GETTING STARTED WITH Industrial Internet

By Lothar Schubert and G. Ryan Spain

INTRODUCTION

INDUSTRIAL INTERNET

While the "regular" Internet is a "network of networks" that connects people with information, the Industrial Internet (sometimes refered to as Industrial IoT or IIoT) networks machines, systems, people, and physical industries—via the Internet—in order to collect, organize, and analyze the world's industrial data, enabling the next generation of data-driven Digital Industrial companies.

OPERATIONAL TECHNOLOGY (OT)

Operational Technology (OT) describes a piece of software or hardware that directly interacts with the physical world. It either receives information about the environment outside of itself through sensors; or, using actuators, it can make alterations to that environment. OT components represent the data sources ingested into the Industrial Internet, the points of connection between the physical and the digital. If the Internet, as a network that relays information, is a central nervous system, with the cloud acting as a brain, then operational technology makes up the body. It gives the Internet eyes and ears, arms and fingers, so that it can gather information for itself and act upon that information. Still, OT components have local autonomous decision and execution capabilities.

IT/OT CONVERGENCE

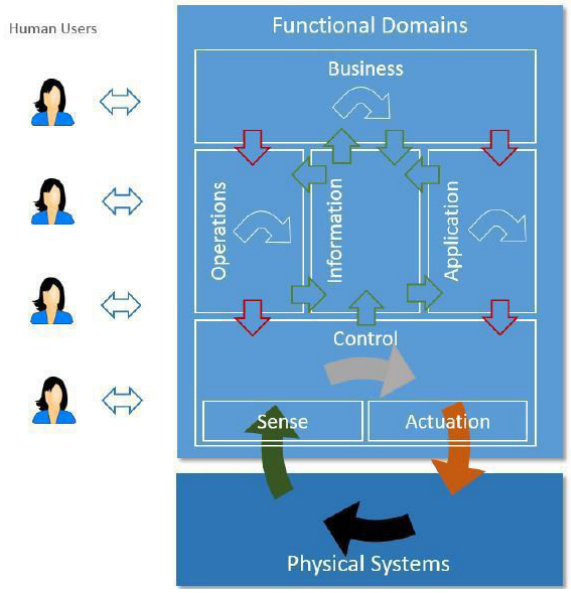
The convergence of information technology (IT) and operational technology (OT) is reshaping long-standing processes in virtually every industry to allow complex systems to monitor, maintain, control and optimize themselves, removing the necessity for human involvement (and thus reducing the possibility for human error) in a growing number of tasks and actions.

IT/OT convergence refers to two distinct trends: First, established IT best practices (for software development, deployment and operations) are being applied to increasingly software-defined OT systems. Second, legacy IT systems (such as ERP accounting or inventory management systems) are being interfaced with business-critical OT systems and Industrial Internet platforms, enabling end-to-end automation of processes such as asset repair and maintenance.

REFERENCE ARCHITECTURE

In an effort to create consistency within Industrial Internet systems with increased interoperability and improved integration, the Industrial Internet Consortium (IIC) drafted the Industrial Internet Reference Architecture.

