P R

B X

POWERBOX
Mastering Power

Smart Grid Security

Is your Smart Grid Secured?

Powerbox

Patrick Le Fèvre – Chief Marketing & Communications Officer

APEC 2017 – Tampa (FL) USA

March 30 - 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.

Smart Grid Security

Is your smart grid secured?

Powerbox – Smart Grid Security
The journey!

→Smart Grid overview

→At start was Aurora

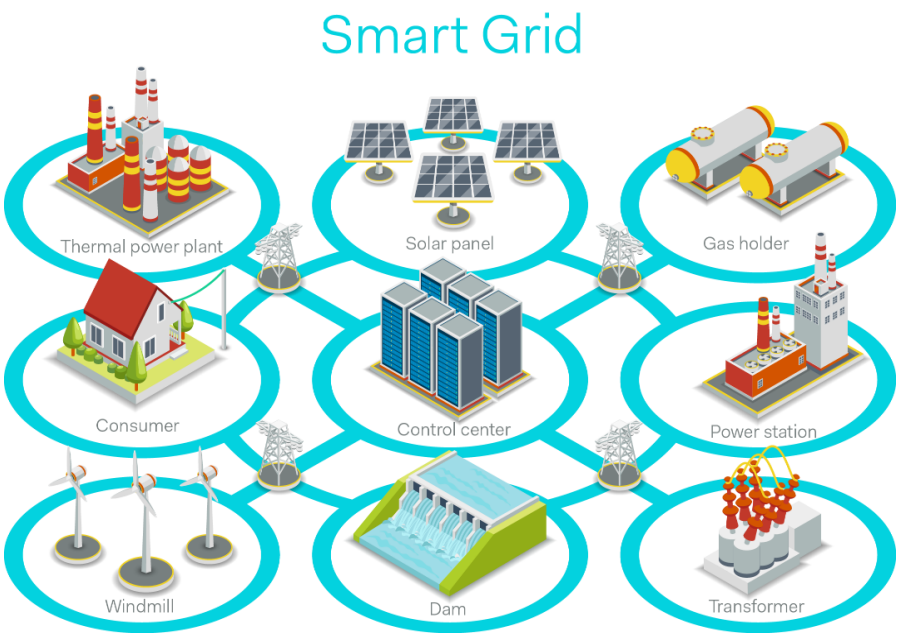
→From simple to complex attacks

→Securing the Smart Grid

→Conclusions

→Happy to answer your questions

