Power Systems Design: Empowering Global Innovation

How smart is the Smart Grid when the computer crashes?

Author: Edward Herbert, PSMA Energy Efficiency Committee
Date: 02/17/2014

Categories: Government & Industry, Power Supplies, Smart Power Grid

Over-reliance on a central computer is an invitation for disaster

Software security in the grid is becoming increasingly important. There have been reports of appliances hacked to send SPAM, and The Wall Street Journal claims that the Smart Grid already has been penetrated and infected with potentially disruptive software programs. There are even fears that terrorists may penetrate the SCADA systems in utilities and wreck a generator as revenge for “Stuxnet.”. Homeland Security surely is giving this attention.

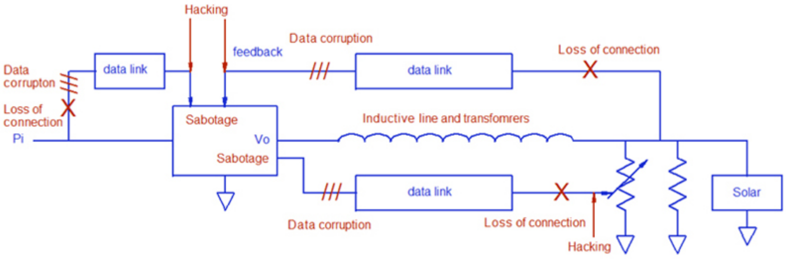
My concern, however, is more mundane: what happens when the computer crashes? What should happen is “nothing,” or at least nothing that does damage or that cannot be managed expediently.

An infrastructure using central computers with multiple sensors overlaying the Grid is a very powerful tool, with great potential for improving Grid performance and reliability. Using real-time measurement, such systems can pinpoint where repair is needed during a crisis, as well as predict problems. Computer-based management systems allow for unprecedented modeling and calibration. For example, the advantages of automated meter reading for billing are well recognized.

However, over-reliance on a central computer is an invitation for disaster. A Grid that requires a central computer and communications for stable operation very likely will become unstable when the computer crashes.

Command & control

One of the justifications for the Smart Grid is that we can avoid building more power plants if we can send out commands to reduce the load in times of stress. What happens if you cannot implement those commands? Times of stress are when a central computer is most vulnerable, most likely to be unusable (see Figure 1).

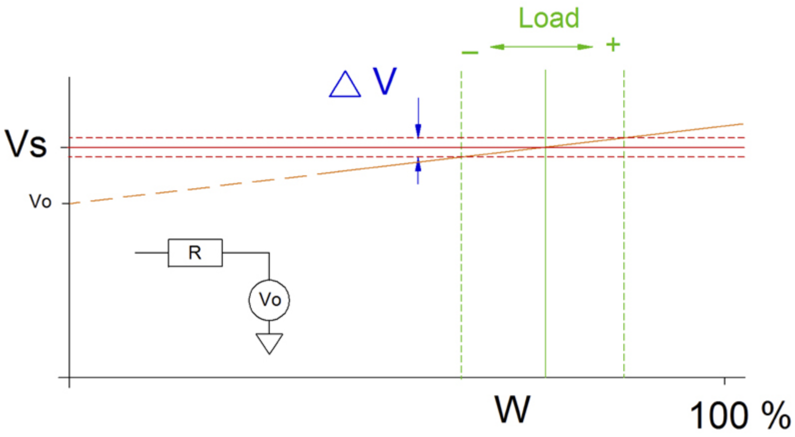


Click image to enlarge

Figure 1:This model of the Smart Grid is based upon a power supply with remote sense. There are many vulnerable points.

Power supply designers understand the need for stability analyses. Loop stability is dependent on response, and lags are a problem. Has the Smart Grid been analyzed to account for lags? What about the time needed to collect and analyze Mega-data, and output the commands to the control devices? A denial-of-service attack could slow the response to a crawl. The lag will make it impossible to respond quickly.

Taken together, the inevitability of computer crashes and the slow response make it imperative that local systems have robust default modes and fast response to rapidly changing line conditions. Local controls need to be there. If well done, they mitigate the need for centralized computer control (see Figure 2).



Click image to enlarge

Figure 2: Local control that varies the load in response to line voltage, as an example, is fast and does not rely on a central computer. Other parameters that can be used are frequency and phase angle.

