Safety management in process industries

Part 2 – The ABB approach

Robert Martinez, Per Christian Juel, Per Fjelldalen

The safe operation of an industrial process requires a structured approach that must be applied to every aspect of every level of operations while seeking to minimize the total risk posed by the process.

ABB has a long tradition of supplying safety systems for industrial processes. This has provided the company with the experience necessary to implement new safety standards such as IEC-61508 and IEC-61511 and integrate these in its System 800xA control system.

ABB has been supplying safety systems to process industries for 25 years and is the most experienced supplier of programmable safety systems. The first safety system was developed and supplied to Mobil Inc. for the Statfjord B oil and gas production platform in 1979. Since then, ABB has been supplying industrial safety systems to most industry segments and major operating companies around the world.

The oil industry has been at the forefront of safety management for many years. National legislation for safety in exploration and development of the oil fields in the North Sea was forcing a shift in safety awareness and supporting technology long before new international standards were introduced. ABB played an important role in the development of the technology that today forms the basis for modern integrated automation and safety systems.

This has provided ABB with the experience necessary to support its process industry customers in facing the technical and organizational challenges and costs related to strict safety management regulations. Another important argument in favor of ABB is the System 800xA control system[1)], providing a broad collection of "out of the box" services enabling the tightly integrated management required by IEC-61511[2)]: auditing, authentication, access management, document management, asset monitoring and CMMS (maintenance) integration. These and other software services provide functionality which help enforce and prove compliance during the operational phases of the safety lifecycle.

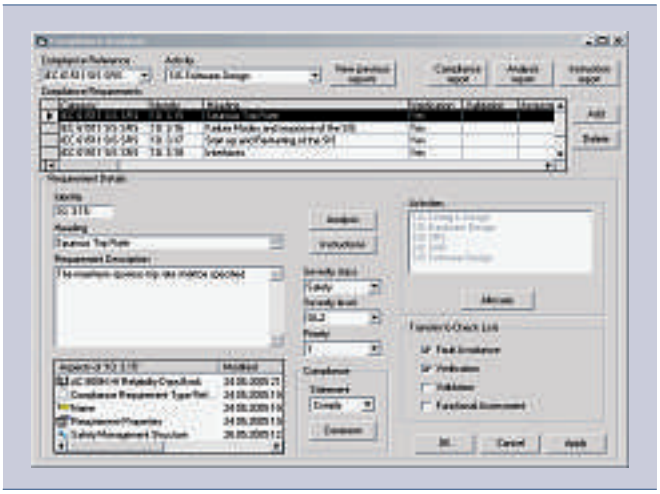
ABB's Corporate Research in Norway performed a gap analysis of the System 800xA platform versus the IEC-61511 management requirements to determine where support of the standard could be strengthened. The study revealed an opportunity to offer complete lifecycle coverage by providing support for this functionality in the following planning and engineering phases:

- Safety project management.
- Hazard and risk assessment.
- Safety function design for integrity and reliability.
- Cause and effect matrix safety programming.

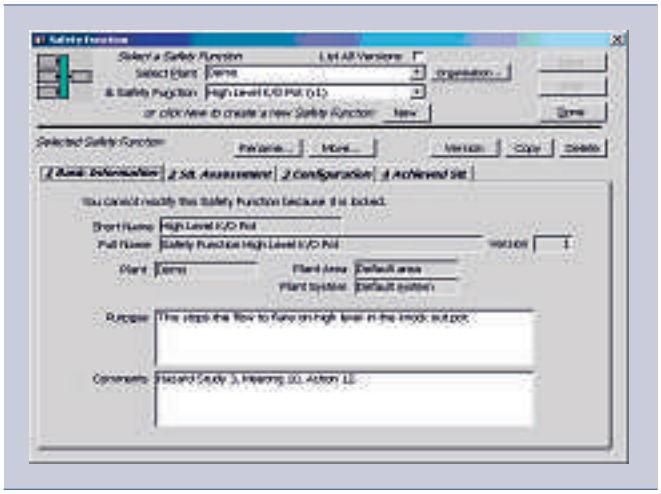
ABB Corporate Research, together with the Safety section of ABB Process Automation, identified the benefits of a System 800xA "Safety Workplace" package, combining the existing and proposed functionality to provide a seamless solution to both engineering and operational users.

