

**APL**

*The Johns Hopkins University*  
APPLIED PHYSICS LABORATORY

# **Coupled Petri Nets for Computer Network Risk Analysis (Application to Process Control Networks)**

Matt Henry, Ryan Layer, David Zaret

# Motivation

---

Estimate the risk associated with a “cyber” attack launched against a particular network.

$$\text{Risk} \leftarrow f(L_{\text{bth}}, C_{\text{bth}})$$

$L_{\text{bth}}$ : Likelihood that bad things will happen

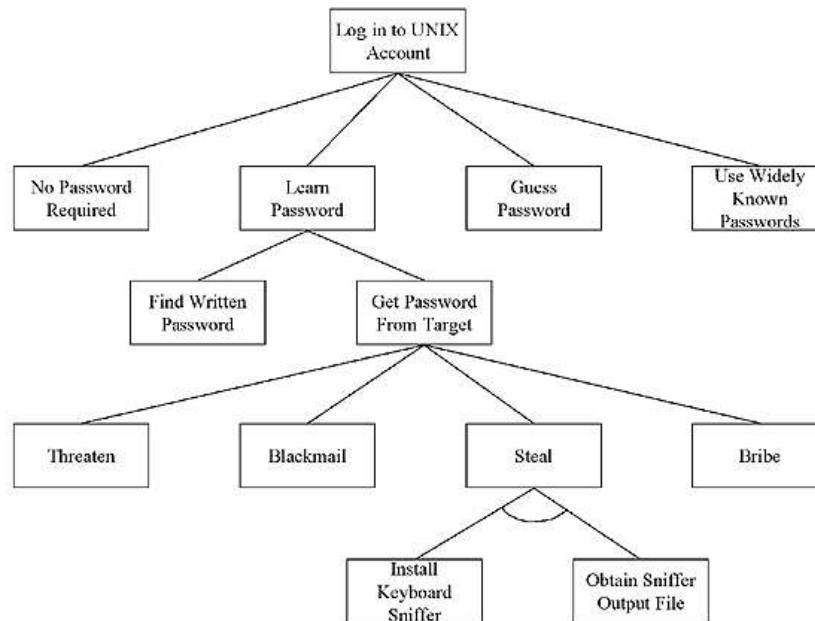
$C_{\text{bth}}$ : Consequences of those bad things if they happen

This is an old problem

# “Traditional” Attack Modeling

Define a set of attack goals

Figure out how hard the goals are to achieve



Source:

M. S. Pallos, Attack Trees: It's a Jungle out there, The Business Forum:

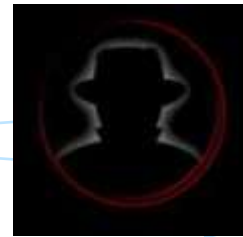
<http://www.bizforum.org/whitepapers/candle-4.htm>

# Horse, then Cart

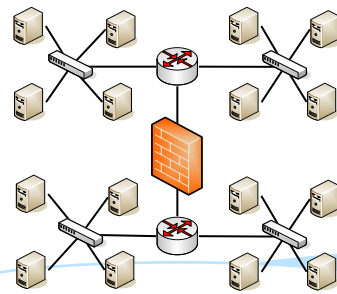
No presumed goal; only constraints and objectives

Figure out how much of the network the attacker can own

Given access to network resources, identify potential operational impact



Attacker



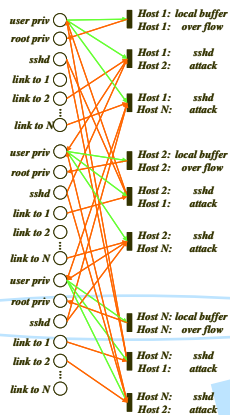
Enterprise Network



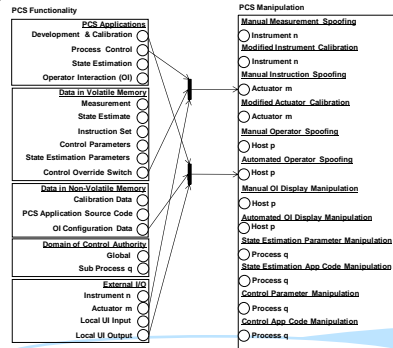
Target Operation



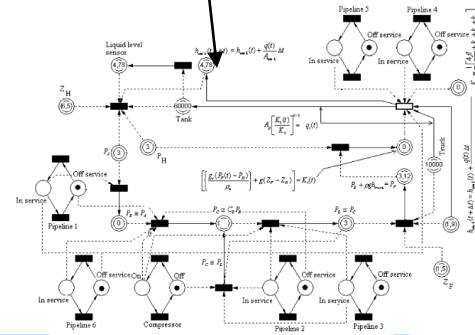
Operational Impact



CNA Petri Net



PCS Petri Net



Process Petri Net

- Inducible Process Failure Modes:**
1. Small qty gaseous ammonia discharge to dilution drum
  - 1A. Large qty gaseous ammonia discharge to dilution drum
  2. Automated fill task disabled
  - 2A. Large qty liquid ammonia discharge to dilution drum
  3. Tank Overflow
  4. High-pressure gaseous ammonia discharge from damaged plumbing
  5. High-pressure liquid ammonia discharge from damaged plumbing
  6. Low-pressure gaseous ammonia discharge from damaged plumbing

# We're not alone

---



This approach is gaining attention in the community. Several research groups have been developing access-based risk assessment techniques.

To name a few ...

MIT-LL: NetSPA (Ingols et al.)

Mitre: RiskMAP (Kertzner et al.)

CMU: Stochastic Games (Lye and Wing)

UIUC: Differential Games (Alpcan and Basar)

# Our Approach is based on State Reachability

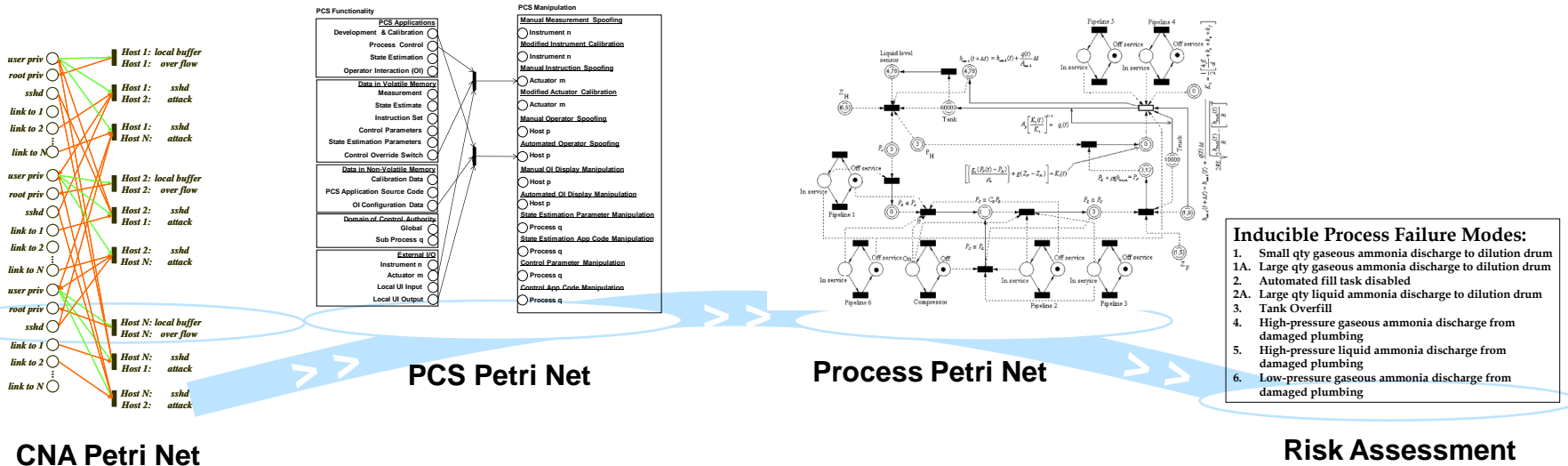


## Coupled models for Risk Analysis

**Attack Model:** Network Resource Accessibility

**Process Control System Model:** Functionality and Authority

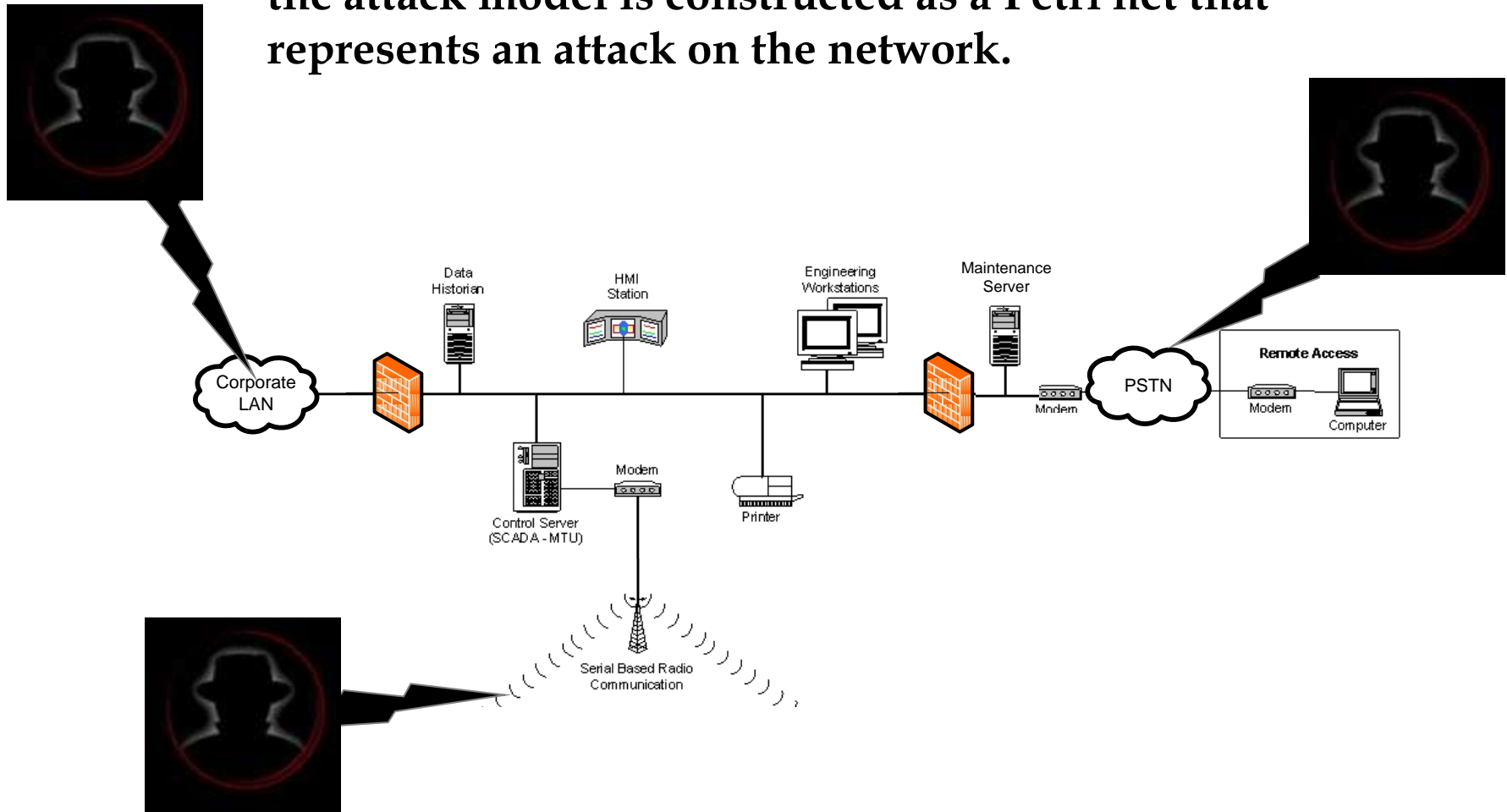
**Process Model:** Process Failure Modes and Consequences



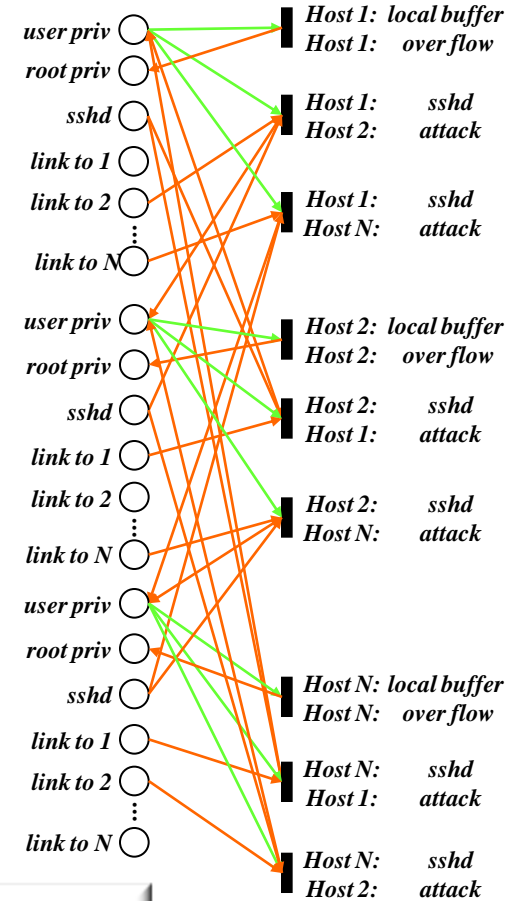
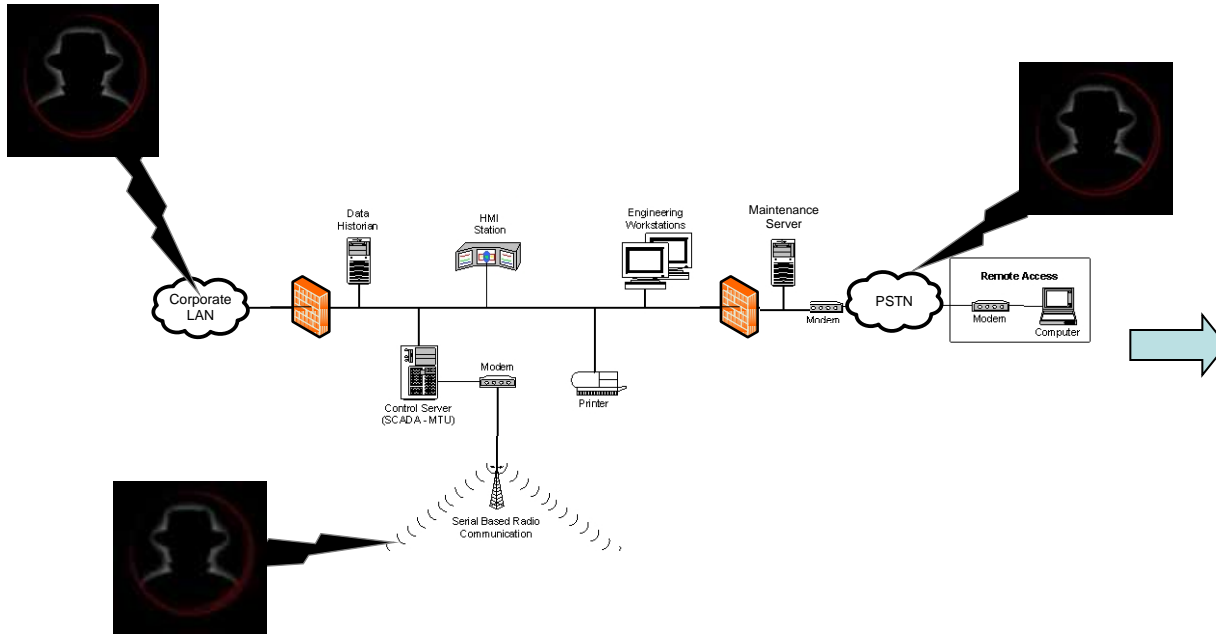
We want to eliminate parametric estimation requirements (no attempts to SWAG “probability of success”) to see how far we can get based on what we know: that exploits launched against known vulnerabilities eventually succeed.

