STPA-Sec Applied Before the SolarWinds Attack

Michael Bear (BAE Systems)
John Thomas (MIT)
Bill Young (USAF)

MIT STAMP/STPA Workshop
June 25 2021

SYSTEM SECURITY ENGINEERING

IDENTIFY • PROTECT • DETECT • RESPOND • RECOVER

Acknowledgements

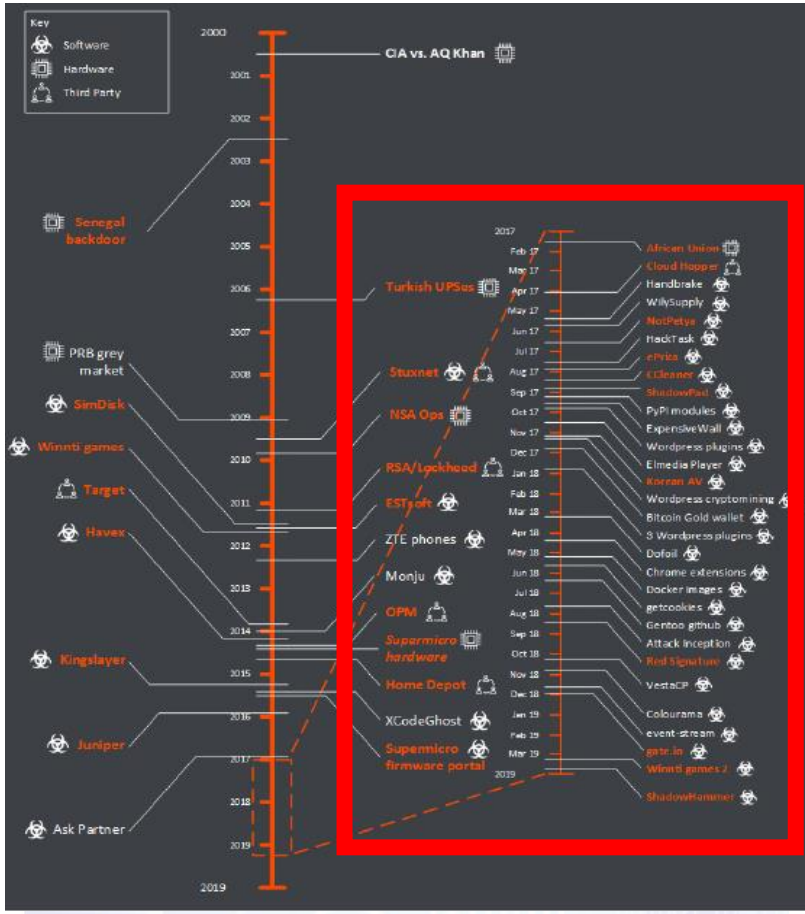
- Ryan Ickes (Navy)

Outline

- Background
- STPA/STPA-Sec for Supply Chain Security
- STPA/STPA-Sec Results Compared to SolarWinds Attack
- Summary

Background

- DoD Customer sponsored an STPA-Sec pilot before the SolarWinds attack
  - Goal: Evaluate STPA-Sec applicability to DoD supply chains. Identify supply chain vulnerabilities and improvements.
- Oct 2020: STPA-Sec identified a set of vulnerabilities. DoD Customer updated their processes and controls to eliminate vulnerabilities based on STPA-Sec results
- STPA-Sec results were not implemented across all supply chains. Many DoD and commercial supply chains continued to rely on traditional approaches.
- Dec 2020: SolarWinds attacks demonstrate several severe supply chain and technical vulnerabilities.
- How did previous STPA-Sec results compare?



SolarWinds hackers accessed DHS acting secretary's emails: What you need to know

Supply Chain Facing Increased Cyber Attacks

With 50% increase in attacks from 2018, the supply chain is very vulnerable to cyber-attacks.

Disclaimer

Disclaimer

- Some STPA-Sec results still cannot be released publicly.
- Details in this presentation have been scrubbed to allow a limited public release to the extent possible.

STPA-Sec Applied to Supply Chain Big Picture

All Controls (including those from different organizations and technology) MUST Work Together or the Policy Will NOT be Successfully Enforced

Problem Framing

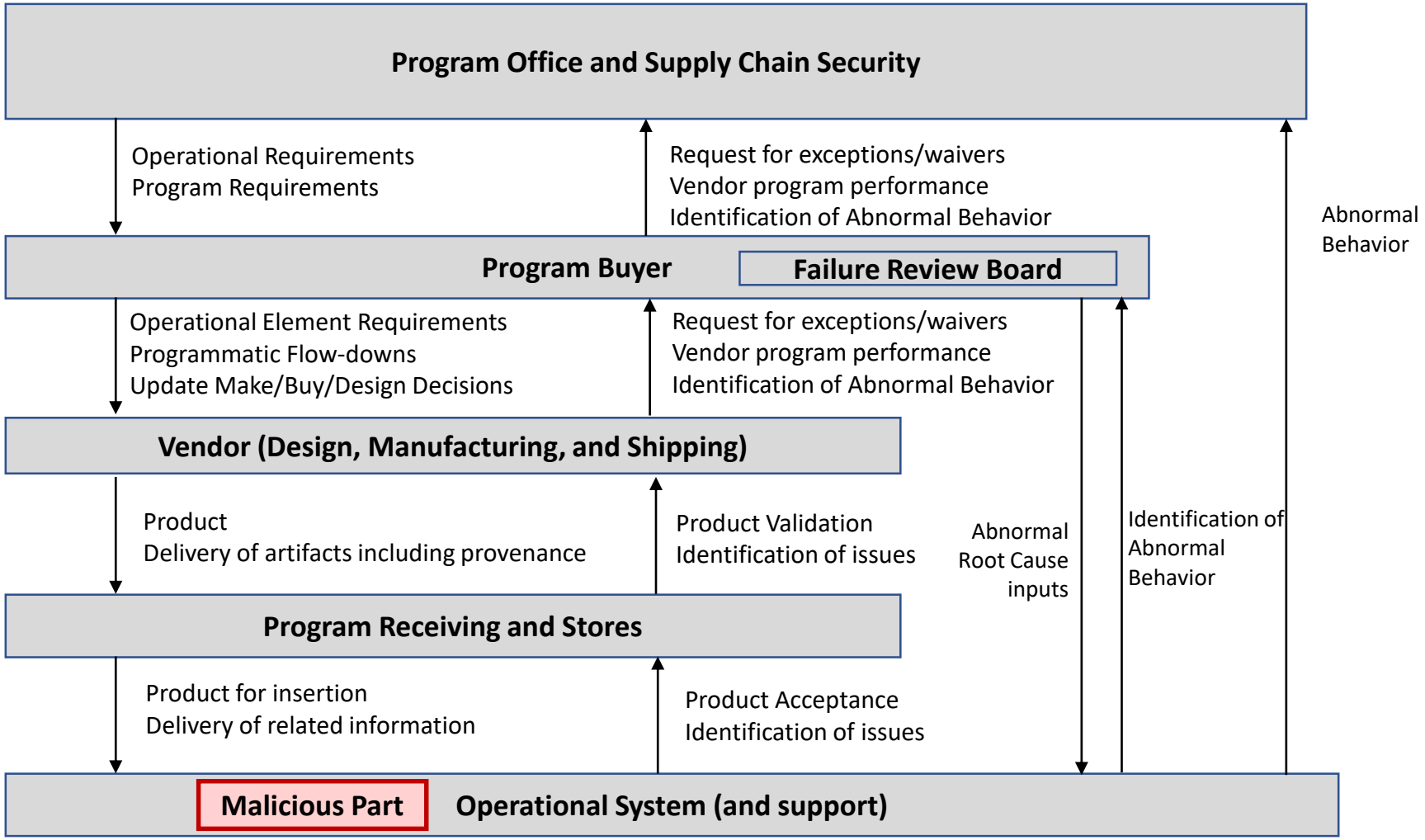
Supply Chain is a system to deliver goods and services to individuals and organizations
By Means of shipping, handling, transporting and storing components through final assembly
In order to contribute to national security and economic prosperity

Losses:
1) Loss of Intellectual Property
2) Loss of Reputation
3) Loss of Mission
4) Loss or Damage to components / products
5) Loss of Critical Protected Data

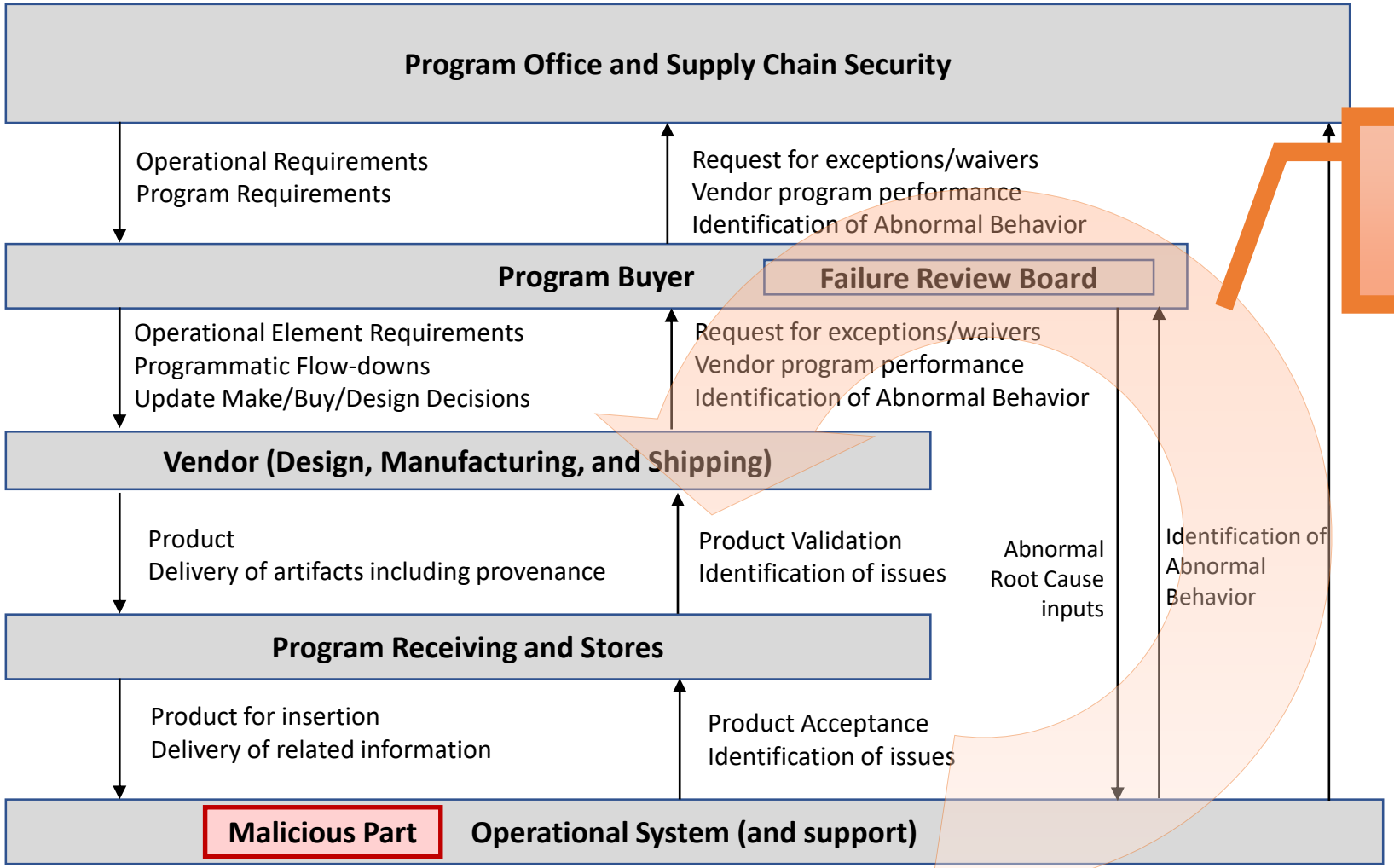
Hazards (Shipping):
… X Ships component / product that received unauthorized modification…

Ref: National Strategy For Global Supply Chain Security https://www.dhs.gov/national-strategy-global-supply-chain-security

