How Insider Risk Develops in OT Environments

A Cybersecurity & Psychological Perspective

John E. Landers, Ph.D.
Clinical/Forensic Psychologist,
Nuclear Security Analyst
Idaho National Laboratory

Shannon L. Eggers, Ph.D.
Nuclear Cybersecurity Specialist
Idaho National Laboratory

U.S. DEPARTMENT of ENERGY

National Nuclear Security Administration

Roadmap: How Insider Risk Develops in OT

Why insider risk matters in OT environments

What OT is and why cyber risk has physical consequences

How OT threat pathways create insider opportunities

Maroochy Shire as a cyber-physical insider case study

Technical attack timeline and psychological risk timeline

Observable changes that appear before escalation

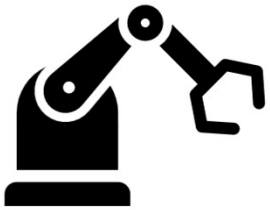
How distributed signals become meaningful when integrated

Early response to disrupt the insider-risk pathway

Q&A and discussion

What is Operational Technology (OT)

Operational Technology (OT)
(Devices & Software)



Monitoring and Control of Physical Systems

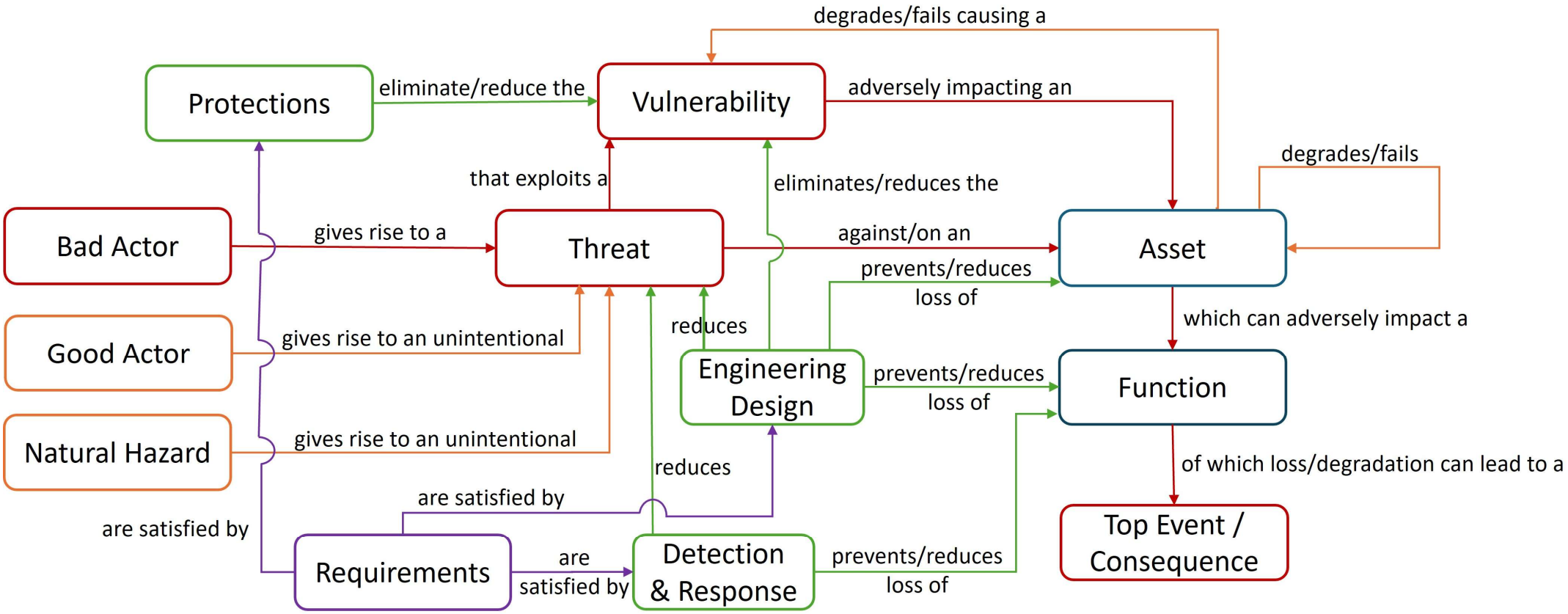
Cyber-physical systems

Very time critical

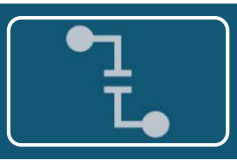
Primary risk is loss of device control and system functions

