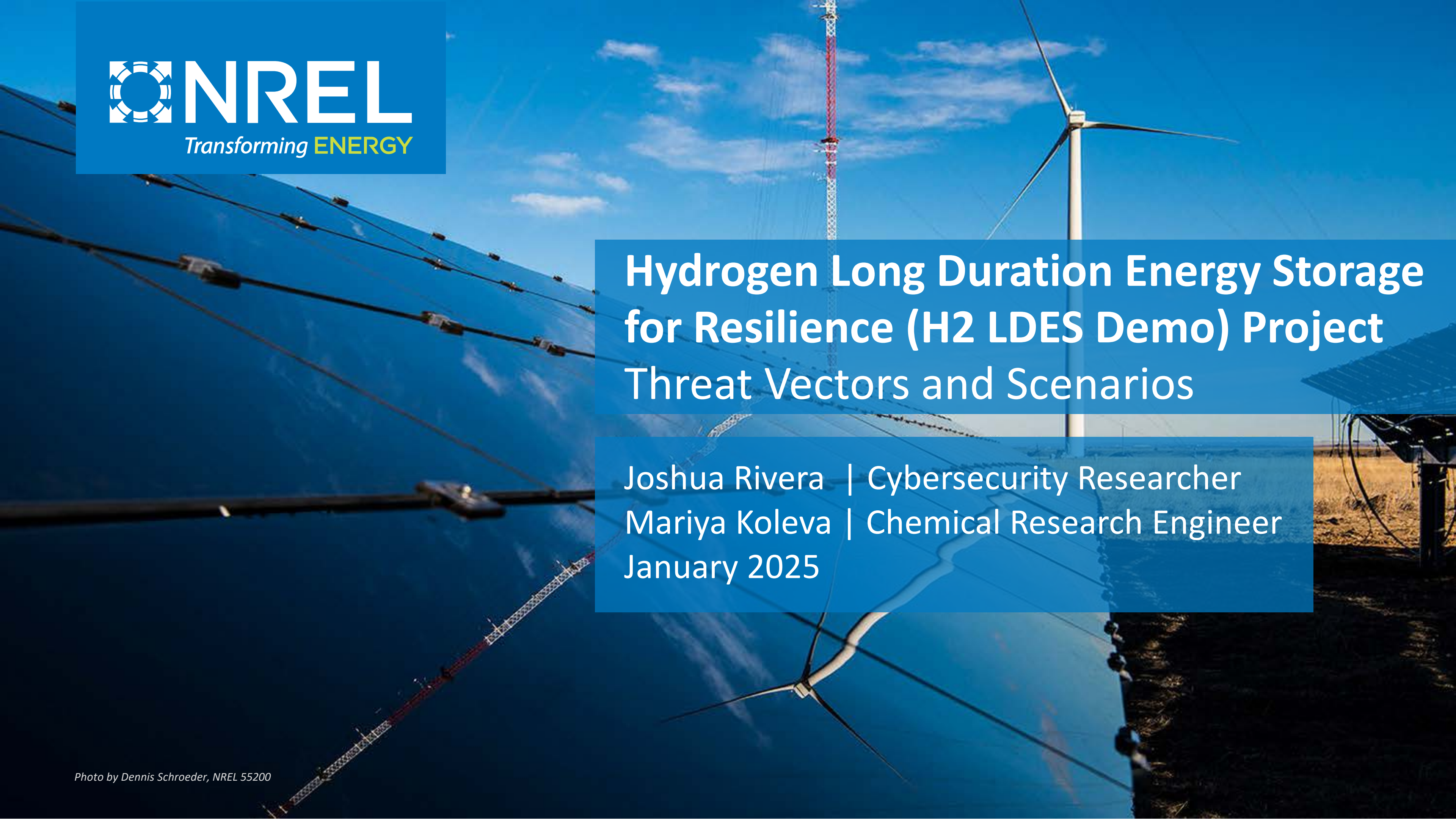


NREL
Transforming ENERGY

Hydrogen Long Duration Energy Storage for Resilience (H2 LDES Demo) Project

Threat Vectors and Scenarios

Joshua Rivera | Cybersecurity Researcher
Mariya Koleva | Chemical Research Engineer

