Project 11: Safety Instrumented Systems

"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 11: Safety Instrumented Systems

Background

Assessment Approach

Assessment Findings

Conclusion

Safety Instrumented Systems (SIS)

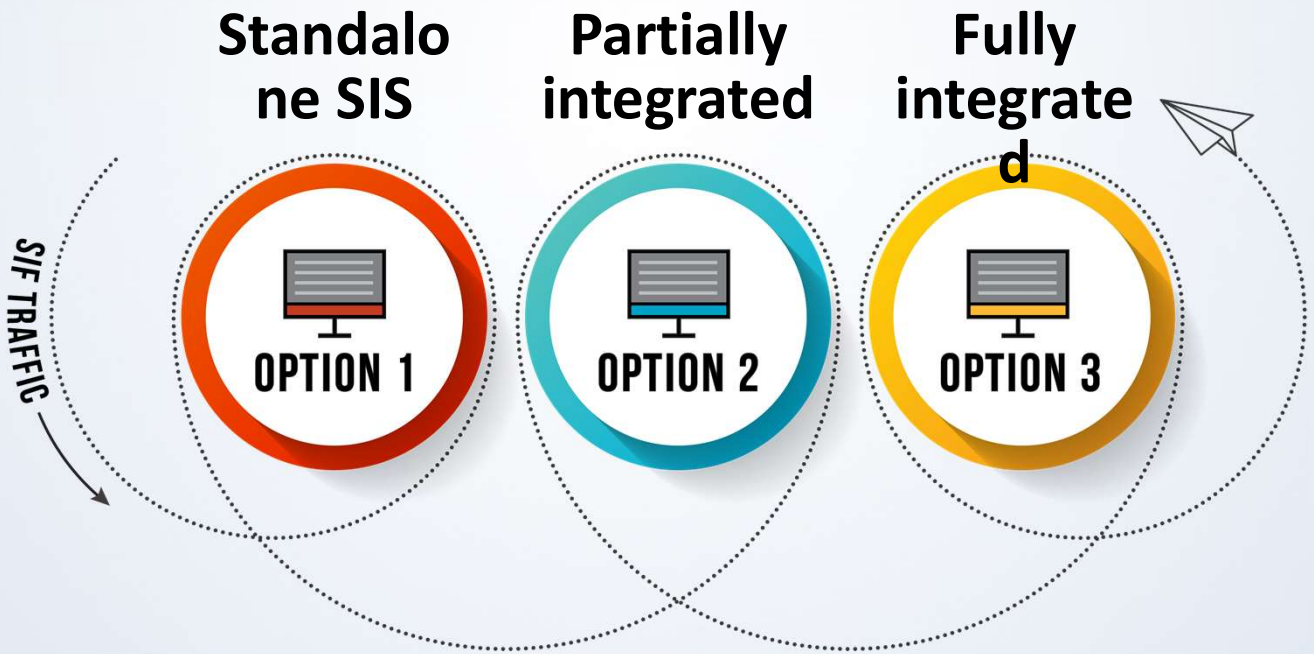
Background

Overview

- Focused on safety instrumented systems
- Built upon LOGIIC Project 2
  - Conducted nearly 10 years ago
  - Investigated the security of three SIS architecture designs
- Significant advancements and changes have occurred in SIS

Objective

Evaluate SIS solutions available in the market presently and develop conclusions about the security of specific architecture designs:



Scope

- Included an assessment of full SIS solution
- Sought to evaluate the security of current SIS designs
- Took into account previous research, findings, and international standards

Surveys

Executive Committee Members, July 2016

- Using SIS is valuable with concerns relating to integrity, availability
- Some upstream/downstream segments within same organization use different architectures
- All members are considering upgrading SIS solutions in the near future

Key Questions

Can a cyber security threat impact the…

- Safety Instrumented Function?
- Performance of SIS?
- By-pass mode?
- Instrumented Management Functionalities?

Key Questions

Can a cyber threat compromise the…

- Engineering function?
- Operational function of SIS?
- BPCS?

Can it provoke SIF spurious trips?

Architectures

- Like Project 2, Project 11 categorizes SIS architectures into three designs based upon interconnectivity.
- Since Project 2, SIS solutions have shifted toward integrated designs
- Industry standards have been developed that support securely integrating SIS and IACS

Integrated Architecture

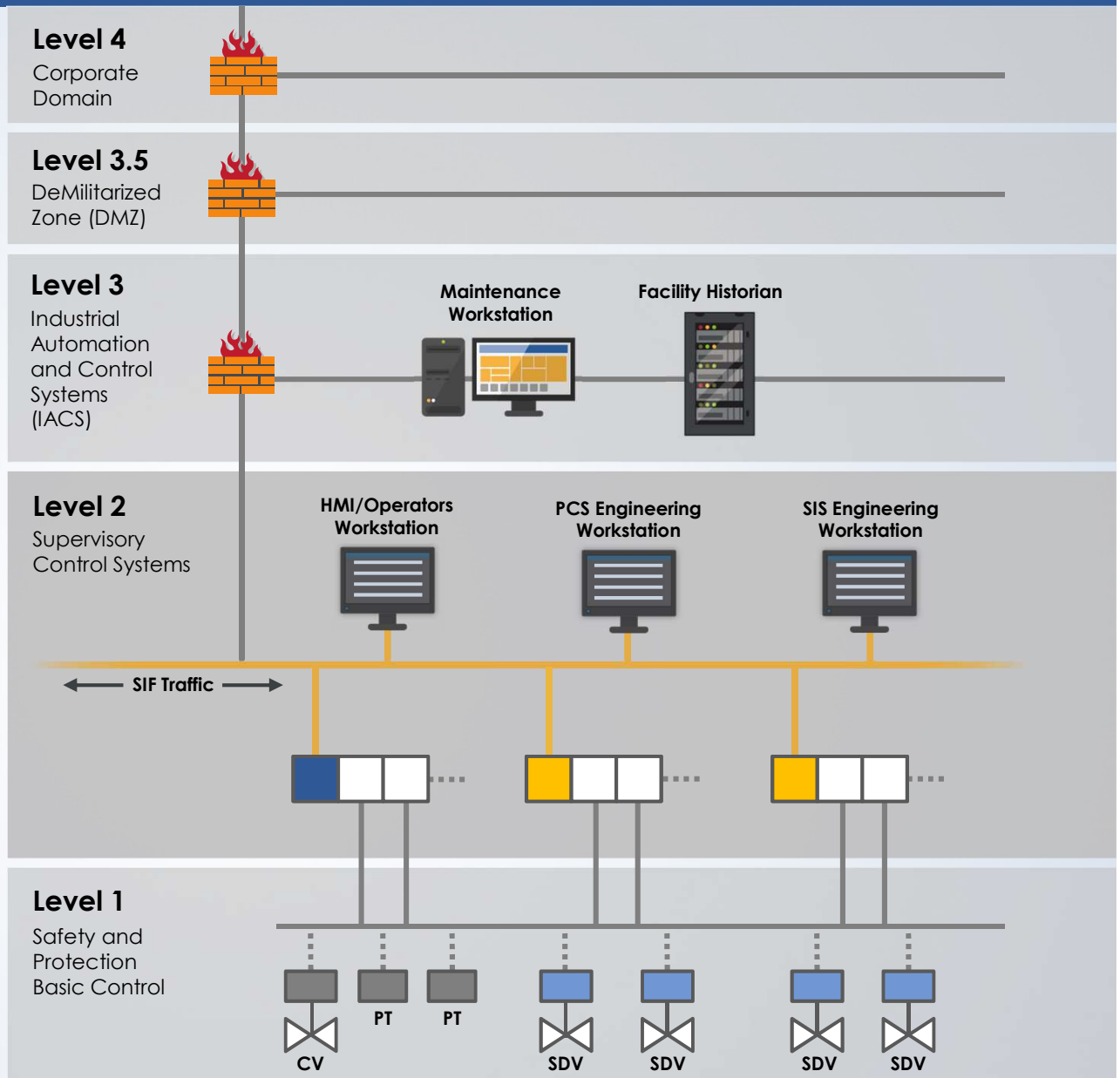
- Network Architecture
- Basic Process Controller
- Safety Logic Solver
- Remote I/O Module

