 © 2008 IChemE

INTEGRATING RISK INTO YOUR PLANT LIFECYCLE – A NEXT GENERATION SOFTWARE ARCHITECTURE FOR RISK BASED OPERATIONS

Dr Nic Cavanagh[1], Dr Jeremy Linn[2] and Colin Hickey[3]
[1]Head of Safeti Product Management, DNV Software, London, UK
[2]Regional Manager, DNV Software, London, UK
[3]Safeti Product Management, DNV Software, London, UK

Over the last three decades, technology for assessing the risks associated with operating major accident hazard facilities has been continuously developed. Over this period the accuracy and speed of the modelling on which this technology is based has improved enormously. The tools for modelling the effects of hazardous releases in terms of emergency response, safety management and Quantitative Risk Analysis (QRA), for example, are now well validated and used extensively by industry. Also, the processing power necessary for using these tools is now routinely available on a typical desktop computer. Other quantitative tools are beginning to appear which use related technology to assist in improving operational performance, particularly for inspection and maintenance planning activities. These tools are also progressively integrating more directly with operational management systems like SAP, ERP and ERM.

Commercial analysis tools like Phast, FRED, Trace and Canary for effects modelling, Safeti, Shepherd and RiskCurves for QRA and Orbit and RBMI for RBI are becoming more and more widely used. These tools are generally used standalone and independently of one another and other design and operational systems, even though they share much common data with the latter. Applying risk technology more directly into the plant life-cycle through integration with design and operational management systems has not kept pace with improvements in other areas.

As developers of Phast, Safeti and Orbit, we are committed to our technology being used throughout the plant life-cycle and that it is as closely integrated with our customers' value chain as possible. This paper describes our vision for a next generation architecture supporting this integration, the development of which is ongoing. A prototype of this architecture, "The Safeti™ Risk Framework", will be presented along with a longer term vision for a fully integrated risk based operations system linking risk technology with mainstream design applications and operational management systems through application of other risk management techniques

CURRENT SITUATION

The maturity of risk management in the process industry has seen much advancement in the areas of hazard analysis, risk analysis and risk assessment. Global recognition of the need for professional risk management has driven the creation of demanding legislative requirements and successful commercial products and services. This has occurred in

parallel with greater need for transparency to the public, increased scrutiny of process plant activities and greater demand for better business performance.

The wide range of advanced tools and methodologies used in risk management have been enhanced greatly by the IT revolution. Advanced consequence modelling tools like Phast continue to be developed to meet the evolving and more stringent needs of hazard and risk analysis in the process industries.

The process industry has in parallel started to take advantage of advanced products and services for other areas of business management. Advanced systems are used for process control, asset management, management systems and financial management.

COMMONALITY

Process facilities have a range of attributes which are drawn upon, measured and controlled as part of the business value chain. Attributes such as people, materials, plant, buildings, transport, utilities, governing legislation, processes, weather conditions and market economics are all part of the dynamic environment process plant operators conduct business within. Specialist tools have been developed to support business optimisation through measuring, monitoring and/or controlling each of these attributes. For this reason many tools and services used across a process plant and within process industry organisations handle and use the same information. (Cavanagh and Linn 2005)

Worthington and Cavanagh 2003, introduced the concept of a data asset as illustrated in Figure 1. Data is contributed throughout the lifecycle of a plant from many sources. Plant design and CAD applications contribute during the design phase, process simulation during design and operational phases, GIS and safety management tools during design and operation, and so on. These data sources add value in relation to how well they can be kept up-to-date, shared and re-used. The Risk Framework provides a means of accessing, maintaining and sharing this data asset.

One example of a system which uses the latest technology and methodologies to measure and manage attributes of a processing facility is a fully integrated process control system. Such systems are used to measure the state of equipment and materials throughout the site. The control system tracks process conditions and, with operator control, makes adjustments to keep process conditions within predetermined limits. This approach ensures design conditions are met and sustained, process efficiency is optimised and also that non-design and potentially hazardous conditions do not arise. In addition to process control, control systems often contain hazard detection devices such as hazardous gas and fire detectors. These devices feed back to decision logic in the control system enabling hazard mitigating response to be carried out. The continuous live feed of data surrounding process plant conditions are common with the generic data used in hazard and risk analysis. Yet in contrast to live control system control and response, a risk management study is off-line and merely a snapshot of design or identified potential non-design conditions.

