Pacific Northwest
NATIONAL LABORATORY

PNNL- 36487
SAND2024-13301R

Large-Scale Hydrogen Storage Cyber Risk Assessment

October 2024

Md Touhiduzzaman
Melissa S. Louie (Sandia National Laboratories)
Arun Veeramany
Brian D. Ehrhart (Sandia National Laboratories)

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

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 Battelle Memorial Institute, 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, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

PNNL- 36487
SAND2024-13301R

Large-Scale Hydrogen Storage Cyber Risk Assessment

October 2024

Md Touhiduzzaman
Melissa S. Louie (Sandia National Laboratories)
Arun Veeramany
Brian D. Ehrhart (Sandia National Laboratories)

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

Hydrogen storage systems are becoming more widely deployed throughout the country, and as their presence continues to grow, it is possible that individual and interconnected systems will be exposed to cyber-attacks. These events can cause physical and financial harm to employees, people in the vicinity, and to the company that owns the facility. The two main mechanisms malicious actors may access information or control from a hydrogen storage facility are through information technology and operations technology devices, the former of which refers to data and information from networked devices and the latter of which refers to onsite controls for the physical system. Both types of entryways into the system should be considered when facility managers conduct cyber risk assessments and when regulators develop or revise relevant codes and standards.

This report analyzes cybersecurity risks applicable to a wide variety of hydrogen storage systems by outlining the system's purpose and the importance of its cybersecurity. The hydrogen storage system architecture and communication protocols are provided to understand potential cyber vulnerabilities. Later, an event tree analysis is performed on hydrogen operation to identify system weaknesses by outlining potential attack scenarios. This report also identifies critical cyber assets related to different hydrogen operations followed by an examination of potential threats, and the impact of cyber assets on those operational assets.

Acknowledgments

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Hydrogen and Fuel Cell Technologies Office (HFTO) Safety Codes and Standards sub-program, under the direction of Laura Hill. This work was performed as part of a cooperative research and development agreement (CRADA) with the Sandia National Laboratories, Seattle City Light (SCL), and the Port of Seattle (POSea). The authors gratefully acknowledge Timothy Berg and Benjamin Karch at Sandia National Laboratories, who provided unpublished analyses and useful discussions on cybersecurity for hydrogen systems, as well as Benjamin Karch, Marina Miletic, and Kristin Hertz from Sandia National Laboratories for their technical reviews of this document.

Contents

Abstract ii
Acknowledgments iii
1.0 Introduction 1
2.0 System Architecture and Regulatory Requirements 2
2.1 System Architecture 2
2.2 Existing Regulations, Codes, and Standards 3
3.0 Cyber Vulnerabilities in Hydrogen Storage Systems 5
3.1 Information Technology 5
3.2 Operational Technology 5
4.0 Assets, Threats, and Impacts 8
5.0 Event Tree Analysis for Cyber Risk 13
6.0 Conclusion 17
7.0 Bibliography 18

Figures

Figure 1 Hierarchical Structured Industrial Control System Architecture for hydrogen (C. Peter, E. Wrettos and F. Buchi, 2022) 3
Figure 2 Event tree illustrating a cyber-attack scenario in storage tank pressure setting 14
Figure 3 Fault tree tracing the HSCU alarm response failure 15
Figure 4 Fault tree tracing the pressure setting abnormalities 15
Figure 5 Fault tree tracing the communication network abnormalities 16

Tables

Table 1 Assets, threats, and impacts associated with hydrogen ICS. 9

1.0 Introduction

As hydrogen storage technology becomes more common, cybersecurity breaches and malicious attacks on systems may become more frequent. The Department of Energy lists “data corruption, financial harm, physical equipment damage, disruption of services, and even loss of life” as potential cybersecurity concerns for energy facilities (DOE, n.d.). One major characteristic of hydrogen storage systems is the presence of hydrogen, which is a highly flammable substance; therefore, there is a need to minimize unintended ignition events. This characteristic of hydrogen storage systems is something that malicious cyber actors can leverage to cause damage to the facility and harm to people.

Cybersecurity is as strong as the weakest link in the system (Chatterjee, 2021). For any critical infrastructure, it is essential to identify and assess cyber assets with a comprehensive cyber risk assessment ensuring that dependencies and vulnerabilities are properly mapped A cybersecurity attack targeting the vulnerability of hydrogen systems could result in significant damage to the system, incurring high repair costs, and putting public safety at risk. Beyond the immediate operational and financial impacts, such an attack could erode public trust and diminish public acceptance or tolerance for hydrogen as an energy carrier. This report presents a high-level overview of hydrogen storage industrial control system (ICS) infrastructure and associated cyber risks. It begins by examining the architecture of hydrogen facilities, with a focus on communication channels and protocols. Next it details typical threats and vulnerabilities for different hydrogen storage operations. A significant portion of this report is dedicated to cyber vulnerabilities related to critical cyber assets, where potential weaknesses and security flaws within the storage system are identified and discussed. Finally, this report uses event tree analysis to assess cyber risk, providing a systematic approach to understanding the possible threat outcomes their likelihood, and the potential severity of their impacts.

The following approach is undertaken to carry out the risk assessment:

- System identification: the functional aspects of the hydrogen storage infrastructure, cyber assets, and communication protocols are identified.
- Threats, vulnerabilities, and impacts: the following are identified - threats (actions) that could potentially cause harm to the operations/life/infrastructure; vulnerabilities (weaknesses) in the infrastructure that could let a threat to exploit them; impacts (effects) of a successful exploitation.
- Risk: the overall risk of each threat is qualitatively assessed based on the identified vulnerabilities and impacts.
- Risk scenarios: the pathways (scenarios) involving initiating events, mitigation attempts, and impacts are identified using event tree analysis.
- Codes and standards: the codes and standards relevant to the protection and safe use of operational and cyber assets are identified.
- Recommendations: the overall cyber posture of the infrastructure could be enhanced by addressing the identified vulnerabilities and following the provided recommendations.

