1.0 INTRODUCTION:

Today's communication technology, spearheaded by the Digital India movement, has made it possible to make any system available at a remote location. Video Calling, Location tracking, Telepresence systems have bridged the distance barrier. Remote Operation of industrial complex is one such technological marvel.

Hydro Power Plants are generally considered suitable for remote operation due to less complexities and also to reduce the hardships entailed due to typical remote locations of such plants. All the more, if the planning of Remote Operation is done at the design stage, the land requirement can be reduced; this can also reduce forest degradation to some extent.

2.0 CRITERIA OF A REMOTE OPERATION SCHEME:

a) **Safety:** Safety is the **fundamental** aspect which cannot be comprised at any cost. Hence, it has to be ensured that doing a remote operation in no way endangers the human lives and equipment. This in effect is ensuring that the system fails **safe**; no spurious command is issued, no accumulation of commands, timely annunciation of a link failure so that the system shifts to local mode from remote in the slightest concern.

b) **Response:** One of the most prominent concern in remote operations is the latency introduced through the communication system of the remote operation. No amount of latency should be perceptible to the operator.

c) **Resiliency:** Needless to say, the communication system should be robust to withstand any single failure, be it in the link, the networking equipment or the end operation devices, not to mention the connecting cables. Hence, the design should have inbuilt resiliency.

d) **Cyber Security**: This is the topmost genuine concern in the sense that many of the recent attacks including the Ukraine blackout has sprung due to cyber attack on remote networks. The fact that the remote connection will be on, 24 X 7 certainly raises security issues, which needs to be mitigated in a foolproof manner.

3.0 PLANNING THE CONCEPT:

As with all new technology implementation, the strategy was to get a proven scheme to build on, or to engage a consultant in this important endeavor.

It was known that remote operation of Hydro units is a standard practice in France in EDF hydro stations. The concept there is for complete man less stations.

Stories of remote operation of gas fired power plant in Australia from a remote center in Brisbane was also heard; but as

per system integrator information, only sequences were operated using OPC protocol.

NTPC being a technology leader, decided to develop the scheme in house, without any external consultant. The technical acumen and the ingenuity of BHEL, EDN expert was a major strength and certainly a key factor in taking this decision.

A visit to Koldam site was undertaken with representatives of Operation Services, IT and BHEL, EDN expert.

4.0 TECHNOLOGY SELECTION:

a) **OPC**: The main interfacing protocol between DCS systems at HMI level is OPC, which is used for signal exchange on a soft link. An advantage of this scheme is that the system at remote end need not be same as that in the Hydro station. Also, since all tags are exchanged, an independent history can be provisioned. However, there have been cases of non-deterministic response time on OPC and response time being a critical requirement; it was not possible to take any chances on this front.

b) **System Bus Extension**: Mooted initially by BHEL, EDN, this option is to extend the DCS bus to the remote operation center, which in this case is a 100 Mbps network. Apart from security concerns, there was no real advantage in this option. Further, with 100 Mbps speed, MPLS link would have been a costlier option. Hence, this was not considered.

c) **Secured Front end communication** In this option, remote control of the HMI at the central control room of power house was made available at the remote center.

Option c) was considered the simplest, efficient and secure method & was finally selected.

Then came the choice of the communication link. An MPLS link was already provided for data transfer to ERP system, but the same was not selected for reasons of non-availability of exclusive bandwidth and also for clear separation of the OT & IT systems. Redundancy of the communication link was needed; hence two links from separate companies were chosen i.e. PGCIL and BSNL. MPLS link being a leased line, provided the security of a virtual point to point link. All the communication and security hardware were made redundant & in HA (High Availability) for obvious reasons of resiliency of the scheme.

5.0 SITUATIONAL AWARENESS:

Apart from providing operation facility, it is also important the operator at the remote-control center gets the same situational awareness as that of the local operator at the central control room of power house. Hence, CCTV system has to be an integral part of the remote operation scheme. Since video signal consumes bandwidth, a separate dedicated MPLS line was earmarked for CCTV.

Further, facility of PA (Public Address System) also becomes necessary, to get in touch with any area of the plant as the local operator. This was not only included; but also, a hotline facility with the local operator was provided to augment the requirement. A VC facility was also provided.

Apart from the main HMI, there are many other systems, which are used in the central control room of power house like ABT, Flood Monitoring etc., which were also included in the Remote Operation scheme, albeit not through the main MPLS links.

6.0 CYBER SECURITY MEASURES:

In terms of Cyber Security measures, there was an edge. NTPC had already designed a secured network architecture for DDCMIS with the help of a consultant in 2008 and the same was included in the engineering of all systems thereafter. This was perhaps the first of its kind in the critical infrastructure of the country. Based on which, IEC 622443-2-4 project team had invited NTPC to contribute in this standard.

But the challenge was that for these DCS systems, only one-way data transfer to Enterprise system was provided only for information purpose. Nowhere, this architecture had been used to operate the unit, as the Unit HMI OWS was totally isolated in the architecture i.e. DCS was totally in air gapped mode. After many deliberations, BHEL, EDN devised a unique method by which operation could be possible without comprising the security.

Further, the latest security measures like VPN tunnel, two factor authentications were implemented, which added to the security posture of the scheme.

7.0VALIDATION OF THE DESIGN:

Since PGCIL is operating the sub-stations remotely from its NTAMC, Manesar facility, a visit to this facility was undertaken. The following takeaways emerged from the visit.

- Remote operation of 104 substations out of 204 is being done from NTAMC, Manesar
- No operation manpower is positioned at 104 substations & maintenance hub is there for several substations from which staff visits site as per requirement.
- Operation is always done along with CCTV monitoring.

- PGCIL is using its own OPGW (optical ground wire) based communication network for both the links.

The scheme of remote operation was studied wherein it was found that the scheme of sub-station operation was exactly in line with the scheme developed for Koldam remote operation, except that both the links were from PGCIL. Thus, the visit to NTAMC, Manesar provided the design validation of the Koldam scheme, even though the applications were totally different.

8.0 IMPLEMENTATION:

Now, Remote operation of Koldam units have been commissioned & put to use in the month of March 2018. Multiple trials are in progress for operation of the four units of Koldam Hydro from Scope Complex office of NTPC.

9.0

10.0 THE WAY FORWARD:

Having accomplished operation from a remote center, situated nearly 400km away, many possibilities further emerge, which can go a long way in shaping O&M strategy. These are discussed below:

(1) **Establishment of Continuous Operation**: It is necessary to build confidence in the remote operations to stand in the event of all emergencies and exigencies.

(2) **Integration of all Local Operations in the Remote Scheme**: Having accomplished all the operations done from the Power House Control room from remote on continuous basis, the next step could be attempting the operations not done in the Power House from the remote center. i.e. operations of Switchyard control room, Spillway, Main inlet valve. However, it is important that nowhere the safety is compromised. Hence, this has to be attempted very slowly giving ample time at each step to build up the confidence.

(3) **Extend Remote Operation to Remote O&M**: Till this time, only remote operation has been presented which will only optimize operation manpower; but with the help of digital technology, opportunity exists for optimization of maintenance manpower as well. In the sub-station case, which is no doubt quite simple compared to a hydro station, there is a maintenance hub for every group of sub-stations. But this depends of the level of reliability of the equipment's in the hydro station. As such, this should the last step in the ''Remote Journey'. Probably, in 2032, we could see such a situation too.

11.0 CONCLUSION:

Technology throws lot of possibilities but has its own list of pitfalls. Hence, it is very important that the design leveraging advanced technology is reliable and meets all the expectations of the end user for whole hearted acceptance. It is also important to learn the lessons from the implementation and do course correction.

12.0 ACKNOWLEDGEMENTS:

The authors are extremely grateful to Mr. P.K. Mohapatra, Director(Technical), NTPC and Mr. G. Venu, Executive Director(Engg.), NTPC for their constant encouragement & support for exploring new horizons. The authors are also grateful to Mr. A.K. Gupta, Director (Commercial), NTPC for initiating this concept in a Professional Circle Meeting, and Mr. S.K. Roy, Director(Projects),NTPC and Mrs. Arundhati Bhattacharya, Ex. ED(PE-C&I),NTPC for their untiring efforts in pursuing this concept and Sh. C.V.Rao, GM(I/C-IT),NTPC for technical guidance. Special thanks are also due to BHEL, EDN's expert Sh D. Prakash for achieving the vision of NTPC through his rich technical expertise and innovative thinking. Last but not the least, the last lap in this journey could not have been completed, had the young & dynamic team of NTPC engineers, namely Sh. Amit Kumar Singh, Ms. Uzma Ayaz, Sh. Rohit Sharma and Sh. Somenath Kundu not put their dedicated & whole-hearted efforts. The authors also express their gratitude to ISA, Delhi section for providing an opportunity to share their work & perspectives, for the benefit of the automation fraternity.

BIOGRAPHIES:

Mr. M.K. Srivastava is General Manager in Project Engineering Division NTPC Ltd. and heading the C&I Dept. in its Engineering Office Complex, based in Noida.

Mr. Srivastava has 30 years' experience in power plant C&I engineering during which he was involved in the engineering of many coal based thermal power plants, gas based combined cycle power plants and hydro power plants as well as factory testing of many DCS systems.

Mr. Srivastava has spearheaded the development of many guidelines, policies & procedures in C&I Engineering and is credited with the success of new bidding processes in NTPC. He has also been associated in the commissioning of several C&I systems at site. Currently, he is a member of the steering committee for Lara. He has contributed in development of intelligent cable engineering and ICS software for which copy right have been obtained by NTPC. Under his tutelage and direction, many new initiatives like Digitalization, Complete Water Management has been undertaken.

He has authored papers, for national & international conferences including the International Society of Automation (ISA) POWID division. He is President- Elect, International Society of Automation (ISA), Delhi Chapter.

Mr. Srivastava has done B.E in Control & Instrumentation from N.I.T., Surat

R. Sarangapani is an Additional General Manager in Project Engineering-C&I Dept of NTPC Ltd. in its engineering office, based in Noida.
His exclusive focus areas are HMI engineering, Third party interfacing & OPC, Display systems, control system networking, Network security, Closed loop control, Power Plant Performance Optimization, Simulator, and Standardization in engineering processes. He has also been associated in the commissioning of closed loop controls at site.

He has authored papers, for national & international conferences including the International Society of Automation(ISA) POWID division, for which he had coined the theme “Empowering Power with Automation” for its first conference of its Delhi Division in 2009.

He has been a topic leader in the team for preparation of IEC 62443-2-4 standard for Cyber Security of Industrial Automation Systems. He was also involved in the preparation of the Indian manual for Cyber Security in Power Systems.

Mr. Sarangapani has done B.E in Control & Instrumentation from Thapar Institute of Engg. & Technology, Patiala & MTech (Eq.) in Computer Science from IETE.

Process Safety: Moving from Voting to High Diagnostics Logic Solvers

Jayesh Bhavsar

Siemens Limited, Mumbai

Abstract:-

In 1970's, most of the safety related logic solvers, examples 1oo2 one out of two architectures, 2oo3-Triple Modular Redundant (TMR) architecture, used redundancy for voting to achieve specific safety availability. These architectures could not tolerate dangerous failures of their voting components without compromising their safety reliability because all their components were necessary to vote for a safe resolution.

Two decades later, the old voting concept was replaced by use of comprehensive diagnostics in order to protect outputs. This new approach was based on the fact that higher degree of safety reliability could be reached in case a fault was detected and if the diagnostic circuit could force a safe switchover. This was a big step forward by implementing the diagnostics as safety availability in safety architectures becomes less dependent on voting.

Today, there are systems, Example- Flexible Modular Redundancy (FMR) that can tolerate several random failures, without compromising safety integrity level and without shutting plants down.

The purpose of this paper is to discuss such architectures.

Introduction

The term "Redundancy" has been used in process automation for decades, yet it meant different things to different people. It all depended on the purpose of the application that each individual was designing. In other words, redundancy has been implemented to only achieve safety, to only increase reliability and with both goals in mind.

Originally, in safety applications for the process industry, the term redundancy meant: "separated resources performing the same logic". The idea was to have a final comparison of each output from each resource with the reasoning that the statistical chances of obtaining the wrong answer would decrease with increasing number of voting individuals. This implied the use of redundancy to minimize dangerous functioning in "Majority Vote" architecture. e.g.: A two out of three voting architecture (2oo3) meant that at least two resources must have agreed on a particular output before it became true.

It all makes sense if we consider all possible behaviors of a safety system (Figure 1-1). Any given system has a probability of performing as intended at a given time. This is known as the "Availability" of the system. On the other hand there is the probability that the system will fail to function correctly. In such cases two things could

Distributed with permission of author(s) by ISA Delhi Section [2018]
Presented at [ISA (D) Petroleum and Power Automation Meet 2018]; http://www.isa.org

happen: 1 – The system may shut down the process without any reason. 2 – The system may fail to stop the process when a dangerous condition is present.