# Attack Model

Given some initial access and a network configuration, the attack model is constructed as a Petri net that represents an attack on the network.



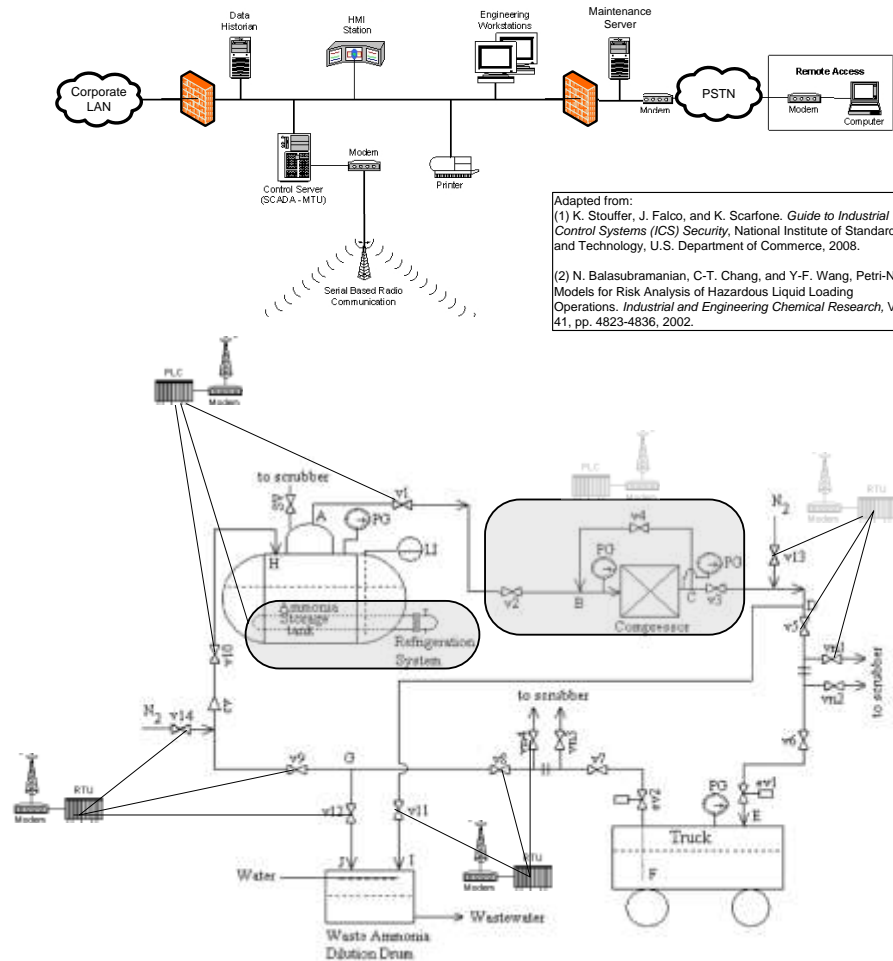
# Attack Model



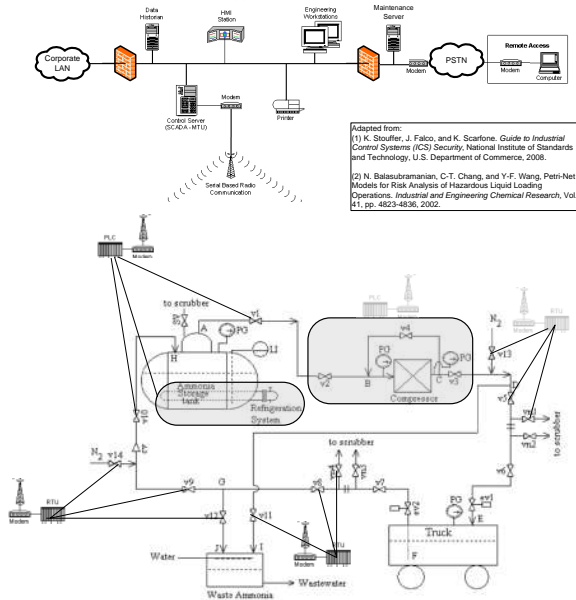
Exploitation of host vulnerabilities permits escalation of privilege and access on the network, represented as state dynamics on the Petri net.

# PCS Model

Relates PCS host attributes (applications, resident data, instrument and actuator I/O, and control authority ) to PCS functionality (state estimation, control, operator interaction) .



# PCS Model



## PCS Functionality

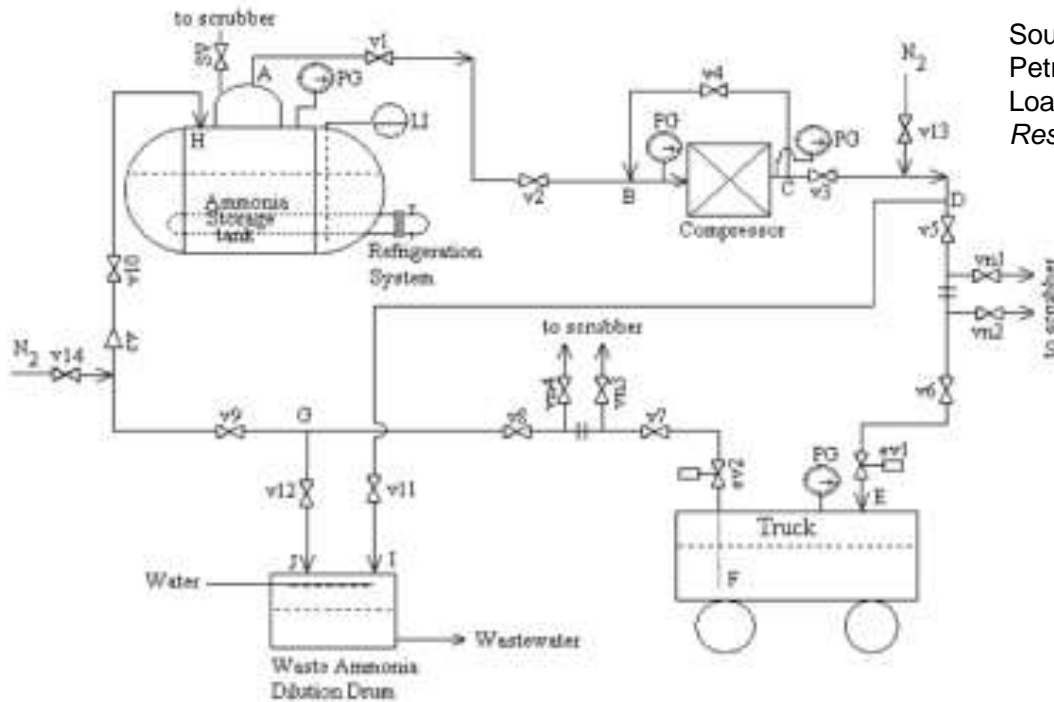
<b>PCS Applications</b>	
Development & Calibration	<input type="radio"/>
Process Control	<input type="radio"/>
State Estimation	<input type="radio"/>
Operator Interaction (OI)	<input type="radio"/>
<b>Data in Volatile Memory</b>	
Measurement	<input type="radio"/>
State Estimate	<input type="radio"/>
Instruction Set	<input type="radio"/>
Control Parameters	<input type="radio"/>
State Estimation Parameters	<input type="radio"/>
Control Override Switch	<input type="radio"/>
<b>Data in Non-Volatile Memory</b>	
Calibration Data	<input type="radio"/>
PCS Application Source Code	<input type="radio"/>
OI Configuration Data	<input type="radio"/>
<b>Domain of Control Authority</b>	
Global	<input type="radio"/>
Sub Process q	<input type="radio"/>
<b>External I/O</b>	
Instrument n	<input type="radio"/>
Actuator m	<input type="radio"/>
Local UI Input	<input type="radio"/>
Local UI Output	<input type="radio"/>

## PCS Manipulation

<b>Manual Measurement Spoofing</b>	
<input type="radio"/> Instrument n	
<b>Modified Instrument Calibration</b>	
<input type="radio"/> Instrument n	
<b>Manual Instruction Spoofing</b>	
<input type="radio"/> Actuator m	
<b>Modified Actuator Calibration</b>	
<input type="radio"/> Actuator m	
<b>Manual Operator Spoofing</b>	
<input type="radio"/> Host p	
<b>Automated Operator Spoofing</b>	
<input type="radio"/> Host p	
<b>Manual OI Display Manipulation</b>	
<input type="radio"/> Host p	
<b>Automated OI Display Manipulation</b>	
<input type="radio"/> Host p	
<b>State Estimation Parameter Manipulation</b>	
<input type="radio"/> Process q	
<b>State Estimation App Code Manipulation</b>	
<input type="radio"/> Process q	
<b>Control Parameter Manipulation</b>	
<input type="radio"/> Process q	
<b>Control App Code Manipulation</b>	
<input type="radio"/> Process q	

Access to network resources permits co-option of control authority through exploitation of PCS functionality.

# Process Model



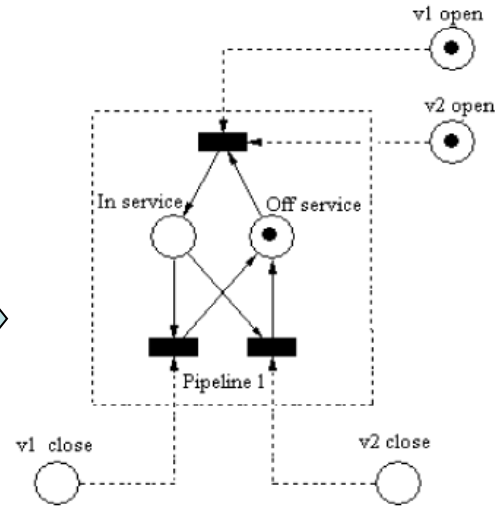
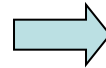
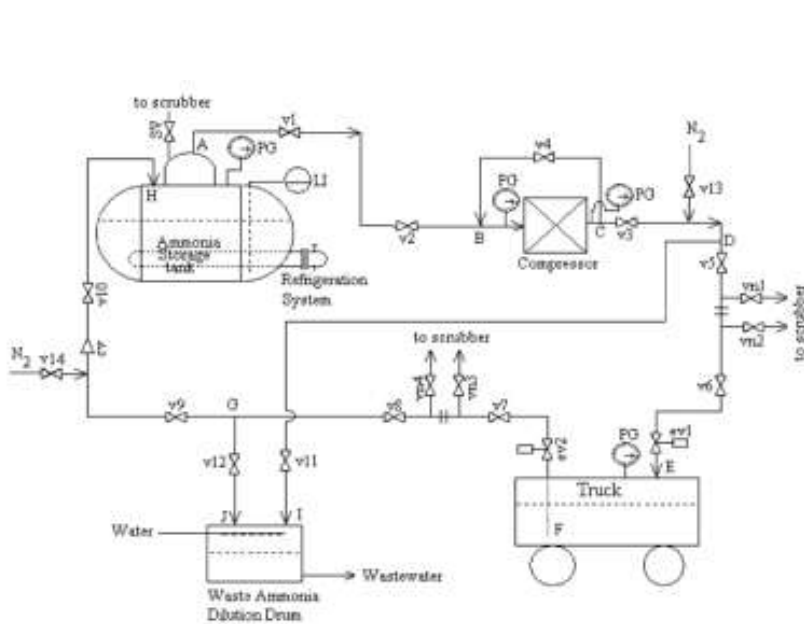
Source: N. Balasubramanian, C-T. Chang, and Y-F. Wang, Petri-Net Models for Risk Analysis of Hazardous Liquid Loading Operations. *Industrial and Engineering Chemical Research*, Vol. 41, pp. 4823-4836, 2002.

**Relates process states (state of valves, pump state) to system states (line pressures and temperatures)**

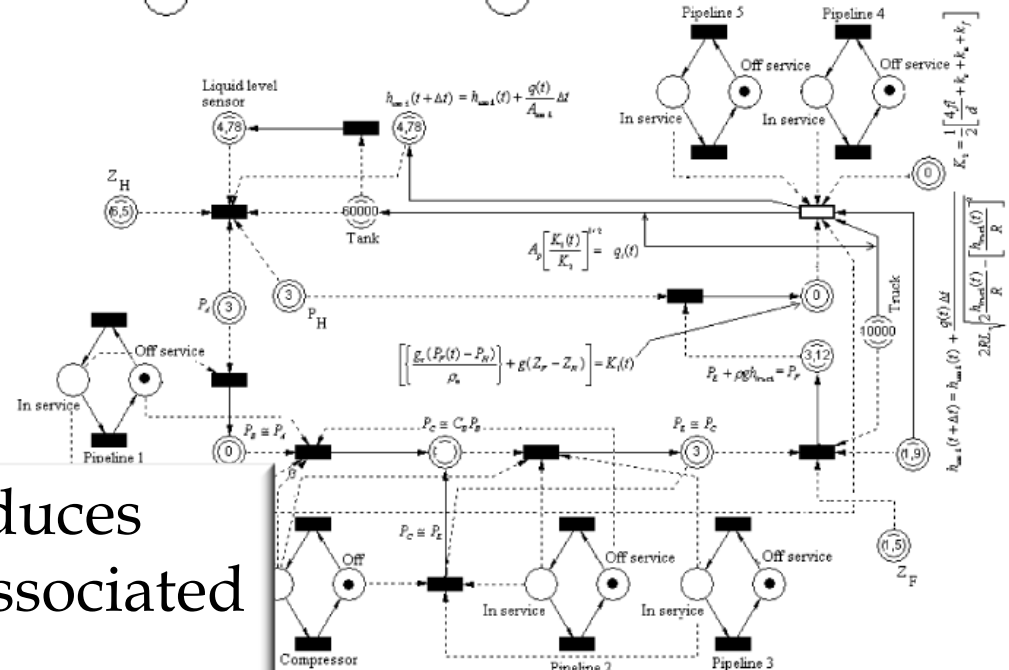
**Permits ready identification of failure modes (process error states)**

**Facilitates analysis of failure mode effects due to system states associated with process error states**

# Process Model



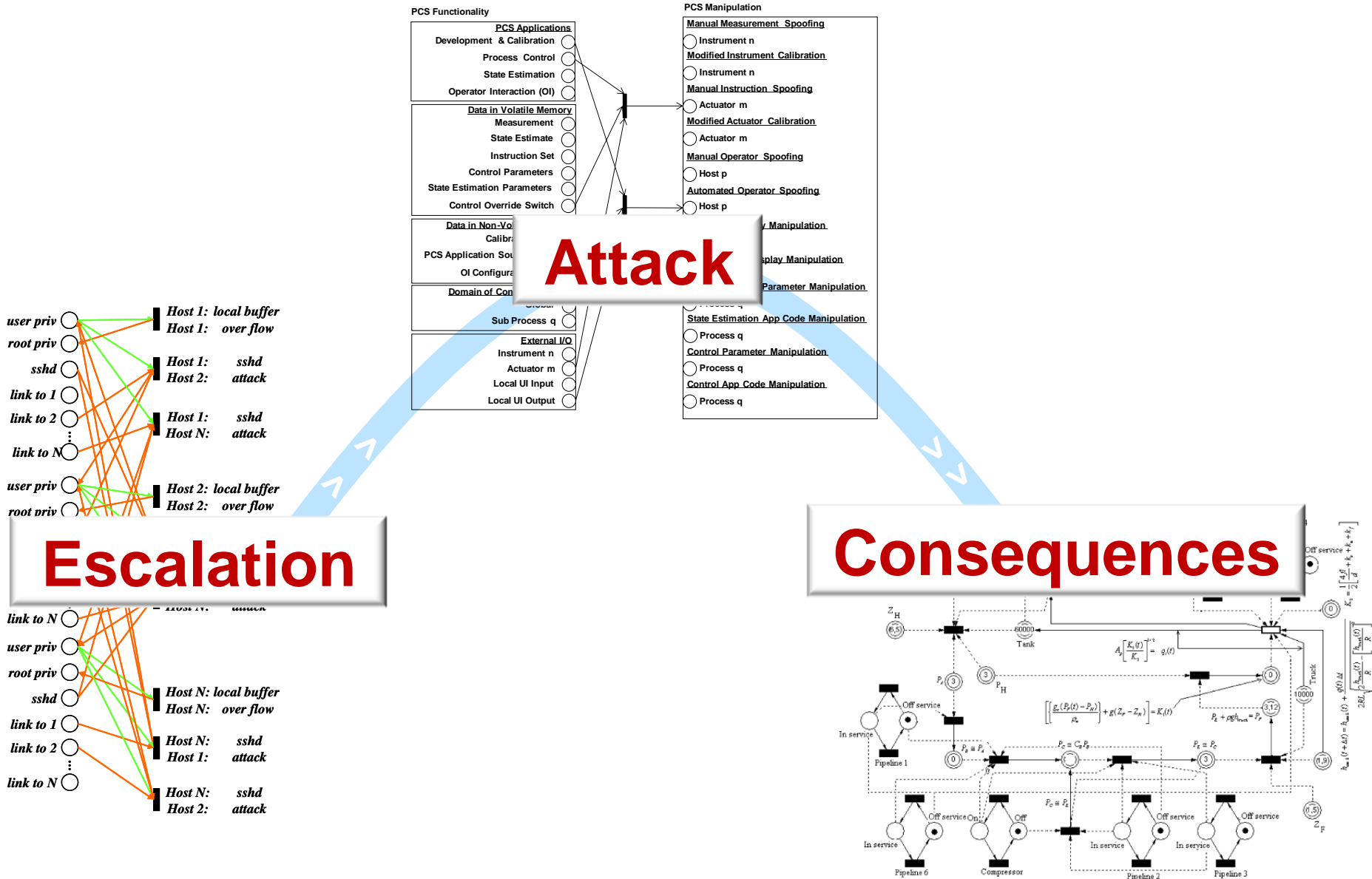
Source: N. Balasubramanian, C-T. Chang, and Y-F. Wang, Petri-Net Models for Risk Analysis of Hazardous Liquid Loading Operations. *Industrial and Engineering Chemical Research*, Vol. 41, pp. 4823-4836, 2002.