2.0 System Architecture and Regulatory Requirements

2.1 System Architecture

The architecture of a hydrogen ICS infrastructure typically consists of several layers, each with its own specific component, functions, and responsibilities. Understanding the system architecture of hydrogen ICS infrastructure helps effectively analyze its cyber vulnerabilities. Typically, a hydrogen storage system follows a layered architecture approach that has three layers (i.e., field, control, and supervisory), and the components residing in those layers have been divided into three sub-systems. This hierarchical breakdown facilitates the systematically identifying of vulnerabilities unique to each layer, enabling implementation of targeted security measures.

- Physical layer – Physical components are the main drivers of the system and perform the actual operations to produce and compress hydrogen gas. The physical components include but are not limited to the electrolyzers, compressors, vacuum pumps, hydrogen dryers, fuel cells, dehumidifiers, and power supplies.

- Sensor layer – The sensor components are used to monitor system characteristics during operation. Characteristics monitored include but are not limited to voltage, current, pressure, and volumetric flow rate. The sensor components include current transducers, voltage transducers, flowmeters, tank level indicators, and pressure transducers.

- Control layer – The control components are the interface between the physical and sensor components of the system. The control components receive data from the sensor components and use that data to regulate the physical components. The control components include controllers, plug-in modules, remote terminal units, switches for the communication channel, and supervisory control and data acquisition (SCADA).

The ICS is a computerized/automated control system used to monitor and control industrial processes, as shown in Figure 1. In the context of hydrogen infrastructure, the ICS is an essential system as it allows for the safe and efficient production, storage, and distribution of hydrogen gas. Hydrogen infrastructure ICS is typically made up of a network of sensors, controllers, remote terminal units, programmable logic controllers, communication channels, and other devices that work together to collect hydrogen data for different zones/points/areas, analyze those data, and issue commands to the various components of the hydrogen system.

The typical communication channels used in hydrogen infrastructure are ethernet, Message Queuing Telemetry Transport (MQTT), Open Platform Communications Unified Architecture (OPC UA), and Advanced Message Queuing Protocol (AMQP).

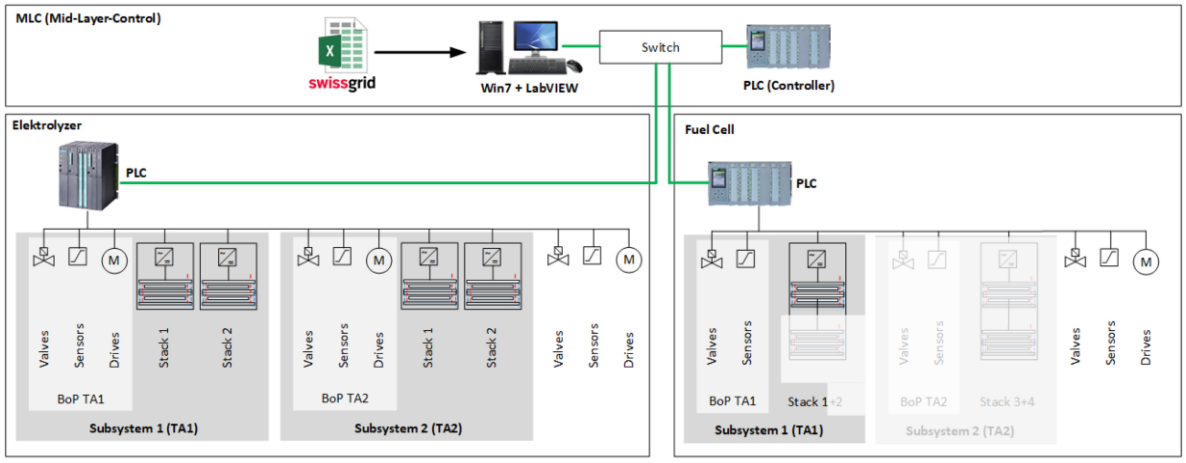


Figure 1 Hierarchical structured industrial control system architecture for hydrogen (C. Peter, E. Wrettos and F. Buchi, 2022)

2.2 Existing Regulations, Codes, and Standards

There is currently precedence in the national regulatory landscape for cybersecurity protocols that are either specific to hydrogen systems, or that provide valuable guidance even if not explicitly applicable. The identified regulations, codes, and standards apply to both or either physical or cyber components, which all help reduce risk in these systems.

There are several regulations that provide a basis for cybersecurity protections in vehicle refueling. Some standards vary based on the type of vehicle that is being refueled. SAE J2601 provides fueling protocols for light duty gaseous hydrogen surface vehicles (SAE J2601, 2020), SAE J2601-2 provides guidance for fueling of gaseous hydrogen powered heavy duty vehicles (SAE J2601-2, 2023), and SAE J2601-3 contains fueling protocols for gaseous hydrogen powered industrial trucks (SAE J2601-3, 2022). While cybersecurity is not explicitly mentioned, the requirements in these regulations guide physical safeguards against potentially hazardous conditions or scenarios that could be induced by a cyber-attack.

