Challenges and Approaches for a Trustworthy Power Grid Cyber Infrastructure

Bill Sanders

CMU CEIC/CyLab Seminar

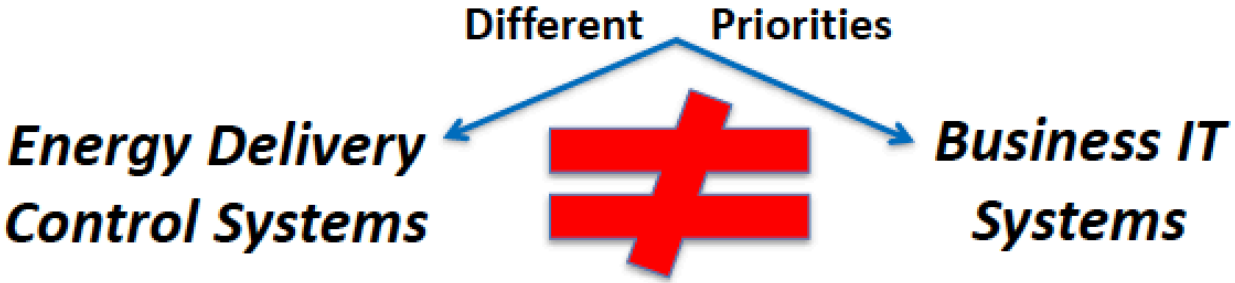
November 15, 2017

The Challenge: Providing Trustworthy Grid Operation in Possibly Hostile Environments

- Trustworthy
  - A system which does what it is supposed to do, and nothing else
  - Safety, Availability, Integrity, Confidentiality …
- Hostile Environment
  - Accidental Failures
  - Design Flaws
  - Malicious Attacks
- Cyber Physical
  - Must make the whole system trustworthy, including both physical & cyber components, and their interaction.

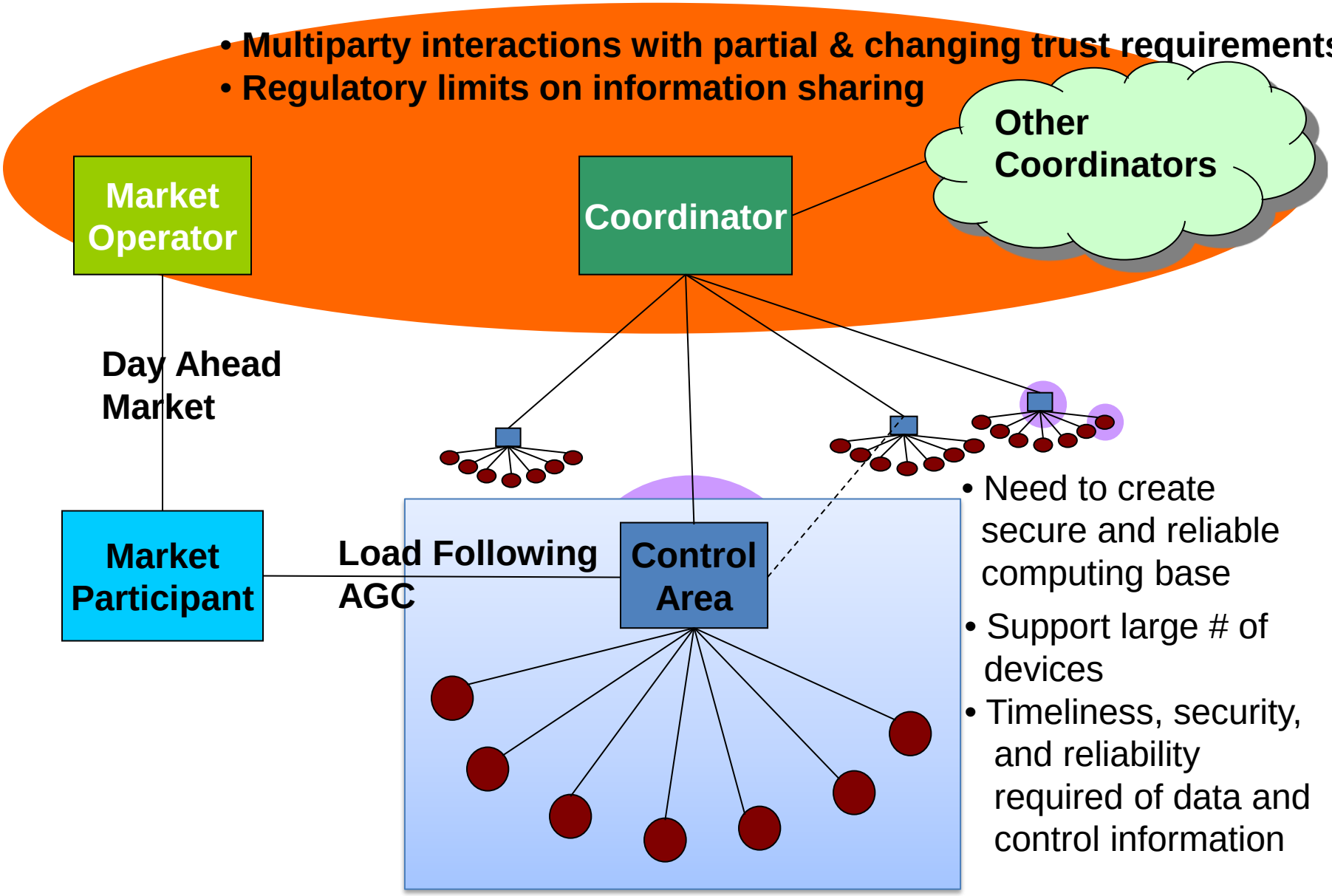
BACKGROUND.

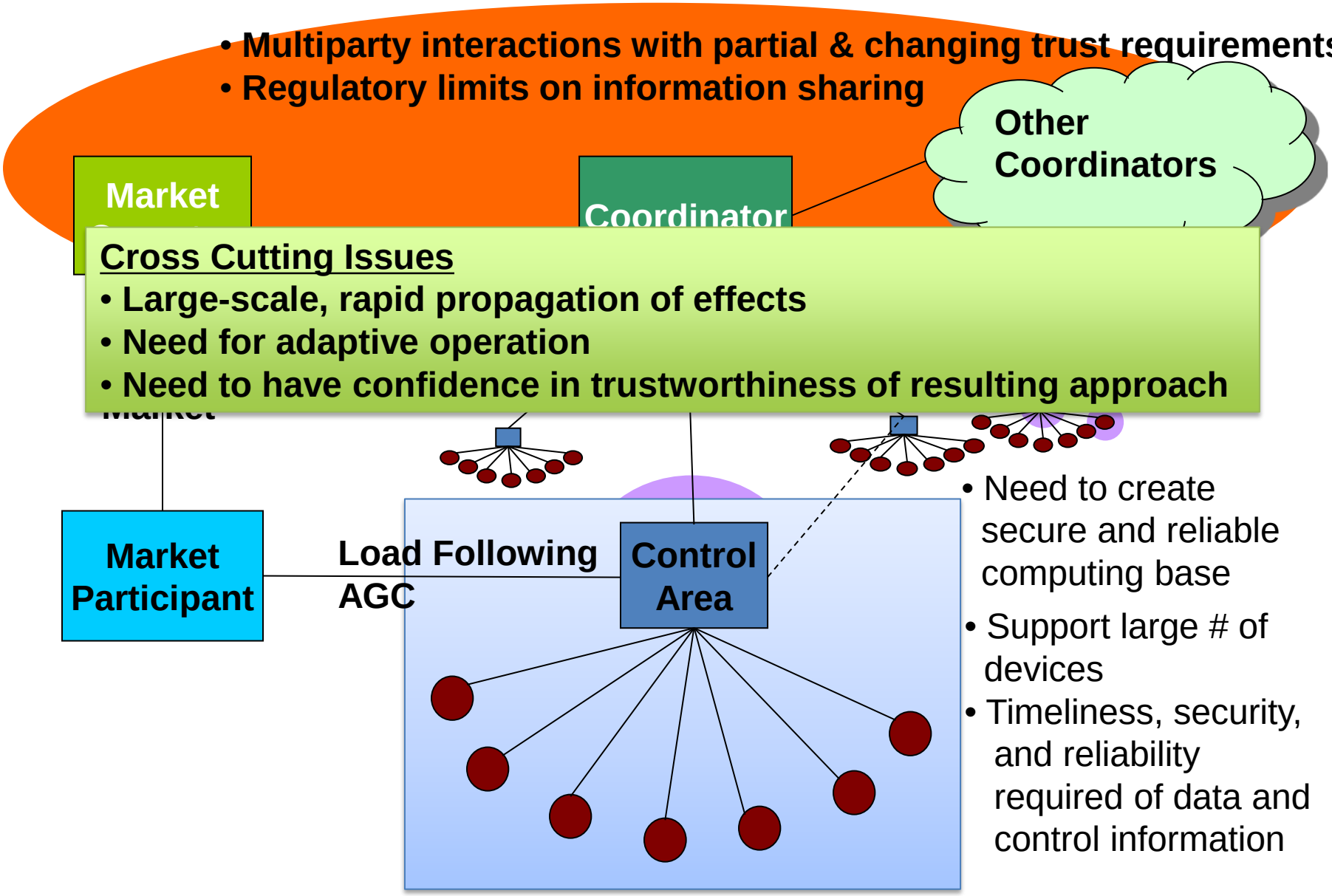
Energy Sector Cybersecurity



- Energy delivery control systems (EDS) must be able to survive a cyber incident while sustaining critical functions
- Power systems must operate 24/7 with high reliability and high availability, no down time for patching/upgrades
- The modern grid contains a mixture of legacy and modernized components and controls
- EDS components may not have enough computing resources (e.g., memory, CPU, communication bandwidth) to support the addition of cybersecurity capabilities that are not tailored to the energy delivery system operational environment
- EDS components are widely dispersed over wide geographical regions, and located in publicly accessible areas where they are subject to physical tampering
- Real-time operations are imperative, latency is unacceptable
- Real-time emergency response capability is mandatory

