TÜVRheinland®

Modifications in the Latest Revision of the IEC 61508 and the Consequences for Final Elements like Valves/Actuator Combinations

Rens Wolters

Mokveld Valves – The Netherlands

Modifications in the Latest Revision of the IEC 61508 and the Consequences for Final Elements like Valves/Actuator Combinations

Rens Wolters
Mokveld Valves – The Netherlands

In 2010 a new revision of the IEC 61508 was formally published.
The previous version dated back to 1998 and since then it is used in the Oil and Gas industry for over-pressure protection systems.

This presentation will focus on the modifications in the IEC 61508 related to the final elements and as example an application in the Oil and Gas industry is used.

It should be clear that this presentation does not cover all modifications / additions or revisions in the standard, for instance specifically on the development of ASIC's a vast work was done by the committee.

Before the IEC 61508 was written in the Oil and Gas business over-pressure protection of for instance a gas well flowing into a separator would be governed by a prescriptive standard like the API.
This standard describes in detail how to design such an installation, including pipe diameters based on flow data, wall thicknesses, but also the safety system to protect the lower pressure part.

Basically the API would prescribe to install an emergency shut-down valve which would close upon high pressure down-stream of the control valve.
In addition to this a full flow flare system would be installed.
This of course had limits while real big platforms off-shore might not have the possibility to burn such big quantities of gas without danger to the platform itself. In some case separate platform to accommodate the flare only would be required.

Therefore instrumented safety shut-down systems were designed, actually the API recognises this in the standard as well.

But for these Instrumented systems no standards were available.
The clients simply added redundant sensors and redundant final elements instead of a full flow relief valve. In general a small relief capacity remains which may then evacuate leakage of the safety shut-down valves.

So these systems still relied on redundancy and actually required 3 valves in series, specifically when fast acting valves were required.

Then in the late 90's people would start to think about how reliable these systems were and the IEC 61508 was being written.
IIf applied in huge steps this standard would say about HIPPS:

- In case the high pressure can severely damage the vessel and then cause injury or death to people close to the separator.
- In case the pressure rise is rapid

Then we assume, for the sake of this example, that a SIL3 over-pressure protection is required.

Based on the 1998 version we would then, if we forget all the other important requirements but focus on the hardware fault tolerance, be able to apply a single final element in case the Safe Failure Fraction is higher than 90%, referring to IEC61508 table 2 architectural constraints on type A safety-related subsystems.
The Safe Failure Fraction is the fraction of the safe and dangerous detected failures to all failures.
This means in case we have many safe failures and many detected failures we can reduce the number of final elements.
Over the past years this was usually done by means of a quite loose definition of a safe failure and electronic devices were added to detect failures.

The standard is quite clear that the dangerous detected failures should be detected by what was called diagnostic. This is a term which mainly comes from the electronic foundation of the standard. In electronic systems it is quite easy to continuously measure and monitor and based on that decide if the system is still safe and still properly performing it's safety mission.

Therefore actually the result of the Safe Failure Fraction and it's implication on the hardware fault tolerance would be that now instead of having a total of three final elements in series we would end up with only one final element. Usually the sensors would still be in a 2oo3 situation while these are not type A equipment.

In 2003 the IEC 61511 was published. This standard is mainly for end-users and integrators and not for the manufacturers of elements. However this standard shows a more conservative table for the application of the number of final elements. There is actually a specific table for final elements and sensors (IEC61511 paragraph 11.4.4 table 6). This table requires a 1 out of 3 (1oo3) configuration for a SIL3 protection level.
Only in case prior use can be justified this may be reduced to 1oo2.

The 2010 release of the IEC 61508 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 standard also defines more in detail at what intervals diagnostic tests shall be performed. Actually several paragraphs are covering different cases, like high demand mode / low demand mode, but also the hardware fault tolerance of the element. The longest possible interval of the different paragraphs requires a diagnostic test shorter than the Mean Time To Repair of the system in case of failure, this would normally be 8 to 24 hours. The shortest interval actually would be within the process time.
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% and then verify if the actuator is still capable to move the valve.
While a partial stroking device usually performs the diagnostic test only once per 3 months these devices cannot be considered diagnostics within the limits of the standard.

