Andy Bochman
& Rita Wells
Idaho National Laboratory

RENDER* Pilot Project
ReACT **& ATAC***Frontier Projects

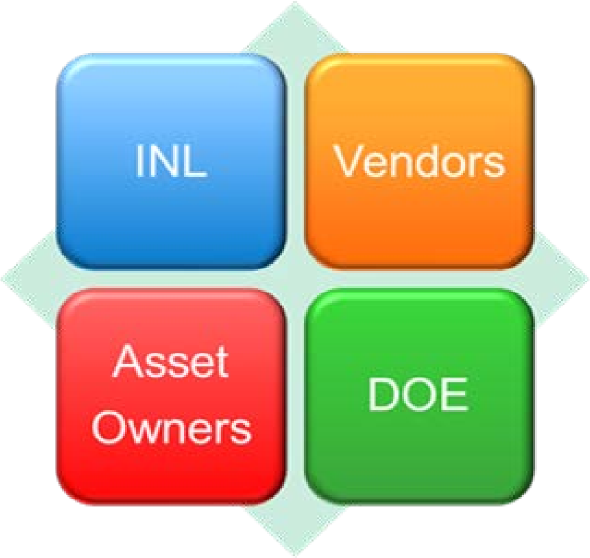
Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

*Risk Evaluation Nexus for Digital -Age Energy Reliability
**Response Analysis and Characterization Tool
***Attack Technology, Analysis and Characterization

Summary: RENDER

- **Objective**
  - Establish a methodology and process to take exploits, malware, and vulnerabilities (EMV) selected by the RENDER working group and analyze for operational impact to the energy sector.
- **Schedule**
  - Start: 10/1/2012 End: 6/30/2014
  - Deliverables: Four Analysis Topic Reports; Final Concept of Operations Report
  - RENDER is a capability to select, evaluate and analyze EMV, then collaborate with vendors and asset owners to determine impact to the grid of cyber attack



RENDER Working Group

- **Total Value of Award:** $1M
- **% Funds expended to date:** 100% **Performer:** Idaho National Laboratory
- **Partners:** DOE-OE, Alstom, Schneider/Telvent, Siemens, Ameren, Dominion

State of the Art & Challenges

- Currently: Evaluation and analysis of EMV is performed by individual vendors and 3rd party researchers and information is shared with customers and/or entities like ICS-CERT
- RENDER Method exercised an approach to characterize and score EMV against specific control systems – sharing results with vendors and asset owns and evaluating overall likelihood and impact metrics
- Value to Industry: The RENDER process results in a deeper understanding of EMVs, including metrics and mitigations, for vendors and asset owners and the potential impact to the energy sector for government.
- Challenges: Legal agreements, Selection of EMV, & Likelihood Metrics

Progress to Date

- **Major Accomplishments**
  - RENDER Pilot Project completed Jun 30, 2014 with delivery of final Concept of Operations Report
  - Analysis Subject (AS)4, Cross-Site Scripting (XSS), completed May 12, 2014
  - AS3, Aegis DNP3 Fuzzer Tool, completed Apr 24, 2014
  - AS2, Privilege Escalation, completed Feb 11, 2014
  - AS1, DNP3 Input Validation Vulnerability, completed Feb 26, 2014
  - Two Vendors with systems at INL; 3rd Vendor executed CRADA after pilot project completion to participate

