UNIK 4750, Guest Lecture, 31.03.2016

Securing Networks for Industrial Automation and Control Systems

Who am I?

- Mushfiqur Rahman Chowdhury, Senior Engineer, Cyber Security & Infrastructure, ABB Oil Gas & Chemicals, ABB Norway
- Lecturer (10%) at UNIK (Currently main teacher at UNIK 4740, every fall)
- Doctorate from Department of Informatics, University of Oslo
- Previously
  - Scientist at ABB Corporate Research Center Norway
  - Postdoc and Research Fellow at UNIK
  - RF Engineer, Telenor/Grameenphone

- ABB a Swiss multinational company
- 135 000 employes (Dec. 2015); Rev. 35.5 billion USD (2015)
- World's leading power and automation company
- World's largest builder electricity grid

Projects

- Project Engineer, Johan Sverdrup (ABB scope), ongoing
- Project Engineer, Aasta Hansteen (ABB scope), ongoing
- Project Engineer, Valemon (ABB scope), finished, currently in production
- IT & Cyber Security Lead Engineer, Gina Krog (ABB scope), soon commissioning will be started

Stuxnet

- Found in 2010 in Iran
- Targets PLC and specifically the ones made by Siemens
- Interesting, some also believe Stuxnet was responsible for killing India's INSAT-4B satellite!!
- According to Symantec since 2010 more than 100 000 PCs infected, ~60% located in iran
- Believed that the malware was launched in 2009 and no. Of centrifuges dropped significantly in Natanz by the end of 2009!!

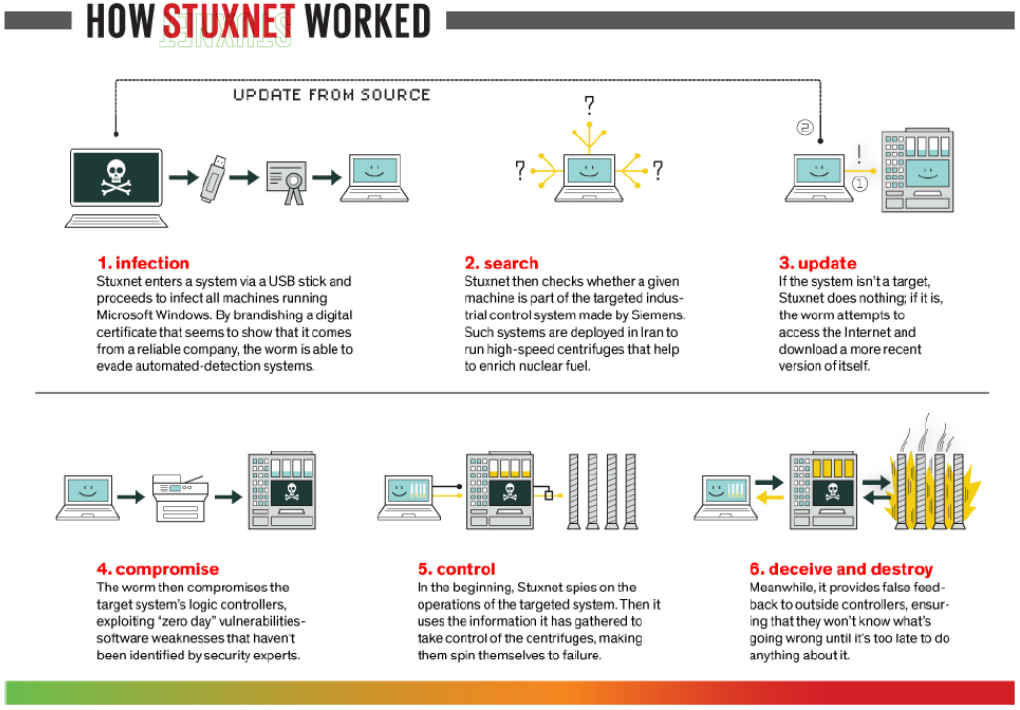


Figure 2: How Stuxnet worked [10].

- Report prepared with Stuxnet
- Good referencing style

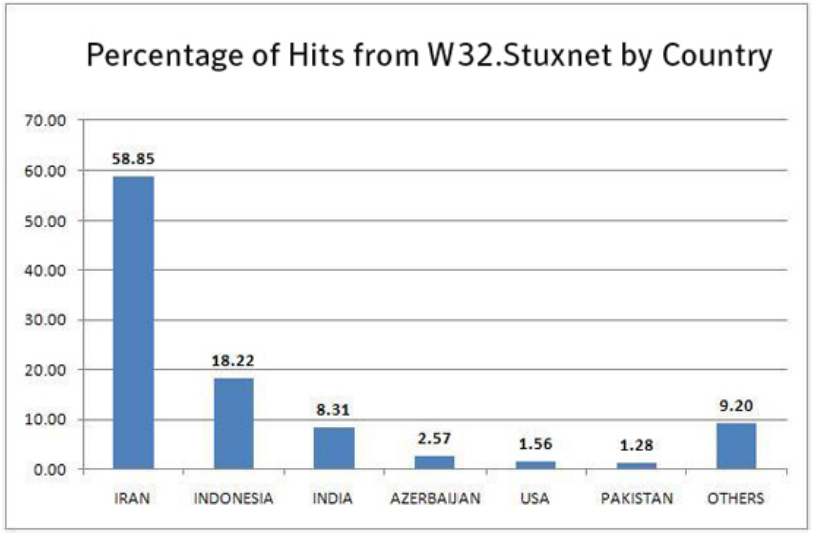


Figure 1: Percentage of hits by country [11].

Duqu

- A collection of malware discovered by security experts (team named CrySyS) in the Budapest Univ. Of Tec. and Economics in Hungary, in Oct. 2011
- Precursor to the next stuxnet (by Symantec, Nov 2011), W32.Duqu
- Similarities with Stuxnet, its modular design and how the moduels are combined to use them to target control systems in nuclear facilities
- It contains code that implements command & control, making it possible to control and pdate it as well as download and execute new payload using dummy .jpg files
- Duqu does not self-replicate

Generic mitigation steps:

1. Make sure all devices connected to the system has some sort of updated security software installed.
2. Keep all operating systems updated with the latest patches and fixes.
3. Disable mounting of USB flash drives.
4. Verify the sender of emails
5. Use extreme caution when opening Microsoft Office documents.

- Report prepared with Latex
- Very good detailes, e.g. include explanations of prerequisite knowledge such as on DLL; Drivers, signing, windows registry, RPC etc.
- Very structured

Duqu architecture

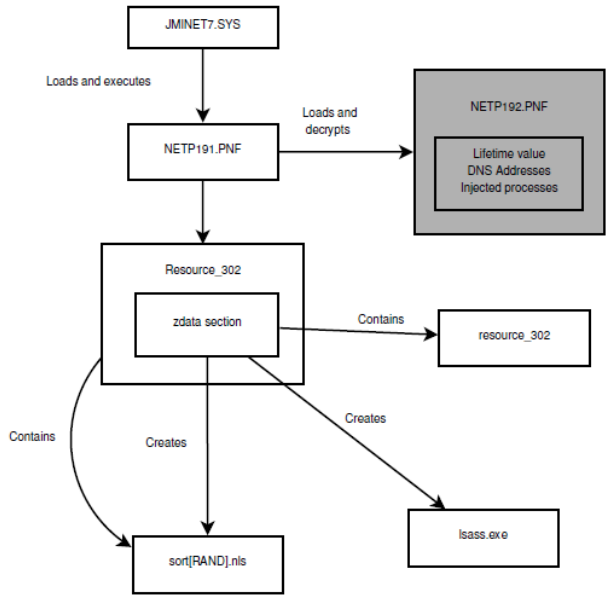
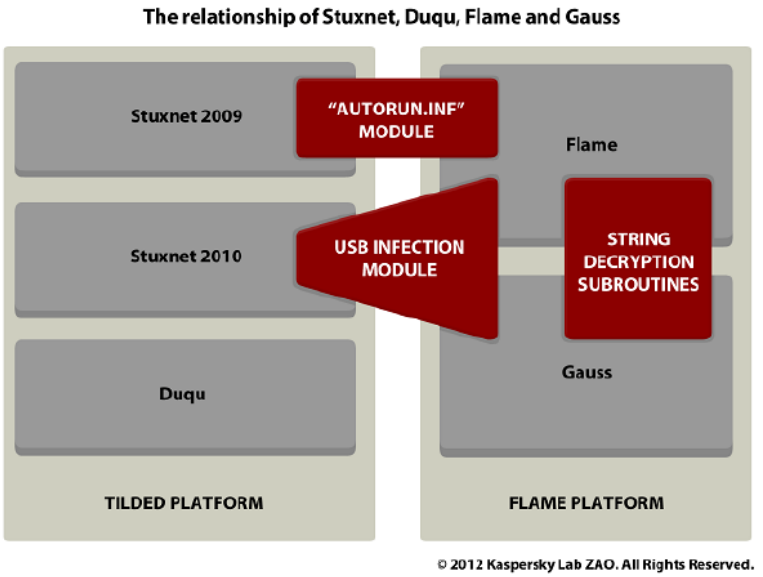


Figure C.1: Diagram showing the architecture of Duqu once installed. [6]

Gauss

- Gauss, a malware of type Cyber Cyberespionage, name came from the mathematician Johann Carl Friedrich Gauss, first discovered in 2012
- It a collection of packages, with modular design, has signature of several other malicious software, e.g. Stuxnet, Duqu, Flame etc.
- Since Gauss is modular, the operator (s) choose which modules to be loaded with the victims. he does not need information about which OS (operating system) the victim has
- Evidence indicates that Gauss comes from the same supplier as "Flame", "Stuxnet" and "Duque". In the picture above you can see that Gauss and Flame have the same subroutine for decrypting stringer and module for USB infection is the same. Gauss and Flame its USB infection module is also the same as Stuxnet uses. Gauss probably comes from the same manufacturer as Flame, on the basis of:
  - The code
  - Communication with the control server (C & C)
  - Module structure

- Good analytical report
- But can be more structured



Antall registrerte infiserte maskiner:

- Libanon: 1660
- Israel: 483
- Palestina: 261
- USA: 43

Halvparten av de infiserte brukte Windows 7 etterfulgt av Windows XP, Windows vista og andre.

