iTrust

Centre for Research in Cyber Security

# Can AI Secure Critical Infrastructure?

**Aditya Mathur**

iTrust

Center for Research in Cyber Security

Singapore University of Technology and Design

Singapore

**Public Sector CIO Convex 2017**
**Putrajaya, Malaysia**

October 5-6, 2017

# Critical Infrastructure and incidents

# Critical Infrastructure

16 sectors identified by ICS CERT

Energy ⟵

Water ⟵

Focus in iTrust

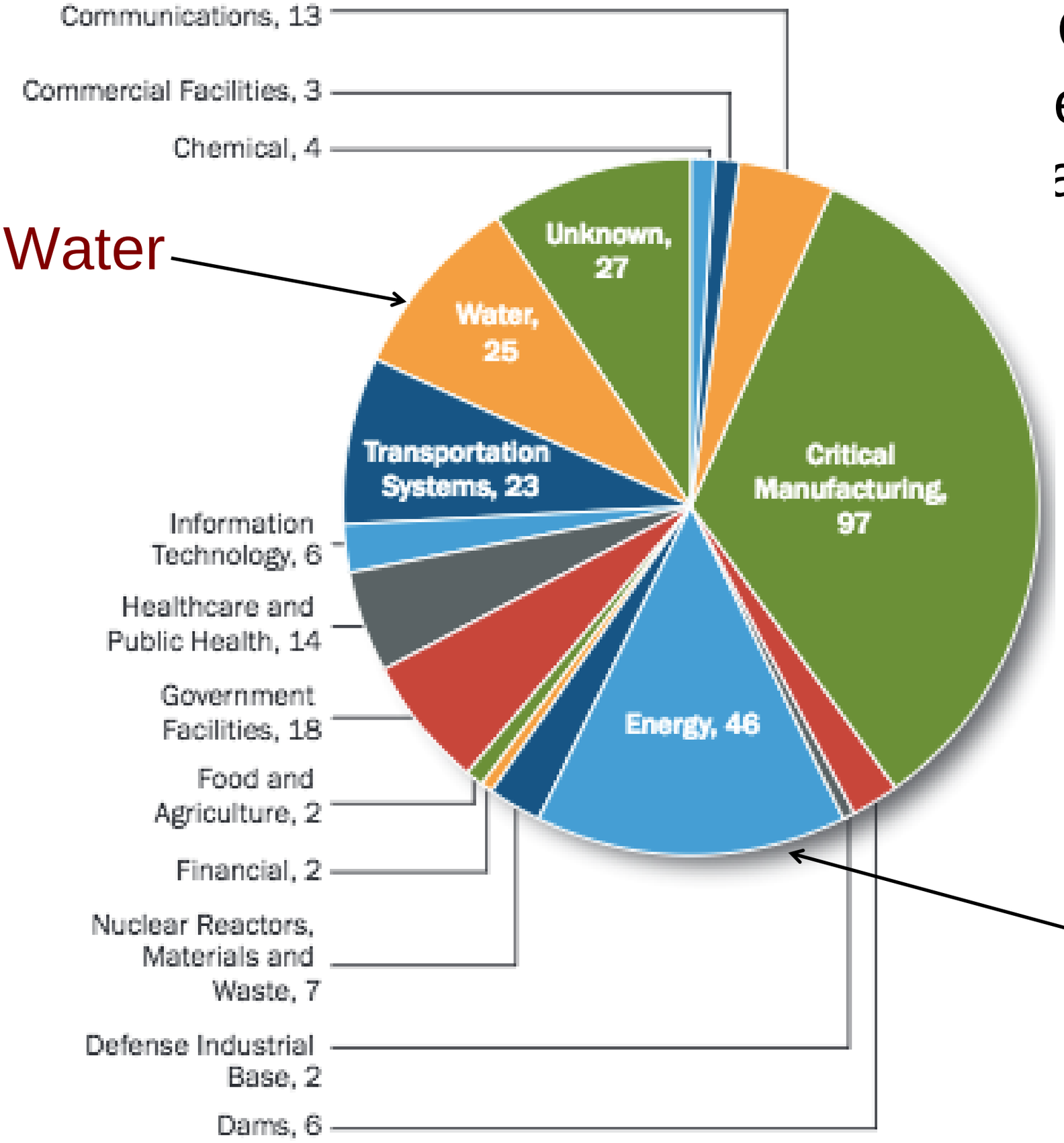
Transportation

Manufacturing

Healthcare

Etc.

