INL/MIS-18-46135-Revision-0

NSDD Partnership Working Together to Prevent Nuclear Trafficking

Jeff Knight, Adrian Pidlusky, Richard Pappas

August 2018

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/MIS-18-46135-Revision-0

NSDD Partnership Working Together to Prevent Nuclear Trafficking

Jeff Knight, Adrian Pidlusky, Richard Pappas

August 2018

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

NSDD Partnership

Working Together to Prevent Nuclear Trafficking

The Office of Nuclear Smuggling Detection and Deterrence

Managing Cyber Risk

Assessing, Monitoring, Responding

Richard Pappas, Adrian Pidlusky,
Jeff Knight

August 2018

National Nuclear Security Administration

Agenda – Day 1

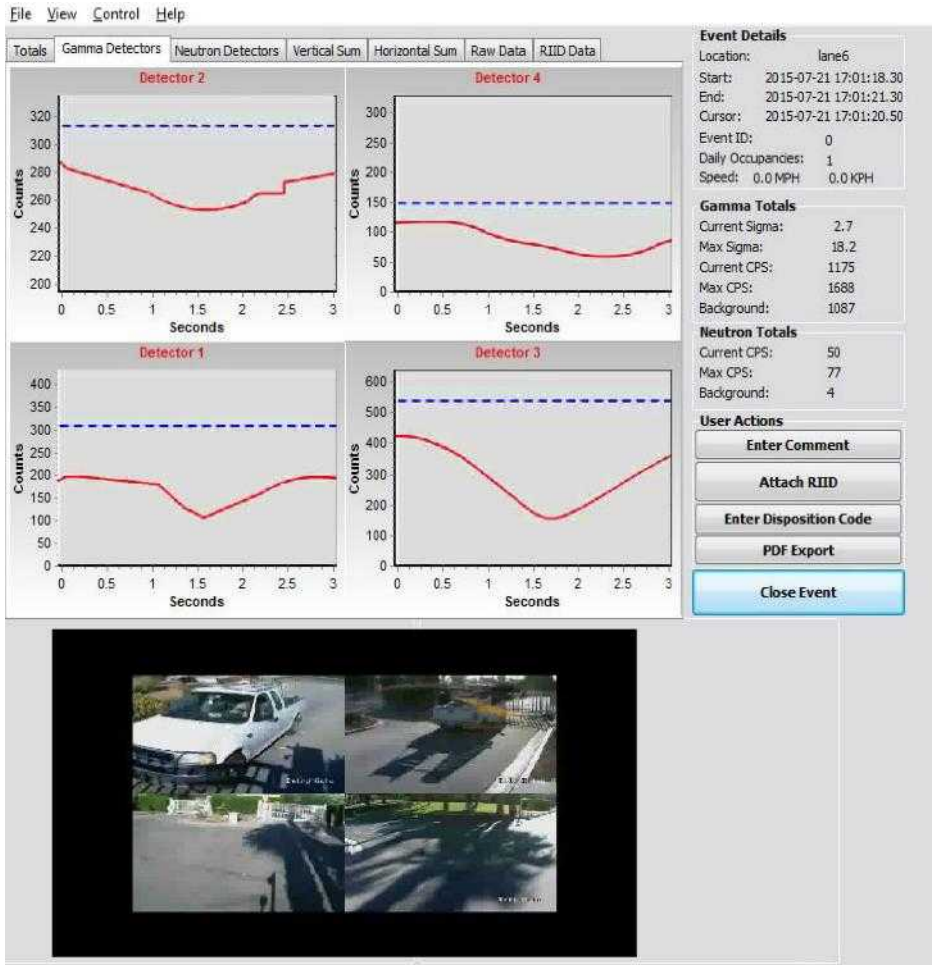
NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

- Cybersecurity and Operational Technology Considerations
- RISK Management Frameworks
  - Overview & Methodologies
- Cybersecurity Frameworks
  - Identify, Protect, Detect, Respond, Recover
- Digital Asset
  - Assessment
  - Categorization, Control Selection, & Implementation
- Portable Media & Mobile Devices
- Virtual Private Networks

