



IoTWorX™

ICONICS IoT Gateway Technology

March 2017
An ICONICS Whitepaper
www.iconics.com



Make the Invisible Visible™

CONTENTS

| | |
|---|----|
| About This Document | 2 |
| Overview and Market Needs..... | 3 |
| Connecting the Internet of Things..... | 3 |
| What is an IoT Gateway?..... | 4 |
| Who Needs a Gateway, Anyway?..... | 4 |
| IoT Gateway Security and Device Management..... | 4 |
| Target Markets..... | 5 |
| Introduction to ICONICS IoTWorX..... | 6 |
| Establishing Secure Cloud Connectivity..... | 8 |
| IoTWorX Transport Protocols..... | 9 |
| AMQP | 9 |
| HTTPS | 9 |
| REST/JSON..... | 9 |
| MQTT | 10 |
| Energy, Building and Industrial Protocols | 10 |
| BACnet | 10 |
| Modbus..... | 10 |
| SNMP..... | 10 |
| OPC Classic..... | 10 |
| OPC Unified Architecture (UA) | 11 |
| ICONICS IoTWorX Options | 12 |
| ICONICS IoTWorX Enterprise | 13 |
| IoT Cloud Connector | 13 |
| IoT Communicator..... | 14 |
| IoT Collector..... | 14 |
| IoT Analyzer | 14 |
| IoT Visualizer..... | 14 |
| IoT Gateway Diagnostics..... | 14 |
| ICONICS IoTWorX Core | 15 |
| IoT Communicator..... | 15 |
| IoT Gateway Diagnostics..... | 15 |
| IoT Alliance Partner Program | 16 |
| Conclusion | 17 |

About This Document

Copyright and Confidentiality

This document contains proprietary information of ICONICS, Inc. and is subject to the condition that no copy or other reproduction be made in whole or in part for any use. No use may be made of information herein except for which it is transmitted, without the express written consent of ICONICS, Inc.

© 2017 by ICONICS, Inc., Foxborough, Massachusetts.

Overview and Market Needs

You have probably heard the term “Internet of Things” (IoT) many times in the recent past, but can you say you really know what it means? Do you know what impact it will have on you and on the work you do? In particular, do you know how it will impact you in the process, factory and building automation industries?

“Internet of Things” can mean a variety of different things to different people in different industries. This paper discusses some opportunities that the Internet of Things brings to the process, factory and building automation industries in general. Additionally, it describes the steps that one company, ICONICS, is taking to leverage this new technology to integrate IoT into one of the world’s most advanced HMI/SCADA, Building Automation, Energy Management and Manufacturing Intelligence packages, along with the benefits that can be achieved.

First, IoT brings a vast communications infrastructure to the process, factory and building automation industries; one that is far beyond anything these industries have typically used in the past. With cloud communications services available from several companies; including Microsoft, Amazon and others; spread across the planet, it has never been easier and more cost-effective to connect even the smallest and least expensive devices to a network – and not just to a local network, but to one that spans the globe.

Second, IoT carries vast amounts of processing power to the process, factory and building automation industries. This processing power, which can also be found in the cloud, is scalable from a single CPU with limited memory and disk space to a large array of CPUs or servers. If used effectively, this processing power can be used to monitor and analyze data, to report events and results, and to solve problems that could never have been solved before.

Third, IoT provides “off the shelf” scalable software applications that enable monitoring, visualization of data, real-time analytics and much more. Due to the openness and standardization in emerging communications protocols, many of these applications will be serviceable with minimal configuration and with little or no middleware.

These are just a few of the important benefits that the Internet of Things can bring to process, factory and building automation applications.

Connecting the Internet of Things

Since relatively few devices actually have the capability to connect to the Internet, to achieve these benefits requires the availability of low-cost bridging devices called “gateways”. In the IoT world, these gateway devices are called “IoT gateways”.

What is an IoT Gateway?

An IoT gateway provides the bridge between an on premise communications network and a cloud-based communications network. Sometimes referred to as an “Edge device”, an IoT gateway provides “Southbound” data connectivity to end devices, completely on premise. It also has a “Northbound” communication path that provides data connectivity between itself and the cloud. In the case of the process, factory and building automation industries, the Southbound communications protocol is typically an industry standard protocol such as OPC UA, BACnet, Modbus, SNMP or Web services, but it can be a proprietary communications protocol as well. The Northbound communication path needs to be highly secure and is often based on a publish/subscribe (“pub/sub”) mechanism. Emerging communication protocols being used for this include Advanced Message Queuing Protocol (AMQP) and Message Queuing Telemetry Transport (MQTT).

Who Needs a Gateway, Anyway?