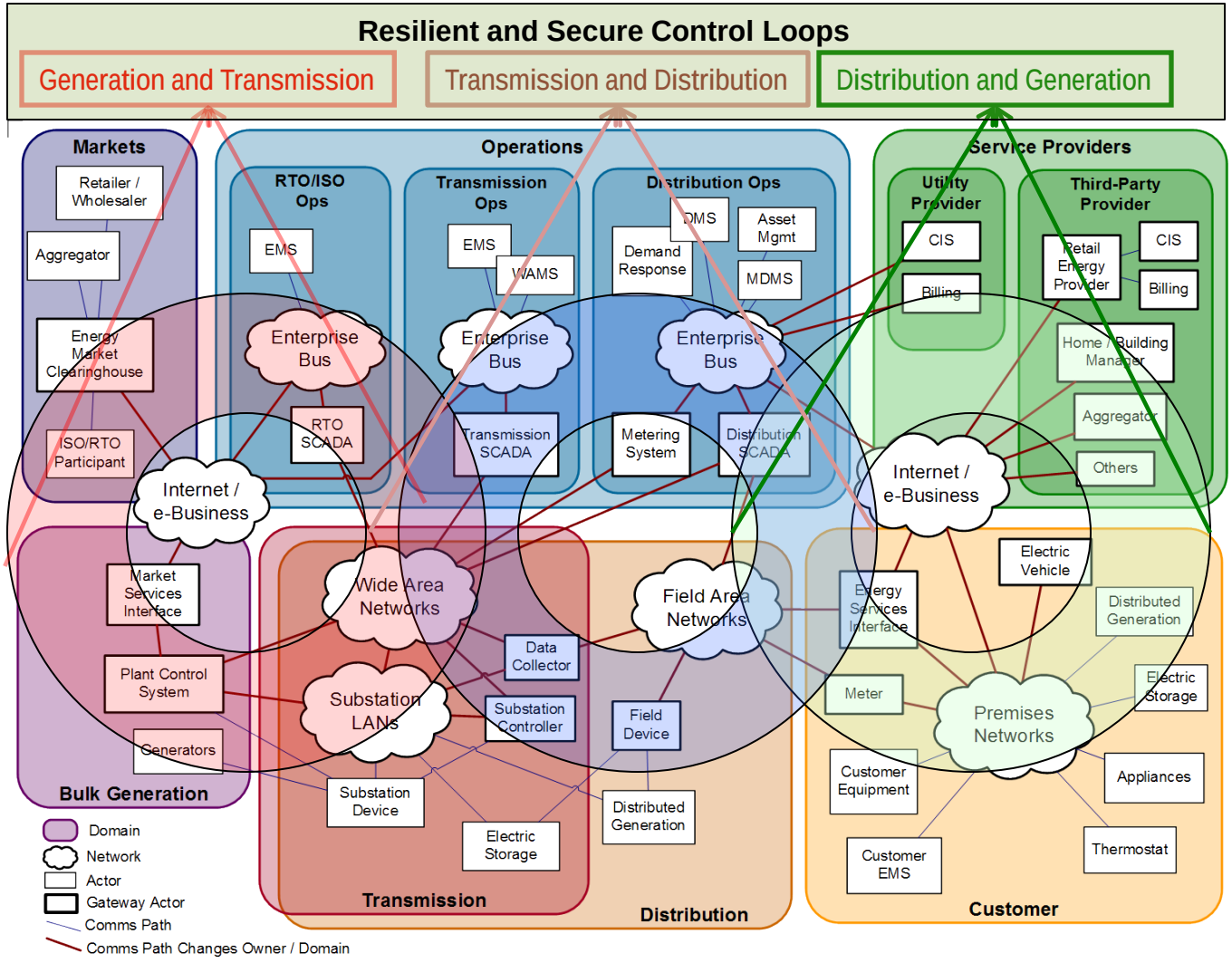
SOURCE: CAROL HAWK, DOE CEDS OVERVIEW PRESENTATION


• Multiparty interactions with partial & changing trust requirements
• Regulatory limits on information sharing
Other Coordinators
Market Operator
Coordinator
Day Ahead Market
Market Participant
Load Following AGC
Control Area
• Need to create secure and reliable computing base
• Support large # of devices
• Timeliness, security, and reliability required of data and control information


• Multiparty interactions with partial & changing trust requirements
• Regulatory limits on information sharing
Other Coordinators
Market
Coordinator
Cross Cutting Issues
• Large-scale, rapid propagation of effects
• Need for adaptive operation
• Need to have confidence in trustworthiness of resulting approach
Market Participant
Load Following
AGC
Control Area
• Need to create secure and reliable computing base
• Support large # of devices
• Timeliness, security, and reliability required of data and control information

In the smart grid, the cyber Infrastructure must provide control at multiple levels

- **Multi-layer Control Loops**
- *Multi-domain Control Loops*
  - Demand Response
  - Wide-area Real-time control
  - Distributed Electric Storage
  - Distributed Generation
- *Intra-domain Control Loops*
  - Home controls for smart heating, cooling, appliances
  - Home controls for distributed generation
  - Utility distribution Automation
- **Resilient and Secure Control**
  - *Secure and real-time communication substrate*
  - Integrity, authentication, confidentiality
  - Trust and key management
  - End-to-end Quality of Service
  - *Automated attack response systems*
  - *Risk and security assessment*
  - Model-based, quantitative validation tools



Note: the underlying Smart Grid Architecture has been developed by EPRI/NIST.

HUMBLE CYBER SECURITY BEGININGS, CIRCA 2000.

RAPID ADVANCE TO ADOLESCENCE.

Classical (Physical) Attack Approaches

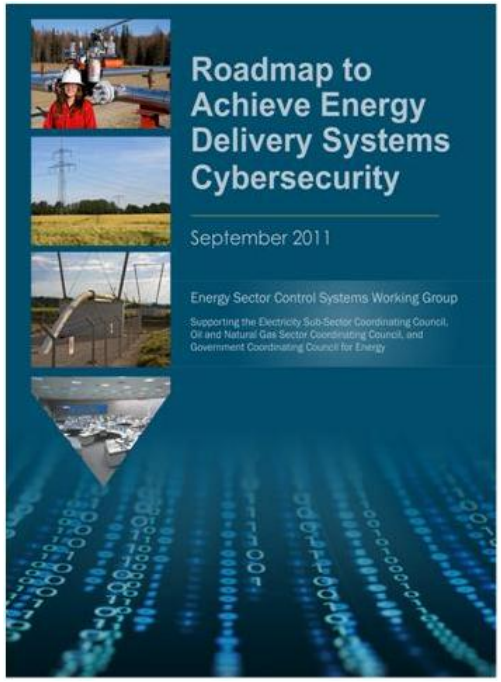
- Physical attacks on lines, buses and other equipment can be locally effective:
  - "low tech" attacks may be easy, and are also difficult to defend against
  - Requires physical proximity of attacker
  - Particularly effective if multiple facilities are attacked in a coordinated manner
- But coordination may be much easier in a cyber attack

J.D. Konopka (a.k.a. Dr. Chaos) Alleged to have caused $800K in damage in disrupting power in 13 Wisconsin counties, directing teenaged accomplices to throw barbed wire into power stations. (From Milwaukee Journal Sentinel)
http://www.jsonline.com/news/Metro/may02/41693.asp

Potential Cyber Attack Strategies

- Tripping breakers
- Changing values breaker settings
  - Lower settings can destabilize a system by inducing a large number of false trips
  - Lowering trip settings can cause extraneous other breakers, causing overloading of other transmission lines and/or loss of system stability
- Corrupting Control Information: Smart Meters, SCADA Data, PMU Data, Dispatch Information, etc.
- Sophisticated multi-stage attacks
- Life cycle attacks
- Insider threats
- Physical damage by cyber means
- Combined physical and cyber attacks

Industry Roadmap – A Framework for Public-Private Collaboration



- Published in January 2006/updated 2011
- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in control systems security

Roadmap Vision

By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

FERC/NERC Cyber security Standards for the Bulk Electric Power Grid

- Energy Policy Act of 2005 created an Electric Reliability Organization (ERO) to develop and enforce mandatory cybersecurity standards
- FERC designated NERC as the ERO in 2006
- NERC worked with electric power industry experts to develop the NERC Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009
- Standards approved by FERC in 2008, making them mandatory for owners and operators of the bulk electric system
- NERC standards continue to evolve, as the threat environment evolves, and more is known about critical infrastructure protection

Real Financial Penalties

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

October 31, 2012

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req.	VRF	Total Penalty
Reliability*First* Corporation	URE1	1448	RFC201100957	CIP-002-1	R1	Medium[5]	$725,000
Reliability*First* Corporation	URE1	1448	RFC201100958	CIP-002-1	R2	High[6]	

http://www.nerc.com/filez/enforcement/Public_FinalFiled_NOP_NOC-1448.pdf

TODAY'S CYBER RESILENCEY TRENDS, CHALLENGES, AND GAPS.

Disruptive Trends
Challenges
Research and Technology Gaps

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

From Security to Resiliency: Opportunities and Challenges for the Smart Grid's Cyber Infrastructure

Introduction

The electric power grid is in the midst of an ongoing modernization to the "smart grid," which includes deployment of an extensive cyber-physical infrastructure with sophisticated networking and computational resources. It includes components from the smart meter to the pole-top to the substation to the regional operation center, systems that measure grid states many times per second over large areas, and sophisticated analytics that support grid operation in

such societal goals of the smart grid, while at the same time improving its security and resiliency in the face of increased opportunities for external disruption.

Our purpose here is to consider *cyber resiliency* as the key enabler of *grid resiliency*. We start by identifying emerging trends in smart grid technology that create demands for increased resiliency, but also increase the number of ways in which disruptions might be introduced. They include:

- the incremental nature of technology introduction,

Position paper available on request

Disruptive Trends in the Smart Grid (1/4): *Transformation of the Smart Grid Infrastructure*

- Large numbers of intelligent devices in the substation and the field
- Smart meters deployed as part of AMI
- Larger-scale wide-area measurement systems
- Mixed legacy environment with older components that cannot support modern security mechanisms

Disruptive Trends (2/4): *Energy "Internet of Things" and Utility Clouds*

- Radical changes in the way industrial control systems will be managed, owing to network virtualization and increased connectivity
- Increased availability of data and analysis
- Many events will become manageable in the cloud as "wide-area system events"
- Increased dependence on computation and communication will increase the attack surface

Disruptive Trends (3/4): *Renewables*

- Wind and solar are both subject to short-term fluctuations that can potentially destabilize a grid
- Resiliency requires technology that can sense fluctuations quickly and respond to dynamic variation in generation
- Requirement for high system “self-awareness” as well as advanced analytics
- Distributed generation ownership complicates issue

Disruptive Trends (4/4): *Electric Vehicles*

- "EV Everywhere" will require a new grid infrastructure, with new security and resiliency requirements
- Control of infrastructure must deal with rapid changes of volume and location of loads
- Billing is likely to follow vehicle
- Will result in complex mobile and human-based cyber-physical system which will create new reliability and security issues

Challenges (1/2):
Grid resiliency tied to Cyber Infrastructure Resiliency

- Grid Resiliency may be impacted by the grid's increased dependence on cyber technology
- Adverse cyber events may arise from cyber attack, or from software/hardware malfunction, or through error in configuration or operation
- Cyber assets might be compromised with no direct attack on the physical grid system, or a blended attack could impact both cyber and physical assets

Challenges (2/2): *Grid Dependency on other Infrastructures*

- Hydroelectric power depends on the correct function of dam controls
- Smart grid communication depends on the telecommunication infrastructure
- The grid features multiple interdependencies with transportation for fuel delivery
- The emerging electric vehicle system will introduce multiple interfaces, including to transportation
- Smart grid market mechanisms will necessitate interfaces to the financial infrastructure, particularly in the case of demand response stimulated by rapid real-time price fluctuations

Research and Technology Gaps (1/4): *Advanced Sensing, Analytics and Control*

- Advanced analytics needed to leverage the wide-area measurement systems being deployed in the smart grid
- Cyber-physical contingency analysis must be developed to support grid resilience
- Advanced controls needed for intelligent autonomous or semi-autonomous islanding to achieve resiliency

Research and Technology Gaps (2/4): *Building a Detection and Response Mechanism*

- Detection of suspicious events
  - Profusion of potential attack points
  - Direct detection via cyber traffic analysis
  - Detection informed by physical system state
- Making sense of potential “event avalanche”
  - Situational awareness
  - Comprehend the joint cyber and physical state
- Response
  - Carefully consider consequence of response
  - Ultimately, operate through cyber attack or failure

Research and Technology Gaps (3/4): *Resiliency Assessment*

- Define appropriate security metrics
  - Integrated at multiple levels
  - Applied throughout system lifecycle
  - Be both “process” and “product” oriented
- Determine methods for estimating metrics
  - To choose appropriate architectural configuration
  - To test implementation flaws, e.g., fuzzing, firewall rule analysis
  - Can be applied in cost effective manner *before* an audit
- Link metrics to technical and business concerns

Research and Technology Gaps (4/4): Addressing Non-Technical Issues

- Smart grid components being deployed today will be in the field for a decade or more
- Social, cultural, and human factors

APPROACHES.

