Session One:

A Practical Approach to Managing Safety Critical Equipment and Systems in Process Plants

Tahir Rafique

Lead Electrical and Instruments Engineer: Qenos Botany Site

Douglas Lloyd

Senior Electrical and Instruments Engineer: Qenos Alkatuff Site

Ken Evans

Senior Electrical and Instruments Engineer: Qenos Altona Site

Summary

This paper presents a model to manage safety critical equipment and systems. It also discusses some practical ways to comply with operations and maintenance aspect of safety life cycle. Although the main focus of this discussion is Safety Instrumented Systems, the management model is applied broadly to manage equipment and systems that form the last line of defence against hazardous events, such as safety relief valves.

The approach has been developed and tested over a considerable period of time and has been continuously improved as the standards and improved technologies have emerged. Ideas on developing management procedures, training, proof testing and performance analysis to improve reliability of safety critical systems are discussed in some detail.

The Management Model

The objective for this management model is to provide the needed focus on integrity of safety critical equipment and systems. To remain competitive, organisations cannot afford to over maintain these systems. However, maximum safety must be ensured in order to minimize risk of incidents. Therefore the management processes and strategies have to be:

- Robust
- Practical to use
- Have leadership at the right level
- Define clear responsibilities
- Improve performance

The proposed model to manage safety critical equipment, devices and systems is shown in figure 1. The key elements of this model are:

a) Having a clear corporate policy on management of safety critical equipment, devices and systems

b) Defining the requirements and standards that reflect the policy

c) Having detailed procedures for proof testing and defeats

d) Training people on these procedures and equipment

d) Scheduling and testing of safety critical equipment and systems

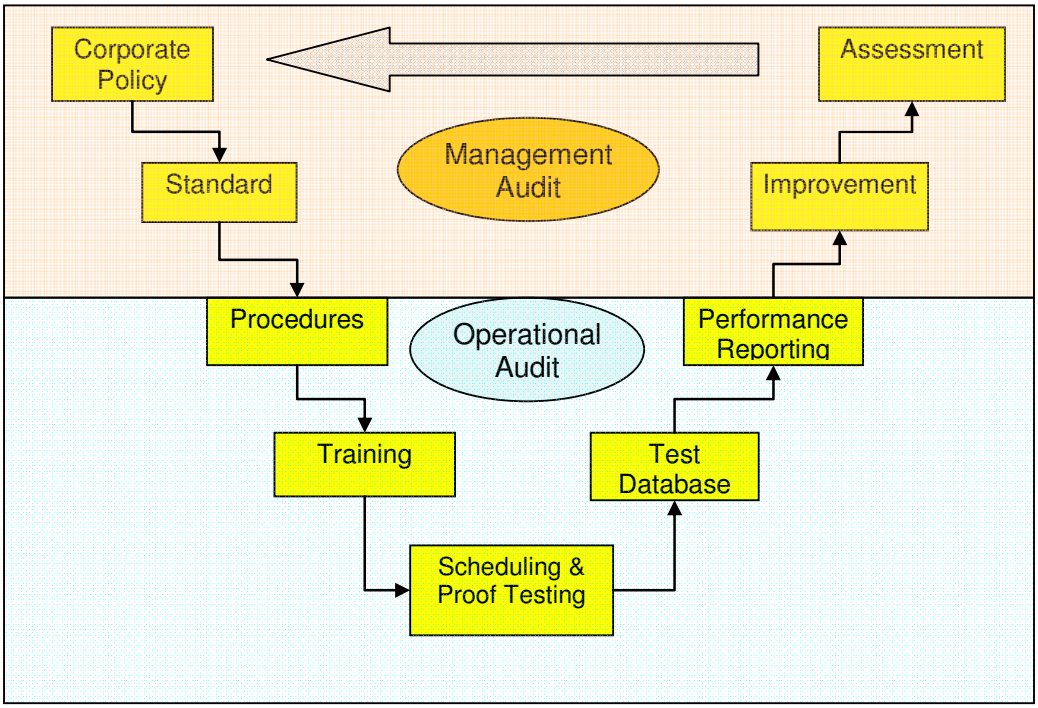
e) Having a system for recording test results

f) Analysing performance

g) Improvement programs to eliminate gaps and bad actors

h) Assessing the model for its effectiveness at an operational as well as management levels

Fig. 1 - Model for managing Safety Critical Equipment and Systems



Policy and Standards

The organisations dealing with hazardous materials and processes need to have a clear policy on safety critical systems. It is not sufficient to say that we will have the process operating safely. A good policy needs to be more specific and direction setting. For example it is better to state that the organisation shall have a system to manage critical equipment and systems. The management system should ensure that the critical equipment is identified, risk assessed, documented and maintained to meet reliability targets.

