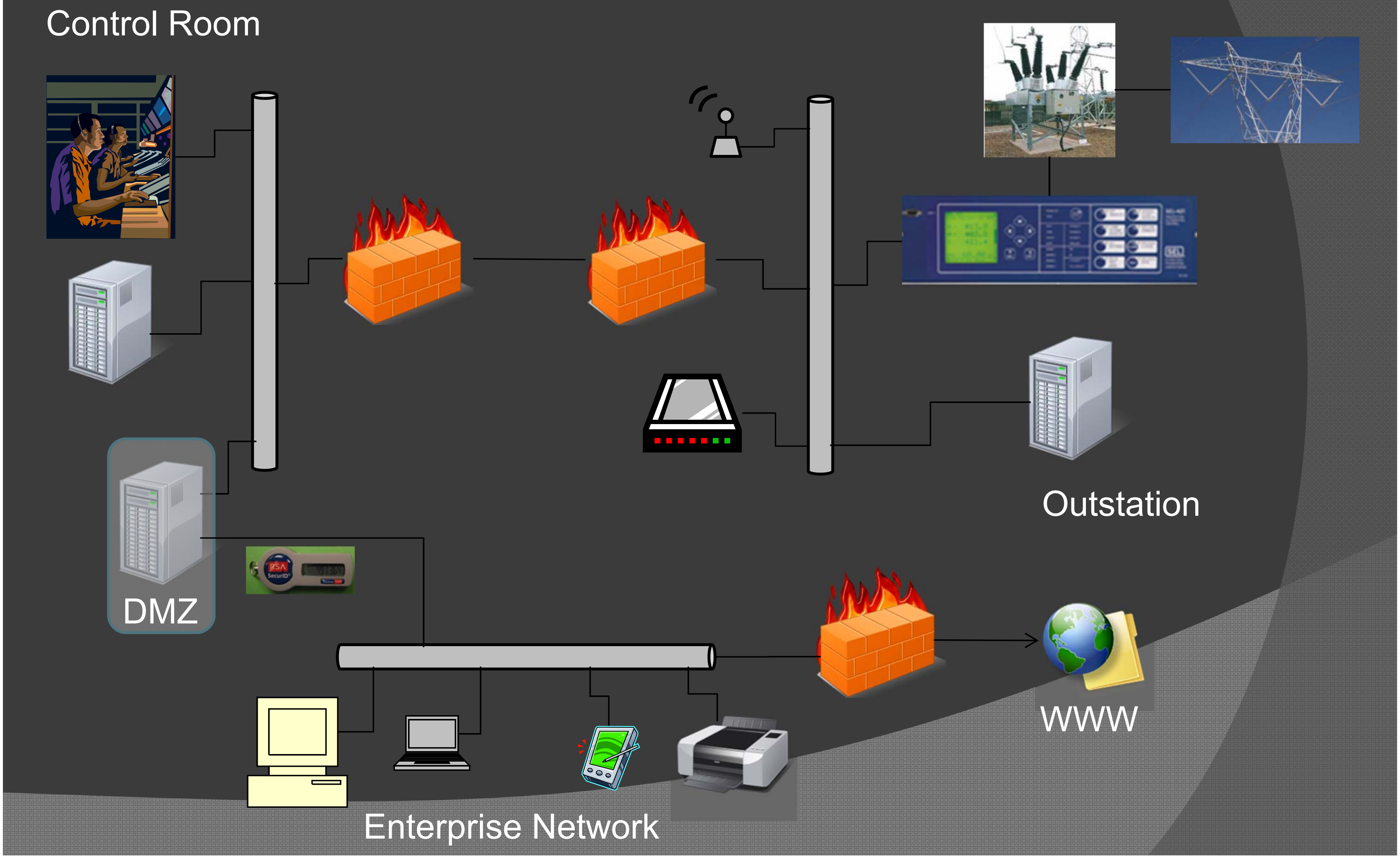
Cyber Security Considerations for Industrial Control Systems

Weichao Wang
College of Computing and Informatics
UNC Charlotte

Common configuration



Control Room

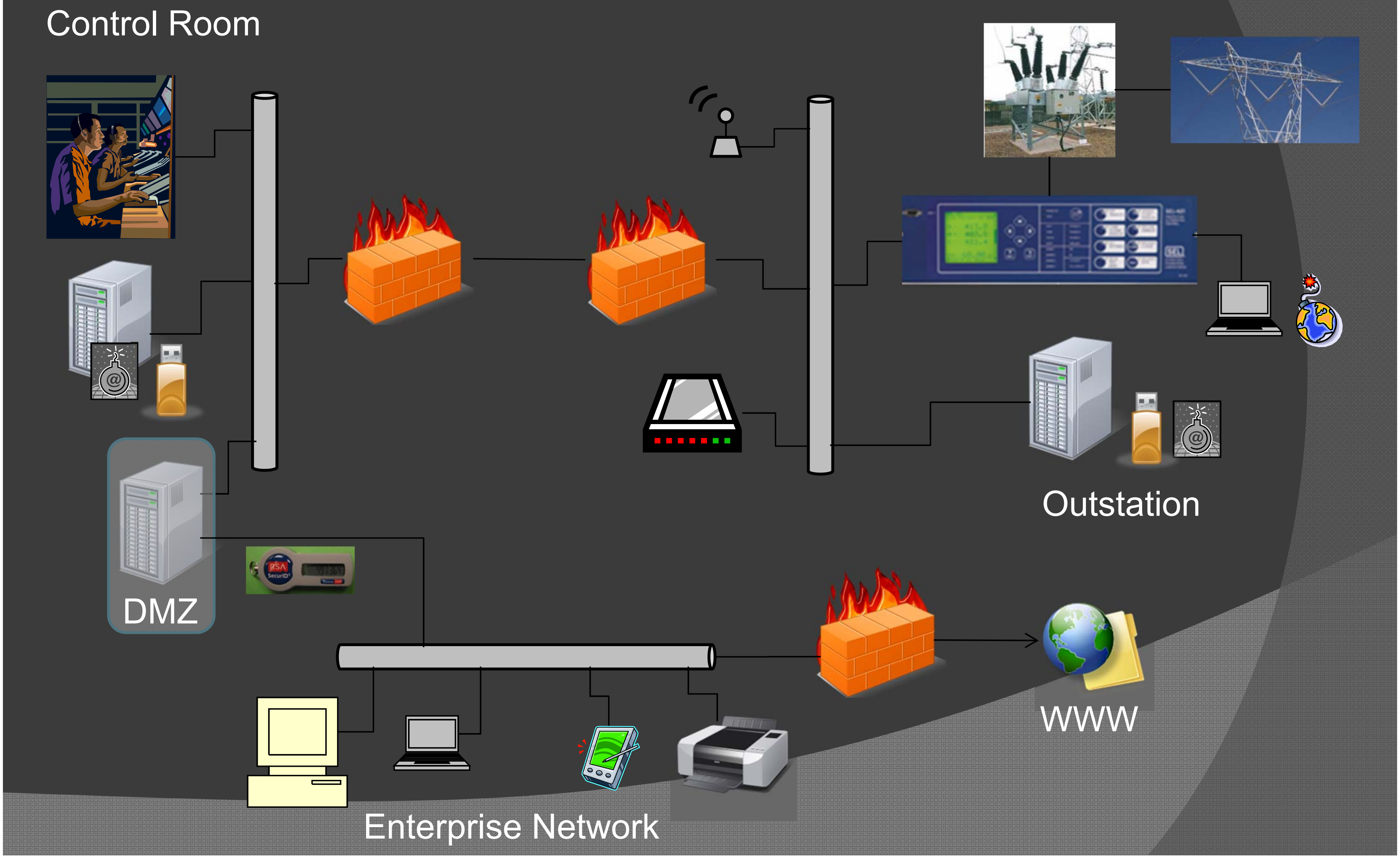
Outstation

DMZ

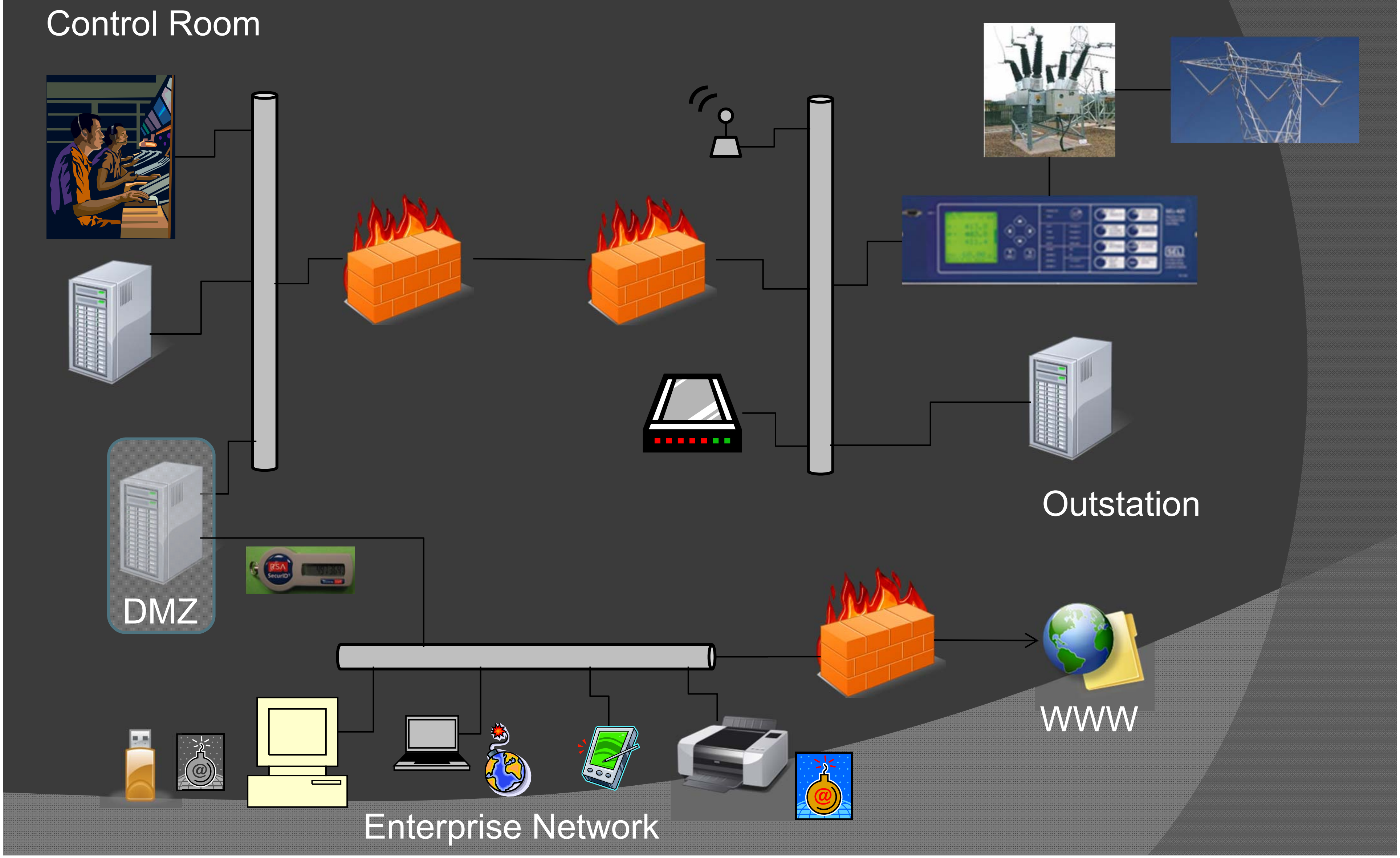
WWW

Enterprise Network

Can malware infect the control room or outstation? Yes



Can malware infect the control room or outstation? Yes



Control Room

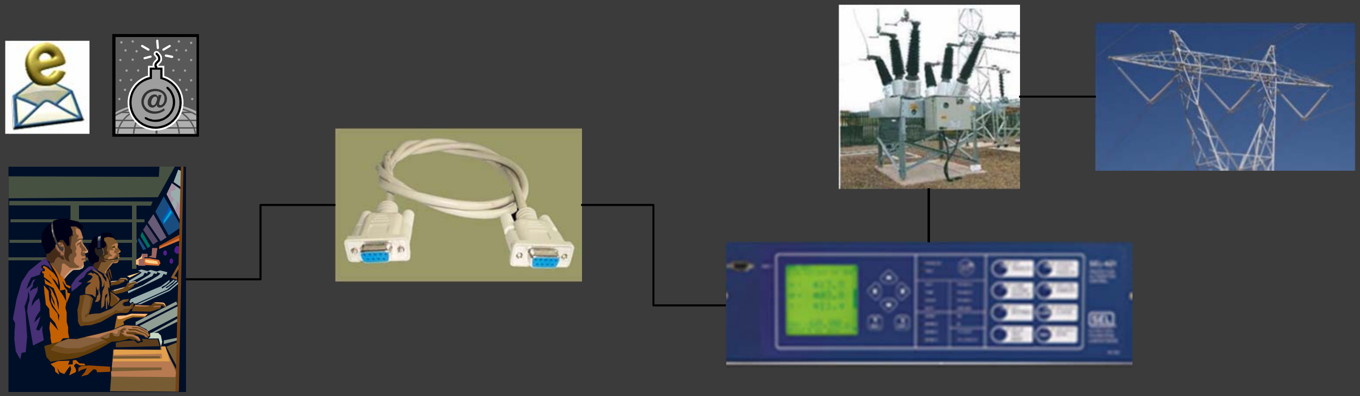
DMZ

Outstation

WWW

Enterprise Network

What about serial? RS-232/485



Stuxnet

Take aways

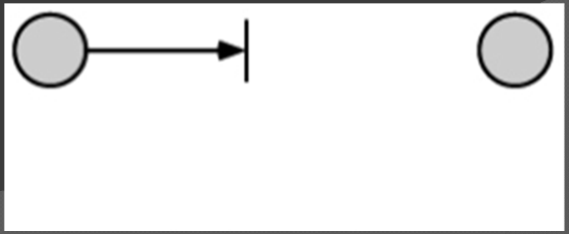
- Industrial control systems can be infected by malware.
- An electronic security perimeter alone is insufficient protection.
- Need a defense in depth approach.

