DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

Cybersecurity Considerations for Hydrogen Infrastructure in Airport Environments

Dana Hatic, Anuj Sanghvi, Joshua Rivera, Scott Cary, and Kazunori Nagasawa

National Renewable Energy Laboratory

Produced under direction of the Federal Aviation Administration (FAA) Office of Airports by the National Renewable Energy Laboratory (NREL) under Interagency Agreement IAG-20-17011-14.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated under Contract No. DE-AC36-08GO28308

This report is available at no cost from NREL at www.nrel.gov/publications.

Strategic Partnership Project Report
NREL/TP- 5T00-91867
June 2025

Cybersecurity Considerations for Hydrogen Infrastructure in Airport Environments

Dana Hatic, Anuj Sanghvi, Joshua Rivera, Scott Cary, and Kazunori Nagasawa

National Renewable Energy Laboratory

Suggested Citation
Hatic, Dana, Anuj Sanghvi, Joshua Rivera, Scott Cary, and Kazunori Nagasawa. 2025. *Cybersecurity Considerations for Hydrogen Infrastructure in Airport Environments*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5T00-91867. https://www.nrel.gov/docs/fy25osti/91867.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated under Contract No. DE-AC36-08GO28308

This report is available at no cost from NREL at www.nrel.gov/publications.

Strategic Partnership Project Report
NREL/TP- 5T00-91867
June 2025

15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

Acknowledgments

The authors acknowledge the sponsorship of the Federal Aviation Administration (FAA) Airport Technology Research and Development Branch Airport Safety (ANG-E261), which has enabled the collection of the content and assessments incorporated within this technical publication. We also appreciate the leadership of Russ Gorman from the FAA in providing focus to this work. The review comments from FAA team members—including Jeremy Casey, Darian Byrd, Wesley Major, and Jonathan Torres—were key to providing a quality outcome relevant to the FAA mission.

List of Acronyms

CAN	Controller Area Network
DER-CF	Distributed Energy Resource Cybersecurity Framework
DNP3	Distributed Network Protocol 3
FAA	Federal Aviation Administration
H2 LDES	Hydrogen Long Duration Energy Storage
HMI	human-machine interface
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IT	information technology
NIST	National Institute of Standards and Technology (NIST)
NREL	National Renewable Energy Laboratory
OCPP	Open Charge Point Protocol
OT	operational technology
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
TLS	Transport Layer Security

Executive Summary

Efforts to pursue additional fueling pathways for aircraft and aviation infrastructures are in the early stages, including research into electrifying through hydrogen power applications. Companies such as Airbus, ZeroAvia, and Joby Aviation are actively developing scalable hydrogen-powered aircraft, with agreements to provide aircraft and fueling infrastructure for commercial flight within the next 20 years.

Hydrogen-powered aircraft and relevant hydrogen fuel infrastructure depend on interconnected digital components for sustaining operations. These infrastructures are subject to existing regulations and standards, including those governing cybersecurity of advanced fuel, power generation, and transportation systems. Cybersecurity concerns center on the key functions of these cyber-physical systems (e.g., communications, control, and interoperability). Rapid changes in cybersecurity threats and system designs provide adversaries asymmetric advantage to disrupt, degrade, or deny operation of cyber-physical systems, so new strategies that mitigate the impacts of successful cyber events and enhance resilience of energy and transportation infrastructure are needed.

This report explores key cybersecurity concerns and best practices within aviation environments that can provide a baseline for the development of hydrogen fueling infrastructure. This analysis leverages prior National Renewable Energy Laboratory studies on: (1) hydrogen fueling station component validation to identify vulnerabilities and failure events documented in physical equipment; and (2) electric aircraft charging infrastructure analysis to explore primary cybersecurity vulnerabilities. It reviews the criticality of digital technologies in sustaining hydrogen fuel production, storage, and fueling systems, noting general cybersecurity concerns to power and industrial control systems, and for aviation, including the following:

- Engaging stakeholders (e.g., aircraft manufacturers, electric utilities, site property owners, and local communities) to inform decision-making regarding future hydrogen fueling infrastructure (e.g., site infrastructure, operations, and resources) to understand operational needs and cybersecurity awareness, including workforce education.
- Identifying gaps in existing codes and standards to help inform the development of baselines for assessing hydrogen-powered aviation cybersecurity postures or for establishing best practices at the outset of infrastructure planning stages.
- Developing cybersecurity mitigation strategies that consider physical attack vectors that emerge with the integration of hydrogen systems into existing airport security requirements.

The cybersecurity assessment in this report yields an understanding of risk that can be understood in comparison with other challenges involved in electric transportation, including vulnerabilities related to compromised access or communications within a supervisory control and data acquisition system. Based on this preliminary analysis, gaps in the scale and complexity of cybersecurity risks within hydrogen fuel infrastructure for aviation require further research to help stakeholders, engineers, or strategists understand connections, criticalities, and standard practices when designing and planning for new systems. In this nascent phase of hydrogen-fueled aviation development, assessing how to integrate cybersecurity best practices into an evolving U.S. aviation landscape provides critical insights into building increased awareness and stakeholder engagement to support cyber-resilient infrastructure.

Table of Contents

List of Figures

List of Tables

1 Introduction

Hydrogen power for transportation is a burgeoning area of innovation. Companies within the United States and abroad have made agreements with federal agencies, airports, and other private entities to plan for the integration of hydrogen-fueled aircraft into aviation infrastructure at varying scales. Airbus has several working agreements under its ZEROe project to deliver multiple design options for hydrogen-powered aircraft with the appropriate supporting infrastructure for refueling (Airbus 2024). The British-American company ZeroAvia has earned financing and grants to pursue hydrogen aviation projects, including one grant from the Federal Aviation Administration (FAA) to test and validate its hydrogen-electric powertrain system (ZeroAvia 2024). Amid these developments, significant uncertainty exists in the cybersecurity risks posed by novel aviation technologies, and this report draws inferences on potential common-mode risks associated with the related fields of battery-powered electric vehicles and electric vehicle supply equipment.

Answering these questions first requires a vision of what the infrastructure for hydrogen-powered aircraft might look like in the United States, including the digital components, physical integrations, site layouts, and existing regulations and standards that will come into play during development. Second, the question of cybersecurity draws upon the key functions of cyber-physical systems, including communications, control, and interoperability, as well as associated adverse impacts that are critical to avoid. Third, it is necessary to understand the landscape of threats as they relate to the cybersecurity of electrical energy systems. Although the potential impacts for cyberattacks on energy infrastructure and connected transportation channels are significant—as demonstrated in the 2017 NotPetya attack that disrupted Ukrainian energy infrastructure and global shipping (Hauet et al. 2017), the attack on Iran's nuclear centrifuges in the late 2000s (Zetter 2014), the Colonial Pipeline attack in 2021 (Easterly 2023), and the repeated critical infrastructure attacks perpetrated by Volt Typhoon (CISA 2024)—mitigation strategies and methods for enhancing resilience can benefit any kind of failure scenario, not just cyber-induced failures.

This report provides a high-level assessment of cybersecurity concerns and best practices for consideration in the development of hydrogen fueling infrastructure in airport environments. Section 2 defines critical functions and classifications of system functions. Section 3 describes methods of cybersecurity risk assessments and mitigations. Finally, Section 4 summarizes the findings and future work.

2 Methods

This report analyzes mitigations of cybersecurity vulnerabilities within hydrogen applications for aviation. Analysis begins with defining critical functions in the processes of production, storage, and fueling infrastructure for hydrogen electrolysis systems. It then classifies those functions according to cybersecurity standards and maps the criticality of these functions to permit further analysis of potential physical and digital structures that are necessary for cyber-resilient systems. These sections provide the basis for the subsequent cybersecurity risk assessment, and they describe the current standards that are relevant to future infrastructure planning.

2.1 Defining Critical Functions

The key capabilities required for hydrogen fueling infrastructure in aviation comprise hydrogen production, bulk storage, and dispensing systems. Each segment of the process contains critical automated functions and system boundaries that present potential cybersecurity vulnerabilities. The following sections offer an overview of the mechanical and digital technologies that are expected to be integrated into the processes that are required to support hydrogen as a fuel source for aircraft. Note that any future hydrogen fueling system in the aviation sector will be site-specific, with the function-level configurations and site layouts tailored on a case-by-case basis to accommodate the needs of individual sites. Describing the functions in general terms helps inform the cybersecurity risk analyses conducted on individual sites, as appropriate, to determine the efficacy of cyber-defense structures.

2.1.1 Hydrogen Production Systems

This cybersecurity analysis focuses on the electrolysis method of hydrogen production for applications in transportation, due to the current prevalence of electrolysis systems in hydrogen fuel production for use in the electric grid at scale. Electrolysis uses electricity to split water into hydrogen and oxygen, which requires an initial energy source alongside the following components: a deionized water tank; an electrolyzer stack; pressure tanks for hydrogen storage; water separators; cooling systems; and various vents, valves, sensors, and meters. Figure 10 (Section 3.4: Functional Architecture for Hydrogen Fueling Infrastructure) shows a process flow diagram detailing the interconnections among these components. At the scale of hydrogen delivery and transport, hydrogen pipeline networks or hydrogen blending into natural gas pipelines should be considered (Topolski et al. 2022).

