

Setting the Standard for Automation™



Inherently Safer Technology for Cyber Security

ISA Safety & Security Division
Symposium

14 April 2011

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

- Introduction
- Inherently Safer Technology definition (IST)
- Industrial Control System security relevance
- Recommendations and discussion

- Bryan S. Owen PE
 - Cyber security manager
 - Engineering manager Oceania region
 - Field service application engineer
 - 15yr chemical, pulp and paper ICS engineer
 - BS ChE Oregon State, Microsoft certified



Energy per Gram	Calories (Watt-hr)	Compared to TNT
bullet @ 1000 ft per sec	0.01	0.015
auto battery	0.03	0.05
TNT	0.65	1
high explosive (PETN)	1	1.6
chocolate chip cookies	5	8
coal	6	10
alcohol (ethanol)	6	10
gasoline	10	15
natural gas	13	20
hydrogen	26	40
uranium-235	20 million	30 million

Richard A. Muller: “Physics for future Presidents”
<http://muller.lbl.gov/teaching/Physics10/PffP.html>

- **Final Report: Definition for Inherently Safer Technology in Production, Transportation, Storage, and Use (July 2010)**
- **Prepared by: Center for Chemical Process Safety (AIChE)**



**Homeland
Security**

Science and Technology



- A philosophy
 - *applies to design and operation life cycle*
- Iterative process considering options for:
 - *eliminating a hazard*
 - *reducing a hazard*
 - *substituting a less hazardous material*
 - *using less hazardous process conditions*
 - *reducing the potential or consequences of human error, equipment failure, or intentional harm.*

- Inherently safer, inherently more secure...
relative to a different technology



Inherently Safer, more Secure

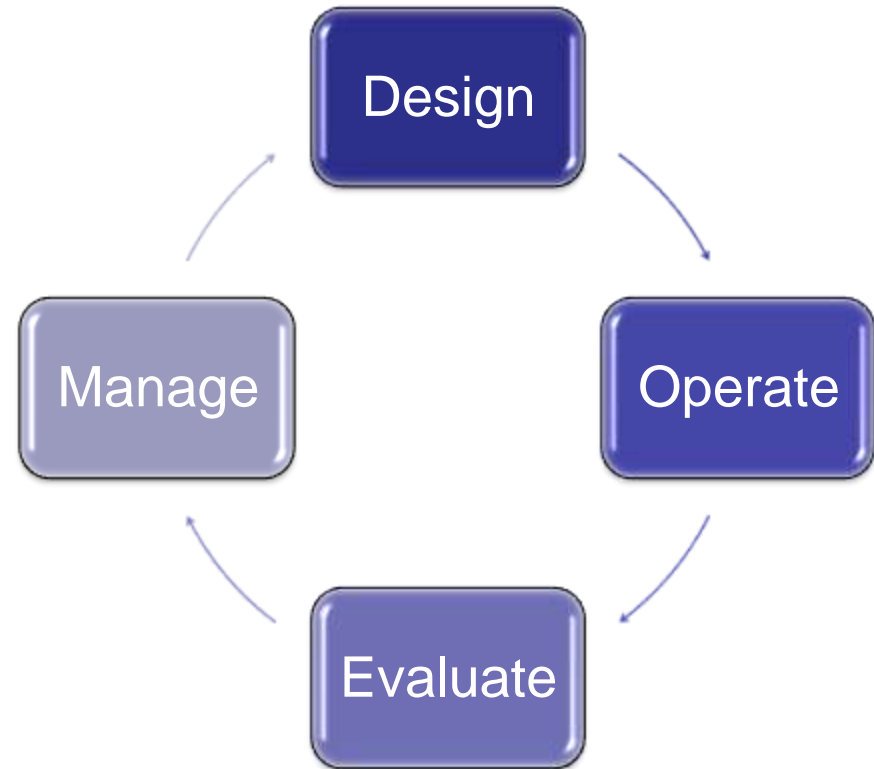


- With respect to some hazards
 - *potentially less safe with respect to other hazards*
- May not be safe enough
 - *to meet societal expectations*