A second example of a system which uses the latest technology and methodologies to measure and manage attributes of a processing facility is an enterprise wide asset

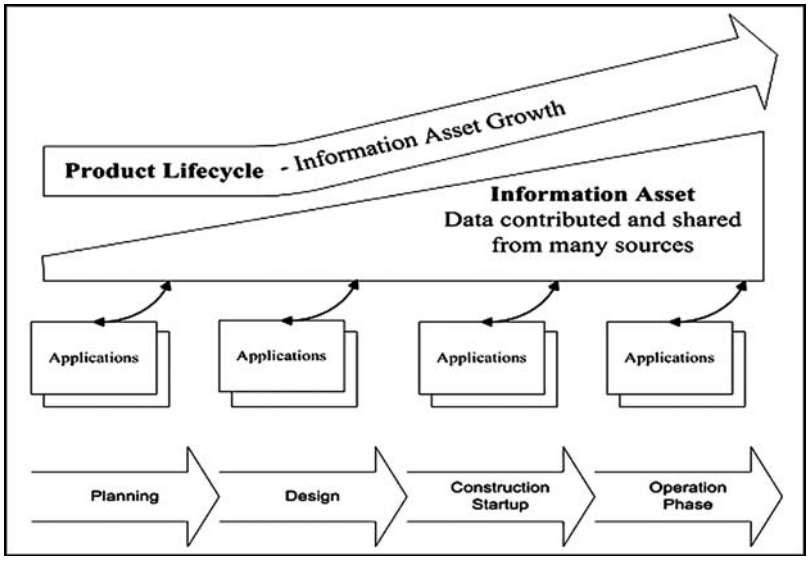

Figure 1. The data asset concept

management database tool. Such systems are used to store and track the wide range of data associated with plant equipment. Modern extensions of these tools provide support for maintenance and inspection management. Risk analysis is already incorporated into asset management tools enabling risks to be quantified for Risk Based Inspection (RBI) using software such as Orbit.

RISK AS A DECISION MAKING TOOL

Today risk analyses tend to be performed as an offline activity by risk specialists either to meet the needs of legislative requirements or as part of a plant modification to reduce risk. These tend to be snapshot studies that are filed once the relevant decision has been made or legislative requirement satisfied.

In recent years techniques have been developed to extend the applicability of risk technology beyond basic assessment of the severity of an incident or its likelihood of being realised. Techniques like the bow-tie approach and Layer Of Protection Analysis (LOPA) take account of the barriers and mitigators put in place to prevent an incident from occurring or escalating or to mitigate its effects if it does occur. All these related activities can be monitored and high risk operations avoided or extra safeguards put in place.

Used effectively in operational decision making these techniques can reduce operational risk and the likelihood of an incident that may result in a loss of life or to the

profitability of a plant. So called Risk Based Operations or RBO enables decisions to be made based on knowledge and understanding of risks attributable to certain operations or processes, both before and after any operational changes are implemented.

As has been mentioned earlier QRA tends to provide a snapshot of the risks associated with a plant under a particular set of conditions. If extended to cover a multitude of scenarios or to take account of changing operational conditions, these quantifications of risk can, when combined with operational risk management techniques, provide a real time measure of the risk to which a plant is exposed. These kinds of systems are able to provide operational managers with quantitative real-time data, rather than static assessments, to support their decision making in an ongoing basis.

This kind of risk-based decision support offers increased benefit from risk analysis, bringing traditional QRA technology and methodology into the operational phase of the plant life-cycle. By using this information in a more dynamic and holistic manner, QRA is brought from the back-office into the daily operational management of your facility.