DNP3 Vulnerability

- **DNP3** (Distributed Network **Protocol**) is a set of communications **protocols** used between components in process automation systems.
- Three subcategories of atatcks: attack against protocol specification, attack against vendor implementation and atatcks on the underlying infrastructure
- Attack against underlying infrastructure may affect any SCADA system
- Vulnerabilities, e.g. user authentication is optional, no ecryption to enforce confidentiality or integrity protection
- Why no security features?: extra overhead required, processing power of the devices limited
- Mitigation: latest DNP3 standard specifies DNP3 secure authentication, not enough!!

- Report well structured and well written

Cyber security attacks on Norwegian Oil and Gas Industry - Past and Present

- Norway's national Security Authority (NSM) issued warnings to the companies including Statoil that they may be targeted

- A good one

Consequence of attacks

- Plant Sabotage/Shutdown
- Utilities Interruption
- Production Disruption
- Hydrocarbon Installation Terrorism
- Facility Terrorism
- Undetected Spills

4.2.1 18th Nov 2011 cyber attack

In 2011, at least 10 firms in the Norwegian oil industry were breached by a group of hackers which compromised company network stealing sensitive data, including industrial project, login credentials and contracts. In an Article email message was published from Kjetil Berg Veire, head of information at NSM to the Norwegian oil and gas companies in which he wrote

4.2.2 27th August 2014 cyber attack

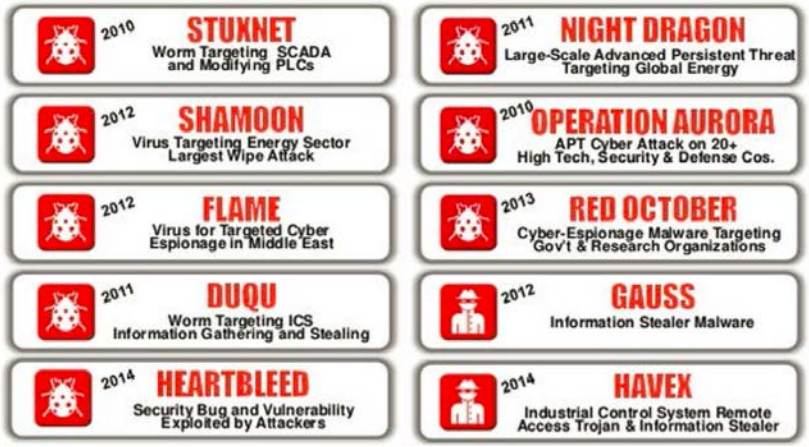
According to a report published in Norwegian newspaper Dagens Naeringsliv on 27th August 2014 , Around 300 oil and energy in Norway companies has been affected by one of the biggest computer hacking attacks ever to happen in the country, a government source said on Wednesday.

NSM is Norway's prevention unit for serious cyber-attacks and, like CERT-UK in Great Britain, warns companies about the newest threats. NSM has issued warnings to the companies it believes may be

Vulnerabilities

96% of all security incidents fall into nine basic patterns

- Point-of-Sale Intrusions
- Crimeware
- Cyber Espionage
- Insider Misuse
- Web App Attacks
- Miscellaneous Errors
- Physical Theft/Loss
- Payment Card Skimmers
- Denial of Service



Overview of Cyber Attacks on Smart Grid Infrasrtucture/Smart Metering

- Introduction of Smart grid / Smart Metering
- Smart meter can be described as a sensor connected in the endpoint at the consumers which records consumption (water, gas or electricity), and transmits the information to the utility provider.
- The smart grid infrastructure consist of many assets, that includes; field devices, power generations, consumers, communicating and network devices, remote terminal units, smart meters and much more. All of these assets are somehow connected together, making it possible monitor, operate and control the infrastructure over large geographical areas.

- Report, a good one
- Well studied

The *Northeast blackout of 2003* is one of the largest power outage which affected Midwest and Northeast United States and Ontario in Canada, more than 50 million lost power during the four days. This was the worlds second largest outage after the 1999 Southern Brazil blackout. The cause of the blackout was a bug in the software [1].

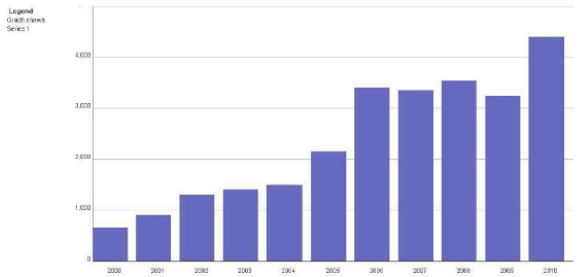


Figure 2: Growth of vulnerabilities in the smart grid infrastructure [3]

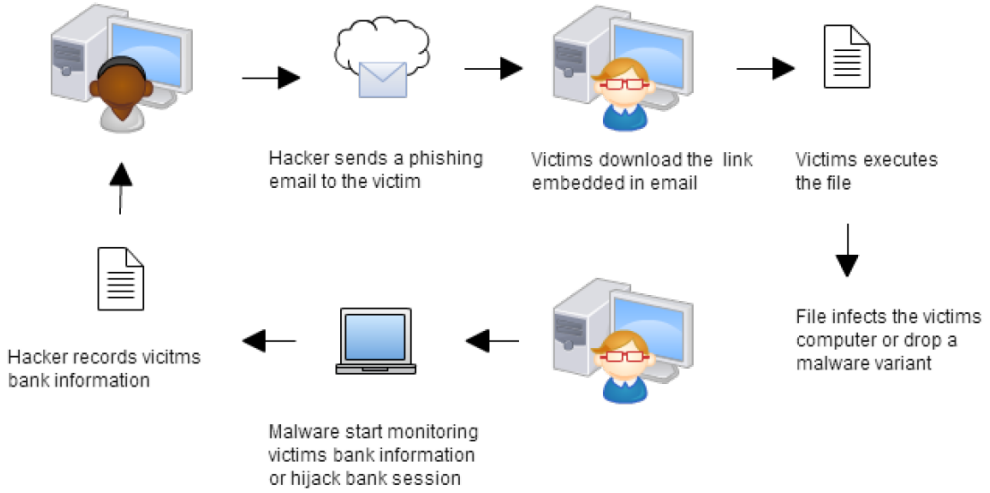
The state utility provider in Malta has been a victim of disgruntled employee who tampered 250 smart meters. While in another case two other employees had tampered 1000 smart meters that were rigged to record small percentage of the household energy consumption, which gave losses of 30 million Euro [6].

The *2006 European blackout* was a major blackout which affected several countries in Europe. More than 15 million people was affected of the blackout. The reason for the blackout was an overload in Germany's power network. The immediate impacts caused the trains to stop in Italy, more than 40 episodes of people being stuck in elevators in Paris, factories had to shutdown and much more [4].

BlackEnergy

- BlackEnergy is a sophisticated malware which is designed to exploit different units of industrial control and computer systems.
- First indentified in 2007, initially developed for DDoS attacks
- In 2010, redesigned, Can steal important system information through custom plugins
- It has the capability to attack ARM and MIPS platform
- attach scripts for Cisco network devices, inject main dll into user processes, harmful plugins, certificates hacking and much more which is responsible for vulnerabilities
- Two version: BlackEnergy Big, BlackEnegery Lite

- Report, is a well structured one
- A good one for basic knowledge about BlackEnergy



Shamoon

- Shamoon, also called W32.Disttrack, is a modular computer virus that has been used for cyber espionage.
- It targeted energy companies in middle east

- Report, is a well studied one

On August 15,2012 ,in the morning at 11:08, a person with privileged access to the Saudi state-owned oil company's computers - a disgruntled insider, unleashed a computer virus to initiate what is regarded as among the most destructive acts of computer sabotage on a company to date.

First target was Saudi Aramco ,Saudi Arabias state-owned oil-production company.Attacked on 2012 ,August 15. This attack compromised about 30,000 computers. Restoration took about two weeks.

Second strike was executed on computer systems at Qatar's energy firm RasGas.They have been taken offline by a computer virus only days after a similar attack on oil giant Aramco.

Likely, other oil and gas concerns in the region were targets for Shamoon attacks.

It has three primary functional components, according to **Symantec**:

1.Dropper - *%System%\trksrv.exe* :The main component and source of the original infection. It installs a number of other modules.

2. Wiper- *%System%\[*NAME SELECTED FROM LIST on Fig3*].exe*: This module is responsible for the destructive functionality of the malware.

3. Reporter- %System%\netinit.exe : This module is responsible for reporting infection information back to the attacker.

Security Incidents

- http://www.risidata.com/

RISI

The Database | About | Contact

Last Updated: Wed, January 28, 2015

Title	Year	Industry Type	Country	Brief
Page 1 of 9 pages **1** 2 3 > Last ›				
German Steel Mill Cyber Attack	2014	Metals	Germany	
Russian-Based Dragonfly Group Attacks Energy Industry	2014	Power and Utilities	United States	
Public utility compromised after brute-force hack attack, says Homeland Security	2014	Power and Utilities	United States	
After 'Godzilla Attack!' U.S. warns about traffic-sign hackers	2014	Transportation	United States	
U-2 spy plane caused widespread shutdown of U.S. flights: report	2014	Transportation	United States	
Virus shuts down county highway department network	2013	Transportation	United States	
Signal problems cause train delays	2013	Transportation	United States	
Computer Glitch Leads to Shutdown of Nuclear Reactor	2012	Power and Utilities	United States	
U. S. Power Plant Infected With Malware	2012	Power and Utilities	United States	
U. S. Electric Utility Virus Infection	2012	Power and Utilities	United States	
Software Manufacturing Company Firewall Breach	2012	General Manufacturing	Canada	
Shamoon virus knocks out computers at Qatari gas firm RasGas	2012	Petroleum	Qatar	
Computer Virus Targets Saudi Arabian Oil Company	2012	Petroleum	Saudi Arabia	
Computer Glitch Causes Roller Coaster Malfunction	2012	Other	United States	
Computer Malfunction Causes Train Delays	2012	Transportation	United States	

