Project 12: Safety Instrumentation and Management

<Subtitle>

<Event>

Acknowledgements

LOGIIC would like to thank the US Department of Homeland Security Science and Technology Directorate for providing leadership, vision, and commitment to enhancing cybersecurity in ICS.

We would like to acknowledge the numerous vendors who fully cooperated in this project and provided equipment and many staff hours. This project could not have been done without the support of these vendors.

Finally, we would like to thank the Project 12 test team, who fleshed out the evaluation strategy, performed the system evaluations, and authored technical reports.

Presenter

Presenter information here

About LOGIIC

The LOGIIC Model of Government and Industry Partnership

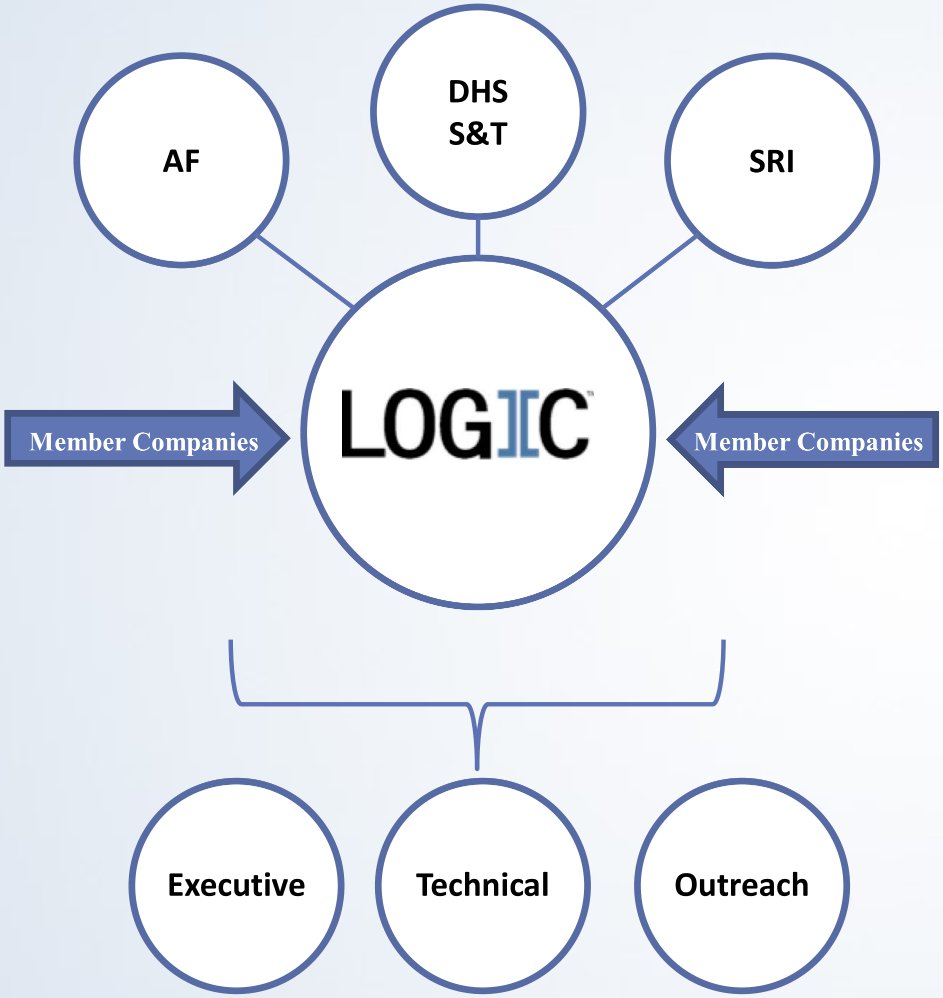
- **Linking the**
- **Oil and**
- **Gas**
- **Industry to**
- **Improve**
- **Cyber Security**

- LOGIIC is an ongoing collaboration of **oil and natural gas companies** and the **U.S. Department of Homeland Security, Science and Technology** Directorate (DHS S&T).
- LOGIIC facilitates cooperative research, development, **testing**, and evaluation procedures to **improve cyber security** in petroleum industry digital control systems.
- LOGIIC undertakes **collaborative research** and development projects to improve the level of cyber security.
- LOGIIC promotes the interests of the sector while **maintaining impartiality, the independence of the participants, and vendor neutrality.**

In 2012, **LOGIIC received the DHS S&T Under Secretary's Award for Outstanding Collaboration in Science and Technology**. LOGIIC has been commended by DHS S&T as a unique framework and a model for establishing similar consortia across other critical sectors.

Collaborative R&D

LOGIIC Broke New Ground in Consortium Governance



- The **Automation Federation** (AF) serves as the LOGIIC host organization.

- The U.S. **Department of Homeland Security**, Science and Technology Directorate has contracted with the scientific research organization SRI International to provide scientific and technical guidance for LOGIIC.

- Member companies contribute and provide staff to serve on the LOGIIC **Executive, Technical and Outreach Committees**. Current members of LOGIIC include **BP, Chevron, ConocoPhillips, Shell, Total** and other large oil and gas companies that operate significant global energy infrastructure.

LOGIIC Projects Timeline (2005 – 2020)

LOGIIC Formation
2007-2008

HPS Project
2010-2011

Wireless Project
2011-2012

Correlation Project
2005-2006

SIS Project
2009-2011

Standards Project
2010-2011

FAT/SAT Project
2012-2013

Virtualization
2013-2014

Mobility
2015-2016

Instruments
2019-2021

Remote Access
2013-2014

Real Time Data Transfer
2014-2015

SIS
2016-2018

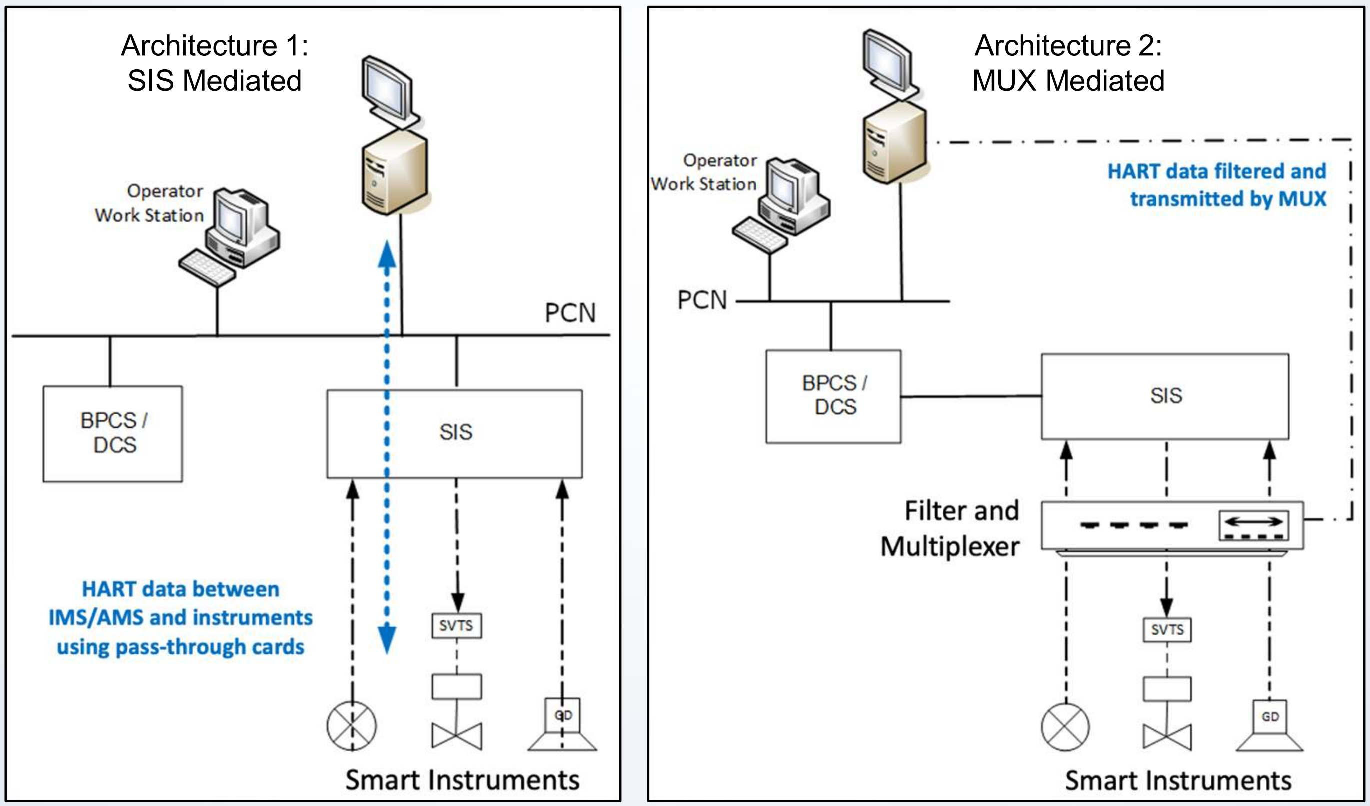
TBD
2021-2022

Future Projects

Public reports and presentations are available on the LOGIIC website

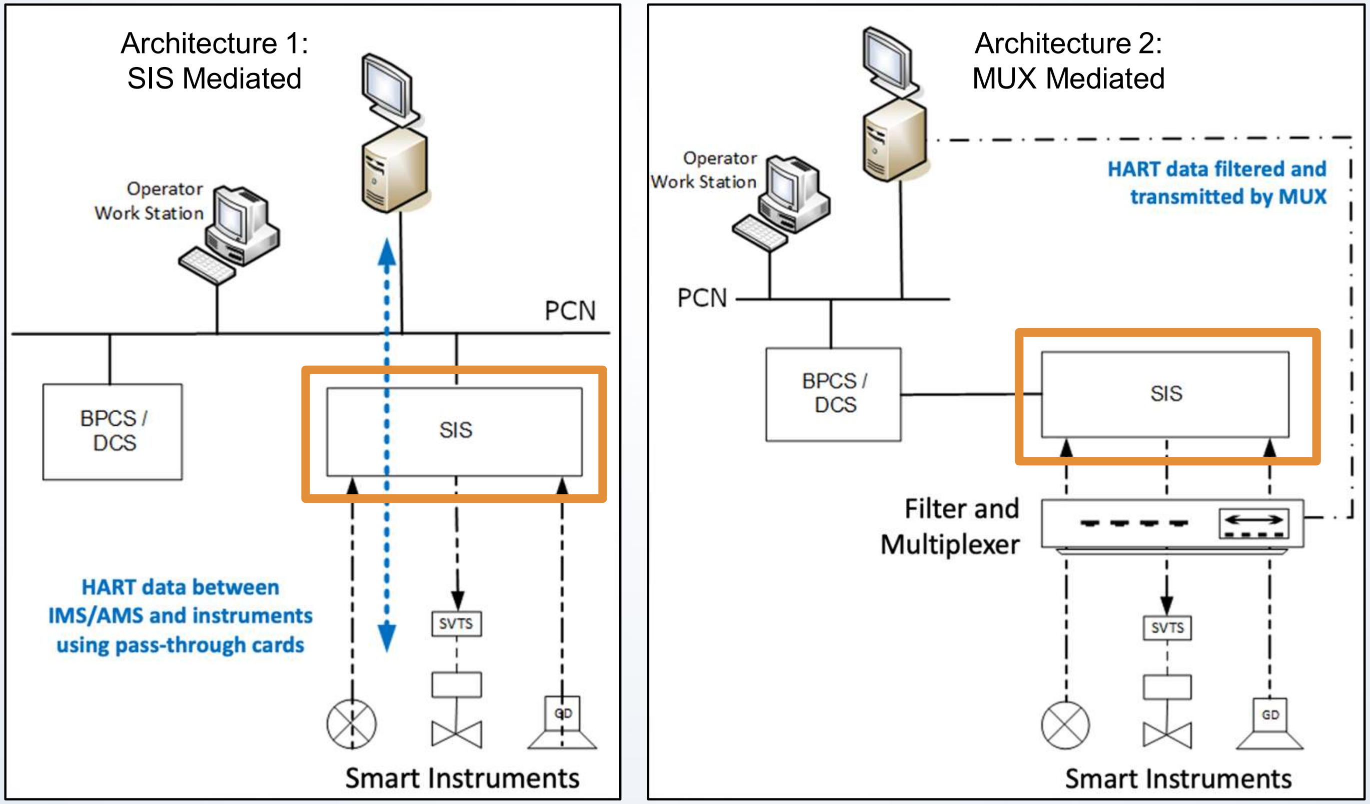
Project 12: Safety Instrumentation and Management

Evaluate cyber security vulnerabilities within safety system instrumentation and its management, in the context of modern safety system architectures.



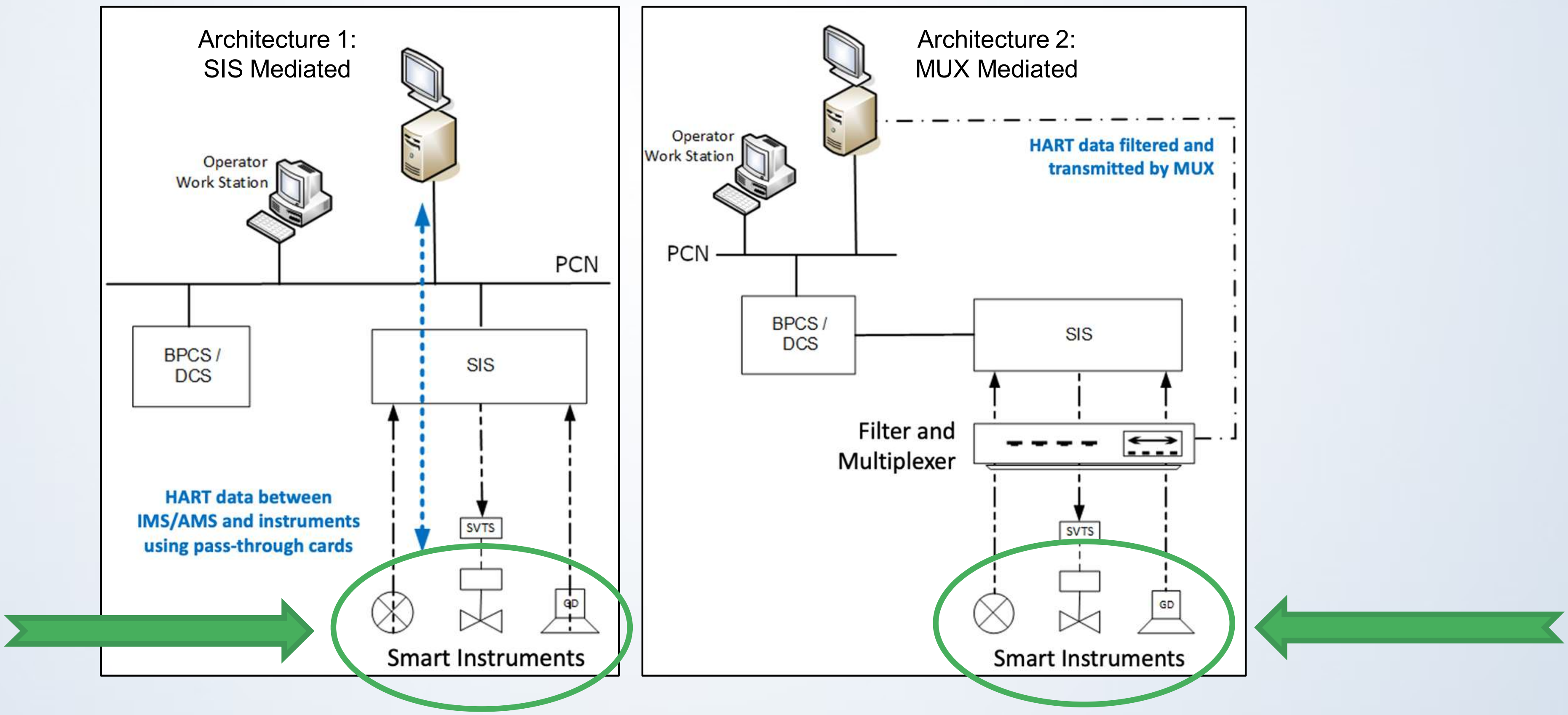
Project 12: Safety Instrumentation and Management

Evaluate cyber security vulnerabilities within safety system instrumentation and its management, in the context of modern safety system architectures.



