WHY A LOOP WITH A SIL 3 CAPABLE VALVE MAY NOT MEET SIL 3

Dr. Peter Clarke, xSeriCon Ltd.

Steve Close, exida LLC

Revision 0.2b, 15 July 2011

SUMMARY

- The SIL rating of a valve depends not only on its failure rate and systematic capability (freedom from human error during design), but also on its safe failure fraction (SFF).
- Slam shut valves, like all mechanical devices, have a rather low SFF by nature. This is independent of design.
- The way SFF is calculated under IEC 61508 standard has changed from the first to the second edition of the standard. The new calculation method gives a much lower SIL for valves, which are very unlikely to achieve SIL > 1 in a 1-out-of-1 configuration.
- Valves certified under the first edition will have to be updated to second edition from 2013 when they are re-certified.

INTRODUCTION: WHAT IS A SIL-CAPABLE VALVE?

It's common in the industry to hear design engineers refer to safety-rated components—valves, for example—as "SIL 2" or "SIL 3". This reflects a widespread misunderstanding of the meaning of SIL. The term SIL (safety integrity level) can only be defined for a whole loop, including sensor, logic solver and final element. This is because SIL is a measure of the integrity (reliability) performance of a safety function *as it is actually implemented* in a real-world application. The job of a safety function is to control a risk, and since no two risks are exactly the same, the safety function's integrity requirements will differ from case to case. Thus, it is meaningless to speak of the SIL of a valve sitting in the warehouse; the full configured performance, and hence the SIL, cannot be determined without a knowledge of the exact conditions of use.

However, we can talk about the SIL *capability* of the valve. The valve's design will enable it to achieve some *maximum* SIL when it is incorporated into a real safety function. How is the actual SIL of a safety function determined? It's important to remember that *three* separate criteria must be met in order to achieve a given SIL target:

- probability of failure on demand (PFD), a measure of susceptibility to random failures;
- safe failure fraction (SFF), a measure to ensure sufficient redundancy is built into the system; and
- systematic capability, a measure of susceptibility to systematic failure (basically, human errors during the design and manufacturing processes).

When we describe a valve as being *SIL 3 capable*, we are making two statements about it:

1. The valve's failure rate is low enough that it is, in principle, possible to build it into a safety function whose overall PFD is low enough to meet SIL 3. The relationship between overall PFD and SIL is simple and clearly defined in the standards (IEC 61508 and IEC 61511).
2. The valve's design and manufacturing processes are proven to be well controlled. This means we can claim the likelihood of human error during the design and manufacturing processes leading to failure is low enough to meet a claim of SIL 3 capability. (The higher the SIL capability claimed, the better the control measures must be.)

Notice we have *not* said anything about the valve's SFF. This is because the SIL achievable will vary depending on the amount of redundancy (as well as the configuration: open-to-trip or close-to-trip). For example, the SFF of a single valve is typically low (<60%), so that any loop with only one valve is often limited to SIL 1—even if the valve itself is "SIL 3 capable" as defined above. This limit of SIL 1 is not a fault of the valve design; it is a basic function of mechanics, as we discuss later. However, if two or more valves are used in a redundant configuration or if automatic diagnostics are added,[1] the SIL achievable by the loop will usually increase to SIL 2 or even SIL 3.

FIRST AND SECOND EDITIONS OF IEC 61508: IMPORTANT DIFFERENCES

Users may be surprised to hear that a loop with a single shutdown valve may be limited to SIL 1—especially if they are familiar with using single valves in previous SIL 2 applications. The underlying reason is that the definition of SFF changed significantly between the first and second editions of IEC 61508. To understand this, let's look at the principle underlying SFF. Any item of safety equipment may fail in many different ways. Some of these will lead to failure to function on demand; these failure types are classified as *dangerous failures.* Others will lead to false trip, which is "safe" but also a nuisance as it causes unwanted shutdown. These are known as *safe failures.* Still more failures are neither safe nor dangerous; these are known as *no-effect failures*. A typical example is failure of the valve position indicator. For any item of equipment, it is possible to calculate[2] the *failure rate* (lambda, λ) for each of these failure modes.

