

# Intrusion Insights – Adapting Intrusion Prevention Functionality for Process Control SCADA Systems

National Workshop on  
Beyond SCADA: Networked Embedded Control  
for Cyber Physical Systems  
November 8<sup>th</sup> & 9<sup>th</sup>  
Pittsburgh, Pennsylvania

Ernest A. Rakaczky



**Invensys**<sup>®</sup>  
Process Systems

Get More from One

Avantis • Foxboro • SimSci-Esscor • Triconex

# Key Issues - Concerns



**invensys**®

# Control System Data Isolation

## The Ever Changing Environment

- **Knowledge of and Attack Sophistication**
- **Ever Increasing Vulnerabilities & Incidents**
- **The decreasing time between launch & actual Incidents...**

**“ The Day Zero Impact ”**



# Control System Data Isolation

- Key Data Concerns
  - **Multiple Connections into most Control Systems**
    - **Some paths developed just for ease, not business driven**
  - **Very weak if any network Monitoring**
  - **Excessive data being transferred**
  - **Very weak control on actual Data access**
    - **Who needs the DATA & why is the Data needed**



# Control System Data Isolation

***“ Our Key Concern ”***

***The possible impact of Day Zero***

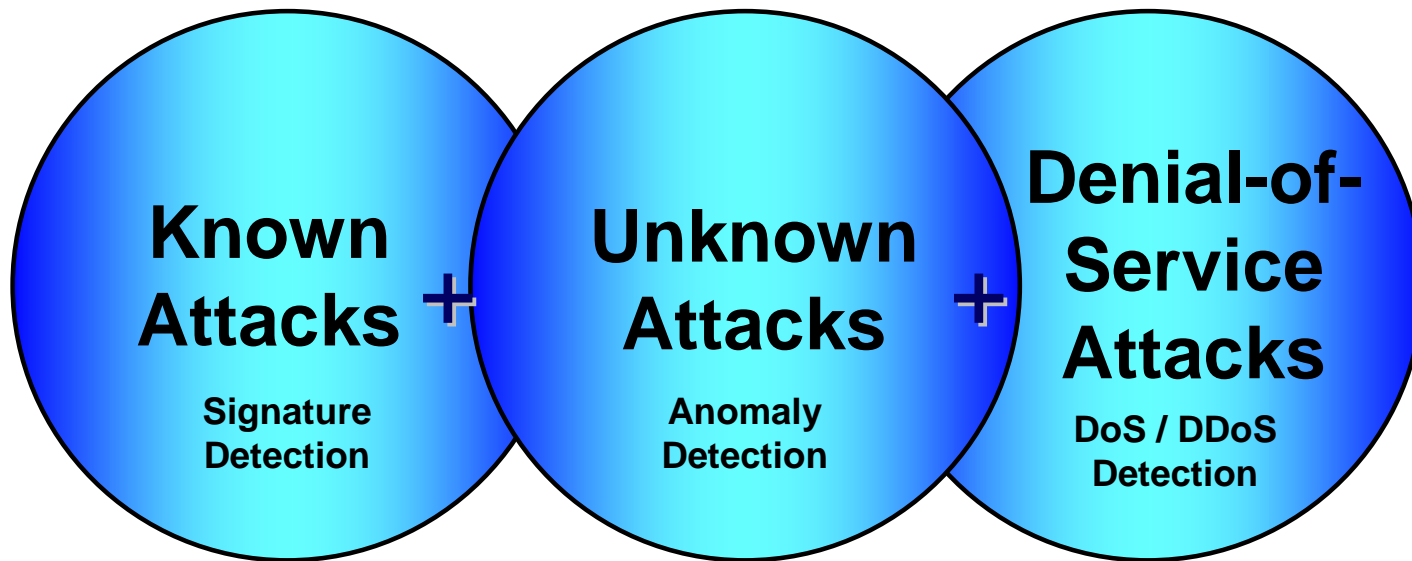
- Not addressed in Anti-Virus Signatures
- Not addressed in Network Detection/Monitoring
- Not addressed with a Patch Management Process

