Probe, Don’t Break:
Conducting OT Pen-Tests Safely

JASON DELY
PRINCIPAL INSTRUCTOR,
SANS INSTITUTE

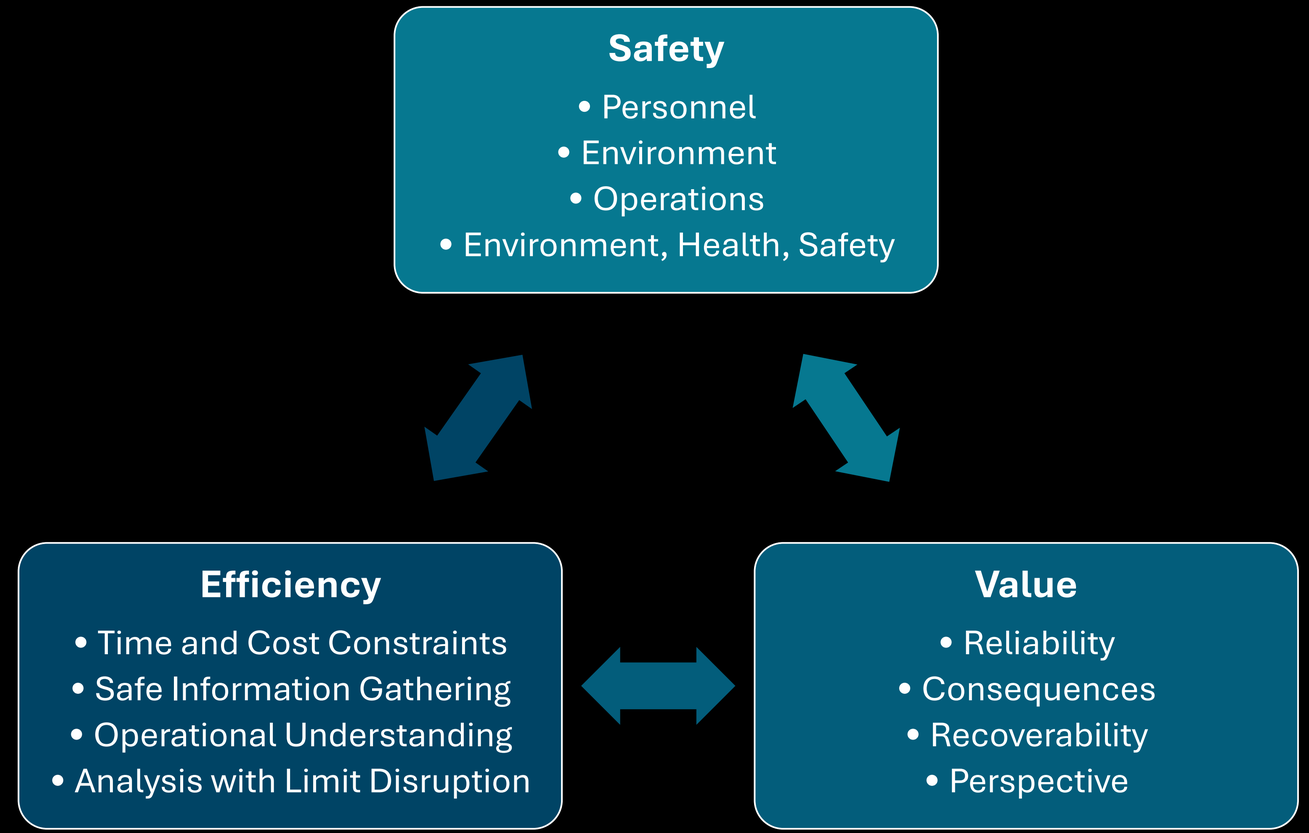
What are ICS/OT penetration tests?