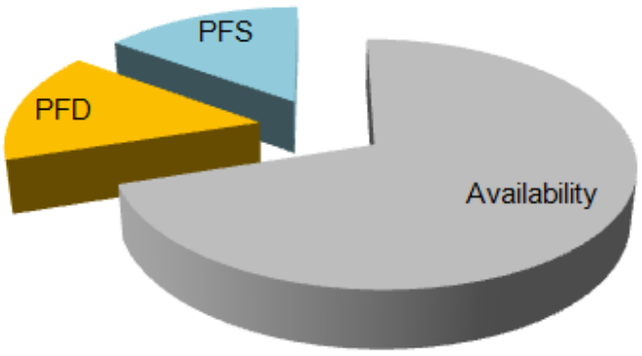


Figure 1-1: Probabilities outcomes with no credit for Diagnostics

Thus, there is a probability that a system will perform correctly, there is a probability that a system will fail safely (PFS) and there is a probability that a system fail dangerously or "On Demand" (PFD). In this paper, we will only consider low demand mode.

As the very first systems to perform a safety function were designed, it became apparent that in order to make a system "Safe" the "Probabilities of Failing on Demand" should be kept as low as possible, and redundancy was applied with this only goal in mind.

In fact as far as safety is concerned, the statistical average probability of the safety function failing to take the process to a safe state is what defines the concept of "Safety Integrity Level" (As defined by IEC 61508, IEC 61511), and redundancy for voting was originally used to achieve the required SIL.

On the other hand, when considering process industries, unnecessary shut downs are to be avoided at all times. This is not only because of economical implications but because it can create unstable unsafe situations. To avoid such nuisance trips designers also used redundancy to increase availability. In this case the "Redundant" resource is in "Stand By" mode, and will be used when the principal resource fails. For example, in Emergency Shut Down Systems (ESD), it is common to duplicate power supplies because an interruption of power would shut down the process.

In the next few pages we will analyze different architectures that were developed to increase safety reliability and we will examine the impact that such architectures have in the process availability.

Architecture "One out of two" – 1oo2

One of the possible solutions to decrease the chances that a logic solver would fail on demand was to duplicate the resources. The idea was to decrease the PFD in the principle that both resources have to fail on demand for the system to fail dangerously. (Figure 2-1)

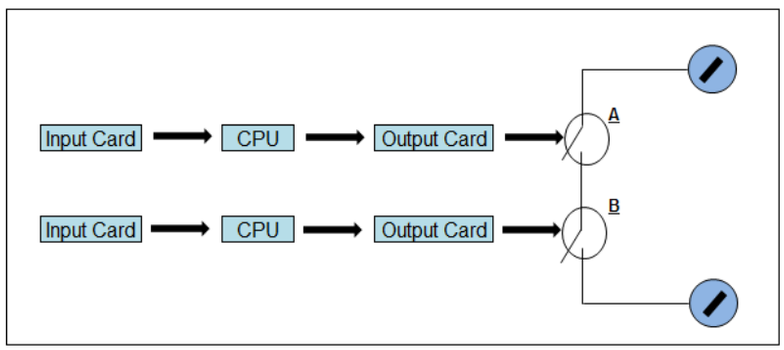


Figure 2-1: Architecure 1oo2 for Safety Related Logic Solver

Here, the advantage is obvious as the PFD of the system is the product of the PFD of each resource (for de-energize to trip, PFDsys = PFDA x PFDB). This can be deduced with a simple fault tree analysis. Since PFD < 1, PDFsys is smaller than PDF of each resource.

Yet this architecture had two disadvantages:

1 – The chances of this system having a spurious trip have doubled as compared to a single resource, thus decreasing availability. In other words, any of the two redundant resources failing safely would cause a spurious trip, and although very safe and suitable for machine or transportation applications, this architecture is not suitable for process safety where such trips are not acceptable (Figure 2-2).

2 – The system tolerates one dangerous failure, but it degrades to an architecture 1oo1 (Figure2-3) with a PFD equal to one of a non-redundant resource. i.e.: The system must be restored quickly as the degraded state (1oo1) does not provide adequate safety protection. (For simplification purposes, common cause and second order effect were not included)

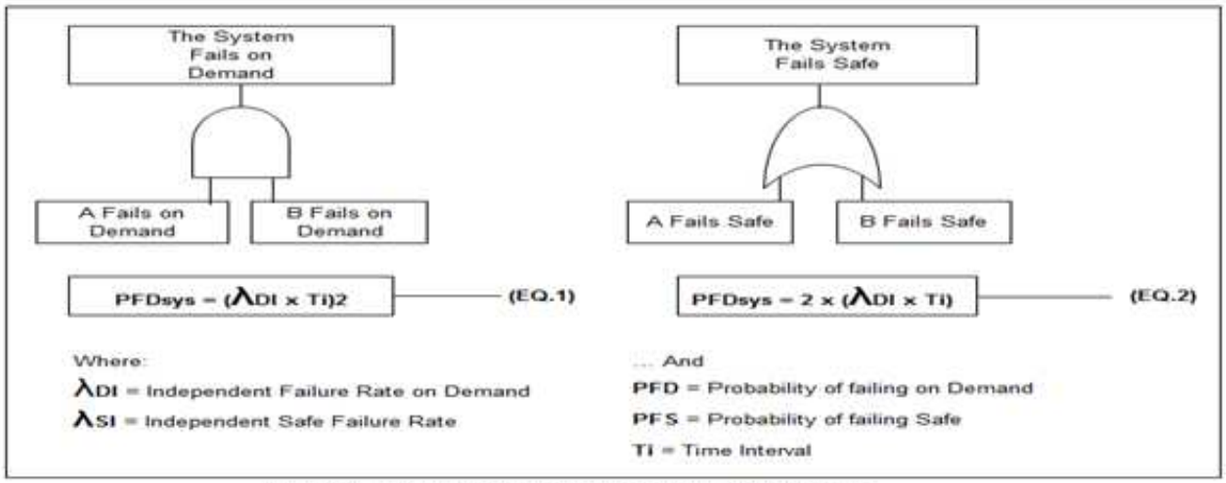


Figure 2-2 : Simplified Fault Tree Analysis for 1oo2 Architecture

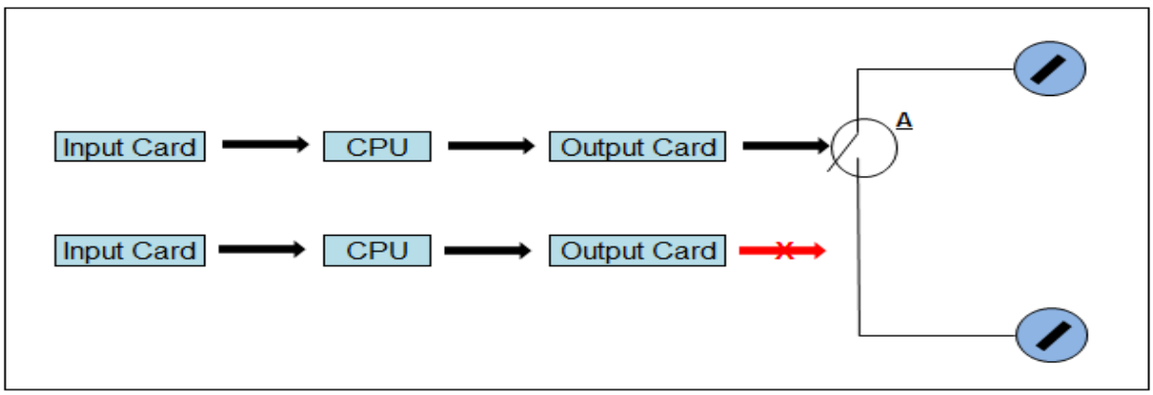


Figure 2-3: When degraded due to a dangerous failure of one of its resources architecures 1oo2 for safety Related Logic Solver becomes 1oo1

Similarly, architectures 1oo3 were found to be even safer, but with three times more nuisance trips. This was not an acceptable process safety solution.

"Triple Modular Redundant" – TMR –Architectures

Another solution in the search for a system with low PFD and increased availability was the so called Triple Modular Redundant architectures (TMR). Here three resources vote the logic output as shown in Figure 3-1.

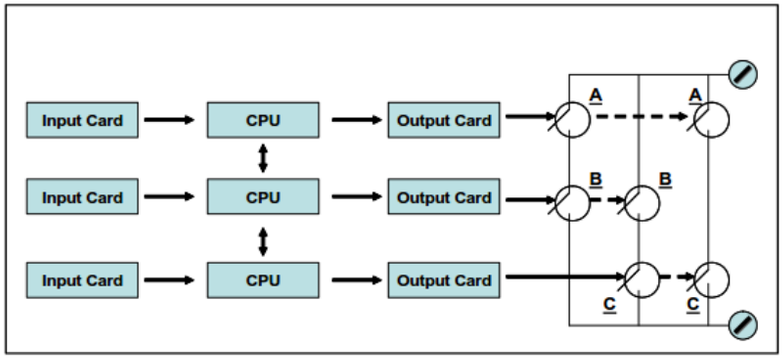


Figure 3-1: Architecture 2oo3 or TMR for Safety Related Logic Solver

The principle is simple: The system is composed of three resources; A, B and C.

It takes two resources to agree for the output to become true or false.

For example: If two resources agree on an output, (because there is at least one contact of each in each of the three branches of the logic) then the output will become true. On the other hand if only one resource produces an output, it will not become true as there is one branch of the logic controlled by the other two resources. Simplifying, this is "majority vote" architecture.

Figure 3-2 shows the fault tree analysis for failure on demand for this system. The advantage that these architectures offered over 1oo2 (and the main reason behind their use) was that their nuisance trip rate was much lower than those for 1oo2 (i.e. for a spurious trip to occur, two of the three resources must fail safe) and therefore this architecture appeared much more suitable for "process" safety than 1oo2. Although comparing EQ.1 and EQ.2 it can also be noticed that PFDTMR is 3 times higher than PFD1oo2.

Another advantage that this architecture offers is that it could tolerate one dangerous failure of one of its voting components in the same way as architectures 1oo2. The problem is that the resulting degraded architecture becomes 2oo2, which is twice as dangerous as a 1oo1 (Figure 3-3). Therefore TMR architectures must be repaired quickly.

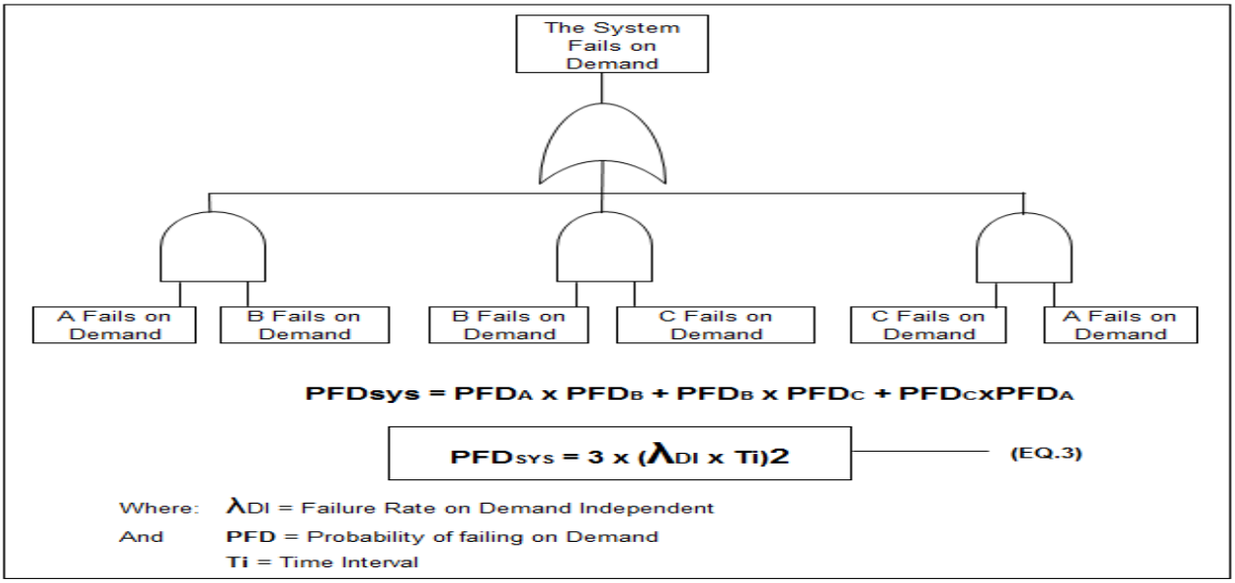


Figure 3-2: Fault Tree Analysis for 2oo3 Architecure

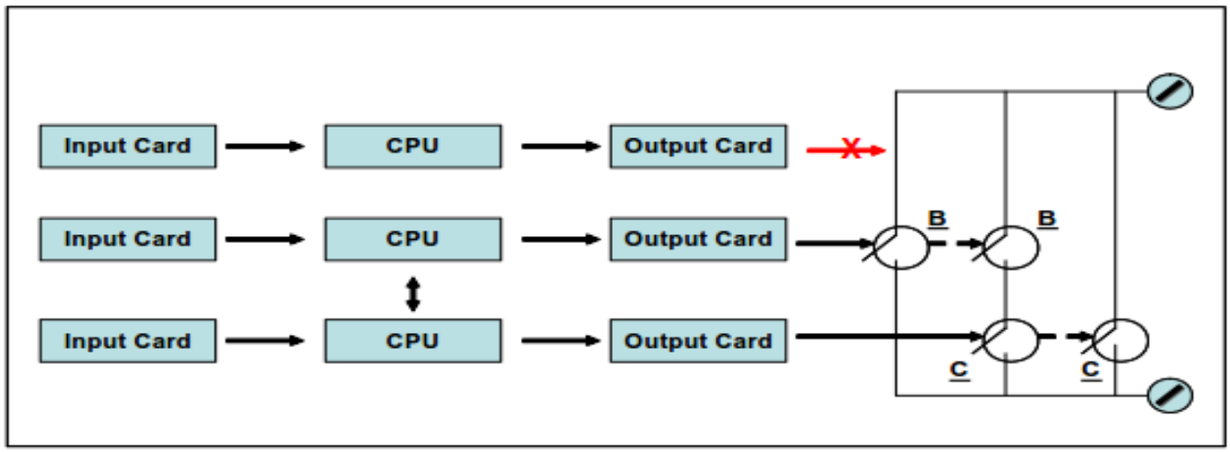


Figure 3-3: When degraded due to a dangerous failure of one resource, architectures 2oo3 for Safety Related Logic Solver becomes 2oo2