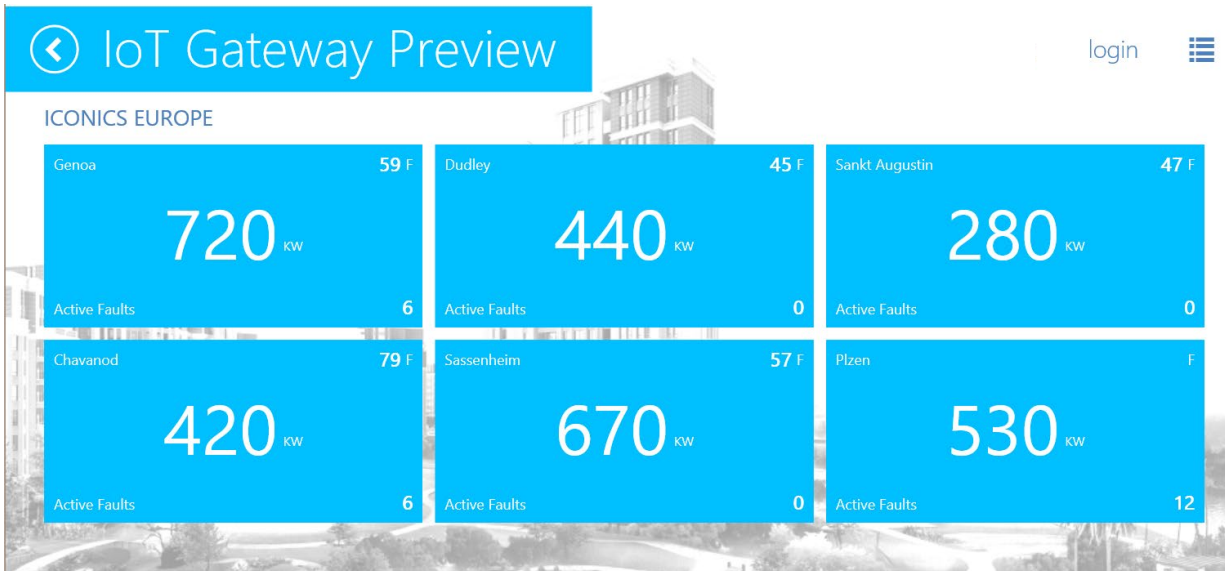
IoT and Industry 4.0 represent the advent of connecting devices, or “things”, with cloud-based systems to harvest hidden information faster than ever before and to drive business value by providing new services. The value to organizations, line of business applications and customers may be attained in the form of cost reduction, new revenue streams, or an improved customer experience. Connectivity is key to achieving these business values. Without being able to connect devices from behind firewalls and securely publish their data to cloud-based applications, organizations will not be able to achieve the promises of advanced analytics through computing power in the cloud. IoT gateways on premise play an important role in this value chain to securely connect things to the cloud. IoT gateways can function in the form of hardware devices and software add-ons to existing installed applications inside a manufacturing site or building.

IoT Gateway Security and Device Management

IoT gateways need to be designed with high security in mind because they serve as a bridge between the data stored on-premise and the outside world. Intel has designed an IoT gateway platform that enables Original Design Manufacturers (ODM) to provide sophisticated IoT gateways that come with advanced security. These security features include unique hardware IDs, secure boot, whitelisting, and disabling onboard peripherals like USB and com ports. With Linux, Windows 10 IoT Core and Windows 10 IoT Enterprise LTSB, we are seeing two major operating system platforms emerging as the cornerstone of IoT gateways. In addition to enhanced security features, edge management is also very important, as IoT gateways need to be managed remotely once they come online and register with the cloud. Remote management and configuration of IoT gateways is imperative to provide efficient and cost effective gateway management. Over-the-air update capabilities will push software updates for the operating system and onboard data communication software.

Target Markets

Target markets for IoT gateways are generally smart buildings or manufacturing applications. Manufacturing applications may require a more robust gateway design for industrial environments. Manufacturing networks are often isolated from the business network and the IoT gateway will need to have two Ethernet adapters to bridge both networks and securely communicate data to the cloud.



ICONICS MobileHMI Tablet View Displaying Data from ICONCS IoTWorX

Introduction to ICONICS IoTWorX

ICONICS IoTWorX is a suite of software that communicates to Microsoft Azure or third-party applications using the most popular transport protocols. Once the IoT Gateway is online, it will register with the IoT Hub so that it can authenticate and send and receive data. Acting as a secure message broker, the IoT Hub will allow for remote device management, provisioning and configuration. Configuration of IoTWorX includes onboard energy, building and industrial protocol point managers (BACnet, OPC UA, Modbus and Web services). Security is inherently built in and provided through the Azure subscription. Relying on Azure security makes IoTWorX one of the most secure IoT gateways in the market. As a result, it can be safely configured from anywhere in the world.

