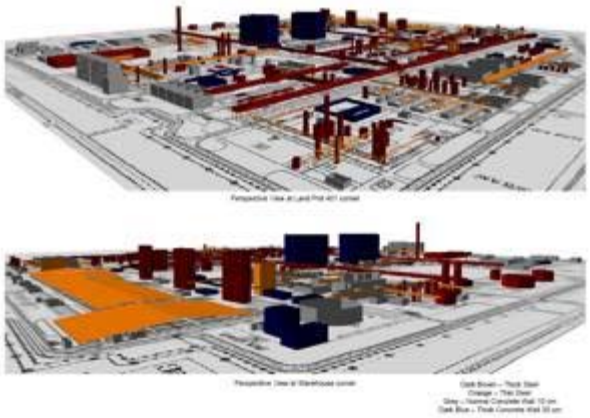
ISRCS 2012

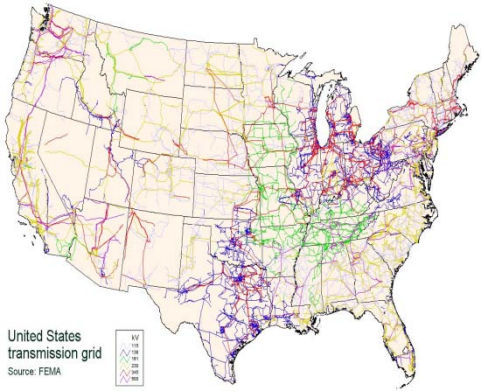
Resilient Control System Execution Agent (ReCoSEA)

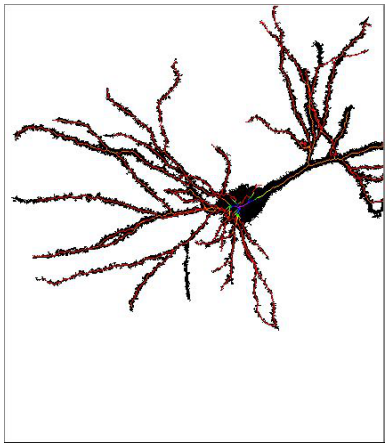
Rieger, C. (INL) and Villez, K. (Purdue)

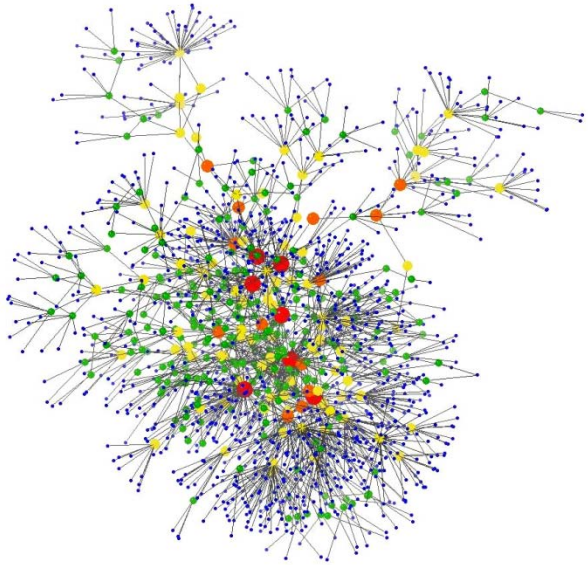
Complexity of systems

- Increasingly connected world
  - Power
  - Electricity
  - Communication
  - Transportation
- Changes in infrastructure
  - More connections
  - Increased intensity of connection









