# CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

David M. Nicol

Franklin W. Woeltge Professor of ECE, Univ. of Illinois

Director, Information Trust Institute

Principal Investigator, CREDC

# CREDC Heritage

## Beginning

NSF with support of DOE and DHS

Trustworthy Cyber Infrastructure for Power

**TCIP: $7.5M**

2004

## Transition to DOE & DHS

DOE Office of Electricity Delivery and Energy Reliability
DHS S&T, Cyber-Security Division

Trustworthy Cyber Infrastructure for the Power Grid

**TCIPG: $18.8M**

2009

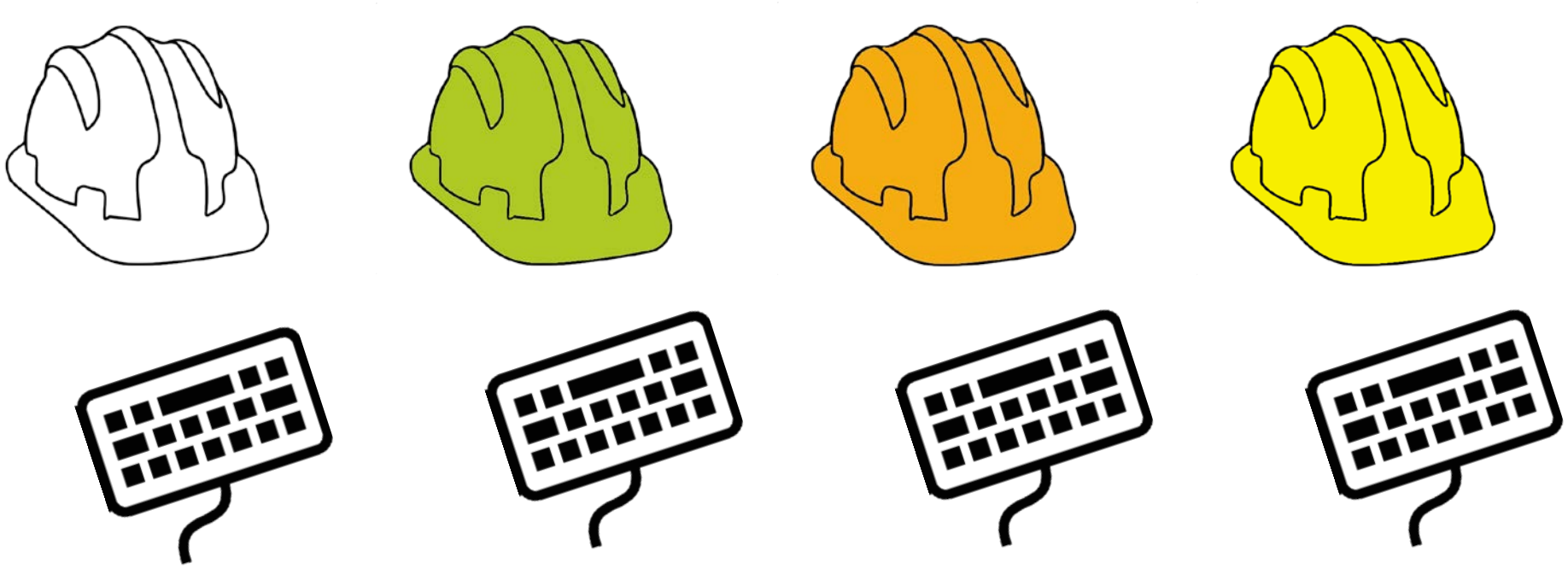
Cyber Resilient Energy Delivery Consortium

**CREDC: $28M**

2015

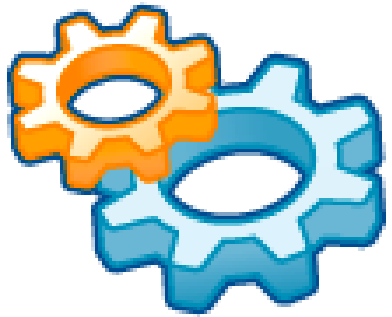
# Principal goal

Identify and perform cutting edge research and development that leads to **tools and technology which are actually used** to increase cyber-resiliency of energy delivery systems



