



SMART CITY CONCEPT & ROLE OF INSTRUMENTATION



Prepared by:-

**Swati Dhawan, Neha Singh
Technip India Limited, Noida**



ABSTRACT

Smart City and Instrumentation can be said as two faces of a single coin. The monitoring, Control, information utilization and final decision making for SMART CITY'S Energy, Power, Water, Environmental and Safety needs can only be fulfilled by proper utilization of Instrumentation and Control techniques. This conceptual paper discusses role of automation in developing smart city as a whole.

The paper poses the first question - what is meant by a 'smart city'. As such there is no universally accepted definition of a Smart City. It means differently to different people. The conceptualisation of Smart City, therefore, varies from city to city and country to country, depending on the level of development, willingness to change and reform, resources and aspirations of the city residents. A Smart City would have a different connotation in India than, say, in Europe or America. Even in India, there is no one way of defining a Smart City.

WHAT IS SMART?

S: SYSTEMATIC (SERVICES, SCHEMES, SCHEDULE)

M: MATURE (MANUSCRIPT, MANAGEMENT, MAGNITUDE)

A: ADEQUATE (ACCEPTABLE, ADMIRABLE, AFFECTIVE)

R: RESPONSIBLE (REGULAR, RESOLUTE, RECALL)

T: TARGET (TACTFUL, TIME BOUND, TRANSFORM)

In the approach to the Smart Cities Mission, the objective is to promote cities that provide core infrastructure and give a decent quality of life to its citizens, a clean and sustainable environment and application of 'Smart' Solutions.

The core infrastructure elements in a Smart City would include:-

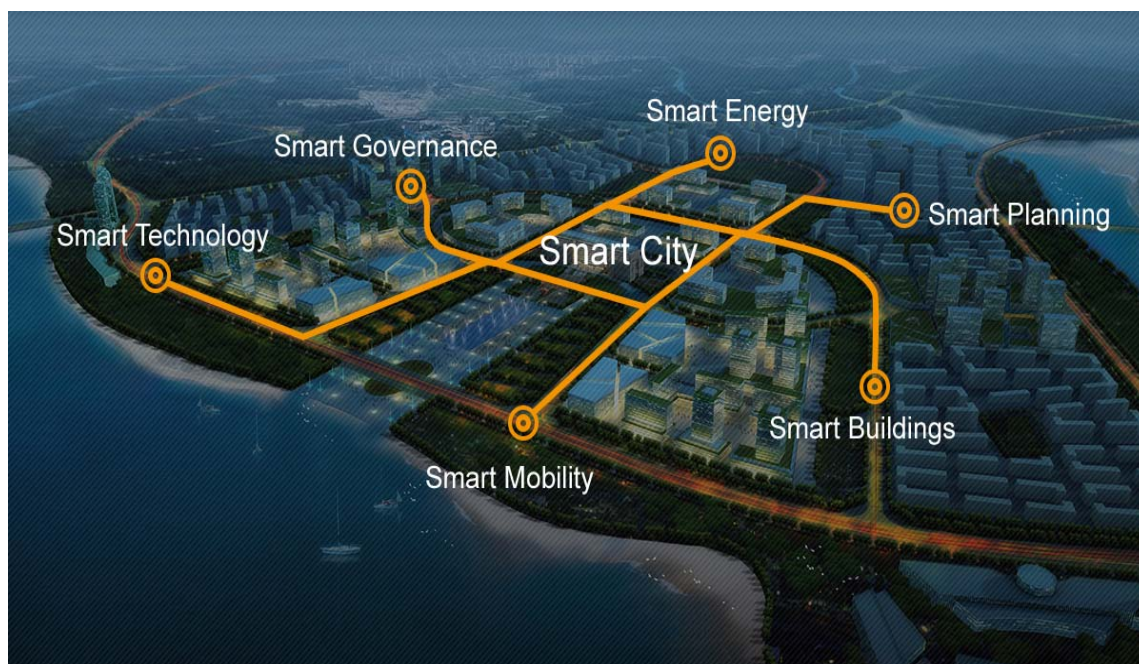
- a) Adequate water supply
- b) Assured electricity supply
- c) Proper sanitation, including solid waste management
- d) Efficient urban mobility and public transport
- e) Affordable housing, especially for the poor
- f) Robust IT connectivity and digitalization
- g) Good governance, especially e-Governance and citizen participation
- h) Sustainable environment
- i) Safety and security of citizens, particularly women, children and the elderly

This paper will present a complete scenario for Smart City needs, its challenges, its implementation Strategy and solutions.



KEYWORDS

Instrumentation, Automation, Smart Solution, Control and Monitoring, Safety, Data transmission, e- Governance, Digitalization, Sustainable environment, Mobility, Technology, Planning, Energy etc.



INTRODUCTION

Urbanization is expected to continue rising in both the more developed and the less developed regions so that, by 2050, urban dwellers will likely account for 86 per cent of the population in the more developed regions and for 64 per cent of that in the less developed regions. Overall, the world population is expected to be 67 per cent urban in 2050

Cities are engines of growth for the economy of every nation, including India. Nearly 31% of India's current population lives in urban areas and contributes 63% of

India's GDP (Census 2011). With increasing urbanization, urban areas are expected to house 40% of India's population and contribute 75% of India's GDP by 2030. This requires comprehensive development of physical, institutional, social and economic infrastructure. All are important in improving the quality of life and attracting people and investments to the City, setting in motion a virtuous cycle of growth and development. Development of Smart Cities is a step in that direction.

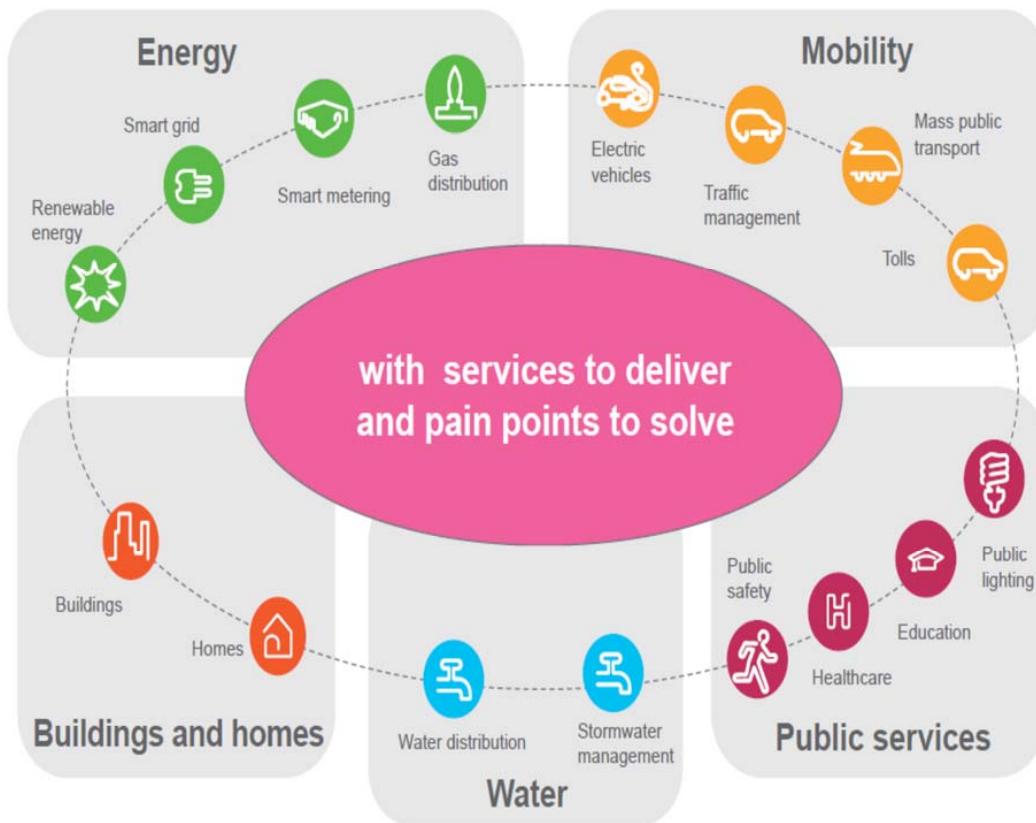


HOW DO YOU MAKE YOUR CITY A SMART CITY? IT STARTS WITH EXPERIENCING EFFICIENCY

Then what is a Smart City? A city is known by its efficiency – how it manages energy



and makes it available round the clock, how it ensures water for everyone, how it runs its public services, how it controls construction, how it maintains and manages its buildings, how it operates its transportation system and so forth.



TOWARDS THE THEORY OF SMART CITIES

WHAT MAKES AN INSTRUMENT SMART?

The definition of a smart instrument has evolved over the past decades (Table 1). Instruments, as specified in the table have travelled a long way to become smart from dumb. Earlier, instruments were used to control the loop locally and display with

gauges, and generally recorded manually with pen and paper as a technician made his or her rounds, the reading in field. A small degree of intelligence was next added to instruments in the form of a 1-5, 4-20, or 10-50 mA dc output proportional to the PV (process variable). Once data could be transmitted remotely, it created the possibility of remote measurement, display, and control. Parallel development of control systems with central processing and I/O introduced more effective means to capture the information produced by these 4-20 mA instruments, scale this



information into engineering units, and centrally act on and record the information. Loop-powered instruments then became feasible, making it possible to power multiple transmitters via one current source, often via an analog I/O module.

In time, HART (Highway Addressable Remote Transducer) technology unified the Multiple and incompatible vendor-specific



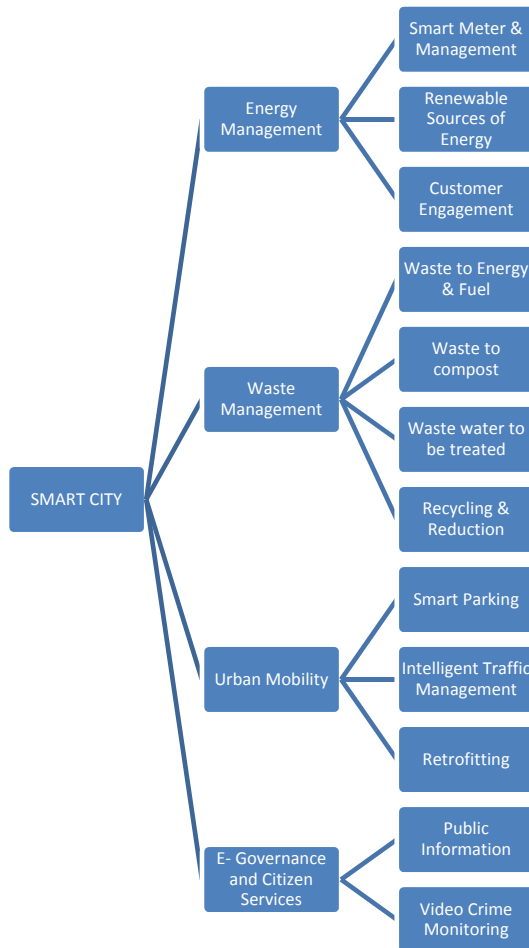
networks that were using the existing 4-20 mA signal as a transmission medium.

Today, a smart instrument is generally defined as a device that includes one or more digital network communication options. Because provision of digital communications requires a microprocessor, a wide range of other capabilities are also typically provided with a modern smart instrument.

	Pneumatic	Analog	Micro-Processor	HART	Fieldbus	Ethernet	Wireless
Output	3-15 psi	1-5, 4-20, 10-50 mA	4-20 mA	4-20 mA HART	Digital	Digital	Digital
Introduced & Adapted	1950-1970	1960-1980	1980's	1980's	1990's	2000-present	2000-present
Remote Communication	N	Y	Y	Y	Y	Y	Y
Digital Communication	N	N	N	Y	Y	Y	Y
Engineering unit PVs	N	N	LOCAL	Y	Y	Y	Y
Data Beyond the PV	N	N	Y	Y	Y	Y	Y
Diagnostics	N	N	Local only	Y	Y	Y	Y
Calibration and Configuration	Local	Local	Local	Remote	Remote	Remote	Remote
High- Speed	Output only	Output only	Output only	4- 20 mA output only	Digital Output	Digital Output	N
Real- time Control	Local	N	Limited	Limited	Y	Y	N
Time Stamp	N	N	N	N	N	Y	Y
Integral Data Security	N	N	N	N	N	Y	Y
Intelligence	None	None	Local only	Medium	High	High	High
Direct integration with IT	N	N	N	Y	Y	Y	Y



STRATEGY & SOLUTIONS



ENERGY MANAGEMENT

INTEGRATED SMART GRID SOLUTIONS-

Distribution intelligence" refers to the part of the Smart Grid that applies to the utility distribution System, that is, the wires, switches, and transformers that connect the utility substation to you, the customers. The power lines that run through people's back yards are one part of the power distribution



System. A key component of distribution intelligence is outage detection and response. By having sensors that can indicate when parts of the distribution System have lost power, and by combining automated switching with an intelligent System that determines how best to respond to an outage, power can be rerouted to most customers in a matter of seconds, or perhaps even milliseconds.

SMART METERS

Smart meters provide the Smart Grid interface between you and your energy provider. Installed in place of your old, mechanical meter, these meters operate digitally, and allow for automated and complex transfers of information between your home and your energy provider. For instance, smart meters will deliver signals from your energy provider that can help you cut your energy costs. Smart meters also provide utilities with greater information about how much electricity is being used throughout their service areas.

Smart meters provide the Smart Grid interface between you and your energy provider. Installed in place of your old, mechanical meter, these meters operate digitally, and allow for automated and complex transfers of information between your home and your energy provider. For instance, smart meters will deliver signals from your energy provider that can help you cut your energy costs. Smart meters also provide utilities with greater information about how much electricity is being used throughout their service areas.



CUSTOMER ENGAGEMENT

As consumers move toward home energy generation systems, the interactive capacity of the Smart Grid will become more and more important. Rooftop solar electric systems and small wind turbines are now widely available, and people in rural areas may even consider installing a small hydropower System on a nearby stream. The Smart Grid, with its System of controls and smart meters, will help to effectively connect all these mini-power generating systems to the grid. A potential feature of the Smart Grid will be to allow your community to use your solar array—and your neighbor’s—to keep the lights on even when there is no power coming from a utility. Called “islanding,” it will allow a home to grab power from “distributed resources,” such as local rooftop solar, small hydropower, and wind projects, until utility workers can bring the grid back online.

RENEWABLE ENERGY

Control is a key enabling technology for the deployment of renewable energy systems.



The main problems with these energy sources are cost and availability: wind and solar power are not always available where and when needed. Unlike conventional sources of electric power, these renewable sources are not “dispatchable”—the power output cannot be controlled. Daily and seasonal effects and limited predictability result in intermittent generation. Smart grids promise to facilitate the integration of renewable energy and will provide other benefits as well.

Technip has been a key contributor to global energy solutions in developing its renewable energy strategy and capability in the following areas:

- a) Biofuels
- b) Solar photovoltaic
- c) Carbon Capture and Storage
- d) Geothermal

Technip has been awarded a contract by Shell UK Limited to provide onshore FEED for world’s first commercial gas carbon capture and storage project in Scotland.

Smart meters	Customer engagement	Demand-side management	Grid Automation	Renewable energy
				



URBAN MOBILITY

TRAFFIC MANAGEMENT CENTERS (TMCS)

Automate the surveillance, coordination and response to events in the transportation network that disrupt the flow of traffic and impact the ability of the network to function normally. Sensors and cameras provide real-time visuals of developing situations across the transportation network. Remote operation of traffic control devices allow for automated and even coordinated emergency response. For example, in cases involving a multi vehicle accident the system initiates first responder activities, such as police, medical and fire. The response also includes updates to traveler information channels, e.g., DMS, 511, emails to subscribers and update posts to social media. The TMC allows us to automate the SOP (standard operating procedures) across the network which enables the TMC to deliver highly efficient and effective event management and response. The real question is “are the automated system responses optimized?”

The answer is yes. Today, most TMC systems deal with a constant on slot of complex operational decisions. We are faced with growing traffic demand that often results in concurrent incidents on a regular basis. We must also account for new requirements created for the protection of critical infrastructure. It is becoming more



difficult for operators to rely solely on a SOP, even an automated one. In response, the functionality of TMC software systems is keeping up and now has the ability to consolidate information and automate their response to incidents, including automated messaging for updates to traveler information and social media feeds.

Automation created big strides in efficiency for transportation networks, but now we have the specialized tools and the relevant data to go beyond ad hoc response. First, the use of rules-based expert systems allows for the system to select and recommend a response plans using a multi-variant approach that applies weights or scores to each rule, applies them to all candidate response plans and then calculates a total score to determine which plan best fits the event or incident. Second, tools such as traffic simulation models and decision support systems can quickly evaluate which of two or three possible response plans will have the best quantitative impact on traffic flow. Decision support for response plan selection, using both rules-based expert system and response plan simulation and comparison allows the TMC to optimize the response to both recurring and non-recurring situations that have negatively impacted transportation flows. When the TMC manager needs to make a decision about the best management alternative (e.g., divert traffic via Plan A; Plan B; or do nothing) he or she has access to quantitative results upon which to base their decision.



In the modern city, with its multitude of interrelated systems, such as transportation, utilities (power, water, waste); public safety and security systems; building management, communications and information systems; no decision can be made in a vacuum – especially decisions about transportation management. The decision support system must factor in all of these variables into account and present the reliable quantitative results to the TMC manager (or the City Manager) for the final decision.

RETRO FIT SOLUTION:-

WHO SHOULD GO FOR BUILDING AUTOMATION?

- a) Power management, thereby saving energy and saving money
- b) Big savings on operational costs
- c) Contribution to a green environment
- d) Enhanced productivity through value addition
- e) Central monitoring and control through SMART central system
- f) Control of complete space with the touch of an icon or button
- g) Enhanced aesthetics on interior décor, turning it more attractive
- h) Keep tab on the progress in your office/space and veiled threats

Ensure complete security and safety of commercial space with access control and surveillance systems like CCTV cameras



ACCESS CONTROL AND SECURITY SYSTEM

Our specialty lies in designing automated home security systems that restrict the movement of unidentified persons and keep a vigil in and around your house. In effect these are effectuated by our access control and surveillance systems respectively. Immense efforts are spent on designing customized safety systems for SMART homes. Though there are standard security solutions, we always insist on customized options as they take care of your exact needs. Certain suggestions would help you in choosing the correct



Access control devices are meant to control the access of persons through a gate or door. At gate, this control takes the form of an iron lever that is pulled up for allowing a vehicle in. Unknown vehicles might not be allowed inside. However entry bars are not a common form of security. The commonest form of automated access control takes the form of secured entrances only operable through swiping of access cards. Cards with encrypted data are swiped through a slot for allowing entry across a door. If this encrypted data fails to match with stored ones, then access is denied. Better form of access control is achieved by installing biometric controls at entrances. These recognize finger prints, retina image, or palm print. These being unique cannot be



copied by duplicated thereby ensuring a perfect security solution.

SMART POWER MANAGEMENT AND SECURITY OF YOUR COMMERCIAL SPACE / OFFICE

Reduction of Operating Costs, Absolute Safety and Power Management by optimizing energy usage thereby increasing profitability is the essence of the sustainability of a commercial building or space. Industrial automation is the solution where as an industrialist you enjoy convenience and efficiency at its best. We, Smart Automation Technologies, having transformed many traditional industries to energy efficient green buildings are a trusted name in industrial automation solutions.

Our objective is enhancing convenience, facilitating security, creating green buildings cost effectively, and improving your overall business efficiency. Innovation is what we focus on. With our industrial automation solutions, you get true value for your money. The lighting solutions, sensor based lighting, blinds control, access control, alarm systems, surveillance systems, and other products offered under the Smart banner represent globally reliable brands. Because we believe in delivering the best!

LIGHTING SOLUTIONS

One of the biggest business expenses is the monthly electricity bill. Why not cut your energy load with green lighting solutions from Smart? The smart way of cutting your office / commercial lighting is using a blend of **LED lights** and motion sensor based lighting. Stress-free control of exterior and interior lights becomes easy with sensor based lighting. It is based on occupancy that the lights will turn on and off automatically.



Why use LED lights for your industrial space? LED lights consume 80 percent less energy compared to traditional lights. They



last long, require low maintenance, rank high on energy saving parameters, are compact and highly efficient, add to the interior décor, emit negligible heat, and the list goes on.

SECURITY SOLUTIONS

Central surveillance is the essence of an office or any commercial space. Installation of a combination of access control systems, alarm systems, gas leak sensors, smoke detectors, CCTV cameras, hidden cameras, and other **Sensors and Detectors** linked to a central monitoring system ensures complete security. Surveillance systems facilitate tracking of inventory besides keeping tab on open and veiled threats. A secured corporate / business milieu and overall enhanced productivity, and thus growth of your business, is what you enjoy with SMART security solutions.

AUTOMATION CONTROLLERS AND ACCESSORIES

It is a blend of **LAN and networking**, cables and wires, PLC and SCADA, touch screen panels, and other control systems that enables automated functioning of lights, HVAC, curtains, electronic



appliances, audio/video, etc. All systems and devices are integrated and linked to a centralized control, generally a smart user interface such as Smartphone or I-pad. Preferences vary from home to home and workplaces. Installation and functioning of the automation systems can be programmed and customized to suit individual or commercial preferences.

PLC or programmable logic controller is a digital computer used for controlling and managing mechanical components and activities electrically. It comes with multiple inputs and outputs and can operate under extended temperature ranges. Resistant to vibration and impact, backed by options of non-volatile and battery-backed memory, and equipped with programming languages and communications capabilities, the PLC can perform numerous tasks at a moment.

SCADA or supervisory control and data acquisition is the solution when it comes to data collection and monitoring, especially in controlling large-scale processes encompassing large distances and multiple sites. It is generally used in industrial and infrastructure processes besides private and public facilities (buildings and entire premises spread over large areas) to monitor and control energy consumption and automate electrical activities. The complete centralized system in the SCADA is interconnected through computer networks.

With the click of an icon or button on any surface technology interface like keypad, smart phones, touch-screens, PC, and remote controllers, you can monitor and control every activity right from choosing the ambience, managing the lights, changing the internal weather, moving the curtains, and following other energy saving parameters. Reliability, performance and ease of use are what we prioritize on. We



have the equipment and understanding to meet your industrial or office automation needs.

We should be committed to re-define and re-invent the overall dynamics of the way you work and enjoy. Work is made fun with SMART industrial automation solutions. Our SMART Experts are trained to deliver the best, satisfying you beyond your expectations, beyond your imagination. We are committed towards transforming your commercial/office space or premises into intelligent sites. Approach us with your requirements and our SMART Experts, integrating their creativity with innovative automation solutions, will provide what you exactly want. We are your trusted single-window partner for life; our endeavor is to make your business secure and cost saving for a sustainable operational excellence and increased productivity.

WASTE MANAGEMENT AND ENVIRONMENTAL MONITORING

WASTE MANAGEMENT

It is the collection of all thrown away materials in order to recycle them and as a result decrease their effects on our health, our surroundings and the environment and enhance the quality of life. Waste Management flows in a cycle: monitoring, collection, transportation, processing, disposal or recycle. Through these steps a company can effectively and responsibly manage waste output and their positive effect they have on the environment.

Approaches to solving this waste problem in a scalable and sustainable manner would lead us to a model that uses waste as an input in the production of commodities and



value monetized, making waste management a true profit center. The conversion of waste as a potential source of energy has a value as a supplemental feedstock for the rapidly developing bio-fuels sector. A variety of new technologies are being used and developed for the production of biofuels which are capable of converting wastes into heat, power, fuels or chemical feedstock.

ENVIRONMENTAL MONITORING

To ensure quality of life, as well as safety, environmental monitoring is of utmost importance. By monitoring the quality of air, quality of water, and other parameters such as humidity, temperature and ambient carbon dioxide level, as well as other harmful gases, it is possible to assess anomalies in the environment; therefore ensuring pollution is kept to an acceptable level. In particular, reducing the level of carbon emissions, which is a serious threat to our planet is one of the main goals of smart cities. Environmental monitoring requires deploying a variety of sensors outdoors, in locations such as parks and rivers, etc.

BENEFITS OF SMART CITIES IMPLEMENTATION

- a) Reducing resource consumption, notably energy and water, hence contributing to reductions in CO2 emissions.
- b) Improving the utilization of existing infrastructure capacity, hence improving quality of life and reducing the need for traditional construction projects.
- c) Making new services available to citizens and commuters, such as real-time guidance on how best to



exploit multiple transportation modalities.

- d) Improving commercial enterprises through the publication of real-time data on the operation of city services
- e) Revealing how demands for energy, water and transportation peak at a city scale so that city managers can collaborate to smooth these peaks and to improve resilience.

f) These approaches have become feasible as a result of recent progress in technology:

- a) The widespread use of digital sensors and digital control systems for the control and operation of urban infrastructure. These include traffic sensors, building management systems, digital utility meters, and so forth.
- b) The growing penetration of fixed and wireless networks that allow such sensors and systems to be connected to distributed processing centers and for these centers in turn to exchange information among themselves.
- c) The development of information management techniques, specifically standardized semantic models that allow the low-level information to be interpreted by the processing centers and that allow these processing centers to interpret each other's information.
- d) The development of both computing power and new algorithms that allow these flows of information to be analyzed in near "real-time" in order to provide operational performance improvement and other insights.



SMART CITY PILOT PROJECTS

The concept of a smart city as a system that is highly intelligent and autonomous is far from being realized. Even with recent breakthroughs in technology, available technology is still not sufficiently mature for smart cities to be truly autonomous. Nevertheless, there are currently pilot projects of smart cities in development worth mentioning.

Development for Songdo, a fully ubiquitous 1,500 acre city in South Korea, was started in 2001. Smart systems in every building are used to monitor the water and electricity, which also allow residents to connect remotely using their smartphones. Sensing technologies include RFID tags on vehicles, which send signals to sensors on the road to monitor traffic flow, surveillance systems as well as smart street lights, which can be adjusted to pedestrian traffic. Some of the innovative technologies in Songdo include home and building automation where users will be able to control the systems in their houses remotely. Ubiquitous sensors are deployed virtually everywhere, from buildings, (for safety purposes, for fire, etc.) to flow sensors, which control the canal in Songdo's Central Park, and on street lights to adjust the level of lighting according to the pedestrians' flow. Smart power in Songdo is generated by natural gas and distributed through a smart grid. Tele-



presence facilities are being installed in homes, hospitals and shopping centers.

Amsterdam, unlike the previously mentioned fully ubiquitous cities which are being built from scratch, has seen some recent developments en route to make it a smart city. Currently, there are various initiatives within the scope of Amsterdam Smart City; It includes innovations such as West Orange (a residential energy management system, which is able to let users know about their energy consumption on a per appliance basis) and a smart grid initiative in Nieuw West which services about 10,000 households.

In Barcelona, there are also important initiatives. As part of this initiative, for instance, sensors have been deployed in garbage bins. Firstly, these allow remote monitoring of the content of bins, which enable the development of an improved garbage collection system, therefore optimizing garbage collection services.

