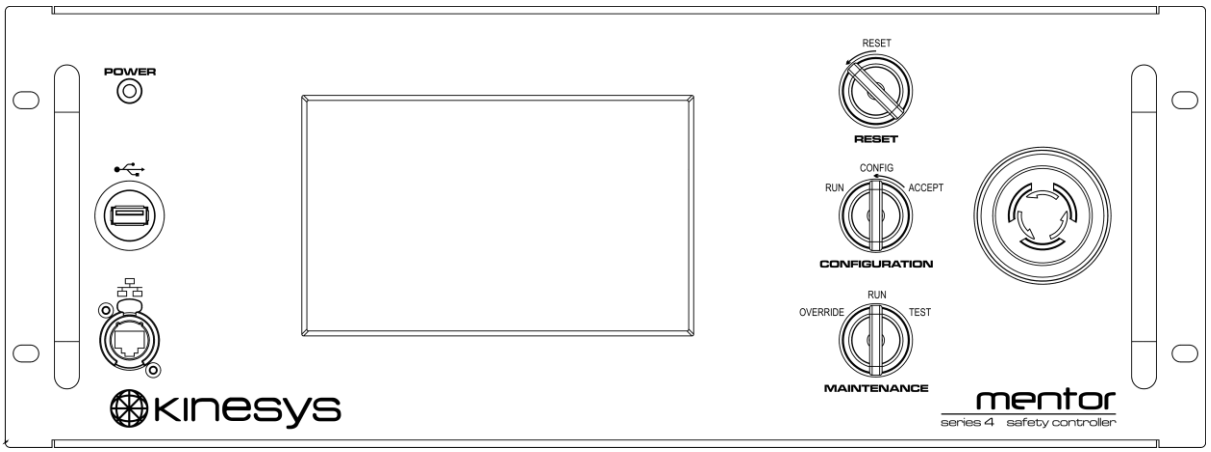
USER GUIDE

MENTOR Model 401
Model 402

Advanced Safety Controller



LIMITATION OF LIABILITY

Kinesys Projects Limited accepts no liability for any consequences resulting from inappropriate, negligent or incorrect installation or use of the equipment.

The contents of this manual are believed to be correct at the time of printing. In a commitment to a policy of continuous development and improvement, Kinesys reserves the right to change the specification of the product, its performance, or the contents of this manual, without notice.

All rights reserved. No parts of this manual may be reproduced or transmitted in any form or by any means, electrical or mechanical including photocopying, recording or by an information storage or retrieval system, without permission in writing from Kinesys Projects Limited.

© Kinesys Projects Limited

MANUFACTURER CONTACT DETAILS

Kinesys Projects Ltd

Unit 2 Kempton Gate Business Centre

Oldfield Road

HAMPTON

Middlesex

TW12 2AF

United Kingdom

Contact Information:

For general enquiries Monday to Friday, 9am to 6pm

Tel +44 (0)20 8481 9850

Fax +44 (0)20 8487 0396

info@kinesys.co.uk

www.kinesys.co.uk

For technical support Monday to Friday, 9am to 6pm

Tel: +44 (0) 20 8481 9850

Fax +44 (0)20 8487 0396
support@kinesys.co.uk

Table of Contents

1 Scope and Purpose

The purpose of this manual is to describe the features, functions and means of operating the Kinesys Mentor 401 safety controller.

This manual refers to features introduced in software version 22. Earlier software versions may not include all of the features described in this document.

2 Introduction

The Mentor 401 is an advanced safety controller allowing the connection of emergency stop switches, enabling switches and other safety devices to a system of Kinesys motion controllers.

Mentor 401 uses PROFIsafe over PROFINET safety communications to permit easy distribution of safety and motion control data using standard Ethernet cabling and data distribution, and to allow safe group halt actions based on axis load or position in addition to device status.

When used with Kinesys safety input devices and suitable output devices, the emergency stop system and dead man's handle system complies with requirements up to PLe (EN 13849) or SIL3 (EN 62061).

2.1 General Description & Safety Warnings

The equipment described in this manual may only be operated by personnel qualified to do so for the specific task as detailed above.
Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with this and associated equipment.

The Mentor 401 is designed for indoor use only.

2.1.1 Safety Advice

- Carry out a full risk assessment for your particular application
- Only allow competent personnel to install and operate the system
- Do not connect or disconnect cables while the system is powered on. Always switch off before making or breaking connections.
- Test all safety devices on a regular basis, and following each new installation of a temporary system
- Safely store shorting plugs and keys to prevent inadvertent or deliberate misuse.
- Do not write down configuration passwords in the vicinity of the equipment.
- Never use equipment, cables or connectors when damaged or wet
- Never operate machinery without having a clear view of the load or reliable communication with an observer
- If an unexpected move presents a potentially hazardous situation, use the emergency stop button to bring all motion to an immediate stop
- An emergency stop system reset may render a previously "dead" circuit live – always disconnect circuits before carrying out any maintenance
- If you are unsure of any aspect of system connection or operation stop and seek advice on the appropriate usage of the system

2.2 Transportation and storage

2.2.1 Condensation

The Mentor 401 is designed for indoor use only. If the product has been exposed to temperature fluctuations, for example during transport, there may be risk of condensation which may result in damage. Do not connect the Mentor 401 to a power source immediately. Leave the Mentor 401 disconnected until the unit has reached the temperature of the location where it is to be installed.

2.2.2 Shocks

Do not shake, knock or drop the Mentor 401. Avoid excessive force when installing and operating the product.

2.2.3 Handling

Never lift the Mentor 401 by any of its cables or connectors as this may cause damage to the unit and/or the cable.

2.2.4 Packaging

The use of a purpose made shock absorbing rack-mount flight case (available from Kinesys as an accessory) is recommended for regular transportation such as in touring applications. Otherwise, where possible, please use the original packaging to transport the Mentor 401.

3 Overview

This section describes the layout of the front panel controls and the rear panel connections on a Mentor 401

3.1 Front Panel

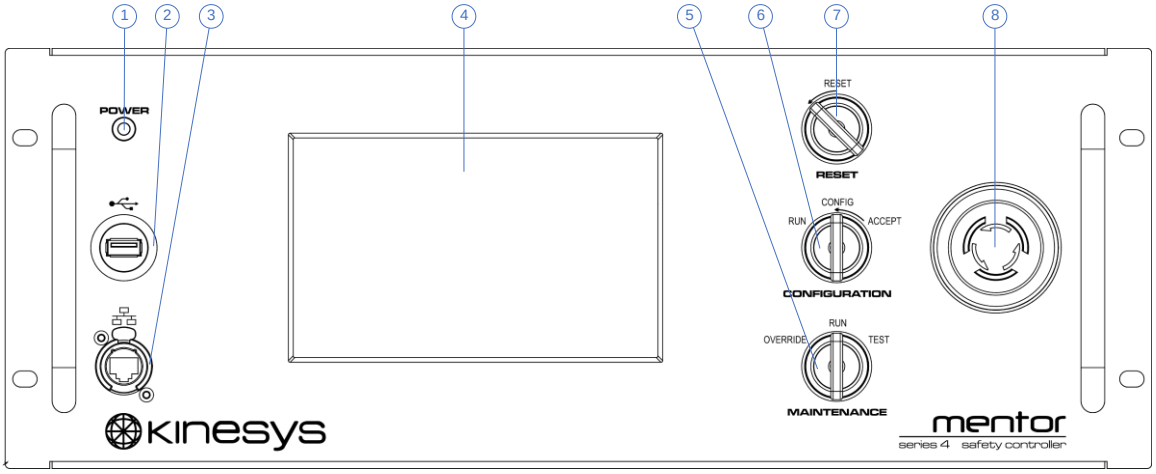


Figure 1 Front panel layout

1. **Power Indicator**
   illuminates blue when the Mentor 401 is connected to the mains supply and turned on
2. **USB Port**
   used for connecting a mouse and keyboard if required, or to allow connection of a storage device for program updates and configuration storage
3. **Ethernet Port**
   connection to the internal Ethernet switch – Ethernet motion control and PROFIsafe data
4. **Touchscreen Display**
   shows system status and allows configuration of the Mentor 401 operation
5. **Maintenance Keyswitch**
   allows safety functions to be overridden for diagnostic and rescue purposes, and permits functions of connected drives (for example, brakes and loadcells) to be tested.
6. **Configuration Keyswitch**
   switches between the RUN and CONFIGURATION modes of the Mentor 401
7. **Reset Keyswitch**
   allows various error conditions to be reset and acknowledges changes to the connected equipment
8. **Emergency Stop Switch**
   initiates an emergency stop on all connected devices

3.2 Rear Panel

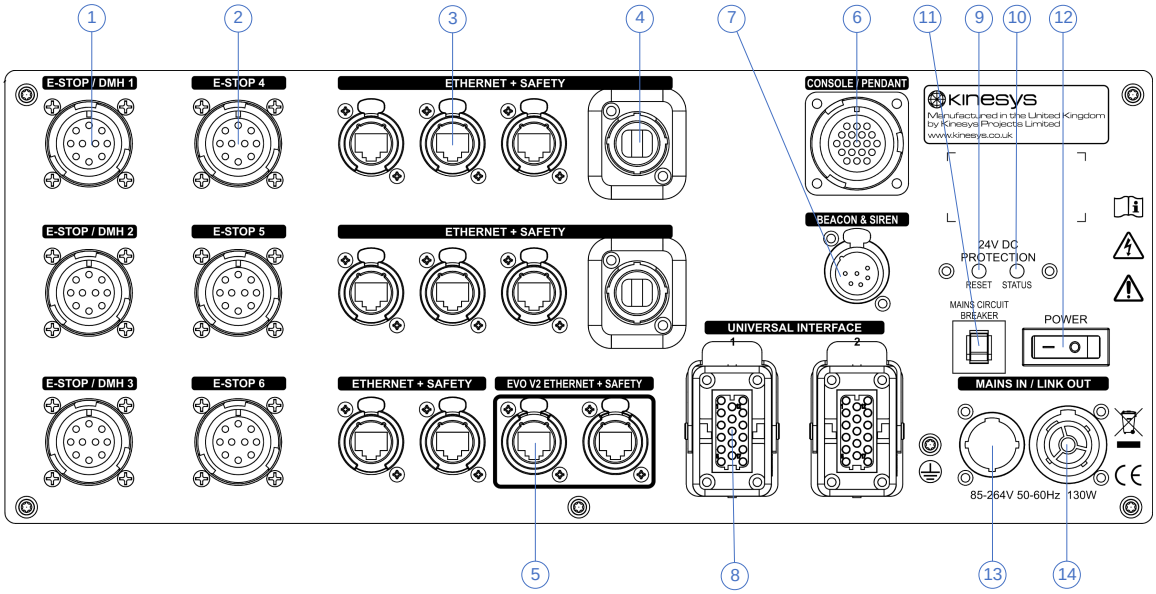


Figure 2 Rear panel layout

1. **Emergency stop & enabling Switch Inputs**
   Connections for emergency stop switches with enabling buttons (dead man's handles). Shorting plugs must be fitted to unused emergency stop inputs.

2. **Emergency stop switch inputs**
   Connections for emergency stop switches only. Shorting plugs must be fitted to unused emergency stop inputs.

3. **Ethernet & Safety Outputs**
   Connections for Ethernet devices, including devices using PROFIsafe such as apexDRIVE.

4. **Ethernet & Safety Outputs (Optional Fibre Optic Connection)**
   Connections for Ethernet devices, including devices using PROFIsafe such as apexDRIVE. Optionally configured at manufacture with 100MB or 1GB copper or fibre optic connectors.

   Mentor M401: 2 x 10/100 MB copper connection (etherCON)
   Mentor M402: 2 x 1000 MB multimode fibre connection (opticalCON QUAD)

5. **EVO V2 Ethernet & Safety Outputs**
   Connection for ethernet devices requiring an EVO V2 safety system interconnection.

6. **Console Power & Data Connection**
   24V power supply, safety signalling and data connection for a console or remote pendant

7. **Beacon & Siren Output**

8. **Universal Device Interface Connections**
   Connection to legacy Kinesys devices or third-party automation or safety systems

9. **24V DC Power Supply Reset Button**
   Resets the electronic circuit protection for the 24V power supply. See page 48 for details.

10. **24V DC Power Supply Status Indicator**
    Shows the status of the electronic circuit protection for the 24V power supply:
    OFF: supply fault
    GREEN: supply OK
    YELLOW: at least one supply is loaded to 80% capacity

11. **Mains Input Circuit Breaker**

12. **Power Switch**

13. **Mains Input Connector**

14. **Mains Link Out Connector**

4 Installation

Although it may be used freestanding, the Mentor 401 is designed to be installed in a standard 19” rack.

4.1 Installation precautions

When considering the location to install the Mentor 401, make sure the device will not be exposed to extremes of heat/cold, moisture, humidity or dust. Refer to the environmental requirements in the summary product specification on page 55.