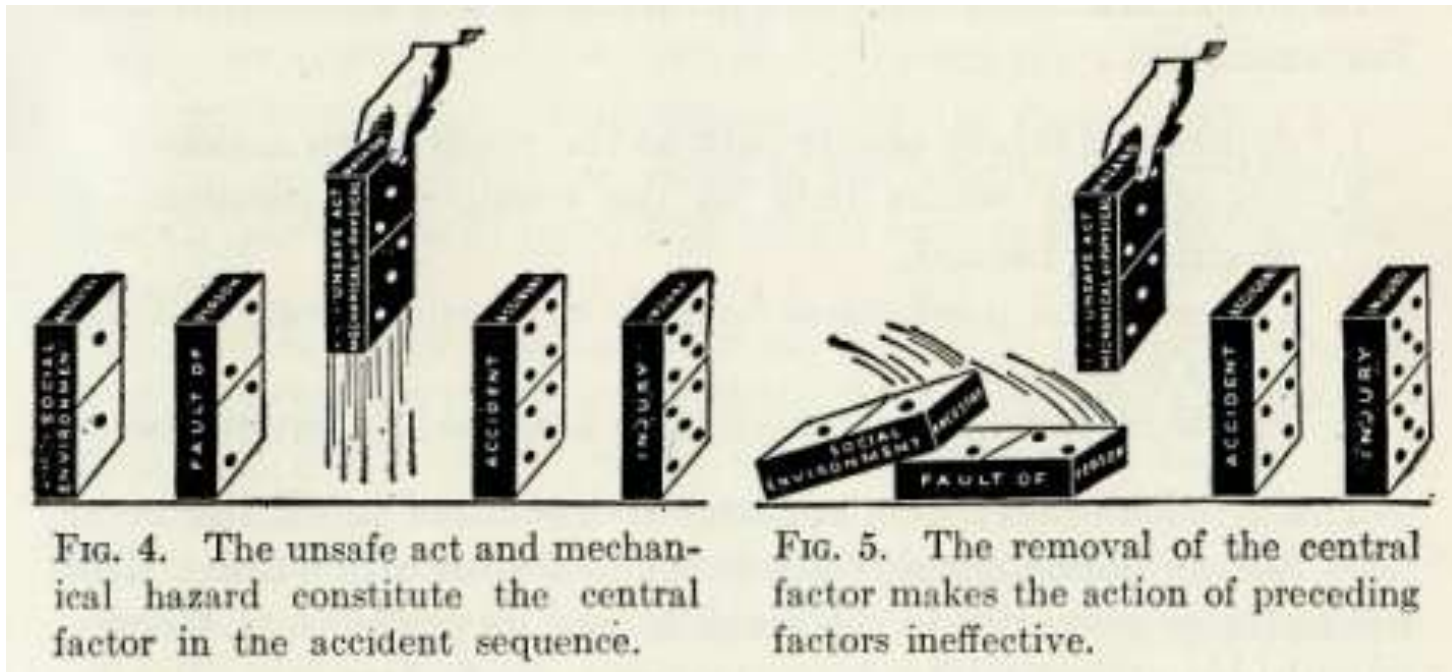
Considerations:

- *Entire life cycle*
- *All hazards and risks*
- *Transfer risk or impact*
- *Economic feasibility*



Completely eliminates a particular hazard

Other hazards may increase, decrease, or remain unaffected



H.W. Heinrich, "Industrial Accident Prevention", 3rd edition, 1950

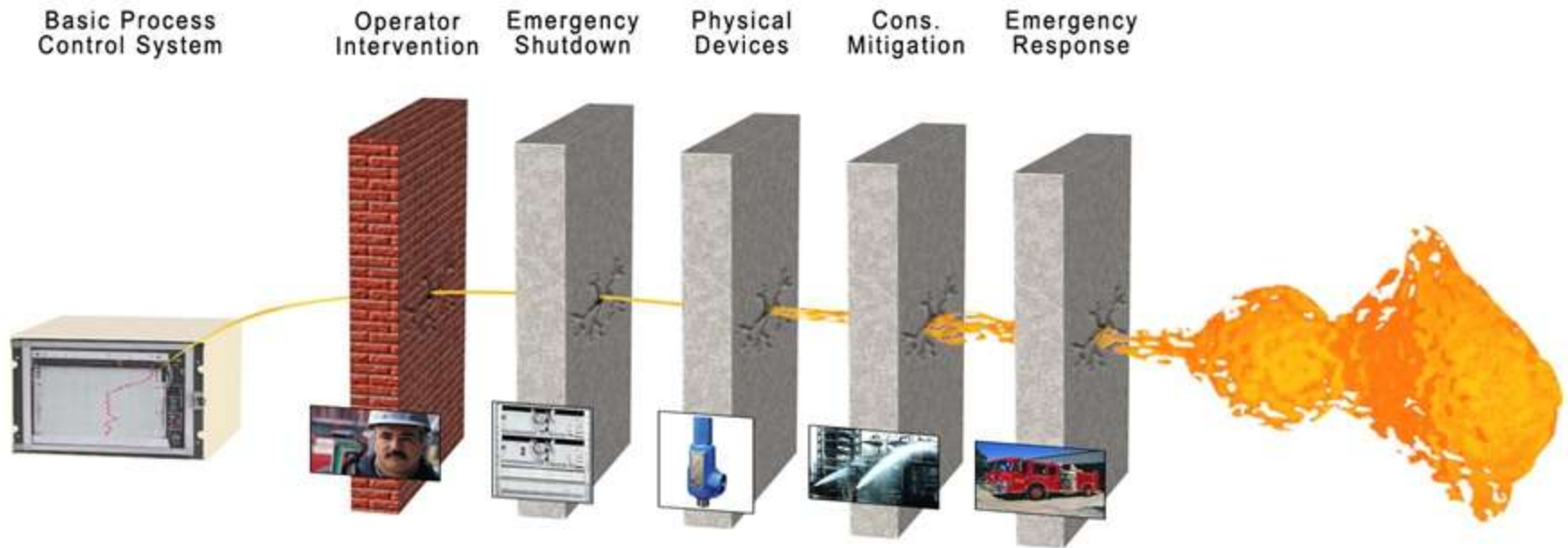
2nd Order IST Change

- Reduces the magnitude of a hazard
 - *likelihood or severity*
- By means of equipment and process
 - *not add-on safety devices*