THE SAFETI™ RISK FRAMEWORK

It is our vision that risk management tools will be used throughout the lifecycle of the plant from design to operation and beyond. Risk management should support engineering design and day to day operation of the plant through live measures of activities and circumstances and use these to model the implications on and potential changes to a business's overall risk exposure. This will provide instant decision support and accurate perception of real time risks leading to continuous risk optimisation and reduction.

We believe best risk management practice is now achievable through the parallel evolution of software, data management and internet technologies already proven and in use by businesses globally.

The vision for the Safeti™ Risk Framework (Figure 2) is to help make risk based decision support a reality at all stages of a plant's lifecycle. By integrating the wide range of existing risk management tools and currently non risk-based process plant management tools into one complete system, risk becomes a key input to the decision making process.

Data of relevance to the risks associated with a process facility will feed in and out of all of the existing tools in a flexible manner. The diagram above illustrates how, for example, asset data relevant to a QRA can be reused for an RBI. It also demonstrates how, for example, a Matrix of Permitted Operations (MOPO) as part of a risk assessment system can use information from the asset database and risk measures to feed the control system or management system for risk based decision support.

The Risk Framework concept creates benefits at a number of levels. Reuse of data, live risk based decision support and integrated business management are some of the many benefits derived from the approach suggested.

The following scenarios illustrate how the Safeti™ Risk Framework can help to avoid undesirable situations arising from typical process plant circumstances.

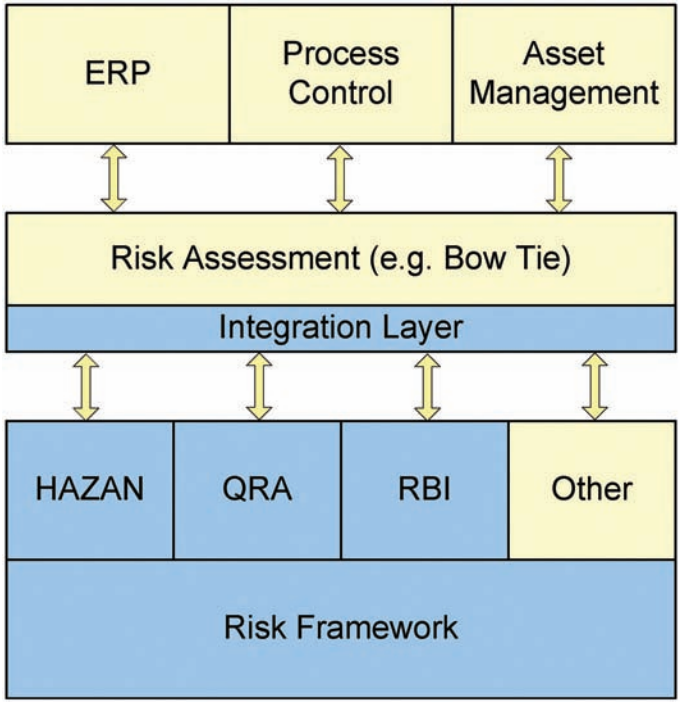

Figure 2. The Safeti™ Risk Framework concept

SCENARIO 1. MY PUMP HAS A FAULT AND THE PARALLEL RESERVE PUMP IS SCHEDULED TO BE DOWN FOR MAINTENANCE WHICH HAS NOT STARTED YET. CAN I USE THE RESERVE PUMP?

This is a commonly occurring situation in the process industry. It involves interaction between a control system for switching the pump on or off, a permit to work system which is part of the management system and a number of assets; pumps, valves and pipework.

Many approaches have been developed to deal with the safe interaction between these business processes. For example, electrical isolation of the pump can be applied to override the control system preventing it from starting a device when it is in an unsafe state that the control system cannot measure. In addition, a permit to work system is a document based activity used in management systems to control and monitor the status of process equipment for clarity and safety during manual operation and maintenance.

In scenario 1 the following are a selection of potentially undesirable events arising from failure of interaction between the controlling and monitoring business processes on the site:

1. The paper based permit to work document indicating that the pump was unsuitable for operation had been logged incorrectly giving the impression that the pump was fit for service.