2.1.2 Hydrogen Bulk Storage Systems

Hydrogen storage systems have critical monitoring technologies to prevent the rapid uncontrolled release of hydrogen. The physical safety systems include pressurized gaseous or liquid storage tanks; and various valves, gauges, and flow controls to regulate temperature, pressure, and flow, when transferring hydrogen either into additional storage tanks or into fuel dispensing mechanisms. Further mechanized equipment—such as compressors, pumps, and chillers and/or coolers—maintain the appropriate conditions for hydrogen fueling to improve performance while ensuring physical safety.

2.1.3 Hydrogen Fueling and Dispenser Systems

Early-stage infrastructure for commercial fueling and dispensing in the United States, primarily for fuel cell electric vehicles, provides a basis for understanding the componentry required for

dispensing at a larger scale. As of September 2024, there were 55 hydrogen fueling stations in the United States, with most public fueling stations located in California (DOE 2024). Each station is required to address site-specific safety considerations to ensure the physical safety of the fueling equipment, vehicles, personnel, and customers.

The National Renewable Energy Laboratory (NREL) conducts regular analyses of fueling station components by tracking multiple data points, including fueling times, time between fueling, station availability, and maintenance by equipment type, along with safety reports (Saur et al. 2020). The following components within hydrogen fueling systems are addressed in the reports: air, chiller, compressor, dispenser, electrical, electrolyzer, feedwater, gas management, purifier, storage, and thermal management.

Hydrogen fueling can be conducted with or without communications between a dispenser and a station to provide end-of-fill pressure targets (SAE 2020). With communications, the data collected can inform better fill quality (e.g., achieve a higher state of charge) (Hydrogen Tools 2024). But a lack of inherently secure communications—or in circumstances where communications are interrupted or compromised—could disrupt operations. A granular-level cybersecurity analysis can look at specific digital processes controlling connections to pressurized hydrogen tanks, valves, dispensers, meters, switches, and sensors to observe the potential outcomes of interference with these connections and what, if any, analog fail-safes are in place to prevent incidents.

2.2 Classifying System Functions

The landscape of hydrogen production, storage, and dispenser systems comprises diverse and interconnected technologies that fall into three categories: (1) physical equipment (i.e., hydrogen system assets), (2) operational technology (OT), and (3) information technology (IT). OT and IT are classified as follows according to the National Institute of Standards and Technology (NIST):

- OT includes "programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment)" and "detect or cause a direct change through the monitoring and/or control of devices, processes, and events." This definition covers industrial control systems, building management systems, fire control systems, and physical access control mechanisms (NIST 2018).
- IT is defined as "any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information." This category includes "computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources" (Barker 2003).

Both OT and IT include hardware elements. The integration of OT and IT assets into physical hydrogen production, storage, and dispenser equipment enhances the capacity to control a delicate process even as it presents vectors for cyberattacks. The following sections detail specific hydrogen system assets, digital properties, and system management tools.

2.2.1 Hydrogen System Assets

The physical, cyber-physical, and digital assets across hydrogen production, storage, and dispensing must work in conjunction to ensure the safe and reliable operation of hydrogen

systems, while preventing adverse impacts to personnel and equipment. An advantage of hydrogen systems lies in the wealth of existing safety codes and standards for equipment to prevent and minimize failure events. With the volume of digital processes in hydrogen infrastructure, as well as the anticipated connectivity for integrating hydrogen fueling for aviation on-site with legacy aviation fueling infrastructure, it is critical to ensure that physical safety controls continue to function even in the event of a successful cyberattack due to an exploited cyber vulnerability. This includes devices that may be incorporated into layered defense mechanisms for hydrogen systems, such as safety instrumented systems (SIS). Assets that are likely to be used within hydrogen production via electrolysis, bulk hydrogen storage, and dispensing systems for aviation include physical regulators, cyber-physical assets, and digital components.

2.2.1.1 Physical Regulators

Physical regulators provide personnel tactile controls to directly manage hydrogen fuel systems. Physical regulators include:

- User/maintenance terminals
- Gas management panels
- Couplers, connectors, valves, and dispensers
- Device controllers, including balance-of-plant operation
- Flame-detection ultraviolet radiation/infrared radiation cameras
- Combustible gas detection

2.2.1.2 Cyber-Physical Assets (Field Controllers)

The following assets, often grouped together as supervisory control and data acquisition (SCADA) systems, are critical in the function and automation of industrial control systems. The critical functions of SCADA systems include transmission and communication of data, remote control, data storage, alarms, reporting, and data presentation (Awati and Loshin n.d.). SCADA systems typically include a mix of wired and wireless connections, which require security measures that are commensurate with the criticality of the physical functions. SCADA can include:

- **Programmable logic controllers:** Placed on hardware in the field, these devices communicate directly with sensors and have low communication latency. Safety actions are performed locally, and sensors directly inform decision-making processes. Any attempts to affect sensors or computations require a malicious actor to be local (for off-network programmable logic controllers) and to have a working understanding of the system. Each component of the hydrogen system is designed to have its own suite of sensors and controllers for additional protection and safety distribution.
- **Intelligent electronic devices:** Devices with one or more processors that are used for the communication of data or control between sources, including controllers, digital relays, and electronic multifunction meters (NIST SP 800-82r3) (Stouffer et al. 2023).
- **Remote terminal units (RTUs):** "A computer with radio interfacing used in remote situations where communications via wire is unavailable. Usually used to communicate with remote field equipment. Programmable logic controllers with radio communication capabilities are also used in place of RTUs" (NIST SP 800-82r3) (Stouffer et al. 2023).

- **Process automation controllers:** "A type of computer system, typically rack-mounted, that processes sensor input, executes control algorithms, and computes actuator outputs" (NIST SP 800-82r3) (Stouffer et al. 2023).

2.2.1.3 Digital Properties of Hydrogen Systems

Purely digital properties involved in sustaining the function and security of hydrogen energy systems include:

- **Local area network/wide-area network connections:** While configurations of command-and-control centers for hydrogen production, storage, and fueling systems may vary, there is often a centralization of servers and communications to enable conformance-based decision-making. IT and the digitization of assets for advanced functionalities within such a remote access environment depend on local and/or wide-area networks, which often rely on managed switches, routers, and firewalls.
- **Authentication:** Various methods ensure secure communication between trusted entities. A common framework found in electric vehicle charging infrastructure relies on Transport Layer Security (TLS), in which digital signatures are used for message exchange, relying on encryption using certificate and key management [15].
- **Vendor/operator cloud services and connections:** Digital assets have diverse ownership models and comprise a complex domain of stakeholders. Original equipment manufacturers, owner/operators, and maintenance personnel, to name a few, have a variety of privileges on system assets. Software-as-a-service providers are moving toward cloud adoption and rely on remote control for performing routine maintenance, upgrades, and patches to components.

2.2.2 Critical Hydrogen System Management Tools

To permit communications between OT and humans-in-the-loop, hydrogen production, storage, and dispenser systems require embedded computer systems for monitoring physical system functions, network communications, and general security (both IT and OT). These systems connect to a human-machine interface (HMI) to enable monitoring and process management. The field devices described in the previous section connect to each other and to field controllers, which subsequently communicate with HMIs, workstations, energy management systems, and any SCADA system integrated into the hydrogen system. Figure 1 shows an example of an HMI for a hydrogen production system at NREL.

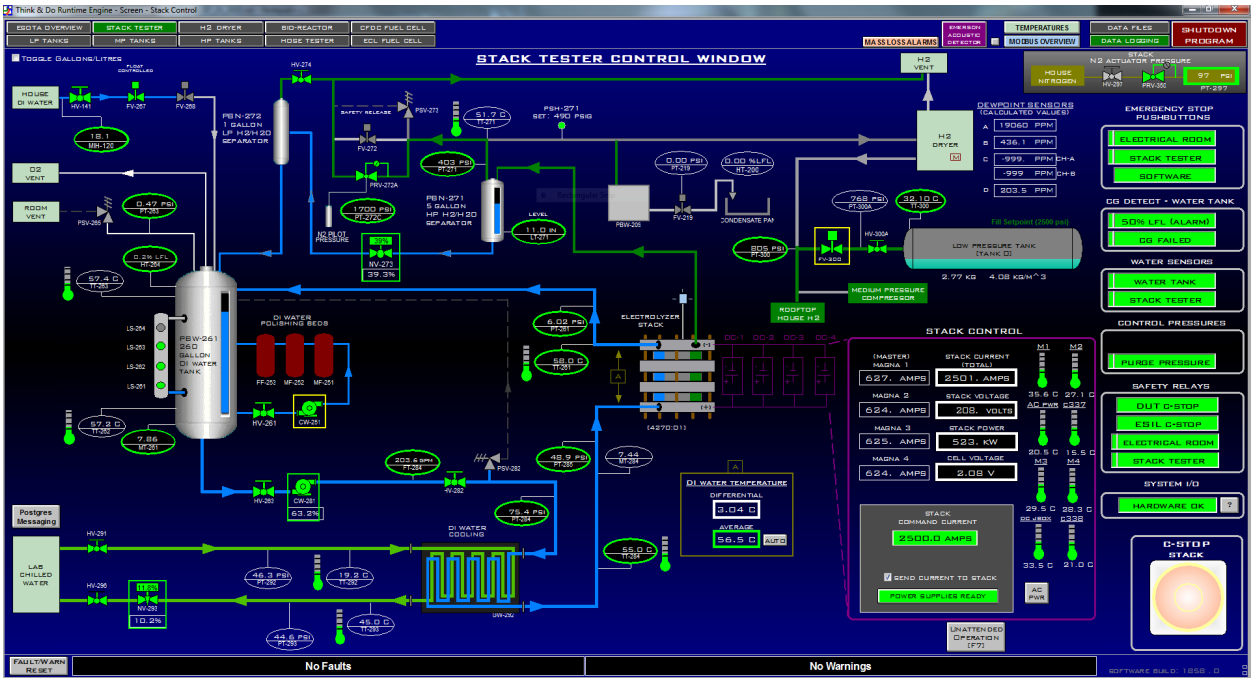

Figure 1. Example HMI for a hydrogen production system at NREL.