# Incidents




CCIC/ICS-CERT
ear in Review,
age 17

# A sample of recent (successful) cyber attacks

Iranian nuclear enrichment plant

German steel mill

Ukraine power grid [twice in two years]

# How to defend critical infrastructure against cyber and cyber-physical attacks?

# Is AI useful? Effective?

# What is “Defense?”

Firewalls, IDS etc.

Prevention: Prevent unauthorized access to the plant

Detection: Identify and report process anomaly with 100% accuracy and zero false alarms

Our focus

Control: Take appropriate actions after detection

# What is Artificial Intelligence?

A field wherein algorithms and tools attempt to mimic human intelligence in their actions.

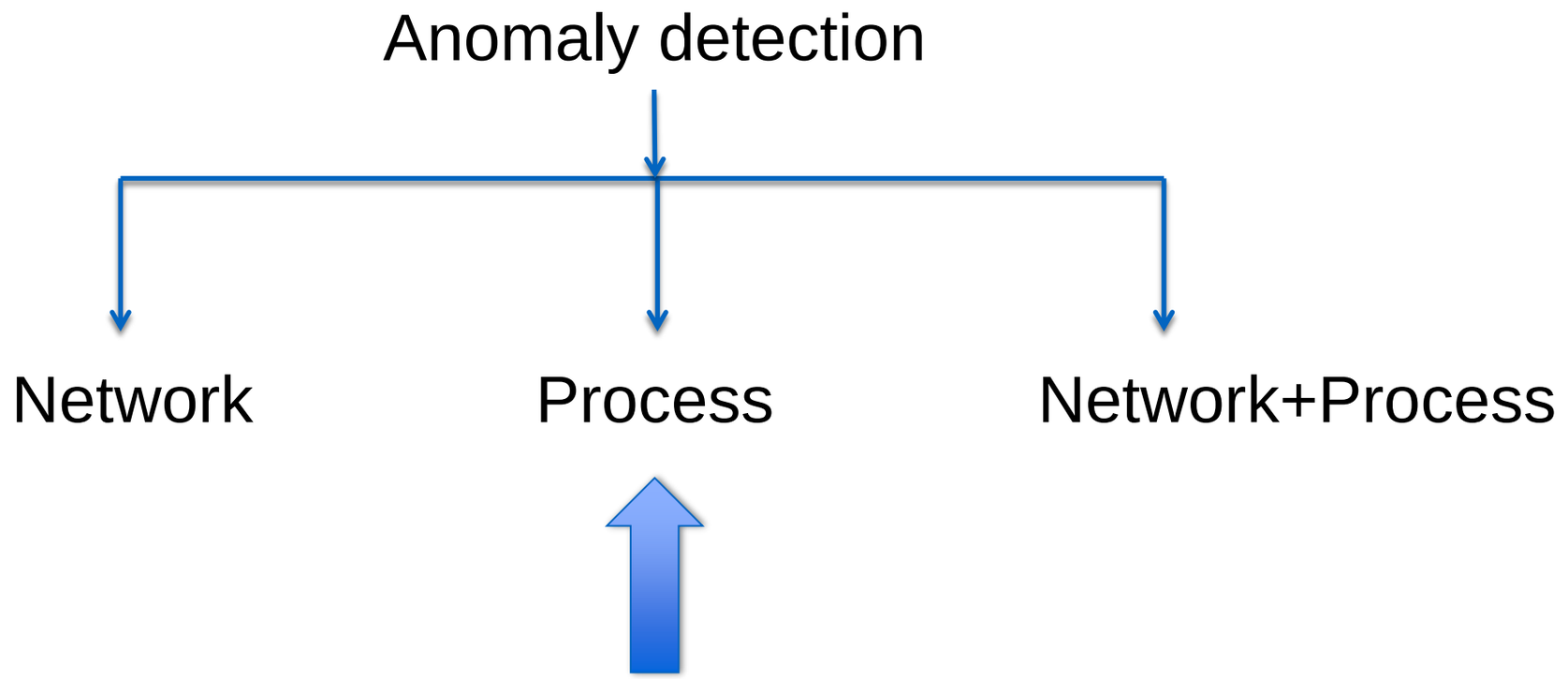
# Attacker types

External: enters the system via network

Internal: is “in the plant”;
has vast plant knowledge and credentials

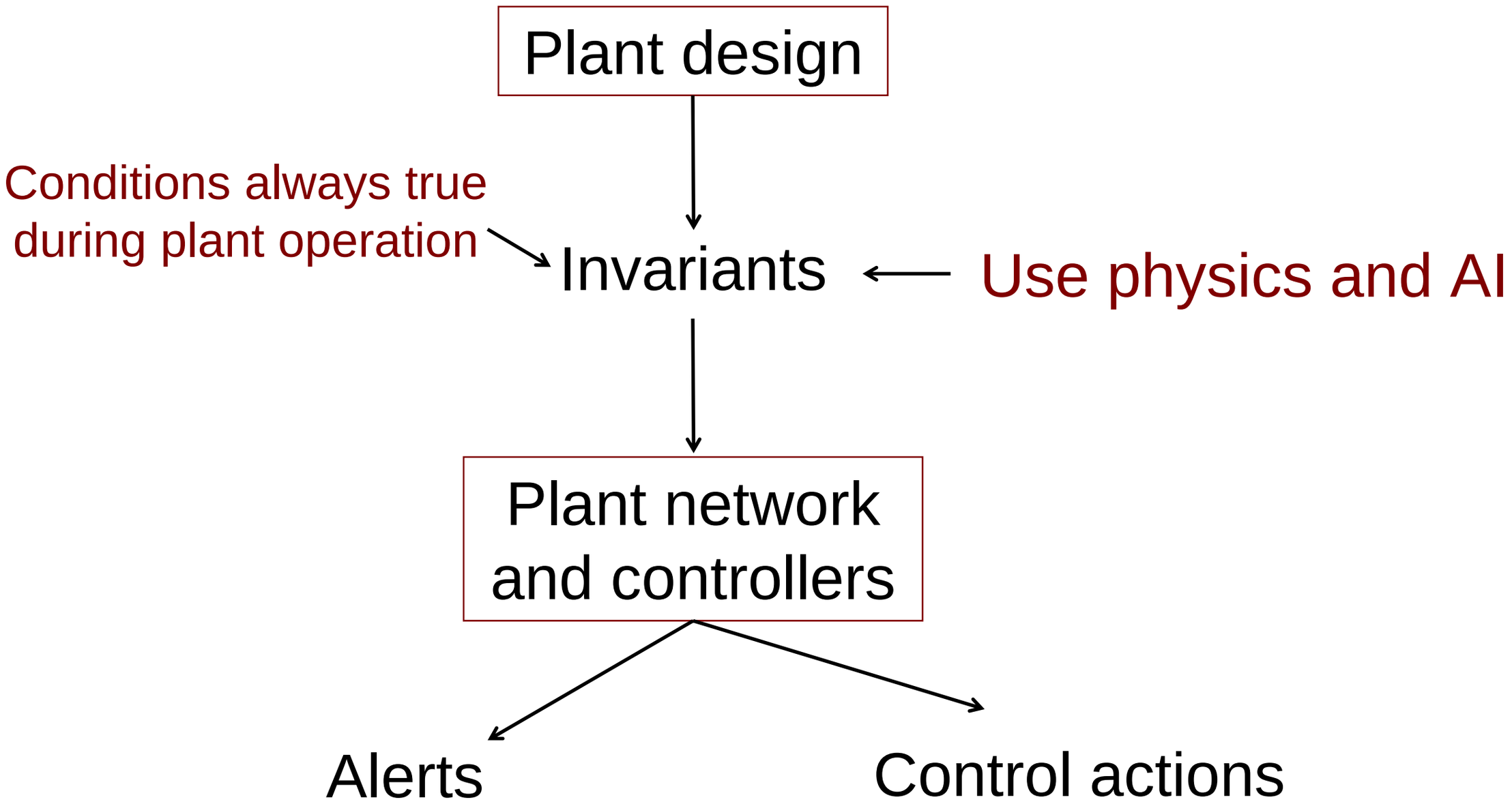
“External” can become “Internal” through extensive r
econnaissance and social engineering.

