

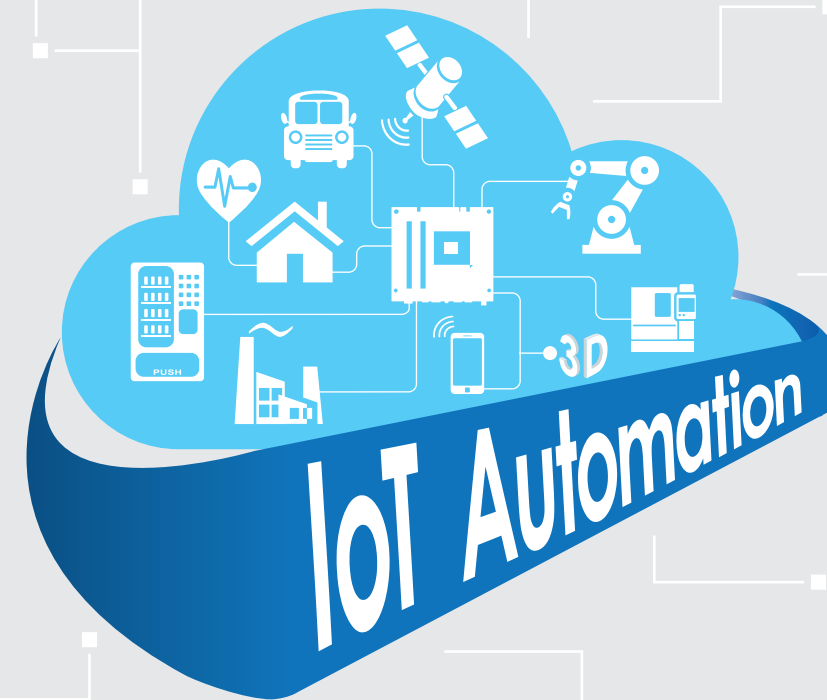


The Intelligent Systems



Connect to Industry 4.0

# Industrial Network and Cloud Product Selection Guide



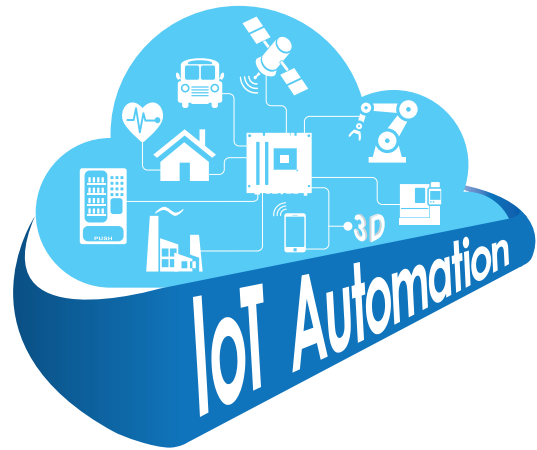
# Connect to Industry 4.0

## Contents

<b>IoT Automation Systems, The Solutions to Industry 4.0</b>	02
<b>Industrial IoT Network Infrastructure</b>	04
<b>Cyber Physical System Connectivity</b>	08
NEXCOM Industrial IoT Studio	10
CPS 100-M	12
CPS 100-RE/DP	14
CPS 200-RE/DP	16
<b>Industrial IoT Security</b>	18
IFA 1610	22
IFA 2610	24
IFA 3610	26
IVD 1000	28
iNAS 330	30
<b>Industry 4.0 Wireless Solution (IWS)</b>	32
<b>nCare I4.0 Network Management Solution</b>	36
IWF 800 nCare	38

<b>Trusted Industrial Wi-Fi Mesh Network</b>	40
IWF 300	44
IWF 310	46
IWF 6300 Series	48
IWF 3310 XH/M	50
NIO 50	52
NIO 51	54
<b>Rugged &amp; Ultra-Fast Gigabit Industrial Wi-Fi Solution for Video Surveillance</b>	56
IWF 503	58
IWF 504D	60
<b>NEXCOM's ISA100.11a/ WirelessHART Gateway for Wireless Process Automation</b>	62
NIO 200 Series	64

# IoT Automation Systems, 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 (iAutomation), 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.

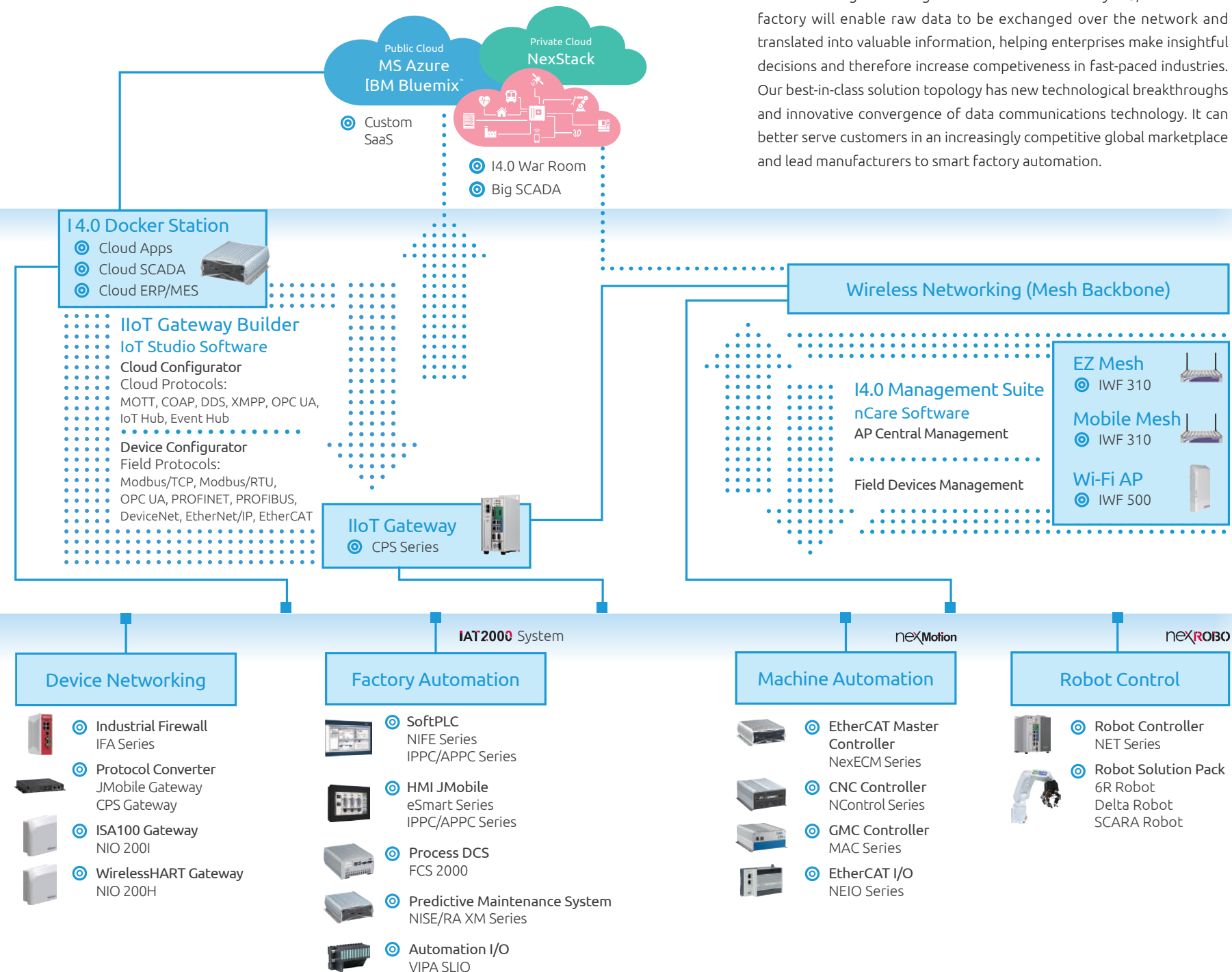
For instance, operators can benefit by getting an accurate measure of machine status and factory operations in real-time, as well as integrating enterprise resource planning (ERP) and manufacturing execution systems (MES) systems to optimize supply chain management. Based on live field data, big data 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 an equipment failure to ensure production efficiency and yield rate.

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

## Application Layer

## Communication Layer

## Device Layer



• Figure 1. Industry 4.0 Solution Map & Topology.

## IoT Automation Solution Brochures



### IoT Automation Solutions Master e-Catalog

USB Driver

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



### IoT Automation Solution Product Selection Guide

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



### Robot & Machine Automation Product Selection Guide

NEXCOM EtherCAT robot solutions, NexROBO, unleash possibilities for in-house development, add-on functionality, and reconfiguration of robots. Based on an open and modular architecture, NexROBO delivers development flexibility and expandable functions with a variety of EtherCAT Master controllers, pre-validated third-party EtherCAT slaves, and NEXCOM EtherCAT Master development stack, aimed to stimulate the broad use of robotic systems and industrial robots.



### Industrial Network and Cloud Product Selection Guide

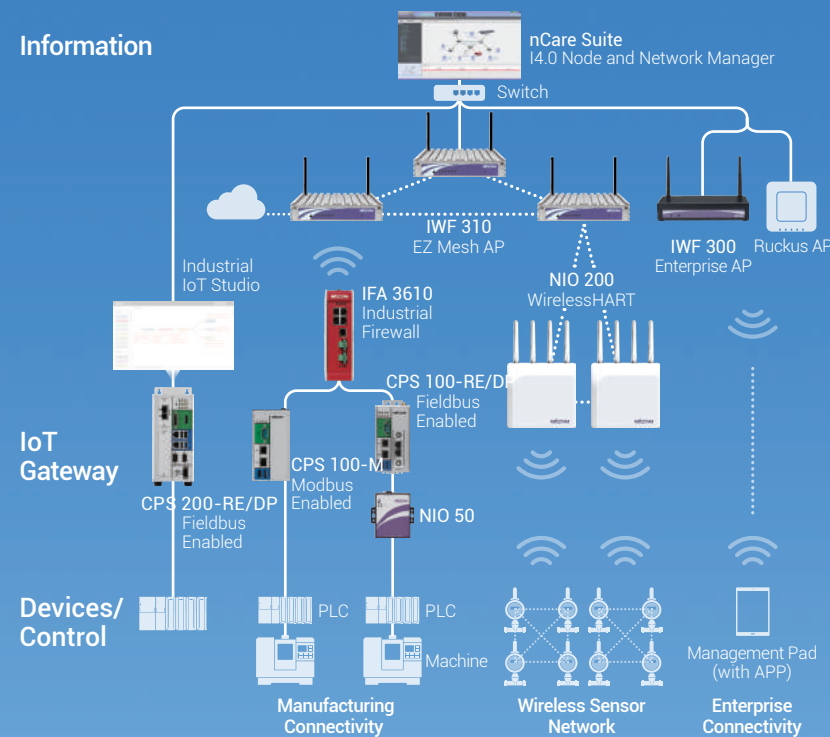
The industrial IoT (IIoT) network lay the important foundation for Industry 4.0. It includes three pillars—Cyber-Physical System (CPS), Industrial Wireless Solution, and Industrial Firewall for IoT Security. NEXCOM provides the IIoT network with complete product solutions which cover all three scopes. The product solutions are designed with the concepts of "ready to use" and "click to connect" so users can easily establish the IIoT network that can encompass existing automation systems in their Industry 4.0 and IIoT applications.



# Industrial IoT Network Infrastructure

Industry 4.0 and Industrial IoT (IIoT) have become the mainstream of smart manufacturing. Devices, software services, and cloud platforms spring up around the IIoT with great stress laid on the importance of horizontal and vertical integration. However, industrial control and automation systems have a close architecture which delivers high reliability, meets operational

Figure 1. Architecture of NEXCOM's IoT Network Solutions.



needs, and yet poses great challenges in system integration on the course of IIoT 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 IIoT (Figure 1).

The foundation of the IIoT 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 IIoT 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).

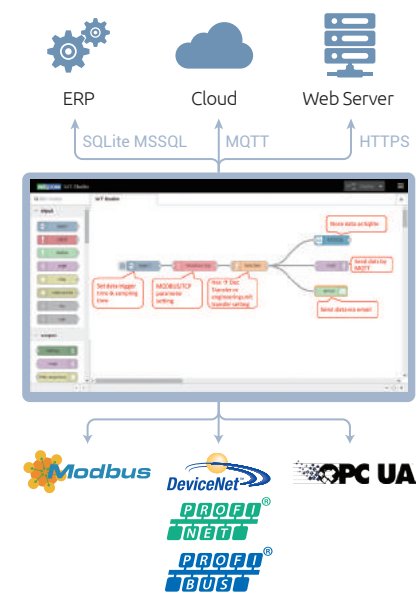


Figure 2. Communication protocols supported by NEXCOM's CPS gateways and IoT Studio.

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

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

NEXCOM's CPS lineup is equipped with Modbus, industrial fieldbus, and OPC UA communication capabilities to amass data from most industrial systems (Figure 4). As to upper connectivity, MQTT, SQLite, and HTTPS are supported so NEXCOM's CPS can integrate with cloud platforms, databases, and web services and therefore give our clients great flexibility to choose a data receiving end they see fit. To further reduce system integration efforts, NEXCOM has developed a configuration tool—NEXCOM Industrial IoT Studio. This tool integrates features required of establishing end-to-end connections and is designed with a graphical user interface (GUI) enabling system integration

engineers to configure connection settings without the need of programming and coding.

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

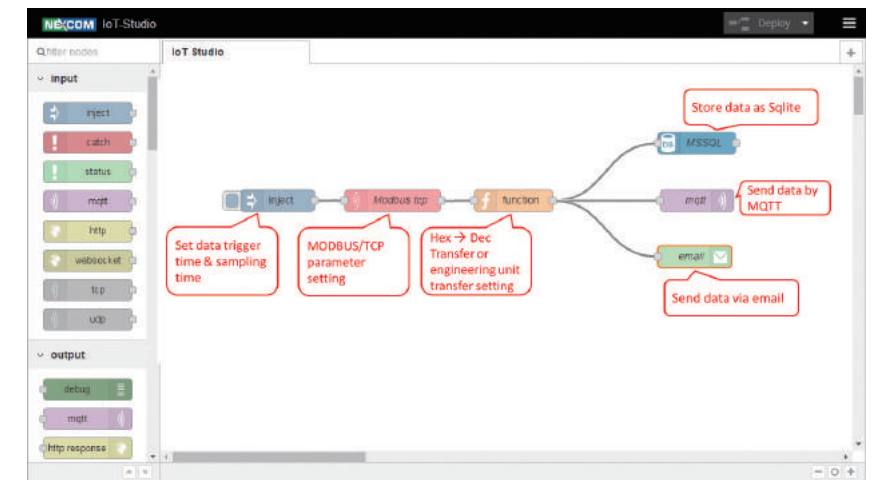


Figure 3. NEXCOM Industrial IoT Studio is a web-based configuration tool designed with a graphical user interface (GUI) and supports drag-and-drop operations.

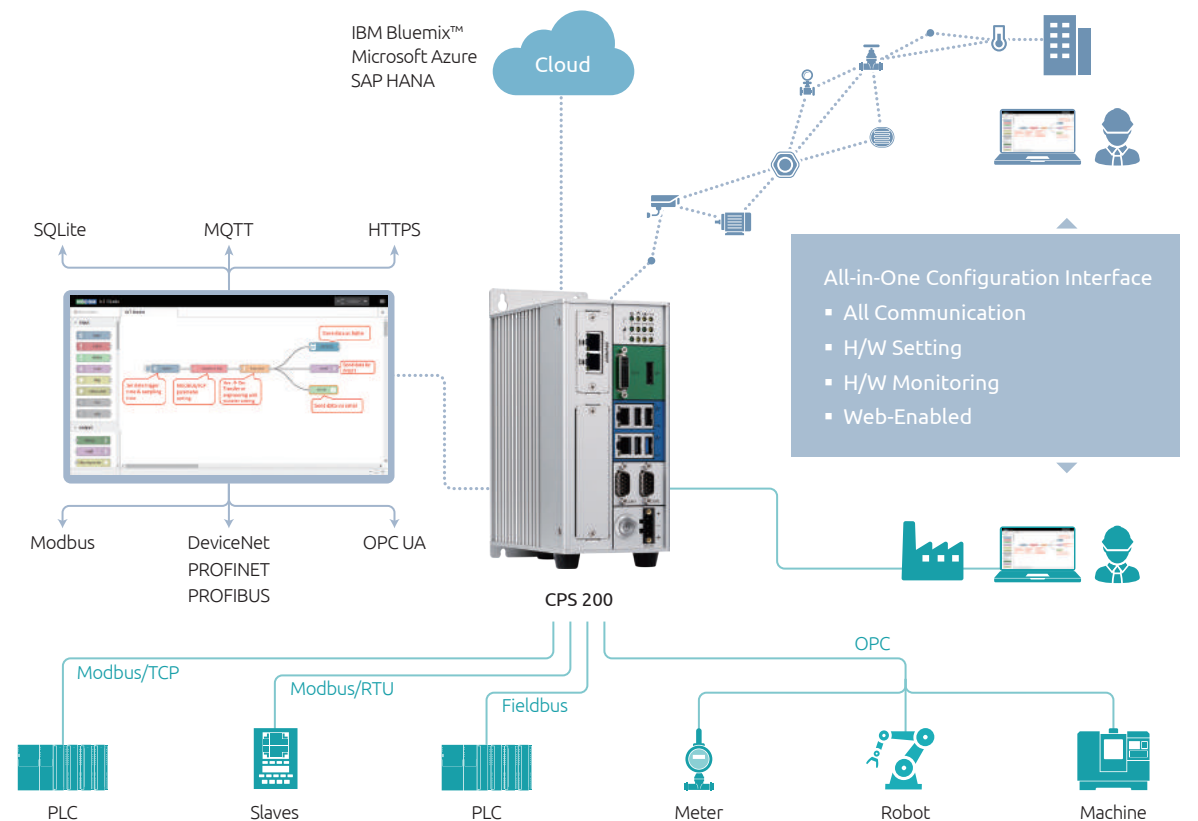


Figure 4. NEXCOM CPS provides seamless end-to-end connection.

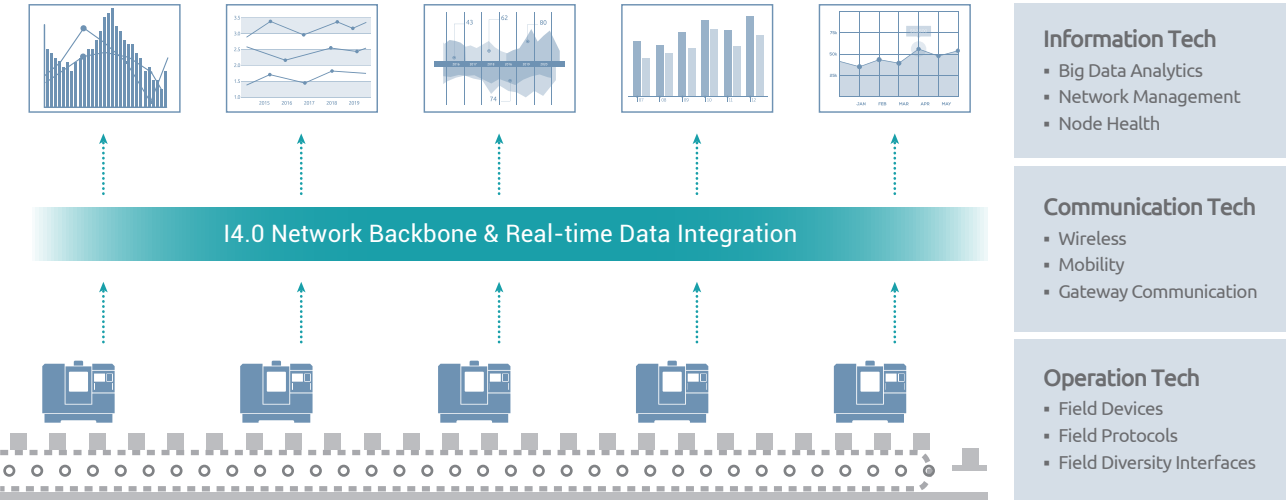


Figure 5. 14.0 wireless solution consists of a 3-layer integration of IT, CT and OT networks—all converged for IIoT.

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 clouds services and big data analysis on upper network layers. To make this happen, factory operations, equipment health status, and manufacturing processes must be able to be monitored and managed from a distance, underlining the importance of a network backbone dedicated to industrial applications.