In addition to the further definition of the diagnostics also the definition of a safe failure is much more stringent in the new revision. The new text is actually so clear that it can only be applied for the integrated combination of valve plus actuator (which make up the final element). According to this definition a final element will have only 1 safe failure. This is the failure of the seal at the actuator, a failure of this seal would evacuate the air or hydraulic pressure and as such the springs can close the valve. (naturally you could also think of dynamic forces that move the closing member after a stem breakage or an unbalanced valve that moves to the safe position after stem breakage)
An unexpected change in the position of the final element because the solenoid would spuriously trip would be a safe failure of the solenoid and not the final element itself. A leak in the tubing or couplings would close the valve and such spurious trip would also not be attributed to the final element.

To be even more specific so-called no effect and no part failures are described as well now and may not 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.

Based on the different definitions it could even be argued that the Safe Failure Fraction is not even applicable for a mechanical component like a final element but only to systems having electronics like the sensors or the voting logic.

So even if we would argue that also for a final element a Safe Failure Fraction can be determined these more stringent definitions will significantly reduce the Safe Failure Fraction of the final element. A SFF of 90% or more cannot be claimed following the 2010 standard. In fact it will be significantly lower than 60%.

In Short conclusion:

1) HFT shall be determined by calculation of the SFF where diagnostics are not used to increase the DD failures and to reduce the HFT.
2) The diagnostic test interval used in PFD calculation shall be at best not longer than the MTTR, hence very frequent testing is required to credit diagnostics.
3) No part and no effect failures shall not be used in the SFF calculations, SF are basically only spurious trip failures, reducing the SFF for FE to below 60%.
For FE elements the partial stroking have become increasingly popular as feature to reduce the full stroke proof test interval. Also there are documented cases where the 'diagnostic capabilities' of partial stroking devices are credited to increase the SFF and by that reduce HFT. However as indicated these devices cannot be considered to perform diagnostics.

While in the definition of the standard it is indicated that the target of a prooftest should be to reach 100% coverage of the prooftest it als seems to be contradictory to the standard to mount a device that is specifically designed to perform only a partial test.

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 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 than actually this route would not be applicable to final elements at all.
If we would apply this route of course the change in Safe Failure Fraction would have an impact on the hardware fault tolerance.

The new route 2 in the standard is based on the prior use / proven in use as it appeared in 2003 in the IEC 61511.
In applications requiring a protection level SIL3 or SIL2 in the high demand mode a hardware fault tolerance of 1 and thus a 1oo2 configuration.

Proven in use is quite clearly defined in the standard. The term “proven in use” itself is quite clear, although it should be understood as “proven in your specific application”. For a final element this would mean that it shall be verified that statistical data is available for the same application. The same type of process data, for instance is it fluid from a well head as the previous example or does it concern clean gas suitable for the consumer market, but also the size and rating or the material selection shall be considered.

All aspects of the applications and safety mission shall be verified, for instance It shall also be considered if the final element has sufficient statistical data for the required response time. In general it can be said that safety shut-down valves move in 1-2

seconds per inch, which means for a 12 inch minimal 12 seconds. Therefore in applications below this response time, which is the lower limit, the statistical data of the final element shall be verified. It shall be demonstrated that that specific combination of valve and actuator have sufficient experience in response time below 1 second per inch or below 12 seconds.

Basically this already applied for route 1 while also in route 1 dependable failure data are required. In all safety systems designed in accordance with the IEC 61508 sufficient confidence level shall exist that the equipment is suitable for the application.

As a conclusion it can be said that in the early days of gas treatment plants the “old” prescriptive standards would require redundant final elements. But that due to the revised definitions of safe failures and diagnostics and the addition of a new route to verify the required hardware fault tolerance the IEC 65108 also requires redundant final elements on higher SIL applications. In additions to this it can be concluded that the use of partial stroking devices on these final elements is not recommended while the standard sets a target for a 100% proof test.