1. Focus on identifying risks to operations, process control, and mechanical equipment
2. Understand the operation data workflow to ensure delivery and integrity
3. Identify implementation issues across complex ICS hardware and software deployments
4. Evaluate alignment of defenses against known threats

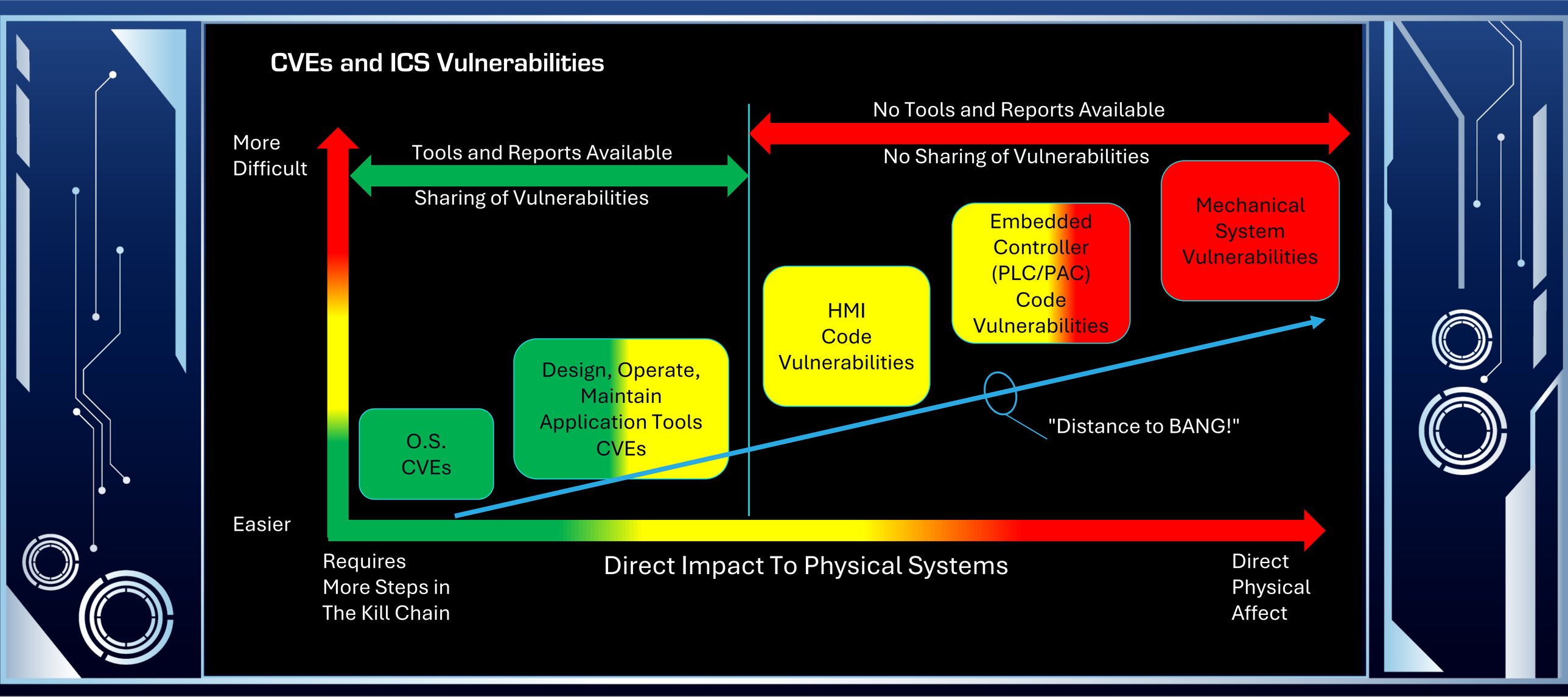
Support for ICS/OT Penetration Testing

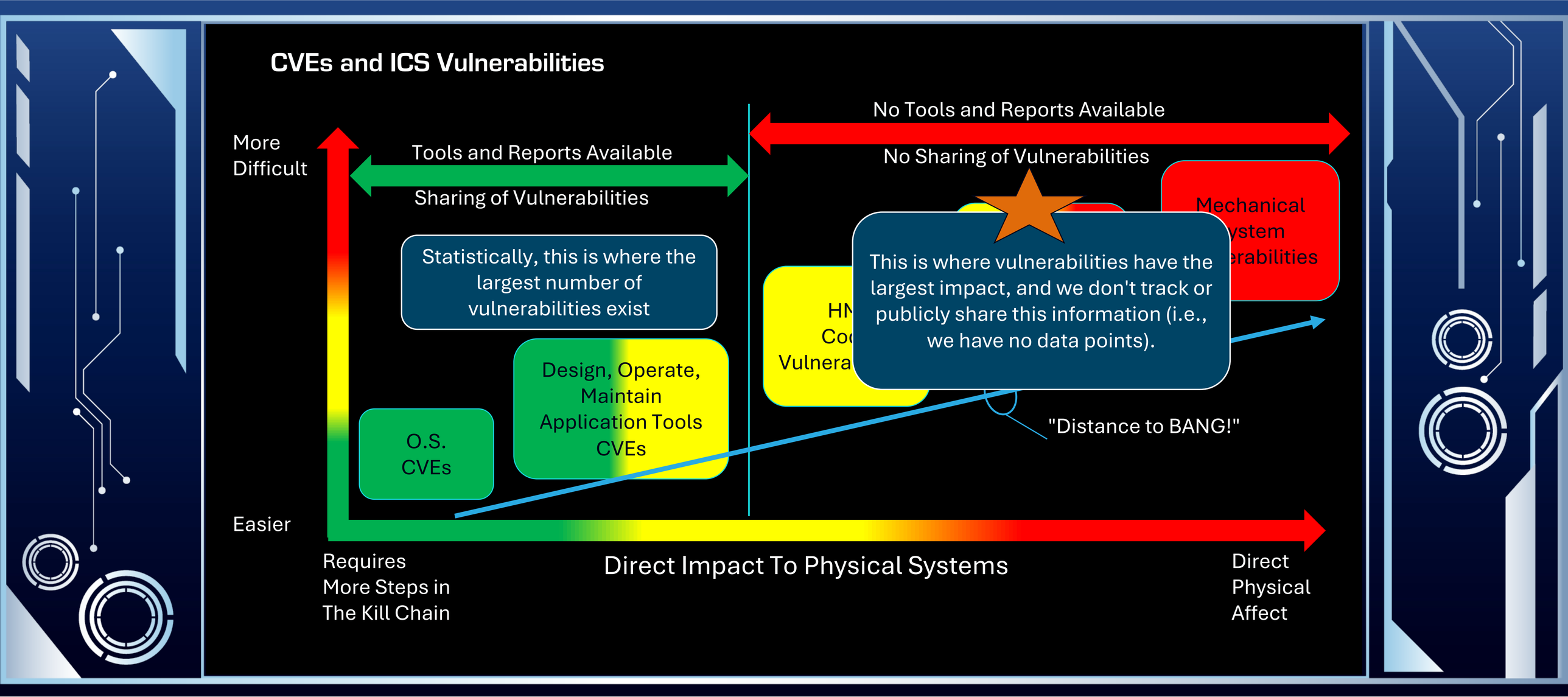
- Cybersecurity programs with identified risk and vulnerability management approaches
- Direct collaboration with OT stakeholders
  - e.g., the engineers, operations, administrators, and leadership
- Previously gathered information
  - e.g., asset inventory, network diagrams, crown jewel analysis, vendor documents, and deployment guides
- Previous assessments
  - e.g., bench testing, attack surface enumeration, gap assessments, and risk mitigation decisions)

Key Tenets of ICS/OT Assessments



Spend Time Wisely


CVEs and ICS Vulnerabilities
More Difficult
Easier
Tools and Reports Available
Sharing of Vulnerabilities
No Tools and Reports Available
No Sharing of Vulnerabilities
O.S. CVEs
Design, Operate, Maintain Application Tools CVEs
HMI Code Vulnerabilities
Embedded Controller (PLC/PAC) Code Vulnerabilities
Mechanical System Vulnerabilities
"Distance to BANG!"
Requires More Steps in The Kill Chain
Direct Impact To Physical Systems
Direct Physical Affect


CVEs and ICS Vulnerabilities
More Difficult
Easier
Tools and Reports Available
Sharing of Vulnerabilities
No Tools and Reports Available
No Sharing of Vulnerabilities
Statistically, this is where the largest number of vulnerabilities exist
This is where vulnerabilities have the largest impact, and we don't track or publicly share this information (i.e., we have no data points).
Mechanical
ystem
erabilities
HN
Co
Vulnera
O.S. CVEs
Design, Operate, Maintain Application Tools CVEs
"Distance to BANG!"
Requires More Steps in The Kill Chain
Direct Impact To Physical Systems
Direct Physical Affect