In other words, considering this is a de-energize to trip system, once one of the resources fails on demand, the failure on demand of ANY of the two remaining healthy resources will produce a failure on demand of the whole system. (Ref.: W. Goble's "Control Systems Safety Evaluation & Reliability – Page 365 EQ. 14-10, NC 2 7709, 1998)

It is possible then to conclude that none of these architectures discussed so far can run in degraded mode without affecting their safety availability.

The 90's New Generation of Architectures

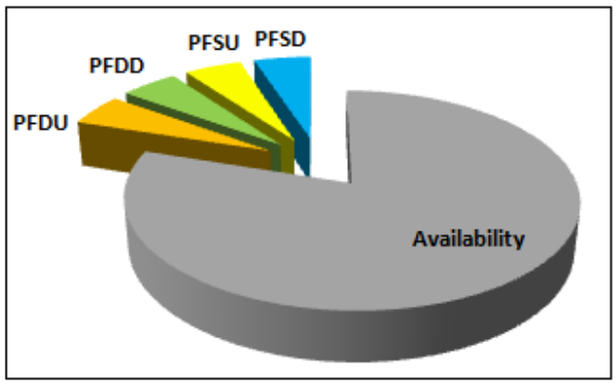


Figure 4-1: Probabilities outcomes with credit for Diagnostics

Within the last decade of the century and with a better understanding of functional safety, new and better architectures where developed. These architectures were based on the hypothesis that if dangerous failures could be detected and the faulty resource could be forced to fail safely, safety availability would increase because all those dangerous failures detected would become safe failures. Figure 4-1 illustrates this point.

Therefore for safety availability, one should only be concerned with the probabilities of having an undetected failure on demand, because those that could be detected would be converted into safe failures.

This is what is known as the big "D" of the 90's. Figure 4-2 shows and example of a "D" architecture. Note that in the expression "1oo1D"; the "D" indicates that the diagnostics protects the outputs.

In these new architectures, as used for Safety Instrumented Functions, there are three important questions:

1 – What does the diagnostic do?

2 – How often does it run?

3 – What is the coverage factor?

Let's consider one such 1oo1D architecture as shown in Figure 4-2:

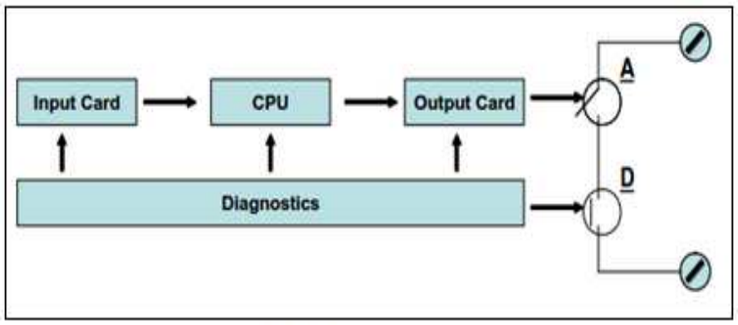


Figure 4-2: Architecture 1oo1D

The input circuit, the CPU and the output circuit are continuously diagnosed. If a fault is found, then the diagnostic circuit "D" will open and this will shut the plant down. Then the chances of this system having a dangerous failure will depend on the probability of a dangerous fault not being detected, and this will depend on the coverage factor.

According to the ANSI/ISA S84.00.01 – Part 1, "Diagnostic Coverage" is the ratio of the detected failure rate to the total failure rate of the component or subsystem as detected by diagnostic test, and it does not cover any faults detected by proof test. (This means that

if the c overage factor is 100%, there is no need for proof test). In the 1oo1D case, the higher the CD, the lower the PFDU (as we have seen before), then if the diagnostic protects the outputs, then PFDU ~ PFD

$$PFDU = \lambda_D \times (1 - C^D) \times TI \qquad \text{(EQ.4)}$$

Where: λ_D = Failure Rate on Demand
PFDU = Probability of failing on Demand Undetected
C^D = Coverage Factor for Dangerous Failures

Figure 4-3: PFD for 1oo1D

The first commercial 1oo1D architectures for Safety Logic Solvers or Safety PLCs developed in the 90's did not have a coverage factor high enough to reach SIL 3, although most were able to reach SIL 2 values.

Redundancy and voting were still required to reach SIL 3. This was the case with most commercial 1oo2D systems.

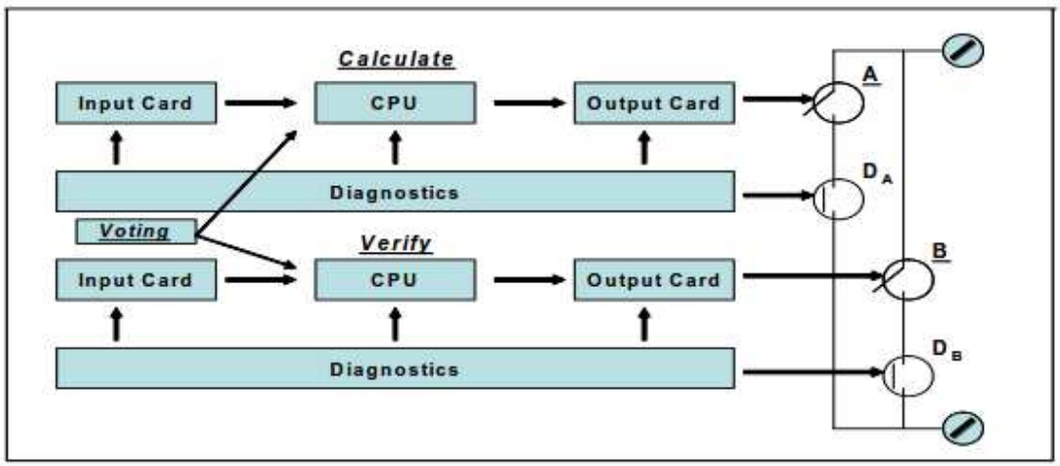


Figure 4-4: Architecture 1oo2D

The obvious advantage of these newer architectures is that when degrading, architectures 1oo2D became 1oo1D, and thus to SIL 2.

Figure 4-4 shows 1oo2D architecture

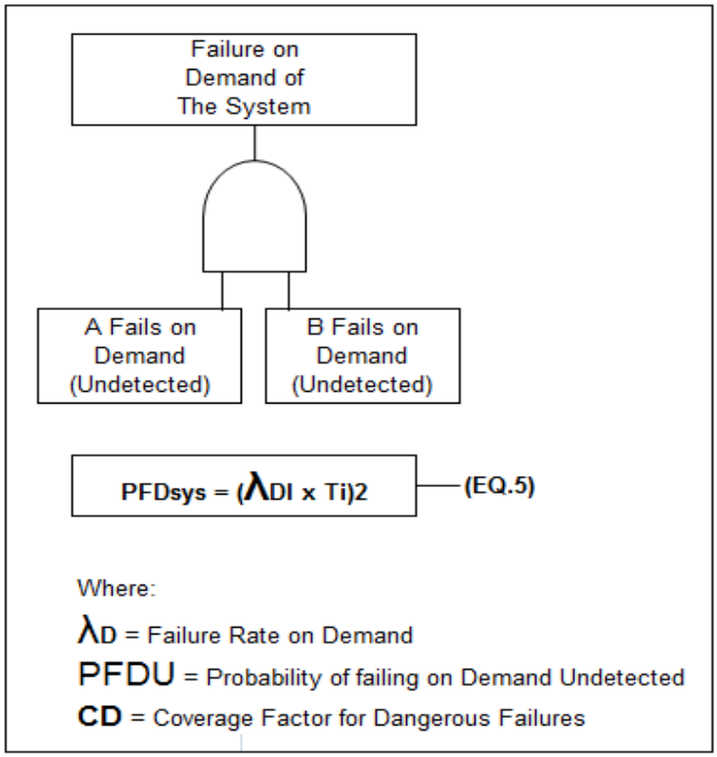


Figure 4-5: Fault Tree Analysis for 1oo2D architecture for a constant failure rate

Let's now analyze the PFD of these of architectures (Figure 4-5)

The value of PFD1oo2D is thus PFD1oo1D of the calculating resource, multiplied by the PFD1oo1D of the verifying or redundant resource. (EQ.5)

As we entered the 21st century, the question remaining was: Could a high enough diagnostics coverage factor be achieved in order to develop "independent from redundancy and voting safety"?

Flexible Modular Redundant Architectures

Starting this century, with new and more powerful processors, and a better understanding of the role of diagnostics in safety instrumented systems, manufacturers invested in the development of new architectures. As a result, the percentage of coverage of the diagnostics increased dramatically, allowing for non-redundant resources to reach SIL 3.

The principle behind this new development is simple if we analyze EQ.4:

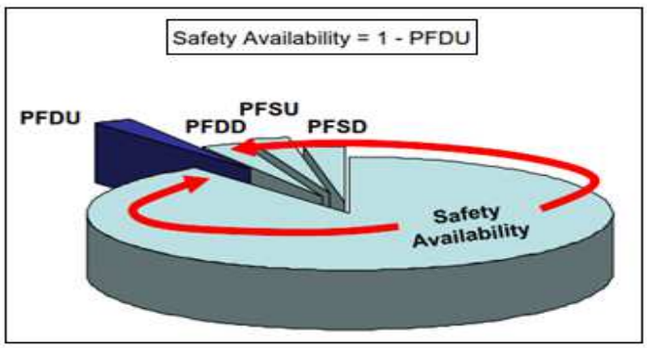


Figure 5-1: Availability with credit for Diadgnostics

As the value of the coverage factor "CD" approaches to 1, or as the coverage approaches to 100%, the expression (1-CD) will approach to cero, and as the value of this expression get smaller so will the PFDU. On the other hand, as explained in previous sections, if the diagnostics forces all detected dangerous failures to become safe trips, then the Safety Integrity Level of systems with diagnostics will be a direct function of the PFDU. (Figure 5-1)

Now, if the value of the PFDU is small enough it will be possible to have a value of PFDUav within the band that defines a given SIL (for low demand mode) for any combination architecture of resources with this new and very high coverage factor. In other words it is possible to have redundant resources in any architecture without affecting safety, because the PFDU of each resource is small enough (Lower end of the band).

Then redundancy could be simply used to increase availability without affecting safety.

One example of this new generation of architectures is offered by SIMATIC S7-400 FH from Siemens. Here the I/O Modules are physically separated from the controllers and linked by a standard certified safety I/O bus that allows for each component to communicate with every other one (Figure 5-2). In this particular case, the result is a system with the capacity to tolerate multiple failures without shutting down or compromising safety availability.

