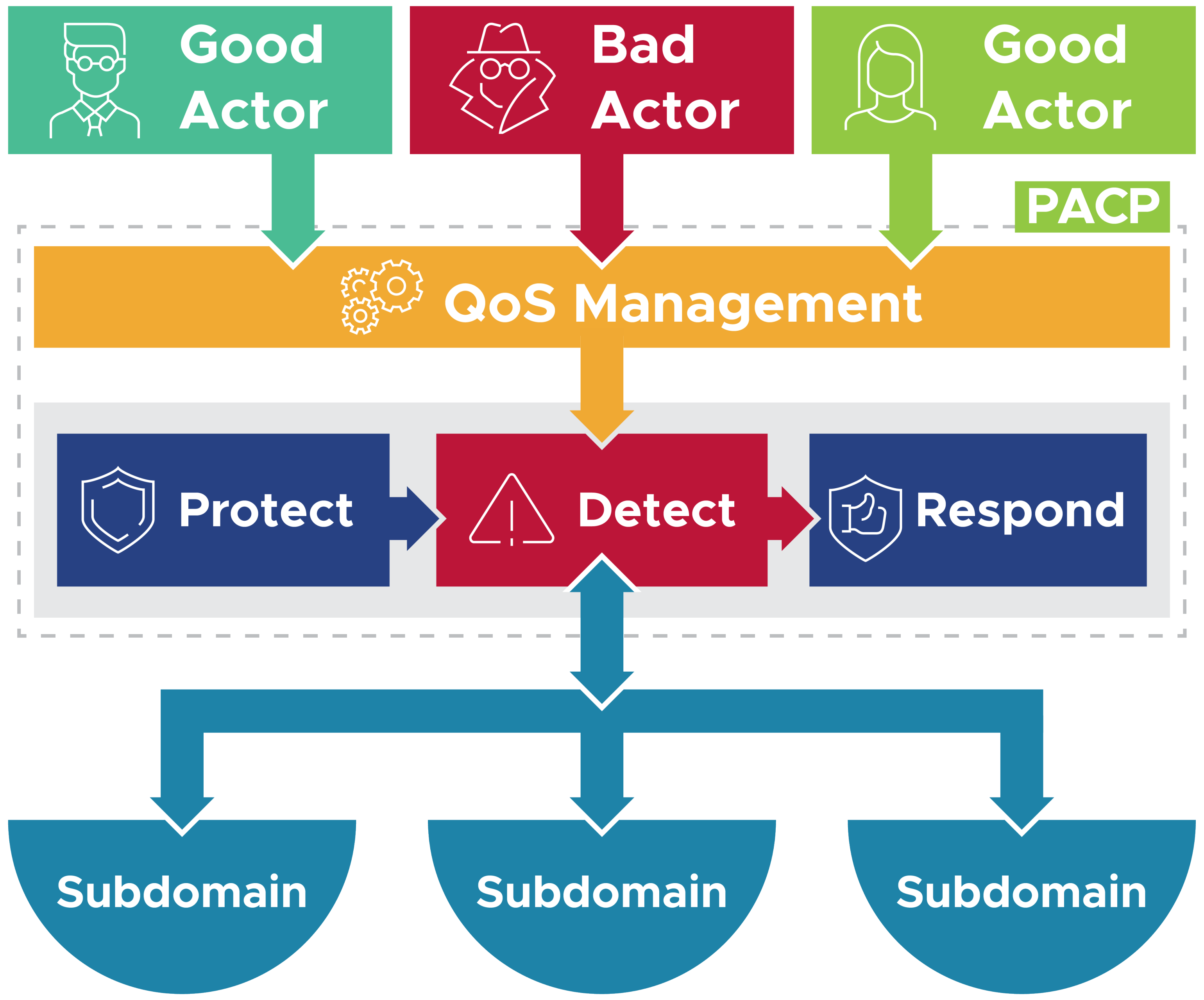
Physical Aware Cyber Platform (PACP) | Thrust 1

Shwetha Niddodi, Ashutosh Dutta, Joonseok Kim, Arman Ahmed, Oceane Bel,
Kevin Underwood



OBJECTIVE

Provide increased resilience to high-fidelity cyber-physical systems at cyber layer through:

- Dynamic support of quality of service (QoS) and security requirements; and
- **Protection**, **detection,** and **response** to cyber natural faults and cyberattacks.

