Figure 7: Risk Profile by RIPS Analysis

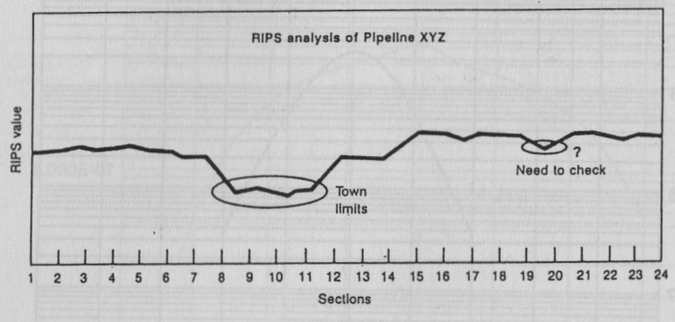
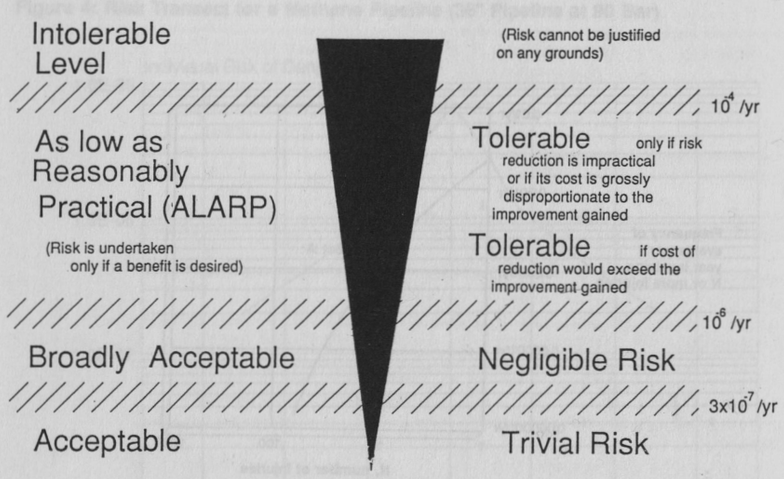


Figure 8: Risk Acceptability Criteria



EMERGENCY SHUT DOWN SYSTEMS IN ONSHORE AND OFFSHORE PROCESS OPERATIONS

J PEARSON, PRINCIPAL SPECIALIST INSPECTOR

HEALTH & SAFETY EXECUTIVE
LIVERPOOL

SYNOPSIS

This paper describes some of the latest developments in the use of Emergency Shut Down Systems in process installations both onshore and offshore. The safety implications of these developments are discussed. The effects of common cause failures and human factors with examples of accidents are described. The assessment of systems against HSE Guidelines, industry standards and future international standards is discussed and the changing offshore legislation.

Keywords : Control, protection, communications, programmable electronic systems.

INTRODUCTION

HSE Inspectors are called upon to inspect and assess safety systems, in a wide range of industries having major hazard potential. Safety systems include Emergency Shut Down (ESD) systems, Fire and Gas (F&G) Detection Systems, Alarms and Control & Communications systems. The experience of Inspectors when assessing computer based control and protection systems in the process industries is that one cause for concern is inadequate design and specification. New and ever developing technology eg Smart transmitters Data Communications, Fibre Optics is being applied to Safety Systems on plants having high hazard potential. This requires the highest level of attention by the project engineers and designers at all phases in the lifecycle of the system. This is because the application of new concepts, systems or devices may affect the operation and safety of the plant.

The HSE is not opposed in principle to these concepts nor does it wish to restrict development. On the contrary many high technology systems have the **potential for improving safety** and this potential should be exploited. The policy of HSE is that the safety implications of using such technology on a process plant where system failures could lead to a hazard should be systematically assessed to ensure that the overall safety performance of the plant is not degraded.

DEVELOPMENTS IN TECHNOLOGY

New concepts are emerging frequently in various fields such as:

- microprocessor sensors,
- communications links, including fibre optics and radio, microwave, satellite,

- local area networks and data highways,
- remote monitoring, and diagnostics,
- sophisticated automation techniques including expert systems.

