www.crysys.hu

Industrial Control Network Security
Critical Infrastructure Protection

Tamás Holczer

CrySyS Lab

Budapest University of Technology and Economics

holczer@crysys.hu

Critical infrastructures (CIs)

- assets that are essential for the functioning of a society and economy
  - energy generation and distribution
    - electricity generation, transmission and distribution;
    - gas production, transport and distribution;
    - oil and oil products production, transport and distribution;
  - food and water supply
    - drinking water production and distribution, waste water/sewage management;
    - food production and distribution;
  - transportation systems
    - fuel supply;
    - railway network;
    - airports and harbors;
  - telecommunication systems
    - wired and wireless network infrastructures (landline phone, mobile, Internet);
  - basic services
    - public health (hospitals, ambulances);
    - financial services (banking, clearing);
    - security services (police, military);

Security of CIs

- CIs increasingly use computer based systems for process control, system monitoring, and storage of information
- computer based systems in CIs more and more resemble those in corporate office environments
  - programmable devices
  - networks
  - multitude of interfaces, interconnected sub-systems
  - interoperability supported by standards
  - service oriented architectures
  - remote access and management via public networks
- computer based CIs face security challenges similar to those in corporate environments with potentially more serious consequences of successful attacks

Outline

- Industrial Control Systems (ICS)
- ICS specific security challenges and vulnerabilities
- Computer security in ICS systems
  - network segmentation
  - defense-in-depth
  - incident response

Industrial Control Systems (ICS)

- general term that encompasses different types of control systems used in industrial environments

  - SCADA – Supervisory Control and Data Acquisition
    - highly distributed, geographically dispersed assets
    - centralized data acquisition and control

  - DCS – Distributed Control System
    - production system within the same geographic location
    - different sub-systems responsible for controlling localized processes
    - supervisory level of control overseeing the sub-systems

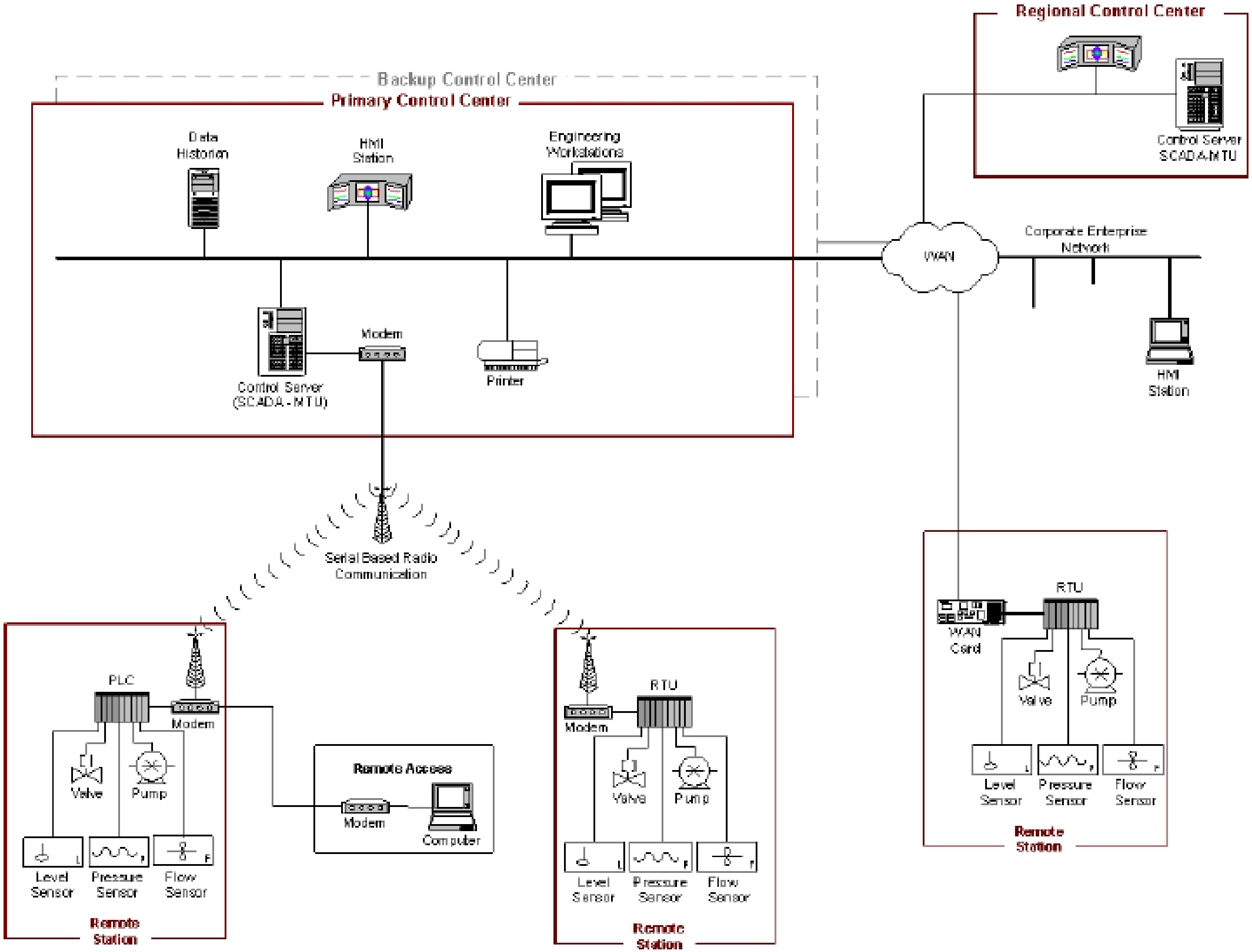
ICS components, networks, and protocols

- components
  - SCADA server / Master Terminal Unit (MTU)
  - Programmable Logic Controller (PLC) / Remote Terminal Unit (RTU)
  - Intelligent Electronic Devices (IED)
  - Human Machine Interface (HMI)
  - Data Historian