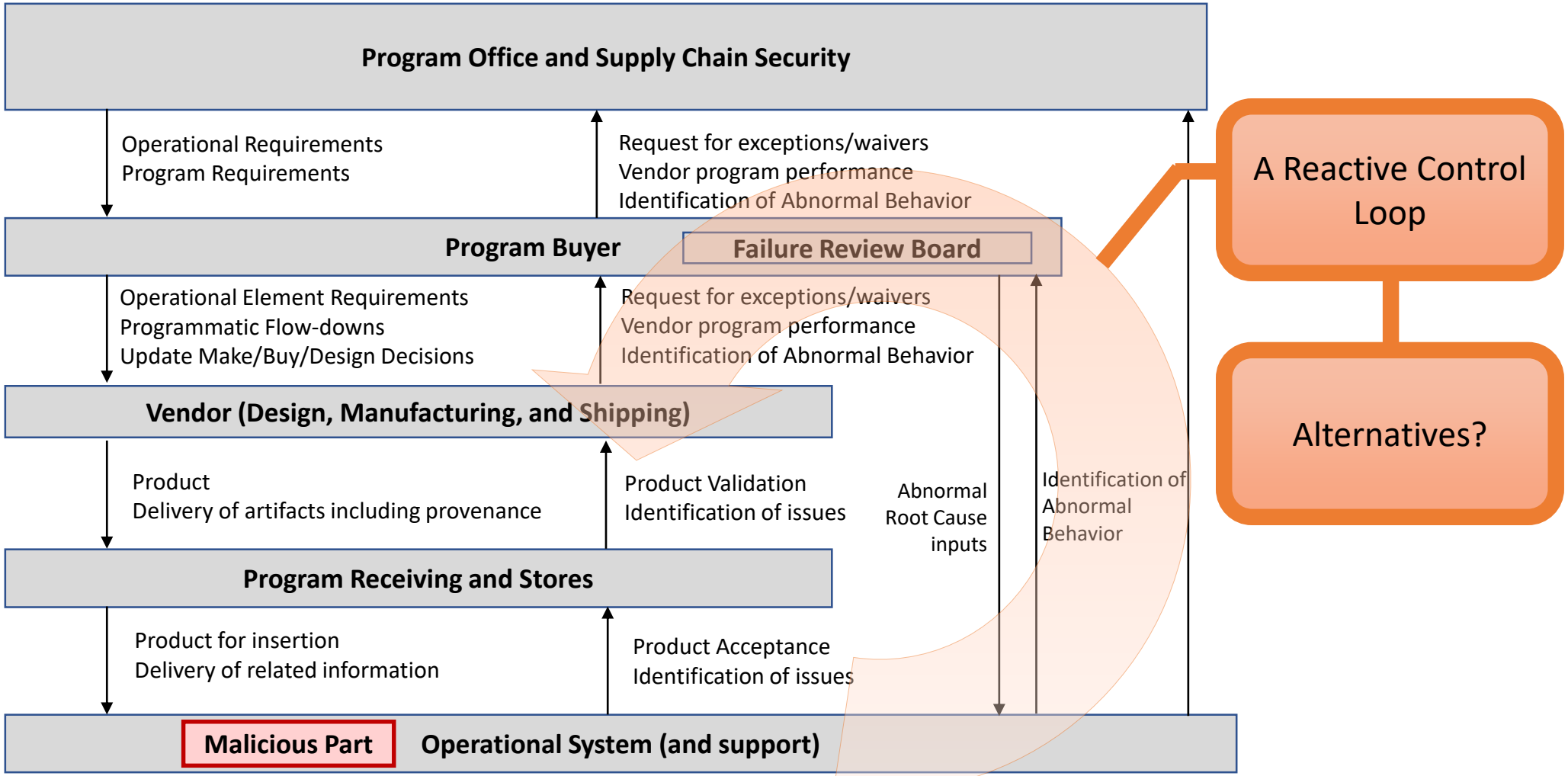
Supply Chain Control Structure



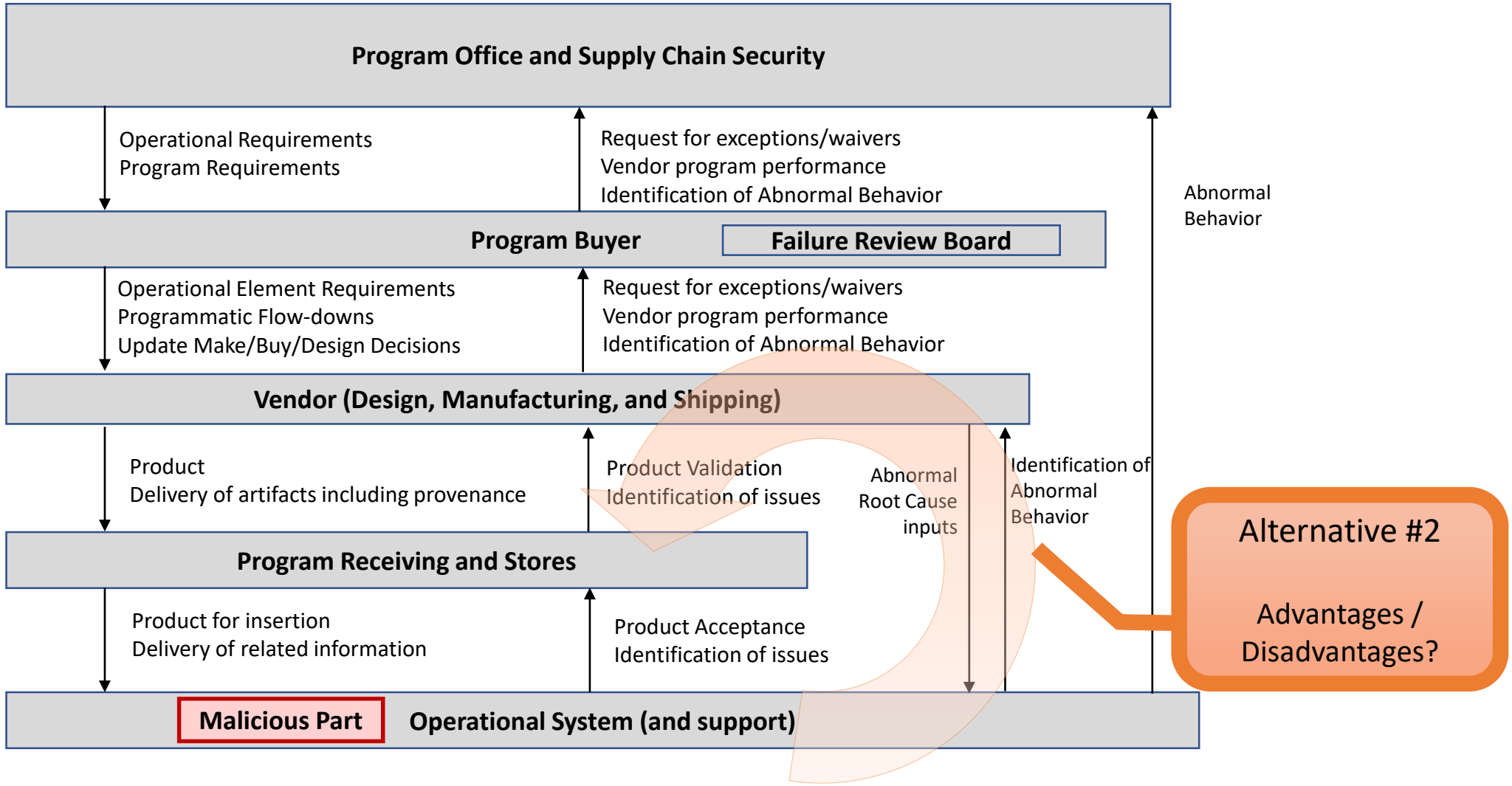
Supply Chain Control Structure



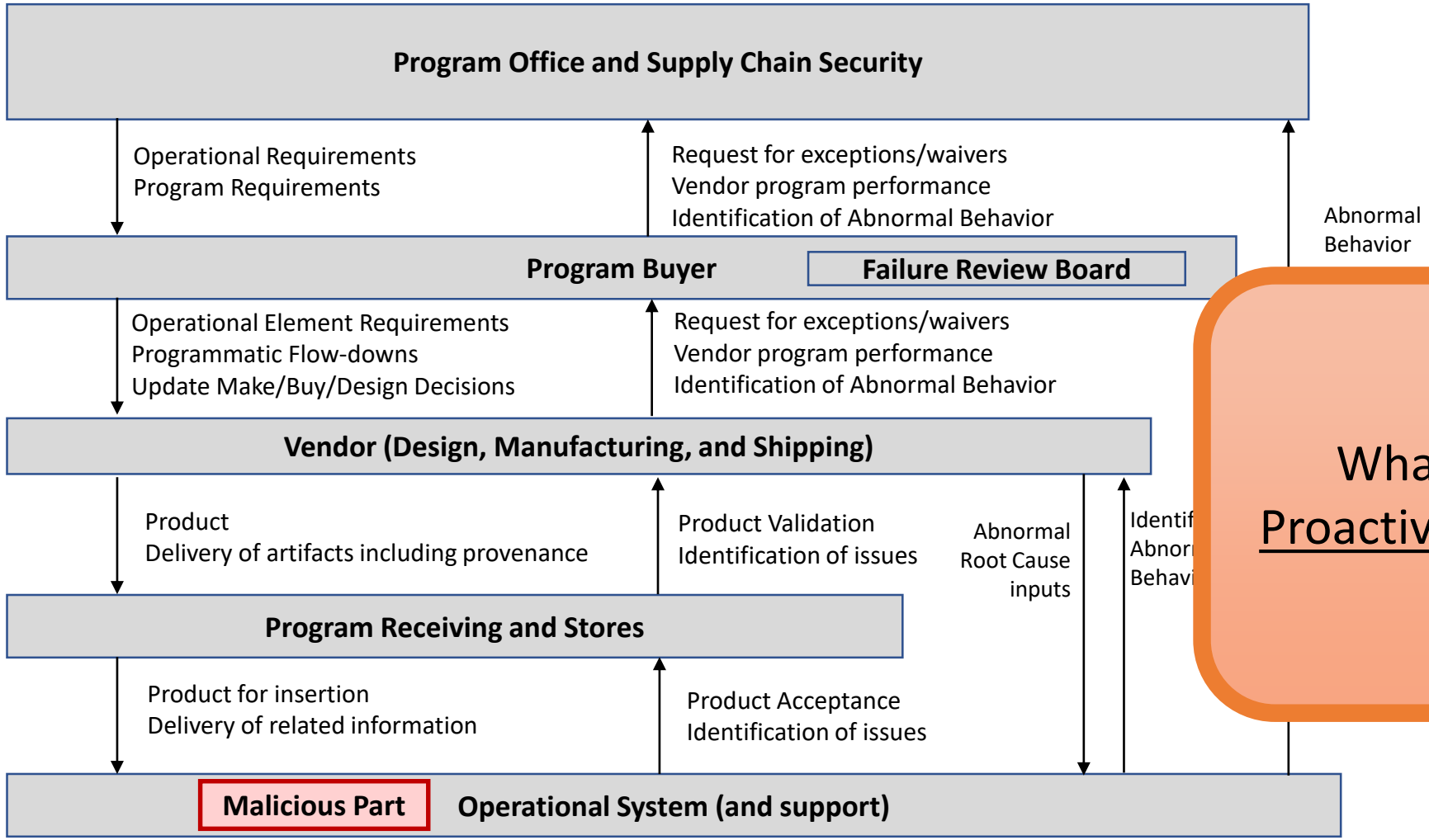
Supply Chain Control Structure



Supply Chain Control Structure

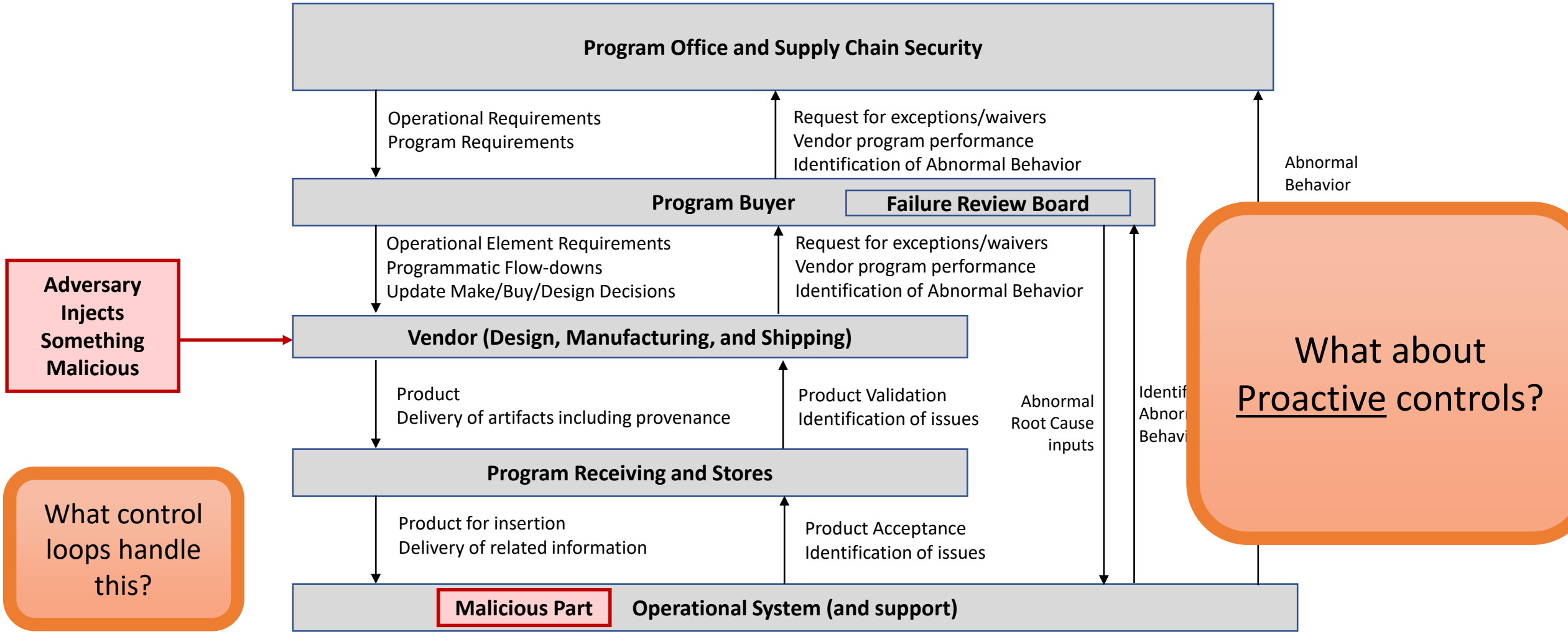


Supply Chain Control Structure

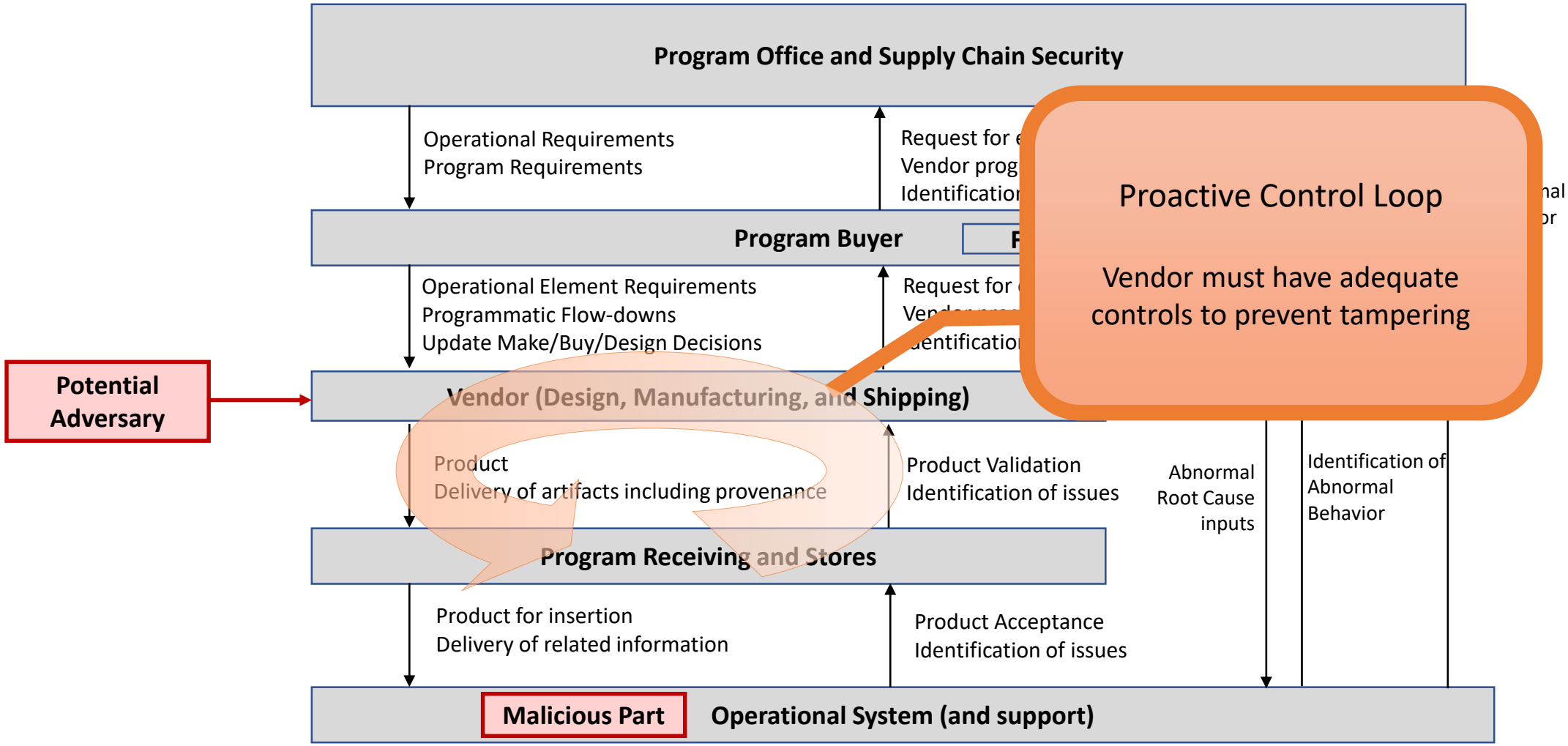


What about
Proactive controls?