The consulting role of safety experts was not forgotten. The proposed *safety tool chain* was conceived to be portable with a minimum of dependencies and with an open design simplifying the import of data from a

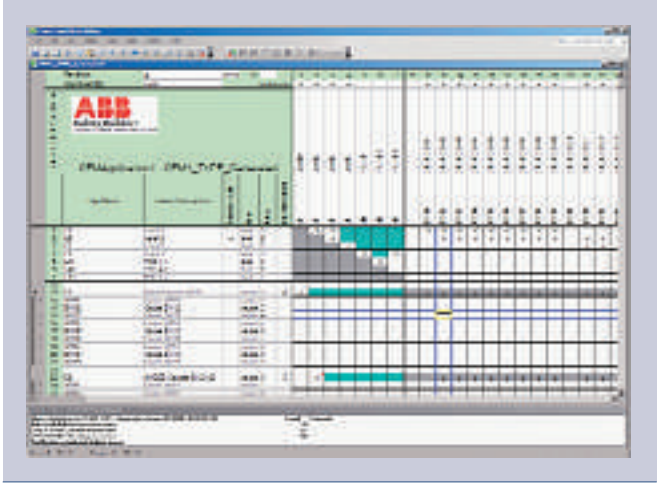
1 Compliance Manger screenshot.



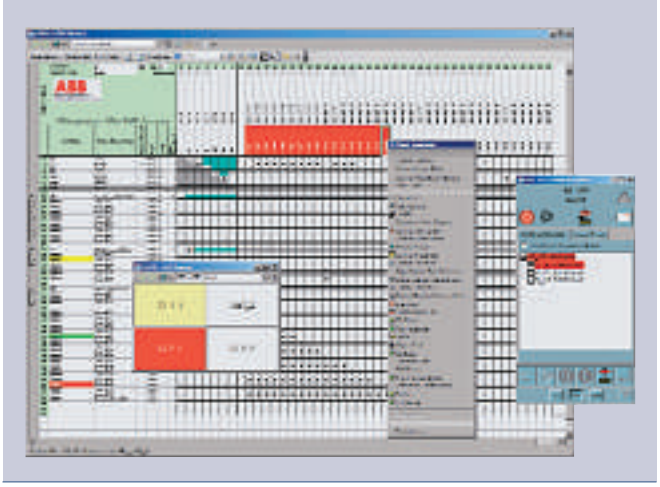
2 ABB TRAC (Trip Requirement and Availability Calculator) SIL Calculator screenshot.



3 System 800xA Safety Builder editor screen shot.



4 System 800xA Safety Builder viewer screen shot.



variety of sources. These features are essential for ABB's safety consulting engineers at customer sites and in customer training.

In 2004 pre-product prototypes were completed for both safety project management, and cause and effect matrix programming. These prototypes are discussed in the following sections.

Supporting safety project management

The ABB Process Automation business area has implemented formal and TÜV-approved safety management within its safety product development organization. This approval was a necessary pre-requisite for the successful development of the new AC 800M HI safety controller. The knowledge-path needed to gain approval provided valuable input to the prototyping of a tool which can be rolled out to project teams and customers: the "Compliance Manager".

Compliance Manager helps the user build safety teams, describe member competences and assign responsibilities using a responsibility-accountability (RACI) chart. The built-in compliance editor allows input of any requirement set. The IEC-61511 standard is pre-loaded so that the user can become productive immediately 1. The user can perform a gap analysis on the requirements and then automatically generate checklists and specification documents. The tool is also loaded with ABB's expert interpretation of IEC-61511 and their applicability to the company's own systems. This feature allows ABB engineers to respond quickly and uniformly to customer safety requirement specifications.