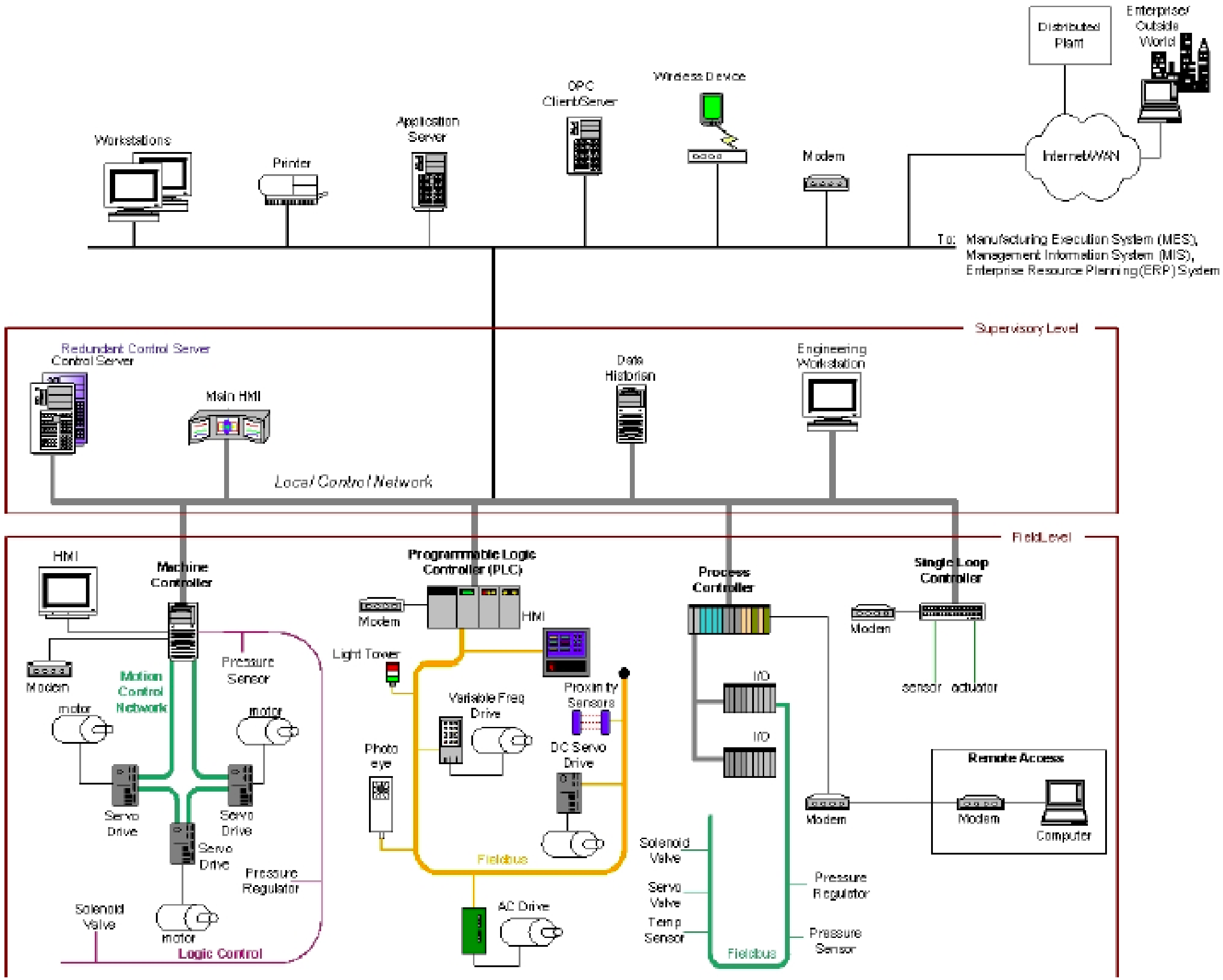
- networks
  - control network
  - field network
  + firewalls, routers, remote access points

- protocols
  - modbus, DNP3, IEEE 802.x, ZigBee, Bluetooth
  - proprietary (e.g., Step7)

SCADA example

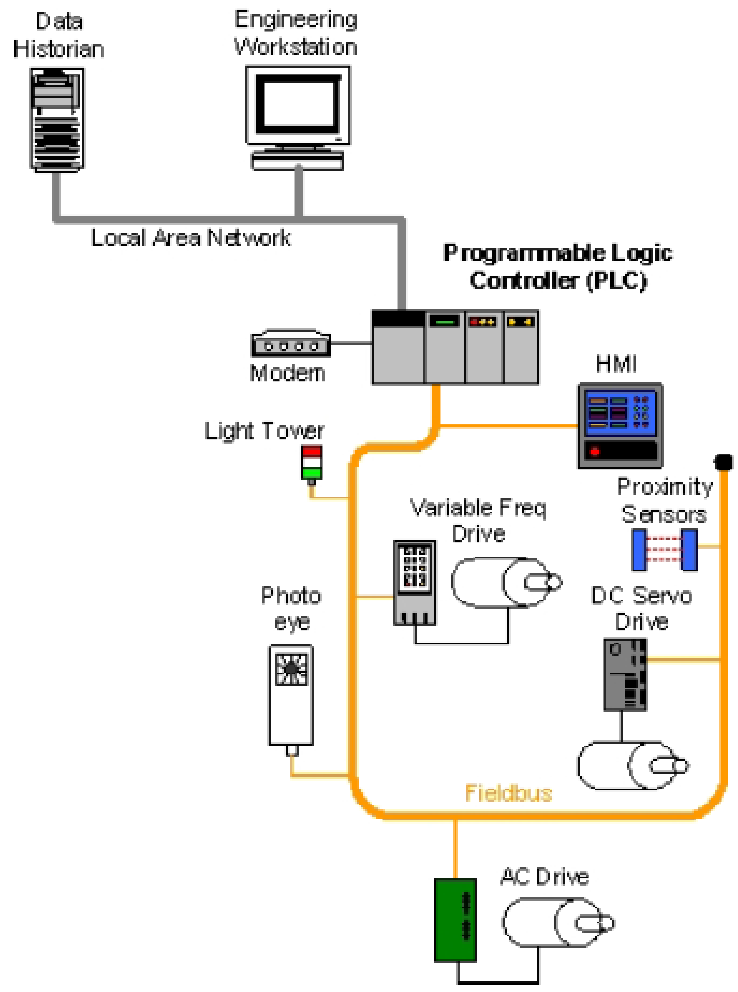


DCS example



Distributed Plant
Enterprise/ Outside World
Workstations
Printer
Application Server
OPC Client/Server
Wireless Device
Modem
Internet/WAN
To: Manufacturing Execution System (MES), Management Information System (MIS), Enterprise Resource Planning (ERP) System
Supervisory Level
Redundant Control Server
Control Server
Main HMI
Data Historian
Engineering Workstation
Local Control Network
Field Level
HMI
Machine Controller
Modem
Motion Control Network
Pressure Sensor
motor
Servo Drive
Pressure Regulator
Solenoid Valve
Logic Control
Programmable Logic Controller (PLC)
Light Tower
Photo eye
Variable Freq Drive
Proximity Sensors
DC Servo Drive
Fieldbus
AC Drive
Process Controller
I/O
Solenoid Valve
Servo Valve
Temp Sensor
Pressure Regulator
Pressure Sensor
Single Loop Controller
sensor
actuator
Remote Access
Computer

PLC example


Data
Historian
Engineering
Workstation
Local Area Network
Programmable Logic
Controller (PLC)
Modem
HMI
Light Tower
Proximity
Sensors
Variable Freq
Drive
Photo
eye
DC Servo
Drive
Fieldbus
AC Drive

