UNIVERSITY OF THE AEGEAN
Department of Shipping
Trade and Transport

Εργαστήριο Πληροφορικής
και Νέων Τεχνολογιών στη Ναυτιλία,
τις μεταφορές και τη Νησιωτική Ανάπτυξη

Maritime SCADA cyber resilience

Prof. Nikitas Nikitakos

Dept. of Shipping Trade and Transport

University of the Aegean - GREECE

Digital Ship

MARITIME CYBER
RESILIENCE FORUM

ATHENS, 25 APRIL

OUTLINES

- Introduction to maritime ICS/SCADA
- Vulnerabilities of maritime SCADA
- Types and Impacts of Exploiting maritime SCADA
- SCADA protection – Risk assessment
- Best practices – Modern Connectivity
- Commissioning and operation of SCADA

Introduction

Typically, control systems collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment

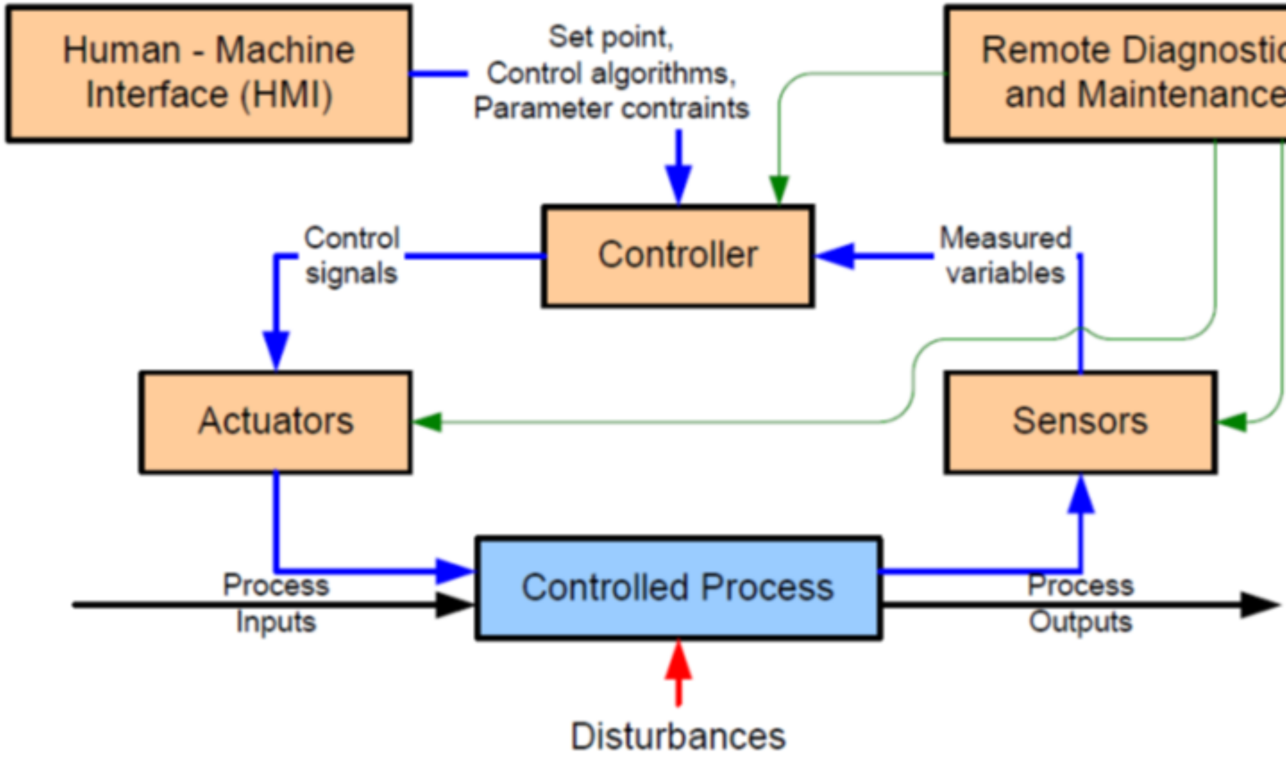
Distributed control systems (DCS) are typically used within a single process or generating plant or used over a smaller geographic area or even a single-site location.

Supervisory control and data acquisition (SCADA) systems are typically used for larger-scale environments that may be geographically dispersed in an enterprise-wide distribution operation.