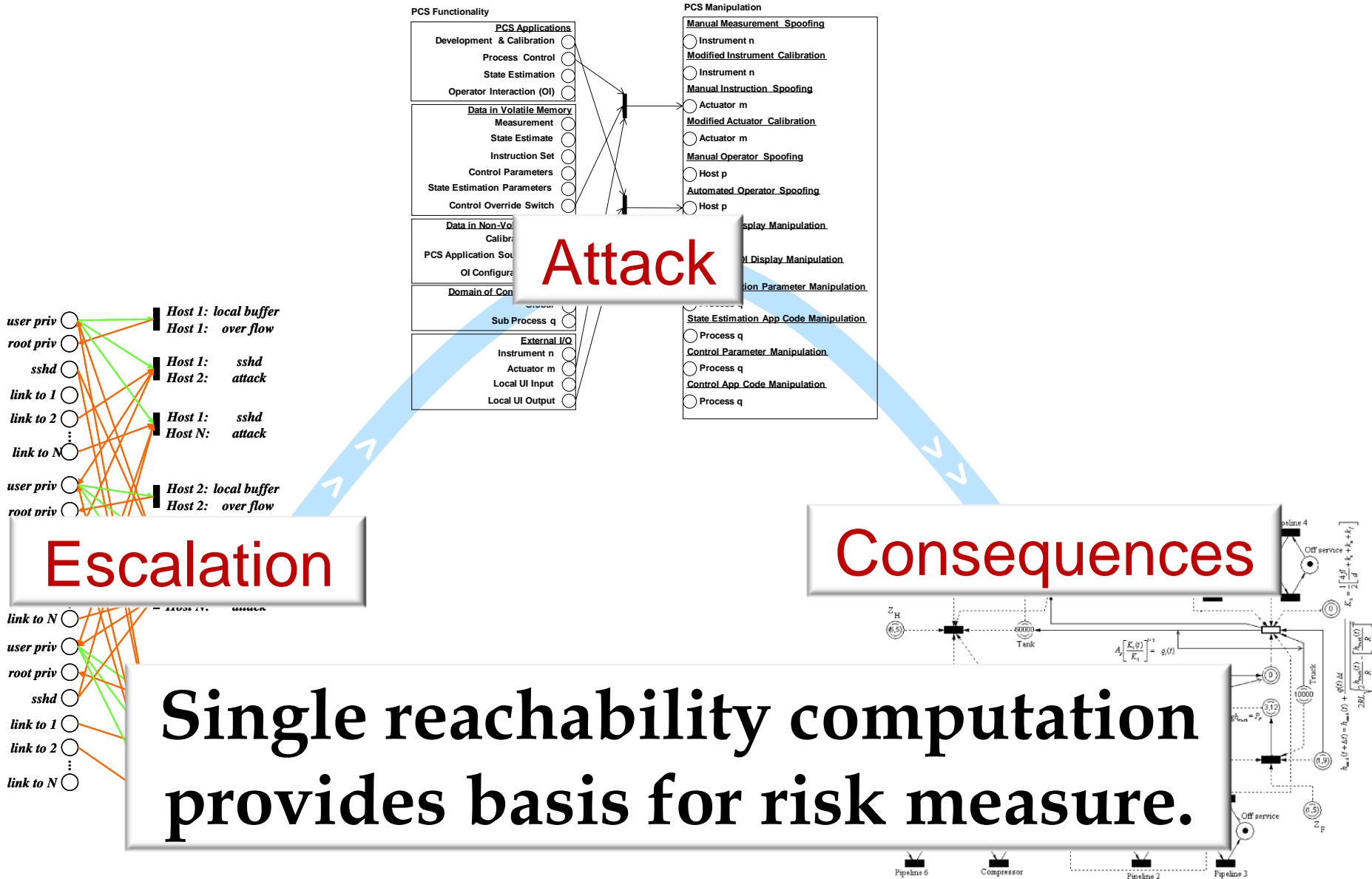
Co-opted process control induces process failure modes and associated operational consequences.

s conditions at different locations.

# Coupled Models for Risk Analysis

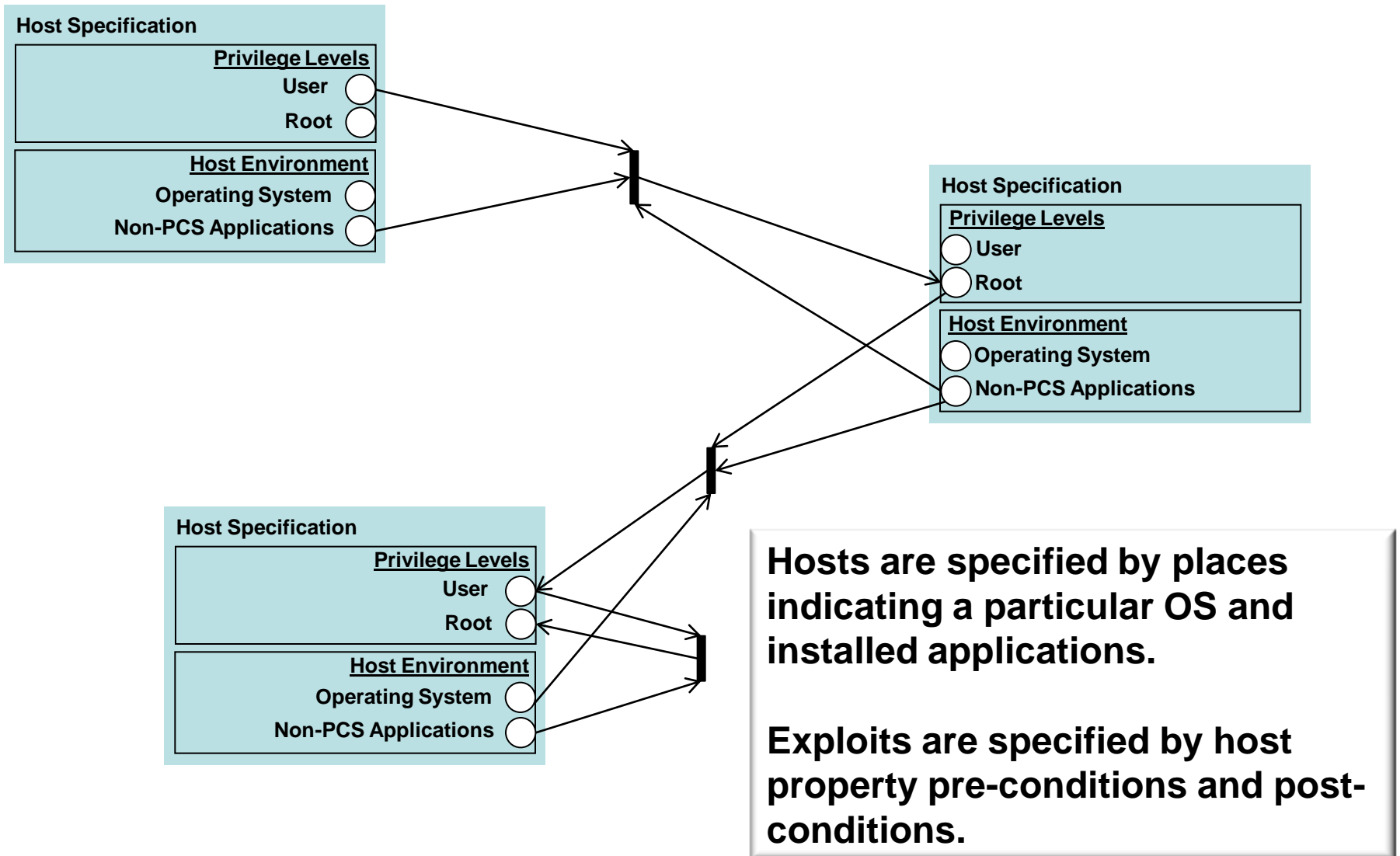


# Coupled Models for Risk Analysis



**Single reachability computation provides basis for risk measure.**

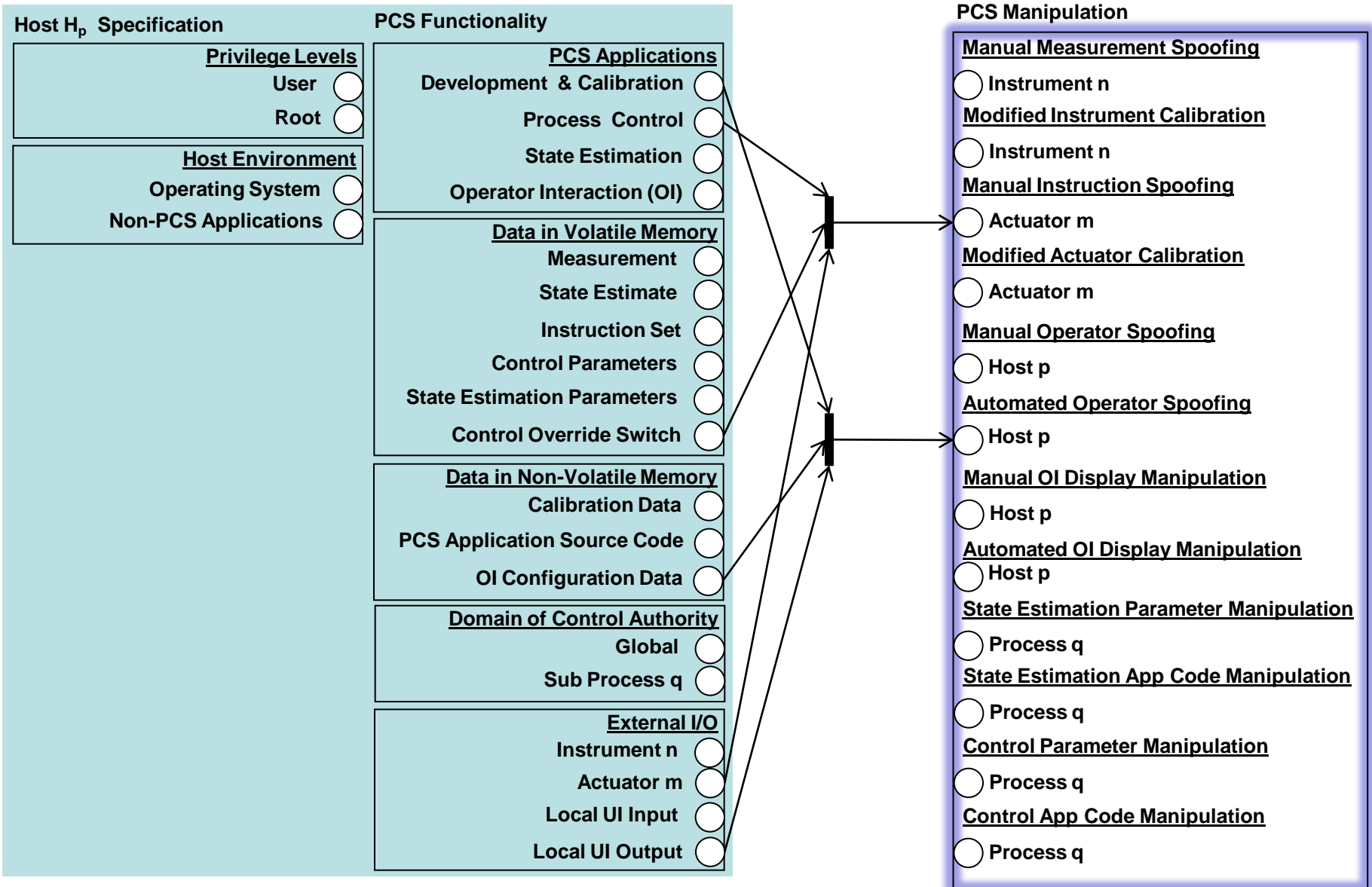
# Specifying the Coupled Model: Escalation



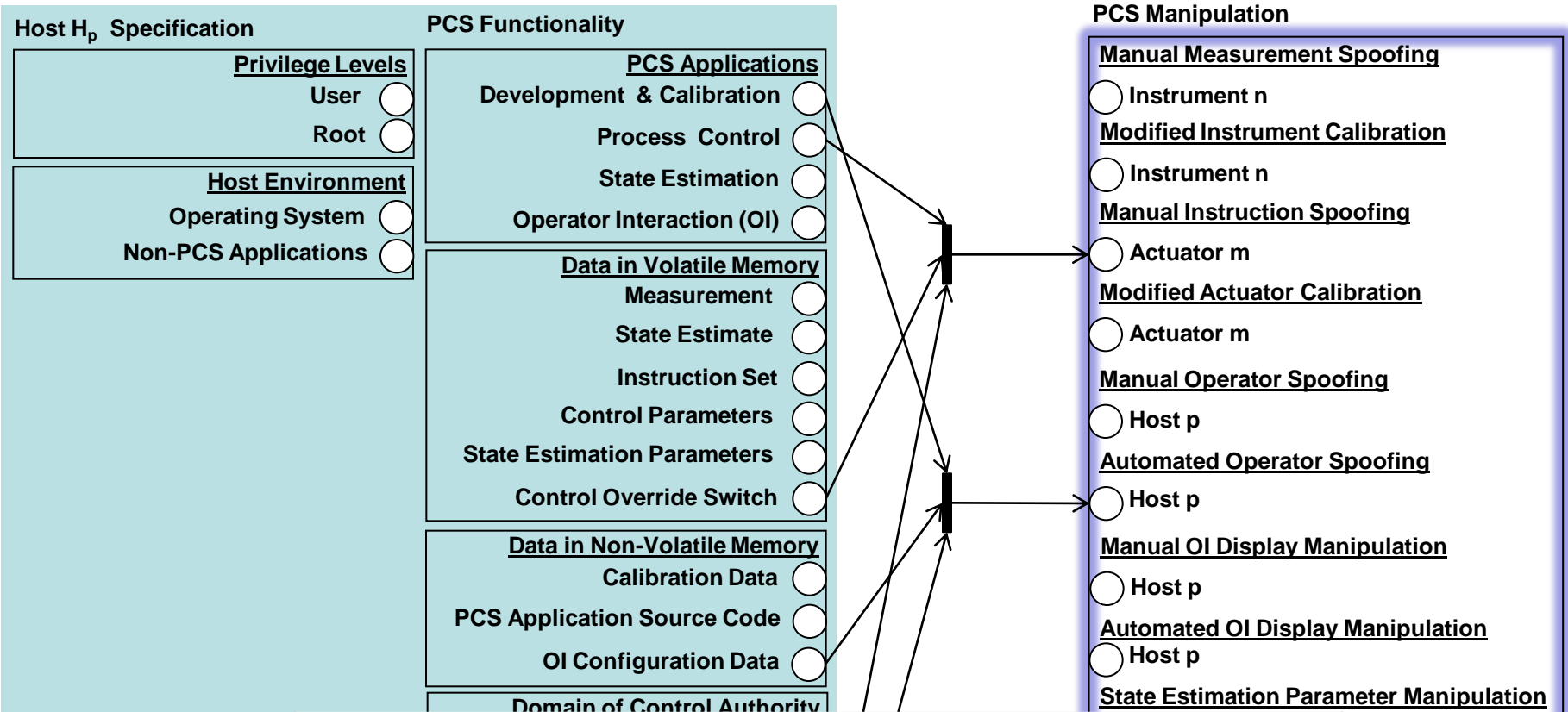
**Hosts are specified by places indicating a particular OS and installed applications.**