When rack mounting, ensure there is enough space within the rack to allow for cables and connections at the rear and the switches and controls at the front.

Ensure there is adequate ventilation when using the Mentor 401 installed in a rack.

4.2 Rack Mounting

Mentor may be mounted in a standard 19” equipment rack or flightcase. A shock-mounted flightcase is recommended for touring use.

It is recommended that the Mentor enclosure is supported at the rear to prevent stress on the front panel and rack structure caused by the weight of the unit and the cables connected to the rear panel.

Mentor may be supported while also allowing easy service access using Accuride 3307 type telescopic rack slides.

4.3 Cooling

Mentor does not require any clear space above or below the rack case, but avoid mounting in proximity to other equipment which may generate heat.

Mentor includes two cooling fans mounted on the right-hand side of the case when viewed from the front panel. Cool air is drawn in through the ventilation slots on the left-hand side panel and blown out by the fans.

When mounting several types of equipment in a rack ensure a supply of cool air to the ventilation inlet slots on the Mentor’s left-hand side panel. Do not obstruct the warm air outlets on the right-hand side of the case or allow the warm exhaust air to enter the cooling intake of other equipment.

4.4 Connections

Always switch the Mentor 401 off before connecting or disconnecting any equipment. The dual-channel error checking used on all safety devices requires both channels of a safety circuit to be made and broken simultaneously. An error may result if connections are not made or broken concurrently while inserting or removing connectors.

All safety input and output devices must be tested following each installation or after any change to the configuration.

4.4.1 Power Supply

Power supply connection is via a Neutrik powerCON TRUE1 type connector. An unprotected link connector is provided for connection to other equipment. The total load of all connected equipment must not exceed the total capacity of the supply.

The Mentor mains supply must be earthed.

Connector:	Neutrik powerCON TRUE1 appliance inlet-outlet NAC3PX
Mating Connector:	Mains in: Neutrik powerCON TRUE1 female cable connector NAC3FX-W Mains link out: Neutrik powerCON TRUE1 male cable connector NAC3MX-W

The mains input to the Mentor 401 is protected by a 2A thermal circuit breaker mounted on the rear panel above the mains input connector.

4.4.2 Emergency Stop / Dead Man's Handle

Six connectors are provided for emergency stop switches, a dead man's handle or enabling switch may additionally be connected to inputs 1 to 3. Emergency stop switches, dead man's handles, foot switches and other safety devices are available from Kinesys. See the supplementary information on page 60 for safety device schematics.

Connector:	MIL-C-5015 reverse bayonet 18-19 female receptacle e.g. Van-System CVBS 03 18-19S
Mating Connector:	MIL-C-5015 reverse bayonet 18-19 male plug e.g. Van-System CVBS 06 18-19P

PIN	FUNCTION	DESCRIPTION
A	TP0	Test Pulse 0 for E-Stop circuit
B	TP1	Test Pulse 1 for E-Stop and DMH circuits
C	ES0	E-Stop switch return
D	ES1	E-Stop switch return
E	TP0'	Test Pulse 0 for DMH circuit
F	DMH0	DMH switch return
G	DMH1	DMH switch return
H	24V	24V DC supply max 500mA*
J	0V	0V supply
K	LED_ES	E-Stop switch LED indicator 24V DC max 75mA*

Maximum recommended cable length using 0.5mm² cable: 250m

Shorting plugs MEN-98-2010 must be fitted to all emergency stop connections when not in use.

Always switch the Mentor off before connecting or disconnecting emergency stop switches or shorting plugs.

* Power outlets on emergency stop switch connectors and beacon / siren connector are protected by a common 1A electronic circuit breaker. Total connected load of all emergency stop switching systems, indicators, beacons and sirens must not exceed 1A

4.4.3 Ethernet + Safety

Ten Ethernet outlets connected to the internal Ethernet switch are available on the rear panel. Two outlets may optionally be factory configured for fibre-optic connections where connections longer than 90m are required, for example, for a front of house snake connection.

All Ethernet outlets may be used for the connection of safety data to devices using PROFIsafe safety signalling, for example apexDRIVE controllers.

Connector: etherCON CAT5
e.g. Neutrik NE8FDV

Mating Connector: etherCON CAT5
e.g. Neutrik NE8MC

Cable Type: Shielded CAT5e or better

PIN	FUNCTION	DESCRIPTION
1	ETH-TX+	Ethernet Data
2	ETH-TX-	Ethernet Data
3	ETH-RX+	Ethernet Data
4		No Connection
5		No Connection
6	ETH-RX-	Ethernet Data
7		No Connection
8		No Connection
Shell	ETH-S	Ethernet Shield

Maximum cable length between devices: 90m (subject to cable manufacturer's recommended maximum cable length)

As this cable carries safety signals and Ethernet automation data the use of a tactical grade cable (for example TMB Proplex PCCAT5EP cable with Neutrik Ethercon connectors) is highly recommended for touring use. Note that not all flexible Ethernet cables are capable of supporting a 90m cable length while conforming to CAT5e standards – refer to the cable manufacturer for further information.

Shielded cables must be used for all Ethernet connections

4.4.4 Ethernet + Safety – Fibre Optic Connection

Mentor M402 has two fibre optic connections compatible with a wide range of entertainment industry Ethernet switches with fibre optic ports, e.g. the ProPlex GBS series from TMB. Fibre optic connection using suitable multimode fibre supports fibre lengths up to 550m.

The fibre optic outlets may be used for the connection of safety data to devices using PROFIsafe safety signalling, for example apexDRIVE controllers.

Connector:	opticalCON QUAD Neutrik NO4FDW-A
Interface Specification:	1GB 1000BASE-SX 850nm Multimode fibre
Cable Type:	Quad multimode fibre e.g. TMB ProPlex OM3

PIN	FUNCTION	DESCRIPTION
a	RECEIVE	Ethernet Data Receive
b	TRANSMIT	Ethernet Data Transmit
A		No connection
B		No connection

Maximum fibre length = 550m

Alternative fibre optic interface configurations are available on request, e.g. single-mode fibre, opticalCON DUO or other connectors.

4.4.5 EVO V2 Ethernet + Safety

Two outlets are provided for connection of Evo devices with a V2 safety interface. Additional devices may be connected using Evo DC8 V2 distribution units

Connector:	etherCON CAT5 e.g. Neutrik NE8FDV
Mating Connector:	etherCON CAT5 e.g. Neutrik NE8MC
Cable Type:	Shielded CAT5e or better

PIN	FUNCTION	DESCRIPTION
1	ETH-TX+	Ethernet Data
2	ETH-TX-	Ethernet Data
3	ETH-RX+	Ethernet Data
4	S-TP0	Test Pulse 0 from remote device
5	S-TP1	Test Pulse 1 from remote device
6	ETH-RX-	Ethernet Data
7	S-ES0	E-Stop circuit return to remote device
8	S-ES1	E-Stop circuit return to remote device
Shell	ETH-S	Ethernet Shield

Maximum cable length: 90m (subject to cable manufacturer's recommended maximum cable length)

As this cable carries safety signals and Ethernet automation data the use of a tactical grade cable is required for all interconnections. The use of TMB Proplex PCCAT5EP cable with Neutrik Ethercon connectors is highly

recommended. Standard “office type” RJ45 patch cables are not permitted. Note that not all flexible Ethernet cables are capable of supporting a 90m cable length while conforming to CAT5e standards – refer to the cable manufacturer for further information.

No shorting plugs are required when the Evo V2 outlets are not in use.

4.4.6 Console / Pendant

The console / pendant connector allows connection of power, data and safety signals for an operator device via a single cable and connector.

Connector:	MIL-C-5015 reverse bayonet 20-A48 female receptacle e.g. Van-System CVBS 00 20-A48S
Mating Connector:	MIL-C-5015 reverse bayonet 20-A48 male plug e.g. Van-System CVBS 06 20-A48P

PIN	FUNCTION	DESCRIPTION
A	TP0	Test Pulse 0 for E-Stop and DMH circuits
B	TP1	Test Pulse 1 for E-Stop and DMH circuits
C	ES0	E-Stop switch return
D	ETH-S	Ethernet Shield
E	ES1	E-Stop switch return
F	DMH0	DMH switch return
G	DMH1	DMH switch return
H	NC	No connection
J	NC	No connection
K	NC	No connection
L	24V	24V DC supply max 1A
M	0V	0V supply
N	ETH-TX-	Ethernet Data
P	ETH-RX-	Ethernet Data
R	NC	No connection
S	NC	No connection
T	NC	No connection
U	ETH-TX+	Ethernet Data
V	ETH-RX+	Ethernet Data

Maximum cable length: 90m

A shorting plug MEN-98-2020 must be fitted to the console / pendant connection when not in use.

Always switch the Mentor off before connecting or disconnecting control devices or shorting plugs.

4.4.7 Beacon / Siren

A connector is provided for connecting beacons, status indicator lights and warning sirens or voice annunciators.

Connector: XLR6 female
e.g. Neutrik NC6FD-LX

Mating Connector: XLR6 male
e.g. Neutrik NC6MXX

PIN	FUNCTION	DESCRIPTION
1	0V	0V supply / common
2	SIGOUT1	24V switched output 1 max 500mA*
3	SIGOUT2	24V switched output 2 max 500mA*
4	SIGOUT3	24V switched output 3 max 500mA*
5	SIGOUT4	24V switched output 4 max 500mA*
6	24V	24V DC supply max. 500mA*

* Power outlets on emergency stop switch connectors and beacon / siren connector are protected by a common 1A electronic circuit breaker. Total connected load of all emergency stop switching systems, indicators, beacons and sirens must not exceed 1A

4.4.8 Universal Device Interface

Two connectors are provided allowing the connection of legacy Kinesys equipment and third-party automation systems. Contact Kinesys for further advice on connecting other equipment such as Elevation 1+ or Digihoist systems, or third-party automation or safety systems.

Connector: Harting DDD17F
e.g. Harting 09 14 017 3101

Mating Connector: Harting DDD17M
e.g. Harting 09 14 017 3001

PIN	FUNCTION	DESCRIPTION
1	M-TP0	Test Pulse 0 from Mentor
2	M-TP1	Test Pulse 1 from Mentor
3	M-ES0	E-Stop circuit return to Mentor
4	M-ES1	E-Stop circuit return to Mentor
5	M-TP0	Test Pulse 0 from Mentor
6	M-TP1	Test Pulse 1 from Mentor
7	M-DMH0	DMH circuit return to Mentor
8	M-DMH1	DMH circuit return to Mentor
9	S-TP0	Test Pulse 0 for E-Stop from remote device
10	S-TP1	Test Pulse 1 for E-Stop from remote device
11	S-ES0	E-Stop circuit return to remote device
12	S-ES1	E-Stop circuit return to remote device
13	S-TP2	Test Pulse 2 for E-Stop from remote device
14	S-TP3	Test Pulse 3 for E-Stop from remote device
15	S-DMH2	DMH circuit return to remote device
16	S-DMH3	DMH circuit return to remote device
17	0V	0V reference

Shorting plugs MEN-98-2040 must be fitted to the Universal Device Interface connectors when not in use.

5 Configuration

5.1 Configuring Hard Wired Safety Devices

The system configuration should be designed following a risk assessment of the required safety devices and implemented and modified only by authorised persons.

Document the system configuration with a layout drawing and a list of required safety devices and output devices.

Test all safety devices following each installation or system reconfiguration, and regularly following installation or reconfiguration. Generally mobile devices connected using flexible should be tested monthly, fixed devices connected using flexible cables every three months, and fixed devices installed using fixed wiring (for example, using conduit or fixed, armoured cable) every 12 months. Your risk assessment or local codes may dictate a different test cycle.

5.1.1 Shorting Plugs

Shorting plugs must be fitted whenever a hard-wired safety input device is not connected. The following connections on the Mentor's rear panel must have either safety devices or shorting plugs connected. In some instances a connection cable may include wiring to short out the emergency stop input where this is not used – for example cables designed to connect output-only devices to the universal device interface connector.

Emergency Stop 1 / DMH
Emergency Stop 2 / DMH
Emergency Stop 3 / DMH
Emergency Stop 4
Emergency Stop 5
Emergency Stop 6
Console / Pendant
Universal Device Interface 1
Universal Device Interface 2

Always store unused shorting plugs securely to prevent misuse. The system configuration should be designed following a risk assessment and implemented and modified only by authorised persons.

5.2 Key Switches

Some operation and configuration of the Mentor 401 is configured by the use of key-operated switches. Keys must be removed after configuration and stored in a location accessible only to personnel authorised to carry out configuration or reset operations.