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 are increasing interfaces

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

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

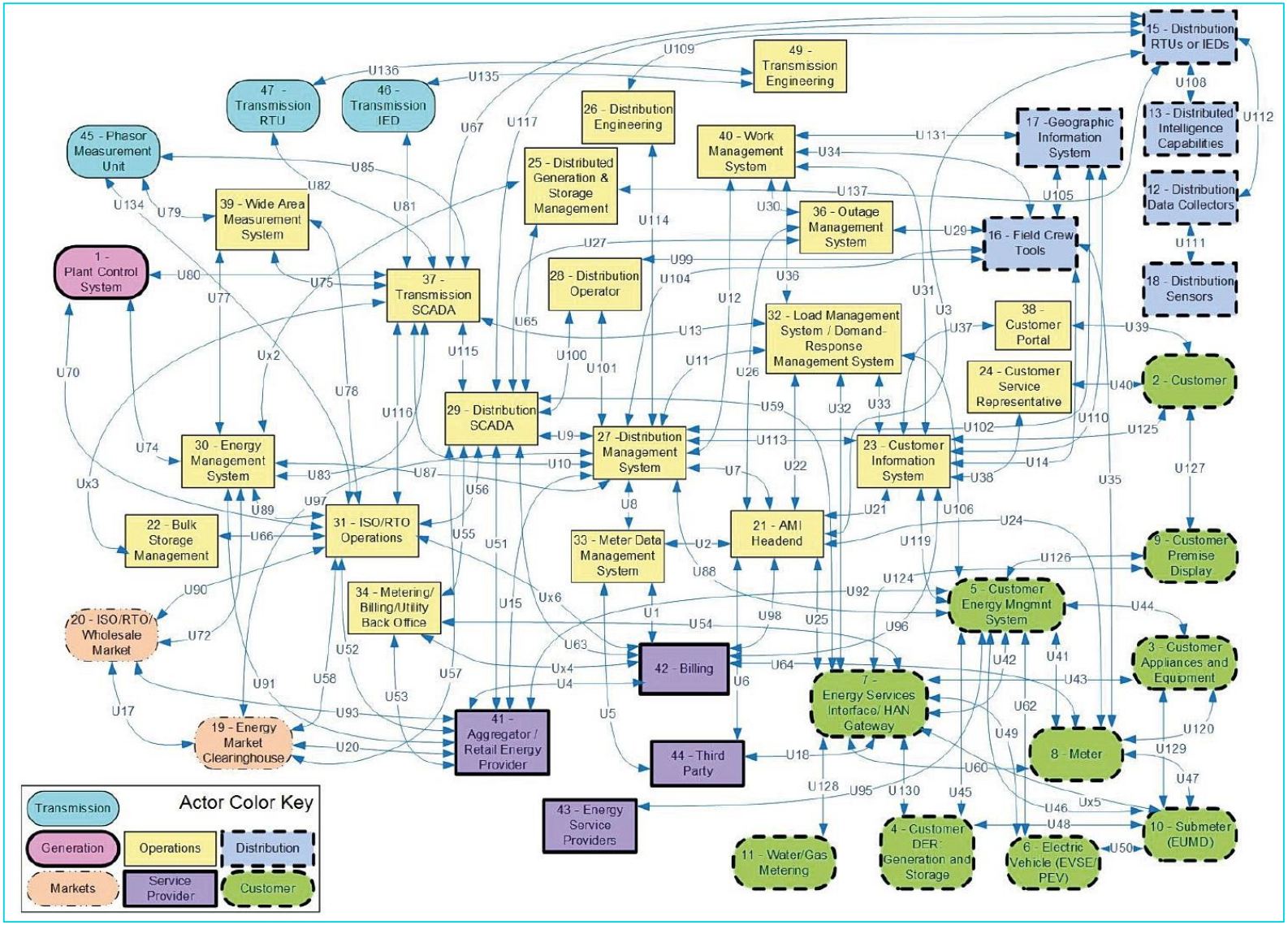
→Smart metering and better control of energy distribution and consumption

→Flexibility

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

Source: Institute for Energy Research (IER)

Powerbox – Smart Grid Security
Then arrived the Smart Grid…



Source: NIST workshop on Smart Grids complexity Supervisory Control & Data Acquisition (SCADA) used to access

