue with some loss of quality or throughput until the failed units have been repaired. Where processes are highly integrated or fast acting the grouped strategy may be appropriate. Effective automatic action in the event of failure may prevent total shutdown by forcing parts of the process to the total reflux or standby modes. Production will be able to be restarted with minimum effort and time delay after repair of the failed unit.

TABLE 1.

	Category of Application.	Type of System.	Purpose.	Consequence of Failure on Demand.	Requirements.
SAFETY SYSTEM	0	Self acting devices such as relief valve, bursting disc or containment.	Safety.	Hazard to persons.	BS 5500 Appendix J BS 6759 BS 2915 BS 1123
		Where Category 0 devices are installed and their capability and integrity alone is adequate to ensure the safety of the plant then Category 1 devices will be unnecessary.			
	1	Instrumentation Safety system.	Safety.	Hazard to persons.	Aspects of these safety systems and their configeration, reliability and quality will need to be assessed in accordance with the EEMUA document and PES 2 to ensure an adequate level of safety is achieved.
		Category 1 Systems will be necessary where mechanical devices cannot be used or are not adequate acting alone to ensure the safety of the plant.			
NON SAFETY SYSTEM	2	Protective System.	Economic or environmental	Loss of production and adverse effect on surroundings.	The reliability of the systems should be comparable to conventional analogue systems so that demands on the final protection will be limited. Further guidance on the degree of assessment necessary are given in the text.
	3	Control system.	Reliable production to an acceptable quality.	Loss of production and possible demand on 0,1 or 2 system.	
		If programmable systems are used for the Category 2 or 3 systems then a full assessment of the systems according to the HSE or EEMUA Document will be unnecessary.			

TABLE 2.

SYSTEM APPLICABILITY.

SYSTEM.	SELF ACTING.	NON PROGRAMMABLE.	FIXED PROGRAM.	LIMITED VARIABILITY	FULL VARIABILITY.
ULTIMATE SAFETY CATEGORY 0.	PREFERRED.	---	---	---	---
ULTIMATE SAFETY CATEGORY 1.	---	PREFERRED.	ACCEPTABLE.	ACCEPTABLE.	AVOID.
PROTECTION CATEGORY 2.	---	PREFERRED.	PREFERRED.	ACCEPTABLE.	AVOID.
REGULATORY CATEGORY 3	---	ACCEPTABLE.	ACCEPTABLE.	PREFERRED.	AVOID.
SUPERVISORY CONTROL	---	AVOID	AVOID.	PREFERRED.	ACCEPTABLE.
INFORMATION.	---	AVOID	AVOID	ACCEPTABLE.	PREFERRED.