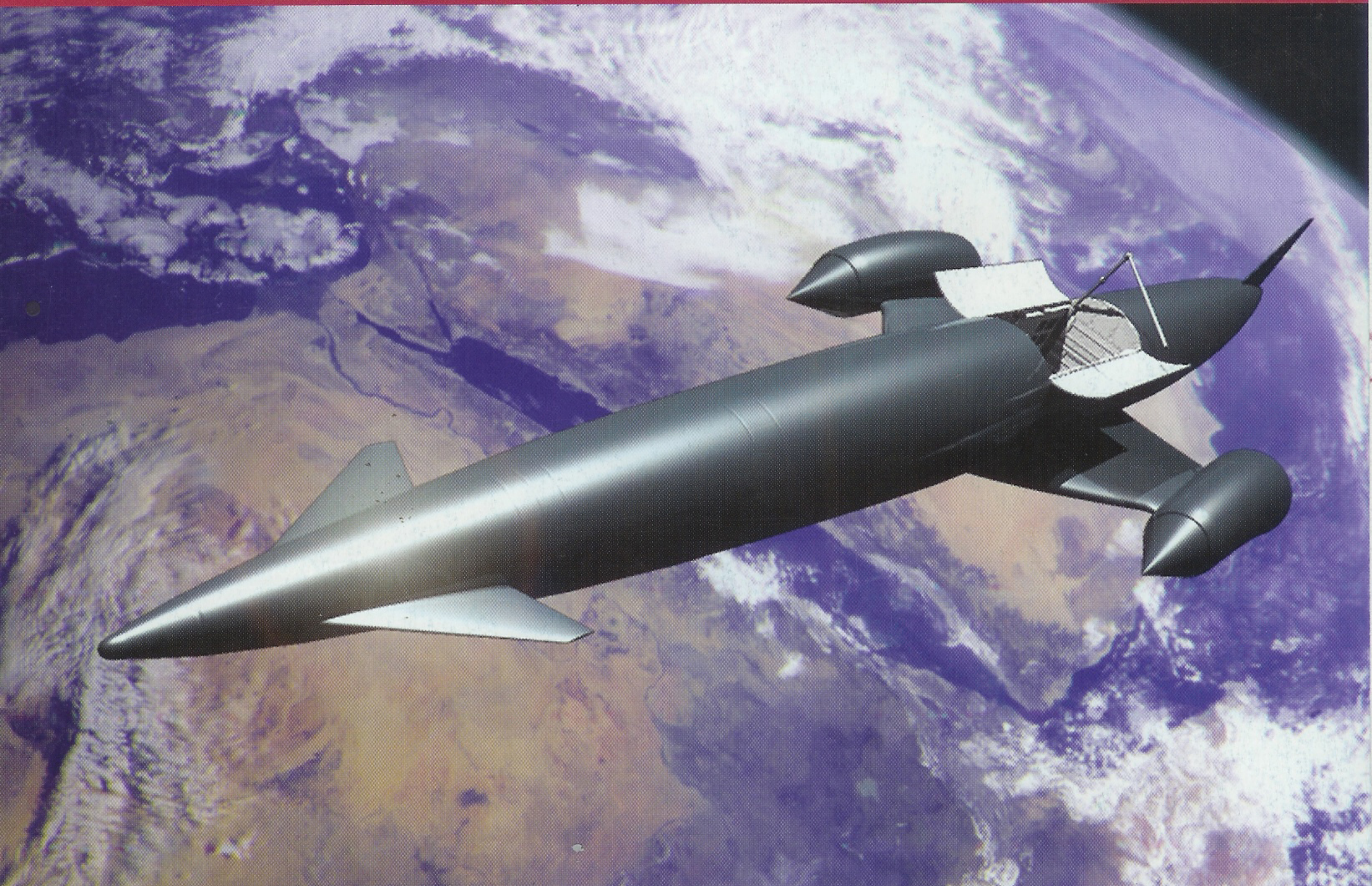
DECEMBER/JANUARY 2005/06

# The IEE Computing & Control Engineering

www.iee.org/control



New Special Interest Group:

## Autonomous Agents in Control

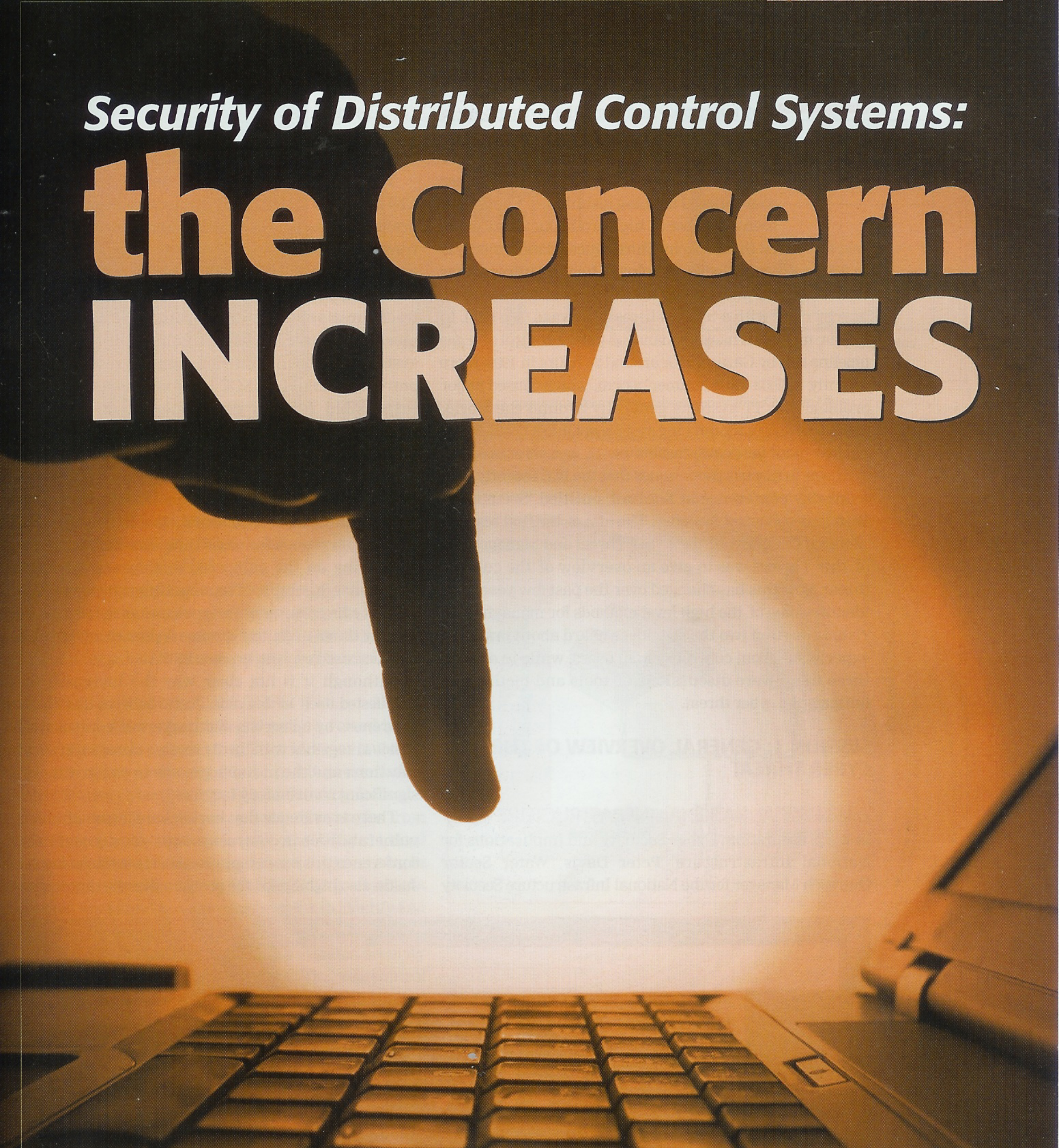
**Inside:**

Distributed computing environments

An alternative to RFID

Security in distributed control systems

# Security of Distributed Control Systems: the Concern INCREASES



***Process automation systems are key to the organisations behind the UK's Critical National Infrastructure (CNI) as they both monitor and control critical processes involved with the production and transportation of gas, electricity and water. As these systems become more 'open' – using Ethernet, TCP/IP and web technologies – they become vulnerable to the same threats that exist for normal IT systems.***

by Steve Mustard

Today many process automation systems are as open to external threats as are IT departments. Whole systems have been disabled by 'worms' and unauthorised access by 'Trojans' or other conventional hacking techniques. There have been a number of high profile incidents in the past few years: In Maroochy Shire, Queensland, Australia in 2000 a disgruntled ex-employee hacked into a water control system and flooded the grounds of a hotel and a nearby river with a million litres of sewage (see p25). In Russia, malicious hackers managed to take control of a gas pipeline run by Gazprom for around 24 hours in 1999. More recently, in 2003 the 'Slammer' worm, which caused major problems for IT systems generally around the world, disabled a safety monitoring system at Ohio's Davis-Besse nuclear plant for nearly five hours.

