LA-UR-13-26212
Approved for public release; distribution is unlimited.

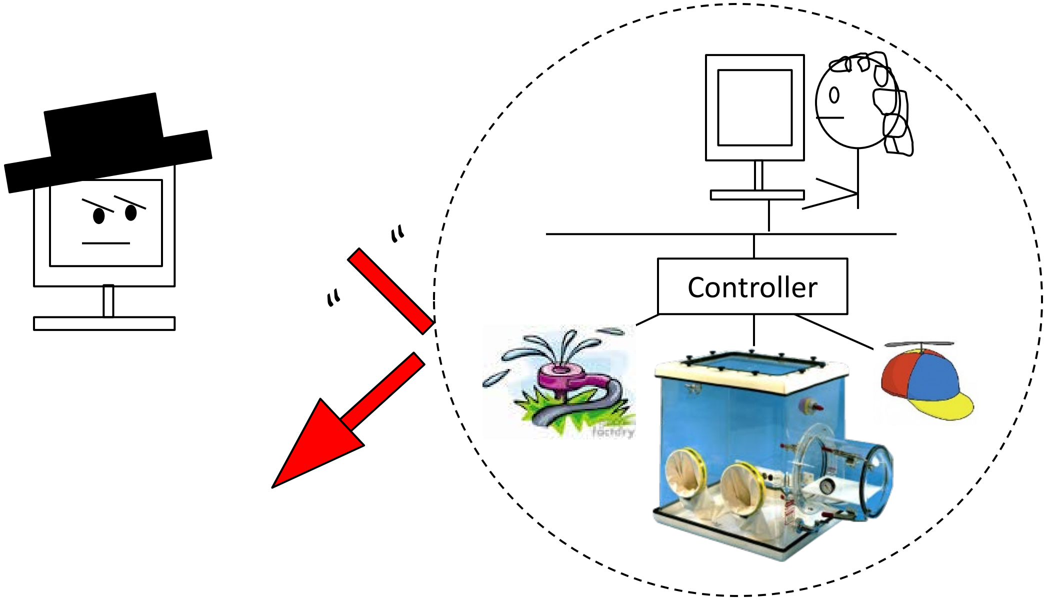
Title: Control System Security

Author(s): Frost, Sandra L.

Intended for: Engineering Managers Council Meeting, 2013-07-25 (Los Alamos, New Mexico, United States)

Issued: 2013-08-06

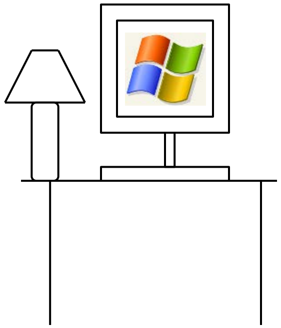
Disclaimer:
Los Alamos National Laboratory, an affirmative action/equal opportunity employer,is operated by the Los Alamos National Security, LLC for the National NuclearSecurity Administration of the U.S. Department of Energy under contract DE-AC52-06NA25396. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Departmentof Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.



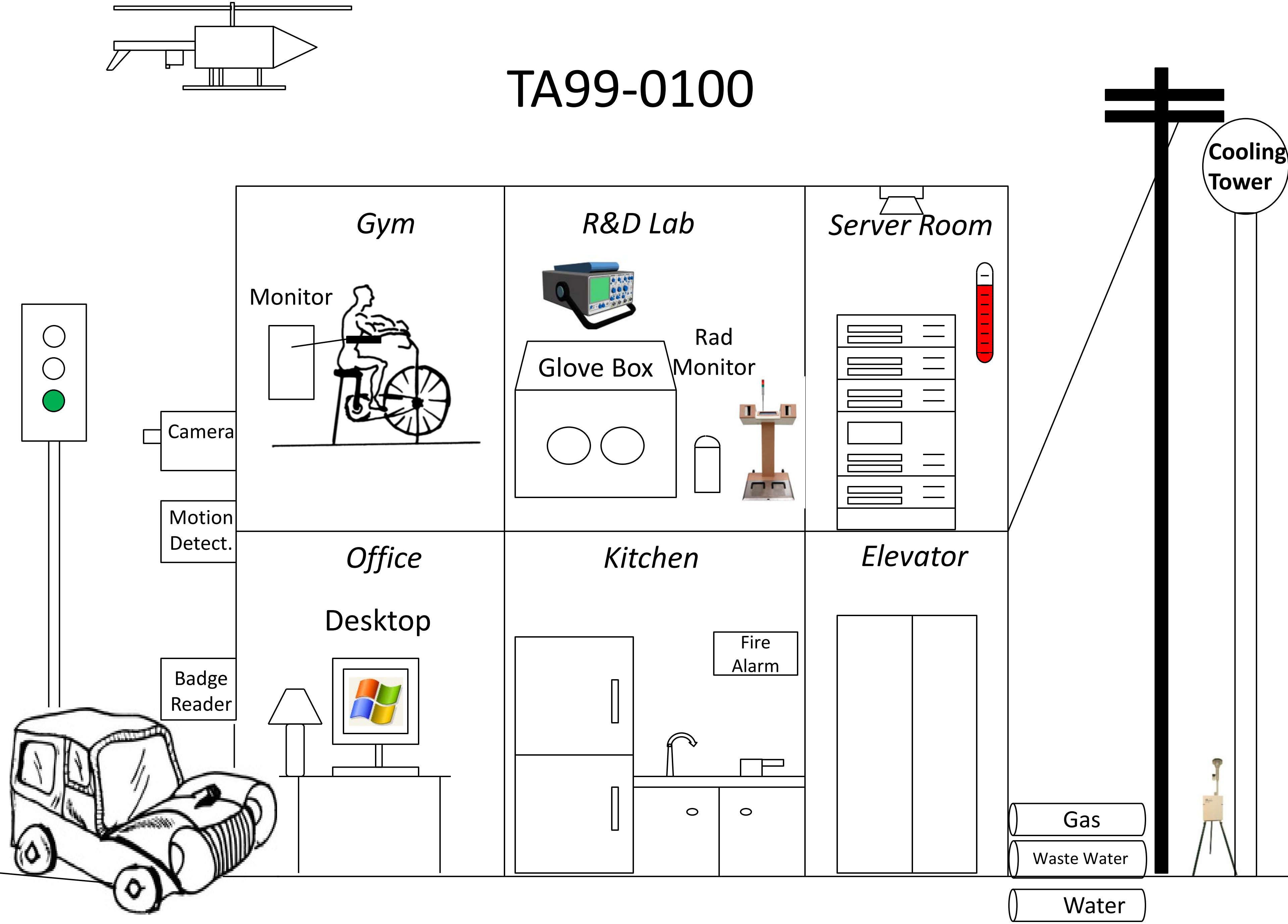
Control System Security

Sandy Frost

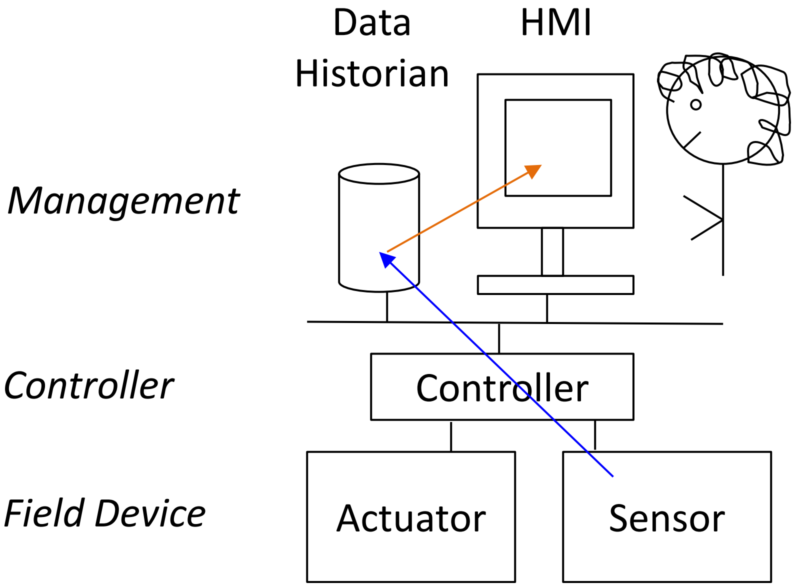
TA99-0100

Office Desktop 		

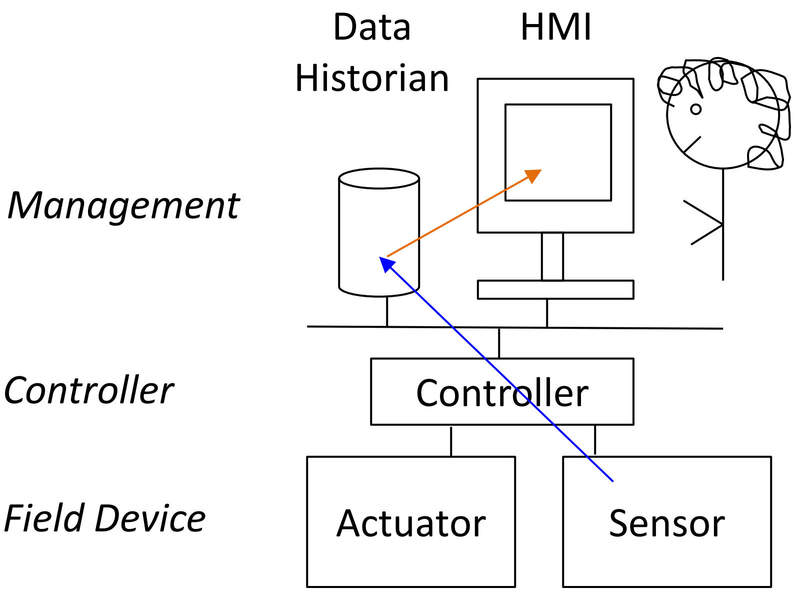
TA99-0100


Gym
R&D Lab
Server Room
Cooling Tower
Monitor
Glove Box
Rad Monitor
Camera
Motion Detect.
Office
Kitchen
Elevator
Desktop
Fire Alarm
Badge Reader
Gas
Waste Water
Water

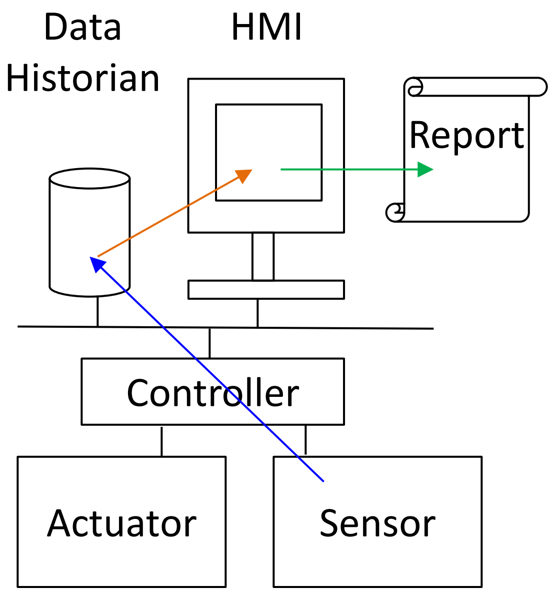
Control System

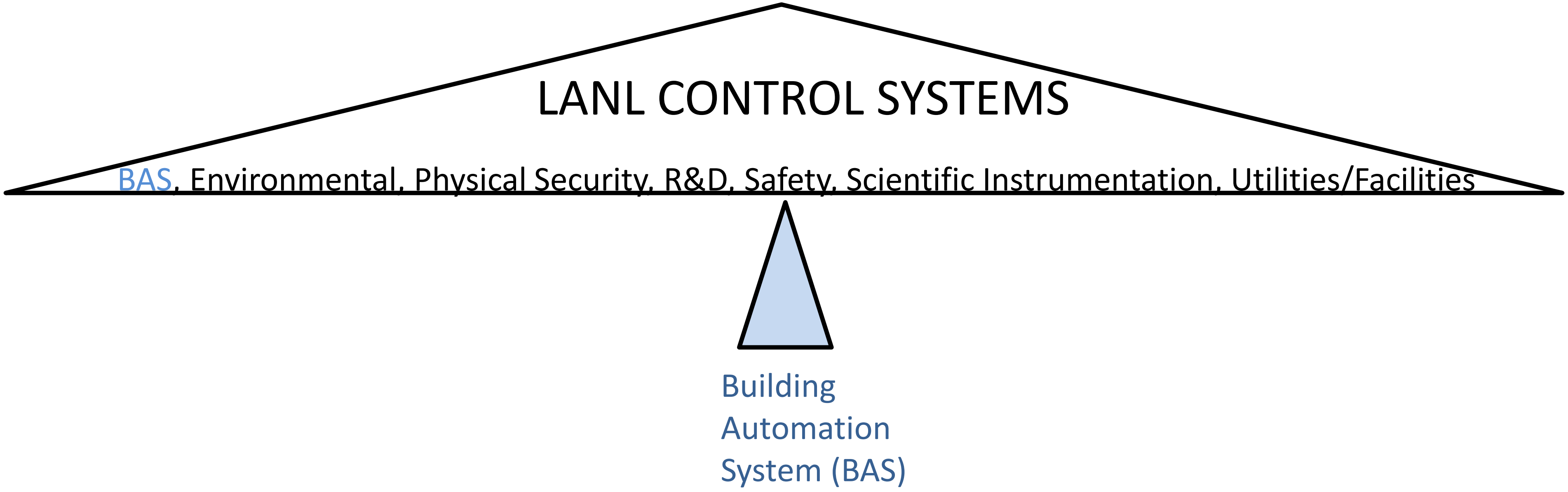


Control System



Data Acquisition System

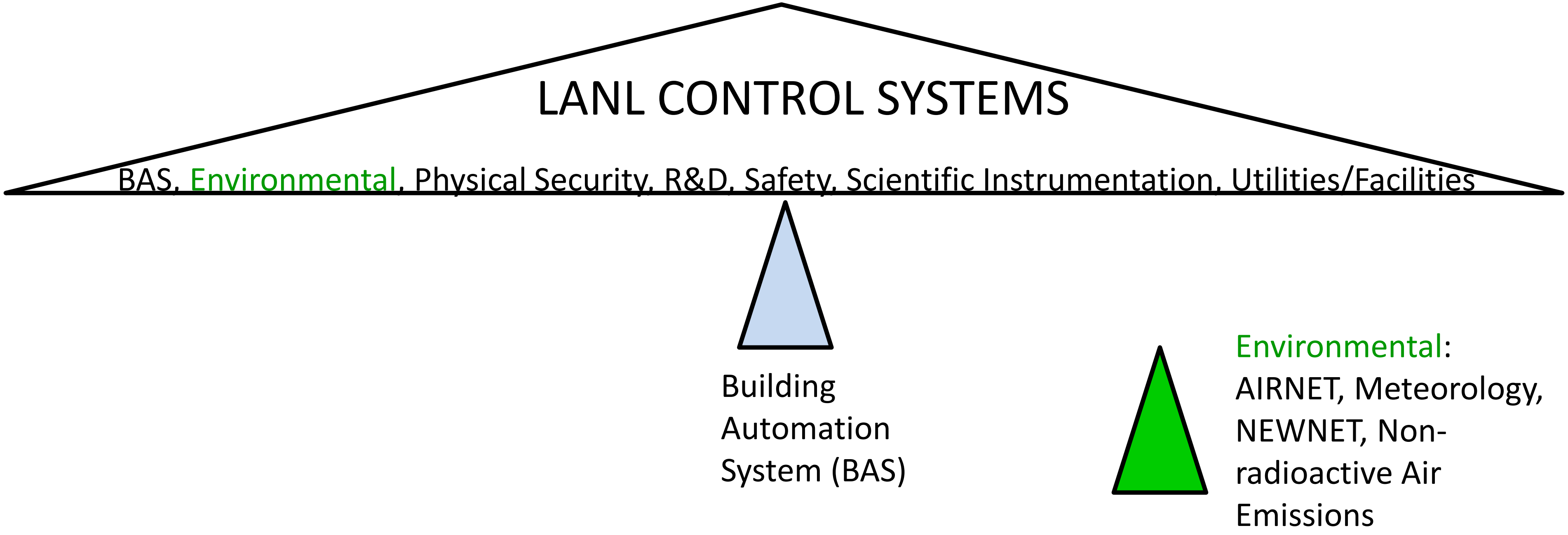




LANL CONTROL SYSTEMS

BAS, Environmental, Physical Security, R&D, Safety, Scientific Instrumentation, Utilities/Facilities

Building
Automation
System (BAS)

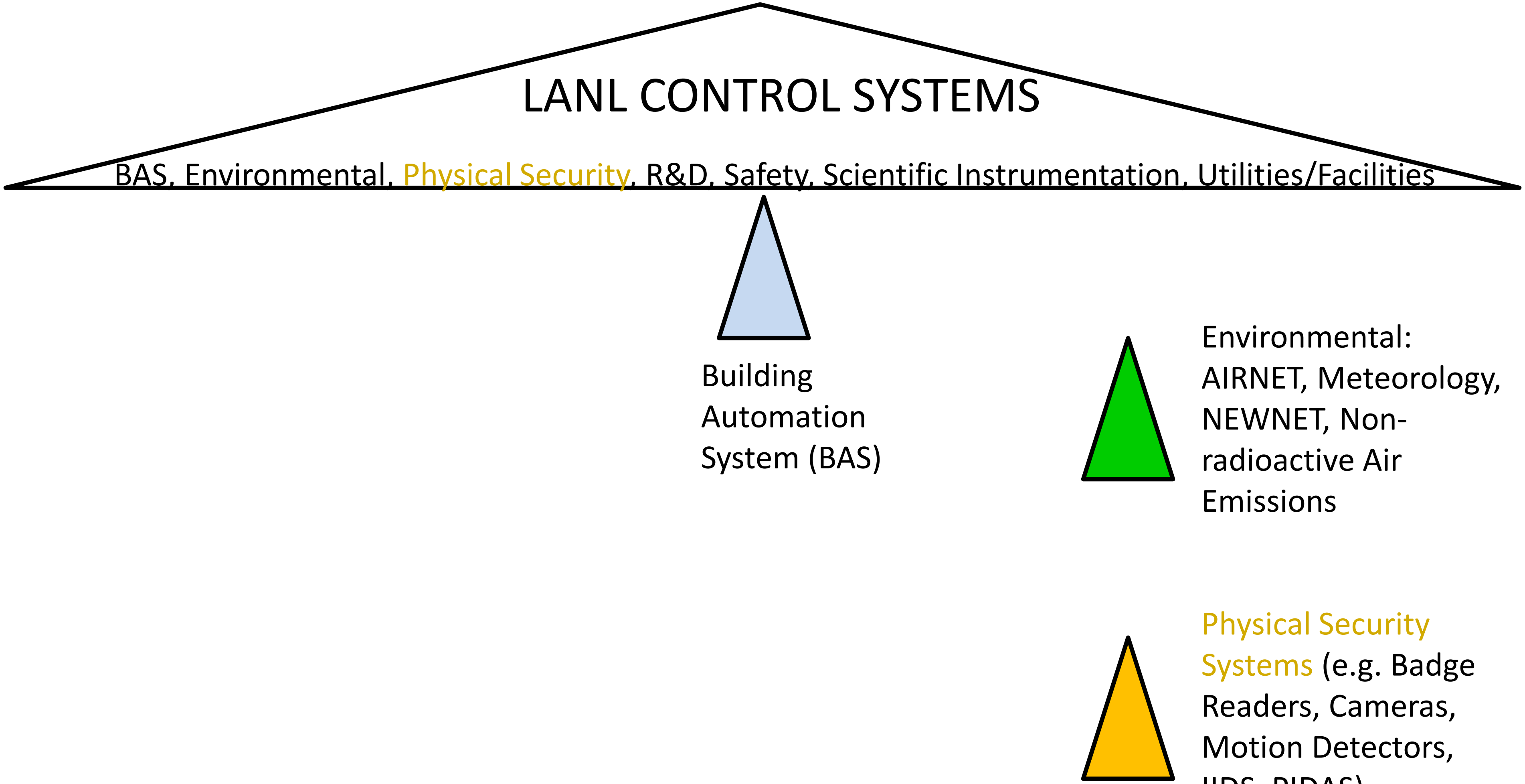


LANL CONTROL SYSTEMS

BAS, Environmental, Physical Security, R&D, Safety, Scientific Instrumentation, Utilities/Facilities