Risk Assessment

- Should consider
  - likelihood of attack
  - cost of attack
  - impact of attack
- Compared to
  - cost of prevention
  - likelihood of prevention

Interruption (Denial of Service)

- An asset of the system is destroyed of becomes unavailable or unusable
- Attack on availability
- Disabling the file management system
- LonTalk protocol example
- May not be physical destruction. (mostly are not)
- May be temporary.

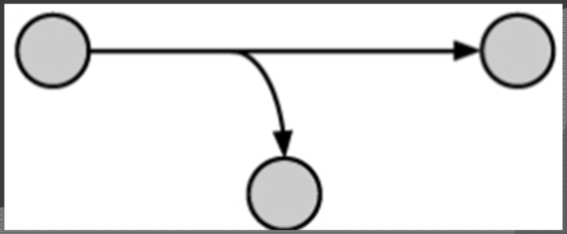


DOS Prevention

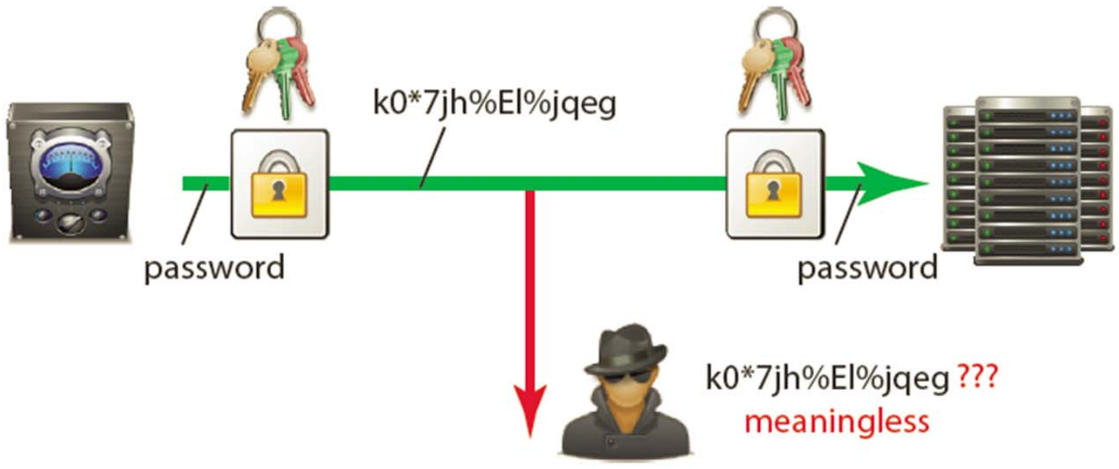
- Defense at the protocol level
  - Monitor the active connections
- Monitor and react
  - Monitor network traffic for DOS attacks
  - Close offending ports
  - Is it OK to close a network port in an ICS network?
- Test devices for vulnerability
    - Protocol mutation (fuzzing)
    - Known attacks
    - Floods

Interception

- An unauthorized party gains access to an asset
- Attack on confidentiality
- Wiretapping to capture data in a network
- Intercepting a password -> bad
- Intercepting a password file -> worse
- Intercepting ICS data -> what can the attackers learn?



Keyed Encryption



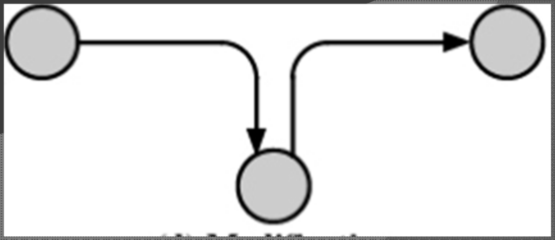
- encryption algorithm: represents a family of transformations used to code data; particular key used selects member of the family employed for coding
- Authorized parties each have access to an appropriate key an can participate in confidential communications.
- Unauthorized parties do not have the secret key limiting access to the confidential information.

- You have to be really careful: encryption does not solve all problems
  - Key distribution and update
  - Forward and backward secrecy
  - Pairwise key or group based communication

Modification

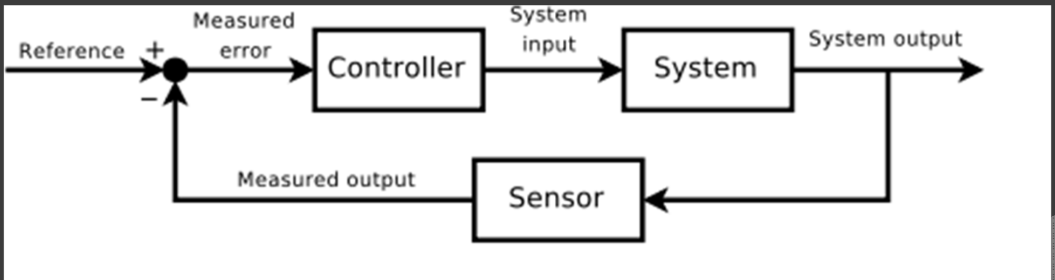
- An unauthorized party not only gains access but tampers with an asset
- Attack on integrity
- Change values in a data file
- Alter a program to make it perform differently
- Modify content of messages transmitted on a network

man-in-the-middle (MITM)



