THE CONTRIBUTION OF THE CONTROL SYSTEM TO LOSS PREVENTION

F.P. Lees
Department of Chemical Engineering, Loughborough University of Technology, Loughborough, Leics.

The paper reviews the role of the control system in handling faults on process plant, in particular its capabilities for failure resistance and graduated response to failure; the assessment of system state and the design of displays; the administration of fault conditions and the design of alarms; instrument failure and its effects; human error on the part of the operator and his response to emergency conditions.

THE CONTROL SYSTEM AND LOSS PREVENTION

The proposition that the control system has a crucial role to play in safety and loss prevention probably commands general assent. Yet very little has been written which attempts to define just what this role comprises. It is the objective of this paper, therefore, to give an overall survey of the features of the control system which seem most relevant to the loss prevention problem.

The purpose of a control system is presumably to keep the process fully under control at all times as far as possible. Usually, however, the control system is designed to maintain control of the process only in the face of normal distrubances and its response to fault conditions tends to be the rather drastic one of plant shutdown.

The conventional functions of the instrument and control hardware relevant to loss prevention can be summarised as

(1) Measurement
(2) Information handling and display
(3) Loop control
(4) Sequential control
(5) Safety shutdown

Here information handling covers transmission, processing and storage and information display covers instrument displays, alarms and logs. Sequential control embraces not only batch operations but startup, shutdown, operating point change, etc.

If a process control computer is incorporated in the control system, these functions are nominally the same but the power and flexibility of the computer may modify considerably the way in which they are carried out.

Particularly important for loss prevention has been the development of trip systems. It should be said at the start that these represent the main contribution to loss prevention in recent years by the control system.

The hardware does not constitute the whole of the control system, however. There is another component, the process operator. As control functions become increasingly automated, the trend is for the role of the operator to be reduced more and more to that of monitoring the process and of administering fault conditions.

There is a marked contrast in the extent to which the functions of these two elements of the control system are defined by the designer. Whereas the functions of the hardware are usually studied in detail, those of the operator are rarely analysed at all. Attention is typically confined to the details of the provision of certain traditional facilities such as displays and

alarms.

Thus although the process operator is to a large extent a component which the designer incorporates to give the control system the capability of monitoring and administering faults very little attention is given to this aspect.

Before considering possible improvements it is as well to recognise the limitations of the control system. Apart from explosion inside the plant, against which trip systems can give protection, the main problem in loss prevention is loss of containment, leading to serious fire, explosion or toxic release. There is only a limited amount that the control system can do to prevent this. Once the incident has occurred, however, it can assist by rapid detection, activation of protective devices, emergency isolation, plant shutdown, etc.

The aspects of control systems which seem capable of most improvement in relation to loss prevention can perhaps be described as failure resistance and graduated response.

In general control hardware tends to lack flexibility in its response to fault conditions. Its action is generally limited to the rather drastic one of shutting the plant down.

The operator by contrast offers much greater flexibility of response. Many of the potential developments are related in some way to assisting the operator in this response, heading off trouble or handling faults before a trip condition develops.

There is, however, a problem in operator reliability, especially under emergency conditions.

A particular type of fault which it is difficult for the control system itself to handle is instrument failure. The operator has a vital role to play here in giving the control system a self-checking and self-repairing capability.

In view of the importance of these aspects of the operator's job it is rather surprising how little attention is paid to them in the design of control systems.

Another related but equally neglected aspect is the checking of the condition and performance of plant equipment and instruments and the detection of incipient malfunctions. In view of the amount of information present in control systems and of the value of warning of impending failures, it seems surprising that there has been so little development here and that the activity of condition monitoring is quite divorced from that of control.

Some control system features which the foregoing discussion suggests are relevant to loss prevention are listed with references in Table 1. Selected aspects of these are now discussed.

It is necessary that fault conditions be handled securely and this must be the top priority. Trip systems have a quite crucial role to play in this. But equally it is not economic to keep shutting the plant down and it is important therefore to develop capabilities for failure resistance and graduated response.

This comment on plant shutdown should not be misinterpreted. It is fully appreciated that there are circumstances in which immediate shutdown is the only possible response.

Many of the developments which can be envisaged are means of assisting the operator to forestall trouble and to handle faults.

The discussion is primarily in terms of continuous processes. Batch processes have some special features which there is not space to treat here.