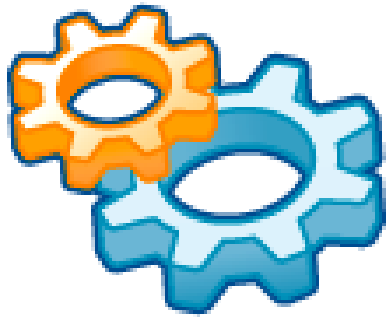
# How to get there

- Identify impediments and find highest impact *adoptable* solutions



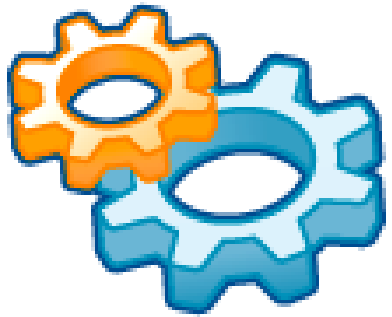
# How to get there

- Identify impediments and find highest impact *adoptable* solutions
- Develop, validate, verify high impact solutions, with industry



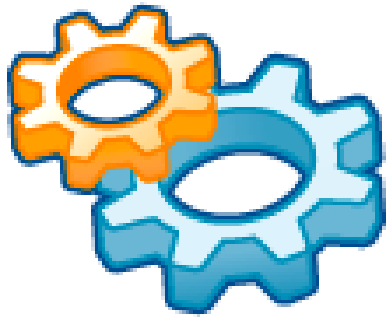
# How to get there

- Identify impediments and find highest impact *adoptable* solutions
- Develop, validate, verify high impact solutions, with industry
- Make solutions available



# How to get there

- Identify impediments and find highest impact *adoptable* solutions
- Develop, validate, verify high impact solutions, with industry
- Make solutions available
- Enhance industry awareness of new solutions




# CREDC Research Areas

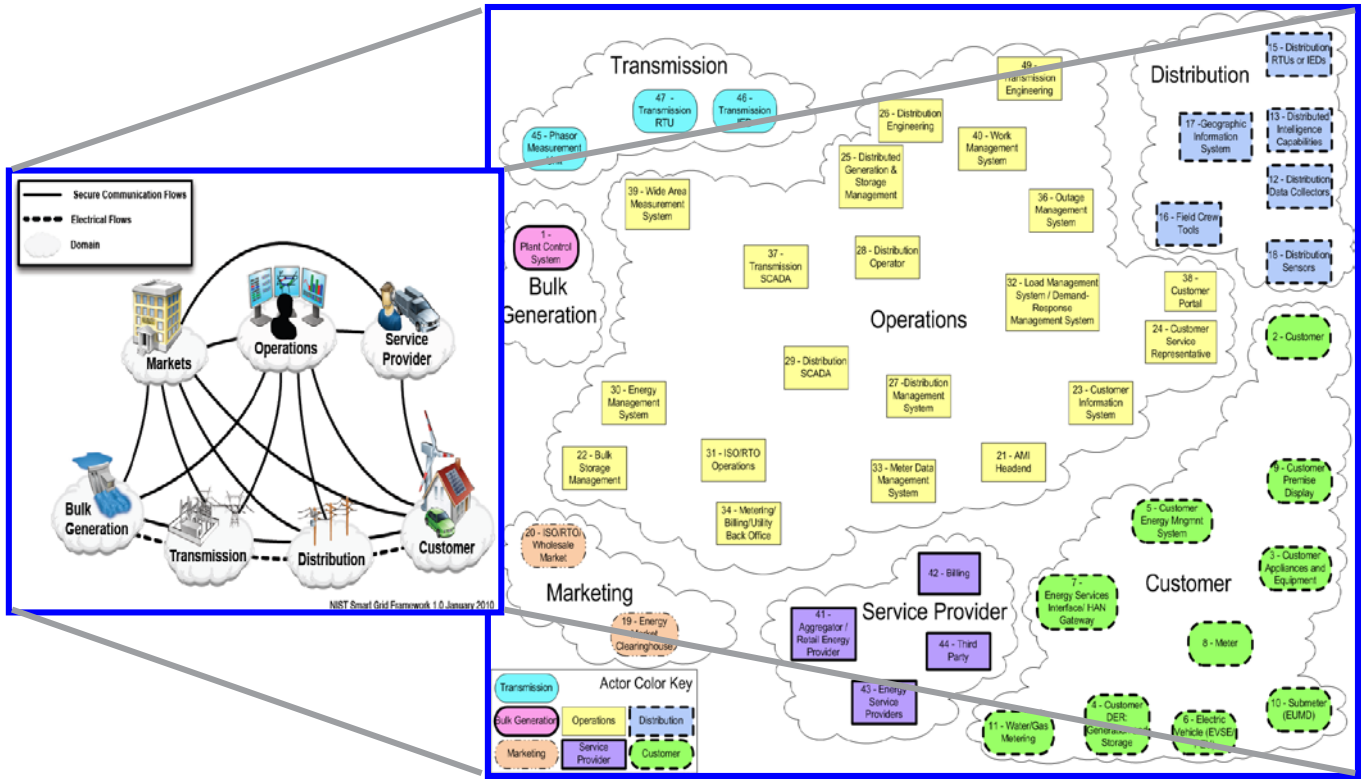
- Cyber-Protection Technology
- Cyber Monitoring, Metrics, and Evaluation
- Risk Assessment of EDS Technology and Systems
- Data Analytics for Cyber Event Detection, Management, Recovery
- Resilient EDS Architectures and Networks
- Validation and Verification