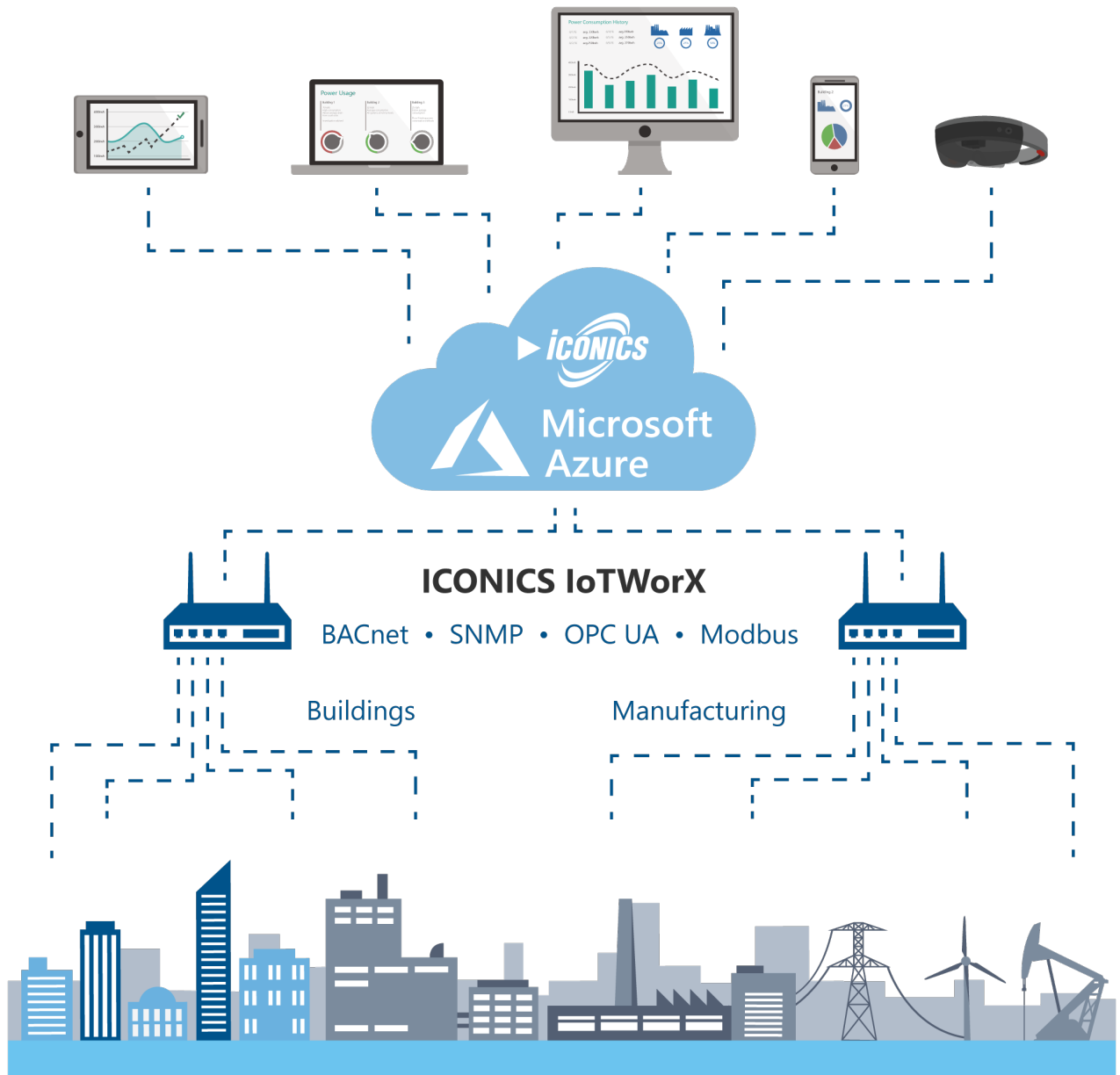
Communication between IoTWorX and the Azure IoT Hub is accomplished via a publish/subscribe method using the bi-directional AMQP transport protocol supported by Microsoft. IoTWorX publishes its messages to the IoT Hub independently from the subscribers that will ingest the data. This decouples the gateway from the consuming applications and services in the cloud. The Azure IoT Hub acts a message broker between the gateway and the connected subscribers, which are the consuming applications.

These consuming applications will be ICONICS GENESIS64, Hyper Historian, AnalytiX and MobileHMI, which are ready to subscribe to the IoT Hub and ingest data provided by IoTWorX. This makes IoTWorX a perfect fit for edge-to-cloud applications taking advantage of Microsoft's Azure IoT Suite services.

IoTWorX is also capable of delivering data to third-party applications such as ERP, MES and other enterprise applications running in private or in public clouds other than Azure. IoTWorX will provide data to third-party applications using Representational State Transfer (REST) and MQTT as established IoT transport protocols. This allows ICONICS to provide the most flexible cloud and IoT solutions in the marketplace.

While IoTWorX can be implemented as a software layer on top of an existing PC or workstation application, the real power of an IoT gateway is in the implementation of low-cost hardware devices that can be placed in remote locations or just about anywhere there is information to be collected. There are a number of vendors that offer a low-cost communications gateway platform, off the shelf. IoTWorX will operate on devices running Intel's Atom processor and Windows 10 IoT Enterprise LTSB (Long Term Service Branch). Hardware manufacturers typically offer several communications options that can include Ethernet, Wireless Ethernet (Wi-Fi), 3G or 4G wireless, ZigBee, Bluetooth, USB ports, and either RS232 or RS485 serial ports.

The following image shows the overall system architecture of IoTWorX and depicts how data is ingested by ICONICS software running in Azure to provide mobile and analytics solutions for remote monitoring. It also demonstrates the concept of providing data to third-party business applications via REST and MQTT.

