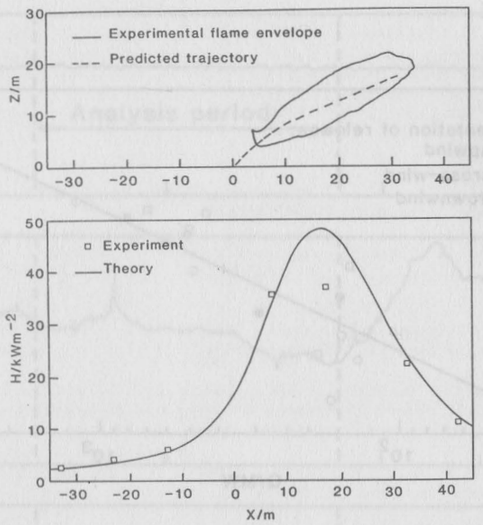


Figure 4.Comparison between theory and experiment for a release from the 300mm diameter vent stack

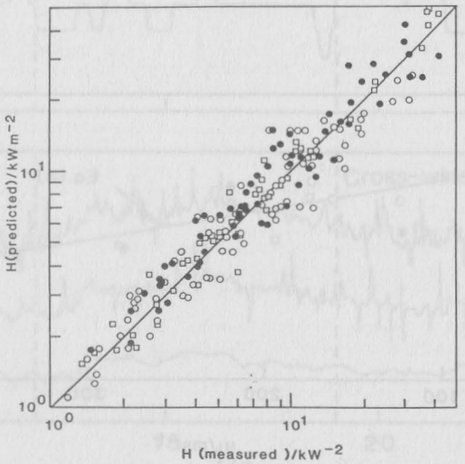


Figure 5. Comparison between predictions of incident thermal radiation and experimental data (key to symbols as figure 2)

PROCEDURES FOR THE SAFETY ASSESSMENT OF PROGRAMMABLE LOGIC CONTROLLERS USED FOR REACTOR TRIP SYSTEMS

A J MARGETTS

PLC's are being used in increasing numbers for control of chemical plants and particularly for monitoring, alarm, and trip systems. To ensure safe operation it is necessary to use simple formal procedures to test the hardware and software. This paper provides an set of procedures to assist this process.

KEYWORDS: PLC'S, PES's, Safety Assessment, Task Analysis, Hazop, Software.

INTRODUCTION

Over Pressure Protection

British Standard 5500 for the design of unfired welded pressure vessels states that "every pressure vessel shall be protected from excessive pressure or vacuum, excessive temperature, over filling, explosion or other hazardous condition by an appropriate protective device, except when the source of pressure (or temperature) is external to the vessel and is under such positive control that the variable cannot exceed the design value".

Within the context of this article over pressure protection can be provided by the following means:

- Safety relief valves
- Bursting discs
- Instrumented protective systems
- Design to the maximum source of pressure

Normally relief valves are specified on the basis of cost and reliability, but relief valves can present problems, and other systems or a combination of systems may be advantageous in particular circumstances. A major problem is what to do with the vented material when the relief lifts, and a flare system or vent scrubbing system may be necessary.

If we use a very reliable instrumented protective system, or design the vessel to the maximum source of pressure, it may be possible to dispense with the need for process relief valves or bursting discs. A relief valve for fire relief may still be required but this can often discharge to atmosphere.

If the instruments are slightly less reliable, then a combined system may be used, relying on the instrumented protective system to prevent the relief valve or bursting disc from lifting more than once in a few hundred years, and the relief valve or bursting disc protects the system in case of instrument failure.

Programmable Controllers

Programmable Logic Controllers (PLC's), sometimes called programmable controllers, started life as replacements for relay logic used for controlling elecrical power supplies to industrial processes. Their use has grown tremendously since 1979 and they now have the power and capability to be considered as alternatives to mini-computer based distributed systems. [7]

PLC's are being used in increasing numbers for control and automation of process plants, they are also being used for alarm systems, trip systems and fire and gas detection systems.[1]

Advantages of using PLC's

One of the most important advantages of using PLC based systems is that they can communicate with other PLC's, with operator control stations, and with other computers, using an industry standard ISO/OSI International Standards Organisation Open System Interconnection protocol. These data highways use simple cable materials and allow a geographically based distributed control system to be set up with much reduced cable costs compared to a completely hard wired system or to a central computer controlled installation.

