Industrial IoT and Automation

Challenges in Industrial Networks

Safety

IIoT sensors and devices play critical role in industrial (manufacturing, transportation, etc.) safety.

IIoT leverages low cost and low power devices to implement energy-efficient safety protocols while improving productivity.

The primary focus of safety is on internal risk-based problems in the manufacturing pipeline to prevent broad-spectrum issues like everyday work related to small accidents and as well as major disasters such as nuclear accidents and incidents.

Many industrial facilities utilize multi-layer safety protocols, such as process control monitoring and alarms, Safety Instrument Systems (SIS), physical protection systems, emergency response (local/external) systems.

Alarms constitute a mechanism to inform a certain threshold is breached for a monitored event.
Monitoring is one of the most critical components of safety protocols. Most of the production pipelines require real-time continuous monitoring.
Sensors generate real-time analog/digital data and transmit them to a control unit to analyze and perform activities based on the monitoring value.
Latency is an important problem in monitoring systems. Moreover, physical monitoring is also important like corrosion/erosion monitoring to figure out detrimental effects. Physical protection system involves following equipment: Pressure-relief valves, rupture discs, stream traps, electrical switch-gear, eyewash stations, safety showers, etc.

Recent trends in IIoT safety systems are as follows:

• Computer Vision (CV): The CV technology is being used for anomaly detection (in detecting physical structural or machinery problems) along with other IIoT sensors.

• Wearable electronics: Involves monitoring of Vital life-signal measurements, fall detection, electric shock detection, etc.

• IIoT security to ensure safety: Cybersecurity is also a major concern for safety systems. All IIoT devices should be cybersecurity proof during the operational phase. An external party like competitors or hackers should not halt or cause physical destruction of a production facility or a pipeline. For instance, in June 2010, Iran suffered a cyber-attack in a nuclear facility located at Natanz via Stuxnet cyber-worm [27]. Another major incident was on 31March 2015, Iranian hackers took down the Turkish power grid which caused a massive power outage of 12 h in 44 out of 81 cities. Approximately 40 million people were affected during this outage [30].

• Robotics: AI-driven software technologies are embedded to achieve autonomous decision-making machinery called robots. These devices can operate where a human cannot. Such as in nuclear power plant or under the sea, etc.

Security and Privacy

Interfacing the smart factories with Cyber-Physical Systems (CPSs) and IIoT improves the intelligence of the infrastructures, yet introduces cyber-security vulnerabilities which may lead to critical problems such as system failures, privacy violations and/or data integrity breaches.

As the privacy of the citizens is becoming into prominence, especially in the EU with the General Data Protection Regulation—2016 act, privacy bearing information of IIoT users such as Personal Identifying Information (PII), need to be treated well, so that they will be kept confidential [7].

On average, these are the cybersecurity analysis of today's Commercial off the shelf IoT products:
vulnerabilities are detected per device, 60% has vulnerable firmware's and user interfaces, 70% do not encrypt any communications at all, and 80% fails to request password for authentication that has a secure length.
Henceforth, there are two main methods to fight against intrusions and cyber-attacks against IIoT. One of them is allowing intrusions to happen and then detecting them via Intrusion Detection Systems (IDS).
The other one is prevention of attacks by means of authentication, authorization and access control.

Intrusion Detection
In practice, Intrusion Detection Systems are installed and on demand from every aspects of technological life, from corporate to universities where IT department exists.
Especially, following are the topics of our interest:
• Industrial network and IIoT security
• Smart grid security
• Critical infrastructure security
• Smart city/factory/home security

The main distinction among the anomaly-based IDS and misuse or specification based IDS is, anomaly detection-based systems can detect any kind of bad behavior (theoretically) on the fly but, misuse or specification detection-based systems can only recognize previously known bad behaviours (signatures) [8].

The reasoning behind this is…
Misuse/specification detection-based systems are designed in a way to match previously modelled attack vectors and rules. If an incidence can be categorized in these, then it is called as an attack.

Otherwise, it is called as normal behavior.

These systems work very well with the defined and categorized attacks up until the time of implementation. However, they are quite useless in the case of new attack vectors that cannot be specified with the old ones.
For these situations, anomaly detection-based IDS is suggested.
Hence it is easy to model the normal state than the abnormal one, it is modelled to specify the good or normal phase of the system behaviours.
Therefore, it is logically opposite of the misuse/specification detection-based systems in which the attack signatures and vectors are directly identified. So, anomaly detection-based IDS uses a kind of live reasoning algorithm, meaning that the decision on a future incident might differ from a past one, even if they are the same events.

Besides, as mentioned deeply in discussions that is made, they are easier to setup, as modelling the normal operating conditions or phase of the network is easier than specifically identifying each attack vector. Therefore, the next subsection is dedicated for that.

Each of these approaches is then sub-classified into various methods.

The interested reader is referred to [9] and also Chap. 6 of this book, for a more detailed discussion.

Intrusion Prevention
It is referred to as taking all necessary actions required in order to prevent intrusions.
It might be analogically similar to theft protection systems in real-life security applications such as installment of advanced door locks, infrared detectors, etc.

Some of the methods to be mentioned are as follows but not limited to [6]: Authentication, authorization, access control, ciphering (encryption/decryption), hashing, etc.

Runtime Security Monitoring

The runtime security monitor operates on the state of the industrial system and observes anomalous behavior that occurs either by failures and operational errors or security threats by adversaries.

To guarantee its successful operation the runtime security monitor requires knowledge about the system as well as the trusted states, operation conditions as well as the system output information i.e. what the system produces.

The objective of the runtime security monitor is to identify suspicious and anomalous indicators when i.e. the system stops producing what is intended.

These are depicted as faults or security threats (Fig. 1.7). Then, it acts proactively by replacing the system with a so-called “reversionary” system, that is performing the minimum industrial system functionality defined by the requirements.

The reversionary system ensures redundancy and reliability.

The presence of a runtime security monitor should be always coupled with an industrial network analyzer (Fig. 1.7), as the events and data that are exchanged in the industrial network are encoded in proprietary protocols and message formats.

An example of a network analyzer isWireshark10 providing support for some industrial protocols such as Modbus and DNP3 as well as libraries and extensions for other proprietary protocols.