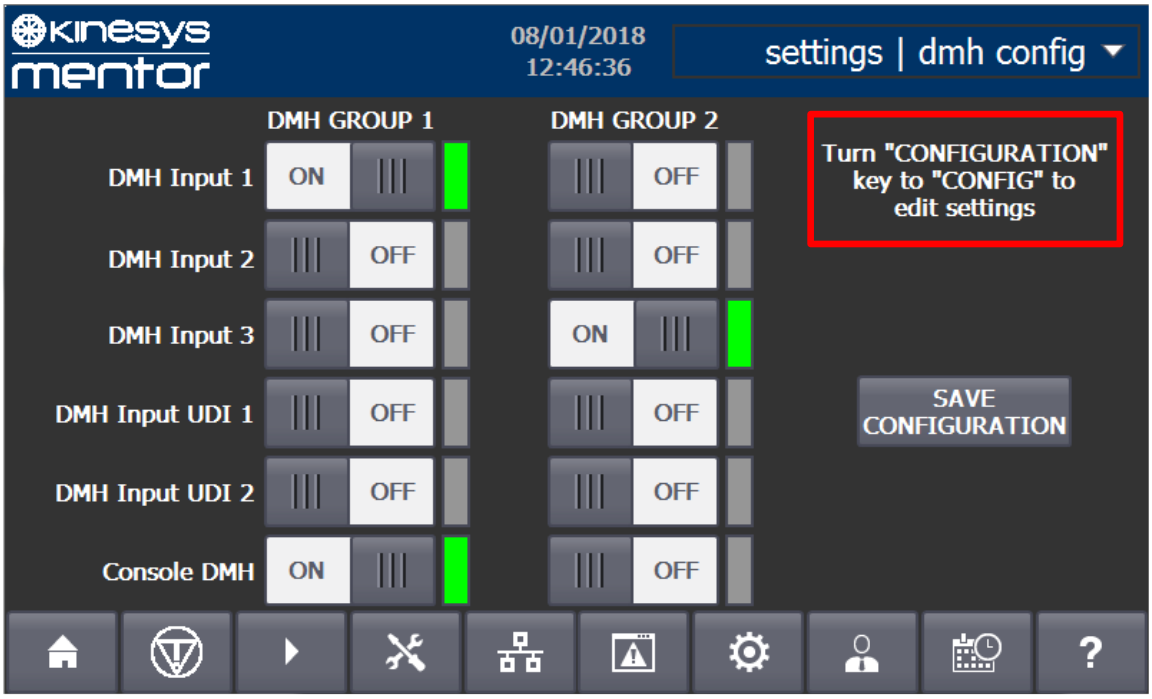
Where the use of common key types may result in reduced security alternative key profiles may be supplied on request.

5.3 Enabling Switch (Dead Man's Handle) Configuration

The enabling switch inputs and processing logic are configured using the touch screen.

Click the Settings icon ⚙ and then press the "DMH Configuration" button on the settings screen to access the configuration menu. The DMH configuration age can also be accessed via the button on the DMH status page.

The login dialog box will be displayed (unless the user is currently logged in). Enter a user name and password with basic configuration rights to continue. Refer to section 5.7 "Security" for further information.



The screen will prompt to turn the "CONFIGURATION" key to "CONFIG" in order to edit settings. Note that moving to CONFIG mode will disable all devices and inhibit movement.

Mentor has two DMH groups, at least one of which must be active to enable the connected drives. Each enabling switch input may be selected for use in either or both DMH groups using the slide switches on the configuration screen.

To use an enabling switch move the slide switch to the right; to disable an enabling switch move the slide switch to the left. Switches may also be toggled by double-clicking. The indicators to the right of the switches show which devices will be enabled in each group. In the example above, Group 1 has DMH Input 1 and the Console DMH enabled; Group 2 has DMH Input 3 enabled. The drives may therefore be enabled by ANY of the following options:

DMH Input 1 AND Console DMH

DMH Input 3
DMH Override

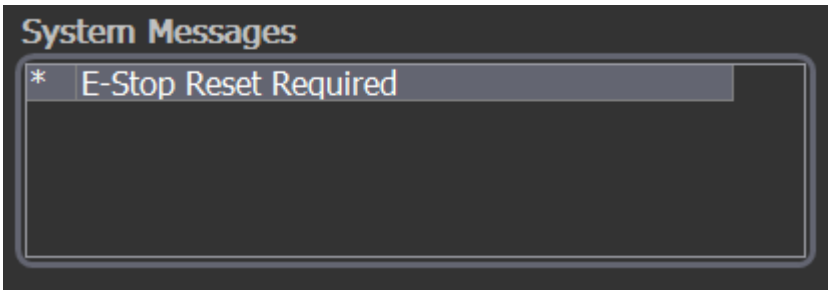
When the DMH configuration has been made, turn the “CONFIGURATION” key to “ACCEPT” and press the “SAVE CONFIGURATION” button.

Turn the “CONFIGURATION” key back to “RUN” once configuration is complete.

5.4 Emergency Stop Reset Mode Configuration

Mentor may be configured to automatically reset the emergency stop ioutputs when all emergency stop switches have been released, or to require a reset command from the RESET key on the front panel to turn on the emergency stop outputs.

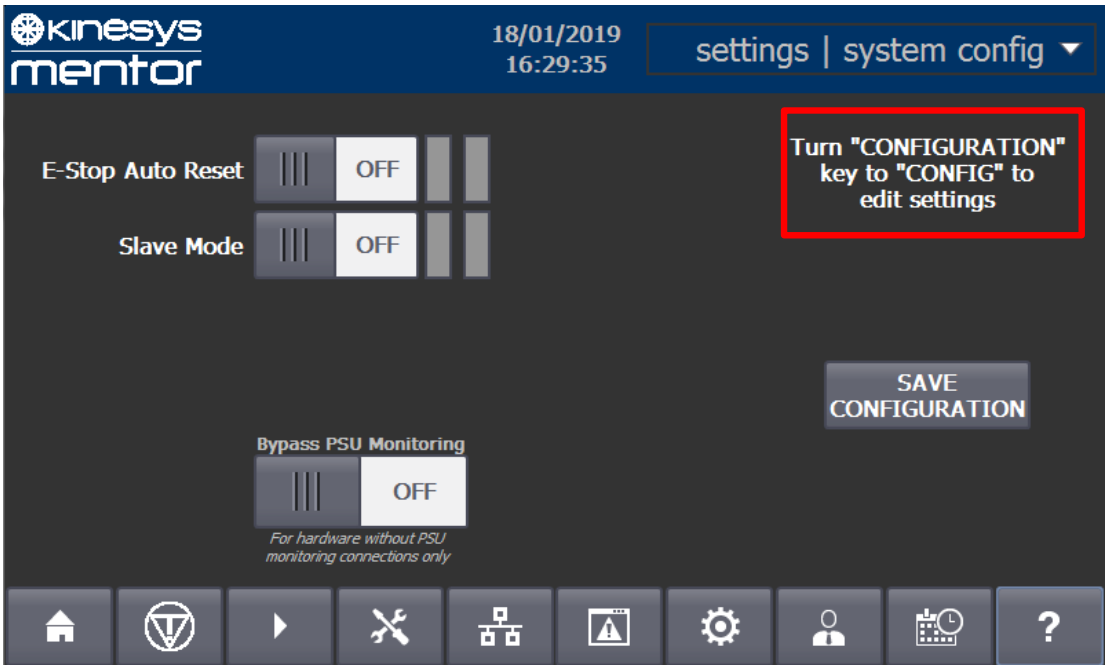
When auto reset is turned off a reset command is required to turn on the emergency stop outputs once all the emergency stop switches have been released. The yellow ring around the front panel emergency stop switch will flash rapidly and a message will be displayed in the System Message Centre when a reset command is required.



Turn the RESET key clockwise to reset the emergency stop system and turn on the emergency stop outputs.

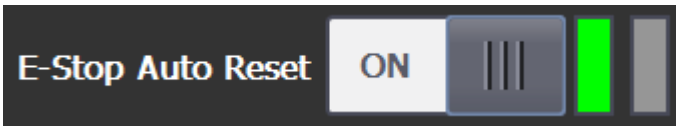
To configure the emergency stop reset operation click the Settings icon ⚙ and then press the “System Configuration” button on the settings screen to access the configuration menu.

The login dialog box will be displayed (unless a user with appropriate access rights is currently logged in). Enter a user name and password with basic configuration rights to continue. Refer to section 5.7 “Security” for further information.

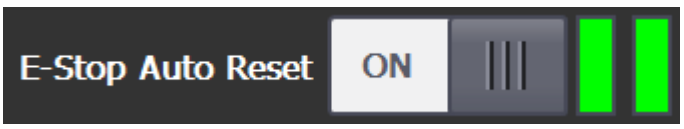


The screen will prompt to turn the “CONFIGURATION” key to “CONFIG” in order to edit settings. Note that moving to CONFIG mode will disable all devices and inhibit movement.

Turn the “CONFIGURATION” key to “CONFIG”. To enable automatic reset mode slide the “E-Stop Auto Reset” switch to the right, To disable automatic reset mode slide the switch to the left. The indicator immediately to the right of the switch confirms the setting which will be saved.



When the configuration has been made, turn the “CONFIGURATION” key to “ACCEPT” and press the “SAVE CONFIGURATION” button. The second indicator to the right of the switch will show the final configuration.



Turn the “CONFIGURATION” key back to “RUN” once configuration is complete.

5.5 Configuration of Network Safety Devices

Mentor 401 may be used to integrate devices using PROFIsafe over PROFINET safety signalling over standard Ethernet cables and data distribution. PROFIsafe uses a coded data transmission which requires a matching “Profinet Device Name” and “F-Device Address” for each connected

device. PROFINET device names and F-device addresses must be unique within the network.

Each Mentor 401 is factory configured for a range of PROFINET device names and matching F-device addresses from an allocated customer block. The configured range can only be re-configured by Kinesys. The available range of devices can be viewed on the help menu.

Each apexDRIVE to be controlled by the Mentor 401 must be assigned a unique PROFINET device name and matching F-device address from the Mentor address range. The following sections describe how to check and change PROFINET device names and F-device addresses where necessary.

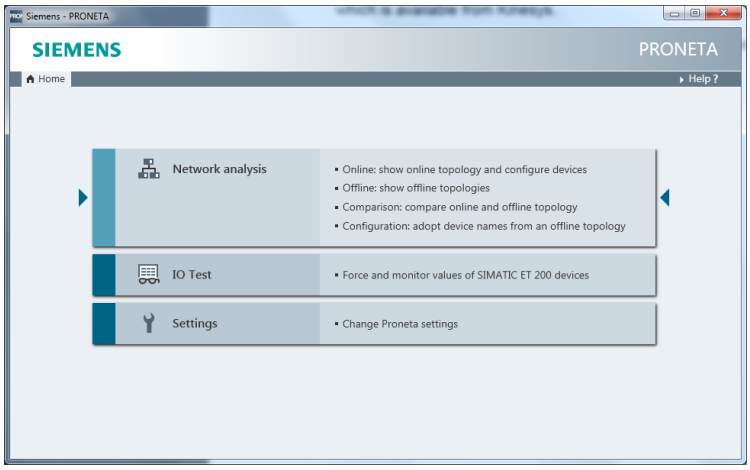
Currently only apexDRIVE supports PROFIsafe over PROFINET signalling.

5.5.1 Checking a Device's Profinet Device Name

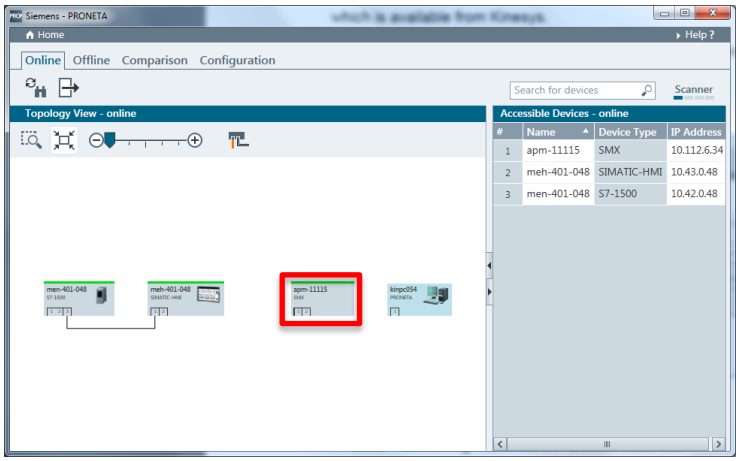
The Profinet device name may be verified using the Proneta configuration software which is available from Kinesys. Refer to the apexDRIVE user manual for further information on using Proneta.

It will be easier to check the device name if only one PROFINET device is connected to the Mentor.

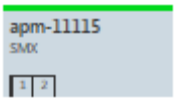
1. Run Proneta and select "Network Analysis"

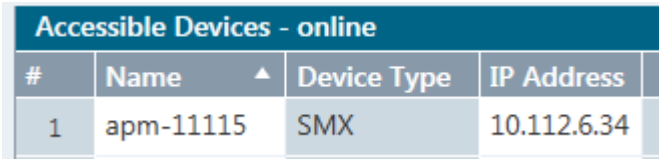


2. The connected devices are shown in graphical and tabular format as shown below.



3. The visible devices should be:
   - any configuration PC with a PROFINET device driver
   - the Mentor SPLC (name **men-401-xxx** where xxx is the last three digits of the serial number)
   - the Mentor display (name **meh-401-xxx** where xxx is the last three digits of the serial number)
   - a PROFINET device – in the example above a Device Type “SMX” which is the SPLC used in apexDRIVE. The PROFINET device name may be read from the Proneta display



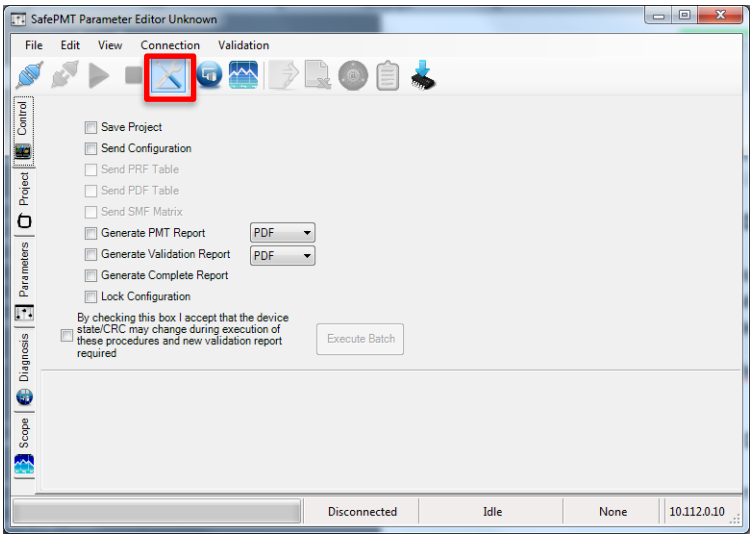


Note that all devices are assigned a unique IP address in the 10.0.0.0 / 24 subnet at manufacture. This must not be changed.

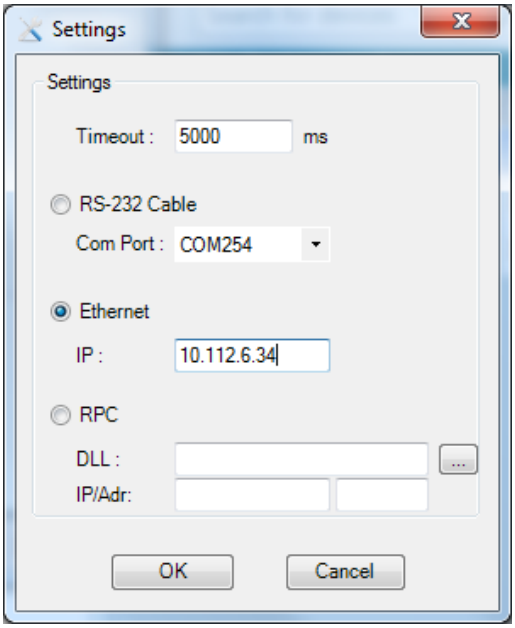
5.5.2 Checking a Device’s F-Device Address

The F-device address is written independently of the Profinet device name into the memory of the SPLC safety processors. The F-device address can only be verified by producing a safety system report using the SafePMT software available from Kinesys.

1. Run the SafePMT software and select the settings dialog from the toolbar or the |Connection |Settings menu option.



2. In the connection settings dialog check the “Ethernet” radio button and enter the device IP address in the “IP:” box



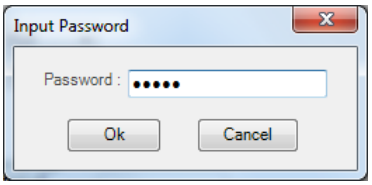
The IP address is shown in the Proneta display (see above)

For apexDRIVE controllers the IP address is in the format 10.112.xx.yy where xxyy is the last 4 digits of the device serial number, for example Serial Number: 12027-0634 IP address: 10.112.6.34

Click “OK” to save the changes.

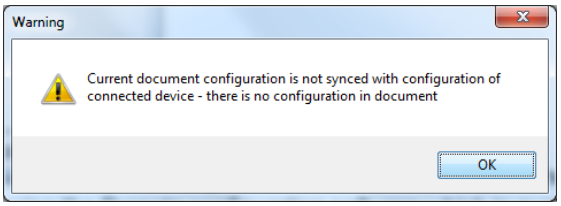
3. Click the connect button on the toolbar or select |Connection |Connect in the menu bar.

4. Enter the device password in the “Input Password” dialog as confirmation that connection has been made to the correct device. The password is the same as the device serial number and can be read from the apexDRIVE SPLC status screen.

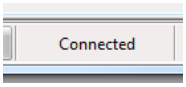


Passwords should be entered as a 5-digit number. If the serial number is less than 5 digits, add “0”s to the beginning of the serial number to create a 5-digit password.
For example:
serial number: **123** Password: **00123**

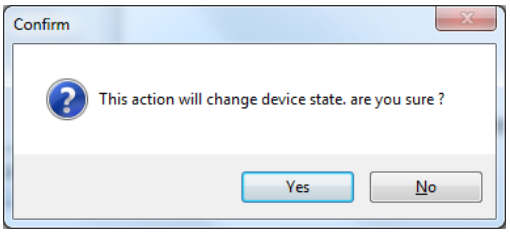
5. If no configuration file is open in SafePMT the following warning dialog appears. Click “OK” to dismiss the warning.



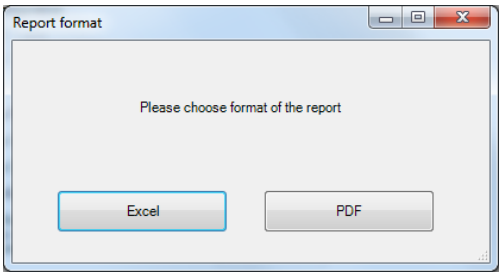
6. When connected the word “Connected” will show in the status bar.



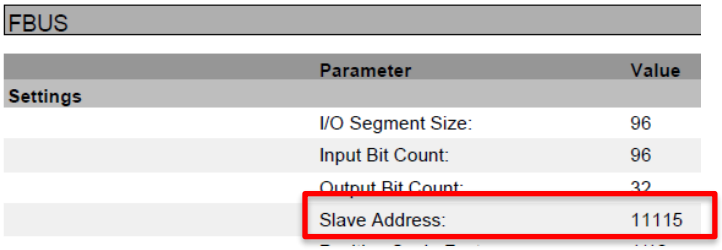
7. Click the “Generate Report” button on the toolbar or select |Validation |Generate Report from the menu. Click “Yes” to confirm the change in device state. Note that the connected SPLC will be stopped – this will stop motion on the connected drive and, if the drive is enabled in Mentor, all other devices connected to the Mentor.



8. Choose the “PDF” report format and then enter a filename and select a location to save the report.



9. When the report is displayed scroll down to the “FBUS” section (or press CTRL + F and enter FBUS in the search dialog). The F-device address is shown in the report in the “slave address” field

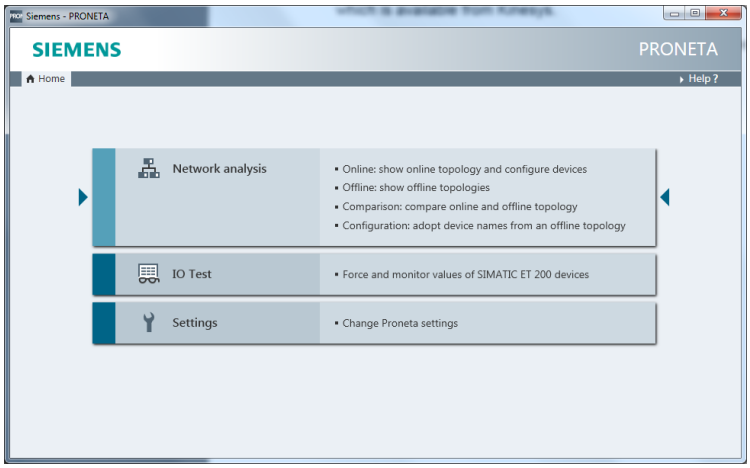


For correct operation the slave address should match the 5-digit number in the Profinet device name.

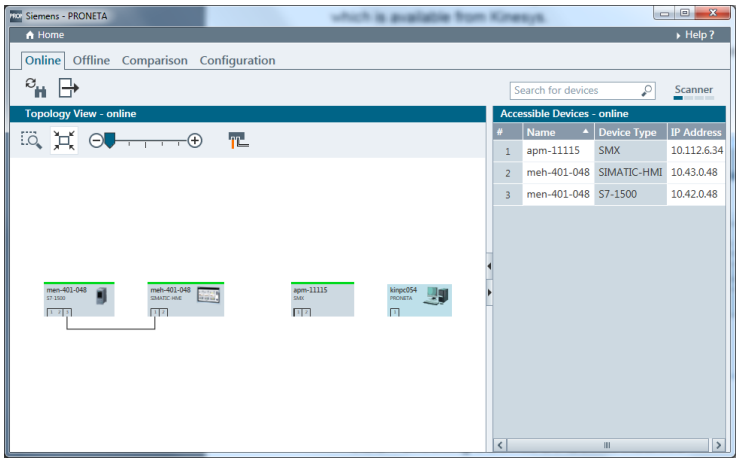
5.5.3 Changing a Device’s Profinet Device Name

The Profinet device name may be changed to fit the available range of the Mentor 401 or to avoid duplicate names using the Proneta configuration software which is available from Kinesys. Refer to the apexDRIVE user manual for further information on using Proneta.

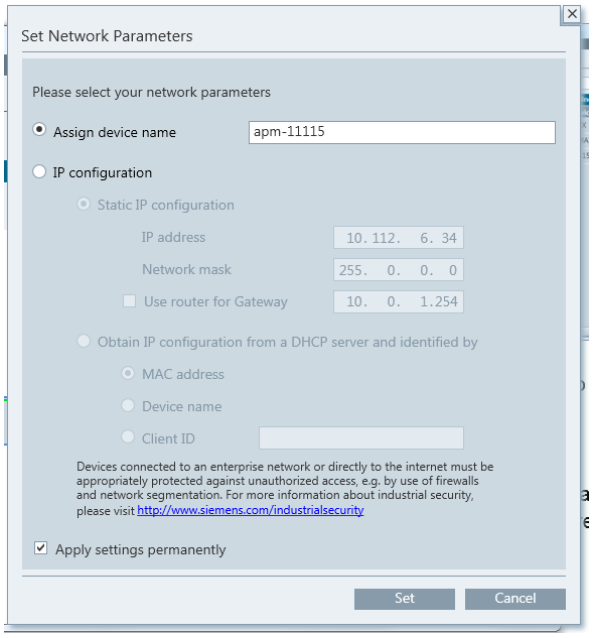
1. Run Proneta and select “Network Analysis”



2. The connected devices are shown in graphical and tabular format as shown below.



3. Double-click the graphical icon for the device to be changed to open the “Set Network Parameters” dialog.



Make sure the “Assign device name” radio button is checked and enter the required device name in the dialog box. Click “Set” to save the new device name.

apexDRIVE controllers all have a device name in the format
apm-abcde
where abcde is a 5-digit numeric sequence.

Note that all devices are assigned a unique IP address in the 10.0.0.0 / 24 subnet at manufacture. This address must not be changed.

The F-device address must be set to match the 5 numeric digits of the Profinet device name otherwise safety communications will not be enabled.

5.5.4 Changing a Device’s F-Device Address

The F-Device Address must be set to match the 5-digit number in the Profinet Device Name.
For example:
Profinet Device Name: **apm-12345** F-Device Address: **12345**

F-Device addresses are set using SafePMT as part of a parameter download. Refer to the apexDRIVE user manual for further details on downloading and verifying parameters with SafePMT.

1. Open the correct parameter (.PMT) file for the hoist and drive, including any user configured settings which may be required.

2. Click the “Parameters” tab on the left hand side of the window

3. Select “F-Bus” at the bottom of the parameter browser

4. In the “value” field next to “F-Destination Address” enter the correct F-Address and press Enter

5. Download and validate the configuration as described in the apexDRIVE manual.

5.6 Linking Mentor Systems

It may be necessary to link multiple Mentor systems to connect large numbers of apexDRIVES, or to use apexDRIVES from different address ranges without re-addressing the devices.

5.6.1 Linking Mentors using the Universal Device Interface Connection

Up to two Mentors operating in “slave” mode may be connected to a single Mentor acting as the “master” using the Universal Device Interface connectors.

Mentor slave mode configuration is currently available only as a factory set option (from software version 21). All Mentor 400 systems with software version 16 or greater can act as the master when the DMH system is configured as detailed below.