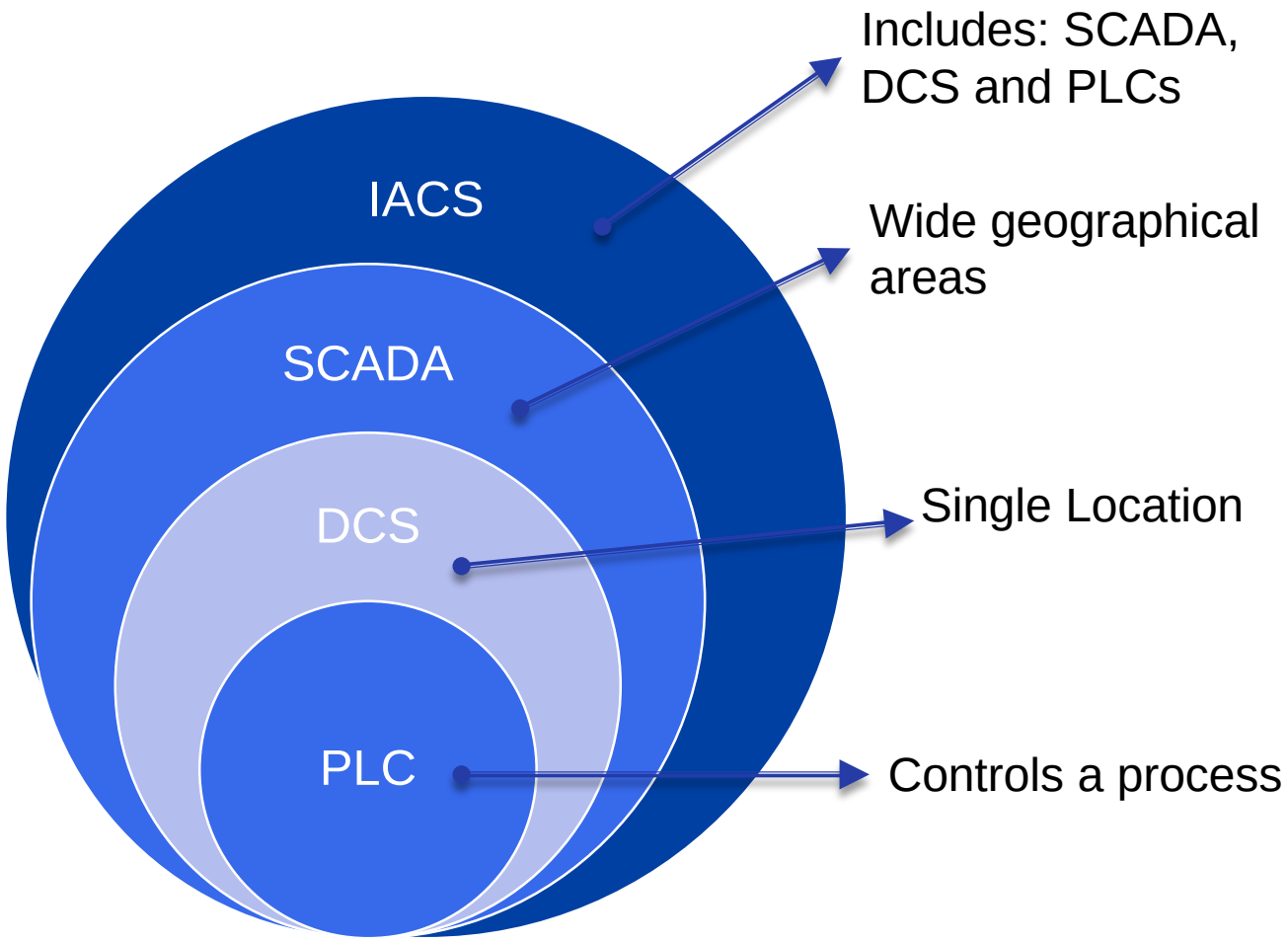
Industrial Automation and Control Systems

Industrial **A**utomation and **C**ontrol **S**ystem

Supervisory **C**ontrol **A**nd **D**ata **A**quisition **S**ystem

Distributed **C**ontrol **S**ystem

Programmable **L**ogic **C**ontroller



C-I-A vs. AIC

- *Availability*—The ability to preserve operational continuity. Information, data, services, networks, applications, and resources should be accessible in a timely manner when needed. It's essential to protect the availability of these assets from intentional or unintentional impact. Additionally, security services cannot impact the operational continuity as they execute.
- *Integrity*—The ability to preserve the authenticity of information, data, service, and configurations and to help ensure no unauthorized clients unexpectedly or covertly modifies any of these aspects.

- *Confidentiality*—The ability to maintain the privacy and confidential nature of potentially private or sensitive information, and to help ensure that only authorized entities have access to it. This applies both to data at rest and data in transit during communication.

Assets to protect

- *IACS endpoints*—The devices or systems terminating an IP communications path and handing the data to the application layer. Endpoints may be interactive or standalone devices (laptops, desktops, servers, etc.). Endpoints considered include all the devices in Levels 0 to 3 and in the Demilitarized zone (DMZ) that are created as part of the architecture for the CPwE solution (see below).
- *Applications and services*—The higher-level processes relying on and using data being communicated or stored. Typically, the application or service uses network communications (and consequently the network infrastructure) to communicate with other applications or services residing on another endpoint.
- *Data in transit*—Data that is traversing the network infrastructure and is in transit between endpoints. Typically, active IP communications may use any subprotocol (UDP, TCP, RTP, etc.) to communicate information between applications on the endpoints. Of primary concern for protection of data in transit are IACS network protocols, such as CIP.
- *Stored data*—Information or data at rest in storage on an endpoint. The architecture designed to protect network access to endpoint systems should include protecting the stored data on those devices (e.g., Historian Server).
- *Network and Network Infrastructure*—The network elements that make up the transport structure moving communications between endpoints (switches, routers, security appliances, etc.) and the links interconnecting them may also be target of attacks such as theft of service, service abuse, denial-of-service (DoS), man-in-the-middle (MITM) and data loss to name a few

Threats

- *Viruses* manipulate legitimate users into bypassing authentication and access control mechanisms in order to execute malicious code. Virus attacks are often untargeted and can spread rapidly between vulnerable systems and users. They can damage systems and data, or decrease the availability of infected systems by consuming excessive processing power or network bandwidth.
- A *worm* is a self-replicating program that uses the network to send copies of itself to other nodes without any involvement from a user. Worm infections are untargeted and often create availability problems for affected systems. They may also carry a malicious code to launch a distributed attack from all infected hosts.
- The *Trojan* horse is a virus in which the malicious code is hidden behind a functionality desired by the end users. Trojan horse programs circumvent confidentiality or control objectives and can be used to gain remote access to systems, gather sensitive data, or damage systems and data.

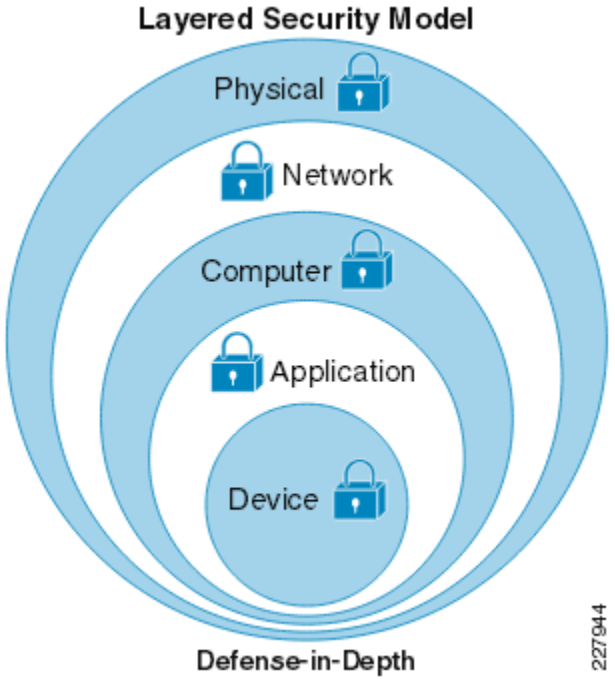
- Distributed denial-of-service (DDoS) attack—A common type of attack used by network saboteurs. DDoS attacks have become notorious over the past few years by flooding the network resources (such as critical servers or routers) of several major retail websites, with the goal of consuming resources or obstructing communication to decrease the availability of critical systems. A similar attack can easily be mounted on a targeted IACS application, making it unusable for a critical period of time.
- Eavesdropping attacks—Used to violate the confidentiality of the communication by sniffing packets on the LAN or by intercepting wireless transmissions. Advanced eavesdropping attacks, also known as man-in-the-middle or path insertion attacks, are typically leveraged by an attacker as a follow-up to a network probe or protocol violation attack.

Threats

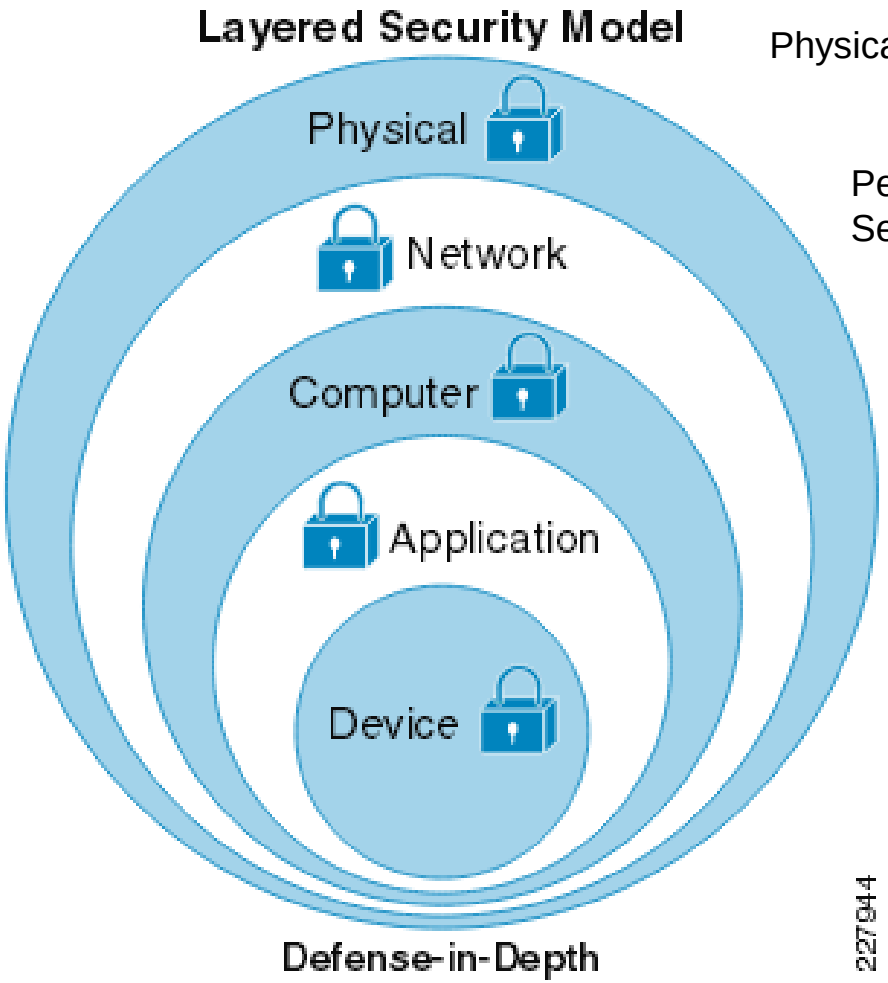
- Collateral damage—An unforeseen or unplanned side effect of techniques being used for the primary attack. An example is the impact that bulk scanning or probing traffic may have on link and bandwidth availability. IACS applications are especially sensitive to network latency and dropped packets. If a network is not properly configured, unintended traffic such as large downloads, streaming video, or penetration tests can consume excessive bandwidth and result in slowed performance and unacceptable levels of network jitter.
- Unauthorized access attacks—Attempts to access assets that the attacker is not privileged or authorized to use. This implies that the attacker has some form of limited or unlimited control over the asset.
- Unauthorized use of assets, resources, or information—Use of an asset, service, or data by someone authorized to use that particular asset, but not in the manner attempted.
- Reconnaissance attacks—Probing that enables the first stage of the attack lifecycle. This serves to provide a more focused attack cycle and improve the attacker's chances for success.