**Exploits are specified by host property pre-conditions and post-conditions.**

# Specifying the Coupled Model: **Attack**



# Specifying the Coupled Model: **Attack**



**PCS host functionality is specified by applications, data, control authority and I/O.**

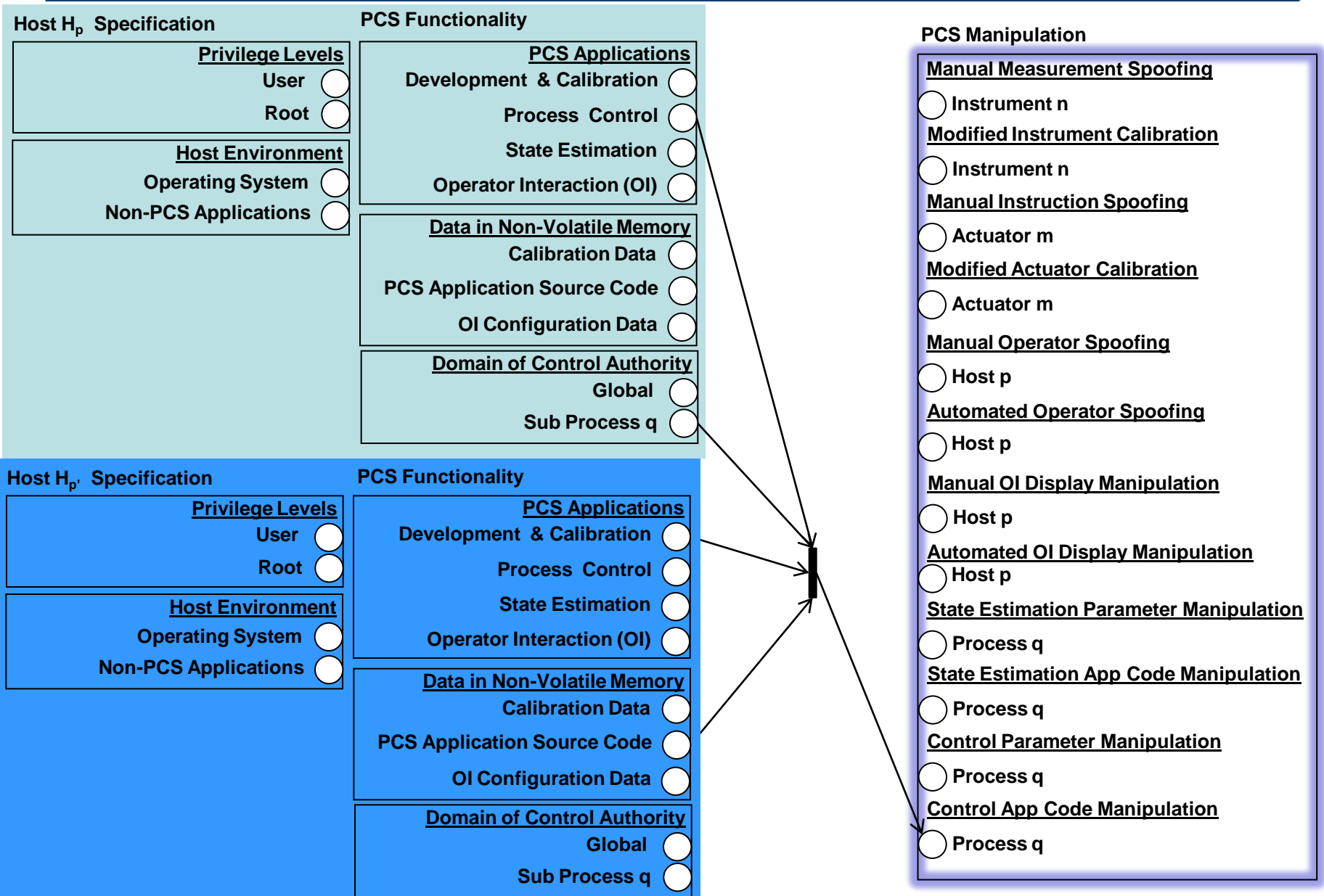
**Functionality co-option attacks are specified by PCS functionality access pre-conditions and functionality co-option post-conditions.**

Code Manipulation

Manipulation

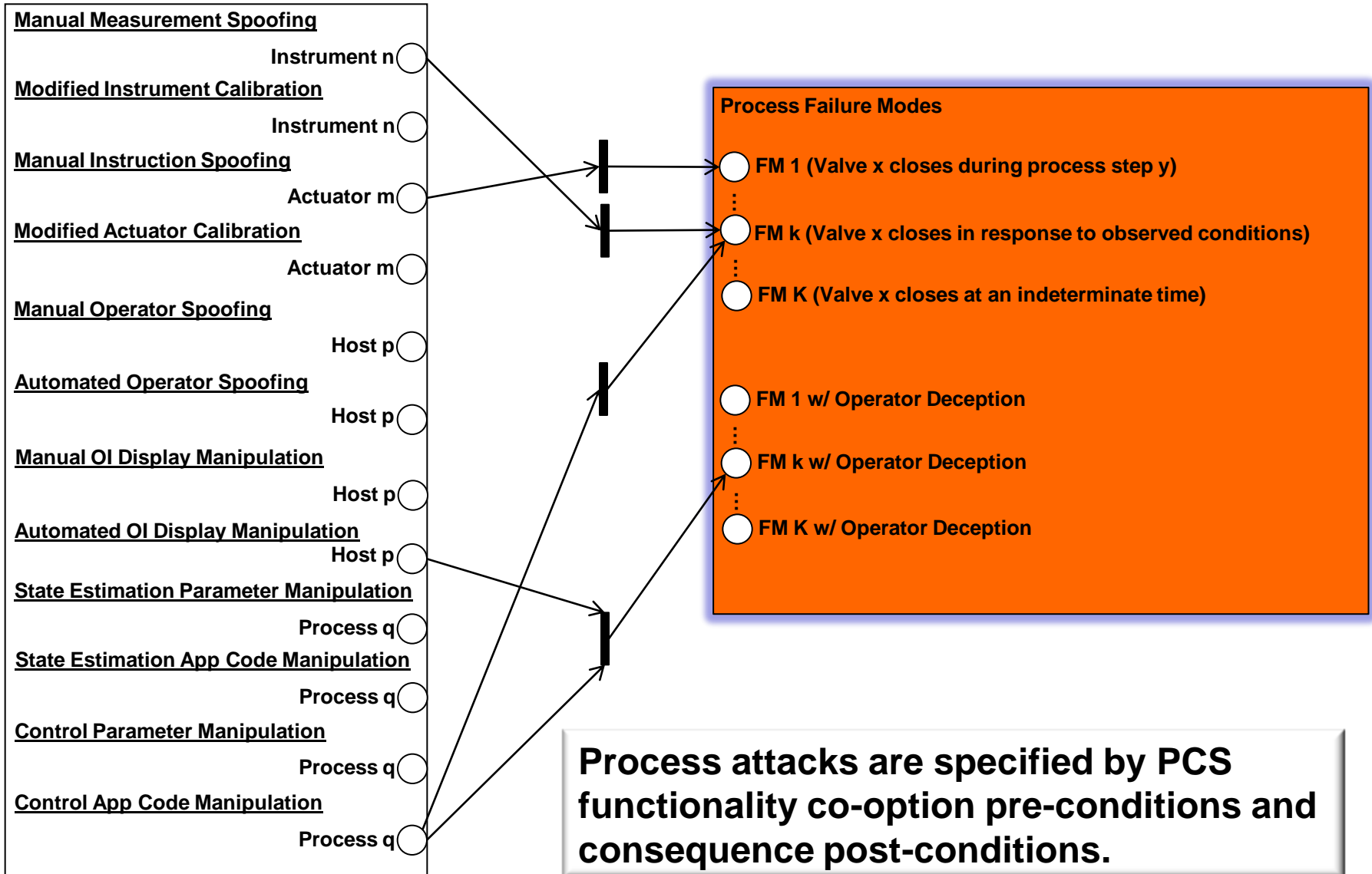
Manipulation

# Specifying the Coupled Model: **Attack**



# Specifying the Coupled Model: **Consequences**

## PCS Manipulation



# Model-Based Analysis

---



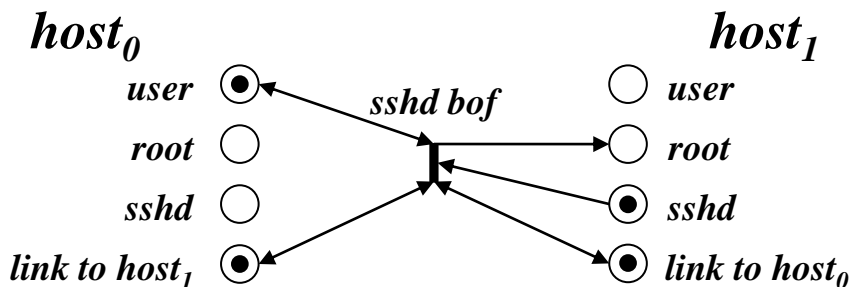
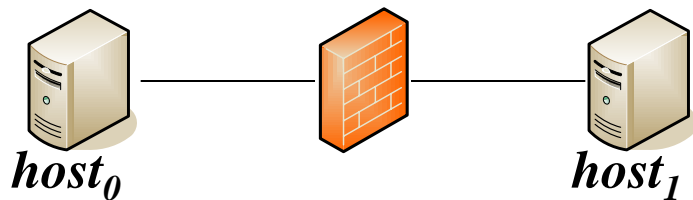
State Reachability

Risk Assessment

Risk Management

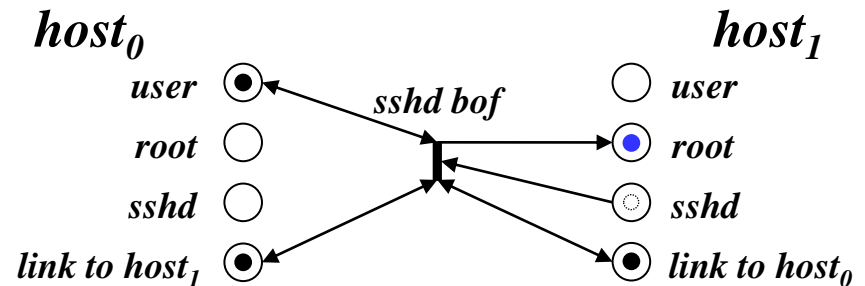
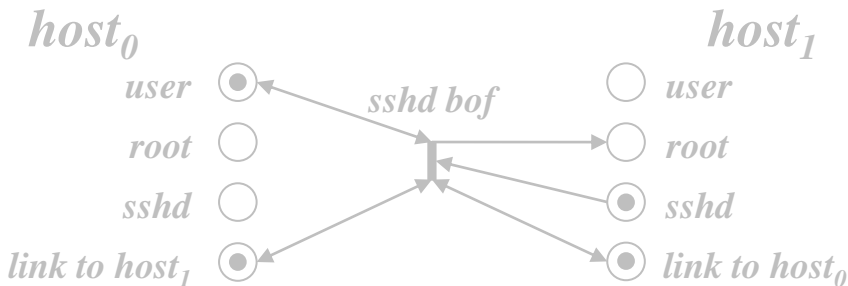
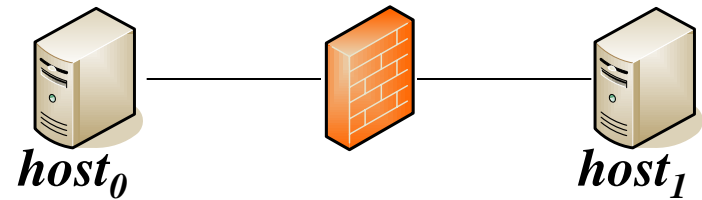
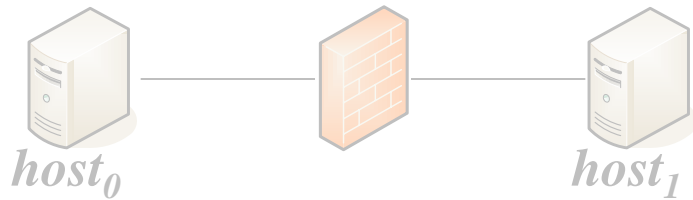
# Petri Nets for Attack Modeling

- places represent conditions (resources, access)
- tokens represent satisfied conditions (resource exists, attacker has access)
- transitions represent events (atomic attack steps)
- → ■ input places are the event's preconditions
- → ○ output places are the event's postconditions
- → ■ → ○ a transition is enabled when its input places are marked
- → ■ → ● an enabled transition can fire, removing input tokens and adding output tokens



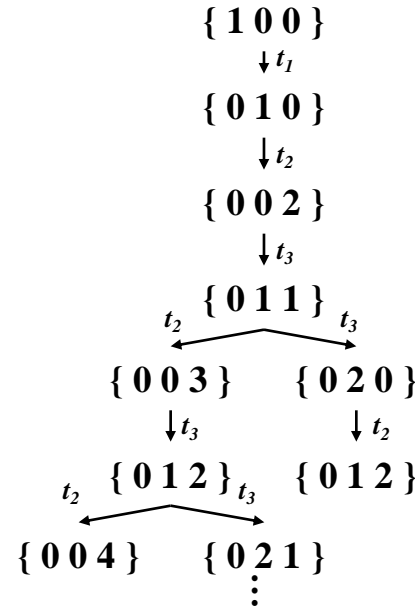
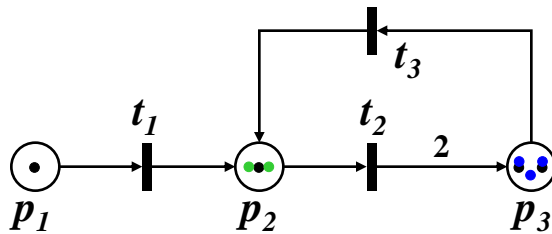
# Petri Nets for Attack Modeling

- places represent conditions (resources, access)
- tokens represent satisfied conditions (resource exists, attacker has access)
- transitions represent events (atomic attack steps)
- → ■ input places are the event's preconditions
- → ○ output places are the event's postconditions
- → ■ → ○ a transition is enabled when its input places are marked
- → ■ → ● an enabled transition can fire, removing input tokens and adding output tokens



# Finding the reachable set is NP-hard!

Build a tree of all markings reachable from some initial marking:

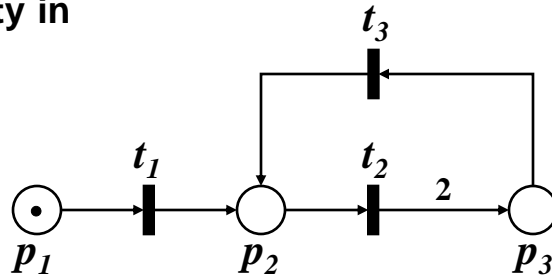


The state space is, in general, countably infinite.

