Keeping the lights on

Matthew Stibbe
matthew@stibbe.net

Energy companies need to be schizophrenic: it helps them deal with their dilemmas.

Energy companies run two types of information system: on one hand, they run real-time mission-critical systems where the smallest deviation from the norm warrants professional attention; on the other, they run conventional business systems where huge sums are lost in rounding errors or managed according to risk.

But many of the engineering systems use old equipment that can't run the latest software, the cost management beanies want them to use standard hardware and software to cut costs, and the telecommunications companies are all shifting to that bastion of data security, the Internet Protocol.

If that weren't enough, they face elevated risks from climate change and associated legislation, eco-activists and even terrorists. On top of this, they still have to keep the business running.

Legacy systems

As an industry, "we have an issue with legacy systems," explains John Tanner, security consultant at RWE Npower. Whether it is control systems running on antique hardware, in-house applications that are too expensive to rewrite or third-party software that doesn't run on modern computers, the energy industry as a whole deals with more than its fair share of history.

The problem is particularly acute in automation software installations. Manufacturers certify the systems against software configurations, which means that they do not guarantee that it will work if, for example, the underlying operating system is upgraded by installing a service pack.

Scottish Power's Graeme Agnew: identifies need to collaborate

It's a dilemma the software industry as a whole must solve: their customers are damned if they break the suppliers' warranty, and damned if they create a security problem by not upgrading.

Individual companies, like RWE Npower, have rolling programmes of upgrades, but these raise new and different challenges. The industry is moving towards off the shelf hardware and software solutions and towards IP-based networking, albeit at different rates and with some circumspection.

"I would be surprised if there is a company out there that isn't considering moving to IP," said Graeme Agnew, group IT security manager at Scottish Power.

Such a move brings risks as well as benefits. On one hand, there is usually increased functionality for engineers to actually manage the power infrastructure and interconnections with other business processes. On the other there is increased exposure to risk.

"Scottish Power has diverse business units from call centres to power management," says Agnew. "For example, if control systems can connect and understand information coming from call centres (e.g. reports of outages) they can manage power issues better."

Divide and conquer

But making these connections risks exposing critical control systems to outsiders.

"Like most generator systems we have two networks, the business infrastructure and the SCADA (supervisory control and data acquisition) networks. These are mostly separated from the outside world. Companies don't usually link SCADA networks to infrastructure and public networks," explains John Tanner.

RWE Npower is an integrated power company that generates, distributes and sells electricity to seven million consumers. Because the control systems for power plants and distribution networks run on completely isolated networks, staff typically have two terminals on their desks, one connected to the proprietary operations network and another connected to the business network using commercial protocols.

The operational networks use point-to-point communications topographies rather than IP-style internets. This limits the access

that a would-be hacker might achieve by subverting a remote node. Its SCADA systems also run on dedicated leased lines and dial-up links rather than public data networks.

Doug Houseman is an enterprise architect in the energy sector at IT consultancy Capgemini. He half-jokes that "one of the nice things is that most of the communications protocols we use were designed in the 1950s and people have lost the documentation so hacking into the system wouldn't do you any good."

Nuclear security

The nuclear power industry is a good role model[I1] , says Houseman. "The good news is that we've been doing (watertight security) for 25 years," he says. "So if there's any model we like, it's the nuclear power plant model. I defy anyone to get into a power plant without someone knowing that they're there."

Non-nuclear power plants are catching up by applying similar levels of physical security. They are also applying the same levels of vetting to employees. Screening means that it can take 10 to 15 years of service to be given access to a control room and, even then, two people tend to monitor each system.

Equipment, components and software undergo similar grilling when they are brought on-site and installed in critical systems.

But the N-word raises the spectre of terrorism, which hovers over the whole sector. People are reluctant to talk about the details of their defensive measures.

People are reluctant to talk.