It was to discuss these issues that the IEE recently held a one-day conference at Solihull, entitled 'Security of Distributed Control Systems'. The aim of the first session, 'General Overview of the Cyber Threat and Management of this Threat' was to give an overview of the current threat, how this has changed over the past few years and identify some of the high level methods for managing the risk. In session two the attendees heard about practical experiences from control system users, while in session three there were discussions of tools and methods to mitigate the cyber threat.

## SESSION 1: GENERAL OVERVIEW OF THE CYBER THREAT

### THE CRITICAL NATIONAL INFRASTRUCTURE (CNI)

In his presentation 'Cyber Security and Implications for National Infrastructure' Peter Davis, Water Sector Outreach Manager for the National Infrastructure Security Co-ordination Centre, gave an overview of who NISCC is and, using the example from Maroochy Shire, Australia, demonstrated how real the threat to control systems is.

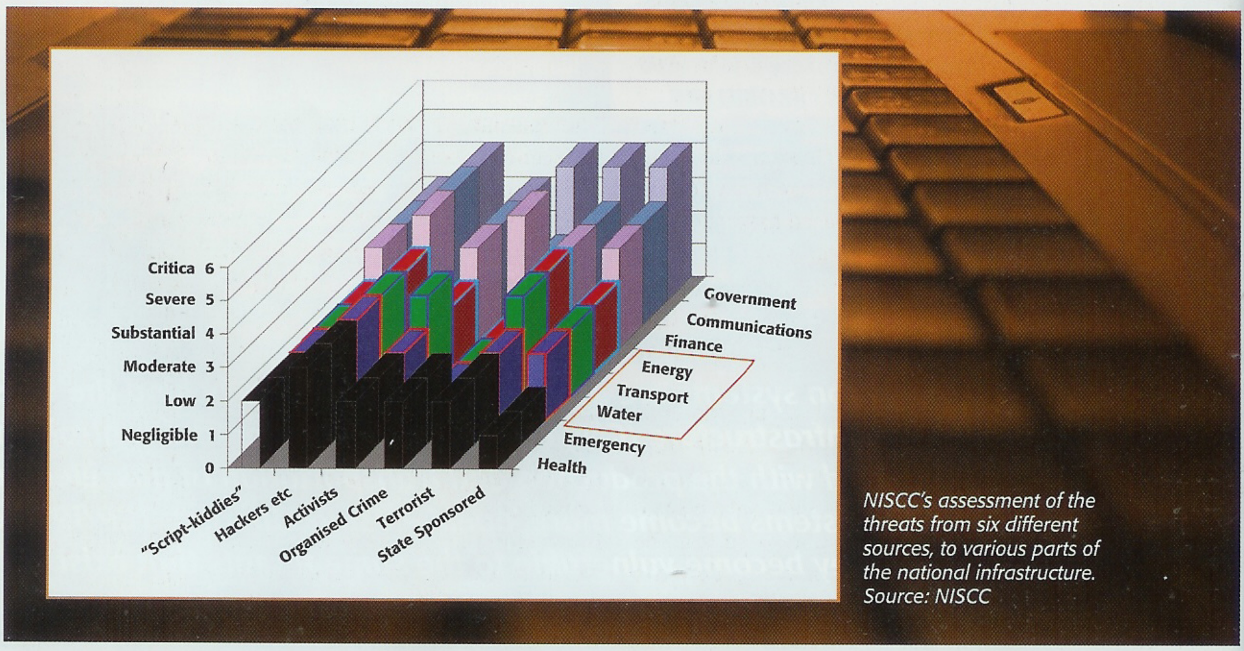
The good news is that NISCC are there to help the UK CNI across all sectors – government, emergency services, health services, finance, telecommunications, energy, water, transport, hazards and food – to mitigate the risk of electronic attack. NISCC shares information with similar organisations in other countries around the world to help track threats and identify responses. NISCC undertakes research to look for generic vulnerabilities in control systems and identify recommended resolutions. The outreach team of NISCC (of which Peter is a part) is responsible for the dissemination of information throughout the CNI community ensuring the issues and experiences are shared for the greater good of all.