For any item of equipment, SFF—safe failure fraction—is the ratio of safe failure rate to total failure rate. Under IEC 61508 first edition, a "safe failure" was considered to be any failure that is not dangerous—in other words, no-effect failures were included in the count of safe failures. The problem with this approach is that, if the no-effect failure rate is increased, the SFF increases too, often quite dramatically. Thus, injecting more no-effect failures into the calculation could result in an artificially high SFF, resulting in over-optimistic claims of SIL capability from a single valve.[3]

To address this loophole, the second edition of IEC 61508 redefined "safe failures" to include *only* those failures leading to an unwanted trip.[4] No-effect failures can no longer be included in the count

[1] "Redundant configuration" means valves in series for close-to-trip (shutdown) valves, or valves in parallel for open-to-trip (e.g. emergency depressurization valves).
[2] This calculation is normally done using an analytical technique known as *Failure Modes, Effects and Diagnostics Analysis* (FMEDA).
[3] For a detailed critique of this viewpoint, see Summers, A. *IEC Product Approvals – Veering Off Course,* http://www.controlglobal.com/articles/2008/187.html
[4] This is valid for systems without diagnostics, such as those under consideration here. The SFF calculation is a little more complex when diagnostics are provided.

of safe failures. The net result has been a plunge in the SFF values typically attainable by simple mechanical devices such as valve/actuator sets. In many cases, the "old" SFF was high enough to allow a single valve to achieve SIL 2, whereas the "new" SFF will allow only SIL 1. If the SIL requirement is greater than 1, the only possible solutions are to add automatic diagnostics or specify redundant valves.

A PRACTICAL EXAMPLE OF SFF CALCULATION

Let's look at an example using a typical globe valve and a spring return diaphragm actuator. Failure rates are shown in the figures below (the values are in FITs, meaning failures per 10^9 hours). Figure 1 shows the division of failures into "safe" (green) and "not safe"[5] (red) according to the first edition, while Figure 2 shows the same for the second edition.

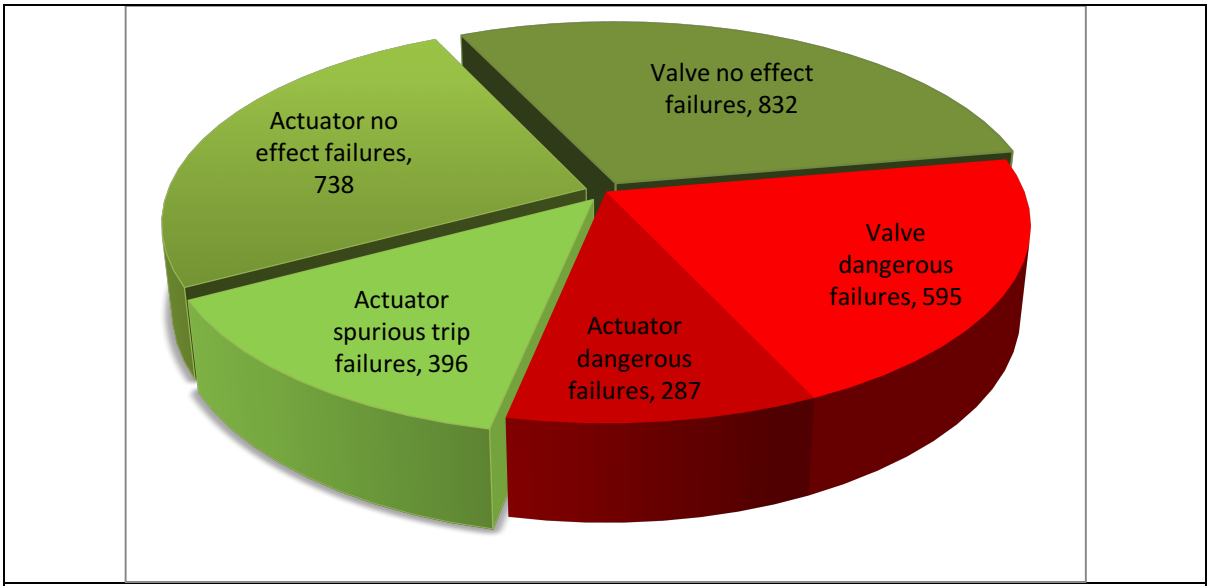

Figure 1: Typical SFF calculation for valve + actuator according to IEC 61508 first edition. The SFF is the percentage of the chart that is coloured green, which is 69%.

