P R

B X

POWERBOX
Mastering Power

From Power Plant to POL
Cyber-Criminals are on you!

Powerbox

Patrick Le Fèvre – Chief Marketing & Communications Officer

Kraftforum - Gothenburg

May 18 - 2017

Powerbox – Smart Grid Security
Presenter – Patrick Le Fèvre

www.prbx.com

Patrick Le Fèvre is an international marketer and engineer who has worked in power electronics for over three decades.

His career has been focused on power products since 1982 when he started with a start-up called Micro-Gisco (France).

He joined Powerbox Sweden in September 2015 as Marketing Director and in January 2016 was promoted Chief Marketing and Communication Officer for the all Group.

Prior Powerbox, he held senior marketing and communication roles at Ericsson, Power Modules division, for 20 years.

Patrick Le Fèvre is the author of several articles and marketing papers presented at various conferences, and deeply involved in a number of groups and associations related to power-supplies, energy efficiency and contributing to promote new technologies within the power community.

Patrick Le Fèvre received most of his education in France, where he studied electronics, microelectronics and industrial marketing, and where he received a civil engineer degree in 1982.

Powerbox – Smart Grid Security
Company key numbers

P R
B X

1974
Gnesta

150
Power people

15
Countries

25
R&D and Engineering

3
R&D center in Europe

>6M
6,000,000 hours
Proven MTBF

>1M
Units/year

>90%
Returning customers

UN.GC
Environmental
Social
Governance
engagement

3.500
Custom projects since 1974

Powerbox – Smart Grid Security
The journey!

→Smart Grid overview

→At start was Aurora

→From simple to complex attacks

→Securing the Smart Grid

→Are we safe at board level?

→Conclusions

→Happy to answer your questions

Powerbox – Smart Grid Security
The business case

→Reduce cost to consumers

→Better ability to manage peaks on demand

→Defer or avoid to build extra infrastructures

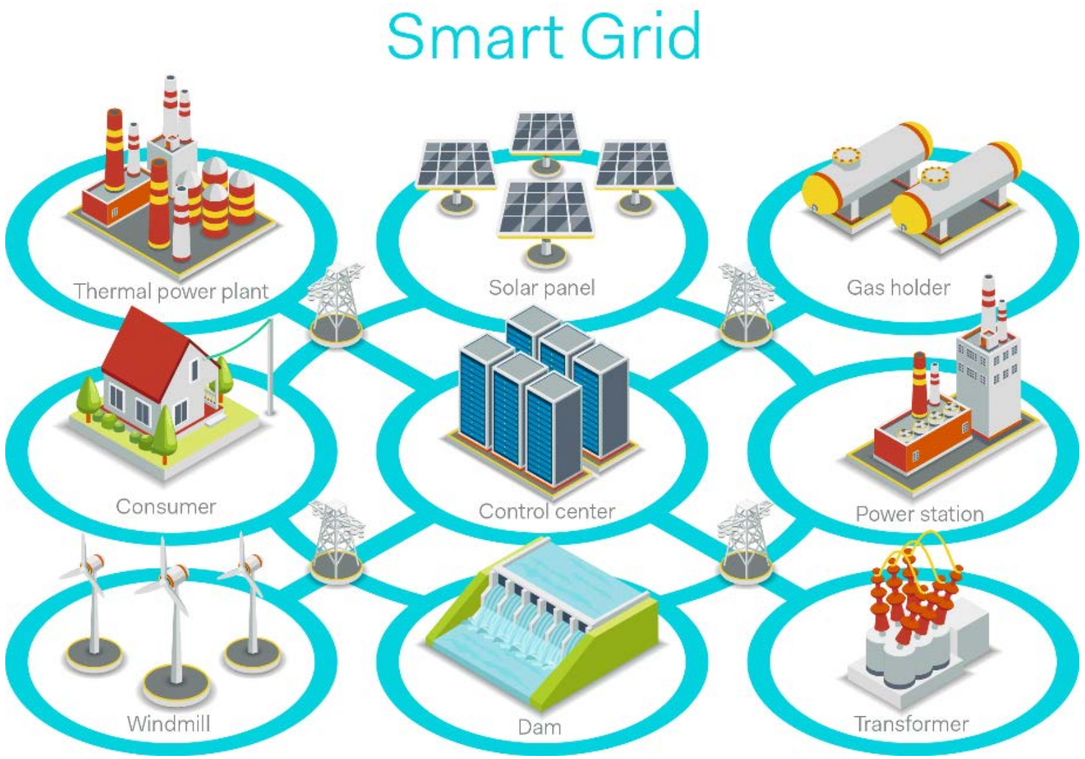
→Reducing greenhouse gases and carbon footprint

