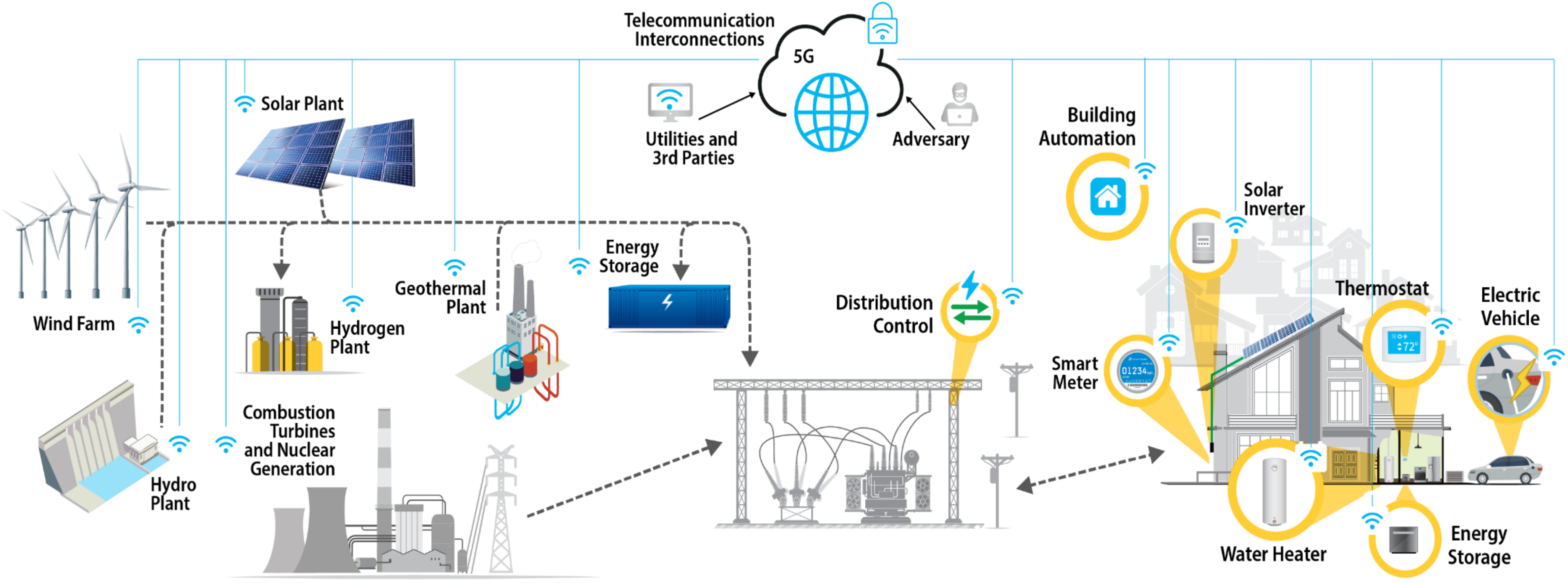
Electric Vehicle Supply Equipment Cybersecurity Through Emulation

Ryan Cryar, Cybersecurity Researcher
National Renewable Energy Laboratory

IEEE PES GM 2024—July 24, 2024

Securing the Energy Future



Bulk Power Generation

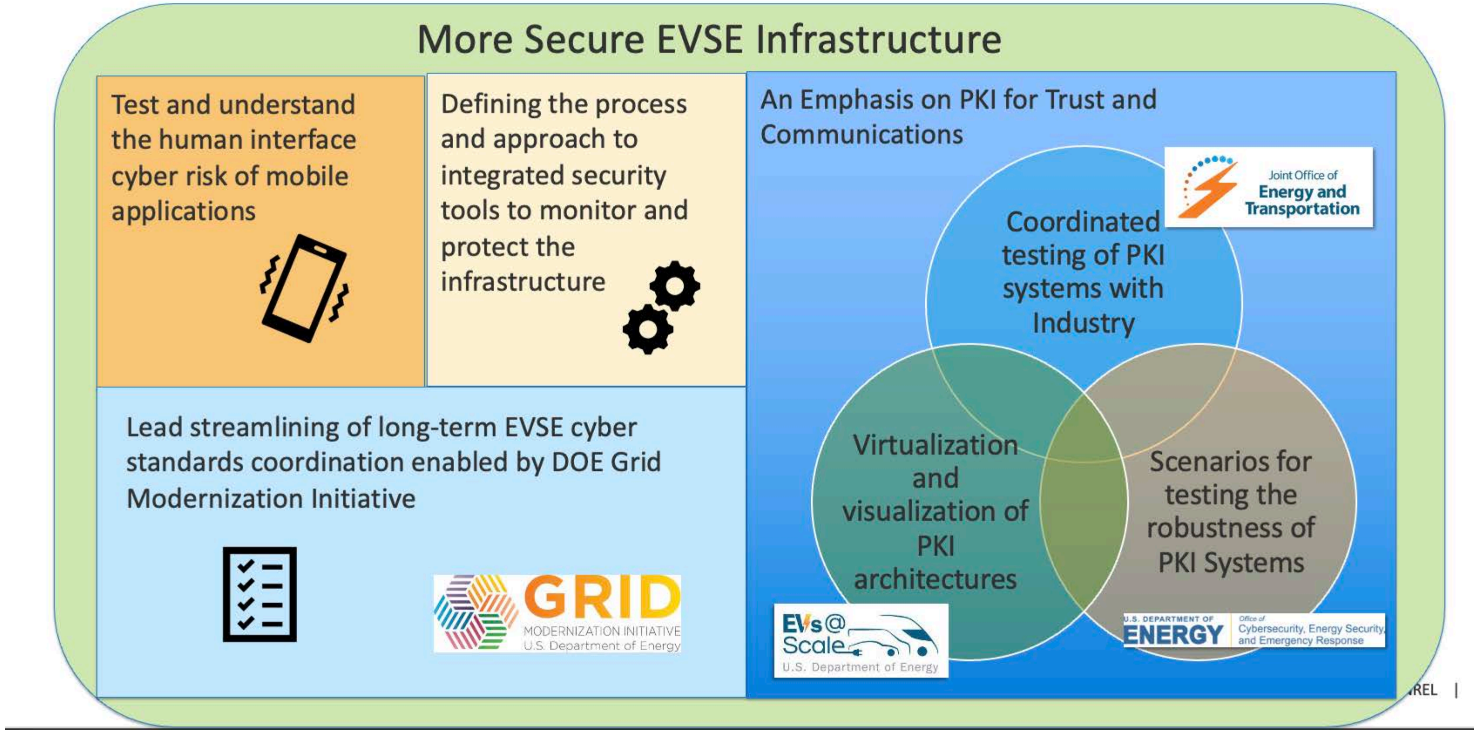
Transmission & Distribution

Prosumer

EVSE Security Is a Multifaceted Endeavor

- Integrating the resources of the U.S. Department of Energy (DOE) Vehicle Technologies Office; Office of Cybersecurity, Energy Security, and Emergency Response; and Joint Office of Energy and Transportation to address the public key infrastructure (PKI) execution challenges

- Complemented with long-term electric vehicle supply equipment (EVSE) cyber standards coordination supported by the DOE Grid Modernization Initiative.



More Secure EVSE Infrastructure

Test and understand the human interface cyber risk of mobile applications

Defining the process and approach to integrated security tools to monitor and protect the infrastructure