ICSS Integrated Control & Safety System

PCS Process Control System

SIS Safety Instrumented System

SIF Safety Instrumented Function



Partially Integrated Architecture

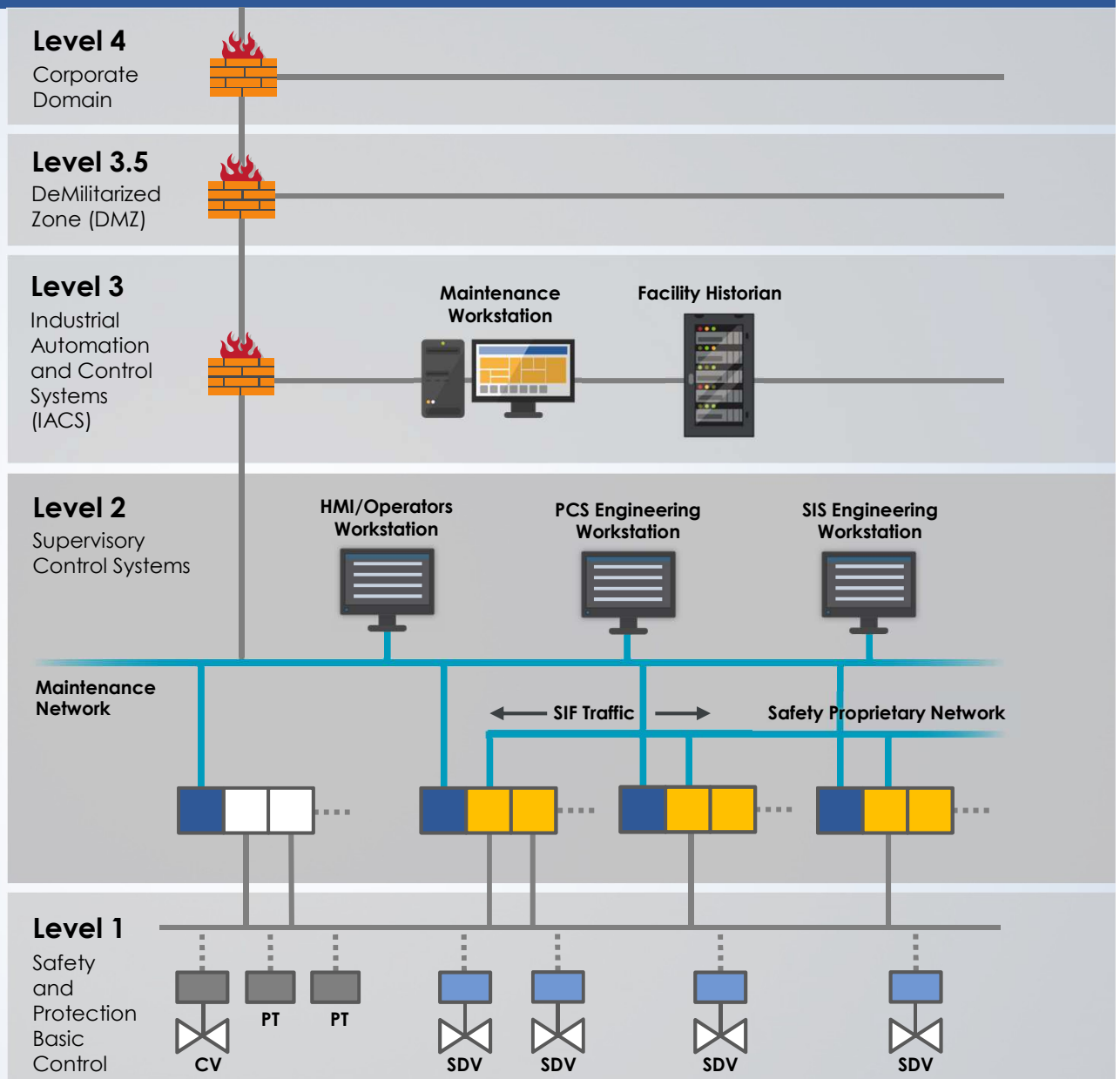
- Network Architecture
- Basic Process Controller
- Safety Logic Solver
- Remote I/O Module

