Increased demands for HIPPS final elements

Rens Wolters describes the impact of the new IEC 61508 Edition 2010 on final elements and HIPPS.

In the oil and gas industry protection against high pressure is increasingly performed by means of instrumented systems rather than mechanical safety relief valves. When the risk is high and the response time is short this application is often referred to as HIPPS (High Integrity Pressure Protection System). The applicable standards - IEC 61508 and IEC 61511 - use the generic term SIF or SIS (Safety Instrumented Function or System), whereas the industry uses HIPPS for this specific application. In the standards the element that shuts-off the incoming flow and isolates the high pressure source (on-off valve) is called the final element. A new revision of the IEC 61508 was published in 2010 and seriously impacts the HIPPS final element.

Prescriptive standards

Before the IEC 61508 existed over-pressure protection was governed by prescriptive standards like the DIN and API. These standards describe in detail how to design an installation and how to design the safety system required to protect its low pressure part. According to the API the safety system should consist of an emergency shut-down (ESD) valve - which would close upon high pressure down-stream of the control valve - and a full flow flare relief system. Nowadays, when instrumented systems are preferred over flaring, the same redundancy will be applied: the ESD valve remains and the full flow relief system is replaced by the HIPPS which often consists of redundant sensors and final elements. This results in an over-pressure protection system with a total of three final elements. A small relief capacity remains to evacuate leakage of the on-off valves.

The IEC 61508 and 61511 standards

In the 1990s questions arose regarding the reliability of instrumented systems and the IEC 61508 was born. This standard was mainly written for electronic and programmable electronic systems. In these systems it is quite easy to continuously measure, monitor and shut-down on detection of failures. For the final element, being a valve, this detection is not possible.

The Safe Failure Fraction - based on the diagnostics capability of electronic systems - it is the fraction of the safe and dangerous detected failures to all failures. This means in case there are many safe failures and many detected failures the number of final elements can be reduced. Over the past years this was usually done following a quite loose definition of a safe failure and even the addition of electronic devices to detect failures.

Let us focus on Hardware Fault Tolerance (HFT) first. A final element usually is considered type A equipment, according to the IEC 61508-2 (table 2) a single element could be allowed for SIL3 in case a Safe Failure Fraction (SFF) over 90 per cent can be justified. This would mean that where the prescriptive standards require 3 final element this table allows only 1 final element if the SFF is over 90 per cent.

In 2003 the IEC 61511 standard was published. This standard is mainly for end-users and integrators rather than for manufacturers and has a more conservative approach on redundancy. There is actually a specific table for final elements and sensors (IEC 61511-1 table 6). This table requires

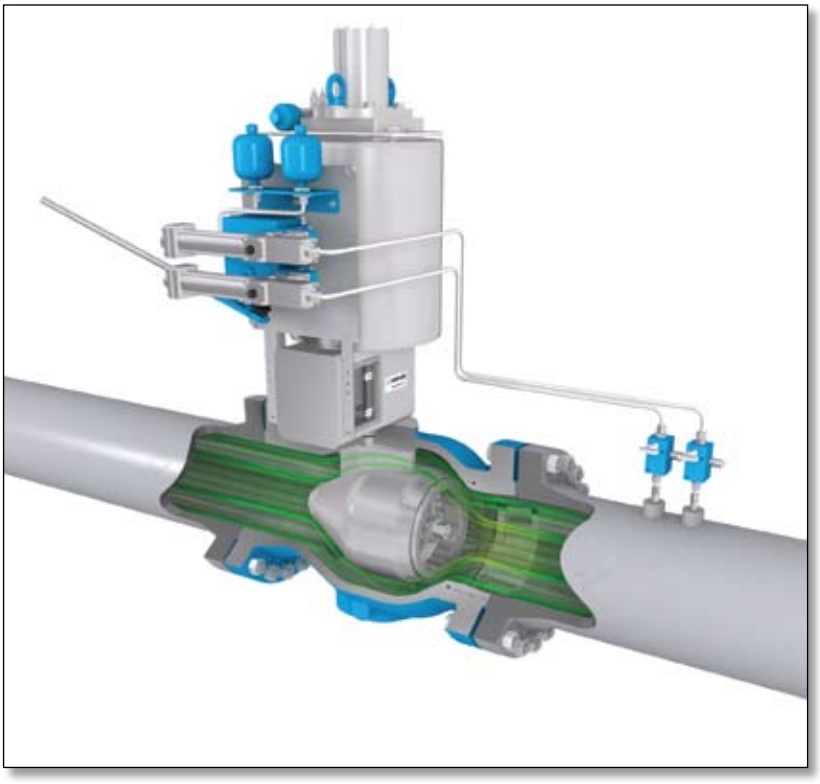

Fig. 1. Full mechanical HIPPS solution suitable for SIL3 application.

Fig. 2. One ball valve for ESD and two axial on-off valves for HIPPS. (The Netherlands)

a 1 out of 3 (1oo3) configuration for a SIL3 protection level. Only if 'prior use' can be justified this may be reduced to 1oo2.

Relevant changes

The new IEC 61508 Edition 2010 has more emphasis on the hardware fault tolerance reduction in general and more specific in the case of additional diagnostics. A paragraph is added indicating that the hardware fault tolerance shall be defined without applying diagnostics (ref. IEC 61508 para 7.4.4.1.1).

The new standard also defines in more detail at what intervals diagnostic tests shall be performed. Several paragraphs cover different cases such as high demand mode/low demand mode, but also depending on the hardware fault tolerance of the element (IEC 61508-2 Para 7.4.4.1.4). The longest possible diagnostic test interval shall be shorter than the Mean Time To Repair which would normally be between 8 to 24 hours. The shortest interval actually would be within the process time (seconds).

For a final element often it is assumed that diagnostics can be performed by means of partial stroking devices mounted to the final element. These are devices moving the final element approximately 10 per cent and then verifying if the actuator is still capable of moving the valve. It is impossible to perform this at an interval that complies with the standard and thus these devices cannot be considered diagnostic devices.

It is also difficult to argue that partial stroke devices perform a proof test as in the definition of the standard it is stated that the target of a proof test should be to reach 100 per cent coverage (IEC61508-4 par 3.8.5 note 2). Then it is contradictory to mount a device that is specifically designed to perform a partial proof test.

New definition of safe failure

In addition to the diagnostics also the safe failure is defined much more stringent now: a safe failure is a failure of the element that brings it to the safe state (closing the valve) without a demand. For a final element this can only be a failure of the seal in the actuator. A failure of such a seal would evacuate the air or hydraulic pressure and release the spring force closing the valve. Please note that a solenoid failure or leak in the tubing is not a safe failure of the valve/actuator but of the accessories. Dynamic forces in

the valve (flow to close) cannot be considered to cause a safe failure while these forces are too small to move the valve.

To be even more specific the IEC introduces so-called no part and no effect failures which are not to be accounted for in the SFF calculation. These changes in the definitions have of course a serious impact to the Safe Failure Fraction of the final element. Following version 2010 a SFF of 90 per cent or more can no longer be claimed. In fact it will be significantly lower than 60 per cent normally.

Fig. 3. A typical control and safety system consisting of an axial control valve and an axial on-off valve (HIPPS valve) according to IEC 61508. (South Africa).

We also want to note that based on the revised definition it could even be argued that the Safe Failure Fraction is not applicable for a mechanical component like a final element but only to systems having electronics such as the sensors or the voting logic.

In conclusion:

- The diagnostic test interval shall be at best not longer than the MTTR to take credit for diagnostics.
- Part and effect failures shall not be used in the SFF calculations, safe failures are basically only spurious trip failures, reducing the SFF for FE to below 60 per cent.
- SFF can be considered as not applicable for mechanical devices.
- Partial proof tests are not in line with the standard which sets a target of 100 per cent coverage.

Different routes to HFT

What is also new in the IEC 61508 are the different routes to assure a proper hardware fault tolerance is applied for each application or actually each SIL level. Route 1 uses the same table as in the 1998 revision and therefore uses the safe failure fraction as a basis for the required hardware fault tolerance. If we would argue that the safe failure fraction is mainly for E/E/PE safety related system where the standard is mainly written for then actually this route would not be applicable to final elements at all. However, if this route is applied the change in Safe Failure Fraction would have an impact on the hardware fault tolerance.

The new route 2 is based on the prior use/proven in use as found in IEC 61511 version 2003. In applications requiring a SIL3 or SIL2 in the high demand mode a hardware fault tolerance of 1 - and thus a 1oo2 configuration - is required. Although the term 'proven in use' itself is quite clear the IEC sets specific requirements (IEC 61508-2 par 7.4.10). Statistical data shall be available for the same application, the same type of process, but for final elements this also means the same closing times. All aspects of the applications and safety mission shall be verified. For example, a valve used in the mining industry closing in 1 second per inch (12 inch valve = 12 seconds) is not 'proven in use' on a gas well specifically when closing in 2 seconds.

Basically this also applies for route 1 where dependable failure data are required (IEC 61508-2 par 7.4.9.3 - 5). Dependable meaning that a sufficient confidence level shall exist that the equipment is suitable for the application (e.g. can close in 2 seconds).

Final conclusion

As a final conclusion it can be said that the new IEC 61508 requires mechanical equipment to be 'proven in use' (new route 2H) rather than using the Safe Failure Fraction. The new definitions of safe failures and diagnostics do not seem fit for mechanical equipment or special devices like partial stroking devices. These partial stroking devices are not in line with the standard which sets a target of 100 per cent coverage. In general the final result is now more in line with the prescriptive standards requiring redundancy in final elements. ●

Rens Wolters is HIPPS Product Manager, Mokveld Valves BV, Gouda, The Netherlands.
www.mokveld.com

This article first appeared in *INTERNATIONAL OIL & GAS ENGINEER, FEBRUARY 2012*
www.engineerlive.com