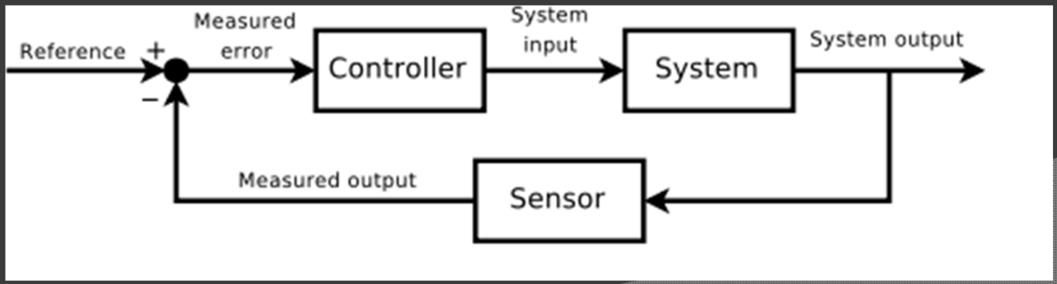
Modification

- Modification in ICS -> very bad
- Feedback control uses
  - sensors to monitor physical process
  - Controllers to control the physical process.
- Modifying measured output, measured error, system input, or reference affects system output.

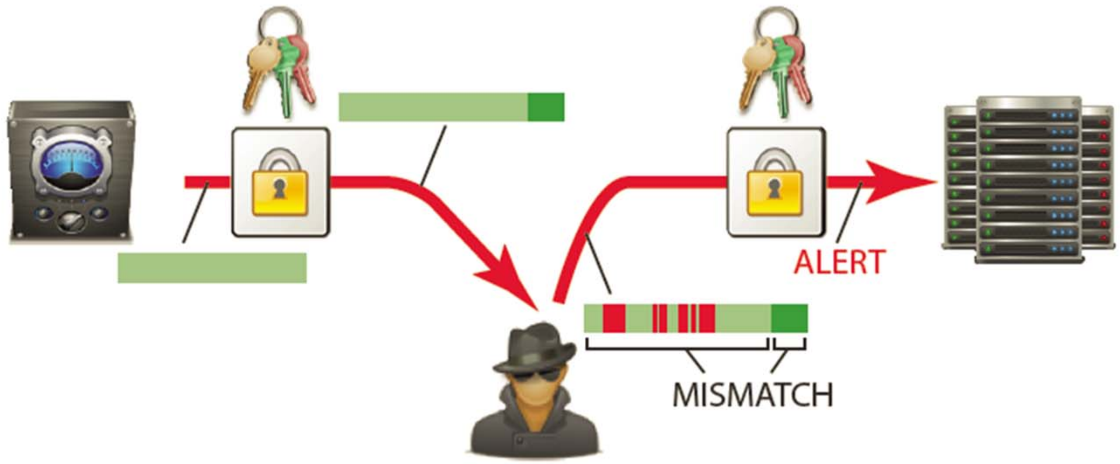


Modification

- Need to defend the sensor.
- Need to defend the device which measures error.
- Need to defend the controller.
- Need to defend the communication network.