Bench Testing vs Production Testing

Variations in Scope and Methodology

Bench Testing:

- Standalone devices or non-production applications and systems

Top-Down (Active) Testing:

- Objective-based active testing focused on access to ICS environments

Bottom-Up (Operations) Testing:

- Passive assessments focused on assessing the impact on mechanical operations

Types and Purpose of ICS/OT Bench Testing

- **Reduces risk to production by vetting data-gathering techniques in a controlled environment**
- Establishes a device's attack surface baseline prior to production deployment
- Validates vendor security claims against real-world implementation
- Informs configuration, hardening, and monitoring requirements

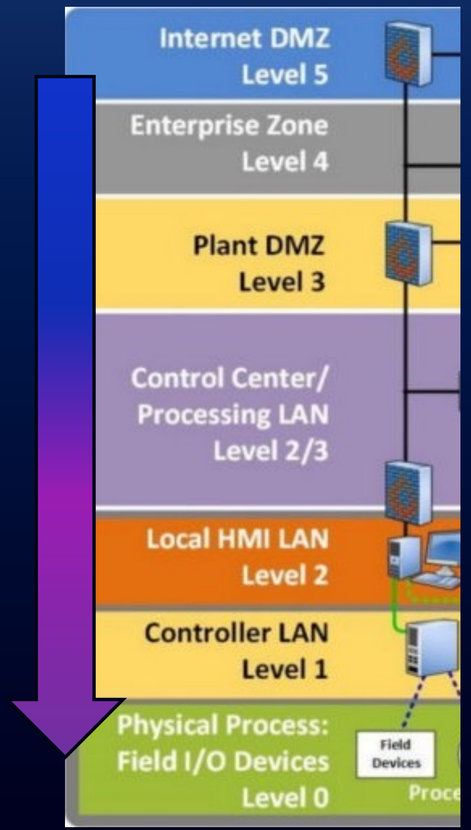
Key Characteristics of ICS Penetration Testing

- **Blend of traditional offensive assessment types**
  - Narrow scope, both in terms of assets and timeframe (pen testing)
  - Active interaction with systems and active exploitation of vulnerabilities (pen testing, red teaming)
  - Objective-based (red teaming)
  - Leverage known ICS adversary TTPs (adversary simulation)
  - Validate detection and response capabilities (purple teaming)
- **Unique test parameters**
  - Adversary- and process-centric ICS attack scenario development
    - Drives **value**
  - Assumed breach
    - Enhances **efficiency**
  - Full knowledge (open box/clear box) information sharing
    - Ensures **safety** and enhances **efficiency**

Top-Down (Active) Assessment

- **Assessment focus**
  - ICS Cyber Kill Chain Stage 1 activities
- **Objectives**
  - Use adversary TTPs to gain access to ICS systems and information necessary to execute an ICS attack
- **Drivers**
  - Often driven by the needs of enterprise/IT security or risk management teams
- **Scope**
  - Higher levels of the Purdue Model (L4 → L3)
  - Traditional IT technologies, more homogenous environments
- **Approach**
  - Active testing and vulnerability exploitation

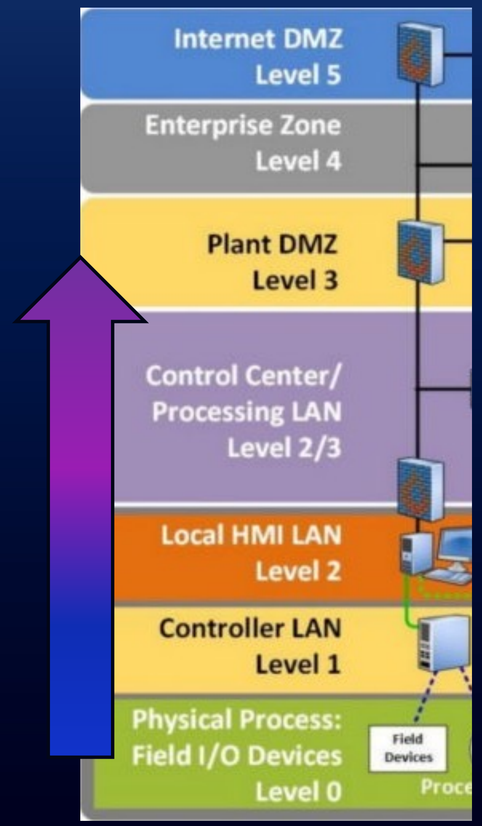
Prove it!