National Nuclear Security Administration

Impact of Digital Dependencies

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence



National Nuclear Security Administration

Understanding Digital Technologies

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

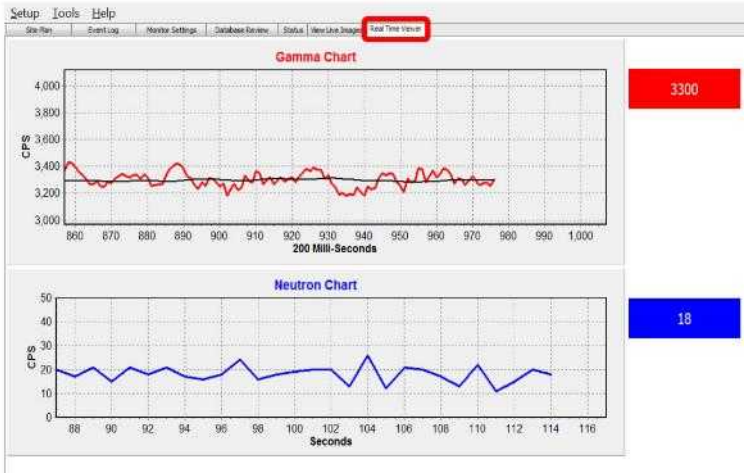
Cyber Systems = Digital Technologies

- Digital Technologies are designed to facilitate the storage, processing, and manipulation of information.

- Previously, RPM data signals would route to an alarm panel to indicate occupancy status

- Digital technologies further automated those processes and provides additional details ranging from integrated video signals, gamma reads, etc.

- **Digital/Cyber Technologies = Intelligent Processes**



Where Are The Digital Assets?

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

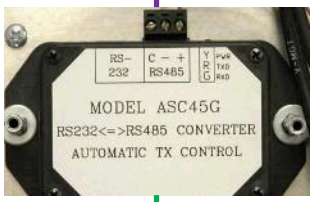
NNSA
National Nuclear Security Administration

A Closer Look at a RPM

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

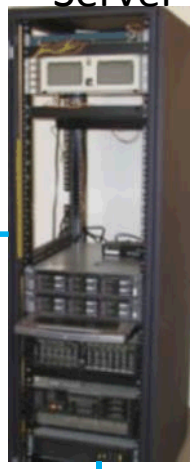
Gamma Detector With PMT

Media Converter



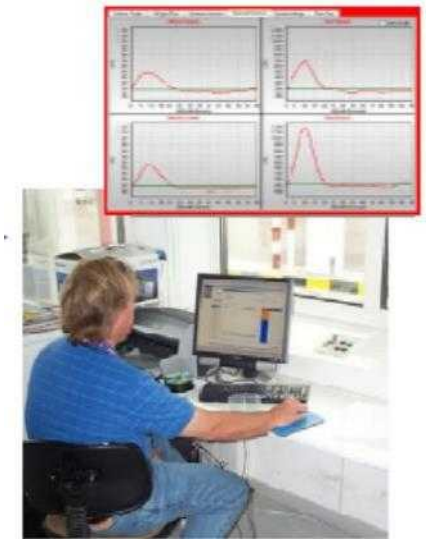
SC-770
PLC / HMI /
Media Converter

Server



SCA-775
Amplifier / Power Supply

Central Alarm Station



Assess Digital Assets: Crossing Point

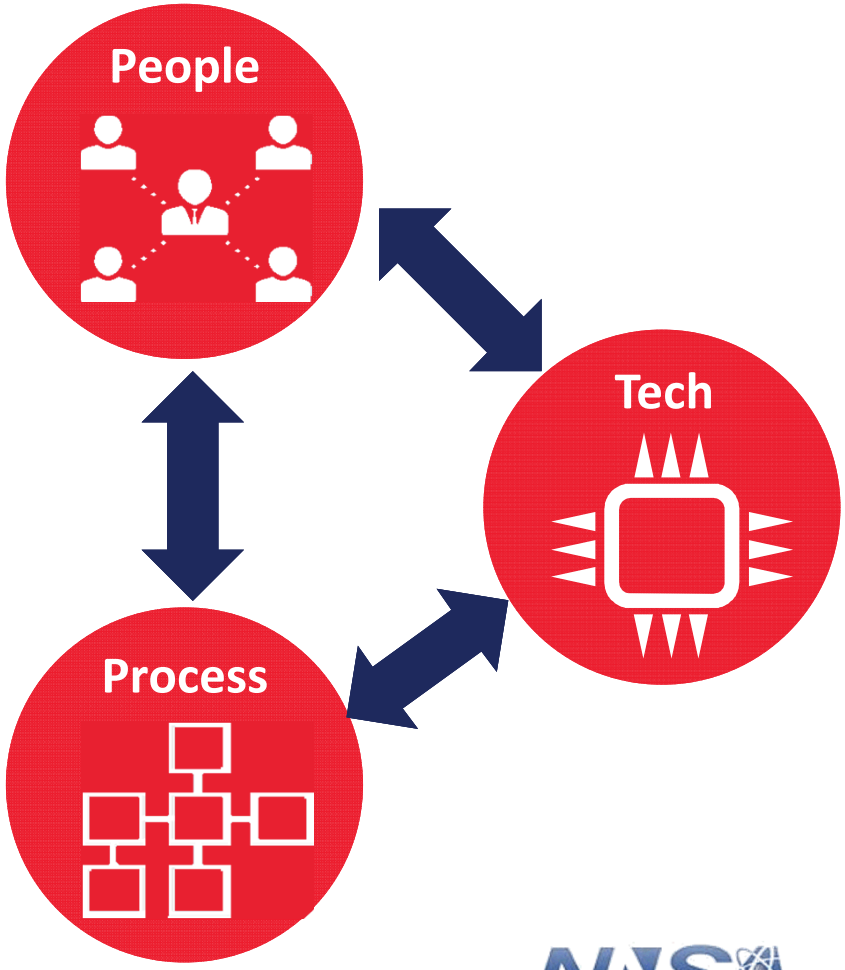
NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

- Physical
  - Locks, gates, logs, other access control
- Personnel
  - Who/What/When/Where
- Operational Technology (OT)
  - Mod/ProfiBus, IP & non-IP comms
  - Border Crossing Points: Flat Network
- Information Technology (IT)
  - IP based
  - Customizable
- DATA… and yes don't forget DATA
  - Host/system resident
    - Logs, set points, operational data
  - Non-resident
    - Assessment, configuration, backups

National Nuclear Security Administration

Cybersecurity: Defined

- Cybersecurity Program:
  - Management to protect digital operations
  - Proactive protection of digital signals to:
    - Identify risks
    - Detect malevolent actions
    - Protect assets
    - Respond to detected adversary
    - Recover promptly from an attack



What is Cyber RISK?

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

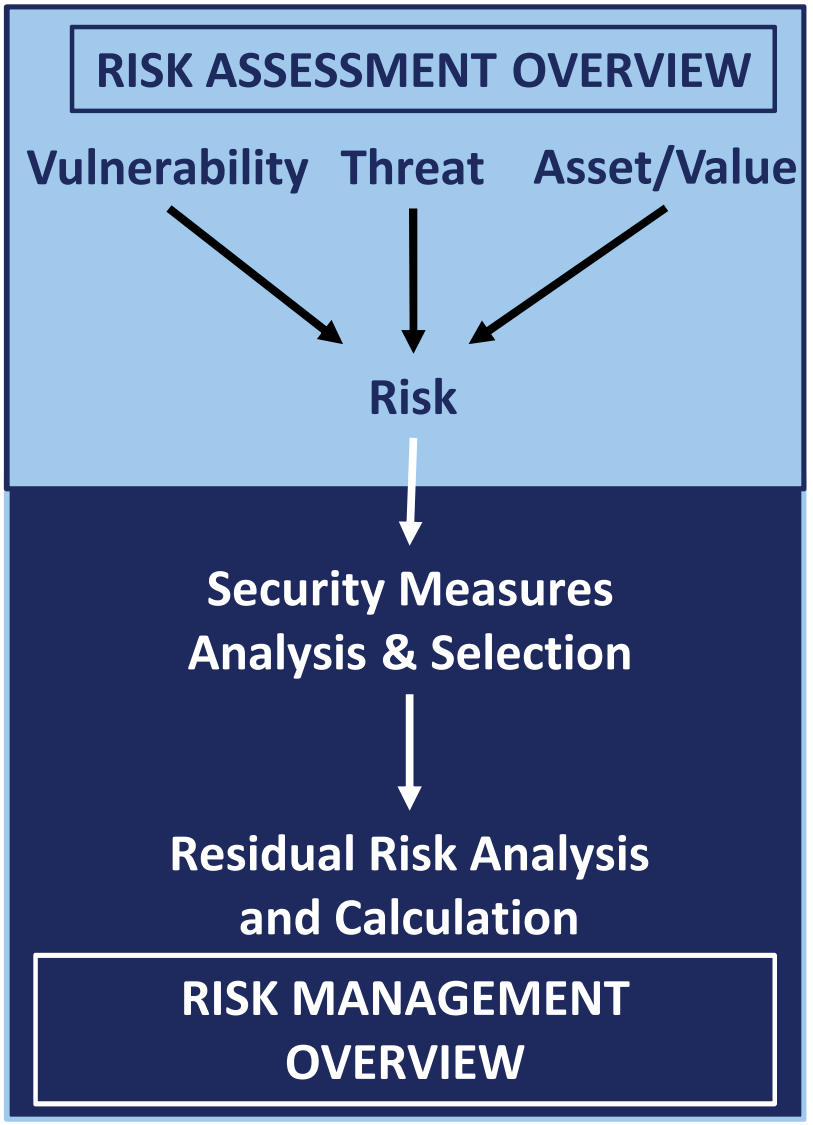
- **Risk** – A combination of variables quantifying an asset, system or missions' exposure to harm
- **Vulnerability** – A weakness in a system, procedure, control, or implementation that can be exploited by a threat
- **Threat** – Any event or group having the potential to adversely impact operations, assets, or functions
- **Asset** – A mission-critical system or technology device – digitally programmable
- **Exploit** – A process, program, or code that enables attackers to leverage a vulnerability to gain unauthorized access into a system