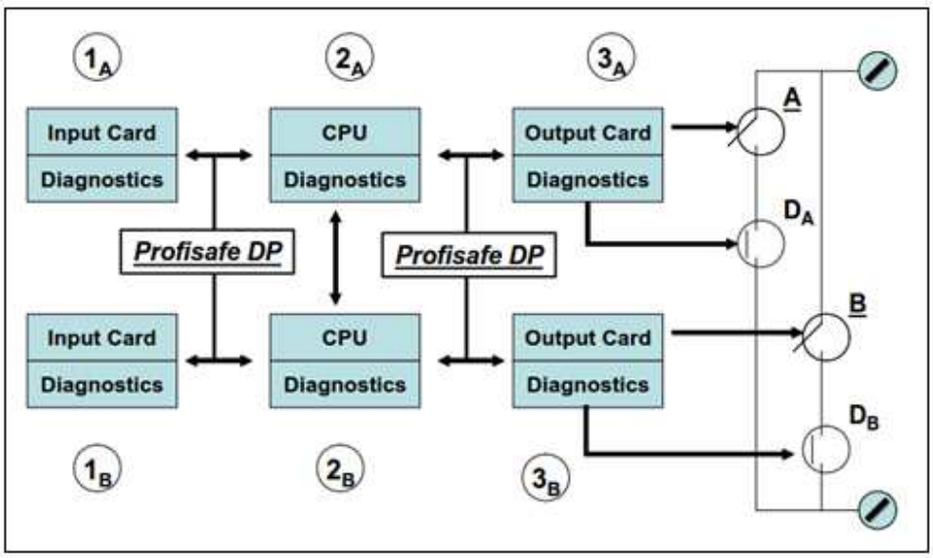


Figure 5-2: Example architecture SIMATIC S7-400FH

Summarizing, SIMATIC S7-400F/FH architecture, bases its design on several facts:

1 - Each component of each resource is physically separated from the others (common cause avoidance)

2 – It has an "independent of redundancy" safety availability value, with such a high coverage factor that it does not need to be proof tested.

3 – Each component has independent diagnostic capabilities and is certified to SIL3.

4 – Each component can communicate with all components of the redundant resource in more than one way.

The result is a very safe architecture that can tolerate several single points of failure.

Figure 5-2 shows one of several possible configurations of these new systems. Each component (1, 2 and 3) of each resource (A and B) can be separated from each other for minimum common cause. While resource A

calculates, resource B is doing its own calculations and waiting for resource A to detect and notify any anomaly in its health. Until then, the CPU of resource A has control over the outputs.

Voting between resources IS NOT needed to achieve SIL 3, since the coverage factor is so extensive that one single resource can reach SIL 3.

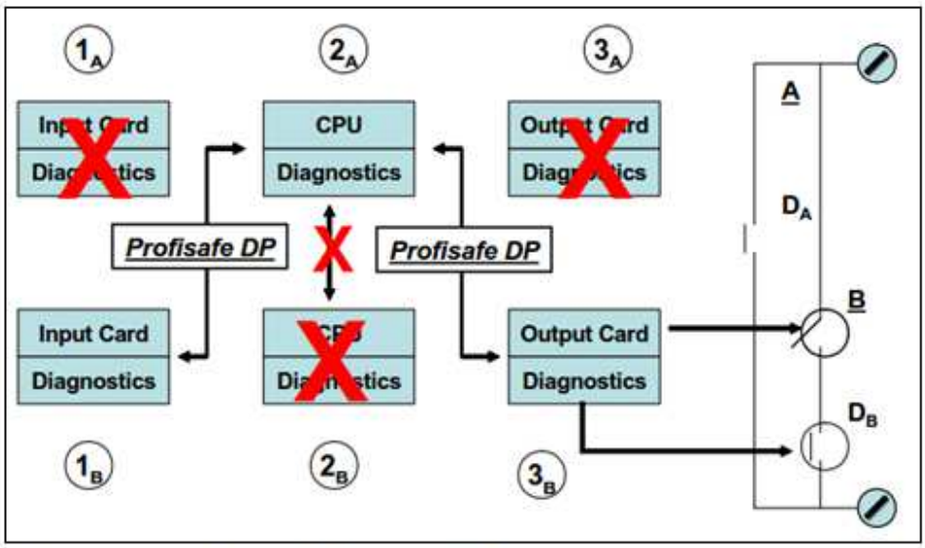


Figure 5-3: Example: after four injected failures, this architecture will continus to operate while maintaining its full SIL for maximum safety availability

In the figure 5-3 it can be seen how failures could occur in 1, 2 and 3 regardless if it happened in resource A or B, without shutting down. Thus we can have a failure in 1A, 2B and 3A and still run the plant with maximum safety availability. In this example, it will take at least a fifth single point of failure in order to shut the system down.

Conclusions

We have shown how architectures for SIS's have evolved from the pure voting solution for high safety availability purposes in the seventies to the Safety Availability - High Availability truly independent architectures.

Everything started with the development of output protection using the diagnostic concept. Since then, redundancy for safety is not required anymore, and now redundancy can be used to improve the functional performance of some of these systems, like the case of SIMATIC S7-400 FH.

While in the 70's 1oo2 & 2oo3 architectures offered a high level of safety or low PFD, because they use voting principles, when degraded would not keep their safety ratings. In the 90's, diagnostics allowed degrading to a lower SIL or higher PFDU as the case of 1oo2D. Today, architectures FMR allow multiple fault tolerance without affecting safety rating.

ACRONYMS

SIS- Safety Instrumented System

SIL- Safety Integrity Level

FMR- Flexible Modular Redundancy

IEC- International Electrotechnical Commission

PFD- Avg. Probability of Failure on Demand

REFERENCES

Various documents & White paper issued by Siemens AG

ACKNOWLEDGEMENTS

Relevant standards, codes and guides of IEC (International Electrotechnical Commission) have been used.

Lightning Protection for Control & Automation System on Existing Installations

Sourav Mukherjee- Dy. Manager (inst.), Mrs. R. Priyamvada- Group General Manager (inst. & ITS) , Engineers India Limited, New Delhi

ABSTRACT

Every year lightning strikes cause tremendous amount of losses to life and property throughout the world. For a control and automation engineer , designing a system which is not just capable of protecting the plant personnel from lightning current, but also, safeguarding the delicate electronic systems located in both safe and hazardous area poses unique challenges.

Apart from the regular challenges of electric shock due to lightning strikes, typical refinery complexes encounter a unique set of plant operational, maintenance and safety challenges due to lightning strikes affecting instrumentation and automation system. Instances of entire plant shut-downs has been recorded due to lightning strikes tripping the gas turbine generators of the captive power plants. Instances of lightning strikes have been reported on the tankages causing tank fire accompanied by extensive damages to the Tank Farm management systems. Instances have been recorded wherein the reactor thermocouple failure has caused shut-down of entire units resulting in down-time due to lightning strikes.Card Failures have been reported in the the IO cards in control rooms, critical analysers and fire & gas detection systems also. Most of these incidents have resulted in compromise in personnel safety as well as plant down-time.

Though most of the complexes are equipped with some basic lightning protection solutions in form of earth strips and earthing wires, they fall short on demand in providing safe lightning protection solutions. The challenges are unique also because, for control and automation systems, in terms of lightning protection, no generalised solutions exist and each and every kind of failures indicated above requires unique solutions.

This paper articulates ready to implement, holistic lightning protection solution in a typical refinery complex which is compliant to latest codes and standards along with the CAPEX involved based on actual site conditions.

Keywords :- LEMP (lightning electromagnetic pulse), SPD (surge protection devices)

1.0 INTRODUCTION

The control and Automation installations under consideration are primarily housed in the control rooms or enclosed shelters (e.g. for Analysers etc.). For protection of control and automation system against LEMP, the two major risks to which the system is subject to are the impulse current and the potential developed due to the lightning strike and the electro-magnetic field generated due to the lightning flash.

Based upon the vulnerability of strike to these parameters, the IEC 62305-1 has defined the following lightning zones i.e.

LPZ 0, LPZ 1 , LPZ 2…n., with severity of effect of strikes going down as we move from LPZ 0 to LPZ 1 , LPZ 2 and onwards. The requirement of LEMP study is to design the lightning system such that the equipment which is to be protected reaches a LPZ level of LPZ 2 or below.

This calls for the design of a lightning protection system which calls for a safe earthing scheme whichcaters to the lightning protection along with minimum interferences due to equalization current from the power earth shall also be realized for various installations.Use of additional Surge protection devices are also recommended wherein the earthing scheme is not sufficient to fulfil the entire lightning protection requirement.

2.0 INTERCONNECTION OF CLEAN EARTH (ELECTRONIC EARTH) WITH ELECTRICAL EARTH

The electrical power systems are provided with the power earthing system to meet the following earthing requirements:-

a. System neural grounding: This is required to clamp the voltage of system neutral relative to earth and provide a return path for the earth fault current .
b. Equipment earth: This is required for personnel safety, bonding all metallic enclosure and non-current carrying metallic parts to the earth.
c. Lightning protection earth: This involves the connection of all lightning protection conductors to the earth.

Sensitive electronic equipments such as instrumentation equipment, numerical relays, computers etc. generally have following earthing requirement:-

a. Signal grounding : This refers to common zero reference voltage for various signals. Since the magnitude of signal voltages are very small, this is required to be common for all signals so as to ensure the reference voltage for all signals is same.
b. Conductor shield grounding: The shield provided for various conductors/ conductor pairs/ traids carrying low voltage electronic signals are to be earthed to prevent the conductors from picking up spurious signals. The shields are earthed only at one end to avoid circulating current in the shield itself, which can adversely affect the signal.
c. Panel or enclosure grounding: This refers to earthing of metallic enclosures or frames or chassis of electronic equipment.
d. IS barrier earth

The earthing requirement of signal grounding, conductor shield grounding and IS barrier earth are sensitive and it is in practice to provide separate earthing system for these which is referred to as clean earth , electronic earth or instrument earth.Theearthing requirement of panel and enclosure grounding is same as the earthing requirement of electrical equipment Therefore, connection is made to the electrical equipment earthing system.

However, for the sensitive electronic system, the earthing is mandatorily done as a separate isolated electronic (instrument)

earthing system. This is done to fulfil the following requirements:-

a. In order to prevent stray currents from circulating and affecting the performance of instrumentation system, it is general practice to connect all earth points to single point isolated from electrical equipment earthing system.

b. The separate connection of instrumentation earth as described above is useful in eliminating pick-up of spurious signals due to stray current. However, several incidents of very large voltages being impressed upon instrument systems and consequent failures have been reported. The cause of this failure has been reported to be separation of the two earthing systems, i.e the separation of earthing between the electronic system and its enclosure.

During lightning strike, voltage of several kilo-volt may build up on the building /panel earth system, however, the electronic earth keeps operating at near zero potential. This causes spurious signal pick up or flashovers. Similar conditions arise due to build-up of charges in atmosphere causing the building / enclosure earth potential to raise up by several kilo-volts.The main aim of the integrated electrical and instrument earthing system is to ensure noise free instrument earth which is also capable of handling lightning strikes without damaging the electronic components. The requirement of integrating the electrical earth and instrument earth is as per IEEE-142-2007 recommendations. The following recommendations shall be followed to realize integrated instrumentation and electrical earthing system.

a. To prevent stray continuous currents or circulating currents from affecting the electronic equipment signals and operation, it is necessary to keep the electronic equipment ground system separate from the equipment ground components and connected together at only one point.

b. The electronic earth/shield earth of each and every panel shall be terminated at a bus bar which is insulated from panel/cabinet body.

c. The equipment body shall be connected to one another in a mesh/ star or star-mesh topology. (Refer figure-1)

d. All the electronic/shield bus bars shall be connected to a single bus-bar in star topology.

e. The panel earth shall be connected to the electrical system earth(SE). This is the earth to which neutral of the electrical system is connected. The instrumentation bus bar shall be connected to the 2 nos of instrument earth pits. (Distance between earth pits shall preferably be 7.6 meters for a 3 meter earthing electrode).Instrument earth pit resistance shall be less than 1 Ohm.

h. The instrument earth pits shall be connected to the electrical earth pit (to the electrical system earth SE) on nail head to nail head connection through insulated cable (Copper cable, CS 6 Sq.mm min.) and an Isolating spark gap based SPD(refer Note-1).

i. In order to realize a LPZ zone-2 area for the instrument control system, the incomer to the UPS system shall have a SPD(section 4.7) followed by an isolation transformer.

j. Use of **isolating spark gaps (ISG)** is recommended to create equipotential bonding throughout the earthing system during lightning incidence as per **IS/IEC 62305-3 Clause 6.2 and Clause E.5.4.3.6**. The purpose of this SPD is to make sure that the electrical and instrument earthing systems remain segregated during normal operation and integrated during the condition of lightning strikes. In this way, both the electrical and instrumentation systems remain protected. SPD shall be mounted in a weather-proof enclosure suitable for outdoor installation (if installed outside).

Preferable installation location shall be between the instrument earth pit and earth pit to which the panel earth is connected to the electrical earthing system.

