Beyond LOPA
Safety integrity assessment

This case study relates to an upper tier COMAH site with a wide range of facilities for reactive chemistry, together with the capability for handling hazardous bulk materials such as chlorine.

The site was assessing the safety aspects for a complex exothermic reactive process relating to the manufacture of a high value pharmaceutical intermediate. The process was being relocated to their current site but a number of changes and improvements had also been made.

The regulator had expressed concerns that a previous Layer of Protection Analysis (LOPA) study carried out by others was inadequate and flawed. The site selected ABB as an organisation with the appropriate experience and methodologies to tackle this complex scenario and establish realistic performance requirements for instrumented protection associated with the batch reactor.

Solution
ABB set about determining the actual level of risk reduction provided by existing instrumented protective measures associated with a batch reactor against thermal runaway.

In the previous analysis of the batch reaction system, the level of complexity was not fully appreciated and LOPA had been used by a third party organisation. The analysis did not explore the separate phases of the batch process and the initiating cause failures associated with each phase. Furthermore, the LOPA did not fully appreciate the nature of the design and made unwarranted assumptions about independence that were not actually valid.

Demonstrating to the regulatory authorities that batch reaction process risks are being managed appropriately.
This had resulted in claims for two instrumented functions which, taken together, were apparently giving an overall performance well beyond SIL 4. This flaw had been readily noticed by the regulatory inspector.

ABB approached the analysis of the batch reactor system using demand trees and fault trees - a method well-suited to the level of complexity of the control and protection arrangements for the reactor. The key stages used were (1) reviewing the hazardous event scenario to be clear about the undesired consequence, (2) using a demand tree as a systematic means of identifying all the relevant initiating causes, and (3) creating an individual fault tree for each initiating cause, (4) linking all the individual fault trees together to describe the overall scenario, and (5) quantifying the fault tree to determine the frequency of the hazardous event.

This approach enables realistic performance requirements to be determined for instrumented protective measures associated with protection against reactor thermal runaway.

Benefits
- Effective demonstration to regulatory authorities that risks are being managed to meet the legal responsibilities under the COMAH regulations
- Application of international standards IEC 61508 and IEC 61511, representing current good practice in the management of functional instrumented protective measures, for determining suitable performance requirements
- Use of fault tree analysis allowed the complexity of the protective measures to be properly represented so that realistic performance requirements were determined.
- Previous use of LOPA by others for the particular level of complexity of the scenario was not correct and was misleading