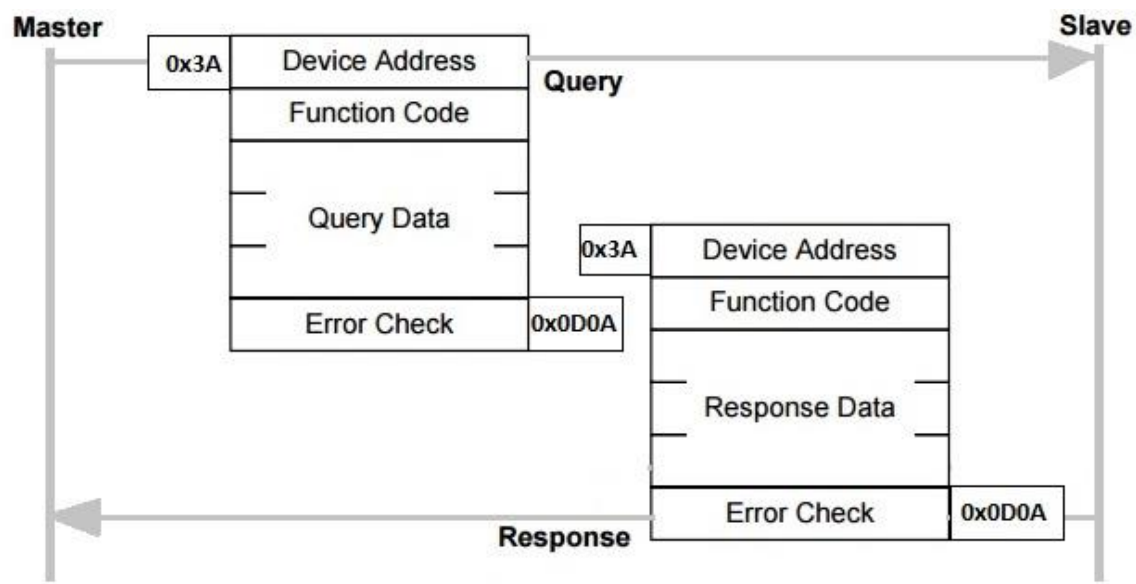
Industrial protocols

- Hundreds of open and closed protocols
- Moving towards TCP/IP
- Real-time requirements
  - Hard real-time: no missed deadline, ~10 ms
  - Soft real-time: some missed deadline, ~100 ms
  - Non real-time: best effort, ~ 1s (but 1Gb Ethernet ~ns)

- Long (but not complete) list for the interested: https://en.wikipedia.org/wiki/List_of_automation_protocols

Industrial protocols: Modbus

- Open protocol
- Developed by Modicon/Schneider in 1979
- De facto standard between industrial electronic devices
- Serial or TCP/IP communication (UDP also exists)
- Good for small data: bit (coil) and word (register), no complex data structures
- No security
- Non (soft) real-time
- Easy to implement

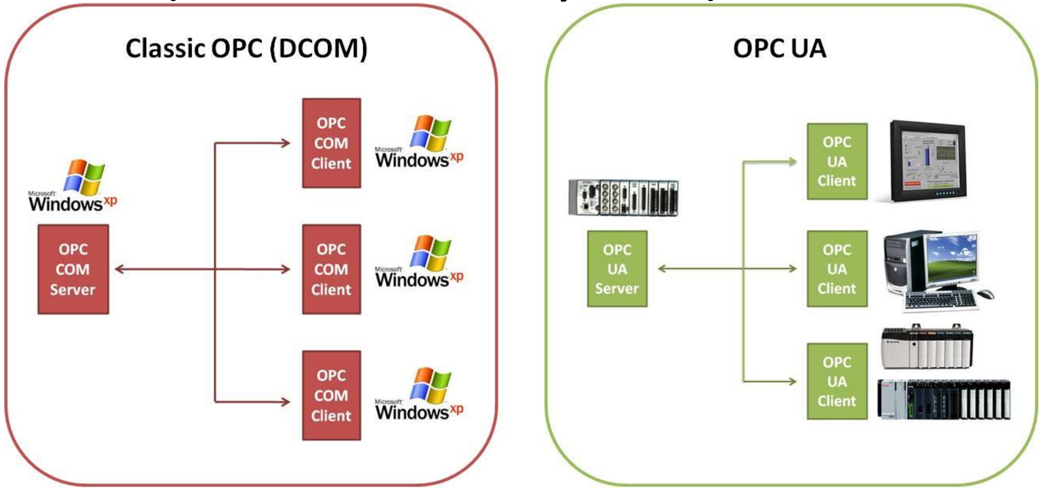


Modbus Message Frames

Industrial protocols: OPC UA

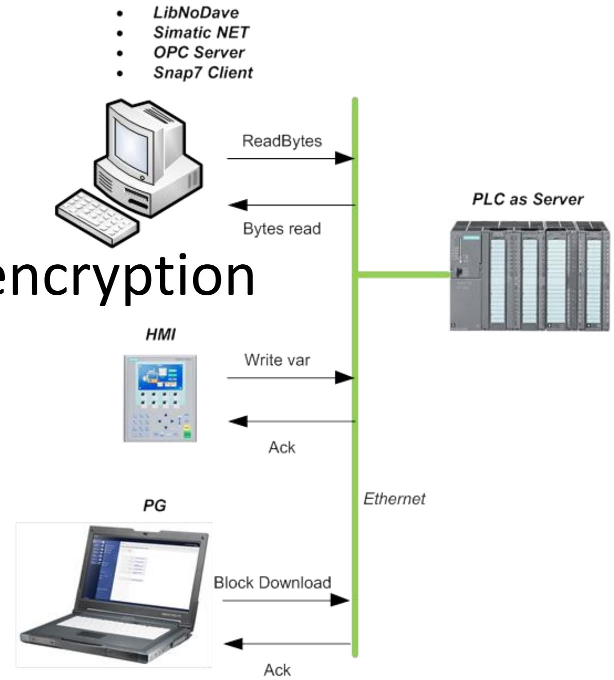
- First version: 2006, current version: 2015
- Machine to machine protocol
- Different vendor's devices can communicate through a common OPC server
- Very complex protocol (~1000 pages)
- Developed with security in mind
- Language and OS independent (c, Java, .NET, Python)
- Open GPL license
- Open Platform