ACHIEVEMENTS

- Targeted paper submission to North America Power Symposium Conference 2022
- Two PNNL Techfest presentations
- Microgrid co-simulation testbed

APPROACH

PACP provides an application programming interface for data transfer, QoS, and security services, while abstracting host, network, and device concerns from the application.

Data Management

- Uses fast data distribution service (DDS) for data transfer, data management
- Creates new:
  - ***DataWriter*** to send new data with defined QoS requirement
  - ***DataReader*** to receive new data with requested QoS requirement

QoS Management

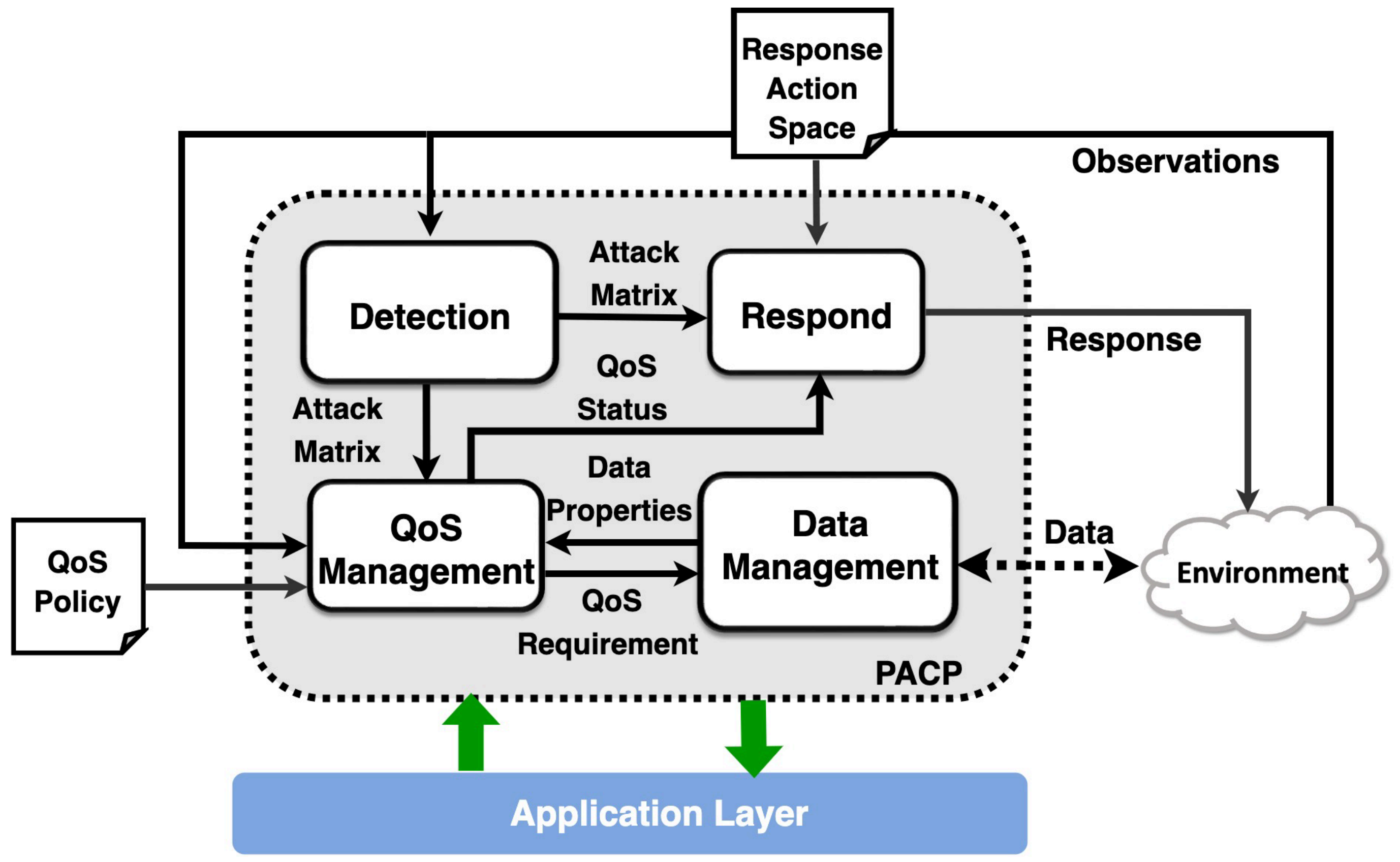
- Manages the QoS policies set by the application/operator
- Provides various QoS policies: reliability, liveliness, priority-based scheduling, authentication, access control, encryption