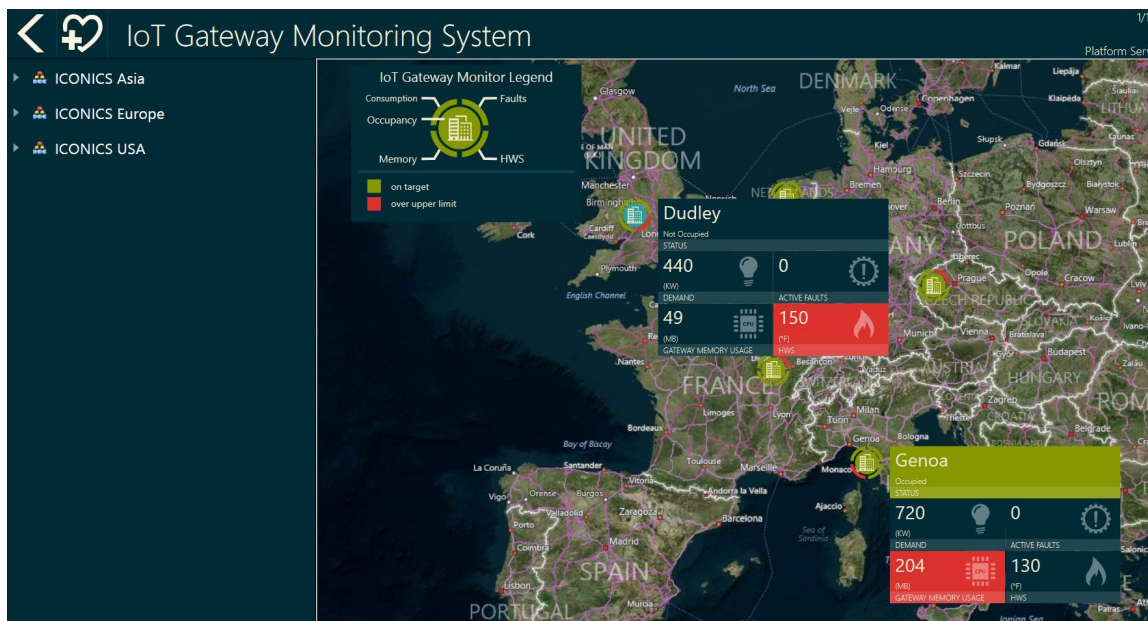


ICONICS IoTWorX System Architecture

Establishing Secure Cloud Connectivity

IoT gateways are cost-effective and easy to deploy with secure communication to the cloud. Facility Directors and Energy Managers now have a great tool at their disposal to quickly deploy proof of concept and production grade applications. IoTWorX is provisioned and communicates data securely via the Microsoft Azure IoT Hub, taking advantage of the inherent security features that come with an Azure subscription. The IoT Gateway securely publishes on premise data to the Azure IoT Hub. The ICONICS IoT solutions don't stop by just providing data to the cloud and leaving it up to the customer to custom write value-add mobile and analytics applications. ICONICS' off-the-shelf visualization, analytics and mobile products running in the Azure cloud subscribe to the IoT Hub and readily ingest the data from the Azure IoT Hub, enabling customers to easily create SCADA, Smart Building, Historian, and mobile applications.

Deployment of IoTWorX is quick and easy. Through secure communications via the Azure IoT Hub, the IoTWorX provisioning and configuration website will display the IoT gateway's location on the map and provide system health monitoring information for the operating system's important processes. IoTWorX onboard communications software, including BACnet, SNMP, Modbus, OPC and more, can be configured remotely from a Web interface. For example, IoTWorX will be able to discover a building's BAS controllers on the BACnet network and publish data to the IoT Hub.



ICONICS IoTWorX Monitoring – Gateway Location and System Status

IoT WorX Transport Protocols

There are several different transport protocols to choose from when it comes to connecting process, factory and building automation devices to the Internet of Things. While there will likely never be a single “winner” amongst them, ICONICS believes it is important to adhere to open standards for maximum interoperability between devices and applications. Each transport protocol offers its own unique set of pros and cons that make it apparent that, when it comes to IoT applications, it is more important to offer the power of choice, rather than just one broad solution. The following is an overview of the leading transport protocols that ICONICS has integrated into IoT WorX.

AMQP

Advanced Message Queuing Protocol AMQP is a binary application layer protocol that was created to substantiate a vast number of messaging applications and communication designs. It provides flow-controlled, message-oriented communication with built-in options for message delivery guarantees, as well as authentication and/or encryption based on widely accepted Internet authentication and data security protocols such as Simple Authentication and Security Layer (SASL) and/or Transport Layer Security (TLS). AMQP is the primary transport layer protocol used by the Azure IoT Hub, and is the default transport layer for IoT WorX, as it supports read and write functionality for command and control of industrial and building automation equipment.

The OPC Foundation has also identified AMQP as one of its protocols of choice upon which to build a reference implementation of Enterprise Service Bus (ESB) connectors, which serves as the basis for its IoT platform. As a charter member of the OPC Foundation, ICONICS plans to support AMQP because of its efficient design, which is optimized for messaging between devices.

HTTPS

The HTTPS transport protocol was designed to serve up requests and responses in the client-server computing model for Web page communications. Clients typically submit an HTTPS request message to the server, which then returns a response message in the form of resources including HTML files and other content, such as completion status details. Within the response message, the HTTP server can also perform other functions on the client’s behalf. The HTTPS protocol can more easily traverse firewalls without the need for specific IT policies to be implemented. This is the main reason that ICONICS is including support for HTTPS, in addition to the other transport protocols, in its IoT WorX software.

REST/JSON

When the need arose to define a stateless means for people to access information in an IoT-friendly way, Representational State Transfer (REST) came to the rescue. REST leverages the HTTP transport protocol to deliver the data, and typically uses JavaScript Object Notation (JSON) to define its presentation. JSON is a flexible, lightweight format similar to XML, and has been proven on many different programming languages.

MQTT

Message Queuing Telemetry Transport (MQTT) is a protocol that was specifically created for SCADA systems and their related networks. It uses a publish/subscribe mechanism to minimize the payload and overhead with application-specific, custom JSON or binary formats. MQTT is widely accepted in IT departments worldwide, with many open source examples available in just about any programming language. ICONICS recommends using MQTT when network bandwidth is at a premium, and always with a secure communication method such as TLS.

Energy, Building and Industrial Protocols

BACnet

The most widely used open communications standard in the Building Automation industry is BACnet. ICONICS GENESIS64™ is the first 64-bit Building Automation system to be certified to the highest level of BACnet Compliance, the B-AWS (BACnet Advanced Workstation Profile), by the independent BACnet Testing Laboratory.