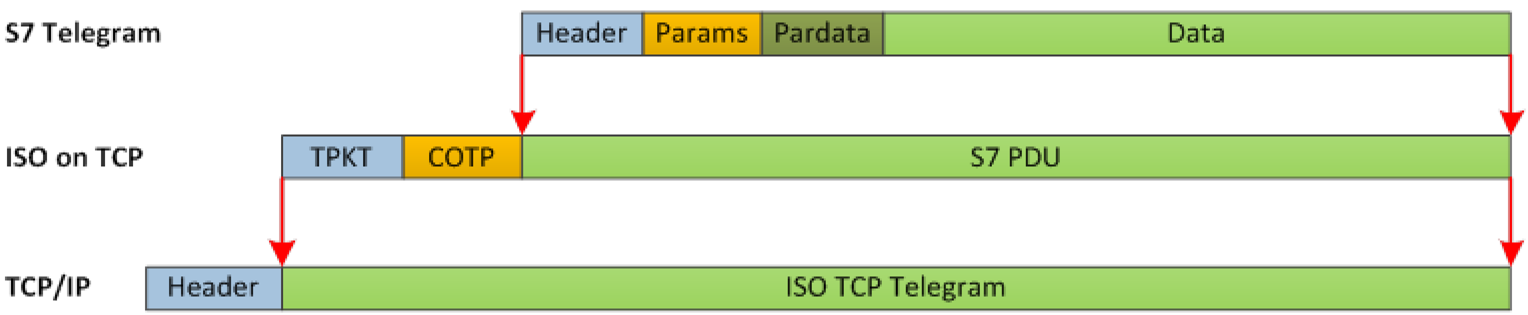
  Communications



Industrial protocols: Siemens S7

- Closed protocol
- Request-response communication
- New variants with integrity protection, encryption





Protocols Encapsulation

ICS specific challenges

- performance requirements
  - real-time, time critical systems (delays, jitter are not acceptable)
  - modest throughput
- availability requirements
  - redundant systems
  - planned outages and maintenance
  - exhaustive pre-deployment testing (including security tools and patches)
  - long lifetime (15-20 years)
- risk management requirements
  - human safety and protection of processes
  - availability vs. confidentiality
- architecture differences
  - proprietary OS, lack of security mechanisms
  - besides standards, many proprietary communication protocols
  - resource constraints on field devices
  - physical access to components may be difficult

Threats

- hacktivists
  - aim for challenge and/or political goal
  - easy access to different attack tools
- organized criminal groups
  - aim for monetary gain
  - well organized, plenty of resources
- industrial spies
  - information gathering and cyber espionage
- terrorists
  - sabotage, disruption of operation
- foreign intelligence services
  - information gathering and cyber espionage
  - sabotage, disruption of operation
  - ”unlimited” resources
- insiders
  - internal knowledge, special privileges

ICS vulnerability categories

- policy and procedural vulnerabilities
- platform vulnerabilities
  - configuration
  - software
  - hardware
  - malware protection
- network vulnerabilities
  - configuration
  - hardware / firmware
  - monitoring and logging
  - communications
  - wireless connections

Additional risk factors

- adoption of standardized protocols and technologies with known vulnerabilities
  - transitioning from proprietary systems to less expensive and more performant standardized technologies
    - » Microsoft Windows and Unix-like operating systems
    - » TCP/IP protocol stack, OPC (OLE for Process Control)
- connectivity of the control systems to other networks
  - demand for remote access
  - connections between corporate networks and ICS networks
  - use of WANs and the Internet to transmit data within the control system
- insecure and rogue connections
  - dial-up modems open for remote diagnostics, maintenance, and monitoring
  - insecure wireless access
- public availability of technical information about control systems
  - open standards and technical information are available on the Internet

Security program for ICS

- effectively integrating security into an ICS requires defining and executing a comprehensive program
  - obtain senior management buy-in
  - build and train a cross-functional team
  - define charter and scope
  - define specific ICS policies and procedures
  - identify and inventory ICS assets
    - commercial enterprise inventory tools are available, but...
    - teams should first conduct an assessment of how these tools work and what impact they might have on the connected control equipment
  - perform a risk and vulnerability assessment
  - define the mitigation controls
  - provide training and raise security awareness for ICS staff

Network architecture design principles

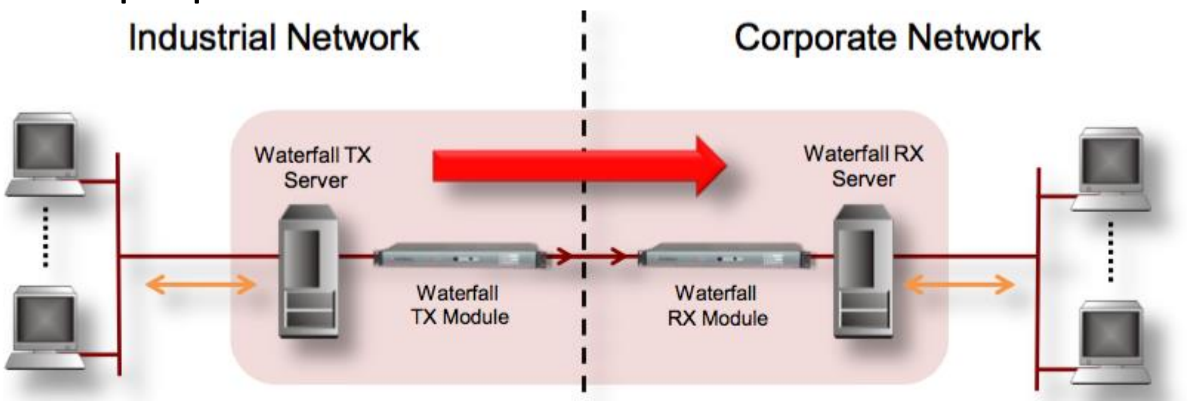
- it is usually recommended to separate the ICS network from the corporate network
  - Internet access, FTP, e-mail, and remote access will typically be permitted on the corporate network but should not be allowed on the ICS network
  - rigorous change control procedures for network equipment, configuration, and software may not be in place on the corporate network, but should be required for the ICS network
- practical considerations may require a connection between the ICS and corporate networks
  - it is strongly recommended that only minimal (single if possible) connections be allowed and it should be through a firewall and a DMZ
  - servers containing data from the ICS that needs to be accessed from the corporate network should be put in the DMZ
  - only these systems should be accessible from the corporate network