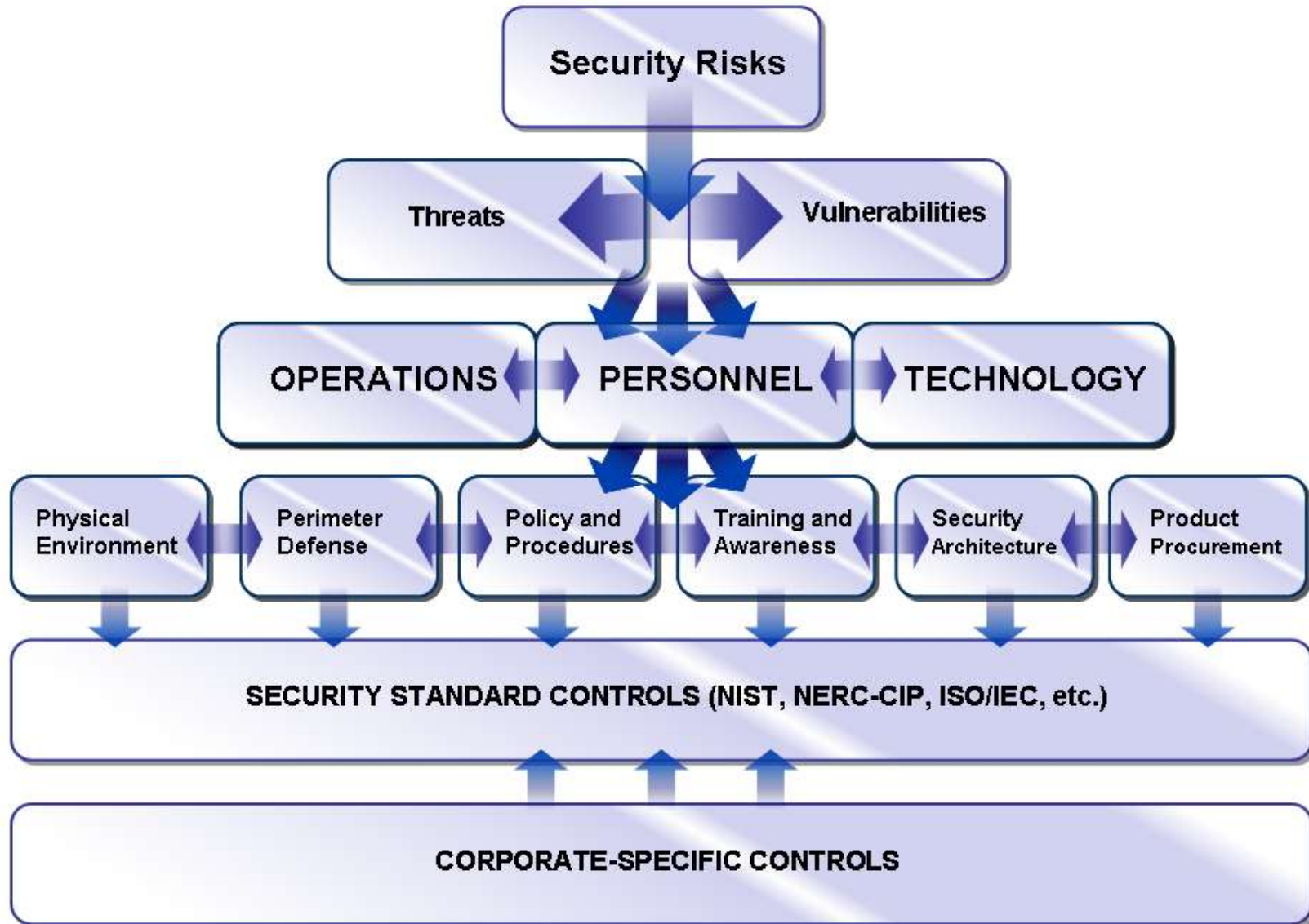
Add-on Layers of Protection

- Layers of Protection are always required
 - *Part of total risk management program*
 - *Made more robust through IST principles*



Source: ISA Safety Symposium 2009

Cyber Security Defense-in-Depth



Inherently Safer	Inherently More Secure
Eliminates a hazard	Eliminates a method of interaction
Reduces a hazard	Reduces interaction
Substitutes a less hazardous material	Substitutes a more secure software component
Uses less hazardous process conditions	Uses least privilege application
Reduces the potential or consequence of human error, failures, or intentional harm	Secure by default implementation, ICS validates input from all potential sources.

Security Controls as IST Changes

IST Iterative Changes

- 1st Order: 'eliminate'
Completely eliminates a particular hazard
- 2nd Order: 'reduce'
Reduce likelihood or severity of a hazard by equipment design, operation or process

Cyber Security Controls¹

- Class A: 'prevent'
Directly influence visibility, access, or trust interactions
- Class B: 'protect'
Protection for assets once a threat is present

¹ Source: Open Source Security Testing Methodology Manual (OSSTMM)

Security Controls?



Sadly, not a control loop.