Modbus

Modbus is an open serial communication protocol that has become a standard communications protocol in industry, and is now the most commonly available means of connecting industrial electronic devices. It is used widely by many manufacturers throughout many industries. Versions of the Modbus protocol exist for serial lines (Modbus RTU and Modbus ASCII) and for Ethernet (Modbus TCP). ICONICS supports all three of these versions of Modbus communication.

SNMP

SNMP stands for Simple Network Management Protocol, and is a simple protocol that allows devices to expose useful information to other devices. This information can be the CPU fan speed of a computer or the routing table of a router. Almost every network device answers to SNMP requests. SNMP gives Network Managers access to information from nearly every device connected to the network.

OPC Classic

ICONICS is a charter member of the OPC Foundation and has assisted the foundation over the years by providing source code and hosting interop studies, as well as serving on the board of directors for the foundation. The OPC Classic specifications are based on Microsoft Windows technology, using COM/DCOM (Distributed Component Object Model) for the exchange of data between software components. These include specifications for real-time data access (DA), historical data access (HDA), alarms and events (A/E), XML data access (XML-DA), and data exchange (DX), complex data, security and batch.

OPC Unified Architecture (UA)

OPC UA is the result of a multi-year collaboration of industry leaders who aimed to create an open standard for exchanging information in a rich, object-oriented and secure way. This standard represents the answer to the fundamental need for mapping and exchanging real-life information in a platform-independent way, while maintaining compatibility with the OPC Classic specifications.

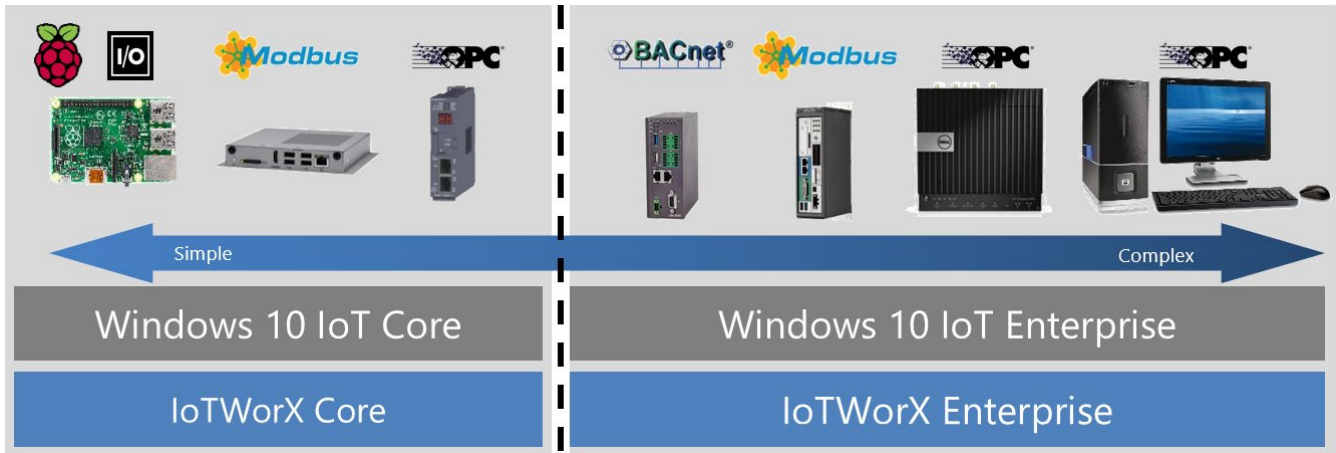
OPC UA is a robust, secure and scalable expansion of the highly successful basic COM/DCOM-based OPC standard communication protocol. It enables the interoperability of best-of-breed, real-time alarm management and historian systems. This allows for a standard model of plant floor integration with the enterprise. Any plant system that is currently using OPC communications can easily add OPC UA applications to their existing system, giving them the added value of Web services that allow for more enterprise connectivity.

ICONICS IoTWorX Options

ICONICS offers two options to deploy IoTWorX based on the complexity and cost considerations of a particular application. Both options support read and write capabilities via AMQP.

- IoTWorX Enterprise is based on Windows 10 IoT Enterprise and supports BACnet, Modbus, SNMP as well as OPC UA and OPC Classic. The application load can be higher due to more performant processors (e.g. Intel Atom or even I5 or I7 used by automation OEMs).
- IoTWorX Core is based on Windows 10 IoT Core and supports simple I/O operations, Modbus, and OPC UA. The application load is lower, as the IoT gateways rely on less performant processors (e.g. Intel Quark or ARM). The target applications are typically cost-sensitive with higher quantities.