DETAILED ASPECTS

Displays

It is important to provide the operator with an effective display interface so that he has as good a chance as possible of keeping up-to-date with the process and recognising trouble at an early stage. A good deal is now known about how the operator samples information (Crossman, Cooke and Beishon (7)) and updates his mental model of the state of the process (Bainbridge (8)). Some desirable characteristics are that the interface assists the operator to obtain information 'at a glance', that it allows him to make confirmatory checks using 'redundant' information and that it facilitates pattern recognition. There are interfaces, such as some conventional panels with high instrument densities and some computer consoles, which are poor in these respects.

As far as individual instruments are concerned the conventional chart recorder has some rather important advantages in ease of information sampling and learning (Crossman, Cooke and Beishon (7)), in fault administration (West and Clark (5)) and in malfunction detection (Anyakora and Lees (29)).

TABLE 1 - Some Control System Features Particularly Relevant to Loss Prevention

Feature	References
General	Edwards and Lees (1); Lees (2)
Process operator	Edwards and Lees (1, 3); Duncan (4); West and Clark (5)
Monitoring behaviour	Edwards and Lees (1, 3); Sheridan and Johannsen (6)
Display systems	Crossman, Cooke and Beishon (7); Bainbridge (8); Rasmussen (9); Edwards and Lees (1, 3); Duncan (4); Stainthorp and West (10); Duncan and Shepherd (11); Lees (12)
Alarm systems	Andow and Lees (13)
Gas, smoke and fire detection	Steel (14); Firth, Jones and Jones (15); H.M. Factory Inspectorate (16)
Operational data recording	Edwards and Lees (1); Department of Employment (17)
Fault diagnosis	Duncan (4); Duncan and Shepherd (11); Duncan and Gray (18)
Alarm analysis	Welbourne (19, 20); Patterson (21); Rasmussen (9); Powers and Tompkins (22); Andow and Lees (23)
Valve sequencing, interlocks	Rivas, Rudd and Kelly (24); Rivas and Rudd (25).
Malfunction detection	Gallier (26); Anyakora and Lees (27); Whitman (28)
Instrument malfunction detection	Anyakora and Lees (27, 29, 30); West and Clark (5); Duncan and Gray (18); Bellingham and Lees (31)
Instrument failure	Green and Bourne (32); Hensley (33); Anyakora, Engel and Lees (34); Lees (35, 36, 37); Skala (38); U.S. Atomic Energy Commission (39)
Human error	Swain (40, 41); Ablitt (42); Lees (43); Lawley (44); U.S. Atomic Energy Commission (39)
Emergency behaviour	Ronan (45); Rigby and Edelman (46); Swain (41); West and Clark (5); U.S. Atomic Energy Commission (39); Lees and Sayers (47)
Trip systems	Hensley (33); Stewart (48); Kletz (49); Lawley and Kletz (50)

There are also developments in computer-aided assessment of system state which may prove useful (Stainthorp and West (10)).

Features of displays relevant to loss prevention have been considered in more detail elsewhere (Lees (12)).

Alarms

The alarm system is virtually the only automatic aid available to the operator for fault administration, other than trip systems. Yet alarm systems are frequently unsatisfactory with too large a number of alarms, confusion between alarms and statuses, alarms permanently up, etc. The need is for much more carefully designed alarm systems which as far as possible give only meaningful alarms. Although process computer alarm systems are in general as bad as conventional ones, the process computer does offer the potential for the creation of more rational alarm systems.

The alarm system and its importance in loss prevention has been discussed by Andow and Lees (13).

Gas, Smoke and Fire Detectors

It seems appropriate to mention at this point a particular area of instrumentation which is concerned with loss of containment and with fire on chemical plants, namely gas, smoke and fire detectors. There has been a rapid development of these instruments both for display and alarm and for initiation of protective devices.

Operational Data Recording

There is considerable interest in the use of the control system, and particularly computers, to log process data for post mortem analysis of incidents. The Flixborough report (17) hinted at the possibility of a statutory data recording facility similar to the 'black box' used in aircraft. The general concept is certainly valid, though the important thing would seem to be to learn from all incidents, including 'near misses', rather than from accidents alone, since these are much rarer.

Fault Diagnosis

Fault detection is followed by fault diagnosis. This is done by the operator usually standing at the control panel. This task has been studied and methods have been developed for training operators in fault diagnosis relying on a pattern recognition approach (Duncan and Shepherd (11)) or a decision tree method (Duncan and Gray (18)).

This work , of course, has implications for the type of interface which is required. There is much less scope for pattern recognition on some interfaces.

Alarm Analysis

In a few systems, such as the nuclear reactors at Oldbury and Wylfa, the operator is assisted in fault detection by computer alarm analysis (Welbourne (19,20), Patterson (21)). The computer scans the alarms and analyses them using an 'alarm tree' embodied in the program. Objectives of the analysis are to assist the operator to diagnose the original fault and to digest further alarms as they come up.

This facility is obviously very attractive in principle but it requires a very large engineering effort. Attempts are currently being made to reduce the amount of work required to produce the program (Powers and Tompkins (22), Andow and Lees (23)).

There is also the human factors problem of the degree of confidence which the operator is able to place in the analysis (Rasmussen (9)).

It is of interest that instrument failure is a critical feature both in manual fault diagnosis and in computer alarm analysis. In both cases it has proved necessary to treat this as a separate problem to be resolved before going on to the main analysis.

Valve Sequencing

The final stage of fault administration is fault correction. Trip systems constitute a form of automatic fault correction, but anything less drastic has to be done by the operator unaided.

There are now developments, however, in computer-assisted sequencing of valve systems. A method has been developed of checking whether a proposed sequence of valve movements is safe or hazardous, which could therefore serve as a computer-based interlock (Rivas, Rudd and Kelly (24)), while other work is has outlined a technique of synthesising sequences which could form the basis for fully

automatic corrective action by a computer (Rivas and Rudd (25)).

Malfunction Detection

Although the operator is involved in the detection of incipient malfunction in plant equipment and instruments this is not generally regarded as a normal function of the control system. Yet the considerable activity in condition monitoring indicates the interest in this aspect. At present this activity is proceeding largely divorced from control.

It would appear, however, that monitoring for malfunctions is an appropriate function for the control system. Malfunction detection involves measurement and information processing, storage and display. These are the normal features of a control system.

The process computer with its powerful information processing and display facilities seems a natural tool for malfunction detection work.

There is another reason why it is appropriate that the control system be more involved in malfunction detection. The growth in the passive monitoring aspect of the operator's tasks and the possibility of underloading pose problems in job design. A common solution to such a problem in human factors is the creation of a secondary task. But it would be undesirable to create an irrelevant task merely for the sake of it. Active checking for incipient malfunctions, however, constitutes an additional task which is fully in line with the operator's role. As already stated he is the component used by the designer to give the system a self-checking and self-repairing capability. This task has the further advantage that it is not critical precisely when the checks are executed so that they can be done in otherwise idle periods.

Malfunction detection by the control system has been discussed by Edwards and Lees (1), by Anyakora and Lees (27) and by Whitman (28).

Instrument Malfunction Detection

The control system is entirely dependent on its instruments and the checking of these is an appropriate starting point for malfunction detection.

Most detection of instrument malfunction is carried out at present by the process operator. The signal indicating malfunction is frequently fairly obvious, but equally there are many situations where it is not. In these circumstances displays such as chart recorders have been shown to be particularly valuable (Anyakora and Lees (29), West and Clark (5)).

A number of process computer systems carry out some form of computer-assisted instrument calibration or checking by mass balance or other models.

There are also developments in generalised computer checking techniques, based on the noisiness of the signal (Anyakora and Lees (30)) or the relation between flow and valve stem position (Bellingham and Lees (31)), and in associated computer graphic displays (Lees (12)).

Instrument Failure

Instrument failure has many implication for loss prevention. There are probably more failure data available on instruments than on most other types of equipment. Moreover, it seems to be broadly true that the data which are available are quite widely applicable. Many data are available only on a commercial basis, such as those in the U.K. Atomic Energy Authority Systems Reliability Service's data bank, but there are some published compilations (Green and Bourne (32), Anyakora, Engel and Lees (34), Skala (38), U.S. Atomic Energy Commission (39)).

Some progress has been made in determining the effect of factors such as operating environment which influence instrument failure (Anyakora, Engel and Lees (34)).

The effects of instrument failure are numerous. The most obvious result of a failure is a control loop moving in the dangerous direction or a trip failing to danger, but failures also affect the operator by undermining his confidence in displays or alarms or making more difficult the task of fault diagnosis.

A review of the problem of instrument failure as a whole, including case histories associated with instrument failure, has been given elsewhere (Lees (36)) and the published data on instrument failure have been reviewed (Lees (37)).

