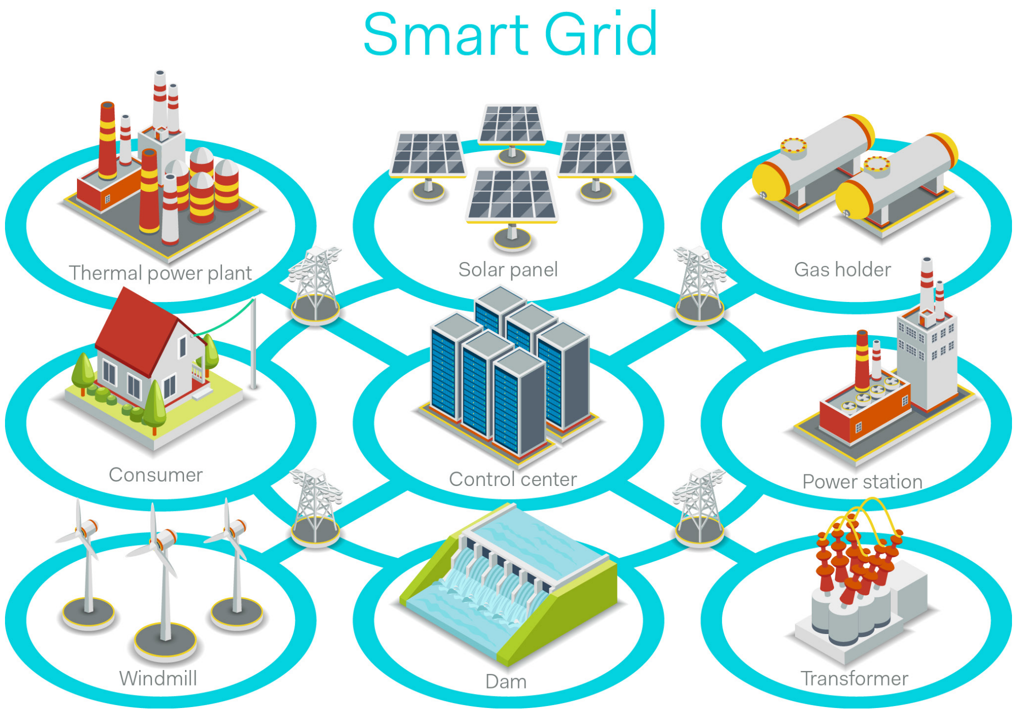


Figure 01 – Smart Grid network very distributed and vulnerable to physical and cyber-attacks.

Is your smart grid secured?

Involved in early days projects to add communication and intelligence to power supplies, which became the so called “Digital Power” I have been frequently asked about software security and how the power supplies industry was prepared to address such issues? If it is for sure, there is very little risk a hacker reaches a single Digital-POL at board level, the risk increases exponentially as we move upward in the value chain and, in that chain, the Smart Grid is probably the highest and the most exposed to attacks (Figure 01).

At time the number of renewable power sources are growing, smart meters deploying and many others connected to the Smart Grid, what is the situation in terms of security? Are we safe?

Risk escalation

From the 2007, when the US government demonstrated, in the Aurora Generator Test, with only 21 lines of codes, how hackers could take control of a power plant and physically destroy a generator; to April 2016 when a water and electricity authority in the State of Michigan, after been victim of a ransomware attack was forced to keep IT systems locked down for a week, the number of cases reported to security authorities is rapidly increasing.

The Florida International University estimated that, during the first six months of 2015, more than100 cyber incidents have affected infrastructure in the US and the energy sector had the largest number of attacks. Cyber-attacks toward Smart Grid is a global threat and all countries exposed to high risk, motivating power experts and networks managers to consider global response and methodology to prevent any damages.

February 2016, the US Department of Homeland Security (DHS) issued an alert (IR-ALERT-H-16-056-01), reporting on a case that happened on December 2015 in Ukraine, lifting the information to a high level of attention to Smart Grid Operators, motivating them to accelerate protections mechanisms and to develop preventive actions policies.

The Ukrainian case combines multiple elements in the attack, including physical sabotage though the sophistication of the part related to the cyber-attack reached a new level of intrusion, motivating the Smart Grid community to strengthen cooperation and efforts to accelerate sustainable security within the Smart Grid.

Black Christmas for Ukrainians!
December 23rd 2015 at 04:00 PM, the Ukrainian's region Ivano-Frankivsk was plunged into darkness for several hours and more than 220.000 customers lose power and, the IT and communications systems of the electricity companies severely damaged by the attackers.