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

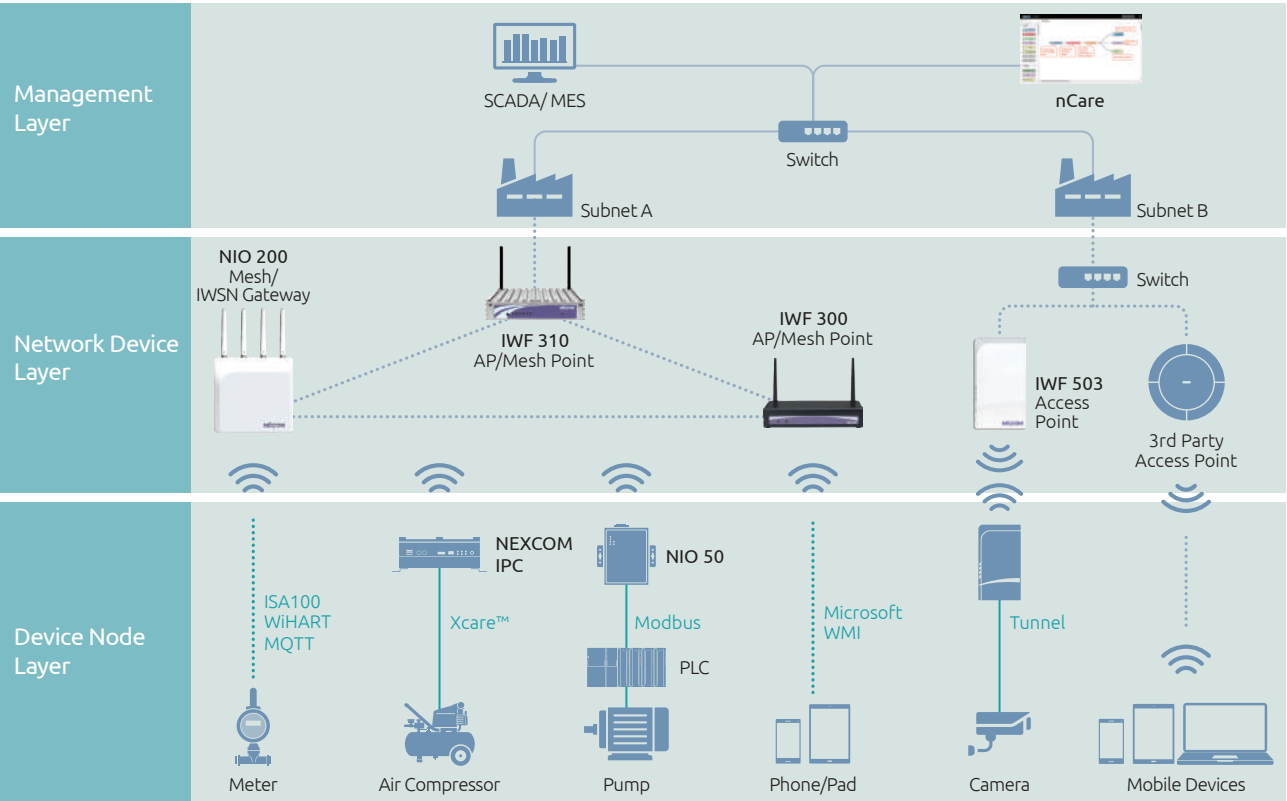


Figure 6. nCare Device and Network Health Management Solution.

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

Industrial Firewall

More and more facilities, systems, equipment are coming online with the aim to improving operational efficiency. To keep improvements on course, NEXCOM has added rich feature sets, expandability, and rugged design to its HENGETM series which is made up of the IFA family of industrial firewalls and VPN dispatcher IVD 1000. It is with ease that users can tap into built-in features to enjoy secure remote access, simplified private network tunneling, reliable connections, stateful edge firewall protection, intrusion prevention, and reliable



Figure 7. HENGETM series.

data storage provided by extremely rugged network-attached storage iNAS 330. To sum up, the high level of function integration of the HENGETM series makes it one of indispensable network security solutions in industrial automation applications (Figure 8).

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 IPsec and SSL VPN protection to arm industrial systems with extra shields. This feature enables industrial system vendors to not only remotely but also securely access and manage their products installed on clients' premises over simplified private network tunnels. Furthermore, the rugged design of the IFA family can withstand rigorous challenges of harsh operating environments, making it ideal for industrial applications. It is worth mentioning that the IFA family can operate over an extended temperature range from -20 degrees Celsius to 70 degrees Celsius.

Equipped with full SSL VPN functionality—VPN server and VPN client—the IFA family can strengthen security protection for high-value industrial systems used in industrial automation, process control, and power stations applications.

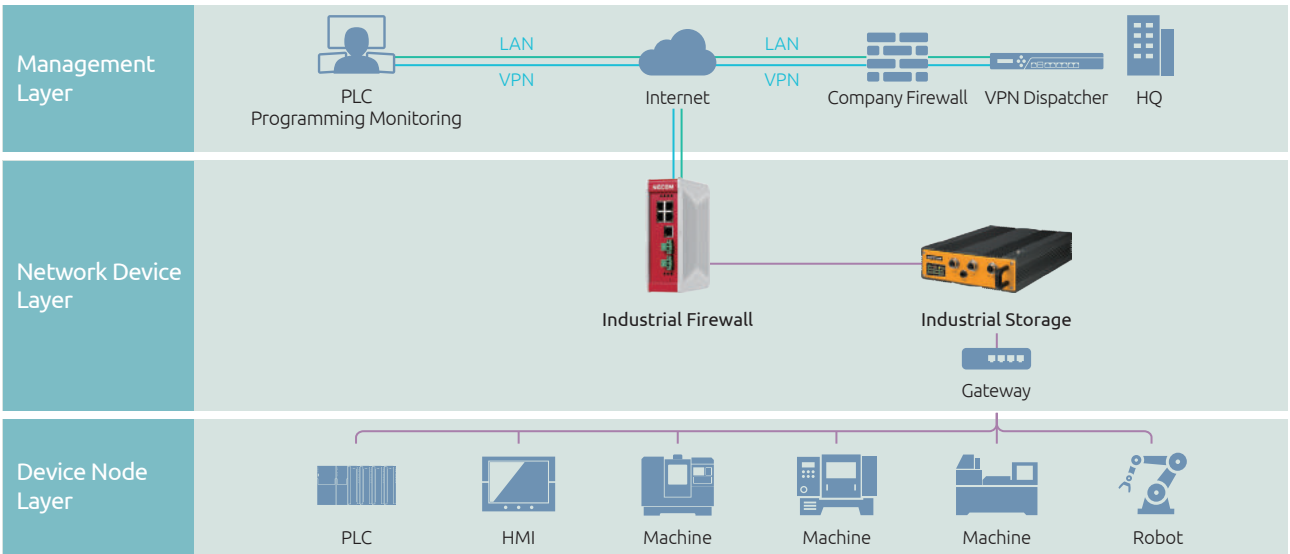


Figure 8. Industrial network architecture.

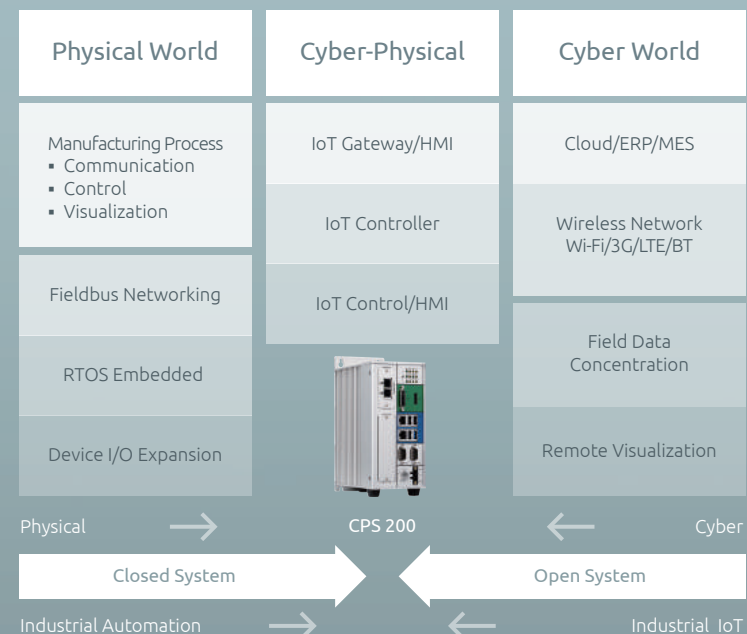


# Cyber-Physical System with Connectivity

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 automatic control capability, and IoT human-machine interface (HMI). IoT communications

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



support is imperative to data processing, integration, and uploads. IIoT automatic control capability allows automation systems to leverage the power of remote big data analysis while delivering high-performance highly reliable real-time control with real-time operating systems. IIoT HMI is aimed to achieve overall management from business to machine levels by taking advantage of information on cloud dashboards and single-unit monitoring for timely and effective system adjustments.

A CPS must meet three technology requirements. Firstly, a CPS has to support special communication protocols, or network interfaces, commonly used in the industrial sector so as to communicate with industrial systems like programmable logic controllers (PLCs) and machine controllers and extract data required of data fusion and big data analysis. Secondly, a CPS must be capable of processing data. Despite the diversity of data formats and industrial communication protocols, a CPS has to parse data for information and convert it into different formats that can be recognized by edge servers and cloud platforms on upper layers of IIoT networks. Thirdly, a CPS must have a user-friendly interface to support protocol conversion functions as well as to deliver

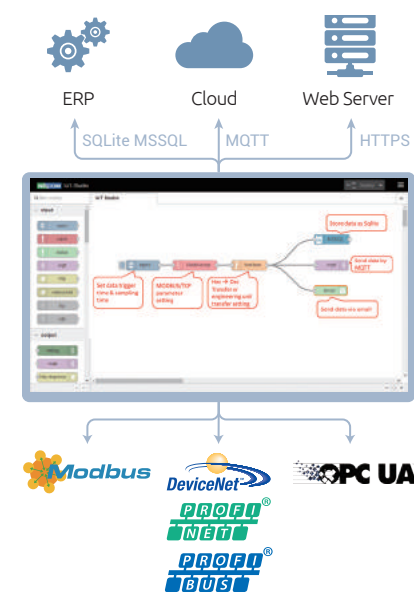


Figure 2. NEXCOM Industrial IoT Studio combines all required features into a unified graphical user interface.

high reliability. The best choice of hardware platform for a CPS is, no doubt, an industrial computer which combines flexible expansion for communications featured in PCs and sturdy design required of industrial products.

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

Highly reliable hardware platform tempered

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

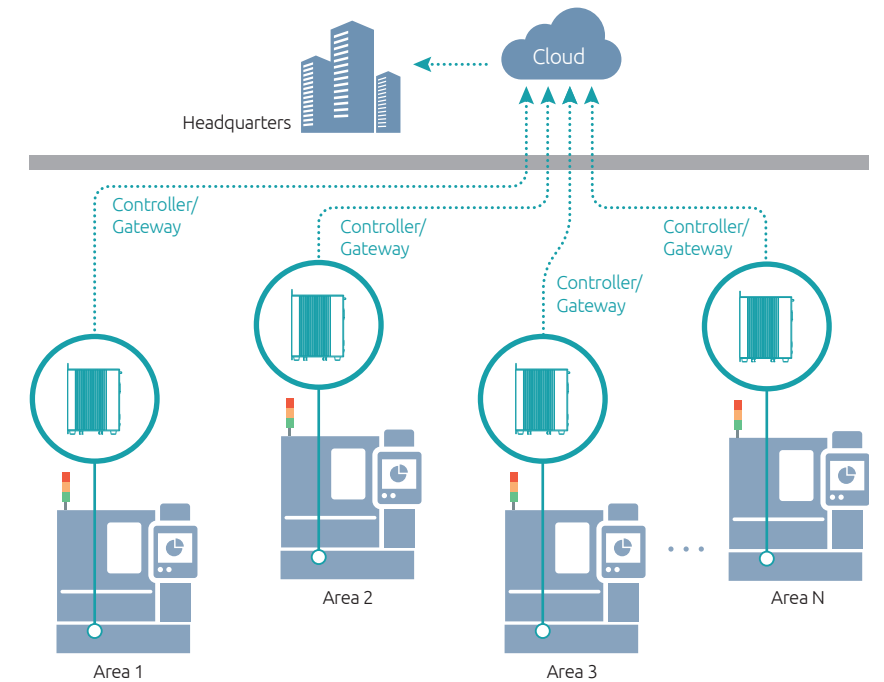


Figure 3. In a real case scenario, a CPS can harvest manufacturing data from a closed-loop machine and send the data the business headquarters over internet.

## Product Selection Guide

Model Name	CPS100-M	CPS 100-RE/DP	CPS 200-RE/DP
Photo			
Category	Industrial IIoT Remote Gateway	Fieldbus Enabled IIoT Remote Gateway	Fieldbus Enabled IIoT Edge Gateway
Communication Protocols for Local Devices	Modbus/TCP, Modbus/RTU, OPCUA (Client)	PROFINET-RT, PROFIBUS-DP, EtherNet/IP (Slave), Modbus/TCP, Modbus/RTU (Master), OPC-UA Client	PROFINET-RT, PROFIBUS-DP, EtherNet/IP (Slave), Modbus/TCP, Modbus/RTU (Master), OPC-UA Client
Communication for Cloud/Server	MQTT, SQLite, Https	MQTT, SQLite, Https	MQTT, SQLite, Https
Wireless Communication Interface Options	Wi-Fi, 3G, 4G/LTE	Wi-Fi, 3G, 4G/LTE	Wi-Fi, 3G, 4G/LTE
Number of LAN Port	2	2	2
Type of LAN	RJ45	RJ45	RJ45
COM Port	1 x RS-232/485	1 x RS-232/485	2 x RS-232/422/485
USB	1 x USB 3.0 1 x USB 2.0	1 x USB 3.0 1 x USB 2.0	1 x USB 3.0 3 x USB 2.0
Display	N/A	N/A	1 x DVH, 1 x DP
Mounting Style	Wall/DIN Rail	Wall/DIN Rail	Wall/DIN Rail
Temperature	-20°C ~ +65°C	-20°C ~ +65°C	0°C ~ +50°C
Dimension (mm)	63 x 100 x 151	63 x 100 x 151	85 x 157 x 214
DC Input	12/24VDC	12/24VDC	24VDC
Certification	CE, FCC	CE, FCC	CE, FCC
Storage	16G eMMC	16G eMMC	128G SSD

Microsoft Azure

Private Cloud

IBM Bluemix™

Connect to Cloud Securely

NEXCOM Industrial IoT Studio

Industrial Gateway Builder

Manage CPS Efficiently

CPS 100

CPS 200

Processing Data Analytically

Controllers

Devices/PLC

Sensors

Main Features

Processing data analytically by 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, Ethernet/IP) 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, demonstrated how developers can swiftly implement customized features by taking advantage of pre-integrated functions with simple clicks, drags, and drops. Accelerating the development of IoT applications with reduced efforts enables immediate testing of innovative ideas, turning proof-of-concept inventions into wide-scale deployment. NEXCOM Industrial IoT Studio which is a GUI tool powered by using Node.js and IBM Node-RED (\*1).

Specifications

Category	Description	Node
Modbus	Get the registers and status with the Modbus protocol	Modbus-TCP read/write
		Modbus-RTU read/write
Fieldbus	Get the registers and status from the controller/devices with Fieldbus interface	PROFIBUS read
		PROFIBUS write
		PROFINET read
		PROFINET write
		EtherNet/IP read
		EtherNet/IP write
Data process	Process or encrypt/decrypt data from buffering	Merge
		Boundary
		Critical section
		H/W Info
		Base64Encode
		Base64Decode
		3DesEncrypt
		3DesDecrypt
		OPC UA Client
Category	Description	Node
Input	Prompt for user input from network or serial port	Inject, catch, status, MQTT, http, websocket, TCP, UDP, serial
Output	Expose the data from service or debug message	Debug, MQTT, http response, web socket, TCP, UDP, serial
Function		Function, template, delay, trigger, comment http request, TCP request, switch, change range, csv, html, json, xml, rbe
Social	Access 'multipart/form-data' content by email	Email in
		Email out
Storage	Read/write the file or database	File in, file out
		SQLite
Cloud	Provides Azure service	eventhub
		IoT hub
		MS SQL

Support OS & Hardware Matrix

Devices	Windows Embedded 8	Yocto (Linux)
CPS 100-M	X	O
CPS 100-RE/DP	X	O
CPS 200-RE/DP	X	O

Note: Products and models are listed but not limited, please contact your sales representatives for updates.  
\*1. Node-RED is a visual wiring tool for the Internet of Things. A creation of IBM emerging technologies.

10

Industrial Network and Cloud Product Selection Guide

NEXCOM

NEXCOM

Industrial Network and Cloud Product Selection Guide

11



Main Features

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

Product Overview

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

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

PDM Rotor Kit Specifications

Seamless Integration

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

Secure Gateway Management

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

Productive Engineering

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

Direct IoT Communication

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

Gateway Platform Specifications

CPU Performance

- Onboard Intel® Atom™ processor E3805 1.33 GHz

Memory

- Built-in DDR3L 2GB system memory

Networking Connectivity

- 2 x 10/100/1000Mbps LAN ports

Major I/O Connectivity

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

Wireless Connectivity (Optional Module)

- IEEE 802.11 a/b/g/n connectivity

Power Requirement

- 1 x 12/24VDC input, ±20% range

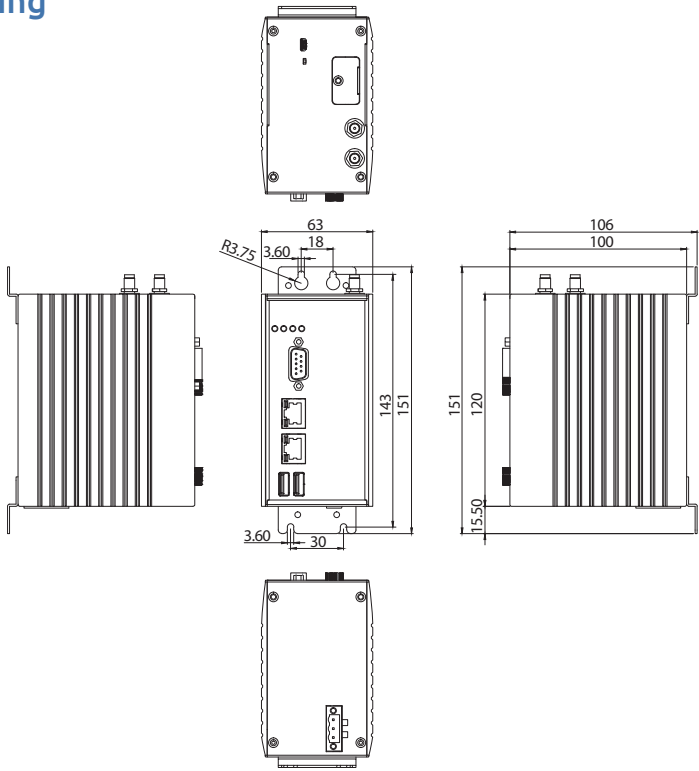
Storage Device

- 1 x eMMC 16GB flash memory

Dimensions

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

Dimension Drawing



Weight

- 600g

Construction

- Aluminum and metal chassis with fanless design

Shock Protection

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

Vibration Protection

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

Operation Temperature

- Ambient with air flow: -20°C~65°C

Storage Temperature

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

Regulation

- CE/FCC

Ordering Information

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



# CPS 100-RE/DP

Industrial IoT Remote Gateway



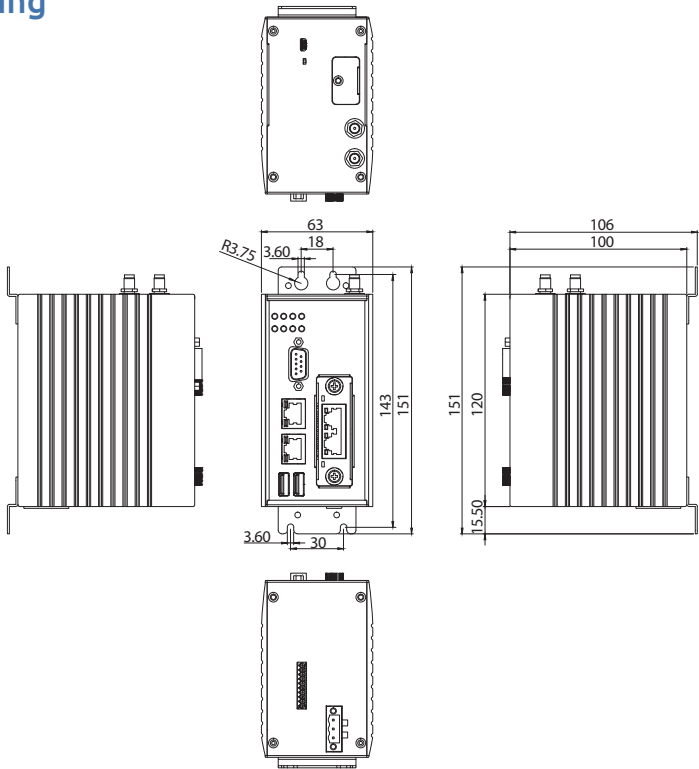
CPS 100-RE

CPS 100-DP

### Main Features

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

### Dimension Drawing



### Product Overview

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

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

#### Dimensions

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

#### Weight

- 600g

#### Construction

- Aluminum and metal chassis with fanless design

#### Shock Protection

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

#### Vibration Protection

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

#### Operation Temperature

- Ambient with air flow: -20°C~65°C

#### Storage Temperature

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

#### Regulation

- CE/FCC

### Ordering Information

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

### Benefits of CPS Solution

#### Seamless Integration

- Compatible with existing installation in field control network
- Multiple fieldbus (slave) support – PROFIBUS®, 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 client, TCP, UDP, HTTP, WebSocket, E-mail

#### Secure Gateway Management

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

#### Productive Engineering

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

#### Direct IoT Communication

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

### Gateway Platform Specifications

#### CPU Performance

- Onboard Intel® Atom™ processor E3805 1.33 GHz

#### Memory

- Built-in DDR3L 2GB system memory

#### Networking Connectivity

- 2 x 10/100/1000Mbps LAN ports
- Isolated field control 10/100Mbps ports, PROFIBUS®, PROFINET® or EtherNet/IP™

