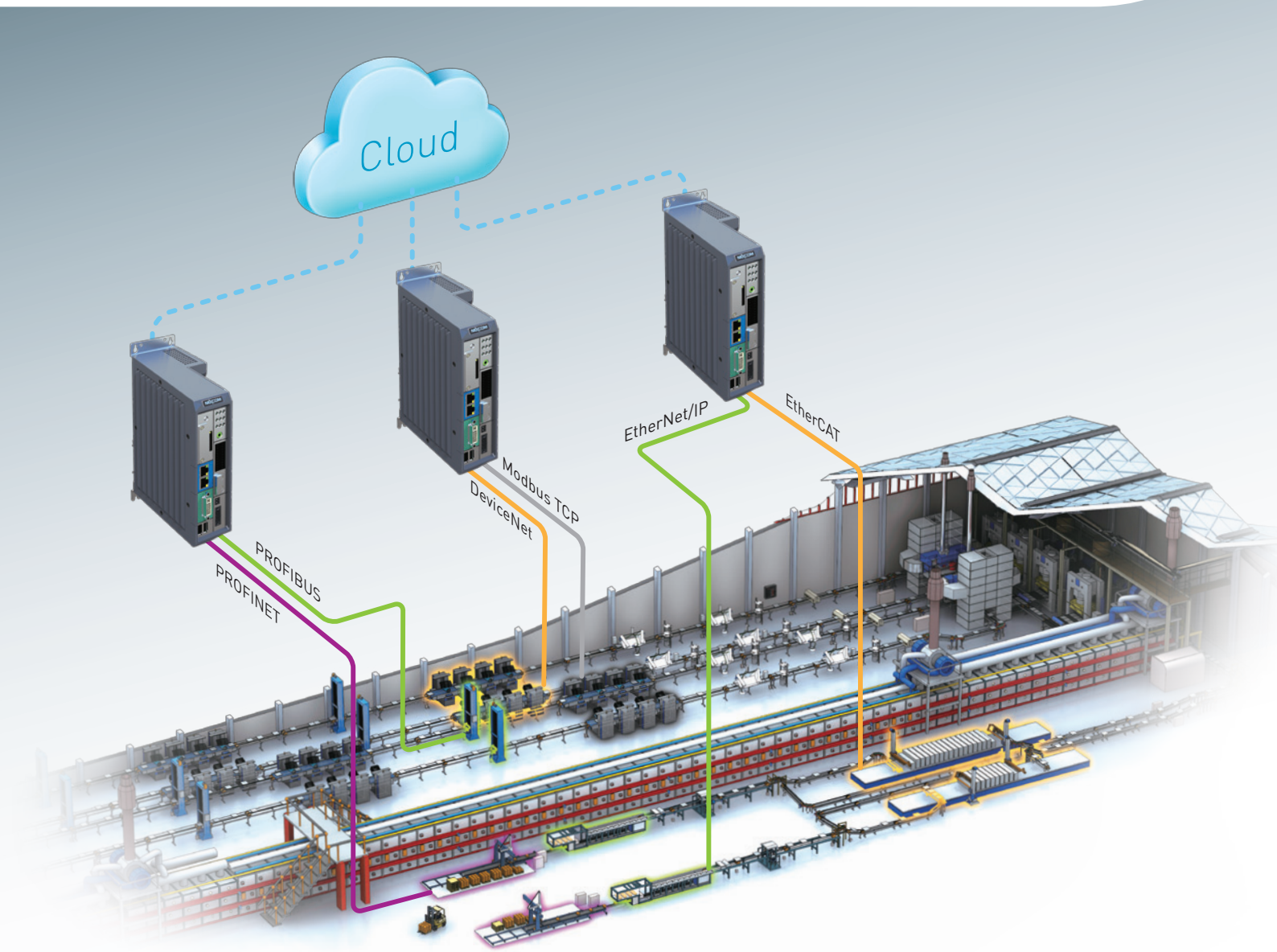
NEXCOM
The Intelligent Systems

White Paper

NEXCOM IoT Controller Solution Brings Intelligence to Manufacturing



Enterprises across industries are looking to big data and the Internet of Things (IoT) to help them increase competitiveness, improve the bottom line, and anticipate trends. Manufacturers are no exception. However, building an industrial Internet of Things, or Factory-of-Things, poses many challenges.

