P.E.S. - AN OPPORTUNITY FOR BETTER SAFETY SYSTEMS

A.S. Fulton, M. Inst. M.C. *
Dr. D.J. Barrett, C. Eng., M.I. Chem. E.*

Programmable electronic systems (P.E.S.) are established as effective and reliable solutions to control problems in every kind of process. There is, however, caution and reluctance in their use for safety related functions. The paper argues that there is a significant area of application, typified by the smaller scale batch process operated by a medium to small company, where the safety functions can be more effectively and reliably fulfilled by P.E.S. The advantages of such an approach and the obstacles to be overcome are examined.

Keywords: P.E.S., safety, reliability, software, batch.

INTRODUCTION

Programmable electronic systems (P.E.S.) are indisputably established as the best available technology for control of a wide range of chemical processes, whether hazardous or not. There are many reasons behind the successful development of the technology, but two in particular are relevant here.

The first concerns reliability. In the author's experience, control systems incorporating P.E.S. maintain their original standards of performance with higher reliability than the conventional, discrete loop control systems they replace. The P.E.S. itself is inherently more reliable, and is less tolerant of degraded performance from sensors, control elements and other equipment in the loop. The system therefore tends to operate at or near its original performance or not at all. Higher standards of maintenance are necessary to keep the plant in operation, and are therefore made available. This contrasts with conventional, discrete-loop systems whose performance typically degrades with time until a significant proportion of the loops are out of commission.

The second reason is that control systems using P.E.S. are a better match for the control requirements of the process. This arises partly from the inherent power and flexibility of the P.E.S., and partly because the implementation of the control strategy using a "configurable" system is more comprehensible to the process engineer. He can therefore influence it more directly than he could with conventional systems where his requirements have to be translated and implemented by instrument engineers.

* Corporate Engineering Department, Albright & Wilson Limited

Both these features, reliability and capability to match the needs of the process, are also important requirements of safety systems. In particular a P.E.S. is much better suited to complex functions of control or safety than a conventional hard wired system. As the complexity of the function required increases, conventional hard wired systems become less effective because the increasing number of items of equipment and their interconnections introduce much greater problems of unreliability and opportunities for error. The reliability of the P.E.S., on the other hand, is little affected by the complexity of the task it is performing. In the case of safety systems, implementing complex functions with hard-wired systems results in a high frequency of spurious trips, which seriously degrade the validity of the system. In addition, human factors considerations, in particular the need to retain the credibility of the safety system with process operators, can be incorporated more effectively if P.E.S. are used. In practice, however, the use of P.E.S. for safety-related functions, other than very specialised dual or triple redundant systems, is discouraged. For example, the Health and Safety Executive's Guidelines, (Ref. 1) recently published in draft, require equipment used in safety systems to be subjected to reliability assessments. Techniques for such assessments such as fault tree analysis, synthesising a reliability figure from component level data, are available and feasible for simple hard wired systems, though the degree of reliance which should be placed on the result is a matter of some debate. However, the scale of work involved in such an assessment of a P.E.S. is well beyond the resources of all but the largest companies, and P.E.S. are therefore ruled out for safety systems unless they are backed up with hard wired systems. In simple terms, therefore, while we believe P.E.S. technology to be reliable, we cannot in practice measure or predict its reliability or its modes of failure, and we will therefore not use it for safety systems without hard-wired back-up.

The purpose of the paper is to question some of the assumptions which lie behind this reasoning, and to suggest that the other benefits of P.E.S. for safety systems may be great enough to outweigh this shortcoming, or that at least considerable efforts to eliminate this problem will be well worth while.

DISCUSSION

The overall system view

A safety system consists of many constituent parts. It can be represented as a closed loop with the following elements (see Figure 1):

Process characteristics
Process measurements
Logic or computation which acts upon process measurement data to produce outputs.
Control elements which use those outputs to act upon the process.