Source: Saur and Nagasawa 2024

3 Cybersecurity Risk Assessment

According to NIST, assessing cybersecurity risks requires evaluating "systemic information security-related risks associated with organizational governance and management activities, mission/business processes, enterprise architecture, or the funding of information security programs," as well as the implementation of risk management frameworks, which cover "security categorization; security control selection, implementation, and assessment; information system and common control authorization; and security control monitoring" (NIST 2018). These practices span three levels within an entity: (1) the organization level, (2) the mission or business process level, and (3) the information system level. An additional layer of risk assessment, informed by guidance from NIST's Risk Management Framework and Cybersecurity Framework 2.0, helps identify categories of cyber vulnerabilities for renewable power systems and informs mitigation strategies tested in other energy production, storage, and dispenser landscapes.

To inform conceptualization of a future landscape of hydrogen energy for aviation applications, this analysis considers NIST's guidance and frameworks alongside cybersecurity vulnerabilities drawn from three contexts:

- First, from NREL studies of hydrogen fueling station component validation, including assessments of existing fuel cell electric vehicle infrastructure within the United States, which help identify vulnerabilities and failure events documented in physical equipment Saur, Gilleon, and Sprik 2022).
- Second, from NREL reports on electric vertiports (Solanki et al. 2023) and electric aircraft charging infrastructure (Markel and Sanghvi 2022), which explore cybersecurity

vulnerabilities in both physical interference with systems and remote access with the subsequent deployment of malware that interrupts operations (Rane et al. 2023).

- Third, from NREL's Hydrogen Long Duration Energy Storage (H2 LDES) project, funded by the U.S. Department of Energy, which was based on a reference architecture for microgrid applications developed at NREL (Saleem et al. 2024). H2 LDES allowed cybersecurity researchers at NREL to explore components of a hydrogen system (e.g., controller, historian, meters, electrolyzer, storage, and fuel cell) and their integration with distribution (i.e., microgrids) (Rivera and Koleva 2025). Figure 2 shows a schematic of a hybrid reference architecture that includes a hydrogen system integrated with the grid. The exploration and analysis introduced emerging threat scenarios and mitigations specific to hydrogen systems, which are highlighted in Section 3.2.

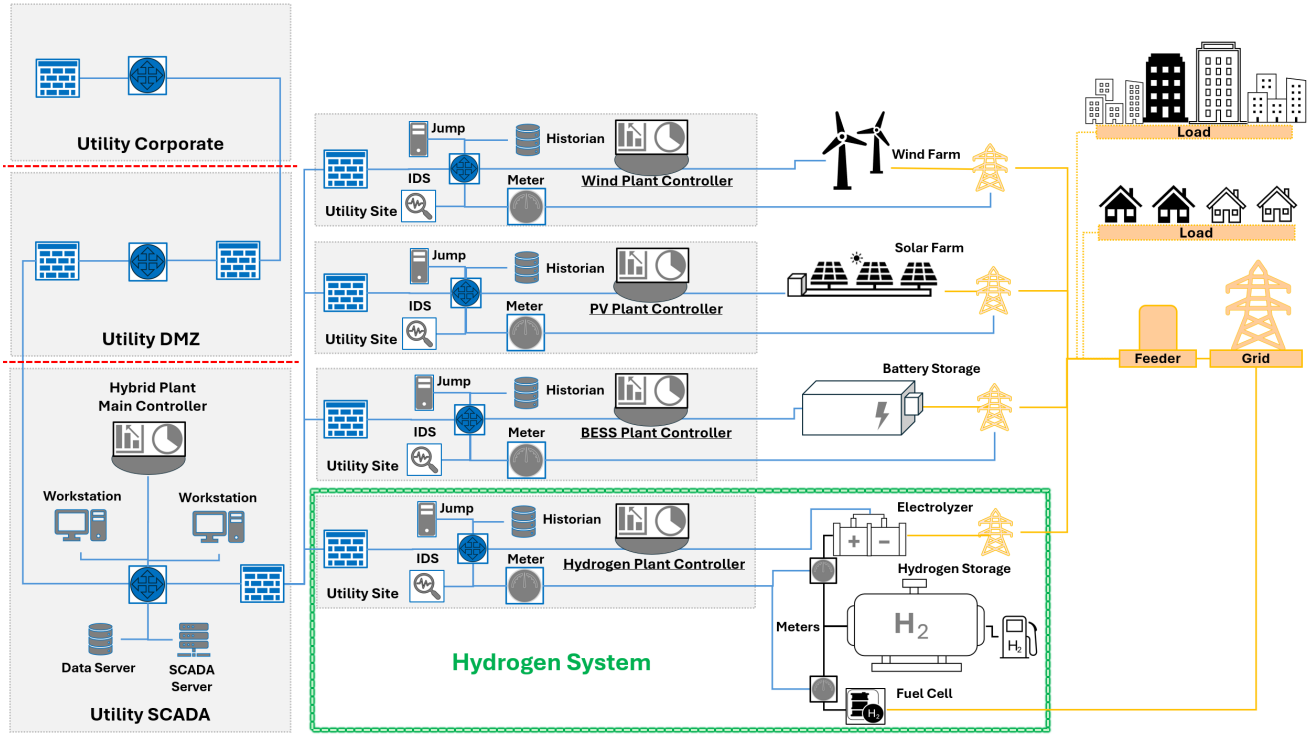

Figure 2. Schematic of a hybrid refence architecture with a hydrogen system integrated in the grid.

Source: Rivera and Koleva 2025

3.1 Common Cybersecurity Concerns for Electric Power

Building an infrastructure grounded in nascent energy technology carries inherent risk but also provides a unique opportunity to ensure cybersecurity is incorporated from initial concept and design. This is critical to manage risks to and concerns for airport hydrogen systems that are vulnerable to universal risks inherent in other industrial control systems. Documented cyberattacks impacting electric power systems include denial-of-service or distributed denial-of-service attacks, malware, phishing, supply chain attacks, and internet-of-things-based attacks, among others (Alexander n.d.). In the process of adopting a new structure of hydrogen fueling for transportation, early-stage preparation to increase awareness and engage stakeholders will increase understanding about existing attack vectors and make managing cybersecurity risk in

the future more tenable. From a cybersecurity perspective, pairing proactive preparation for cyber threats with strategic resilience planning can help overcome or recover from accidental/natural or intentional cyber disruptions with minimal damage (Pearlson 2024).

Figure 3 depicts a high-level example of pathways for both cyberattacks and physical attacks and the generalized cyber-physical systems that can serve as attack vectors. In particular, vulnerabilities of grid-connected devices could affect equipment and SCADA, creating a complex attack vector profile. Each attack penetrates various control devices, which causes physical, cyber-physical, and digital security risks. Figure 3 illustrates attack vectors from interconnected control systems, grid-connected technologies, and other field devices that support hydrogen system operations. This complex ecosystem relies on increasingly deployed cloud technologies from vendors and equipment manufacturers. Several geographically remote connections depend on radio frequencies and cellular or satellite communications and present potential risks. Some categories of impact are described in Section 3.3.

