RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SBX1-R12

Industrial Defence In-Depth

Andrey Nikishin

Special Projects Director
Kaspersky Lab
@andreynikishin

#RSAC

Agenda

- Industrial specifics
- Industrial Cyber Security in Depth

INDUSTRIAL SPECIFICS

Critical infrastructure sectors By State

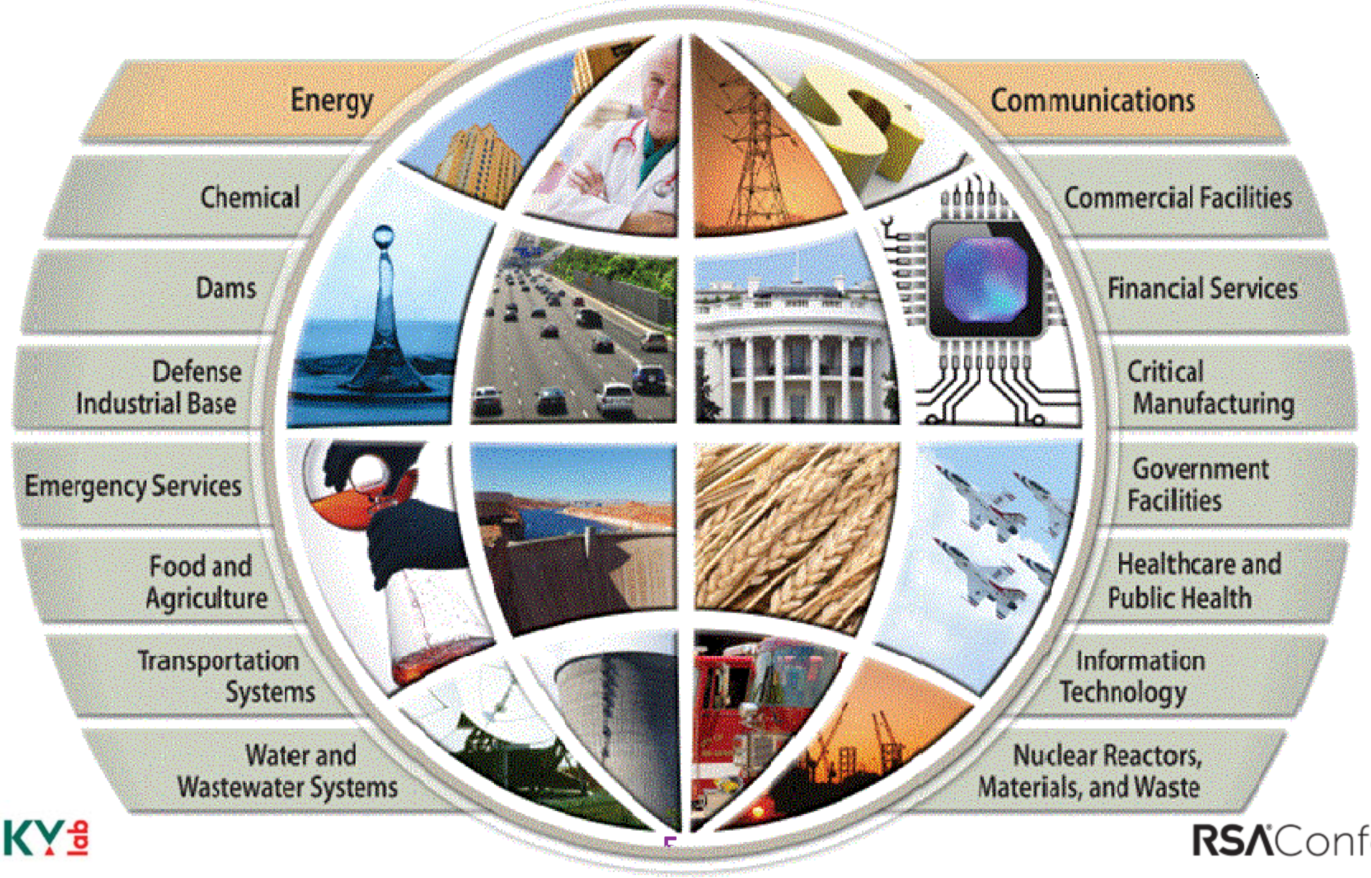
CPNI
Centre for the Protection of National Infrastructure

- Energy
- Transport
- Water
- Food
- Communications
- Emergency Services
- Financial Services
- Government
- Health

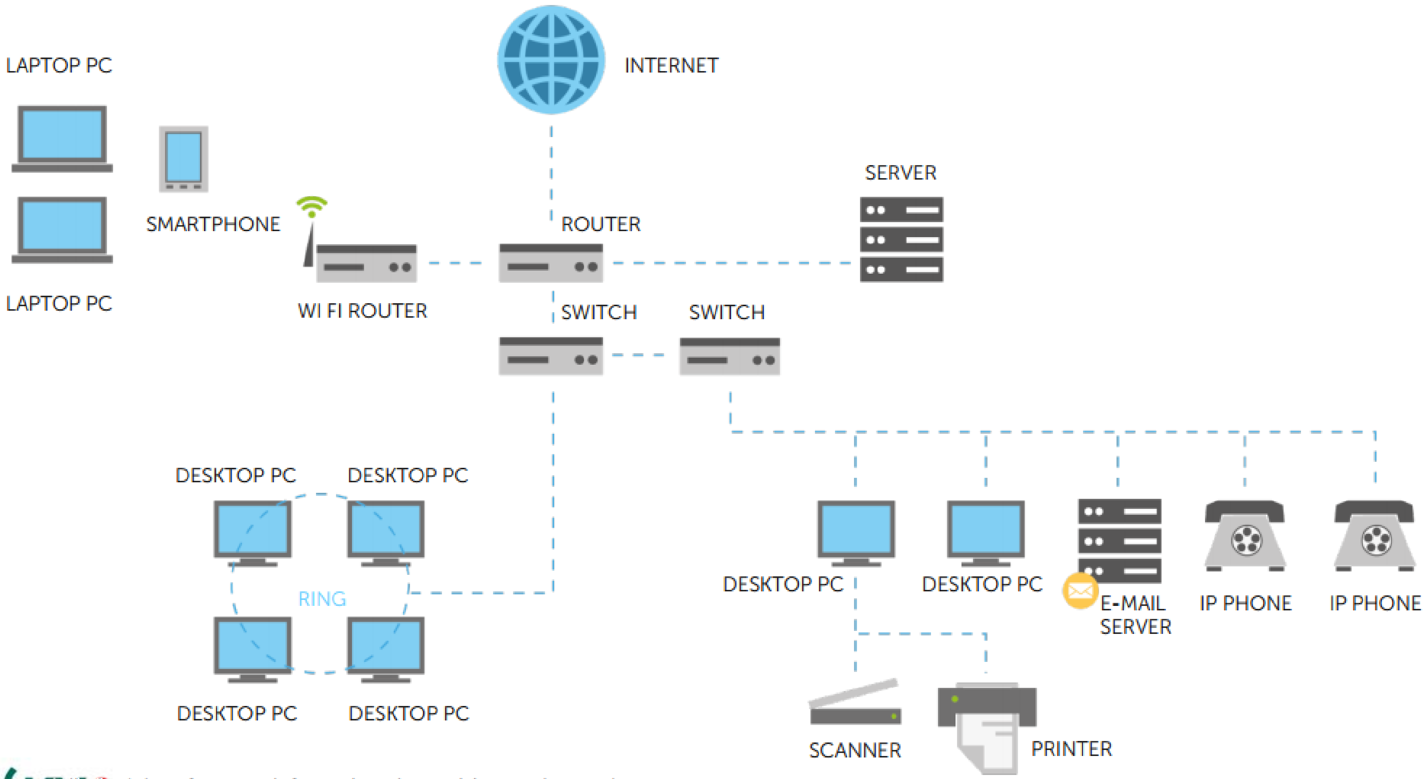
U.S. DEPARTMENT OF HOMELAND SECURITY

- Energy
- Chemical
- Commercial Facilities
- Nuclear
- Transportation Systems
- Water and Wastewater
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Food and Agriculture
- Emergency Services
- Communications
- Financial Services
- Government Facilities
- Healthcare and Public Health
- Information Technology

IS all INDUSTRIAL Infrastructure Critical?

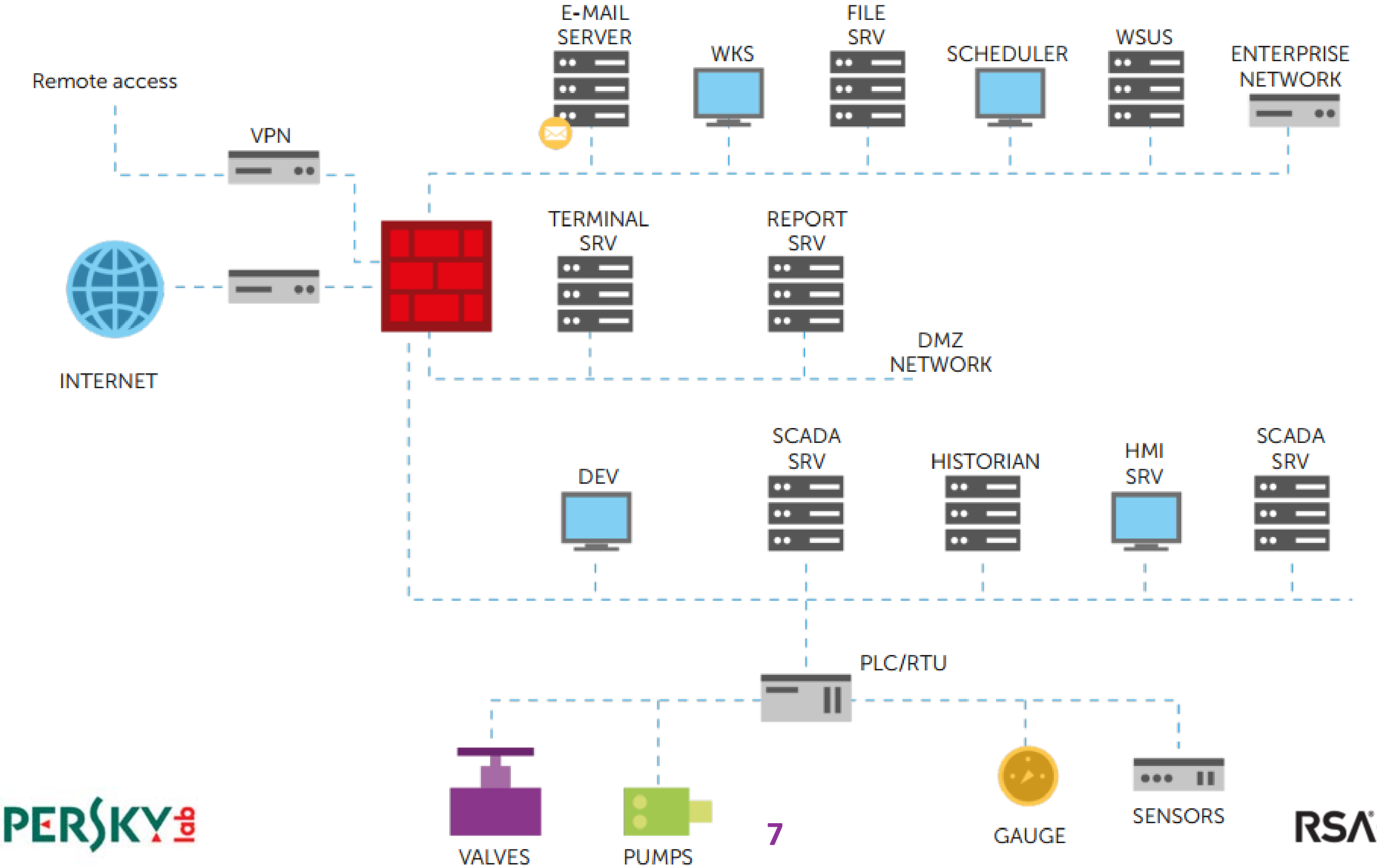


Simplified IT schema



The page represents limited data, for more information please visit www.kaspersky.com

Simplified ICS (OT) network schema



ICS Network: Common devices

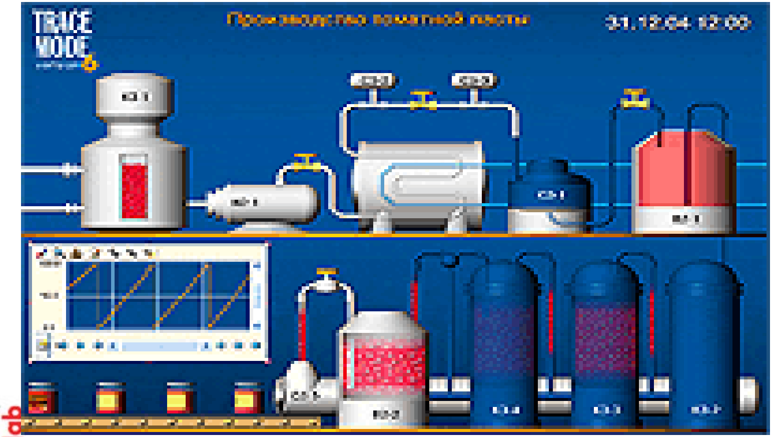
HMI

SCADA server

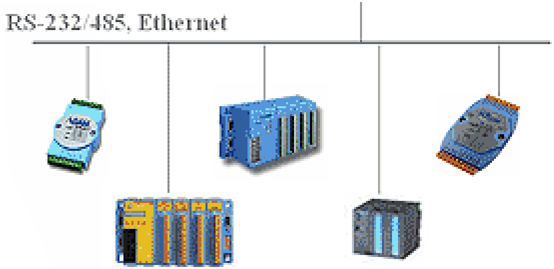
Data Historian

Development system (IDE) / Engineering WS

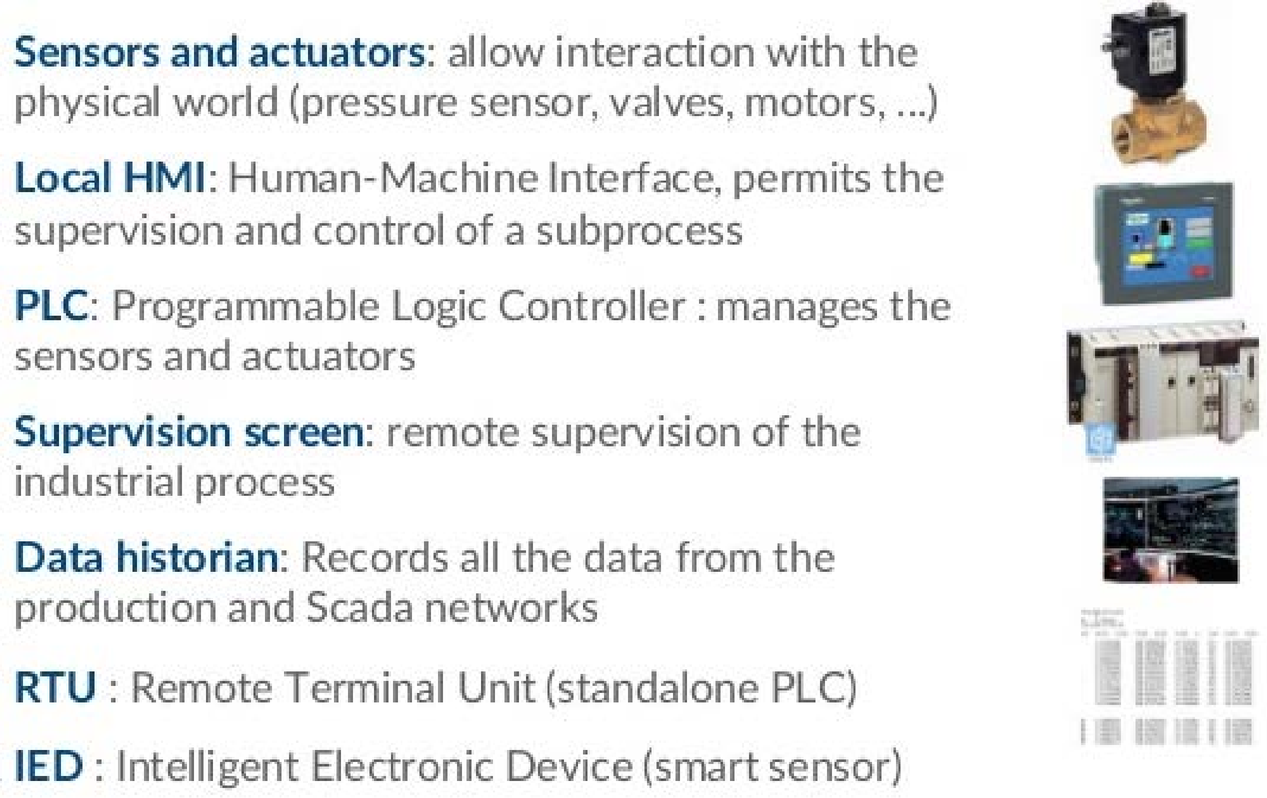
Field equipment



PLC/DCS



ICS Network: Common devices



Sensors and actuators: allow interaction with the physical world (pressure sensor, valves, motors, ...)

Local HMI: Human-Machine Interface, permits the supervision and control of a subprocess

PLC: Programmable Logic Controller : manages the sensors and actuators

Supervision screen: remote supervision of the industrial process

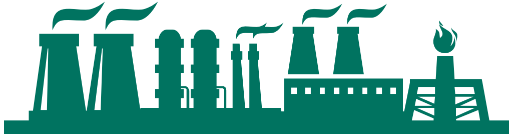
Data historian: Records all the data from the production and Scada networks

RTU : Remote Terminal Unit (standalone PLC)

IED : Intelligent Electronic Device (smart sensor)

Industrial Security Approach

Industrial Network



1. Availability
2. Integrity
3. Confidentiality

Corporate Network

1. Confidentiality
2. Integrity
3. Availability

- Corporate IT Security is about Data protection
- Industrial Security is about Process protection
- Process should be continuous and only then secure

WHY NOT TO USE IT SOLUTIONS? (1)

Technologies	IT	ICS
Antivirus	Typical, highly automated	Difficult, performance, FP, legacy systems
Patching	Typical, highly automated	Difficult, Require switching to service mode
Security testing and audit	Use of modern tools, external experts	Modern method and tools not applicable

WHY NOT TO USE IT SOLUTIONS? (2)

Technologies	IT	ICS
Change management	Typical	Non-standard, Per case solutions
Incident management	Event handling, recording is automated. Post mortem and audit analysis is common	Difficulty replaying events
Equipment life cycle		Not automated only when necessary

WHY NOT TO USE IT SOLUTIONS? (3)

Technologies	IT	ICS
Physical security	Low security for offices, High for data centers	Highly demanded
Security development cycle	Integrated into development cycle	Rare in use
Compliance to standards	Limited to some areas	Highly demanded

Industrial Security today — Low awareness

C-level

Doesn’t see how
Cyber Security spending
relates to Revenues

IT Security

Is not allowed to go
into Industrial sites

Engineers

Are more concerned
about security measures
than malware

Mutual understanding and partnership between these 3 are crucial to successful cyber security and Critical Infrastructure Protection

What makes protection difficult today

Low awareness, mix of hype and real, no 'hard data'

Typical 'office' IT security is not applicable

Most attacks target the following objects: old, unsecure and hard to update

Lack of cyber security skills, and industrial cyber security practice

Lack of OT cyber security ownership

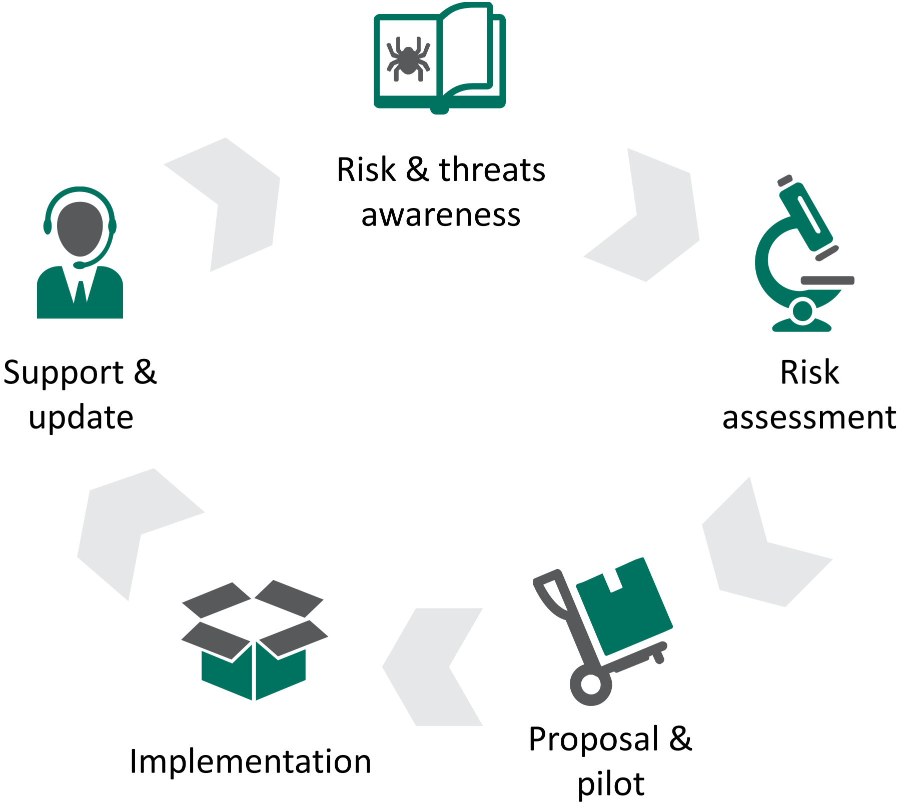
Industrial Specifics. Summary

- Industrial Security is about Process protection
- Process should be continuous and only then secure
- IT vs OT
- The ICS network protocols do not have integrity check, user authorization and authentication
- Old or unsupported OS with no patching (Windows XP too)

- Specially designed approach, products & services

Industrial Defence In-Depth

Cyber security is a process not a project



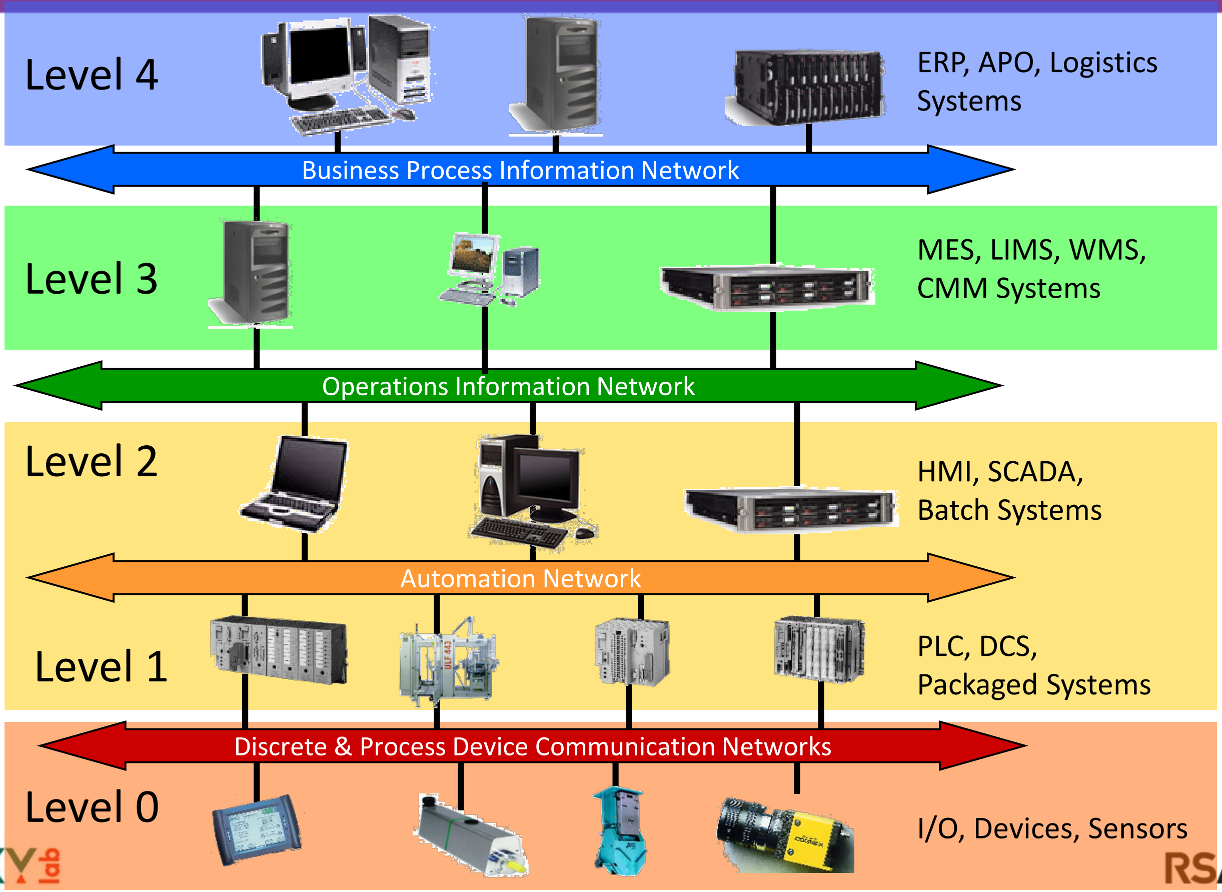
Cyber risks and threats

- Mistakes by SCADA operators or contractors (3rd parties)
- Actions of Insiders (made on purpose or not)
- Incidental infection
- Infection via contractors (removable media or network connection)
- Lack of awareness and hard data for incident forensics
- Hacktivists actions and cyber hooligans attacks
- APTs and Governmental-backed attacks
- Cyber sabotage (any sort of it)
- Compliance
- Fraud

ATTACK VECTORS

- Vulnerable software (SCADA, OS, 3rd-party)
- ERP/MES & Internet connections
- Uncontrolled software usage
- Unauthorized mobile device usage
- Uncontrolled external devices (USB, SATA, etc.)
- 3rd parties and contractors
- Supply chain
- Malware

Conceptual Topology


Level 4
ERP, APO, Logistics Systems
Business Process Information Network
Level 3
MES, LIMS, WMS, CMM Systems
Operations Information Network
Level 2
HMI, SCADA, Batch Systems
Automation Network
Level 1
PLC, DCS, Packaged Systems
Discrete & Process Device Communication Networks
Level 0
I/O, Devices, Sensors

Risks, Malware & Internet Treats

LEVEL 3

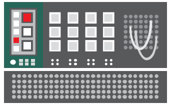
- Manufacturing Operations management

- Malware via USB, Network, Corporate network, email, Web
- Human actions (intention or not) (insiders, contractors)
- Internet attacks (hackers, radicals, hacktivists, etc)

LEVEL 2, 1

- SCADA
- HMI
- Engineering Wks
- PLC, TRU
- etc

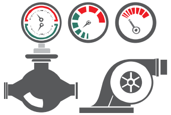
- Malware via USB, Network, Contractors
- Human actions (insiders, contractors)
- Internet attacks



- Malware via Industrial network
- Human actions

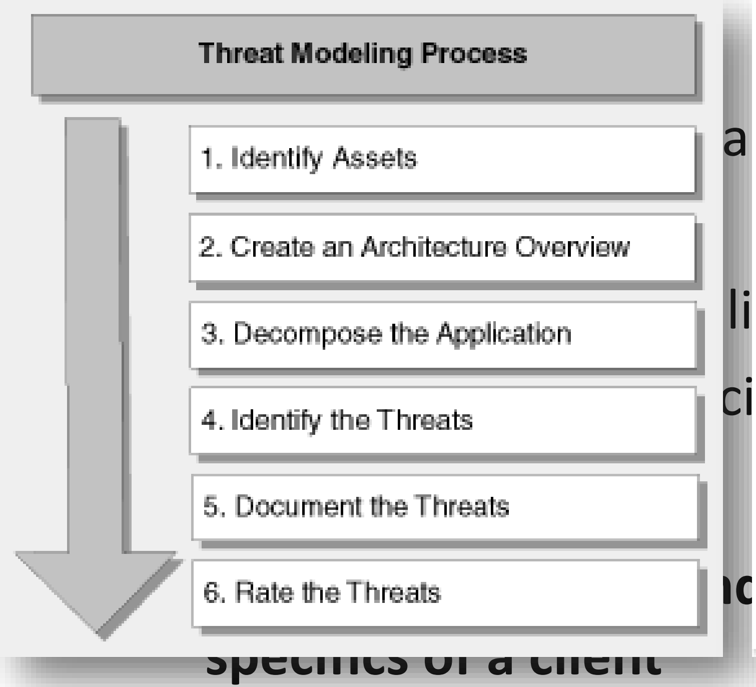
LEVEL 0

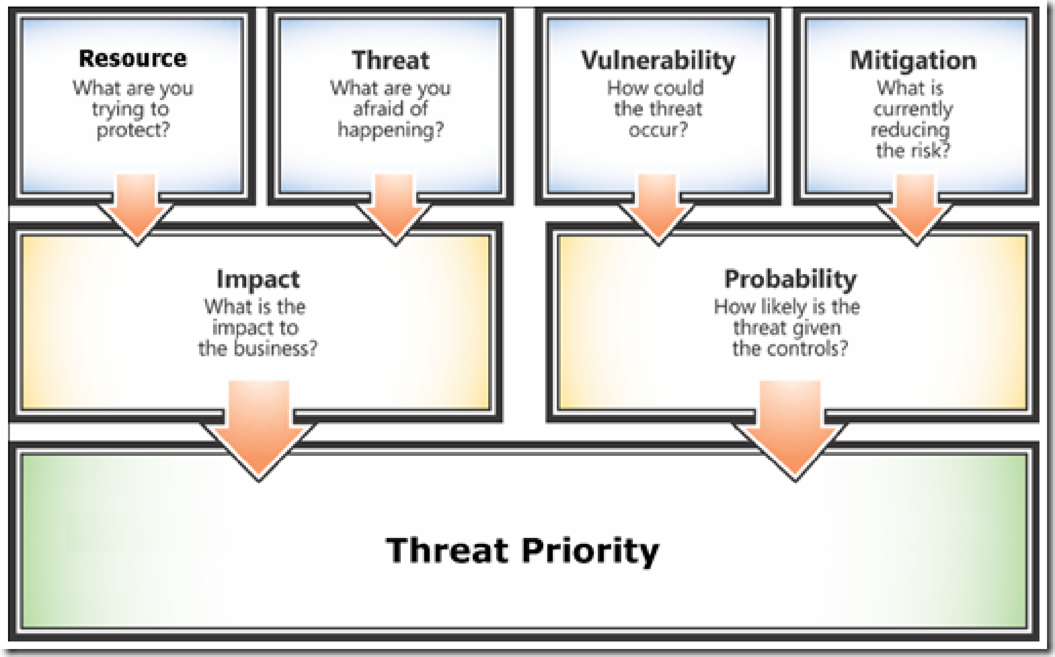
- Physical



- Human

Risk assessment (Security gap assessment)




Resource
What are you trying to protect?
Threat
What are you afraid of happening?
Vulnerability
How could the threat occur?
Mitigation
What is currently reducing the risk?
Impact
What is the impact to the business?
Probability
How likely is the threat given the controls?
Threat Priority

a

li

ci

nc

specifics of a client

Cyber risks and threats

- Malware & Attacks
  - Incidental infection
  - Infection via contractors (removable media or network connection)
  - Hacktivists actions and cyber hooligans attacks
  - APTs & Governmental-backed attacks
  - Cyber sabotage (any sort of it)
- Human actions
  - Mistakes by SCADA operators or contractors (3rd parties)
  - Actions of Insiders (made on purpose)
- Compliance
- Lack of awareness and hard data for incident forensics

Nodes Security
Firewall/IDS
Policy
Education
Protect, Prevent,
Report & Remediate

Network Security
Policy
Education
Detect, report

Defense strategies

Seven Strategies to Defend ICSs

Implement Application Whitelisting – 38%

Implement Secure Remote Access – 1%

Ensure Proper Configuration/Patch Management – 29%

Monitor and Respond – 2%

Reduce your Attack Surface Area – 17%

Manage Authentication – 4%

Build a Defendable Environment – 9%

Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy

Node Security

Protect & Prevent & Report & Remediate

- Works on ICS/SCADA Servers, engineering workstations and supports Human Machine Interfaces
- Run in high-availability mode & without updates
- Whitelisting is main technology
- External Device Control
- Vulnerability Assessments

Network Security

Detect & Report

- Network traffic anomaly detection in a passive mode
- Detection of potentially dangerous control commands from technological process point of view
- Network integrity monitoring (Detection of new network devices and communications in ICS network)
- Collect and store events -- Forensic, monitoring and incident detector tool

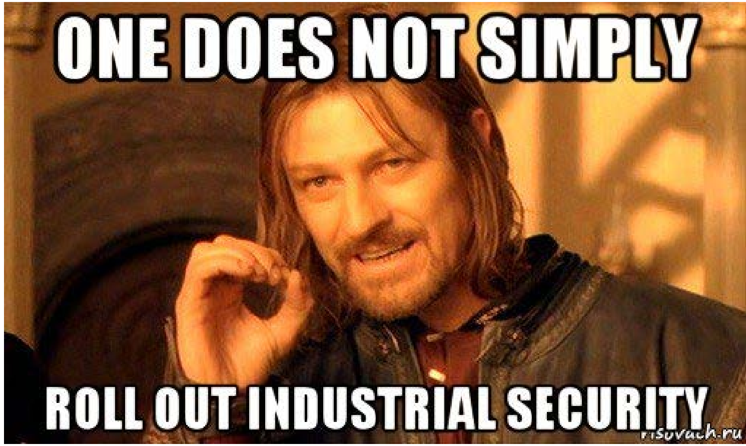
Firewall/IDS/Remote access

Protect & Prevent & Detect & Report

- Support industrial protocols
- Knows specific industrial attacks

Pilot testing

- Pilot testing on test environment is an essential part
- Fine-tuning
- Customisation/for industry/ for customer / for product line
- Certification / vendors & regulators
- Approval by a client



Standards & best practices

International:

- ISA/IEC-62443 (Formerly ANSI/ISA-99): Security for Industrial Automation and Control Systems
- ISO/IEC 27009: Information technology — Security techniques — Sector-specific application of ISO/IEC 27001
- ISO/IEC 15408: Information technology — Security techniques — Evaluation criteria for IT security
- IEEE 1402 : IEEE Guide for Electric Power Substation Physical and Electronic Security

Industrial:

- NIST SP 800-53 : Information Security
- NERC : Cybersecurity Risk Management Process (RMP) Guideline
- NERC CIP-002-3 : Cyber Security - Critical Cyber Asset Identification
- NERC CIP-005-3a : Cyber Security - Electronic Security Perimeter(s)
- American Petroleum Institute : API 1164 'SCADA Security'
- American Gas Association : AGA 12-4 Protection Embedded in SCADA Components

Other:

- NERC : Cybersecurity Risk Management Process (RMP) Guideline
- NERC CIP-002-3 : Cyber Security - Critical Cyber Asset Identification
- NERC CIP-005-3a : Cyber Security - Electronic Security Perimeter(s)
- American Petroleum Institute : API 1164 'SCADA Security'
- American Gas Association : AGA 12-4 Protection Embedded in SCADA Components

Education

- Cyber Security Awareness (should be part of induction process)
  - Employee cyber security training
  - ICS Cyber Security basics
  - Social attack in critical infrastructure environment
- Cyber Security for SOC
  - Advanced cyber security trainings (malware analysis, reverse engineering etc.) on yearly basis

Incident response & Forensic

- Common response and forensic services
  - On-demand reports
  - Customized reports on incidents/infections
  - Early warnings on threats
  - Private investigations (from malware analysis to complex service)
- Own CERT
  - Help with organizing it
  - Training for staff
  - Reports

Summary

- Industrial Cyber Security is not like Office Cyber Security
- It requires specific approach, products and services
- Employees are the weakest link so education is extremely important
- Cyber security is not a project, it is a process

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SBX1-R12

Industrial Defence In-Depth

Andrey Nikishin

Special Projects Director
Kaspersky Lab
@andreynikishin

#RSAC