

Adaptive bio-inspired resilient cyber-physical systems: R&D prospective

Presented at:

Int'l Symp on Resilient Control Systems

Cyber Awareness

August 9-11, 2011 in Boise Idaho

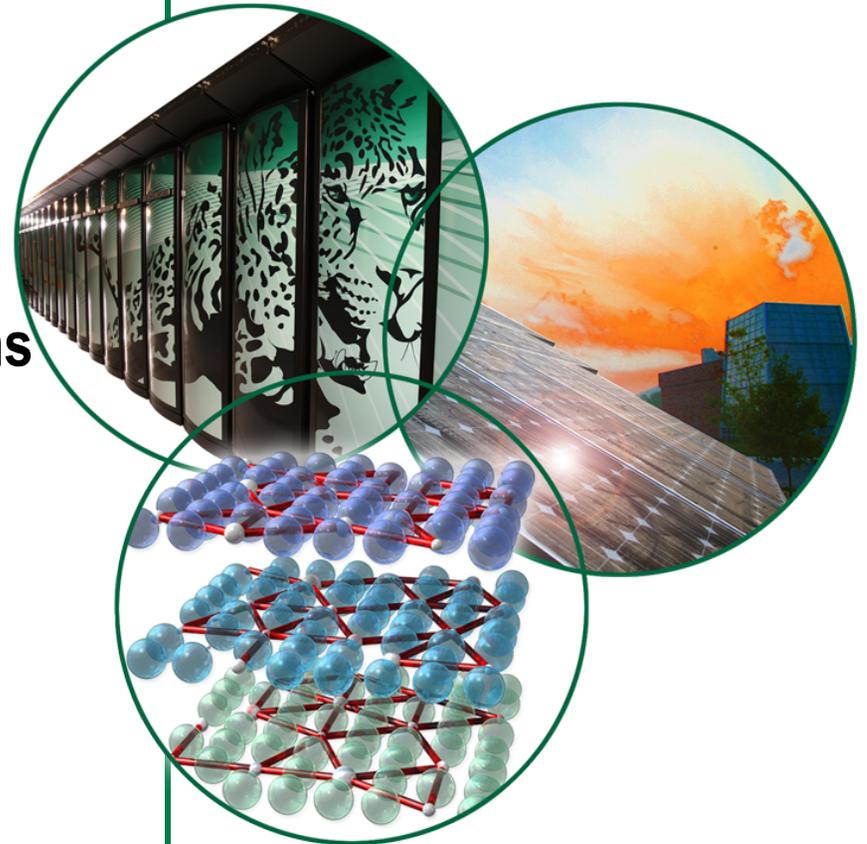
Frederick Sheldont[†], Hal Aldridge and Mike Duren

L. Hively[†], D. Dasgupta and R. Abercrombie

[†]Cyberspace Sciences and Information Intelligence Research Group



U.S. DEPARTMENT OF
ENERGY



 **OAK RIDGE NATIONAL LABORATORY**
MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY

Outline†

- **Shameless Plug: CSIRW Call For Abstracts (Deadline Sept. 2)**
- **Moving Toward Trustworthy Systems**
 - Recap of federal policy leadership and recent developments
 - Coordinated effort to inspire Game-Changing R&D themes
- **Toward Scalable Trustworthy Computing Using the HPI Metaphor**
 - Effective cybersecurity solutions must be scalable
 - Facile composability
 - Analogies of immune function
 - Bio-inspired signaling in cyber defense
- **Proactive risk management in the context of cryptographic key management system (CKMS) for the smart grid (SG)**
- **Centralized Cryptographic Key Management System (CKMS)**

† Portions of this presentation were excerpted from the Federal Cybersecurity R&D Themes Kickoff Event presentations held at the IEEE Symposium on Security & Privacy and organized by NITRD (<http://www.nitrd.gov/CSThemes.aspx>), May 19, 2010 and from F. T. Sheldon and C. Vishik, “Moving Toward Trustworthy Systems: R&D Essentials” IEEE Computer, pp 31-40, Sept 2010.

Theme: Energy Infrastructure Cyber Protection (www.csiir.ornl.gov/csiirw)



CSIIRW

7th Annual Cyber Security and Information Intelligence Research Workshop
October 12 - 14, 2011

[Home](#)[Contacts](#)[Speakers](#)[Registration](#)[Publisher](#)[Sponsors](#)

Oak Ridge National Laboratory

CSIIRW sessions will be held in the ORNL conference center

[Oak Ridge National Laboratory](#)[Plenary Keynote Speakers](#)[Government Cyber Leadership Panel](#)[Roundtable Dinner Banquet](#)[Sandia National Laboratory](#)

Important deadlines

September 2
Extended 4-page abstract submission deadline

September 12
Author notification

September 30
Early registration (\$180)
Final draft & copy right released

October 7
Slides up-loaded to Share-point

December 7
ACM Proceedings published

Topics Include

Security assurance/interoperability for Energy Delivery Systems (EDS)

Scalable/trusted control (cyber-physical) systems security

Visual Analytics for Cyber Security

Next generation control systems

Submissions

[Guidelines](#)[Submit Abstract](#)[Sharepoint Registration](#)[Submit Final Abstract and slides](#)

Important Links

[Keynotes and Invited Speakers](#)[Last Year's Final Program](#)[Last Year's Keynote Biographies](#)[Proceedings Archive](#)[Travel/Hotel](#)[Subscribe to Notifications](#)

Research Opportunities

[CSIIR Group Site](#)[ORNL Job Site](#)[HERE Program](#)[Staff Directory](#)