In this case, the attackers combined a large number of attacking tools, spreading phishing e-mail containing a variant of the BlackEnergy 3 and KillDisk malwares, exploiting MS Office documents security holes to get into the IT network of the electricity companies and inhibited most of the security agent in firewalls (Figure 02). At the same time they managed to break credential codes to access deeper level of the system, controlling industrial communication busses such as the ones interconnecting Uninterruptible Power Systems (UPS) and to the Supervisory Control and Data Acquisition (SCADA) systems.

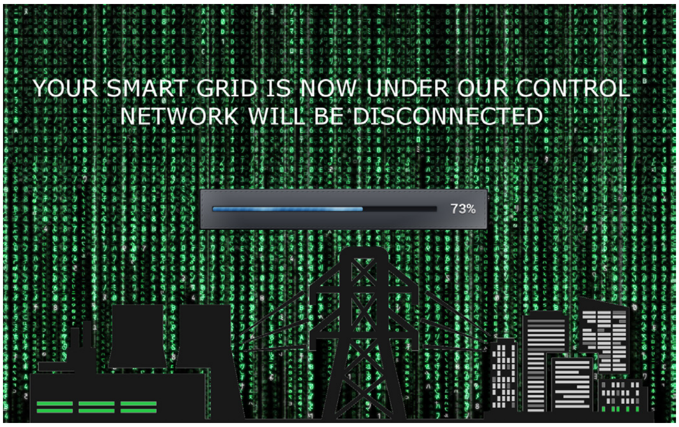

YOUR SMART GRID IS NOW UNDER OUR CONTROL
NETWORK WILL BE DISCONNECTED
73%

Figure 02 – Cyber criminals taking control of Smart Grid is now reality!

SCADA systems are basically Process Control Systems (PCS) that are used for monitoring, gathering, and analyzing real-time environmental data. PCSs are designed to automate electronic systems based on a predetermined set of conditions, such as traffic control or power grid management. For the ones used to lower energy and board power systems, it's a super Software Define Power Architecture, which, considering the strategic role it plays, requires an extremely high level of security. Managing to control the SCADA systems, the hackers accessed the electricity network, with possibility to shut down and severely damage equipment.

The Ukrainian's case is considered as "real life example" of what could happen to larger networks and lessons to learn from that case part of the ongoing Smart Grid security standardization projects run in USA, Europe and Japan.

Making Smart Grid safer!
Smart Grid is an extremely complex architecture with a lot of areas for intrusions and attacks. Especially when operating a Smart Grid has moved from managing electricity distribution to a supper Information and Communication Technology machinery. Michael McElfresh, Adjunct Professor of Electrical Engineering at Santa Clara University, very well summarized the situation, saying: "Technological advances in grid operation have made the power grid increasingly vulnerable to cyberattacks, writes The growth of the smart grid has created many more access points for penetrating grid computer systems – the "internet of things" will only make this worse."

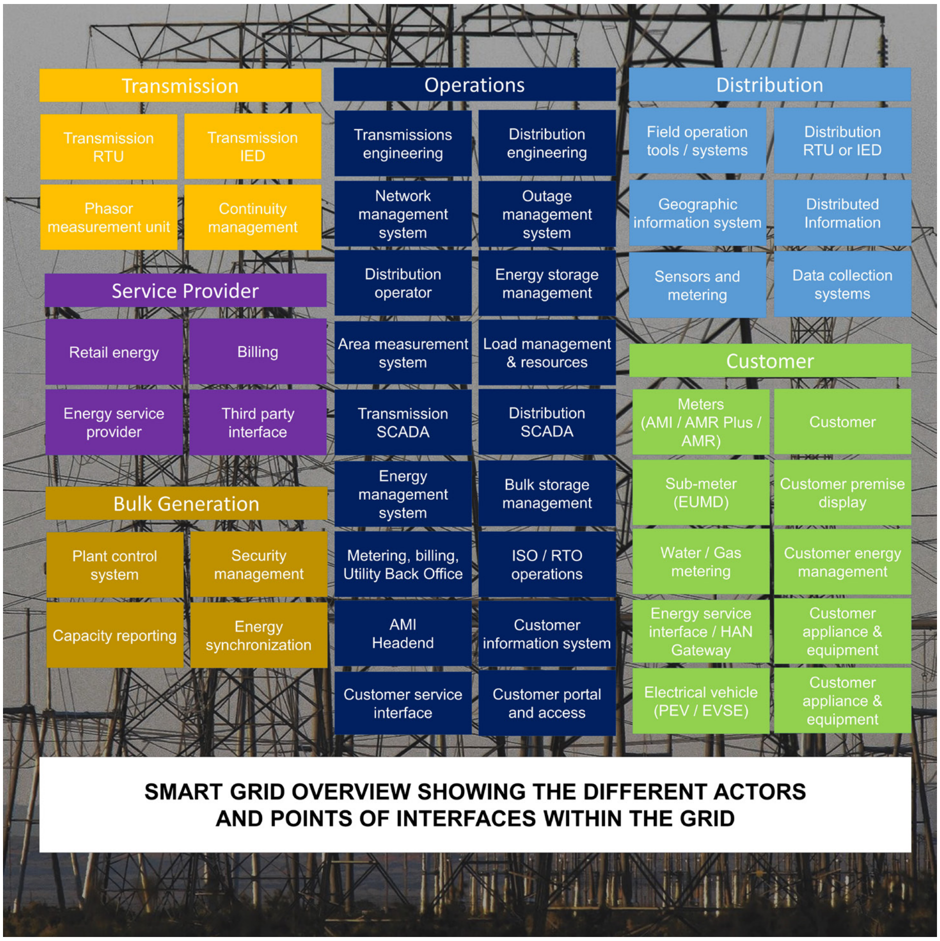
All over the world, governmental, consortiums and group of experts are engaged in an amazing race to deploy security methods and protocols to make the Smart Grid safer. In USA, the set of Critical Infrastructure Protection (CIP) standards issued by the North American Electric Reliability Corporation (NERC) became mandatory in 2007 for owners, operators and users of the Bulk Electric System (BES) to ensure that certain assets on the grid critical to reliable operation are protected from both a cybersecurity and physical security standpoint, is going through a wave of new revisions, moving from CIP V3 to CIP V5, skipping V4, and accelerating V6! That situation reflects the situation faced by the standardization organization developing security standards in a fast evolving world of threats.