2. The control system is independent of the permit to work system and maintenance scheduling tools. It may detect that the state of the process equipment is normal and allow for remote commands to be sent to the process equipment for start up leading to undesirable circumstances.

Information involved in this scenario which will be linked via the Safeti™ Risk Framework:

- Asset database
- Equipment design conditions
- Live process conditions, supplied from control system devices
- Maintenance Schedule
- Live status of risk picture on site based on current circumstances
- Rules and responsibilities within the management system governing maintenance schedule and permit to work

The undesirable outcomes of this scenario could be avoided by having one hub with access to all interrelated risk relevant information. An electronic permit to work system tied to high risk equipment provides transparency of plant status for safe operation. Also, the live intelligent permit to work system, integrated with the control system provides a software back-up for the hardware electrical isolation. This creates an extra layer of protection in cases of management system processes failure. Ultimately the status of each piece of process equipment could be found by drilling down through details on an enterprise wide risk dashboard.

SCENARIO 2: DUE TO INCREASED PRODUCTION AND SIMULTANEOUS CONSTRUCTION AND ENGINEERING PROJECTS, MORE STAFF ARE REQUIRED ON MY SITE. CAN I TEMPORARILY LOCATE THEM AT THIS LOCATION?

The spatial layout of population can change the risk picture of a process facility. Locating temporary buildings, for example, can become a critical part of a facility's risk exposure. This is the type of decision where risk based support can be critical in the safe operation of a site.

It is often the case that the offline, periodic reports created to comply with some European countries' local implementation of the EU Seveso Directive or the consequence based US Risk Management Programme (RMP) form the foundation for the overall risk management of a process plant. These reports are therefore usually offline – taking idealised standard operating conditions or hypothetical non-ideal operating conditions.

They are also usually out-of-date soon after they have been created due to the dynamic operating environment of modern process plants.

A site being managed with mature risk management processes will undertake what-if studies using tools such as Phast and Safeti. These effectively predict what new risk or hazard levels may be posed due to required changes to a site. An arbitrary line is often drawn under activities for which potential hazards and overall risks are assumed to be tolerable. The overhead of performing risk assessment is often a disincentive to it being carried out.

The undesirable events posed by selecting different siting locations for temporary staff facilities can be described using firstly individual risk contours overlaid on population siting options giving a qualitative assessment of risks. In this example based on one simple failure case individual risk contours are generated in the form illustrated in Figure 3.