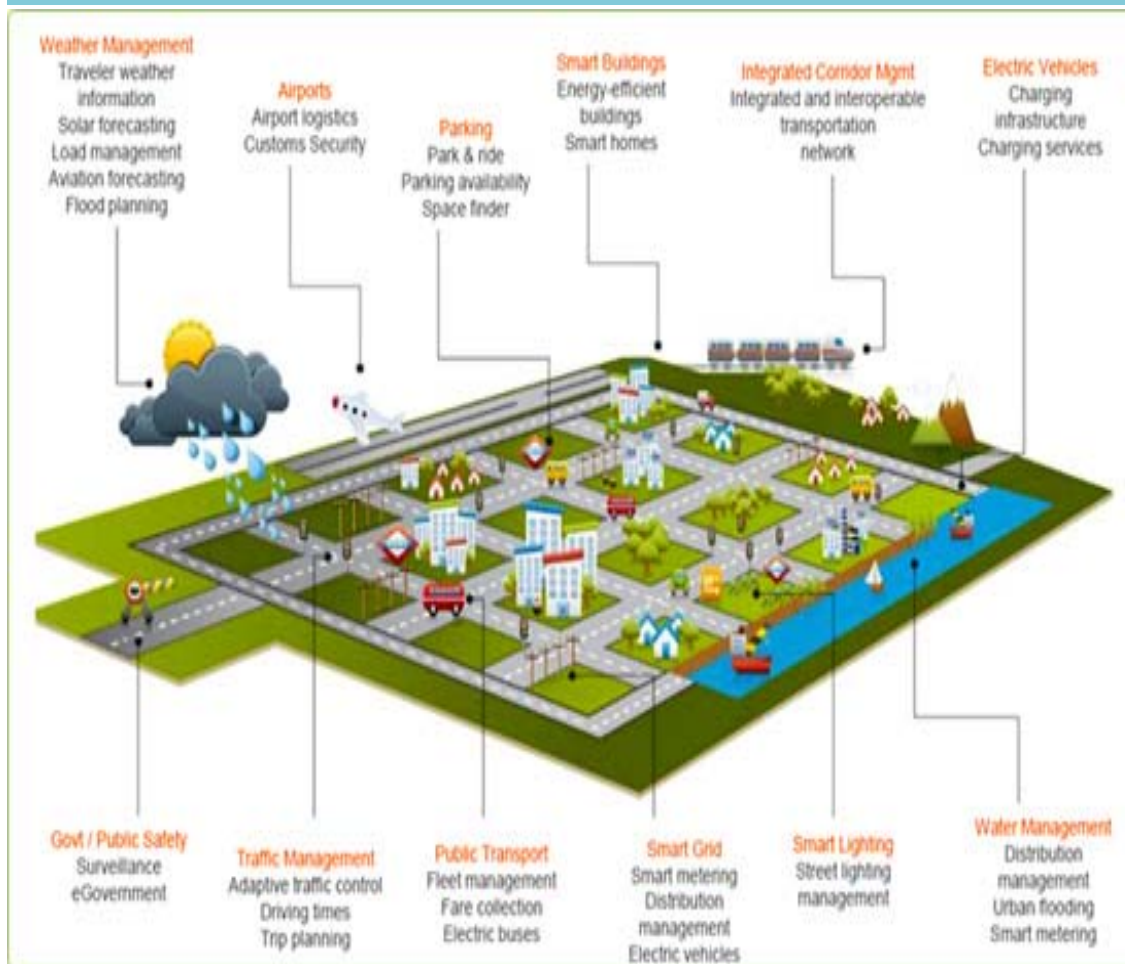
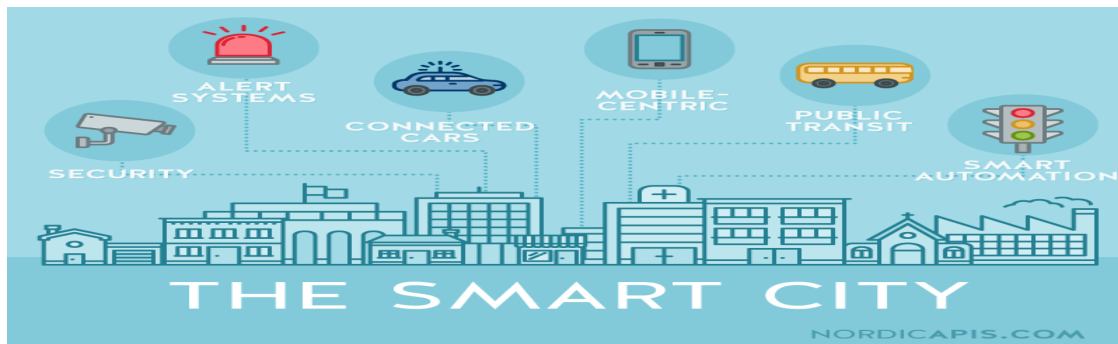
Vienna is another city with a number of initiatives from the smart city perspective. The main initiatives in Vienna deal primarily with energy efficiency, carbon footprint reduction and climate protection. A large number of projects are currently underway in Vienna.

GIFT (Gujrat International Finance Tec-City) is an under construction central business district between Ahmedabad and Gandhinagar in the state of Gujrat. So far GIFT boost modern under-ground



infrastructure, the plan however, is for meticulously planned metropolis complete with gleaming towers, drinking water on

tap, automated waste collection and a dedicated power supply – luxury to many Indians



On-line determination of total sulfur in fuels

Rodney W. Spitzer, Patrick J. Moore, and Rodney Friundenberg

Thermo ONIX
 A Thermo Electron Business
 9303 W. Sam Houston Parkway S.
 Houston, TX 77099

Introduction

Environmental regulatory agencies, such as the U.S. E.P.A., are promulgating dramatic motor fuel sulfur level reductions. By 2006 the U.S. E.P.A requires the sulfur content of highway diesel to be reduced from 500 ppm S (w/w) to 15 ppm S (w/w).¹ The reduction of gasoline sulfur content is equally dramatic with the sulfur cap moving from 300 ppm S (w/w) to 80 ppm S (w/w) by 2006.² Reduction of motor fuel sulfur content is not isolated to the U.S. Sweden and Finland have had 10 ppm S (w/w) diesel for several years. Japan will require 50 ppm S (w/w) diesel by 2005 and Australia by 2006. Proposals being considered by the European Union may require < 10 ppm S (w/w) gasoline and diesel to be available by January 2005.³ Latin American countries are also considering significant reductions in gasoline and diesel sulfur content. The challenge of meeting low sulfur fuel specifications is having a worldwide impact.

Low sulfur fuel specifications are presenting challenges to both refining and distribution. In the U.S., the low sulfur gasoline specifications, together with the expected elimination of MTBE, poses a new and potentially expensive challenge to gasoline blending operations. Should MTBE be eliminated as a gasoline additive the refiner will lose the use of a valuable gasoline diluent. Elimination of MTBE will increase the value of low sulfur gasoline blend components, such as, alkylate.⁴ Distribution of refined motor fuels by pipelines presents yet another set of challenges. It is expected that 15 ppm S (w/w) diesel will necessarily be transported in a common pipeline system with 1,000 to 3,000 ppm S (w/w) distillates, such as, jet fuel. The opportunity for sulfur contamination of the 15 ppm S (w/w) diesel is enormous.⁵ Rapid, precise and on-line determination of total sulfur will enable the economic operation of fuel blenders and provide a means for sulfur contamination detection in the fuel distribution system.

To meet these challenges, we have developed and validated a fully automated method for the on-line determination of total sulfur in diesel and gasoline. The method is similar to the well-accepted ASTM method D5453-00, "Determination of Total Sulfur in Light Hydrocarbons, Motor Fuels and Oils by Ultraviolet Fluorescence".⁶ In our on-line method the sample is oxidized in an air atmosphere at 1100 °C. The oxidation process converts organic sulfur compounds and hydrogen sulfide to CO₂, H₂O and SO₂. The concentration of SO₂ in the oxidized sample is proportional to the total sulfur content of the fuel. Quantification of the SO₂ is accomplished with a pulsed ultra violet fluorescence, PUVF, spectrometer. Dominate applications for the on-line determination of total sulfur include: 1) detection of sulfur contamination in pipelines (pipeline transmix) and 2) fuel blending operations. In order to address these applications, particular attention was paid to response time and measurement precision during the development of our on-line method.

Experimental

Instrumentation. Figure 1 is a simplified diagram of the instrumentation developed in this study. An automated liquid sample valve is used to pulse sample into the air bath oven at a typical rate of 2 µl/min. Air was selected as the carrier gas/oxidant over oxygen to

ensure safe operation in potentially explosive atmospheres (the common installation environment for on-line analyzers). The air bath oven is typically held at 190 °C to ensure the complete vaporization of the sample. A mixing chamber is used to create a near constant flow of vaporized fuel and air to the combustion furnace. The combustion furnace is held at 1100 °C to ensure the complete oxidation of all sample components. Following oxidation a constant flow of analyte is presented to the PUVF spectrometer. The PUVF is selected for its superior sensitivity over ultraviolet fluorescence spectrometers with continuous UV light sources.

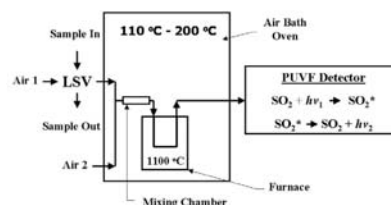


Figure 1. Simplified block diagram of instrumentation used for on-line determination of total sulfur in fuels.

Results and Discussion

Validation of Total Sulfur Measurement. Gasoline and diesel contain a wide variety of organic sulfur compounds plus potentially some hydrogen sulfide. Since approximately 90% of the gasoline pool sulfur comes from fluid catalytic cracked, FCC, gasoline, we examined its sulfur compound distribution.⁷ FCC gasoline can contain thiophene, C₁-C₄ alkyl substituted thiophenes, benzothiophenes, tetrahydrothiophene, sulfides, disulfides and thiols.^{8,9} To ensure that our on-line method fully accounts for all gasoline sulfur species a series of various sulfur compounds dissolved in iso-octane, toluene, hexane and benzene were analyzed as unknown samples. The instrument was calibrated with a thiophene in iso-octane standard prior to beginning these analyses. The purpose of these tests was to determine the conversion efficiency of the various sulfur compounds to SO₂ and to quantify errors, if any, resulting from dissimilar matrices. Results of this series of tests are presented in **Figure 2**. Examination of **Figure 2** indicates an ideal linear relationship between the reported and calculated total sulfur values, demonstrating a full accounting for the organic sulfur compounds tested. Additionally, one can conclude there is no aromatic matrix measurement error.

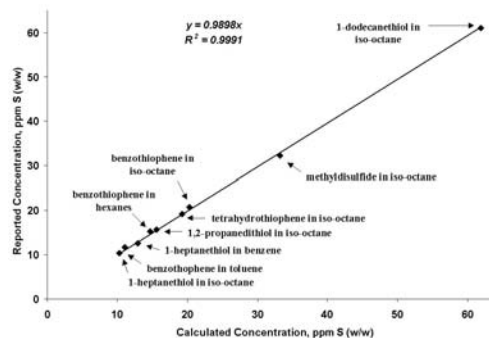


Figure 2. Reported vs. calculated values for gasoline range organic sulfur compounds in paraffinic and aromatic solvents.

Diesel fuel contains the same classes of sulfur compounds as gasoline, however, the sulfur compounds found in diesel will necessarily have higher boiling points than those found in gasoline. Unlike gasoline, low sulfur diesel (≤ 15 ppm S (w/w)) can contain significant

concentrations of refractory sulfur compounds, such as, dibenzothiophenes with alkyl substitutions at the 4 and 6 positions. Refractory sulfur compounds are difficult to remove by hydrotreating because steric hindrance prevents the sulfur atom from interacting with the catalytic site.^{10,11} The response to various diesel range sulfur compounds were measured as described previously for gasoline range sulfur compounds, however, sulfur free (≤ 1 ppm S (w/w)) # 2 diesel fuel was used as the solvent. The results of this study are presented in **Figure 3**. **Figure 3** indicates an ideal linear relationship between the reported and calculated total sulfur values, demonstrating all sulfur compounds tested are fully converted to SO_2 , including, the common refractory sulfur compound, 4,6-dimethyldibenzothiophene.

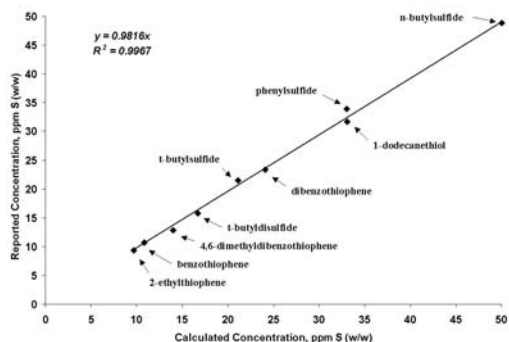


Figure 3. Reported vs. calculated values for diesel range organic sulfur compounds.

Measurement Linearity. Measurement linearity was evaluated for gasoline and diesel applications by preparing successive dilutions of thiophene in iso-octane and thiophene in # 2 diesel, respectively. **Figure 4** indicates excellent measurement linearity for thiophene in iso-octane from 4.98-99.60 ppm S (w/w) and thiophene in #2 diesel from 2.24-99.60 ppm S (w/w).

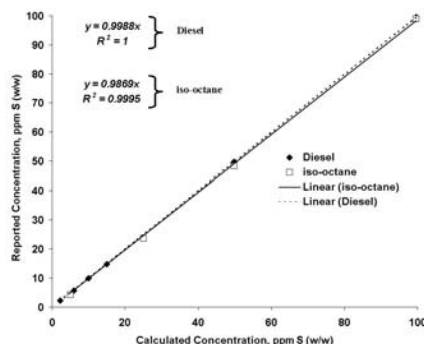


Figure 4. Thiophene in iso-octane and thiophene in #2 diesel measurement linearity.

Measurement Precision. **Table 1** shows key statistics for a 14 hour run of a California gasoline and a 16 hour run of a Japanese diesel with mean sulfur concentrations of 4.01 ppm S (w/w) and 21.59 ppm S (w/w), respectively. More than 800 data points were collected for each measurement precision study. Excellent measurement precision is indicated for each fuel.

Table 1. Measurement Precision

Statistic	Gasoline	Diesel
	14 hr Run	16 hr Run
Mean	4.01	21.59
Median	4.01	21.59
Mode	4.02	21.58
Standard Deviation	0.12	0.10
Range	0.79	0.66
Minimum	3.60	21.28
Maximum	4.38	21.93

Response Time. Response time was evaluated by switching between #2 diesel samples containing 22 ppm S (w/w) and 66 ppm S (w/w). The results of this test are summarized in **Figure 5**. As shown in **Figure 5** when switching from 22 ppm S (w/w) to 66 ppm S (w/w) approximately 1.0 minute is required to begin detecting the change in sulfur concentration. When switching from 66 ppm S (w/w) to 22 ppm S (w/w) approximately 1.5 minutes are required to begin detecting the change in sulfur concentration.

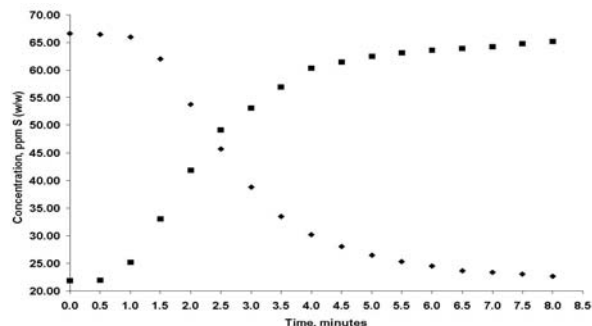


Figure 5. Response Time Measurements.

Conclusions

An on-line method for determination of total sulfur in gasoline and diesel was shown to provide an excellent linear accounting for gasoline and diesel range organic sulfur compounds at the lower expected future concentration requirements. The demonstrated response time of 1.0-1.5 minutes may be useful for detection of pipeline transmix, however, it is likely that improved response time would be valuable. The demonstrated measurement precision will allow this on-line method to be a valuable fuel blending control tool.

References

- (1) *Federal Register*, **2000**, 66 (12), 5064.
- (2) *Federal Register*, **2000**, 65 (28), 6754.
- (3) Huss, A. In *Production of Low Sulfur Gasoline and Diesel Fuels*, Oral Presentation August **2002**.
- (4) Barsamian, A. *World Refining* September **2001**, 30.
- (5) Higgins, T. *World Refining* January/February **2002**, 4.
- (6) *Annual Book of ASTM Standards* **2002**, Vol. 05.03, 446.
- (7) Golden, S.; Fulton, S. *World Refining* July/August **2000**, 20.
- (8) Shiraiishi, Y.; Tachibana, K.; Taki, Y.; Hirai, T.; Komasaawa, I. *Ind. Eng. Chem. Res.* **2001**, 40 (4), 1225.
- (9) Albro, T.; Dreifuss, P.; Wormsbecher, R. *J. High Res. Chrom.* **1993**, 16, 13.
- (10) Rodgers, R.; White, F.; Hendrickson, C.; Marshall, A.; Andersen, K. *Anal. Chem.* **1998**, 70 (22), 4743.
- (11) Isoda, T.; Nagao, S.; Ma, X.; Korai, Y.; Mochida, I. *Energy Fuels* **1996**, 10 (2), 482.

Speaker

Ms. Jaya Nangia was born in Jodhpur, India in the year 1972. She graduated in Electronics & Communication engineering from Engineering College, Kota (Rajasthan Technical University). She has 20+ years experience and is presently working with Thermo Fisher Scientific handling Process Analyser business. During her career she has been associated with proposals and sales related activities at Thermo, ABB and Chemtrols.

Setting new standards with 80 GHz

First radar level sensor for liquids with 80 GHz

VEGA Grieshaber KG is now introducing VEGAPULS 64, the first radar level sensor on the market for liquids that measures at a frequency of 80 GHz. This feature allows considerably better focusing of the radar beam. With this new instrument, measuring is much easier and more reliable, even under difficult conditions, such as tanks fitted with heating coils, baffles or agitators.

Until now, a radar sensor with a transmission frequency of 26 GHz and an 80 mm-diameter antenna had a beam angle of approximately 10°. With the same size of antenna, the VEGAPULS 64 has a beam angle of only 3°. This allows the sensor to be used even in vessels with internal installations or heavy build up on the walls, as its focused microwave beam simply avoids these obstacles.

The larger the dynamic range of a radar sensor, the higher the measurement certainty and the wider the range of applications that the sensor can be used for. Until now there was no radar sensor for liquid applications on the market with a dynamic range like that of the VEGAPULS 64. This means that media with very poor reflective properties, i.e. a low dielectric constant, can now be measured with more certainty than previous radar sensors. Even foam, turbulent product surfaces, condensation or build up on the antenna are no problem – VEGAPULS 64 measures more reliably due to its greater measurement certainty. It has an accuracy of

+/-2 mm, even with a measuring range of 30 m.

The new radar level sensor VEGAPULS 64 is not only ideal for wide use in the chemical industry, but also

in the pharmaceutical and food industries, because of its hygienic materials and design. The relevant approvals for this sector, such as 3A and EHEDG, are available at launch. Thanks to its small antenna – the diameter of the smallest version is no larger than a

1-euro coin – it results in very compact process fittings, which means the sensor can offer an interesting alternative for confined spaces in small vessels. In addition to applications in mainstream manufacturing and processing industries, the sensors open up application possibilities in pilot plants and even laboratories, which, for space reasons, had to do without radar level measurement technology until now

Eighteen months ago a new sensor for the continuous measurement of bulk solids, VEGAPULS 69, was introduced with great success. This sensor also operates with a transmission frequency 3 times higher than the widely used 26 GHz frequency. The market has shown that this technology is the thing of the future – since the market launch, over 10,000 VEGAPULS 69 level sensors have already been installed. These instruments have proven their worth, especially on media with poor reflective properties, in production shafts up to 120 m deep, or in silos with numerous internal installations that generate strong false echoes.

VEGAPULS 64 for liquid applications will follow this leap, also setting a milestone in measurement technology with its high dynamics and superior focusing. "Media with poor reflective properties, i.e. low dielectric constant, can now be measured significantly better than with previous radar sensors.

Thanks to the vastly better focusing, the beam simply passes by internal tank installations or buildup. Interfering signals, which previously had to be filtered out with false signal suppression, now play hardly any role in the measurement process.



PN-VEGAPULS-64-2016-Small-Antenna

The challenges and recommended steps to improve cyber security within industrial control systems

(Safety & security alignment benefits for operational integrity)

Rahul Gupta

Wood Group Mustang, Kuala Lumpur (Malaysia)

Keywords

Safety Instrumented System (SIS), ISA 84 (IEC 61511 Modified) standard, IEC 61508 standard, IEC 61511 standard, ISA 99 standard, IEC-62443 standard, Functional Safety (FS), Safety Life Cycle, Cyber Security, Defense in Depth, Security, ICS, Information Technology (IT), Operation technology (OT), Risk, Human factor, Hazop, Chazop

Abstract:

“Security - Protection against attack, Safety - Freedom from risk and harm”

End users or operators of industrial control systems (ICS) are responsible for the security of the systems. Many end users, however, find a challenge in addressing simple issues, typically: What requires protection from cyberattacks and how much protection is required? Will a critical system disruption or cyber theft cause a disruption to the business? If yes, how much? What is the recovery process? What is the recovery cost?

This paper will provide insight to the challenges end users face related to cybersecurity for an ICS. It will also discuss & recommend the steps to improve the security and reliability of very critical ICS, including how maturity models can improve energy sector cybersecurity capabilities and provide options in prioritizing cybersecurity investments.

Safety and security has received a lot of attention in recent years. This paper represents a compilation of benefits based on best practice; lessons learnt and author experience if functional safety and cyber Security for an ICS are integrated.

Effective management of cybersecurity challenges and exposures in the ICS environment has emerged as an important and dynamic element in the operational safety, security and reliability of the oil and gas industry infrastructure. Management information systems (MIS) are not within the scope of this paper; solely their interfaces with ICSs are discussed.

When considering security for businesses and industry, there are three traditional areas: physical security, personal security and cybersecurity. Cybersecurity aspects are the main focus of this paper.

This paper will provide an oil and gas industry insight into cybersecurity risk management as per ISA-99/IEC-62443. It will explore the similarities / differences between IT and ICS protection plus risk management, inclusive of possible ways for the integration of safety and security in an oil and gas industry ICS.

What is an Industrial Control System (ICS)?

An industrial control system (ICSs) designates a set of devices that directly control the manufacturing processes or operate technical installations (consisting of a set of sensors and actuators). Naturally, this covers the control-

command systems that we find in many operating sectors – oil and gas, energy, power, water, chemicals, pipelines, military systems, medical systems, etc.

Other frequently used terms for ICS, apart from slight differences in connotation, are distributed control systems (DCS), industrial automation

control systems (IACS), process control systems (PCS), and supervisory control and data acquisition (SCADA), intelligent electronic device (IED), digital protective relay, smart motor starter/controller, remote terminal unit (RTU), smart sensors and drives, emissions controls, equipment diagnostics, AMI (smart grid), programmable thermostats, building controls etc.

Challenges with ICS cybersecurity faced by end users

Before any end user spends time to increase the ICS plant floor security, a few simple issues need addressing by the business management:

Plant Manager

- Are there any personnel, process safety or environmental consequences to an ICS security breach, and how severe are those consequences?
- What needs protecting and how much protection is required?
- Will a critical system disruption or a data theft cause a disruption to the business?
- How long will the business be down?
- What is the recovery process, cost to recover?
- Will the business ever recover?
- And most importantly, who could threaten the business (who is the enemy?).....the big dark underworld cyber terrorist or one of the company's best employees?

CEO

- What are the Cybersecurity risks and potential business impacts to the prime business objectives?
- What are the current Cybersecurity risk level and potential business impacts?
- Does the business risk assessment follow ALARP principle meeting current regulations, industry standards and good practices?
- What governance structures / incident response structures are in place where accountabilities and responsibilities for ICS security are clearly defined and accepted?
- Is the workforce fully aware / appropriately trained on possible cyber threats to the ICS?

Information Security Officer (ISO)

- What strategies are in place to identify and manage the cybersecurity risks to the ICS?
- How are cybersecurity maturity and compliance levels measured?

- Has an effective set of controls that will reduce the risk to ICS to ALARP been selected?
- How comprehensive is the ICS incident response plan? How often is it tested?
- How many and what types of cybersecurity incidents to the ICS occur per reporting period? What is the threshold for notifying the executive leadership about a cybersecurity incident?
- How well do the IT and process automation / production departments communicate and collaborate on cybersecurity?

Maturity Models

A maturity model is a framework that allows an organization to assess the rigor of its security practices and processes according to industry best practices. The U.S. Department of Energy (DOE) has developed a maturity model specifically for the oil and gas industry - the Oil and Natural Gas Cybersecurity Capability Maturity Model (ONG-C2M2). This model, part of a broader effort to improve security in the energy sector, is one of the few that includes both IT and OT and provides a mechanism to help evaluate, prioritize and improve cybersecurity capabilities in both areas.

It is intended to help:

- Strengthen cybersecurity capabilities in the oil and gas subsector.
- Enable oil and gas organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities.
- Share knowledge, best practices and relevant references within the subsector as a means to improve cybersecurity capabilities.
- Enable oil and gas organizations to prioritize actions and investments to improve cybersecurity

The ONG-C2M2 model is descriptive rather than prescriptive, allowing companies to select their own goals and establish the appropriate controls and policies for meeting them.

IT /OT and their relationship to ICS:

ICS vendors have traditionally functioned most often as comprehensive vendors, meaning that they have both designed and built the systems

they supplied. These days, increasingly standardized technologies and components from the traditional IT world (often referred to as commercially available off-the-shelf, (COTS) are being used in ICS. Some examples of COTS products used are Microsoft operating systems, IP-based communication technology (Ethernet/IP, TCP/IP etc.), MS-SQL and Oracle database solutions. This shift to standard components is changing the role of the vendor from system supplier to system integrator. This, in turn, can lead to a reduction in vendor insight and control of important components of the integrated system. Subsequently, increased knowledge of ICS security is required by the end users of the systems.

Let's first look at IT and OT and their relation to ICS:

Operational Technology (OT) is an umbrella term used for various technologies that support operations. It consists of hardware and software systems that monitor and control physical equipment and processes for safe & reliable operation, often found in industries that manage

vital activities in the production and distribution of various industries such as oil & gas, not only produce a wealth of sensitive and proprietary information, they are also essential to the economic health and physical safety of the company, its facilities and its people.

While the technology is familiar to operators and engineers in these sectors, outside of people working in or with these specialized environments, there is a limited understanding of what's involved. Within the control systems industry, ICSs are often referred to as OT systems.

In contrast, **Information Technology (IT)**, managed by information officer (IO) and IT departments, is the application of computers to process, transmit and store data, typically in a business or enterprise environment. IT systems are in place to allow machines to exchange information directly with humans, usually within seconds. Various industries have experienced an exponential increase in both quantity and quality of IT systems. Improved enterprise resources

	Information Technology	Operational Technology
Purpose	Process transactions, provide information	Control, monitor, or protect physical processes and equipment
Operating environment	Offices, data centers, control centers	Field equipment, substations, control centers
Architecture	Enterprise-wide infrastructure and applications (generic)	Event-driven, real-time, embedded hardware and software (customized), highly distributed data processing and control
Interfaces – inputs and outputs	GUI, web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays, hand-held devices as well as GUI / human-machine interfaces
Ownership	CIO and computer graduates, finance and administration departments.	Engineers, technicians, operators and managers
Connectivity	Corporate network, IP-based	Proprietary and industry standard control networks, hard-wired twisted pair and IP-based
Role	Supports people	controls machines and process conditions
Security objective priority	Confidentiality, integrity, availability	Availability, integrity, confidentiality

Table 1 – Security focus and other performance parameters in IT versus OT

critical infrastructure, such as water, oil & gas, energy, and utilities, but also in automated manufacturing, pharmaceutical processing and defense networks.

This technology uses many specialized terms such as PCD, PLC, DCS, SCADA and SIS, often collectively referred to as industrial control systems (ICS).

The operational technology (OT) systems that oversee the volume, velocity, location and other

planning (ERP), geographic information systems (GIS), and customer relationship management (CRM) systems, along with office-based productivity tools and mobile computing devices, have permeated the business workplace.

IT versus OT

Historically, OT and IT have not overlapped and were managed as separate organizational silos. IT

and OT have long, isolated histories with many examples of failed attempts to integrate them or even use tools from one environment to the other.

OT and IT were developed to accomplish two distinctly different missions, with contrasting agendas and dissimilar tools and priorities. There are several other similar differences between IT and OT [Refer table-1].

ICS cybersecurity- organization challenge IT or OT

The hurdles, however, of ensuring good cyber safety do not stop at choosing the right technical protection. It is the organizational structure of companies that holds a whole new set of challenges.

The difficulty in the oil and gas industry is that invariably there are two organizations: the IT organization that is traditionally responsible for security and the engineering organization, which is traditionally responsible for operation technologies. In order to achieve effective cyber safety it is imperative that these two organizations work together and learn to understand each other's objectives / start speaking the same language.