### SECURITY IMPROVEMENTS

PA Consulting have been heavily involved in the security of control systems for some time. Justin Lowe has been presenting on the subject at conferences and at this conference his topic 'Constructing a Process Control Security Improvement Programme' gave hard evidence that the threat to control systems is present, and this threat has increased especially since 2003.

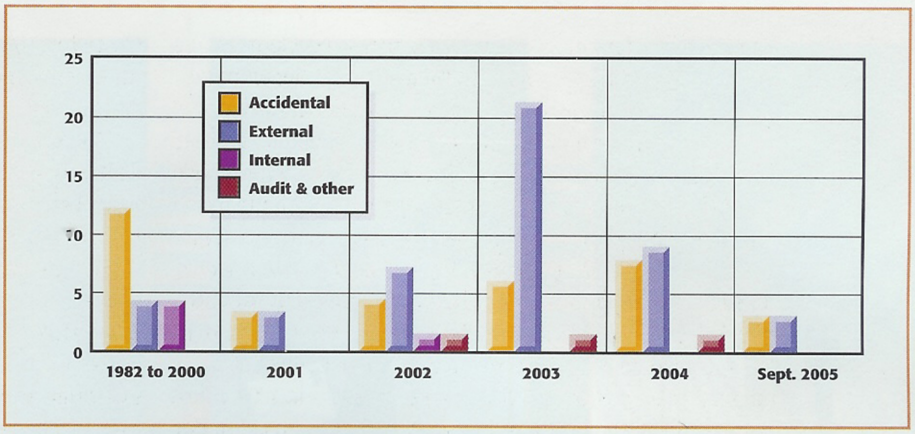
Although it is not clear why the increased threat manifested itself at this time, Justin believes that increased awareness by terrorists and hackers of control systems post 9/11 together with the increasing use of open standard solutions and the massive growth in worm attacks are significant contributory factors.

There is evidence that hackers are aware of potential vulnerabilities in control systems – at a recent hackers conference this exact topic was discussed in some detail. Justin also highlighted the problem that the time to develop



*NISCC's assessment of the threats from six different sources, to various parts of the national infrastructure. Source: NISCC*

Justin Lowe



*Extracted from a database of approximately 100 incidents maintained by Eric Meyer at the British Columbia Institute of Technology, this chart shows that accidental intrusions are currently a major part of control system problems. External intrusions apparently peaked in 2003, but there may be a reporting lag of 1 - 3 years in the data. Source: PA Consulting Group*

attacks has reduced from months to just days, so suppliers and users have to react much more quickly to avoid the impact of new methods. The average cost of impact is estimated to be around $1.8m.

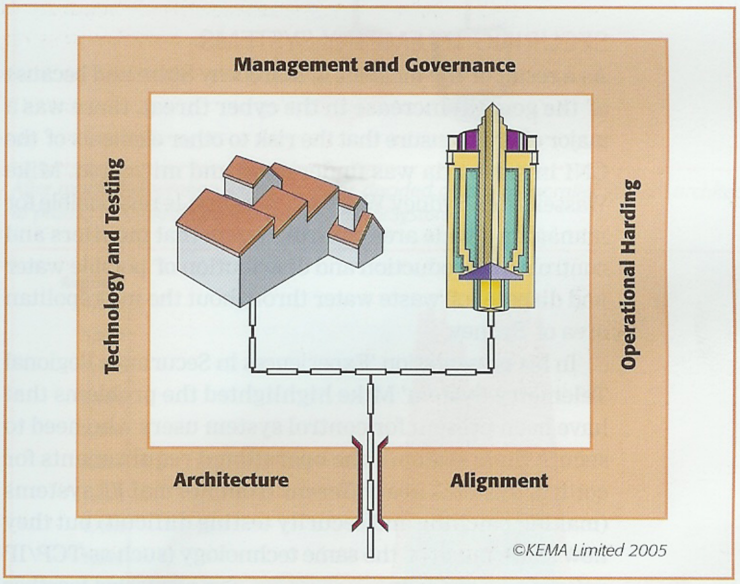
PA Consulting help organisations manage the threat to their control systems using a security programme which identifies the threats, impacts and vulnerabilities and produces a remediation plan to manage business risk.

## SECURITY THROUGH OBSCURITY

KEMA are another organisation heavily involved in the security of control systems. Marc Tritschler continued the theme started by Peter and Justin in his presentation 'Control System Cyber Security – Understanding the Issues and Addressing Them'. He presented real examples from the US that control systems are at risk of attack and indeed are attacked often with significant impact to operations. In the examples that Marc gave it took the organisations concerned weeks and in some cases months to identify and resolve the issues.