Powerbox – Smart Grid Security
The Threats

→Hackers & Crackers

→Computer Criminals

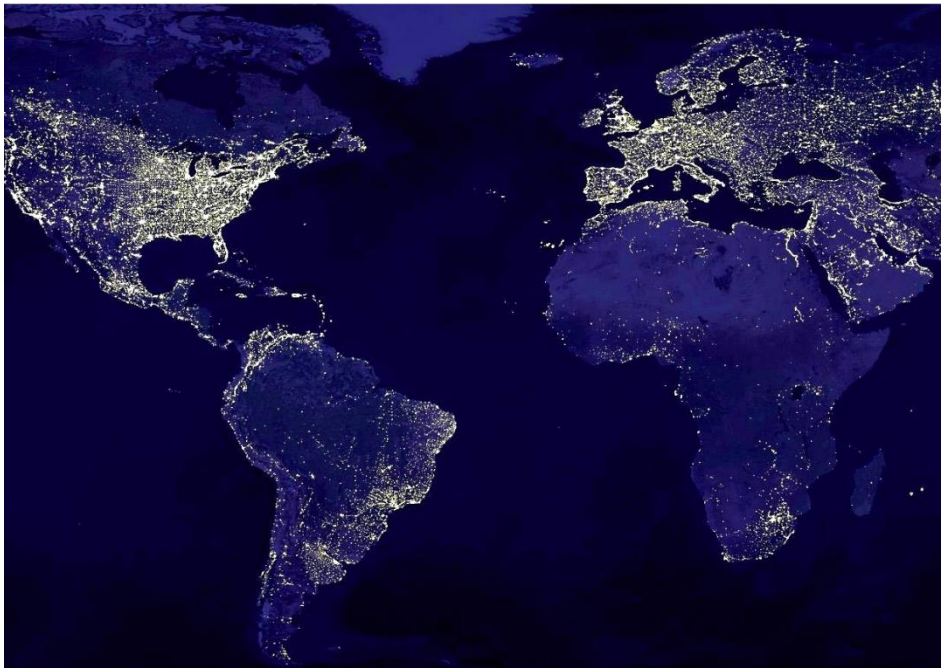
→Terrorism

→Cyberwar

→Industrial Espionage

→Insiders

Powerbox – Smart Grid Security
The Consequences



→Population

→Reputational

→Infrastructures

→Regulatory

→Equipment

→Data protection and privacy

→Safety

→Economic

The real life…

Powerbox – Smart Grid Security
At start was the AURORA

→March 4, 2007 The Aurora project

- Idaho National Lab. accessed a generator
- Supervisory Control & Data Acquisition (SCADA) used to access
- 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

