Our holistic view on Cyber Security for wind farm critical infrastructures

Digital Data Integration & Management

Wolf Freudenberg

26 October 2016

Ungraded

SAFER, SMARTER, GREENER

Contents

- Introduction to Cyber Security for critical infrastructures
- Current challenges
- Our holistic approach

Understanding the difference between IT and OT
Impact of OT

Ungraded

Understanding the difference between IT and OT
Vital infrastructures

Oil & Gas

Automotive

Chemicals

Energy & Utilities

Transport

Ungraded

DNV·GL

Understanding the difference between IT and OT

Impact of wind farms

Current large wind farms ~600MW – Future this will be larger >1200MW?

Wind farms will supply stability to the grid in the future (reactive and apparent power)

What if a wind farm is totally shutdown by accident?

Disruption of the power grid possible when ICS/SCADA fails of wind farms?

2015 annual installations

- 12,800 MW of wind power capacity was installed and grid-connected in the EU during 2015, an increase of 6.3% on 2014 installations. 9,766 MW were installed onshore and 3,034 MW offshore.
- Wind power installed more than any other form of power generation in 2015. Wind power accounted for 44.2% of total 2015 power capacity installations.
- Renewable energy accounted for 77% of all new EU power installations in 2015: 22.3 GW of a total 29 GW.
- Big variations between countries in their 2015 new installations reflect the relative effectiveness of policy and regulatory frameworks and uncertainty over future energy policy in EU Member States.

source: windeurope.org

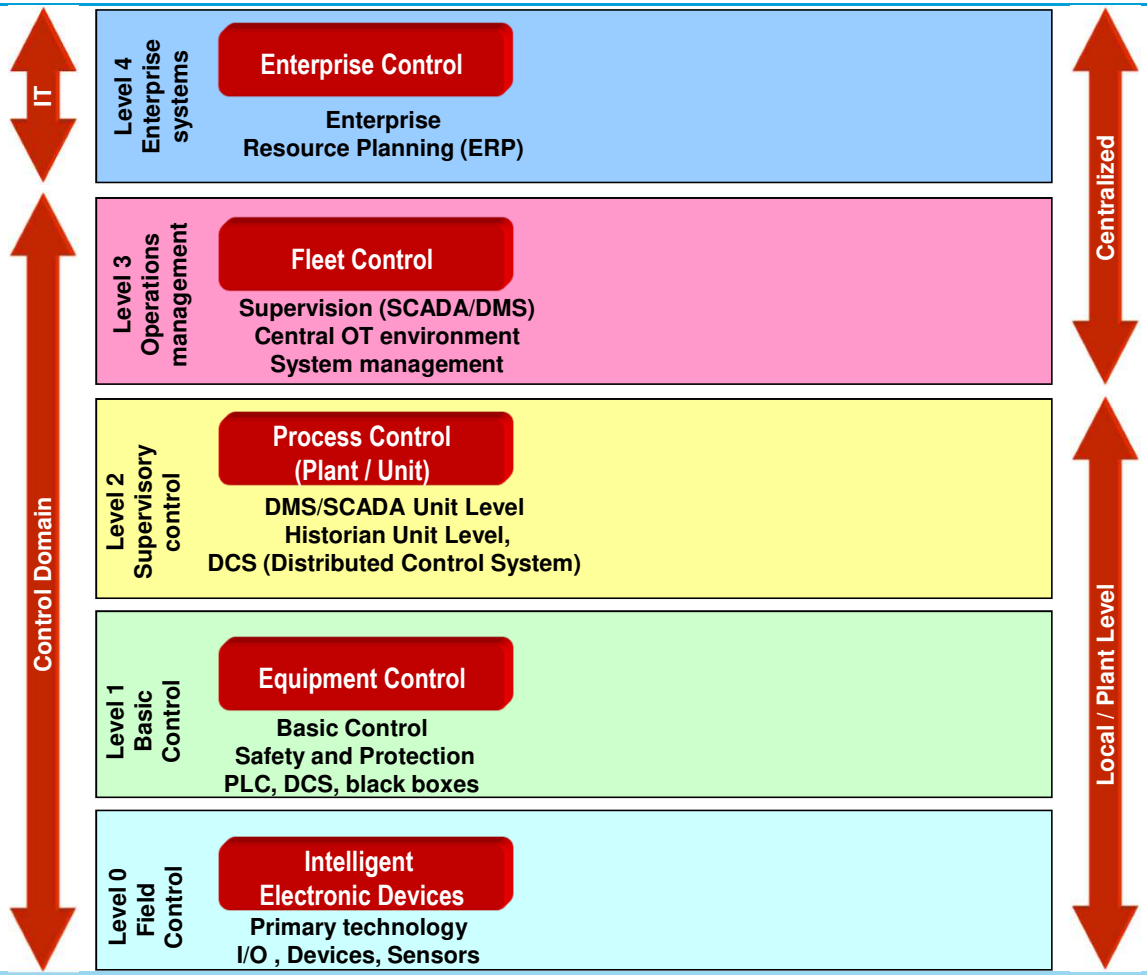
Understanding the difference between IT and OT