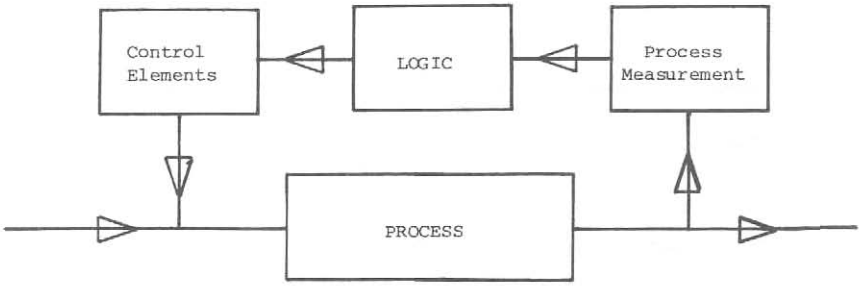

Figure 1

The question under discussion is whether the element labelled "Logic" should be implemented with a P.E.S. or by hard-wired equipment, typically relays etc. Comparisons between these two approaches have tended to be dominated by the question of the reliability or integrity of the equipment used and the extent to which it can be predicted. Prediction of the reliability of a P.E.S. is inherently more difficult, particularly because its modes of failure are much more complex and hence unpredictable.

The result is the familiar preference for hard-wired systems for safety functions. As described earlier, however, hard-wired systems do not perform complex functions well, because frequent spurious trips degrade their performance. The conventional solution to the problem therefore is to simplify the safety function to the point where hard-wired systems can be effective. This approach is often entirely acceptable, but there are cases which are significant in number and importance where simplifying the safety functions in this way causes a serious reduction in the degree of protection which the system provides.

In general, the safety logic required for continuous processes operating under steady state conditions tends to be simple. Detection of potentially hazardous situations is achieved by comparing critical process parameters with predetermined limits which do not vary with time. Transgression of any of these limits initiates automatic actions to render the process safe. These actions also tend to be simple; a shut down of the process is the most common. This can be represented as a target operating condition surrounded by an envelope of permissible deviations corrected by normal control actions. Deviations outside this envelope initiate a plant shut down.

Hard-wired logic imposes few limitations on safety systems for processes of this type. There are, however, many hazardous processes in which operating conditions are not constant in time. Batch processes, and continuous processes in a start-up phase are examples. In particular the detection of potentially hazardous situations is greatly complicated because safety limits vary with time or with progress through a batch, and often instantaneous measured values of process parameters provide inadequate information for such detection. In many cases, safety is assured by preventing certain actions or operations taking place at the wrong stage of the batch cycle, while permitting them at other times.

The following examples illustrate some such cases.

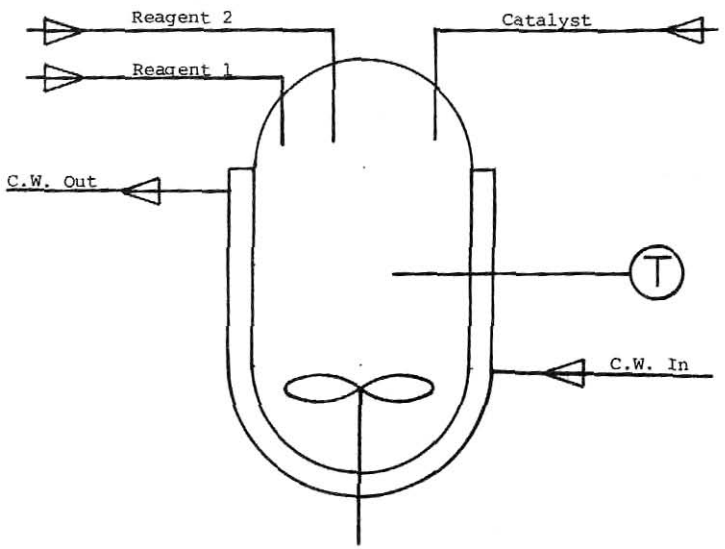

Figure 2

Exothermic Batch Reaction

Outline Batch Cycle

1. Charge predetermined quantity of Reagent 1 to the reactor.
2. Start the agitator.
3. Add predetermined quantity of catalyst.
4. Add Reagent 2 at a rate determined by the cooling capacity.

