

Fire And Gas Systems

Effectiveness and Functional Safety

By *Mr. Valeriano Barrilà*



Mr. Valeriano Barrilà is Technical Director of SA Fire Protection S.r.l. and has an extensive experience in Industrial Fire Suppression for onshore and offshore industrial complex. Mr. Barrilà holds a BEng in Engineering from the University of Pisa, Italy and an MSc in Fire Engineering from Ulster University, UK. Mr. Barrilà is a Chartered Engineer MIEI of Engineers Ireland and the inventor of VDD model of deluge valves.

After the major accidents occurred in the Oil & Power industry in the last ten years, the technical community involved in the design of industrial processes has shown an increased and more intense interest in system reliability and availability. The attention is no longer limited to the core process but is also extending its boundaries to all those safety systems to which the monitoring and the mitigation effects are demanded.

If it is paramount that a process shall be designed with high reliability criteria, sometimes it is not fully understood that the process reliability cannot rule out the risk of an accident taking place. Engineering limitations also apply to a stressed safety oriented design approach and therefore, one way or another, systems are finalized and built accepting a certain level of residual risk.

If the risk of an accident cannot be lowered below a certain point, we should focus our attention on those systems designed to monitor the environment and provide mitigation effects. Those process sub-systems, such as Fire & Gas, deluge, monitors and gaseous based fire extinguishing systems, play a fundamental role in the safety of the plant and its occupants.

These systems are called into action when the residual risk of the hazard turns into an accident of major consequence, and their duty is to warn the occupants and the operators and mitigate the accident effects to the best of their capabilities. In this respect, it is well known that a gas cloud detected and confined in time or a fire outbreak detected and extinguished by a deluge water spray system have the same objectives: saving lives, limiting the impact on the environment, reducing the production losses and safeguarding investments.

For the reasons above, functional safety is moving into Fire & Gas detection and suppression systems, with the objective of increasing the reliability and hence the performance of the safety functions used to monitor and mitigate the effects of a possible accident.

IEC 61508 AND IEC 61511

Safety is the acceptable reduction of an unacceptable risk of physical injury to people or damage to the properties. Functional Safety is part of the overall safety that depends on a safety-related system operating correctly in response to its input.

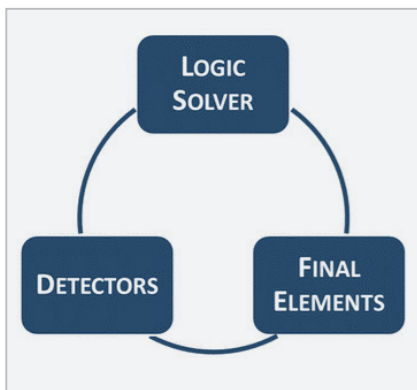
The significant hazards for the system have to be identified via a hazard analysis. If the hazard analysis shows that functional safety is necessary, appropriate systems are required to perform specific Safety Functions to reduce the risk. These systems are called Safety-Related Systems or Safety Instrumented Systems (SIS).

Two types of requirements are necessary to achieve Functional Safety:

Safety Function Requirements: the scope of the safety function, derived from the hazard analysis.

Safety Integrity Requirements: the probability that the safety function will be performed satisfactorily, derived from the risk assessment.

The Standard IEC 61508 "Functional Safety of electrical / electronic / programmable electronic (E/E/PE) safety-related systems" covers the safety lifecycle of the product, from the initial concept through hazard analysis and risk assessment, development of safety requirements, specification, design and implementation, operation and maintenance. IEC 61508 contains requirements for preventing failures and controlling failures, ensuring safety even when faults are present. It specifies the techniques



and measures to achieve the required Safety Integrity.

The Standard IEC 61511 “Functional Safety – Safety Instrumented Systems for the process industry sector” covers the safety lifecycle of the installation and contains the requirement for the correct selection of safety related equipment and the erection of Safety Instrumented Systems. IEC 61508 specifies alternative techniques to determine the Safety Integrity of the installation.

The Safety Integrity is the probability that the Safety Instrumented Systems will perform the required Safety Functions satisfactorily. IEC 61508 specifies four levels of safety performance for a safety function, called Safety Integrity Level (SIL): SIL1 is the lowest level and SIL4 the highest level.