Safety system design and programming

After the Safety Instrumented Function (SIF)[2] has been configured, the reliability of all its components is input to a Safety Integrity Level (SIL) calculation to check that it meets the target risk reduction. This calculation is not trivial, especially when the effects of redundancy and common-cause failures are considered. Fortunately, a group of safety engineers at ABB Engineering Services in England had earlier developed a stand-alone SIL calculator called TRAC (Trip Requirement and Availability Calculator) 2. The ABB team in Norway compiled a roadmap for integrating the calculator with System 800xA and the other tools in the safety suite.

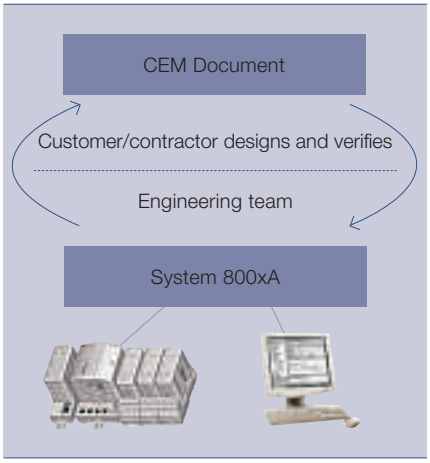
The SIL calculations are very useful for validating the SIF design, but they can also provide valuable data such as time intervals after which the customer must perform proof-testing on the SIF components. Other useful figures from this phase are the availability and total downtime, mean time between failures (MTBF), and the mean time to restoration (MTTR). There is a strong demand from project teams and sales engineers for integrated tools which can calculate and aggregate this data to all levels of a control structure.

At this stage of the lifecycle, all SIF hardware has been configured, but the safety application software has still to be implemented. The most challenging task in this phase is faced by programmers of large ESD/PSD (emergency/process shutdown) systems. These SIS systems span all process areas and access a huge number of process variables or "tags". Shutdowns are typically structured in a cascading hierarchy of many levels with the higher "emergency" levels tripping lower "process" levels.

Due to these special requirements, cause and effect matrix (CEM) programming has emerged as the de-facto standard for programming ESD/PSD safety systems or any system with interlock logic. In its simplest form, a CEM is a matrix containing named tags. The matrix symbols indicate that a "trip" of a column's effect occurs when the corresponding "cause" row is triggered 3.

To support CEM programming for IEC 61131 control platforms, ABB developed the "System 800xA Safety Builder" toolkit. The Editor tool helps users specify complex emergency and process shutdown logic visually and intuitively with a matrix grid. High-quality SIL-certified code for the new AC 800M HI controller is automatically generated from this matrix.

5 Flexible "cause and effect" programming.



The "Viewer tool" can then be invoked to generate a fully-integrated System 800xA operator display and navigation element 4. The navigation element shows the aggregate alarm, or inhibit status of the entire safety system divided into process areas "sheets". With one click, the operator can drill-down to the sheet in alarm and see at a glance which devices and which levels have been tripped. One-click navigation to all the system's devices is provided.

The System 800xA Safety Builder tools build on the success of the Safety Builder product for Safeguard, adding many new features and more flexibility. System 800xA Safety Builder introduces the powerful concept of "single-source engineering": drawing, programming and display all based on the same underlying document. The design approach enables the underlying CEM document to be shared with contractors who are not System 800xA equipped. They specify the design in the matrix and then send the document back for System 800xA code and display generation 5. This facilitates flexible and distributed development practices.

Translation errors are eliminated by automatically generating the control logic and operator display from the same safety design matrix. This reduces initial engineering effort by a factor of ten and makes modifications easier to implement, test and trace.

Robert Martinez
Per Christian Juel
ABB Corporate R&D
Billingstad, Norway
robert.martinez@no.abb.com
per.c.juel@no.abb.com

Per Fjelldalen
ABB Process Automation
Oslo, Norway
per.fjelldalen@no.abb.com

Footnotes

1) Taft, Mark W., "IndustrialIT System 800xA, Extending the reach of automation to achieve continuous productivity improvements", ABB Review 1/2004 pp 32–37.

2) See also pp 47–50 in this edition of ABB Review.