Defense-in-Depth

- *Physical Security*—This limits physical access of areas, control panels, devices, cabling, the control rooms and other locations to authorized personnel with provisions to escort and tracks visitors.
- *Network Security*—This includes the network infrastructure, such as firewalls with intrusion detection and intrusion prevention systems (IDS/IPS), and integrated protection of networking equipment such as switches and routers.
- *Computer Hardening*—This includes patch management and antivirus software as well as removal of unused applications, protocols and services.
- *Application Security*—This contains authentication, authorization and audit software.
- *Device Hardening*—This handles change management and restrictive access.



Defense-in-Depth



Physical access control

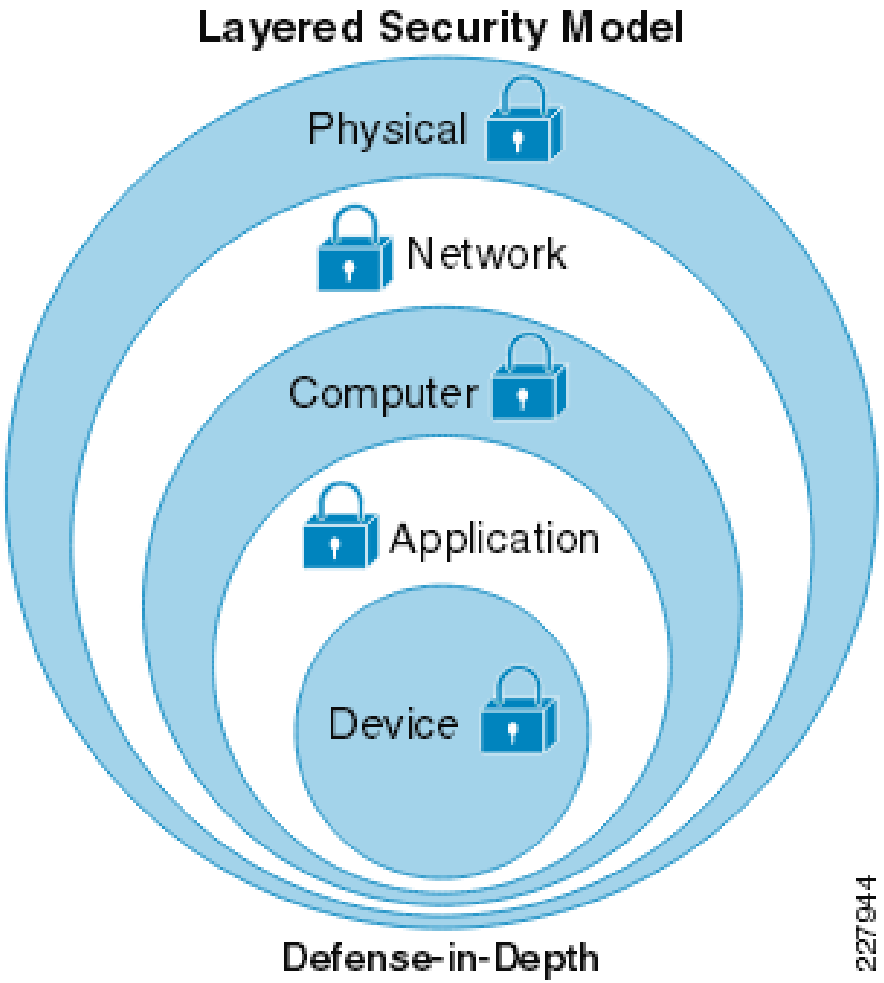
Perimeter defence (e.g. Firewall); Network Segmentation; De-Militarized Zone

Computer hardening, e.g. patching, access control, host level firewall

Access control in applications, only install necessary applications and services

Control of USB usage; Only open ports necessary; disabled unused ports on Network Devices etc.

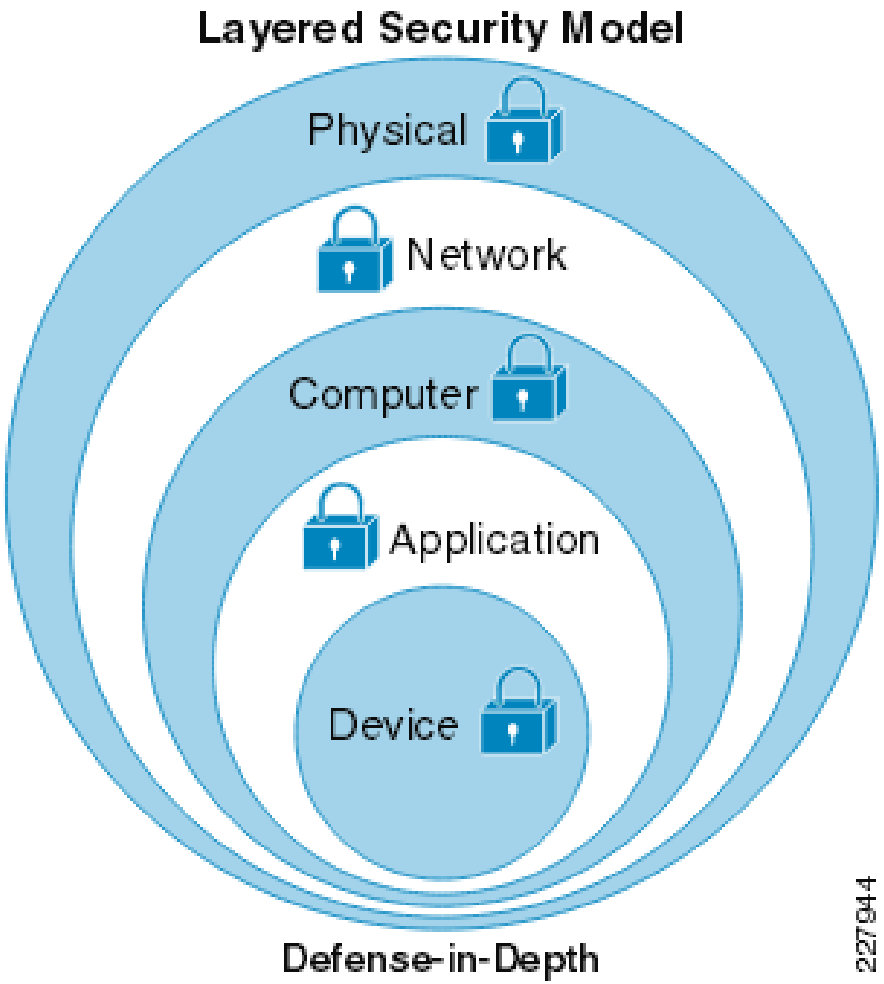
Defense-in-Depth



Security monitoring, alerting, reporting, logging, and auditing

- Accounts and Access
- Devices
- Applications & Services
- Protocols

Defense-in-Depth



Incident response:

- Policies
- Restore & recovery

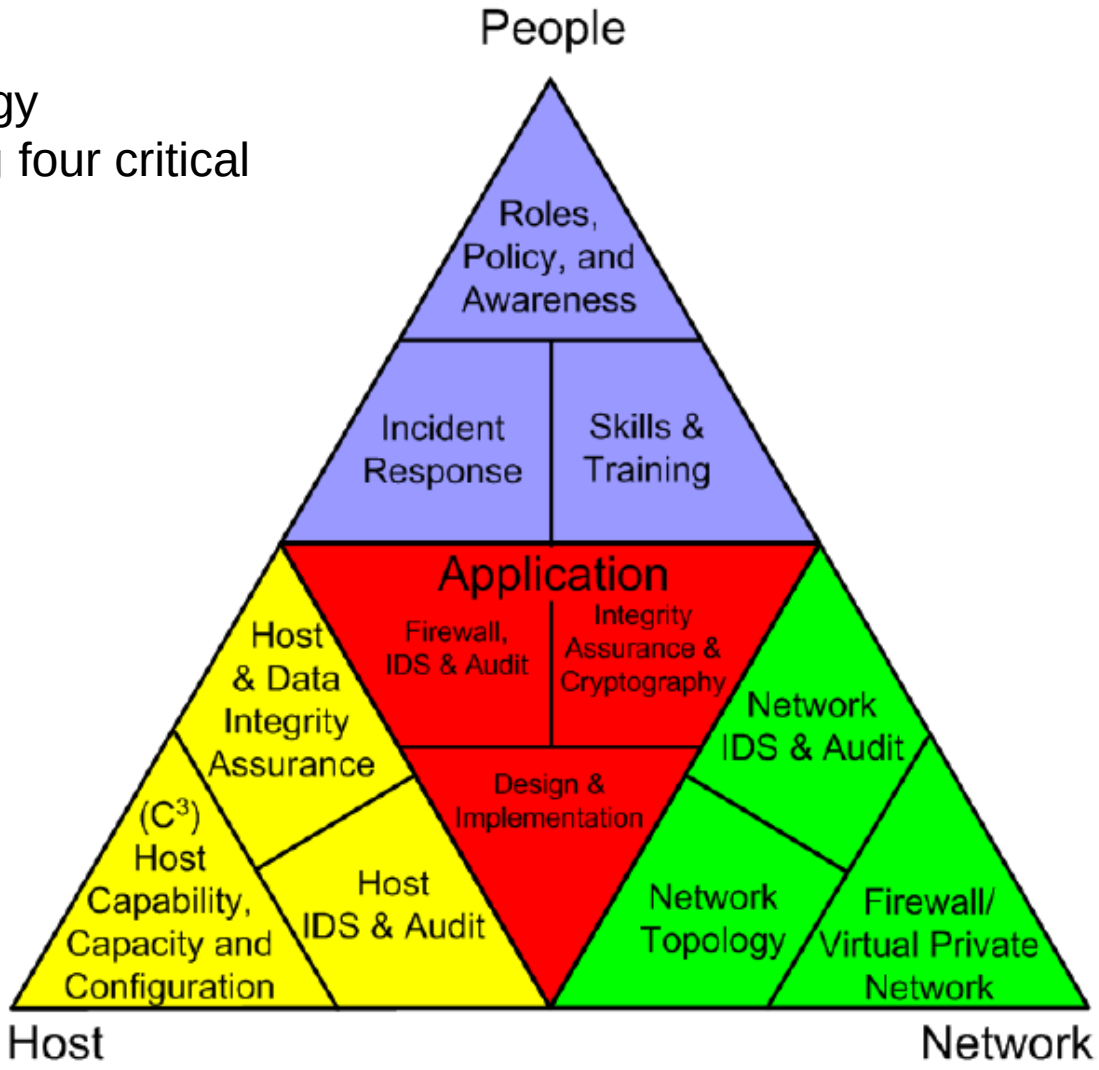
Backup of critical data

- Backup strategies

Defence-in-Depth: People

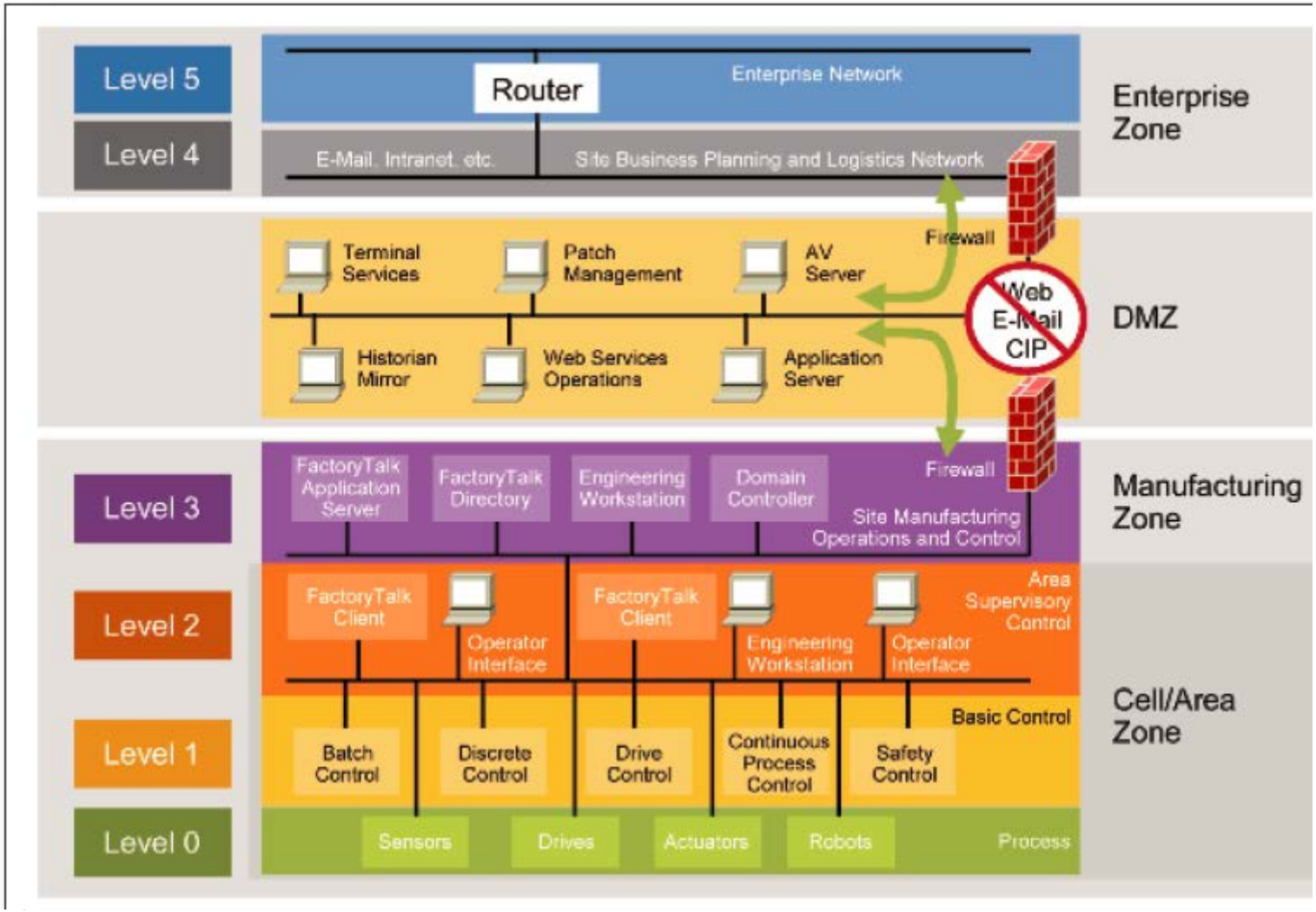
The Defense-in-depth strategy encompasses the following four critical categories:

- People
- Network
- Host
- Application



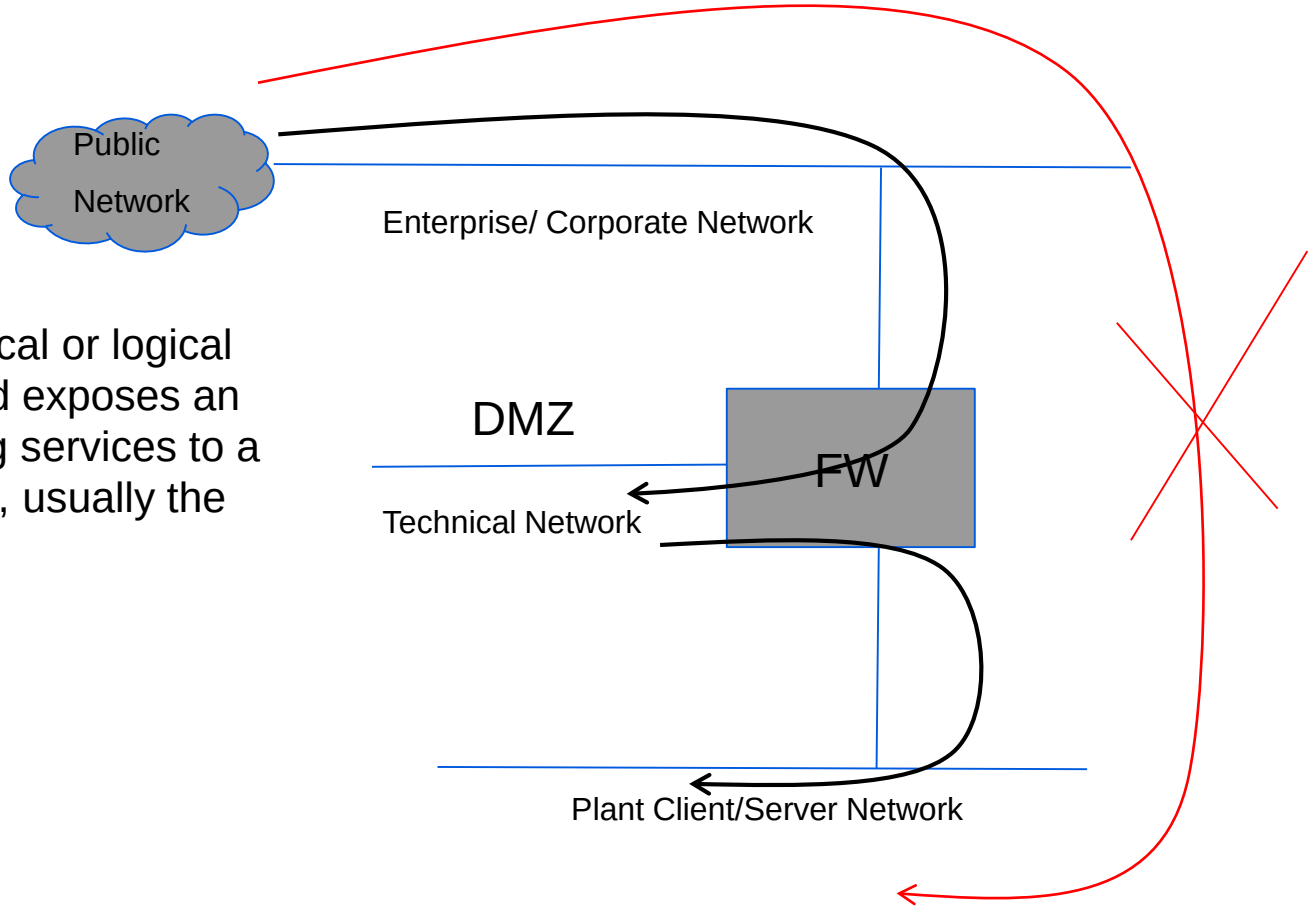
Network Segmentation
ISA 99 (utilized by IEC62443) reference architecture

ISA-99's Manufacturing and Control Systems Security, and the Purdue Reference Model for Control Hierarchy.