Cyber Resilient Energy Delivery Consortium (CREDC)

- **Will improve the resilience and security of the cyber networks that serve as the backbone of energy infrastructure**
- **11 universities and national laboratories:** Argonne, Arizona State, Dartmouth, MIT, Oregon State, PNNL, Rutgers, Tennessee State, Univ. Houston, and Wash. State
- **Funded by DOE: $28.1 million initiative**
- **Led by David Nicol, with Sanders and Sauer as co-PIs**
- Broadens TCIPG research scope to include the oil & gas industry and provides focus on resiliency

CREDC Goals

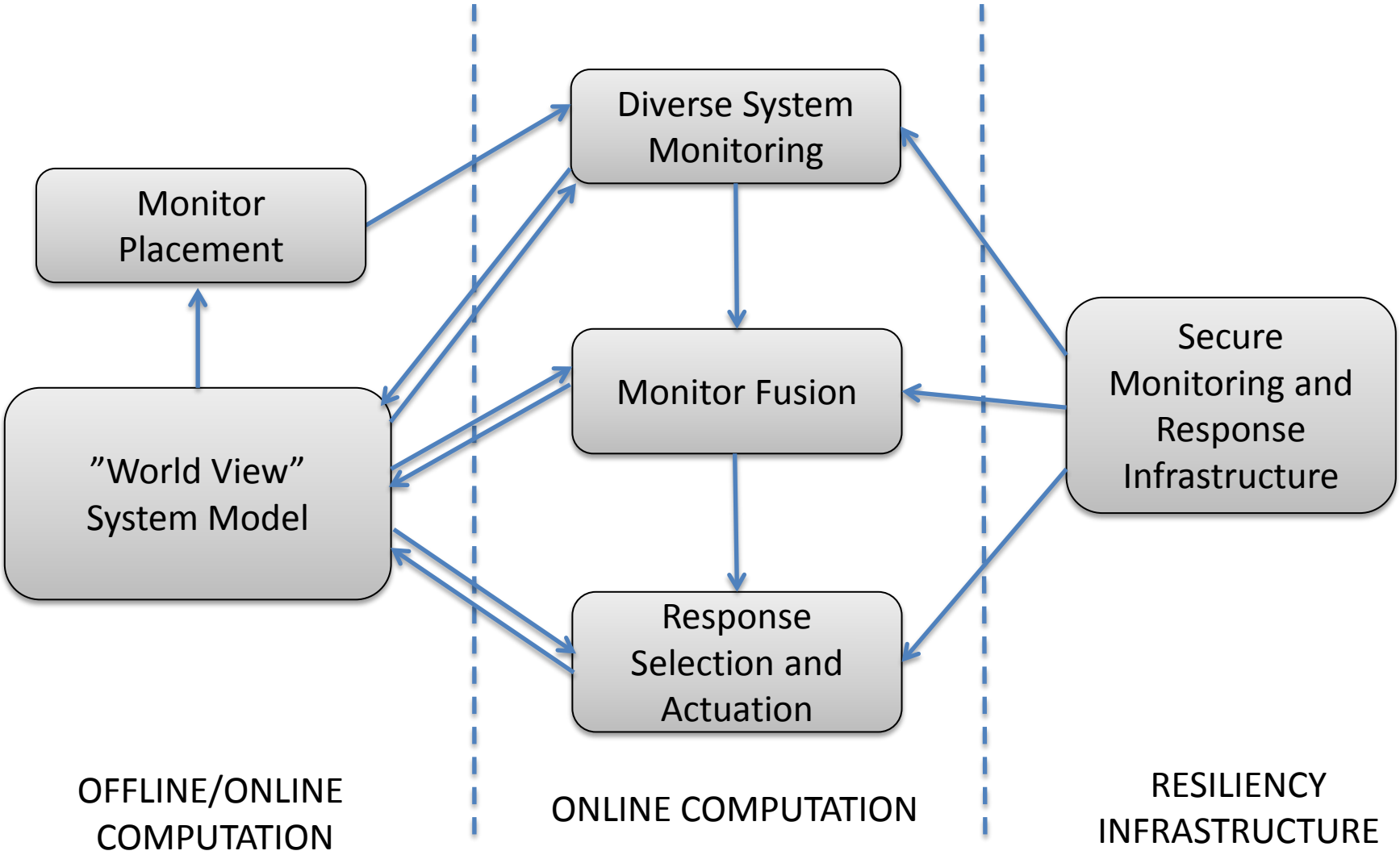
- Identify gaps in the existing cyber infrastructure for energy delivery with respect to enhancing EDS resiliency
- Identify trends in emerging technologies that may impact resiliency
- Perform long-term and mid-term research closing gaps, with mid-term research leading to validated solution prototypes
- Develop software infrastructure for empirical evaluation on hardware testbeds
- Develop educational and out-research activities

CREDC Research Areas

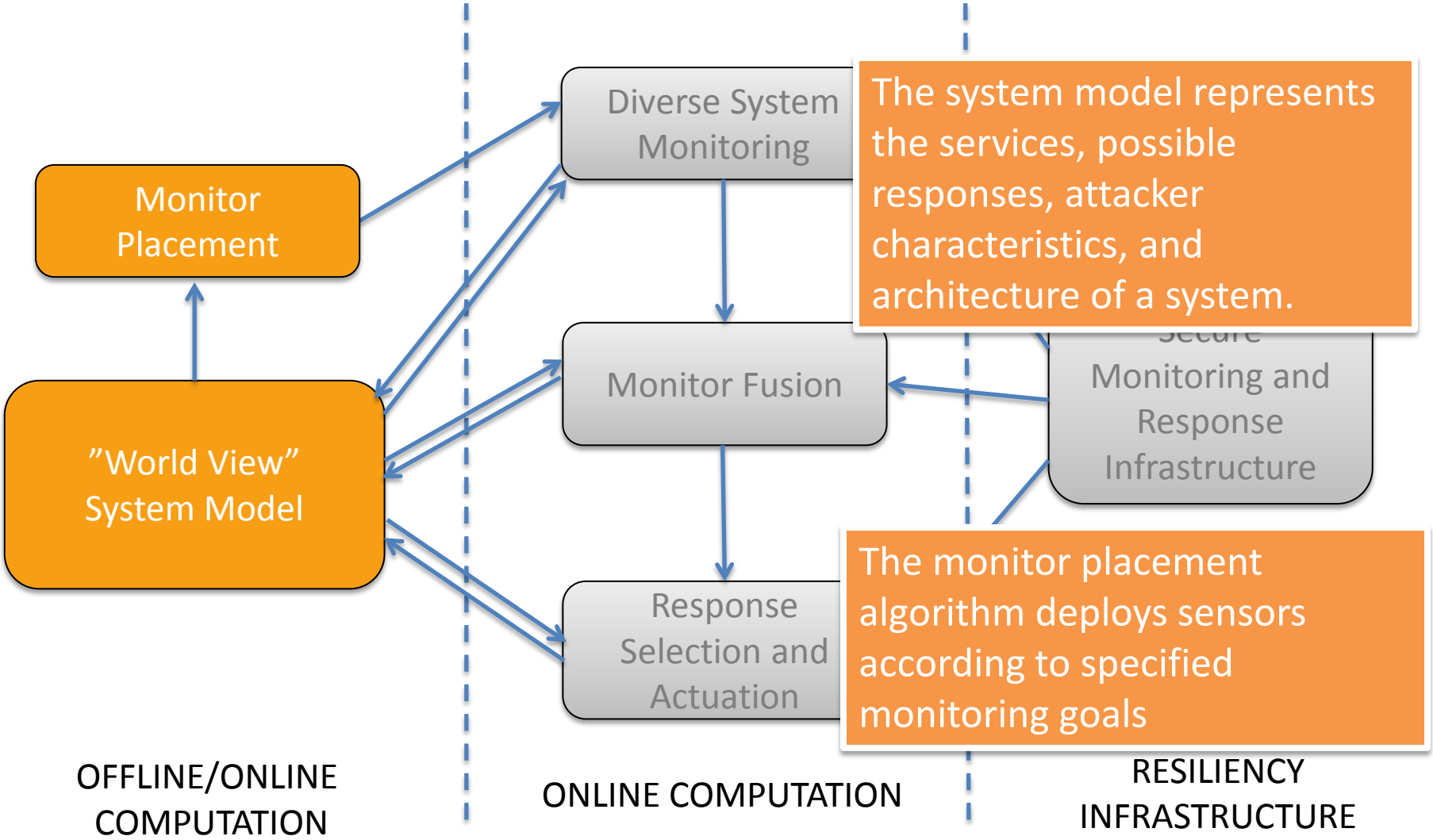
- Cyber-Protection Technology
- Cyber Monitoring, Metrics, and Evaluation
- Risk Assessment of EDS Technology and Systems
- Data Analytics for Cyber Event Detection, Management, Recovery
- Resilient EDS Architectures and Networks
- Impact of Disruptive Technologies on EDS
- Validation and Verification