January 2025

Photo by Dennis Schroeder, NREL 55200

Hydrogen LDES Demo Project Objectives

Project objectives

- Meet resilience goals for a diversified portfolio of policies and agencies by demonstrating that the hydrogen-based long duration energy storage (LDES) system on Flatirons campus can provide 24+ hours of backup power of at least 500 kW
- Develop and validate a high-fidelity simulation model of the system
- Strategize system replication, simulation and deployment at potential sites across multiple geographical locations
- Evaluate the cybersecurity considerations of a generalized real-world hydrogen-based LDES system

Cybersecurity Assessment Goals and Objectives

Goals

- Raise awareness of threat vectors that may exist in the hydrogen LDES system
- Inform cybersecurity best practices and secure-by-design principles outlined in DOE's National Cyber-Informed Engineering Strategy*

Cybersecurity assessment objectives

- Discover system integration components of a hydrogen system
- Identify threat scenarios through the lens of the Cyber Kill Chain in conjunction with the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework
- Determine an approach for security controls and mitigations
- Determine and inform secure-by-design choices in the context of cyber-informed engineering (CIE)

*DOE, National Cyber-Informed Engineering Strategy from the U.S. Department of Energy, 2022, available at https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf

H2 LDES Cybersecurity Assessment Steps

Discovery: Identify parts that comprise the H2 LDES system (assets, components) as well as system diagrams and models that help inform the scenario

Planning: Determine the perspective from which the H2 LDES cybersecurity assessment will be performed (Research Capability/Real-Life System)

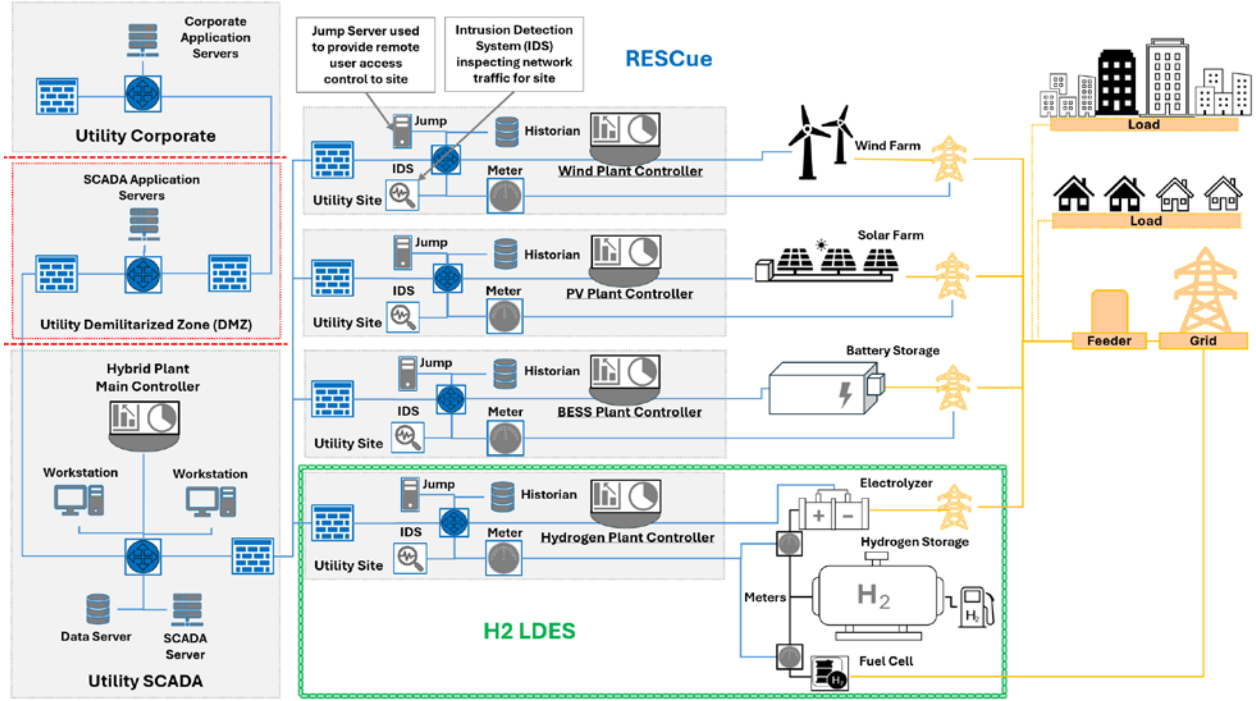
Analysis: Leverage cybersecurity frameworks, compliance standards/regulations, and controls to identify gaps in cybersecurity across the system