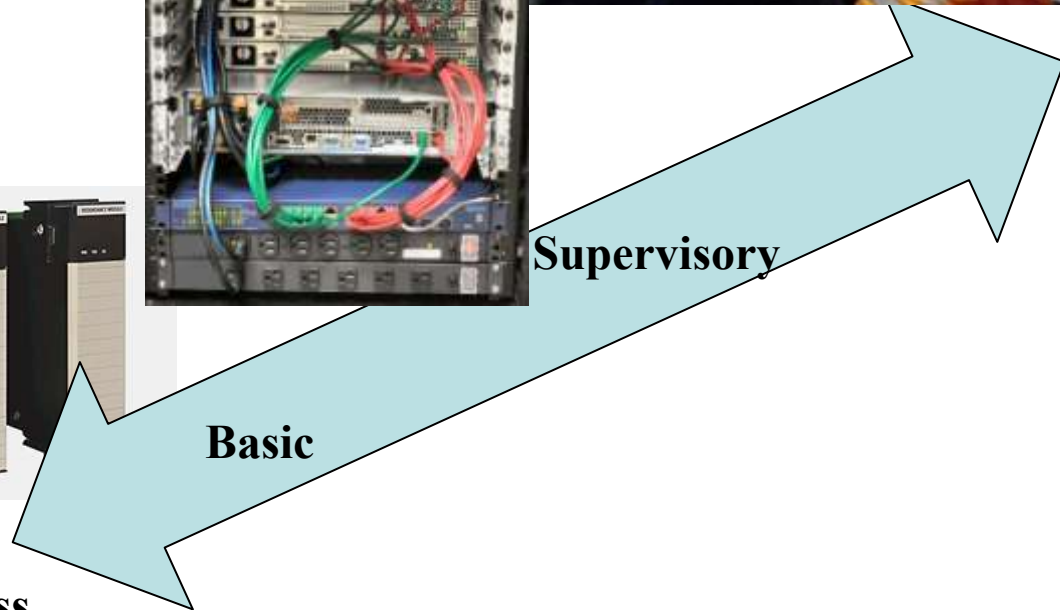
Continuity Control

Prevent loss of interaction

- Inline spares
- Redundant controllers
- Alternate paths
- Visualization



Process



Operations

- Continuity assures access to vulnerability
 - What vulnerabilities are known and how do you know?
- Patching is a 1st order change
 - How often can you patch?
- Patch may be unavailable
 - Process or technology can be too ‘fragile’ to risk change

ISA 99 WG6 Patch Management Practices

1. Is 'anonymous' access effectively prevented?
2. Is 'administrator' reasonably traceable to an individual?

Hacking Breach by Type

Default or Shared Credentials

SQL Injection

Improper ACLs

Stolen Credentials

Authentication Bypass

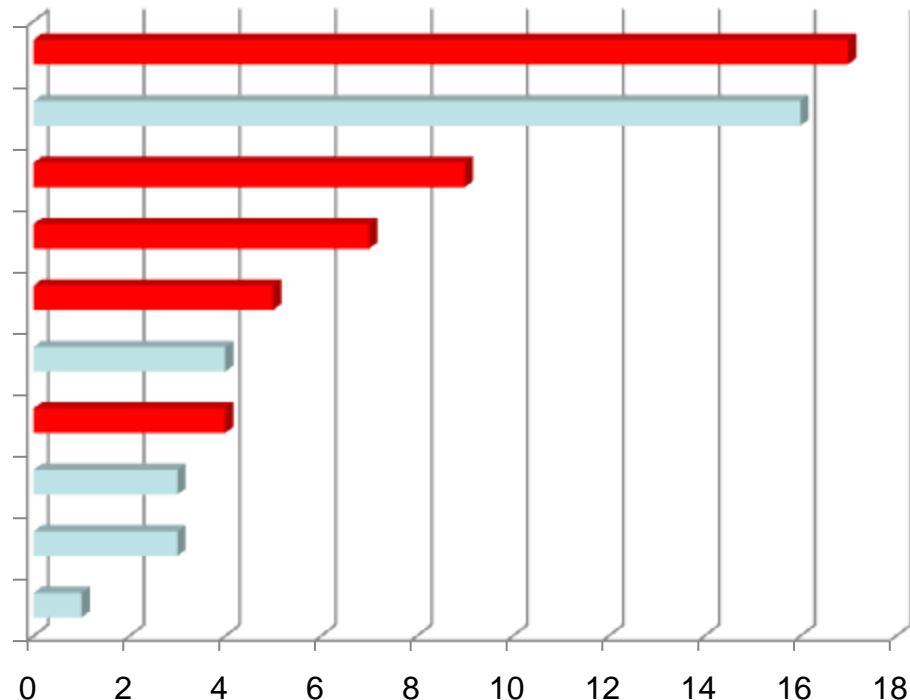
Privilege Escalation

Brute Force

Buffer Overflow

Session Variables

Cross-Site Scripting



- Indemnification

- Are the bits on your computer the bits you think they are?
- Are sensitive data, diagrams, and reports properly labeled?
- Are liability and incident response part of service agreements?
- Are users made aware of security policy?

WARNING

Unauthorized access to this system is forbidden and will be prosecuted by law. By accessing this system, you agree that your actions may be monitored if unauthorized usage is suspected.

ISA-99 Reference Model

If it's not control... move it up the stack!