In the previous generation of control systems, security was obtained through obscurity, he said. Bespoke control systems were built to proprietary standards with limited connectivity to the outside world. There were no hidden or disabled communication channels. But present day control systems, with off-the-shelf Windows-based hardware and Ethernet connections, are good targets for external adversaries: terrorists, disgruntled employees, 'script kiddies' (young hackers), and vendors and third parties, who may inadvertently open up routes to their developers in East Europe.

Marc presented KEMA's 'MOAT' methodology, which is an acronym for Management, Operational hardening, Architecture alignment, and Technology and testing. What this means, in a nutshell, is that management must ensure that all interested parties are engaged and there must be clear management and governance in place. Specific security policies should be developed for control systems, following existing standards (e.g., ISO17799) where possible.



*KEMA suggests building a 'MOAT' around critical control and IT systems. Source: KEMA Ltd.*

The company must understand the difference between corporate and control networks and maintain an appropriate level of separation. And security must be designed in on new and current projects, and then tested very carefully.

Like PA Consulting, KEMA help organisations manage the threat to their control systems using structured security management programmes. KEMA have also been key to organising the first meeting of interested parties from around the world to define an internationally recognised standard for security of control systems.

➔

Marc Tritschler

Mike Wassell

Ian Henderson

Bill Fulton

Stephen Robinson

## SESSION 2 – PRACTICAL EXPERIENCES

### SECURING TELEMETRY SYSTEMS

As a result of the incident in Maroochy Shire and because of the general increase in the cyber threat, there was a major effort to ensure that the risk to other elements of the CNI in Australia was understood and mitigated. Mike Wassell from Sydney Water Corporation is responsible for managing a wide area control system that monitors and controls the production and distribution of potable water and disposal of waste water throughout the metropolitan area of Sydney.

In his presentation 'Experiences in Securing a Regional Telemetry System' Mike highlighted the problems that have been present for control system users who need to secure their system – the operational requirements for control systems are different from normal IT systems (making patching and security testing difficult) but they now share much of the same technology (such as TCP/IP networking) and in many cases are now connected together to provide business users with important information from the control system. When Mike embarked on his security programme in 2002 there was little experience of how to secure control systems and a lot of work was undertaken from scratch. He suggests using a third party to audit all mission critical systems. "Don't let IT run your SCADA system" was his warning.

An international standard for security of control systems would undoubtedly have helped Mike and the experiences of Sydney Water will help to make sure that a future standard provides what is needed for similar organisations.

### THE BP EXPERIENCE

BP have taken security of their control systems very seriously, resulting in the creation of a digital security function solely responsible for cyber security including that of control systems. BP established a Centre of Excellence using staff from both the control systems and IT functions, created their own security framework and set about identifying and managing security issues in the installed base of control systems. These activities were described by Ian Henderson in his paper, 'Process Control Security – the BP Experience'.

"Process automation demanded open systems, and we got what we wanted," he said, noting that operators of older systems never had to worry about Internet worms. But now we have open systems, and the typical response to security requirements is to hire a team of security consultants. But this is not the way it should be done, he maintained. "Control teams on the site need to 'own' security, it's a part of their day job," he said.

BP now contribute to standards authorities such as ISA, governmental groups such as NISCC and work with leading cyber security research organisations such as the British Columbia Institute of Technology (BCIT). BP have been particularly instrumental in engaging control system providers in the resolution of vulnerabilities and Ian has observed significant improvements in response times for security patches and general awareness of security issues and solutions.

### COOKIES AND COFFEE

PowerSystems are an electricity transmission and distribution utility in the UK and as such they are a key element of the UK CNI. Bill Fulton, like Mike and Ian, has had significant experience in the issues surrounding the securing of control systems, and described them in his paper, 'Technical and Administrative Cyber Security Issues with Implementation of a SCADA Upgrade'.

The adoption of modern IT standards in operating systems and networking together with demands from the business to integrate control systems into the business architecture required the introduction of traditional IT security measures such as Network Intruder Detection Systems (NIDS), firewalls and antivirus protection.

However as with other control system installations the introduction of these measures needed to recognise the differences between these systems and traditional IT. There were many back-and-forth meetings between IT and the

Kevin Regan

control systems group before the appropriate security could be agreed upon.