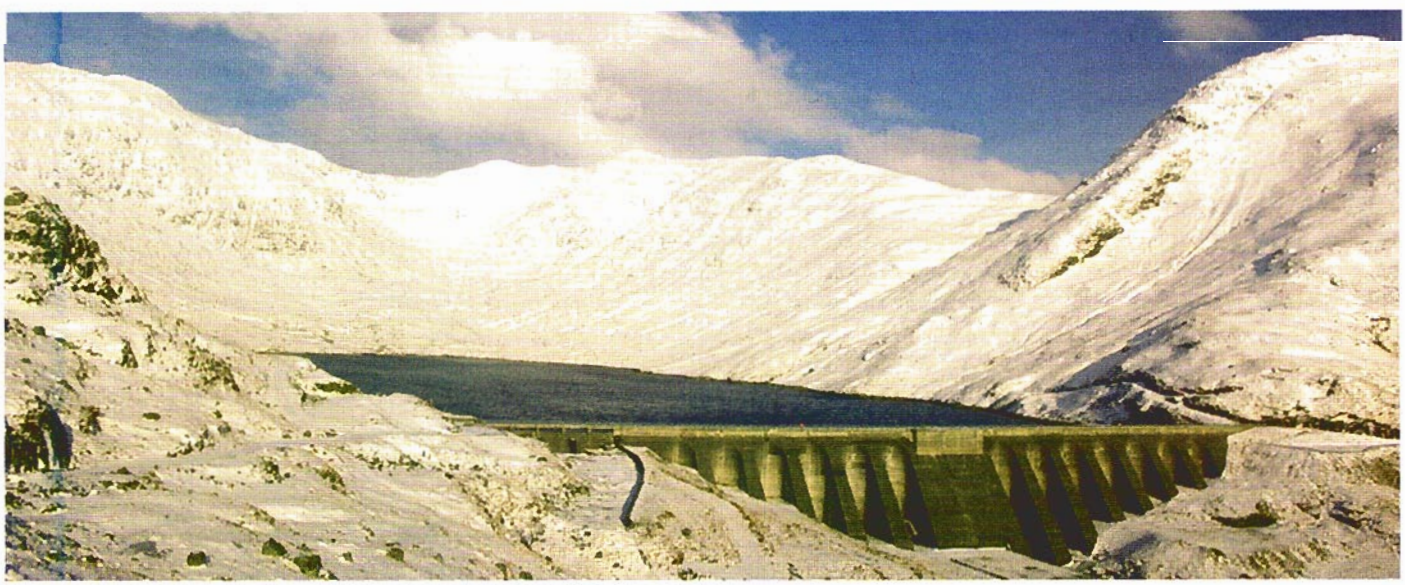
"There are groups out there that want to switch the lights out ... we have discussions with government agencies in key areas," said one industry insider.

"We do worry about threats to national infrastructure," says John Tanner, "but the scale and size of the company also makes us a target."

But many people worry more about the gas network than the electricity grid. Without electricity life becomes difficult, but gas explosions wreak physical havoc. As a result of national security concerns, information has disappeared from public websites. Maps of transmission grids or pipelines were taken down soon after 9/11.

In addition, the industry is paying a lot of attention to intrusion detection [I3] and other sensors to make sure that people can't tamper with the supply meaning surveillance and monitoring of physical systems rather than intrusion detection in a network sense.

Doug Houseman is more candid than most. "We're doing a lot of electronic monitoring that we didn't use to do. We're worried about the endpoints that go into factories and office blocks. While eventually we'll be able to monitor anything anywhere with automatic meter reading, we're going to start with the places that would cause the biggest headlines and a lot of that equipment is already in place."



Cruachan power station: spot the cyber terrorist. Picture © Scottish Power.

"a choice of having their caking or eating it"

Business continuity

The electricity and gas networks are critical elements of the national infrastructure. This demands the highest standards of risk management and contingency planning to ensure business continuity. The industry is coy about details, but it is clear that there are protocols to make sure that taking out a control station or even a power station doesn't break the whole system.

As most Britons know, the weather ensures these are tested every winter. Using a similar approach to the banks', energy companies have installed and tested disaster recovery centres. Vital systems are kept ready on a hot back-up basis with additional step-up equipment ready for delivery on a pre-agreed timetable over the following days and weeks.

Energy exchange

The ability to trade energy is an important part of Britain's deregulated industry. It allows suppliers who sell to end-users to source power from different generators and balance fluctuations in capacity and demand. It is also an important part of the redundancy needed nationally to make sure that the lights stay on. Some 178 parties trade on Britain's wholesale electricity market. This is run by Elexon which subcontracts software house Logica to run the central services that keep the electronic market running smoothly.

Protecting these transactions is vital. Most trades are made by exchanging encrypted files over a private network that connects the parties. "Our main priority is the integrity of settlements. Everyone has to get paid in the end. The correctness of this data is imperative," says Paul Broderick, a consultant at Elexon.

"Central Services is very resilient. It has a number of firewalls, back-up sites, cutovers between databases, and all of that."

Business as unusual

Moving from the control systems to more recognisable business IT infrastructure, energy companies face the same challenges that every business has to deal with, such as viruses and firewalls, protecting customer data and financial transactions, encryption and authentication.

"The key thing is that Scottish Power has assessed the risk to all its business processes and we have identified what systems are critical to the business," says Agnew. "We tend to align our funding against the critical systems. I will always say, as a security manager, that I'm not given enough funding, but I think the budget is in line with other industries."

... they seek him here, they seek him there. (Picture: Longannet power station. © Scottish Power.

He identifies an industry-wide need to collaborate. Sharing information is a way of strengthening industry-wide security, he says. "I think organisations need to talk and be able to build a bond of trust," he says.

He acknowledges that this is already happening, but says it needs to be expanded. "I think different countries have different platforms that they use to bring together companies. The government also tries to do the same. I think we're going in the right direction but I think it should also be sponsored by professionals."

Like the rest of the IT world, the power sector faces a dilemma. By sharing information players can win the benefits of networking, industry standards and commodity hardware; these include improved business processes, reduced costs and improved productivity. But sharing increases the security risks, and as systems become increasingly web-enabled and interconnected, the risks grow.

Says one industry expert, "They're faced with a choice of having their cake or eating it — either they work in isolation or they have ease of use."

Because of the importance of energy to the rest of the economy, the cost of wrong decisions will be very high.

Matthew Stibbe is a freelance business and technology journalist and writes for Director *and* Wired *among others. On the web at www.stibbe.net.*