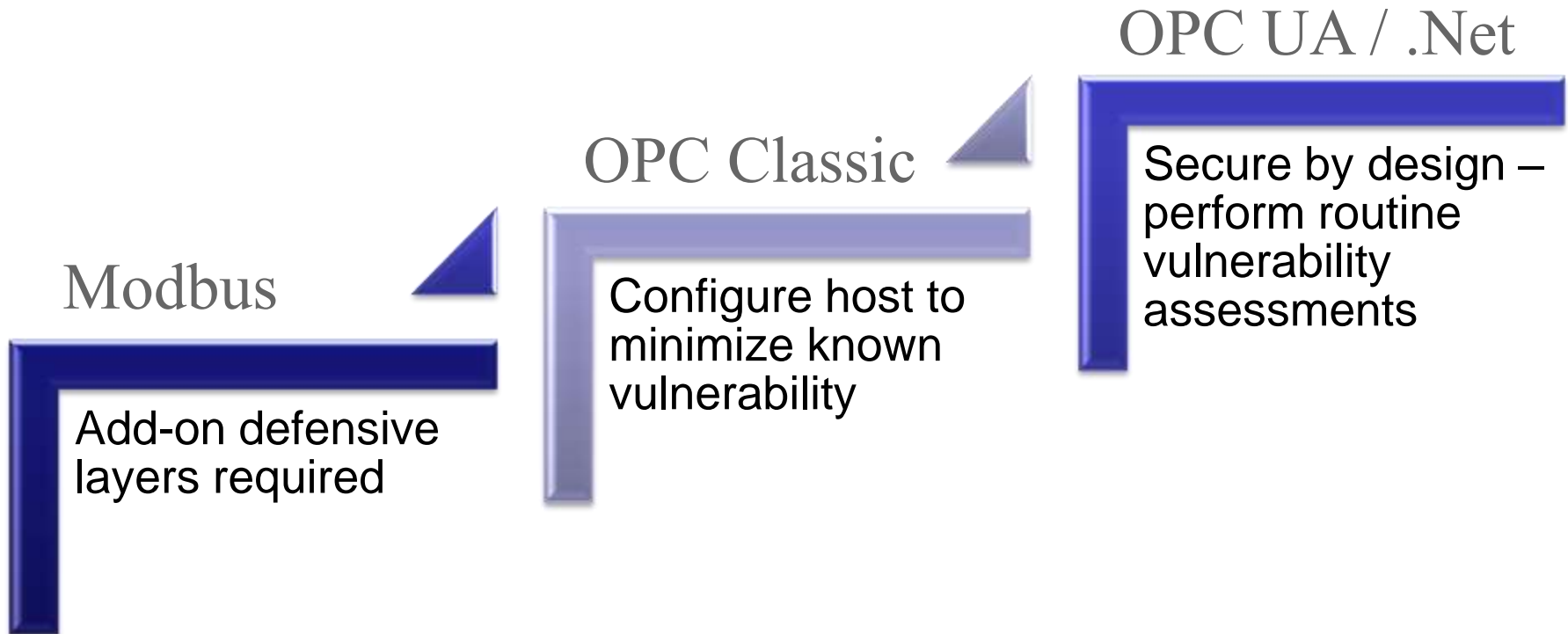
Enterprise Zone

- Level 4: Business systems

Control Zone

- Level 3: Site operation and control
- Level 2: Area and supervisory control
- Level 1: Basic control / SIS
- Level 0: Process devices

Protocol Substitution



DHS US-CERT: “Hardening Guidelines for OPC Hosts”
http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