# Examples of Industrial Engagement

- Riverside Public Utilities is providing full access to streaming μPMU measurements to ASU
  - Supports research in anomaly detection
- Dartmouth & UIUC working to augment work of Automatak in CES21 program
  - Lightweight authentication / crypto for remote substations
- Siemens supports Rutgers development of security tools for PLCs
- IBM supported UIUC internship and then RA on predictive analytics for wind generation
- ODU collaborative agreement with ReliabilityFirst
  - Developing metrics to evaluate cyber-resiliency of bulk power systems

# Examples of Available CREDC Technology

- NISTIR 7628 Logical Reference Model Visualization Tool
  - Aid in understanding NIST guidelines for Smart Grid OT security
- Licensing through Kaedago



# Examples of Available CREDC Technology

- Compact Rapid Authentication (SCRA) algorithm
  - Fast signature generation and checking for broadcast C&C messages in real-time systems
  - Open source implementation available now
  - With small effort can be ported in various embedded devices

| | *RA* | PKC | | OTS | | *Online/Offline [25]* | *TESLA* | *Symmetric* (pairwise) |
|---|---|---|---|---|---|---|---|---|
| | | RSA/ECDSA | Amortized | HORS | TV-HORS | | | |
| *1. Practical for Time-Critical Applications* | Yes | No | No | Yes | Yes | No | No | Yes |
| *2. Scalability for Large and Distributed Systems* | High | High | High | Low | Moderate | High | High | Very Low |
| *3. Free from Public Key Re-Distribution Problem* | Yes | Yes | Yes | No | Partial | Yes | Yes | Yes |
| *4. Free from Synchronization Need* | Yes | Yes | No | Yes | No | Yes | No | Yes |
| *5. Immediate Ver. (no buffering/delayed disclosure)* | Yes | Yes | No | Yes | Yes | Yes | No | Yes |
| *6. Free from Time-Bounded Security* | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| *7. Non-repudiation* | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| *8. Packet Loss Tolerance* | Full | Full | Partial | Full | Partial | Full | Partial | Full |
| *9. Real-Time (end-to-end) Computational Efficiency* | High | Very Low | Low | High | Moderate | Very Low | High | High |
| *10. Communication Efficiency (tag size)* | High | High | High | Low | High | Low | High | Low |
| *11. Verifier Storage Efficiency* | High | High | High | Low | Moderate | High | High | High |
| *12. Signer Storage Efficiency* | Low | Varies | Varies | Low | Moderate | Moderate | High | Moderate |