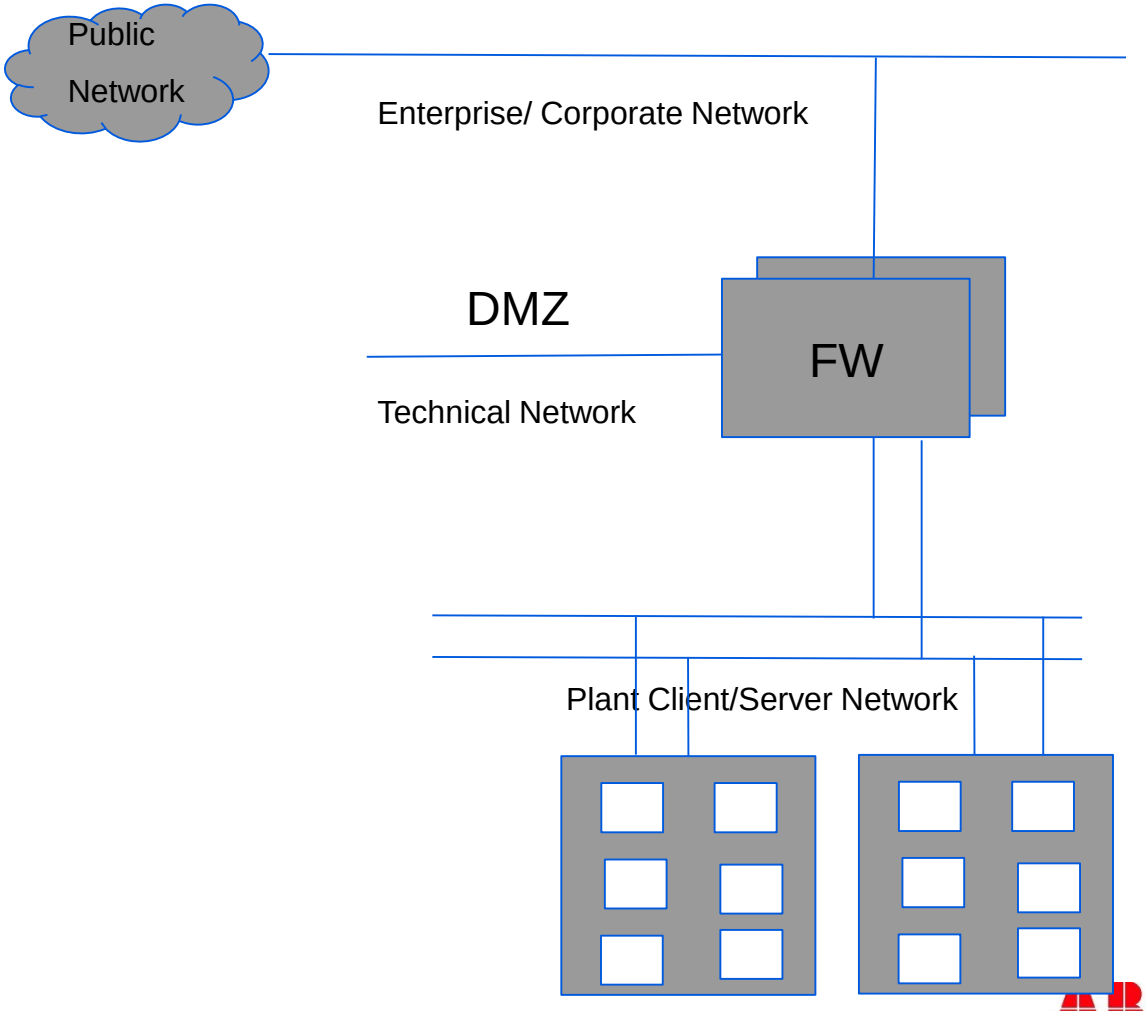
DMZ

Demilitarized zone is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet



Availability

- Through redundancy, e.g. Device, Network, Resources such as storage disks, RAID configuration
- Mitigations against DoS



Hardening

For computers

User level hardening

- RBAC principle, users assigned to roles, roles have permissions
- Only one role at a time
- minimum permissions necessary, Administrator has more permissions than Engineer or Operator
- Restrict access to resource, applications, folders, drives, USB ports, OS items, e.g. operator cannot shut down the computer

Computer level hardening

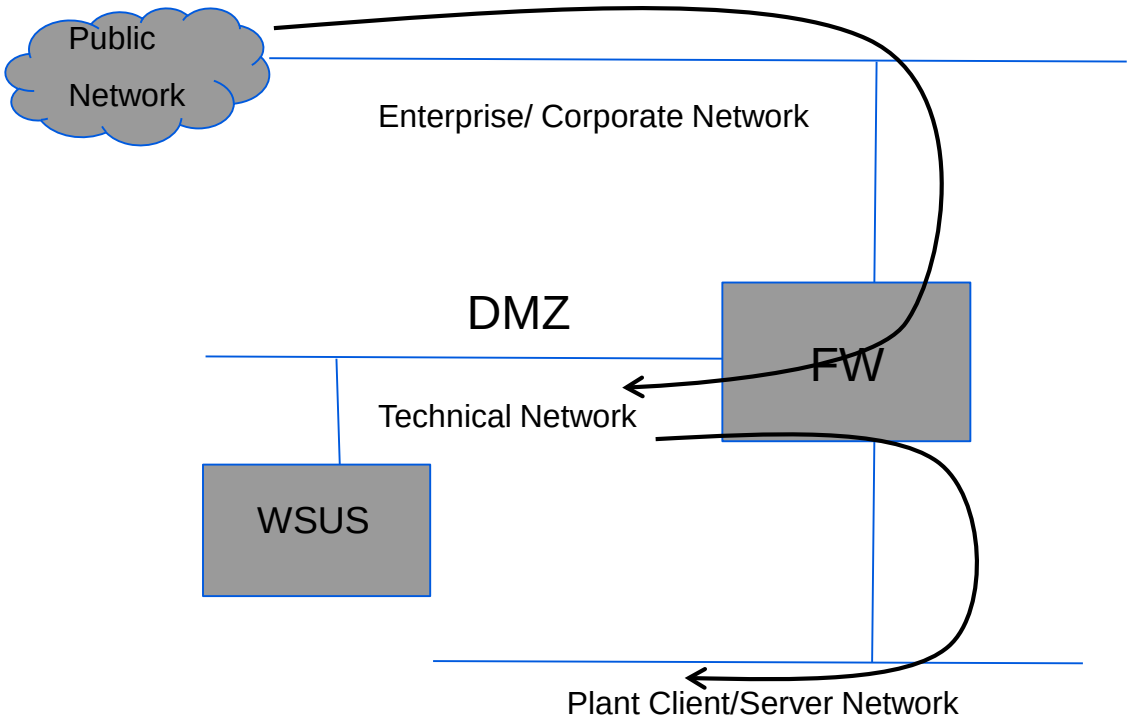
- Disabled USB
- Allow RDP
- Allow logging
- Dont allow copy/paste'
- Define windows firewall settings
- Patching the system with updates, e.g. patching windows
- No internet connectivity
- etc

Hardening

For network devices

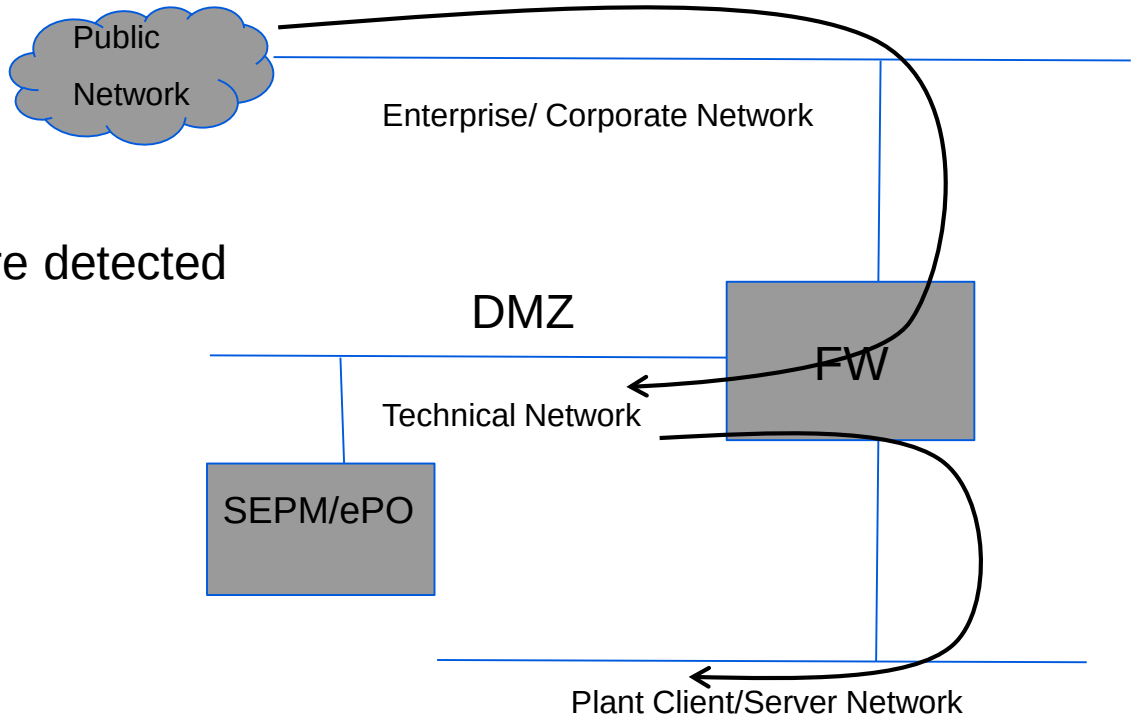
- Remove/disable default account
- Create new Administrator credentials
- Update firmware
- Always use secure interface (e.g. SSH, HTTPS) to administrative console
- Disable HTTP, Telnet
- Disable unused ports

