

e-monitor

e-MONITOR is produced by [Engineers Media](#) – Engineers Australia's publishing company. The statements made or opinions expressed in this newsletter do not necessarily reflect the views of [Engineers Australia](#).

Editor: [Michael Lee](#)

Managing Editor: [Dietrich Georg](#)

To contribute a story or give feedback, email mlee@engineersmedia.com.au

To have your email address changed, email memberservices@engineersaustralia.org.au

If this email is not displaying correctly [click here](#) to view online.

February 2011

In this issue

- [Year of humanitarian engineering](#)
- [Temporary closure of Egypt's internet](#)
- [University website defaced, records compromised](#)
- [Contracts for the NBN](#)
- [Extinguishing Firesheep through SSL](#)
- [Stuxnet virus dossier updated](#)
- [NBN corporate plan reviewed](#)
- [Smartphone developer opens windows](#)
- [The internet runs out of addresses](#)
- [Australia ill prepared for cyber war](#)

[New Products](#)

[Calendar](#)



ENGINEERS
AUSTRALIA

FROM THE CHAIR

NEWS

NEW PRODUCTS

CALENDAR

ITEEC

[engineer.career](#)

Engineers Australia's
careers website
provides extensive
career information.

from the chair

Year of humanitarian engineering

by Peter Hitchiner



It is perhaps fitting at the outset of 2011 that, apart from wishing all College members all the best for 2011, I reflect on the opportunity for ITEE College members to participate in activities and initiatives in this Year of Humanitarian Engineering.

Several of our members have set a great example with the initiative of providing critical support to mobile phone and internet users in Brisbane in the immediate

aftermath of the floods.

The importance of robust, in particular wireless, telecommunications and data centre (including disaster

recovery) infrastructure in the wake of floods, cyclones and other catastrophic failure situations has become very apparent.

The development and resilience of such infrastructure will be of increasing importance in all countries and, with the continual growth in the electronic services and associated digital economies, there will be an increasing role for ITE/ICT engineers.

This will include support for developing economies in such matters as eHealth, eEducation, financial services (eg. micro-financing), and access to spatial information to support new (electronic) services and smart solutions. The need for more people skilled in these areas throughout the community will become a growing challenge if the opportunities are not to be inhibited. These needs also exist in many parts of Australian society.

So, here is a challenge to all ITEE College members to create and contribute to various EA initiatives in this Year of Humanitarian Engineering.

I also take this opportunity to encourage ITEE College members to contribute to the issues currently subject to EA policy development in urban policy, population strategies and sustainability.

The potential contribution of the ITE/ICT industries to enabling sustainability in the face of urban development and population growth is enormous and essential here and overseas!

This column also appears in the [ITEE College Board Chair blog](#): please post your feedback.

Peter Hitchiner is the ITEE College Chair 2011

[back to top](#)

news

Temporary closure of Egypt's internet

On 28 January, in response to protests and riots, the Egyptian government took unexpected action against its 80 million citizens. It cut off its internet routes to the rest of the world.

Shortly after midnight Cairo time, the Egyptian government ordered internet service providers to stop announcing almost all of their BGP (Border Gateway Protocol) routes to the rest of the world. These effectively let other routers know of the possible routes that can be taken to reach their networks.

Mobile network operators were also ordered to shut down their services. Vodafone was one of the service providers that provided comment on the order to shutdown its route announcements. On its website (now removed), it said, "All mobile operators in Egypt have been instructed to suspend

services in selected areas. Under Egyptian legislation the authorities have the right to issue such an order and we are obliged to comply with it.”

In a later statement, the company said there are “no legal or practical options open to Vodafone, or any of the mobile operators in Egypt, but to comply with the demands of the authorities.”

Physical links to Egypt were intact, with European-Asian traffic continuing to route via fibre links in Egypt.

Initially, one exception to the BGP blackout was service provider Noor Group. While it is unknown as to why the service provider continued to announce its routes (or if it was ordered not to), speculation existed that it was due to its routes to several financial services such as the Egyptian Credit Bureau and Egyptian Stock Exchange (ESE).

On 1 February, Noor stopped announcing its routes.