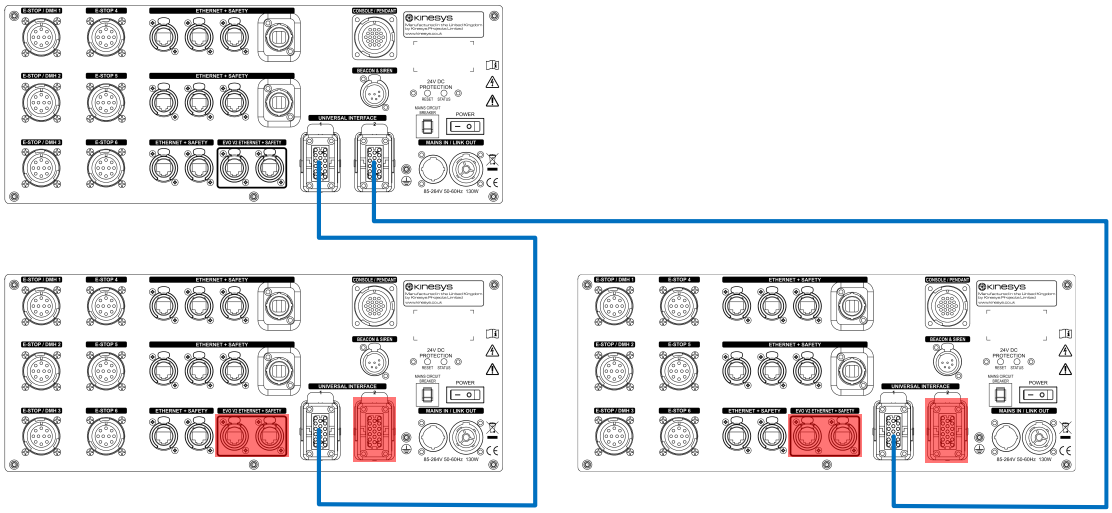
5.6.1.1 Connecting Mentors in Master-Slave Configuration using the UDI Connector

The safety circuits (emergency stop and dead man’s handle) are connected via the Universal Device Interface connectors. Ethernet control data may be linked for control by a common control computer or pendant or may be left separated if two independent control systems are required.

Notes:

- A male-male UDI link cable (Kinesys part number 9280201) will be required for each Mentor slave connection
- The second UDI connector and the Evo V2 outputs on Mentors connected as slaves must not be used. Unused UDI connectors and Evo V2 outputs on the master Mentor may be used for connection of other devices.
- Connected devices MUST have unique PROFINET names and F-device addresses. Any duplicate addresses will cause network conflicts.

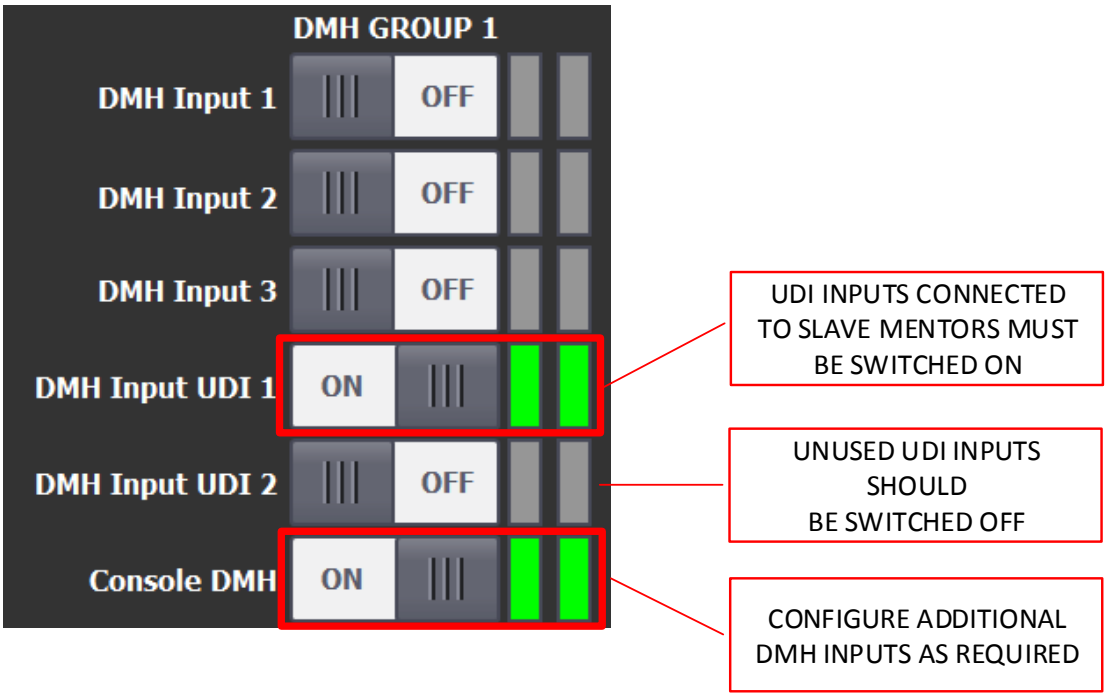
Connection Diagram



5.6.1.2 Configuring the Master Mentor for connections using the UDI Connectors

The Mentor used as the Master must have the Dead Man's Handle inputs for the relevant UDI connector(s) enabled.

Refer to section 5.3 Enabling Switch (Dead Man's Handle) Configuration on page 22 for full details on configuring the dead man's handle system.

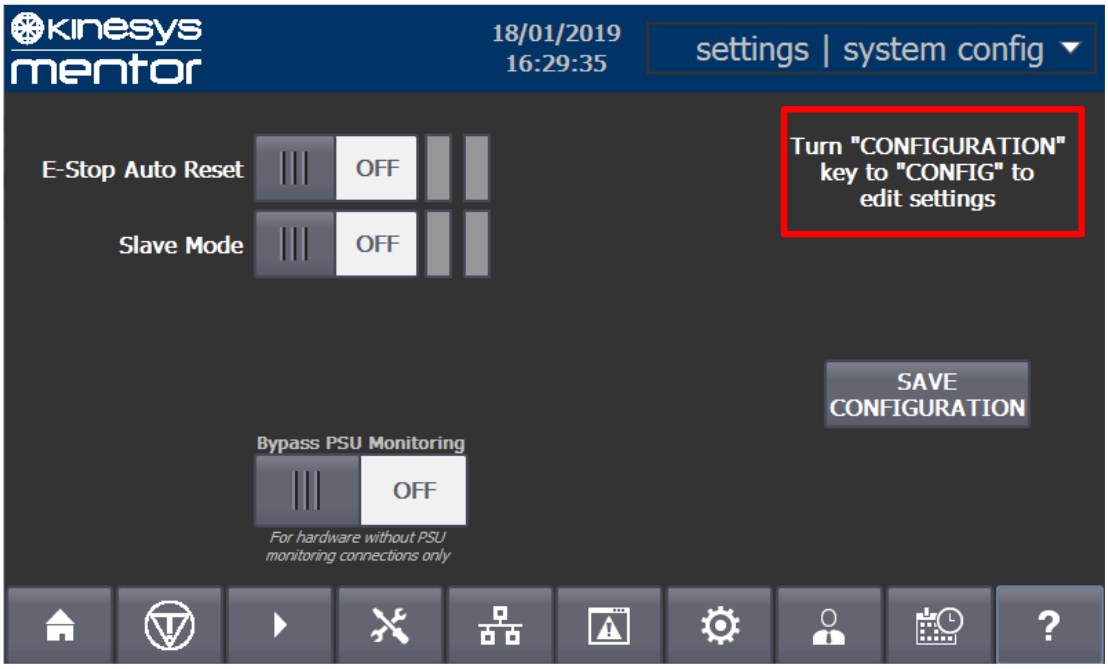


A different configuration may be entered for DMH Group 2 but the UDI DMH inputs connected to slave Mentors must be switched ON in both groups.

5.6.1.3 Configuring the Slave Mentor for connections using the UDI Connectors

Click the Settings icon ⚙ and then press the "System Configuration" button on the settings screen to access the configuration menu.

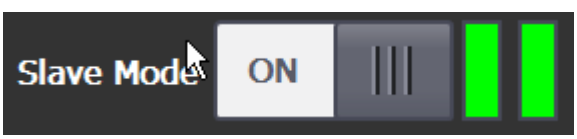
The login dialog box will be displayed (unless a user with appropriate access rights is currently logged in). Enter a user name and password with basic configuration rights to continue. Refer to section 5.7 "Security" for further information.



The screen will prompt to turn the "CONFIGURATION" key to "CONFIG" in order to edit settings. Note that moving to CONFIG mode will disable all devices and inhibit movement.

Turn the "CONFIGURATION" key to "CONFIG". To enable slave mode slide the "Slave Mode" switch to the right, To disable slave mode slide the switch to the left. The indicator immediately to the right of the switch confirms the setting which will be saved.

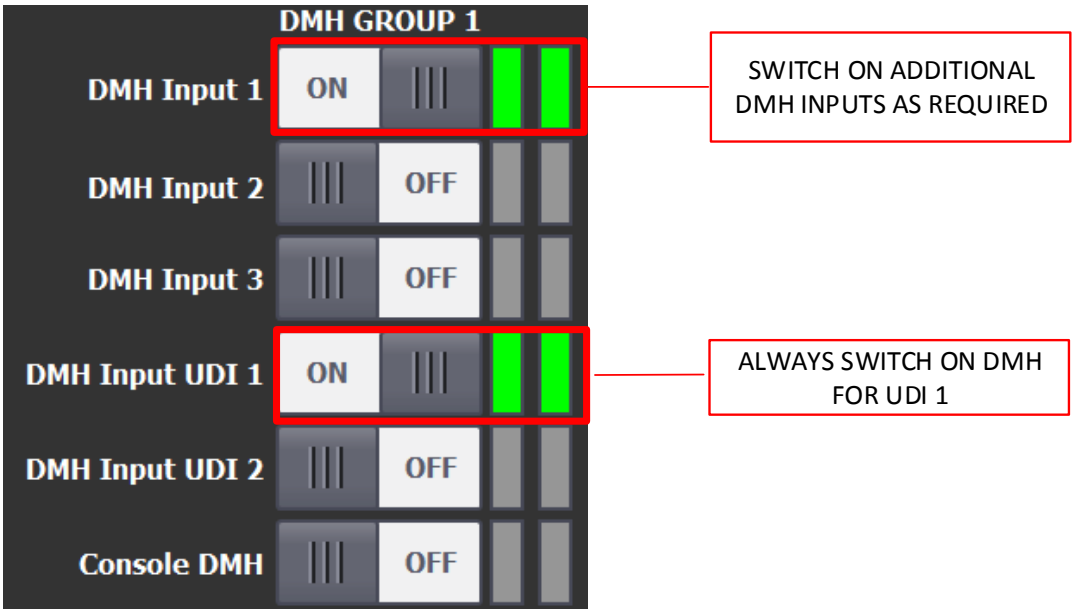
When the configuration has been made, turn the "CONFIGURATION" key to "ACCEPT" and press the "SAVE CONFIGURATION" button. The second indicator to the right of the switch will show the final configuration.



Turn the "CONFIGURATION" key back to "RUN" once configuration is complete.

A Mentor which has been set to Slave mode will show a slave mode banner on the home screen.

The Mentor(s) used as slaves must have the dead man's handle input for UDI 1 enabled. Any other inputs on the slave Mentor which have dead man's handles connected should also be switched on.



A different configuration may be entered for DMH Group 2 but the UDI 1 DMH input must be switched ON in both groups.

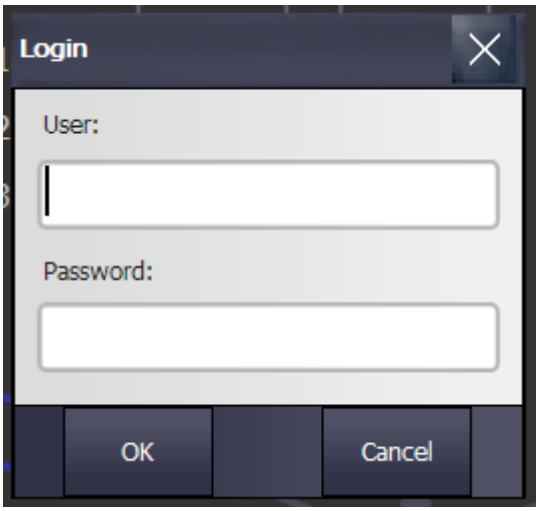
Refer to section 5.3 Enabling Switch (Dead Man's Handle) Configuration on page 22 for full details on configuring the dead man's handle system.

