ENEVO GROUP

Integrated Solutions for the Energy Value Chain

EVOLUTION OF THREATS TO ELECTRIC POWER GRID OPERATORS

#DEFCAMP8, BUCHAREST
9.11.2017

Power & Automation in brief

Engineering & Consulting

Substation Automation & Protection Systems

Process Control & Electrical Automation

IT, Telecom & Cyber Security

7

industries:

Power Generation, Power Transmission and Distribution, Water, Oil & Gas, Steel, Food & Beverages, Chemicals

4

offices:

Bucharest, Resita, Saudi Arabia (Al Jubail) and Australia (Melbourne)

40

Projects

on SCADA and control, for power generation, power T&D, steel and diary industries

50%

Of revenue

From international projects

3.500+

IEDs

integrated and monitored through our solutions

3

EMS-SCADA Dispatch Centers

Designed and implemented by ENVO Group

500.000+

Data collection points

aggregated

100+

Equipment providers

Integrated in ENEVO's dispatch and automation solutions

What is different

What is different?

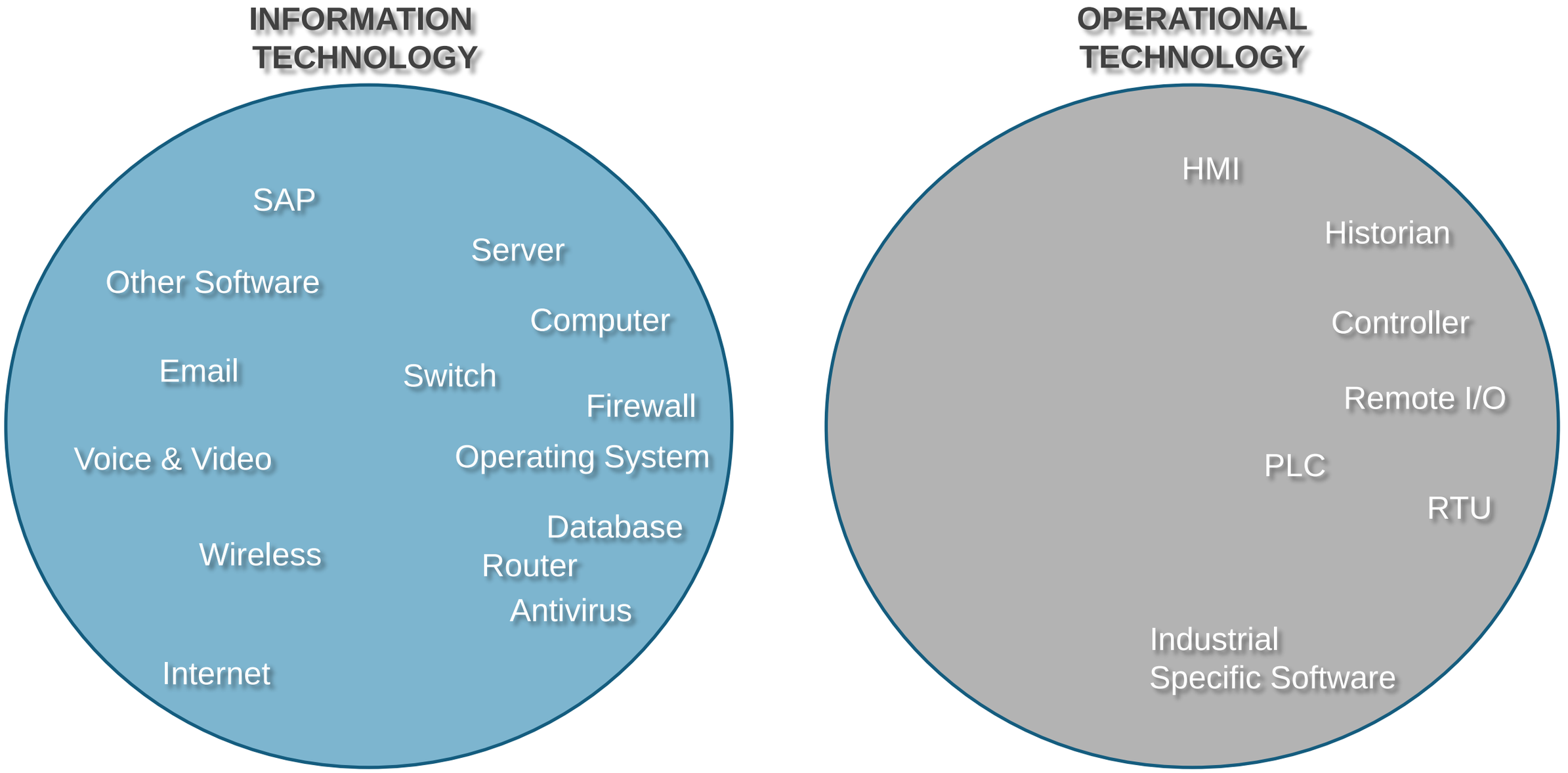
Corporate IT	Automation Systems IT
Not life threatening	Safety first
Availability important	Non-interruption is critical
Transactional orientation	Real-time focus
IBM, SAP, Oracle, …..	ABB, Emerson, GE, Honeywell, Siemens…
People ~= Devices	Few people; Many, many devices
PCs and Servers	Sensors, Controllers, Servers
Web services model is dominant	Polled automation control model
MS Windows is dominant OS	Vendor-embedded operating systems
Many commercial software products installed on each PC	Purpose-specific devices and application
Protocol is primarily HTTP/HTTPS over TCP/IP -- widely known	Many industrial protocols, some over TCP/IP – vendor and sector-specific
Office environment, plus mobile	Harsh operating plant environments
Cross-industry IT jargon	Industry sector-specific jargon
Cross-industry regulations (mostly)	Industry-specific regulations