→Integration of renewable energies (wind, solar…) into the grid

→Smart metering and better control of energy distribution and consumption

→Flexibility

Powerbox – Smart Grid Security
From Electricity to Intelligent Network



→Smart Grid (SG) is an ecosystem

→Migration from Electricity generation and distribution to intelligent network

→From Generator to Consumer SG is transforming into a huge data network

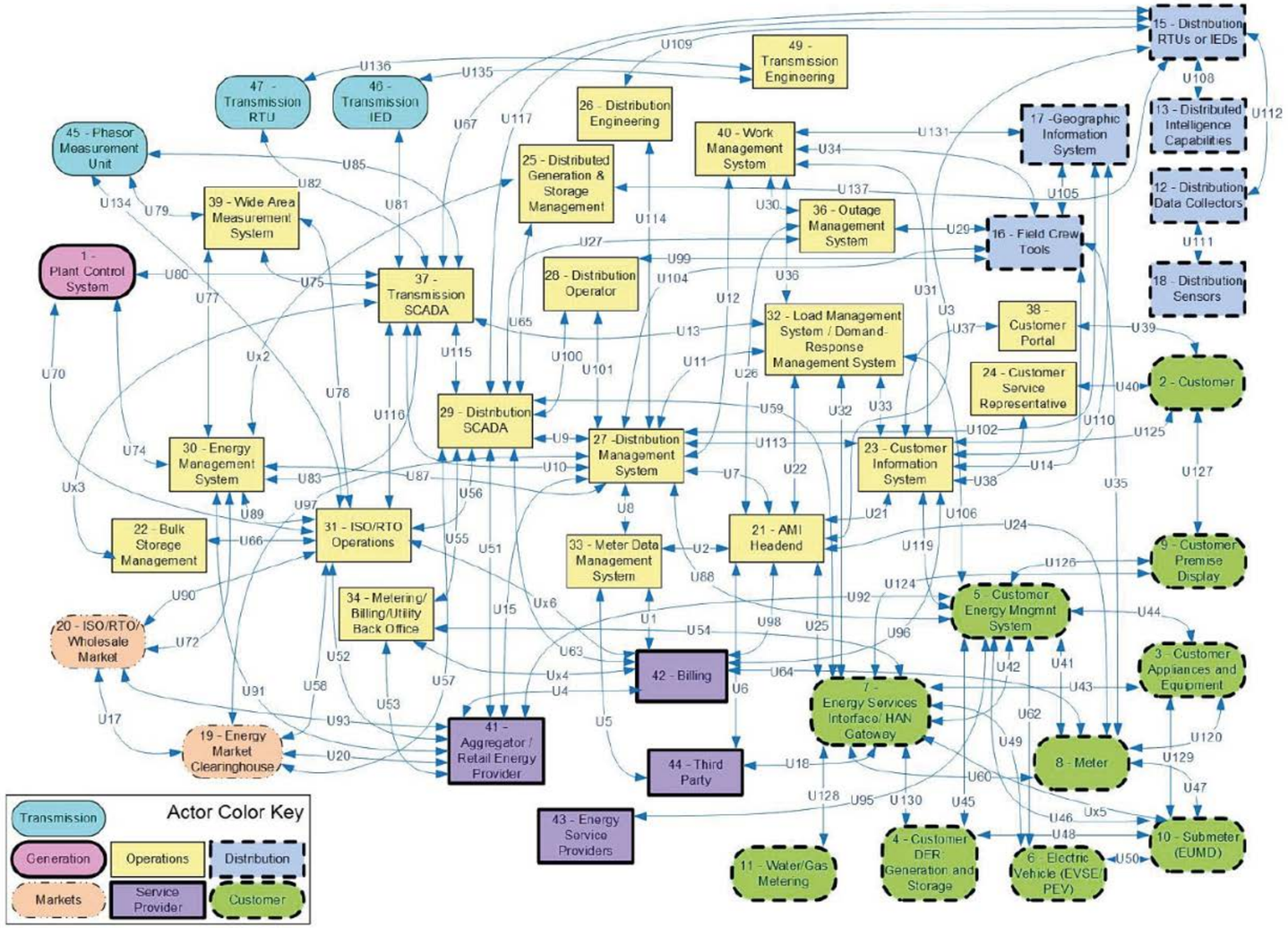
→New technologies and connected devices (e.g. IoT) are increasing interfaces

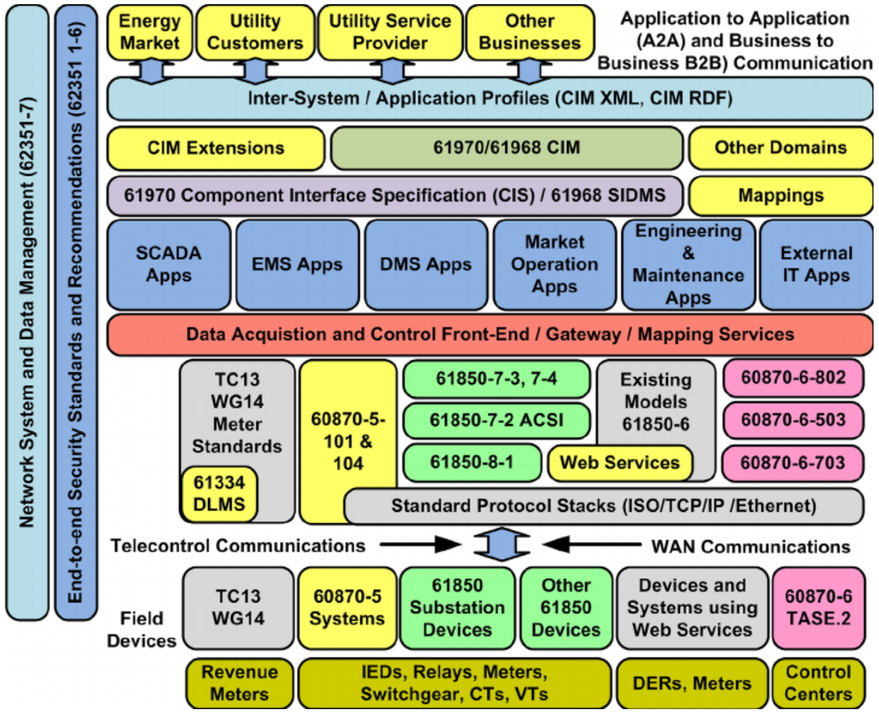
→Risk of intrusion and cyber-attacks are increasing as Grid connectors booming

Powerbox – Smart Grid Security
At start it was a Grid…

Source: Institute for Energy Research (IER)

Powerbox – Smart Grid Security
Then arrived the Smart Grid…





e.g. The IEC 60870 is a set of standards which define systems used for tele-control in supervisory control and data acquisition (SCADA) in electrical engineering and power system automation applications.