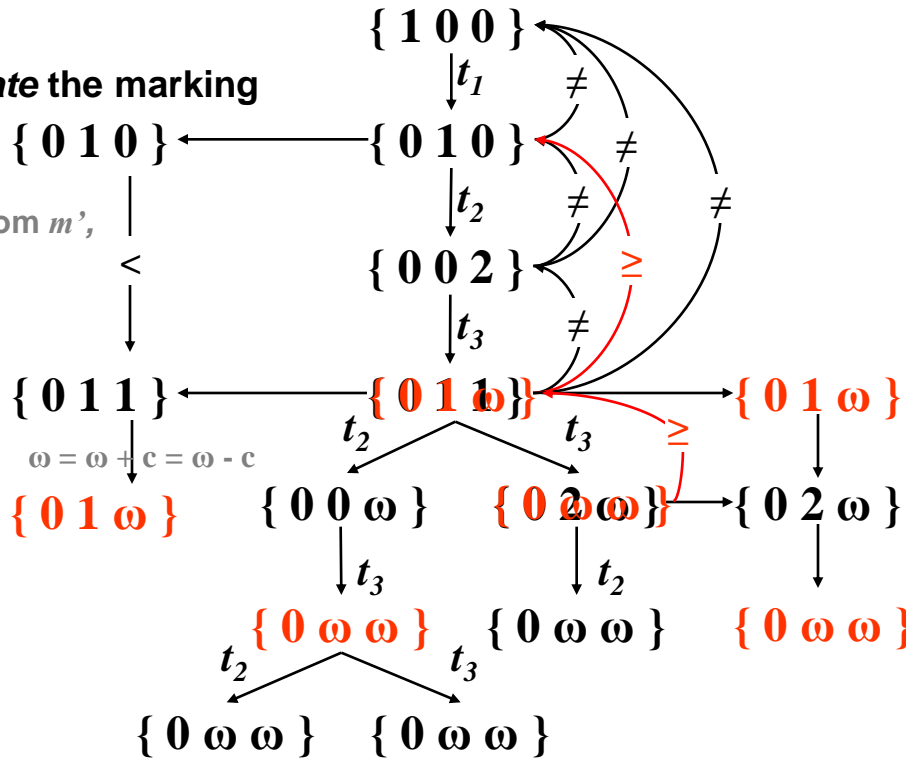
Even when finite, it is at least  $O(2^N)$  big.

# Practical Alternative: Coverability

Look for cases of strict monotonicity in the reachability tree:  
 $m \leq m'$  and  $m \rightarrow m'$



Accelerate the marking



The sequence  $\{t_2, t_3\}$  can fire from  $m'$ , so all places  $p$  such that  $m(p) < m'(p)$  are unbounded

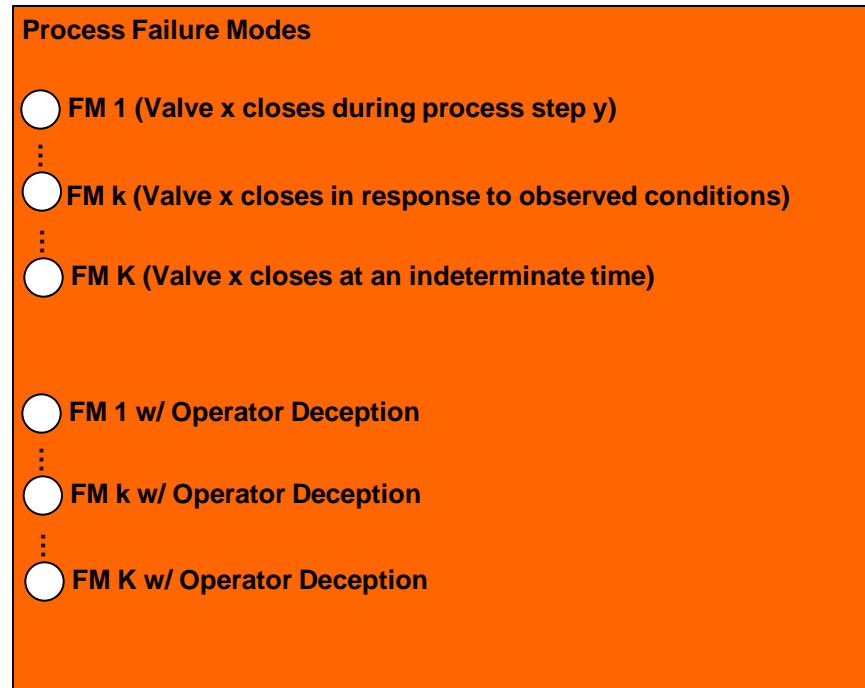
# Defining and Evaluating Risk Metrics

In the Coverability Set CS, one or more of the Process Failure Modes  $m^i$  will be marked.

Each of these Process Failure Modes has associated Material Consequences  $c^i$ .

Our metric:

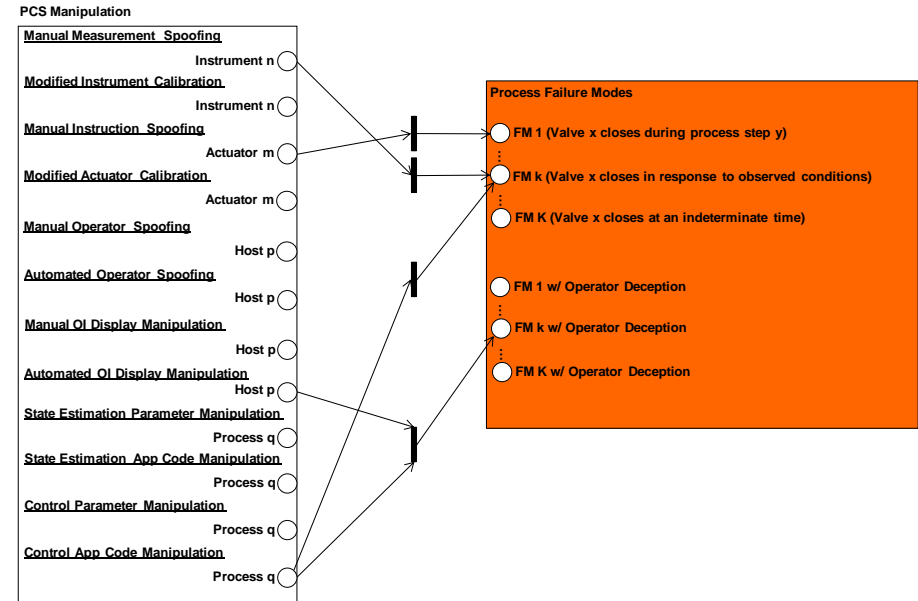
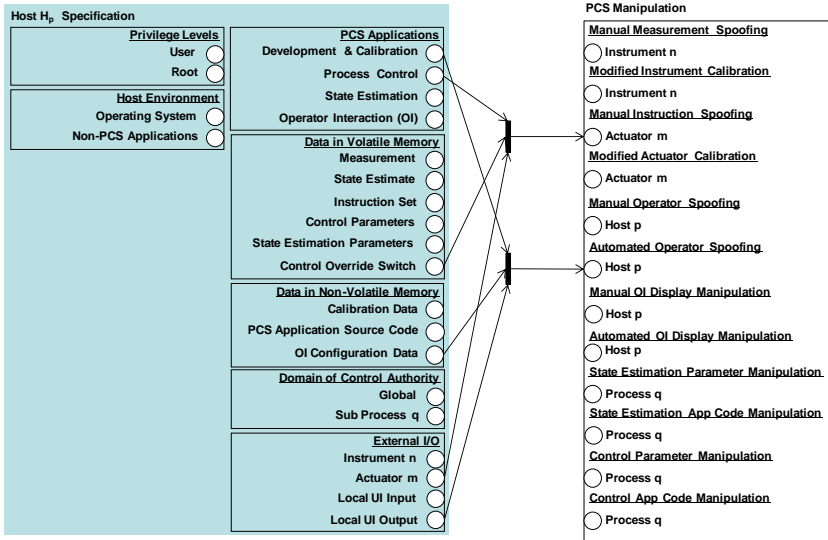
$$\text{Risk} = \max\{c^i | m^i \in \text{CS}\}$$



The diagram, titled "Process Failure Modes", is contained within an orange rectangular box. It lists seven failure modes, each preceded by a white radio button. The modes are: FM 1 (Valve x closes during process step y), FM k (Valve x closes in response to observed conditions), FM K (Valve x closes at an indeterminate time), FM 1 w/ Operator Deception, FM k w/ Operator Deception, and FM K w/ Operator Deception. Vertical ellipses are used between the first three modes and between the last three modes to indicate a sequence.

# Trace-back for Risk Management

**Identify and Evaluate the Value of preventing first-order transitions that lead to Process Failure Modes**



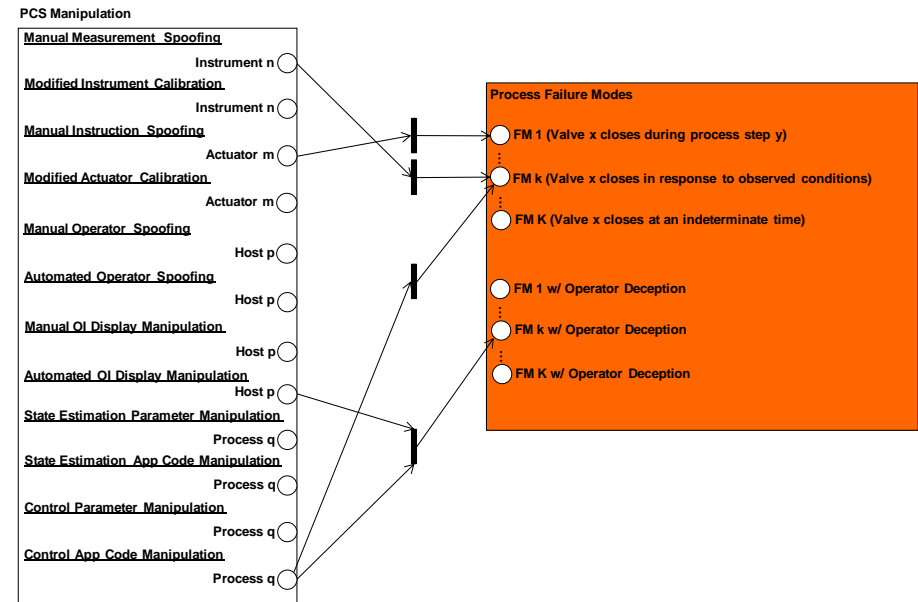
**Identify and Evaluate the Value of preventing higher order transitions that lead to preconditions of high-value first-order transitions**

# Trace-back for Risk Management

A transition  $t$  is a “first-order” transition if at least one of its post-conditions is a process failure mode,  $m$ , and it is enabled in at least one marking in the coverability set.

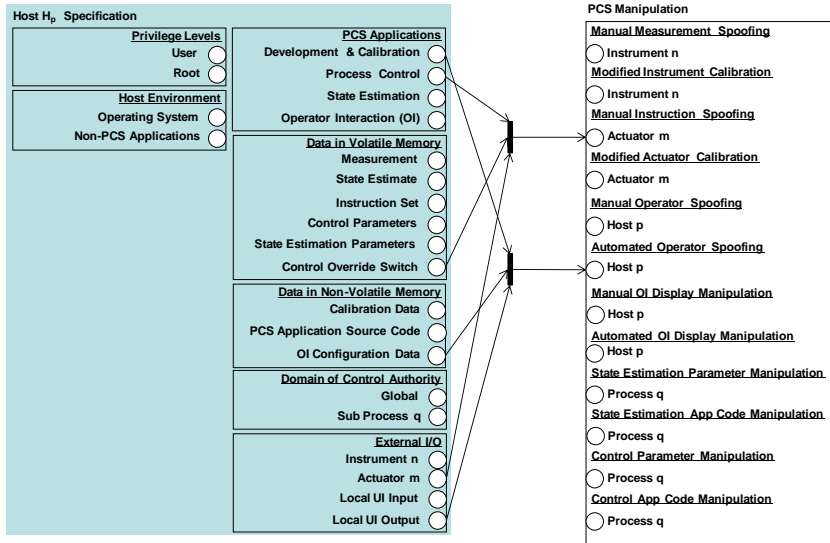
Let  $T_1$  denote the set of first-order transitions

The subset  $S_1 \subseteq T_1$  is assigned a value derived from the set of consequences avoided if the transitions are rendered inactive:



$$V^{S_1} = \sum \left\{ c^i \mid (\forall t \in S_1) m^i \in t^\bullet \wedge (\forall t' \in T_1) (t' \notin S_1 \rightarrow m^i \notin t'^\bullet) \right\} \quad (1)$$

# Trace-back for Risk Management



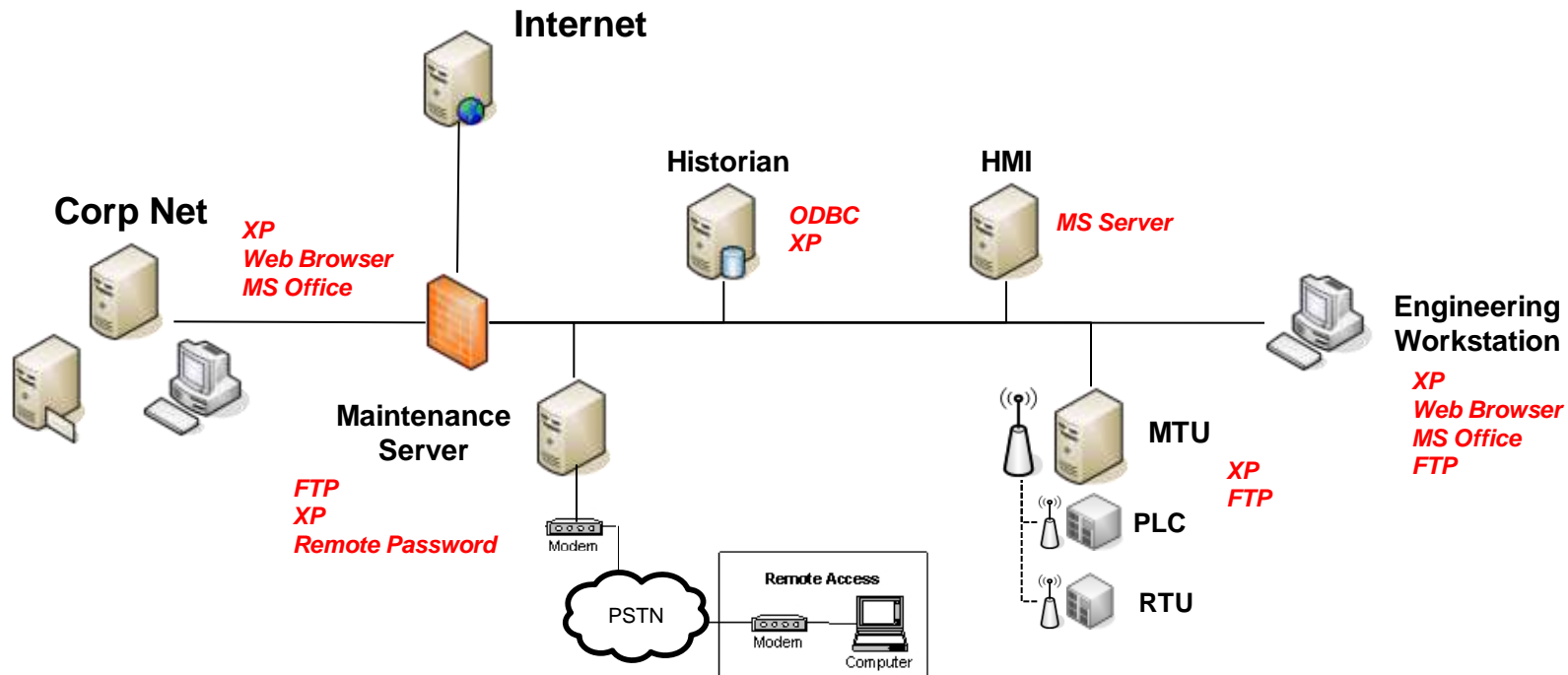
A transition  $t$  is a “second-order” transition if at least one of its post-conditions is a precondition for a first-order transition,  $t \in T_1$ , and it is enabled in at least one marking in the coverability set.