Those cut off from the rest of the world had to find alternate ways to connect to the internet. As landline phone access was still available, many made use of dial-up accounts to establish outbound connections.

BGP routes were restored on 2 February, with Noor reannouncing its routes a few hours later than other providers.

[back to top](#)

University website defaced, records compromised

The website of the University of Sydney was defaced last month and a vulnerability was discovered that could be used to read student records.

In a message left on the defaced site, a hacker going by the name of Evil ridiculed the existing network administrator. Evil pointed out that the web server’s logs showed three previous intrusions and no action had been taken to secure it.

While the damage from defacing websites is usually limited to the web server hosting the site, Evil also claimed to have access to three quarters of the rest of the administrator’s network.

For several days after the defacing of the site, the main site displayed that it was undergoing maintenance.

Following the attack, University of Sydney vice-chancellor and principal Michael Spence initially sent out an email to all students of the university which stated that “much of the University’s website remained untouched and no systems were compromised” and that “no student or financial records were impaired.”

In an article by the *Sydney Morning Herald*, an anonymous

security expert was able to demonstrate access to the records of past and present students. According to the article, leaked details included financial records, names and addresses. It also stated that the university was alerted of the vulnerability in 2007.

It is not clear whether the defacing of the site is related to the security flaw that allowed access to student records.

Shortly after the article was published, Spence sent out another email confirming the existence of the flaw, and that they were previously aware of it.

“The University was advised of such a flaw in our security in 2007. At that time the matter was swiftly rectified as it has been today. Regrettably, some time later as a result of a software update, the security patch was inadvertently removed without anyone becoming aware of its function in protecting the security of student records.”

His email also states that student records “could only be viewed and could not in that way have been changed”.

In addition to securing student records and its web server, the university has engaged two web security organisations to investigate the attack.

[back to top](#)

Contracts for the NBN

The National Broadband Network Company (NBN Co) is continuing to make progress on the network with the award of a number of equipment contracts and the selection of a data centre in Queensland.

Victorian fibre optic equipment manufacturer Warren & Brown Technologies has been awarded an equipment contract worth up to \$110 million over five years. The company, which has built a research, development and manufacturing facility in Maidstone, north-west Melbourne, will provide optical distribution frames and sub-racks. These products require sheetmetal manufacture and assembly of fibre optic connectors.

NBN Co has also awarded a contract for multiple types of equipment worth up to \$1.2 billion over five years to Corning, a manufacturer of fibre optic cabling. Corning’s existing manufacturing facility in Clayton, Melbourne, has already supplied fibre optic cable and other equipment to help build NBN Co’s first release sites.

Corning will be the initial supplier of aerial cable, provide selected types of splice closures and will jointly supply feeder cables and drop cables which will connect individual user premises to the fibre network.

NBN Co awarded a third equipment contract worth \$300 million over five years to Prysmian, a global manufacturer of telecommunications cabling with manufacturing facilities in

Dee Why and Liverpool, Sydney. It is being contracted to provide underground cabling for the NBN project.

NBN Co has also contracted Polaris Data Centre in Queensland to host its second data centre.

The data centre will house NBN Co's IT infrastructure and its operational and business support systems. The value of the contract is approximately \$5 million over five years.

[back to top](#)

Extinguishing Firesheep through SSL

Organisations have begun to provide end-to-end encryption by default in response to session hijacking or "sidejacking", with Facebook and Hotmail among the first to enable users to use SSL (Secure Socket Layer) across their entire session.

While the use of sidejacking is not a recent development, it has received more attention after the release of Firesheep, a sidejacking tool which made it easy for the average user to hijack other users' sessions over open networks.

Most organisations are taking an opt-in approach, where users must enable SSL for it to be used across their entire logged-in session, as opposed to just during the log-in period.

Facebook has stated it [hopes to offer end-to-end encryption as a default](#) some time in the future, but until then users must manually activate it in their account settings. This means that those who are not as technically literate (and are generally those most at risk) will be less likely to find and activate the option.