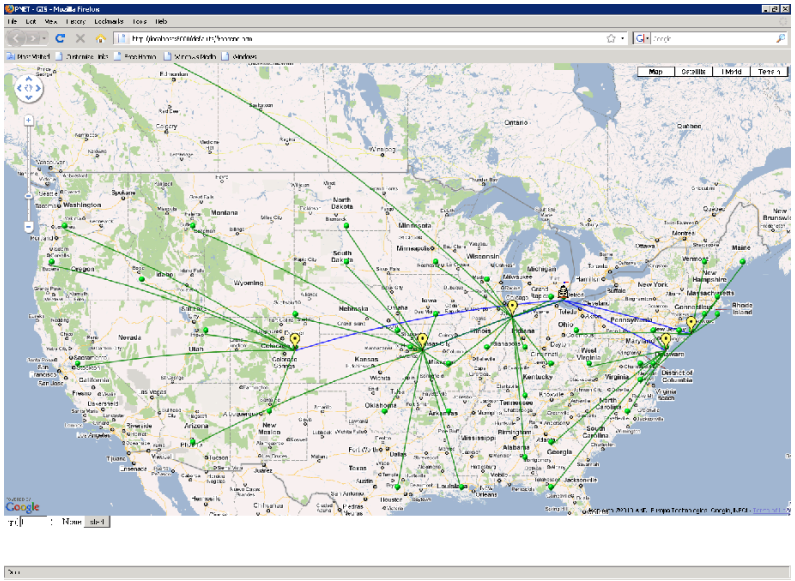
Complexity of systems

- Cascading failures
  - Single point failure
  - Delayed / inaccurate assessment
  - Propagation through system
- Malignant actors
  - Cyber intrustion
  - (1) False data -> false assessment
  - (2) Mask degradation

Challenge

- Achieve/maintain resiliency
  - Stability
  - Efficiency
  - Security
- In context of
  - Complexity (cascade)
  - Cyber intrusion
- Via
  - Coordination: Account for interactions between components
- Result
  - Accuracy of availability assessments
  - Identify faults/failures before propagation
  - Decrease incidence of multiple faults at once

