KLM Technology Group
#03-12 Block Aronia,
Jalan Sri Perkasa 2
Taman Tampoi Utama
81200 Johor Bahru
Malaysia

PROTECTIVE INSTRUMENTATION SYSTEMS

(PROJECT STANDARDS AND SPECIFICATIONS)

TABLE OF CONTENT

SCOPE

This Project Standard and Specification provides guidance to the selection and use of equipment for Instrument protection systems. It contains sections that have general application to the provision of protective instrumentation systems, alarm systems, fire and gas detection and control systems and pipeline leak detection. These include general principles, documentation and requirements for common systems.

REFERENCES

Throughout this Standard the following dated and undated standards/codes are referred to. These referenced documents shall, to the extent specified herein, form a part of this standard. For dated references, the edition cited applies. The applicability of changes in dated references that occur after the cited date shall be mutually agreed upon by the Company and the Vendor. For undated references, the latest edition of the referenced documents (including any supplements and amendments) applies.

1. IEC 85 Thermal Evaluation and Classification of Electrical
2. ISO 5208 Industrial Valves - Pressure Testing for Valves
3. ISO 9000 Series Quality Management Systems
4. ANSI/ISA-S18.1 Annunciator Sequences and Specifications

DEFINITIONS AND TERMINOLOGY

Addressable system - a system in which analogue or digital signals from each head (detector or manual callpoint) are individually identified at the control panel.

Addressable head module - the control panel mounted unit in an addressable detection system interfacing with the field equipment via a data highway, handling alarm and fault detection functions. Also know as an Addressable Loop Interface Module (ALIM).

Circuit - the most precise identification in a hard-wired detection system of the location of an alarm within the fire area.

Contract - the agreement or order between the purchaser and the vendor (however made) for the execution of the works including the conditions,

specification and drawings (if any) annexed thereto and such schedules as are referred to therein.

Control action - an output from the control panel that can initiate extinguishant discharge, request ESD action, stop fans and close fire dampers etc. Control actions are divided into two groups per fire area for inhibit functions:
- Extinguishant outputs
- Remaining executive actions.

Control panel - the panel which integrates all the control and indicating equipment necessary for the Fire and Gas System.

Cost of ownership - the life cost of a system including initial supply contract value, installation cost, ongoing support costs (e.g. spares, maintenance and service charges).

Detector interface module - the control panel mounted unit in a hard-wired detection system interfacing with detector circuits handling alarm and fault monitoring functions.

Ex - electrical apparatus protected to meet hazard classification.

Fire area - an area normally bounded by fire walls, physical boundaries such as platform edges, site limits, building walls or partitions and notional boundaries, subject to their fire protection limitations.

Lower Explosive Limit (LEL) - the lowest concentration by volume, of a flammable gas in air that will sustain combustion of the flammable gas. Also known as Lower Flammable Limit (LFL).

Occupational Exposure Limits (OEL) - the concentration, in air, of a toxic gas as defined in HSE Guidance Note EH40. These are normally long term (8 hour time weighted average) and short term (10 minute time weighted average).

Status - the relative condition of a control panel input or output.

Voting system - confirmed fire or gas detection is normally required to initiate a Control Action. Voting generally occurs between 2 - out-of-3 (or more) independently wired circuits of the same type, e.g. smoke, heat, flame or gas.

Works - all equipment to be provided and work to be carried out by the vendor under the contract.

Zone - a part or whole of a fire area monitored by 1 or more detectors, a zone may cover more than 1 room within a fire area.

SYMBOLS AND ABBREVIATIONS

SYMBOL/ABBREVIATION	DESCRIPTION
ALIM	Addressable Loop Interface Module
ANSI	American National Standards Institute
API	American Petroleum Institute
ARE	Admiralty Research Establishment
BS	British Standard
CAD	Computer Aided Design
CCR	Central Control Room
d.c.	Direct Current
DN	Nominal Diameter
EDP	Electronic Data Processing
EC	European Community
EN	European Standards issued by CEN (European Committee for Standardisation) and CENELEC (European Committee for Electrotechnical Standardisation)
ESD	Emergency Shutdown
FGCP	Fire and Gas Control Panel
HSE	Health and Safety Executive (UK Government)
HVAC	Heating, Ventilation and Air Conditioning
IP	Institute of Petroleum
IR	Infra-Red
ISA	Instrument Society of America
ISO	International Organisation for Standardisation
LED	Light Emitting Diode
LEL	Lower Explosive Limit
LFL	Lower Flammable Limit
LPG	Liquefied Petroleum Gas
MAC	Manual Alarm Call Points
NFPA	National Fire Protection Association
NPS	Nominal Pipe Size
OEL	Occupational Exposure Limit
OTDR	Optical Time Domain Reflectometry
OTIM	Optical Transform Image Modulation
PA	Public Address
PAU	Pre-Assembled Units
PC	Personal computer