Other sites have not adopted the use of SSL. One example is Twitter. Although it sends login requests to an https:// address, it is vulnerable to code injection. Such man-in-the-middle attacks occurred during the Tunisian protests when passwords for Twitter and Facebook accounts were stolen (Facebook temporarily solved the issue by forcing all Tunisian traffic to use SSL).

Furthermore, once logged in, sessions are not encrypted unless users explicitly force their browser to Twitter's https:// address.

To ensure that all requests go via SSL (where sites support it), the [Electronic Frontier Foundation](#) in collaboration with the [Tor Project](#) have developed a Firefox extension called [HTTPS Everywhere](#).

[back to top](#)

Stuxnet virus dossier updated

Computer security research firm Symantec has updated its dossier on Stuxnet after gathering more information on the worm. The new version of the dossier provides further

infection statistics, outlines the behaviour of infected PLCs in further detail, and discusses other variants of Stuxnet.

Stuxnet targets specific industrial control systems. While the targeted organisation of Stuxnet is unknown, about 12,000 infections can be traced back to five organisations, each of which have a presence in Iran. Symantec have stated that the target is likely to be a gas pipeline or power plant.

Further speculation exists that the intended targets are the centrifuges at Iran's Natanz uranium enrichment plant. Iran president Mahmoud Ahmadinejad confirmed late last year that those centrifuges were experiencing problems due to installed software, although he did not specifically name Stuxnet as the cause.

Stuxnet attempts to sabotage specific frequency converter drives that normally operate between 807Hz and 1210Hz. It modifies the output of the frequency drives to 1410Hz, 2Hz and 1064Hz for short periods. It also provides false information to the safety, warning and monitoring systems for these drives to disguise its actions.

It employs the use of four zero-day vulnerabilities, can spread over local area networks or via USB drives, can update itself remotely, and previously used a compromised signed driver certificate to aid infection.

The complete dossier is available on the [Symantec website](#).

[back to top](#)

NBN corporate plan reviewed

The National Broadband Network Company's (NBN Co) corporate plan has been completed to high professional standards, according to independent corporate advisory firm Greenhill Caliburn.

Greenhill Caliburn was asked to review NBN Co's corporate plan and provide a commercial assessment, identifying and analysing the plan's key assumptions and potential risks.

While the Australian government has only released the executive summary of the report to the public, due to concerns that the complete document would reveal sensitive, commercial-in-confidence material.

The executive summary of the report concluded that the plan provides, "the level of detail and analytical framework that would be expected from a large listed public entity evaluating an investment opportunity of scale", and that, "the corporate plan for the development of the NBN is reasonable".

The full report provides an overview of NBN Co, a preliminary commercial assessment of the corporate plan including assumptions and potential risks, and a summary of potential performance management strategies.

[back to top](#)

Smartphone developer opens windows

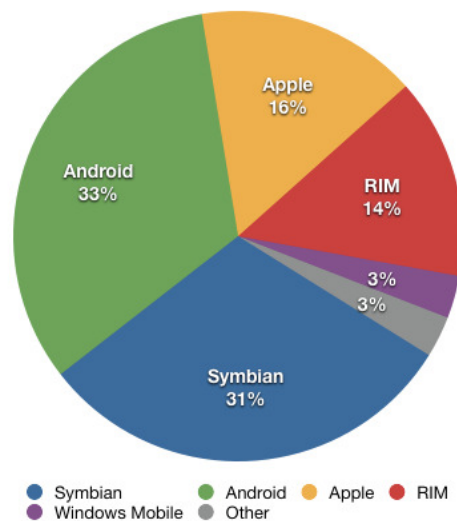
Finnish communications corporation Nokia has surprised the mobile phone industry by announcing it will use Microsoft Windows Phone 7 as its primary operating system.

The company had been working with Intel on MeeGo, a Linux-based open-source mobile operating system. Its existing Symbian operating system has recently received criticism for its inability to keep pace with the rest of the market, falling behind Apple's iOS and Google's Android platforms.

According to Canalys, Google has taken market leadership, holding 32.9% of the global market share, up 24.2 percentage points from last year. Nokia fell 13.8 percentage points to 30.6%. Apple experienced a small decrease of 0.3 percentage points to 16%. Microsoft holds just 3.1% of the market share, down 4.1 percentage points.