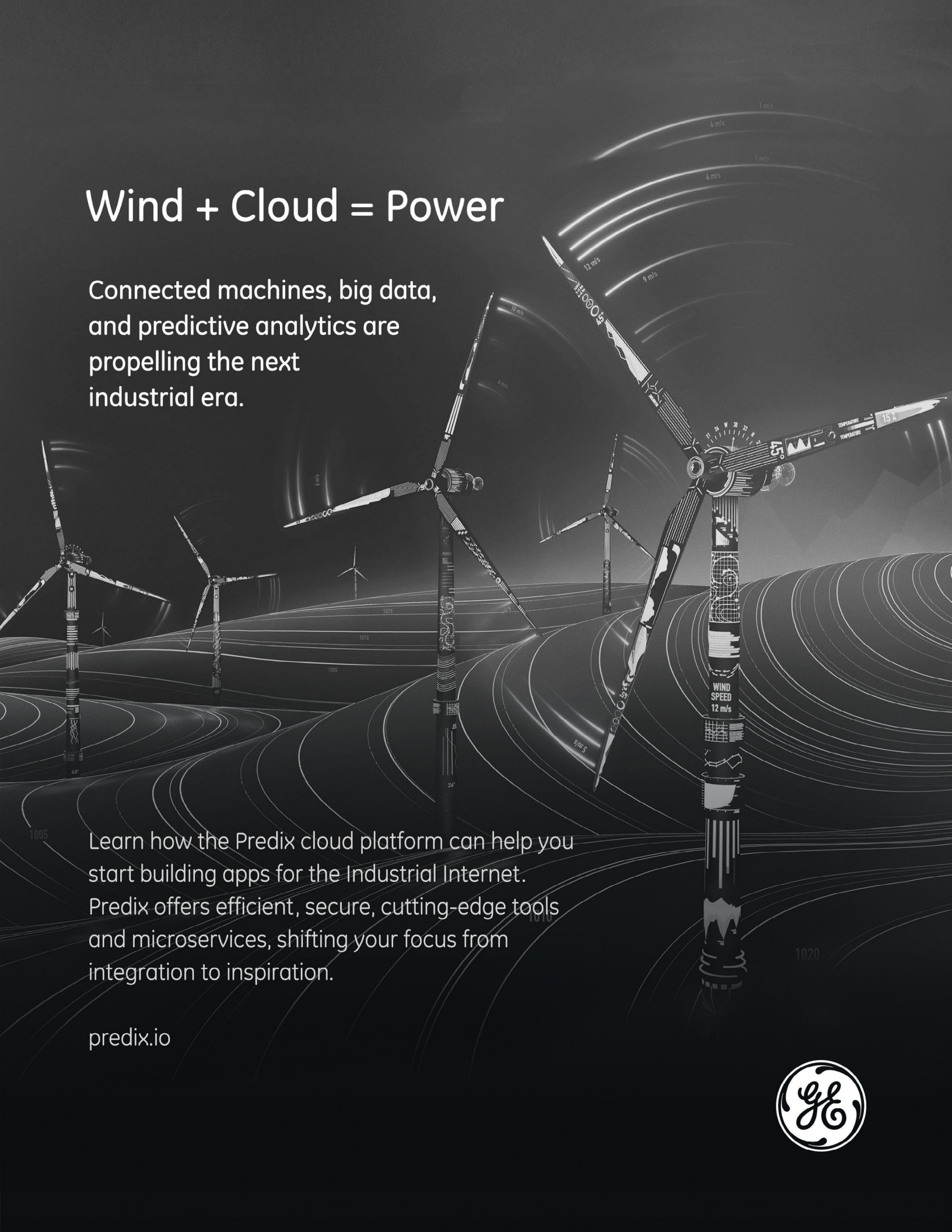
The reference architecture has classified "typical" Industrial Internet Systems into five distinct domains: control, operations, information, application, and business. The following diagram shows how the IIC identifies these domains as relating to one another:



GREEN ARROWS: DATA/INFORMATION FLOWS
GREY/WHITE ARROWS: DECISION FLOWS
RED ARROWS: COMMAND/REQUEST FLOWS

FIGURE 1: *Industrial Internet Systems Functional Domains from the IIC Industrial Internet Reference Architecture*

This Reference Architecture aims to address many Industrial Internet concerns, including security, safety, privacy, and more.



Wind + Cloud = Power

Connected machines, big data, and predictive analytics are propelling the next industrial era.

Learn how the Predix cloud platform can help you start building apps for the Industrial Internet. Predix offers efficient, secure, cutting-edge tools and microservices, shifting your focus from integration to inspiration.

predix.io

SENSORS AND ACTUATORS

SENSORS

Sensors allow for the immediate retrieval of data from the environment around them—essentially translating operating conditions into information that an industrial system can analyze and utilize. They provide these systems with the ability to react to real-time changes without the need for human observation.

Sensors for the Industrial Internet can collect data from environmental factors like:

- Pressure
- Temperature
- Moisture
- Air flow
- Acceleration
- Position/Velocity
- Proximity

An Industrial Internet system must be able to minimize the risk of sensor failure through a fault tolerant control system and ensure that system architecture includes appropriate levels of redundancy. If there is a malfunctioning sensor, it should be identified, and if possible, a backup should be brought online. The platform should have a sensor failure detection method that is based on estimating the displacement (or velocity or acceleration) at a sensor's location using the outputs of other sensors and comparing the estimated value with the sensor's measurement. Lastly, a system should be in place to predict sensor failure and prescribe a fix with minimal operational disruption and downtime.

ACTUATORS

Actuators are what manipulate the physical world in an Industrial Internet system. They are a type of motor, and they convert some form of energy into actual movement. Without actuators, data gathered from sensors would have to be acted upon manually, and automation of industrial systems would be impossible.