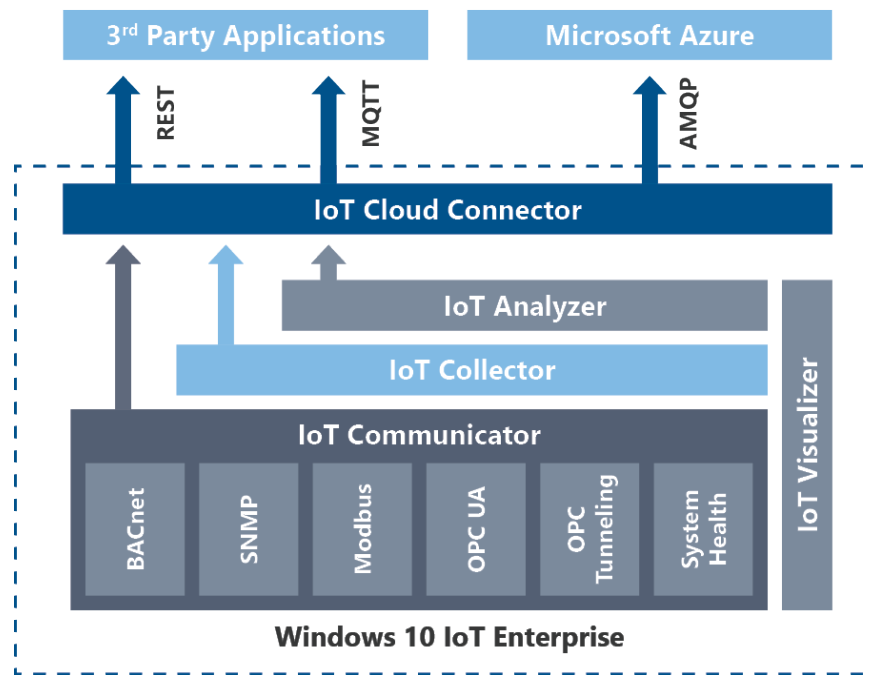
The two options from which customers can choose are shown in the figure below. It indicates which option to select based on the complexity of the application.



ICONICS IoTWorX Options

ICONICS IoTWorX Enterprise

There are five models of IoTWorX Enterprise edition: “IoT Cloud Connector”, “IoT Communicator”, “IoT Collector”, “IoT Analyzer” and “IoT Visualizer”. These provide rich connectivity, data collection, analytics and monitoring for any application. They also provide connectivity to the cloud and third-party applications for maximum interoperability. The Enterprise edition is based on the Windows 10 IoT Enterprise operating system and is able to support all industrial protocols described on the previous page.



ICONICS IoTWorX Architecture for Windows 10 IoT Enterprise

IoT Cloud Connector

The IoT Cloud Connector acts as a protocol converter to transform telemetry data collected from BACnet, OPC, SNMP and Modbus into messages sent to the Azure IoT Hub via AMQP transport protocol. The messages sent to the IoT Hub are TLS encrypted. ICONICS rich client application running in the cloud will readily subscribe to the IoT Hub for data ingesting providing remote monitoring and analytics solutions.

The IoT Cloud Connector can also convert telemetry data into messages sent via MQTT transport protocol to other 3rd party cloud based services or cloud platform (e.g. IBM Watson, Amazon Web Services, Google Cloud etc.). The user has the choice between http or https when sending MQTT messages.

IoT Communicator

The IoT Communicator is the base model. Its purpose is to provide real-time data from facilities and manufacturing sites to the Azure cloud. The IoT Communicator provides data communications for industrial and IT protocols including BACnet, Modbus TCP/IP, OPC Classic, OPC UA, SNMP and much more.

IoT Collector

The IoT Collector is the enterprise model and includes the features of the IoT Communicator model, providing real-time data communications for industrial and IT protocols. In addition, the Collector model has the ability to store and forward data messages in packets with a built-in scheduler to periodically publish that data to the Azure IoT Hub. ICONICS Hyper Historian for Azure, as the subscriber, will be able to consume the data packets.

IoT Analyzer

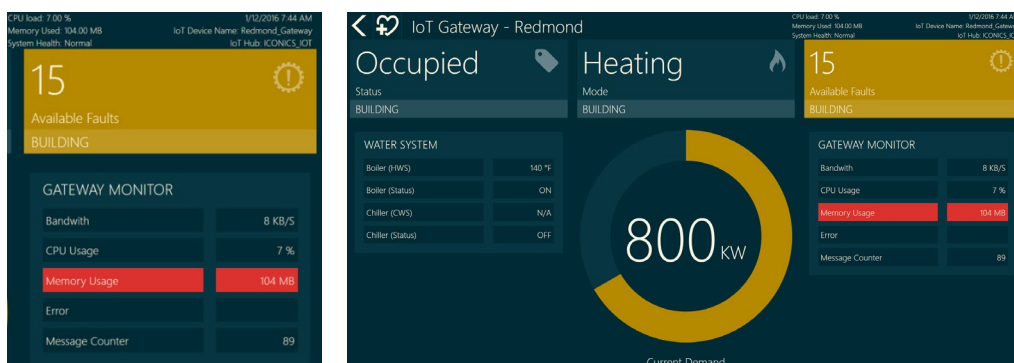
The IoT Analyzer is the enterprise model that includes the features of the IoT Collector model, providing real-time data communications for industrial and IT protocols, plus has the added benefit of edge analytics with onboard Fault Detection and Diagnostics and Workflow technologies. Data will be processed at the edge, which limits the data being published to the cloud.

IoT Visualizer

The IoT Visualizer is an option that will initially be offered to strategic Original Equipment Manufacturers (OEMs) and is meant for applications behind an organization’s firewall to provide an ICONICS HTML5 server on the IoT gateway. This will enable OEM customers to serve up ICONICS graphics directly from the gateway to browsers on an isolated automation network.

IoT Gateway Diagnostics

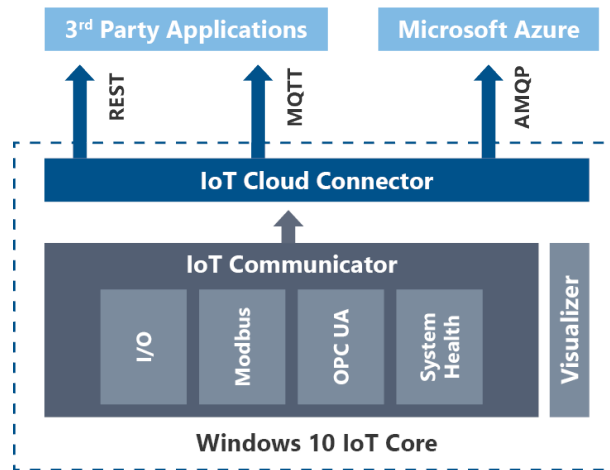
A key benefit of IoTWorX is that it provides built-in system health monitoring that allows for remote diagnostics of the gateway’s system performance. These diagnostics are available via an easy-to-use, intuitive dashboard, some examples of which are shown in the figure below.



ICONICS IoTWorX Monitoring – Gateway System Detail View

ICONICS IoTWorX Core

IoTWorX Core is limited to the “IoT Cloud Connector” and “IoT Communicator”. This provides data connectivity capabilities for applications requiring simple I/O, Modbus TCP/IP, and OPC UA. It also provides connectivity to the cloud and third-party applications for maximum interoperability. The Core version is based on the Windows 10 IoT Core operating system and is intended for lightweight applications.



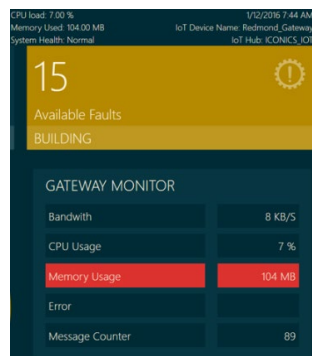
ICONICS IoTWorX Architecture for Windows 10 IoT Core

IoT Communicator

The IoT Communicator is the base model. Its purpose is to provide real-time data from facilities and manufacturing sites to the Azure cloud. The IoT Communicator provides limited data communications for simple I/O, Modbus TCP/IP and OPC UA.

IoT Gateway Diagnostics

A key benefit of IoTWorX is that it provides built-in system health monitoring that allows for remote diagnostics of the gateway’s system performance. These diagnostics are available via an easy-to-use, intuitive dashboard, an example of which is shown in the figure below.



ICONICS Gateway System Monitoring

IoT Alliance Partner Program

ICONICS' IoT Alliance Partner program is geared toward device manufacturers and provides end users with the ability to select from a number of hardware platforms from preferred partners. ICONICS is working in close collaboration with Intel as a General Member of the Intel® Internet of Things Solutions Alliance to help developers test and recommend IoT gateways that customers can rely on for high-performance operations. Through this working partnership, ICONICS and Alliance members provide cutting-edge IoTWorX software technology for the energy, smart buildings and industrial automation markets, delivering ready-to-go communications infrastructure and reducing costs.

As an IoT Alliance Partner, ICONICS will work with you to create a fully-tested IoT gateway solution that is ready for customers to deploy for any energy, smart building or industrial automation application, pre-loaded with standard industry drivers. ICONICS' IoT Alliance Program offers the following benefits:

- Market pull-through will boost Alliance Partners' IoT gateway sales
- Alliance Partners can sell industry-specific solutions
- Ready-to-use IoT gateway with preinstalled industrial protocols
- Pre-tested and approved by ICONICS in cooperation with Alliance Partner
- Featured in ICONICS online directory
- Co-marketing opportunities at ICONICS-sponsored IoT seminars and events
- Option to include a plugin for your native communications protocol on the IoT gateway

Learn more at: www.iconics.com/IoT-Alliance.