Hardening – patch management

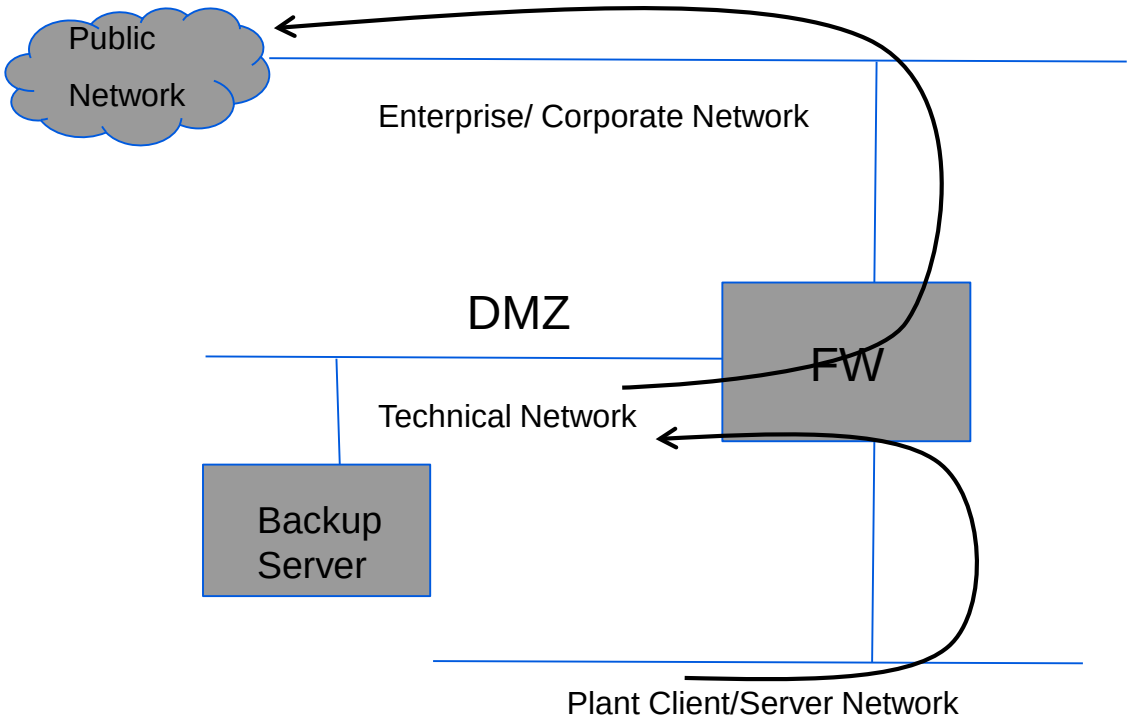


Protecting of Host with Antimalware

- Use of antimalware SW
- Update virus definition file regularly
- Distribute virus definition file to all computers in the system
- Add policies
  - Exclusion list
  - Daily scan
  - Weekly scan
  - Policy when malware detected
- Reporting



Backup


Public
Network
Enterprise/ Corporate Network
DMZ
FW
Technical Network
Backup
Server
Plant Client/Server Network

Time Synchronization

- Why?: timely and accurate identification of incidents
  - Important for troubleshoot
  - Important to audit
  - Analyse attacks
  - Real—time response, ~ ms of delay acceptable
- A GPS time source distributes times internally
  - Windows time
  - NTP/SNTP

Advanced feature – Application Whitelisting

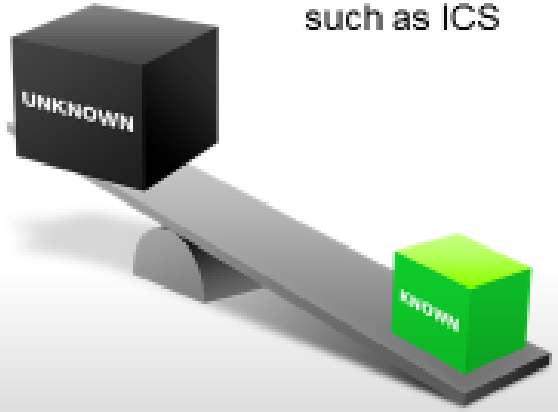
Known vs. Unknown

Anti-Virus

- Defensive approach
- Scans against a database of known problems
- More than 10,000 virus signatures
- Resources intensive
- Cannot block memory-based exploits
- Useful in environments with constant change

Whitelisting

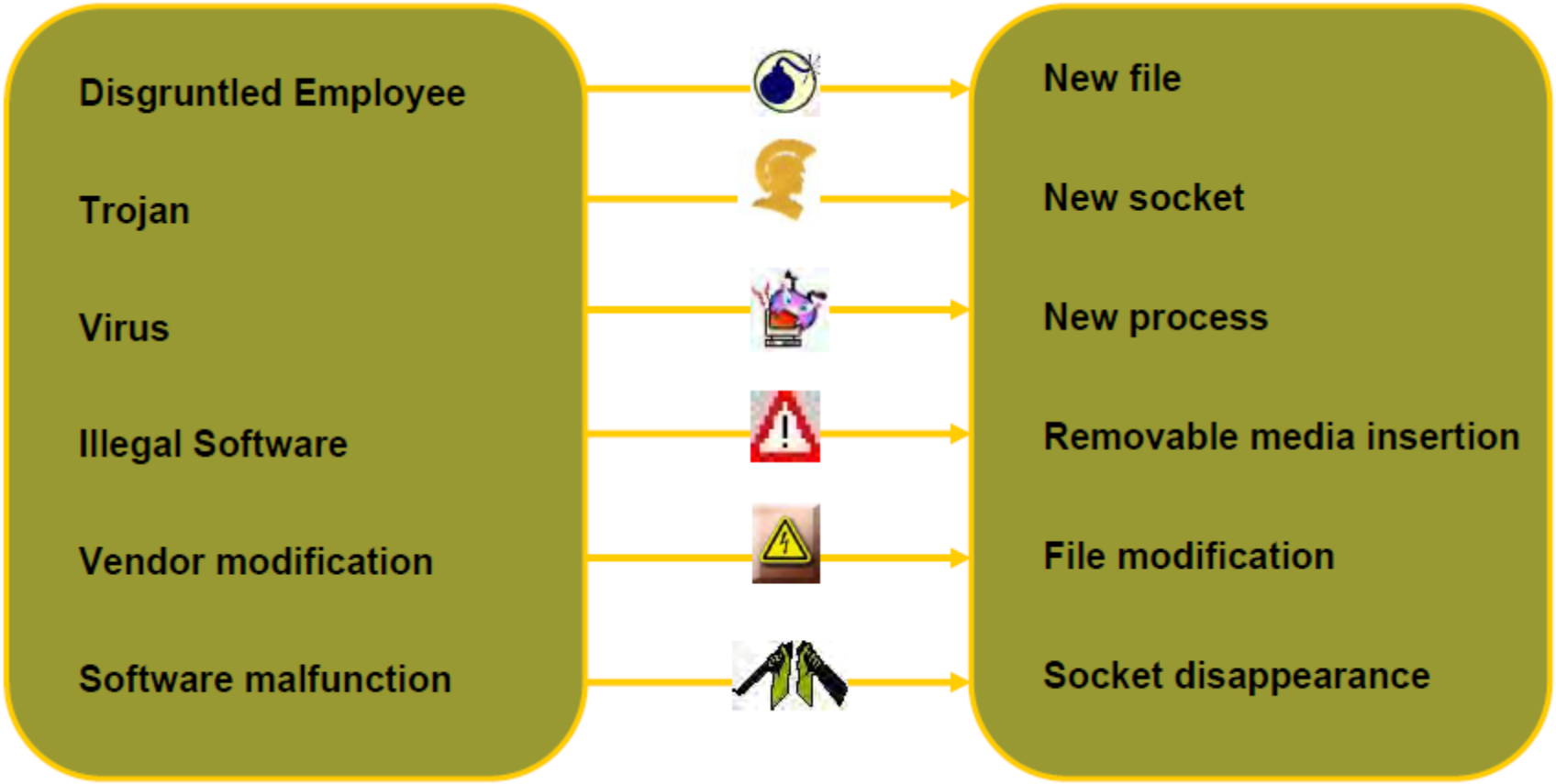
- Proactive, Offensive approach
- Only approved and trusted applications can run
- Protects at OS level
- Short list to scan against
- Stops memory based attacks
- Ideal for endpoints that rarely change, such as ICS



Advanced feature – Intrusion Detection and Protection System

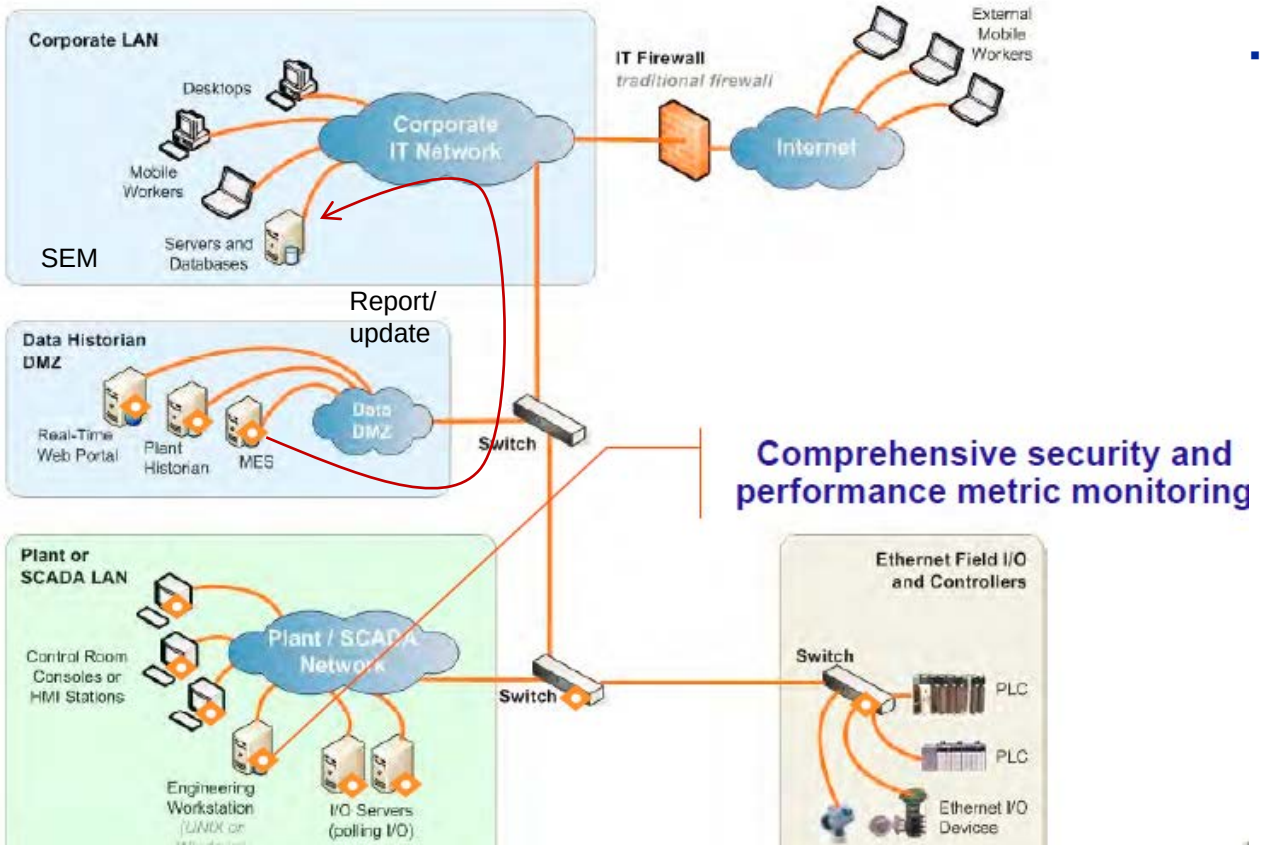
- **Intrusion Detection System (IDS) :** Software/Hardware that automates the intrusion detection process. An IDS is a passive system; the system detects a potential security breach, logs the information and signals an alert
  - Passive system
- **Intrusion prevention system (IPS):** Software/Hardware that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. is a reactive system; responds to suspicious activity typically by reprogramming a firewall to block network traffic or dropping traffic on the network
  - Reactive system
- **Intrusion Detection and Prevention System (IDPS):** refers to both IDS and IPS. The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents.