3.0 LIGHTNING PROTECTION SOLUTIONS FOR SYSTEMS & UNITS

In this section, lightning protection for few critical plant systems which are extremely vulnerable to lightning strikes are discussed. Such systems are as follows:-

a. Turbine Control & CPP
b. Tankages
c. SPM Analysers
d. Skin thermocouples attached to critical installations like reactors etc.
e. Lightning solutions for the various units

3.1 Gas Turbine control System alongwith CPP

Gas turbine generators are important in the sense that failure of such systems leads to failure of the CPP, which eventually causes entire refinery to shut-down. In this study, Gas turbine control system and the balance instruments of the GTG has been

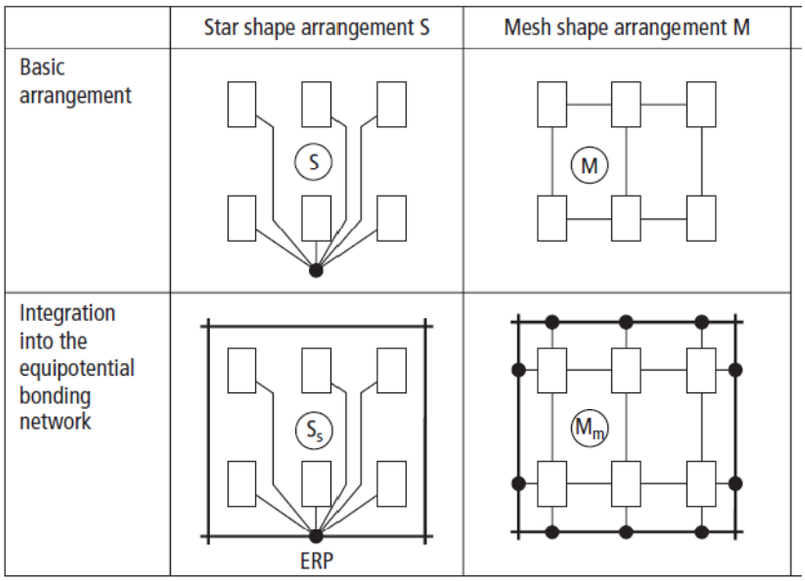


Figure-1

studied separately and SPDs have been recommended for both. In case of gas turbine control system, SPDs have been recommended at both ends for all the tags i.e. panel and field end for conventional IOs (4-20 mA + HART analog IOs as well as Digital IOs).For the temperature elements directly connected to temperature cards, SPDs have been recommended at one end (panel end) only because of vulnerability of thermocouple junctions to temperature fluctuations.

The following observations were made in the gas turbine control system panels in typical refinery complexes:-

a. Shields are not connected at the panel end
b. Cabinet body shorted with the frame.
c. Shields cut out at the cabinet end and not terminated to the instrument earth.
d. No lightning/surge protection devices located

In order to provide sufficient & proper lightning protection solution, the following steps shall be taken:-

a. The cable shields to be earthed to the system earth using cable sleeves.
b. In case the shield is also terminated at the JB end, the shield terminations at the Junction box end shall be removed.
c. For cables whose shields are not connected to the panel system earth, the same shall be done as per the above mentioned in general recommendations
d. The SPDs shall be installed as per the following table.

In order to recommend the Surge protection devices for the Turbine control System, past reference of SPDs were sought from the turbine control system manufacturer. In absence of any such information , the electrical properties of the IO cards were compared with the general PLCs of reputed makes, where SPDs have been installed before. On comparing it was found the electrical properties of the Turbine control panel PLC are identical to those of the other PLCs. Therefore, the suitable SPDs can be installed. SPDs are recommended for 100% of IOs of the turbine control panel. However, for the balance instruments of the CPP, SPDs are recommended only at selective installations prone to lightning strikes.

3.2 Tanks & Auto- Tank Gauging Systems

In case of tanks, the installation of Surge protection device on instruments is not just for protection of instruments, but also the safety of the tanks. Not only are they capable of causing card failure and damage, but also a severe tank fire may be initiated due to spark between the instrument shield and instrument body due to huge potential difference during lightning strikes.

The following observations were made in the tankages in typical refinery complexes.

a. The surge protection devices were not found in the tank instrumentation for both the tanks in the auto tank farm management system as well as general tanks.
b. Therefore, adequate protection against lightning surges did not exist.

Based on the survey, the following solutions are recommended

TFMSa. The SPDs shall be installed in the secondary level instrument, multi-point temperature instrument,

pressure transmitter as well as the tank side indicator at both ends.

b. On the primary level instrument, SPDs are usually installed by TFMS vendor, however, the SPD type shall be ascertained first. In case it is found to be of Type-1+2, then additional SPDs are not required. Otherwise, additional SPDs shall be installed.

Shift Tanks1.In the shift tanks, SPDs shall be considered for primary and secondary level instruments, the pressure and temperature instrument respectively.

3.3 SPM Analysers

The SPM analysers are installed such that there is sensor unit with electronic cards on top of a column alongwith the shelter unit located at grade.In this paper, SPM analysers have been chosen specifically because it has electronics at all three loations, i.e. field, shelter and control room and these analysers are extremely susceptible to lightning strikes.
The SPM analysers have been found to have multiple card failures in the past. The analysers have 1 no. of sensor and electronic unit located at elevation and the shelter is located at grade. The sensor electronics is communicating with the electronics at the shelter via RS-232 cable. The shelter communicates with the control room via RS-485.

The following are the observations.
1. Multiple card failure observed on RS 232 and RS 485 cards.
2. Failure of electronics at control rooms could be located as well.

The following are the recommendations for such systems:-

1. Isolation transformer shall be provided to the power cable at the analyser shelter end along-with SPZ 0 -2 SPD of the voltage rating suitable for the UPS output to generate a SPZ-2 area. Same SPD shall be provided at the UPS end also. The earth of the transformer shall be connected to an electrical system earth Bus bar which is connected to the grid.
2. SPD shall be added to the serial cable at both ends.
3. The separate and isolated instrumentation earth at the shelter end shall be merged to the grid by nail head to nail head connection.
4. The analyser earth bus bar shall be checked to ensure that all earthing terminals are terminated at single bus only(star topology). The equipment body and instrument earth shall be at a single point itself to avoid circulation current.
5. SPDs at both end for the serial cables.

3.4 Skin Type thermocouples

The reactor skin thermocouples located in some units like VGO-HDS etc. which are connected to the T/C cards located in the control room. Failure has been observed in the thermocouples due to lightning strikes, which caused unit shut-down due to interlock actuation.

The following are the recommendations

1. Surge protection devices shall be installed at the control room end.
2. Installation of surge protection device is recommended at control room end only (not at field end), because , in case of thermocouple extension cables, any metal contact induces potential due to seabeck effect. This potential induction is zero only of no temperature gradient exists across the inlet and outlet terminals of the SPDs. This situation can be safely realized in the control room end.

3.5 Lightning Protection for various units

Apart from the systems described above, card failures had been identified in the various units also in the PLC and DCS systems. On further investigation, we found out the cause of such failures as the lightning currents migrating from the instruments located at the top tiers.

Vulnerability of such instruments to either direct or indirect lightning surges necessities the need for SPDs on them. Therefore, unit wise instruments located on top tier were identified and SPDs were recommended for them.

Besides, intermixing of electronic earth with the electrical earth was located at many control cabinets and necessary segregation was recommended.

4.0 SURGE PROTECTION DEVICE SELECTION CRITERIA

The surge protection device selection for electronic system is strictly dependent upon the signal levels and frequency of the data transfer protocol. Similarly for power systems, it is dependent upon the voltage levels, frequency and phases.

This section indicates few of the critical parameters which shall be considered for SPD selection.

4.1 Foundation Fieldbus & 4-20mA+HART instruments :-

The following table shows the indicative parameter of the SPDs used for intrinsically safe circuits (Suitable for both fieldbus and non-fieldbus application).

S No.	Technical Requirement	SPD Parameter
1.	Installation site	Zone 1 gas gr. IIC T6 Ex Ia
2.	Voltage Uc	32 V DC
3.	Current In	500Ma
4.	Frequency (Freq. modulated)	6MHtz
5.	Immunity	10kA (8/20micro sec)
6.	Test std.	IEC 61643-21
7.	Capacitance and Inductance	Negligibly small
8.	Approvals	ATEX,IEC-Ex, CCOE

4.2 SPDs mounted on serial and MODBUS lines

The selection of SPDs on MODBUS shall be governed by the capacitance and series impedance of the SPD.

The following table indicates the max. baud rate based on the M-Bus segment capacitance.

SNo.	Total capacity of segment	Max. Baud Rate
1.	Upto 12222 nF	300
2.	Upto 1528 nF	2400
3.	Upto 382 nF	9600

Selection of SPD shall be done keeping in mind the series

impedance of the SPD as well as the capacitance of the SPD.

4.3 SPDs for Power cables at the inlet of LPZ 0A to 2

The following section indicates SPD selection for the electrical power supply lines

a. The use of combined SPDs which caters to lightning current and surge arrester shall be preferred.
b. The use of separate SPDs is also acceptable, provided the devices are properly energy co-ordinated.
c. The lightning current arresting SPD shall be SPD type –I (EN 61643-11) for lightning impulse current waveform 10/350 micro sec.
d. The surge protecting device shall be SPD Type-2 (EN 61643-11) also for coordinating SPDs for type-1 and Type-2 tests. It is suitable for impulse current waveform 8/20 microsec.
e. SPDs must be chosen as per the over-voltage categories defined in IEC-60664-1 for the given power supply.
f. SPD's shall must have mechanical indication for all the modes (L-N and N-E) for monitoring healthiness of the device.

5.0 CONCLUSION:-

Lightning protection study is a continuously emerging field with continuous changes and updates happening even in the international standards. This study is an endeavour to provide solutions up to date with the latest standards and international trends.

Controlling Fugitive Emission
A Challenge for Control Valve Manufacturer

S.Sivaprakash, Manager-R&D, KSB MIL Controls Limited

KEY WORDS

Fugitive emission, Control valve, Gland packing, Low emission, Packing box, Bellow seal, Ecolock packing, Rising stem

ABSTRACT

Fugitive Emission control in process industries is one of the major challenges faced in this century as far as the process industry is concerned. Hazardous process fluids from process equipments like valves, pipe connections, pump seals etc. are the foremost reason for plant emission. Gland packing and seals are used to isolate the process fluid from the environment in process equipments, where hydrocarbon or other hazardous fluids are present in the gaseous form. Even though emission from individual component may be negligible, the cumulative effect can be very damaging. Moreover if we consider the energy loss due to the emission and leakage of any process fluid and its cost in maintaining back to its intended volumes, the impact would be just beyond imagination. Any effort put in controlling the fugitive emission even in micro levels will fetch a considerable savings and will have a positive impact on the planet Earth. The article covers the concepts, challenges and practical guidelines for designing an effective gland seal for control valves.

INTRODUCTION

From simple control devices of the 1800's to the 'smart' valves of today, control valve technology has come a long way.It was in the early 18th century that James Watt came up with what may be called the first automatic control valve: the Moving Stem valve which was introduced as part of his Fly Ball Governor to regulate the speed of the steam engine. Since then automatic control valve technology has moved forward keeping pace with the Industrial Age.

The advent of Pneumatic Transmitters and Controllers turned out to be a significant milestone; it led to the introduction of Pneumatic Control Valves which used instrument air instead of process fluids. The 1930s and 40s witnessed the introduction of Positioners which brought about substantial increase in control valve efficiency. Another key event during this phase was the adoption of the concept of CV as a universal standard for valve sizing. Towards the 1970s the 80s, processes got much more complex throwing up new challenges such as Velocity, Noise and Cavitation. Design efforts to address these issues resulted in Anti Cavitation and Low Noise valves.

The introduction of the Federal Clean Air Act in the US in 1990 proved to be yet another milestone as it marked a new era of increased environment consciousness. In control valves it prompted a worldwide move towards 'clean' technologies such as advanced gland sealing systems that cut down emission levels dramatically.

This article covers the advancement in Fugitive Emission Control Technologies possible in Control Valves and also an overview of KSB MIL developed advanced Gland packing system for control valves upto pressure class of ASME 2500. We also shall take a brief look into some useful maintenance tips and also the international standards in place for limiting control valve gland leakage.

FUGITIVE EMISSION AND MITIGATION IN CONTROL VALVES

The control of emission and minor leakage in process industries is one of the major challenges faced in this century as mentioned. Different type of gland packing and Seals are used to isolate the process fluid from the environment in process equipments, where hydrocarbons (Volatile Organic Compounds¬ VOC) are present in the gaseous form.

In the United States, the Clean Air Act enforced to control air pollution on a national level, requires the Environmental Protection Agency (EPA) to develop and enforce regulations to protect the general public from exposure to hazardous airborne contaminants. The act has evolved over the years and generally the gland leakage through control valve stem seal requires to be limited below 500ppmv and in some stringent cases below 100ppmv.

As far as India is concerned, strict enforcements regarding industrial fugitive emissions is yet to be in place and control valves are a major source of fugitive emission in process industries. While lot of emphasis is laid by the plant designers on control valves characteristics like noise, cavitation, and velocity during the design phase, an often forgotten aspect is the gland leak potential, which gains utmost relevance in the Chemical, Petrochemical and Refinery sectors. Apart from the harm the emission does to the ecology, the leakage also can lead to loss of energy or an expensive product or a potential explosion hazard or a health hazard to humans.

HIGH LEAKAGE POTENTIAL IN RISING STEM VALVES

Reciprocating stem Control valves have higher potential for gland leakage compared to rotary valves as the valve stem makes intermittent contact with the service fluid and the atmosphere unlike other type of valves. When the stem moves upwards, it drags the fluid inside along with it through the packing; and when the stem moves downwards it draws dirt, dust and other particles from atmosphere onto the packing box.

