Cyber Aspects of Hydrogen

By Yosi Shavit MBA, CISO, CISM, CDPSE, CC

Head of ICS Cyber Security Dept. at the Ministry of Environmental Protection

==

Cyber aspects of Hydrogen manifest in various areas, including production, transportation, storage, and use.

1. **Production:**
   a. **Electrolysis**: Involves passing an electric current through water to decompose it into hydrogen and oxygen for Hydrogen production.

      Cyber risk: Hydrogen is highly flammable and can be explosive, especially in an environment containing oxygen. Cyber intervention in the process may create a detonation effect (Hydrogen, oxygen, and ignition).

   b. **Steam Methane Reforming** (SMR): Natural gas, mainly composed of methane, reacts with steam at high temperatures, releasing Hydrogen.

      Cyber risk: Remote takeover of the process through a cyber-attack may lead to methane gas leakage and explosion, as well as carbon monoxide (CO) release at high concentrations, which is toxic and can cause asphyxiation.

   c. **Heating organic materials** to high temperatures and collecting the generated hydrogen during the heating process.

      Cyber risk: Intervention in the heating process and raising temperatures, as well as altering pressures beyond the required limits, may lead to explosions. Additionally, there is a risk of toxic CO gas leakage.

d. Production of Hydrogen from Alkali Metals (e.g., Sodium or Magnesium):

Process Description: Alkali metals react with water aggressively to produce Hydrogen. The challenge with this method is the release of high-energy, which can cause the Hydrogen to explode.

Cyber risk: Interfering with the process and introducing water could result in the release of high-energy, potentially leading to explosions.

2. Transportation:

Scenario: Hijacking of trucks transporting hazardous materials.

In this scenario, the threat involves the takeover of trucks carrying dangerous materials on their route.

This situation poses risks such as unauthorized access, potential tampering with the cargo, or even the hijacking of the entire vehicle. The consequences of such actions could include the misuse or release of hazardous materials, posing a danger to public safety and the environment. Cybersecurity measures should be implemented to safeguard the transportation infrastructure and prevent unauthorized access or manipulation of vehicles transporting dangerous substances.

3. Storage:

Scenario: Leakage and Explosion Manipulation in a controlled storage system:

The risk is that the potential adversary will take control of the ICS system by cyber-attack and Increasing pressure or temperature in the container or open critical valves.

These actions may result in leakage of Hydrogen from the system (container or pipes connected to the container). Consequences:

Ignition or explosion upon contact with an ignition source (combined cyber operation).

In the case of a leak, the Hydrogen may concentrate in the upper part of the space due to its lighter-than-air nature, reaching a concentration within the explosion range.

In such a case, activating an ignition source near the ceiling (igniting a fluorescent lamp, turning on a fan, or an air conditioner) could lead to a significant explosion.

4. Usage:

Scenario: Remote Cyber Takeover of Vehicles/Trucks Carrying Hydrogen, Resulting in Environmental Damage and Human Harm.

In this scenario, the threat involves the remote cyber takeover of vehicles or trucks transporting Hydrogen, leading to their transformation, and causing environmental damage and harm to human life. The consequences could include the intentional release of Hydrogen, posing risks to both the environment and human safety. Implementing cybersecurity measures for vehicle control systems is crucial to prevent unauthorized access and manipulation, ensuring the safe transportation of hazardous materials.