Project 9:
Real Time Data Transfer

"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 9: Real Time Data Transfer

Background

Assessment Approach

Assessment Findings

Conclusion

Real Time Data Transfer (RTDT)

Background

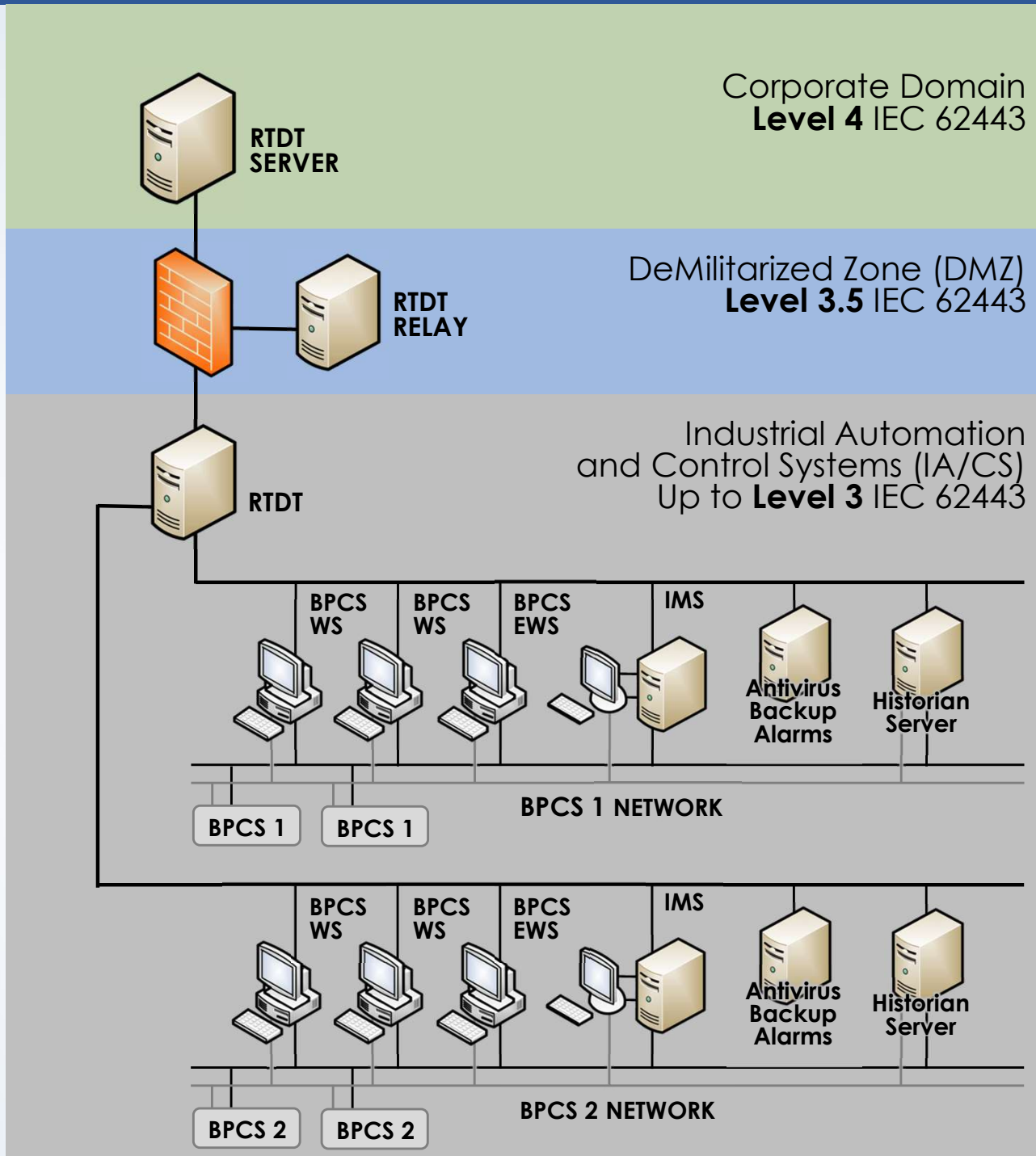
Overview

- Focused on assessment and analysis
- Solutions provide data sets that support decisions
- Evaluated different RTDT technologies
- Conducted assessments in an IACS laboratory
- Findings were published in a report