National Nuclear Security Administration

RISK Concepts – Benefits & Concerns

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

- Identify Risks for Programmatic Action
  - Identify assets and/or operations that are the most exposed to the adversary
- Design Basis Threat
  - Does the threat capabilities and asset vulnerabilities align?
- What can you do with RISK?
  - Categorize and prioritize
  - Prevent, accept, transfer, reduce, and eliminate
- Can you fully address RISK?
  - Residual
  - Zero



Are Your Assets at RISK?

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

The Internet of Things

- During 2008,the number of things connected to the internet exceeded the number of people on earth
- By 2020,there will be 50 billion devices connected to the internet
- Are your assets connected?

National Nuclear Security Administration

Managing & Prioritizing Risk

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

Risk Rating = Likelihood * Consequence

Consequence							
	Catastrophic	5	5	10	15	20	25
	Significant	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Negligible	1	1	2	3	4	5
			1	2	3	4	5
			Improbable	Remote	Occasional	Probable	Frequent
			Likelihood				

National Nuclear Security Administration

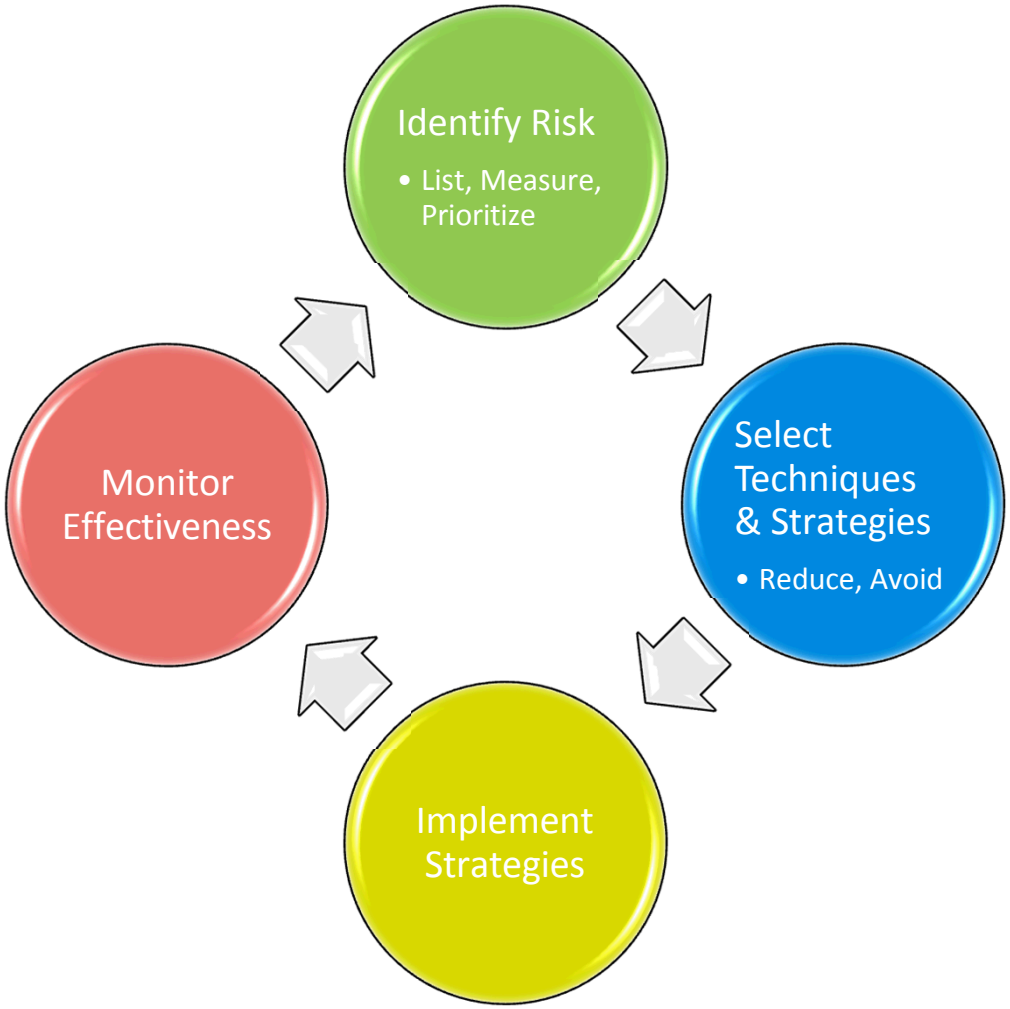
Organizations – RISK Management Standards & Methodologies

