User Manual UMAX141200
Version 5A
Firmware 5.xx

USER MANUAL

Wi-Fi to CAN Converter

P/N: AX141200

Axiomatic Technologies Oy
Höytämöntie 6
33880 LEMPÄÄLÄ, Finland
Tel. +358 103 375 750
salesfinland@axiomatic.com
www.axiomatic.fi

Axiomatic Technologies Corporation
1445 Courtneypark Dr. E.
Mississauga, ON Canada L5T 2E3
Tel. 1 905 602 9270
sales@axiomatic.com
www.axiomatic.com

ACRONYMS

A	Ampere
AP	Access Point
ARP	Address Resolution Protocol
AT	Austria (country code)
AX	Axiomatic
BAT	Battery
BE	Belgium (country code)
BG	Bulgaria (country code)
°C	Celsius (degree)
CAN	Controller Area Network or Canada
CE	Conformité Européenne (European Conformity)
CY	Cyprus (country code)
CZ	Czech Republic (country code)
DE	Germany (country code)
DIN	Digital Input
DK	Denmark (country code)
EA	The Axiomatic Electronic Assistant (a PC application software)
EE	Estonia (country code)
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
EN	European Norms (European Standards)
EL	Greece (country code)
ES	Spain (country code)
ESD	Electrostatic Discharge
ETSI	European Telecommunications Standards Institute
EU	European Union
FCC	Federal Communications Commission
FI	Finland (country code)
FR	France (country code)
G	Acceleration in Gravity Units
GHz	Gigahertz
GND	Ground
GO	Group Owner
GPL	General Public License
HIB	Hibernation
hr	hour
HR	Croatia (country code)
HTTP	Hypertext Transfer Protocol
HU	Hungary (country code)
IC	Industry Canada or Integrated Circuit
ICES	Interference-Causing Equipment Standard (Canada)
ICMP	Internet Control Message Protocol
ID	Identifier
IE	Ireland (country code)

IEC	International Electrotechnical Commission
IP	Internet Protocol or Ingress Protection (for housing)
ISED	Innovation, Science and Economic Development Canada
ISO	International Organization for Standardization
IT	Italy (country code)
L	Length (for size)
LAN	Local Area Network
LED	Light-Emitting Diode
LT	Lithuania (country code)
LU	Luxembourg (country code)
LV	Latvia (country code)
m	meters
MAC	Media Access Control (address)
MDIX	Medium Dependent Interface Crossover (MDI-X)
MIC	Ministry of Internal Affairs and Communications (Japan)
MPE	Maximum Permissible Exposure
ms	millisecond
MT	Malta (country code)
NL	Netherlands (country code)
NMB	Norme sur le Matériel Brouilleur (Interference-Causing Equipment Standard. Canada, in French)
NoA	Notice of Absence
NWP	Network Processor
ORRE	Ordinance Regulating Radio Equipment (Japan)
OTA	Over the Air
OUI	Organizationally Unique Identifier
P2P	Point-to-Point
PA	Polyamide
PBC	Push Button Configuration
PL	Poland (country code)
P/N	Part Number
PT	Portugal (country code)
RED	Radio Equipment Directive
RF	Radio Frequency
RGB	Red-Green-Blue
RO	Romania (country code)
RoHS	Restriction of Hazardous Substances
RSS	Radio Standards Specification
RTOS	Real-Time Operating System
SE	Sweden (country code)
SI	Slovenia (country code)
SK	Slovakia (country code)
SP	Service Pack
SSID	Service Set Identifier
SSP	Software Support Package
STA	Station

SW	Software
TI	Texas Instrument
TBD	To Be Determined
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UK	United Kingdom (country code)
UL	Underwriters Laboratories (safety organization)
USB	Universal Serial Bus
V	Volt
VDC	Volt Direct Current
W	Watt or Width (for size)
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	Wireless Protected Access
WPA2	Second version of the WPA (Wireless Protected Access) standard
WPS	Wi-Fi Protected Setup

TABLE OF CONTENTS

1 INTRODUCTION

The following user manual describes architecture, functionality, and configuration parameters of the Wi-Fi to CAN Converter. It also contains technical specifications and installation instructions of the converter.

The user should check whether the application firmware installed in the converter is covered by this user manual. It can be done using any web browser connected to the converted ether directly over the Wi-Fi connection or indirectly over the LAN, see: Configuration Parameters section for more details.

The user manual is valid for application firmware with the same major version number as the user manual. For example, this user manual is valid for any application firmware version 5.xx. Updates specific to the user manual are done by adding letters: A, B, …, Z to the user manual version number.

2 CONVERTER DESCRIPTION

The Wi-Fi to CAN Converter is a simple device converting CAN frames into UDP or TCP IP datagrams and sending them over a wireless Wi-Fi network. The device can also convert the received UDP or TCP datagrams into CAN frames.

The converter has one CAN port. It supports a high-speed CAN with a configurable baud rate up to 1Mbit/s and a dual-band 2.4GHz and 5GHz 802.11 a/b/g/n Wi-Fi. All standard and extended CAN frames, including data and remote frames, are supported.

The converter can work in: Station (STA), Access Point (AP) and Wi-Fi Direct (P2P) modes. The P2P mode operates only in 2.4GHz frequency band. The wireless connection is provided by an internal antenna to maintain ruggedness. A three-color LED on the housing displays an internal state of the converter.

The converter contains a web server to setup configuration parameters and monitor the internal state of the converter using a web browser. The user can also update the converter firmware over the air (OTA) using the web browser.

The converter has two digital inputs. One of them is used to switch the converter to a default AP mode and then access it using a standard wireless device (e.g., a laptop or a smartphone). The second one can be used to disable all Wi-Fi communication.

A simple command-line `AxioDisc.exe` Windows application is provided to locate a converter on the LAN.

To ensure low latency in processing CAN messages, the converter software runs under control of a real-time operating system.

The converter is designed to work on off-road machinery or in a harsh industrial environment with power transients, high humidity, and vibrations.

2.1 Hardware Block Diagram

The converter hardware block diagram is presented in Figure 1.

The converter is powered from a standard automotive 12V or 24V battery. Reverse polarity, overvoltage, and transient protection is provided.

The CAN port is connected to a powerful 32-bit ARM Cortex-M4 microcontroller that runs IP protocol stack and all IP to CAN conversion logic.

The wireless part is provided by the Texas Instrument CC3135 network processor (NWP), which sends and receives IP messages over a wireless Wi-Fi network, establishes and maintains the wireless connection in 2.4GHz or 5GHz Wi-Fi frequency band.

The converter has two digital inputs. They have internal pull-up resistors and are activated by connection to the digital ground (DIN_GND pin).

A three-color RGB Status LED indicates the internal state of the converter.

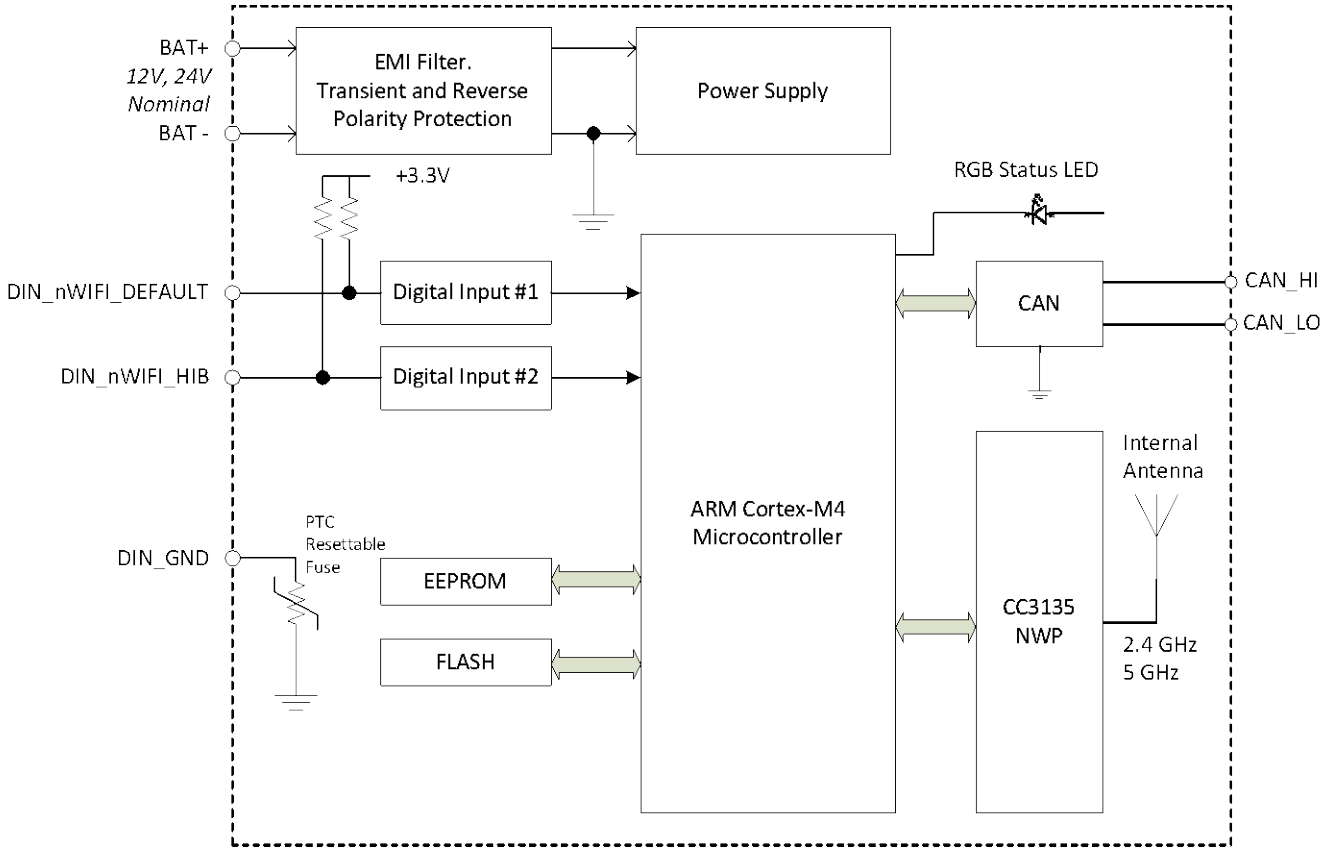

Figure 1. The Converter Hardware Block Diagram

2.2 Status LED

The Status LED on the housing displays the internal state of the converter the following way, see Table 1:

Table 1. Converter Status LED

LED	Subsystem state		Converter Status	Description
	Wi-Fi	CAN		
Green (steady or blinking)	Connected	Active	Normal Operation	CAN and Wi-Fi ports are ready for communication. If blinking, data is being transferred between CAN and Wi-Fi ports.
Steady Yellow	Disconnected	Active	Waiting for Wi-Fi Connection	Wi-Fi port is enabled but not connected to the user's STA, AP or P2P device. Waiting for the Wi-Fi connection. The LED blinks in Wi-Fi Direct (P2P) mode each time a connection request is made[1].
Flashing Yellow	Disconnected	Active	Waiting for Wi-Fi Connection with Default Settings	Wi-Fi port is enabled with default AP settings but not connected to the user's STA. Default settings have been activated by connecting the DIN_nWIFI_DEFAULT pin to DIN_GND on power-up.

LED	Subsystem state		Converter Status	Description
	Wi-Fi	CAN		
Steady Violet	Disconnected	Active	Wi-Fi Hibernated	Wi-Fi port is disabled. DIN_nWIFI_HIB pin is connected to DIN_GND. The Wi-Fi NWP is in the hibernation (low power) state with RF transmitter and receiver disabled.
Flashing Violet	Disconnected	Disconnected	Idle. NWP factory default configuration has been successfully restored.	The NWP factory default configuration has been successfully restored. Disconnect DIN_nWIFI_DEFAULT and DIN_nWIFI_HIB pins from DIN_GND and cycle the power for the normal converter operation.
Steady Red	Any	Passive	CAN Error	CAN controller is in the Passive state due to CAN errors. *Check the CAN line connection, baud rate, terminating resistors.*
Flashing Red	Any	Any	System Error	Unrecoverable system error. Device failure. This status should not happen during converter operation. *Try to perform the hardware reset by cycling the power. Contact Axiomatic if this does not help.*
Alternate Green/Red	Disconnected	Disconnected	Bootloader Mode	The converter will go to the Bootloader mode for a short period of time to flash the new firmware uploaded through the converter website. It will leave the Bootloader mode automatically after the flashing operation is over.
Alternate Red/Yellow	Disconnected	Disconnected	Restoring NWP factory default configuration	The converter is in the process of restoring NWP factory default configuration. DIN_nWIFI_DEFAULT and DIN_nWIFI_HIB pins have been connected to DIN_GND on power-up.

[1] For firmware version 4.00 or higher.

2.3 Logical Structure

The Wi-Fi to CAN Converter is internally organized as a system of interconnected independent modules. It includes the following internal modules: *Communication Device, Web Server*, and *Network Discovery*. They are connected to an external Wi-Fi network via the *Network Processor*, see Figure 2.

All internal converter modules are accessed using IP (internet protocol) network interface. They share the same address, mask and default gateway settings assigned to the *Communication Device* but use different communication ports and protocols.

The *Network Processor* module connects all internal converter modules to an external IP network via a wireless Wi-Fi connection.

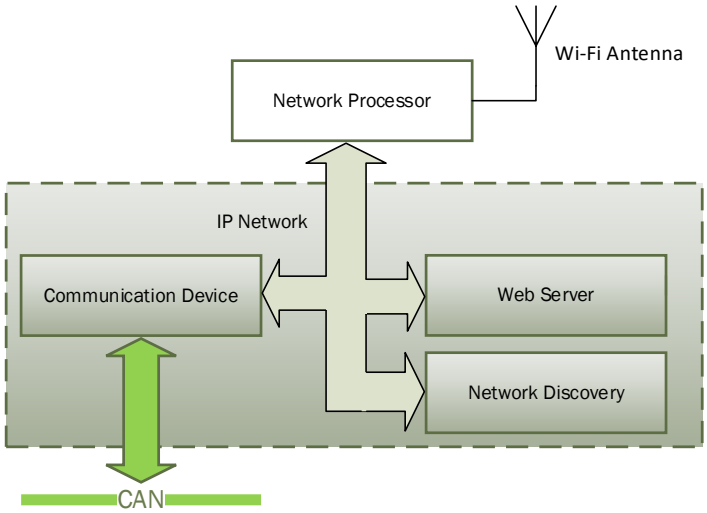

Figure 2. Converter Logical Structure

2.3.1 Communication Device

The *Communication Device* module is responsible for the protocol conversion between CAN and IP networks. It utilizes a proprietary communication protocol to communicate CAN messages and other auxiliary information over the IP network.

The *Communication Device* supports a client/server communication model. In this model, the converter has a primary server role, allowing external clients to establish independent connections with the converter.

In addition to the server role, the converter can also act as a client, if the *Auto Connect to Remote* configuration parameter is set to *Yes*. In this case, the converter will try to establish a connection with a customer specified remote server.

The total number of remote connections is limited to 10. If the CAN network traffic is high, this number should be further reduced, or the connections will become unstable due to limited internal resources of the microcontroller, which are dynamically allocated between open connections.

The *Communication Device* can use either UDP or TCP IP, depending on the value of the *Device Port Type* configuration parameter.

2.3.1.1 UDP Protocol

The UDP protocol is set by default. Since it is a connectionless protocol, one data socket serves all device communication needs, see Figure 3.

