Craig Miller

NRECA

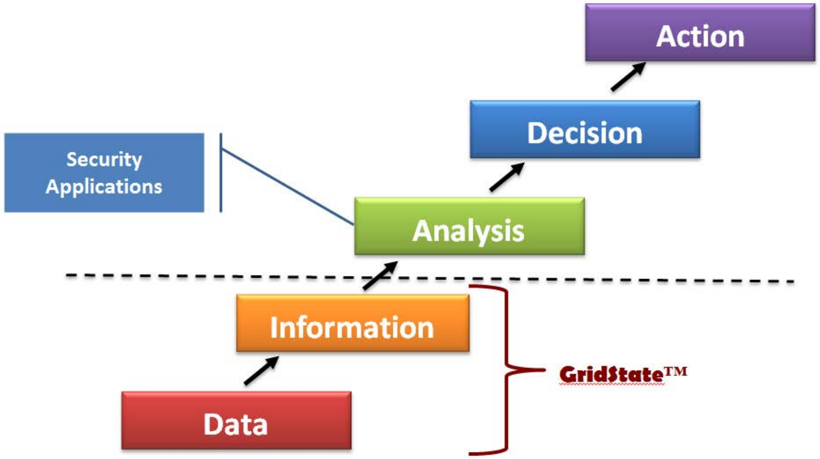
# Essence

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

# Summary: Essence

- **Objective**
  - To develop an integrated security appliance that will enable utilities (especially co-ops) to define, configure, manage and monitor utility networks with high fidelity
- **Schedule**
  - Oct. 2013 – April 2016
  - Prototype Design Completed (Feb. 2014)
  - Lab Test (Dec. 2014)
  - Field Test (Feb. 2015)
  - Essence will produce an open specification for network management



- **Total Value of Award: $4,707,222**
- **% Funds expended to date:** 26%
- **Performer:** NRECA
- **Partners:** Pacific Northwest National Lab, Cigital, Honeywell, Carnegie Mellon University

# Advancing the State of the Art (SOA)

- **Network security is currently mostly prescriptive.**
- **The next generation is reactive and adaptive.**
- **Essence builds on decades-old principles of system abstraction while leveraging new database technology.**
- **Utilities will enjoy next generation network security at a price accessible to any size organization.**
- **Essence will use deep packet inspection with knowledge of utility protocols.**
- **Firewalls are easily penetrated. Essence will provide a more agile and adaptive approach to cyber security.**

# Challenges to Success

- **Data gathering and processing**
  - Ultra-fast databases needed
    - *High speed dedicated processors for primary collection*
    - *Hybrid database technology*
    - *Hadoop platform*

- **Confidentiality**
  - Making sure that sensitive IP packets remain secure
    - *Content-based filtering*
- **Acceptance**
  - Essence may seem like a too-radical departure from traditional approaches to interoperability
    - *Co-op community is ideal for testing*
- **Attack Surfaces**
  - Concern that Essence represents another attack surface
    - *Out of band data collection*

# Progress to Date

- **Data sensor prototype built and tested**
  - *Secure data collection technology already deployed at one utility*
- **Network simulator created**
  - *Essence team can now simulate network data from a utility*
- **Interfaces between layers identified**
  - *Essence team members can work on different project layers in parallel*