An important consideration in batch processes is that the emergency shutdown procedure will depend on the state of the process. During charging or discharging any failure or shut down involves abandoning the control sequence and setting the valves to their safe states. During the active reaction phase operating parameters of temperature, pressure, and level are monitored and if predetermined limits are exceeded, alarms prompt the operator to intervene. If safe limits are exceeded then the reaction must be stopped.

A PLC based system can be used to decide which shut down or trip route to use according to the process conditions.

Disadvantages of using PLC's

The Health and Safety Executive (HSE) recommended practice document 'Guidance on the use of Programmable Electronic Systems' (which is published this month [9]) offers advice on the use of PES's which includes PLC's in alarm and trip systems.

Potential software problems include:

1) Faults in design may not be detected because it is very difficult if not impossible to test all combinations of outputs for all combinations of inputs at each step in the progam.

2) Failure modes are unpredictable and it is not always possible to guarantee that outputs fail to a known safe state.

3) Some of the low voltage electronic devices maybe subject to interference from outside electrical sources which can corrupt the software.

4) Hardware and software are under contiuous development and it can be difficult to consolidate practical experience with particular systems.

5) PLC's can be reprogrammed easily which may be a source of errors.

These disadvantages mean that a safety assessment of a PLC based trip system must involve an assessment of the PLC itself.

If a PLC is used in a safety system in a high risk application then the level of safety achieved must be at least as good as that achieved by a non programmable system.

It is important to note that in some situations the safety analysis may need to refer to previous designs or to proven high reliablity systems. In these cases hard wired logic maybe the solution.

Use of Procedures

To ensure safe operation of a PLC system it is necessary to use formal assessment procedures for hardware and software throughout the life cycle of the project, from specification, through design to testing, commissioning and maintenance. This paper provides a set of procedures to assist this process.

CASE STUDY

In this paper the procedures discussed refer to a batch reactor fitted with over pressure protection consisting of a combined system of an instrumented trip using a PLC, and a conventional bursting disc. The trip system allows the contents of the reactor to flow through a valve in the base of the vessel into a drown out tank containing cold water to quench the reaction. The bursting disc which provides backup for the trip system is mounted in a suitably sized branch in the top dished end. A P&I diagram of the equipment is shown in Figure 1.

TASK ANALYSIS

Before the software sequences can be written it is vital that logic flow charts or ladder diagrams be drawn to specify the detail of the process or operation concerned. One technique which is useful for writing detailed operating instructions is hierarchical task analysis (HTA), developed by Annet et al in 1971 [2].

Task analysis begins by making a general statement of the task being examined. This is written in the form of an instruction, such as 'Run reactor unit', 'Start up plant', or 'Start check and trip sequence'. These instructions are called operations. When the operation to be examined has been selected, analysis progresses by this operation being re-described in greater detail. To do this, the analyst writes down the subordinate operations (again in the form of instructions) and a plan stating the conditions when each of the subordinate operations should be carried out. Re-description of the subordinate operations may be necessary.

The plan in HTA is crucial, since the difficulties facing operators may be completely overlooked if an analyst uses an approach which concentrates on what should be done - usually the observable actions - without systematically examining when these things should be done. Indeed, many complex jobs appear superficial if their planning aspects are ignored.

HTA was originally developed for analysing and specifying operating instructions on manually operated plants but the technique is very useful for defining the detail of process operations on automatically controlled plants.

Lihou and Jackson [3] have described the use of task analysis to specify PLC software for batch processes.

A set of instructions for the reactor case study are given in figure 2. Each of the operations needs to be redefined as a separate sequence, and all of the operations within these sequences will in turn need redefining to a sufficient level of detail to describe each step of the sequence by the instrumentation on the plant. In addition a parallel set of operations need to be defined for each sequence detailing the trip or shut down operations required in any fault condition. An example of these operations for the reaction sequence is given in Figure 3.

