SECONOMICS 5/11/14

Cyber Security and Critical Asset Protection

David Willacy

entsoe

Reliable Sustainable Connected

Background

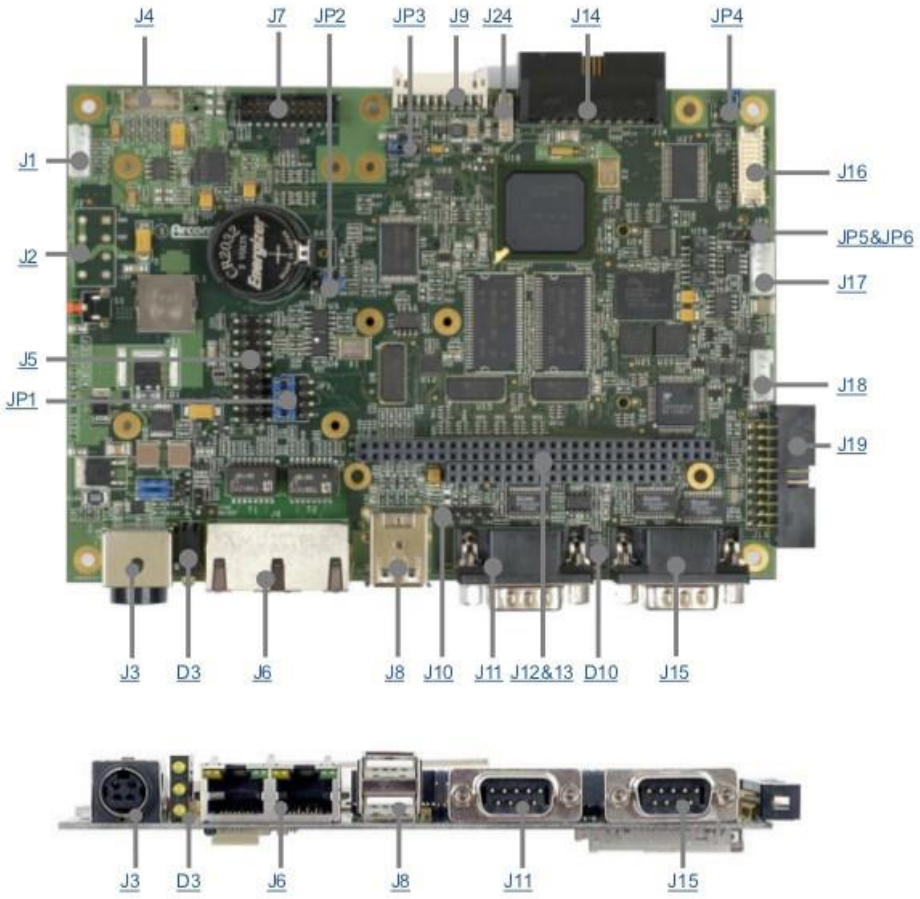
- Historically operational assets such as breakers were mechanically operated, this evolved to become electromechanical operation monitored by specialist Operational Technology (OT) systems.
- Operational technologies have evolved and are now based upon the same standard Information Technology (IT) as we have in the office and home such as Microsoft Windows.
- This convergence of distinctly different operating environments (OT IT) has fundamentally changed the risk landscape.

What the heck has cyber security got to do with Electricity ?

- The level of exploitation of IT within the Energy sector as a whole will continue to grow, driven by initiatives such as SMART grid, smart metering, Enterprise Asset Management, Advanced Network Control Systems and Complex Event Processing.

The key question is how to deal with lifecycle management and security for IT in the engineering environment…

Example Modern Remote Telemetry Unit



J1 Touchscreen controller
J2 Power (5V DC)
J3 Power (10-30V DC)
J4 Audio
J5 JTAG
J6 10/100BaseTX Ethernet
J7 GPIO
J8 Dual USB host
J9 Camera interface
J10 USB client
J11 Serial port – COM1
J12 64-way PC/104 expansion
J13 40-way PC/104 expansion
J14 LCD panel interface
J15 Serial port – COM2
J16 LCD panel LVDS interface
J17 CAN bus
J18 Serial port (RS422/485)
J19 Serial ports (COM3/4)
J20 CF+ interface
J21 IEEE802.15.4 / ZigBee
J22 SDIO
J23 Wireless interface
J24 Backlight power .