Real differences

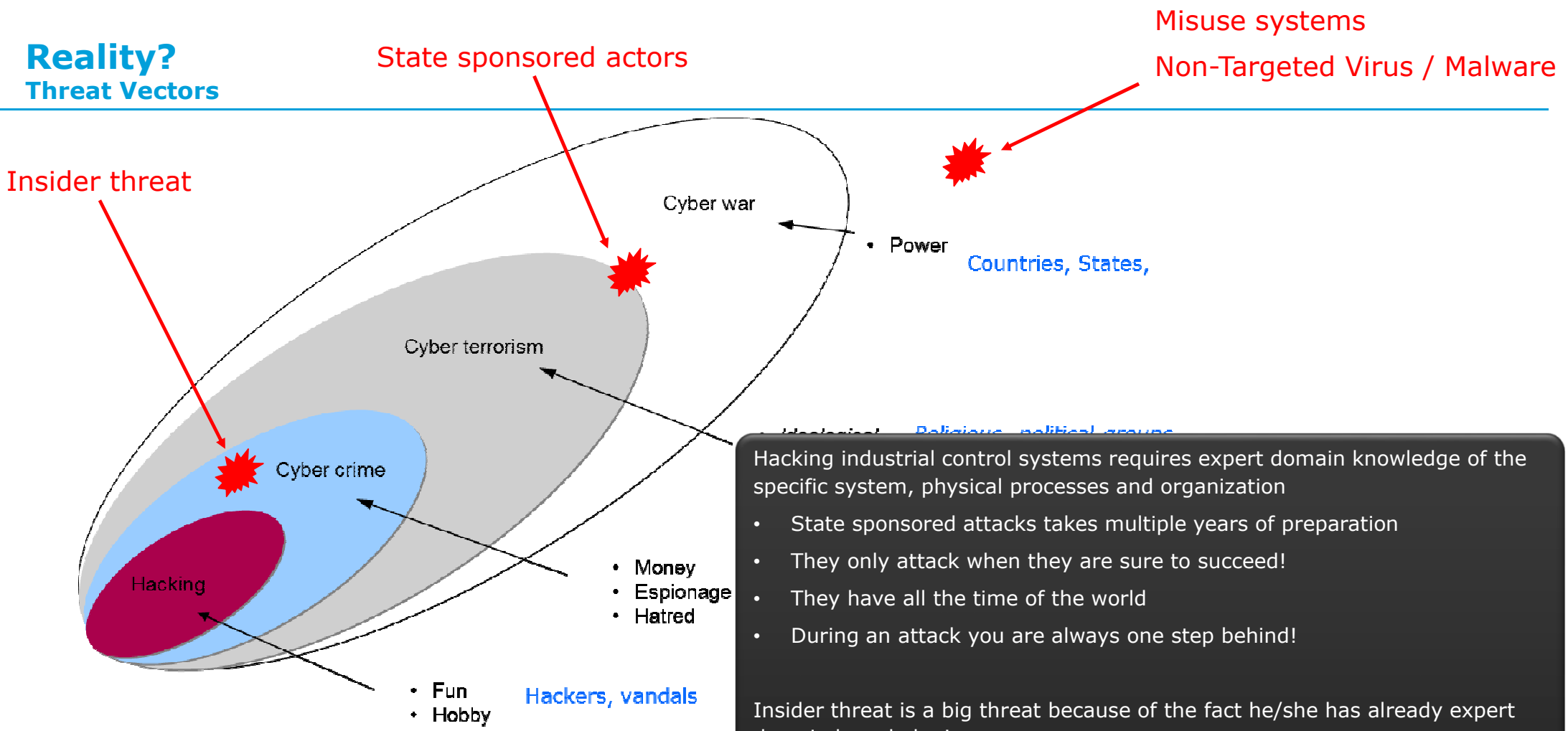
IT	OT
• **Confidentiality**, Integrity, Availability	• **Availability**, Integrity, Confidentiality
• Transactional process	• Real-time process
• Information Risk	• Automation Risk
• Component lifetime 3-5 years	• Component lifetime 15-20 years
• Loss of data	• Loss of life
• Recover by reboot	• Fault tolerance essential
• High throughput, high delay accepted	• Modest throughput, time critical
• Maturity and knowledge on cyber security	• First steps on cyber security, lack of awareness
• Many messages per connections	• Many connections with few messages
• Computer Scientists	• Engineers, Technicians
• Patching straightforward, automated often	• Patching difficult, outage planned, vender needed
• Incident: linear cost and easy predicted	• Incident: difficult to predict and poss. high costs
• Standard methods and architectures	• Landscape very diverse

Dealing with automation environments

ISA-95/IEC62264 and ISA-99/IEC62443



Reality?
Threat Vectors



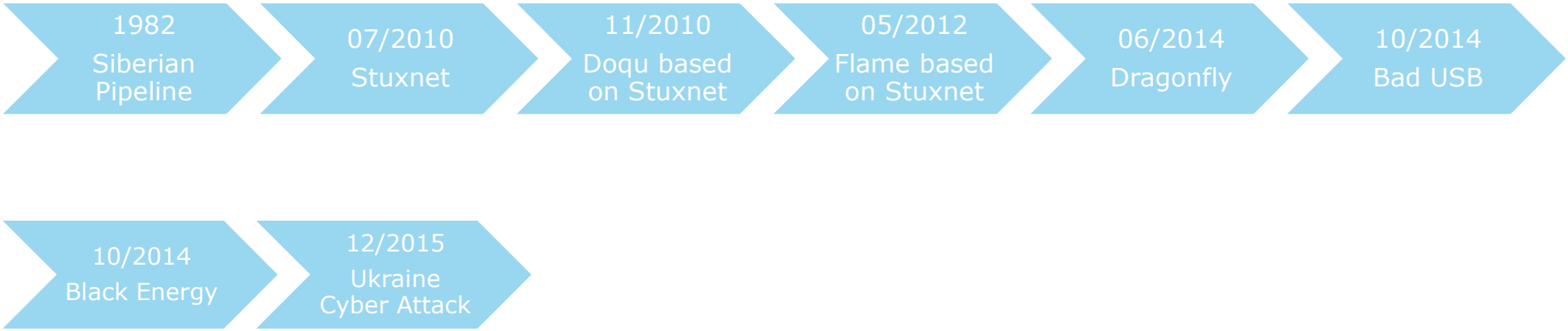
Hacking industrial control systems requires expert domain knowledge of the specific system, physical processes and organization

- State sponsored attacks takes multiple years of preparation
- They only attack when they are sure to succeed!
- They have all the time of the world
- During an attack you are always one step behind!

Insider threat is a big threat because of the fact he/she has already expert domain knowledge!

Everyone can break a computer!
Only experts can break the energy supply

Reality?
Just some incidents

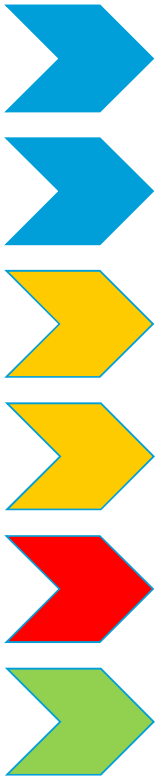


Current Challenges

Wolf Freudenberg

26 October 2016

Current Challenges
Availability, Integrity, Confidentiality



- Availability is the most important aspect and main focus
- We have always relied on our control systems, but can we still do that?
- False sense of trust? Cyber security was not really part of the design and implementation! Interconnections do exist!
- Do we have time, knowledge and experience to really check the full system integrity every day or even every hour?
- Our first priority should be maintaining system's integrity in real-time before availability!
- Monitoring systems to detect changes will support engineers to maintain and check integrity of the control systems in real-time.

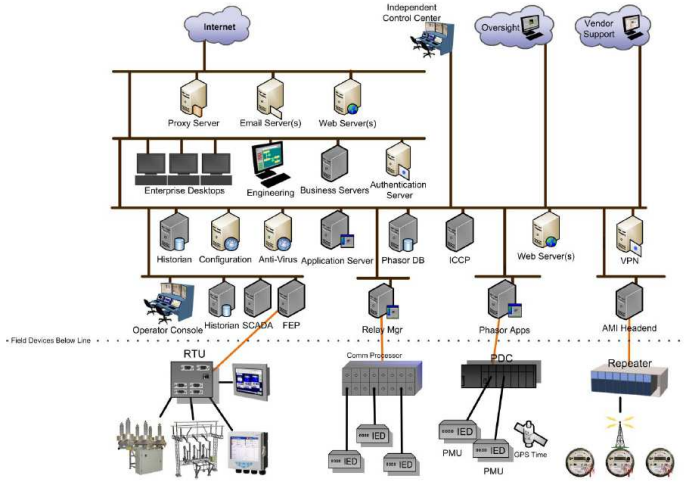
Real-time integrity checking is important to be able to quickly respond to possible cyber attacks!

Current Challenges
IT Security projected on OT/SCADA

IT Security Methods

- OT deals with different kind of threats
- OT/SCADA tailor made for their designed function
- Personnel tailor made for their job; training
- Attacks on OT/SCADA well prepared and tailored made
- OT/SCADA security needs to be tailor made as well
- IT Security great inspiration, we need to re-invent it!

OT/SCADA Landscape



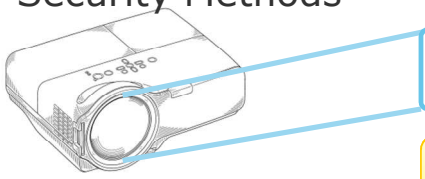
OT/SCADA security is tailor made that starts with risk assessment

DNV·GL

Current Challenges

IT Security projected on OT/SCADA - Patching

IT Security Methods



Patching and Patch Management

Best practices and seen as the most important method to protect against cyber attacks

Patching is fixing systems to known vulnerabilities

OT/SCADA systems are mostly hacked with zero-day vulnerabilities and tailor made malware that both will not be detected

OT/SCADA systems are difficult to patch due to possible risk on unavailability, overhauls are prepared and planned

It is also possible the vendor does not have the solution or it requires an total update of several millions of dollars

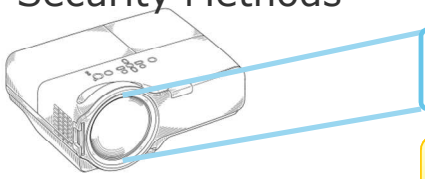
It shows that patching is not the number one for OT/SCADA. How to protect these vulnerable systems?

Something to think about!

Current Challenges

IT Security projected on OT/SCADA - Encryption

IT Security Methods



Encryption, Cryptography

Seen as the cyber security solution against disclosure of information

Encryption is a good method, however it makes OT/SCADA support and maintenance more difficult!

Risk on availability and making support more difficult! Do we really need encryption?

Key management on highly decentralized applications is very cumbersome, update keys of hundreds of devices

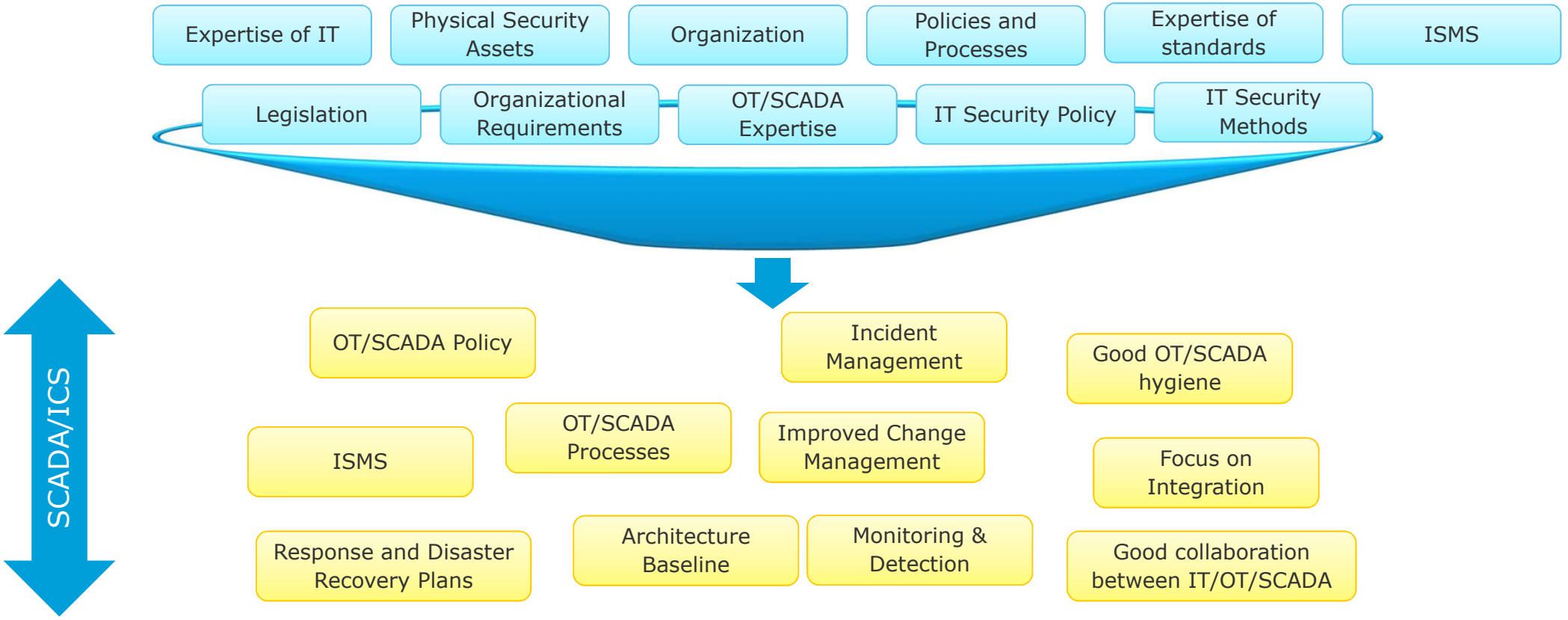
End-to-End encryption makes it for attackers more difficult to learn from captured traffic, it really need to be a trade off

Just implementing encryption? Use risk assessment to determine the right actions to solve your problems!

Something to think about!

Current Challenges

Appropriate translation to the OT landscape



Time to change and focus on OT!

Our holistic approach

Wolf Freudenberg

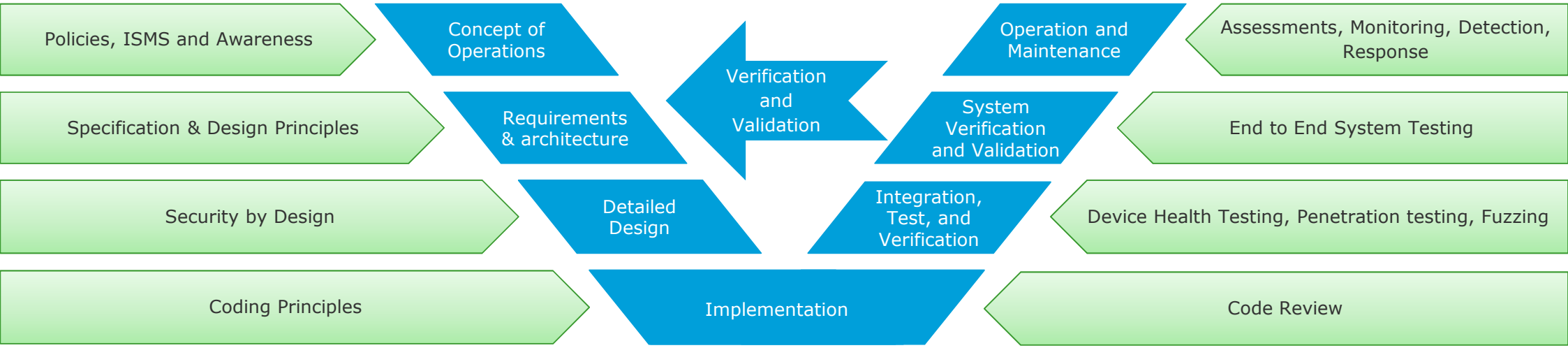
26 October 2016

How to address the cyber security challenge?
Security Management: A Holistic approach

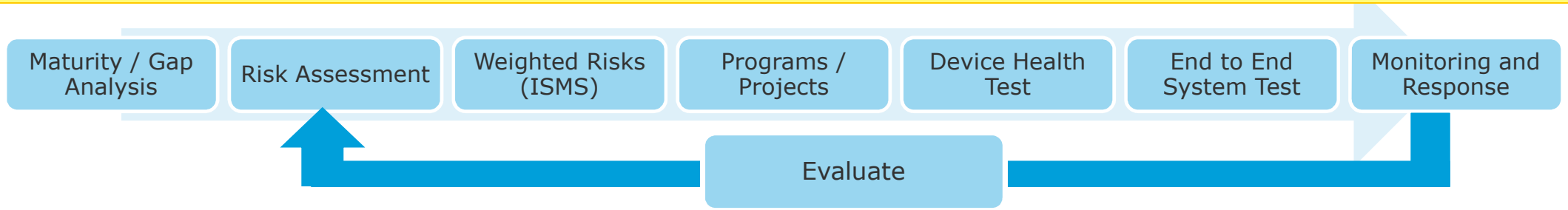
Holism is the idea that natural systems (physical, biological, chemical, social, economic, mental, linguistic, etc.) and their properties should be viewed as wholes, not as collections of parts

This often includes the view that systems function as wholes and that their functioning cannot be fully understood solely in terms of their component parts

Cyber Security portfolio



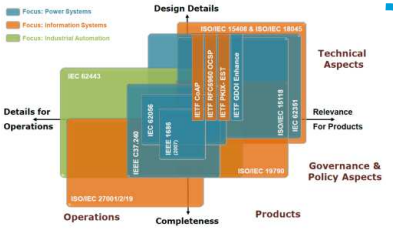
Extend well known V model with cyber security services



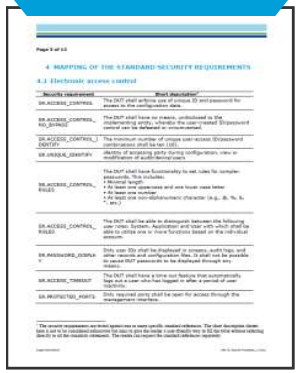
Risk based approach

Cyber Security Health Test approach

Smart grid and security standards



Requirements test pack



In-situ, smart grid equipment

Common criteria methodology

Testing topics

1. Functional testing

2. Negative and robustness testing

3. Known vulnerability testing, leveraging global vulnerability database

Findings and recommendations

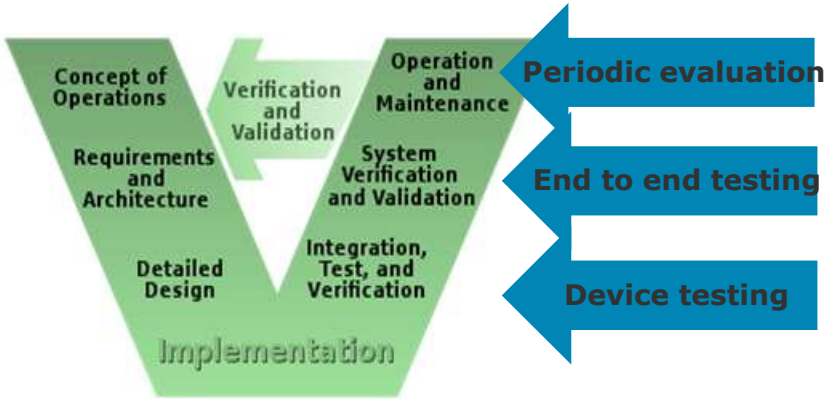
Ungraded

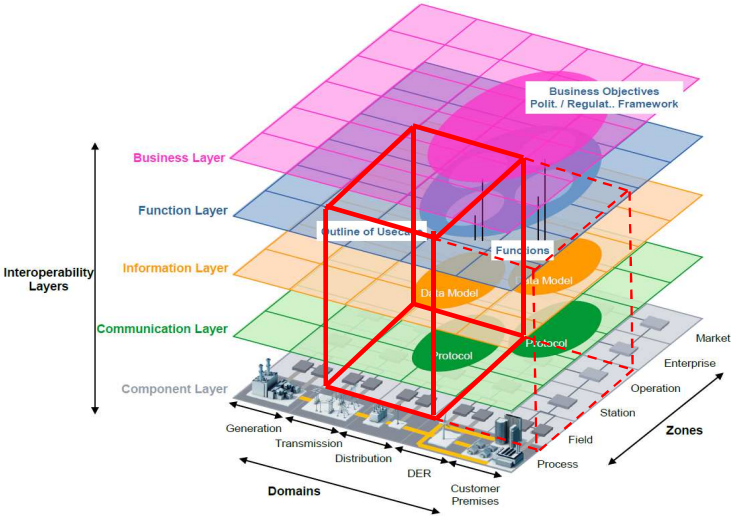
DNV·GL

Cyber Security End-To-End Test

Comprehensive, cost effective testing for energy IT systems and smart grids

- The service will provide cost effective 3rd party technical validation services to provide bottom up proof that proper security measures have been taken for a complete system from an end to end perspective.
- We assess your system regarding
  - Secure network design principles.
  - Physical cyber defences and intrusion prevention.
  - Data stream analysis.
  - Policy and procedures for prevention, detection, mitigation and recovery.
- Deliverable:
  Report describing the cyber secure state of your OT / ICS / smart grid system.





Ungraded

DNV GL Cyber Security

Wolf Freudenberg
Wolf.Freudenberg@dnvgl.com
+31 26 3 56 3572

www.dnvgl.com

SAFER, SMARTER, GREENER

Ungraded

DNV·GL