Task analysis allows division of software tasks and reduces the complexity of the overall program making for precise specification, and easier programming, fault finding, and testing. Modular software that is debugged and tested can be incorporated into any system with a high degree of confidence and programs can be developed by an evolutionary approach rather than creating new designs for each new project.

HAZARD AND OPERABILITY STUDIES

When the project definition is complete, current practise is to subject the P & I diagram to a hazard and operability (H & O, or hazop) study to try to find out and correct all the safety and operational problems before the plant is built. This is done by using a check-list of property words which are a function of the process, together with guide words, to investigate deviations from normal operation. A suggested check list for a batch process is given in Table 1. A typical study group consists of the project engineer, process engineer, instrument engineer, plant manager and trained team leader. The Chemical Industries' Association guide provides all the detail of the hazop technique [3].

Table 1 H & O STUDY PROPERTY WORDS AND GUIDE WORDS

Property words	Guide words
Flow	no
Pressure	less
Level	more
Temperature	reverse
Amount	part
Composition	other
Maintenance	early
Corrosion	late
Testing	

The above list is not exhaustive.

Fig. 1 shows part of the P & I diagram for the feed of reactant to the reactor during the reaction sequence. The H&O study on this line considers each of the property words shown in Table 1, together with the guide words, to sudy the deviation from the normal condition of the property. The team can formulate the answers to the potential problems raised by for example high flow rate of reactant, low flow rate of coolant, high temperature, high pressure in the reactor. These answers form the basis of the control safety scheme for the process, and the documentation of these meetings forms the structure of the control sequence.

ANALYSIS OF THE CONTROL LOGIC USING THE HAZOP TECHNIQUE

Refering to the case study, Fig. 3 shows a flow chart for the check sequence monitoring the reaction step of the main sequence. The mode of operation is an endless loop involving checks on three instruments and four valves. The trip sequence is shown in Fig. 5 and involves opening the dump valve and checking that the batch is dumping.

The logic must be subject to a critical examination along the lines of the H & O study. This must be done in a meeting with three or four persons present (process engineer, instrument engineer, plant manager and the control engineer who specified the logic, are suggested). The study should analyse each step in detail. Refering to the P & I diagram and the flow chart, it should analyse all the possible deviations from intended operation.

Table 2 shows the modified Hazop study questions which assist in this analysis. Attention is focused on each property word in turn and the guide words are used to prompt discussion on deviations from design intent.

Of the measurable properties of the reaction, temperature is the one measurement which is likely to provide the earliest indication of a fault condition. The guide words applied to temperature suggest that an important variable not considered is rate of change of temperature. Further analysis indicates that additional software should be provided to calculate rate of temperature rise and provide a high temperature alarm and trip from the installed temperature transmitter, in addition to the trip from the existing temperature switch. Similar additional hardware and software can be provided to improve the reliability of the pressure measurement.

If necessary 2 out of 3 voting systems can be used to reduce the chance of spurious faults accidently shutting down the reactor. The fractional dead time of the system can be improved by using a redundant 'hot standby' configuration. Details of this technique are given elswhere, [1], [8].

Questions about Maintenance can reveal situations not considered at the design stage. Usually in batch processes maintenance can be done between batches without affecting safety on the plant. It should be remembered that some aspects of the process can be considered as continuous as far as safety is concerned. Examples are service supplies of cooling water, inert gas, steam, and vent scrubbing facilities. In this example it is necessary to consider maintaining the PLC equipment without affecting its ability to monitor the plant, and this can be done between batches. However if the PLC monitors plant or service equipment that must work continuously, then the equipment specification should ensure that the maintenance can be performed on line.

The question in Table 2 about Testing refers to the testing of the safety system to reveal fail danger faults. Again because the process is operated batchwise it is possible to fully test the safety system every batch if necessary. The dump valve can be tested by opening it, indeed one possibility is to empty the batch by this route. The dump valve is actuated by operating a solonoid pilot valve to vent the air supply to the diaphragm. Redding [10] has described how provision of a current detector on the 24v supply line to the intrinsically safe solonoid enables much information to be deduced about the health of the circuit and will reveal the fail danger faults of the components as follows:

normal current	circuit healthy
zero current	circuit break
high current	zenner diode fault
current not falling to target value in given time after test	capacitor fault

A PLC system can monitor the current and alarm if the circuit is not healthy.

