

# **COMBUSTION ANALYZER REQUIREMENTS FOR SIL CERTIFICATION AND SIS IMPLEMENTATION**

Larry E. Sieker, PE & Chris Kolesar, EE  
150 Freeport Road Pittsburgh, PA 15238  
Ametek Process Instruments

## **KEYWORDS**

SIS, SIF, SIL, IEC 65108, NFPA 85, BMS, FMEDA, SFF, PFD, O<sub>2</sub>, CO Break Through, Methane, Zirconium Oxide, Catalytic Bead, Asset Management System, MODBUS, Ethernet, Web Enabled, Preventative Maintenance, Proactive Maintenance.

## **ABSTRACT**

The reliable identification of low combustion oxygen and/ or high or low combustibles (CO) in a fired heater or boiler has always been critical to the effectiveness of the Burner Management System (BMS) for proper control and safety.

Modified burners and aggressive firing control points to achieve increased efficiency and emission reductions has led the industry to realize tighter control leads to a potential higher probability of combustion “events” which need to be addressed . The need to add additional layers of safety to the Basic Process Control System (BPCS) to reduce the risk of a combustion event has become a high priority within industry and has led to implementation of Safety Instrumented Systems independent of the Basic Process Control System (BPCS).

Additional layers of Safety can be achieved with the measurement of excess O<sub>2</sub>, Combustibles, and Methane and using these readings to insure safe operation of the process or shut it down if it gets out of control. In safety applications, it is critical that the “availability” of the analyzer (is it operational and correct?) is as high as possible.

A Combustion analyzer now needs to be designed to provide the complete solution for combustion process control and process control safety with redundancy and diagnostics to monitor performance and health as well as provide statistical data needed to implement

Predictive and Proactive maintenance programs which will maximize the availability of the analyzer and reduce the Probability of Failure on Demand ( $P_{FD}$ ) factor used in SIL level calculations

The needed design characteristics of a Combustion analyzer for SIS implementation and preventative and proactive maintenance programs will be reviewed.

## **COMBUSTION ANALYZER**

The combustion analyzer has been a necessary component of combustion control for many years. In its simplest form, the combustion analyzer provides an excess Oxygen ( $O_2$ ) reading so that an air to fuel ratio can be maintained throughout the firing range of the process heater. The analyzer is typically installed in the convective area of the process in a close proximity of the top of the radiant section so as the analyzer provides a realistic value of how much extra air was added to combust the fuel. This excess air set point is considered a “safety factor” so that by adding more air than required for complete combustion, operations can have a “control cushion” so that if conditions change dramatically, the combustion process will not swing to a “fuel rich” situation where fuel is not completely consumed and the potential for a hazardous event could occur. Hazardous events created by a fuel rich situation would include burner flame-out, CO flood, black stack, convective section burning, slag formation, an explosion, etc. In this regard, operators have opted to control with a higher than necessary set point of  $O_2$  to insure a fuel rich situation is avoided. This insurance does have a price, though. The high  $O_2$  set points for safety results in less efficient combustion, using more fuel gas than necessary and higher  $NO_x$  emissions.

Most industrial users today realize the need to run the combustion process at the lowest level of excess  $O_2$  to insure a complete burn of fuel for efficiency, and to reduce  $NO_x$  without sacrificing safety. Therefore, the combustion analyzer now used to control the combustion process incorporates besides the excess  $O_2$  sensor, an additional sensor for “part per million” (ppm) “CO” or ppm “combustibles” for feedback on the  $O_2$  set point. The combined  $O_2$  and CO combustion analyzer can provide an output to control combustion air to a specific set point based on a specific firing rate and then use the CO output as feedback on the efficiency the  $O_2$  set point. An  $O_2$  set point with no trace of CO in the combustion gas would mean that a lower  $O_2$  set point could be achieved without affecting safety and to reduce  $NO_x$  emissions. An  $O_2$  set point with over 500 ppm CO in the combustion gas would mean the  $O_2$  set point would need to be increased to completely burn the fuel and avoid a potential combustion swing into a “fuel rich” operating area.

## **COMBUSTION SAFETY**

Since the detection of low oxygen and/ or high combustibles (CO) in a combustion process can also determine unsafe operation, the combustion analyzer is now evolving from just a process analyzer providing “air to fuel ratio” feedback to the BPCS, to the utilization of the analyzer for implementation of “Safety Instrumented Systems” per IEC 65108/ IEC 61511 independent of the control system to provide operational permissive and interlocks to limit unsafe control or to shut the process down in the event of an identified uncontrollable state of operation.