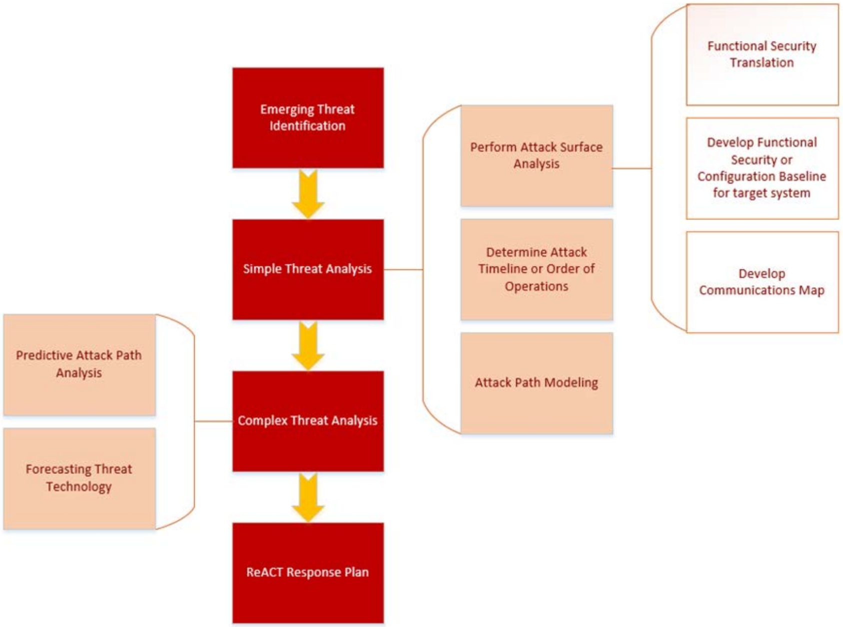
Collaboration & Next Steps

- **Plans to transfer technology/knowledge to end user**
  - Direct information and collaboration is targeted to all vendors and energy sector asset owners
    - Sanitized information could be used also by other research entities and knowledge bases
- **Next Steps: Pilot and Production**
  - Integrate ATAC and ReACT methodology
  - Secure Information Sharing Portal to communicate with the working group
  - Improve of the RENDER method
  - Open RENDER configurations to more R&D entities

Summary: ATAC

Objective

- Threat intelligence is not immediately useful and actionable for most teams. ATAC is an information schema and analysis process for integrating threat analysis into risk decision making.
- ATAC focuses on how adversaries select technology and implement attacks.



Functional Security Translation
Emerging Threat Identification
Perform Attack Surface Analysis
Develop Functional Security or Configuration Baseline for target system
Simple Threat Analysis
Determine Attack Timeline or Order of Operations
Develop Communications Map
Predictive Attack Path Analysis
Attack Path Modeling
Complex Threat Analysis
Forecasting Threat Technology
ReACT Response Plan

Schedule

- Feb 2013-May 2014
- Develop ATAC process (Oct 2013)
- Case study (Dec 2013)
- Onsite process review (Feb 2014)
- Final report (Mar 2014)

- **Total Value of Award:** $250k
- **% Funds expended to date:** 100%
- **Performer:** Idaho National Laboratory
- **Partners:** Dominion

Advancing the State of the Art (SOA)

- Hackers have project managers, too
  - Have to do work to get paid (no more script kiddies)
  - Requires organized work flow
  - Use ATAC Life Cycle and Functional Security Matrix (FSM) to understand how adversary works
- ATAC Life Cycle
  - Based on Lockheed Martin Cyber Kill Chain
  - Defines life cycle and work flow of attacks (DIME)
  - Built on Attack Surface Analysis (ASA)
- ATAC is tailored to group of adversaries and their capabilities
- Threat information that can be applied to create attack surface analysis to recommended or specific configurations
- Characterization of whole classes of adversaries

Challenges to Success

- **Why isn't threat intelligence actionable?**
  - Have sufficient quantity AND quality of open-source threat intelligence
  - Defenders don't know how to consume threat intelligence making actionable
  - Needed to define threat relationships define a way to analyze
- **History of threat intelligence matters**
  - National Security Risk = f(Threat, Vulnerability, Consequence)
    - Threat intelligence traditionally used by national security groups
    - Threat = f(Capabilities, Opportunity, Intent)
  - Operational Risk = f(Probability, Impact)
    - Threat not a factor in this equation
    - How do we use threat intelligence if it's not in the risk equation? → ATAC
- **Conflicting impact assessments in existing threat feeds**
  - Operational or business – What happens if breached
    - Determined and prioritized by organization, not adversary
  - Technical – What attackers can do if attack against target succeeds
    - Describes technical gains by adversary (STRIDE – Spoofing Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of privilege)

Progress to Date

Major Accomplishments

- ATAC Life Cycle
- Simple vs. Complex Threat Analysis
- Forecasting Threat Technology (2 year review, ICS-CERT advisories)
- Predictive Attack Path Analysis
- Attack Style Characterization (Red October vs. Night Dragon)

