BLOG/DARESBURY, UNITED KINGDOM | FEBRUARY 2022

Determination of Process Safety Times – a Common Oversight?

Blog by John Whitaker, Senior Process Engineer, ABB UK

Introduction

Process Safety Time (PST) may be defined as the time period between a failure occurring in a process plant or in the plant control system, and the occurrence of a hazardous event caused by that failure. Prevention of the hazardous event may be achieved through a Safety Instrumented Function (SIF) that must be complete before the PST has elapsed. Time is required for the SIF sensor & logic solver to detect and respond to the failure, and for the final element in the SIF to complete its action as determined by the logic (such as closure of a valve). In addition, an alarm may also be used to warn an operator of a failure in plant operations and so in this case there must also be time available within the PST for the operator to correctly respond to the alarm in order to prevent the hazardous event from occurring. The simplest example of a process failure that could be considered in this way is a tank being filled with a liquid, and the hazardous event being overfill of the tank (and subsequent loss of containment). However the concept applies to a wide range of scenarios; for example overpressure of a pipeline due to the sudden closure of a valve, or the initiation of a runaway reaction in a reactor vessel due to an excess of energy input from a steam coil or jacket.

Process Safety Time Requirements

The methodology for determining SIF and alarm requirements with regard to PST are laid out in standard BS EN 61511. First, credible hazardous events above a certain consequence threshold will typically be identified from a SIL or LOPA review (often following a Hazard Identification Study such as HAZOP). The PST for any hazardous event is normally calculated as the process variable at the time of the event minus the process variable at the time of the SIF detection point, all divided by the rate of change of the process variable over time between the two. A dynamic simulation model of the plant process may be used to simulate the scenario and determine what the PST is and what the setting of the SIF and alarm should be as a result of that. This will take into account factors such as the mode of operation and the equipment design limit. The model must be sophisticated enough to enable any non-linear behaviour of the process to be assessed. The PST for each hazardous event should be recorded in a suitable project instrumentation

database, and this record should be maintained after the commissioning phase and handover of the project to the duty holder.

Managing Hazards in Design

When designing a plant, a design team will document the safety aspects of the process in Hazard Studies that consider the deviations from design intent that could occur, and the ways in which they may be safeguarded against. The safeguards will often take the form of a SIF or alarm. However, after the safeguard has been specified the correct design of the SIF may be omitted due to lack of proper awareness and consideration of the PST and the methodology for determining it. This may seriously undermine the rigour of the project Hazard Studies, as the eventually installed SIF items may not in fact be suitable safeguards. The Process Engineer and the Controls Engineer may be focused on the correct design parameter specification and material selection of the equipment and instrumentation, and consideration of required response times may then be neglected by both. Dynamic analysis of the process deviation may not be conducted at all. As a result, the understanding of the relationship between the PST and the required response time of a SIF may not be specified correctly within the Safety Requirements Specification (SRS). Alternatively the designers may revert to standard rules of thumb for specifying design requirements, with the suitability of these rules not being assessed. It is sometimes the case that completed designs have the same required response time entered for every SIF item.
In addition, the requirements for PST and SIF or alarm response times may not be properly specified by the End User with the result that no budget is allocated for this work in the project estimate. The Duty Holder company may be relying on the EPC organisation or the wider supply chain for determination of the response times of safety systems.

Conclusion

As a result of these issues the inclusion of correctly developed PST and SIF demand response calculations may be omitted in project delivery, and the work does not then take place. The resulting design oversights may exist unrevealed in the process plant until the potential failure event actually takes place, and by then it will be too late.

For further information please email me at John Whitaker or see ABB Pressure Relief