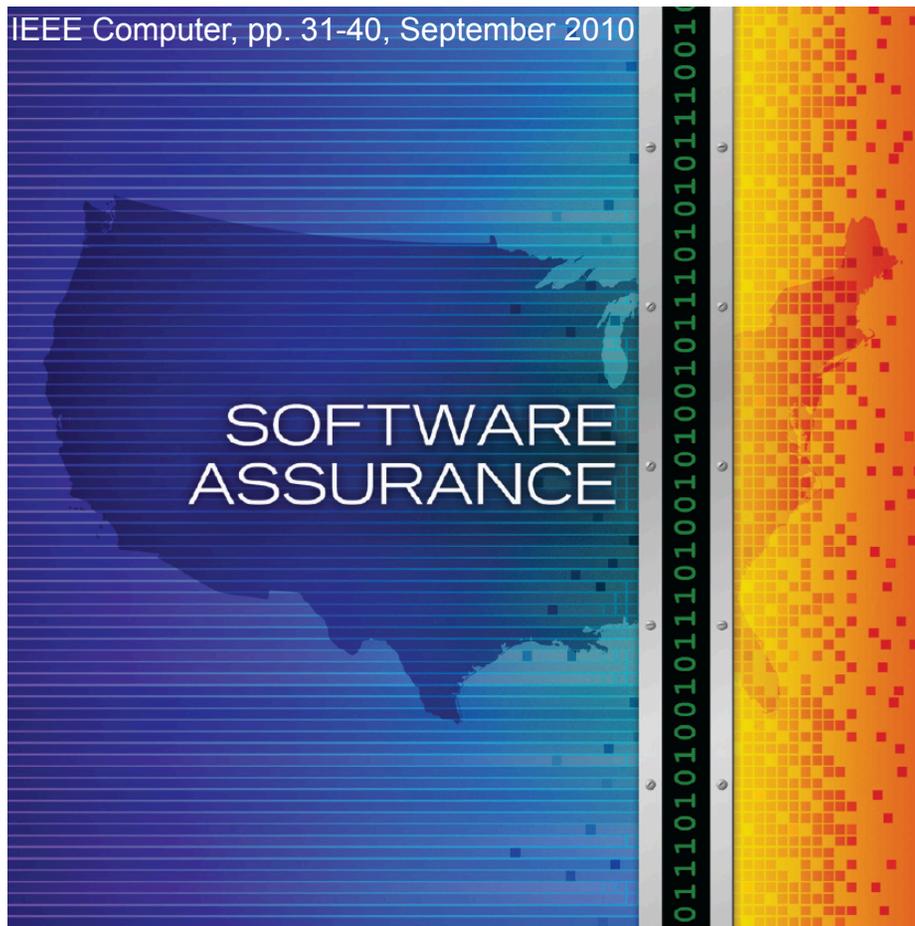
Keynotes

The Annual CSIIR Workshop will be held at Oak Ridge National Laboratory and published by [ACM](#). This year's event is being co-organized with [LLNL](#), [PNNL](#), [Sandia](#) and [NNSA](#). The aim of this workshop is to introduce and discuss novel theoretical and empirical research focused on (the many) different aspects of cyber security and information intelligence....

[read more](#)