Functional Security Layer	Functional Baseline of Target	Attack Path Model		
		Protocol	Services	Ports
UR&R				
Network	TCP/IP			
Firmware				
Operating System	Microsoft Windows	TCP, UDP	RPC over HTTP	80
Virtualization				
Applications	Windows Explorer	TCP, UDP	HTTP	80
Cloud, hosted, or vendor services				
Custom code				
Data & Data Stores				

Collaboration/Technology Transfer

- **Plans to transfer to end user:**
  - Develop training and documentation to support implementation
  - Build defensive and detection controls catalog
  - Produce case studies that demonstrate how to use ReACT
- **Plans to gain industry acceptance:**
  - ATAC for Vendors
    - ASA of RENDER configurations
    - What attack paths and techniques are most likely to be used against your software?
  - ATAC for Asset Owners
    - ASA of Original Equipment Manufacturer (OEM) and vendor products
    - How does your attack surface change when product ‘X’ is added to your ICS environment?
    - What can be done to minimize the cyber security risk product ‘X’?

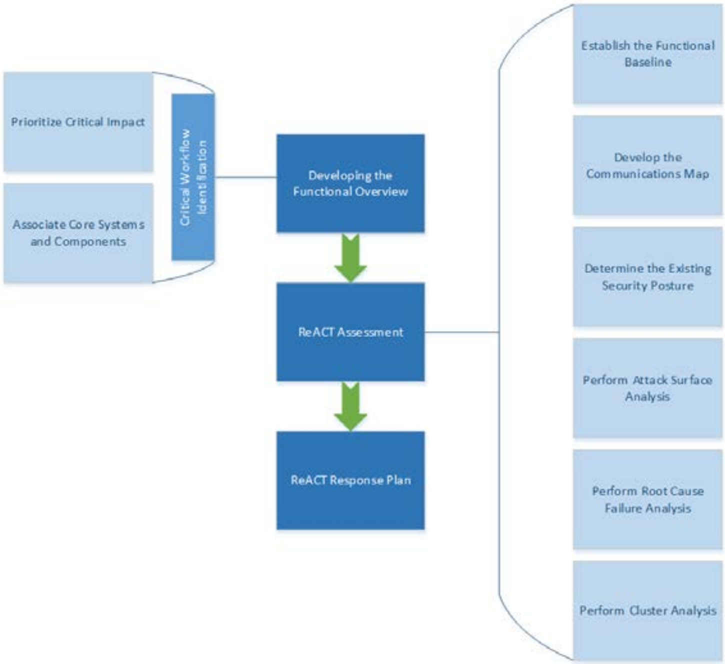
Next Steps for ATAC

- **Attack Surface Analysis**
  - Default configuration (OEM and vendor software & equipment)
  - Customized configuration (asset owners)
- **Threat trending and complex ATAC analysis**
  - ICS-CERT advisories (targets, vulnerability discovery patterns)
  - Confirmed energy sector attack campaigns (APT, criminal)
- **Customer feedback loop**
  - Agile feedback process for all stakeholders
  - What works? What doesn't? If not, why not?
    - Secure code development & application implementation strategy(vendors)
    - Defensive & Detection Catalog (asset owners)
    - Attack Style Characterization (energy security community)
  - Process improvement→ next iteration of documentation, training, etc.

Summary: ReACT

Objective

- Provide an information schema, set of tools and analysis processes teams can use to relate technical cyber security data directly into risk management decision-making
- ReACT focuses on what defenders know and control – their environment and its attack surface.