The new guidelines of IEC 65108/ IEC 61511 and ISA 84.01-2004 are currently being used to implement these combustion SIS systems. Even where the application of these new guidelines are not yet mandatory, still governed by NFPA 85/86 or OSHA, global users have already started to apply the new standard to new or existing installations for three key reasons. First, global users recognize that adopting a single standard for all of their sites provides consistent engineering and maintenance practices, potentially reducing design, procurement and documentation costs. Second, users in most jurisdictions recognize that the IEC standard will eventually become mandatory. Finally, the new standard potentially provides users with flexibility to improve safety and availability, while reducing maintenance costs. For instance, with the right equipment and installation, the new standard may allow the user to significantly stretch out calibration and inspection intervals.

## **THE SAFETY INSTRUMENTED FUNCTION AND THE SAFETY INTEGRITY LEVEL**

A Safety Instrumented Function (SIF) is defined as a “function to be implemented by a SIS which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event”. A SIS can consist of one or many SIF functions and each SIF usually incorporates one or more sensors for redundancy. During a “Hazard Analysis & Risk Assessment”, the SIS committee will review the various control parameters in a particular SIF for a process and determine each control loops potential to bring the process to a catastrophic state either by control, final element, soft logic and/or operator failure, and is assigned a risk level, or “Safety Instrumented Level” (SIL) which dictates the required equipment integrity and redundancy required to achieve the required SIS availability to mitigate a potential event. The basic factors considered for determining the required SIL level are the potential severity of the event, the frequency of the event occurring, and how much risk needs to be reduced to place the potential event into an acceptable level of risk.

An important consideration in the SIL rating of a combustion analyzer is the required safety availability and the Probability of Failure on Demand (PFD)

Several manufacturer's now make available SIL certified equipment which have been reviewed and tested by a third party agency to IEC 61508 and IEC 61511, and publish the failure rate data in the same way as temperature specifications or accuracy figures, as well as having their equipment certified to a specific SIL function level.

It is important to note that no device can actually be certified at a SIL 1, 2, or 3 devices. The only thing that can be actually classified as SIL 1, SIL 2, or SIL 3 is the Safety Function itself. Devices such as combustion analyzers can only be certified as "SIL 1, 2, or 3 Capable" where their Architectural Constraints (Safe Failure Fraction) and their Probability of Failure on Demand (PFD) determine their suitability for use in the Safety Instrumented Function.

## **FMEDA OR "PROVEN IN USE"**

IEC 65108 describes two valid approaches for selecting combustion analyzers and obtaining data for SIS calculations-"validated/ certified" devices or "proven in use.

The letters FMEDA form an acronym for "Failure Model Effects and Diagnostics Analysis" which is a systematic analysis technique to obtain subsystem/ product level failure rates, failure modes, and diagnostic capabilities This is completed by an independent third party organization, such as Exida or TUV, where the analyzer is reviewed and tested and failure rate and failure mode data is generated for use in SIS calculation. An important aspect to the FMEDA is the analyzer's ability to detect internal failures and weaknesses in operation through automatic on-line diagnostics.

"Proven in Use" is where a user documents operating experiences such as failure rates, repair histories, calibration records, and longevity of their own combustion analyzers installed in SIS and basic process control applications to determine failure rate and failure mode data through the entire life cycle of the analyzer.

There are advantages and disadvantages to both approaches. Using certified devices transfers the burden of calculating and documenting device safety from the user to the supplier. This reduces cost, especially for the small user who might not have the resources to perform their own Prior Use analysis. Unfortunately, data from third party SIL certified analyzers are based on calculations and laboratory analysis and cannot qualify the impact of real world effects. Analyzers installed in a process environment, as opposed to the laboratory, are exposed to extreme temperatures, vibration, installation abnormalities, poor sample gas, or poor maintenance practices which could cause the analyzer to read false high or false low, that might not be detected during normal operation, and would affect the Safe Failure Fraction (SFF) and/or the Probability of Failure on Demand (PFD) data.

In practice, users are gravitating towards an approach which combines the best of both the FMEDA “validated/ certified” and the “Prior Use” approach. The user can start with the third party certified data supplied with the SIL capable certified analyzer for the SIS calculations and determination of calibration and SIF inspection intervals, and then through real world data from the installed analyzer, record pertinent operational data into an Asset Management System, and adjust calibration and inspection intervals through a preventative/ proactive maintenance program.

## **COMMON CAUSE STRENGTH**

Using either of the FMEDA certified or the Prior use approaches, it becomes evident that a combustion analyzer itself could be a trivial component of the overall risk of a dangerous failure. Consider a SIL 2 capable analyzer poorly mounted on a waste fuel boiler sampling particulate laden gas. Even though the analyzer has laboratory failure data and has prior use data installed in other areas of the plant on natural gas, an undetected sample system blockage could cause an undetected analyzer failure and a catastrophic combustion event.