Characteristic	Description
Availability	24 x 7 x 365
Time critical content	Critical – time precision
Technology support lifetime	20+ years
Security upgrades	No common practice
Security awareness	Poor except for physical
Antivirus	Uncommon and can be difficult to deploy
Outsourcing	Rare
Incident response	Uncommon
Security testing/audits	Not well established

What is OT Cyber Risk?



Cyber Attack Pathways
Where is the Insider Threat?



WIRED NETWORKS

- Exploited through insecure architectures.

WIRELESS NETWORKS

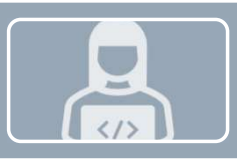
- Exploited through unencrypted, over-the-air transmissions.

PORTABLE MEDIA & MOBILE DEVICES

- Malicious software portable devices is transferred to OT equipment.

SUPPLY CHAIN

- Compromised hardware or software; or vendors/contractors with access to OT equipment



DIRECT PHYSICAL ACCESS

- Hands-on manipulation of OT equipment.

Maroochy Shire Attack (2000)

THE FIRST PUBLICLY DOCUMENTED MALICIOUS CYBERATTACK ON A CRITICAL INFRASTRUCTURE CONTROL SYSTEM

The Target

- Maroochy Shire Council sewage SCADA system—142 pump stations
- Controlled via analog UHF radio. No authentication, encryption, or logging.

The Attacker—Vitek Boden

- Site Supervisor for Hunter Watertech (HWT), the company that installed the system.
- Resigned in Dec 1999; rejected for a council job Jan 2000
- Motive: Retaliation against HWT and the Council

