KENDRION

Software User Guide

Econo 328 / FIO Controller 328

Embedded Compact PC/PLC

E 869 EN 04.05.2026

PRECISION. SAFETY. MOTION.

Table of Contents

1 Foreword

1.1 Imprint

Contact Details

Kendrion Kuhnke Automation GmbH
Industrial Control Systems
Lütjenburger Straße 101
D-23714 Malente
Germany

Tel. Support	+49 4523 402-300
E-Mail-Support	controltechnology-ics@kendrion.com
Tel. Headquarters	+49 4523 402-0
Email Sales	sales-ics@kendrion.com
Internet	www.kendrion.com

1.1.1 Release Information

Manual history

Date	Comments / Changes
16.06.2022	Original version

1.2 About this guide

This software user book is intended primarily for designers, project engineers and device developers. It does not provide any information about delivery options. Changes, omissions and errors excepted. Illustrations similar.

This software user manual is a supplement to the respective user manual of the device, which describes the hardware, its installation and safe handling. The Software User Guide may only be used in conjunction with the relevant Device User Book.

1.2.1 Limitations of Liability

The data provided are for product description purposes only and are not to be understood as a guaranteed quality of the product in the legal sense. Quality agreements are reserved for the specific contractual relationship. Any claims for damages against us – regardless of the legal basis – are excluded, unless we are guilty of intent or gross negligence

1.2.2 Terms of delivery

The general terms and conditions of sale and performance of Kendrion Kuhnke Automation GmbH apply.

1.2.3 Urhebeschutz / Copyright

1.2.4 Licenses

Firmware

The firmware of the devices contains open source software.

A list of the packages used and the corresponding licenses can be found on the device in the web interface under the menu item Home/Packages and Licensens.

The source code of the free software can be requested from Kendrion Kuhnke Support Steuerungstechnik at cost price within three years of delivery of the device.

CODESYS

The installed CODESYS Runtime, like all CODESYS products, is subject to the terms of the End User License Agreement (EULA) of CODESYS GmbH, which can be viewed on the CODESYS website.

1.2.5 Warranty Policy

With regard to the warranty, reference is made to the provisions of the terms and conditions of sale of Kendrion Kuhnke Automation GmbH or, if available, to the existing contractual agreements.

1.3 Reliability, safety

1.3.1 Scope of application

This instruction manual contains information that you must observe for your personal safety and to avoid property damage when working with the Kendrion Kuhnke product.

1.3.2 Target group of the user manual

This user manual contains the necessary information for the intended use of the described product (control unit, control terminal, software, etc.). It is aimed at specialist personnel from design, project planning, service and commissioning. Comprehensive knowledge of automation technology is required for the correct understanding and error-free implementation of technical descriptions, operating information and, in particular, hazard and warning information.

1.3.3 Intended use

Kendrion Kuhnke products have been designed, developed and manufactured for ordinary industrial use. and may only be used for the applications provided for in the catalogue and in the associated technical documentation. The flawless and safe operation of the products requires proper transport, proper storage, installation, assembly, installation, commissioning, operation and maintenance. The permissible environmental conditions must be observed. Notes in the associated documentation must be observed.

1.3.4 Reliability

The reliability of Kendrion KUHNKE products is driven as high as possible through extensive and cost-effective measures in development and production.

These include:

- Selection of high-quality components,
- Quality agreements with our suppliers,
- Measures to prevent static charges when handling MOS circuits,
- Worst-case dimensioning of all circuits,
- Visual inspections at various stages of production,
- Computer-aided testing of all assemblies and their interaction in the circuit,
- Statistical evaluation of the production quality and all returned goods for the immediate initiation of corrective measures.

1.3.5 Hazard and warning information

Despite the fact that the 0 In accordance with the measures described, the occurrence of errors in electronic control systems must be expected, no matter how unlikely they may be.

Please pay special attention to the additional instructions that we have marked with symbols in this manual. Some of these hints draw attention to dangers, others serve more as orientation for the reader. In order of decreasing importance, they are described below.

The content in the hazard and warning information is structured as follows:

Type and source of danger

Possible consequences of non-compliance

⇨ Measures to prevent

	***DANGER***
	The notice with DANGER refers to an immediately dangerous situation which, if the notice is disregarded, will inevitably lead to a serious or fatal accident.

	***WARNING***
	The WARNING note refers to a potentially dangerous situation that failure to comply with the advice could lead to a serious or fatal accident or damage to this device or other devices.

	***CAUTION***
	The note CAUTION refers to a potentially dangerous situation that if the advice is disregarded, it may lead to an accident or may cause damage to this device or other equipment.

	***NOTE***
	This refers to a potentially dangerous situation that could lead to damage to this device or other devices if the advice is disregarded.

1.3.6 Other notes

	***Information***
	This mark draws attention to additional information concerning the use of the product described. It can also be a cross-reference to information found elsewhere (e.g. in other manuals).

1.3.7 Electrical safety

Our products usually become part of larger systems or plants. The following tips are intended to help integrate the product into the environment without danger to people and machines/systems.

	***DANGER***
	Disregard for the operating instructions
	Precautions to prevent dangerous errors can be overridden or additional sources of danger can be created.
	⇨ *Read the operating instructions carefully*
	⇨ *Pay special attention to hazard warnings*

	***Information***
	In order to achieve the highest level of conceptual safety when designing and installing an electronic control unit, it is essential to follow the instructions contained in the operating instructions exactly, as incorrect handling may override precautions to prevent dangerous errors or create additional sources of danger.

When planning a project , consider

- 24 V DC supply: Generated as a safely electrically isolated extra-low voltage. Transformers with separate windings that are designed in accordance with EN 60742 (in accordance with VDE 0551) are suitable, for example.
- In the event of power failures or dips: the program must be set up in such a way that a defined state is established during restart, which excludes dangerous conditions.
- Emergency stop devices must be implemented in accordance with EN 60204/IEC 204 (VDE 0113) and must be effective at all times.
- The safety and accident prevention regulations applicable to the specific incident must be observed.
- Please pay particular attention to the hazard warnings, which are intended to draw attention to possible sources of error at the appropriate point.
- In any case, the relevant standards and VDE regulations must be complied with.
- Install controls in such a way that unintentional actuation is excluded.
- Route control cables in such a way that there are no interferences (inductive or capacitive) that could affect the function of the control unit.

Observe during servicing or servicing

- When measuring and testing the control unit is switched on, the accident prevention regulation BGV A3 (Electrical systems and equipment must be observed), in particular §8 (Permissible deviations when working on parts).
- Spare parts: Use only those spare parts that are approved by Kendrion Kuhnke. Only Kendrion Kuhnke original modules may be used in the modular control units.
- For modular systems: Modules may only be plugged in or removed from the control system when there is no voltage. Otherwise, they can be destroyed or their function (possibly not immediately recognizable!) impaired.
- Batteries and accumulators, if available, should only be disposed of as hazardous waste.

1.3.8 IT Security

Kendrion Kuhnke products are designed to operate within closed industrial networks.

If the industrial networks are publicly accessible, e.g. through freely accessible network interfaces, or publicly accessible, e.g. through data connections via public data traffic (Internet), then the integrator and operator must take appropriate organisational and technical security measures to protect the internal network and ensure IT security.

	***Information***
	Information for the safe operation of plants, systems, machines and networks can be found in the information brochures of the BSI and IEC 62443, among others.

1.3.9 CODESYS Security

Automation devices contain functional units that are worth protecting. This includes classic control and regulation functions and algorithms, but also production data of the system users. Since no automation solution is error-free, there are potential, risky vulnerabilities.

A threat exists mainly via LAN networks, but attacks via local interfaces are also possible.

The following attack paths must be considered:

- Interfaces (USB, LAN, WLAN, Bluetooth, ...)
- Services, drivers, protocols (RPC, HTTP(S)...)
- Authentication, encryption (force login, encrypt PW)
- Physical access (locked rooms, cupboards)
- External systems, external employees

As much as possible, avoid exposing the PLC and control networks to open networks and the Internet. For protection, use additional layers of security such as a VPN for remote access and install firewall mechanisms. In principle, all unnecessary interfaces and services should be deactivated or access restricted. Effective protection of automation devices can also be carried out via segmentation, e.g. routers with firewalls.

	***NOTE***
	Third-party access to the computer
	Control failure and data loss
	⇨ When integrating into publicly accessible networks, the user must take appropriate measures to prevent unauthorized access.

	***NOTE***
	Please note the security information issued by CODESYS and continuously updated at: https://www.codesys.com/security

2 System Description

2.1 Overview

General device data			
Product name	FIO Controller 328 LAN	FIO Controller 328 CAN	Econo 328

			
Realtime OS	•	•	•
Integrated I/O	-	-	-
Dokker Functionality Integration	•	•	•
User and rights management	•	•	•
Firewall	•	•	•
FTP-Server	•	•	•
Realtime Clock NTP Client	•	•	•
CODESYS Features			
Automation Server Connectivity	•	•	-
Extensibility SL	•	•	-
CODESYS Key	•	•	-
Soft containers	•	•	-
Software License Containers	•	•	-
CODESYS Security			
Online user management	•	•	-
Encrypted communication	•	•	-
Encrypted application	•	•	-
Adaptation of the security policy	•	•	-

2.2 Realtime OS

Linux

Linux is one of the most powerful embedded operating systems of our time due to the high number of supported CPU architectures, the almost infinite number of drivers, and the good portability and scalability. Even systems with hard real-time requirements can be easily implemented with Linux.