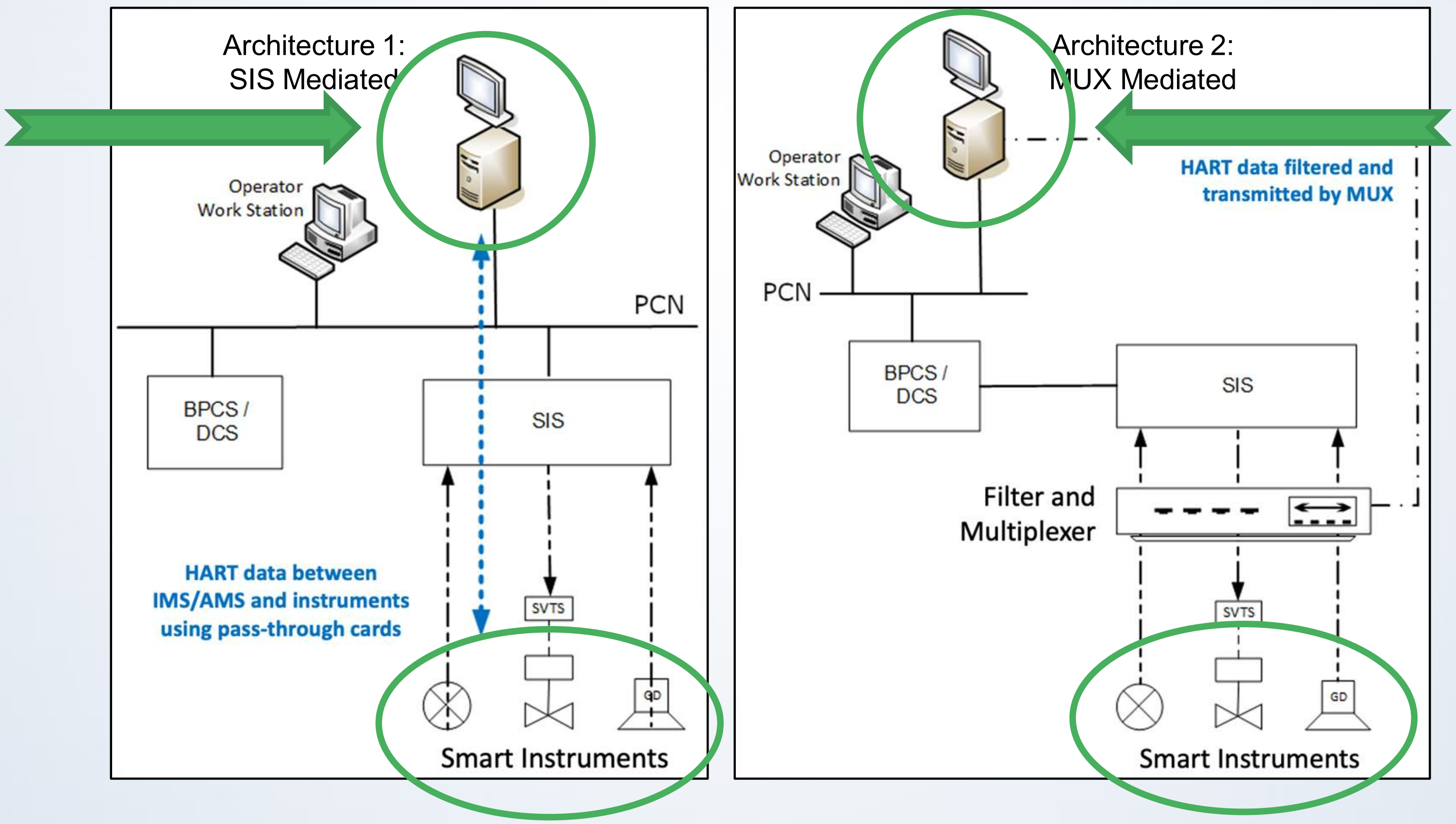
Project 12: Safety Instrumentation and Management

Evaluate cyber security vulnerabilities within safety system instrumentation and its management, in the context of modern safety system architectures.



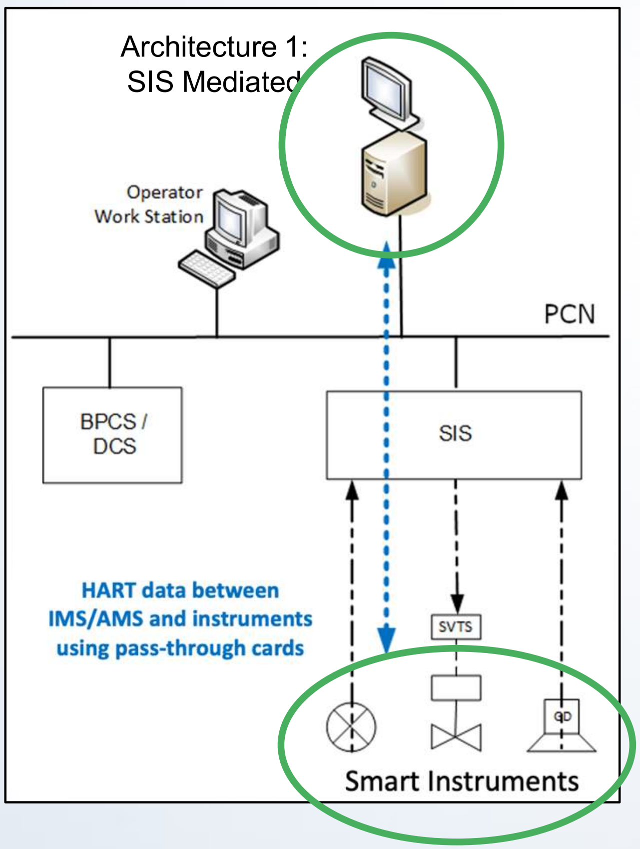
Project 12: Safety Instrumentation and Management

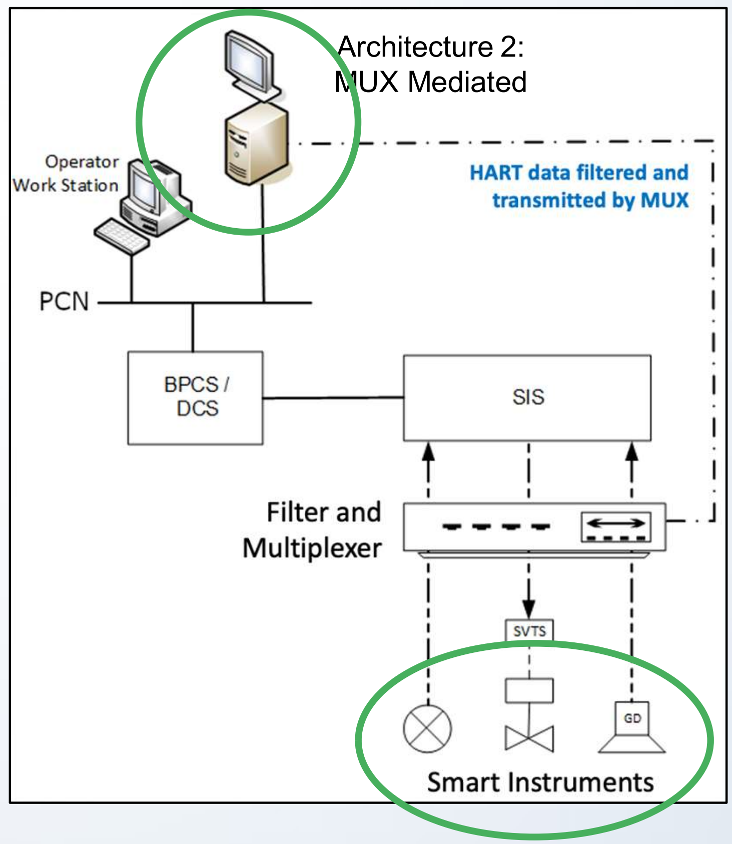
Evaluate cyber security vulnerabilities within safety system instrumentation and its management, in the context of modern safety system architectures.



Project 12: Safety Instrumentation and Management

Evaluate cyber security vulnerabilities within safety system instrumentation and its management, in the context of modern safety system architectures.





Project 12 Results

- Numerous consequential and reoccurring exploitable weaknesses found across Project 12 assessments
  - All issues found are covered by the *MITRE Common Weakness Enumeration* for architectures
- Attackers can make harmful device changes at will and evade detection due primary to
  - Unchecked HART passthrough
  - The tested HART and HART-IP protocols have no built-in security concepts
  - Devices do not authenticate the source of HART commands before execution
  - Industry uses unverified 3rd party DTMs downloaded from the Internet
- There is no single countermeasure that will stop all attacks
- Layered defenses are needed:
  - Technologies to prevent and detect attacks
  - Policies and procedures to fill technology gaps

If cybersecurity best practices were followed, most of these issues would not exist