Let  $T_2$  denote the set of second-order transitions

The subset  $S_2 \subseteq T_2$  is assigned a value derived from the set of consequences avoided if the transitions are rendered inactive:

$$V^{S_2} = \sum_{S_1 \subseteq T_1} \left\{ V^{S_1} \left| \begin{array}{l} (\forall t_1 \in S_1) (\exists t_2 \in S_2) (\exists p \in (t_2 \cdot \cap \cdot t_1)) \\ \wedge (S_2' \subset S_2) \rightarrow (\exists t_1 \in S_1) (\forall t_2 \in S_2') (t_2 \cdot \cap \cdot t_1) = \emptyset \end{array} \right. \right\} \quad (2)$$

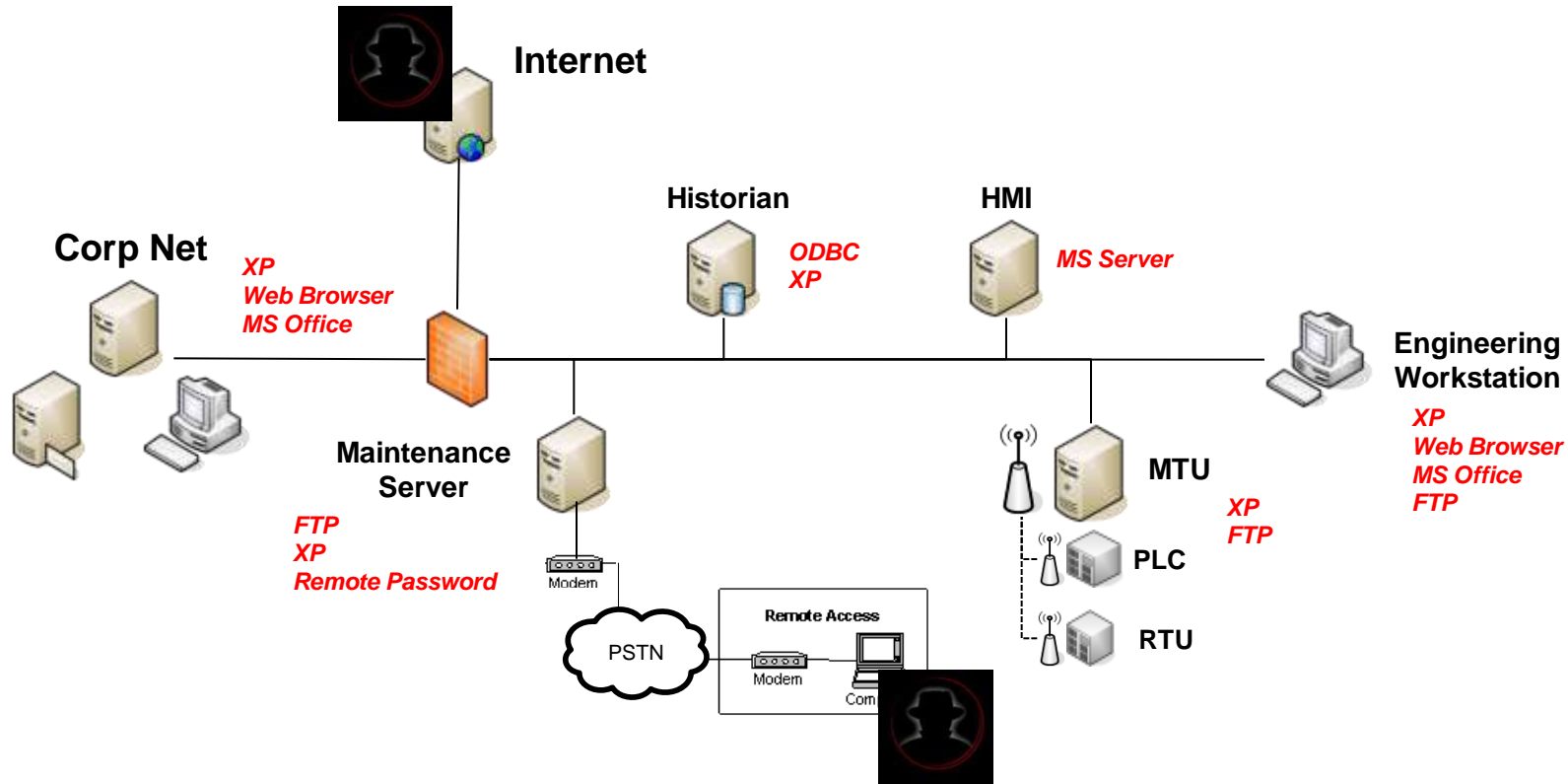
# Demonstration: PCS



## Firewall rules

- BLOCK** inbound connections from Internet to PCS
- ALLOW** outbound from PCS to Internet
- ALLOW** ODBC and FTP allowed from Corp to PCS

# Base Case



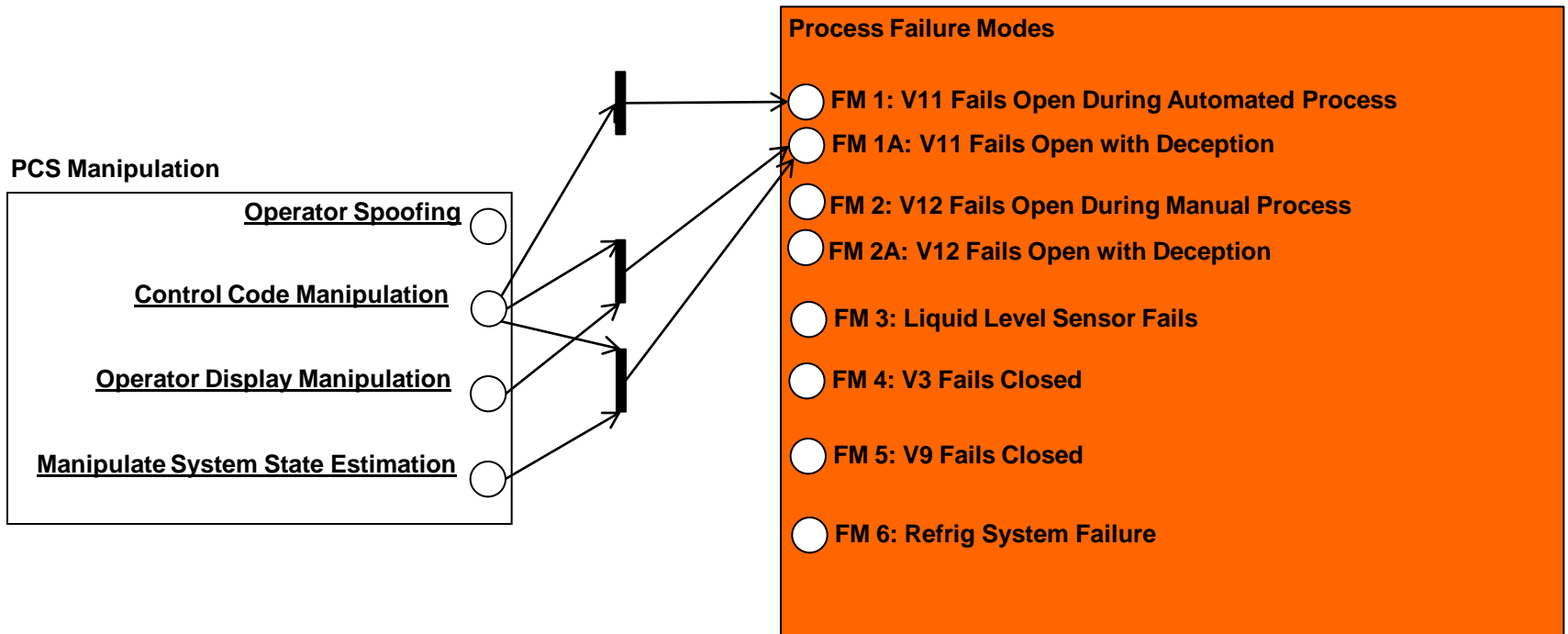
## Initial Conditions

Internet: Root Access  
Dial-up: Root Access

## Coverability Set (Reachable Adversary Control)

Historian: user, root  
HMI: user  
Maintenance: user, root  
MTU: user, root  
Engineering: user, root  
Corp: user, root