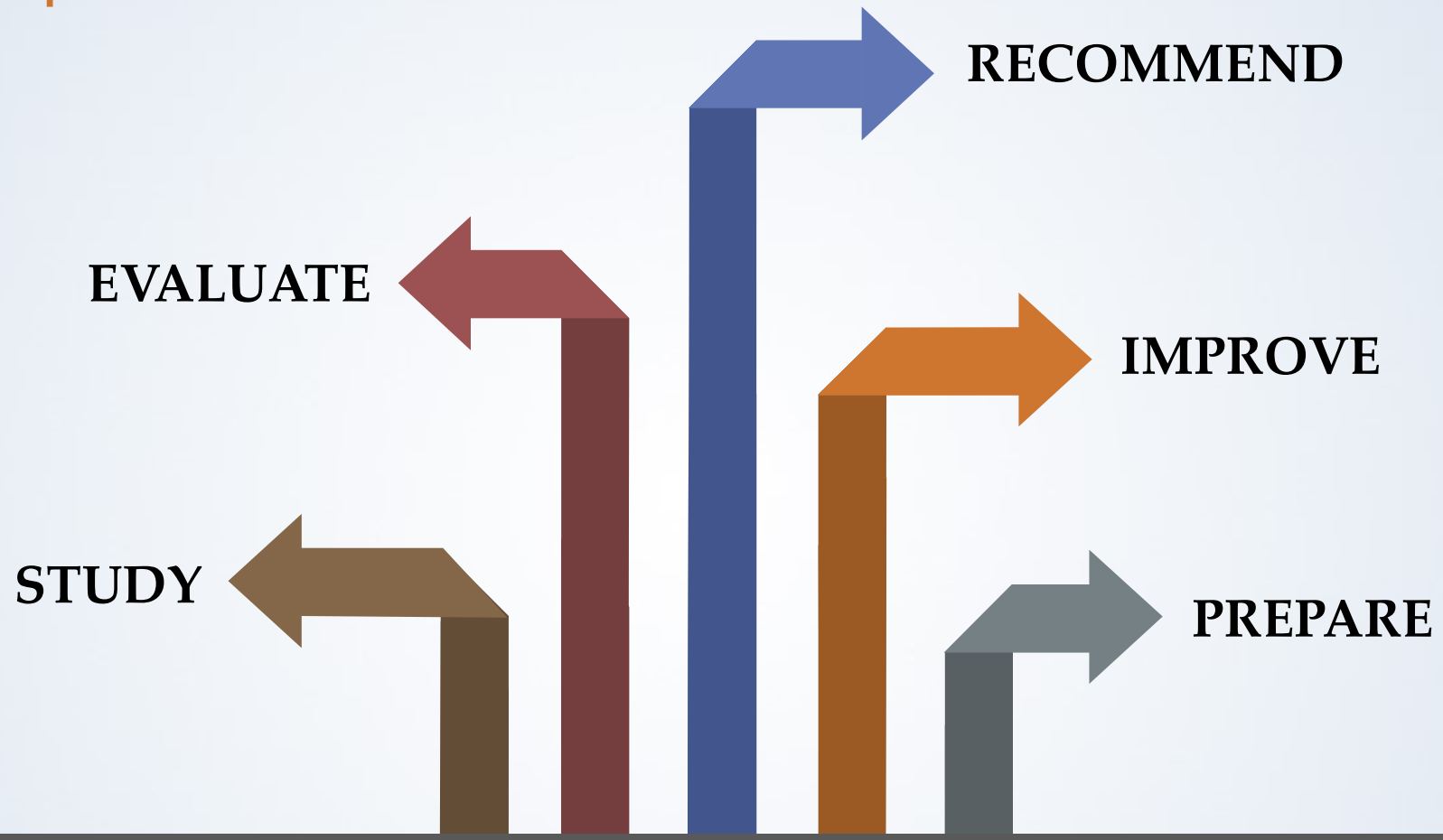
Objective

Evaluate Solutions Presently Available

Reference Architecture



Purpose



PROVIDE FOUNDATIONS

Surveys

- Identified available vendor technologies
- Surveyed Executive Committee members
- Used to define scope, use cases, and test scenarios

Real Time Data Transfer (RTDT)