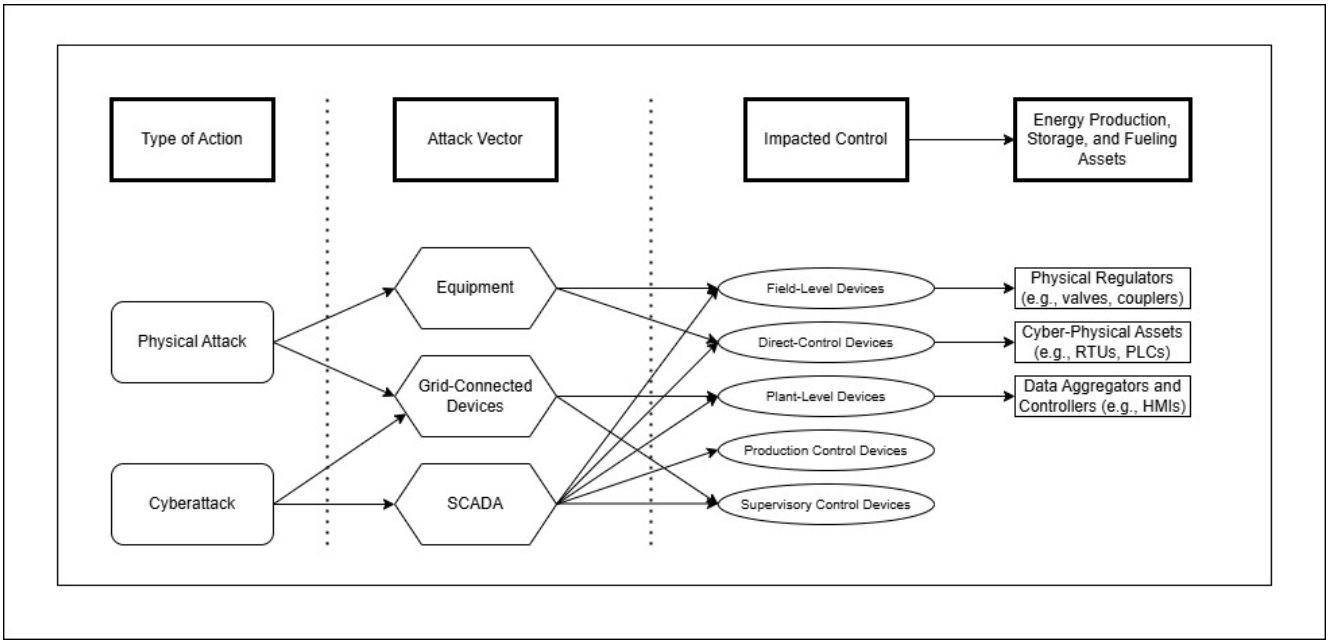

Figure 3. Pathways for cyberattacks and physical attacks and the cyber-physical systems that can serve as attack vectors.

NREL studies of California's fuel cell electric vehicles fueling infrastructure provide additional insights into existing hazards and undesirable outcomes associated with hydrogen systems (Topolski et al. 2022). For example, one analysis (Saur, Gilleon, and Sprik 2020) breaks down data consolidated from hydrogen fueling stations to identify safety incidents occurring due to component failure; inadequate training, protocol, or standard operating procedure; inadequate/nonworking equipment; required maintenance; operator/personnel errors; or undefined errors. These categories are then rated based on severity, with an "incident" constituting:

- Lost time and/or injury to personnel
- Financial losses
- Damage/unplanned downtime for project equipment, facilities, or property

- Impact on the public or environment
- Any hydrogen release that unintentionally ignites
- Release of any volatile, hydrogen-containing compound (including the hydrocarbons used as common fuels)

In addition to the above categories of incidents are two that are specific to hydrogen energy systems. First, a "near miss" refers to an event that could have resulted in any of the above or a hydrogen release that could ignite but did not. Second, a "minor hydrogen leak" is insufficient to ignite or sustain a flame. These benchmarks for safety incidents with hydrogen dispenser systems represent undesirable physical outcomes in any context and provide additional insight into the implications of both physical and cybersecurity vulnerabilities to consider for future hydrogen infrastructure across transportation, including aviation.

3.2 Cybersecurity Threat Methods and Considerations

NREL's H2 LDES threat vector and scenario study (Rivera and Koleva 2025) provided cybersecurity researchers with insights and considerations regarding the stages of the Cyber Kill Chain (Lockheed Martin 2024) (i.e., reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives) that a threat actor might use against hydrogen systems and their components. The study also employed the MITRE ATT&CK (MITRE 2024) framework to identify and evaluate the potential tactics, techniques, and procedures that threat actors might employ against the critical components of hydrogen infrastructure, such as plant controllers, historians, electrolyzers, and fuel cells. The confluence of the H2 LDES study and the MITRE framework are detailed in Figure 4.

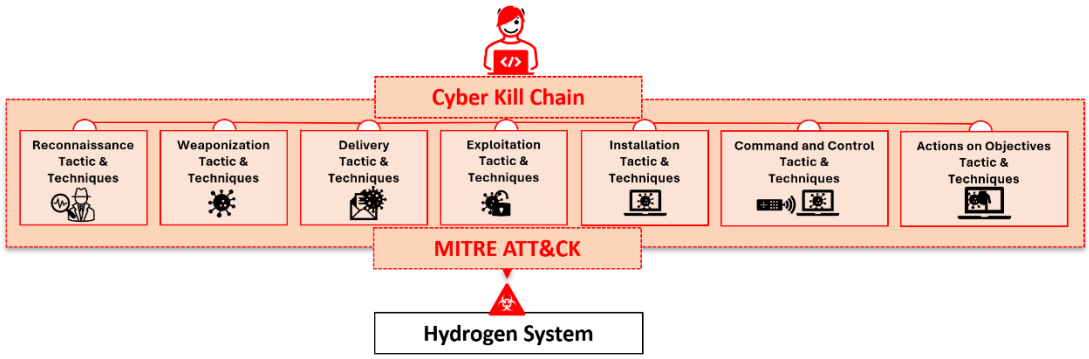

Figure 4. Theoretical threat actor process for advancing on systems, networks, and/or applications.

Source: Rivera and Koleva 2025

The following threat considerations from NREL's H2 LDES study (Rivera and Koleva 2025) are hypothetical in nature yet illustrate various threat vectors and scenarios by mapping the Cyber Kill Chain stages and MITRE ATT&CK techniques to specific hydrogen system components. Figure 5 highlights potential attack vectors and scenarios within a hydrogen system, offering a generalized representation of where adversaries might exploit weaknesses. By studying these diagrams, cyber analysts can better understand the specific risks and develop more targeted strategies to mitigate potential threats to hydrogen infrastructure.

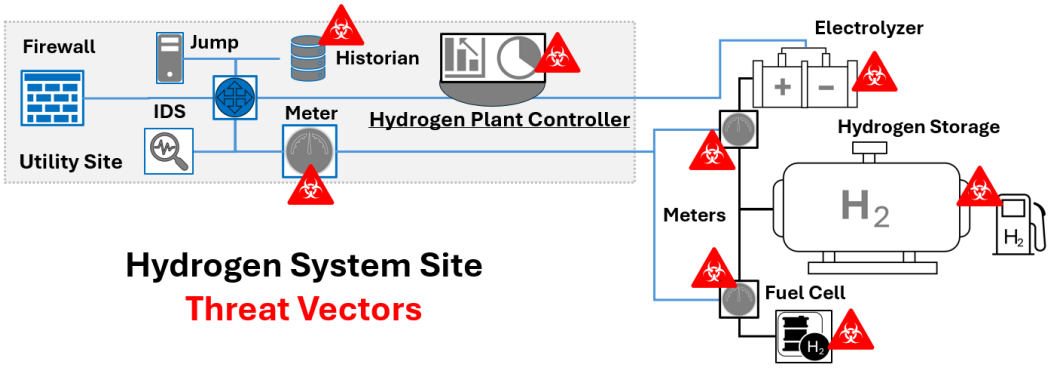

Figure 5. Cyber threat vectors (in orange) overlay a high-level representation of a hydrogen system.

Source: Rivera and Koleva 2025

3.2.1 Hydrogen Threat Scenarios

Figure 6 shows a Cyber Kill Chain scenario using the MITRE ATT&CK tactics, techniques, and procedures for a hydrogen plant controller and a data historian. It outlines each phase of a theoretical attack and how it might apply to a hydrogen system.

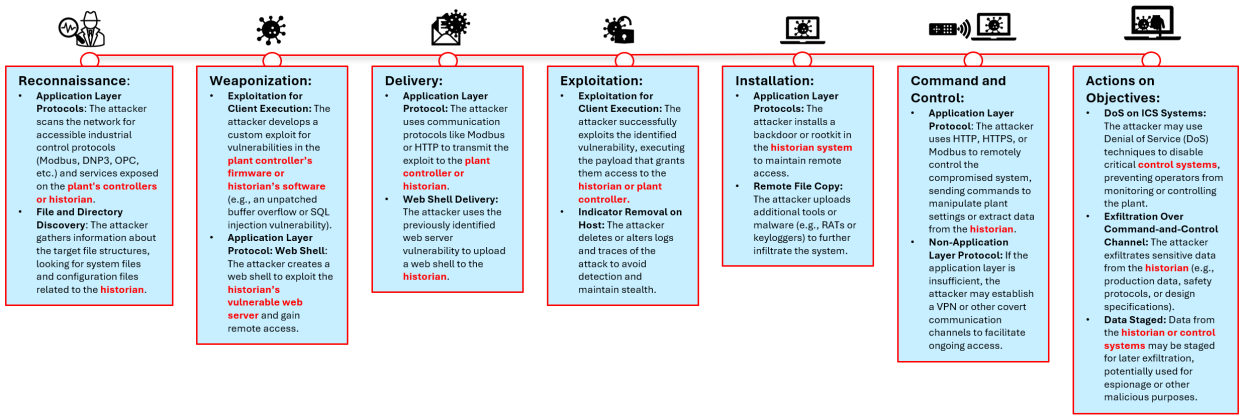

Figure 6. Threat scenario focused on controller and historian.