Large-scale requires distributed solution

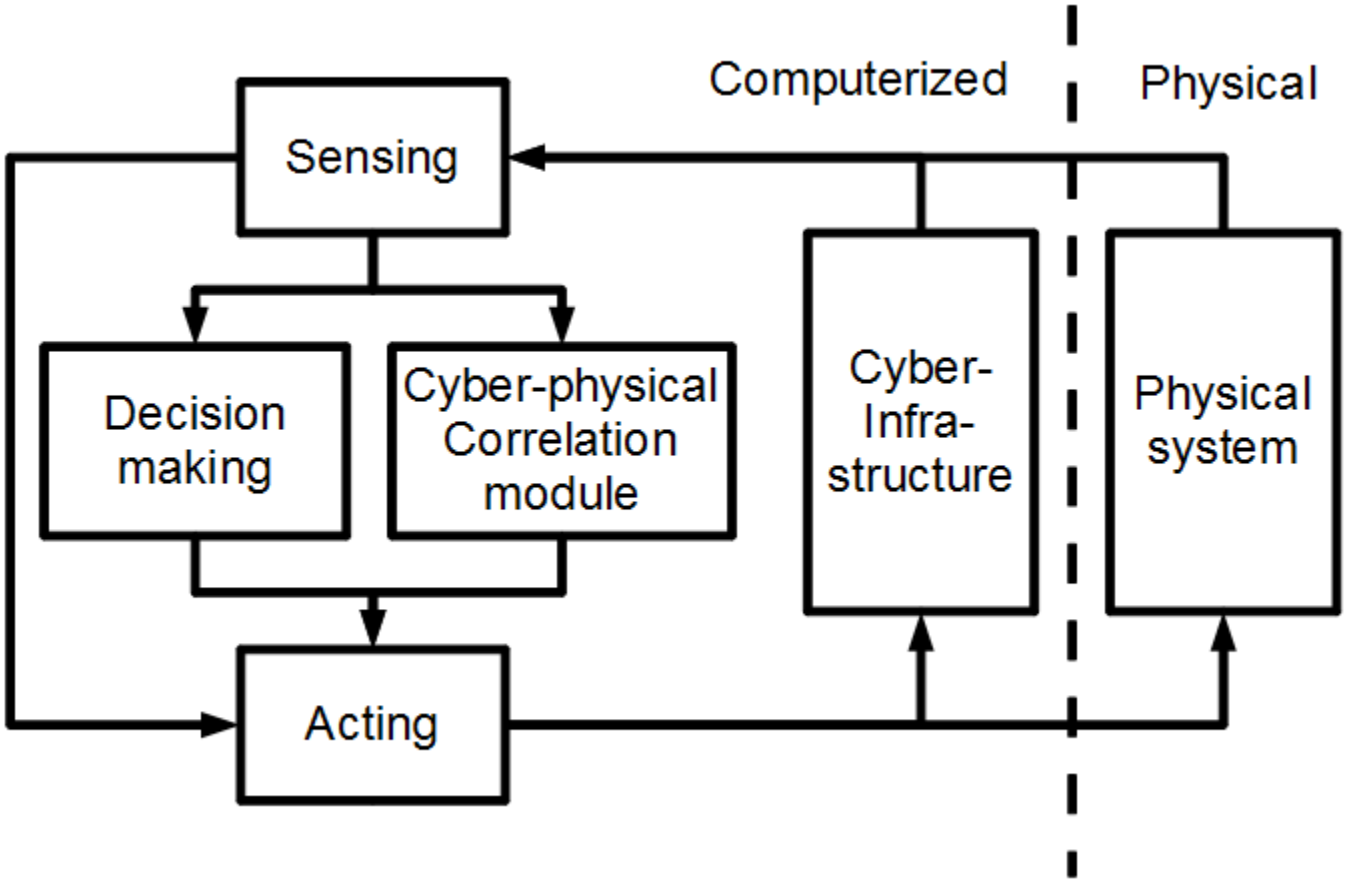


- Agent-based solution
  - Instead of centralized supervision
- Individual agent
  - Influences neighborhood
  - To obtain information
  - Awareness of faults/failures
  - Corrective actions
- Information in data
  - Depends on dynamic response of connected components
  - Introduce disturbance in connected node and analyze response

ReCoSEA design

- Sensing:
  - Collecting data
  - Physical
  - Cyber
- Assessment/Analysis
  - Jointly
- Action
  - Physical
  - Cyber
  - Human interaction

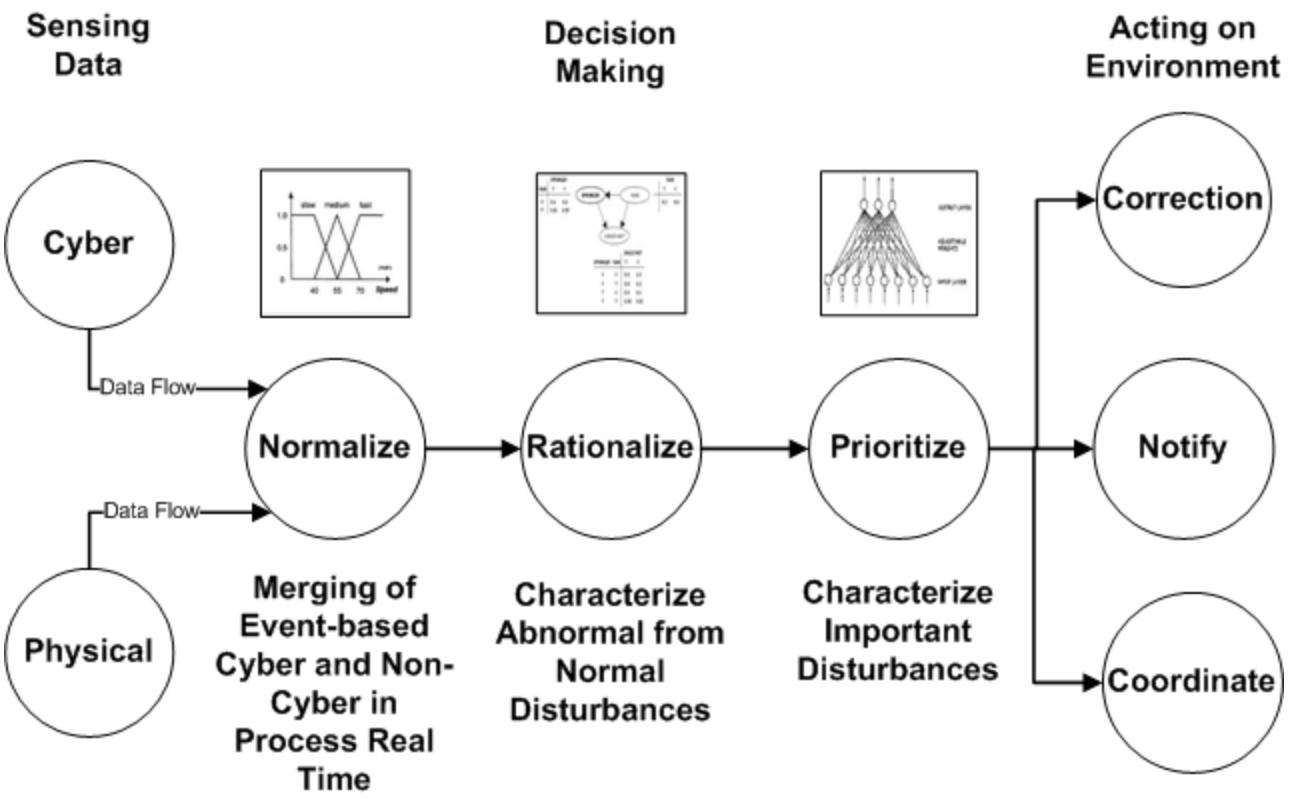
ReCoSEA design



ReCoSEA design

- Normalize
  - Transforming multiple data types into consistent format
  - Model: Fuzzification
- Rationalize
  - Identify anomalies
  - Identify root causes
  - Identify impact
  - Model: BBN
- Prioritize
  - Generate alarms to operator
  - Take automatic actions
  - Model: ANN

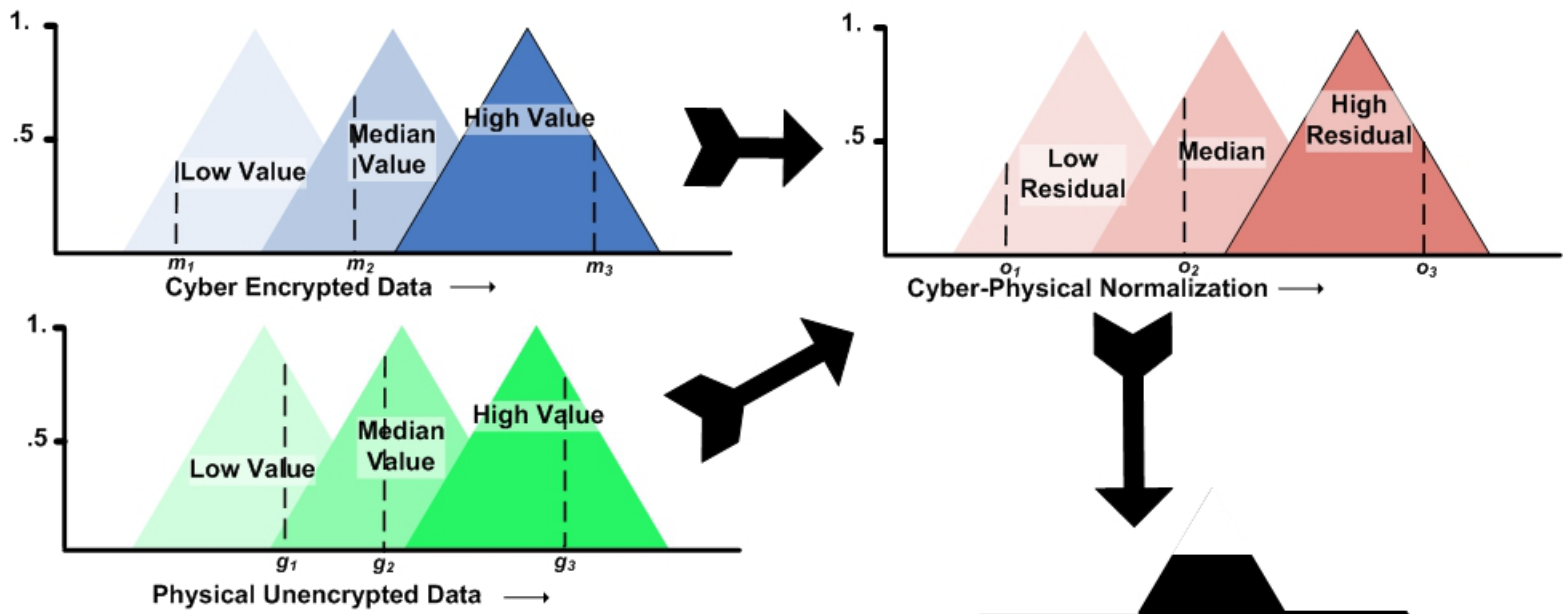
ReCoSEA design



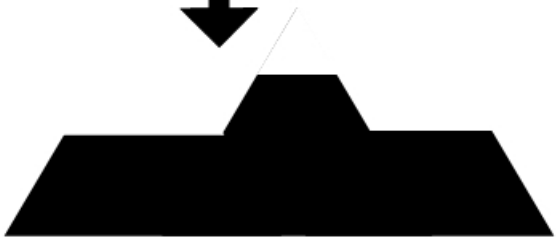
Normalize

- Combine physical and cyber-data
- Physical data
  - Continuous measuring range
  - Continuous time processes
- Cyber data
  - Discrete states
  - Discrete time-event