[5] We are using "not safe" here to mean any failure that is not included in the count of "safe" failures for the SFF calculation. For a valve+actuator set, according to the first edition, "not safe" failures are basically only dangerous failures (those which prevent the safety function from working on demand). Under the second edition, the "not safe" group includes both dangerous failures and no-effect failures.

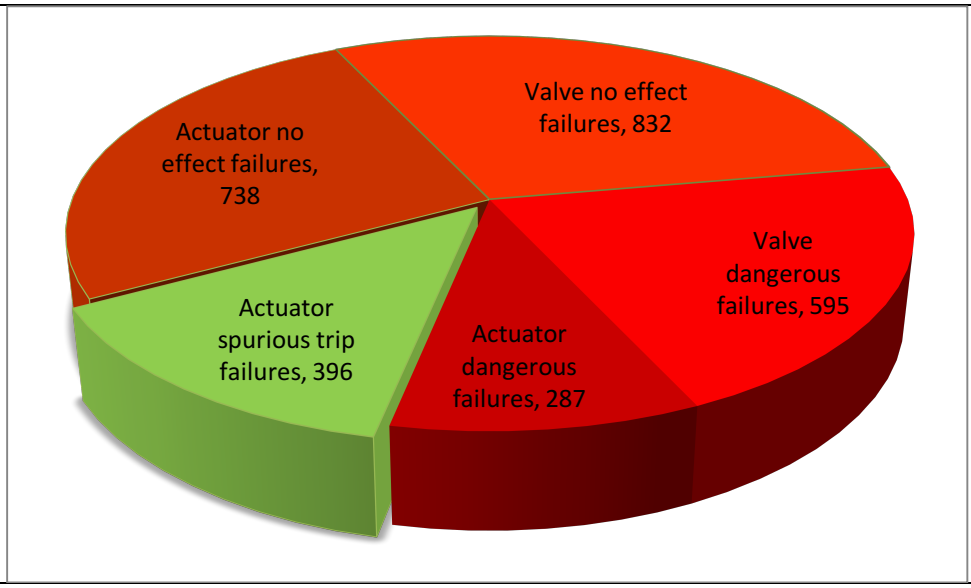

Figure 2: Typical SFF calculation for valve + actuator according to IEC 61508 second edition. This time, the SFF is only 31%.

The dramatic impact of removing no-effect failures from the count of safe failures is evident from these figures. (Note that there are no "spurious trip" failures arising from the valve itself, as there is typically no means by which a valve can close itself in the absence of an actuator.) It is easy to see that the total safe failures per the second edition are on the order of one-fifth of what they were under the first edition. While the SFF may change somewhat depending on the valve/actuator design, the results will always be similar to this example.

This analysis does not include automatic Partial Valve Stroke testing, which can be implemented on a safety system final element to increase the SFF. However, this does not apply to Slam Shut Valves, because they cannot be partially stroked. Once the trip mechanism is triggered, the valve will go full stroke.

IT'S A QUESTION OF PHYSICS

Why is the SFF of a valve so low, compared with other safety products such as PLCs and smart transmitters? It's a simple matter of mechanics: for close-on-trip applications, none of the credible failures of a valve—such as component breakage, binding or seal failure—will lead to unexpected trip, and therefore they cannot be classified as "safe failures" under the second edition.

This comes as a surprise to valve manufacturers getting their equipment SIL-certified for the first time (or re-certified). Their competitors' products may have achieved SIL certification under the first edition, and can thus claim a much higher SFF. The consolation will come when the competing products' certification expires: after the end of the transitional period (2010-2013), the second edition must be used for the re-certification. That means the playing field will once again be level.

For further information on this topic, please contact Dr. Peter Clarke at xSeriCon Limited via peter.clarke@xsericon.com