The use of microprocessor sensors or "smart transmitters" is increasing in the quest for higher plant efficiency. The application of smart transmitters however needs careful consideration of the safety implications, for example, the Human Factors. A smart transmitter has many useful features leading to very high accuracy and can be re-ranged or calibrated using the communications facility either locally on plant or from a remote equipment room or central control room. This action could lead to errors being introduced by the instrument technician and could lead to loss of control. The management control of work on live transmitters and the discretion of the technician to make adjustments needs to be formally established.

COMMUNICATIONS

One of the major developments made possible by the use of programmable electronics is the communications capability between systems for example between emergency shut-down systems (ESD) and distributed control systems (DCS). This gives the ability to display the ESD system status on the DCS screens which may be at a different location to the ESD system. Such information as input alarm conditions, system fault, maintenance override and "first up" indication can all be displayed to the operator on VDU screens using the system graphics.

The facility for communications over data highways between ESD and DCS systems allows great flexibility for transfer of information concerning the operational ESD status to the operator who may be in a remote or central control room. For an offshore installation the remote control room may be onshore or on another offshore installation. This transfer of information via data highways in accordance with the system protocol has valuable contributions for both safety and operability.

Of great influence on ESD integrity however, is the capability of operators to use these communication links which rely on software, to override the actions of an ESD system. The possibility of errors introduced by the software and the effect on the overall integrity, needs to be carefully considered. The assessment of plant integrity and operational security should take into account the reliability of data communication links.

The increasing use of data transmission by copper cable, fibre optic cable and VHF radio, for which standards are in preparation, is likely to increase dramatically the volume of data to be handled, stored and subsequently displayed to operators or managers. It is anticipated that the publication of the International "Fieldbus" standard with its hardware specifications and message protocol is likely to encourage an increase in the use of fully digital signal transmission from sensor and transmitter through distributed

control systems up to the valve actuator. This will require a greater commitment to safety and observation of basic principles of safety engineering such as:

- separate control and protection systems,
- protection against common cause failures,
- use of components of known reliability with a track record in similar applications,
- attention to detail in terms of software preparation, documentation and quality assurance procedures,
- quality of power supplies, and
- protection against electromagnetic and radio frequency interference,
- compatibility between systems and humans in respect of data handling.

Accidents have occurred on plants due to failure to take account of and make provision for each of the above aspects.

Two incidents have occurred in the UK to our knowledge due to data overload between systems and between system and operator. These are:

1. Release of flammables/toxics due to CPU/memory data transfer overload.

2. Fires and explosions on a refinery due to loss of control caused by Operator overload due to alarm avalanche in emergency conditions.

The use of the check-lists in the HSE PES guidelines (reference 1) to ensure compliance with its recommendations would have prevented accidents from these causes.

OFFSHORE

Following the Piper Alpha accident and the Cullen report the UK offshore sector is now investing heavily in the safety of offshore platforms in terms of additional safety systems, Temporary Safe Refuges, Formal Safety Assessments and Safety Cases. The Regulatory body, HSE, is also investing in a substantial increase in numbers of inspectors to inspect installations and examine, and respond to safety cases. In terms of hardware the installation of emergency shut-down valves for example on gas and oil risers to comply with the Offshore Installations (Emergency Pipeline Valves) Regulations 1989 will enable rapid shut-down of plant and isolation of pipelines.

The safety of an installation depends entirely on the correct operation of these ESD valves, costing sometimes in excess of £3 million each. In turn this may rely on correct detection of a hazardous condition by sensors, the processing of data in electrical, electronic or programmable electronic

systems and signalling from outputs to actuators. It is likely that the safety contribution from automatic safety systems such as emergency shut-down, and fire and gas detection and alarm systems will be an important part of the formal safety assessment.

