Industrial Network and Cloud Product Selection Guide
NEXCOM maps out a solution blueprint for Industry 4.0, which seamlessly integrates connected manufacturing and big data cloud computing. NEXCOM IoT Automation Solutions (IAS) Business Group has broadened its Industry 4.0 solutions to include cyber-physical system (CPS) ready solutions (Automation), robot solutions (NexROBO), EtherCAT motion solutions (NexMotion), and industrial network & cloud solutions. All solutions leverage NEXCOM IoT Studio and IoT gateways to stream field data to cloud services powered by world-renowned cloud services such as Microsoft Azure, IBM Bluemix™ and iSAP etc.

The integrated cloud-enabled services such as remote management, big data analytics, machine learning, and business intelligence (BI) can provide benefits such as remote monitoring, to ensure exception management and advanced process control.

For instance, operators can benefit by getting an accurate measure of machine status and factory operations in real-time, as well as integrating enterprise resource planning (ERP) and manufacturing execution systems (MES) systems to optimize supply chain management. Based on live field data, big data analytics and machine learning can establish predictive models that assist operators in managing factory operations, identifying causes for abnormal conditions, and taking corrective actions. Preventive maintenance can be executed prior an equipment failure to ensure production efficiency and yield rate.

Positioning itself as an industrial IoT forerunner, NEXCOM has broadened its Industry 4.0-ready Automation solutions, including cyber-physical system (CPS) ready solutions, robot solutions, EtherCAT motion solutions, and industrial network & cloud solutions for smart manufacturing. Mirroring the ambition for Industry 4.0, a connected factory will enable raw data to be exchanged over the network and translated into valuable information, helping enterprises make insightful decisions and therefore increase competitiveness in fast-paced industries. Our best-in-class solution topology has new technological breakthroughs and innovative convergence of data communications technology. It can better serve customers in an increasingly competitive global marketplace and lead manufacturers to smart factory automation.

The convergence of physical and digital worlds is giving rise to the smart factory and a new generation of industrial machinery. This new era, known as Industry 4.0, focuses on using the IoT and CPS to streamline manufacturing and business processes, improve versatility and precision, and boost quality and capacity.

NEXCOM provides a wide range of IoT Automation solutions for increasing demands of industrial applications. NEXCOM IoT Automation Solutions Master e-Catalog covers NEXCOM’s most up-to-date and completed solutions, detailed product datasheets, and selection guides of high-performance industrial fanless computers, different-size industrial panel PCs, machine and robot automation lineups, PC-based factory automation families, IoT solutions, industrial wireless solutions, and embedded computing and customization services.

The industrial IoT (IIoT) network lay the important foundation for Industry 4.0. It includes three pillars—Cyber-Physical System (CPS), Industrial Wireless Solution, and Industrial Firewall for IoT Security. NEXCOM provides the IIoT network with complete product solutions which cover all three scopes. The product solutions are designed with the concepts of “ready to use” and “click to connect” so users can easily establish the IIoT network that can encompass existing automation systems in their Industry 4.0 and IoT applications.
Industries 4.0 and Industrial IoT (IIoT) have become the mainstream of smart manufacturing. Devices, software services, and cloud platforms spring up around the IoT with great stress laid on the importance of horizontal and vertical integration. However, industrial control and automation systems have a close architecture which delivers high reliability, meets operational needs, and yet poses great challenges in system integration on the course of IoT transformation. How to integrate and connect industrial systems to upper layers of network and cloud platforms without compromising system reliability and information security becomes an important subject and defines a unique architecture for IoT (Figure 1).

The foundation of the IoT architecture rests on cyber-physical systems (CPSs). A CPS can acquire data generated by on-premises industrial systems in a closed-loop network and share it over internal and external networks for the purposes of data fusion and analysis. A CPS plays such a crucial role in the formation of IoT networks that its importance is strongly stressed by Industry 4.0.

**Cyber-Physical System**

A CPS must meet three technology requirements. Firstly, a CPS has to support special communication protocols, or network interfaces, commonly used in the industrial sector so it can communicate with industrial systems like programmable logic controllers (PLCs) and machine controllers and extract data required of data fusion and big data analysis (Figure 2).

Secondly, a CPS must be capable of processing data. Despite the diversity of data formats and industrial communication protocols, a CPS has to parse data for information and convert it into different formats that can be recognized by edge servers and cloud platforms on upper layers of IoT networks.

Thirdly, a CPS must have a user-friendly interface to support protocol conversion functions as well as to deliver high reliability (Figure 3).

NEXCOM’s CPS lineup is equipped with Modbus, industrial fieldbus, and OPC UA communication capabilities to amass data from most industrial systems (Figure 4). As to upper connectivity, MQTT, SQLite, and HTTPS are supported so NEXCOM’s CPS can integrate with cloud platforms, databases, and web services and therefore give our clients great flexibility to choose a data receiving end they see fit. To further reduce system integration efforts, NEXCOM has developed a configuration tool—NEXCOM Industrial IoT Studio. This tool integrates features required of establishing end-to-end connections and is designed with a graphical user interface (GUI) enabling system integration engineers to configure connection settings without the need of programming and coding.

Building on top of CPS are industrial wireless connectivity and network security. The former offers a flexible alternation that extends the reach of internet, and the latter helps strengthen network security of open IoT architecture. NEXCOM has developed NEXCOM Industry 4.0 Wireless Solutions and Industrial Firewall Solutions in this regard.

**Figure 1. Architecture of NEXCOM’s IoT Network Solutions.**

**Figure 2. Communication protocols supported by NEXCOM’s CPS gateways and IoT Studio.**

**Figure 3. NEXCOM Industrial IoT Studio is a web-based configuration tool designed with a graphical user interface (GUI) and supports drag-and-drop operations.**

**Figure 4. NEXCOM CPS provides seamless end-to-end connection.**
Industry 4.0 Wireless Connectivity

The main concept of Industry 4.0 is to reduce unexpected machine downtime and production interruption and optimize the efficiency of process management by leveraging cloud services and big data analysis on upper network layers. To make this happen, factory operations, equipment health status, and manufacturing processes must be able to be monitored and managed from a distance, underlining the importance of a network backbone dedicated to industrial applications.

As Industry 4.0 is taking the industrial sector by storm, factory operators are putting down great efforts to meet ever-changing manufacturing needs and adhere to operational requirements. Wired network connections can no longer satisfy operational demands for mobility, unmanned operations, and customization. As a result, the indispensable role of network backbone falls on wireless communications to provide reliable and stable network connections between factories and business headquarters.

NEXCOM Industry 4.0 Wireless Solutions are designed for industrial environments which are characterized by being harsh, highly complex, capricious, and interference-prone. The solutions feature Wi-Fi Mesh technology to provide multipath routing for not only connecting onsite wireless mobile devices but also building a high level of reliability and flexibility into network backbones. Combining NEXCOM Wi-Fi Device Gateways and nCare Device and Network Health Management Solution (Figure 6), users can form a three-layer network architecture for Industry 4.0. The Industry 4.0 Wireless Solutions offer several advantages including reliable network connections, seamless Wi-Fi coverage, deployment speed and flexibility, and unified visualized interface, and have tremendous applications—shop floor device monitoring, automated guided vehicles (AGV), video wireless, and process automation in the oil, gas and chemical industry.

Industrial Firewall

More and more facilities, systems, equipment are coming online with the aim to improving operational efficiency. To keep improvements on course, NEXCOM has added rich feature sets, expandability, and rugged design to its HENGE™ series which is made up of the IFA family of industrial firewalls and VPN dispatcher IVD 1000. It is worth mentioning that the IFA family can withstand rigorous challenges of harsh environments which are characterized for being harsh, highly complex, capricious, and interference-prone. The solutions feature IPsec and SSL VPN protection to arm industrial systems with extra shields. This feature enables industrial system vendors to not only remotely but also securely access and manage their products installed on clients’ premises over simplified private network tunnels. Furthermore, the rugged design of the IFA family can withstand rigorous challenges of harsh operating environments, making it ideal for industrial applications. It is worth mentioning that the IFA family can operate over an extended temperature range from -20 degrees Celsius to 70 degrees Celsius. Equipped with full SSL VPN functionality—VPN server and VPN client—the IFA family can strengthen security protection for high-value industrial systems used in industrial automation, process control, and power stations applications.
Cyber-Physical System with Connectivity

A cyber-physical system (CPS) serves a pivotal role in the industrial IoT (IIoT). Since industrial equipment uses special protocols incompatible with other applications, enabling data sharing among physical devices at the field site and cyber layers of networks requires manufacturers and system integrators to go the extra mile to enjoy the benefits of big data analysis and realize the value of Industry 4.0 and IoT (Figure 1). Therefore, by provide two-way communication and control, a CPS can help bridge the last mile connection gap to seamlessly integrate OT and IT.

Acquiring data from on-premises facilities is one key feature of a CPS. Other features required of a CPS include IoT communications support, IoT automatic control capability, and IoT human-machine interface (HMI). IoT communications support is imperative to data processing, integration, and uploads. IoT automatic control capability allows automation systems to leverage the power of remote big data analysis while delivering high-performance highly reliable real-time control with real-time operating systems. IoT HMI is aimed to achieve overall management from business to machine levels by taking advantage of information on cloud dashboards and single-unit monitoring for timely and effective system adjustments.

A CPS must meet three technology requirements. Firstly, a CPS has to support special communication protocols, or network interfaces, commonly used in the industrial sector so as to communicate with industrial systems like programmable logic controllers (PLCs) and machine controllers and extract data required of data fusion and big data analysis. Secondly, a CPS must be capable of processing data. Despite the diversity of data formats and industrial communication protocols, a CPS has to parse data for information and convert it into different formats that can be recognized by edge servers and cloud platforms on upper layers of IIoT networks. Thirdly, a CPS must have a user-friendly interface to support protocol conversion functions as well as to deliver high reliability. The best choice of hardware platform for a CPS is, no doubt, an industrial computer which combines flexible expansion for communications featured in PCs and sturdy design required of industrial products.

NEXCOM’s CPS lineup is made up of a series of industrial computers equipped with Modbus, fieldbus, and OPC UA communication capabilities to amass data from most industrial systems. As to upper connectivity, MQTT, SQLite, and HTTPS are supported so NEXCOM’s CPS can integrate with cloud platforms, databases, and web services and therefore give our clients great flexibility to choose a data receiving end they see fit (Figure 2). To further reduce system integration efforts, NEXCOM has developed a configuration tool—NEXCOM Industrial IoT Studio. This tool has combined features required to establish end-to-end connections into a unified graphical user interface (GUI) (Figure 2). That is to say that system integration engineers can configure connection settings without the need of programming and coding.

Highly reliable hardware platform tempered for industrial environments, full compatibility with industrial communication protocols, and simple and fast system configuration are qualities expected of an ideal and practical CPS solution which enables IoT to be applied to real-case scenarios and scale fast (Figure 3).

![Image](image_url)

**Figure 1. A CPS which can bridge the last mile connection gap between the cyber and physical ends serves a pivotal role in IIoT.**

![Image](image_url)

**Figure 2. NEXCOM Industrial IoT Studio combines all required features into a unified graphical user interface.**

![Image](image_url)

**Figure 3. In a real case scenario, a CPS can harvest manufacturing data from a closed-loop machine and send the data the business headquarters over internet.**

---

**Cyberworld**

- Network Interface
- Fieldbus Networking
- Wireless Networking
- IO Expansion
- RS-232/422/485
- RS-485
- RJ45
- 1 x RS-232/485
- 2 x RS-232/485
- 1 x USB 3.0
- 3 x USB 2.0
- Status LED
- Display:
  - 320 x 240
- Temperature:
  - -20°C ~ +65°C
- Humidity:
  - 10% to 90%
- Power:
  - 24VDC
- Storage:
  - 16G eMMC
- Ethernet:
  - 1 x RJ45
- Wireless
  - 802.11bgn
- WiFi
  - 2.4GHz
- Bluetooth
- Barcode Reader
- PC/104
- SAT-500/600/800
- SAT-700/900
- SAT-4000/6000

**Physical World**

- Manufacturing Process
- Communication
- Control
- Visualization
- Fieldbus Networking
- RTOS Embedded
- Device IO Expansion
- Field Data Concentration
- Remote Visualization
- Remote Monitoring
- Remote Control
- Area 1
- Area 2
- Area 3
- Area N

**Networking**

- LAN
- Type of LAN:
  - RJ45
- USB
  - 1 x USB 2.0
- COM Port
  - 1 x RS-232/485

**Storage**

- 16G eMMC

**Certification**

- CE
- FCC

**Model Selection Guide**

<table>
<thead>
<tr>
<th>Model Name</th>
<th>CPS 100-M</th>
<th>CPS 100-RE/DP</th>
<th>CPS 200-RE/DP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photo</td>
<td><img src="image_url" alt="Image" /></td>
<td><img src="image_url" alt="Image" /></td>
<td><img src="image_url" alt="Image" /></td>
</tr>
<tr>
<td>Category</td>
<td>Industrial IoT Remote Gateway</td>
<td>Fieldbus Enabled IoT Remote Gateway</td>
<td>Fieldbus Enabled IoT Edge Gateway</td>
</tr>
<tr>
<td>Communication Protocols for Local Devices</td>
<td>Modbus/TCP, Modbus/RTU, OPC-UA (Client)</td>
<td>PROFINET-RT, PROFINET-DP, EtherCAT ( Slave), Modbus/TCP, Modbus/RTU (Master), OPC-UA Client</td>
<td>PROFINET-RT, PROFINET-DP, EtherCAT (Slave), Modbus/TCP, Modbus/RTU (Master), OPC-UA Client</td>
</tr>
<tr>
<td>Communication For Cloud/Server</td>
<td>MQTT, SQLite, HTTPS</td>
<td>MQTT, SQLite, HTTPS</td>
<td>MQTT, SQLite, HTTPS</td>
</tr>
<tr>
<td>Wireless Communication Interface Options</td>
<td>WiFi, 3G, 4G/LTE</td>
<td>WiFi, 3G, 4G/LTE</td>
<td>WiFi, 3G, 4G/LTE</td>
</tr>
<tr>
<td>Number of LAN Ports</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Type of LAN</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45</td>
</tr>
<tr>
<td>COM Port</td>
<td>1 x RS-232/485</td>
<td>1 x RS-232/485</td>
<td>2 x RS-232/422/485</td>
</tr>
<tr>
<td>USB</td>
<td>1 x USB 2.0</td>
<td>1 x USB 2.0</td>
<td>1 x USB 2.0</td>
</tr>
<tr>
<td>Display</td>
<td>320 x 240</td>
<td>320 x 240</td>
<td>320 x 240</td>
</tr>
<tr>
<td>Mounting Style</td>
<td>Wall Mount, DIN Rail</td>
<td>Wall Mount, DIN Rail</td>
<td>Wall Mount, DIN Rail</td>
</tr>
<tr>
<td>Temperature</td>
<td>-20°C ~ +65°C</td>
<td>-20°C ~ +65°C</td>
<td>-20°C ~ +65°C</td>
</tr>
<tr>
<td>Humidity</td>
<td>10% to 90%</td>
<td>10% to 90%</td>
<td>10% to 90%</td>
</tr>
<tr>
<td>Power</td>
<td>12/24VDC</td>
<td>12/24VDC</td>
<td>12/24VDC</td>
</tr>
<tr>
<td>Storage</td>
<td>16G eMMC</td>
<td>16G eMMC</td>
<td>16G eMMC</td>
</tr>
<tr>
<td>Certification</td>
<td>CE, FCC</td>
<td>CE, FCC</td>
<td>CE, FCC</td>
</tr>
</tbody>
</table>
NEXCOM Industrial IoT Studio

Main Features
- Processing data analytically by redefining the categories and offered customized nodes
- Manage cyber physical system efficiently by NEXCOM hardware information nodes
- Connect to cloud securely with verified MQTT and AMQP nodes
- Support SQLite for database application and https for web service
- Support Fieldbus (PROFINET, PROFIbus, Ethernet/IP) configuration, Modbus/RTU and Modbus/TCP master, OPC-UA client for field device/controller data concentration

Product Overview
IoT is transforming business across industries with innovative applications. To spur more innovations, NEXCOM Industrial IoT Studio, a web-based configuration tool, demonstrated how developers can swiftly implement customized features by taking advantage of pre-integrated functions with simple clicks, drags, and drops. Accelerating the development of IoT applications with reduced efforts enables immediate testing of innovative ideas, turning proof-of-concept inventions into wide-scale deployment. NEXCOM Industrial IoT Studio which is a GUI tool powered by using Node.js and IBM Node-RED (*1).