Building Automation System (BAS)

Environmental: AIRNET, Meteorology, NEWNET, Non-radioactive Air Emissions



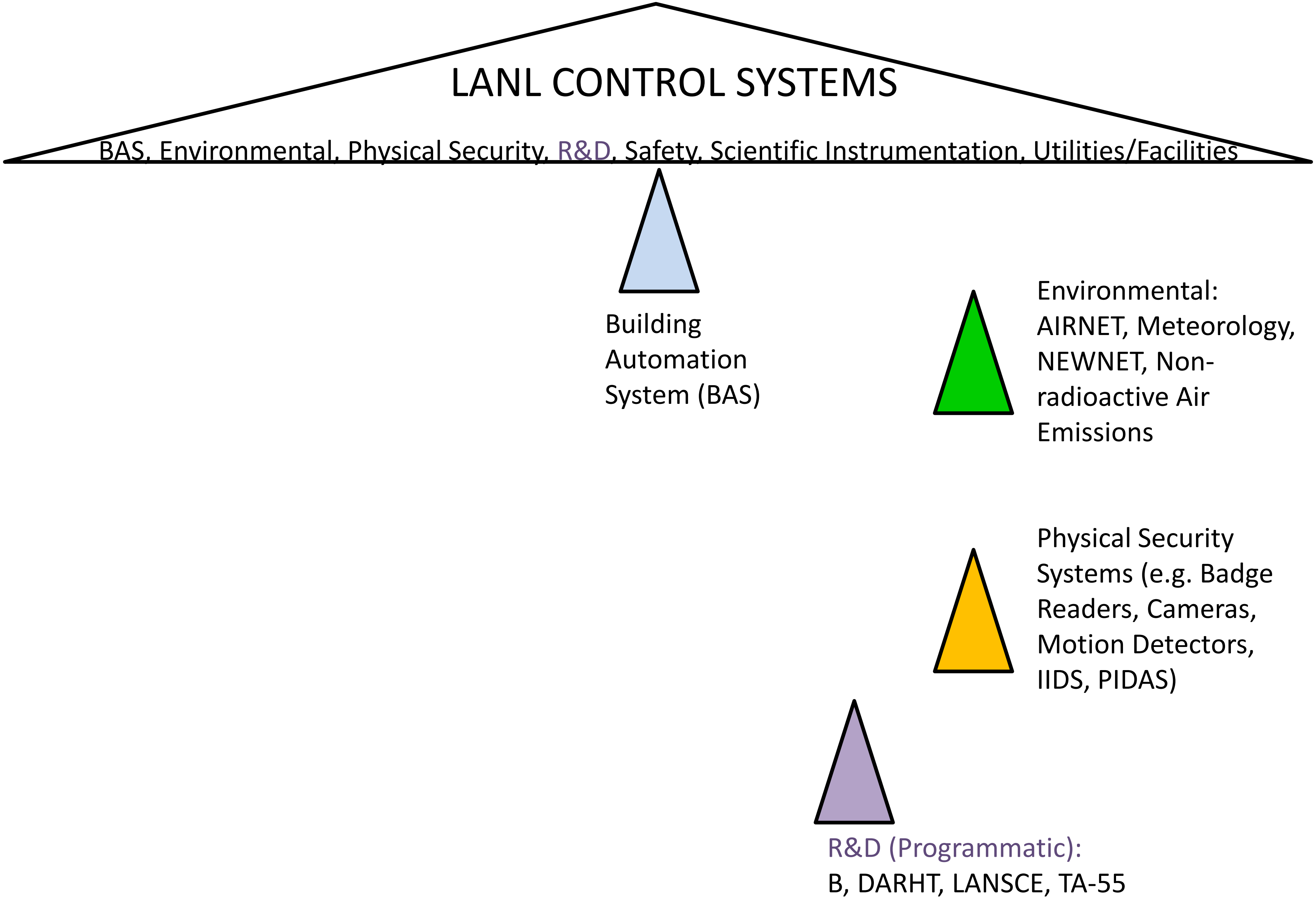
LANL CONTROL SYSTEMS

BAS, Environmental, Physical Security, R&D, Safety, Scientific Instrumentation, Utilities/Facilities

Building Automation System (BAS)

Environmental: AIRNET, Meteorology, NEWNET, Non-radioactive Air Emissions

Physical Security Systems (e.g. Badge Readers, Cameras, Motion Detectors, IIDS, PIDAS)



LANL CONTROL SYSTEMS

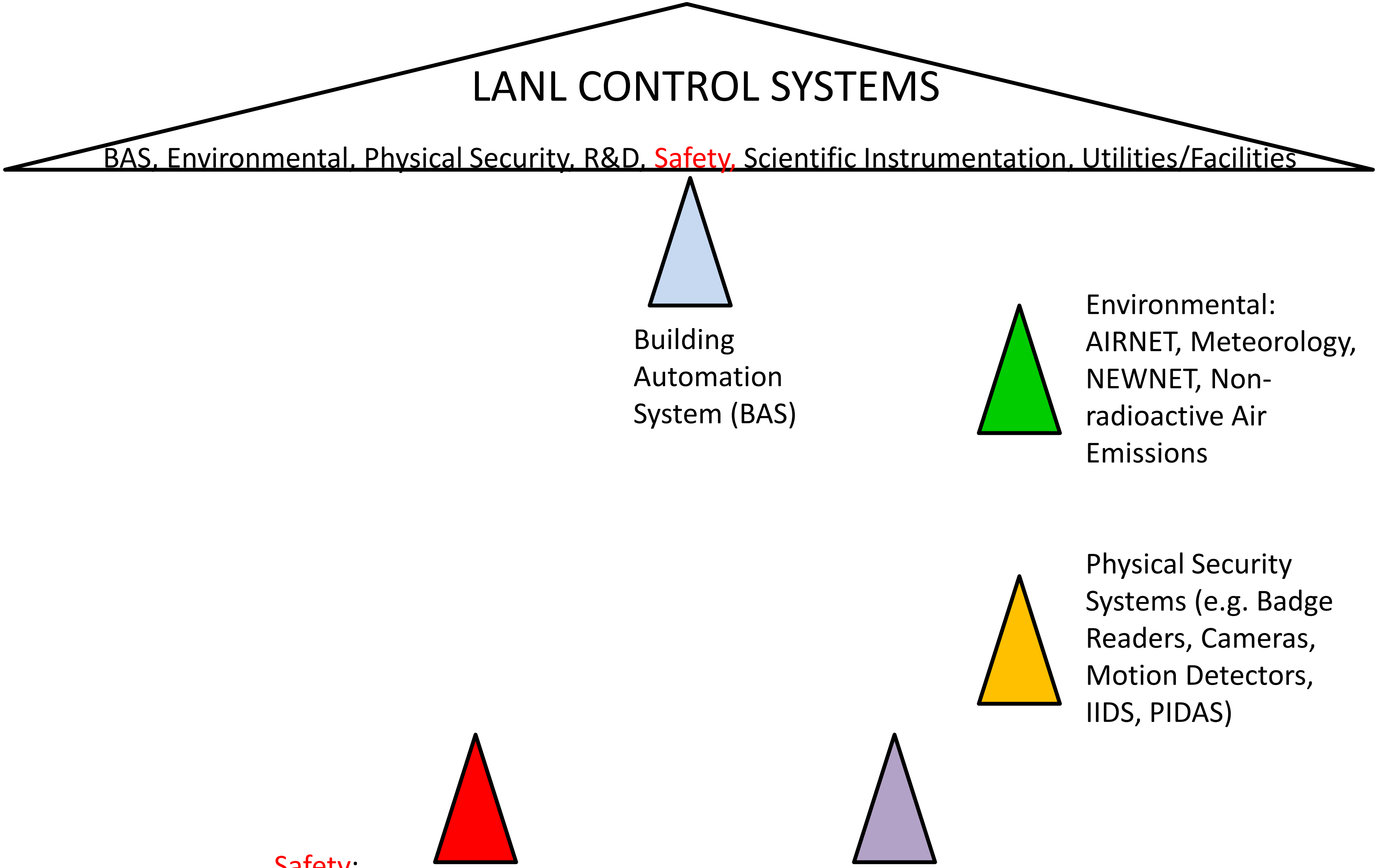
BAS, Environmental, Physical Security, R&D, Safety, Scientific Instrumentation, Utilities/Facilities

Building Automation System (BAS)

Environmental: AIRNET, Meteorology, NEWNET, Non-radioactive Air Emissions

Physical Security Systems (e.g. Badge Readers, Cameras, Motion Detectors, IIDS, PIDAS)

R&D (Programmatic): B, DARHT, LANSCE, TA-55



LANL CONTROL SYSTEMS

BAS, Environmental, Physical Security, R&D, Safety, Scientific Instrumentation, Utilities/Facilities

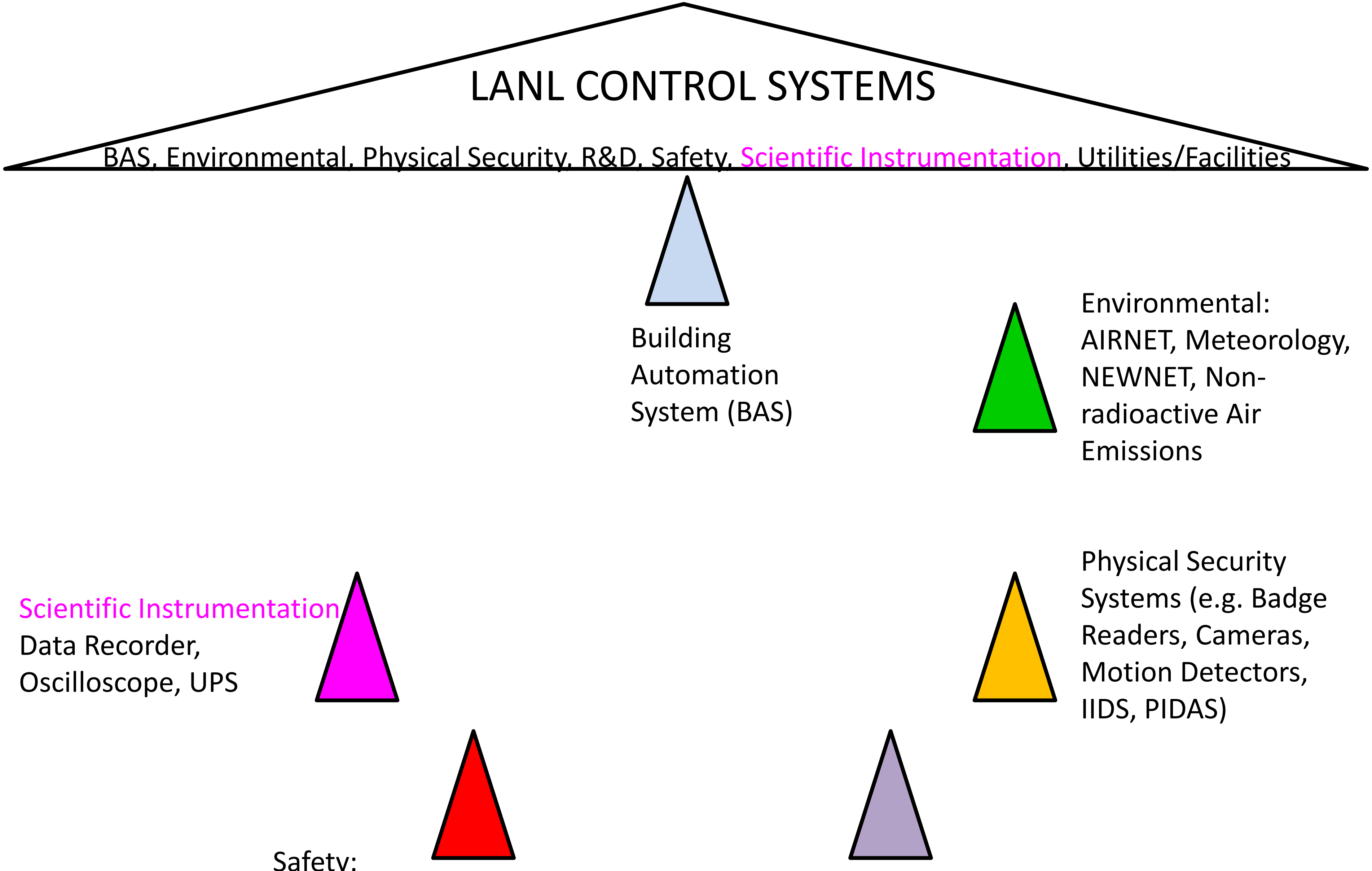
Building Automation System (BAS)

Environmental:
AIRNET, Meteorology, NEWNET, Non-radioactive Air Emissions

Physical Security Systems (e.g. Badge Readers, Cameras, Motion Detectors, IIDS, PIDAS)

Safety:
Airborne Radioactivity,
External Radiation Fields,
Occupational Medicine, Material At Risk,
Safety Instrumented Systems, UAV

R&D (Programmatic):
B, DARHT, LANSCE, TA-55



LANL CONTROL SYSTEMS

BAS, Environmental, Physical Security, R&D, Safety, Scientific Instrumentation, Utilities/Facilities

Building Automation System (BAS)

Environmental:
AIRNET, Meteorology, NEWNET, Non-radioactive Air Emissions

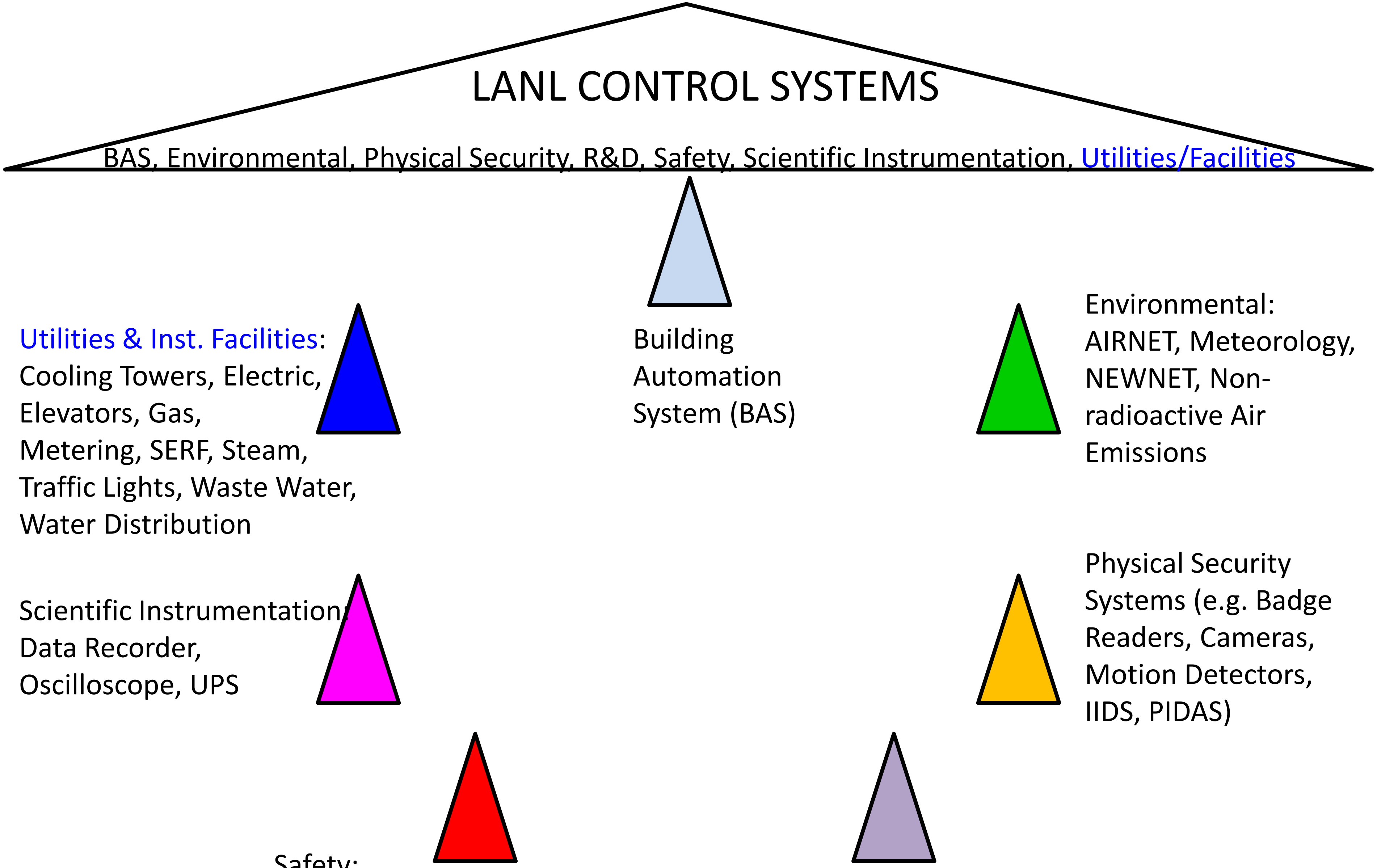
Scientific Instrumentation
Data Recorder, Oscilloscope, UPS

Physical Security Systems (e.g. Badge Readers, Cameras, Motion Detectors, IIDS, PIDAS)

Safety:
Airborne Radioactivity,
External Radiation Fields,
Occupational Medicine, Material At Risk,
Safety Instrumented Systems, UAV

R&D (Programmatic):
B, DARHT, LANSCE, TA-55

LANL CONTROL SYSTEMS



BAS, Environmental, Physical Security, R&D, Safety, Scientific Instrumentation, Utilities/Facilities

Building Automation System (BAS)

Utilities & Inst. Facilities: Cooling Towers, Electric, Elevators, Gas, Metering, SERF, Steam, Traffic Lights, Waste Water, Water Distribution

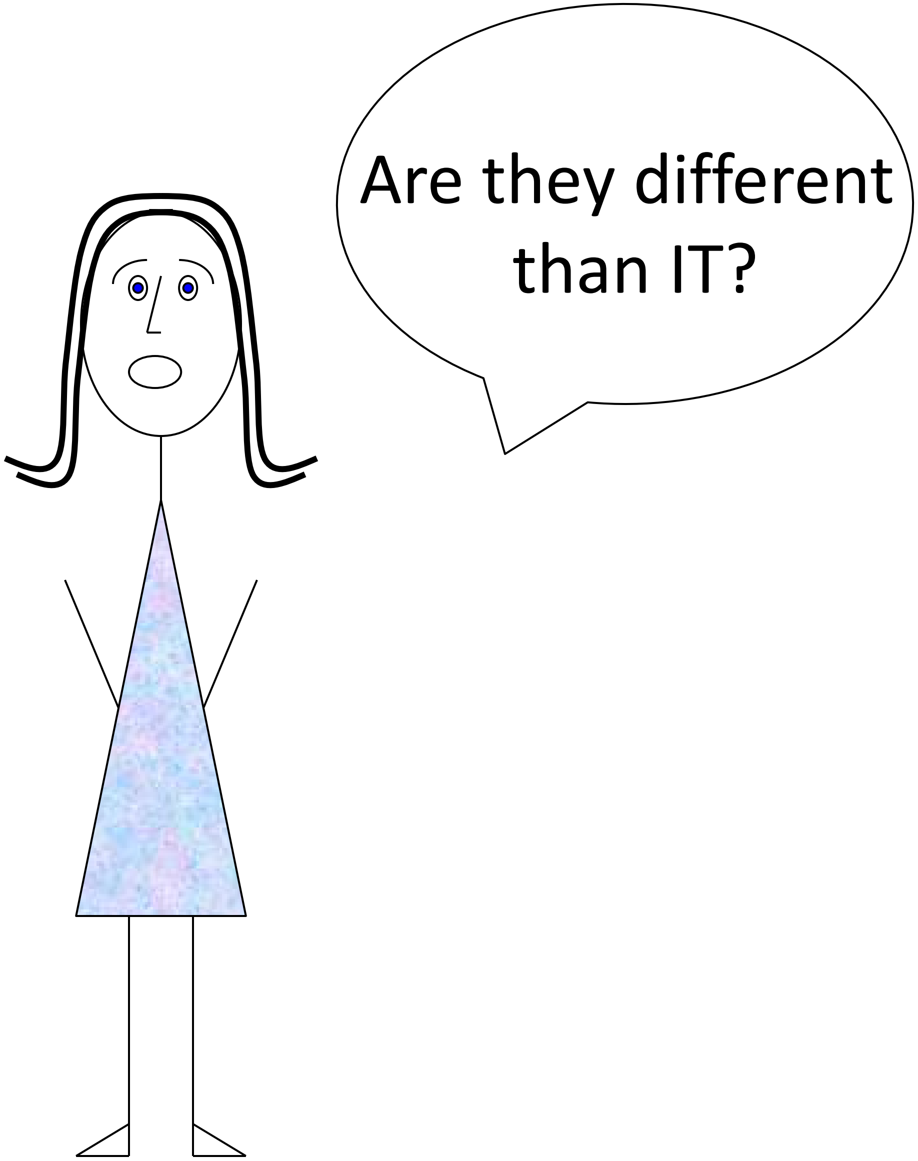
Environmental: AIRNET, Meteorology, NEWNET, Non-radioactive Air Emissions

Scientific Instrumentation: Data Recorder, Oscilloscope, UPS

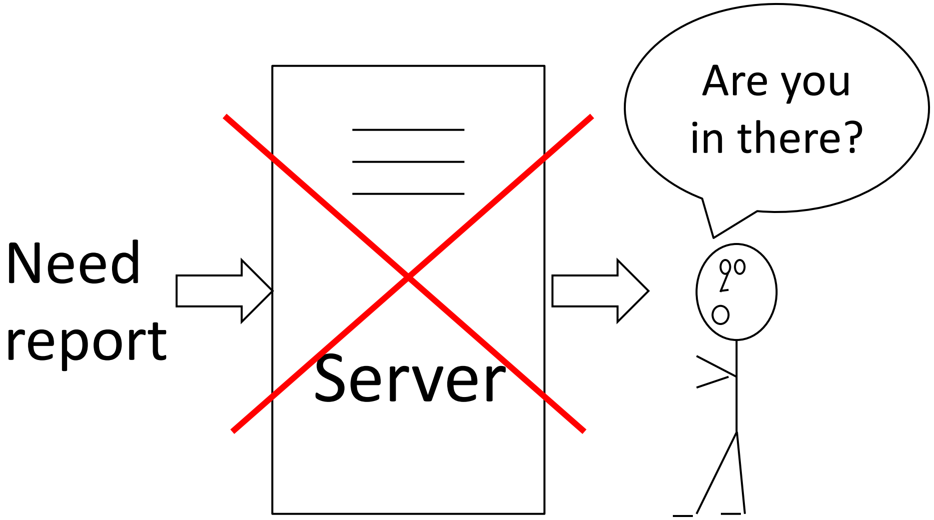
Physical Security Systems (e.g. Badge Readers, Cameras, Motion Detectors, IIDS, PIDAS)

Safety: Airborne Radioactivity, External Radiation Fields, Occupational Medicine, Material At Risk, Safety Instrumented Systems, UAV

R&D (Programmatic): B, DARHT, LANSCE, TA-55


Are they different than IT?