Additionally, the point in the refueling process where communication occurs between a dispenser and a vehicle being refueled is especially vulnerable to potential cybersecurity risks. Standards addressing these concerns include SAE J2601 (SAE J2601, 2020), a standard for gaseous hydrogen vehicle refueling applicable whether or not communication between the dispense and the vehicle is present. Additionally, SAE J2799 (Hydrogen Surface Vehicle to Station Communications Hardware and Software) (SAE J2799, 2019) focuses on protocols where communication is present between the dispenser and vehicle. SAE J2799 contains protocols for a data link layer between the transmitting and receiving sides of a data link (i.e., the dispenser and vehicle), data integrity checks. It also specifies requirements for communications hardware; for example, placement of the vehicle transmitter, the number of allowed nozzle receivers, and the size or angle of the nozzle. This standard helps mitigate a cyber attacks' potential adverse physical outcomes by incorporating software and hardware safeguards.

More broadly, some standards that relate to either industrial cybersecurity or hydrogen systems but not both still provide a foundation for implementing cybersecurity protections in a hydrogen system. For example, International Electrotechnical Commission (IEC) 62443 (Security of Industrial Automation and Control Systems) (ISA/IEC 62443 Series of Standards) is a series of

codes and standards focused on cybersecurity protection in industrial systems. Alternatively, the Occupational Safety and Health Administration (OSHA) regulation 29 CFR 1910.103 includes requirements for the implementation of physical devices that can help protect against cyber-attacks. However, it does not explicitly refer to them in the context of cybersecurity. For example, 29 CFR 1910.103 includes requirements for shutoff valves, which could protect the system from over pressurization attempts and define minimum setbacks to reduce exposures in and near the hydrogen facility, which could prevent damage to those exposures if a cyber-attack causes physical damage to the system.

The identified codes and standards that regulate either physical or cyber components, or both, can help to reduce system risk in a hydrogen storage facility.

3.0 Cyber Vulnerabilities in Hydrogen Storage Systems

3.1 Information Technology

Enterprise-class information technology (IT) refers to networked or cloud-based devices in the system such as phones, laptops, and devices for data storage. Data and software stored on these devices may be especially vulnerable to cyber-attacks if Internet connectivity is present. Depending on how the storage system network is configured, these devices can provide attack vectors for malicious cyber actors. Sensitive information related to the physical system operations and proprietary information about the company that owns the system (or personally identifying information about its employees) can be susceptible to consequences like data theft, privilege escalation, and ransomware. Furthermore, adversaries with access to information about the system operations may be able to inflict more calculated cyber-attacks on the system in the future. They may use sensitive information to block the company's access to its own system, make financial demands, steal employee or customer identities and information to further infiltrate into the IT system, and gather enough information for a later premeditated attack on the physical system. Overall, these outcomes could lead to both financial damage to the company and a degradation in public trust in the company. In a greater capacity, malicious cyber actors who have entry into one company's IT systems may then be able to collect information from other connected systems or even the broader grid. Implementing intrusion protection and detection systems and ensuring that the system is segmented appropriately can prevent and mitigate cyber-attacks. Additionally, maintaining access controls can help prevent cyber-attacks because better control can be exerted over who has access to controls.

Internet-of-things (IoT) devices can be vulnerable to cyber-attacks, especially because they tend to be interconnected over the Internet. IoT devices may not only contain information, but in some cases can also provide a platform for remote device control within the system. These devices could bring operational technology (OT)-based cyber-attacks into the physical realm if an adversary gains remote access to devices within the system. This type of infiltration could be used to change alarms in the facility: for example, if alarms thresholds for pressure measurements are too low, operators may experience alarm fatigue and complacence during an actual emergency; if the thresholds are set too high, the system could physically become unstable and possibly over pressurize and rupture before operators are alerted of an issue. In refueling operations, over- or under-filling of storage tanks themselves can occur if networked instrumentation and sensing devices are tampered with.

3.2 Operational Technology

OT refers to the physical and digital systems used to control hardware devices within the system, including devices for monitoring and controlling system operations. This category of devices includes ICS such as SCADA systems and programmable logic controllers (PLCs); these systems are used to monitor and control devices within the physical storage system to ensure that safe operational conditions are maintained. OT devices are generally not networked or cloud-based, making them more difficult for cyber actors to access or control them remotely. Companies may develop custom control and data acquisition systems run on physical, onsite servers, which would make it difficult for bad actors to target without physical access to the system and server. However, they often carry greater responsibility for the physical safeguards of the system than IT devices: a physical mishap in a hydrogen system could lead to events like fires and explosions that could cause extensive harm to people and infrastructure in the vicinity. Thus, OT is an important consideration when safeguarding against cyber-attacks.

Pressure relief devices (PRDs) are a potential target for cyber attackers. PRDs can be set physically and may not be connected to a digital network at all; however, if PRDs are connected to a network, they could be tampered with remotely. Lowering the release pressure on PRDs could lead to pressure relief more often than expected in the system; these loud releases, especially in publicly operated spaces like light-duty refueling stations, may degrade public trust in hydrogen refueling stations and in the hydrogen vehicle industry overall. Additionally, a release of hydrogen into the air has the potential to ignite either immediately, resulting in a jet fire, or after a delay, resulting in an explosion. Regulations, codes, and standards (such as 29 CFR 1910.103 (29 CFR 1910.103), NFPA 2 (NFPA 2, 2023), and CGA G-5.5 (CGA H-5, 2020) provide some guidance regarding the orientation of PRDs to prevent hydrogen directly venting onto other components, which would reduce the chances of system damage from either high-pressure hydrogen impingement or from a jet fire. However, any high-pressure venting and potential fires carry risks for operators and personnel in the vicinity, especially when it is an unexpected or malicious event rather than expected based on conditions within the system. Unnecessary venting also leads to loss of product, which can lead to operational issues or financial losses.