Prioritize Critical Impact
Associate Core Systems and Components
Critical Workflow Identification
Developing the Functional Overview
ReACT Assessment
ReACT Response Plan
Establish the Functional Baseline
Develop the Communications Map
Determine the Existing Security Posture
Perform Attack Surface Analysis
Perform Root Cause Failure Analysis
Perform Cluster Analysis

Schedule

- Feb 2013-May 2014
- Develop ATAC process (Oct 2013)
- Case study (Dec 2013)
- Onsite process review (Feb 2014)
- Final report (Mar 2014)

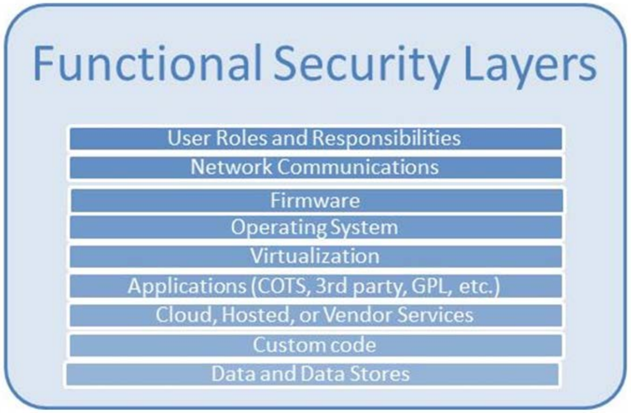
- **Total Value of Award:** $250k
- **% Funds expended to date:** 100%
- **Performer:** Idaho National Laboratory
- **Partners:** Dominion

Advancing the State of the Art (SOA)

- Connects the dots → risk, cyber security, and technical threat
- Provides mechanism for:
  - Equivalent risk comparisons
  - Integrated threat response
  - Risk prioritization
- Provides repeatable, organized approach to understanding existing security posture
  - Helps identify gaps in existing security posture and why gaps exist
  - Potential ties into existing risk management strategies
  - Feeds seamlessly into work planning and prioritization
- Attack Surface Analysis
  - Modified Code security concept for use in asset owner environment
  - Maps technical data to risk factors (probability)

Progress to Date

- **Major Accomplishments**
  - Attack Surface Analysis (ASA)
  - Top 5 Energy Management targets
  - Functional Security Layers
  - Functional Baseline
  - Communications Map
  - Attack Surface Analysis



Functional Security Layers

User Roles and Responsibilities
Network Communications
Firmware
Operating System
Virtualization
Applications (COTS, 3rd party, GPL, etc.)
Cloud, Hosted, or Vendor Services
Custom code
Data and Data Stores

Functional Security Layer	Functional Baseline	Communications Map			Existing Security Posture		Gap Analysis
		Protocol	Services	Ports	Existing Defense Measures	Existing Detective Measures	
UR&R	Local accounts (user, service, machine)	N/A			Guest account disabled	Enhanced audit policy & logging	Missing 1 defensive measure
Network	TCP/IP				DMZ firewall	Enhanced audit policy & logging	No gaps
Firmware	N/A						
Operating System	Windows Server 2003 R2	TCP	RPC	135	Anti-virus	Enhanced audit policy & logging	Missing 1 defensive measure
Virtualization	N/A						
Applications	.Net framework	TCP	HTTP	80	Patches applied quarterly	App & security events monitored daily	Missing 1 detection measure
Cloud, hosted, or vendor services	N/A						
Custom code	CMS	TCP	HTTP	80	N/A	N/A	Missing 3 defensive measures
Data & Data Stores	N/A						

Collaboration/Technology Transfer

- **Plans to transfer to end user:**
  - Develop training and documentation to support implementation
  - Build defensive and detection controls catalog
  - Produce case studies that demonstrate how to use ReACT
- **Plans to gain industry acceptance:**
  - ReACT for Vendors
    - ASA of RENDER configurations
    - Prioritize where to allocate code security resources?
    - Help develop or supplement secure deployment efforts?
  - ReACT for Asset Owners
    - ASA of Original Equipment Manufacturer (OEM) and vendor products
    - What other defensive and detection controls are required or could be used?

Next Steps for ReACT

- **Attack Surface Analysis (ASA)**
  - Default configuration (OEM and vendor software & equipment)
  - Customized configuration (asset owners)
- **Defensive & Detection (D&D) Catalog (Asset Owners)**
  - Defensive & detection techniques, controls and strategies specific to ASA
- **Secure Code Development & App Implementation Strategy**
  - Prioritize code security work based on ASA
  - Enhance secure software implementation strategy based on ASA
- **Customer feedback loop**
  - Agile feedback process for all stakeholders
  - What works? What doesn’t? If not, why not?
  - Process improvement → next iteration of documentation, training, etc.