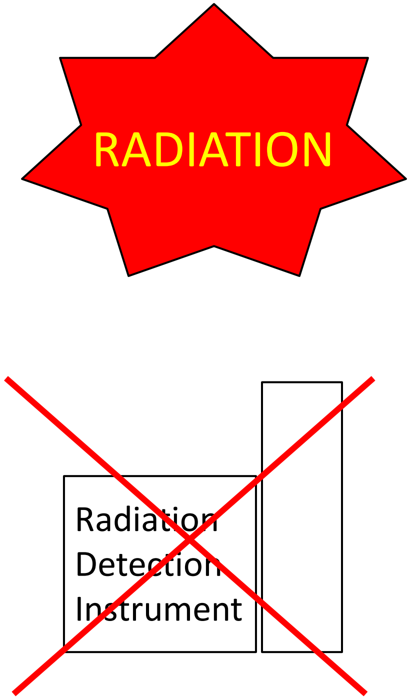
Risk Management



Need report

Server

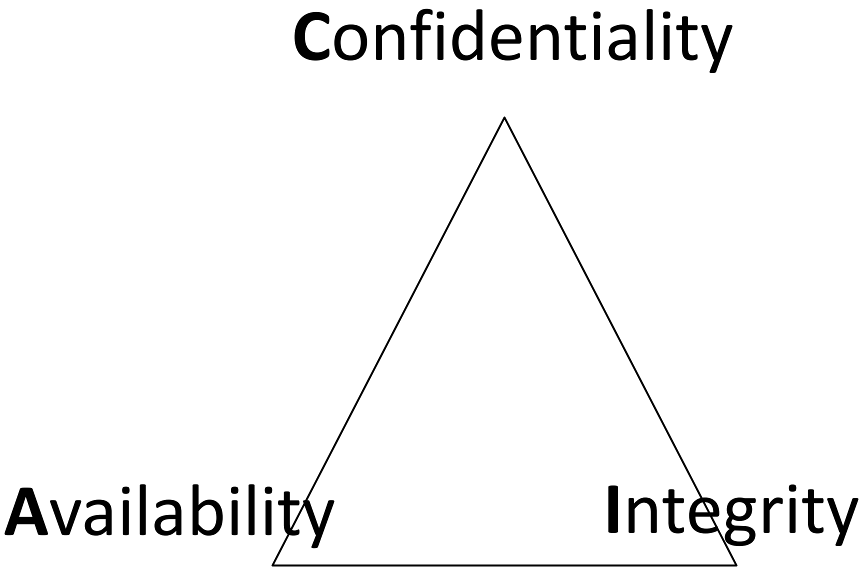
Are you in there?



RADIATION

Radiation Detection Instrument

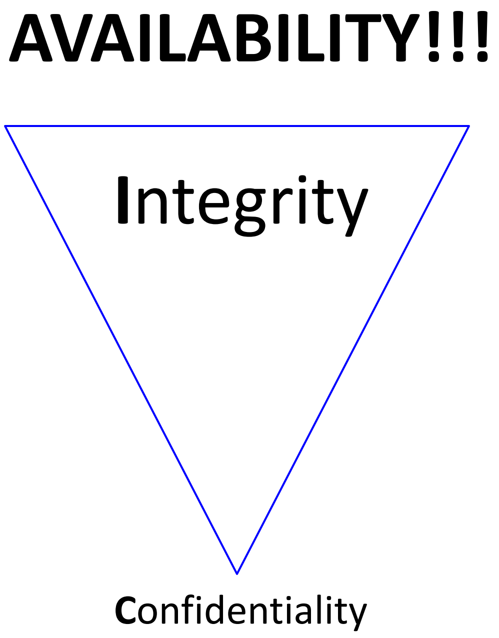
Security Objectives



Confidentiality

Availability

Integrity

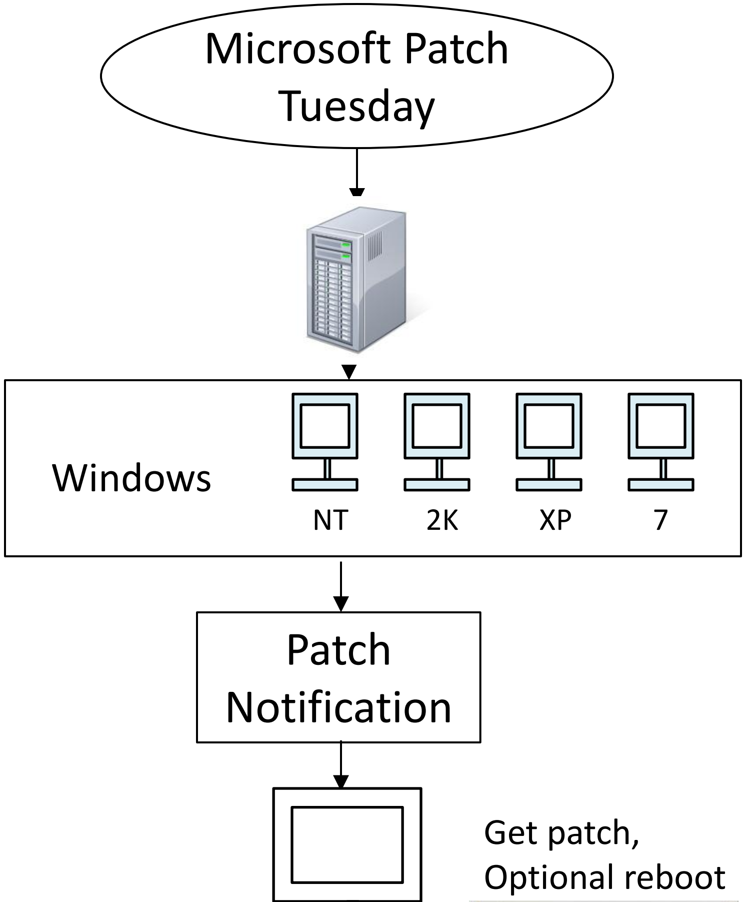


AVAILABILITY!!!

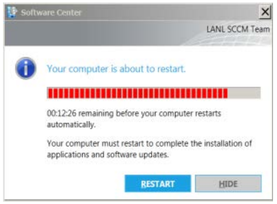
Integrity

Confidentiality

Change Management



Get patch,
Optional reboot

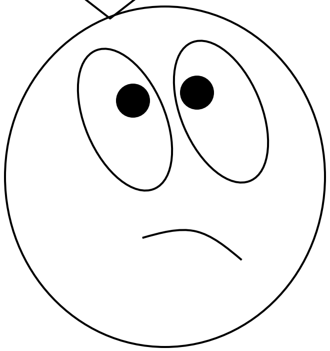


Your computer is about to restart.

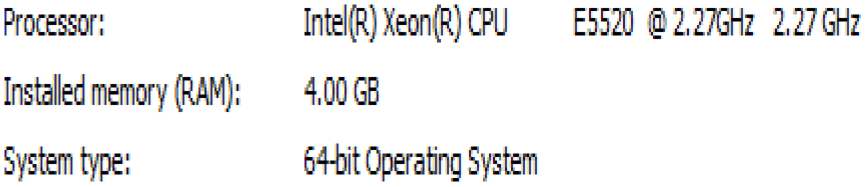
00:12:26 remaining before your computer restarts automatically.

Your computer must restart to complete the installation of applications and software updates.

- Individual vendor sites
- Little test equipment
- Few dedicated teams to test patches
- Have to schedule update, especially if reboot reqd
- Change firmware?
- …



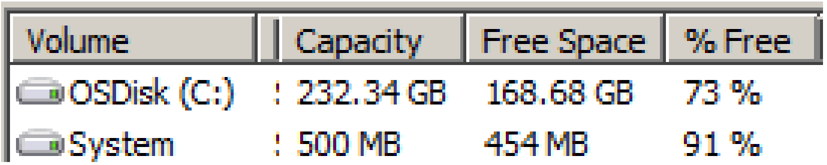
Resource Constraints



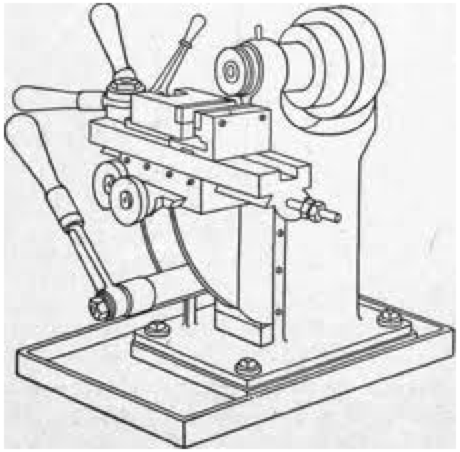
Processor: Intel(R) Xeon(R) CPU E5520 @ 2.27GHz 2.27 GHz

Installed memory (RAM): 4.00 GB

System type: 64-bit Operating System

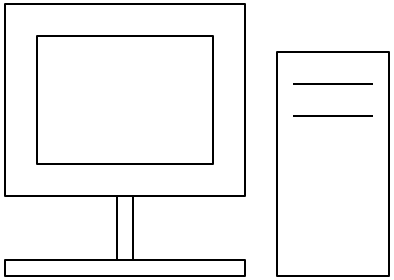


Volume	Capacity	Free Space	% Free
OSDisk (C:)	232.34 GB	168.68 GB	73 %
System	500 MB	454 MB	91 %



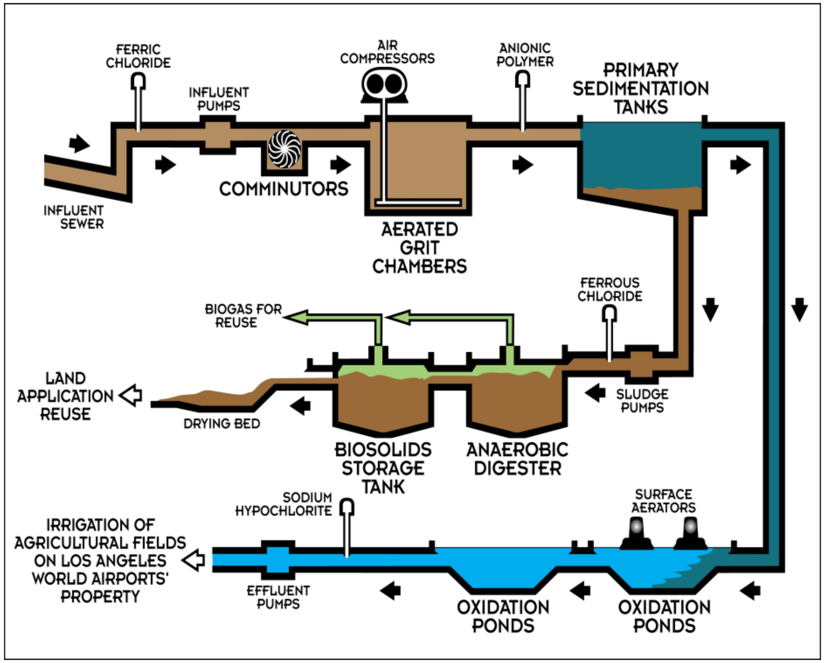
OS: DOS 3.0
Processor: ?
RAM: ? (bubble memory)
Disk capacity: ?

Component Life Cycle



Tech refresh is 3-5 years

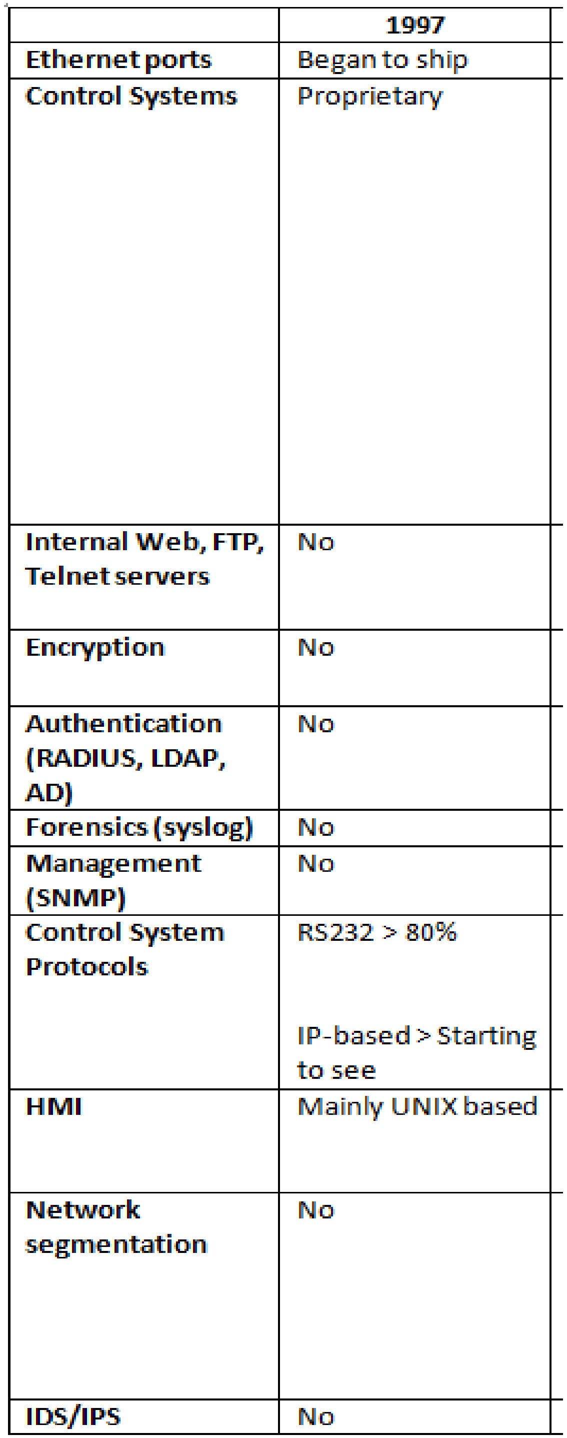
Wastewater Treatment



What "tech refresh"?

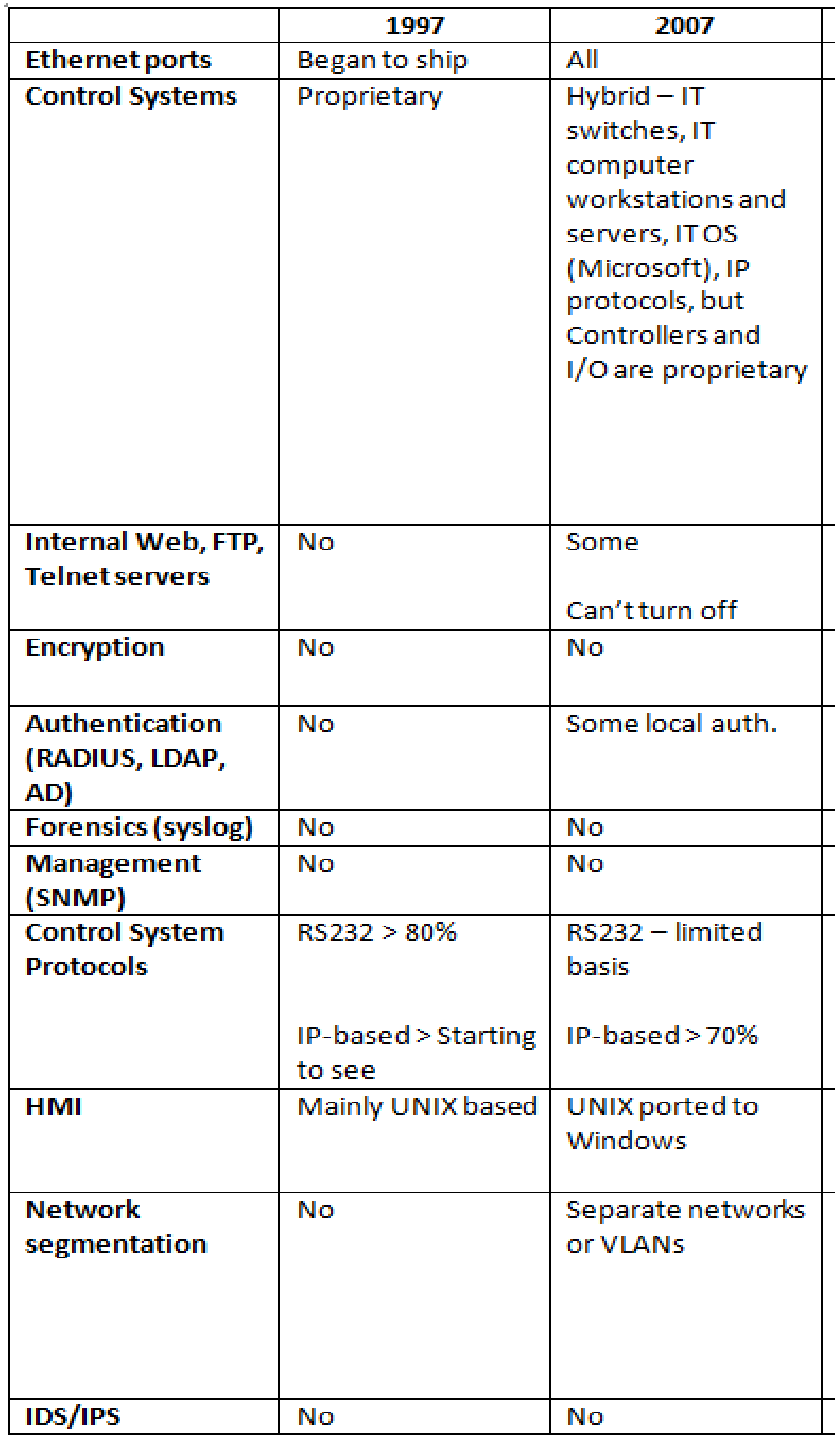
Are they vulnerable?