Even the type and placement of the various firewalls became a long and involved discussion. At one point, they had decided to use two firewalls in series, but ended up using two parallel firewalls. "Get a budget for cookies and coffee," he said, meaning that the control systems people should plan to have constructive meetings with IT.

## SESSION 3 – TOOLS AND METHODS

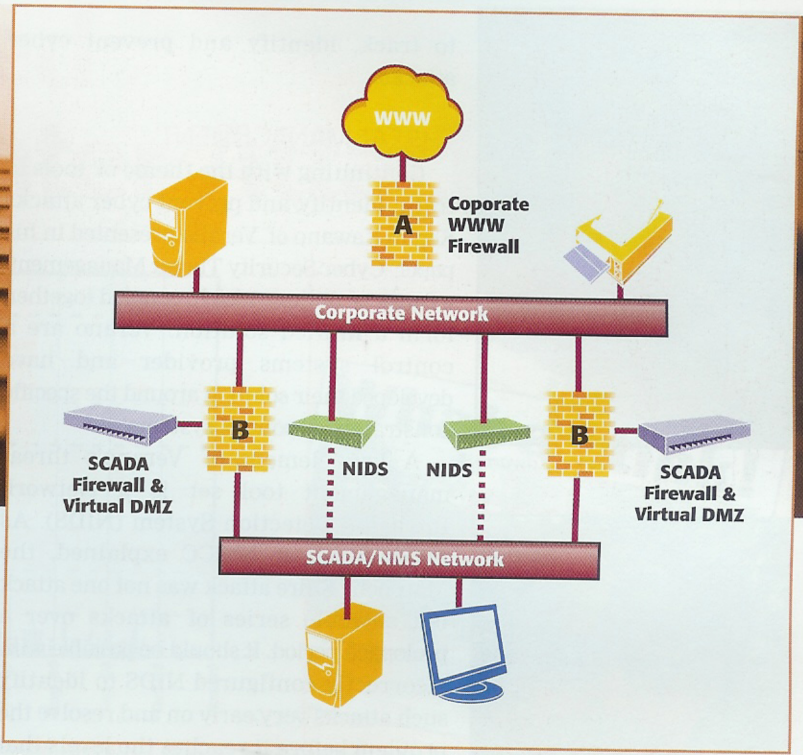
### AUTHORISED HACKING

Penetration testing is an established method of providing an objective and independent view of the security of any IT infrastructure or application. Penetration testing is, in effect, authorised hacking. Experts in IT vulnerabilities identify potential issues and then physically test to see if they can take advantage of them and invade the system. They then make recommendations to strengthen the security of the system. Penetration testing of control systems needs to take special care since they often control safety related process equipment. But it is clear that this is one method to mitigate the risk of the cyber threat.

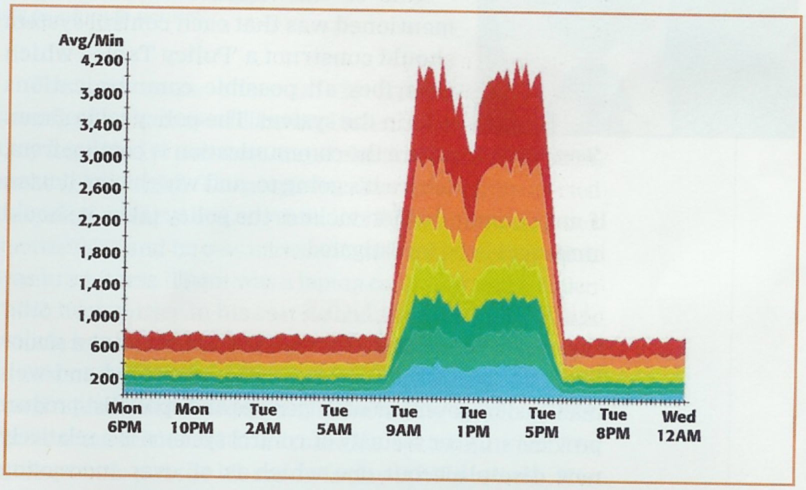
LogicaCMG provides IT security management services to a wide range of governmental and non-governmental organisations and has performed penetration testing on a wide range of IT applications and systems. Stephen Robinson described his services and experiences as a penetration tester in his presentation, 'The Art of Penetration Testing'.

### SECURING COMMUNICATIONS NETWORKS

While control systems have traditionally been based around point-to-point serial communications with little or no connectivity to the business IT world, we have seen from earlier presenters that this is changing. Increasingly control systems are being directly connected to business systems via TCP/IP networks. Remote site monitoring equipment (Programmable Logic Controllers and Remote Telemetry Units) are transmitting data to central systems using similar methods and there is an increasing use of standard IT products such as operating systems.