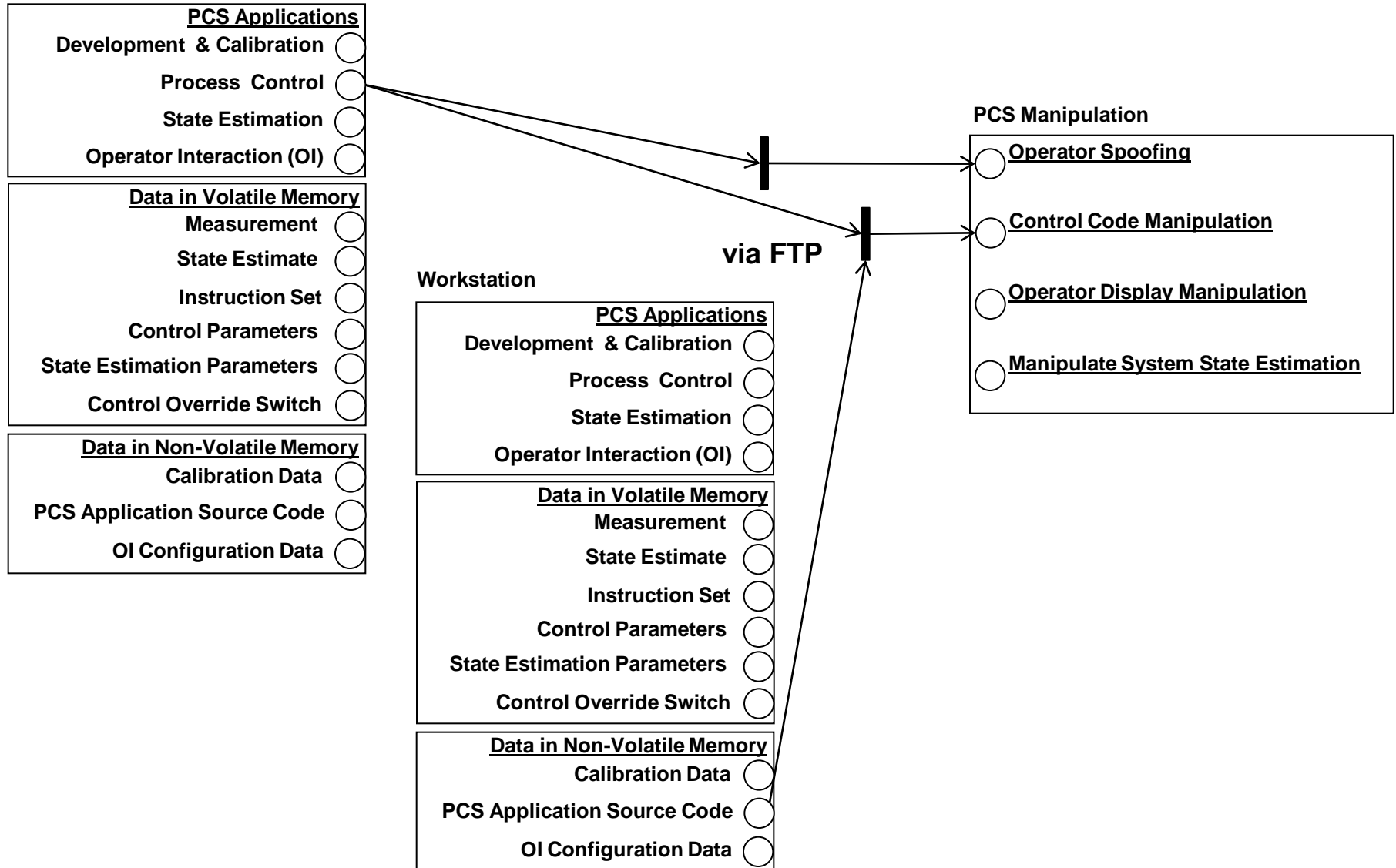
# Trace-back: First-Order Transitions



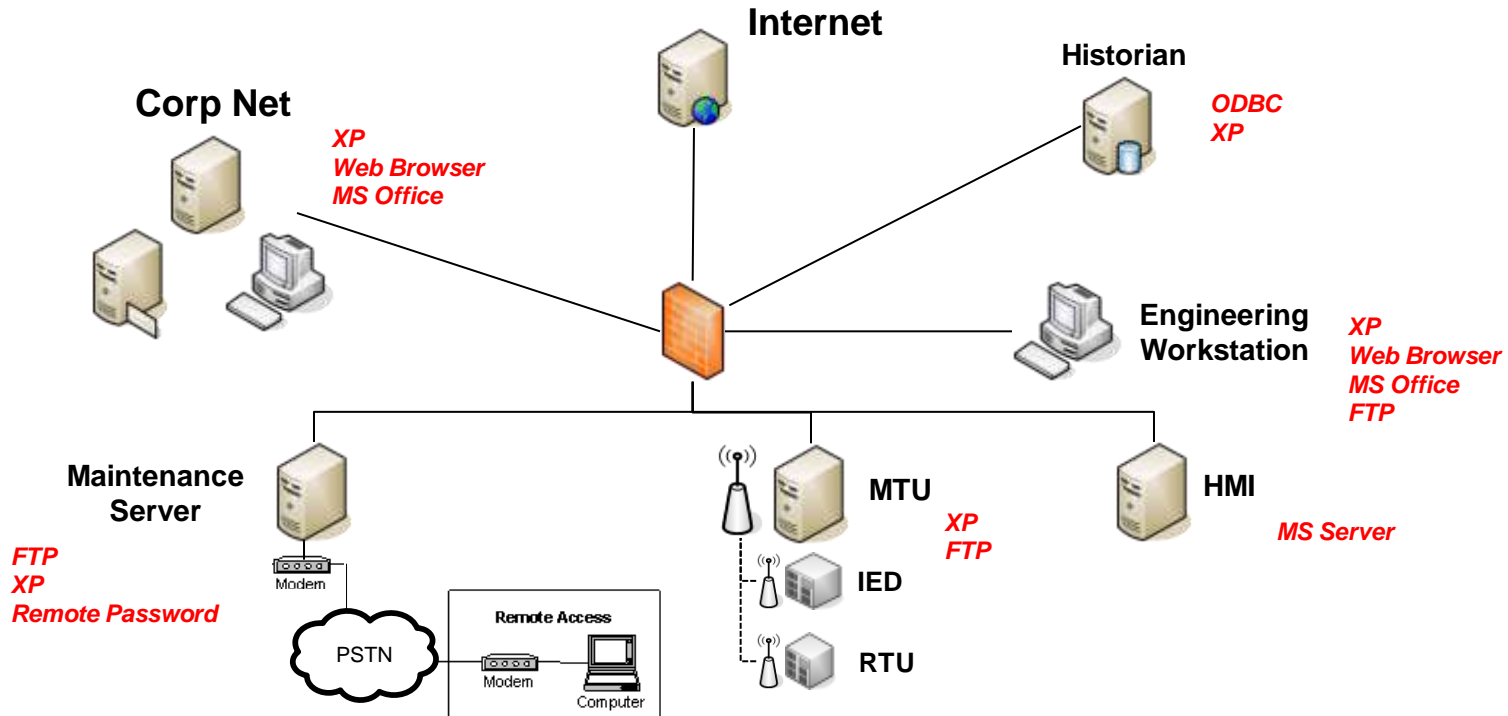
# Trace-back: Second-Order Transitions



MTU



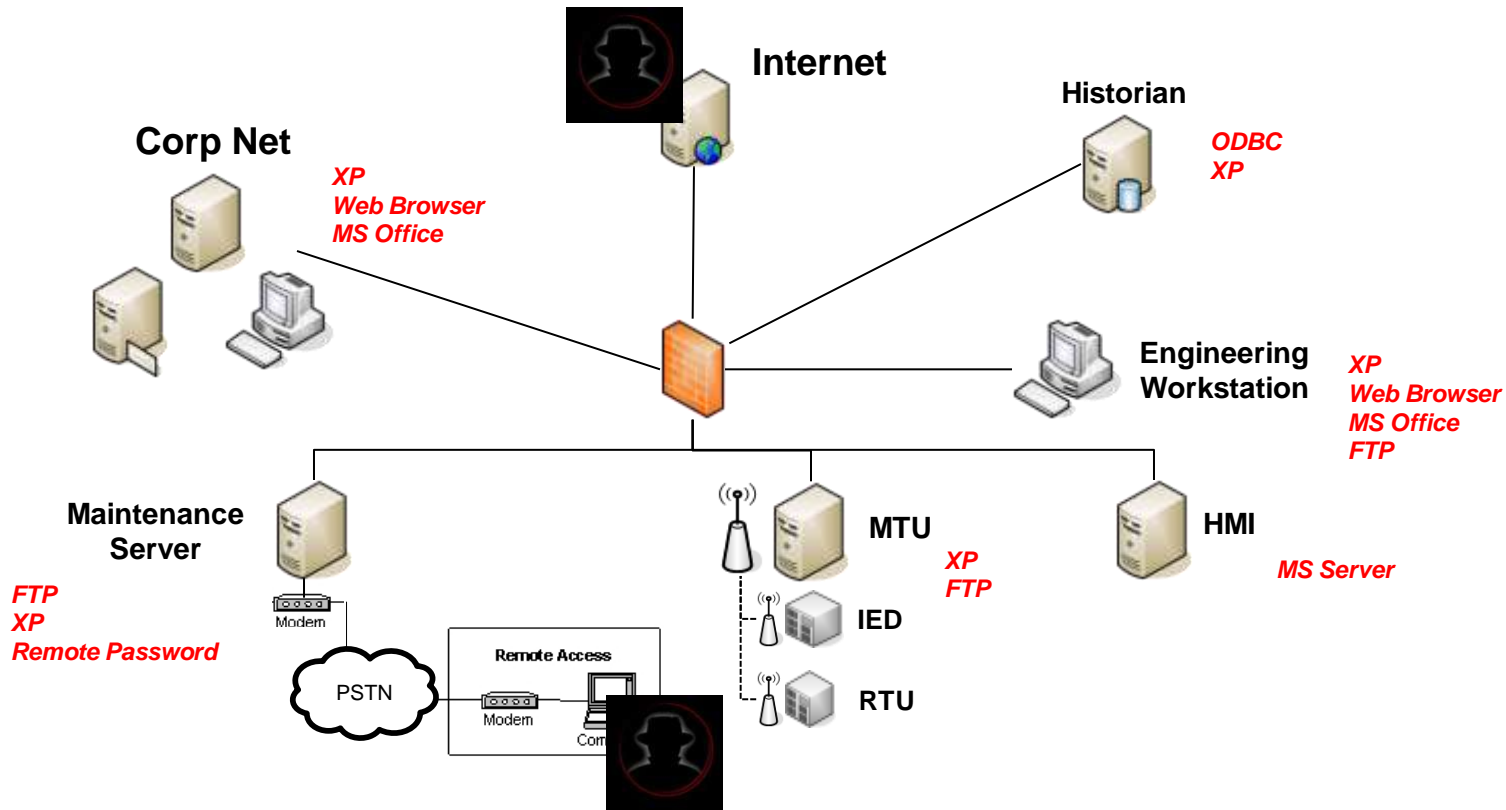
# Network Separation



## Firewall rules

- BLOCK** all connections from Internet to/from PCS, Historian, Engineering
- ALLOW** FTP to/from Corp to Engineering
- ALLOW** FTP to/from Engineering to PCS
- ALLOW** ODBC from Corp to Historian
- ALLOW** ODBC from Engineering to Historian
- ALLOW** Modbus from PCS to Historian

# Network Separation



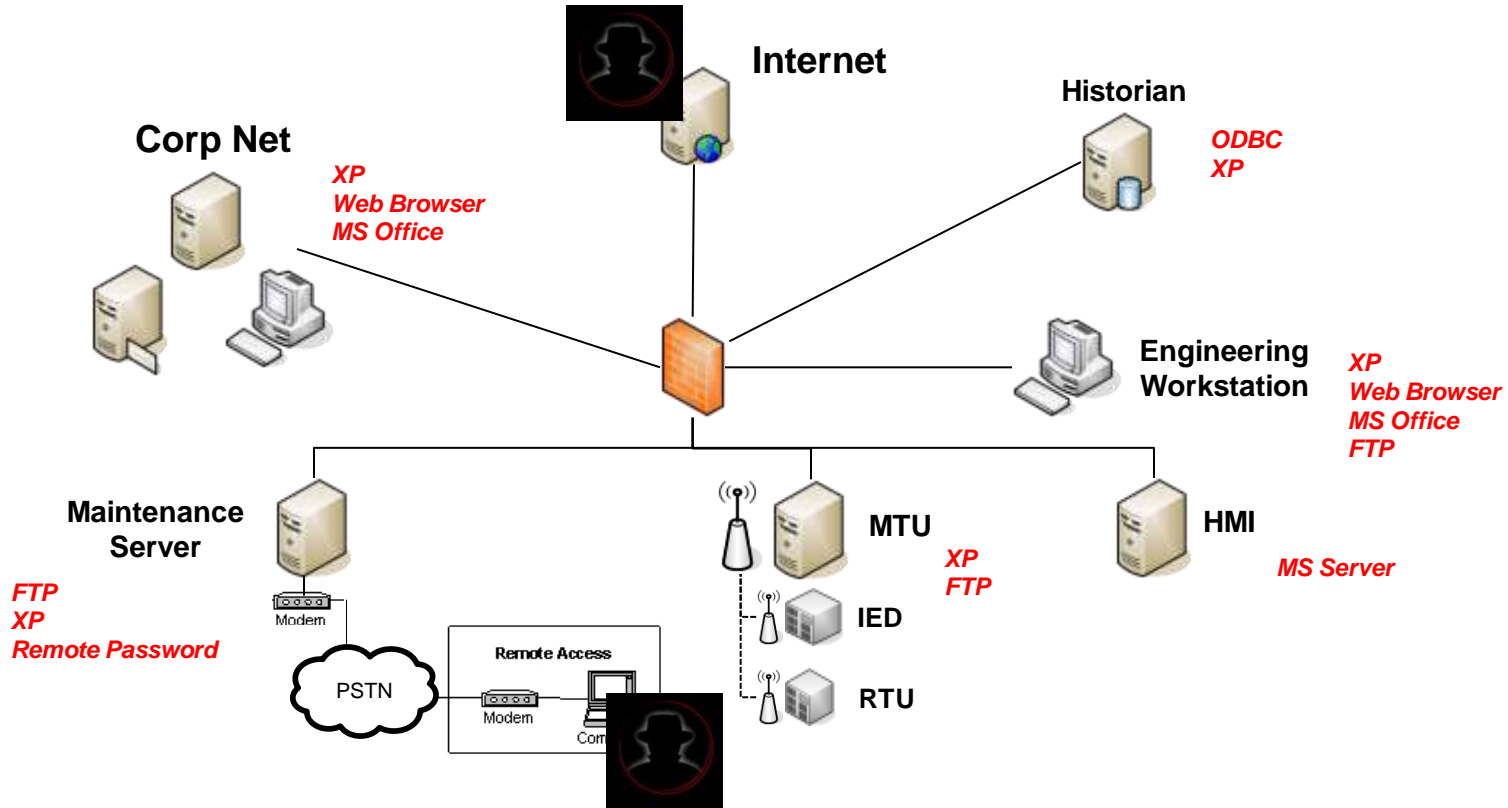
## Initial Conditions

Internet: Root Access  
Dial-up: Root Access

## Coverability Set (Reachable Adversary Control)

Historian: user, root  
HMI: user  
Maintenance: user, root  
MTU: user, root  
Engineering: user, root  
Corp: user, root

# Network Separation



## Initial Conditions

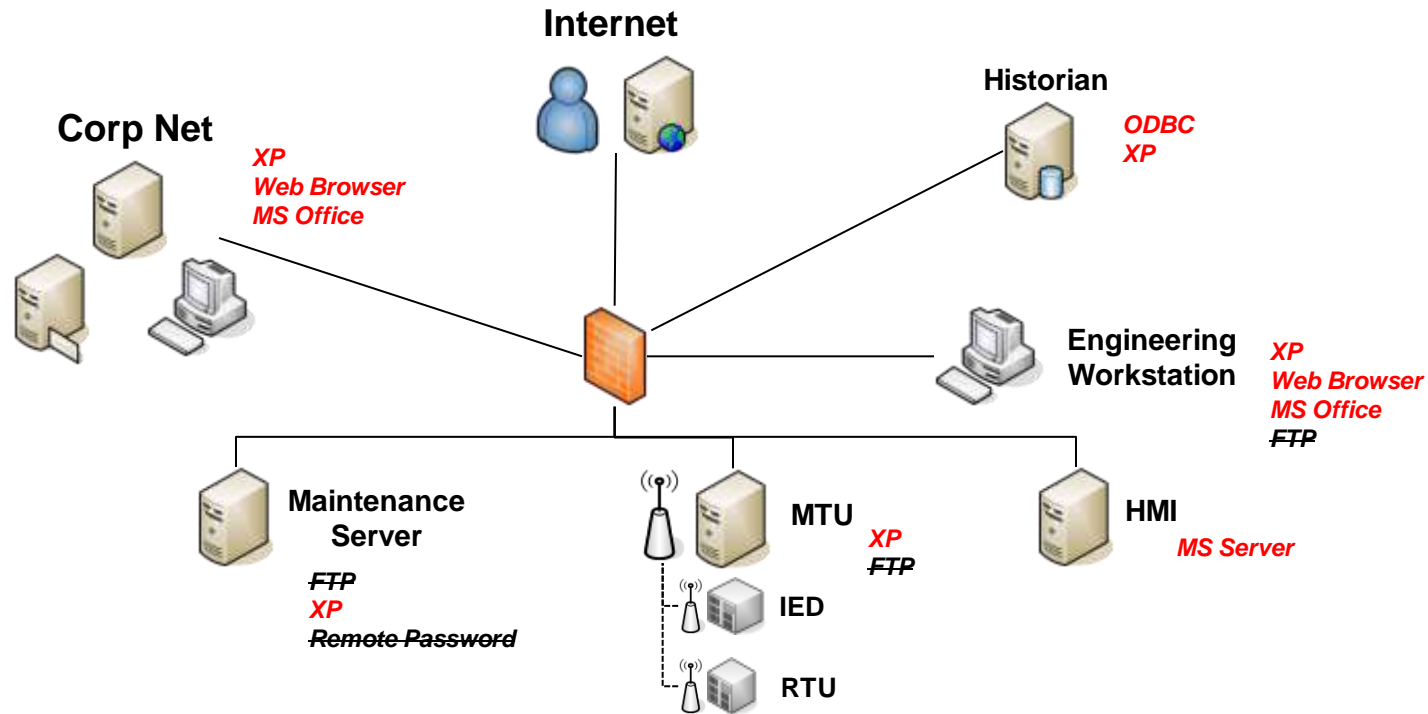
Internet: Root Access  
Dial-up: Root Access

## Coverability Set (Reachable Adversary Control)

Historian: user, root  
HMI: user  
Maintenance: user, root  
MTU: user, root  
Engineering: user, root  
Corp: user, root

**Same as  
Base Case!**

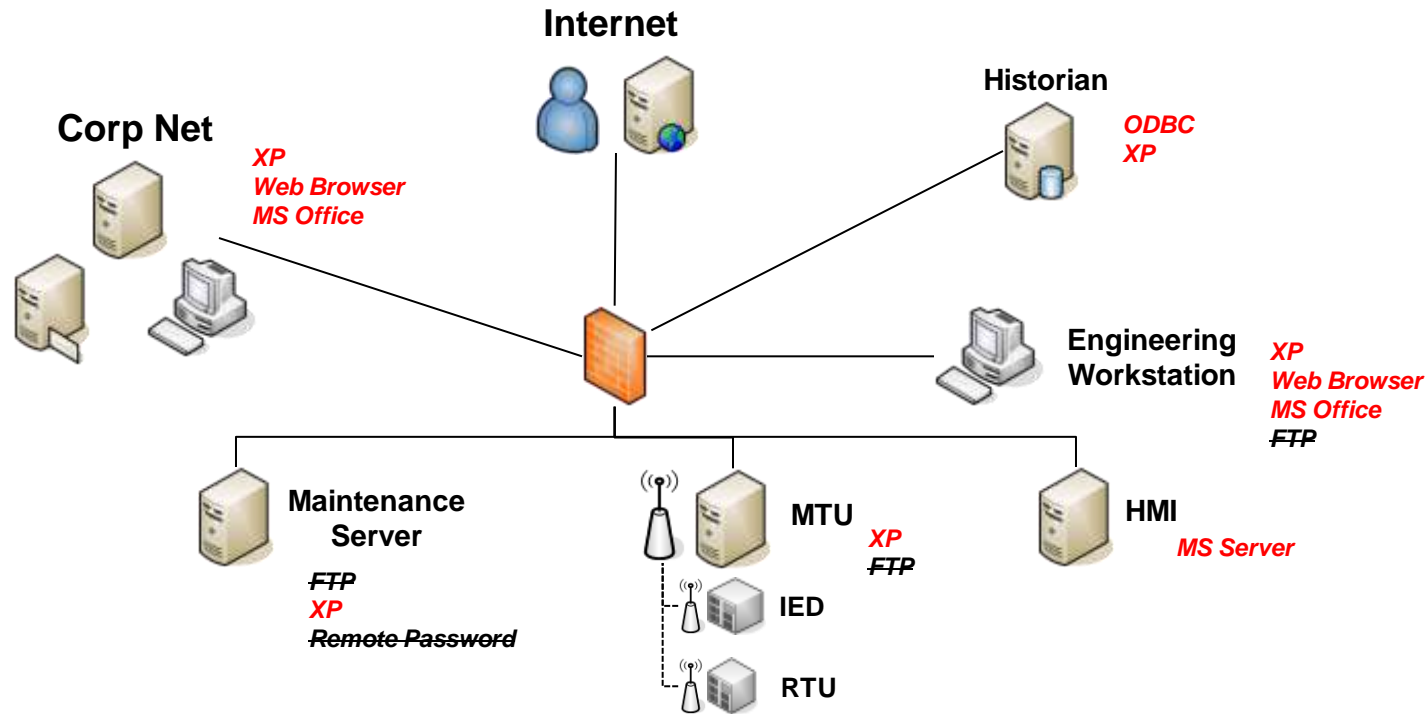
# Separation and Patch



## Firewall rules

- BLOCK** all connections from Internet to/from PCS, Historian, Engineering
- BLOCK** FTP to/from Engineering to PCS
- ALLOW** FTP to/from Corp to Engineering
- ALLOW** ODBC from Corp to Historian
- ALLOW** ODBC from Engineering to Historian
- ALLOW** Modbus from PCS to Historian

# Separation and Patch



## Initial Conditions

Internet: Root Access  
Dial-up: Root Access

## Coverability Set (Reachable Adversary Control)

Historian: user, root  
HMI: none  
Maintenance: none  
MTU: none  
Engineering: user, root  
Corp: user, root

## Coverability Set (Base Case)

Historian: user, root

HMI: user

Maintenance: user, root

MTU: user, root

Engineering: user, root

Corp: user, root

## Coverability Set (with DMZs)

Historian: user, root

HMI: user

Maintenance: user, root

MTU: user, root

Engineering: user, root

Corp: user, root

## Coverability Set (with DMZs and Patch)

Historian: user, root

HMI: none

Maintenance: none

MTU: none

Engineering: user, root

Corp: user, root

### Inducible Process Failure Modes:

1. Small qty gaseous ammonia discharge to dilution drum
- 1A. Large qty gaseous ammonia discharge to dilution drum
2. Automated fill task disabled
- 2A. Large qty liquid ammonia discharge to dilution drum
3. Tank Overfill
4. High-pressure gaseous ammonia discharge from damaged plumbing
5. High-pressure liquid ammonia discharge from damaged plumbing
6. Low-pressure gaseous ammonia discharge from damaged plumbing