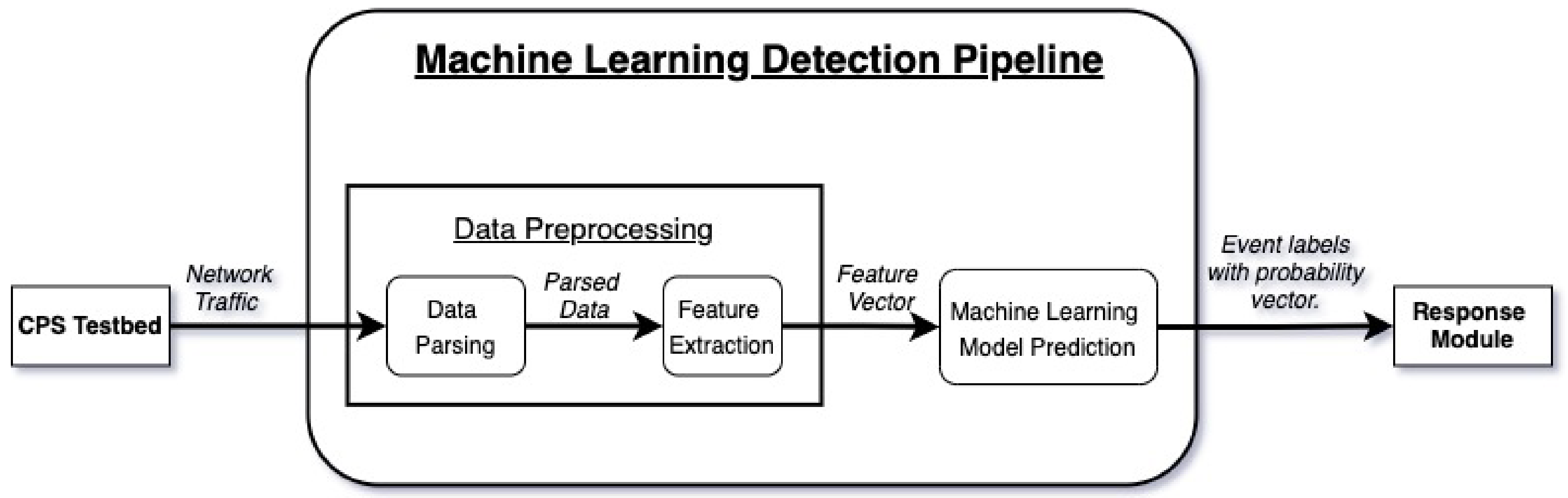
Detection

- Computes an attack matrix defining likelihood of each cyberattack. The detection pipeline:
  - Captures data from underlying network
  - Converts data into feature vector and feeds prediction model
  - Generates attack matrix with attack type and likelihood information

Response

- Executes optimal response action for the current QoS status and attack matrix





RESULTS/IMPACT

- Several off-the-shelf, supervised learning algorithms were used on cyber-physical datasets to detect cyberattacks
  - Random Forest showed best performance
- Requirements were derived through discussions with several Thrust 2 projects
  - Anomaly detection capability provided by our platform was found to be most useful
- A microgrid co-simulation platform was developed to create several power fault and cyberattack scenarios
- Different flavors of DDS were evaluated; fast-DDS was identified as most suitable

Algorithm	Accuracy (%)
Random Forest	96.548
Ada-Boost	77.925
Extra Tree	96.507
Logistic Regression	94.516
Linear Discriminant Analysis	73.219
K-Nearest Neighbors	96.106
Naive Bayes	62.359

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	96.340	96.284	96.340	96.311

Detection Algorithm Performance Results

U.S. DEPARTMENT OF ENERGY
BATTELLE
PNNL is operated by Battelle for the U.S. Department of Energy

8/17/2022 | PNNL-SA-174993

Pacific Northwest
NATIONAL LABORATORY
www.pnnl.gov