# Existing Approaches for Attack Detection

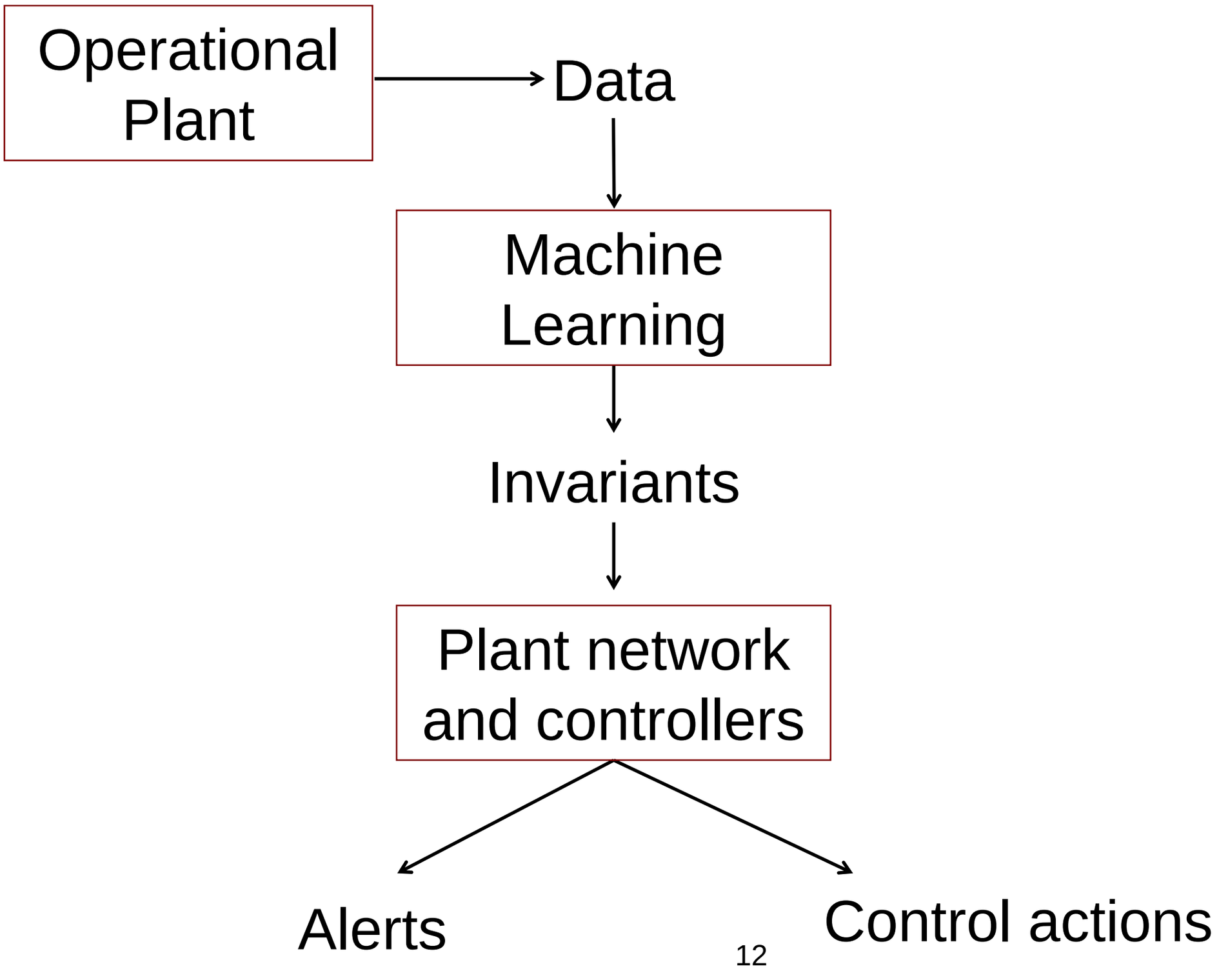



Our focus

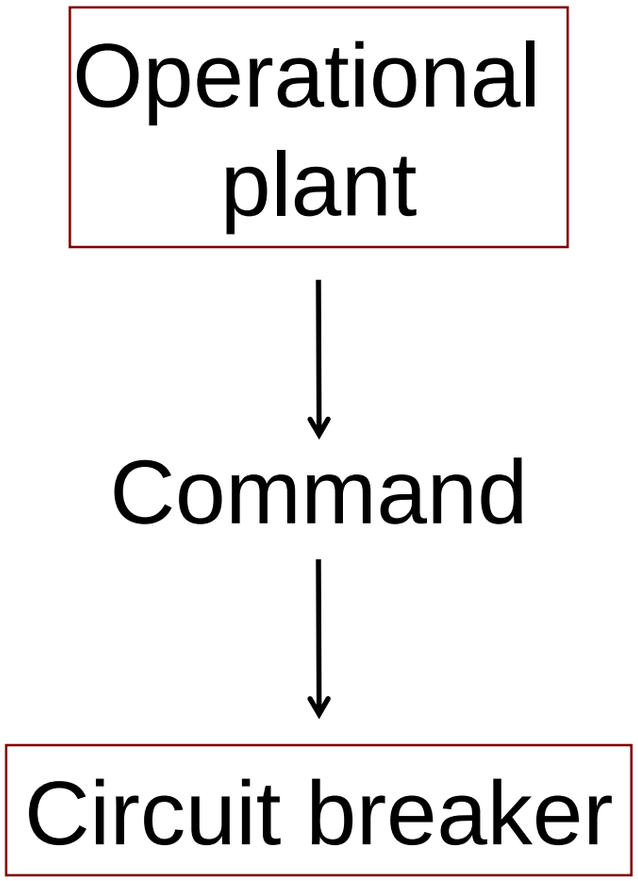
# Detection: Design-Centric Approach



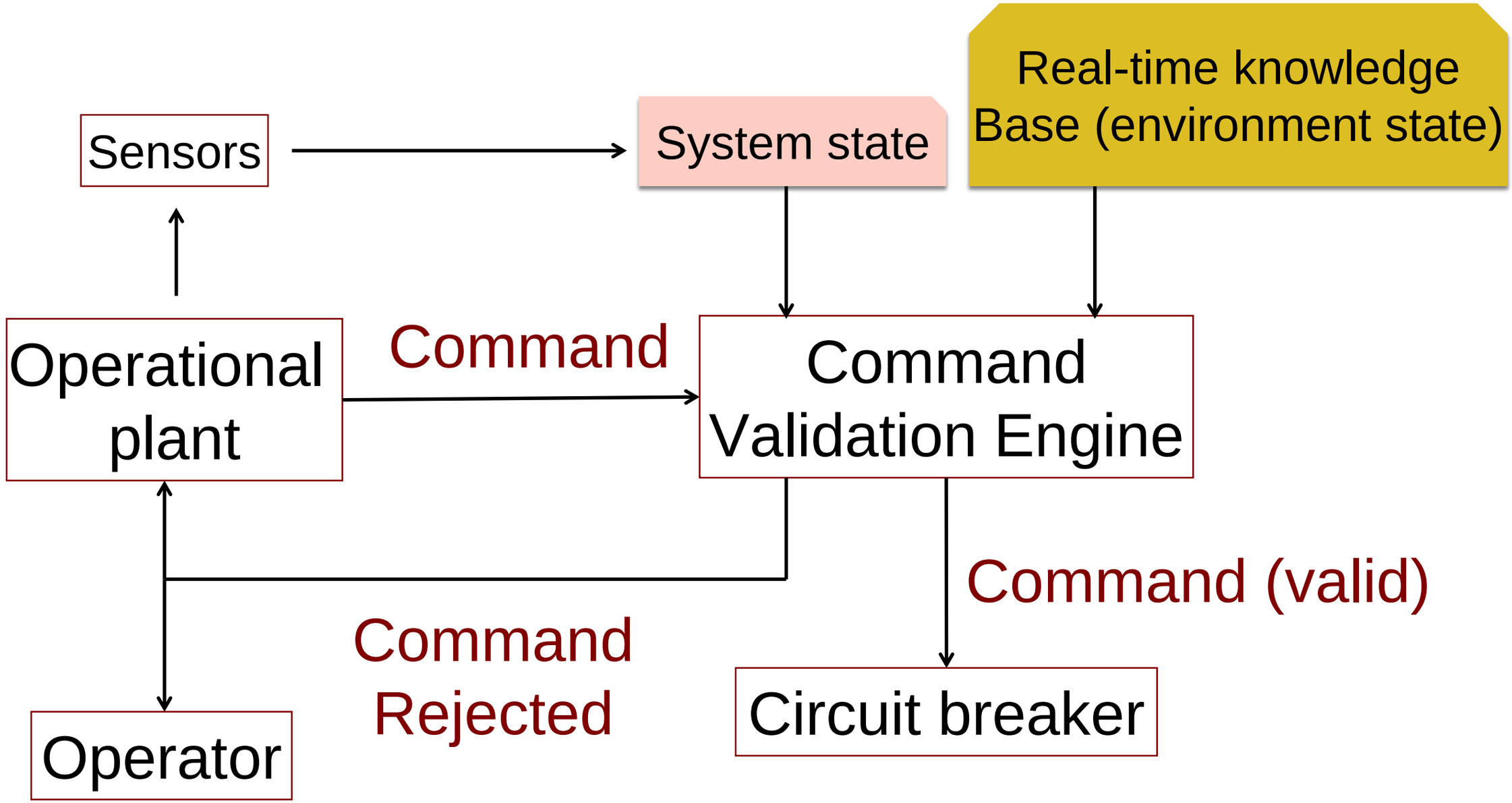
# Detection: AI-Centric Approach



# Control as implemented TODAY



# AI-based Control for Tomorrow?