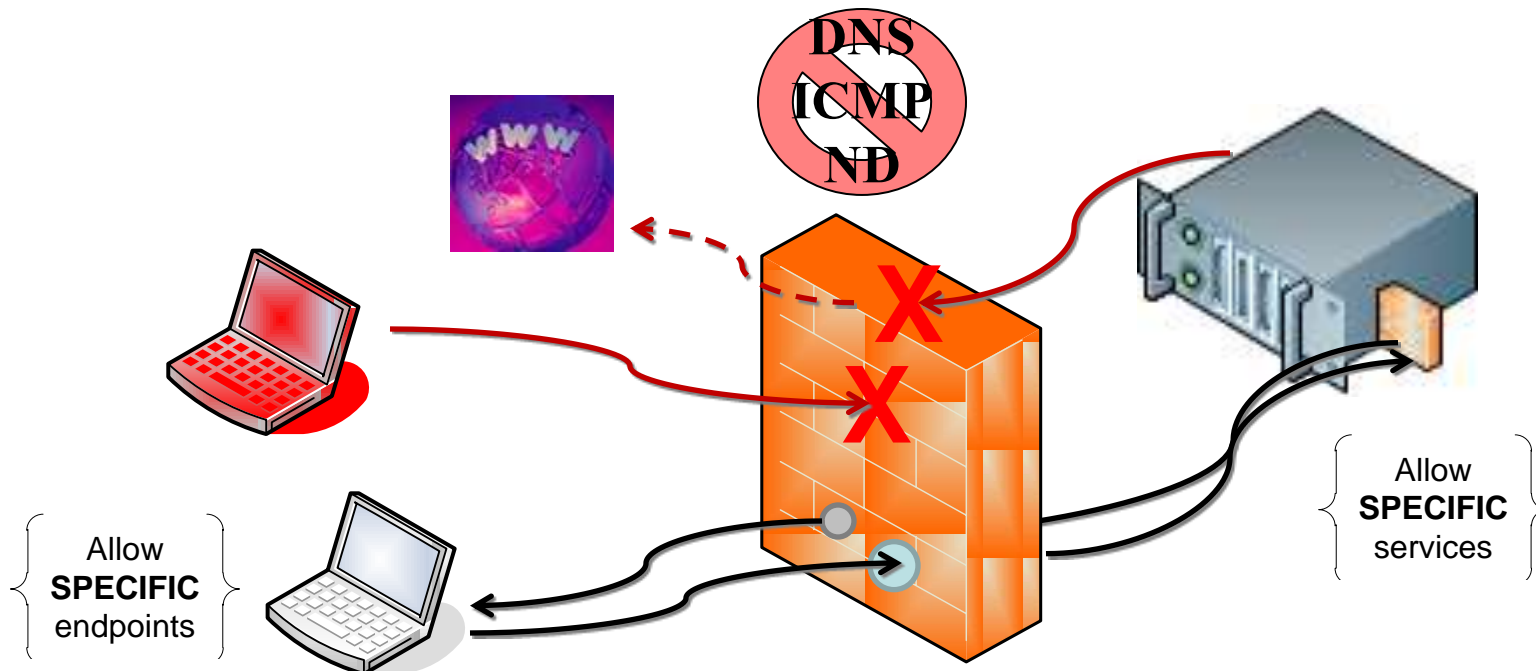
Firewalls

Network Firewall

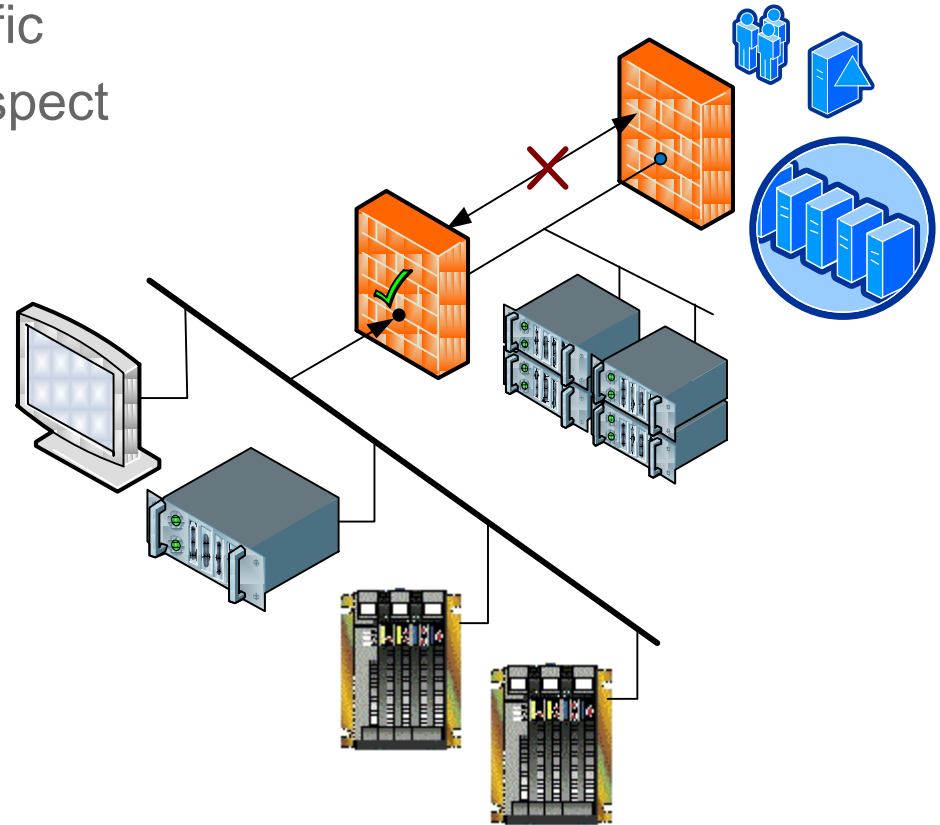
- Layered defense
- Filter host and protocol
- *Caution: VPN tunnels*

Host Firewall

- 2nd Order IST
- Filter application endpoints
- *Caution: outbound bypass*

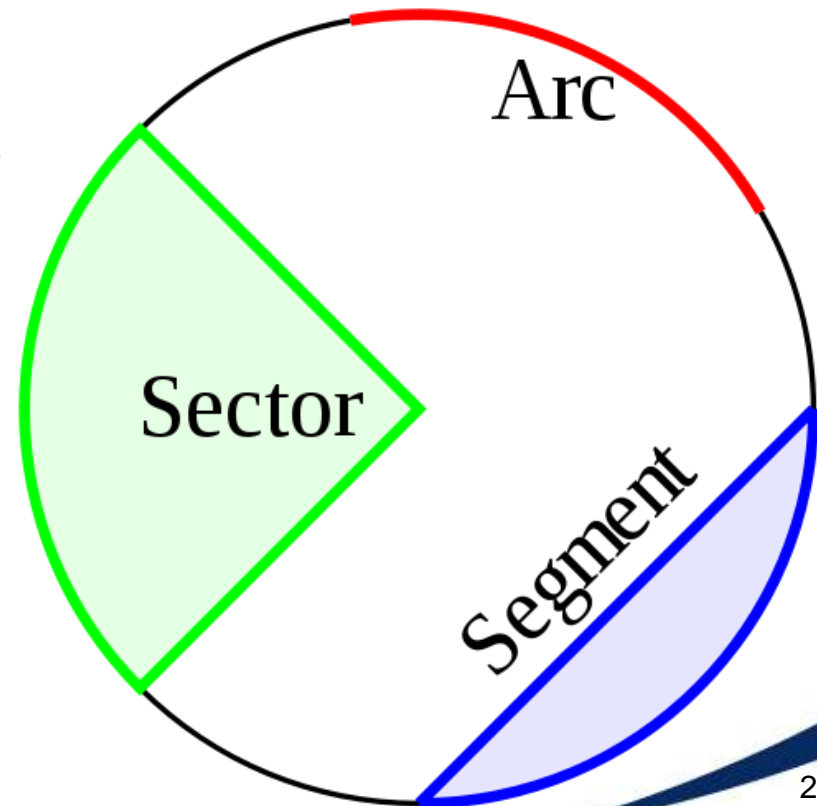


- Railway “Break-of-Gauge” concept
 - Eliminate direct end to end traffic
 - “Choke” point to unload and inspect
 - Did not survive move to air
- Control network
 - Push data out
 - Pull data in
 - Necessary protocols only
 - Separate logon authority
 - Non routable IP address space