ICSS Integrated Control & Safety System

PCS Process Control System

SIS Safety Instrumented System

SIF Safety Instrumented Function



Standalone Architecture

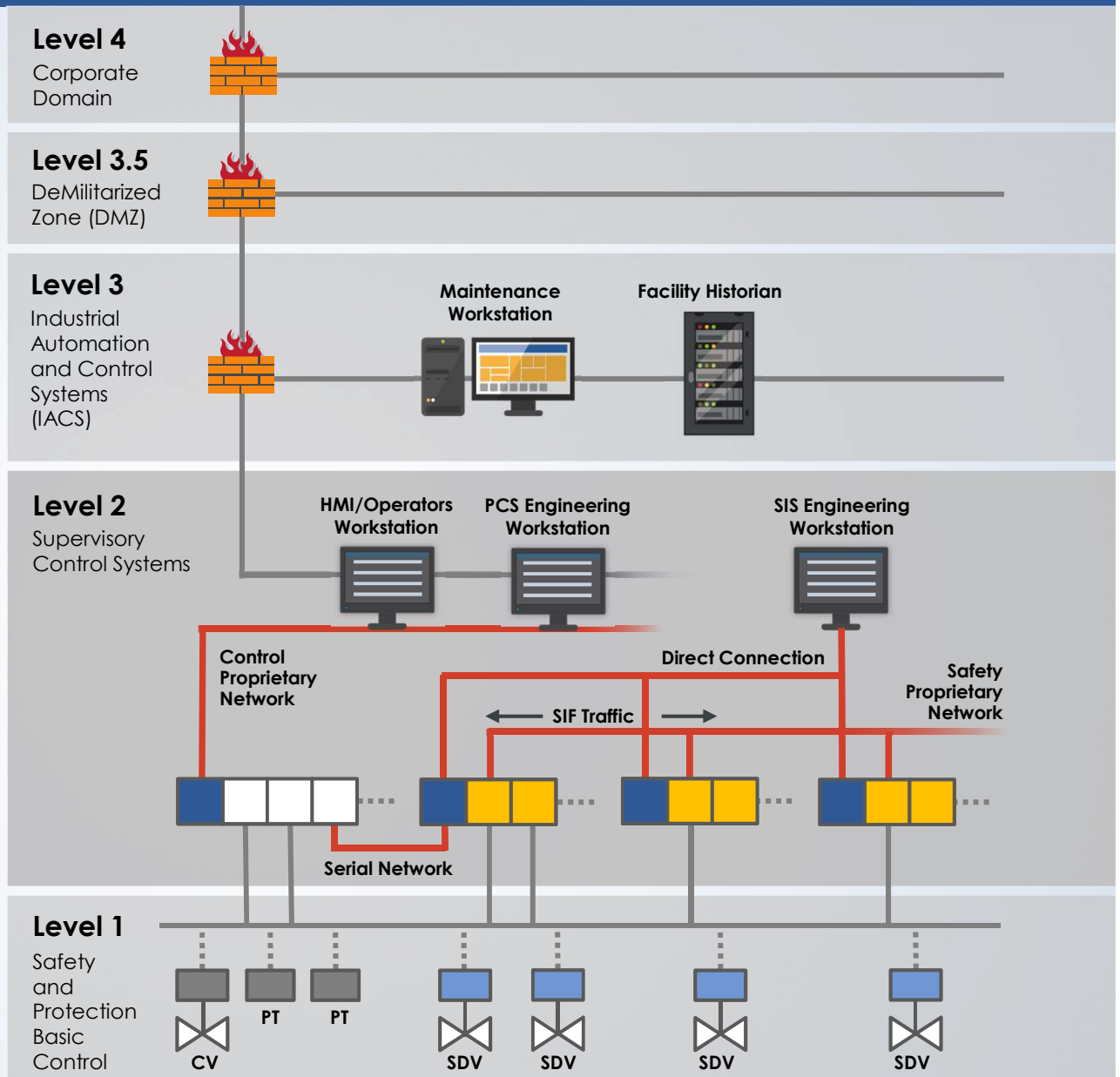
- Network Architecture
- Basic Process Controller
- Safety Logic Solver
- Remote I/O Module

ICSS Integrated Control & Safety System

PCS Process Control System

SIS Safety Instrumented System

SIF Safety Instrumented Function



Safety Instrumented Systems (SIS)

Assessment Approach

Methodology

Risk = Threat x Vulnerability x Consequence

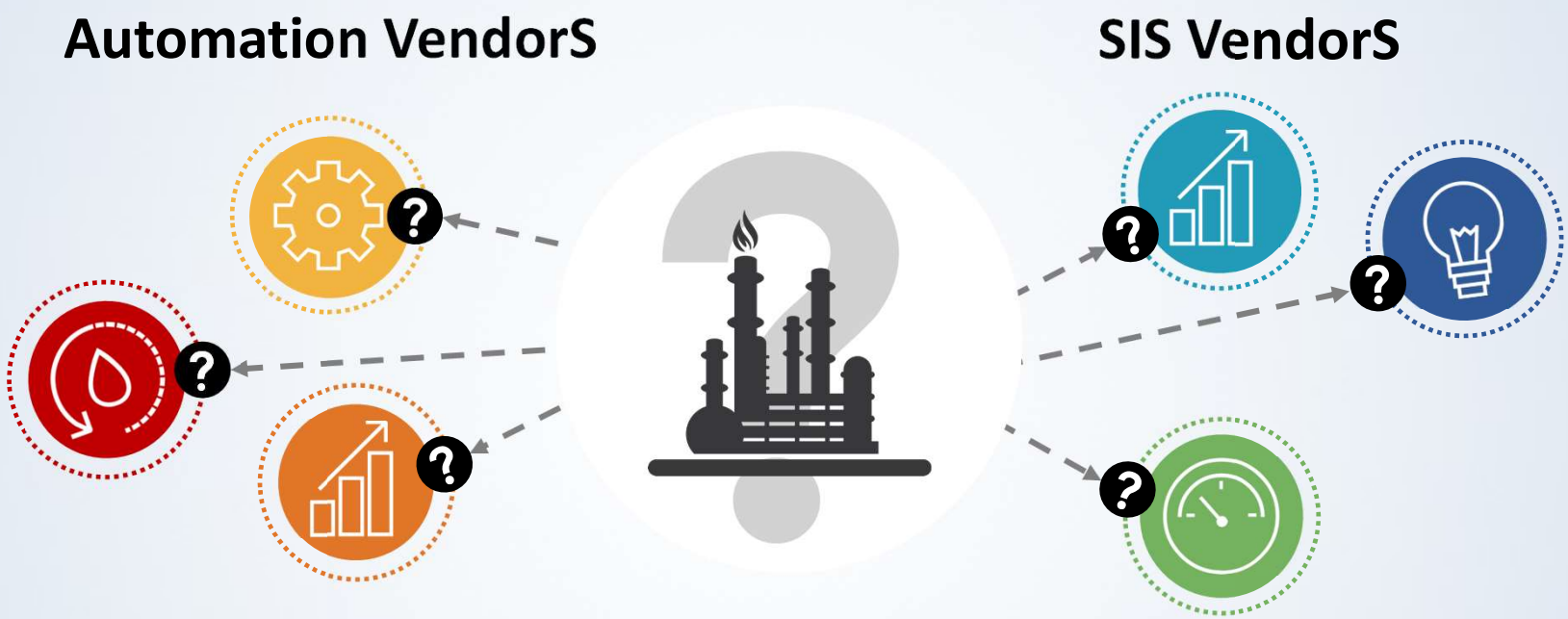
Approach

Vendors + Scenarios + Rules = Plan

Onsite Assessment

- Reconnaissance
- Information capture and data retrieval attempts
- Targeted attacks
- Denial of service (DoS)

Vendor Approach



Each assessment was conducted as an independent sub-project.

