

# Information Trust

T N S T T T I I T F

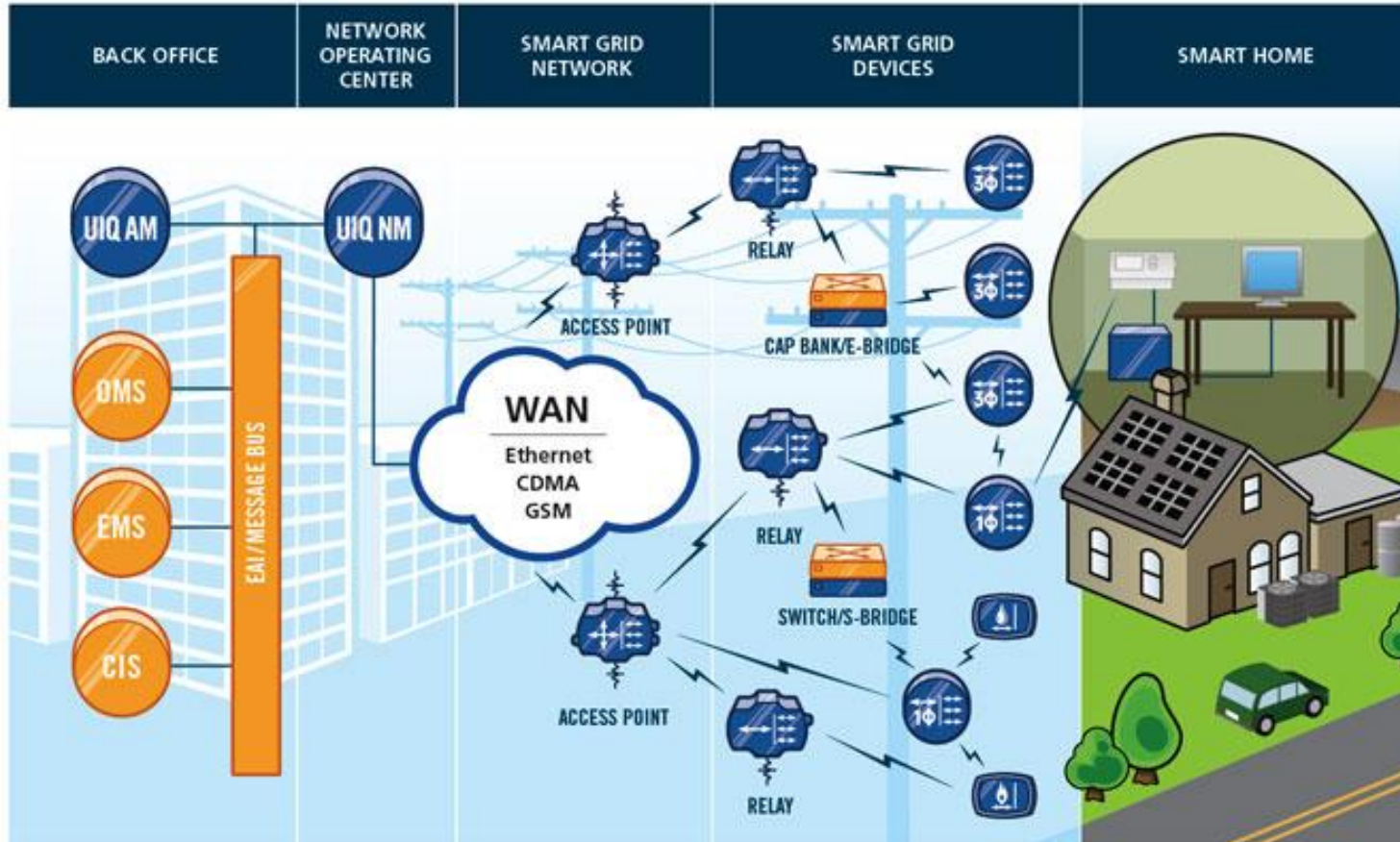
## Distributed IP Watch List Generation for Intrusion Detection on the Electrical Smart Grid