What is different?

- 25 year lifespan
- Technological freeze
- As-built
- Shutdown periods
- AIC not CIA

Information Technology – Operational Technology Convergence, Opportunities and Challenges

IT – OT Convergence



Advantages of modern technology

- Standardized Hardware and Software
- Greater Interoperability through Standardization
- Cost Reduction
- Higher Availability
- Increased Speed
- Faster Deployment
- Easier Troubleshooting

Challenges

- Disrupting Innovation (IT) vs Predictable Stability (OT)
- Different Mindsets
- Knowledge gap in IT/OT environment
- Market Pressure
- Increased Complexity & Interdependencies
- Closed Systems
- Cybersecurity
  - IT: Confidentiality, Integrity, Availability
  - OT: Availability, Integrity, Confidentiality, Traceability

Key elements

Sensor & Command Elements

- Sensors measure various physical units and convert them to either analog or digital values
- Command Elements are the mechanism by which a control system acts upon an environment

PLC

- **Features**:
  - PLC: Programmable Logic Controller
  - Reads data from the field and sends it upstream for processing
  - Executes control logic

- **Cybersecurity**:
  - Limit data flows
  - Monitor network traffic
  - Disable unused services

RTU

- **Features**:
  - RTU: Remote Terminal Unit
  - Intermediary data storage
  - Protocol translation
  - Limited logic

- **Cybersecurity**:
  - Limit data flows
  - Monitor network traffic
  - Disable unused services

Process Servers, Historians & Computers

- **Features**:
  - Regular x86 server/computer running dedicated software
  - Uses “off-the shelf” OS & 3rd party applications
  - Used for long-time storage of data
  - Source for consolidated reporting
- **Cybersecurity**:
  - Advanced Anti-Virus software with correct configurations
  - Application White-Listing
  - Centralized policy and user management
  - Disable logical and physical access
  - Disable administrative rights (when possible)
  - Disable unused OS services

HMI – Human to Machine Interface

- Dedicated Software
- Overview of industrial process
- Visualization and alarming
- In-memory database