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

- International Standards Organization (ISO)
  - ISO 3100 family of standards & guide 73:2002
  - ISO 2700 series
  - Principles and generic guidelines
- National Institute of Standards & Technologies (NIST)
  - NIST 800-37 & NIST 800-39
  - Applying and implementing the Risk Management Framework
  - Assess, respond, monitor
- International Atomic Energy Agency
  - IAEA-TECDOC-1209
  - NSS-17 and others
  - A Tool for Improving Cybersecurity Risk Management
- European Union Agency for Network and Information Security (ENISA)
  - Good reference for inventory of risk assessment and risk management methods

Risk Management – IAEA TecDoc-1209

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence



National Nuclear Security Administration

Risk Management – NIST 800-39

Cybersecurity Framework – NIST v1.1

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

Credit: N. Hanacek/NIST

National Nuclear Security Administration

Cybersecurity Framework – Identify

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

Asset Management

- NIST Cybersecurity Framework: Asset Management is the first principle for establishing a strong cybersecurity program
- Categorize and prioritize assets based on criticality
- Critical Systems are primary to safe and secure facility operation
- Critical/Sensitive Digital Assets (CDA or SDA) are assets that must be protected

Function/ Category	Sub-Category
IDENTIFY Manage Asset	Physical devices and systems within the organization are inventoried
	Software platforms and applications within the organization are inventoried
	Organizational communication and data flows are mapped
	External connected systems are cataloged
	Resources (hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

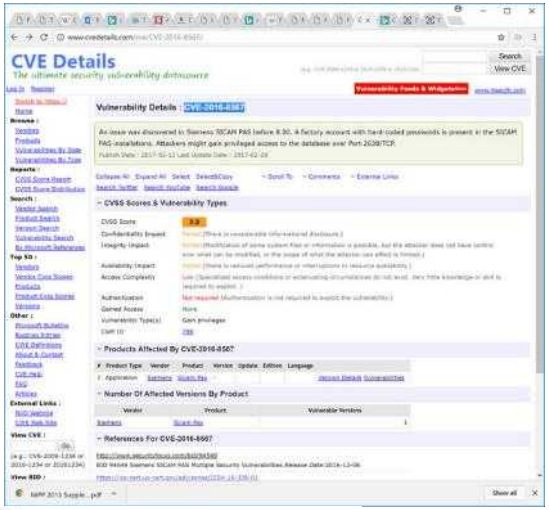
National Nuclear Security Administration

Cybersecurity Framework – Protect

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

Define CS and CDA Exposure and Controls

- During asset characterization, record any previous unaddressed vulnerabilities
- Control Selection & Baselines
- Record vulnerabilities that have been addressed by security controls
- Residual vulnerabilities in a CS and/or CDAs could harm the facility and the risk profile



