9th International Conference
on Control, Instrumentation
and Automation

December 20-21, 2023

نهمین کنفرانس بین المللی
کنترل، ابزار دقیق و اتوماسیون

۲۹- ۳۰ آذرماه ۱۴۰۲

Panel Discussion

Security of Industrial Automation Systems: necessities and challenges

Wednesday Dec. 20, 2023

10:30 AM till 12.00 (Iran Time)

The Issue (From GPT Point of View)

The security of Industrial Automation Systems (IAS) is a critical concern in today's digital landscape. Some of the most important issues in this domain include:

1. Vulnerabilities and Exploits: Industrial control systems can be susceptible to various vulnerabilities and exploits, making them potential targets for cyberattacks. Identifying and addressing these vulnerabilities is crucial to ensuring the security of IAS.
2. Insider Threats: Insider threats pose a significant risk to the security of IAS. Malicious insiders or negligent employees may intentionally or unintentionally compromise the system's security, necessitating robust access controls and privileged user management.
3. Network Security: Industrial Automation Systems are typically connected to networks, making them vulnerable to network-based attacks. Securing the network infrastructure, implementing strong firewalls, and employing intrusion detection systems become essential to prevent unauthorized access or data breaches.
4. Lack of Security Awareness: A potential issue is the lack of awareness and understanding about cybersecurity among individuals working with Industrial Automation Systems. Educating employees about best practices and promoting a security-conscious culture can significantly enhance the overall security stance.

5. Legacy Systems and Interoperability: Many IAS installations still rely on legacy systems or have interoperability challenges. These older systems may lack the necessary security features and updates, making them more susceptible to attacks. Proper modernization and integration strategies are crucial to address these issues.
6. Supply Chain Risks: The supply chain involved in procuring components and software for IAS can introduce security risks. Ensuring the authenticity, integrity, and security of the supply chain becomes vital to prevent tampering with components or introducing compromised software.
7. Incident Response and Recovery: Having well-defined incident response and recovery plans is crucial in case of a security breach. Rapid identification, mitigation, and recovery processes can minimize potential damages and downtime in IAS.

Addressing these issues requires a multi-layered approach to industrial cybersecurity, combining technology advancements, employee training, robust policies, and collaboration with security experts.

(Created by https://GPTGO.ai)

The following questions have been raised

1. How serious is this issue in the world and in Iran?
2. Which steps have been taken by Industries in the world and in Iran?
3. What the Governments and Policy Makers have done?
4. What do we suggest to the Policy Makers, Academia, and Industries?

Panel Members

- Prof. Heidar Ali Talebi (Amirkabir University of Technology, Iran)
- Prof. Vijay Varadharajan (The University of Newcastle, Australia)
- Mr. Ali Kiaeifar (Modaberan Company, Iran)

The Panel Chair

- Prof. Heidar Ali Talebi