NEXCOM
The Intelligent Systems

White Paper

IoT Gateways Secure Productivity through Predictive Maintenance

Predictive maintenance allows manufacturers to address failure risks lying in plants in early phases. To be able to make accurate predictions, manufacturers need IoT gateways to monitor manufacturing equipment, systems, and sensors spread across plants and to collect data from them in order to run big data analysis in the cloud. Gaining access to these field devices plays a pivotal role in securing productivity and smoothing plant operation (see Figure 1).

In this white paper, we examine the challenges of deploying IoT gateways and show how these challenges can be met with the NEXCOM cloud-ready IoT gateway solution NIO 100 which integrates critical hardware and software components. We explain how the NIO 100 uses the Intel® IoT Gateway platform to offer a universal solution to bridge the last mile gap between the edge and the cloud. We demonstrate how edge servers installed with NEXCOM IoT Cloud Studio simplify implementation of data handling policies, third-party cloud service integration, and gateway management. We then discuss how the security of IoT gateways can be enhanced with pre-integrated Wind River® Intelligent Device Platform and McAfee® Embedded Control.

Need for cloud-ready solutions

Manufacturers require IoT gateways to provide end-to-end connectivity for monitoring and maintaining manufacturing assets. The IoT gateways connect standalone devices in only partially connected industrial networks to the cloud, filling the critical gap between them. To be useful, IoT gateways must be able to extract information from field data and transfer information to the cloud for analytical, archival, or other purposes. To ensure low cost of ownership and maximum utility, IoT gateways must be easy-to-manage and flexibly adapt to diverse industrial environments.

Figure 1. Gaining access to field devices plays a pivotal role in securing productivity and smoothing plant operation.

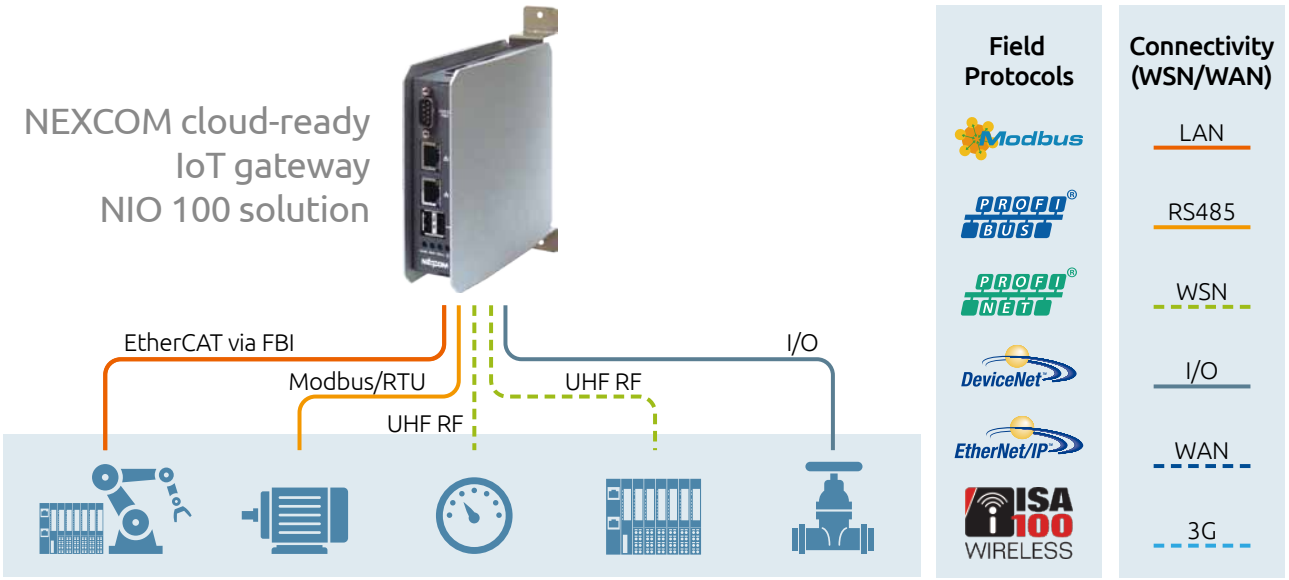

Figure 2. NEXCOM NIO 100 connects standalone devices in only partially connected industrial networks to the cloud, filling the critical gap between them.

The lack of fully integrated IoT gateway solutions has challenged non-IT professionals without programming background like manufacturers in many ways. Problems ranging from incompatible hardware to a deficit in application features compel manufacturers to spend considerable time and efforts struggling to fit IoT gateways into existing infrastructures.

Build end-to-end connectivity

To build end-to-end connections from the edge to the cloud, IoT gateways must support a wide variety of industrial communication protocols, and wired and wireless connectivity. The NEXCOM cloud-ready IoT gateway solution NIO 100 does this by delivering an open-architecture solution based on the Intel IoT Gateway platform powered by an Intel® Quark™ SoC X1021 and fieldbus expansion capability (see Figure 2).

The Intel Quark SoC series features a rich I/O set including two on-chip Ethernet interfaces, PCI Express, USB 2.0, SD/SDIO/eMMC, SPI, UART, and I2C/GPIO. This I/O assortment enables the NIO 100 to establish wired connection to a wide variety of edge nodes. Coupled with pre-validated NEXCOM industrial fieldbus modules, the NIO 101—a modified version of the NIO 100—ensures interoperability with fieldbus-based industrial networks, allowing data communication using Modbus RTU/TCP, PROFIBUS, PROFINET, DeviceNet, EtherNet/IP, and EtherCAT protocols. For industrial networks incorporating image sensors like cameras, a NIO 100 variant powered by a multi-core processor from the Intel® Atom™ processor E3800 product family delivers the graphics performance for image processing.

As to devices or device networks exchanging data over radio frequency waves, the NIO 100 can include wireless connectivity through expansion options to connect to ZigBee-based wireless sensor networks (WSN), Z-Wave-enabled meters, other machine-to-machine (M2M) networks, and of course the internet via 3.5G/LTE and Wi-Fi.

The multi-protocol support and flexible configuration of the Intel® processor-based NIO 100 IoT gateway enables manufacturers to set up heterogeneous networks comprised of field devices, enterprise intranet, and the internet.

Bring intelligence to the edge

With data channels opened, the volume of machine- and sensor-generated data gushing into IoT gateways can be overwhelming and stress network resources at peak hours of data transfer. Setting data handling policies to extract the necessary information for manufacturers therefore takes on practical importance.

To simplify the implementation of data handling policies, NEXCOM edge server installed with the programming tool NEXCOM IoT Cloud Studio offers a web-based graphics user interface (GUI) for network provisioning. Providing a

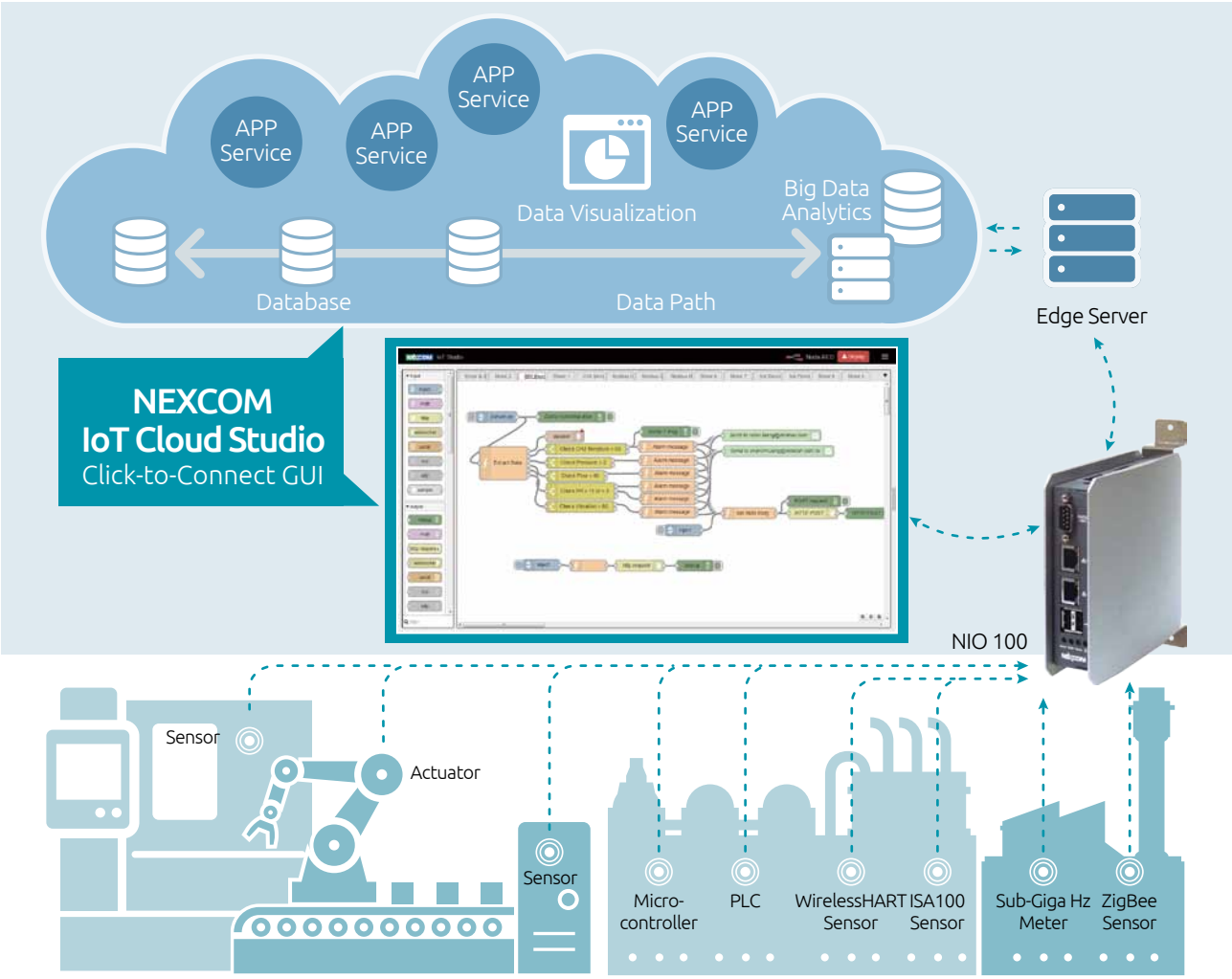

Figure 3. NEXCOM IoT Cloud Studio simplifies network provisioning and third party API integration.

click-to-connect command and pre-integrated third party application programming interfaces (API), this solution allows manufacturers to create granular policies, defining physical connection interfaces, data collection intervals, network protocols, data parsing rules, and data receiving ends for every device connected to NIO 100 (see Figure 3). For manufacturers with special protocol needs, NEXCOM IoT Cloud Studio includes add-on support for proprietary protocol expansion.

Once NIO 100 IoT gateways are installed and data handling polices are applied, NEXCOM edge server will parse the incoming data into small pieces, extract the pieces that matter to manufacturers, convert the pieces into pre-defined formats so that they can be recognized by receiving ends, and then send the pieces to private enterprise clouds, IBM Bluemix, or Axeda Machine Cloud Service.

In addition, NEXCOM edge server can perform preliminary data analysis on the edge, as well as event management. Since NEXCOM edge server can make sense of sensor readings — for instance a pH value — it can decide whether a response is required and incorporate cloud application services to take actions like issuing alert messages via short message services (SMS) or emails. NEXCOM edge server can also help distribute over-the-air update packages if IoT gateways need updating.

Data-driven maintenance

Taking compressed air systems, for example, these systems are widely used in production processes across industries and require custom engineering to meet individual client's needs. With NEXCOM edge server, it takes system manufacturers only a few clicks to put NIO 100-enabled systems under remote monitoring even when these systems are installed on remote sites (see Figure 4).

