Power Systems Design: Empowering Global Innovation

The Smart Grid Needs Muntzing

Author: Edward Herbert, Co-Chairman, PSMA Energy Efficiency Committee
Date: 04/05/2014

Categories: Internet / Web

“Muntzing is the practice and technique of reducing the components inside an electronic appliance to the minimum required for it to function.”

Increased monitoring and automation of The Grid will significantly improve stability and reliability, avoiding blackouts and allowing a better response to anomalous line conditions. However, things get out of control over the ambitious goal of reaching through the Smart Meter to monitor and control everyone’s appliances, connecting it all to the Internet with powerful processors and full-featured communications.

Mr. Muntz stripped circuits of extraneous parts to save money, with the added benefits of reducing size, weight, and power. Processors and communication circuits are cheap, so the tendency now is to pile on the functionality and connect everything to the Internet of Things (IoT) so that all can be controlled remotely.

The control is seductive, and the risks are largely unrecognized or ignored. When this concept is linked to the mantra that it is necessary to stabilize the grid, avoid blackouts, and save building new power plants, it has been accepted, hook, line and sinker. So, what’s the problem?

Issues & questions

It requires a very extensive and expensive hardware and software infrastructure to control everything in the IoT. What are our chances of getting it right? If we build a grid that relies on a computer-based infrastructure, do we get a blackout when the computer crashes? It is very profitable for those who make the equipment, so they will promote it aggressively – at least until they face product liability and recalls.

Anything connected to the Internet can be hacked, as we’ve seen in the news. In one recent incident smart appliances were hacked to send SPAM, and we’ve all heard of the infamous case of Target being hacked to steal millions of credit card numbers and PINs. The list goes on. Security is an issue that will only increase in importance as the grid develops.

What if they get it wrong? Utilities should think twice about the liability in controlling millions of appliances. There has already been an increase in demand for insurance to cover energy firms, but many are being denied because their cyber-security is inadequate. There are also reports that Smart Meter sales have plummeted over security concerns, with large-scale layoffs.

Is it needed? Are there alternatives? Largely ignored is the need for a robust default mode to control the grid when the computer crashes, which could eliminate the need to micro-manage appliances. An infrastructure that is more responsive to line conditions may provide better power management with a faster response than is possible with a command-response protocol from remote computers.

A homeowner who wants smart appliances controllable from his smart phone should have that option, but for the utility, the Smart Meter should be a firewall, not a conduit for hacking.

This article reflects the opinion of the author, not necessarily that of the PSMA.

References:

Who controls the off switch? Ross Anderson, Shailendra Fuloria, Computer Laboratory, Cambridge University, UK – www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf

Smart Meter Slowdown Blues: Itron Cuts Workforce, Greentechgrid, Jeff St. John, September 13, 2013. – www.greentechmedia.com/articles/read/smart-meter-slowdown-blues-itron-cuts-workforce

Smart refrigerators and TVs hacked to send out spam, according to a new report, NBC News, Julianne Pepitone, Jan. 18, 2014. – www.nbcnews.com/tech/internet/smart-refrigerators-hacked-send-out-spam-report-n11946

Energy firm cyber-defence is 'too weak', insurers say Mark Ward, Technology correspondent, BBC News 26 February 2014 – www.bbc.com/news/technology-26358042

Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ, Spencer Ackerman and James Ball, The Guardian, Thursday 27 February 2014 – www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo