

Smart Grid and Ops

Author: Guy Huntington, President, Huntington Ventures Ltd.

Date: August 16, 2010

Note: The views expressed herein are the author's own personal opinions.

Smart Grid and Ops

This paper is the author's personal opinion re the impact smart grid has on the utility control room.

You Receive a Call

You receive a call from a grumpy utility customer, who is part of a smart grid program where the utility can control their appliances. They're complaining some of their appliances don't work and they're blaming the utility. What could be the problem? Could it be:

- The actual appliance?
- The network connection between the appliance and the home energy controller?
- The home energy controller?
- The home area network?
- The electrical supply to the home?
- The connection between the home and the utility's corporate network where the applications controlling the appliances are located?
- The different network segments within the utility storing the applications talking to the home?
- A security attack against the utility developing?

So what does this mean? It has implications across the utility's departments.

This Crosses Over All the Internal Utility Fiefdoms

Most utilities have separate departments running "engineering/asset management", control room ops, logical and physical security and IT. To address the above situation, it requires instantaneous monitoring, integrated incident management and personnel responses from systems, infrastructure and applications that are likely currently silo-ized within the utility. The deployment of smart grid services to the customer opens up the utility to addressing the problem listed above.

Control Room of the Future

I see four major roles in the control room of the future:

1. Traditional SCADA operator – Their role will not be greatly changed with smart grid. Their screens will change somewhat with the introduction of smart transformers, power line monitors and feeder automation as will some of their escalated responses. However, in the main I see these changes as evolutionary and not revolutionary in nature. One exception to this will be in the area of new power generation from home owners and small businesses. The operator will have to monitor this as well and new processes, authentication and monitoring implemented in the control room.
2. "General Ops" – I see a new type of person sitting in the control room beside the traditional SCADA operator. This person is responsible for monitoring everything from the home (i.e. appliances, HAN (home area network), utility-home network connection, corporate firewalls, corporate network segments, applications controlling and talking to the home) up to the SCADA firewall. This person doesn't exist today in the control room. Additionally, the monitoring

systems and management screens are mostly new technology that will have to be developed. This is really an IT type person now in the control room.

3. “Global Incident Management” – the third position was a much expanded incident management person. All utilities have good to excellent incident management folks in the control room monitoring the SCADA infrastructure and dispatching crews. However, there is often a separate IT incident management team monitoring what goes on in the corporate network. I foresaw much of the IT incident management being moved into the control room and heavily integrated with the existing utility incident management. This will likely require new people in the control room who are cross-trained on SCADA and IT systems. The incident management system will require all sorts of new monitoring systems that either don’t exist today or will have to be adapted to get the information from the home through the external networks and internal networks and applications. It is my guess that this would take significant resources to develop.
4. “Integrated Security Ops”. One thing smart grid does is open up all sorts of new security attack vectors into a utility. It also opens up new opportunities for terrorists or organized crime to seriously disrupt home and commercial customers. I foresaw the need for an integrated security ops desk in the control room to address this. This role would be responsible for determining if an attack was occurring in the home, utility corporate or utility SCADA. The security management system would be an extension of some of the new emerging utility defence software being developed to also include the home and corporate.

Utility Reorganization

I predict that most utilities deploying smart grid over the next several years will likely have to do a re-organization of their departments and functions to effectively manage the new services they will be offering to their customers. I think that engineering and grid ops will assume many of the functions that IT is currently doing. Further, I also believe security would become tightly integrated across the enterprise and centrally managed with a body in the control room having their own security ops incident management screens tightly integrated with global incident management.

Summary - Smart Grid is like an Iceberg

This paper is meant as a discussion point for senior utility managers when thinking about smart grid. It is so much more than buying some portal type software from any of the main smart grid vendors or deploying smart transformers et al on your SCADA networks.

My point is that smart grid is like an iceberg. What you see on the surface (energy reduction software to the customer and creating a swift self-healing grid) come below the surface with a large, unseen, infrastructure, personnel and departmental reorganization requirements. I think it's a significant price tag.

Canadian and American regulatory authorities, shareholders of utility companies, utility senior management and utility customers need to become aware of the increasing complexity, cost and security risks they are deploying with smart grid.

About the Author

Guy Huntington is a learned and burned identity management and security consultant. He has led a utility identity management program, participated in a utility security assessment, integrated physical and logical security and rescued several large Fortune 500 identity projects. His white papers can be read at <http://www.authenticationworld.com/papers.html>. He can be reached at guy@hvl.net or 1-604-861-6804.