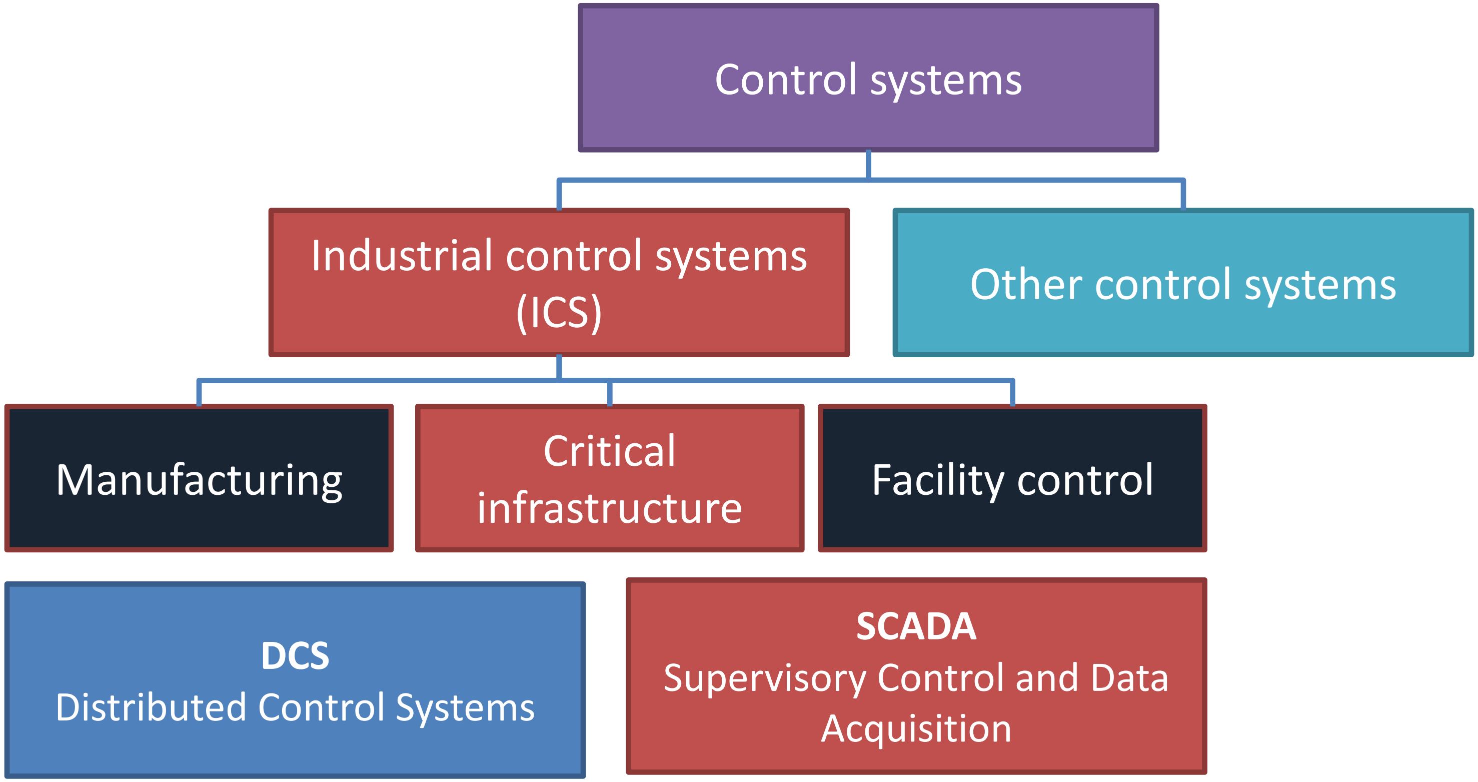
Control loops in a SCADA system tend to be open, whereas control loops in DCS tend to be closed.

The SCADA system communications infrastructure tends to be slower, and less reliable, and so the remote terminal unit (RTU) in a SCADA system has local control schemes to handle that eventuality

Industrial Control system



Introduction



Control systems

Industrial control systems (ICS)

Other control systems

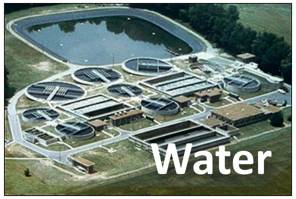
Manufacturing

Critical infrastructure

Facility control

DCS
Distributed Control Systems

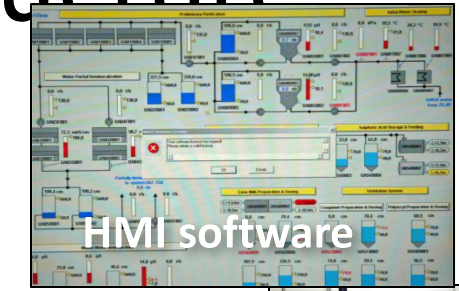
SCADA
Supervisory Control and Data Acquisition



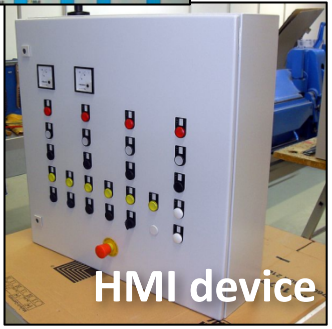
The SCADA industry

- People are expensive, but computers are cheap.
  - Commercial and profit-driven
  - A truly global industry
- Idiosyncratic
  - Few standards
  - New processes bolted on to existing facilities
- Pragmatic and functional
  - Built to last
  - Early systems are still running

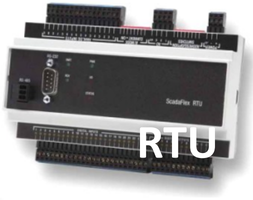
Basic SCADA structure



A few **Human-Machine Interfaces (HMI)**
(computer screens and buttons for people)



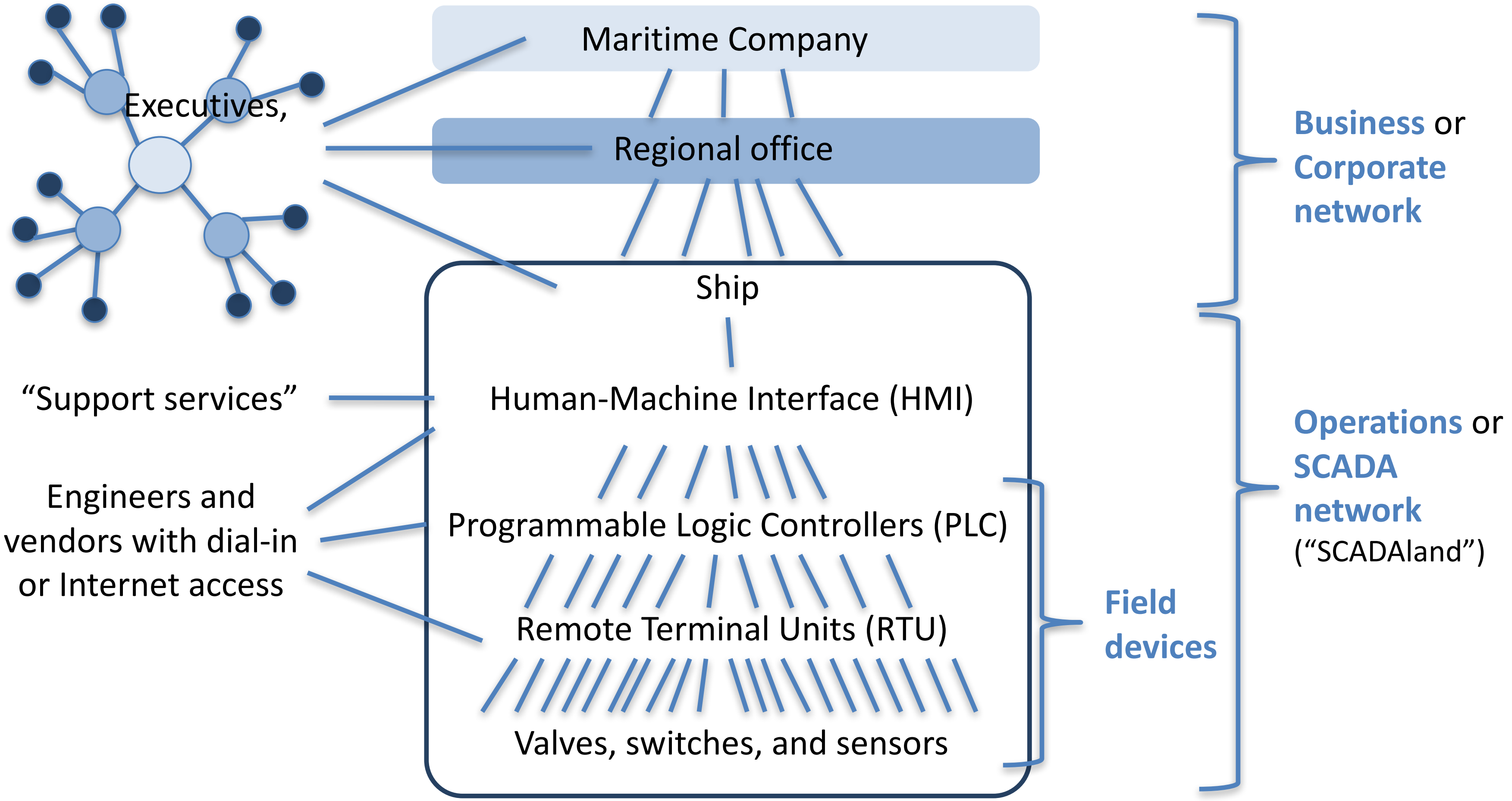
Many **Programmable Logic Controllers (PLC)**
(watching system and making routine decisions)