Bottom-Up (Operations) Assessment

- **Assessment focus**
  - ICS Cyber Kill Chain Stage 2 activities
- **Primary objective**
  - Leverage information gained during Top-Down testing to develop realistic ICS attack scenarios that impact physical processes and systems
- **Driver**
  - Knowledge and perspective of those operating and maintaining the target systems
- **Scope**
  - Lower levels of the Purdue Model (L2 > L0)
  - Unique, heterogenous ICS environments
- **Approach**
  - Passive enumeration
  - Collaborative dialogue about attack scenarios and consequences
  - Active demonstration only in safe, controlled environments

Nothing interesting ever happens in an office …



Scope Flexibility

- **Scope best effort prior to on-site**
  - Lean on risk-based target selection and the on-site activity plan.
  - Prepare for flexibility.
- **Time-bound on-site activities.**
- **Key on-site considerations**
  - Personnel availability and approval.
  - Physical system weaknesses and vulnerabilities.
  - Impact identification and consequence-driven hypothetical attack scenarios.
  - Measurement against prevention, detection, response, and recovery.
- **Operations assessments are exploratory by nature, guided through collaboration with local on-site personnel.**

"Where do we start?"

"How do we scale out?"

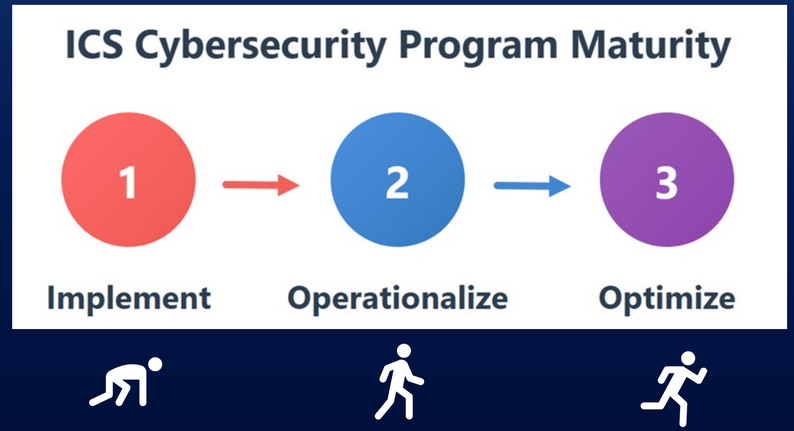
Proceed with Care

Four Principles of Process Assessments

- **Safety, resiliency, and reliability**
  - Tightly coordinated activities with operations staff
  - Clear understanding of specific devices and communications that can disrupt or influence
- **Minimal and contained network communications**
  - Requires visiting the sub-system under escort
  - Introduce little to no traffic to environment
  - Careful interactions with systems and devices
- **Actions and decisions of people**
  - Understand staffing and personal resources
  - Align with factual physical impacts and consequences
- **Passive to active**
  - Mostly passive in discovery, may lead to active (likely lab) for validation