Control System Timeline



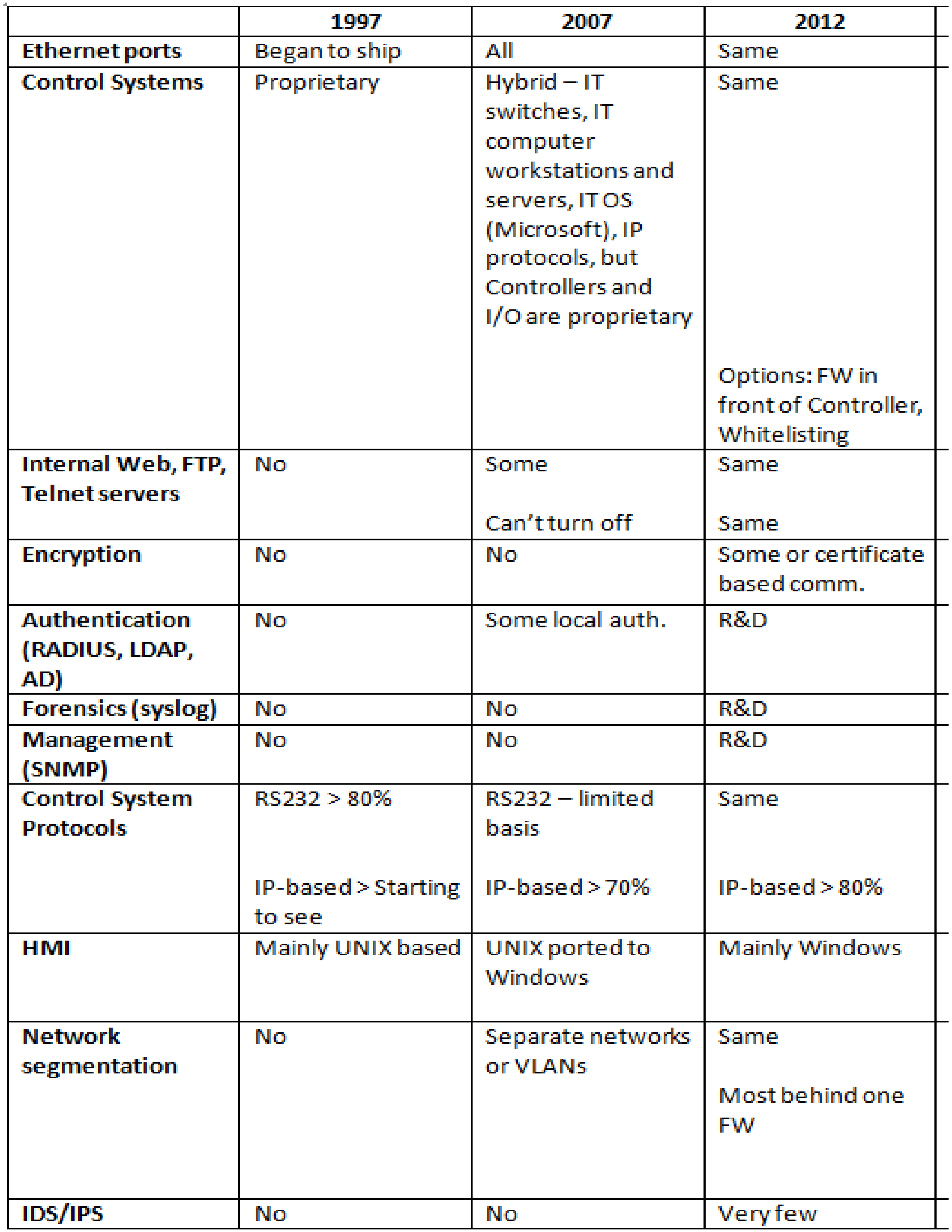
	1997
Ethernet ports	Began to ship
Control Systems	Proprietary
Internal Web, FTP, Telnet servers	No
Encryption	No
Authentication (RADIUS, LDAP, AD)	No
Forensics (syslog)	No
Management (SNMP)	No
Control System Protocols	RS232 > 80% IP-based > Starting to see
HMI	Mainly UNIX based
Network segmentation	No
IDS/IPS	No

Control System Timeline



	1997	2007
Ethernet ports	Began to ship	All
Control Systems	Proprietary	Hybrid – IT switches, IT computer workstations and servers, IT OS (Microsoft), IP protocols, but Controllers and I/O are proprietary
Internal Web, FTP, Telnet servers	No	Some Can't turn off
Encryption	No	No
Authentication (RADIUS, LDAP, AD)	No	Some local auth.
Forensics (syslog)	No	No
Management (SNMP)	No	No
Control System Protocols	RS232 > 80% IP-based > Starting to see	RS232 – limited basis IP-based > 70%
HMI	Mainly UNIX based	UNIX ported to Windows
Network segmentation	No	Separate networks or VLANs
IDS/IPS	No	No

Control System Timeline



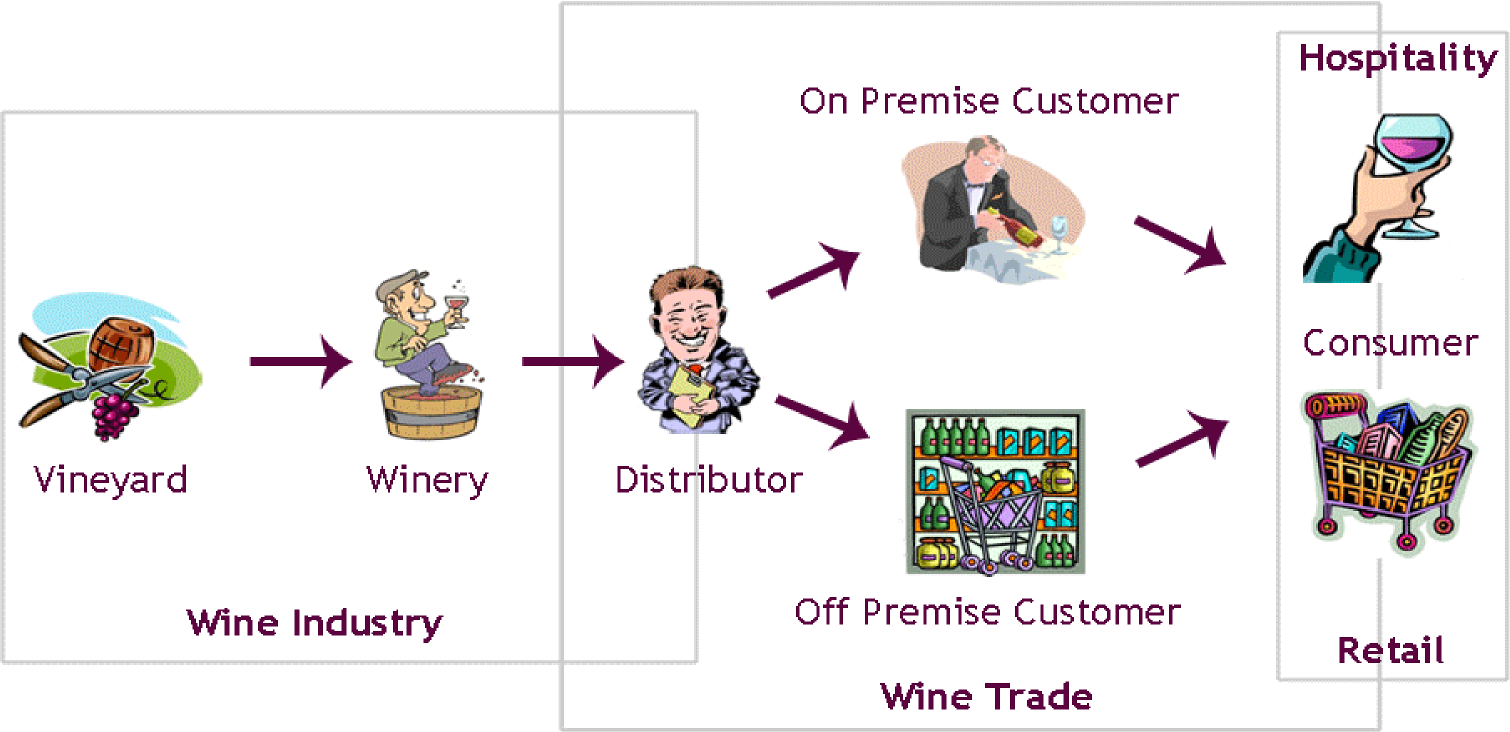
	1997	2007	2012
Ethernet ports	Began to ship	All	Same
Control Systems	Proprietary	Hybrid – IT switches, IT computer workstations and servers, IT OS (Microsoft), IP protocols, but Controllers and I/O are proprietary	Same Options: FW in front of Controller, Whitelisting
Internal Web, FTP, Telnet servers	No	Some Can't turn off	Same Same
Encryption	No	No	Some or certificate based comm.
Authentication (RADIUS, LDAP, AD)	No	Some local auth.	R&D
Forensics (syslog)	No	No	R&D
Management (SNMP)	No	No	R&D
Control System Protocols	RS232 > 80% IP-based > Starting to see	RS232 – limited basis IP-based > 70%	Same IP-based > 80%
HMI	Mainly UNIX based	UNIX ported to Windows	Mainly Windows
Network segmentation	No	Separate networks or VLANs	Same Most behind one FW
IDS/IPS	No	No	Very few

Control System Timeline

	1997	2007	2012	2017
Ethernet ports	Began to ship	All	Same	Same
Control Systems	Proprietary	Hybrid – IT switches, IT computer workstations and servers, IT OS (Microsoft), IP protocols, but Controllers and I/O are proprietary	Same Options: FW in front of Controller, Whitelisting	Same Security by default
Internal Web, FTP, Telnet servers	No	Some Can't turn off	Same Same	Fully supported Can turn on/off
Encryption	No	No	Some or certificate based comm.	Yes
Authentication (RADIUS, LDAP, AD)	No	Some local auth.	R&D	Yes
Forensics (syslog)	No	No	R&D	Yes
Management (SNMP)	No	No	R&D	Yes
Control System Protocols	RS232 > 80% IP-based > Starting to see	RS232 – limited basis IP-based > 70%	Same IP-based > 80%	Same IP-based > 90%
HMI	Mainly UNIX based	UNIX ported to Windows	Mainly Windows	Pushback from Microsoft vuls to UNIX
Network segmentation	No	Separate networks or VLANs	Same Most behind one FW	same Most behind layered FW system with multiple DMZs
IDS/IPS	No	No	Very few	Yes

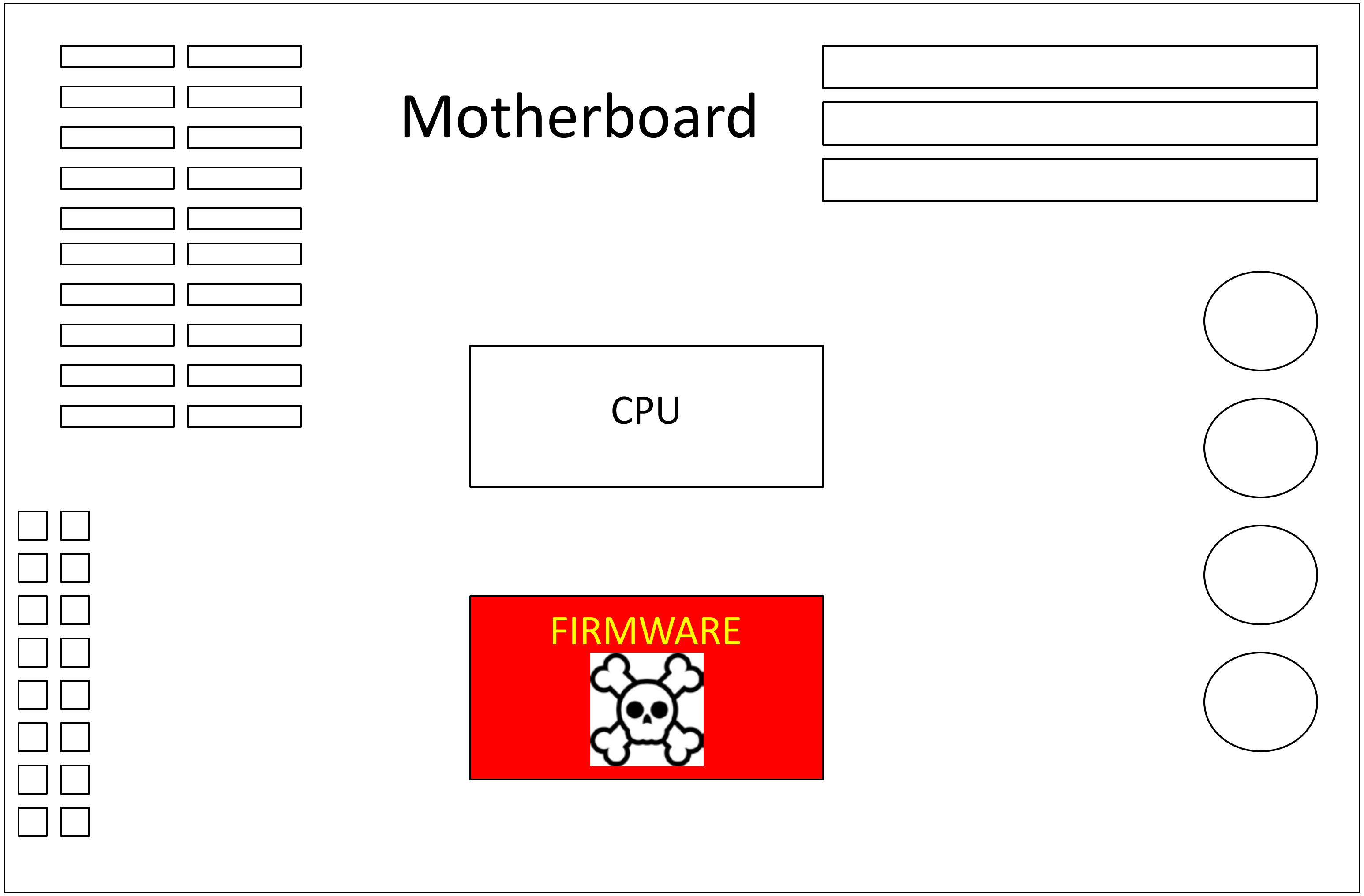
Supply Chain

- A system of organizations, people technology, activities, information and resources involved in moving a product of service from supplier to customer. Wikipedia



http://www.thewinerep.com/index.php/why-thewinerep-com/

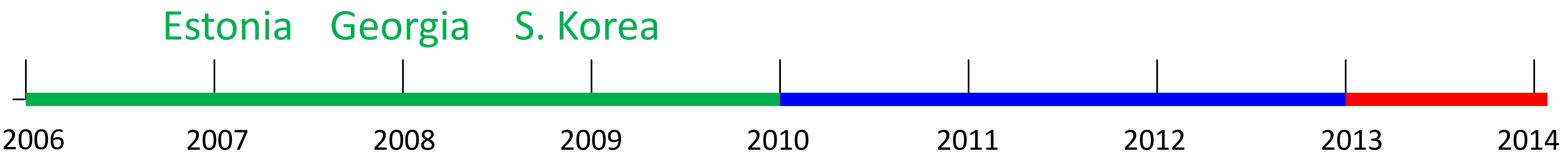
Are you already owned?



What are the threats?

Timeline

Pre-Stuxnet

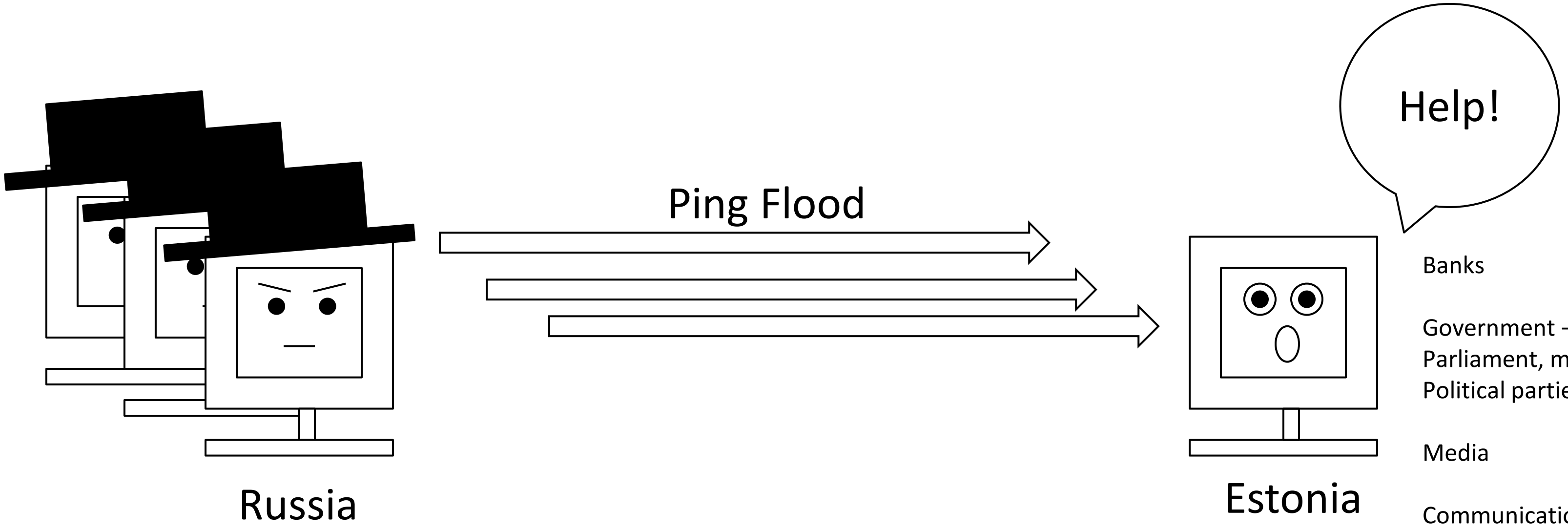


Estonia Georgia S. Korea

2006 2007 2008 2009 2010 2011 2012 2013 2014

Estonia – April 2007

Relocated Bronze Soldier of Tallinn



Banks

Government – presidency,
Parliament, ministries,
Political parties

Media

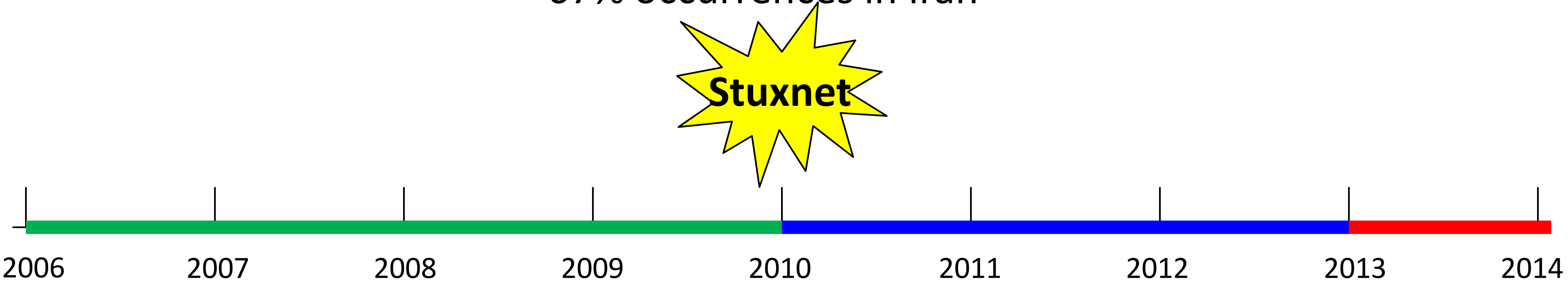
Communications

http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia,
http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