On maintenance aspect, control valve glands maintenance is always a major headache for the process owner. Many a times the leakage can be arrested by loading the gland follower (till the packing reaches its permanent compression). But a very tight packing will create high friction on the valve stem, which will lead to poor control of the process variable and also will create dead band in the operation. A good balance between control performance and good gland sealing capability is most essential.

Other Reasons for Leakage through Packing Box include poor finish of the stem and the packing box, improper packing ring compression, improper alignment of the stem, chemical attack on the stem, rapid/wide thermal cycling and simple mechanical wear can be some of the reasons for packing leakage.

GLAND PACKING AND VARIOUS OPTIONS

The resilient material used for packing is forced into the void between the stem and the packing box. The stressed packing pushes itself against the stem and forms a tight seal.

Any leakage should pass through the space between the packing and the stem. Modern packing like PTFE or Graphite is virtually impermeable or is made impermeable with better process of manufacturing and the primary leakage occurs between the stem and the packing.

There aretwo types of packing designs used namely compression packing and Lip type packing. The Compression packing consists of a soft material (PTFE or Graphite) which is stuffed into the stuffing box and compressed by a gland. When the gland is tightened by a bolting mechanism, it applies a compressive force on the packing, resulting in the radial pressure of the packing on the stem. The radial pressure must exceed the fluid pressure to ensure proper leak tightness.

The lip type packing or V packing expands laterally (because of the flexibility of the lips, when pressurized) and are forced against the restraining walls of the packing box and the stem. This requires lesser external applied force for gland sealing. It should be noted that, the sealing action can be one sided or two sided depending on the configuration/ combination and much care is to be taken during assembly to ensure that the lips are directed towards the pressure side.

Both single packed and double packed gland designs are widely available. A single packing arrangement is a more economical option with a stack of packing and the top of the packing box is supported by either a spring or lantern ring.

With uniform density identical packing rings, Double Packing is a better gland sealing method, with packing rings distributed above and below the lantern ring (or packing spacer), with the lantern ring helping to exert a higher load on the lower packing rings while tightening the gland studs. Optionally disc or coil springs can be provided on the gland studs to apply a pre-determined constant load on the gland. This reduces the frequency of gland packing adjustment, which helps to maintain low emission performance, over a period of time.

Studies have proven that when uniform density packing rings are used, the top two or three packing rings are compressed and it exerts maximum radial force on the valve stem. The lower rings are not compressed, rendering them ineffective. Thus maximum radial force is at the top end of the gland, which reduces exponentially with the packing box length. Even in double packing, with uniform density packing rings or Lip Type Packing (V-Rings), it is difficult to exert even radial sealing pressure throughout the length of the valve stem. As a result, these generally fail to meet the stringent EPA regulations and other international test requirements like VDI, CAA, TA- Luft, ISO. Combination of packing with varied density is used to overcome this issue and has achieved a very promising results.

BELLOW SEALED DESIGN

Valve handle toxic fluids or the process fluid is to be completely sealed off from the atmosphere, bellows sealed construction is the best option. It is also the optimal solution where the valve handles extremely toxic or highly hazardous fluids, or valves are used in in-accessible locations, where periodic inspection of the valve packing is practically impossible. In Bellow sealed valves, the conventional gland packing is replaced by a metallic bellows welded to the valve stem. The upper end of the bellows is retained with a gasketted joint. As the valve stem strokes, the bellows expands or compresses with the travel. The bellows sealed design thus eliminates any sliding or rotating seals through which process fluid can pass. The choice between low emission and bellows sealed construction is generally made considering the criticality of the application or the potential leak hazard consequence. The bellows sealed construction is comparatively expensive and also may not be always technically practical (in high pressure or larger size, longer travel valves etc.).

LOW EMISSION GLAND PACKING DESIGN FOR FUGITIVE EMISSION CONTROL – DESIGN CONSIDERATIONS

- Type of Valve – Linear Reciprocating Motion or Rotary Motion

- Stem size: As the stem size increases the area of contact between the stem and packing as well as the area between packing and packing bore increases and therefore the allowable leak rate (as insisted in ISO 15848-1) also increases accordingly.

- Surface roughness: Gland packing life cycle and leak rate largely depend on the surface roughness of the valve stem and stuffing box. The surface roughness shall be optimised for valve stem and for stuffing box according to the type of valve and application.

- Type of packing: During the stem movement, extrusion of the packing happens which may result in leakage through the packing. Since braided rings are more extrusion resistant than the die formed flexible rings, packing sets are designed with braided type end rings and die formed type inner rings, which has a better sealability.

- Geometric tolerance: Any minor misalignment in stem movement with respect to the packing may cause leakage in locations where lateral pressure is smaller. Sogeometric tolerances (concentricity, perpendicularity etc.) are to be strictly maintained to the specified values to prevent any misalignment in the stuffing box assembly.

Packing Design: Continual research by Valve and Packing manufacturers have led to the evolution of cartridge type gland packing, where special packing sets (cartridges) are designed with packing rings of varying density so that it ensures even and uniform compression. The upper rings would be of higher density material and the lower rings with decreasing density. This ensures even and uniform compression and thus uniform radial thrust on the stem. They provide a good balance between control performance and good gland sealing capability, ensuring that the stringent emission norms are met. The material of construction is either PTFE or Graphite or a combination of the two, determined based on the service fluid and process parameters.

INTERNATIONAL STANDARD FOR FUGITIVE EMISSION TESTING

Various nations released regulations for setting limit on the amount of allowable FE emissions from any sources/ installations like "Clean air act" in North America and "TA Luft" in Europe. The development and harmonization of practicable emission standards and legislation for use in the EU has been worked out by Industrial Valve Standards committees and a new family of international standard ISO 15848 was evolved. This will help to enhance the demands on the valve industry and process industry regarding emission control and to regulate it stringently in future.

The international Standard ISO 15848 has two parts;

a. ISO 15848-1:2015. Part 1 describes a classification system and qualification procedures for type testing of valves.

b. ISO 15848-2:2015. Part 2 is for production acceptance testing of valves.

ISO 15848-1specifies the testing procedures for evaluation of external leakage of valve stem seals and body joints of globe control valves and Isolating valves intended for application in volatile air pollutants and

hazardous fluids. Test medium can be Helium or Methane and shall be selected according to the tightness class requirement. Leakage measurement shall be done in PPMV (Parts per Million Volume) or in mg/s/m. The Valve performance class as per ISO 15848-1is defined by the combination of the following criteria.

- Tightness class: Six tightness classes; three for helium (AH, BH and CH) and three for methane (AM, BM and CM).

- Endurance class: Based on the number of mechanical cycles carried out three endurance classes are specified for both globe control valves & Isolating valves. For isolatingvalves it is specified as CO1(500 cycles with two thermal cycling), C02 (1500 cycles with three thermal cycling), C03 (2500 cycles with four thermal cycling) and for globe control valves it is specified as CC1 (20,000 cycles with two thermal cycling), CC2 (60,000 cycles with three thermal cycling), CC3 (1,00,000 cycles with four thermal cycling)

- Temperature class:Thermal cycling shall be performed within a standard temperature range (upto 400degC for graphite and upto 200degC for PTFE gland packing).

Table – 1 : Leakage Class (as per ISO 15848-2015 part 1)

Class	Measured leak rate (Mass flow)	Measured leak rate (Volumetric flow)	Remarks	Measured leakage (using Sniffing method)
	mg·s−1·mm−1 stem diameter	mbar·l·s−1 mm−1 stem diameter		Ppmv (Methane)
AH	≤3,14·10−8	≤1,78·10−7	Typically achieved with **bellow seals** or equivalent stem (shaft) sealing system for quarter turn valves	≤50
BH	≤3,14·10−7	≤1,78·10−6	Typically achieved with **PTFE based packing or elastomeric seals**	≤100
CH	≤3,14·10−5	≤1,78·10−4	Typically achieved with flexible **graphite based packing**	≤500

TEST METHOD

Test Valve shall be pressurized to its rated pressure. The target number and combination of mechanical and thermal cycles shall be selected as per the required endurance class & temperature class mentioned above. Leakage through the stem seal & body seal shall be measured. While doing thermal cycling test pressure shall be the rated pressure at that selected temperature only.

The standard has different classes (tightness class, endurance class and temperature class) to qualify the valves. The number of mechanical cycles and thermal cycles vary and packing adjustment is also allowed for some classes.

ISO 15848-2 is the standard for factory acceptance testing of control valves, which has qualified the type testing. Production testing is done at 6 bar pressure and room temperature. The leakage rates allowed are different with stringent acceptance norms for Bellows sealed valve and higher leak rates for PTFE or Graphite based packing.

Helium or Methane gas is used for testing the valves. This measurement is done using a helium mass spectrometer, which is commonly used to detect and locate small leaks.

FUGITIVE EMISSION TEST SETUP

KSB MIL has successfully established the high temperature Fugitive emission test facility for developing suitable gland packing systems capable of controlling FE emission as per ISO 15848. FE testing is carried out with various type of packing designs and combinations both in PTFE and Graphite material.

Fig.1-KSB MIL FE test setup

FE Test Set-up details

The high temperature test set up consists of two heating pads which can heat valves up to 500degC, thermocouples to measure the temperature, thermocouple welding unit for fixing the thermocouple on to the valve/bonnet surface, temperature indicators and ceramic wool for heat insulation, and Helium gas source etc. Valves are to be tested for 20,000, 40,000 & 1,00,000 mechanical cycles as described in the standard.

KSB MIL ECOLOCK PACKING SYSTEM

As per the recommendation in ISO 15848 Part-1 the packing systems with graphite MOC is supposedto be in Class C and PTFE in Class B. This also would be a hard target to achieve, when we consider the endurance class and temperature class. As mentioned in Table 1 the graphite packing is supposed to perform 1000 times and PTFE 10 times better to reach the desired leak rates as per Class A. KSB MIL could achieve this cumbersome target by reengineering and fine tuning the hardware as well as the soft parts.

The system consists of precisely engineered packing with supporting hardware which enhances the FE performance as well as the reliability of the system. The packing is specially engineered to meet the stringent emission norms set by the ISO standard. The combination of expanded graphite/ PTFE packing with variable density and close braided construction will seal the gland to the best possible way. The extrusion property of the soft material is controlled by the precisely manufactured support hardware like anti extrusion rings, lower stem guide and geometrically characterised packing bore. With this advance design, KSB MIL could achieve the highest emission requirement of Class A as per ISO 15848, even with graphite packing. The test was successfully conducted in-house as well as at a third party laboratory with TPI witness. The graphite packing was tested at rated pressure and 400degC on anASME 1500 class valve and an ASME 2500 class valve. With the exhaustive tests, KSBMIL valves with stem sizes of 3/8inch to 1.5inch are qualified for both Class A and Class B upto the pressure class of ASME 2500.

Fig.2-KSB MIL Ecolock Packing system

The certification is granted for valves with both graphite and PTFE packing as

ISO-FE AH-CC1-SSA0-t200degC-Class1500-ISO 15848-1:2015for PTFE packing

ISO-FE AH-CC1-SSA1-t400degC-Class2500-ISO 15848-1:2015 for Graphite packing

Fig.3-Valve after CC2 test

Fig.4-Trim set after CC2 test

Fig.5-Graphite Packing after CC2 test

FEW USEFUL TIPS FOR PACKING BOX MAINTENANCE

- Packing tightness shall be checked and ensure for proper bolt tightness as per the recommendation and smooth stem movement before start up.
- Packing can compress further in service and the packing compression may have to be readjusted. Tighten the packing nuts when found necessary.
- In dusty or dirty conditions, better to provide a suitable boot around the stem to protect the packing.
- The valve stem finish is most significant in avoiding the packing leakage. If the stem dimension is not correct and if the finish is poor, then score marks will appear and in no time packing fails.
- Alignment of the stem is important in avoiding leakage between the stem and packing. Hence ensure that only genuine spares (soft and hard) are used for re-assembly of the valve.

- Gland packing and gaskets to be changed every time the valve is opened and re-assembled. Ensure that the packing used are genuine and correct. Procure the packing only from original equipment manufacturer and keep in stock. This ensures the packing is exactly matching the stem and packing box ID. The quality of the material of the packing is also ensured.

- Do not buy replacement parts from non-OEMs. Over-emphasis on short-term cost savings can sometimes lead to hazardous working environments for personnel, process downtime and increased operating costs.

CONCLUSION

With the advent of new materials and technologies it is possible to develop gland packing system which can perform equally good as that of the bellow sealed system while considering the emissions permitted. KSB MIL has successfully developed the ECOLOCK packing system with both PTFE and graphite for catering to pressure class upto ASME 2500.The temperature range of qualification is upto 200degC for PTFE and upto 400degC for graphite. This would enable KSB MIL to extend its capability in offering valves with Class AH qualification throughout its product models ranging upto valve size of 32inches comprising the stem size upto 1 ½".