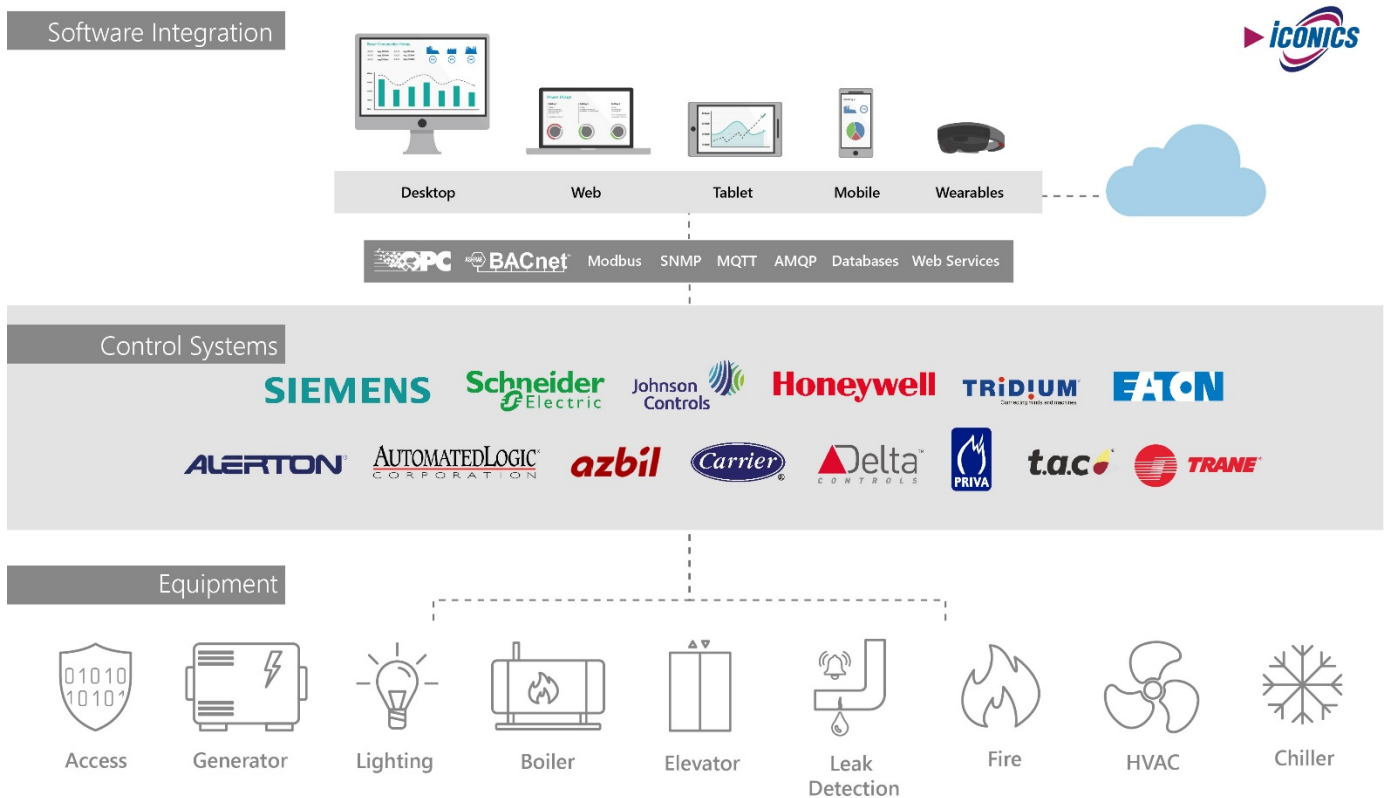
IoT Alliance Program



Conclusion

ICONICS is leading the way in cloud-based solutions with applications to help customers embrace the Internet of Things (IoT). ICONICS products are used in energy smart buildings, automotive, oil & gas, renewable energy, utilities, water/wastewater, pharmaceuticals and many other industries.

Ideally suited for energy solutions, IoTWorX, combined with devices from IoT Alliance Partners, provides a platform for delivering secure and IoT-friendly real-time and historical information to the cloud. It connects to popular energy meters, gas meters, water meters and other critical equipment to provide infrastructure monitoring and timely analytics for energy applications.



In buildings, IoTWorX offers extensive connectivity to the wide variety of building systems available worldwide. It adds value and advanced analytics to any energy management or building automation system. With innovative fault detection and diagnostics technology, IoTWorX advises personnel of actions to prevent equipment failures or excessive use of energy, resulting in reduced downtime and lower energy costs.

For industrial automation, IoTWorX delivers equipment monitoring, predictive maintenance and operational efficiency solutions for manufacturing, water & wastewater, oil & gas, automotive, food & beverage, pharmaceutical and many other industries. It enables rapid access to operational dashboards with real-time key performance indicators (KPIs) for OEE, downtime, quality and production.

ICONICS' IoTWorX is uniquely positioned to keep energy, building and industrial automation companies competitive in this ever-changing world. ICONICS offers a number of additional materials and resources to help in decision-making for IoT-related software solutions. Visit www.iconics.com/loT for a collection of case studies, videos and whitepapers, as well as additional product info.





Founded in 1986, ICONICS is an award-winning independent software provider offering real-time visualization, HMI/SCADA, energy management, fault detection, manufacturing intelligence, MES, and a suite of analytics solutions for operational excellence. ICONICS solutions are installed in 70 percent of the Fortune 500 companies around the world, helping customers to be more profitable, agile and efficient, to improve quality, and to be more sustainable.

ICONICS is leading the way in cloud-based solutions with its HMI/SCADA, analytics, mobile and data historian to help its customers embrace the Internet of Things (IoT). ICONICS products are used in manufacturing, building automation, oil and gas, renewable energy, utilities, water and wastewater, pharmaceuticals, automotive, and many other industries. ICONICS' advanced visualization, productivity, and sustainability solutions are built on its flagship products: GENESIS64™ HMI/SCADA, Hyper Historian™ plant historian, AnalytiX® solution suite, and MobileHMI™ mobile apps. Delivering information anytime, anywhere, ICONICS' solutions scale from the smallest standalone embedded projects to the largest enterprise applications.



ICONICS promotes an international culture of innovation, creativity, and excellence in product design, development, technical support, training, sales, and consulting services for end users, systems integrators, OEMs, and channel partners. ICONICS has over 350,000 applications installed in multiple industries worldwide.

World Headquarters



100 Foxborough Blvd.
Foxborough, MA, USA,
02035

 +1 508 543 8600
 us@iconics.com



Australia

 +61 2 9605 1333
 australia@iconics.com



Canada

 +1 647 544 1150
 canada@iconics.com



France

 +33 4 50 19 11 80
 france@iconics.com



Germany

 +49 2241 16 508 0
 germany@iconics.com



Middle East

 +966 540 881 264
 middleeast@iconics.com



Singapore

 +65 6667 8295
 china@iconics.com



European Headquarters Netherlands

 +31 252 228 588
 holland@iconics.com



China

 +86 10 8494 2570
 china@iconics.com



India

 +91 265 6700821
 india@iconics.com

UK

 +44 1384 246 700
 uk@iconics.com

Czech Republic

 +420 377 183 420
 czech@iconics.com

Italy

 +39 010 46 0626
 italy@iconics.com

Gold
Microsoft Partner

