Project 7: Remote Access

"Name of Presenter"

Presenter

Enter details about the presenter here.
More details about the presenter.

The LOGIIC Model of Government and Industry Partnership

Linking the Oil and Gas Industry to Improve Cyber Security

Project 7: Remote Access

Background

Assessment Approach

Assessment Findings

Conclusion

Remote Access

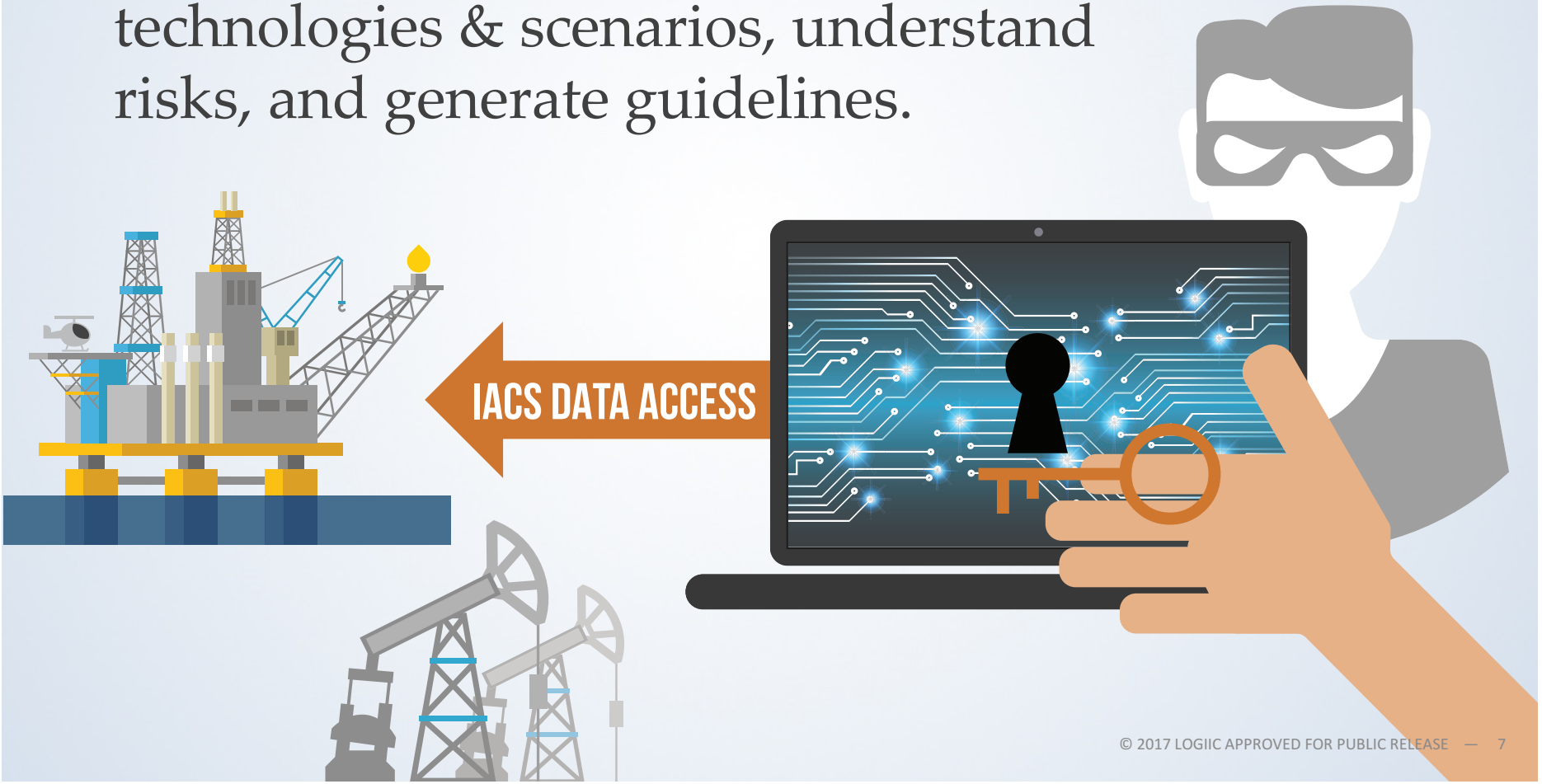
Background

Overview

- Focused on evaluating technologies that allow remote monitoring of, and access to, equipment in the IACS environment
- Evaluated different remote access technologies
- Conducted assessments in an IACS laboratory
- Findings were published in a report

Objective

Evaluate currently available remote access technologies & scenarios, understand risks, and generate guidelines.