Different actuators might be categorized in a number of ways, including input and/or output energy types, or type of movement (e.g. rotational, trajectional, etc.)

Much like with sensors, actuators must be monitored. A fault-tolerant control system must be designed to deal with actuator failures. For instance, the actuator failure detection method can be based on estimating the system input at the actuators' locations and comparing it with the commands given to the actuators. The design of a fault-tolerant control system depends on the use case and the degrees of freedom in terms of hardware redundancy.

POWER CONSUMPTION

Remote industrial sensors and actuators are expected to operate in some of the toughest environments for extended duration of time, often autonomously.

As such, managing power consumption in the overall Industrial Internet system architecture is an ongoing challenge. For example, putting a lot of computing resources on a machine's multicore processor makes it more self-sufficient, but also requires more local power. In contrast, making the machine dumber (for example, leaving only sensors and a micro controller) may remove the need for CPU-intense local processing, however may result in higher power requirements for data transmission.

CONTROL SYSTEMS

Industrial Control Systems (ICSs) are used to monitor and control the processes and interactions between sensors and actuators. ICSs have existed for as long as industrial processes; but the Industrial Internet—by connecting sensors, actuators, and control systems with cloud-based systems—provides ICSs with new meaning. Not only do ICSs become feeders to Industrial Internet platforms, but also the Industrial Internet improves the capabilities of ICSs, for example by delivering optimized decision-making rules and policies.

A few common types of ICS are:

PLC	Programmable Logic Controller An Industrial computer used for automation of (often electromechanical) processes. Often programmed with IEC 61131-3 languages such as Ladder Logic and Structured Text. Continuously monitors input and determines necessary output based on programmed logic. Similar to Programmable Automation Controllers (which can be programmed in languages like C, in addition to ladder logic).
SCADA	Supervisory Control and Data Acquisition Provides supervisory-level control over a larger-scale "system of systems" (e.g. systems that span over multiple areas of the plant rather than one local set of processes). Often includes HMI/SCADA systems, remote terminal units, and local operator interfaces. Evolved with the Industrial Internet of Things to allow for near-real-time state reports and increased security over more standard protocols such as OPC UA.
DCS	Distributed Control System Distributes elements of control across the system itself, rather than centralizing these through a single controller. Generally used to control continuous plant processes (e.g. chemical production). Increased Human-Machine Interface accessibility could simplify access, but could increase security concerns as well.

MACHINE SOFTWARE AND CONNECTIVITY

M2M

Machine-to-machine technology is fundamental to the Industrial Internet of Things. It describes the actual connection and communication between machines, either directly point-to-point, or via the Internet.

M2M connections and communications among Industrial IoT devices are enabled through the use of protocols.

PROTOCOLS

Protocols allow information to be transmitted from one device or system to another device or system over the Internet, or over serial, Ethernet, or other local LANs for inter controller and controller to local application connectivity; they define the ways in which two separate connected entities may communicate with each other.

While HTTP is the standard protocol for the Web, there is no such standard for the Industrial Internet of Things. And it's likely that no one protocol will emerge as a standard any time soon. The Web, at its most basic, needs only to communicate the location of information. But operational technology complicates communications because of the complexity of interacting with system-external environments, and the need for hi-speed transmission of signals.

There are a number of protocols currently being used in Industrial IoT. Some of these include:

PROTOCOL	DESCRIPTION
MQTT	A publish-subscribe protocol used over TCP/IP. Lightweight, low code footprint, minimal bandwidth.
CoAP	*Constrained Application Protocol* Application layer protocol used for constrained (low-power, low-memory, etc.) nodes and networks.
AMQP	*Advanced Message Queuing Protocol* Application layer, wire-level protocol that supports a variety of messaging patterns.
HTTP/2	*Updated version of Hypertext Transfer Protocol* Built with HTTP 1.1 compatibility and performance enhancement in mind.
IPv6	*Internet Protocol Version 6* Updated version of the Internet Protocol Version 4, necessary for assigning unique addresses to the rapidly growing number of machines connected to the Internet (due partially to the increase of Things and M2M connections).
6LoWPAN	*IPv6 over Low power Wireless Personal Area Networks* The 6LoWPAN group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks.

DATA MANAGEMENT

The Internet of Things is completely changing the landscape of data collection and management. The concept of Big Data has often been defined by the three Vs (volume, velocity, and variety), and the data required for the management of sensors, actuators, control systems—and everything in between—is often larger, faster, and more varied than any data that can be collected from a mere website or application.