In this white paper, NEXCOM will explain how the NEXCOM IoT controller NIFE 100 provides a unique open-architecture solution with the configuration flexibility to surmount communication barriers in building the Factory-of-Things and supporting the necessary data communications for connecting the enterprise domain and the operation domain. We will look at how the NIFE 100 based on the Intel® Atom™ processor E3800 product family can perform a wide variety of tasks expected of Factory-of-Things devices. We will show how the NIFE 100 simplifies factory transformation and maintenance, including enabling factory operation monitoring using mobile devices. And, in addition, we will consider how by supporting the Intel® Gateway Solutions for the Internet of Things (Intel® Gateway Solutions for IoT), the NEXCOM NIFE 100 integrates Wind River® Linux operating system and McAfee® Embedded Control to help manufacturers speed to market of secure Factory-of-Things solutions.

Speak the Same Language

Manufacturers are enthusiastic about tapping the power of big data and ad-hoc analysis, but face a significant barrier in gaining access to field data. In most cases, a factory is full of legacy field devices including machinery, robots, PLCs, and sensors. These field devices use different communication protocols and run independently. If a factory network exists for these devices, the network is usually built on a closed-loop intranet that is separate from the Internet.

To make the data flow and realize all the

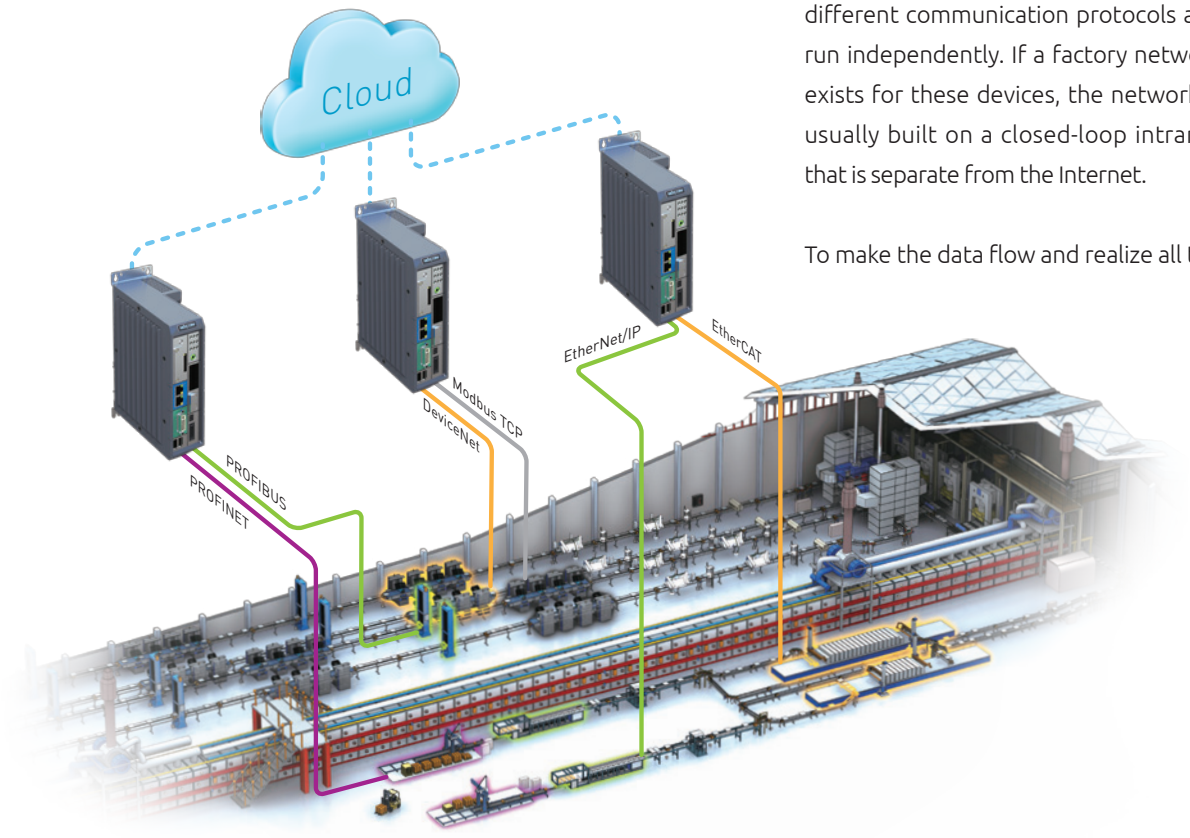


Figure 1. Manufacturers face a significant barrier in gaining access to field data.

advantages of the Factory-of-Things, manufacturers must find a way to lift the communication barriers among these field devices and connect them to the Internet.

Connecting Legacy Devices to the Internet

The NEXCOM IoT controller NIFE 100 uses the Intel Gateway Solutions for the IoT to deliver an open-architecture solution for providing cross-protocol communication capabilities to fieldbus modules to support both downstream and upstream data communication.

Intel Gateway Solutions for the IoT are the result of a collaboration with McAfee and Wind River. By providing *pre-integrated, pre-validated* hardware and software building blocks, the gateways connect legacy and new systems, and enable seamless and secure data flow between edge devices and the cloud. Intel Gateway Solutions for the IoT offer factories a key ingredient for enabling the connectivity of legacy industrial devices and other systems to the IoT. It integrates technologies and protocols for networking, embedded control, enterprise-grade security, and easy manageability on which application-specific software can run.

To aggregate downstream data, the NIFE 100 supports serial communication and fieldbus protocols at the same time. Given the fact that different communication protocols are used from factory to factory, the fieldbus protocols supported by the NIFE 100 include PROFINET, PROFIBUS, EtherNet/IP, DeviceNet, EtherCAT, CANopen, and Modbus. The NIFE 100 can act as a fieldbus contractor and provide the last-mile connection for field devices. The NIFE 100 also supports LAN, Wi-Fi, and 3G/4G networking to enable the upstream data traffic.

With the NIFE 100, manufacturers can build a Factory-of-Things that integrates PLCs, remote I/Os, and legacy field devices using different protocols and across different control subsystems. Manufacturers can also send field data to the cloud for big data analytics and remote monitoring of factory operations.

Figure 2. To aggregate field data, the NIFE 100 supports fieldbus communication and 3G/LTE/Wi-Fi networking at the same time.

To help manage the amount of data sent to the cloud for processing, some control and analytic workloads can be delegated to edge devices such as IoT controllers and industrial gateways on the factory floor, supporting Industry 4.0 and the movement to the Smart Factory based on cyber-physical systems.

Cyber-Physical Systems (CPS)

The term cyber-physical systems refer to a new generation of systems with integrated computational and physical capabilities that can interact with human processes thorough many new modalities. 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.[1]

To address the needs of computation, communication and control in the manufacturing sector, the NIFE 100 integrates Intel Atom E3800 processor product family, CODESYS SoftLogic, and OPC server software, and distributed I/O modules.

The multi-core architecture of Intel® Atom™ processors equips the NIFE 100 with outstanding 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 built-in soft logic programming tool CODESYS