Potential Hazard

If reaction does not start when Reagent 2 is added initially, an excessive quantity of unreacted material can accumulate. If reaction does then start, the heat evolution may be greater than the maximum cooling capacity, leading to uncontrolled runaway reaction.

Safety System

A conventional safety system using hard-wired components would be initiated by a high temperature in the reactor causing all feeds to be shut off and maximum cooling applied. In the situation described above, this would be inadequate, because excessive unreacted material would already be present.

A P.E.S. could provide more effective protection by calculating a continuous balance between the theoretical heat of reaction of the material added and the measured heat removed by the cooling system. Discrepancies between these could be used to shut off feeds well before any temperature rise could take place.

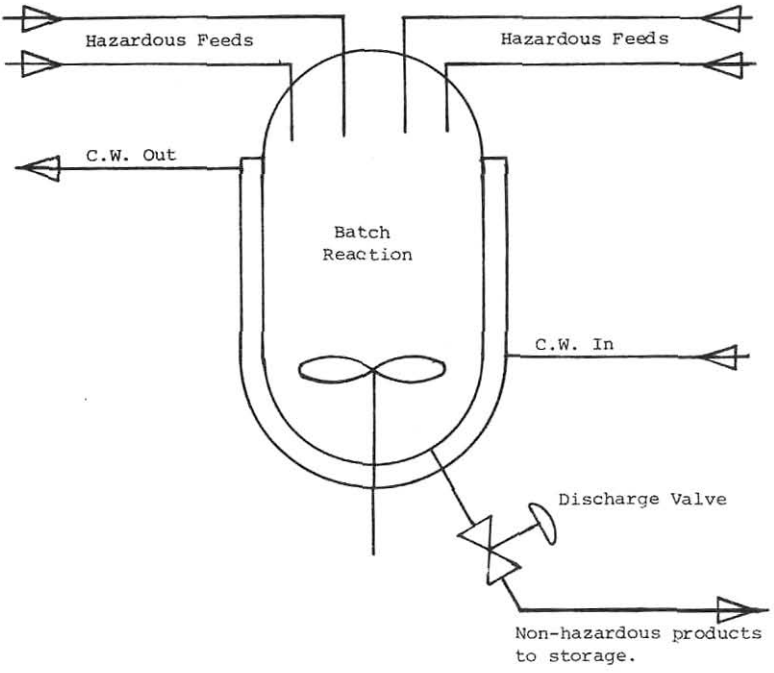

Figure 3

Process
A batch reaction takes place which converts hazardous raw materials (toxic, flammable, etc.) to a non-hazardous product.

Safety
The primary safety function is to ensure that the discharge valve is not opened until the reaction cycle is complete, and the reactor contents are fully converted and therefore safe to discharge. This function can only be carried out effectively by monitoring the progress of the batch sequence control, and releasing the discharge valve interlock only when all the prerequisite stages of the batch cycle have been properly completed. This requires the logical capability of a P.E.S. Conventional interlock arrangements, such as prohibiting the opening of the discharge valve until the reactor pressure drops below a predetermined value, are subject to incorrect operation under abnormal conditions and are therefore less effective.

Other Considerations
This process, in which hazardous raw materials are converted to non-hazardous products, poses problems for conventional safety systems in another way. The normal action of a safety system, on detecting a

malfunction during a batch, is to stop the reaction and shut down the process. In this case, the safest course of action, whenever possible, is to continue the reaction to its conclusion, because recovery of partially reacted hazardous materials poses greater problems of safety than conversion to non-hazardous products as the process is designed to do. Spurious operation of a safety system therefore causes not only nuisance and loss of output, but introduces new problems of safety. The flexibility of the P.E.S., allowing a better match between the safety functions designed and the needs of the process, can contribute significantly to reducing the likelihood of spurious operation of the safety system.