Alternatively, PRDs or pressure relief valve sensors could be targeted in a way that prevents pressure relief when it is needed, such as raising the pressure on a PRD. This type of tampering could lead to a buildup of pressure within the system that exceeds pressure limits, which could result in a pressure leak or even a catastrophic rupture in the system, in which a large quantity of hydrogen becomes exposed to the air at once. This second possibility could lead to subsequent events like pressure vessel bursts that can cause even more harm to the people in the vicinity of the system and the system itself.

Systems should be designed with manual or physical overrides for devices like PRDs. For example, non-networked pressure relief valves with pressure thresholds set directly on the device may be implemented in addition to (or instead of) pressure relief valves that are included in a control system. In this way, a digitally controlled pressure relief may be vulnerable to a cyber-attack, but the system could still be protected by physical pressure relief devices that are not digitally controlled. These types of safeguards are very difficult for cyber adversaries to tamper with if they do not have access to the physical system. Some codes and standards currently recommend and require such physical safeguards; for example, the OSHA regulation 29 CFR 1910.103 mandates the incorporation of safety relief devices in the system, which would provide a manual override for malicious attempts to use digital controls to over pressurize the system. Other requirements in 29 CFR 1910.103 include maintaining sufficient distance between the stored hydrogen and piping carrying flammable substances, not locating stored hydrogen directly under power lines, and ensuring that all electrical equipment within the facility is regulation-approved. These measures can help to limit the amount of physical damage inflicted from a cyber-attack on the system, surroundings, and people in the vicinity.

Devices monitoring or controlling temperature may also be targeted, although pressure ultimately provides the best indication of the physical condition of the system. Temperature is especially important to monitor for liquid hydrogen; if cryogenic temperatures are not maintained and safeguards like thermally activated pressure relief devices (TPRDs) fail to open, high-consequence events like boiling liquid expanding vapor explosions (BLEVEs) can occur. However, devices like TPRDs are unlikely to fail even if temperature-monitoring devices fail, since they are physically designed to release at certain temperatures rather than responding to any sort of feedback from other devices. Additionally, other devices such as vibration and flow sensors can be vulnerable to cyber-attacks; tampering can prevent system controls from detecting and correcting irregular signals or conditions occurring within the system.

OT devices connected to SCADA systems or PLCs may be vulnerable to cyber-attacks but are still very difficult to infiltrate because of the custom nature of many companies' systems and the lack of networked or cloud-based control. If a malicious actor does gain access or control to OT devices, the implementation of pressure relief devices and pressure and temperature instrumentation that can be read directly by operators without any information exchange with computer systems can act as an additional safeguard against tampering of the physical system.

OT devices that are connected to enterprise infrastructure have the potential to provide an attack vector as well. In this case, both the manual overrides discussed earlier and the protections for the IT systems described in the previous section can help prevent an attack that begins with an IT device and targets the higher-consequence OT system.

Industrial internet-of-things (IIoT) devices are emerging technologies that somewhat combine the usage of IT and OT, using sensors and data collection in conjunction with machine learning or artificial intelligence technology to optimize operations within the system. The inclusion of an IIoT system, if left unprotected to cyber-attacks, could lead to adversaries having an easier time gaining access to physical systems. Devices that are tampered with may lead to the collection of faulty data and false conclusions about recommended conditions for the system. Therefore, IIoT technologies should be thoroughly considered and vetted by regulators and companies seeking to use them before being implemented.

4.0 Assets, Threats, and Impacts

Cyber risk is a function of the likelihood of a threat targeting the system, the system's vulnerability to that threat, and the potential impact on the business if the threat is realized. The cyber risk assessment in this study follows the methodology of NIST 800-30: Guide for Conducting Risk Assessment (NIST SP 800-30, 2012). The first step in accessing cyber risk is to identify potential cyber threats and vulnerabilities to hydrogen operations, along with their related business and public health impact. In this section, we provide a detailed identification of common cyber threats and vulnerabilities for different hydrogen storage operations. Note that this table specifically identifies threats caused by cyber vulnerability associated with cyber assets and does not take into account mechanical devices that provide safety relief in the event of an overpressure. The list of these cyber assets, along with their associated threats and impacts are presented in Table 1. The analysis is illustrative of a cybersecurity risk assessment and does not guarantee completeness given the combinatorial attack pathways and evolution of new techniques.

Table 1 Assets, threats, and impacts associated with hydrogen ICS.

Hydrogen Operation	Function	Critical Cyber Assets	Asset Vulnerabilities	Threats	Impact
Plant Auxiliary System	Electrical high-voltage yard or powerhouse AC service station	Station service local control system;	Lack of physical security, legacy systems with weak cyber security, insecure communications	Denial of service attack against local control system causes the system to become unresponsive for the station operator, ransomware; data breaches, insider attack; physical attack or sabotage; equipment failure	Plant operation failure
	Station lighting	Lighting plant control system	Unauthorized remote access, lack of physical security	Unauthorized individuals gain physical access to the lighting plant control system and manipulate the setting Remote exploitation by attackers if the lighting plant control system is accessible over the internet or connected to an external network	Plant and staff safety
	DC system (supply power to critical component – relay/ protection)	Panel protection and control system**,** sensors, relays, battery backup	Supply chain vulnerabilities, unauthorized remote access	Unauthorized access to DC system and disabled control relays that operate through DC	Unplugged outage, critical component disruption
	Emergency power system (provide backup power)	Control unit, transfer switch relay	Weak cybersecurity control of remote service, supply chain compromise through procurement of counterfeit parts	network or control systems overload with excessive traffic, rendering them inaccessible unauthorized access to control systems, manipulation of settings, disable alarms, or backup generator shut down	hampers the backup operation
	Service transformer	Transformer monitoring system	Disgruntled insiders, lack of or dysfunctional physical security (Metcalf attack)	Unauthorized individuals locally access the transformer monitoring system and manipulate the data collected by the monitoring system, leading to incorrect decisions about the condition of the transformers	Plant operation failure
	Fire detection system	Plant fire detection system, CO_2 fire suppression system, H_2 flame detector	Lack of physical security, inadequate/remote access control, disgruntled insiders	If the fire detection system is connected to the broader plant network without proper segmentation, then an attacker gains access to the network and manipulates and disables the plant fire detection system	Equipment damages, staff safety, operational interruption (trigger the false alarm and unnecessary shut down)