Once an organisation develops such a policy on safety critical equipment the engineers can start defining the specific requirements and standards that will be necessary to meet the company policy. This will need defining the tolerable risk level for the organisation and equipment reliability necessary to bring the process risks to the tolerable level. The definition of critical equipment and systems therefore needs to be broader than just Safety Instrumented Systems. It includes any equipment or device that forms a last line of defence against a hazardous event. For example pressure relief devices, safety block valves, and even the devices that mitigate risks such as gas detector, aviation light on top of a distillation column or an effluent diversion valve to safeguard environment needs to be included in the scope of management. The first step is to identify inherent process risks and then the protection layers that mitigate the risk and help achieve a tolerable level of risk. The identification of these devices will result in establishing a register for safety critical devices. It is also equally important to indicate these devices on the PI&D drawings with a special symbol and identify them in the field with a colour or a distinctive label. For example if a control valve is being used as an emergency block valve, and if there is a bypass valve for control valve then the bypass valve closure should be identified as critical and labelling this bypass valve on the drawings and in the field along with a chain lock will help reduce possibility of the valve being in wrong position. Once a register is established, the targets for integrity of each device can be defined and SIL calculations done to determine if integrity levels will be met based on certain test frequencies.

Ideally an organisation should cover these issues in a safety or risk control manual. The manual should give guidance on how to assess risk; document common risk control measures and availability targets for safety equipment; and give guidance on how to comply with industry standards such as IEC 60511

Another key aspect of developing standards is to have a structure of ownership that is associated with the management model. It is essential to have a sponsor on the top management level to steward the policy and to have some one champion the administration of the model at each site or a plant. The administrator ensures the model is operational and that each component of the model for the management of safety critical equipment is effective.

Developing Procedures

The Management of safety equipment requires clear procedures for maintenance, testing and defeat. Three key categories of procedures needed are.

- Proof Testing Procedures
- Management of Defeats Procedures
- Management and Control of Change

The proof testing procedures define what is to be tested and the rationale behind it and how it should be tested. These also include what equipment is to be used for testing and links to work permit system and communication of precautions to process operators and maintenance technicians. If there are defeats to be applied for testing it is recommend to have a joint operational / maintenance sign off when the defeat is placed as well as when it is removed to minimise human error. The procedures should be controlled documents and verified in the field for their practicality. Failure criteria and the action to be taken on failure must be specific and clear to the tester and operator. It is important to find the root cause of failures and apply appropriate corrective actions to eliminate the root cause especially for situations where a device is found failed to danger during testing.

Try to avoid situations where testing would drive process into a demand or where logistics of carrying out a test would put people and/or plant at risk.

In one particular audit of a test procedure a pressure sensing device was located on top of a column. The access was by a ladder. The procedure required pressure injection using a nitrogen cylinder. It was obvious that it was risky for the technician to carry all the equipment to the top of the column. Therefore it was necessary to look at a different approach and put in a corrective action to remedy this procedure.

In process plants it is often necessary to defeat a trip for operational reasons such as start-up, repairs or for testing. Procedures around management of defeats have to be robust. The defeat procedure should require a formal authorisation of a defeat at an appropriate level depending on the risk and the length of time it is to be applied. The documentation for defeat approval should as minimum have:

- What is being defeated
- The reason the defeat is being applied
- What hazard is created
- What alternate protection is available
- What precautions are required
- How long the defeat is to be applied
- What level it needs to be authorised

Once the defeat is authorised it should be communicated to operators and all other people who work on the equipment. It may be incorporated in the shift logs. We have also found that having a board specifically for defeats in the control room is a good way to prompt discussion at shift handovers and doing job safety analysis for work permits. It also gives a good indication of the number of active defeats and if the system is being used effectively.