Background

- Historically, remote access from the IACS network has been restricted or limited
- Business demand increases the need for connectivity and information flow
- Remote access creates fundamental changes in the threat landscape

Additional Project Benefits

- Assist LOGIIC members with short-term risk mitigations for remote access solutions already implemented
- Assist vendors in improving solutions
- Help develop best practices for implementing remote access

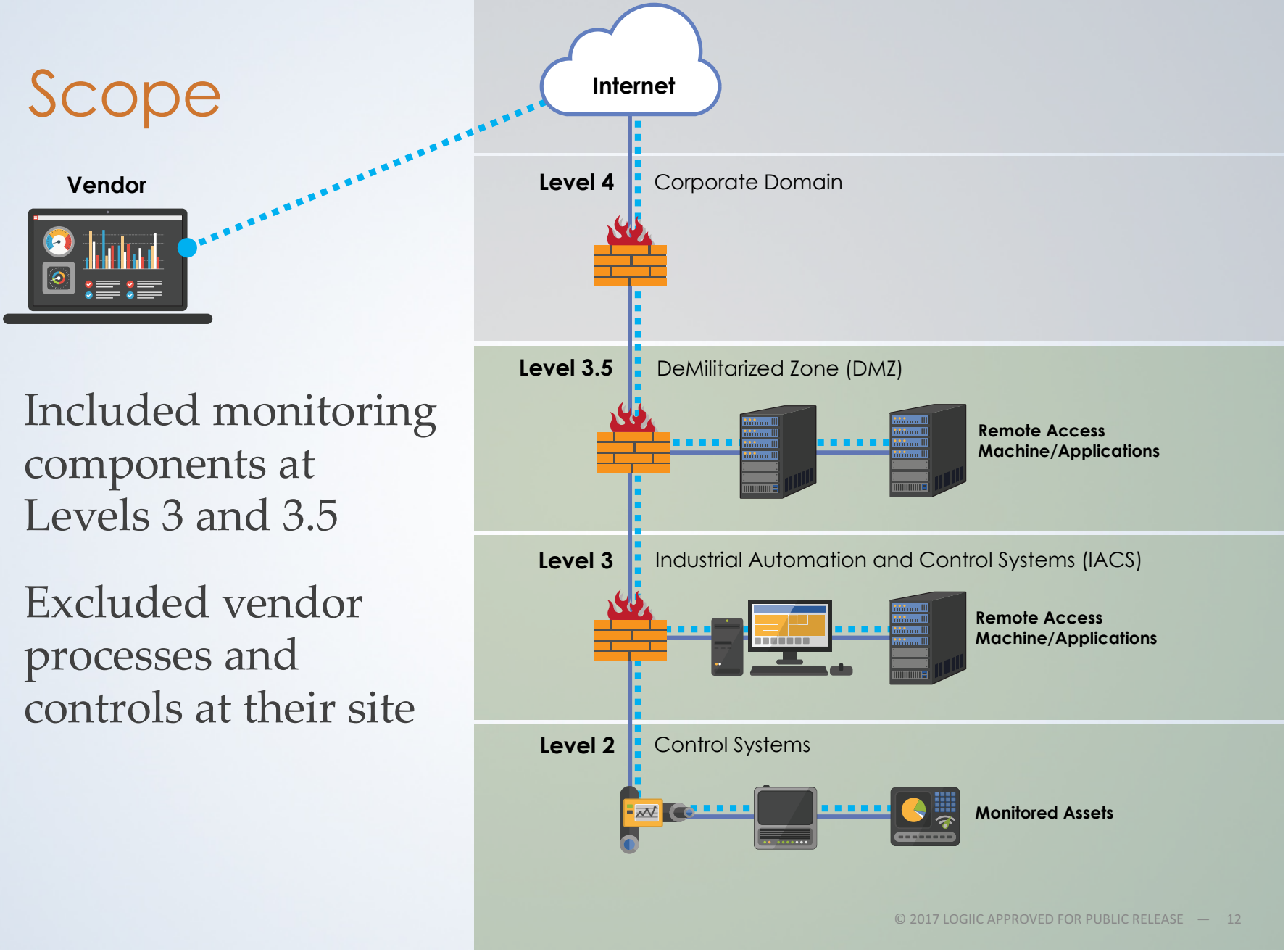
Survey

Executive Committee Members
August 2013

- Findings show that remote access was already in use among members, with limitations based on security
- Many planned to expand (with caution)

- Members wanted to understand vendor offerings, methods of securing, and overall security exposure
- Members sought confidence and clarity in the remote access design and implementation