Hydrogen Operation	Function	Critical Cyber Assets	Asset Vulnerabilities	Threats	Impact
	Plant security system	Access control mechanism; video surveillance; network security (firewall); alarm system	Lack of access control mechanism, lack of authentication; lack of redundancy; physical vulnerabilities	Remotely access the plant security system if the access control system relies on weak or default passwords An attacker tampers with or bypasses the plant security system if physical access to the access control system components (such as card readers or control panels) is not adequately protected	Plant and staff safety' unauthorized access; compromised plant security; regulatory non-compliance
Compression System	Hydrogen compressor	**Pressure sensor** – monitor the hydrogen gas pressure at inlet, outlet, and intermediate stage, **Temperature sensor Vibration sensor, –** detect vibration or mechanical anomalies in compressor, **Flow sensor –** measure the flow rate of hydrogen gas being compressed, **Pressure relief valve sensor** – monitor the pressure relief valves, **Control and monitoring system**	Use of counterfeit sensors and weak cybersecurity control	access to control and monitoring system utilizing command-line interface and changes to the pressure setting above/below the set level Remote access to the control and monitoring system (if the system is accessible over the public internet or connects to the central office network) and shut down of the compression unit	Pressure sensor diaphragm rupture, automatic shutdown; equipment damage
Storage System	Pressurized hydrogen storage tank	Hydrogen storage control unit (HSCU), H_2 sensor, Pressure sensor, Temperature sensor, Tank level indicator sensor, Flow meter sensor, H_2 flame detector	Counterfeit sensors in the supply chain, malicious insiders, weak authentication systems	Change the temperature/pressure setting of hydrogen storage tank by accessing the hydrogen storage system control unit remotely or locally Man-in-the-middle attack on the communication channel between the fuel cell control system and HSCU By accessing the HSCU, an attacker masks the hydrogen gas concentration warning Change the critical tank parameter and reaction to limit value	Pressure rupture, safety valve malfunction, instrumentation malfunction

Hydrogen Operation	Function	Critical Cyber Assets	Asset Vulnerabilities	Threats	Impact
Electrolyzer	Generate hydrogen gas through the process of water electrolysis	**Gas sensor –** detect the presence and concentration of hydrogen (H_2) and oxygen (O_2) gases produced during electrolysis, **Voltage and current sensor** – measure the electrical parameters (voltage and current) applied to the electrolyzer, **Pressure sensor, Temperature sensor, Electrolyte level sensor –** monitor the level of the electrolyte solution in the electrolyzer, **Electrolyzer control unit –** responsible for controlling various parameter in electrolysis process, **Load cell sensor** – monitoring and controlling the mechanical force or load applied within the electrolyzer	Counterfeit sensors in the supply chain, weak remote access, compromised firmware	Attacker intercepts the communication (inadequately encrypted or secure) between the electrolyzer and the central control system to gather sensitive information or issue unauthorized commands	Equipment malfunction (unplugged gas monitoring system, risk of leaks, pressure buildup)
Fuel Cell	Produce electricity from hydrogen	**Cell monitoring unit** – supervision cell, **Fuel cell control unit** – enable efficient transfer of energy from the fuel cell stack to other power rails, **Fuel cell sensors –** voltage sensor, pressure sensor, temperature sensor	unpatched firmware, weak remote access configuration, inadequate buffer memory	Changing the flow of hydrogen and oxygen in fuel cell stack by locally or remotely accessing the fuel cell control unit DoS attack on control unit	Equipment malfunction, degraded performance

Hydrogen Operation	Function	Critical Cyber Assets	Asset Vulnerabilities	Threats	Impact
Chiller System	Chiller controller system, condenser circuit, cooling capacity system	Temperature sensor, Water valve actuator (PLC), Flow sensor, Chiller control system	Unpatched firmware, malfunction actuator, lack of physical security, single point of failure	The attacker accesses the chiller control system locally and changes temp setpoint/capacity setpoint/chill water flow setting; Denial of services; malware; insider threats;	Degrade the performance and energy efficiency, stop cooling fan, open/close condenser valve; overheating; operational downtime; regulatory non-compliance
Communication Medium	The communication medium of the hydrogen infrastructure	Ethernet, fiber, different ICS protocols	Eavesdropping, man-in-in-the-middle, data spoofing, malware (infected communication medium with malware)	Network connection enumeration, network sniffing, eavesdropping of command and measurements over protocol implementation, network denial of service	Disrupt the operation, introduce latency
Heat Exchanger	Thermal management of hydrogen system, especially fuel cell	Temperature sensor, Temperature controller, Heat exchanger monitoring unit; coolant pump; flow control valves control.	Unpatched software, insecure remote access, lack of network segmentation (often connected to the same network as other critical infrastructure); weak network security.	Change the thermal setting by accessing the heat exchanger unit, disable the overheating protection; malware; data tampering to manipulate temp or flow data to appear normal when in reality the system is overheating	Disable the temperature control; overheating fuel cell;
Dispenser	Safely and efficiently dispense hydrogen gas to vehicles equipped with hydrogen fuel cell systems	Electronic pressure controllers, Automatic shut-off valve sensors, Temperature sensors, Pressure sensors, Flow meter sensors, Flow monitor sensors, Gas control panels, Dispenser monitoring and control unit		Attacker manipulating the firmware of the dispenser's components to modify its behavior, compromise safety features, or gain unauthorized control Ransomware attack – data breaches on dispensers lead to the theft of critical user data (fueling transactions, user data, payments, etc.) DoS attack	Reputation damage, disrupt the operation