Mitigation Roadmap

SHORT-TERM

Hardware write-protect

Cybersecurity best practice protections for IMS/AMS

Safe DTM handling procedures

MID-TERM

Use SIS to mediate device comms

Apply existing SIS protections

Encrypt communications

Robust monitoring

Risk analysis

Robust security policy

Training

LONG-TERM

Standards improvements

Product improvements and deployment

Project 12: Safety Instrumentation and Management

Project Definition

Assessment Methodology

Results

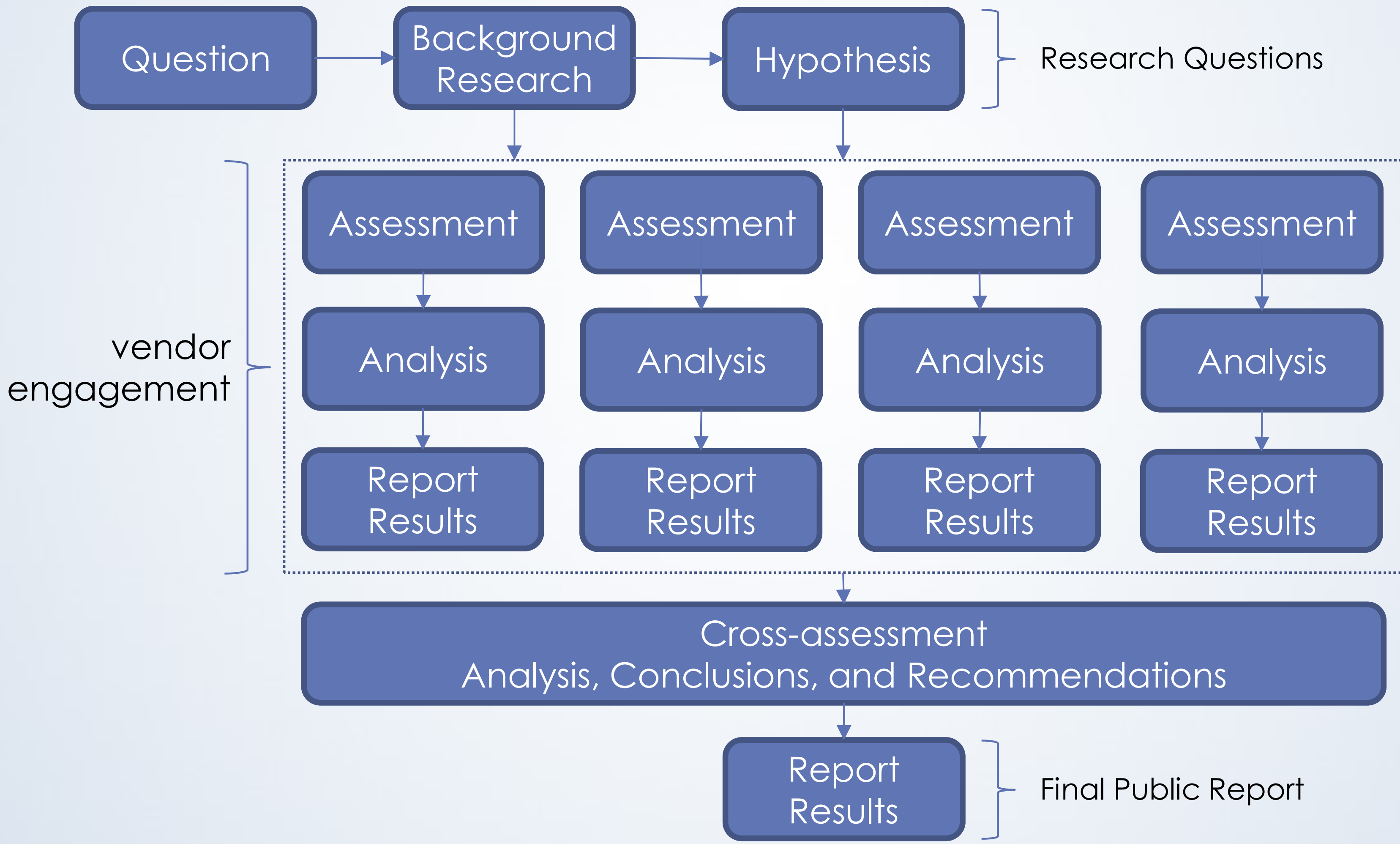
Recommendations

Conclusion

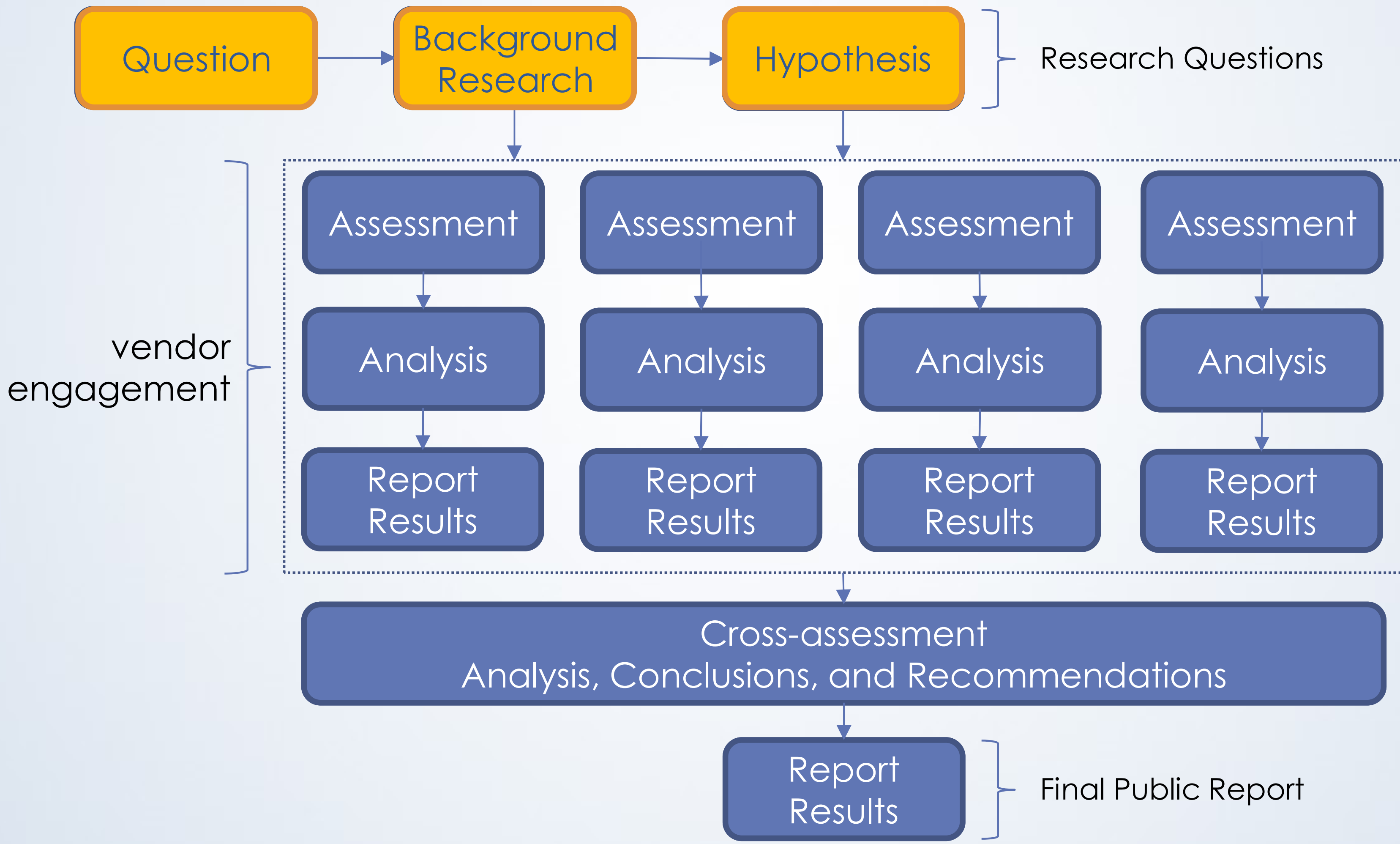
Safety Instrumentation and Management

Project Definition

Project Methodology



Project Methodology



Objective

Understand an attacker's ability to compromise an IMS or AMS and use that trusted platform to alter the function of safety instruments to

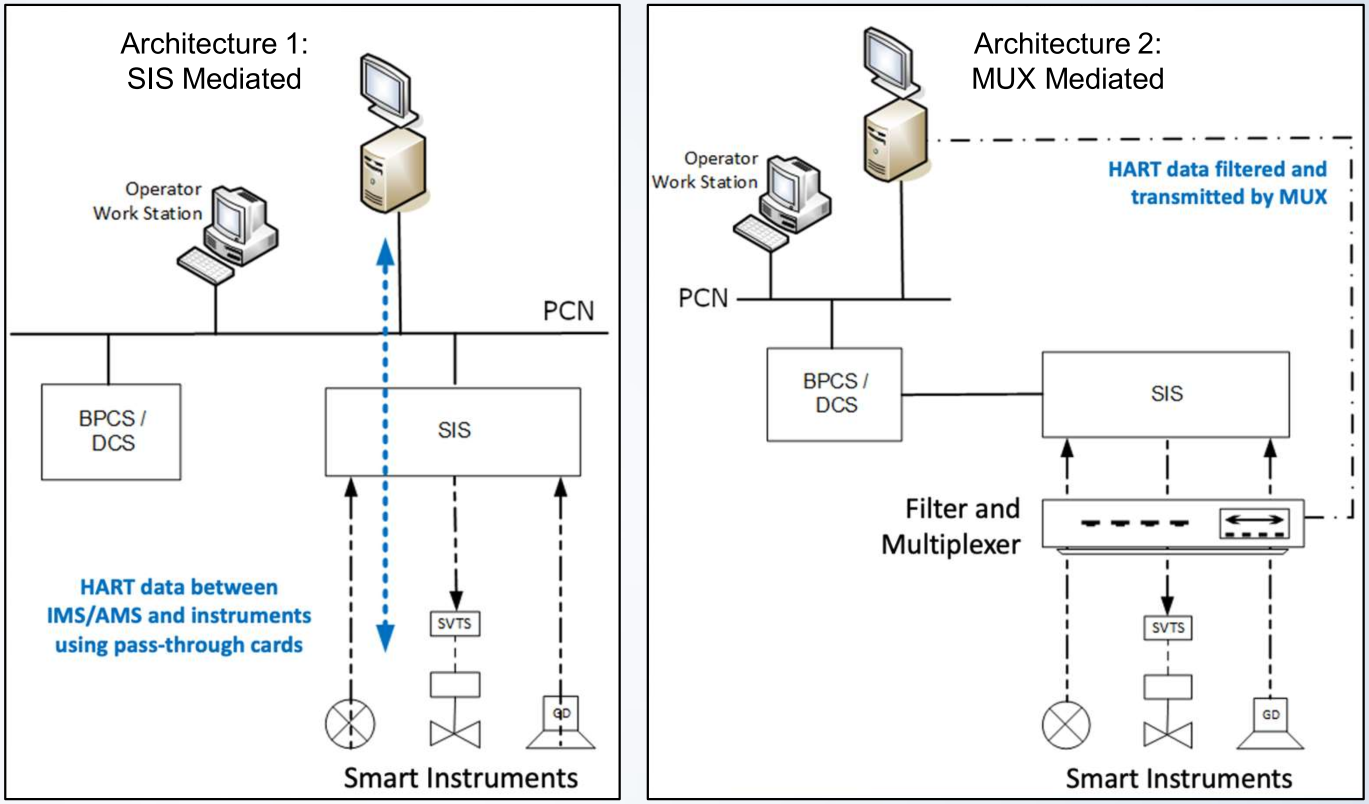
- Create unsafe operating conditions
- Take control away from asset owners
- Render instruments inoperable

Objective

What can an attacker do?

Background Research

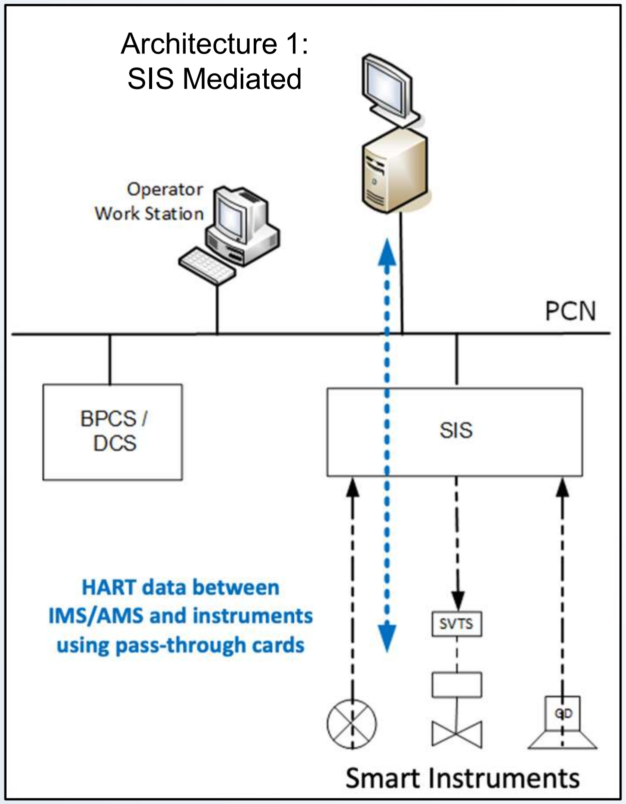
- Identified common safety system designs used in the O&G sector
  - Adopted from Project 11
- Identified instrument types commonly used in safety systems
  - Transmitters, fire and gas detectors, smart valve positioners

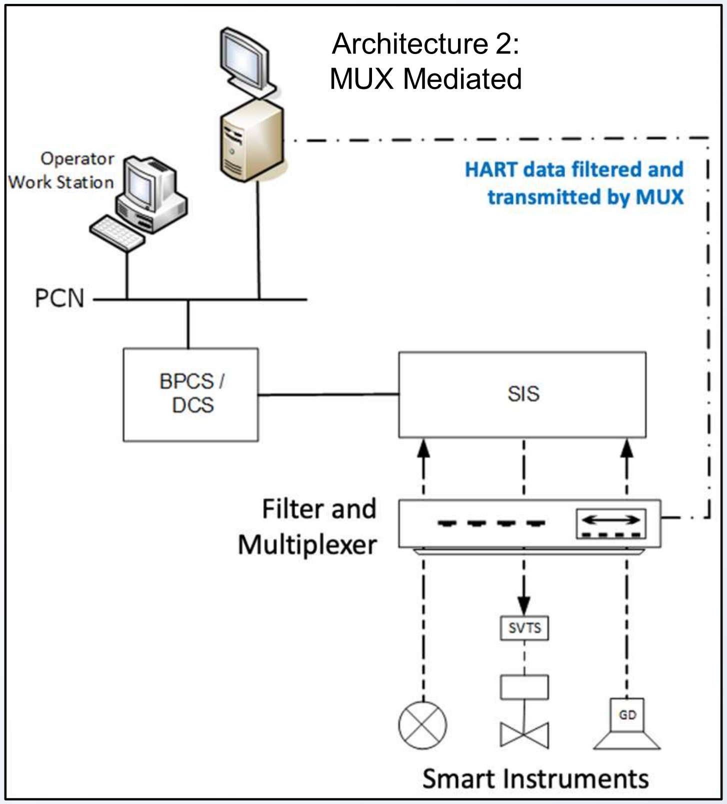


- Identified product candidates to use in assessments
  - Engaged vendors to participate
- Researched HART and HART-IP standards

Hypothesis

An architecture in which an SIS mediates communications between an IMS/AMS and the devices it manages can better mitigate device vulnerabilities than can an architecture in which the IMS/AMS communicates with the devices through a MUX.





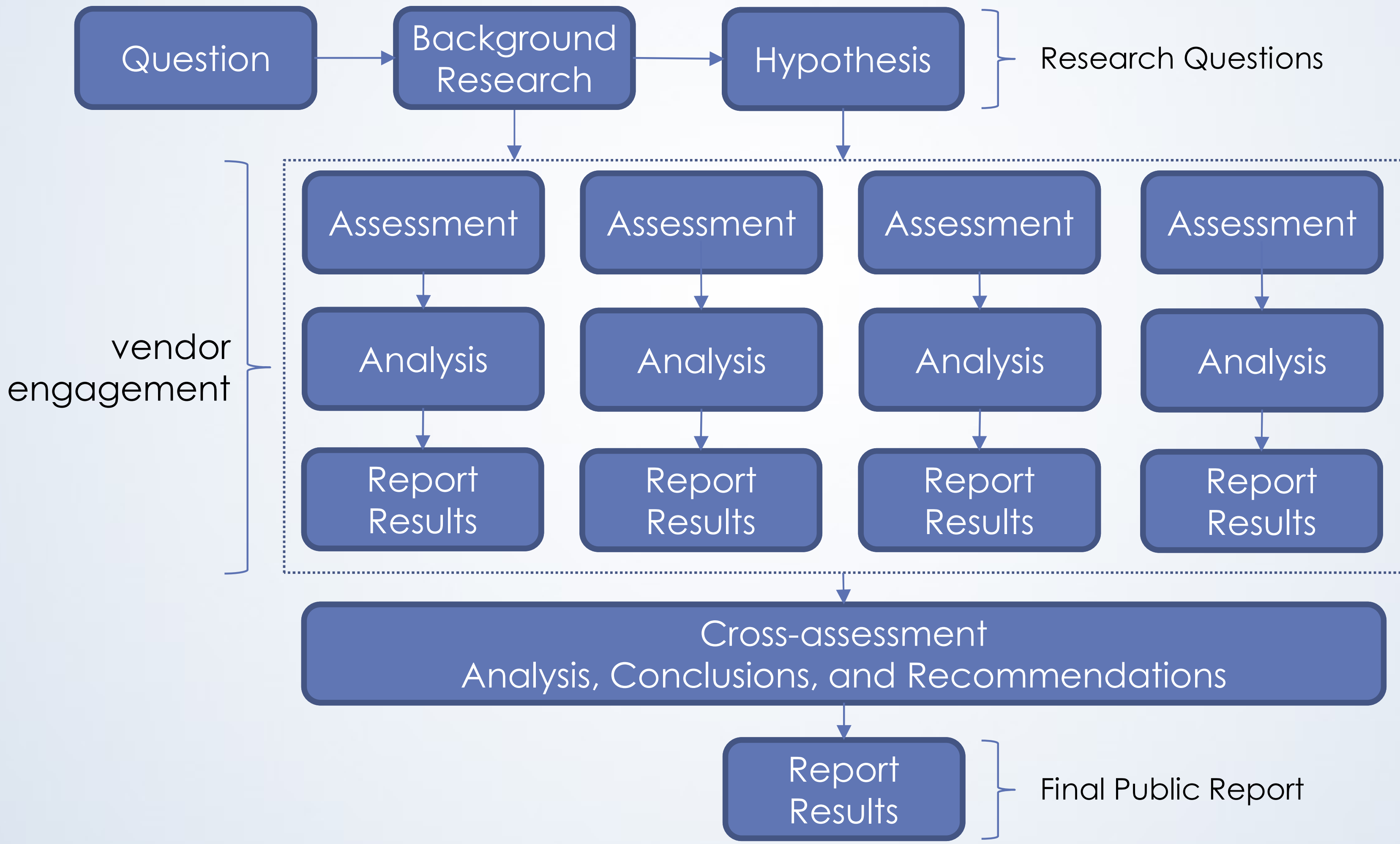
Key Questions

1. Can an attacker compromise the IMS/AMS platform?
2. Can an attacker gain administrative privilege on the IMS?
3. Can an attacker gain remote control of an IMS?
4. Can an attacker compromise the IMS software and/or system either from the IMS system host platform or by remote means?
5. Can an attacker intercept a safety instrument password via keystroke analysis, memory leakage, or network sniffing?
6. Can an attacker affect smart instruments by remotely controlling the IMS software using stolen or cached credentials, with or without IMS administrative privilege?
7. Can an attacker affect smart instruments using a vulnerability exploit, with or without IMS administrative privilege?
8. Can an attacker change an instrument parameter to an unsafe setting while evading detection?
9. Can an attacker bypass any instrument's physical lock or password and cause harm?

