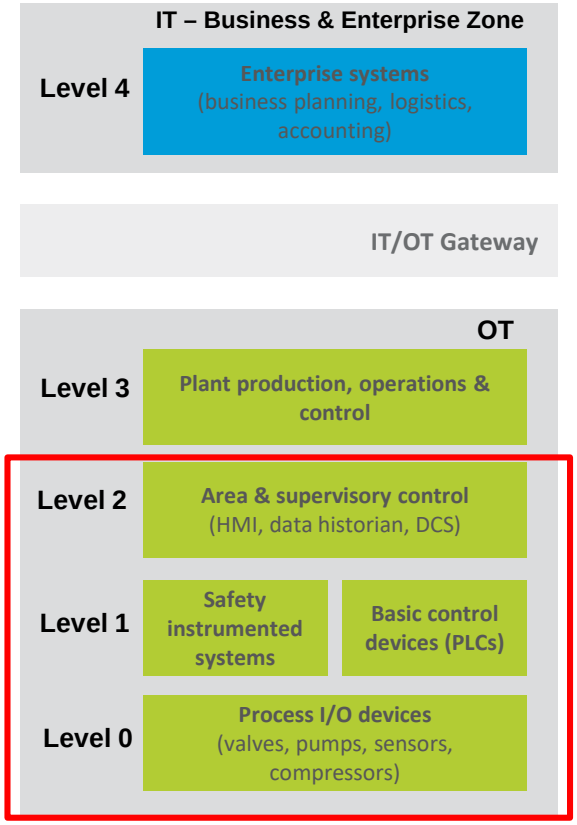
# OT Component Level Cyber Protection : A New Paradigm

## The Problem

Purdue Model **levels 0-2 currently lack cyber protections** leaving process control systems vulnerable when an attack penetrates into the operational technology (OT) space




Purdue ICS Cyber Model

### What Current IT Protections Do (IDS/IDP/Firewalls)

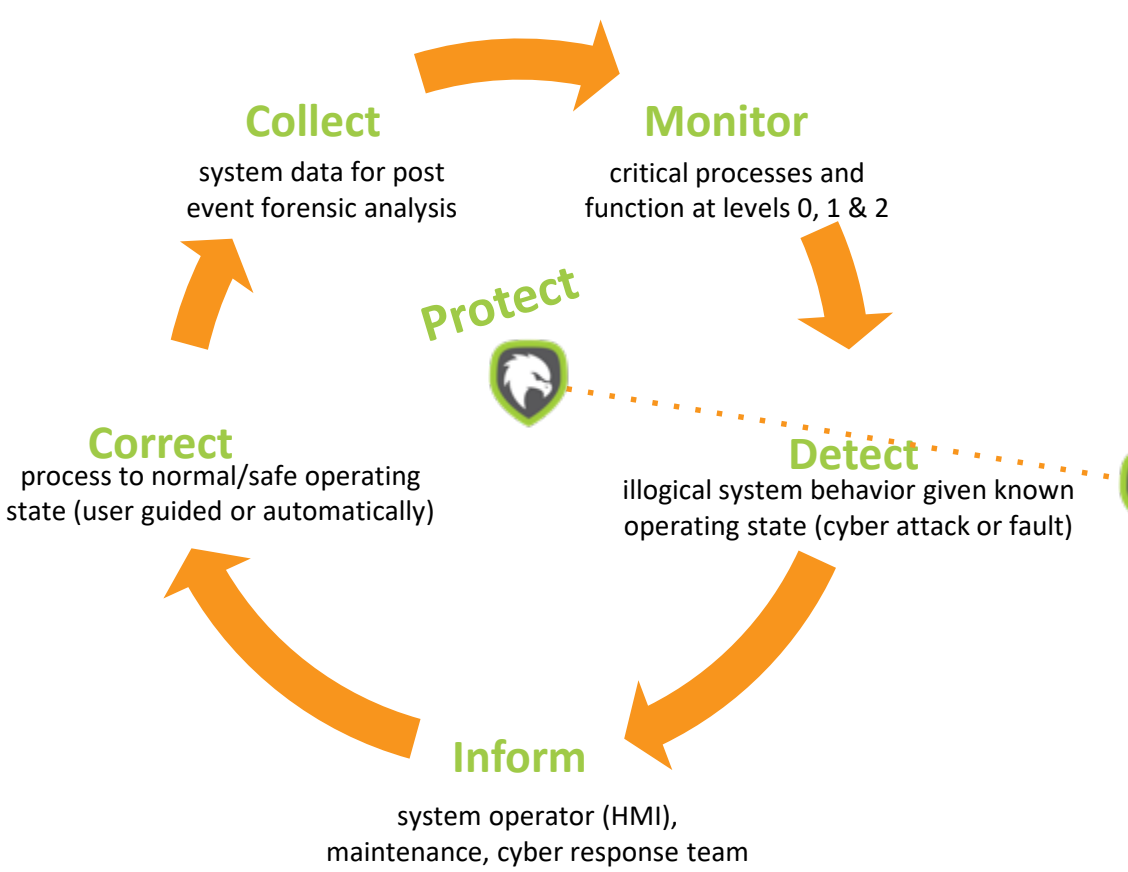
- Stop entry based on known exploits and rules, not on Zero Day attacks
- Forewarn that an event might occur
- Monitor network looking for “abnormal” behavior
- Provide Data to what has happened at the network level (not specific to equipment)