Test Approach

Test scenarios included:

Insider and outsider threat scenarios

SME attack methods

Public and customized exploits/payloads

Test equipment

Test Approach

Pre-work phase included:

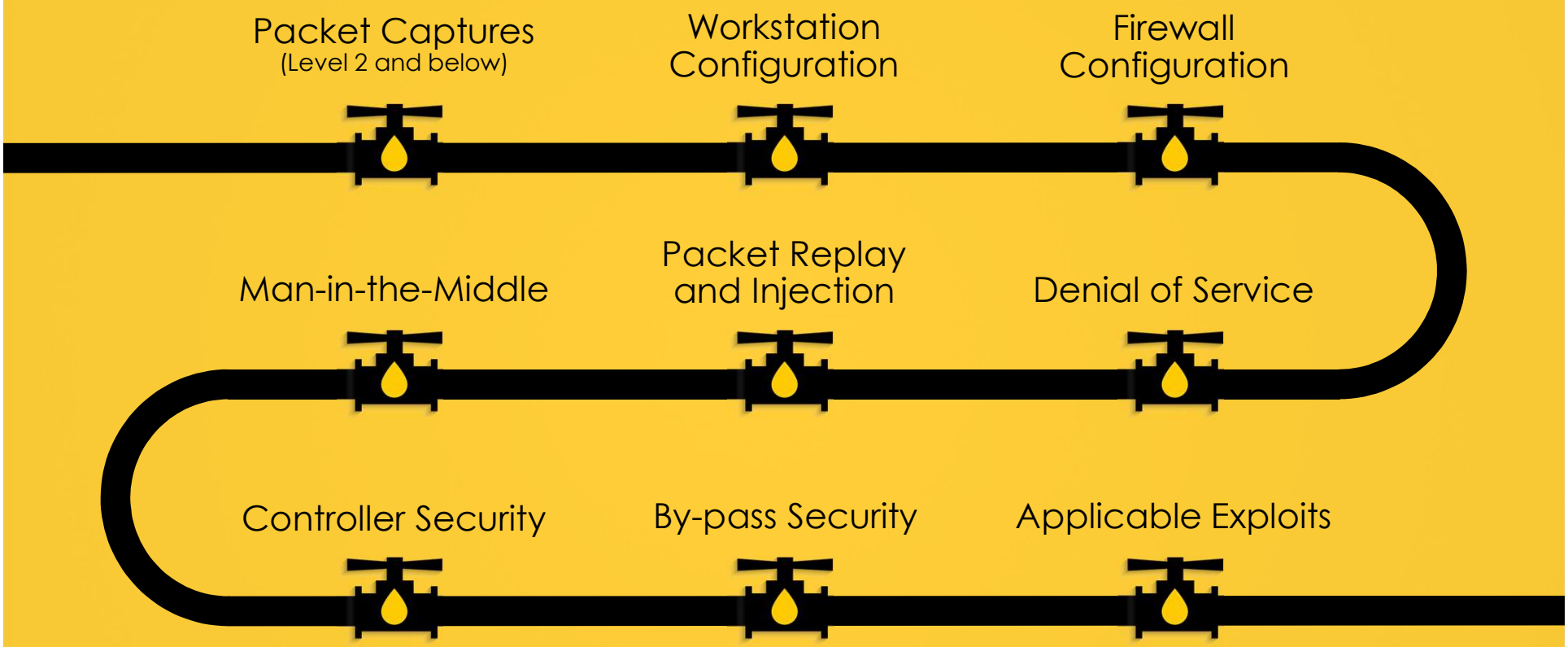
Connection of test equipment

Network validation

Reconnaissance

Traffic capture

Test Scenarios & Vectors



Test Tools

Wireshark®

Nessus®

Custom Test Scripts

Nmap

Kali Linux™

Analysis of Findings

Technical

Research

Documentation

Assessment Tests

Background Info

Observations

Functional Tests

Operational

Usability

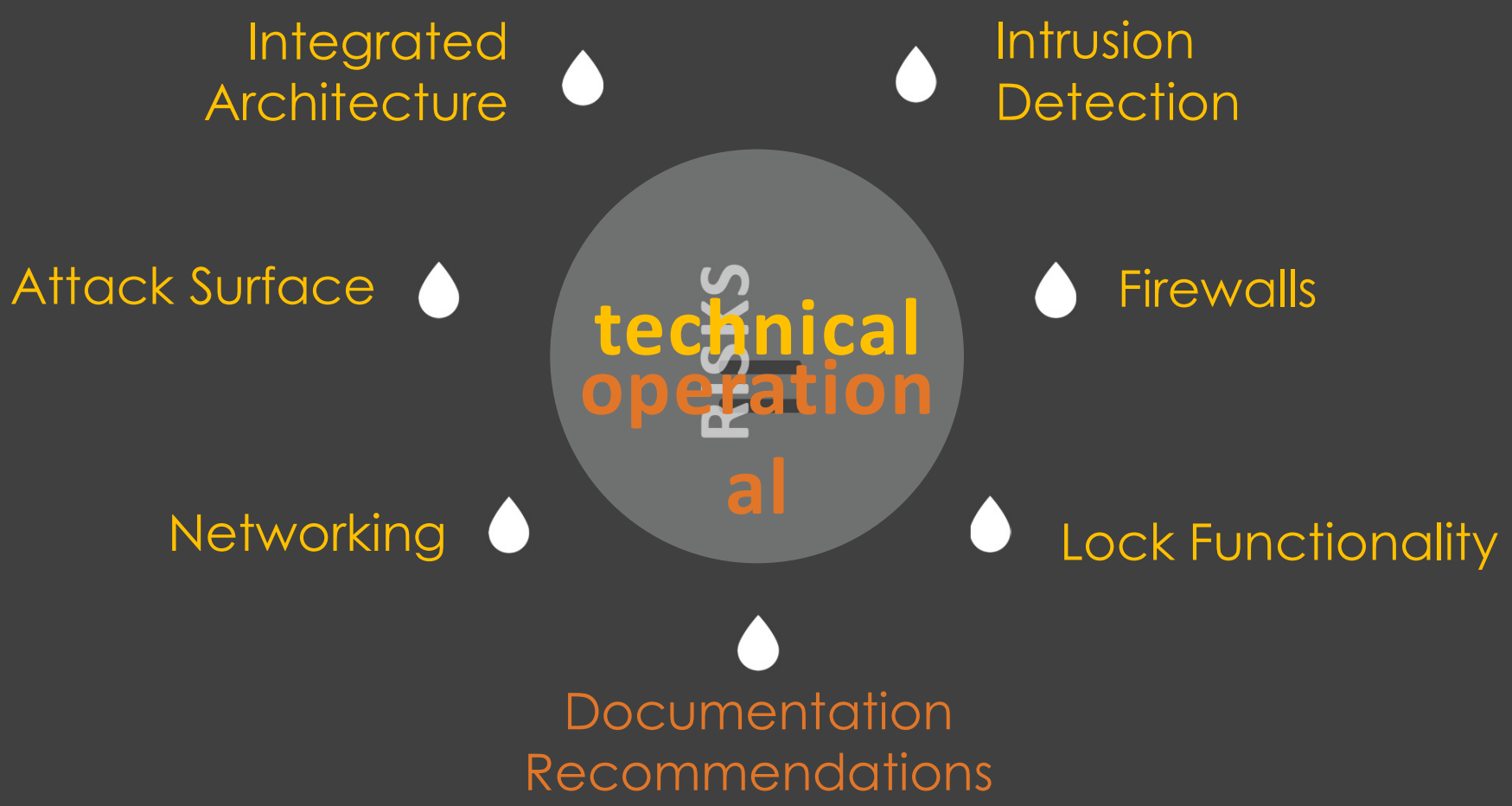
Ease of Implementation

Maintenance Requirements

Skillsets to Maintain and Use System

Safety Instrumented Systems (SIS)