Ray Klump, Information Trust Institute,  
University of Illinois

Matt Kwiatkowski, Argonne National Lab



# The Emerging Smart Grid



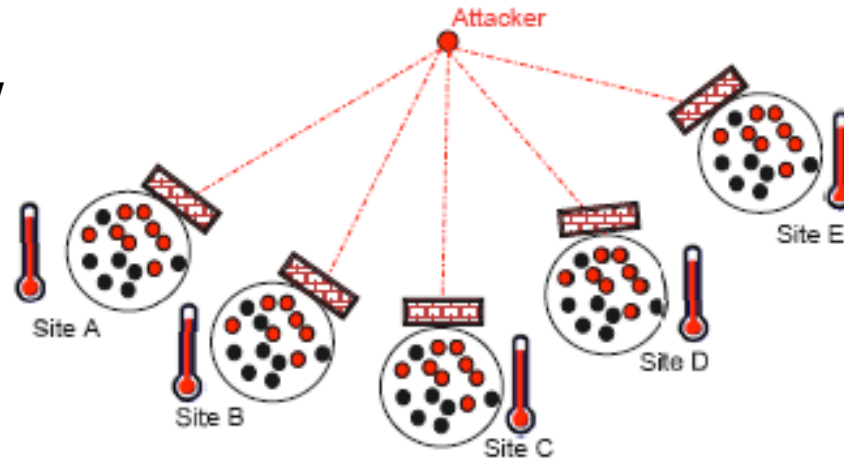
# Goal of this work

Distributed IP Watch and Warn List  
Generation for the Smart Grid

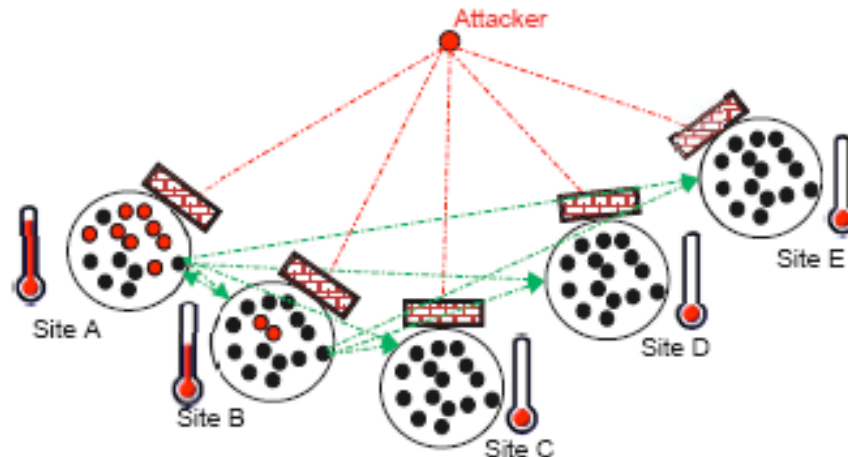
# Work Inspired by **Federated Model**

Argonne National Laboratory

Local View



**Zero-  
Day  
Threat**

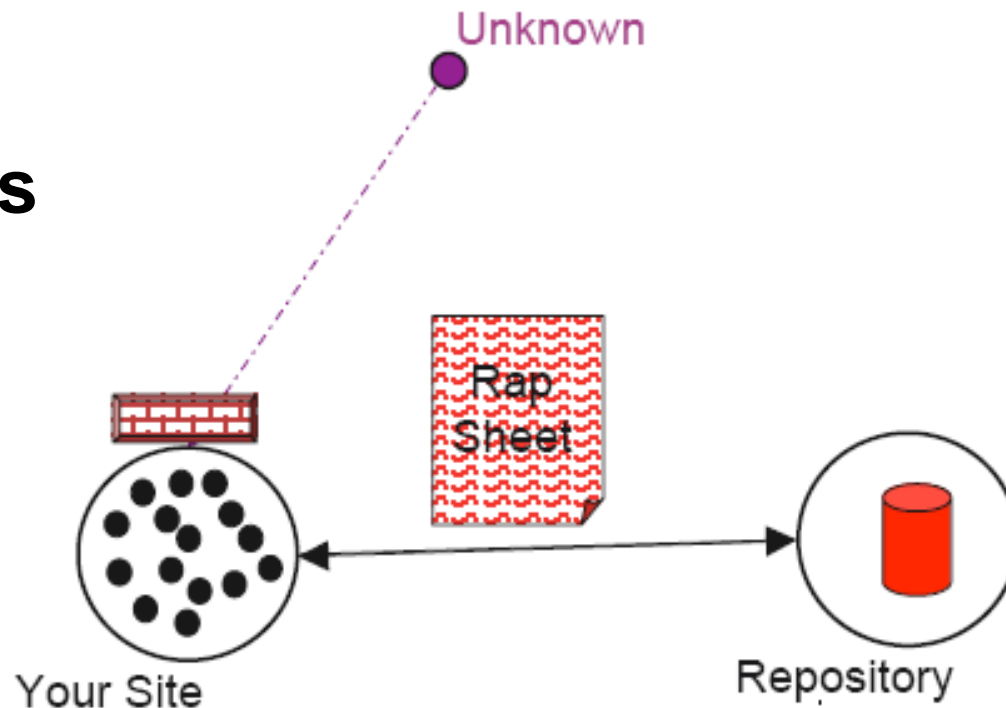


Federated View

# Work Inspired by Federated Model

Argonne National Laboratory

## Suspicious Behavior Scenario



# The Federated Model is flexible.

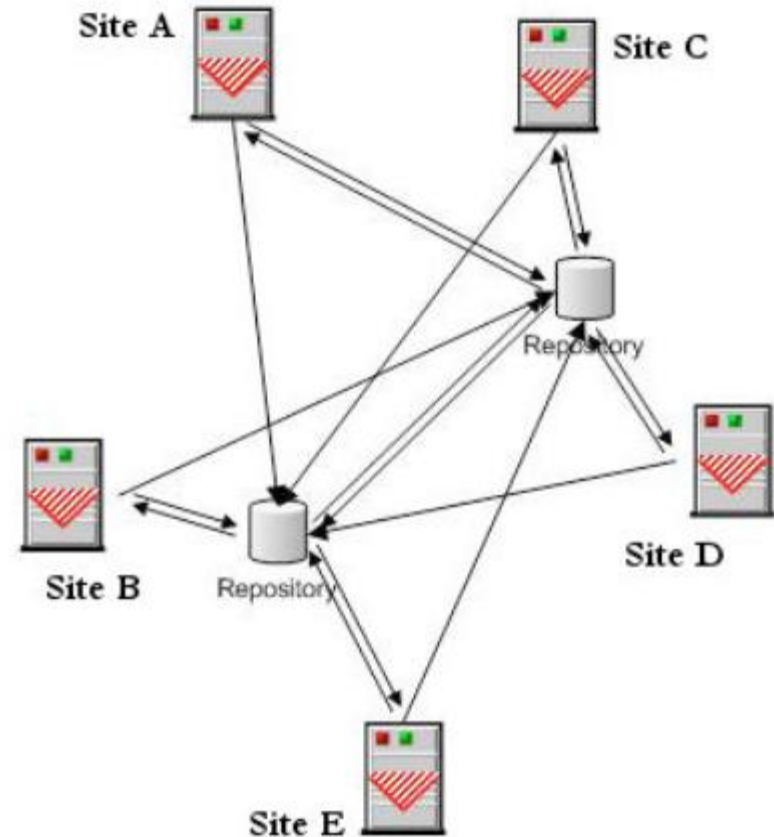
Participants decide how to use it.

# Federated Model Features

- Grass-roots concept
- Sites maintain local control
- Sites decide with whom they interact
- Implemented through limited-function website

# Federated Model Technical Details

- Uses Standard Messaging Technology
  - IDMEF - Intrusion Detection Message Exchange Format RFC-4765
- HTTPS - Secure Hypertext Transfer Protocol
- PGP - Pretty Good Privacy Encryption
- Redundant Repositories
- IP-Restricted Participation



# Federated Model Usage

- 47 Participants
  - US-CERT/DHS, Argonne National Lab, National Center for Supercomputing Application, .EDU's, Small Businesses, Corporations.
- Range of 58 to 139213 messages per day of hostile activity reported between sites with an average of 4137 per day

# Three Categories of Information Shared

- Announcements from a site
- Query about an IP address
- Action request (warning)

# What is Communicated in an Announcement or Warning?

- IP Address (TCP/UDP and port #)
- Time of attack
- Type of attack
- Exploit attempted
- Severity of attack
- Previous history of offending IP at that site

# Sample IDMEF

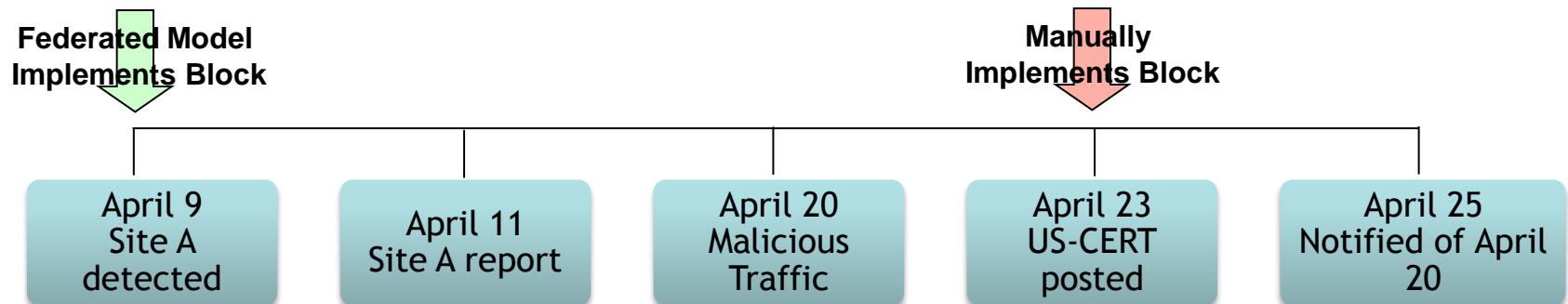
## XML (Extended Markup Language) Standard

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IDMEF-Message PUBLIC "-//IETF//DTD RFC XXXX IDMEF v1.0//EN"
"idmef-message.dtd">
<IDMEF-Message>
<Alert>
  <Analyzer analyzerid="ANL">
    <Node>
      <location>Argonne National Laboratory</location>
      <name> Contact Name, XXX-XXX-XXXX, email@anl.gov </name>
    </Node>
  </Analyzer>
  <AnalyzerTime>2006-07-06T11:41:59-0500</AnalyzerTime>
  <AdditionalData meaning="report type" type="string">alerts</AdditionalData>
  <AdditionalData meaning="report schedule" type="string">hourly</AdditionalData>
  <AdditionalData meaning="report start time" type="date-time">2006-07-06T10:41:59-
0500</AdditionalData>
  <AdditionalData meaning="number of alerts in this report" type="integer">2</AdditionalData>
</Alert>
```



# Success Story

- Timeline of events
  - April 9 - Site A detected malicious activity (event)
  - April 11 - Site A issued digital (pdf) report on event
  - April 20 - Traffic from Argonne to malicious site
  - April 23 - US-CERT posted malicious site
  - Argonne downloaded email
  - Read and decipher email to find malicious site
  - Implement block action against malicious site manually
  - April 25 - US-CERT notified Argonne of traffic on April 20