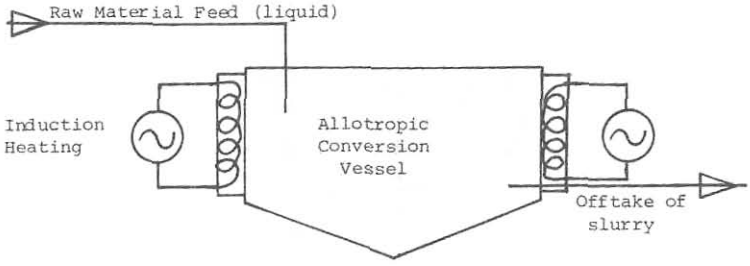

Figure 4

Process

The purpose is to satisfy a variable rate demand from the downstream process for a slurry of the converted solid allotrope in the liquid raw material. Conversion is effected by induction heating of the vessel, and the rate of conversion is dependent on the temperature of the vessel.

Hazard

If conversion proceeds too rapidly and the ratio of the solid allotrope in the vessel exceeds a safe limit, the conversion process will run away, resulting in solidification of the contents of the vessel. Recovery from this situation involves hazardous manual work to dig the vessel out. In addition, direct measurement of the slurry solids content can only be done by sampling the vessel contents and laboratory analysis. The sampling procedure is inherently hazardous.

Safety System

The solution to the problem is to use a real-time model of the conversion process to simulate conditions in the vessel at all times. This model can be used to calculate a safe operating temperature, depending on production rate required, and to carry out a continuous mass balance over the vessel. The model can in fact produce a more accurate and reliable basis of control than manual sampling and laboratory analysis, while eliminating the hazards of sampling. A P.E.S. is clearly necessary to run such a model.

In the examples shown, detection of the original malfunction which gives rise to the hazard requires the flexibility and computing power of a P.E.S. A hard wired system which can only be triggered by the instantaneous value of one or more process measurements would be significantly less effective because it could only detect the subsequent effects of the malfunction, not the malfunction itself. While hard-wired systems of the required complexity could be designed to carry out the functions described, they would, as mentioned earlier, be excessively complex and therefore prone to spurious operation.

It has been shown, therefore, that in some processes at least, P.E.S. offers the capability to achieve a significantly better match between the safety system logic and the safety requirements of the process. There are four other ways in which the performance of safety systems can be improved by the use of P.E.S. These are the use of self-checking or automatic test facilities, the prevention of inadvertent alterations, avoiding communication errors in the design process, and human factors considerations.

Self Checking

The performance of a safety system depends on the correct operation of all its constituent parts. Process materials which are corrosive, prone to build-up, or otherwise difficult to handle pose formidable problems of reliable measurement and dependable operation of control valves, etc. These parts of the system are more likely to be the weak link in the chain than the logic element. The P.E.S. can make a useful contribution here. It is possible, for instance, to check for consistency between two or more measurements or detect measurement signals which indicate instrument faults, such as improbably high or low rates of change. The following example shows a case in which a test of virtually a complete loop of a safety system is carried out every batch cycle and a printed record of the success or failure of the test is available (Figure 5).

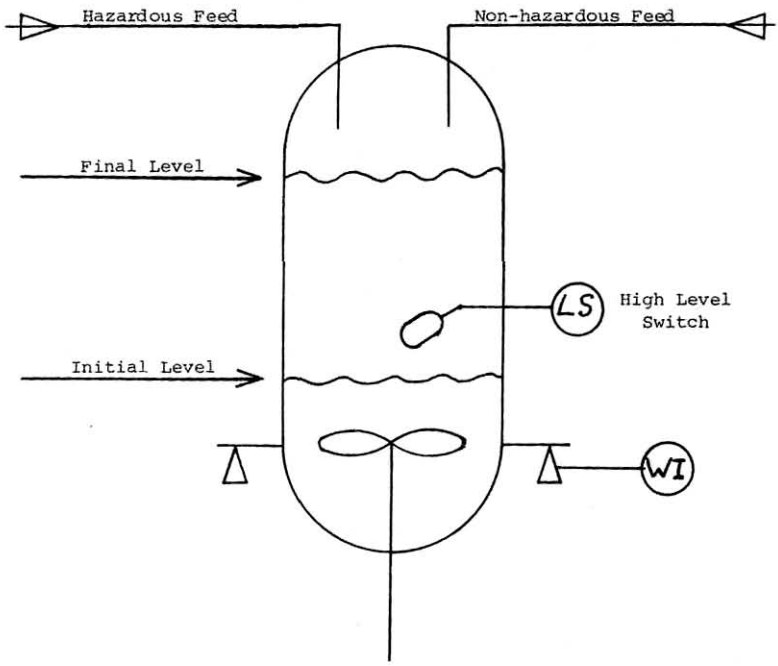

Figure 5

Process
Hazardous raw material is charged. Agitator is started and non-hazardous raw material is added gradually over remainder of batch cycle.