National Nuclear Security Administration

Cybersecurity Framework – Detect

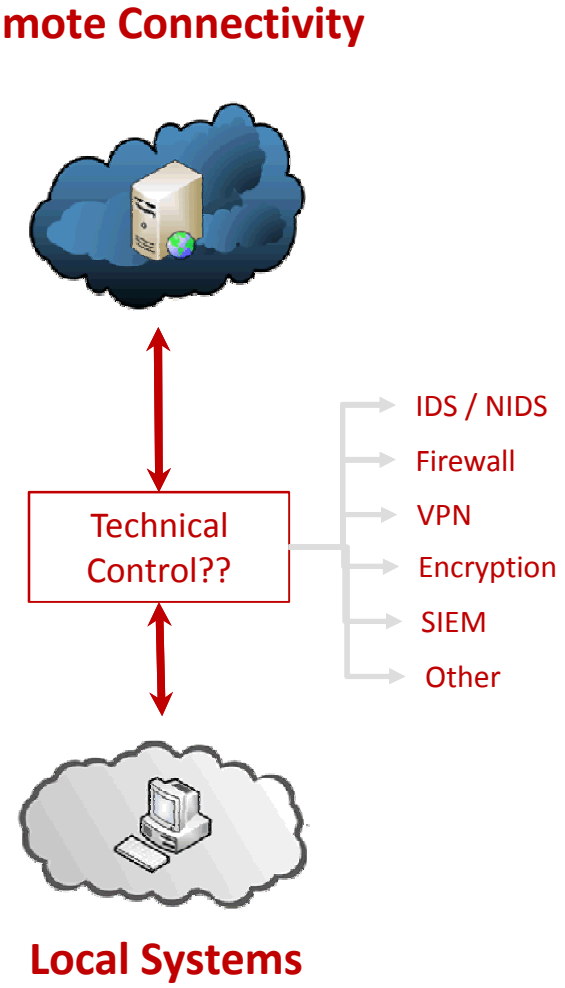
NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

Monitoring and Enforcement

- Technological controls monitor and enforce data traffic and operations
- Architecture rules should maintain parity among zones and levels

What is the difference between monitoring and detecting?

How does asset lifecycle affect overall cybersecurity protection profile?



National Nuclear Security Administration

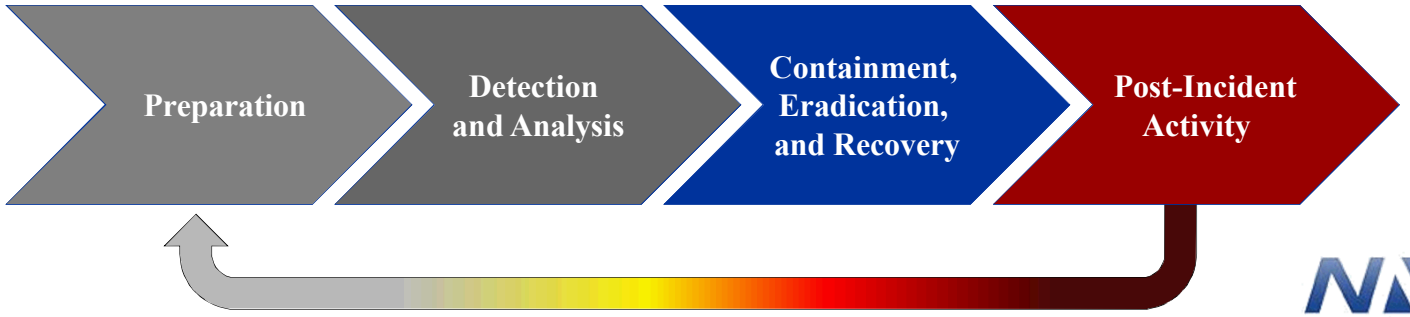
Cybersecurity Framework – Respond & Recover

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

What is a computer security incident?

> "an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a computer based, networked or digital information system or the information that the system processes, stores, or transmits or that constitutes a violation or imminent risk of violation of security policies, security procedures, or acceptable use policies" (IAEA NSS-17)

- Have defined roles and responsibilities
- Establish reporting criteria
- Advance capabilities include forensics and malware analysis



National Nuclear Security Administration

RISK Assessment Tools

- Software Engineering Institute
  - OCTAVE
  - Operationally Critical Threat Asset and Vulnerability Evaluation
- Military – 1970s
  - CARVER
  - Criticality, Accessibility, Recoverability, Vulnerability, Effect, and Recognizability
  - Think like an aggressor
- Electric Power Research Institute (EPRI)
  - Technical Assessment Methodology
- ENISA
  - Inventory of Risk Management and Risk Assessment tools