Sensors have to be tested on a routine basis by subjecting them to a high pressure or temperature. Pressure sensors can be connected to a gas cylinder via an impulse line while the normal impulse line is isolated. Procedures have to be used to ensure that the sensor is not left isolated from the plant after the test. In a batch process it may be possible to pressurise the whole vessel to test the sensors which avoids the isolation problem.

This testing procedure should not be fully automatic because it provides much-needed operator interaction: the PLC can run through a test menu which acts as a prompt to the operator and ensures that he keeps a close watch on the test procedure.

TABLE 2 :MODIFIED H & O QUESTIONS FOR ANALYSING A BLOCK OF CONTROL LOGIC

Main property words	Guide words
FLOW	no, less, more, reverse or negative,
LEVEL	
TEMPERATURE	early, late, other
PRESSURE	

Questions for digital inputs/outputs

1. Are alarms/trips/messages needed?
2. Do outputs need to be monitored?
3. What provision must be made for testing alarms/trips?
4. What are the maintenance implications for equipment/instruments?

Additional questions for analog/control inputs/outputs

5. Can the control action result in process conditions outside the design range?
6. Is the control sensitive to process disturbance upstream or downstream?
7. What is the effect of a measurement input reading that is:
   a. zero? b. full scale? c. wrong? d. drifting?

RELIABILITY STUDIES

When the H & O study highlights a particular hazard or operability problem then some degree of quantification sometimes necessary to generate enough information to make a decision to instal extra protective equipment, or to change the design. Hazard analysis [5] and reliablity techniques are methods of quantifying these problems. An example of a reliability analysis of of a PLC system is described by Wilkinson and Balls. [1]

MODIFICATIONS

A formal procedure must be established for authorising and assessing application software changes. One procedure is to create a proposal form for software changes and to convene a meeting of the logic study group to approve the changes. The changes can then be programmed either by the engineers directly or by a person responsible for programming. The new logic must be tested before use.

System software based on firmware should be accessible to change only by the manufacturer and should only be done if the change incorporates considerable operating experience and has been exhaustively tested.

HARDWARE AND SOFTWARE TESTING

Before implementation of a computer control scheme, it is very important to test it to ensure that the programmed instructions accurately follow the agreed sequence flowcharts. It is also just as important to train the operators in the logic and to gain their confidence in the proposed mode of operation. The best way to do this is to connect the PLC to a simple simulator which consists of a bank of switches and lights for digital input and output, and to simulate measured valve inputs and control outputs using variable voltage sources and voltmeters. The operators can carry out the testing work and this also provides an excellent vehicle for training. In this way the operators can really get a feel for the process and the operating philosophy and can suggest changes based on their experience.

CONCLUSIONS

A safety system differs from a control system in that although continuously energised.it does not actually function unless tested or in an emergency, and when the emergency occurs there must be a high probability that the system will function as designed. In other words the system must have a low fractional dead time.

PLC's now offer the user a standard of design, manufacture and component reliability to achieve the above objective. The problem is that the reliability of the software is difficult to assesss. Now that many thousands of these devices are being used for routine industrial control purposes there is building up a body of knowledge and confidence in the system software or firmware which runs the applications software written by the user. When this body of knowledge becomes consolidated we will be much more confident in the use of these devices in safety systems. The application software will always have to be written and tested by the user and/or manufacturer, and the procedures outlined in this paper will assist this process.

