BRIEFING NOTES

BN-24-Emerging technology and military application-Oct2020

SMART MANUFACTURING AND INDUSTRY 4.0

Authors:Edward Gharibian[1] and Kash Khorasani [2]
[1]Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada
[2]Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

SUMMARY

- Advances in AI systems, computational capabilities, and storage capacities have led to emergence of facial recognition technologies where a machine can identify a face using images.
- The Industry 4.0 represents as an emerging technology in the manufacturing sector that has potentially introduced many cybersecurity changeless.
- The main concern for adoption of appropriate security measures in industry is the lack of awareness and expertise in the fields of security, cyber-physical and/or Industry 4.0 systems.
- Industry 4.0 represents as a combination of cyber-physical systems, the Internet of Things, and the Internet of Systems. Industry 4.0 also related to smart manufacturing processes.

CONTEXT

- The use of IoT and cyber-physical systems in everyday life and specially in the manufacturing industry has resulted in major changes, if not revolutionized them. These new technologies that are known as Industry 4.0, mainly represent integration of cyber-physical systems (CPS), the Internet of Things (IoT), and the Internet of Systems (IoS).
- The Industry 4.0, Smart Manufacturing are among the emerging technologies in the manufacturing sector that have introduced many cybersecurity challenges. The challenges are in three main categories People, Processes, and Technologies.
- **People:**
  The main problem for adoption of appropriate security measures in industry is lack of awareness and expertise in the field of cyber-physical and/or Industry 4.0 systems. The engineers and staff who deploy solutions generally have knowledge on security of either IT technologies or operational technologies (OT), and not both, whereas smart manufacturing systems need expertise on several areas including, network security, embedded systems, OT and IT security. Finding qualified expertise becoming a more and more challenging goal.
- **Processes:**
  A gap that is identified for most emerging technologies, including Industry 4.0, is liability of technologies. This is due to the fact that accountability of incidents is becoming more unclear. Considering the number of stakeholders involved in the supply chain of an Industry 4.0 product, and deciding on whom is liable and what is the share of different stakeholders on incidents is a challenging issue. In particular, the longer lifespan of an industrial product relative to an IT product makes the issues of liability more complicated. The liability for Industry 4.0 technologies is actually to be shared among developers, manufacturers, vendors, after sales services, among others.
- **Technologies:**

Integration of Industry 4.0 devices (IoT, and others) with legacy manufacturing equipment introduces interoperability issues for these systems. Secure interconnection of industrial systems specially those which are out of support, is always challenging. For instance, the need to interoperate different devices and platforms from different vendors, with prosperity protocols that are not properly secure, may need careful study of these systems to ensure their seamless and secure operation. By adding the complexity of supply chain of Industry 4.0, makes the need for a common cybersecurity layer across all elements of Industry 4.0 and smart manufacturing as the most challenging issue.

- **The challenges in general can be stated as follows:**
  - Considering the relatively new nature of subjects, there is lack of a comprehensive documentation to address the security issues.
  - Supply chain management represents as one of the well-known challenges. Effective control of the supply chain is an important factor for being able to track components to its source.
  - The security challenges of Industry 4.0 to some extend is due to lack of technological capabilities to connected industrial systems, specifically for the legacy systems, as well as lack of fundamental protection mechanism in the design phase, and lack of advanced security measures such as resilient control systems and encryption protocols for protection of devices that are close to industrial processes. A common and only specific approach of securing the network is insufficient in case an attacker breaks into the network.
  - There are three main challenges for security of Industry 4.0 systems: shortage of expert human resources, lack of comprehensive standards and national and international legislation, and finally technical shortcomings of Industry 4.0 systems.
  - From the point of view of policy issues there are many options and opportunities for issuing proper law enforcements and regulations for implementation of these technologies and defining liability of stakeholders.

CONSIDERATIONS

Considering the current trend in industry toward smart manufacturing, the Industry 4.0 security becomes imperative and essential for sustainable industry and economic growth of the country.

NEXT STEPS (If applicable)

- Cybersecurity should be considered as a critical safety measure in the industry
- Defining guidelines and public policy mandates and regulations regarding liability of technologies is required.
- It is also recommended to offer relevant courses in universities on Industry 4.0 security, for younger future workforce that in the long term will contribute to awareness of cybersecurity of cyber-physical systems