Scope

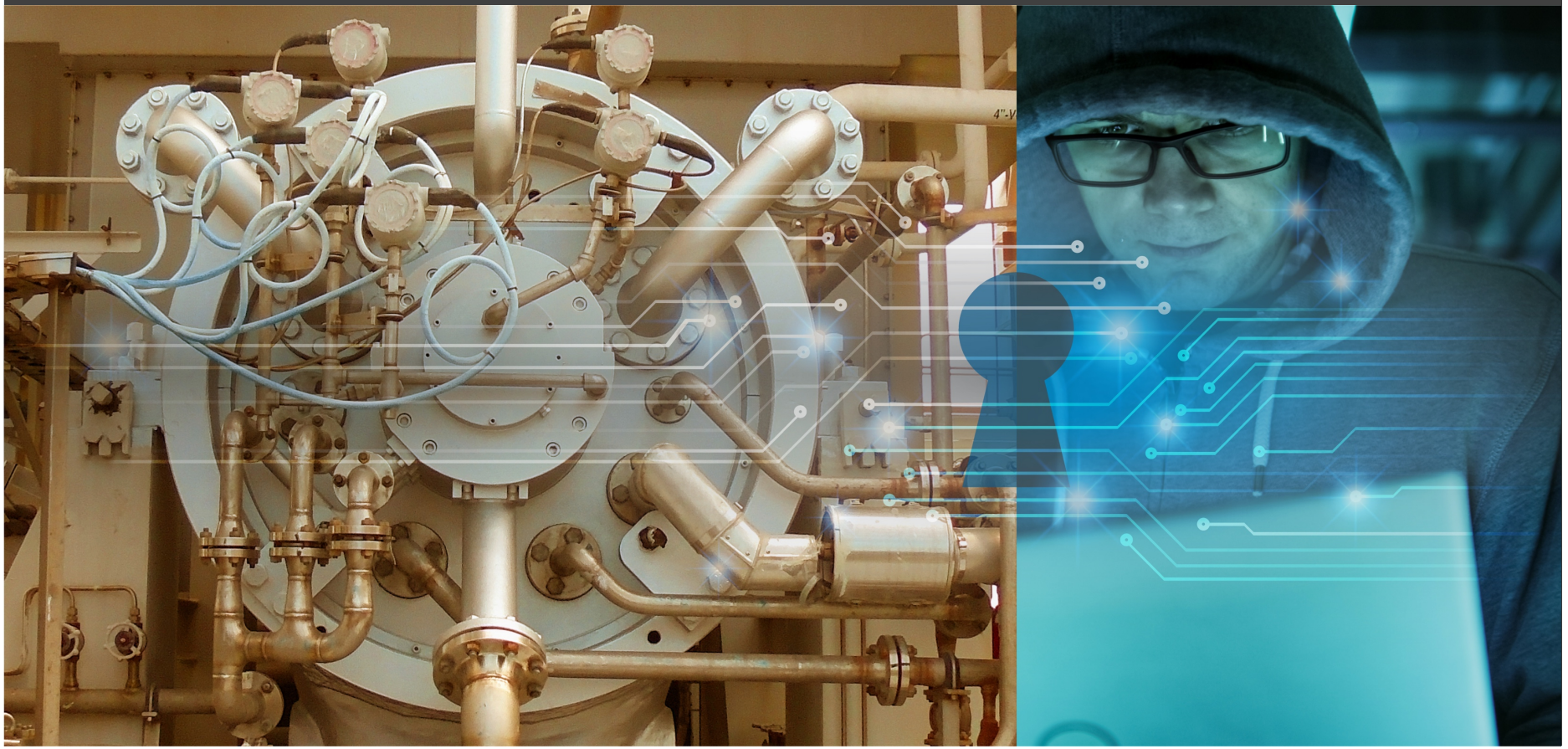


Included monitoring components at Levels 3 and 3.5

Excluded vendor processes and controls at their site

Remote Access

Assessment Approach



Methodology

Risk = Threat x Vulnerability x Consequence

Approach

Vendors + Scenarios + Rules = Plan

Onsite Assessment

- Configuration Review
- Execution of Test Scenarios
- Observations
- Analysis and Conclusions

Test Vectors

- Design and Configuration
- Remote Access Server
- Remote Access Clients

- Remote Communication Gateways
- Data Collection Systems
- PLC Access

- Firewalls and Network Security Devices
- Data in Transit (i.e., IPSEC)
- Tunneling Endpoints

Test Approach

Plausible threats

Reconnaissance

SME attack methods

Public and customized exploits and payloads

Test equipment

Analysis of Findings

Technical conclusions are based on SME findings including:

Raw Data from Test Scenarios

Severity ranked by SME

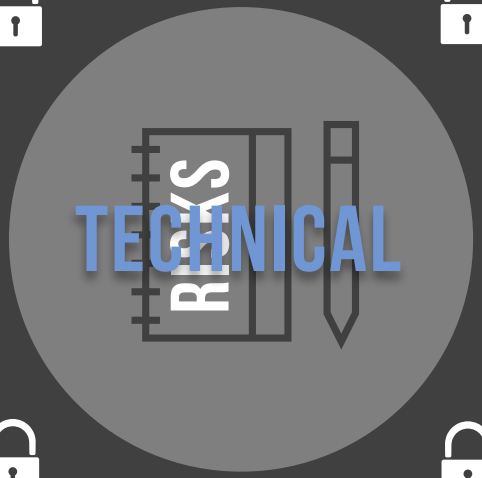
On-Site Observations

Remote Access

Assessment Findings

Recommended Implementations

Network Separation