The IT organization is used to the concept of cybersecurity and building security into their solutions. Whereas, the engineering organization, which is focused on the reliability and availability of its plants, invariably has no or only a limited understanding of cybersecurity.

The responsibility for cybersecurity often lies with the IT department, which fails to understand the embedded IT in the ICS. At the OT working level there is a certain amount of push-back due to the concern about how cybersecurity measures may impact operations safety and efficiency. Not recognizing that, nor implementing these measures, may have a greater potential for impacting safety. The end result is that the organization may fail to adequately manage the cybersecurity risks to the ICS.

Since the turn of the century, however, business demands and economics have had a major impact on these problems. For example, in the energy sector the introduction of real-time energy trading markets has demanded responses that

have necessitated more convergence between the two systems. The OT community needs the IT community because they are able to identify issues that OT doesn't see but, IT does not understand the OT environment so bridges between the two groups are required.

OT and IT certainly have significant hurdles to overcome in pursuit of collaboration, none greater than the challenge of achieving security and interoperability without disrupting critical services or diverting excess capital from the enterprise.

How cyberattacks are identified also looks vastly different. Enterprise IT owners know they've been hacked whereas OT owners must recognize a physical event (e.g. a pipe breaks) and work it backward to find the culprit, cyber or otherwise. So the ICS needs forensics and cyber logging.

Integrated IT and OT security - New trend

Integrated IT and OT security is a new trend in the oil and gas industry, although there are varying levels of awareness and implementation:

- Some organizations have little or no awareness of, or interest in, the issue,
- Some are aware of the need but are unsure how to proceed.
- Some are addressing security but are not as advanced as they believe,
- Whilst others have misplaced confidence in IT perimeter defenses that cannot adequately protect OT systems.
- A very few have established a robust and on-going security program and management system.

There still exist misconceptions with ICS being monitored by IT professionals resulting in many oil and gas companies that are poorly protected against cyber threats, at best. They are secured with IT solutions that are ill adapted to legacy control systems Or OT being negatively impacted by IT Cyber Security measures that are not aligned with the criticality of Availability and Integrity in OT systems.

To those not directly involved it may seem that the ICS falls under the umbrella of the IT experts, but typically, that is not the case.

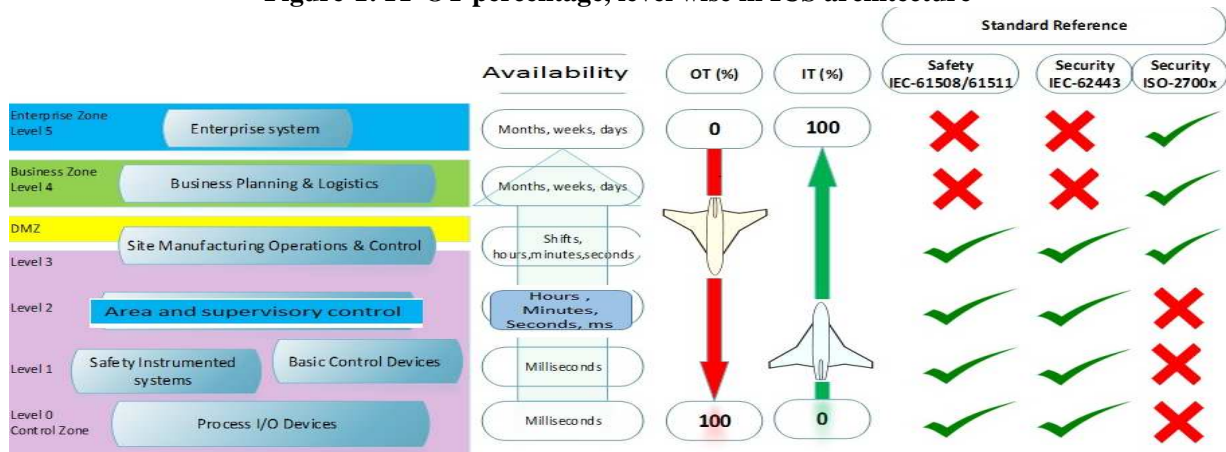
ICS architecture-combination of IT and OT

The ICS-level architecture is used to define the accreditation boundary for OT systems and is a logical representation of the OT network. The actual physical system can span many miles; for example, pipelines, electric transmission and distribution systems can have many non-contiguous components, and there are a number of protocols commonly used by ICSs to allow the devices within the layers to communicate both horizontally and vertically.

The ICS architecture is described in five levels (and multiple sub-levels), where each level represents a collection of components that can be logically grouped together by function. Generally this is the preferred reference model as per ISA 99/IEC 62443. This model has become the standard for networks in industrial companies being adopted from the Purdue model that was

developed to define and segregate the systems, components and activities in an industrial company. This ensured that higher level activities, such as reporting, would not interfere with the control and data acquisition of the process. As cybersecurity risk management needs emerged, the reference model facilitated the clear identification of segregation points where network protection/ isolation devices could be installed. It is worth noting that not every implementation of an ICS makes use of every level and that the same device may reside in different levels, depending on its configuration. A composition of IT & OT components in a level (as shown in figure-1) is for discussion purposes and may vary depending on system architecture, application etc. Most current ICSs and subsystems are now a combination of OT and IT.

Figure-1: IT-OT percentage, level wise in ICS architecture



ICS cybersecurity - recommended actions for end users:

It is important that ICS cybersecurity requirements are defined at the start of the project such that system manufacturers are informed from the outset.

ICS manufacturers are starting, and soon it will be mandatory, to include security requirements in the design phase of ICS components and applications. Operators, however, indicate that independent evaluations and tests are missing to effectively guarantee that these devices are secure, and interoperability has also been considered when new security features/capabilities are included.

ICS operators, must understand the relevant dependencies, including managing the cyber risks across interfaces with third parties. The following good practices should be adopted:

- Include cybersecurity requirements in the system requirements presented to suppliers. These cybersecurity requirements should be derived from cybersecurity risk assessments and analysis of possible mitigating controls.
- When possible, contractually demand that suppliers and their subcontractors comply with end user's cybersecurity approach and policies. Owner/Operators also need to be cognizant of how different parts of their control systems have different functions, risks, and potentially exposed edges that must be communicated to the control systems designer

and provider. Otherwise, the threats cannot be properly identified, evaluated and mitigated.

- Mandate that suppliers demonstrate their teams have relevant cybersecurity qualifications for the required tasks and responsibilities. Where required, awareness training on relevant security policies should be provided.

During the specification phase:

- Define the means for conducting preventive and curative maintenance operations
- Specify the location of devices to ensure their physical security; specify the security level requirement of each zone in the required control system. At a minimum, specify who will have access to each zone, area or segment of the physical network.
- Require that software provided be not exclusively compatible with a specific version of another software platform
- Require that software not essential to the running of a system be installed on other machines

During the design phase:

- Reduce system interfaces and complexities to limit the introduction of vulnerabilities during implementation;
- Select components offering the best characteristics to meet security requirements,
- Clearly distinguish user profiles from administrator profiles;
- Make provision for mechanisms to standardize changes on a group of machines

During the integration phase:

- Change default configurations (for example, passwords);
- Delete or deactivate functions that are not used but activated by default;
- Consider deleting debugging functions such as tracking used to analyze ICS behavior.

During the test phase:

- Conduct functional security tests; error tests for business functions and check exceptions
- Test threat scenarios (penetration tests and attempts to gain control)
- Test ways of carrying out maintenance operations at the cybersecurity

Safety and security integration- can we relate functional safety and cybersecurity?

Now we understand that the ICS is a combination of IT and OT but that both IT and OT are different and so is their related security.

Security has not been a crucial factor in the development of industrial control systems or OT. Also OT has one more critical aspect of importance – safety.

An ICS is actually a system of systems. A crude distinction between mainstream IT and control systems is that IT uses physics to manipulate data while an ICS uses data to manipulate physics. The potential consequences from compromising an ICS can be devastating to public health and safety, national security, and the economy. Compromised ICS systems have led to extensive cascading power outages, dangerous toxic chemical releases, fire, floods, chemicals spill, and explosions. It is therefore important to implement an ICS with security controls that allow for reliable, safe and flexible performance [Refer Table-2 for more details of comparison of IT vs ICS].

As systems are becoming more complex and integrated, the distinction between safety and security is beginning to weaken. ISA has also identified a need of alignment between safety and security and defined in ISA-99 (IEC-62443) and ISA-84 (Modified IEC-61511)/IEC-61508. Safety and security are two key properties of the ICS; they share identical goals – protecting the ICS from failures. Safety is aimed at protecting the systems from accidental failures in order to avoid hazards, while security is focusing on protecting the systems from failures through intentional attacks.

Due to safety traditionally being the primary objective of OT systems, and that safety largely depends on the stability of the systems, Cybersecurity has been a secondary consideration for OT systems, if it has been considered at all. This is changing, however, with the integration of IP networking and the adoption of other standardized protocols in OT, Cybersecurity, with the ability of cyber-attacks to produce physical world results, is now becoming essential to safety.

Weak alignment between security and safety may produce inefficient development and partially-protected systems. A given system is only as Safe as it is Secure” (if the availability or integrity of a

no alignment between safety and security countermeasures, these interdependencies are not detected in the early system development phases

SECURITY TOPIC	INFORMATION TECHNOLOGY	INDUSTRIAL CONTROL SYSTEM (ICS)
Anti-virus/Mobile Code	Common widely used	Uncommon/difficult to deploy effectively
Support Technology Lifetime	2-3 Years diversified vendors	Up to 20 years single vendor
Outsourcing	Common widely Used	Operations are often outsourced, but not diverse to various providers
Application of Patches	Regular scheduled	Rare, unscheduled, vendor specific
Change Management	Regular Scheduled, higher risk tolerance for untested changes in commodity user systems	Highly managed and complex
Response Time	Response time generally not critical. Components may be rebooted	Response time may be part of safety case Availability is paramount to operation
Availability	Generally delays accepted 95 – 99%	24 x 7 x 365 (continuous) 99.9 – 99.999... %
Security Awareness	Moderate in both private and public sector	Poor except for physical
Security Testing/Audit	Part of a good security program	Occasional testing for outages
Physical Security	Secure (server rooms, etc.)	Remote/unmanned secure
Primary subject for protection	Information	Physical process
Primary risk impact	Information disclosure, economic	Safety, health, environment, economic
Security focus	Central server security	Control device and process stability
Operating environment	Interactive, transactional	Interactive, real-time
Problem response	Reboot	Fault tolerance, on-line repair
Authentication	Often centrally managed user accounts	Often local to each device. May be very basic
Performance requirement	Not real time, response must be consistent, delay acceptable	Real time, response is time –critical, delays can create serious problems
Risk management	Data secrecy (confidentiality) and correctness (Integrity) are most important, fault tolerance not serious	Safety is important for both people and production systems, fault tolerance are very important.
Security solutions	Designed for typical IT systems	Security tools and updates must be tested to guarantee that they don't jeopardize the ICS operations
Communications	Communication protocols are standard types and primarily using telephone network/wireless networks	In addition to standard protocol, proprietary protocols are in use. Different media is used - radio links, optical fiber, satellites, VPN etc.

Table 2 – IT versus ICS Comparison

safety system or other layer of protection is reduced by a security risk or breach, its ability to provide the required protection is also summarily reduced).

For example, excess costs could be spent on redundant safety and security countermeasures. Furthermore, security counter-measures may weaken ICS safety, or vice versa – safety countermeasures may weaken security. If there is

and may lead to a number of problems that affect later ICS development or even in the operation phases.

Safety and security are interdependent, and these dependencies have to be considered during ICS design phase.

Why to deal cybersecurity & safety together:

To cover all risks, cybersecurity and safety must be dealt with together, using a joint approach.

For example:

- 1) The potential causes of a temperature increase at a plant above its nominal threshold may be:
 - A reading issue linked to the failure of a sensor:
 - Physical failure of a sensor,
 - Incorrect calibration of the sensor,
 - An intentional change e.g. sensor value, range parameter units, time, location hierarchy, etc. made to the parameters of a sensor by an unauthorized person (gaining control by a hacker or a virus) or as a result of negligence;
 - A problem associated with a cooling circuit valve:
 - Mechanical failure,
 - Servo-motor failure,
 - Results of an act not undertaken - e.g. remote-auto, intentional forcing of the command valve value by an unauthorized person (gaining control by a hacker, a virus) or as a result of negligence,
 - A problem with the setting of the set point for regulating the cooling system,
 - An input error made by an operator,
 - A change made to the set point by an unauthorized person.
- 2) The worst scenarios for an ICS are:
 - Introduction of malware into the ICS;
 - An intrusion into the ICS.

This malicious action may be carried out by an individual on site, remotely via the MIS or via a compromised work station or inadvertent malware injection by portable media or computers connecting to the ICS.

The scenario results in either the loss of one or more operator stations or HMIs (e.g. black or frozen screens, erroneous information displayed) or commands being sent with the intention of causing malfunction. This incident would result in downtime for some units, commonly lasting one to three days until the source of the problem is isolated and remediated.

Functional safety is the part of the overall safety of a system or piece of equipment that depends on the system or equipment operating correctly in response to its inputs, including the safe management of unintentional but likely operator

errors, hardware failures and environmental changes.

Safety (and functional safety) deals with random and unintentional events (accidents and failures). Statistics can be used and mean time between failures (MTBF) rates can be calculated. Additionally, security also deals with intentional acts, targeting a subject; statistics are not applicable as mean time between attack can't be calculated. However, the prevalence of persistent threats (e.g. malware and active threat actors) raises these threats to high relative probability. It has been advocated that the threat probability is a 1.0, and the only factor in the Cyber risk equation to really focus on is the Vulnerability, and assessing or assigning a coverage factor (or confidence factor, highly subjective) for how well common threats are being mitigated by a given system design and the owner/operators systemic capability to maintain the mitigation in sustained operation.

Both safety and security issues can cause potentially dangerous events within a plant. As a result, cybersecurity is covered in the recent edition of Functional Safety Standard IEC61508 (Edition 2, Section 7.4 Hazard Analysis). The revised standard requires that in the case where the hazard analysis identifies that malevolent or unauthorized action, constituting a security threat, is reasonably foreseeable, a security threat analysis should be carried out. Section 7.5. (Overall Safety Requirements) recommends undertaking a vulnerability analysis in order to specify security requirements. Similarly security requirements are specified in Clause 8.2.4 and 11.2.12 of IEC-61511 -1:2015.

It can be said that both safety and security imply the need for protection, however, the chosen protection must address risks that are radically different in nature but there is an important similarity; neither safety nor security is a one-time event. As indicated in IEC61508 and ISA 99/ IEC 62443, a common mistake is to address safety and cybersecurity as being similar to a project with a start and end date. When this occurs, the safety and the security level will tend to decline over time. Particular to cybersecurity, risks constantly change as new threats and vulnerabilities surface along with ever-changing technology implementations.

It is no longer possible to be truly safe without also being secure. The challenge though, is to not

only address security issues, but to get the most from the ability to connect systems and share data. There seems to be a fine line between security and productivity.

As today's cyber threats become increasingly malicious with the focus now firmly on automation systems, the continued evolution of the threats suggests that we battle them with the combined force of both the IT cybersecurity approach and an engineering functional safety approach.

Functional safety and IT assessments

Functional safety assessments typically focus on the failure of a piece of equipment, addressing the probability of failure, the potential consequences, and the impact on safety, the environment, and the business.

IT assessments are very similar, but the consequences of a system being compromised would more likely be the massive economic impact of a production interruption, rather than loss of life.

Following corporate IT practices, tools have been created for use on process control engineering networks that scan the system for details such as asset identification, protocols in use, operating system status, version levels, patch levels, service pack installation, etc. If not applied with cybersecurity concerns in mind, however, these same tools, by the nature of the network design, might provide potential hackers with intelligence that was not previously accessible to them. For this reason a combination of skillsets or departments should be employed in all aspects of security from the field device to the corporate firewall that connects to the Internet.

One commonly suggested security solution is to isolate the ICS from the corporate and Internet systems through the use of firewalls. Unfortunately, while firewalls are widely used in the traditional IT sector, their effectiveness in ICS environments is still under development. IT firewalls are generally unaware of ICS protocols and may introduce unacceptable latency into time-critical systems that face operational constraints not typical in the IT world. To make matters worse, many end users are not

knowledgeable exactly how these firewalls should be deployed in terms of architectures, configuration and management.

IT systems evolved with a tactical mentality in their approach to security, whereas process control has taken a more strategic approach. Only now are they becoming more tactical, making it essential that both IT and engineering skills and practices be combined in the assessment of today's plant risk.

Is human factor common in safety and security?

When new technology is introduced, it still has to be managed by people, so people have to understand that technology in terms of its capabilities and limitations to ensure the correct application; for that people require procedures and training.

If we look at the rise in recent attacks, the Stuxnet virus is probably the most well-known due to the surrounding publicity, in-depth reporting and the fact that it specifically targeted process automation systems. This threat was created outside the plant and designed to cause disruption to the routine running of a process or processes. The virus was designed with the specific knowledge of the protocols used on the process control network, enabling it to wreak havoc. It would be interesting to know if any pre-HAZOP or risk and threat assessment considered this type of attack when the systems were designed and implemented.

But Stuxnet wasn't just about technology; it also involved human weakness and error. One of the principal vectors for introduction of the virus was reportedly via a USB device that was left where employees would find it. Did the persons finding such a device consider the risk, impact, and consequence of using the device in the process control domain? Probably not.

So which department's safety, security, risk, and threat assessment should be responsible for addressing this type of threat? The answer should be both!

In retrospect it is easy to see that from an IT perspective, better management of the USB ports

would have helped. Had cybersecurity been considered during the functional safety assessment, then the consequences and impact might have been assessed and understood, driving the relevant risk reduction measures to be implemented. These could have included disabling USB ports, ensuring that policies and procedures are implemented, and training personnel on the risks of using rogue USB devices, and so on. It is worth noting that USB attack case for Stuxnet is just only one (but the simplest) viable route for seeding the attack but there were many other secondary attack vectors.

How should we measure security risk and carry out risk assessments?

Before acquiring ICS, cybersecurity requirements should be derived from cyber risk assessment. There are numerous definitions and equations for risk, and they change depending on the industry and the discipline. A common risk equation can be defined as:

$$\text{Risk} = \text{threat} \times \text{vulnerability} \times \text{target attractiveness} \times \text{consequence}$$

The problem with this is it is difficult to assign actual numbers to the equation e.g. the probability of any risk scenario involving a terrorist attack is effectively unknown; and predicting isolated and rare events is generally accepted as virtually impossible to calculate. Threat and vulnerability (both very qualitative terms) are used to represent probability without specifying the mathematical formula. In addition, it would likely need to be recalculated on a regular basis due to external changes. For instance, Microsoft releases patches to their operating systems every month; these may directly affect the vulnerability of one or more control systems and hence drive the risk up. Asset owners have to decide if the increased risk is worth accepting, eliminating (by installing the patch), or mitigating by other means.

The Confidentiality, integrity and availability (CIA) triad is used widely within IT security circles, but the importance is often reversed in control systems as availability is usually far more important than protecting actual information. For critical safety and control system it would be totally different and priorities would be in the order of safety, integrity, availability and then confidentiality.

The increase in news channels around hacking critical infrastructure obviously also raised the target attractiveness index.

The final factor, consequences, needs to be very carefully considered. Disaster at the Deepwater Horizon drilling rig in the Gulf of Mexico in 2010 etc. showed how easy it is to underestimate the consequences of any incident. Apart from the human and environmental cost, the industry as a whole will likely be impacted by increased regulation.

Technology is not the main protector of an organization. There is an illusion that if as much technology as possible is bought that will guarantee safety but that is not a possible and effective solution.

Managing risk assessments correctly can often make the difference between suffering millions of dollars in damages and keeping assets safe. Referring to Figure 1, level-0 may include standalone TCP/IP devices, which require to be updated, causing an issue with process data going out to a L1 controller or PLC to control the process, but the TCP/IP devices being updated from level 3. Note, this is not supported in the ISA 99/IEC 62443 standards, proving there will always be exceptions in a network and so a risk analysis must be made.

As per ISA 99/IEC 62443 standards securing the process environment from the inside is about working with zones and conduits. By identifying the zones in the network infrastructure it is possible to keep data transfer within these zones or transfer limited data between zones via the conduits.

The cyber risk assessment study can be performed with the following approach and be seen as an iterative and continuous process:

- Define the risk analysis methodology
- Identify major items and their security impacts in term of availability, integrity, confidentiality and data loss.
- Identification - evaluation of the threat scenarios with their impact and likelihood.
- Reduce the risks by designing adequate countermeasures.
- Summarize the results in a risk register.

Relationship between Safety Integrity Levels (SIL) and Security levels (SL)

SIL - As per IEC-61511 - 1:
Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems.

SL- As per IEC 62443-1-1:
Level corresponding to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit.

1. **Safety examines** by assessment of whether the SIS meets the SIL requirement
2. **Security examines** the vulnerability of components that interfere with or disrupt the ICS operation. This again is a failure analysis, but the process of analysis is significantly different. The result requires improvement of security mitigation functions, but does not require an improved SIL.

The relationship between SIL and SL comes from the similarity of possible consequences but with completely different root causes. The failure of a safety system could be severe, such as damage to equipment, the environment or even loss of life. A cyber-induced attack could do the same by either altering the database or disabling the safety system.

Some requirements for SLs are already covered in IEC-61508/61511.

How can we integrate practices and procedures for safety and security?

Just having IT and engineering groups in communication is not enough. Effective collaboration requires a close analysis of the practices and procedures for both departments to see if there are any contradictions. Synergy is good, but any contradictions could be a potential weakness in the system.

The time has come to combine the best of the IT world and the functional safety world. The next time that a HAZOP is performed, consider not just the process hazards, but also the IT hazards,

consequences, and impact. ISA has life-cycle models for security and safety, defined in ISA99/IEC-62443 and ISA84, respectively. In the ISA99, a process is defined to assess the security of control systems (and IT systems) using a scale very similar to that used in the safety industry. Asset owners can start to look at the security of control systems today using another process taken from the safety industry — the HAZOP (hazards and operability analysis). This can be used as a basis for a Control hazards and operability analysis methodology (CHAZOP), which is being used by a number of enterprises in the control systems space. The time taken to fully complete a CHAZOP cannot be underestimated, especially on large interconnected systems.

Within the security world, the phrase “defense in depth [DID]” is used widely, and is a means to deploy numerous defensive mechanisms throughout the control systems to block (or at least delay) hackers trying to break into a system. The number and sophistication of these deterrents will decrease the likelihood of an attack succeeding. The principle of DID means creating multiple independent and redundant prevention and detection measures. The security measures should be layered, in multiple places and diversified. This reduces the risk that the system is compromised if one security measure fails or is circumvented. DID is a term used to describe the full complimentary suite of controls for consideration in protecting systems and networks, such as [Refer Table-3 for DID]:

Policies & Procedures	Security policies, procedures, standards, training, business continuity and recovery plan
Physical Security	Locks, access control, guards
Perimeter Security	Firewalls, intrusion prevention system (IPS), internet access filtering, remote access controls, email filtering, denial of service mitigation, data loss prevention tools, Intrusion / leakage detection system(IDS), multi-factor authentication and authorization, access control lists (ACL)
Internal Network Security	Network segregation-zone and conduits, port management, ACL, device authentication, wireless network encryption, asset inventory management, vulnerability scanning tools, Internal firewalls, Network-based IDS

Host security	Authentication & privilege management, patch management, anti-virus and host intrusion prevention system, blacklisting, white listing, removable media restrictions, host based firewall, server hardening, access controls, continuous monitoring
Application defenses	Unique user and password required, secure coding practices, training, testing tools, penetration tests, code analysis tools, software inventory management, access control, authentication, secure software
Data Defenses	Access controls, encryption, crown jewel protection, data leakage protection(DLP),secure communication, access control, authentication

Table-3: Defense in Depth

Defense-in-depth strategy focuses on incremental but intelligent controls at each layer of the organization. The following are the most commonly known attack vectors for ICS, DID strategy is most effective in controlling them if applied systematically:

- Backdoors and holes in network perimeter
- Vulnerabilities in common protocols
- Attacks on field devices
- Database attacks
- Communications hijacking and man-in-the-middle attacks

To reduce systematic errors, standards IEC 61511-1 (Safety) and IEC 62443-3-3 (Security) require separate levels of protection and autonomy of the operating equipment and protective equipment. By design, an autonomous process control system and a safety system from different manufacturers require different engineering tools, databases, and operating procedures. Such systems from different manufacturers avoid common cause risks and reduce the security risk through diverse technology. In practice diverse technology also ensures a clear separation of the areas of responsibility and supports the different handling of operating equipment and protective devices.

Conclusion

ISA 99 / IEC 62443 introduced the concept of a Security Management System, which, in a similar fashion to IEC61511/ISA84 Functional Safety Management System, defines a security lifecycle that assists the users in establishing and

maintaining the installation security level over time.

Benefits of Integration of safety and security are

- More safe and secured systems
- Systematic analysis of threats and hazards
- Identification of safety function where security is important
- Define common mitigations and requirements
- Harmonize safety and security contradictions

Although safety and security focus on different problems, causes and consequences, it is no longer possible to be truly safe without also being secure. The challenge however, is to not only address safety and security issues, but to get the most from the ability to connect systems and share information conducive to effective and efficient decision making. There seems to be a fine line between safety, security and productivity.

References:

1. IEC, "Functional safety – safety instrumented systems for the process industry sector IEC 61511,
2. IEC, "Functional Safety of electrical/ electronic/ programmable electronic safety-related systems IEC 61508,
3. DHS Cyber security Self Evaluation Tool (CSET)
4. National Institute of Science and Technology (NIST) Publication
5. ISA-99/IEC-62443-security for Industrial Automation and control systems
6. Wikipedia



Biography: Rahul Gupta was born in Ajmer (India) in year 1968. He graduated in Electronics & Communications engineering from University engineering college, Kota (Rajasthan). He worked in Instrumentation and Control department in Engineers India Ltd. New-Delhi between 1994 to 2005. At present he is Technical Authority (Automation and Control) at Wood Group Mustang Kuala Lumpur (Malaysia)-covering primarily Asia Pacific region. He is a certified Functional Safety Expert (TÜV Rheinland) and Industrial Automation and Control Systems Cyber Security specialist (ISA) for control and safety system. He has over 25 years of global working experience in the oil and gas industry. He provides consultancy advice in functional and process safety particularly on practical aspects for the implementation of functional safety and its management requirements as per IEC-61508/61511 for the whole safety instrumented system (SIS) life cycle on new projects, as well as for the installed base of SIS, Cyber Security Risk Assessment as per IEC 62443, Alarm Management, Reliability and Availability of Control and Safety Systems. He has participated and presented technical papers in several global conferences/ symposium.

EFFECTIVE MERCURY MEASUREMENT IN POWER PLANT

Vijay Nair
Chemtrols Industries Ltd.

KEYWORDS

Mercury, Power plants, MERCEM 300Z, ZEEMAN effect

ABSTRACT

Even trace amounts of mercury can cause serious poisoning. Mercury starts to vaporize in traceable amounts even at room temperature. In this state it is even more hazardous than when it is in liquid or solid form. It's no wonder therefore, that mercury is strictly monitored in Power plants, incineration plants and cement kilns. Allowed Hg concentrations are in the low μg -range. For this reason, measurement devices must be both extremely sensitive and highly accurate.

The MERCEM300Z from SICK with its patented direct measurement system is a high-performance mercury analyzer for providing reliably measured values of elemental and chemically bound Hg in gases at any time.

INTRODUCTION

Mercury is a naturally occurring element that exists in several forms: elemental mercury, inorganic mercury compounds and organic mercury compounds. Elemental mercury is a shiny, silver-white metal that is liquid at room temperature. Elemental mercury can evaporate to become an invisible, odorless toxic vapor. Inorganic mercury compounds take the form of mercury salts that are generally a white powder or crystalline, with a notable exception being mercuric sulfide, which is red. Organic mercury compounds,

such as methyl mercury, are formed when mercury combines with carbon.