Threats and Mitigations: Considering the Cyber Kill Chain and the MITRE ATT&CK framework, identify threat scenarios and ramifications of incidents and events, as well as present a comprehensive mitigation strategy

Secure by Design and Best Practices: Adopt the U.S. Department of Energy (DOE)'s established secure-by-design principles through a Cyber-Informed Engineering (CIE) approach for energy systems

Community Engagement: Establish communication pathways through technical reporting, publications, and/or webinars for community engagement focused on cybersecurity for hydrogen and battery storage systems

Hydrogen LDES Load Provision Architecture



- Work based on the **Renewable Energy and Storage Cybersecurity Research (RESCue)** pilot effort*
- Backup power generation fulfilled by hydrogen LDES system (i.e., controller, historian, meters, electrolyzer, storage, and fuel cell) integration with microgrids and loads
- More generic cases and applications addressed, such as transmission back to grid
- Analysis introduces emerging threat scenarios and mitigations specific to hydrogen LDES systems

*NREL, Renewable Energy and Storage Cybersecurity Research (RESCue) Pilot Final Report, 2024, available at https://www.nrel.gov/docs/fy24osti/89921.pdf

Hydrogen LDES System Components & Threat Vectors

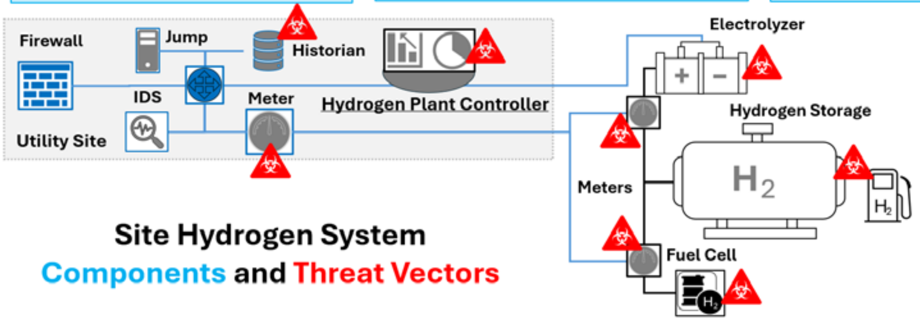
- A series of different **threat vectors** may exist within a utility site based on mal configuration or lack of security control among systems, networks, and applications
- Integrating components through communication networks as well as running software and application layer protocols can introduce potential vulnerabilities or security breaches
- Security strategy, controls, and design must be considered for such systems, networks, and applications

Utility Site: A utility site for hydrogen controls is a facility designed to produce, store, and distribute hydrogen, often integrating hydrogen into the broader energy grid. It typically involves the use of electrolyzers, hydrogen storage, fuel cells, and other components that are closely monitored and controlled to ensure safe, efficient, and reliable operations.

Historian: Stores and retrieves large volumes of historical data from various plant systems for analysis, reporting, and optimization.

Hydrogen Plant Controller: Centralized system for controlling and managing hydrogen production, including electrolyzers, storage, and fuel cells.

Electrolyzer: Uses electricity to split water into hydrogen and oxygen, producing hydrogen gas for energy storage and fuel.



Site Hydrogen System
Components and Threat Vectors

Hydrogen Storage: Safely stores hydrogen gas for later use in vehicles, power generation, or other industrial applications.

Fuel Cell: Converts hydrogen into electricity, used for clean energy production in various applications.

Energy Meter: Measures electrical energy use or generation. Electrolyzers (electricity consumption), Fuel Cells (electricity generation), Hydrogen Storage (energy use for compression).

Temperature Meter: Measures temperature of systems. Electrolyzers (temperature control), Hydrogen Storage (safety monitoring), Fuel Cells (thermal management).

Flow Meter: Measures the flow rate of gases (hydrogen, oxygen). Electrolyzers (hydrogen production), Fuel Cells (hydrogen consumption), Hydrogen Storage (filling/dispensing).

Pressure Meter: Measures the pressure of hydrogen gas. Hydrogen Storage (pressure regulation), Electrolyzers (internal pressure monitoring), Fuel Cells (hydrogen supply pressure).

Hydrogen Purity Meter: Hydrogen purity meters measure the composition of hydrogen gas, determining the percentage of hydrogen in the gas mixture. Ensuring that the hydrogen is of the correct purity is critical for both safety and the performance of fuel cells and other end-use applications.

