U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Keyless Infrastructure Security Solution (KISS)
Pacific Northwest National Laboratory (PNNL)

Bev Johnson, PM / Michael Mylrea, PI

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: Keyless Infrastructure Security Solution - M617000254

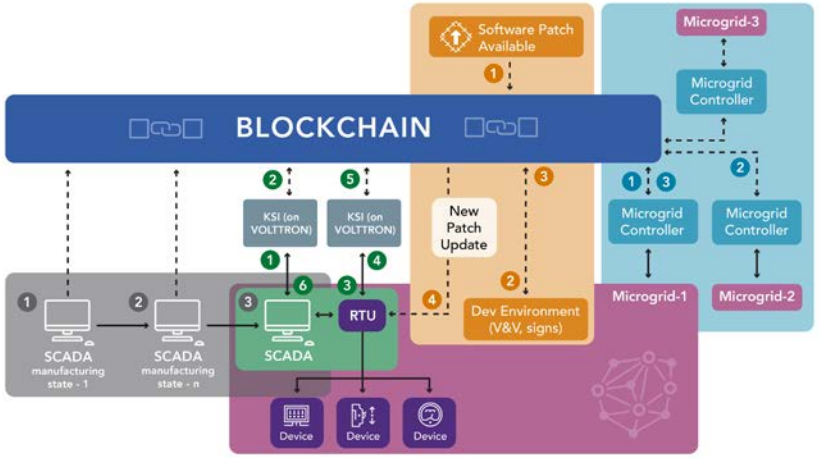
KISS

Objective

- Develop “KISS” to increase the trustworthiness, integrity, and resilience of energy delivery systems (EDS) responsible for complex grid edge energy exchanges and integration of distributed energy resources

Schedule

- October 2017 – September 2020
- Phase 1 – Design Application
- Phase 2 – Develop Prototype
- Phase 3 – Demonstrate Use of Prototype and Outreach



Total Value of Award:	**$ 3,000,000**
Funds Expended to Date:	**25%**
Performer:	**Pacific Northwest National Laboratory**
Partners:	**Guardtime, Washington State University, Nevermore Security IAB: Avista, Cisco, Rocky Mountain Institute, Energy Blockchain Consortium, IEEE Blockchain in Energy TWG, DoD HDIAC, OATI, DOE EIA**

Advancing the State of the Art (SOA)

- Develop the first blockchain VOLTTRON™ agent (KISS) to continuously monitor and autonomously verify data, command, and energy exchanges
- Increase the trustworthiness, integrity, control and security of EDS responsible for energy transactions
- Successful lab demonstration could lead to potential real-world deployment of the system in energy utility space
- KISS will be interoperable with other OT systems without the requirement to tap into system firmware
- Research teams planning to demonstrate a utility-to-utility scale secure data exchanges while maintaining an immutable ledger of grid data and communications
- Engaging with CISCO and partners to develop and deploy Guardtime KSI-based data validation system in the utility ICS environment

Challenges to Success

KISS

Administrative

- Engaging multiple external collaborators in complex software development

Technical

- Prototype design: Interaction of energy management and distribution management systems (EMS/DMS) with VOLTTRON™ agent
- Aligning energy utility business, operational and security requirements
- Improving the state of the art in an unexplored area of research and development

Proposed Approaches to Addressing Challenges

- Key partners with in-depth blockchain expertise and knowledge
- Sustaining close collaboration with project's partners, using their insight to inform software design and development, test environment setup, and software validation and verification
- Leveraging IAB expertise to engage with utility and industry
- Collaboration in developing and implementation of use cases with partners, IAB, utilities and vendors
- Feedback from partnering utilities to feed software improvement

Progress to Date

- Completed D0.1, Intellectual Property Management Plan 1/31/18
- Completed D0.2 Technology Landscape Analysis Report 4/24/18
- Completed D1.1, Establishment of Industry Advisory Board (IAB) 8/15/18. Conducted first project meeting with IAB, 8/13/18.
- Completed D1.2 White Paper Examining Security and Trust Gaps; KISS Use Cases 10/15/18
- Completed D1.3 Blockchain for Transactive Energy Requirements Document 8/7/10.
- Tested the VOLTTRON DNP3 driver and using it to interface with EMS and RTU
- Setup a utility scale historian to stage the EMS data in real-time for KISS experimentation
- Guardtime installed and deployed Black Lantern and Resonance – provenance layer of Guardtime KSI blockchain stack 8/14/18
- Developed LinkLite® for KISS and integrated with VOLTTRON™ agent
- Extracted DMS data and digitally signed using KSI on WSU test bed
- Completed the first set of use-cases to test security of data-at-rest; continue with the approach to test data-in-transit
- Engagement with Cisco, which plans to submit prototype hardware on KISS test bed

Progress to Date (cont'd)

- **Papers:**
  - Michael Mylrea and Sri Nikhil Gourisetti, "Blockchain: Next Generation Supply Chain Security for Energy Infrastructure and NERC Critical Infrastructure Protection (CIP) Compliance" was published and presented at Resilience Week 2018
  - Michael Mylrea and Sri Nikhil Gourisetti, "Blockchain NERC CIP Compliance for Supply Chain Management," was selected as one of the top papers to be published in the Journal of Systemics, Cybernetics and Informatics.
- **Presentations:**
  - Michael Mylrea presented KISS blockchain project at closed conference sponsored by the Department of Homeland Security's Office of Intelligence and Analysis on behalf of the Office of the Director of National Intelligence 04/27/18
  - Michael Mylrea participated and presented at Washington loT Council and Blockchain Meeting 2/8-10/18
  - Sri Nikhil Gourisetti presented "Blockchain Technology for Decentralized Coordination of Grid Systems" at EnergySec 14th Annual Security & Compliance Summit at Anaheim, CA 8/26/18
  - Sri Nikhil Gourisetti served as a panelist at the IEEE Global Blockchain Cybersecurity Implications for the Energy Sector Panel

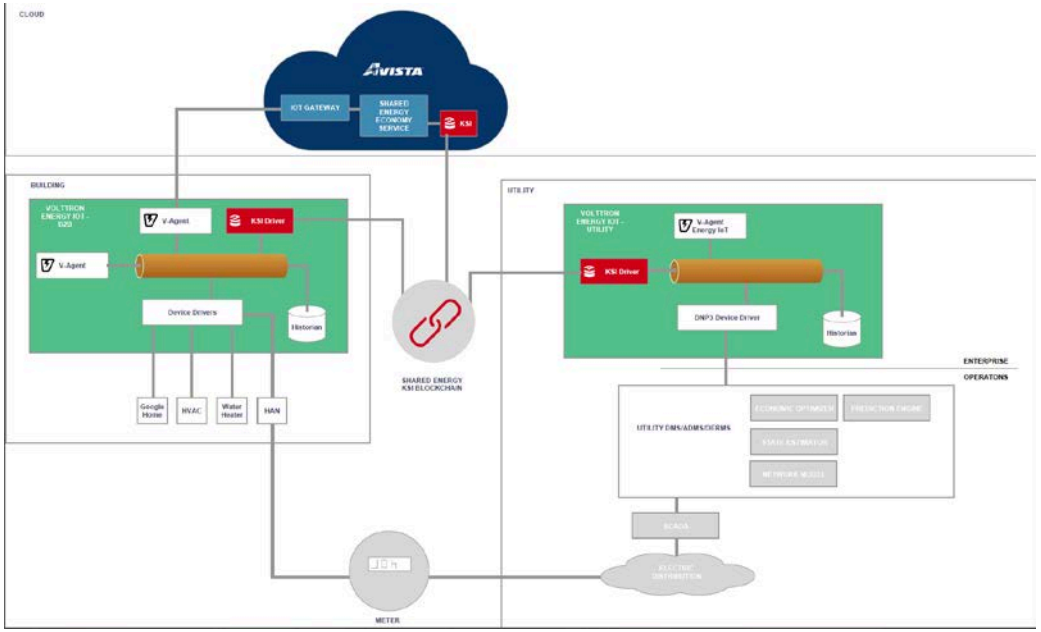
Collaboration/Technology Transfer

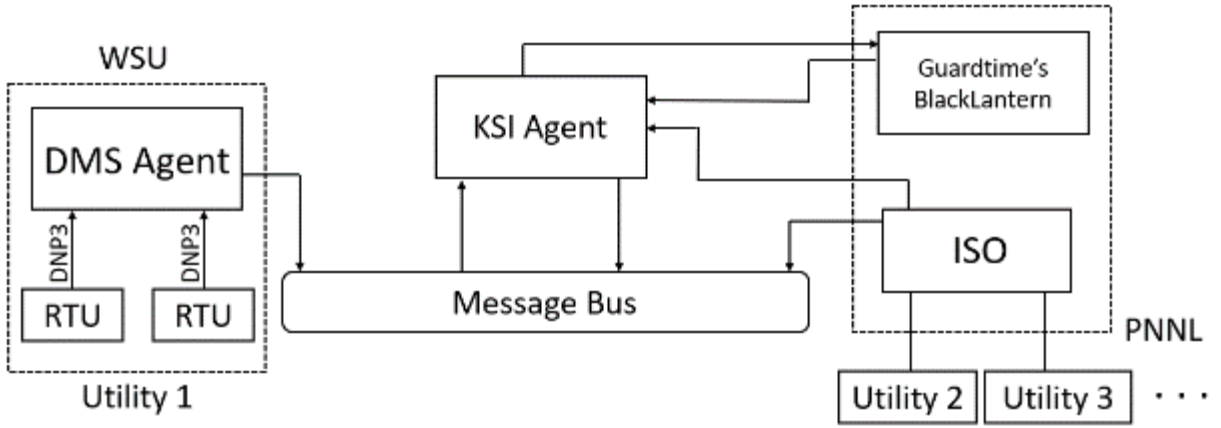
Plans to transfer technology/knowledge to end user

- Technology transfer to vendor space; both Guardtime and Cisco are leveraging project to develop next generation blockchain enabled technology to secure EDS
- Piloting multiple use cases with KISS enabled EDS, including testing at:
    - Washington State University Lab
    - PNNL Lab
    - Interconnection between PNNL and WSU for live telemetry testing
    - Lab demonstrations to IAB and select utility(ies)
    - Testing/demonstration prototype at participating utility

Next Steps for this Project

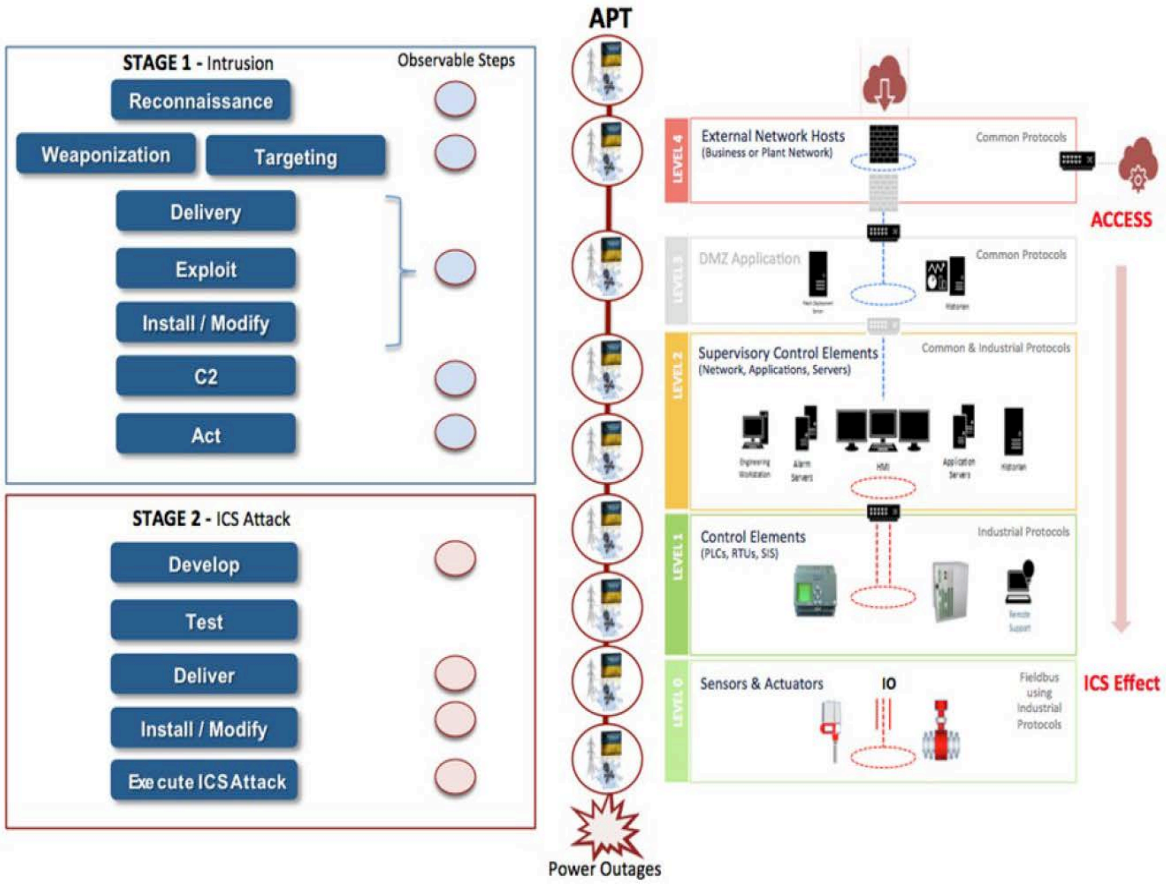
- **EDS Machine State Integrity**
- **Configuration and Patch Management**
- **Secure Data sharing**
- **Supply Chain Security**





Next Steps for this Project (Contd.)

- **Applying KISS to mitigate configuration and identity management vulnerabilities.**
- **Validating and verifying efficacy of approach through testing and real world use cases.**



Conclusion

KISS