Methylmercury is special among organic mercury compounds because large numbers of people are exposed to it and its toxicity is better understood. Methylmercury in food, such as fish, is a particular health hazard because it is easily taken up into the body through the stomach and intestines. It is a poison for the nervous system. Exposure during pregnancy is of most concern, because it may harm the development of the unborn baby's brain. Some studies suggest that small increases in exposure may affect the heart and circulatory system.

Elemental mercury is also poisonous to the nervous system. Humans are mainly exposed by inhaling vapors. These are absorbed into the body via the lungs and move easily from the bloodstream into the brain. However, when elemental mercury is ingested, little is absorbed into the body. The inhalation of elemental mercury vapors can cause neurological and behavioural disorders, such as tremors, emotional instability, insomnia, memory loss, neuromuscular changes and headaches.

Mercury is released into the environment through both natural processes (e.g. volcanic activity, weathering of rocks) and human activities. Human activity is now the main source of mercury being released into the environment. Much is released unintentionally from processes where mercury is an unwanted impurity. Emissions into the air, mainly from fossil fuel power plants and waste incinerators, are expected to increase unless other energy sources are used or emissions better controlled.

All statutory requirements are based on absolute emissions values, in other words, the sum total of elemental mercury Hg⁰ and oxidized mercury Hg⁺. The amounts and ratios of these two mercury forms in the flue gas depend largely on the raw materials being incinerated and the fuels used in the kilns. In addition, the gas flow within the process and the purification methods used for cleaning the flue gas, which differ depending on the operation, both influence the mercury characteristics. Due to these various influences, the ratio between Hg⁰ and Hg⁺ changes continuously and therefore it cannot be reliably predicted. For this reason, measurement is vital.

There are many different detection methods available on the market. These range from offline laboratory analysis through to continuous measurement analyzers, which work on **spectroscopic principles and are only able to detect Hg⁰**.

This means that a highly-efficient, reliable method of converting Hg⁺ to Hg⁰ is required in order to derive the measured values. This conversion process can be achieved with various methods.

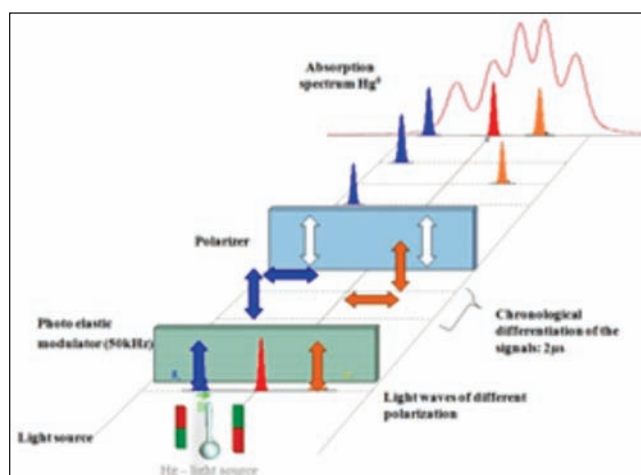
On the one hand, **liquid chemicals** can be used. However, this increases the operating expenditure and costs. Another option is to use a solid matter converter. The disadvantage here is the risk of contamination as a result of sulfur and chlorine compounds, which may be present in the flue gas. This results in higher operating costs due to the shortened operational lifetime of the converter and low measured values due to a reduced conversion rate.

The third method for Hg conversion is based on a purely thermal process. At temperatures of approximately 900 °C, all Hg compounds can be reliably converted back into their elementary form. In doing so, the application of chemical and solid

converters is intentionally dispensed. With the help of this purely thermal method it is possible to achieve a long service life with simultaneously low operating costs.

Measure and monitor mercury: with MERCEM300Z

A fast, reliable mercury analyzer which can monitor both elementary as well as oxidized mercury vastly simplifies the continuous monitoring process. The MERCEM300Z mercury measuring system from SICK provides extremely reliable monitoring of Hg emissions in flue gases down to the lowest certified measuring range of 0 to 10 µg/m³. This represents a concentration considerably lower than the generally accepted emission concentrations of SO₂, NO_x or dust. This measurement quality together with a unique certified maintenance interval of three months makes MERCEM300Z an outstanding mercury analyzer system.



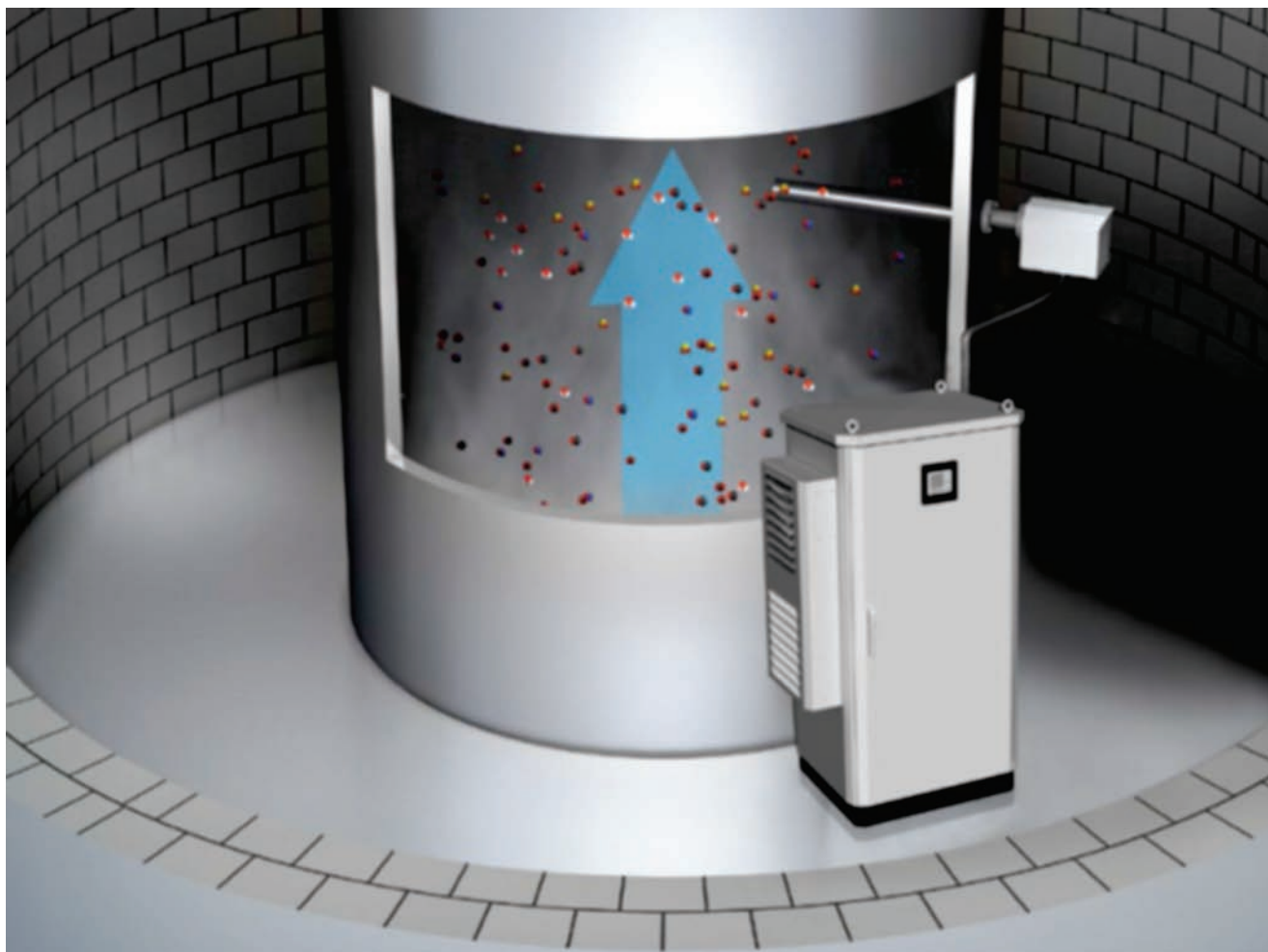
MERCEM300Z: characterized by patented direct measurement.

There is no point in trying to re-invent the wheel. For this reason, SICK made use of Nobel Prize winner Pieter Zeemann's achievement by adapting his atom absorption spectroscopy methods for use in the MERCEM300Z mercury analyzer. This innovative measuring system combines thermal conversion at high temperatures with Zeemann- AAS analysis in a unique, compact,

user-friendly analyzer. Hg-measurement directly in the hot cell is patented and has been approved exclusively for the MERCEM300Z from SICK. The direct measurement system immediately detects even minute Hg concentrations in the hot converter. All in all, the thermal conversion at temperatures of around 1000 °C and the detection of Hg immediately after conversion in the undiluted sample ensures extremely precise results at simultaneously low costs.

MERCEM300Z: impressive even prior to the measurement. Sometimes it is the little extras in life which provide the decisive impetus. MERCEM300Z offers a whole host of convincing arguments up front, which make this measuring device the clear choice:

1. **No carry-over effects** No solid converter and no gas cooling are required – both often falsify results. MERCEM300Z measures and converts all-in-one. Mercury is measured directly where it is converted, resulting in no carry-over effects.
2. **No influence of cross-sensitivities** The MERCEM300Z is resistant to interference components such as SO₂. If changes occur in the gas composition, this is compensated for in the analysis process by the Zeemann effect.
3. **Stress-free testing** It's good to hear that the device has passed several comparative tests in various power plants, incineration plants and cement kilns with flying colors. These include



standard RATA tests based on EPA method 30b in the USA and the DIN EN 13211/VDI method 4200 in Europe.

In all cases, the results were within the required levels of accuracy for the tests. In some tests, the AAS mercury analyzer MERCEM300Z was deployed in parallel with devices developed by other manufacturers, including those with liquid-chemical conversion and subsequent amalgamation, 2-beam AAS analyzers with catalytic conversion and atomic fluorescence analyzers based on the principle of dry conversion and sample dilution. It was determined that the combination of purely thermal conversion at high temperatures and the Zeemann AAS method used by the MERCEM300Z was the least affected by changes in plant operation, which is known to influence the Hg⁰/Hg⁺ ratio in flue gases. Comparisons have shown that the MERCEM300Z also exhibits excellent conversion rates. The proven accuracy of MERCEM300Z and its rapid response times serves to confirm its suitability for efficient measurement of process changes which could affect mercury emissions. Likewise, it has also been shown that MERCEM300Z is subject to minimal maintenance and service requirements. The running times for all test installations confirmed a continuous operation of more than 4 months, without any maintenance requirement. Even in the lowest measured range of 0 to 10 ug/ m³, the analyzer exhibited exceptional performance in the field

Summary

System operators are coming to the realization that mercury limit values are only going to get lower. As a result, they need to adapt their measuring equipment accordingly.

Certified to EN 15267, the MERCEM300Z is the only system suitable for use in such stringent

requirements.

It is even able to monitor mercury with precision in the smallest range from 0 to 10µg/m³. What's more, maintenance requirements are very low. The innovative and future-fit nature of this measuring technology is currently unrivalled.

CV INFORMATION

Name: VIJAY NAIR

Work Experience: Has been in Process Analytical field for more than 2 decades,

Engineer by profession, holds a Bachelor of Engineering (Industrial Electronics) degree from Pune University.

Started his career as a Service Engineer at Chemtrols, he moved into Engineering & Design followed by Production and System Integration, is now working as Marketing Head (Analytics Business unit) in Chemtrols which is one of the biggest in Process Analytical field in INDIA.

Has been associated with major Process Analyzer companies worldwide over these last years. Has rich experience in the field of Process Analytics in various Refining and Petrochemical processes because of the association of these foreign OEMs.

Application knowledge of how and why the process analysis is benefitting the process has been a key interest!

Backed by the life of service engineer earlier, the eye for technical aspects has been always there.

Present job profile involves extensive travelling including abroad, strategic planning for project positioning, interactions with Foreign principals,

Support to Global group.

Has experience on process analyzers from Moisture and Gas analyzers, Mass Spectrometer, Gas Chromatograph, Laser analyzers, Blending analyzers and Sulfur Recovery analyzers.

Has worked with Process, Stack analyzers and Gas chromatographs with all possible technologies.

Widely travelled across the world, has attended overseas trainings at Panametrics Ireland, General Monitors, Ireland, Thermofisher Scientific, Houston USA, Ametek Process Analytical, Delaware, Siemens Applied Automation Inc, OK, USA, Siemens Germany, Sensitron Italy, Optek Germany, Flexim Germany, PAC Netherlands, SICK Germany, AMS Germany.

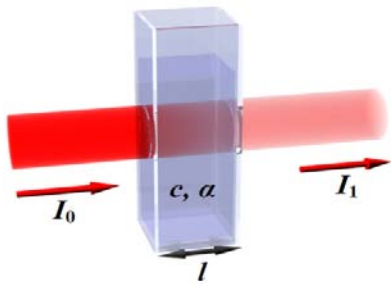
“Use of Advanced Optical Technologies (TDL and Raman Effect) for Gas Phase measurements in Refineries and Petrochemicals Industries.”

Rapid advances in the field of Lasers, signal processing and computation techniques has brought new Optical measurement techniques for Petrochemical industry. In this paper we present TDLAS , Raman Effect based on line analysers and Quench Fluorescence based Oxygen analysers.

Tunable Diode Laser Absorption Spectroscopy for Trace gas measurements.

Currently India has more than 13000 kms of Natural Gas pipelines transporting vast quantities of natural gas across the country. Natural Gas which is being transported through these pipelines many a times has a high moisture content and also the presence of H₂S , CO₂ , O₂ and other contaminants. Presence of these gases along with moisture is a potential recipe for disaster, and world has seen many tragic examples of pipeline explosions / fires . Many of these accidents are reported to have been happened because of corrosion of the pipelines due to presence of these acidic gases and moisture.

Reliable measurement of these therefore becomes imperative and historically many technologies have been used for these measurements. Al₂O₃ based probes for moisture, and Lead Acetate tapes for H₂S are well known. But due to limitations of these prevalent technologies , new technologies like Tunable diode laser (TDL) absorption spectroscopy (TDLAS) based gas analysis and trace gas analysis have rapidly grown in various applications, in recent years.



Concept of Beer-Lambert's Law

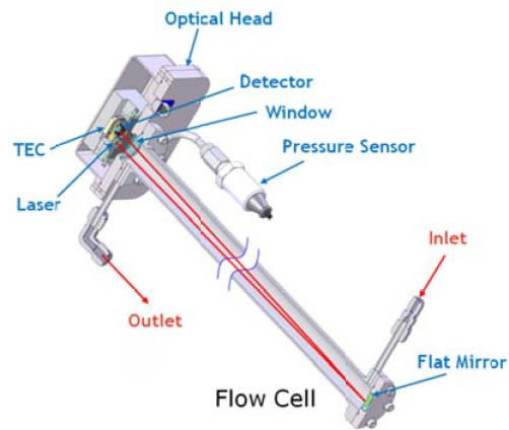


Fig: 1;

Fig.2 : A Complete TDL cell

TDLAS is based on Beer-Lambert's law Fig:1, which correlates the ratio of transmitted intensity (I_1) over incident laser intensity (I_0) to target molecule's concentration (C), optical path length (l), and the characteristics of the absorption transition (α). Wavelength modulated spectroscopy (WMS) and a $2f$ signal is preferred for practical industrial use because it provides relatively high sensitivity with relatively short path lengths.

In high concentration measurements, the $2f$ spectra alone would be sufficient to show a distinct peak where the target molecule is present. However, when measuring 1 ppmv or 10 ppmv H_2S in natural gas, a differential scheme is used, where, by selectively removing measured molecule from the process stream through a scrubbing medium, target molecule's absorption spectra is isolated from the background spectra.

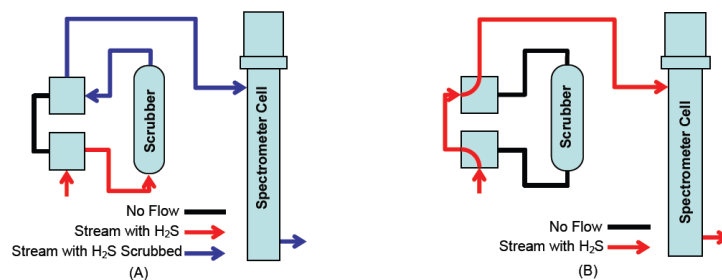


Fig. 3 Differential spectroscopy: (a) scrubbing cycle; (b) Live measurement cycle

Typical applications of TDLAS in Hydrocarbon Industry include:

- i) H₂O, H₂S and CO₂ in Natural Gas and Gas Processing including pipelines
- ii) H₂O, H₂S, CO₂, Acetylene and Ammonia in Refining and Petrochemicals
- iii) Moisture, H₂S and CO₂ in LNG.
- iv) Speciality and Bulk Gases.

Raman Spectroscopy and In-situ Raman analyser.

When a beam of light impinges upon a sample, photons are absorbed by the material and scattered. A tiny portion of the scattered photons are shifted to a different wavelength. **These wavelength shifted photons are called Raman scatter.** Most of the Raman scattered photons are shifted to longer wavelengths (Stokes shift), but a small portion are also shifted to shorter wavelengths (anti-Stokes shift). Figure 4 shows a diagram of Rayleigh scattering, Stokes Raman scattering, and anti-Stokes Raman scattering. These energy transitions arise from molecular vibrations. Because these **vibrations involve identifiable functional groups, when the energies of these transitions are plotted as a spectrum, they can be used to identify the molecule.**

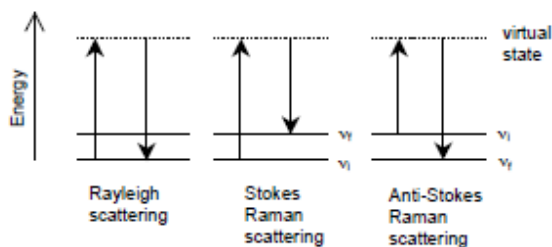


Fig. 4. Energy-level diagrams of Rayleigh scattering, Stokes Raman scattering, and anti-Stokes Raman scattering.

On Line Raman Analysers

These analysers represent an on line approach for taking Raman analysers on-line. This is a Laser based analysis system coupled via an optical fiber to a process. Sampling interface is integrated with the optical probe which is the analysis sensor. A typical Raman analyser is made up of a laser, a collection device, a spectrograph and the Fiber Optic cable

Laser: A laser is used to excite Raman spectra because it gives a coherent beam of monochromatic light. This gives sufficient intensity to produce a useful amount of Raman scatter and allows for clean spectra.

Probe: The probe is a collection device that collects the scattered photons, and sends the Raman scatter to the spectrograph.

Spectrograph: When Raman scattered photons enter the spectrograph, they are passed through a transmission grating to separate them by wavelength and passed to a detector, which records the intensity of the Raman signal at each wavelength. This data is plotted as the Raman spectrum. Fig. 5 provides an overview of the on line in-situ Analysis Model of Raman analysis.

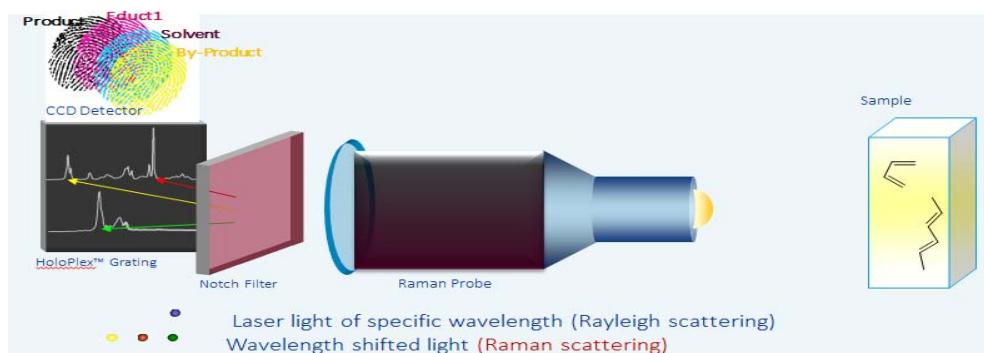


Fig. 5: On line, in-situ Raman analyser schematic.

A unique feature of this analyser is that unlike any other spectroscopy, it can measure the di-atomics H₂ and N₂.

Fig. 6 is the Optogram of a full component slate of Raw Syngas after the carbon scrubber of a Petcoke Gasifier (this stream includes moisture vapour). Optogram looks like a chromatogram and in fact, the Optogram is interpreted and analyzed the same as a chromatogram. Optogram is transparent to moisture in the frequency range that is shown. By normalizing the analysis, the equivalent of a “dry” analysis is provided without having to have a bone dry sample, which is a typical need of GCs and Mass Spectrographs

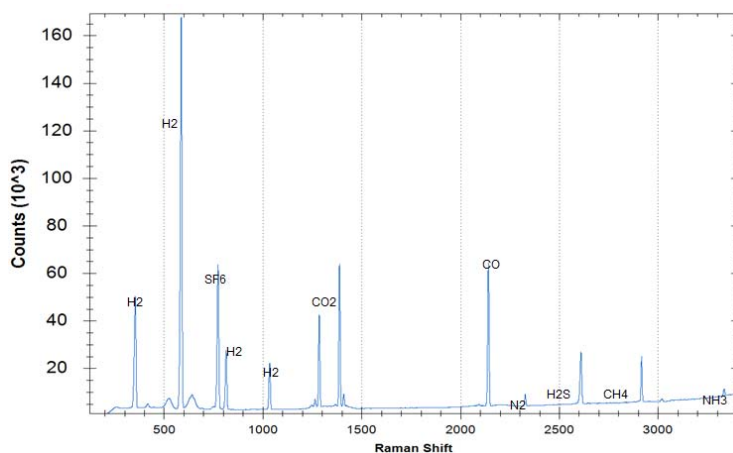


Figure 6: Optogram of Raw SynGas after Carbon scrubber

Some Typical applications for an On line Raman Analyser.

Gasifiers,

Natural Gas to Burners (BTU), Syngas from Primary Reformer,

HT/ LT Shift Converter Outlet / Inlet, Feed to Synthesis Loop (H₂/N₂ Ratio),

Synthesis Loop Recycle Gas and Purge gas,

Oxygen Measurement : Quench Fluorescence

The principle of measurement is based on the effect of dynamic luminescence quenching by molecular oxygen. The following scheme explains the principle of dynamic luminescence quenching by oxygen. Principle of dynamic quenching of luminescence by molecular oxygen (refer to Figure 7):

- Luminescence process in absence of oxygen (1)
- Deactivation of the luminescent indicator molecule by molecular oxygen (2)

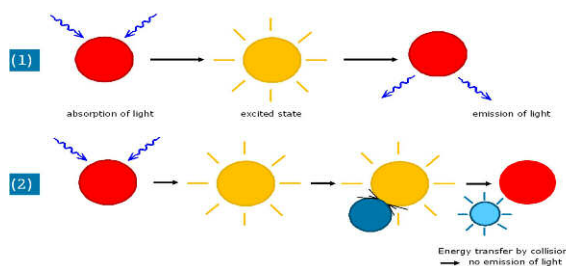


Figure 7 Quench Fluorescence (QF) principle

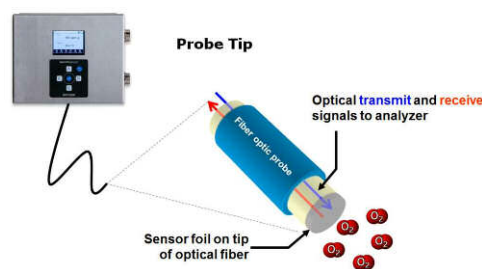


Fig.8 QF based O2 analyser

The collision between the oxygen-sensitive material in its excited state and the quencher (oxygen) results in radiation-less deactivation and is called collisional or dynamic quenching. After collision, energy transfer takes place from the excited indicator molecule to oxygen which consequently is transferred from its ground state (triplet state) to its excited singlet state. As a result, the indicator molecule does not emit luminescence and the measurable luminescence signal decreases.

Applications:

Natural Gas applications like production , Vapour Recovery units, Storage Caverns, etc.

Conclusion:

These technologies provides significant advantages for certain measurements over other technologies in Hydrocarbon Backgrounds. Significant ones include :

- i) Use of long life solid state lasers
- ii) superior sensitivity and repeatability,
- iii) fast response times,
- iv) long-term reliability in harsh conditions, no retention or wet-up/dry-down delays.
- v) Low cost of ownership

With Inputs from:

- Kaiser Optical Systems Technical note 1101.
- Various other Kaiser and Spectrasensors Publications
- Pictures courtesy: Spectrasensors and Kaiser Optical



(Jiwan Jain is Graduate in Electrical Engineering and has more than 24 years of experience in the field of Gas and Liquid Analysesrs. Currently Working with Endress+Hauser as GM- Solutions.)



