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

Module-OT : Modular Security Apparatus for Managing Distributed Cryptography for Command & Control Messages on Operational Technology (OT) Networks

National Renewable Energy Laboratory (NREL)

Maurice Martin

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: Module-OT

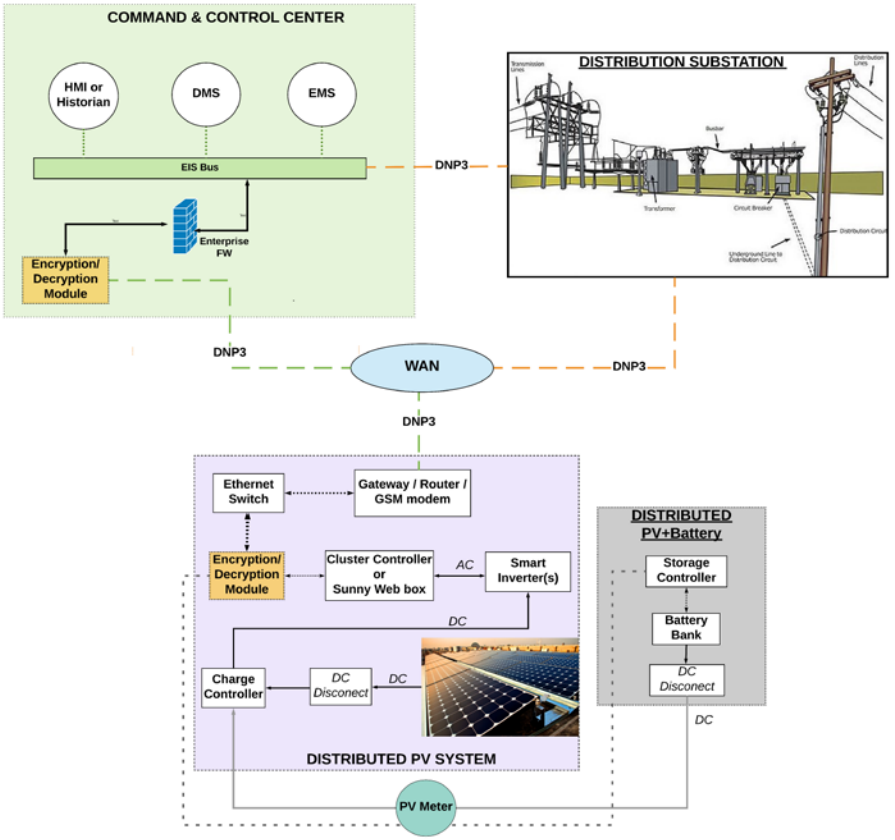
Modular Security Apparatus for Managing Distributed Cryptography for Command & Control Messages on Operational Technology (OT) Networks

Objective

- Create a lightweight cryptographic module suitable for use in DERs and related devices.

Schedule

- Oct. 2017 – Sep. 2020
- Key deliverables
  - Workshop report 11/18
  - Module design 5/19
  - Test system design 9/19
  - Test results 9/20
- Vendor-agnostic, open source design of cryptographic module



Total Value of Award:	**$ 2,775,000**
Funds Expended to Date:	**% 28**
Performer:	**NREL**
Partners:	**SNL, PNM, Solectria Solar**

Advancing the State of the Art (SOA)

- **Current SOA:**
  Survey of OT equipment shows wide variety of security controls. Testing reveals weak security even on DER devices (e.g. inverters)
- **Feasibility of approach:**
  Leveraging existing cryptographic libraries lowers cost of development; close engagement with utilities, vendors, and other stakeholders ensures applicability and practicality of approach
- **Improvement over SOA:**
  Vendor agnostic; modular (separates power system from crypto system); compliance with emerging DER security standards
- **End user benefit:**
  Improved confidence for investors and system operators in the security of DER
- **Advancing cybersecurity for EDS:**
  Mitigation against man-in-the-middle and other attacks and other that could result in mis-operation of large numbers of DERs

Challenges to Success

Ensure that module is interoperable with product lines

- Stakeholder advisory group vendors
- Solectria Solar added as a project partner for testing and evaluation
- Careful definition of hardware and software interfaces

Variety of devices and placement within DER architecture

- For initial evaluation and design, narrow focus to a subset of devices
- Engagement with utility and vendor community regarding DER architectures

Ensure that cryptographically induced latency does not interfere with real-time control needs for DER

- Simulation and field testing

Ensure that key management is management for all parties

- Draw from existing research on PKI for industrial applications (so-called “industrial key infrastructure”)

Progress to Date

Major Accomplishments

- Research on current security controls in DER-related devices
- Day-long workshop with industry stakeholders (and workshop report)
- Defined hardware and software interfaces and key features
- Export control issues resolved
- Technical report drafted (useful for design)
- Investigated DER communication requirements and impact
- Initial lab analysis of SEL 3025 Serial Shield
- Submitted two concept papers to *IEEE Power and Energy* conference

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

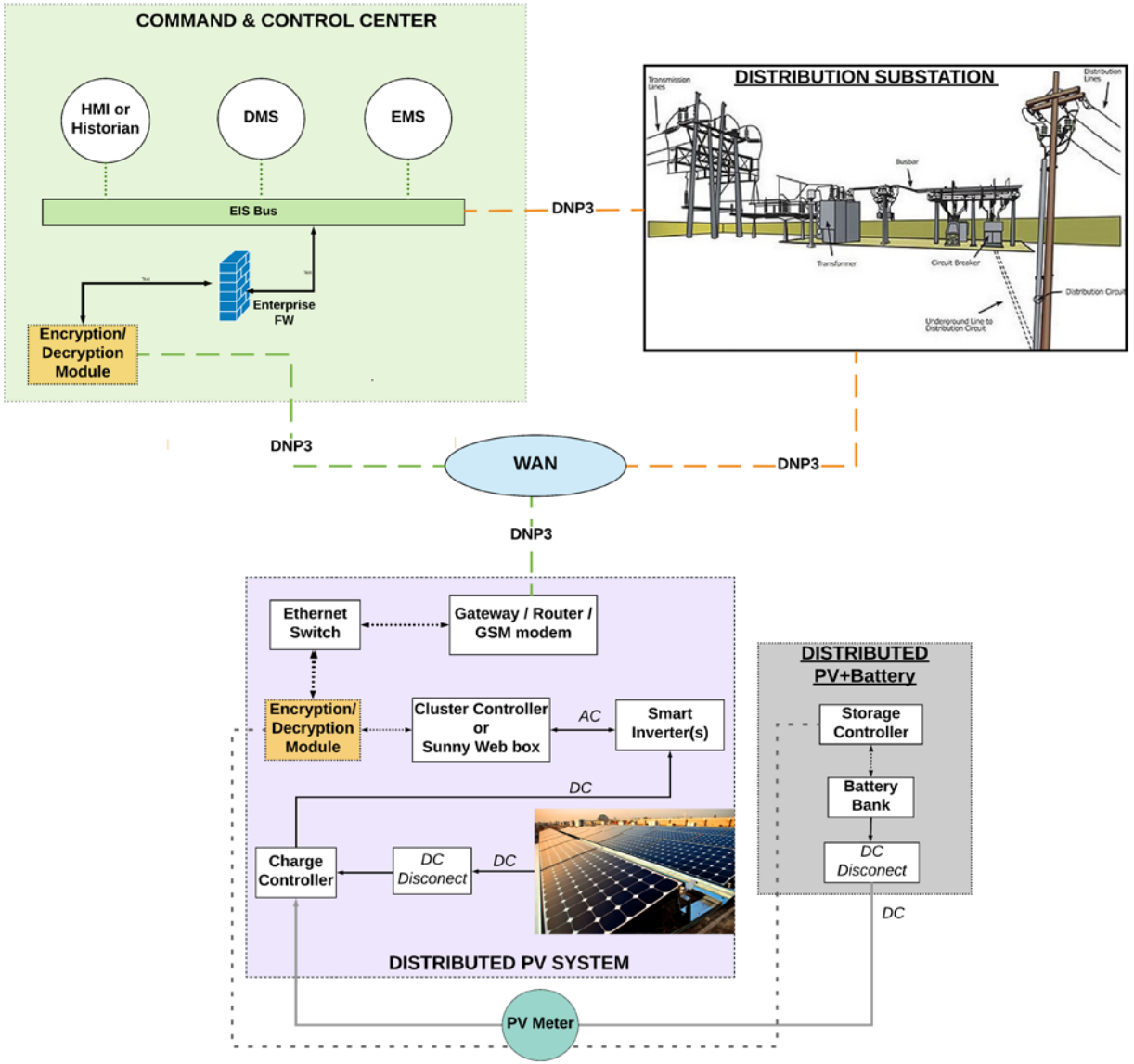
- End users:
  - **Vendors** – Will publish all project results, including design and code, under an open source license in a form useful to anyone wishing to commercialize. The project will conduct outreach to vendors via conferences and other industry events.
  - **End users** – Will reach out to utilities, DER owners and aggregators, and others to raise awareness about the need for DER security and the availability of this module for vendor implementation.
- Testing and demonstration:
  - In addition to lab testing, two field demonstrations are planned at project partner sites: PNM and Solectria Solar. Details of testing architecture currently being developed.

Next Steps for this Project

To the end of project:

- Build testing architecture
  - Will include testing in an emulated environment prior to field testing
  - Researching and analyzing existing procedures (e.g., FIPS 140-2, FIPS 197, IEEE 1547-2018)
- Detailed design technical report
- Design, test, and validate prototype module
- Validation of cryptographic implementation
- Lab testing (including pen testing)
- Field testing
- Final report

Assumptions and architecture



DER Communication Requirements and Impact

Requirements

- Studied standard communications for DER support of grid functions, including the Common Smart Inverter Profile (CSIP) and SunSpec Information Models
- Examples include setting the mode of the inverter, setpoints, alarms, and more

Impact

- The consequence if its confidentiality, integrity, availability is compromised
- The additional cost of applying security to protect and corresponding impact to communications

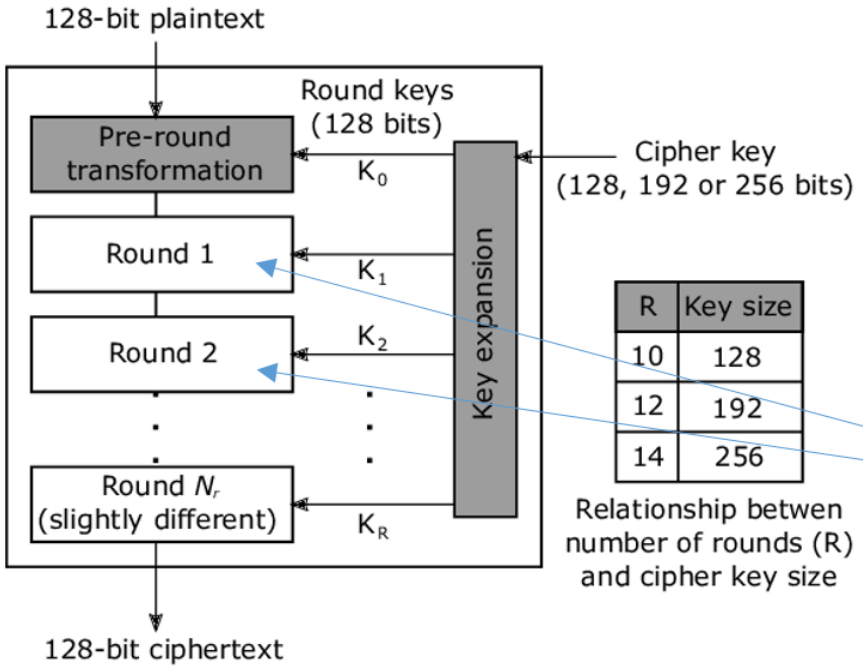
Report

- Information from this document can be used to inform the design of the Module OT prototype and recommendations on security modules for DER in general