→Aurora opened the Pandora Box

Powerbox – Smart Grid Security
From simple to complex attacks

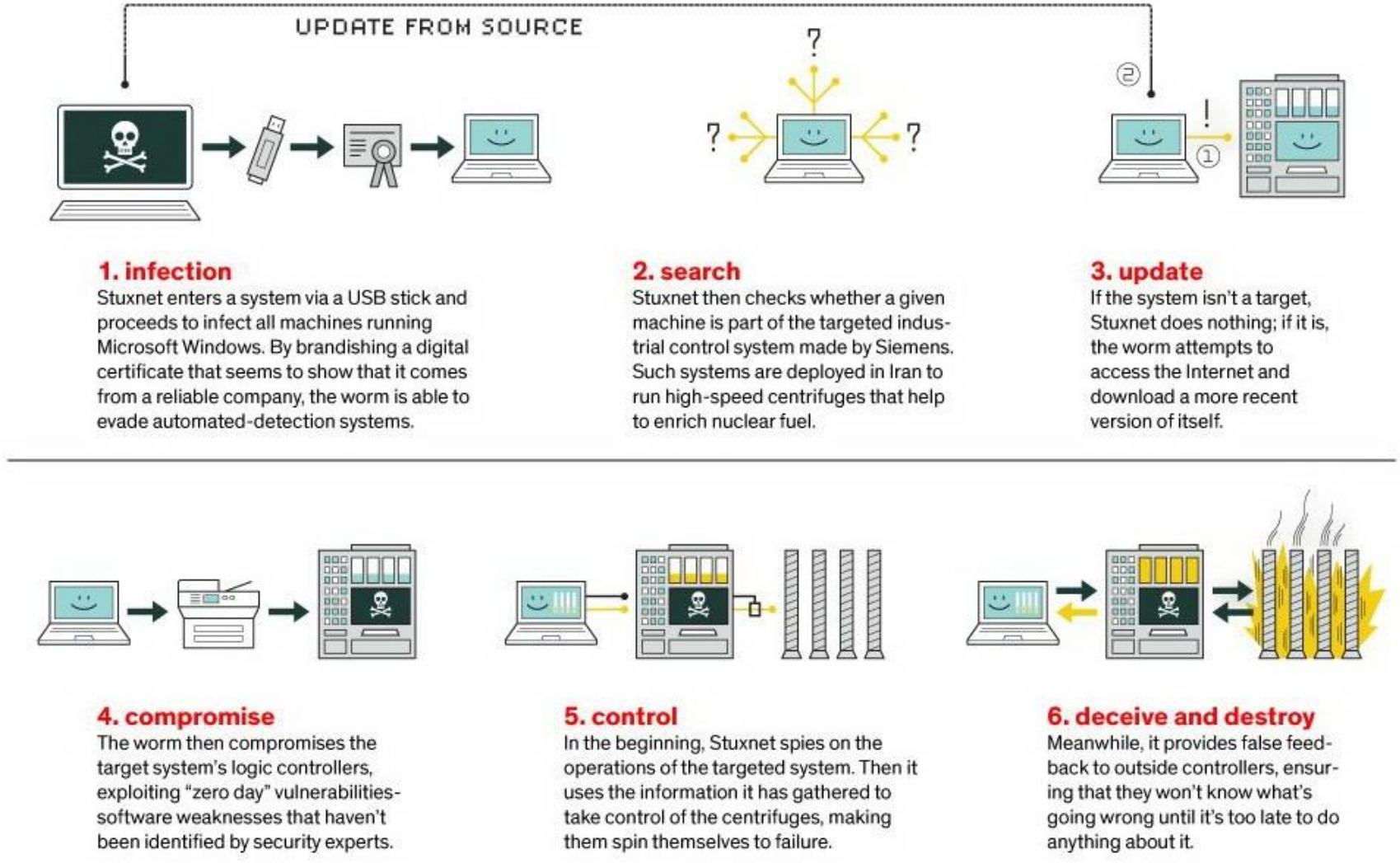
→April 2007

- 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

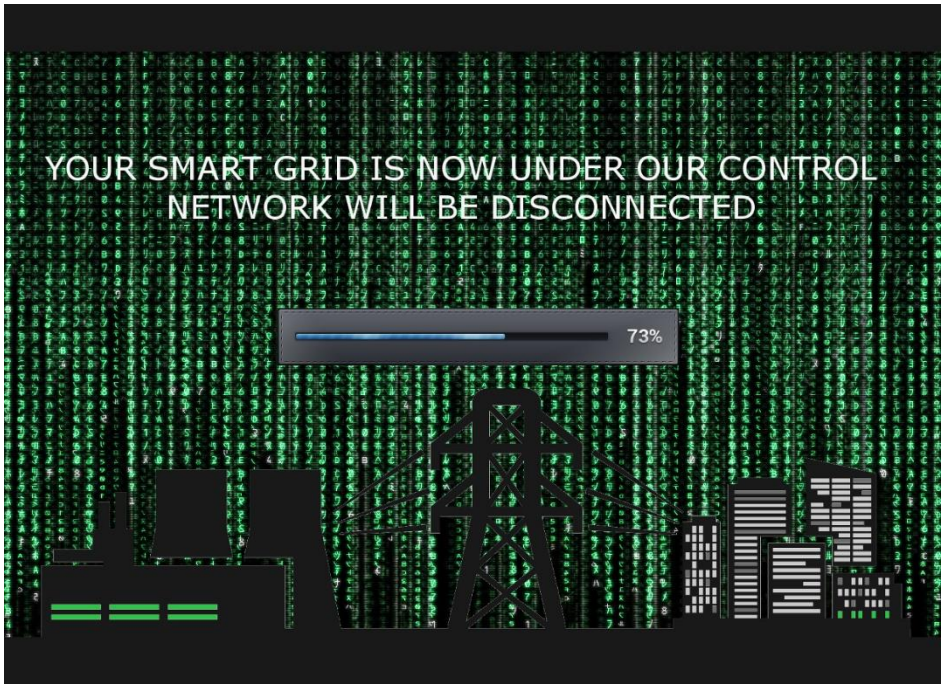
- Mutant of the Stuxnet worm propagated through SCADA
- Suspected to be the first attack from another government not involving military action