In Europe, despite a number of initiatives within the European network and information security community to establish frameworks and standard operating procedures, the EU-level response to cyber incidents lacks consistency though projects such the EU-funded Smart Grid Protection Against Cyber Attacks (SPARKS) are showing very good signs of progresses.

Step by step, the worldwide Smart Grid is getting stronger and safer though the potential of threats remains high.

In conclusion

Because of the complexity and the variety of connected devices to the Smart Grid (Figure 03), power supplies manufacturers will have to consider the security aspect when their products integrated within a Smart Grid. As I introduced at APEC 2015 Software Defined Power Architecture is deploying fast in the ICT industry and some systems, already installed in data-centers, are connected to the Smart Grid and communicating through the SCADA system.



Transmission
Transmission RTU
Transmission IED
Phasor measurement unit
Continuity management

Service Provider
Retail energy
Billing
Energy service provider
Third party interface

Bulk Generation
Plant control system
Security management
Capacity reporting
Energy synchronization

Operations
Transmissions engineering
Distribution engineering
Network management system
Outage management system
Distribution operator
Energy storage management
Area measurement system
Load management & resources
Transmission SCADA
Distribution SCADA
Energy management system
Bulk storage management
Metering, billing, Utility Back Office
ISO / RTO operations
AMI Headend
Customer information system
Customer service interface
Customer portal and access

Distribution
Field operation tools / systems
Distribution RTU or IED
Geographic information system
Distributed Information
Sensors and metering
Data collection systems

Customer
Meters (AMI / AMR Plus / AMR)
Customer
Sub-meter (EUMD)
Customer premise display
Water / Gas metering
Customer energy management
Energy service interface / HAN Gateway
Customer appliance & equipment
Electrical vehicle (PEV / EVSE)
Customer appliance & equipment

SMART GRID OVERVIEW SHOWING THE DIFFERENT ACTORS AND POINTS OF INTERFACES WITHIN THE GRID

Figure 03 – The complexity of the Smart Grid makes it very difficult to protect globally.

To close the loop, if there is little risk a hacker to send a command to a POL blasting local core processor, the risk for UPS and even frontend rectifier to receive a fatal command is not excluded. The Ukrainian's case trigged the alarm ON and for all of us involved in developing power systems connected to the Smart Grid a signal that we should never forget about the final application and to be Smart Security Innovators to power Smart Grid with excellence.

About Powerbox

Founded in 1974, with headquarters in Sweden and operations in 15 countries across four continents, Powerbox serves customers all around the globe. The company focuses on four major markets - industrial, medical, transportation/railway and defense - for which it designs and markets premium quality power conversion systems for demanding applications. Powerbox's mission is to use its expertise to increase customers' competitiveness by meeting all of their power needs. Every aspect of the company's business is focused on that goal, from the design of advanced components that go into products, through to high levels of customer service. Powerbox is recognized for technical innovations that reduce energy consumption and its ability to manage full product lifecycles while minimizing environmental impact.

For more information

Visit www.prbx.com
Please contact Patrick Le Fèvre, CMCO
+46 (0)158 703 00

PRBX white paper 008 Rev A
2016.09.15