Human Error

The attempt to asses the reliability of control systems has led to a requirement for methods of assessing the reliability of the operator also. Methods of human error assessment have been developed (Swain (41)) and there are a number of published operator reliability assessments (Ablitt (42), Lawley (44)). The most comprehensive of these is in the U.S. Atomic Energy Commission's work on accident risks in U.S. commercial nuclear power reactors (39).

The problem of operator reliability has been reviewed elsewhere (Lees (43)).

Emergency Behaviour

Particularly important in relation to loss prevention is the behaviour of process operators in emergencies. There is a small amount of data on emergency behaviour in general (Ronan (45), Rigby and Edelman (46)) and in process control (West and Clark (5), Lees and Sayers (47)). But the overall conclusion is that the probability of effective action by the operator in an emergency is not high enough to rely on for safety though it is high enough to be very useful. The U.S. Atomic Energy Commission study (39) mentioned above gives the fullest treatment.

Since the operator cannot be relied on to take critical safety action the trend is towards the use of trip systems to guard against seriously hazardous situations.

Trip Systems

If the hazard is sufficiently great the trip system itself must be very reliable. It is also highly desirable that the trip system should not shut the plant down too often due to spurious trips. These considerations have led to the development of sophisticated High Integrity Protective Systems (Stewart (48)) with 2 out of 3 (2/3) voting features.

These very complex trip systems are not typical, however. Simple 1/1 trips are more usual (Lawley and Kletz (50)). Instrument reliability is thus an important aspect of trip systems.

CONCLUSION

It is envisaged that the development of control systems in relation to loss prevention will certainly involve a much more widespread use of trip systems. But there appears to be scope also for the design of control systems which are capable of a more flexible response to fault conditions.

ACKNOWLEDGEMENTS

The author wishes to acknowledge the support of the Science Research Council in this work.

REFERENCES

1. Edwards, E. and Lees, F.P., 1973, "Man and Computer in Process Control", Instn. Chem.Engrs., London.

2. Lees, F.P. , 1972, Measmt. Control, 5, T118.

3. Edwards, E. and Lees F.P. (eds.), 1974, "The Human Operator in Process Control", Taylor and Francis, London.

4. Duncan, K.D., 1974, in Edwards, E. and Lees, F.P. (1974), op.cit.,p. 283.

5. West, B., and Clark, J.A., 1974, in Edwards, E. and Lees, F.P. (1974), op.cit.,p. 206 .

6. Sheridan, T.B., and Johannsen, G. (eds.), 1976, "Monitoring Behaviour and Supervisory Control", Plenum Publishing Co., London.

7. Crossman, E.R.F.W., Cooke, J.E. and Beishon, R.J., 1964, "Visual Attention and the Sampling of Displayed Information in Process Control", Univ. of California, Berkeley, Calif., Hum. Factors in Technol. Res.Gp.Rep. HFT 64-11-7. See also Edwards, E. and Lees, F.P. (1974), op.cit., p.25.

8. Bainbridge, L., 1974, in Edwards, E. and Lees, F.P. (1974), op.cit., p.146.

9. Rasmussen, J., 1968, "On the Communication between Operators and Instrumentation in Automatic Process Plants", Danish Atomic Energy Commission Res. Estab. Rep. Riso-M-686, Riso, Denmark. See also Edwards, E. and Lees, F.P. (1974), op.cit., p. 222.

10. Stainthorp, F.P. and West, B., 1974, Chem.Engr., London, 289, 526.

11. Duncan, K.D. and Shepherd, A., 1975, "Analysis and Training of Fault Location Tasks in the Chemical Industry", Chemical and Allied Products Industry Training Board Rep., Staines, Middlesex, England.

12. Lees, F.P., 1974, "Visual Displays and Man Machine Interfaces", Acta IMEKO 76, North Holland.

13. Andow, P.K. and Lees, F.P., 1974, "Process Plant Alarm Systems: General Considerations", "Loss Prevention and Safety Promotion in the Process Industries" (edited by C.H. Buschmann) Elsevier, Amsterdam.

14. Steel, B.G., 1971, "Fire Detectors for Use on Chemical Plants", "Major Loss Prevention in the Process Industries", Instn. Chem. Engrs., London, p.133.

15. Firth, J.G., Jones, A. and Jones T.A., 1974, "Flammable Gas Detectors", "Chemical Process Hazards with Special Reference to Plant Design", Vol.5., Instn. Chem. Engrs., London, p.307.

16. H.M. Factory Inspectorate, "Industrial Use of Flammable Gas Detectors", Tech. Data Note No.45, H.M. Stationery Office, London.