Setting the Standard for Automation™

PPA MEET 2016

8TH April-9TH April 2015

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

The International Society of Automation Delhi Section

Design and Implementation

- ESD Philosophy
- PLC Configuration and SIL Requirement
- Interface of ESD and BPCS
- Input/ output list
- Detail specification and Procurement
- System Engineering
- Factory Acceptance Test
- Site Testing and Acceptance

Design and Implementation

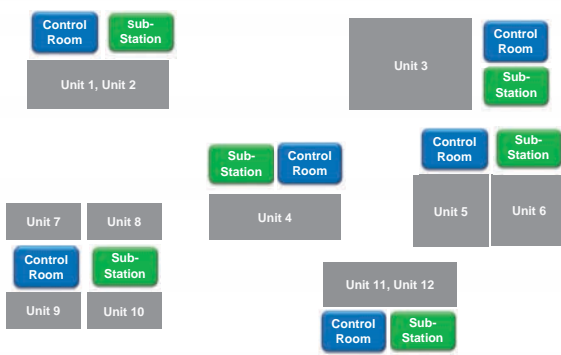
- ESD Philosophy
- PLC Configuration and SIL Requirement
- Interface of ESD and BPCS
- Input/ output list
- Detail specification and Procurement
- System Engineering
- Factory Acceptance Test
- Site Testing and Acceptance

ESD Philosophy

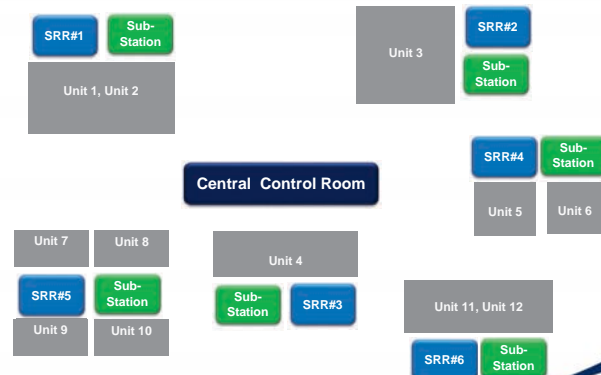
- Geographical location of plants/ units and ESD systems
- Grouping of ESD systems
- Plant equipments ESD philosophy



Plant with multiple Control Rooms




CCR with satellite rack rooms



Grouping of ESD systems

Benefits of Combining




Benefits of Standalone

Optimizing ESD capability vis-à-vis operational segregation

- ❑ Location of plants/ units
- ❑ Size of ESD I/Os of each plant
- ❑ Plants operational, start-up and shutdown philosophy
- ❑ Economic consideration

Equipments ESD Philosophy

- ❑ Integrated with main plant ESD system
 - Advantage: Inventory, maintenance, training
- ❑ Dedicated OEM supplied ESD system
 - Complexity of logic
 - Proprietary nature
 - OEM's standardization
 - Project schedule optimization

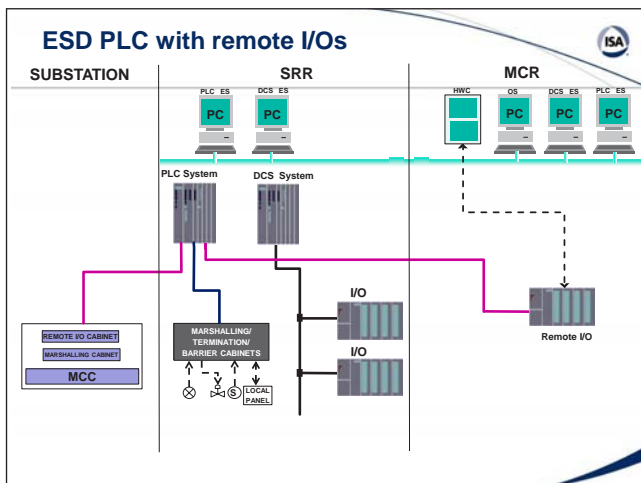
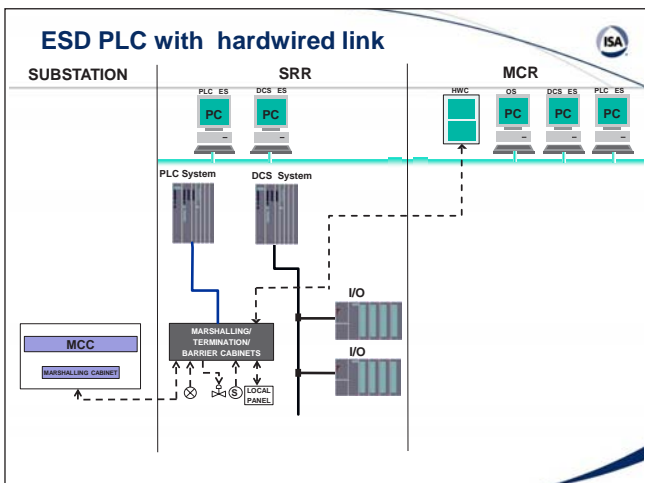



Design and Implementation

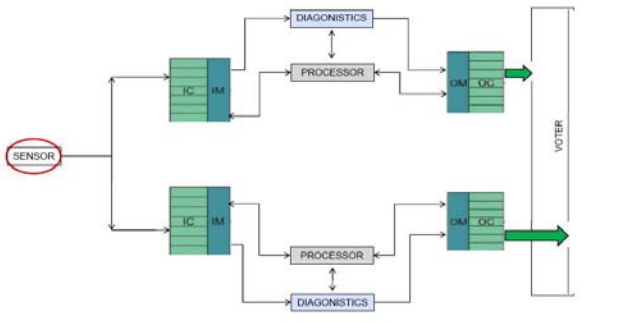
- ESD Philosophy
- PLC Configuration and SIL Requirement
- Interface of ESD and BPCS
- Input/ output list
- Detail specification and Procurement
- System Engineering
- Factory Acceptance Test
- Site Testing and Acceptance

PLC Configuration and SIL requirement

- ❑ ESD system – SIL or no SIL?
 - SIL PLC is default choice in process plants. Non SIL can be used in less critical plants.
- ❑ Segregation of safety and operational interlocks
- ❑ Connection of hard wired console and substation I/Os
- ❑ Peer to peer communication
- ❑ PLC configuration
 - DMR
 - TMR
 - Quad

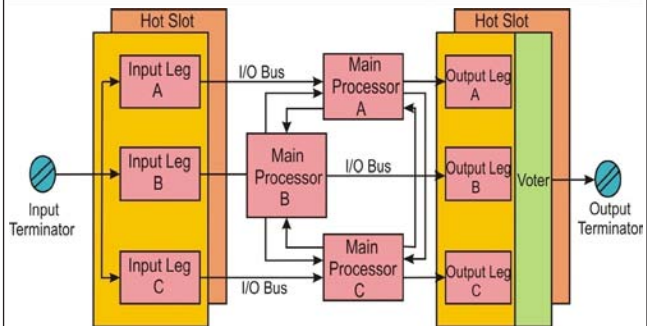


Typical Configuration – DMR PLC



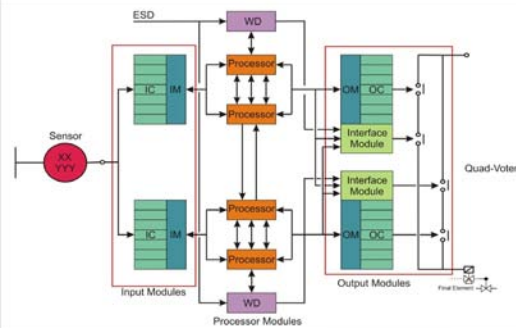
During normal operation both channels need to agree to execute the shutdown action. During failure of one, healthy channel controls the system

Typical Configuration – TMR PLC



Agreement of two channels is required to execute a shutdown. The output is not changed by disagreement from only one channel.

Typical Configuration – Quad PLC



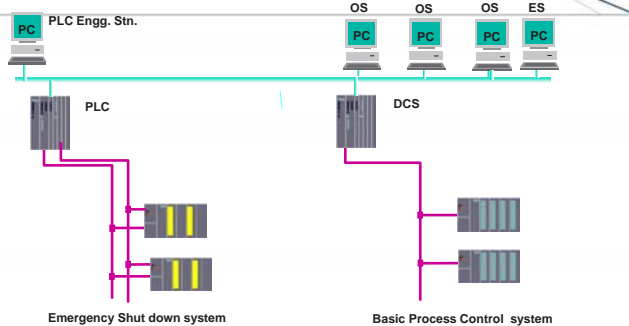
Dual I/O module with dual central module. Each central module with dual processor and in case of failure of one central module, secondary de-energisation of output cards by other central module.

Design and Implementation



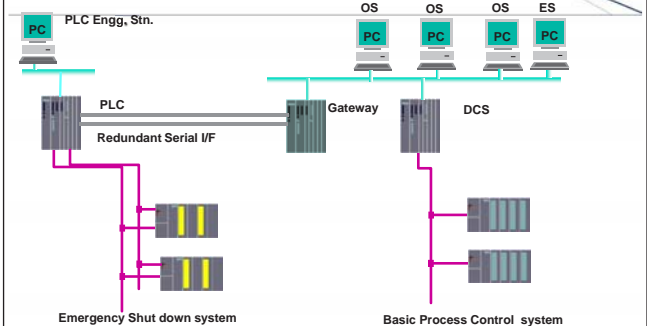
- ESD Philosophy
- PLC Configuration and SIL Requirement
- Interface of ESD and BPCS
- Input/ output list
- Detail specification and Procurement
- System Engineering
- Factory Acceptance Test
- Site Testing and Acceptance

Interface with Process Control System

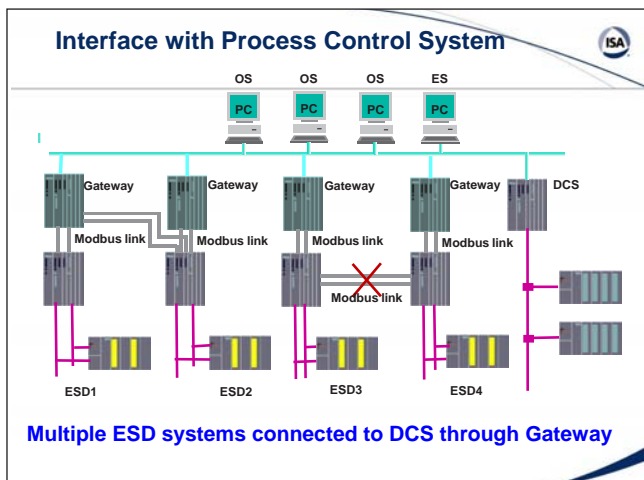


PLC directly connected to DCS Communication Bus

Interface with Process Control System



PLC connected to DCS through serial communication



Serial Communication between ESD and BPCS

- Where gateway is used:
 - Not to be shared with BPCS I/Os.
 - Dedicated or combined for some ESD systems.
-
- Direction of Serial Communication: Bidirectional

Design and Implementation

- ESD Philosophy
- PLC Configuration and SIL Requirement
- Interface of ESD and BPCS
- Input/ output list
- Detail specification and Procurement
- System Engineering
- Factory Acceptance Test
- Site Testing and Acceptance

ESD I/O Summary for Refinery (Typical)

UNITS IN REFINERY PROJECT													
	CDU/VDU	HGU	VGO-HDT	DHDT	PPU	DCU	LPG/FUEL GAS, TREATER, MEROX	FCC-PC & PRU	UTILITY & OFFSITE	NHT-ISO	CCR-HEXANE	SRU	Total I/Os
Analog Input	135	180	280	270	260	260	70	230	120	190	255	240	2490
Digital Input	250	320	330	400	295	365	125	325	185	370	385	450	3900
Digital Output	285	365	320	310	275	380	110	295	280	390	350	440	3790
Total I/Os	670	855	930	980	830	1005	305	850	585	950	990	1130	10080

Total ESD I/O count 10080

ESD I/O Summary for Petrochemical (Typical)

UNITS IN PETROCHEMICAL PROJECT													
	GSU	C2+	ECU SS-1	ECU SS-2	PGH	C4/C5	SCTP	PP SS-1	PP SS-2	PE SS-1	PE SS-2	U&O	Total I/Os
Analog Input	60	370	340	100	20	120	40	130	50	360	40	360	1990
Digital Input	90	450	1050	300	40	60	80	225	125	540	100	390	3445
Digital Output	95	430	650	280	55	50	70	290	130	600	140	540	3330
Total I/Os	245	1250	2040	680	115	230	190	645	305	1500	280	1290	8770

Total ESD I/O count 8770

Design and Implementation

- ESD Philosophy
- PLC Configuration and SIL Requirement
- Interface of ESD and BPCS
- Input/ output list
- Detail specification and Procurement
- System Engineering
- Factory Acceptance Test
- Site Testing and Acceptance

Detail Specification and Procurement



- ❑ Power supply distribution philosophy
- ❑ Process specific requirements, if any
- ❑ Selection of auxiliary like relays and barriers
- ❑ Whether to buy ESD PLC separately or with Basic Process Control System
- ❑ Reducing variations in PLC make for dedicated ESD system of Equipments
- ❑ Synchronizing procurement cycle with various units/ equipments schedules.
Delivery can be phased as per schedule and different units readiness.



Design and Implementation



- ESD Philosophy
- PLC Configuration and SIL Requirement
- Interface of ESD and BPCS
- Input/ output list
- Detail specification and Procurement
- System Engineering
- Factory Acceptance Test
- Site Testing and Acceptance

ESD System Engineering



- ❑ System engineering of various units, which can be from different process technologies
 - Logic diagram/ Ladder diagram/ C&E/ Structured Text
 - Standardize loop drawings/ connectivity
 - Standardize MCC Interface for LT Motors and HT Motors
 - Standardize Maintenance Override Switches, bypass switches
- ❑ Defining responsibilities of all stake holders like Basic Designer, OEMs, Engineering Company, EPCC contractors, ESD suppliers
- ❑ I/O Assignment philosophy



Design and Implementation



- ESD Philosophy
- PLC Configuration and SIL Requirement
- Interface of ESD and BPCS
- Input/ output list
- Detail specification and Procurement
- System Engineering
- Factory Acceptance Test
- Site Testing and Acceptance

Factory Acceptance Test



- ❑ Complete System Configuration Loading
- ❑ Hardware testing/ redundancy check
- ❑ Complete logic checking at FAT with simulation
- ❑ Checking of operation from different Engg. Stations
- ❑ Checking of Remote I/O link/ Peer to peer communication
- ❑ Scheduling FAT of different units as per project schedule and respective units engineering progress
- ❑ Participation of all stake holders: Basic Process Designers, End User, DEC, EPCC contractors, major equipments OEMs
- ❑ Review of Burn-in Test Reports of Pre-FAT
- ❑ Documentation and change management



Design and Implementation



- ESD Philosophy
- PLC Configuration and SIL Requirement
- Interface of ESD and BPCS
- Input/ output list
- Detail specification and Procurement
- System Engineering
- Factory Acceptance Test
- Site Testing and Acceptance

Site Testing and Acceptance



- ❑ Checking by Basic Process Designers, Equipment suppliers, Operation & Commissioning team
- ❑ End to end logic checking
- ❑ Checking of Changeover of Redundant Devices and Components
- ❑ Reporting of System Diagnostic messages during failures
- ❑ Final Documentation
- ❑ Logistic Support and Technical assistance



Design and Implementation



- ESD Philosophy
- PLC Configuration and SIL Requirement
- Interface of ESD and BPCS
- Input/ output list
- Detail specification and Procurement
- System Engineering
- Factory Acceptance Test
- Site Testing and Acceptance




FORBES MARSHALL

Remote Vibration Monitoring System

New technology

24 X 7 Machine surveillance



Proprietary content

FORBES MARSHALL

Shinkawa Philosophy

**Contribution to the society
with created new value**



- High Quality
- High Reliability
- Flexibility
- Satisfied After-Sales Service

FORBES MARSHALL

Forbes Marshall Today...

Our new campus has been set up on 50 acres of land at Chakan MIDC under the Mega Project Scheme of Government of Maharashtra. The campus has won three awards :

- Indian Institute Of Architects Award For Excellence In Architecture (Industrial Category)
- Builders Association Of India (Pune Chapter) Award for Well Built Structure
- Artists in Concrete Awards – Asia Fest 2014-15





FORBES MARSHALL

RVMS Concept ...

- Time of Analyst is very important
- Moving Analysis is really time consuming & expensive
- Analyst can manage corrections looking to the waveforms /FFT & other plots
- Move information to Analyst – not move analyst to information

FORBES MARSHALL

Current Trend ...

- Many sites are equipped with complete machine protection systems & on the top of that Condition monitoring software's
- These software's are very expensive & gives expert data which determines machine health
- Analyst plays a very vital role to understand the machines by using these software data
- Availability of Expert at all sites is not possible & also it's time consuming & within same time Expert can add value by looking data of other site
- So if this data available with expert ,he can do better prediction by saving travelling time.

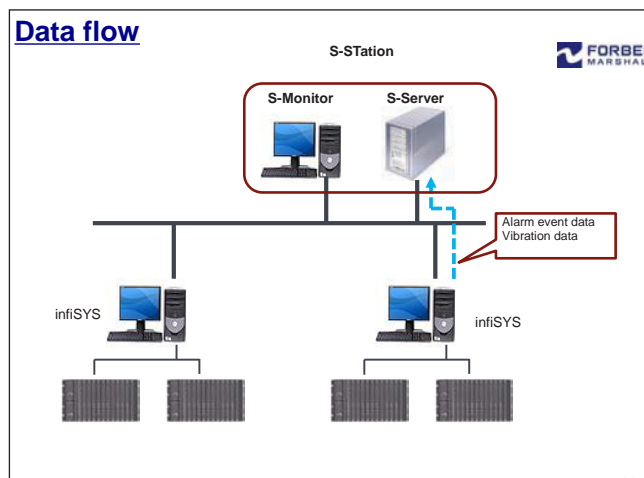
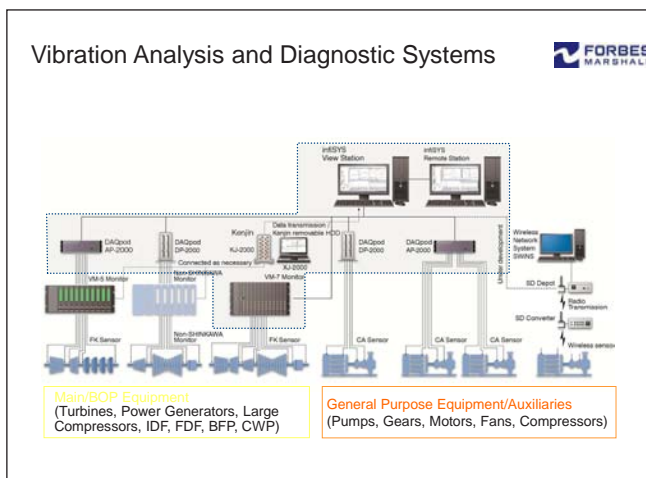
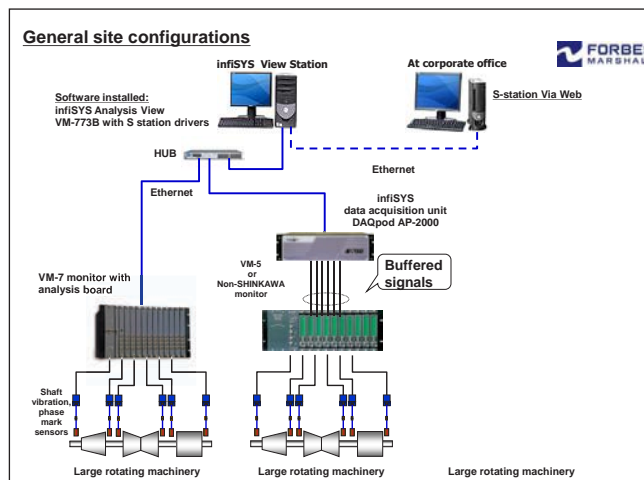
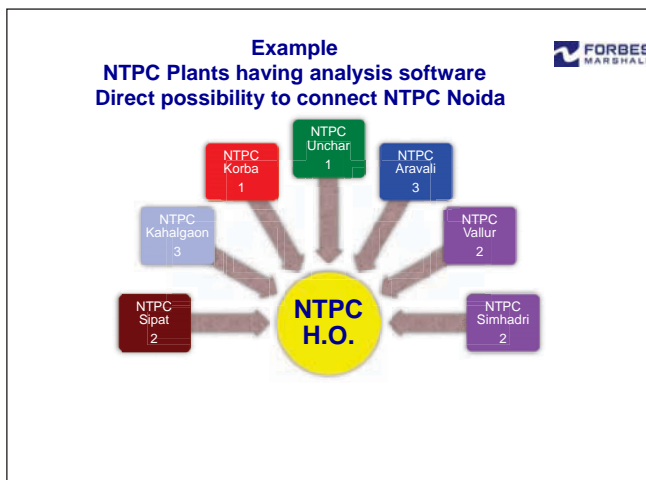
FORBES MARSHALL

Shinkawa Solution...

S- Station

Connection to multiple sites

- Alert based Monitoring system, Hence not required to look system always .In-fact system will give you alert when there is issue with any rotating machine ,remember system works 24X7 & keep watching machines continuously.
 - It engage analyst only at the crucial time



Main Features

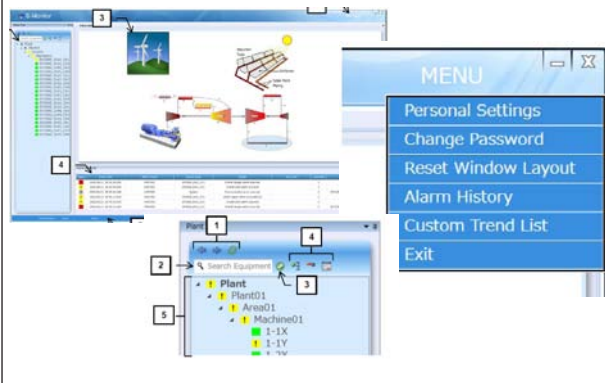
- Scalability**
 - Up to 30 infiSYS in one S-Station (>12,000 sensor channels)
 - Up to 10 S-Stations accessible via G-Monitor
- Alarm focused**
 - Only alarm & event information are stored in S-Station
 - Vibration data & trend data are stored in each infiSYS
- Realtime view of infiSYS vibration data and OPC process values**
- Simple means for remote accessing infiSYS**
- Cross infiSYS/S-Station data trend capability for easier vibration diagnosis**

Main Screen

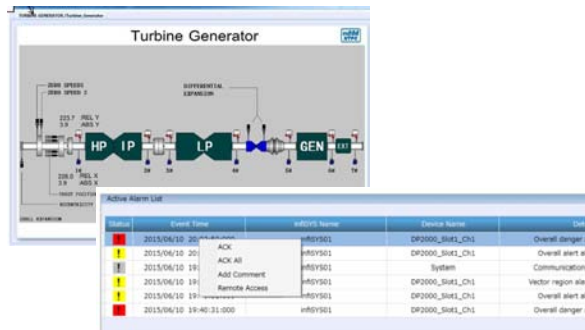
The main screens of this product are as follows:

Function Classification	Screen
Alarm Monitoring	Main window
	Alarm Detail window
	Alarm History window
Trend display	Trend Property window
	Custom Trend List
	Trend View
	Trend Tile View
Remote control	Remote Access screen
Others	Personal Settings window
	Chart Property window
	Change Password window

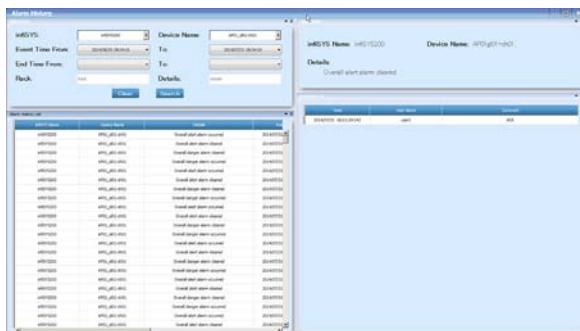
Easy Menu



Mimic creation & Alarm History

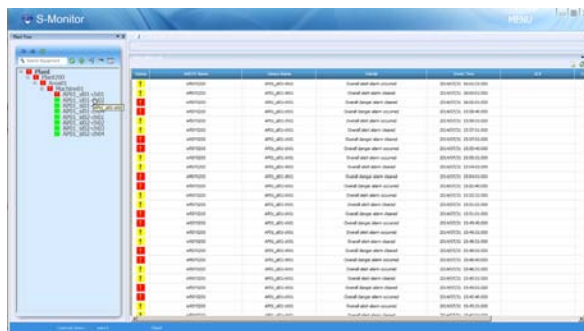


S-Monitor screen sample Historic alarm list



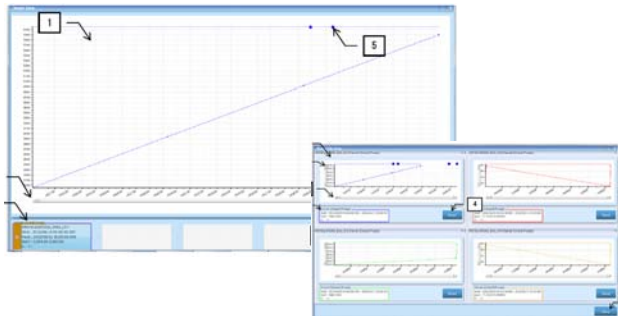
SSTB

S-Monitor screen sample GUI, Device tree list and active alarm list

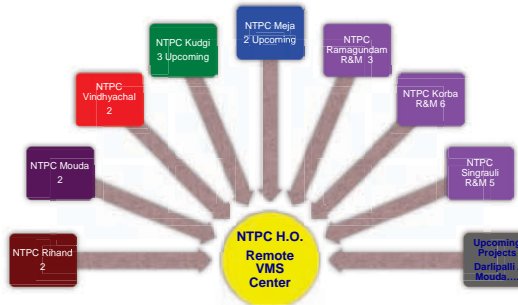


SSTB

Trend View



One Solution For multiple Plant sites Connecting All



TOPIC: Modern age approach to Fire & Gas System

INTRODUCTION:

In most of the countries it is observed now that productivity from traditional land-based installations is getting declined & attention is switching to other unconventional sources, such as heavy crude oil, oil sands, and oil shale and offshore

Customers are keen on relooking into various modes of Investment that would eventually optimize the Utility to cost ratio.

Fire and Gas Application is hence not a subject that can easily escape such turmoil as well in the same industry

Fire and Gas Detection systems are key components in the overall safety and operation of any production facility and its on-site personnel. These facilities have had serious safety problems over the years

When we look at Fire and Gas Application some of the most common “Customer Need” found in the Industry today are:

- Be able to be modified without disrupting production processes and/or removing existing levels of protection”
- Fire & Gas Detection System would act as an autonomous local protection system. Several such local systems could be distributed around a site/platform, all of which would be addressable and controllable from a unit”
- “Need Reliable FGS system, in terms of not raising false alarms and erroneously triggering a disruptive and costly ESD”
- “Be more responsive, in terms of reacting in near real-time (as delaying an ESD by even a fraction

of a second can make a huge difference”

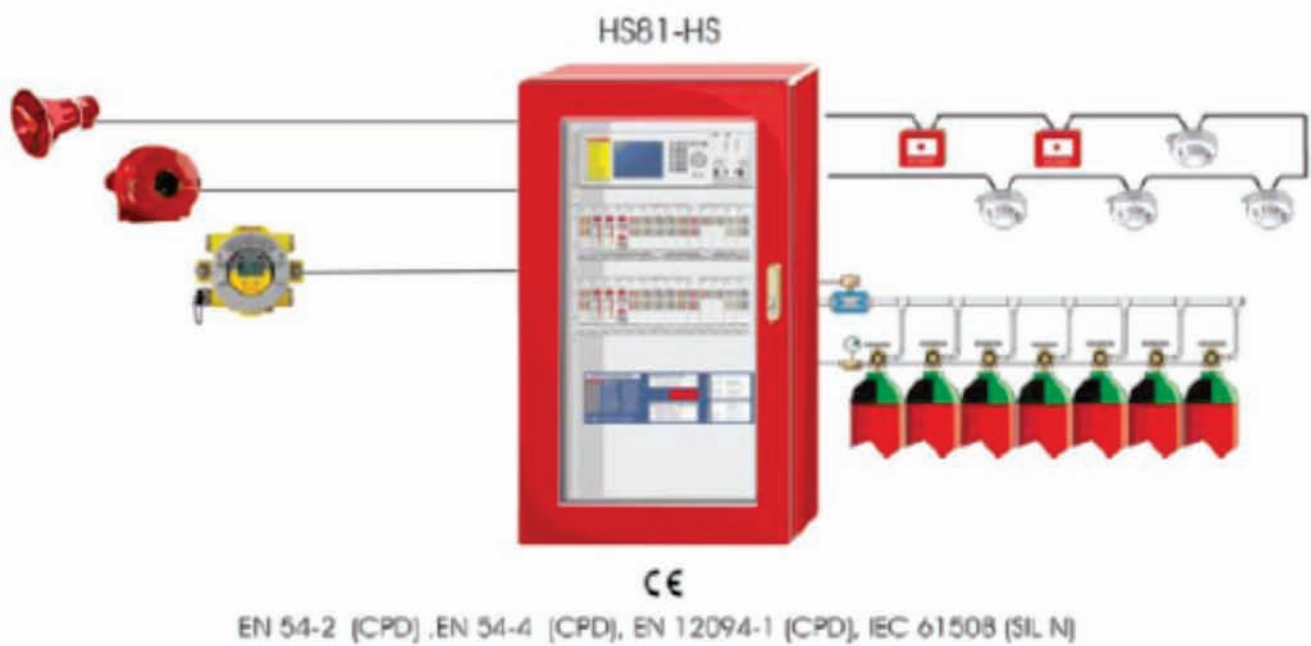
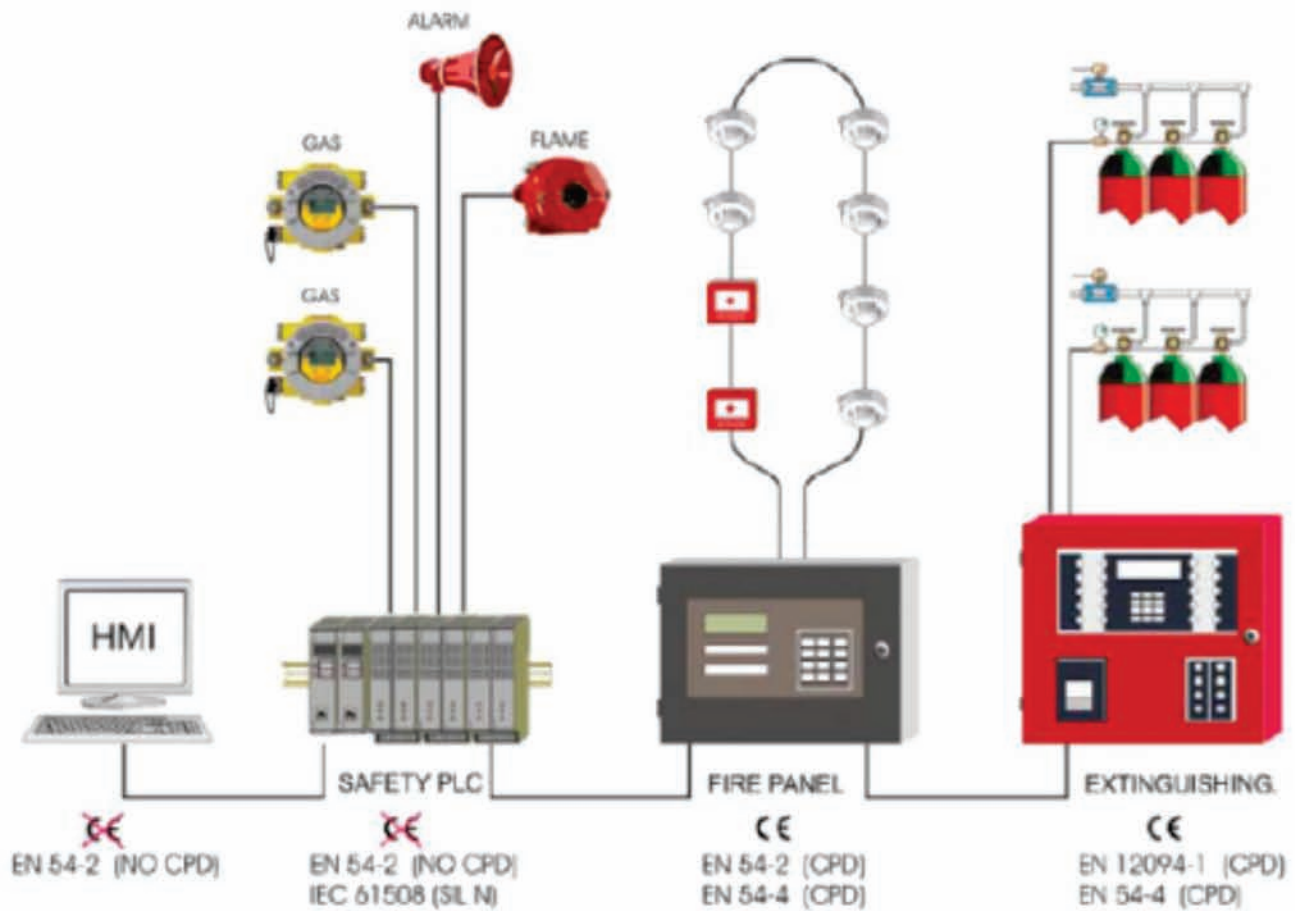
- “Where space is luxury FGS Panel should Compact & Wall mountable and operator accessible at any point of time
- System would have proper assessment done before being used for certain specific application like Offshore where higher IP rating in addition of anti-corrosive conformal type coating would be important

Performance requirement is very critical for Process Areas than Prescriptive Codes:

Fire and Gas Detection and Mitigation Systems are key components in the overall safety and operation of any production facility and its on-site personnel. However, in many instances the overall importance of these systems has not been fully comprehended. Applicable national standards (eg :NFPA 72) are typically prescriptive and do not address process areas. In many cases they have been implemented using the DCS (Distributed Control System), or a COTS PLC (Commercial-Off-The-Shelf Programmable Logic Controller), with too few detectors and alarm devices, and without clearly defined performance goals. This is partly due to the fact that Process Safety Standards did not include F&G Detection and Mitigation Systems. However, it is to the credit of IEC 61511 that it includes both prevention and mitigation systems; F&G being considered under the mitigation aspects of this Standard.

