WindowMaster International A/S
Skelstedet 13
2950 Vedbæk
Denmark

Document ID: 260623
Date: 23.06.2026
Version: 1.0

# Product Cybersecurity Brief –

WxC 310/320 Plus & WSC 5x0 Series Controller Family

This document outlines the security architecture, network requirements, and compliance posture to assist customer IT/OT teams in validating the device for deployment within **NIS2**, **CRA**, **UK PSTI** and similar regulated environments.

## Product Information

The WCC 310 Plus and WCC 320 Plus product family is a series of controllers aimed at Natural and Mixed-Mode Ventilation control, while the WSC 310 Plus, WSC 320 Plus and the WSC 520/540/560 series are aimed at Smoke and Heat exhaust ventilation. These controllers also incorporate the necessary technology to enable NV Embedded® Control functionality as well as Cloud-Enhanced functionality.

While this document will touch on data information and exchange as part of the security topic, it is not intended to cover aspects such as the EU Data Act.

### Network Architecture & Connectivity

The controller functions as a controller and gateway device, facilitating communication between the IT/Cloud and the OT network. To do so, the interfaces below are supported.

**Table 1.1:** Supported interface:

| Interface | Type | Scope | Accessory | Description |
|---|---|---|---|---|
| BACnet MSTP | Fieldbus | OT Network | WCA 3FM (WxC 3x0) | BACnet MSTP Interface for connection with a BMS system |
| BACnet IP | Fieldbus | OT Network | WCA 3FB (WxC 3x0)<br>WSA 5MC KNX (WSC 5xx) | BACnet IP Interface for connection with a BMS system |
| KNX | Fieldbus | OT Network | WCA 3FK (WxC 3x0)<br>WSA 5MC KNX (WSC 5xx) | KNX Interface for connection with a BMS system or used for accessories |
| SD Card | Integrated | Diagnostics & Backup | NA | The SD Card is provided with the controller and is used for diagnostic logging and configuration backup |
| USB Host | Accessory | Diagnostics & Licensing | WCA 304 or NVE Dongle | The USB interface can be used for diagnostic logging and/or to enable the NVE functionality |
| USB Device | Accessory | Configuration | NA | The USB interface can be used for commissioning and configuration of the controller and firmware upgrading. |
| Ethernet | System Integration | IT and OT Network | NA | The 2-port switch can be used to daisy-chain controllers together, for BACnet IP and for external connectivity such as NVE Cloud. |
| CAN | Fieldbus | OT Network | WSC 5xx | Exclusively for controller-to-controller communication |
| WSK-Link™ | Fieldbus | OT network | WxC xxx | Exclusively for controller-to-peripherals communication |

### OT Layer

On the OT layer, the following protocols are supported:

- BACnet MS/TP Standard via twisted pair interface
- BACnet IP Standard via Ethernet interface
- KNX Standard via twisted pair interface
- Modbus RTU Standard via twisted pair interface
- Modbus TCP Standard via Ethernet interface
- CAN bus Standard via CAN interface
- WSK-Link™ via LIN interface
- AOnet via Ethernet interface

The device is fully air-gap compatible and can function without internet access

### IT Layer

The IT layer is facilitated exclusively through ethernet and is used for remote commissioning, service as well as cloud connectivity and logging.

Cloud Connectivity requires an active NVE Cloud subscription as well as an NVE Dongle. The architecture is based on MS Azure IoT, and the device acts as an edge gateway in the architecture.

Note: The ethernet ports are internally connected through a layer-2 switch, there is no segregation between the IT and OT layer if the controller is configured as such.

**Table 1.2:** Firewall requirements based on functionality:

| Functionality | Service | Port | Protocol | Destination/Origin |
|---|---|---|---|---|
| NVECloud | MQTTs | 8883/tcp | Outbound | windowmaster.azure-devices.net |
| AOnet | DTLS | 55557/udp | Bidirectional | Controller to Controller communication and/or Remote Configuration |
| Firmware OTA | HTTP | 80/tcp | Inbound | nvcomfort.com |
| Remote Commissioning | HTTP | 80/tcp | Inbound | XML-Based interface for writing controller parameters. Access can be set to write or read-only. |
| Remote UI Access | Proprietary | 55555/tcp | Inbound | Used for remote control via WMaFlexiSmokeRemote |
| Remote Terminal Access | Telnet | 55556/tcp | Inbound | Used for remote terminal (UART) access |
| Fieldbus | BACnet | 47808/udp | Bidirectional | |
| Fieldbus | Modbus | 502/tcp | Bidirectional | |
| Fieldbus | KNX | 3671/udp | Bidirectional | IP/KNX Gateway, not implemented on the device |

### OTA and FW Update Mechanisms

While OTA updates are supported by the controller, they are not initiated remotely and/or unattended. FW Updates can be delivered via USB Mass Storage, USB DFU Mode or by pulling the update files remotely, but they are always initiated by the user via the interface.

## Access & Maintenance

Access to the controller is divided between 4 levels:

**Table 1.3:** Access Level Overview:

| Access Level | Access to | Who has access |
|---|---|---|
| 1 | Physical Access | Persons with access to the room of installation |
| 2 | Status | Persons with a key to the housing of the controller. Operational status can be seen on the controller screen. |
| 3 | Service Information | Service Technicians with the purpose of resetting the service timer. Access requires a pin code set by a commissioning engineer with level 4 access |
| 4 | Commissioning | Commissioning engineers. Access is provided to all options with a factory-set pin code. |

Pin codes are specific to each controller, i.e. per MAC address, and the factory assigned codes are printed inside the cabinet. It is recommended to change the pin code during the initial commissioning.

### Remote Access

Remote access to the controller is possible via the ethernet interface and, depending on the deployment method, can be done in several different ways.

## Deployment Concepts

Choosing the right method depends on the site's infrastructure, security requirements, and firewall policies. Network restrictions are generally governed by the level of security needed:

- **Air Gapped**
  No physical connection exists or is allowed between the OT and IT networks and/or individual network segments. This is the most restrictive type of setup and almost always requires physical presence
- **White-Listing**
  Connections between the OT and IT networks and/or individual network segments exist, but communication between them is denied by default. Each domain, port, or protocol needs to be whitelisted in order to facilitate communication.
- **Black-Listing**
  Connections between the OT and IT networks and/or individual network segments exist, and communication between them is allowed by default. Specific domains, port and protocols are denied, typically based on security lists provided by external security partners

  **Note:** The above is a generalization of typical setups; Most implementations will allow (White-Listing) all outgoing connections to the internet while denying (Black-Listing) ingoing connections.

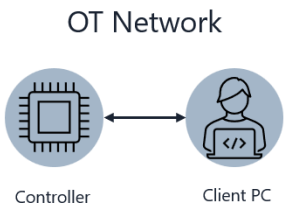
## Deployment Options

Our recommendation is to deploy the controllers on a dedicated OT LAN or VLAN separated by the IT network by a corporate firewall. Recommended firewall settings are provided in table 1.2. We recommend that IP addresses are statically assigned to the controllers through DHCP, by the IT organization.

Other options:

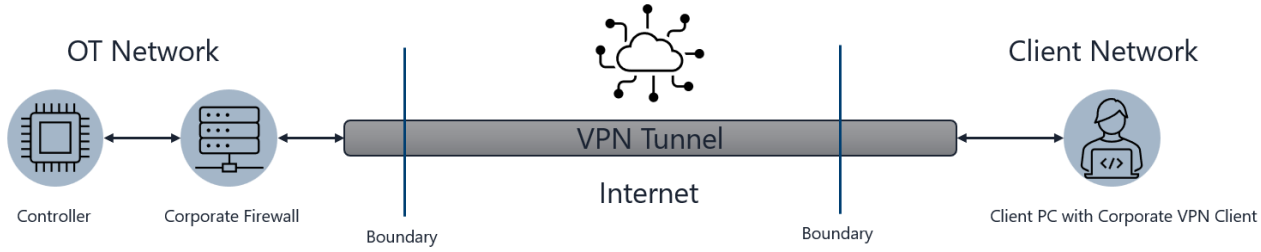
### On-Site via OT Network

The controller(s) are deployed in a closed OT environment, and remote access requires a PC with access to said network. In an air-gapped network, on-site presence is required.




### Remote via Tunneling & Forward Proxy

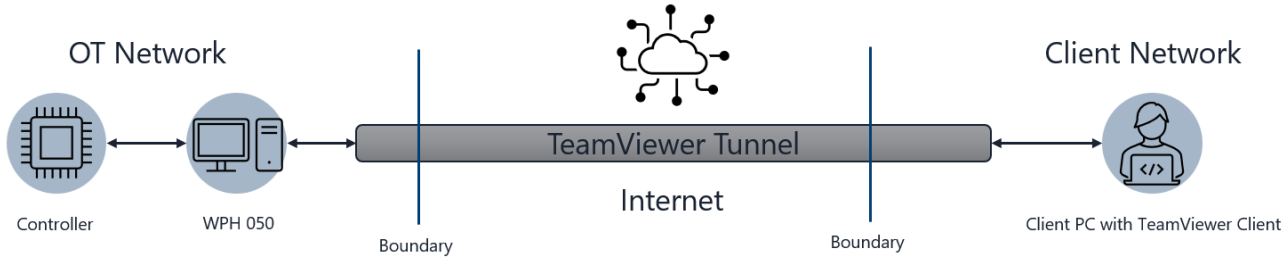
The local IT department can choose to deploy tunnelling services via TUN or TAP, i.e. via a VPN or forward proxy services and provide that access either permanently or on a time-limited basis to the required personnel. The local IT department would then be in charge of RBAC, maintenance, and support.




*Requires configuration of inbound connections through the firewall, specific to the tunneling service used.*

### Remote via WPH 050

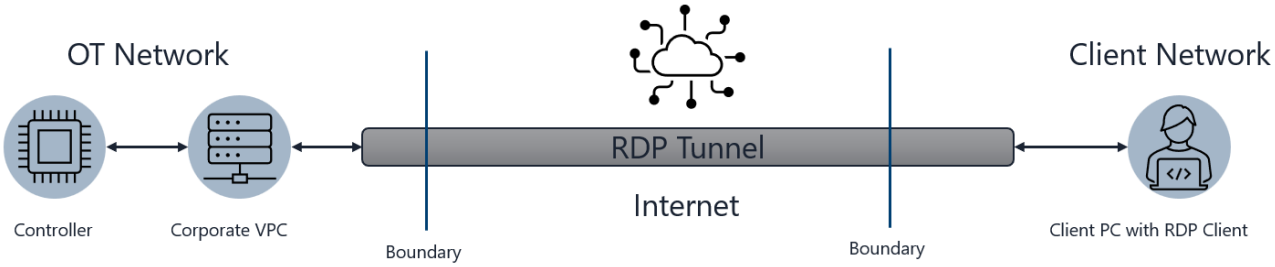
The WPH 050 is a PC containing the maintenance and configuration software required to interface with the controllers. The PC can be deployed in the OT environment, and access can be granted through Tunneling services or VNC services.




*Requires configuration of inbound connections through the firewall, specific to the tunneling or VNC service used. Examples: Remote Desktop Services, TeamViewer, RealVNC, etc.*

**Remote via VPC**

The local IT department can also choose to provide a virtual PC with the maintenance and configuration software. The required firewall rules and remote access services are dependent on the infrastructure at the client's site.

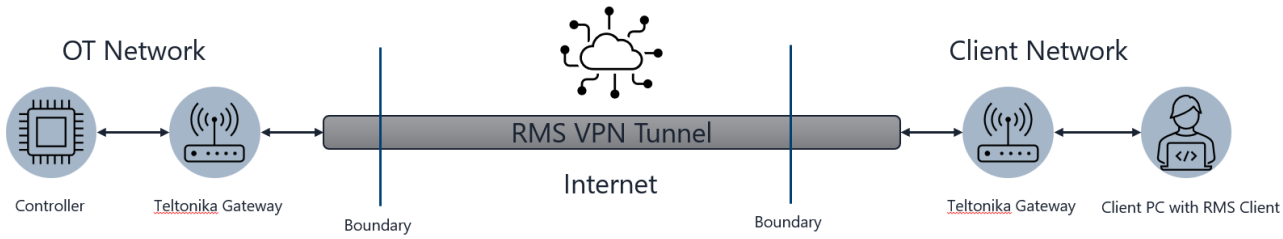



*Requires configuration of inbound connections through the firewall, specific to the tunneling or VNC service used. Examples: Remote Desktop Services, TeamViewer, RealVNC, etc.*

**Remote via Gateway & Reverse Proxy**

For plug-n-play installations and/or in cases where the local IT security setup is deemed insufficient, a gateway utilizing a reverse proxy can be installed in the OT cabinet. The Teltonika RUT series is recommended for this.

These devices operate using punch-through tunneling services, e.g. Wireguard, and do not require inbound firewall configuration. As long as UDP is allowed out of the network, the service will function. The routers can be deployed either as gateways, which means that remote access is only provided to the downstream network segment or as clients that allow remote access to the entire LAN segment.




**NOTE:** Direct connections, whether via port forwarding or DMZ, over the public internet are strongly discouraged.

## Contact

Please use the following addresses if you have further questions or concerns:

| | |
|---|---|
| Denmark: | info.dk@windowmaster.com |
| Norway: | info.no@windowmaster.com |
| UK: | info.uk@windowmaster.com |
| Switzerland: | info.ch@windowmaster.com |
| Germany: | info.de@windowmaster.com |
| USA: | info.us@windowmaster.com |
| Others: | info.dk@windowmaster.com |

Please use the following link to submit a Cyber Security Incident: Cyber Security Report Form

# FAQ

## General Security

**Q: Does the product use default or shared credentials?**
A: Each device is provisioned with unique credentials during manufacturing and can be changed during commissioning. See the product manual for details.

**Q: Does the product require internet connectivity to function?**

A: No. SHEV and ventilation controllers operate autonomously on the local OT network. Cloud connectivity (SaaS platform) is optional and provides monitoring, alerting, and remote management capabilities. All safety-critical functions can operate without cloud connectivity.

**Q: How should the product be segmented on our network?**

A: We recommend deploying controllers on a dedicated OT VLAN, separated from corporate IT by a firewall or industrial DMZ. A detailed network architecture guide and recommended firewall ruleset is provided in this document.

**Q: Can NVECloud send commands to the controllers?**

A: Yes, the NVECloud platform can send parameter updates and configuration changes to controllers via Azure IoT Hub device twins and direct methods. Safety-critical SHEV activation commands are not sent via the cloud path.

**Q: What happens if cloud connectivity is lost?**

A: Controllers continue to operate using their local configuration and respond to BMS commands and local inputs (fire alarm signals, temperature sensors, etc.). Telemetry is not buffered locally, and intermittent connectivity would result in data gaps in the NVECloud solution.