Countermeasures

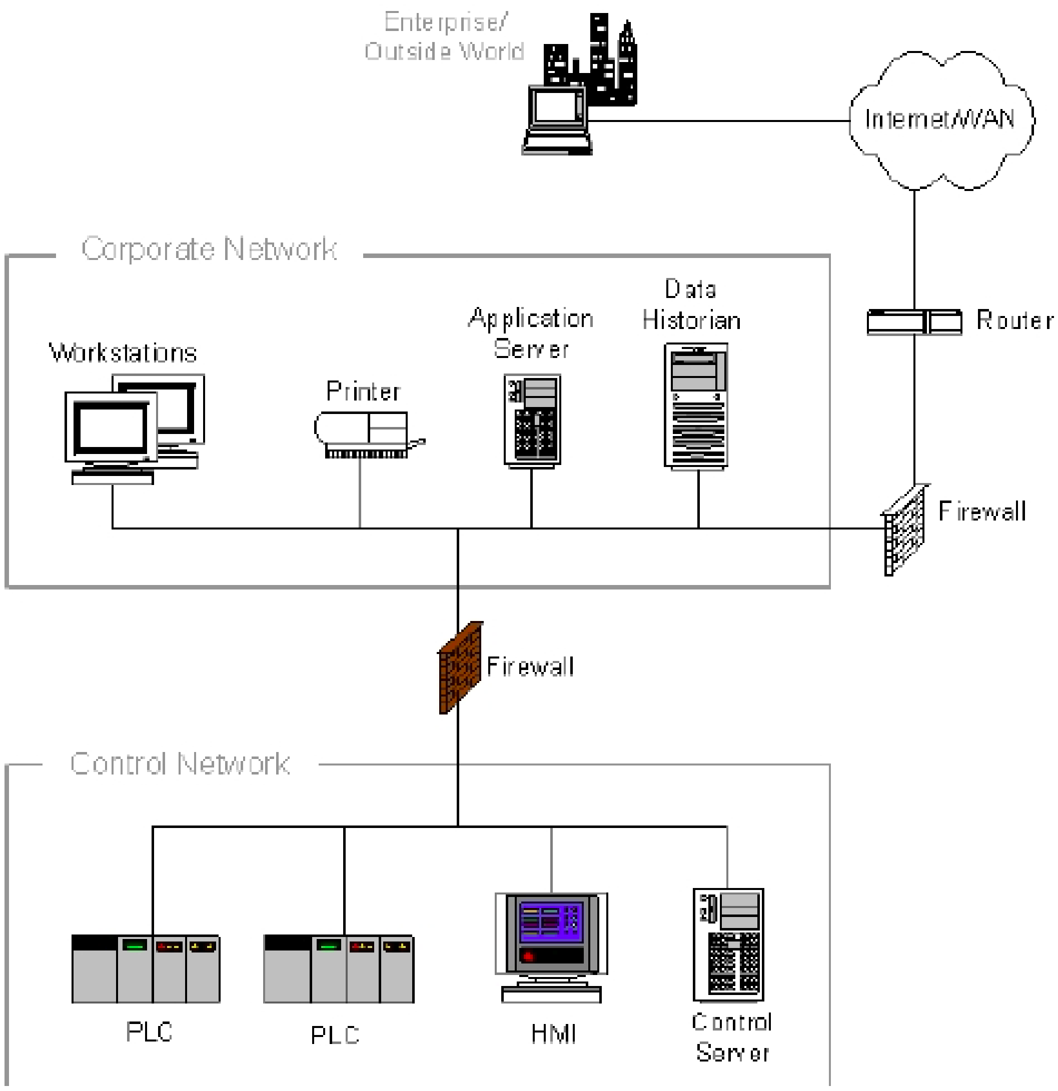
- Policy, policy, and more policy
- Firewalls (hard(?) to configure well)

} Must

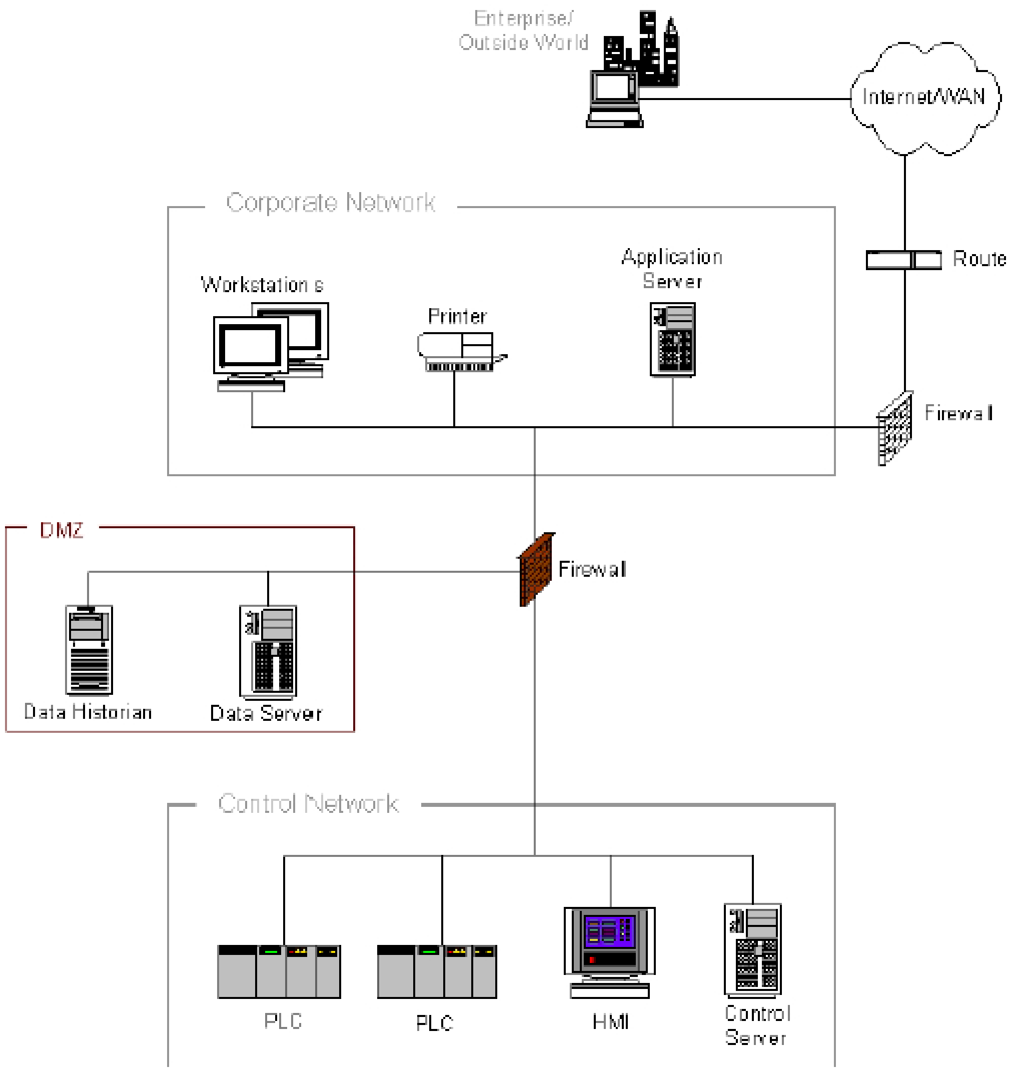
- Read only drives (write only with PIN)
- Unidirectional gateways, diodes
- Air-gapped network, but is it possible?
  - Time sync
  - Power consumption
  - USB drives, maintenance laptops
- Anomaly detection
  - Predictable traffic
  - Future?