Powerbox – Smart Grid Security
The Threats

→Hackers & Crackers

→Computer Criminals

→Terrorism

→Cyberwar

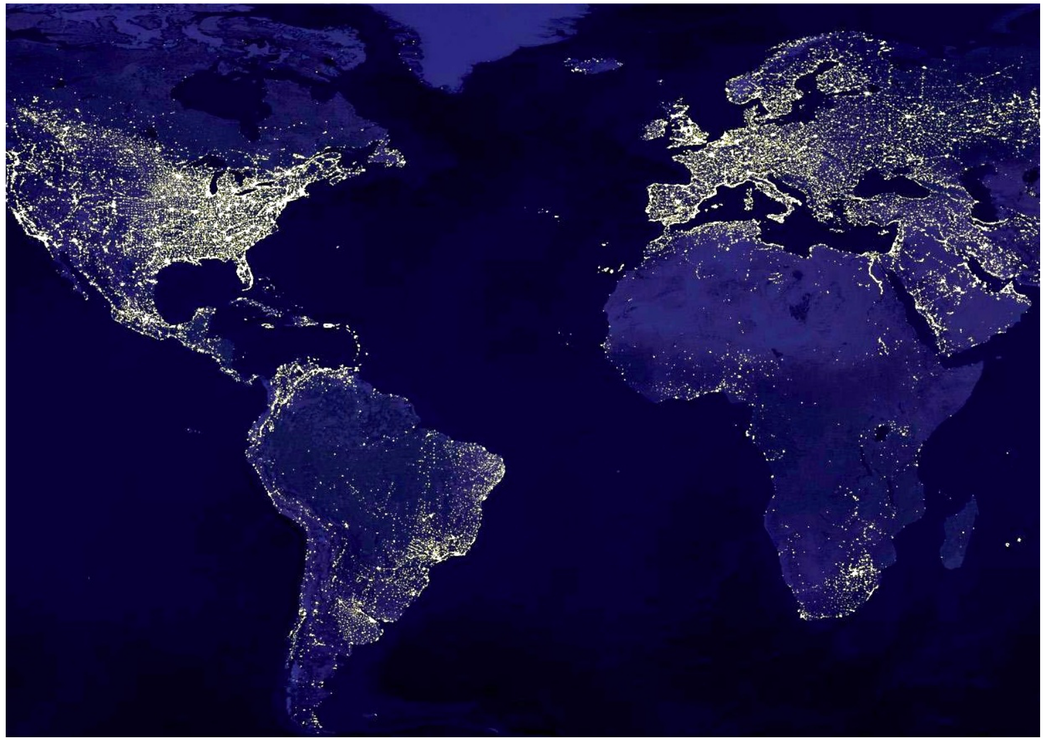
→Industrial Espionage

→Insiders

Powerbox – Smart Grid Security
The Threats

Threat-Source	Motivations	Threat Actions
Hacker, cracker	• Challenge • Ego • Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	• Destruction of information • Illegal information disclosure • Monetary gain • Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, interception) • Information bribery • Spoofing • System intrusion
Terrorism	• Blackmail • Destruction • Exploitation • Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denied of service) • System penetration • System tampering
Industrial espionage (companies, foreign government, other government interest)	• Competitive advantage • Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration and unauthorized access
Insiders	• Curiosity • Ego • Intelligence • Monetary gain • Revenge	• Blackmail • Malicious code (e.g., virus, logic, Trojan horse) • Fraud and theft • System sabotage • Input falsified, corrupted data interception

Powerbox – Smart Grid Security
The Consequences



→Population

→Reputational

→Infrastructures

→Regulatory

→Equipment

→Data protection and privacy

→Safety

→Economic

Powerbox – Smart Grid Security
The Consequences

Category	Consequences
Population	• Population affected, e.g., loss of power or observable quality issues (flicker) • Safety related issues
Reputational	• Loss of trust and confidence
Infrastructures	• Shut down of dependent infrastructure
Regulatory	• Sanctions / Warnings, penalties (€), disgorgement (€) and other compliance measures
Equipment	• Damage to ICT equipment • Damage to power systems equipment
Data Protection and Privacy	• Disclosure or modification of personal or sensitive data
Safety	• Minor or serious injury • Loss of life
Economic	• Cost of electrical losses • Customer outage costs, i.e. cost of energy not supplied • Congestion costs, resistive power losses, power import, ancillary service usage • Investigation and repair time, work time lost