***All are Critical & Imperative - but fall short.....***



# Control System Data Isolation

## Intrusion Prevention Through Innovation

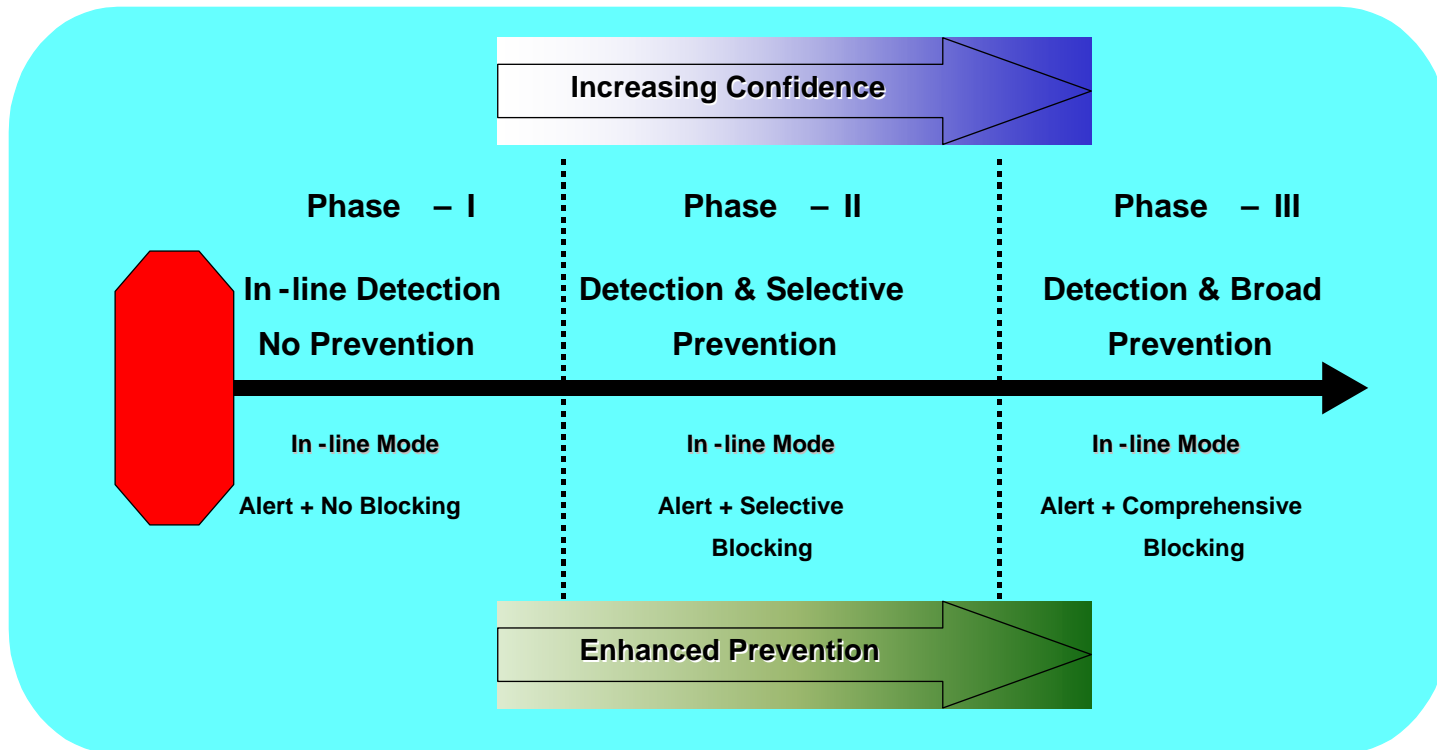


**Both Network & Host IPS should incorporate all Three Functions...**



# Control System Data Isolation

## Three Phases Of NIPS Implementation



Prevention is an evolutionary process... it builds upon TRUST

**An IPS must be Highly Accurate IDS first!**

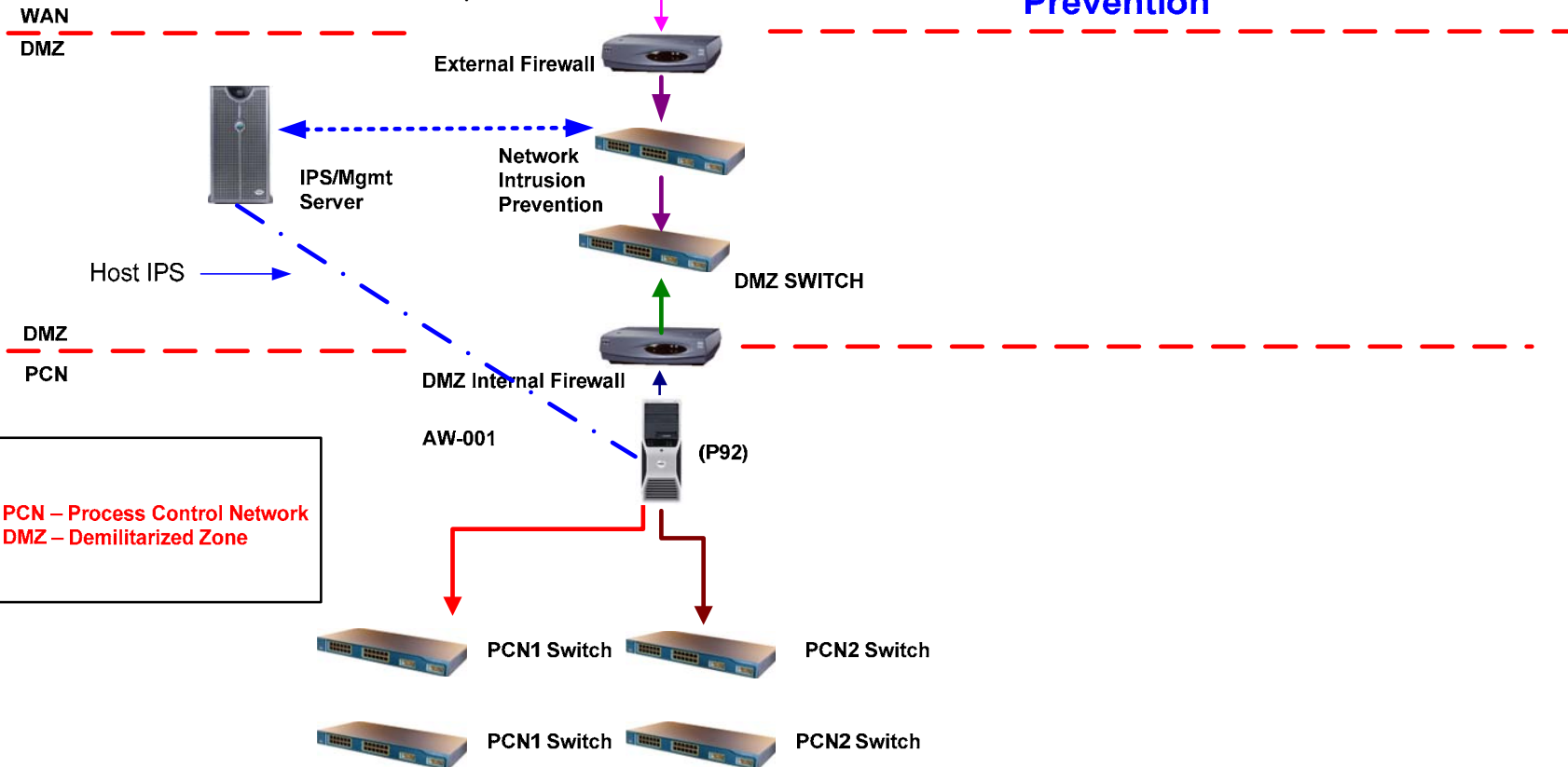
# Control System Data Isolation

Legend	
	Office Network Subnet
	DMZ Network Subnet (External-side)
	DMZ Network Subnet (Internal-side)
	TCP/IP Process Network Subnet
	I/A Control Network Subnet A
	I/A Control Network Subnet B

Proposed System Architecture



“ Adding Network Host Intrusion Prevention ”



PCN – Process Control Network  
DMZ – Demilitarized Zone

# Thank You

Ernest A. Rakaczky

[Ernest.rakaczky@ips.invensys.com](mailto:Ernest.rakaczky@ips.invensys.com)