RISK Assessment – Scoping & Grouping

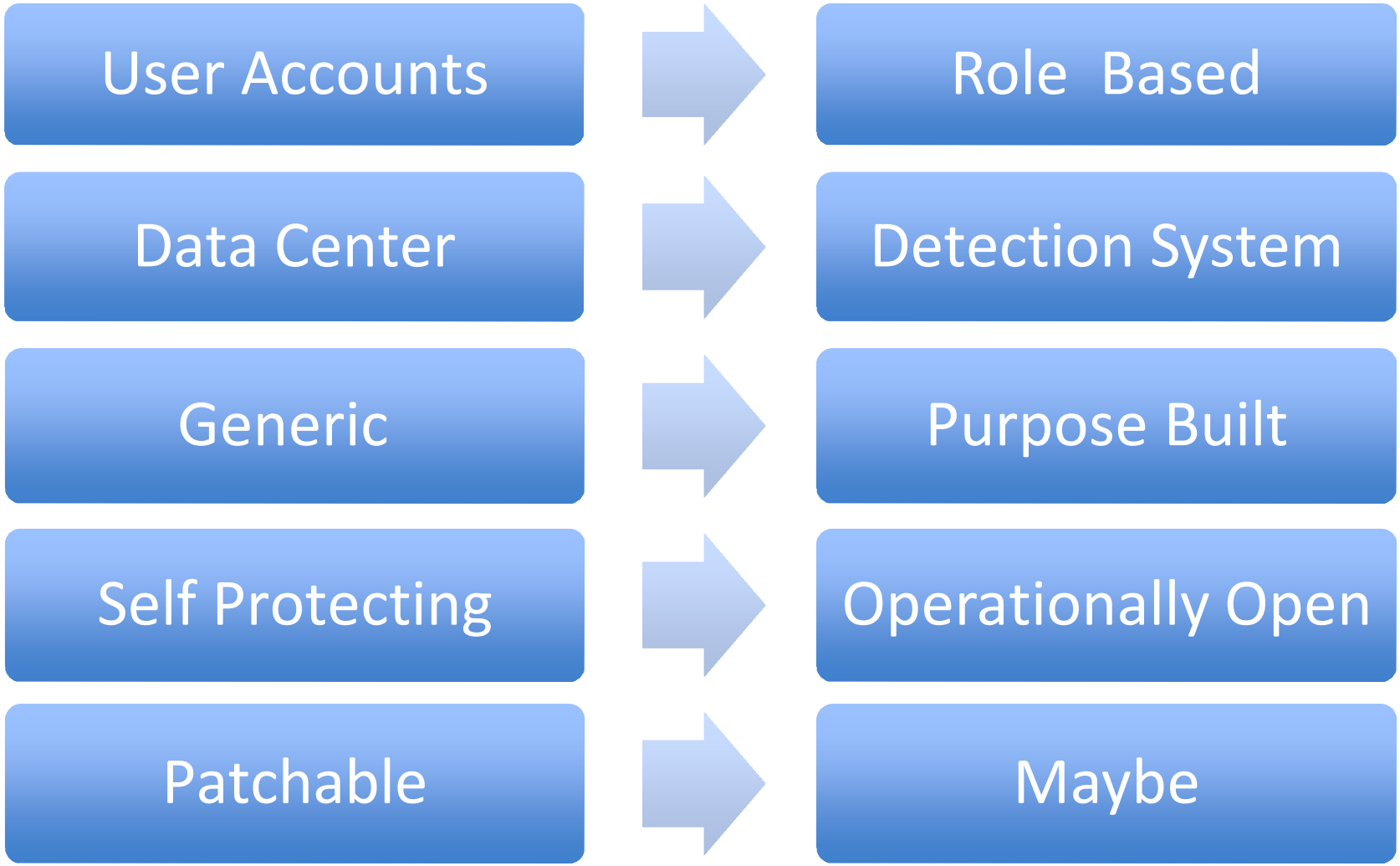
NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

Assessment Process

1. Site
2. System
3. Device

IT versus OT Challenges

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence



National Nuclear Security Administration

Patching Challenges – Hatch Nuclear Power Plant

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

- Event: March 2008, a software update caused a control system to initiate plant shutdown
- Impact: The plant was shut down for 48 hours
- Specifics: An engineer installed a software update on a computer operating on the plant's business network. When the updated computer rebooted it reset the data on the control system, causing safety systems to misinterpret the data.
- Recovery time: 48 hours

