Contents

IoT Automation Systems, The Solutions to Industry 4.0 02

Industrial IoT Network Infrastructure 04
Cyber Physical System Connectivity 08
NEXCOM Industrial IoT Studio 10
CPS 100 12
CPS 200 14
NISE 50 16

Industrial IoT Security 18
IFA 1610 22
IFA 2610 24
IFA 3610 26
IVO 1000 28
INAS 330 30

Industry 4.0 Wireless Solution (IWS) 32
nCare 4.0 Network Management Solution 36
IWF 800 nCare 38

Trustworthy Industrial Wi-Fi Mesh Network 40
IWF 300 44
IWF 310 46
IWF 6300 48
IWF 3310XH/M 50
NIO 50 52

Rugged & Ultra-Fast Gigabit Industrial Wi-Fi Solution for Video Surveillance 54
IWF 501/501D 56
IWF 502/502D 57
IWF 503 58
IWF 504D 60

NEXCOM’s ISA100.11a/ WirelessHART Gateway for Wireless Process Automation 62
NIO 200 64
**IoT Automation System: The Solutions to Industry 4.0**

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 enable 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 to 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 benefit customers in an increasingly competitive global marketplace and lead manufacturers to smart factory automation.

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 enable 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 to 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 benefit customers in an increasingly competitive global marketplace and lead manufacturers to smart factory automation.
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 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.

NEXCOM’s CPS lineups are designed with a graphical user interface (GUI) and supports drag-and-drop operations.
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 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.

As Industry 4.0 is taking the industrial sector by storm, factory operations 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.

From the technology point of view, the network architecture for Industry 4.0 is formed of three layers: operational technology, communications technology, and information technology (Figure 5). The operational technology layer includes a wide array of on-site equipment devices generating a flood of data on field operations. Communications technology makes up a network backbone that transfers data to remote ends where information technology can be applied to generate feedbacks on operations based on results of big data analysis.

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, and equipment are coming online with the aim to improving operational efficiency. To keep improvements on course, NEXCOM has added rich features sets, expandability, and rugged design to its HENGE™ series which is made up of the IFA family of industrial firewalls and VPN dispatcher. The IFA family consists of three all-round broadband-compatible multi-port industrial firewalls/VPN routers. They offer stateful packet inspection (SPI), denial-of-service/dynamic denial-of-service protection, intrusion inspection, port scanning detection, and real-time alerts. The IFA family provides IPv6 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.

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 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.

As Industry 4.0 is taking the industrial sector by storm, factory operations 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.

From the technology point of view, the network architecture for Industry 4.0 is formed of three layers: operational technology, communications technology, and information technology (Figure 5). The operational technology layer includes a wide array of on-site equipment devices generating a flood of data on field operations. Communications technology makes up a network backbone that transfers data to remote ends where information technology can be applied to generate feedbacks on operations based on results of big data analysis.

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, and equipment are coming online with the aim to improving operational efficiency. To keep improvements on course, NEXCOM has added rich features sets, expandability, and rugged design to its HENGE™ series which is made up of the IFA family of industrial firewalls and VPN dispatcher. The IFA family consists of three all-round broadband-compatible multi-port industrial firewalls/VPN routers. They offer stateful packet inspection (SPI), denial-of-service/dynamic denial-of-service protection, intrusion inspection, port scanning detection, and real-time alerts. The IFA family provides IPv6 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 IIoT (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 control capability, and IoT human-machine interface (HMI). IoT communications features required of a CPS include IoT communications support, IoT automatic control capability, and IoT human-machine interface (HMI). IoT communications features required of a CPS include IoT communications support, IoT automatic control capability, and IoT human-machine interface (HMI).

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 IoT 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 a double, 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 industrial computers equipped with Modbus, fieldbus, and OPC UA communication capabilities to amass data from most industrial systems. As to upper connectivity, MQTT, SQua, 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.

A CPS 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. The best choice of hardware platform for a CPS is a double, 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 industrial computers equipped with Modbus, fieldbus, and OPC UA communication capabilities to amass data from most industrial systems. As to upper connectivity, MQTT, SQua, 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

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

![Diagram of CPS architecture](image)

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

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.
NEXCOM Industrial IoT Studio

Main Features
- Processing data analytically redefined 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, EtherCAT/PI) configuration, Modbus/RTU and Modbus/TCP master, OPC-UA client for field devices/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, demonstrates 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modbus-TCP write</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modbus-RTU read</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modbus-RTU write</td>
</tr>
<tr>
<td>Fieldbus</td>
<td>Get the registers and status from the controller/devices with Fieldbus interface</td>
<td>PROFIBUS read</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PROFIBUS write</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PROFINET read</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PROFINET write</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ethernet/IP read</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ethernet/IP write</td>
</tr>
<tr>
<td>Data</td>
<td>Process or encrypt/decrypt data from buffering</td>
<td>Merge</td>
</tr>
<tr>
<td>process</td>
<td></td>
<td>Boundary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical section</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GPIO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HW Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Base64Encode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Base64Decode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3DesEncrypt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3DesDecrypt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OPC-UA Client</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Graph</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<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, cv, nni, join, wait, the</td>
<td></td>
</tr>
<tr>
<td>Social</td>
<td>Access 'multipart/form-data' content by email</td>
<td>Email in</td>
</tr>
<tr>
<td>Storage</td>
<td>Read/write the file or database</td>
<td>Email out</td>
</tr>
<tr>
<td>Cloud</td>
<td>Provides Azure service</td>
<td>eventhub</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</td>
<td>X</td>
<td>Q</td>
</tr>
<tr>
<td>CPS 200</td>
<td>X</td>
<td>Q</td>
</tr>
</tbody>
</table>

Note: Products and modules 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

Industrial IoT Remote Gateway

Main Features
- Seamless integration of field devices, web, database and cloud services
- Fieldbus (slave) PROFINET®, 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 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 storage/analytics/statistics...and so on.

Benefits of CPS Solution
- 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

Gateway Platform Specifications
CPU Performance
- On-board Intel® Atom™ processor E3805 1.33 GHz
Memory
- Built-in DDR3L 2GB system memory
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 USB 3.0 (900mA)
- 1 x USB 2.0 (500mA)
- 1 x RS232/485, 2.5KV isolation protection
- Management console
- 4 x RJ45

Wireless Connectivity (optional module)
- IEEE 802.11 a/b/g/n connectivity

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

Storage Device
- 1 x eMMC 4GB 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 ~ 70°C

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

Regulation
- CE/EN
- LVD

Ordering Information
- CPS 100-RE (P/N: 10JC0010001X0)
Industrial IoT Remote Gateway, E3805, 2GB RAM, 16GB eMMC, PROFINET®
- CPS 100-DP (P/N: 10JC0010000X0)
Industrial IoT Remote Gateway, E3805, 2GB RAM, 16GB eMMC, PROFINET®
CPS 200

Main Features
- Seamless integration of field devices, web, database and cloud services
- Fieldbus (slave) PROFBUS®, PROFINET® or EtherNet/IP® support
- Modbus TCP/RTU, OPC UA support in parallel
- Intuitive visual flow-based programming paradigm
- Secure HTTP/HTTPS 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 processing, exchange field data over network security between edge and the Cloud, flexible field data storage/analytics/statistics... and so on.

Benefits of CPS Solution
- Seamless integration of field devices, web, database and cloud services
- Fieldbus (slave) support – PROFBUS®, PROFINET® or EtherNet/IP®
- Industrial protocol support – Modbus TCP/RTU, OPC UA client
- Data mining – MQTT-broker, OPC UA client
- Data processing and distribution – JavaScript, JSON, XML, MQTT-broker, TCP, UDP, HTTP, web socket, E-mail

Secure Gateway Management
- Secure boot
- Gateway monitoring
- Network protocol – HTTP, HTTPS, DHCP, TCP, UDP, SSH, SNMP
- Wireless support – Wi-Fi, 3G/4G, WiMAX

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
- On-board Intel® Celeron® processor J1900 Quad Core 2.0 GHz
Memory
- Built-in DDR3L 4GB system memory
Display
- DIP and DVI-I display output
Networking Connectivity
- 2 x 10/100/1000Mbps LAN ports
- Isolated field control 10/100Mbps ports, PROFBUS®, PROFINET® or EtherNet/IP™
Major I/O Connectivity
- 1 x miniSIM card holder
- 1 x USB 3.0 (3000mA)
- 3 x USB 2.0 (500mA per each)
- 2 x RS232/485, 2.5KV isolation protection on COM1
- Power on/off switch
- 1 x DIO

Wireless Connectivity (optional module, up to 2)
- IEEE 802.11 a/b/g/n connectivity
- 3G/4G 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)
- 2.25K g (w/ Disk)

Construction
- Aluminum and metal chassis with fanless design

Shock Protection
- SSD: 20G, half sine, 11ms, IEC60068-2-27
- CFast: 50G, half sine, 11ms, IEC60068-2-27

Vibration Protection w/ CFast & SSD condition
- Random: 2Grms @ 5~500HZ, IEC60068-2-6
- Sinusoidal: 2Grms @5~500Hz, IEC60068-2-6

Operation Temperature
- Ambient with air flow: 0°C ~ 50°C
- Storage Temperature
- -20°C ~ 80°C, relative humidity: 10% ~ 95%

Regulation
- CE/FC C
- LVD

Ordering Information
- CPS 200-DP (P/N: 10JC0020000X0)
  Industrial IoT Edge gateway, J1900, 4GB RAM, 128GB SSD, PROFBUS®
- CPS 200-RE (P/N: 10JC0020001X0)
  Industrial IoT Edge Gateway, J1900, 4GB RAM, 128GB SSD, Real-time Ethernet
NISE 50

Intel® Atom™ Processor E3826 Dual Core Fanless System

Main Features
- Onboard Intel® Atom™ processor E3826 dual core, 1.46GHz
- 1 x HDMI display
- 2 x Intel® i210AT QFE LAN ports; support WOL, teaming and PXE
- 4 x USB 2.0
- 3 x mini-PCIe sockets for optional Wi-Fi/3.5G/LTE modules
- 1 x RS232, 1 x RS232 (only Tx/Rx/GND), 1 x RS422/485 with auto flow control
- Support 5 ~ 55 degree C operating temperature
- Support 24V DC input

Product Overview
Powered by the latest generation of Intel® Atom™ processor E3826 (formerly codenamed "Bay Trail-M"), NISE 50 series positions at the intelligent IoT gateway for factory automation and for smart utility applications. Up to 4G on-board DDR3L memory, the NISE 50 series support operating temperature from -5 up to 55 degree C with 24V DC input with +/-20% range. The NISE 50 series have strong connectivity - Ethernet-based LAN port and traditional RS485, mainly for Modbus TCP or Modbus RTU communication. For wireless connectivity, there are 3 mini-PCIe sockets which can support optional wireless modules for IoT applications, for example, WiFi, Bluetooth, 3.5G and 4G LTE module. NISE 50 is definitely the best choice for M2M intelligent system as an intelligent IoT gateway.

Specifications

CPU Support
- Default: onboard Intel® Atom™ processor E3826 Dual Core, 1.46GHz
- Option: support Intel® Atom™ processor E3845 Quad Core, 1.91GHz (by request)

Main Memory
- On-board 2GB DDR3L 1066/1333 RAM
- Max up to 4GB for option

Display Option
- 1 x HDMI display

I/O Interface-Front
- 1 x Line-out
- Support 24V DC input

I/O Interface-Internal
- 4 x GPIO programmable LED
- 4 x GPIO (programmable to GPIO or GPI)
- 1 x DIP switch
- Support 24V DC input

I/O Interface-Rear
- 3 x DB9 for COM1 & COM2 & COM3
- 3 x mini-PCIe sockets for optional WiFi/3.5G/LTE modules
- COM1: full RS232 signal
- COM2: RS232, only support Tx/Rx/GND
- COM3: RS422/485 auto flow control

Support OS

<table>
<thead>
<tr>
<th>Model Name</th>
<th>NISE 50</th>
<th>NISE 50-4G-32G</th>
<th>NISE 50W</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>eMMC</td>
<td>mSATA</td>
<td>mSATA</td>
</tr>
<tr>
<td>Storage</td>
<td>2GB</td>
<td>4GB</td>
<td>2GB</td>
</tr>
<tr>
<td>OS</td>
<td>Android4.4 64bit</td>
<td>WIN10 IoT Ent. 64bit</td>
<td>WES8 32bit 32bit 64bit 64bit 32bit</td>
</tr>
<tr>
<td></td>
<td>WIN 7 PRO 32bit 64bit 32bit</td>
<td>WEC7 32bit 32bit 32bit</td>
<td></td>
</tr>
</tbody>
</table>

* Note: only one LAN can be active under Android 4.4

Dimensions
- 162mm(W) x 26mm(H) x 150mm(D) without wall-mount bracket
- Metal Chassis with fanless design

Environment
- Operating temperature: Ambient with air flow: 0°C to 55°C (according to IEC60068-2-1, IEC60068-2-2, IEC60068-2-14)
- Storage temperature: -20°C to 75°C
- Relative humidity: 10% to 95% (non-Condensing)
- Shock protection:
  - mSATA / eMMC: 50G, half sine, 11ms, IEC60068-2-7
  - Vibration protection with SATA or eMMC condition:
    - Random: 2Grms @ 5~500 Hz, IEC60068-2-6
    - Sinusoidal: 2Grms @ 5~500 Hz, IEC60068-2-6

Certifications
- CE
- FCC Class A
- UL/cUL

Ordering Information
- NISE 50 (P/N: 10J00005000X0)
  Intel® Atom™ Processor E3826 Dual Core Fanless System, with on-board 16GB eMMC and 2GB DDR3L RAM
- 24V, 60W AC/DC power adapter w/o power cord
  (P/N: 1400060033X00)
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 HENCE™ family, which is made up of industrial firewalls of the IFA series, VPN dispatchers IVD 1000, and the extremely rugged network-attached storage NAS 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 edge firewall protection, intrusion prevention protection, and robust data storage at once. To sum up, the high level of function integration of the HENCE™ 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) protection, intrusion detection, port scanning detection, and real-time alerts. To arm industrial systems with extra shields, the IFA series is equipped with IPv4 and IPv6 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 premises, automation systems in industrial automation industries, 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 can neither 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 viruses spread by USB devices. With severe ramifications like power outage proven in some cases, precautions must be considered in the early stages of planning.

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,

Increasing 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. 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 on a public or private network so VPN gateways and field devices can securely connect to a network to allow for real-time, remote monitoring and data acquisition.

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.
and anti-vibration protection. As to data availability, an iNAS must support RAID configuration, buffer 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 nysnc commands to help users choose from mirror backup and incremental backup according to application’s 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 into place.

Lastly, the iNAS 330 has rugged design which has been a hallmark of NECOM 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

Vulnerabilities of backdoor intrusion can trigger all kinds of attacks, for instance denial of service and backdoor intrusion. There are a variety of 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 can trigger all kinds of attacks, for instance denial of service and backdoor intrusion.

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 factories 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).

**Figure 3. Vulnerability assessment processs.**

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.

Q: Expert advice to the question is using vulnerability assessment. VA services. Despite the benefits of gaining online, being connected also increases the possibilities of getting attacked. There are a variety of 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 can trigger all kinds of attacks, for instance denial of service and backdoor intrusion.

A: 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.
IF A 1610
CoreFort™ Industry Firewall, 2 Ports VPN Router

Main Features
- Stateful (L4) 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

Specifications

Network Security
- Stateful packet firewall
- Intrusion detection/prevention (DoS/IPS)
- Multiple public IPs
- SSH/SSL support
- Portscan detection
- DoS and DDoS protection
- SYN/ICMP flood protection
- DoS and DDoS protection
- Portscan detection
- VoIP/SIP support
- SNMP support (V1/V2/V3)
- Multiple public IPs
- Stateful packet 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 builders/system integrators 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.

Product Overview

The CoreFort™ Industry Firewall series is a fully integrated, 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 builders/system integrators 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 (DoS/IPS)
- Multiple public IPs
- SSH/SSL support
- Portscan detection
- DoS and DDoS protection
- SYN/ICMP flood protection
- DNS proxy/routing
- WAN
- Supports uplink/s Wan: Ethernet (Static/DHCP), PPPoE
- Traffic Shaping
- Bandwidth management
- User Authentication
- Active directory/NTLM
- LDAP
- Local

Network Address Translation
- Destinalion NAT
- Incoming routed traffic

VPN (Virtual Private Network)
- One-to-one NAT
- Source NAT (SNAT)
- IPsec NAT Traversal
- Bridging
- Firewall stealth mode
- OSI layer 2 firewall function
- Spanning tree
- Unlimited bridges
- Unlimited interfaces per bridge

VPN (Virtual Private Network)
- One-to-one NAT
- Source NAT (SNAT)
- IPsec NAT Traversal
- Bridging
- Firewall stealth mode
- OSI layer 2 firewall function
- Spanning tree
- Unlimited bridges
- Unlimited interfaces per bridge

Services
- Event notification & handling
- HTTPS (network time protocol)
- DHCP server
- SMTP/POP server
- DynDNS

Logs and Reports
- Customizable real-time dashboard
- Live log viewer (AJAX-based)
- Detailed user-based web access report
- System/Network monitoring statistics
- Rule-based logging settings (Firewall rules)
- Skylog: 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

Hardware Specification
- 1 x 10/100/1000 Base-T Ethernet LAN
- 2 x USB
- RS232/422/485
- microSD 4GB

Physical and Power
- DIN rail/wall mount (optional/desk top)
- Fanless
- Dimension (H X W X D): 110 x 25.4 x 100mm
- Weight (G.W): 0.51 Kg
- IP30
- DC Jack/terminal block, 24V DC

Environmental Specification
- Operating temperature: 0°C ~ 60°C (32°F ~ 140°F)
- Storage temperature: -20°C ~ 70°C (-4°F ~ 158°F)
- Humidity: 10% ~ 90%, non-condensing

Certification
- Safety: UL 508
- FCC/CE/ROHS

Package Content
- IFA 1610 (P/N: 10IF0161000X0)
- Qty 1 x 1
- Power input 5.08mm terminal block x 1

Ordering Information
- IFA 1610 (P/N: 10IF0161000X0)

Industry firewall 2 ports VPN router (3 years service & maintenance)
IFA 2610

CoreFort™ Industry Firewall, 3 Ports VPN Router with Rugged Design

Main Features
- Stateful (L4) packet firewall
- Intrusion prevention (IPS)
- SSL/VPN secure remote access
- D/DO support
- Serial gateway (RS485)
- Versatile logging & report system

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) 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.

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
- SN/DPSP support
- Portscan detection
- DoS and DoS protection
- SYN/ICMP flood protection
- DoS and DDoS protection
- Portscan detection
- VoIP/SIP support
- SNMP support (V1/V2/V3)
- Multiple public IPs
- Intrusion detection/prevention (IDS/IPS)
- Stateful (L4) packet firewall
- Firewall stealth mode
- QoS layer 2 firewall function
- Spanning tree
- Unlimited bridges
- Unlimited interfaces per bridge
- IPsec NAT Traversal

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
- QoS layer 2 firewall function
- Spanning tree
- Unlimited bridges
- Unlimited interfaces per bridge

VPN (Virtual Private Network)
- IPsec
- Encryption: AES 128/192/256-BC, CAST5, Blowfish
- Authentication: Pre-shared key, X.509 certificates, certificate authority
- Support for VPN over HTTP/HTTPS proxy
- PPTP pass-through
- VPN: client-to-site
- VPN: client-for-Microsoft Windows, Mac OS X and Linux
- Multiple logins per user
- VPN Failover
- SSL/TLS VPN (OpenVPN)
- True SSL/TLS VPN (OpenVPN)
- Authentication: Pre-shared key, RSA keys X.509-certificates
- Encryption: 3DES, AES 128/256-bit, MD5, SHA1
- Compression
- PFS (perfect forward secrecy)
- DPD (dead peer detection)
- Authentication: Pre-shared key, X.509 certificates
- Encryption: DES, 3DES, AES 128/192/256-bit, CAST5, Blowfish
- Authentication: Pre-shared key, X.509 certificates, certificate authority, and local
- Support for VPN over HTTP/HTTPS proxy
- PPTP pass-through
- VPN: client-to-site
- VPN: client-for-Microsoft Windows, Mac OS X and Linux
- Multiple logins per user
- VPN Failover

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
- 2 x 10/100/1000 Base-T Ethernet LAN
- 1 x USB
- 1 x DVI
- RS-232/422/485
- microSD 4GB

Physical and Power
- DIN rail/wall mount (optional)
- Fanless
- Dimension (H x W x D): 167 x 59 x 140 mm
- Weight (G. W. Kg): 1.16 Kg
- IP30
- Terminal block, 2-4 V DC

Environmental Specification
- Operating temperature: 0°C ~ 60°C (32°F ~ 140°F)
- Storage temperature: -20°C ~ 70°C (-4°F ~ 158°F)
- Humidity: 5% ~ 95%, non-condensing

Certification
- Safety: UL 508
- FCC/UL/CE

Package Content
- IFA 2610 x 1
- QRC x 1
- Power input 5.08mm terminal block x 1
- DVI terminal block x 1

Ordering Information
- IFA 2610 (P/N: 10IF0261000X0)
- Industry firewall 3 ports VPN router (3 years service & maintenance)
### Product Overview

The CoreF\textsuperscript{TM} 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/DDoS/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 CoreF\textsuperscript{TM} 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 CoreF\textsuperscript{TM} 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)
- VPP/PPPOE support
- Portscan detection
- Out and Bots protection
- SYN/ICMP flood protection
- DIO, DND, DSR protection
- DNS/SMTP/POP3/IMAP 587

**Main Features**
- Stateful (L4) packet firewall
- Network address translation (NAT)
- Stateful firewall
- Port scan
- Stateful routing
- MAC address filtering
- Source routing
- Dynamic DNS
- Network address translation (NAT)
- PAT
- IP filtering
- Quality of Service (QoS)
- Traffic shaping
- Traffic management
- Policy-based routing
- Destination-based routing
- Source-based routing
- Static routes
- Source-based routing
- Destination-based routing
- Policy-based routing (based on interface, MAC, protocol, or port)

**Network Address Translation**
- Network address translation (NAT)
- Source NAT (SNAT)
- IPsec NAT TRaversal

**High Availability**
- Hot stand-by (active/active)
- Node data/configuration synchronization

**Bridging**
- Firewall Stealth Mode
- OS layer 2 firewall function
- Spawning tree
- Unlimited bridges
- Unlimited interfaces per bridge

**VPN (Virtual Private Network)**
- IPsec
- Authentication: Pre-shared key, X.509-certificates, certificate authority, and local
- Support for VPN over HTTPS proxy (OpenVPN)
- Port tunneling
- VPN: site-to-site
- 3DES, AES 192/256-bit, CAST5, Blowfish

**Logs and Reports**
- Customizable real-time dashboard
- Live Log Viewer (AJAX based)
- Customizable real-time dashboard
- Live Log Viewer (AJAX based)
- Detailed user based web access report
- Authentication: Pre-shared key, X.509-certificates, certificate authority, and local
- Support for VPN over HTTPS proxy (OpenVPN)
- Port tunneling
- VPN: site-to-site
- 3DES, AES 192/256-bit, CAST5, Blowfish

**Network Address Translation**
- Network address translation (NAT)
- Source NAT (SNAT)
- IPsec NAT TRaversal

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

**Physical and Power**
- Fanless
- Dimensions: 167mm x 59mm x 140mm
- Humidity: 5% - 95%, non-condensing

**Certification**
- FCC/CE/RoHS
- UL 508
- UL 60950

**Software**
- Original software: CoreF\textsuperscript{TM} industry firewall 5 ports VPN router (3 years service & maintenance)

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

**Certification**
- Safety: UL 508
- FCC/CE/RoHS

**Package Content**
- CoreF\textsuperscript{TM} industry firewall 5 ports VPN router (3 years service & maintenance)

**Ordering Information**
- CoreF\textsuperscript{TM} industry firewall 5 ports VPN router (3 years service & maintenance)
CorelFort™ VPN Dispatcher 25/100 Licenses

Main Features
- Fully-integrated VPN server
- Stateful (L4) packet firewall
- SSL VPN secure remote access

Specifications
- Network Security
  - Stateful packet firewall
  - Intrusion detection/prevention (IDS/IPS)
  - Multiple public IPs
  - SNMP-support (V1/V2/V3)
  - VRRP support
  - Port scan detection
  - DoS and DDoS 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
    - One-to-one NAT
    - Source NAT (SNAT)
    - IPSec NAT traversal
  - High Availability
    - Hot standby (active/passive)
    - Node data/configuration synchronization
  - Bridging
    - Firewall stealth mode
    - O/S Layer 2 firewall function
    - Spanning tree
    - Unlimited bridges
    - Unlimited interfaces per bridge
  - VPN (Virtual Private Network)
    - IPsec
      - Encryption: DES, 3DES, AES 128/192/256-SAC, CAST5, blowfish
      - Authentication: Pre-shared key, X.509-certificates, certificate authority, and local
      - Support for VPN over HTTP(S) proxy (openVPN)
      - PPTP pass through
      - VPN: client-to-site (road warrior)
      - VPN: client for Mac OS X and Linux
      - Multiple logins per user
      - PFS (perfect forward secrecy)
      - IPSec NAT traversal
      - Compression
      - RR (Round robin)
      - Certificate-based authentication
      - IP (Internet protocol)
    - IKEv1
      - Encryption: 3DES, AES 128/192/256-SAC, CAST5, blowfish
      - Authentication: Pre-shared key, X.509-certificates, certificate authority, and local
      - Support for VPN over HTTP(S) proxy (openVPN)
      - PPTP pass through
      - VPN: client-to-site (road warrior)
      - VPN: client for Mac OS X and Linux
      - Multiple logins per user
      - PFS (perfect forward secrecy)
      - IPSec NAT traversal
      - Compression
      - RR (Round robin)
      - Certificate-based authentication
      - IP (Internet protocol)

Product Overview
With the CorelFort™ VPN Dispatcher, users can define and manage network connections with extreme flexibility, adapting them to suit the specific needs, like creating 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)
  - Multiple public IPs
  - SNMP-support (V1/V2/V3)
  - VRRP support
  - Port scan detection
  - DoS and DDoS 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
  - One-to-one NAT
  - Source NAT (SNAT)
  - IPSec NAT traversal
- High Availability
  - Hot standby (active/passive)
  - Node data/configuration synchronization
- Bridging
  - Firewall stealth mode
  - O/S Layer 2 firewall function
  - Spanning tree
  - Unlimited bridges
  - Unlimited interfaces per bridge
- VPN (Virtual Private Network)
  - IPsec
    - Encryption: DES, 3DES, AES 128/192/256-SAC, CAST5, blowfish
    - Authentication: Pre-shared key, X.509-certificates, certificate authority, and local
    - Support for VPN over HTTP(S) proxy (openVPN)
    - PPTP pass through
    - VPN: client-to-site (road warrior)
    - VPN: client for Mac OS X and Linux
    - Multiple logins per user
    - PFS (perfect forward secrecy)
    - IPSec NAT traversal
    - Compression
    - RR (Round robin)
    - Certificate-based authentication
    - IP (Internet protocol)
  - IKEv1
    - Encryption: 3DES, AES 128/192/256-SAC, CAST5, blowfish
    - Authentication: Pre-shared key, X.509-certificates, certificate authority, and local
    - Support for VPN over HTTP(S) proxy (openVPN)
    - PPTP pass through
    - VPN: client-to-site (road warrior)
    - VPN: client for Mac OS X and Linux
    - Multiple logins per user
    - PFS (perfect forward secrecy)
    - IPSec NAT traversal
    - Compression
    - RR (Round robin)
    - Certificate-based authentication
    - IP (Internet protocol)
iNAS 330

CoreVault™ Rugged-Design Industry Storage

Main Features
- 2 Gigabit Ethernet ports for data/power redundancy with PoE+
- Data protection in harsh environments
- Fully compliant with EN50155 (railway applications), EN61373 (vibrations & shocks)
- Wide temperature range support: -40°C ~70°C
- IP rating: IP 54 (NEMA)
- Max capacity: Up to 37

Specifications

Hardware Features
- Computer
  - Processor: Dual Cortex-A9 CPU
  - Storage: Up to 3 x 2.5" HDD/SSD
  - On board SSD storage
  - Storage buffer available for anytime status
- Ethernet
  - 2 x Gigabit LAN ports for data redundancy (M12)
  - 1 x Gigabit LAN port for management (M12)
- Button
  - Reset button: Reset to factory default
  - (Pressing and holding the button for 5 seconds will reset to factory default)
- LEDs
  - Power LED: power On/Off
  - System LED: system status
  - PoE/Temp LED: PoE/Temp status
  - HDD LED: HDD1, HDD2,HDD3 (read/write/empty)
  - LAN LED: 10/100/1000M x 3 (status)

Power Requirements
- Input: PoE (IEEE 802.3af), or PoE+ (IEEE 802.3at)
- Power redundancy

HS Control
- Smart heating system

Physical Characteristics
- Fanless
- Housing: metal, IP 54 protection
- Mounting: wall mount (optional)

Environmental Specification
- Operating temperature: -40°C ~ 70°C (-40°F ~ 158°F) For SSD
- -25°C ~ +55°C (-13°F ~ +131°F) For HDD
- Storage temperature: -40°C ~ 85°C (-40°F ~ 176°F)
- Humidity: 5% ~ 95%, non-condensing

Certifications
- FCC/CE
- RoHS/IEC

Compliance
- EN50155 (railway applications)
- IEC61373 (vibrations & shocks)
- EN60950; EN61000 (immunity, emission)

Package Content
- iNAS 330 unit x 1
- QIG x 1
- CD x 1

Optional Accessories
- Wall-mount-kit: 2 extra brackets and screws
- M12 cables: waterproof 8pin male M12 to RJ45 gigabit Ethernet cable, rated IP 54

System Dimensions
- 256mm (w) x 174mm (D) x 60mm (H) (9.69” x 7.64” x 2.36”)

Software Features
- OS: Linux
- Firmware upgrade via system web UI
- System management via management web UI
- RAID management: RAID 0,1,5,JBOD
- IP Settings: fixed IP, DHCP
- Auto data rebuilding
- Remote backup

Ordering Information
- iNAS 330 (P/N: 101G0033000X0)
  - Rugged-design industry storage (5 years service & maintenance)

Product Overview
The iNAS 330 is an extremely rugged-design network-attached storage (NAD), which was designed to provide high performance, reliability and capacity data storage in harsh environments. Equipped with a unique storage technology, it is able to record the accurate data in harsh environments, such as Oil & Gas, Transportation, and Industrial automation… and so on.

Furthermore, it offers various data backup options. Remote replication supports data backup from target unit to another remote unit, FTP servers and file-level synchronization. By integrated with sftc protocol, it’s able to keep critical data always consistent. Also, it supports SMB/CIFS, NFS, and AFP protocols for file sharing among cross-platforms such as Windows, Mac and Linux/UNIX.

The iNAS 330 supports Power over Ethernet (PoE/PoE+) and following the specifications in IEEE 802.3af/IEEE 802.3at. It’s has dual PoE+ interfaces which could support power redundancy. In addition, iNAS 330 could be used on video recording system widely which supports RAID 5 function and also offers the data protection. The iNAS 330 was built with a fanless, thermally efficient, dust- and water-protected IP 54-rated chassis. It’s sealed enclosure eliminates internal fans as a point of critical system failure, protecting the internals.

Web Browsers Support
- Internet Explorer 9.0 later
- Mozilla Firefox
- Apple Safari
- Google Chrome

Networking
- HTTP/HTTPS, Samba/CIFS, NFSv4, AFPv3.3, SNMPv3, FTP, TLS 1.0, TLS 1.2(TCP/IP)+IP(v6),IEEE 802.3x

Backup management
- Green power management
- Data protection (Support data buffer available for vibration status and harsh temperature environment)

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

Building a Secure, Reliable I4.0 Connectivity Framework

A complete Industry 4.0 wireless solution consists of a 3-layer integration of enterprise information technology (IT), communication technology (CT) and operational technology (OT) networks, 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 reliability required for a dedicated, always-on industrial Wi-Fi network.
- 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 and operational technology (OT), communication technology (CT) and operational technology (OT) networks, and fulfills the following requirements:
- 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’s 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’s nCare manager.

Figure 1. NEXCOM’s wireless solution competence.

Figure 2. A digital factory implementing NEXCOM’s complete I4.0 wireless solution.

Figure 3. NEXCOM’s Industry 4.0 Wi-Fi complete solution.
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 can 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.
- The close distance between the ground surface and AGV often blocks the coverage of Wi-Fi signal.

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 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 hazardous environments.

Application Challenge
- The connectivity of Wi-Fi gateways is crucial for the integration of devices with different protocols, ensuring that all devices are connected to the central management system.

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 unmanned 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 (PMP) 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
- EZ Mesh technology enables simple and flexible deployment of mesh backbone networks.
- nCare software support for remote management and monitoring of the network and devices in the wireless video surveillance system.

Plant Floor Monitoring

Whether it is predictive maintenance or production optimization, the smart factory of IIoT 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.
- nCare software support for remote management and device health monitoring.

Figure 7. Plant floor monitoring system layout.
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 diverse devices:

- 3rd Party Management
- Modbus/Xcare/MQTT/MS WMI
- Meter
- Pump
- Air Compressor
- PLC
- Network Router
- AP/Mesh/P2MP/Securiy Wi-Fi

Features & Benefits

nCare has been specifically designed with I-4.0 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. Protocols such as SNMP, CAPWAP and LLDP are supported to interface with third-party network devices with different levels of administration to delegate tasks between nCare and third-party AAA systems. 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
- nCare supports a variety of industrial fieldbus protocols such as NEXCOM Xcare™, Modbus TCP, MQTT and transparent tunneling protocols to provide management for a wide range of field devices (Figure 7).
- 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).
IWF 800 nCare

Main Features
- Automatically discover managed devices by SNMP, CAPWAP & Modbus scan.
- Visual topology to display device and wireless link status for remote management.
- Support to Modbus TCP protocol to communicate with Modbus device to manage its network and device.
- 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 Modbus TCP scan.
- SNMP supports v1/v2c & v3.
- NEXCOM & Rogue AP detection.
- Auto discovery supports Modbus TCP scan.
- SNMP supports v1/v2c & v3.

Product Overview
Nowadays, lots of production data or device information need 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

Operating System
- Windows 7
- VM supported by project base

Hardware
- CPU Support: Intel® Atom™ processor C2558/4 cores 2.4GHz
- Main Memory: 8GB memory with DDR3 1600MHz Long-DIMM sockets
- Ethernet Speed: Giga Ethernet
- I/O Interface-Front
  - 2 x USB 2.0 ports
  - 1 x RJ45 type console port
  - 4 x copper ports
- I/O Interface-Rear
  - 2 x USB 2.0 ports
  - 1 x VGA port
- HDD Storage: 500GB

Software
- Auto Discovery
  - CAPWAP (RFC3568 & RFC5415), LLDP & SNMP
  - Auto discovery supports Modbus TCP scan
- SNMP supports v1/v2c & v3

Ordering Information
- IWF 800 nCare, I4.0 Node and Network Manager
(P/N: 10T0NCARED0X10)

- Remote device control: reboot, watchdog enable/disable
- Customized service for customer owned device asset management
  - Report & Log: Asset status
    - Export (Excel, csv and txt file)
    - System log
    - Usage report (traffic, usage, device)
  - Event Notification: Event trigger
    - Pre-defined event list
    - Link up
    - Link down
    - Generic trap rules
    - Outbound notice
    - Email
    - SMS
    - Social media (Line, WeChat, Facebook, Twitter)
  - Administration: Authority (Default: admin, manager, user) by username/password
    - Concurrent user: 5
    - Scale-up (additional license key is required) to 6,000 nodes

- Mechanical
  - Chassis Dimension: 430mm x 260mm x 44mm
- Weight:
  - Without packing: 5kg
  - With packing: 7kg
- System
  - Environment
    - Operating temperature: 0°C~40°C
    - Storage temperature: -20°C~75°C
    - Relative humidity: 10%~90% non-condensing
  - Certifications: CE/FCC

- Remote device control: reboot, watchdog enable/disable
- Customized service for customer owned device asset management
- Report & Log: Asset status
- Event Notification: Event trigger
- Administration: Authority (Default: admin, manager, user) by username/password
- Scale-up (additional license key is required) to 6,000 nodes

- Mechanical
- System

- Environmental

- Order: CE/FCC

- Monitoring: Historically (HDD life, CPU/memory usage, temperature, etc.) Condition and provisioning

- Interface: Modbus TCP/RTU/ASCII, NEXCOM Xcare, WMI (Windows Management Interface)*

- Device management
  - Support device protocol: Modbus TCP/RTU/ASCII, NEXCOM Xcare, WMI (Windows Management Interface)*
  - Remote device threshold setting and provisioning

- Network
  - Operating temperatures: 0°C~40°C
  - Storage temperatures: -20°C~75°C
  - Relative humidity: 10%~90% non-condensing
  - Certifications: CE/FCC

- Network

- Environment

- Order: CE/FCC
Trustworthy 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 interference 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 either dual link reroute to the most optimal network path, ensuring that data is reliably delivered.

NEXCOM’s mesh technology will adapt and route to the most optimal network path, ensuring that data is reliably delivered to the central office.

The dual radio design offers either dual link reroute to the most optimal network path, ensuring that data is reliably delivered.

**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 inter-plant communication and high-speed vehicle communication. All industrial wireless products in EZ Mesh and Mobile Mesh are supported by NEXCOM 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 802.11n MIMO Technology with the capability to sustain up to 33Mbps 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 300 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 traveling <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. NEXCOM’s EZ Mesh provides multiple paths for highest link reliability, which results in the lowest amount of packet loss.

Figure 3. 4-device mesh network in 160m² 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.
Industrial Network and Cloud Product Selection Guide

Mobile Mesh AP 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. In addition, the M series of the Mobile Mesh family offers fast wireless roaming speed of 20ms, enabling smooth data transmission for applications requiring low latency such as video images and high-speed vehicles traveling up to 120km/h. Coupled with IP67 protection and high-power RF design, Mobile Mesh delivers high reliability in tough, outdoor environments.

NEXCOM’s Mobile Mesh family includes a complete range of outdoor Wi-Fi and industrial Wi-Fi solutions. The IWF 6320 and IWF 6330 outdoor Wi-Fi APs 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. For example, the Wi-Fi APs can be used to build a wireless mesh network with fast roaming speeds for railway vehicles, offering passengers seamless on-train Wi-Fi roaming service.

Mobile Mesh Highlights
- Easy installation & scalability for large-scale deployment
- Multi-path bridge
- Self-forming and Self-healing
- 1200Mpbs bandwidth capacity after 10+ hops
- Fast roaming speed of 20ms
- Support Mesh/AP/Bridge modes
- IP67, high-power and Dual/Triple RF design

Mobile Mesh Application in Outdoor Environments

The IWF 6320 series of the Mobile Mesh family offers a Mesh/Mapping 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.

NEXCOM’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.
- NEXCOM’s proprietary security technology and self-forming/healing capability enable deployment of a trusted and secure Wi-Fi mesh network with path redundancy.

Figure 7. Mobile Mesh outdoor application scenario.

Product Selection Guide

<table>
<thead>
<tr>
<th>Model Name</th>
<th>EZ Mesh Family</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>IWF 300</td>
<td>IWF 310</td>
<td>IWF 6320M/H</td>
<td>IWF 6330M/H</td>
<td>IWF 3310XM/H</td>
</tr>
<tr>
<td>Category</td>
<td>Industrial</td>
<td>EZ Mesh AP</td>
<td>Rugged/Industrial</td>
<td>Outdoor Mobile Mesh AP</td>
<td>Outdoor Mobile Mesh AP</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>
</tr>
<tr>
<td>Number of Radios</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Number of Antennas</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>2</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>
</tr>
<tr>
<td>Number of WAN Port</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Number of LAN Ports</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Type of LAN</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45 (Encapsulated by M25)</td>
<td>RJ45 (Encapsulated by M25)</td>
<td>RJ45</td>
</tr>
<tr>
<td>IP Rating</td>
<td>IP30</td>
<td>IP30</td>
<td>IP67</td>
<td>IP67</td>
<td>IP30</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>
</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>
</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>
</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>
</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>
</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>
</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>
</tr>
<tr>
<td>Operation Mode</td>
<td>AP/Router/EZ Mesh</td>
<td>AP/Router/EZ Mesh</td>
<td>AP/Station/Mesh* (*Mesh Model Only)</td>
<td>AP/Station/Mesh* (*Mesh Model Only)</td>
<td>AP/Station/Mesh* (*Mesh Model Only)</td>
</tr>
<tr>
<td>Management Mode</td>
<td>NEXCOM nCare Management</td>
<td>NEXCOM nCare Management</td>
<td>NEXCOM nCare Management</td>
<td>NEXCOM nCare Management</td>
<td>NEXCOM nCare Management</td>
</tr>
</tbody>
</table>
**IWF 300**

**Main Features**
- Dual radios and compliant with 1x IEEE 802.11a/n and 1x IEEE 802.11 b/g/n 2x2 MIMO
- 1+4 port RJ45/RS4 ports
- Up to 27dBm high RF power

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

**Frequency Ranges**
- USA: 2.400–2.483 GHz, 5.15–5.35 GHz, 5.5–5.7 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, 5.725–5.85 GHz

**RF Output Power:**
- **IEEE802.11a**
  - 12dBm@5GHz
  - 12dBm@2.4GHz
  - 11dBm@HT40
  - 11dBm@HT20
- **IEEE802.11n**
  - 27dBm@1M
  - 24dBm@11M
  - 24dBm@54M
  - 24dBm@HT40
  - 23dBm@HT20
  - 19dBm@HT52/15
  - 18dBm@MC57/15
- **IEEE802.11ac**
  - 76dBm@5GHz
  - 74dBm@MC57
  - 71dBm@MC57

**Receive Sensitivity:**
- **IEEE802.11a**
  - -76dBm@5GHz
  - -74dBm@HT20
  - -71dBm@MC57
- **IEEE802.11n**
  - -93dBm@1M
  - -91dBm@11M
  - -94dBm@6M
  - -80dBm@5GHz
  - -94dBm@MC57/8
  - -77dBm@MC57/15
  - -92dBm@HT40
  - -69dBm@MC57/8
  - -73dBm@MC57/15

**Hardware**
- WAN: 1G/10/100 Base-TX/MDIX/MDIX RJ-45 x 1
- LAN: 10/100/1000 Base-TX MDIX/MDIX RJ-45 x 4
- Compliant with:
  - IEEE802.3/802.3u

**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
- Note: The available RF output power will be given by certified power in different region