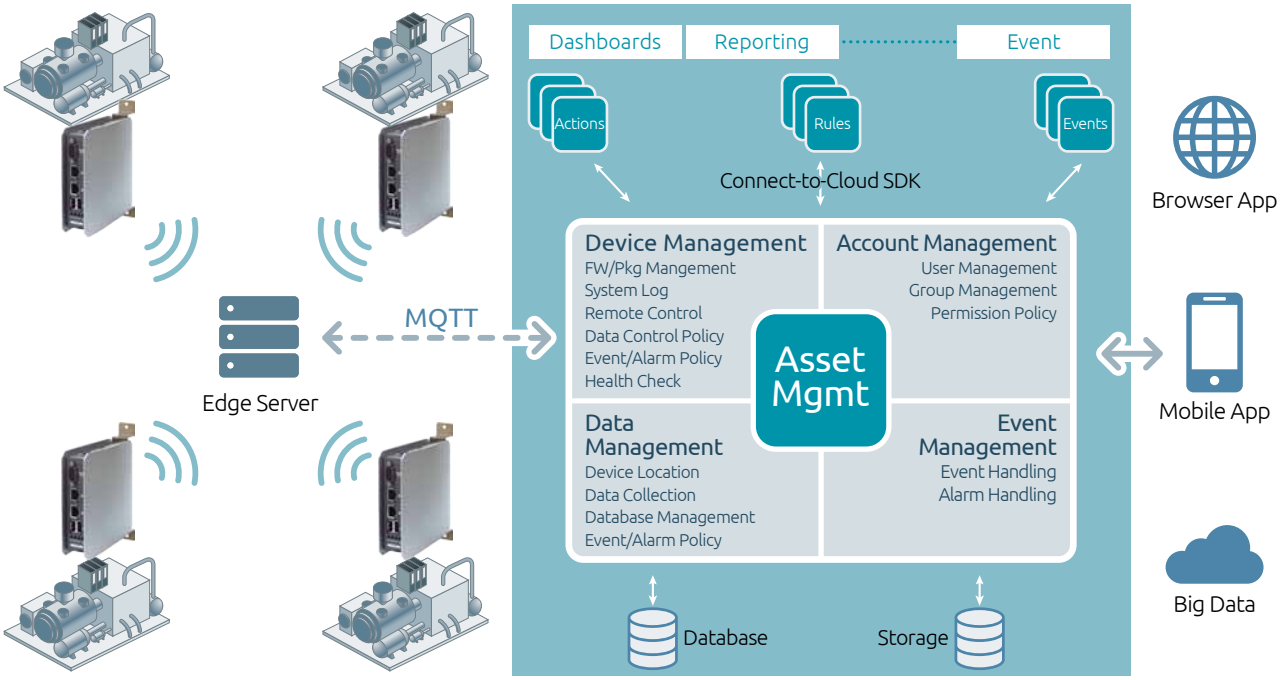

Figure 4. NEXCOM cloud-ready IoT gateway solution NIO 100 allows data-driven maintenance.

If a system's readings or measurements fall out of the expected ranges, system manufacturers will be warned and can run a thorough inspection on the NIO 100-enabled system from the office. Based on the inspection results, manufacturers can either keep a closer watch on the system by shortening data collection intervals using NEXCOM edge server or, if necessary, schedule a maintenance visit with the client to prevent potential system failures from affecting the client's productivity. Furthermore, the collected data can be used as the base for further system design improvement and new extended warranty programs.

Secure data from the bottom up

With productivity at stake, it is important to keep IoT gateways up and running as well as protected from unauthorized access. The NIO 100 based on the Intel IoT Gateway platform and Intel Quark SoC X1021 supports error correcting code (ECC) to avoid potential gateway crashes and changes in data, increasing data integrity. The NIO 100 also benefits from the extended temperature support of the Intel Quark SoC X1021 by faithfully gathering and transmitting data at temperatures from -20 to 70 degree Celsius.

With pre-integrated Wind River Intelligent Device Platform XT and McAfee Embedded Control—both are key parts of the Intel® IoT Gateway platform—the NIO 100 includes Secure Boot. This security feature provides protection from system boot to operations and allows only trusted software to run while stopping applications that have been tampered with.

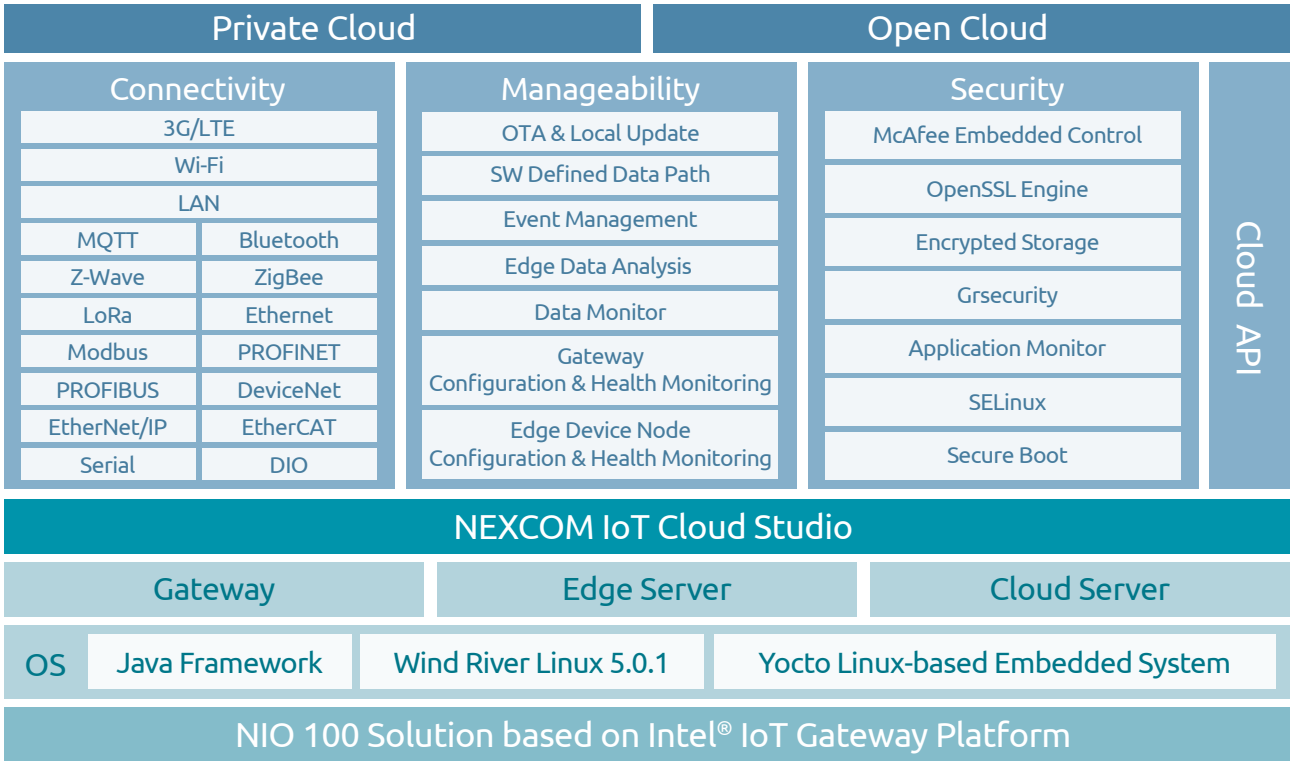

Figure 5. NEXCOM NIO 100 integrates critical hardware and software components to meet the challenges of deploying IoT gateways.

In addition, the included McAfee Embedded Control is an endpoint protection software which uses whitelisting to block malware from execution and installation on the NIO 100. Given the fact that IoT gateways like the NIO 100 are purpose-built appliances that execute only a limited set of applications, the whitelisting approach is more effective at protecting against zero-day attacks than traditional anti-virus software. McAfee Embedded Control allows only policy-based changes that are expected and authorized. Also, the built-in OpenSSL engine can encrypt and decrypt data to avoid in-transit data manipulation.

Conclusion

Designed to simplify and accelerate the implementation of the IoT gateways, the NIO 100 based on the Intel IoT Gateway platform and Intel Quark SoC X1021 lifts barriers to data communication, seamlessly and securely integrating industrial networks with business intranet and the cloud (see Figure 5). Not only does the NIO 100 provide the last mile connection required of the IoT gateways, but the NIO 100 also helps manufacturers take advantage of available cloud applications, shortening deployment time from months to within an hour. As a result, manufacturers can nearly immediately realize the benefits of big data analysis in predictive maintenance, harvesting many benefits in terms of smooth production, higher productivity, financial savings, and more efficient energy use.

Founded in 1992, NEXCOM integrates its capabilities and operates six global businesses, which are Multi-Media Solutions, Mobile Computing Solutions, IoT Automation Solutions, Network and Communication Solutions, Intelligent Digital Security, and Medical and Healthcare Informatics. NEXCOM serves its customers worldwide through its subsidiaries in five major industrial countries. Under the IoT megatrend, NEXCOM expands its offerings with solutions in emerging applications including IoT, robot, connected cars, Industry 4.0, and industrial security.

www.nexcom.com

NEXCOM is an Associate member of the Intel® Internet of Things Solutions Alliance. From modular components to market-ready systems, Intel and the 250+ global member companies of the Alliance provide scalable, interoperable solutions that accelerate deployment of intelligent devices and end-to-end analytics. Close collaboration with Intel and each other enables Alliance members to innovate with the latest technologies, helping developers deliver first-in-market solutions.