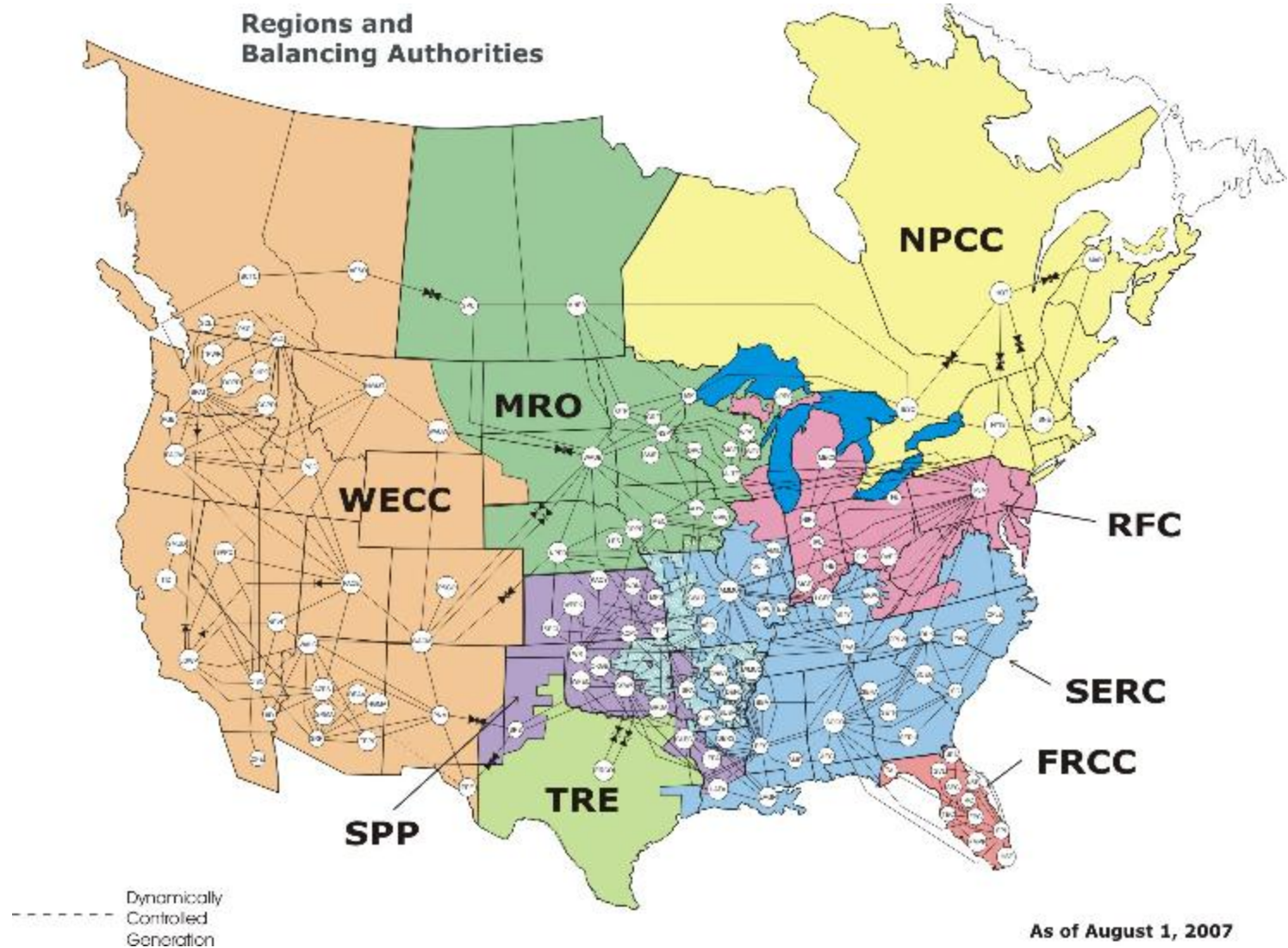


# Project Growth

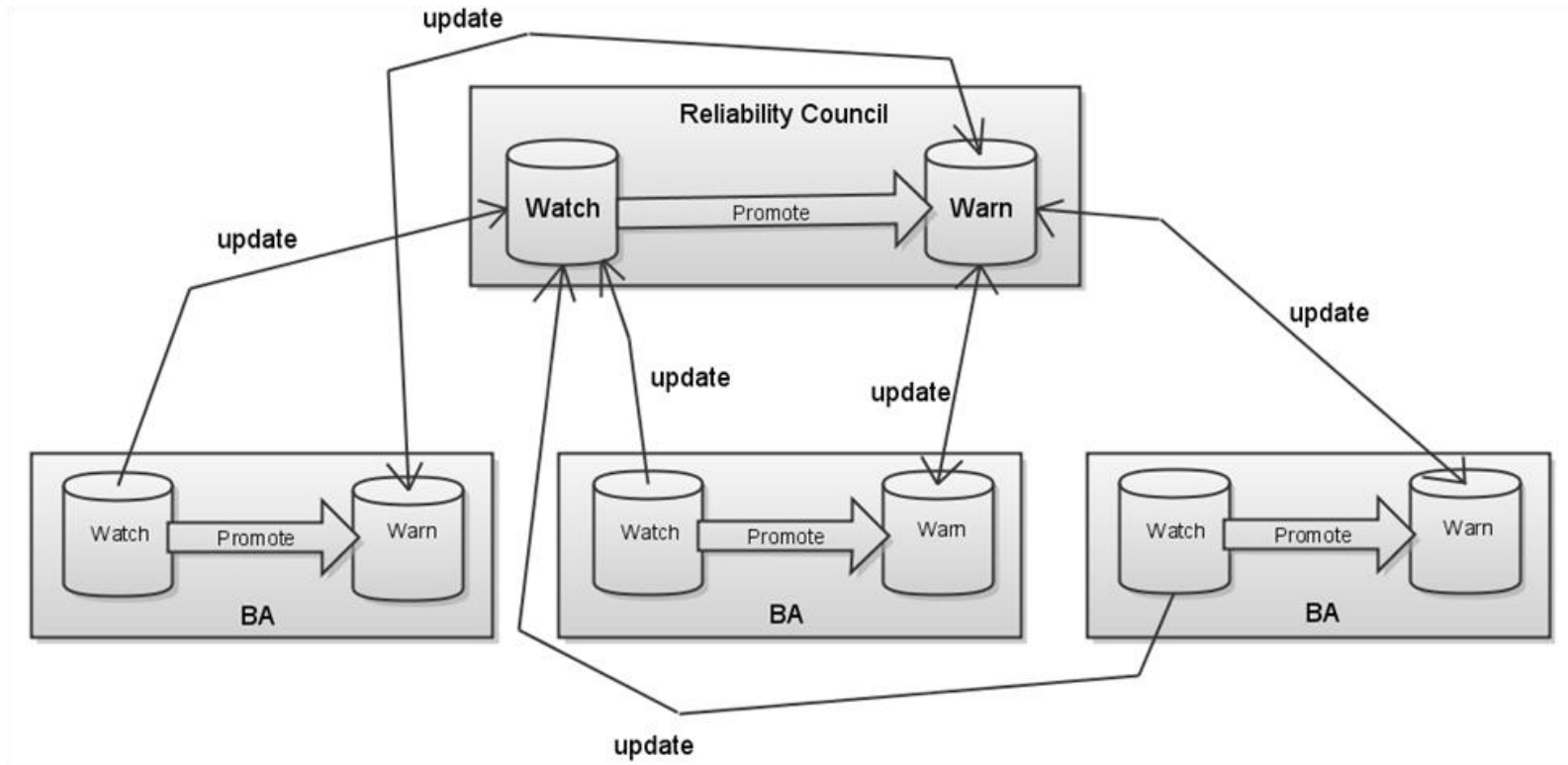
- Build infrastructure, automate data transfer
- Implement query / response capability
- Expansion to reporting more than IP addresses and enacting response plans



# Federated Model Applied to the Grid



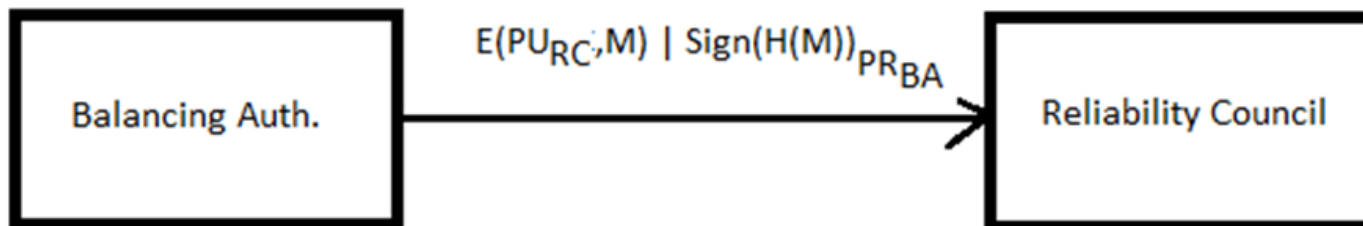
# Possible Implementation



# Two Key Issues

Security  
Scalability

# Security

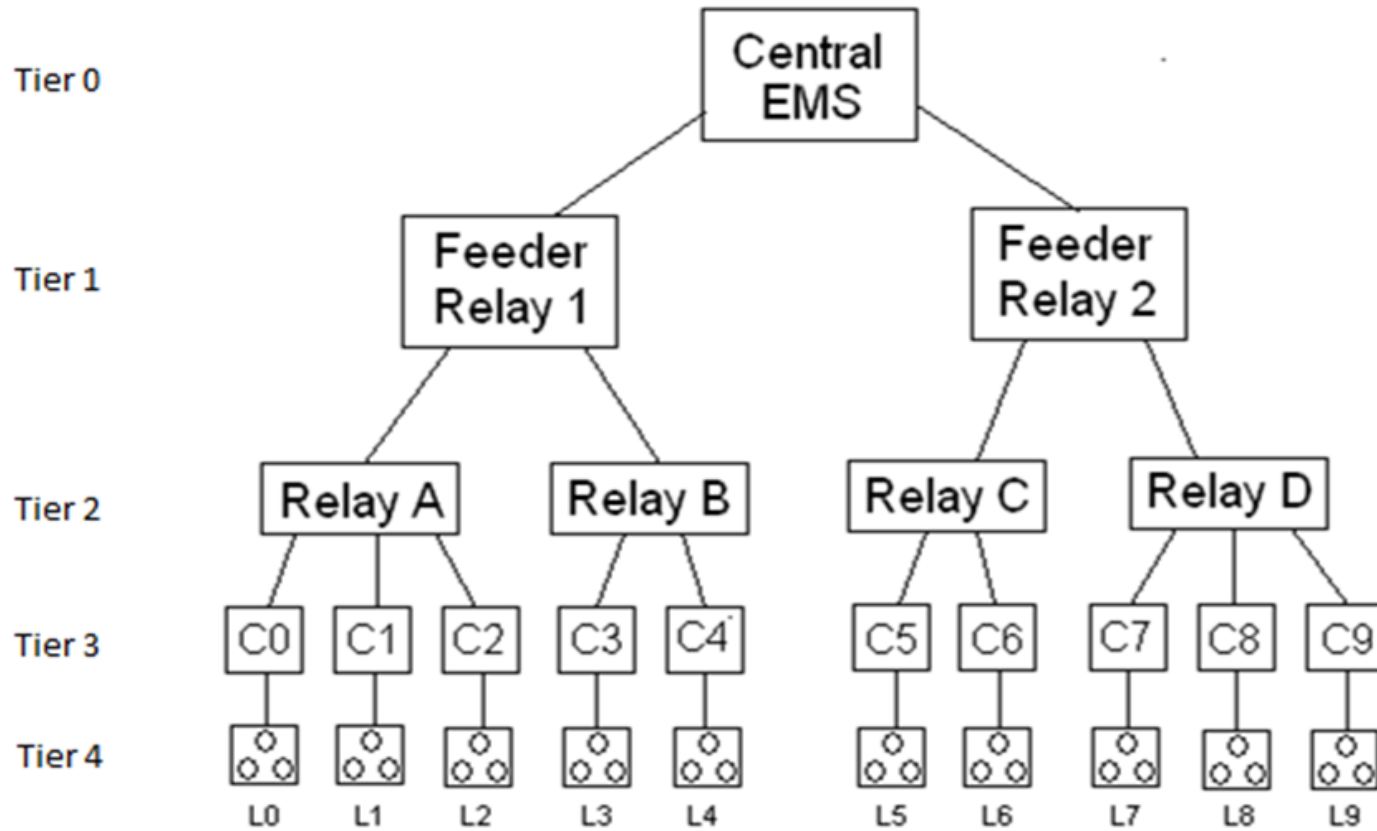


# Scalability

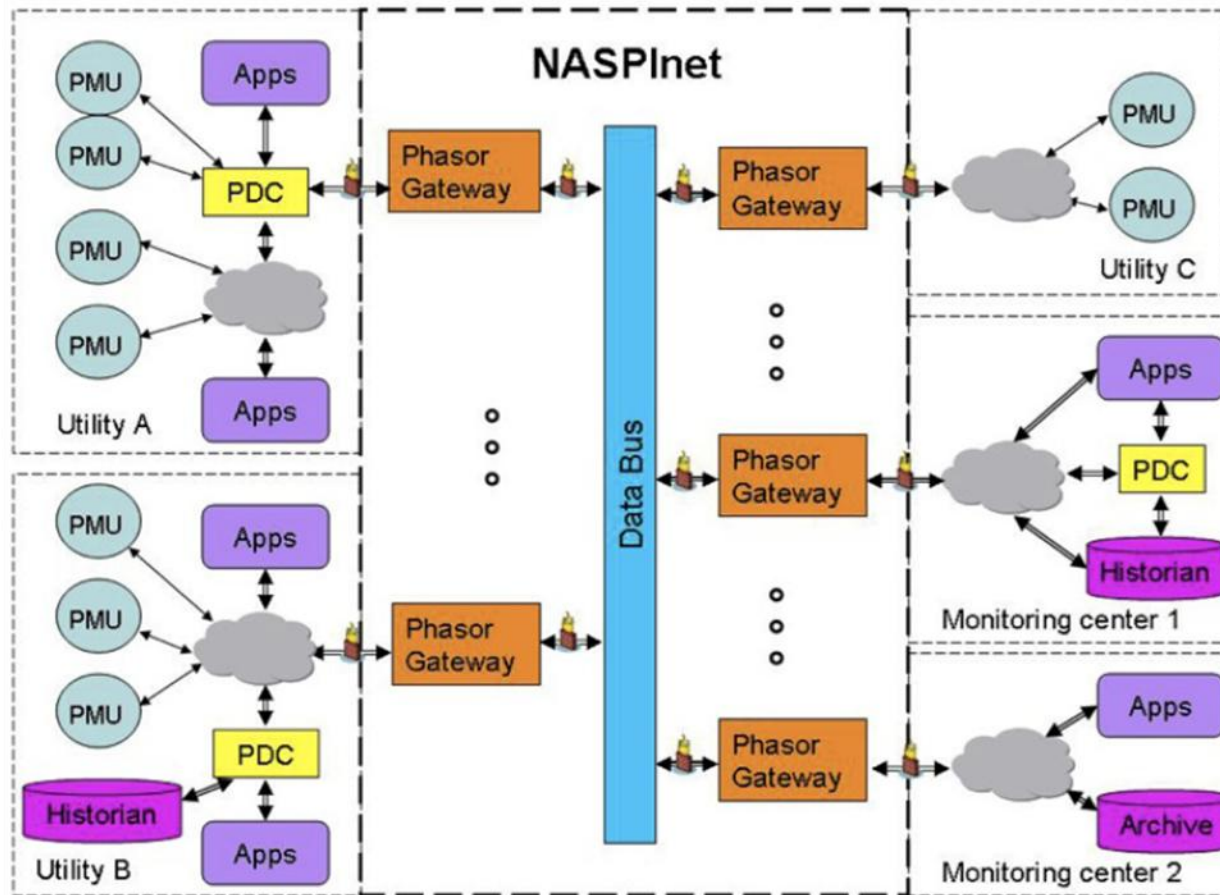
Filtering  
Decentralization



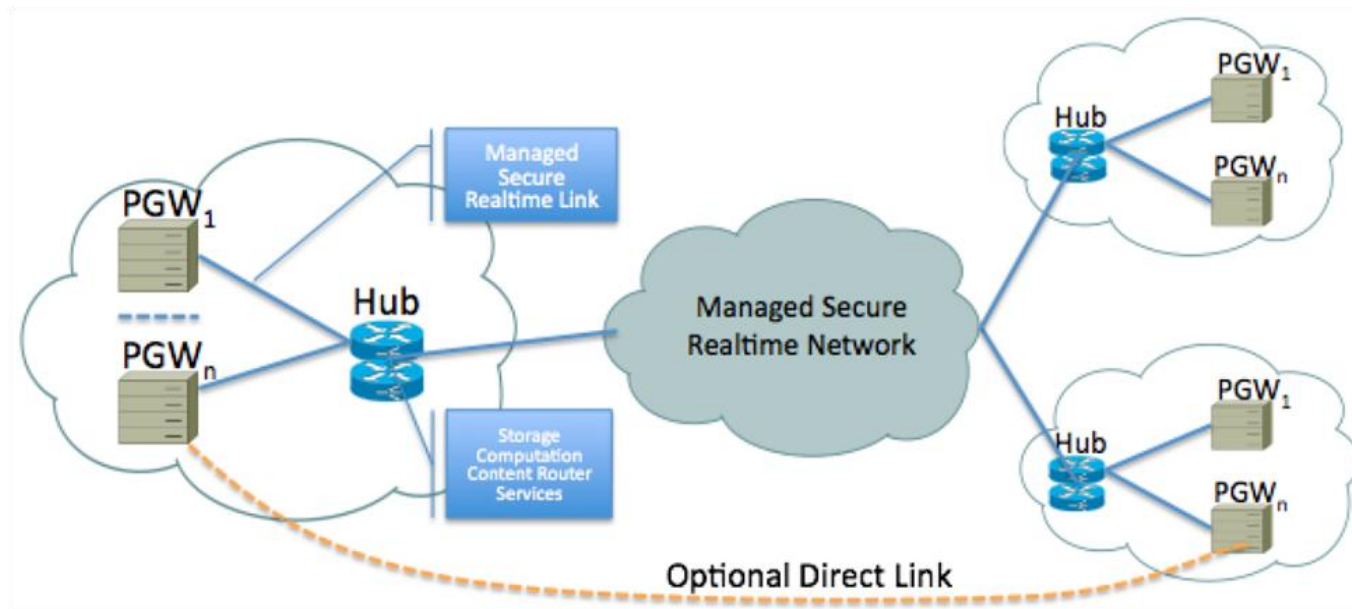
# Decentralization



# Integration with NASPInet



# Alternative NASPINet Integration



# Future Work

More detailed implementation strategies

Simulation

Pilot and performance tuning

# Acknowledgements

Ray Klump's work at the University of Illinois is supported by the National Science Foundation under Grant No. CNS-0524695 and by the Department of Energy under Award Number DE-OE0000097

Matt Kwiatkowski acknowledges that the submitted manuscript has been created by UChicago Argonne, LLC, Operator of Argonne National Laboratory ("Argonne"). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

Thank you.