One Header single Window Solution Architecture

One Single Equipment Offering comprehensive one Window complete F&G function play now a key role



towards 100% Mitigation

Some key Trends we see now getting adopted in Mission Critical space where down time is huge running cost :-

- Use of Addressable Loop in the F&G System so that separate Fire Alarm hardware cost is reduced specially in the process area
- Mix of Performance and Prescriptive Design for Fire and Gas system
- Use of F&G System (including Fire Alarm) which should be at least SIL2 in terms of reliability , so that probability of appropriate mitigation would be 99% of time
- One header serving the purpose of both Fire Detection and Automatic releasing system
- Analysis of Data on a HMI or Mobile Application to understand key factor that may result in interruption of process before hand
- Multi-Level redundancy that will ensure fault tolerant system with constant availability

CONCLUSION

Unlike past experience, it is realistic to apply performance-based criteria to Fire and Gas System design and implementation in accordance with the ISA S84.00.01/IEC 61511 Standard. Because of the limitations of current technology, it is unlikely that Fire and Gas Detection Systems in process facilities will achieve a level of performance greater than SIL 1 (RRF between 10 and 100), due to the fact that achievable risk reduction is limited by detection coverage, rather than Safety Availability. However, it is quite possible to achieve a SIL 2 level of performance in enclosed areas using current technology. In any case, employing a performance-

based framework is a major milestone in establishing safety performance requirements for these critical systems.

The work in progress by the S84 WG6 F&G Committee and others worldwide will provide essential guidelines and a consistent framework for the implementation of Fire and Gas Systems in process areas, utilizing a risk based approach as per the ISA S84.00.01/IEC 61511 Standard. This effort is absolutely essential and long overdue. These guidelines will encourage manufacturers to develop better detection technologies to satisfy market demand, thereby improving the safety performance of Fire and Gas Detection and Mitigation Systems in process facilities.

BIOGRAPHY

Mr Arpan Bhattacharya is currently working as APAC Marketing Manager for HONEYWELL Industrial Fire and Security solution with 6 plus years of Experience in handling Fire Mitigation solution business. His primary work involves understanding of Customer key needs & in turn develop Product Road Map and solution to quickly address solution gap in the market today towards Fire and Gas system in Process plants. He is graduate in Mechanical Engineering and did Masters in Business management from Pune University

Cyber Security in COTS

Neeraj Agrawal,
Associate Director (Process Control)

Nuclear Power Corporation of India Limited, Mumbai

Presented in PPA meet 2016, Delhi from April 8th -9th, 2016

OVERVIEW

- What is COTS ?
- Issues of Cyber Security in COTS
- Care during Procurement of COTS
- Precautions during O&M of COTS

What is COTS ?

What is COTS?

- Commercial Off The Shelf (COTS) product
- These are not designed to meet the specific requirements of a customer, rather they are generic in nature



Examples of COTS



DCS
PLC



Numeric Relays



Smart transmitters



Controllers

Examples of COTS



Network switches/
Modems




PC/Display devices
Keyboard/ Mouse




Printers


Hardware as COTS




Processors



ICs




FPGAs




Memory Chips


Software as COTS




Operating System




Database Software




Application Software



Antivirus Software



Development Tools



Testing Tools


Issues of Cyber Security in COTS

Issues of Cyber Security in COTS



Issues in Network Security


- Confidentiality
- Data Integrity
- Access Control
- Timeliness
- Transmission of “infected” files



Issues in Data Security

Major issues

- Database corruption
- Internal data loss
- External hacking – Data Leakage
- Securing data if hardware stolen
- Unapproved Administrator Access



Issues in Software Security

- Buffer Overflow
- Stack Overflow
- Command Injection
- SQL Injections

```

<Variable name="color" description="Title Color" type="color" default="#204063" value="#204063"/>
<Variable name="color" description="Blog Title Color" type="color" default="#4e6f8e" value="#4e6f8e"/>
<Variable name="color" description="Blog Description Color" type="color" default="#4e6f8e" value="#4e6f8e"/>
<Variable name="color" description="Post Title Color" type="color" default="#4777ba" value="#4777ba"/>
<Variable name="color" description="Date Header Color" type="color" default="#81acc8" value="#81acc8"/>
<Variable name="color" description="Sidebar Title Color" type="color" default="#809fb4" value="#809fb4"/>
<Variable name="color" description="Link Color" type="color" default="#809fb4" value="#809fb4"/>
<Variable name="color" description="Visited Link Color" type="color" default="#404040" value="#404040"/>
<Variable name="color" description="Sidebar Link Color" type="color" default="#999999" value="#999999"/>
<Variable name="color" description="Link Color" type="color" default="#809fb4" value="#809fb4"/>
</Variable name="color" description="Visited Link Color" type="color" default="#404040" value="#404040"/>
</Variable name="color" description="Sidebar Link Color" type="color" default="#999999" value="#999999"/>
</Variable name="color" description="Link Color" type="color" default="#809fb4" value="#809fb4"/>
</Variable name="color" description="Visited Link Color" type="color" default="#404040" value="#404040"/>
</Variable name="color" description="Sidebar Link Color" type="color" default="#999999" value="#999999"/>
</Variable name="color" description="Link Color" type="color" default="#809fb4" value="#809fb4"/>

```

Hardware Security?

- Hardware is the last line of defence before damage is done
- Hardware cannot be updated (only wholesale replacement) whereas software can be updated.
- Hardware issues can be injected during Design and Manufacture Only
- Hardware security concerns the entire lifespan of a cyber-physical system
 - ✓ Even after hardware outlives its usefulness, we must dispose of it properly or risk attacks such as theft of the data or software still resident in the hardware

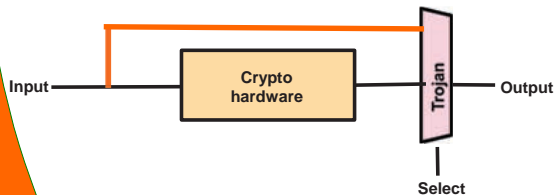
Hardware Security Issues

Trojans
Tempest



HARDWARE TROJANS

- Hardware Trojan is a malicious and deliberately stealth modifications made to an electronic device such as ICs
- It can change the chips functionality and undermine trust in the system using that chip



TEMPEST


- Using these techniques data/ confidential information like pass words etc. can be stolen
 - ✓ Car with remote
- Compromising emissions are defined as unintentional intelligence bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment

TEMPEST

- Spying using leaking emanations e.g.
 - ✓ Electromagnetic Emanations
 - ✓ Sounds
 - ✓ Mechanical Vibrations





Care during Procurement of COTS



Ask following questions



Purpose: How do user knows that unauthorised changes in hardware/software/data has not taken place or data is lost/stolen etc.?

- Whether you as a user has organizational security policy?

Ask following questions

- What Security Standards Vendor/Sub-vendor is following?
 - ✓ NIST
 - ✓ ISO/IEC-27001
 - ✓ Advanced Encryption Standard (AES) NIST 2001
 - ✓ Check what standards are being followed for encryption by Vendor/Sub-Vendor
 - ✓ If no, then whether company (Vendor/Sub-vendor) has its own standards for cyber security
 - ✓ Is equipment TEMPEST approved (NATO SDIP-27- Level A, B, C)?
- Is the answers to questions matches with your organizational security policy?

Ask following questions

- CMM Level qualification
- Verification and Validation Policy of the company
- Configuration management during development
- Version Control policy
- Hardening of Operating System




Software Security

Does the system has following features?

- Good Programming techniques followed
- Anti-Virus Software
- Anti Spyware
- Anti Malware
- Anti-Key logger
- Anti-Subversion Software
- Anti-tamper Software
- Cryptographic Software
- Log Management






Hardware Security

Trojan

- ✓ New testing procedures and tools to detect corrupted chips
- ✓ Inclusion of built-in defences into chips to identify and thwart attacks as they occur.
- ✓ Software checks correctness of its execution by verifying the underlying hardware

Tempest

- ✓ Manufacturing exactly as per the original equipment
- ✓ Changing even a single wire can invalidate the tests.

TEMPEST SECURITY



Following techniques are used in installation to prevent loss of data/information (NATO SDIP-29)

- Amount of shielding in buildings and equipment
- Filters on cables
- Follow Distance, Zoning (AMSG 799B NATO Zoning Procedures) philosophy
 - ✓ Separating wires carrying classified vs. unclassified materials
 - ✓ Following "Red/Black" separation principle
 - ✓ Distance and Shielding between wires/equipment and building pipes
 - ✓ Equipment distance from walls
- Introduce noise to mask the actual data

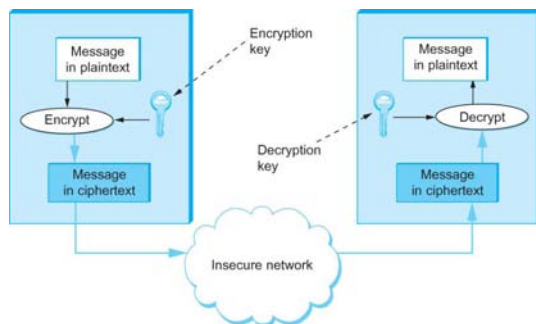
Network Security?



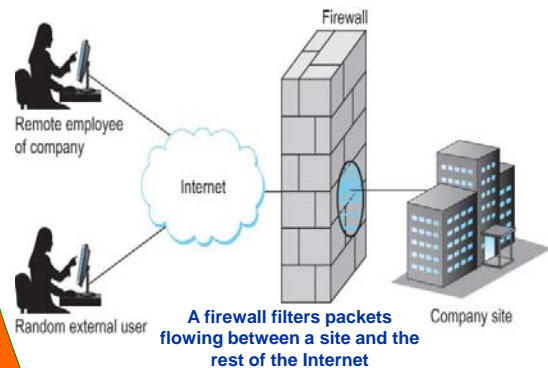
- Maintain Air-Gap
- Is system automatically connects to Internet – Supplier can access your system via internet say for diagnostics etc..
- When systems are connected on internet ensure the following:
 - ✓ Is vendor using secure system e.g. PGP, SSH, IPSec?
 - ✓ Cryptographic Building Blocks
 - ✓ Key Pre Distribution – Different key for each session
 - ✓ Authentication Protocols
 - ✓ Using intrusion detection and prevention
 - ✓ Firewalls – Is its configuration safe?
 - ✓ Network Hardening : Unused network ports in the systems are disabled and locked



Cryptographic Building Blocks



FIREWALL



Data Security



- Is he using 3rd party software for data security
- Data Obfuscation (Masking, Scrambling)
- Encryption of data
- Database intrusion/Extrusion prevention
- Use complex Passwords
- Keep Internal and External facing database separate
- Restrict Downloading- Do not keep data in Excel etc.
- Data leak prevention



Precautions during O&M of COTS



Precautions during O&M of COTS

Access Control

Hardware

- Physical Security
- Biometrics access to the control area
- Panel doors locked and annunciation on door opening
- Passkey (kept with Shift incharge)

Software

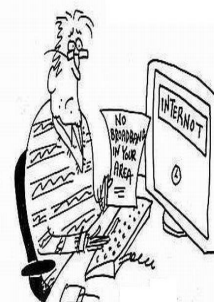
- Role based access (Admin/Maint/Oper)
- Update privileges
- Two level password including biometrics
- Is password changed after supply?
- Detection and alerting Unintended behaviour (security breach annunciated)



Precautions during O&M of COTS

Hardening of devices (Blocking of possible entries)

- Remote access disabled
- Ensure that all connections to Internet (present in instrumentation e.g. smart transmitters) are disabled during commissioning
- Removable media disabled
- Unused ports of network switches disabled
- Patch cords are locked
- No wireless devices in the control area



Precautions during O&M of COTS

- Configuration Management Plan (O&M)
- Uninstall unnecessary software
- Backups of software and important data
- Updates/Security Patch
 - Latest security patch up-dation only if it addresses the security issue(s) present in the running system.
- Maintain Air Gap
 - Have separate plant wide network from Internet. There shall be no connection between the two networks.
 - Segmentation
 - If at all any connection is there, it shall be intermittent and shall be isolated from internet via firewalls
- Recovery procedures

Precautions during O&M of COTS

- Security Audit and testing at regular intervals
 - Vulnerability scanning
 - Penetration Testing
 - Data integrity scanning
 - Malware Detection
 - Network scanning
- Regular Training and Security awareness program
- Sanitization before disposal of Media



CONCLUSION

- The only system which is fully secure is the one which is unplugged and switched off
- Only way to be safe is pay attention and Act Smart



Thank You

Fundamentals of Wireless technologies

By – Vivek Roy, Siemens Limited

General properties of radio networks

Cables compared to radio waves

The use of cables and lines for communication has certain advantages since an exclusive medium is available: the transmission characteristics of this medium are well defined and constant (provided that cables, routers or similar components are not replaced) and it is distinctly recognizable at any time which nodes are connected to a “local area network” (abbreviation: “LAN”) and which are not. However, in return the complexity of the cabling (and the possibility of cable breaks and other hardware faults) increases with the number of nodes. The use of wire-bound methods for the communication with freely moving nodes is only feasible in exceptional cases. Radio links additionally enable to bridge zones for which cabling would otherwise be difficult (streets, waters). In these applications, radio-based networks can show their advantages (which, in summary, consist in the fact that they are less tied to a specific location). In these cases, the possibly higher investment costs are compensated by increased customer benefits.

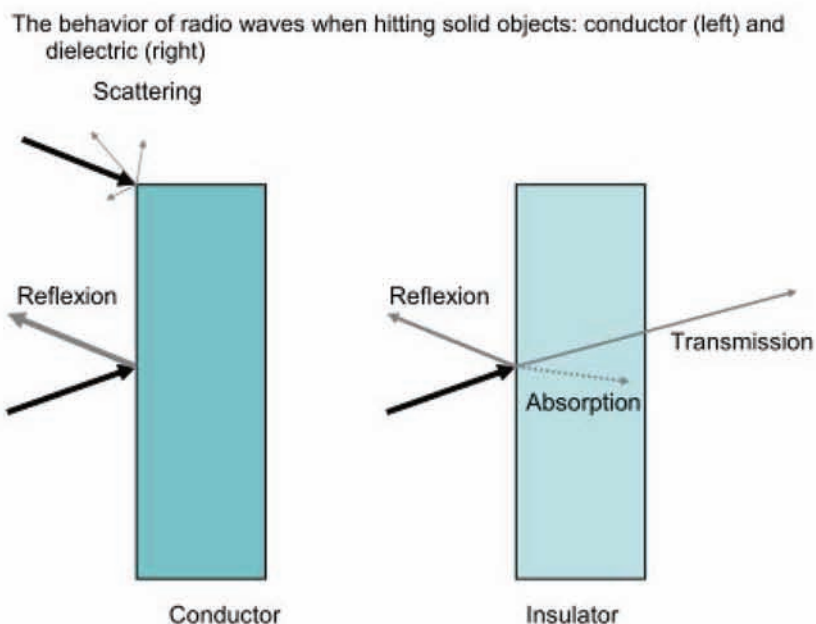
Complexity of the radio field

Radio waves propagate through space, are diffracted at obstacles or attenuated when passing through and thus generate a complex radio field which changes when the obstacles move. It is obvious that the range illuminated by one or several transmitter(s) is not sharply defined. There is no clear delimitation of the radio field which causes a fluctuation of the transmission characteristics for the individual nodes of the radio network depending on their position. In addition, it is practically impossible to discover a “silent listener” in a radio network. These properties have considerable consequences on questions regarding connection reliability and bug proof or interference immunity of a network. Assuming responsible administration, careful planning and the use of trained employees who are sensitized to the specific concerns of a radio network, radio networks are as reliable, secure and robust as wire-bound networks.

The physics of radio waves

Propagation

Unlike signals in a line, radio signals propagate three-dimensionally in space as electromagnetic waves. When the waves hit an object, they are reflected virtually completely if the object is electro conductive. If the object is non-conducting, a part of the waves is reflected, another part is absorbed in the object, and a rest is finally let through the object. When hitting edges, radio waves are scattered into virtually all directions.



Interference and diffraction

Two additional properties are important for the development of the radio field:

- On the one hand, radio waves (unlike incoherent light) can amplify or even extinguish one another (“interference”). If a receiver is located in both, the direct beam and the reflexion of a transmitter, it does not necessarily detect the double signal strength, but it will possibly not detect any signal at all.
- On the other hand, the propagation properties of the waves depend on their wavelength, i.e. high-frequency radio waves behave differently than low-frequency radio waves. In particular, radio waves of long wavelength (i.e. low-frequency) can be “diffracted” around objects. Similar to sound or water waves, it is then possible to receive signals even in the “shadow” of a radio source.

Interference and diffraction phenomena are basically in magnitudes that correspond to the wavelength of the used radiation. For WLANs following the IEEE 802.11 standard it is between 12 cm and 6 cm, which mean that shifts by one module width may already cause a changed transmission and reception behavior.

Frequency sensitivity of the properties of radio waves

As a rule of thumb, it can be said that the higher the frequency and the shorter the wavelength of the oscillations, the closer the properties of radio waves come to the properties of light: high-frequency transmitters propagate in a straight line and no longer reach receivers behind objects. On surfaces, they are almost completely absorbed or reflected. Signals of longer wavelength, however, also go “around objects” and penetrate deeper into non-conducting objects or can pass through them.

Bands and channels

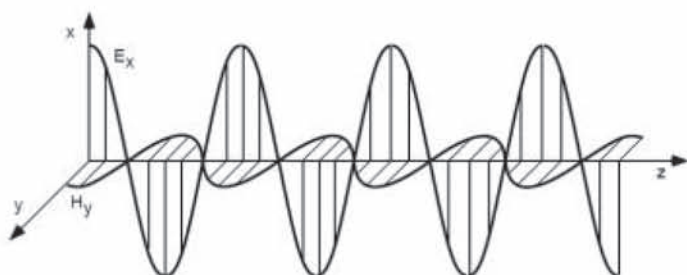
To keep the clarity, the radio spectrum, i.e. the entire frequency range of the radio communication, is divided into individual “bands”. The different bands differ in the radio characteristics (transmission range, susceptibility to interferences, possible data rate,) and consequently also in their applications. The frequency bands are divided into “channels” which are distributed on the respective band at a specific distance. For instance, the 2.4 GHz range of the ISM band is divided into thirteen channels between 2.412 GHz and 2.472 GHz; the spacing between neighboring channels is 5 MHz so that theoretically thirteen transmitters can use the band simultaneously.

Antennas

An antenna transforms electrical currents into electro-magnetic waves and vice versa. They send out electro-magnetic waves and receive them in the same way. Each antenna has a certain frequency range within which the coupling between the antenna current and the surrounding wave is at its maximum.

Electromagnetic waves

Electromagnetic waves consist of an electrical field vector E_x and a magnetic field vector H_y which are always at right angle with each other. The current is the cause of the magnetic field vector and the voltage causes the electrical field vector. (see graphic)



Characteristics of an antenna

Impedance

Impedance refers to a frequency-dependent resistor. For the WLAN components (antenna, cable) this resistor has 50 Ohm. It is important here that the impedance of an antenna, i.e. input/output at the antenna and at the antenna cable are matched to each other.

Polarization

The polarization specifies the direction of the vector of the electrical field intensity in the radiated electro-magnetic wave. It is differentiated between linear and circular polarization. For linear polarization the electrical field lines run in one plane. If they are directed vertical to the ground surface this is referred to as vertical polarization; if they run horizontal to ground level this is a horizontal polarization.

Non-directional and directional antenna

The radiation of antennas can be either non-directional or directional. In general, directional antennas achieve higher transmission ranges; however, this is not the effect of a higher transmitter power but the result of the shape of the radio field.

Antenna gain

The antenna gain is a parameter which describes how strong an antenna sends and receives compared with a reference emitter. An isotropic radiator, i.e. an idealized point source which continuously sends into and receives from all directions. The gain of the isotropic point source is set to zero. The unit of the antenna gain is normally “dBi” (i = isotropic point source). A gain of 3 dBi corresponds approximately to a doubled send/receive line.

The network standards of the IEEE 802 series

The Institute of Electrical and Electronics Engineers IEEE has made it its job to develop, publish and promote electronic and electro technical standards and can be remotely compared to DIN. Under the project number “802”, a number of task groups have been formed to develop standards for the installation and operation of networks. For instance, group “802.3” is concerned with the standards for Ethernet connections. Task group “802.11” has now developed specifications for wireless LANs. Nowadays, these specifications are the de facto standard for radio networks, the most important variants being “802.11 a/h” and “802.11 b/g”.

The IEEE continuously develops the standards to adapt them to new requirements and technical conditions. The following table gives an overview of the topics of some IEEE 802 standards regarding WLANs.

Substandard	Definition area
802.11 a	Communication
802.11 b	Communication
802.11 e	Quality of Service (see 6.3)
802.11 g	Communication
802.11 h	Communication (reduce interference)
802.11 i	Data security (see 5.2)
802.11 n	Communication
802.1 Q	Virtual LANs (see 4.4.1)
802.1 X	Data security (see 5.2)

Basics of IEEE 802.11

The original 802.11 standard 9 (today often referred to as “802.11 legacy” for reasons of clarity) defines the connection of the network nodes via radio in the frequency band at 2.4 GHz or alternatively via infrared interfaces. The gross data rate was up to 2 Mbps, however, the actually achieved net data throughput was considerably less. The standard was improved by the expansions “b”, “a”, “g”, “h” and “n”, which were put on the market in this order. The transmission capacities were increased by more complex and more efficient modulation methods. Over time other sub standards were also defined each relating to certain aspects of operating wireless radio networks. Expansion 802.11n is still in the development phase; this standard is expected to be released before the end of 2009. Devices which support the standard already or after a firmware update are already available on the market.

The following table lists the technical properties of the 801.11 sub standards.

	802.11 “a”/“h”	802.11 “b”	802.11 “g”	802.11 “n”
Frequency band	5 GHz	2,4 GHz	2,4 GHz	2,4 GHz 5 GHz**)
Gross data rate	54 Mbits/s	11 Mbits/s	54 Mbits/s	600 Mbit/s
Net data rate approx.	23 Mbit/s	4,3 Mbit/s	19 Mbit/s	74 Mbit/s
Modulation / multiplex method*)	OFDM	DSSS	OFDM	MIMO

If the connection quality is not good enough to maintain the maximum data rate, the transmission rate is successively reduced until a stable connection is achieved. Basically, a 802.11 a device cannot communicate with a 802.11 b/g device, the “b” and “g” versions of the standards are not compatible.

Transmission range and special antennas

Within buildings the used antennas achieve ranges of typically 30m. Since reflections and shadowing have less effect in the exterior, ranges of up to 100m and more can be achieved. A connection with line of sight is particularly advantageous since the radio waves can then propagate without being disturbed. The use of directional antennas allows to increase this value to a multiple of 100m.

Comparison 2.4 GHz and 5 GHz band

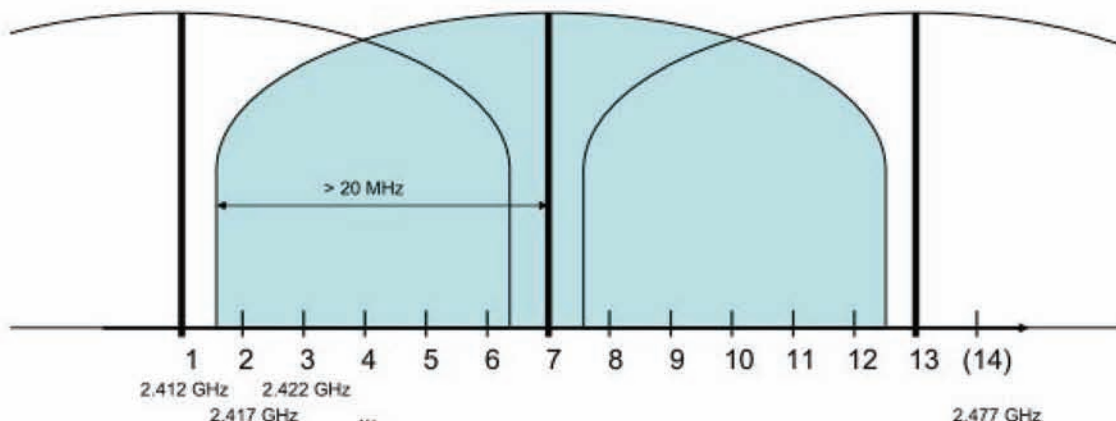
The 2.4 GHz band

The frequency band at 2.4 GHz is a frequency range that can be used without a license in almost all nations. Since it is relatively inexpensive to manufacture transmitters and receivers, the 2.4 GHz technology is very popular and not only used for WLANs but also for numerous other applications.

Channel distribution

The 2.4 GHz band, as used in the 802.11 b/g standard, is normally divided into 13 channels, which have a distance of 5.5 MHz to one another. However, this does not at all mean that 13 independent frequencies are available for each WLAN.

