Functional Safety

Fire Protection Solutions

SIL Fire Systems

Foreword

After the major accidents which have happened 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 safety 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 must 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 finalised 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, their duty is to warn the occupants and the operators and to 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 deluge water spray 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.

Functional Safety

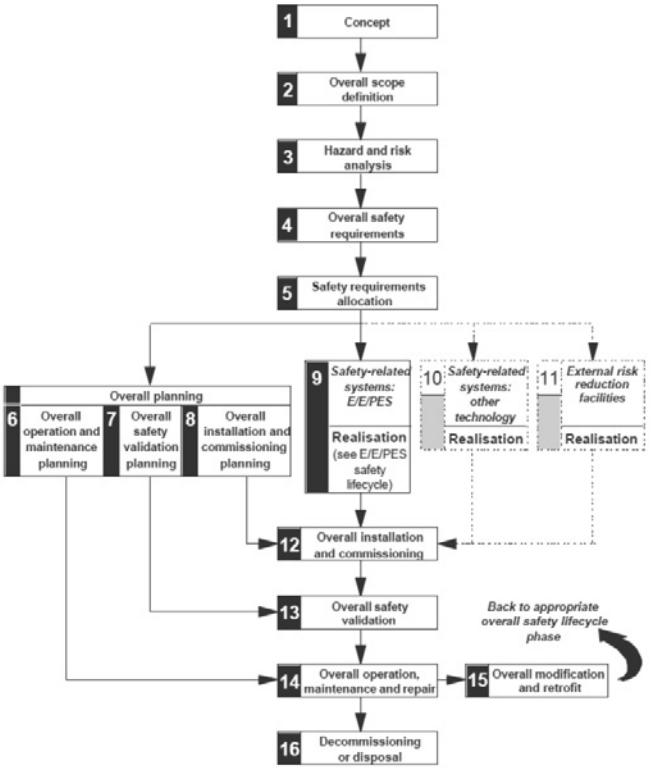
Safety is the absence of an unacceptable risk of physical injury to people or damage to the properties. Functional Safety is part of the overall safety that depends on a system or equipment operating correctly in response to its input.

The significant hazards for the system have to be identified via 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 all the safety lifecycle activities, 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.

IEC 61508 specifies 4 levels of safety performance for a safety function, called Safety Integrity Level (SIL). SIL1 is the lowest level and SIL4 the highest level. The Standard

details the requirements necessary to achieve each Safety Integrity Level.
The table below 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

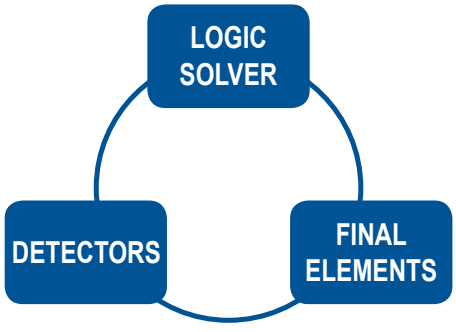
The tasks of a F&G system is to monitor environmental conditions and to detect any hazardous fire or gas condition related to an emerging fire or gas leakage. The systems are designed to alert the personnel in the area and to activate the control and mitigation systems. More often the F&G system is comprised of one or more control panels each of

Safety Integrity Level (SIL)	Average Probability of Failure on Demand (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

which is interconnected with field detectors, signaling units and actuators. The panel and the detectors are monitored in order to distinguish any environmental deviation that can be connected to irregular environmental conditions. This is the case in detecting the presence of Smoke, Heat, Flame or Gas either combustible or toxic within the monitored area. Furthermore, the panel and the monitoring instrumentation are analysed to validate the condition of the firefighting systems. The trip function is correlated with other superior systems such as the ESD or DCS and it is used to transfer the confirmation that certain hazardous conditions have been detected. When hazardous conditions are detected. The mitigation systems (water or foam deluge skid) will be actuated with the purpose of containing a gas cloud or to suppress an emerging fire.
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;
· Deluge system, Shut Down system, etc. (Final Elements).

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 rated 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 in the chain of its components.



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

· The Double Chamber Deluge Valves Model VDD, suitable for SIL3 systems;

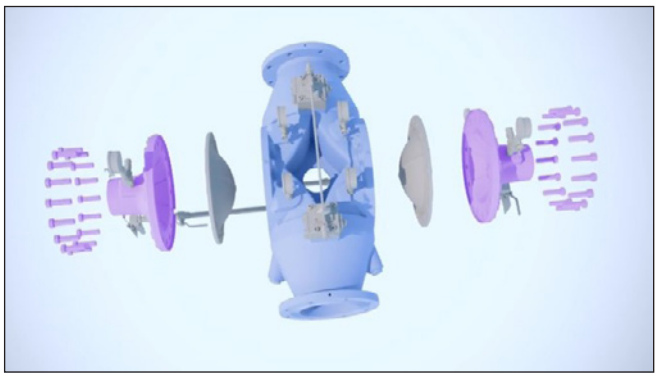
· The Electric Niagara Monitor Series, suitable for SIL2 systems;

· The Double-Coil Electric Actuators for gaseous based systems, suitable for SIL2 systems.

The SA Fire 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 Valve 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

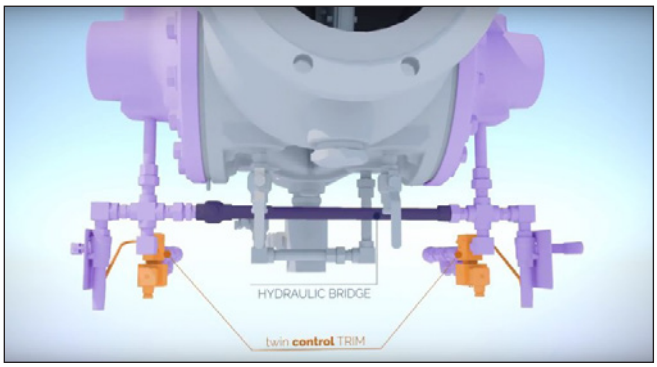


valve combines all the functions available on the traditional deluge valves with a fully redundant architecture, designed to achieve higher reliability.

In fact, the VDD deluge valve has two priming chambers, each one provided with its own diaphragm (made of EPDM reinforced with Nylon) 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 in the trim + priming chamber.



Advantages:

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

The subsequent example is often used to describe the VDD valve's performance. Consider a fire or gas emergency condition where the deluge system has to be actuated to respond to a fire outbreak or to mitigate a gas cloud detected by the F&G.

All the deluge systems commonly used comprise of a main deluge valve and an external bypass line, installed on the deluge skid, intended to provide manual actuation should the deluge valve fail on demand. It is when similar scenarios take place that the VDD deluge valve makes the real difference. The VDD design can overcome a double failure affecting the whole valve assembly, meaning that it is very unlikely for the VDD valve to fail on demand.

Besides its increased reliability, which by itself is essential when fighting a fire or an expanding gas cloud, the time required for the VDD to respond to a failure affecting the valve is reduced to zero.

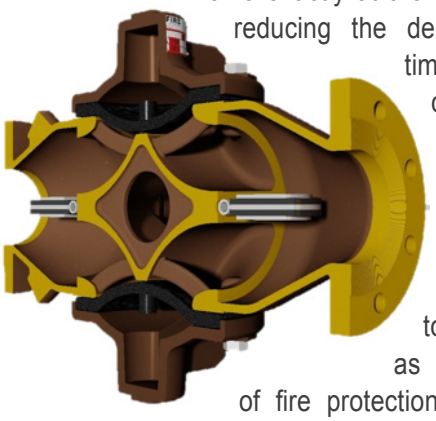
Looking back at the traditional deluge valves, the time needed for the operator to respond to a failure can be summarised as follows:

TR = T1+T2+T3+T4

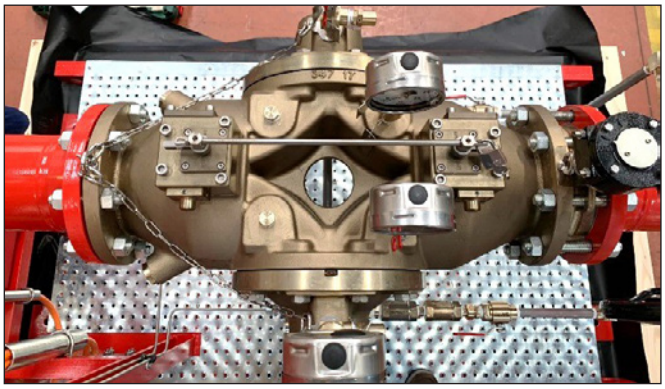
Where:

TR = Time required to respond manually and activate the water spray system via the bypass line.

T1 = Time needed from signal sent via logic controller or manual activation to come back to Control Room signalling that deluge valve did not open.
T2 = Time needed for operator to analyse the signal and initiate emergency procedures.
T3 = Time needed for operator to respond to a given emergency message
T4 = Time needed for the operators to reach the failed deluge skid and open the bypass line.
Anyone can argue about the length of each time interval shown above, but the final conclusion is always the same: the time for VDD to respond to a failure is zero.
The reason is simple and lies in the fact that the procedures required to operate standard deluge skids are not necessary with the VDD valve. In fact, the VDD deluge valve responds automatically to any failure affecting the valve exactly at the same time as it occurs, reducing the deluge system response time to zero even in faulty conditions and granting the opening of the valve.

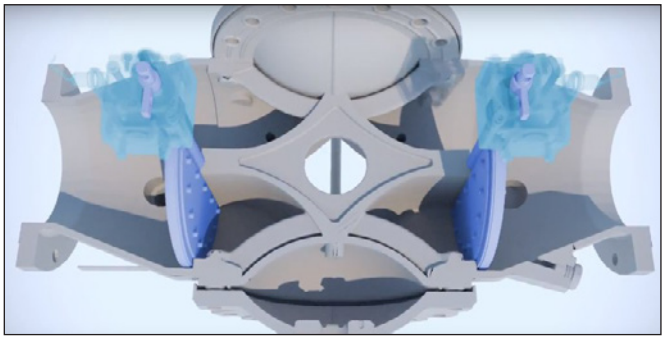


Another advantage is the limited operational man power required to operate the system as well as the continuity of fire protection service, which allows equipment to always be protected.
It is in fact good common practice for owners & operators to perform maintenance of their fire systems on a regular basis, following the procedures given by NFPA 25 and their deluge valve manufacturer.
When performing an internal inspection of a deluge valve or cleaning the filters and orifices of the trim, there is no possibility of keeping the deluge valve in service and, therefore, the system must be completely isolated. In such cases, operators have very little choice and are left with two possibilities: shutting down the production process or keeping an operator, who is in contact with the control room, “nearby” the bypass line of the deluge valve, ready to open water. With the VDD deluge valve these issues will no longer be on top of the operator’s head.
The new deluge systems equipped with the VDD deluge valves will be subject to maintenance or repair with the exact same frequency and procedures required for traditional deluge valves. The main difference concerns the protected plant process which does not require shutting down. This reduces all production losses, due to fire protection impairment, to



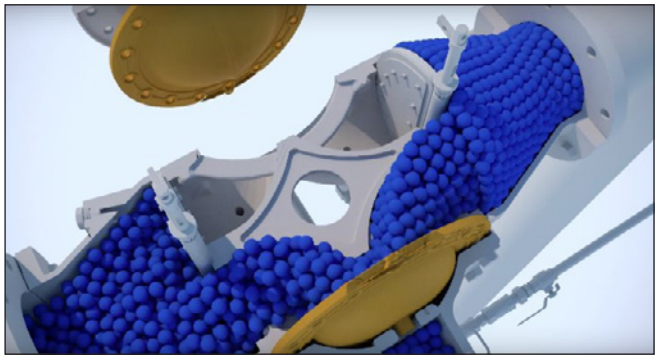
zero. Last but not least, the operators are not required to stand by the deluge bypass line during maintenance or repair.

All this is possible because of the VDD deluge valve’s redundancy, the maintenance isolation mechanism and the distributed activation trim.
When deciding to perform maintenance or repair on a VDD deluge valve, the operator can work on the external of the VDD valve unlocking the isolation system. This allows the isolation of one of the two chambers. The chamber must be isolated downstream and upstream by the two built-in isolation valves and the interlock system must be repositioned to move forward. The interlock system is designed to fit and close only when the valve chamber is correctly isolated, to prevent human error and increase the overall reliability of the VDD assembly. The following operation is to isolate the trim closing specific valves. In this way, the operators can work on the isolated trim and chamber and can even perform the internal inspection of the chamber as prescribed by NFPA 25. While working on one chamber, the other chamber remains in operation providing continuous fire protection.
Once the inspection procedures of the first chamber are finished, the isolation system may be moved towards the other chamber to complete the inspection.



An external indicator and proximity sensors provide visual and remote information on the isolation status of the VDD

valve. So, the control room can monitor the maintenance work and receive feedback about the valve status after the inspection.



The built-in isolation device grants continuous fire protection, and therefore does not require the user to alert the local fire brigade every time the deluge valve is under maintenance or repair, as required by NFPA 15 and NFPA 25.
From the designer prospective, the VDD deluge valve combines high safety availability with low weight and small dimensions of the deluge skid. The integrated redundancy and hot back up rule out the need of an external bypass line on the skid, sensibly reducing weight, dimensions and cost of the whole skid.
The VDD deluge valve concept has been developed by SA Fire designers in order to meet the criteria set forth in IEC 61508 and therefore providing the highest reliability possible for water/foam fire systems meant to provide mitigation effects and likely to be involved in life saving actions.
Thus, the design in terms of functional safety has become of paramount importance for systems performing safety functions, and particularly for fire suppression systems. This is the reason that has led SA Fire to develop firefighting equipment designed to meet Safety Integrity Level (SIL) criteria according to IEC 61508.

Minimum SIL ratings for deluge systems intended for fire protection in the Oil & Gas and Power generation plants, are already recommended by the major international organisations.

As an example, the Norwegian Oil Industry Association recommends ("Recommended Guidelines for the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian Continental Shelf") a minimum SIL2 level for the "deluge valve including actuator, solenoid and pilot valve".
For these installations requiring high safety function performances, SA Fire has specifically developed and patented the Double Chamber Deluge Valve Model VDD, designed to overcome double failure.
The VDD valve is available in diameter sizes from 3" (DN 80) to 8" (DN 200).
Model VDD is used to control water flow in deluge, pressure reducing and ON/OFF systems. It can be controlled manually and automatically by electric or electro-pneumatic release systems.
The deluge valve model VDD is validated by Bureau VERITAS (BV) for being used in safety instrumented functions with an expected SIL3 level in low demand mode, when equipped with electric, electric ON/OFF, electro-pneumatic and electro-pneumatic ON/OFF trim. VDD is UL/cUL Listed.

Application:
Model VDD deluge valve is specifically designed for harsh industrial 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 SIL3 systems;
3) Continuity of fire protection during maintenance or repair;
4) Reduction of weight, dimensions and cost of the skid.
The VDD deluge valve is made of Nickel Aluminium Bronze and it is specifically designed for sea water, foam concentrate and water foam solution.

Electric Monitors

The SA Fire Niagara firefighting monitor series are electric type remote controlled water cannons intended to deliver large amounts of water or water foam solution towards remote targets. They are commonly used to protect petrochemical jetties 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 systems, or at least in the simplest version, the detector is not normally integrated and the system responds 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.

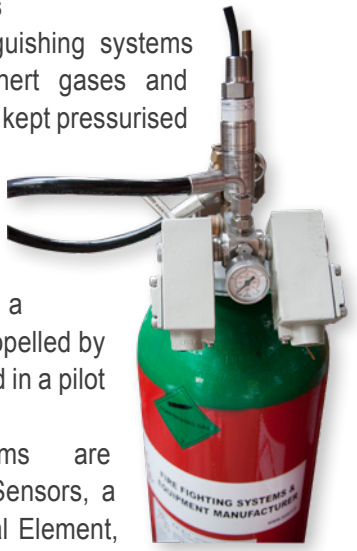
The increased reliability performance of the Niagara series monitor is related to its particular design, which allows automatic self-diagnostic analysis to be performed. At regular intervals, the self-diagnostic system implemented in the Logic Controller checks the correct operation of the monitor actuators 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:
The possible failure of a traditional electric remote-controlled monitor can be detected only when periodic maintenance and tests are performed. The constant monitoring of the system status implemented in the Niagara monitor series, 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 an improvement reduces the probability that faults, taking place between 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 in the success of the emergency operation.

Application:
The Niagara series monitors are specifically designed for petrochemical jetty and marine harbour 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. The Niagara series monitors are designed for sea water and water foam solution.

Electric Actuator for Gaseous Based & Water Mist

Fire Extinguishing Systems



Gaseous based fire extinguishing systems include carbon dioxide, inert gases and halocarbons. All of them are kept pressurised in 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. The SA Fire pilot actuators have been developed for sensibly reducing the probability of such failures and 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 rating.

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 should fail, the other coil is able to open the cylinder valve.

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

Application:

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 the 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 off-shore platforms or FPSO vessels, where generally a fire brigade is not easily available to compensate a possible firefighting system failure.