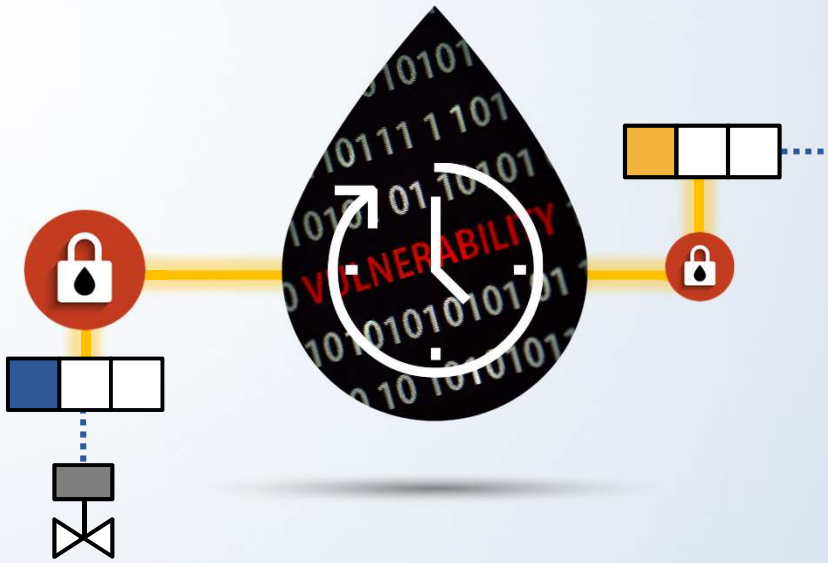
Assessment Findings


Integrated Architecture
Intrusion Detection
Attack Surface
Firewalls
technical
operational
RISKS
Networking
Lock Functionality
Documentation Recommendations

Integrated Architecture

- Due to industry design standards and asset owner desire for increased visibility into the system
- All tested architectures aligned with integrated or partially integrated

- Integration requires added security
- Security should be implemented at the beginning of the life-cycle and maintained
- LOGIIC members expect SIL3 or higher ratings

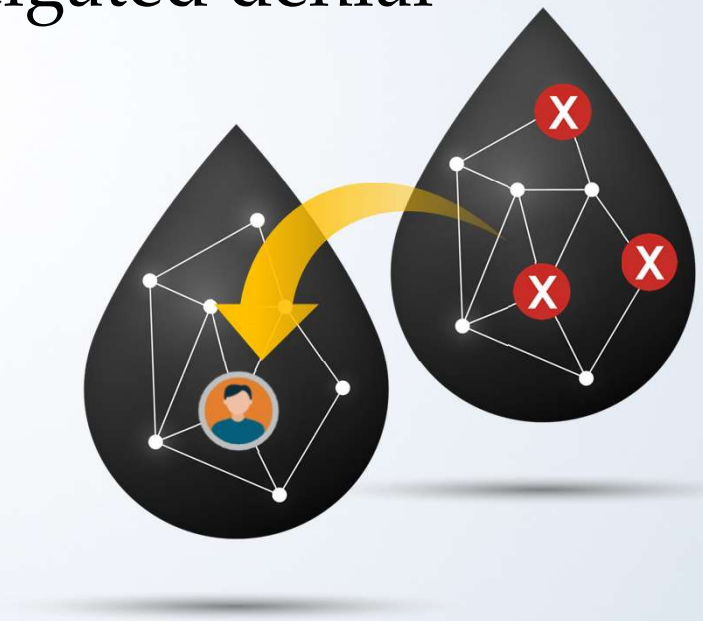


Reducing the Attack Surface

- Redundant networks, numerous components
- Reducing attack surface requires mitigation of vulnerabilities
- Patching and updating is critical
- Solutions varied in size and complexity

Networking: Redundancy

- All solutions tested included redundant safety networks with automatic failover
- Careful configuration mitigated denial and disruption of service



Networking: Protocols

- Use of proprietary protocols
- Packet structures make reverse engineering by an adversary more complicated
- Timestamps, cyclic redundancy checks, and sequence numbers add to complexity
- Unattractive to an adversary

- Protocols that use peer-to-peer communication create a complicated attack surface requiring multiple compromised devices
- Encryption benefits

Networking: Domains

- Security is important to ensuring
  - Principle of least privilege
  - Reduced attack surface
  - Role-based access control
- Includes domain controller, and user/service accounts
- Many SIS solutions offered
- Maintain throughout the life-cycle

Firewalls

Testing revealed that firewalls are needed to:

- Filter malicious network traffic
- Protect against denial of service
- Protect against packet manipulation and injection

Firewalls require:

- Configuration with principle of least access
- Regular maintenance and updates
- Additional layers of protections
- Patching processes
  - Can be complicated due to architectural placement

Intrusion Detection Mechanism

- Certain actions made by the assessment team produced alerts during testing
- Configurability of intrusion detection varies highly by solution
- Configuration of alerts should be fully leveraged by asset owners

Lock Functionality

- Solutions tested included a software and/or hardware locking mechanism
- Provide significant protection against unauthorized changes to the SIS

- Locks are configurable, including duration and automatic re-lock
- Asset owners should assess goals and configure accordingly
- Vendor defaults may be sufficient, but additional review and configuration by the asset owner is recommended

Documentation Recommendations

- Vendors maintain detailed documentation
- Some produce detailed security recommendations
- If documentation is weak, asset owners should require the vendor to define and recommend the most secure implementation and design

Asset owners should look for and use:

- Best practices
- Configuration recommendations
- Implementation guidance to reduce the attack surface
- Layered protections offered

Safety Instrumented Systems (SIS)

Conclusion

SIS Considerations

SIS can be highly configurable, with built-in redundancy and protective mechanisms.

In the past decade, SIS have shifted towards a more integrated design due to the movement of real-time data for situational awareness.

Asset owners and vendors are driving integration for various reasons, such as optimization and maintenance.

Securing an integrated architecture requires more collaboration and work ahead.

- Integrated SIS design can be done securely with appropriate controls
- Design should be reviewed for:
  - Access controls
  - Network separation
  - Principle of least privilege
- Vendor technology that is compliant with IEC and industry standards can be a good starting point

Reducing the attack surface requires layered security throughout the operating system, application, and network.

Good security practices are required such as disabling unnecessary ports, services, and accounts, and removing default passwords.

Maintenance of all SIS components includes patching, updates, and periodic assessment.

A reduced attack surface, good security practices, and maintenance can reduce vulnerabilities.

- Network security plays an important role in overall security and stability of the SIS
- Should include:
  - Packet security through CRC
  - Timestamps and/or sequence numbers
  - Proprietary protocol security
  - Encryption
  - Network redundancy
  - Firewalls
  - Domain security

Configurable intrusion detection capabilities provide situational awareness and alerting.

Hardware and software locks on the safety controllers prevent unauthorized changes to safety logic.