Hundreds of **Remote Terminal Units (RTU)**
(reading sensors and controlling valves and switches)

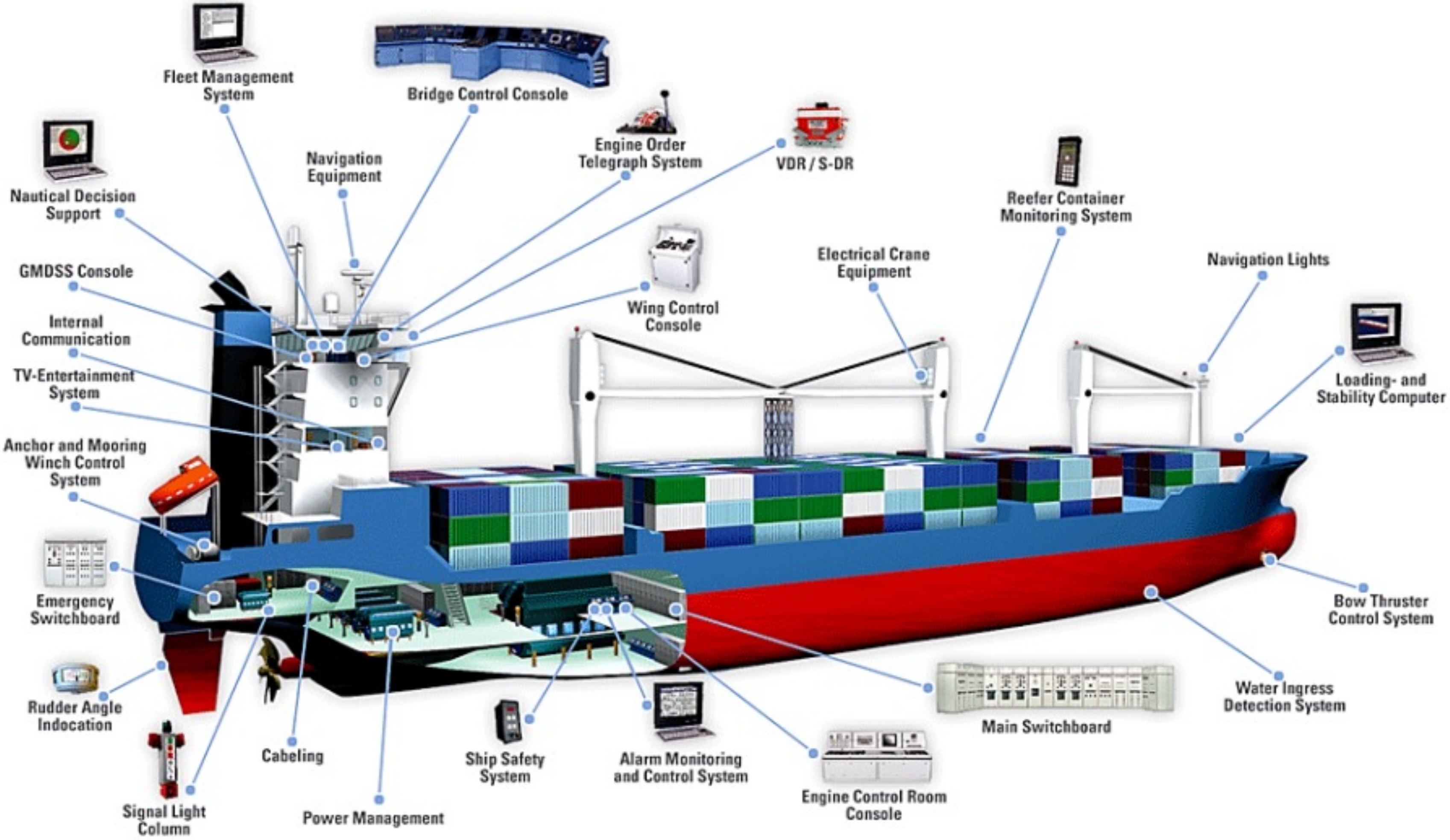
The **process**: Many thousands of valves, switches, and sensors (temperature, pressure, flow, etc)