Assessment Approach

Methodology

Risk = Threat x Vulnerability x Consequence

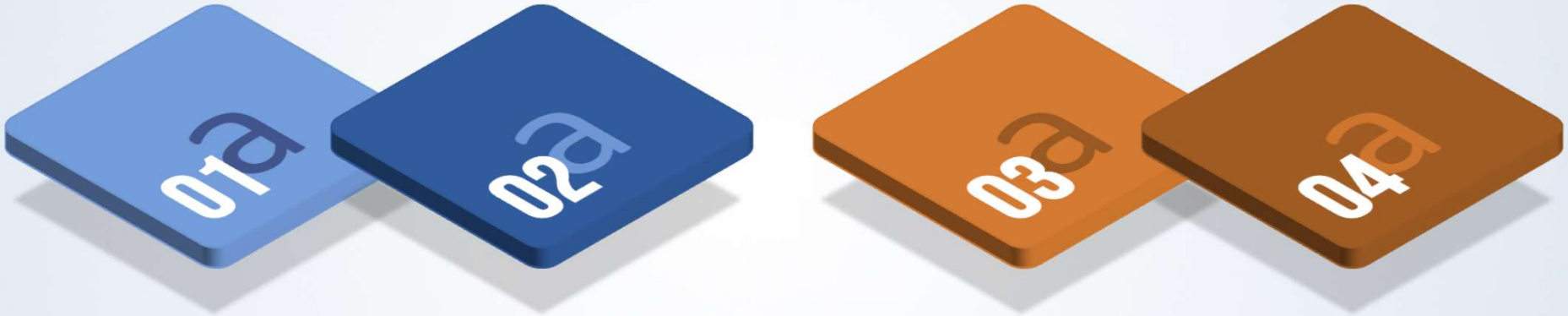
Onsite Assessment

- Reconnaissance
- Information Capture and Data Retrieval Attempts
- Targeted Attacks
- Denial of Service (DoS)

Vendor Approach

Automation Vendor Solutions

Third-Party Solutions

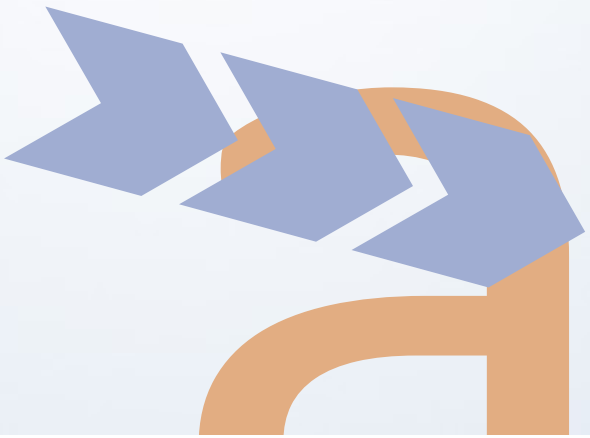


Each assessment conducted as an independent sub-project.

Test Approach

Insider and Outsider Threat Scenarios using SME Methods

- Public and customized exploits
- Custom payloads
- Specialized test equipment



Pre-work Phase

- Connection of test equipment
- Network validation
- Reconnaissance
- Traffic capture