EXAMPLE APPROACH: Resilient EDS Architectures and Networks

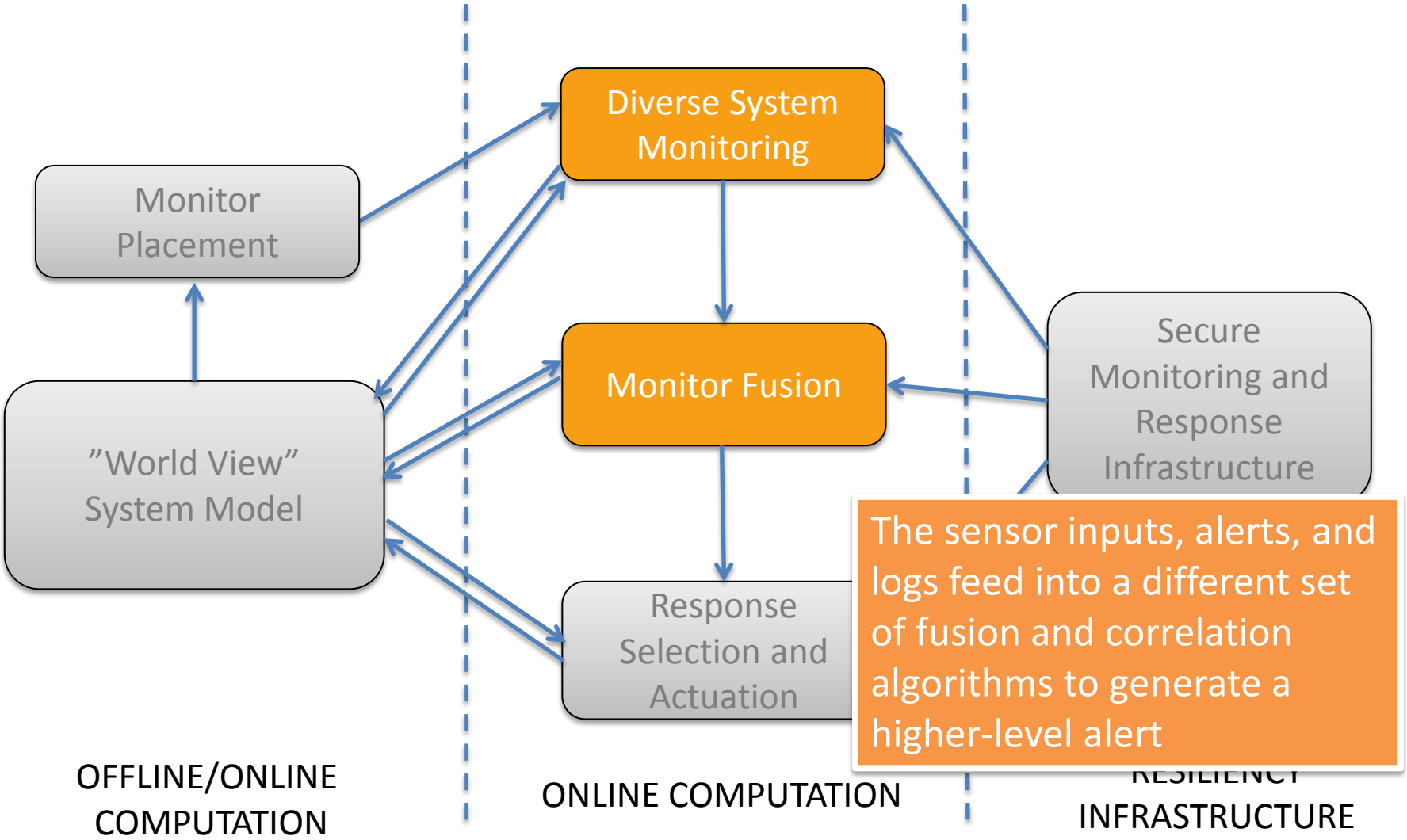
Notional Architecture for Resiliency



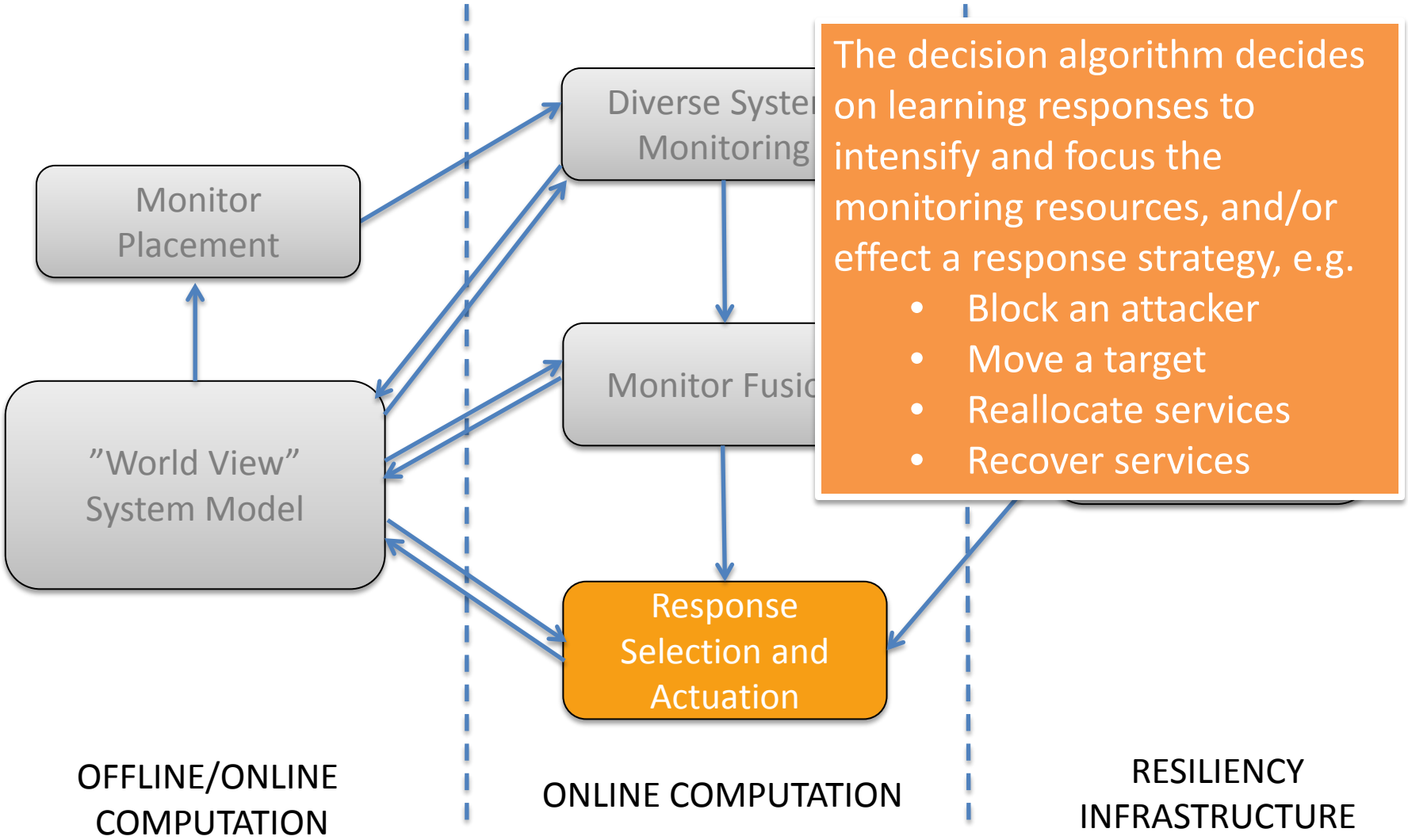
Notional Architecture for Resiliency



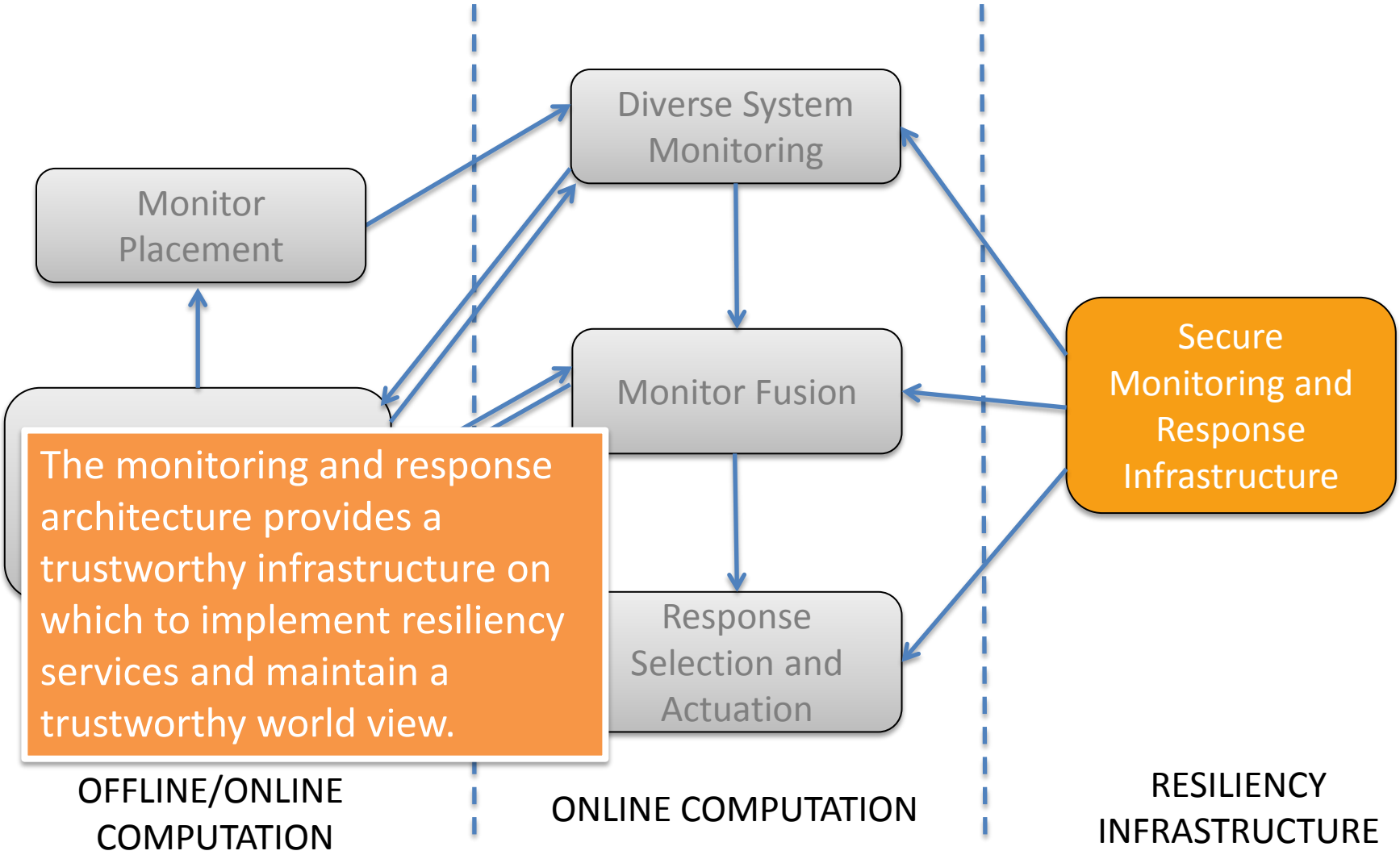
Notional Architecture for Resiliency



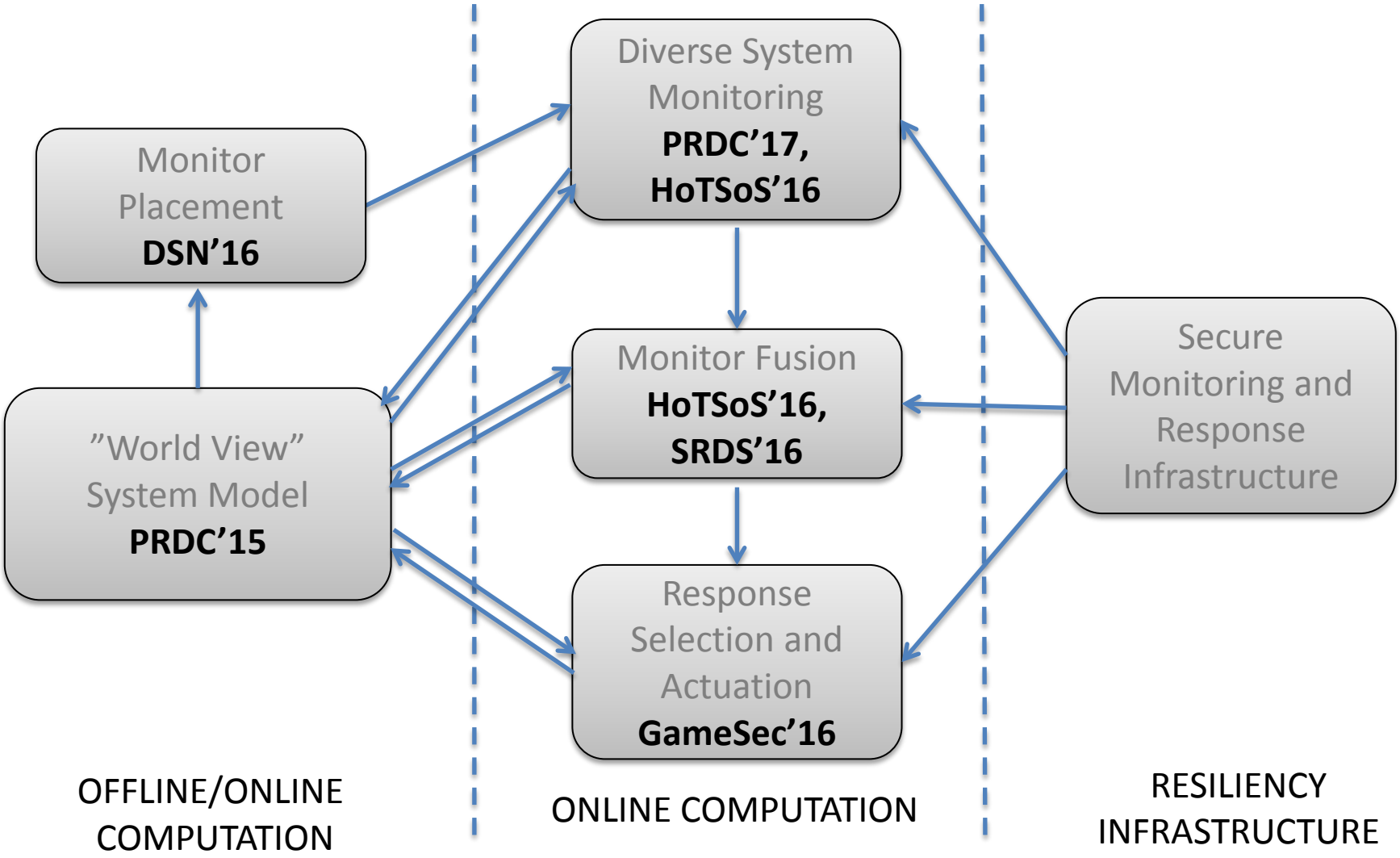
Notional Architecture for Resiliency



Notional Architecture for Resiliency



Current Work Guided is by Notional Architecture



New Challenge/Opportunity: SCADA as a Service

- Traditional SCADA is an artifact of the "old" centralized power grid.
- SCADA is inflexibile to support "new" microgrids and renewables.

Benefits for SCaaS:

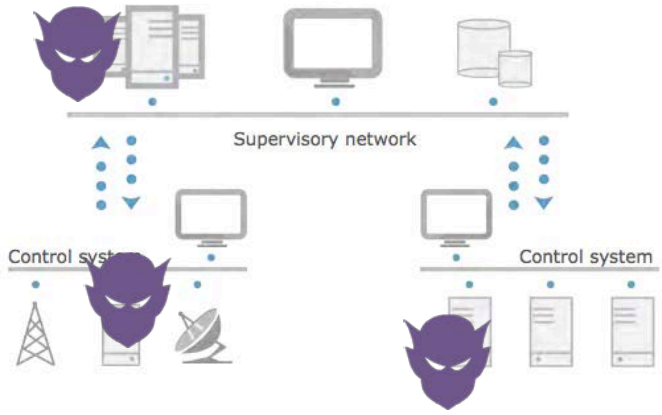
- Reduce cost as opposed to hosting an in-house system
- Facilitate remote support and expertise.
- Reduce risk of data loss during disaster.
- Provide on-demand computational resources.