**Ordering Information**
- IWF 300-EU (P/N: 10T00030000X0)
- IWF 300-US (P/N: 10T00030001X0)
IWF 310

Main Features
- Dual radios and compliant with 1x 802.11an + 1x 802.11 b/g/n 2x2 MIMO
- 1x4 port CAT 5e RJ-45 ports
- Up to 27dBm high RF power
- Multiple functions: AP/Router/EZ Mesh
- Support 12V DC input
- Support -40 ~ 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 IEEE802.11a/n 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
- IEEE802.11a
  - 2412MHz-2462MHz
- IEEE802.11b
  - 2412MHz-2472MHz
- IEEE802.11g
  - 2412MHz-2462MHz
- IEEE802.11n
  - 2412MHz-2462MHz
- IEEE802.11ac
  - 5.15 ~ 5.35 GHz, 5.725 ~ 5.825 GHz
- IEEE802.11ad
  - 5.725 ~ 5.825 GHz

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, 5.725 ~ 5.825 GHz
- Japan: 2.400 ~ 2.497 GHz, 5.15 ~ 5.35 GHz, 5.725 ~ 5.825 GHz
- China: 2.400 ~ 2.483 GHz, 5.725 ~ 5.85 GHz

RF Output Power: IEEE 802.11an (±2dBm)
- IEEE802.11n
  - 12dBm@5G4M
  - 11dBm@HT80
  - 12dBm@HT40
  - 11dBm@HT80

RF Output Power: IEEE 802.11 b/g/n (±2dBm)
- IEEE802.11b
  - 27dBm@1M
  - 24dBm@11M
- IEEE802.11g
  - 27dBm@1M
  - 24dBm@54M
- IEEE802.11n
  - 27dBm@1M
  - 24dBm@54M
- IEEE802.11ac
  - 71dBm@HT40

Receive Sensitivity: IEEE 802.11an
- IEEE802.11a
  - -76dBm@54M
  - -74dBm@HT20
  - -71dBm@HT40
- IEEE802.11n
  - -76dBm@5G4M
  - -74dBm@HT20
  - -71dBm@HT40
  - -71dBm@HT80

Receive Sensitivity: IEEE 802.11 b/g/n
- IEEE802.11b
  - -93dBm@1M
  - -91dBm@11M
- IEEE802.11g
  - -94dBm@5M4M
  - -80dBm@5G4M
- IEEE802.11n
  - -94dBm@64M
  - -80dBm@64M
- IEEE802.11ac
  - -94dBm@HT20
  - -71dBm@HT40
  - -71dBm@HT80
  - -71dBm@HT160

Hardware
- WAN: 10/100/1000 Base-TX MDI/MDIX RJ-45 x 1
- LAN: 10/100/1000 Base-TX MDI/MDIX RJ-45 x 4
- Compliant with:
  - IEEE802.3 / 802.3u
  - Hardware based 10/100/1000, full/half, flow control auto negotiation
  - Push button: 1x Reset
  - LED: 1x power status, 5x Ethernet
  - Antenna connectors: 2x with RP-SMA

Operating Mode
- AP
- AP router
- Client router
- EZ mesh

Security
- WEP (64/128)
- WPA/WPA2 Mixed
- WPA2-personal (PSK+COM+AES)
- Hidden ESSID support
- MAC address filtering (MAC ACL)

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

Built-in Servers & Client Interfaces to Other Services
- DHCP client
- SNMP V1/V2c (Coming Soon)

Physical and Power
- 12VDC power input with DC jack
- Wall mountable
- Dimension: 185 x 108 x 43 mm

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

Certification
- CE
- RoHS compliant
- EN50155 compliant

Package Contents
- IWF310 unit x 1
- Antenna x 2
- Ethernet cable x 1
- Wall mount kit x 1
- AC-DC power adapter x 1

IWF 310 is designed with Aluminum and Metal Chassis and complies with IEEE802.11b/g/n and IEEE802.11a/n 2x2 MIMO technology. It can deliver a data rate up to 300Mbps/each radio. With up to 27dBm high RF power, it can provide extensive coverage and service. IWF 310 also functions as an EZ Mesh network Wi-Fi access point with a cost-effective option.
**Product Overview**

The IWF 6300/6330 series are enterprise and carrier grade 802.11n Triple Radios Outdoor Wireless Access Point which offers customer a robust, high performing solution for wireless networking, Mesh/Mobility WiFi applications in both license-free 2.4GHz and 5GHz bands. The IWF 6300/6330 series are the most ideal candidate for Service Providers looking to deliver carrier-grade wireless services to multiple market segments performing solution for PTP/PTMP/Hotzone/Hopping/Mesh/Mobility Wi-Fi applications in both license-free 2.4GHz and 5GHz bands. Designed to meet customer needs in a broad range of industries, the IWF 6302/6330 offers the following benefits:

**Flexible wireless backbone deployment options**

Multiple wireless interfaces were integrated by NEXCOM core data switching technology inside the IWF 6330 series. Each radio interface can be configured independently to reconfigure wireless connectivity. With the fast data switching between multiple radio interfaces, the backbone throughput will remain in a high level even after several reconfigurations between AP's.

**High-performance wireless backbone**

With the next generation 802.11n MIMO technology, the IWF 6300s/6330s offer data link rate up to 300Mbps in each single radio interface. Short Guard Interval and Frames Aggregation methodology configurations improve the efficient of backbone usage.

**IWF 6300/6330 Series Category**

<table>
<thead>
<tr>
<th>Model</th>
<th>Radio Spec</th>
<th>P/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>IWF 6320H</td>
<td>Hopping AP, Dual Radios, IEEE 802.11 a/b/g/n Dual Band 2x2 MIMO, High Power</td>
<td>(P/N: 10T00632002X0)</td>
</tr>
<tr>
<td>IWF 6320M</td>
<td>Mesh/Mobility AP, Dual Radios, IEEE 802.11 a/b/g/n Dual Band 2x2 MIMO, High Power</td>
<td>(P/N: 10T00632003X0)</td>
</tr>
<tr>
<td>IWF 6330H</td>
<td>Hopping AP, Triple radios, IEEE 802.11 a/b/g/n Dual Band 2x2 MIMO, High Power</td>
<td>(P/N: 10T00633002X0)</td>
</tr>
<tr>
<td>IWF 6330M</td>
<td>Mesh/Mobility AP, Triple Radios, IEEE 802.11 a/b/g/n Dual Band 2x2 MIMO, High Power</td>
<td>(P/N: 10T00633003X0)</td>
</tr>
</tbody>
</table>

**Specifications**

- **Wireless Radio**: 2 x 2 MIMO radios
- **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 – 5.835 GHz
- **IEEE 802.11g**
  - 26dBm (EM) (all)
  - 22dBm (54M) (all)
  - 17dBm (11M) (all)
  - 14.5dBm (54M) (all)
  - 11.5dBm (54M) (all)
- **IEEE 802.11a HT20**
  - 24dBm (6/10/14MHz) (all)
  - 20.5dBm (54/65MHz) (all)
- **IEEE 802.11g HT20**
  - 24dBm (6/10/14MHz) (all)
  - 20.5dBm (54/65MHz) (all)
  - 21dBm (20/54MHz) (all)
- **IEEE 802.11n HT40**
  - 24dBm (54/108MHz) (all)
  - 20.5dBm (54/108MHz) (all)
- **Receive Sensitivity**
  - IEEE 802.11a
    - -82dBm @ 6M (all)
    - -79dBm @ 11M (all)
  - IEEE 802.11g
    - -82dBm @ 6M (all)
    - -79dBm @ 11M (all)
  - IEEE 802.11n
    - -82dBm @ 6M (all)
    - -79dBm @ 11M (all)

**Ordering Information**

- IWF 6320M-HE (P/N: 10T00632002X0)
- IWF 6320M-EU (P/N: 10T00632003X0)
- IWF 6320M-UK (P/N: 10T00632004X0)
- IWF 6320M-AU (P/N: 10T00632005X0)
- IWF 6320M-CA (P/N: 10T00632006X0)
- IWF 6320M-IN (P/N: 10T00632007X0)
- IWF 6320M-JP (P/N: 10T00632008X0)
- IWF 6320M-MX (P/N: 10T00632009X0)
- IWF 6320M-ZA (P/N: 10T00632010X0)
- IWF 6320M-ME (P/N: 10T00632011X0)
- IWF 6320M-AF (P/N: 10T00632012X0)

**IWF 6330 Series**

- **IEEE 802.11g**
  - -25dBm (EM) (all)
  - -22dBm (54M) (all)
  - -20.5dBm (148MHz) (all)
  - -17dBm (152MHz) (all)
  - -14.5dBm (156MHz) (all)
- **IEEE 802.11a HT20**
  - -24dBm (6/10/14MHz) (all)
  - -20.5dBm (54/65MHz) (all)
- **IEEE 802.11g HT20**
  - -24dBm (6/10/14MHz) (all)
  - -20.5dBm (54/65MHz) (all)
  - -21dBm (20/54MHz) (all)
- **IEEE 802.11n HT40**
  - -24dBm (54/108MHz) (all)
  - -20.5dBm (54/108MHz) (all)

**Features**

- Multiple radios and compliant with IEEE 802.11b/g/n/5 GHz
- Fast roaming (hand-over switch time less than 20 ms)
- Smart installation utilities: distance calculation, antenna alignment and site survey tools
- 48VDC PoE input
- Gigabit Ethernet waterproof RJ45
- IEEE 802.11a
  - -85dBm @ 6M (all)
  - -82dBm @ 11M (all)
  - -79dBm @ 14M (all)
  - -77dBm @ 18M (all)
  - -63dBm @ 24M (all)
- IEEE 802.11g
  - -85dBm @ 6M (all)
  - -82dBm @ 11M (all)
  - -79dBm @ 14M (all)
  - -77dBm @ 18M (all)
  - -63dBm @ 24M (all)
- IEEE 802.11n
  - -85dBm @ 6M (all)
  - -82dBm @ 11M (all)
  - -79dBm @ 14M (all)
  - -77dBm @ 18M (all)
  - -63dBm @ 24M (all)

**Main Features**

- 802.11n MIMO technology
- The IWF 6320/6330 offer data link rate up to 300Mbps in each single radio interface.
- Short Guard Interval and Frames Aggregation methodology configurations improve the efficient of backbone usage.
- Multiple radio interfaces were integrated by NEXCOM core data switching technology inside the IWF 6330 series. Each radio interface can be configured independently to reconfigure wireless connectivity. With the fast data switching between multiple radio interfaces, the backbone throughput will remain in a high level even after several reconfigurations between AP's.
- **High-performance wireless backbone**

**Utilization**

- IP Fast path
- RSSI and Path loss Calculation
- Wireless Site survey
- Antenna Alignment Tool
- System Status
- Link Information

**Advanced Technology**

- Multiple handing (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: Pole/Wall mountable
- Dimensions: 220 x 220 x 77mm
- Weight: 2.8kg (3.7kg with rail kit included)
- Outdoor IP67 rated
**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
- Single 2 x 2 MIMO radio
- IEEE 802.3at Power over Ethernet
- Gigabit Ethernet RJ45
- IEEE 802.1X/RADIUS, TKIP and AES
- Operating temperature range from -40 to 80°C
- FCC/CE certification
- EN50155 compliant
- IEEE 802.1p VLAN Priority Based QoS
- IEEE 802.1q Tag VLAN
- IEEE 802.1v VLAN Priority Based QoS

**Product Overview**
The IWF 3310X series are enterprise and carrier grade 802.11n Industrial Wireless Access Point which offers customer a robust and high performing solution for PTP/PTMP/Hotzone applications in both license-free 2.4GHz and 5GHz bands.