An Emphasis on PKI for Trust and Communications

Coordinated testing of PKI systems with Industry

Virtualization and visualization of PKI architectures

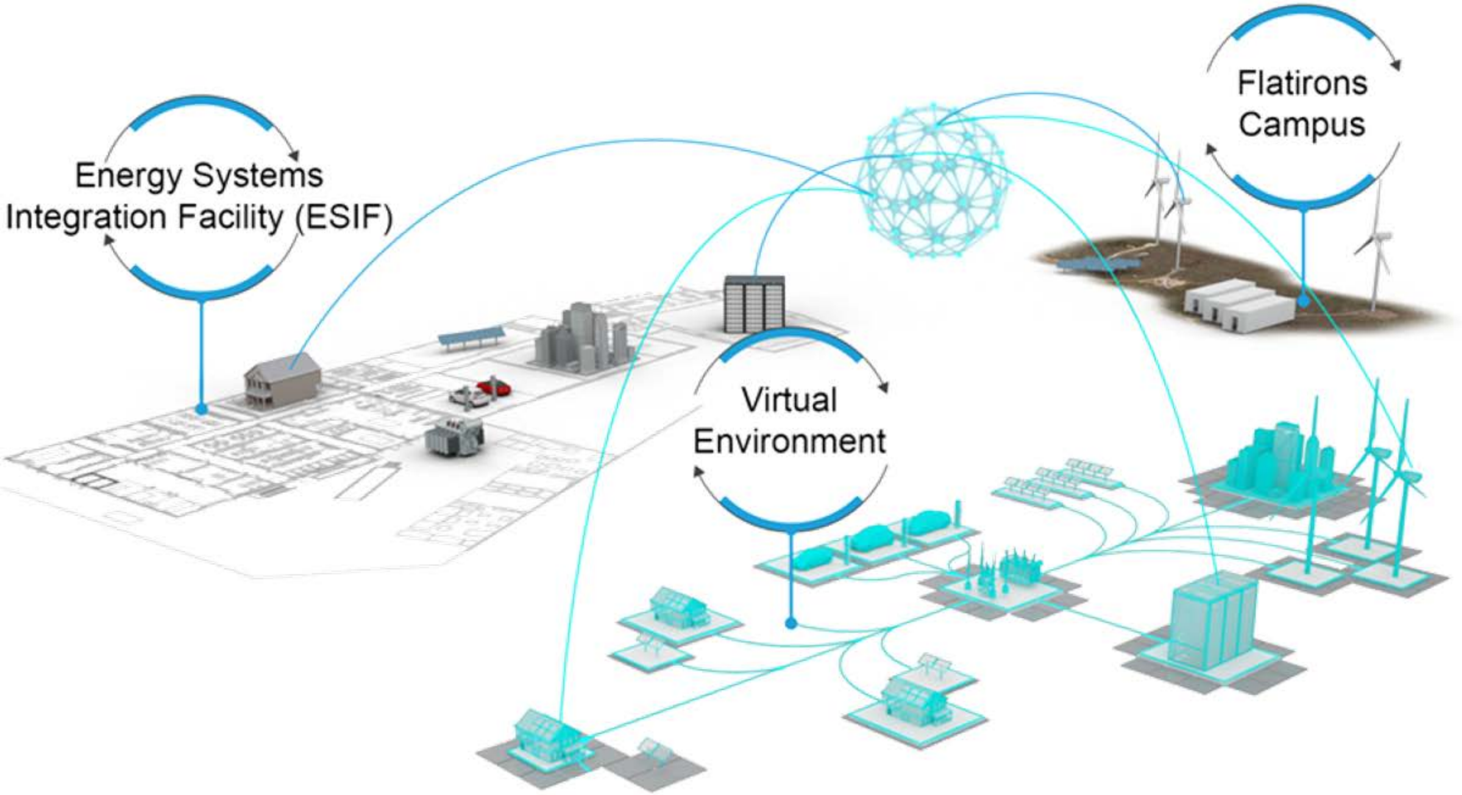
Scenarios for testing the robustness of PKI Systems

Lead streamlining of long-term EVSE cyber standards coordination enabled by DOE Grid Modernization Initiative

Joint Office of Energy and Transportation
GRID MODERNIZATION INITIATIVE U.S. Department of Energy
EVs@Scale U.S. Department of Energy
U.S. DEPARTMENT OF ENERGY Office of Cybersecurity, Energy Security, and Emergency Response
REL |

ARIES Cyber Range

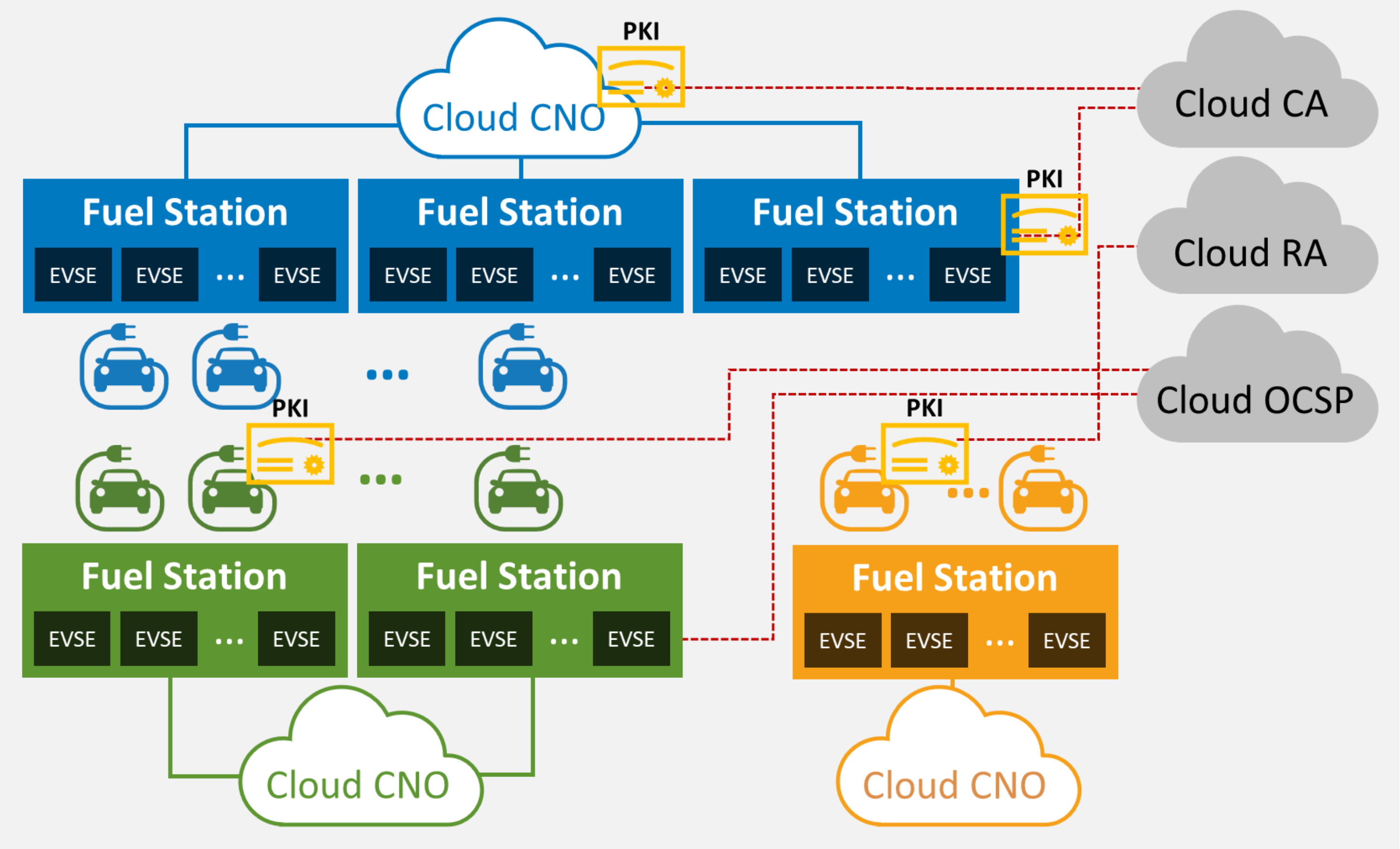
- Industry-leading **visualization** for cyber-physical systems R&D
- Unparalleled **laboratory resources** across the Advanced Research on Integrated Energy Systems (ARIES) platform
- Focus on **future distributed energy system challenges**, with support from NREL's experts in all relevant grid-edge domains
- Strong **industry partnerships** transition applied research into market impact.



