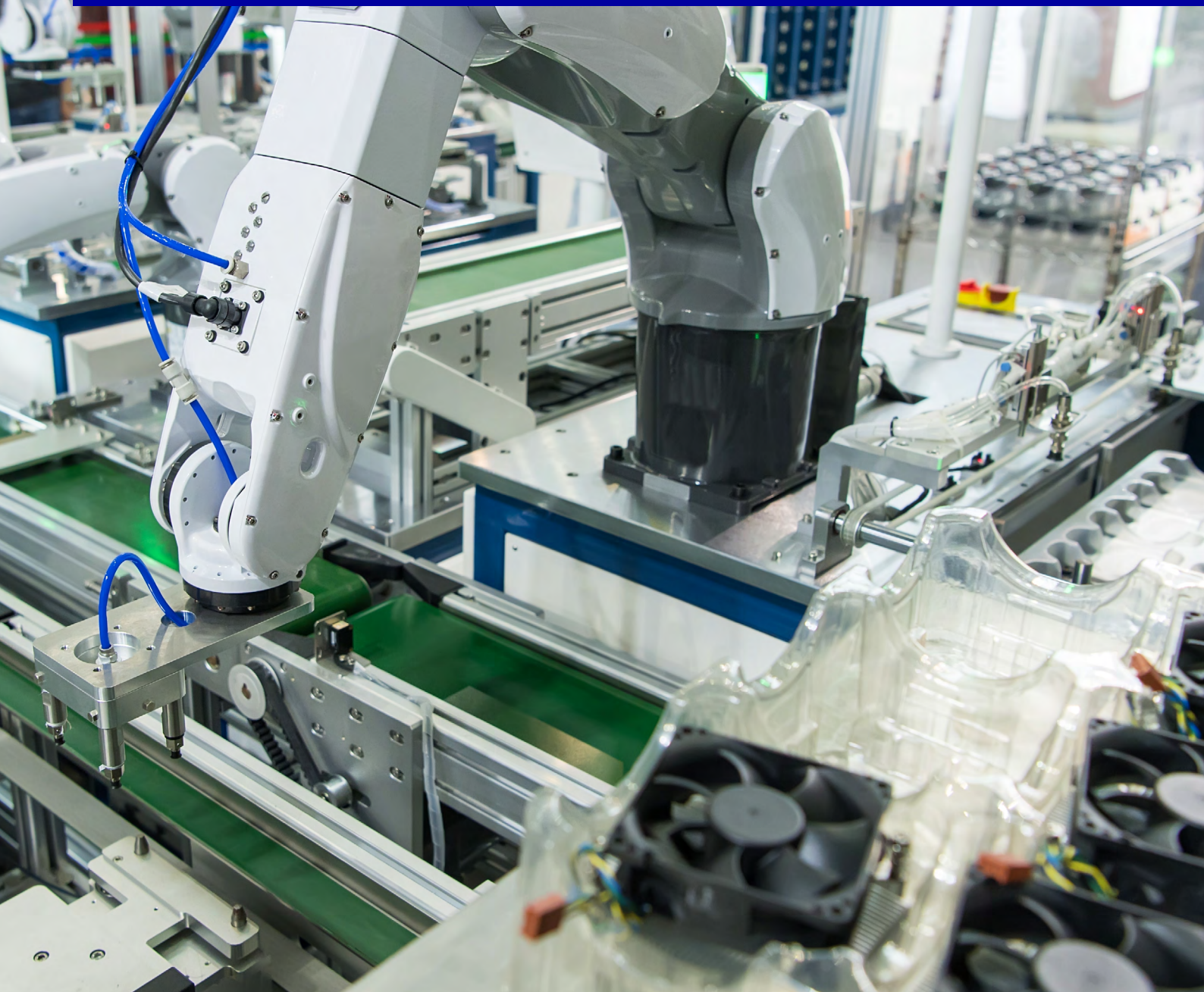
opentext™

How the Internet of things (IoT) drives competitive advantage and establishes new business models

How the Internet of Things drives competitive advantage and establishes new business models



opentext™

Contents

The business drivers and potential gains from IoT solutions are numerous. The business may improve quality of process and operations, reduce downtime, respond to real-time alerts and maintenance issues, and gain greater visibility into assets and production. These are just a few of the possible improvements to the top and bottom line. But the cost of installing new IoT-enabled equipment can be a barrier and existing equipment or assets are functional and may not fully depreciated. The challenge is how to cost-effectively and securely IoT enable legacy equipment. This paper will explain the technical approach to removing that barrier and open the door to future benefits.