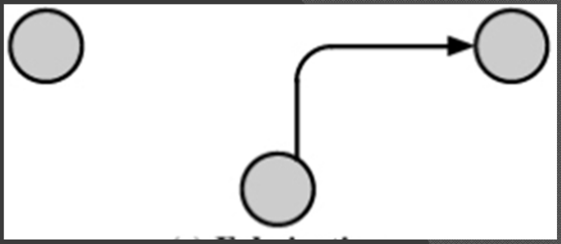


Digital Signatures



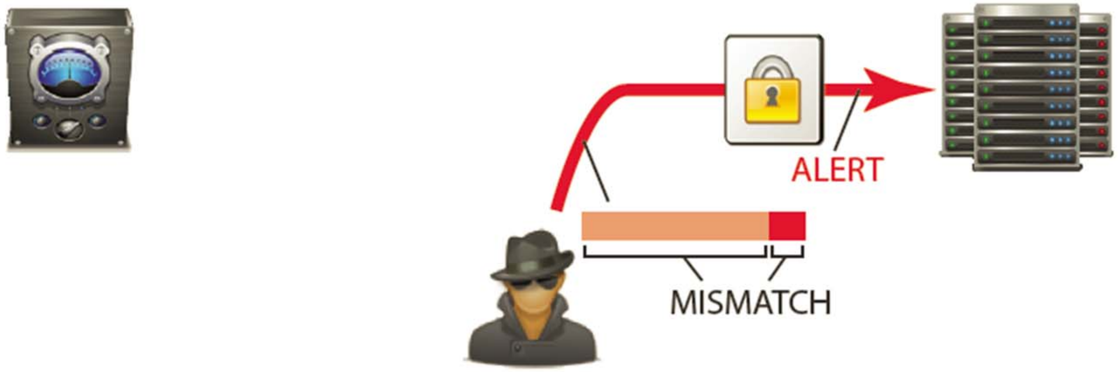
- communicated information is coded such that an unauthorized party cannot make changes without arising mistrust of authorized parties
- receiver expects a certain redundant structure in the coded data that cannot be preserved by unauthorized parties
- redundancy is introduced by adding an encrypted hash to the end of the original data

Fabrication

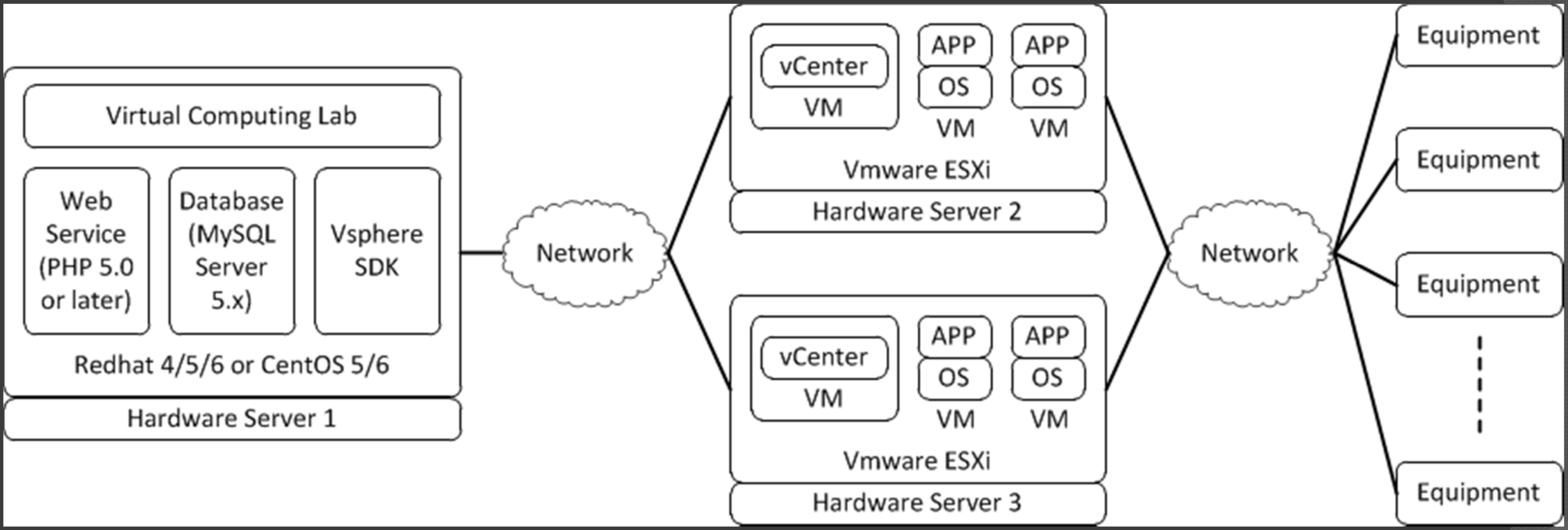


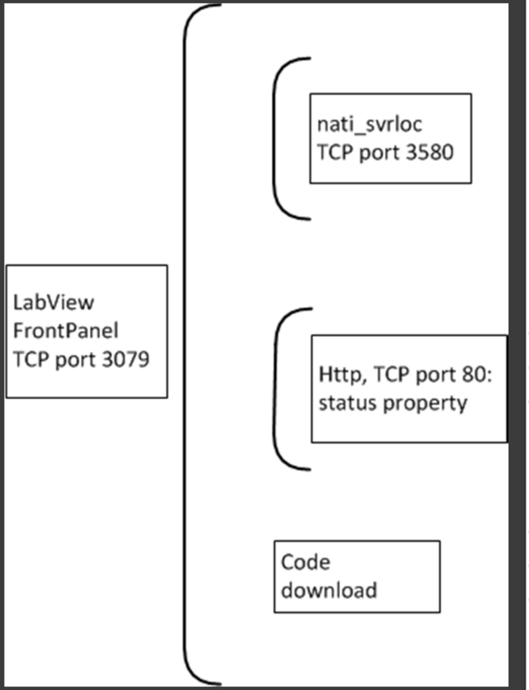
- Unauthorized party inserts counterfeit objects into the system
- Attack on authenticity
- Insertion of spurious messages in a network
- Addition of records to a file
- ICS – insertion of spurious/unwanted/unauthorized control
- ICS – adding data to a historian