Pros:

- Real-time capability
- Low storage space requirement
- Wide range of drivers
- Multi Core compatible
- Long-term availability

2.3 CODESYS

CODESYS is a software platform for many tasks in industrial automation technology. The basis is the IEC 61131-3 programming system. The tool offers the user integrated solutions for his work – with the aim of supporting him in the realisation of his task in a practical way.

All five of the languages specified by IEC 61131-3 (International Electrotechnical Commission) are available in CODESYS:

- IL (Instruction List)
- ST (Structured Text)
- LD (Ladder Diagram)
- FBD (Function Block Diagram)
- SFC (Sequential Function Chart)

In addition to the languages in the IEC standard, CODESYS offers:

- CFC (Continuous Function Chart) is a FUP (Function Plan) editor with a free-graphical layout: while FUP editors work in a network-oriented manner and arrange the building blocks automatically, in the CFC it is possible to place all building blocks freely and thus also to realize feedback without intermediate variables. This is why this language is particularly well suited for the overview display of an application.

2.4 CODESYS Control

The soft PLC runtime system CODESYS Control is already installed on the devices and matched to the existing hardware. This makes the devices an IEC 61131-3 compliant industrial controller. In addition, this runtime system includes important additional functionality so that the controller can communicate with other components in the automation environment.

2.4.1 Software Options

The devices are equipped with various software options, which can also be installed in combination on the devices. Please ask Control Technology Support for your desired combination.

Software Options		
Option	**Marking**	**Function**
CODESYS WebVisu	**WV**	Extension of a CODESYS controller for displaying visualization masks directly on the controller with output to the HDMI interface for monitors and displays. A control with the CODESYS WebVisu also allows the display of your masks created in CODESYS in any web browser, anywhere in the world.
CODESYS SoftMotion	**SM**	Single or multi-axis movements up to curve writing can be configured in the familiar IEC 61131-3 development interface - together with the logic application. A motion controller with CODESYS SoftMotion implements the motion functionality in the form of a modular system in the PLC programming system. Motion controllers with CODESYS SoftMotion enable the user to create extensive configuration variants for his movement tasks. Among other things, certified motion modules according to PLCopen and the full range of services of the IEC 61131-3 programming interface are available for this purpose.
CODESYS SoftMotion CNC+Robotics	**SM CNC***	3D CNC motion control for motion controllers with full 3D CNC or robotics functionality including interpolator and kinematic transformations. CODESYS SoftMotion CNC+Robotics enables the user to conveniently configure complex robot axis groups with an integrated editor. In it, he can select the desired kinematics, parameterize them and connect them to the physical robot axes. The robot function is processed using standardized function modules in accordance with PLCopen MotionControl Part 4.

* Please note that controllers with the SM CNS software variant are subject to approval for export from the EU (e.g. as spare parts) in accordance with point 2D002 of the dual-use list of goods Appendix 1 Cat. 2. Find out about the licensing procedure at the responsible office (Germany: Federal Office of Economics and Export Control). If the device is installed in a machine with the SM CNC software version, the machine classification automatically applies.

For more information, please visit the product pages of CODESYS GmbH: CODESYS Group

2.4.2 CODESYS Extension

With single-device licenses (CODESYS Store products with the ending "SL" for Single License), the range of functions of the device can be easily and flexibly adapted to the respective application. These are stored on the target device via the CODESYS Development System.

The license will be stored either in the integrated soft container of the controller or on CODESYS Key (USB stick).

The key is plugged into a free USB interface of the controller and allows the license to be used on other controllers by simply plugging it in.

The software license container on the controller offers several significant advantages. It allows it to be used without additional hardware, which not only reduces the installation effort but also avoids additional costs. Since no physical delivery is required, the process of license distribution is significantly accelerated and simplified. Finally, the license container also provides enhanced security by eliminating the risk of physical loss of the license.

2.4.3 Fieldbus Technology

Directly in the CODESYS programming system, the Fieldbuses CANopen (device variant), Modbus RTU, Modbus TCP and EtherCAT. In addition, some systemsProtocol Stacksavailable in the form of downloadable CODESYS libraries.

2.4.3.1 EtherCAT MainDevice

EtherCAT is a high-performance real-time Ethernet fieldbus system with an exposed protocol. Short cycle times, low jitter and different network topologies have made the system a standard in many industrial automation applications.

The EtherCAT MainDevice and the connected EtherCAT SubDevices can be conveniently configured by the CODESYS Development System.

The configuration of EtherCAT modules is based on the device description files for the MainDevices and SubDevices used and can be adjusted in the project in configuration dialogs.

Supported Features

Distributed Clocks

Different bus topologies

Bus diagnosis: in the configurator and through the PLC application

Network Scan: Detect and insert connected SubDevices

2.4.3.2 CANopen Manager

The CANopen configurator based on EDS or DCF files is fully integrated into the CODESYS Development System, so no external tool is required for configuring the bus system or the I/O data used.

The software offers an application interface according to CiA 405 for the diagnosis and use of SDO Extensive diagnostic functions.

2.4.3.3 Modbus TCP/RTU Client

The entire configuration of the CODESYS Modbus Client (TCP / RTU) is done directly in the CODESYS Development System.

The parameters for communication with Modbus RTU are specified in the configurator, e.g. the settings of the serial port such as baud rate or port number.

The parameters for communication with Modbus TCP, such as the settings of the Ethernet adapter or the port number, are specified in the TCP configurator.

In the configurator, so-called Modbus channels are defined. Behind a Modbus channel is a single Modbus command (read/write data) and the associated I/O channels. For which commands are supported, please refer to the documentation of the connected Modbus server.

2.4.3.4 Safety

With the installation as a package, CODESYS Safety is fully integrated into the PLC programming system. It covers all aspects such as programming, configuration of secure fieldbuses and secure library modules.

Kendrion offers a

2.4.4 Visualization

Directly in the CODESYS Development System, the user can use the integrated visualization editor to create complex visualization masks, link them to the application variables and animate them. Integrated visualization elements are available for this purpose. The generated masks can be used, for example, for application tests and during commissioning in the online operation of the programming system. With the optional visualization clients **CODESYS TargetVisu**, **CODESYS WebVisu** and **CODESYS HMI**, the created masks can also be used to operate the machine or system.

2.4.4.1 Visualization in the Development System

The integrated visualization in the development system is ideal for application tests, service or diagnostic purposes, as well as for commissioning a plant. As soon as you are connected to the controls, the visualization editor switches and animates the displayed elements. This variant is part of the free CODESYS Development System and can always be used regardless of the controller used.

2.4.4.2 CODESYS WebVisu (Option WV)

This variant means web-based representation of the user interface in a standard browser (PCs, tablets, smartphones). This enables remote access, remote monitoring, as well as service and diagnostics of a system via the Internet. A standard web browser communicates via JavaScript (optionally with SSL encryption) with the web server in the control system and displays the visualization using HTML5. This technology is supported on almost all browsers and is therefore also available on devices with iOS or Android.

Kendrion offers devices with the CODESYS WebVisu optionally for all control systems. In the type designation of the device, this function is marked with the abbreviation "WV".

2.4.4.3 CODESYS HMI

This variant is visualization or display on dedicated display devices (Vico). This enables access to the process data of several controllers via the same user interface.

The user interfaces created with CODESYS are displayed on a remote display device. This eliminates the computing load on the controller. Communication with the controller is done via the data source manager. This variant is ideal for operating and observing the machine on site, whereby the values of several controllers can also be displayed in one visualization. The display takes place on one or more control panels without control functionality and I/O control.

Kendrion offers devices with the CODESYS HMI functionality under the device designation "Vico HMI".

2.4.5 SoftMotion (version)

Single or multi-axis movements up to curve writing can be configured in the familiar IEC 61131-3 development interface together with the logic application.
Controllers with CODESYS SoftMotion enable the user to create extensive configuration variants for his movement tasks. Among other things, certified motion modules according to PLCopen and the full range of services of the IEC 61131-3 programming interface are available for this purpose.

- Function modules for single- and multi-axis movements
- Visualization templates for easy and fast commissioning

2.4.5.1 CODESYS SoftMotionLight

CODESYS SoftMotionLight is a functionally reduced motion solution for single-axis movements. It makes it possible to control a large number of axes with a small controller.

The control system and the fieldbus are relieved by shifting the movement execution to the axes. Only the status updates and movement commands are sent via the fieldbus. For the command and monitoring of the axes, the well-known PLCopen function modules for motion control (such as MC_Home, MC MoveAbsolute, MC_ReadStatus) are implemented. In addition, a simplifying functionality is provided.

For use with CODESYS SoftMotionLight, a drive must support EtherCAT or CAN fieldbus as well as various operating modes of the CiA 402. With the help of the *SML_CompatibilityCheck_DS402.project* project, it can be checked whether a drive is suitable for the use of the CODESYS SoftMotionLight.

2.4.5.2 CODESYS SoftMotion (Option SM)

Single or multi-axis movements up to curve writing can be configured in the familiar IEC 61131-3 development interface together with the logic application.
Controllers with CODESYS SoftMotion enable the user to create extensive configuration variants for his movement tasks. Among other things, certified motion modules according to PLCopen and the full range of services of the IEC 61131-3 programming interface are available for this purpose.

- Function modules for single- and multi-axis movements
- Visualization templates for easy and fast commissioning
- Integrated graphical cam editor with extensive configuration options

2.4.5.3 CODESYS SoftMotion CNC+Robotics (Option CNC)

Single or multi-axis movements up to curve writing can be configured in the familiar IEC 61131-3 development interface - together with the logic application. Kuhnke controllers with CODESYS SoftMotion enable the user to have extensive configuration options for his motion tasks. Among other things, certified motion modules according to PLCopen and the full range of services of the IEC 61131-3 programming interface are available for this purpose.

- Single- or multi-axis movements with PLCopen® Motion devices
- Multidimensional CNC control
- Multi-axis robot controllers with convenient project planning

2.4.6 OPC UA Server

Platform-independent standard access to variable data.

OPC UA (Unified Architecture) is a new development of the OPC specifications, which not only transports data from machines and systems, but also describes them semantically in a machine-readable way. Data exchange can take place independently of the manufacturer, making it one of the most important communication protocols for Industry 4.0 and the IoT.

The ES6 device family integrates the CODESYS OPC UA Server as a component of the runtime system. The powerful controller can transfer data from the controller to OPC UA clients, such as a visualization. The data to be published is defined in the symbol configuration. Data transmission can be secured and encrypted. A well-known OPC client can request the defined data.

2.5 Power Fail

"Powerfail" is a feature in CODESYS that allows the system to shut down properly in the event of a power failure or other unexpected loss of power.

The controller detects that the power supply has been interrupted for more than 10 ms and automatically stores all relevant data in the non-volatile memory and stops running CODESYS processes. The "Run / Stop" LED flashes 2 times if the undervoltage persists.

This functionality ensures that the system can be quickly and easily restored to its previous state once power is restored and control is started.

Overall, the Power Fail function in CODESYS helps to ensure the reliability and stability of industrial automation systems even in the event of unexpected power outages.

If other functions in the application have to be handled in the event of a power fail, such as writing large log files, stopping axes or sending the Powerfail signal to other participants, the automatic CODESYS function "Powerfail" can be deactivated by the system function "PowerFailToManual". In this case, only the "Powerfail" event is generated and all necessary steps for a proper shutdown must be handled in a function module to be created in CODESYS.

Supporting functions are collected in the System Library. → 4.3 CODESYS System Library

	NOTE
	Damage to the control system or machine
	Control failure and data loss
	⇨ The residual energy in the buffer capacitors and thus the functionality of the system is limited.
	⇨ Check the manual shutdown and thus the individual power fail solution extensively.

For more information on Power Fail, please contact Kendrion Kuhnke's control technology support.

3 System configuration

The Controller ES system can be configured via web interface or via USB stick.

3.1 Webinterface

3.1.0 IP address

The ControllerES6 device family has a fixed IP address and subnet mask when it comes out of the box.

IP- LAN1 Address (X6/X7): 192.168.0.228

Subnet Mask: 255.255.255.0

In order to connect to the device for the first time, you must be in the same IP address range as the device with your PC.

If necessary, change the IP address of your PC accordingly.

	***NOTE***
	Dual assignment of IP addresses
	Dual assignment of IP addresses can lead to severe disruption in a network.
	⇨ Make sure that there are no duplicate IP addresses on your network.
	⇨ For the first commissioning of the device, we recommend a direct network connection between the device and the programming PC with fixed IP addresses. You may need a cross-over network cable for this.

Clear assignment of the network address of the Ethernet interfaces.

If both network interfaces are given the same network address (net ID) and operate on the same subnet, there is no guarantee which of the two interfaces will be used for traffic. For secure operation, the network addresses (Net-ID) of the interfaces must be different. The network address (Net-ID) refers to computers and not to an Ethernet interface.

If the devices connected to the Ethernet interfaces have to work in a network, an external switch can be used for this purpose, or the switch function of LAN 1.1/1.2 or LAN 2.1/2.2 can be used

	***NOTE***
	Same network addresses (Net-ID) at the interfaces of a device
	If the network interfaces of a device are operated with the same network addresses, interference can occur.
	⇨ Make sure that the Ethernet interfaces of a device have different network addresses (Net-ID).

3.1.1 Webinterface

To access the web interface, start a web browser on your PC. Currently, the Microsoft Edge browser, Internet Explorer, Chrome and Firefox are supported.

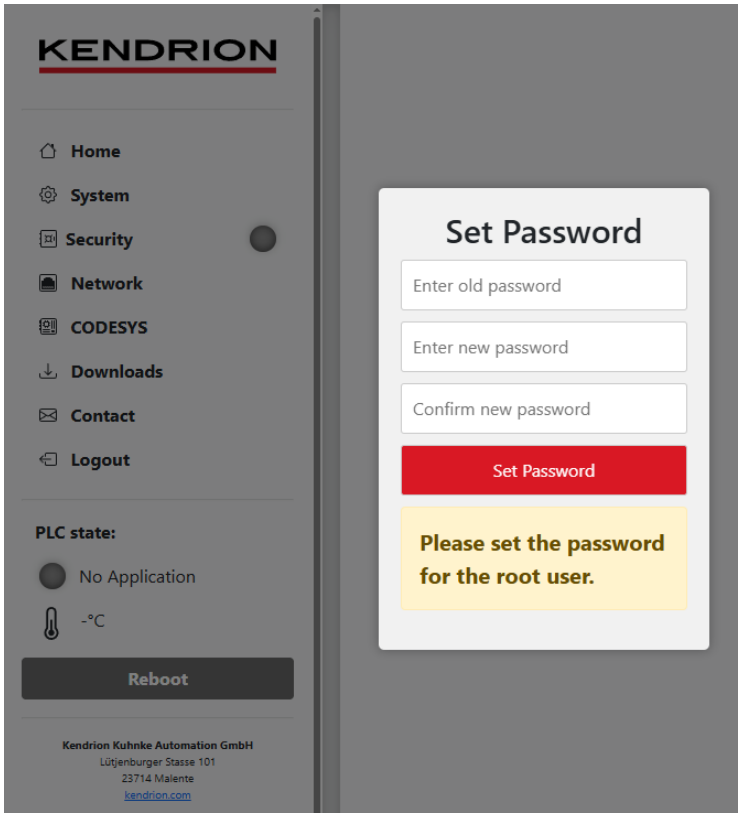
Enter the following IP address in the address bar of your web browser:

When connected via LAN1 (X6/X7)

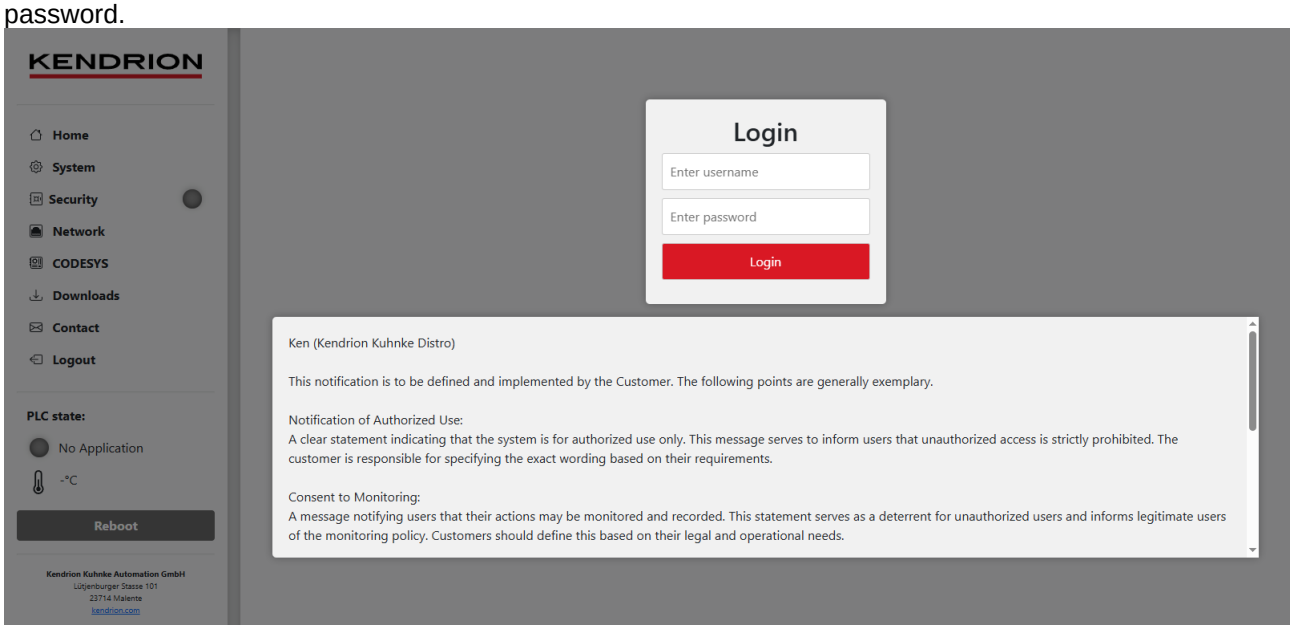
https://192.168.0.228

	Information
	The web interface is provided with a login. When the web interface is called up for the first time, a password must be assigned to the user "root". Enter the serial number of the device in the "Enter old password" field and a new individual password in the "Enter new password" and "Confirm new password" fields. Note the information for strong passwords.

	Information
	A strong password must meet the following requirements: • At least 8 characters in length • At least one digit (0–9) • At least one special character (for example: !, @, #, $, %, &) • At least one uppercase letter and one lowercase letter Don't use easily guessable information such as names, dates of birth, or simple strings of characters (e.g., "12345678" or "password").



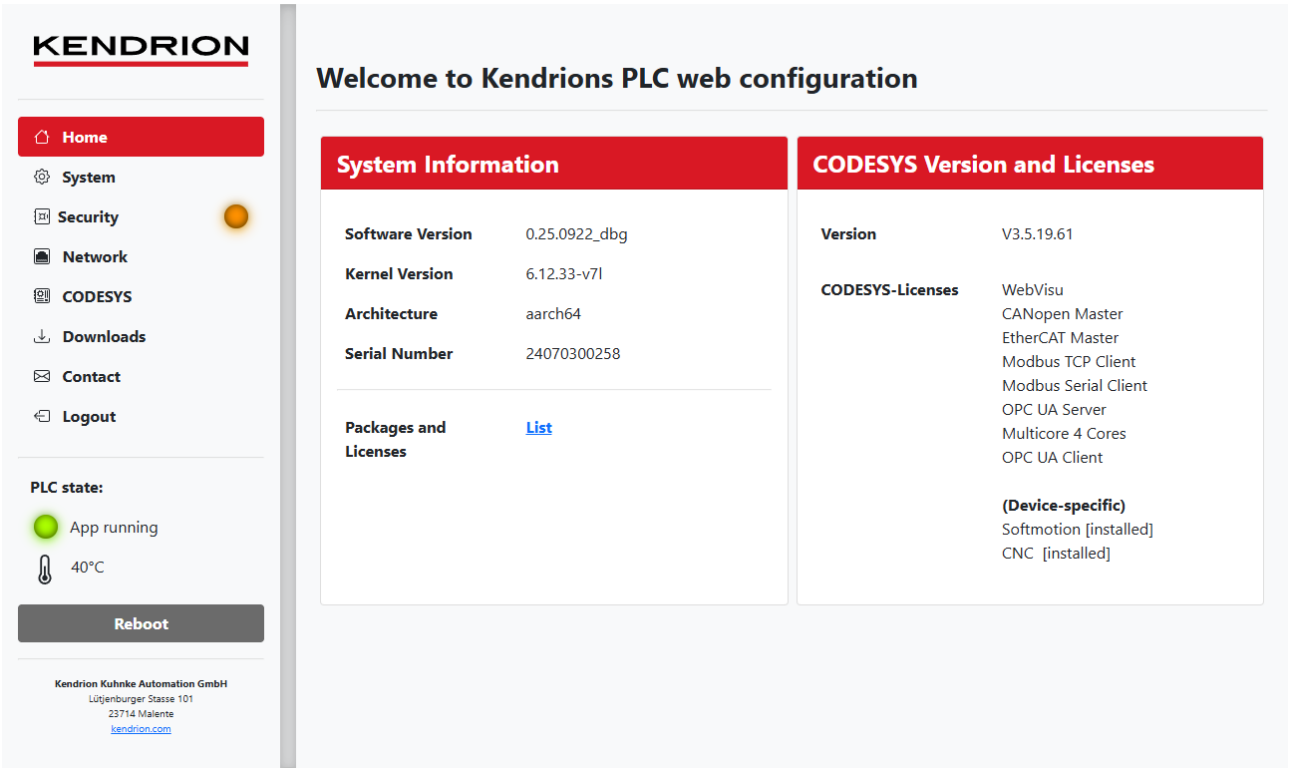
After the password has been changed, you will need to log in with the user "root" and the newly chosen password.



3.1.2 Webinterface - Home

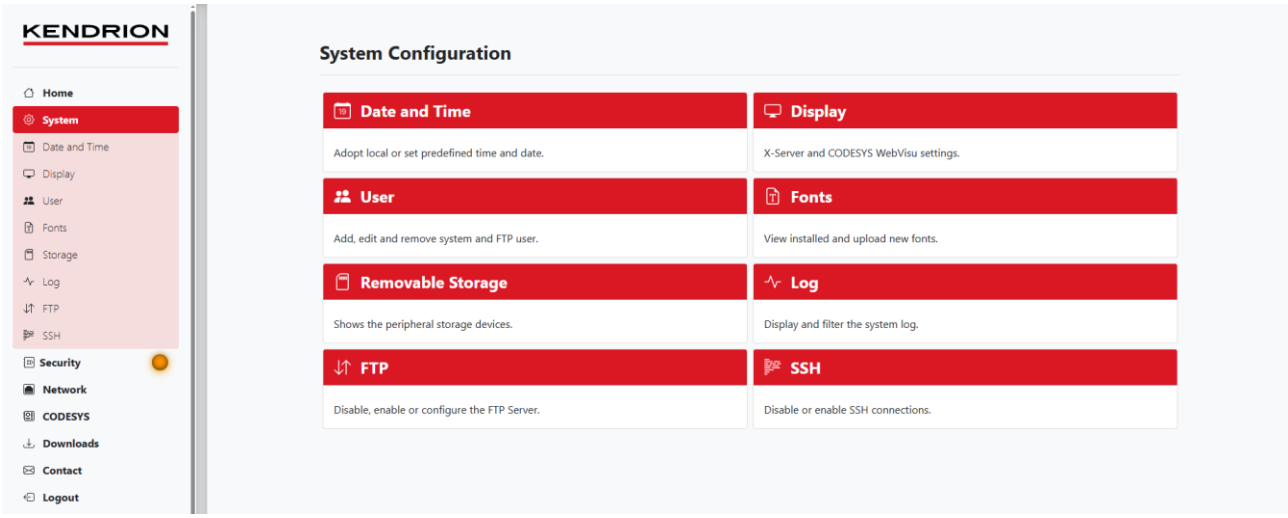
The home page displays general information about the device.

- System Information
  - Software versions installed on the device
  - Serial number of the device
  - Information about packages used and their licenses
- CODESYS Version and Licenses
  - Version der CODESYS Runtime
  - Interfaces and fieldbus support included in the standard
  - Additional licenses installed on the device



*Display in the web interface depending on the available options and web browser

3.1.3 Webinterface – System



System

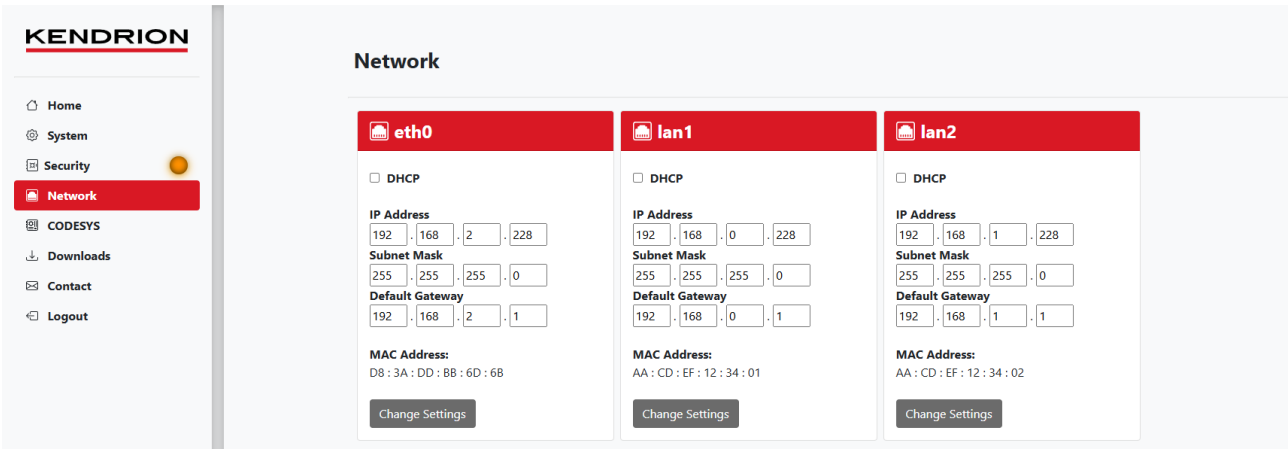
- SystemOverview of possible system settings
- Date and Time
  Apply local or predefined time and date, NTP server configuration
- DisplayX server and CODESYS WebVisu settings.
- Users
  Add, edit and remove system and FTP users.
- FontsView installed fonts and upload new fonts.
- Storage
  Information on internal storage and removable storage devices including their "mount points"
- LogView and filter the system log.
- FTPEACTIVATE, enable, or configure the FTP server.
- SSHDenable or enable SSH connections.

3.1.4 Webinterface – Security

Information and settings in the Security section

- Authentication
  The system usage notification is displayed every time you log on to inform users of system usage policies or other important information. This notification should be customized to meet the specific operational requirements and compliance needs of the system administrator or control operator.
- FirewallDisable, enable, or configure the firewall. Based on iptables.
- System integrity
  System integrity check using AIDE (Advanced Intrusion Detection Environment – Wikipedia)
  ToDo: Add a description?
- SSH

3.1.5 Webinterface – Network

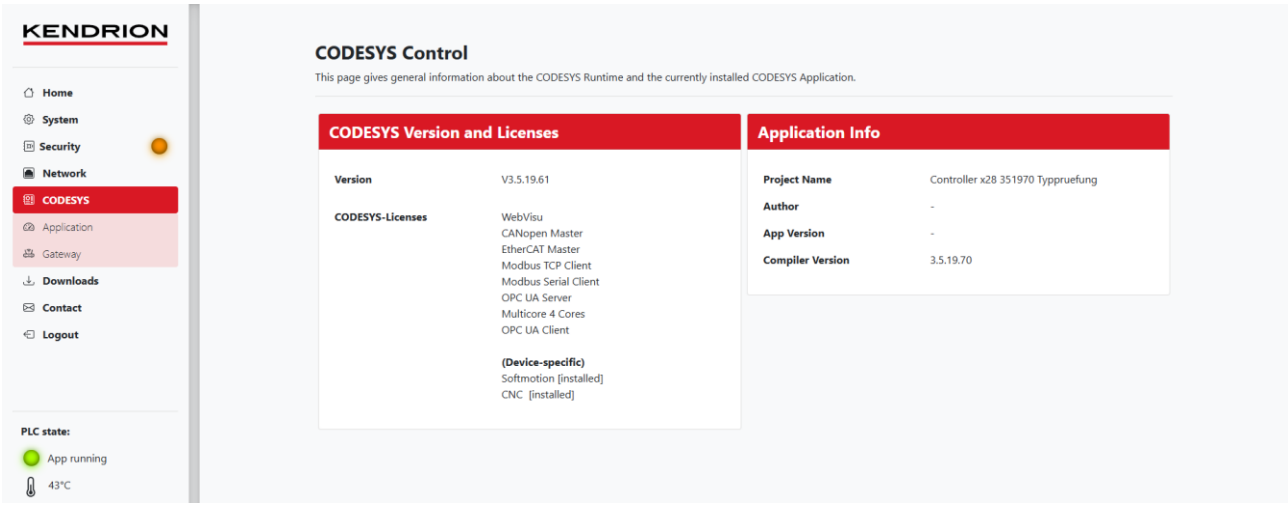


*Display in the web interface depends on the available options

Settings

- Network configuration of the available interfaces
- (WLAN (external WLAN stick)) ToDo: Clarification

3.1.6 Webinterface – CODESYS



Settings / Displays

- Integrated CODESYS licenses and versions
- Application -Information about the CODESYS application and options for downloading, uploading and removing the CODESYS application
- Gateway – Information and Settings for the CODESYS (Edge) Gateway

3.1.7 Webinterface – Downloads

Download des Controller CODESYS Package

The CODESYS package contains the following device descriptions and libraries necessary for the device:

- CODESYS Device Description des Controllers
- Device Description des Controllers
- Device Description KICS_ModbusComPort
- System Library

3.1.8 Webinterface – Contact

Contact Information

3.1.9 Webinterface – Logout

	Information (Logout)
	Log out of the device when you have completed your adjustments.

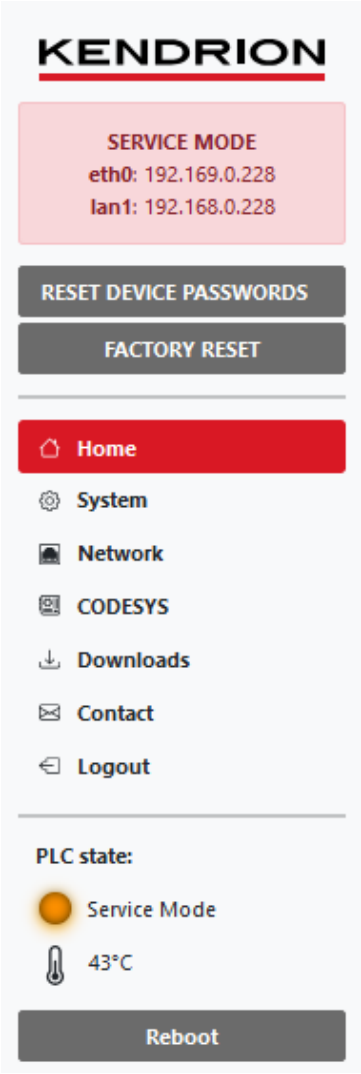
3.2 Webinterface – Service Mode

In Service Mode, the IP addresses can be read out in the web interface, the application can be deleted and the control system can be reset to the delivery state.

To start the web interface in Service Mode, follow the instructions 4.2 Service Mode (RESET Taste).

In Service Mode, the web interface can be reached with the default IP address of the device and the serial number as a password. Both information can be found on the nameplate.

The web interface starts in Service Mode with additional information and functions.



- Display of current IP addresses
- PLC Passwort Reset
-
- Factory Reset

- Reboot

3.3 CODESYS Soft Container

A CODESYS SoftContainer is a software-based licensing and security solution designed specifically for the CODESYS automation platform. The SoftContainer enables the management of software licenses for CODESYS modules and libraries and offers flexible handling as licenses can be easily activated, deactivated and managed.

A key feature of the SoftContainer is protection against unauthorized access and manipulation. Encryption and other security measures ensure the integrity of license and project data, which increases the security and reliability of the automation solutions.

In industrial automation, the SoftContainer offers a cost-efficient and flexible alternative to hardware dongles.

3.3.1 Single License Mechanism

With single-device licenses (CODESYS Store products with the ending "SL" for Single License), the range of functions of the device can be easily and flexibly adapted to the respective application. These are stored on the target device via the CODESYS Development System.

The Single License mechanism binds a license to a unique hardware ID to ensure exclusive use on the device.

Once purchased from the Store, the license goes through an activation process that uses a special code to unlock the licensed CODESYS functionality. This activation is device-specific, which means that the license usually cannot be easily transferred to other devices.

To manage and check the licenses, CODESYS provides the programmer with the license manager. The entire mechanism is designed to ensure a high level of security and prevent unauthorized access or duplication.

	NOTE
	Risk of License Loss!
	Immediate deactivation of rights-managed features
	⇨ Perform hardware changes only after consulting support ⇨ Caution with system updates Make sure that you are using the correct update file for your device with correct system configuration for an update.

3.4 USB Update Functions

You can use the USB update functions to load adapted system configurations, install the CODESYS boot application on the device or perform a complete system update. A template for the system configuration and the loading of a CODESYS boot application can be found on the Internet in our product finder.

	NOTE
	Incorrect or faulty update
	Control failure and data loss
	⇨ Make sure that you are using the correct update file for your device with correct system configuration for an update. ⇨ For a USB update, use a USB stick with SLC or pSLC technology in industrial design, a status LED in the USB stick simplifies the tracking of the update process.

3.4.1 Updating the system

A system update is provided as an archive file upon request. This is to be unzipped onto a USB stick. The update can also update the system configuration.

3.4.2 System Configuration Update

The system configuration update is configured in the sysconf file. This must be located in the root directory of the USB stick. Since the sysconf file is just a text file with special formatting, it can be edited with any text editor. The file contains sections [section] and keys, similar to the structure of a *.ini file. System configurations can also be carried out during operation. If a stick with the file "sysconf" is inserted, the running CODESYS application is terminated and the update is processed. The CODESYS application is then started again.

Section [users]

Add users by listing the desired users with corresponding passwords separated by spaces below the [users] section, e.g.

```
[users]
Username Password
```

Section [ts_conf]

Here you have the option of saving the touchscreen calibration, e.g. before performing a system update.

```
[ts_conf]
save
```

Should the previously saved touchscreen calibration be restored during a system update? Enter the following in the "sysconf":

```
[ts_conf]
load
```

The key "calibrate_on_plugin" causes the touchscreen calibration to start when the USB stick is inserted.

```
[ts_conf]
calibrate_on_plugin
```

Section [autocopy]

With the help of the [autocopy] section, files can be copied to the device. Knowledge of the directory structure on the controller is essential. There must be a "root" directory on the USB stick, in which the directory structure and the files that are to be copied to the device are located. Example:

```
[autocopy]
/usr/bin/codesys
## !! DO NOT REMOVE "list_end" !! ##
list_end
```

Copies all files and subdirectories from <USB>:\root\usr\bin\codesys to the device in /usr/bin/codesys.

Section [ip_conf]

Changes the setting of the available Ethernet interfaces. The key below the [ip-conf] section is structured as follows:

<Name> <IP-Address>/<NetMask Bit kodiert> <Optional: Gateway IP-Address>

Example

```
[ip_conf]
eth0 192.168.0.215/24 192.168.0.1
eth1 192.168.0.216/24 192.168.0.1
WLAN0 192.169.0.1/24
```

Section [codesys_control]

This section contains control commands for external control of the CODESYS Runtime. Activate only one key at a time in this section

- stop: leaves the CODESYS boot application in the stop state during and after plugging in the USB stick
- disable: turns off the codesyscontrol service
- enable: activates the codesyscontrol service
- deny_start: prevents a boot application from starting
- enable_start: (re)enables the start of a boot application
- remove_app: deletes the current boot application
- deploy_app: provides a plclogic.tar as an app (plclogic.tar can be created via the web server)
- enable_webvisu:
- disable_webvisu:
- enable_codesysedge:
- disable_codessedhe:

```
[codesys_control]
#stop
#disable
#enable
#deny_start
#enable_start
#remove_app
#deploy_app
#enable_webvisu
#enable_codesysedge
```

Section [log]

Copies the log files dmesg and /var/log/messages to the storage medium to ./log/

```
[log]
copy_logs
```

Section [vsftpd_control]

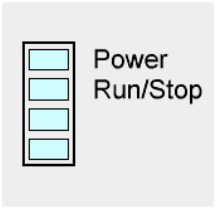
Enables or disables the vsftpd FTP service

```
[vsftpd_control]
#enable_vsftpd
#disable_vsftpd
```

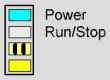
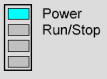
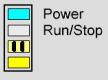
3.4.3 Baseline Installation Status Message

The progress of the initial firmware display (baseline) is signaled by the LEDs.

LEDs:



LED Meaning

Step	LED	Significance
1		Submarine
2		uboot ♦☐ Linux
3		(Flash code 1 Hz) USB/SD working
4		reboot
5		Submarine
6		Uboot –Linux
7		(Flash code 1 Hz) USB / SD working
8		(Flash code 1 Hz) Update done

4 System Features

4.1 Operating System Features

4.1.0 SSH Connection

SSH refers to a network protocol that allows you to establish an encrypted network connection with the device in a secure way.

On Windows, an SSH client is required (e.g. Putty).

The SSH connection is deactivated in the delivery state of the device.

To log in via SSH, the following information is required:

Server Address:	<IP address>, delivered 192.168.0.228
Username:	root
Password:	-
Port	22

4.1.1 Autostart

If further programs are to be started on the system, this is configured by configuring the background program "systemd". Configuration requires experience. Our control technology support will be happy to support you.

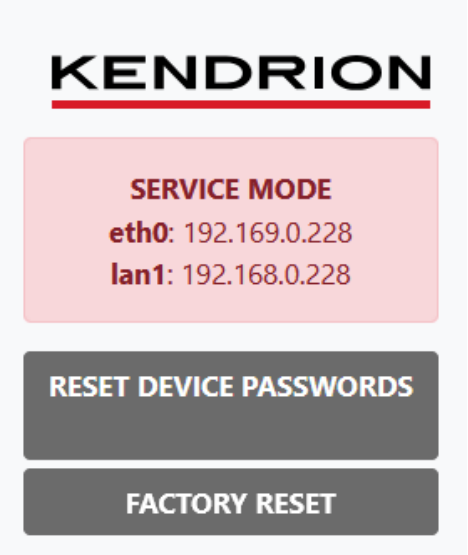
4.1.2 Kernel Update Tool

If a kernel / operating system update is necessary, please contact the support control technology at Kendrion Kuhnke.

4.2 Service Mode

Service Mode differs from normal operating mode in the following ways:

- The CODESYS V3 Runtime is not running, so no control programs are running. The factory settings are loaded during the network configuration, so that each controller can be addressed via a clearly defined IP address. For information about this network configuration, see → 3.1 Webinterface
- To enter Service Mode, the device must be switched off.
- Then the S/R button is held down and the device is switched on again.
- The button must be held down until the Run/Stop LED and the LED underneath light up yellow (approx. 5s).
- Service Mode is ready when the Run/Stop LED lights up yellow.
- The lettering "Service Mode" appears in the web interface



4.3 CODESYS System Library

Hardware-specific functions of the device are to be used with the "KICS Controller ES6 System Library" library in COSYS. The library must be integrated into the project via the library manager.

In the library administrator, short documentation is stored for all usable function blocks and functions. For more information, please contact Kendrion Kuhnke's Control Technology Support.

FUNCTION PowerFailToManual

Changes the PowerFail mode of the PLC to manual. In this case, the PLC only sends the PowerFail event and does not suspend the application or save the retains. Saving the retains must be done using the SaveRetains function.

Input parameters: BOOL

TRUE for manual PowerFail,

FALSE for automatic PowerFail.

Return Value: BOOL

PowerFailToManual

Successful: TRUE, Failed: FALSE

FUNCTION SaveRetains

Function to save the retains and exit the application

Return Value: BOOL

Successful: TRUE, Failed: FALSE

FUNCTION SysGetMountableDevices

Reads the disk/destination. The returned device names can be used to shut down a specific device (SysUnmountDevice)

Return Value: STRING

Array of strings with the currently mounted devices

FUNCTION SysGetSerialNumber

Query the serial number of the system

Return value: STRING

Serial number of the device

FUNCTION SysGetTemperature

CPU Temperature Query

Return Value: INT

Temperature [°C]

FUNCTION SysGetVersion

Query the controller version of the system

Return Value: STRING

Controller-Version

FUNCTION SysReboot

Restart the control system

Return Value: Reset Control

FUNCTION SysSetEthAddr

Setting the Ethernet interface

The gateway can be omitted by setting the leading GW byte to zero.
Possible interfaces are eth0, eth1 and wlan0

Input parameters: STRING + 3 x array

Ethernet name, IP Address, Subnet Mask, Gateway

Return Value: BOOL

TRUE

FUNCTION SysStartTouchCalibration

Starts touch calibration

Input parameters

Return Value: BOOL

Successful: TRUE, Failed: FALSE

FUNCTION SysUmountDevice

Turn off a device

Input parameters: STRING

Name of the device

Return Value: BOOL

Successful: TRUE, Failed: FALSE

5 CODESYS DEVELOPMENT SYSTEM

5.1 CODESYS installation on the project planning PC

	NOTE
	For development, use only the CODESYS version that matches the released runtime version of the controller. The version is stored on the device housing and in the web interface.

CODESYS is a device-independent control programming system. In accordance with the IEC 61131-3 standard, it supports all standard IEC programming languages, but also allows the integration of C routines and supports object-oriented programming.

Together with the CODESYS Control runtime system, it allows "multi-device" and "multi-application" programming. The component-based structure makes customer-specific configuration and extension of the user interface possible.

Before installing CODESYS, please refer to the following system requirements information.

System Requirements

Operating System

Windows 8 / 10 / 11 (64 bit operating system)

The versions maintained by Microsoft are supported.

Recommended System Features

2.5 GHz processor

8 GB RAM

12 GB of free hard disk space

Additional requirements

Microsoft Internet Explorer 11, or later

Note

No license is required

Please note the license agreement with the CODESYS Group

The development environment can be downloaded in different versions from the CODESYS Store.

5.2 Prepare CODESYS

5.2.1 Installing the Device Description in the CODESYS Development System

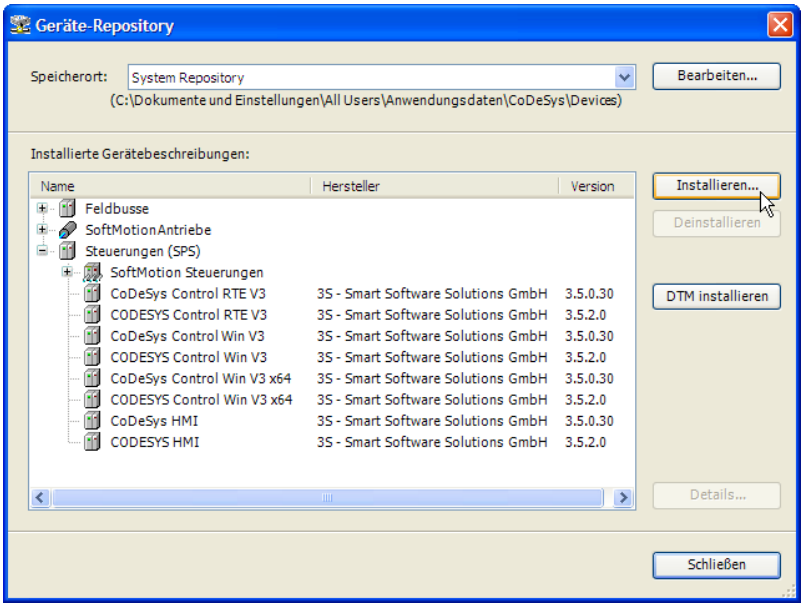
In order to be able to operate a device, the IEC 61131-3 development tool, the runtime system must be made known to the CODESYS Development System of this device.

The functions for managing device definitions on the local system and in projects are provided by the 'Device Repository' plug-in. Among other things, it provides commands of the command category 'Devices', which can be found by default in the 'Tools' menu.

- Open the 'Device Repository...' in the 'Tools' menu
- The Device Repository dialog is launched
- Expand the tree labeled 'Controllers (PLC)'

The device repository is the database of device descriptions that are installed on the local system to be available for programming in COSYS. Installing and uninstalling the devices is done in the device repository itself.

In the 'Installed Device Descriptions' window, the devices that have already been installed are displayed with the "name", "manufacturer" and "version" of the device. The "branches" can be opened/closed with the help of the plus and minus signs.



Install Device Description

Use the "Install..." button: to reinstall a device on the local system so that it becomes available in the programming system.

The 'Install Device Description' dialog will open, where you can search the system for the corresponding device description file. For the standard devices, the file type filter is set to "*.**devdesc.xml**" (Device Description). But also manufacturer-specific description files, such as "*gsd" files for Profibus DP modules, *.eds and dcf files for CAN devices can be selected.

As soon as the selection is confirmed with "OK", the dialog closes and the new device is inserted in the 'Device Repository' dialog in the device tree. Errors during installation (e.g. missing files referenced by the device description) are displayed in the lower part of the device repository dialog.

Device Description

For all variants of the Scout or Econos with the iMX6 processor system, the device description "ContollerES6" is used. This can be downloaded from the device, as well as the device description for the optionally integrated 4DI/4DO in the web configurator in the "Download" menu.

Device version	Device Id	Device Name
Econo XX6 Scout XXX6	64	ControllerES6
Optional internal 4DI/4DO	1064	ControllerES6IO

Install Device Description

Use the "Install..." button to reinstall a device on the local system so that it becomes available in the programming system.

The 'Install Device Description' dialog will open, where you can search the system for the corresponding device description file. For the standard devices, the file type filter is set to "*.**devdesc.xml**" (Device Description). But also manufacturer-specific description files, such as "*gsd" files for Profibus DP modules, *.eds and dcf files for CAN devices can be selected.

As soon as the selection is confirmed with "OK", the dialog closes and the new device is inserted in the 'Device Repository' dialog in the device tree. Errors during installation (e.g. missing files referenced by the device description) are displayed in the lower part of the device repository dialog.

Device Description Download

The appropriate device description is stored on the device and can be loaded via the Web Configuration menu item "Downloads".

To do this, switch to the Download tab in the web configuration and select the "Download DevDescr" button.

5.2.2 Special features of the device description

There is only one device description for the ControllerES6 platform. It is therefore no longer necessary to distinguish between standard and soft-motion devices or between single- and multi-core. This reduces the software maintenance effort. However, depending on the use, certain settings must be made.

Activate Softmotion

To use CODESYS Softmotion, select "Activate SoftMotion" from the "Project" menu.

The command causes the SoftMotion General Axis Pool device to be added below the control configuration, if the object is still missing. There is a maximum of one SoftMotion General Axis Pool per PLC device. In addition, the SoftMotion libraries (prefixed with SM3_) are added to the library manager.

If your device is disabled for SoftMotion and you add any SoftMotion object under the device, the Enable SoftMotion command is implicitly executed immediately. A SoftMotion object is a cam object, a CNC object, an axis group object, or any SoftMotion axis.

Single Core

For single-core processor-based controllers, task groups cannot be assigned to specific processor cores. By default, the device description creates the task group "IEC Tasks" with the core setting "FixedPinned". No further settings are to be made.

Multi Core

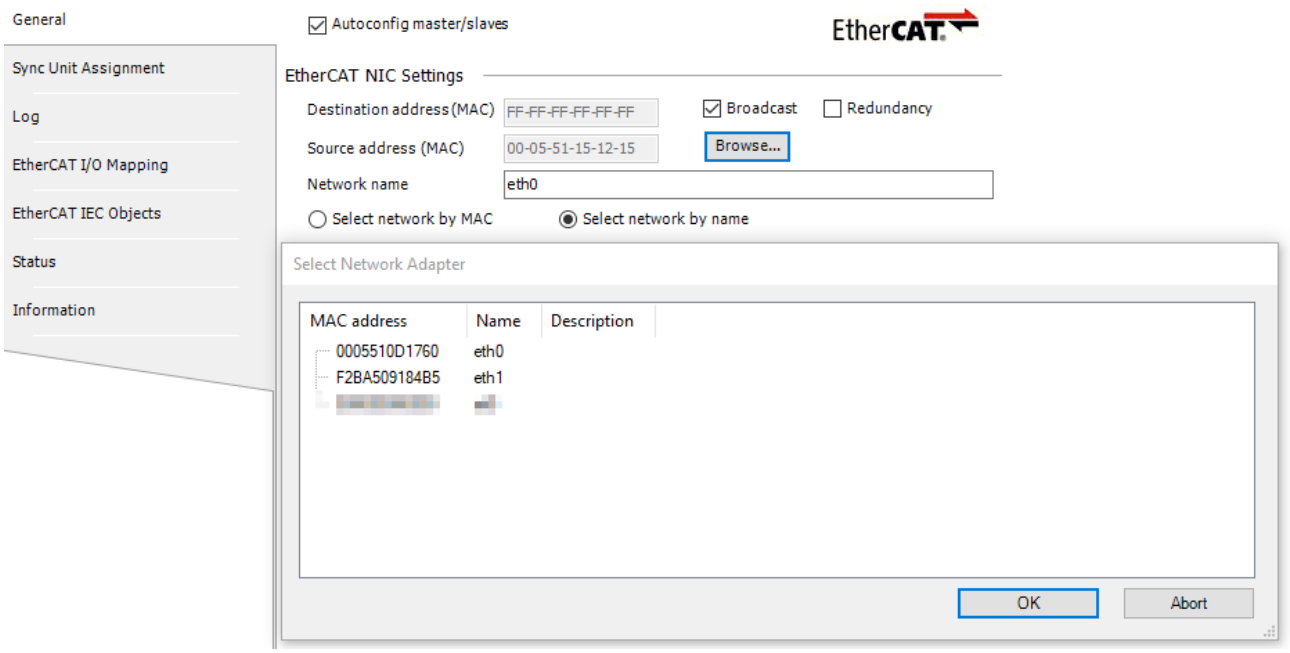
In the case of controllers with multi-core processors and multi-core soft PLC, it is possible to assign task groups to specific processor cores.

The following "core" settings are possible:

- FreeFloating: All tasks are dynamically bound to different processor cores - the user cannot influence them, the assignment is done by the operating system.
- SequentialPinned: All tasks are firmly bound to different processor cores - the user cannot influence them.
- FixedPinned: All tasks are bound to a processor core. Which processor core this is is decided in the runtime system (default setting).
- <Core Number>: Firmly defined processor core. If the processor core is not present, an error message is displayed.

5.2.3 Physical interfaces

EtherCAT



CAN bus

In Device Construction, add the "CAN-Bus" device below the controller. Under "Network", set the assigned CAN bus interface.

Assignment of the CAN bus interfaces:

CAN 1 (X8): Network 0

CAN 2 (X7): Network 1

Serial interfaces (RS232, RS485)

The serial ports are mapped to the COM ports as follows:

RS485 (X7): COM Port 1

RS232 (X8): COM Port 2

When using Modbus RTU via the RS485 interfaces, add the device "KICS Modbus COM" below the controller in the device tree. In the settings, select "1" for the COM port.

	Information
	Always use the device "KICS Modbus COM" for Modbus RTU, as this sets device-specific settings (RTS_CONTROL = TOGGLE) correctly.

Internal IO (4DI / 4DO)

The internal IO module does not require any configuration. It is automatically hooked into the device tree.

6 Security

Due to the increasing networking of control systems and systems, the threat potential is also increasing rapidly! Therefore, take a close look at the possible security measures!

Security measures are absolutely necessary to protect data and communication channels from unauthorized access.

6.1 Security features of CODESYS

CODESYS offers various security functions for the development system, the communication from the development system to the PLC, the application and for the use of the WebVisu.

6.2 Security for communication with the PLC

You should protect communication with the controller connected to the CODESYS project against unwanted access by the following means:

- Activation of user management: simple or group-based
- Certificate-based encryption of communication with the controller

	***Information***
	As of V3.5 SP17, user management is mandatory for the SL runtime systems. For earlier versions, see below under "Enforcing user management".

6.2.1 Activation of security features

First, switch communication to encryption so that no access data is disclosed to other participants in the network when transferring user management.

Enforcing encrypted communication

- On the controls:
  - LZS version >= 3.5 SP14: Encryption *can be enabled as a communication policy* and enforced for all clients
  - LZS version < 3.5 SP14: The controller can communicate encrypted or unencrypted! No encryption enforced.

    See the current help:

    Encrypt communication, change security settings
- In CODESYS:
  - Encrypted communication is selectable as an option in the Device Editor, *Communication* tab (Command or *Change Communication Policy* dialog), or in the *Security Screen view*

    See the current help:

    Encrypt communication, change security settings

    If the CODESYS Security Agent is installed, you will see the CODESYS Security Agent Help Center

Enforce user management

- On the controls:
  - LZS version >= 3.5 SP17: User *management is enforced by default* as a communication policy

    Note: To activate user management, at least a development system CODESYS V3.5 SP16 is required. This means that if you have forced user management that hasn't been enabled yet, you won't be able to connect to an older development system.
  - LZS version >= 3.5 SP14 < 3.5 SP17: User *management can be explicitly activated and enforced as a* communication policy
  - LZS version < 3.5 SP14: Simple user management or one for users/groups with their rights can be enabled
- In CODESYS:
  - See the current help:

    Encrypt communication, change security settings

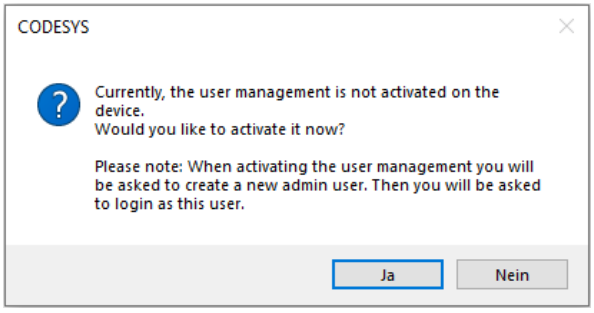
    Handle Device User Management

6.2.2 Establishing a connection with the PLC

In order to minimize the risk of data breaches, the CODESYS device user management is activated and FTP and SSH are deactivated in the delivery state of the Kendrion devices from 09/2023.

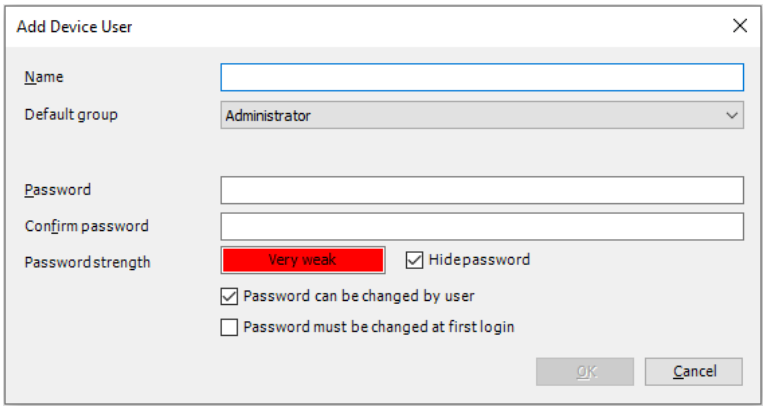
When connecting to a new device for the first time, you will be prompted to create a device user with a new user password.

	Information
	Further information on user management can be found online in the CODESYS Online Help: ***CODESYS Online Help***

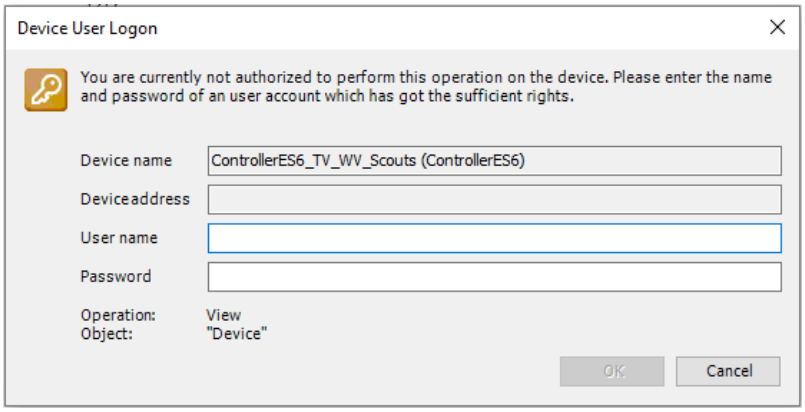


Define the name and password for the user. Initially, only the Administrator group is available. The password strength is displayed.

Also note the options set regarding a password change. By default, the password can be changed by the user at any time. Confirm with OK.



The selected data is then requested every time you log in with the device.



Disable Device User Management

	NOTE
	After disabling user management, your control is accessible to everyone in the control network. For this reason, user management should only be deactivated in justified exceptional cases.

- If the device user management security policy is set to Enforced, first set it back to Optional.
- Select the Reset Origin Device command. This deletes the user management and allows you to reconnect to the controller without entering user credentials.

6.3 Encrypt communication in the application

Note

Recommendations for data security

- To minimize the risk of data breaches, we recommend the following organizational and technical measures for the system running your applications:
- As much as possible, avoid exposing the PLC and control networks to open networks and the Internet. Use additional layers of security for protection, such as a VPN for remote access.
- Install firewall mechanisms.
- Restrict access to authorized people.
- Use high-strength passwords.
- Change any existing default passwords when you first use them and regularly thereafter.

- Use the security functionalities supported by CODESYS and the relevant control device, such as encryption of communication with the control device and targeted restriction of user access.

CODESYS offers the user a variety of security settings and tools, which are described in the online help of the development system.

	Information
	CODESYS Online Help for the CODESYS Development System: Overview (helpme-codesys.com) ***Encrypt communication, change security settings:*** CODESYS Online Help

6.4 Security for CODESYS WebVisu

Protect the connection between the controller's web server and the visualization client from unwanted access by doing the following:

- Configure an HTTPS connection (encryption with SSL/TSL) between the visualization client and the web server
- Restrict access to visualization and configure visualization user management

	Information
	CODESYS Online Help for CODESYS: CODESYS Online Help ***Configure encrypted connection:*** CODESYS Online Help

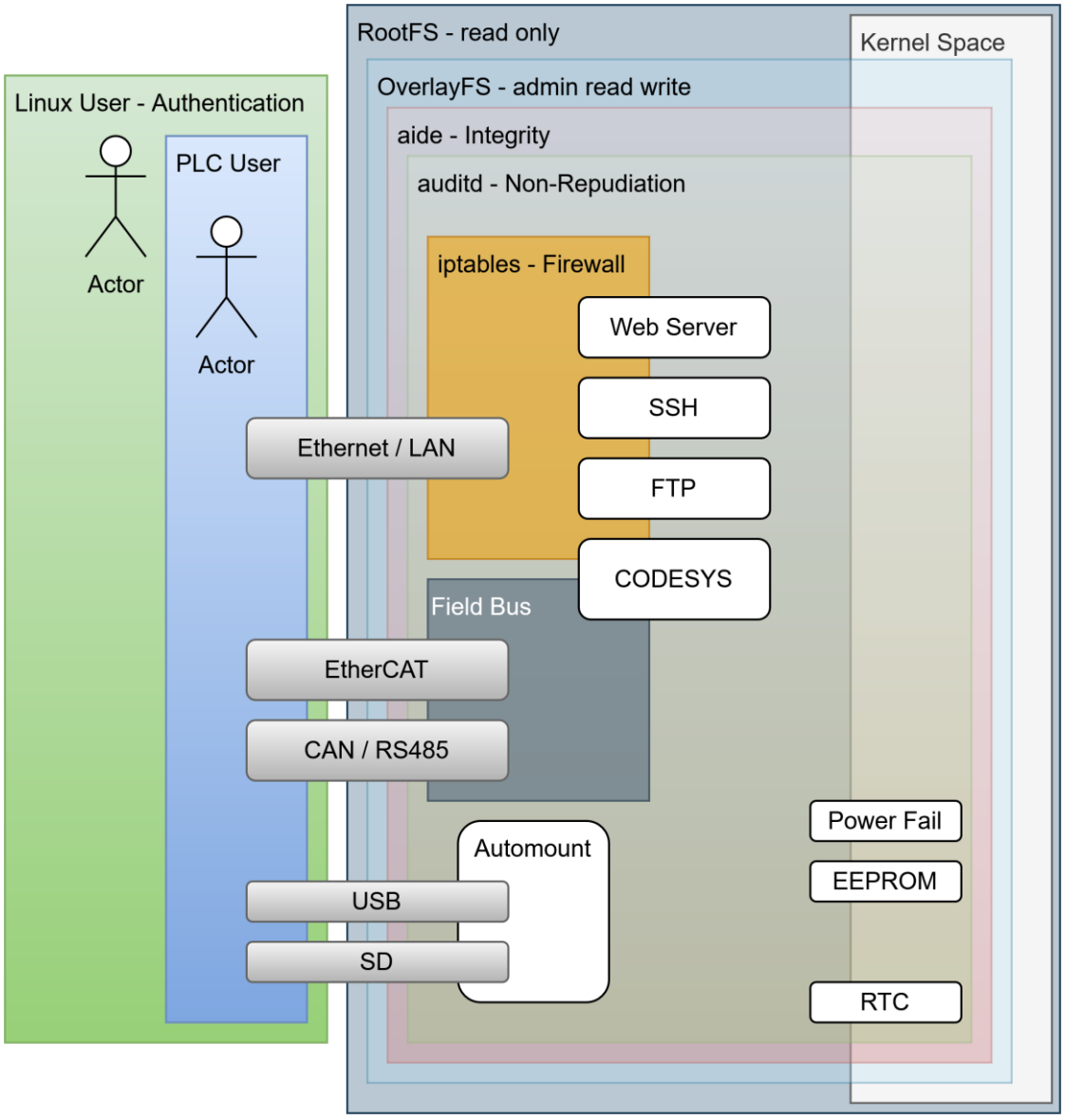
6.5 CRA and IEC 62443 Cybersecurity Notice

For more information on the requirements and measures in the field of cybersecurity, especially in connection with the Cyber Resilience Act (CRA) and the international series of standards IEC 62443, we recommend reading the *Kendrion Security Whitepaper*. The document provides a comprehensive overview of legal requirements, technical standards, risk assessments, and strategies for vulnerability management and security level implementation. It serves as a supplementary source of information for the safe use and integration of our products. The white paper is available at www.kendrion.com.

6.6 File System Structure

The structured organization of files and directories plays a central role in the clarity, traceability and security of the use of digital systems. The file system structure enables the user to quickly find relevant information and identify security-critical components in a targeted manner. It forms the basis for consistent data storage throughout the entire product life cycle – from development to operation and maintenance.

In the following, you will find detailed information on the specific design of the file system structure and its logical structure.



6.7 System overview and functionality

The integrated Linux system is based on a robust OverlayFS architecture. As an end user, you benefit from a particularly secure system: The read-only root file system (RootFS) protects the basic installation from accidental changes, while you can still make all the necessary configurations in the writable OverlayFS layer.

The architecture is divided into color-coded layers , which are shown in the attached diagram: The outer white layer represents the kernel space with hardware-related components. The light blue layer indicates the main file system (OverlayFS), within which the writable admin layer is located. The orange layer includes the system services and applications behind the firewall. The dark gray layer shows the fieldbus area with industrial communication protocols. This structure means that even in the event of misconfigurations, you can easily reset the system.

6.7.1 Access options and user roles

As an end user, you have different access options depending on your role: As a standard Linux user (shown in green), you can perform general system operations, while as a specialized PLC user, you can also program and configure industrial automation tasks. There are several ways to access it: You can work via standard network connections (Ethernet/LAN), integrate external storage devices via USB/SD interfaces, or use specialized communication protocols such as EtherCAT and CAN/RS485 for fieldbus applications in industrial applications. These user and network components are shown in the **blue (PLC user) and green (Linux user) layers** , which form the top abstraction layer of the system and give you direct access to the system.

6.7.2 Available applications and services

The system provides you with various applications that you can use as needed: You can configure and monitor the system conveniently via your browser via the integrated web server. For advanced system management, SSH is available. You can use the FTP service to transfer files, programs, and configuration files.

CODESYS is particularly important for industrial applications, with which you can develop, test and transfer PLC programs to the system. These services are secured by the Linux firewall system (iptables) and can be configured depending on your user role and network policies. The **orange layer** visually highlights these application containers and shows their central role in your daily work.

6.7.3 Security features and monitoring

The system provides you with various security and monitoring features: The auditd daemon automatically logs all system-critical events, so you can understand what happened in your system when needed - especially important for compliance requirements and error analysis.

The Advanced Intrusion Detection Environment (AIDE) system continuously performs integrity checks and alerts you to unauthorized changes. Both security components – auditd and AIDE – are integrated into the writable OverlayFS layer and are shown accordingly in the diagram.

In addition, the hardware-related components in the kernel space ensure reliability: Critical configuration data is backed up in the non-volatile memory areas EEPROM and nvRAM. A real-time clock (RTC) ensures correct time tracking even without a network connection. Power fail management ensures that the system is safely shut down in the event of a power failure without losing data.

6.7.4 Maintenance and administration

As an end user, you benefit from the system's user-friendly maintenance structure: the OverlayFS architecture allows you to perform secure updates without fear of damaging the system. All your configuration changes are stored in the writable overlay layer, while the base installation (factory default) remains protected. If you ever have a problem, you can simply revert the system to its original configuration.

The automount function, shown in the **brown hardware interface layer**, works automatically for you: USB sticks and SD cards are automatically detected and mounted, so you can easily transfer files. For industrial applications, you can use various communication interfaces to flexibly integrate the system into existing networks.

KENDRION

PRECISION. SAFETY. MOTION.

Kendrion Kuhnke Automation GmbH
Industrial Control Systems

Lütjenburger Str. 101
23714 Malente

Phone: +49 4523 402 0
Fax: +49 4523 402 201

sales-ics@kendrion.com
www.kendrion.com