Switches

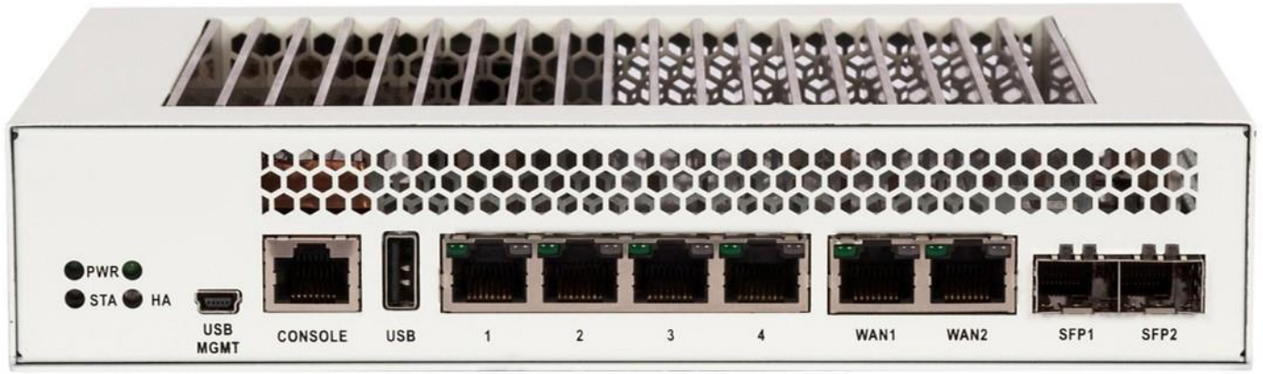
- **Features:**
  - Network access and aggregation
  - First security barrier
  - First level of redundancy
  - First level for QoS
- **Cybersecurity:**
  - Shutdown unused ports
  - Blackhole VLAN
  - Port security
  - ARP inspection
  - Control Plane security
  - Authenticated (and encrypted) control plane protocols
  - Local and remote port mirroring

Routers

- Features:
  - Encrypted transport between remote locations
  - Redundancy between remote locations
- Cybersecurity:
  - Shutdown unused ports
  - Blackhole VLAN
  - Port security
  - ARP inspection
  - Control Plane security
  - Authenticated (and encrypted) control plane protocols

Firewalls

- Roles:
  - Network segmentation
  - Enforcing communication flows
  - In-line or passive network monitoring
  - Industrial protocols inspection
- MUST HAVE:
  - UTM, not L4
  - SCADA protocols filtering, including commands
  - Restrictive traffic flows
  - IDS/IPS “near” data path
  - Log all network traffic



Protocols

Modbus:

- Developed by Modicon (now Scheider Electric)
- Serial or TCP
- Authentication based on Layer 3 (Network)
- Master-Slave
- Address approach

DNP3:

- US Standard
- Serial or TCP
- Timestamps
- Event driven
- Server-Client
- Unsolicited messages