17. Department of Employment, 1975, "The Flixborough Disaster", H.M. Stationery Office, London.

18. Duncan, K.D. and Gray, M.J., 1975, J.Occup. Psychol., 48, 199.

19. Welbourne, D., 1965, "Data Processing and Control by a Computer at Wylfa Nuclear Power Station","Advances in Automatic Control", Instn. Mech. Engrs., London, p.92.

20. Welbourne, D., 1968, Proc. I.E.E., 115, 1726.

21 Patterson, D., 1968, Proc. I.E.E., 115, 1858.

22. Powers, G.J. and Tompkins, F.C., 1974, A.I.Ch.E.J., 20, 376.

23. Andow, P.K. and Lees, F.P., 1975, Trans. Instn. Chem. Engrs., 53, 195.

24. Rivas, J.R., Rudd, D.F. and Kelly, L.R., 1974, A.I.Ch.E. J., 20, 311.

25. Rivas, J.R. and Rudd, D.F., 1974, A.I.Ch.E. J., 20, 320.

26. Gallier, P.W., 1968, Chem.Engng. Prog., 64(6), 71.

27. Anyakora, S.N. and Lees, F.P., 1972, "Principles of the Detection of Malfunction using a Process Computer", "Decision, Design and the Computer", Instn. Chem. Engrs., London, 6:7.

28. Whitman, K.A., 1972, Instrum. Technol., 19(7), 50.

29. Anyakora, S.N. and Lees, F.P., 1972, Chem. Engr., London, 264, 304.

30. Anyakora, S.N. and Lees, F.P., 1973, "The Detection of Malfunction Using a Process Control Computer: Simple Noise Power Techniques for Instrument Malfunction", "The Use of Digital Computers in Measurement", Instn. Elec. Engrs. Conf. Pub.No. 103, London.

31 Bellingham, B. and Lees, F.P., "The Detection of Malfunction Using a Process Control Computer: A Simple Filtering Technique for Flow Control Loops", Trans. Instn. Chem. Engrs., in press.

32. Green, A.E. and Bourne, A.J., 1972, "Reliability Technology", Wiley, New York.

33. Hensley, G., 1968, Measmt. Control, 1, T72.

34. Anyakora, S.N., Engel, G.F.M. and Lees, F.P., 1971, Chem. Engr., London, 255, 396.

35. Lees, F.P., 1973, Chem. Engr., London, 277, 418.

36. Lees, F.P., 1976, Chemy. Ind., March 6, 195.

37. Lees, F.P., 1976, "A Review of Instrument Failure Data", "Process Industry Hazards - Accidental Release, Assessment, Containment and Control", Instn. Chem. Engrs., London.

38. Skala, V., 1974, Instrum. Technol., 21(10), 27.

39. U.S. Atomic Energy Commission, 1975, "Reactor Safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Reactors", WASH 1400, Washington, D.C.

40. Swain, A.D., 1969, "Human Reliability Assessment in Nuclear Reactor Plants", Sandia Laboratories, Albuquerque, New Mexico.

41. Swain, A.D., 1972, "Design Techniques for Improving Human Performance", Industrial and Commercial Techniques Limited, London.

42. Ablitt, J.F., 1969, "A Quantitative Approach to the Evaluation of the Safety Function of Operators on Nuclear Reactors", U.K. Atomic Energy Authority, Rep. AHSB(S) R160.

43. Lees, F.P., 1973, I.E.E.E. Trans. Reliab., R-22, 124.

44. Lawley, H.G., 1974, Chem. Engng. Prog., 70(4), 45.

45. Ronan, W.W., 1953, "Training for Emergency Procedures in Multiengine Aircraft", American Institute for Research, Rep. AIR - 153 - 53 - FR - 44.

46. Rigby, L.V. and Edelman, D.A., 1968, Hum. Factors, 10, 475.

47. Lees, F.P. and Sayers, B., 1976, in Sheridan, T.B. and Johannsen, G., op.cit.,p. 251.

48. Stewart, R.M., 1971, "High Integrity Protective Systems", "Major Loss Prevention in the Process Industries", Instn. Chem. Engrs., London, p. 99.

49. Kletz, T.A., 1972,"Specifying and Designing Protective Systems", "Loss Prevention", Vol. 6, Am. Inst. Chem. Engrs., New York, p. 15.

50. Lawley, H.G. and Kletz, T.A., 1975, Chem. Engng., Albany, May 12, 81.