INTELLIGENT ENERGY SYSTEM

With smart apps come security risks

Vulnerability to attacks, privacy pitfalls among matters to be addressed

BY GRACE CHUA

THE smart grid detects an event: 1,000 electric vehicles parked in one spot, all waiting to be charged.

Electricity gets channelled to the demand site – which turns out to be fake – causing other parts of the network to shut down.

Then it becomes clear: The city's power supply has come under attack.

While such a scenario may sound like the plot of a sci-fi thriller, security concerns over the use of smart technologies are real.

With smart energy applications – such as power networks, vehicles and buildings – gaining ground in Singapore and abroad, analysts are taking a hard look at the potential security risks involved.

Smart technologies are often touted as being able to make the economy more energy-efficient and lowering emissions of the greenhouse gas carbon dioxide.

The term "smart" means that the physical hardware contains computer infrastructure, which allows it to monitor and communicate energy use.

Smart grids, for example, could allow users to sell excess power back to the grid, from their electric-car batteries or home solar panels.

This year, Singapore embarked on its Intelligent Energy System (IES) project when technology firm Accenture was awarded a contract to design and implement 4,500 smart meters and other infrastructure in households, offices and other buildings.

Security for such infrastructure is one challenge that Institute for Infocomm Research scientist Zhou Jianying hopes to overcome.

Earlier this month, the scientist from the Agency for Science, Technology and Research (A*Star) institute was given a grant under the Energy Market Authority's (EMA) Smart Energy Challenge scheme to develop new energy technologies. From the scheme's first grant call came five projects. Nanyang Technological University, for instance, is working on a project to turn food waste into useful gas for power generation, while the National University of Singapore is working on making better electric-car batteries.

Dr Zhou explained that smart grids allow for two-way communication between power suppliers and users, and these communication channels must be kept secure.

Ultimately, he said, the project's goal is to make hardware and software that can be used in smart cars and smart meters.

He added that because Singapore is so small, it is likely to be highly connected by networks, making it more vulnerable to attacks.

Earlier this year, security experts at the Black Hat conference in Las Vegas warned that current smart-grid hardware and software lack protection against hacking.

Berkeley professor Shankar Sastry, who works on smart buildings, said information attacks are "real, and you have to expect them".

So smart systems must be able to operate smoothly in the face of hacking attempts. "If something goes wrong," he said, "the system should continue to function."

Smart-grid privacy is another possible concern for governments and consumers, said Accenture's Mr Paul Gosling, managing director of its utilities industry group, which is working on the IES programme.

While smart metering can help consumers track their energy use and perhaps even control individual household appliances remotely, it comes with possible privacy pitfalls.

Said Mr Gosling: "If it's possible to disconnect your home appliances over the network, how do you know you and the power company are the only ones who can do that?"

There are also technical challenges, such as integrating the intermittent power supplied by solar panels or wind into the power grid.

These are issues which users should be informed about. Hence, involving and educating consumers is also an important aspect in the promotion of smart technologies.

Accenture, for instance, is working with the EMA on a plan for consumer engagement.

And one issue the consumers will be concerned with is: Will smart energy technology help save on costs?

Mr John Parkinson of global insurance firm Axis Capital wrote in a recent Harvard Business Review article: "We need to remember that making the grid smart will be expensive – telemetry, monitoring and management systems, data storage and new software will all be costly.

"So making the grid smarter isn't necessarily going to make electricity cheaper for the business user or consumer. More reliable? Almost certainly. Less unsightly infrastructure? Very possibly. Cheaper? Probably not."

The IES pilot scheme will help figure out what systems work best for Singapore, Mr Gosling said.

"It's a huge challenge, but also a huge opportunity."

caiwj@sph.com.sg