Test Scenarios

01 Packet Captures

02 Configuration of Servers

03 Configuration of Firewalls

04 Network Access Control

05 Man-in-the-Middle

06 Data Packet Replay

07 Application Authentication

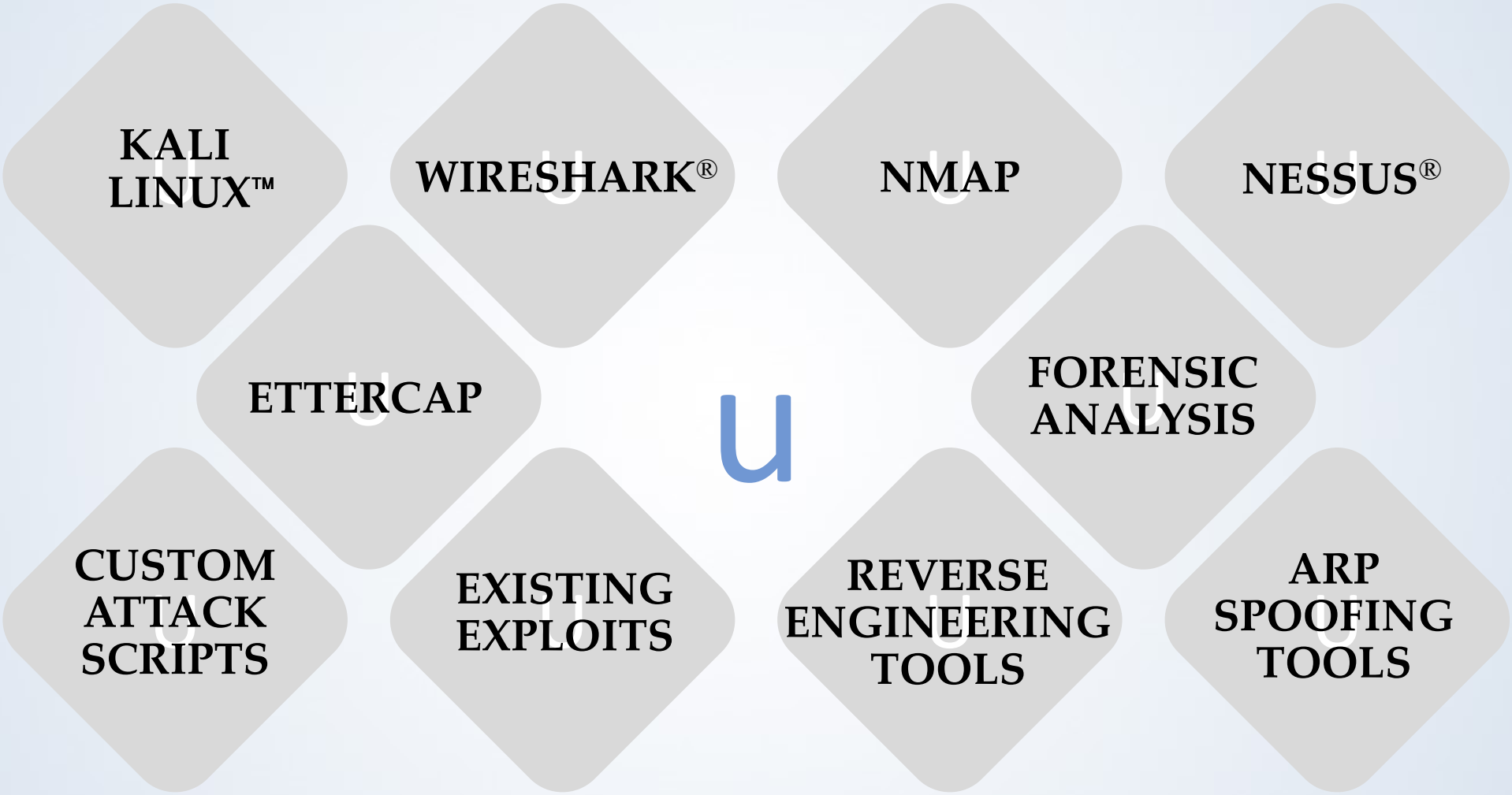
08 Denial of Service

09 Default Account Configuration

10 Audit Logs

11 Applicable Existing Exploits

Test Tools



Analysis of Findings

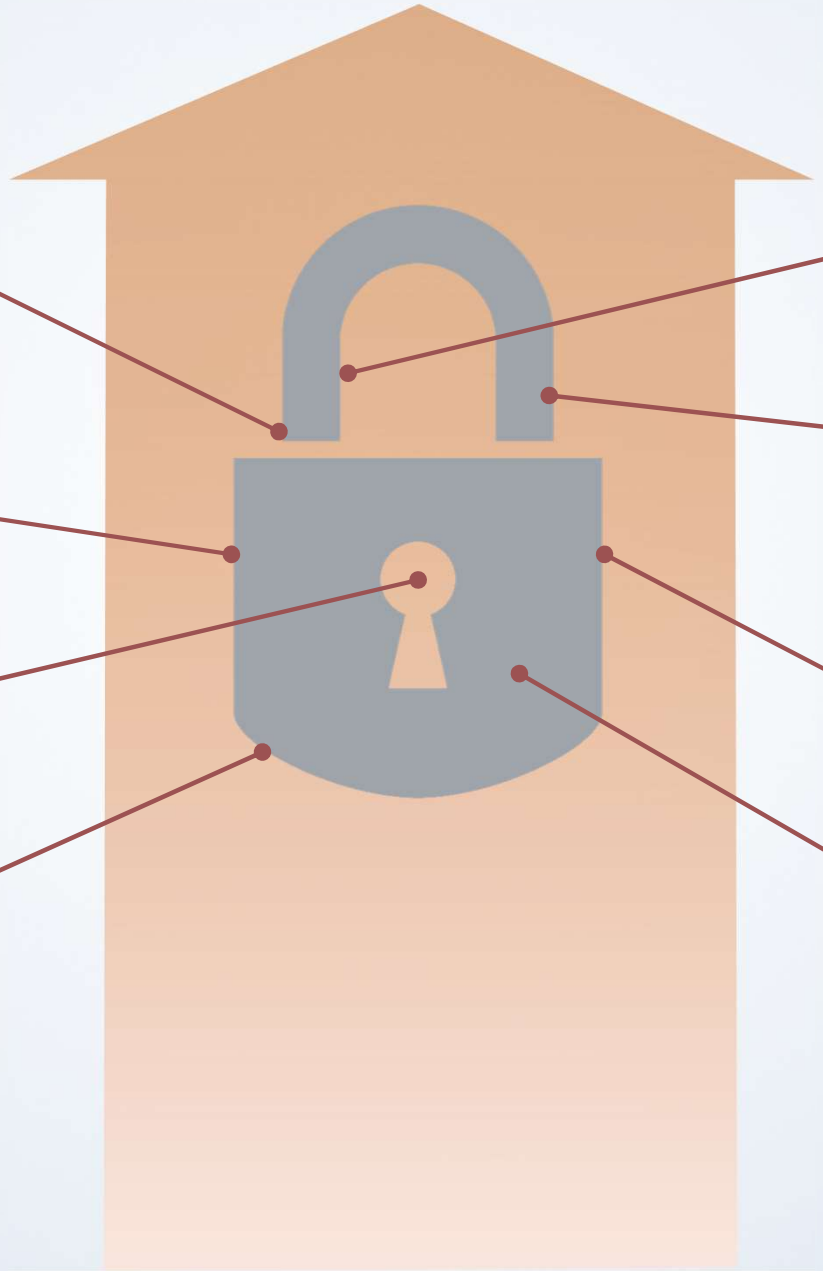
TECHNICAL	OPERATIONAL
Research	Usability
Documentation	Ease of Setup
Assessment Tests	Maintenance Requirements
Background Info	
Observations	Skillsets to Maintain and Use System
Functional Tests	

Real Time Data Transfer (RTDT)

Assessment Findings

Positive Security Attributes	Automation and Third-Party Vendors	Solution Footprint
Third-Party Technology within Automation Vendor Solutions	Networking Components	Encryption
Network and Packet Handling	Layered Security	Management and Maintenance

Positive Security Attributes



Correct Encryption Implementation

Packet Integrity and Privacy

Patching

Disabling Unnecessary Ports and Services

Securing Data at Rest

Log File Structure and Protection

Removal of Default Settings

Configuration of Network Devices

Automation and Third-Party Vendors

- **Automation Vendors** who offer full control systems alongside RTDT solutions
- **Third-Party Vendors** who specialize in the RTDT area and do not sell full control systems

Both vendor solutions use OPC UA, DA, and DCOM protocol standards

Automation Vendor Solutions

- Designed primarily to interface with a particular control system
- Larger footprint, more components, more configurability
- Typically more hardware and networking components
- Comprehensive “package” for asset owners
- Assured it will work with their control system

Third-Party Vendors

- Perform a single objective
- Significantly smaller and consisted only of software
- No networking hardware is included in the solution

Solution Footprint

THIRD-PARTY VENDORS	AUTOMATION VENDORS
Smaller footprint	Larger footprint
Smaller attack surface	Broader attack surface
Less threat vectors	Vendor maintenance ops
Requires protection from surrounding architecture	Accreditation is attractive, but not necessarily more secure