Vendor Documentation

Network and System Security

Recommended Implementation

- Vendors often provide recommended design and architecture
- Asset owners should follow vendor recommendations or carefully assess the risks to alternative designs

- Customized solutions may not offer the same level of security
- Location of servers and clients within different network levels significantly changes the security of a solution

- Some vendors use an informal implementation and design model that should be formalized and documented
- Use of a recommended architecture means effective use of the security controls built into the design

Example: placement of client and server in the DMZ rather than business network or core IACS network

Vendor Documentation

- Design recommendations, patching guidelines, and maintenance procedures can be extremely helpful for ongoing security
- Documentation varied from minimal to comprehensive

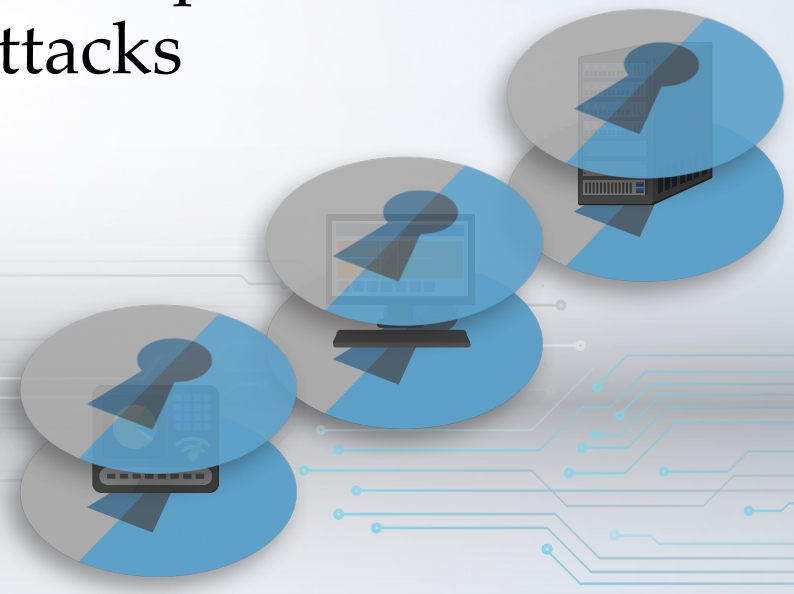
- Comprehensive vendor documentation included clearly defined roles, responsibilities, and maintenance procedures