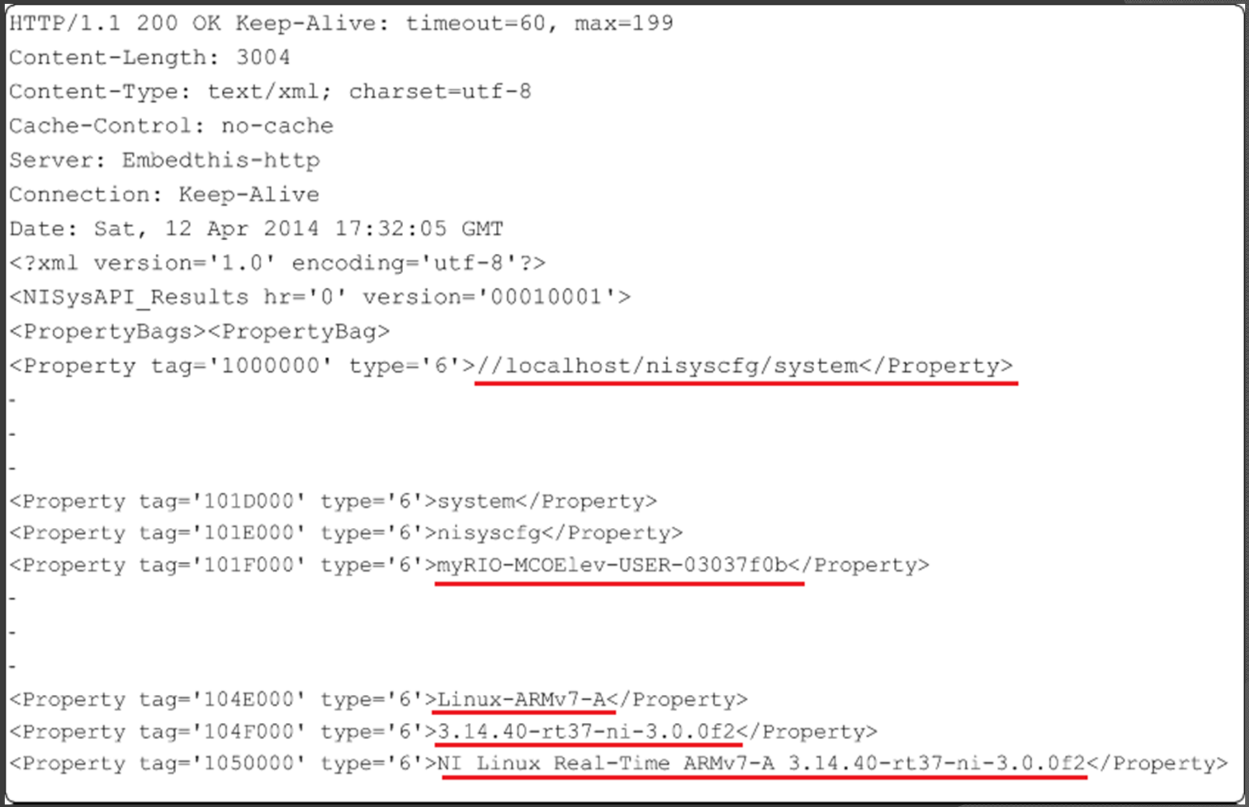
Authentication



- the digital signature adds a specific redundant structure to the information that can be verified publicly by others, but not reproduced
- the secret keying information is required to successfully produce an authentic message