Integration of Charging Protocols

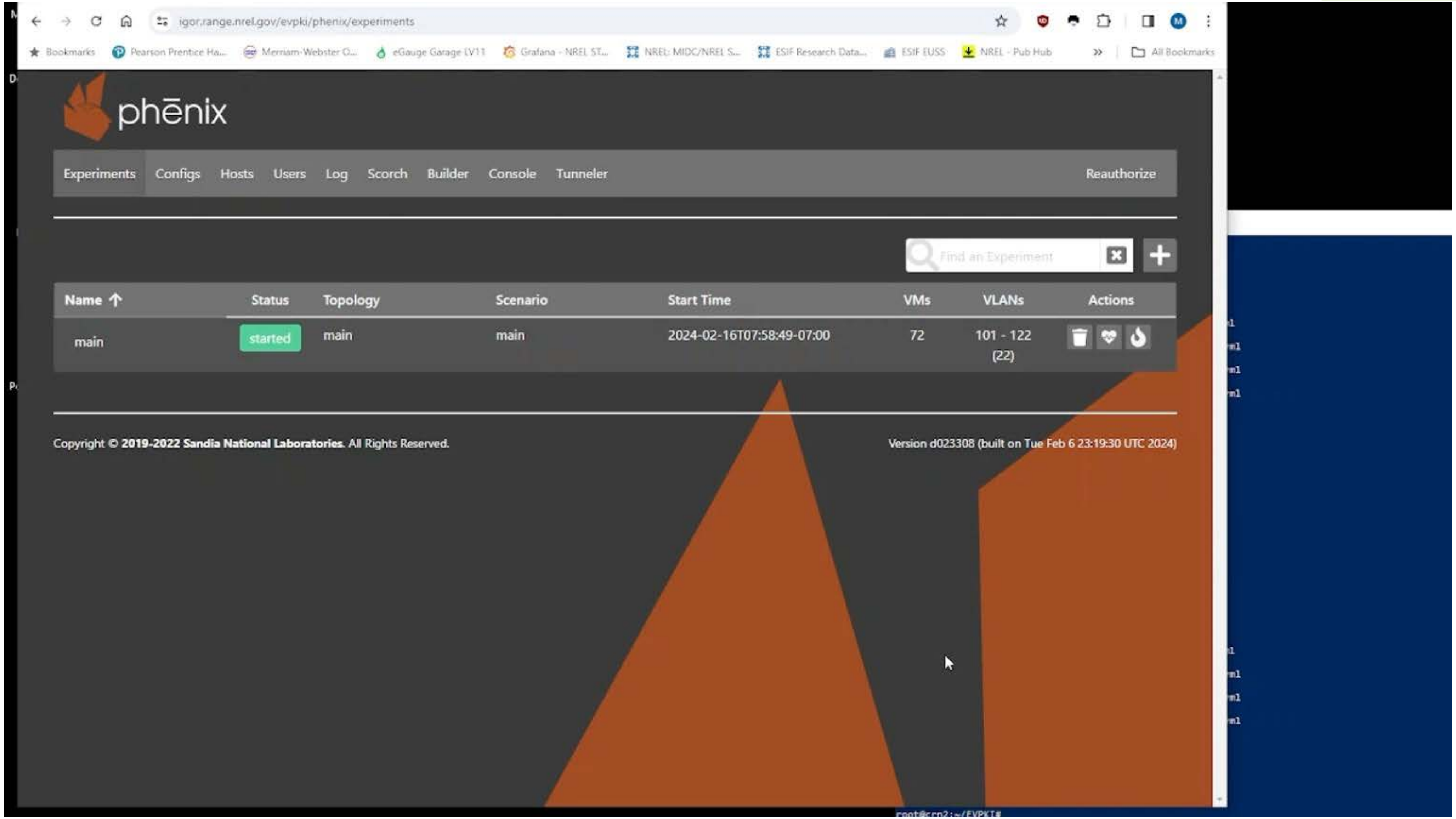
OBJECTIVE—Develop and test the security of charging protocols to help secure EV infrastructure:

- ISO 15118 - 2
- Open Charge Point Protocol (OCPP)
- Planned: Open Charge Point Interface
- Exploring applicability of IEEE 2030.5



U.S. Department of Energy

Experiment Construction

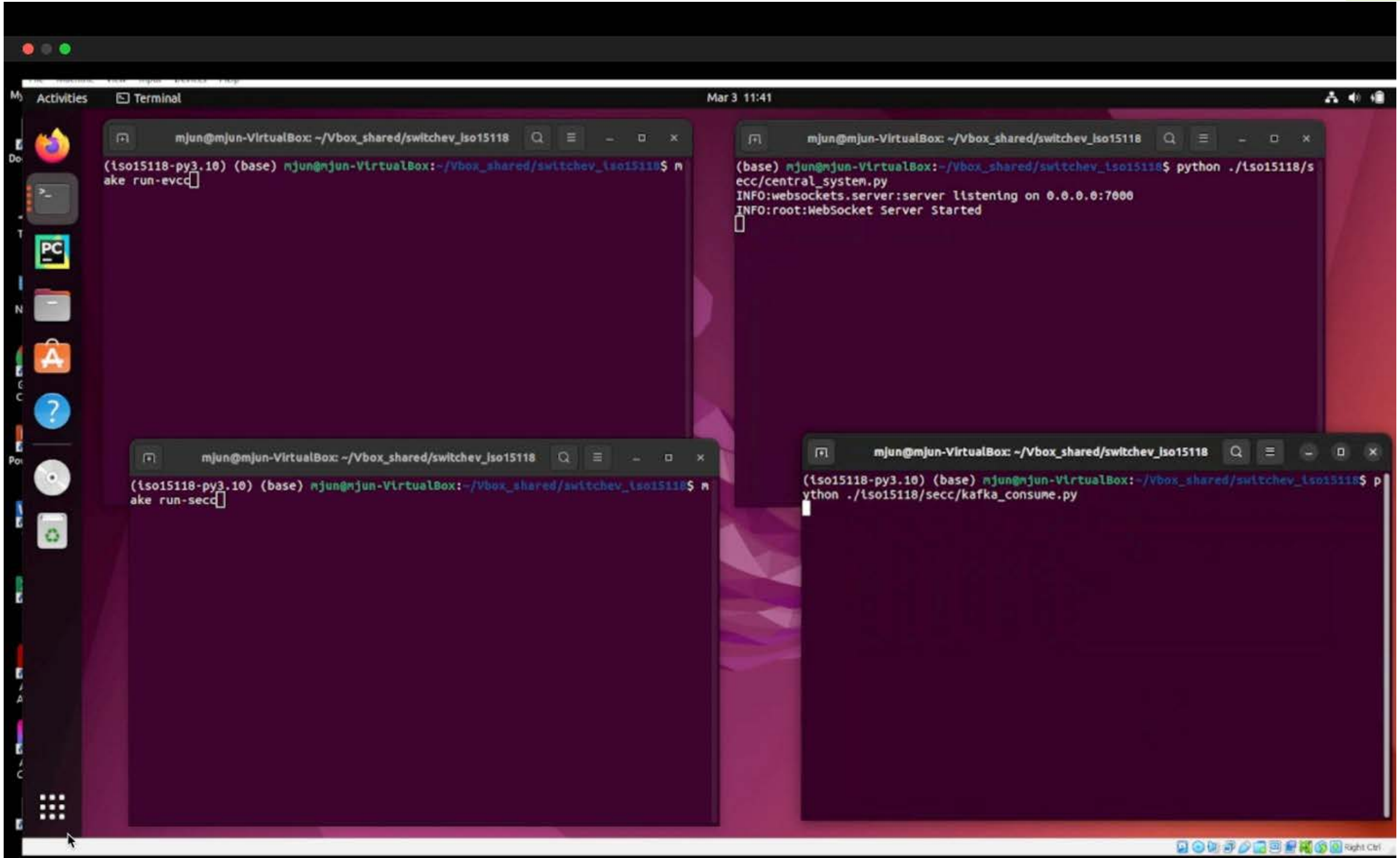


Name ↑	Status	Topology	Scenario	Start Time	VMs	VLANs	Actions
main	started	main	main	2024-02-16T07:58:49-07:00	72	101 - 122 (22)	

Copyright © **2019-2022 Sandia National Laboratories**. All Rights Reserved.

Version d023308 (built on Tue Feb 6 23:19:30 UTC 2024)

Protocol Implementation



```
(iso15118-py3.10) (base) mjun@mjun-VirtualBox:~/Vbox_shared/switchev_iso15118$ m
ake run-evcc
```

```
(base) mjun@mjun-VirtualBox:~/Vbox_shared/switchev_iso15118$ python ./iso15118/s
ecc/central_system.py
INFO:websockets.server:server listening on 0.0.0.0:7000
INFO:root:WebSocket Server Started
```

```
(iso15118-py3.10) (base) mjun@mjun-VirtualBox:~/Vbox_shared/switchev_iso15118$ m
ake run-secc
```

```
(iso15118-py3.10) (base) mjun@mjun-VirtualBox:~/Vbox_shared/switchev_iso15118$ p
ython ./iso15118/secc/kafka_consume.py
```

Interoperability vs. Cybersecurity

- Many industry test events focus on interoperability
- The goal of this environment is to focus on the cybersecurity aspects
- Cybersecurity must be thought about first

Testing the Public Key Infrastructure

- Due to widespread adoption, testing the PKI was prioritized
- Revocation was identified as a potential issue
- Risk-focused testing

Scenario: Revocation of certificates using different PKIs using two separate certificate revocation lists (CRLs). In this scenario, each PKI manages its own CRL that must be downloaded to each participant’s devices.

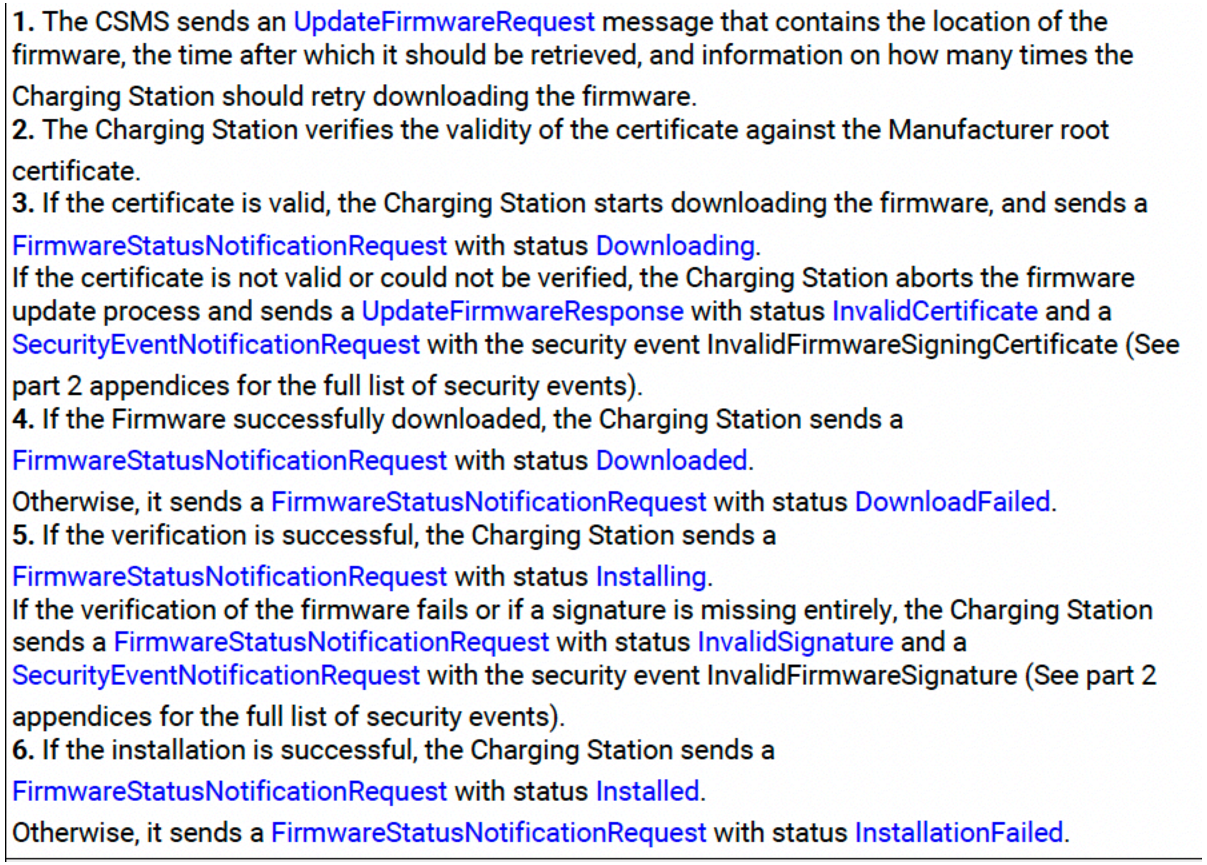
Next Steps

Multi-PKI Testing Strategies

- Findings from the integration of multi-root architecture in environment
- Recommend mitigation strategies for risks found
- Publication slated for end of September.

Firmware Updates

- OCPP enables secure firmware updates
- Ensures the firmware update cannot be tampered
- Key for deploying cybersecurity updates for aging hardware



1. The CSMS sends an UpdateFirmwareRequest message that contains the location of the firmware, the time after which it should be retrieved, and information on how many times the Charging Station should retry downloading the firmware.
2. The Charging Station verifies the validity of the certificate against the Manufacturer root certificate.
3. If the certificate is valid, the Charging Station starts downloading the firmware, and sends a FirmwareStatusNotificationRequest with status Downloading.
If the certificate is not valid or could not be verified, the Charging Station aborts the firmware update process and sends a UpdateFirmwareResponse with status InvalidCertificate and a SecurityEventNotificationRequest with the security event InvalidFirmwareSigningCertificate (See part 2 appendices for the full list of security events).
4. If the Firmware successfully downloaded, the Charging Station sends a FirmwareStatusNotificationRequest with status Downloaded.
Otherwise, it sends a FirmwareStatusNotificationRequest with status DownloadFailed.
5. If the verification is successful, the Charging Station sends a FirmwareStatusNotificationRequest with status Installing.
If the verification of the firmware fails or if a signature is missing entirely, the Charging Station sends a FirmwareStatusNotificationRequest with status InvalidSignature and a SecurityEventNotificationRequest with the security event InvalidFirmwareSignature (See part 2 appendices for the full list of security events).
6. If the installation is successful, the Charging Station sends a FirmwareStatusNotificationRequest with status Installed.
Otherwise, it sends a FirmwareStatusNotificationRequest with status InstallationFailed.

Bug Bounty Prize Program

- Building on prior experience in prize programs, NREL is facilitating a bug bounty program for EVSE

- NREL, using current capabilities and resources, will provide technical assistance to the program participants

- The feasibility study on the program is in development, subject to change, with the goal to launch in FY25

Thank You

Ryan.Cryar@nrel.gov

www.nrel.gov

NREL/PR-5T00-90408

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided in part by U.S. Department of Energy and U.S. Department of Transportation Joint Office of Energy and Transportation and U.S. Department of Energy Vehicle Technologies Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

Photo from iStock-627281636

NREL
Transforming ENERGY