5.0 Event Tree Analysis for Cyber Risk

Event tree analysis (ETA) is a forward-looking, graphical modeling technique used in risk assessment and decision making. It starts with an initiating event and explores possible outcomes by following different paths, represented as branches of a tree. Each branch represents a possible event or decision, leading to the next set of branches. The end points of the tree, known as leaf nodes, represent the final outcomes. Benefits of event tree analysis for accessing cyber risk are described below:

- Visually communicates complex cyber risks to stakeholders.
- Helps identify the most critical cyber threats to focus on.
- Assesses the effectiveness of existing security controls.
- Provides data for informed decisions on resource allocation for cybersecurity.

In the context of hydrogen cybersecurity, an event tree analysis can be used to model and assess the potential consequences of a cyber incident or security breach on hydrogen infrastructure. The event tree illustrated in Figure 2 traces down a storage tank pressure failure initiating event that is displayed on the hydrogen storage system control unit (HSCU). As soon as the HSCU unit identifies a change in the pressure setting of the hydrogen storage tank, it initiates an alert through the alarm. The HSCU alarm might be triggered for multiple reasons which are shown in the fault tree in Figure 3. When an operator sees an alarm, they immediately diagnose the abnormalities in pressure settings. The causes of abnormalities in the pressure setting are shown in Figure 4. The next two progressions are manual diagnosis of the pressure valve and communication network diagnosis. Figure 5 shows the fault tree tracing the communication network failure. After finding abnormalities in the communication network, the mitigation procedure was activated. If the two mitigation procedures are not successful and the operator diagnoses communication abnormalities, the system failure happens due to a cyber-attack. It is required to enhance the cybersecurity posture of the hydrogen storage tank pressure unit and its related components and reduce the risk of cyber-attacks. One of the most needed recommendations is to implement a robust network segmentation strategy to isolate the storage tank control systems from other parts of the industrial network. This will help against man-in-the-middle attacks, lateral movement attacks, denial of service (DoS) attacks, and supply chain compromise. This recommendation can be achieved by deploying firewalls or intrusion detection/prevention systems (IDS/IPS) between the HSCU and the hydrogen tank. These firewalls and IPS/IDS need to be configured properly so that they can permit only necessary traffic and block unauthorized access. Another recommendation is to enforce strong access controls and authentication mechanisms in HSCU. This will help to limit access to hydrogen storage components only to authorized personnel and thus prevent insider attacks. We used Idaho National Laboratory's "Saphire" (Idaho National Laboratory, n.d.) tool to generate event trees. The <pass> tag used in the event tree indicates an event outcome that has no bearing on the risk scenario.