Powerbox – Smart Grid Security
From simple to complex attacks



Source: L-Dopa

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 to November 2016

→September 2016 – OVH (France)

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

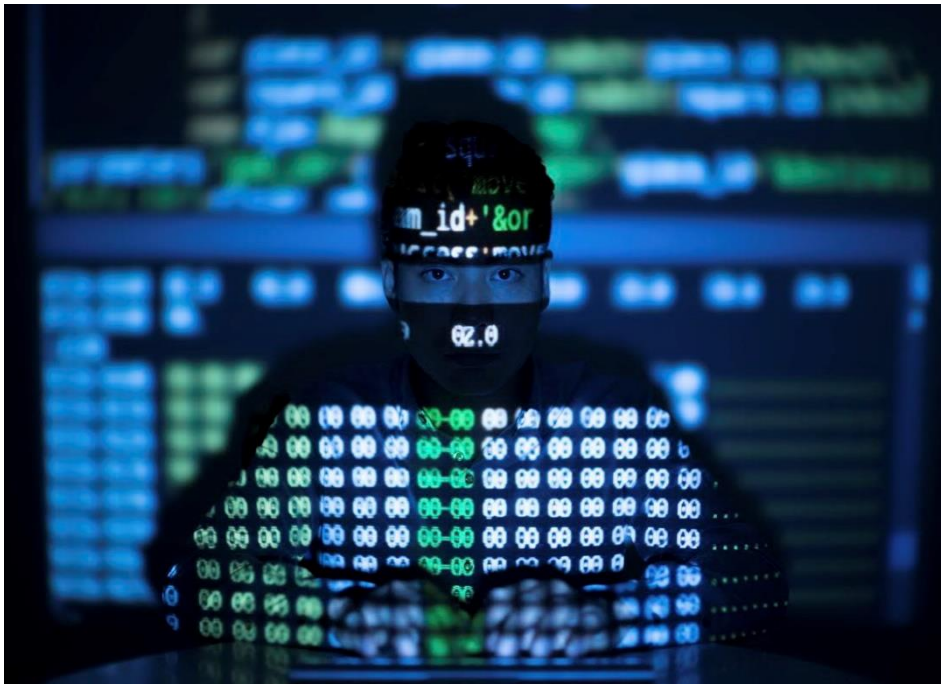
→October 2016 – Dyn (USA)

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

→November 2016 – Deutsche Telekom

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

Powerbox – Smart Grid Security
How severe is the threat?



→Silence is GOLD

→In 2015/6 more than 800 cyber incidents estimated in USA

→Similar number in Europe with collateral effects

→Ransomware exposure increasing

→Ukrainian case could easily be duplicated

→IoT accelerating the level of risks

Powerbox – Smart Grid Security
Securing the Smart Grid

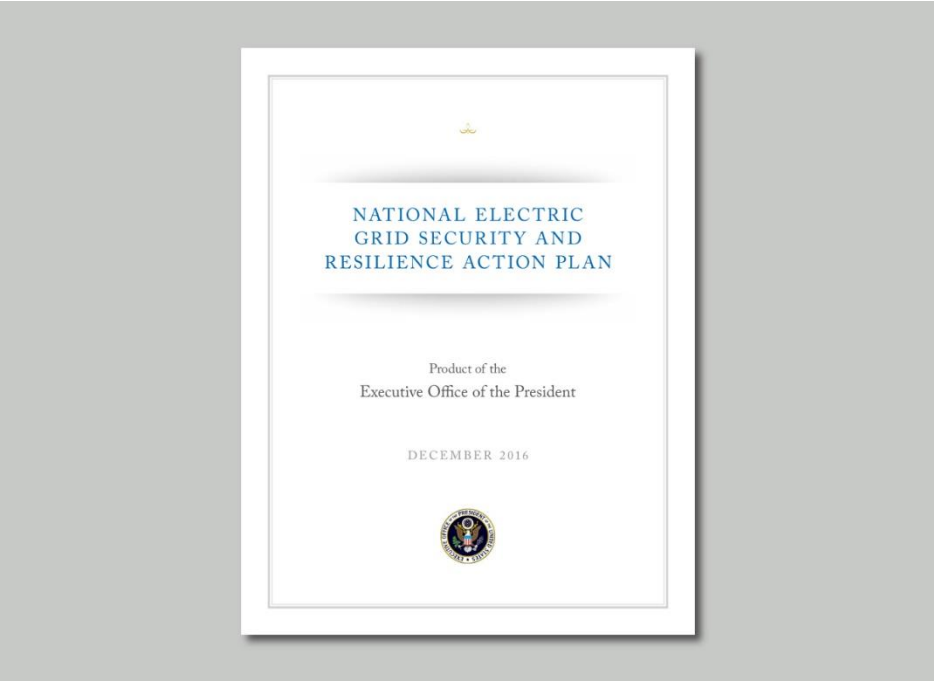
→ The US Department Of Energy (DOE) released a number of projects and initiatives, as well other governmental agencies