Timeline

Pre-Stuxnet

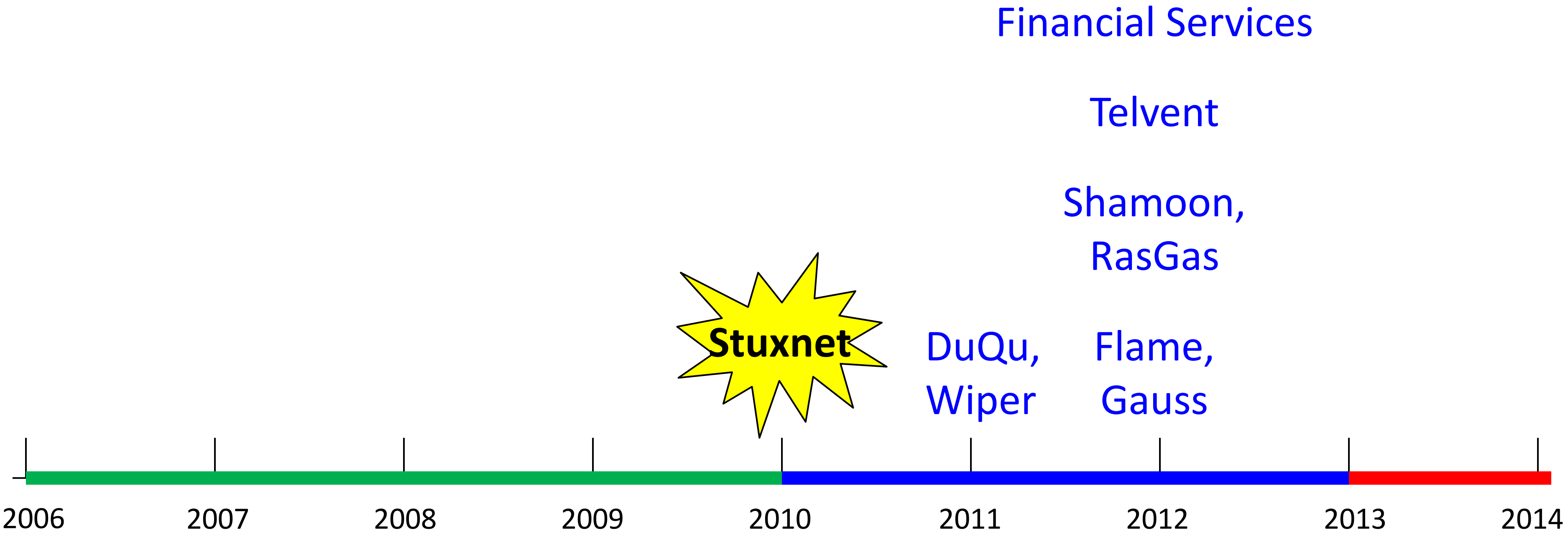
- 4 zero days
- 2 stolen dig. Certificates
- Disables AV
- USB jumps “air gap”
- First PLC rootkit
- Took 10 people 6 months to create
- 67% occurrences in Iran



Timeline

Pre-Stuxnet

Stuxnet Awareness



Financial Services

Telvent

Shamoon,
RasGas

DuQu,
Wiper

Flame,
Gauss

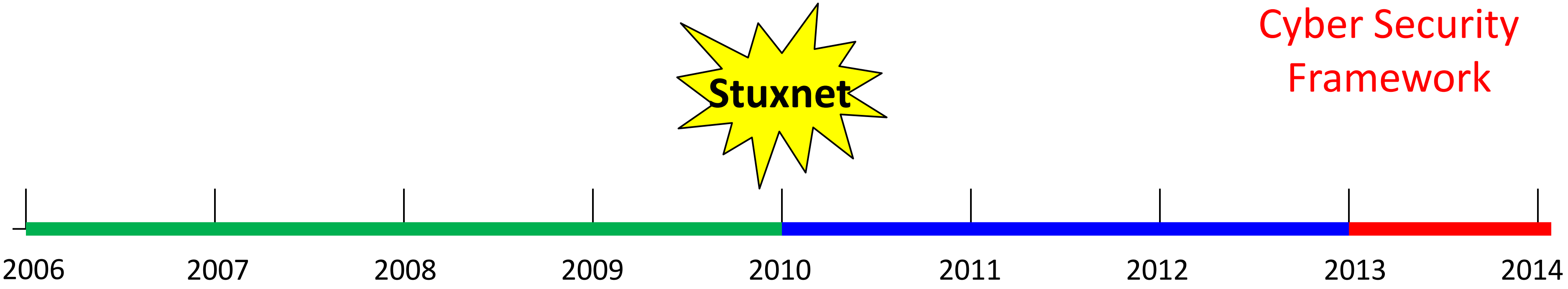
Timeline

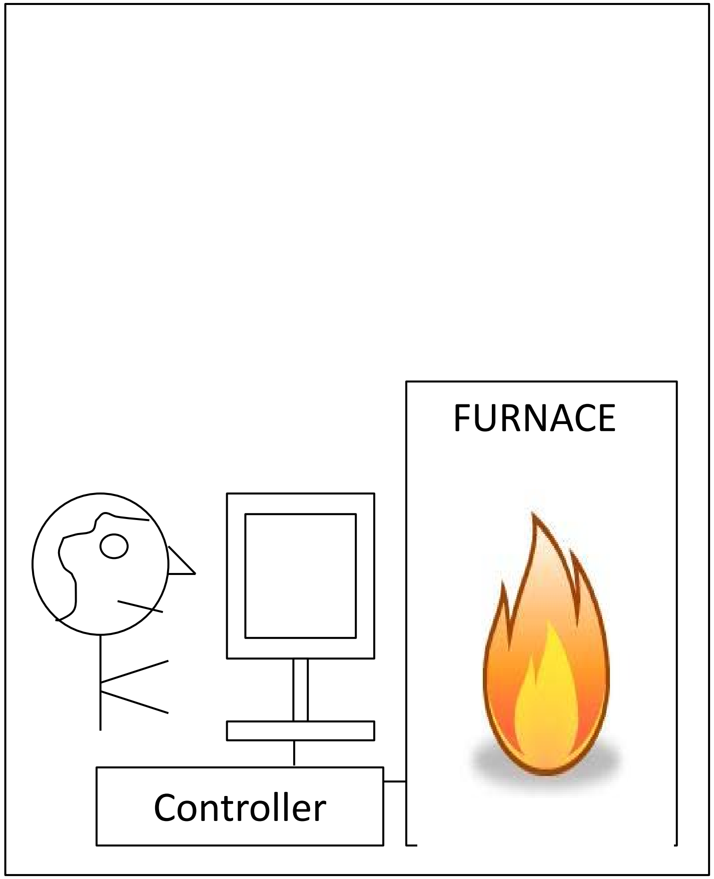
Pre-Stuxnet

Stuxnet Awareness

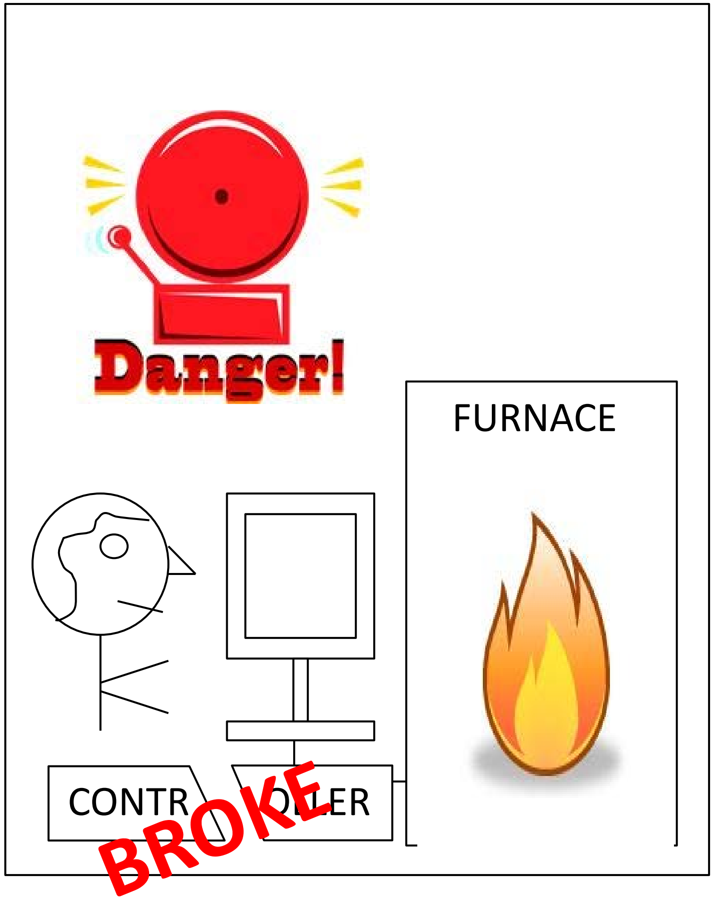
Call to Action

President's Executive Order: Critical Infrastructure Cyber Security Framework

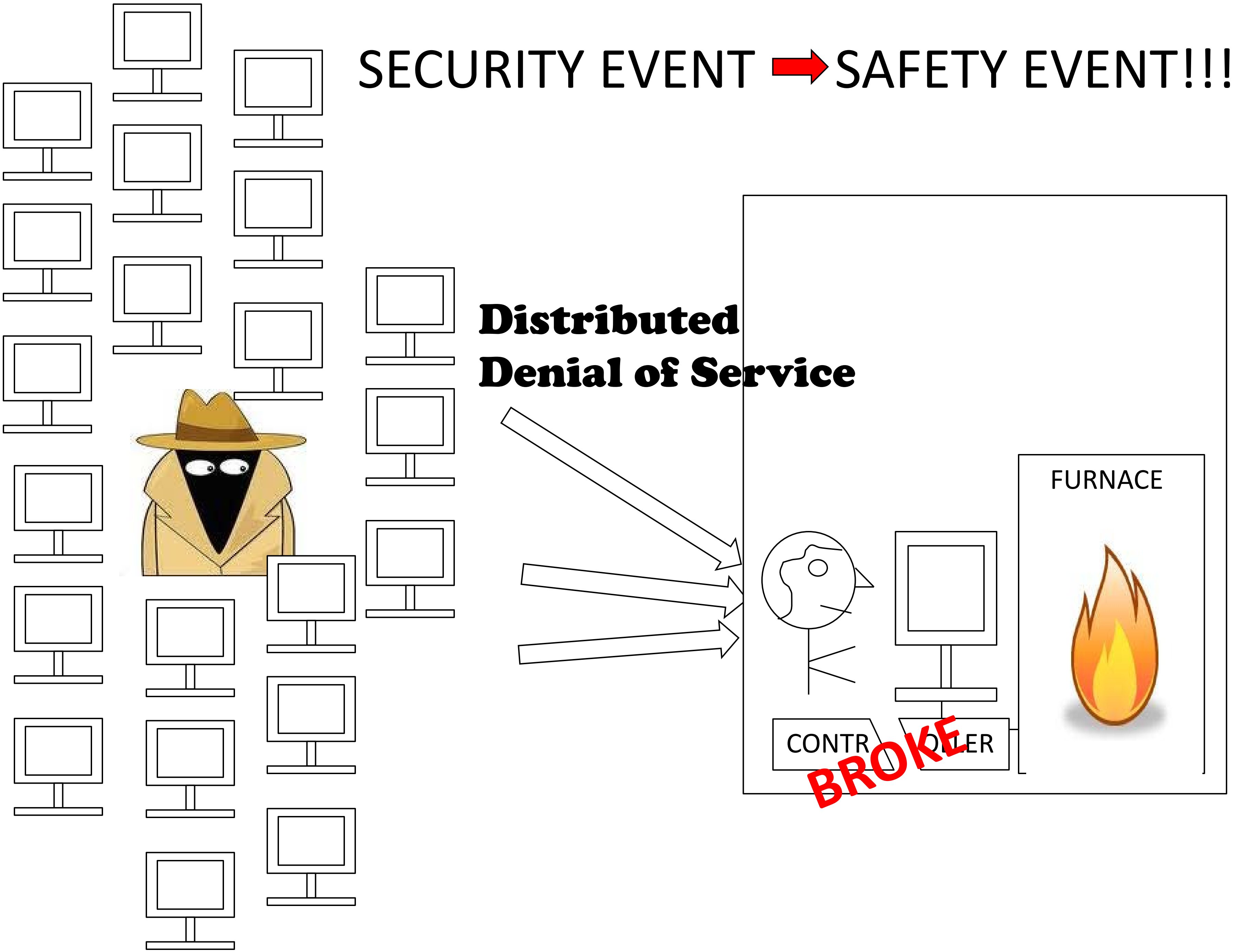



FURNACE
Controller

SAFETY EVENT!!!



SECURITY EVENT ➡ SAFETY EVENT!!!



Distributed Denial of Service

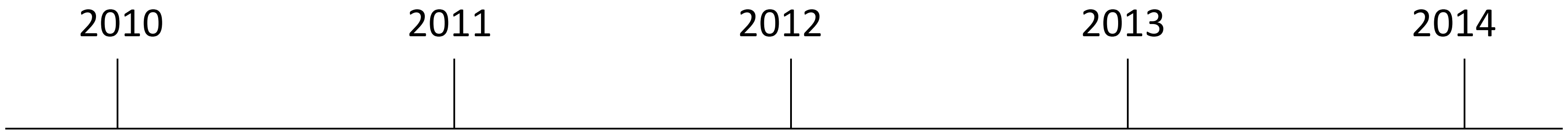
What are the mitigations?

Control Systems treated like IT

~~HCS Production~~

NA-00-LA

- Inventory
- Security State
- Roadmap



2010

2011

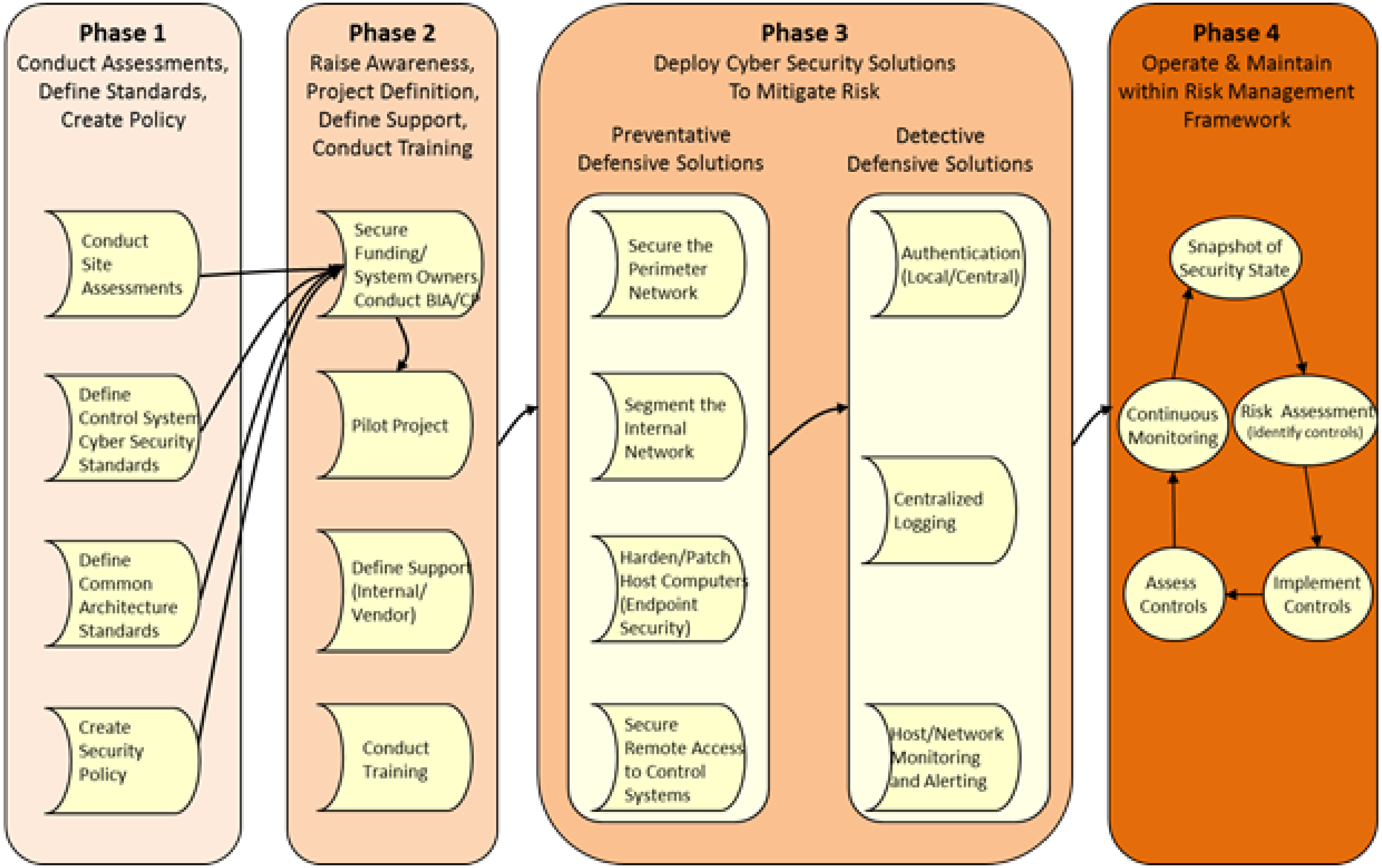
2012

2013

2014

Roadmap to Secure Control Systems

- Strategic, Tactical, Operational



Phase 1
Conduct Assessments,
Define Standards,
Create Policy

Conduct Site Assessments

Define Control System Cyber Security Standards

Define Common Architecture Standards

Create Security Policy

Phase 2
Raise Awareness,
Project Definition,
Define Support,
Conduct Training

Secure Funding/ System Owners, Conduct BIA/CP

Pilot Project

Define Support (Internal/ Vendor)

Conduct Training

Phase 3
Deploy Cyber Security Solutions
To Mitigate Risk

Preventative
Defensive Solutions

Secure the Perimeter Network

Segment the Internal Network

Harden/Patch Host Computers (Endpoint Security)

Secure Remote Access to Control Systems

Detective
Defensive Solutions

Authentication (Local/Central)

Centralized Logging

Host/Network Monitoring and Alerting

Phase 4
Operate & Maintain
within Risk Management
Framework

Snapshot of Security State

Risk Assessment (identify controls)