For the used data rates of up to 54 Mbps, each individual transmitter uses a band with a width of more than 40 MHz. To exclude that the transmitters in the WLAN disturb each other, it is required that they keep at least this distance from each other. This reduces the number of frequencies that can be used independently of one another in practical operation to three: usually, only the channels 1, 7 and 13 (the “non-overlapping channels”) are simultaneously used for 802.11 networks.



The above figure shows the envelope curve of a station transmitting on channel 7 of the 2.4 GHz band. The envelope of the spectrum taken up by it is displayed in blue. Non-overlapping transmission of other stations of the WLAN is only possible on the channels 1 or 13 (open envelope). When many access points are used in a network, it is required that many channels that are independent of one another, i.e. non-overlapping channels, are used. In this case, it may be advisable to switch to the 5 GHz band of the 802.11 a/h standards, which offers a larger number of non-overlapping channels.

The 5 GHz band

For the 5 GHz band different numbers of non-overlapping channels are approved in the various regions of the world. The modulation method is OFDM. Generally 5 GHz waves are “harder”, i.e.

the propagation behavior is similar to that of light beams: There is less diffraction around objects, the absorption is higher and the penetration depth lower than for 2.4 GHz waves. Generally, the practically achievable transmission range is a little less than in the 2.4 GHz band. Compared with the 2.4 GHz band the 5 GHz band is clearly less “busy”, and there are only few interference sources in this range. An exception is military radar and satellite tracking systems, whose operators naturally are rather sensitive towards system interferences from a WLAN. To harmonize the operation of 5 GHz WLANs with these systems the IEEE standard 802.11h was created.

Comparison of the properties of the 2.4 GHz and 5 GHz band

Connection security, interference by other devices:

The great popularity of the 2.4 GHz band also results in the fact that a large number of devices that actually have nothing to do with WLANs also transmit in this range – these devices include microwave ovens as well as Bluetooth devices and cordless DECT telephones. This may cause interferences and problems when setting up a WLAN. Depending on the interference source type, it may be advisable to switch to the 5 GHz band. In any case the optimal configuration of illumination, frequency band and antennae must be clarified by a radio field analysis prior to setting up the system.

Data rate

The net data rate for both networks is in the same range of approx. 54 MBit/s. Since the 5 GHz band is less occupied by interference sources and has a higher number of overlap-free channels the 5 GHz band normally has a higher net data throughput.

Range

Mainly, the range of both systems is approximately equally high, within the range of 30 to 100 m; more when using directional antennae. However, 5 GHz systems suffer from severe dampening through obstacles, so that the actual range yield is slightly less than that of 2.4 GHz networks.

Size

Due to the shorter used wave length 5 GHz components of smaller size than 2.4 GHz modules can be produced. (This naturally does not apply for devices designed for operation in both bands (“dual-use”))

Costs

Generally, 5 GHz devices are more expensive than 2.4 GHz devices due to the more expensive technology; however, today many components combine both technologies in one casing.

About the author..



Mr. Vivek Roy is based out of Mumbai, India. He has graduated in Bachelor of Electronics Engineering with Mumbai University. He started his career in “product marketing” with M/s Core Technologies, Mumbai. Later he joined Siemens Limited in year 2005 in their Process Automation Solutions team, later moved to Automation & Drives sales for Mumbai region. Currently he is heading the business segment – Industrial Communication & Identification. He has a total of 12 years of professional experience in sales and marketing for automation & communication solutions.

SMART MICROCHIP BASED NATURAL GAS CHROMATOGRAPHS

- TREND-SETTING OPTIONS TO IMPROVE THE INTELLIGENCE AND PERFORMANCE OF THE TOTAL SOLUTION FOR CALORIFIC VALUE ANALYSIS –

Manoj Singh, Harald Mahler

Siemens AG
Process Automation Sector, Analytical Products and Solutions
Siemensallee 84
76187 Karlsruhe, Germany

KEYWORDS

Custody transfer, process gas chromatography, C6+ determination, relative response factors, hydrogen, power to gas.

ABSTRACT

Natural gas is one of the major energy sources worldwide. Actually, it is expected that this energy source will gain further importance in the global fuel mix during the next decades. Consequently, the demand of automation equipment for natural gas applications will grow as well. From production to distribution network, it is necessary to determine quality parameters automatically. Gas chromatographs play a significant role in on-line process analysis in order to determine the components of the gas and its physical properties. Here, a major parameter is the chromatographic determination of the calorific value, which is particularly mandatory for custody transfer. For this application, the requirements on chromatographs regarding analytical precision and instrument reliability are extremely high. Standardized natural gas chromatographs with measurement capability up to C6+ or C9+ applications have been established in the market. Nevertheless regional variations in terms of best application fit when customizing the

analyser are often necessary. There is a significant potential to improve the best measurement uncertainty of the analyser when optimizing the determination of C6+. For example the Russian natural gas contains an extremely low concentration level of C6+ constituents. Meeting the requirements of the relevant standards are challenging for the gas chromatograph. On the other hand the gas composition can have also significant variations within the national gas grids since different sources are supplying gas to the grid. This influences especially the presence of individual C6+ species. Innovative solutions are available to integrate relative response factors in the calibration model of the gas chromatograph for best performance to determine all individual C6+ constituents of the gas.

Another issue is the changing gas composition within the natural gas grid due to the increasing injection of renewable energy sources. Biomethane from biogas upgrading plants or hydrogen generated by power to gas plants are influencing the overall gas quality inside of the European wide open grid. Gas quality analysers such as on-line gas chromatographs must be able to provide data of the full gas composition including the “new” species

hydrogen, helium and oxygen.

New innovative analytical configurations of a miniaturized process GC are available to meet these individual measuring tasks and performance requirements. The objective of this paper is to present and discuss innovative analytical solutions in the field of natural gas custody transfer. The presentation elaborates the capabilities to improve

best measurement uncertainty of the analyzer which contributes to best plant efficiency. Some representative application examples will be shown. A specific focus is on recent trends in the energy market which influences analytical solution requirements.

1. INTRODUCTION

1.1 - MICRO ELECTRO MECHANICAL SYSTEM (MEMS) :

Micro-Electro-Mechanical Systems, or MEMS, is a technology that in its most general form can be defined as miniaturized mechanical and electro-mechanical elements (i.e., devices and structures) that are made using the techniques of microfabrication.

While the functional elements of MEMS are miniaturized structures, sensors, actuators, and microelectronics, the most notable (and perhaps most interesting) elements are the microsensors and microactuators. Microsensors and microactuators are appropriately categorized as “transducers”, which are defined as devices that convert energy from one form to another.

MEMS products first installed in vehicle airbag systems, video projectors, and ink jet printers. A MEMS accelerometer sensor informs the airbag when to trigger; an optical MEMS sensor is utilized for the phenomenal clearness of modern projectors; and a MEMS nozzle allows ink jet printers to produce

high-resolution printouts.

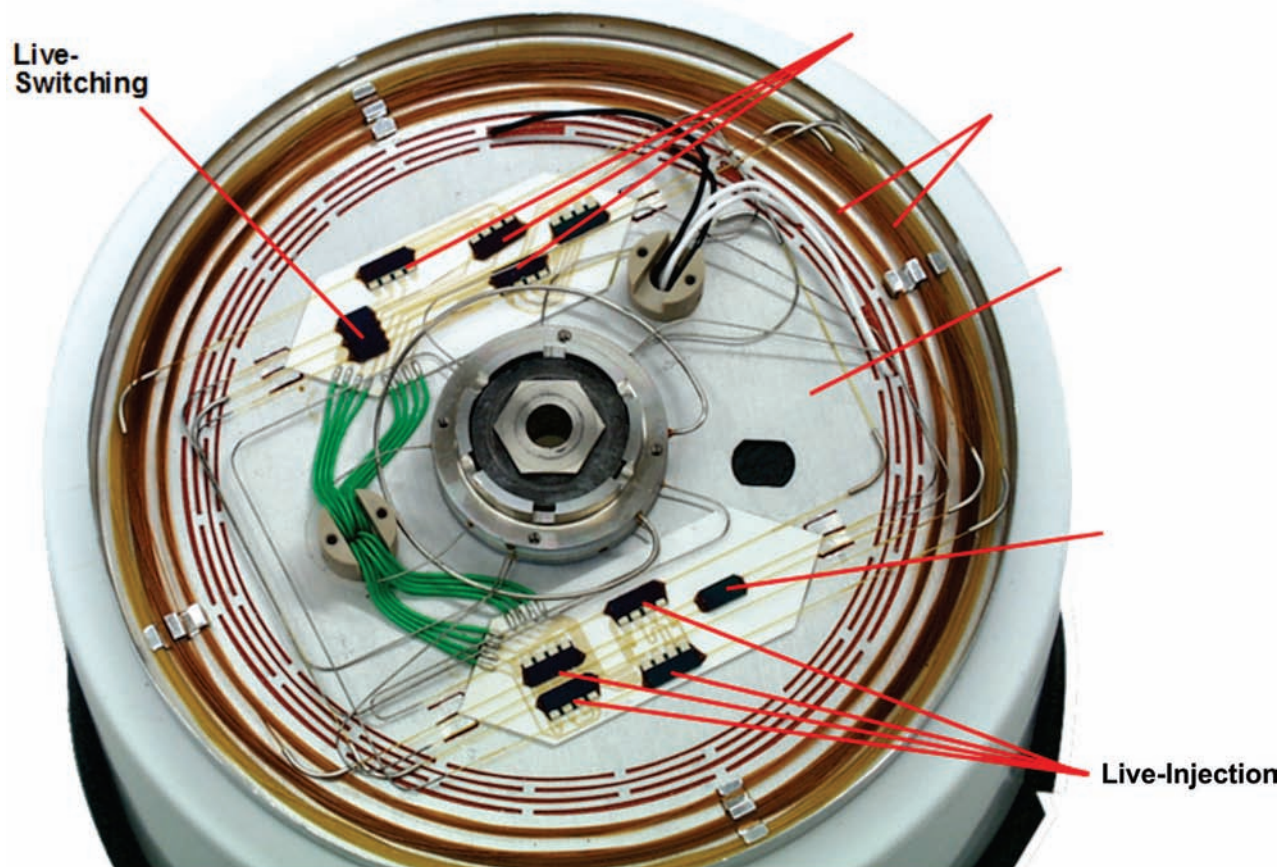
The motivation for using MEMS for the development of new and innovative products is a combination of lower manufacturing costs, compact size, low weight, and low power consumption, as well as increased intelligence and multi-functionality.

These benefits establish the opportunity to improve existing solutions or to provide new products with special functionalities for additional fields of application. The future for the MEMS market is promising. MEMS have consolidated their position in established markets and are continuously finding new applications. This trend in favor of MEMS technology has also characterized new developments in the process industry, e.g. in process analytics. Consider the following product technologies:

- Micro process technology with micro-structured components works for manufacturing in the process industry and delivers particular benefits for chemical synthesis. The small dimensions of the critical components, like micro reactors, mean significant heat generation and flammable reactants and solvents are easier to control. In addition, the product yield is better.
- Micro spectrometers allow the spectroscopist to acquire spectra of extremely small samples and with little sample preparation. Measurements can be made while light is transmitted through the sample, reflected from it, or even when the sample is made to emit light, e.g. due to fluorescence.
- Micro process chromatographs open a new dimension to simplify the analytical system and its installation capabilities outside of analyzer shelters. There is a high potential that micro process GCs will also participate in this trend.

2. IMPLEMENTATION OF MEMS IN GAS CHROMATOGRAPHY:

Following figure shows typical MEMS based GC used for Natural Gas Applications:



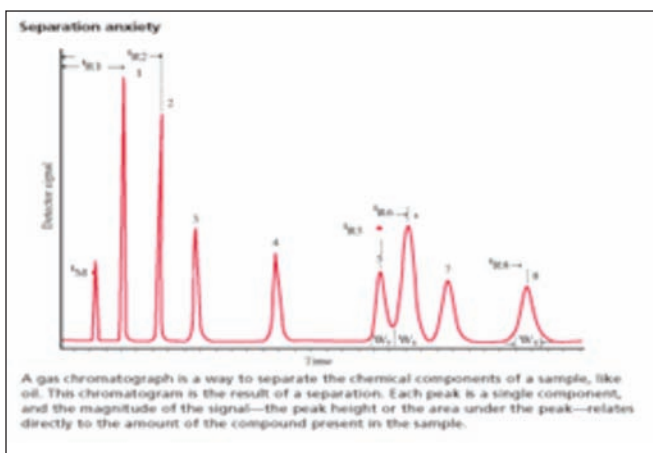
The process GC here uses MEMS technology in microchip scale. The miniaturization of all essential components using this innovative technology allows an extremely compact design of the whole device in the size of a football. This also results in high robustness against ambient influences (degree of protection is IP65 and NEMA4X, ambient temperature range -20°C to $+55^{\circ}\text{C}$) and simplified design engineering for the pressure resistant casing to guarantee explosion protection.

This design offers the possibility to install this analyzer directly at the sample point even in remote locations. The analyzer is modular way and comes as three main units: the analytical module, the electronic section, and the pneumatic interface.

All three parts integrated into housing similar to that of a transmitter. Even as features based on software functionalities are more and more important, the heart of each gas chromatograph is still the analytical hardware around the chromatographic column. These provide separation of the gas mixture into individual components and allow detection according to the measuring task.

Column switching systems are in process gas chromatography as a standard tool for cleaning the system, coupled with short cycle times, which results in optimum repeatability. The switching of the internal gas streams typically uses pneumatically driven valves.

The most important column switching configurations are straight-on, back flush, back flush sum, heart-cut, and distribution. Depending on the valve type, the practicability for column switching systems can have limits depending on the occurrence of pressure pulses

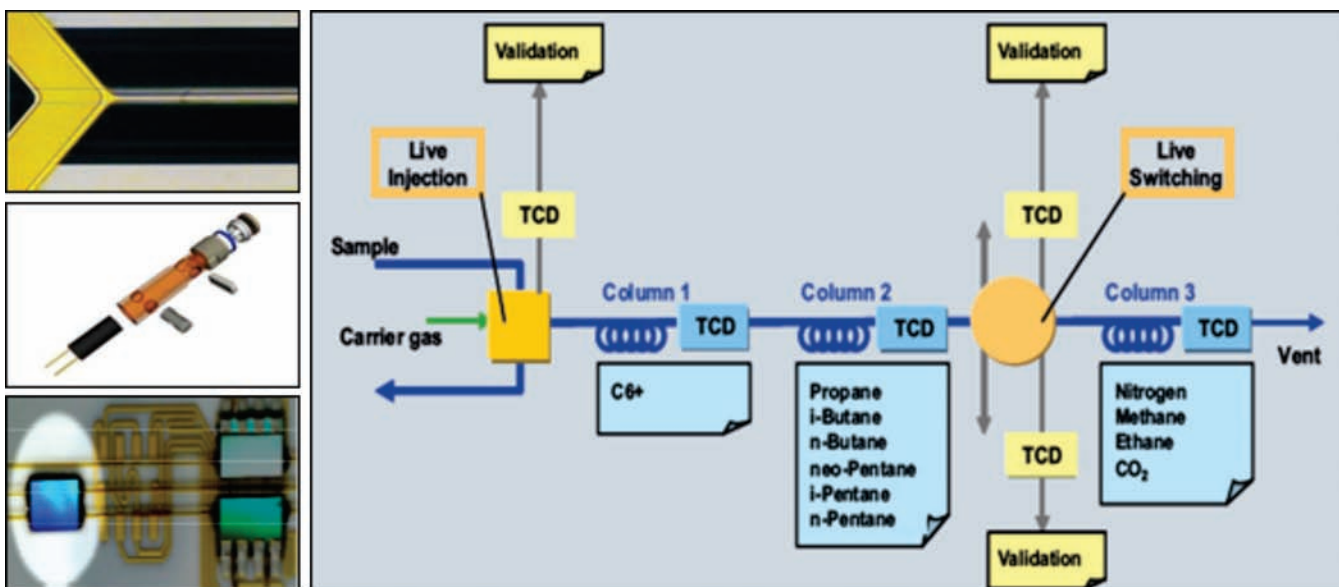


when switching the valves, by diffusion of control medium into the sample path, by chemical reactions, or adsorption of sample constituents with the valve material.

Most all valve types have a significant dead volume. This can lead to peak broadening and to a loss of separation capacity, especially with capillary columns.

These disadvantages disappear when using valveless column switching systems. This analyzer uses MEMS-based technology for key components like injection and detection. The MEMS-based valveless column-switching unit eliminates dead volume. This guarantees the best coupling to the applied high-speed narrow-bore capillary columns. Typically, the adjustment of gas flow in a chromatographic system happens manually by an empirical optimization method of restrictors and electronic pressure controllers. Especially for valveless column-switching this adjustment presupposes experience and time to balance the various internal gas flows.

2.1 Injection and detection: A Micro TCD based gas chromatograph working can be explained from following figure

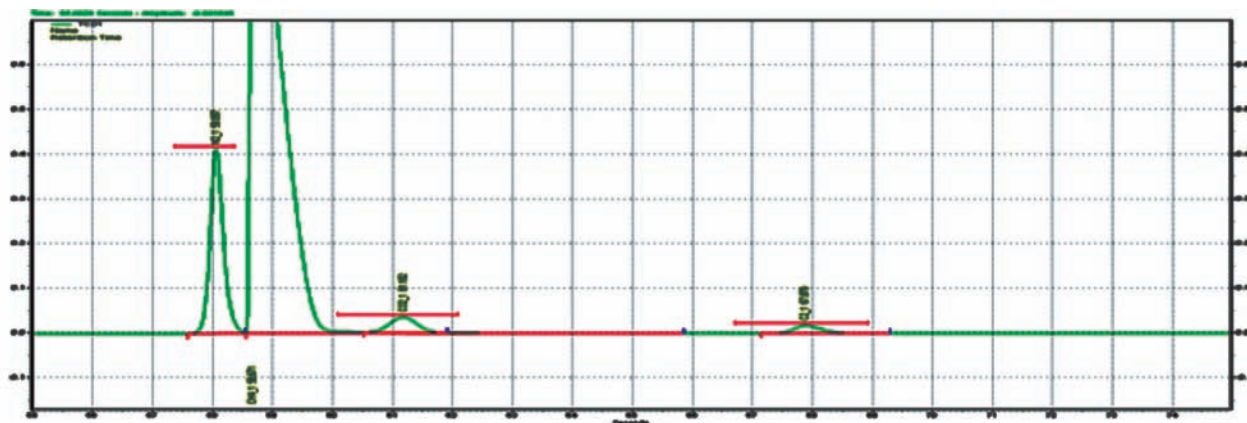


Here you can see the whole chromatographic system with all functional components. All of them are micro-mechanically constructed. Functions such

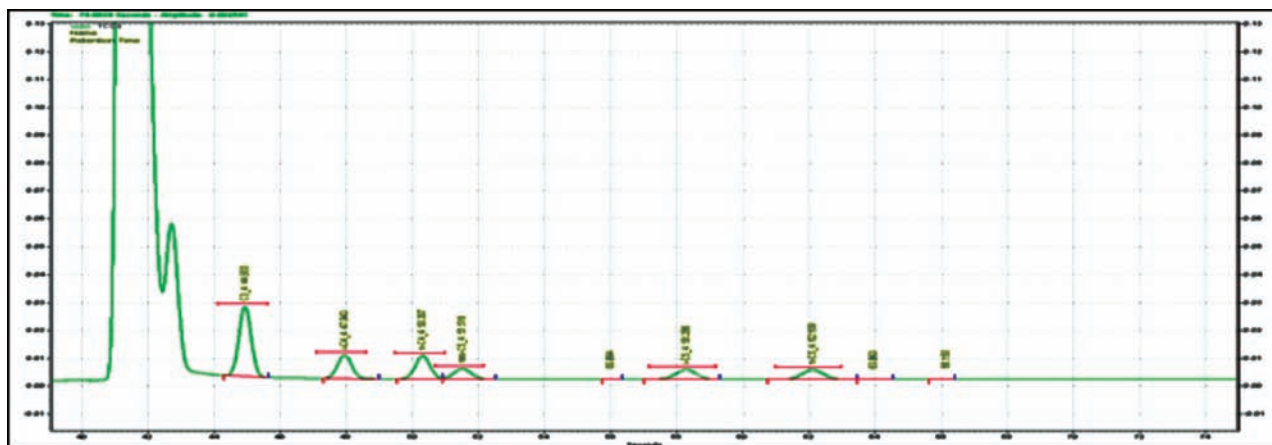
as fill and purge of injection volume or backflush are actuated by the specific device on the chip. The analytical elements are fixed on substrates

(constructed using micro electro mechanical system (MEMS) technology. It Includes the live-injection-chip and 4 half-cell TCD-Chips.

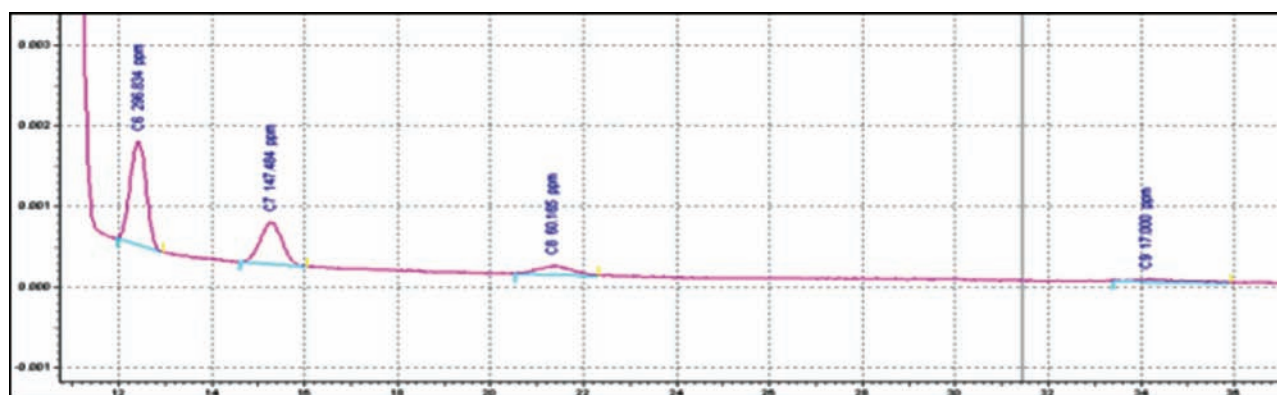
High separation power using narrow-bore-columns results in flexible ranges for various measuring tasks on site, e.g. in gas mixing stations where N₂ load could be high.



The above response predicts the response of TCD 1. Similarly TCD 4b works for detection of Low detection limit using powerful micro TCDs results in low ranges for key components such as neo Pentane; can be used as validation parameter. Components which are analysed are C₃, i-C₄, n-C₄, i-C₅, n-C₅, neo-C₅



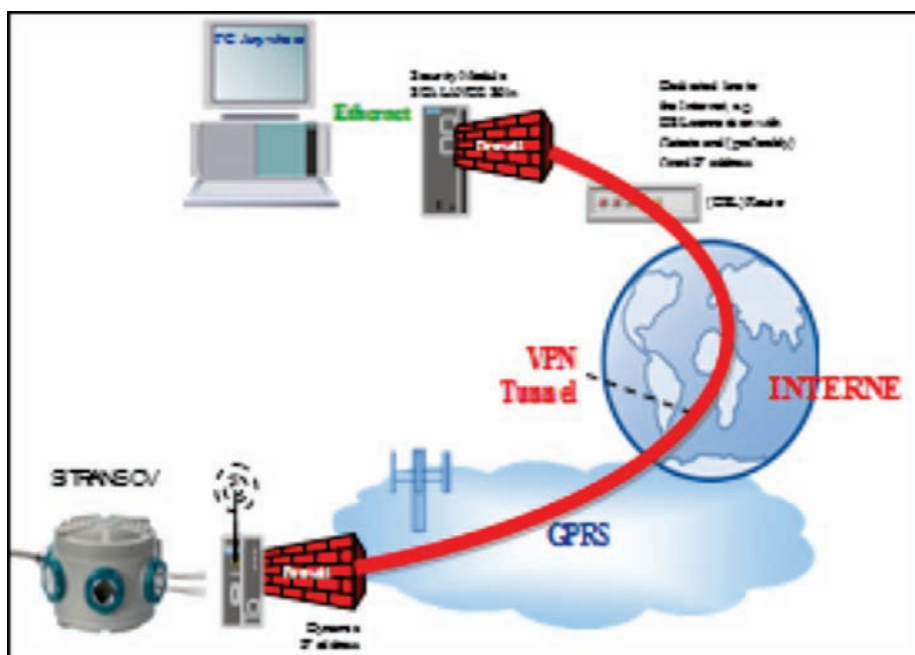
TCD 3a Separation of C₆+. Using MEMS Technology it is also possible to measure individual components C₆ until C₉, The sum C₆ plus could be measure until 50 ppm.



3. SIMPLE INSTALLATION REQUIREMENTS

Process analyzers, such as process GCs, usually get some kind of protection against climatic influences. The GC's mount together with other analyzers in

longer distances to transport the sample from the extraction point to the analyzer shelter is important. A micro GC can go directly inside the plant even above the ground at higher platforms.



centralized walk-in type air-conditioned shelters. Sometimes the GCs are in open, more cost-effective, three-sided stands, or non walk-in type cabinets. The preferred option depends on local (e.g. hazardous area, space requirements) climatic pre-conditions or on the user's philosophy. In most cases, cost is important.

Micro process GCs open new opportunities regarding the system integration installation in the process environment. The size of the Micro GC (12"H x 14"W x 9"D) versus the size of a conventional GC (39"H x 26 1/16"W x 16 3/16"D) enables a smaller capital investment without any degradation of analyzer performance. Nevertheless, there are process requirements as a result of which the plant operator might prefer an analyzer installation as close as possible to the process sampling point. For example, in an acetylene plant, the fast analysis of nitrogen is important to control the process. Avoiding the

Some process samples tend to change during transportation from the sampling point to the remote analyzer shelter where the GC is. When upgrading process plants, space restraints could occur, which prevent traditional analyzer concepts using shelters. Both are further aspects for installation of process GCs at the sampling point. The primary advantage of such solutions is significantly lower capital costs compared to installations in shelters.

The micro GC is best qualified for installations directly at the sampling point:

- Minor requirements regarding consumables: no instrument air necessary, low gas and power consumption
- Reduced space: Installation in small transmitter box or under a rain roof is sufficient
- Practical service concept with easy monitoring

of the analyzer status from remote location and short time to repair

4. COMMUNICATION FEATURES

Process GCs are applicable within a plant infrastructure on various occasions. Therefore, in recent years, many different concepts have been developed and used to integrate the analyzers in the plant-specific communication environment. In the past, analogue links to dedicated communication systems (DCS) have been dominant. The information content for this type of data link is limited to the measured value. Another disadvantage is the high hardware expense when wiring all individual measuring components, especially for multi-component analysis. Digital communication techniques can provide additional information such as status messages, sample stream name or number, or date and time stamp and are predominantly the preferred solutions today. Optimization in process plants is necessary in order to increase their efficiency and for competitive reasons. This also influences modern communication concepts in terms of data safety. DCS links are increasingly redundant.