Theme: Energy Infrastructure Cyber Protection

The energy industry is embarking upon an infrastructure transformation that will



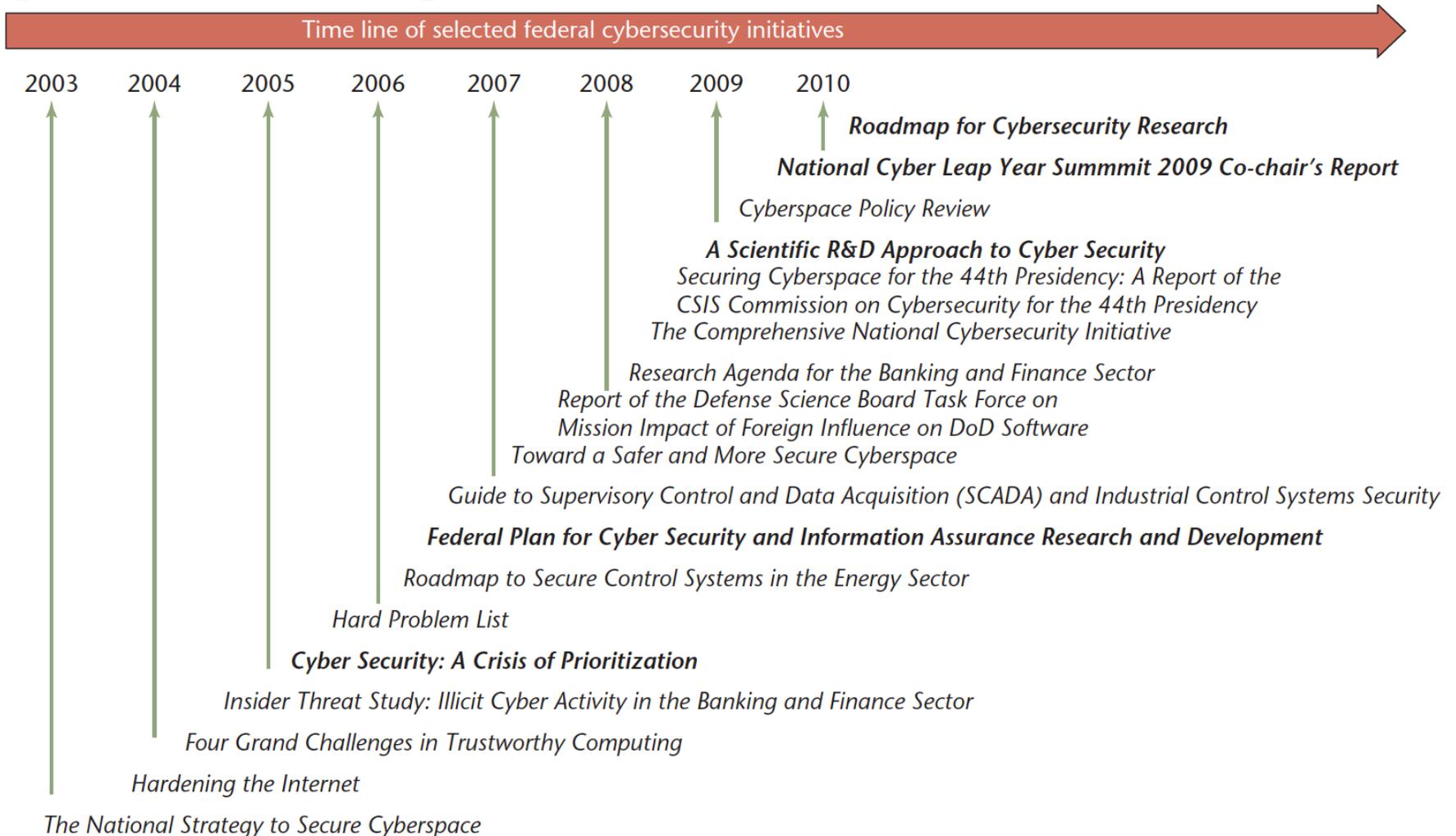
MOVING TOWARD TRUSTWORTHY SYSTEMS: R&D ESSENTIALS

Frederick T. Sheldon, *Oak Ridge National Laboratory*

Claire Vishik, *Intel*

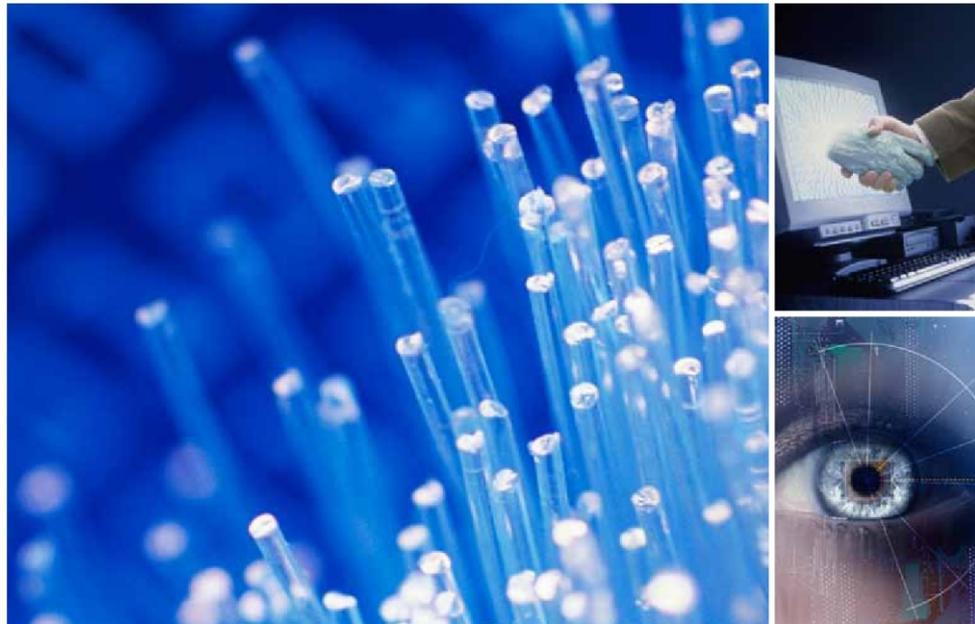
In February 2010, former ODNI Director Dennis Blair advised Congress “malicious cyber-activity is growing at an unprecedented rate,” and stated that the country’s efforts to defend against cyber-attacks “are not strong enough.” The Pentagon has since experienced an “explosion” of computer attacks, currently averaging about 5,000 per day. Indeed, with cyber-threats steadily increasing in sophistication and frequency, the need for software assurance to ensure scalable trust at all levels—personal, private, public, and national—is crucial.

Timeline of selected Federal Cybersecurity Initiatives





A Roadmap for Cybersecurity Research



DSEC Research Council
)



HARD PROBLEM LIST

November 2005

CRA → Four Grand Challenges

- **Challenge 1:** Eliminate Epidemic Attacks by 2014
- **Challenge 2:** Enable Trusted Systems for Important Societal Applications
- **Challenge 3:** Develop Accurate Risk Analysis for Cybersecurity
- **Challenge 4:** Secure the Ubiquitous Computing Environments of the Future

DOE Roadmap to Secure Control Systems for the Energy Sector

- **VISION:** In 10 years, ... control systems for critical applications will be designed, installed, operated and maintained to survive an intentional cyber assault with no loss of critical function.

Coordinated Effort to Inspire Game-Changing R&D Themes

- It's about **trustworthiness** of digital infrastructure
 - Security, reliability, resiliency, privacy, usability
 - How can we:
 - Enable risk-aware safe operations in compromised environments
 - Minimize critical system risk while increasing adversaries' costs and exposure
 - Support informed trust decisions, necessitating flexible security strategies, and allow for effective risk/benefit analyses and implementations
- **Strong commitment to focus on game-changing technologies for coordinated cybersecurity R&D agenda**
 - Comprehensive National Cybersecurity Initiative, Cyberspace Policy Review: <http://www.whitehouse.gov/cybersecurity>
 - Aneesh Chopra, US Chief Technology Officer
 - Howard Schmidt, President's Cybersecurity Coordinator
 - NITRD Senior Steering Group, Interagency WGs (e.g., CSIA R&D SSG, ...)

NCLY Summit Solution Themes

- (1) Hardware-enabled trust *knowing when you've been had* {P1|2|3|4|5, N1-5|7|9|10, D1-3|5-7|9-11}
- (2) Cyber economics *crime and fraud do not pay* {P3|8|9|10, N1-3|6|8|11, D1|2|4|10|11}
- (3) Moving-target defense *attacks work once if at all* {P1|4|7|9, N4-6|8-10, D1|2|5|7|9}
- (4) Digital provenance *basing trust decisions on verified assertions* {P1|2|5|7, N1|3|4|7|11, D3|4|6|7-11}
- (5) Nature-inspired cyber health *move from forensics to real-time diagnosis* {P3|4|6-10, N1-3|6-11, D1|4-9}

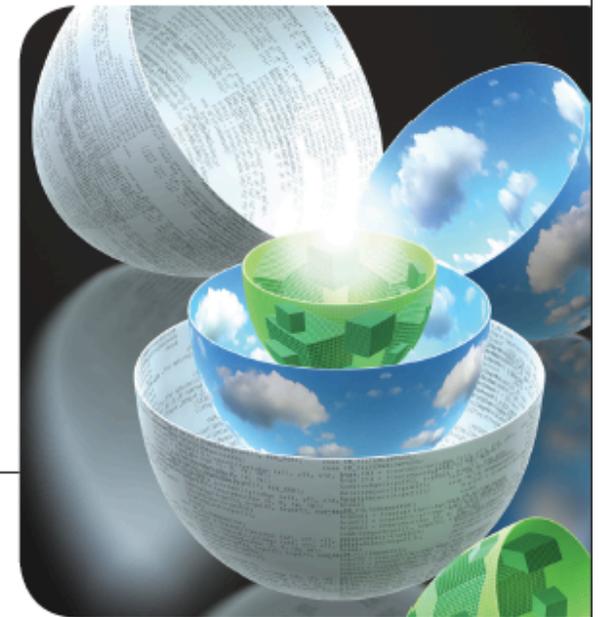
Cross-cutting themes among US federal cyber security priorities[†]

Selected federal problems characterization efforts			Solution themes(†)
PITAC 2005 cybersecurity priorities	NSTC 2006—Some of the top cybersecurity/IA R&D priorities	DHS 2009 Roadmap for Cybersecurity Research (Hard Problem List v. 2)	NITRD 2009 National Cyber Leap Year Summit
P1 Authentication (3)	N1 Authentication, authorization, trust management, and access control and privilege management (4)	D1 Scalable trustworthy systems (including system architecture and requisite development methodology) (4)	(1) Hardware-enabled trust {P1 2 3 4 5, N1-5 7 9 10, D1-3 5-7 9-11}
P2 Secure software engineering (2)	N2 Large-scale cyber situational awareness and automated attack detection, warning, and response (3)	D2 Enterprise-level security metrics (including measures of overall system trustworthiness) (3)	
P3 Holistic system security (2)	N3 Insider threat detection and mitigation and forensics, traceback, and attribution (4)	D3 System evaluation life cycle (including approaches for sufficient assurance) (2)	(2) Cybereconomics {P3 8 9 10, N1-3 6 8 11, D1 2 4 10 11}
P4 Monitoring and detection (3)	N4 Secure DNS and routing protocols and process control systems (3)	D4 Combating insider threat (3)	
P5 Secure fundamental protocols (2)	N5 Domain-specific security (such as wireless and RFID) (2)	D5 Combating malware and botnets (3)	
P6 Mitigation and recovery (1)	N6 Detection of vulnerabilities and malicious code; metrics and software testing and assessment (3)	D6 Global-scale identity management (3)	(3) Moving-target defense {P1 4 7 9, N4-6 8-10, D1 2 5 7 9}
P7 Cyberforensics (3)	N7 Secure OS and software engineering and information provenance (3)	D7 Survivability of time-critical systems (4)	
P8 Modeling and testbeds (3)	N8 Cybersecurity and IA R&D testbeds and IT systems, and Internet modeling, simulation, visualization (3)	D8 Situational understanding and attack attribution (2)	(4) Digital provenance {P1 2 5 7, N1 3 4 7 11, D3 4 6 7-11}
P9 Metrics, benchmarks, best practices (3)	N9 Trusted computing base architectures and composable, scalable, secure systems (3)	D9 Provenance (relating to information, systems, and hardware) (4)	
P10 Nontechnology issues (2)	N10 Inherently secure, high-assurance, and provably secure systems and architectures (3)	D10 Privacy-aware security (3)	
	N11 Trust in the Internet and privacy (3)	D11 Usable security (3)	(5) Nature-inspired cyberhealth {P3 4 6-10, N1-3 6-11, D1 4-9}

[†] Progress in a solution theme area will support advances in the other problem areas listed {P1-10, N1-11, D1-11}; (#) indicates a priority (or in the case of column 3, a hard problem). Larger numbers indicate the priority's stronger cross-cutting nature.

Toward Scalable Trustworthy Computing Using the Human-Physiology-Immunity Metaphor

Achieving scalable trustworthy computing is possible through real-time knowledge-based decisions about cybertrust. This vision is based on the human-physiology-immunity metaphor and the human brain's ability to extract knowledge from data and information.



LEE HIVELY
AND FREDERICK
SHELDON
*Oak Ridge
National
Laboratory*

ANNA CINZIA
SQUICCIARINI
*Pennsylvania
State
University*

Recent US federal policy documents have emphasized the importance of cybersecurity for society's welfare (see Figure 1). For example, *Cyber Security: A Crisis of Prioritization* described 10 technologies needed for cybersecurity.¹ The *Federal Plan for Cyber Security and Information Assurance Research and Development* discussed 49 cybersecurity technical topics in eight major R&D areas with corresponding funding priorities.² The Department of Homeland Security's *Roadmap for Cybersecurity Research* listed 11 "hard problems" (eight from the 2005 Infosec Research Council Hard Problem List).³ The *National Cyber Leap Year Summit Co-chairs*

in areas such as constructive system design, meticulous use of best practices, error-correcting code to overcome unreliable communications and storage, and encryption to protect insecure communications' integrity and confidentiality. Such techniques are incomplete if they rely on the trustworthiness of developers, users, and administrators. The challenges are, then, to develop

- a sound basis for composability that scales to large, complex, trustworthy systems;

Continuous Evolution of Attacks

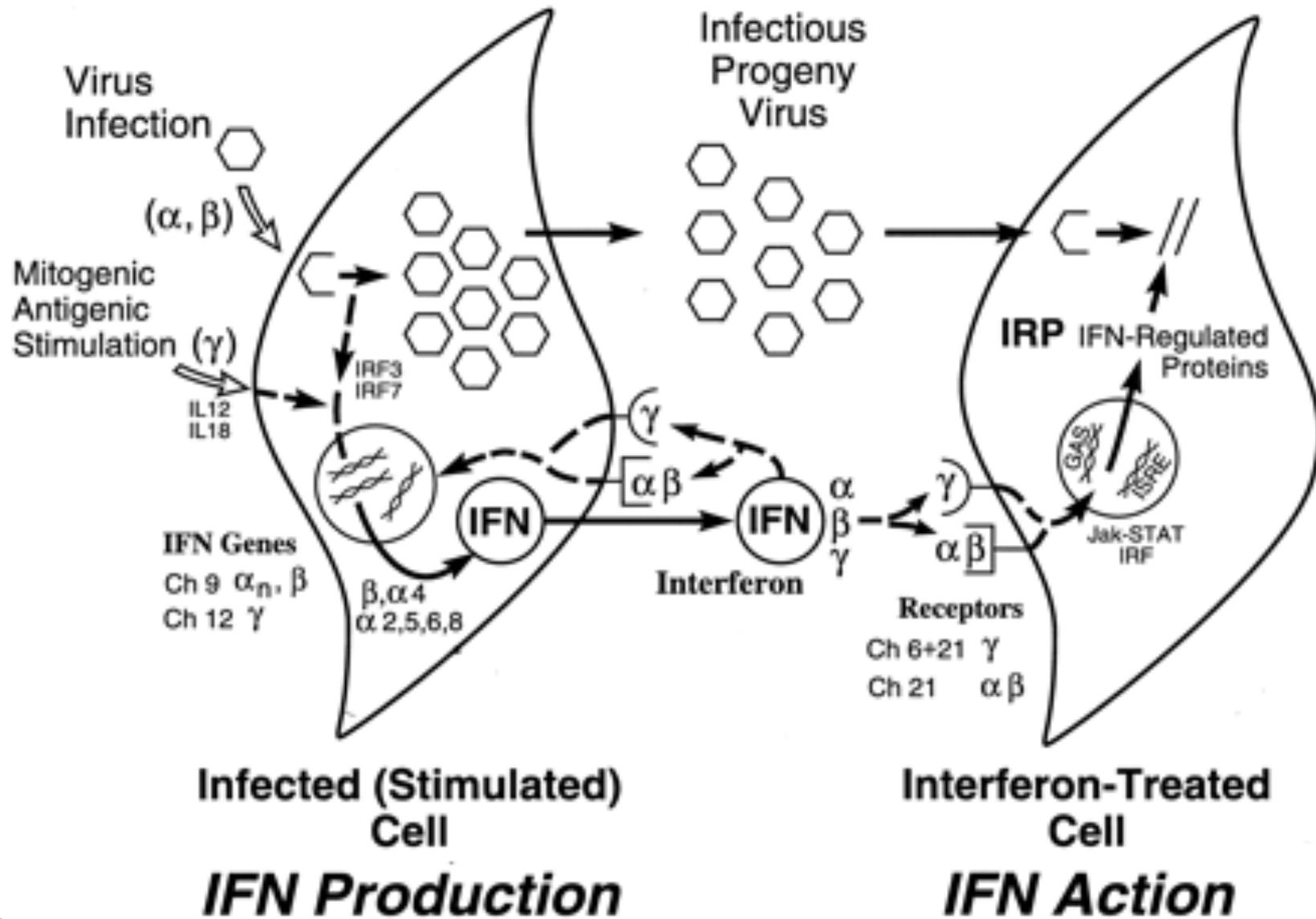
- **Solutions for known threats do not address new attacks**