Minimum setup



Desired setup



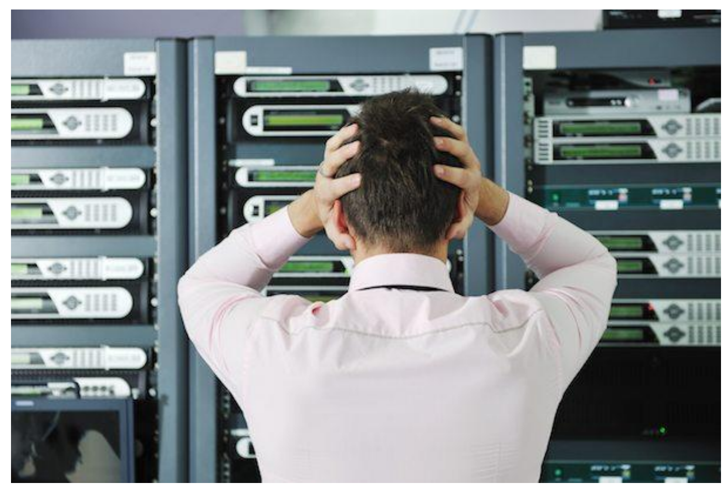
More design principles

- apply technologies at more than just the network layer
- use the principles of least privilege and need-to-know
  - if a system doesn’t need to communicate with another system, it should not be allowed to
- implement whitelisting instead of blacklisting
  - grant access to the known good, rather than deny access to the known bad
  - the set of applications is essentially static, making whitelisting practical
- protect information and infrastructure based on security requirements
  - use different security mechanisms in different risk environments
  - the most critical components require more strict isolation

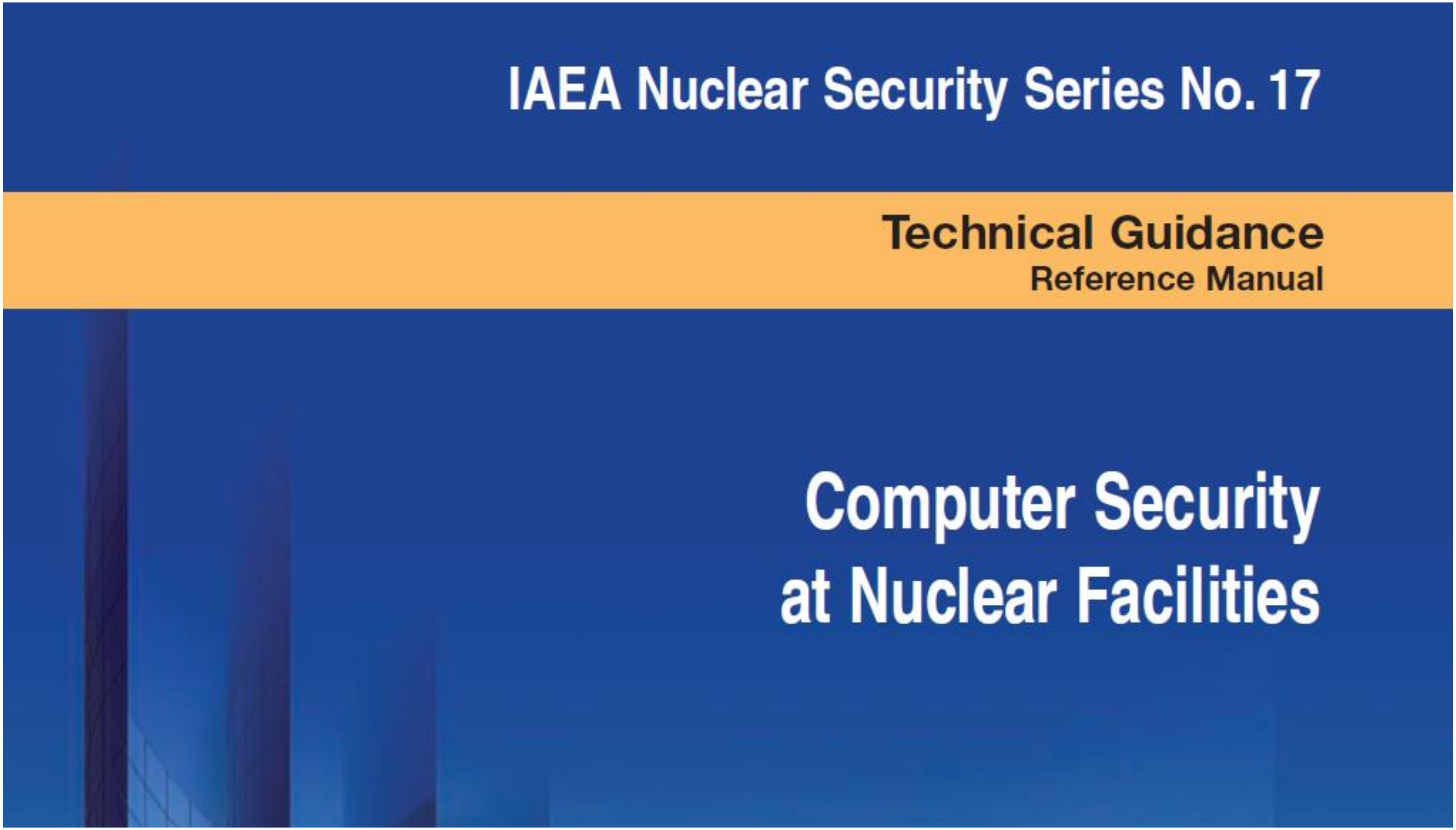
Design-basis threat

- Used mainly in nuclear industry
- Profile of the type, composition, and capabilities of an adversary
- Base to design safeguards
- Operators must demonstrate they can defend against DBT
  - Stronger attackers are out of scope (national responsibility)
- Hard to write cyber DBT, hard to demonstrate preparedness

Protecting nuclear facilities requires all the security features to come together and work as one.