Each Safety Integrity Level is correlated with an increased Risk Reduction Factor (RRF).

IEC 61508 details the requirements necessary to achieve each Safety Integrity Level.

The table provides the target failure measures for a safety function allocated to a SIS operating in low demand mode. Low demand mode means that the frequency of demands for operation of the SIS is not greater than once per year, and not greater than twice the proof-test frequency.

FIRE & GAS SYSTEMS

The tasks of a F&G system are to detect any hazardous fire or gas

TABLE 1. IEC 61508 REQUIREMENTS TO ACHIEVE EACH SAFETY INTEGRITY LEVEL

Safety integrity level (SIL)	Average probability of failure on demand (PFDavg)	Risk reduction factor (RRF)
4	≥ 10 ⁻⁵ to < 10 ⁻⁴	10.000...100.000
3	≥ 10 ⁻⁴ to < 10 ⁻³	1000...10.000
2	≥ 10 ⁻³ to < 10 ⁻²	100...1000
1	≥ 10 ⁻² to < 10 ⁻¹	10...100
0	Basic Process Control Systems (BPCS)	

condition, to alert the personnel in the area and to activate the control and mitigation systems.

The F&G system effectiveness is the product of the following three factors:

- Detection Coverage: the fraction of the monitored area in which an eventual fire or gas hazardous condition would be detected.
- Mitigation Effectiveness: the probability that the activation of the Final Elements would reduce the consequences of a defined hazard.
- F&G Safety Availability, SA: it is connected to the Probability of Failure on Demand (PFDavg) by the following equation: 1-PFDavg. The PFDavg measures the Safety Integrity Level (SIL) of the system.

The Safety Availability of a F&G system can be evaluated through a Fault Tree Analysis (FTA) based on the PFDavg of each component. The main components of a F&G system are the following:

- Fire, Gas or Heat Detectors
- Logic Solver
- Final Elements (Deluge system, Shut Down system, etc.)