The real life…
From Aurora to POL

Powerbox – Smart Grid Security
At start was the AURORA

March 04, 2007

→2006 / 2007 The Aurora project

- Idaho National Lab. accessed a generator
- Supervisory Control & Data Acquisition (SCADA) used to access and send commands
- Generator destroyed through simulated “cyber attack”

→Lessons learned

- Physical damage can result from a cyber attack
- Public / Private partnership complicated
- Lack or regulatory and guidance
- Discovering a new word of threats

→Aurora opened the Pandora Box

Powerbox – Smart Grid Security
From simple to complex attacks

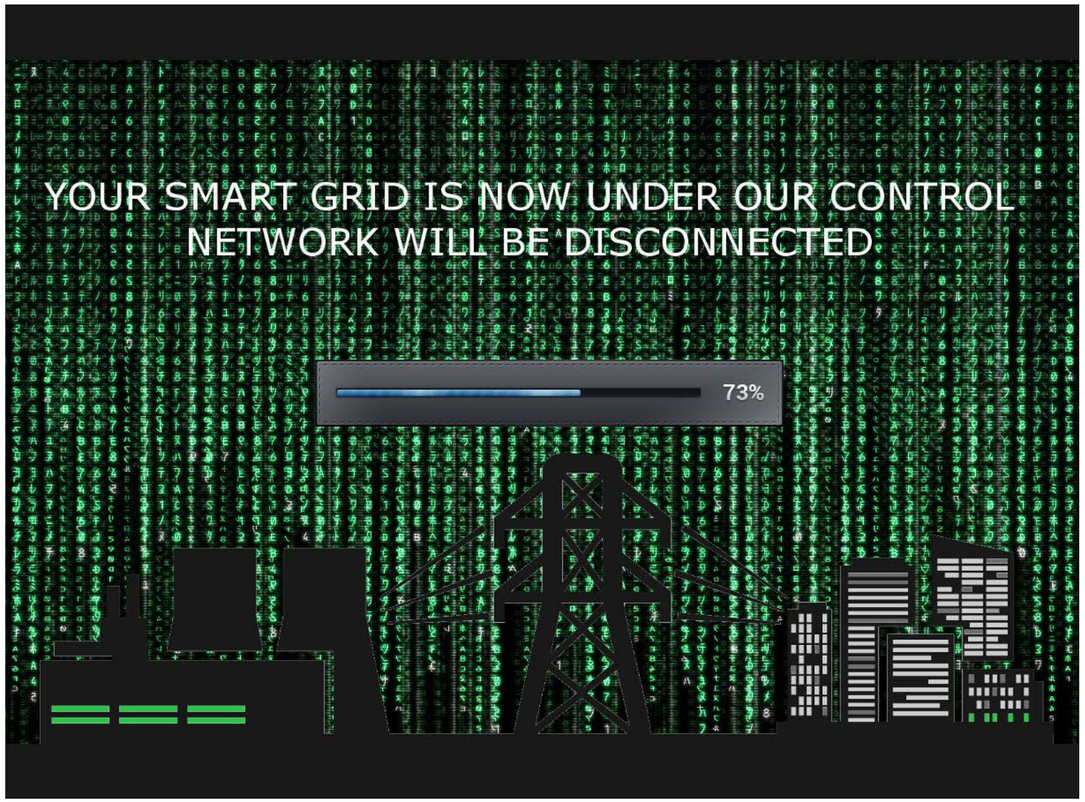
→April 2007

- Exploit of Microsoft zero-day vulnerability to access energy company SCADA
- Origin of the attach through simple phishing
- Taking advantage of windows DNS vulnerability

