Solution Blueprint
Internet of Things (IoT)

Bringing Intelligence to Manufacturing with the Internet of Things (IoT)

NEXCOM* uses Intel® IoT Gateway software to deliver an open-architecture solution that connects field devices the cloud.

Driving a data revolution in manufacturing

Executive Summary

Many manufacturers are eager to tap the power of big data in order to increase competitiveness, improve the bottom line, and anticipate trends. They are exploring the Internet of Things (IoT), which facilitates communications between all types of field devices and enables manufacturers to act upon decisions derived from data analytics. However, a major challenge is gaining access to field data, made more difficult by field devices that use different fieldbus protocols, run independently, or lack connectivity.

Helping to overcome communication barriers amongst various field devices, including machinery, robots, PLCs, and sensors, the NEXCOM* NIFE* 100 IoT Controller provides cross-protocol communication capabilities, among many other benefits. The NIFE 100, a PC-based controller running the Intel® IoT Gateway stack, is an open-architecture solution design for connecting fieldbus modules to the cloud. This paper discusses this controller, as well as other NEXCOM offerings that can be used to build IoT solutions that improve operations, strengthen security barriers, simplify device management, and reduce maintenance costs.

Table of Contents

Key Business Objectives

Increase operations efficiency and reduce maintenance costs, thus improving the bottom line and competitiveness.

Business Challenge

Today, the use of various device networks on the factory floor is driving up cost and complexity, as more people and training are required to maintain them all. It is common for separate networks, such as PROFIBUS*, PROFINET*, DeviceNet*, EtherCAT*, etc., to support different applications, as shown in Figure 1. If a factory network exists for these devices, the network is usually built on a closed-loop intranet that is isolated from the Internet.

In order to realize the benefits of big data, manufacturers must first eliminate the communication barriers that impede data flow. This can be done with IoT technologies expressly developed to bridge the gap between the enterprise and operation domains, allowing for data aggregation and analytics to achieve informed decision making and increased productivity.

Solution Benefits

Open standard infrastructure and IoT technologies from NEXCOM and Intel can help manufacturers achieve their major objectives:

- **Improve Operations**
  Factory staff can easily keep an eye on field devices when SMS alerts are sent to their smartphones by a local or remote management service, and field devices can also be monitored, configured, and serviced remotely. These features enable the staff to address device issues more quickly and save time.
- **Strengthen Security Barriers**
  Data at rest or in transit is protected by a combination of data encryption, application whitelisting, secure sockets layer (SSL) certificates, and secure boot of devices. From field device to cloud, software- and hardware-based security mechanisms provide multiple safeguards to better protect manufacturing data and intellectual property (IP).