Third-Party Technology within Automation Vendor Solutions

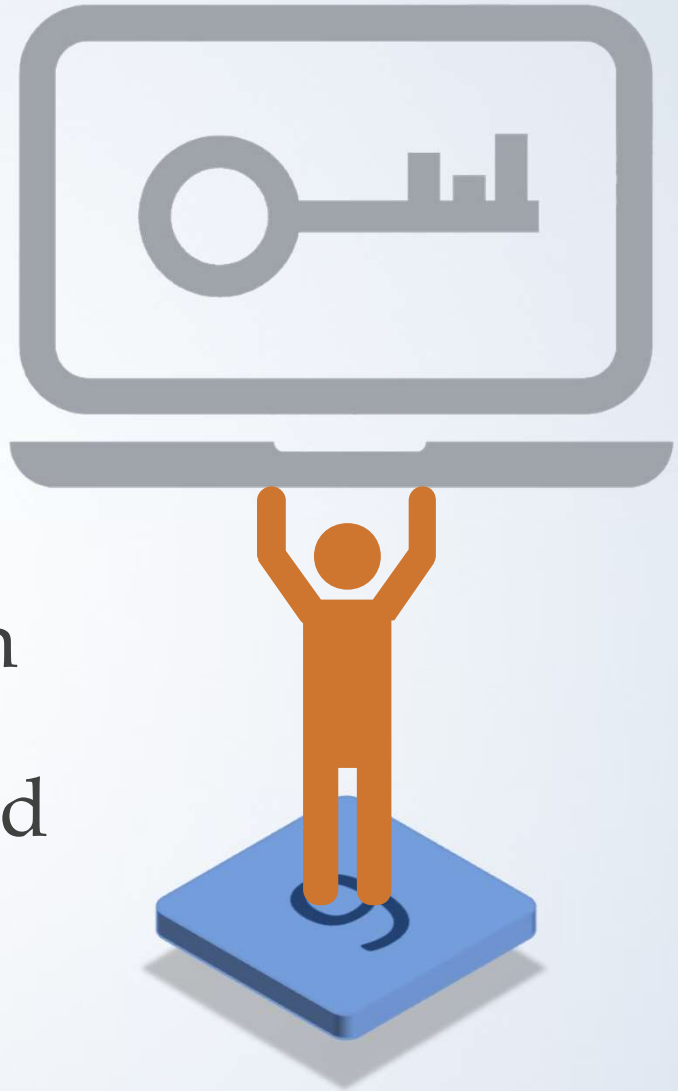
- Common
- Vulnerabilities may exist at various levels
- Unpatched third-party OPC components
- Components must be configured to recommendations made by the third-party vendor
- Asset owners need supply-chain assurance

Networking Components

- Often include networking hardware and firewall configuration
- Components did not always provide the required security or perform as anticipated
- Asset owner assurance
- Management and patch maintenance

Encryption

- When encryption is available, correct implementation is critical
- Significant assessment findings focus on encryption
- All solutions assessed offered some type of encryption



Encryption Algorithm

- Commensurate with industry best practices
- Vendors should clearly identify the algorithm in use
- Asset owners assumptions
- Assessments identified algorithm implementation discrepancies
- Independent validation and testing

Encryption Implementation

- Secure only when implemented correctly
- Key generation, handling, and storage details
- Hard-coded keys or confusion on how to change a key creates risks

Understanding When and Where Encryption Exists

Data Paths

Passwords

Server authentication

Data at Rest

Storage locations (optional)

Network and Packet Handling

- Firewalls and switches do not necessarily protect against MiTM attacks
- ARP spoofing may also be possible
- Packet integrity or privacy protected against MiTM attacks and data alteration
- Use of a true DMZ (as defined by industry guidelines)

Layered Security

Storage

- Commonly a SQL database
- Configured with access controls

Log Files

- Content and system information
- Access controls such as read-only restrictions