Network Separation and Layering

- In a remote monitoring architecture, implementing network separation and layering is extremely important for a secure network

- This approach isolates critical components and assigns protections accordingly
- Protects against outsider and insider threats
- Layers should be formed around end devices under monitoring, data collection points, servers, and clients

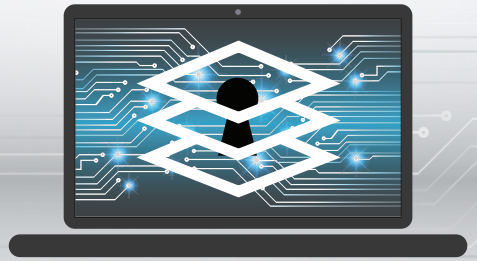
- End devices are then protected behind several layers of security
- This approach protects end devices that may not be robust or capable of device-level protection, and may be susceptible to vulnerabilities or DoS attacks



- Vendors employ various mechanisms to protect the server
- Basic separation through the use of firewalls is common and can be effective
- Proper network isolation includes port lockdown

- Traffic that crosses network segments should be unidirectional
- Bidirectional communication may be necessary when initiated from another location (common)
- Asset owner's policies may restrict inbound traffic into a DMZ or the core IACS network

- Controls can assist in layered protection:
  - Secure VPN
  - IP-based restrictions
  - Use of IPSEC



Network and System Security

- Define prior to implementation
- Discuss with vendor
- Establish with maximum protections in place

- Protect against insider and outsider threats
  - Access control
  - Layered security
- Protect against unauthorized privilege escalation
  - Role-based, read/write access control
  - Principle of least privilege

- System/application accounts lockdown
  - Maintain least privilege
  - Obfuscate stored passwords

- Systems lockdown
  - Disable vulnerable services (Telnet, FTP, VNC)
  - Limit ports
  - Disable residual and unneeded services

- Larger attack surface lockdown (DCOM, SQL)
  - Vendor-accredited patches
  - Current updates
  - OS patches

- Firewall restrictions
  - Limiting traffic to SSH, HTTPS, and RDP
  - Limiting traffic to read-only requests
  - Application-level filtering

- Design considerations discussed between asset owner and vendor prior to implementation:
  - Mitigation for end-device vulnerabilities
  - Implementing a firewall
  - Layering protections
  - Application-level protections
  - Firmware and hardware vulnerability testing

- VPN and two-factor authentication where possible
- Secure methods of handling pre-shared keys
- If RDP is used, avoid publishing an entire remote desktop