It is often the case that components in a safety instrumented functions have to be replaced or a logic change has to be made. A robust control of change procedure will ensure that risks associated with the change are assessed and the impact of change on the process and operations are minimised. These procedures should be applied whenever the hardware change is not like for like, and when making changes to logic or changes to trip or set points. Sometimes a change may seem simple but can have dire consequences. For example a simple change of a process isolation valve which looks the same in every respect may have different materials that are not compatible with process medium could prove disastrous. Similarly a change in set point to the unsafe side of design parameters can prove catastrophic. Therefore, changes must follow structured hazard risk assessment, carry out necessary safety studies and multidisciplinary reviews.

Training People

Once the standards and procedure are defined, training needs of different groups can be assessed as training is normally specific to the job roles. For a start, every one in the organisation will need awareness training on:

- what is the policy for managing safety critical equipment
- what is expected to be achieved
- who is responsible for what equipment and system

Personnel such as operators and maintenance technicians will need a detailed training on testing and defeat procedures. This training needs to be formal and documented for people to be authorised for testing and repairing safety critical devices and systems. A refresher every two or three years ensures that knowledge is kept current.

Proof Testing

The aim of proof testing is to discover any covert failures, confirm the correct operation and calibration of the sensors, logic and final elements. Ideally process variables should be manipulated for a full functional test if it is practical. However in process plants that were built without trip testing in mind manipulating process variables to trip test is not always practical, therefore the only practical way is to test such loops in segments. The operation of sensors and calibration has to be checked independently.

- **Testing Pressure Loops**

It is often difficult to manipulate process pressure for testing. One of the common approaches to test is by injection of a pressure signal in to the measuring instrument while the instrument is isolated from the process. The vent connection is used for injecting a compatible fluid and pressuring up. The actuation of trip is usually defeated with alarms still active. A certified hand held calibrator can be used to check if the trip operates at the correct pressure. This however does not check plugged impulse lines. Therefore proof testing should include procedures for clearing impulse lines where it is safe to do so. With smart transmitters replacing conventional transmitters, there is increased confidence in the measurement due to self diagnostic features of these devices and some sites are making use of this capability to monitor transmitter problems, and also being able to drive their outputs to test the rest of the loop. Even though it is practical it is not a replacement for a complete proof testing which should be done every time the opportunity is presented.

- **Testing Temperature Loops**

The manipulation of process temperatures is also not practical in most cases and proof testing temperature loops presents a real challenge. Using temperature baths is also not practical in many cases especially where hazardous areas are present. Most common approach is to use duplex sensors and comparison of two sensors or comparing with another local thermometer. Some plants just disconnect sensor to test the rest of the loop by simulating signal from sensors and rely on changing sensors regularly during periodic maintenance. Diagnostic coverage can be improved by using smart transmitters or interface devices to detect burnout or broken wire to drive signals up to a detectable value. However these methods do have a disadvantage of not testing problems of sensor / pocket interface

- **Testing Level Loops**

Proof testing of level loops depends on the type of devices used. Manipulation of process variable is preferred if doing so does not present too much of a risk. For example where vessels are fitted with level gauges in addition to trip switches, correct operation of the level switch can be tested by observing level on the level gauge and operator action can be taken to avoid a hazardous situation during testing. Where manipulation of level is not possible the level switch is isolated from the process, drained and filled to activate the critical function. It is critical that the Specific Gravity of test fluid is compatible with the process.