Source: Rivera and Koleva 2025

Figure 7 depicts a Cyber Kill Chain threat scenario using the MITRE ATT&CK tactics, techniques, and procedures against a hydrogen system (i.e., electrolyzer, storage, and fuel cell). It outlines each phase of the attack and how it might apply to a hydrogen system.

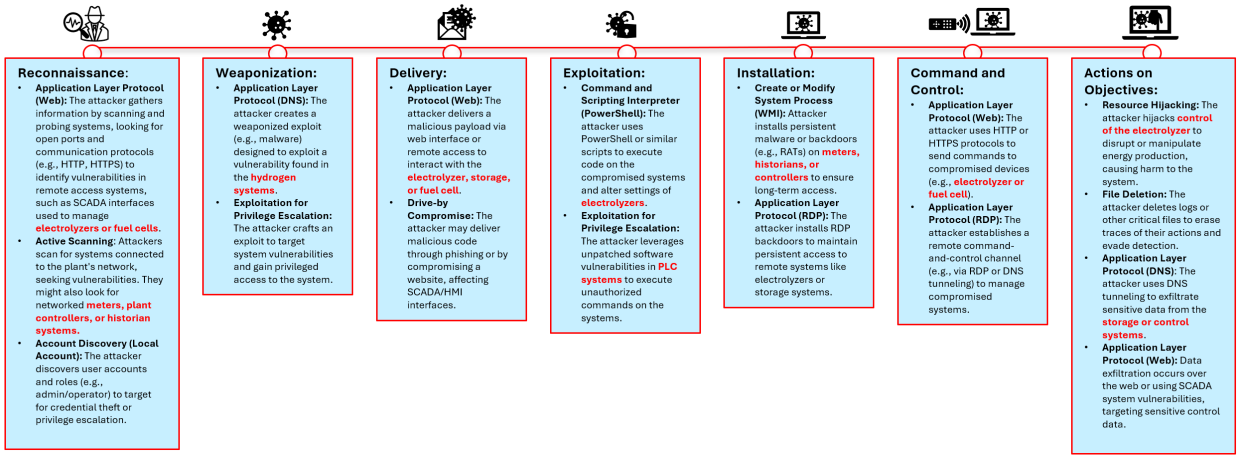

Figure 7. Threat scenario focused on device applications (electrolyzer, hydrogen storage, fuel cell).

Source: Rivera and Koleva 2025

Figure 8 highlights how a threat actor might influence different meters across a hydrogen system, using the MITRE ATT&CK tactics, techniques, and procedures. These considerations were deduced as an exercise to understand different methods a threat actor might take against hydrogen system metering infrastructure.

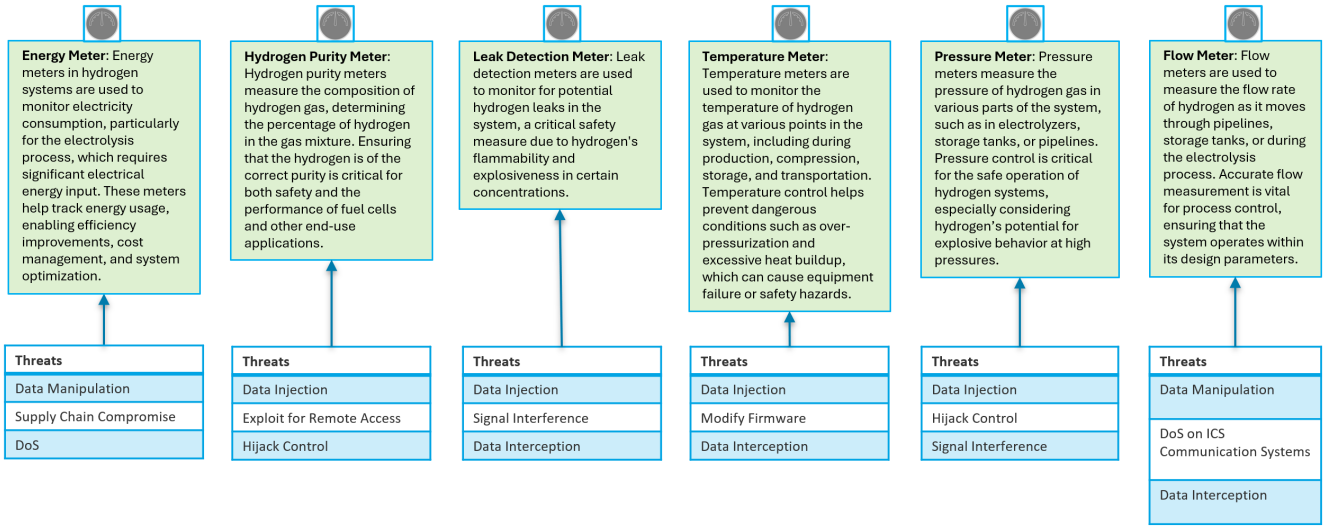

Figure 8. Threat considerations focused on hydrogen system metering infrastructure.

Source: Rivera and Koleva 2025

3.2.2 Threat Mitigation Mapping

The H2 LDES project also explored mapping threat vectors and scenarios to hydrogen systems using security controls as a mitigation strategy. Figure 9 depicts a practical approach toward identifying threats and applying cybersecurity design choices across a hydrogen system with a focus on threat mitigation. This mapping intends to illustrate the convergence between security controls and threat scenarios against hydrogen LDES systems, and that hydrogen system

engineers and cybersecurity analysts can holistically assess the system when making design choices.

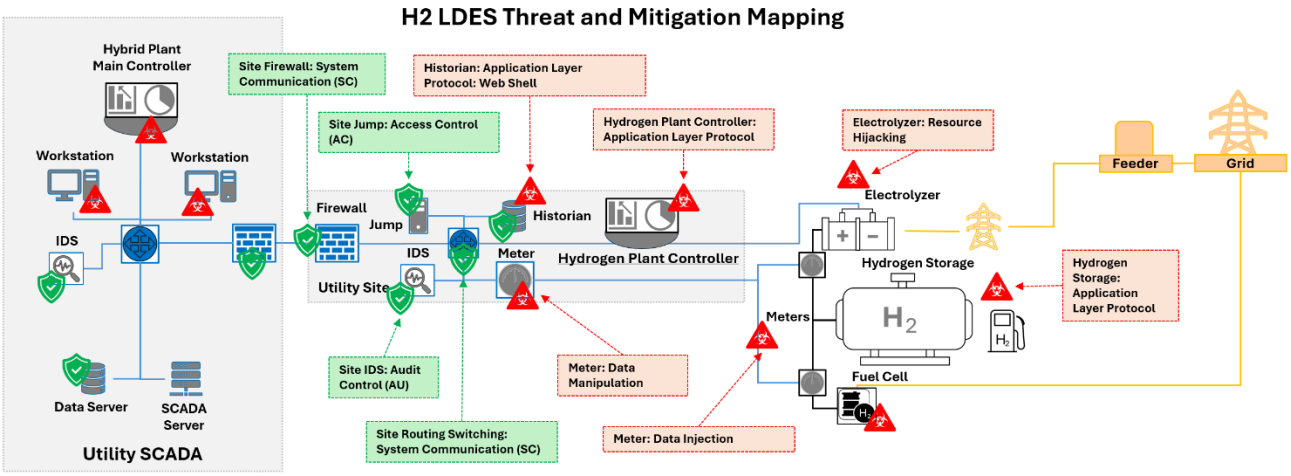

Figure 9. Threat and mitigation mapping.

Source: Rivera and Koleva 2025

3.3 Categories of Impact

Cybersecurity incidents are possible across a multitude of vectors, as demonstrated in the previous section, and can likewise impact diverse categories of assets and processes. This section generalizes potential areas of impact from cybersecurity incidents, drawing upon recent examples that targeted critical energy infrastructure assets (Casanovas and Nghiem 2023). Breaking down the technology domains found in most transportation fueling or charging infrastructure can help identify vulnerabilities and thereby potential mitigation strategies to consider in building out a hydrogen fueling infrastructure for transportation. Depending on the site-specific configuration of hydrogen production, storage, and fueling processes, a hydrogen fueling system could contain the following technology domains (MITRE 2024):

- Enterprise networks and dependencies on cloud technologies
- Mobile communication devices
- Industrial control systems

Malicious actors can use various techniques to target any of these domains, with impacts stretching beyond the digital realm. Any kind of fuel mechanism with digital control integrations—particularly a fuel that carries high-consequence failure outcomes—carries the potential risk of real, tangible effects due to successful cyberattacks. Table 1 presents generalized examples and impacts, which consist of five categories that are not mutually exclusive.