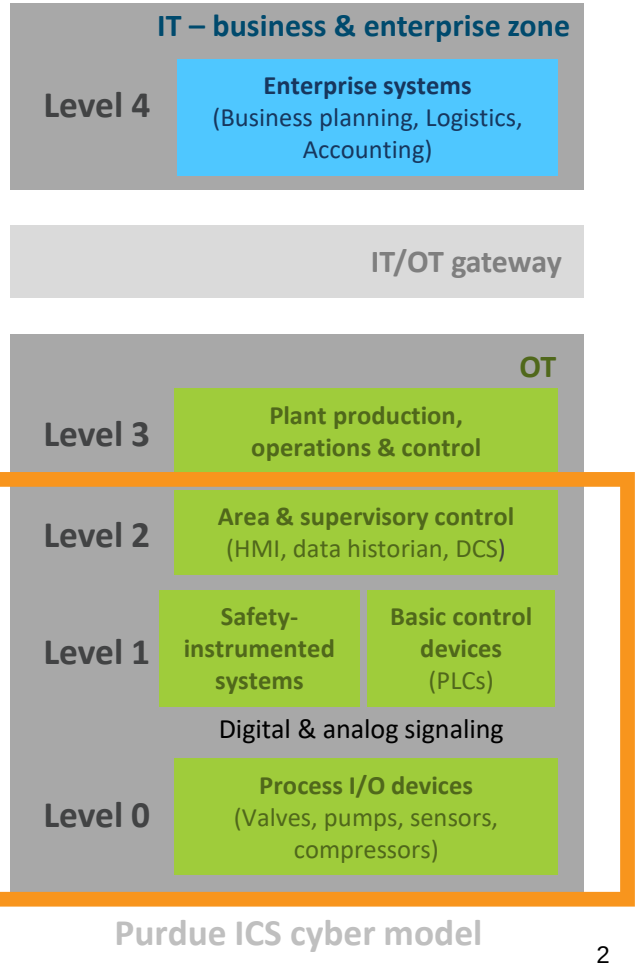
### The Gap - OT Protections

- Clearly understand an attack is underway and stop it from occurring - real time
- Detect attacks no matter how they are being initiated (no need for prior pattern)
- Provide detailed, specific forensic data for post event analysis
- Protect against, Zero Days, Supply Chain Attacks, Insider Attacks, ransomware, etc.

# Protection: IT Security without OT Security isn't Security

## Protection from Cyber Attacks




Purdue ICS cyber model