Common cause strength is improved with communication technology. Combustion analyzers today installed in control and safety applications must have the ability to not only have internal diagnostics to determine component and analyzer failure, but also have the ability to detect degradation of analyzer operation or sample flow before a critical failure or event can take place. Internal diagnostics and the availability of this diagnostics information to the logic solver, operator, Asset Management System, and maintenance scheduling are crucial to the effectiveness of the analyzer and to maximize availability of the analyzer to the SIS and to the basic control system. Further, this information from the analyzer can be collected and provide an audit trail of failures and corrective actions to establish predictive and proactive maintenance programs as well as developing and refining prior use data. Calibration frequency and inspection intervals could be extended longer saving maintenance time and dollars.

## **COMBUSTION ANALYZER TECHNOLOGY**

In the author’s opinion, Close Coupled extractive Zirconium Oxide (ZrO<sub>2</sub>) based O<sub>2</sub> analyzers are the analyzer of choice for SIS and Basic Process Control installations due to their fast response, ease of maintenance, and their ability to measure CO and CH<sub>4</sub> with one process penetration. Close coupled extractive analyzers can measure hot dirty flue gas near the radiant zone with gas temperatures up to 2000F, and have an established reliability record in the application, providing the most reliable and accepted measurement for Oxygen. ZrO<sub>2</sub> sensors provide an extractive “point type” measurement and are “net oxygen” analyzers which are heated and utilize platinum electrodes with catalytic properties to determine oxygen concentrations of

flue gas. They will, however, burn any combustible compounds with oxidation potential such as hydrocarbons, CO, Hydrogen, and high concentrations of sulphur dioxide. During combustible flood conditions, H<sub>2</sub> and CO are the largest combustible components and they will consume oxygen in the flue gas sample as they combust on the zirconium cell. The ratio of consumption of combustibles to oxygen is 2:1, thereby, if 1000ppm combustibles is present in the flue gas, 500ppm of O<sub>2</sub> will be consumed from the flue gas sample. This decrease of the oxygen reading due to the burning of combustibles is normally considered negligible. Due to the operating principle of Zirconium Oxide sensor having to operate at 695 deg. C to function, this does create concern that the sensor could cause combustible vapors to ignite on heater light off. Shut down, or in a “non-operational heater” outage state. Precautions are met by the installation of “Flame Arrestors” before and after the measurement section of the analyzer to suppress any ignition as well as the possibility of back-purging the sensor with instrument air to prevent vapors from entering the sensor, or removal of sensor power in an outage situation.

The addition of catalytic bead type combustible sensors can be added to the close coupled extractive analyzer O<sub>2</sub> sample system to provide independent measurements of PPM combustibles and percent levels of Methane. These sensors, treated with a catalyst to allow combustible compounds to burn on them at below ignition temperatures, are calibrated with combustible gas they are designed to detect. The PPM combustible detector will respond to CO as well as H<sub>2</sub>, with both normally present in fuel rich combustion when burning hydrocarbons, and this reading is considered the feedback for O<sub>2</sub> trim as well as the indication of a CO flood condition. The Methane detector is calibrated strictly for Methane and is utilized as a permissive for a “Purge & Light Off” cycle to detect any methane present before the burners are lit. It can also utilized on shutdown where combustible fuel can accumulate as the process heater begins to cool.

The combustion analyzer is normally mounted by a flange connection and extracts a combustion gas sample by an air aspiration into a fast sample loop where a small portion is directed to the combustion sensors for measurement.

Control electronics for the combustion analyzer can either be internal to the combustion analyzer sensor or remotely mounted from the sensor up to 1000 feet away from the process penetration. Analog outputs with superimposed HART, discrete contact alarms, MODBUS, TCP/IP Ethernet, and web enabled interface are available for control and communication.

Most installations also include a Remote Calibration Unit (RCU) which allow the automatic or manual injection of calibration gas to the sensor for periodic verification or calibration.

## **COMBUSTION ANALYZER DIAGNOSTICS**

The proper combustion analyzer design for accurate measurement, maximum availability, minimal maintenance and testing frequencies, and unnecessary process shutdowns requires the analyzer to have the ability to continually perform performance and health status and be able to

communicate the need for service when appropriate. With this, maintenance and calibration staff can avoid unnecessary time in the field and in hazardous areas reducing operational costs and spurious process trips can be avoided

Combustion analyzers must have the ability to communicate as many parameters and diagnostics to the basic process control system or logic server, Asset Management System, Maintenance personnel, and engineering staff as possible. This is typically achieved through a MODBUS or HART type digital communication, TCP/IP Ethernet based communication to the plant LAN, or by utilizing a USB Data port to collect archived data in the analyzer itself.