Vendor security recommendations are included in documentation suites.

Documentation suites provide valuable info on configurable security options.

Project 2 Findings

Security conclusions include:

Greater integration may introduce greater risk

Default configurations are not secure

Defense in depth reduces risk

Project 2 Findings

Security conclusions include:

Clear vendor guidance on secure implementation is needed

Ongoing research is needed in security of SIS

Project 2 Findings

Security conclusions include:

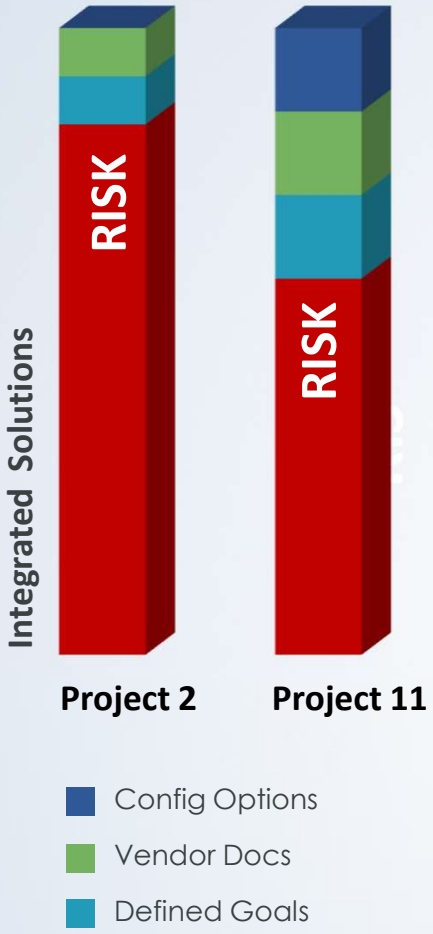
IT security best practices need to be evaluated with respect to applicability in the safety domain

Engagement between the vendor and asset owners is necessary

Project 2 and 11 Analysis

Greater integration definitely means greater risk

- Integrated design standards now exist
- Asset owners demand more access to data, *and* a consistent level of security
- Vendors developed integrated solutions with more inherent security and consider industry recommendations

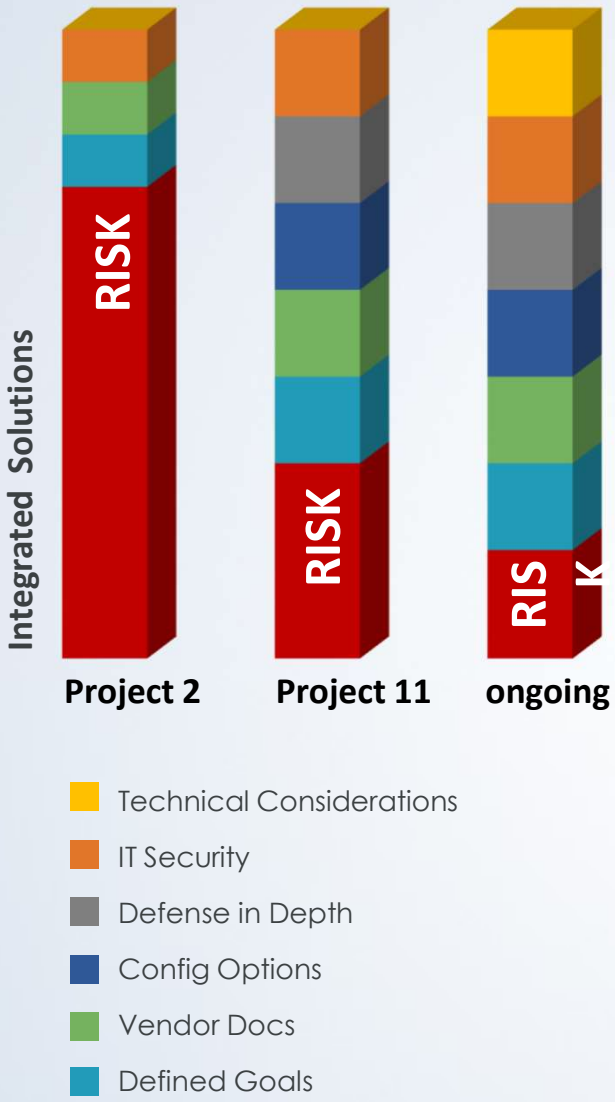


Progress and improvements

- Asset owner and vendor engagement has led to a clearer understanding of operational goals
- Most vendors have security recommendations and documentation for a more secure implementation
- Default configurations provide some security, but many configurable options exist to increase security

Defense in depth and IT security

- Defense in depth was included in the Project 11 testing, should continue as an ongoing recommendation
- IT security measures, such as securing accounts, domains, and removing default passwords, have a defined role in securing aspects of an SIS
- The criticality of an SIS requires advanced security measures and prevention of downtime or disruption



Operational safety net

- Requires consideration of security beyond standard IT implementations
- Redundancies, protocols, and packet security is present in current SIS solutions, but should evolve as technology changes

Conclusions

SIS solutions continue to evolve into integrated designs with security mechanisms and configurable options.

Asset owners should align SIS capabilities with security and operational goals.

Asset owner and vendor engagement created robust solutions with defense in depth, access control, and situational awareness.

Recommendations for Asset Owners

1. Check and close ports that are not needed

2. Consider using modern versions of protocols that prevent the passing of data in clear-text

3. Ensure that a SIEM is used to monitor logs in real-time

4. Review and verify all default passwords are changed

5. Ensure patches are applied in a timely manner to ensure vulnerabilities are managed appropriately

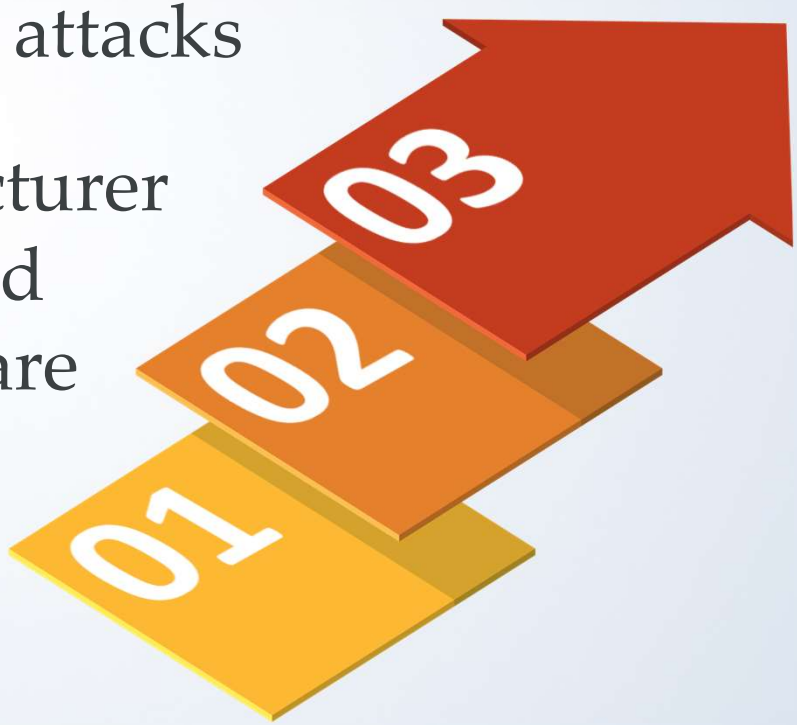
6. Evaluate security options and configure to achieve maximum security