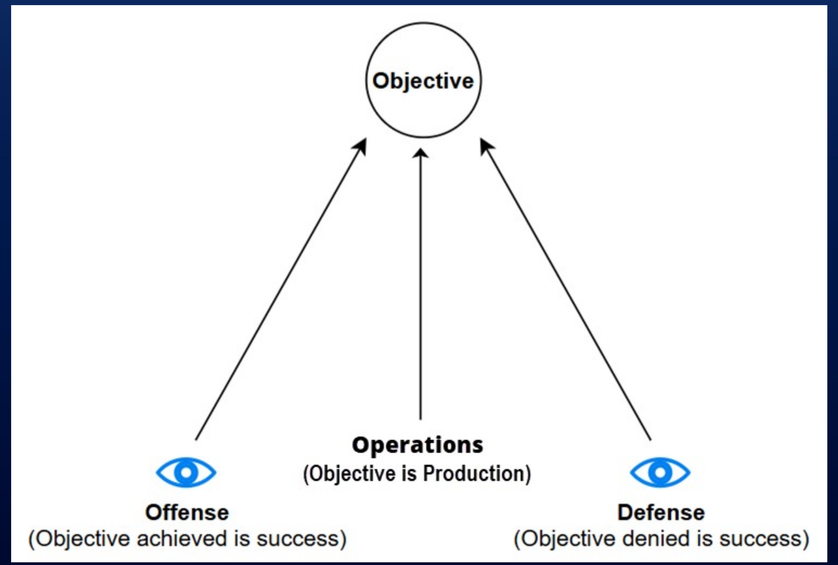
Define Desired Outcomes

- **Asset owner maturity**
  - Where are they currently?
  - Where do they want to be?
- **Assessment drivers**
  - Regulation
    - Support regulatory obligation
  - Security program
    - Validate of specific security controls
  - Threat emulation
    - Assess specific threat group techniques
- **Useful questions**
  - Does this engagement support a particular internal effort?
  - Is it required for regulatory compliance?
  - Is there an opportunity to solve a strategic problem or get leadership buy-in for a program?
- **Understanding desired outcomes helps define goals and objectives.**



Parallax View (Defense in Depth Perception)

- **Objectives**
  - Pivot from IT to OT
  - Impact process control
  - *May or may not be accomplished*
- **Goals**
  - Identify weaknesses
  - Identify strengths
  - Identify mitigations
  - Validate detection and response
  - *Can always be accomplished regardless if objectives are achieved*



Significant Actions

- **A significant action**
  - Contributes to a **state change** in the customer environment (adding/deleting files, changing configurations, etc.)
  - Contributes to **progress** toward the engagement objectives
  - **Was or should be seen** by the endpoint or network detection and response solutions
- **All significant actions should be documented to support:**
  - Efficient, accurate, and valuable reporting
  - Detection and response validation
  - Evidence in the case of an outage or incident
  - Leaving the environment in the same condition you found it

Beyond Computer and Networking Systems

- Industrial Control Systems (ICS) are engineered components brought together to control complex physical equipment and processes.
- Items under consideration in your assessment should include:
  - Instrumentation and sensors
  - PLCs, DCS CPUs, Remote Terminal Units (RTUs)
  - Fieldbus devices
  - The security features of ICS/DCS/SCADA-related software tools
- ICS assessments should also have a focus on mechanical systems to determine the effect of a targeted attack.

Operations Assessment Steps

Discover vulnerabilities and weaknesses that have a clear path to cause direct impacts on a mechanical operation with the intent to prioritize defense improvements.

- **On-Site Planning**
  - Does the operations personnel understand and support our on-site activities?
- **Process Enumeration**
  - How do we enumerate, and what information can be gained?
- **ICS Attack Scenario Development**
  - How could an effective attack be successful on the target process?
- **ICS Attack Scenario Methods**
  - What attack methods and vectors exist that could lead to such an attack?
- **ICS Attack Scenario Execution**
  - If an attack occurred, how prepared is operations?
- **ICS Attack Scenario Defense**
  - What defenses could help mitigate, minimize impact, or improve recovery?

Mitigations: Limitations

- **Architecture**
  - Validated systems
    - Vendor and engineered
  - Network equipment
  - Manual control
- **Visibility**
  - Management of Change
  - Network visibility
  - Triage and incident response plans
  - Training and tabletop exercises
- **Recovery**
  - Coverage, accuracy, and validation

Associated Findings

- ABB System is a validated architecture; user changes unsupported
- Rockwell/Drive systems validated by System Integrator; user or integrator changes supported
- No network security monitoring
- No formal change control

Strategic vs. Tactical Mitigations

- **Tactical mitigations**
  - Config changes
  - New controls
  - Existing controls
  - Shorter-term efforts (e.g., 3 months–1 year)
- **Strategic mitigations**
  - Architectural
  - Monitoring
  - Programs & Policies
  - Audit
  - Longer-term efforts (e.g., 1–5 years)
- **Considerations**
  - How do recommended mitigations help an asset owner move forward on their cybersecurity maturity journey?
  - How can mitigations be prioritized for greatest effect?

THANK YOU