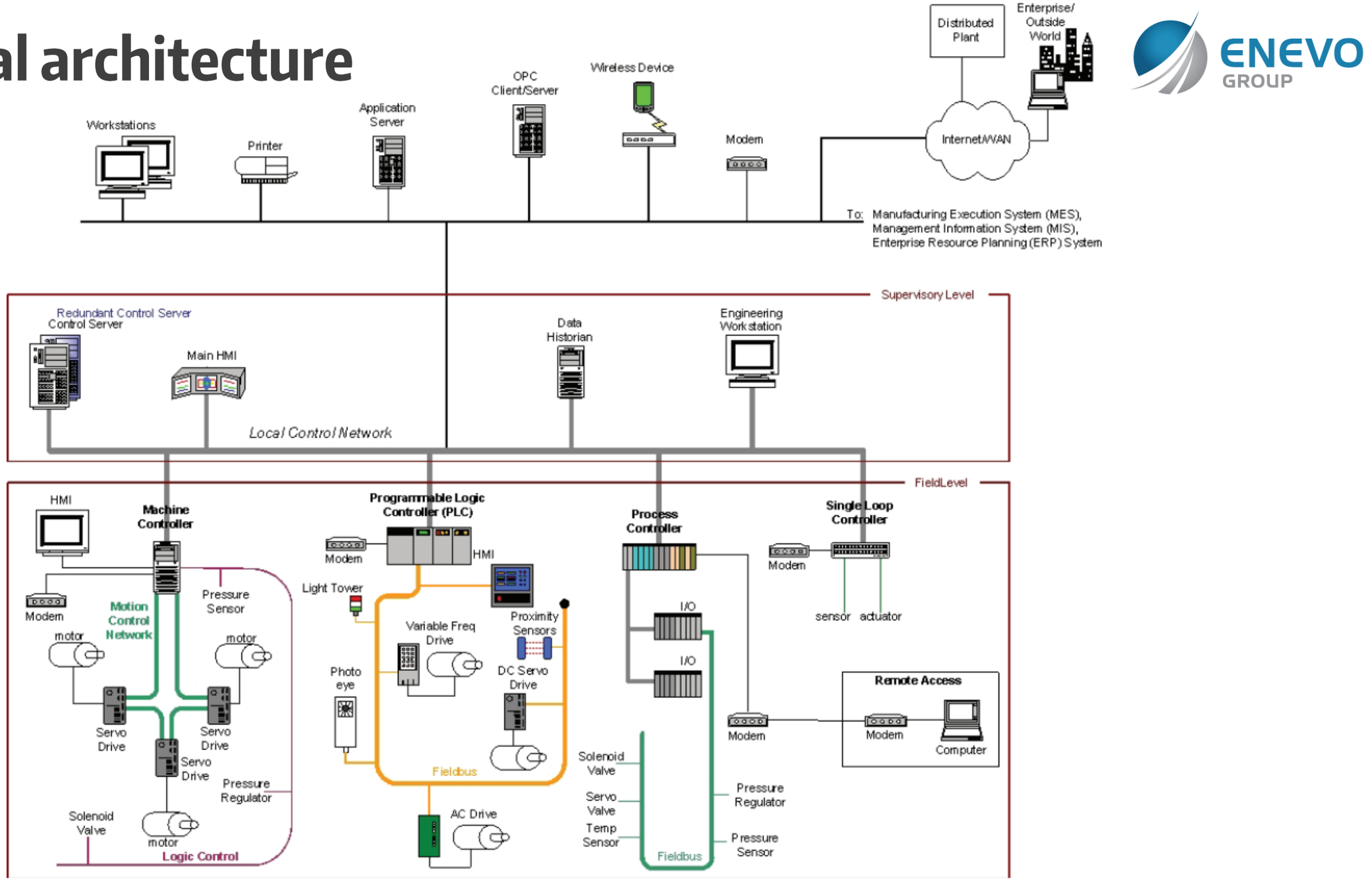
IEC-101/104:

- European Standard
- IEC-101 over Serial
- IEC-104 over TCP

IEC-61850:

- European standard
- Used more often in substation environments
- Object approach

Typical architecture



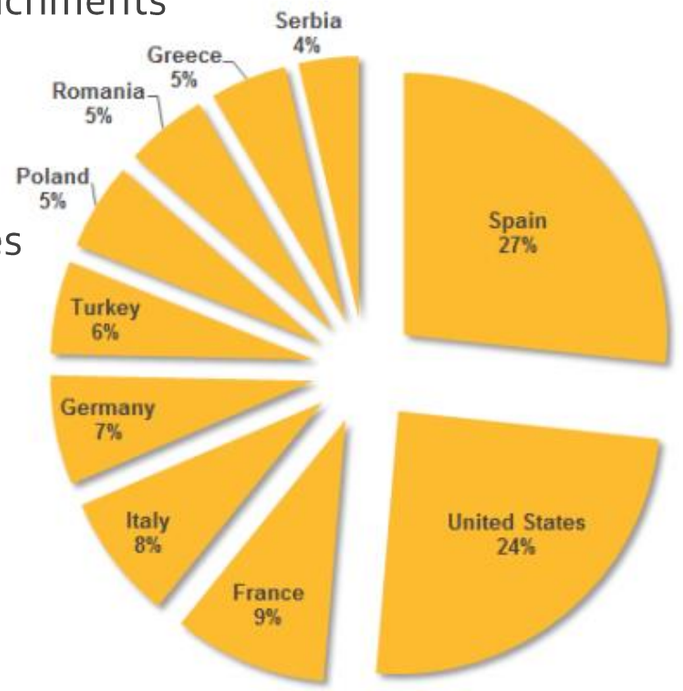
Threat Evolution

Case 1: Stuxnet - 2010

- Where: Iran
- Target system:
  - Natanz Uranium Enrichment Facility
  - Siemens S7-315 CPU with 6 CP-342-2 modules connected to 31 Vacon or Fararo Paya frequency converters per module
- Attack vector: infected USB key from one of the 5 subcontractors involved in Industrial processing
- Impact: IAEA (International Atomic Energy Agency) reported 1000 centrifuges withdrawn from service
- Key facts:
  - first confirmed example of ICS tailored malware
  - detailed understanding of the industrial process
  - **no direct access to the facility (isolated network)**
  - infect organizations that interact with target (pivoting attack)
  - modifies and hides code on Siemens PLCs