**IWF 3310X Series Category**

<table>
<thead>
<tr>
<th>Model</th>
<th>Radio Spec.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IWF 3310XH</td>
<td>Hopping AP/CPE, IEEE 802.11 a/b/g/n Dual-Band 2x2 MIMO</td>
</tr>
<tr>
<td>IWF 3310XM</td>
<td>Mesh/Mobility AP/CPE, IEEE 802.11 a/b/g/n Dual-Band 2x2 MIMO</td>
</tr>
</tbody>
</table>

**Specifications**

**Wireless Radio**
- Single 2 x 2 MIMO radio
- IEEE 802.11a
  - 21dBm@64M
  - 16dBm@94M
- IEEE 802.11b
  - 21dBm@11M
  - 19dBm@11M
- IEEE 802.11g
  - 23dBm@24M
  - 19dBm@54M
- IEEE 802.11n HT20/40
  - 17dBm@384M
  - 15dBm@128M
  - 14dBm@64M
- IEEE 802.11n HT40
  - 21dBm@96M
- IEEE 802.11ac
  - 21dBm@576M
  - 17dBm@384M

**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, 5.725 ~ 5.825 GHz
- Japan: 2.400 ~ 2.497 GHz, 5.15 ~ 5.35 GHz, 5.725 ~ 5.825 GHz
- China: 2.400 ~ 2.497 GHz, 5.15 ~ 5.35 GHz, 5.725 ~ 5.825 GHz

**RF output power:** (±2dBm)
- IEEE 802.11a
  - 19dBm@42M
  - 16dBm@94M
- IEEE 802.11b
  - 21dBm@11M
  - 19dBm@11M
- IEEE 802.11g
  - 23dBm@24M
  - 19dBm@54M
- IEEE 802.11n HT20/40
  - 14dBm@MS37/15
  - IEEE 802.11n HT40
  - 21dBm@MCS5/8
  - 17dBm@MCS7/15
- IEEE 802.11ac
  - 21dBm@MCS7/15
  - 17dBm@MCS5/8

**Receive Sensitivity**
- IEEE 802.11a
  - -93dBm@64M
  - -87dBm@11M
- IEEE 802.11g
  - -93dBm@64M
  - -76dBm@54M
- IEEE 802.11n HT20/40
  - -95/91dBm@MCS9/8
  - -77/73dBm@MCS7/15
- IEEE 802.11n HT40
  - -95/91dBm@MCS9/8
  - -79/75dBm@MCS7/15

**Wireless Site survey**
- RSSI and Path loss Calculation
- Ping test
- Throughput

**Advanced Technology**
- Multiple Hopping (up to 10 hops with more than 100Mbps throughput)
- Wireless Bandwidth Limitation
- Support Mobility function in IWF 6330M

**Physical and Power**
- Support 48Vdc Power over Ethernet
- Form Factor: DIN-rail and Wall-mount
- Dimensions: 139.6 x 139 x 6.17 mm
- Weight: 1.73kg
- IP30 rated

**Environment Protection**
- Operating temperature: -40°C to 80°C
- Storage temperature: -40°C to 80°C
- Humidity: 0% to 95% maximum (Non-condensing)
- Vibration: Random 0.3g

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

**Package Contents**
- IWF 3310x unit x 1
- Terminal block x 1
- Detachable Dual-Band Antenna x 2 (2.4/5GHz)
- Ethernet Cable x 1
- Wall mount kit x 1

**Ordering Information**
- IWF 3310XM-US (P/N: 10T00331003X0)
- IWF 3310XM-US (P/N: 10T00331003X0)
- IWF 3310XM-US (P/N: 10T00331003X0)
- IWF 3310XM-US (P/N: 10T00331002X0)
**NIO 50**

**Industrial Wi-Fi Serial/Ethernet Device Server**

**Main Features**
- Support transparent Modbus TCP/RTU, Modbus ASCII & MQTT
- 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 transparent Modbus TCP/RTU, Modbus ASCII & MQTT
- 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

**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**

- **CPU Support**
  - Onboard STM32F407ZE processor
- **Main Memory**
  - 512KB (embedded Flash in STM32)
- **Serial Port**
  - 1 x RS232/422/485 (software selectable)
- **Wireless**
  - Wi-Fi: 802.11 b/g/n 1x1
- **Ethernet**
  - 1 x 10/100 Base-TX
  - MDI/MDIX Auto cross
- **Reset**
  - 1 x Reset/restore to default push button
- **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

**SW Features**
- OS: FreeRTOS
- Management: nCare, Web-GUI
- Web-GUI for configuration
- Ethernet firmware upgrade
- SNTP client (real IP, static)
- Factory default/Reset (press reset button 3 seconds interval for factory default)

**Environment Protection**
- Operating temperature: -20°C~70°C
- Storage temperature: -40°C~85°C
- Relative Humidity: Operating: 5%~95%, non-condensing

**Certification**
- EMI: FCC, CE Class A
- RF:
  - FCC: PART15C
  - CE: EN 300328
- EN60950-1
- EMC: EN 301 489-1/17, FCC Part 15 Subpart B, EN 55022/55024

**Ordering Information**
- NIO 50 (P/N: 10T00005000X0)
  - Industrial Wi-Fi serial/Ethernet device server

---

---

---
Rugged & Ultra-Fast Gigabit Industrial Wi-Fi Solution for Video Surveillance

As Wi-Fi technology advances and Industry 4.0 (I4.0) gains traction, wireless 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 remote areas to central control centers.

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 1167 Mbps. Equipped with a dual radio design, the 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 500 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 500 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 from 500m to 3km (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.
- 24VDC 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:
- Waterproof 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 500 product family provides IP55-rated waterproof and dust-tight protection to withstand harsh conditions in outdoor and factory environments.
- The IWF 503 and IWF 504D offer over 1Gbps data rate with IEEE 802.11ac technology to provide large bandwidth capacity for wireless video data transmission.
- The embedded models configure differently.

Product Selection Guide

<table>
<thead>
<tr>
<th>Model Name</th>
<th>IWF 501/501D</th>
<th>IWF 502/502D</th>
<th>IWF 503/503D</th>
<th>IWF 504D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photo</td>
<td><img src="image1" alt="Photo" /></td>
<td><img src="image2" alt="Photo" /></td>
<td><img src="image3" alt="Photo" /></td>
<td><img src="image4" alt="Photo" /></td>
</tr>
<tr>
<td>Category</td>
<td>PtP/PtMP AP/CPE</td>
<td>PtP/PtMP AP/CPE</td>
<td>PtP/PtMP AP/CPE</td>
<td>PtP/PtMP AP/CPE</td>
</tr>
<tr>
<td>WLAN Standard</td>
<td>IEEE 802.11a/b/g/n</td>
<td>IEEE 802.11a/b/g/n</td>
<td>IEEE 802.11a/b/g/n</td>
<td>IEEE 802.11a/b/g/n</td>
</tr>
<tr>
<td>Number of Radios</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Number of Antenna</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Number of LAN Port</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Type of LAN</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45</td>
</tr>
<tr>
<td>IP Rating</td>
<td>IP55</td>
<td>IP55</td>
<td>IP55</td>
<td>IP55</td>
</tr>
<tr>
<td>Conformal Coating</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Mounting Style</td>
<td>Wall/Pole Mount</td>
<td>Wall/Pole Mount</td>
<td>Wall/Pole Mount</td>
<td>Wall/Pole Mount</td>
</tr>
<tr>
<td>Temperature</td>
<td>-35°C ~ +70°C</td>
<td>-35°C ~ +70°C</td>
<td>-35°C ~ +70°C</td>
<td>-35°C ~ +70°C</td>
</tr>
<tr>
<td>Dimensions</td>
<td>280 x 133 x 45</td>
<td>280 x 133 x 45</td>
<td>240 x 133 x 58</td>
<td>240 x 133 x 58</td>
</tr>
<tr>
<td>Wi-Fi Throughput</td>
<td>455 Mbps</td>
<td>455 Mbps</td>
<td>455 Mbps</td>
<td>1Gbps</td>
</tr>
<tr>
<td>Ethernet Throughput</td>
<td>1Gbps</td>
<td>1Gbps</td>
<td>1Gbps</td>
<td>1Gbps</td>
</tr>
<tr>
<td>DC Input</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Certification</td>
<td>CE, FCC</td>
<td>CE, FCC</td>
<td>CE, FCC</td>
<td>CE, FCC</td>
</tr>
<tr>
<td>Safety</td>
<td>EN60095-1</td>
<td>EN60095-1</td>
<td>EN60095-1</td>
<td>EN60095-1</td>
</tr>
<tr>
<td>Operation Mode</td>
<td>AP/Client/Router/WISP</td>
<td>AP/Client/Router/WISP</td>
<td>AP/Client/Router/WISP</td>
<td>AP/Client/Router/WISP</td>
</tr>
<tr>
<td>Management Mode</td>
<td>GUI Management</td>
<td>GUI Management</td>
<td>GUI Management</td>
<td>GUI Management</td>
</tr>
</tbody>
</table>

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.
**Product Overview**

IWF 501 series are cost effective 802.11b/g/n outdoor AP/CPE operating in 2.4GHz band. It has a built-in dual-polarity antenna or detachable SMA connectors with dual Ethernet ports. The IWF 501 series support passive 24VDC PoE allowing easy installation without any environment limitation.

**IWF 501 Series Category**

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
<th>Antenna</th>
</tr>
</thead>
<tbody>
<tr>
<td>IWF 501</td>
<td>Outdoor AP/CPE 2.4GHz 802.11 b/g/n 2x2</td>
<td>12dBi embedded antenna</td>
</tr>
<tr>
<td>IWF 501D</td>
<td>Outdoor AP/CPE 2.4GHz 802.11 b/g/n 2x2</td>
<td>2 x SMA connectors</td>
</tr>
</tbody>
</table>

**Specifications**

**Wireless Radio**
- 2 x 2 MIMO radios
- Frequency Ranges
  - USA: 2.412 ~ 2.462 GHz
  - Europe: 2.412 ~ 2.472 GHz
  - Japan: 2.412 ~ 2.484 GHz
  - China: 2.412 ~ 2.472 GHz
- RF Output Power: (± 2dBm)
  - IEEE 802.11g/n HT20: 27± 2dBm@MCS0/8, 22± 2dBm@MCS7/15
  - IEEE 802.11g/n HT40: 27± 2dBm@MCS0/8, 21± 2dBm@MCS7/15
- Receive Sensitivity
  - IEEE 802.11g: 91dBm@MCS5/8, 89dBm@MCS7/15
  - IEEE 802.11h: 91dBm@MCS5/8, 89dBm@MCS7/15

**Physical and Power**
- Support 24Vdc power over Ethernet
- Dimension: 280 x 90 x 47 mm
- Weight: 342g
- Outdoor IP55 rated

**Environment Protection**
- Operating temperature: -35°C to 75°C
- Storage temperature: -35°C to 75°C
- Humidity: 5% to 95% maximum (non-condensing)
- Vibration: random 0.3g

**Ethernet**
- 10/100 Base-TX MDI/MDIX RJ-45 x 2

---

**Main Features**
- AP/Client/Bridge/Router mode supported
- Compliant with IEEE 802.11 b/g/n 2x2 MIMO
- 240 Mbps data rate
- Fast Ethernet RJ45
- WEP, WPA, WPA2
- Operating/temperature range from -35 to 75°C
- FCC/CE certification

---

**Security**
- Hide SSID/MAC filtering
- ACL/WEP/WPA/WPA2

---

**Management**
- HTTP(s) web GUI
- Firmware upgrade
- Configuration backup and restore
- Factory default configuration
- SNMP V1/V2c

---

**Utility**
- Wireless site survey
- Link information
- Bandwidth control
- Distance adjustment
- Adjustable output power

---

**Physical and Power**
- Support 24Vdc power over Ethernet
- Dimension: 280 x 90 x 47 mm
- Weight: 342g
- Outdoor IP55 rated

---

**Environment Protection**
- Operating temperature: -35°C to 75°C
- Storage temperature: -35°C to 75°C
- Humidity: 5% to 95% maximum (non-condensing)
- Vibration: random 0.3g

---

**IWF 502 Series Category**

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
<th>Antenna</th>
</tr>
</thead>
<tbody>
<tr>
<td>IWF 502</td>
<td>Outdoor AP/CPE 5GHz 802.11 a/n 2x2</td>
<td>14dBi embedded antenna</td>
</tr>
<tr>
<td>IWF 502D</td>
<td>Outdoor AP/CPE 5GHz 802.11 a/n 2x2</td>
<td>2 x SMA connectors</td>
</tr>
</tbody>
</table>

**Specifications**

**Wireless Radio**
- 2 x 2 MIMO radios
- Frequency Ranges
  - USA: 5.15 ~ 5.25 GHz, 5.725 ~ 5.825 GHz
  - Europe: 5.15 ~ 5.17 GHz, 5.15 ~ 5.17 GHz
  - Japan: 5.15 ~ 5.17 GHz, 5.15 ~ 5.17 GHz
- RF Output Power: (± 2dBm)
  - IEEE 802.11a/n HT20: 27± 2dBm@MCS0/8, 21± 2dBm@MCS7/15
  - IEEE 802.11a/n HT40: 27± 2dBm@MCS0/8, 21± 2dBm@MCS7/15
- Receive Sensitivity
  - IEEE 802.11a/n: 91dBm@MCS5/8, 89dBm@MCS7/15
  - IEEE 802.11h: 91dBm@MCS5/8, 89dBm@MCS7/15

**Physical and Power**
- Support 24Vdc power over Ethernet
- Dimension: 280 x 90 x 47 mm
- Weight: 342g
- Outdoor IP55 rated

**Environment Protection**
- Operating temperature: -35°C to 75°C
- Storage temperature: -35°C to 75°C
- Humidity: 5% to 95% maximum (non-condensing)
- Vibration: random 0.3g

---

**Main Features**
- AP/Client/Bridge/Router mode supported
- Compliant with IEEE 802.11 a/n 2x2 MIMO
- 240 Mbps data rate
- Fast Ethernet RJ45
- WEP, WPA, WPA2
- Operating/temperature range from -35 to 75°C
- FCC/CE certification

---

**Security**
- Hide SSID/MAC filtering
- ACL/WEP/WPA/WPA2

---

**Management**
- HTTP(s) web GUI
- Firmware upgrade
- Configuration backup and restore
- Factory default configuration
- SNMP V1/V2c

---

**Utility**
- Wireless site survey
- Link information
- Bandwidth control
- Distance adjustment
- Adjustable output power

---
IWF 503 Series

IP55 Outdoor AP/CPE Single Radio Single Band, 802.11 ac/an/a

Main Features
- AP/Client bridge/AP router/Client router/WDS mode supported
- Compliant with IEEE 802.11 ac/an/a 3x3 MIMO
- 1300 Mbps data rate
- 24Vdc PoE input

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
- 1x 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

RF Output Power: IEEE 802.11ac (±2dBm)
- IEEE802.11a
  - 27dBm@6M
  - 23dBm@54M
- IEEE802.11ac/H720
  - 25dBm@MCS0
  - 23dBm@MCS9
- IEEE802.11ac/H860
  - 25dBm@MCS0
  - 23dBm@MCS9
- IEEE802.11ac/H940
  - 25dBm@MCS0
  - 23dBm@MCS9

Receive Sensitivity: IEEE 802.11ac
- IEEE802.11a
  - -77dBm@MCS8
  - -96dBm@MCS9
  - -72dBm@MCS5
  - -66dBm@MCS7
  - -60dBm@MCS9
- IEEE802.11ac/H740
  - -74dBm@MCS5
  - -68dBm@MCS7
  - -62dBm@MCS9

Receive Sensitivity: IEEE 802.11ac
- IEEE802.11a
  - -70dBm@MCS8
  - -90dBm@MCS9
  - -72dBm@MCS5
  - -66dBm@MCS7
  - -60dBm@MCS9
- IEEE802.11ac/H740
  - -74dBm@MCS5
  - -68dBm@MCS7
  - -62dBm@MCS9

Hardware
- WAN: 10/100/1000 Base-TX MDI/MDIX RJ45 x 1
- LAN: 10/100/1000 Base-TX MDI/MDIX RJ45 x 1
- Compliant with:
  - IEEE2003.3 / 802.3
  - IEEE2003.3 / 802.3u
- Hardware based 10/100/1000, full/half, flow control auto negotiation
- Push buttons: 1x Reset
- LED: 1x Power/Status, 1x WPS, 1x X6-Fi
- SMA: 3x with RP-SMA connections

Operating Mode
- AP
- Client bridge
- AP router
- Client router
- WDS

Security
- WEP(64/128/152)
- WPA-PSK
- WPA2-Personal
- WPA2-Enterprise (802.1X certificate)
- Hidden ESSID support
- MAC address filtering
- MAC ACL

Operating Temperature
- -35 to 75°C

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
- IWF503 unit x1
- 24V PoE injector
- Steel clamps*2 for pole mount
- QIG

Ordering Information
- IWF 503-US (P/N: 10T00050301X0)
- IEEE 802.11 ac/an/a with built-in 10dBi directional antennas
- IWF 503D-US (P/N: 10T00050302X0)
- IEEE 802.11 ac/an/a with SMA connection to supports users’ choice of external antennas
IWF 504D

Main Features
- AP/Client bridge router/Client router/WDS mode supported
- Compliant with IEEE 802.11 a/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
- IP55 Outdoor AP/CPE Dual Radio Dual Band, 802.11 ac+b/g/n
- AP /Client bridge router/Client router/WDS mode supported
- Compliant with IEEE 802.11 ac+b/g/n 2x2 MIMO
- 867+300 Mbps data rate
- 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

Product Overview
IWF 504D is an IP55 outdoor cost effective AP/CPE router. IWF 504D is dual radios AP/CPE with IEEE802.11ac+b/g/n 2x2 MIMO with high RF power solution. The maximum data rate up to 867+300Mbps with external antenna which by customer selectable for high gain in long distance transmission. IWF 504D also design as high power solution, up to 27dBm in both 2.4GHz and 5GHz.

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, 5.5 ~ 5.7 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 ~5.85 GHz
RF Output Power: IEEE 802.11ac/a/n (12dBm)
- IEEE802.11a - 27dBm@64M
- 24dBm@512M
- IEEE802.11a/n HT40
- 26dBm@MC50
- 23dBm@MC57
- 22dBm@MC58 in VHT40
- IEEE802.11a/n HT20
- 26dBm@MC50
- 23dBm@MC57
- 22dBm@MC58 in VHT20
RF Output Power: IEEE 802.11b/g/n (12dBm)
- IEEE802.11b - 27dBm@1M
- 24dBm@11M
- IEEE802.11g - 27dBm@11M
- 24dBm@54M
- IEEE802.11n - 23dBm@MC50
- 22dBm@MC57
- 21dBm@MC58
- IEEE802.11n - 23dBm@MC58 in VHT20
- IEEE802.11n - 22dBm@MC58 in VHT40
- IEEE802.11n - 21dBm@MC58 in VHT80

Receive Sensitivity: IEEE 802.11b/g/n
- IEEE802.11b - -95dBm@6M
- -91dBm@11M
- IEEE802.11g - -94dBm@11M
- -80dBm@54M
- IEEE802.11n - -77dBm@MC50/8
- -70dBm@MC57/15
- IEEE802.11n - -73dBm@MC57/15

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 mode
- 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
- Tether (EHS)
- Support iCare 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
- FCC
- CE
- RoHS compliant

Package Contents
- IWF 504D unit x 1
- 24V PoE injector
- Steel clamps*2 for pole mount
- QIG
* Note: The available RF output power will be given by certified power in different region

Ordering Information
- IWF 504D-EU (P/N: 10T00504D00X0)
- IWF 504D-US (P/N: 10T00504D01X0)
NEXCOM's ISA100.11a/ WirelessHART Gateway for Wireless Process Automation

The demand for maximized productivity has led to an increase in large-scale process automation deployments. With more field devices being deployed in increasingly larger plants, the adoption of wireless connectivity solutions is crucial for effective management. NEXCOM offers the NIO 200 series, a gateway that supports ISA100.11a or WirelessHART technology, including a design that focuses on the communication and processing requirements of Industry 4.0.

In response to this demand, NEXCOM offers the NIO 200 series which features ISA100.11a or WirelessHART support and Wi-Fi mesh backbone technology, including a design that focuses on the communication and management requirements of Industry 4.0.

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, and chemical process automation can be found 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 12V to 48V 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 in locations with wiring limitations and offers redundant communication paths to ensure high network uptime.

Flexible Deployment for Critical Field Wireless Networks

- NIO 200 bridges communication between Wi-Fi Mesh backbone and ISA100.11a/WirelessHART field wireless networks.
- Flexible distributed topology with backbone router.
- Reliable wireless communication infrastructure ideal for oil, gas and chemical process automation.

Support of Multiple Field Protocols over ISA100.11a

- Open, object-oriented wireless framework accommodates legacy field device/instruments regardless of communication protocols (such as HART and Modbus).
- Enable consolidation of a diverse range of field devices into one field wireless network.

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, and chemical process automation can be found 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 12V to 48V 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 in locations with wiring limitations and offers redundant communication paths to ensure high network uptime.

Flexible Deployment for Critical Field Wireless Networks

- NIO 200 bridges communication between Wi-Fi Mesh backbone and ISA100.11a/WirelessHART field wireless networks.
- Flexible distributed topology with backbone router.
- Reliable wireless communication infrastructure ideal for oil, gas and chemical process automation.

Support of Multiple Field Protocols over ISA100.11a

- Open, object-oriented wireless framework accommodates legacy field device/instruments regardless of communication protocols (such as HART and Modbus).
- Enable consolidation of a diverse range of field devices into one field wireless network.

Product Selection Guide

<table>
<thead>
<tr>
<th>Model Name</th>
<th>NIO 200IDR</th>
<th>NIO 200IDG</th>
<th>NIO 200HAG (NIO 200IDG + NIO 200IDG)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photo</td>
<td><img src="image1" alt="Photo" /></td>
<td><img src="image2" alt="Photo" /></td>
<td><img src="image3" alt="Photo" /></td>
</tr>
<tr>
<td>WLAN Standard</td>
<td>802.11a</td>
<td>802.11a</td>
<td>802.11a</td>
</tr>
<tr>
<td>Wireless Field Protocol</td>
<td>ISA100</td>
<td>ISA100</td>
<td>ISA100</td>
</tr>
<tr>
<td>Gateway Function</td>
<td>Standalone gateway</td>
<td>All-in-One gateway</td>
<td>All-in-One gateway</td>
</tr>
<tr>
<td>Ethernet speed</td>
<td>10/100/1000</td>
<td>10/100/1000</td>
<td>10/100/1000</td>
</tr>
<tr>
<td>Ethernet speed</td>
<td>10/100/1000</td>
<td>10/100/1000</td>
<td>10/100/1000</td>
</tr>
<tr>
<td>IP Rating</td>
<td>IP67</td>
<td>IP67</td>
<td>IP67</td>
</tr>
<tr>
<td>Temperature</td>
<td>-40°F to 75°F</td>
<td>-40°F to 75°F</td>
<td>-40°F to 75°F</td>
</tr>
<tr>
<td>PdF Type</td>
<td>IEEE 802.3ae</td>
<td>IEEE 802.3ae</td>
<td>IEEE 802.3ae</td>
</tr>
<tr>
<td>Power Input Range</td>
<td>12 ~ 48V</td>
<td>12 ~ 48V</td>
<td>12 ~ 48V</td>
</tr>
<tr>
<td>Network Management</td>
<td>SNMP V1/V2c/Web GUI/SSH/ICMP</td>
<td>SNMP V1/V2c/Web GUI/SSH/ICMP</td>
<td>SNMP V1/V2c/Web GUI/SSH/ICMP</td>
</tr>
<tr>
<td>Certification</td>
<td>CE, FCC, C-UL, ATEX</td>
<td>CE, FCC, C-UL, ATEX</td>
<td>CE, FCC, C-UL, ATEX</td>
</tr>
<tr>
<td>Safety</td>
<td>UL 60950-1, UL 60950-22</td>
<td>UL 60950-1, UL 60950-22</td>
<td>UL 60950-1, UL 60950-22</td>
</tr>
<tr>
<td>Anti-Explosive</td>
<td>HART</td>
<td>HART</td>
<td>HART</td>
</tr>
</tbody>
</table>

Flexible Deployment for Critical Field Wireless Networks

- NIO 200 bridges communication between Wi-Fi Mesh backbone and ISA100.11a/WirelessHART field wireless networks.
- Flexible distributed topology with backbone router.
- Reliable wireless communication infrastructure ideal for oil, gas and chemical process automation.

Support of Multiple Field Protocols over ISA100.11a

- Open, object-oriented wireless framework accommodates legacy field device/instruments regardless of communication protocols (such as HART and Modbus).
- Enable consolidation of a diverse range of field devices into one field wireless network.

Designed for Mission-Critical Applications

- Redundant power with DC and PoE input.
- Dual high power; S/G/H+ Wi-Fi mesh ensures a double-link backbone.
- Rugged, level 4 ESD, EFT and surge protection.
- Anti-explosive protection (C1D2 and ATEX).
- High wireless radio sensitivity.
NIO 200 Series

**Product Overview**

NEXCOM NIO 200 is a powerful and flexible distributed network topology ISA100 1a access point integrating 802.11n Mesh technology, with ISA100 1a/WirelessHART technology, NIO 200 enables a reliable, full mesh network to ensure robust and reliable connectivity for mission critical industrial wireless applications. The integration of both 802.11n Mesh & ISA100.11a/WirelessHART technology 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 C20 and ATEX certified requirement and is perfect solution to critical data monitoring and serving in oil & gas, chemical plant, etc…

**Specifications**

**Wireless Radio**
- IEEE802.11g + 2, MIMO 2 x 2
- IEEE802.15.4, T Tx, R X

**Wi-Fi Frequency Ranges**
- USA: 5.725~5.85 GHz
- Japan: 5.15~5.35 GHz, 5.47~5.725 GHz
- China: 5.725~5.85 GHz

**RF Output Power**: IEEE 802.11a
- 802.11a: -27 dBm with 2 antennas
- 802.11n (HT20): -27 dBm with 2 antennas
- 802.11n (HT40): -27 dBm with 2 antennas

**Radio approvals**
- UL 60950-1, 60950-22
- EN 301 893
- EN 300 328
- AS/NZS 4268.2003
- RSS-210
- FCC Part 15.247, 15.407
- EN 301 489-1, -17
- FCC part 15.107, 15.109

**Network topology**
- Dual Wi-Fi Mesh path establishes better stability in backbone transmission
- Dual Wi-Fi Mesh path establishes better stability in backbone transmission
- Perfect triple play infrastructure: video surveillance via high throughput Wi-Fi backbone ensures video transmission without compromising video performance
- Full Mesh topology: robust wireless connectivity from ISA100/WirelessHART field device coverage to Wi-Fi backbone
- Distributed network topology provides scalable infrastructure: easy integration and cost saving

**Environment Protection**
- Operating temperature: -40~75°C (altitude: up to 3000m)
- Storage temperature: -40~80°C
- Humidity: 0% to 95% maximum (non-condensing)
- Vibration: random 0.3g
- IEC 61000-4-2 level 4 ESD immunity
- IEC 61000-4-5 level 4 AC surge immunity
- IEC 61000-4-4 level 4 electrical fast transient burst immunity

**Performance Parameters**
- Weight: TBD
- Dimension: 256mm x 226mm x 91mm

**Ordering Information**

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIO 200IDR</td>
<td>Backbone Router</td>
<td>P/N: 10T00021004X0</td>
</tr>
<tr>
<td>NIO 200IDG</td>
<td>Distributed Gateway</td>
<td>P/N: 10T00021003X0</td>
</tr>
<tr>
<td>NIO 200IAG</td>
<td>Distributed Gateway</td>
<td>P/N: 10T00021002X0</td>
</tr>
<tr>
<td>NIO200HAG</td>
<td>ISA 100 WirelessHART</td>
<td>P/N: 10T00021000X0</td>
</tr>
</tbody>
</table>

**Radio approvals**
- CE: EN 301 489-1, -17
- FCC part 15.107, 15.109
- UL 60950-1; 60950-22
- EN 300 328
- AS/NZS 4268.2003
- RSS-210
- FCC Part 15.247, 15.407
- EN 301 489-1, -17

**Radio specifications**
- IEEE802.11a: 10/100/1000 Base-TX MDI/MDIX
- IEEE802.11n (HT20): 10/100/1000 Base-TX MDI/MDIX
- IEEE802.11n (HT40): 10/100/1000 Base-TX MDI/MDIX

**Compliance**
- IECEE CB Marks
- ENEC Class I, Zone 2; Ex nA II, T5
- CE: EN 301 489-1, -17
- FCC part 15.107, 15.109
- EN 300 328
- AS/NZS 4268.2003
- UL 60950-1; 60950-22
- EN 60950, 2nd edition
- IEC 61000-4-5 AC surge immunity
- IEC 61000-4-4 electrical fast transient burst immunity

**Additional features**
- Network monitoring and management
- Packet loss monitoring
- Event logs
- configurable backup and restore
- One button/LED to restore factory default setting
- Firmware upgrade

**Built-in Services & Client Interfaces to Other Services**
- SNMP v1/v2c/v3 client

**Physical and Power**
- 10-48 VDC
- CE: EN 301 489-1, -17
- FCC part 15.107, 15.109
- EN 300 328
- EN 301 893
- EN 301 893
- UL 60950-1; 60950-22
- FCC Part 15.247, 15.407

**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

**Hardware**
- IEEE802.11g + 2, MIMO 2 x 2
- IEEE802.15.4, 1 X, 1 Rx
- IEEE802.15.4, 1 X, 1 Rx

**Wi-Fi Frequency Ranges**
- USA: 5.725~5.85 GHz
- Japan: 5.15~5.35 GHz, 5.47~5.725 GHz
- China: 5.725~5.85 GHz

**RF Output Power**
- IEEE 802.11a
  - 802.11a: -27 dBm with 2 antennas
  - 802.11n (HT20): -27 dBm with 2 antennas
  - 802.11n (HT40): -27 dBm with 2 antennas

**Compliance**
- UL 60950-1, 60950-22
- IEC 60950, 2nd edition
- EN 60950, 2nd edition
- IEC 60950-2-2 level 4 ESD immunity
- IEC 60950-4-5 AC surge immunity
- IEC 60950-2-4 level 4 electrical fast transient burst immunity

**Security**
- WEP: 64/128/256
- Wi-Fi Protected Access (WPA)
  - WPA Personal (WPA-PSK)
  - WPA Enterprise (WPA-Enterprise)

**System Management**
- N-Care Web GUI Management
- SNMP v1/v2c/v3
- Event log

**Ordering Information**

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIO 200IDR</td>
<td>Backbone Router</td>
<td>P/N: 10T00021004X0</td>
</tr>
<tr>
<td>NIO 200IDG</td>
<td>Distributed Gateway</td>
<td>P/N: 10T00021003X0</td>
</tr>
<tr>
<td>NIO 200IAG</td>
<td>Distributed Gateway</td>
<td>P/N: 10T00021002X0</td>
</tr>
<tr>
<td>NIO200HAG</td>
<td>ISA 100 WirelessHART</td>
<td>P/N: 10T00021000X0</td>
</tr>
</tbody>
</table>