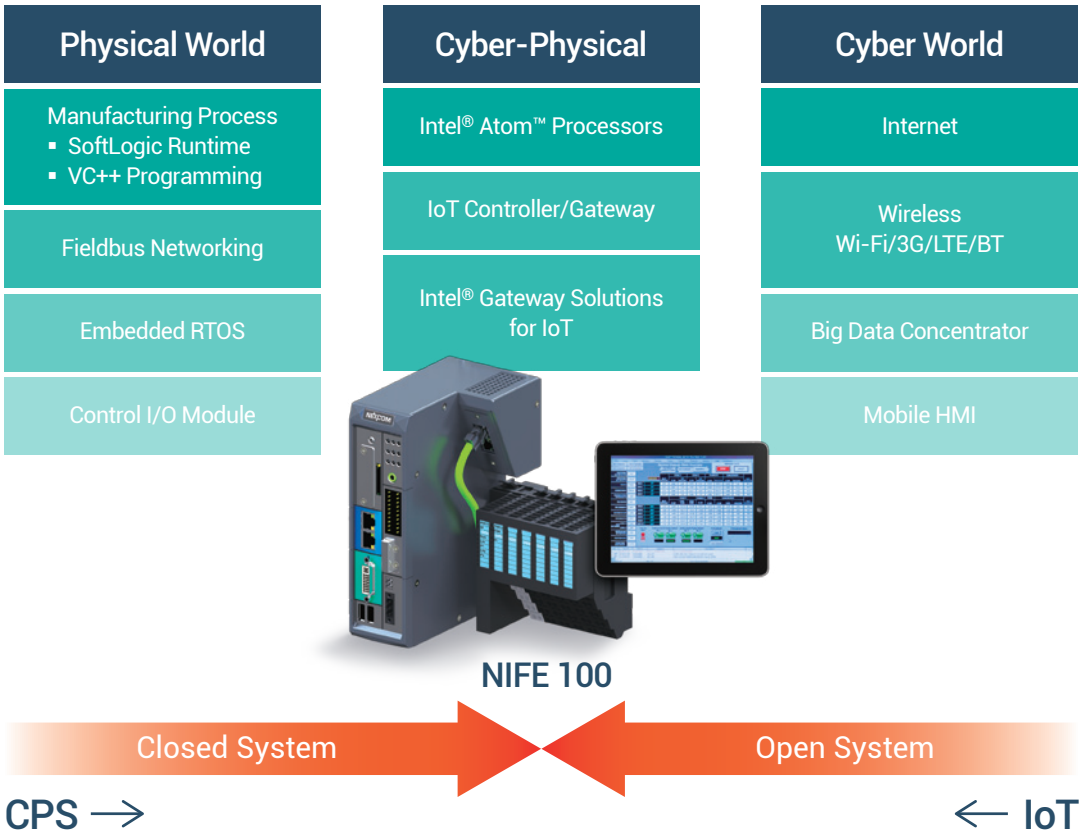


Figure 3. NEXCOM PC-based factory automation building blocks

SoftLogic is based on the IEC 61131-3 standard. This programming tool can facilitate programming across multiple controllers and allow the NIFE 100 to adapt to different factory settings. 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 costly factory overhaul.

Take pharmaceutical manufacturing for example. The NIFE 100 can monitor the pressure level of a reactor when excipients are added. 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.

Remote Management

So far, we have discussed the importance of cross-communication capabilities and interoperability to realize the Factory-of-Things and smart manufacturing. However, it is just as important to simplify the management and maintenance of the Factory-of-Things operations.

To this end, the NIFE 100 is available with a mobile HMI App JMobile. This app provides remote access to real-time monitoring and control of factory operation. Starting a new manufacturing process only takes a few taps on a tablet or a smartphone. Instead of being confined to a desk in a factory control room, a factory operator can check a factory anytime anywhere, making a virtual appearance on the factory floor.

This mobile app is bundled with NEXCOM Xcare™ 3.0 Suite. This remote management utility integrates software applications and a cloud server to support remote hardware status checks, remote system restore, remote keyboard/video/mouse (KVM) operation, and remote configuration of the NIFE 100.

The benefits of Xcare 3.0 Suite are huge. For example, the remote hardware status check gives factory IT staff an opportunity to detect a potential problem before a costly failure occurs. The system restore and remote KVM functions enable immediate response, making possible preventive actions and maintenance of the NIFE 100 to reduce downtime and increase management efficiency.

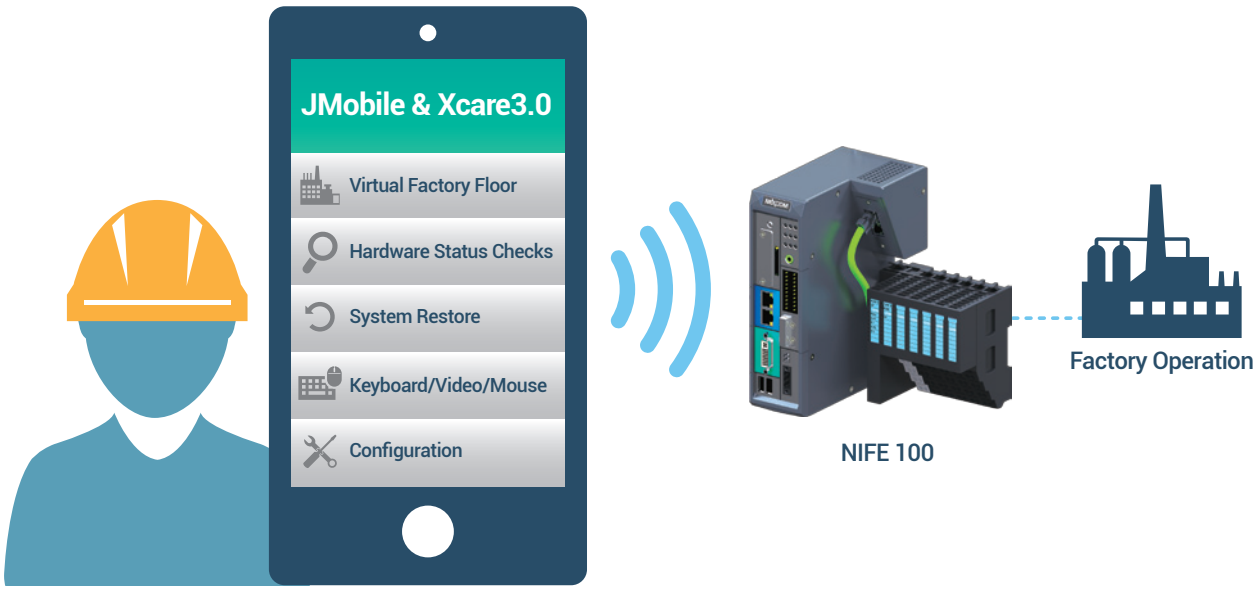


Figure 4. The NIFE 100 simplifies factory transformation and maintenance, including enabling factory operation monitoring using mobile devices.

A Secure and Instant Solution

As factories adopt the Factory-of-Things model to achieve smart manufacturing, it is critical that they also include security mechanisms to protect operations and productivity.

The Intel Atom processor E3800 product family plays a key role here. It offers security enhancements not available on previous Intel® Atom™ processors. It delivers fast hardware-assisted data encryption and decryption through Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) and supports Secure Boot to allow only trusted software to run on a device. It also supports error correcting code (ECC) for extra reliability. Intel® Virtualization Technology (Intel® VT) is also available to provide near-native performance of virtualized workloads for greater reliability, security, investment protection, and flexible resource management.

The NIFE 100 can also benefit from McAfee Embedded Control, a key ingredient of the Intel Gateway Solutions for the IoT. This endpoint software uses whitelisting to allow only authorized software to run, blocking malware from execution and installation on the NIFE 100. Given the fact that an IoT controller like NIFE 100 is a purpose-built appliance that executes only a limited set of applications, the whitelisting approach is more effective at protecting against zero-day attacks than traditional anti-virus software. In addition, to assist with regulatory compliance, McAfee Embedded Control only allows policy-based changes that are expected and authorized.

Conclusion

By supporting Intel Gateway Solutions for the IoT, NEXCOM NIFE 100 is an application-ready solution that can enable business transformation based on Factory-of-Things. Packed with cross-communication capabilities,

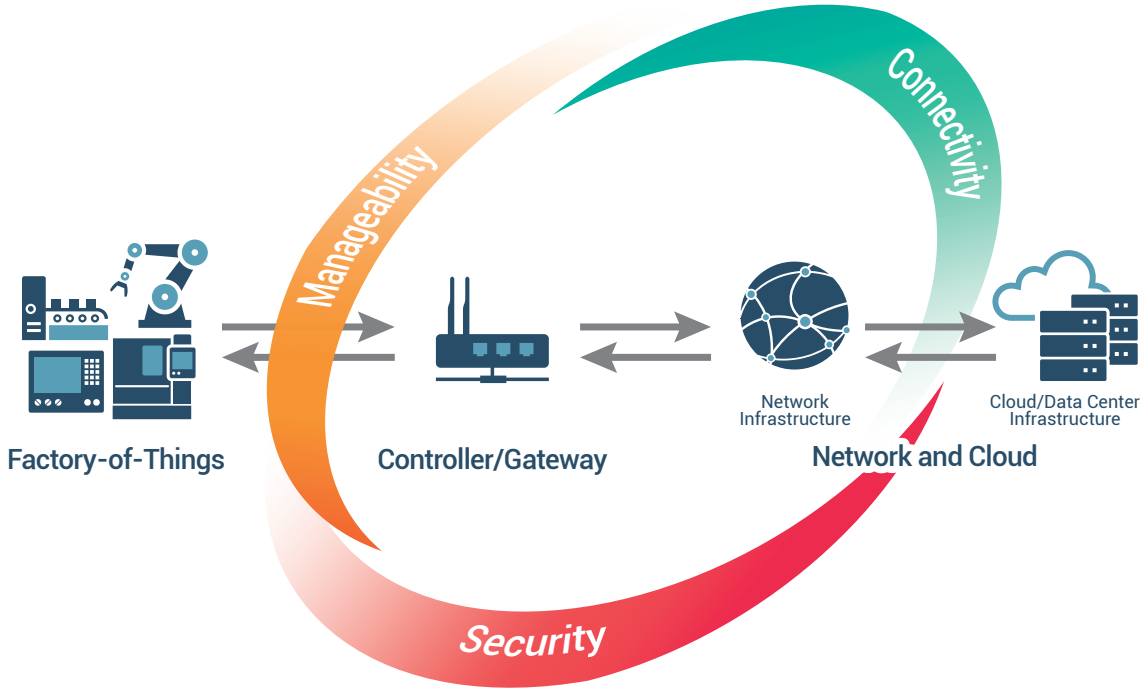


Figure 5. Intel® Gateway Solutions for the IoT brings together essential solutions including security, manageability and network connectivity.

high performance computing, remote manageability, and security mechanisms, the NIFE 100 exemplifies how a smart factory can be built based on legacy devices, preventing costly factory overhauls.

With its open architecture, the NIFE 100 can play many roles—from data acquisition server to high-level IoT automation controller—to securely connect the Ethernet-based business domain and the fieldbus-based factory domain. Using the NIFE 100, industrial companies can begin to transforms their factories by taking advantage of big data analytics. Equally important, they can immediately reduce business costs and improve operations with a simplified control scheme, simplified control network architecture, and reduced maintenance efforts.

[1] R. Baheti and H. Gill. Cyber-physical systems. In The Impact of Control Technology, 2011.

Founded in 1992, NEXCOM has five business units which focus on vertical markets across industrial computer, in-vehicle computer, multimedia, network and communication, and intelligent digital security industries. NEXCOM five its customers worldwide through its subsidiaries in seven major industrial countries. NEXCOM gains stronghold in vertical markets with its industry-leading products including the rugged fanless computer NISE series, the in-vehicle computer VTC series, the network and security appliance NSA series and the digital signage player NDiS series.

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 Intel® Internet of Things Solutions 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. Find out more at intel.com/IoTSolutionsAlliance.

Intel, the Intel logo, Intel Atom, Intel Core, and Intel Inside are trademarks of Intel Corporation in the U.S. and/or other countries.

© 2014 NEXCOM International Co., Ltd. All Rights Reserved. Published in September 2014