Normalize



Rule base subset for determining generation policy:
1) If the encrypted value (*m*) is high AND the unencrypted value (*g*) is high, then the cyber-physical normalization (*o*) is high.
2) If the encrypted value (*m*) is low AND the unencrypted value (*g*) is low, then the cyber-physical normalization (*o*) is low.
3) If the encrypted value (*m*) is high AND the unencrypted value (*g*) is median, then the cyber-physical normalization (*o*) is high.



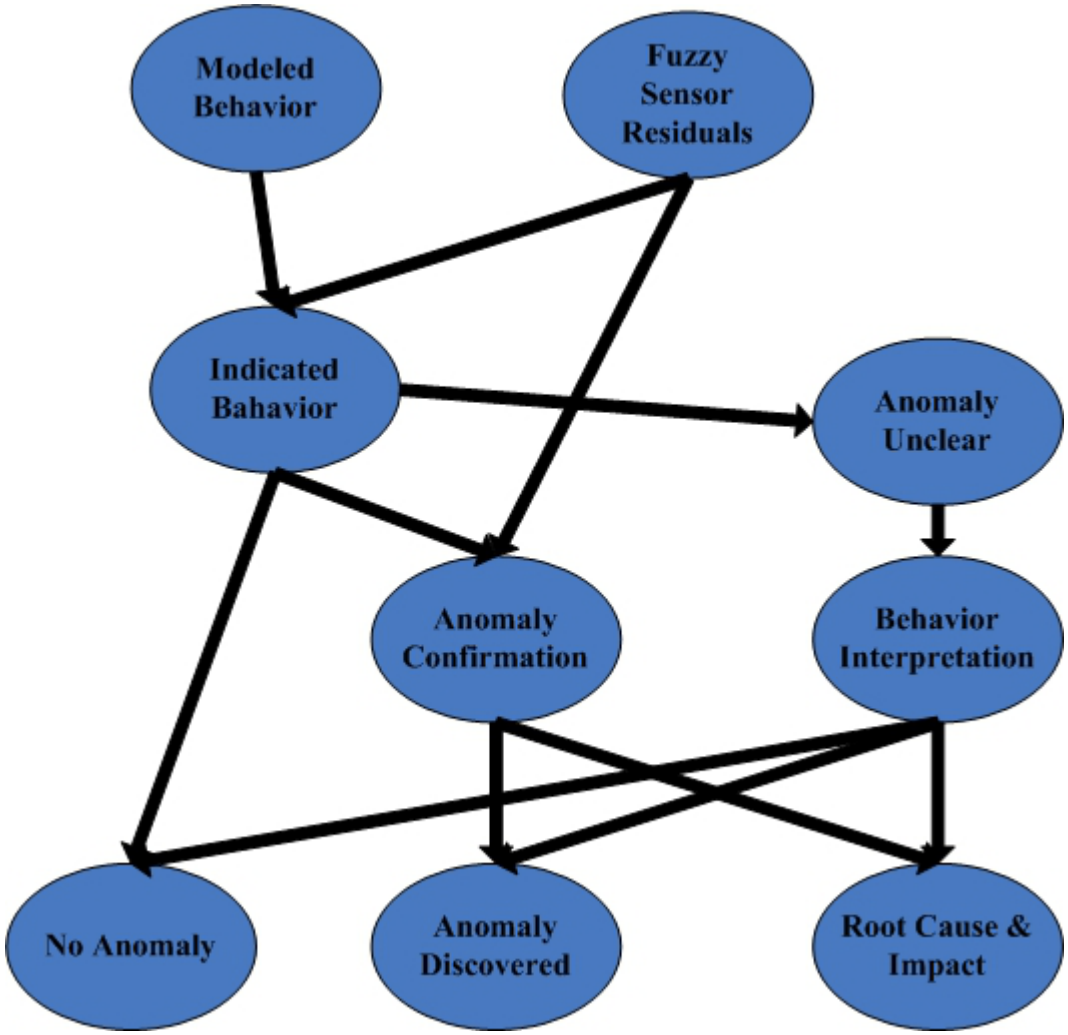
Sensor Residuals = Centroid of Area

Rationalize

- Integration of sensory information
- Bayesian Belief Network (BBN)
  - Provide dependence structure and parameters
  - Assess probability of discrete states in the network
- Allows
  - To incorporate expert knowledge
  - Make probabilistic assessment
  - Quantify uncertainty of assessment (entropy)
- Recent developments at INL
  - Add probabilities as inputs
  - Probabilities derived with other tools

Rationalize

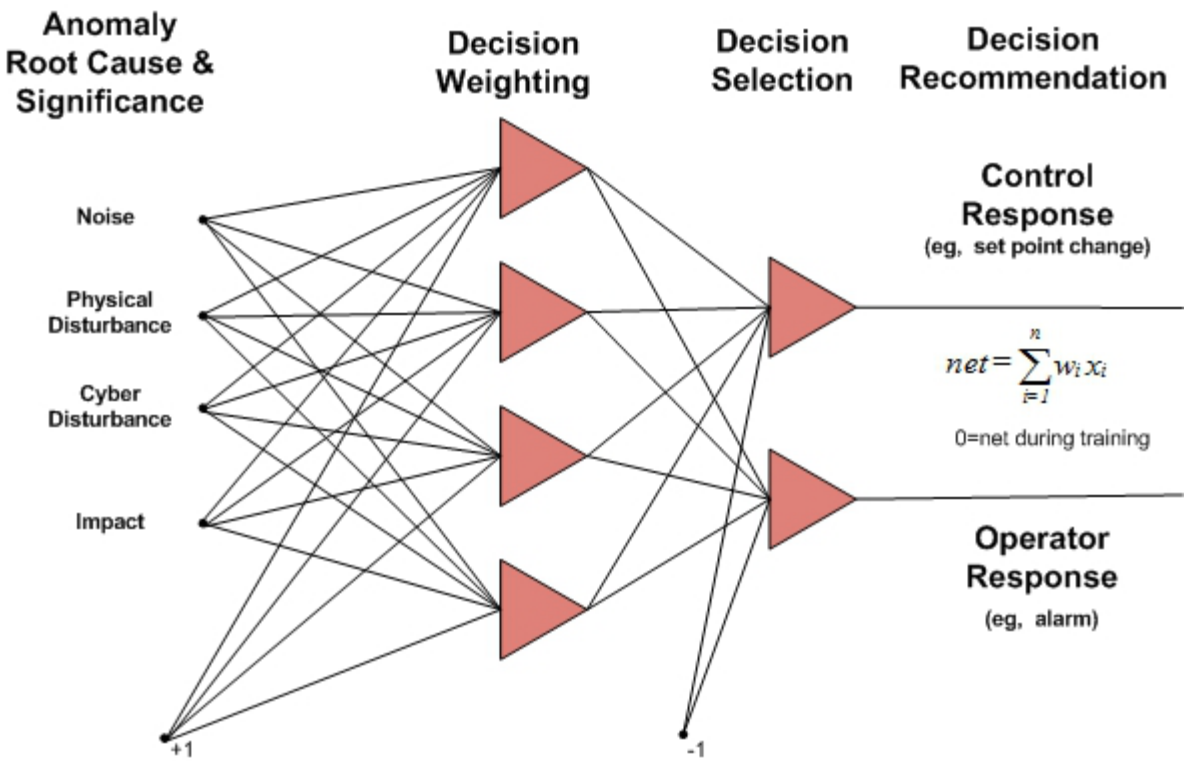
- BBN



Prioritization and decision-making

- Decision-making
  - Based on non-linear modeling of appropriate action
  - Operator response
  - Control response
- Weight different anomalies according to
  - Location
  - Type
  - Impact
- Tool: ANN model
- Active learning of network
  - Introduce disturbances in neighbor
  - Record / learn from
    - Resulting performance
    - Operator decisions