→August 2010

- Mutant of the “Stuxnet” worm propagated through SCADA into Smart Grid
- Suspected to be the first attack from another government not involving military action

Powerbox – Smart Grid Security
Dark Christmas for Ukraine



December 24, 2015

→Direct attacks toward regional distribution system (Ivano-Frankivsk region)

→225 000 customers impacted

→Multiple modus operandi

- Phishing e-mails - BlackEnergy 3 malware
- KillDisk attacking Master Boot record
- Control of Human Machin Interface (HMI)
- Control of UPSs operation
- Physical sabotage

→February 25, 2016 US Dept. of Homeland Security (DHS) issued a formal alert

Powerbox – Smart Grid Security
Ransomware shutdown BWL

April 26, 2016

→Michigan - Board of Water & Light (BWL) attacked through Ransomware

→BWL forced to shutdown all IT systems

→FBI involved in the investigations

→Several months for BWL to restore

→Attack suspected to come from another country from cyber-criminal organization

→This case is considered as part of a mechanism to attack Energy Suppliers

Powerbox – Smart Grid Security
Connecting SG to DDoS

→September 2016 – OVH (France)

– Massive Distributed Denial-of-Service DDoS attack through 150 000 IoT devices (CCTV cameras and smart-meters) 1Tbps

→October 2016 – Dyn (USA)

– Dyn getting “tens of millions” of messages from Internet-connected devices, including smart-meters

→November 2016 – Deutsche Telekom

– More than 900 000 customers knocked offline - Routers infected by a new variant of a computer worm known as Mirai

Powerbox – Smart Grid Security
Securing the Smart Grid

→The US Department Of Energy (DOE) released a number of projects and initiatives, as well other governmental agencies

→December 2016 – White House published the “National Electric Grid Security And Resilience Plan”

→The European Network and Information Security Agency (ENISA), the EU-funded SPARKS (Smart Grid Protection Against Cyber Attacks – project) and many others building safer SG

→International projects aiming to bridge US and EU into a common protection alliance in discussion

Powerbox – Smart Grid Security
What about at board level?

→Power community is not used to deal with security

→Hacker could access a system through industrial SCADA without any problem

→How much is PMBus secured?

→Is the power industry too confident?

→Insider threats are real (Dolphin case)

→Cyber criminality is increasing faster than we could imagine

→Power industry must deploy strategies to include highest level of security in any layer of software

Powerbox – Smart Grid Security Conclusions

→Smart Grid is a very complex architecture requiring high level of cooperation to protect

→Learning by mistake is not an option!

→Governmental initiatives are accelerating though political instability increasing threats at high pace

→Creating awareness and educating power designers and systems architects business critical

→In front of Cyber Criminality, nothing is for granted

→Cyber security starts at board level

→Sounds dramatic though a lot of fun ahead!

Powerbox – Smart Grid Security References

P R
B X

Is your Smart Grid Secured (IEEE)
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7790948

February 25, 2016 US Dept. of Homeland Security (DHS) issued a formal alert
https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Analysis of the Cyber Attack on the Ukrainian Power Grid
http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

ENISA – Smart Grid Security
https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf

Salesforce Security CTO: How A DDoS Attack Can Impact A Smart Grid
http://www.crn.com/news/internet-of-things/video/300083164/salesforce-security-cto-how-a-ddos-attack-can-impact-a-smart-grid.htm

White House – National Electric Grid Action Plan
https://www.whitehouse.gov/sites/whitehouse.gov/files/images/National_Electric_Grid_Action_Plan_06Dec2016.pdf

Digital attack tracking
http://www.digitalattackmap.com

Book to read:
"Countdown to Zero Day“ by Kim Zetter
https://www.amazon.com/Countdown-Zero-Day-Stuxnet-Digital/dp/0770436196

P R

B X

POWERBOX
Mastering Power

Thanks for your attention!

For more information contact patrick.le-fevre@prbx.com