Reliance verification of Safety Instrumented Systems

Dr. Bernd Schroers
Bayer AG, BTS-OSS-PPS-FS
Building B407
51368 Leverkusen, Germany
bernd.schroers@bayer.com

Abstract

A common protection task in the area of process industry is e.g. to prevent a vessel from bursting due to overpressure. Typical approaches towards that task comprise of

- inherently safe design
- mechanical safeguards (e.g. pressure safety valves)
- Process Control Technology (PCT) related measures

International and national regulations and standards control the Process and Plant Safety (PPS). With IEC 61508 and IEC 61511 (ANSI/ISA-84.00.01) a probabilistic approach found it’s way into the Process and Plant Safety through Process Control Technology (PCT) also called Functional Safety. Since this time PCT broadly applied in accordance with these standards in the entire process industry.

Around the actual core process together with its automation system preventive safety measures are set up. These are intended to do usually nothing at all. But right at the very moment the underlying process starts to get out of control they execute their intended appropriate action and bring the process back to its safe state. They therefore prevent primary loss of containment.

The safety related reliance of a Safety Instrumented Function has to be verified quantitatively by calculation. The PCT based safety measures can be traced back to the desire to have the measure’s function available at the very moment a demand arises from the process. This can be altered by making the measures more or less robust against failures that could prevent it from the execution of its intended function – more or less, depending on the related quality (expressed by the Safety Integrity Level, SIL) and thus the related risk class.

A bunch of problems had to be solved since this time. Instrument reliability data had to be collected and the existing safety instruments had to be evaluated. Existing installations with often complex functionality had to be reviewed. Diagnostics and proof test coverage needed to be defined and assessed new. The independency of safety systems and safety functions created new questions about implementational aspects.

Together with the introduction of the Functional Safety philosophy, an important design variable, the proof test interval, has become flexible. Instead of being fixed to one year, it is now integral part of the probabilistic calculation and thus only serves as one impact factor on the SIL proof among others. This yields an important advantage, as the flexibilization of the proof test interval contributes to the maximization of a plant’s uptime.