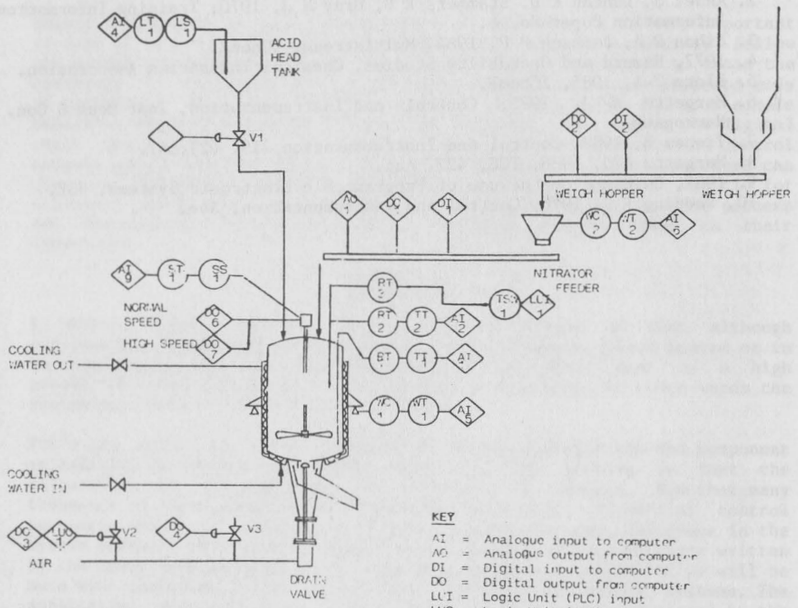
The HSE publication "Guidance on the use of Programmable Electronic Systems" contains a very useful set of check lists to help engineers with the specification , design, testing, modification and operation of PLC based control and safety systems.

Note finally that these procedures demand more time and more meetings during project definition. This must be allowed for in the planning of the project, but benefits are: faster start-up, safer and more reliable operation, better documentation, and reduced risk of loss.

REFERENCES

1. Wilkinson T A, Balls B W, 1985, Advances in Instrumentation, Vol 4, pp 1211 - 1221.
2. Annet J, Duncan K D, Stammers R B, Gray M J, 1970, Training Information Information Paper No. 6.
3. Lihou D A, Jackson P P, 1984, Multistream, IChemE.
4. 1977, Hazard and Operabilty Studies, Chemical Industries Association.
5. Kletz T A, 1985, IChemE.
6. Margetts A J, 1985, Control and Instrumentation, Inst Meas & Con, Harrogate.
7. Tinham B, 1987, Control and Instrumentation, 19, (2),p47.
8. Margetts A J, 1986, TCE, 427, Aug.
9. 1987, Guidance on the use of Programmable Electronic Systems, HSE.
10. Redding R J, 1976, Control and Instrumentation, Nov.

FIGURE 1



KEY

AI	=	Analogue input to computer
AO	=	Analogue output from computer
DI	=	Digital input to computer
DO	=	Digital output from computer
LUI	=	Logic Unit (PLC) input
LUO	=	Logic Unit (PLC) output
RT	=	Resistance thermometer
TT	=	Temperature transmitter
TSW	=	Temperature switch
LS	=	Level sensor
LT	=	Level transmitter
WC	=	Load cell
WT	=	Weight transmitter
LSW	=	Level switch
SS	=	Speed sensor
ST	=	Speed transmitter
ZS	=	Position switch