Table 1. Vulnerability Impacts of Digital Control Integration

Impact	Example
Functional or operational	A cyberattack cuts off digital communications between the fueling mechanism and the vehicle equipment, disrupting operations.
Financial	Operations are disrupted due to a cyber interference that causes delays, increasing the financial burden on vehicle/fleet operators.
Safety (harm to people or equipment damage)	A cyberattack interferes with the HMI displays to misrepresent real-time data, compromising decision-making and risking the safety of individuals and physical damage to equipment.
Interconnection and grid (power supply interruptions)	Interference with digital controls takes the hydrogen production processes offline, disrupting the supply.
Privacy	An attacker gains access to the monitoring systems and lurks to learn more about the process, controls, and protocols.

Where cyber interference can produce physical outcomes, there are ways to enhance cybersecurity measures and awareness while also introducing controls and processes in the early planning stages to mitigate threats and to more securely deploy hydrogen fueling and charging infrastructure. One such method, supported by the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response, is Cyber-Informed Engineering, whereby potentially high-impact consequences of cyberattack on cyber-physical systems are identified and, if possible, mitigated using engineering controls (CESER 2024).

3.4 Functional Architecture for Hydrogen Fueling Infrastructure

Mapping the cyber components within a generalized hydrogen reference architecture that includes production, storage, and dispenser systems improves understanding of the connections, functions, and points of vulnerability. Building on Figure 2, which connects attack vectors to the impacted assets, this reference architecture highlights some technologies that are specific to hydrogen production, storage, and dispensing. Though simplified, this process flow reveals the points of connection between assets and the potential sensors that are vulnerable to manipulation in the event of compromised access or communications within a SCADA system. Working with a generalized architecture such as this block diagram can help stakeholders, engineers, and strategists understand connections, criticalities, and standard practices when it comes to designing and planning for new systems.

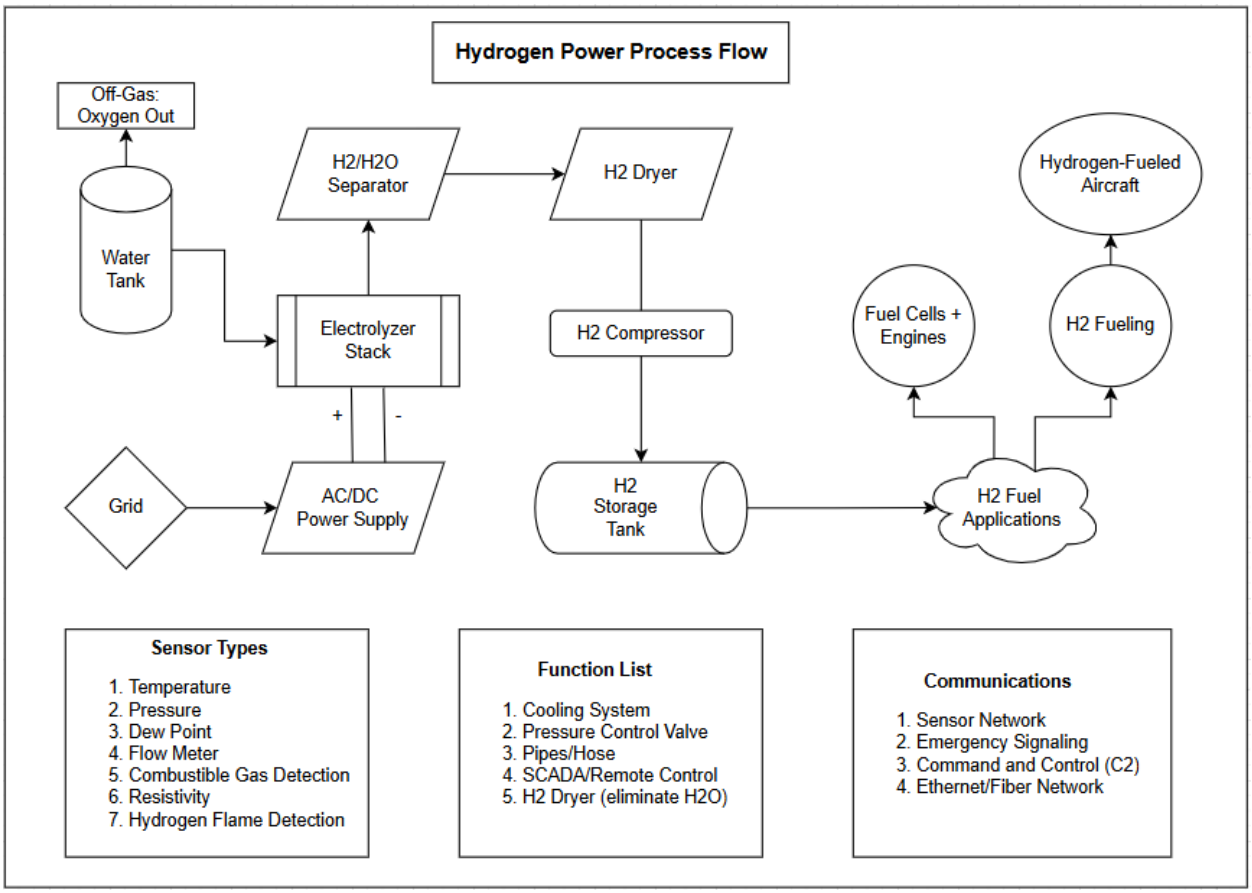

Figure 10. Reference architecture for a hydrogen production, storage, and distribution system.

3.5 Cybersecurity Standards and Industry Guidelines

Recent grid modernization initiatives (OTT 2021) have established a baseline of cybersecurity standards and mitigations for hydrogen energy infrastructure. Drawing upon existing guidance for electric vehicle charging infrastructure, as well as cybersecurity-specific guidance, this section compiles information that can support the planning process for a hydrogen fueling infrastructure for aviation.

The FAA cybersecurity strategy and guidance focuses on governance, risk mitigation, workforce awareness, and partnerships for sustaining and improving cybersecurity across the aviation ecosystem (U.S. Department of Transportation 2021). Additional documented FAA cybersecurity initiatives incorporate common standards and guidelines that are often applied to industrial control systems and can inform the development of hydrogen infrastructure (FAA 2017). Further insights can be gleaned from both the existing standards that would automatically apply to assets under FAA purview and the cybersecurity standards or guidelines that could enhance cybersecurity resilience within a hydrogen energy network with advanced cyber-physical systems.

Additionally, key tenets of a mature cybersecurity posture include the overall governance, technical management, and physical security guidelines, which can all be assessed based on tiers

of implementation, ranging from partial to risk-informed, to repeatable, to adaptive cyber-secure postures. Some key issues to consider for cyber-physical systems include:

- Cybersecurity vulnerabilities will depend on the architecture of the on-site production, storage, and fueling system.
- If individual hydrogen fueling sites connect to public utilities, such sites will be subject to interconnection standards, such as the Institute of Electrical and Electronics Engineers (IEEE) 1547 and IEEE 2030.5 for physical reliability and local regulatory requirements (see Section 3.5.2).
- Standards can cover specific technologies, requirements for cybersecurity preparedness, network and connection setups, and communication protocols for energy systems.

3.5.1 Overview of Relevant Standards for Cybersecurity Assessment

The following (non-exhaustive) list of standards for hydrogen energy systems prioritizes starting points for planning hydrogen fueling infrastructure for aviation, based on anticipated transportation safety and cybersecurity requirements. The list offers an overview of the resources that can be used as baselines for assessing cybersecurity postures or for establishing best practices at the outset of the infrastructure's planning stages. The codes and standards related to hydrogen fire safety are consolidated in a separate NREL technical report (NREL 2013).

- National Association of Regulatory Utility Commissioners Phase 1: Outlines the cybersecurity baselines for protecting electric distribution systems and connected distributed energy resources. The guidance offers structures for the governance of IT and OT cybersecurity activities as well as techniques for mitigating cybersecurity issues that can be applied to the distribution of hydrogen energy resources (NARUC 2024)
- NIST Cybersecurity Framework 2.0: Provides an overview of core functions of cybersecurity (e.g., governance, identification, protection, detection, response, and recovery) and approaches for mapping an organization's cybersecurity posture in terms of outcomes (NIST 2024)
- NIST Special Publication 800-30: Provides guidance for conducting risk assessments for federal organizations in compliance with the Federal Information Security Management Act (NIST 2012). The Federal Information Security Management Act applies to commercial entities that contract with federal agencies as well. Related publications include:
    - NIST Special Publication 800-39—Managing Information Security Risk: Organization, Mission, and Information System View
    - NIST Special Publication 800-37—Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
    - NIST Special Publication 800-53—Recommended Security Controls for Federal Information Systems and Organizations
    - NIST Special Publication 800-53A—Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.
- NIST Special Publication 800-50 Rev. 1: Provides guidance on building IT security awareness and training, incorporating widely accepted standards, regulations, and best practices, as well as legislation (Merritt et al. 2024)

- IEEE 1547: Provides functional technical requirements and specifications for connecting renewable energy technologies and distributed generation and energy storage technologies into electric power systems (Basso 2014)
- International Electrotechnical Commission (IEC) 62443: Offers requirements and processes for electronic security in industrial automation and control systems (ISA 2024)
- SAE J2847/1: Offers specific information relevant to digital communications for plug-in and off-board vehicle chargers, which can inform the development of communication standards or the identification of commonalities for hydrogen fueling processes (Pratt, Tuffner, and Gowri 2011)
- SAE J2601/5 and J2799: Though under revision, SAE J2601 establishes protocols that permit fueling with or without communications to meet end-of-fill pressure targets (SAE 2020). With communications, the protocols are used in concert with SAE J2799, which outlines hardware and software requirements for vehicle fueling (SAE 2024).