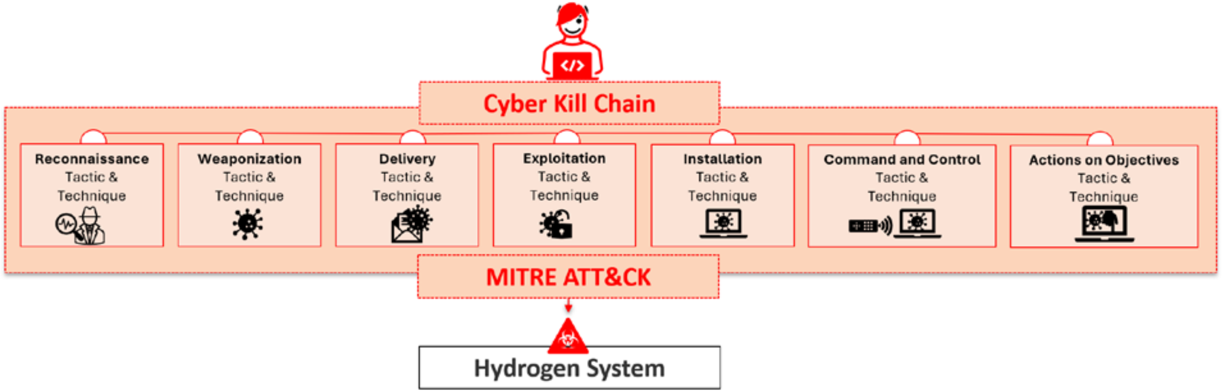
Leak Detection Meter: Leak detection meters are used to monitor for potential hydrogen leaks in the system, a critical safety measure due to hydrogen's flammability and explosiveness in certain concentrations.

The ramifications of a series of cyberattacks taking place on a hydrogen LDES system can be disruptive, or even destructive, depending on the threat actor's objectives

Hydrogen Threat Analysis Method

Method combines 2 strategies:

- **Cyber Kill Chain** provides valuable insights into how adversaries may execute threat scenarios targeting these systems*
- **MITRE ATT&CK** framework helps deduce and evaluate the potential tactics, techniques, and procedures (TTPs) that threat actors may employ against critical components of hydrogen infrastructure**



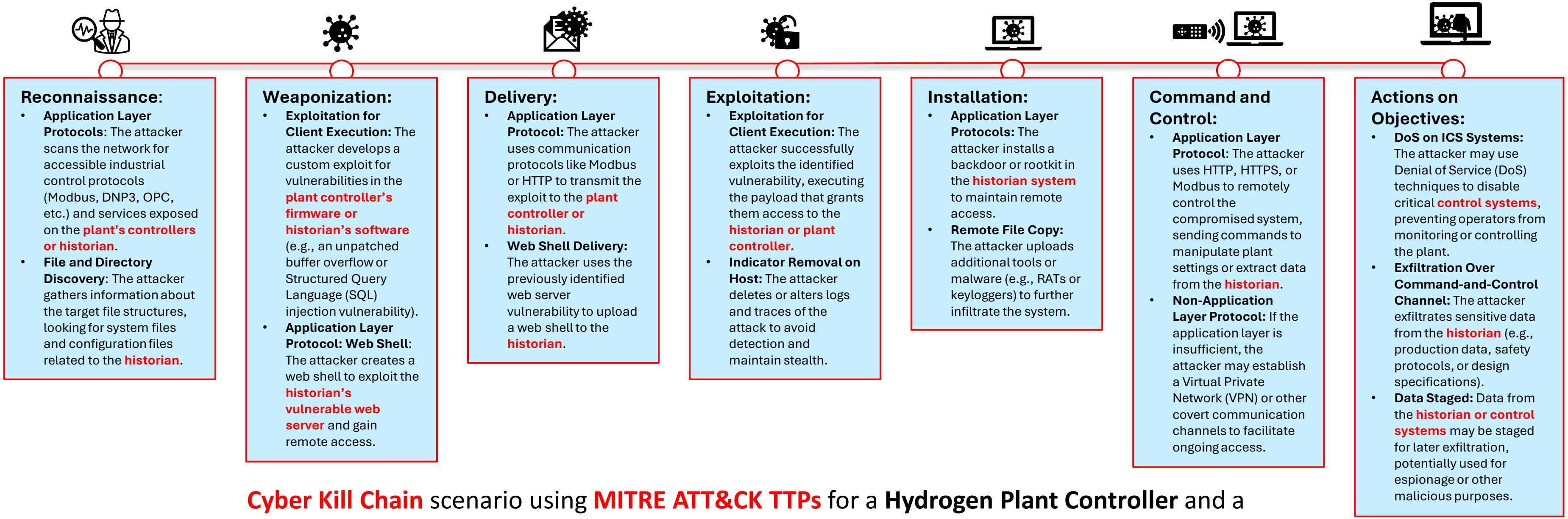
Cyber Kill Chain
Reconnaissance Tactic & Technique
Weaponization Tactic & Technique
Delivery Tactic & Technique
Exploitation Tactic & Technique
Installation Tactic & Technique
Command and Control Tactic & Technique
Actions on Objectives Tactic & Technique
MITRE ATT&CK
Hydrogen System