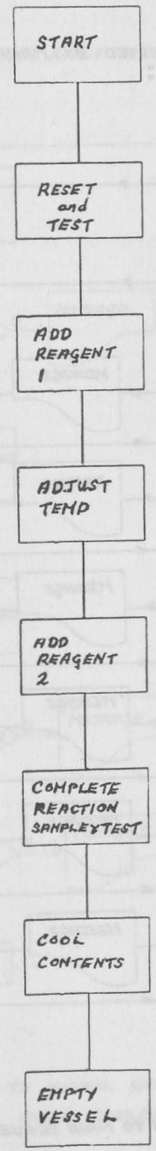


FIG 2 REACTOR SEQUENCE

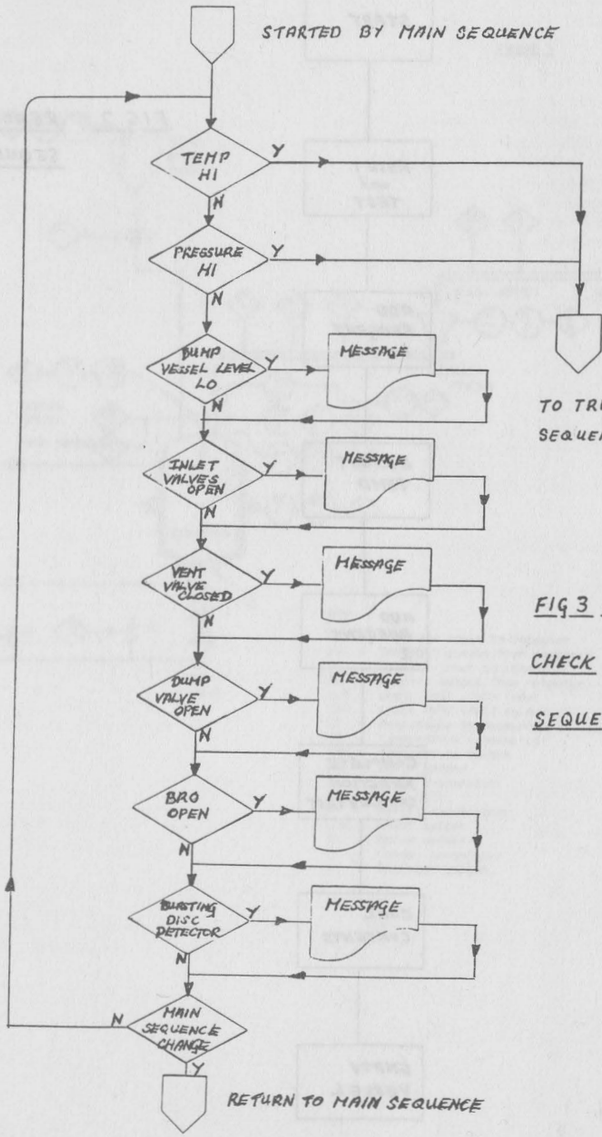


FIG 3 REACTOR CHECK SEQUENCE

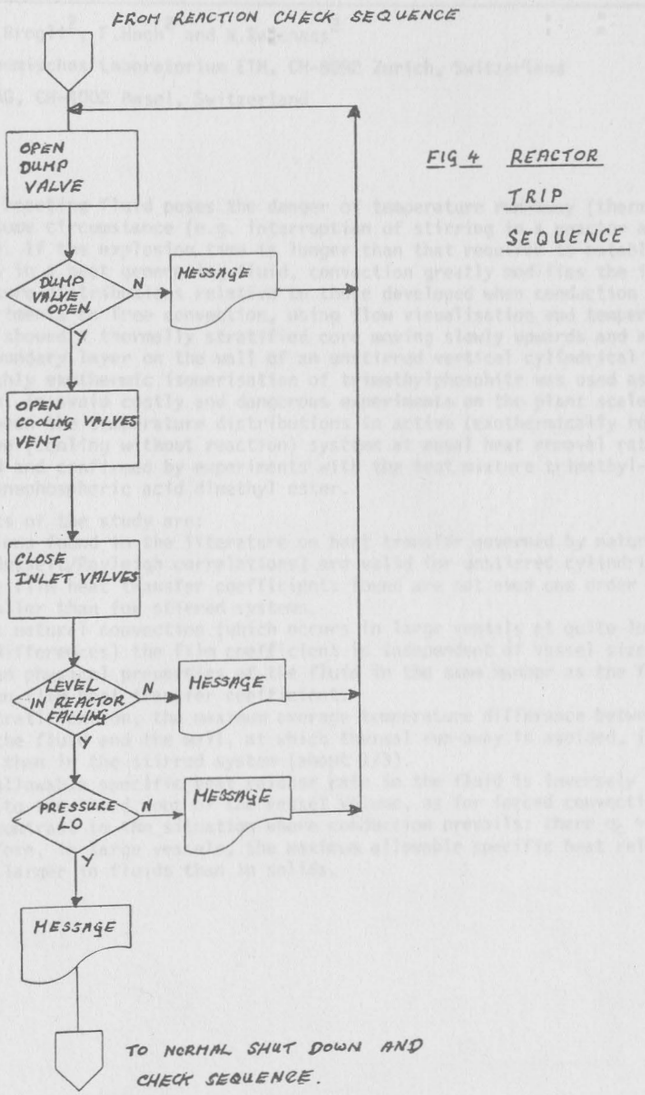


FIG 4 REACTOR TRIP SEQUENCE