Case 2: Dragonfly/HAVEX - 2013

- Where: U.S. and Europe
- Target system:
  - power grid and petrochemical asset owners
  - devices on TCP ports 44818 (Omron, Rockwell Automation), 102 (Siemens) and 502 (Schneider Electric)
- Attack vector: vendor websites and spear phishing in the form of e-mails with PDF attachments
- Impact: > 2,000 sites (1,000 energy companies in 84 countries)
- Key facts:
  - leveraged legitimate functionality in the OPC protocol to map out industrial devices
  - no physical disruption or destruction of the industrial process



Case 3: Sandworm/Blackenergy 2 - 2014

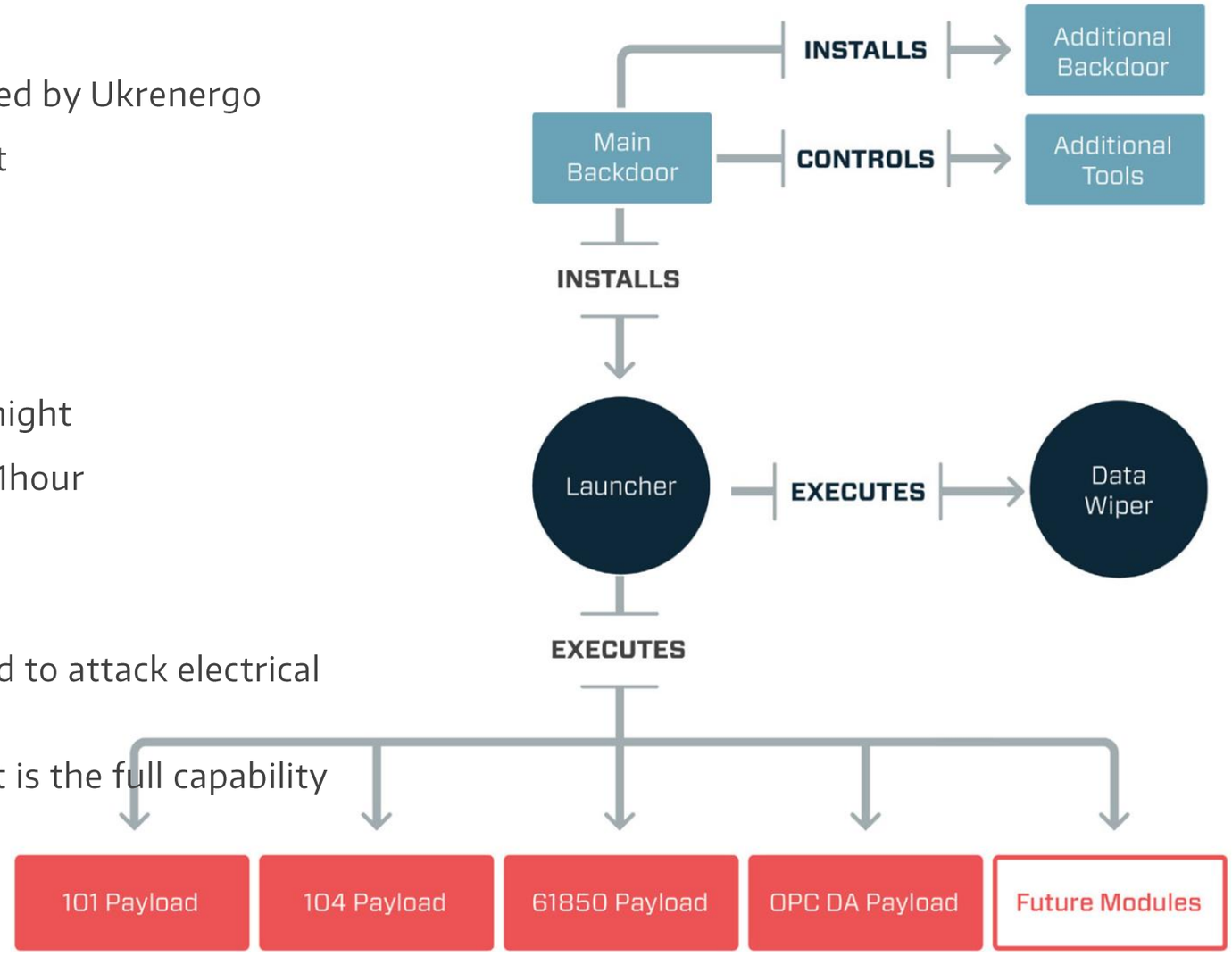
- Where: U.S. and Europe
- Target system:
  - power generation site owners / operators
  - large suppliers and manufacturers of heavy power related materials
  - HMI applications including:
    - Siemens SIMATIC WinCC (V7.0, V7.2, V7.3) PCS 7 (V7.1, V8.0, V8.1), TIA Portal V13
    - GE CIMPLICITY Version 8.2 with SIM 23 and prior
    - Advantech WebAccess
- Attack vector: phishing campaign/ known or 0-day vulnerability in Microsoft Windows
- Impact: multiple systems of NATO, European Union, and energy sectors
- Key facts:
  - Advanced Persistent Threat Toolkit to develop modular malware;
  - capabilities to attack ARM and MIPS platforms, scripts for Cisco network devices, destructive plugins, certificate stealer and more