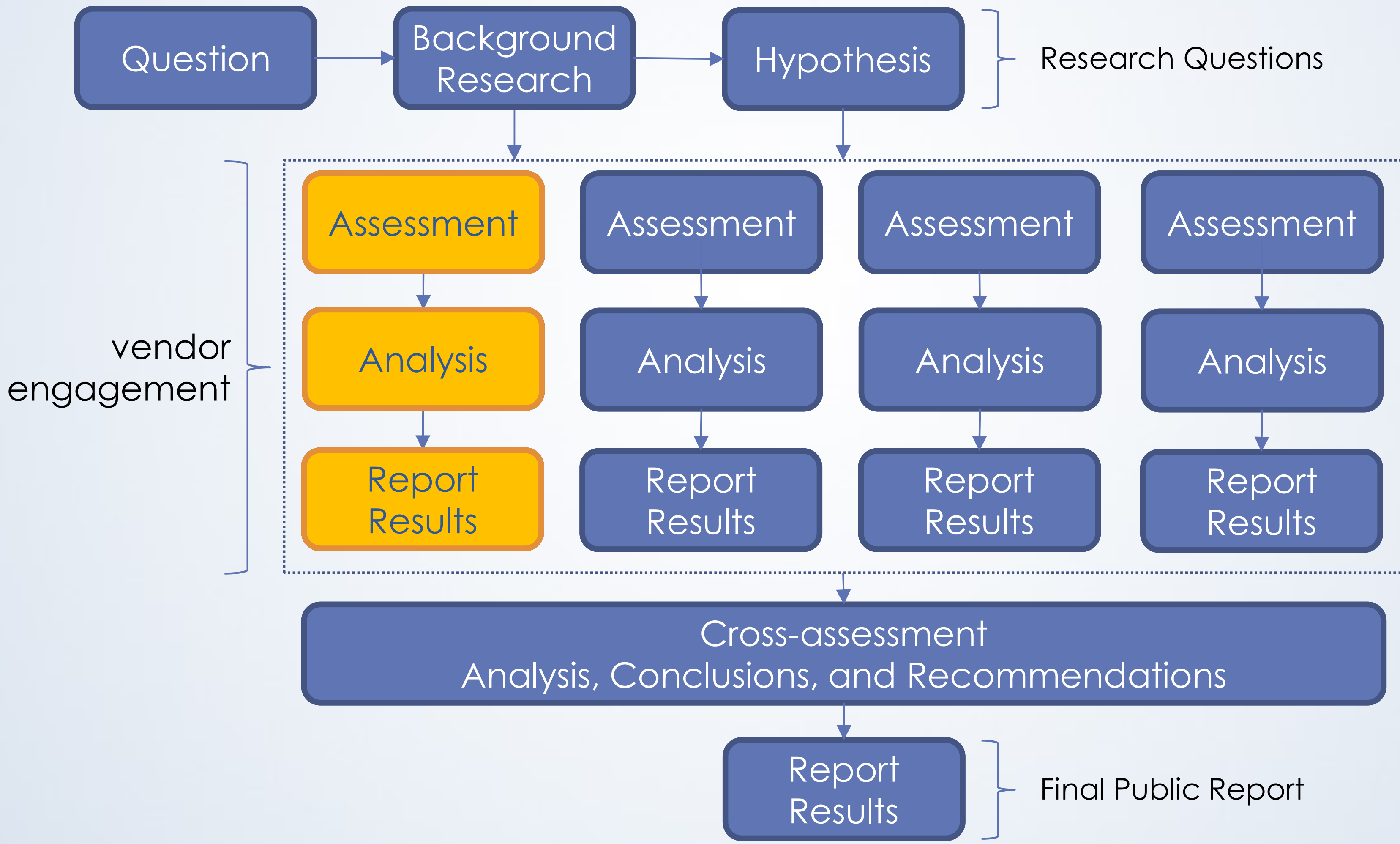
Safety Instrumentation and Management

Assessment Methodology

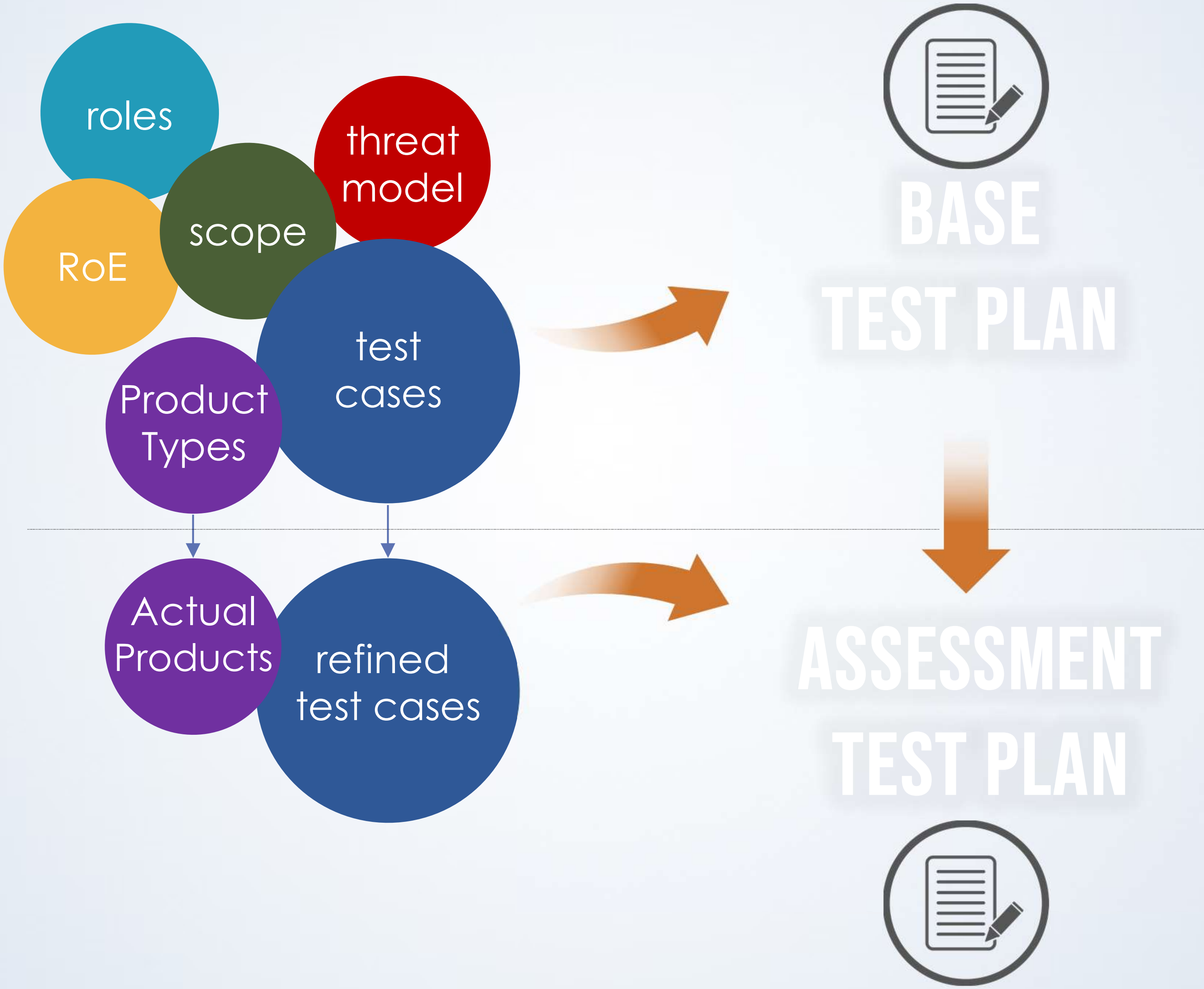
Project Methodology



Project Methodology



Assessment Methodology



Threat Model

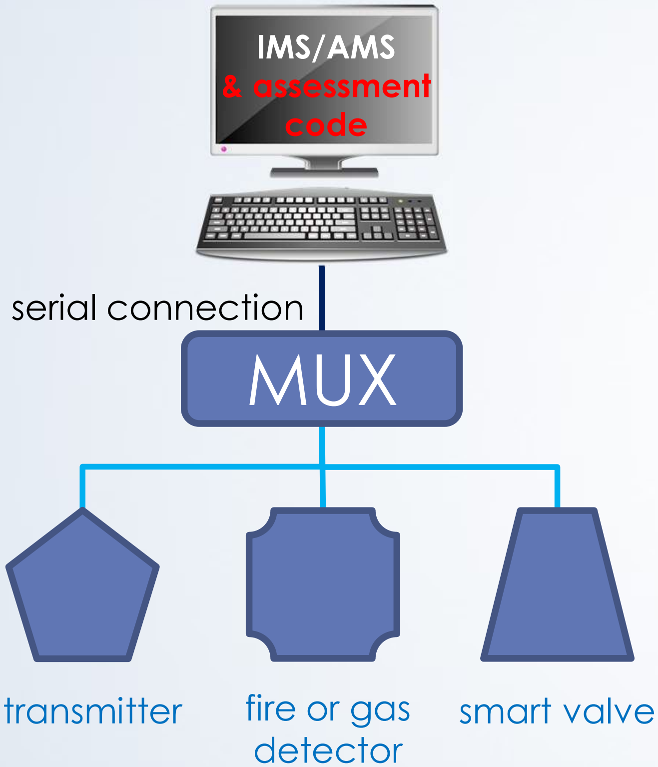
Source	Asset and/or Access Provided
O&G company insider	List of specific safety system products and versions in use and how they are used within the system
	Network switch access, including the ability to insert a network sniffer
	Physical access to IMS/AMS that is connected to the PCN
	Copies of IMS/AMS, device type manager (DTM), and device description (DD) software installed on IMS/AMS platform
	Ability to install IMS/AMS patches and DTMs on an IMS/AMS platform (i.e., administrator access)
Used-devices.com	Used industrial control system (ICS) instruments for probing and analysis
Product vendor public websites	Product sales literature, user manuals, and other documentation
	HART protocol specification
	Product DTMs, software updates and/or patches (only available publicly)
Public web site	ICS-CERT and other advisories
	Other public information (e.g., from product resellers)
Dark web	Working product exploits

- O&G insider
  - Witting and unwitting
  - Limited physical access with no direct access to fielded instruments
- No inside access to any product vendor companies
  - Access only to publicly available product information
  - Unable to inject malware into device firmware
  - Able to create and distribute trojan versions of software product components