The threat of hacking
The conversation needs to include hacking, as it is a sub-set of computer failure. Anything that connects to the Internet has the potential of being hacked.

The most effective hack renders the equipment inoperable and non-repairable. Unfortunately, this is much easier than most people realize, partly because of the features that are built in for tight security. Consider a malicious command that turns an appliance off, followed by a firmware update that makes it non-responsive to any command or override. Or a hack that changes the encryption key, so that the appliance responds only to the hacker, or to no one at all.

Contrary to popular perception, the greatest threat of hacking is not the foreign terrorist but disgruntled employees. Regardless of security and encryption, most commands originate with a person or an algorithm. The bookkeeper that notes that a customer is delinquent disconnects him with a click of a mouse, and security won't stop her. She probably cannot update the firmware or change the encryption keys, but if you substitute the consultant who is hired to upgrade the anti-virus software, he could. He can plant a logic bomb that simultaneously shuts off thousands of customers after he has moved on. Thousands of Smart Meters, shutoff, with corrupted encryption keys, is scary.

The best defense against hacking is having it not do much, the same as the preferred response to computer crashes. If hacking did not do much, it would be no fun and the hackers would stop trying.

So, what can commands from a central computer do that is safe? Often, the concern is "data security," whether a burglar could tell who isn't home by motoring appliance use. While important, that will not threaten the stability of the Grid. So, monitoring and collecting data are OK. But why does a refrigerator need the computer power to send emails? Part of the answer may be limiting function to what really is needed.

Market issues

Much of power management is arbitrage. Arbitrage cannot be managed by detecting line conditions, so it needs to be authorized and commanded from a central authority. However, arbitrage does not require abrupt changes. One way to limit the ability to do damage is to apply power changes due to arbitrage at a very slow rate, slow enough so that errors will be detected and corrected before damage is done.

One function that the utilities would never give up is the ability to shut off the power to delinquent customers. There is no urgency. If shut-off commands were sent but could only decrease the power by 4 % per hour, constrained by hardware, it would take a day to be turned off entirely. That's OK. Mistakes could be caught and corrected, and the customer might even pay his bill.

What if the encryption keys were hacked? The default mode should be “On.” Absent commands that maintained the off-state, the Smart Meter should ramp up 4% per hour to their baseline power.

How about power control during heat waves? The same mechanism can apply. The default power allowed by the Smart Meter should be a reduced level, a baseline power that would not overload the system even in times of high demand. Buying more power above the default level is arbitrage, and would require command and response to enable and sustain it. 99.9% of the time, this would be fully functional. When the computer crashes, everyone has enough power to get by and the total load is low enough not to overload the Grid..

Note that in the above scenarios, the Smart Meter is not relaying commands to control specific appliances. It is just enabling a percentage of baseline power, lower or higher. It is up to the customer to turn-off some appliances or buy more power on the spot market when necessary. The sophisticated customer may have a load management computer tied to his smart phone. Others may just unplug what is not needed. The computational power and software needed by the utilities is much less, therefore much less expensive.

Little mention is made of liability, but once it is considered, the utilities may realize that the risk of having explicit control of specific appliances may be unacceptable. What is the liability if a freezer is turned off, but cannot be turned on? Times 10,000?

There was a surge in Smart Meter deployment with large grants, but now the Smart Meter manufacturers are in trouble as sales lag. Security concerns may be a significant factor. Utilities may be realizing that getting it wrong could be very expensive.

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

Puerto Rico smart meters believed to have been hacked – and such hacks likely to spread, Metering.com, April 11, 2012

Smart Grid Threat Landscape and Good Practice Guide, Louis Marinos, European Union Agency for Network and Information Security

Security Concerns Behind Slowdown in Itron Rollout? Greentechgrid, Jeff St. John February 9, 2009.

Smart Meter Slowdown Blues: Itron Cuts Workforce, Greentechgrid, Jeff St. John, September 13, 2013.

Electricity Grid in U.S. Penetrated By Spies, The Wall Street Journal, Siobhan Gorman, April 8, 2009

Smart refrigerators and TVs hacked to send out spam, according to a new report, NBC News, Julianne Pepitone, Jan. 18, 2014.