- Current security-driven assessments lack specific guidelines for evaluation of emerging threats

- **Reduce attacker's advantages**

- Thwarting malicious cyber activity through signaling, implementation of diversity, and immunogenic detection as hardware-software solutions.
- Rapidly regenerating (self-healing) survivable capabilities in mission-critical systems after a sophisticated attack.
- Evolving immunity to attacks through evolutionary computing to create new deceptions (gaming strategies) as new threats emerge.
- Self-learning while monitoring insider activity and developing profiles for appropriate and legitimate behavior (modeling).
- Assimilating the many disparate security tools using both feed-forward and feedback signaling mechanisms in a cyber defense system to help ensure tolerance and identify attacks while minimizing false alarms.

Interferon (*IFN*) Signaling Mechanisms



Scalable Trustworthy Computing

- To be effective, cybersecurity solutions must support scalability.
- To enhance scalability, high-assurance systems should consist of components and subsystems, in a system architecture that inherently supports facile composability[†].
- Each component and subsystem should itself be suitably trustworthy, down to the most basic level, thus avoiding development of new methodologies at each successively larger scale.
- Scalability should enhance trustworthiness in areas such as
 - constructive system design,
 - meticulous use of best practices,
 - error-correcting code to overcome unreliable communications and storage, and
 - encryption to protect insecure communications' integrity and confidentiality.

[†]Composability is the ability to create systems and applications with predictably satisfactory behavior

Proactive risk management in the context of cryptographic key management system for the smart grid

Challenge

- **Good Security Metrics are required**
- **Size and Complexity of Smart Grid with respect to key management**
 - Generating millions of keys securely is a challenging problem both operationally and technically

Solution

- **Team (ORNL as part of Sypris team, which includes Purdue) are testing and evaluating**
 - the security and usability of the proposed distribution methodology and
 - suggesting changes and mitigating techniques that can address the identified issues.
- **ORNL and NJIT are using its patent pending Cyber Security Econometrics Model to address mitigating risks which employees Prof. Ali Mili's Mean Failure Cost Algorithm**

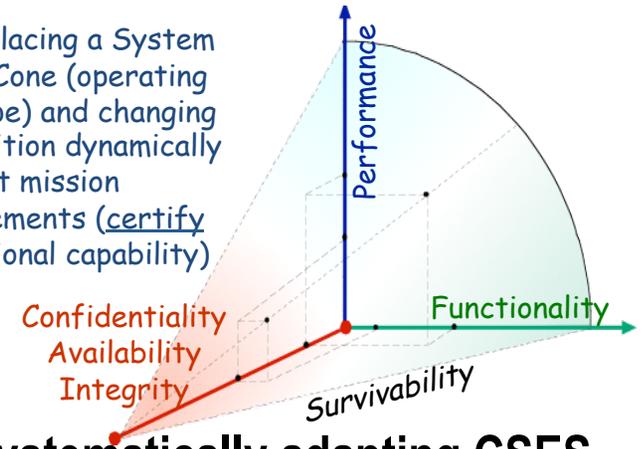
Cyber Security Econometrics System (CSES)

Framework for measurement and evaluation to:

- Choose between alternative security architectures/protocols (e.g., CKM)
- Improve security (including reliability and safety) during both design/development and operational phases.
- Estimate Mean Failure Cost
 $MFC = SM \cdot DM \cdot IM \cdot PV$ as a basis for determining:
 - Mitigation costs matrix and risk assessment
 - Return on investment (ROI) justification
 - Failure Modes Effects and Criticality Analysis (FMECA)

Provides a comprehensive basis for choosing courses of action that have the highest risk reduction return on investment

Goal: Placing a System in the Cone (operating envelope) and changing its position dynamically to meet mission requirements (certify operational capability)