Modern Maritime SCADA



Maritime Company
Executives,
Regional office
Ship
Human-Machine Interface (HMI)
"Support services"
Engineers and vendors with dial-in or Internet access
Programmable Logic Controllers (PLC)
Remote Terminal Units (RTU)
Valves, switches, and sensors
Business or Corporate network
Operations or SCADA network ("SCADAland")
Field devices

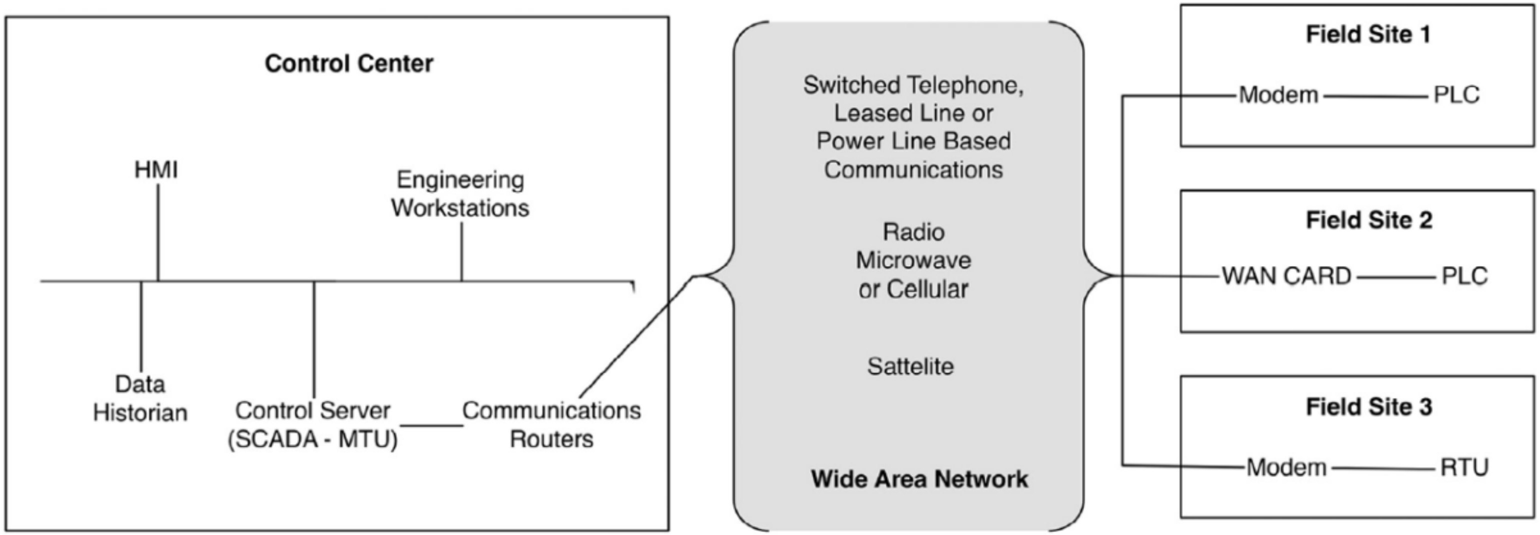
Typical Shipboard ICS


Fleet Management System
Bridge Control Console
Engine Order Telegraph System
VDR / S-DR
Navigation Equipment
Nautical Decision Support
Reefer Container Monitoring System
GMDSS Console
Electrical Crane Equipment
Navigation Lights
Wing Control Console
Internal Communication
TV-Entertainment System
Loading- and Stability Computer
Anchor and Mooring Winch Control System
Emergency Switchboard
Bow Thruster Control System
Water Ingress Detection System
Rudder Angle Indocation
Main Switchboard
Cabeling
Ship Safety System
Alarm Monitoring and Control System
Engine Control Room Console
Signal Light Column
Power Management