REFERENCES

- ISO 15848-1: Industrial valves-Measurement, test and qualification procedures for fugitive emissions - Part 1: Classification system and qualification procedures for type testing of valves

- ISO 15848-1: Industrial valves-Measurement, test and qualification procedures for fugitive emissions - Part 2: Production acceptance test of valves

- API 622 : Type Testing of Process Valve Packing for Fugitive Emissions

- API 624 : Type Testing of Rising Stem Valves Equipped with Graphite Packing for Fugitive Emissions

- MESC SPE 77/312 - Technical Specification Fugitive Emission Production Testing

ACKNOWLEDGEMENTS

- Support offered from FCRI in Testing and certifying along with Third Party Inspection Agencies Bureau VeritasIndia and TUV Nord India for a year long experiments.

- JamesWalker for supporting by supplying various options of gland packing for trials and development.

BIOGRAPHY

Mr. S Sivaprakash was bornin Kerala, India in the year1974. He graduated in Mechanical Engg.from MG University, Kerala. He joined Fluid Control Research Institute (FCRI), Palakkad, Kerala in 1996 after graduation as Research engineer. During hiscareer at FCRI, he has been associated with Evaluation of Flow elements, development of flow measuring techniques and advanced test systems. At present he is with KSB MIL Controls Limited as Manager-R&D and involved in product development and value engineering on Control valves and critical valves.

Topsoe Furnace Manager

Asset protection and optimal performance by Automation

Abstract:

Continuous real-time monitoring inside your furnace and heaters for performance and efficiency.

Topsoe Furnace Manager is a multi-camera monitoring system for continuous monitoring of critical process equipment like tubular reformers and fired process heaters. The system utilizes cameras to gather information from multiple locations, and can be used for continuous observation of numerous internal furnace temperatures, and burner statuses.

Market key factors for efficiency in process plants

A key factor in increasing profitability and capitalizing on growth opportunities is the ability to achieve the full potential of plant performance, especially from the tubular reformers and fired process heaters. Correcting inefficiencies in the tubular reformers and fired process heaters should be prioritized because even very small changes can have a large impact on overall performance.

Market pains and desires

Fired heaters in refinery processes pose numerous challenges. Among them are fire, process tube failures, poor burner operation, mechanical equipment failures and process upsets. Historically, these challenges required plant personnel to directly interface with the firebox to evaluate equipment and process status. A critical activity, this interaction involves inherent risk. While specialized personal protective equipment and hand-held data collectors have been developed, risks remain. Continuous firebox monitoring technology relieves the dependence upon human firebox interaction. By using a system of image collectors operating continuously, millions of images and data points can be amassed annually. Associated alarms activate when temperatures are out of range. Images and data are also stored in a historian for easy retrieval. Continuous firebox monitoring technology minimizes furnace firebox personnel safety risks, thus allowing personnel to perform important work, such as troubleshooting, diagnoses, data analysis planning and collaboration with colleagues.

Operational efficiency

In order to better help producers upgrade their steam reformer performance and reliability, Topsoe has combined innovative thinking with decades of experience to improve upon the already extensive repertoire of services and tools used for assessment and optimization. A primary focus of the improvements is on tube wall temperatures (TWT) due to the lack of precision when using conventional methods for measuring TWT. Results from extensive infrared pyrometer studies reveal why and when to use different pyrometer types, and this knowledge will help producers optimize their steam reformers by maintaining operation closer to design temperatures. Topsoe is also introducing a system for advanced reformer surveillance, which provides additional temperature data via continuous monitoring. With these advances in steam reformer services, Topsoe can better help customers adhere to design limits, identify bottlenecks, save energy, increase tube lifetime, and optimize operations.

Distributed with permission of author(s) by ISA 2018
Presented at
ISA-D: "Petroleum & Power Automation Meet-2018" (PPAM-2018);http://www.isadelhi.org

The performance of the primary reformer and fired heaters is of crucial importance to plant efficiency and production because of n their role as the single largest consumer of energy. It is therefore extremely valuable to conduct regular reformer and heaters assessments that result in solutions aimed at optimizing parameters for peak reformer performance. One of the key parameters affecting reformer performance is the tube wall temperature (TWT) profile. Suboptimal TWT profiles and temperature spread can result in reduced efficiency and production. More severe consequences includ premature tube failure and unplanned downtime. To obtain maximum utilization, operating temperatures must be kept very close tomechanical design limits. This requires accuracy in measurement techniques and reformer simulation.

Current Methods

However, accurate temperature measurement, where good thermal contact is established with no impact on temperature, is difficult in the harsh environment of the reformer. The most common technique currently used in the industry is optical infrared (IR) pyrometry, but the effectiveness of IR pyrometers is compromised by user inaccuracies and by inherent sources of error. These sources of error include reflection of radiation from tube surroundings, tube wall emissivity, and flue gas absorption and emission effects. Most often, the errors lead to a temperature reading that is 20 to 100 °C too high, which in turn results in a higher than necessary temperature margin. This paper discusses the various measurement techniques available and describes Topsoe studies that have led to valuable insights in reformer temperature management.

TFM system

TFM is a system-of-systems includingelectronics, optics, data handling, data analysis, placement design, visual display, self-protection, compliance, and human-machine-interface. Image acquisition is at the heart of the system. The image collectors send the images to the data collectors, which organize, transmit, store and analyses the data. Alarm safeguards are immediately available to the plant operators, and remotely to the organization outside of the plant supporting operations.

TFM capabilities include:

- Image collection: Over 500,000 images per image collector per year.
- Data collection: Over 50,000,000 data points per collector per year.
- Alarms: Metal temperatures and burner flame quality, such as impingement, jet-ting and poor mixing.
- Benchmarked images of good examples and bad examples of burners and tubes.
- Historian: Time and date stamped images with data.
- Remote access to images and data.
- Wireless computer interface with firebox
- 24/7 persistence of the entire system.
- Self-protection for reliability.

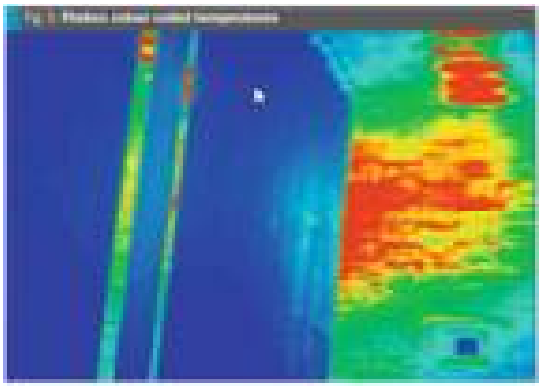
TFM process safety benefits

Process safety management mandates certain important areas of focus for industrial plant operations. Process safety represents best practice, and is a compliance requirement. TFM provides critical information for several process safety areas of focus.

Mechanical integrity and asset protection

Asset protection is a very high priority in plant operations. Inside the firebox, catalyst tubes experience "creep." Creep is a metallurgical deformation with dependence upon stress, time-in-service and temperature-in-service of metalsexposed to high operating temperatures.

TFM provides images and temperature data to correlate combustion and process variations within the firebox. The resulting analysis and correlation provides specific mechanical integrity information that can be acted upon by mechanical integrity and process subject matter experts (SMEs) to reduce variation and improve overall tube mechanical integrity. TFM imagery and data also drive action on other aspects of firebox components, such as burner failure, refractory failure and structural compromise.(Fig. 3)



Administrative safeguard and alarm history

TFM's alarm and historian capabilities also support the overall intent of process safety management by providing immediate feedback for operational mitigation, and historical capture of important equipment status. This duality of immediate information and historical data capture enables safe day-to-day operations, and continuous improvement through engineering over time.

Furnace burner balancing

TFM will provide the data and the tools to effectively balance firing to minimize the temperature variation across each row of tubes, as well as, throughout the furnace. Based on previousstudies, fuel gas consumption improvements of 1-2% are possible. Burner balancing may provide a production increaseexcluding other bottlenecks. Balancing tube skin temperatures will result in longer tube and catalyst lives while significantly reducing the risk of tube failures and costly downtime. Expected efficiency improvements pay for TFM during a reformer catalyst life cycle.

Reliability economics

TFM's burner balancing also improves reliability that results in savings over time due to longer catalyst tube life. TFM is paid for in a tube harvesting protocol based on creep measurements when about 10% of the reformer tubes avoid replacement at the first outage.

Incident investigation

Sudden incidents (such as power failures) on firebox component integrity have been difficult to correlate. Overheating events during start-up and shutdown have been difficult to capture without increased exposure of personnel to firebox conditions. Subjectivity permeates most firebox incident investigations resulting in potentially inaccurate conclusions. TFM images and stored data show exactly when an event began, and the consequences of that initial event. TFM information is readily available to the entire incident investigation team, even remotely, in a matter of minutes so that the root-cause-analysis can begin quickly, and the next incident can be avoided.

Training

Training of new and existing personnel on firebox operations has traditionally involved a steady-state model with a minimal amount of information available regarding firebox behavior during transitions. With reformers and heaters, there are several dynamic scenarios that impact burner operation and catalyst tube temperatures, especially during transitions such as start-up and shutdown. TFM captures images with data to provide actual transient information that can be implemented in training, including dynamic training simulators. Additionally, training benchmarks are captured, and can be inserted in-to training documentation to establish best practices.

Process hazard analysis

Mitigation of firebox overheating scenarios and consequences typically rely on safeguards such as fuel pressure, firebox draft, and spot process temperatures. These process measurements represent historical safeguards based on the capability of prior furnace process measurement technology. TFM provides additional firebox process measurements. Actual flame intensity and flame shape; and actual catalyst tube temperatures over a large surface area are now available to utilize as administrative safeguards without reliance on personnel directly interacting with the firebox.

Standard operating procedures (SOPs)

SOPs traditionally have relied upon historical operational information collected and documented based on past best practices. For firebox operations, SOPs typically require a person to physically inspect the firebox condition on a recommended frequency. This inspection frequency can be unrealistic, especially during start-up and shutdown when other operational priorities take precedence. TFM provides continuous firebox inspection, and image targets with data targets can be captured and documented to provide new best practice examples. These examples can be embedded within the SOPs, whether or not electronic, and provide direct comparison with real-time images and data captured by TFM during operation.

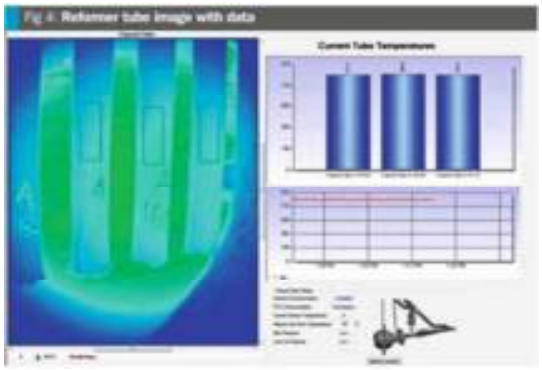
Compliance audits

Self-auditing of firebox compliance has traditionally relied upon written tube temperature and fireboxinspection reports generated by operations personnel. The fundamental basis of the measurements is difficult to correlate. For example, tube temperaturemeasurements are typically reliant upon a map generated by engineering or operations management specifying locations on the tubes and locations of the person performing the measurement, with specification of the measurement device (camera), and direction to capture results manually on a log sheet. This series of information handoffs is vulnerable to inaccuracy, even with the best efforts of trained personnel.

TFM information is captured and stored with locations, device, images and data specifications held constant. TFM captures firebox burner imagery and data, which has historically been absent. Better audits result from better information and data.

Firebox data collection

TFM reduces frustration resulting fromrepeated firebox, visual data collection requests by non-plant colleagues. Collaboration is a great operational lever, and is highly valued in today's business environment. When data is remotely available, engineers can engineer, planners can plan, and managers can manage. When data is not remotely available, and with today's communication channels, such as cell phones, firebox information requests can overload those residing in closest proximity to the firebox. Often the task of firebox data collection falls on the furnace operators, or junior plant furnace image engineers. This can be a good training activity, but it also can lead to very high levels of frustration from those collecting the data. This frustration can lead to unpredictable behaviors in a plant environment, which is inherently dangerous, complex and frustrating by nature. There is high value by not adding any degree of frustration to a plant operating environment. TFM provides images and data remotely regarding firebox status. Requests for firebox information can then be directed toward TFM functionality rather than human firebox data collection.



Furnace stair climbing

Although arguably good for health, physical exertion and stair climbing, especially on modern supersized furnaces, is difficult. The design of many modern-day furnaces exasperates the exertion requirement. The furnaces are larger, taller, and more complex

than in the past. The exertion required to climb up and down a large furnace is better spent ensuring that TFM remains on station collecting important firebox images and data rather than looking through many peep doors and manually recording data.

Furnace problems

TFM reduces confusion and anxiety during periods of time with furnace issues. Problems can be shared within the organization to make plans and provide guidance quickly. Furnace issues are nearly inevitable due to the nature of the operation.