- **Unobtrusive Testing**

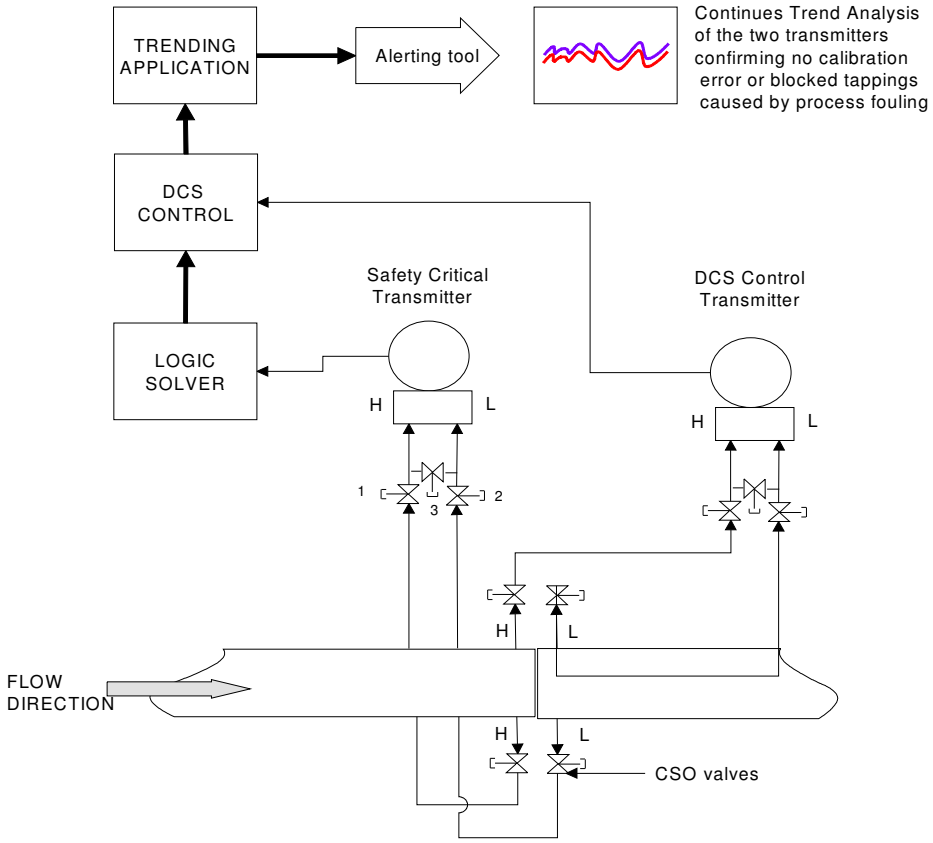
One of the other practical ways to testing is what we call unobtrusive testing. If monitoring tools are put in place such that deviations are being checked continuously and maintenance response to any unacceptable deviations is guaranteed within a certain timeframe then it is reasonable to consider applying test intervals matching that timeframe. In such instances, the reliability of the system providing the deviation alarm, as well as the reliability of the maintenance response procedures, must be reviewed and documented to ensure they don't compromise the base SIL calculation. This approach is practical when there are independent control and trip sensors used for the same process parameter. It can be applied to most kinds of sensors that provide a continuous measurement of a parameter rather than switches.

As described above, although the trip logic integrity is ensured by having independent sensors and logic solvers, the monitoring and alerting tools also become a critical part of the system. A better diagnostic coverage can be achieved with automatic alerts to maintenance people. The monitoring system essentially looks at comparing signals of trip sensors with that of process control system in DCS and creating deviation alarms. The monitoring alert is setup to notify of problems. This also reduces the potential negative impact of testing disturbances and human errors on the safety critical device

Each application will have to be individually assessed to determine if the service is suitable and if so what trend deviation is acceptable, how many transmitters can be monitored and what sort of common cause failures could occur. All these factors will be taken into account in the SIL calculation to determine the frequency of test against common cause failure, predominantly process related. (eg blocked impulse tapings). If the response times are short then PFD levels in the SIL calculations will approach those of final elements. The communication channels from logic solvers to DCS are generally in redundant configuration and alarmed for failures therefore the integrity of monitoring systems is high. It is expected that trip sensor testing interval can be stretched considerably saving maintenance resources and costs.

The example of this set up is shown in figure 2. This shows a flow element with two independent tapings incorporating a standard DP transmitter. This concept equally applies to Pressure, Level or Temperature transmitters with 2 or more sensor tapping points as long as the process variable is not static. It provides a better monitoring of covert failures also taking into account the flow from the actual tapping points rather than just testing from the manifold.