Diagnostic and Alarm parameters that combustion analyzers should have available includes:

Zirconium Cell: Sensor resistance measurement for the detection of “open” or cracked cell due to a ceramic sensor installed in a high temperature, high vibration environment.

Zirconium Cell Temperature: Verification error of proper cell temperature by redundant thermocouple readings of actual cell temperature.

Combustible Sensor: The detection of sensor failure based on sensor bridge imbalance.

Enclosure Temperature: Detector stability and sample system heat to maintain combustible sensor accuracy and integrity of sample system above sample dew point.

Sample Flow: Detection of low or no sample flow to the sensors to indicate a suspect sample system for flame arrestor degradation.

Sensor Age Tracking: End of life prediction with alarm to signify end of life limit on sensors so as to plan for required maintenance.

Calibration Required: Warning that calibration is needed when sensor sensitivity decreases beyond a targeted value.

Analog Output Verification: Compares analog output value to digital value for accuracy in analog variable translation.

## **ASSET MANAGEMENT SYSTEMS**

Asset Management Systems is a necessity and is here to stay for any Basic Process Control System (BPCS) or Safety Instrumented System (SIS). The ability to track analyzer performance, repair history, calibration accuracy, and the required maintenance throughout an analyzer life cycle can only increase availability to the BPCS or SIS and identify troublesome installations or weakness in a measurement installation. This information would be critical to “prior use” data

for SIS documentation and can reduce unjustified process downtime. Calibration and inspection times can be reduced saving the user personnel work hours and unjustified expense.

A key to analyzer selection is that the combustion analyzer provides enough information required in a proper format to populate such a data base. One should evaluate the diagnostic information available through an appropriate media such as MODBUS, Ethernet, or HART. A web enabled interface can also be a useful tool for maintenance personnel to address alarms in the BPCS or SIS as informed by operators through the plant LAN network.

## **DISCUSSION**

The choice of a combustion analyzer for BPCS or SIS takes more consideration than just the fact that is “SIL” approved/ capable. One must realize that besides the basic functions for control, there are a lot of additional parameters that the analyzer can provide to improve safety, availability, and to reduce maintenance time involved throughout the analyzer life cycle.

Is the analyzer third party SIL certified capable? Can we install the analyzer in the process effectively to eliminate environmental and installation effects? Can we utilize more than just a combustion control output or safety function to minimize maintenance costs and increase availability? Will the combustion analyzer interface to our existing plant communication network? Does the manufacturer have the experience and installed base in our application to accept and believe the “failure data” provided by the third party based on a “laboratory” environment?

## **CONCLUSIONS**

International standard IEC 61508 is gaining traction within the process industry and most combustion control systems and safety systems will be designed around this specification going forward in the years to come. The equipment standardization, risk reduction, and the traceability and maintenance savings, more than justifies the implementation of applying these standards to BPCS and SIS type systems. The user must evaluate whether a “SIL” approved type device has the appropriate “Probability of Failure on Demand for the SIF, the application history and installed base for “prior use” evaluation and documentation, and the required information available in a “plant friendly” media to populate plant data bases which will be used for future calibration and maintenance reduction programs through Asset Management Systems.



## REFERENCES

### BOOKS

1. Gruhn, Paul and Cheddie, Harry: *Safety Shutdown Systems: Design, Analysis, and Justification*. (ISA, 1998), ISBN 1-55617-665-1
2. Goble, William and Cheddie, Harry: *Safety Instrumented Systems Verification: Practical Probabilistic Calculations*. (ISA, 2005), ISBN 1-55617-909-X.
3. O'Brien, Chris and Bredemeyer, Lindsey: *Final Elements: & the IEC 61508 and IEC 61511 Functional Safety Standards*. (Exida, 2009), ISBN-13: 978-1-934977-01-9

### REPORTS

1. Schwartz , William A., Hochleitner , Monica L: *3 Important Factors in Evaluating your SIL Certified Device*. (January 2007), <http://www.exida.com>.
2. Goble, Dr. William M: *Field Failure Data-the Good, the Bad, and the Ugly* (Dec 2000). <http://www.exida.com>.
3. Grebe , John C., Goble, William M.: *FMEDA-Accurate Product Failure Metrics* (Feb 2007, <http://www.exida.com>).
4. Brown, Stephen R., Menezes, Mark: *Measurement best Practices for Safety Instrumented Systems*. (Oct 2005), ISA EXPO 2005