Implement Controls

Assess Controls

Continuous Monitoring

Control Systems treated like IT

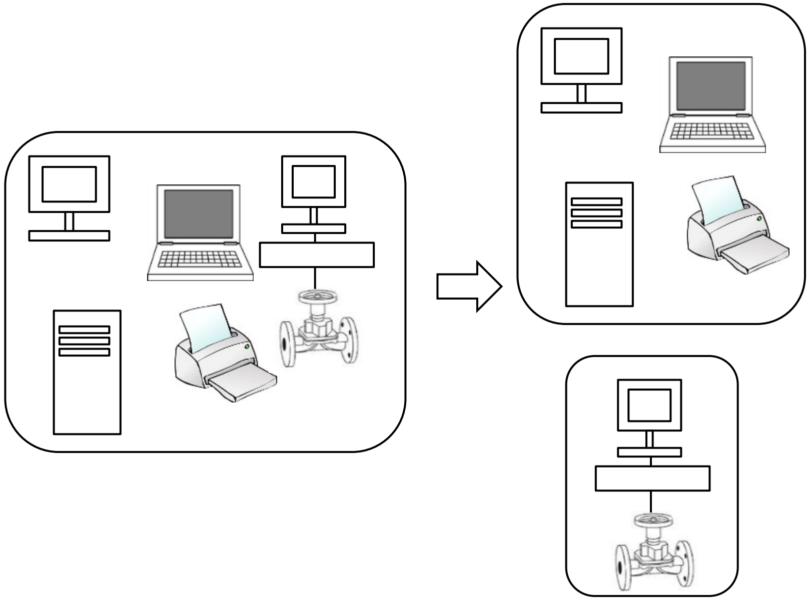
~~HCS Production~~

NA-00-LA

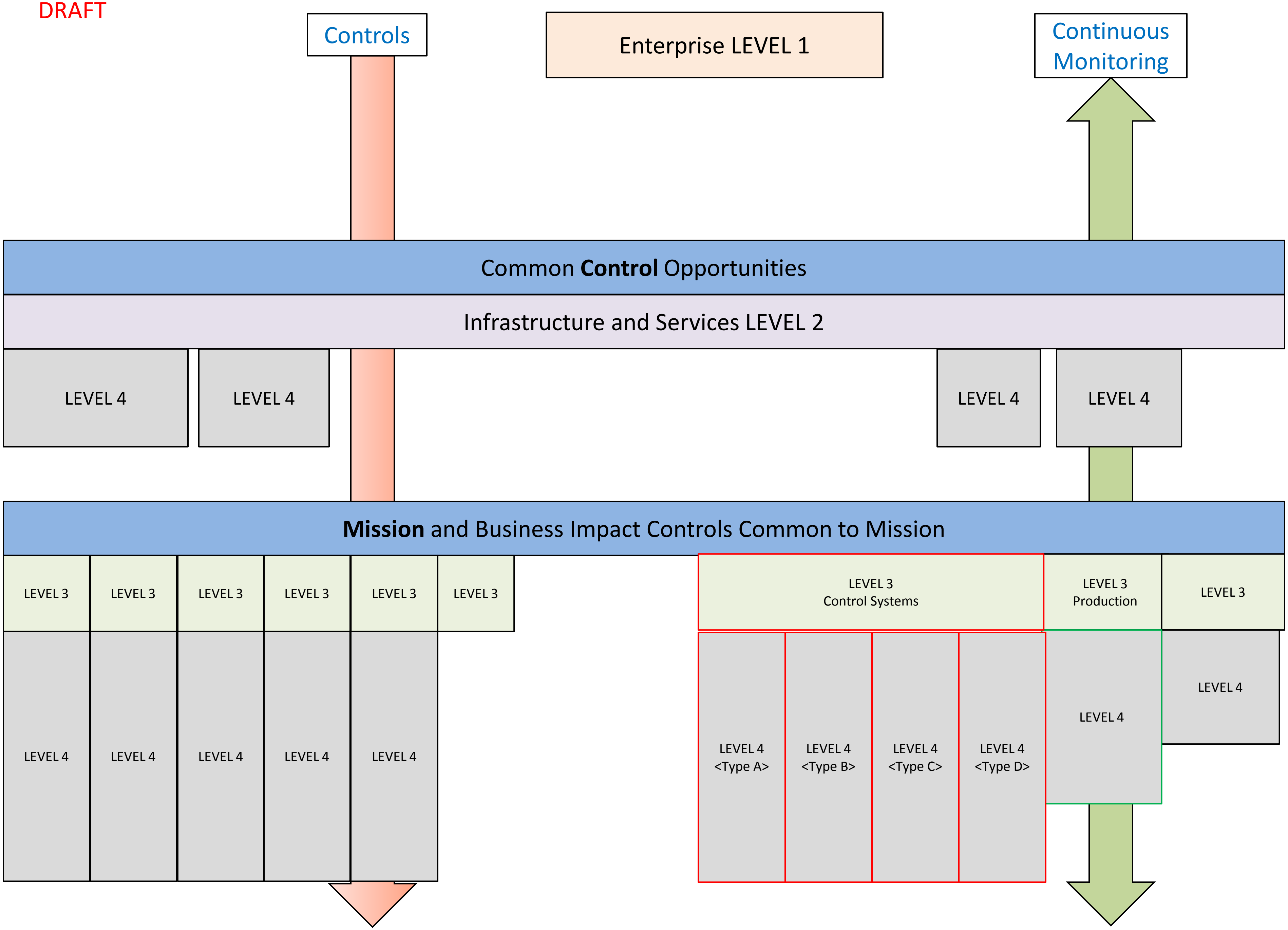
- Inventory
- Security State
- Roadmap

LANL RMF SP

2010 2011 2012 2013 2014



DRAFT



Controls

Enterprise LEVEL 1

Continuous Monitoring

Common **Control** Opportunities

Infrastructure and Services LEVEL 2

LEVEL 4

LEVEL 4

LEVEL 4

LEVEL 4

Mission and Business Impact Controls Common to Mission

LEVEL 3

LEVEL 3

LEVEL 3

LEVEL 3

LEVEL 3

LEVEL 3

LEVEL 3
Control Systems

LEVEL 3
Production

LEVEL 3

LEVEL 4

LEVEL 4

LEVEL 4

LEVEL 4

LEVEL 4

LEVEL 4
<Type A>

LEVEL 4
<Type B>

LEVEL 4
<Type C>

LEVEL 4
<Type D>

LEVEL 4

LEVEL 4

Control Systems treated like IT

~~HCS Production~~

NA-00-LA

- Inventory
- Security State
- Roadmap

LANL RMF SP

June 2014 BIA/CP Critical Facilities

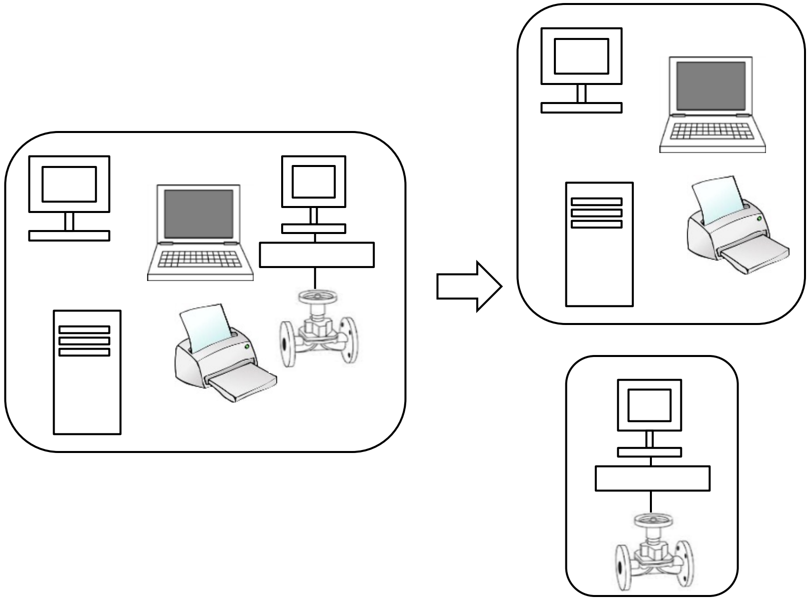
2010

2011

2012

2013

2014

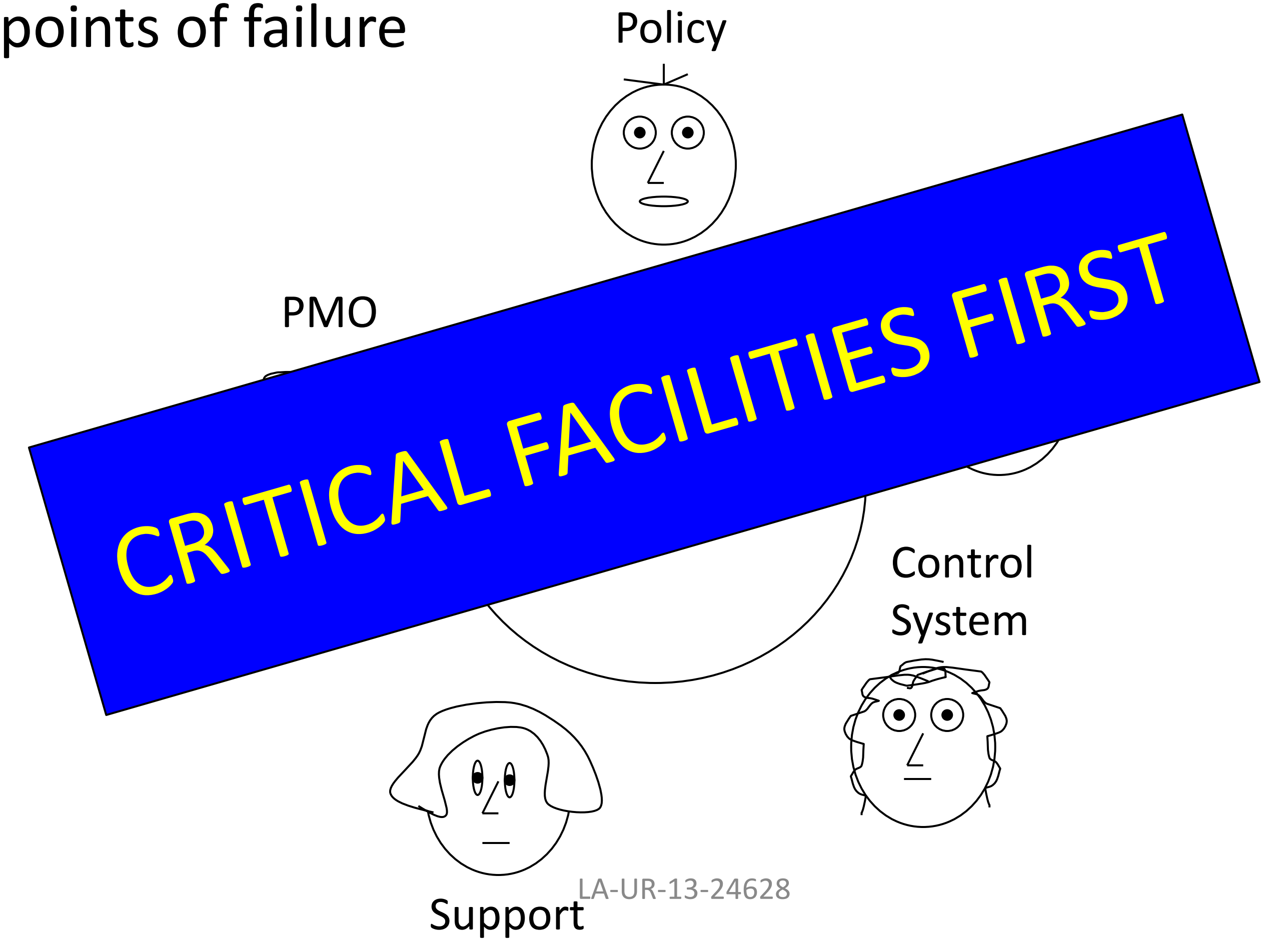


Business Impact Analysis

- Prioritize systems & mitigations
- Dependencies
- POCs (LANL, vendors)
- MAD
- Single points of failure

Contingency Planning

- Guide during a crisis
- Activation, notification, recovery



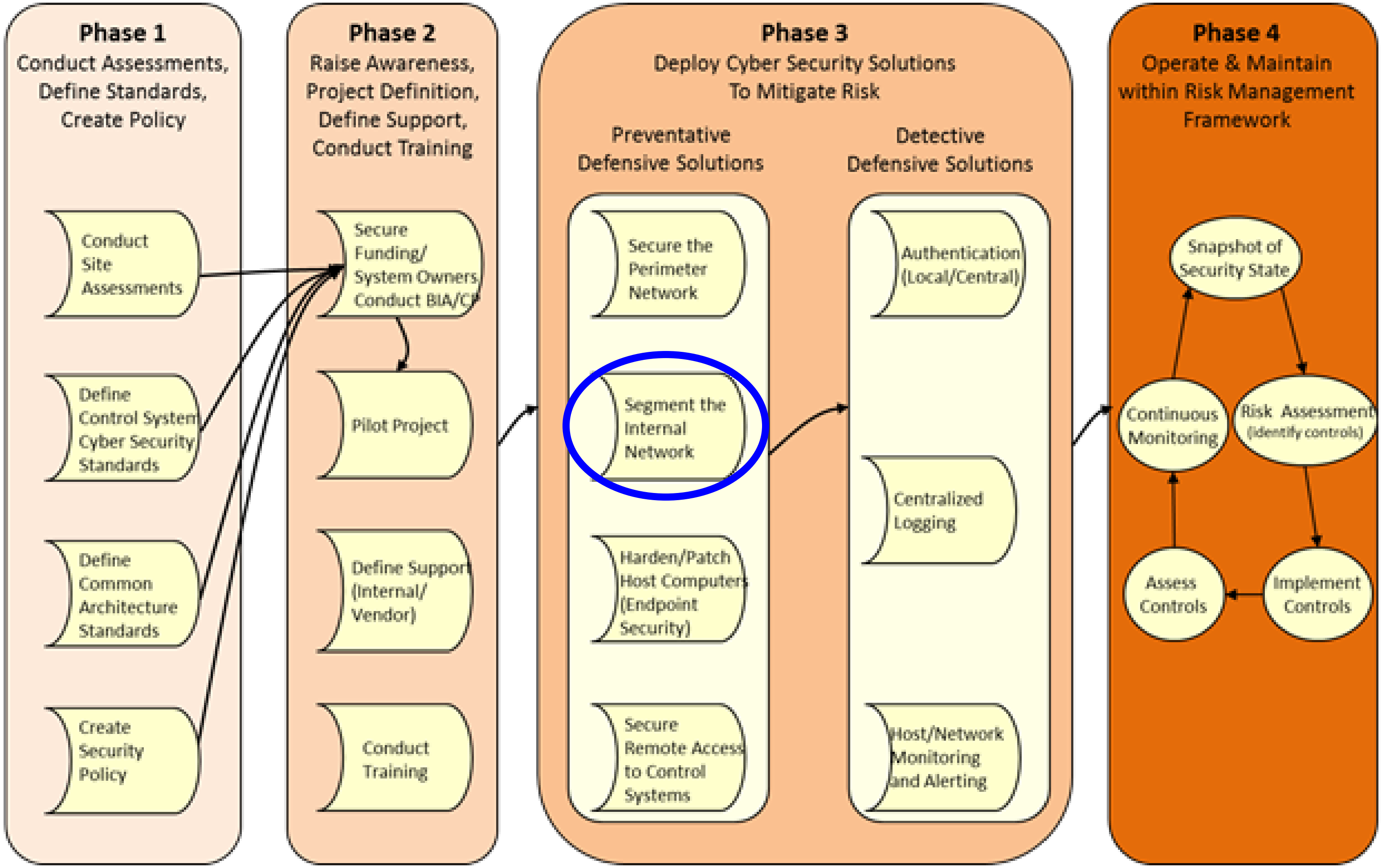
CRITICAL FACILITIES FIRST

NEXT STEPS

The plan to secure Control Systems will happen at the following levels:

- Strategic – high level, long range plan (Figure 2, Phases 1-2)
  - The new Security Plan enclosures for Control Systems will be based on the Risk Management Framework, which will separate out classes with common ownership, characteristic risks and mitigations.
  - Subject Matter Experts (SME) will conduct a Risk Assessment and Business Impact Analysis (BIA) to determine the risks and mitigations unique to their environment.
  - The BIA will focus on first identifying mission critical resources (e.g. hardware, software, network, people, environmental components), their dependencies and then restoration of critical services after an interruption or outage. It will be vetted with group discussions and scenario walkthroughs. This living document will be tracked with Continuous Monitoring (e.g. Validation and Verification, annual security assessments, host security software, table tops).
  - Once HCS Production is re-accredited, remaining Unclassified and Classified Security Plans will follow the same process.
- Tactical – mid-term focus on events that will affect an organization's functional plans (Figure 2, Phases 2-3)
  - Each BIA will be updated on an annual basis, which will revisit risks and mitigations. This may require tasks such as network redesign, installation of new equipment and controls, support model change (e.g. multi-person team with both Control System and IT expertise, Service Level Agreement) and incident tracking (e.g. utility and network outages, flaws in processes [e.g. change management) or training).
- Operational – near-term focus on events that affect an organization's day-to-day operations to accomplish the mission (Figure 2, Phase 4)
  - Daily operation and maintenance are performed and continuously evaluated against existing and potential controls to enhance the system's security posture.
  - New security education classes will better enable integration between IT and Operational Technology (OT) personnel in terms of roles, responsibilities and secure behaviors.

Roadmap to Secure Control Systems



Phase 1
Conduct Assessments, Define Standards, Create Policy
Conduct Site Assessments
Define Control System Cyber Security Standards
Define Common Architecture Standards
Create Security Policy
Phase 2
Raise Awareness, Project Definition, Define Support, Conduct Training
Secure Funding/ System Owners Conduct BIA/CP
Pilot Project
Define Support (Internal/ Vendor)
Conduct Training
Phase 3
Deploy Cyber Security Solutions To Mitigate Risk
Preventative Defensive Solutions
Secure the Perimeter Network
Segment the Internal Network
Harden/Patch Host Computers (Endpoint Security)
Secure Remote Access to Control Systems
Detective Defensive Solutions
Authentication (Local/Central)
Centralized Logging
Host/Network Monitoring and Alerting
Phase 4
Operate & Maintain within Risk Management Framework
Snapshot of Security State
Risk Assessment (identify controls)
Implement Controls
Assess Controls
Continuous Monitoring

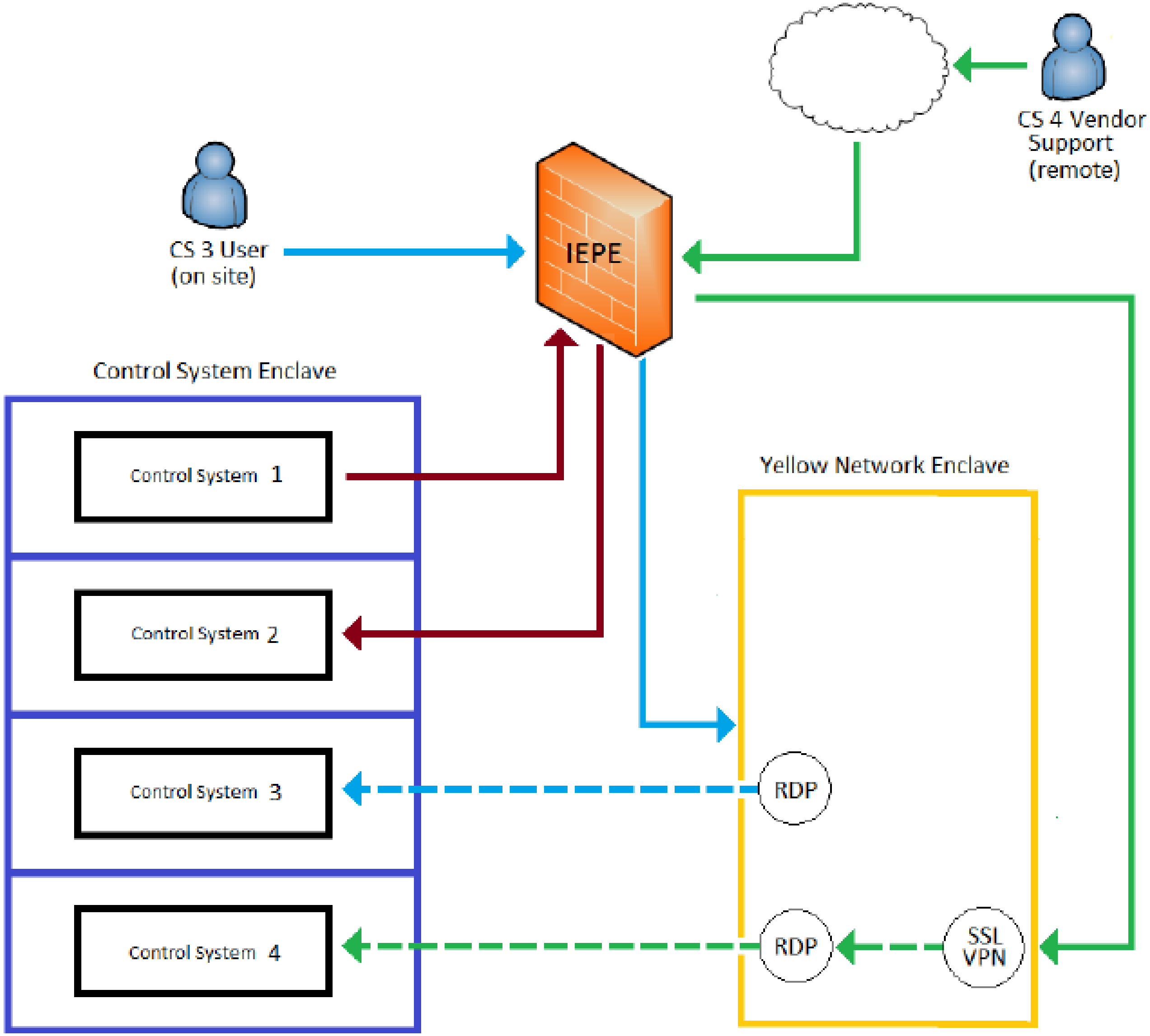
Why a Control Systems Enclave?