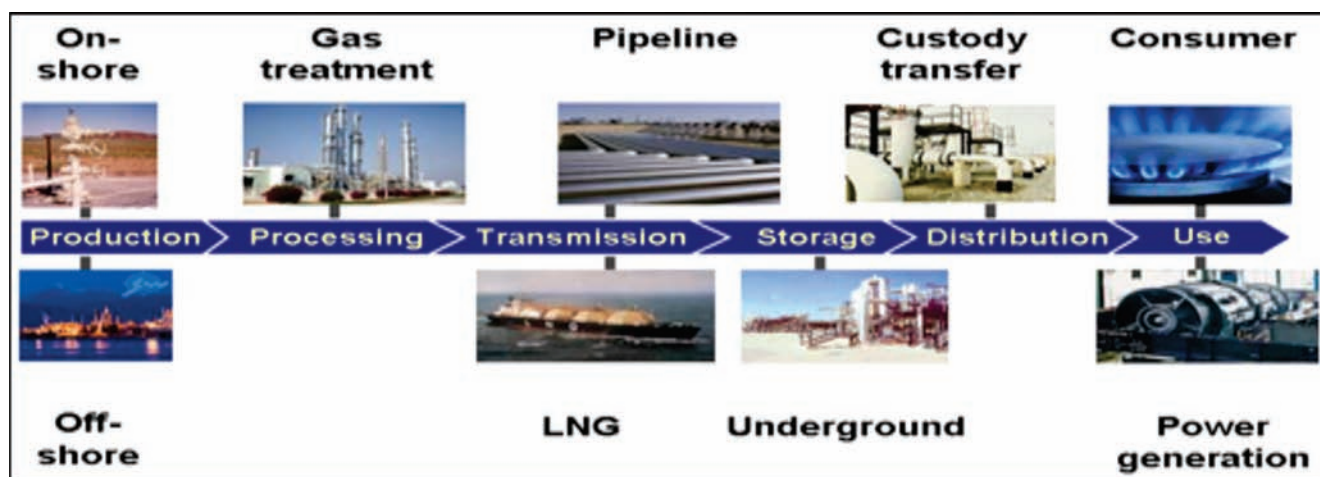
5. INDUSTRIAL APPLICATIONS:

MEMS based miniaturized gas chromatography

solutions because of its features finds its suitability for measurement of Calorific value from production till distribution to the users.

One of the key applications using process GCs is the measurement of lower hydrocarbons and inert gases (N₂, CO₂, C₁ to C₅, sum C₆₊, or C₆, C₇, C₈, C₉ individually). Based on these components, the GC calculates the calorific value, density, or WOBBE index. The components or fractions of these have to be analyzed in various plant locations within the huge transportation grids worldwide. Additional applications are required in natural gas processing plants for sulfur and carbon dioxide removal or for the separation of natural gas liquids. The Micro GC is able to measure pipeline quality natural gas with repeatability for CV and density of better than 0.01 %. Based on the MEMS concept with narrow-bore capillary columns and multi-line and in-line detection, the analyzer provides high separation capacity for all measuring components within a short analysis time of 180 seconds. An accuracy for CV and density of <0.1 % can be achieved. Special CV control operation software is available to meet the requirements in terms of verification and access to a fiscal metering mode.

Applications are required in saturated gas plants, summarization plants, reformers. Depending on the sampling points, the measured components and its



concentration range are varying. Another market segment where process GCs based on MEMS technology exceed the requirements is the Power to Gas , Renewable energy like Bio Gas , custody transfer when injecting biogas into the natural gas grid. Component determination including Hydrogen and Helium for natural gas. This application can be accomplished by using Micro Gas chromatograph. It finds its application where natural gas contains He and it is important in Power to gas application .

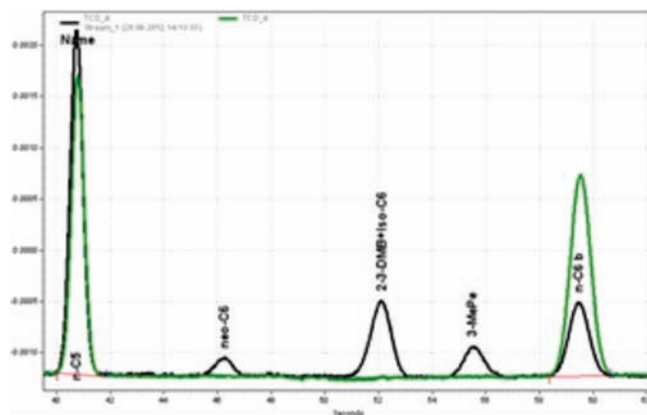
Another application which is gaining popularity for use of chip based gas chromatograph is determination of C6+ Fraction by using Relative Response Factors. In this application Analyze all C6+ components individually (e.g. neo-C6, 2-3DMB, iC6, 3-MePe, n-C6, Benzene, Toluene, MeCyC6, C8, C9). Identify main C6 species in various local natural gases types.

Use the C6 species for calculating the relative response factors of other C6 components which can be used to calibrate the GCs and hence reduce the gap in the analysis results between Lab and process . This helps in accurate billing in custody transfer applications .

Liquefied natural gas (LNG) terminals (in liquefaction as well as in LNG vaporization plants) and floating production storage off-loading ships in offshore

applications are examples where Process GCs utilize state of the art technology to determine the CV value.

The MEMS analyzer is available that works for various analytical tasks in the oil and gas industry. Features like narrow-bore capillary columns and multi and in-line detection guarantee high separation power and repeatability of measuring results within a short analysis time. The compact and modular analyzer concept allows flexibility in field



installations such as decentralized locations close to the sampling point or inside of shelters. Therefore, micro Process GCs are a promising tool for the planner and user to reduce their capital investment. The simplification of analytical systems using a novel mathematical network model will support the trend of standardization of process GC solutions.

As the sources of natural gas become more diverse, the trace constituents of C6+ become of increasing interest quality as. The C6+ fraction affects gas quality issues and safety considerations, such as anomalies associated with odorization. C6+ Backflush sum is the preferred solution when using GCs with packed separation column technology. C6+ straight forward approach (individual components calculated to C6+) is the common solution for modern Micro GC capillary column type versions. Light gases with very low concentration levels of C6+ down to 5 ppm . Typical light gases occur in Russia – considered in GOST 31 371.7-2008

6. KEY ADVANTAGES:

1. Standard & Extended Measurement:

We can achieve extended measurement of concentrations for components which by using Micro gas chromatograph. It finds an extensive suitability of applications in Natural gas Grid where bio gas is injected and it becomes important to measure Oxygen Content in the mixture along with

other components like CO₂ and Hydrogen.

The extended measurement brings an advantage in the fiscal metering applications eg: considering

Components	Symbol	Concentration (mol%)
Carbon dioxide	CO ₂	1,0010
Nitrogen	N ₂	14,7170
Methane	CH ₄	80,8450
Ethane	C ₂ H ₆	2,8160
Propane	C ₃ H ₈	0,3850
iso-Butane	i-C ₄ H ₁₀	0,0630
n-Butane	n-C ₄ H ₁₀	0,0720
iso-Pentane	i-C ₅ H ₁₂	0,0180
n-Pentane	n-C ₅ H ₁₂	0,0170
neo-Pentane	neo-C ₅	0,0080
Sum C6+	C6+	0,0560
<hr/>		
Heating value	34,8907 (MJ/Nm ³)	
	9,69186 (kWh/Nm ³)	

Components	Symbol	Concentration (mol%)
Carbon dioxide	CO ₂	1,0010
Nitrogen	N ₂	14,7170
Methane	CH ₄	80,8450
Ethane	C ₂ H ₆	2,8160
Propane	C ₃ H ₈	0,3850
iso-Butane	i-C ₄ H ₁₀	0,0630
n-Butane	n-C ₄ H ₁₀	0,0720
iso-Pentane	i-C ₅ H ₁₂	0,0180
n-Pentane	n-C ₅ H ₁₂	0,0170
neo-Pentane	neo-C ₅	0,0080
Group C6	C6	0,0300
Group C7	C7	0,0155
Group C8	C8	0,0070
Group C9	C9	0,0035
<hr/>		
Heating value	34,9028 (MJ/Nm ³)	
	9,69523 (kWh/Nm ³)	

C6+ Measurement:

Heating value: 9,6919 kWh

Price: 12 cent per kWh

Volume: 10 Million Nm³ per day*1

â = 11630000 €

C9+ Measurement:

Heating value: 9,6952 kWh

Price: 12 cent per kWh

Volume: 10 Million Nm³ per day*1

â = 11634000 €

Extended measurement results in saving of 4000 € per day

• **Analytical Results**

Accurate measurement means precise energy flow calculation.

-High separation power using narrow-bore-columns results in flexible ranges for various measuring tasks

on site, e.g. in gas mixing stations where N₂ load could be high. Highest range for nitrogen up to 25%; Lowest range for CO₂ of < 500 ppm

-Low detection limit using powerful micro TCDs results in low ranges for key components such as neo Pentane; can be used as validation parameter . High separation power of i-C₄ vs. neo-C₅ and Detection limit for neo-Pentane < 10ppm.

It is also possible to receive information about the individual components C6 until C9, The sum C6 plus could be measure until 50 ppm. Lowest range for C6+ < 30-50 ppm; Individual measurement of C6, C7, C8 and C9.

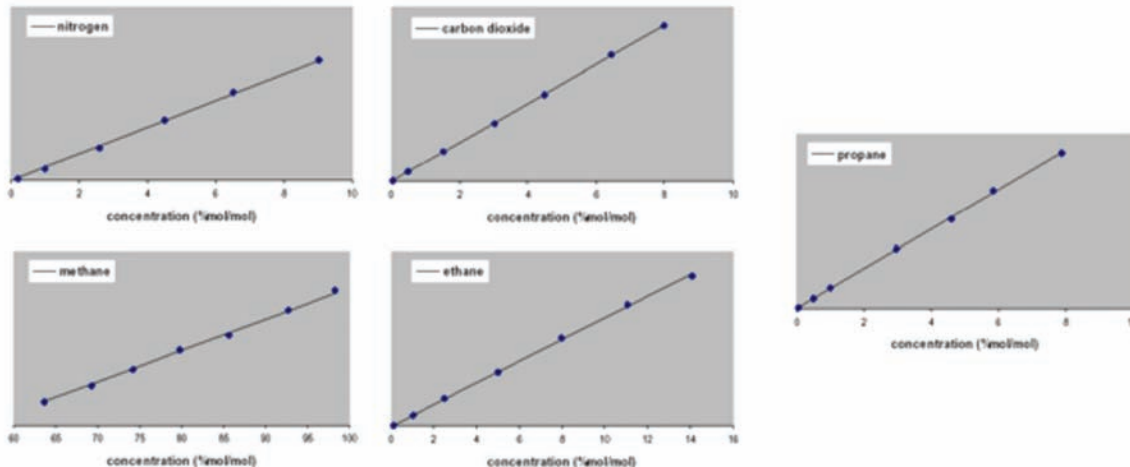
- -Use of MEMS based technology brings greater linearity (ref figure below) throughout the entire measuring range enables single-point calibration . Less calibration expenses in comparison to multi level calibration (time, man power, just 1 calibration gas) and hence no linearization service

needed over the measuring range.

easily installed at any locations in the plant.

• **Repeatability**

-< 0,01% for all Calculated Values.



-Ambient temperature and pressure influences are negligible due to unique “live injection” which is possible by using MEMS technology.

-No Memory Effects for alternating Contrast Streams. Multi stream installations also for “contrast streams” through live-injection

7. SUMMARY:

Process gas chromatography has proven its worth in the oil and gas industry as an important tool for process analytics. This technology has high availability and is extremely flexible for a variety of applications despite the varying requirements of the market.

-Micro Gas Chromatograph technology is highly flexible to adapt new applications to be able to meet changing requirements in the natural gas market .

-Based on its innovative MEMS technology the GCs consist of a highly tuned system with best accuracy, repeatability and detection limits.

-Through the compact and rugged design the analyzer is simple, flexible, cost-saving and can be

REFERENCES:

1. Mahler H. (2008) Process analysis with MEMS technology. Refineries benefit from micro-process gas chromatographs, P&A Select Oil&Gas
2. NG & metering skids by Dr. Stefan Malcharek.

BIOGRAPHIES



Mr.Harald Mahler : Born on 05.09.1960,from Germany is a Gas Analysis Expert, and is working for Siemens Process Analytics since 27 years .He is associated with Siemens as Global Business Development Manager . for Gas Chromatography Products



Mr.Manoj Singh: Born on 26,11,1973 started his career in 1993 with Hartman and Braun after his Engineering in Electronics and continues to be in Gas Analytical field. He is working with Siemens Ltd since 2011 as ‘Business Head for Analytical Products’.

END USER EXPECTATION AND AUTOMATION CHALLENGES IN OIL SECTOR

T. K. Chattopadhyay & S. Saha

Indian Oil Corporation Limited, Mathura Refinery, Mathura.

ABSTRACT

Automation in Oil sector has resulted in significant economic, environmental, technical and operational benefits. In this paper various automation challenges and end user expectation are discussed.

KEYWORDS

Asset Management, Loss Control monitoring,

INTRODUCTION

The automation used in oil sector can broadly divided into three categories.

1. Field Instrumentation
2. Control Room Instrumentation
3. Special Instrumentation

The Field instrumentation mainly consists of Transmitters and automatic valves. The control room instrumentation consists of PLCs, DCSs and ESD systems and their HMI. The special instrumentation mainly consists of Machine Monitoring systems, Electronic governors and Anti-surge control systems.

ASSET MANAGEMENT

HART management systems are installed in various refinery units for monitoring of smart transmitters and smart positioner mounted control valves. These HMS provide wide variety of features such as instrument diagnostics and alerts. However, the HMS is restricted only to the smart instruments. There is no such Asset management system for monitoring

the special instrumentation such as vibration monitoring probes and proximeters. The main Control Systems like DCS and PLCs have their own software for indicating System alarms and diagnostic messages with fault annunciation. The challenge presented here is that we are faced with referring to islands of several systems and instrumentation for fault identification and diagnosis. Also we have some systems which have diagnostic features at an elementary level. This presents a great challenge in meeting the needs of managing the Assets in a Planned manner which can be possible to achieve if we have an Integrated Asset management system for all the instrumentation systems involved in our plant. The Integrated Asset Management system should possess features for early fault identification, fault annunciation, fault history, fault diagnosis with a decision making tool to indicate time of replacement of parts. This will enhance our capabilities of true implementation of predictive maintenance and overall Asset management.

LOSS MONITORING AND CONTROL

In today's competitive scenario, every organisation in oil sectors wants to improve their operating margin by various means viz., optimization of operations. Loss control is one of the key area by which the operating margins can be improved by reducing costs. In general, in oil sector the losses occur in Flare, steam and utilities such as compressed air systems. Ultrasonic flow meters are available for monitoring flare gas flow and acoustic wireless transmitters are available for monitoring of Relief Valves and Control valve passing through which flare losses from individual unit or equipment occur.

Similar monitoring and early detection systems are required for monitoring the leaks and losses of steam and utilities (Compressed air, water) in equipments/vessels/Control valves, Relief valves.

EFFICIENCY MONITORING OF MACHINERY

Machinery such as compressors and turbines have been integral part of oil industries and significant development is made in the machinery automation to improve the monitoring and control of the Rotary machines. However, monitoring of efficiencies of these machines and optimization through selection and operation and optimal level with minimum energy loss have been a challenge for oil sector.

CONTROL SYSTEM FRONT END

Almost all control system vendors, whether DCS or PLC, have moved on from the proprietary hardware and OS to MS Windows based PC as front end for the control systems. Though, these windows based PCs have added new functionalities to the control system frontend, these PC based frontends have always lacked the reliability and life cycle of the proprietary front ends.

The life cycle of these PC based front ends are driven by the hardware availability and OS obsolescence and this results in upgrade of the frontends of the critical control systems every 5 years now a days and this becomes very big challenge for oil industries to replace or upgrade the frontends of the critical control systems in such intervals.

This PC based front ends unlike their predecessors, are vulnerable to cyber security threats which is a greater risk and challenge.

While the Control and Instrumentation suppliers the world over have arrived at a common Instrumentation Bus concept through Field bus

which is universal in its acceptance: similarly it is expected that, a Operating system is developed by a multi-suppliers group for our Front-end which shall be vendor independent. This Operating System can be used in any Operator Stations and vendor specific GUI/HMI software shall be loaded as overlays on this OS. So this OS will be a replacement of the Microsoft Windows OS. Being Control System specific it shall have the additional advantage of being immune to normal malware/virus software which destroy/disable the functionalities of Windows OS.

COMMON CONTROL SYSTEM SOFTWARE

All control system vendors use proprietary software for engineering and configuration of their control system. As an end user of these software, the engineers of oil industries are required to be trained in different software for performing the same job. Apart from the control systems, special instrumentation systems such as Governor control systems, MMS have their own software. This requires developing and mastering special skills for each type and make of Systems. In today's scenario of frequent manpower turnover, it is a challenge to find and retain engineers with skill-set conforming to all the varied Control systems. Having a common software platform for engineering and configuration of any control system will become easier, faster and acquiring time of such skill-set will also be drastically reduced for oil industries.

LARGE SCALE APPLICATION OF WIRELESS INSTRUMENTATION IN REFINERIES - CHALLENGES

For Instrumentation, after the advent of Fieldbus the next frontier lies in large scale application of wireless instrumentation Plant-wide in the Process Units and Offsites of the Oil industry. The principal challenge faced by all automation users in large

scale implementation of Wireless instrumentation systems, is the limitation of Battery life for the wireless Transmitters. While solar powered batteries have been launched by some of the Instrumentation suppliers, this is not a lasting solution of those regions/countries where bright sunlight is not easily available. The limitation of Battery life seriously impedes the user/engineer to configure the transmitters for a scan time of 0.2 second which is the present day standard for all smart transmitters. This prevent the use of wireless instrumentation in Closed Control Loops. As an user we believe that the application of wireless instrumentation (which has several advantages over conventional wired instrumentation) will take a quantum jump if suitable technology becomes available for increasing the battery life to 10 years with an instrument working on a 0.2 second scan time.

CONCLUSION

With focussed and concentrated research, collaborative effort from all the stakeholders in Automation (Manufacturers/Suppliers, Integrators, End-users) through sharing of the fruits of technological advancement achieved, it will bring us closer to meet the Automation challenges being faced in these times, thus achieving the expectations of the Oil industry.

NON CONTACT NUCLEONIC DENSITY MEASUREMENT USING SODIUM AND POTASSIUM SOURCE REDUCING HAZARD AND SECURITY CONCERNS

**Mr. Vladislav , EPT Limited
Moscow, Russia**

**Dr. Abhishek Goyal
Mr. Rajat Goyal
EIP Technologies Pvt. Ltd., Noida, India**

KEYWORDS

Density Measurement, Power Plants, Steel Plants, Mining Industry, Slurry, Liquid, Nuclear, Na-22, Radioactivity

ABSTRACT

Large-scale manufacturing industries ranging from power industry to cement to steel, plastics, foods, fertilizers and others must overcome challenges of accurately measuring the liquid density. There are many technologies for measuring the same namely, Conventional Nucleonic Density Measurement, Coriolis based, Microwave based, Ultrasonic based and Gravimetric based. However, all the technologies have their limitations with major affects being the temperature, pressure, vibration, damage and suspended solids but the technology that has really stood the test of time is Nucleonic Density Measurement. However, with the stringent restrictions on the import and use of radioactive sources (Cs-137 and Co-60) for the conventional nucleonic technology has faced its hardships in the past.

In this paper we will introduce a Nucleonic technology which used Na-22 and K-40 as the radioactive sources. The density meter uses gamma radiation of the radiation free source of Na-22, the natural background or gamma radiation of chemical potassium compounds with the natural concentration of the isotope K-40. Due to its principle, these devices do not exceed the minimum significant activity level pursuant to the existing IAEA radiation on safety standards and regulations. These devices do not generate any radiation background, do not require any special radiation shield, do not pollute the environment and can be used for typical applications without restriction on temperature, pressure and suspended solids.

TYPES OF DENSITY MEASUREMENT

Coriolis

Coriolis density meters, also known as mass flow meters or inertial flow meters, work on the principle of vibration to measure phase shifts in the vibration of a bent thin walled tube. The bent thin walled tube is rotated around a central axis. When there is no mass in the bent section, the tube remains untwisted. However, when the density inside the bent section increases, the inbound flow portion of the bent pipe drags behind the out flow portion. This twisting causes phase shifts which result in changes in the resonant frequency of the thin walled tube. Therefore, the resonant frequency is directly affected by the density. Higher density media causes a larger coriolis effect. Flowing media causes a frequency phase shift at both ends of the bent pipe. This is proportional to the mass flow rate of the sample.

Coriolis meters measure the mass flow of the system. They do not measure the volumetric flow. However, a volumetric flow can be inferred from the mass flow measurement. These measurements are restricted to small diameters for flow tubes. However, this measurement technique results in high accuracy and high repeatability. Coriolis meters also have a fast response time.

Coriolis meters need to be calibrated for temperature and pressure. The zero points for these values are used to calibrate the system. Coriolis meters cannot be calibrated while in use. The span difference is used to see how temperature and pressure have changed.

Microwave

Microwave density meters have various ways to measure what solids are in the sample. All microwave meters measure microwaves but some use different methods such as measuring the microwave propagation speed change, amplitude reduction, time of flight, single phase difference, or dual phase shift. Each technique has certain accuracies.^[1]

Some microwave meters use a ceramic probe that is directly inserted into the sample. This allows the meter to have direct contact to the sample in question. However, this limits the types of slurries and sludges that can flow through the pipe line. Abrasive slurries with particulates can damage the sensor probe.

Microwave meters are also limited to liquids with unvarying dielectric constants. The percentage of solids of the slurry affects the dielectric constant for the entire sample. Typically, percent solids greater than 20% result in large errors. Similar inconsistencies happen with large pipe diameters.

Microwave meters are very good at detecting dissolved solids. Homogenous solutions are easily seen by microwave meters. This makes them a fit for applications where the solution is consistent and non-abrasive.

Ultrasonic

Ultrasonic density meters work on various principles to calculate the density. One of the methods is transit-time principle (also known as the time of flight principle). In this

technique, two transducers are mounted to the sides of the pipe walls. The transducers alternate between sending and receiving ultrasonic signals. From this transit time measurement, the flow velocity and volume flow based on the diameter of the pipe are calculated.^[2]

Another method this is used is ultrasonic attenuation method. This method measures the count of various signals with certain amplitudes. The density of the media flowing through the pipe affects the signal sent through the pipe. This changes the strength of the signal, causing a weaker signal and smaller amplitude.

Another method that is utilized in ultrasonic meters is the envelope energy average method. This method is based on not only the amplitude of the signal but also the shape of the signal. These packets of information are called envelopes.

Doppler ultrasonic meters measure the suspension flow where the concentration of solids in the slurry is above 100ppm and the particles that are suspended are larger than 100 microns in diameter. However, the Doppler method only works on concentrations of less than 10% solids.

Gravitic

Gravitic density meters work on the principle of gravity to calculate the density of a sample. A flexible hose is used to determine the change in weight. Using the principle of beam deflection of two fixed ends, the weight can be calculated. Increases in weight result in a larger deflection. Decreases in weight result in a smaller deflection. The volume inside of the hose never changes. Since the volume is constant and the weight is known, the density is easily calculated from this information.

Displacement is measured with a high precision displacement laser. Micron scale deflections can be read by the density meter. Minute changes in weight are seen at this scale.

The entire volume is measured using gravitic methods. This means that the sample size is the entire volume of what needs to be measured.

Nuclear

Nuclear density meters work on the principle of measuring gamma radiation. Gamma radiation is emitted from a source. This source is typically Cesium-137 (half-life: ~30 years). The radiation is seen by a scintillator device. The radiation is converted into flashes of light. The number of flashes of light is counted. Radiation that is absorbed by the mass is not seen by the scintillator device. Therefore, the density of the media is inversely proportional to the radiation captured and seen by the scintillator.

Conventional Nuclear density meters are limited in scope to what is seen by the gamma radiation beam. The sample size is a single, thin column with small longitudinal length.

Conventional Nuclear equipment requires certified and licensed staff in order to operate the instruments.

DISADVANTAGES OF CONVENTIONAL NUCLEAR DENSITY MEASUREMENT

- Uses Highly Active Radioactive Source of Cs/ Co
- Radioactive Activity Very High and dangerous for people and environment
- Emission is higher than the levels pursuant to current IAEA radiation safety standards and regulations
- Significant Radiation Background
- Special Heavy Protection casing for background Radiation
- Pollutant to the environment
- Special training required to handle the instrument
- Dismantling and Disposal is a significant problem
- AERB Certification and Import License for each import

NUCLEAR DENSITY MEASUREMENT WITH NA-22 SOURCE AND HIGH SENSITIVITY DETECTOR

The technology used in the device consists of natural or artificial gamma radiation sources emitting 1 -20 **micro Curie** (with Maximum Source Radioactivity of less than 1 MBq) which does not exceed the minimum significant activity level pursuant to the existing IAEA radiation safety standards and regulations therefore the devices are not subject to the supervision by the State Nuclear Supervision Authority, Sanitary Epidemiological Service. Moreover, the device is not subject to licensing by AERB as the Source Na-22 and the radioactivity level is under the exempted category allowing for an NOC for the source import.

In contrast to its conventional Radio-isotopic analogues, the device uses natural and artificial gamma radiation sources which activities do not exceed the minimum significant activity levels pursuant to the applicable IAEA radiation safety standards and regulations.

Emitter/ Radiation Source

In various applications the gamma radiations of the radiation-free source of Na-22, the natural background or the gamma radiation of chemical potassium compounds with the natural concentration of the isotope Potassium-40 are used .

These devices have all advantages of traditional radioisotope analogs, namely they are indispensable in difficult process conditions when used for:

- toxic, aggressive and biologically hazardous materials;
- corrosive and abrasive substances;
- molten and cryogenic materials;
- radioactive substances of high or alternative activity;
- foams, slurries and sludge;
- powder and other highly dispersed free-flowing substances;
- pulp, ore, feed stock and other similar materials;
- vessels without pressure restrictions;
- vessels without temperature restrictions.

These devices are free from the main disadvantage of traditional radioisotope analogs, i.e. necessity to use a powerful radionuclide source.

Following are special features our device:

- Natural Sources of Na-22 and K-40 with very low activity (less than minimal significant activity-MSA)
- do not generate a radiation background;
- do not require a special radiation shield;
- do not pollute the environment;
- do not require specially prepared and certified premises and personnel;
- do not create problems during dismantling of the equipment.
- Do not require special heavy protection casing

Due to the absence of a radiation source or its small dimensions (there is no radiation protection) the devices can be mounted in the places where it is impossible to install conventional devices.

The non-contact density meter do not contain moving parts and do not require maintenance. You really can "plug and forget".



With Best Compliments from
Pyrotech Electronics Pvt. Ltd.

Our Products :-



Shelter



NG & LAVT Cubicle



ECP UCP



Drawout type MCC/PCC



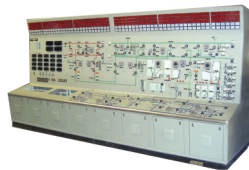
Large Video Screen



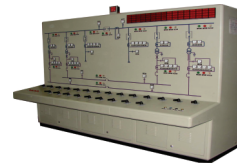
Control Rooms



Mosaic Control Desk



Synchronization Desk



Wired & Bare Control Desk



LIE / LIR



Wired and Bare Panel



PDB/LDB/DB



Console Desk



19" Rack



Metering Box

Pyrotech Electronics Pvt. Ltd. Unit-II
 E-329, Road No. 12 MIA, Udaipur-313003
 (Rajasthan) India
 Tel.no. : 0294-2492122/31/34
 Fax No. : 0294-2492130, 2414458
 Email: pyrotech@pyrotechindia.com

Pyrotech Electronics Pvt. Ltd. Unit-IV
 A1-193, Road No. 5 MIA, Udaipur-313003
 (Rajasthan) India
 Tel.no. : 0294-2490628
 Fax No. : 0294-2492130, 2414458
 Email: pyrotech@pyrotechindia.com

Pyrotech Electronics Pvt. Ltd. (Delhi)
 C-140, Sec-63,
 Noida (UP) India
 Tel.no. : 0120-4210633
 Email: electricals@pyrotechindia.com

control your future

 **Pyrotech**
 www.pyrotechindia.com

SIEMENS



Siemens Process Instrumentation

Enhancing your service experience with Siemens Process Instrumentation

Introducing, a new range of service offerings.

Siemens Process Instrumentation introduces its all new and improved service and support offering that will help you maximize the return on your investment through personalized service and assistance.

Our enhanced service & support offerings will help you protect your investments by fulfilling your every requirements throughout the life of your installations.

Our new range of services:

- Dedicated Toll Free Number
- New Repair Centre for SIPART PS2 Valve Positioner
- Expert Technical Support
- Proactive Service
- Maximum Uptime
- Affordable Replacement outside Warranty
- Online Support

For more details on our services & support,
call our dedicated toll-free no. **1800 208 3000** between 6 AM to 12 Midnight.

www.siemens.co.in/pi-services