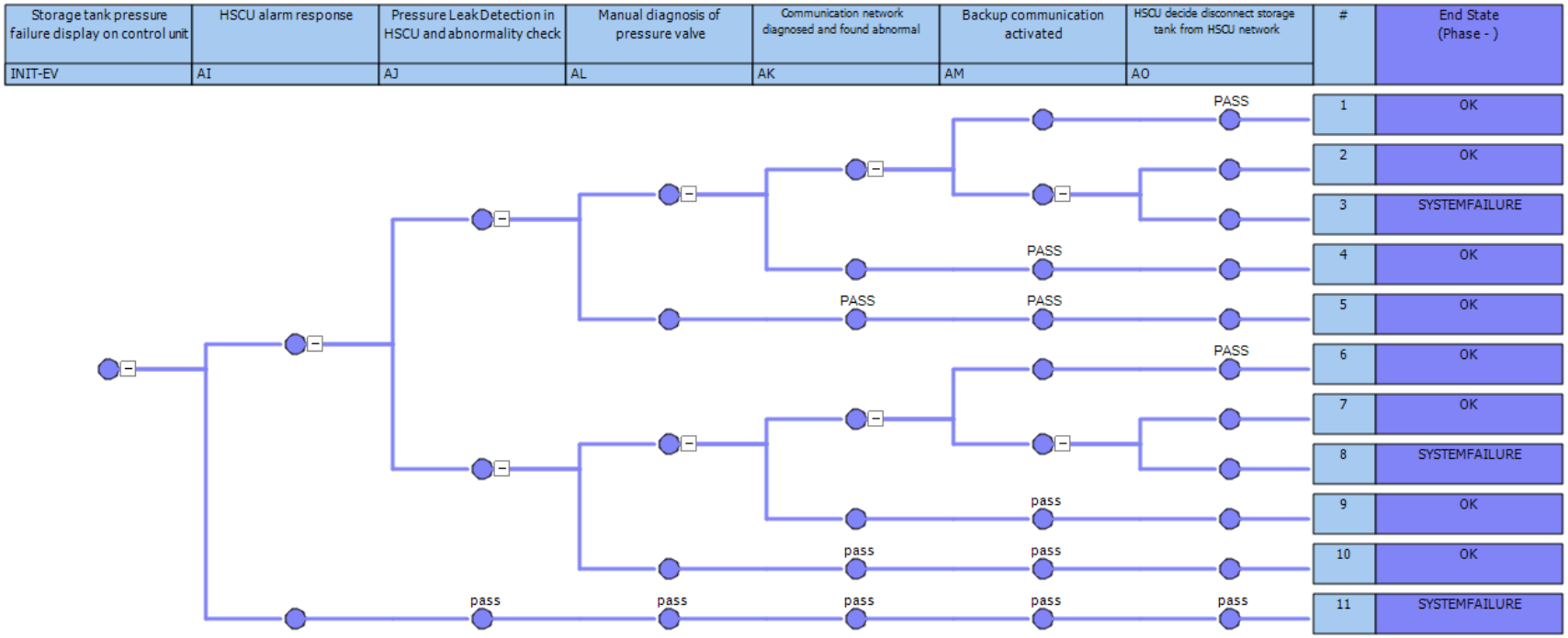


Figure 2 Event tree illustrating a cyber-attack scenario in storage tank pressure setting

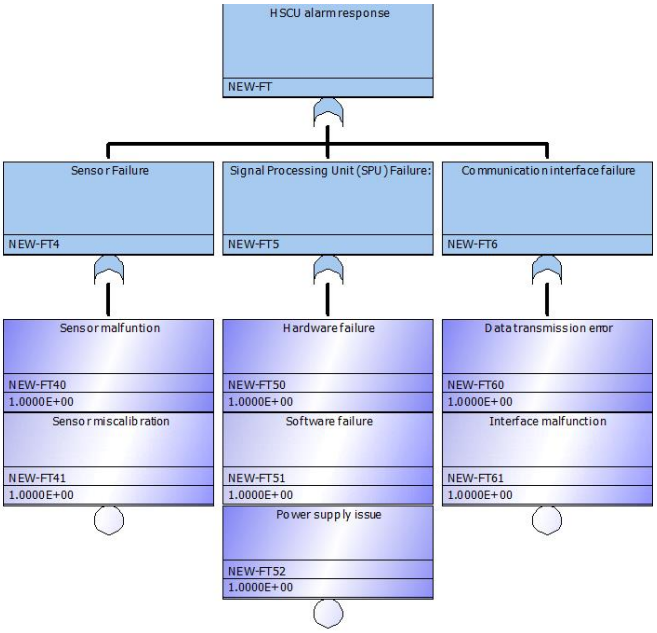


Figure 3 Fault tree tracing the HSCU alarm response failure

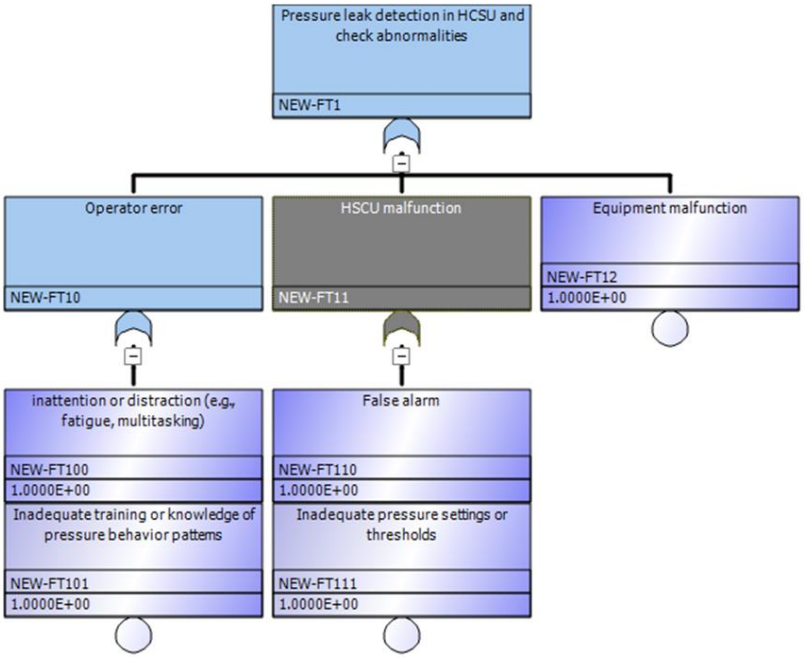


Figure 4 Fault tree tracing the pressure setting abnormalities

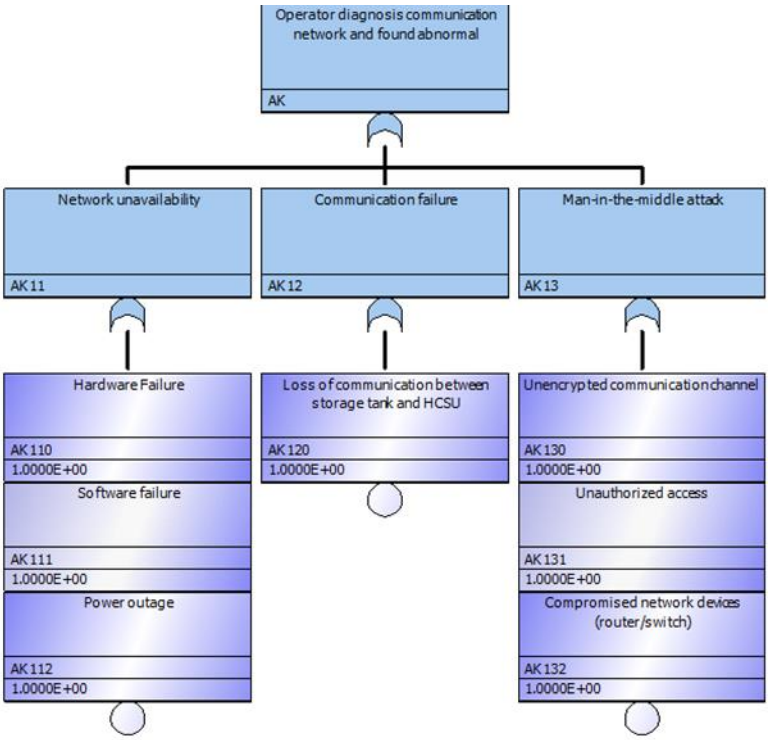


Figure 5 Fault tree tracing the communication network abnormalities

6.0 Conclusion

As companies in the hydrogen storage and dispensing space continue to build facilities, it is important to anticipate and protect key parts of the system to minimize abuse or tampering by malicious cyber actors.