Additional reference points for codes and standards applicable to hydrogen safety (e.g., station requirements; storage, compression, generation, and dispensing system requirements; valving, piping, tubing, and venting requirements; and fire safety requirements), are consolidated in an NREL brochure (NREL 2013). Recent updates are available from individual standards organizations, including those governing compressed hydrogen fuel containers, fuel system components for compressed hydrogen gas-powered vehicles, and hydrogen dispensing systems.

3.5.2 Communication Standards for IT/OT Security

Key, critical needs for communication networks for hydrogen fueling can be drawn from mature electric vehicle technologies. In networks that connect charging infrastructure and central controllers, Open Charge Point Protocol (OCPP), if not implemented securely, could leave sites vulnerable to cyberattack. Within the context of hydrogen infrastructure and specific to communications among production, storage, and dispenser systems, relevant energy and cyber standards include IEC 61850, which provides guidance on data and communications security; and relevant communication protocols include Modbus, Distributed Network Protocol 3 (DNP3) and Controller Area Network (CAN) bus, which is particularly relevant for battery systems in fuel-cell electric vehicles, with implications for electric-powered aircraft.

Systems engineers can use various tools to conduct cybersecurity assessments when developing plans for hydrogen infrastructure. Determining the needs for communication security within a hydrogen system could include the following steps:

- Conduct a preliminary analysis of hydrogen system dispenser communication protocols and processes.
- Identify critical component functions and dependencies.
- Disseminate industry standards and best practices and highlight cybersecurity gaps.
- Leverage existing models and architectures to conduct a risk assessment overview.

The Distributed Energy Resource Cybersecurity Framework (DER-CF), which evaluates an existing or potential facility's distributed energy resource cybersecurity posture (NREL 2024), is another resource for the holistic assessment of cybersecurity resilience.

4 Discussion and Conclusion

The nature of risk management for hydrogen energy systems requires integration of engineering principles that forestall impacts from successful cyberattacks. Although the physical safety standards for hydrogen are comparatively mature relative to cybersecurity, several gaps remain in assessing the future of hydrogen production, storage, and fueling for aviation. Proactive evaluation and incorporation of cybersecurity of airport hydrogen systems from initial concept and design is the most successful and cost-effective way to address and manage risks long term. The following list identifies some knowledge and execution gaps for inclusion in future assessments:

- **Stakeholder analysis:** Potential stakeholders for cybersecurity of hydrogen fueling infrastructure for aviation include aircraft manufacturers, electric utilities, property owners, and local communities (Solanki 2023). Engaging these stakeholders to improve understanding of operational needs, cyber risk accountability, and cybersecurity awareness will inform decision-making around site structure, operations, and resources for fueling infrastructure.
- **Environmental impact assessments:** Any additions to the aviation infrastructure involving substantive energy generation, storage, and fueling systems adds a layer to a site's potential vulnerability in the event of natural disasters, along with potential correlations with human-made or cybersecurity incidents. Future analyses could consider the potential means of sustaining operations—either digital or physical—in case malicious actors take advantage of vulnerable locations that are recovering from natural disasters by launching cyberattacks.
- **Site design:** Future strategies must consider physical attack vectors that emerge with the integration of hydrogen systems into existing airport security requirements, such as those referenced in Figure 1. From a cybersecurity perspective, these include access and authentication control mechanisms and role-based and attribute-based access control.
- **Cost-benefit analyses**: Future research could expand the granularity of data available when considering component-level structures of hydrogen fueling sites. These analyses would complement the assessment of whether the costs of implementing hydrogen fueling for aviation balance the benefits of introducing renewable energy for electrification in the aviation sector. These could include electric energy loads that are required for operation, grid impact analysis, labor or economic considerations, and hazard analysis. Additionally, analysis pertaining to the cost of introducing cybersecurity risk mitigations while calculating risk-reduction benefits is also needed.
- **Sparse data**: Due to the nascent stage of the hydrogen fueling infrastructure for transportation, there is limited reporting on hydrogen-specific cybersecurity vulnerabilities. Future research can address specific vulnerabilities therein, with potential to consider the cybersecurity factors at play when it comes to fuel storage and power devices on aircraft.

Additional research and questions can address cyber vulnerabilities at a more granular level (e.g., consider the nuances of hydrogen production, storage, and dispensing systems) when assessing physical or remote access vulnerabilities, determining how the scale of the hydrogen fuel infrastructure for aviation impacts the volume of cyberattack vectors, and determining what, if any, vulnerabilities are associated with different types of on-board hydrogen systems. Further research from NREL can include the virtualization of testing scenarios to enhance confidence in cybersecurity vulnerability mitigations. Where certain elements of power systems have not yet

been tested or validated—including hydrogen fueling for aviation—further research can inform the infrastructure landscape design and clarify needs for future planning and implementation. Consideration of the people and responsibilities connected with the management of technical components were not within the scope of this study but will be important in future research.

The following non-exhaustive lists provide interim guidance on the codes and standards for cybersecurity considerations. The lists offer an overview of the resources that can be used as baselines for assessing cybersecurity postures or for establishing best practices at the outset of different stages of infrastructure planning.

Overview of relevant standards for cybersecurity assessments:

- NARUC Phase 1: Guidance for establishing foundational cybersecurity practices for distribution systems and connected distributed energy resources. Covers governance of IT and OT cybersecurity activities and cyber risk mitigations, which can be applied to the distribution of hydrogen energy resources (NARUC 2024)
- NIST Cybersecurity Framework 2.0: Outlines the core functions of cybersecurity (i.e., governance, identification, protection, detection, response, and recovery) and provides approaches for mapping an organization's cybersecurity posture in terms of outcomes (NIST 2024)
- NIST Special Publication 800-30: Guidance for conducting risk assessments for federal organizations in compliance with the Federal Information Security Management Act (NIST 2012). The Federal Information Security Management Act applies to commercial entities that contract with federal agencies as well. Related publications include:
    - Special Publication 800-39—Managing Information Security Risk: Organization, Mission, and Information System View
    - Special Publication 800-37—Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,
    - Special Publication 800-53—Recommended Security Controls for Federal Information Systems and Organizations
    - Special Publication 800-53A—Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.
- NIST Special Publication 800-50 Rev. 1: Guidance for building IT security awareness and training, incorporating widely accepted standards, regulations, and best practices, as well as relevant legislation (Merritt et al. 2024)
- IEEE 1547: Functional technical requirements and specifications for connecting clean renewable energy technologies and distributed generation and energy storage technologies into electric power systems (Basso 2014)
- IEC 62443: Requirements and processes for electronic security in industrial automation and control systems (ISA 2024).

Communication standards for IT/OT security:

- SAE J2847/1: Specific information relevant to the required digital communications for plug-in and off-board vehicle chargers, which can inform the development of communication

standards or the identification of commonalities for hydrogen fueling processes (Pratt, Tuffner, and Gowri 2011)

- SAE J2799: Guidance for communication hardware and software requirements for hydrogen fueling
- IEC 61850: Guidance on data and communication security
- IEEE 2030.5: Functions to allow utility management of the end user environment.

References

Airbus. 2024. "Airbus Partners with Avolon to Explore Future of Hydrogen Aviation." Accessed September 18, 2024. https://www.airbus.com/en/newsroom/press-releases/2024-07-airbus-partners-with-avolon-to-explore-future-of-hydrogen-aviation.

Alexander, Otis, Misha Belisle, and Jacob Steele. 2020. *MITRE ATT&CK® For Industrial Control Systems: Design and Philosophy*. Mclean, VA: MITRE. Project No.: 01ADM105-OT. https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf.

Awati, Rahul and Peter Loshin. n.d. "What is SCADA (Supervisory Control and Data Acquisition)?" TechTarget. Accessed September 18, 2024. https://www.techtarget.com/whatis/definition/SCADA-supervisory-control-and-data-acquisition.

Basso, Thomas. 2014. *IEEE 1547 and 2030 Standards for Distributed Energy Resources Interconnection and Interoperability with the Electricity Grid*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5D00-63157. https://www.nrel.gov/docs/fy15osti/63157.pdf.

Barker, William C. 2003. *Guideline for Identifying an Information System as a National Security System*. Gaithersburg, MD: National Institute of Standards and Technology. NIST SP 800-59. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf.

Byers, Eric, Andrew Gintner, and John Langill. n.d. "How the Stuxnet Computer Worm Spreads in an Industrial Process Plant." Accessed September 18, 2024. https://blog.isa.org/how-stuxnet-computer-worm-spreads-industrial-process-plant-cybersecurity.