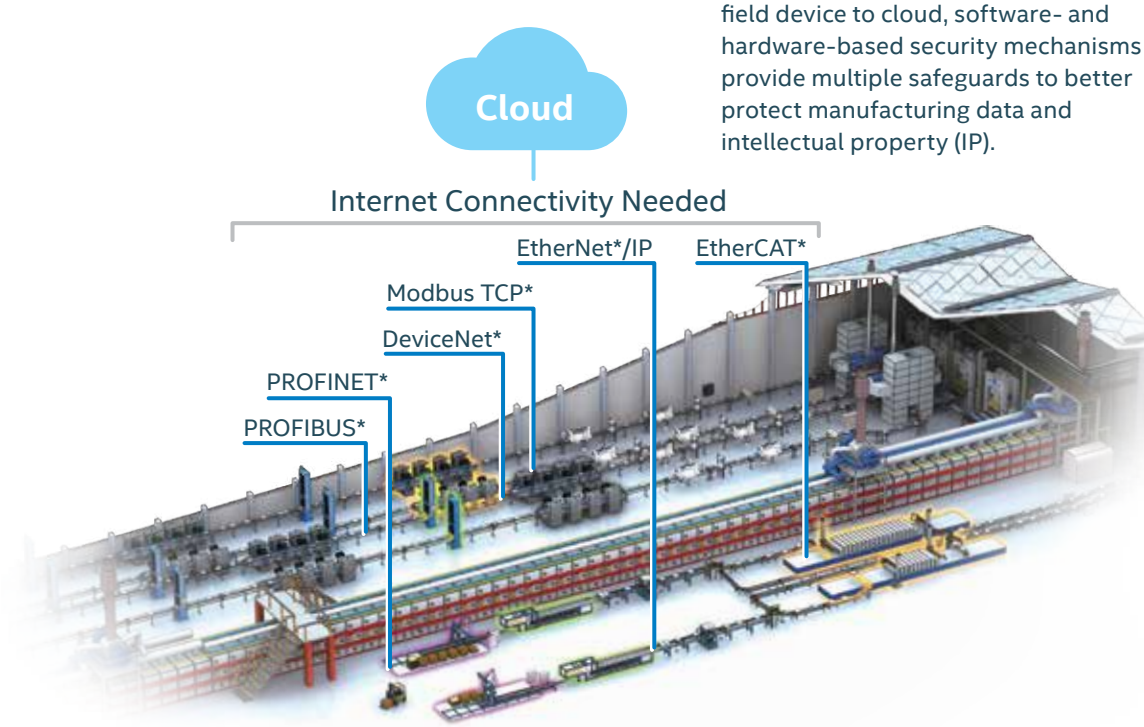

Figure 1. Gaining Access to Field Data Is a Significant Barrier

Figure 2. Simplified Architecture Connecting Field Devices to SCADA/HMI, the Cloud or Data Center

- **Simplify Device Management**
  The solution works with centralized management tools that seamlessly integrate existing PLCs and HMI, while providing features, tools, and methods of access to make it simple to monitor and control devices from anywhere.
- **Reduce Maintenance Costs**
  Predictive maintenance based on big data analysis is extremely versatile. For instance, analytics may indicate a machine part, which is normally replaced at regular intervals, is still functioning well and need not be replaced at that time. Thus, the part can be swapped out less frequently, thereby reducing spares and labor costs. This was demonstrated by a manufacturing module at Intel, where predictive maintenance led to a 20 percent reduction in spare costs.[1] (Read more)

Solution Overview

The NEXCOM NIFE 100 IoT Controller communicates downstream to manufacturing modules over various fieldbus protocols and upstream to an on-premise SCADA system or to the cloud (or data center) via LAN, Wi-Fi, or 3G/4G networks. At the same time, it supports serial communication and fieldbus protocols to devices (as shown in Figure 2), allowing it to aggregate all types of downstream data.

Given the fact that different communication protocols are used from factory to factory, the NIFE 100 can interface to different types of fieldbus modules and support many fieldbus protocols, including PROFINET, PROFIBUS, EtherNet*/IP, DeviceNet, EtherCAT, CANopen*, and Modbus*. This capability enables the NIFE 100 to act as a fieldbus concentrator and provide the last-mile connection for field devices. As a result, manufacturers can build a Factory-of-Things that integrates PLCs, remote I/Os, and legacy field devices across different control subsystems, and sends field data to the cloud for big data analytics and remote monitoring of factory operations.

NEXCOM* NIFE* 100 IoT Controller

The NEXCOM NIFE 100 IoT Controller offers a unique open-architecture solution (Figure 3) with the configuration flexibility needed to eliminate communication barriers on the factory floor. It can run Wind River* Linux* operating systems and Wind

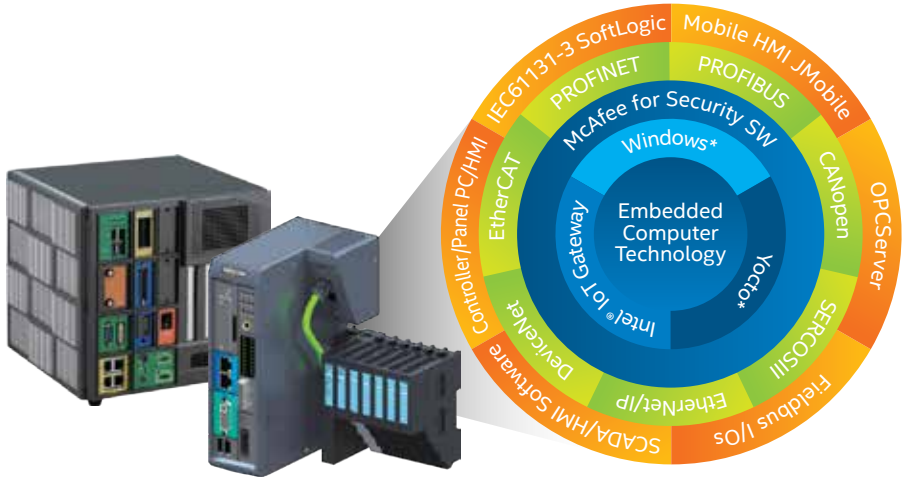

Figure 3. Key Components of the NEXCOM* NIFE* 100 IoT Controller Platform

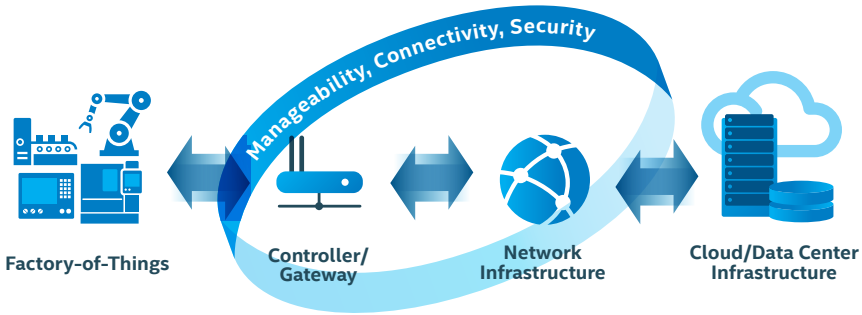

Figure 4. IoT Solution Brings Together Essential Ingredients, including Security, Manageability, and Network Connectivity.

River Intelligent Device Platform (IDP) stack, and handles the aforementioned fieldbus protocols. Rounding out this automation solution is software for SCADA/HMI client, Panel PCs, protocol conversion (e.g., IEC61131-3 Softlogic*), and fieldbus I/O drivers.

Addressing the computation, communication, and control requirements in manufacturing, this embedded computing platform integrates the power-efficient Intel® Atom™ processor E3800 product family. The multi-core architecture of Intel® Atom™ processors equips the NIFE 100 with ample computing performance to collect and process input data and command field devices to take appropriate actions. The NIFE 100 is available with up to quad-core computing power to accelerate response time, control a large volume of field devices, and perform more complicated control schemes.

The NIFE 100 controller may run the Intel IoT Gateway software stack, developed in collaboration with McAfee and Wind River. The controller can connect to legacy and new industrial devices, thereby enabling seamless and secure data flow between field devices and the cloud. The Intel IoT Gateway software stack integrates technologies and protocols for networking, embedded control, enterprise-grade security, and manageability on which application-specific software can run.

Example Use Models

The NIFE100 supports a development environment and multiple operating systems that be used to implement different factory scenarios, such as:

- **Factory of Things model:** Microsoft* Windows* and Wind River Linux
- **Internet of Things model:** Wind River Linux and Wind River IDP development environment

Technology

This section describes how NEXCOM's NIFE 100 IoT Controller delivers connectivity, manageability, and security technologies for deploying manufacturing solutions that connect field devices to the cloud (or manufacturing data center), as illustrated in Figure 4.

Connectivity

The NEXCOM NIFE 100 IoT Controller is designed to be the conduit between the physical world and the cyber world, as shown in Figure 5. The physical world consists of cyber-physical systems (CPS), which refers to a new generation of systems with integrated computational and physical capabilities that can interact with human processes in new ways (e.g., augmented reality, wearable devices). The NIFE 100 provides the interoperability necessary for CPS and sets up a solid foundation for Factory-of-Things operations, transforming a factory to a Smart Factory without a costly overhaul.

CPS systems are typically closed, but through the use of IoT technologies that provide a cyber-physical bridge, these systems can connect to the cyber world. The ability to interact with and expand the capabilities of the physical world through computation, communication, and control is a key enabler for future technology development.[2]

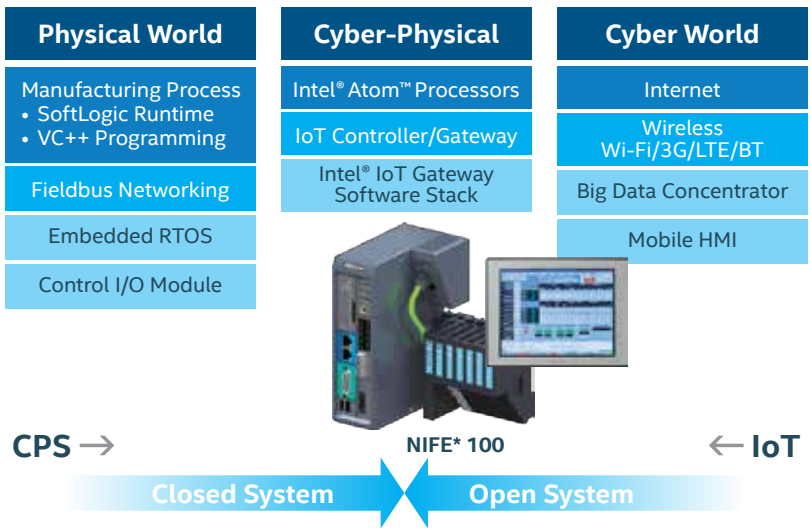

Figure 5. NEXCOM* PC-based Factory Automation Building Blocks

Control and Analytic Workloads

In addition to providing connectivity, the NIFE 100 has sufficient computational power to run control and analytic workloads, which reduces the amount of data that needs to be sent to the cloud for processing. When employed in pharmaceutical manufacturing, for example, the NIFE 100 can monitor the pressure level of a reactor when binding agents are added to deliver a drug in pill or tablet form. As soon as the pressure reaches a certain level, the NIFE 100 can close inlet valves and activate a motor to spin an impeller to start the blending process. All is done automatically without manual effort.

Software Suite for Automation Technology

The NIFE 100 ships with the CODESYS Softlogic* programming tool from 3S-Smart Software Solutions*. This programming tool, based on the IEC 61131-3 standard, facilitates programming across multiple controllers and allows the NIFE 100 to adapt to different factory environments.

Broad Equipment Vendor Support

The NIFE 100 can control devices manufactured by Siemens*, Rockwell*, Beckhoff*, and other industrial equipment vendors using a series of optional fieldbus modules. For example, the controller comes with software that communicates with Siemens devices over PROFIBUS and PROFINET, and with Rockwell devices over EthernetIP, etc.

NEXCOM offers a bundled service pack that includes the driver, firmware (SYCON.net utility) and OPC server (i.e., OLE for process control) for NEXCOM fieldbus cards. After configuration with SYCON.net, the NIFE 100 can recognize the different vendors' devices, providing an easy-to-implement solution to conduct multiple-protocol communications.

Fieldbus Protocol Communication

For manufacturers using the NIFE 100 on the factory floor, NEXCOM provides the soft logic containing the driver for fieldbus protocol use. For Modbus TCP/RTU applications, libraries are commercially-available; and for SCADA applications, the driver is included with the SCADA software.

Security

As factories adopt the IoT technologies to achieve smart manufacturing, it is critical to protect operations and productivity with a variety of security mechanisms. The Intel Atom processor E3800 product family plays a key role here. It delivers fast hardware-assisted data encryption and decryption through Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) and only allows trusted software to boot the device through a feature called Secure Boot. In addition, error correcting code (ECC) can be used to detect and correct bit errors in system memory, which increases reliability.