Safety
Primary hazard is an excessive charge of the hazardous raw material at the start of the batch. Two safeguards are provided to prevent this. The reactor is mounted on load cells, and the weight of material added is monitored. A level switch is also provided to detect an excessive volume after the initial charge. The weight and level both exceed the safety trip point of the initial charge during the remainder of the batch.

The advantage of the P.E.S. in this case is that it can monitor the weight measurement and the operation of the level switch and check them for consistency with other measurements such as totalised flows of raw materials every batch cycle. If such checks fail, it can then prevent the start of the next batch cycle until authoritative personnel have confirmed that inaccuracies or malfunctions have been corrected. The safety trip system is therefore subjected to a full functional test every batch cycle, which is an impossibly high test frequency for manual testing.

Prevention of inadvertent or unauthorised modifications

One of the objectives of maintenance of a safety system is to ensure that no modifications have been made which would prevent correct operation. Such modifications can arise either inadvertently, when restoring the system after testing for example, or by deliberate but unauthorised action, at a time of process malfunction for example. It is very difficult to check hard-wired systems for such modifications, and they are likely to remain unrevealed unless discovered by the regular proof test. The current programme of a P.E.S., however, can be checked more effectively, either by manual comparison of printed copies, or in some cases by electronic comparison.

Avoiding communication errors in the design process

The functions required of a safety system are always initially specified by the process engineer, because he has the expert knowledge of the potential hazards and the characteristics of the process. If a hard wired safety system is to be installed, the process engineer's specification must be translated by an instrument engineer into a design of interconnected logic elements such as relays, etc. Opportunities therefore arise for misunderstanding and misinterpreation of specifications between the two disciplines which are difficult to discover because the form of the solution, (relays, interconnection diagrams, etc.) is not comprehensible to the process engineer. By contrast, some P.E.S., known as configurable systems, are programmed in a manner which is comprehensible to process engineers with relatively little training. The logic used to implement the process engineering specification of the safety system can therefore be checked by the process engineer to eliminate at least some of the misinterpretations and errors of communication which may arise.

Human Factors Considerations

Experience has shown that it is most important to maintain the credibility of the safety system in the process operator's mind. The form and extent of the information presented to the operator about the actions taken by the safety system play a significant part here. The P.E.S. undoubtedly offers useful features of information presentation, and some systems provide the flexibility of data display to take full account of these human factors requirements.

In particular it is possible to design displays which present information to the operator about the cause of the trip or safety action, the actions taken, the effect on the process condition which initiated the action, and other relevant information to enable the operator to take the correct supporting action. If this information is presented in a comprehensible form at the time it is required, it will assist greatly in convincing the operator that the trip is a genuine one and assisting him to make better decisions at a time of stress. Conventional hard-wired systems are inherently poor at providing this sort of information, but P.E.S. technology in principle allows displays of this sort to be provided.

Alleviating the problem

The problem remains that identification of modes of failure and prediction of reliability of P.E.S. is a task beyond the resources of many users. There are however techniques of application which can considerably reduce the probabilities of dangerous failures. Some such techniques are outlined below.

1. "Active" systems

   It is often possible to design the safety system in such a way that it is required to be active and working correctly to enable the process to operate. By far the most common result of corruption of software or malfunction of the logical processing parts of a system is that it ceases to operate at all. A system which is required to be active to enable the process to operate is therefore "fail-safe" under these conditions. The integrity of the input and output hardware of the system is a separate issue, but it is often much easier to quantify the integrity of these parts of the system by other means.