Multi-phase Assessment

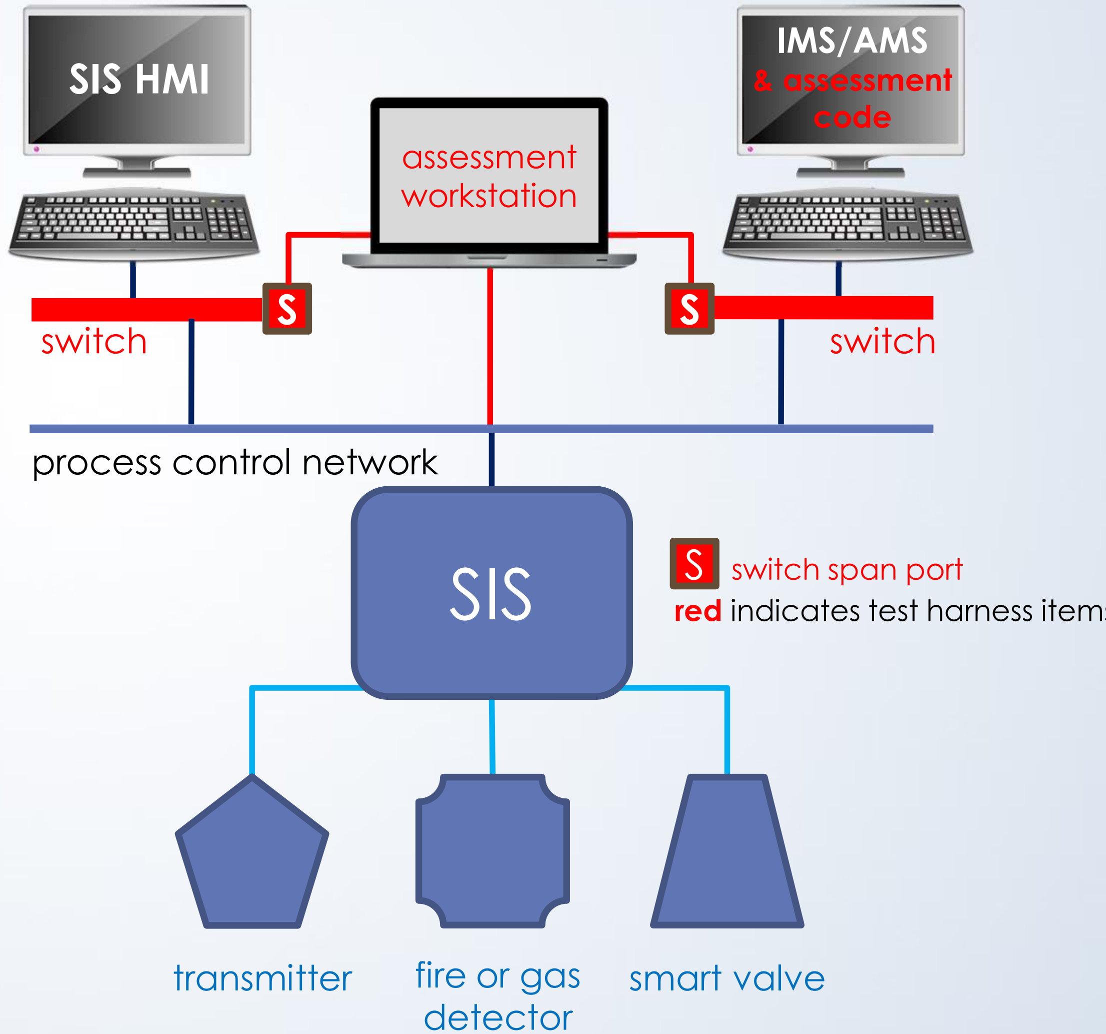
Test Environments

MUX Mediation



red indicates test harness items

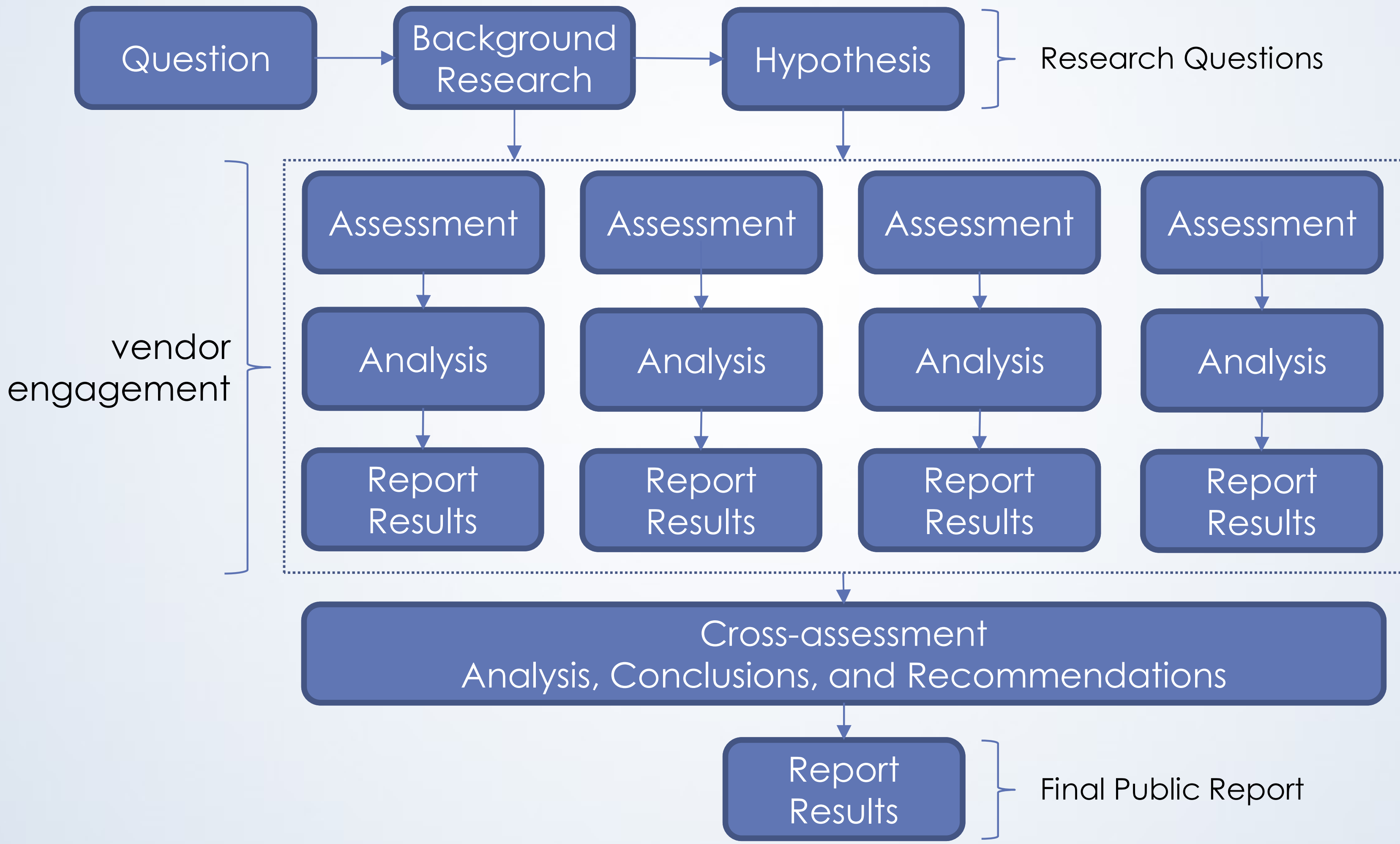
SIS Mediation



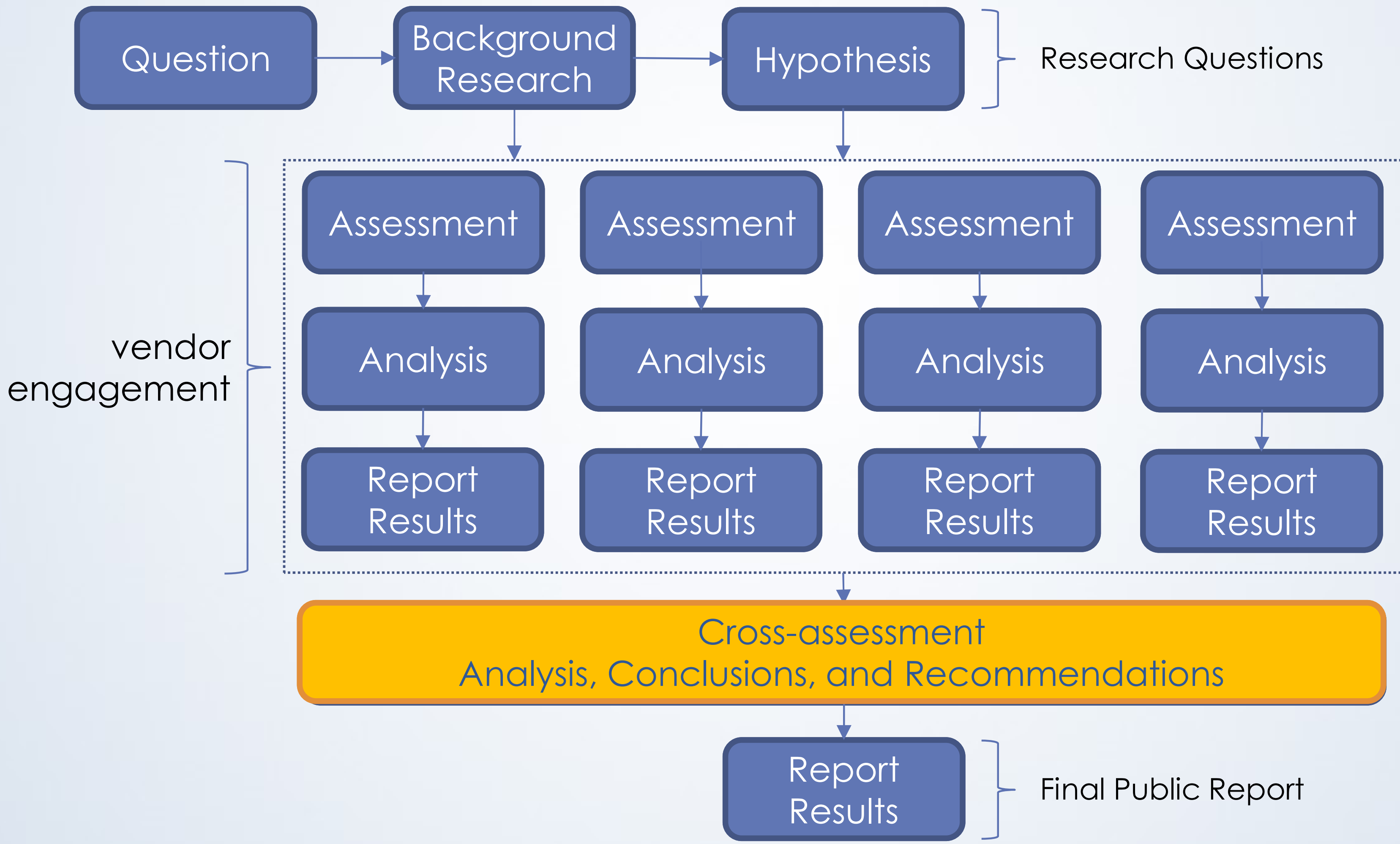
Safety Instrumented Systems (SIS)

Results

Project Methodology

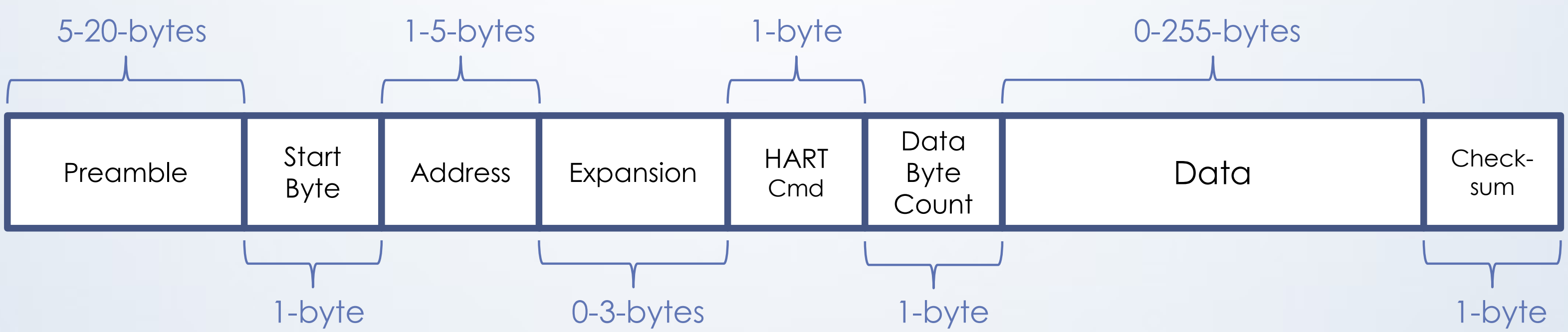


Project Methodology

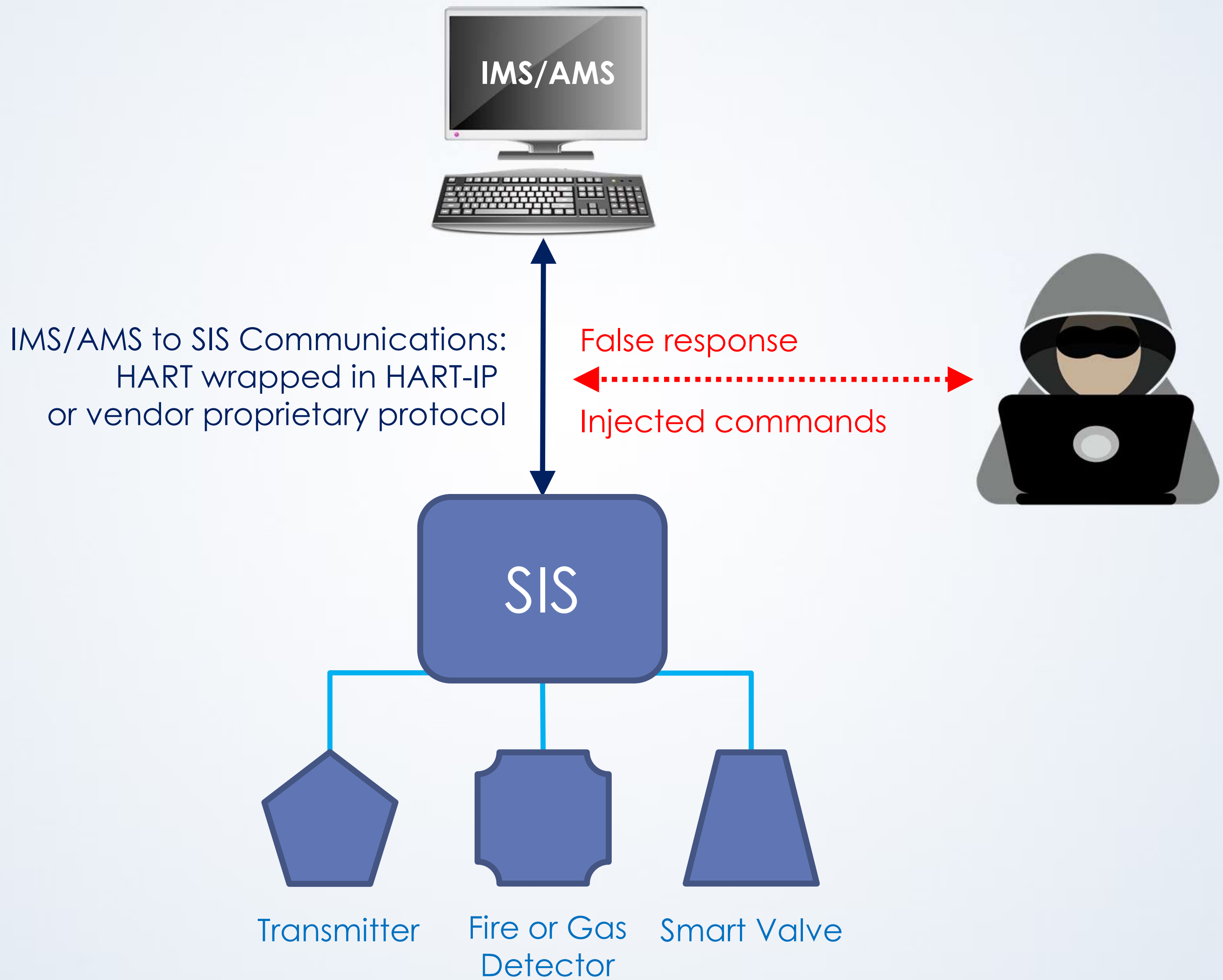


HART Protocol

- Highway Addressable Remote Transducer (HART) Protocol
- Used by safety instrumentation over serial connections
- Can be enveloped in HART-IP or proprietary protocols to use over IP
- Specify a set of common and universal device read and write commands
- Supports additional, undefined device-specific commands, but provides no means to determine which update device configurations and which are read-only
- No inherent security concepts – no authentication, no encryption
- No standard commands for security relevant actions (e.g., clear log files)
- The protocol contains a 1-byte checksum that can easily be recomputed by attackers after packet modification



HART Protocol



Safety Instruments

- All devices tested
  - Use HART 5 or 7
  - Implemented common, universal, and device-specific HART commands
  - Did not implement authentication, even through device-specific commands
  - Assumed any valid HART command received was legitimate and executed it
    - In general, invalid commands were silently dropped or returned an error code
    - Only one device exhibited evidence to attempting to execute an invalid command
  - Can be reconfigured by an attacker if not write protected

Safety Instruments

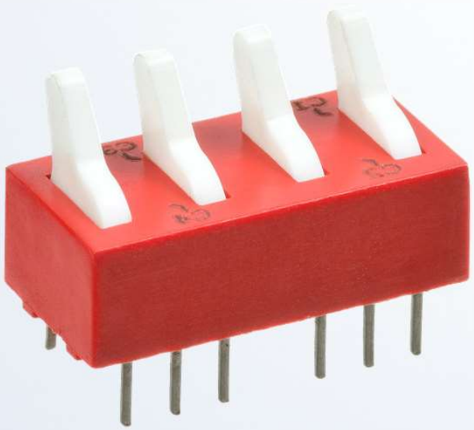
- In the absence of device write protection or other external protective measures, attackers can execute any device-supported HART command at will from the IMS/AMS host platform

Configurations	States	Reset/Evasion
Password and pin code values	Disable write protect	Wipe device alert logs
Alarm settings	Enable write protect	Wipe device history
Valid range limits	Force offline	Reset device change bit
Scaling factors	Put in firmware upgrade mode	
Valve high-low cut off values	Conduct partial stroke test	
Valve positioner feedback values	Put in fixed current mode	
Relay latching behavior	Put in loop current mode	
Partial stroke values	Reset device repetitively	
Positioner calibration	Value position (override)	
Polling address		

- Multiple commands can be combined to create a greater effect
- What can be done depends on the commands implemented by each device

Safety Instruments

- Hardware-based write-protections were effective in preventing most unauthorized changes
  - 2/3 sampled devices did not have hardware-based write-protections
- All software-based write-protections were bypassable
- Write-protections are implemented inconsistently, even on same-vendor products



versus

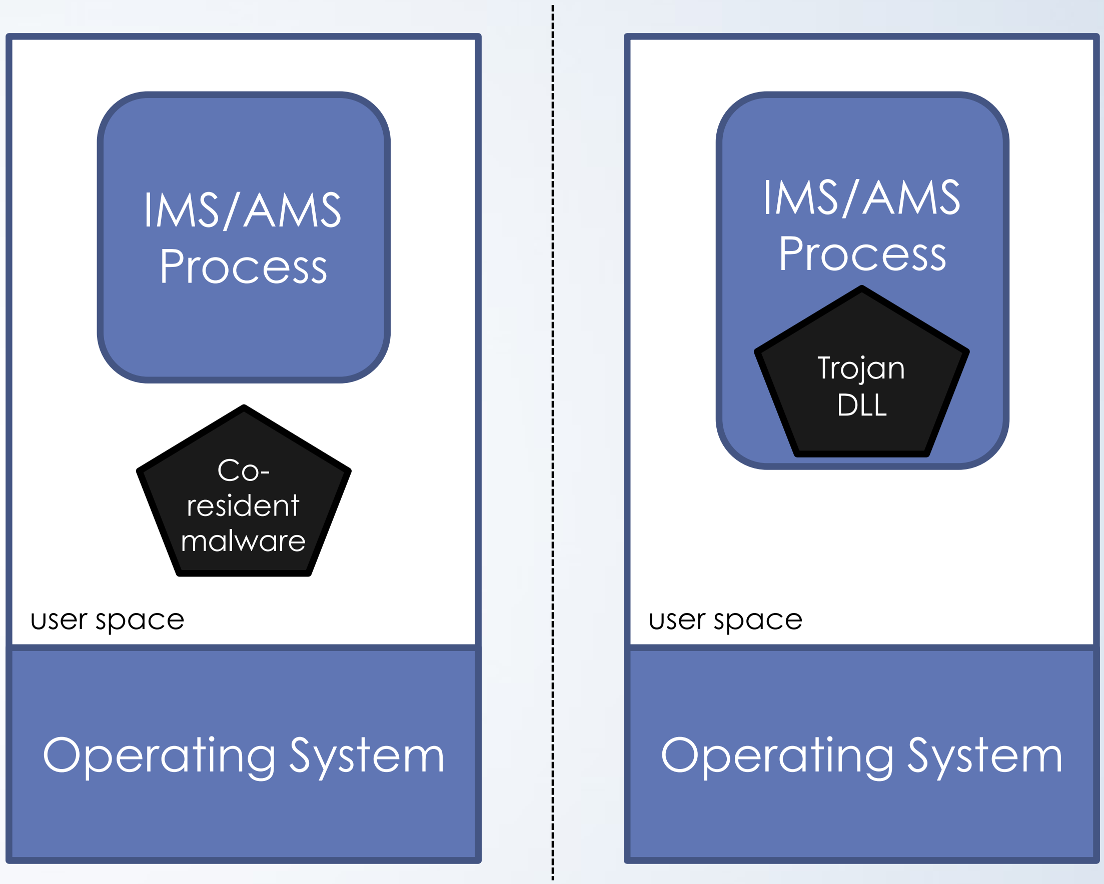
Instrument DTMs and DDs

DTM = Device Type Manager
DD = Device Description

- What are they?
  - Plug-ins used by IMS/AMS for instrument control
  - DDs contain configuration files and provide basic controls
  - DTMs contain configuration files and *executable code* and provide enhanced controls
- Assessment revealed
  - Most are directly downloadable from the Internet, some in clear text
  - None have verified publishers that are checked at installation time
  - Only 22% had signed DLLs to prevent modification
  - 22% were written in a way that facilitated source code extraction for reverse engineering

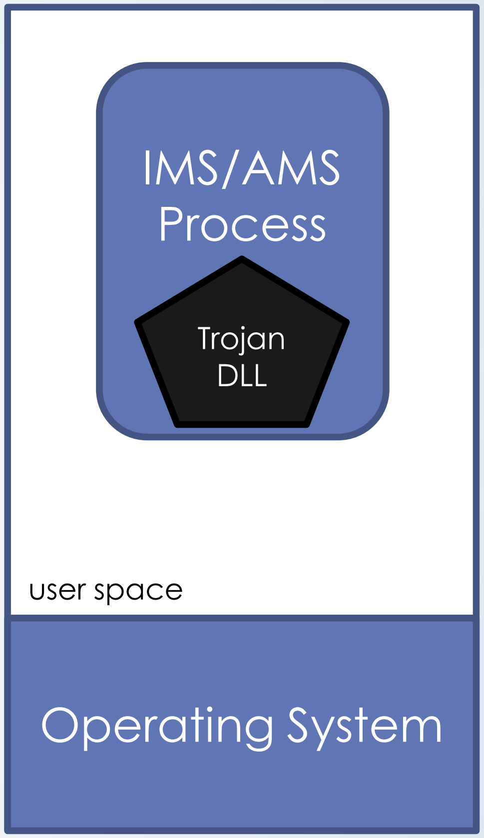
DTMs and DDs on the IMS/AMS Platform

- Software installers require administrative privileges
- Malicious software packages can install
  - Malware executables along side legitimate software files
  - Trojan IMS/AMS DLLs
  - Trojan DTM DLLs
  - Trojan DD or DTM configuration files



DTMs and DDs on the IMS/AMS Platform

- Why are trojan DLLs possible?
  - All tested IMS/AMS solutions loaded DTMs and DDs without first checking their integrity
  - Once loaded, trojan DLLs operate as part of the IMS/AMS process, which is a safety-system trusted component
- The test team created and inserted trojan DDs and DTMs that successfully altered device configurations for 78% of tested devices

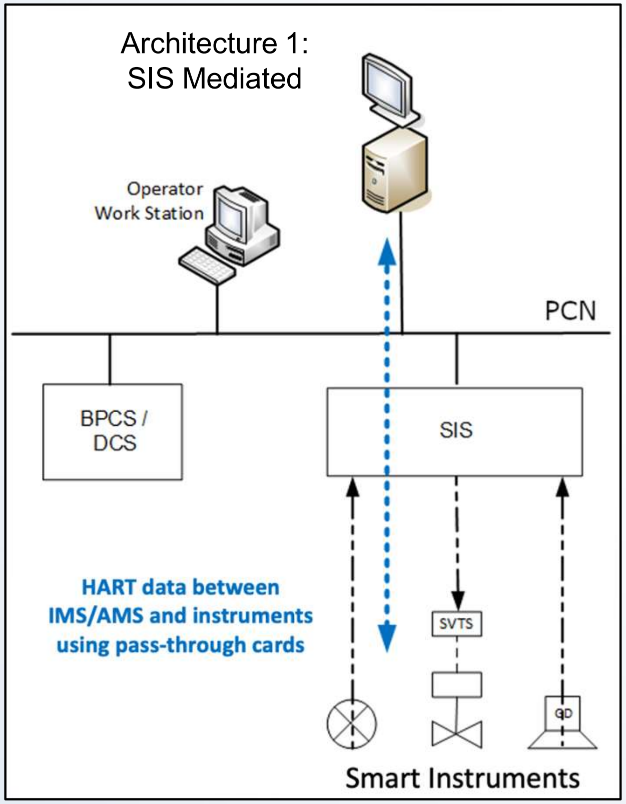


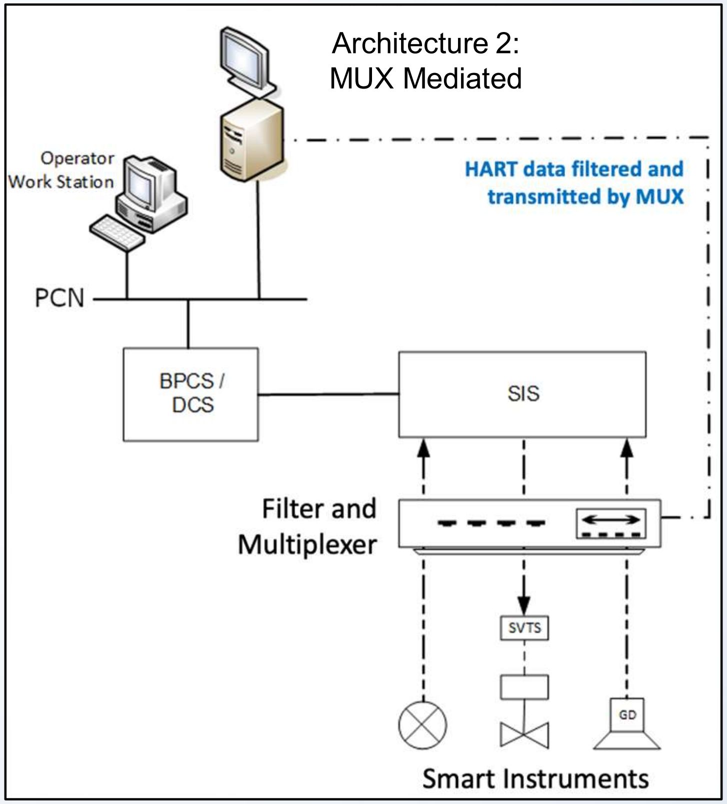
Key Questions

1. Can an attacker compromise the IMS/AMS platform?
2. Can an attacker gain administrative privilege on the IMS?
3. Can an attacker gain remote control of an IMS?
4. Can an attacker compromise the IMS software and/or system either from the IMS system host platform or by remote means?
5. Can an attacker intercept a safety instrument password via keystroke analysis, memory leakage, or network sniffing?
6. Can an attacker affect smart instruments by remotely controlling the IMS software using stolen or cached credentials, with or without IMS administrative privilege?
7. Can an attacker affect smart instruments using a vulnerability exploit, with or without IMS administrative privilege?
8. Can an attacker change an instrument parameter to an unsafe setting while evading detection?
9. Can an attacker bypass any instrument's physical lock or password and cause harm?

Hypothesis Revisited

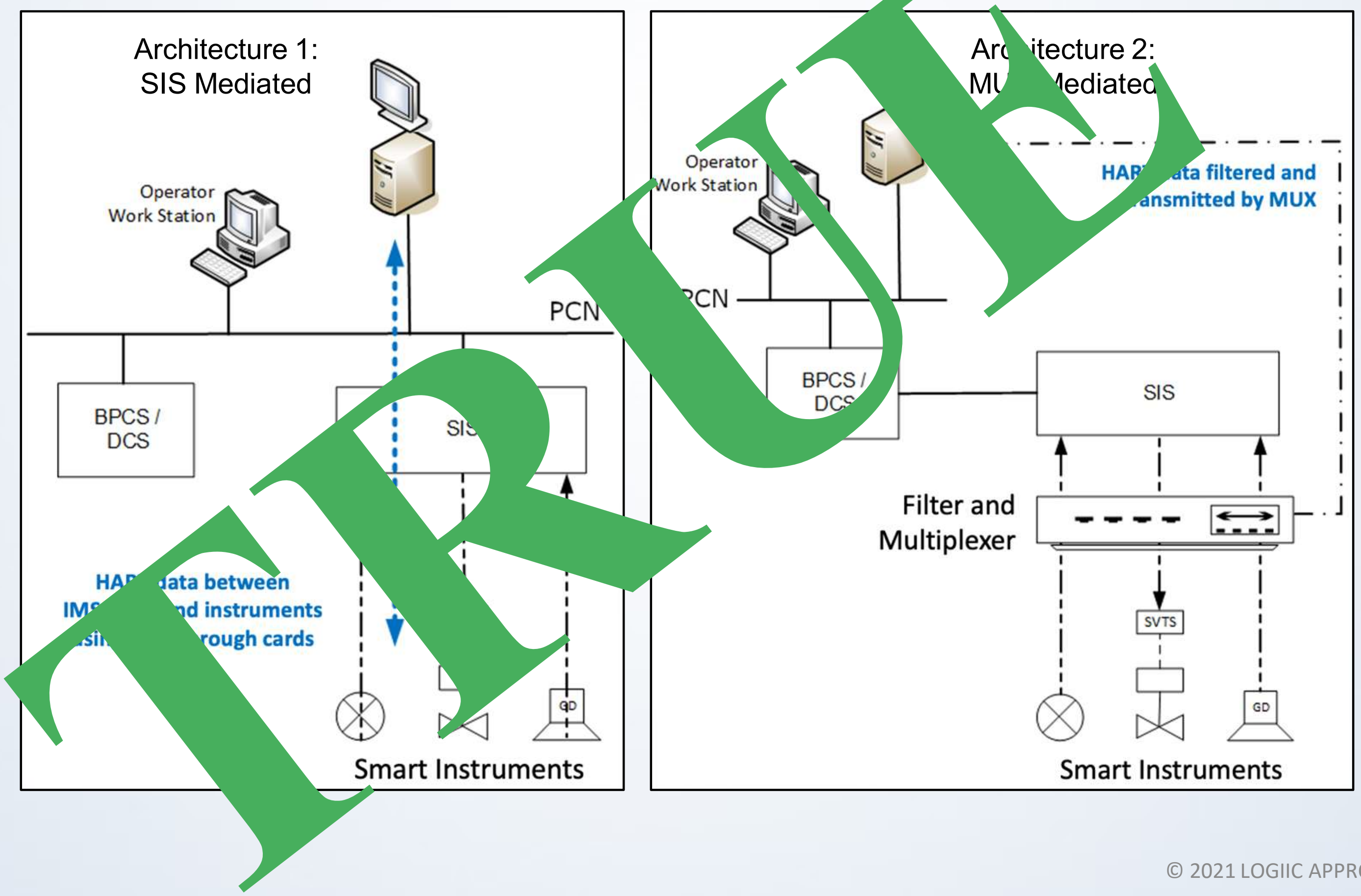
An architecture in which an SIS mediates communications between an IMS/AMS and the devices it manages can better mitigate device vulnerabilities than is an architecture in which the IMS/AMS communicates with the devices through a MUX.





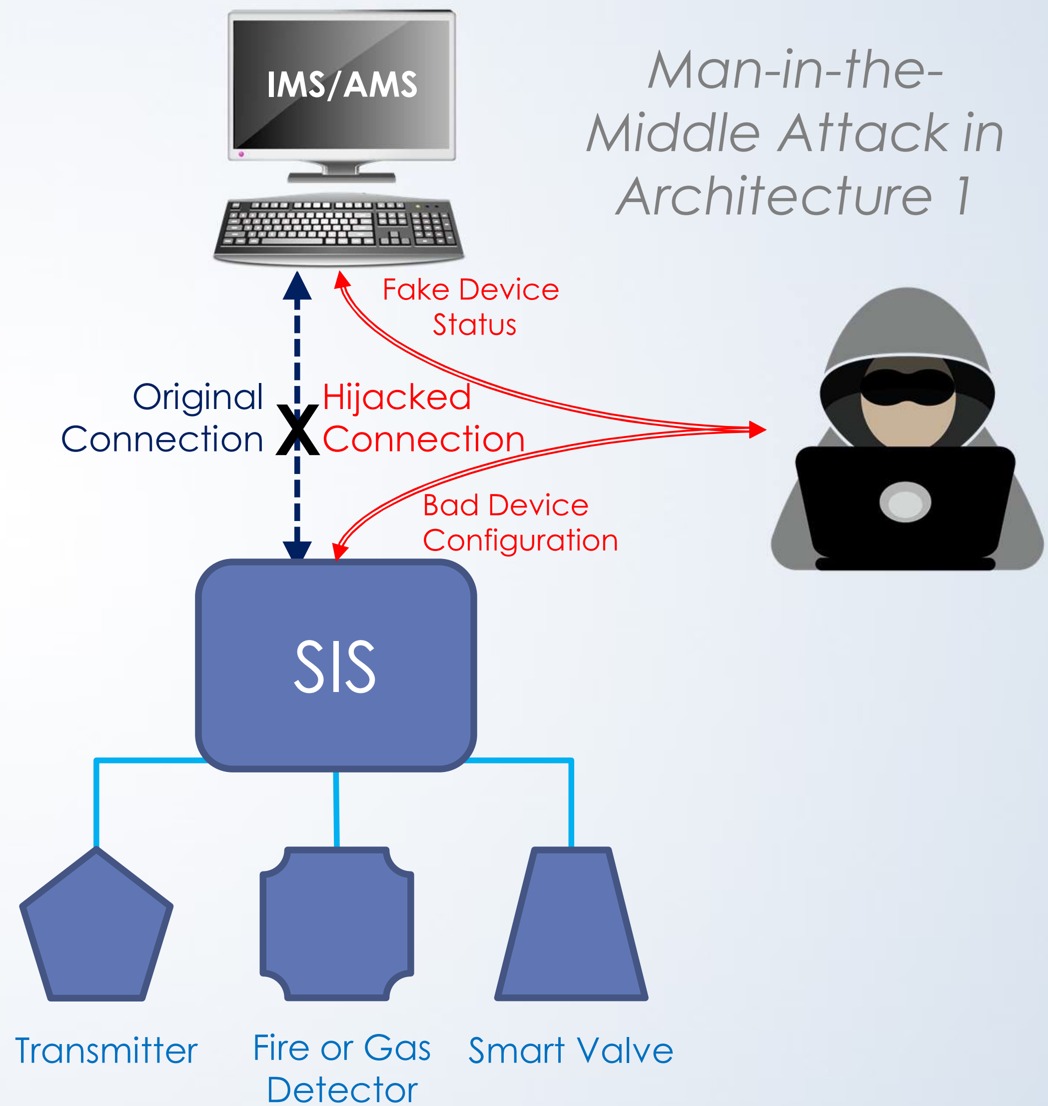
Hypothesis Revisited

An architecture in which an SIS mediates communications between an IMS/AMS and the devices it manages can better mitigate device vulnerabilities than can an architecture in which the IMS/AMS communicates with the devices through a MUX.