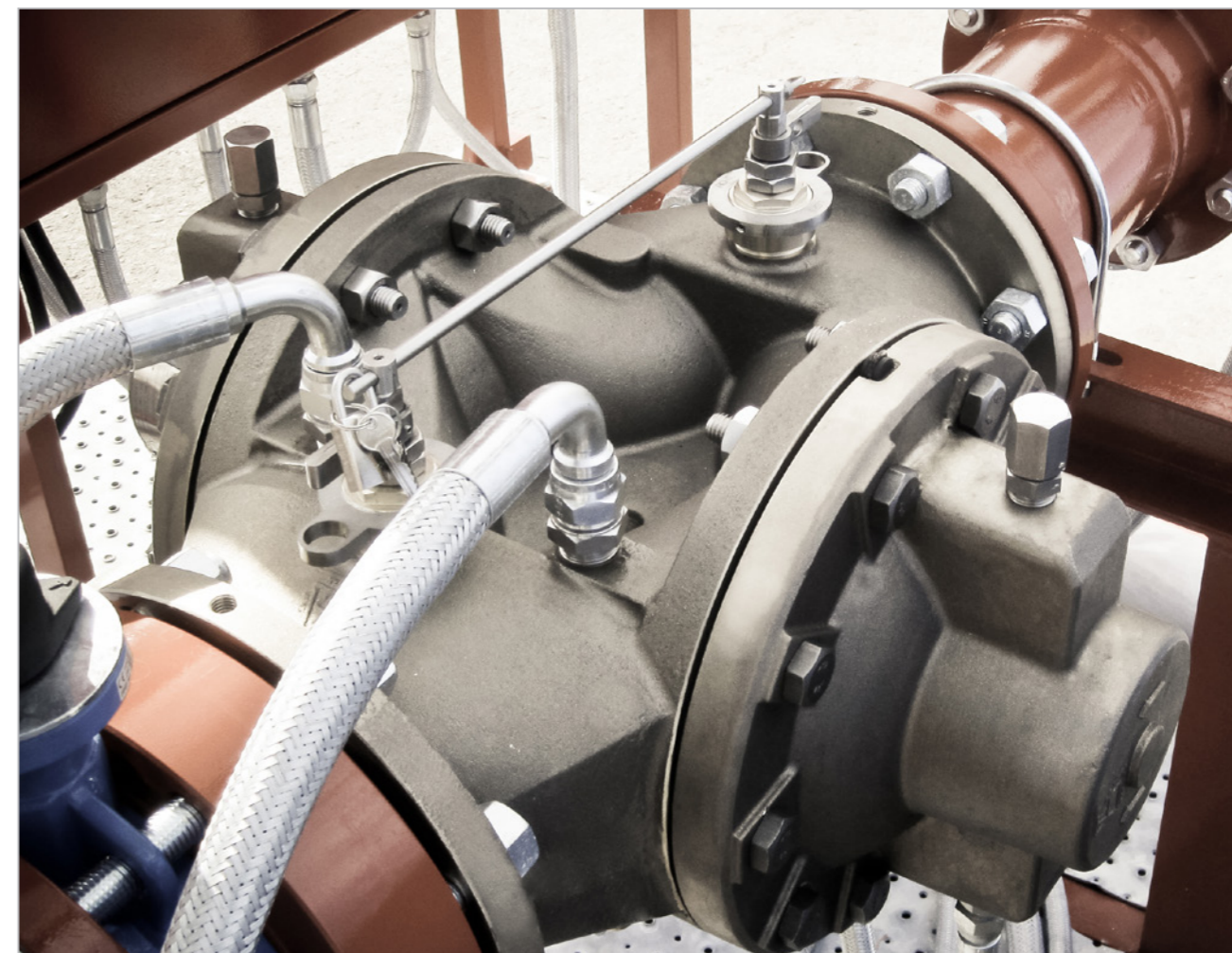
SIL SUITABLE FINAL ELEMENTS

So far the manufacturers’ efforts to meet the functional safety criteria for F&G systems have focused mainly on electric and electronic devices, providing components suitable for increasing SIL level systems according to the desired level of functional safety.

However, the F&G system effectiveness is related to the Safety Availability of all its components: the overall performance of the system is affected by the weakest element of the chain of its components.

This is the reason that has led SA Fire Protection to focus its attention on the Final Elements, developing the following SIL suitable solutions according to IEC 61508 for the main types of fire protection systems (i.e. deluge water spray systems, monitors and gaseous based systems):

- The Double Chamber Deluge Valves Model VDD, suitable for SIL3 systems
- The Double-Coil Electric Actuators for gaseous based systems, suitable for SIL2 systems
- The Electric Monitors Niagara Series, suitable for SIL2 systems



The SA SIL suitable Final Elements are validated by Bureau Veritas for integration within safety functions performing fire protection service in low demand mode.

DOUBLE CHAMBER DELUGE VALVES MODEL VDD

The deluge valve Model VDD is an innovative concept valve designed for fire protection systems according to NFPA 15, UL 260 and IEC 61508/61511. The VDD deluge valve combines all the functions available on the traditional deluge valves with a fully redundant architecture, designed to achieve higher reliability. In fact, the VDD deluge valve has two priming chambers, each one provided with its own diaphragm and actuation trim, which offer two independent waterways to the water spray system. Each priming chamber provides the nominal design waterway for the fire protection system: in case of failure of one diaphragm, the opening of the other diaphragm allows the hydraulic waterway for the correct operation of the water spray system.

In practice this new concept translates into a built-in emergency bypass line that operates on both priming chambers in hot back-up.

Moreover, a hydraulic bridge between the trims allows each trim to control both the diaphragms, releasing the water trapped in the two priming chambers. If one trim should fail, the other trim can open both the priming chambers through the hydraulic bridge. Thus the double chamber deluge valve can overcome a double failure trim + priming chamber.

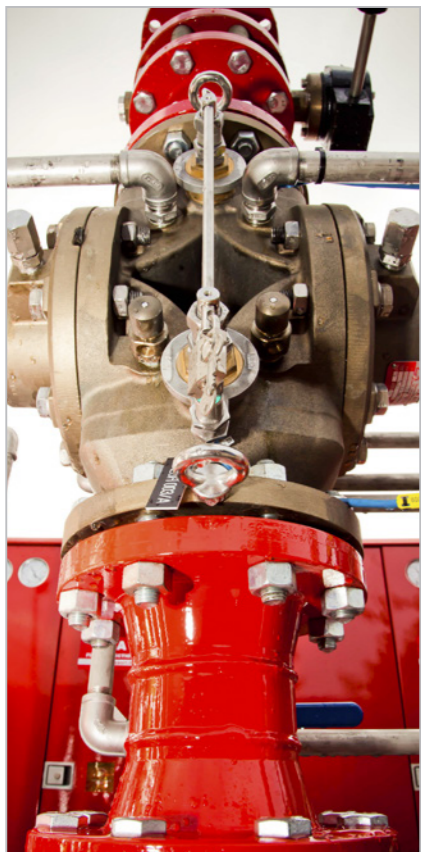
Advantages:

The advantage of using the VDD deluge valves can be measured in terms of increased reliability, lower response time and easier system operations.