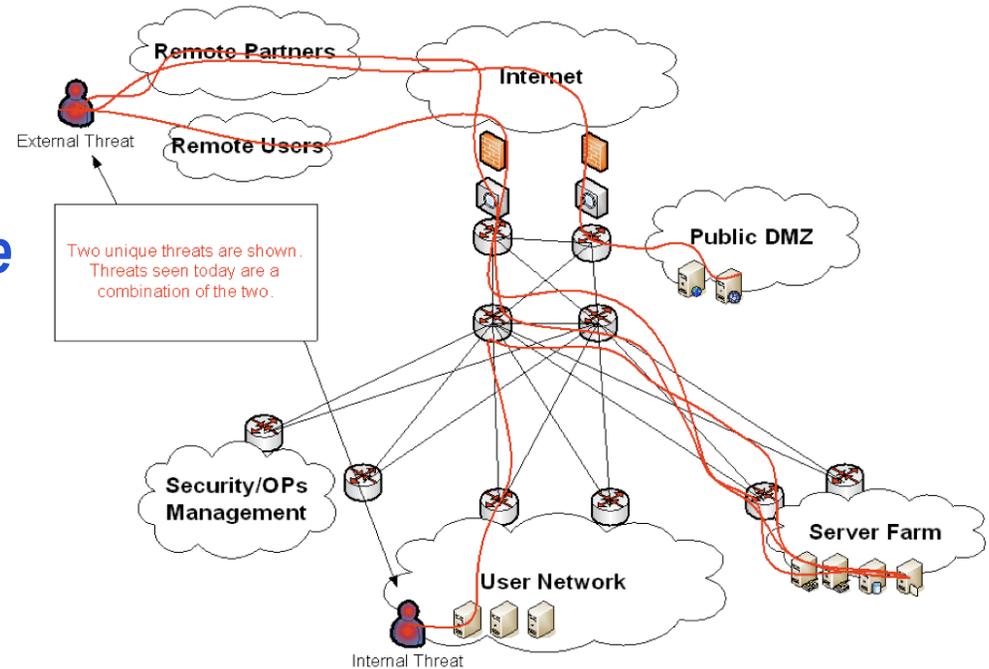


- Approach to systematically adapting CSES for AMI & Synchro-phasors
 - [SM] Identify stakeholders and their mission requirements and failure cost
 - [DM] Identify and cross-tabulate grid components that satisfy mission requirements
 - [IM] Develop structural model (using Mobius / ADVISE†) to identify and assess the likelihood of a particular threat leads to failure of a component
 - [PV] probability of emergence of the identified threats
 - [MCM] Estimate of the probabilities of service delivery as a function of the effort invested in enhancing the security of the individual components

†Mobius 2.3 is an extensible dependability, security, and performance modeling environment for large-scale discrete-event systems. It provides multiple model formalisms and solution techniques, facilitating the representation of each part of a system in the formalism that is most appropriate for it, and the application of the solution method or methods best-suited to estimating the system's behavior.

CSE Rationale

- Consistent with the spirit of *Value Based Software Engineering* and comprehends the different organizational mission needs for all stakeholders.
 - For example, CSE identifies information assurance controls and mitigation costs as an investment toward assuring mission success, including
 - Essential activities such as real-time threat analysis and
 - Fed by knowledge discovery tools and capabilities within the threat and vulnerability space.
- Framework enables us to rapidly develop new metrics that offer a bottom line understanding of the costs and benefits of alternative approaches to securing cyberspace assets.



Summary of Calculation of MFC

$$Y_i = \sum_{i \leq j \leq m} X^j \times A_i^j, 1 \leq i \leq n$$

Y: vector of size n
 A: n×m matrix
 X: vector of size m

$$Y = A \circ X$$

$$MFC(S_i) = \sum_{R_j} FC_{i,j} \times P(R_j)$$

ST: Stakes Matrix
 PR: vector of requirement failure probabilities

$$MFC = ST \circ PR$$

$$P(R_i) = \sum_{j=1}^{k+1} \pi(R_i|E_j) \times \pi(E_j)$$

DP: Dependency Matrix
 PE: vector of component failure probabilities

$$PR = DP \circ PE$$

$$\pi(E_i) = \sum_{j=1}^{h+1} \pi(E_i|V_j) \times \pi(V_j)$$

IM: Impact Matrix
 PV: vector of threat emergence probabilities

$$PE = IM \circ PT$$

$$MFC = ST \circ DP \circ IM \circ PT$$

Mitigation Costs (MC) Matrix

		Components						
		C1	C2	C3	C4	C5		
Requirement Fulfilled or Service Delivered	S1						Verification Cost by Service	VS1
	S2							VS2
	S3							VS3
	S4			D_i^j				VS4
	S5							VS5
		Verification Cost by Component					$VS_i = \sum_{j=1}^n D_i^j \times VC_j.$	
		VC1	VC2	VC3	VC4	VC5		

- Each *requirement fulfilled* or *service delivered* by the system depends on the correct operation of one or more system components.
- This dependency can be quantified by the statistical correlation between the failure of the component and the failure to deliver the service or fulfill the requirement.
- If we combine this dependency with the cost of verifying each component of the system, we can maintain an estimate of the probabilities of service delivery as a function of the effort invested in enhancing the dependability of the individual components. Maintaining this information can serve two purposes:
 - Which components must be enhanced first to improve overall stakeholder satisfaction.
 - Charge verification costs according to stakeholder benefit. For any particular verification measure, we charge stakeholders according to the gains they have achieved as a result of this measure (which are quantified by the reduction in MFC).

Estimating the Probability of Threats

- Utilizing the previous defined matrices,
 - the **Stakes matrix** (ST) is filled by stakeholders according to the stakes they have in satisfying individual requirements;
 - the **Dependency matrix** (DP) is filled in by the system architect (i.e., cyber security operations and system administrators) according to how each component contributes to meet each requirement;
 - the **Impact matrix** (IM) is filled by analysts according to how each component is affected by each threat.
- The remaining question is how to fill the vector of threat emergences probabilities (PV) that represents the probability of emergence of the various threats that are under consideration?
 - This is done empirically, by simulating and/or operating the system for some length of time and estimating the number of threats that have emerged during that time and continue to be refined as the system evolves.
 - From these numbers, we infer the probability of emergence of all the threats during one hour of operation.
- This results in a vector of mean failure costs of all stakeholders as :