The NIFE 100 can also run McAfee Embedded Control, a key ingredient of the Intel IoT Gateway software stack. This endpoint software uses whitelisting to allow only authorized software to run, blocking malware from execution. In addition, McAfee Embedded Control facilitates regulatory compliance by only allowing authorized policy-based changes to be made to the system.

Manageability

Factory staff is typically on the go, which means they can be more productive if they can manage factory devices from a smartphone or other mobile device. With this in mind, the NIFE 100 is available with a mobile HMI App JMobile, which provides remote access to real-time monitoring and control of factory operation. Starting a new manufacturing process only takes a few taps on a mobile device. Instead of being confined to desks in a factory control room, staff members can check a field device connected to the NIFE 100 – anytime, anywhere.

IoT Tenets

The NEXCOM NIFE 100 is designed to provide security and interoperability from edge to cloud in keeping with five key tenets defined by Intel:

- World-class security as the foundation
  - The solution implements robust hardware and software-level protection that secures data from field devices to IoT gateway to cloud.
- Automated discovery and provisioning of edge devices to ease deployment
  - After configuring the IoT gateway, field devices from multiple vendors can be connected in Plug and Play fashion.
- Data normalization through protocol abstraction to improve interoperability
  - The service pack from NEXCOM can perform fieldbus protocol translation (e.g., PROFINET, EthernetIP).
- Broad analytics infrastructure from edge to cloud to realize customer value
  - The NIFE 100 support MQTT-based or HTTP-based connectivity to cloud solutions with analytics capabilities.
- Infrastructure to monetize hardware, software, and data management from edge to cloud
  - Manufacturers can realize substantial savings through increased operations efficiency and reduced maintenance costs.

Summary

With the Intel IoT Gateway software stack, the NEXCOM NIFE 100 is an application-ready solution that can enable business transformation based on the Factory of Things. Packed with cross-communication capabilities, high performance computing, remote manageability, and security mechanisms, the NIFE 100 exemplifies how legacy devices can be incorporated into a smart factory, thus avoiding costly factory overhauls.

With its open architecture, the NIFE 100 can play many roles – from a data acquisition server to a high-level IoT automation controller – while securely connecting together the Ethernet-based business domain and the fieldbus-based factory domain. Using the NIFE 100, manufacturers can begin to transform their factories by taking advantage of big data analytics used to generate new business insights. At the heart of this solution are IoT technologies from NEXCOM and Intel that are driving a data revolution in manufacturing.

Resources

Intel® Internet of Things Solutions Alliance
Members of the Intel® Internet of Things Solutions Alliance provide the hardware, software, firmware, tools, and systems integration that developers need to take a leading role in IoT.

Intel® IoT Gateway Development Kits
Intel® IoT Gateway development kits enable solution providers to quickly develop, prototype, and deploy intelligent gateways. Available for purchase from several vendors, the kits also maintain interoperability between new intelligent infrastructure and legacy systems, including sensors and data center servers.

For more information about the NEXCOM IoT controller NIFE 100, visit **http://www.nexcom.com/news/Detail/nexcom-nife-100-intelligent-controllers-drive-digital-manufacturing-in-the-iot-era**

For more information about Intel® solutions for the IoT, visit **www.intel.com/iot**.

NEXCOM is a 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.

[1] Intel White Paper, "Optimizing Manufacturing with the Internet of Things," www.intel.com/content/www/us/en/internet-of-things/white-papers/industrial-optimizing-manufacturing-with-iot-paper.html.

[2] Source: "The Impact of Control Technology," 2011, section by R. Baheti and H. Gill, Cyber-physical Systems, pg. 161, R. Baheti and H. Gill, http://ieeecss.org/sites/ieeecss.org/files/documents/IoCT-FullReport.pdf.

 Printed in USA 0215/MS/CS/SD/PDF ♻ Please Recycle 331969-001US