*After much deliberation, PowerSystems decided on a dual parallel firewall architecture to protect its control system. Source: PowerSystems*



*Cisco Systems' NetFlow based anomaly detection looks for statistical changes in network activity. It is used to detect worms propagating, denial of service attacks, exfiltration of data, or back-door sessions. Source: CISCO Systems*

Products like routers, firewalls and switches from Cisco or their competitors are highly likely to appear now somewhere in the modern control system environment. How to secure them in the industrial environment was the topic of Kevin Regan's presentation, 'Securing Communication Networks'. Cisco Systems provide a significant part of the networking equipment that makes the Internet work. Because of the very significant cyber threat to the Internet there are a lot of tools available →

Kegan Kawano

Steve Mustard

to track, identify and prevent cyber attacks.

## THREAT MANAGEMENT

Continuing with the theme of tools to track, identify, and prevent cyber attacks Kegan Kawano of Verano presented in his paper 'Cyber Security Threat Management' a range of options which, coupled together, form a unified solution. Verano are a control systems provider and have developed their solution around the specific constraints of control systems.

A key element of Verano's threat management tool set is a Network Intrusion Detection System (NIDS). As Peter Davis of NISCC explained, the Maroochy Shire attack was not one attack but a whole series of attacks over a prolonged period. It should be possible with a correctly configured NIDS to identify such attacks very early on and resolve the problem before it reaches the levels that were experienced in Queensland.

One of the suggestions that Kegan mentioned was that each control system should construct a 'Policy Table', which describes all possible communications within the system. The policy table shows where the communication is coming from, where it's going to, and which port it uses. If any communication violates the policy table, it should immediately be investigated.

## SHARING EXPERIENCES

General cyber security for the IT world remains a major issue but one which is now well understood and well managed by governmental agencies and specialist product providers. Cyber security of control systems is a relatively new discipline but one which is of ever increasing significance as attackers learn of the potential vulnerabilities in the CNI.

The need to share knowledge of new threats and ensure that product vendors and users respond promptly to such issues is key to managing the risk in future.

The prospect of an international standard for security of control systems is very attractive, as it should provide a common framework for any control systems user, without having to reinvent the wheel.

The conference has helped to share experiences of end users, practitioners and product providers so that best practice can be used for the greater good of all. ■

**Steve Mustard, Telemetry Business Manager, LogicaCMG was the conference chairman. He may be reached at steven.mustard@logicacmg.com**

When cyber security people warn process automation companies about possible hackers' attacks, they like to point their finger to the Maroochy Shire Council's (MSC) sewage control system, in Queensland Australia, which was attacked in 2000 and resulted in substantial environmental damage. Located in a tourist area on the east coast, the sewage system has 142 pumping stations connected by radio to monitoring computers.

The troubles began when the installation company, Hunter Watertech, finished installing the control system in December 1999 and the site supervisor for HWT, Vitek Boden, resigned "under circumstances that are not exactly explained". He applied to MSC for a position, but was rejected.

The following month, January 2000, strange things started to happen. Pumps were not running when needed, alarms were not being reported to the control centre, and there was a loss of communications between the control centre and the pumping stations.

HWT came back to the site and re-installed their software and thoroughly checked out the system and verified that it was operating properly, but this did not solve the problem. The sewage system operators were completely baffled; they thought they had a leak, but when they went out to examine the various pipes and valves at the pumping stations, they found nothing. The putrid odour infuriated the local residents.

