Introduction

Chemical processes involve the use of complex systems and technologies to produce various chemicals and materials used in everyday life. Automation and digitalization have become integral to optimizing efficiency, productivity, and safety in chemical engineering processes. However, they also introduce cybersecurity risks, such as malware, ransomware, phishing attacks, insider threats, and nation-state-sponsored cyber espionage. These threats can disrupt operations, compromise safety systems, equipment damage, and cause environmental and economic damage.

This research aims to provide an overview of the connectivity of cybersecurity and the chemical industry and proposes formulation of Cyber-Physical Systems (CPS) consisting of control models and strategies to tackle these cyber threats for more sustainable operations.

Discussion

Analysis of previous accidents, such as the Stuxnet worm targeting Iranian nuclear facilities in 2010 and the NotPetya ransomware attack in 2017, shows that vulnerabilities most susceptible to attack are present in the Industrial Control Systems (ICS) and the Supervisory Control and Data Acquisition (SCADA) systems, causing anomalies and process failure. To detect anomalies caused by cyberattacks to processes, we have (2):

- Model-based Detection: A predefined model of the system’s behaviour compares real-time sensor data with the expected values generated by the model.
- Data-based Detection: Historical or real-time data is used to identify abnormal patterns or anomalies using Machine Learning (ML) techniques.

While model-based detection is effective in identifying known patterns of cyber-attacks that deviate from the expected system behaviour, surge attacks can manipulate the system too quickly for detection if sensors are compromised. Hence, advanced data-driven methods (using Machine Learning) are crucial for countering intelligent attacks, they are more adaptable to detecting novel or previously unseen cyber-attacks. They can learn and evolve based on new data and emerging threats.

Thus, a collaborative detection system connected through a feedback loop is proposed that uses both systems to combat cyber threats efficiently.

Benefits of Cyber Protection to Sustainability Initiatives

Cyber-security measures in chemical processes are pivotal for sustainability. Pre-emptive mitigation of cyber-attacks through implementation of cyber-security CPS detection systems prevents catastrophic events like toxic leaks, preserving human health and environmental integrity, fortifying public safety and underscoring environmental preservation.

Integrating Industrial Control Systems (ICS) with internet technologies enables remote process monitoring and when complimented by robust cyber-security system, bolsters operational efficiency and reducing the carbon footprint by minimizing on-site personnel. This diminishes emissions and resource utilization. Promoting sustainable paradigms through digitalization yields enduring benefits: resource optimization, pollutant abatement, and resilient societal cooperation. Strategic digital initiatives pave the way for a technologically empowered, ecologically sustainable future.

Securing the Digital Ecosystem: Designing a CPS Framework for Cyber-Threat Detection for Sustainable Chemical Processes and Operations

By: Zoha Tariq

Priority Topic Area: Digitalisation, including Cybersecurity

Figure 1: New cybersecurity vulnerabilities discovered each year (1)

**Cyber-Physical System (CPS) to Intersect Cyber threats**

To counter cyber threats in chemical processes, a collaborative two-model detection and control system is proposed—demonstrated using a water level control scenario controlled by Programmable Logic Controllers (PLCs):

1. **Initial Screening with Model-Based Detection**: Quickly identifies deviations from expected system behaviour.
2. **Refinement with Data-Based Detection**: Analyses deviations detected to distinguish genuine threats from false alarms.
3. **Feedback Loop for Continuous Improvement**: Establishes a continuous feedback loop between the two detection systems to refine models and algorithms based on new insights and data.
4. **Decision Fusion for Enhanced Accuracy**: Integrates outputs of both detection systems using decision fusion techniques to make more accurate decisions about potential cyber-attacks, then sent to the PLC.

Figure 2: Simple PFD of a Cyber-Physical System (CPS) designed to detect and cross-examine flow anomalies

Figure 3: PFD of a Simple Water Flow System designed to show the implementation of a Cyber-Physical System (CPS) to combat cyber threats

Figure 4: Conceptual cybersecurity bowtie, including examples of cybersecurity breach prevention and mitigation tools (1)

Figure 5: Comparison of features for process and OT cybersecurity bowties (5)