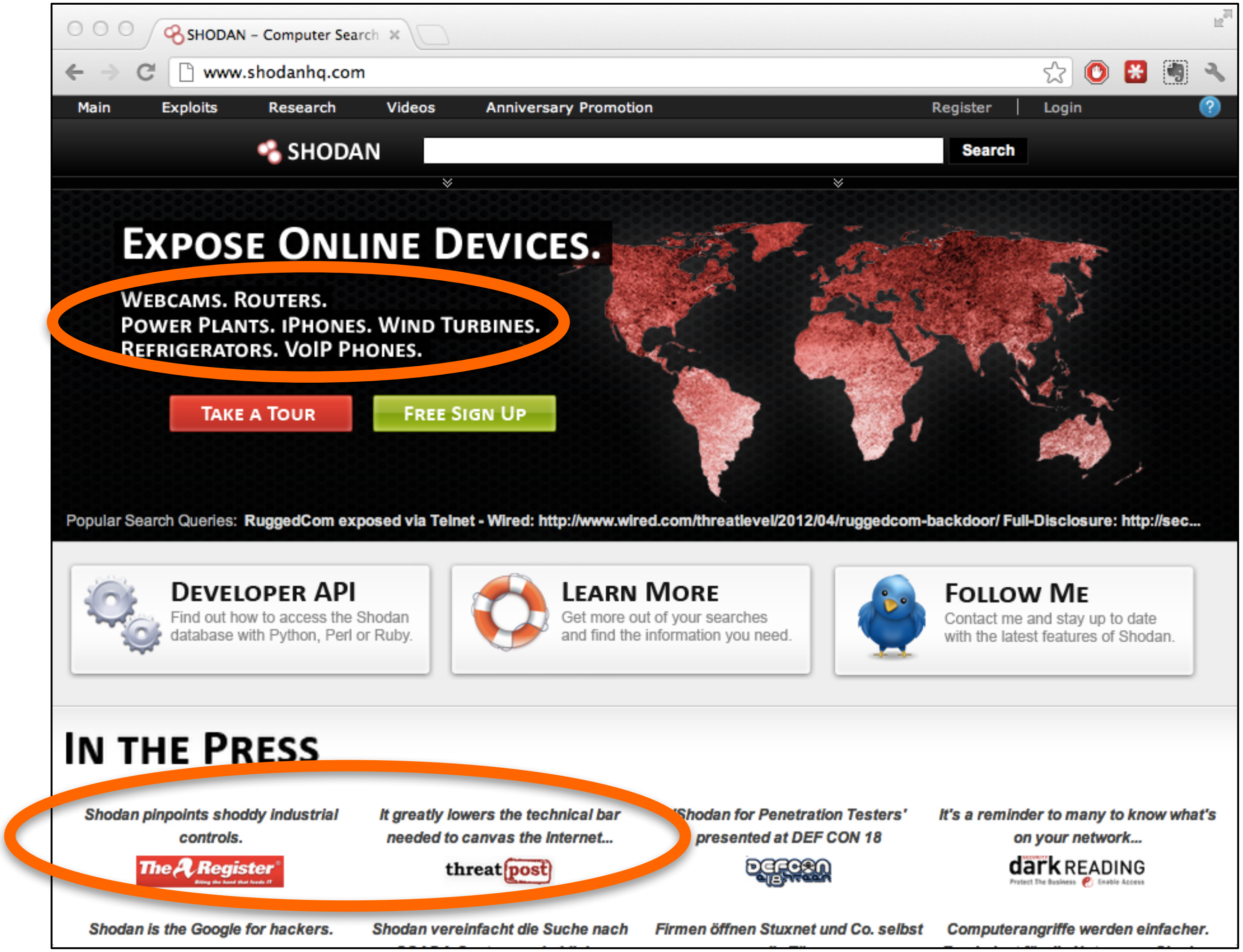
Maritime SCADA systems

- Alarm and Monitoring System
- Auxiliary Control System
- Power Management System
- Cargo Control System
- Propulsion Control System
- Ballast Automation System
- Air Conditioning System
- Anti – Heeling
- Reefer Monitoring
- Fire System
- Main Engine Monitoring System

Generic SCADA Hardware Architecture (NIST SP 800-82)



Shodan: “Google for hackers”



Expose Online Devices.

Webcams. Routers.
Power Plants. iPhones. Wind Turbines.
Refrigerators. VoIP Phones.

Popular Search Queries: RuggedCom exposed via Telnet - Wired: http://www.wired.com/threatlevel/2012/04/ruggedcom-backdoor/ Full-Disclosure: http://sec...

Developer API
Find out how to access the Shodan database with Python, Perl or Ruby.

Learn More
Get more out of your searches and find the information you need.

Follow Me
Contact me and stay up to date with the latest features of Shodan.

In the Press

Shodan pinpoints shoddy industrial controls. — The Register

It greatly lowers the technical bar needed to canvas the Internet... — threatpost

'Shodan for Penetration Testers' presented at DEF CON 18 — DEFCON 18

It's a reminder to many to know what's on your network... — dark READING

Shodan is the Google for hackers.

Shodan vereinfacht die Suche nach

Firmen öffnen Stuxnet und Co. selbst

Computerangriffe werden einfacher.

SCADA Vulnerabilities

- The adoption of standardized technologies with known vulnerabilities

- The connectivity of many control systems via, through, within, or exposed to unsecured networks, networked portals, or mechanisms connected to unsecured networks (which includes the Internet)

- Implementation constraints of existing security technologies and practices within the existing control systems infrastructure (and its architectures)

- The connectivity of insecure remote devices in their connections to control systems

- The widespread availability of technical information about control systems, most notably via publicly available and/or shared networked resources such as the Internet

SCADA Vulnerabilities

- Disrupt the operations of control systems by delaying or blocking the flow of information through the networks supporting the control systems, thereby denying availability of the networks to control systems’ operators and production control managers.
- Attempt, or succeed, at making unauthorized changes to programmed instructions within PLC, RTU, or DCS controllers, change alarm thresholds, or issue unauthorized commands to control station equipment, Send falsified information to control system operators either to disguise unauthorized changes or to initiate inappropriate actions
- Modify or alter control system software or firmware such that the net effect produces unpredictable results (such as introducing a computer “time bomb”)
- Interfere with the operation and processing of safety systems
- Many control systems are vulnerable to attacks of varying degrees; these attack attempts range from telephone line sweeps (a.k.a. wardialing), to wireless network sniffing (wardriving), to physical network port scanning, and to physical monitoring and intrusion

Types and Impacts of Exploiting ICS(1)

Direct physical damage to affected equipment and systems…

by exploiting an ICS, the controlled mechanism can fail with catastrophic results, damaging a single piece of equipment, interrupting a larger system, or disabling or destroying an entire ship.

Small-scale, local disruptions…

which damage or interrupt individual systems or single ships within a single organization, without widespread impact beyond the affected function or service.

Types and Impacts of Exploiting ICS(2)

Injury or death to operators, passengers or the general public.

-An incident can affect an single operator or a larger number of crewmembers or bystanders. Targeted attacks on a safety-critical safety can result in a fire or explosion that injures or kills hundreds.

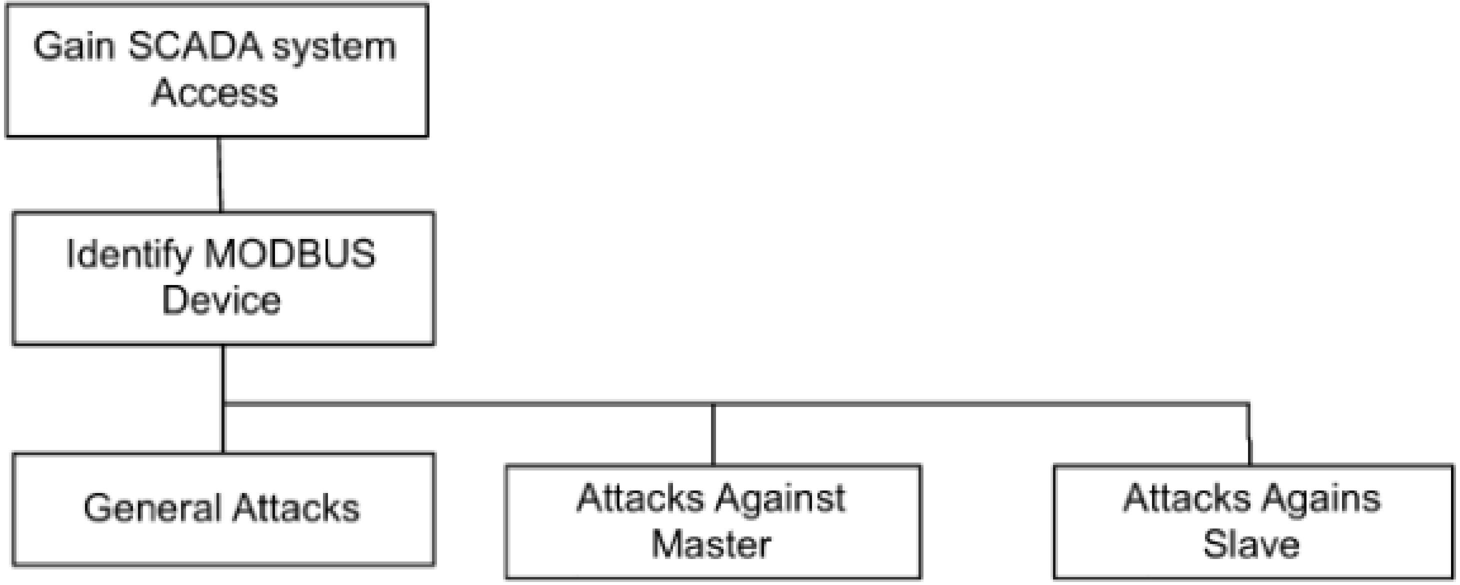
Catastrophic disruptions to the transportation system.

–A vessel sunk in a shipping channel, an explosion at an oil or LNG facility, sabotage to canal locks, or a series of mishaps involving cargo container cranes in critical ports can have long-term impacts to the safety, stability and reliability of elements of the transportation system.

Source: Volpe, 2013

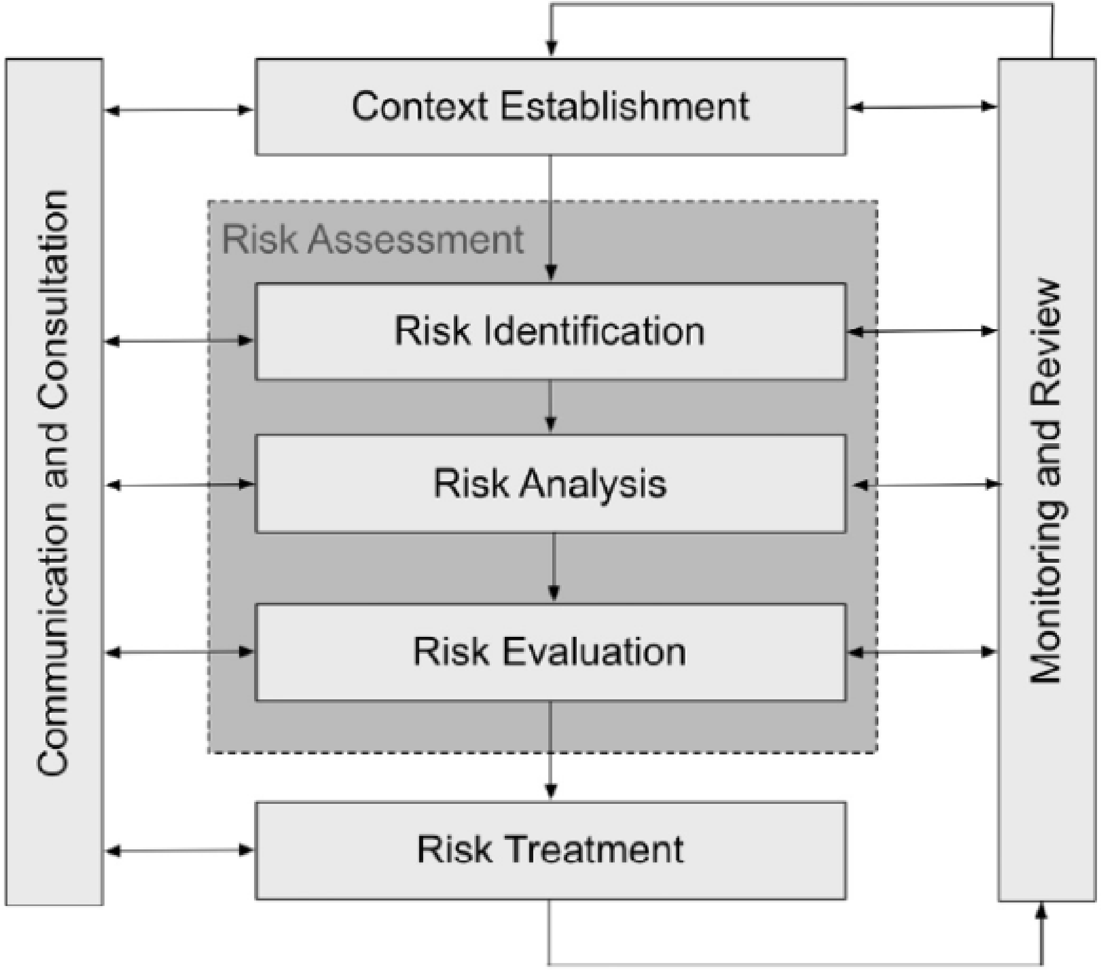
Types and Impacts of Exploiting ICS(3)

Attack Tree for MODBUS – based SCADA system



MODBUS: is a serial communications protocol for use with its programmable logic controllers (PLCs)

Risk management process (ISO)



A review of Cyber security methods for SCADA (Y.Cherdanseva et.all 2016)

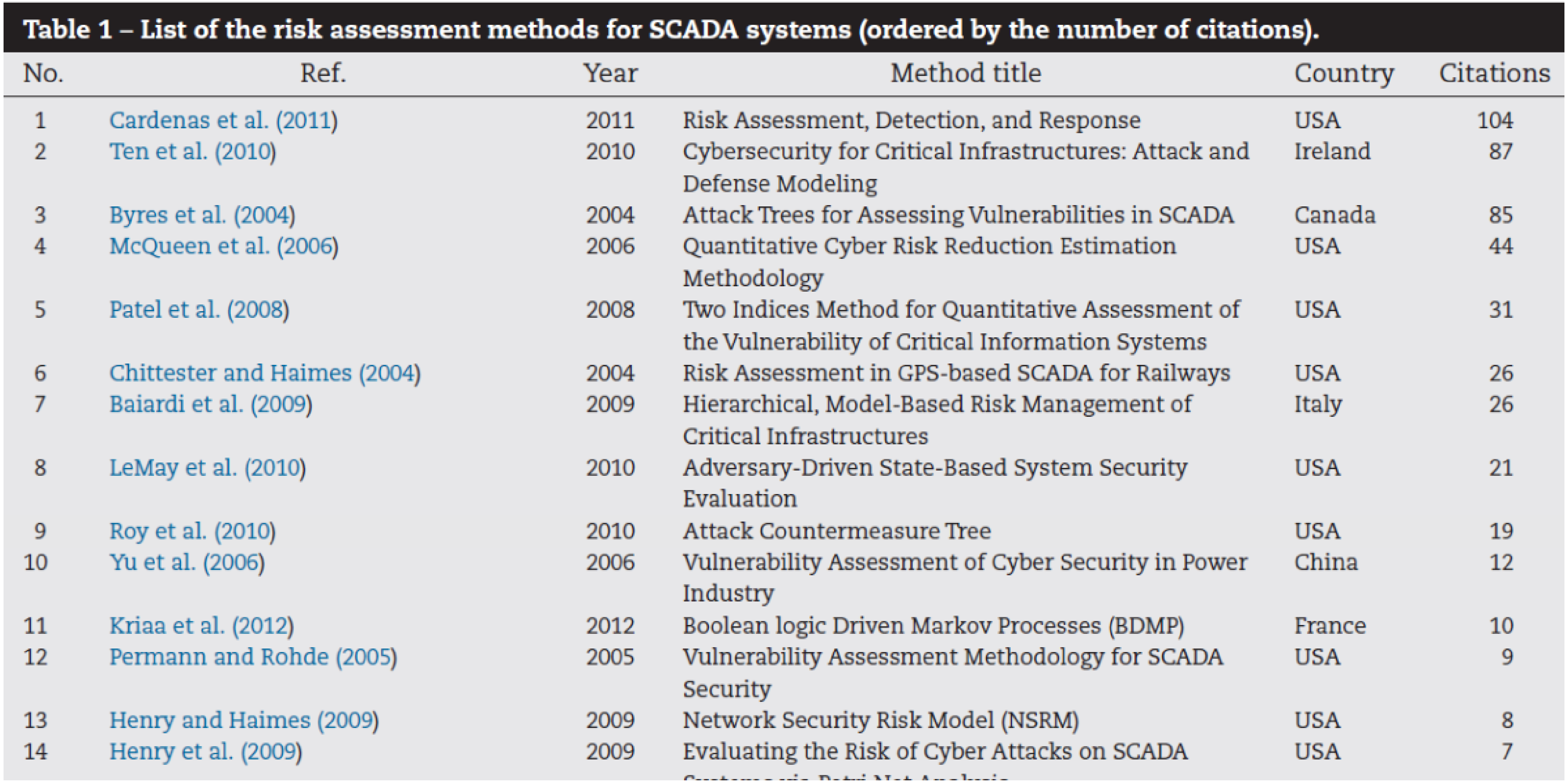


Table 1 – List of the risk assessment methods for SCADA systems (ordered by the number of citations).

No.	Ref.	Year	Method title	Country	Citations
1	Cardenas et al. (2011)	2011	Risk Assessment, Detection, and Response	USA	104
2	Ten et al. (2010)	2010	Cybersecurity for Critical Infrastructures: Attack and Defense Modeling	Ireland	87
3	Byres et al. (2004)	2004	Attack Trees for Assessing Vulnerabilities in SCADA	Canada	85
4	McQueen et al. (2006)	2006	Quantitative Cyber Risk Reduction Estimation Methodology	USA	44
5	Patel et al. (2008)	2008	Two Indices Method for Quantitative Assessment of the Vulnerability of Critical Information Systems	USA	31
6	Chittester and Haimes (2004)	2004	Risk Assessment in GPS-based SCADA for Railways	USA	26
7	Baiardi et al. (2009)	2009	Hierarchical, Model-Based Risk Management of Critical Infrastructures	Italy	26
8	LeMay et al. (2010)	2010	Adversary-Driven State-Based System Security Evaluation	USA	21
9	Roy et al. (2010)	2010	Attack Countermeasure Tree	USA	19
10	Yu et al. (2006)	2006	Vulnerability Assessment of Cyber Security in Power Industry	China	12
11	Kriaa et al. (2012)	2012	Boolean logic Driven Markov Processes (BDMP)	France	10
12	Permann and Rohde (2005)	2005	Vulnerability Assessment Methodology for SCADA Security	USA	9
13	Henry and Haimes (2009)	2009	Network Security Risk Model (NSRM)	USA	8
14	Henry et al. (2009)	2009	Evaluating the Risk of Cyber Attacks on SCADA Systems via Petri Net Analysis	USA	7

Challenging issues

- Dealing with fragmentation
- Overcoming attack- or failure-orientation
- Search for reliable sources of data
- Improving validation of risk assessment methods
- Supporting risk management methods with elaborate tools