$$MFC = ST \circ DP \circ IM \circ PV.$$

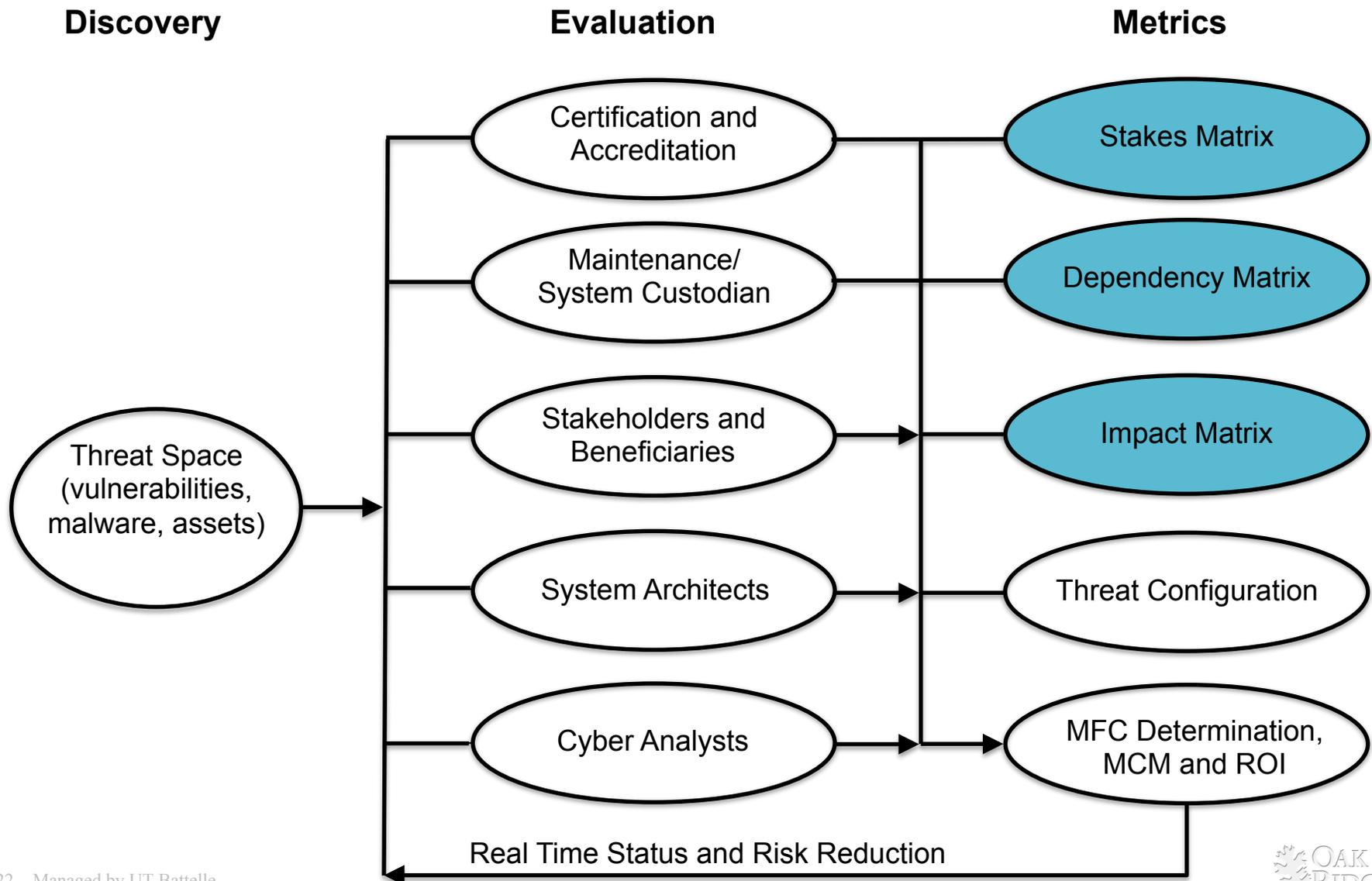
Integrating Quality Costs

- **Stakeholder standpoint: the mean failure cost (i.e., cost we expect to incur as a result from the lack of security) must be balanced against the cost of improving system security. Our mean failure cost model allows us to formulate the tradeoff of quality versus cost in terms of a return on investment equation. Specifically, a return on investment model is defined by the following parameters:**
 - An initial investment cost, say IC ,
 - An investment cycle (duration), say T ,
 - An return over the investment cycle, say $B(t)$, for $1 \leq t \leq T$, and
 - A discount rate, say d .
- Then the return on investment is given by the following formula:

$$ROI = -1 + \sum_{t=1}^T \frac{B(t)}{IC \times (1 + d)^t}.$$

- The formula of mitigation costs can be used to compute IC , estimating the benefit gained by Stakeholder S during time period t by computing the difference between the mean failure cost with the current component and the mean failure cost with a validated component.

Process of discovery, evaluation/measurement and metrics computation and generation



Centralized Cryptographic Key Management System (CKMS)

PURDUE
UNIVERSITY



EPRI | ELECTRIC POWER
RESEARCH INSTITUTE

 **OAK RIDGE NATIONAL LABORATORY**

MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY

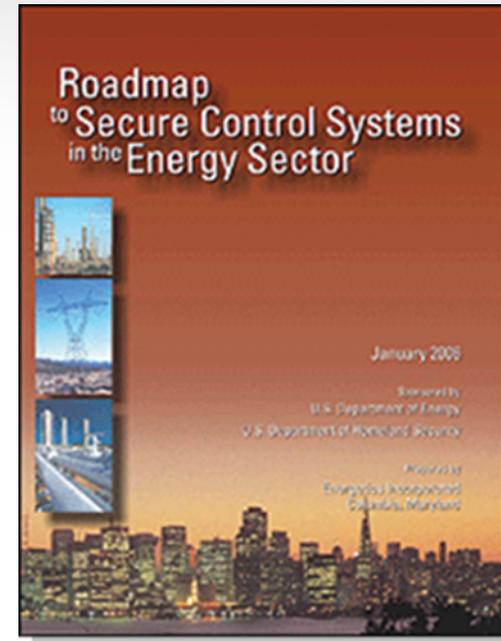
SyprisElectronics.com

INTEGRATED CUSTOMER SOLUTIONS FROM THOUGHT TO FINISH.



Smart Grid

- DOE Roadmap to Secure Control Systems
- Energy Sector's synthesis of critical control system security challenges, R&D needs, and implementation milestones



Roadmap Vision

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to **survive** an intentional cyber assault with no loss of critical function.