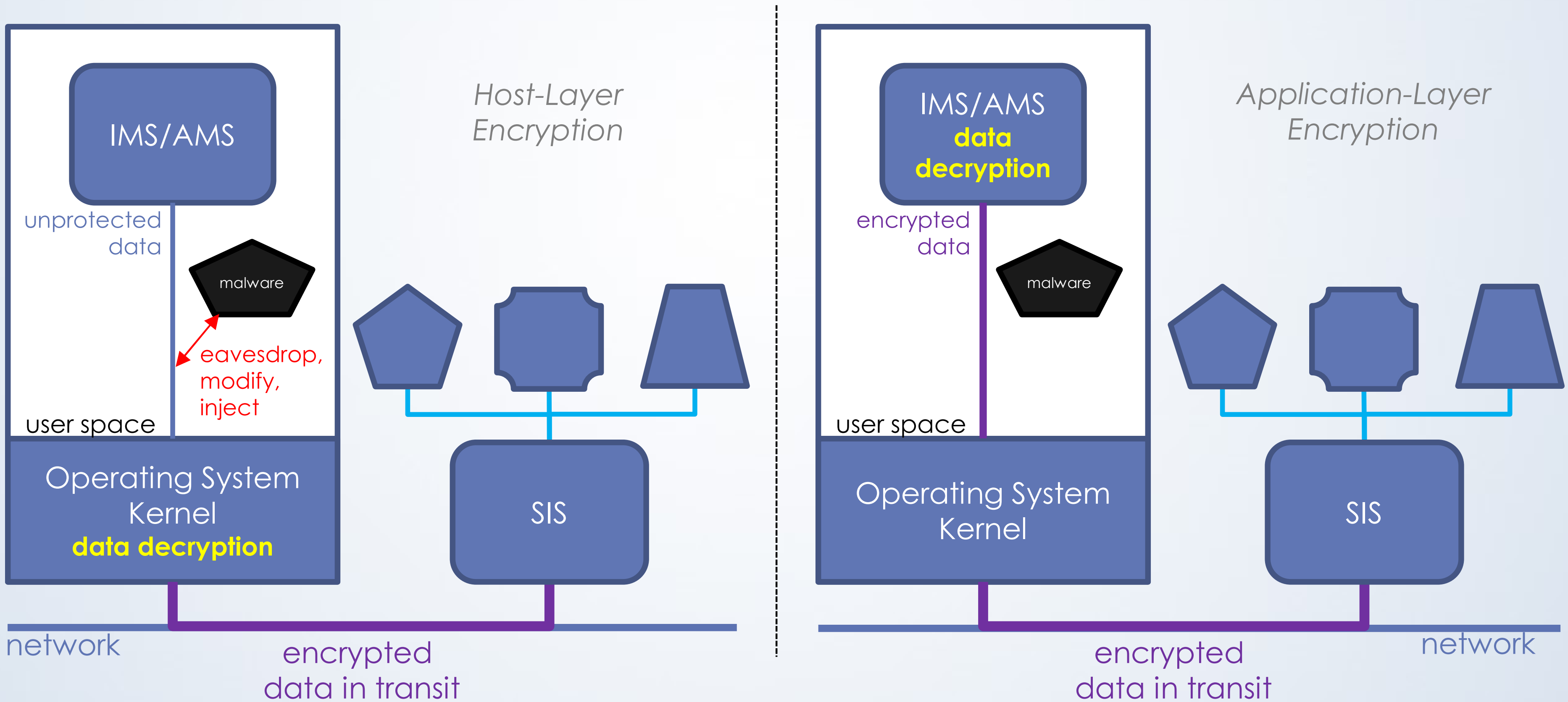
SIS-Mediated Safety Systems Communications

- IP-based communications were implemented using either HART-IP or vendor proprietary protocols
- All protocols were clear text by default
- Some solutions included an option for encrypted communications
- In most cases, when using unencrypted communications, the test team was able to hijack communications in one or both directions. This enabled
  - Changing device commands in transit
  - Injecting new device commands
  - Sending false information to the IMS/AMS
- Enabling encrypted comms between the SIS and IMS/AMS stopped these attacks when launched from points on the network



SIS-Mediated Safety Systems Communications

- Network access is not required to do this
- The same thing can be done using malware directly on the IMS/AMS platform depending on how the encryption is implemented



Findings Summary

- The HART protocol used by safety instruments is inherently insecure
- Attackers can make unauthorized harmful changes to devices, if not hardware write-protected
  - Software write-protections are bypassable
  - Devices do not authenticate sources of HART commands received
- The industry practice of DTM and DD distribution provides a path for attackers to install malware on the trusted IMS/AMS platform
- SIS solutions have protective features that significantly reduce the risk of unauthorized device modifications over that of a MUX-based solution
  - These features must be enabled manually

Safety Instrumentation and Management

Recommendations

Mitigation Roadmap

SHORT-TERM

Hardware write-protect

Cybersecurity best practice protections for IMS/AMS

Safe DTM handling procedures

MID-TERM

Use SIS to mediate device comms

Apply existing SIS protections

Encrypt communications

Robust monitoring

Risk analysis

Robust security policy

Training

LONG-TERM

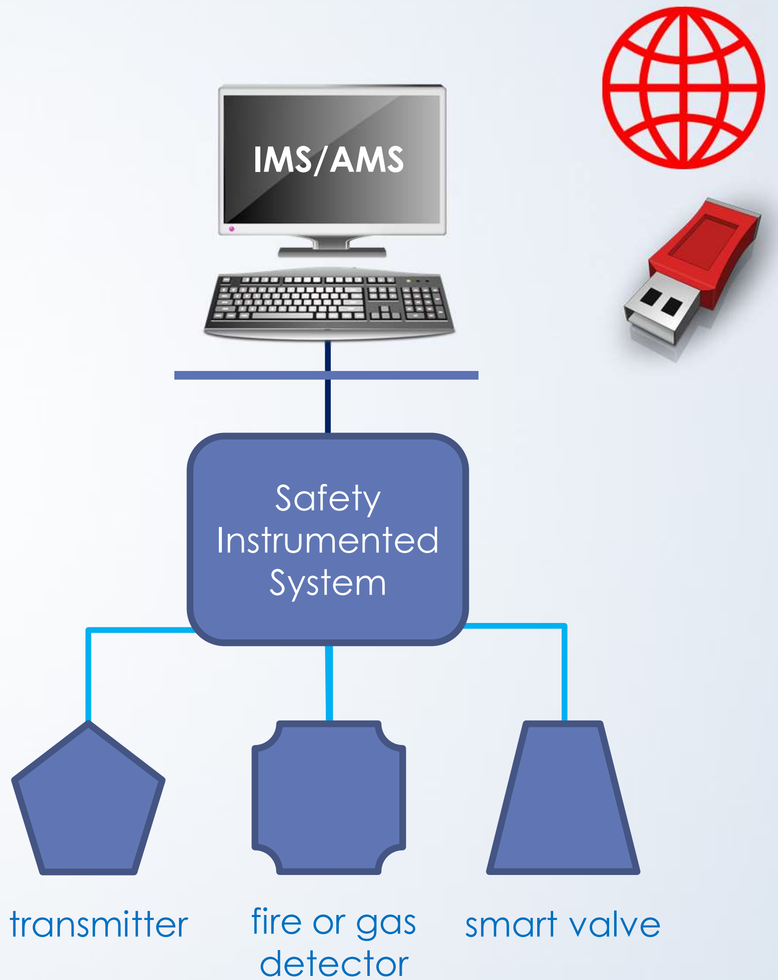
Standards improvements

Product improvements and deployment

Short-Term

Asset Owners: Strategies to Prevent Unauthorized Device Modifications

- Reminder: malware can be installed by
  - Connecting directly to the Internet
  - Using a USB stick to transport software updates across an “air gap”



Short-Term

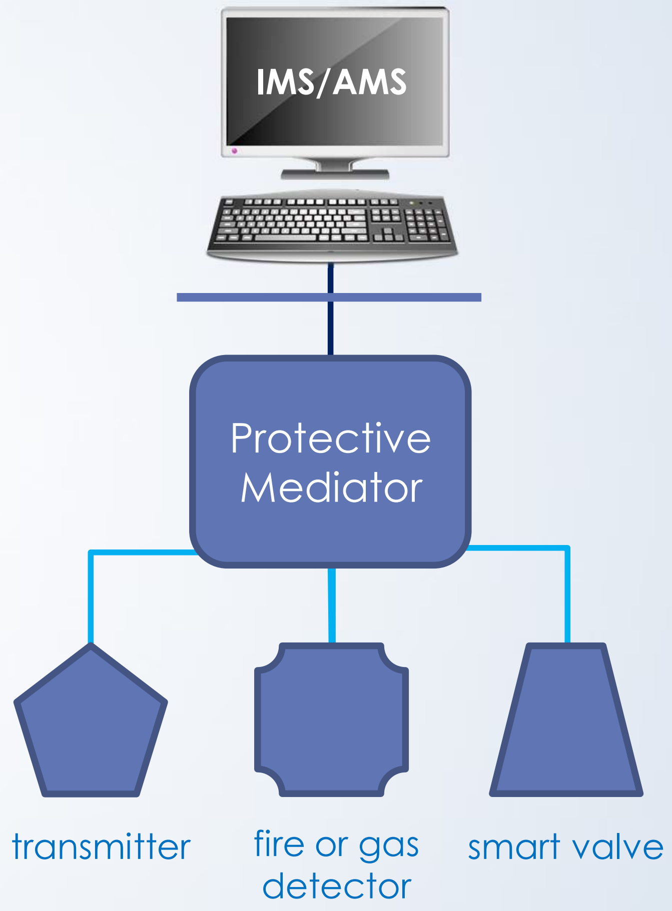
Asset Owners: Strategies to Prevent Unauthorized Device Modifications

- Don’t allow writing to device during normal operations
  - Place write-protections as close to the device as possible
    - Use hardware-based device write-protections where they exist
    - When using software-based device write-protections, always use additional protections
  - Only unblock these commands when device configurations must be modified

Mid-Term

Asset Owners: Strategies to Prevent Unauthorized Device Modifications

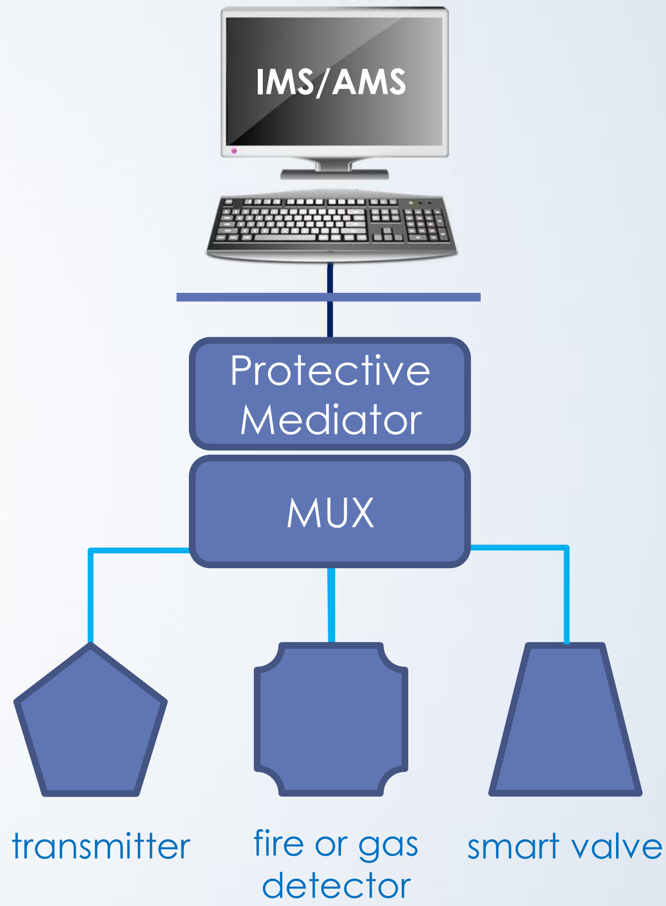
- Use a *protective mediator* between devices and the network
  - Block device write commands at the device mediator
    - Common and universal writes
    - Device specific commands*
  - Use the SIS to mediate device communications



Mid-Term

Asset Owners: Strategies to Prevent Unauthorized Device Modifications

- Use a *protective mediator* between devices and the network
  - Block device write commands at the device mediator
    - Common and universal writes
    - Device specific commands*
  - Use the SIS to mediate device communications
  - When using a MUX
    - If ethernet-based, place a mediating firewall between the MUX and the network
    - If serial-based, the IMS/AMS is the mediator; its protection is imperative



Mid-Term

Asset Owners: Strategies to Prevent Unauthorized Device Modifications

- Only permit authorized hosts and processes to send commands to devices
  - Require authentication to the device mediator by the connecting process/host
  - Block unauthorized connection attempts at the device mediator
  - Encrypt communications between authorized hosts and the device mediator to prevent communications confidentiality and integrity attacks