PLC	Programmable Logic Controller
PPA	Pressure Point Analysis
QA	Quality Assurance
SI	Systeme International d'Unites
UK	United Kingdom
VESDA	Very Early Smoke Detection Apparatus
UV	Ultra Violet
VDU	Visual Display Unit

UNITS

This Standard is based on International System of Units (SI) except where otherwise specified.

PROTECTIVE INSTRUMENTATION SYSTEMS

General Requirements

1. A schedule should be prepared listing all process conditions to be monitored by protective systems. It shall define the limits of safe operation and protective action to be taken in the event of a transgression. The schedule shall list the consequences of failure on demand and the application category.
2. Failure of the protective instrumentation shall not cause the plant to go to an unsafe condition. The effect of failure of any function or group of functions should be fully analysed and the results of this investigation used to determine the design of the protective instrumentation.
3. The action on loss of power supply to protective instrumentation system shall cause the plant to trip.

   In such case a study should be carried out to determine the following:

   a. The cost and probability of spurious trips.
   b. The cost and probability of failure to act on demand.
   c. The risk to cables, sensors and actuators from events which would cause failure to act on demand e.g. fire or explosion.
   d. The additional provision which needs to be made in terms of equipment or routine maintenance e.g. fire proofing.

Choice of Equipment for Protective Systems

1. For Category 1 applications programmable systems shall not be used.

   The main problem of using programmable systems for Category 1 application is establishing the integrity of the software. Emerging International Standards will make such systems non-cost effective for the small number of simple applications in a typical process.

2. For Category 2 applications the choice of systems will depend on the size and complexity of the application. In making the choice the whole life cost including design, installation and support should be considered.

   Protective systems can be classified as follows:

   a. Relay systems (electro mechanical)

      Relay systems should be used where the ease of application, reliability of operation and low cost are paramount. Typical applications are the interlocking and protection of spare pumps or the protection of self contained packages which need not be integrated with the remainder of the process protection.

   b. Solid state systems (hardwired electronic logic)

      Solid state systems should be used where their ease of application, greater reliability and self-checking capability are of importance. They are generally applicable where the function of the system is fixed and unchangeable. Majority voting systems may be applied to achieve the desired reliability and availability.

   c. Programmable systems

      Programmable systems can be split into the following categories:

      i) Fixed Program System

         Where the function of the system is fixed and unchangeable.

      ii) Limited Variability System

         Where the user can configure the particular logic requirement, typically provided by a PLC.

      iii) Full Variability System

         Where the system, in addition to providing facilities similar to those offered by limited variability systems, provide facilities similar to those in a mini-computer based real-time system, e.g. displays, high level languages and data links.

      iv) Pneumatic or hydraulic logic systems. These systems are only applicable to simple applications.

      v) Hybrid system comprising more than one of the above.

Points to be considered in the application of programmable electronic systems include:

a. Failure and Failure Modes

Because a single microprocessor is often used to execute the logic of the application, its, or associated component failure will usually result in some or all logic being halted, e.g. plant protection may be lost.

It is unlikely that the mechanism of failure can be predicted and it is also possible that a fault may lie unrevealed. To overcome these two difficulties, it is necessary to arrange, usually by external equipment, to detect failure and take action (usually by forcing plant outputs to a safe state). In addition, to reveal dormant faults, it is necessary to test the system regularly. It is therefore of the utmost importance to consider the outcome of the failure states in plant design.