The ability to handle any problem is made easier with information. Without information, confusion, anxiety, and frustrationbuild up to an unacceptable level. The remote viewing capability of TFM, supported by the capture of images and data stored in the historian, enable communications, planning and organizational coordination during periods of furnace problems.

Furnace guidelines and documentation

TFM reduces confusion regarding linkage between hazard reviews, firebox Sops, firebox critical safety systems, and actual operation. It is difficult and time consuming to 'connect-the-dots' between all sources of required process safety information. It is especially difficult to link process information if fundamental process parameters are not available. Reformer furnace and heaters tube surface area is one of the largest heattransfer surfaces in the process plant. It is also one of the least monitored for data due to the harsh operating environment.

TFM's non-contact temperature data and image acquisition provides the information needed to link process information so that it makes sense and isn't confusing.

(Fig. 4) This is especially important in fundamentally understanding critical safety system intent.

Personnel risk exposure

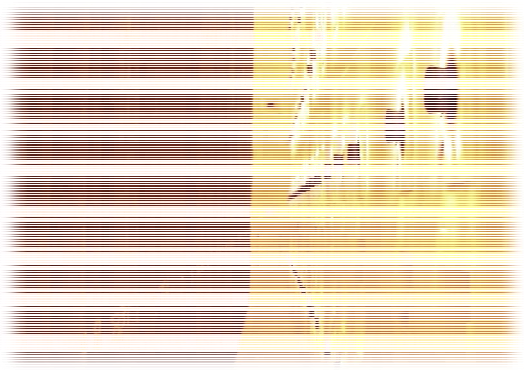
TFM supports remote location of personnel with reduced risk exposure frequency. For example, a major, instantaneous reformer piping incident occurred on a reformer with TFM installed that resulted in no injuries because personnel were remotely located away from the furnace. Some older, existing plants were built with a lower emphasis on risk and exposure to personnel. Modern risk evaluations, including QRAs, actually quantify personnel exposure and risk. The quantified risk matrix considerswork patterns, which are a function ofequipment inspection frequencies, or "rounds." Furnace rounds have typically been historically set by previous habits and patterns established many years ago. With TFM, the furnace rounds are not required on the same frequency as historicallyunderstood to be required. Just as the industry trend has been to move personnel away from operations unless necessary, personnel within the plant itself are at less risk when exposed less frequently to the furnace firebox.

Burner evaluations

TFM eliminates frustration associatedwith human burner evaluations. Modern day, low NOx, industrial furnace burners are difficult to see with the human eye. When fired on a mixed fuel consisting of a significant amount of hydrogen, the low NOx burners develop a flame that cannot truly be evaluated with the human eye.

TFM's capability to monitor flames which the human eye cannot see, and to provide alarms when the flame is underperforming, eliminates the need for personnel to visually decipher flame quality. TFM provides a flame intensity measurement which is charted and graphed continuously, so that the impact of rate changes and fuel/air changes is captured. When the flame is not behaving correctly, TFM will alarm to notify the organization that there is a burner issue. Sunburnt eyes from looking inside a firebox at flames too long are not necessary with TFM. Eliminating a source of physical pain is a very tangible improvement for personnel. TFM encourages burner tuning. Proper burner operation contributes directly to proper furnace operation. With TFM's ability to adjust view angles and regions-of-view, burner adjustments and burner performance improvewith increased levels of understanding.

Additionally, TFM captures the images to benchmark exactly how burners should appear during various process scenarios.



Weather

Operations personnel monitoring and managing large reformers face interesting and challenging scenarios involving weather events. Rain, snow, heat, cold, and wind all impact the ability to physically monitor a reformer. Weather compounds any difficulties associated with specialized PPE that is typically required for furnace interaction.

Face shields and fire retardant clothing can be cumbersome during normal activities such as stair climbing. Weather events make the situation even more difficult, which can lead to personal safety events, such as tripping or falling. Importantly, serious furnace monitoring needs to occur during a weather event. Critical management decisions to continue operation during weather events depend on operations personnel climbing stairs and looking into the reformer firebox. TFM can eliminate the need, or greatly reduce the frequency, of physical human reformer inspections during weather events. This capability provides time for higher value plant activities while reducing personal safety risks.

Process control schemes

TFM provides data to establish actual equipment-operating-envelopes for tubes and burners. TFM data can be integrated into DCS. Tube temperatures and burner quality can be mapped and characterized for use in advanced firebox analysis.

Operational excellence

Support groups collaborate using the same TFM images and data as reference for discussions. HIistorical information is available "on demand" without relying on the operations group for retrieval. Compliance data is available at all times. Subject matter experts have remote access to furnace operations with time-and-date stamped images (Fig. 5).

Furnace lifecycle

Furnace equipment performance and repair history are captured with time and date stamped images. Temperature data is correlated with equipment performance, metallurgical analysis and repairs. Visual images are available for operations and reliability team training. Historical tube and burner performance is captured with images and data (Fig. 6)

Easy installation

Sensor tiles can be installed during a shutdown, and the sensor head can be mounted, while the unit is in operations to minimize downtime from installation.

Technical support

Haldor Topsoe can, as an option, monitor and assist the customer using a secure internet connection, for more optimal solutions for furnaces.

References:

S. W. Sexton: "24/7 firebox monitoring": Nitrogen Syngas 345, January - February 2017

S. W. Sexton: "Continuous monitoring improves Fired Heater operation": Downstream Business, June 2016

Acronyms

TFM: Topsoe Furnace manager

TWT: Tube wall temperatures

PPE: Personal protection equipment

SME: Subject matter experts

SOP: Standard operating procedure

Author:

Aditya Saini was born atPanipat, India in the year 1989. IIe has graduated in Instrumentation engineering from Institute of Instrumentation Engineering, Kurukshetra University,Kurukshetra. Previous to Topsoe, he had worked with Yokogawa India Limitedas FESengineer forHMEL, Bhatinda and BORL,BINA refinery. His experience at Topsoe includes Engineering, site erection, commissioning start-up & maintenance. This includes a number of Basic engineering projects of Instrumentation for Topsoe Formaldehyde, Hydrogen, Ammonia, Methanol, Diesel Hydrotreater and GTL plants catering to clients across the globe. Nowa day, works closely for Topsoe Furnace Manager.

"Safety Integrity Requirement for Fire & Gas system"

Hemantkumar J. Patel
Control Systems Engineer, Fluor Daniel India Pvt. Ltd., Gurgaon, India
Email-Id: Hemant.J.Patel@Fluor.com,

ABSTRACT

Many industrial processes, especially those in the chemical, Oil & gas and Petroleum industries, involve inherent risk due to the presence of hazardous chemicals, gases or flammable mixtures. Safety instrumented functions (SIF) protect personnel, equipment, and the environment by reducing the likelihood of an identified emergency hazardous event. Due to explosions and fires, millions of dollars of losses occur in the Chemical, Oil & gas and Petroleum industries each year. Since a great potential for loss exists, it is common for industry to employ safety instrumented systems (SIS) to provide safe isolation of flammable or potentially toxic material in the event of a fire or accidental release of fluids. A SIS is a collection of a number of SIF. As we know, safety is achieved through different layers of protection. Fire & Gas Systems (F&GS) fall under the definition of a mitigation layer in the structure of layer of protection and are designed to mitigate unexpected events.

Hence a question may be asked, "Can anF&GS be considered as a SIS, and do we really need to consider safety integrity level (SIL) for a fire &gas systems, including the detection and alarm devices?"

KEYWORDS

Fire & Gas System (F&GS), safety instrumented system(SIS), safety instrumented function (SIF), IEC 61508/61511, ANSI/ISA 84, EN54, NFPA 72, FMEDA.

INTRODUCTION

ThisPaper represents the current trends in the market place and industries in general with respect toF&GS and their relationship to SIS. There has been much industry contention over the categorization of F&GS as SIS, especially as the concept of functional safety matures in the marketplace and compliance to IEC 61508 / 61511 standards is more prevalent.

Fire and gas detection products and measuring technologies are fundamentally different from other forms of process instrumentation in a plant. Incorrect detector placement and insufficient quantity of F & G devices and environmental constraints can prevent the F & G device from detecting a hazardous gas leak or flame, even when the device is functioning properly. And hence, when a safety hazard is undetected, then the appropriate safety action (e.g. shutdown of equipment, activation of deluge, shutdown of Isolation dampers, venting, etc.) cannot be initiated. Because of this, many end-users and system integrators are wondering if the functional safety standards are applicable to F&GS or not.

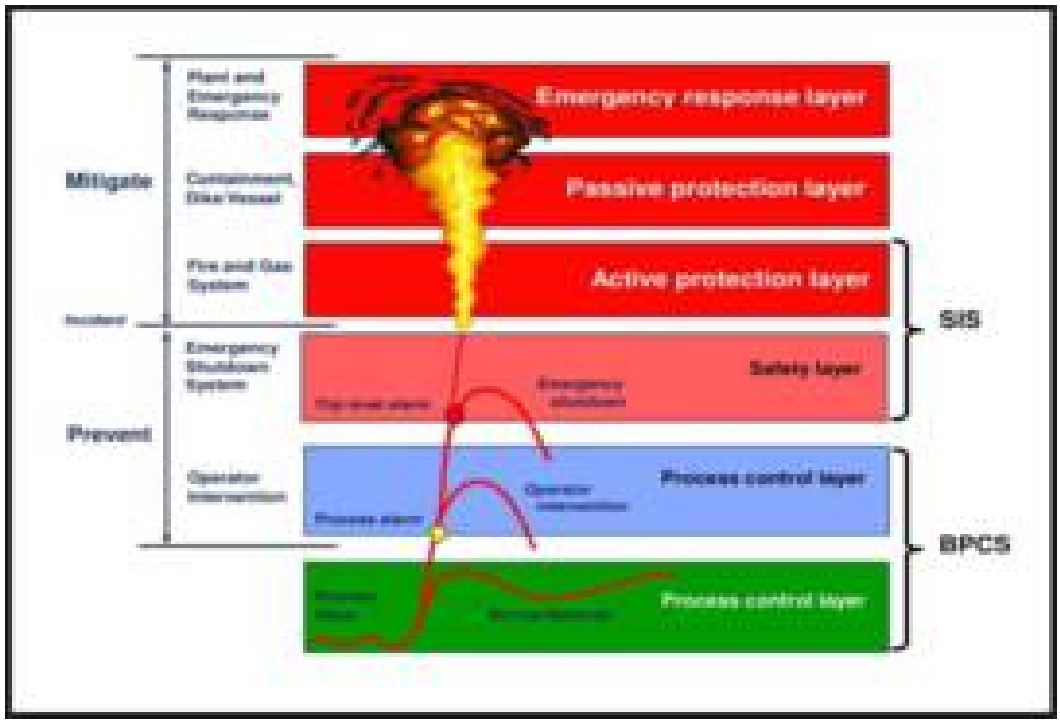
DIFFERENCE BETWEEN FIRE & GAS SYSTEMS AND SAFETY INSTRUMENTED SYSTEMS

To understand the concept of F&GS to be considered as SIS, let us first explore the layers of protection. Safety is provided by layers of protection. These layers of protection start with safe and effective process control, extend to manual and automatic prevention layers, and continue with layers to mitigate the consequencesor severity of an event.

The first layer is the basic process control system and inherent safe process design. The proper design of a process control system itself provides significant safety. The next layer of protection is also provided by the control system and the control system operators. Automated shutdown routines in the process control system, combined with operator intervention to shut down the process, arethe next layer of safety.

Next is the SIS. It is a safety system independent of the process control system. It has separate sensors, valves, and logic system. Its only role is

safety. Normally process control is not performed in this system.



These layers are designed to prevent a safety related event. If a safety related event occurs, there are additional layers designed to mitigate the impact of the event.

A safety instrumented system, by definition, is designed to bring the process to a safe statewhen demand is placed upon it. AnF&GS may include some preventative functions; however, it is typically comprised of mitigating functions. A mitigating function is described as an action that does not prevent the hazardous event from occurring, but instead initiates actions that reduce the potential consequences of the event after it has occurred. The F&GS acted after the primary event had occurred in an attempt to lessen the consequence of hazard consequence. The fire & gas system will also take actionssuch as the shutdown of equipment, activation of deluge, activation of suppression system, shutdown of isolation dampers, venting, etc. Even if the fire &gas system does not initiate these actions, sounding alarms / beacons prompt people to take mitigating action.

SO CAN WE APPLY FUNCTION SAFETY TO FIRE & GAS DETECTION SYSTEM?

A justifiable argument can be made both for and against the classification of a F&GS as a SIS. Those that oppose the concept typically believe that because of the inherent limitations of fire and gas detection, a F&GS should only augment a plant safety system and not be considered a critical safety function. If a properly functioning F&GS comprises a SIL 3 logic solver, a SIL 2 sensor, and a SIL 2 final element, but fails to see the hazardous gas or flame and effectively eliminate or mitigate the hazard, then the SIL 2 risk reduction factor of 100 has not been achieved. For this reason, many people think that