Challenges:

- Cloud requires power to operate.
- Power grid is a real-time system with hard deadlines.
- Cloud and Internet are not reliable.

Resilient SCaaS

- Provide hybrid sensor fusion to detect malicious behavior on the expanded SCADA attack surface.
- Design response mechanisms in SCaaS to support resilient operation during cyber attacks.



Trend Micro Inc., "SCADA in the Cloud A Security Conundrum?", 2013

New Challenge/Opportunity: SCADA as a Service

Attack surface expands to include:
- Communication between the RTU and cloud
- Virtual machines (public cloud setting)

- Traditional SCADA is an artifact of the "old" centralized power grid.
- SCADA is inflexibile to support "new" microgrids and renewables.

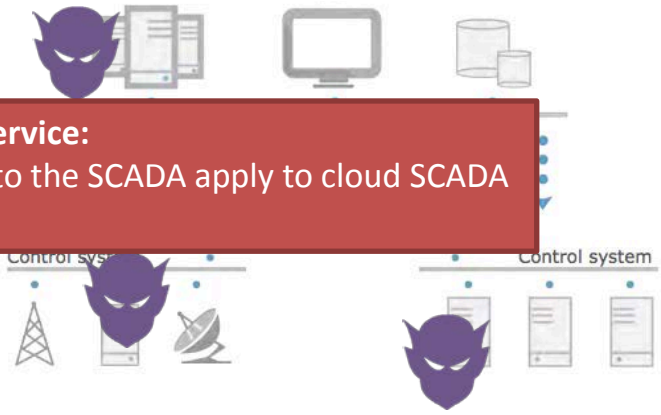
Benefits for SCaaS:

- Reduce cost as opposed to hosting an in-house system
- Facilitate remote support and expertise.
- Reduce risk of data loss during disaster.
- Provide on-demand computational resources.

Challenges:

- Cloud requires power to operate.
- Power grid is a real-time system with hard deadlines.
- Cloud and Internet are not reliable.

Threats to SCADA as a Service:
- "Traditional" threats to the SCADA apply to cloud SCADA
- Cloud threats



Trend Micro Inc., "SCADA in the Cloud A Security Conundrum?", 2013

Resilient SCaaS

- Provide hybrid sensor fusion to detect malicious behavior on the expanded SCADA attack surface.
- Design response mechanisms in SCaaS to support resilient operation during cyber attacks.

EXAMPLE APPROACH: Risk Assessment of EDS Technology and Systems (1)

Failure to Comply with NERC/CIP Requirements: Real Financial Penalties

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

October 31, 2012

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req.	VRF	Total Penalty
Reliability*First* Corporation	URE1	1448	RFC201100957	CIP-002-1	R1	Medium[5]	$725,000
Reliability*First* Corporation	URE1	1448	RFC201100958	CIP-002-1	R2	High[6]	

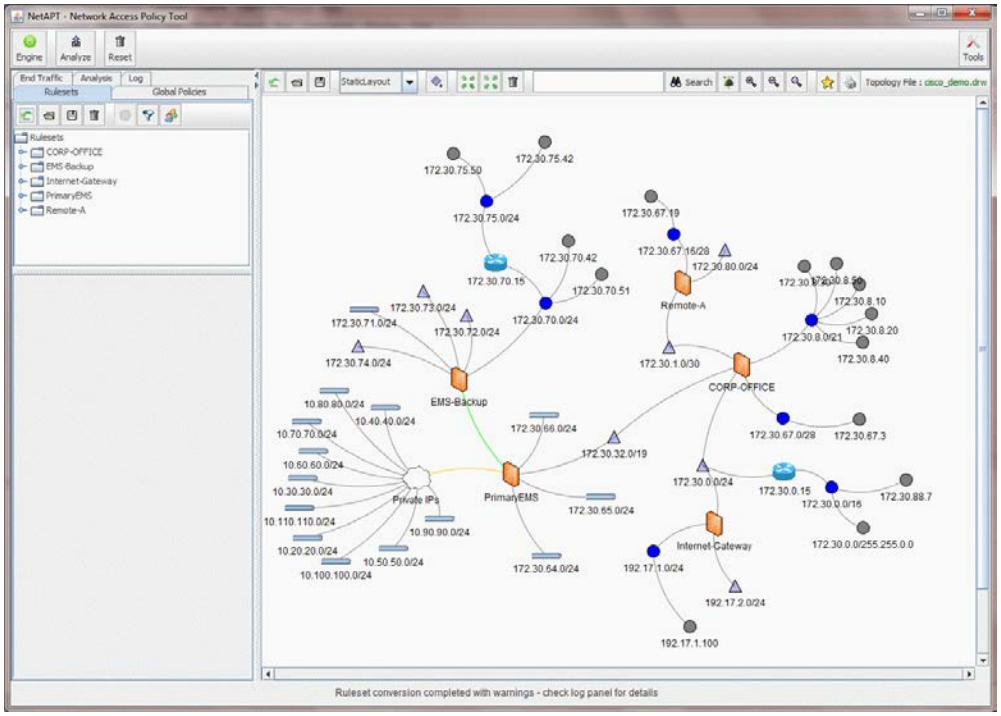
http://www.nerc.com/filez/enforcement/Public_FinalFiled_NOP_NOC-1448.pdf

Operation-Time Compliance/Risk Assessment Needs

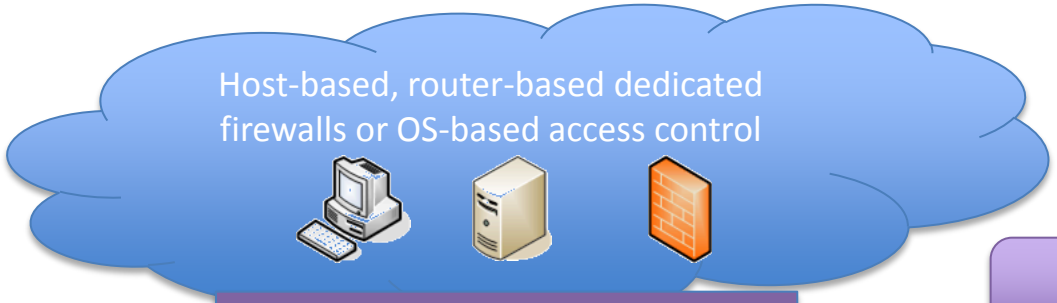
- Complexity of network infrastructures is growing every day
  - Security policies become too large to be manually verified
  - Utilities do not have IT resources to manage incidents
- Lack of situational awareness solutions to understand the impact of potential threats
- High cost to comply with security regulations
  - Critical Infrastructure, Protection (CIP) Reliability standards
- Even higher cost when infractions are found

Analysis Approach

- NP-View tool performs a comprehensive security policy analysis
  - Understand complex interactions in a system where multiple firewalls are deployed
- Automate most of the reporting process required during an audit



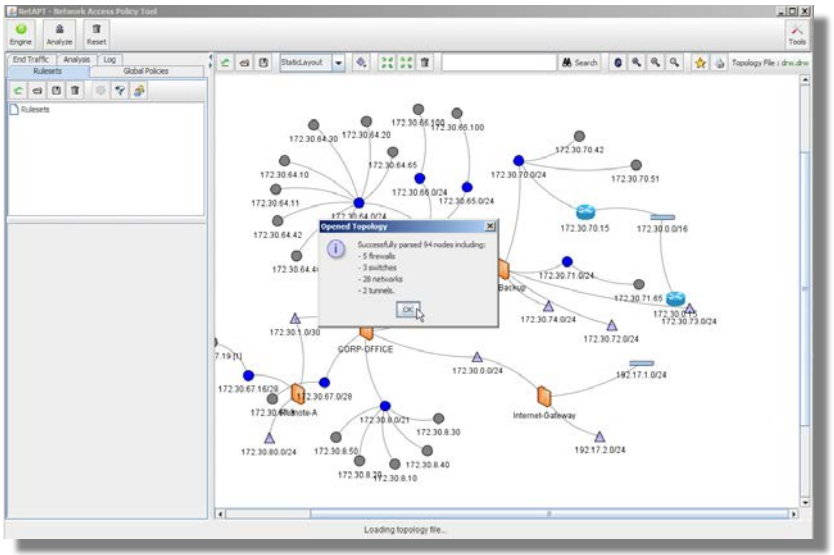
Analysis Overview



Securely import rule-sets

1. Parse Native Configuration Files

2. Infer topology:
- Inspecting routes
- Creating primary networks
- Marking VPN networks
- Creating nodes from group definitions
- Building border cloud of unmapped IP
- Saving results to XML files

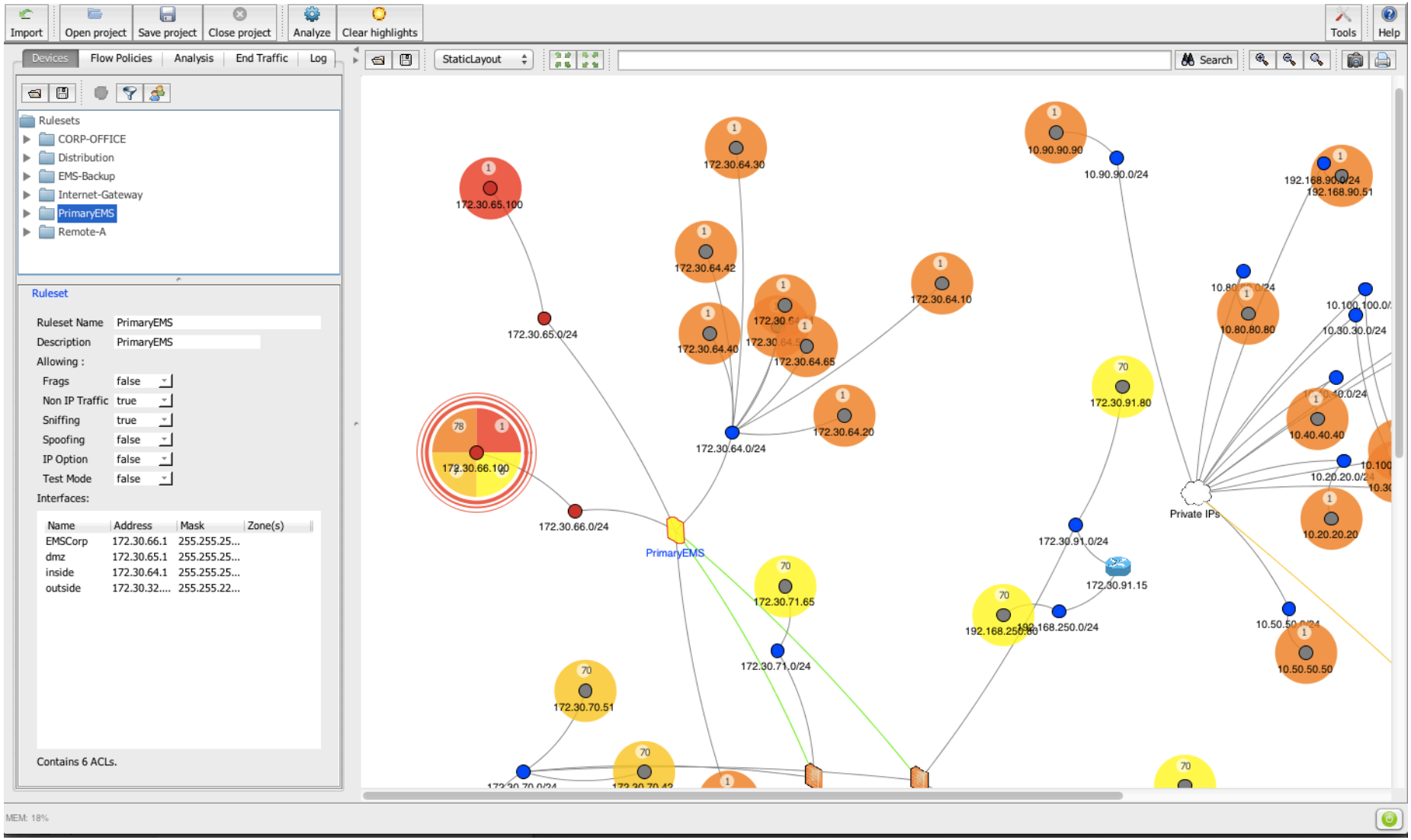


3. Load model into engine:
- Looking up dynamic IP addresses
- Creating data structures to store rules
- Generating graph to store topology