5.6.1.4 Testing the Master-Slave Configuration

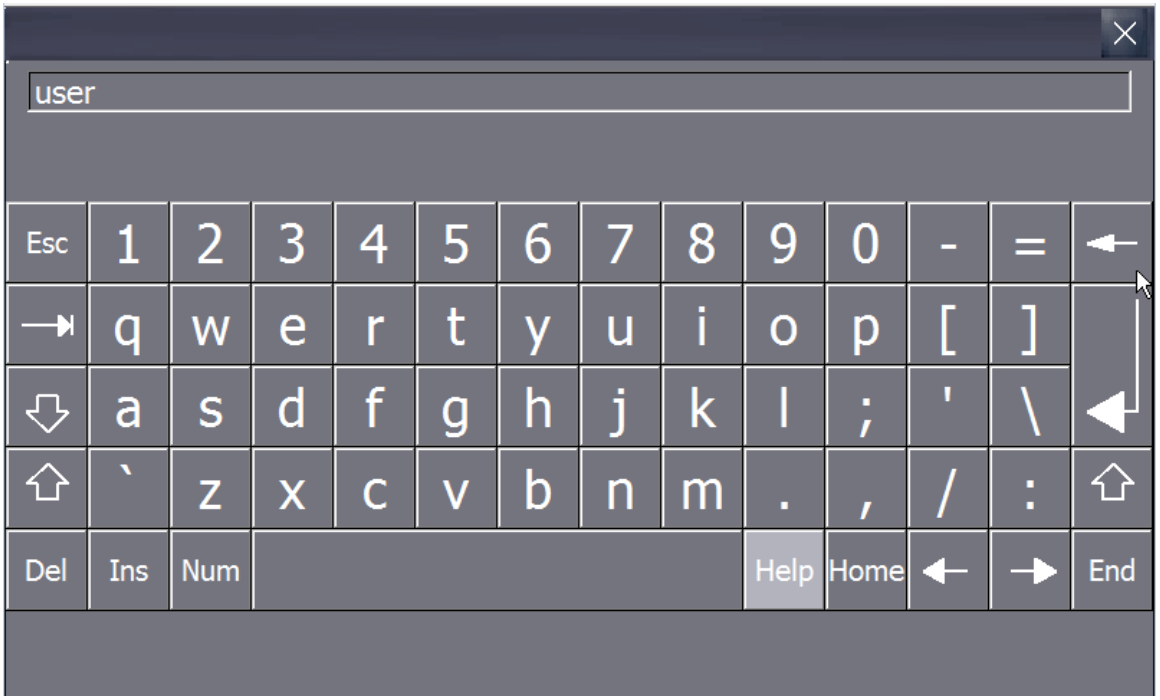
Always test all connected emergency stop devices and dead man's handles after connection and configuration to ensure that all of the drives connected to the master and slave Mentors operate correctly and receive the emergency stop and dead man's handle commands as required. Retest the entire system following any change in configuration.

5.7 Security

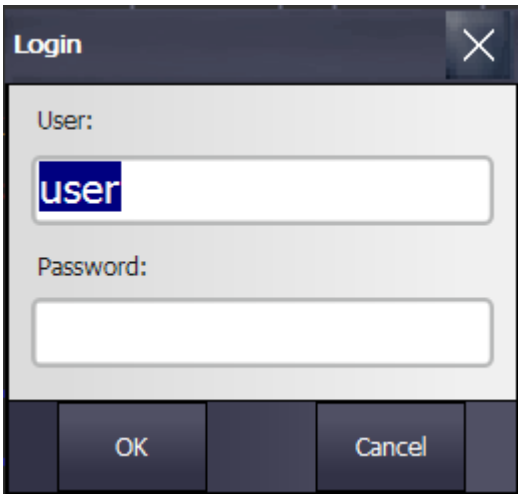
Certain operations on the Mentor display are protected by passwords. When an attempt to access a protected area or operate a protected function is made by a user with insufficient permissions a Login dialog box will be displayed:



Touch the “User” field and a text entry keyboard will be displayed to allow a user name to be entered. Touch “Cancel” to exit.

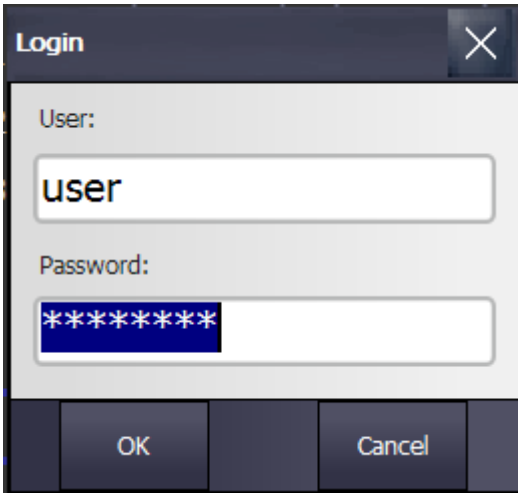


Enter a user name (not case-sensitive) and press ↵ or press “Esc” or X to quit.



Touch the “Password” field and the text entry keyboard will be displayed to allow a password to be entered. Note that passwords are case-sensitive.

When a user name and password have been entered touch OK to log in.



Re-select the protected function and, if the user has sufficient access permissions, access will be granted.

Users will automatically be logged out after 5 minutes for security. The currently logged in user can be displayed by pressing the button.

5.8 User Management

6 Operation

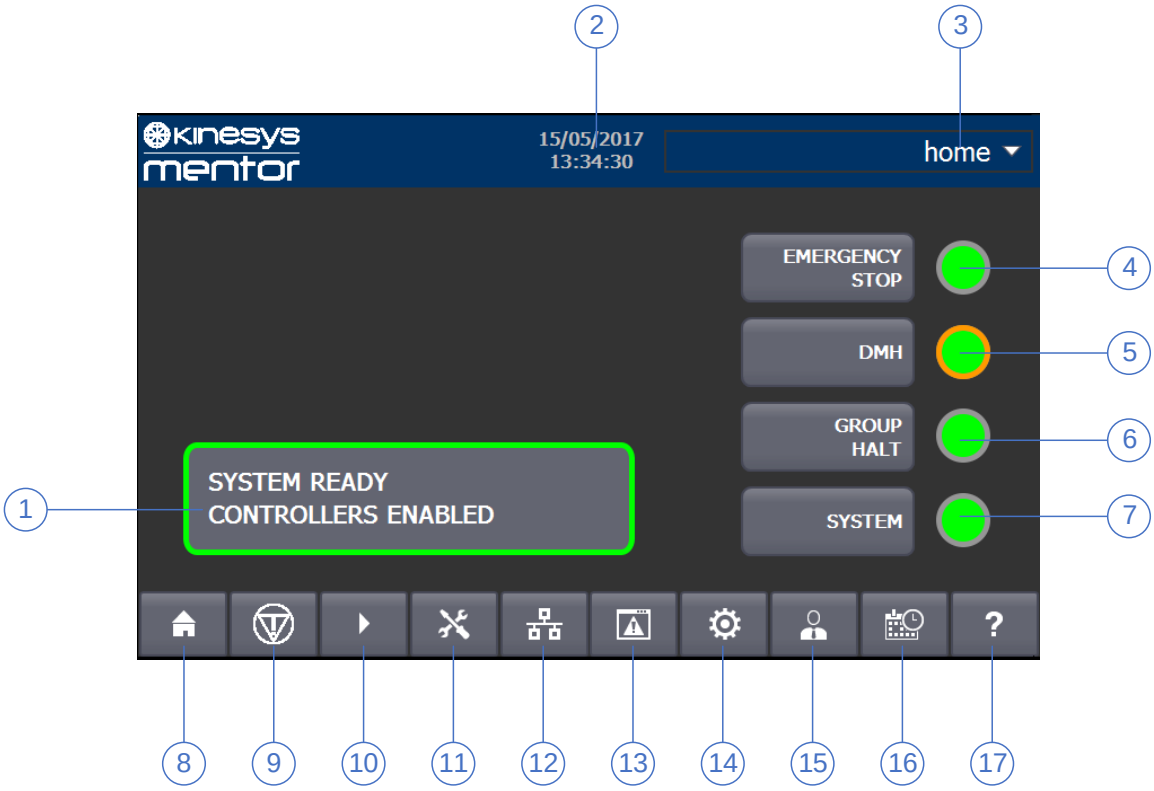
6.1 System Startup

Make all connections as described in section 4.4 prior to switching on. Switch the Mentor on using the power switch located on the rear panel above the mains input connector. The system will start and after initialisation the home screen will be displayed on the touchscreen display.

6.2 Touchscreen Display

WARNING! Use only a finger or touchscreen stylus to operate the touchscreen. Do not use sharp objects such as pens or screwdrivers as these may cause permanent damage to the touchscreen.

6.2.1 Home Screen



1. **Status Area**
   displays the status of the Mentor outputs. The Status Area border shows the current system status:

GREEN	System is operational and one or more drives are enabled
YELLOW	All drives are disabled, for instance because of an activated emergency stop button or a released enabling switch

RED	There is a system fault preventing any devices from being enabled

2. **Date and Time Display**
   Shows the current system date and time. Mentor can act as a time server for suitable devices enabling log files to have a consistent time stamp across multiple devices. Touch the date and time display or the calendar menu button to set the date and time.

3. **Screen Navigation**
   indicates the title of the currently displayed screen. Touch the drop-down arrow to navigate through all available screens.

4. **Emergency Stop Status Indicator**
   shows the status of all connected emergency stop switches.

GREEN	All emergency stop switches are released and the emergency stop system is ready
YELLOW	All emergency stop switches are released but the emergency stop system is awaiting a reset signal
RED	One or more emergency stop buttons have been pressed

5. **Dead Man's Handle (Enabling Switch) Status Indicator**
   shows the status of the dead man's handle (enabling switch) system.

GREEN	The output of the dead man's handle system is on and drives are enabled
OFF	The output of the dead man's handle system is off

6. **Group Halt Status Indicator**
   shows the status of the group halt system.

GREEN	All groups are OK and enabled
YELLOW	One or more groups have a warning status (for example, are close to a position or load synchronisation error)
RED	One or more groups have a shutdown status (for example, a position or load synchronisation error has occurred or a device in the group has failed)

7. **System Status Indicator**

8. **Home Menu Button**

9. **Emergency Stop Menu Button**

10. **Dead Man's Handle Menu Button**

11. Tools Menu Button

12. Network Configuration Menu Button

13. Alarms Menu Button

14. Settings Menu Button

15. User Administration Menu Button

16. Calendar Menu Button

17. Help Menu Button

6.3 Emergency Stop Buttons

Pressing any emergency stop button will immediately initiate an emergency stop of all connected equipment. The red LED indicator in the activated emergency stop button will flash and a message will be shown on the display.

If an emergency stop button has been activated and thereby shut down all devices, a dangerous situation may still remain. Only release the emergency stop button once the cause of the emergency stop has been assessed and resolved.

Turn the emergency stop button to release it.

The yellow ring around the emergency stop switch on the Mentor front panel illuminates to indicate the status of the emergency stop system:

OFF:	SPLC has not yet started or system fault
ON:	emergency stop system is ready for operation
FLASH 1Hz:	an emergency stop button has been pressed
FLASH 5Hz:	all emergency stop buttons are released and the system is waiting for a reset signal

All emergency stop buttons must be tested following any new installation or configuration of the system, and at regular intervals thereafter.

WARNING! When apexDRIVE controllers are operated in “EVO V2” mode or with “Use Emergency Stop on Network Devices” turned off the emergency stop buttons on the apexDRIVEs will only stop the local drive and not all other connected devices. This should be assessed as part of your risk assessment, and if there is any possibility of confusion appropriate measures must be taken, for example the use of warning notices, operator training, or covering the emergency stop switches on the apexDRIVEs.

6.4 Enabling Switches (Dead Man’s Buttons)

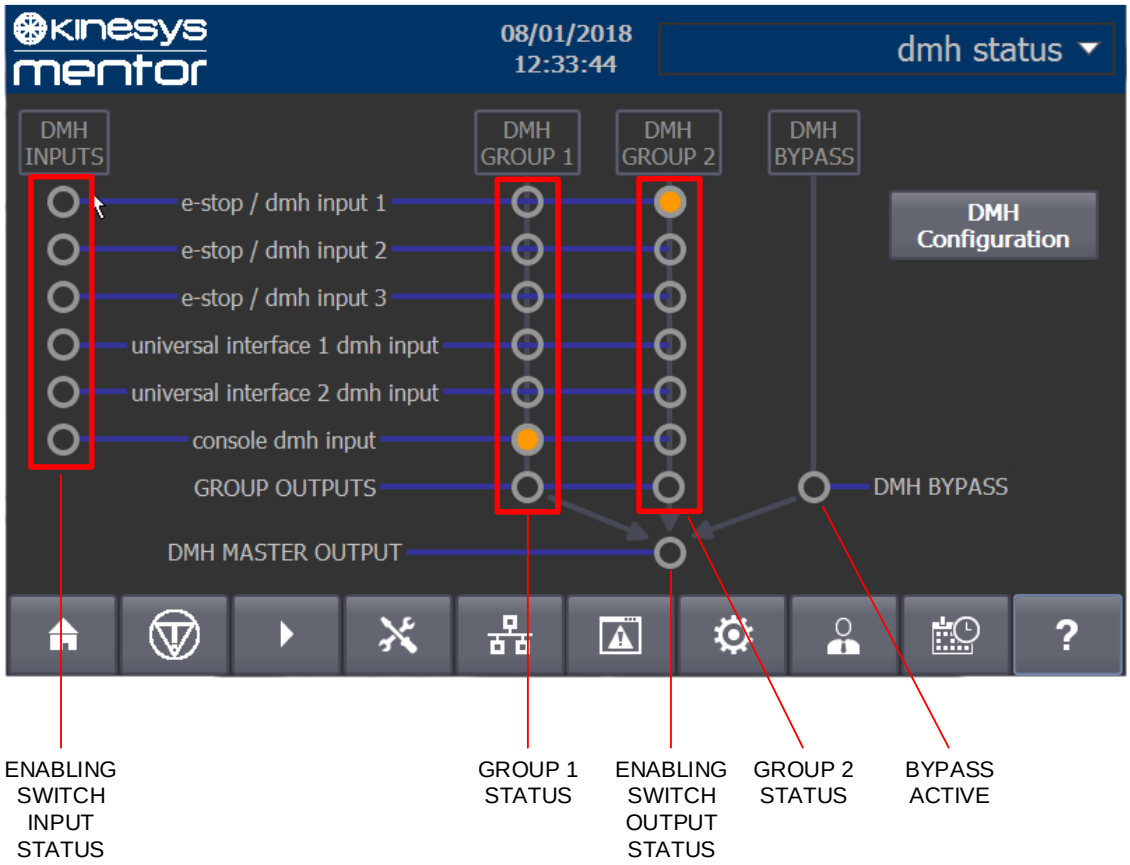
Up to six hard-wired enabling switches (Dead Man’s Handles, Dead Man’s Buttons or DMH) may be connected to the Mentor 401. The use of at least one enabling switch is highly recommended in all applications; further switches may

be required where, for instance, the operator does not have a clear line of sight to the axis being controlled.