COMPLEXITY AND AVAILABILITY

Modern emergency shut-down or fire and gas systems can be designed to have extremely high availability theoretically approaching 100 per cent. This is due to redundancy, self testing, line monitoring, and self diagnostics in addition to the use of the best available electronics, integrated circuits or other components. In contrast the valves and associated actuators, power supplies and hydraulic systems may have comparatively very low availability. The difficulty and cost of fully testing, and the extremely arduous conditions in which they operate can lead to this poor reliability. The complexity of the central processing panel introduced in the quest for high availability may have an adverse effect in the level of system availability actually achieved by increasing the component defect rate and as a result of this the maintenance induced errors. The availability of the central processing part of the shut-down system should be designed to be adequate without unnecessary additional complexity.

COMMON CAUSE FAILURES

A major weakness discovered by inspectors is the failure to give thought at the design or installation stage to common cause failures that can lead to simultaneous failure of control and protection systems. An example of CCF occurred in 1982 in Canadian waters when the entire 84 man crew of the Ocean Ranger semi-submersible drilling unit were lost when the unit sank due to total loss of ballast control and loss of stability. The US National Transportation Safety Board inquiry into the disaster established that the loss of control was due to ingress of sea-water into the ballast control panel when a portlight glass broke in severe storm conditions. Despite 4 hours frantic efforts the crew failed to recover the situation.

A similar incident occurred in the North Sea in 1986 when a semi-submersible lost ballast control and was almost lost. On this occasion the fault was lack of a filter and ingress of foreign particles into the hydraulic systems which prevented control valves from closing correctly.

Common cause failures such as these can occur and history demonstrates that they do occur due to systematic failures including specification errors, software errors and environmental factors such as electrical interference or maintenance errors.

HUMAN FACTORS

Another concern is that of the human response to control systems of increasing complexity. An analysis carried out by SINTEF (reference 3) of alarms and shut-down incidents in the Norwegian sector of the North Sea established that a major cause of incidents was the incorrect conception of the state of the system and the plant. The analysis also established that when an emergency occurs then human behaviour is critical to the outcome of

the event. A further conclusion was that human error in operations or maintenance was one of the main factors causing spurious shut-downs of plant, for example welding operations affecting fire detectors.

A serious incident occurred recently on a chemical plant when operators mistakenly overrode a shut-down system function instead of resetting the protective function after abnormal high pressure had caused a trip. This action caused a further overpressure and a release of materials on a plant handling highly toxic substances.

The above problems highlight the need for:

1. Careful design of the operator interface both in terms of information display and controls layout and the alarm handling capabilities of operators.

2. Sufficient training and supervision to prevent incorrect actions in times of high activity.

The use of simulators is becoming an accepted way of giving operators the necessary experience to handle emergency situations.

EXPERT SYSTEMS

"Over 600 expert systems in use world-wide for real time control of plant" is the claim of one supplier. The main areas of concern of programmable electronic systems extend to expert systems; namely the specification, the software, and the setting of boundaries or limits to operating conditions over which the expert system has control. The promise of operator assistance by an expert system during times of emergency has yet to be fully realised.

A major problem in the development of expert systems is capturing the knowledge in a suitable form and also the inconsistency of knowledge between different "experts" (Ref 6, 7.)

ASSESSMENT

The HSE PES guidelines (reference 1) based assessment on 3 criteria:

the configuration (or architecture of safety systems),

the reliability and

the overall quality of implementation.

It also based its criteria for acceptability on what was considered acceptable using conventional control and protection systems. This comparison of new for old has limitations in terms of assessment of new concepts. For example a data highway and a 4-20 mA control loop or relay logic trip circuit are not directly comparable. In many ways a data highway is much more powerful, is continuously exercised, and has self monitoring features but its failure may cause the loss of a large number of functions.

An alternative approach to assessment is to specify a system certified by TUV, the German organisation. This is valuable in that an independent body has examined the design, the hardware and in some cases the system software against detailed standards for a particular class of hazard. HSE acknowledge the value of TUV certification but are aware of the limitations in that it does not include field equipment, cables, application software, installation or commissioning.

NEW STANDARDS

Two new IEC Standards (Ref 2) on Safety Related Systems have been circulated in draft form for public comment. They are:

a. IEC 65A WG9 "Software for Computers in the application of industrial Safety Related Systems".

b. IEC 65A WG10 "Functional safety of electrical/electronic/Programmable Electronic Systems: Generic aspects".