Cybersecurity & Infrastructure Security Agency (CISA). 2024. "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure." Accessed April 22, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

Easterly, Jen. 2023. "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years." Cybersecurity & Infrastructure Security Agency (CISA). Accessed September 18, 2024. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

Grossman, Larry. 2021. "The Evolving Cybersecurity Landscape: Federal Perspectives on Securing the Nation's Infrastructure. Hearing Before the United States House of Representatives Committee on Transportation and Infrastructure. https://www.transportation.gov/evolving-cybersecurity-landscape-federal-perspectives-securing-nations-infrastructure.

Hauet, Jean-Pierre, Patrice Bock, Romain Françoise, and Robert Foley. 2017. "Ukrainian Power Grids Cyberattack: A Forensic Analysis Based on ISA/IEC 62443." Accessed September 18, 2024. https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack.

Hydrogen Tools. 2024. *SAE J2601/5 High-Flow Prescriptive Fueling Protocols for Gaseous Hydrogen Powered Medium and Heavy-Duty Vehicles*. https://h2tools.org/fuel-cell-codes-and-standards/sae-j26015-high-flow-prescriptive-fueling-protocols-gaseous-hydrogen.

"Hydrogen Vehicle Infrastructure Codes and Standards Citations." Golden, CO: National Renewable Energy Laboratory. NREL/BR-5400-57943. https://www.energy.gov/eere/fuelcells/articles/hydrogen-vehicle-and-infrastructure-codes-and-standards-citations.

International Society of Automation. "The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards: ISA/IEC 62443 Series of Standards." ISA Standards and Publications. Accessed September 18, 2024. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

Lockheed Martin. 2025. "The Cyber Kill Chain." 2025. Accessed April 5, 2025. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Markel, Anthony, and Anuj Sanghvi. 2022. *Addressing Electric Aviation Infrastructure Cybersecurity Implementation*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-82856. https://www.nrel.gov/docs/fy23osti/82856.pdf.

MITRE. 2024. "MITRE ATT&CK®." Accessed September 9, 2024. https://attack.mitre.org/resources/.

MITRE. 2025. "MITRE ATT&CK®." Accessed October 1, 2024. https://attack.mitre.org/.

Casanovas, Mark and Aloys Nghiem. 2023. "Cybersecurity – Is the Power System Lagging Behind?" *IEA*. August 1, 2023. https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind.

Merritt, Marian, Susan Hansche, Dr. Brenda Ellis, Kevin Sanchez-Cherry, Julie Nethery Snyder, and Donald Walden. National Institute of Standards and Technology (NIST). *Building a Cybersecurity and Privacy Learning Program*. Gaithersburg, MD, 2024. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf.

National Institute of Standards and Technology (NIST). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. NIST SP 800-37, Revision 2. Gaithersburg, MD, 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

National Association of Regulatory Utility Commissioners (NARUC). 2024. "Cybersecurity Baselines for Electric Distribution Systems and DER." Accessed September 18, 2024. https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/.

National Institute of Standards and Technology (NIST). *The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29*. Gaithersburg, MD, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

National Institute of Standards and Technology (NIST). *Guide for Conducting Risk Assessments*. Gaithersburg, MD, 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

National Renewable Energy Laboratory. 2025. "DER Cyber Framework." Accessed September 18, 2024. https://dercf.nrel.gov/.

Office of Cybersecurity, Energy Security, and Emergency Response (CESER). 2024. "Cyber-Informed Engineering." Accessed September 18, 2024. https://www.energy.gov/ceser/cyber-informed-engineering.

Pearlson, Keri. 2024. "When Cyberattacks are Inevitable, Focus on Cyber Resilience." Harvard Business Review. Accessed July 18, 2024. https://hbr.org/2024/07/when-cyberattacks-are-inevitable-focus-on-cyber-resilience.

Pratt, R.M., F.K. Tuffner, and K. Gowri. 2011. *Electric Vehicle Communication Standards Testing and Validation – Phase I: SAE J2847/1*. Richland, WA: Pacific Northwest National Laboratory. PNNL-20913. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20913.pdf.

Rane, Jayaraj, Bharatkumar Solanki, Scott Cary, Prateek Joshi, and Subhankar Ganguly. 2023. *Overview of Potential Hazards in Electric Aircraft Charging Infrastructure*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-83429. https://www.nrel.gov/docs/fy24osti/83429.pdf.

Rivera, Joshua and Mariya Koleva. 2025. *Hydrogen Long Duration Energy Storage for Resilience (H2 LDES Demo) Project: Threat Vectors and Scenarios*. Golden, CO: National Renewable Energy Laboratory. NREL/PR-5700-92485, 2025. https://www.nrel.gov/docs/fy25osti/92485.pdf.

SAE International. 2020. *Fueling Protocols for Light Duty Gaseous Hydrogen Surface Vehicles*. May 29, 2020. SAE J2601. https://www.sae.org/standards/content/j2601_202005/.

SAE International. 2024. *Hydrogen Surface Vehicle to Station Communications Hardware and Software*. June 2024. SAE J2799. https://www.sae.org/standards/content/j2799_202406/.

Saleem, Danish, Charles Magill, Venkatesh Venkataramanan, Zoe Dormuth, Adarsh Hasandka, and Emily Waligoske. 2024. *Renewable Energy and Storage Cybersecurity Research (RESCue) Pilot Final Report*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5T00-89921. https://www.nrel.gov/docs/fy24osti/89921.pdf.

Saur, Genevieve and Kazunori Nagasawa. 2024. "Offshore Wind to Hydrogen – Modeling, Analysis, Testing, and International Collaboration Work." Presented at the 2024 Annual Merit Review and Peer Evaluation Meeting. DOE Hydrogen Program. https://www.nrel.gov/docs/fy24osti/89549.pdf.

Saur, Genevieve, Spencer Gilleon, and Sam Sprik. "Fueling Station Component Validation." Presented at the H2@Scale Working Group/May 19, 2020. National Renewable Energy Laboratory (NREL). Golden, CO. NREL/PR-5400-76846. https://www.nrel.gov/docs/fy20osti/76846.pdf.

Saur, Genevieve, Spencer Gilleon, and Sam Sprik. 2023. "Next Generation Hydrogen Station Composite Data Products: Retail Stations." National Renewable Energy Laboratory (NREL), Golden, CO (United States), NREL/PR-5400-86247, May 2023. https://www.nrel.gov/docs/fy23osti/86247.pdf.

Solanki, Bharatkumar, Peyton Sanders, Eric Miller, Priti Paudyal, Bhavesh Rathod, Sherinn Ann Abraham, Michael Young, Andre Fernandes Tomon Avelino, Harsha Vardhana Padullaparti, Scott Cary, Chris Hallock, Kristi Moriarty, Grant Ellwood, Jiyu Wang, Francisco Flores-Espino, Jayaraj Rane, Tony Markel, and Anuj Sanghvi. 2023. *Federal Aviation Administration Vertiport Electrical Infrastructure Study*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-86245. https://www.nrel.gov/docs/fy24osti/86245.pdf.

Stouffer, Keith, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman, Adam Hahn, Stephanie Saravia, Aslam Sherule, and Michael Thompson. 2023. *Guide to Operational Technology (OT) Security*. NIST Special Publication (SP) NIST SP 800-82r3. Gaithersburg, MD, 2023. https://doi.org/10.6028/NIST.SP.800-82r3.

Topolski, Kevin, Evan P. Reznicek, Burcin Cakir Erdener, Chris W. San Marchi, Joseph A. Ronevich, Lisa Fring, Kevin Simmons, Omar Jose Guerra Fernandez, Bri-Mathias Hodge, and Mark Chung. 2022. *Hydrogen Blending into Natural Gas Pipeline Infrastructure: Review of the State of Technology*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5400-81704. https://www.nrel.gov/docs/fy23osti/81704.pdf.

U.S. Department of Energy Office of Energy Efficiency and Renewable Energy. 2024. "Alternative Fuels Data Center." Accessed September 9, 2024. https://afdc.energy.gov/fuels/hydrogen-locations.

U.S. Department of Transportation Federal Aviation Administration (FAA). 2017. *Report to Congress.* https://www.transportation.gov/evolving-cybersecurity-landscape-federal-perspectives-securing-nations-infrastructure.

U.S. Department of Transportation Office of Technology Transitions (OTT). 2021. "Advancing Cybersecurity to Strengthen the Modern Grid." https://www.transportation.gov/evolving-cybersecurity-landscape-federal-perspectives-securing-nations-infrastructure.

ZeroAvia. 2024. "Federal Aviation Administration Awards ZeroAvia $4.2 Million US Federal Grant to Advance Electric Propulsion for Clean Aviation." Accessed September 18, 2024. https://zeroavia.com/federal-aviation-administration-awards-zeroavia-4-2-million-us-federal-grant-to-advance-electric-propulsion-for-clean-aviation/.

Zetter, Kim. 2014. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*. Published November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.