The two major component types of a hydrogen storage system discussed in this report are IT and OT devices. IT devices are more susceptible to cyber entry by adversaries because of their networked nature. The main concerns surrounding IT are related to unauthorized access to data that may contain sensitive information about the system layout, employees or customers of the company, and the company itself. The main concerns for OT devices are related to the severe physical consequences that could result in injuries and even fatalities for people in the vicinity of the facility, as well as the potential for catastrophic and high-cost damage to infrastructure. While OT systems and devices are not as easy to infiltrate as IT, both should be considered by companies and regulatory bodies when designing cyber risk mitigation protocols and standards. Standards like those in IEC 62443, SAE J2601, SAE J2799, and 29 CFR 1910.103 currently contain guidance that can act as safeguards against cyber-attacks, including refueling protocols for hydrogen vehicles, requirements for the incorporation of pressure relief devices into system design, and setback distances from various exposures. Manual valves and setback distances in particular can provide physical protection against an intended over pressurization event from a cyber-attack. Cyber risk mitigation, both in practice and in the regulatory landscape, will continue to be a crucial consideration in the design, maintenance, and operations of hydrogen storage systems. At the site-level, many cyber-attacks are implementation-specific, particularly ones that target physical effects through control of IT assets. Thus, a site-specific approach to risk assessments would be beneficial for cyber risk mitigation.

In addition, ongoing conversations between stakeholders such as component manufacturers, software developers, and the system owner-operator can help clarify responsibility for cyber defenses. Currently, there is ambiguity in the regulatory landscape regarding which actors have responsibility for ensuring that their products are safe for use from a cyber standpoint. Some standards do explicitly explain which stakeholders are responsible for implementing cybersecurity safeguards – for example, SAE J2601-3 specifies that the fueling system has responsibility over fueling process controls and must implement a mechanical overpressure protection system to protect the system. As the hydrogen industry continues to expand, continued discussion to enhance this guidance for other hydrogen applications accompanied by clear guidance around cyber requirements for relevant hardware and software will assist in the development of more robust and resilient hydrogen infrastructure. In this report, we explore a cyber-attack scenario that interferes with hydrogen storage pressure settings through an event tree. The major benefit of event tree analysis is that it shows how a cyber-attack progresses step-by-step along with fault tree tracing, this helps hydrogen operators plan for and respond to cyber security incidents more effectively.

Continuing work on the cyber vulnerabilities of large-scale hydrogen storage systems will help improve the safety of hydrogen storage systems. One key area of research is understanding how interactions between sub-systems, for example, IT and OT devices or even auxiliary components within the hydrogen system influence the physical flow of hydrogen through the system. Additionally, technical improvement of interactions between system devices manufactured by different stakeholders as well as general communications between involved parties can bolster cyber responsibility and overall cybersecurity.

7.0 Bibliography

29 CFR 1910.103. (n.d.). Hydrogen. Occupational Safety and Health Administration. Retrieved from https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.103

C. Peter, E. Wrettos and F. Buchi. (2022). Polymer electrolyte membrane electrolyzer and fuel cell system characterization for power system frequency control. *International Journal of Electrical Power and Energy Systems*.

CGA H-5. (2020). Publication Guides Safe Design, Installation, and Use of Bulk Hydrogen Supply Systems. Compressed Gas Association. Retrieved from Compressed Gas Association: https://portal.cganet.com/publication/details?id=H-5

Chatterjee, D. (2021). *Cybersecurity Readiness: A Holisitic and High-Performance Approach.* SAGE Publications.

DOE. (n.d.). *Operational Technology Cybersecurity for Energy System*. Retrieved from https://www.energy.gov/femp/operational-technology-cybersecurity-energy-systems

Idaho National Laboratory. (n.d.). Retrieved from https://saphire.inl.gov

ISA/IEC 62443 Series of Standards. (n.d.). International Society of Automation/International Electric Council. Retrieved from https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

NFPA 2. (2023). Hydrogen Technologies Code. National Fire Protection Association.

NIST SP 800-30. (2012). Guide for Conducting Risk Assessments. National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/pubs/sp/800/30/r1/final

SAE J2601. (2020). Fueling Protocols for Light Duty Gaseous Hydrogen Surface Vehicles. SAE International. Retrieved from https://www.sae.org/standards/content/j2601_202005/

SAE J2601-2. (2023). Fueling Protocol for Gaseous Hydrogen Powered Heavy Duty Vehicles. SAE International. Retrieved from https://www.sae.org/standards/content/j2601/2_202307/

SAE J2601-3. (2022). Fueling Protocol for Gaseous Hydrogen Powered Industrial Trucks. SAE International. Retrieved from https://www.sae.org/standards/content/j2601/3_202209/

SAE J2799. (2019). Hydrogen Surface Vehicle to Station Communications Hardware and Software. SAE International. Retrieved from https://www.sae.org/standards/content/j2799_201912/

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov