INDUSTRIAL FIRE JOURNAL

THE WORLD'S LEADING VOICE FOR THE INDUSTRIAL HIGH-RISK FIRE INDUSTRY

Summer 2013 issue no. 92 www.hemmingfire.com

Under the spotlight

THE VALENCIA 2006 METRO DERAILMENT

True redundancy

VALERIANO BARRILÀ AND ALESSANDRO BRONCO OF SA FIRE PROTECTION (ITALY) RESPOND TO A HEIGHTENED DEMAND FOR FULLY REDUNDANT ARCHITECTURE BY INTRODUCING A NEW SIL 3-SUITABLE DOUBLE-CHAMBER DELUGE VALVE.

Following major accidents in the oil and power industry in the last decade, the technical community involved in the design of industrial processes has shown an increased and more intense interest in system safety and availability. Attentions are no longer limited to the core process but are now extended to all the safety systems that encompass monitoring and the mitigation processes.

Although it is accepted that a process must be designed with high reliability criteria, that the process reliability cannot rule out the risk of an accident to take place is not always fully appreciated. Engineering limitations 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, the attention should be focussed on those systems that are designed to monitor the environment and provide mitigation effects.

Those process sub-systems such as fire and gas detection, 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 consequences, and their duty is both 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 that is quickly detected and confined, or a fire outbreak that is detected and extinguished by a deluge water spray, both fulfil the same objectives of saving lives, limiting the impact on the environment, reducing the production losses and safeguarding investments.

For the reasons outlined above, functional safety is moving into fire and gas detection and suppression systems, with the objective of increasing the reliability and hence the performance of the safety functions that are used to monitor and mitigate the effects of a possible accident.

IEC 61508 specifies four levels of safety performance or safety integrity level (SIL) – where SIL1 is the lowest and SIL4 the higest.

Functional safety

Safety is the absence of unacceptable risk of physical injury to people or damage to property. 'Functional safety' is part of overall safety but it is dependant on system/equipment that is operating correctly in response to outside inputs.

Should a hazard analysis show that functional safety is necessary, appropriate systems are required to perform specific safety functions to reduce that 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 life cycle of a generic SIS, from the initial concept through to 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, as well as ensuring safety even when faults are present. It specifies the techniques and measures to achieve the required safety integrity.

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. The Standard details the requirements necessary to achieve each SIL.

The table below provides the target failure measures for a

safety function allocated to an 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.

Safety integrity level (SIL)	Average probability of failure on demand (PFDavg)
4	≥ 10-5 to < 10-4
3	≥ 10-4 to < 10-3
2	≥ 10-3 to < 10-2
1	≥ 10-2 to < 10-1

Fire and gas (F&G) systems

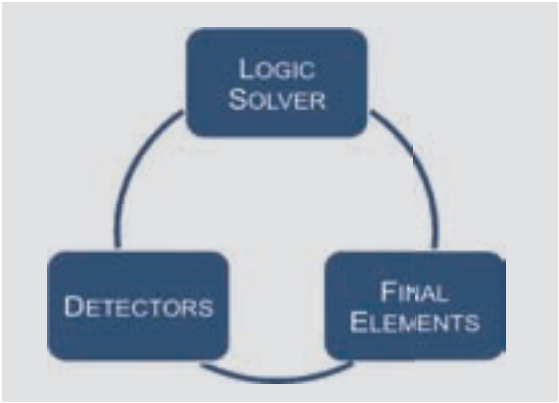
The tasks of a fire and gas system are to detect any hazardous fire or gas condition, to alert the personnel in the area and to activate the control and mitigation systems.

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 fire and gas system can be evaluated through a fault tree analysis based on the PFDavg of each component. The main components of a fire and gas system are as follows:

- Fire, gas or heat detectors;
- Logic solver;
- Deluge system, shut down system, etc (final elements).



Final elements

Up to now, manufacturers' efforts towards meeting the functional safety criteria for fire and gas 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 fire and gas system's effectiveness is related to the safety availability of all its components: so overall performance of the system is affected by the weakest element of the chain of its components.

This is why SA Fire Protection Srl decided to focus on the 'final elements', developing a number of SIL-suitable solutions according to IEC 61508 for the main types of fire fighting systems (ie deluge water spray systems, monitors and gaseous-based systems):

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

The SA FP SIL-suitable final elements have been validated by Bureau Veritas for integration in safety functions that perform fire protection activities in low demand mode for the actuation of fire suppression and cooling systems.

We will now focus on the VDD Double Chamber Deluge Valve.

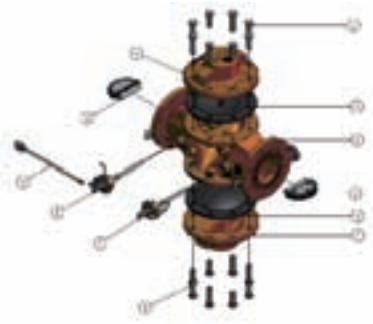
VDD Double Chamber Deluge Valve

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

The VDD has two priming chambers, each one with its own diaphragm and actuation trim, thereby providing two independent waterways to the water spray system.

Each priming chamber provides the nominal design waterway for the fire protection system: in the event one diaphragm fails the other will open and provide a 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 mode.



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 priming chambers through the hydraulic bridge. Thus the double chamber deluge valve can overcome a double failure (trim + priming chamber).

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

The following example is often used to illustrate the VDD valve 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 fire and gas system.

All the deluge systems commonly used today consist of a main deluge valve and an external bypass line that is installed on the deluge skid, and which is intended to provide manual actuation should the deluge valve fail on demand.

It is in these circumstances that the VDD Deluge Valve makes the real difference – the VDD design can overcome a double failure affecting the whole valve assembly, therefore it

is very unlikely for the VDD Valve to fail on demand.

Besides its increased reliability (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 the control room signalling that the 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.

Procedures to operate standard deluge skids are unnecessary with the VDD valve because it responds automatically and immediately to any failure affecting the valve, reducing the deluge system response time to zero – even in faulty conditions.

Other advantages include the limited operational man power required to operate the system, as well as the fact it affords continuous fire protection.

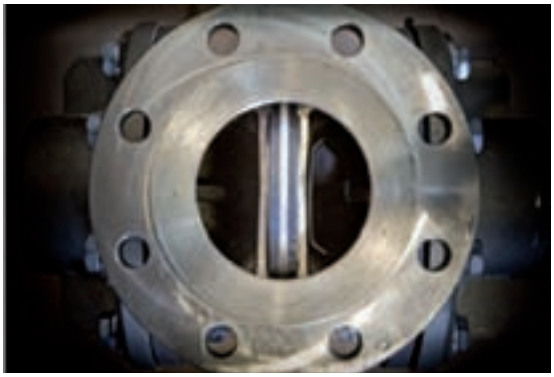
Maintenance

It is good common practice for owners and operators to perform maintenance on their fire systems on a regular basis as per NFPA 25 as well as the procedures outlined by the deluge valve manufacturer.

When performing an internal inspection of a normal deluge valve or cleaning the filters and orifices of the trim, it is impossible to keep the deluge valve in service and, therefore, the system has to be completely isolated. In such cases operators have very little choice: either they shut down the production process or keep an operator near the bypass line of the deluge valve whilst in contact with the control room, ready to open water manually in case of an incident.

The VDD deluge valve makes these issues redundant, although deluge systems equipped with the VDD deluge valves are subject to maintenance or repair with the exact same frequency and procedures required for traditional deluge valves. However, the protected plant process does not require shutting down, nor is it necessary to have an operator on standby next to the deluge bypass line during maintenance.

All this is possible because of the VDD deluge valve's redundancy, its maintenance isolation mechanism and its distributed activation trim.



To carry out maintenance/repair on a VDD deluge valve, the operator begins by unlocking the isolation system of one of the two chambers.

Two built-in isolation valves (upstream and downstream) must first be activated for the interlock system to be released (see bottom left). The interlock system (see below) is designed to fit and close only when the valve chamber is correctly isolated, in order to prevent human error.

The next step is to isolate the trim by 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 one chamber is being worked on the other remains in operation, providing continuous fire protection.

Once the inspection procedures of the first chamber are finished, the isolation system is applied to 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, meaning that the control room can monitor the maintenance work and receive feedback about the valve status after the inspection.

In addition, because the built-in isolation device provides continuous fire protection there is no requirement for the local fire brigade to be alerted each time the deluge valve is under maintenance or repair, as specified by NFPA 15 and NFPA 25.

From a design perspective the VDD deluge valve combines a high safety availability with low weight and dimensions of the deluge skid. The integrated redundancy and the hot back up rule out the need for an external bypass line on the skid, sensibly reducing weight and dimensions of the whole skid.

The VDD deluge valve concept was developed by SA FP engineers to meet the criteria set forth IEC 61508.

It is worth noting that minimum SIL levels for deluge systems intended for fire protection in oil, gas and power generation plants are already recommended by the major international organisations. For example, the Norwegian Oil Industry Association recommends a minimum SIL2 level for the 'deluge valve including actuator, solenoid and pilot valve' ('Recommended guidelines for the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian

System	Control Trim	λ_D	λ_S	λ_{DD}	SFF	PFD_{avg}
Deluge	Electrically operated	$1{,}116 \cdot 10^{-06}$	$2{,}564 \cdot 10^{-05}$	$1{,}097 \cdot 10^{-06}$	>99,9%	$5{,}41 \cdot 10^{-04}$
	Electro-pneumatically operated	$1{,}127 \cdot 10^{-06}$	$2{,}599 \cdot 10^{-05}$	$1{,}104 \cdot 10^{-06}$	>99,9%	$5{,}60 \cdot 10^{-04}$
ON/OFF	Electrically operated	$1{,}123 \cdot 10^{-06}$	$2{,}612 \cdot 10^{-05}$	$1{,}097 \cdot 10^{-06}$	>99,9%	$5{,}72 \cdot 10^{-04}$
	Electro-pneumatically operated	$1{,}133 \cdot 10^{-06}$	$2{,}646 \cdot 10^{-05}$	$1{,}104 \cdot 10^{-06}$	>99,9%	$5{,}91 \cdot 10^{-04}$

λ_D: Rate of Dangerous failure, λ_S: Rate of Safe failure, λ_{DD}: Rate of Dangerous Detectable failure
SFF: Safe Failure Fraction, PFD_{avg}: Average Probability of Failure on Demand

continental shelf').

For these installations requiring high safety function performances, SA FP has specifically developed and patented the double chamber VDD deluge valve, designed to overcome a double failure.

The VDD valve is available in diameter sizes from 3'' (DN 80) to 8'' (DN 200).

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. It has been validated by Bureau Veritas for use 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 also under UL testing for UL/cUL listing and a complete assessment is expected by the end of 2013. The certification will include the valve body material in nickel aluminum bronze, stainless steel and titanium, while the associated control trim are in stainless steel or Monel.

In summary

For some years the fire industry has been developing solutions capable of meeting the SIL requirements for logic solver and detectors, in line with an increasing realisation of the importance of functional safety in fire systems. However, the availability on the market for SIL-suitable final elements that are designed to be integrated in fire suppression systems is still very limited.

Whilst in emergency shut down systems we are used to seeing properly-designed SIL valves interconnected to logic solvers, it is not unusual to see installations in which a deluge system meant to perform a mitigation action (fire suppression, cooling or gas cloud control) being equipped with SIL unsuitable deluge valve.

Most of the time the deluge valves are assembled with SIL 2 or 3-capable solenoid valves (or in some cases even redundant solenoid valves) to activate a single control trim and its chamber. Unfortunately these architectures represent an erroneous application of the basic principle of safety integrity.

The VDD deluge valve presented in this paper is a complete actuation solution validated by a third party, and is suitable for SIL 3 fire suppression SIF (safety instrumented functions) in low demand mode, providing full redundancy and uninterrupted availability.

VDD is validated by Bureau Veritas for use in safety instrumented functions with an expected SIL3 level in low demand mode.

About the authors

Valeriano Barrilà is Technical Director of SA Fire Protection Srl and has an extensive experience in industrial fire suppression for on-shore and off-shore industrial complexes. He holds a BEng in Engineering from Pisa University and an MSc in Fire Engineering from Ulster University. He is an Ordinary Member of Engineers Ireland and a good standing member of NFPA.

Alessandro Bronco is a lead engineer of SA Fire Protection Srl. specialising in safety and reliability of fire products and solutions. He holds a BEng from the Polytechnic in Milan and an MEng in Aerospace Engineering from University of Pisa.