#### 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 DI/DO

#### Wireless Connectivity (Optional Module)

- IEEE 802.11 a/b/g/n connectivity

#### Power Requirement

- 1 x 12/24VDC input, ±20% range

#### Storage Device

- 1 x eMMC 16GB flash memory



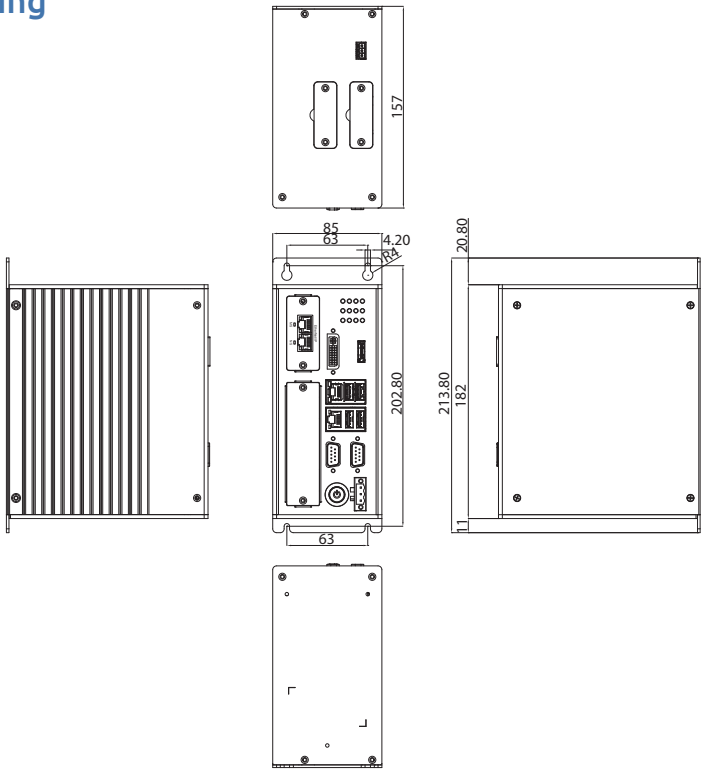
CPS 200-RE

CPS 200-DP

Main Features

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

Dimension Drawing



Product Overview

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

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

Power Requirement

- 1 x 24VDC input, ±20% range

Storage Device

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

Dimensions

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

Weight

- 2.25Kg (w/ disk)

Construction

- Aluminum and metal chassis with fanless design

Shock Protection

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

Vibration Protection w/ CFast & SSD condition

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

Operation Temperature

- Ambient with air flow: 0°C~50°C

Storage Temperature

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

Regulation

- CE/FCC
- LVD

Ordering Information

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

Benefits of CPS Solution

Seamless Integration

- Compatible with existing installation in field control network
- Multiple fieldbus (slave) support – PROFIBUS®, 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 client, TCP, UDP, HTTP, WebSocket, E-mail

Secure Gateway Management

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

Productive Engineering

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

Direct IoT Communication

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

Gateway Platform Specifications

CPU Performance

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

Memory

- Built-in DDR3L 4GB system memory

Display

- DP and DVI-I display output

Networking Connectivity

- 2 x 10/100/1000Mbps LAN ports
- Isolated field control 10/100Mbps ports, PROFIBUS®, PROFINET® or EtherNet/IP™

Major I/O Connectivity

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

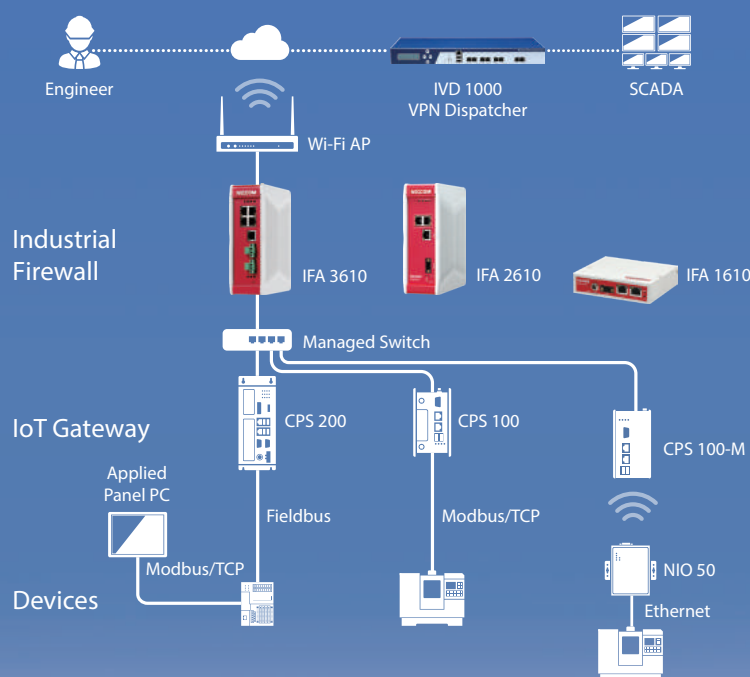
Wireless Connectivity (Optional Module, up to 2)

- IEEE 802.11 a/b/g/n connectivity

# Industrial IoT Security

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

Figure 1. Industrial IoT security architecture.



## The Industrial Firewall Series

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

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

## Protect Critical Assets Against Cyber Threats

To kick business into higher gear, energy companies are contemplating the possibility of incorporating the internet technology in their infrastructure in the hope to automate operational processes, consolidate solutions, and improve efficiency. However, the pace of internet adoption in the industrial sector has been slow because common IT network security solutions 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 virus spread by USB devices. With severe ramifications like power outage proven in some cases, precautions must be considered in the early stages of planning.

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

## Increase Operational Efficiency

Remote access and data acquisition are of paramount importance in strengthening operational efficiency, winning a bigger market share, differentiating an enterprise from competitors, and more. However, industrial process control networks were narrow-band closed-loop networks that are not suited for remote access, let alone remote system monitoring and inspection. Thanks to the proliferation and cost reduction of Ethernet, VPN, and other networking technologies, vendors and system integrators of automation systems can take advantage of remote access to reduce unexpected system downtime and travel time and costs related to onsite services. The technologies also provide benefits of ease of installation and integration, better network expandability, and a leaner cost structure.

Designed with remote system monitoring and inspection in mind, the SSL VPN-equipped IFA series can provide private network tunnels (Figure 2). Leveraging a combination of tunneling, data encryption and decryption, key management, and authentication technologies, the IFA series can easily build a virtual private channel 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.

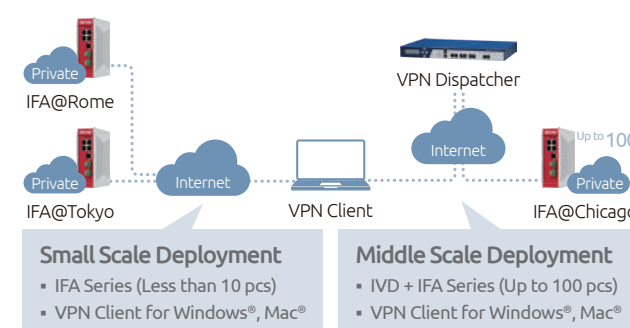


Figure 2. Secure remote access with VPN tunneling.

## 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.

## IFA Features

### Network Security

- Stateful Packet Firewall
- Intrusion Prevention
- SNMP Support
- Portscan Detection
- DoS and DDoS Protection
- SYN/ICMP Flood Protection
- VLAN Support (IEEE802.1Q)

### True SSL/TLS VPN

- Encryption: DES, 3DES, AES 128/192/256-bit, CAST5, Blowfish
- Authentication: Pre-Shared Key, X.509-Certificates, Certification Authority, and Local
- PPTP Passthrough
- VPN Client-to-Site
- Support for VPN over HTTPS Proxy (Open VPN)
- VPN Client for Microsoft® Windows®, Mac® OS X and Linux
- Multiple Logins per User
- VPN Failover

### IPSec

- Encryption: 3DES, AES b128/256-bit, MD5, SHA1
- Diffie Hellman (2,5,14,15,16,17,18)
- Authentication: Pre-Shared Key, RSA Keys X.509-Certificates IKEv1
- L2TP
- DPD (Dead Peer Detection)
- NAT-Traversal
- Compression
- PFS (Perfect Forward Secrecy)
- VPN Site-to-Site
- VPN Client-to-Site (Road Warrior)
- Integrated Certificate Authority

### Logging and Reporting

- Network/System/Performance Statistics
- Rule-Based Logging Settings (Firewall Rules)
- Syslog: Local or Remote
- Real-Time Dashboard
- Event Handling and Notification
- Live Log Viewer

### Network Address Translation

- Destination NAT
- One-to-One NAT
- Source NAT (SNAT)
- IPsec NAT Traversal

### Update and Backup

- Scheduled Automatic Backup
- Instant Recovery/Backup to USB Stick

### Bridging

- Firewall Stealth Mode w/ Bypass Function
- OSI-Layer 2 Firewall-Function
- Spanning Tree

## Connect with Simplicity, Efficiency & Security

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

## The Industrial Network-Attached Storage Series

NEXCOM iNAS 330 is a network-attached storage (NAS) offering high availability with rugged design, RAID support, and buffer cache. With the incremental growth of distributed computing in industrial applications, the need for safe reliable data storage units on the field is surging because data needs to be well kept until sent to a cloud platform for further processing. From the hardware perspective, such storage units must have redundant routing and power supply, extended operating temperature range, water and dust resistance,



and anti-vibration protection. As to data availability, an NAS must support RAID configuration, 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 sync commands to help users choose from mirror backup and incremental backup according to applications’ needs. As different backup methods and cycles would have different effects on data recovery schemes, avoiding data loss takes both thoughtful evaluation and solid execution. The iNAS 330 is a trustworthy data storage solution to ensure data backup and recovery plans fall into place.

Lastly, the iNAS 330 has a rugged design which has been a hallmark of NEXCOM products. It is compliant with standards for railway applications, such as EN 50155 and EN 61373, and incorporates M12 connectors to offer the IP54 level of water and dust resistance.

Supporting various file transfer protocols of network communications, the iNAS 330 answers the need for data storage spawned by the growing proliferation of distributed computing. The bottom line is that the iNAS 330 is easy to deploy and can reliably operate in harsh operating environments faced by industrial automation solutions, railway applications, alternative energy management systems, and the oil and gas industry.

## Vulnerability Assessment

Questions that every plant manager has: We are expanding production with an estimate of hundreds of PC-based programmable logic controllers (PLCs) which would download manufacturing process software over the network. We are concerned about potential security risks. What should we do?

Expert advice to the question is using vulnerability assessment (VA) services. Despite the benefits of going online, being connected also increases the possibilities of getting attacked. There are a variety of automated malicious programs on the internet that can trigger all kinds of attacks, for instance denial of service and backdoor intrusion.

In this regard, VA services offer to scan service ports—including HTTP, SSH, and Windows Update—on networked equipment and produce VA reports. Thanks to ubiquitous network infrastructure, VA services present as a reliable and quick interface medium for all kinds of systems for remote management, system monitoring, data acquisition, and contingency actions.

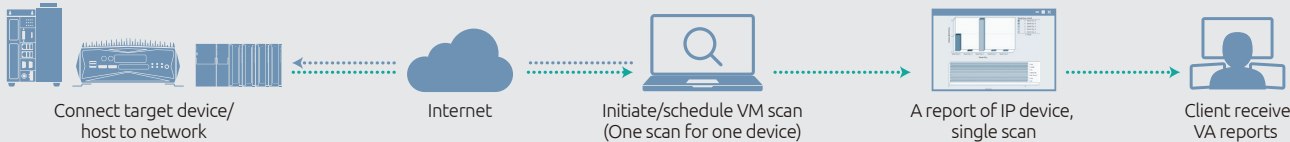


Figure 3. Vulnerability assessment processes.

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

Two major operating systems (OSs) used by industrial automation and control equipment are Windows and Open Linux. These general-purpose OSs activate service ports by default. However, not all equipment is protected and therefore exposed to security loopholes like unchanged default factory passwords and security exploits in known versions of operating systems.

Using VA tools offered by world-renowned vendors, such as Qualys, users can perform VA by taking four simple steps (Figure 3). Compared with complex penetration tests, VA services are a fast and economical way to assess systemic risks.

- Connect target devices to the network
- Initiate VA services
- Set VA schedules
- Receive VA reports

### iNAS Features

#### Link Aggregation

- Balance-rr
- Active Backup
- Balance-xor
- Broadcast
- IEEE 802.3ad
- Balance-tlb
- Balance-alb

#### RAID Level

- JBOD
- RAID 0
- RAID 1
- RAID 5

#### Firmware Upgrade

- Via System Web UI

#### Backup Solutions

- Remote Backup
- System Configuration Backup (Stage II)

#### FTP/SAMBA/AFP/ACL

#### AES Volume Encryption

- Yes (Stage II)

#### Green Power Management

#### Client O.S. Support

- Windows 7+
- Windows Server 2003 R2
- Windows Server 2008, 2008 R2 & 2012 or Later
- Linux & UNIX
- Mac OS X 10.7 or Later





#### Web Browsers Support


- Internet Explorer IE 9.0 Later
- Mozilla Firefox
- Apple Safari
- Google Chrome

#### Networking Support

- HTTP/HTTPS
- Samba/CIFS
- NFSv4
- AFP (v3.3)
- SNMP (v3)
- FTP
- TLS 1.0
- TLS 1.2
- TCP/IP
- IPv4/IPv6
- IEEE 802.3x

## Product Selection Guide

Model Name	Industry Firewall Multi-port VPN Router			VPN Dispatcher
	IFA 1610	IFA 2610	IFA 3610	IVD 1000-S/A
Photo				
Network Security	Yes	Yes	Yes	Yes
VPN Connections	Unlimited	Unlimited	Unlimited	25/100 Licenses
VPN Function	Client/ Site-to-Site	Client/ Site-to-Site	Client/ Site-to-Site	VPN Management
LAN Bypass	-	-	Yes	Yes
High Availability	-	Yes	Yes	Yes
WAN Failover	-	Yes	Yes	Yes
Network Address Translation	Yes	Yes	Yes	Yes
Routing	-	Yes	Yes	Yes
Logging/ Reporting	Yes	Yes	Yes	Yes
Updates and Backup	Yes	Yes	Yes	Yes
Centralized Management	Yes	Yes	Yes	Yes
Hardware Specification				
Mounting	Wall Mount/ Desktop	Wall Mount/ DIN Rail	Wall Mount/ DIN Rail	Rack Mount
Power Input	24V DC Terminal/ DC Jack Input	24V DC Input	Dual 24V DC Input	65W Power Supply
CPU	ARM® Cortex™ A8	ARM® Cortex™ A8	ARM® Cortex™ A8	Intel® Atom™
Memory	512MB	512MB	512MB	1GB
Ethernet	2 x 110/100/1000 Mbps	3 x 10/100/1000 Mbps	5 x 10/100/1000 Mbps	6 x 10/100/1000 Mbps
Serial Communication	RS232/485/422	RS232/485/422	RS232/485/422	Console Port
USB	2 x USB	1 x USB	1 x USB	2 x USB
Digital Input/ Output	-	1 x D1/1 x DO	1 x D1/1 x DO	-
Storage	MicroSD 4GB	MicroSD 4GB	MicroSD 4GB	2.5" HDD (RAID)
Cooling	Fanless	Fanless	Fanless	-
Dimension (H x W x D) mm	114 x 28 x 100	167 x 59 x 140	167 x 59 x 140	44 x 462 x 238
Operating Temperature	0°C ~ +60°C 32°F ~ +140°F	0°C ~ +60°C 32°F ~ +140°F	-20°C ~ +70°C -4°F ~ +158°F	0°C ~ +40°C 32°F ~ +104°F
Storage Temperature	-20°C ~ +70°C -4°F ~ +158°F	-20°C ~ +70°C -4°F ~ +158°F	-40°C ~ +80°C -40°F ~ +176°F	-20°C ~ +70°C -4°F ~ +158°F
Relative Humidity	Operating 10% ~ 90%, Non-Condensing	Operating 5% ~ 95%, Non-Condensing	Operating 5% ~ 95%, Non-Condensing	Operating 10% ~ 90%, Non-Condensing
SIM Card Holder	-	Yes	Yes	-
Service & Maintenance	3 Years	3 Years	3 Years	3 Years
Regulation				
Safety	UL 508	UL 508	UL 508	UL
Certification	CE/FCC/RoHS	CE/FCC/RoHS	CE/FCC/RoHS	CE/FCC/RoHS
Protection Class	IP 30	IP 30	IP30	-
Ordering Information	10IF0161000X0	10IF0261000X0	10IF0361000X0	TBD

Model Name	Rugged Industry Network-Attached Storage iNAS 330
Photo	
Hardware Specification	
CPU/Memory	ARM® Dual Cortex®-A9 CPU; Onboard 4G eMMC; 512MB DDRIII
Disk/ Max Capacity	Up to 3 x 2.5" HDD/SSD; Up to 3T
LEDs	Power LED/System LED/PoE/ Temp LED/HDD LED/LAN LED
Ethernet	2 x Gigabit LAN Ports for Data & PoE Redundancy (M12)
	1 x Gigabit LAN Port for Management (M12)
Power Supply	PoE (IEEE 802.3af)/ PoE+ (IEEE 802.3at)
Reset Button	Reset to Factory Default (Pressing and Holding the Reset Button for 5 Seconds will Reset to Factory Default)
System Dimensions (H x W x D) mm	60 x 246 x 194 (2.36" x 9.69" x 7.64")
Vibration/ Tem. Protection	Yes
Heating Solution	Yes
Housing	Metal, Aluminum, Fanless
Mounting	Wall Mount Kit (Optional)
Environmental Limits	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
Service & Maintenance	3 Years
Regulation	
Compliance	*EN50155 (Railway Applications); IEC61373 (Vibrations & Shocks); EN60950 *EN61000 (Immunity, Emission); EN60068-2-32/IEC68-2-32 (Environmental Testing)
Certification	*FCC/CE/RoHS/WEEE
IP Rating	IP 54 (NEMA)
Ordering Information	10IG0033000X0*

\*Available in Q4

# IFA 1610

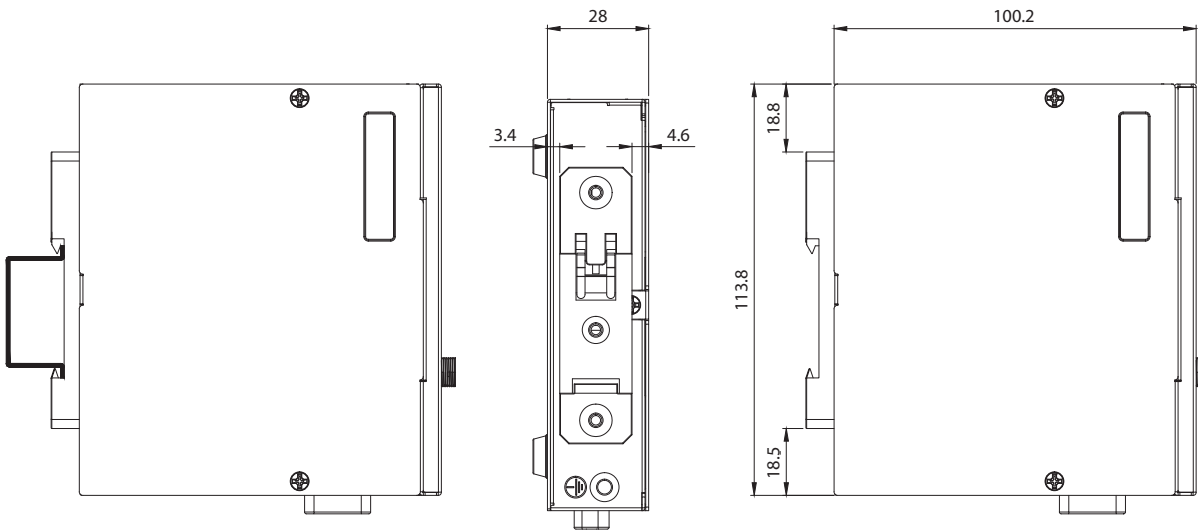
CoreFort™ Industry Firewall, 2 Ports VPN Router



### 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

### Dimension Drawing



### Product Overview

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

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

### Specifications

#### Network Security

- Stateful packet firewall
- Intrusion detection/prevention (IDS/IPS)
- Multiple public IPs
- SNMP support (V1/V2/V3)
- VoIP/SIP support
- Portscan detection
- DoS and DDoS protection
- SYN/ICMP flood protection
- DNS proxy/routing

- 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)

- IPsec
  - Encryption: 3DES, AES 128/256-bit,MD5, SHA1
  - Diffie Hellman (2, 5, 14, 15, 16,17,18)
  - Authentication: Pre-Shared Key, RSA Keys X.509-certificates IKEv1, L2TP
  - DPD (dead peer detection)
  - NAT Traversal
  - Compression
  - PFS (perfect forward secrecy)
  - VPN: site-to-site
  - VPN: client-to-site (road warrior)
  - Integrated certificate authority

#### WAN

- Supports uplinks/WANs: Ethernet (Static/DHCP), PPPoE

#### Traffic Shaping

- Bandwidth management

#### User Authentication

- Active directory/NTLM
- LDAP
- Local

#### Network Address Translation

- Destination NAT
- Incoming routed traffic

- True SSL/TLS VPN (OpenVPN)
  - Encryption: DES, 3DES, AES 128/192/256-bit, CAST5, Blowfish
  - Authentication: Pre-shared key, X.509-certificates , certification authority, and local
  - Support for VPN over HTTPS proxy (OpenVPN)
  - PPTP passthrough
  - VPN: site-to-site
  - VPN: client-to-site (road warrior)
  - VPN client for Microsoft Windows, Mac OS X and Linux
  - Multiple logins per user

#### Services

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

#### Logs and Reports

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

#### Management

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

#### 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 WAN
- 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)/desktop
- Fanless
- Dimension (H x W x D): 110 x 25.4 x 100mm
- Weight (G.W. Kg): 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~ 58°F)
- Humidity:10%~90%, non-condensing

#### Certification

- Safety: UL 508
- FCC/CE/RoHS

#### Package Content

- IFA1610 x 1
- QIG 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)



Main Features

- Stateful (L4) packet firewall
- Intrusion prevention (IPS)
- SSL VPN secure remote access
- DI/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
- SNMP support (V1/V2/V3)
- VoIP/SIP support
- Portscan 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
- Incoming routed traffic
- One-to-one NAT
- Source NAT (SNAT)
- IPSec NAT Traversal

High Availability

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

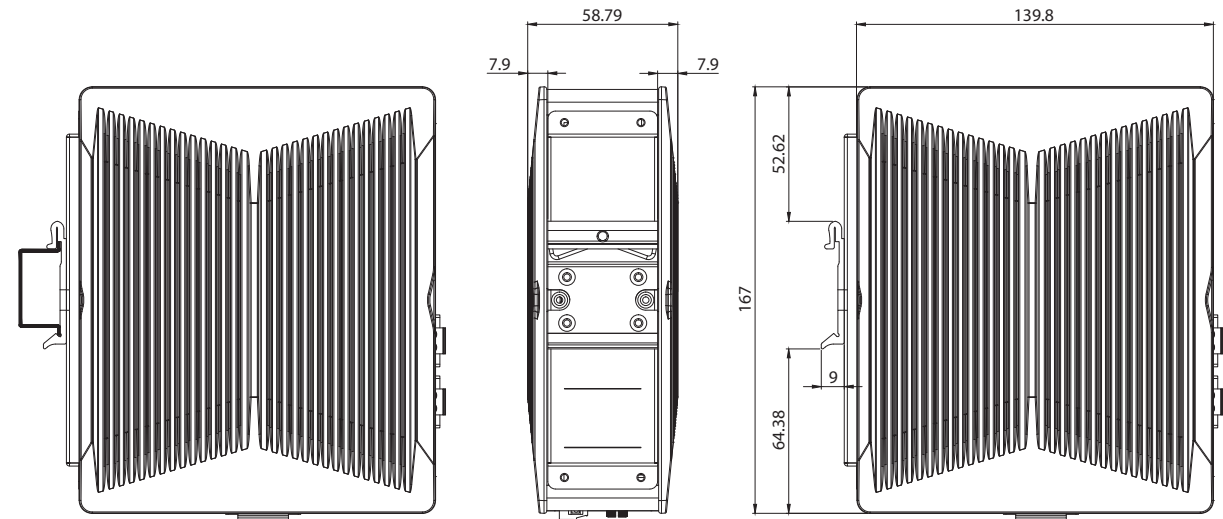
Bridging

- Firewall stealth mode
- OSI-Layer 2 firewall-function
- Spanning tree
- Unlimited bridges
- Unlimited interfaces per bridge

VPN (Virtual Private Network)

- IPsec
  - Encryption: 3DES, AES 128/256-bit,MD5, SHA1
  - Diffie hellman (2, 5, 14, 15, 16,17,18)
  - Authentication: Pre-shared key, RSA keys X.509-certificates IKEv1, L2TP
  - DPD (Dead Peer Detection)
  - NAT Traversal
  - Compression

Dimension Drawing



- PFS (Perfect Forward Secrecy)
- VPN: site-to-site
- VPN: client-to-site (road warrior)
- Integrated certificate authority
- True SSL/TLS VPN (OpenVPN)
  - Encryption: DES, 3DES, AES 128/192/256-bit, CAST5, Blowfish
  - Authentication: pre-shared key, X.509-certificates , certification authority, and local
  - Support for VPN over HTTPS proxy (OpenVPN)
  - PPTP passthrough
  - VPN: site-to-site
  - VPN: client-to-site (road warrior)
  - VPN: client for Microsoft Windows, Mac OS X and Linux
  - Multiple logins per user
  - VPN failover

Services

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

Logs and Reports

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

Management

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

Updates and Backup

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

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 DI/DO
- 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 140mm
- Weight (G.W. Kg): 1.90Kg
- IP30
- 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: 5%~95%, non-condensing

Certification

- Safety: UL 508
- FCC/CE/RoHS

Package Content

- IFA 2610 x 1
- QIG x 1
- Power input 5.08mm terminal block x 1
- DI/DO terminal block x 1

Ordering Information

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



# IFA 3610

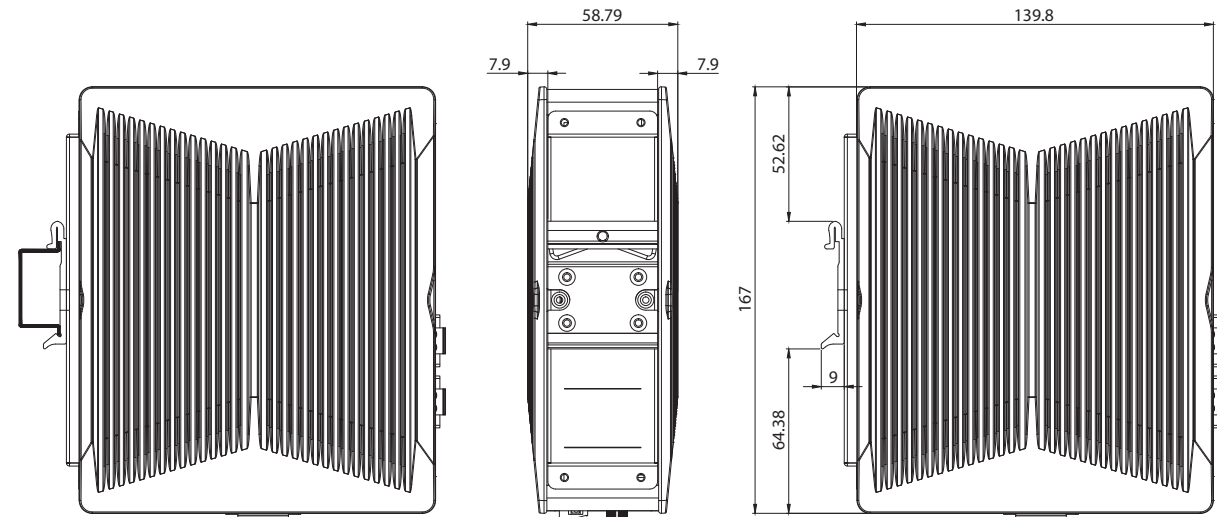
CoreFort™ Industry Firewall, 5 Ports VPN Router  
with Wide Temperature Range



### Main Features

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

### Dimension Drawing



### Product Overview

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

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

### Specifications

#### Network Security

- Stateful packet firewall
- Intrusion detection/prevention (IDS/IPS)
- Multiple public IPs
- SNMP support (V1/V2/V3)
- VoIP/SIP support
- Portscan 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
- 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
- OSI-layer 2 firewall-function
- Spanning tree
- Unlimited bridges
- Unlimited interfaces per bridge

#### VPN (Virtual Private Network)

- IPsec
  - Encryption: 3DES, AES 128/256-bit,MD5, SHA1
  - Diffie Hellman (2, 5, 14, 15, 16,17,18)
  - Authentication: Pre-Shared Key, RSA Keys X.509-certificates IKEv1, L2TP
  - DPD (Dead Peer Detection)
  - NAT Traversal
  - Compression
  - PFS (Perfect Forward Secrecy)

- VPN: site-to-site
- VPN: client-to-site (road warrior)
- Integrated certificate authority
- True SSL/TLS VPN (OpenVPN)
  - Encryption: DES, 3DES, AES 128/192/256-bit, CAST5, Blowfish
  - Authentication: Pre-shared key, X.509-certificates , certification authority, and local
  - Support for VPN over HTTPS proxy (OpenVPN)
  - PPTP passthrough
  - VPN: site-to-site
  - VPN: client-to-site (road warrior)
  - VPN: client for Microsoft Windows, Mac OS X and Linux
  - Multiple logins per user
  - VPN failover

#### Services

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

#### Logs and Reports

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

#### Management

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

#### Updates and Backup

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

#### Routing

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

#### Hardware Specification

- 1 x 10/100/1000 Base-T Ethernet WAN
- 4 x 10/100/1000 Base-T Ethernet LAN
- 1 x USB
- 1 x DI/DO
- RS-232/422/485
- microSD 4GB

#### Physical and Power

- DIN rail/wall mount (optional)
- Fanless
- Dimension (H x W x D): 167mm x 59mm x 140mm
- Weight (G.S. Kg): 1.90Kg
- IP30
- Dual power input 24VDC

#### Environmental Specification

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

#### Certification

- Safety: UL 508
- FCC/CE/RoHS

#### Package Content

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

### Ordering Information

- IFA 3610 (P/N: 10IF0361000X0)  
Industry firewall 5 ports VPN router (3 years service & maintenance)



Main Features

- Fully-integrated VPN server
- Stateful (L4) packet firewall
- SSL VPN secure remote access
- Serial gateway (RS485)
- Up to 25/100 concurrent licenses
- Redundant storage (RAID1)

Product Overview

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

Specifications

Network Security

- Stateful packet firewall
- Intrusion detection/prevention (IDS/IPS)
- Multiple public IPs
- SNMP support (V1/V2/V3)
- VoIP/SIP support
- Portscan 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
- 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
- OSI-layer 2 firewall-function
- Spanning tree
- Unlimited bridges
- Unlimited interfaces per bridge

VPN (Virtual Private Network)

- IPsec
  - Encryption: 3DES, AES 128/256-bit,MD5, SHA1
  - Diffie hellman (2, 5, 14, 15, 16,17,18)
  - Authentication: pre-shared key, RSA keys X.509-certificates IKEv1, L2TP
  - DPD (Dead Peer Detection)
  - NAT Traversal
  - Compression
  - PFS (Perfect Forward Secrecy)
  - VPN: site-to-site
  - VPN: client-to-site (road warrior)
  - Integrated certificate authority
- True SSL/TLS VPN (OpenVPN)
  - Encryption: DES, 3DES, AES 128/192/256-bit, CAST5, Blowfish
  - Authentication: pre-shared key, X.509-certificates, certification authority, and local
  - Support for VPN over HTTPS proxy (openVPN)

- PPTP passthrough
- VPN: client-to-Site (road warrior)
- VPN: client for Microsoft Windows, Mac OS X and Linux
- Multiple logins per user
- VPN failover

Services

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

Logs and Reports

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

Management

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

Updates and Backup

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

Routing

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

Hardware Specification

- Intel® Atom™ CPU
- 6 x 10/100/1000 Base-T Ethernet
- 2 x USB
- 1 x Console port
- 2 x 2.5" HDD (RAID1)

Physical and Power

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

Environmental Specification

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

Certification

- FCC/CE/RoHS

Package Content

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

Ordering Information

- IVD 1000-S (P/N: TBD)**  
VPN dispatcher server with 25 licenses  
stateful packet firewall, SSL VPN, unified VPN management  
(3 years services & maintenance)



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)

Product Overview

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

Furthermore, it offers several data backup options. It supports FTP service and SMB/CIFS protocol for file sharing among cross-platforms.

Atlas OS™ provides real-time information, toolkit, widgets and easy mode of operation; software center provides more application extensions in the future, based on application requirements. iNAS330 also can be networking surveillance storage, with high-resolution camera, the file system could be used on video recording which supports RAID 5 and also that offers the better data protection.

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

Specifications

Hardware Features

- Computer
  - Processor: Dual Cortex®-A9 CPU
  - Storage: Up to 3 x 2.5" HDD/SSD (optional)

Ethernet

- 2 x Gigabit LAN ports for data redundancy (M12)
- 1 x Gigabit LAN port for management (M12)

Button

- Reset button: Reboot System/Reset to factory default

LEDs

- Power LED: power On/Off
- System LED: system status
- PoE/Temp LED: PoE/Temp status
- HDD LED: HDD1, HDD2,HDD3 (read/write/fail)
- LAN LED: 10/100/1000M x3 (link/activity)

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

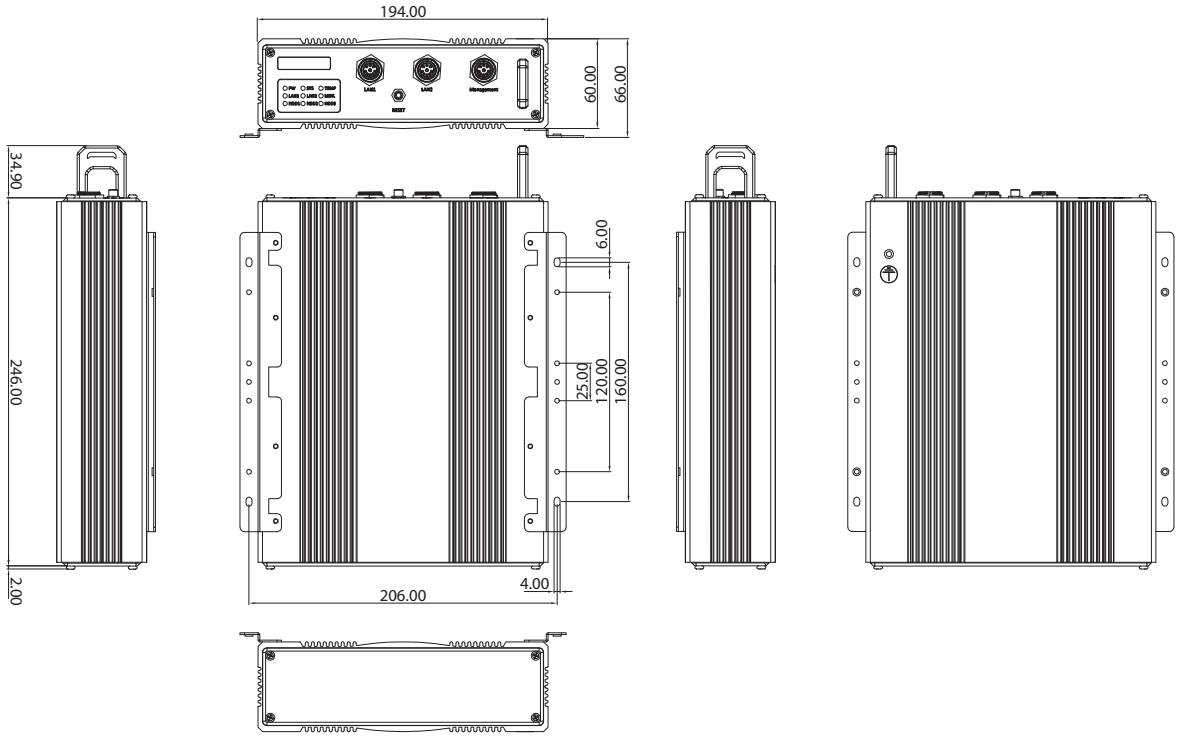
Certifications

- FCC/CE
- RoHS/WEEE

Compliance

- EN50155 (railway applications)
- IEC61373 (vibrations & Shocks)
- EN60950; EN61000 (immunity, emission)
- EN60068-2-30/IEC68-2-30 (environmental testing)

Dimension Drawing



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 IP67

System Dimensions

- 246mm (w) x 194mm (D) x 60mm (H) (9.69" x 7.64" x 2.36")

Software Features

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

Client O.S. support

- Windows 7+, Windows Server 2003 R2, 2008, 2008 R2 & 2012 or later
- Linux & UNIX
- Mac OS X 10.7 or later

Web Browsers Support

- Mozilla Firefox
- Mac Safari
- Google Chrome
- Opera

Protocol

- HTTP/H - SAMBA 2 (CIFS),Open SSL (TLS),FTP / FTPS
- HTTP 1.1 / HTTPS
- IPv4,Link Aggregation, DHCP,NTP,HTTP Authentication
- RESTful API

Ordering Information

- iNAS330 (P/N: 101G0033000X0)  
Rugged-design industry storage (3-years service & maintenance)

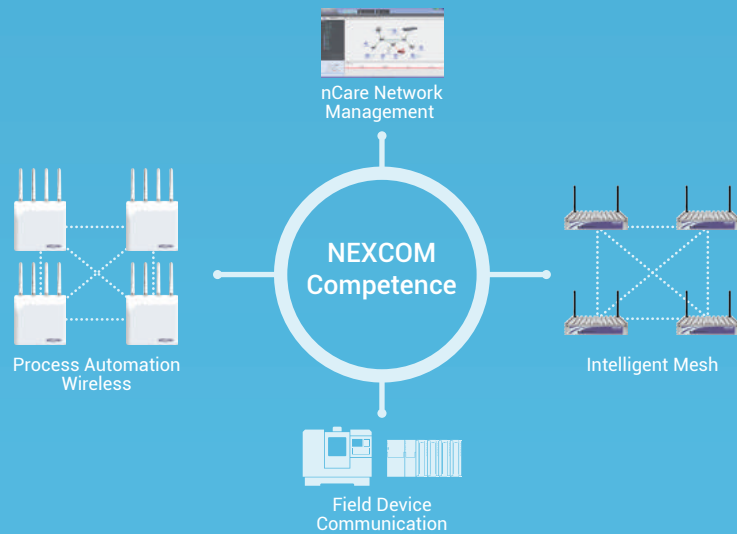


# Industry 4.0 Wireless Solution (IWS)

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

Figure 1. NEXCOM wireless solution competence.



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 Application Layer, Communication Layer and Device Layer and fulfills the following the 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

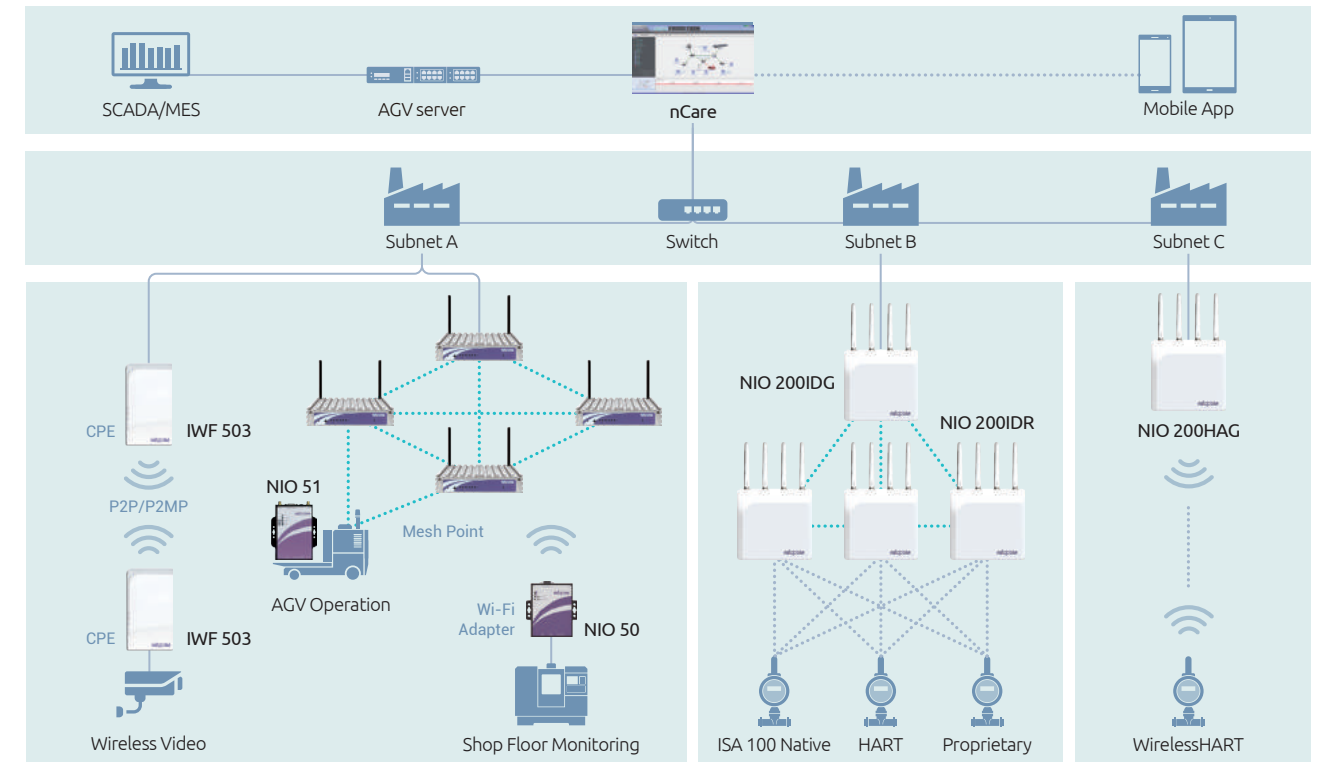


Figure 2. A digital factory implementing NEXCOM's complete I4.0 wireless solution.

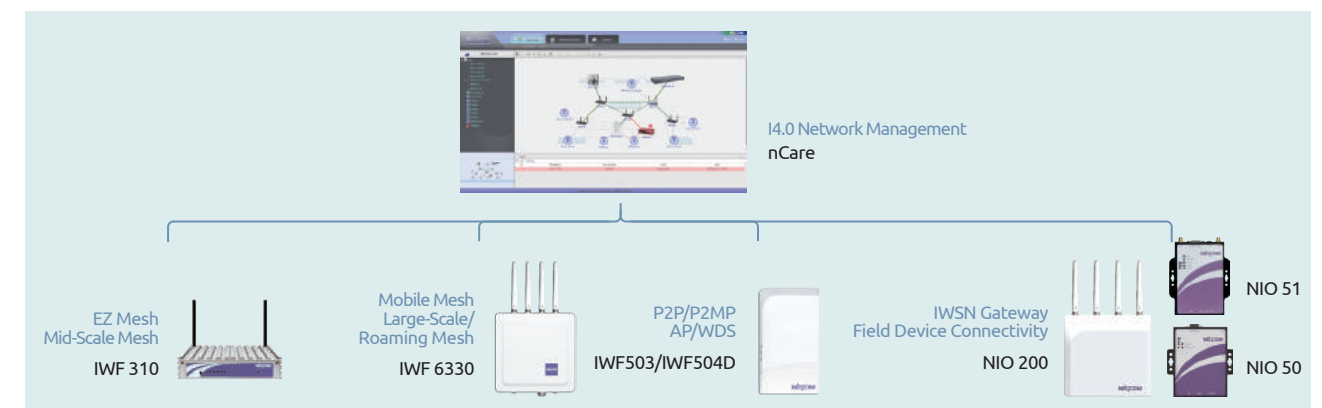
reliability required for a dedicated, always-on industrial Wi-Fi network.

- **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 of the entire enterprise network to help facilitate the network installation, operation, maintenance, troubleshooting process as well as field device platform health monitoring.
- **Field device communication:** NEXCOM's I4.0 wireless solutions support a diverse range of wireless device gateways to bring the field data from different devices to management

level through different industrial protocols such as Modbus, HART and Fieldbus protocols.

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

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.
- Manage a wireless network can be a daunting undertaking for AGV SI and their clients.

### NEXCOM Solution Advantage

- Automatic routing to the most optimal mesh path ensures AGVs are connected to the link with the best possible signal strength.
- Support remote management through NEXCOM nCare, allowing administrators to easily monitor and manage the status of the wireless network and AGVs.
- Mesh points can link neighboring IWF 310 and NIO51 to allow the Wi-Fi coverage to elastically expand to the whole operation area of AGVs.
- Industrial grade rugged design include metal chassis' wide temperature and high EMC level protection to fulfill harsh environment inside AGV.

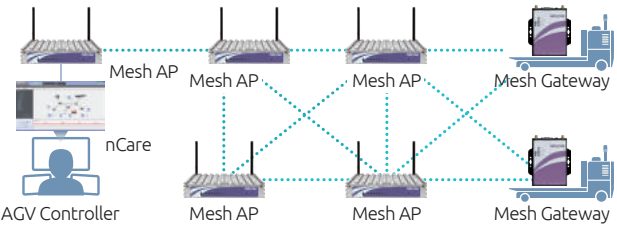


Figure 4. Advanced mesh network of AGVs and APs.

## Process Automation Monitoring

Vertical industrial applications such as chemical, oil and gas processing require strict monitoring and management of manufacturing processes. Pipeline conditions, tank levels and other critical processes require close surveillance to ensure smooth ongoing operations. Due to the strict nature of these applications, most field devices use industrial protocols that deliver transmission reliability and low latency characteristics. Two of the most common protocols are ISA100 and WirelessHART. To respond to this demand, NEXCOM's NIO 200 series of IoT gateways offers ISA100 and WirelessHART support, and features C1D2 and ATEX certifications for reliable operation in process automation environments (Figure 5).

### Application Challenges

- Most wireless process automation networks are based on an All-in-One Gateway topology which lacks the flexibility to scale in size.
- All outbound connections for the field network are restricted

to a single wired Ethernet interface, limiting flexible network deployment options.

- Limited RF sensitivity reduces the distance of wireless network coverage, requiring the use of additional repeaters.

### NEXCOM Solution Advantages

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

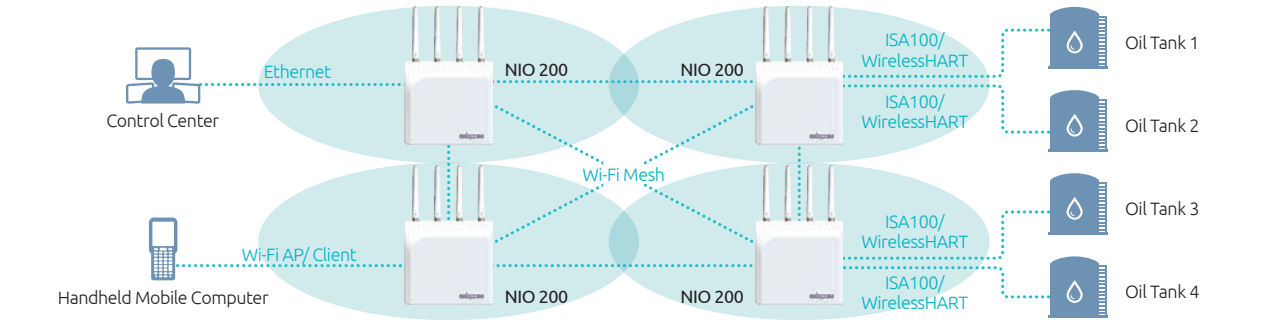


Figure 5. Tank level monitoring and measurement.

## 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 (PtMP) video surveillance applications (Figure 6).

### Application Challenge

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

### NEXCOM Solution Advantages

- NEXCOM's industrial grade Wi-Fi based on IEEE 802.11ac delivers wireless performance at up to Gigabit speeds, and features high-

power radio modules to cover a wide transmission distance.

- IP55-rated waterproof and dust protection, and wide operating temperature range for reliable operation in both outdoor and industrial environments.
- Feature nCare software support for remote management and monitoring of the network and devices in the wireless video surveillance system.

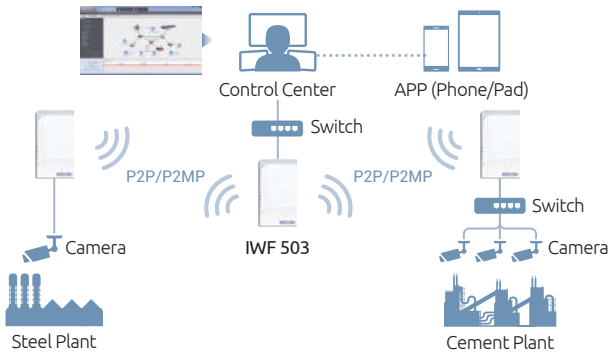


Figure 6. Wireless video surveillance system layout.

## Plant Floor Monitoring

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

### Application Challenge

- Using an Ethernet-based wired backbone limits the flexibility to expand the network to accommodate extra manufacturing capacity.

- Devices in areas with wiring constraints prevent remote management and device health monitoring.
- Require a multi-protocol gateway to connect low layer field devices to higher layer networks for upper management supervision.

### NEXCOM Solution Advantage

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

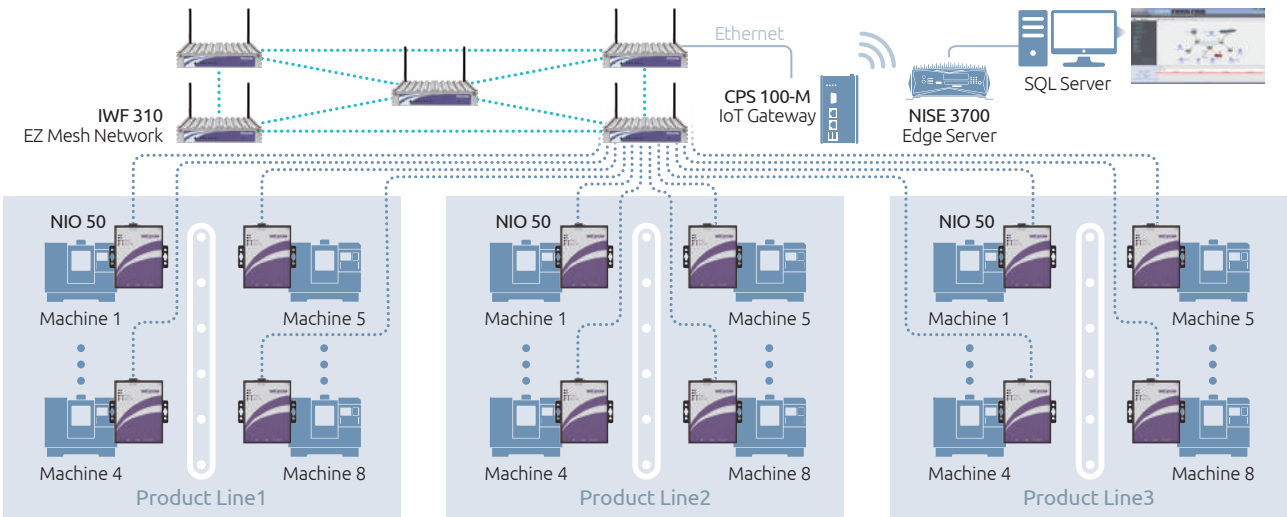


Figure 7. Plant floor monitoring system layout.

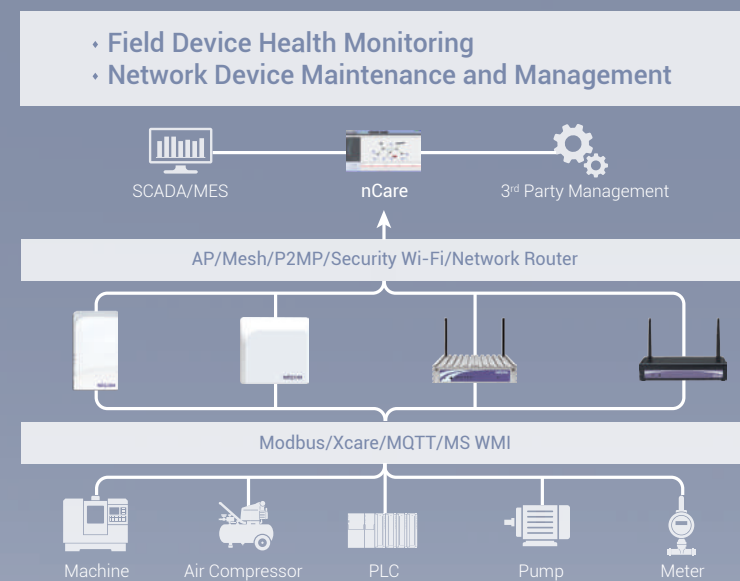


# nCare I4.0 Network Management Solution

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

Figure 1. nCare Node and Network Health Management Solution.



devices running proprietary protocols. Vital health data from devices in the lower layer network can be retrieved and transferred through the backbone network to nCare for device health management.

NEXCOM's IWF 800 nCare Edition is a fully integrated 1U industrial grade network appliance featuring nCare that supports centralized management of up to 1000 nodes, which can be further scaled for future expansions. A free license for a 30-day trial version is also available upon request.

## nCare Highlights

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

## Features & Benefits

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

### Flexible Visualization of Network Topology

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

- **Complete visual mapping:** The development of globalization has increased the number of factories built across the globe. Therefore, utilizing a map integrated with floor plans of factories as visual representations of the entire topology is the most efficient way for managing large-scale systems. nCare incorporates Google Maps and Baidu Maps to offer accurate map data from any location. For visualization of the interiors of factory plant floors, nCare can categorize devices on different floor levels to different groups. A total of up to 15-story floor plans can be supported to fulfill mass requirements (Figure 5).

### Device Health Management from Top to Bottom

- Devices can be managed in real-time through layered security mechanism to carry out surveillance, maintenance, troubleshooting and updating tasks. The basic management items of nCare include the following:
  - Provisioning & configuration
  - Configuration backup & restore
  - Remote AP reboot/device reset
  - Mobile management through App (Figure 2)
- nCare connects to lower layer devices using industrial protocols for system monitoring and management (Figure 6). For example, NEXCOM's industrial fanless computers with NEXCOM Xcare™ support can be managed by nCare to give administrators hardware visibility and control. The following configuration items and hardware health status are available for NEXCOM Xcare-

enabled devices:

- CPU usage, system temperature, memory usage & storage life cycle
- Device image upgrade & provisioning
- Remote reboot
- Warning notification

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).

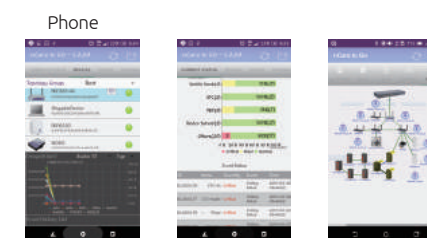


Figure 2

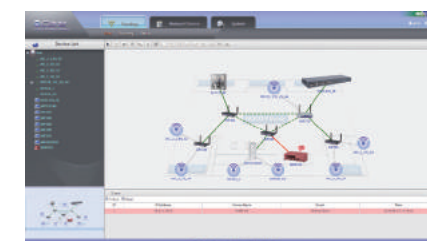


Figure 3



Figure 4

Figure 2. Mobile App for remote management.

Figure 3. Automatic alerts of abnormal events.

Figure 4. nCare categorizes severity of issues based on the warning information received.

Figure 5. Support Industrial Switch topology and alarm.

Figure 6. Commonly used configuration items help improve device deployment efficiency.

Figure 7. Support a variety of industrial protocols to provide management for a wide range of devices.

Figure 8. nCare provides alert notifications to users through email, SMS and social media.

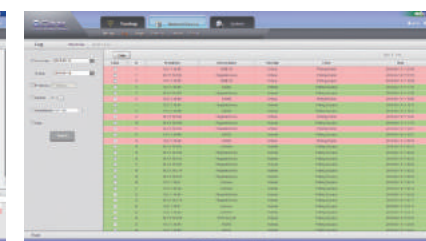


Figure 3



Figure 4

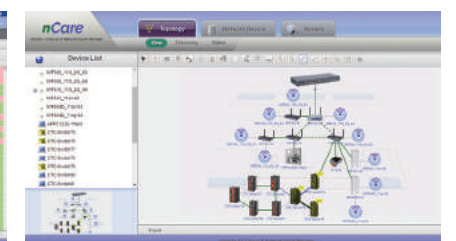


Figure 5

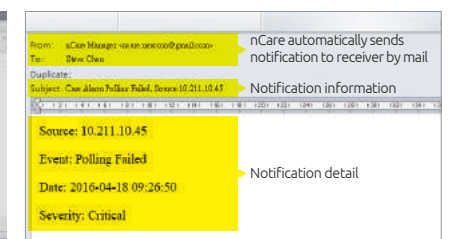


Figure 6

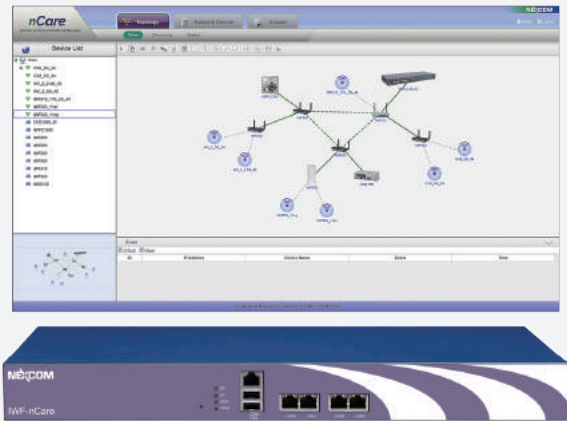


Figure 7



Figure 8





Main Features

- Automatically discover managed devices by SNMP, CAPWAP & Modbus scan
- Visual topology to display device and wireless link status for remote management
- Supports Modbus TCP protocol to communicate with Modbus device for asset management
- Easy remote provisioning, configuration, firmware upgrade and reboot for NEXCOM IWF devices
- Flexible events and notifications with pre-defined threshold
- Supports third-party devices with MIB compiler and MIB browser
- Comprehensive report and log, including asset status, system log and usage report
- Supports smart phone/tablet APP for mobile management
- Support API, customization service for management of private protocol communication
- Co-existing with 3rd party management solution through standard, open interface
- Management scope can be up to 6,000 nodes

Product Overview

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

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

Specifications

nCare Manager Platform Requirement

Operating System

- Windows 7 (64-bit)
- VM supported by project base

Hardware

- CPU support: Intel® Atom™ Quad-core 2.4GHz
- Main memory: 8GB memory with DDR3 1600MHz Long-DIMM sockets
- I/O interface-front
  - 2 x USB 2.0 ports
  - 1 x RJ45 type console port
  - 4 x GbE copper ports
  - 1 x reset button
- I/O interface-rear
  - 2 x USB 2.0 ports
  - 1 x VGA port
- HDD storage: 500GB

Client Platform Requirement

PC System

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

Functionality

Auto Discovery

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

Visual Topology

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

AP/Mesh Networking Device Management (Only to NEXCOM IWF)

- Provisioning & configure
- Configuration setting backup & restore
- Restore to factory default
- Remote AP reboot/reset
- Firmware upgrade thru manual/batch/schedule\*\*

Device Node Management

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

Report & Log

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

Event Notification

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

Administration

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

Physical

- 1U 19" rack mount, 430mm x 260mm x 44mm
- Net weight: 5kg
- Operating temperatures: 0°C~40°C
- Storage temperature: -20°C~75°C
- Relative humidity: 10%~90% non-condensing
- Certifications: CE/ FCC

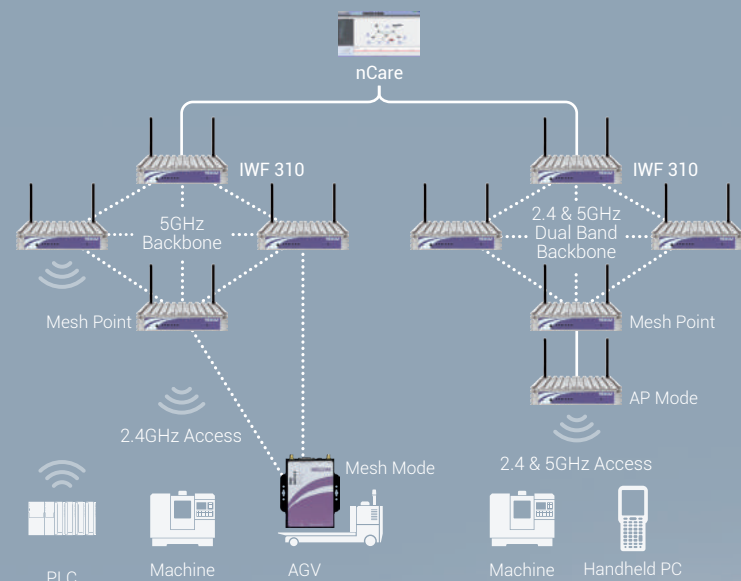
Ordering Information

- IWF 800 nCare, I4.0 node and network manager (P/N: 10T0NCARE00X0)

# Trusted Industrial Wi-Fi Mesh Network

Stable network transmission is one of the most crucial requirements for Industry 4.0 (I4.0). NEXCOM's industrial Wi-Fi mesh products offer a unique wireless mesh solution utilizing self-forming and self-healing technology to create a reliable wireless backbone network (Figure 1). When interferences to the transmission signal of a mesh path are present, NEXCOM's mesh technology will adapt and reroute 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 redundant mesh backbone or Hybrid Mesh + AP topology for connecting Wi-Fi clients to the internet (Figure 1).

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



## 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 802.11an 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

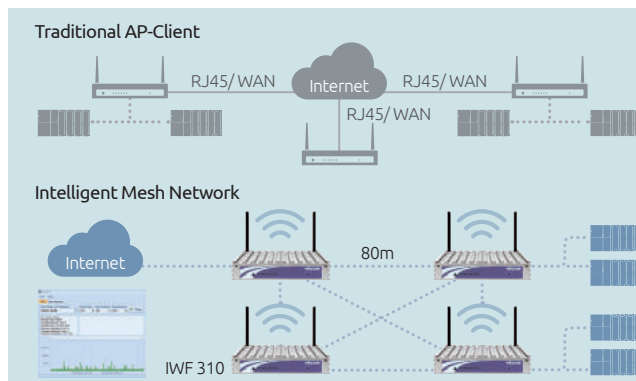


Figure 2. Traditional AP-client mode is linked with a single path. NEXCOM's EZ Mesh provides multiple paths for highest link reliability, which results in the lowest amount of packet loss.

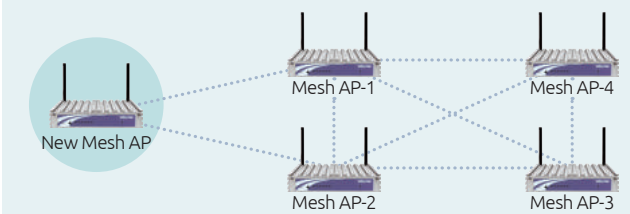


Figure 4. EZ Mesh offers easy scale-up flexibility. New mesh APs can be scanned and joined to the network automatically. Additional mesh APs can make mesh links more reliable.

also features high resistance to any potential radio interference that may be present in industrial environments. Designed with transmission reliability in mind, EZ Mesh enables factory operators to build a stable and capable wireless IoT network backbone.

#### EZ Mesh Highlights

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

## EZ Mesh Application in Factories

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

#### Requirements of the application:

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

#### NEXCOM's EZ Mesh solution:

- IWF 300 and IWF 310 offer industrial grade reliability with wide operating temperature ranges for industrial factory

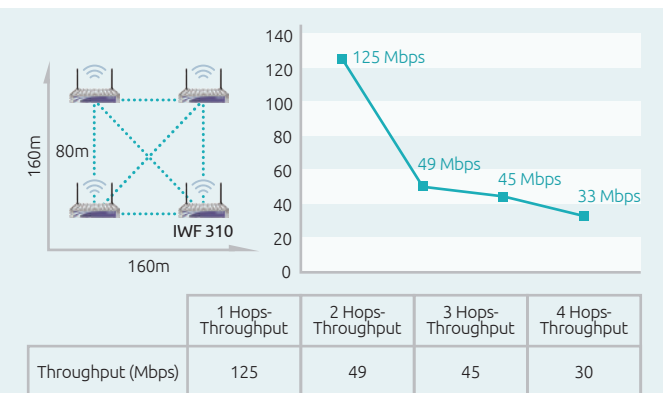


Figure 3. 4-device mesh network in 160m<sup>2</sup> space and 4-hop coverage and performance figures.

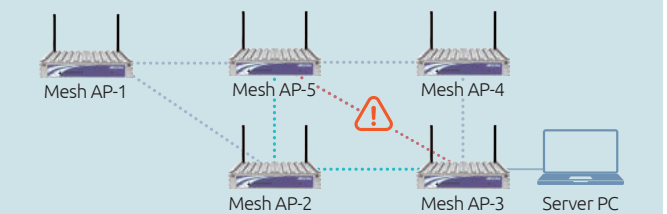


Figure 5. EZ Mesh topology provides self-forming and self-healing benefits to form an automatically connected/ maintained network.

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.

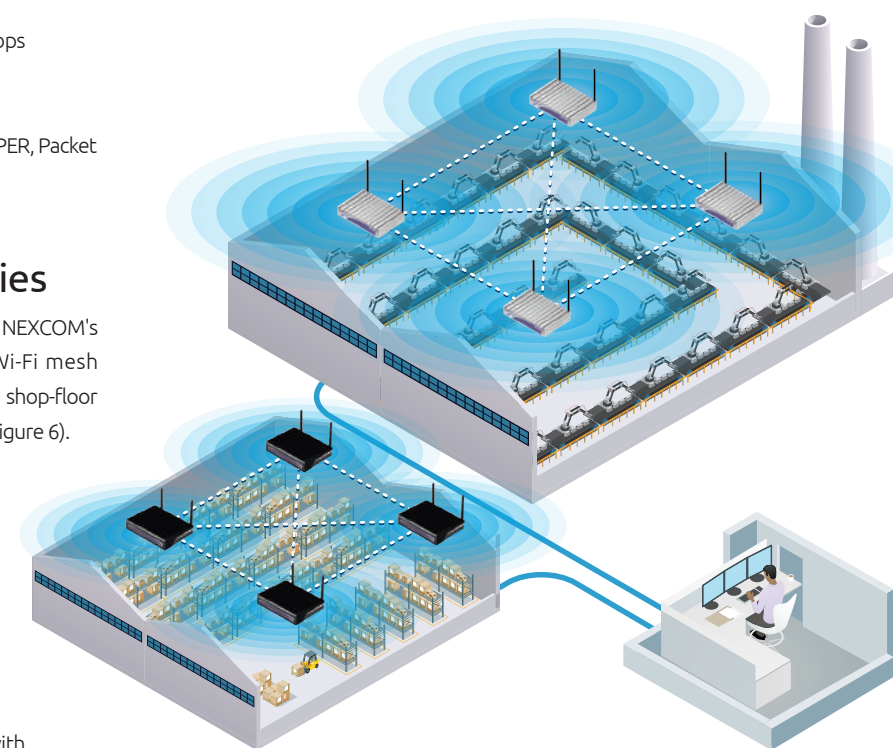


Figure 6. EZ Mesh application scenario.



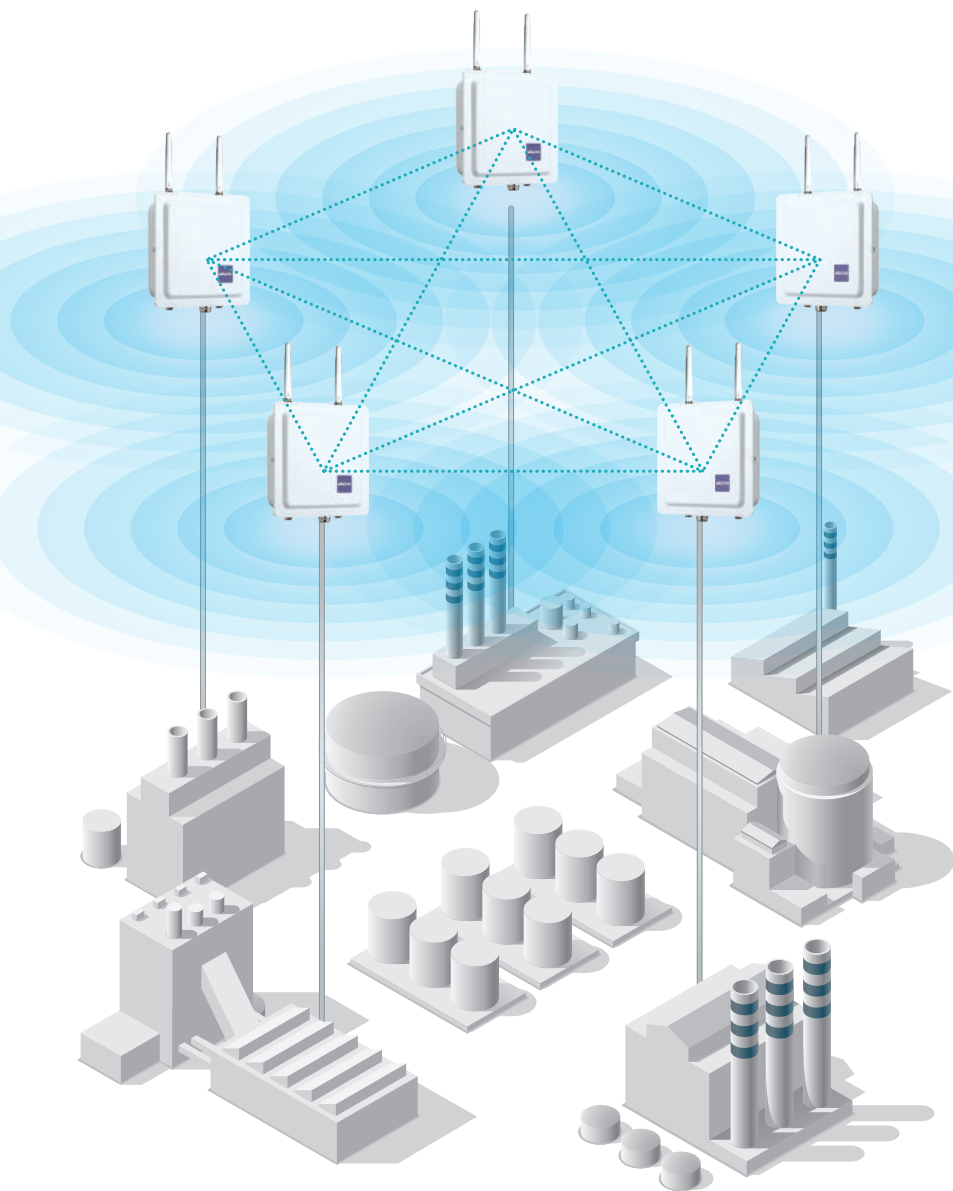
Mobile Mesh Wi-Fi Backbone

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

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 Mesh Wi-Fi feature a dual and triple RF module design respectively, and are based on IEEE 802.11n with 2x2 MIMO technology. IWF 3310X, on the other hand, is an industrial Wi-Fi with EN50155 certification to provide reliable operations for railway applications. Both the IWF 6300 series and IWF 3310 series can be used in conjunction for a variety of Wi-Fi applications.

Mobile Mesh Highlights

- Easy installation & scalability for large-scale deployment
- Multi-path bridge
- Self-forming and Self-healing
- 120Mbps bandwidth capacity after 10+ hops
- Support Mesh/AP/Bridge modes
- IP67, High-power and Dual/Triple RF design



Mobile Mesh Application in Outdoor Environments

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

Requirements of the application:






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

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

Model Name	EZ Mesh Family		Mobile Mesh Family		
	IWF 300	IWF 310	IWF 6320M/H	IWF 6330M/H	IWF 3310XM/H
Photo					
Category	Industrial EZ Mesh AP	Rugged Industrial EZ Mesh AP	Outdoor Mobile Mesh AP	Outdoor Mobile Mesh AP	Industrial Mobile Mesh AP
WLAN Standard	802.11an+b/g/n 2x2 MIMO	802.11an+b/g/n 2x2 MIMO	802.11a/b/g/n 2x2 MIMO	802.11a/b/g/n 2x2 MIMO	802.11a/b/g/n 2x2 MIMO
Number of Radios	2	2	2	3	1
Number of Antenna	2	2	4	6	2
Type of RF Connector	RP-SMA	RP-SMA	N-Type Female	N-Type Female	RP-SMA
Number of WAN Port	1	1	1	1	1
Number of LAN Port	4	4	0	0	0
Type of LAN	RJ45	RJ45	RJ45 (Encapsulated by M25)	RJ45 (Encapsulated by M25)	RJ45
IP Rating	IP30	IP30	IP67	IP67	IP30
Mounting Style	Wall Mount	Wall Mount	Wall/Pole Mount	Wall/Pole Mount	Wall/DIN-Rail Mount
Temperature	-40°C ~ +80°C	-40°C ~ +80°C	-35°C ~ +75°C	-35°C ~ +75°C	-40°C ~ +80°C
Dimension (H x W x D) mm	205 x 105 x 25	185 x 108 x 43	220 x 220 x 77	220 x 220 x 77	58.8 x 139.6 x 167
PoE Input	N/A	N/A	Passive PoE: 48V	Passive PoE: 48V	IEEE802.3at
DC Input	12VDC	12VDC	N/A	N/A	2 x DC Input: +12 ~ +48V
Certification	CE, FCC	CE, FCC	CE, FCC	CE, FCC	CE, FCC, EN50155
Safety	EN60950-1	EN60950-1	EN60950-1	EN60950-1	EN60950-1
Operation Mode	AP/Router/EZ Mesh	AP/Router/EZ Mesh	AP/Station/Mesh* (* Mesh Model Only)	AP/Station/Mesh* (* Mesh Model Only)	AP/Station/Mesh* (* Mesh Model Only)
Management Mode	SNMP/GUI/ nCare Management	SNMP/GUI/ nCare Management	SNMP/GUI/ nCare Management	SNMP/GUI/ nCare Management	SNMP/GUI/ nCare Management



# IWF 300

Industrial Access Point

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



### Main Features

- Dual radios and compliant with 1 x 802.11an+1 x 802.11 b/g/n 2x2 MIMO
- 1+4 port GbE RJ45 ports
- Up to 27dBm high RF power
- Multiple function: AP/Client/WDS/EZ Mesh
- Support 12V DC input
- Support -40~80°C extended operating temperature

### Product Overview

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

### Specifications

#### Wireless Radio

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

#### Frequency Ranges

- USA: 2.400~2.483 GHz, 5.15~5.35 GHz, 5.5~5.7 GHz, 5.725~5.825 GHz
- Europe: 2.400~2.483 GHz, 5.15~5.35 GHz, 5.47~5.725 GHz

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

#### RF Output Power: IEEE 802.11an (±2dBm)

- IEEE802.11a
  - 12dBm@54M
- IEEE802.11an HT20
  - 12dBm@MCS7
- IEEE802.11an HT40
  - 11dBm@MCS7

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

- IEEE802.11b
  - 27dBm@1M
  - 24dBm@11M
- IEEE802.11g
  - 27dBm@6M
  - 24dBm@54M
- IEEE802.11g/n HT20
  - 23dBm@MCS0/8
  - 19dBm@MCS7/15
- IEEE802.11g/n HT40
  - 22dBm@MCS0/8

- 18dBm@MCS7/15

#### Receive Sensitivity: IEEE 802.11an

- IEEE802.11a
  - 76 dBm@54M
- IEEE802.11a/n HT20
  - 74dBm@MCS7
- IEEE802.11a/n HT40
  - 71dBm@MCS7

#### Receive Sensitivity: IEEE 802.11a/b/g/n 2Rx

- IEEE802.11b
  - 93dBm@1M
  - 91dBm@11M
- IEEE802.11g
  - 94dBm@6M
  - 80dBm@54M
- IEEE802.11g/n HT20
  - 94dBm@MCS0/8
  - 77dBm@MCS7/15
- IEEE802.11g/n HT40
  - 89dBm@MCS0/8
  - 73dBm@MCS7/15

#### Hardware

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

- Hardware based 10/100/1000, full/half, flow control auto negotiation
- Push buttons: 1 x reset; 1 x WES
- LED: 1 x Power & Status; 5 x RJ45; 1 x WES
- Dual band antenna: 2 x with RP-SMA connectors

#### Operating Mode

- AP
- AP router
- Client router
- EZ Mesh (at 802.11ac, 5GHz)

#### Security

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

#### System Management

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

#### Built-in Servers & Client Interfaces to Other Services

- DHCP client
- SNMP v1/v2 client (coming soon)

#### Physical and Power

- 12VDC power input

- Wall mountable
- Dimension: 205 x 105 x 25 mm
- Weight: 640g

#### Environment Protection

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

#### Certification

- FCC
- CE
- RoHS compliant

#### Package Contents

- IWF300 unit x 1
- Dual band antenna x 2
- Ethernet cable x 1
- Wall-mount kit x 1
- AC-DC power adaptor x 1

### Ordering Information

- IWF 300-EU (P/N: 10T00030000X0)
- IWF 300-US (P/N: 10T00030001X0)

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

# IWF 310

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



### Main Features

- Dual radios and compliant with 1 x 802.11an+1 x 802.11 b/g/n 2x2 MIMO
- 1+4 port GbE RJ45 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 IEEE802.11an/a 2x2 MIMO technology. IWF 310 can deliver data rate up to 300Mbps/each radio. In addition, the radio power can be up to 27dBm for wide range coverage and service. IWF 310 also functions as EZ Mesh network Wi-Fi access with cost-effective option.

### Specifications

#### Wireless Radio

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

#### Frequency Ranges

- USA: 2.400~2.483 GHz, 5.15~5.35 GHz, 5.5~5.7 GHz, 5.725~5.825 GHz
- Europe: 2.400~2.483 GHz, 5.15~5.35 GHz, 5.47~5.725 GHz

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

#### RF Output Power: IEEE 802.11an (±2dBm)

- IEEE802.11a
  - 27dBm@54M
- IEEE802.11a/n HT20
  - 25dBm@MCS7
- IEEE802.11a/n HT40
  - 24dBm@MCS7

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

- IEEE802.11b
  - 27dBm@1M
  - 24dBm@11M
- IEEE802.11g
  - 27dBm@6M
  - 24dBm@54M
- IEEE802.11g/n HT20
  - 23dBm@MCS0/8
  - 19dBm@MCS7/15

- IEEE802.11g/n HT40
  - 22dBm@MCS0/8
  - 18dBm@MCS7/15

#### Receive Sensitivity: IEEE 802.11an

- IEEE802.11a
  - -76dBm@54M
- IEEE802.11a/n HT20
  - -74dBm@MCS7
- IEEE802.11a/n HT40
  - -71dBm@MCS7

#### Receive Sensitivity: IEEE 802.11 b/g/n

- IEEE802.11b
  - -93dBm@1M
  - -91dBm@11M
- IEEE802.11g
  - -94dBm@6M
  - -80dBm@54M
- IEEE802.11g/n HT20
  - -94dBm@MCS0/8
  - -77dBm@MCS7/15
- IEEE802.11g/n HT40
  - -89dBm@MCS0/8
  - -73dBm@MCS7/15

#### Hardware

- WAN: 10/100/1000 Base-TX MDI/MDIX RJ-45 x 1
- LAN: 10/100/1000 Base-TX MDI/MDIX RJ-45 x 4

- 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; 5 x Ethernet
- Antenna connectors: 2 x with RP-SMA

#### Operating Mode

- AP
- AP router
- Client router
- EZ Mesh

#### Security

- WEP (64/128)
- WPA/WPA2 mixed
- WPA2-personal (PSK+CCMP/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 client(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

- FCC
- CE
- RoHS compliant


#### Package Contents

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

### Ordering Information

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

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



IWF 6320IWF 6330

### Main Features

- Multiple radios and compliant with IEEE 802.11a/b/g/n 2x2 MIMO
- Fast roaming (hand-over switch time less than 20 ms)
- Smart installation utilities: distance calculation, antenna alignment and site survey tools

- 48VDC PoE input
- Gigabit Ethernet waterproof RJ45
- WEP, WPA, WPA2-PSK/EAP (IEEE 802.1X/RADIUS, TKIP and AES)
- Operating temperature range from -35 to 75°C

Product Overview

The IWF 6320/6330 series are enterprise and carrier-grade 802.11n Triple Radios Outdoor Wireless Access Point which offers customer a robust and high performing solution for PTP/PTMP/Hotzone/Hopping/Mesh/Mobility Wi-Fi applications in both license-free 2.4GHz and 5GHz bands.

The IWF 6320/6330 series are the most ideal candidate for Service Providers looking to deliver carrier-grade wireless services to multiple market segments such as Railway train, Bus, MRT fast roaming, campuses Mesh network, hospitality, healthcare, warehousing and wider metropolitan area deployments.

Designed to meet customer needs in a broad range of industries, the IWF 6320/6330 offers the following benefits:

Flexible wireless backbone deployment options

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

High-performance wireless backbone

With the next generation 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.

IWF 6320/6330 Series Category

Model	Radio Spec.
IWF 6320H	Hopping AP, Dual Radios, IEEE 802.11 a/b/g/n Dual-Band 2x2 MIMO, High Power
IWF 6320M	Mesh/Mobility AP, Dual Radios, IEEE 802.11 a/b/g/n Dual-Band 2x2 MIMO, High Power
IWF 6330H	Hopping AP, Triple Radios, IEEE 802.11 a/b/g/n Dual-Band 2 x 2 MIMO, High Power
IWF 6330M	Mesh/Mobility AP, Triple Radios, IEEE 802.11 a/b/g/n Dual-Band 2 x 2 MIMO, High Power

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 ~ 5.85 GHz

RF Output Power: (± 2dBm)

- IEEE 802.11a
  - 24dBm@6M (all)
  - 21dBm@54M (all)
- IEEE 802.11b
  - 24dBm@1M (all)
  - 24dBm@11M (all)

- IEEE 802.11g
  - 25dBm@6M (all)
  - 22dBm@54M (all)
- IEEE 802.11a/n HT20
  - 24dBm@MCS0/8 (all)
  - 18dBm@MCS7/15 (5180MHz)
  - 17dBm@MCS7/15 (5825MHz)
- IEEE 802.11a/n HT40
  - 22dBm@MCS0/8 (all)
  - 17dBm@MCS7/15 (5190MHz)
  - 16dBm@MCS7/15(5795MHz)
- IEEE 802.11g/n HT20
  - 25dBm@MCS0/8 (all)
  - 21dBm@MCS7/15 (all)
- IEEE 802.11g/n HT40
  - 24dBm@MCS0/8 (all)
  - 20dBm@MCS7/15 (all)

Receive Sensitivity

- IEEE 802.11a
  - 82dBm@6M, 1Rx
  - 95/-91dBm@6M, 2Rx
  - 65dBm@54M, 1Rx
  - 79/-75dBm@54M, 2Rx
- IEEE 802.11b
  - 82dBm@1M, 1Rx
  - 92/-88dBm@1M, 2Rx
  - 76dBm@11M, 1Rx
  - 92/-88dBm@11M, 2Rx
- IEEE 802.11g
  - 82dBm@6M, 1Rx
  - 95/-91dBm@6M, 2Rx
  - 65dBm@54M, 1Rx
  - 80/-76dBm@54M, 2Rx
- IEEE 802.11a/n HT20
  - 82dBm@MCS0, 1Rx
  - 95/-91dBm@MCS0, 2Rx
  - 64dBm@MCS7, 1Rx
  - 77/-73dBm@MCS7, 2Rx
- IEEE 802.11a/n HT40
  - 79dBm@MCS0, 1Rx
  - 91/-87dBm@MCS0, 2Rx
  - 61dBm@MCS7, 1Rx
  - 73/-69dBm@MCS7, 2Rx
- IEEE 802.11g/n HT20
  - 82dBm@MCS0, 1Rx
  - 95/-91dBm@MCS0, 2Rx
  - 64dBm@MCS7, 1Rx
  - 77/-73dBm@MCS7, 2Rx
- IEEE 802.11g/n HT40
  - 79dBm@MCS0, 1Rx
  - 92/-88dBm@MCS0, 2Rx
  - 61dBm@MCS7, 1Rx
  - 74/-70dBm@MCS7, 2Rx

Ethernet

- 10/100/1000 Base-TX MDI/MDIX RJ-45 x 1
- Compliant with :
  - IEEE 802.3/802.3u
  - Hardware based 10/100/1000, full/half, flow control auto negotiation

Bridge Mode

- Layer 2 switching learning technology
- Spanning tree protocol -IEEE 802.1d STP/IEEE 802.1w RSTP
- Store-and-Forward
- Static IP
- DHCP server
- IEEE 802.1q tag VLAN
- IEEE 802.1p VLAN priority based QoS

Router Mode

- DHCP server
- RIP
- IP filter
- Port filter
- Port forward
- DMZ support
- Static route

Security

- Hide SSID
- MAC filtering ACL
- WEP 64/128/152 bits
- IEEE 802.1x EAP-TLS/EAP-TTLS/MSCHAPv2/GTC
- WPA/WPA2 PSK/EAP with TKIP/CCMP AES based Encryption

Management

- HTTP(s) Web GUI
- Telnet
- SSH
- CLI commands
- SNNP v2c and V3 standard (Private MIB)
- Syslog
- Layer management utility
- Management VLAN tag
- NTP client
- Firmware upgrade
- Configuration backup and restore
- Factory default configuration

Utility

- Ping test
- RSSI and path loss calculation
- Wireless site survey
- Antenna alignment tool
- System status
- Link information

Advanced Technology

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

Physical and Power

- Support 48VDC power over Ethernet
- Form factor: pole/wall mountable
- Dimension: 220 x 220 x 77 mm
- Weight: 2.0kg (3.7kg mount kit included)
- Outdoor IP67 rated

Environment Protection

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

Ordering Information

- IWF 6320H-US (P/N: 10T00632003X0)
- IWF 6320H-EU (P/N: 10T00632000X0)
- IWF 6320M-US (P/N: 10T00632003X0)
- IWF 6320M-EU (P/N: 10T00632002X0)
- IWF 6330H-US (P/N: 10T00633003X0)
- IWF 6330H-EU (P/N: 10T00633002X0)
- IWF 6330M-US (P/N: 10T00633001X0)
- IWF 6330M-EU (P/N: 10T00633002X0)



IWF 3310XH/XM

Industrial IP30 Hopping/Mesh/Mobility AP/CPE  
Single RF, Dual Band, 802.11 a/b/g/n



Main Features

- Single radios and compliant with IEEE 802.11a/b/g/n 2x2 MIMO
- Fast roaming (hand-over switch time less than 20 ms)
- Installation utilities: antenna alignment, distance calculation and site survey tools
- Compliant with IEEE 802.11a/b/g/n 2x2 MIMO
- 300 Mbps data rate
- 2 x 12~48VDC redundant power
- IEEE 802.3at power over Ethernet
- Gigabit Ethernet RJ45
- WEP, WPA, WPA2-PSK/EAP (IEEE 802.1X/RADIUS, TKIP and AES)
- Operating temperature range from -40 to 80°C
- FCC/CE certification
- EN50155 compliant

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.

The IWF 3310X series are the most ideal candidate for Service Providers looking to deliver carrier-grade wireless services to multiple market segments such as Railway train, Bus, MRT fast roaming, campuses Mesh network, hospitality, healthcare, warehousing and wider metropolitan area deployments.

IWF 3310X Series Category

Model	Radio Spec.
IWF3310XH	Hopping AP/CPE, IEEE 802.11 a/b/g/n dual-band 2x2 MIMO
IWF3310XM	Mesh/Mobility AP/CPE, IEEE 802.11 a/b/g/n dual-band 2x2 MIMO

Specifications

Wireless Radio

- Single 2 x 2 MIMO radio

Frequency Ranges

- USA: 2.400~2.483 GHz, 5.15~5.35 GHz, 5.725~5.825 GHz
- Europe: 2.400~2.483 GHz, 5.15~5.35 GHz, 5.47~5.725 GHz
- Japan: 2.400~2.497 GHz, 5.15~5.35 GHz, 5.47~5.725 GHz
- China: 2.400~2.483 GHz, 5.725~5.85 GHz

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

RF output power: (± 2dBm)

- IEEE 802.11a
  - 21dBm@6M
  - 16dBm@54M
- IEEE 802.11b
  - 21dBm@1M
  - 19dBm@11M
- IEEE 802.11g
  - 23dBm@6M
  - 19dBm@54M

- IEEE 802.11a/n HT20/40
  - 19dBm@MCS0/8
  - 14dBm@MCS7/15
- IEEE 802.11g/n HT20
  - 21dBm@MCS0/8
  - 17dBm@MCS7/15

Receive Sensitivity

- IEEE 802.11a
  - 91dBm@6M
  - 75dBm@54M
- IEEE 802.11b
  - 91dBm@1M
  - 87dBm@11M
- IEEE 802.11g
  - 91dBm@6M
  - 76dBm@54M
- IEEE 802.11a/n HT20/40
  - 95/-91dBm@MCS0/8
  - 77/-73dBm@MCS7/15

- IEEE 802.11g/n HT20/40
  - 95/-91dBm@MCS0/8
  - 79/-75dBm@MCS7/15

Ethernet

- 10/100/1000 Base-TX MDI/MDI-X RJ-45 x 1
- Compliant with
  - IEEE 802.3/802.3u
  - Hardware based 10/100/1000, full/half, flow control auto negotiation

Bridge Mode

- Layer 2 switching learning technology
- Spanning tree protocol -IEEE 802.1d STP/IEEE 802.1w RSTP
- Store-and-forward
- Static IP
- DHCP server
- IEEE 802.1q tag VLAN
- IEEE 802.1p VLAN priority Based QoS

Router Mode

- DHCP server
- RIP
- IP filter
- Port filter
- Port forward
- DMZ support
- Static route

Security

- Hide SSID
- MAC Filtering ACL
- WEP 64/128/152-bit
- IEEE 802.1 x EAP-TLS/EAP-TTLS/MSCHAPv2/GTC
- WPA/WPA2 PSK/EAP with TKIP/CCMP AES based encryption

Management

- HTTP(s) Web GUI
- Telnet
- SSH
- CLI commands
- SNMP v2c and V3 standard (private MIB)
- Syslog
- Layer management utility
- Management VLAN tag
- NTP client
- Firmware upgrade
- Configuration backup and restore
- Factory default configuration

Utility

- Ping test
- RSSI and path loss calculation
- Wireless site survey
- Antenna alignment tool
- System status
- Link information

Advanced Technology

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

Physical and Power

- Support 48Vdc power over Ethernet
- Form Factor: din-rail and wall-mount
- Dimension: 58.8 x 139.6 x 167 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 4/5dBi (2.4/5GHz)
- Ethernet cable x 1
- Wall mount kit x 1

Ordering Information

- IWF 3310XH-US (P/N: 10T00331001X0)
- IWF 3310XH-EU (P/N: 10T00331000X0)
- IWF 3310XM-US (P/N: 10T00331003X0)
- IWF 3310XM-EU (P/N: 10T00331002X0)

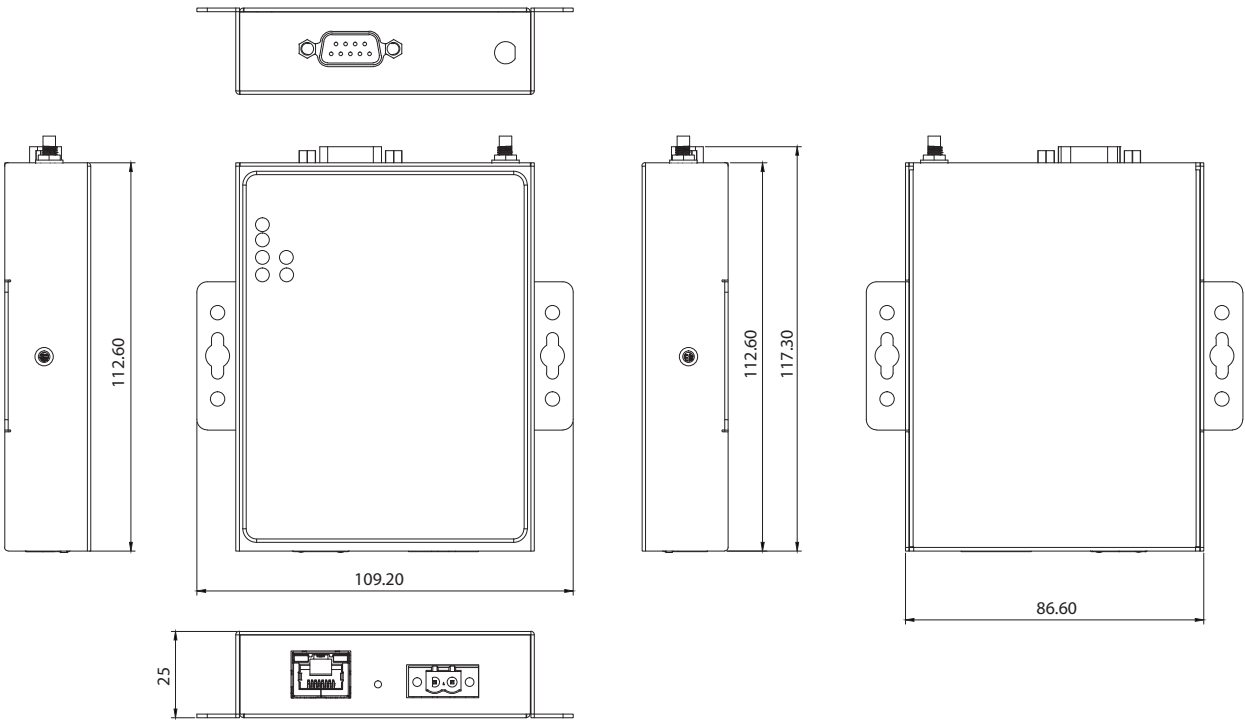
\* Note: The available RF output power will be given by certified power in different regions.



Main Features

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

Dimension Drawing



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.

Ordering Information

- **NIO 50 (P/N: 10T00005000X0)**  
Industrial Wi-Fi Serial/Ethernet device gateway

Specifications

Serial Port

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

LED Indicator

- 1 x Power
- 1 x Serial status (orange, green, bi-color)
- 4 x RSSI indicator

Wireless

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

SW Features

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

Ethernet

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

Protocol

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

Reset

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

Environment Protection

- Operating temperature: -20°C~70°C
- Storage temperature: -40°C~85°C

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

Relative Humidity

- Operating: 5%~95%, non-condensing

Certification

- EMI: FCC, CE Class A
- RF
  - FCC: Part 15C
  - CE: EN 300328
- EN60950-1
- EMC: EN 301 489-1/17, FCC Part 15 subpart B, EN 55022/55024



Main Features

- Support EZ Mesh and client Wi-Fi operation mode
- Selectable 2.4GHz/5GHz
- Support Serial, Ethernet and Wi-Fi interface
- Support Modbus TCP, RTU, ASCII/ MQTT/ Transparent
- Built-in offline port buffer with over 20 MB of storage
- High immunity to surge, ESD & EFT protection
- Up to 921.6 Kbps baud rate for RS-232/422/485 transmissions
- Web-based configuration
- SNTP client for time synchronization
- Support nCare remote configuration
- Wide DC input range with 12 - 48V
- Wide operation temperature from -40°C to 70°C

Product Overview

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

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

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

Specifications

Wi-Fi Radio

- IEEE802.11a/b/g/n , MIMO 2 x 2

Serial Interface

- RS232/422/485 with isolation
  - Data bits: 8
  - Stop bits: 1
  - Parity: none, even, odd
  - Baud rate: 9600 bps to 921.6 Kbps

Ethernet Interface

- 10/100 Mbps

Power Supply

- 12~48 VDC

LED Indicator

- 1 x Power/status
- 1 x Serial status
- 3 x RSSI indicator
- 1 x Wi-Fi 2.4/5GHz indicator
- 1 x Link/Act indicator
- 1 x Extension module

Factory Default/Reset Button

- Press reset button 10 seconds interval for factory default

Connector type

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

Wi-Fi Operating Mode

- EZ Mesh
- Client router

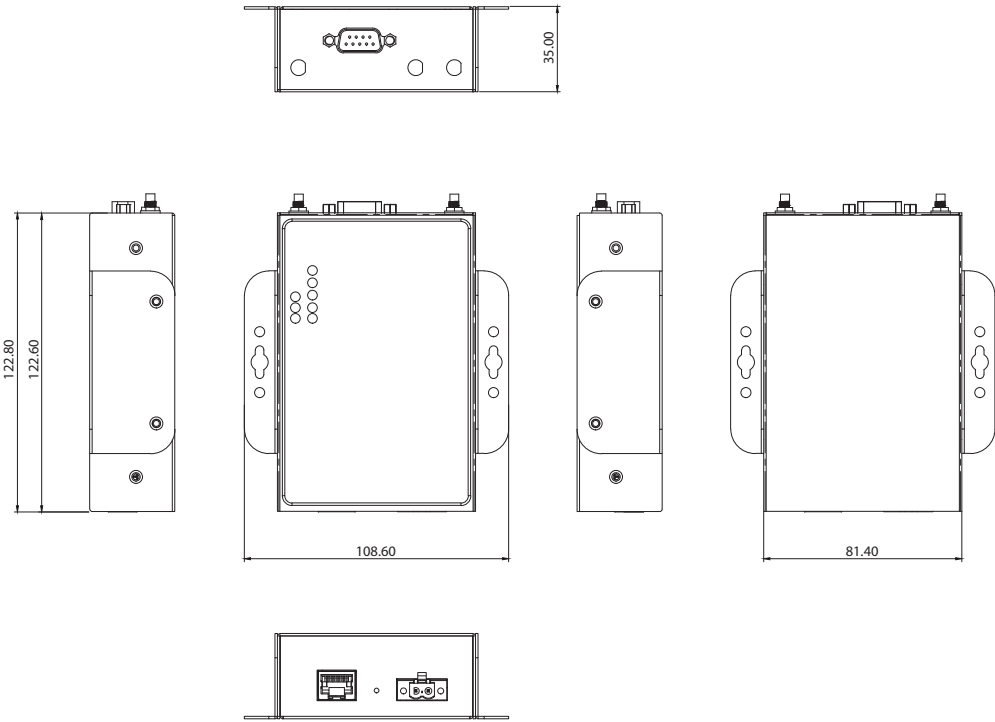
Wi-Fi Security (Client Mode)

- WEP (64/128)
- WPA/WPA2 mixed
- WPA2-personal (PSK+CCMP/AES)

Protocol

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

Dimension Drawing



Serial Port Characteristics

- Flow control: XON/XOFF
- Serial data log: 64 KB
- Offline port buffering: 20MB
- Max. RS485 connecting device number: 128
- Min. concurrent TCP client number: 10

Software Watchdog

Dimension

- 81.4 mm x 122.6 mm x 35 mm

Mounting

- Wall mounting
- DIN mounting

Construction

- SGCC chassis with fanless design

Certification

- EMI: FCC, CE Class A
- RF
  - FCC: Part 15C
  - CE: EN300328, EN301893
- EN60950-1
- EMC
  - EN301 489-1/17, FCC Part 15 subpart B, EN55022/55024
  - IEC61000-4-2: level 4
  - IEC61000-4-4/5: level 3
  - Serial line surge protection: 1KV (level 2)

Environment

- Operating temp: -40°C to 70°C
- Storage temp: -40°C to 85°C
- Relative humidity: operating: 5%~95%, non-condensing
- RoHS compliant
- Vibration
  - Random: 2Grms @ 5~500 Hz, IEC60068-2-64
  - Sinusoidal: 2Grms @ 5~500 Hz, IEC60068-2-6
- Shock: 50G, half sine, 11ms, IEC60068-27

Ordering Information

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



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

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

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



## NEXCOM Product Strengths

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

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

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

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

Featuring a wide operating temperature range of -35 to 75 degrees Celsius, a compact housing with IP55-rated waterproof and dust protection, and high-power RF design to effectively resist noises

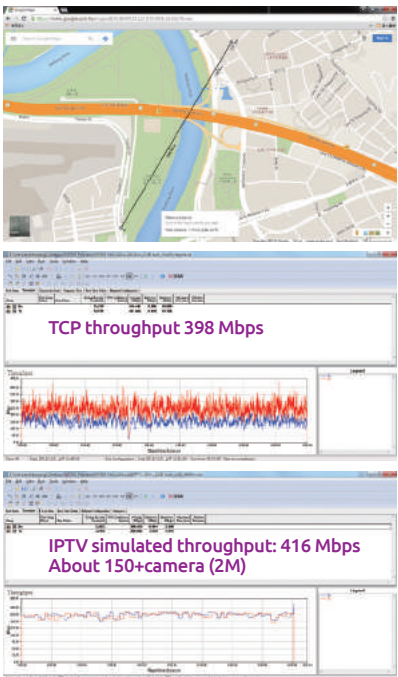


Figure 2. TCP throughput at 1km distance with 1km link.

from other RF interference sources, the IWF 503/4 product family is not only ideal for outdoor areas, but also ideal for harsh factory environments where physical cabling is impractical.

### Multi-topology Support for Application Flexibility

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

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

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

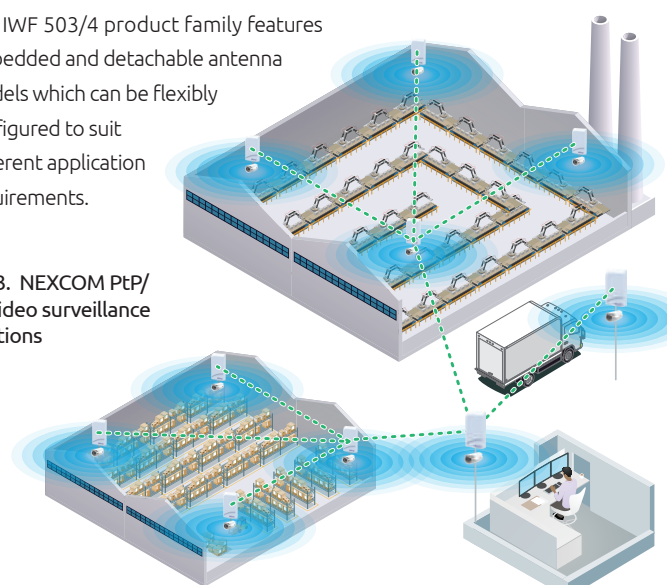
Requirements of the application:

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



NEXCOM's IWF solution:

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

Figure 3. NEXCOM PtP/ PtMP video surveillance applications



## Product Selection Guide

Model Name	IWF 503/503D	IWF 504D
Photo		
Category	PtP/PtMP AP/CPE	PtP/PtMP AP/CPE
WLAN Standard	802.11ac/a/n/a 3x3 MIMO	802.11ac+b/g/n 2x2 MIMO
Number of Radios	1	2
Number of Antenna	IWF503: 10dBi Embedded Antenna, IWF503D: 3 x RP-SMA Female	4
Type of RF Connector	IWF503D: 3 x RP-SMA Female	4 x RP-SMA Female
Number of WAN Port	1	1
Number of LAN Port	1	1
Type of LAN	RJ45	RJ45
IP Rating	IP55	IP55
Conformal Coating	N/A	N/A
Mounting Style	Wall/Pole Mount	Wall/Pole Mount
Temperature	-35°C ~ +75°C	-35°C ~ +75°C
Dimension (H x W x D) mm	240 x 135 x 58	240 x 135 x 58
PoE Input	Passive PoE: 24V	Passive PoE: 24V
DC Input	N/A	N/A
Certification	CE, FCC	CE, FCC
Safety	EN60950-1	EN60950-1
Operation Mode	AP/Client Bridge/ AP Router/Client Router	AP/Client Bridge/ AP Router/Client Router
Management Mode	SNMP/GUI/nCare Management	SNMP/GUI/nCare Management

# IWF 503 Series

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



IWF 503      IWF 503D

### Main Features

- AP/Client bridge/AP router/Client router/WDS mode supported
- Compliant with IEEE 802.11 ac/a/n 3x3 MIMO
- 1300 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 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

<b>Wireless Radio</b> <ul style="list-style-type: none"><li>• 1 x IEEE 802.11ac/an/a 3x3 MIMO</li></ul>	<ul style="list-style-type: none"><li>• IEEE802.11ac/n HT20<ul style="list-style-type: none"><li>- -82dBm@MCS0</li><li>- -71dBm@MCS7</li><li>- -70dBm@MCS8</li></ul></li><li>• IEEE802.11ac/n HT40<ul style="list-style-type: none"><li>- -92dBm@MCS0</li><li>- -72dBm@MCS7</li><li>- -66dBm@MCS9</li></ul></li><li>• IEEE802.11ac/n HT80<ul style="list-style-type: none"><li>- -88dBm@MCS0</li><li>- -68dBm@MCS7</li><li>- -62dBm@MCS9</li></ul></li></ul>
<b>Frequency Ranges</b> <ul style="list-style-type: none"><li>• USA: 5.15~5.35 GHz, 5.5~ 5.7 GHz, 5.725~5.825 GHz</li><li>• Europe: 5.15~5.35 GHz, 5.47~5.725 GHz</li><li>• Japan: 5.15~5.35 GHz, 5.47~5.725 GHz</li><li>• China: 5.725~5.85 GHz</li></ul> <p><small>* Note: The available frequency range may be different according to different certification.</small></p>	
<b>RF Output Power: IEEE 802.11ac (±2dBm)</b> <ul style="list-style-type: none"><li>• IEEE802.11a<ul style="list-style-type: none"><li>- 27dBm@6M</li><li>- 25dBm@54M</li></ul></li><li>• IEEE802.11ac/n HT20<ul style="list-style-type: none"><li>- 25dBm@MCS0</li><li>- 23dBm@MCS9</li></ul></li><li>• IEEE802.11ac/n HT40<ul style="list-style-type: none"><li>- 25dBm@MCS0</li><li>- 23dBm@MCS9</li></ul></li><li>• IEEE802.11ac/n HT80<ul style="list-style-type: none"><li>- 25dBm@MCS0</li><li>- 23dBm@MCS9</li></ul></li></ul>	<b>Hardware</b> <ul style="list-style-type: none"><li>• WAN: 10/100/1000 Base-TX MDI/MDIX RJ-45 x 1</li><li>• LAN: 10/100/1000 Base-TX MDI/MDIX RJ-45 x 1</li><li>• Compliant with<ul style="list-style-type: none"><li>- IEEE802.3/802.3u</li><li>- Hardware Based 10/100/1000, full/half, flow control auto negotiation</li></ul></li><li>• Push buttons: 1 x reset</li><li>• LED: 1 x Power &amp; Status; 1 x WAN; 1 x Wi-Fi</li><li>• SMA: 3 x with RP-SMA connectors</li></ul>
<b>Receive Sensitivity: IEEE 802.11ac</b> <ul style="list-style-type: none"><li>• IEEE802.11a<ul style="list-style-type: none"><li>- -95dBm@6M</li><li>- -77dBm@54M</li></ul></li></ul>	<b>Operating Mode</b> <ul style="list-style-type: none"><li>• AP</li><li>• Client bridge</li><li>• AP router</li><li>• Client router</li><li>• WDS</li></ul>

<b>Security</b> <ul style="list-style-type: none"><li>• WEP (64/128/152)</li><li>• WAP/WPA2 mixed</li><li>• WPA2-personal (PSK+CCMP/AES)</li><li>• WPA2- enterprise (802.1X certification)</li><li>• Hidden ESSID support</li><li>• MAC address filtering (MAC ACL)</li><li>• Station isolation</li></ul>	<b>Environment Protection</b> <ul style="list-style-type: none"><li>• Operating temperature: -35~75°C</li><li>• Storage temperature: -40~80°C</li><li>• Humidity: 0% to 95% maximum (non-condensing)</li><li>• Vibration: random 0.3g</li></ul>
<b>System Management</b> <ul style="list-style-type: none"><li>• Web-based administration</li><li>• SNMP V1/V2c</li><li>• Provides event log</li><li>• Syslog information support</li><li>• Statistics</li><li>• Configuration backup and restore</li><li>• One-button-click to restore factory default setting</li><li>• Firmware upgrade</li><li>• WES</li></ul>	<b>Certification</b> <ul style="list-style-type: none"><li>• FCC</li><li>• CE</li><li>• RoHS compliant</li></ul>
<b>Built-in Servers &amp; Client Interfaces to Other Services</b> <ul style="list-style-type: none"><li>• DHCP client</li><li>• SNMP V1/V2c client</li></ul>	<b>Package Contents</b> <ul style="list-style-type: none"><li>• IWF 503 unit x 1</li><li>• 24V PoE injector</li><li>• Steel clamps* 2 for pole mount</li><li>• QIG</li></ul>
<b>Physical and Power</b> <ul style="list-style-type: none"><li>• 24VDC passive PoE</li><li>• Wall/Pole mountable</li><li>• Dimension: 240x135x58 mm</li><li>• Weight: TBD</li></ul>	<b>Ordering Information</b> <ul style="list-style-type: none"><li>• IWF 503-EU (P/N: 10T00050300X0)</li><li>• IWF 503-US (P/N: 10T00050301X0) IEEE 802.11 ac/an/a with built-in 10dBi directional antennas</li><li>• IWF 503D-EU (P/N: 10T00050302X0)</li><li>• IWF 503D-US (P/N: 10T00050303X0) IEEE 802.11 ac/an/a with SMA connectors to supports users choice of external antennas</li></ul>
<p><small>* Note: The available RF output power will be given by certified power in different regions.</small></p>	

# IWF 504D

IP55 Outdoor AP/CPE Dual Radio Dual Band, 802.11 ac+b/g/n



### Main Features

- 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

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

#### RF Output Power: IEEE 802.11ac/an/a (±2dBm)

- IEEE802.11a
  - 27dBm@6M
  - 24dBm@54M
- IEEE802.11a/n HT20
  - 27dBm@MCS0
  - 24dBm@MCS7
  - 23dBm@MCS8 in VHT20
- IEEE802.11a/n HT40
  - 26dBm@MCS0
  - 23dBm@MCS7
  - 22dBm@MCS8 in VHT40
- IEEE802.11ac VHT 80Mhz
  - 24dBm@MCS0
  - 22dBm@MCS7
  - 21dBm@MCS8

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

- IEEE802.11b
  - 27dBm@1M
  - 24dBm@11M
- IEEE802.11g
  - 27dBm@6M
  - 24dBm@54M
- IEEE802.11g/n HT20
  - 23dBm@MCS0/8
  - 19dBm@MCS7/15
- IEEE802.11g/n HT40
  - 22dBm@MCS0/8
  - 18dBm@MCS7/15

#### Receive Sensitivity: IEEE 802.11ac/an/a

- IEEE802.11a
  - -95dBm@6M
  - -80dBm@54M
- IEEE802.11a/n HT20
  - -95dBm@MCS0
  - -76dBm@MCS7
  - -72dBm@MCS8 in VHT20
- IEEE802.11a/n HT40
  - -92dBm@MCS0
  - -75dBm@MCS7
  - -71dBm@MCS8 in VHT40

- IEEE802.11ac VHT 80Mhz
  - -90dBm@MCS0
  - -72dBm@MCS7
  - -68dBm@MCS8

#### Receive Sensitivity: IEEE 802.11 b/g/n

- IEEE802.11b
  - -93dBm@1M
  - -91dBm@11M
- IEEE802.11g
  - -94dBm@6M
  - -80dBm@54M
- IEEE802.11g/n HT20
  - -94dBm@MCS0/8
  - -77dBm@MCS7/15
- IEEE802.11g/n HT40
  - -89dBm@MCS0/8
  - -73dBm@MCS7/15

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

#### System Management

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

#### Built-in Servers & Client Interfaces to Other Services

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

#### Physical and Power

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

#### Environment Protection

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

#### Certification

- FCC
- CE
- RoHS compliant

#### Package Contents

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

### Ordering Information

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

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

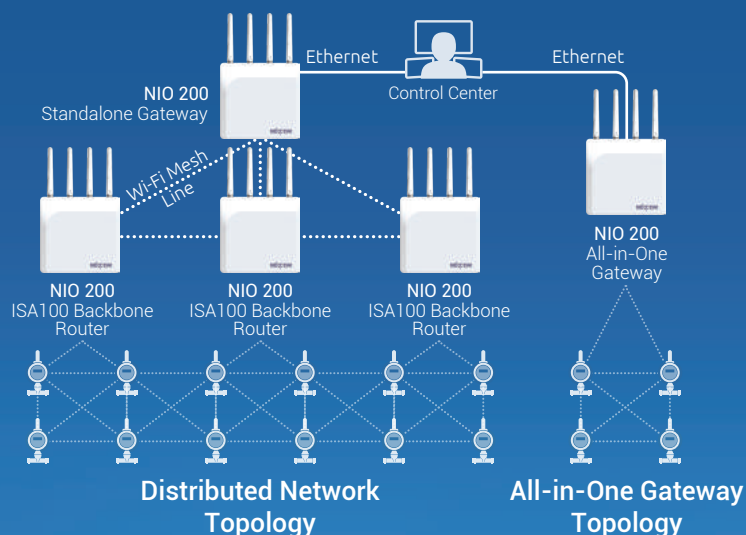


# NEXCOM's ISA100.11a/ WirelessHART Gateway for Wireless Process Automation

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, using wired connectivity solutions for such large-scale deployments is complex and costly compared to wireless connectivity solutions. Furthermore, process automation applications such as chemical, oil and gas processing require a reliable network with low latency, in which most common protocols such as ZigBee and LoRa lack to offer. As a result, ISA100.11a and WirelessHART are quickly becoming the mainstream wireless communication protocols for process automation.

In response to this demand, NEXCOM offers the NIO 200 series which features ISA100.11a (IEC 62734) or WirelessHART support and Wi-Fi mesh backbone technology, including a design that focuses on the communication and management requirements of Industry 4.0.

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



## NEXCOM Product Strengths

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

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

### Unique Wi-Fi Mesh Backbone Technology

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

### C1D2 and ATEX Certified for Anti-Explosion

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

### High Wireless Radio Frequency (RF) Sensitivity

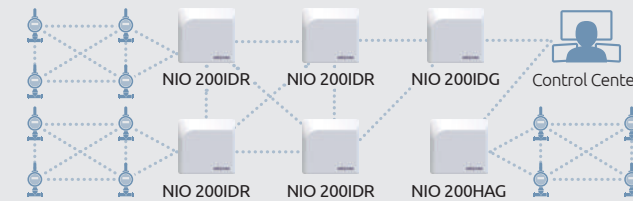
For wireless sensor/instrument communication, the NIO 200 series features a radio module with increased receiver sensitivity capable of providing more than twice the transmission distance over other similar devices using the same radio frequency (RF) power.

## 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

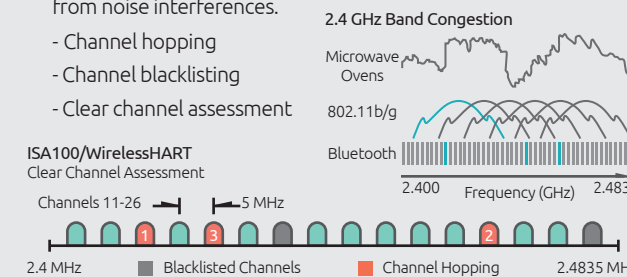
### Flexible Deployment for Critical Field Wireless Networks

- 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.



### Robust Communication over ISA100.11a/WirelessHART Field Wireless Networks

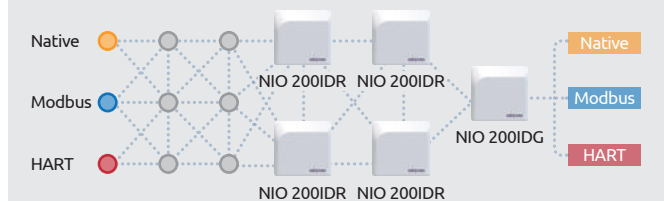
- Spectrum management technology shields field radio signals from noise interferences.
  - Channel hopping
  - Channel blacklisting
  - Clear channel assessment



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.

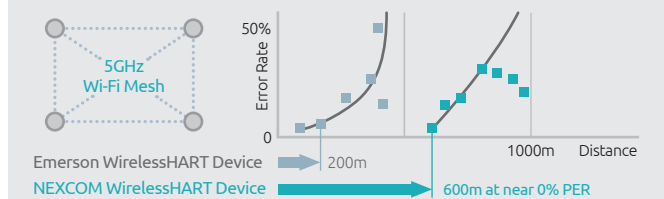
### Support of Multiple Field Protocols over ISA100.11a

- 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 5GHz 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.




## Product Selection Guide

Model Name	NIO 200IDR	NIO 200IDG	NIO 200IAG/NIO 200HAG
Photo			
WLAN Standard	802.11 a/n	802.11 a/n	802.11 a/n
Wireless Field Protocol	ISA100	ISA100	NIO 200 IAG:ISA100 NIO 200HAG: WirelessHART
Gateway Function	N/A	Standalone gateway	All-in-One gateway
Wi-Fi Mode	Mesh/AP	Mesh/AP	Mesh/AP
Ethernet Speed	10/100/1000	10/100/1000	10/100/1000
IP Rating	IP67	IP67	IP67
Temperature	-40°C to +75°C	-40°C to +75°C	-40°C to +75°C
PoE Type	IEEE802.3at	IEEE802.3at	IEEE802.3at
DC Input Range	12 ~ 48V	12 ~ 48V	12 ~ 48V
Network Management	SNMP V1/V2c/Web GUI/nCare	SNMP V1/V2c/Web GUI/nCare	SNMP V1/V2c/Web GUI/nCare
Certification	CE, FCC	CE, FCC	CE, FCC
Safety	UL 60950-1, UL 60950-22	UL 60950-1, UL 60950-22	UL 60950-1, UL 60950-22
Anti-Explosive	CID2/ATEX	CID2/ATEX	CID2/ATEX

# NIO 200 Series

ISA100/WirelessHART Process Automation Wireless Gateway



NIO 200 C1D2      NIO 200 ATEX

### 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

## Product Overview

NEXCOM NIO 200 is a powerful distributed network topology ISA100.11a access point integrating 802.11n Mesh technology. With ISA100.11a/WirelessHART technology, NIO 200 can establish fully Mesh network to ensure robust and reliable communication for mission-critical industrial wireless applications. The integration of both 802.11n Mesh & ISA100.11a/WirelessHART 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 CID2 and ATEX certified requirement and is perfect solution to critical data monitoring and sensing in oil & gas, chemical plant, etc...

## Specifications

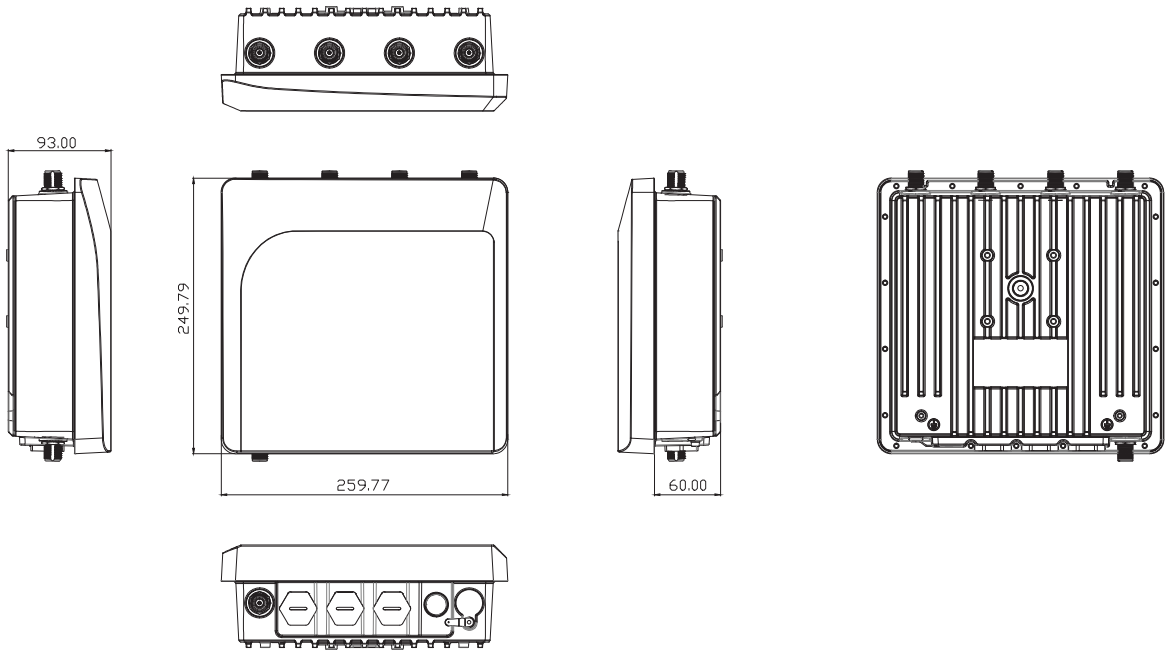
- Wireless Radio**
  - IEEE802.11a/n x 2, MIMO 2 x 2    • IEEE802.15.4, 1 Tx, 1 Rx
- Wi-Fi Frequency Ranges**
  - USA: 5.15~5.25 GHz, 5.725~5.825 GHz    • Europe: 5.47~5.725 GHz
- RF Output Power: IEEE 802.11a**
  - 802.11a - 28 dBm with 2 antennas
  - 802.11n (HT20) - 27 dBm with 2 antennas
  - 802.11n (HT40) - 27 dBm with 2 antennas

\* Note:  
The available RF output power will be given by certified power in different region
- Hardware**
  - WAN: 10/100/1000 Base-TX MDI/MDIX
  - LAN: 10/100/1000 Base-TX MDI/MDIX
  - Ethernet compliant with:
    - IEEE802.3/802.3u
    - Hardware based 10/100/1000, full/half, flow control auto negotiation
  - Push buttons: 1 x reset/restore to default
  - LED: - 2 x Ethernet    - 2 x 11an radio
    - 1 x IWSN radio    - 1 x Power/Status
  - N-Type:
    - 5 x N-type connector for NIO 200IDR/IAG/HAG
    - 4 x N-type connector for NIO 200IDG
- Safety Compliance**
  - UL 60950-1; 60950-22    • IEC 60950, 2nd edition
  - EN 60950, 2nd edition    • 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
- Wi-Fi Security (AP Mode)**
  - WEP (64/128/152)    • WAP/WPA2 mixed
  - WPA2-personal (PSK+CCMP/AES)    • Hidden ESSID support
  - MAC address filtering (MAC ACL)    • Station isolation

\* Note: The AP Function is to be quipped in 2nd phase stage.
- System Management**
  - nCare, web GUI management    • SNMP V1/V2c/V3
  - Event log    • Syslog information support
  - Configuration backup and restore
  - One-button-click to restore factory default setting
  - Firmware upgrade    • SNMP V1/V2c/V3 client
- High-Side Communication Interfaces**
  - Monitoring and Control System (MCS)
  - MODBUS/TCP
  - Gateway Services Access Point (GSAP) (only for NIO200IAG/IDG)
  - HART-IP (only for NIO200HAG)
- Physical and Power**
  - 12~48 VDC PoE (standard PoE 802.3at)
  - Wall/pole mountable
  - Dimension: 256mm x 226mm x 91mm
  - Weight: 2.5Kg

## Dimension Drawing



- 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
- Certification**
  - UL 60950-1; 60950-22
  - Radio approvals
    - FCC Part 15.247, 15.407    - EN 300 328    - EN 301 893
  - EMI and susceptibility - FCC Part 15.107, 15.109    - EN 301 489-1, -17
- Anti-Explosive Certification**
  - UL: Class I, Division 2, Groups A, B, C and D, T4
  - ATEX: Class I, Zone 2; Ex nA II, T4

Wireless Communication Interface Specifications	
Standard IEEE	802.15.4
Data Rate	250 kbps
Modulation	Q-PSK
Spread Spectrum	DSSS
RF Output Power	Max +15 dBm
Sensitivity	-95 dBm
Connector	N type
Antenna	2 dBi@ 2.4GHz
Performance Parameters	
Scalability	NIO 200IAG: 100 field instruments
	NIO 200IDG: 200 field instruments, 20 subnets
	NIO 200IDR: 50 field instruments
	NIO 200HAG: 250 field instruments
Mesh Network Depth	3 hops
Field Device Join Time	As low as 20 seconds

Reporting Rate	ISA100: 1, 5, 10, 20, 30 and 60 seconds; 10 devices publishing/second
	WirelessHART: 8,16,32 secs and 1-60 minutes; 10 devices publishing/second

## Ordering Information

	ISA100	WirelessHART
All-in-One Gateway	NIO 200IAG-US P/N: 10T00020008X0	NIO 200HAG-EU P/N: 10T00020010X0
Distributed Gateway	NIO 200IDG-US P/N: 10T00020009X0	-
Distributed Backbone Router	NIO 200IDR-US P/N: 10T00020004X0	-

## Optional Accessories

- **P/N: 5040210012X00**  
SIMPLE WALL MOUNT KIT VER: A SIN SUPER CIRCLE
- **P/N: 5040410110X00**  
POLE MOUNT FOR NIO200 VER: A SIN SUPER CIRCLE 92x228x90mm  
SECC=2.0t WHITE
- **P/N: 7A00000066X00**  
Antenna arrester, DC-6 GHz N-MALE TO N-FEMALE
- **P/N: 603ANT0012X00**  
Dual Polarization-Directional Antenna for 5 GHz 20dBi
- **P/N: 603ANT0009X00**  
Directional Antenna 2300~2700 MHz 16~17 dBi
- **P/N: 603ANT0010X00**  
Directional Sector Antenna 2400~2500 MHz 14±0.5 dBi
- **P/N: 603ANT0013X00**  
Directional Sector Antenna 5150~5875 MHz 15±0.5 dBi

## Headquarters

### NEXCOM International Co., Ltd.

9F, No.920, Chung-Cheng Rd., ZhongHe District, New Taipei City, 23586, Taiwan, R.O.C.  
Tel: +886-2-8226-7786  
Fax: +886-2-8226-7782  
www.nexcom.com

---

## America

### USA

#### NEXCOM USA

2883 Bayview Drive,  
Fremont CA 94538, USA  
Tel: +1-510-656-2248  
Fax: +1-510-656-2158  
Email: sales@nexcom.com  
www.nexcom.com

## Asia

### Taiwan

#### NEXCOM Intelligent Systems

##### Taipei Office

13F, No.920, Chung-Cheng Rd.,  
ZhongHe District,  
New Taipei City, 23586, Taiwan, R.O.C.  
Tel: +886-2-8226-7796  
Fax: +886-2-8226-7792  
Email: sales@nexcom.com.tw  
www.nexcom.com.tw

#### NEXCOM Intelligent Systems

##### Taichung Office

16F, No.250, Sec. 2, Chongde Rd.,  
Beitun Dist.,  
Taichung City 406, R.O.C.  
Tel: +886-4-2249-1179  
Fax: +886-4-2249-1172  
Email: sales@nexcom.com.tw  
www.nexcom.com.tw

### Japan

#### NEXCOM Japan

9F, Tamachi Hara Bldg.,  
4-11-5, Shiba Minato-ku,  
Tokyo, 108-0014, Japan  
Tel: +81-3-5419-7830  
Fax: +81-3-5419-7832  
Email: sales@nexcom-jp.com  
www.nexcom-jp.com

## China

### NEXCOM China

Floor 5, No.4, No.7 Fengxian Middle Rd.,  
(Beike Industrial Park), Haidian District,  
Beijing, 100094, China  
Tel: +86-10-5704-2680  
Fax: +86-10-5704-2681  
Email: sales@nexcom.cn  
www.nexcom.cn

### NEXCOM Shanghai

Room 603/604, Huiyinmingzun Plaza Bldg. 1,  
No.609 Yunlin East Rd.,  
Shanghai, 200333, China  
Tel: +86-21-5278-5868  
Fax: +86-21-3251-6358  
Email: sales@nexcom.cn  
www.nexcom.cn

### NEXCOM Surveillance Technology Corp.

Room 202, Building B,  
the GuangMing Industrial Zone Zhonghua Rd.,  
Minzhi Street, Longhua District,  
Shenzhen 518131, China  
Tel: +86-755-8364-7768  
Fax: +86-755-8364-7738  
Email: steveyang@nexcom.com.tw  
www.nexcom.cn

### NEXCOM United System Service

Hui Yin Ming Zun Building Room 1108, Bldg.  
No.11, 599 Yunling Rd., Putuo District,  
Shanghai, 200062, China  
Tel: +86-21-6125-8282  
Fax: +86-21-6125-8281  
Email: frankyang@nexcom.cn  
www.nexcom.cn

## Europe

### United Kingdom

#### NEXCOM EUROPE

10 Vincent Avenue,  
Crownhill Business Centre,  
Milton Keynes, Buckinghamshire  
MK8 0AB, United Kingdom  
Tel: +44-1908-267121  
Fax: +44-1908-262042  
Email: sales.uk@nexcom.eu  
www.nexcom.eu

### Italy

#### NEXCOM ITALIA S.r.l

Via Lanino 42,  
21047 Saronno (VA), Italia  
Tel: +39 02 9628 0333  
Fax: +39 02 9625 570  
Email: nexcomitalia@nexcom.eu  
www.nexcomitalia.it