Changing world

- Recently a pilotless passenger plane flew over Britain, the aviation industry is predicting pilotless aviation as a commercial reality in the next few years. They state that human error is the main risk, so why not take the human out of the equation, this can also hold true for the key control systems in the electricity network
- It used to be possible to run electricity networks manually by manning sites and sending the key data by phone. In many transmission networks this is no longer the case
- As we put more and more intelligence into the assets that we use to run our critical systems like power, we have to manage the increased risk of accidental or malicious failure
- So what are the key risks to those assets?

Embedded Vulnerabilities

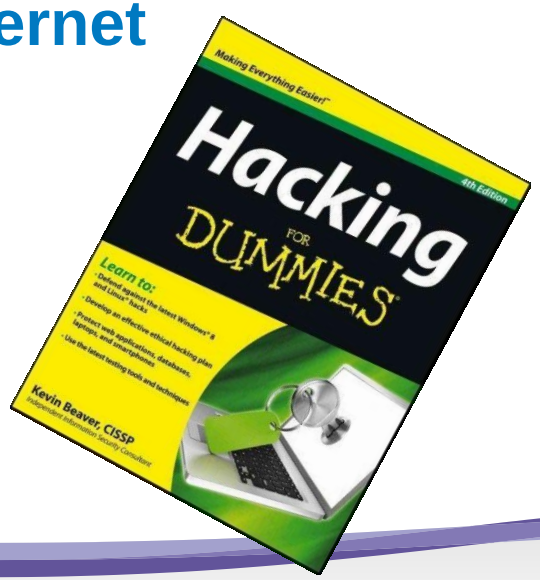
- There is a risk that due to the lack of security awareness when purchasing, upgrading and deploying IT and OT assets into energy companies that vulnerabilities and malware are introduced.
- Consequences if risk materialises – Loss of key systems supporting electricity delivery; impairing and impacting the ability to manage electricity networks

Acquiring embedded risk through uninformed procurement.

Widely Available Vulnerability Data

- There is a risk that information about the technology widely used across the electricity sector and how to affect its operation is now widely available on the internet.
- Consequences if risk materialises – Loss of key systems supporting electricity delivery; impairing and impacting the ability to manage electricity networks

Information about how to hack proprietary insecure protocols like Modbus is available on the internet



Inappropriate Lifecycle Management

- No appropriate IT asset management strategy or process:-
- IT assets do not have a thirty year lifespan, this needs to be factored into both depreciation and investment planning
- No patching no anti malware protection
- Little understanding of the threats
- No defined / managed secure perimeter, the increasing use of wireless / remote IT technology
- Little coordination between corporate IT managed systems and business managed systems
- Consequences if risk materialises – Loss of key systems supporting electricity delivery; impairing and impacting the ability to manage electricity networks

Millions is spent protecting corporate IT, but little on the operational technology that is critical to running key operational systems

Shared Threats

- There is an increasing risk of system failure due to the increased threat level evidenced by events within the energy sector, the level of sophistication is increasing on a daily basis with new malware targeting both OT and IT.
- Consequences if risk materialises – Loss of key systems supporting electricity delivery; impairing and impacting the ability to manage electricity networks

Thousands of variants of viruses are made daily, one day a virus will have the right DNA to damage key energy assets unless they are protected

Increased connectivity

- Increasing connectivity and accessibility provides more and more points of access into the energy sector. Electricity networks are no longer stand alone but are connected to many other systems, companies and networks.
- Consequences if risk materialises – Loss of key systems supporting national Grid operations that could significantly impair and impact our ability to manage our networks.

We are opening more doors than we are closing

Interdependence

Electricity transmission is dependant on many other sectors like generation, distribution and even telecoms

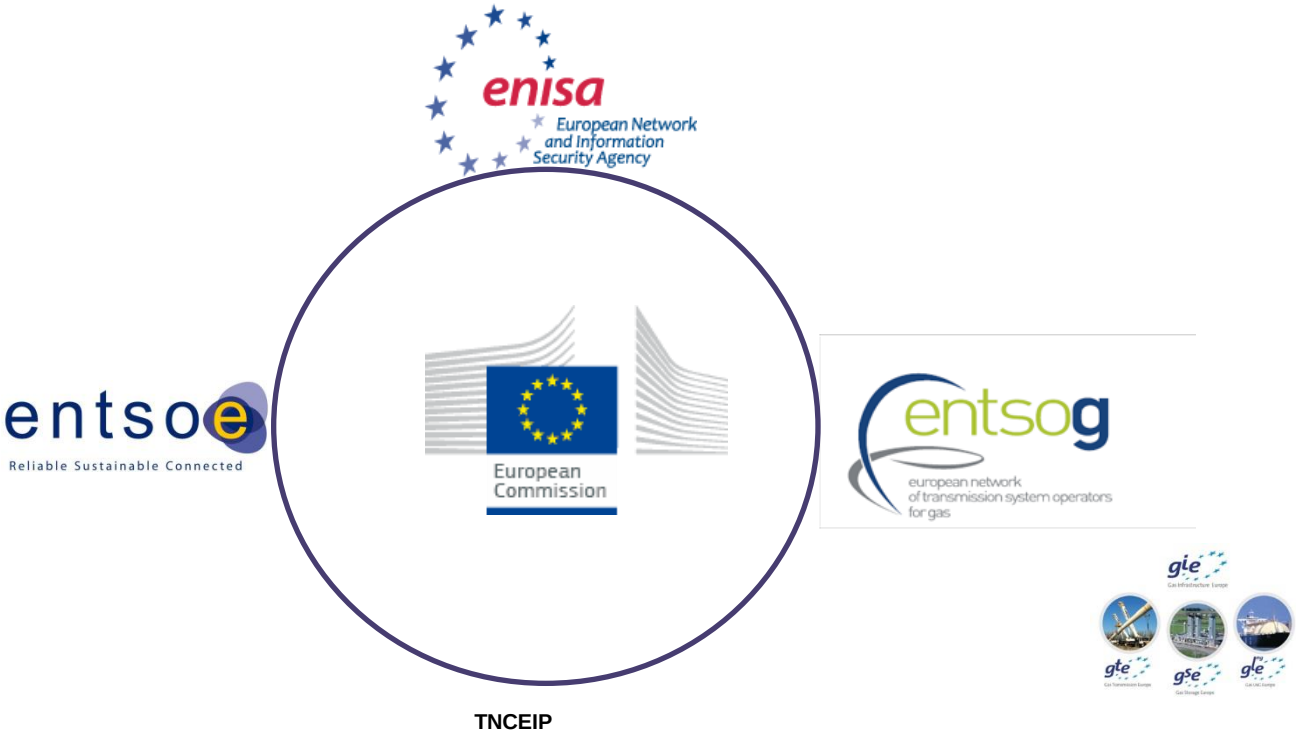
All other CNI sectors have a dependency upon electricity in one way or another

These interdependencies need to be mapped to ensure the associated risks are managed. Iterative risk assessments are one of the most powerful tools, if done well, to drive an on-going security strategy and program

So what are we doing?

- ENTSOE has a number of groups that are working to protect the critical assets of the electricity transmission networks
    - Critical Systems Protection (CSP)
    - Electronic Highway Working Group (EHWG)
    - Cyber Security Special Interest Group (CSSIG)

EUROPEAN ENERGY SECTOR CYBER SECURITY
KEY STAKEHOLDERS



TNCEIP

How can we protect critical cyber assets?

A lot of the legacy systems are hard to protect so what can we do!

- Understand the Business Risk
- Understand the Vulnerabilities
- Establish ongoing Governance
- Implementing Secure Architecture
  - Perimeter Defence
  - Malware Protection
  - Manage Physical security
- Improve Awareness and Skills
- Establish Response Capabilities
- Manage Third Party Risk
- Engage Projects
- Procurement

Conclusion

- A lot of work is being carried out to protect key energy cyber assets however more could be done. The energy sector is evolving at a rapid rate renewable generation is adding to the need for ever smarter systems. The dependence of the energy sector upon standard IT is growing as is the threat level.
- The growing dependence of critical power infrastructures on interconnected physical and cyber-based control systems has resulted in a growing and previously unforeseen cyber security threat to supervisory control and data acquisition (SCADA) and distributed control systems (DCSs).
- It is critical that engineers and managers understand these issues, cyber security and the use of risk assessments that quantitatively determine the probability of an attack, the impact of the attack, and the reduction in risk associated with particular countermeasures are required.