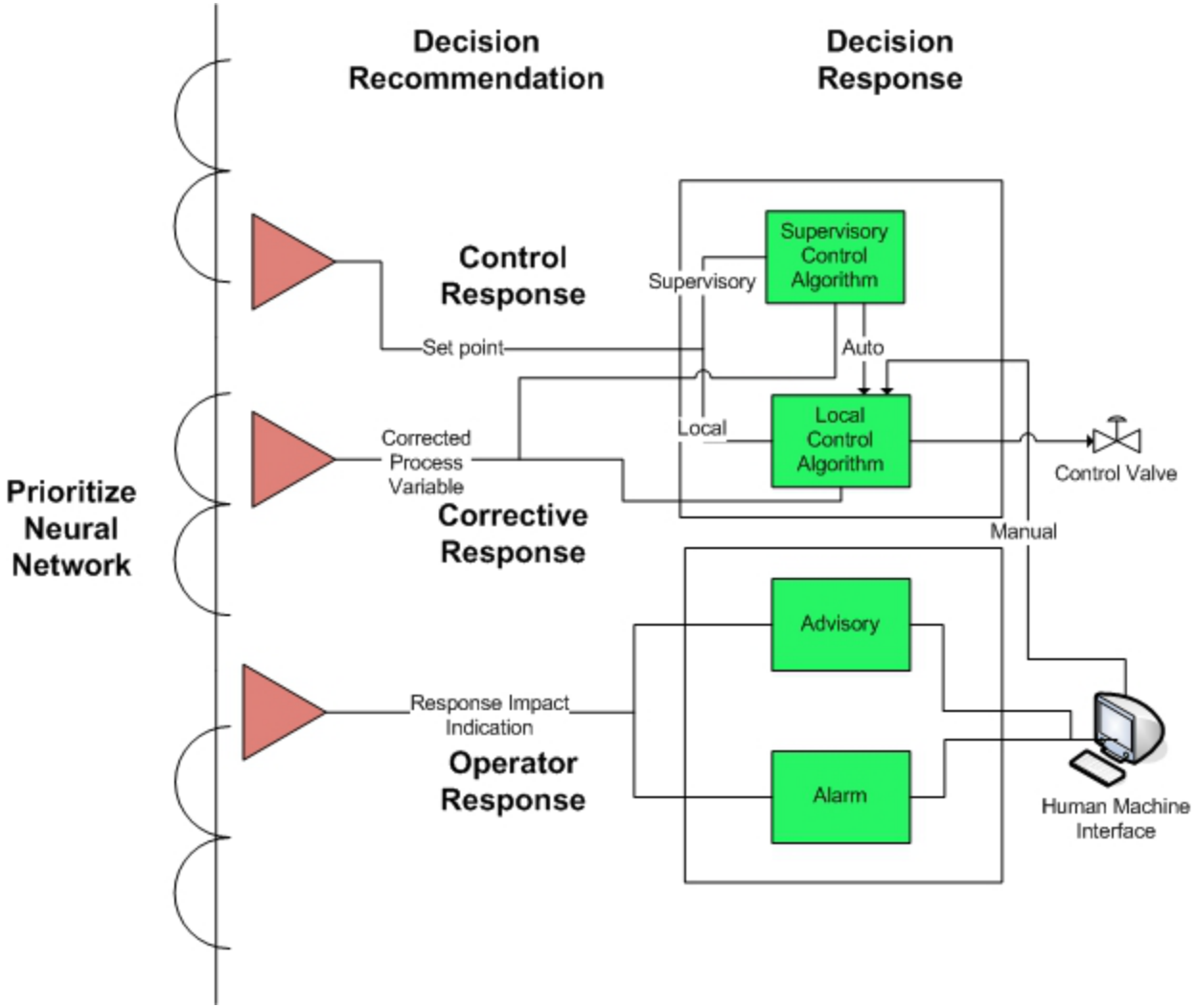
Prioritize


Anomaly Root Cause & Significance
Decision Weighting
Decision Selection
Decision Recommendation
Noise
Physical Disturbance
Cyber Disturbance
Impact
+1
-1
Control Response
(eg, set point change)
$net = \sum_{i=1}^{n} w_i x_i$
0=net during training
Operator Response
(eg, alarm)

Prioritize

- Active learning of network
  - Introduce disturbances in neighbor
  - Record response
  - Learn from resulting performance
    - State of environment
    - Constraints in neighbors

Action level



Conclusions

- ReCoSEA
  - Template for resilient control design of agents in agent-based system
- Nature:
  - Diagnostics of joint Cyber/Physical realm
    - Normalize
    - Rationalize
    - Prioritize
  - Multiple tools for different tasks
    - Expert knowledge representation
    - Automated learning
      - Passive
      - Active