IoT in the Industrial Sector Commentary

It is important to differentiate the Internet of Things into two distinct categories of use cases: Consumer, and Industrial. IoT is used in industrial applications such as energy (oil and gas, etc..), mining, chemicals, transportation (rail, aerospace, etc.) such as manufacturing, monitoring, process control and operations, and supply chain management. Many equipment manufacturers use Industrial Control Systems, otherwise known as ICS, that are used to control processes like manufacturing, product handling, production, and distribution. ICS includes Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems, and programmable logic controllers that incorporate IoT technologies. These are different from IoT technologies used in the consumer market that are prevalent in devices like smartphones, smart wearables, and smart home devices that collect and share data through an internet connection.

IoT technologies in industrial markets together with components like sensors, data storage and integration, data analytics, and machine learning, can be applied to SCADA systems to improve interoperability and coordination among different machines. The sensors collect new data from various equipment and continuously feed the data into the analytics. This way, machine learning algorithms can learn from past data and fine-tune the settings on different machines for thousands or even millions of cycles to reach the optimal point of the entire system. Harnessing IoT in industrial markets brings several benefits:

1. **Increased efficiency in manufacturing operations**. IoT gives manufacturers and industrial operators the ability to automate and optimize their operating equipment efficiency and/or utilization. The use of robotics and automated machinery can boost productivity and help manufacturers streamline productions, reducing unplanned equipment downtime. Using sensors, manufacturers and utilities gain valuable insight into operational performance of pieces of equipment as well as entire systems.
2. **Reduction of errors**. Through digitalization, manufacturers can reduce operational and manufacturing errors generally associated with manual labor. IoT can help reduce errors in operations, even in those operations that are automated like in continuous manufacturing operations. For example, IoT sensors can detect anomalies and/or variabilities in a chemical processing operation and adjust certain parameters to reduce process waste and increase yields. AI and machine learning can do much of the required computing and data analysis and make subsequent predictive recommendations which can improve a manufacturing process.
3. **Predictive maintenance.** IoT technologies can alleviate issues and unplanned machine downtime associated with reactive maintenance. By monitoring equipment performance consistently, industrial operators are able to identify issues before they occur and allows them to schedule maintenance prior to any downtime.
4. **Improved safety**. A fully functioning manufacturing operation that incorporates sensors and other IoT technologies can use the collected data to bolster worker and product safety. Integrated systems can protect workers by providing alerts which could automatically and safely cease operations if an accident is predicted or until an incident is resolved. Safety can be improved with sensors monitoring hazardous conditions and sending alerts when necessary, such as detecting chemical leaks or equipment malfunctions, reducing the risk of accidents.
5. **Cost reduction**. The data provided to manufacturers through Industrial IoT technologies is giving them the knowledge and tools to reduce costs and increase marginal revenue. By

using data-driven insights into operations, production, marketing, and sales manufacturers can steer their business into a more profitable direction.

6. **Enhanced Productivity & Quality:** IoT technologies can improve productivity by providing workers with real-time data and insights. Continuous monitoring of product quality can automatically adjust processes to maintain consistent quality levels.
7. **Data-Driven Insights, Reporting, Compliance:** The data collected by industrial devices incorporated with IoT technologies can be analyzed to gain valuable insights. This data-driven decision-making can lead to innovations, process improvements, and a better understanding of customer needs. It can also simplify regulatory compliance by automatically recording and reporting data required for compliance purposes.

There is a tendency to often place both the Industrial sector and Consumer sector into the same category when discussing applicable standards, best practices, regulations, and legislations. Because, they have different use cases that is not necessarily accurate. As an example, this sector utilizes existing standards and conformity assessment schemes such as the ISA/IEC 62443 series of standards and conformity assessment programs that provide a systematic, practical, and holistic approach to address cybersecurity in product development and across the overall product lifecycle, starting at its inception. Additional justification for the need for this distinction between these two distinct categories of use cases is provided below:

- **Use/Scope**: Consumer devices with IoT technologies are typically used for personal and home use, whereas IoT in industrial devices are used in settings for manufacturing, transportation, energy, and other critical infrastructure.
- **Utility:** Consumer devices with IoT technologies are generally used for convenience, health, personal productivity and entertainment purposes, whereas IoT in industrial devices are used for enhancing productivity, improving efficiency, quality and reducing costs in industrial processes.
- **Applications:** Consumer devices with IoT technologies are used for a range of applications such as home automation, health monitoring, and entertainment, whereas IoT in industrial devices are used for industrial applications such as monitoring and control of machinery, inventory management, and supply chain optimization. These operations may be in harsh environments, require low latency and may operate in long time scales before replacement.
- **Impact:** Cybersecurity breaches in consumer devices with IoT technologies may result in loss of personal data and privacy violations, whereas security breaches in industrial devices with IoT technologies can cause significant damage to critical infrastructure, including production downtime, supply chain disruptions, and safety risks.
- **Life Support:** Some industrial devices with IoT technologies such as medical devices and aerospace systems may involve human safety, and their cybersecurity vulnerabilities can lead to fatal outcomes.
- **Automation:** Industrial devices with IoT technologies are often automated and may interact with other machines and systems, whereas consumer devices with IoT technologies interact primarily with their human users and other consumer devices that have IoT technologies.

- **Reliability:** Industrial devices with IoT technologies must operate reliably and continuously in harsh environments, whereas consumer devices with IoT technologies typically operate in more controlled environments.
- **Privacy and Confidentiality:** Consumer devices with IoT technologies may collect and transmit personal data, and protecting user privacy is a critical cybersecurity concern. Industrial devices with IoT technologies may also collect sensitive data, but the privacy concerns may differ based on the application. The data being transmitted and processed in Industrial IoT environments can be highly sensitive and critical to business operations. This includes manufacturing data, process control information, supply chain data, and proprietary intellectual property. Confidentiality in Industrial IoT extends beyond personal information to safeguard critical industrial processes and trade secrets.
- **Interoperability:** Industrial devices with IoT technologies are often part of larger systems and must be interoperable with other devices and systems, including legacy equipment and other operations technologies. whereas consumer devices with IoT technologies are often standalone and may not require interoperability (although there is a trend towards increased interoperability in certain scenarios)
- **Scalability:** Industrial systems with IoT technologies often involve a large number of devices and must be scalable to accommodate growth, whereas consumer systems with IoT technologies may be smaller in scale
- **Attack Surface:** Industrial devices with IoT technologies have a larger attack surface due to their connectivity and may be vulnerable to various types of cyber threats such as hacking, malware, and ransomware. Consumer devices with IoT technologies may also be vulnerable to similar threats, but the attack surface may be smaller.
- **Criticality:** The cybersecurity of industrial devices with IoT technologies is critical for the operation of critical infrastructure, whereas consumer devices with IoT technologies may not be as critical

The advancement of IoT technologies in industrial applications can further amplify the efficiencies of the manufacturing process, allowing for production goals and outcomes to reach levels of scale that are previously unimaginable and physically attainable. And when properly and responsibly governed and applied, these technologies can achieve these efficiencies while enhancing workers safety and privacy while fostering energy and environmental stewardship.