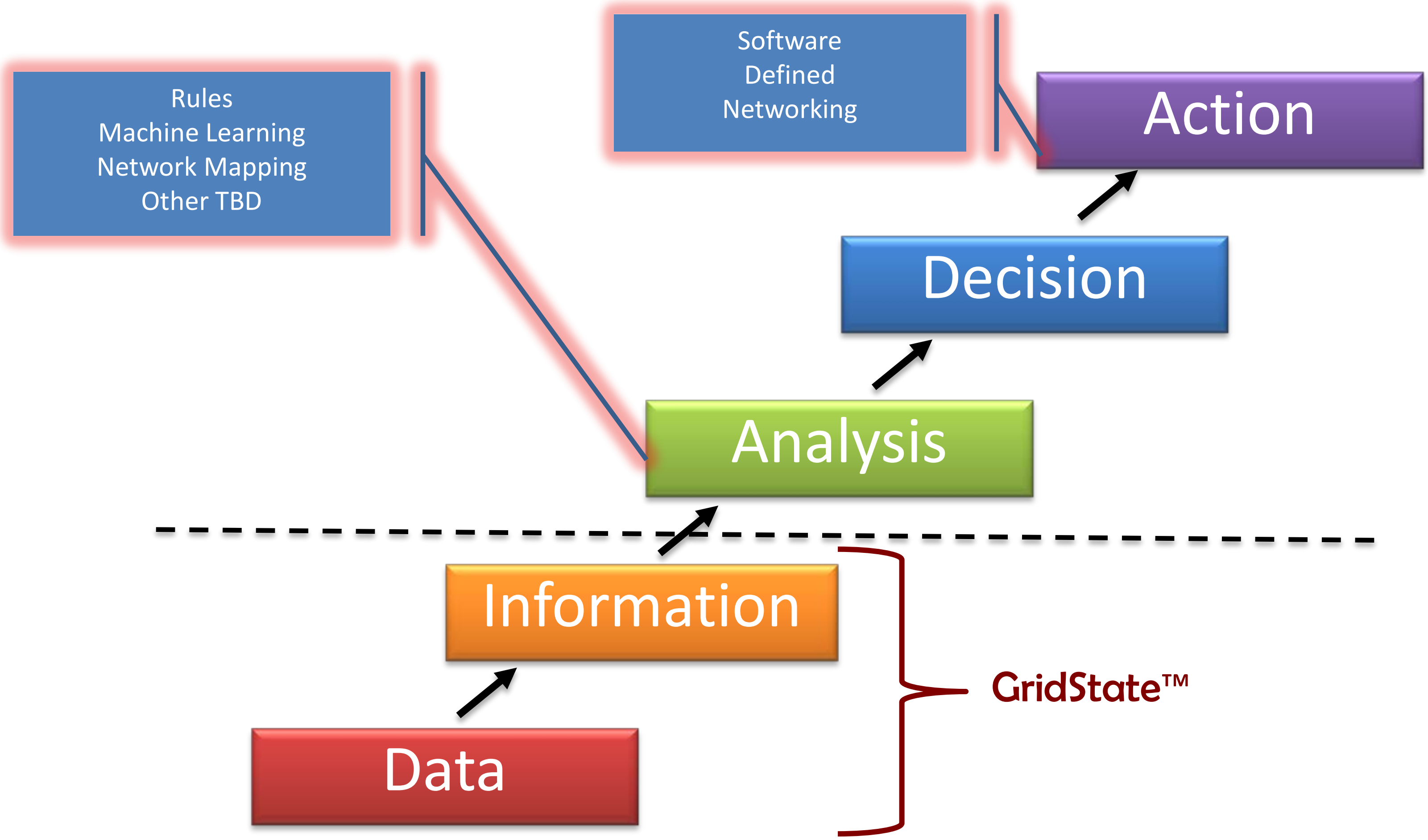
# Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - What category is the targeted end user for the technology or knowledge?
    - **Asset owners**
    - **Vendors**
  - What are your plans to gain industry acceptance?
    - *34 potential commercial customers already engaged*
    - *In negotiation with 2 to support development (major companies)*
    - *Abstraction model with open specification invites others to participate*

# Next Steps for this Project

- **Lab Testing in fall of 2014 at PNNL**
- **Deployment to test at utilities in first quarter 2015**