- Protect against lateral movement
- Some systems are sensitive to scanning/patching
- Centralized controlled access to system

Proposed Control Systems Enclave

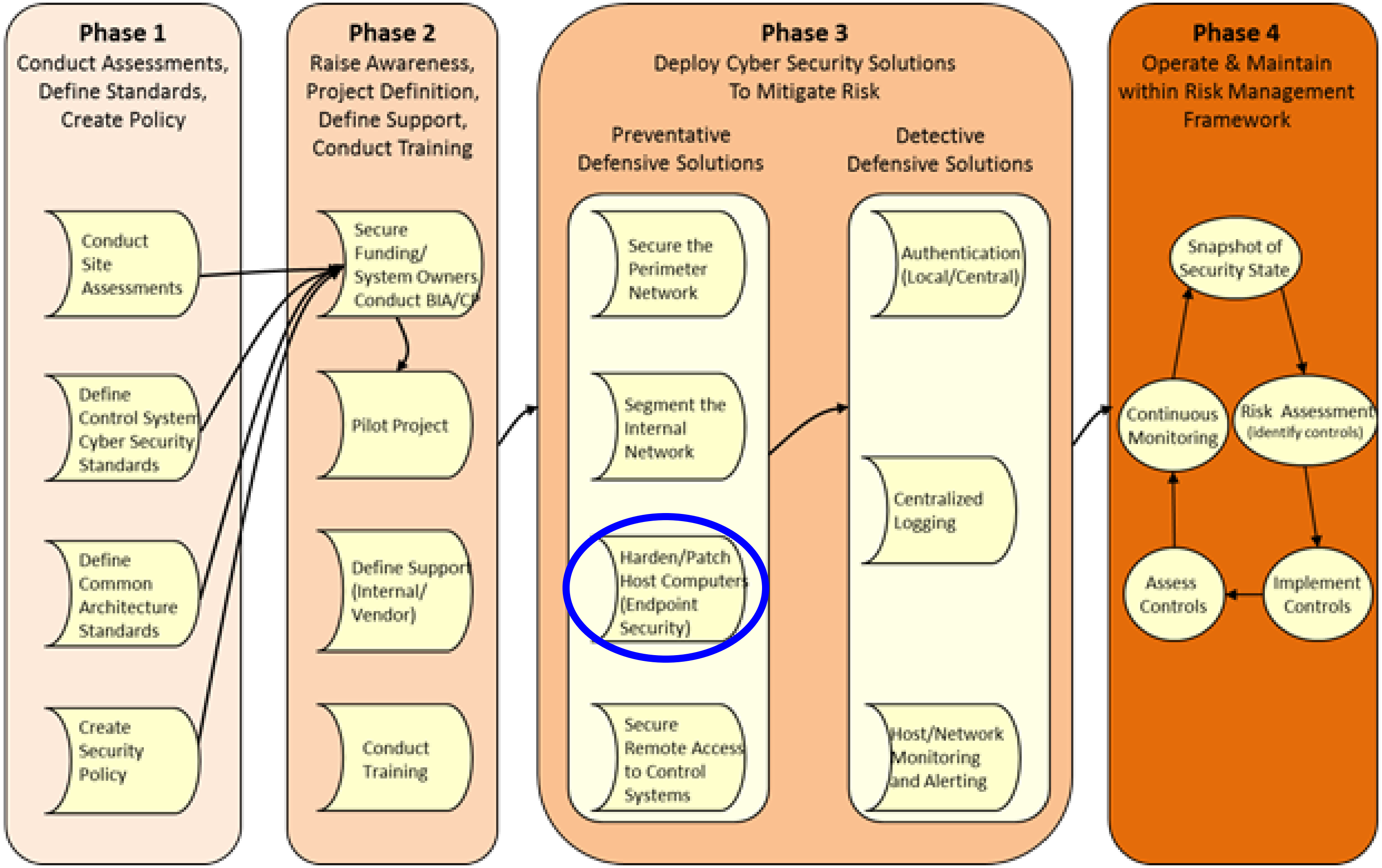
- One Enclave with high fences
- A “system” will be on one subnet
  - Subnet can span campus
- IP address will need to be changed
  - Unless the system is completely isolated

Control Systems (CS) Enclave



Network Segmentation, T. Bowman, D. Degrazio, June 2013 Control Systems Workshop

Roadmap to Secure Control Systems



Phase 1
Conduct Assessments,
Define Standards,
Create Policy

Conduct Site Assessments

Define Control System Cyber Security Standards

Define Common Architecture Standards

Create Security Policy

Phase 2
Raise Awareness,
Project Definition,
Define Support,
Conduct Training

Secure Funding/ System Owners Conduct BIA/CP

Pilot Project

Define Support (Internal/ Vendor)

Conduct Training

Phase 3
Deploy Cyber Security Solutions
To Mitigate Risk

Preventative
Defensive Solutions

Secure the Perimeter Network

Segment the Internal Network

Harden/Patch Host Computers (Endpoint Security)

Secure Remote Access to Control Systems

Detective
Defensive Solutions

Authentication (Local/Central)

Centralized Logging

Host/Network Monitoring and Alerting

Phase 4
Operate & Maintain
within Risk Management
Framework

Snapshot of Security State

Risk Assessment (identify controls)

Implement Controls

Assess Controls

Continuous Monitoring

IT Security Suite

Logging
Snare

Scanning
CPAT

Inventory
SCCM/CS OU

Config Mgmt
SCCM

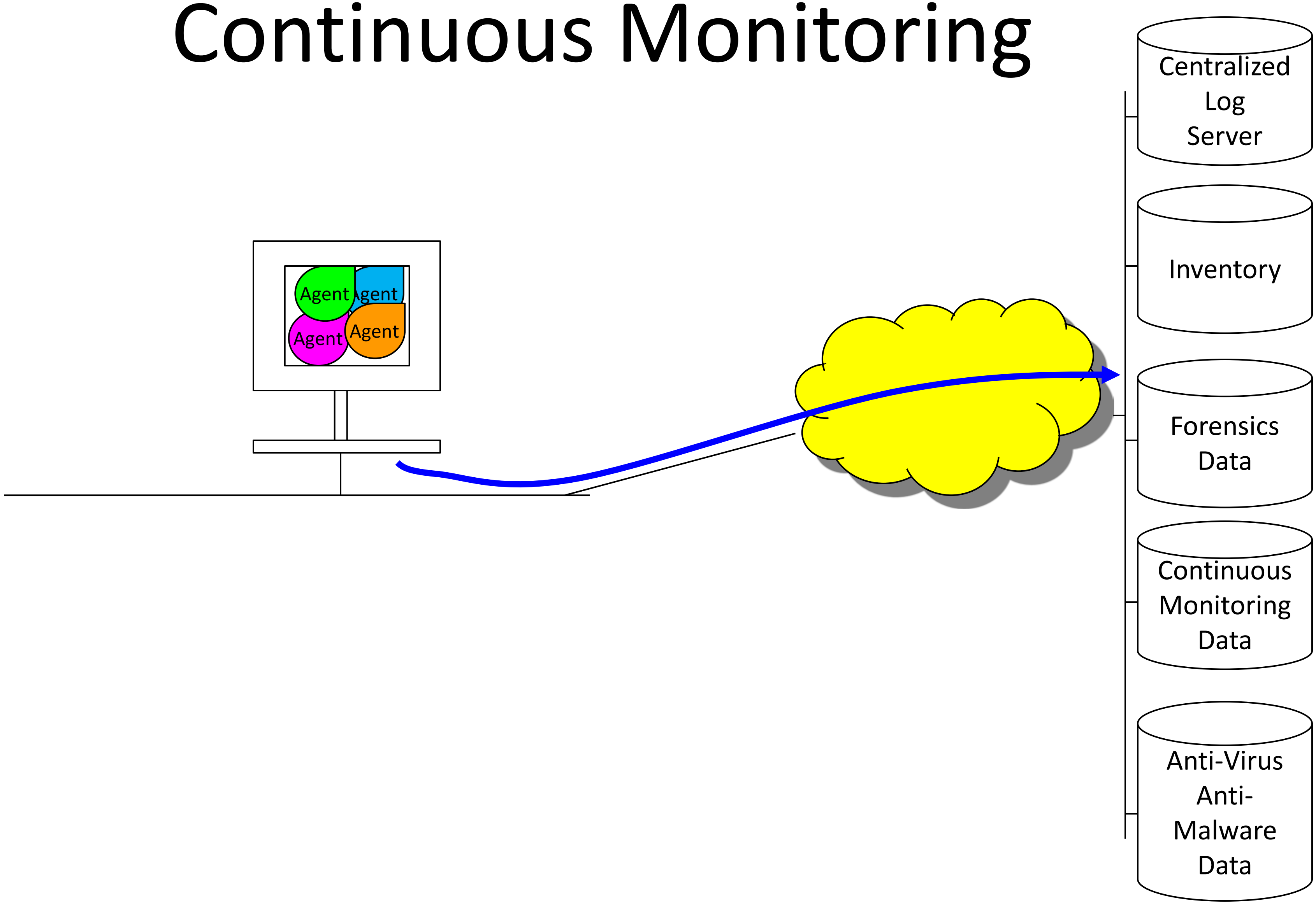
System Hardening
STOx

Anti-virus/ Anti-malware
SEP

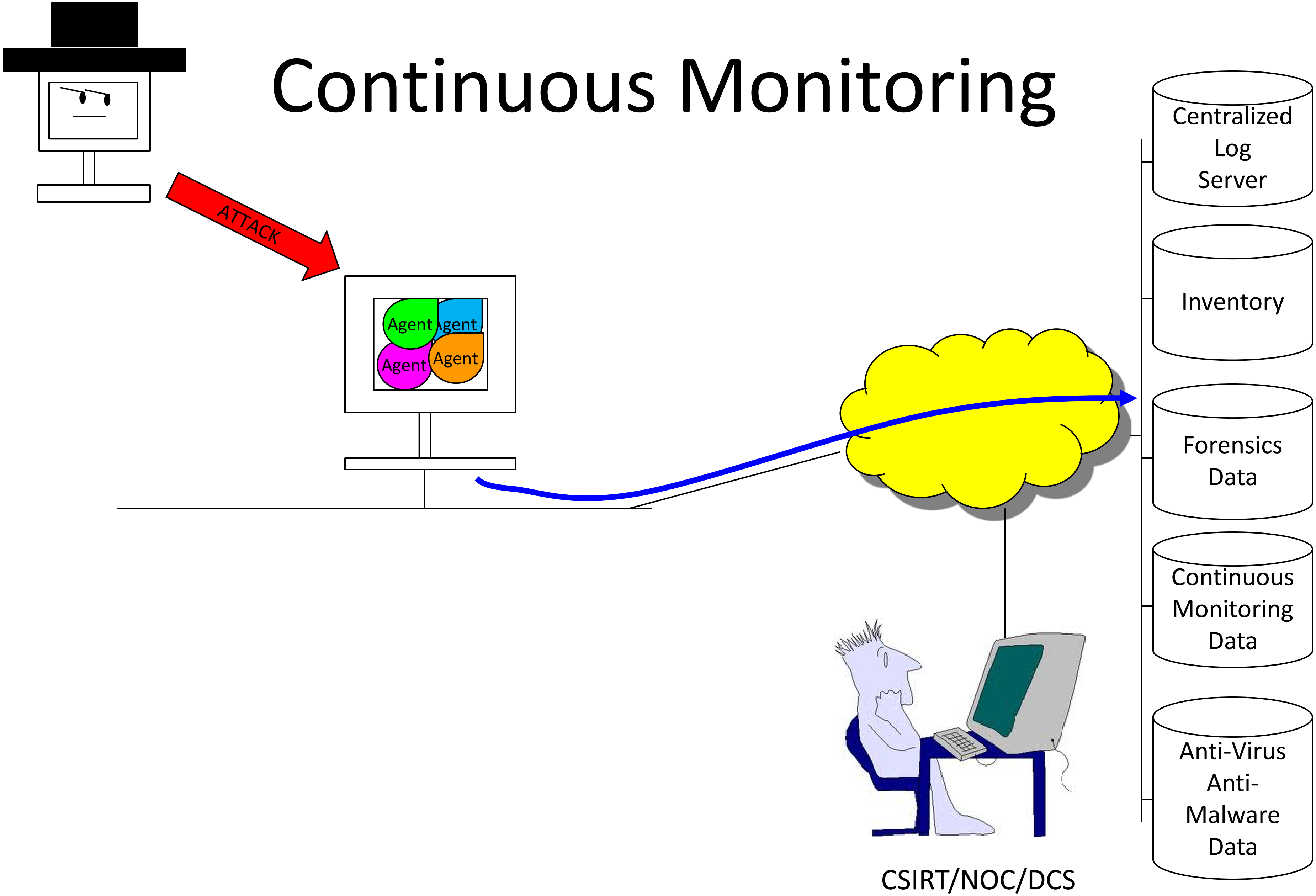
Forensics
Encase/Mir

Host Vuln/Config Assessment
RAS

Continuous Monitoring

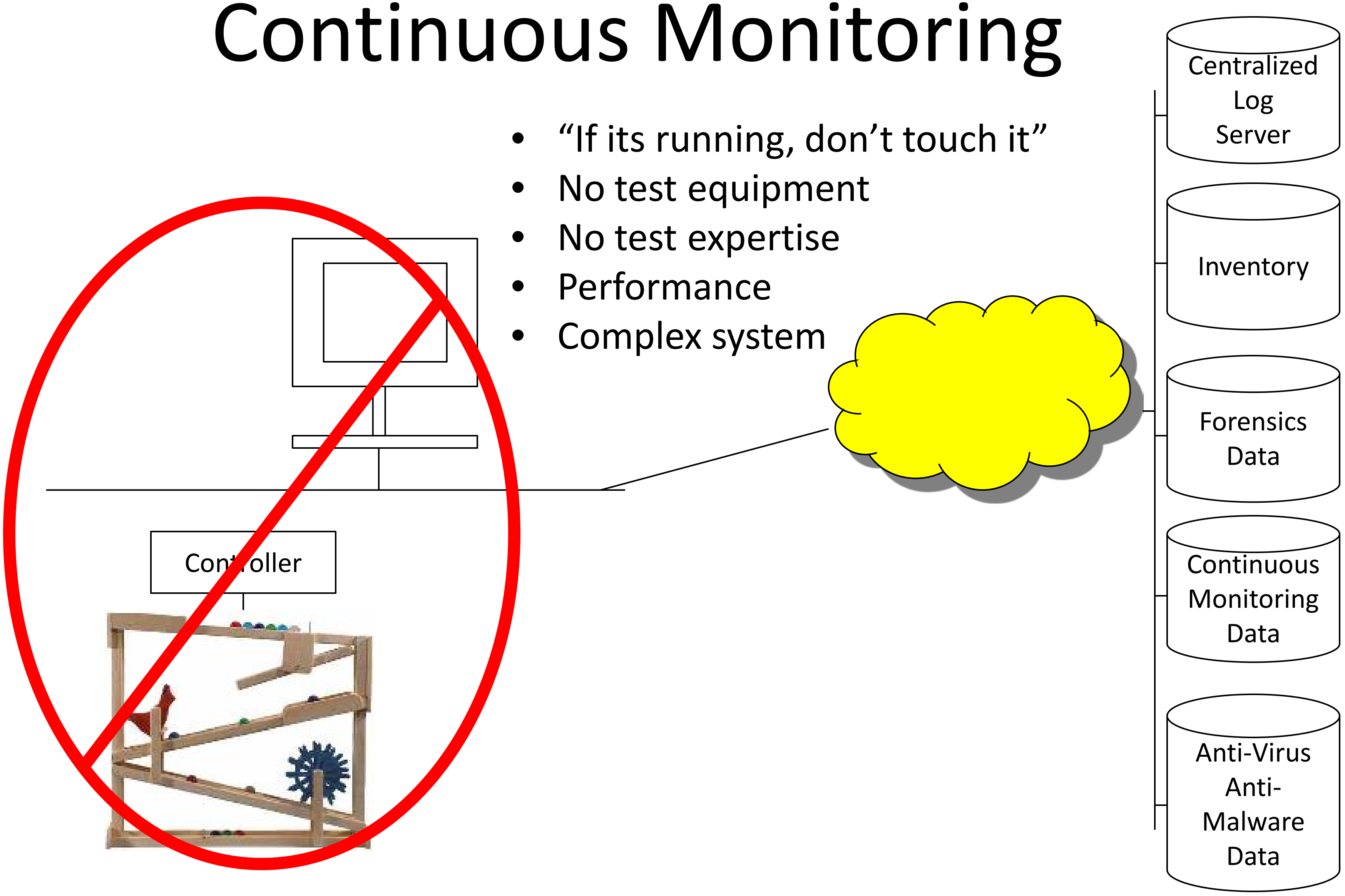


Continuous Monitoring

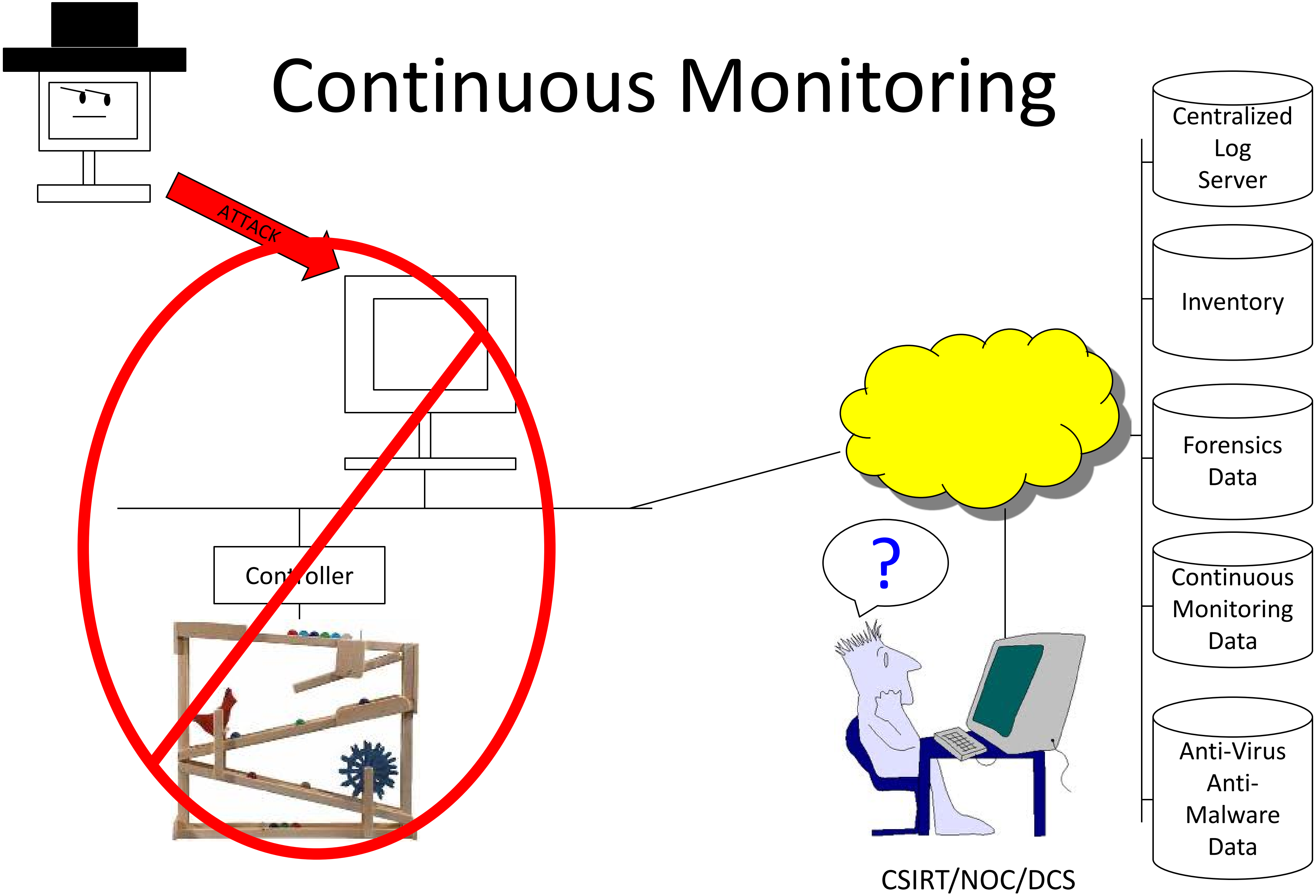


Continuous Monitoring

- “If its running, don’t touch it”
- No test equipment
- No test expertise
- Performance
- Complex system



Continuous Monitoring



ATTACK

Controller

?