Lessons Learned

- Test before deploying
- Business (IT) to Operational (OT) networks must be tightly managed

National Nuclear Security Administration

Communication Pathways

- Wired
  - IP, OT protocols
  - Fiber, Ethernet, RS-xyz
- Wireless
  - WiFi, Bluetooth
  - Wireless Access Points
  - Hot spots - Portable phones
- Media
  - Thumb drives, CDROMS
  - Many, many types
- People
  - Keyboards

Portable Media & Mobile Devices

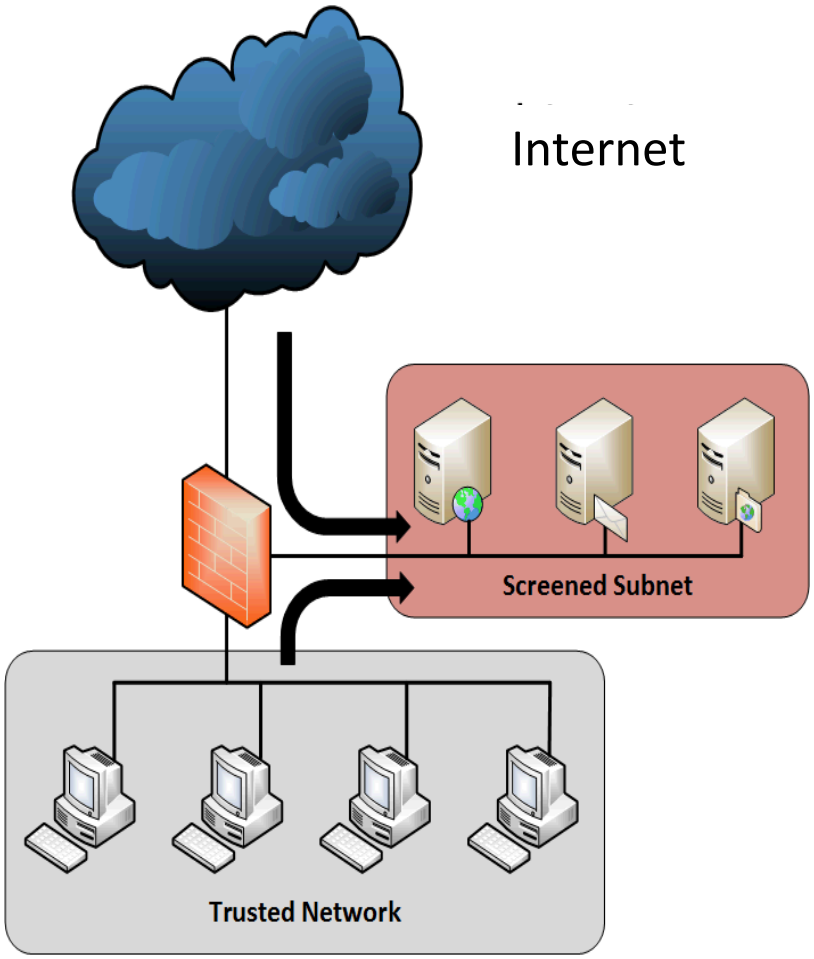
How to Develop a PMMD Program

- Policies and Procedures
  - Devices in scope
  - Check-in / check-out process
  - Storage locations and access control
- Training
  - Generic for all personnel
  - Job specific
- Malware Scanning Kiosk
  - Used to verify that media is free of harmful files
  - Should be HARDENED – cannot become a vector!

Sneaker net can circumvent the most secure architecture!

Remote Connectivity – VPNs

- Guide to Securing VPNs
  - NIST 800-77
  - Various technical controls such as firewalls and VPNS can be implemented across defensive architectures to protect critical systems and assets
  - Common configurations utilize VPN Gateways for enterprise connectivity
  - VPNs can provide data protection, including confidentiality, integrity, data origin authentication, and access control



Agenda – Day 2

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

- BGHQ
  - Threat Assessment
    - Determination process & tools
    - Design Basis Threat determination
  - Vulnerability Assessment
    - Determination process & tools
    - Control selection & implementation
- Site Visit
  - Risk Assessment
    - Table-tops & walk-downs
    - Site, systems, assets – hardware, software

National Nuclear Security Administration

Your Turn – Who has a Question?

NSDD Partnership
Working Together to Prevent Nuclear Trafficking
The Office of Nuclear Smuggling Detection and Deterrence

National Nuclear Security Administration