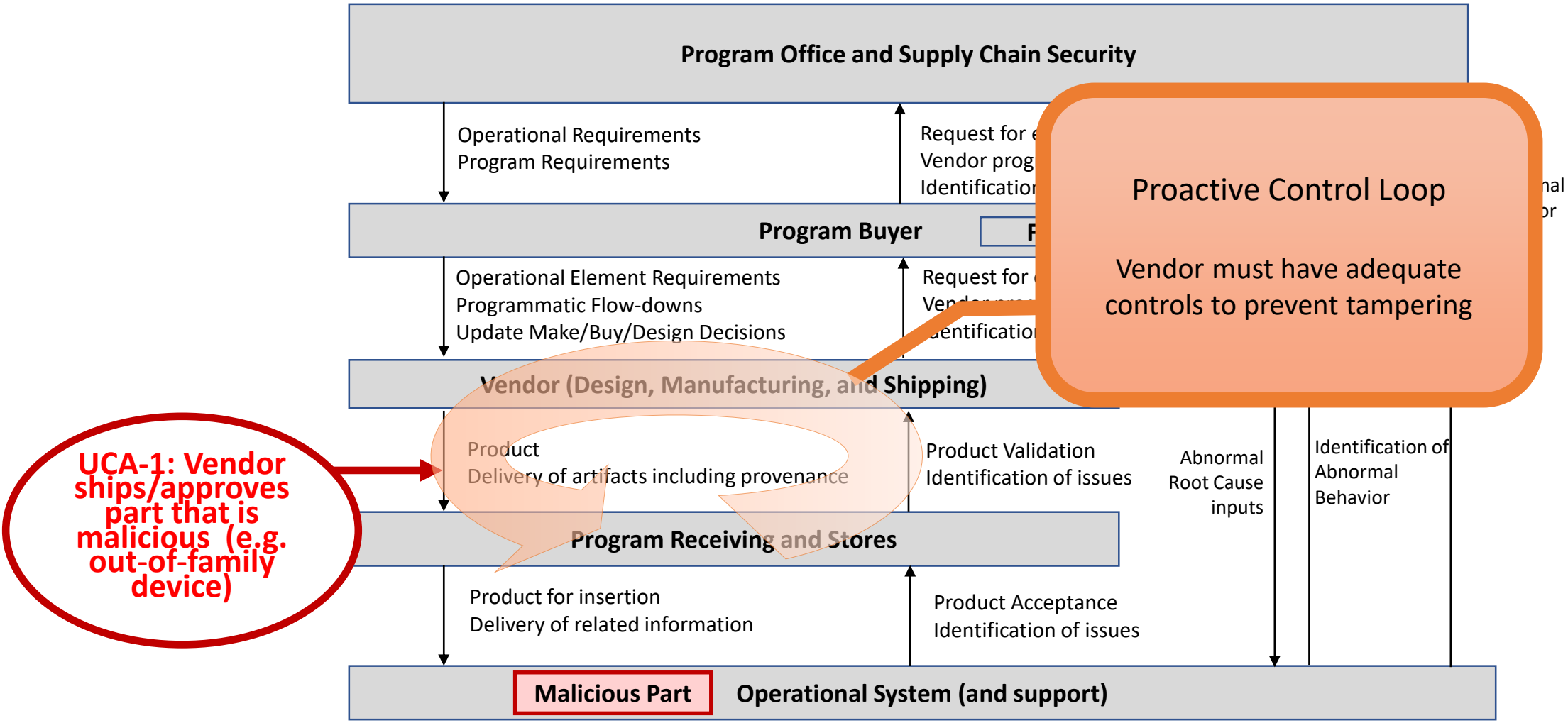
Supply Chain Control Structure



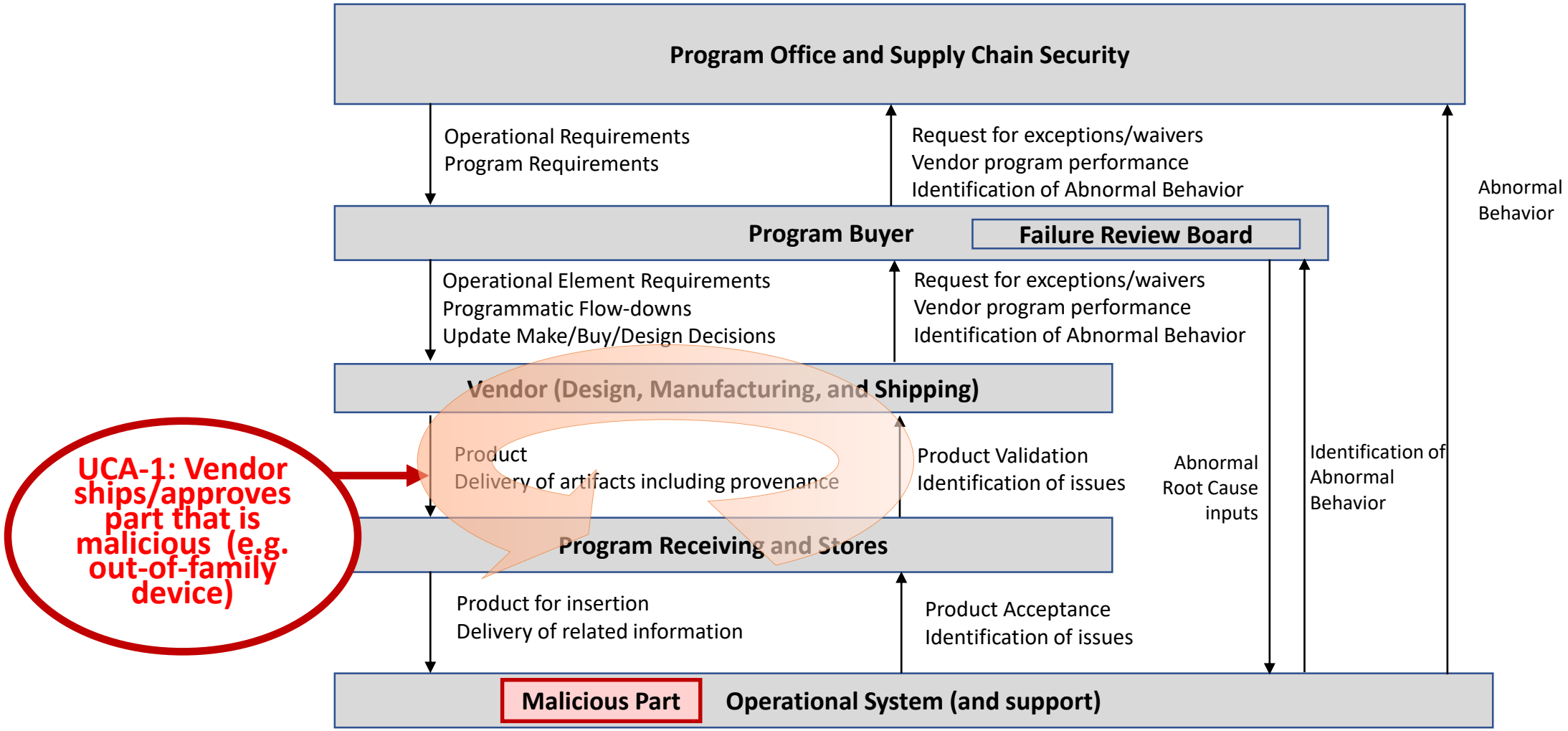
Supply Chain Control Structure



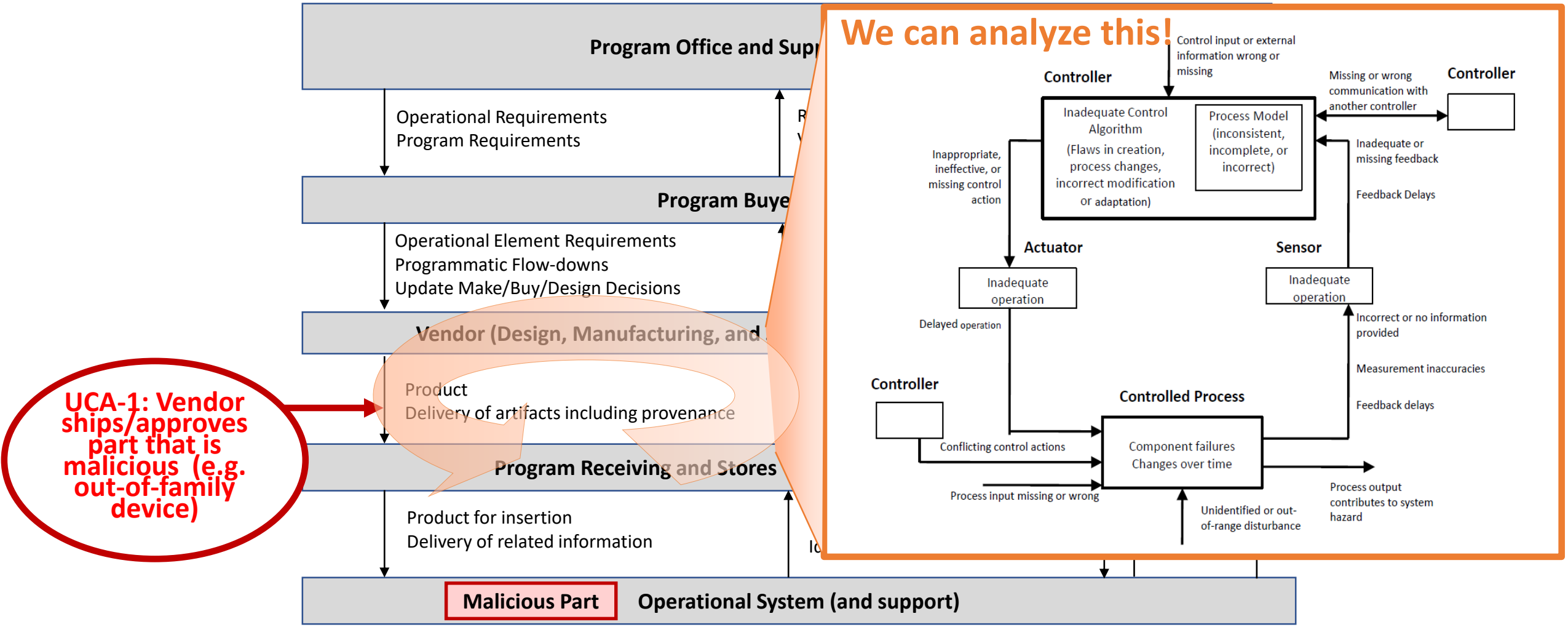
Supply Chain Control Structure



Supply Chain Control Structure

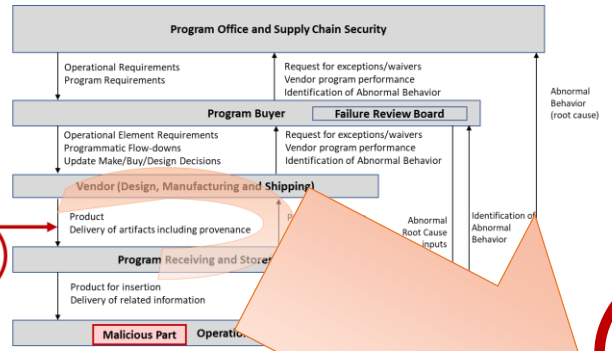


Supply Chain Control Structure



Malicious Device Insertion Overview

Approved for Distribution Statement A Public Release



Malicious Device inserted into supply

Program/Vendor Policies

Requirements update based on events

Potential Adversary

Vendor

Assumption of "Correct" device is the default

Part is procured from list of vendors (using flowed down requirements)
- Waiver to requirements - allows new vendor
- Waiver to requirements – reduces screening/acceptance criteria

UCA-1: Vendor ships/approves part that is malicious (e.g. out-of-family device)

Vendor receives incorrect confirmation that the product is validated

Vendor does not receive, or receives a delayed, warning that device is suspect

Potential Adversary

Potential Adversary

Vendor Shipping

System Actuation

System Feedback

Inventory Confirmation

Incorrect confirmation of proper operation

Delayed or missing indication of improper operation

Incorrect, missing, delayed verification of inventory and supplier

Vendor ships a part that is malicious (e.g. out-of-family device)

Potential Adversary

System Monitor

Identification of part failure

Insider to identify part needs to be replaced

PRS places malicious device in Storage

PRS does not promptly report issue with product

PRS incorrectly validates a malicious device

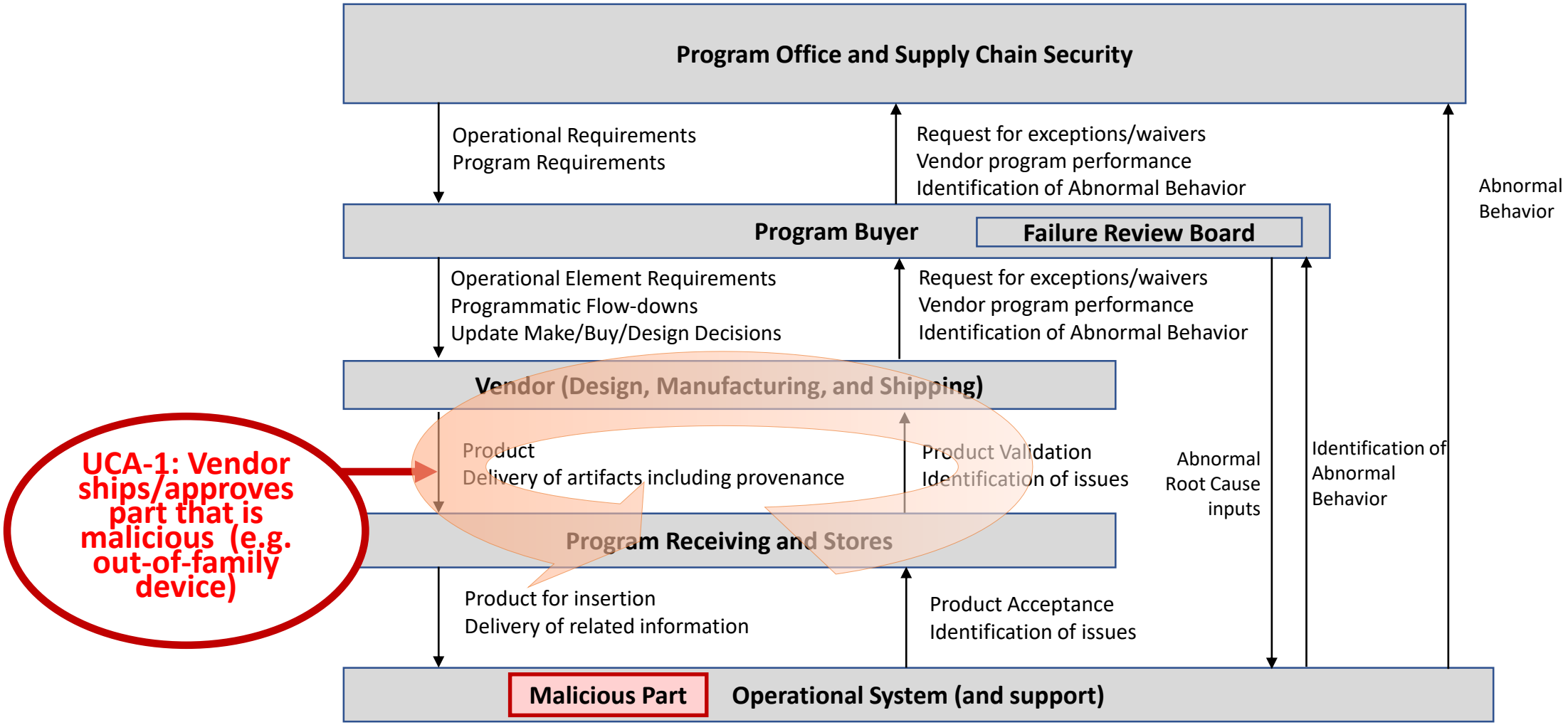
Program Receiving and Stores (PRS)

Verification of failed part - logging

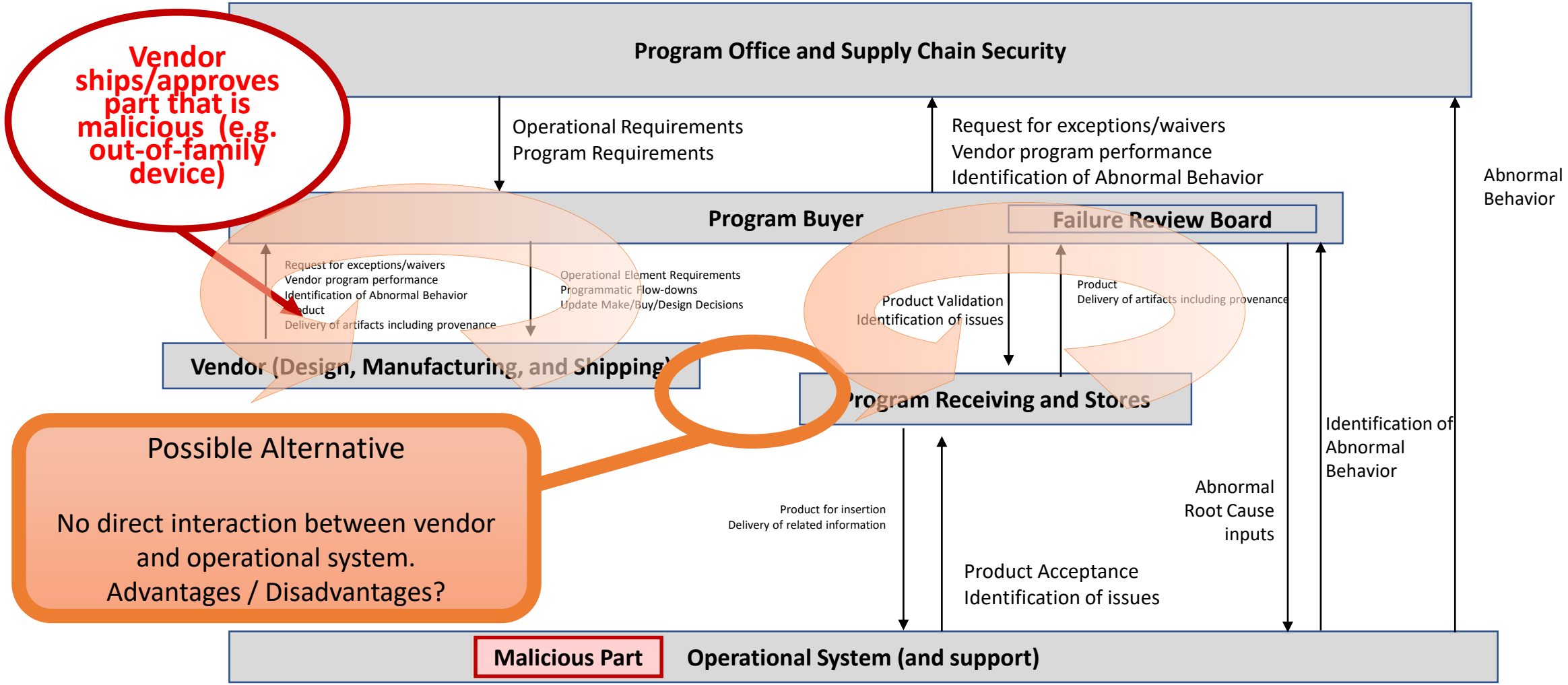
Abnormal system behavior

Pre-defined input / operational state / environmental condition to device (to activate)

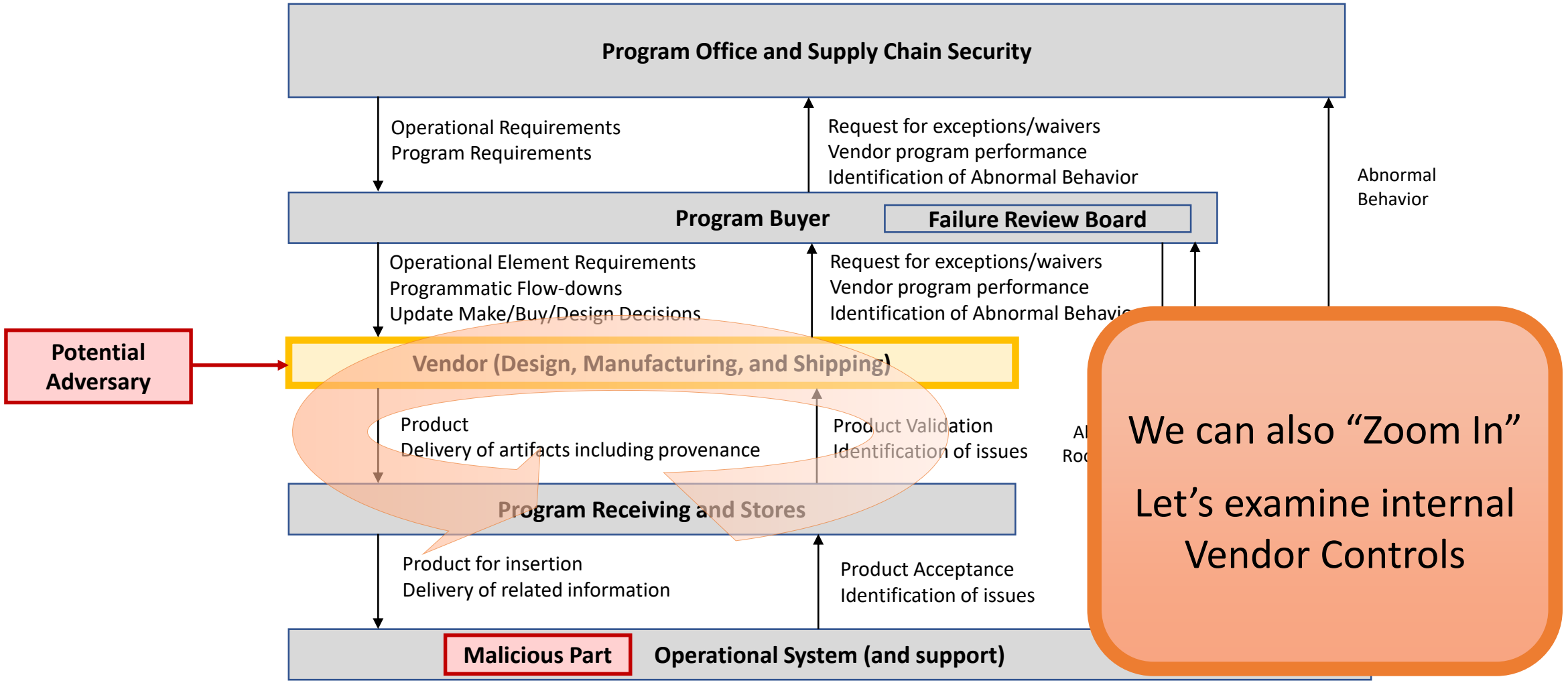
Supply Chain Control Structure



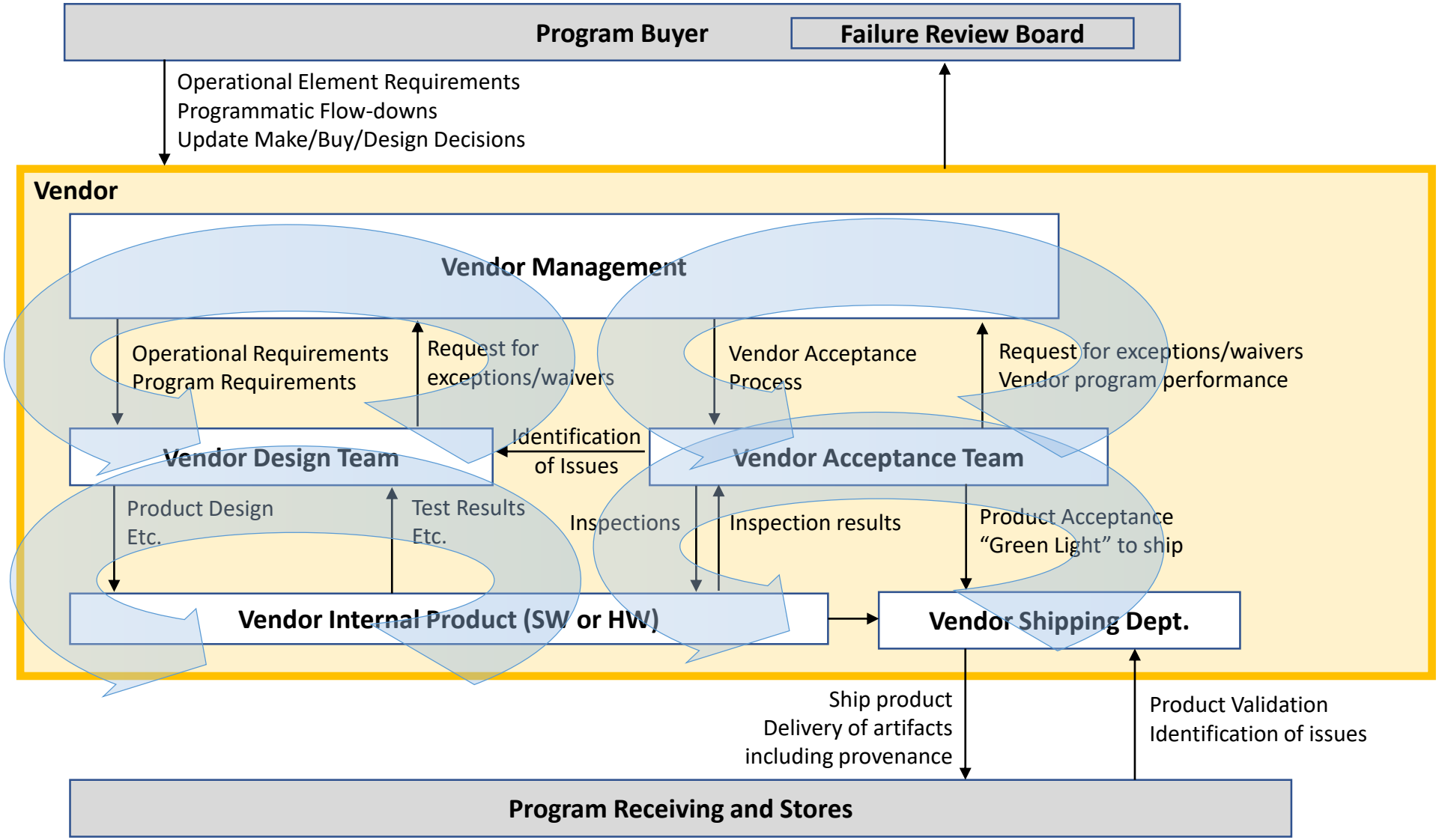
Supply Chain Control Structure



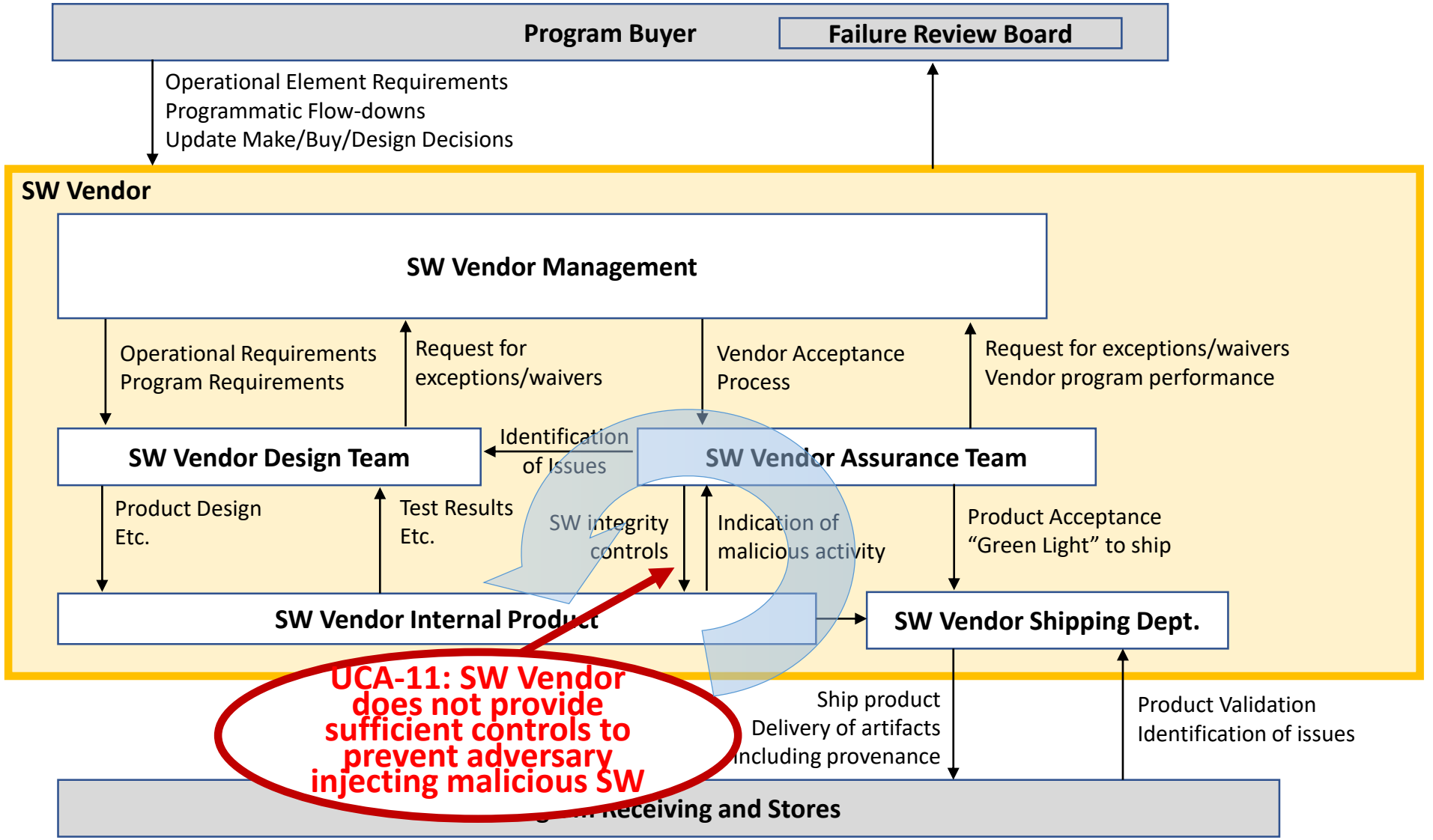
Supply Chain Control Structure



Vendor Internal Control Structure



SW Vendor Internal Control Structure



SW Vendor Internal Control Structure

Program Buyer

Failure Review Board

Operational Element Requirements
Programmatic Flow-downs
Update Make/Buy/Design Decisions

SW Vendor

SW Vendor Management

Operational Requirements
Program Requirements

Request for exceptions/waivers

Vendor Acceptanc
Process

SW Vendor Design Team

Identification of Issues

SW Vendo

Product Design
Etc.

Test Results
Etc.

SW integrity controls

Indication of malicious activity

Product Acceptance
"Green Light" to ship

SW Vendor Internal Produ

SW Vendor Shipping Dept.

Potential Adversary Injects Malicious Code

UCA-11: SW Vendor does not provide sufficient controls to prevent adversary injecting malicious SW

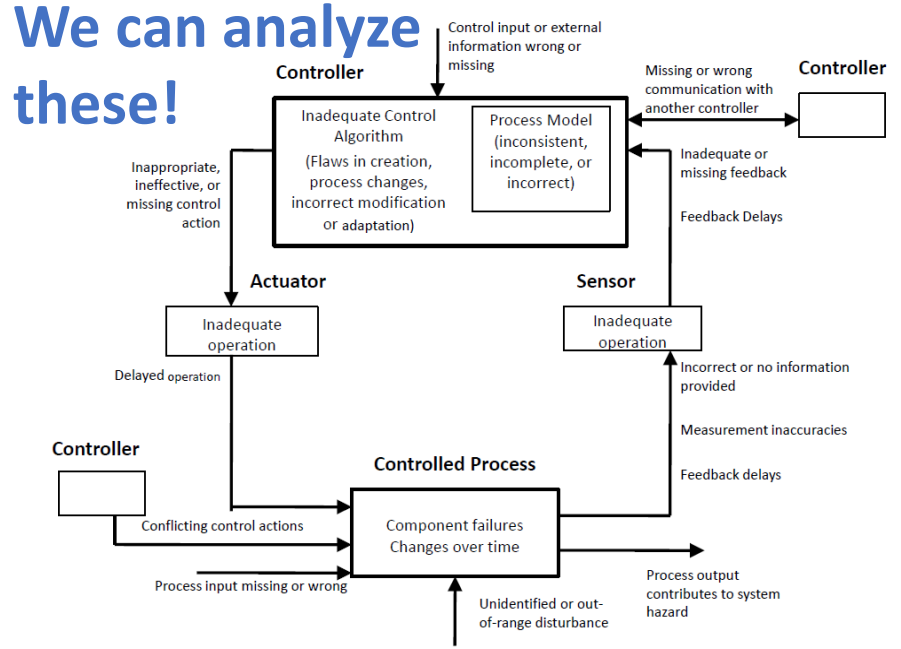
Ship product
Delivery of artifacts
including provenance

Product Validation
Identification of issues

Receiving and Stores

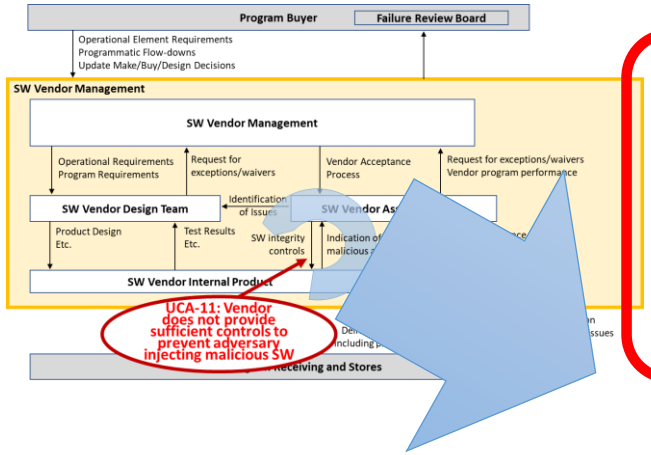
UCA-19: SW Vendor approves malicious software (e.g. out-of-family device)

We can analyze these!



Malicious Device enters Supply Chain at SW Vendor

Approved for Distribution Statement A Public Release



UCA-11: SW Vendor does not provide sufficient controls to prevent adversary injecting malicious SW (e.g. prevent adversary to replace file or "tarball")

Adversary creates replacement object(s)

Program/Vendor Policies

Requirements update based on events

SW Vendor Assurance Team (VAT)

- VAT may have flawed but approved Vendor Acceptance Process
- Weak training/procedures - Inability to identify out-of-family device in set of objects to be packaged
- Weak cyber controls – allows outsider to insert objects
- Weak TTP – allows entry of malicious file into vendor CM/DM flow or insight for later substitution in flow to system

Assumption of "Correct" process flow is the default

Potential Adversary

Without component specific information, no updated techniques

Verification process missed tampered file or file substitution

SW File Assembly Verification

Does not verify file hash, just confirms log…

SW Logging

Verification process missed abnormal assembly or assembly substitution

SW Tarball Verification

Does not verify assembly hash and other key indicators, just confirms log…

Logs are insufficient, or adversary "cleaned" logs to allow for traceability of TTP weaknesses at vendor

SW Vendor Final Acceptance Quality Control

Identification of inadequate part

Inability or lack of TTP to distinguish between original and malicious files

Unauthorized component accepted into "Git" or other CM/DM delivery tool

SW Vendor Shipping

Potential Adversary

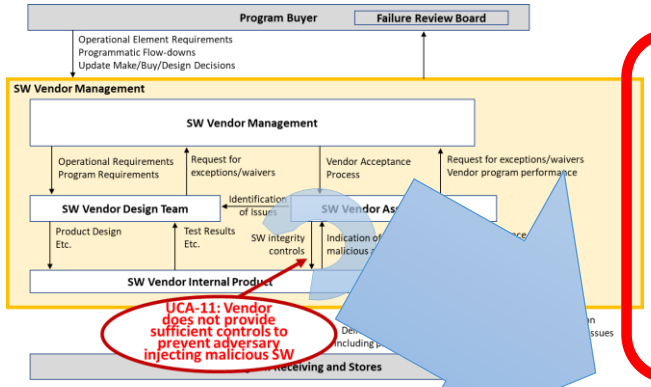
Improper "verification" of malicious files

Malicious files marked as "good" in vendor delivery logs

Provenance and HASH identified as "valid" due to weaknesses

Malicious Device enters Supply Chain at SW Vendor

Approved for Distribution Statement A Public Release



UCA-11: SW Vendor does not provide sufficient controls to prevent adversary injecting malicious SW (e.g. prevent adversary to replace file or "tarball")

Adversary creates replacement object(s)

Program/Vendor Policies

Requirements update based on events

SW Vendor Assurance Team (VAT)

- VAT may have flawed but approved Vendor Acceptance Process
- Weak training/procedures - Inability to identify out-of-family device in set of objects to be packaged
- Weak cyber controls – allows outsider to insert objects
- Weak TTP – allows entry of malicious file into vendor CM/DM flow or insight for later substitution in flow to system

Assumption of "Correct" process flow is the default

Potential Adversary

Without component specific information, no updated techniques

Vendor Internal Verification

Verification process missed tampered file or file substitution

SW File Assembly Verification

Does not verify file hash, just confirms log…

Verification process missed abnormal assembly or assembly substitution

SW Tarball Verification

Does not verify assembly hash and other key indicators, just confirms log…

SW Logging

Logs are insufficient, or adversary "cleaned" logs to allow for traceability of TTP weaknesses at vendor

SW Vendor Final Acceptance Quality Control

Identification of inadequate part

Inability or lack of TTP to distinguish between original and malicious files

Unauthorized component accepted into "Git" or other CM/DM delivery tool

SW Vendor Shipping

Potential Adversary

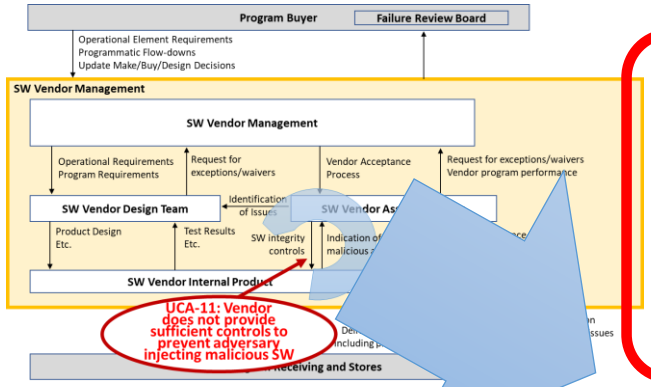
Improper "verification" of malicious files

Malicious files marked as "good" in vendor delivery logs

Provenance and HASH identified as "valid" due to weaknesses

Malicious Device enters Supply Chain at SW Vendor

Approved for Distribution Statement A Public Release



UCA-11: SW Vendor does not provide sufficient controls to prevent adversary injecting malicious SW (e.g. prevent adversary to replace file or "tarball")

Adversary creates replacement object(s)

Program/Vendor Policies

Requirements update based on events

SW Vendor Assurance Team (VAT)

- VAT may have flawed but approved Vendor Acceptance Process
- Weak training/procedures - Inability to identify out-of-family device in set of objects to be packaged
- Weak cyber controls – allows outsider to insert objects
- Weak [illegible] vend[illegible] subs[illegible]

Assumption of "Correct" process flow is the default

Potential Adversary

Without component

Unmitigated Vulnerability: SW VAT perfectly follows a flawed Vendor Acceptance Process

Vendor Internal Verification

Verification process missed tampered file or file substitution

SW File Assembly Verification

Does [illegible] hash [illegible] indica[illegible]

Verification process missed abnormal assembly or assembly substitution

SW Tarball Verification

[illegible] allow for traceability of TTP weaknesses at vendor

SW Vendor Final Acceptance Quality Control

Identification of inadequate part

Inability or lack of TTP to distinguish between original and malicious files

Unauthorized component accepted into "Git" or other CM/DM delivery tool

SW Vendor Shipping

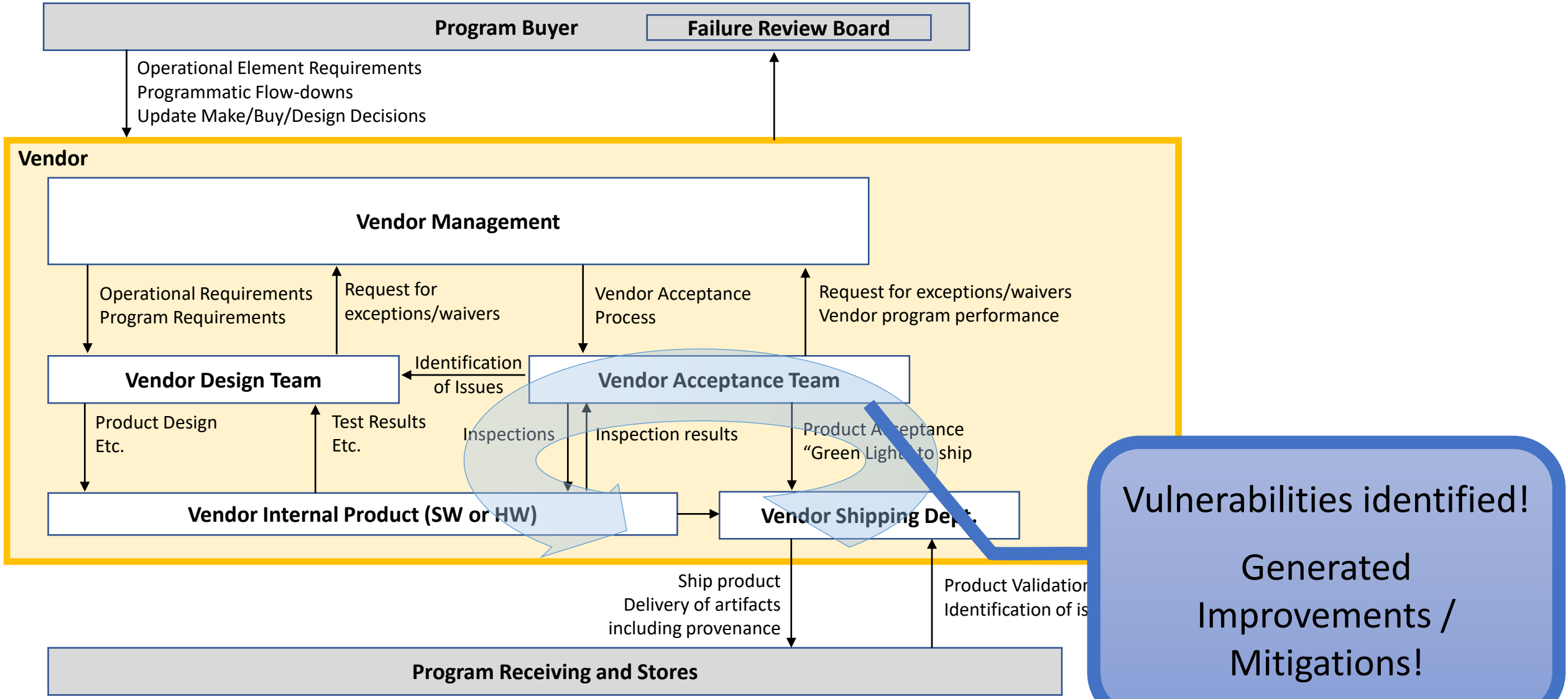
Potential Adversary

Improper "verification" of malicious files

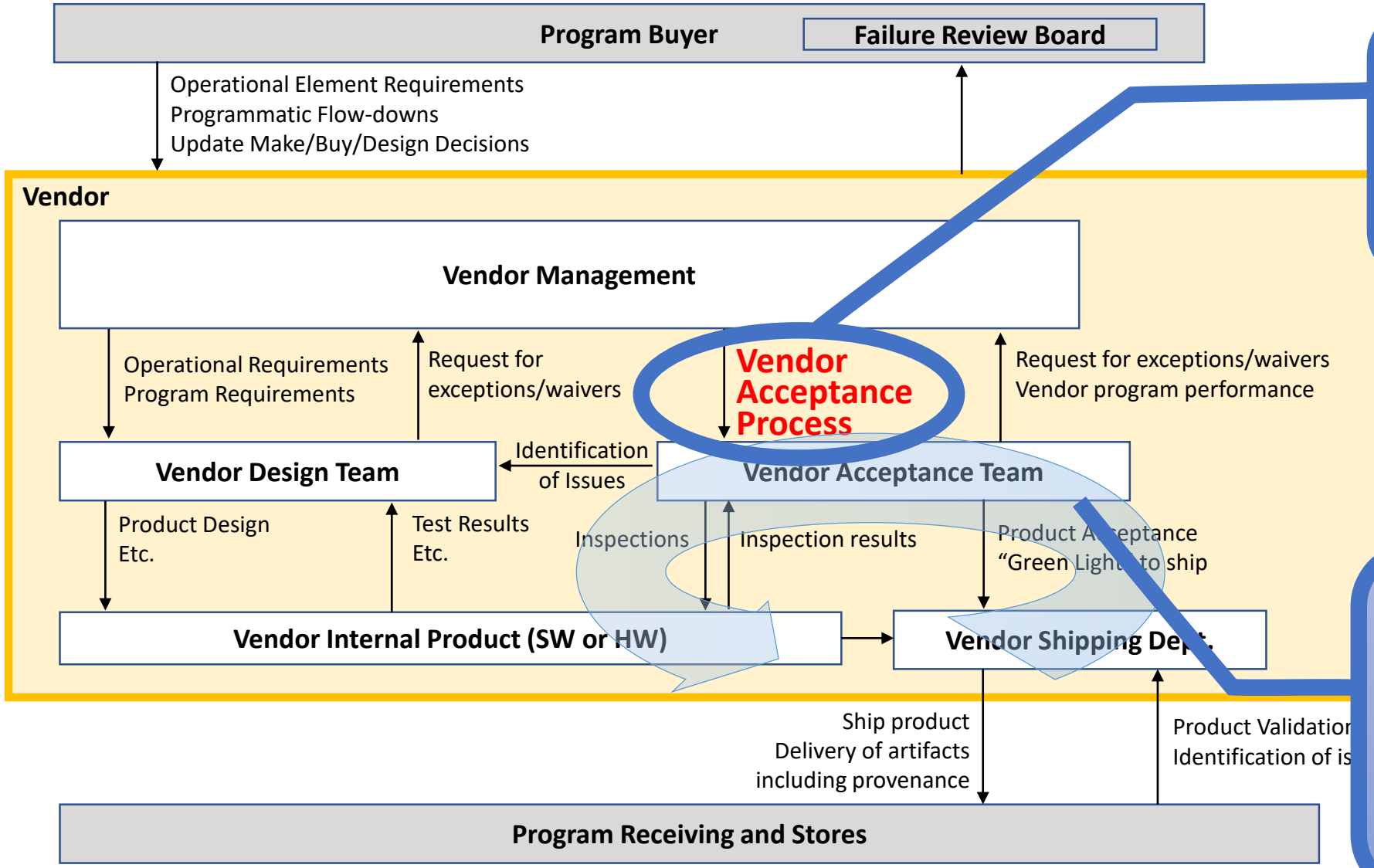
Malicious files marked as "good" in vendor delivery logs

Provenance and HASH identified as "valid" due to weaknesses

Vendor Internal Control Structure



Vendor Internal Control Structure



Unmitigated Vulnerability!

Vulnerabilities identified!

Generated Improvements / Mitigations!

Vendor Internal Control Structure

Program Buyer

Failure Review Board

Operational Element Requirements
Programmatic Flow-downs
Update Make/Buy/Design Decisions

Vendor

Vendor Management

Operational Requirements
Program Requirements

Request for
exceptions/waivers

Vendor
Acceptance
Process

Request for exc
Vendor progra

Vendor Design Team

Identification
of Issues

Vendor Acceptance Team

Product Design
Etc.

Test Results
Etc.

Inspections

Inspection results

Product Acceptan
"Green Light" to s

Vendor Internal Product (SW or HW)

Vendor Shipping De

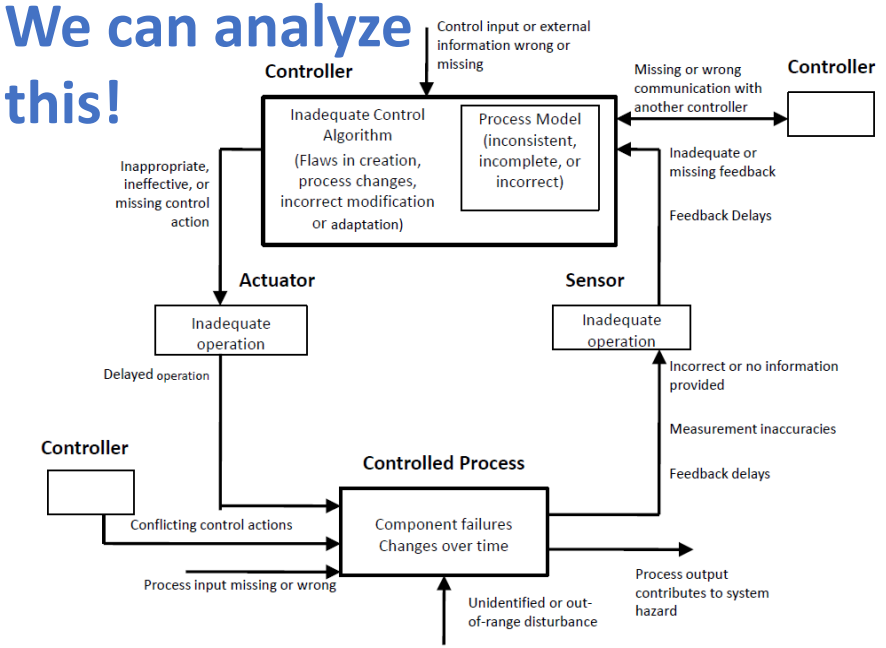
Ship product
Delivery of artifacts
including provenance

Pr
Ide

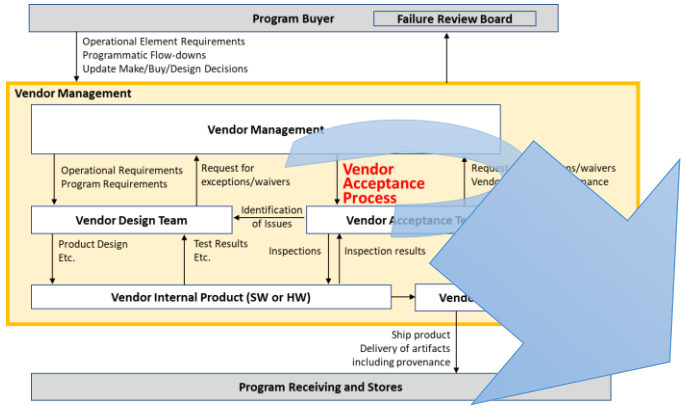
Program Receiving and Stores

Unmitigated Vulnerability!

We can analyze this!



Malicious Device Insertion Overview



UCA-1: VM provides a requirements / acquisition process that is flawed (incapable of preventing malicious device from entering supply chain)

Program Buyer Requirements are inadequate

Program/Vendor Policies

Vendor Management (VM)

Assumption of "Correct" process is the default

- New Vendor
- VM obtains waiver to requirements - allows new vendor
- VM obtains waiver to requirements – reduces screening/acceptance criteria

Requirements update based on events

VM does not receive sufficient info about weaknesses in process, inspections, or component specific information. So VM won't update techniques when necessary.

Potential Adversary

Potential Adversary

Process Updating

System Actuation

System Feedback

Process Monitoring

Vendor process is changed after it is issued

Potential Adversary

System Monitor

Identification of part failure

Insider to identify process and weaknesses to exploit

Issue with process is not promptly reported

No report about process weaknesses that prevent tracing abnormal behavior to specific device

Potential Adversary

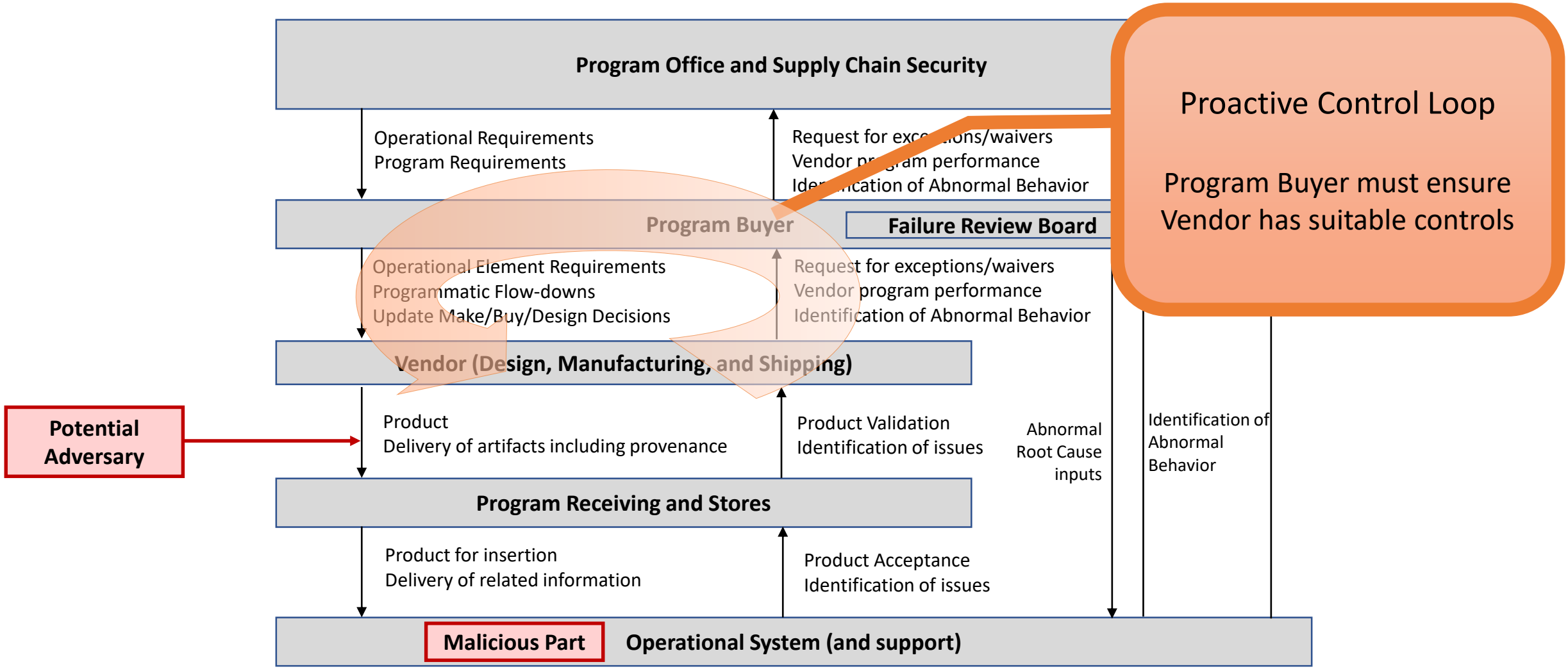
Vendor Acceptance Team (VAT)

Verification of part and changes- logging

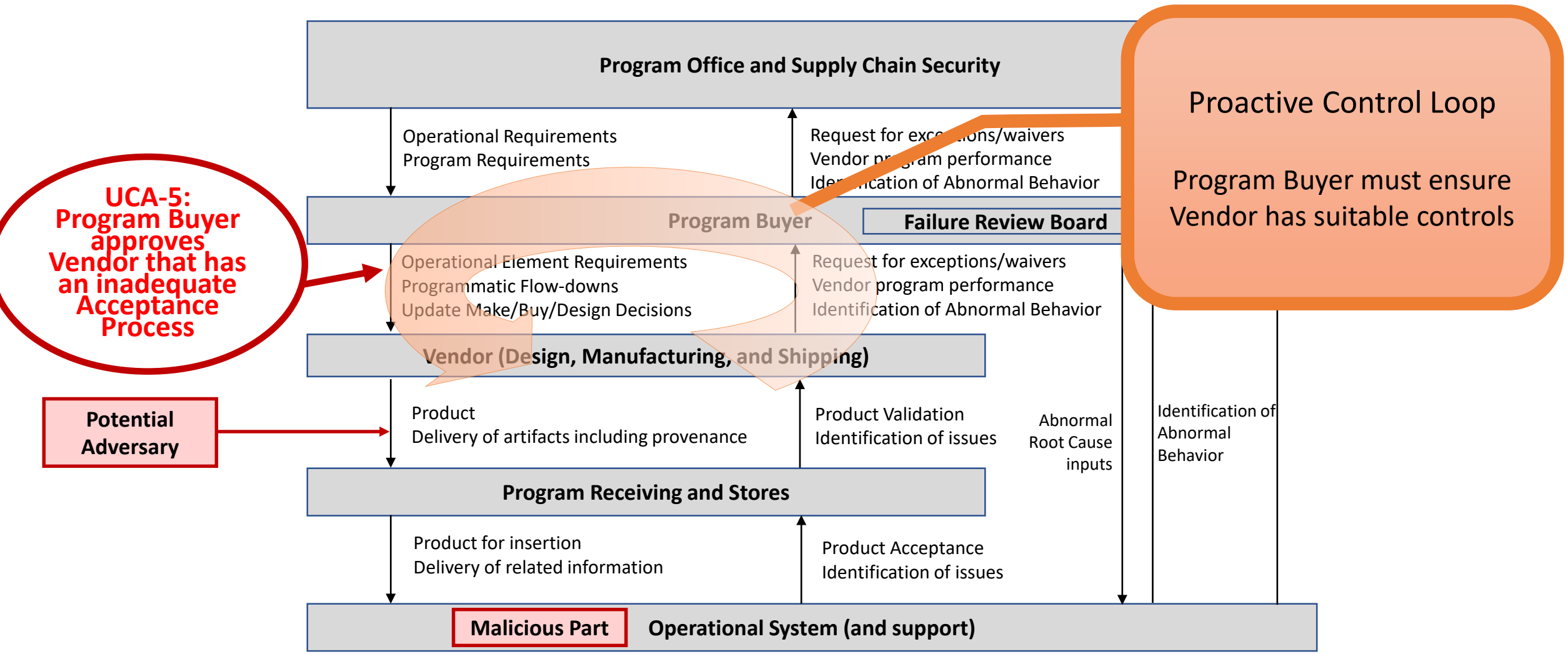
Process not followed properly

Pre-defined input / operational state / environmental condition that interferes with acceptance process

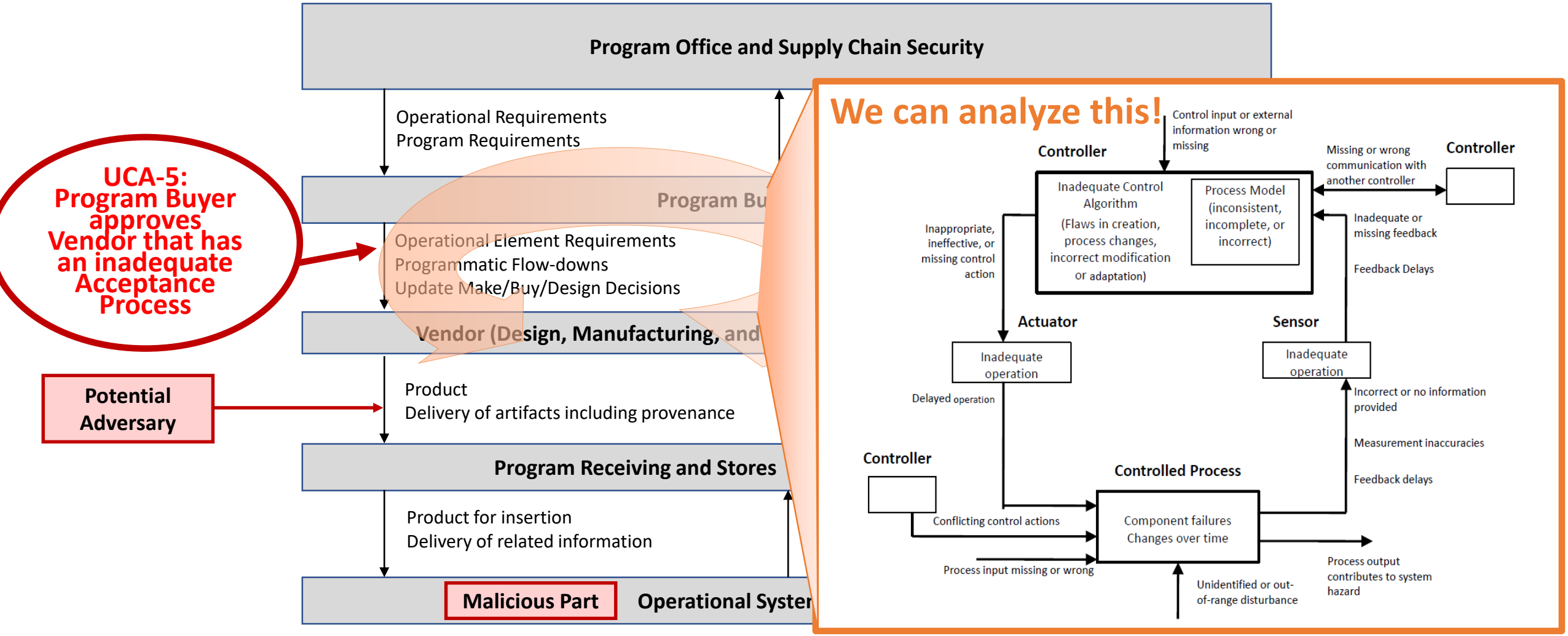
Program – Vendor Control Loop



Program – Vendor Control Loop

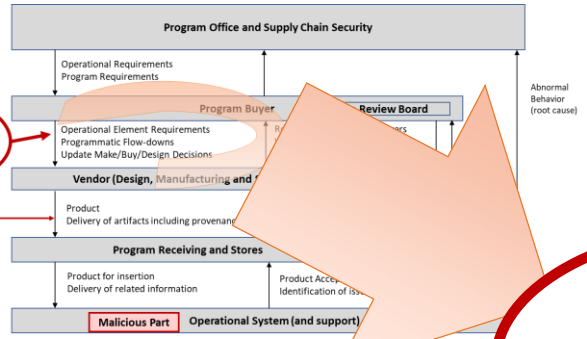


Program – Vendor Control Loop



Vulnerabilities in Program Oversight

Approved for Distribution Statement A Public Release



UCA-5:Program Buyer accepts Vendor with an inadequate Acceptance Process

Program Requirements are inadequate

Program Buyer (PB)