Defense-in-depth in IAEA style



”Graded approach”

- security measures are applied proportional to the potential consequences of an attack
  - categorize computer systems into *zones* (co-located computers with the same or similar importance concerning safe and secure operation)
  - assign a *security level* to each zone
  - apply protective measures to zones based on their security level
  - use decoupling mechanisms for data flow at zone borders (e.g., data diode)

zones vs security levels

- zones are logical and physical grouping of computer systems
- security levels represent the degree of protection required

Examples for security levels

- generic (applied everywhere)
  - appropriate access control and user authentication are in place
  - system vulnerability assessments are undertaken periodically
  - ...
- level 5 (least secure)
  - only approved users are allowed to make modifications
  - access to the Internet is allowed (with adequate protection)
  - remote external access is allowed for authorized users
- level 4
  - only approved users are allowed to make modifications
  - access to the Internet may be given (with adequate protection)
  - remote maintenance access is allowed and controlled
  - system functions available to users are controlled by access control mechanisms
  - security gateways are used for isolation

Examples for security levels

- level 3
  - access to the Internet is not allowed
  - remote maintenance access is allowed on a case by case basis
  - logging and audit trails for key resources are monitored
  - system functions available to users are controlled by access control mechanisms, and based on the ‘need to know’ principle
  - security gateways are used for isolation

- level 2
  - only an outward, one-way data flow is allowed from level 2 to level 3
  - remote maintenance access may be allowed on a case by case basis
  - the number of staff given access to the systems is kept to a minimum
  - physical connections to the systems should be strictly controlled

Examples for security levels

- level 1 (most secure)
  - only strictly one-way, outward communication is allowed (data must flow out, not even acknowledgments and signalization can flow in)
  - no remote maintenance access is allowed
  - physical access to systems is strictly controlled
  - the number of staff given access to the systems is limited to an absolute minimum
  - two person rule is applied to any approved modifications
  - all activities should be logged and monitored

Examples for zones

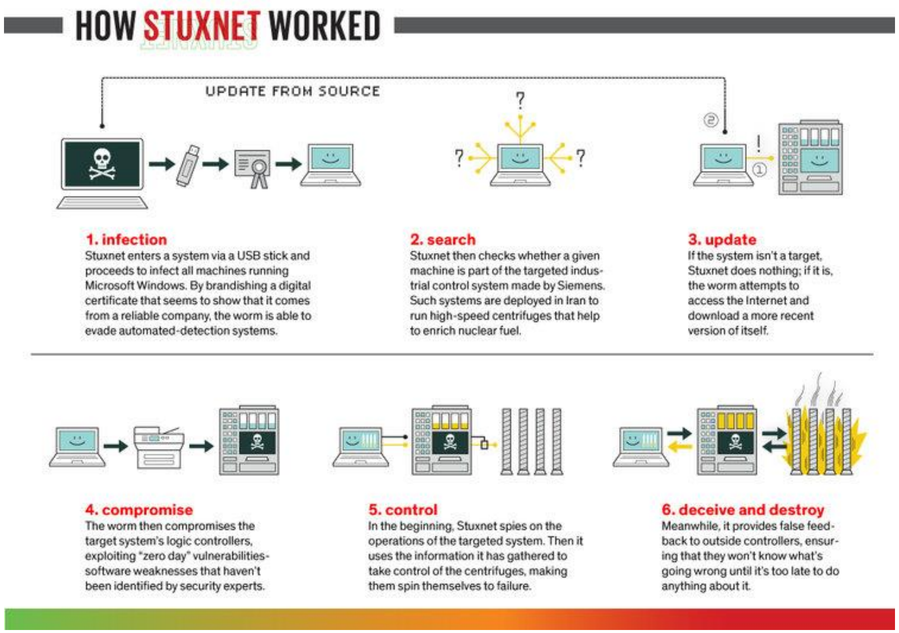
- systems that are vital to the facility and require the highest level of security (e.g., nuclear protection systems)
- operational control systems
- real time supervision systems not required for operations (e.g., process supervision system in a control room)
- technical data management systems used for maintenance or operation activity management (e.g., work order management, documentation management)
- systems not directly important to technical control or operational purposes (e.g. office automation systems)

SHODAN


SHODAN
Search
EXPOSE ONLINE DEVICES.
WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.
TAKE A TOUR
FREE SIGN UP
Popular Search Queries:
default password - Finds results with "default password" in the banner; the named defaults might work!

Well known attacks: Stuxnet

- Worm, found in 2010 (probably started in around 2005)
- Most probably against Iran’s Nuclear program
- 4 zero days against Microsoft Windows
- Makes centrifuges spin over and under the critical speed
- Infection by USB flash drives
- Attacks Siemens Step7 software
- Modifies operation of the PLCs
- Shows normal values to operators



Well known attacks: Black energy

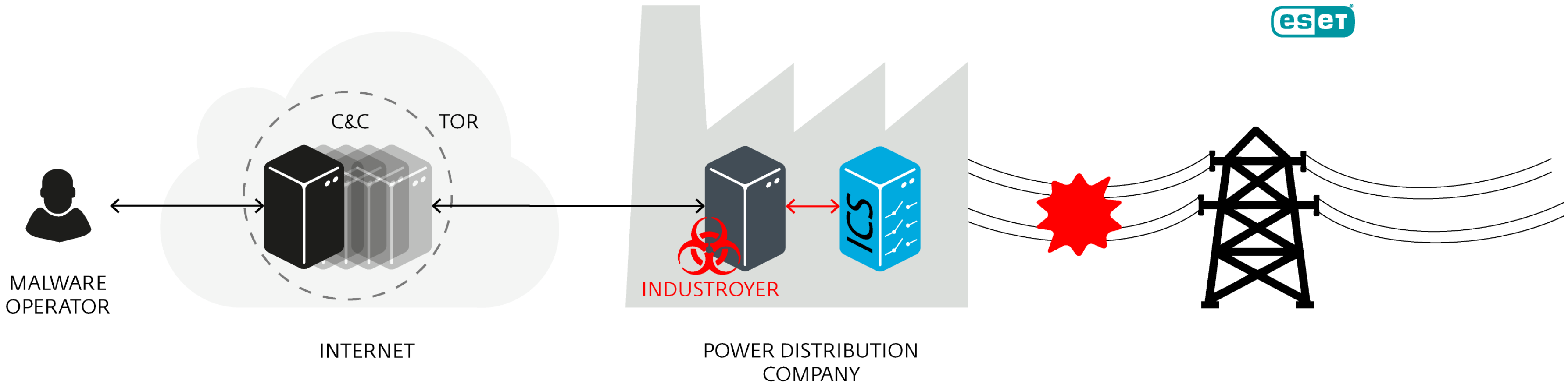
- Attacks against Ukraine in 2015 December
- Also attacks in 2014 in Ukraine and Poland
- Information collection
- KillDisk: electrical power industry (see some targets below left) and news media (see some targets below right)
- Terminate ELTIMA Serial to Ethernet Connector process
- Install SSH server (Dropbear SSH) with predefined password (passDs5Bu9Te7)

```
unicode 0, <.crt.bin.exe.db.dbf.pdf.djvu.doc.docx.xls.xlsx.jar.ppt.pp>
unicode 0, <tx.tib.vhd.iso.lib.mdb.accdb.sql.mdf.xml.rtf.ini.cfg.boot>
unicode 0, <.txt.rar.msi.zip.jpg.bmp.jpeg.tiff>,0
```

```
unicode 0, <a.ivf.ivr.ivs.izz.izzy.jmv.jss.jts.jtv.k3g.kmv.lrec.lrv.l>
unicode 0, <sf.lsx.lvix.m15.m1pg.m1v.m21.m21.m2a.m2t.m2ts.m2v.m4e.m4u>
unicode 0, <.m4v.m75.mani.meta.mgv.mj2.mjp.mjpg.mk3d.mkv.mmv.mnv.mob.>
unicode 0, <mod.moff.moi.moov.mov.movie.mp21.mp21.mp2v.mp4.mp4.infovi>
unicode 0, <d.mp4v.mpe.mpeg.mpeg1.mpeg4.mpf.mpg.mpg2.mpgindex.mpl.mpl>
unicode 0, <s.mpsub.mpv.mpv2.mqv.msdvd.msh.mswmm.mts.mtv.mvb.mvc.mvd.>
unicode 0, <mve.mvex.mvp.mvy.mxf.mxv.mys.ncor.nsv.nut.nuv.nvc.ogm.ogv>
unicode 0, <.ogx.orv.otrkey.par.pds.pgi.photoshow.piv.pjs.playlist.pl>
unicode 0, <proj.pmf.pmv.ppj.prel.pro.pro4dvd.pro5dvd.proqc.prproj.pr>
```