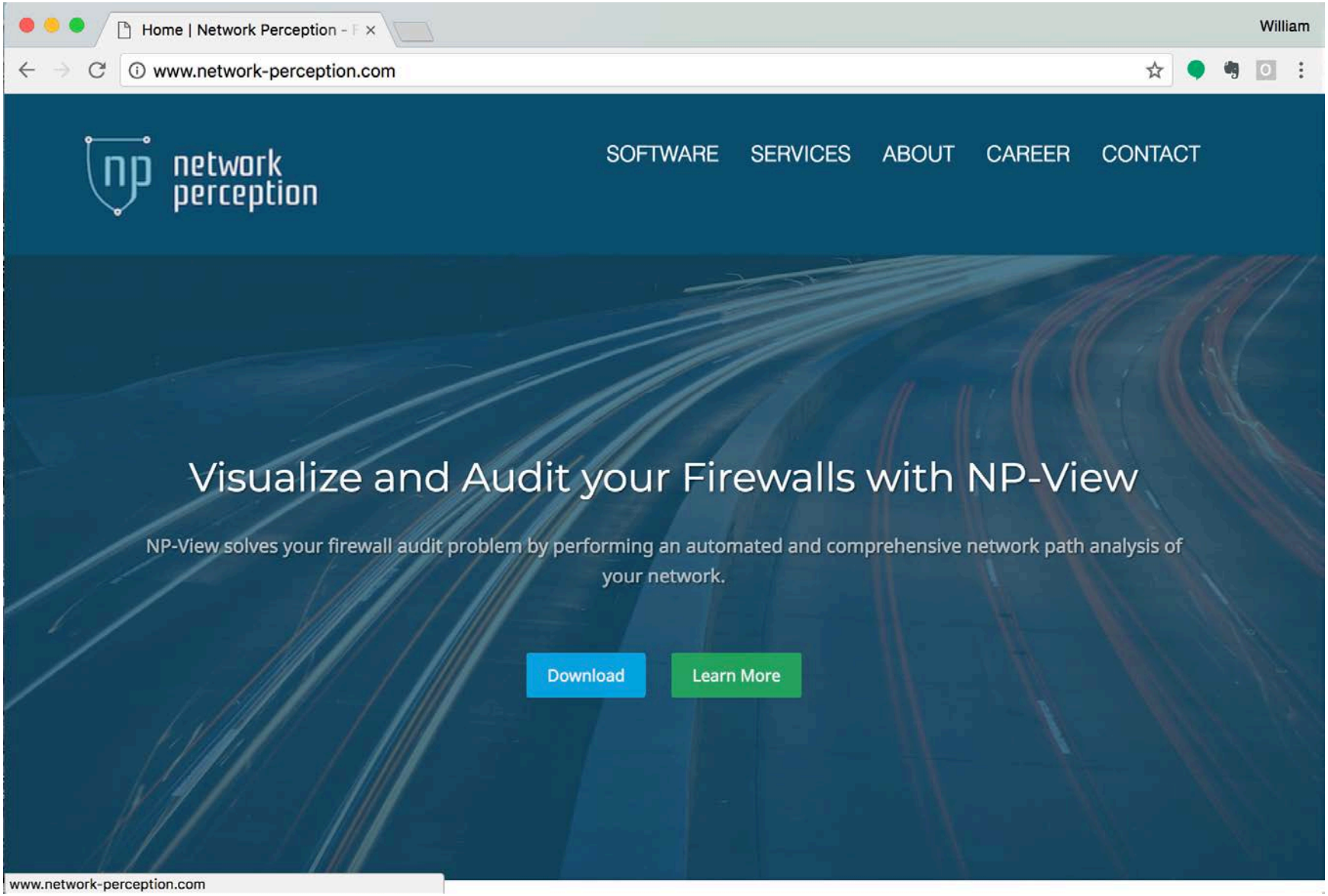
Path Analysis is Key

- The engine keeps a model of the network in memory
- Type of path analysis queries:
  - **Exhaustive** path analysis
    - Return all possible paths in the network
    - Prone to scalability issues for large networks
  - **End point** (a network or a host)
    - Return all possible paths originating or ending at the selected end point
  - **Firewall**
    - Return all possible paths permitted by a selected firewall
    - Can be refined for a specific ACL and a specific rule
  - **Tunnel**
    - Return all possible paths that go through a selected tunnel
  - **Pair analysis**
    - Return all possible paths going from a selected source to a selected destination
    - Provide a “path halt” mode to troubleshoot why a path doesn’t reach its destination

Network Vulnerability Analysis



Commercialization

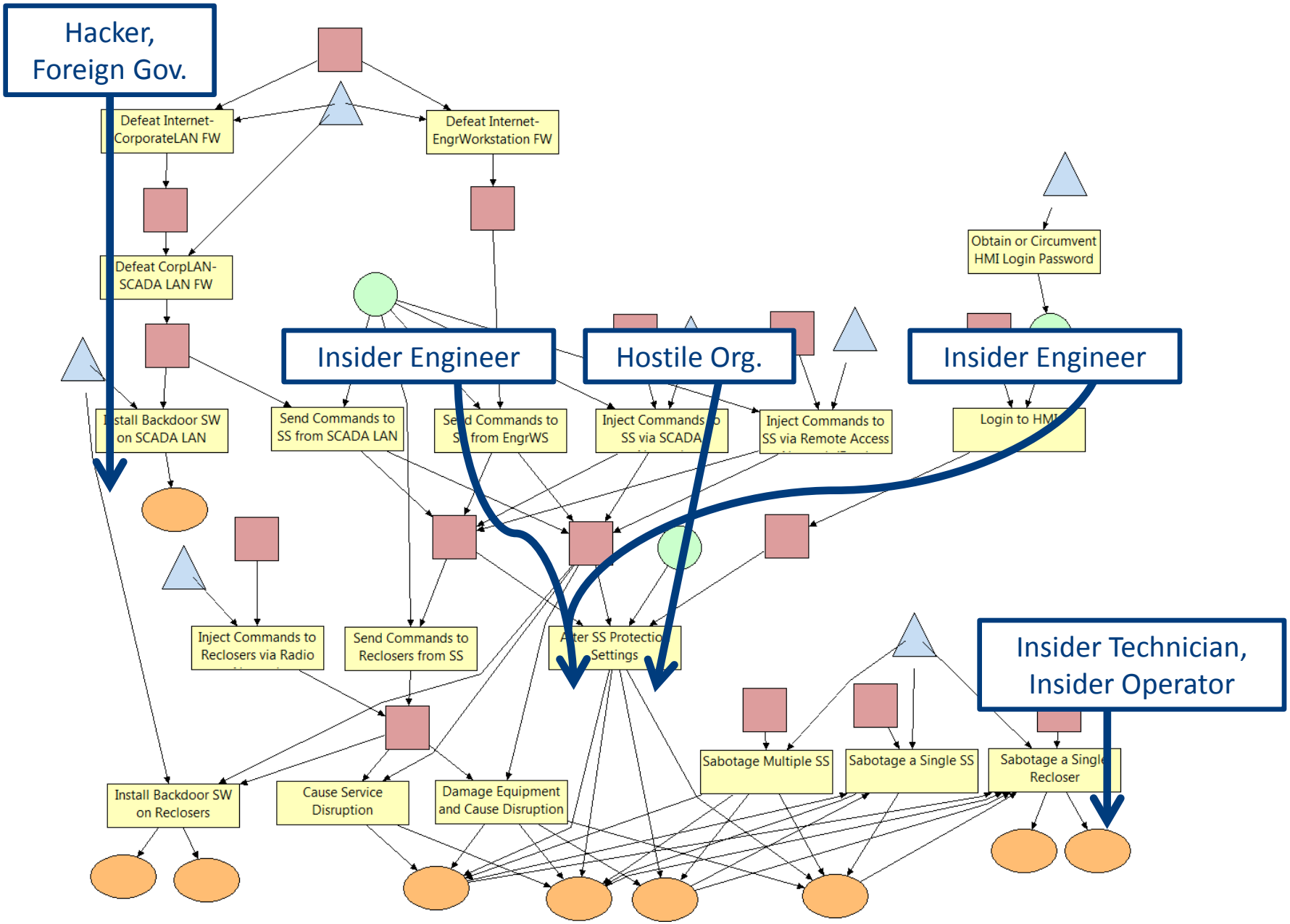


EXAMPLE APPROACH: Risk Assessment of EDS Technology and Systems (2)

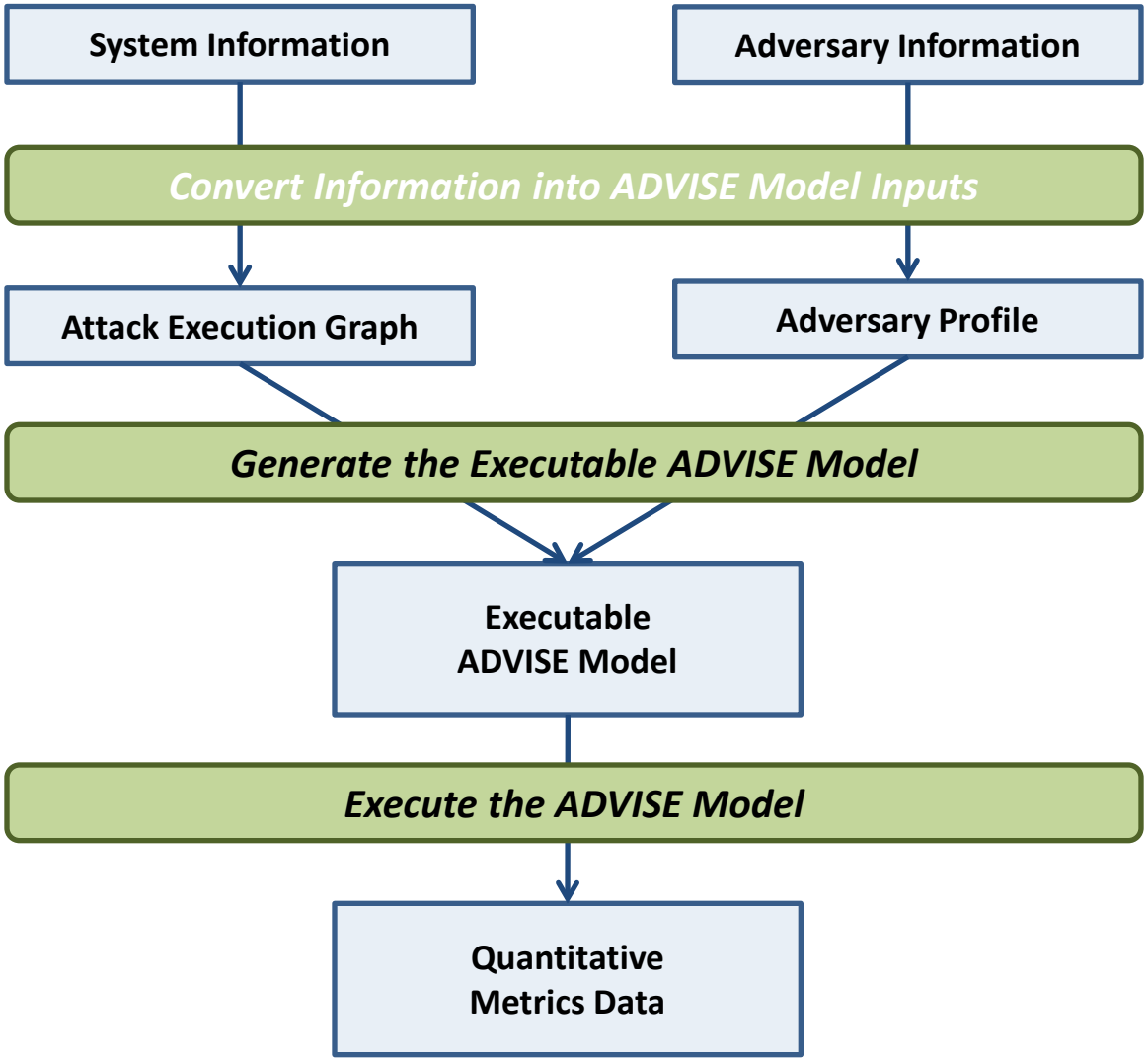
Quantifying Resiliency

- At design time
  - System architects make trade-off decisions to best meet all design criteria
  - Other design criteria can be quantified: performance, reliability, operating and maintenance costs, etc.
  - *How can we quantify the security of different system designs*?
- During system operation and maintenance
  - Modifying the system architecture can improve or worsen system security
  - *How can we compare the security of different possible system configurations?*