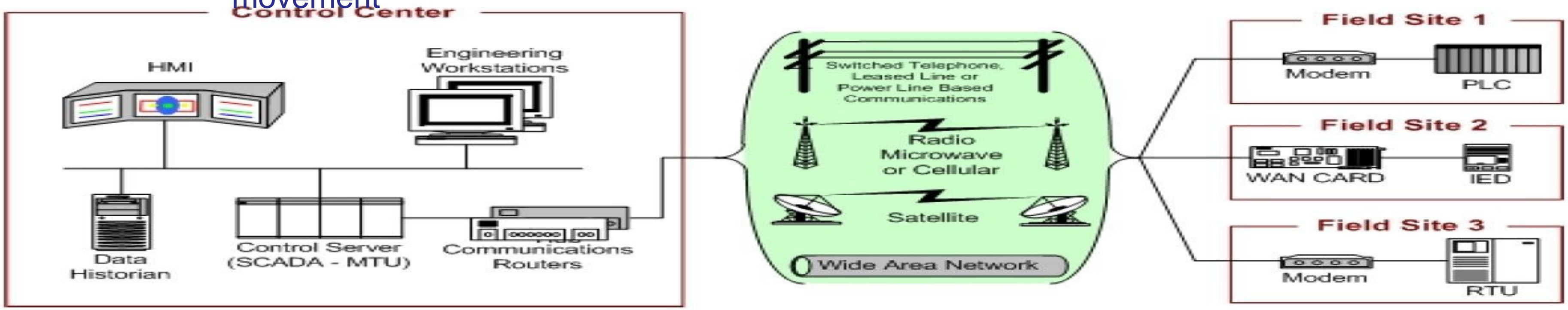
Industrial Control Systems (ICS)

BlackEnergy

- Sophisticated campaign
- Ongoing since at least 2011
- Highly modular
- Targets human-machine interfaces (HMI)
- Modules search out network-connected file shares and removable media for lateral movement

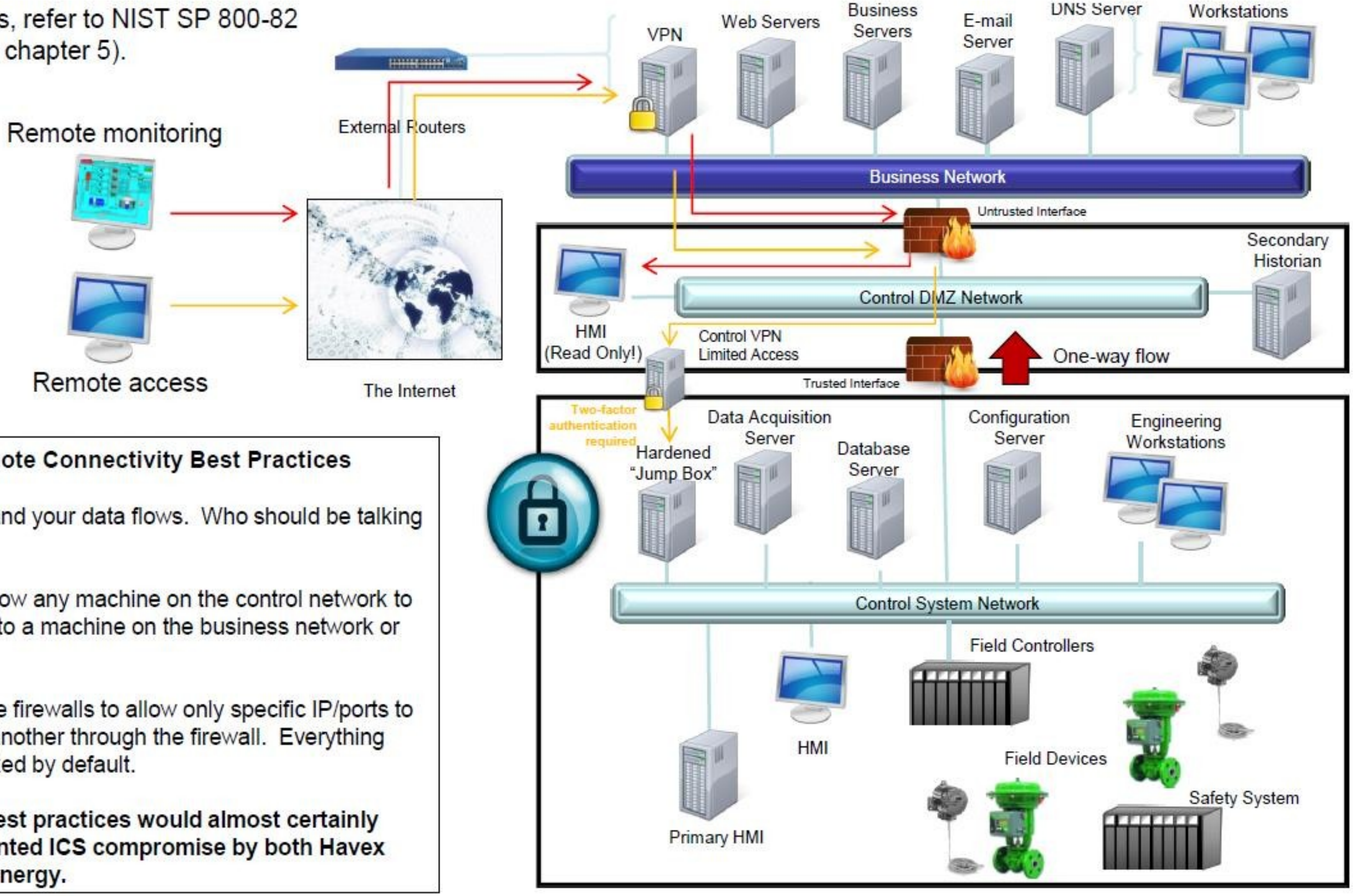
Havex

- Remote Access Trojan
- Multiple infection vectors (phishing, website redirects, watering hole attacks on ICS vendor websites)
- Targeted energy and oil sectors
- ICS/SCADA scanning



ICS Best Practices – Modern Connectivity

For specifics, refer to NIST SP 800-82 (specifically chapter 5).



Remote Connectivity Best Practices

1. Understand your data flows. Who should be talking to who?

2. Never allow any machine on the control network to talk directly to a machine on the business network or Internet

3. Configure firewalls to allow only specific IP/ports to talk to one another through the firewall. Everything else is blocked by default.

4. These best practices would almost certainly have prevented ICS compromise by both Havex and BlackEnergy.

Source: USCG

UNIVERSITY OF THE AEGEAN

Department of Shipping Trade and Transport

Thank you for your attention

nnik@aegean.gr