SECURITY GUIDELINE

Astraada One & CODESYS

1. PORTS

All ports represent a potential target for attackers. Always disable all unused or unnecessary ports!

1.1 Ethernet

The Ethernet interface is one of the main means of communication for logging into the device. This affects:
-Web interface (application & configuration)
-CODESYS programming interface
-SSH access
-FTP access

Please disable any access that is not required or not in use.
The network in which the controller is located must be separated from the company network.
Be sure to separate the network in which the controller is located from the company network using a firewall.
Deactivate unused ports in the firewall.
Segment the network to reduce accessibility.
Lock the control cabinet and prevent access to the network outside the control cabinet. Monitor the network for unknown participants.
Only allow access to the network in a secure area. Encrypt communication wherever possible.

1.2 EtherCAT

Reduce network accessibility as much as possible.
Lock the associated control cabinet. Access to the network only in the secure area

1.3 RS232/RS485

Minimize network accessibility as much as possible. Lock the associated control cabinet.
Encrypt communication where possible.
Please disable any access points that are not required or not in use.

1.4 CAN

Reduce network accessibility as much as possible. Lock the associated control cabinet.
Encrypt communication where possible.

1.5 USB

1.5.1 USB update

The USB update is a feature for all devices that allows you to completely configure a device, install firmware and application updates, and reinstall licenses using a script provided by Astor. From a security perspective, USB access must therefore be specially protected.
The individual tasks to be performed by the USB update are configured via an INI file. Possible settings In its default state, the INI file is configured so that all tasks are disabled.

Firmware – Ini Section [firmware]	
do_update	*Perform firmware update*
firmware_name	*Name of the firmware file*
Licenses – Ini Section [license]	
do_update_licenses	*Install licenses*
Web theme (logo) – Ini section [webtheme]	
do_update_webtheme	*Update web logo*
Splash screen (logo) – Ini Section [splashcreen]	
do_update_splashscreen	*Update splash screen logo*
System configuration – Ini section [sysconfig]	
do_sysconfig_from_file	*Perform system configuration* *replace_config_file_instead_of_merge* *Replace system configuration file on control instead of adding to it*
do_reset_syscfg_to_factory_defaults	*Reset system configuration*
do_reset_touch_calibration	*Reset touch calibration*
PLC application – Ini section [plcapp]	
do_update_plcapp	*Perform PLC application update*
plcapp_name	*Name of the PLC application file*
do_clean_plcfolder	*Empty PLC application folder*
do_clean_codesysretain	*Reset CODESYS retain data*
do_copy_plcdata	*Copy additional PLC data from USB to controller*
Fonts – Ini Section [fonts]	
do_update_fonts	*Perform font update*
do_clean_fontsfolder	*Empty fonts folder*
Update control – Ini Section [updatecontrol]	
check_skip_update_flag	*Check for update skip (set in control panel)*

Recommended settings:
Only use USB updates that you have obtained through official channels. Never offer your own USB update package for public download.
To avoid accidental updates, it is recommended to activate the Skip Update option in the control system using the library function CNF_SetSkipUsbUpdateFlag from the System Library.
It is recommended to operate all devices in a locked control cabinet to prevent unauthorized access to the USB interface.

1.5.2 USB update with reset button

The USB update can be disabled via a setting. In the event that the system has been misconfigured and it is no longer possible to establish a connection, a USB update can be enabled during the boot process by pressing the reset button simultaneously.

Therefore, the reset button of the controller must be protected against unauthorized access by installing it.

1.5.3 USB data/logging

When logging USB data, please note that the data could fall into the wrong hands. Please encrypt sensitive data and protect the USB port from unauthorized access. Avoid automatic logging when a USB stick is plugged in. Additional identification is recommended.

1.5.4 USB Ethernet

By using USB-to-Ethernet adapters, it is possible to establish an Ethernet connection via the USB interface.

1.6 USB SD card slot

It is recommended that all devices be operated in a locked control cabinet to prevent unauthorized access to the SD slot.

Caution:
Even if the SD card is deactivated, an SD card could still be used as a boot device.

2. INTERNET/REMOTE MAINTENANCE

2.1 OpenVPN

Each device comes with an OpenVPN client installed, which is disabled by default.

In order to activate this service, an additional license must be installed on the device. It is not possible to run the OpenVPN client and the IXON client at the same time.

With the OpenVPN client, it is possible to connect to your own OpenVPN server via a closed VPN channel. The configuration is done via an *.ovpn file and the associated certificate, which can be exported from the OpenVPN server. This makes it possible to connect to the device remotely and work with it as if it were on a local network. To use the OpenVPN functionality, the device must have a valid Internet connection.

Possible settings:

OpenVPN client startup	*disabled / enabled (default: disabled)*

VPN config file upload	*Search and upload function for loading the *ovpn file and certificate*
Activate new/changed configuration certificate	*Button for applying the uploaded *ovpn file and*
OpenVPN	*Ports 53, 443, 1194*

Recommended settings:

If the OpenVPN client is not used, leave the IXON client switched off.

If the OpenVPN client is required, it is recommended that the device only be operated behind an Internet access point with a firewall. Port 443 may require an exception rule that allows non-SSL traffic through SSL ports, as this is required for the VPN connection handshake before TLS encryption is used.

2.2 System Tooling

2.2.1 Service Screen

When in stop mode, each device displays a service screen that allows you to change various settings. Devices with integrated displays show the service screen directly, while devices without displays show the service screen either via the VNC server or via the display interface. The number of settings in the service screen and the individual options in the settings themselves may vary depending on the device. Controllers only allow you to change the network settings of the eth0 interface, while display panels can be configured entirely via the service screen.

Possible settings:

Network mode	*eth0 static/dhcp (default: static)*
IP eth0	*IP address (default: 169.254.255.xx)*
Netmask eth0	*IP mask (default: 255.255.255.0)*
Gateway eth0	*IP address (default: 0.0.0.0)*
DNS 1	*IP address (default: 0.0.0.0)*
DNS 2	*IP address (default: 0.0.0.0)*
Start as Mode	*E-terminal/Web terminal (default: E-terminal)*
Ntp server 1	*IP address (default: 0.0.0.0)*
Ntp Server 2	*IP address (default: 0.0.0.0)*
Ntp Server 3	*IP address (default: 0.0.0.0)*
Ntp Client State	*disabled/enabled (default: disabled)*
VNC server IP	*IP address (default: 192.168.3.1)*
VNC Scaling	*no scaling / keep aspect ratio / scale to screen (Default: no scaling)*
VNC Lifeguard	*Ping LG / VNC LG (Default: Ping LG)*
VNC Password	*Password (Default: empty)*
VNC Quality	*low / medium / high (Default: high)*
VNC Server Port	*Network Port (Default: 5900)*
Visu URL	*URL (Default: http://localhost:8080/webvisu.htm)*
Browser Mode	*Kiosk / Fullscreen (Default: Kiosk)*
Browser Pinch Zoom	*disabled / enabled (Default: enabled)*

Browser Onscreen KBD	*disabled / enabled (Default: disabled)*
Web server state	*disabled / enabled (Default: enabled)*
Modbus server status	*disabled / enabled (Default: disabled)*
SSH server status	*disabled / enabled (Default: enabled)*
Screen rotation	*0° / 90° / 180° / 270° (Default: 0°)*
Keyboard layout	*US / DE (Default: US)*
Keyboard autorepeat	*disabled / enabled (Default: enabled)*
Brightness	*0-9 (Default: 8)*

Recommended settings:

The individual settings in the service menu are always user-dependent and can vary greatly. Important settings are explained in detail in this manual.
For all devices, it is recommended to activate password protection for the service screen in the Config protection menu of the web interface or USB update in order to prevent unauthorized changes to the device.
It is also recommended to change all default passwords for all users in the Users menu of the web interface or via USB update.

2.2.2 FTP

Each device comes with an installed FTP server that is enabled by default.
The FTP server allows you to access the device's file system and upload or download files. Possible settings:

FTP server	*Disabled/enabled (default: enabled)*
Brute force detection	*Disabled/enabled (default: disabled) FTPS*
(FTP over TLS)	*On/off (default: off)*

The following users can access the FTP server:

Username	Start directory	Start directory change	Rights
root	/root	Yes	Read/Write
ftpuser	/flash/ftpupload	No	Read/Write (only ftpupload)
ftpadm	/flash/ftpupload	Yes	Read/Write (ftpupload only)
ftpreader	/flash/ftpupload	No	Read
ftp custom users	configurable	configurable	configurable (ftpreader/ftpuser/ftpadm)

The default password is the same for all users and can be found on the label of the respective device. The default passwords are randomly generated on each device and consist of eight characters with upper and lower case letters. Ports used:

FTP Port 21
FTPS Port 22

Recommended settings:

If the FTP server is not used, disable it in the FTP menu of the web interface or via USB update. If the FTP server is used, the following settings are recommended:
Change all default passwords for all users in the Users menu of the web interface or via USB update
Enable brute force detection in the FTP menu of the web interface or via USB update.
Enable FTPS in the FTP menu of the web interface or via USB update.

If the FTP server is used, it is recommended to use the device only within a closed network. In the case of online access, it is recommended to operate the device only behind an Internet access with a firewall and to use VPN if possible.

2.2.3 NTP

Each device comes with an NTP client installed, which is disabled by default.
When enabled, this checks the configured IP address for an NTP server during startup and synchronizes the system time. After the initial synchronization, the device updates the system time every 24 hours.
Some devices allow synchronization of the real-time clock (RTC).

Possible settings:

NTP client	*On/Off (Default: Off)*
Sync RTC	*On/Off (Default: Off)*
NTP server	*IP address (default: 0.0.0.0)*

Ports used:
NTP Port 123

Recommended settings:

If NTP time synchronization is not required, leave the NTP client switched off.
If NTP time synchronization is required, it is recommended to use a local NTP server within a closed network. In the case of an online NTP server, it is recommended to operate the device only behind an Internet access with a firewall and to use VPN if possible.
The NTP settings can be configured in the web interface or via USB update.

2.2.4 VNC

Every device without a display comes with an installed VNC server, which is disabled by default.
This VNC server allows you to remotely display and operate the target visualization of the device using a compatible VNC client.

Possible settings:

Server	*disabled / enabled (default: disabled)*
Resolution	*320x240 – 1920x1080 (default: 320x240)*
Color depth	*16/32 bit (default: 32 bit)*
Password	*Password as string (default: empty)*

Ports used:
VNC Port 5900
If no VNC display is required, leave the VNC server switched off.
If a VNC display is required, it is recommended to use a local VNC client within a closed network. In the case of a remote VNC client, it is recommended to operate the device only behind an Internet access with a firewall and to use VPN if possible.

Set a password for access to the VNC server in the VNC server menu of the web interface or via USB update. When a password is set, a connection is always checked.
The VNC settings can be configured in the web interface or via USB update.

2.2.5 Telnet/SSH

Each device comes with an installed SSH server that is enabled by default.
The SSH server allows you to log in to the device's Linux console and monitor and influence system processes. In addition to the SSH server, an SCP server service also runs. The SCP server allows you to access the device's file system and upload or download files.

Possible settings:

SSH server	*On/Off (Default: On)*
Brute Force Detection	*On/Off (Default: Off)*
Connection attempts	*3-10 (Default: 3)*
Lockout time (sec.)	*5-600 (default: 60)*

The following users can access the SSH and SCP servers:

Username	Start directory	Start directory change	Rights
root	/root	Yes	Read/Write

The default password for this user can be found on the label of the respective device.
The default passwords are randomly generated on each device and consist of eight characters with upper and lower case letters.
Ports used:
SSH/SCP Port 22

Recommended settings:
If the SSH server is not used, disable it in the SSH menu of the web interface or via USB update.

Change all default passwords for all users in the Users menu of the web interface or via USB update.
Enable brute force detection in the SSH menu of the web interface or via USB update.
Set connection attempts to three attempts in the SSH menu of the web interface or via USB update.
Set lockout time to 600 seconds in the SSH menu of the web interface or via USB update.

If the SSH server is used, it is recommended to use the device only within a closed network. In the case of online access, it is recommended to operate the device only behind an Internet access with a firewall and to use VPN if possible.

2.3 System logs

2.3.1 Web server / https:

Each device comes with a web server installed, which is enabled by default.
The connection to the web server is always encrypted (https) by default and works with certificates. All devices are equipped with a self-signed certificate by default, which must be manually trusted when first accessed on the web server.
This web server, also known as the web interface or web configuration, can be used to configure the device, install licenses, firmware, and software, and read out diagnostic information about the device.

The web server settings can be configured in the web interface. Possible settings:

Startup	*disabled / enabled (default: enabled)*
Redirect http->https	*enabled (default: enabled)*
Standard (http)	*Network port (default: port 80)*
Secure (HTTPS)	*Network port (default: port 443)*
Upload web logo	*Function that allows you to replace the logo displayed in the web configuration*
Create new certificate	*Function for creating a self-signed web certificate*
Create CSR	*Function for creating your own certificate request Download*
CSR	*Function for downloading your own certificate request Upload*
Certificate	*Function for uploading an officially signed certificate*

The following users can access the web server:

Username	Rights
root	Read/Write
admin	Read/Write

The default password for these users can be found on the label of the respective device.
The default passwords are randomly generated on each device and consist of eight characters with upper and lower case letters.

Ports used:

http	Port 80 in default
https	Port 443 by default

Recommended settings:
If the web server is not used, it is possible to switch it off, but this is not recommended as otherwise there are no diagnostic options. The setting for starting the web configuration can be changed in the web server settings menu of the web configuration itself or via USB update. If the web server is switched off, it can only be activated via USB update.

Change all default passwords for all users in the Users menu of the web configuration or via USB update
When using the web server, it is recommended that the device only be used within a closed network. In the case of online access, it is recommended that the device only be operated behind an Internet access point with a firewall and, if possible, that a VPN be used.
For maximum security, change the default port for accessing the web server and work with an officially signed web certificate.

2.3.2 Web browser / https:

Certain devices come with a web browser installed that is disabled by default.
Using the web browser, it is possible to display CODESYS WebVisu or other web-based visualizations either locally on the device or externally from other devices. The web browser supports encrypted (https) and unencrypted (http) connections.

The web browser settings can be configured in the web interface. Possible settings:

Destination URL	*URL (default: http://localhost:8080/webvisu.htm)*
URL connectivity check	*disabled / enabled (default: enabled)*
Browser decorated mode	*disabled / enabled (default: disabled)*
Browser remote debugging	*disabled / enabled (Default: disabled)*
Activate onscreen keyboard	*disabled / enabled (Default: disabled)*

Ports used:
http Port 80 by default
https Port 443 by default

Other connection ports can be specified via the URL

If the web browser is not used, it is recommended to leave it turned off. The setting for starting up the web browser can be changed in the web interface itself or via USB update using the Visualization type setting.
If the web browser is used, it is recommended to use the device only within a closed network. In the case of online access, it is recommended to operate the device only behind an Internet access with a firewall and to use VPN if possible.
For maximum security, only use encrypted connections (https) and work with the appropriate certificates.

2.3.3 Certificates

Certificates must always be used to connect to the web server or to display encrypted web pages via the web browser.
Certificates can be managed in the web interface in the respective submenus for web servers and web browsers.

Web server:

In the **Certificate (self-signed)** submenu, the device can create a self-signed certificate with other references. The self-created certificate can be downloaded and imported into an external browser that is to display the web interface. Alternatively, you can trust the certificate again the next time you call up the web interface.

In the Certificate (self-signed) submenu, the device can create a certificate request with other references. This request can be downloaded and signed by an external certification authority (CA). Once the externally signed certificate is available, it can be uploaded to the controller using the Upload button.

After restarting the device and calling up the web interface for the first time, the browser should automatically recognize and trust the externally signed certificate.

Each certificate process—whether self-signed or externally signed—must be performed individually for each device.

Web browser:

The **"Certificates"** submenu shows an overview of all installed certificates used by the internal web browser. This certificate submenu is **not** related to the certificates for the web server.

There are options to **delete selected certificates or the entire list**, as well as an **upload function** that can be used to load external certificates into the internal web browser.

After restarting the device, the web browser will accept the certificate and can load the encrypted website.

2.4 CODESYS programming tool

The following setting must be used in the module's configuration interface to reduce the integrity risk of the application due to unauthorized access via CODESYS:

CODESYS PLC Enforced User Management

Enables the forcing of the CODESYS User management. This means when connecting to the controller for the first time via CODESYS V3, the user must set a username and a password. This user management is independent from the CODESYS project used.

The Ethernet interfaces of the controller must be protected against unauthorized use.

Application recommendations

- Have user levels and password management everywhere by default
- Manage passwords and change them regularly
- No static superuser passwords
- Secure configuration
- Repeated incorrect entries lead to temporary deactivation of the device/account
- Logging of configuration changes
- Checking the logs during service
- Update/change important passwords - Limit validity period
- Only store necessary information on the device
- Store sensitive information in encrypted form
- Observe state of the art and check the security strategies applied in this regard
- Encrypt log entries
- Minimize attack surface