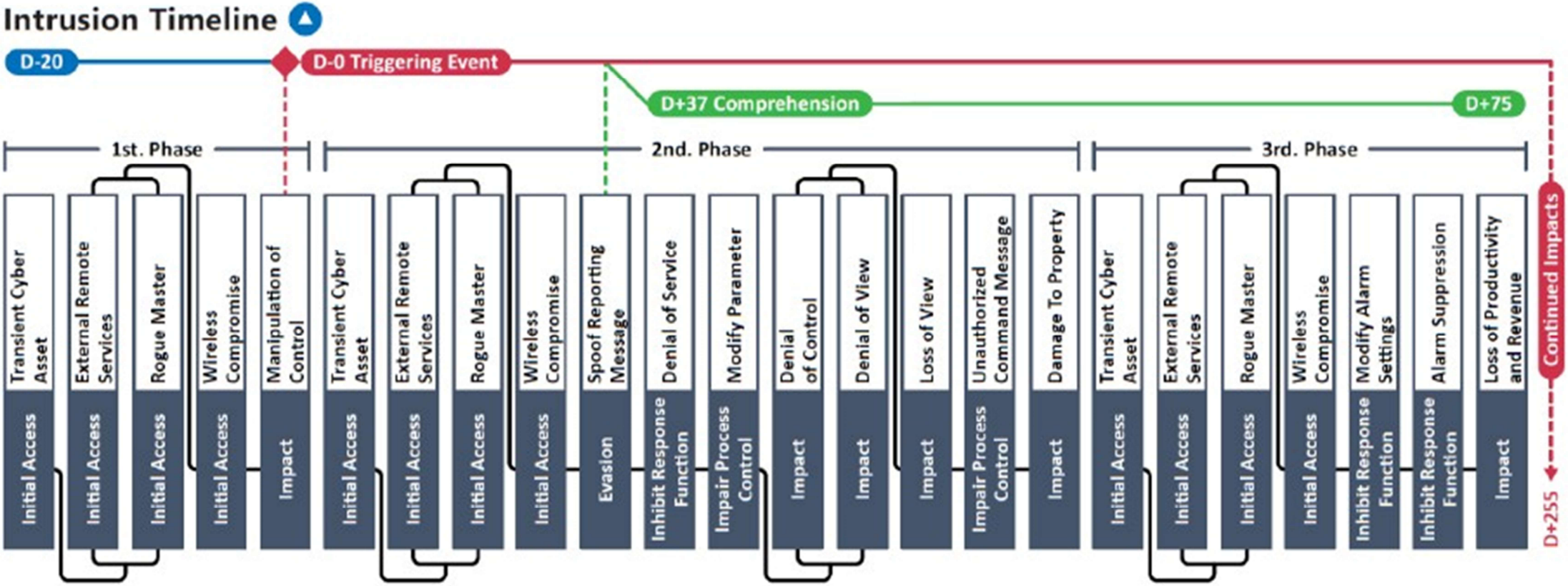
Method & Impact

- Drove around the area issuing unauthorized radio commands from his vehicle using stolen equipment and a laptop with proprietary software.
- Spoofed pumping stations to evade detection

DURATION **74 days**	SEWAGE RELEASED **800,000L**
COUNCIL COST **$176K AUD**	HWT COST **$500K+ AUD**

- Caught by a routine traffic stop.

Attack Timeline Mapped to MITRE ATT&CK for ICS Framework



Maroochy Shire: Psychological Timeline

This did not begin with the attack. It unfolded over time.

Employment:

Trusted role with system access and knowledge

Strain:

Relationship friction and increasing distance from the organization

Job rejection:

Attempted reaffiliation unsuccessful

Retained capability:

Knowledge and capability remain beyond role or affiliation

System anomalies:

Unexplained system events begin and escalate

Attack:

Deliberate misuse of system access causes real-world harm

Risk develops when signals remain fragmented across organizational boundaries.

What Changed Before the Maroochy Shire Event

Observable shifts in reliability – not indicators of intent

RELATIONSHIP TO ORGANIZATION

- Strained relationship with employer
- Attempted reaffiliation unsuccessful

ENGAGEMENT WITH WORK / SYSTEM

- Continued focus on the system
- Retention of system knowledge and capability

CONTEXTUAL SIGNALS

- Grievance or perceived unfairness
- Lack of shared awareness across functions

★ Individually explainable

★ Collectively meaningful

Observable Changes Across Cases

Seen across environments – not predictive of malicious action

WORK BEHAVIOR

- Conflict with supervision
- Withdrawal or reduced engagement

Deviation from established practices

ACCESS / SYSTEM INTERACTION

- Unusual system interaction patterns
- Workarounds or boundary testing

Retained or misused capability

ORGANIZATIONAL CONTEXT

- Grievance or perceived unfairness
- Role change, transition, or exclusion

Lack of shared awareness across functions

These signals are distributed across the organization.

These patterns are drawn from multiple cases across nuclear and industrial environments.

U.S. DEPARTMENT of ENERGY

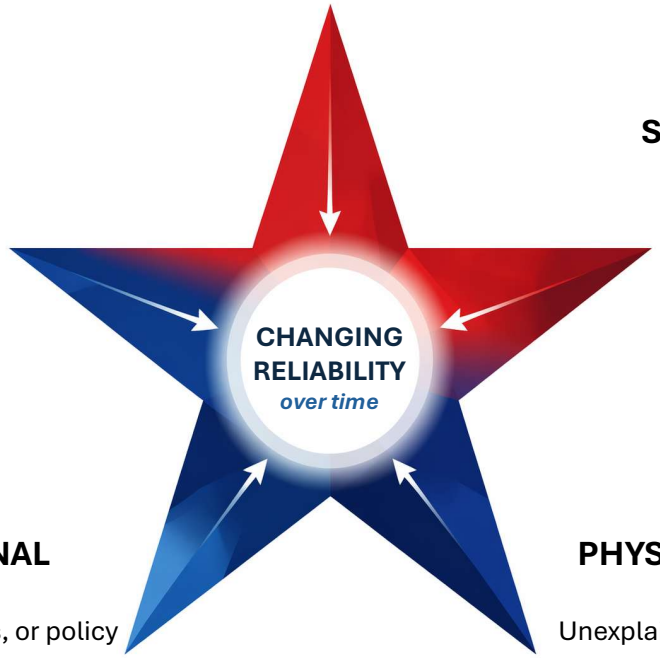
National Nuclear Security Administration

How Distributed Signals Become Meaningful

Risk becomes visible at the intersection – not from any single observation

SUPERVISORY OBSERVATIONS
Changes in behavior, attitude, or performance

PEER / WORKPLACE INTERACTION
Shifts in relationships, communication, or engagement



SYSTEM / ACCESS BEHAVIOR
Anomalies in access, use, or configuration

Integration enables earlier, more effective risk mitigation.