For configuration of the enabling switches refer to Enabling Switch (Dead Man's Handle) Configuration on page 22

6.4.1 Enabling Switch Status Display

Touch the ⊕ button to access the enabling switch status page.



To enable drives at least one of the DMH groups must be active, or the DMH bypass must be enabled. The status of the enabling switches and their group assignments is shown on the DMH status screen. An enabling switch which is assigned to a group is shown by an orange indicator, an enabled device by a green indicator. A device which is not assigned to a particular group is shown by an empty circle.

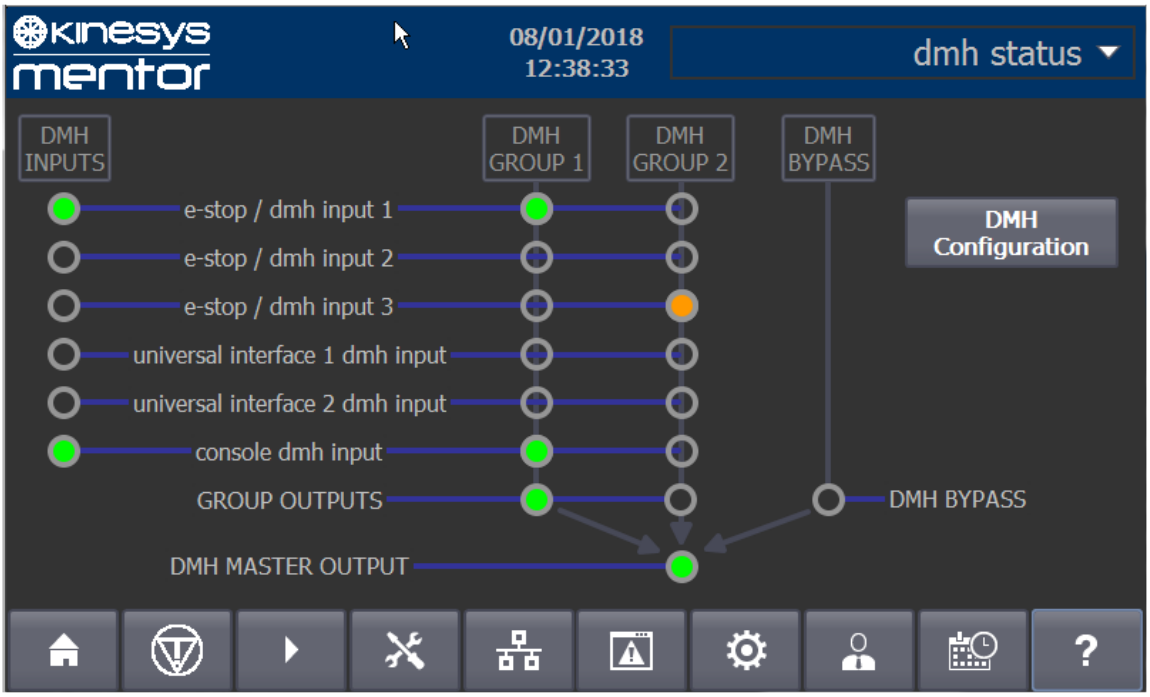
In the example shown above the connected drives may be enabled by one of the three following combinations:

A) DMH input 1 + Console DMH

B) DMH input 3 + Console DMH

C) DMH Bypass

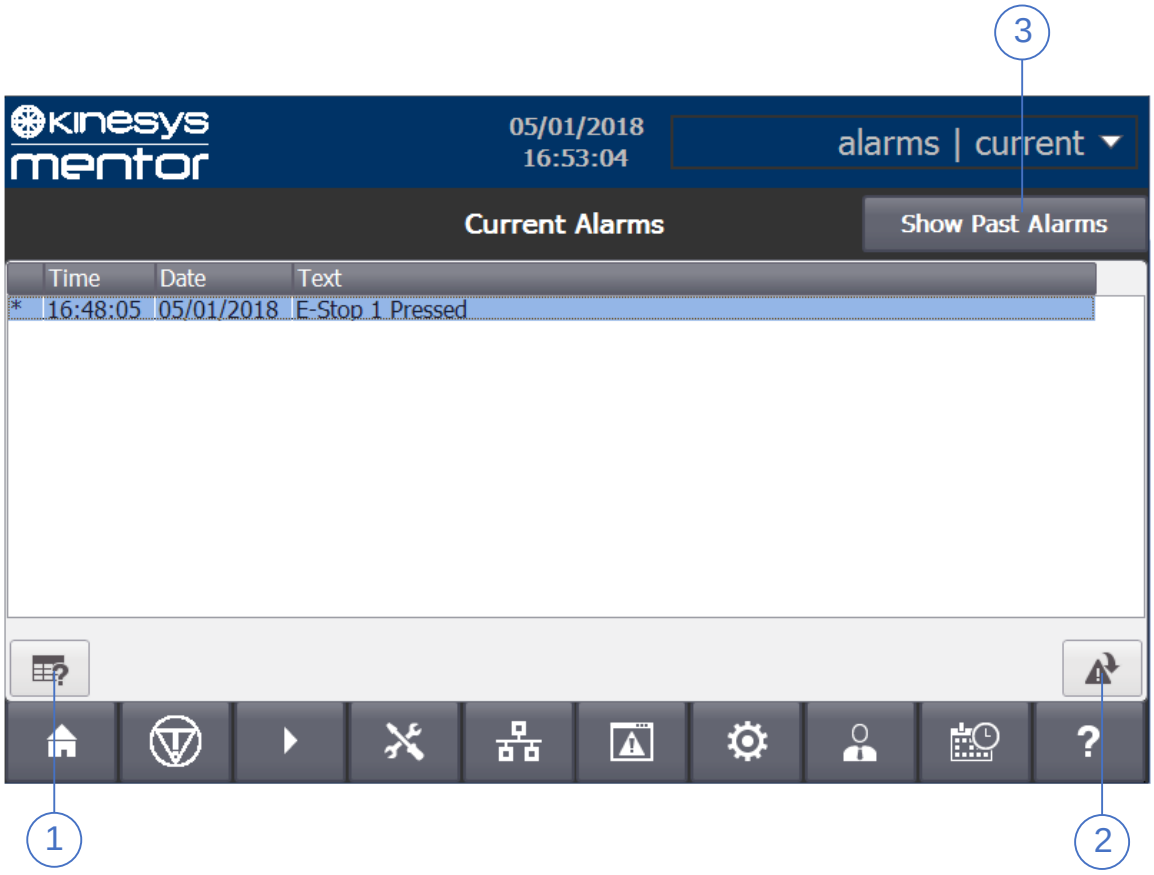
When all the selected enabling switches in a group are active, the group output, and in turn the master output, will be enabled.



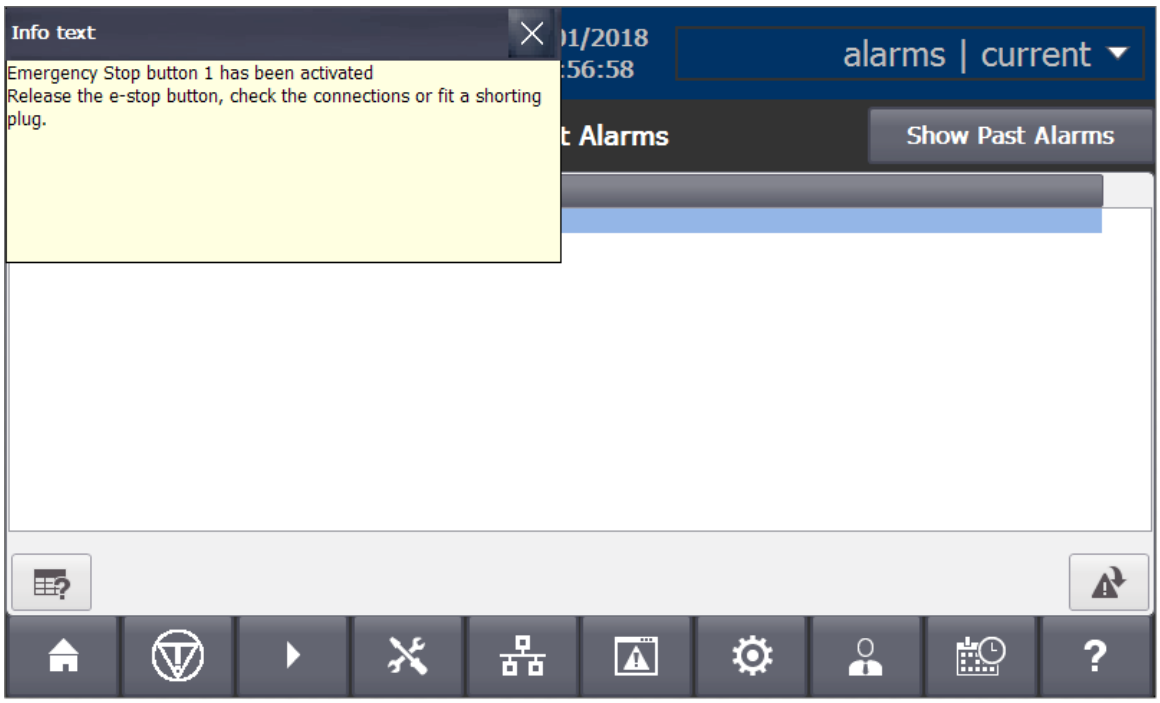
6.5 Alarm Display

The Alarm Display may be accessed using the ⚠ button.

The initial display shows all currently active alarms.

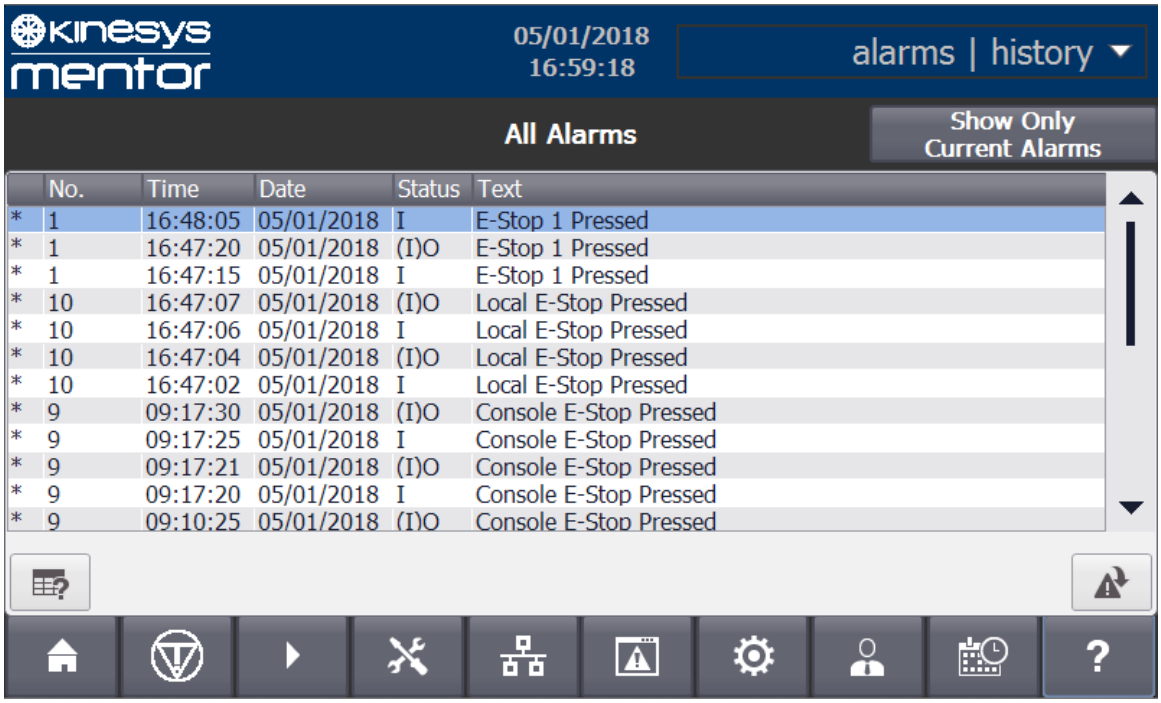


Highlight an alarm and press the  button (1) to receive further information.