The WG10 draft document applies to all electrically based systems and breaks new ground in 2 main areas:

i. The Safety System Lifecycle.

ii. Integrity levels based on risk.

The lifecycle requirements are based on a strict quality assurance approach and requires comprehensive documentation at each phase of the lifecycle from initial concept of a project through to decommissioning.

The draft documents from IEC 65A Working Groups 9 and 10 on Safety Related Systems establish integrity levels for systems and software appropriate to the application. This will allow the process Industry to develop standards which will specify the type of system and the procedures for quality assurance for software appropriate to the level of potential hazard. This work is progressing in a number of joint HSE/Industry working groups on for example Offshore Installations. Until this work is completed and the application sector standards are published then the HSE PES guidelines should be used as a basis for assessment in conjunction with other guidance, for example, the EEMUA document and the Institute of Gas Engineers publication (Refs 4 and 5).

OFFSHORE LEGISLATION

The regulation of safety in the offshore industry is changing at a dramatic pace. Each Offshore installation will need a safety case to be submitted to HSE giving evidence of safe operation, safety management systems, and formal safety assessments. Also new regulations made under the HSWA will be in the form of "goal setting" regulations specifying objectives to be achieved rather than detailed prescriptive requirements. An example would be the fire resistance duration of the TSR and the maximum probability of a hydrocarbon fire to which it may be subjected.

This implies that a quantified assessment is required to demonstrate compliance.

This philosophy, ie safety cases and objective setting, is based on a "risk based approach" and follows well the future standards from IEC on assessment of systems against hazards from first principles.

CONCLUSION

The IEC 65A concept of integrity levels for safety systems is a sound one. The allocation of integrity levels to industry applications however is a difficult task as also is the specification of the methods of achieving the specified safety level. This is the future work of IEC and industry committees. Until specific standards are produced then the design and assessment should be carried out on the basis of the HSE PES guidelines and check-lists and industry codes of practice such as the E.E.M.U.A. and the Institute of Gas Engineers publications on programmable electronic systems (references 4 and 5) and on companies own internal standards.

The incidence of accidents caused by computers controlling or protecting process plants is relatively low but as the potential hazards and possible consequences of a major accident are severe there is no room for complacency. The rate of development of technology and applications of this technology in areas having increasing safety considerations requires a corresponding increase in awareness, adoption of standards, and commitment to safety aspects at all life cycle phases of a project.

REFERENCES

1. Programmable Electronic Systems in Safety Related Applications, HSE, HMSO 1987, Part 1 An Introductory Guide ISBN 011 8839 136, Part 2 General Technical Guidelines ISBN 011 8839 063.

2. IEC Draft Standards: WG9 "Software for Computers in Applications of Industrial Safety Related Systems". IEC 65A/WG9 BSI.

WG10 "Functional Safety of Programmable Electronic Systems; Generic Aspects; Part 1 (IEC reference "65A (Secretariat) 96"). BSI.

3. Alarm and Shut-down Frequencies In Offshore Production. SINTEF. The Foundation for Scientific and Industrial Research, Norwegian Institute of Technology N-7034 Trondheim NTH, Norway.

4. Safety Related Instrument Systems for the Process Industries (including Programmable Electronic Systems) Publication No 160. The Engineering Equipment and Materials Users Association (EEMUA), 14/15 Belgrave Square, London SW1X 8PS.

5. Use of Programmable Electronic Systems In Safety Related Applications in the Gas Industry, The Institute of Gas Engineers, Reference IGE/SR/15/1989, The Institution of Gas Engineers, 17 Grovenor Crescent, London SW1X 7ES.

6. Expert Systems in Britain, Ovum Ltd, DTI, Information Technology Division, Kingsgate House, 66-74 Victoria Street, London, SW1E 6SW.

7. Industrial Expert Systems - Status Report, January 1992. SIRA Ltd, Chislehurst, Kent. Ref SIRA 2/9137/00.