Nokia had refused to consider Android for its future operating system under concerns that there would be long-term problems if used.

Nokia will continue to develop MeeGo in conjunction with Intel, but as a secondary, optional operating system.



Global smartphone market share for Q4 2010

Credit: [Eraserhead1](#)

[back to top](#)

The internet runs out of addresses

The last pool of IPv4 internet addresses have been allocated, to five global Regional Internet Registries (RIRs), signalling the depletion of the 4.3 billion addresses available and the need for IPv6 for future addressing needs.

Two "blocks" of the dwindling number of IPv4 addresses, about 33 million of them, were allocated to the RIR for the Asia Pacific region. When that happened, it meant the pool of

IPv4 addresses had been depleted to a point where a global policy was triggered to immediately allocate the remaining small pool of addresses equally among the five global RIRs.

The allocation of the final IPv4 addresses is analogous to the last crates of a product leaving a manufacturer and going to a regional store or distribution centre. They can still be distributed to the public, but, once they are gone, the supply is exhausted.

"It's only a matter of time before the RIRs and internet service providers must start denying requests for IPv4 address space," said Raúl Echeberria, chair of the Number Resource Organisation, the umbrella organization of the five RIRs. "Deploying IPv6 is now a requirement, not an option."

IPv6 has many design improvements over IPv4, most notably the use of 128-bit addressing as opposed to IPv4's 32-bit addressing.

The theoretical maximum number of addresses under IPv6 is about 3.4×10^{38} , as opposed to IPv4's 4.3×10^9 . Only about one eighth of the addresses are expected to be used.

[back to top](#)

Australia ill prepared for cyber war

Australians are grossly underestimating the threat of cyber warfare and the Australian government is not doing enough to keep up with the growth rate of threats, according to the Kokoda Foundation.

The independent research think-tank this month released a paper, titled *Optimising Australia's Response to the Cyber Challenge*, which sought to answer the question of whether Australia is doing enough to address growing threats in the cyber environment and if not, what needs to be done.

While the report applauds the intent behind the government's Cyber Security Strategy, it notes that the strategy is "not keeping pace with the growing threat and as a result is placing the collective and individual security of the nation's people at risk."

The report criticises the current strategy's horizon of only a few years, stating that while the actions taken to date are excellent, it lacks long-term planning and goal setting. Instead, the report recommends a whole-of-nation, government-led, long-term National Cyber Strategy and Plan, which could be developed as a subset of the existing National Security Strategy.

Development of the National Cyber Strategy and Plan would define the government's roles and responsibilities, identify priorities and ensure the necessary resources are dedicated towards mitigating cyber threats.

The report also recommended the appointment of a minister for cyber issues, together with a ministerial committee.

With regards to research and development in the cyber environment, the report identified a number of initiatives to improve cyber education such as a virtual cyber academy (formed by linking universities and relevant educational institutions), a cyber range, and a cyber cooperative research centre.

A [full copy of the report](#) will be available to download from their website in March.

[back to top](#)

new products

Managing fibre

Belden has introduced FiberExpress@EASE: a new standard in fibre patch panel solutions for quicker and easier fibre management

Connectivity and networking products manufacturer Belden has added a new fibre patch panel to its FiberExpress family.

Each SC and LC FiberExpress@EASE unit incorporates a coupler management bar that enables the coupler to sit flush on the front face of the panel. This creates a greater bend radius and a better fit for patch cords within a standard rack.

www.beldenapac.com



The FiberExpress@EASE panel provides improved fibre management.

Visual programmable logic controller

Micromax Sensors & Automation has released the Unitronics Vision560 OPLC. It combines 1024 I/O options with data logging and built-in recipe capability, while maintaining minimum wiring and reduced programming time.

The Vision560 is capable of 24 auto-tuned PID loops to control temperature, level, and pressure, while the 320x240 resolution colour touch screen displays data, colour trend graphs, and alarm screens.