Remote Access

Conclusion

Remote Access Takeaways

CONTROL
Ensure that recommended controls are applied

IMPLEMENT
Follow vendor implementation model if available

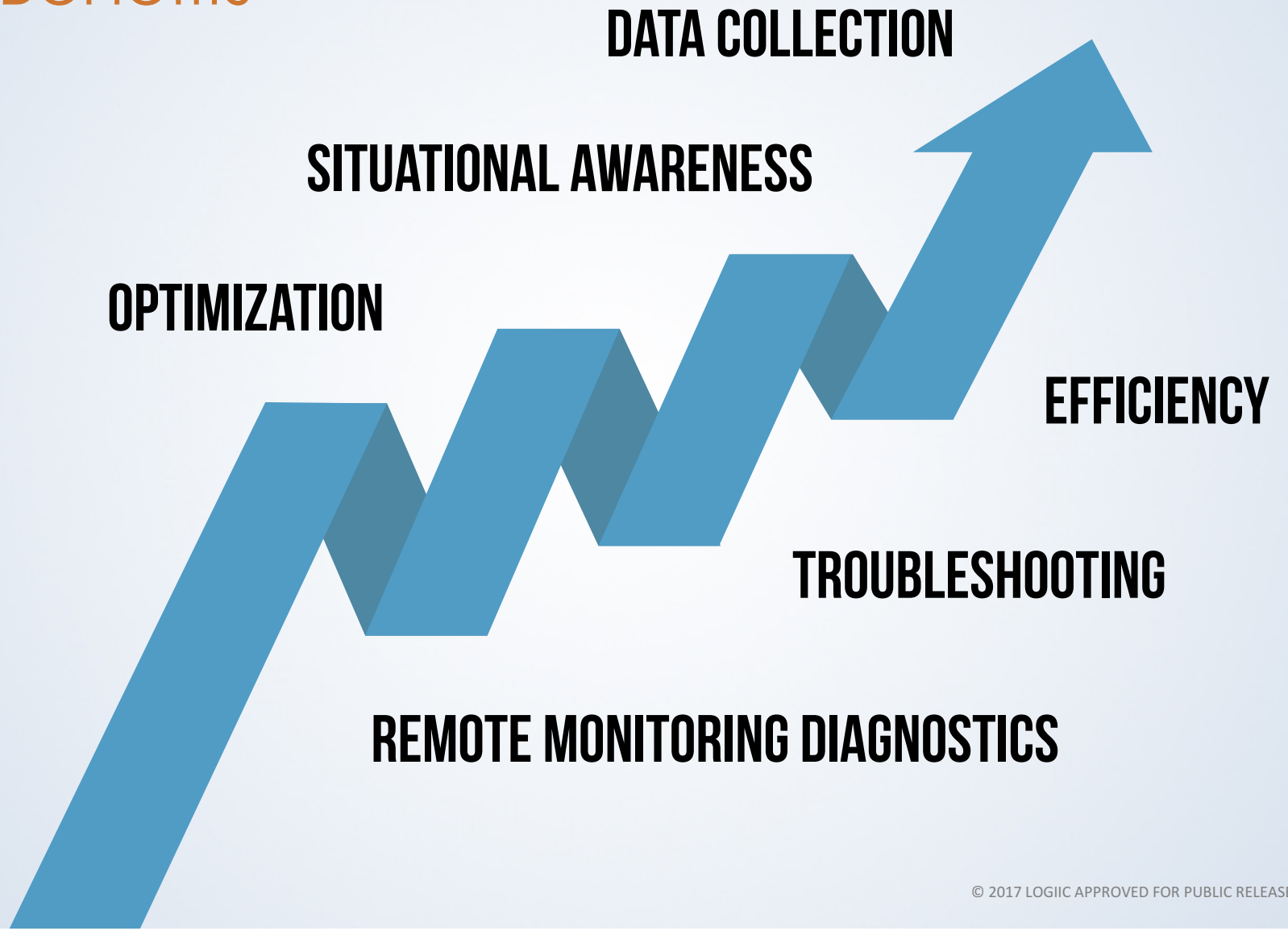
MAINTAIN
Follow vendor maintenance documentation if available

PROTECT
Protect against insider and outsider threats

SECURE
Access control, strong system passwords, and application passwords

UPDATE
Maintain patches and updates for continued protection

Benefits



Five Key Considerations

Careful Design and Implementation

- Access must be focused on authorized systems
- Core IACS assets must remain protected

Important Vendor Documentation

- Planning
- Design and scoping
- Implementation
- Maintenance

The importance of vendor's recommended architecture is significant

Patching and Maintenance

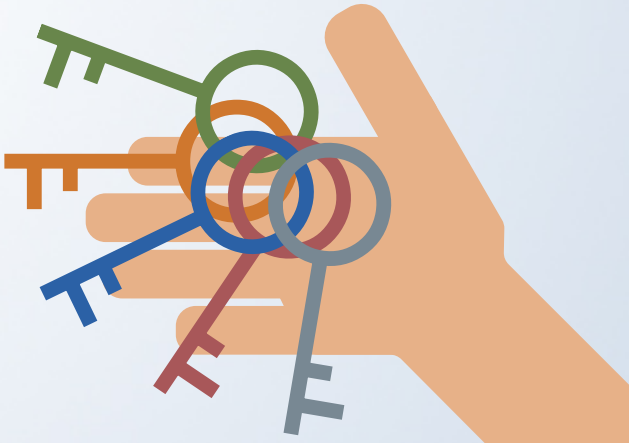
- Establish a long-term patch management process defined with the vendor
- Maintain critical patches on all components
- Clear path for patch delivery and installation
- Lack of patching can create significant risks