2. Diversity of logic within the software structure

   Many P.E.S., designed for process control in the chemical and other process industries and typically known as "configurable systems", provide a variety of control and logical functions for the use of the application programmer. For example, Boolean logic functions, sequence control facilities and continuous feed-back control loops are typically available as software modules in the same system. Safety functions which are implemented using only one such type of module are susceptible both to malfunction of the system in servicing that type of module, and to programming errors. Both of these sources of failure can be greatly reduced by using two or more types of module to back each other up in the same safety function.

3. Common control and safety systems

   Where hard-wired systems are used for safety, especially in continuous processes, there are strong arguments for complete separation of the safety system from the control system. If a P.E.S. is used, however, there is a major benefit in implementing both control and safety functions and operator interface in the same system. The reason is that the failure mode of a P.E.S. which is of most concern is one in which software becomes corrupted or hardware malfunctions in such a way as to cause it to produce active output signals which it is not designed to do. (By contrast the failure mode of a hard-wired system of concern is an inactive one, in which it does nothing when it should do something). In an integrated system where control, operator interface and safety functions are all under the control of one system, it is almost inconceivable that the safety functions could fail without affecting the process control and operator interface. In other words it is most unlikely that the process will continue to run without the protection of a safety system. Additionally, if malfunctions do occur, operators are likely to notice faults in the display systems, which provides a further opportunity to shut the process down in safety.

CONCLUSION

In many ways, therefore, P.E.S. offer the possibility of safety systems which are more effective, better tested and less prone to errors arising from misinterpretation in design or unauthorised alterations. The obstacle to their use for safety functions without hard wired back-up, however, remains that their reliability is difficult to quantify, their modes of failure are unpredictable, and the integrity with which their software can be expected to perform under all circumstances is difficult to prove.

The remedy for these problems is not immediately available although some ways of mitigating them have been outlined, but the examples and arguments of this paper are intended to show the potential benefits of finding such a remedy. Some progress would be possible if co-operation between users were more effective. In particular, pooling of information on the performance of systems in real applications, and joint funding of rigorous functional testing of systems would be of benefit.

The term P.E.S. covers a wide range of systems. It is not suggested that large and complex process control computers which are custom built for each application can ever be used with confidence for ultimate safety protection. There are available, however, a variety of standard systems which are produced in volume and are in use in large numbers. It should be possible to gather data from users' experience and functional tests of these systems which would validate their use in safety applications.

It is suggested therefore, that the key to progress in the use of P.E.S. technology for safety systems with all its attendant advantages, is to concentrate on well-established modular systems whose application software is generated in a language comprehensible to process engineers, which are manufactured in volume to a standard specification. Such modules can then be tested for integrity and reliability as functional "black boxes". The results of such tests, it is suggested, carry more weight with users than conventional reliability estimates, synthesised from component level data. Meanwhile application software can be written in such a way that the probabilities of dangerous malfunctions are minimized.

NOMENCLATURE

P.E.S.

The term programmable electronic system, is used to describe a control system or module, normally containing one or more microprocessors, whose function is determined by loading a program, in whatever language. Data received from the inputs of the system is then processed according to the program, resulting in the generation of output signals to effect control actions on the process. The distinction is made between P.E.S. and hard-wired systems, in which electronic hardware and physical interconnections alone determine the logical or control function of the system. The characteristic of P.E.S. of particular relevance is that the microprocessor and other common electronic sub-assemblies are used for a variety of tasks at different times. The results of malfunctions of electronic items are therefore less predictable than in hard-wired systems, where each electronic item performs only one function.

Configurable systems

The term configurable system is commonly used to describe P.E.S. which can be programmed to perform the required control or logical function without expert computer software or programming skills. Effectively they are programmed in a special high level language which is comprehensible by a process engineer after relatively short periods of training and familiarisation. The programming process often involves supplying answers to sequential questions, or filling in the blanks in preformatted pages of information.

REFERENCES

1. Guidance on the safe use of programmable electronic systems - Parts 1, 2 and 3, published in draft by the Health and Safety Executive, June 1984.