### Inducible Process Failure Modes:

None

## **Highly conservative approach**

- **Provides an upper bound on “known” risk**
- **Implicit assumption that the IDS/IPS has failed**

## **Difficult to scale without simplifying assumption (monotonicity)**

- **Not bad, this is common and reasonable assumption**
  - **Can practically deal with network of up to  $O(10k)$  hosts**
- 
- **Good complement to our current work**

**Scalability**

**Metrics**

**Active Defense**

# Questions

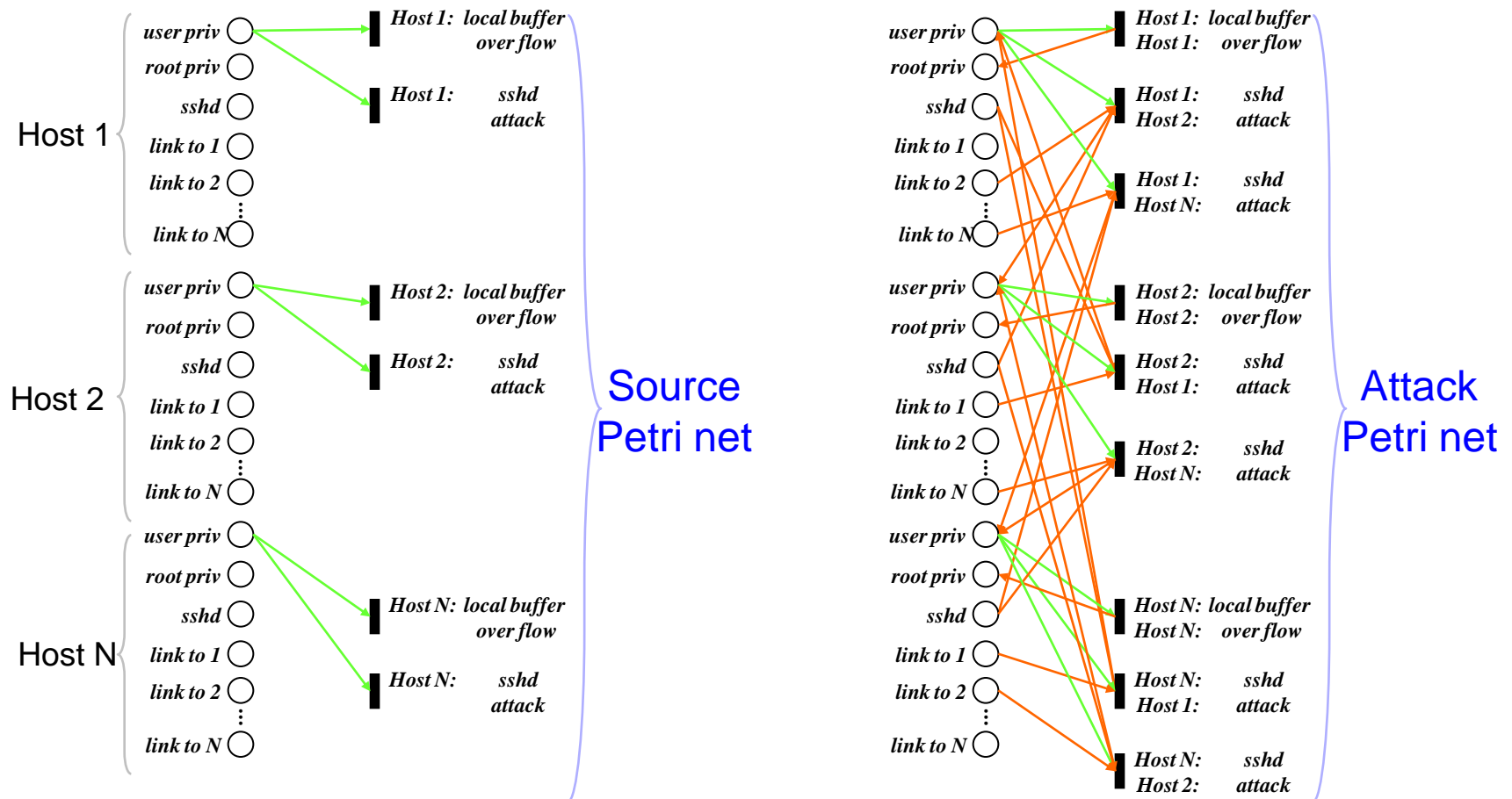
# Backup

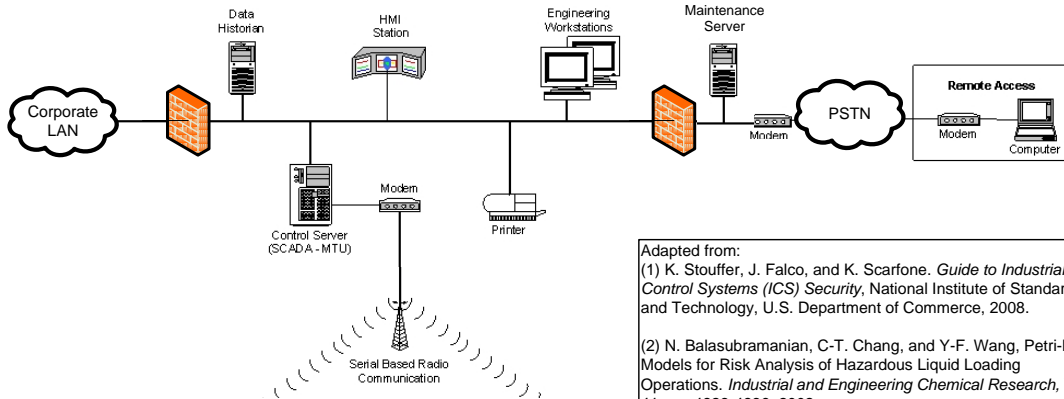
# Automated Petri Net Generation

Input: exploits and network attributes

each exploit has a set of pre- and post-conditions

network attributes includes host properties and connectivity





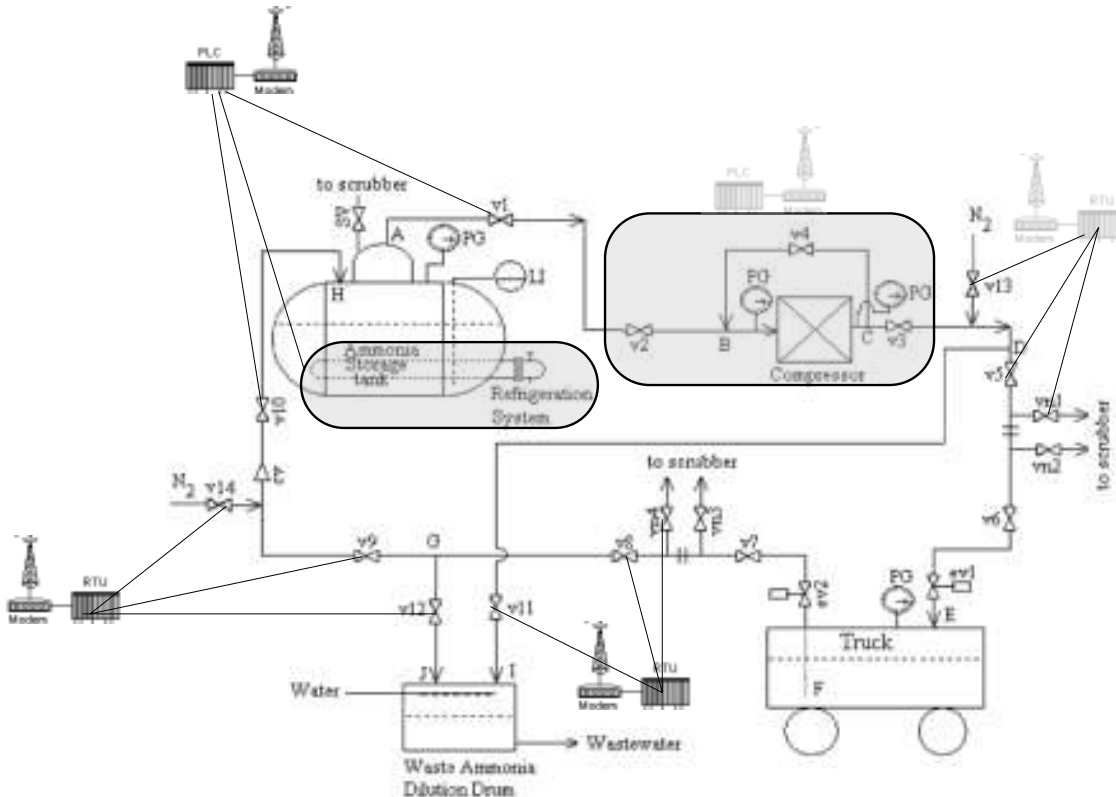
Adapted from:  
 (1) K. Stouffer, J. Falco, and K. Scarfone. *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, U.S. Department of Commerce, 2008.  
 (2) N. Balasubramanian, C-T. Chang, and Y-F. Wang, Petri-Net Models for Risk Analysis of Hazardous Liquid Loading Operations. *Industrial and Engineering Chemical Research*, Vol. 41, pp. 4823-4836, 2002.

## Remote Manual Control of

- V1-V3, V9-V12
- Compressor
- Refrigeration System

## Automation of

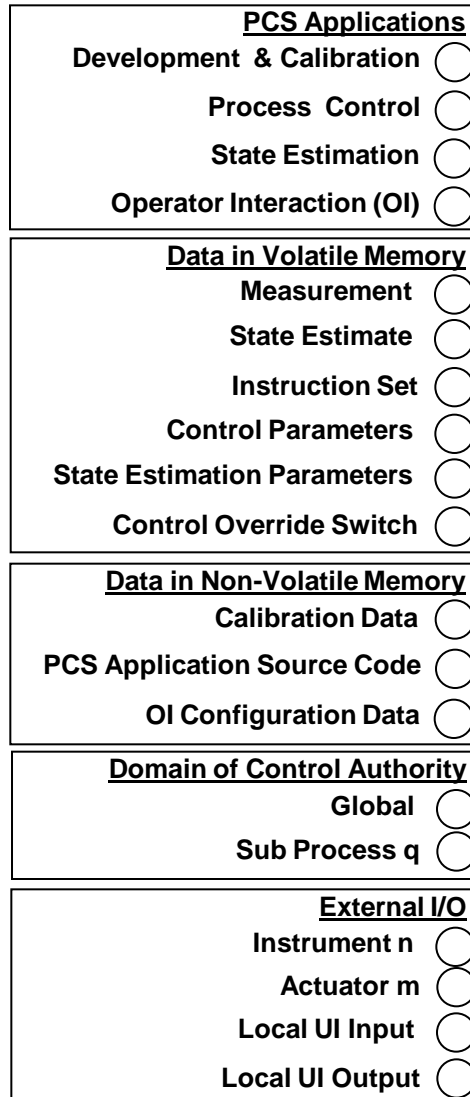
- Compressor Prime Process
- Tank Fill Process
- Compressor Shut-down Process



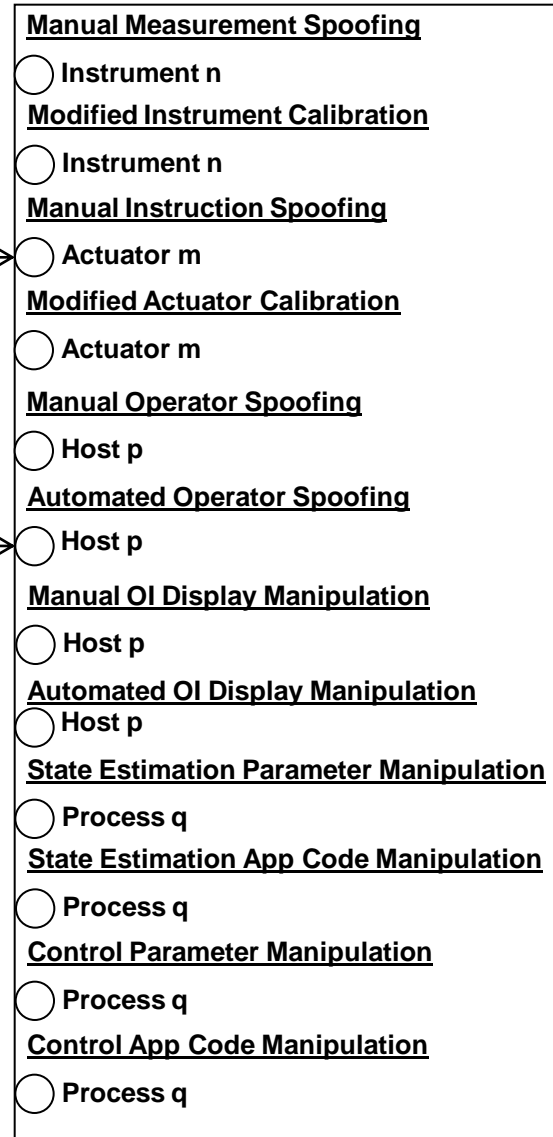


# Host Access to Process Control Coupling

## PCS Functionality



## PCS Manipulation



Case 1: Valve V11 Fails Open prior to executing Task 4 (Part of Automated Task)

- Consequence: Gaseous ammonia discharges into dilution drum
- Resources Required: Any one of the following
  - MTU root (manipulate automation software on host)
  - Workstation root (manipulate automation software via FTP)
  - Maintenance server super-user (manipulate automation software via FTP)

Case 1A: Valve V11 Fails Open prior to executing Task 4 AND V11 state spoofed as closed at HMI (Part of Automated Task)

- Consequence: Large qty gaseous ammonia discharges into dilution drum
- Resources Required: [HMI root (manipulate state representation driver) OR MTU root (manipulate state tracking software)] AND any one of the following
  - MTU root (manipulate automation software on host)
  - Workstation root (manipulate automation software via FTP)
  - Maintenance server root (manipulate automation software via FTP)

Case 2: Valve V12 Fails Open during execution of Task 2 (Manual operations)

- Consequence: Automated Fill Task (Tasks 3,4, and 5) will be disabled
- Resources Required: Any one of the following
  - HMI user Access (Issue direct instruction)
  - MTU user access (Spoof HMI instruction)

Case 2A: Valve V12 Fails Open during execution of Task 2 (Manual operations) without being noticed at HMI

- Consequence: Large quantity liquid ammonia discharge to dilution drum
- Resources Required:
  - MTU super-user access (spoof HMI instruction and manipulate state tracking software on host)
  - Workstation root (manipulate automation software via FTP)
  - Maintenance server root (manipulate automation software via FTP)

Case 3: Liquid Level Sensor Failure during execution of Task 4 (Part of Automated Task)

- Consequence: Overfill of tank
- Resources Required:
  - MTU super-user (manipulate automation software on host)
  - Workstation super-user (manipulate automation software via FTP)
  - Maintenance server super-user (manipulate automation software via FTP)

Case 4: Valve V3 Fails Closed after Compressor Warm-up during execution of Task 3 (Part of Automated Task)

- Consequence: Pressure Surge at V3 induces structural pipeline failure and discharge of high-pressure gaseous ammonia from damaged plumbing
- Resources Required:
  - MTU super-user (manipulate automation software on host)
  - Workstation super-user (manipulate automation software via FTP)
  - Maintenance server super-user (manipulate automation software via FTP)

## Case 5: Valve V9 Fails Closed during Task 4 (Part of Automated Task)

- Consequence: Pressure Surge at V9 induces structural pipeline failure and discharge of high-pressure liquid ammonia from damaged plumbing
- Resources Required:
  - MTU super-user (manipulate automation software on host)
  - Workstation super-user (manipulate automation software via FTP)
  - Maintenance server super-user (manipulate automation software via FTP)

## Case 6: Refrigeration System Fails

- Consequence: Increase in pressure on gaseous ammonia pipelines and low-pressure gaseous ammonia discharge from damaged plumbing
- Resources Required:
  - MTU super-user (manipulate automation software on host)
  - Workstation super-user (manipulate automation software via FTP)
  - Maintenance server super-user (manipulate automation software via FTP)