Business drivers

There are many business drivers compelling Industrial (IIoT) implementation and digital transformation. By 2025, 60% of manufacturers will use IoT platforms with digital innovation platforms to operate networks of asset, product, and process digital twins for a 25% reduction in cost of quality[1]. Additional business drivers for considering Industrial IoT can assist or augment are:

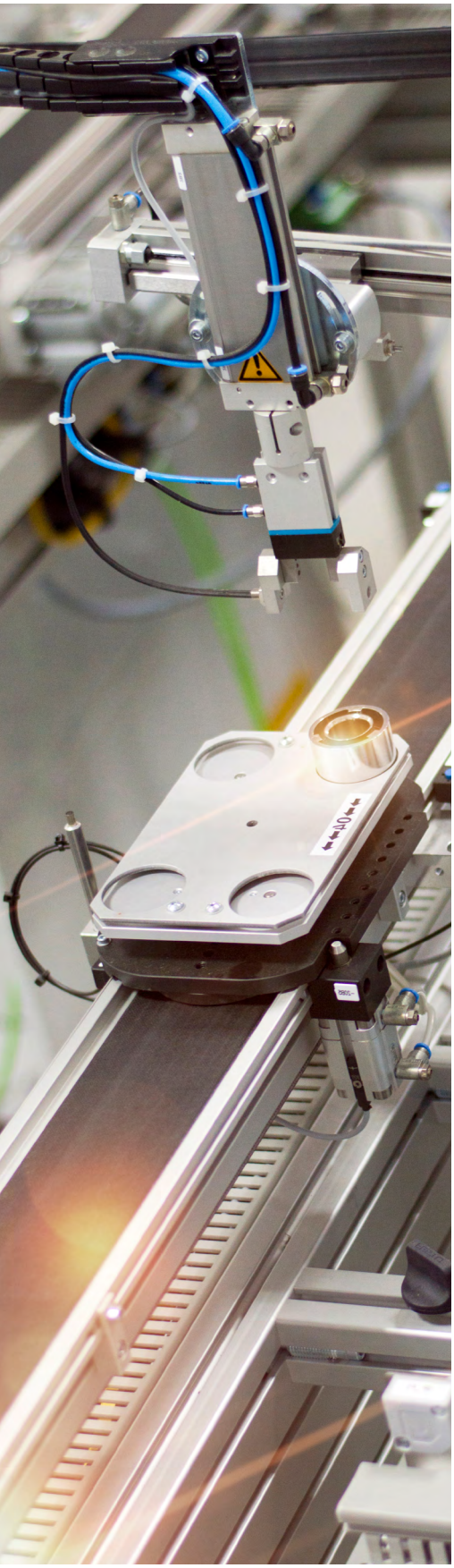
- Reduced asset downtime
- Improved process performance
- Improved rapid service response
- Increase operational reliability and quality control
- Deploy fewer on-site personnel, control hazardous environments
- Respond to real-time alerts on environmental risks
- Remote asset monitoring
- Operational insights for better resource management
- Regulatory compliance

Retrofit

Investments in new equipment solely to enable digital transformation are difficult to justify. The retrofit of sensors to existing equipment, or gather data for IoT from existing equipment, is a compelling alternative. There are additional benefits and reasons for retrofitting existing equipment.

One such benefit is the realization that productivity decreases as assets age. Older equipment has increasing planned and unplanned downtime. Retrofitting existing equipment with IoT technology enables greater visibility into how assets function and how operations can be predictive and efficiently plan and reduce costly downtime. Furthermore, this enables the business drivers described above to be realized and expanded.

1 IDC FutureScape: Worldwide IoT 2020 Predictions, October 2019.



Security

The Internet Society's Online Trust Alliance reports that cyber incidents cost $45B annually. The report further mentions that the vast majority could be avoided through the implementation of proper approaches improving security[2].