*Lockheed Martin Corporation, The Cyber Kill Chain, 2024, available at https://attack.mitre.org/

*The MITRE Corporation, MITRE ATT&CK, 2024, available at https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Hydrogen Threat Scenario | Controls and Data

The **threat scenario** below, although hypothetical in the context of this analysis, helps bring insights into how threat actors might advance on a hydrogen system's **Plant Controller and/or Data Historian**.



Reconnaissance:

- **Application Layer Protocols**: The attacker scans the network for accessible industrial control protocols (Modbus, DNP3, OPC, etc.) and services exposed on the **plant's controllers or historian**.
- **File and Directory Discovery**: The attacker gathers information about the target file structures, looking for system files and configuration files related to the **historian**.

Weaponization:

- **Exploitation for Client Execution:** The attacker develops a custom exploit for vulnerabilities in the **plant controller's firmware or historian's software** (e.g., an unpatched buffer overflow or Structured Query Language (SQL) injection vulnerability).
- **Application Layer Protocol: Web Shell**: The attacker creates a web shell to exploit the **historian's vulnerable web server** and gain remote access.

Delivery:

- **Application Layer Protocol:** The attacker uses communication protocols like Modbus or HTTP to transmit the exploit to the **plant controller or historian**.
- **Web Shell Delivery:** The attacker uses the previously identified web server vulnerability to upload a web shell to the **historian**.

Exploitation:

- **Exploitation for Client Execution:** The attacker successfully exploits the identified vulnerability, executing the payload that grants them access to the **historian or plant controller.**
- **Indicator Removal on Host:** The attacker deletes or alters logs and traces of the attack to avoid detection and maintain stealth.

Installation:

- **Application Layer Protocols:** The attacker installs a backdoor or rootkit in the **historian system** to maintain remote access.
- **Remote File Copy:** The attacker uploads additional tools or malware (e.g., RATs or keyloggers) to further infiltrate the system.

Command and Control:

- **Application Layer Protocol**: The attacker uses HTTP, HTTPS, or Modbus to remotely control the compromised system, sending commands to manipulate plant settings or extract data from the **historian**.
- **Non-Application Layer Protocol:** If the application layer is insufficient, the attacker may establish a Virtual Private Network (VPN) or other covert communication channels to facilitate ongoing access.

Actions on Objectives:

- **DoS on ICS Systems:** The attacker may use Denial of Service (DoS) techniques to disable critical **control systems**, preventing operators from monitoring or controlling the plant.
- **Exfiltration Over Command-and-Control Channel:** The attacker exfiltrates sensitive data from the **historian** (e.g., production data, safety protocols, or design specifications).
- **Data Staged:** Data from the **historian or control systems** may be staged for later exfiltration, potentially used for espionage or other malicious purposes.

Cyber Kill Chain scenario using **MITRE ATT&CK TTPs** for a **Hydrogen Plant Controller** and a **Data Historian**, outlining each phase of the attack and how threat actors might advance on a hydrogen system.

Hydrogen Threat Scenario | Device Applications

The **threat scenario** below, although hypothetical in the context of this analysis, helps bring insights into how threat actors might advance on a hydrogen system's cyber-physical system, such as the **Electolyzer, Hydrogen storage, and/or Fuel Cell**.

Reconnaissance:

- **Application Layer Protocol (Web):** The attacker gathers information by scanning and probing systems, looking for open ports and communication protocols (e.g., HTTP, HTTPS) to identify vulnerabilities in remote access systems, such as SCADA interfaces used to manage **electrolyzers or fuel cells**.
- **Active Scanning**: Attackers scan for systems connected to the plant's network, seeking vulnerabilities. They might also look for networked **meters, plant controllers, or historian systems.**
- **Account Discovery (Local Account):** The attacker discovers user accounts and roles (e.g., admin/operator) to target for credential theft or privilege escalation.

Weaponization:

- **Application Layer Protocol (DNS):** The attacker creates a weaponized exploit (e.g., malware) designed to exploit a vulnerability found in the **hydrogen systems**.
- **Exploitation for Privilege Escalation:** The attacker crafts an exploit to target system vulnerabilities and gain privileged access to the system.

Delivery:

- **Application Layer Protocol (Web):** The attacker delivers a malicious payload via a web interface or remote access to interact with the **electrolyzer, storage, or fuel cell**.
- **Drive-by Compromise:** The attacker may deliver malicious code through phishing or by compromising a website, affecting Supervisory Control and Data Acquisition (SCADA)/Human Machine Interface (HMI) interfaces.

Exploitation:

- **Command and Scripting Interpreter (PowerShell):** The attacker uses PowerShell or similar scripts to execute code on the compromised systems and alter settings of **electrolyzers**.
- **Exploitation for Privilege Escalation:** The attacker leverages unpatched software vulnerabilities in Programmable Logic Controller **(PLC) systems** to execute unauthorized commands on the systems.

Installation:

- **Create or Modify System Process (WMI):** Attacker installs persistent malware or backdoors (e.g., RATs) on **meters, historians, or controllers** to ensure long-term access.
- **Application Layer Protocol (RDP):** The attacker installs RDP backdoors to maintain persistent access to remote systems like electrolyzers or storage systems.

Command and Control:

- **Application Layer Protocol (Web):** The attacker uses HTTP or HTTPS protocols to send commands to compromised devices (e.g., **electrolyzer or fuel cell**).
- **Application Layer Protocol (RDP):** The attacker establishes a remote command-and-control channel (e.g., via RDP or DNS tunneling) to manage compromised systems.

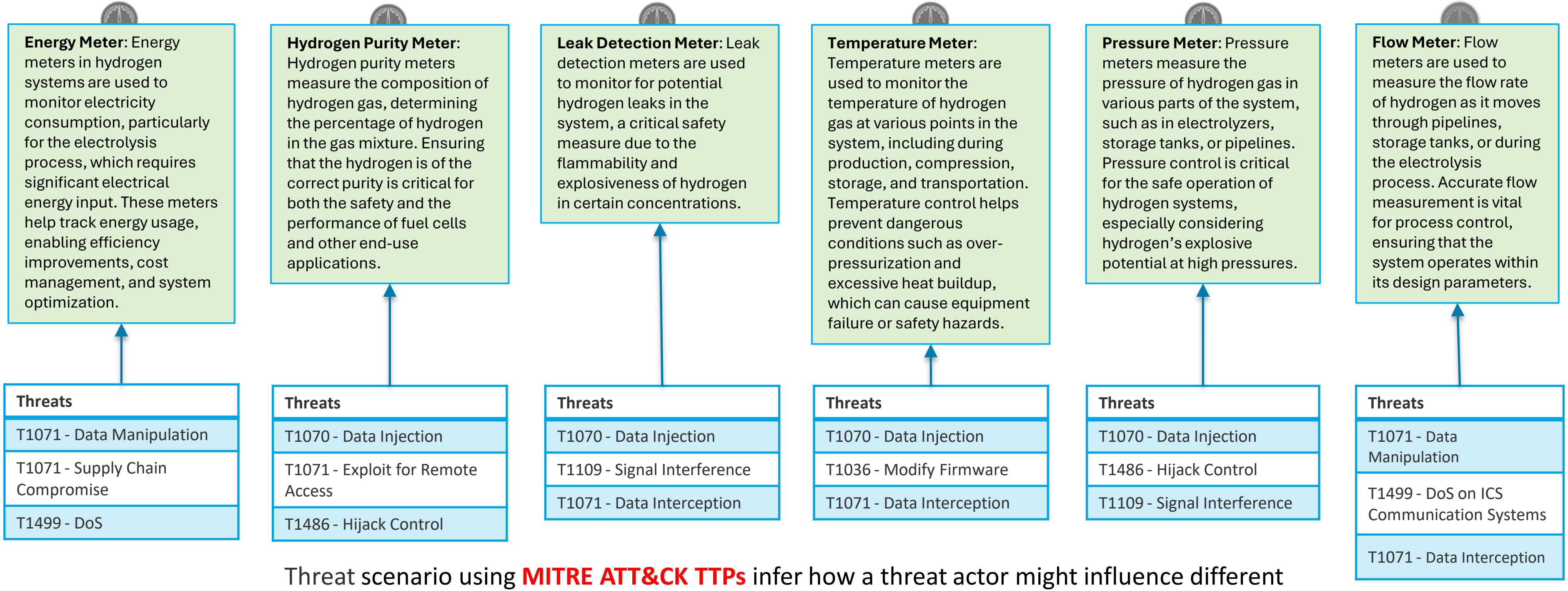
Actions on Objectives:

- **Resource Hijacking:** The attacker hijacks **control of the electrolyzer** to disrupt or manipulate energy production, causing harm to the system.
- **File Deletion:** The attacker deletes logs or other critical files to erase traces of their actions and evade detection.
- **Application Layer Protocol (DNS)**: The attacker uses DNS tunneling to exfiltrate sensitive data from the **storage or control systems**.
- **Application Layer Protocol (Web):** Data exfiltration occurs over the web or using SCADA system vulnerabilities, targeting sensitive control data.

Cyber Kill Chain threat scenario using **MITRE ATT&CK TTPs** against **Hydrogen System (Electrolyzer, Storage, and Fuel Cell)**, outlining each phase of the attack and how it applies to a hydrogen system.

Hydrogen Threat Scenarios | Metering Data

The **threat scenarios** below, although hypothetical in the context of this analysis, helps bring insights into how threat actors might advance on a hydrogen system's **Metering infrastructure**.



Energy Meter: Energy meters in hydrogen systems are used to monitor electricity consumption, particularly for the electrolysis process, which requires significant electrical energy input. These meters help track energy usage, enabling efficiency improvements, cost management, and system optimization.

Threats
T1071 - Data Manipulation
T1071 - Supply Chain Compromise
T1499 - DoS

Hydrogen Purity Meter: Hydrogen purity meters measure the composition of hydrogen gas, determining the percentage of hydrogen in the gas mixture. Ensuring that the hydrogen is of the correct purity is critical for both the safety and the performance of fuel cells and other end-use applications.

Threats
T1070 - Data Injection
T1071 - Exploit for Remote Access
T1486 - Hijack Control

Leak Detection Meter: Leak detection meters are used to monitor for potential hydrogen leaks in the system, a critical safety measure due to the flammability and explosiveness of hydrogen in certain concentrations.

Threats
T1070 - Data Injection
T1109 - Signal Interference
T1071 - Data Interception

Temperature Meter: Temperature meters are used to monitor the temperature of hydrogen gas at various points in the system, including during production, compression, storage, and transportation. Temperature control helps prevent dangerous conditions such as over-pressurization and excessive heat buildup, which can cause equipment failure or safety hazards.

Threats
T1070 - Data Injection
T1036 - Modify Firmware
T1071 - Data Interception

Pressure Meter: Pressure meters measure the pressure of hydrogen gas in various parts of the system, such as in electrolyzers, storage tanks, or pipelines. Pressure control is critical for the safe operation of hydrogen systems, especially considering hydrogen's explosive potential at high pressures.

Threats
T1070 - Data Injection
T1486 - Hijack Control
T1109 - Signal Interference