Short-Term

Asset Owners: Strategies to Prevent Unauthorized Device Modifications

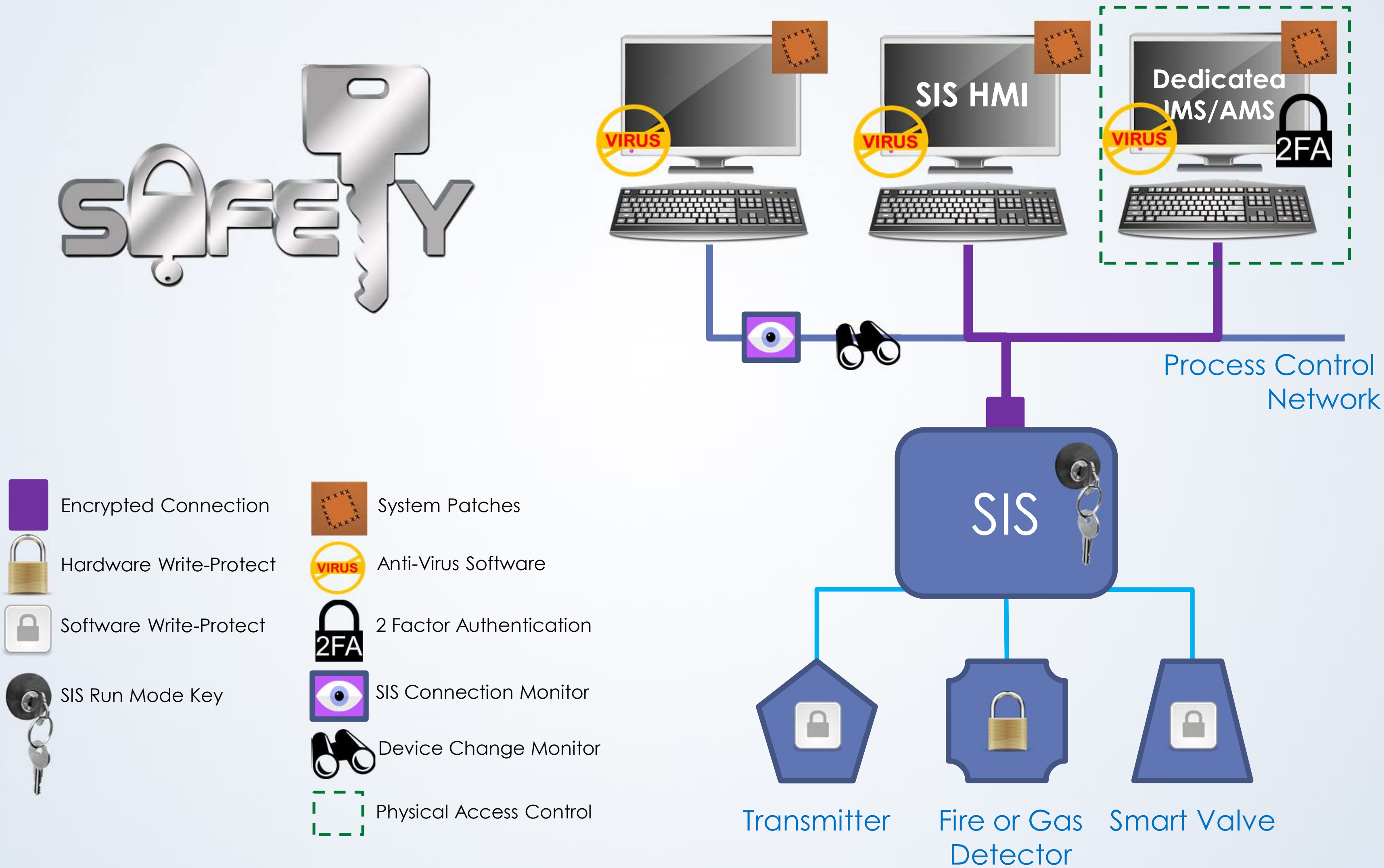
- Protect the IMS/AMS
  - The IMS/AMS is a trusted component and can be used by adversaries to attack the system
  - Use cybersecurity best practices, e.g.,
    - Strong, accountable authentication and access control (including physical access)
    - Remove unneeded software
    - Keep system patches and antivirus protection up to date
    - Host-based firewall, block inbound network connections
    - Process, filesystem, and registry integrity monitoring
  - Use good software installation practices
    - Vet DTMs and DDs that are already deployed and being used
    - Where possible, use DDs instead of DTMs
    - Only install software (including vendor DTMs and DDs) from trusted vendors and verify software and configuration file integrity prior to installation
    - Use only trusted media for transfer

Mid-Term

Asset Owners: Strategies to Detect Unauthorized Device Modifications

- Log all connection attempts made to device mediator; alert on unauthorized sources
- Log all update commands received by device mediator
- Use independent device state monitoring
  - Periodically poll device states and compare with expected states; log and alert on deltas
  - Confirm state information displayed in IMS/AMS, and alarm if IMS/AMS shows incorrect state for any device

Example Fortified SIS-Mediated Safety System



Mitigation Roadmap

SHORT-TERM

Hardware write-protect

Cybersecurity best practice protections for IMS/AMS

Safe DTM handling procedures

MID-TERM

Use SIS to mediate device comms

Apply existing SIS protections

Encrypt communications

Robust monitoring

Risk analysis

Robust security policy

Training

LONG-TERM

Standards improvements

Product improvements and deployment

Safety Instrumentation and Management

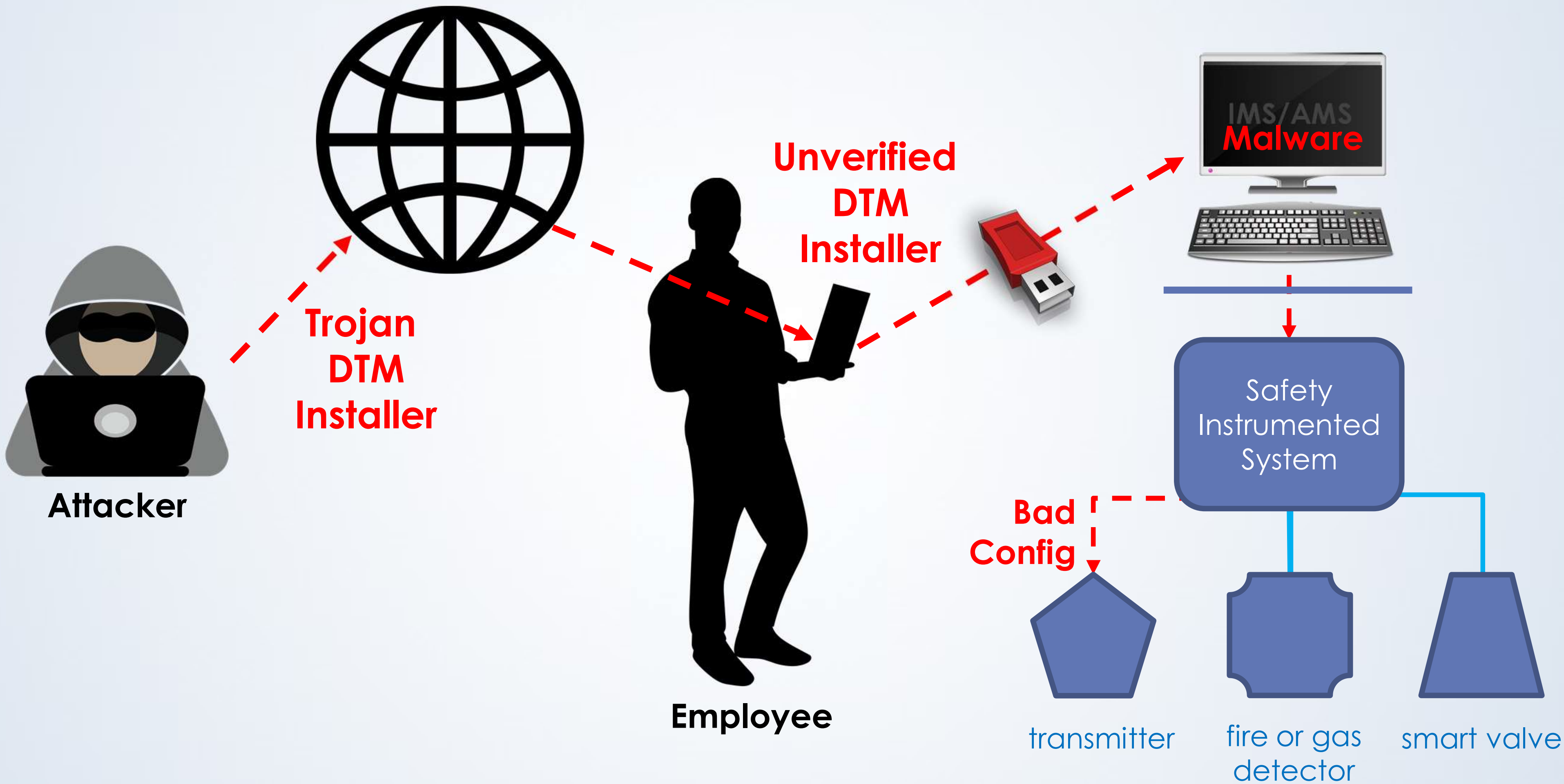
Conclusions

Summary Findings

- Numerous consequential and reoccurring exploitable weaknesses found across all four assessments, due to
  - Unchecked HART passthrough
  - HART and HART-IP* have no built-in security concepts
  - Devices do not authenticate the source of HART commands before execution
  - Industry uses unverified 3rd party DTMs downloaded from the Internet

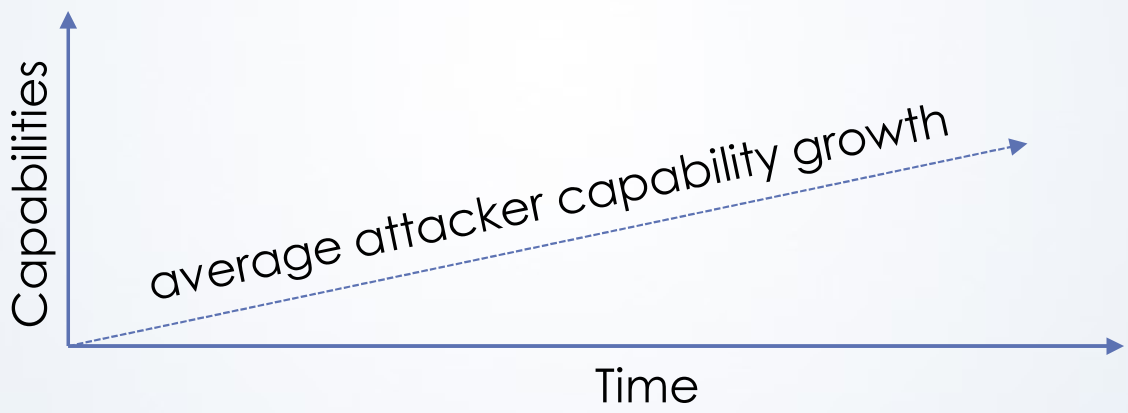
*As of July 2020, there is a new secure HART-IP standard that encrypts communications at the application layer

The Supply Chain Threat



Threat of Attack

- Attacks such as these do not require a high degree of "sophistication" today
- Yesterday's sophisticated attacks are today's average attacks



- Bottom line: low to moderately skilled attackers can make harmful changes at will and evade detection

Conclusion

- The safety system environment is vulnerable to malicious attacks that *may be undetectable* in practice.

- Extreme caution should be taken before introducing any software into this environment.

These are common, preventable issues

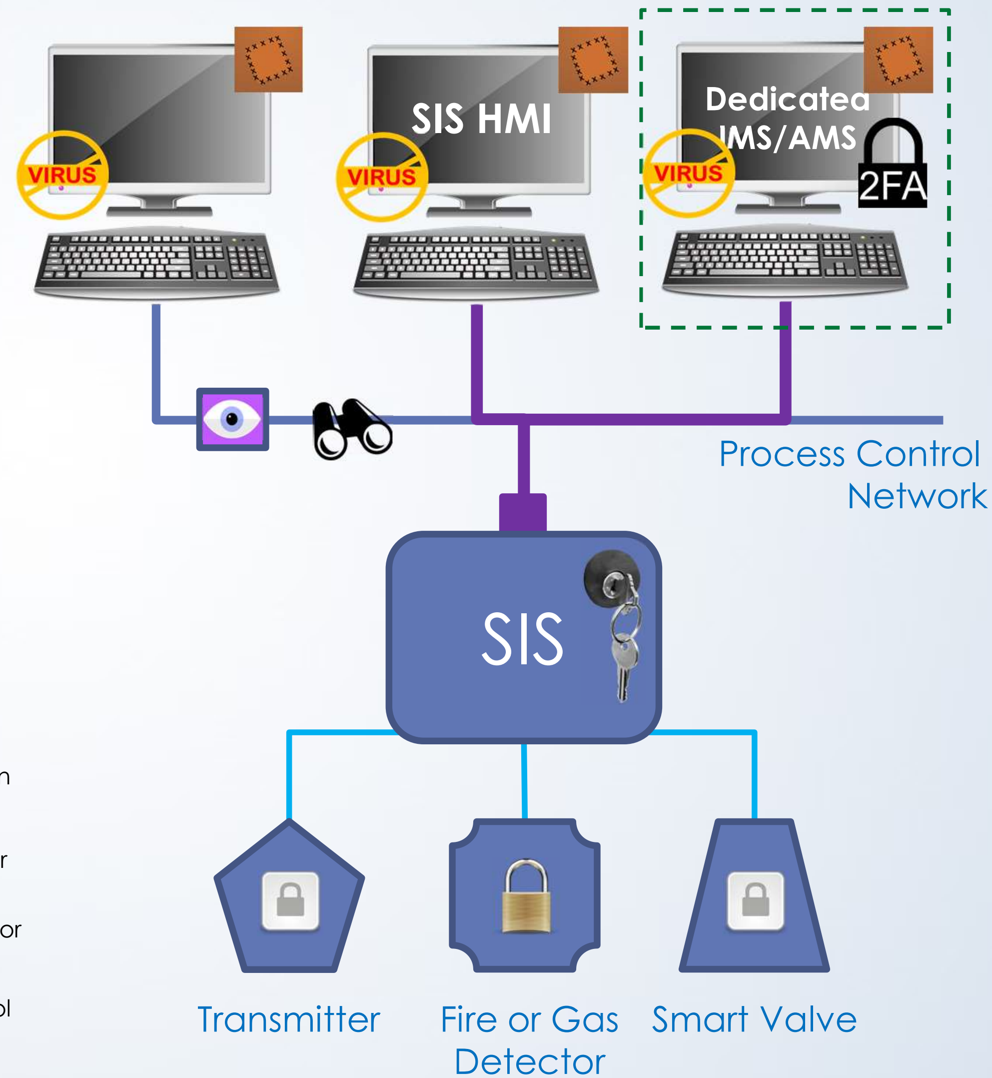
- These are not zero-day software vulnerabilities
- All issues found are documented in the *MITRE Common Weakness* Enumeration for architectures
- If cybersecurity best practices were followed, most of these issues simply would not exist

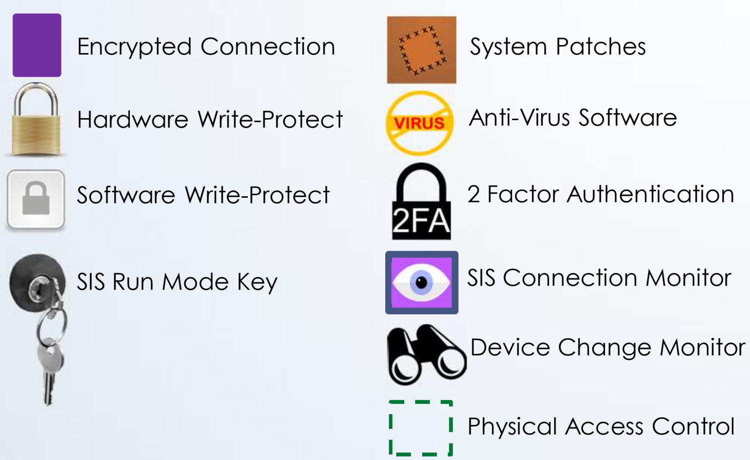
Lessons on Attack Countermeasures

- There is no single countermeasure that will protect 100% of all safety systems
- Device hardware-based write-protections provide the best protection, but 66% of sampled devices did not have hardware protections
- Layered protective measures are needed and will reduce much of the risk

Goal: Fortified Safety Systems

Example Fortified Safety System Architecture 1





Mitigation Roadmap

SHORT-TERM

Hardware write-protect

Cybersecurity best practice protections for IMS/AMS

Safe DTM handling procedures

MID-TERM

Use SIS to mediate device comms

Apply existing SIS protections

Encrypt communications

Robust monitoring

Risk analysis

Robust security policy

Training

LONG-TERM

Standards improvements

Product improvements and deployment

Read the full Project 12 Final Report

LOGIIC.org