Recommendations for Vendors

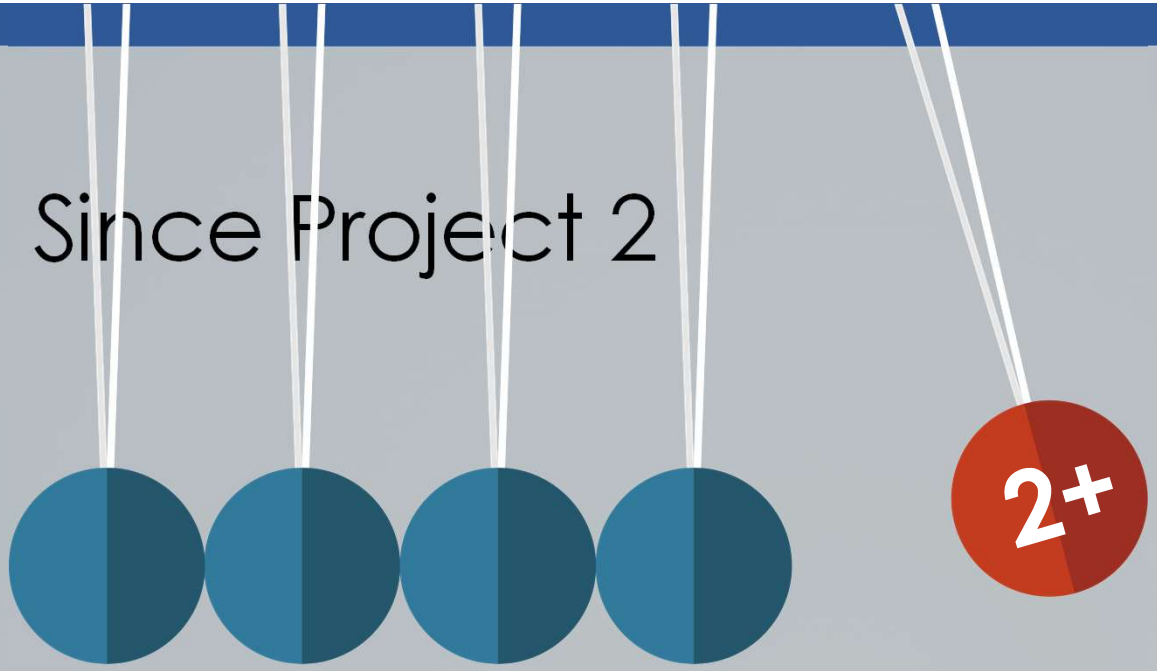
1. Remove unnecessary applications and services

2. Verify all versions of firmware result in full recovery from DoS attacks

3. Work with OS manufacturer to mitigate risks associated with auto installed software that cannot be deleted



Since Project 2

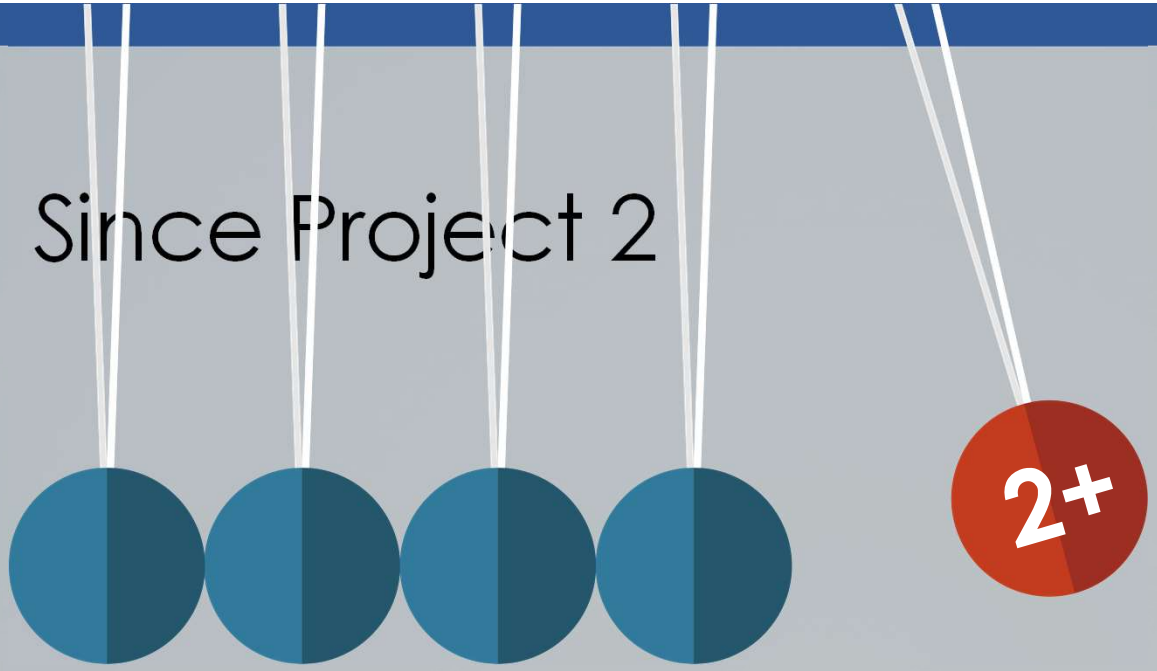


Security improvements include:

Enhanced security capabilities (e.g. controllers)

New access control mechanisms (e.g. Smart Card for the EWS)