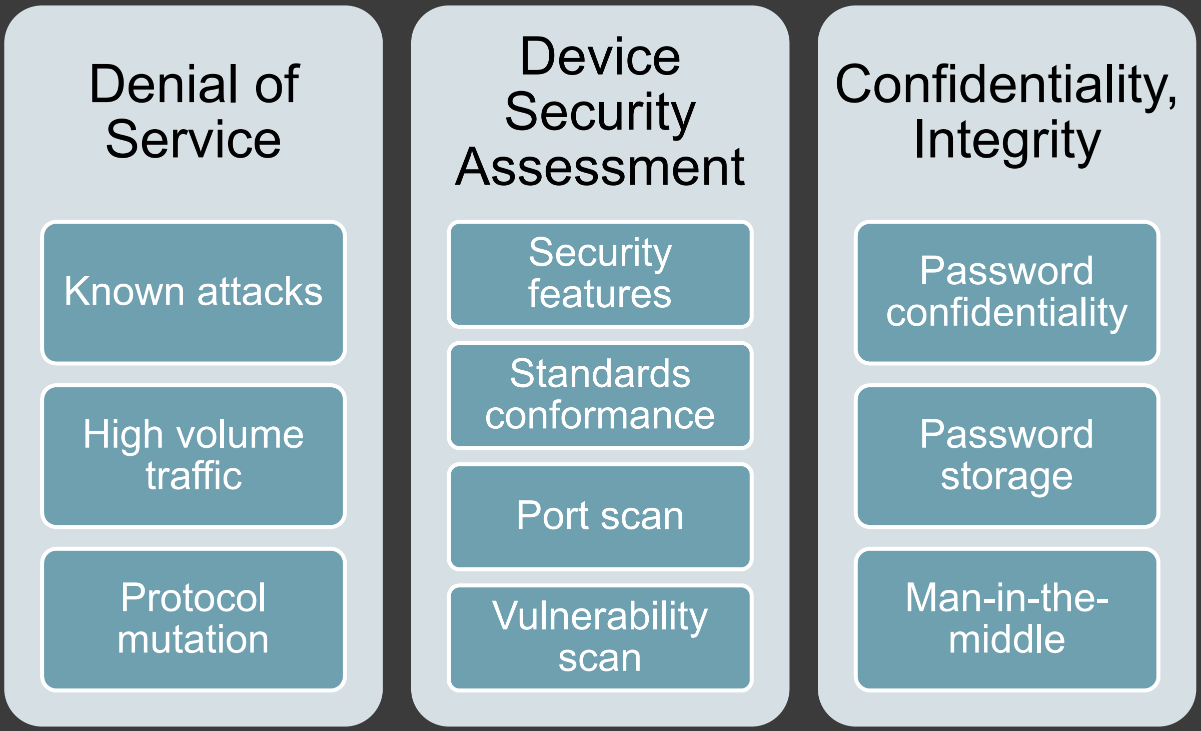

Virtual Computing Lab
Web Service (PHP 5.0 or later)
Database (MySQL Server 5.x)
Vsphere SDK
Redhat 4/5/6 or CentOS 5/6
Hardware Server 1
Network
vCenter
VM
APP
OS
VM
APP
OS
VM
Vmware ESXi
Hardware Server 2
vCenter
VM
APP
OS
VM
APP
OS
VM
Vmware ESXi
Hardware Server 3
Network
Equipment
Equipment
Equipment
Equipment


LabView FrontPanel TCP port 3079
nati_svrloc TCP port 3580
Http, TCP port 80: status property
Code download



```
HTTP/1.1 200 OK Keep-Alive: timeout=60, max=199
Content-Length: 3004
Content-Type: text/xml; charset=utf-8
Cache-Control: no-cache
Server: Embedthis-http
Connection: Keep-Alive
Date: Sat, 12 Apr 2014 17:32:05 GMT
<?xml version='1.0' encoding='utf-8'?>
<NISysAPI_Results hr='0' version='00010001'>
<PropertyBags><PropertyBag>
<Property tag='1000000' type='6'>//localhost/nisyscfg/system</Property>
-
-
-
<Property tag='101D000' type='6'>system</Property>
<Property tag='101E000' type='6'>nisyscfg</Property>
<Property tag='101F000' type='6'>myRIO-MCOElev-USER-03037f0b</Property>
-
-
-
<Property tag='104E000' type='6'>Linux-ARMv7-A</Property>
<Property tag='104F000' type='6'>3.14.40-rt37-ni-3.0.0f2</Property>
<Property tag='1050000' type='6'>NI Linux Real-Time ARMv7-A 3.14.40-rt37-ni-3.0.0f2</Property>
```

Cybersecurity Testing and Risk Assessment for Industrial Control Systems



Denial of Service

- Known attacks
- High volume traffic
- Protocol mutation

Device Security Assessment

- Security features
- Standards conformance
- Port scan
- Vulnerability scan

Confidentiality, Integrity

- Password confidentiality
- Password storage
- Man-in-the-middle

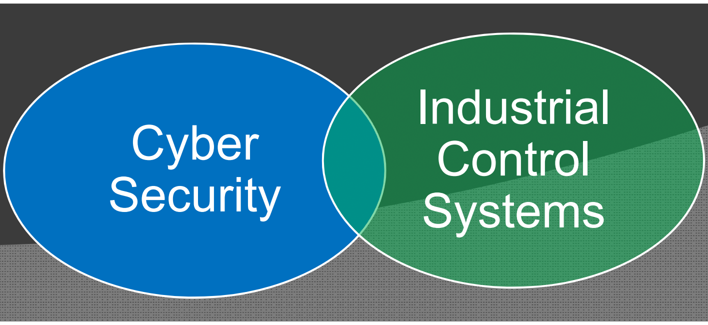
•Many vulnerabilities identified and communicated to vendor and project partner.

Critical Infrastructure Protection Center

Identify vulnerabilities, implement attacks, investigate impact on physical systems.

Develop security solutions; system protection, intrusion detection, attack resilience

Train engineers and scientists for control systems security careers.



Thank you!