1. Increased deluge system reliability and availability on demand (SIL 3 Validated by third party)
2. Response time to failure reduced to zero
3. Continuous fire protection (no downtime for service or even repairs)
4. Deluge skid dimension & weight can be reduced accounting on the built-in by-pass in hot back-up

Application:

Model VDD deluge valve is specifically designed for industrial harsh



environments such as oil & gas onshore and offshore, chemical, conventional or nuclear power, military and those which require:

1. A low probability of failure on demand
2. A safety instrumented system with a deluge system as final element capable of being integrated into SIL 3 systems
3. Continuity of fire protection during maintenance or repair
4. Reduction of weight, dimensions and cost of the skid.

Application typical include fire suppression or cooling of critical process equipment, toxic vapour mitigation and confinement.

DOUBLE-COIL ELECTRIC ACTUATORS

Gaseous based fire extinguishing systems include carbon dioxide, inert gases and halocarbons. All of them are kept pressurized into cylinders or containers ready to be discharged to the protected area. On a similar principle, water mist systems are made of a series of water cylinders propelled by a nitrogen reserve contained in a pilot cylinder. Normally these systems are composed of a series of sensors, a logic controller and a final element, which is often represented by a pilot cylinder.

When such systems are called for duty a missed activation of the pilot cylinder can lead to an unacceptable consequential scenario. SA pilot actuators have been developed for sensibly reducing the probability of such failures, increasing the Safety Availability of the fire extinguishing system. They have been validated by BV as suitable for safety instrumented systems with an expected SIL2 level. When used in combination to form external activation packages the actuator can contribute to form architectures that can be qualified to SIL 3.

Advantages:

The redundancy of the double-coil electric actuator increases the reliability of the overall pilot cylinder. The actuator has two coils which receive two independent signals from the logic controller (F&G). If one coil fails, the other coil is able to open the cylinder valve. On the same principle these redundancy increase the overall system availability as the loss of one cable or the failure of the F&G discharge cards do not compromise the fire suppression system activation.