Impact of Encryption on DER Systems

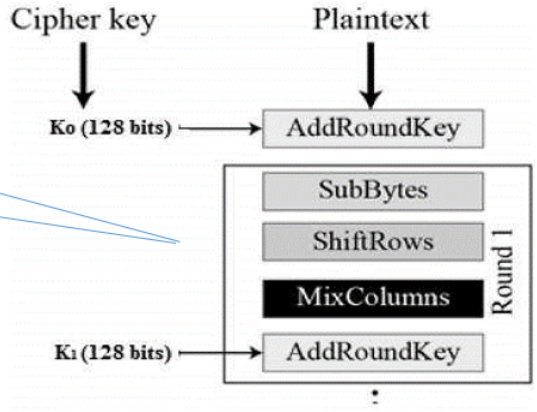
Investigated symmetric cryptography algorithms for reducing complexity and resource utilization

- Focused on Advanced Encryption Standard (AES)



R	Key size
10	128
12	192
14	256

Relationship betwen number of rounds (R) and cipher key size



Performance Impact of Different AES Algorithms

AES implemented in different modes

- Example comparison results for a lightweight microcontroller, using a mid-range ARM Cortex-M3 processor encrypting 1024 input bytes is shown below
- Key lengths: 128, 192, 256; Modes CBC, GCM, CCM

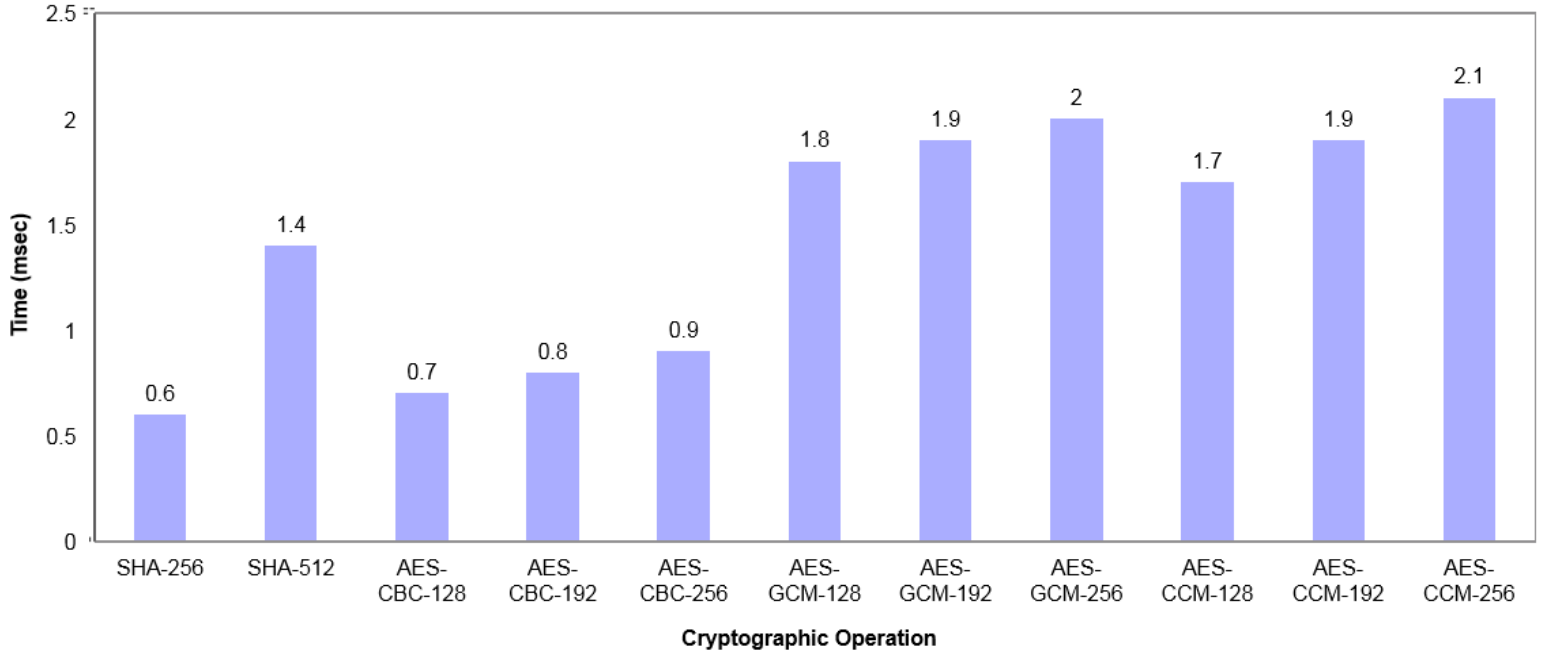


Image Credit: "Performance of State-of-the-Art Cryptography on ARM-based Microprocessors," ARM, 2015.

Encryption Impact Testing in Emulated Environment

Testing on emulated DERs

- In-progress, obtaining results on AES key length and mode impact on latency within system
- Modeled within SCEPTRE, a Sandia-developed Emulytics™ tool, and includes the SunSpec System Validation Platform (SVP) communicating with multiple DERs through encrypted tunnels
- Initial conclusions find that average latency impact to DERs is very low, despite mode and key length

Example Initial Results

DER-01 • aes128-ctr
DER-02 • aes192-ctr
DER-03 • aes256-ctr
DER-04 • aes128-gcm@openssh.com
DER-05 • aes256-gcm@openssh.com
DER-06 • chacha20-poly1305@openssh.com
DER-07 • aes128-ctr
DER-08 • aes192-ctr
DER-09 • aes256-ctr
DER-10 • aes128-gcm@openssh.com
DER-11 • aes256-gcm@openssh.com
DER-12 • chacha20-poly1305@openssh.com
DER-13 • aes128-ctr
DER-14 • aes192-ctr
DER-15 • aes256-ctr
DER-16 • aes128-gcm@openssh.com
DER-17 • aes256-gcm@openssh.com
DER-18 • chacha20-poly1305@openssh.com
DER-19 • None
DER-20 • None

DER	Conversations	Duration (sec)	Bytes per second?
01	413	0.00626087167070237	0.00000247872995293356
02	249	0.006617823293173	0.00000266618844551191
03	249	0.00542079518072254	0.00000323822890126795
04	249	0.00462665863453782	0.0000055276686195195
05	249	0.00592648594377467	0.00000238610485655672
06	249	0.005095827309237	0.00000304410233526702
07	249	0.00634124497991958	0.00000255345906651277
08	249	0.00534820883534131	0.00000319486788252169
09	249	0.00440785140562246	0.00000526625018592886
10	249	0.00577964257028106	0.00000232669440862818
11	249	0.00517054618473861	0.00000308873726686894
12	249	0.0060533734939762	0.00000243759150066669
13	249	0.0053129397590364	0.00000319249758892216
14	249	0.00423736144578344	0.00000506255847763852
15	249	0.00586545381526144	0.00000236122710403046
16	249	0.00517209638554168	0.00000311012029000081
17	249	0.00620723694779127	0.00000249831114824806
18	249	0.0053389076305223	0.0000032130913138817
19	249	0.00480277108433753	0.00000115474873329975
20	247	0.00565287044534433	0.000000966206034090618