CSIRT/NOC/DCS

Centralized Log Server

Inventory

Forensics Data

Continuous Monitoring Data

Anti-Virus Anti-Malware Data

Baby Steps

Host Vuln/Config Assessment
RAS

Forensics
Encase/Mir

Anti-virus/ Anti-malware
SEP

System Hardening
STOx

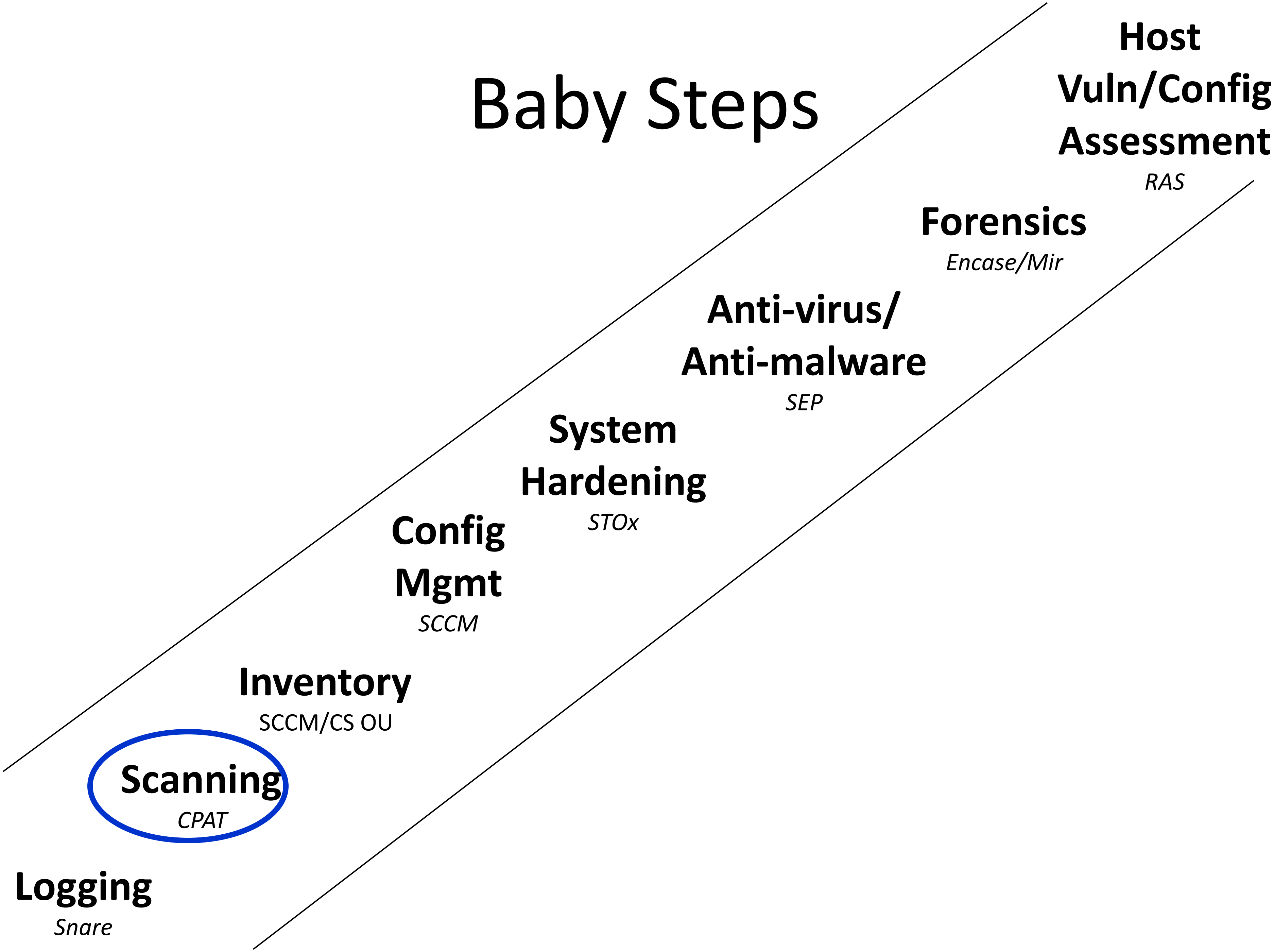
Config Mgmt
SCCM

Inventory
SCCM/CS OU

Scanning
CPAT

Logging
Snare

Baby Steps



Logging
Snare

Scanning
CPAT

Inventory
SCCM/CS OU

Config Mgmt
SCCM

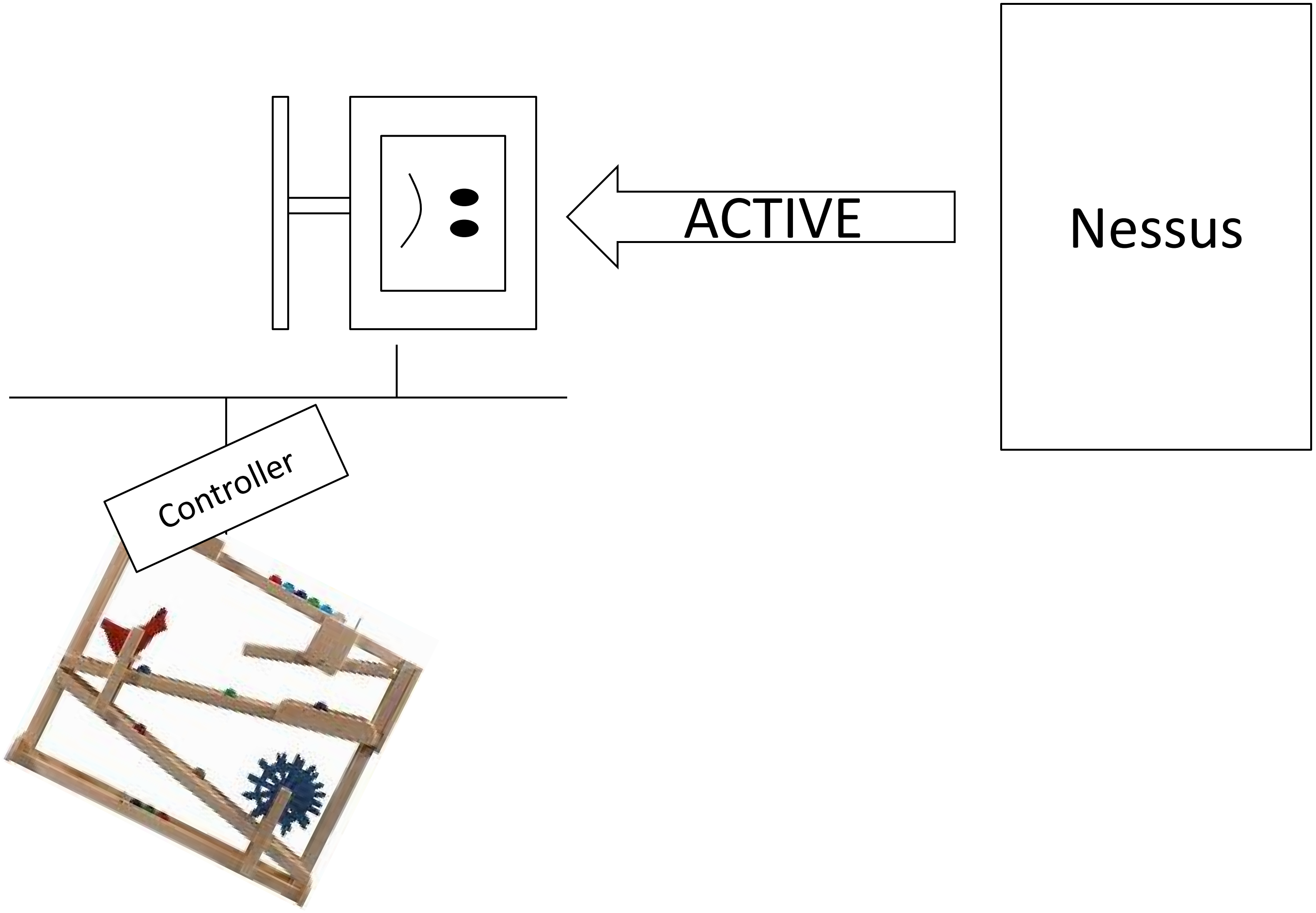
System Hardening
STOx

Anti-virus/ Anti-malware
SEP

Forensics
Encase/Mir

Host Vuln/Config Assessment
RAS

Scanning

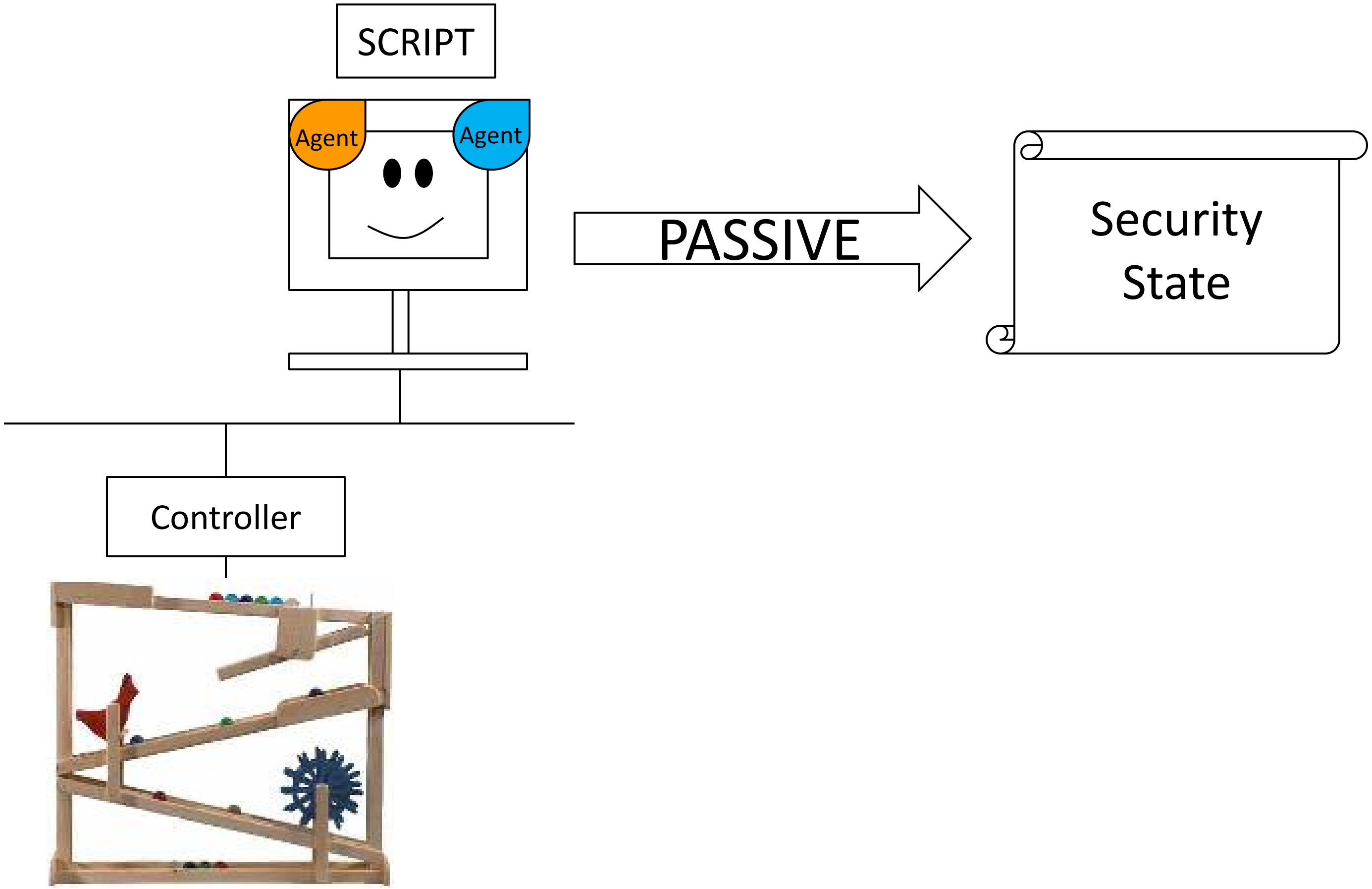


ACTIVE

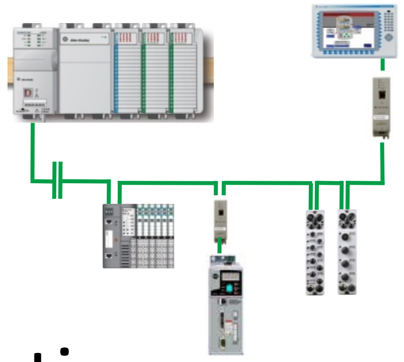
Nessus

Controller

Scanning



New Technology Lab
TA46-42-226

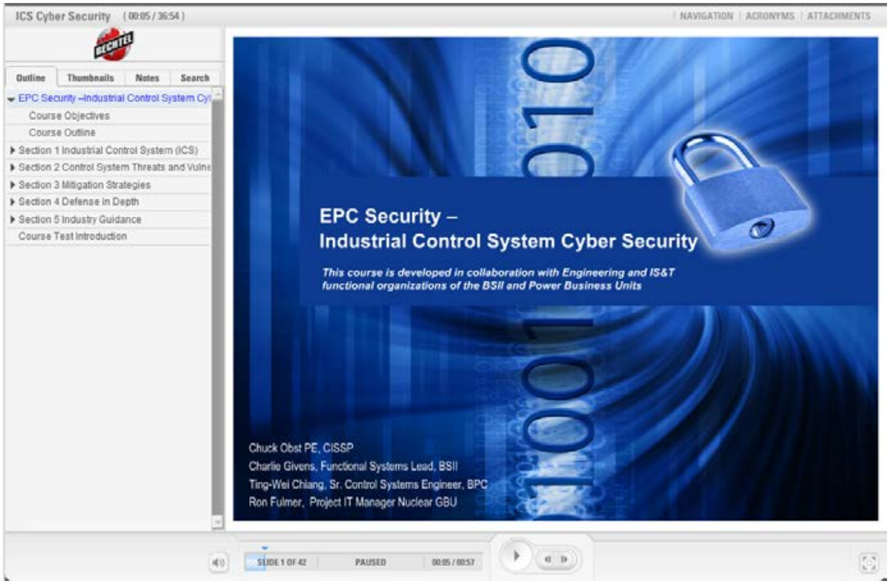


- Uses: testing, training, vendor interactions
- Standard equipment + community donations
- Sign “Rules of Use”
- Make appointments (M-F, 8-5) starting Aug. 12
  - techlab@lanl.gov, 665-6820

Training - Future

- UTRAIN – IT/Control System Security Awareness (1.5 hour near Tech Lab)

- Bechtel online training



ICS Cyber Security (00:05 / 36:54)

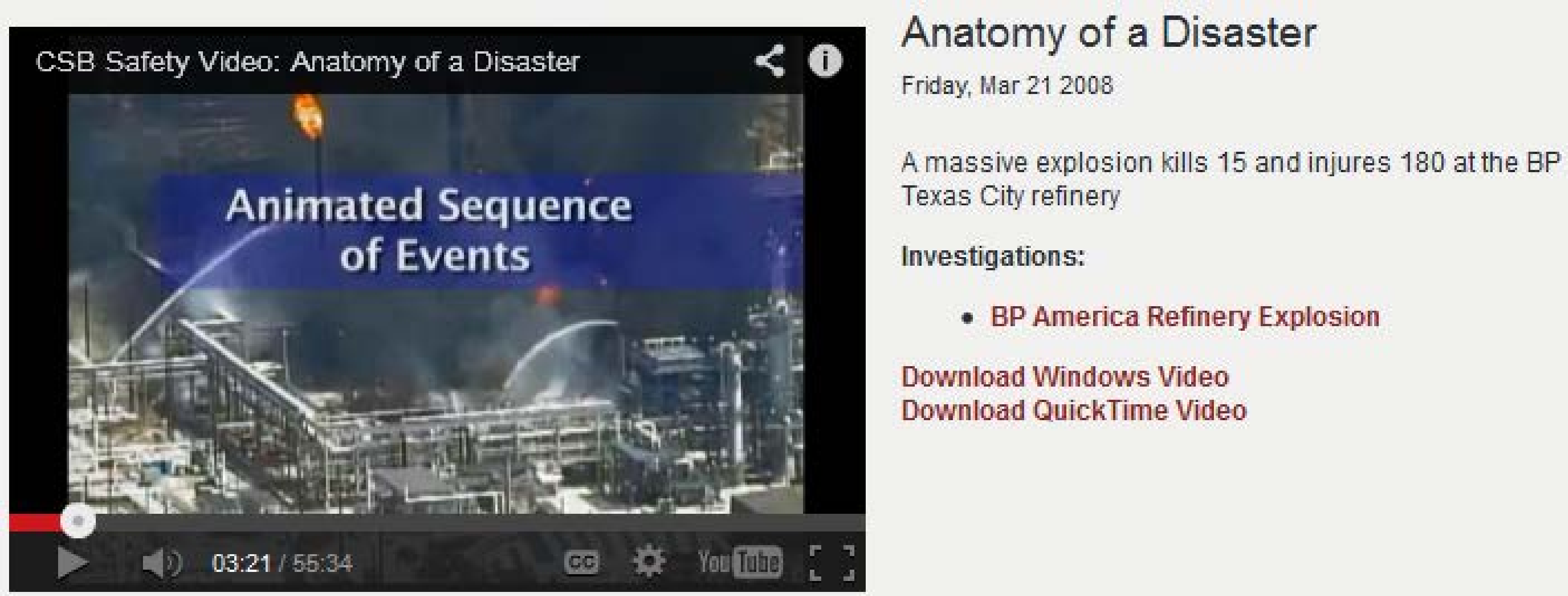
EPC Security –
Industrial Control System Cyber Security

This course is developed in collaboration with Engineering and IS&T functional organizations of the BSII and Power Business Units

Chuck Obst PE, CISSP
Charlie Givens, Functional Systems Lead, BSII
Ting-Wei Chiang, Sr. Control Systems Engineer, BPC
Ron Fulmer, Project IT Manager Nuclear GBU

NAVIGATION | ACRONYMS | ATTACHMENTS
BECHTEL
Outline
Thumbnails
Notes
Search
EPC Security –Industrial Control System Cy
Course Objectives
Course Outline
Section 1 Industrial Control System (ICS)
Section 2 Control System Threats and Vulne
Section 3 Mitigation Strategies
Section 4 Defense in Depth
Section 5 Industry Guidance
Course Test Introduction
SLIDE 1 OF 42
PAUSED
00:05 / 00:57

Anatomy of a Disaster


CSB Safety Video: Anatomy of a Disaster
Animated Sequence of Events
03:21 / 55:34

Anatomy of a Disaster

Friday, Mar 21 2008

A massive explosion kills 15 and injures 180 at the BP Texas City refinery

Investigations:

- BP America Refinery Explosion

Download Windows Video
Download QuickTime Video

http://www.csb.gov/videos/anatomy-of-a-disaster/, animation starts at 3:21

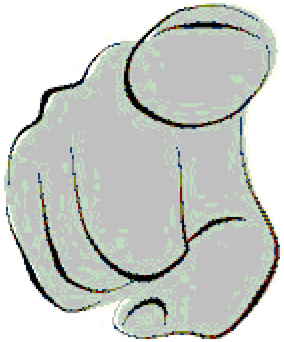
Summary

- IT ≠ Control Systems

- Communities
  - Awareness: LANL, Technology Lab, DOE

- Roadmap
  - Strategic, Tactical, Operations

- BIA/CP – Critical facilities first



Questions

http://2kindproject.blogspot.com/2012/02/latest-and-greatest.html

Contact

- Sandy Frost
- slf2@lanl.gov
- 665-6820