The OWASP (The Open Web Application Security Project) Internet of Things Project provides a context and framework in which to make better security decisions[3]. When implementing a retrofit gateway solution, the framework suggests consideration of the following attack vectors:

1. Secure Network Services—The gateway, at a minimum, will interface with both the retrofit sensor devices and equipment as well as the IoT cloud server and services. Also include these considerations in any implementation.
   a. Strict adherence to local protocol standards with anomaly detection and reporting. In other words, if an inbound message does not adhere or meet the established local protocol standard it must issue an alert with diagnostic information and should be reported to the IoT cloud server an/or logged locally for further investigation.
   b. Establish mutual authentication between the gateway client software and the cloud server.
2. Secure data at rest and in motion—The gateway will perform some compute, storage and transmission functions. Each of these systems and functions must be protected by encryption.
   a. Compute—Attestation for activation of a trusted execution environment (TEE).
   b. Storage—Disk encryption and TEE.
   c. Transmission—In addition to mutual authentication with transmission servers, the protocol should leverage transport layer security (TLS) and common encryption protocols such as Advanced Encryption Standard (AES), simon, or others.
3. Ability to update the gateway software or firmware remotely via over-the-air updates (OTA) is necessary to defend against evolving security threats.
4. Physical Hardening—The gateway software will reside within a physical device. The device should be tamperproof to prevent easy access to internal components. Main processor manufacturers such as ARM, Intel and AMD, support the TEE approach to isolated execution and prevent tampering.
5. Device Lifecycle Management—This is necessary to properly maintain and monitor the health, status and audit of the gateway and the associated sensors. This is a system that not only provides full lifecycle management but is designed to support the virtual digital twin and will make the IoT ecosystem more scalable and secure.

Most importantly, because the solution will include the use of insecure and disparate components that were not designed for IoT security, it is critical that the retrofit solution leverage a method to uniquely identify the equipment. The solution must include some form of device attestation to enable strict data governance.

[2] Internet Society, *Internet Society's Online Trust Alliance Reports Cyber Incidents Cost $45B in 2018,* July 09 2019

[3] Open Web Application Security Project (OWASP)

The solution

Protocol conversion

As has been previously described, the core function of the gateway is to be a protocol translator. This protocol translator is a combination of hardware and software to allow the data to flow securely from one discrete network to another.

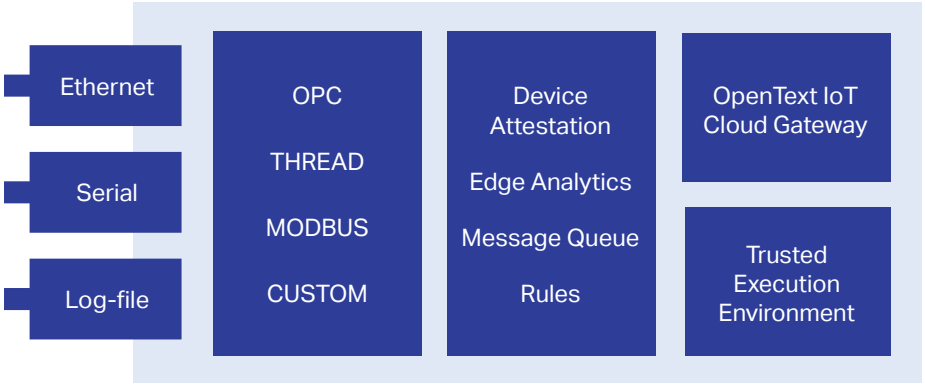


Diagram 1

Diagram 1 illustrates the logical architecture of a retrofit IIoT deployment. The gateway will receive messages from installed, retrofit sensors via a local network interface or other hardwire standard such as twisted pair, serial or parallel i/o bus. Inbound messages will be decoded by the local protocol converter from native protocol such as OLE for Process Control (OPC), MODBUS, Thread or other standard or custom communication method. Within a secure trusted execution environment, the gateway software will then take the standardized message, map the data through the semantic layer. Given a canonical version of the device data, the gateway may apply real-time analytics and rules before forwarding messages to the cloud based IoT platform.

Device attestation

To this point this paper has described the retrofit concept and how it can enable visibility to operating technology that was previously unconnected. Achieving this connectivity, existing equipment, not yet IoT-enabled, will be connected to the internet via a gateway. A gateway acts as the hub and translator of sensor or machine data and communicates it to the cloud for actionable insights.

