Is a TÜV certificate enough?

Robin McCrea-Steele, **TÜV FSExp**
Invensys-Premier Consulting Services

International safety application standards require that manufacturers document compliance of SIS logic solvers to IEC61508. A TÜV certificate of compliance goes a long way, but as a user, is this all you need? Most all safety practitioners and process plant operating companies will very definitely say that although essential, product certification should not be the only criterion.

The compliance to all phases of the IEC61511 safety lifecycle, the assignment of safety integrity requirements to all the independent layers of protection, as well as verification, validation, audits and management of change are only some of the requirements for a successful risk reduction implementation.

A third party certificate of compliance for the SIS logic solver will validate the design and “fail safe” suitability for use in a safety instrumented function up to the SIL claim limit. It does not say anything about the spurious trip vulnerability, which is an issue that the end user needs to evaluate based on the specific application.

Furthermore, and extremely critical, is the fact that when a SIS logic solver receives certification, it is done so in isolation, with an additional review of safe communications to external equipment and protection against interference with the integrity of the safety functions.

For systems where the SIS logic solver is embedded within the platform of a control system (DCS), the certification will validate the non-interference of failures in the DCS affecting the SIS safety functions. Is this enough?

Well, the first problem is that the certification does nothing to avoid the common cause failures of the SIS and DCS, which are based on the same hardware/software platform. Neither does it say anything about the systematic errors inherent in using the same platform for SIS and DCS. The certification basically validates the “functional separation” and non-interference of control system failures on the SIS, firewalls and password based access protection.

What about independence of the layers of protection in the plant? This is not part of the SIS logic solver certificate. This is a responsibility of the operating plant company.

Compliance to the “functional separation” requirements of IEC61511 is enough to obtain a TÜV certificate, but when the SIS is embedded in the control system, this eliminates the credit that could have been taken for a DCS as an independent protection layer (IPL).

An independent layer of protection needs to be just that. Independent. If a common cause error can affect both the DCS and the SIS, then no credit can be taken for the control system as an independent layer of protection.

Therefore, although a TÜV certificate for a certain SIL capability limit for the SIS logic solver validates the use of a functionally separate, but common platform DCS-SIS, great caution needs to be taken in the overall implementation of the plant risk reduction requirements.

In the initial stages of design of the SIS, hazards are identified and safety integrity requirements are assigned to each layer of protection. Layers of protection analysis (LOPA) is one of the most popular methodologies used in the assignment of the SIL requirements for each safety instrumented function (SIF).

LOPA takes credit for all available independent protection layers (IPL) that qualify per the IEC 61511 requirements. During the LOPA evaluation, the DCS is many times considered as an IPL and a credit up to the maximum allowable by the standards is taken (10^{-1} or RRF=10).

Taking a risk reduction factor (RRF) of 10 for the DCS as an IPL has considerable weight in the final SIL requirement for the SIF. A control system that qualifies as an IPL will substantially reduce the demand rate on the SIS. Actually, the SIL of the SIF will be one whole order of magnitude higher if the DCS does not qualify as an IPL.

Considering the above, during the detail design phase of a SIS, it is very important to verify the assumptions made during the SIL assignment phase.

For example, when a LOPA study determines the need for a SIL 2 safety instrumented function, based on credit taken for all IPLs' including a RRF of 10 for the control system, the verification phase should make sure all the assumptions are still valid. If, however, the SIS logic solver is embedded in the same hardware/software platform as the DCS, then the control system will no longer qualify as an IPL and the RRF credit taken will need to be nullified. As a consequence, the resulting SIF requirement will be increased by one order of magnitude to a SIL 3.

Conclusions:

A TÜV certificate for a SIS logic solver embedded in a DCS platform validates the functional separation and non-interference of the control system on the safety functions. However, no credit can be taken for the DCS as an independent layer of protection (IPL) and the potential for all SIL requirements to be increased by an order of magnitude is real. A plant with requirements for SIL 1 and SIL 2 safety instrumented functions will end up with mostly SIL 2 and SIL 3 requirements. This means incremental costs in field redundancy, installation, maintenance and testing.

Worst of all, if a SIL 3 requirement was determined during the LOPA with credit for the DCS as an IPL, using a SIS logic solver embedded in the DCS will render a requirement for a SIL 4, which means going back to the drawing board.

The supposed advantages of lower hardware and training costs for using a common embedded platform comes at the expense of safety and has too many downsides.

It is safer, renders a lower SIL requirement and is less expensive to implement physically separate and diverse independent safety and control systems, with smart integration at the information, configuration, asset management and HMI levels. All the capabilities of field diagnostics, asset management, including partial stroke testing, can be implemented effectively through smart integration. The scales are heavily against trying to commingle safety and control in the same platform.

****