Anomaly Detection Examples



Advanced feature -

Intrusion detection & protection system



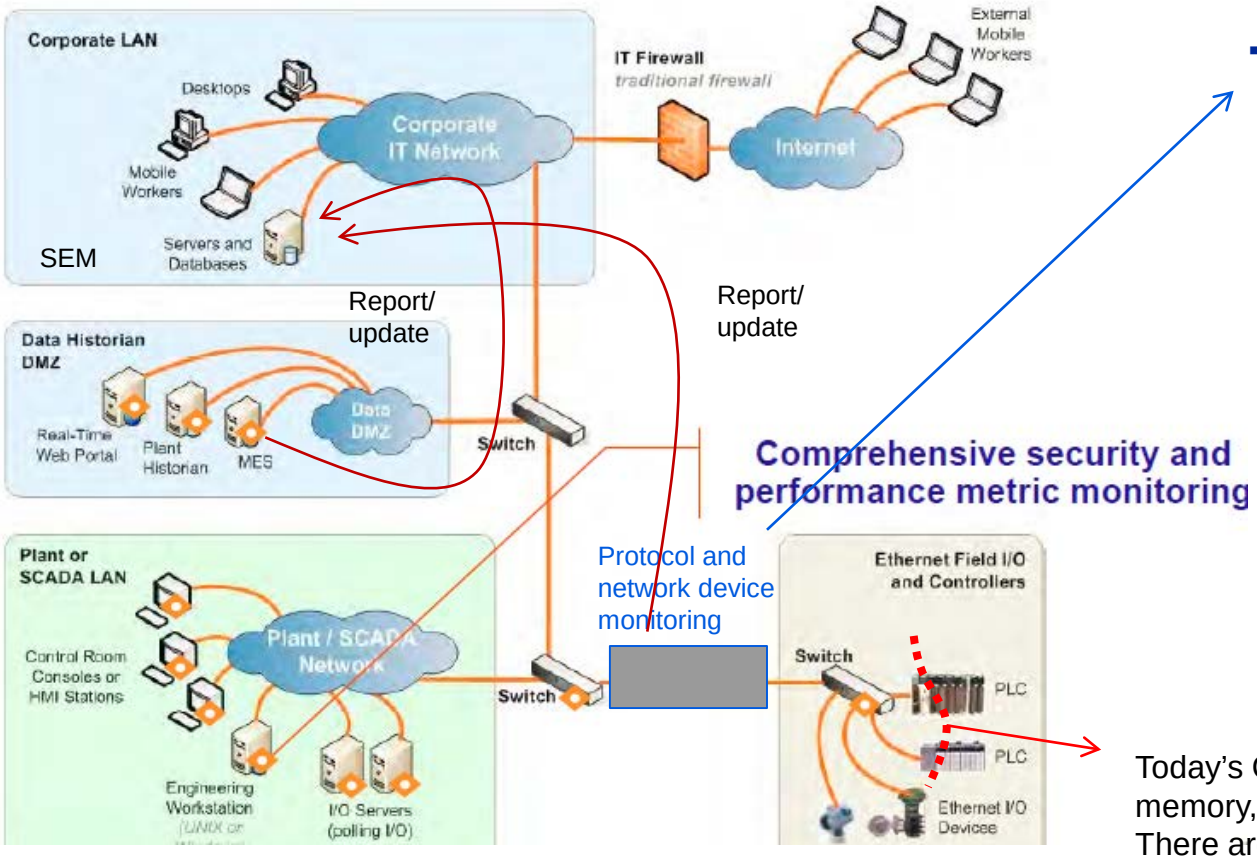
- **HIDS: Host Intrusion Detection Systems**
  - Detects any unusual activity on the host
  - Alarm only raised on abnormal behavior

Source of fig: Chris Martin, Industrial Defender

SEM: Security Evenet Management

Advanced feature -

Intrusion detection & protection system



- **NIDS: Network Intrusion Detection Systems**
  - Placed in network
  - Monitors network
    - Internally launched attacks
    - Unauthorized traffic etc.

Anomaly detection examples
Example: network attacks such as IP spoofing, packet floods, DoS better detected through examining packets

Today's Controllers/PLCs contain CPUs, memory, communication modules.
There are threats/attacks targeting them
What about monitoring them?

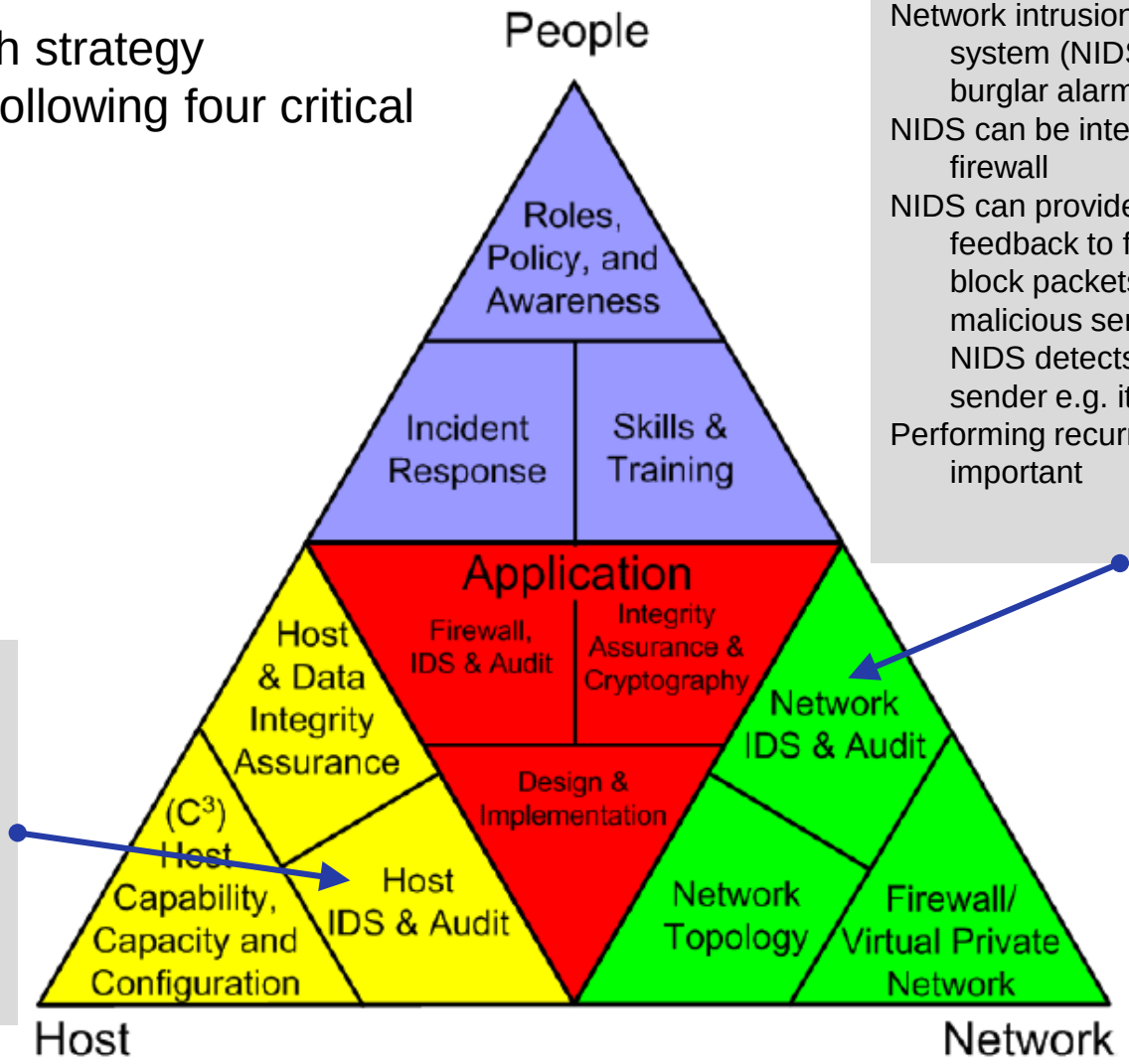
Source of fig: Chris Martin, Industrial Defender

SEM: Security Evenet Management

Why Is Intrustion Detection/Protection Needed?
Important part of a Defense in Depth Stragegy

The Defense-in-depth strategy encompasses the following four critical categories:

- People
- Network
- Host
- Application



Network intrusion detection system (NIDS) acts like burglar alarm.
NIDS can be integrated to a firewall
NIDS can provide real-time feedback to firewall e.g. to block packets from a malicious sender (once NIDS detects the malicious sender e.g. its IP address)
Performing recurring audit is important

Host intrusion detection system (HIDS) detects intrusion signatures and unusual events in the logs and provide timely into suspected intrusion attempts
Performing recurring host audit is important

Power and productivity
for a better world™