The memory holds 2MB of application logic, plus 1MB for fonts and 6MB for images. Features include SD card memory storage for log, backup, and clone. The controller scans 1K of a typical application in 9µsec, making it an ideal solution for rapid-response applications such as packaging machines.

Communication options include TCP/IP Ethernet, cellular, and industrial protocols such as MODBUS and CANopen. In addition, the Vision560 can be taught to communicate via almost any device-based protocol.

The Vision560 supports high-speed, digital, and analog I/Os, plus direct temperature measurement inputs via snap-in I/O. Unitronics' complimentary VisiLogic software provides one user-friendly environment for hardware configuration, modular Ladder application development, and HMI design – including a rich color library of industrial images.

www.micromaxsa.com.au



The Vision560 is ideal for rapid-response applications.

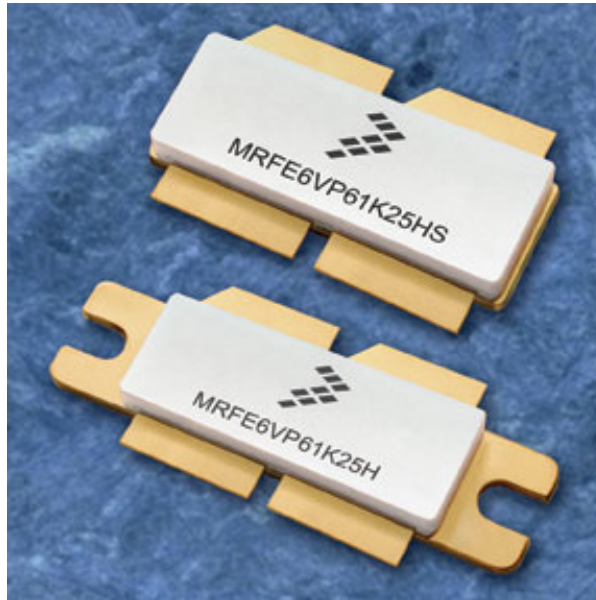
New power transistor

Freescale Semiconductor has introduced a 50V LDMOS power transistor that can deliver its full rated output power of 1.25kW after withstanding a load mismatch VSWR of 65:1 and across all phase angles.

The MRFE6VP61K25 has applications in defence/aerospace amplifiers, CO2 laser exciters, plasma generators, magnetic resonance imaging RF amplifier systems, particle accelerator amplifiers, FM and DVB-T broadcast amplifiers, and a wide variety of HF/VHF communications equipment linear amplifiers over the frequency range from 1.8 to 600MHz.

The MRFE6VP61K25H/HS can be used single-ended or in a push-pull configuration, while its robust 24dB gain allows for fewer stages in many amplifier designs.

The power transistor is available in bolt-down and solder-down ceramic packaging. www.rell.com



The new power transistor is rated at 1.25kW.

[back to top](#)

calendar

Engineers Australia conferences

The [Systems Engineering and Test and Evaluation conference \(SETE2011\)](#) with the theme "**Systems engineering in the next decade**" will be held on 2-4 May in Canberra. It will focus on the experiences, lessons and issues of systems integration.

The [Australian Control Conference \(AUCC2011\)](#) will be held on 10-11 November 2011 in Melbourne. It will provide a forum for Australian researchers, students and control engineers from industry and government organisations to exchange ideas and recent results, as well as discuss current problems, arising in control engineering research and industrial practice.

Other events

The 10th [National SCADA conference](#) will be held on 1-2 March in Sydney. The event will host a program of key Industry personnel to address issues surrounding the SCADA industry and topics raised at the previous summit. Email registration@informa.com.au for more information.

Cisco's annual marquee event, [Cisco Live](#) will be held in Melbourne on 29 March – 1 April. It will offer three distinct event programs (Networkers, IT Management and Service Provider) and provide technical education. Email cisco@veritas.com.au for more information.

Ovum is hosting a breakfast seminar on the [Data centre explosion and its technologies](#) in Sydney on 28 March to explore the data center market locally, its impact and opportunities to Australian enterprises. Other topics include how to keep the data centres cool, and what impacts the rapid expansion and massive investment have to the enterprise buyer. Email jdq@ovum.com for more information.

[back to top](#)