Network Design

- Layered network security
- Multiple controls between critical assets and a potential adversary (insider or outsider)
- End devices often have limited capability for inherent security
- Separation of the solution from other parts of the network

Security at all Locations

- System and network security at both asset owner and vendor sites
- Security should be defined prior to implementation
- Reduce attack surface at all locations
  - Review needs, maintain patches and updates

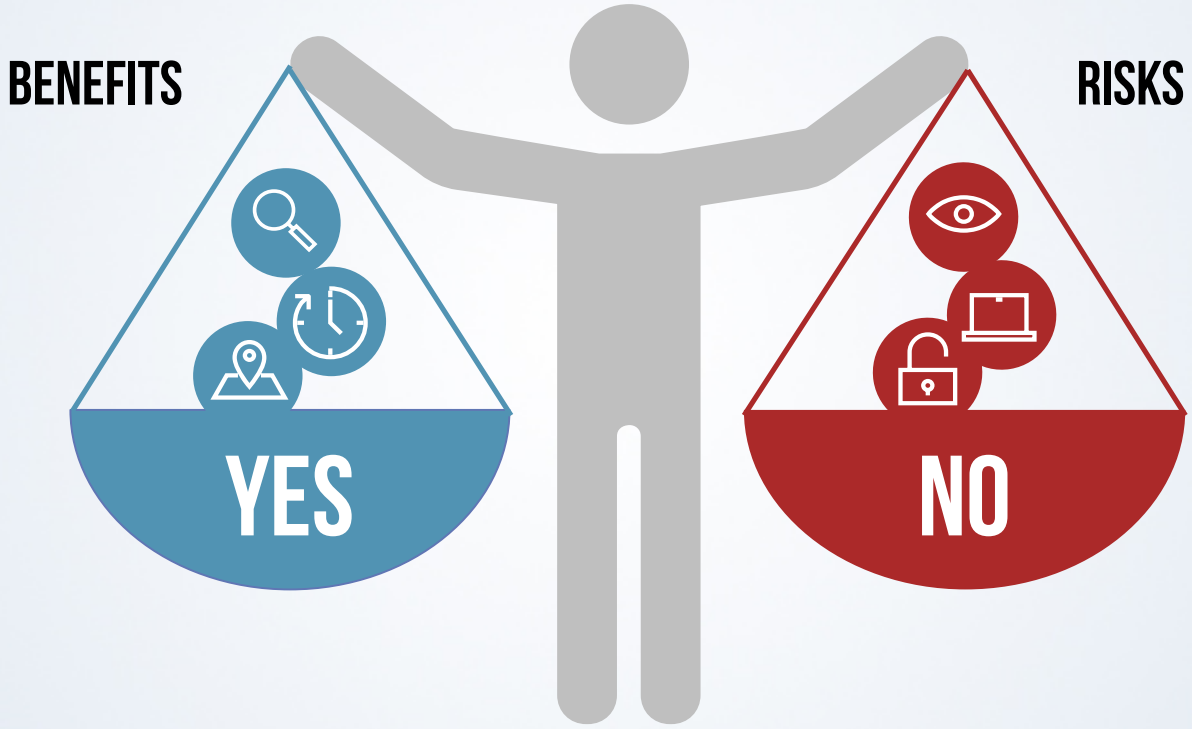


Conclusions

Remote Access Solutions

- Provide value to the asset owner and increase efficiency
- Are becoming more common as interconnectivity and desire for optimization increases

All benefits of using remote access should be balanced with risks inherent to the technology



Design and implementation requires

- Network and system configuration
- Maintenance
- Access control
- Defense-in-depth
- Owner and vendor collaboration

Implementing Remote Access
in the IACS environment
can be done securely
if benefits are balanced
with technology risks
and design/implementation
requirements are followed.