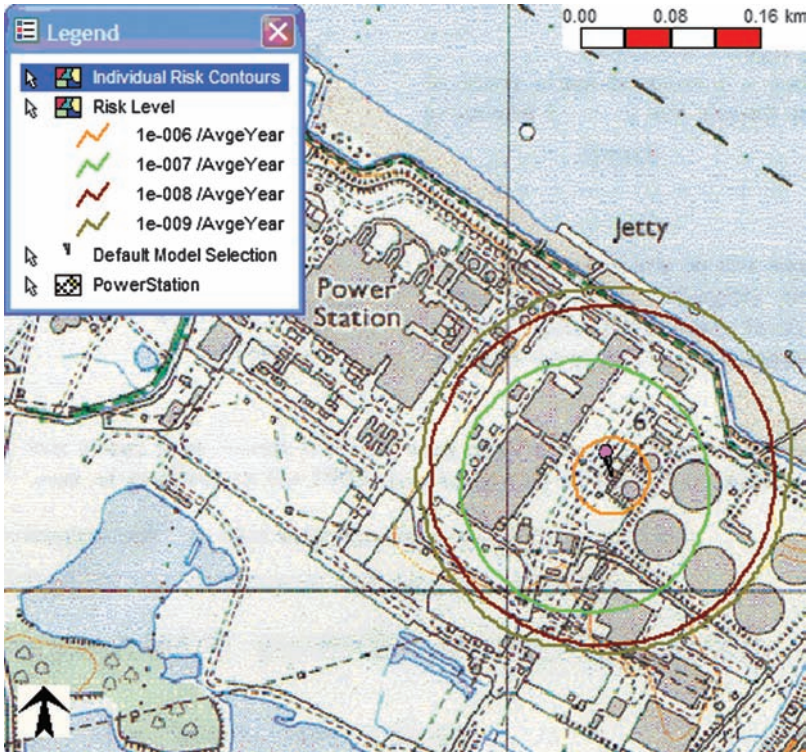

Figure 3. Individual risk contours of Scenario 2

For this particular facility we have two temporary office siting options as illustrated in Figure 4. Both options require temporary accommodation to be sited close to the source of hazard also illustrated in Figure 4. But each option will pose different levels of societal risk. This is traditionally enumerated using F-N curves as illustrated in Figure 5. As can be seen in the societal risk comparison from the F-N curves in Figure 5, option 2 is the preferred location in the context of risk.

The Safeti™ Risk Framework concept will help to make such decision easier by having all necessary input data continuously linked to the organisation's risk management console as illustrated in Figure 6. What-if studies can be performed quickly and thoroughly.

In addition to what-if analysis the same functionality within the Risk Framework can be used as a continuous monitor of real time risks, providing a live risk dashboard for the site.