Project Summary

- Develop Centralized Cryptographic Key Management Solutions for Smart Grid
- Leverage cryptographic key management capabilities
 - Unique policies and architectures that mimic those in government DoD systems
 - Combined Symmetric and Asymmetric keying system
 - Scalability not matched in commercial sector products (manage over 1 million devices)
- Sypris teamed with Purdue University, Oak Ridge National Laboratory (ORNL), Electric Power Research Institute (EPRI)

Centralized Cryptographic Key Management System (CKMS)

Situation Awareness

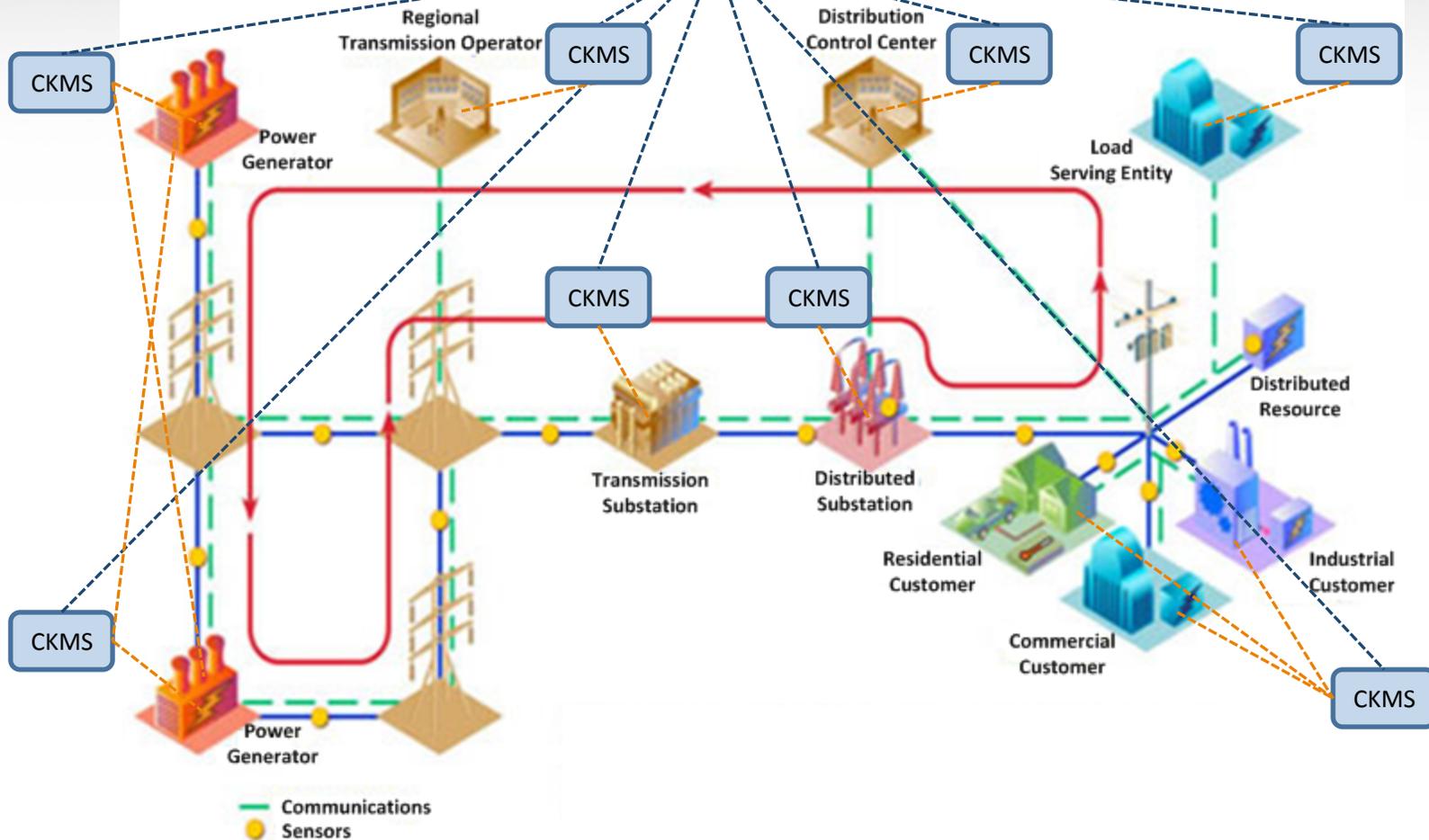
Audit and Record

Event Response

Key Distribution

Key Generation

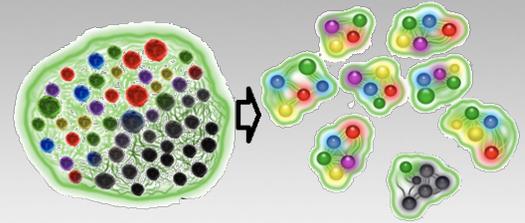
System Key Policy



Technology Investigations

- Group keying technology to lower overhead
- Modeling and simulation using Cyber Security Econometric Enterprise System to show cost trade-offs
- Physically Unclonable Functions (PUFs) to reduce cost/improve security of devices

Biological Ties



- PUFs behavior is based on a device's physical makeup
 - Unique from device to device
 - Could form the basis for determination of self
- Consider viral infection of the AMI or an Electric Vehicle fleet
 - Scenario: Mobile malware infecting millions of vehicles
 - Attack charges or prevents charging on a massive scale
 - Impacts to grid power management and to large number of individuals
 - Unresolved could cripple a community
- Isolation of attacks and recovery are critical matters

Research Challenges

- **Trustworthy systems research:**
 - Is complex and full of hard/wicked problems
 - Requires skills and input from diverse groups of stakeholders
 - Lack of good examples/models of how to engage/leverage and fuse all aspects that *work well* together
- **Cyberspace Science:**
 - We must understand the rules of the game, the hard problems toward establishing science based solutions
 - Define operative trust parameters, information and tools
 - Cross-cutting from system + device architectures → economic incentives is the type of scientific problem that must be solved
 - Societal and economic components are crucial parts of the game

Plans

- **Efficient/effective methods for performing large scale modeling and simulation of CKMS Smart Grid devices**
 - Identify the security aspects of devices requiring cryptographic keys (mgmt, distribution and revocation) from the control systems perspective AMI
 - Models that address the risk exposure of candidate solutions
 - Standards guidance in the domain of AMI

Oak Ridge National Laboratory

Meeting the challenges of the 21st century

A photograph of the Oak Ridge National Laboratory building at night. The building is a large, multi-story structure with a prominent glass facade that reflects the sky. The building is illuminated from within, and the sky is a deep blue. In the foreground, there is a set of stairs leading up to the building, and a tall flagpole with an American flag. The overall scene is a professional and modern architectural shot.

Frederick Sheldon, Ph.D.
Email: SheldonFT@ornl.gov
Phone: 1 + 865 576-1339
www.csiir.ornl.gov/sheldon

www.csiir.ornl.gov/csiirw