Case 4: Blackenergy 3 - 2015

- Where: Ukraine
- Target system: 3 regional distribution power companies
- Attack vector: spear-phishing
- Impact:
  - **7 x 110 kV** and **23 x 35 kV substations disconnected** from the grid
  - **225,000+ customers** without power for **~6 hours**
- Key facts:
  - first known instance where a cyber-attack had disrupted electric grid operations
  - destruction of serial-to-Ethernet devices through malicious firmware updates
  - lost the ability for automated control, for upwards of a year in some locations
  - leveraged the grids systems against itself

Case 5: Crashoverride - 2016

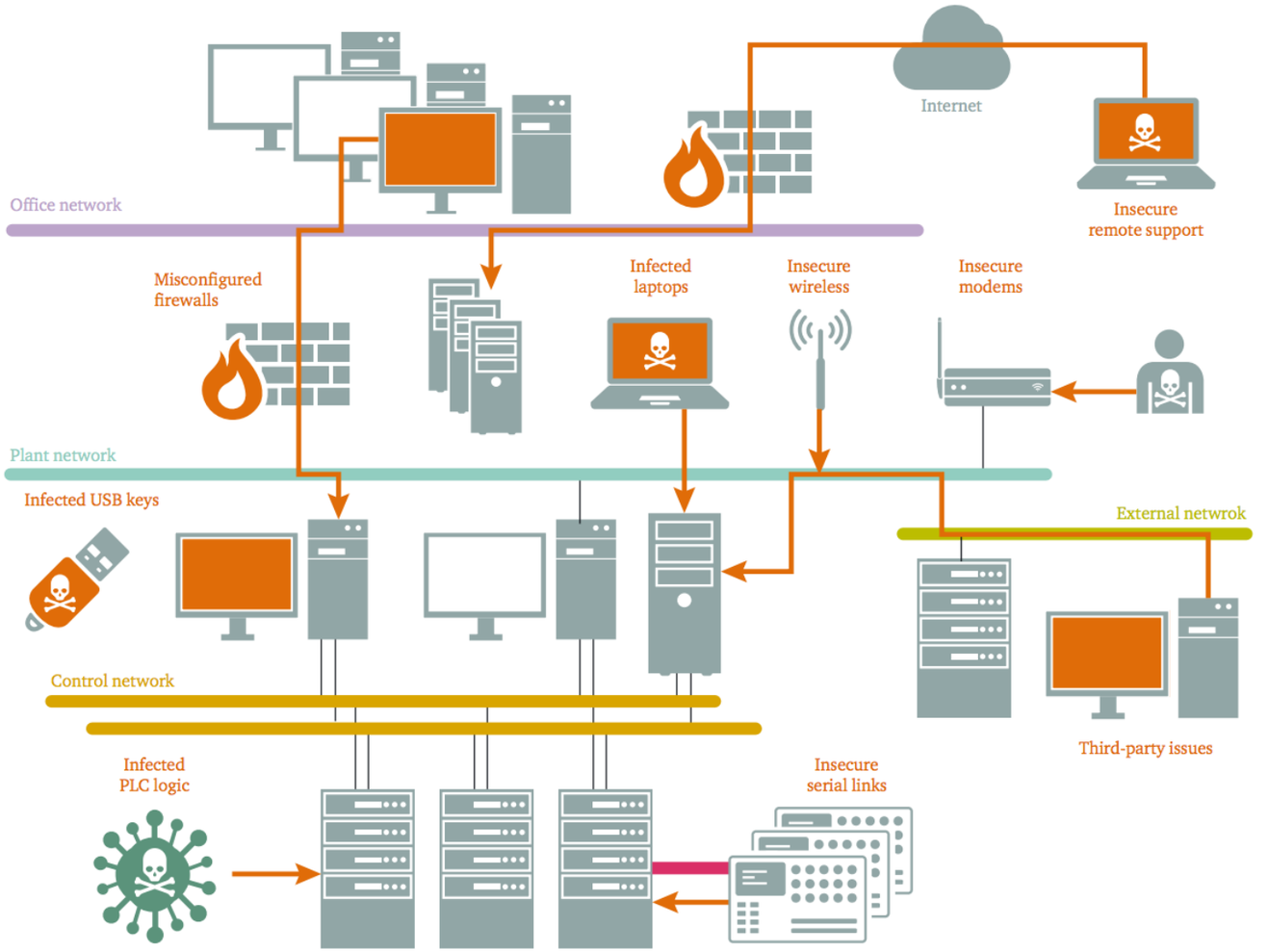
- Where: Ukraine
- Target system:
  - 330 kW transmission substation in Kiev owned by Ukrenergo
  - Siemens SIPROTEC 4 and SIPROTEC Compact
- Attack vector: unknown for now
- Impact:
  - 200 MW of capacity
  - ~1/5 of the capital's energy consumption at night
  - black out a portion of Ukrainian capital for ~1hour
- Key facts:
  - modular framework dedicated for ICS
  - first ever known malware specifically designed to attack electrical grids
  - appears more of a proof of concept than what is the full capability of the malware