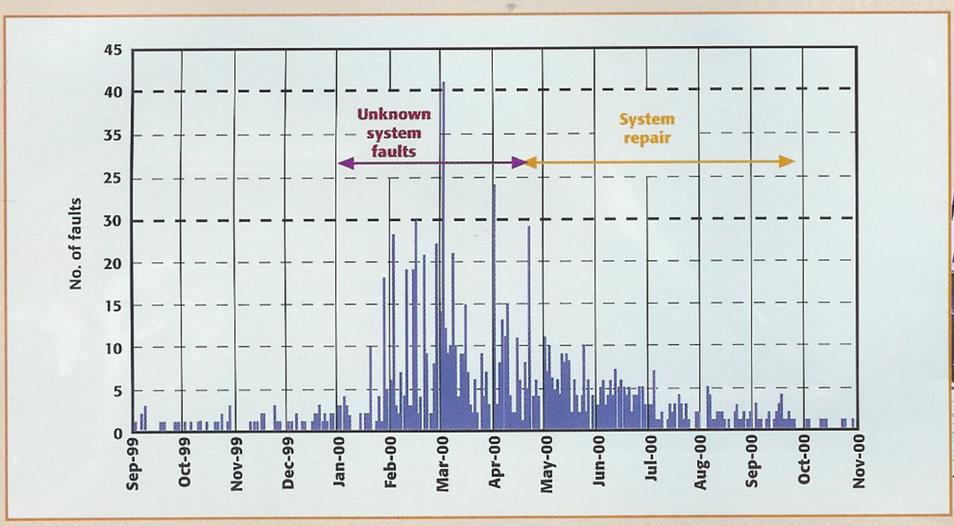
## THE NEED FOR LOGGING

Except for simple messages like "pump running" or "tank full" the HWT engineers couldn't see much of what was going on because the system didn't do any logging. So their first action was to initiate a programme to log more information, especially control messages and radio traffic.

The evidence began to point to outside agents interfering with the system. With data logging this became more apparent when engineers noticed a spoofed pump station ID. The system was receiving signals from a pumping station ID that wasn't where it should have been – and it wasn't sending the right sort of signals. After inspecting one particular pump station site and re-coding its ID, it became clear that they were receiving signals coming in from a station that didn't exist.

Radio monitoring was also starting to detect these transmissions. After nearly two months of baffling problems, on 16 March they began to get some hard evidence of what was going on. They spotted radio transmissions controlling various pump stations from the fake ID. From the control centre they sent signals to the pump station to override the fake signals but without success: The bogus station would just change its ID and continue. Efforts to regain control over the pump stations

# The Celebrated Maroochy Water Attack



## What a stink!

raged residents demand answers over million-litre sewage spill

*Until late January, the number of faults recorded never exceeded two or three per day, but increase dramatically as intrusions were made. The last attack was made on 23 April, but by this time system problems had compounded to such an extent it took several months for the level of faults to return to normal.*

were failing. Needless to say, it was an uncomfortable process that HWT were going through at this time.

## THE PRIME SUSPECT

Evidence was leading away from a random hacker who had stumbled into their system; it would have to be someone who had a fairly good idea how to send control signals. This was a proprietary system; there wasn't anything 'open' about it. The hacker obviously understood radio control systems and was evidently joining in on the radio control conversations.

By this time Vitek Boden was under suspicion. The 48-year-old disgruntled techie had left the company under dodgy circumstances. He knew a lot about HWT's control systems, so the company hired private investigators to follow him, and notified the local police of their suspicions.

By this time, in the middle of March, a lot of faults were occurring and it was obvious that the hacker wasn't just playing around with the control system. There were sewage leaks, caused by overflowing tanks when pumps were turned off. The golf course next to the Hyatt Hotel was flooded with a million litres of sewage. A major overflow into a residential area and tidal canal polluted an estuary; in the surrounding area on Australia's Sunshine Coast, creeks turned black and cost the government Au$100,000 to set up an environmental monitoring programme. People were starting to notice that there was something wrong. The police were definitely interested.

The end game came on 23 April 2000. Private investigators had been following Boden but on this occasion they lost him. He was near one of the three radio repeaters, making intrusions. The people in the control centre alerted the police who put out an All Points Bulletin. A police car spotted him and he was arrested while his 46th intrusion was in progress. There was a laptop computer and a stolen radio transmitter in his car; he had, in effect, turned his vehicle into a pirate command centre for sewage treatment.

Boden denied responsibility, in spite of the fact they had caught him with the equipment, including a stolen HWT radio transmitter with a traceable serial number. He attempted to put the blame on faulty HWT systems. His behaviour at the trial suggested that he was angling for a consulting contract to solve the problems he had caused. But the jury didn't accept his explanation. After his court case in October he was imprisoned for two years and fined Au$13,110.17 – the total cost of the clean up work. HWT estimates it spent around Au$500,000 to solve the problem.

Boden wasn't just stopping pumps; he was actually reprogramming the control system, explained the chief executive of Hunter Watertech. To make the attacks, he used his laptop to identify itself as "pumping station 4", logged on and suppressed all alarms. With unlimited command of 300 control nodes for both sewage and drinking water, his attacks were actually quite restrained. "He could have done anything he liked to the fresh water", the chief executive said. He faced virtually no obstacles to breaking in. ■