ORGANIZATIONAL CONTEXT
Role changes, grievances, or policy friction

PHYSICAL / OPERATIONAL SIGNALS
Unexplained events, errors, or safety / security deviations

Information about a person is distributed across the organization. No single part sees the whole picture.

U.S. DEPARTMENT of ENERGY

National Nuclear Security Administration

Early Response: Disrupt the Pathway

Timely, proportionate action reduces risk and supports the individual

Integrated understanding enables earlier, more effective action

Clarify and Understand

- Engage early and directly
- Ask questions
- Seek context

Stabilize Risk

- Adjust access or privileges
- Increase oversight as needed
- Reduce operational exposure to risk

Support the Individual and System

- Provide support and resources
- Offer options for resolution
- Enable a path back to reliability

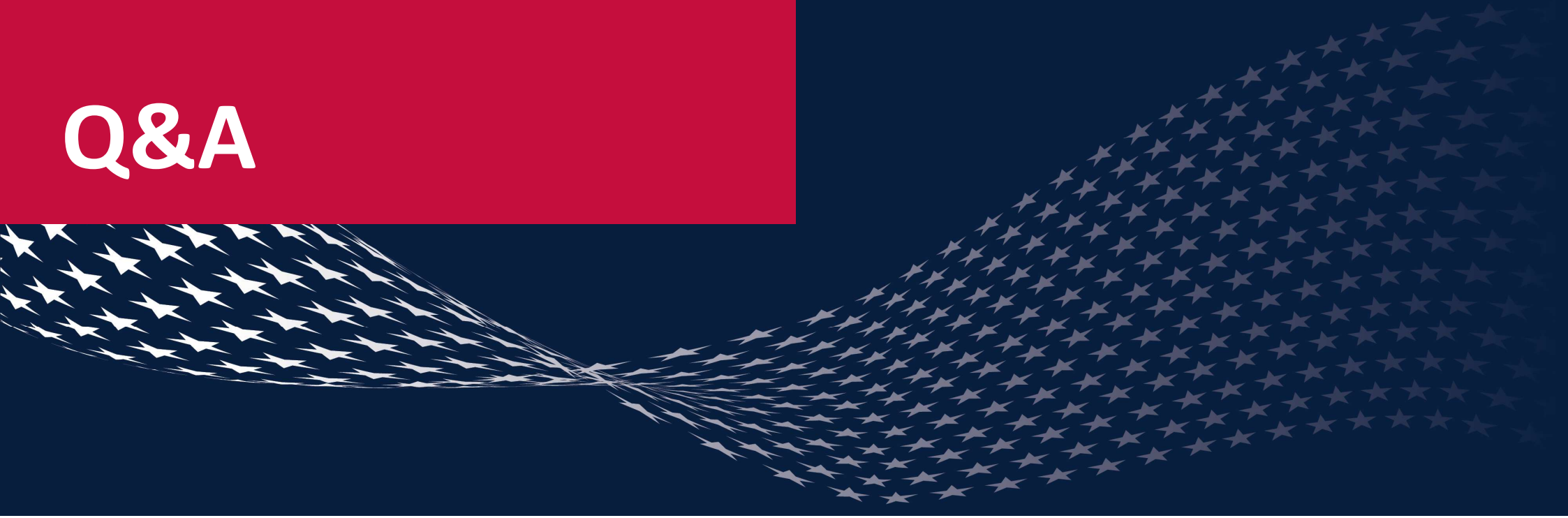
- ★ The goal is not to detect malicious action.
- ★ It is to disrupt the pathway.

Guided by observable workplace behavior • No profiling or prediction • Proportionate and early response

U.S. DEPARTMENT of ENERGY

National Nuclear Security Administration

Q&A



U.S. DEPARTMENT of ENERGY

National Nuclear Security Administration