Since Project 2

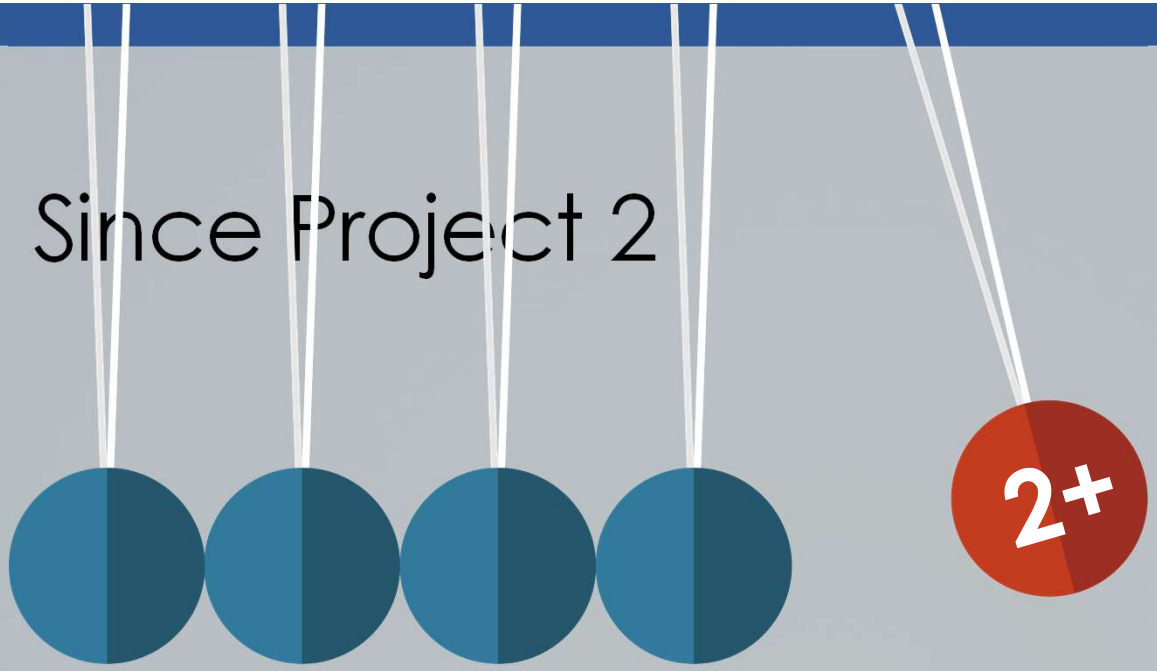


Security improvements include:

New and enhanced network solutions (e.g. new switches, better firewalls)

Added/improved hardware and software locks to protect credentials and devices

Since Project 2

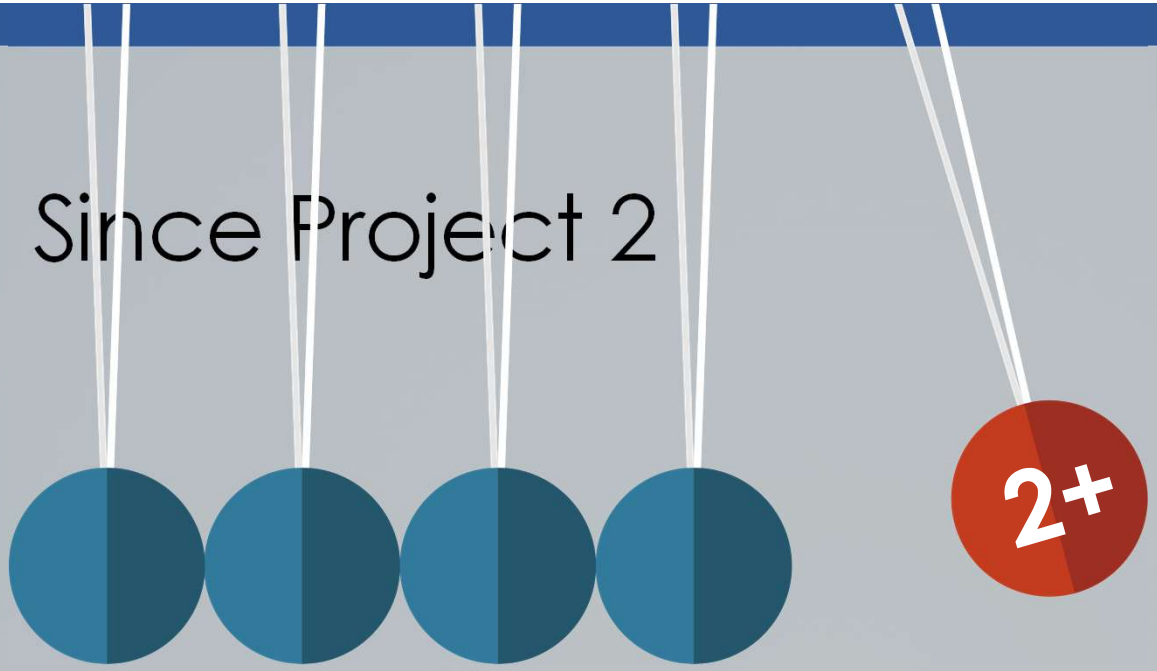


Security improvements include:

Certification of components (e.g. Achilles) by some vendors

Separation of functions (e.g. domain controllers) simplifies maintenance and facilitates patching

Since Project 2

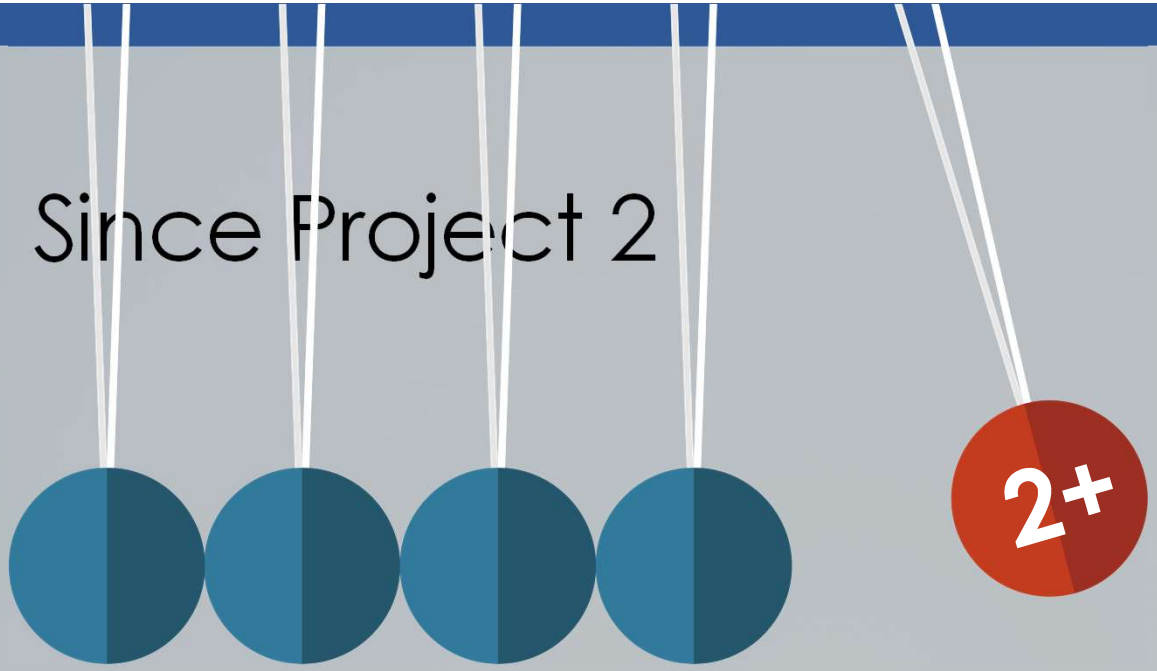


Security improvements include:

Integration and support for Security Information and Event Management (SIEM) solutions

Wider support for antivirus and application whitelisting

Since Project 2



Security improvements include:

Increased focus on security and managing risks associated with end-of-life components