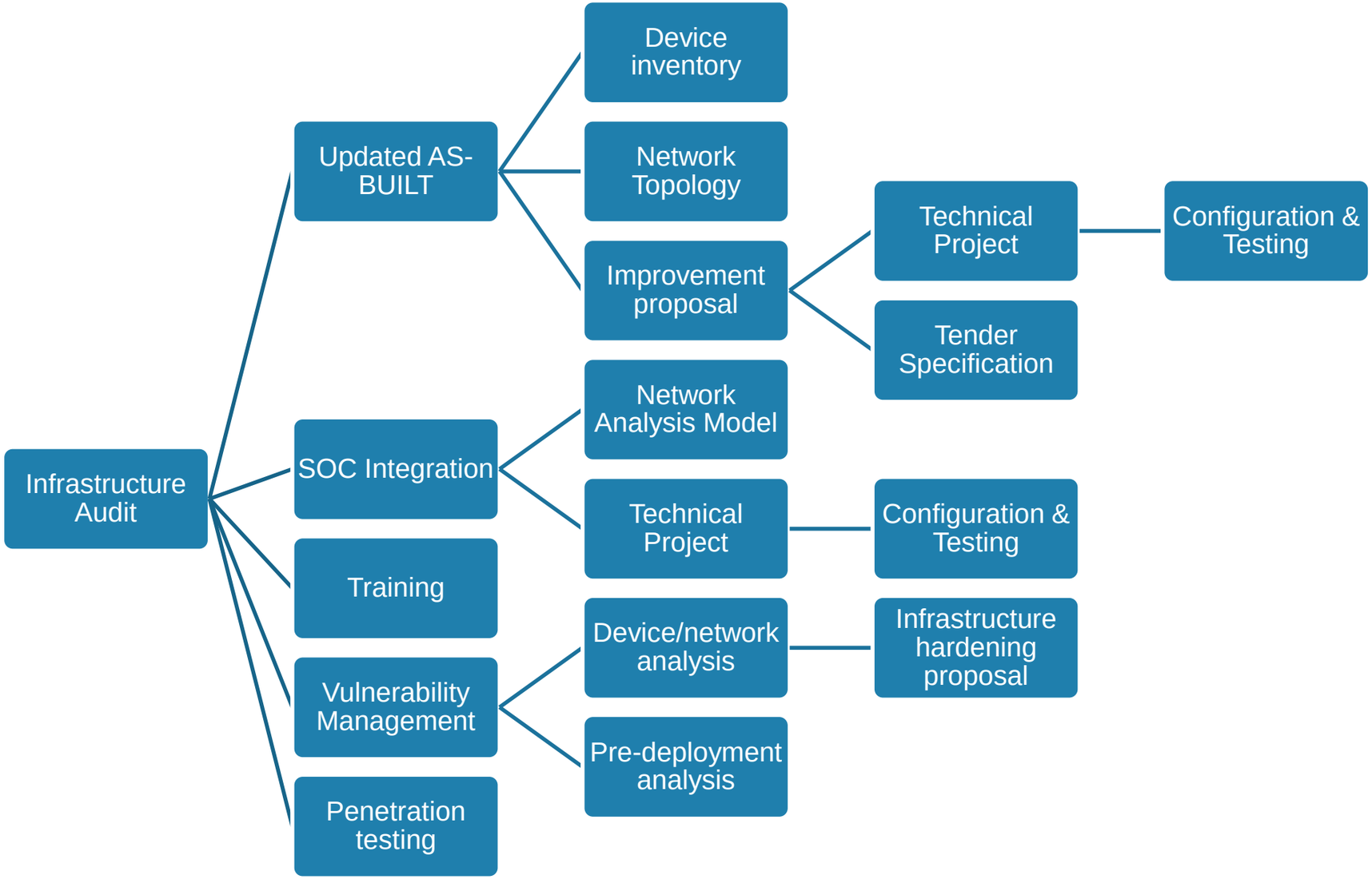
Where are we now and what to do

Weaknesses and Gaps - Vulnerabilities

- Lack of awareness and training among employees
- Lack of proper network segmentation
- Lack of network access control
- IT firewalls, not OT firewalls
- Blurry lines between IT and OT boundary
- Default accounts and/or generic accounts
- Legacy and/or unpatched systems
- Challenges in infrastructure update/upgrade
- Lack of visibility



Securing IT&OT: Step-by-step



Improvement proposal – IT & OT

ENEVO GROUP

IED	Process Server & Computer	Switches, Routers	Firewall	Insight
• **Monitor and restrict network traffic** • **Disable unused SCADA protocols** • Manage administrative access • Configure logging	• **Advanced Anti-Virus software with correct configuration** • Application Inventory • Application Whitelisting • Establish running processes baseline • **Centralized policy and user management** • Manage logical and physical access • Manage Administrative Rights • Disable unused services	• **Shutdown unused ports** • Blackhole VLAN • **Port security** • ARP inspection • Control Plane security • Limit MAC flows • Local and remote port mirroring	• UTM, not L4 • **SCADA protocols filtering, including commands** • Restrictive traffic flows using least privilege principle • **IDS/IPS "near" data path** • Log all network traffic	• Define log sources and information types • **Intercept, store and analyze network traffic** • Store all logs • Correlate all information using SIEM software • Consider non IT/OT information sources

Industrial cybersecurity – our vision

- **Security is a mindset, not a magic wand!**
  - Physical
  - Architecture
  - Hardware
  - Software
  - Insight
  - Operational & Procedural

Education

Education is important

(*) ENISA - European Union Agency for Network and Information Security

Thank you for your attention!

Romania Office

Address: 16 Negustori Street
Bucharest, Romania
Phone: +40 371 017 242
Fax: +40 372 258 353
Email: romania@enevogroup.com

Saudi Arabia Office

Address: Al Jubail 31961, Support
Industrial Zone,
Kingdom of Saudi Arabia
Phone: +966 013-3408324
Fax: +966 013-3408322
Email: ksa@enevogroup.com

Australia Office

Address: Level 2, 172-192 Flinders
Street, Melbourne, Australia
Phone: +61 414 384 430
Email: australia@enevogroup.com

www.enevogroup.com