→ 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
Conclusion



“A robust, secure, and resilient electric grid is essential to serving the needs of the public in terms of health and safety, economic security, and national security. A physical incident, cyber incident, or natural event affecting the electric grid can be potentially catastrophic for our way of life. A security mechanism that works today may not be effective tomorrow—the ways and means of threats and hazards constantly change, whether by design of a cyber incident or through unpredicted climate trends. Electric grid stakeholders must prepare for disruptive events and continue to work to address the potential threats, hazards, and vulnerabilities in the systems they manage.”

P R

B X

POWERBOX
Mastering Power

Thank you !
Merci !
Tack !

Appendix

Powerbox – Smart Grid Security
The Threats

P R
B X

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

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

Powerbox – Smart Grid Security
Smart Grid related security guidelines

Organization	Reference
NIST	Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82 Rev 2, February 2015. Guidelines for Smart Grid Security, NISTIR 7628 Rev 1, September 2014.
ISO	Information technology – Security techniques - Information security risk management, ISO/IEC 2nd Edition, June 2011.
CESG	HMG IA Standard No. 1, Technical Risk Assessment, Issue: 3.51, October 2009. Security for Industrial Control Systems, Manage Vulnerabilities, a Good Practice Guide, CESG, Ver. 1, 2015.
CNPI	Cyber Security Assessments of Industrial Control Systems Good Practice Guide, DHS CPNI, November 2010.
ENISA	Protecting Industrial Control Systems Recommendations for Europe and Member States, ENISA, December 2011.
DHS	Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, DHS, October 2009
Council of Internet Security	The Critical Security Controls for Effective Cyber Defense Version 5.1
ISA/IEC	ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security
CEN-CENELEC ETSI	CEN-CENELEC-ETSI Smart Grid Coordination Group — Smart Grid Information Security, 2014
IEC	IEC 62351 standard for addressing security issues of the IEC TC57 series of standards, e.g., IEC 61850.

Powerbox – Smart Grid Security
Securing the Smart Grid (DOE)

Roadmap to Achieve Energy Delivery Systems Cybersecurity	
Build a Culture of Security	Through extensive training, education, and communication, cybersecurity “best practices” are encouraged to be reflexive and expected among all stakeholders.
Assess and Monitor Risk.	Develop tools to assist stakeholders in assessing their security posture to enable them to accelerate their ability to mitigate potential risks.
Develop and Implement New Protective Measures to Reduce Risk	Through rigorous research, development, and testing, system vulnerabilities are revealed and mitigation options are identified which has led to hardened control systems.
Manage Incidents	Facilitate tools for stakeholders to improve cyber intrusion detection, remediation, recovery, and restoration capabilities.
Sustain Security Improvements.	Through active partnerships, stakeholders are engaged and collaborative efforts and critical security information sharing is occurring.