Specifications

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modbus</td>
<td>Get the registers and status with the Modbus protocol</td>
<td>Modbus-TCP read/write, Modbus-RTU read/write</td>
</tr>
<tr>
<td>Fieldbus</td>
<td>Get the registers and status from the controller/devices with Fieldbus interface</td>
<td>PROFIBUS read, PROFIBUS write, PROFINET read, PROFINET write, EtherNet/IP read, EtherNet/IP write</td>
</tr>
<tr>
<td>Data process</td>
<td>Process or encrypt/decrypt data from buffering</td>
<td>Merge, Boundary, Critical section, HW Info, Base64Encode, Base64Decode, 3DESEncrypt, 3DESDecrypt, OPC-UA Client</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Prompt for user input from network or serial port</td>
<td>Inject, catch, status, MQTT, HTTP, websocket, TCP, UDP, serial</td>
</tr>
<tr>
<td>Output</td>
<td>Expose the data from service or debug message</td>
<td>Debug, MQTT, HTTP response, websocket, TCP, UDP, serial</td>
</tr>
<tr>
<td>Function</td>
<td>Function, template, delay, trigger, comment, http request, TCP request, switch, change range, csv, html, json, xml, rbe</td>
<td></td>
</tr>
<tr>
<td>Social</td>
<td>Access ‘multipart/form-data’ content by email</td>
<td>Email in, Email out</td>
</tr>
<tr>
<td>Storage</td>
<td>Read/write the file or database</td>
<td>File in, file out, SQLite</td>
</tr>
<tr>
<td>Cloud</td>
<td>Provides Azure service</td>
<td>eventhub, IoT hub, MS SQL</td>
</tr>
</tbody>
</table>

Support OS & Hardware Matrix

<table>
<thead>
<tr>
<th>Devices</th>
<th>Windows Embedded 8</th>
<th>Yocto (Linux)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPS 100-M</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>CPS 100-RE/DP</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>CPS 200-RE/DP</td>
<td>X</td>
<td>O</td>
</tr>
</tbody>
</table>

Note: Products and models are listed but not limited, please contact your sales representatives for updates.

*1. Node-RED is a visual wiring tool for the Internet of Things. A creation of IBM emerging technologies.
CPS 100-M
Industrial IoT Remote Gateway

Main Features
- Seamless integration of field devices, web, database and cloud services
- Modbus TCP/RTU, OPC-UA support in parallel
- ISO-on-TCP RFC 1006 support
- Intuitive visual flow-based programming paradigm
- Secure HTTPS/TLS encrypted data transmissions

Product Overview
CPS 100-M, an edge IoT gateway, is fully integrated with Modbus TCP/RTU accessibility, OPC-UA and IoT studio for extremely easy deployment of both centralized/decentralized field data implementation in automation process. Equipped with fieldbus accessibility, user can not only retrieve the data for live monitoring but also extract key information for custom process, like prediction and maintenance, yield rate of production... and so on. Furthermore, IoT studio brings benefits of drag-and-drop data process, exchange field data over network securely between edge and the cloud, flexible field data store/analysis/statistics... and so on.

CPS 100-M is a perfectly matched solution for remote field data processing in automation.

PDM Rotor Kit Specifications
Seamless Integration
- Compatible with existing installation in field control network
- Industrial protocol support – Modbus TCP/RTU, OPC UA client
- Data processing – MQTT, Kafka, OPC-UA client
- Data processing and distribution – JavaScript, JSON, XML, MQTT client, TCP, UDP, HTTP, WebSocket, E-mail

Secure Gateway Management
- Secure boot
- Gateway monitoring
- Network protocol – HTTP, HTTPS, TCP/IP, UDP
- Wireless support – WiFi

Productive Engineering
- Drag-and-drop workflow builder
- Versatile pre-defined function blocks
- Initialize-configure-read/write-close pattern

Direct IoT Communication
- For devices with OPC-UA, Modbus and fieldbus protocol support
- In parallel to the PLC over a direct communication channel
- With data semantics for easy abstraction in the cloud

Gateway Platform Specifications
CPU Performance
- Onboard Intel® Atom™ processor E3805 1.33 GHz

Memory
- Built-in DDR3L 2GB system memory

Networking Connectivity
- 2 x 10/100/1000Mbps LAN ports

Major I/O Connectivity
- 1 x USB 3.0 (900mA)
- 1 x USB 2.0 (500mA)
- 1 x RS232/485, 2.5KV isolation protection

Wireless Connectivity (Optional Module)
- IEEE 802.11 a/b/g/n connectivity

Power Requirement
- 1 x 12/24VDC input, 25% range

Storage Device
- 1 x eMMC 16GB flash memory

Dimensions
- 63mm (W) x 100mm (D) x 151mm (H)

Ordering Information
- CPS 100-M (P/N: 10JC0010002X0)
- Industrial IoT remote gateway, E3805, 2GB RAM, 16GB eMMC, Modbus TCP/RTU

Weight
- 400g

Construction
- Aluminum and metal chassis with fanless design

Shock Protection
- 5G, half sine, 11ms, IEC60068-2-27

Vibration Protection
- Random: 2Gms @ 5–500Hz, IEC60068-2-64
- Sinusoidal: 2Gms @5–500Hz, IEC60068-2-6

Operation Temperature
- Ambient with air flow: -20°C–65°C

Storage Temperature
- -20°C–85°C, relative humidity: 10%–95%

Regulation
- CE/FCC
Main Features
- Seamless integration of field devices, web, database and cloud services
- Fieldbus (slave) PROFIBUS®, PROFINET® or EtherCAT® support
- Modbus TCP/RTU, OPC UA support in parallel
- Intuitive visual flow-based programming paradigm
- Secure HTTPS/TLS encrypted data transmissions

Product Overview
CPS 100/100 series, an edge IoT gateway, is fully integrated with fieldbus accessibility, Modbus TCP/RTU, OPC UA and IoT studio for extremely easy deployment of both centralized/decentralized field data implementation in automation processes. Equipped with fieldbus accessibility, user can not only retrieve the data for live monitoring but also extract key information for custom process, like prediction and maintenance, yield rate of production... and so on. Furthermore, IoT studio brings benefits of drag-and-drop data process, exchange field data over network securely between edge and the cloud, flexible field data store analitics/statistics... and so on.

CPS 200/100 series is a perfectly matched solution for remote field data processing in automation.

Benefits of CPS Solution
- Compatible with existing installation in field control network
- Multiple fieldbus (slave) support – PROFIBUS®, PROFINET®, or EtherCAT®
- Industrial protocol support – Modbus TCP/RTU, OPC UA client
- Data mining – MQTT-broker, OPC UA client
- Data processing and distribution – JavaScript, JSON, XML, MQTT client, TCP, UDP, HTTP, WebSocket, E-mail

Secure Gateway Management
- Secure boot
- Gateway monitoring
- Network protocol – HTTP, HTTPS, IPv4, TCP/UDP
- Wireless support – Wi-Fi

Productive Engineering
- Drag-and-drop workflow builder
- Versatile pre-defined function blocks
- Initialize-configure-read/write-close pattern

Direct IoT Communication
- For devices with OPC UA, Modbus and fieldbus protocol support
- In parallel to the PLC over a direct communication channel
- With data semantics for easy abstraction in the cloud

Gateway Platform Specifications
CPU Performance
- Onboard Intel® Atom™ processor E3805 1.33 GHz
Memory
- Built-in 2GB DL 2GB system memory
Networking Connectivity
- 2 x 1/10/100/1000Mbps LAN ports
- Isolated field control 10/100Mbps ports, PROFIBUS®, PROFINET®, or EtherCAT®

Major I/O Connectivity
- 1 x USB 3.0 (500mA)
- 1 x USB 2.0 (500mA)
- 1 x RS232/485, 2.5KV isolation protection

Power Requirement
- 1 x 12/24VDC input, ±20% range

Storage Device
- 1 x eMMC 16GB flash memory

Dimensions
- 63mm (W) x 100mm (D) x 151mm (H)

Weight
- 600g

Construction
- Aluminum and metal chassis with fanless design

Shock Protection
- 50G, half sine, 11ms, IEC60068-2-27

Vibration Protection
- Random: 2Grms @ 5~500HZ, IEC60068-2-64
- Sinusoidal: 2Grms @5~500Hz, IEC60068-2-6

Operation Temperature
- Ambient with air flow: -20°C~65°C

Storage Temperature
- -20°C~85°C, relative humidity: 10%~95%

Regulation
- CE/FCC

Ordering Information
- CPS 100-DP (P/N: 10JC0010000X0) Industrial IoT remote gateway, E3805, 2GB RAM, 16GB eMMC, PROFIBUS®
- CPS 100-RE (P/N: 10JC0010001X0) Industrial IoT remote gateway, E3805, 2GB RAM, 16GB eMMC, real-time Ethernet
Main Features

- Seamless integration of field devices, web, database and cloud services
- Fieldbus (slave) PROFIBUS®, PROFINET® or EtherCAT® support
- Modbus TCP/RTU, OPC UA support in parallel
- Intuitive visual flow-based programming paradigm
- Secure HTTPS/SSL encrypted data transmissions

Product Overview

CPS 200/100 series, an edge IoT gateway, is fully integrated with fieldbus accessibility, Modbus TCP/RTU, OPC UA and IoT studio for extremely easy deployment of both centralized/decentralized field data implementation in automation process. Equipped with fieldbus accessibility, user can not only retrieve the data for live monitoring but also extract key information for custom process, like prediction and maintenance, yield rate of production... and so on. Furthermore, IoT studio brings benefits of drag-and-drop data process, exchange field data over network securely between edge and the cloud, flexible field data store/analytics/statistics... and so on.

CPS 200/100 series is a perfectly matched solution for remote field data processing in automation.

Benefits of CPS Solution

- Compatible with existing installation in field control network
- Multiple fieldbus (slave) support – PROFINET®, PROFINET® or EtherCAT®
- Industrial protocol support – Modbus TCP/RTU, OPC UA client
- Data mining – MQTT-broker, OPC UA client
- Data processing and distribution – JavaScript, JSON, XML, MQTT client, TCP, UDP, HTTP, WebSocket, E-mail

Secure Gateway Management

- Secure boot
- Gateway monitoring
- Network protocol – HTTP, HTTPS, IPv4, TCP/IP, UDP
- Wireless support – Wi-Fi

Productive Engineering

- Drag-and-drop workflow builder
- Versatile pre-defined function blocks
- Intuitive-collaborative read/write/execute pattern

Direct IoT Communication

- For devices with OPC UA, Modbus and fieldbus protocol support
- In parallel to the PLC over a direct communication channel
- With data semantics for easy abstraction in the cloud

Gateway Platform Specifications

CPU Performance

- Onboard Intel® Celeron® processor J1900 Quad Core 2.0 GHz

Memory

- Built-in DDR3L 4GB system memory

Display

- 2D and 2D/HD display output

Networking Connectivity

- 2 x 10/100/1000Mbps LAN ports
- Isolated field control 10/100Mbps ports, PROFINET®, PROFINET® or EtherCAT®

Major I/O Connectivity

- 1 x miniSIM card holder
- 1 x USB 3.0 (900mA)
- 3 x USB 2.0 (500mA per each)
- 2 x RS232/485, 2.5KV isolation protection on COM1
- Power on/off switch

Wireless Connectivity (Optional Module, up to 2)

- IEEE 802.11 a/b/g/n/AC connectivity

Power Requirement

- 1 x 24VDC input, ±20% range

Storage Device

- 1 x 2.5” front accessible 128GB SSD support
- 1 x SD card socket

Dimensions

- 85mm (W) x 157mm (D) x 214mm (H)

Weight

- 2.25Kg (w/ disk)

Construction

- Aluminum and metal chassis with fanless design
- SSD: 50G, half sine, 11ms, IEC60068-2-27
- CFast: 50G, half sine, 11ms, IEC60068-2-27
- Vibration Protection w/ CFast & SSD condition
  - Random: 2Grms @ 5~500HZ, IEC60068-2-64
  - Sinusoidal: 2Grms @5~500Hz, IEC60068-2-27

Operation Temperature

- Ambient with air flow: 0°C~50°C

Storage Temperature

- -20°C~80°C, relative humidity: 10%~95%

Regulation

- CE/FCC
- LVD

Ordering Information

- CPS 200-DP (P/N: 10JC0020000X0)
  - Industrial IoT Edge gateway, J1900, 4GB RAM, 128GB SSD, PROFIBUS®
- CPS 200-RE (P/N: 10JC0020001X0)
  - Industrial IoT Edge gateway, J1900, 4GB RAM, 128GB SSD, real-time Ethernet
Industrial IoT Security

Increasingly, industrial facilities, systems, and equipment are connecting to the network with the aim to improve operational efficiency. To promote continuous improvements, NEXCOM has expanded its offerings with the HENGE™ family which is made up of industrial firewalls of the IFA series, VPN dispatcher ND 1000, and the extremely rugged network attached storage INAS 330. The family features rich function sets, expandability, and rugged design. It is with ease that users can tap into built-in functions and have secure remote access, simplified private network tunneling, reliable connections, stateful firewall protection, intrusion prevention protection, and robust data storage at once. To sum up, the high level of function integration of the HENGE™ Family makes it one of indispensable network communications and security solutions in industrial automation applications (Figure 1).

The Industrial Firewall Series

The IFA series consists of three all-round broadband-compatible multi-port industrial firewall/VPN routers loaded with advanced technologies for stateful packet inspection (SPI), denial-of-service (DoS)/dynamic denial-of-service (Dynamic DoS) protection, intrusion detection, port scanning detection, and real-time alerts. To arm industrial systems with extra shields, the IFA series is equipped with PwC and SSL VPN protection to provide secure remote access and simplify VPN tunnel management for industrial system vendors to remotely and safely communicate with and manage their products installed on clients’ premises. Furthermore, the rugged design of the IFA series can withstand rigorous challenges of harsh operating environments. It is worth mentioning that the IFA series can operate over an extended temperature range from -20 degrees Celsius to 70 degrees Celsius.

Equipped with full SSL VPN functionality—VPN server and VPN client, the IFA series can secure network connections and communications for high-value on-premises automation systems used in industrial automation, process control, power station, and medical inspection applications.

Protect Critical Assets Against Cyber Threats

To kick business into higher gear, energy companies are contemplating the possibility of incorporating the internet technology in their infrastructure in the hope to automate operational processes, consolidate solutions, and improve efficiency. However, the pace of internet adoption in the industrial sector has been slow because common IT network security solutions cannot survive electrical environments nor meet operational requirements, and therefore expose critical industrial systems and equipment to malicious software and security risks. Compounding the problem is cross infection of virus spread by USB devices. With severe ramifications like power outage, system down in some cases, precautions must be considered in the early stages of planning.