Properties relative to other methods

# Examples of Available CREDC Technology

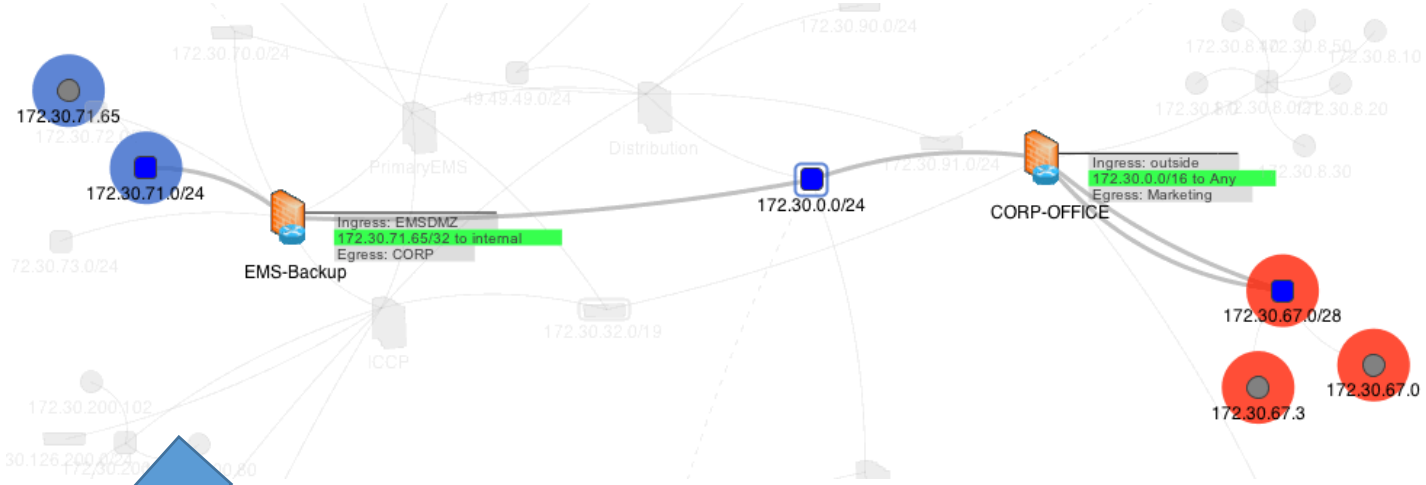
From testbed V&V

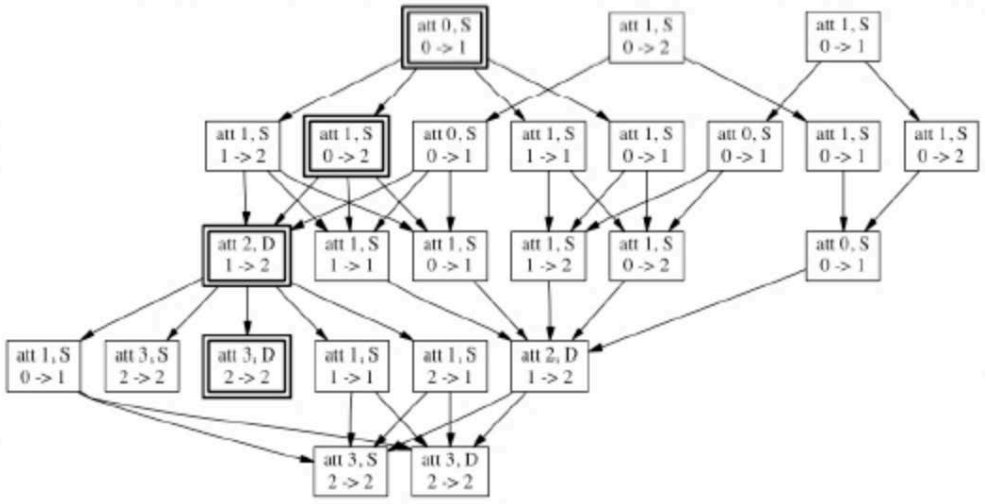
- Models of power systems used in conjunction with
  - Cyber-security assessment within various testbeds
  - Validation of various security technologies within various testbeds
- SCADA traffic generation models
  - “Melody” system open source, basis for a number of projects, e.g.,
    - ML characterization of normal SCADA traffic
- RTDS automation
  - Aid in use of complex power flow simulation tool
- ICS Security Tools repository