# Abstraction Model



Rules
Machine Learning
Network Mapping
Other TBD

Software
Defined
Networking

Action

Decision

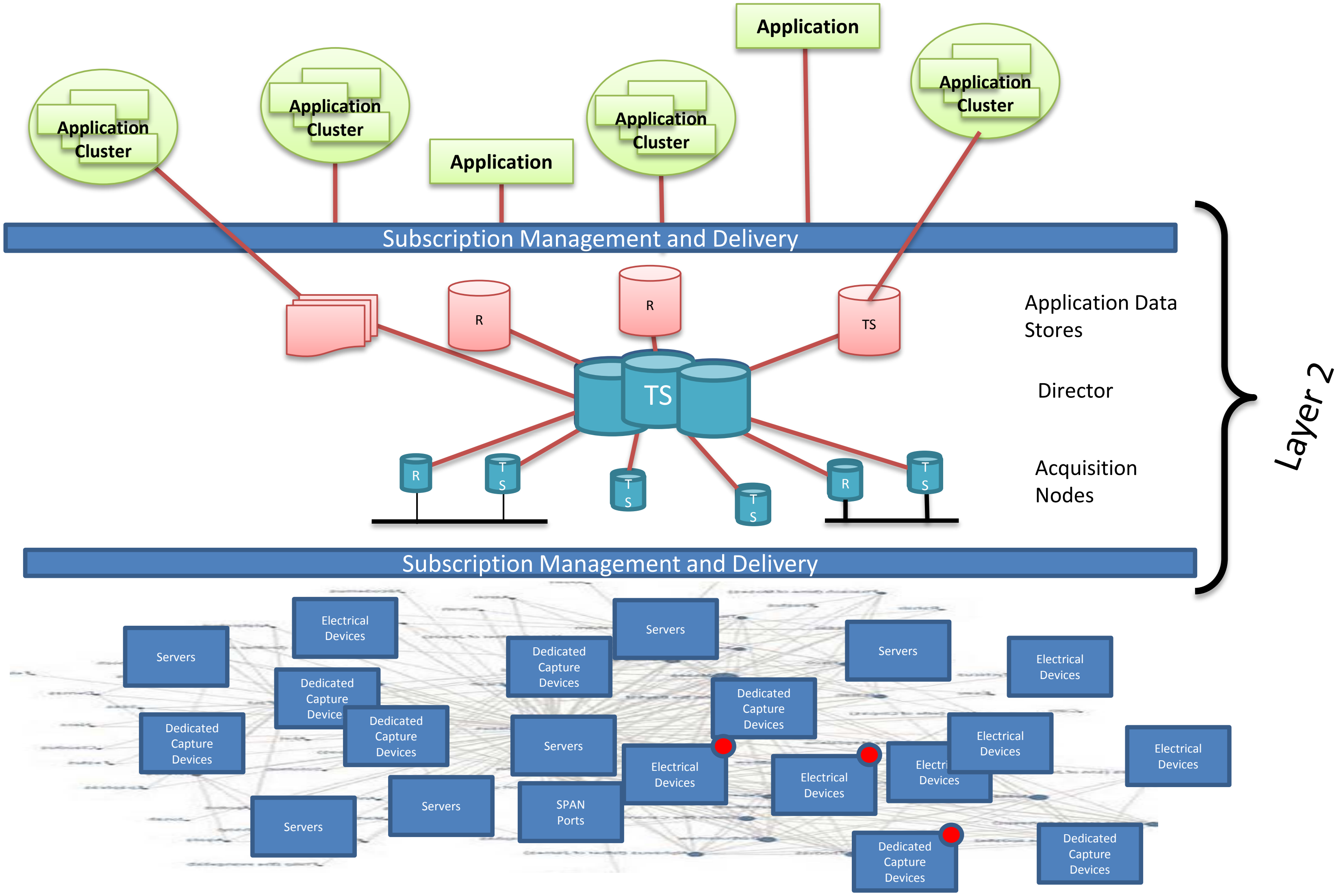
Analysis

Information

Data

GridState™

# General Architecture of Layer 2


Application
Application Cluster
Application Cluster
Application
Application Cluster
Application Cluster
Subscription Management and Delivery
R
R
TS
Application Data Stores
TS
Director
R
T S
T S
T S
R
T S
Acquisition Nodes
Subscription Management and Delivery
Layer 2
Electrical Devices
Servers
Servers
Dedicated Capture Devices
Servers
Electrical Devices
Dedicated Capture Device
Dedicated Capture Devices
Dedicated Capture Devices
Dedicated Capture Devices
Servers
Electrical Devices
Electrical Devices
Electri Devices
Electrical Devices
Electrical Devices
Servers
Servers
SPAN Ports
Dedicated Capture Devices
Dedicated Capture Devices