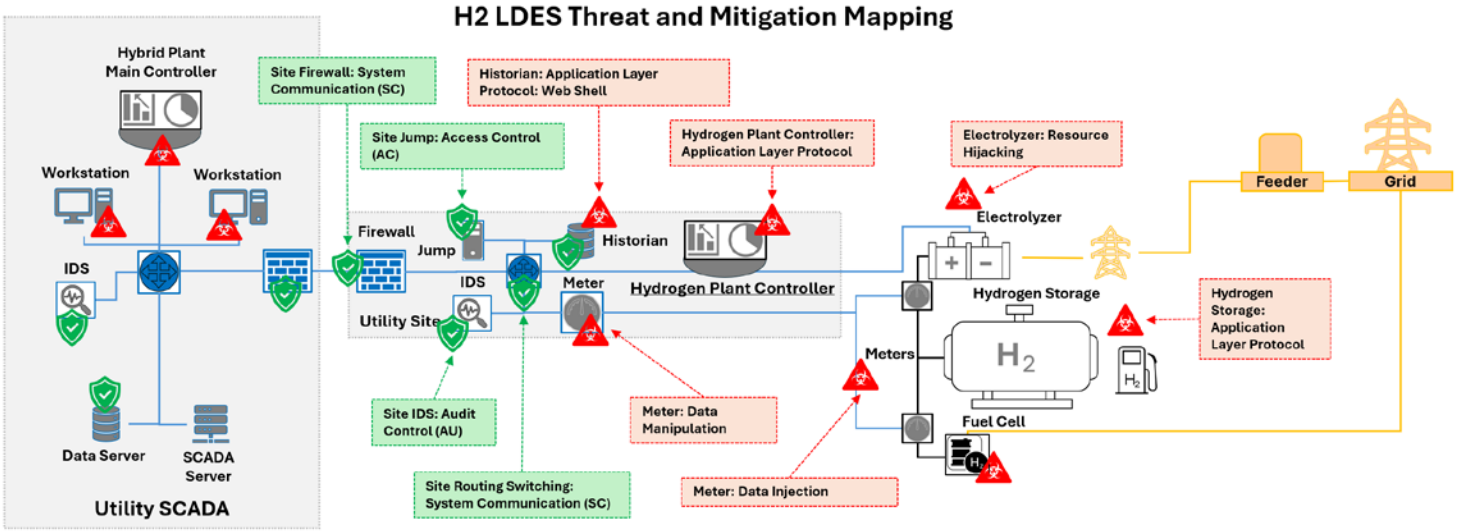
Flow Meter: Flow meters are used to measure the flow rate of hydrogen as it moves through pipelines, storage tanks, or during the electrolysis process. Accurate flow measurement is vital for process control, ensuring that the system operates within its design parameters.

Threats
T1071 - Data Manipulation
T1499 - DoS on ICS Communication Systems
T1071 - Data Interception

Threat scenario using **MITRE ATT&CK TTPs** infer how a threat actor might influence different **Meters** across a hydrogen system.

Initial Hydrogen Threat and Mitigation Mapping

This initial assessment is not a complete mapping of threat and mitigations of hydrogen LDES systems. This mapping is more of a thought exercise between hydrogen system engineers and cybersecurity analysts.



H2 LDES Threat and Mitigation Mapping
Hybrid Plant Main Controller
Workstation
Workstation
IDS
Data Server
SCADA Server
Utility SCADA
Site Firewall: System Communication (SC)
Site Jump: Access Control (AC)
Historian: Application Layer Protocol: Web Shell
Hydrogen Plant Controller: Application Layer Protocol
Electrolyzer: Resource Hijacking
Firewall
Jump
Historian
IDS
Meter
Hydrogen Plant Controller
Utility Site
Site IDS: Audit Control (AU)
Site Routing Switching: System Communication (SC)
Meter: Data Manipulation
Meter: Data Injection
Electrolyzer
Hydrogen Storage
Meters
Fuel Cell
H_2
Hydrogen Storage: Application Layer Protocol
Feeder
Grid

The diagram above:

- Demonstrates a viable approach toward identifying threats and applying cybersecurity design choices with a focus on threat mitigation.
- Intends to illustrate the convergence between security controls and threat scenarios against hydrogen LDES systems; as such, hydrogen system engineers and cybersecurity analysts can assess the system holistically when making design choices.

Hydrogen Secure by Design Transition

Next steps

- Bring clarity to defense posturing, security controls, best practices, and secure-by-design principles
- Provide insight into how hydrogen system engineers and cybersecurity analysts should think about and approach system, network, and application security

Secure by Design Engineering Transition and Mindset

The goal is to transition away from the cherry-on-top cybersecurity approach and considerations to a cherry-flavored approach, thought process, and design choices.

Acknowledgements

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. OCED-IIJA/AL16/24/IIJA. Funding provided by U.S. Department of Energy Office of Clean Energy Demonstrations. 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.

Thank you!

www.nrel.gov

NREL/PR-5700-92485

Photo from iStock-627281636

NREL Transforming ENERGY

45Th anniversary