- Drop unused features
 - Low implementation risk
 - Only reduces ‘potential’ abuse
- Assess used features
 - Provide alternatives
 - Minimal build for dedicated service

**Hidden Benefit:
Less Patching**

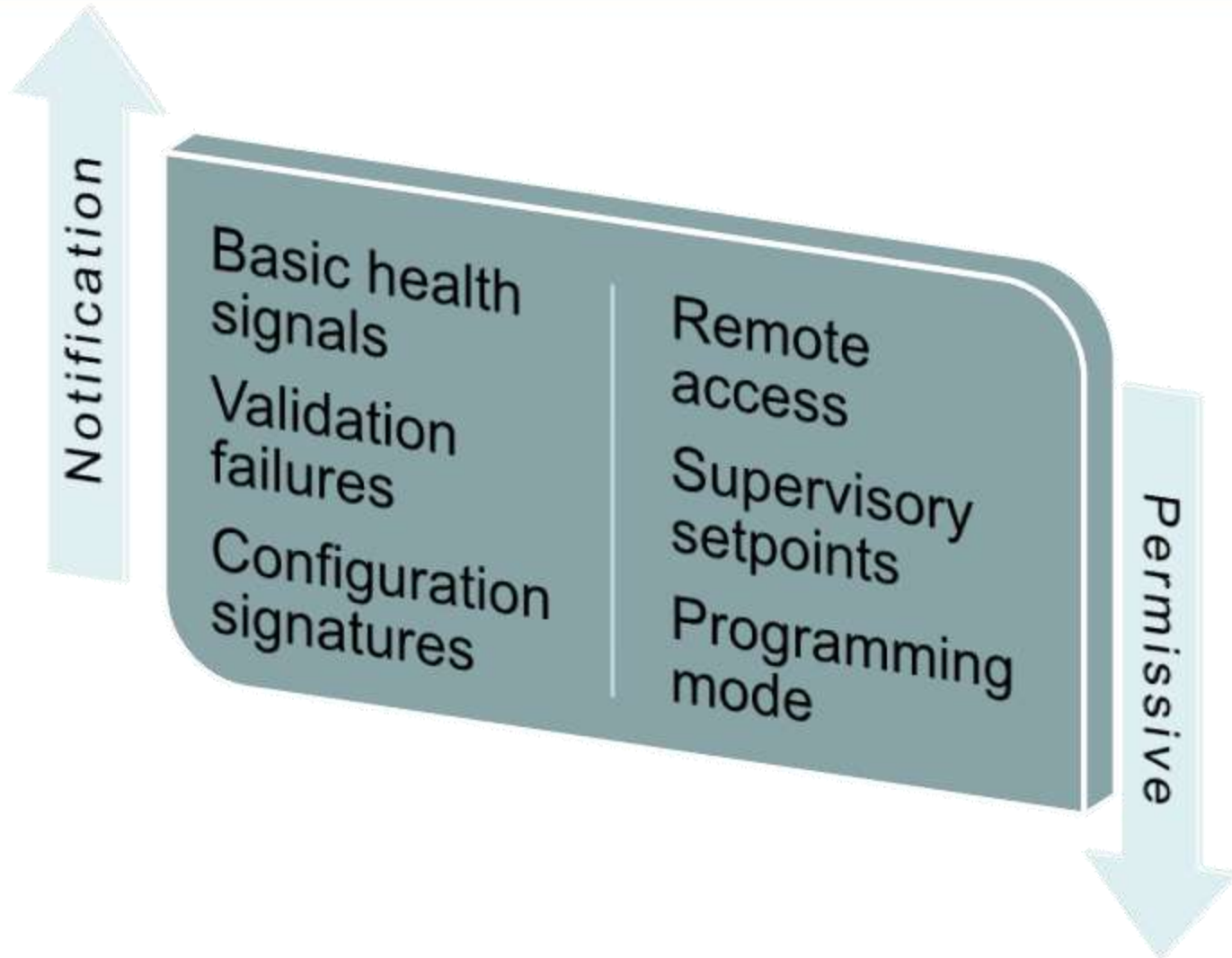


- Reduces damage potential
 - Integrate with system design
 - Work with vendors on usability
- Assess common activities

If admin/root is required:

- “Run As” shortcuts
- “Drop my rights”
- *nix “sudo”