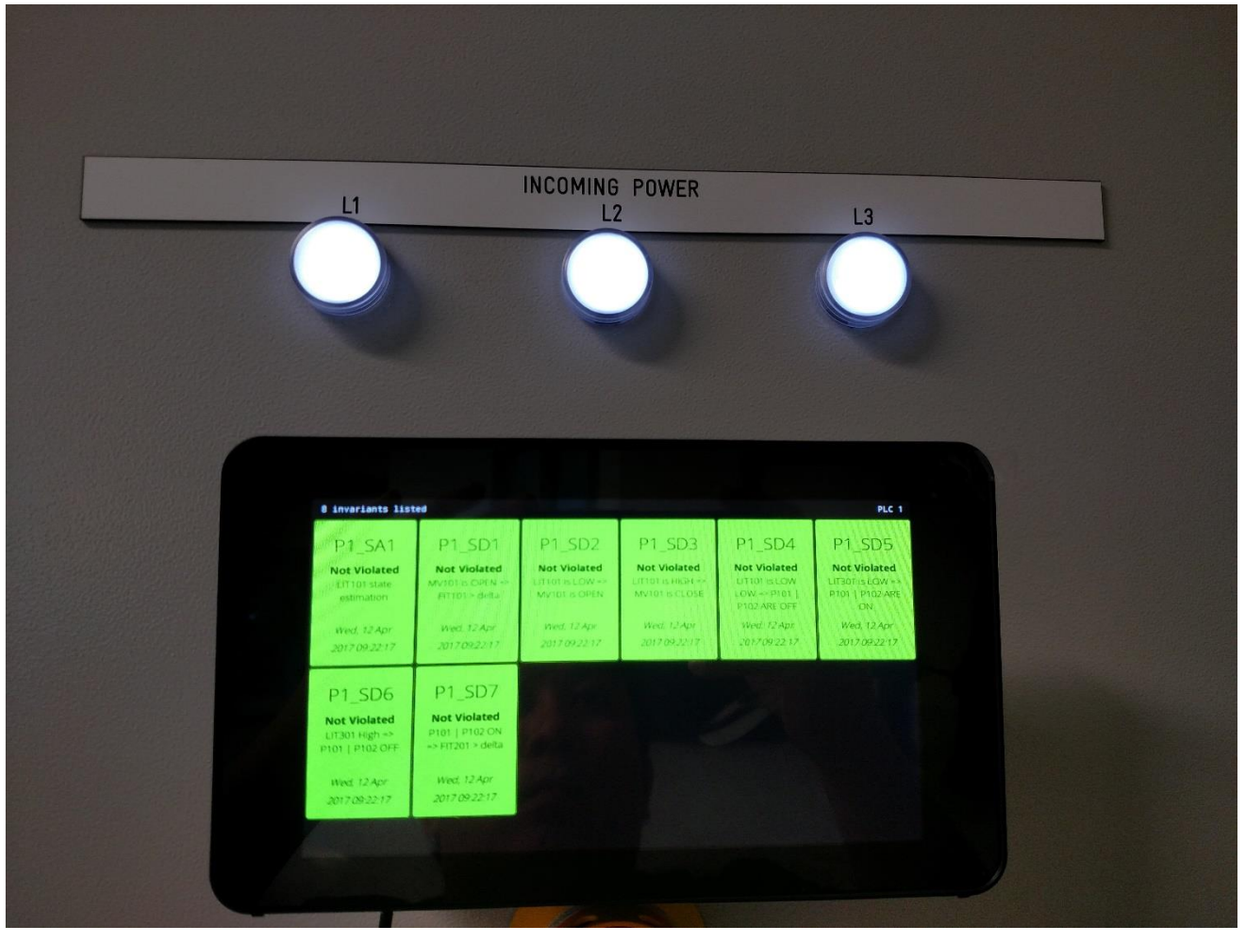
# Testbeds at iTrust

## Water Treatment

## Water Distribution


Electric power generation, transmission, distribution, AMI

# Invariant observation (physical)

# Summary

Attack detection can be highly accurate with near zero false alarm rate when using design-centric approach combined with ML.

AI holds promise in command validation as a means to prevent any attacker initiated commands that arrive at actuators.

Challenge: creation of real-time (accurate and useful) knowledge base and command validation engine!

Thank

You?