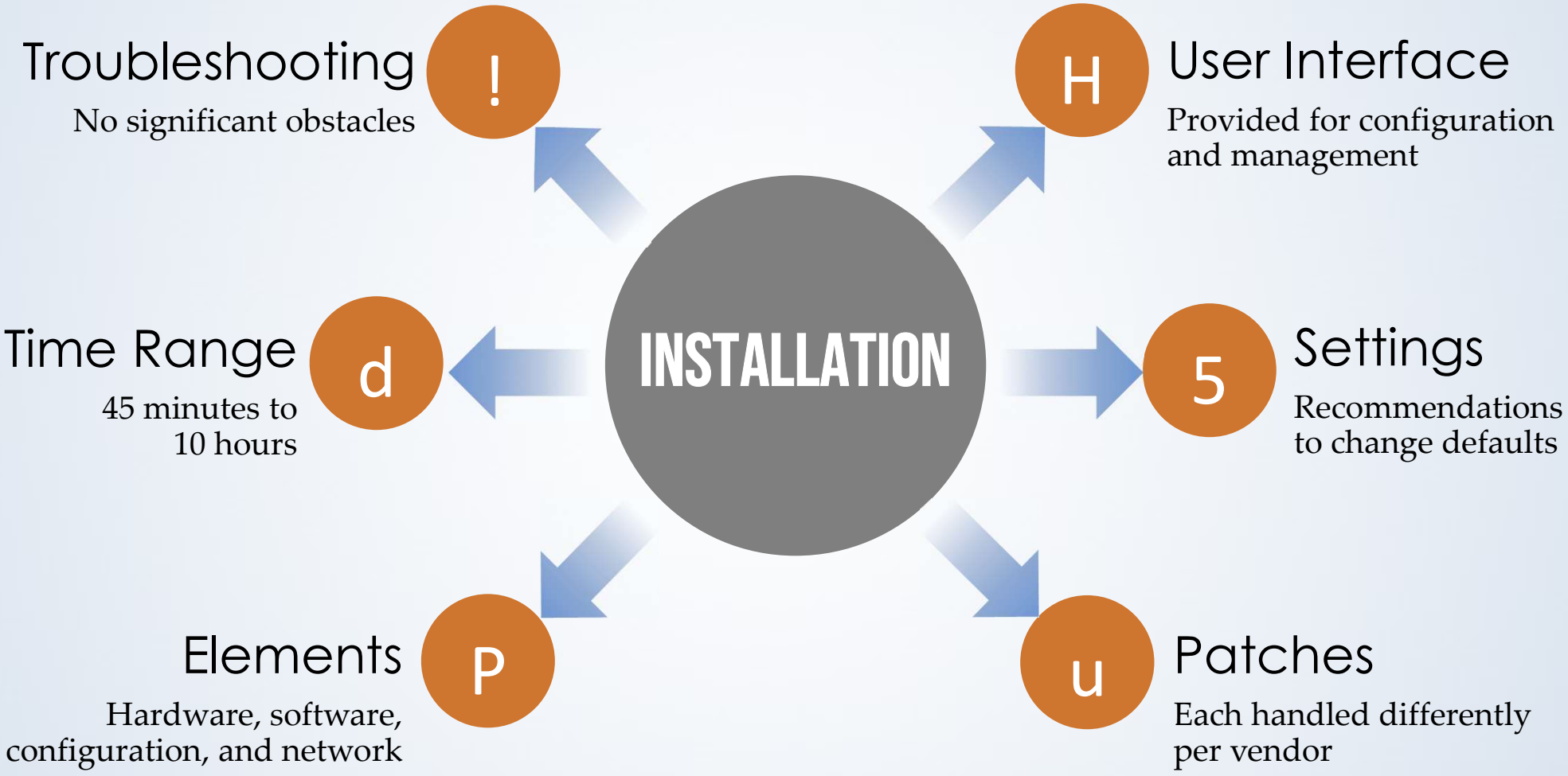
Default Settings

- Default accounts and passwords
- Permission levels
- Application settings
- Unnecessary ports and services disabled

Tag Security

- Configurable tag security
- Granular access controls
- Default settings

Management and Maintenance



Real Time Data Transfer (RTDT)

Conclusion

Solutions

- Functionality is effectively the same for automation and third-party vendors
- Varied in size, structure, and integration
- Automation vendor solutions typically include hardware, software, and networking components
- Third-party vendors typically provided software-only solutions

Technical Findings

- Larger footprints create an increased attack surface
- Solutions with third-party components require security at all layers
- Encryption to protect data in transit
  - Algorithm
  - Key generation
  - Key handling
  - Storage

Security

- Securing networking components is critical
- Configure user settings, tag security, application security
- Patching and updates are necessary
- A defense-in-depth approach within the design

Process

- Asset owners should work closely with vendors
- All technical details should be considered
- Operational considerations should be evaluated

It is possible to
securely transfer data
outside the core IACS environment
if all facets of the RTDT solution
have been secured and
a plan is established to maintain
the needed level of security
throughout the life-cycle.