- Inadequate process for sole source vendors
- Unable to identify alternative vendors
- Process allows waivers for new vendors
- Process allows waivers of acceptance requirements (reduces screening/acceptance criteria)

Assumption of "Correct" process/device is the default

Program/Vendor Policies

Requirements update based on events

PB does not receive info about weaknesses in process, inspections, or component specific information. So PB won't reject vendor.

Vendor Inspection

System Actuation

System Feedback

Vendor Monitoring

Potential Adversary

Vendor process is changed after it is accepted

Potential Adversary

System Monitor

Identification of part failure

Insider to identify process and weaknesses to exploit

Issue with process is not promptly reported

No report about process weaknesses that prevent tracing abnormal behavior to specific device

Vendor

Potential Adversary

Verification of part and changes- logging

Process not followed properly

Pre-defined input / operational state / environmental condition that interferes with acceptance process

STPA Identified Scenario

Program Buyer authorizes new Vendor with inadequate controls (due to [….])

Vendor doesn't have adequate controls to detect a malicious object (HW, SW)

Program Receiving doesn't have adequate controls to detect a malicious object (HW, SW)

Operational System encounters a need for the part. The malicious part is installed.

The malicious part creates new hazards / vulnerabilities.

Failure Review Board does not provide an effective fix (because no defect found)

Failure Review Board does not immediately assess the cause of the malicious activity. (NDF: No Defect Found)

Operational System and Support eventually detects and reports malicious activity

Operational System and Support does not immediately detect malicious object (delayed response)

Program Office and Supply Chain Security

Operational Requirements
Program Requirements

Request for exceptions/waivers
Vendor program performance
Identification of Abnormal Behavior

Program Buyer | **Failure Review Board**

Operational Element Requirements
Programmatic Flow-downs
Update Make/Buy/Design Decisions

Request for exceptions/waivers
Vendor program performance
Identification of Abnormal Behavior

Threat: Adversary Injects Malicious SW

Vendor (Design, Manufacturing, and Shipping)

Product
Delivery of artifacts including provenance

Product Validation
Identification of issues

Abnormal
Root Cause
inputs

Identification
Abnormal
Behavior

Behavior

Program Receiving and Stores

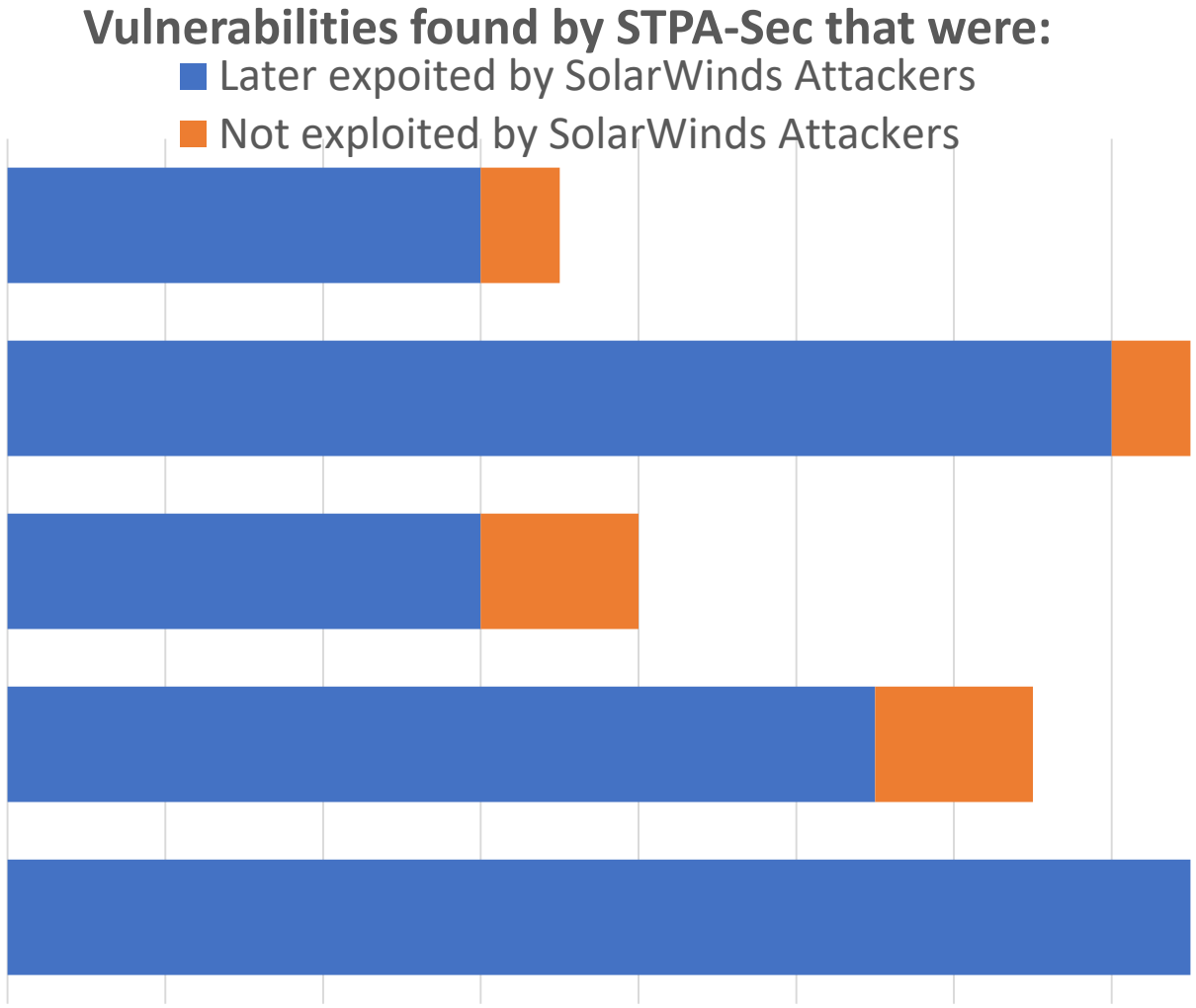
Product for insertion
Delivery of related information

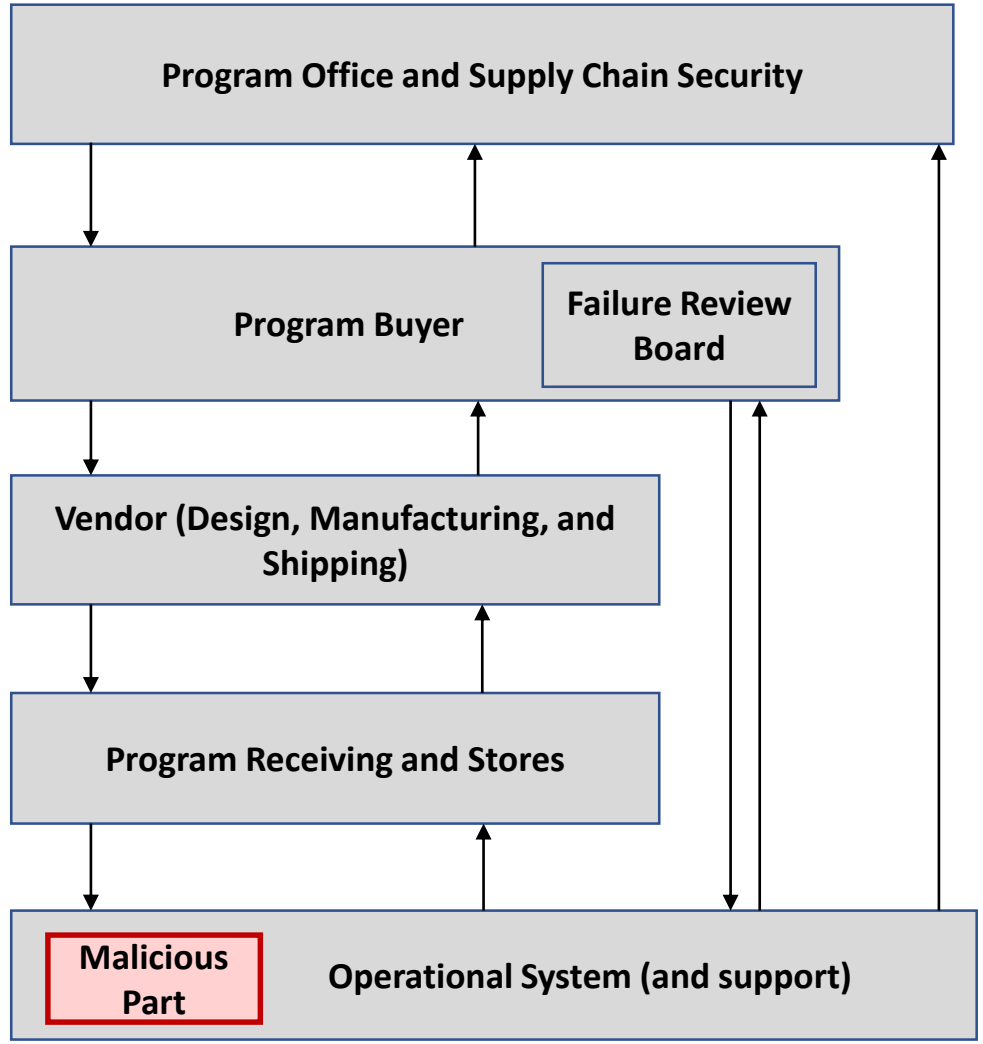
Product Acceptance
Identification of issues

Malicious Part | **Operational System (and support)**

Comparison to SolarWinds Attack

How relevant were the STPA Results to SolarWinds Attacks?





STPA Findings Vs. SolarWinds Attack (1/2)

STPA-sec controls defined in October 2020 vs SolarWinds Attack in December 2020*

- **Weak Cyber Controls**
  - Lazy Password on Update Server
  - Inability to detect adversary presence since early 2020
  - Inability to detect file deletions and log manipulation
- **Weak Training (to detect out-of-family activities)**
  - Adversary use of Temporary Replacement Technique and Temporary Task Modification
  - Abnormal traffic on authorized port - Use of OIP (Orion Improvement Program)
  - Source code review – Fake variable names tied to legitimate code
  - Malicious functions had dormant period before wakeup.

* FireEye notice and other public summaries

STPA Findings Vs. SolarWinds Attack (2/2)

STPA-sec controls defined in October 2020 vs SolarWinds Attack in December 2020*

- **Weak TTPs (poor techniques allowing abnormal operations)**
  - High Trust level – allowed lateral movement at elevated status (SAML tokens…)
  - Lack of external verification – external labs could only use composite analysis
- **Weak Verification during Packaging/Assembly**
  - Obsolete hashing and file provenance controls, eliminating the usefulness of later confirmation checking
- **Customer Verification and corrective action issues (limited options)**
  - Corporate digital signature
  - Short-term recommendation – shut down network management tool making them blind to other malicious activities

* FireEye notice and other public summaries

Conclusions

- Supply chains have increasingly become targets, with dramatic increases in Global Supply Chain attacks
- New methods and techniques are required to catch up and get ahead of adversaries
- STPA-Sec offers a comprehensive top-down methodology to conduct secure systems engineering and analysis
- STPA-Sec anticipated the actual supply chain vulnerabilities later used by SolarWinds hackers
- STPA-Sec identified vulnerabilities that were not effectively mitigated by traditional techniques
- STPA-Sec generated effective new solutions that were implemented by DoD customer, eliminating vulnerabilities that remained in other supply chains.
- STPA-Sec findings from Oct 2020 were a remarkable match to the findings from the Dec 2020 SolarWinds attacks. **Why wait for attackers to find these weaknesses?**