In addition to hardware faults, software problems can occur. Software failure cannot occur, but software faults can result either from operating system software being insufficiently tested to reveal faults, or from the application software being unable to cope with a certain plant condition. The danger is that in each case the fault may lie dormant until a particular plant condition is reached and the system then 'fails'. Recognition of these two possibilities leads to important strategies concerning the selection and testing of the system. In the case of faults in the operating system, these can be minimised by selecting a manufacturer who has a standard product implemented widely in industry. In the case of application software it is necessary to apply strict control of the development process and undertake verification of each stage. It is also essential to allow adequate time to test the functions of the application software, both at the development phase and on the actual plant.

To minimise problems with software full variability systems should be avoided. They should only be considered where the complexity of application requires advanced algorithms.

Some manufacturers offer designs which are fault tolerant and this can be of benefit in applications where high integrity is required.

b. Modifications

Because such systems provide flexibility and convenience in configuring logic to meet plant requirements, there is a danger that such flexibility applied in an uncontrolled fashion can lead to downgrading of plant protection following injudicious modification of application software. It is therefore important to ensure that access to, and modifications of, the application software is closely controlled.

c. Overrides and Interlocks

Where override or interlock facilities are provided by application software, a facility should be provided to ensure that the operator and plant manager are aware that the plant is being operated in such a fashion. If the application of overrides is not closely monitored, there is a danger that plant protection is gradually downgraded.

Advantages of programmable systems include the following:

- Space saving
- Low power
- Ease of configuration
- Ease of reconfiguration
- Fault diagnosis
- Simple interface to computers

Disadvantages of programmable systems include:

i) Statutory authorities may impose strict requirements for their application on any safety related duty.

ii) Hardware and software faults (revealed or unrevealed) may result in common mode failure and seriously impair functionality. Careful selection of vendor and his proposal is essential to ensure:

- Vendor has a proven experience in the supply of similar sized systems.
- Vendor has established and effective QA system for both hardware and software design and implementation; including modification procedures.
- Bought-in hardware and software complies with above.

iii) Additional costs can arise in meeting the software QA requirements.

iv) Such systems can be complex leading to more difficult and time consuming fault finding. This can lead to higher cost of training.

3. When programmable systems are provided, their failure modes should be fully considered. The systems should be designed such that in the event of a system failure the plant is not put into an unsafe condition. If failure of the shutdown system could cause an unsafe condition, other equipment or systems should be provided to ensure that the plant is maintained in a safe state.

   A hybrid system using both discrete logic and programmable systems may provide the optimum solution. Hybrid systems also have the advantage of diversity and reduce the probability of common mode failure.

System Design

1. For a Category 1 application a single failure during normal operation shall not cause the system to fail to perform its intended function.
2. For a Category 2A application involving serious commercial or environmental loss, multiple sensors, logic and final actuation devices should be used unless evaluation of the additional reliability and costs against the probability of reducing business loss can be shown to be uneconomic or environmentally unacceptable.
3. For a Category 2B application the use of single sensor, logic and final actuation device is normally considered adequate.
4. In voting systems, precautions shall be taken to avoid degradation of the protection through common faults in the system.

   Examples of common mode problems include blockage of single pressure tappings, blowing of common supply fuses to input channels, or accidental damage to cables run on a common cable tray, or along the same route. Separation of individual protection channels is normally required.
5. Category 1 systems need not comprise of one discrete system of sensors, voting systems and valves.

   An equally satisfactory solution may comprise two or three totally independent trip loops providing each is able independently to take the required action and they jointly have the appropriate integrity.
6. Operational constraints may make it impractical to proof-test the final actuated valve at the frequency necessary to ensure fitness for purpose. In such cases, two valves should be provided, arranged in parallel, with separate isolation and depressuring for on-line testing and maintenance without interruption of the process.

   Additional valves to allow testing on line will normally only be required for Category 1 or 2A applications. Their use should only be considered where temporary shutdown for testing is shown to be uneconomic.
7. Each input shall initiate a latched alarm. The alarm shall signal to the operator the state of the input irrespective of the operation of any defeat mechanism provided in the protection system.
8. Where protection systems are complex and speed of operation would make accurate and timely diagnosis of cause of shutdown difficult, facilities should be provided to record and display the sequence of events occurring in a shutdown.

   The time resolution of events on distributed control systems may not be good enough to diagnose the original cause of shutdown on equipment such as

compressors, turbines and extruders. In such cases special equipment such as sequence of events recorders may be necessary.

9. The dynamics of a system should be considered, in particular, the set point of the detection system should be set such that the end activator can operate and take the system into a safe state, before a dangerous condition is achieved. Quantitative simulation of the system dynamics shall be carried out where systems are identified where speed of response of the protective instrumentation is critical.

   The speed and sequencing of operation of the valves shall also be determined after considering the time available. Closure shall not cause pressure surges in the pipework which could cause damage to equipment.

10. In order to warn the operator, each trip function should be preceded by a pre-alarm from a separate device serving the same process variable or condition.

    It is usual to give the operator warning of an approaching trip condition. In some cases such as flame failure on boilers or turbines, the change from a normal condition to a fault condition is instantaneous or does not allow the operator time to take action. In these cases, pre-alarms serve no useful purpose and should not be used.

11. In programmable systems, facilities shall be provided to test the logic of the program at regular intervals, in order to check the performance of the system.

12. For operational reasons (e.g. plant start-up), it may be necessary to provide override switches on operator control panels and work stations.

13. The need for manual override facilities or defeat facilities to enable testing shall be avoided for Category 1 applications. Where there is a need, such as manual overrides for start-up, the locking facilities provided shall be such as to require a unique control procedure and higher approval authority e.g. Operations Manager.

14. Category 1 trip valves shall not be used for any other function unless confirmed acceptable by reliability analysis. There shall be no manual bypass of such valves. Handwheels shall not be fitted. Where dual parallel valves are fitted to enable on-line testing, isolation valves shall be secured in such a way as to prevent unauthorised operation

15. Where a control valve is used on a Category 2B application or as one of the valves on a Category 2A application a bypass or handwheel may be provided. Where bypass valves or handwheel facilities are fitted these shall be secured in such a way as to prevent unauthorized operation and inhibition of main trip valve operation.

16. For each shutdown system at least one covered and shrouded emergency shutdown button shall be provided. This button should be hardwired to the shutdown system and should bypass any override switch.
17. To maintain the designed integrity of the protective system, unauthorised or inadvertent manual operation should be prevented.
18. The designer should consider the facilities required and the procedures to be followed to allow reliable operation and maintenance during startup, normal operation , equipment repair and shutdown. The facilities and procedures shall be agreed with those responsible for system operation.
19. The system should be designed such that individual items of equipment such as power supplies and input and output modules can be isolated for repair and maintenance whilst the remainder of the system continues in normal operation.

    Account should be taken of any redundancy within the system which could feed a component or input/output device with power from more than one source.
20. Where the protective instrumentation switches and alarms from several plants are in a single control room, it shall be possible to isolate the protective instrumentation system on a unit without impairing operation or protection on the other plants areas.

Equipment Recommendations

1. Input Devices

   Measurements should relate closely to the potential hazard; inferred measurements should be avoided.

   Sensors shall have ranges selected for effective response at the scheduled value of the abnormal plant condition. This may require the provision of additional over-range protection, e.g. for 'low pressure' switches. The switching differential should be checked to ensure that the switch will reset when plant conditions return to normal.

   Where overrange protection devices are used the effect on reliability and failure modes need to be considered. Such devices have proved unreliable in many cases.

   The following should not be used on protective systems:

   a. Mercury bottles as switching mechanism.
   b. Filled systems for temperature switching.
   c. Instruments using self-balancing potentiometers.

d. Differential pressure switches where the switching differential is less than 10% of absolute pressure.

The above have been found to be unreliable in service and difficult to maintain.

The failure modes of the complete measurement system should be assessed to ensure that identifiable instrument, power supply or wiring faults will not result in an unrevealed failure to danger (e.g. one arm of a bridge circuit failing open circuit).

In selecting equipment for shutdown purposes the aim should be to use instruments with a low probability of covert failures. The majority of faults on transmitters are self revealing and these are preferred to equipment such as pressure switches. For Category 2 application the incidence of covert failures can be reduced further by using software trip levels rather than trip amplifiers.

2. Output Devices

For the protection of associated equipment, relays and solenoids should be fitted with correctly rated suppression devices connected directly to the coils.

Solenoid coils shall be d.c. operated. The insulation shall be rated for continuous operation at the maximum ambient temperature. Solenoid coils shall be capable of dissipating the additional power resulting from a higher than normal supply voltage during on-line boost charging.