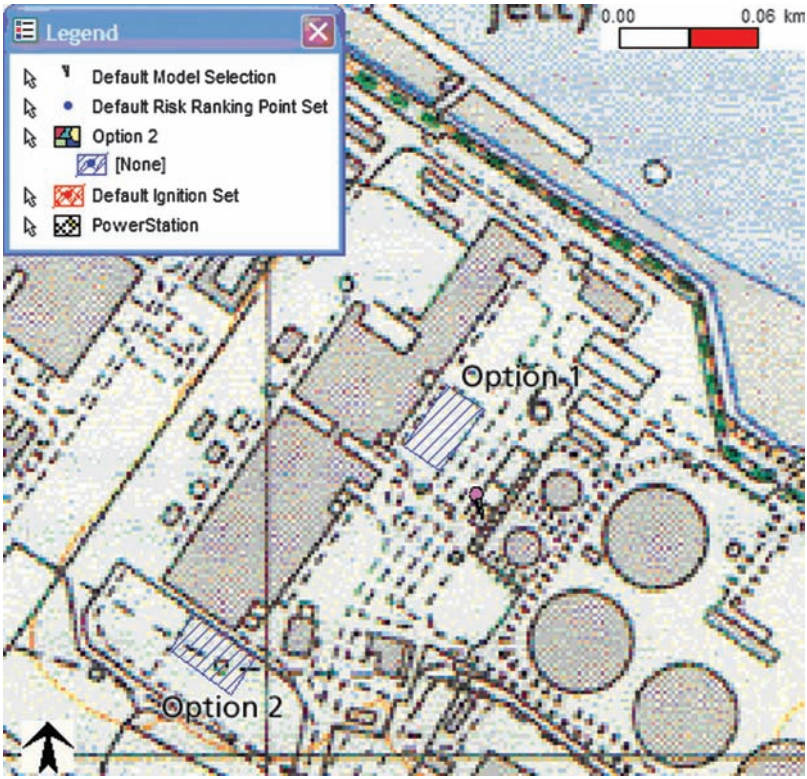

Figure 4. Two temporary office siting options

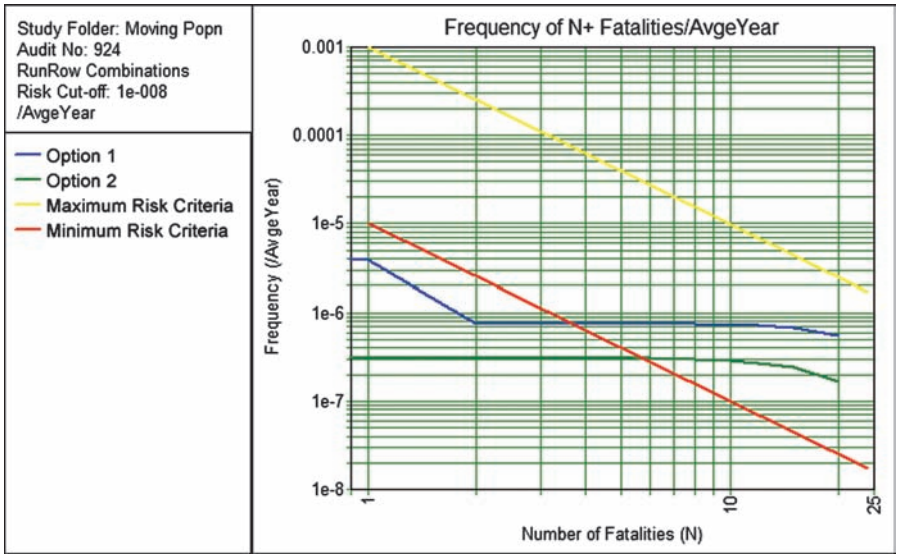

Figure 5. Societal risk comparison of two office location options

This requires the Risk Framework to be continuously processing the risk relevant data on the site to calculate the live risk picture. The typical measures of risk – societal and individual – would be calculated continuously as various aspects of site conditions change. With individual and societal (e.g. risk integral) risks continuously displayed with drill-down capabilities for easy identification of main contributors in terms of both equipment and personnel.

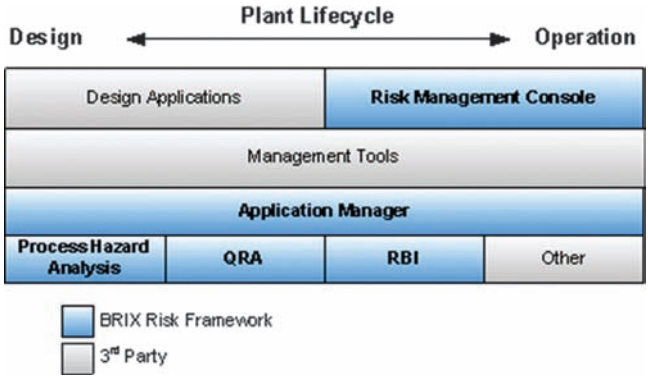

Figure 6. The Safeti™ Risk Framework architecture

THE SAFETI™ RISK FRAMEWORK ARCHITECTURE

DNV Software already manages an array of world leading risk management software tools. The Risk Framework concept is an evolution of these tools providing, amongst other things, the next generation architecture for these tools. This is the enabler facilitating integration of existing technology with new technology and 3rd party systems. The resulting risk framework service platform supports full lifecycle management. This ensures cost effective reuse of an organisation's data asset and delivers real time risk based decision support for design and operation.

At the core of the Risk Framework is the plant's asset database. It is from here that all activities begin. From hazard analysis through frequency analysis to control and management system decision support through the Risk Management Console/Dashboard all data pivots on the underlying asset database. At this stage the Safeti™ Risk Framework exists in prototype form and will be the basis for the next generation of the Phast application which is well underway. A key development is the evolution from a scenario based to an equipment based model.

This facilitates integration of the underlying data models for QRA, RBI and PHA in Safeti, Orbit and Phast respectively. This is also the first step in integration with 3rd party applications, CAD and other databases and provides the enabler for integration with other operational systems. A further development is the ability to map data from one model or data source to another using a configuration utility rather than hard coded into the software. Again, this development has previously been prototyped and is now well under way.

REFERENCES

Cavanagh, NJ. and Linn J., April 2005, Beyond Compliance – The Future Role of Risk Tools, AIChE Global Safety Symposium, Annual Conference of Centre for Chemical Process Safety, Atlanta, Georgia, USA

Worthington, D.R.E. and Cavanagh, N.J., June 2003, The development of software tools for chemical process quantitative risk assessment over two decades, ESREL 2003 Conference, Safety and Reliability, Maastricht, The Netherlands.