Featuring stateful edge firewall protection, NEXCOM industrial firewalls/VPN routers IFA 3610, 2610, and 1610 can not only perform deep packet inspection to identify malicious codes disguised in legitimate packets, but also screen out suspicious inquiries by keep track of connection status. Additionally, the DoS conversion feature enables the IFA series to prevent malicious codes from accessing mission-critical networked industrial equipment, reducing the risks of system breakdowns and information leaks.

Increase Operational Efficiency

Remote access and data acquisition are of paramount importance in strengthening operational efficiency, winning a bigger market share, differentiating an enterprise from competitors, and more. However, industrial process control networks were narrow-band closed-loop networks that are not suited for remote access, let alone remote system monitoring and inspection. Thanks to the proliferation and cost reduction of Ethernet, VPN, and other networking technologies, vendors and system integrators of automation systems can take advantage of remote access to reduce unexpected system downtime and travel time and costs related to onsite services. The technologies also provide benefits of ease of installation and integration, better network expandability, and a leaner cost structure. Designed with remote system monitoring and inspection in mind, the SSL-VPN-equipped IFA series can provide private network tunnels (Figure 2). Leveraging a combination of tunneling, data encryption and decryption, key management, and authentication technologies, the IFA series can easily build a virtual private network tunnels (Figure 2). Leveraging a combination of tunneling, data encryption and decryption, key management, and authentication technologies, the IFA series can easily build a virtual private network. The IFA series also provide benefits of ease of installation and integration, better network expandability, and a leaner cost structure.

Endure Harsh Environments

It is worth mentioning that the IFA 3610 is a high-end model which can operate over an extended temperature range from -20 degrees Celsius to 70 degrees Celsius. The IFA series is designed with features including advanced stateful firewall, intrusion detection, IP forwarding, NAT, industrial protocol filters, secure virtual tunneling, and ease of installation and maintenance. Therefore, the IFA series is an ideal solution to industrial network communications.

Connect with Simplicity, Efficiency & Security

Giving consideration to the urge for remote access and an expandable system architecture, NEXCOM VPN dispatcher HENGE™ ND 1000 can support up to 100 IFA-series short- and long-range network connections, and public and hybrid networks. The ND 1000 simplifies the management of user accounts and authorization, creation and maintenance of VPN tunnels, and connection management, giving users high-system flexibility and manageability.

The Industrial Network-Attached Storage Series

NEXCOM INAS 330 is an network-attached storage (NAS) offering high availability with rugged design, RAID support, and buffer cache. With the incremental growth of distributed computing in industrial applications, the need for safe reliable data storage units on the field is surging because data needs to be well kept until sent to a cloud platform for further processing. From the hardware perspective, such storage units must have redundant: routing and power supply, extended operating temperature range, water and dust resistance,
and anti-vibration protection. As to data availability, an NAS must support RAID configuration, backup cache, and redundant network access. Meeting all requirements, the iNAS 330 is an ideal choice for industrial applications of oil and gas, water treatment, and traffic control, for instance among others.

High Performance, Reliability, Capacity & Endurance

The iNAS 330 can accommodate up to three hard drives to store 3TB of data or to deliver high data integrity with RAID 0/1/5 support, while the internal buffer cache can keep writing data into the iNAS 330 even when hard drives cease to function in distress. When configured for network redundancy, the iNAS 330 can prevent network access from being affected by a single component failure. Furthermore, the iNAS series provides many data backup and recovery options. Users can opt to backup data to local RAID systems, create remote replication, and transfer batch files to FTP servers; all methods serve the purpose of remote data backup. To facilitate the data backup process, the iNAS 330 uses sync commands to help users keep track of mirror backup and incremental backup according to applications’ needs. As different backup methods and cycles would have different effects on data recovery schemes, avoiding data loss takes both thoughtful evaluation and solid execution. The iNAS 330 is a trustworthy data storage solution to ensure data backup and recovery plans fall in place.

Lastly, the iNAS 330 has a rugged design which has been a hallmark of NEXCOM products. It is compliant with standards for railway applications, such as EN 50155 and EN 61373, and incorporates M12 connectors to offer the IP54 level of water and dust resistance. Supporting various file transfer protocols of network communications, the iNAS 330 answers the need for data storage spawned by the growing proliferation of distributed computing. The bottom line is that the iNAS 330 is easy to deploy and can reliably operate in harsh operating environments faced by industrial automation solutions, railway applications, alternative energy management systems, and the oil and gas industry.

Vulnerability Assessment

Questions that every plant manager has: We are expanding production with an estimate of hundreds of PC-based programmable automation (VA) services present as a reliable and quick interface medium for all applications, alternative energy management systems, and the oil and gas industry.

A

Quick expert advice to the question is using vulnerability assessment (VA) services. Despite the benefits of going online, being connected also increases the possibilities of getting attacked. There are a variety of automated malicious programs on the internet that can trigger all kinds of attacks, for instance denial of service and backdoor intrusion. In this regard, VA services offer to scan service ports—including HTTP, SSH, and Windows Update—on networked equipment and produce VA reports. Thanks to ubiquitous network infrastructure, VA services present as a reliable and quick interface medium for all kinds of systems for remote management, system monitoring, data acquisition, and contingency actions.

VA services can be carried out before factory expansion to remotely appraise security risks. Also, VA services can be performed on existing systems to spot security loopholes if there is any. Either way, assessing security risks help increase system reliability and availability.

Two major operating systems (OSs) used by industrial automation and control equipment are Windows and Open Linux. These general-purpose OSs activate service ports by default. However, not all equipment is protected and therefore exposed to security loopholes like unchanged default factory passwords and security exploits in known versions of operating systems. Using VA tools offered by world-renowned vendors, such as Qualys, users can perform VA by taking four simple steps (Figure 3). Compared with complex penetration tests, VA services are a fast and economical way to assess systemic risks.

- Connect target devices to the network
- Initialize VA software
- Initiate VA scan
- Receive VA reports

Figure 3. Vulnerability assessment processes.

INAS Features

- **Link Aggregation**
  - **Balance/IEEE 802.3ad**
  - **Balance-xor**
  - **Balance-alb**

- **Firmware Upgrade**
  - **Via System Web UI**

- **Backup Solutions**
  - **Remote Backup**
  - **System Configuration Backup (Option)**

- **AES Volume Encryption**
  - **Yes (Option)**

- **Green Power**
  - **Yes**

- **Web Browsers Support**
  - **Internet Explorer**
  - **Firefox**
  - **Safari**
  - **Chrome**

**Product Selection Guide**

<table>
<thead>
<tr>
<th>Model Name</th>
<th>Industry Firewall Multi-port VPN Router</th>
<th>VPN Dispatcher</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFA 1610</td>
<td>IFA 2610</td>
<td>IFA 3610</td>
</tr>
<tr>
<td>IVD 1000-5A</td>
<td>IVD 1000-10A</td>
<td>IVD 1000-15A</td>
</tr>
</tbody>
</table>

- **Power Supply**
  - **FCC/CE/RoHS/WEEE**

- **Power Over Ethernet**
  - **Yes**

- **Environmental Limits**
  - **Storage Temperature:**
    - **-25°C ~+55°C (-13°F ~+131°F)**
  - **Operating Temperature:**
    - **-15°C ~+38°C (5°F ~+100°F)**

- **Certification**
  - **CE/CCC/Nema/UL**

- **IP Rating**
  - **IP 65 (NEMA)**

- **Ordering Information**
  - **10100305000**

> Industrial Network and Cloud Product Selection Guide
IFA 1610

CoreFort™ Industry Firewall, 2 Ports VPN Router

Main Features
- Stateful packet firewall
- Intrusion prevention (IPS)
- SSL VPN secure remote access
- Serial gateway (RS485)
- Operating temperature range, from 0°C (32°F) up to 60°C (140°F)
- Compact palm size

Product Overview
The CoreFort™ Industry firewall series is a fully integrated industry 2 ports firewall router with VPN function. The fully equipped, broadband-capable firewall router offers a stateful packet inspection firewall, denial-of-service(DoS)/distributed denial-of-service(DDoS) protection and intrusion prevention, portscan detection, and real-time alerts. It gives additional protection for machinery and equipment installed on the secure side of the firewall. Equipped with SSL VPN functions, the CoreFort™ industry firewall provides a remote access infrastructure to secure connections, and helps machine builder/system integrator to design easily maintained systems. Furthermore, its full-industrial design is ideal for industrial environment application.

Pairing VPN capabilities, the CoreFort™ industry firewall series is an ideal endpoint connectivity and security solution for industrial automation, process control, energy and medical/Instrument remote management application.

Specifications

Network Security
- Stateful packet firewall
- Intrusion detection/prevention (IDS/IPS)
- Multiple public IPs
- SNMP support (v1/v2/v3)
- VoIP/SP support
- Portscan detection
- DOS and DoS protection
- SYN/ICMP flood protection

WAN
- Supports uplink/VMAN: Ethernet (Static/DHCP), PPPoE

Traffic Shaping
- Bandwidth management

User Authentication
- Active directory/NTLM
- LDAP
- Local

Network Address Translation
- Translation NAT
- Site-to-site

VPN (Virtual Private Network)
- L2TP
- PPTP
- L2F
- PPTP/L2F
- L2TP/PPTP
- PPTP/L2TP

Bridging
- Firewall stealth mode
- OSI layer 2 firewall function
- Spanning tree

Services
- Event notification & handling
- NTTP (Network Time Protocol)
- DHCP server
- SMNP server
- Syslog

Logs and Reports
- Customizable real-time dashboard
- NTP (Network Time Protocol)
- DHCP server
- Syslog
- On-Diag

Management
- Easy web-based administration (SSL)
- Secure remote SSH/SCP access
- Centralized management (via SSL)

Upgrades and Backup
- Centralized updates through CoreFort™ network
- Scheduled backup
- Encrypted backups via e-mail
- Instant recovery/backup to USB stick

Ordering Information
- IFA 1610 (P/N: 10F0161000X0)
  - Industry/Firewall 2 ports VPN router (3 years service & maintenance)
### CoreFort™ Industry Firewall, 3 Ports VPN Router with Rugged Design

**Main Features**
- Stateful (L4) packet firewall
- Intrusion prevention (IPS)
- SSL/VPN secure remote access
- DoS/DDoS protection
- Intrusion detection/prevention (ID/IPS)
- Multiple public IPs
- SNMP support
- Telnet/SSH
- Webpage
- Multi-WAN/Failover
- Supports multiple uplinks/WANs: Ethernet (Static/DHCP), PPPoE, analog/UMTS modem
- Automatic WAN/uplink Failover
- Monitoring of WAN uplinks

**Specifications**

**Network Security**
- Stateful packet firewall
- Intrusion detection/prevention (ID/IPS)
- Multiple public IPs
- SNMP support
- Telnet/SSH
- Webpage
- Multi-WAN/Failover
- Supports multiple uplinks/WANs: Ethernet (Static/DHCP), PPPoE, analog/UMTS modem
- Automatic WAN/uplink Failover
- Monitoring of WAN uplinks

**Traffic Shaping**
- Bandwidth management

**User Authentication**
- Active directory/NTLM
- LDAP
- Local

**Network Address Translation**
- Destination NAT
- Incoming routed traffic
- One-to-one NAT
- Source NAT (SNAT)
- IPSec NAT Traversal

**High Availability**
- Hot standby (active/passive)
- Node data/configuration synchronization

**Bridging**
- Firewall stealth mode
- OSLayer 2 firewall function
- Spanning tree
- Unlimited bridges
- Unlimited interfaces per bridge

**VPN (Virtual Private Network)**
- IPsec
  - Encryption: 3DES, AES 128/256-bit, SHA1
  - Diffie-Hellman (2, 5, 14, 16, 17, 18)
  - Authentication: Pre-shared key, RSA keys, X.509 certificates (SHA-1, 128)
  - DoS (Denial-of-Service) Protection
  - NAT Traversal
  - Compression

**Logs and Reports**
- Customizable real-time dashboard
- Live log viewer (AJAX based)
- Detailed user-based web access report
- Network/system performance statistics
- Rule-based logging settings (firewall rules)
- Sparse: Local or remote
- openTSA trusted time stamping

**Management**
- Easy Web-based administration (SSL)
- Secure remote SSH/SCP access
- Centralized management (via SSL)

**Updates and Backup**
- Centralized updates through CoreFort™ network
- Scheduled backup
- Encrypted backups via e-mail
- Instant recovery/backup to USB stick

**Physical and Power**
- DIN rail/wall mount (optional)
- Fanless
- Unbreakable
- Dimensions (W x D x H): 167 x 64.38 x 59 mm
- Weight: 1.90Kg
- Power input: 5.08mm terminal block x 1
- Terminal block, 24V DC

**Certification**
- Safety: UL 508
- FCC\(\text{c}\)/CE/RoHS
- FIPS 140-2

**Ordering Information**
- IFA 2610
  - CoreFort™ Industry firewall 3 ports firewall router (3 years service & maintenance)

**Product Overview**

The CoreFort™ Industry firewall series is a fully integrated industry 3 ports firewall router with VPN function. The fully equipped, broadband-capable firewall router offers a stateful packet inspection firewall, denial-of-service(DoS/DDoS) protection and intrusion prevention, portscan detection, and real-time alerts. It gives additional protection for machinery and equipment installed on the secure side of the firewall. Equipped with SSL/VPN functions, the CoreFort™ industry firewall provides a remote access infrastructure to secure connections, and helps machine builder/system integrator to design easily maintained systems. Furthermore, its tough fully-rugged design is ideal for harsh environment application.

Pairing VPN capabilities, the CoreFort™ industry firewall series is an ideal endpoint connectivity and security solution for industrial automation, process control, energy and medical/instrument remote management applications.
IFA 3610

CoreFort™ Industry Firewall, 5 Ports VPN Router
with Wide Temperature Range

Main Features
- Stateful (L4) packet firewall
- Intrusion prevention (IPS)
- SSL VPN secure remote access
- DDoS support
- Serial gateway (RS485)
- Wide temperature range, up to 70°C (158°F)

Product Overview
The CoreFort™ Industry firewall series is a fully integrated industry multi-port firewall router with VPN function. The fully equipped, broadband-capable firewall router offers a stateful packet inspection firewall, denial-of-service (DoS) distributed denial-of-service (DDoS) protection and intrusion prevention, portscan detection, and real-time alerts. It gives additional protection for machinery and equipment installed on the secure side of the firewall. Equipped with SSL VPN functions, the CoreFort™ industry firewall provides a remote access infrastructure to secure connections, and helps machine builder/system integrator to design easily maintained systems. Furthermore, its tough fully-rugged design is ideal for harsh environment application. With wide temperature range up to 70°C (158°F) degree, it offers reliable communication network in extreme temperature conditions. Pairing VPN capabilities, the CoreFort™ industry firewall series is an ideal endpoint connectivity and security solution for industrial automation, process control, energy and medical instrument remote management application.

Specifications
Network Security
- Stateful packet firewall
- Intrusion detection/prevention (IDS/IPS)
- Multiple public IPs
- SNMP support (v1/v2/v3)
- VoIP/ISDN support
- Portfilter detection
- DoS and DoS protection
- SYN/ICMP flood protection
- DNS proxy/routing

Multi-WAN/Failover
- Supports multiple uplinks/WANs: Ethernet (Static/DHCP), PPPoE, analog/UMTS modem
- Automatic WAN uplink Failover
- Monitoring of WAN uplinks

Traffic Shaping
- Bandwidth management

User Authentication
- Active directory/NTLM
- LDAP
- Local

Network Address Translation
- Destination NAT
- Incoming routed traffic
- One-to-one NAT
- Source NAT (SNAT)
- ISec NAT Traversal

High Availability
- Hot standby (active/active)
- Node data/Configuration Synchronization

Routing
- Static routes
- Source-based routing
- Destination-based routing
- Policy-based routing (based on interface, MAC, protocol, or port)

Hardware Specification
- 1 x 10/100/1000 Base-T Ethernet WAN
- 4 x 10/100/1000 Base-T Ethernet LAN
- 1 x USB
- 1 x DI/DO
- IFA 3610 (P/N: 10IF0361000X0)
- microSD 4GB
- FCC/CE/RoHS

Physical and Power
- DIN rail/wall mount (optional)
- Fanless
- Dimension (P x W x D): 167mm x 59mm x 140mm
- Weight (G.S. Kg): 1.90Kg
- Dual power input 24VDC

Environmental Specification
- Operating temperature: -20°C~70°C/-4°F~158°F
- Storage temperature: -40°C~80°C/-40°F~176°F
- Humidity: 5%~95%, non-condensing

Certification
- Safety UL 508
- FCC/CE/RoHS

Package Content
- IFA 3610 x 1
- QIG x 1
- Power input 5.08mm terminal block x 2
- DI/DO terminal block x 1

Ordering Information
- IFA 3610 (P/N: 10IF0361000X0)
Industry firewall 5 ports VPN router (3 years service & maintenance)
**Main Features**
- Fully integrated VPN server
- Stateful (L4) packet firewall
- SSL VPN secure remote access
- Serial gateway (RS485)
- Up to 25/100 concurrent licenses
- Redundant storage (RAID1)

**Specifications**
- Network Security:
  - Stateful packet firewall
  - Intrusion detection/prevention (IDS/IPS)
  - SNMP support (V1/V2/V3)
  - VoIP/SIP support
  - Portscan detection
  - Multiple public IPs
  - SNMP support (V1/V2/V3)
  - VoIP/SIP support
  - Portscan detection
  - Multiple public IPs
- Multi-WAN/Failover:
  - Supports multiple uplinks/WANs:
    - Ethernet (Static/DHCP), PPPoE, analog/UMTS modem
  - Automatic WAN uplink failover
  - Monitoring of WAN uplinks
- Traffic shaping:
  - Bandwidth management
- User Authentication:
  - Active directory/NTLM
  - LDAP
  - Local
- Network Address Translation:
  - Destination NAT
  - Source NAT (SNAT)
  - Reverse NAT (RAT)
  - Source NAT (SNAT)
  - Reverse NAT (RAT)
- Traffic shaping:
  - Bandwidth management
- User Authentication:
  - Active directory/NTLM
  - LDAP
  - Local

**Product Overview**
With the CoreFort™ VPN Dispatcher, users can define and manage network connections with extreme flexibility, adapting them to suit the specific needs, like create multiple and distributed networks using VPN gateway to gateway and enable remote connections to your network and take advantage of the intuitive VPN client, which is universally compatible with Windows, Mac OS X and Linux… and so on.

**Specifications**
- Network Security:
  - Stateful packet firewall
  - Intrusion detection/prevention (IDS/IPS)
  - SNMP support (V1/V2/V3)
  - VoIP/SIP support
  - Portscan detection
  - Multiple public IPs
  - SNMP support (V1/V2/V3)
  - VoIP/SIP support
  - Portscan detection
  - Multiple public IPs
- Multi-WAN/Failover:
  - Supports multiple uplinks/WANs:
    - Ethernet (Static/DHCP), PPPoE, analog/UMTS modem
  - Automatic WAN uplink failover
  - Monitoring of WAN uplinks
- Traffic shaping:
  - Bandwidth management
- User Authentication:
  - Active directory/NTLM
  - LDAP
  - Local
- Network Address Translation:
  - Destination NAT
  - Source NAT (SNAT)
  - Reverse NAT (RAT)
  - Source NAT (SNAT)
  - Reverse NAT (RAT)
- Traffic shaping:
  - Bandwidth management
- User Authentication:
  - Active directory/NTLM
  - LDAP
  - Local

**High Availability**
- Hot standby (active/passive)
- Node data/configuration synchronization

**Bridging**
- Firewall stealth mode
- OS/layer 2 firewall function
- Spanning tree
- Unlimited bridges
- Unlimited interfaces per bridge

**VPN (Virtual Private Network)**
- IKEv2
  - Authentication: pre-shared keys, X.509 certificates
  - PFS (Perfect Forward Secrecy)
  - IPSec/SSL
  - L2TP
  - PPTP
  - L2TP
  - PPTP

**Routing**
- Static routes

**Update and Backup**
- Centralized updates through CoreFort™ network
- Scheduled backup
- Encrypted backups via e-mail
- Instant recovery/backup to USB Stick

**Services**
- Event notification & handling
- NTP (Network Time Protocol)
- DHCP server
- SNMP server
- DynDNS

**Logs and Reports**
- Customizable real-time dashboard
- Live log viewer (AJAX-based)
- Detailed user-based web access report
- Network system/performance statistics
- Rule-based logging settings (firewall rules)
- Syslog local or remote
- OpenTSA trusted time-stamping

**Management**
- Easy web-based administration (SSL)
- Secure remote SSH/SCP access
- Centralized management (via SSL)

**Environment**
- Rack mount:
  - Dimension (H x W x D): 44mm x 426mm x 238mm
  - Weight: 100W ATX power supply

**Environmental Specification**
- Operating temperature: 0°C~40°C (32°F~104°F)
- Storage temperature: -20°C~70°C (-4°F~158°F)
- Humidity: 10%~90%, non-condensing

**Certification**
- FSC/CE/RoHS

**Package Content**
- IVD1000-S/A x 1
- QIG x 1
- Power cord
- Rack mount kit

**Ordering Information**
- IVD 1000-S (PN: TBD)
  - VPN dispatcher server with 25 licenses
  - Stateful packet firewall, SSL, VPN, unified VPN management
  - 3 years services & maintenance
Product Overview

The iNAS330 is extremely rugged-design network-attached storage (NAS), which was designed to provide high performance, reliability storage in harsh environments. Equipped with SSD storage technology, it is able to record the data correctly in harsh environments, such as oil exploration, transportation, and industrial automation, etc.

Furthermore, it offers several data backup options. It supports FTP service and SMB/CIFS protocol for file sharing among cross-platforms. Atlas OS™ provides real-time information, toolkit, widgets and easy mode of operation; software center provides more application extensions in the future, based on application requirements. iNAS330 also can be networking surveillance storage, with high-resolution camera, the file system could be used on video recording which supports RAID 5 and also that offers the better data protection.

The iNAS330 supports Power over Ethernet (PoE/PoE+) and follows the specifications in IEEE 802.3af/IEEE 802.3at. It has dual PoE+ interface which supports power redundancy. The iNAS330 is fanless but high-efficient for thermolysis, dust- and water-protected IP 54-rated chassis.

Specifications

**Hardware Features**
- **Computer**
  - Processor: Dual Cortex®-A9 CPU
  - Storage: Up to 3 x 2.5” HDD/SSD (optional)
- **Ethernet**
  - 2 x Gigabit LAN ports for data redundancy (M12)
  - 1 x Gigabit LAN port for management (M12)
- **Button**
  - Reset button: Reboot System/Reset to factory default
- **LEDs**
  - Power LED: power On/Off
  - System LED: system status
  - PoE/Temps LED: PoE/Temps status
  - HDD LED: HDD1, HDD2, HDD3 (read/write/fail)
  - LAN LED: 10/100/1000M x3 (link/active)
- **Power Requirements**
  - Input: PoE (IEEE 802.3af), or PoE+ (IEEE 802.3at)
  - Power redundancy

**Software Features**
- **OS**: Atlas OS™
  - Web-based GUI (based on HTML5 and CSS3)
  - Centralized navigation panel and Dual-desktop system:
    - Navigation Panel: For system configurations, with some toolkits on the toolbar
    - Home: For applications operations
    - Dashboard: For widgets exhibition
  - APPs:
    - Storage Manager
    - RAID management (JBOD, RAID1, RAID 5)/Auto RAID rebuilding
    - Data Vault
    - Log Book
    - Software Center
  - Widgets:
    - System Guardian
    - Network Surveillance
    - Configurations:
      - Files and permissions
      - Network and connectivity
      - System and devices
    - Toolkit:
      - Profile account management
      - Real-time notification
      - System information
      - Network status

**Power Specifications**
- **Input**: PoE (IEEE 802.3af), or PoE+ (IEEE 802.3at)
- **Output**: 35WPoE+-38W/PoE+ (IEEE 802.3at)
- **PoE Port**: 1x PoE+ (IEEE 802.3at)

**Environmental Specification**
- **Temperature**
  - Operating: -40°C to 70°C (14°F to 158°F)
  - Storage: -25°C to 55°C (1°F to 131°F)

**Certifications**
- **CE**
- **FCC**
- **RoHS**
- **WEEE**

**Ordering Information**
- **Part Number**: 101G0033000X0
- **Description**: Rugged-design industry storage (3-years service & maintenance)
- **Price**: $194.00

**Client O.S. support**
- Linux & UNIX
- Mac OS X 10.7 or later

**Web Browsers Support**
- Mozilla Firefox
- Max Safari
- Google Chrome
- Opera

**Protocol**
- HTTP: Samba 2.2/FTP
- OpenSSL (TLS)
- HTTPS
- HTTP 1.1
- HTTP/1.1
- IPv6 Link Aggregation
- DHCP
- NTP
- HTTP Authentication
- RESTful API

**Dimensions**

```
<table>
<thead>
<tr>
<th>Dimension</th>
<th>Width</th>
<th>Depth</th>
<th>Height</th>
</tr>
</thead>
<tbody>
<tr>
<td>246mm</td>
<td>9.69&quot;</td>
<td>7.64&quot;</td>
<td>2.36&quot;</td>
</tr>
</tbody>
</table>
```
Industry 4.0 Wireless Solution (IWS)

One of the most prevalent applications of Industry 4.0 (I4.0) is extracting field data to monitor factory operations and device health status, and using those data for big data analytics to reduce potential system malfunctions and increase production efficiency and yield. To achieve this, a cyber-physical system (CPS) is required to mine and transfer data from lower layer devices to cloud service platforms for analytics processing (Figure 1).

As I4.0 introduced the shift to unmanned factories, the need for flexible and agile factory operations has gained increased importance due to the varying production needs of increasingly individualized products. To expand and agile factory operations has gained increased importance due to the varying production needs of increasingly individualized products. To expand.

Building a Secure, Reliable I4.0 Connectivity Framework

A complete Industry 4.0 wireless solution consists of a 3-layer integration of Application Layer, Communication Layer and Device Layer and fulfills the following requirements:

- Deliver remote management for monitoring and troubleshooting of the wireless network and field devices.
- Provide the flexibility to easily and quickly deploy a wireless mesh backbone.
- Able to integrate with various field devices with different industrial protocols.
- Support advanced network security features.

Industry 4.0 Wireless Network Architecture

NEXCOM’s Industrial Wi-Fi solutions cover the entire spectrum of the 3-layer architecture, and feature an always-on and ruggedized design to meet the industrial requirements of Industry 4.0 (Figure 2).

Compared to generic enterprise wireless solutions which focus design on the user usability and bandwidth utilization, NEXCOM’s I4.0 wireless solutions (Figure 3) offer the following advantages:

- Dedicated Wi-Fi network for field devices: NEXCOM’s I4.0 wireless solutions feature seamless, integrated wireless connectivity and ruggedized manufacturing capacity and meet demands; using traditional approach such as installing complex physical wiring or costly leased lines, is no longer feasible and may also introduce new wiring limitations for certain manufacturing equipment. As a result, wireless connectivity has become a vital component of Industry 4.0, offering the flexibility to easily build and deploy a reliable wireless backbone network without wiring constraints.

- Easy and flexible deployment through EZ Mesh: Utilizing proprietary self-forming and self-healing functions, EZ Mesh provides communication redundancy and low latency path routing to create a reliable, high-speed wireless backbone network.

- Visualized network and field device health management: NEXCOM nCare provides instant visibility to the management of the entire enterprise network to help facilitate the network installation, operation, maintenance, troubleshooting process as well as field device platform health monitoring.

- Field device communication: NEXCOM’s I4.0 wireless solutions support a diverse range of wireless device gateways to bring the field data from different devices to management level through different industrial protocols such as Modbus, HART and Fieldbus protocols.

- Process Automation Wireless Solution for oil and gas industries: To fulfill the challenges in mission-critical industries such as oil, gas and chemical, NEXCOM offers ISA100.11a (IEC 62734)/WirelessHART (IEC 62591) wireless field device connectivity besides the Wi-Fi network solution. The wireless field connectivity solution is based on 802.15.4 radio with tightened security and robust protocols to ensure its reliability in field. NEXCOM industrial wireless solution contains Gateway Systems (integrates gateway, system manager and security manager), Backbone Routers (applies to distributed topology), Device Adaptors and can be managed by NEXCOM nCare manager.
Industry 4.0 Wi-Fi Solution Application

Automated Guided Vehicle (AGV)

In response to the growing production needs, more and more AGVs have been deployed in factories. AGVs are typically controlled through an onboard controller or external controller. However, the actual transport assignments and vehicle route monitoring are assigned and monitored by the control center. By establishing a Wi-Fi network using NEXCOM’s EZ Mesh Wi-Fi control centers, remotely monitor AGV operations in real-time and dispatch job requests wirelessly to AGVs (Figure 4). Compared to conventional roaming methods, NEXCOM’s EZ Mesh solution provides a wireless roaming network with multiple mesh paths to ensure AGVs can roam seamlessly within plant floors with no connection interruption or data loss.

Application Challenge
- The interiors of the plant floors contain various objects that obstruct Wi-Fi signals.
- Delayed data transmissions and data loss when AGVs roam between APs.
- Manage a wireless network can be a daunting undertaking for AGV SAs and their clients.

Process Automation Monitoring

Vertical industrial applications such as chemical, oil and gas processing require strict monitoring and management of manufacturing processes. Pipeline conditions, tank levels and other critical processes require close surveillance to ensure smooth ongoing operations. Due to the strict nature of these applications, most field devices use industrial protocols that deliver transmission reliability and low latency characteristics. Two of the most common protocols are ISA100 and WirelessHART. To respond to this demand, NEXCOM’s NIO 200 series of IoT gateways offers ISA100 and WirelessHART support, and features C1D2 and ATEX certifications for reliable operation in harsh environments.

Application Challenges
- Most wireless process automation networks are based on an All-in-One Gateway topology which lacks the flexibility to scale in size.
- All outbound connections for the field network are restricted to a single wired Ethernet interface, limiting flexible network deployment options.
- Limited RF sensitivity reduces the distance of wireless network coverage, requiring the use of additional repeaters.

NEXCOM Solution Advantages
- Support All-in-One Gateway and Distributed Network topology configurations with a redundant and scalable design to ensure high network availability and ease of deployment.
- Support Wi-Fi AP/Wi-Fi Mesh/Ethernet connections for outbound communication, enabling flexible deployment options for the backbone network with significant cost savings in wiring and installation.
- Unified remote management and monitoring through NEXCOM nCare.
- Ruggedized design featuring IP67 protection, C1D2 and ATEX certifications, and high receiver sensitivity with strong interference resistance.

Wireless Video Surveillance

IP cameras have been widely used in different industries for security surveillance. As IP camera technology advances and gains widespread adoption, many new surveillance applications have emerged. One example is wireless video surveillance of unattended factories. NEXCOM offers industrial Wi-Fi based on the IEEE 802.11ac standard to deliver Gigabit speeds to provide smooth video streaming for point-to-point (PTP) and point-to-multipoint (PTMP) video surveillance applications (Figure 6).

Application Challenge
- Implementing an Ethernet-based wired network incurs high installation costs and wiring challenges.
- Overcome external interferences affecting wireless signal strength while providing adequate wireless bandwidth over long distances to ensure smooth video transmission.

NEXCOM Solution Advantages
- NEXCOM’s industrial-grade Wi-Fi based on IEEE 802.11ac delivers high network availability and ease of deployment.
- Ruggedized design featuring IP67 protection, C1D2 and ATEX certifications, and high receiver sensitivity with strong interference resistance.
- Support Wi-Fi AP/Wi-Fi Mesh/Ethernet connections for outbound communication, enabling flexible deployment options for the backbone network with significant cost savings in wiring and installation.
- Unified remote management and monitoring through NEXCOM nCare.

Plant Floor Monitoring

Whether it is predictive maintenance or production optimization, the smart factory of I4.0 requires plant-wide data from a range of field devices. These data are collected to a central SCADA system for monitoring and control of plant floor operations. To meet the growing demands for maximized productivity, a network that can cover the connectivity of increasingly larger plants and extra manufacturing equipment is needed. In such large-scale networks where physical wiring is infeasible, NEXCOM’s EZ Mesh offers wide wireless coverage through a reliable multi-path mesh network (Figure 7).

Application Challenge
- Using an Ethernet-based wired backbone limits the flexibility to expand the network to accommodate extra manufacturing capacity.
- Devices in areas with wiring constraints prevent remote management and device health monitoring.
- Require a multi-protocol gateway to connect low layer field devices to higher layer networks for upper management supervision.

NEXCOM Solution Advantages
- EZ Mesh technology enables simple and flexible deployment of mesh backbone networks.
- NEXCOM’s nCare offers unified management of the entire network and connected devices, giving administrators hardware visibility of the system to effectively monitor and manage device health status.
- Multi-protocol WiFi gateways are available to connect to field devices with different protocols, bringing them online from the edge to the cloud for upper management supervision.
nCare I4.0 Network Management Solution

A complete industry 4.0 (I4.0) connectivity solution requires a sound management mechanism and a solid backbone network. Not only the backbone network needs to be managed to ensure optimal network performance, the equipment and devices in the network also require close management to ensure stable operation. This will reduce any unexpected device malfunction and increase production efficiency and yield rate.

NEXCOM has released an I4.0-based remote network management tool, nCare (Figure 1), to respond to the connectivity requirements of I4.0. nCare supports various common network management protocols such as SNMP, CAPWAP and LLDP, as well as Modbus to communicate with industrial devices. With various protocol support, nCare not only can manage NEXCOM’s wireless equipment and devices, but also third-party devices (based on the management functions made available by the device) and devices running proprietary protocols. Vital health data from devices in the lower layer network can be retrieved and transferred through the backbone network to nCare for device health management.

NEXCOM’s IWF 800 nCare Edition is a fully integrated I4.0-grade network appliance featuring nCare that supports centralized management of up to 1000 nodes, which can be further scaled for future expansions. A free license for a 30-day trial version is also available upon request.

nCare Highlights

- Network & node device health manager
- Wired & wireless device manager
- Co-exist with 3rd party solutions
- Mobile device app for remote management
- Customization service for vertical device management
- Management capacity of up to 1000 nodes as default for IWF 800 appliance management

Features & Benefits

nCare has been specifically designed with I4.0 in mind. It features an intuitive visualized interface to provide users with simple operations for managing devices. nCare offers users with the following benefits:

Flexible Visualization of Network Topology

- Automatic discovery function for diverse devices: Besides supporting common network management protocols such as SNMP and CAPWAP, nCare also supports Modbus protocol to provide Modbus discovery functions for industrial devices, fulfilling the management needs of diverse devices in I4.0.
- Dynamic status update: nCare offers users with dynamic status update feature. Any device malfunction will be marked by a red icon on the visual topology. At the same time, a log record will be displayed below the topology to show descriptions of the issue to aid in the troubleshooting process (Figure 3 and 4).

Device Health Management from Top to Bottom

- Devices can be managed in real-time through layered security mechanism to carry out surveillance, maintenance, troubleshooting and updating tasks. The basic management items of nCare include the following:
  - Provisioning & configuration
  - Configuration backup & restore
  - Remote AP reboot/device reset
  - Mobile management through App (Figure 2)
- nCare connects to lower layer devices using industrial protocols for system monitoring and management (Figure 6). For example, NEXCOM’s industrial fanless computers with NEXCOM Xcare™ support can be managed by nCare to give administrators hardware visibility and control. The following configuration items and hardware health status are available for NEXCOM Xcare-enabled devices:
  - CPU usage, system temperature, memory usage & storage life cycle
  - Device image upgrade & provisioning
  - Remote reboot
  - Warning notification
  - Support vertical device health management customization service.
- nCare can be customized to support customer-specific proprietary protocols. Furthermore, with added Modbus support, nCare can serve as the health management platform to assist factory managers in acquiring data from various devices for predictive analysis.

System Log Tracking and Notification

nCare utilizes a unique Time Machine log tracking mechanism to assist administrators to effectively analyze and diagnose system errors. It also supports notifications through email, SMS, social media (Facebook, Twitter, WeChat and Line) to alert users about abnormal events (Figure 8).
Main Features
- Automatically discover managed devices by SNMP, CAPWAP & Modbus scan
- Visual topology to display device and wireless link status for remote management
- Support Modbus TCP protocol to communicate with Modbus device for asset management
- Easy remote provisioning, configuration, firmware upgrade and reboot for NEXCOM IWF devices
- Flexible events and notifications with pre-defined threshold
- Supports third-party devices with MB compiler and MB browser
- Comprehensive report and log, including asset status, system log and usage report
- Supports smart phone/tablet APP for mobile management
- Support APP customization service for management of private protocol communication
- Co-existing with 3rd party management solution through standard, open interface
- Management scope can be up to 6,000 nodes

Product Overview
Nowadays, lots of production data or device information needs to be smoothly transmitted to server or cloud for big data analytic in I4.0 applications. Thus, a good management tool to ensure the connectivity facilities, including networking and field devices, run in good condition is very important.

NEXCOM provides nCare, I4.0 Node and Network Manager to fulfill the demand of such management. nCare is designed with protocols for network management and Modbus. This enables nCare to manage not only NEXCOM’s IWF products but also third-party devices. In addition, nCare can also manage those devices implemented with Modbus protocol. nCare is a perfect tool to manage connectivity products from device to network backbone and construct 3-layer management solution in I4.0 applications.

Specifications
nCare Manager Platform Requirement
- Operating System
  - Windows 7 (64-bit)
  - VM supported by project base
- Hardware
  - CPU support: Intel® Atom™ Quad-core 2.4GHz
  - Main memory: 8GB memory with DDR3 1600MHz Long-DIMM sockets
  - (I/O) Interface: Front
    - 2 x USB 2.0 ports
    - 1 x RJ45 type console port
    - 4 x GbE copper ports
  - (I/O) Interface: Rear
    - 2 x USB 2.0 ports
    - 1 x VGA port
  - HDD storage: 500GB

Client Platform Requirement
- PC System
  - Display resolution: 1024 x 768 or above
  - Browser: Chrome, IE11, Firefox
    - Hardware: Intel® Atom™ above, 8GB DDR3
    - Mobile device for APP
      - Android: 5.0 or above (iOS9 will be supported later)

Functionality
Auto Discovery
- Support CAPWAP, LLDP & SNMP, Modbus TCP
- Support NEXCOM IWF AP/Mesh, NIO series gateway, industrial PC series via Xcare utility*
- Support rogue AP detection through SNMP
- Manually add/edit/delete managed devices

Visual Topology
- View multi-layer topology at a glance
- Display Mesh Paths & Neighbor Links dynamically
- Show link traffic and threshold setting instantly
- One click for Device Asset information
- Support remote PMG function
- Support Google, Baidu and customized layout Map
- Support location coordinate remark

AP/Mesh Networking Device Management (Only to NEXCOM IWF)
- Provisioning & configure
- Configuration setting backup & restore
- Restore to factory default
- Remote AP reboot/reset
- Firmware upgrade thru manual/batch/schedule**

Device Node Management
- Support device protocol: Modbus TCP/RTU/ASCII, NEXCOM Xcare, WinM (Windows Management Interface)
- Monitor device health condition: MO ID, CPU/memory usage, temperature, etc. (through Xcare)
- Remote device threshold setting and provisioning
- Remote device control: reboot, watchdog enable/disable
- Customized service for customer owned device asset management

Report & Log
- Managed device profile report
- Managed device status report: network traffic, system usage
- Export formats: csv and txt file
- System log: 6-month log in local database

Event Notification
- Event trigger by
  - Pre-defined threshold
  - generic trap rules
  - Link-up
  - Link-down
  - Warm start
  - Cold start
- Outbound notice
  - Email
  - S.M.S. (Clickatell service subscribed by end user)
  - Social Media: WeChat, Facebook, Twitter

Administration
- Privilege: 3-level (admin, manager, users)
- Concurrent access user: 5
- Supported node number: 1,000 (default)
- Scale up to max. 3,000 nodes by project base

Physical
- 1U 19” rack mount, 430mm x 260mm x 44mm
- Net weight: 4kg
- Operating temperature: 0°C~40°C
- Storage temperature: -20°C~75°C
- Relative humidity: 10%~90% non-condensing
- Certifications: CE/FCC

Ordering Information
- IWF 800 nCare, I4.0 node and network manager
  (P/N: 10T0NCARE000X0)
**Trusted Industrial Wi-Fi Mesh Network**

Stable network transmission is one of the most crucial requirements for Industry 4.0 (I4.0). NEXCOM’s industrial Wi-Fi mesh products offer a unique wireless mesh solution utilizing self-forming and self-healing technology to create a reliable wireless backbone network (Figure 1). When interferences to the transmission signal of a mesh path are present, NEXCOM’s mesh technology will adapt and route to the most optimal network path, ensuring that data is reliably delivered to the central office. At the same time, the dual radio design offers dual link redundant mesh backbone for high reliability, which results in the lowest amount of packet loss.

**Rugged EZ Mesh and Outdoor Mobile Mesh**

NEXCOM’s industrial Wi-Fi mesh solutions consist of two product families: Rugged EZ Mesh and Outdoor Mobile Mesh. EZ Mesh is targeted for mid-size Wi-Fi networks in factory floors, such as wireless communication between low-speed auto guided vehicles (AGV) and control room systems.

Mobile Mesh, on the other hand, is aimed for large-scale Wi-Fi networks requiring a reliable mesh backbone network for enhanced mobility, including the capability to support plant communication and high-speed vehicle communication. All industrial wireless products in EZ Mesh and Mobile Mesh are supported by NEXCOM’s nCare management for remote central management.

**EZ Wi-Fi Mesh Network Solution**

**Secure, Reliable and Intelligent Network Topology**

EZ Mesh is based on the IEEE 802.11s standard and utilizes proprietary protocol to establish an interference-free network communication path. Each single mesh point formed by the EZ Mesh Wi-Fi APs supports self-routing functions without the need and assistance of an extra controller (Controller-less Intelligent Mesh). Furthermore, the EZ Mesh family incorporates a resilient radio module design featuring dual RF, dual band and concurrent dual link to provide network redundancy for the backbone network, as well as the flexibility to adapt to different Wi-Fi application topologies (Figure 2).

**High Performance, Ruggedized for Tough Production Environments**

The EZ Mesh family also implements IEEE 802.11an MIMO technology with the capability to sustain up to 31Mbps of bandwidth even after 4 hops. Combined with the high-power radio design, the EZ Mesh family not only provides far-reaching wireless communication, but also features high resistance to any potential radio interference that may be present in industrial environments. Designed with transmission reliability in mind, EZ Mesh enables factory operators to build a stable and capable wireless IoT network backbone.

**EZ Mesh Highlights**

- Easy installation & scalability for mid-scale deployment (Figure 4)
- Controller-less Self-forming and self-healing (Figure 5)
- High bandwidth: 33Mbps bandwidth capacity after 4 hops
- Support multiple topologies: Mesh/AP/bridge modes
- Rugged, high-power and dual/triple RF design
- High stability with a rate of under 0.01% for packet loss (PER, Packet Error Rate)

**EZ Mesh Application in Factories**

For I4.0 Wi-Fi networks in industrial factory environments, NEXCOM’s IWF 310 industrial EZ Mesh AP can build a trusted Wi-Fi mesh network with central management using nCare to provide shop-floor monitoring and wireless communication with online AGV (Figure 6).

**Requirements of the application**

- Industrial grade Wi-Fi equipment
- Self-healing/ forming with easy installation and central management.
- Support wireless roaming for AGV connection.

NEXCOM’s EZ Mesh solution:

- IWF 300 and IWF 310 offer industrial grade reliability with wide operating temperature ranges for industrial factory environments.
- EZ Mesh supports central management through NEXCOM nCare and provides concurrent dual band operation: 5GHz for mesh networking, and 2.4GHz for Wi-Fi client access.
- EZ Mesh offers wireless roaming ideal for low-speed vehicles travelling <50km/h such as AGV applications in factories.

**Figure 1.** NEXCOM’s Industry 4.0 Wi-Fi Mesh framework offers robust and reliable network transmission.

**Figure 2.** Traditional AP-client mode is linked with a single path.

**Figure 3.** 4-device mesh network in 160m space and 4-hop coverage and performance figures.

**Figure 4.** EZ Mesh offers easy scale-up flexibility. New mesh APs can be scanned and joined to the network automatically. Additional mesh APs can make mesh links more reliable.

**Figure 5.** EZ Mesh topology provides self-forming and self-healing benefits to form an automatically connected/maintained network.

**Figure 6.** EZ Mesh application scenario.
Mobile Mesh Wi-Fi Backbone

Designed for long-distance coverage and large-scale deployments, the Mobile Mesh family of industrial Wi-Fi is capable of delivering up to 100Mbps sustained bandwidth even after 10 hops over the mesh backbone network. Equipped with IP67 protection and high-power RF design, Mobile Mesh delivers high reliability in tough, outdoor environments.

NECOSM’s Mobile Mesh family includes a complete range of outdoor Wi-Fi and industrial Wi-Fi solutions. The IWF 6320 and IWF 6330 outdoor mesh Wi-Fi feature a dual and triple RF module design respectively, and are based on IEEE 802.11n with 2x2 MIMO technology. IWF 3310X, on the other hand, is an industrial Wi-Fi with EN50155 certification to provide reliable operations for railway applications. Both the IWF 6300 series and IWF 3310 series can be used in conjunction for a variety of Wi-Fi applications.

Mobile Mesh Application in Outdoor Environments

The IWF 6330 series of the Mobile Mesh family offers a Mesh/Hopping feature designed for long-distance coverage and large-scale deployments. The IWF 6330 series is ideal for wireless outdoor video surveillance where video data from devices in remote areas need to be transmitted wirelessly over a reliable mesh network (Figure 7).

Requirements of the application:
- Industrial-grade reliability for tough outdoor environments.
- Reliable and stable wireless data transfer rate.
- Trusted and secure Wi-Fi network.

NECOSM’s Mobile Mesh solution:
- IP67-rated waterproof and dust protection to withstand outdoor conditions.
- High-power RF design supporting over 10 mesh hops at up to 100Mbps to provide long-distance wireless coverage.
- NECOSM’s proprietary security technology and self-forming/healing capability enable deployment of a trusted and secure Wi-Fi mesh network with path redundancy.

Mobile Mesh Highlights
- Easy installation & scalability for large-scale deployment
- Multi-path bridge
- Self-forming and Self-healing
- 1200Mbps bandwidth capacity after 10+ hops
- Support Mesh/AP/Bridge modes
- IP67, High-power and Dual/Triple RF design

Figure 7. Mobile Mesh outdoor application scenario.

Product Selection Guide

<table>
<thead>
<tr>
<th>Model Name</th>
<th>EZ Mesh Family</th>
<th>IWF 300</th>
<th>IWF 310</th>
<th>IWF 6320M/H</th>
<th>IWF 6330M/H</th>
<th>IWF 3310XM/H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photo</td>
<td>Industrial EZ Mesh AP</td>
<td><img src="image1.jpg" alt="Image" /></td>
<td><img src="image2.jpg" alt="Image" /></td>
<td><img src="image3.jpg" alt="Image" /></td>
<td><img src="image4.jpg" alt="Image" /></td>
<td><img src="image5.jpg" alt="Image" /></td>
</tr>
<tr>
<td>Category</td>
<td>Industrial EZ Mesh AP</td>
<td>Rugged Industrial EZ Mesh AP</td>
<td>Outdoor Mobile Mesh AP</td>
<td>Outdoor Mobile Mesh AP</td>
<td>Industrial Mobile Mesh AP</td>
<td></td>
</tr>
<tr>
<td>WLAN Standard</td>
<td>802.11a/b/g/n 2x2 MIMO</td>
<td>802.11a/b/g/n 2x2 MIMO</td>
<td>802.11a/b/g/n 2x2 MIMO</td>
<td>802.11a/b/g/n 2x2 MIMO</td>
<td>802.11a/b/g/n 2x2 MIMO</td>
<td></td>
</tr>
<tr>
<td>Number of Radios</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Number of Antennas</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Type of RF Connector</td>
<td>RP-SMA</td>
<td>RP-SMA</td>
<td>N-Type Female</td>
<td>N-Type Female</td>
<td>RP-SMA</td>
<td></td>
</tr>
<tr>
<td>Number of WAN Port</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Number of LAN Port</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Type of LAN</td>
<td>TIA45</td>
<td>TIA45</td>
<td>TIA45 (Encapsulated by M25)</td>
<td>TIA45 (Encapsulated by M25)</td>
<td>TIA45</td>
<td></td>
</tr>
<tr>
<td>IP Rating</td>
<td>IP30</td>
<td>IP30</td>
<td>IP67</td>
<td>IP67</td>
<td>IP30</td>
<td></td>
</tr>
<tr>
<td>Mounting Style</td>
<td>Wall Mount</td>
<td>Wall Mount</td>
<td>Wall/Pole Mount</td>
<td>Wall/Pole Mount</td>
<td>Wall/DIN-Rail Mount</td>
<td></td>
</tr>
<tr>
<td>Temperature</td>
<td>-40°C ~ +80°C</td>
<td>-40°C ~ +80°C</td>
<td>-35°C ~ +75°C</td>
<td>-35°C ~ +75°C</td>
<td>-40°C ~ +80°C</td>
<td></td>
</tr>
<tr>
<td>Dimension (H x W x D) mm</td>
<td>205 x 105 x 25</td>
<td>185 x 108 x 43</td>
<td>220 x 220 x 77</td>
<td>220 x 220 x 77</td>
<td>58.8 x 139.6 x 167</td>
<td></td>
</tr>
<tr>
<td>PoE Input</td>
<td>N/A</td>
<td>N/A</td>
<td>Passive PoE: 48V</td>
<td>Passive PoE: 48V</td>
<td>IEEE802.3at</td>
<td></td>
</tr>
<tr>
<td>DC Input</td>
<td>12VDC</td>
<td>12VDC</td>
<td>N/A</td>
<td>N/A</td>
<td>2 x DC Input: +12 ~ +48V</td>
<td></td>
</tr>
<tr>
<td>Certification</td>
<td>CE, FCC</td>
<td>CE, FCC</td>
<td>CE, FCC</td>
<td>CE, FCC</td>
<td>CE, FCC, EN50155</td>
<td></td>
</tr>
<tr>
<td>Safety</td>
<td>EN60950-1</td>
<td>EN60950-1</td>
<td>EN60950-1</td>
<td>EN60950-1</td>
<td>EN60950-1</td>
<td></td>
</tr>
<tr>
<td>Operation Mode</td>
<td>AP/Router/EZ Mesh</td>
<td>AP/Router/EZ Mesh</td>
<td>AP/Station/Mesh* (*Mesh Mode Only)</td>
<td>AP/Station/Mesh* (*Mesh Mode Only)</td>
<td>AP/Station/Mesh* (*Mesh Mode Only)</td>
<td></td>
</tr>
<tr>
<td>Management Mode</td>
<td>nCare Management</td>
<td>nCare Management</td>
<td>nCare Management</td>
<td>nCare Management</td>
<td>nCare Management</td>
<td></td>
</tr>
</tbody>
</table>
IWF 300

Industrial Access Point
Dual RF, 1 x 802.11an+1 x 802.11 b/g/n 2x2 MIMO

Main Features
• Dual radios and compliant with 1 x 802.11an+1 x 802.11 b/g/n 2x2 MIMO
• Up to 27dBm high RF power
• Multiple function: AP/Client/WDS/EZ Mesh
• Support 12V DC input
• Support -40~80°C extended operating temperature

Product Overview
IWF 300 is QCA9344-based industrial-grade AP/Router/EZ Mesh AP designed with IEEE 802.11 b/g/n 2x2 MIMO and IEEE 802.11an 2x2 MIMO technology. IWF 300 can deliver data rate up to 300Mbps/each radio. In addition, the Radio power can be up to 27dBm for wide range coverage and service. IWF 300 also functions as EZ Mesh network Wi-Fi access with cost-effective option.

Specifications

Wireless Radio
• 1 x IEEE 802.11an 2x2 MIMO
• 1 x IEEE 802.11 b/g/n 2x2 MIMO

Frequency Ranges
• USA: 2.400-2.483 GHz, 5.15-5.35 GHz, 5.725-5.825 GHz
• Europe: 2.400-2.483 GHz, 5.15-5.35 GHz, 5.47-5.725 GHz
* Note: The available frequency range may be different according to different certification.

RF Output Power: IEEE 802.11an (±2dBm)
• IEEE802.11a
  - 13dBm@64M
• IEEE802.11an HT20
  - 13dBm@64M
  - 11dBm@64M
• IEEE802.11an HT40
  - 11dBm@64M

RF Output Power: IEEE 802.11 b/g/n (±2dBm)
• IEEE802.11b
  - 27dBm@1M
  - 24dBm@11M
• IEEE802.11g
  - 27dBm@6M
  - 24dBm@54M
• IEEE802.11an HT20
  - 23dBm@64M
  - 19dBm@54M
• IEEE802.11an HT40
  - 19dBm@54M
  - 15dBm@54M
  - 22dBm@54M

Receive Sensitivity: IEEE 802.11an
• IEEE802.11a
  - -76 dBm@64M
  - -74 dBm@64M
• IEEE802.11an HT20
  - -74dBm@64M
  - -72dBm@64M
• IEEE802.11an HT40
  - -71dBm@64M

Receive Sensitivity: IEEE 802.11a/b/g/n 2Rx
• IEEE802.11b
  - -93dBm@1M
  - -91dBm@11M
• IEEE802.11g
  - -94dBm@6M
  - -80dBm@54M
• IEEE802.11an HT20
  - -94dBm@64M
  - -80dBm@54M
  - -77dBm@54M
• IEEE802.11an HT40
  - -87dBm@54M
  - -73dBm@54M

Built-in Servers & Client Interfaces to Other Services
• DHCP client
• SNMP/v1/v2 client (coming soon)

Physical and Power
• 12VDC power input
• Wall mountable
• Dimensions 205 x 105 x 25 mm
• Weight: 640g

Environment Protection
• Operating temperature: -40~80°C
• Storage temperature: -45~85°C
• Humidity: 0% to 95% maximum (non-condensing)
• Vibration random 0.3g

Certification
• FCC
• CE
• RoHS compliant

Package Contents
• IWF300 unit x 1
• Dual band antenna x 2
• Ethernet cable x 1
• Wall mount kit x 1
• AC-DC power adapter x 1

Ordering Information
• IWF 300-EU (P/N: 10T00030000X0)
• IWF 300-US (P/N: 10T00030001X0)
* Note: The available RF output power will be given by certified power in different regions.
IWF 310

Dual RF, 1 x 802.11an+1 x 802.11 b/g/n 2x2 MIMO

Main Features
- Dual radios and compliant with 1 x 802.11an+1 x 802.11 b/g/n 2x2 MIMO
- 1-4 port CPE RJ45 ports
- Up to 27dBm high RF power
- Multiple functions: AP/Router/EZ Mesh
- Support 12V DC input
- Support 48-80°C extended operating temperature

Product Overview
IWF 310 is QCA9344-based rugged industrial-grade AP/Router/EZ Mesh AP designed with Aluminum and Metal Chassis, and IEEE802.11b/g/n 2x2 MIMO and IEEE802.11an/a 2x2 MIMO technology. IWF 310 can deliver data rate up to 300Mbps/each radio. In addition, the radio power can be up to 27dBm for wide range coverage and service. IWF 310 also functions as EZ Mesh network Wi-Fi access with cost-effective option.

Specifications

**Wireless Radio**
- 1 x IEEE 802.11an 2x2 MIMO
- 1 x IEEE 802.11 b/g/n 2x2 MIMO

**Frequency Ranges**
- USA: 2.400-2.483 GHz, 5.15-5.35 GHz, 5.725-5.825 GHz
- Europe: 2.400-2.483 GHz, 5.15-5.35 GHz, 5.47-5.725 GHz
  * Note: The available frequency range may be different according to different certifications.

**RF Output Power: IEEE 802.11an (±2dBm)**
- IEEE802.11a
  - 27dBm@5GHz
- IEEE802.11n
  - 24dBm@5GHz
  - 63dBm@4GHz
- IEEE802.11g
  - 23dBm@5GHz
  - 19dBm@4GHz

**RF Output Power: IEEE 802.11 b/g/n (±2dBm)**
- IEEE802.11b
  - 27dBm@11M
- IEEE802.11g
  - 27dBm@11M
- IEEE802.11n
  - 24dBm@5GHz
- IEEE802.11n+11a
  - 23dBm@5GHz
  - 19dBm@4GHz

**Receive Sensitivity: IEEE 802.11an**
- IEEE802.11a
  - -76dBm@5GHz
- IEEE802.11n
  - -74dBm@4GHz
- IEEE802.11g
  - -65dBm@5GHz
- IEEE802.11n
  - -19dBm@4GHz

**Receive Sensitivity: IEEE 802.11 b/g/n**
- IEEE802.11b
  - -93dBm@11M
- IEEE802.11g
  - -94dBm@6M
- IEEE802.11n
  - -80dBm@5GHz

**Hardware**
- WAN: 10/100/1000 Base-TX NQ3MDX RJ-45 x 1
- LAN: 10/100/1000 Base-TX 4x4 MDX RJ-45 x 4

**System Management**
- Web-based administration
- SNMP V1/V2c (Coming Soon)
- Syslog information support
- Statistics
- Configuration backup and restore
- One-button button to restore factory default setting
- Firmware upgrade

**Built-in Servers & Client Interfaces to Other Services**
- DHCP client
- SNMP V1/V2c client (coming soon)

**Physical and Power**
- 12VDC power input with DC jack

**Environment Protection**
- Operating temperature: -40~80°C
- Storage temperature: -45~85°C
- Humidity: 0% to 95% maximum (non-condensing)
- Vibration: random 0.5g

**Certification**
- FCC
- CE
- RoHS compliant

**Package Contents**
- IWF310 unit x 1
- Dual band antenna x 2
- Ethernet cable x 1
- Wall-mount kit x 1
- AC/DC power adaptor x 1

**Ordering Information**
- IWF 310-US (P/N: 10T00031001X0)
- IWF 310-EU (P/N: 10T00031000X0)

* Note: The available RF output power will be given by certified power in different regions.
Main Features

- Multiple radios and compliant with IEEE 802.11a/b/g/n 2x2 MIMO
- Fast roaming (hand-over switch time less than 20 ms)
- Smart installation utilizes distance calculation, antenna alignment and site survey tools
- 48VDC PoE input
- Gigabit Ethernet waterproof RJ45
- WEP, WPA, WPA2-PSK/EAP (IEEE 802.1X/RADIUS, TKIP and AES)
- Operating temperature range from -35 to 75°C
- Layer management utility
- Hopping AP, Triple Radios, IEEE 802.11a/b/g/n Dual-Band 2x2 MIMO, High Power
- Static route
- IEEE 802.11i HT20
- 24dBm@1M (all)
- -82dBm@6M, 1Rx
- -76dBm@11M, 1Rx
- IEEE 802.3i HT40
- 22dBm@1M (all)
- -17dBm@5/715 (910MHz)
- 16dBm@5/715 (5790MHz)
- IEEE 802.11a HT20
- 25dBm@5/715 (all)
- -82dBm@6M, 1Rx
- -76dBm@11M, 1Rx
- IEEE 802.11n HT40
- 24dBm@5/715 (all)
### Main Features
- Single radios and compliant with IEEE 802.11a/b/g/n 2x2 MIMO
- Fast roaming (hand-over switch time less than 20 ms)
- Installation utilities: antenna alignment, distance calculation and site survey tools
- Compliant with IEEE 802.11a/b/g/n 2x2 MIMO
- 300 Mbps data rate
- 2 x 12-48VDC redundant power

### Radio Specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>Radio Spec.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IWF3310XH</td>
<td>Hopping AP/CPE, IEEE 802.11 a/b/g/n dual band 2x2 MIMO</td>
</tr>
<tr>
<td>IWF3310XM</td>
<td>MeshMobility AP/CPE, IEEE 802.11 a/b/g/n dual band 2x2 MIMO</td>
</tr>
</tbody>
</table>

### Wireless Radio
- Single 2 x 2 MIMO radio

### Frequency Ranges
- USA: 2,400-2.483 GHz, 5.15-5.35 GHz, 5.725-5.825 GHz
- Europe: 2.400-2.483 GHz, 5.15-5.35 GHz, 5.47-5.725 GHz
- Japan: 2.400-2.497 GHz, 5.15-5.35 GHz, 5.47-5.725 GHz
- China: 2.400-2.483 GHz, 5.725-5.825 GHz

### Receive Sensitivity

<table>
<thead>
<tr>
<th>Model</th>
<th>IEEE 802.11a/h HT20/40</th>
</tr>
</thead>
<tbody>
<tr>
<td>IWF3310XH</td>
<td>-91dBm@100MHz</td>
</tr>
<tr>
<td>IWF3310XM</td>
<td>-84dBm@100MHz</td>
</tr>
</tbody>
</table>

### Environment Protection

<table>
<thead>
<tr>
<th>Model</th>
<th>FCC/CE certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IWF3310XH</td>
<td>Certified</td>
</tr>
<tr>
<td>IWF3310XM</td>
<td>Certified</td>
</tr>
</tbody>
</table>

### Advanced Technology
- Multiple hopping (up to 10 hops with more than 100Mbps throughput)
- Wireless bandwidth limitation
- Support mesh/mobility function in IWF 6330M

### Physical and Power
- Support 48VDC power over Ethernet
- Form Factor: din-rail and wall-mount
- Dimensions: 139.6 x 58.8 x 167 mm
- Weight: 1.73kg
- IP30 rated

### Ordering Information

- IWF 3310XH-US (PN: 10T00331001X0)
- IWF 3310XM-US (PN: 10T00331002X0)
- IWF 3310XM-EU (P/N: 10T00331002X0)
NIO 50
Industrial Wi-Fi Serial/Ethernet Device Gateway

Main Features
- Support transparent Modbus TCP/RTU, Modbus ASCII & MQTT
- Support nCare & Web GUI remote configuration
- Web-based configuration
- 9600~115200 bps baudrate for RS-232/422/485 transmissions
- Secure data access with WPA, WPA2
- 1 x 10/100 fast Ethernet port
- Support 9~36V wide range DC input with 2 pin Phoenix contact terminal block
- Support -20~70°C extended operating temperature
- LED indicators to display: power, serial status and Wi-Fi RSSI signal strength
- SMTP client for time synchronization

Product Overview
NIO 50 brings IoT connectivity into factories, gearing unconnected industrial equipment and machines for smart manufacturing and Industry 4.0. The NIO 50 delivers data acquisition capability, IoT connectivity, convenience of remote monitoring, and industrial durability to provide end-to-end connectivity for the Industrial Internet of Things (IIoT). For Fieldbus-based controllers, legacy manufacturing machines, and serial-based devices, NIO 50 fills the communication gap between edge nodes to the cloud, enabling field data to be harnessed for manufacturing process optimization, remote management, and preventive maintenance.

Specifications
Serial Port
- 1 x RS232/422/485 (software selectable)
- RS232/422/485 with isolation
  - Data bits: 8
  - Stop bits: 1
  - Parity: none, even, odd
  - Baud rate: 9600 bps to 115.2 Kbps

Wireless
- Wi-Fi: 802.11b/g/n 1x1

Ethernet
- 1 x 10/100 Base-TX
- MDI/MDIX auto cross

Reset
- 1 x Reset (restore to default push button)
- Press reset button 3 seconds interval for factory default

Physical and Power
- DC 9~36V with 2 pins Phoenix contact terminal block
- Din rail (optional)/wall mountable
- Dimension: 110 mm x 87 mm x 25 mm
- Weight: 600 g

LED Indicator
- 1 x Power
- 1 x Serial status (orange, green, bi-color)
- 4 x RS22 indicator

SW Features
- OS: FreeRTOS
- Wi-Fi operating mode: Client mode
- Management: nCare, web GUI
- Web GUI for configuration
- Ethernet firmware upgrade
- SMTP client (real IP, static)
- Factory default/reset

Protocol
- Modbus TCP
- Modbus RTU
- Modbus ASCII
- MQTT client for Serial/Ethernet to Wi-Fi
- Transparent mode

Environment Protection
- Operating temperature: -20°C to 70°C
- Storage temperature: -40°C to 85°C

Ordering Information
- NIO 50 (P/N: 10T00005000X0)
  Industrial Wi-Fi Serial/Ethernet device gateway
NIO 51
Industrial Mesh Wi-Fi Serial/Ethernet Device Gateway

Main Features
- Support EZ Mesh and client Wi-Fi operation mode
- Selectable 2.4GHz/5GHz
- Support Modbus TCP, RTU, ASCII/MQTT
- Built-in offline port buffer with over 20 MB of storage
- High immunity to surge, ESD & EFT protection

- Up to 921.6 kbps baud rate for RS-232/422/485 transmissions
- Web-based configuration
- SMTP client for time synchronization
- Support nCare remote configuration
- Wide DC input range with 12-48V
- Wide operation temperature from -40°C to 70°C

Product Overview
NIO 51 brings the wireless connectivity from serial devices or Ethernet devices perfectly to Wi-Fi Mesh backbone in smart factories. Thanks to the Wi-Fi Mesh technology, every device connecting to NIO 51 can easily keep multiple Wi-Fi connecting paths to either IWF310 EZ Mesh backbone or neighbor NIO51 devices to communicate with the control center even the devices are in moving status such as AGV application in factories.

NIO 51 provides flexible conversion between Modbus RTU to Modbus TCP protocols as well as serial to Ethernet/Wi-Fi interfaces within one box. It’s also equipped with high immunity to EMC high level protection in Surge, ESD and EFT, wide operation temperature and redundant power so people do not need to concern about impact from harsh environment. Optional mPCIe port can be used as 3G/LTE WAN connection in the mobility applications or the environments where no Wi-Fi coverage is possible.

NIO 51 fills the communication gap between legacy edge nodes to the control center, enabling field data to be harnessed for manufacturing process optimization, asset management, and preventive maintenance.

Specifications
Wi-Fi Radio
- IEEE802.11a/b/g/n, MIMO 2 x 2

Serial Interface
- RS332/422/485 with isolation
- Data bit: 8
- Stop bit: 1
- Parity: none, even, odd
- Baud rate: 9600 bps to 921.6 Kbps

Ethernet Interface
- 10/100 Mbps

Power Supply
- 12~48V DC

LED Indicator
- 1 x Power/Status
- 1 x Serial status
- 3 x RS485 indicator
- 1 x Wi-Fi 2.4/5GHz indicator
- 1 x Link/Act indicator
- 1 x Extension module

Factory Default/Reset Button
- Press reset button 10 seconds interval for factory default

Connector type
- DC input: Phoenix contact terminal block
- Ethernet: RJ-45 connector
- Serial signal: DB9

Wi-Fi Operating Mode
- EZ Mesh
- Client router

Wi-Fi Security (Client Mode)
- WEP (64/128)
- WPA/WPA2 mixed
- WPA2 personal (PSK+CCMP/AES)

Protocol
- Modbus TCP
- Modbus RTU
- Modbus ASCII
- MQTT client for serial/Ethernet to Wi-Fi (Phase II)
- Transparent mode for Serial to Wi-Fi/Ethernet

Software Watchdog
- DC input: Phoenix contact terminal block
- Ethernet: RJ-45 connector
- Serial signal: DB9

Environment
- Operating temp: -40°C to 70°C
- Storage temp: -40°C to 85°C
- Relative humidity: operating: 5%~95%, non-condensing
- RoHS compliant
- Vibration
  - Random: 2Gms @ 5~500 Hz, EN60068-2-6
  - Sinusoidal: 2Gms @ 5~500 Hz, EN60068-2-2
- Shock: 50G, half sine, 1ms, EN60068-27

Ordering Information
- NIO 51 (P/N: 10T00005101X0)
  Industrial Mesh Wi-Fi Serial/Ethernet device gateway

Dimension Drawing
- Dimension: 81.4 mm x 122.6 mm x 35 mm
- Mounting: Wall mounting, DIN mounting
- Construction: SGCC chassis with fanless design

Certification
- EN60950-1
- EN61000-4-2: level 4
- EN61000-4-3: level 3
- EN61000-4-4: level 3
- EN61000-4-5: level 3
- Serial line surge protection: 1KV (level 2)

Product Overview
NIO 51 brings the wireless connectivity from serial devices or Ethernet devices perfectly to Wi-Fi Mesh backbone in smart factories. Thanks to the Wi-Fi Mesh technology, every device connecting to NIO 51 can easily keep multiple Wi-Fi connecting paths to either IWF310 EZ Mesh backbone or neighbor NIO51 devices to communicate with the control center even the devices are in moving status such as AGV application in factories.

NIO 51 provides flexible conversion between Modbus RTU to Modbus TCP protocols as well as serial to Ethernet/Wi-Fi interfaces within one box. It’s also equipped with high immunity to EMC high level protection in Surge, ESD and EFT, wide operation temperature and redundant power so people do not need to concern about impact from harsh environment. Optional mPCIe port can be used as 3G/LTE WAN connection in the mobility applications or the environments where no Wi-Fi coverage is possible.

NIO 51 fills the communication gap between legacy edge nodes to the control center, enabling field data to be harnessed for manufacturing process optimization, asset management, and preventive maintenance.

Specifications
Wi-Fi Radio
- IEEE802.11a/b/g/n, MIMO 2 x 2

Serial Interface
- RS332/422/485 with isolation
- Data bit: 8
- Stop bit: 1
- Parity: none, even, odd
- Baud rate: 9600 bps to 921.6 Kbps

Ethernet Interface
- 10/100 Mbps

Power Supply
- 12~48V DC

LED Indicator
- 1 x Power/Status
- 1 x Serial status
- 3 x RS485 indicator
- 1 x Wi-Fi 2.4/5GHz indicator
- 1 x Link/Act indicator
- 1 x Extension module

Factory Default/Reset Button
- Press reset button 10 seconds interval for factory default

Connector type
- DC input: Phoenix contact terminal block
- Ethernet: RJ-45 connector
- Serial signal: DB9

Wi-Fi Operating Mode
- EZ Mesh
- Client router

Wi-Fi Security (Client Mode)
- WEP (64/128)
- WPA/WPA2 mixed
- WPA2 personal (PSK+CCMP/AES)

Protocol
- Modbus TCP
- Modbus RTU
- Modbus ASCII
- MQTT client for serial/Ethernet to Wi-Fi (Phase II)
- Transparent mode for Serial to Wi-Fi/Ethernet

Software Watchdog
- DC input: Phoenix contact terminal block
- Ethernet: RJ-45 connector
- Serial signal: DB9

Environment
- Operating temp: -40°C to 70°C
- Storage temp: -40°C to 85°C
- Relative humidity: operating: 5%~95%, non-condensing
- RoHS compliant
- Vibration
  - Random: 2Gms @ 5~500 Hz, EN60068-2-6
  - Sinusoidal: 2Gms @ 5~500 Hz, EN60068-2-2
- Shock: 50G, half sine, 1ms, EN60068-27

Ordering Information
- NIO 51 (P/N: 10T00005101X0)
  Industrial Mesh Wi-Fi Serial/Ethernet device gateway

Dimension Drawing
- Dimension: 81.4 mm x 122.6 mm x 35 mm
- Mounting: Wall mounting, DIN mounting
- Construction: SGCC chassis with fanless design

Certification
- EN60950-1
- EN61000-4-2: level 4
- EN61000-4-3: level 3
- EN61000-4-4: level 3
- EN61000-4-5: level 3
- Serial line surge protection: 1KV (level 2)
Rugged & Ultra-Fast Gigabit Industrial Wi-Fi Solution for Video Surveillance

As Wi-Fi technology advances and Industry 4.0 (I4.0) becomes mega trend, Wi-Fi transmission is gradually becoming the main medium for connecting and monitoring devices in remote areas, such as video surveillance in outdoor and factory environments. Such wireless video surveillance applications often require a reliable wireless network with future-proof bandwidth capacity to transmit video data from the field to the central control center (Figure 1).

**NEXCOM Product Strengths**

Ultra-fast 802.11ac Wi-Fi Reinforces Seamless Transmission for Intensive Video Data

NEXCOM’s IWF 503/4 product family of industrial IP55 outdoor Wi-Fi is based on the advanced IEEE 802.11ac standard, offering wireless broadband performance up to at Gigabit speeds.

The IWF 504D industrial outdoor Wi-Fi features IEEE 802.11ac and IEEE 802.11b/g/n with 2x2 MIMO technology and a maximum data rate of up to 1167Mbps. Equipped with a dual radio design, IWF 504D can operate on one 5GHz band and provide a secondary 2.4GHz band for Wi-Fi client access, enabling factory operators to remotely access and monitor the surveillance system in real time.

**IP55 Ruggedness for Outdoor Areas and Tough Industrial Production Floors**

Featuring a wide operating temperature range of -35 to 75 degrees Celsius, a compact housing with IP55-rated waterproof and dust protection, and high-power RF design to effectively resist noises from other RF interference sources, the IWF 503/4 product family is not only ideal for outdoor areas, but also ideal for harsh factory environments where physical cabling is impractical.

**Multi-topology Support for Application Flexibility**

The IWF 503/4 product family offers quick deployment of wireless backbone networks for point-to-point (PtP) and point-to-multipoint (PtMP) applications, and incorporates high-power radio modules to provide ample amount of network bandwidth at transmission distances ranging within 1 Km (Figure 2).

Main highlights of the IP55 grade IWF 503/4 outdoor Wi-Fi series:

- Reliable wireless backbone network for video transmission.
- Support advanced IEEE 802.11ac with Gigabit bandwidth.
- IP55 protection and compact design for both outdoor and tough indoor environment in production floors.
- High power RF design (27dBm) for long distance communication.
- 24/7 Passive PoE input.

**PtP/PtMP Video Surveillance Application for Factories**

PtP/PtMP video surveillance applications require robust and resilient wireless backbone networks to reliably stream video data from harsh field sites to central control (Figure 3). NEXCOM’s IWF 500 product family equipped with IEEE 802.11ac technology and dual high-power radio provides reliable sustained bandwidth over long distances to ensure smooth video playback.

Requirements of the application:

- Water resistant and dust-tight protection.
- Sustained and reliable wireless transmission of large data volumes.
- Embedded antenna for easy installation and cost effectiveness.

NEXCOM’s IWF solution:

- The IWF 503/4 product family provides IP55-rated waterproof and dust-tight protection to withstand harsh conditions in outdoor and factory environments.
- IWF 503/4 offer over 1Gbps data rate with IEEE 802.11ac technology to provide large bandwidth capacity for wireless video data transmission.
- The IWF 503/4 product family features embedded and detachable antenna models which can be flexibly configured to suit different application requirements.

**Product Selection Guide**

<table>
<thead>
<tr>
<th>Model Name</th>
<th>Photo</th>
</tr>
</thead>
<tbody>
<tr>
<td>IWF 503/503D</td>
<td><img src="Image" alt="Product Selection Guide" /></td>
</tr>
<tr>
<td>IWF 504D</td>
<td><img src="Image" alt="Product Selection Guide" /></td>
</tr>
</tbody>
</table>

- **Category**: PtP/PtMP AP/Router/Client Router
- **MIMO Standard**: 802.11ac, 2x2 MIMO
- **Number of Radios**: 2
- **Number of Antenna**: IWF 503/4: 2 x RP-SMA Female
- **Type of RF Connector**: IWF 503D: 2 x RP-SMA Female
- **Type of LAN**: RJ45
- **IP Rating**: IP55
- **Conformal Coating**: N/A
- **Mounting Style**: Wall/Pole Mount
- **Temperature**: -35°C to +75°C
- **Dimension**: 240 x 135 x 58 mm
- **PoE Input**: Passive PoE, 24V
- **DC Input**: N/A
- **Safety**: EN60950-1, CE, FCC
- **Operation Mode**: AP/Client Bridge, AP/Router/Client Router
- **Management Mode**: Smart/Cloud Management, nCare Management

**Figure 1.** NEXCOM offers Wi-Fi video streaming solutions ideal for harsh outdoor and factory environments.

**Figure 2.** TCP throughput at 1km distance with 1km link.

**Figure 3.** NEXCOM PtP/PtMP video surveillance applications
IWF 503 Series

Product Overview

IWF 503 is an IP55 outdoor cost effective AP/CPE router. IWF 503 is single radio AP/CPE with IEEE802.11ac/an/a 3x3 MIMO with high RF power solution. The maximum data rate up to 1.3Gbps with two SKUs for internal patch antenna (IWF 503) and external antenna (IWF 503D) by customer selectable for high gain in long distance transmission. IWF 503 also design as high power solution, up to 27dBm in 5GHz.

Specifications

Wireless Radio
- 1 x IEEE 802.11ac/an/a 3x3-MIMO

Frequency Ranges
- USA: 5.15~5.35 GHz, 5.5~5.7 GHz, 5.725~5.825 GHz
- Europe: 5.15~5.35 GHz, 5.47~5.725 GHz
- Japan: 5.15~5.35 GHz, 5.47~5.725 GHz
- China: 5.725~5.85 GHz

Note: The available frequency range may be different according to different certification.

RF Output Power: IEEE 802.11ac (12dBm)
- IEEE802.11a - 27dBm@64
  - 25dBm@54M
- IEEE802.11a/n/HT20 - 25dBm@MCS0
  - 23dBm@MCS9
- IEEE802.11a/n/HT40 - 25dBm@MCS0
  - 23dBm@MCS9
- IEEE802.11a/ac/HT80 - 25dBm@MCS0
  - 23dBm@MCS9

Receive Sensitivity: IEEE 802.11ac
- IEEE802.11a - -95dBm@64
  - -77dBm@54M
- IEEE802.11a/n/HT20 - -90dBm@MCS0
  - -70dBm@MCS7
  - -70dBm@MCS8
- IEEE802.11a/n/HT40 - -88dBm@MCS0
  - -68dBm@MCS7
  - -62dBm@MCS9
- IEEE802.11a/ac/HT80 - -88dBm@MCS0
  - -68dBm@MCS7
  - -62dBm@MCS9

Physical and Power
- 24VDC passive PoE
- Wall/Pole mountable
- Dimension: 240x135x58 mm
- Weight: TBD

Built-in Servers & Client Interfaces to Other Services
- DHCP client
- SNMP v2c/3 client

Security
- WEP (64/128/152)
- WPA/WPA2 mixed
- WPA2-personal (PSK=CCMP/AES)
- WPA2-enterprise (802.1X certification)
- Hidden ESSID support
- MAC address filtering (MAC ACL)
- Station isolation

System Management
- Web-based administration
- SNMP V1/V2c
- Provides event log
- Syslog information support
- Statistics
- Configuration backup and restore
- One-button click to restore factory default setting
- Firmware upgrade
- WES

Environment Protection
- Operating temperature: -35~75°C
- Storage temperature: -40~80°C
- Humidity: 0% to 95% maximum (non-condensing)
- Vibration: random 0.3g

Certification
- FCC
- CE
- RoHS compliant

Package Contents
- IWF 503 unit x 1
- 24V PoE injector
- Steel clamps* 2 for pole mount
- QIG

Ordering Information
- IWF 503-US (P/N: 10T00050300X0)
- IWF 503-US (P/N: 10T00050301X0)
- IWF 503-US (P/N: 10T00050302X0)
- IWF 503-US (P/N: 10T00050303X0)

* Note: The available RF output power will be given by certified power in different regions.
Main Features

- AP/Client bridge router/Client router/WDS mode supported
- Compliant with IEEE 802.11 ac+b/g/n 2x2 MIMO
- 24VDC PoE input
- 1 WAN + 1 LAN ports GbE Ethernet RJ45
- WEP, WPA, WPA2
- Operating temperature range from -35 to 75°C
- FCC/CE certification

Specifications

Wireless Radio

- 1 x IEEE 802.11ac 2x2 MIMO
- 1 x IEEE 802.11b/g/n 2x2 MIMO

Frequency Ranges

- USA: 2.400~2.483 GHz, 5.15~5.35 GHz, 5.47~5.725 GHz
- Europe: 2.400~2.483 GHz, 5.15~5.35 GHz, 5.47~5.725 GHz
- Japan: 2.400~2.483 GHz, 5.25~5.85 GHz
- China: 2.400~2.483 GHz, 5.725~5.85 GHz

RF Output Power: IEEE 802.11b/g/n (±2dBm)

- IEEE802.11b
  - 27dBm@1M
  - 24dBm@11M
- IEEE802.11g
  - 27dBm@1M
  - 24dBm@11M
- IEEE802.11g/HT20
  - 23dBm@MCS8 in VHT20
  - 19dBm@MCS15
- IEEE802.11g/HT40
  - 23dBm@MCS8
  - 19dBm@MCS15
- IEEE802.11ac VHT 80Mhz
  - 24dBm@MCS0
  - 22dBm@MCS7
  - 18dBm@MCS15

Receive Sensitivity: IEEE 802.11a/ac

- IEEE802.11a
  - -95dBm@1M
  - -91dBm@11M
- IEEE802.11n
  - -94dBm@1M
  - -80dBm@54M
- IEEE802.11n/HT20
  - -72dBm@MCS5/15
- IEEE802.11n/HT40
  - -72dBm@MCS5/15

Hardware

- WAN: 10/100/1000 Base-TX MDI/MDIX RJ-45 x 1
- LAN: 10/100/1000 Base-TX MDI/MDIX RJ-45 x 1
- Compliant with
  - IEEE802.3/802.3u
- Hardware Based 10/100/1000, full/half, flow control auto negotiation
- Push buttons: 1 x reset
- LED: 1 x Power & Status; 1 x WAN; 1 x Wi-Fi
- SMA: 4 x with RP-SMA connectors

Operating Mode

- AP
- AP/router
- Client router
- Client bridge
- WDS

Security

- WEP
- WPA/WPA2 mixed
- WPA2-personal (PSK+CCMP/AES)
- Hidden ESSID support
- MAC address filtering (MAC ACL)
- Station isolation

System Management

- Web-based administration
- SNMP V1/V2c, NEXCOM private MIB
- syslog, information support
- Statistics
- Configuration backup and restore
- One-button click to restore factory-default setting
- Firmware upgrade
- Telnet/SSH
- Support nCare management system

Built-in Servers & Client Interfaces to Other Services

- DHCP client
- SNMP V1/V2c, client (coming soon)

Physical and Power

- 12~24VDC passive PoE
- Wall/pole mountable
- Dimension 240 x 135 x 58 mm
- Weight: 442g

Environment Protection

- Operating temperature: -35~75°C
- Storage temperature: -40~80°C
- Humidity: 0% to 95% maximum (non-condensing)
- Vibration: random 0.3g

Certification

- CE
- RooS compliant

Package Contents

- IWF 504D unit x 1
- 24V PoE injector
- Steel clamps* 2 for pole mount
- QIG

Ordering Information

- IWF 504D-EU (P/N: 10T00504D00X0)
- IWF 504D-US (P/N: 10T00504D01X0)

* Note: The available RF output power will be given by certified power in different regions.
**NEXCOM Product Strengths**

**Manageable ISA100.11a & WirelessHART Compliant Gateway**

The NIO 200 series is also supported by NEXCOM’s nCare manager for remote central management. Using nCare, administrators can easily monitor and manage device status and mesh network links through an intuitive, graphical user interface, simplifying the management of large-scale deployments.

**Unique Wi-Fi Mesh Backbone Technology**

In addition to ISA100.11a or WirelessHART support, the NIO 200 series also utilizes NEXCOM’s EZ Mesh Wi-Fi backbone technology, which features proprietary self-forming and self-healing functions to help construct a reliable and robust wireless mesh backbone for connecting field devices with wiring constraints.

**C1D2 and ATEX Certified for Anti-Explosion**

Chemical plants, oil and gas refineries are often located in areas with tough environmental conditions and require ruggedized systems. To provide reliable operation, the NIO 200 series is C1D2 and ATEX certified for explosion proof, and complies with level 4 criteria of the IEC 61000 standard for electrostatic discharge, surge and electrical fast transients protection. For power input, all products in the NIO 200 lineup accept wide-range DC input of 12 V to 48 V and a secondary PoE power input for power redundancy.

**High Wireless Radio Frequency (RF) Sensitivity**

For wireless sensor/instrument communication, the NIO 200 series features a radio module with increased receiver sensitivity capable of providing more than twice the transmission distance over other similar devices using the same radio frequency (RF) power.

**NIO 200 Series Supported Deployment Architectures**

The NIO 200 series supports two types of deployment architectures: All-in-One Gateway and Distributed Network (Figure 1). Currently, All-in-One Gateway is the most widely adopted architecture in the industry. This architecture consists of a single gateway serving as the main communication device for multiple field devices. Although ideal for simple deployments, All-in-One Gateway lacks the flexibility to scale in size. Distributed Gateway, on the other hand, uses a Wi-Fi mesh backbone ideal for large-scale deployments with wiring limitations and offers redundant communication paths to ensure high network uptime.

**Figure 1. The NIO 200 series offers two types of deployment architectures: All-in-One Gateway and Distributed Network.**

**Product Selection Guide**

<table>
<thead>
<tr>
<th>Model Name</th>
<th>NIO 200IDR</th>
<th>NIO 200IDG</th>
<th>NIO 200IDG/ATEX</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Photo</strong></td>
<td><img src="image1.jpg" alt="Photo" /></td>
<td><img src="image2.jpg" alt="Photo" /></td>
<td><img src="image3.jpg" alt="Photo" /></td>
</tr>
<tr>
<td><strong>Wireless LAN Standard</strong></td>
<td>802.11 a/b/g</td>
<td>802.11 a/b/g</td>
<td>802.11 a/b/g</td>
</tr>
<tr>
<td><strong>Wireless Field Protocol</strong></td>
<td>ISA100</td>
<td>ISA100</td>
<td>ISA100</td>
</tr>
<tr>
<td><strong>Gateway Function</strong></td>
<td>N/A</td>
<td>Standalone gateway</td>
<td>All-in-One gateway</td>
</tr>
<tr>
<td><strong>Wireless Mode</strong></td>
<td>Mesh/MP</td>
<td>Mesh/MP</td>
<td>Mesh/MP</td>
</tr>
<tr>
<td><strong>Ethernet Speed</strong></td>
<td>10/100/1000</td>
<td>10/100/1000</td>
<td>10/100/1000</td>
</tr>
<tr>
<td><strong>IP Rating</strong></td>
<td>IP67</td>
<td>IP67</td>
<td>IP67</td>
</tr>
<tr>
<td><strong>Temperature</strong></td>
<td>-40°C to +75°C</td>
<td>-40°C to +75°C</td>
<td>-40°C to +75°C</td>
</tr>
<tr>
<td><strong>PoE Type</strong></td>
<td>IEEE802.3af</td>
<td>IEEE802.3af</td>
<td>IEEE802.3af</td>
</tr>
<tr>
<td><strong>DC Input Range</strong></td>
<td>12 – 48V</td>
<td>12 – 48V</td>
<td>12 – 48V</td>
</tr>
<tr>
<td><strong>Network Management</strong></td>
<td>SNMP/V1/V2c/Web GUI</td>
<td>SNMP/V1/V2c/Web GUI</td>
<td>SNMP/V1/V2c/Web GUI</td>
</tr>
<tr>
<td><strong>Certification</strong></td>
<td>CE, FCC</td>
<td>CE, FCC</td>
<td>CE, FCC</td>
</tr>
<tr>
<td><strong>Anti-Explosive</strong></td>
<td>C1D2/ATEX</td>
<td>C1D2/ATEX</td>
<td>C1D2/ATEX</td>
</tr>
</tbody>
</table>
**Main Features**

- Full Mesh topology: robust wireless connectivity from ISA100/WirelessHART field device coverage to Wi-Fi backbone
- Perfect triple-play infrastructure: video surveillance via high-throughput Wi-Fi backbone ensures video transmission without compromising video performance.
- Dual Wi-Fi Mesh path establishes better stability in backbone transmission.
- Wide temperature range, high EMC immunity to Surge, ESD and EFT
- Suitable for deployment in hazardous environments.
- Incorporates power redundancy (DC- and PoE).
- Distributed network topology provides scalable infrastructure: easy integration and cost saving.

**Specifications**

- **Wireless Radio**
  - IEEE 802.11a/b/g or 2.4-MM6 2.4-2.5 GHz
  - IEEE 802.15.4 2.4-2.5 GHz
- **Wi-Fi Frequency Ranges**
  - USA: 5.15-5.25 GHz, 5.725-5.825 GHz
  - Europe: 5.47-5.725 GHz
- **RF Output Power: IEEE 802.11a**
  - 5.15 GHz: 15 dBm (2 antennas)
  - 5.8 GHz: 15 dBm (4 antennas)
- **Wi-Fi Security (AP Mode)**
  - WEP (64/128/152)
  - WPA (PSK, TKIP, AES)
  - WPA2 (PSK, AES)
- **Wi-Fi Frequency Ranges**
  - 2.4 GHz: 20 MHz
  - 5 GHz: 40 MHz
- **Modulation**
  - DSSS
  - FHSS
  - OFDM
- **Data Rate**
  - 250 kbps
- **Standard IEEE**
  - 802.11a
  - 802.15.4
- **Modulation**
  - 802.11a/Wi-Fi: OFDM
  - ISA100: GFSK, 802.15.4, 1 Tx, 1 Rx

**Product Overview**

NIKCOM NIO 200 is a powerful distributed network topology ISA100.11a access point integrating 802.11n Mesh technology. With ISA100.11a/WirelessHART technology, NIO 200 can establish fully Mesh network to ensure robust and reliable communication for mission-critical industrial wireless applications. The integration of both 802.11n Mesh & ISA100.11a/WirelessHART technologies gives a full Mesh infrastructure from field devices to Wi-Fi backbone, thus a concrete wireless connectivity can be assured. It's designed to meet CID2 and ATEX certified requirement and is a perfect solution to critical data monitoring and serving in oil & gas, chemical plant, etc...

**Environment Protection**

- Operating temperature: -40-75°C (4Bar)
- Storage temperature: -40-80°C
- Humidity: 0-95% maximum (non-condensing)
- Vibration: random 9.3g

**Certification**

- UL 60950-1; 60950-22
- Radio approvals:
  - FCC Part 15.247, 15.407
  - EN 300 328
  - EN 301 893
- EN and susceptibility - FCC Part 15.107, 15.109
- IEC 61000-4-2 level 4 ESD immunity

**Anti-Explosive Certification**

- ATEX: Class I, Zone 2; Ex tA II, T4
- UL: Class I, Division 2, Groups A, B, C and D, T4

**Ordering Information**

<table>
<thead>
<tr>
<th>Product Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIO 200HAG-US</td>
<td>Backbone Router</td>
</tr>
<tr>
<td>NIO 200IDR-US</td>
<td>Distributed Gateway</td>
</tr>
<tr>
<td>NIO 200IAG-US</td>
<td>Distributed Gateway</td>
</tr>
<tr>
<td>NIO 200IDG-US</td>
<td>All-in-One Gateway</td>
</tr>
</tbody>
</table>

**Optional Accessories**

- **P/N: 5040210012X00**
  - SIMPLE WALL MOUNT KIT VER: A SIN SUPER CIRCLE 92x228x90mm
  - SENG: 3.2x white

- **P/N: 5040210010X00**
  - POLE MOUNT FOR NIO200 VER: A SIN SUPER CIRCLE 92x228x90mm
  - SECC: 3.2x white

- **P/N: 5A00000066X00**
  - Antenna arrayer, DC-6 MHz N MALE TO T N FEMALE

- **P/N: 6034T90013X00**
  - Directional Antenna 2.4GHz-3.7GHz 16–17 dB

- **P/N: 6034T90009X00**
  - Directional Antenna 2.4GHz-3.7GHz 16–17 dB

- **P/N: 6034T90001X00**
  - Directional Antenna 2.4GHz-3.7GHz 16–17 dB

- **P/N: 6034T90003X00**
  - Directional Antenna 2.4GHz-3.7GHz 16–17 dB