Fig 2
Typical Flow DP transmitter calibration check with Diagnostic Coverage



- **Testing Final Elements**

It is well known in process industry that final elements failures account for half of all failures. Ideal case would be to test final elements as part of an integral testing of whole loop. This is usually possible if process can tolerate a shutdown. In plants where production is shut down regularly for maintenance, extensive loop testing can be done during the shutdown. The argument that is usually presented is that final elements don't see process conditions during testing. In such cases where it is crucial to test final element under actual process conditions, testing of the final elements can be practiced by actually tripping the process when it is being taken off line for a shutdown. The care should be taken that such testing does not create any other safety risks when tripping process in anger. The main concern here is to consider how to control the risk if the final element fails.

The testing of final elements really presents challenge where process can not be shut down and time intervals for maintenance turnarounds are substantially longer than calculated test frequencies. The policy and standards of the organisation should give guidance to such situations. Before IEC 61511 was introduced not many processes used fault tolerant designs for final elements even for situations that required SIL 2 type of

integrity. In many cases the control valves with a solenoid trip were used to perform safety function. The operators considered it was sufficient to test such loops up to solenoid valves arguing that control valve is being exercised regularly but this does not test the valve for its intended functionality.

Where emergency block valves are fitted, limited testing can be done by manually inching the valve and again this does not test the full functionality of the valve. There is always reluctance to test emergency block valves that open to vent to mitigate hazardous situation. Partial stroke testing devices are improving with technology and retrofitting such valves with partial stroke testing is gaining pace. Some manufactures claim good credits in PFD levels. We are currently evaluating retrofitting these on existing emergency block valves that are production as well as safety critical. There is also an increased awareness of testing requirements and having fault tolerant systems in designing process plants today than it was 10 years ago for example we see tandem Pressure Relief devices are becoming common where one device can be removed for pop testing.

System for Recording Test Results

A system to record the test results is absolutely essential and it is a lot easier if it is linked to overall maintenance scheduling and recording system of the organisation. The results should indicate correct operation and calibration as found. The results should also record failures where the device fails to meet its criteria and protective function. It has been a commonly observed that technicians would calibrate even if an instrument deviates within the defined limits on either side if trip point. Therefore, it is a good idea to clarify the requirements of recalibration of devices. It is better to leave the device as found if it is within the defined limits.

Analysing Results, Identifying Bad Actors and Performance Reporting

The system of recording results will be no good if one can not analyse test data for:

- Systems and device reliability targets are being met. Comparing current PFD for device against calculated.
- Any bad actors emerging. A Critical safety device failing more than once would need its test interval reviewed and test intervals may need to be more frequent based on the type of service, its environment.
- On the other hand test intervals for the critical devices which are far exceeding their MTBF expectations can be optimised
- Analysing exceptions that exist if a function is not being tested or not being tested right down to final element. These exceptions have be brought into management review

Improvement Programs to Eliminate Bad Actors

Common causes or root cause failures are established to identify corrective actions and improvements. There should be a three yearly rolling improvement plan and review of this plan every six months

Best practice sharing should be encouraged between sites through combined review meetings with sponsors and owners of the systems

Assessing the System of Managing Critical Safety Equipment for Effectiveness

The system effectiveness has to be evaluated at two levels:

- At operational level
- At management level

The operational level will look at performance indicators that come out of testing the devices such as:

- Number of tests scheduled and number of tests overdue
- No. of Dangerous Faults uncovered in testing
- No of spurious trips
- No of defeats placed for maintenance and testing
- Number of overdue Safety Critical tests
- Progress of Improvement plans

At management level the sponsor has to be satisfied that the model for management of safety critical equipment and systems is effective. The assessment can be independent like an audit of systems and compliance to the systems. The gaps should be identified and long term improvement plans should be actively pursued. Such extensive audits do consume time and resources and should be carried out every two to three years once the model is implemented.

Conclusion

The management of the safety critical equipment and systems can be effective with the use of management model suggested in the paper. The organisations policy and standards determine how effectively the management system operates. The proof testing has its challenges. However, practical ways to test the equipment have to be implemented. The improvement cycle can only be closed if performance is regularly assessed and reported.