The challenge is to uniquely identify each device, machine, or sensor and the data sourced from each as being unique in this new ecosystem. When you consider the millions of devices possible in an extended ecosystem, this can be a herculean effort and is often overlooked. An identity-centric IoT platform, leveraging strong authentication systems and processes can address this challenge and allow to the establishment of a unique, digital identity, or a “digital twin” of any entity in an ecosystem, be it a person or a system. In this case, the entity is a device or a piece of equipment. It is the “thing” within the Internet of Things.

When equipment or a device is manufactured and IoT enabled, it will have a unique identifier (for example, a media access control address (MAC) or International Mobile Equipment Identity (IMEI) number) built in. Many software systems use the Universally Unique Identifier (UUID) or Globally Unique Identifier (GUID) standards. Common network equipment often use MAC or other Extended Unique Identifier (EUI) standard to identify and provision allowable equipment to interact within a defined

network architecture. The gateway hardware itself will have a unique, standards-based network identifier, but the legacy equipment and sensors attached to the gateway will be numerous and without a standard identifier.

Device attestation is the action where a human will interact with the IoT system to verify the identity of the equipment. When this occurs, the system will generate unique identifiers for the associated equipment and then as equipment and sensor messages are received, the system will associate the unique identity with those messages.

Why is a unique identity in IoT so important? Data quality begins with device validity and is at the core of any successful and secure IoT project. A critically important aspect of the quality of data is uniqueness. Knowing that the information is uniquely identifiable, its context and thus other aspects of that data including origination, validity, timeliness and consistency are amplified and can be securely orchestrated.

Security and device attestation

Like any other authentication, device attestation should employ expected and established security best practices. Identity governance should be centralized with delegated administration. In other words, those with the authority to attest for a device should have their identity governed by a central authority. Corporate security policy and administration should be applied to the user identity. This way the identity and associated entitlements may be granted, suspended or removed when appropriate (e.g. an employee changes from a designated role, leaves the organization or a machine goes offline for a set period of time).

Furthermore, when centrally controlled, each authentication will be supported by advanced multifactor authentication. The identity usage may be monitored to detect anomalies (e.g. an attempt to authenticate when equipment should be off-line or from a remote location). Leveraging this centralized approach, additional best practices such as audit and forensics may be employed.

Filtering and anomaly detection

The primary use case for nearly all IoT solutions begins with analysis of data. Instinctually one might assume that more data is better. We know that in precision engineering and manufacturing a high level of control is necessary to achieve the required levels of quality. But there is a cost consideration when transmitting large amounts of data over the internet in order to centralize analysis.

As IoT quality algorithms and control loops become more mature, IoT-driven solutions can better define the steady state. In other words, as these retrofit Industrial IoT solutions move beyond the initial use case, operators and stakeholders will be able to know when systems and processes are in control and data scientists can establish thresholds to maintain that control. The local, identified and attested sensor network will provide critical operating technology data in real-time to applications and systems to monitor that steady state. In simple terms, there is no need to continuously report that the lights are on, only send and alert if the lights go off or change from the desired operating state.

OpenText defines big data in terms of variety, velocity and volume. Simple edge analytics will trigger rules to drive actions. Locally, the data is coming at a high volume and velocity and will need to be integrated and stored. Forwarding large data volumes, especially unstructured data to the cloud is inefficient. The edge gateway will monitor the steady state until certain thresholds are passed. Established rules will indicate an undesired or possibly an interesting state, or that an operation could be out of control. When this occurs, the gateway needs to initiate granular and permissible communication to the cloud so action can be taken to address the situation.

opentext™

- OpenText IoT and Supply Chain blogs
- The OpenText Internet of Things Platform
- The OpenText IoT Platform Developer Trial

Why choose the OpenText IoT platform?

Authenticating an ecosystem of things requires experience and understanding of the complex web of relationships between them. The interaction of people, systems and things requires dynamic control of what each unique thing can do, with whom and when. The OpenText IoT Platform is massively scalable and delivers secure data integration, exchanging millions of messages per second, between millions of things, in realtime. It allows organizations to design for the future by connecting manufacturers to products, while providing robust security and connectivity.

OpenText IoT Services accelerate secure, scalable connected product solutions, enabling organizations to register and manage physical things and create solutions that connect their people and systems with the integrated world. The OpenText IoT Platform provides an identity-centric approach needed to securely monitor the status or condition of products and equipment, create secure interactions and integrations, and manage the identity lifecycle of connected things.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

opentext.com/contact