# Examples of Available CREDC Technology

## Automated attack graph generation

np-view



**MulVAL**

- Path discovery licensed from Network Perception
- Attack graph and risk assessment licensed from ODU

# CREDC Roadmap for Tools (2018)

| Project | Description | User | Type |
|---|---|---|---|
| OntoDES (ASU) | Static Ontology-based checking of security policies | Utilities | Offline tool |
| EDSGuard (ASU) | Firewall policy management | Utilities | Offline tool |
| EDS-SAT (ASU) | On-line data monitoring | Utilities | Monitors deployed in EDS |
| Secure Parsers (Dartmouth) | Secure parsers for EDS protocols | Equipment manufacturers | Built into embedded code |
| Secure Conduits (Dartmouth) | Components to safely patch and otherwise harden legacy systems | Utilities | Offline tool |

# CREDC Roadmap for Tools (2018)

| Project | Description | User | Type |
|---|---|---|---|
| AMIDetect (UI) | Anomaly detector in AMI | Utilities | Monitors Deployed in EDS |
| ContextAwareAD (UI) | Anomaly detection tools in Bro and Python | Utilities, Researchers | Monitors Deployed in EDS (Online or Offline) |
| EDSAuth (UI/Dartmouth) | Secure authentication of ICS/EDS protocols | Equipment manufacturers | Components built into systems |
| ProResponse (UI) | Tool to fortify communication channel and control infrastructure in EDS, including cloud SCADA | Utilities | Monitors Deployed in EDS |
| Robust GPS (UI) | Multi-receiver direct time estimator (MRDTE) Python prototype | Equipment manufacturers | Reference implementation |

# CREDC Roadmap for Tools (2018)

| Project | Description | User | Type |
|---|---|---|---|
| IIotDevEval (MIT) | Agent-based IIoT device security | OT Operators | Monitors built into EDS |
| PreventOTPD (MIT) | Prevent or mitigate OT physical damage | OT Operators | Monitors built into EDS |
| CRMetricsBPS (ODU) | Cloud-based resiliency self-assessment | Utilities | Offline tool |
| RiskModels (ODU) | Optimal attack countermeasure selection | Utilities | Monitors built into EDS |
| RTSAtRisk (OSU) | Module to compute cyber-physical risk metrics (prototype) | Utilities | Planning tool |
| OpControls (UH) | Operational control self-assessment | Utilities | Planning tool |

# CREDC Roadmap for Tools (2018)

| Project | Description | User | Type |
|---|---|---|---|
| NFI Messaging (UH) | Reference implementation and specification document for secure messaging over insecure networks | Utilities and O&G asset owners | Reference implementation |
| Metrics (WSU) | Tools to measure resiliency for planning and monitoring. Cypher and TSV 2.0, plus CP-Sam 1.0 available 2018 | Utilities | Planning. Eventually support monitoring |

# CREDC Roadmap for Tools (2019)

| Project | Description | User | Type |
|---|---|---|---|
| ANREDS (UI) | SDN provisioning for critical flows | OT system integrators | Offline tool |
| Robust GPS (UI) | C/C++ implementation of MRDTE | Equipment providers, Utilities | Code built into systems |
| BlockChainProvenance (ODU) | Prototype tool on IBM HyperLedger to assess secure provenance of EDS components | Equipment providers | Reference implementation |

# CREDC Self-Sustainability

- Charged with building structure for self-sustaining entity post-CREDC
- Partnering with SEEDS in NSF IUCRC proposal
- Explore joining some other organization
- Critical questions :
  - What's the value proposition for industry to *partner* with universities?
  - What's the value proposition for industry to *invest* in a university consortium?