“A key mission of the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) is to enhance the reliability and resilience of the nation's energy infrastructure. Cybersecurity of energy delivery systems is critical for protecting the energy infrastructure and the integral function that it serves in our lives. OE designed the Cybersecurity for Energy Delivery Systems (CEDS)”

Powerbox – Smart Grid Security
Cybersecurity for Energy Delivery Systems (CEDS)”

ADDSec	The Artificial Diversity and Defense Security (ADDSec) project will develop solutions to introduce unpredictability and enhance situational awareness to energy delivery control systems, protecting them against cyber attack. The project will leverage software defined networking (SDN) to introduce randomness to control system networks and extend solutions from the local network area to the WAN.
Alliance	The Alliance project is developing a proximity card reader and controller that allows physical and cybersecurity access to be monitored, tracked, and controlled using a single system. The reader and controller consist of four easy-to-deploy components: an access terminal, an access control processor, enhanced firmware for the SEL-3620 and SEL-3622 security gateways, and a card enrollment solution
ARMORE	The Applied Resiliency for More Trustworthy Grid Operation (ARMORE) project will provide reliable, secure communications, augmented defense-in-depth security, and an analysis framework to enable faster and more secure ways to transfer substation data from both legacy and modern devices. Similar to data encapsulation methods, placing ARMORE in line with the devices to be protected allows it to transparently provide enhanced security with the ability to report violations of stated policy.
CAPMS:	Security policies must be implemented as a part of grid control systems as well as the servers and networks that are part of traditional information technology (IT) security management. The Cyber-Intrusion Auto-Response Policy and Management System (CAPMS) project is unifying both worlds and applying advanced cybersecurity incident behavioral models to analyze, predict, offer advice and, where appropriate, act autonomously to sustain energy delivery systems during a cybersecurity incident.

Powerbox – Smart Grid Security
Cybersecurity for Energy Delivery Systems (CEDS)”

CODEF	The Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF) project is developing a distributed security domain layer that enables transmission and distribution grid protection and control devices to collaboratively defend against cyber attacks.
Cybersecurity Intrusion Detection and Security Monitoring	This project conducts research to accelerate development of a utility monitoring system to detect anomalous behavior, improve situation awareness, and provide visibility into wireless advanced metering infrastructure and distribution automation field area networks.
CYMSA	The Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA) project is developing a cybersecurity situational awareness technology suite to detect adversarial manipulation of power grid components and communications networks. The project involves novel cyber-physical modeling and simulation research on communications networks and substations.
Essence	The Energy Sector Security Appliances in a System for Intelligent Learning Network Configuration Management and Monitoring (Essence) project is developing tools that facilitate more secure operational network management. Software defined networking will provide a solution to assist small electric cooperatives with mapping their networks, analyzing traffic, and learning expected traffic flow to better inform human operators.

Powerbox – Smart Grid Security
Cybersecurity for Energy Delivery Systems (CEDS)”

Patch and Update Management Program for Energy Delivery Systems	This project will research, develop, and demonstrate technology and techniques to identify, verify the integrity of, and facilitate deployment of patches and updates for energy delivery system software, hardware, and firmware. The project comprises several elements that can each stand alone to improve security posture and, when integrated, can provide a comprehensive solution to meet energy sector patch and update needs.
Secure Policy-Based Configuration Framework	The Secure Policy-Based Configuration Framework (PBCONF) project is developing an extensible, open-source, policy-based configuration framework to support the secure configuration and remote access of modern and legacy devices from a variety of vendors.
Secure Software Defined Radio Project	The Secure Software-Defined Radio Project (SEL-3070) is developing a flexible platform for secure wireless communications to utility distribution automation devices, providing capabilities not offered in cellular, narrow-band licensed, or other unlicensed-band radios.
Software Defined Networking	The Software Defined Networking project is developing an energy sector flow controller to be used with the SEL-2740S substation hardened switch, developed through the Watchdog Project. The SDN project is using the open-source OpenDayLight project as the core flow controller, which will be interoperable with OPENFLOW™ protocol-enabled network appliances