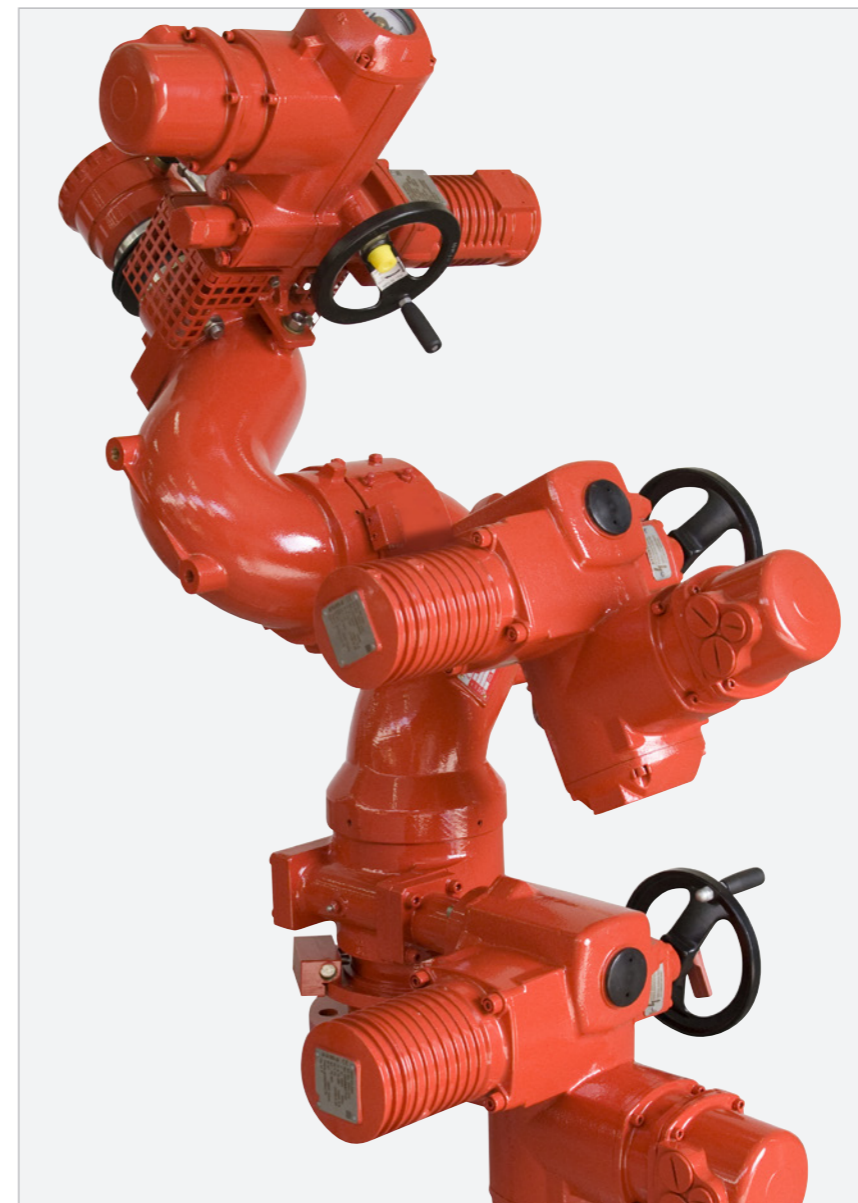
Such solution has been implemented to cover all those fire hazards which require an increased reliability for the fire extinguishing system and, therefore, a safety function with an expected SIL2 level.

Applications:

The double-coil actuator is designed for those systems which require:

1. A low probability of failure on demand
2. A safety instrumented system with a gaseous based fire protection system as final element, capable of being integrated into SIL2 systems
3. The combination of a high safety integrity level with low dimensions and weight.

The double-coil electric actuator is specifically designed for the protection of gas turbines and their generators, critical IT server farms, electronic rooms governing industrial processes, and all general purpose installations on offshore



The increased reliability performance of the Niagara series monitor is related to its particular design, which allows an automatic self-diagnostic analysis to be performed. At regular intervals the self-diagnostic system implemented in the Logic Controller checks the correct operation of the monitor actuators on given commands, allowing for constant monitoring of any possible failure of the monitor and the nozzle. In case of an anomalous condition, a warning signal is sent to the control station.

Advantages:

A possible failure of a traditional electric remote controlled monitor can be detected only when periodic maintenance and test are performed. The constant monitoring of the system status implemented in the Niagara series monitors, instead, allows a possible failure to be detected and repaired when the fire protection system is in "safe condition", sharply increasing the reliability of the overall fire system on demand. Such improvement reduces the probability that faults, taking places among regular maintenance intervals, will pass undetected.

Detecting a possible fault in a safety system in time, rather than in a fire condition, can make the difference on the emergency operation success.

Application:

The Niagara series monitors are specifically designed for petrochemical jetty and marine harbor protection, structure and vessel cooling, and those systems which require:

1. A low probability of failure on demand
2. A safety instrumented system with monitors as final elements capable of being integrated into SIL2 systems
3. A large amount of water towards remote targets. ■

platforms or FPSO, where generally a fire brigade is not easily available to compensate a possible fire-fighting system failure.

ELECTRIC MONITORS NIAGARA SERIES

The Niagara electric type remote controlled monitors are designed to deliver large amounts of water or water foam solution towards remote targets. They are commonly used to protect petrochemical jetty or within the process areas to cool structures, vessels or fight potential fires of a considerable magnitude.

From the safety availability point of view, the remote controlled monitor architecture comprises of a Logic Controller and one or more final elements (Monitor assembly). The logic controller is the heart of the system and distributes the commands to the monitor itself. In such system, or at least in the simplest version, the detector is not normally integrated and the system respond directly to human actions.

The Niagara monitors have been assessed and validated by BV as suitable for safety instrumented systems with an expected SIL2 level.