As such, data management becomes even more complex when dealing with Things. When dealing with data within IIoT, many considerations must be made, such as:

- Which data should be collected
- Which data should be transferred
- Where data should be transferred
- Which data should be stored
- How data should be analyzed as it is collected
- How stored data should be analyzed
- What quality of data is required
- What kind of data transformation needs to occur

But not all data received needs to be stored or analyzed. Storing every piece of data from a sensor may be unnecessary if the environment the sensor detects rarely changes.

In fact, the data itself—once its real-time value has been expended—has no utility until it is analyzed, and useless still unless that analysis provides value. While an actuator might need to constantly transmit data to a control system for monitoring and failure-recovery, that data stream may be static for months if the actuator is properly functioning. For many IIoT devices, only a subset of collected data may need to be transmitted to a Cloud system for central analysis. In cases like this, a data historian can help to gather data on-device for local analysis without the need to transmit every byte.

ANALYSIS

Data Analytics in IIoT has its own significant intricacies. At its most simple, an industrial system may need to analyze data for an alarm check—the system gets a value, checks it against configured thresholds, and generates an alarm if needed. The value here can be low, as the industry has such a high false alarm rate (95% in some cases). Straightforward M2M analytics don't provide much value, though, when compared to what's possible in an IIoT system.

Consider a wind farm as an example. Through an M2M connection, a wind turbine can change the angle of its blades based on the immediate direction of the wind. When all sensors on the farm are connected, however, sensor data can be analyzed so that, as wind begins blowing from the east, more western turbines can start readjusting their blades in relation to the wind and each other, to maximize output across the entire windfarm.

This (extremely simplistic) example is just the tip of the iceberg. Real-time analytics can be combined with historical/trend analytics to increase efficiency within a system, better predict failures, and more.

Industrial Data Science is a fast-growing field, going beyond traditional data science. It applies deep knowledge of industrial processes and actual physical asset properties (such as material compositions or machine designs), to develop and deploy complex mathematical models, delivering often unsurpassed predictive accuracy.

MACHINE LEARNING

Machine Learning provides computers with the ability to learn from data without being explicitly programmed. Due to that, it can improve the state of knowledge workers' decision making and/or completely automate big data discovery and execution processes. There are many factors driving the growth of machine learning:

1. High volume of data generated by sensors, controllers and machines
2. Complexities of connected subsystems and their interactions result in system dynamics that can no longer be fully comprehended, even by the smartest engineers
3. Realization that traditional system engineering has become a bottleneck in delivering cost-effective solutions
4. Availability of less-expensive in-memory storage, faster compute hardware and easy-to-use cloud solutions

Due to the above factors, digital industrial businesses will adopt machine learning in more and more use cases. For instance, in healthcare's computer-aided diagnostics, machine learning models take as their input the patient's condition —such as vital signs, symptoms, lab tests or toxic exposure—to provide disease classification or even recommended therapy. Adoption of computer-aided diagnostics has been low, driven by physicians' resistance and the current lack of confidence society has in these models. This will change as evidence-based diagnostics continue to improve — to offer more accurate diagnosis than human judgments, given the enormous and ongoing proliferation of sensors as well as the use of Big Data to capture expert diagnoses and improve recommendations based on this knowledge base.

HUMAN-MACHINE INTERFACE

The traditional human-machine interface (HMI) is a software interface to a physical asset that is used to provide the operator with information about state, alarms when something goes wrong, and a control interface for managing the asset. In the past, as the systems became more complex, the HMIs became more complex as well, and the result has often been a decrease in productivity and an increase in errors.

The Industrial Internet improves that interface for the operator. The system is now smart, with analytics available to support the user and his or her decisions. The interface continuously adapts to the user based on the user's goals. The interface isn't a list of parameters to be set; it is a model-based interface that lets the user identify the combination of settings that result in the best outcome. The user isn't faced with an overwhelming number of alarms about what has gone wrong, but is presented with projections of how to head off problems and recommended actions.

The actual form factor of the Human-Machine Interface is evolving as well, increasingly also leveraging wearable devices and augmented / virtual reality technology. An oil field rig worker, for example, may wear thick gloves, making interactions with traditional or touch screen panels impractical.

Overall, this allows for better situational awareness and better decision support. Furthermore, as operators grow their expertise and move from controlling systems to, in essence, collaborating with systems, that expertise can be harvested to provide even more effective support and to enable new users to become more effective faster.