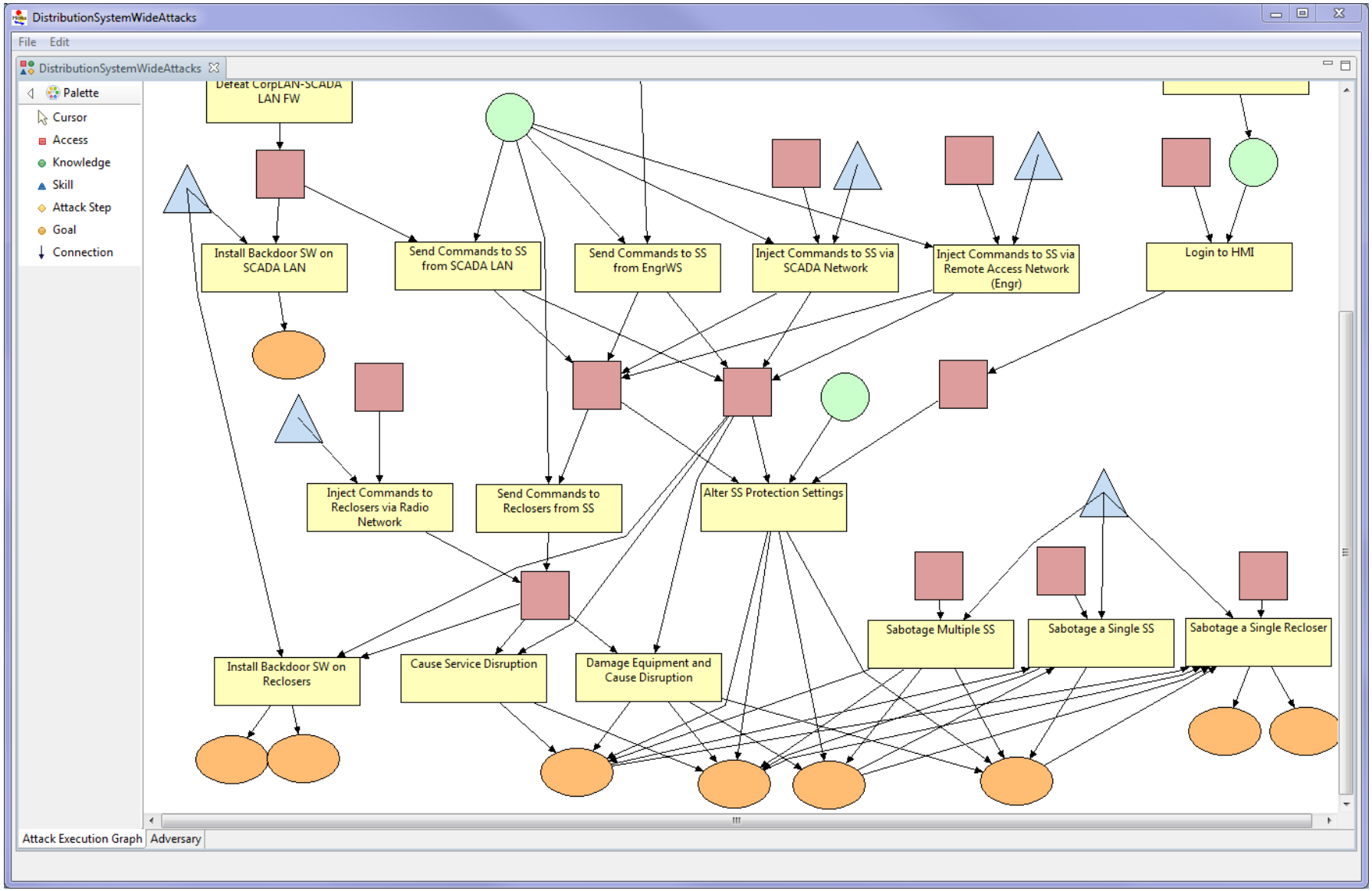
Model-based system-level resiliency evaluation


Hacker, Foreign Gov.
Defeat Internet-CorporateLAN FW
Defeat Internet-EngrWorkstation FW
Defeat CorpLAN-SCADA LAN FW
Obtain or Circumvent HMI Login Password
Insider Engineer
Hostile Org.
Insider Engineer
Install Backdoor SW on SCADA LAN
Send Commands to SS from SCADA LAN
Inject Commands to SS via Remote Access
Inject Commands to Reclosers via Radio
Send Commands to Reclosers from SS
Insider Technician, Insider Operator
Sabotage Multiple SS
Sabotage a Single SS
Install Backdoor SW on Reclosers
Cause Service Disruption
Damage Equipment and Cause Disruption

