

Most risk managers and employees in energy companies are familiar with the concepts of market risk and credit risk, but operational risk is receiving more attention in corporate boardrooms these days, writes *Sandy Fielden*

Coping with setbacks

★ To understand the term ‘operational risk’ and its use in risk management, I turned to three documents that seek to define risk management theory and practice. In their ‘Introduction and executive summary of recommendations’, published in November 2002¹, the US-based Committee of Chief Risk Officers (CCRO) listed nine categories of merchant energy business risks.

The list includes four types of risk linked with markets and credit, as well as five types of risk associated with company operations. The operational risks were defined as follows:

- business continuity risk: the risk of loss from a disruption of normal business functions where the expected time to return to

“Human greed will always attempt to exploit weaknesses in financial systems. Energy risk managers must pay more attention than most to this operational risk”

Sandy Fielden

normalcy would materially affect the ability to maintain customer commitments and regulatory compliance;

- operations risk: the risk of loss resulting from energy assets failing to perform as expected, such as unacceptable forced outage rates and poor availability factors – includes construction risk;
- operational risk: the risk of loss resulting from failed or inadequate management of internal processes, people, and systems once in place in the organisation;
- volumetric risk: the risk of not being able

to deliver a contractual amount of energy, including operations risk as well as the impact of other external uncertainties (eg, weather);

- staffing/organisation risk: the risk that the organisation does not have adequate resources to successfully execute the business strategy or that it uses them inappropriately.

Addressing operational risk

In November 2005, the governing body of the world’s commercial and central banks, the Basel Committee on Banking Supervision, published an updated version of its Basel II – ‘International convergence of capital measurement and capital standards’² – a series of recommendations designed to bolster the capital adequacy of the banking system. Basel II directly addressed the issue of operational risk, which was defined as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.”

The definition includes legal risk, but excludes strategic and reputation risk.

Basel II recommends three methods of managing operational risk, depending on the sophistication of the financial institution involved.

The most advanced approach requires that “the bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures concerning the operational risk management systems, which must include policies for the treatment of non-compliance issues”.

The 2002 Sarbanes Oxley (Sox) legislation in the United States³ also addressed the

operational risk of poor or failed internal controls in companies. Specifically, sections 302 and 404 require that the chief executive officers' and chief financial officers' independent auditors and audit committees "certify the accuracy of financial statements and disclosures", "indicate whether there were significant changes in internal controls and disclose all deficiencies in the design or operation of internal controls", "provide auditors attestation to, and report on, management assessment of the internal controls and procedures for financial accounting" and "report that controls and procedures for financial reporting and disclosure have been evaluated for effectiveness within the past 90 days".

These documents tell us that operational risk is a recognised fact of business life and that appropriately managed companies are required to implement policies and procedures to address its implications. However, they also tell us that operational risk can be a lot less obvious to quantify than market or credit risks.

For anyone involved in the delivery of energy to customers, it has always been a fact of life that a capital-intensive and technically complex business is subject to the vagaries of the elements. For every fierce rainstorm, there are downed power lines preventing the delivery of electricity. Major tropical storms multiply the impact on infrastructure.

Accounting for the elements

During the autumn of 2005, Hurricanes Katrina and Rita blasted through the US Gulf, causing havoc to offshore gas drilling facilities. The hurricanes then knocked out refineries and flooded facilities onshore. The impact on business in terms of loss and damage was bad enough, but the subsequent impact on energy supplies and prices reverberated around the globe (see figure 1).

One common approach to mitigating the risk of weather disruption is by including a *force majeure* clause in contracts for physical delivery of commodities. The clause essentially frees one or both parties from liability when an extraordinary event beyond the control of the parties, such as flood, war, riot or act of God, prevents one or both parties from fulfilling their obligations under the contract.

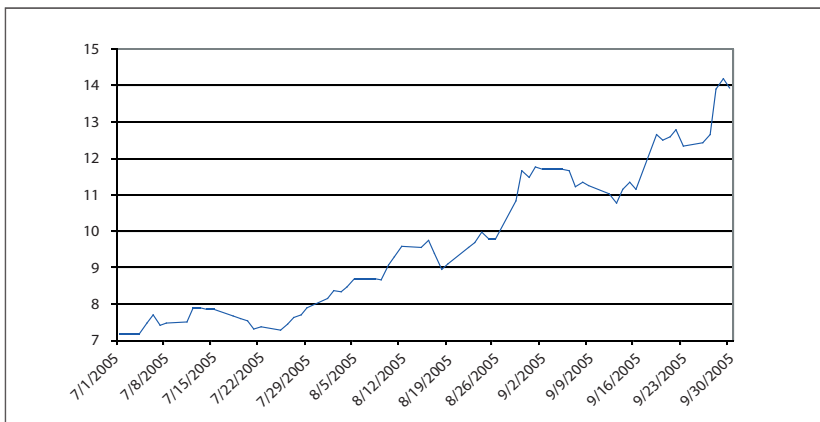
Notably, the Henry Hub terminal in Sabine Louisiana, was flooded by Hurricane Rita in September 2005 and forced to declare force majeure on deliveries, causing a quandary in the financially-traded Nymex natural gas futures market, which uses Henry Hub as its delivery point. The Nymex extended the delivery period for contracts until the facility was restored.

Force majeure simply reduces the contractual risk of not being able to deliver because of a crisis. Energy companies must also invest in insurance against flooding or other disasters that is often costly.

The sheer scale of the facilities involved in energy production and distribution have always made insurance critical. In some cases such as nuclear power plants and oil tankers, significant investment upgrades are required ahead of time to reduce the risk of disaster at any point in the future.

The 'volumetric' risk that the CCRO referred to in their definitions is another area of operational risk that is, perhaps, peculiar to energy companies. Simply defining volumetric risk as the inability to deliver, hides a magnitude of problems. Oil traders are all too familiar with density and temperature issues that alter the volume of large shipments significantly en route.

For many years, North Sea Brent contracts for physical delivery contained a 5% variation clause that permitted over or under delivery of 5% of the cargo. This flexibility was



F1. Henry Hub Natural Gas Futures (US\$/mmBtu)

Prices for Nymex Henry Hub natural gas rose significantly after Hurricanes Katrina and Rita interrupted gas production from rigs in the Gulf Coast and flooded onshore facilities during August and September 2005.

designed to help the seller operationally, but was removed when traders abused the system, for example, to short-change buyers when prices were lower than expected.

Aside from volume, product quality is frequently an issue in oil trading. Cargoes have to meet vigorous product specifications to be accepted by the buyer. If the cargo is 'off-spec', then it can be rejected by the buyer and despite continued freight costs, become a floating liability if the market hears it is 'distressed' due to poor specifications.

Volumetric risk in oil is quite easy to understand, but the same issue also impacts on the natural gas and electricity markets. Gas pipelines have to be maintained at standard pressure in order to operate efficiently. In many cases, low inventory of gas triggers an operational flow order from the pipeline company, requiring shipment of gas that may have little commercial value.

Electricity is the most complex energy form to deliver. The absence of storage (outside of hydroelectric plants) makes electricity markets prone to delivery issues. The worst events are system blackouts such as the event

triggered in the Midwest in August of 2003. The blackout left most of the northeastern United States and parts of Canada without electricity for more than a day. The impact on electricity pricing mechanisms was severe (figure 2).

The Basel II and Sox regulations did not address energy specific operational risks, but instead focused on human and system failures in organisations. Much of the intent of Sox for example, is to do with setting in place control and compliance procedures to prevent rogue individuals or poor management from damaging the business or more specifically, shareholder value. A lot of the impetus of Sox legislation, however, came from the events at Enron in the autumn of 2001.

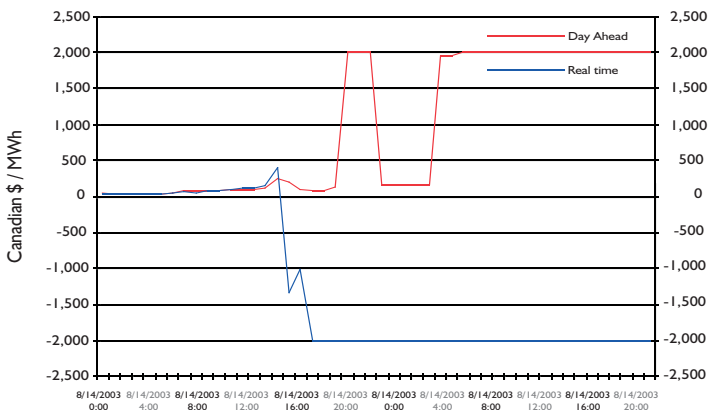
As I write, the senior managers of Enron are being tried in federal court for alleged crimes such as misrepresenting the company's results to shareholders. Stories of 'rogue' traders such as Nick Leeson at Barings Bank in Singapore (who lost the company \$10 billion by covering up trading losses until it was too late) have always made headlines.

The bottom line of the new regulations appears to be that human greed will always attempt to exploit weaknesses in financial systems. Energy risk managers must pay more attention than most to this operational risk, if for no other reason than that there are always large sums of money involved in energy trading. There is no need to explain to an electricity system operator the importance of system reliability. Electricity-generating plants, gas pipelines and oil refineries all operate around the clock, seven days a week.

Vulnerable to systems failure

Operational systems risk is endemic to the physical business. For energy companies, the costly possibility of equipment failures has always required elaborate maintenance schedules and duplication of units. The 'unplanned outage' is the worst enemy of normal operations because of its impact on storage, production and distribution.

Increasingly, however, the trading operations of energy companies have become hostage to a new system risk – that of computer failure or error. Of course, the risk of computer failure inspired an overnight industry in 1999 to fix the Y2K bug and much of that turned out to be a false alarm.



F2. Canadian Ontario Electricity Prices at Canadian Border with New York on August 14-15, 2003

A power blackout between 3.00pm and 4.00pm in the US Midwest on August 14, 2003, that affected the whole of the northeastern United States, led to wild gyrations in the Canadian (Ontario) electricity market. As the failure occurred, price signals in real time went to minus Canadian \$2000/megawatt hour (MWh) to encourage generators to shut down at the border with New York. At the same time, pre-dispatch hour ahead prices soared to plus Canadian \$2,000/MWh to bring power back onto the grid, once the outage ended. A price range of \$4,000 in a single 24-hour period like this demonstrates the extent of operational risk in electricity markets if there is an unplanned outage.

Usually, computerisation entails devising plans for the backing up of trading systems. Traders are also relocated to alternative trading facilities when systems go down for any reason. The risks of not being able to continue trading in an environment where markets may be in turmoil justifies heavy investment in continuity plans.

On a smaller, but perhaps, no less significant scale, reliance on computer systems exposes companies to the risk of the old adage 'garbage in, garbage out'. In other words, putting bad data into systems makes the output useless, too.

A 'fat finger' typing error by a natural gas distributor in North America in November 2004 led the Energy Information Administration to significantly underestimate United States gas storage for the previous week. When the result was published, Nymex gas futures prices rose 15%. It is estimated that the cost to the industry runs into millions

of dollars. This is not an isolated incident, however. Similar errors occur all the time inside company's systems. Managing the risk of data errors requires careful attention to where data comes from and how accurate it is.

In conclusion, operational risk covers a broad range of human and system issues that all companies are now required to consider and respond to.

For energy risk managers, it seems that the scope of operational risks are multiplied by the sheer scale and cost of sourcing and delivering energy to customers. Although no stranger to *force majeure* and high insurance costs, the new paradigm of tight supply and the possibility of continued turbulent weather mean operational risk management cannot be overlooked today. **ER**

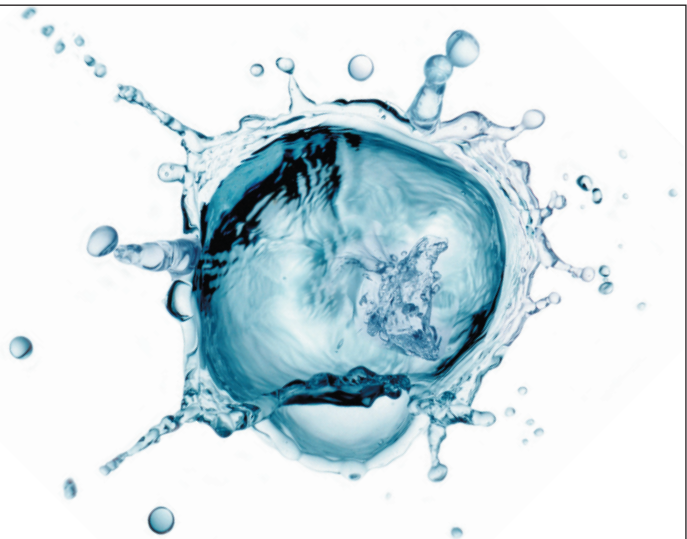
Sandy Fielden is energy products manager at Texas-based software provider Logical Information Machines
E-mail: sandy@lim.com

Footnotes

1. 'Introduction and executive summary of recommendations', published in November 2002 (www.cro.org/pdf/intro.pdf).
2. 'International convergence of capital measurement and capital standards', (www.bis.org/publ/bcb118.htm).
3. The Sarbanes Oxley (Sox) legislation in the US (www.law.uc.edu/CCL/SOact/soact.pdf).

Big splash

Low cost



Reprinted sections of *Energy Risk* are a high-impact, cost-effective promotional tool.

Reprints can be customised with your company logo and adverts. For bespoke pricing and packages to suit your business requirements please contact: reprints@incisivemedia.com

www.incisivemedia.com