Solenoid valves should latch in the shutdown position and have facilities for local reset only.

Using solenoid valves which are manually reset locally makes identification and safe clearance of the fault condition more probable. In complex plants involving cascaded shutdowns such practice may be difficult to apply. Where agreed with local operations management solenoids may be reset from a central location except for applications involving the isolation of fuel lines.

Solenoid valves should be sized NPS 1/2 (DN 15) maximum. Their use shall be restricted to pilot valves for pneumatic and hydraulic control and safety systems. They may be used also for the isolation of fuel gas to pilot burners.

Where the protective circuits actuate electrical equipment, this shall be done through interposing relays which are located in separate cabinets.

Where cabinets containing shutdown equipment such as relays are located with equipment not specifically used for shutdown, e.g. in electrical substations, the cabinets should be locked and clearly identified to show that the equipment has a shutdown function.

The operation of motor operated valve actuators shall be controlled by d.c. operated interposing relays, integral with the motor starter. The d.c. supply

voltage shall be derived from the protective system and shall be independent of the contactor control supply.

The reversing starter, interlocking and signaling switches shall be integral with the actuator.

When the operation of two or more electrically operated valves has to be interlocked, (e.g. in order to ensure that a bypass valve is open before the line main valve is permitted to close and vice versa), this interlocking shall be done only in the main electrical contactor circuits. The design shall ensure that any interlocks are effective in all 'remote' and 'local' modes of control.

Actuators fitted to emergency shutdown valves on critical applications involving plant safety shall conform with should be provided with transducers for measuring on-line performance.

If the actuator does not reach the required position within a predetermined time period after action is initiated, a 'valve fault' alarm shall warn the operator. The alarm supply shall be independent of the actuator supply.

Performance measurement is particularly important on large valves where the actuator design margin may be reduced by wear or fouling.

3. Circuit Modules

Removal of a plug-in module should initiate a shut-down action to/from the system for that module position. Alternatively for Category 2b applications the system may remain in the untripped state providing diagnostics are provided to indicate to the operator that the system is no longer active.

Modules that need to be calibrated, e.g. analogue input modules, should have defeat and test facilities that allow in situ calibration by a single technician.

The system as a whole, and each type of module, shall be unaffected by radio frequency interference, even when doors or covers are removed for maintenance.

When the modules incorporate self diagnostic circuitry, the choice of alarm or trip action to be taken on detection of a fault. Each output module shall control a separately fused supply to each associated actuator. The output fuses shall be individually accessible.

Plug-in modules should be removable under power.

4. System Alarms

Protective systems should have facilities to monitor failure states. There should be alarms for system malfunctions, and for the loss of power supplies to the logic and external circuits.

5. Power Supplies

   Relay systems shall be segregated into functional loops, each supplied through a separate switch and fuse.

   On earth-free systems, double pole power switches shall be used.

   Separate power supplies should be used for actuation circuits unless it can be shown that the effect of switching transients is unlikely to effect input or logic circuits.

   The filter circuits of input modules and logic power supplies will need to be considered to establish adequate rejection of transients.

   Batteries shall be capable of maintaining power for logic and actuating devices for pre-defined period following a primary power supply failure.

   The pre-defined period will need to be sufficient to allow an orderly shutdown of the process. The period will depend on the complexity of the process and the available manning. The period should be agreed with those responsible for Operations Management.

   The components of the logic power supplies should be so arranged as to permit any one of them to be removed for maintenance while the system stays on line, and under power.

Testing

1. Facilities to enable on-line testing of protective instrument systems should be provided unless adequate reliability can be achieved by testing during planned shutdowns. On spared equipment, batch or cyclic processes, test facilities for use on line are not required provided testing can take place during normal operation without prejudice to production.

   Test procedure should be considered at the design stage and an outline test philosophy defined.

   It is of paramount importance that systems installed for the protection of plant and personnel will operate correctly and reliably when a potentially dangerous condition is approached. Systems may remain static and may not be called on to operate for long periods of time. Failure of a component part of a system may not be apparent to the plant operator since the system does not play any part in the normal routine control of the plant.

2. The quality of shut-off and the on-stream testing required should be stipulated during the design stage. During the reliability analysis the sensitivity of leakage rates should be ascertained and where leakage cannot be tolerated in any circumstances, alternative designs should be considered.