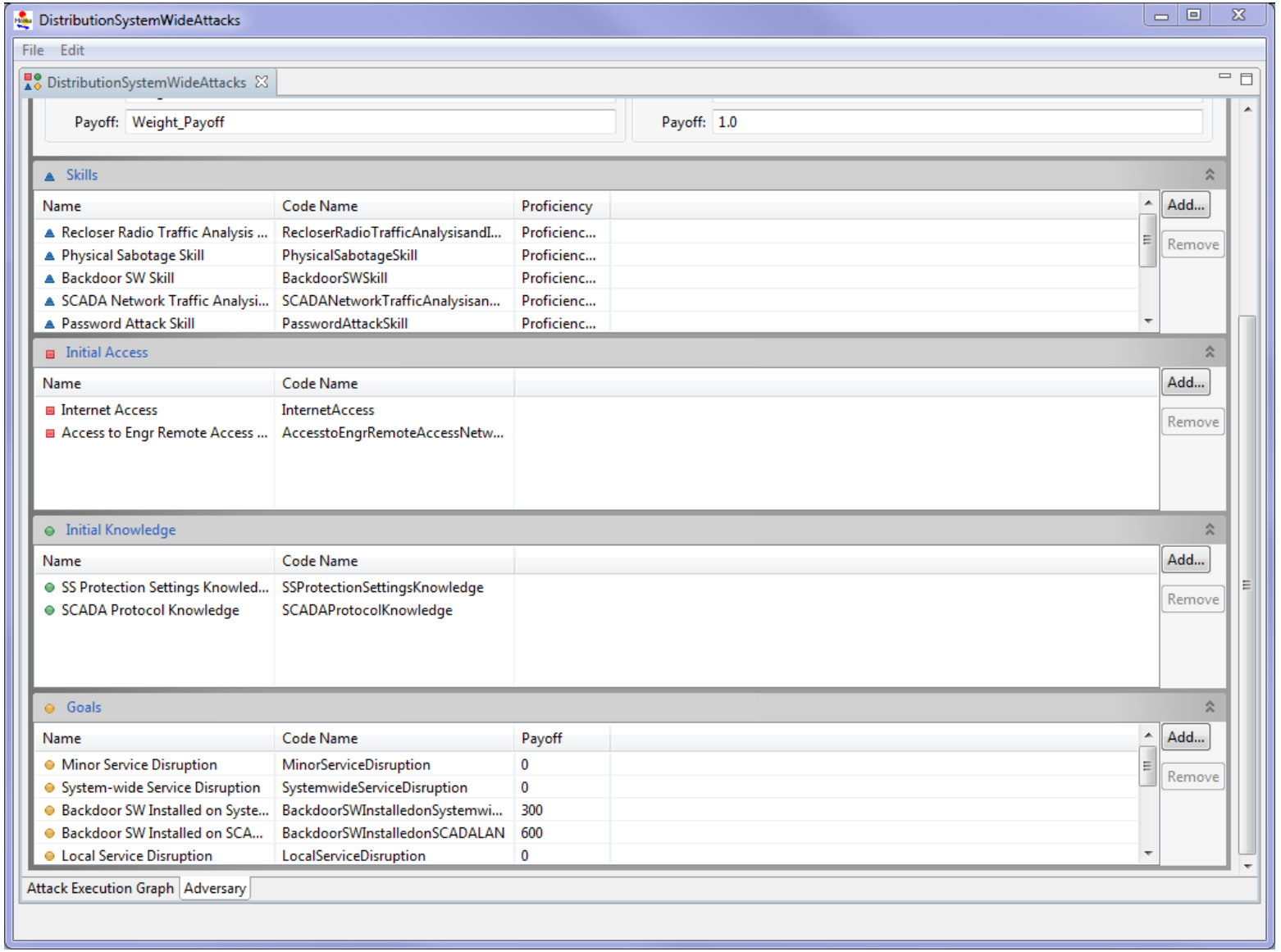
Design-Time Risk Assessment: ADVISE



Attack Execution Graph Editor

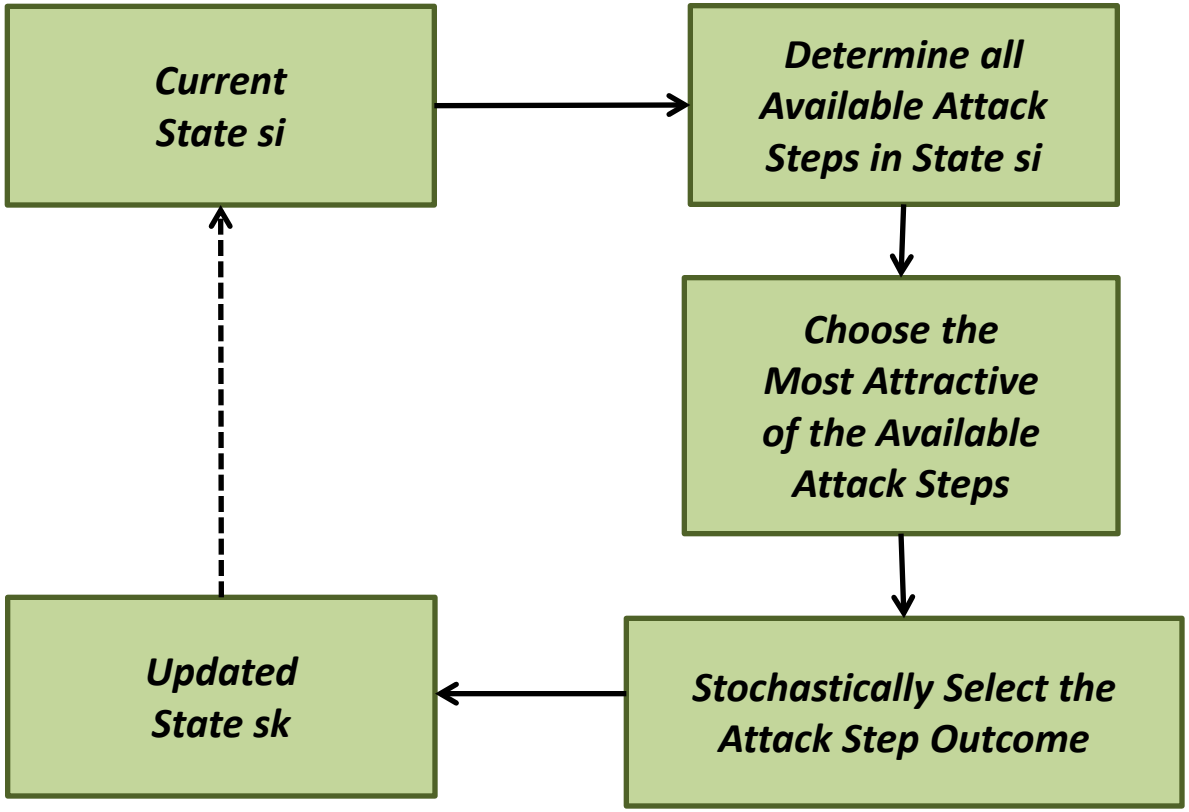


Adversary Editor

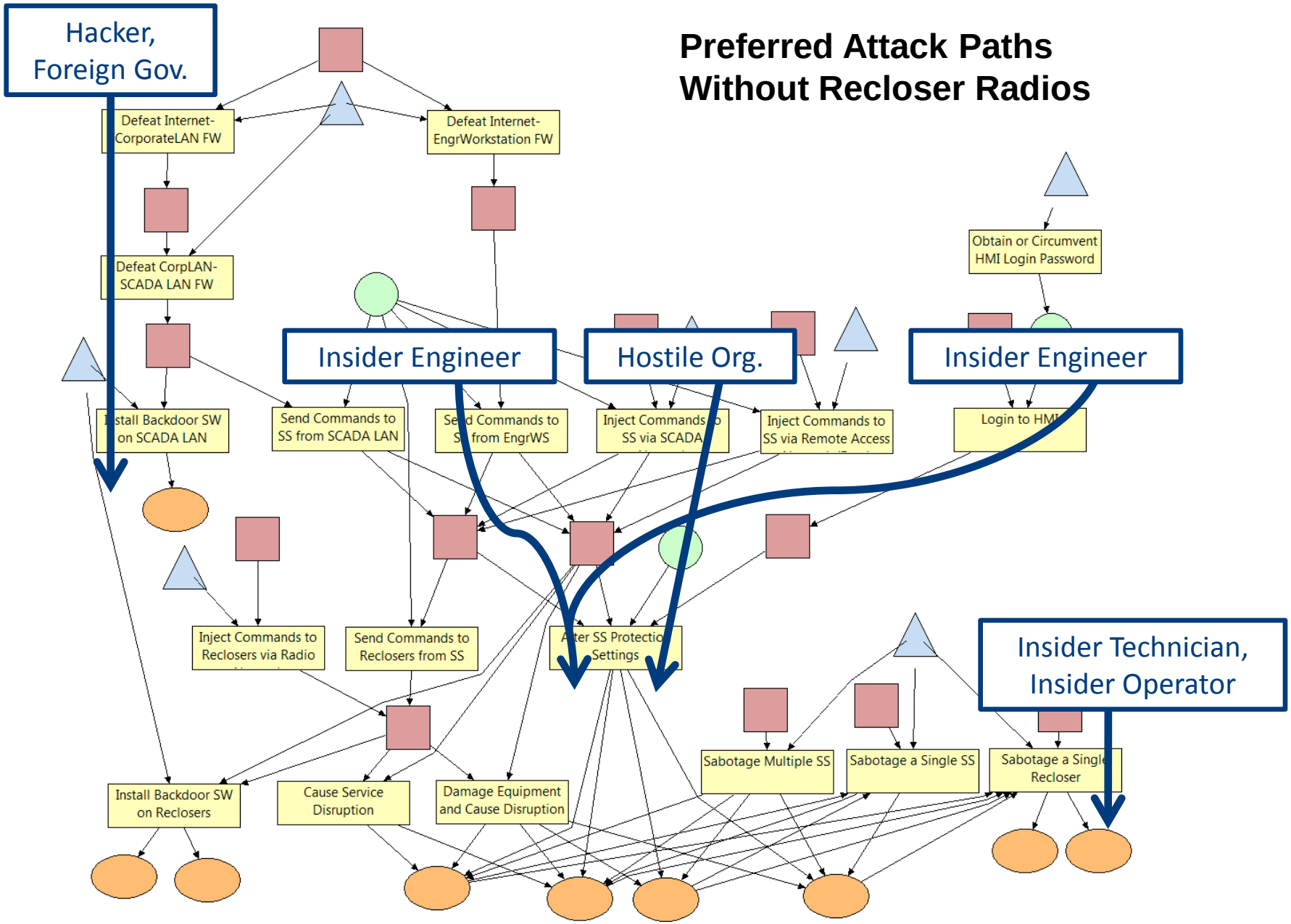


Model Execution: the Attack Decision Cycle

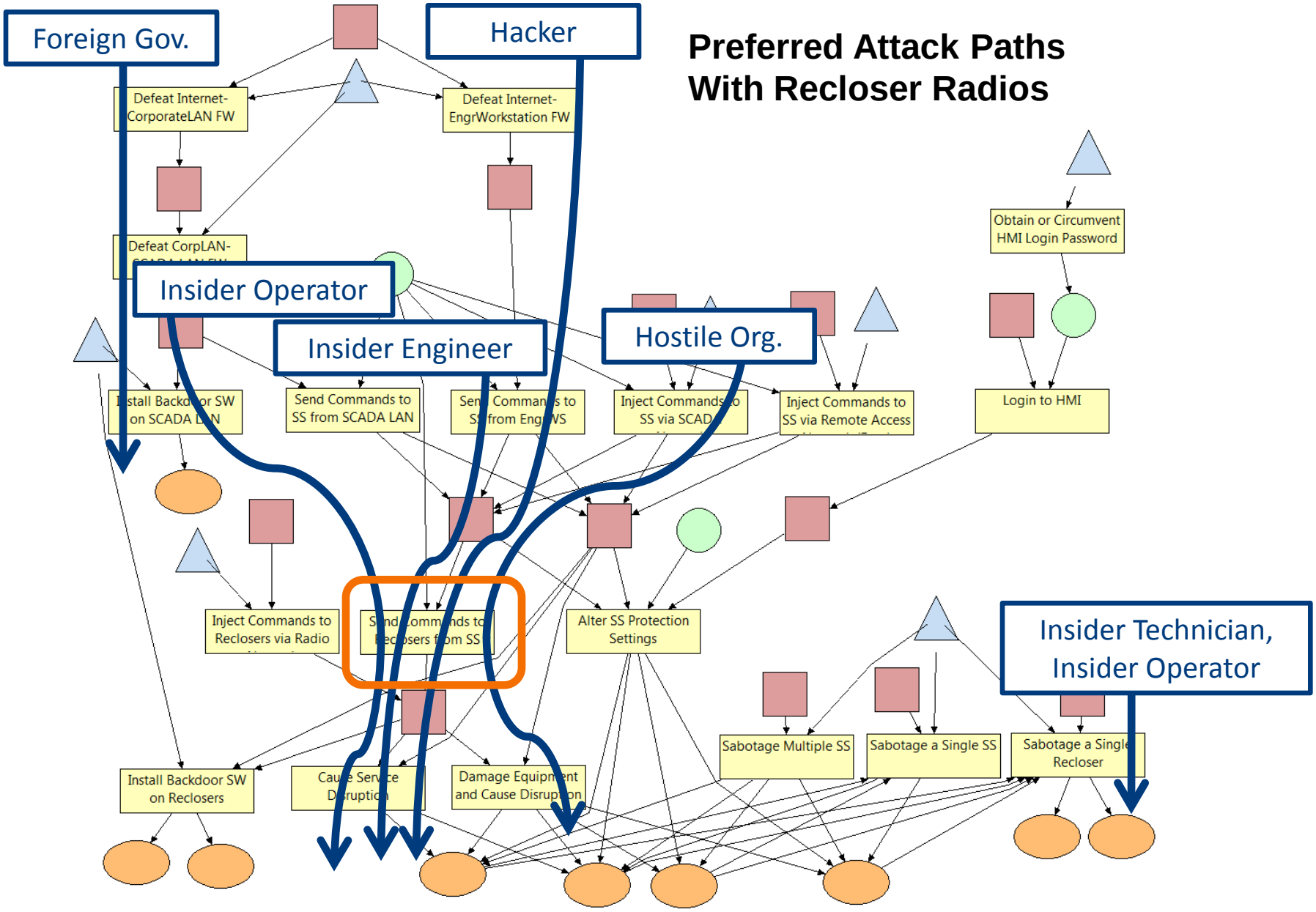
- The adversary selects the most attractive available attack step based on his attack preferences.
- State transitions are determined by the outcome of the attack step chosen by the adversary.



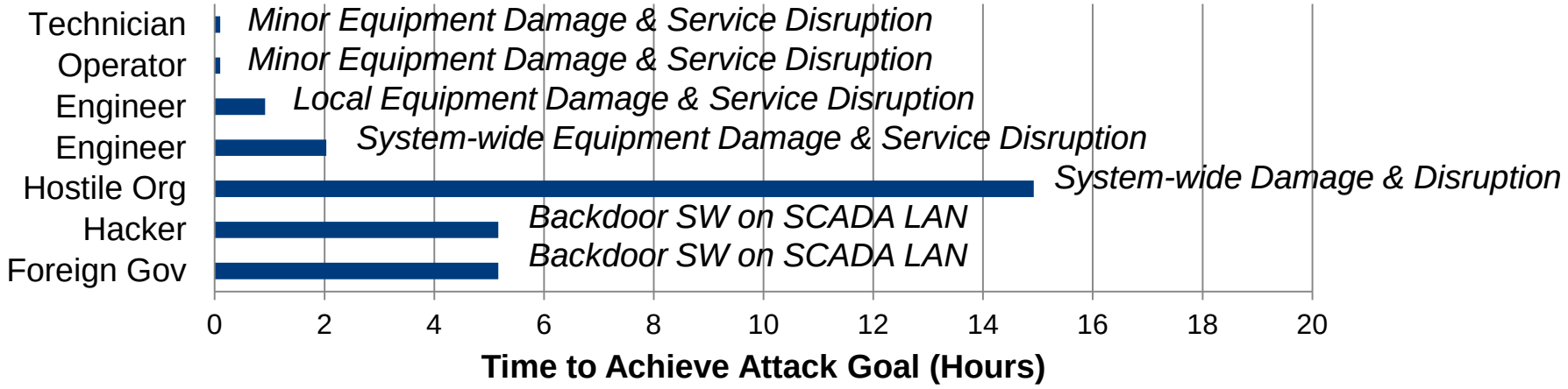
Preferred Attack Paths Without Recloser Radios



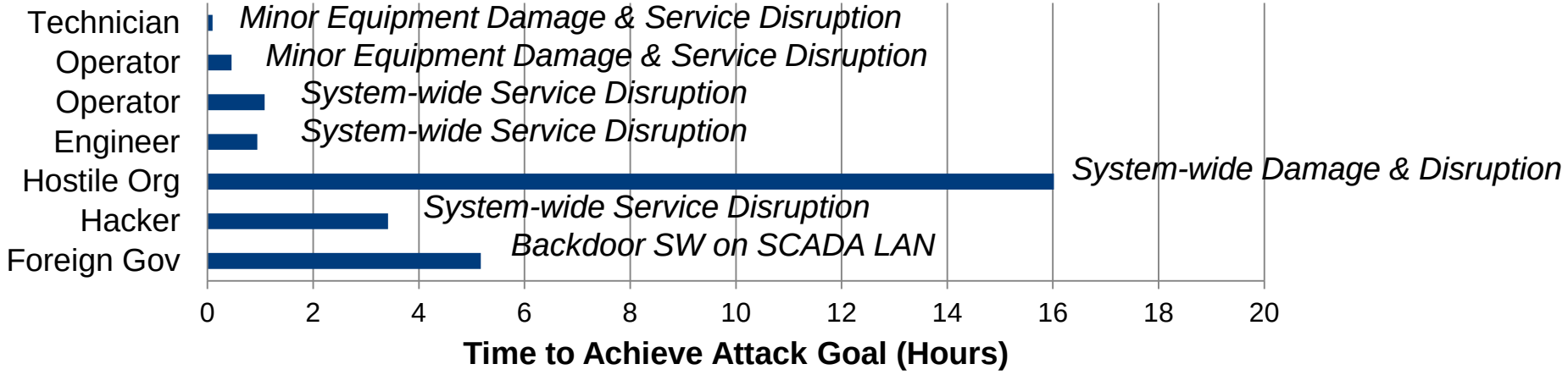
Preferred Attack Paths With Recloser Radios



Attack Speed Without Recloser Radios



Attack Speed With Recloser Radios



Final Thoughts

- Incredible opportunity for academics, rich with opportunity for algorithms and analysis
  - Can make progress by solving parts of the problem
- Must break out of the current “pierce and patch” mentality
- Solutions require thinking short term and long term at the same time
- Must deeply engage academia, industry, and government
- All parties must work closely together