All connections with the device are virtual. On the server side, the device analyzes the incoming traffic to check for the new connections. Once a new IPAddress:Port combination is detected, the connection is established, and the device starts sending CAN data with *Heartbeat* messages to the new node.

There are no restrictions on the IP address and port for the incoming connections.

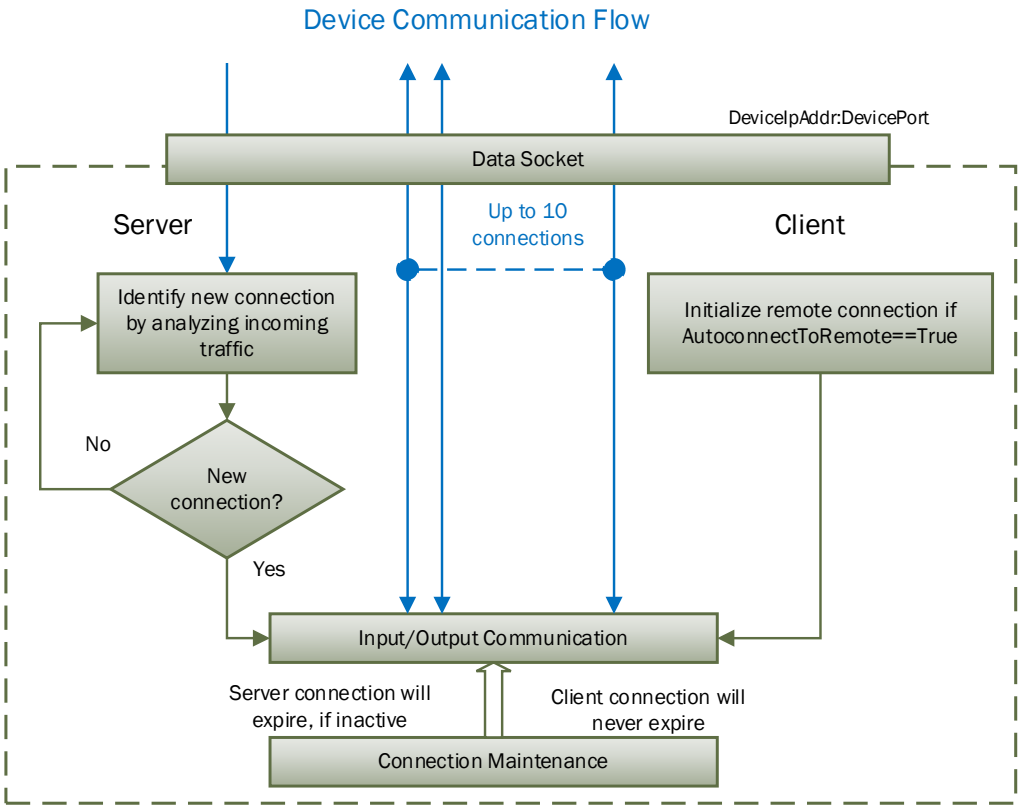

Figure 3. Communication Device. UDP Protocol

If a client-side is activated by the *Autoconnect to Remote* configuration parameter, the device will automatically start sending CAN data with Heartbeat messages to the remote node on start-up.

To ensure that the device does not send data to not functioning (“dead") or disconnected nodes, the server-side connections will expire in 10 sec of inactivity, when no valid data is received from the remote node. The client-side connection will never expire.

2.3.1.2 TCP Protocol

When TCP protocol is used, the *Communication Device* opens an individual data socket for each device connection, see: Figure 4.

The server side opens a listening socket for incoming connections. Once a connection is accepted, a new data socket is created to handle input/output communication with the remote node. There are no restrictions on the IP address and port for the incoming connections, similar to the UDP mode.

On the client side, if *Auto Connect to Remote* is set to *Yes*, a data socket is created for connection with the remote node. A random free port number is assigned to the socket. If the connection drops, the device will try to automatically reconnect with the node to maintain the client connection.

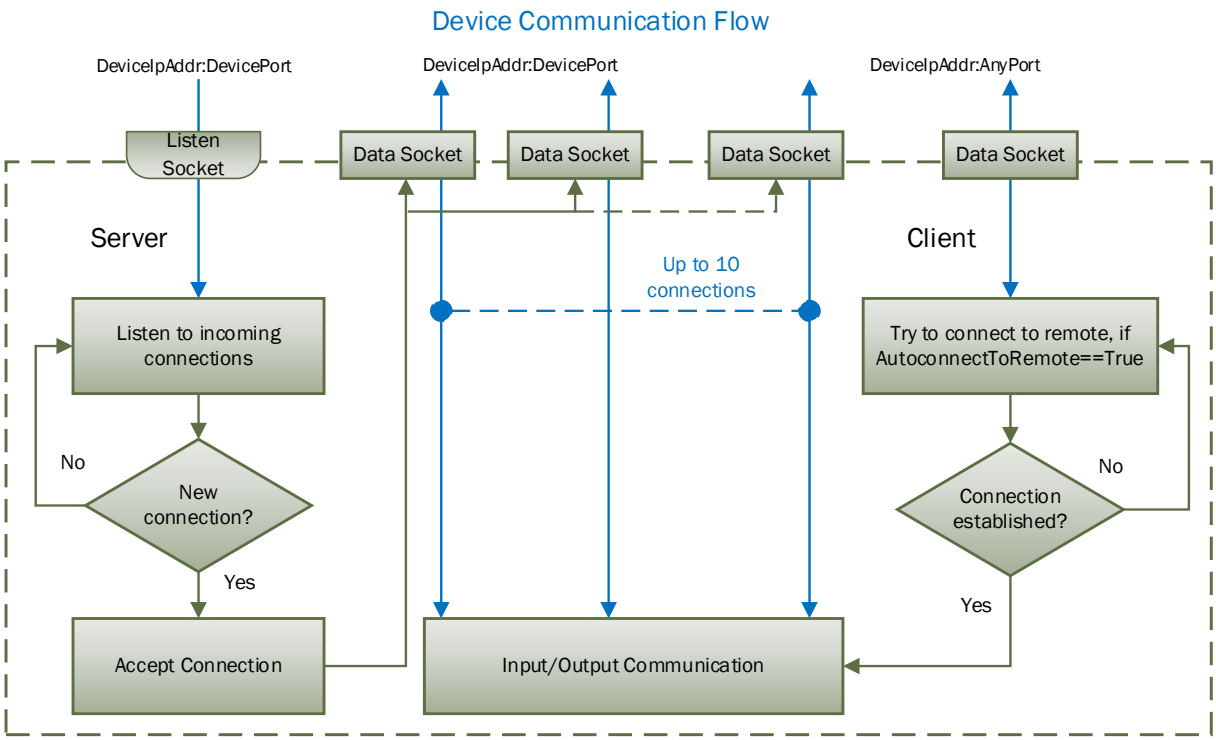

Figure 4. Communication Device. TCP Protocol

2.3.2 Web Server

The *Web Server* provides a user front-end interface with the converter. It runs a dynamic website that shows: the converter general information, configuration parameters, and the converter real-time diagnostics.

The user can also change configuration parameters and upload the new firmware through this website.

The web browser should support JavaScript.

2.3.3 Network Discovery

The *Network Discovery* module supports a proprietary Axiomatic discovery protocol. It allows to locate a converter with unknown IP address and/or web server port on a LAN using a simple Axiomatic discovery application `AxioDisc.exe`.

2.3.4 Network Processor

The *Network Processor* module is responsible to maintain a wireless Wi-Fi connection with an external IP network. It can work in: Station (STA), Access Point (AP) or Wi-Fi Direct (P2P) mode. The connection can be secured with a password using WEP or WPA / WPA2 security protocols in STA and AP modes.

The user has an ability to select an RF channel in either 2.4GHz or 5GHz frequency band in the AP mode. Up to 4 stations can be simultaneously connected to the module in the AP mode.

The P2P mode works only in 2.4GHz frequency band. The user can select operational and listen channels.

The user should explicitly select whether the P2P device operates in Client or GO mode. Only one Client can be connected to the converter in P2P GO mode. GO-NoA protocol is not supported.

3 CONVERTER CONFIGURATION

The converter supports configuration over the internal website running on the device embedded web server. To configure the device, the user should establish a wireless Wi-Fi connection between the converter and a user's device, which can be, for example, a laptop or a smartphone.

3.1 Wireless Connection

The converter default wireless settings, configured at the factory, are presented in Table 2. The user's device should use these settings to connect to the Wi-Fi to CAN converter.

Table 2. Wi-Fi Default Settings

Parameter	Default Value
Connectivity Mode	AP (Access Point)
Country/Region Code	USA
AP Channel	6 (2.4GHz frequency band)
Security	WPA / WPA2[1]
SSID (Network Name)	Axiomatic_CANWiFi
Password	CANWiFi_16025

[1]WPA / PSK and WPA2 / PSK security types, or a mixed mode of WPA / WPA2 PSK security type (TKIP, AES, mixed mode).

In case the converter settings were changed at the customer site, the default settings can be activated by pulling the DIN_nWIFI_DEFAULT input low on power-up. This can be achieved by connecting the DIN_nWIFI_DEFAULT input to DIN_GND. The Status LED on the housing will be flashing yellow in this case.

The default Wi-Fi settings, activated by the DIN_nWIFI_DEFAULT input, do not rewrite the original Wi-Fi settings in the von-volatile memory. The converter will return to its original settings after the next power-up or reboot.

When the default settings are used, the converter will appear on the list of available Wi-Fi networks on the user's device, see an example on Figure 5.

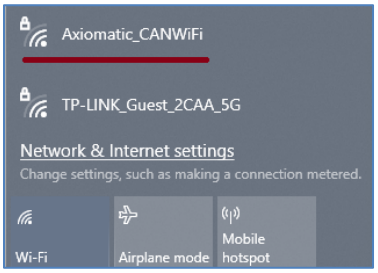

Figure 5. Converter AP on the List of Available Networks

If the converter does not appear on the list of available Wi-Fi networks after waiting for a reasonable time, there is a possibility that the network processor (NWP) needs to be reset to the factory default configuration, see Reset Network Processor to Factory Defaults section.

The user should connect to the converter using the default password "CANWiFi_16025" and with the manual IP settings. The assigned IP address should not conflict with the converter

Device IP Address (default value 192.168.0.34) and with addresses of other devices connected to the user's device, if any. See an example on Figure 6.

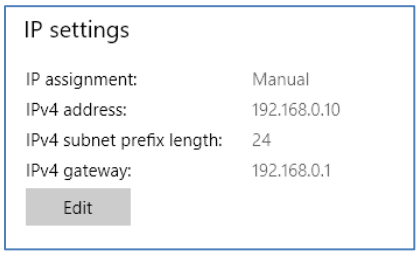

Figure 6. User Manual IP Settings

When the wireless connection is established, the user can access the converter embedded web server using any web browser on their device. The web browser should be pointed to the *Device IP Address* (default value 192.168.0.34). It is not necessary to specify the *Web Server Port* if the web server uses a standard port 80, which is set by default.

In case the *Device IP Address* or port has been changed and the value is lost, the Axiomatic `AxioDisc.exe` Windows console application can be used to recover the values, see Converter Discovery section for details.

After a successful connection, the user will see the device home page, see Figure 7.

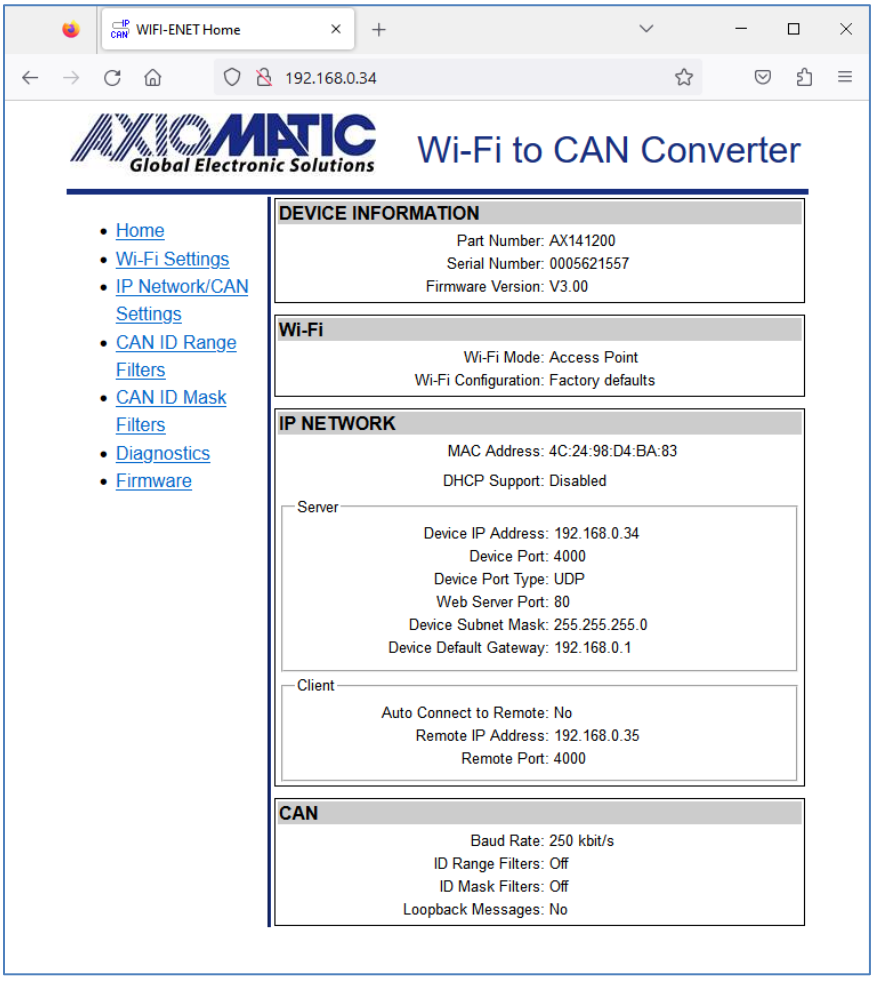

Figure 7. Converter Home Page[1]

[1] *Firmware Version Number* on the figure may not match the user manual version number.

The home page shows the device information, including the converter part number, serial number, and firmware version. It also shows *Wi-Fi*, *IP Network* and *CAN* configuration parameters including the status of *CAN ID Range* and *CAN ID Mask* input filters.

You will need to allow the site to run JavaScript (this setting is default in the majority of web browsers). If JavaScript is disabled, the website will show a message asking to activate JavaScript at the top of the web page, see Figure 8.

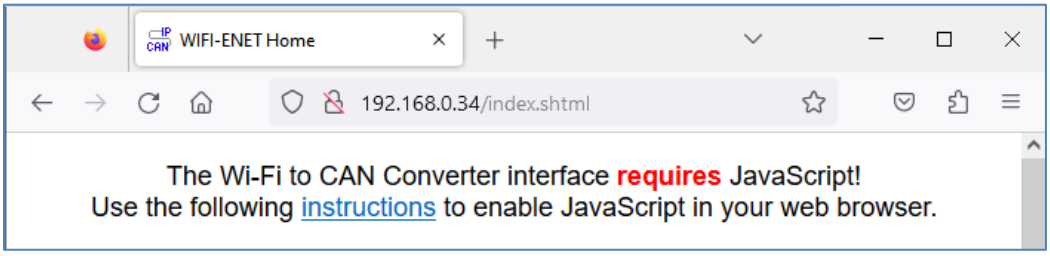

Figure 8. Enable JavaScript Prompt

The *IP Network* configuration parameters are combined into *Server* and *Client* groups for convenience.

The *IP Network* and *CAN* configuration parameters have tooltips clarifying their meaning, see Figure 9.

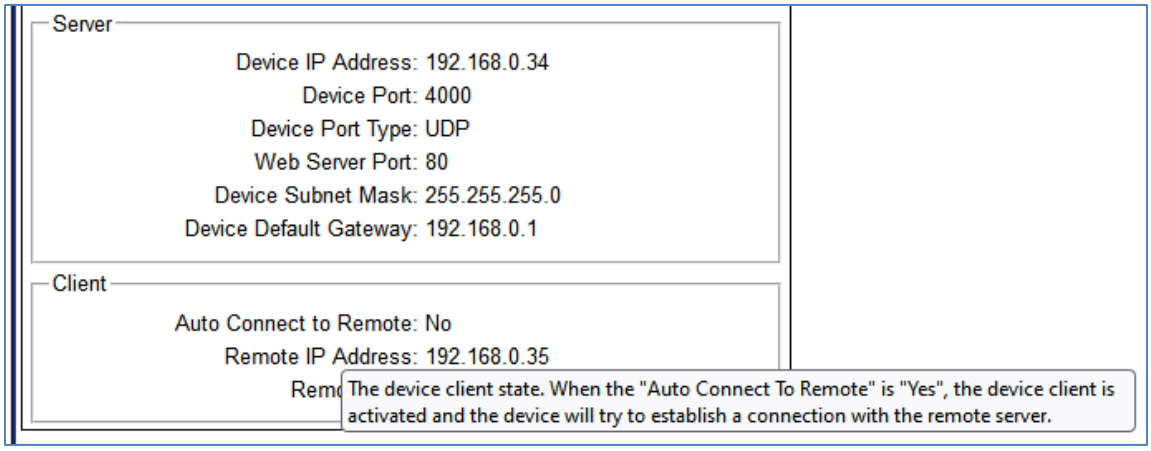

Figure 9. A Tooltip for the "Auto Connect to Remote" Configuration Parameter

3.2 Changing Configuration Parameters

The converter configuration parameters are grouped into the following configuration pages: *Wi-Fi Settings*, *IP Network/CAN Settings*, *CAN ID Range Filters* and *CAN ID Mask Filters*. The configuration pages can be reached by clicking on their links on the left side of the website, see Figure 10.

Each configuration web page has fields to enter values of the configuration parameters and four buttons: *Save Settings*, *Discard Settings, Reboot Converter* and *Set Defaults*, see Figure 10. The CAN configuration web pages, *CAN ID Range Filter* and *CAN ID Mask Filter,* do not have *Reboot Converter* button since the changes to the CAN interface are applied immediately upon saving the new settings in non-volatile memory without rebooting of the whole converter[1].

[1]Firmware versions 2.03 or earlier applied IP Network settings immediately after saving. Starting from firmware version 3.00, IP Network settings on the *IP Network/CAN Settings* web page are applied only after the converter reboot the same way as Wi-Fi Settings.

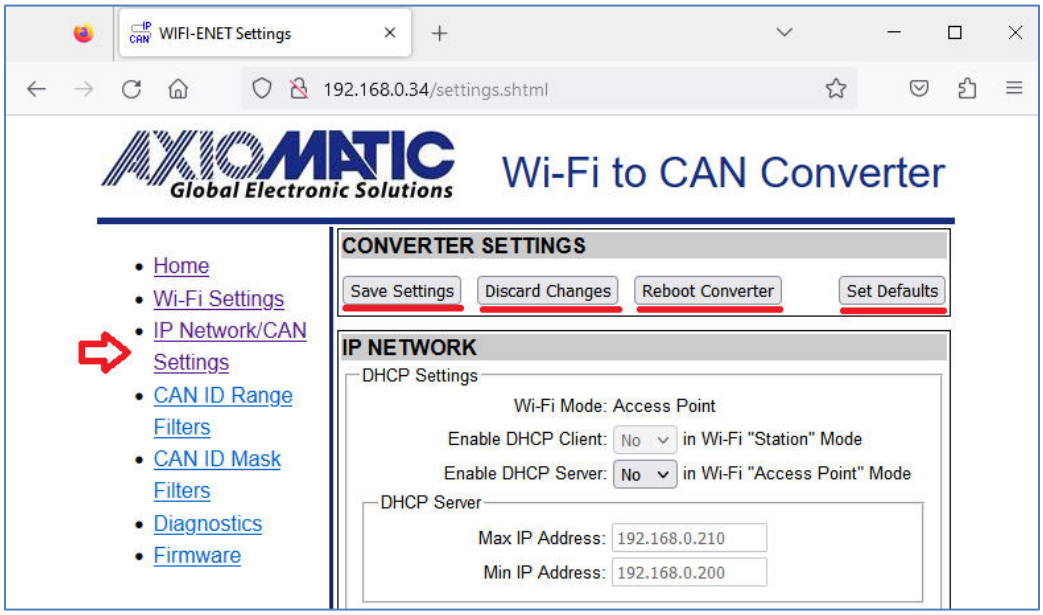

Figure 10. IP Network/CAN Settings Configuration Web Page

The *Save Settings* button will save configuration parameters in non-volatile memory and apply changes to the CAN interface if necessary.

The *Discard Changes* button will bring back the original converter settings before they have been changed on the website. In case the user leaves the page without saving, all changes will be also discarded.

The *Set Defaults* button will load default values of the configuration parameters into the data fields on the configuration page. The *Set Defaults* button will only set default values to configuration parameters on the current configuration page. Configuration parameters on other configuration web pages will not be affected.

The configuration parameters have tooltips for the user convenience.

When the user presses *Save Settings* button, the web page runs a script to check the validity of the new configuration parameters before uploading them to the web server. For example, the following alert message will be displayed if the user enters the same value for the *Device Port* and the *Web Server Port*, see Figure 11.

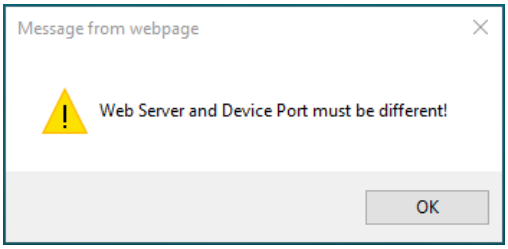

Figure 11. Settings Alert. Error in Configuration Parameters

The website messages should be enabled (not suppressed) in the browser to see this and other feedback messages.

After pressing the *Save Settings* button and saving the configuration parameters in non-volatile memory, the converter replies with a confirmation message showing the result of the saving operation. For example, if the user has successfully changed the *IP Network/CAN* configuration parameter, the following message will appear, see Figure 12.

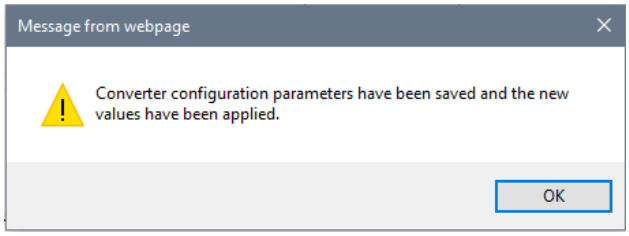

Figure 12. Settings Alert. Configuration Parameters have been Changed Successfully

3.3 Wi-Fi Configuration

The Wi-Fi configuration parameters control the converter wireless connection. Their status is shown on the home page, see Figure 13.

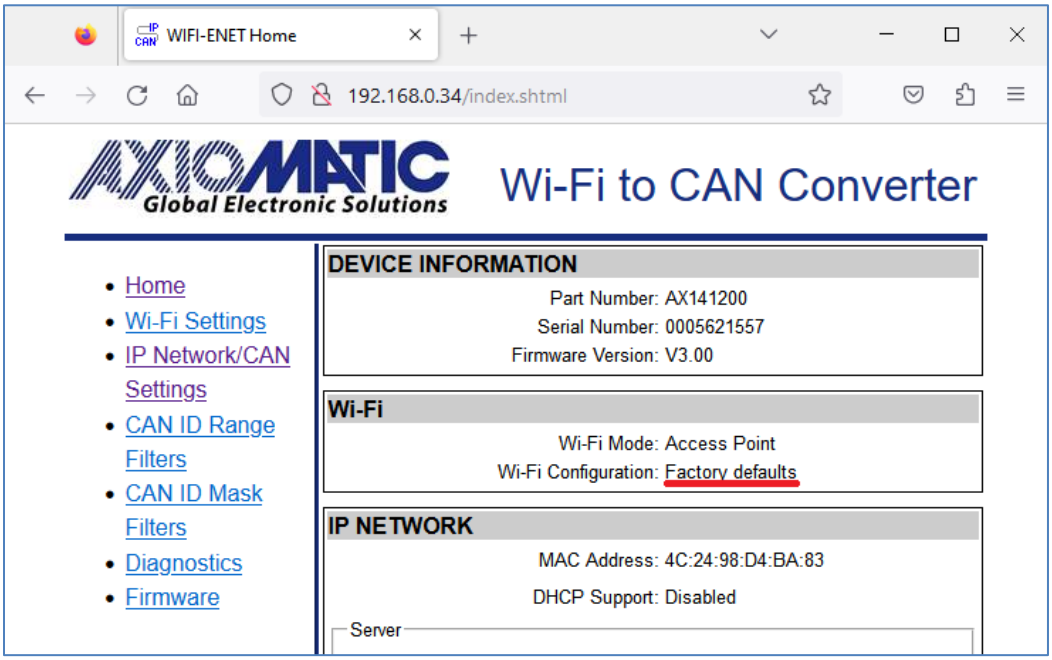

Figure 13. Wi-Fi Configuration Status[1]

[1] *Firmware Version Number* on the figure may not match the user manual version number.

The user can change the Wi-Fi configuration parameters on the *Wi-Fi Settings* configuration page, see Figure 14.

Parameters in *Station, Access Point* and *Wi-Fi Direct* modes are set separately. The *Country* configuration parameter applies to both: *Station* and *Access Point* modes.

The Wi-Fi configuration parameters are presented in Table 3. The converter needs to be reboot for the changes to be applied. Remember that connection with the user's device running the web browser can be lost after the reboot.

Figure 14. Wi-Fi Settings Configuration Page

Table 3. Wi-Fi Configuration Parameters

Configuration Parameter	Default Value	Range	Description
Wi-Fi Mode	Access Point	{Access Point, Station, P2P Client, P2P GO}	In the Station (STA) mode, the converter connects to an external Wi-Fi access point (AP), for example a router. In the Access Point (AP) mode, other wireless devices are connected to the converter.

Configuration Parameter	Default Value	Range	Description
			In the P2P Client mode, the converter is connected to a P2P GO device. In the P2P GO mode, a P2P Client device is connected to the converter.
Country	USA	{List of countries and regions of the world[4]}	Select a country or region where the converter is used. Defines the list of RF channels used by the converter. This is necessary to conform with local laws since incorrect settings may cause RF interference.
Station Mode			
Wireless Network Name	Axiomatic_CANWiFi	ASCII String, 1…32 characters	SSID of the AP the converter will try to connect
Security	WPA2	{Open, WEP[1], WPA2[2]}	Security protocol of the wireless connection with the AP. *WPA2* applies to both: WPA and WPA2 protocols. No security if *Open*
Password	CANWiFi_16025	For WEP: 5 or 10 characters in HEX format[3], 13 or 26 characters in ASCII format.	Password of the AP. Not used if *Security* is *Open*
		For WPA2: 8...63 characters in ASCII format.	
Fast Connection[7]	No	{Yes, No}	Connect to the previously successfully connected AP. Roaming is disabled. If connection is not successful within 2 minutes or at first-time connection, connect to any AP with *Wireless Network Name* SSID.
Access Point Mode			
Wireless Network Name	Axiomatic_CANWiFi	ASCII String, 1…32 characters	SSID of the converter
Security	WPA2	{Open, WEP[1], WPA2[2]}	Security protocol of the wireless connection used by the converter. *WPA2* applies to both: WPA and WPA2 protocols. No security if *Open*
Password	CANWiFi_16025	For WEP: 5 or 10 characters in HEX format[3], 13 or 26 characters in ASCII format.	Password of the converter. Not used if *Security* is *Open*
		For WPA2: 8...63 characters in ASCII format.	
RF Channel	6	{List of available channels depends on the selected *Country*}	Select an RF channel with the minimum interference from 2.4GHz or 5GHz frequency range. Only channels allowed in the selected country/region

Configuration Parameter	Default Value	Range	Description
			will be shown in the list of available channels.
Wi-Fi Direct (P2P) Mode			
Device Name	Axiomatic_CANWiFi	ASCII String, 1…32 characters	Name of the Wi-Fi Direct device
Device Type[6]	FF-B437D100-00	ASCII String, 12…17 hex characters	Type of the Wi-Fi Direct device. Use format: <*Category ID*>-<*OUI*>-<*Sub Category ID*>[5]. Fields are in hexadecimal format. Default value encodes: Axiomatic, category "Others" device.
Auto-Connect to GO	Yes	{Yes, No}	Defined only in the *P2P Client* mode. The pairing GO Device should have "CANWiFi" sub-string in its *Device Name* to activate the auto-connection procedure.
Listen Channel	11	{1, 6, 11}	Channel used for device discovery
Operational Channel	6	{1, 6, 11}	Channel used for device communication

[1] WEP open security.
[2] WPA / PSK and WPA2 / PSK security types, or a mixed mode of WPA / WPA2 PSK security type (TKIP, AES, mixed mode).
[3] HEX format contains ASCII characters: "0…9", "a…f", "A…F", representing a hexadecimal value. The HEX option was added starting from firmware version 2.01.
[4] Worldwide option was removed from the *Wi-Fi Country* list starting from firmware version 2.01 and automatically replaced with USA if set in earlier versions.
[5] See Appendix B.2. Primary Device Type. Wi-Fi Direct® Specification v1.9.
[6] Added in Firmware version 3.00. Firmware versions 2.03 or earlier have a non-configurable *Device Type* with default value 1-0050F204-1.
[7] Added in Firmware version 5.00.

Warning for users of firmware version 2.00 or earlier. Do not set the *Wi-Fi Country* configuration parameter to "Worldwide". This can cause a permanent lock-up of the converter that cannot be fixed in the field.

Users of such versions are encouraged to update their firmware to the newest one from Axiomatic website www.axiomatic.com, log-in section.

Both: *P2P Client* and *P2P GO* Wi-Fi Direct modes use Push-Button Configuration (PBC) as Wi-Fi Protected Setup (WPS) Method.

3.4 IP Network Configuration

The converter IP network configuration parameters are presented on the *IP Network/CAN Settings* web page, see Figure 15.

The converter *MAC Address* shown on the *Home* page is a read-only parameter. The user-changeable network configuration parameters are presented in Table 4.

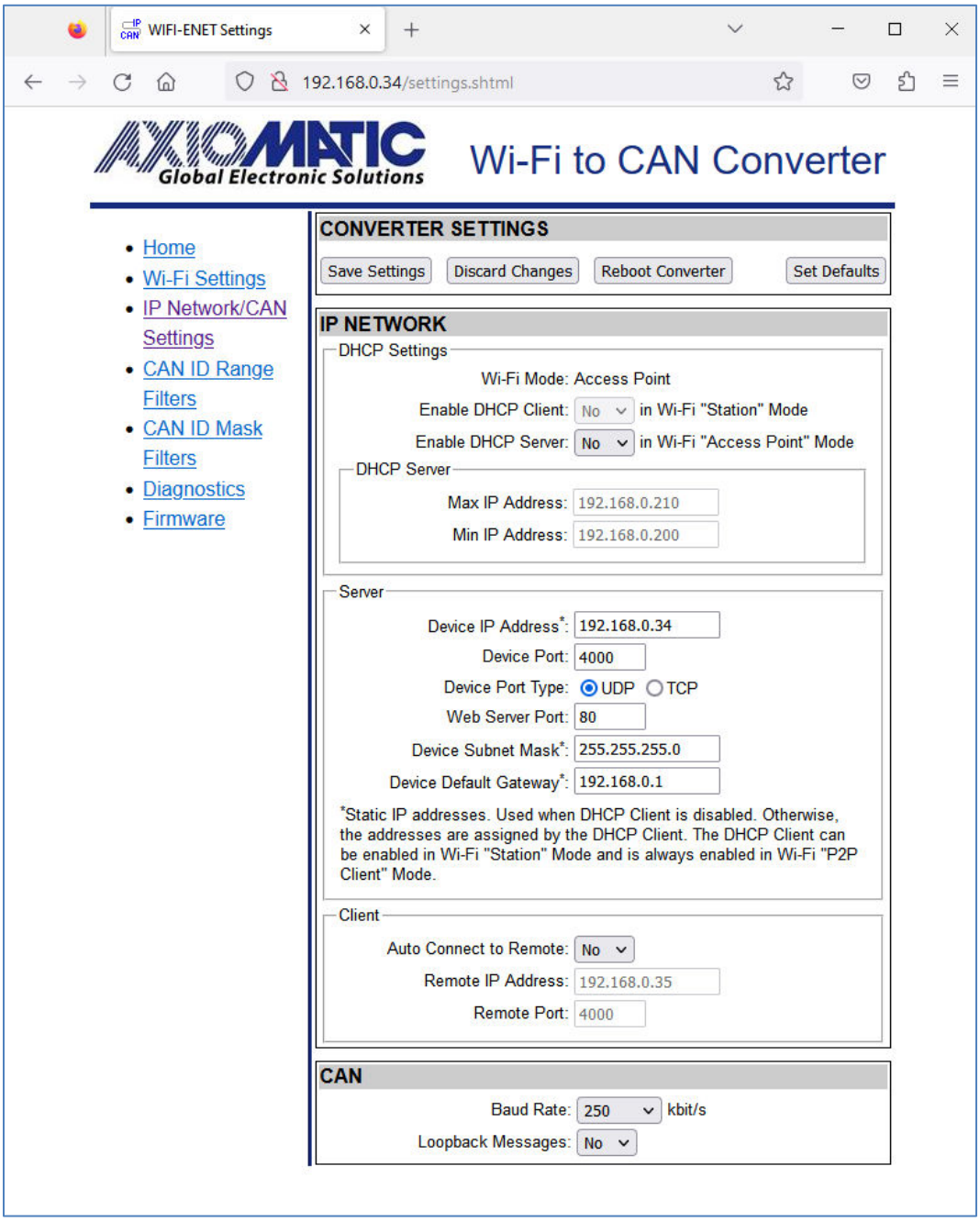

Figure 15. IP Network/CAN Configuration Page

Table 4. Network Configuration Parameters

Configuration Parameter	Default Value	Range	Description
DHCP Setting			
Enable DHCP Client in "Station" Mode[1]	No	{No, Yes}	Enable DHCP Client in "Station" mode only. DHCP Client is always enabled in Wi-Fi Direct P2P Client mode.
Enable DHCP Server in "Access Point" Mode[1]	No	{No, Yes}	Enable DHCP Server in "Access Point" mode only. DHCP Server is always enabled in Wi-Fi Direct P2P GO mode.

Configuration Parameter	Default Value	Range	Description
Max IP Address[1]	192.168.0.210	Any IP address except the *Device IP Address*	The address should be on the same subnet as the *Device IP Address*. The maximum number of addresses between the *Min IP Address* and *Max IP Address* cannot exceed 10 independently of the *Max IP Address* value.
Min IP Address[1]	192.168.0.200	Any IP address except the Device IP Address	The address should be on the same subnet as the *Device IP Address*.
Server			
Device IP Address[2]	192.168.0.34	Any IP address	The converter IP address
Device Port	4000	Any port value except the *Web Server Port* and the *Discovery Protocol Port*	The device server port. The device is listening to this port for incoming connections. The *Discovery Protocol Port* (35100) and the *Web Server Port* should not be used.
Device Port Type	UDP	{UDP, TCP}	Type of the IP protocol used by the device. The device server and client use the same IP protocol.
Web Server Port	80	Any port value except the *Device Port* and the *Discovery Protocol Port*	The communication port of the converter web server
Device Subnet Mask[2]	255.255.255.0	Any IP address	The converter subnet mask
Device Default Gateway[2]	192.168.0.1	Any IP address	The converter default gateway
Client			
Auto Connect to Remote	No	{No, Yes}	The device client state. When the *Auto Connect to Remote* is *Yes*, the device client is activated, and the device will try to establish a connection with the remote server.
Remote IP Address	192.168.0.35	Any IP address	The remote server IP address. Used by the device client when the *Auto Connect to Remote* is *Yes*.
Remote Port	4000	Any port value	The remote server port. Used by the device client when the *Auto Connect to Remote* is *Yes*.

[1] Added in Firmware version 3.00.
[2] Common parameter shared with all internal converter modules including the embedded web server. Must be assigned by a network administrator when DHCP Client is not used. Otherwise assigned by the DHCP Client.

The user can assign the IP network parameters either statically or dynamically, using DHCP[1]. The IP network parameters are always assigned dynamically in Wi-Fi Direct (P2P) modes.

[1] The IP network parameters were assigned only statically in firmware versions 2.03 or earlier.

For statical configuration, the user should avoid using special IP addresses (broadcast, multicast, loopback, etc.) when configuring the *Device IP Address* since this can lead to a permanent loss of communication with the embedded web server.

Using DHCP in *Station* mode can limit the converter server-side usage since the device address will be assigned by an external DHCP server. The converter client side will not be affected and can be used to connect to another converter.

When the device client is activated by setting the *Auto Connect to Remote* configuration parameter to *Yes*, the server side of the converter will still accept connections on the *Device Port* from other clients. This adds versatility to the converter configurations since the same converter can be used together with both: client and server communication nodes.

The DHCP *Max IP Address* and *Min IP Address* are disabled when Wi-Fi is in *Station* or *P2P Client* modes. It is also disabled in *Access Point* mode if the *Enable DHCP Server in "Access Point" Mode* is set to *No*.

The *Device IP Address*, *Device Subnet Mask*, and *Device Default Gateway* are disabled in Wi-Fi *P2P Client* mode and in the *Station* mode when *Enable DHCP Client in "Station" Mode* is set to *Yes*.

The *Remote IP Address* and *Remote Port* are disabled when *Auto Connect to Remote* is set to *No*.

If the user has changed the *Device IP Address* or the *Web Server Port*, the converter website should be manually relocated to the new location after the converter reboot[1].

[1] This relocation was done automatically in firmware versions 2.03 or earlier where the new IP parameters were applied immediately, without the converter reboot.

3.5 CAN Configuration

The main CAN configuration parameters can be configured on the *IP Network/CAN Settings* web page. They are presented in Table 5.

Table 5. Main CAN Configuration Parameters

Configuration Parameter	Default Value	Range	Description
Baud Rate	250 kbit/s	{1000, 666.6(6), 500, 250, 125, 100, 83.3(3), 50, 20, 10}	The CAN baud rate
Loopback Messages	No	{No, Yes}	Specifies, whether the messages received over the IP network and transmitted on the CAN bus, are sent back to the IP network. Setting this value to *Yes* can create an eternal loop when the same messages are bounced between two or more converters. Use with caution.

The CAN filters are set through their own web pages: *CAN ID Range Filters* and *CAN ID Mask Filters*. If all filters are disabled, all input CAN messages will be output on the IP network.

3.5.1 CAN ID Range Filters

The CAN ID range filters are configured on the *CAN ID Range Filters* configuration web page.

The user can independently configure five CAN ID range filters: *Filter 1, Filter 2, …, Filter 5.*

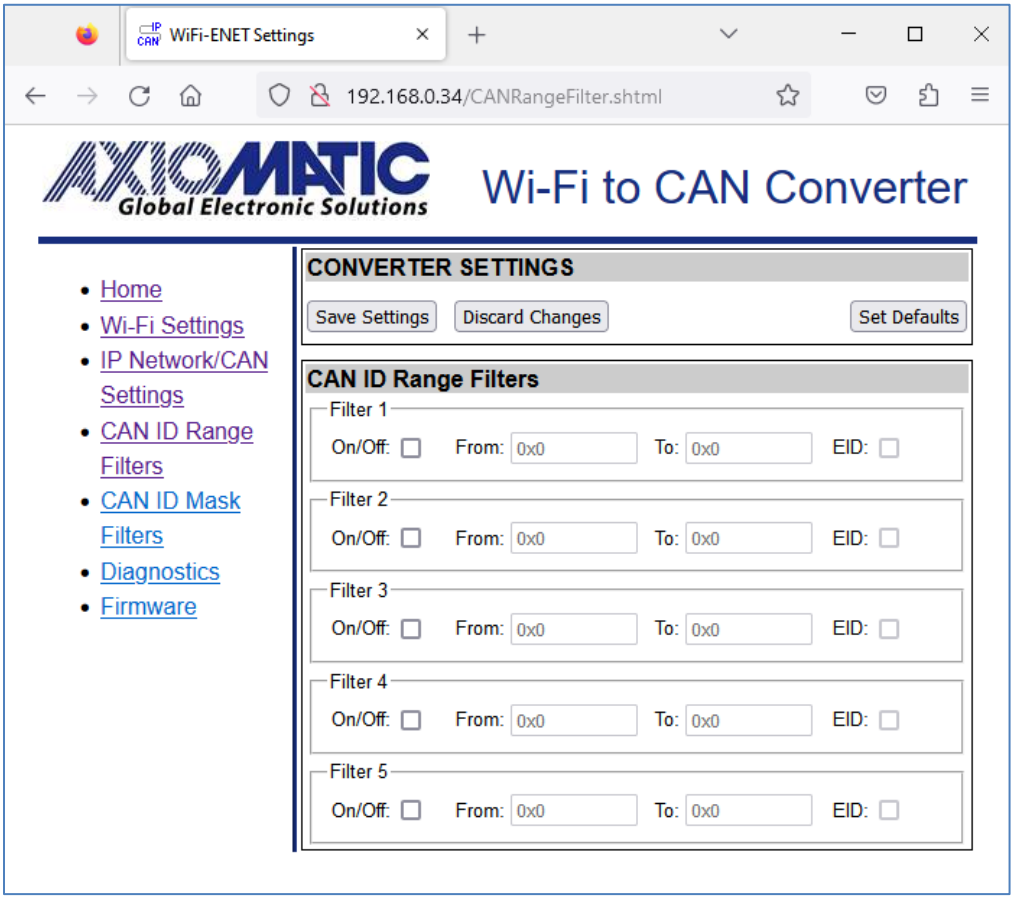

Figure 16. Converter CAN ID Range Filters Page

Once the filter is activated by checking the *On/Off* box, the CAN input messages will pass through to the IP network only if their CAN ID is within the range specified by *From* and *To* configuration parameters.

$$If\ ID_{CAN} \in [From;\ To],\ then\ the\ message\ is\ accepted. \qquad (1)$$

Where: ID_{CAN} – CAN message ID,
$From$ – *From* configuration parameter,
To – *To* configuration parameter.

The *EID* box (*Extended ID* box) defines whether the CAN message ID is regular or extended.

All CAN ID range filters run in parallel. It is sufficient to satisfy requirements of any active filter to pass the CAN message to the IP network.

If no active filters are defined, it is considered that the CAN ID range filters are disabled, and do not participate in the message filtering process. In this case, *ID Range Filters* are *Off* on the

home page, and, if other filters are also disabled, all CAN input messages will be sent to the network.

3.5.2 CAN ID Mask Filters

The CAN ID mask filters are set through the *CAN ID Mask Filter* configuration web page.

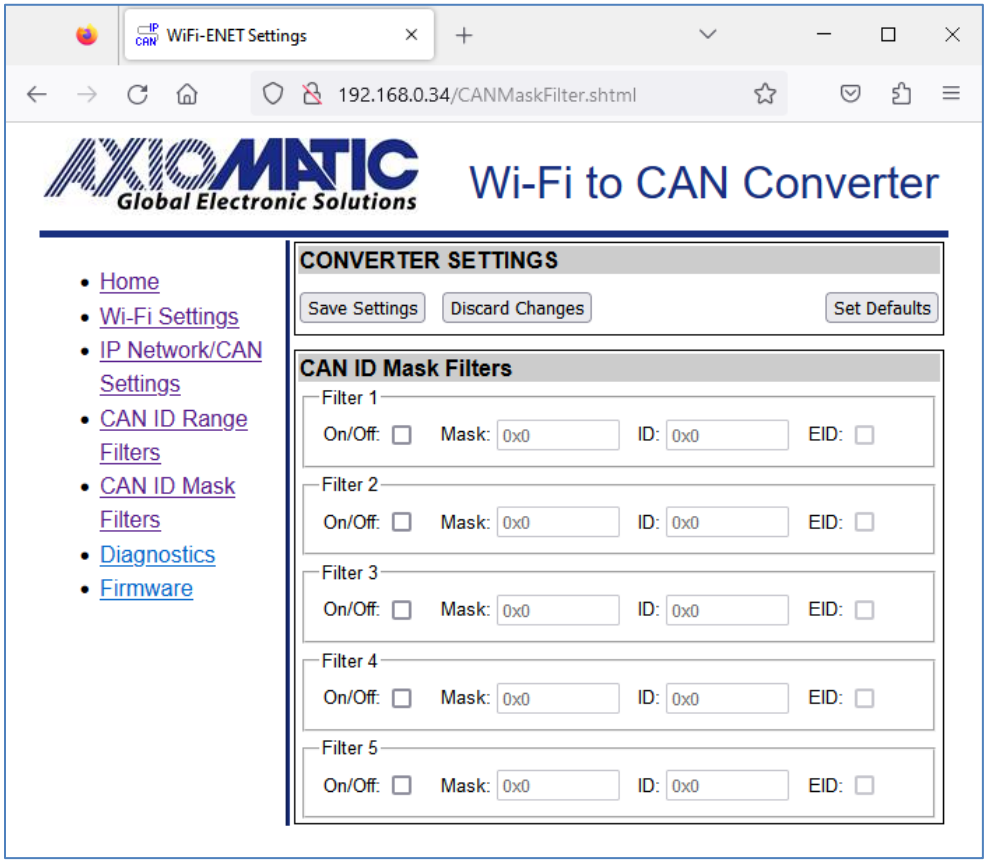

Figure 17. Converter CAN ID Mask Filters Page

There are five independent CAN ID mask filters: *Filter 1, Filter 2, …, Filter 5* available to the user.

Once the filter is activated by checking the *On/Off* box, the CAN input messages will pass through the filter to the IP network only if their CAN ID satisfies the following condition:

$$If\ ID = ID_{CAN}\ \&\ Mask,\ then\ the\ message\ is\ accepted. \qquad (2)$$

Where: ID_{CAN} – CAN message ID,
$Mask$ – *Mask* configuration parameter,
ID – *ID* configuration parameter,
& – Bitwise AND operator.

The *EID* box (*Extended ID* box) defines whether the CAN message ID is regular or extended.

All CAN ID mask filters run in parallel the same way as CAN ID range filters. It is sufficient to satisfy requirements of any active filter to send the CAN message to the IP network.

If no active filters are defined, it is considered that the CAN ID mask filters are disabled, and do not participate in the message filtering process. In this case, *ID Mask Filters* are *Off* on the home page, and, if other filters are also disabled, all CAN input messages will be sent to the IP network.

4 CONVERTER DIAGNOSTICS

The user can see a real-time diagnostic information on the *Diagnostics* page on the converter internal website. The connection to the converter embedded web server is described in the Converter Configuration section.

To load the *Diagnostics* page, Figure 18, the user should click on the *Diagnostics* link on the left side of the web page.

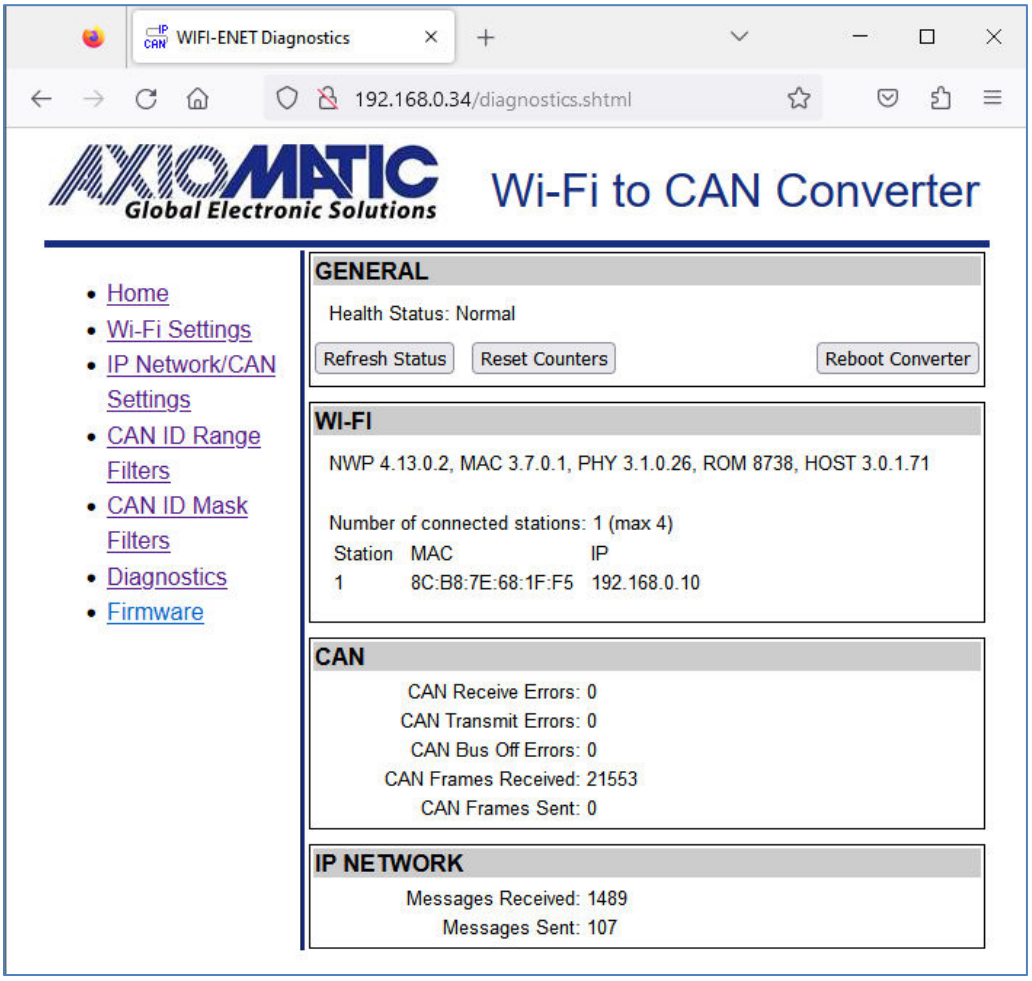

Figure 18. The Converter Diagnostics Page

The *Diagnostics* page shows *Health Status* of the converter together with the Wi-Fi diagnostic information, CAN, and IP Network statistics.

The user can refresh the values on the page by pressing the *Refresh Status* button or reset the statistic counters by pressing *Reset Counters* button. The *Reboot Converter* button activates the converter rebooting.

The converters do not retain the diagnostic information. All information is lost when the power is shut down.

4.1 Health Status

The converter *Health Status* is an aggregated system run-time parameter calculated on the base of operational statuses of the major device hardware and software components.

The *Health Status* presents the overall operational status of the converter, based on the following rules, see Table 6.

Table 6. Health Status

Health Status	Condition
Error	*Error* is reported when at least one operational status is in the *Error* state.
Warning	*Warning* is reported when at least one operational status is in the *Warning* state and there are no operational statuses in the *Error* state.
Undefined	*Undefined* is reported when at least one operational status is in the *Undefined* state and there are no operational statuses in the *Error* or *Warning* state.
Normal	*Normal* is reported when all operational statuses are in the *Normal* state.

If the *Health Status* is different from *Normal*, the user will see a verbose message on the *Diagnostics* web page below the *Health Status* describing which operational status is causing a problem.

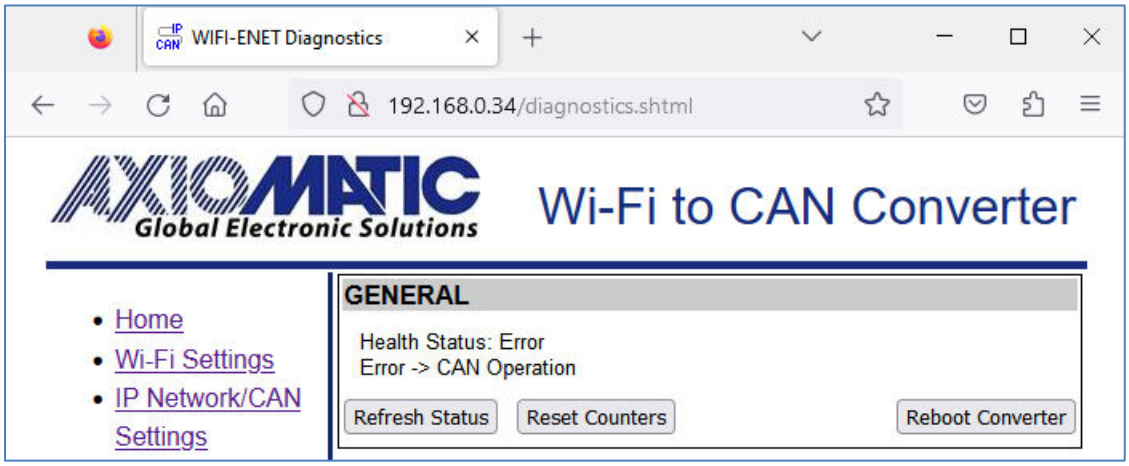

Figure 19. Health Status Message on CAN Error

In case several operational statuses differ from *Normal*, all of them will be shown on the *Diagnostics* page.

4.2 Converter Rebooting

The user can reboot the converter, when necessary, using the *Reboot Converter* button.

The converter rebooting operation takes 10 seconds. The user will see the *Reboot* screen with a countdown counter during this operation, see Figure 20.

When the rebooting is over, the *Diagnostics* page will be reloaded.

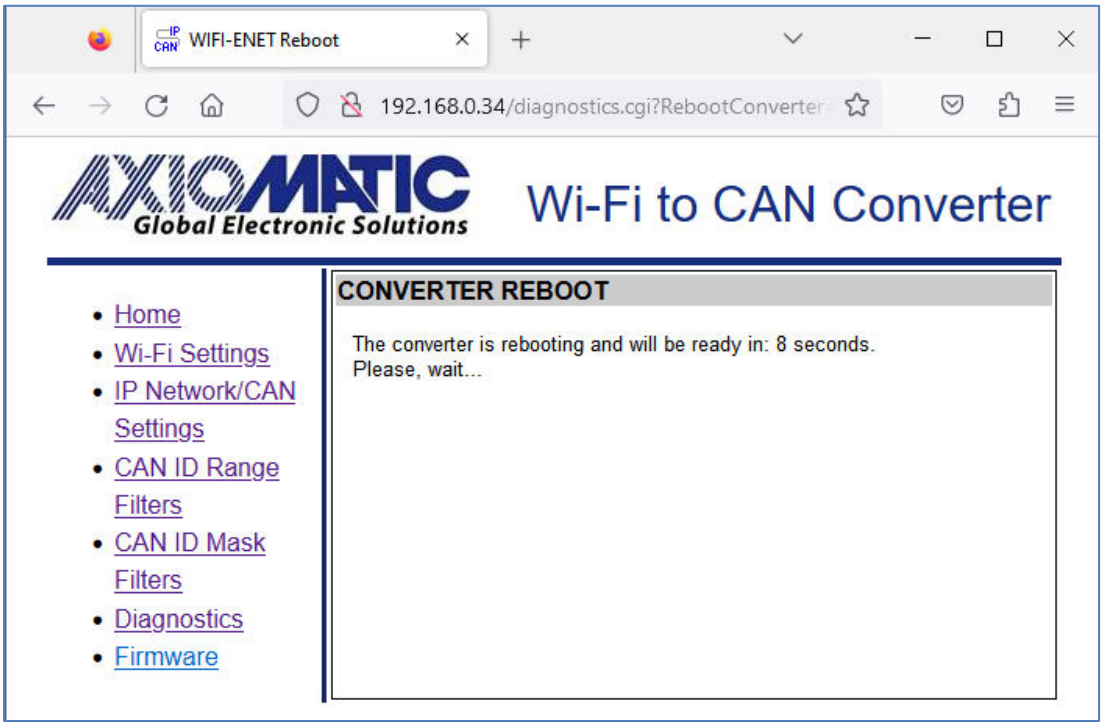

Figure 20. The Converter Reboot Screen

5 FIRMWARE UPDATE

The converter firmware can be updated over the air (OTA) through the converter internal website in the field.

The update procedure is performed in two stages. First, the application firmware is uploaded into the converter internal flash memory. During this stage, the converter checks the firmware checksum and whether it can be programmed into the unit.

Then, upon the user confirmation, the firmware is programmed into the microcontroller and the unit is restarted. At the end of this process, the user should see the version number of the installed firmware on the converter home page in the browser.

The details of the firmware update are provided below.

5.1 Uploading the New Firmware

To upload the new firmware, the user should activate the *Firmware Uploading* page, Figure 21, by clicking on the *Firmware* link on the left side of the web page.

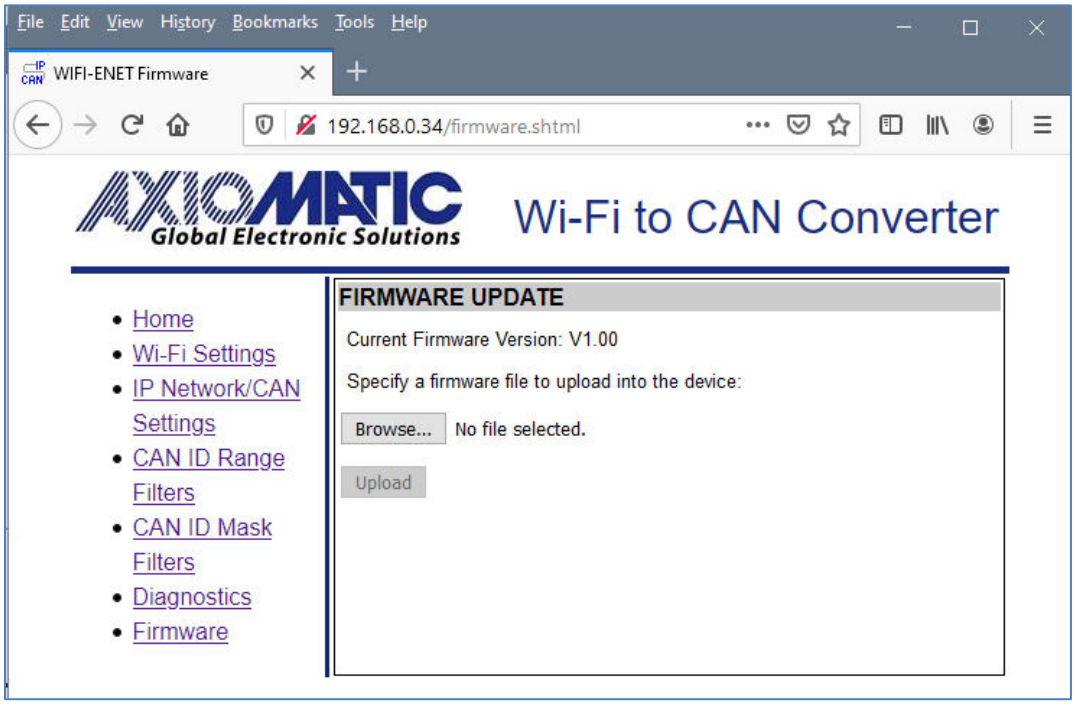

Figure 21. Firmware Uploading Page[1]

[1] Value of the *Current Firmware Version* on figure is for illustration only. The user will see the actual version number installed on the converter.

Then the user selects the new firmware file using the *Browse…* button.

The firmware file is provided by Axiomatic in a proprietary binary format with extension: `.af`.

The file name should have the following format: `AF-16025-X.XX.af`, where the `<X.XX>` field wildcard reflects the firmware version number. We will use `AF-16025-1.00.af` file for illustration of the firmware update process in this manual.

When the file is selected, the user should press the *Upload* button. The user will see the dynamic message: “Loading…” in the bottom of the screen and then, if everything is in order, the converter will switch automatically to the *Firmware Update* page.

5.2 Applying the New Firmware

On the *Firmware Update* page, the user will see the new firmware file information, see Figure 22.

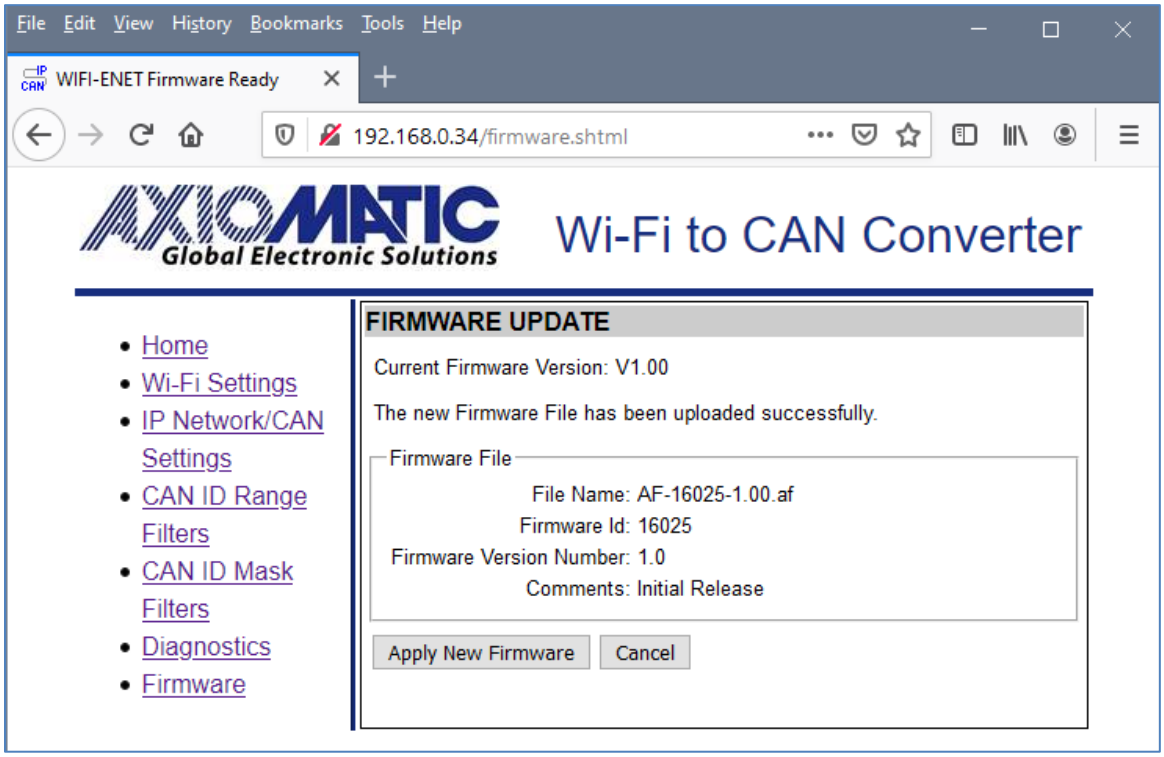

Figure 22. Firmware Update Page

From this point, the user can cancel the firmware update process and keep the old firmware or proceed with flashing the new firmware into the microcontroller by pressing the *Apply New Firmware* button.

When the user presses the *Apply New Firmware* button, the firmware update process is activated, and the *Firmware Upload* page will show the countdown timer, see Figure 23.

The countdown timer is set for 30 seconds that is necessary to complete the flashing process and reboot the unit.

Once the unit is rebooted, the Wi-Fi connection with the converter will be lost and the user will need to manually restore the wireless connection at the end of the countdown process. Once the Wi-Fi connection is restored, the converter home page will be displayed.

The user will see the new uploaded application firmware version number in the *Device Information* section on the converter home page, see Figure 24. In our example, it is the same 1.00 version number since we used the firmware version 1.00 to illustrate the firmware update process.

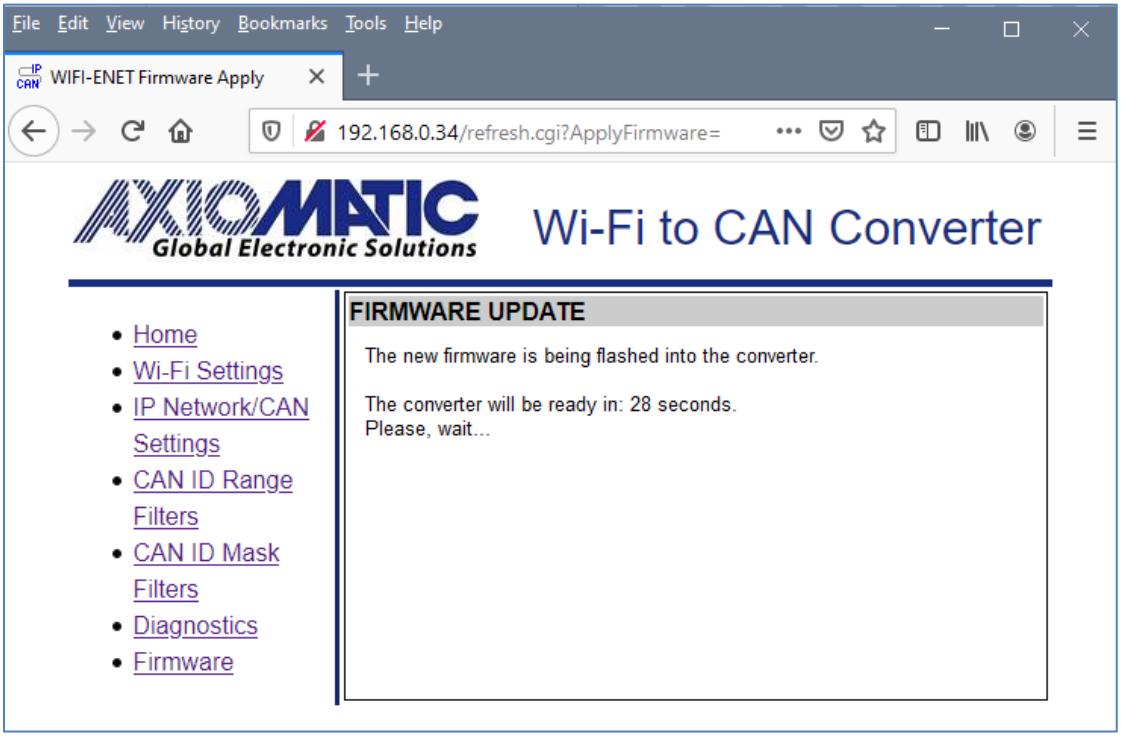

Figure 23. Firmware Update Countdown has been Started

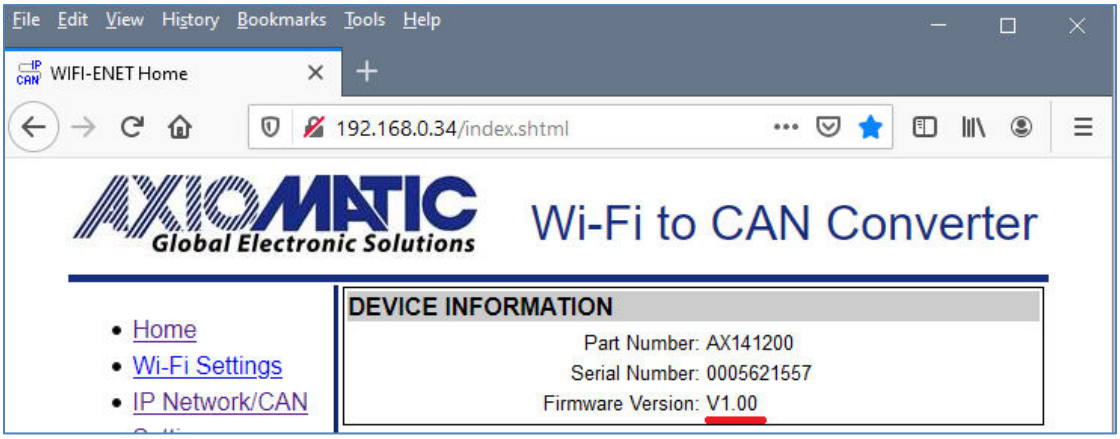

Figure 24. Firmware Version Number

6 RESET NETWORK PROCESSOR TO FACTORY DEFAULTS

There can be situations when it is necessary to reset the network processor (NWP) to the factory default configuration. In most cases this happens when the unit does not enter the configured or default state after switching the Wi-Fi mode several times.[1]

[1]Reset to NWP factory default configuration is available in firmware version 3.00 or higher.

To reset the network processor to the factory default configuration, the user should pull down both digital inputs: DIN_nWIFI_DEFAULT and DIN_nWIFI_HIB by connecting them to DIN_GND and cycle the power.

The reset procedure takes approximately 8 seconds. The Status LED will be alternating between red and yellow. At the end of the procedure, the Status LED will be flashing violate indicating that the NWP has been successfully reset to the factory default configuration.

The user should disconnect DIN_nWIFI_DEFAULT and DIN_nWIFI_HIB inputs from DIN_GND, and cycle the power to return to the device normal operation. Alternatively, only DIN_nWIFI_HIB input can be disconnected to return to the device default settings after the power cycle.

In case of an error condition, the Status LED will be flashing red. Contact Axiomatic if repeating the reset procedure does not solve the problem.

7 CONVERTER DEPLOYMENT

The converter can be used in two major ways. One way is to use a pair of converters as a wireless CAN bridge with or without a baud rate conversion. The second way is to connect the converter directly to monitoring device or indirectly through a Wi-Fi hotspot and access the CAN network remotely over the IP network.

7.1 Wireless CAN Bridge

In this configuration, a pair of coupled Wi-Fi to CAN converters can connect two CAN networks together over the air. This configuration can be extended to several CAN networks running at different baud rate and connected together using the Wi-Fi to CAN converters, see Figure 25.

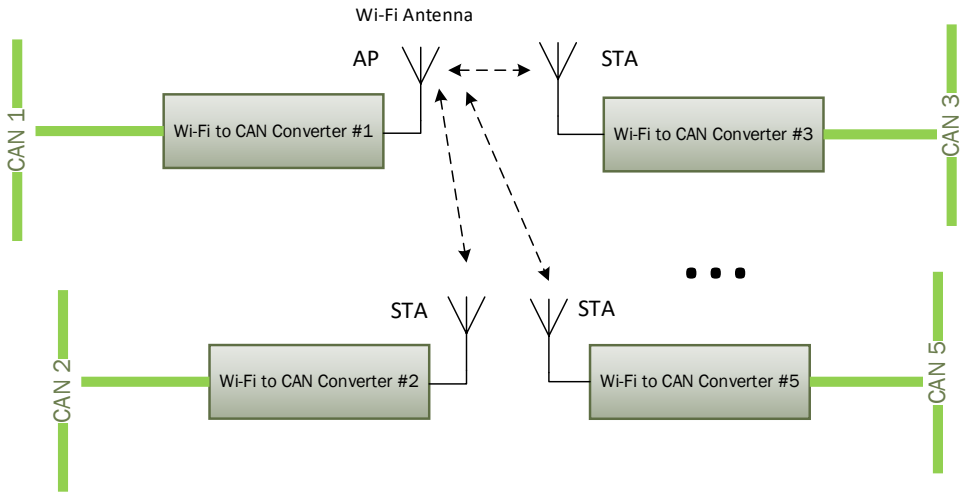

Figure 25. Wireless CAN Bridge with AP/STA Configuration

One converter should be configured as an Access Point (AP) and all others – as Stations (STA). Up to 4 STA can be connected to one AP bringing the maximum number of CAN networks bridged together in this configuration to 5.

This configuration does not require any custom software design. An example of the converter settings in case of a wireless CAN bridge with two Wi-Fi to CAN converters is described in the Wireless CAN Bridge Configuration Example.

7.2 Wireless CAN Access Point

A Wi-Fi to CAN converter in the wireless CAN bridge configuration, see Figure 25, can be replaced with a CAN monitoring IP device with a Wi-Fi interface, for example with a laptop or a smartphone, see Figure 26.

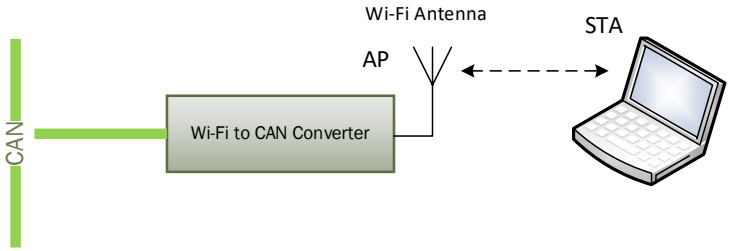

Figure 26. Wireless CAN Access Point

In this configuration, the converter is directly connected to the monitoring device through the Wi-Fi wireless link. The Wi-Fi to CAN converter acts as an Access Point (AP) and the IP device – as a STA. The same configuration is used for the initial converter setup, see Converter Configuration section.

7.3 Wireless CAN Station

In this configuration, a converter in STA mode is connected to a third-party AP and then all communication with the converter goes through this AP, see Figure 27.

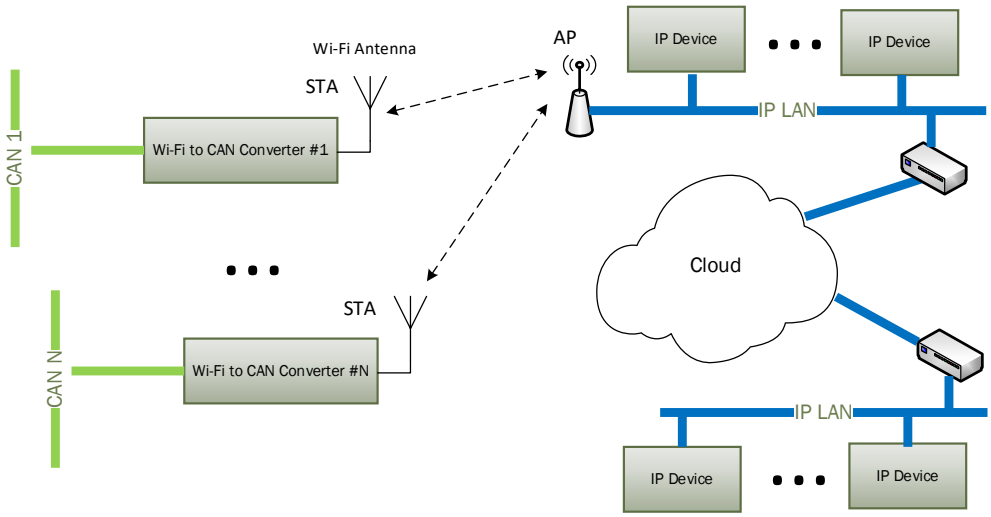

Figure 27. Wireless CAN Station

There can be several converters connected to one AP. The AP can be connected to IP devices through a LAN or over the cloud.

This configuration is the most versatile. It practically has no limits on the number of converters and CAN monitoring IP devices and the distance between the devices and the converters.

7.4 Wi-Fi Direct Connection

Two Wi-Fi to CAN converters can be connected together using Wi-Fi Direct (P2P) connection without creating an Access Point (AP), see Figure 28.

One of the converters should be configured as P2P Client and the other one – as P2P GO device. The Client will automatically connect to GO device when *Auto-Connect to GO* is set to *Yes* and the GO *Device Name* contains “CANWiFi” substring. The *Listen* and *Operational Channel* configuration parameters should be the same for the Client and GO devices.

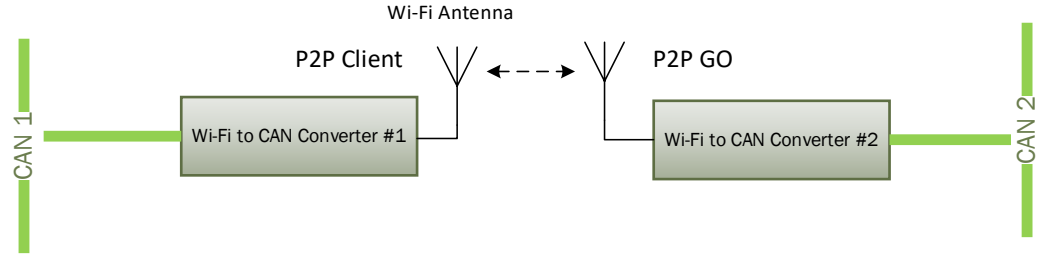

Figure 28. Wireless CAN Bridge with P2P Configuration.

This wireless CAN bridge configuration is limited to one Client and one GO device. Only 2.4GHz frequency band can be used. It can take up to several minutes to pair two converters in the Wi-Fi Direct mode.

To avoid limitations of the P2P connection, it is advisable to use AP/STA configuration, see Figure 25.

7.5 Converter Communication

All CAN monitoring IP devices should use an Axiomatic proprietary communication protocol to communicate with Wi-Fi to CAN converters. This protocol converts CAN messages into IP datagrams, see the Reference Documents in Table 9. The protocol is the same as being used in the Axiomatic Ethernet to CAN converter, p/n AX140900.

Axiomatic provides CAN-ENET Software Support Package (SSP), p/n AX140910, for interfacing with the converter and performing all necessary data conversions. The SSP is downloadable from www.axiomatic.com, log-in section. Due to differences in the *Health Status* coding between Ethernet to CAN and Wi-Fi to CAN converters, SSP version 2.0.0 or higher should be used.

All Axiomatic PC software tools supporting the Ethernet to CAN converter also support Wi-Fi to CAN converter by default; the user can select *Ethernet to CAN Converter* in configuration *Options* to communicate with the Wi-Fi to CAN Converter.

The *Axiomatic Electronic Assistant* (EA) can communicate with both: Ethernet to CAN and Wi-Fi to CAN Axiomatic converters starting from version 5.11.82.0, and the *CAN Assistant – Scope* and *CAN Assistant – Visual* support the converters starting from version 3.0.0.

7.6 Wireless CAN Bridge Configuration Example

An example of the converter settings for a CAN wireless bridge with two Wi-Fi to CAN converters is presented below. The converters are using AP/STA connection, see Figure 25.

The first converter is set to AP mode. We can use the default settings, see Table 3 and Table 4. The second converter should be in STA mode with security/password the same as the first converter, see Figure 29.

Do not reboot the converter right after saving the new Wi-Fi settings. Otherwise, the link with the user's device running the web browser can be lost.

The *IP Network Settings* of the second converter should be configured the way that its IP address be different from the IP address of the first converter, the client mode should be activated by setting the *Auto Connect to Remote* configuration parameter to *Yes*, and the client IP settings should match the server IP settings of the first converters, see Figure 30.

Now, after the second converter reboot, the two converters are fully configured and can be used to connect two CAN networks over the Wi-Fi wireless connection.

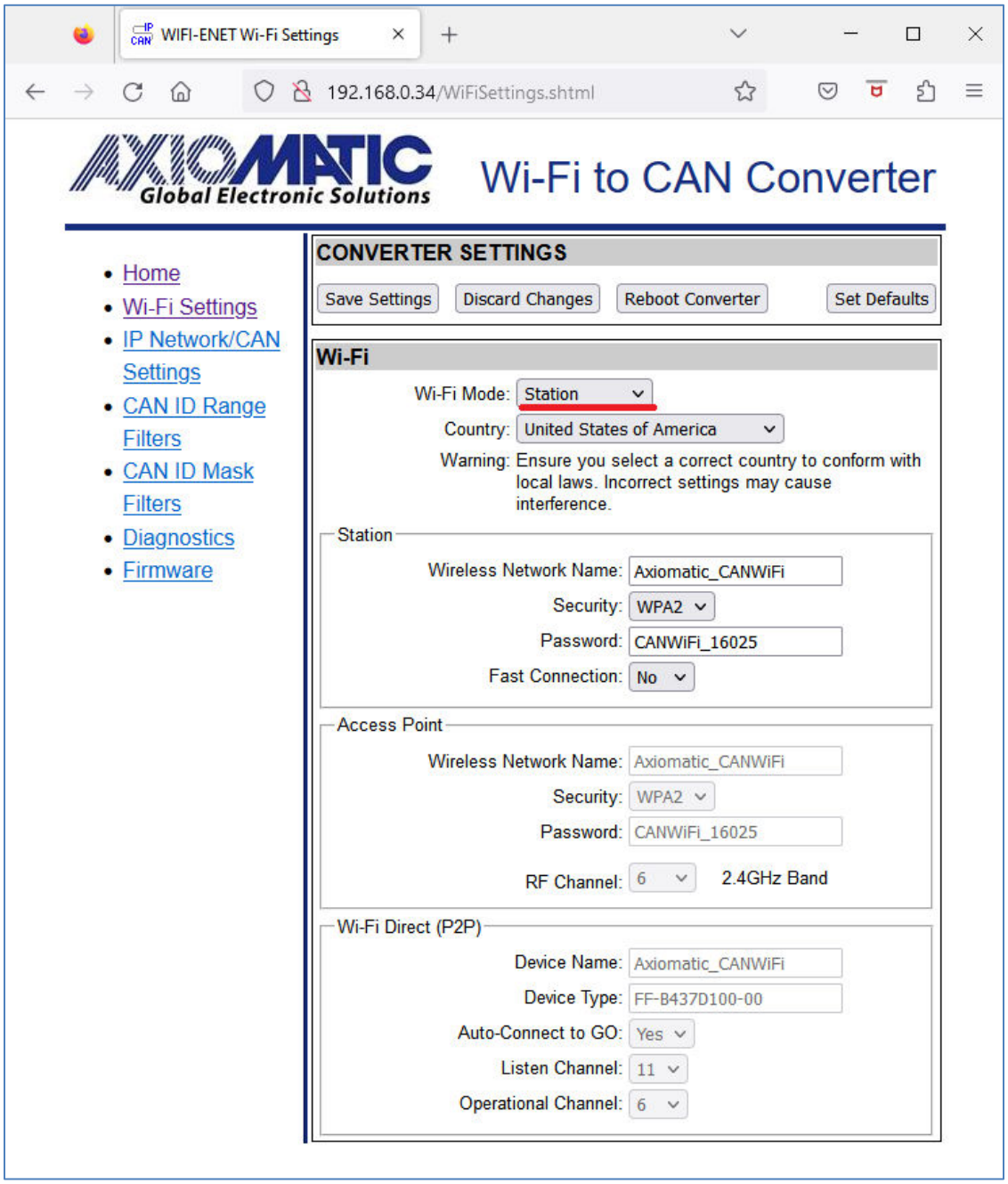

Figure 29. Wireless CAN Bridge Wi-Fi Settings

In case the baud rate of the CAN network is different from 250 kbit/s, it can be adjusted using *Baud Rate* configuration parameter on any of the converters. The same way, *CAN ID Range / CAN ID Mask* filters can be used to filter out CAN messages received by any of the converters.

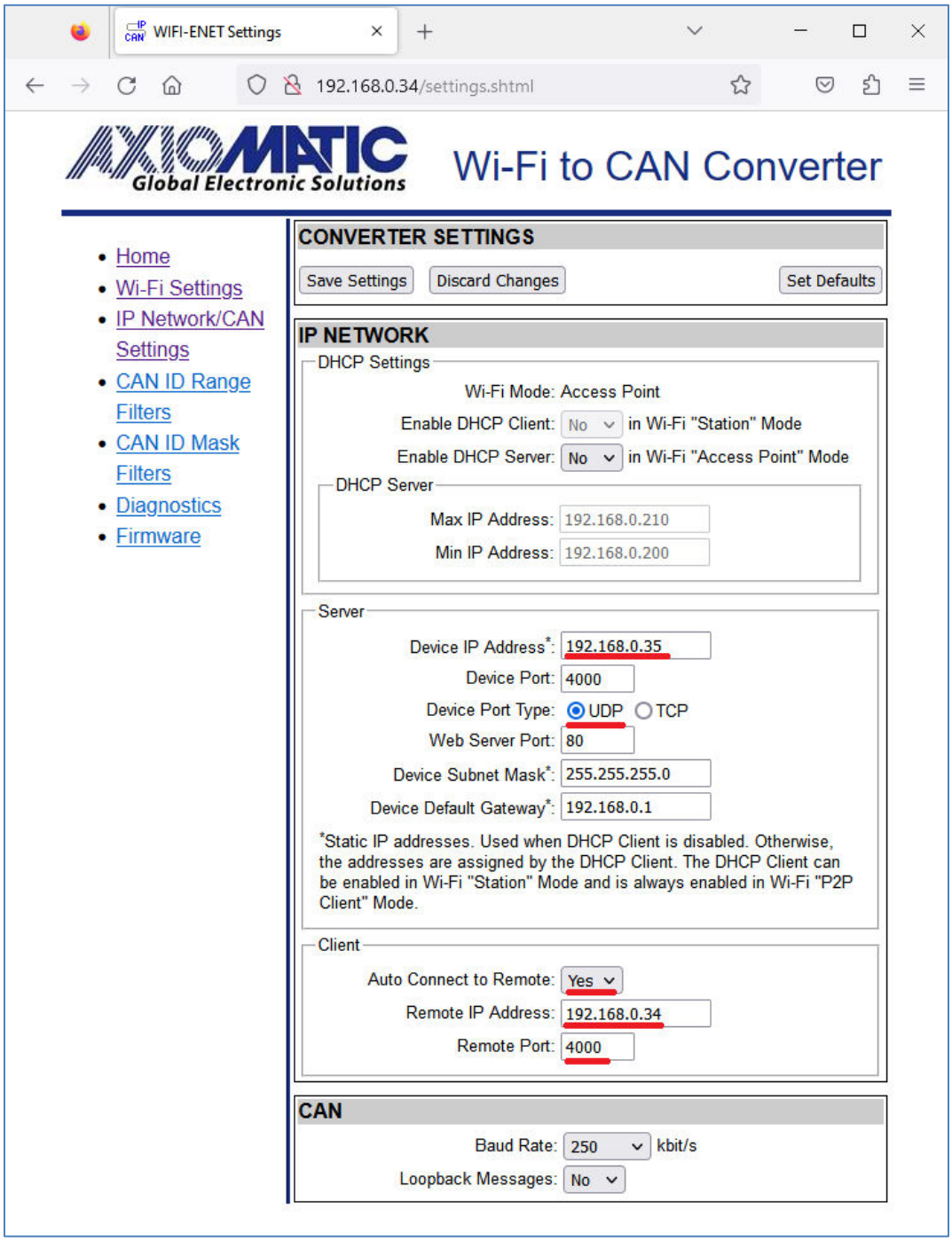

Figure 30. Wireless CAN Bridge IP Network Settings

8 CONVERTER DISCOVERY

In case the IP address and/or web server port is unknown or has been lost, the user can recover them using the Axiomatic `AxioDisc.exe` Windows console application. The application uses a proprietary discovery protocol and can recover IP locations of Axiomatic converters on a LAN. The `AxioDisc.exe` application is available upon request.

The application sends a UDP request to the global IP address `255.255.255.255`, port `35100`, and waits for the responses from converters located on the same local network.

The converter discovery response includes the unit MAC Address, IP Address, web server port, device port, device port type, the converter part number and serial number, see Figure 31.

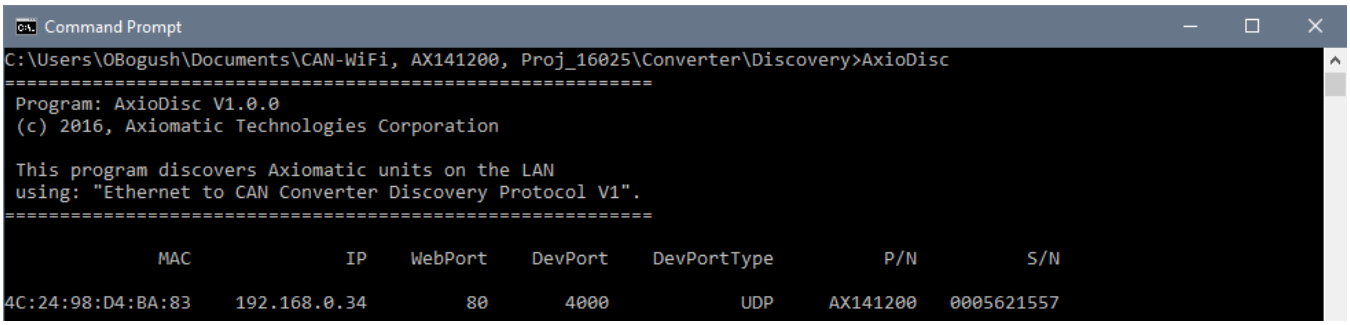

Figure 31. `AxioDisc.exe` Converter Discovery Application

The user should have a working Wi-Fi connection with the converter, see Wireless Connection section. If the user's laptop is also connected to other IP networks, for example to a LAN over Ethernet, these other networks should be temporarily disconnected and disabled for a reliable discovery of the Wi-Fi to CAN converter. This includes disabling of any virtual adapters from VPN, virtual machines, etc., installed on the PC.

The discovery protocol is also supported by the CAN-ENET Software Support Package, p/n AX140910.

The `AxioDisc.exe` application can run on Windows starting from Win XP SP3. It was tested on Win XP SP3, Win 7 and Win 10. In case the application cannot find standard dlls, the Visual C++ Redistributable for Visual Studio 2015 x86 must be installed on the user's computer from the Microsoft website: https://www.microsoft.com/en-ca/download/details.aspx?id=48145

9 TECHNICAL SPECIFICATIONS

9.1 Power Supply

The power supply uses automotive battery power.

Table 7. Power Supply Input

Parameter	Value	Remarks
Supply Voltage	9…36 VDC	12V, 24V – nominal
Supply Current[1]	65 mA 35 mA	Maximum at 12V Maximum at 24V
Protection	Reverse Polarity, Overvoltage, Transients	

[1]CAN bus is connected. Wi-Fi is in station mode connected to an access point.

9.2 Wi-Fi Port

Table 8. Wi-Fi Port Parameters

Parameter	Value	Remarks
Wireless Standards	802.11 a/b/g/n	802.11 a/b/g in Access Point mode
Frequency Ranges	2.4 GHz, 5 GHz	Available channels depend on the user selectable country/region of operation.
Antenna	Internal	
Communication Range	40 m	Reliable communication between two converters in open space
Connectivity Modes	Station, Access Point, Wi-Fi Direct (P2P)	Wi-Fi Direct is only supported in 2.4 GHz frequency range
Maximum Number of Stations	4	In Access Point mode
Maximum Number of Clients	1	In Wi-Fi Direct (P2P) GO mode
Security	Open, WEP, WPA / WPA2-PSK, PBC WPS in Wi-Fi Direct (P2P)	In Station and Access Point modes. PBC WPS in Wi-Fi Direct (P2P) Client and GO modes.
Firmware update	OTA	Using internal web server
Communication Protocols	IP, ICMP, ARP, UDP, TCP, HTTP, DHCP[2], Proprietary[1]	CAN messages are transmitted using a proprietary application protocol running on top of the user selectable UDP or TCP transport protocol [1]. Internal web server uses HTTP protocol. The unit supports an Axiomatic proprietary discovery protocol [2]. DHCP can be used for dynamic address assignment in Station and Access Point modes. It is always used in Wi-Fi Direct (P2P) Client and GO modes.
Server Mode	Up to 10 bi-directional simultaneous connections	Up to 9 connections, if the Client mode is enabled
Client Mode	1 remote connection	Auto-connect to a remote server if connection is dropped or temporarily unavailable. Client mode can be disabled.

Web server	Provided	Always enabled for converter configuration, diagnostics, and OTA firmware update
Internal Diagnostics	Health Status[1]	Internal health status of the converter is transmitted in heartbeat messages [3]. It is also available from the web server.
Wi-Fi Hibernation State	Provided	Controlled by an external digital input

[1]Supported by *CAN-ENET Software Support Package* (SSP), p/n AX140910, v2.0.0+.
[2]Added in firmware version 3.00.

Reference documents describing proprietary protocols and *Health Status* field format are presented below. The documents are available upon request.

Table 9. Reference Documents

Reference Number	Document Name
[1]	O. Bogush, "Ethernet to CAN Converter Communication Protocol. Document version: 4", Axiomatic Technologies Corporation, April 5, 2021.
[2]	O. Bogush, "Ethernet to CAN Converter Discovery Protocol. Document version: 1A", Axiomatic Technologies Corporation, April 5, 2021.
[3]	O. Bogush, "Ethernet to CAN Converter Health Status. Document version: 3", Axiomatic Technologies Corporation, April 5, 2021.

9.3 CAN Port

Table 10. CAN Parameters

Parameter	Value	Remarks
Number of Ports	1	
Port Type	High Speed, ISO 11898-2 compatible	120Ohm terminated twisted pair, baud rate up to 1 Mbit/s. External 120Ohm terminating resistor is required.
Baud Rate	1000, 666.6(6), 500, 250, 125, 100, 83.3(3), 50, 20, 10	[kbit/s]. Programmable through the web interface
Protocol	CAN Bosch 2.0A and B	Data Frames and Remote Frames with Standard and Extended IDs are supported.
Filtering	CAN ID Range/Mask	Disabled by default

CAN port does not contain 120 Ohm terminating resistor.

9.4 LED Indicator

A three-color LED indicator on the top side of the housing displays the current status of the converter.

9.5 General Specifications

Table 11. General Specifications

Parameter	Value	Remarks
Operating Temperature	-40…+85 °C	Industrial temperature range
Environmental Protection	IP67	IEC 60529
Vibration	TBD	
Shock	TBD	
Size	3.47 x 2.75 x 1.31 inches (88.2 x 70.0 x 33.3 mm)	L x W x H including integral connector. See dimensional drawing.

Parameter	Value	Remarks
Weight	0.15 lb	

9.6 RF Regulatory Restrictions

Caution. This converter should be installed and operated with a minimum distance of 20 cm from a human body.

The user is responsible to properly select the country or region of operation to conform with local laws. Incorrect settings may cause RF interference.

The converter is restricted to indoor use only when operating in the 5GHz frequency range, channels: 32…68 (5150 to 5350 MHz) in the following countries.

AT	BE	BG	HR	CY	CZ	DK
EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL
PT	RO	SK	SI	ES	SE	UK

9.7 RF Module Compliances

The converter uses Texas Instrument CC3135MOD RF module. The CC3135MOD module meets the following regulations.

Table 12. CC3135MOD Regulatory Compliances

Regulatory Body	Regulation	Certificate ID (If Applicable)
FCC (USA)	Part 15C + MPE FCC RF Exposure	Z64-CC3135MOD
IC/ISED (Canada)	RSS-102 (MPE) and RSS-247 (Wi-Fi)	451I-CC3135MOD
ETSI/CE (Europe)	RED 2014/53/EU and RoHS2 2011/65/EU	—
MIC (Japan)	Article 49-20 of ORRE	201-190034

9.7.1 Module FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
• This device may not cause harmful interference.
• This device must accept any interference received, including interference that may cause undesired operation of the device.

CAUTION

FCC RF Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

9.7.2 Module CAN ICES-3(B) and NMB-3(B) Statement

This device complies with Industry Canada license-exempt RSS standards. Operation is subject to the following two conditions:

- This device may not cause interference.
- This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deus conditions suivantes:

- L'appareil ne doit pas produire de brouillage.
- L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage ests susceptible d'en compromettre lu fonctionnement.

CAUTION

IC RF Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cut équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

9.7.3 Module EC Declaration of Conformity

The module is in compliance with Radio Equipment Directive 2014/53/EU and RoHS2 Directive 2011/65/EU.

9.8 Accessories

Table 13. Accessories

Axiomatic P/N	Description
AX140910	Software Support Package (SSP). Downloadable from www.axiomatic.com, log-in section.
AX070112	Mating plugs kit. It includes: P/N: DT06-08SA — Quantity: 1 piece P/N: W8S — Quantity: 1 piece P/N: 0462-201-16141 — Quantity: 8 pieces P/N: 114017 — Quantity: 3 pieces

9.9 Connector

8-pin receptacle (equivalent to TE Deutsch P/N: DT04-08PA). Mates with DT06-08SA. Mating plugs kit, AX070112, is available.

Table 14. Converter Pinout

Pin #	Description
1	BATT -
2	BATT +
3	CAN_L
4	CAN_H
5	DIN_GND

Pin #	Description
6	DIN_nWIFI_DEFAULT (Active Low)
7	Not Used
8	DIN_nWIFI_HIB (Active Low)

Digital inputs DIN_nWIFI_DEFAULT and DIN_nWIFI_HIB have internal pull-ups and are activated by connecting them to DIN_GND.

When digital inputs DIN_nWIFI_DEFAULT and DIN_nWIFI_HIB are pulled down simultaneously at power-up, they activate procedure that restores NWP factory default configuration.[1]

[1]Available in firmware version 3.00 or higher.

9.10 Housing

Injection molded enclosure and 8-pin welded faceplate, which is equivalent to a TE Deutsch P/N. Material: PA66, 30% glass fiber reinforced, flame retardant UL 94 V-0. Ultrasonically welded. For dimensional drawing, see Figure 32.

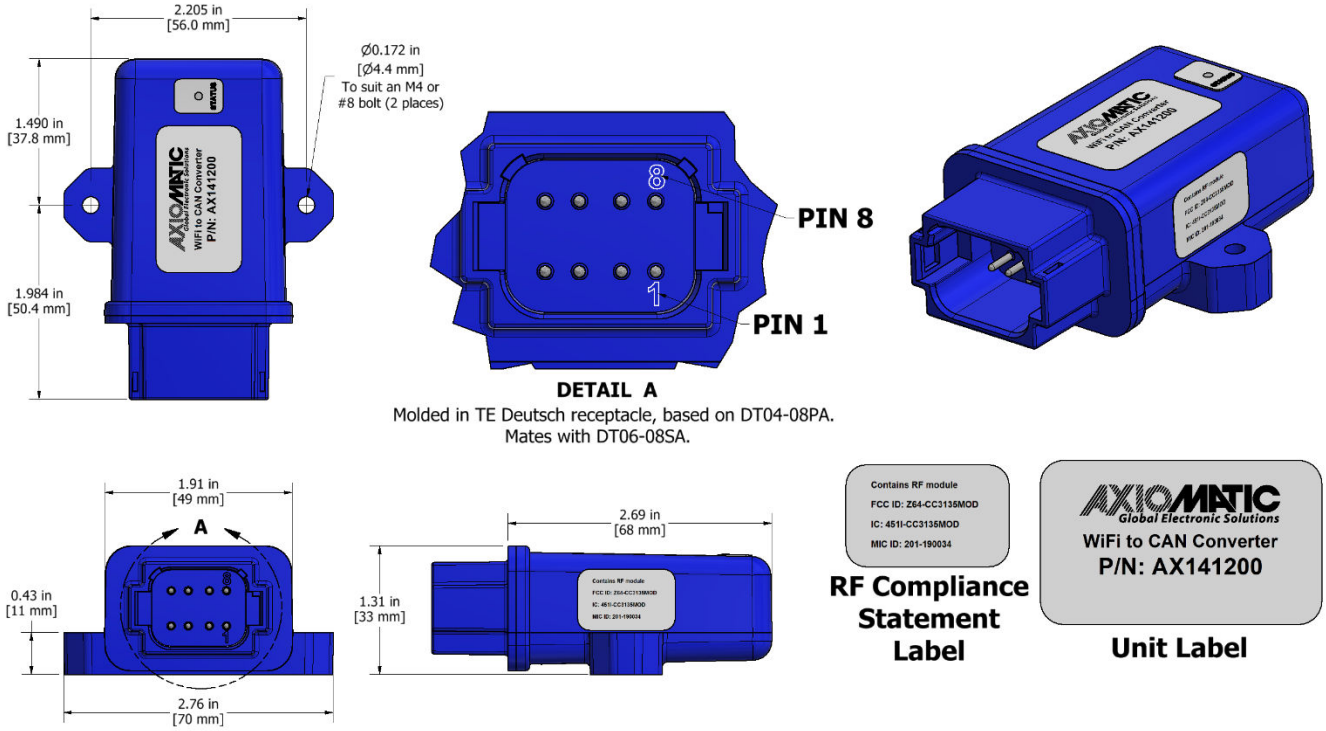

Figure 32. Dimensional Drawing

10 THIRD PARTY SOFTWARE LICENSE NOTICES

This section contains Third Party Software License Notices and/or Additional Terms and Conditions for licensed third-party software components included in the Wi-Fi to CAN Converter firmware.

Table 15. Third Party Software License Notices

Third Party Software	License Notice/Terms
STMicroelectronics microcontroller support software	COPYRIGHT(c) 2015 STMicroelectronics Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of STMicroelectronics nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. COPYRIGHT(c) 2014 STMicroelectronics Licensed under MCD-ST Liberty SW License Agreement V2, (the "License"); You may not use this file except in compliance with the License. You may obtain a copy of the License at: http://www.st.com/software_license_agreement_liberty_v2 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. Copyright (c) 2016 STMicroelectronics This software component is licensed by STMicroelectronics under the **BSD-3-Clause** license. You may not use this file except in compliance with this license. You may obtain a copy of the license [here](https://opensource.org/licenses/BSD-3-Clause).
ARM CMSIS	Arm CMSIS is licensed under Apache License, Version 2.0, January 2004, http://www.apache.org/licenses/LICENSE-2.0

Third Party Software	License Notice/Terms
FreeRTOS V10.4.3	Copyright (C) 2021 Amazon.com, Inc. or its affiliates. All Rights Reserved. MIT License Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Simplelink SDK WiFi Plugin V4.20.00.10 Simplelink cc32xx SDK V6.10.00.05	Copyright (c) 2017, Texas Instruments Incorporated All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * Neither the name of Texas Instruments Incorporated nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
LwIP v2.1.2	Copyright (c) 2001-2004 Swedish Institute of Computer Science. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Third Party Software	License Notice/Terms
	1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The license is available at: http://lwip.wikia.com/wiki/License

Third party software version numbers are shown for application firmware 2.00. Higher version numbers can be used in subsequent releases.

11 VERSION HISTORY

User Manual Version	Firmware version	Date	Author	Modifications
5A	5.xx	September 13, 2023	Kiril Mojsov	• Performed Legacy Updates
5	5.xx	April 10, 2023	Olek Bogush	• Added *Fast Connection* in Wi-Fi *Station* mode. Updated *Wi-Fi Configuration* subsection and other related parts of the user manual.
4	4.xx	March 15, 2023	Olek Bogush	• Updated *Converter Status LED* table. Added LED blinking in Wi-Fi Direct (P2P) mode each time a connection request is made.
3	3.xx	March 4, 2023	Olek Bogush	• Added DHCP Client and Server. Updated *Wi-Fi Port Parameters* in *Technical Specifications* section. Updated *Convertor Configuration* section. • Added PBC WPS in Wi-Fi Direct (P2P) modes to *Wi-Fi Port Parameters* in *Technical Specifications* section. • Added configuration parameters: *Enable DHCP Client in Wi-Fi "Station" Mode* and *Enable DHCP Server in Wi-Fi "Access Point" Mode*. For DHCP server added configuration parameters: *Max IP Address* and *Min IP Address*. • Updated *IP Network/CAN Settings*, *Wi-Fi Settings*, and *Home* webpages on the embedded web server. • Disabled changing of IP configuration parameters without the converter reboot. Updated *IP Network/CAN Settings* subsection. Removed *Website Automatic Relocation* figure. • Added *Device Type* configuration parameter in Wi-Fi Direct (P2P) modes. The default value is set to: FF-B437D100-00. • Added *Reset Network Processor to Factory Defaults* section. Updated *Connector* in *Technical Specifications* section, and *Wireless Connection* in *Convertor Configuration* section. Updated *Converter Status LED* table. • Updated *Converter Discovery* section. • Updated the title page with Canadian business address. Removed fax number from Finnish business address.
2B	2.xx	January 18, 2023	Olek Bogush	• Updated *Third Party Software License Notices*.
2A	2.xx	October 20, 2022	Olek Bogush	• Added warning and comments about "Worldwide" option of *Wi-Fi Country* configuration parameter. • Corrected *Wi-Fi Password* for WEP. Corrected the maximum length of *Wi-Fi Password* for WPA2. • Updated *Third Party Software License Notices*.
2	2.xx	August 31, 2022	Olek Bogush	• Added *Wi-Fi Direct* mode. Multiple sections updated.

User Manual Version	Firmware version	Date	Author	Modifications
1B	1.xx	Nov 15, 2021	Olek Bogush	• Added warning not to use special IP addresses for *Device IP Address* in *IP Network Configuration* subsection.
1A	1.xx	July 16, 2021	Olek Bogush	• Added unit weight.
1	1.xx	April 27, 2021	Olek Bogush	• Initial release

OUR PRODUCTS

AC/DC Power Supplies

Actuator Controls/Interfaces

Automotive Ethernet Interfaces

Battery Chargers

CAN Controls, Routers, Repeaters

CAN/WiFi, CAN/Bluetooth, Routers

Current/Voltage/PWM Converters

DC/DC Power Converters

Engine Temperature Scanners

Ethernet/CAN Converters, Gateways, Switches

Fan Drive Controllers

Gateways, CAN/Modbus, RS-232

Gyroscopes, Inclinometers

Hydraulic Valve Controllers

Inclinometers, Triaxial

I/O Controls

LVDT Signal Converters

Machine Controls

Modbus, RS-422, RS-485 Controls

Motor Controls, Inverters

Power Supplies, DC/DC, AC/DC

PWM Signal Converters/Isolators

Resolver Signal Conditioners

Service Tools

Signal Conditioners, Converters

Strain Gauge CAN Controls

Surge Suppressors

OUR COMPANY

Axiomatic provides electronic machine control components to the off-highway, commercial vehicle, electric vehicle, power generator set, material handling, renewable energy and industrial OEM markets. ***We innovate with engineered and off-the-shelf machine controls that add value for our customers.***

QUALITY DESIGN AND MANUFACTURING

We have an ISO9001:2015 registered design/manufacturing facility in Canada.

WARRANTY, APPLICATION APPROVALS/LIMITATIONS

Axiomatic Technologies Corporation reserves the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. Users should satisfy themselves that the product is suitable for use in the intended application. All our products carry a limited warranty against defects in material and workmanship. Please refer to our Warranty, Application Approvals/Limitations and Return Materials Process at https://www.axiomatic.com/service/.

COMPLIANCE

Product compliance details can be found in the product literature and/or on axiomatic.com. Any inquiries should be sent to sales@axiomatic.com.

SAFE USE

All products should be serviced by Axiomatic. Do not open the product and perform the service yourself.

This product can expose you to chemicals which are known in the State of California, USA to cause cancer and reproductive harm. For more information go to www.P65Warnings.ca.gov.

SERVICE

All products to be returned to Axiomatic require a Return Materials Authorization Number (RMA#) from sales@axiomatic.com. Please provide the following information when requesting an RMA number:

- Serial number, part number
- Runtime hours, description of problem
- Wiring set up diagram, application and other comments as needed

DISPOSAL

Axiomatic products are electronic waste. Please follow your local environmental waste and recycling laws, regulations and policies for safe disposal or recycling of electronic waste.

CONTACTS

Axiomatic Technologies Corporation
1445 Courtneypark Drive E.
Mississauga, ON
CANADA L5T 2E3
TEL: +1 905 602 9270
FAX: +1 905 602 9279
www.axiomatic.com
sales@axiomatic.com

Axiomatic Technologies Oy
Höytämöntie 6
33880 Lempäälä
FINLAND
TEL: +358 103 375 750
www.axiomatic.com
salesfinland@axiomatic.com