SECURITY

Security is a primary concern where developing IoT systems is concerned. When developing anything for Industrial Internet devices, security should be at the forefront of your mind. By increasing the number of connected devices, IoT also increases the number of potential security vulnerabilities.

Furthermore, security breaches in the Industrial Internet could create serious consequences. Where interactions with the physical world are involved, the effects can reach beyond the data-theft enabled by the Internet; without appropriate security, attacks could bring down power grids, manufacturing plants, or healthcare systems. While these are "worst-case" scenarios, the possibility of these kinds of remote attacks is opened when everyday systems are connected.

Security must be built into all IIoT applications from the beginning. Retrofitted security rarely covers the whole of the application, and even if it does, changes to an application built on a non-secure architecture constantly threaten to expose risks.

When developing for the Industrial Internet of Things, consider the following practices:

Device Level

- Encrypt transmitted and stored data
- Authenticate all devices
- Limit direct M2M connections to/from devices
- Integrate security into each device

Gateway Level

- Process all device authentication
- Authenticate to cloud/data store endpoints
- Encrypt gateway credentials

System Level

- Authenticate gateway data
- Encrypt system data
- Collect only necessary data
- Implement a layered defense

Of course, token authentication, data encryption, and layered security aren't all there is to security in IIoT. But building industrial applications with core security concepts in mind from the start will produce more secure systems.

INDUSTRIAL CLOUD

As the Internet of Things increases in popularity, so does cloud computing. The cloud offers technologies—through software, platforms, infrastructures, etc.—to organizations and applications that might not otherwise be available. Whatever the cause, whether it's a lack of skilled developers or excessive up-front costs, cloud solutions can fill any number of gaps in one's IT needs.

This kind of coverage can apply to solutions in the IIoT space, as well. A cloud service for IIoT can handle data collection and analytics; connectivity and M2M connections; encryption, authentication, and other security services; and more, without requiring up-front development costs. And as these services become more mainstream, the number of industrial systems and processes that will be Internet-connected will continue to grow.

Specifically, industrial cloud platforms can handle certain pressing requirements within the Industrial Internet without the need for ad hoc or in-house solutions for:

- Device integration
- Compliance mandates
- Data management
- Data sovereignty
- Security
- Software lifecycle management
- Industrial scale

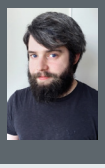
And these platforms can integrate seamlessly between cloud and edge, handling new requirements, issues, and volumes as they occur (e.g., dealing with Industrial Internet data that is growing twice as fast as consumer internet data).

CONCLUSION

The Internet of Things has gained a lot of traction lately, but the realm of consumer IoT—with wearables and home automation—has thus far dominated the scene, at least insofar as mass social opinion and awareness are concerned. But it's the Industrial Internet that will really shake things up in the IT world. As systems become increasingly connected in healthcare, utilities, transportation, manufacturing, agriculture, and more, IoT has the potential to shift from a novelty to a brand new paradigm.

ABOUT THE AUTHORS

Lothar Schubert is leading Developer Relations for Predix, GE's cloud platform for the Industrial Internet. His team helps software developers engage with Industrial IoT through activities ranging from technical onboarding to community engagement, and development of marketing strategies for commercial success.



G. Ryan Spain is the Director of Publications at DZone; he lives in Cary, North Carolina. He received his MFA in Poetry in 2014 and loves mixing his passions of poetry, science, and technology. When he's not producing DZone Refcardz and Guides, he enjoys writing poetry, programming with Java, and learning SQL and R.

RESOURCES

Industrial Internet Consortium:
www.iiconsortium.org

Open Interconnect:
openinterconnect.org

Transparent Cloud Computing Consortium:
www.t-cloud.org/?lang=en

Industrie 4.0 Roadmap:
bit.ly/15Mr1hu

DZone

DZone communities deliver over 6 million pages each month to more than 3.3 million software developers, architects and decision makers. DZone offers something for everyone, including news, tutorials, cheat sheets, research guides, feature articles, source code and more.

"DZone is a developer's dream," says PC Magazine.

DZONE, INC.
150 PRESTON EXECUTIVE DR.
CARY, NC 27513
888.678.0399
919.678.0300

REFCARDZ FEEDBACK WELCOME
refcardz@dzone.com

SPONSORSHIP OPPORTUNITIES
sales@dzone.com

ISBN-13: 978-1-936502-77-6
ISBN-10: 1-936502-77-1
50795
9 781936 502776

VERSION 1.0 **$7.95**