Well known attacks: Crash Override

- December 2016
- Black out in Kiev for an hour
- Test or proof of competence of code
- Alternative name: Industroyer
- Controlls switches and circuit breakers
- Analysed by ESET and Dragos Inc.

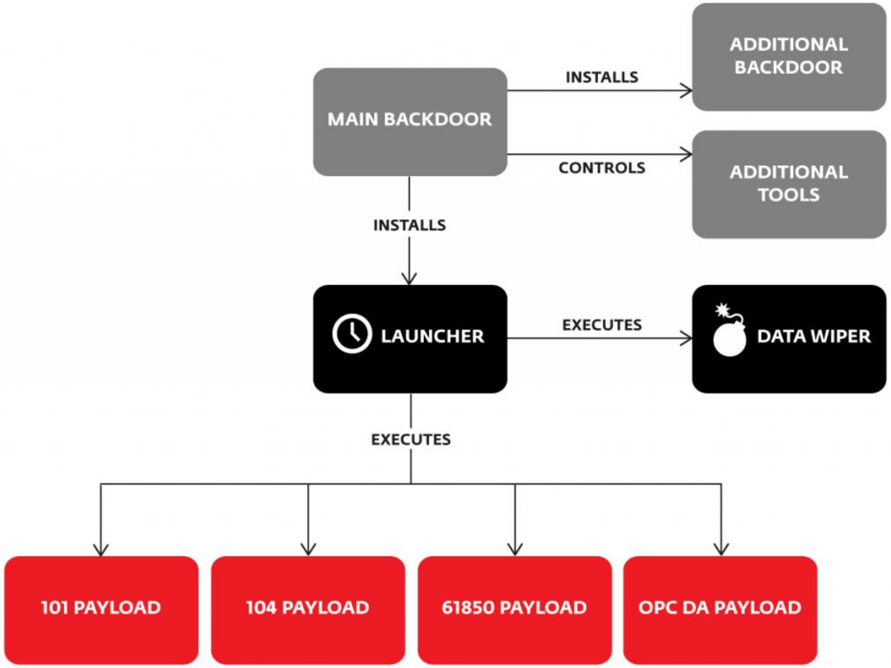


Well known attacks: Crash Override 2.

- Installs backdoor
- „Normal” use of: IEC 60870-5-101, IEC 60870-5-104, IEC 61850, and OLE for Process Control Data Access (OPC DA)
- C&C: Tor, non-working hours
- Extra backdoor ~ Notepad
- Wiper: registry, files
- CVE-2015-5374 (DoS) against

  Siemens SIPROTECT,

  61850 protocol



Incident response

- incidents happen despite all precautions
- incidents must be handled in a controlled manner
- efficient incident handling requires
  - proper preparation
  - fast detection
  - evidence collection and analysis (who, what, how, ...)
  - containment and recovery
  - post-incident activities (feeding back lessons learned)
- incident response is hard in any environment, but ICS systems have their additional specific challenges

Preparation

- computer security incident response policy
- computer security incident response plan and procedures
- Computer Security Incident Response Team (CSIRT)
  - establishment
  - training and exercises
  - tools
- attack prevention and detection tools
- log collections
- backups

Evidence collection and analysis

- evidences
  - log files
  - network traces
  - memory content of devices
  - storage media

- ICS related challenges:
  - logging is not supported on controllers (or very limited)
  - controllers may not be stopped to retrieve log storage media
  - retrieving log files via the network may generate large amount of traffic
  - network traffic capture not supported on control equipment
  - no free span ports may be available on networking equipment
  - memory dump not supported on control equipment
  - live data collection and analysis affects the system and may destroy evidence

Containment and recovery

- goal: prevent escalation of incident and ensure restoration of normal operational conditions
- recovery needs backups (golden images, approved configuration settings)

- ICS related challenges:
  - failed containment or simply too slow reaction may have fatal consequences
  - containment may require isolating subsystems or stopping services, but such steps may affect operational conditions, including safety
  - recovery from backups may require stopping an entire subsystem
  - long outages may result in huge losses

IAEA incident severity categorization

- focuses on the impact of the incident
- severity category V
  - incidents that result in serious breaches of nuclear security and safety, usually with physical consequences
- severity category IV
  - incidents that may pose an immediate and severe threat to nuclear security and safety objectives
  - examples: successful system compromise, malware infection, denial of service
- severity category III
  - incidents that pose long term threats to computer security
  - examples: attempted intrusion, reconnaissence activity
- severity category II
  - exploits and activities that occurred elsewhere but could impact the nuclear facility
- severity category I
  - detection of a security vulnerability that could impact nuclear security and safety

Summary

- CIs are often based on ICS systems → we focused on ICS security, with some examples from the nuclear domain
- we gave an overview of
  - how ICS systems look like, and how they are different from traditional IT systems
  - the threats and vulnerability classes relevant for ICS systems
  - possible elements of a security program for ICS systems
- we looked at in more details
  - network segmentation
  - defense-in-depth (in the style of IAEA)
  - incident response challenges (and IAEA incident severity classes)

Further readings

- http://ics-cert.us-cert.gov/
- Bengt Gregory-Brown, Securing Industrial Control Systems-2017, SANS
- Guide to Industrial Control Systems (ICS) Security, NIST 800-82
- Managing Cybersecurity for Industrial Control Systems, https://www.ssi.gouv.fr, 2014
- IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities
- SCADASEC mailing list

Control questions

- What are the ICS specific challenges?
- Which network security tools can be used in ICS environment?
- Why IPS is NOT used in ICS networks?
- What is the difference between SCADA and DCS?
- What are security levels used for?
- Describe one ICS specific targeted attack!