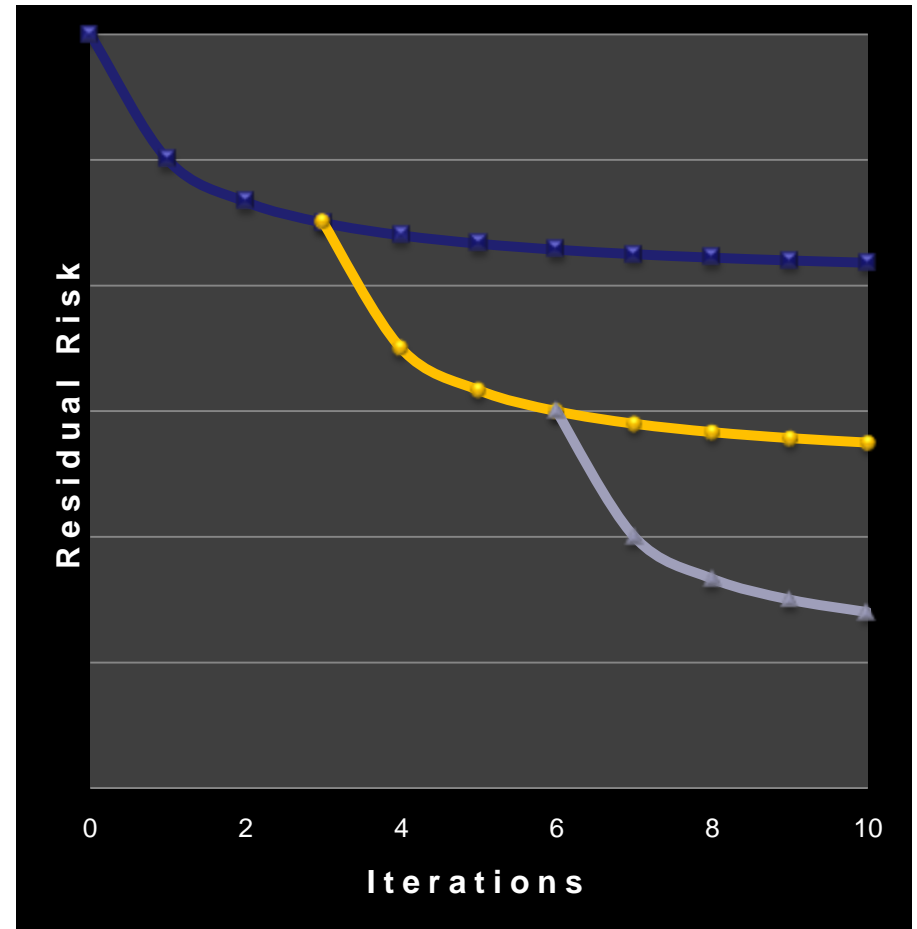


Discussion Question

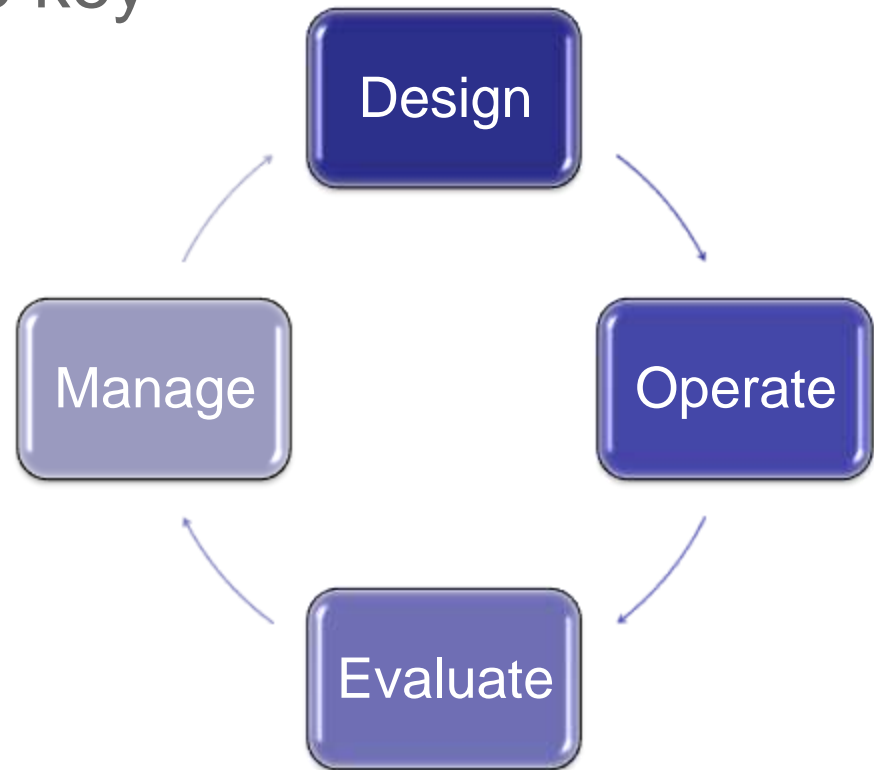


What is most effective for ICS cyber security?

- a) Eliminate and Prevent
- b) Reduce and Protect
- c) Layers of Protection
- d) Iterative Process



- IST philosophy is useful for ICS security
- Consistent with security standards (ISA-99)
- Iterative approach is the key
- Establish a cadence



trust *loyalty*
honesty *integrity*
courage

The CODE of the WEST



TEN PRINCIPLES TO LIVE BY



- 1 LIVE EACH DAY WITH COURAGE
- 2 TAKE PRIDE IN YOUR WORK
- 3 ALWAYS FINISH WHAT YOU START
- 4 DO WHAT HAS TO BE DONE
- 5 BE TOUGH, BUT FAIR
- 6 WHEN YOU MAKE A PROMISE, KEEP IT
- 7 RIDE FOR THE BRAND
- 8 TALK LESS AND SAY MORE
- 9 REMEMBER THAT SOME THINGS AREN'T FOR SALE
- 10 KNOW WHERE TO DRAW THE LINE