Press the X button to close the information dialog.

Press the “Show Past Alarms” button (3) to show all current and historical alarms, along with time and date stamps..



An incoming alarm will be shown by “I” in the “Status” column. A cleared alarm will be shown by (I)O in the status column.

6.6 Remote Status Display

The Mentor display may be viewed on a remote Windows PC using the Sm@rtClient application. Connect to the Mentor display IP address shown on the
| Help | About screen.

Refer to Appendix C on page 66 for further information.

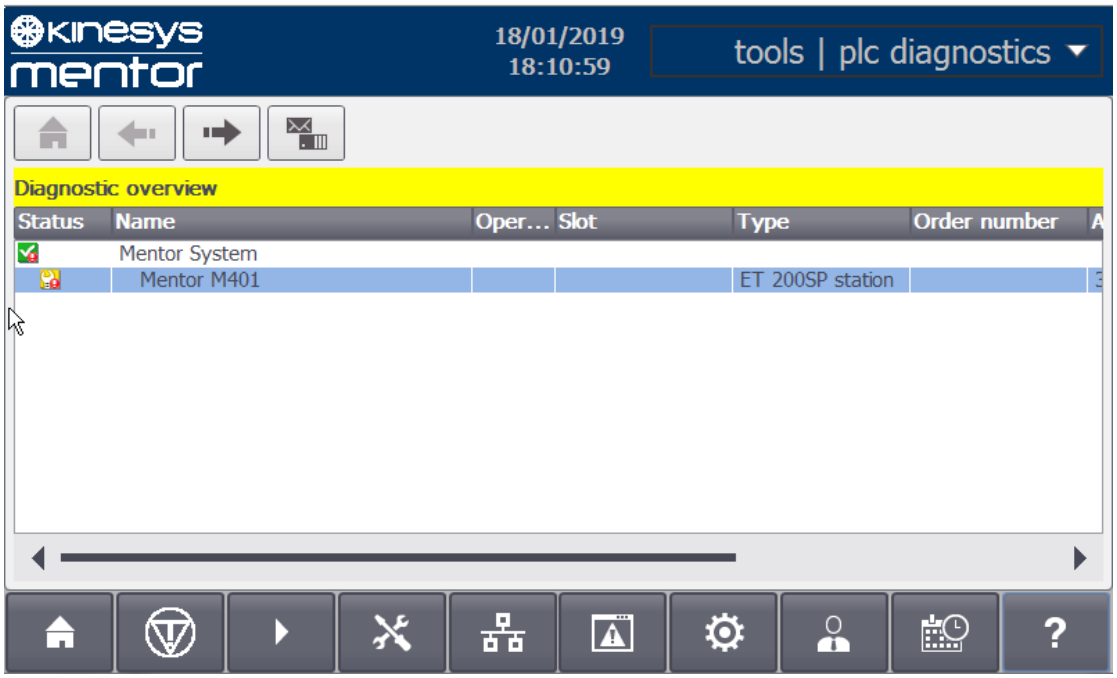
7 Fault Finding & Maintenance

7.1 Diagnostics

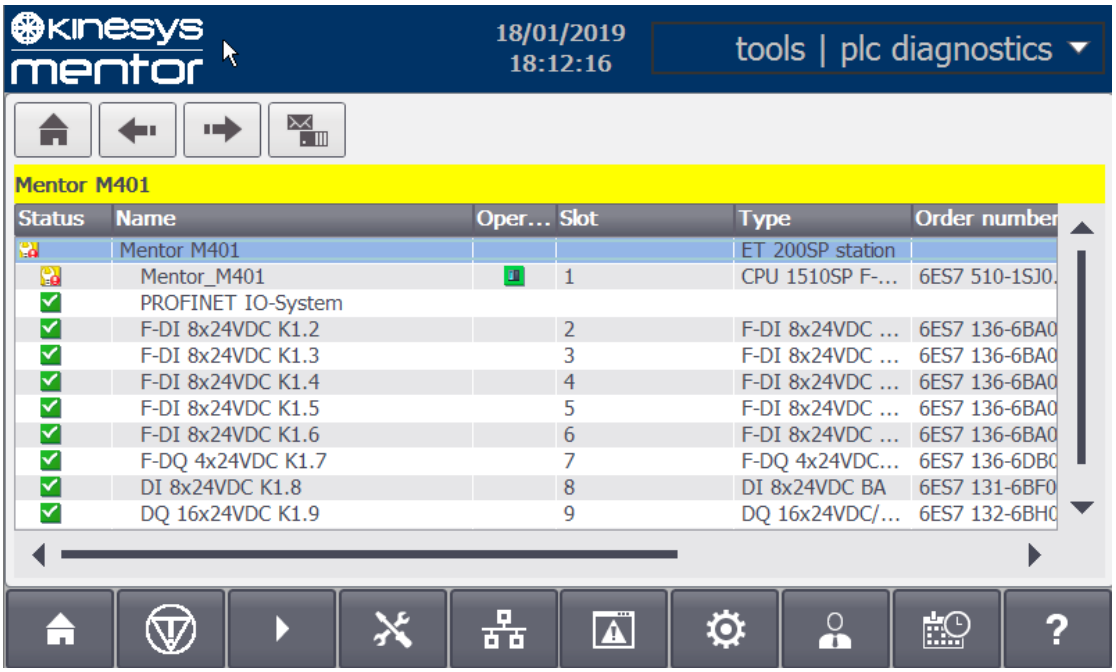
7.1.1 PLC Diagnostics Display

The PLC diagnostics display provides information on the Mentor hardware and software which may be helpful to Kinesys engineers when diagnosing a problem.

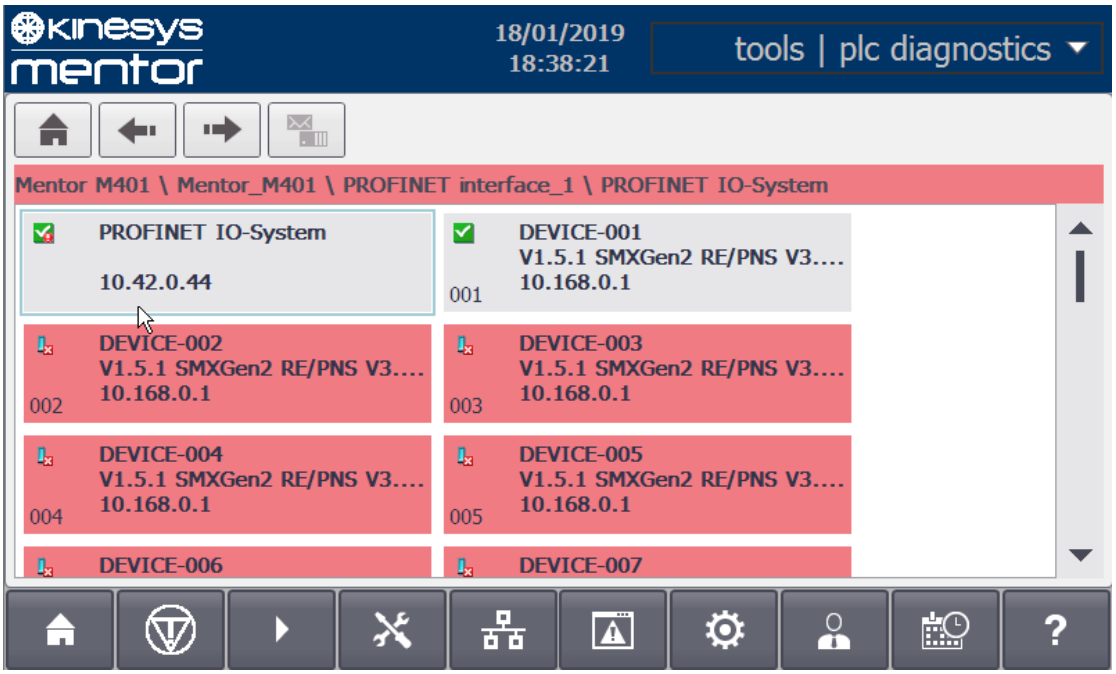
To view the PLC diagnostics display click the “Diagnostics” button on the Tools menu .



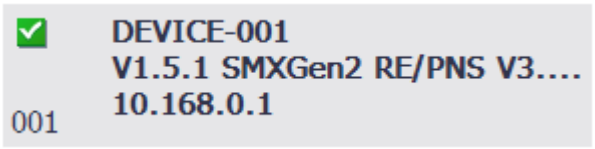
Select the “Mentor 401” entry and click the ➡ button to drill down into the system.



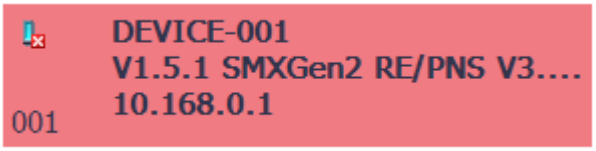
To see the status of connected devices, select the “PROFINET IO_System” line and click the ➟ button. Each apexDRIVE is represented by a rectangle on the screen.



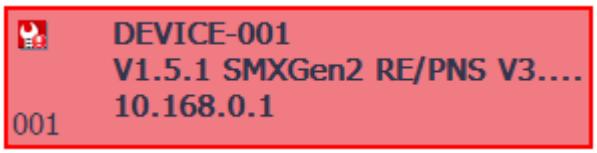
A grey rectangle with the “device OK” icon indicates a device which has connected successfully, including the safety communications



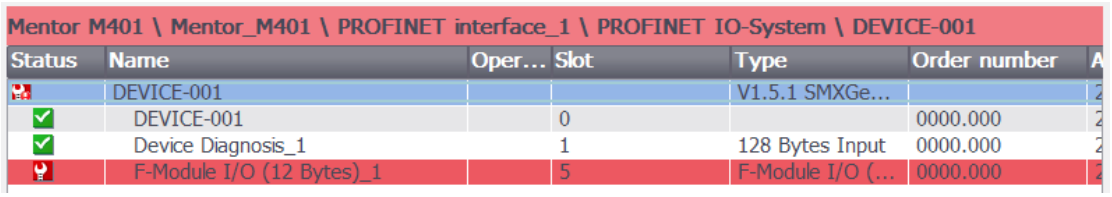
A red rectangle with the “device disconnected” icon indicates that the device is not connected (no Ethernet connection or incorrect PROFINET address)



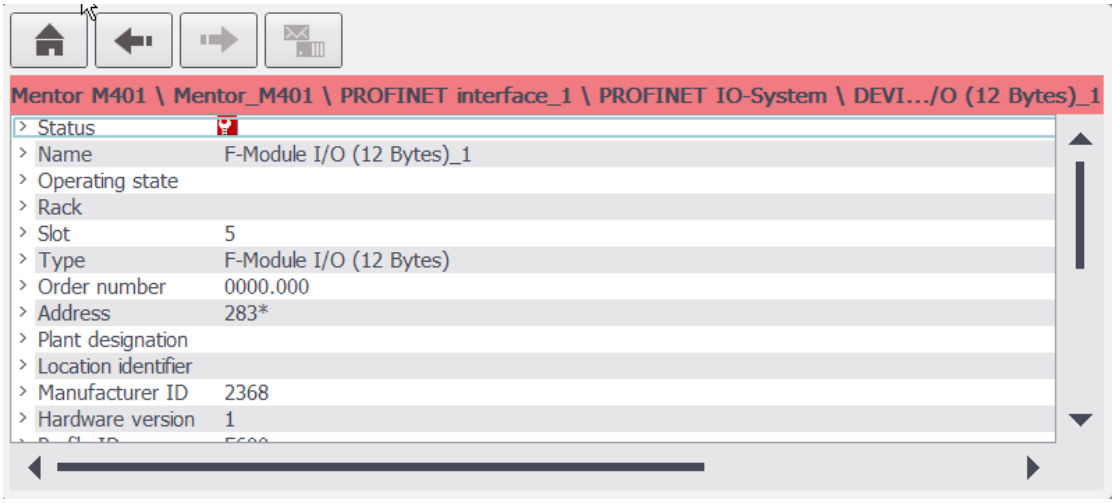
A red rectangle with a red border with the “maintenance” icon indicates that the device is connected but there is a fault with the safety communications – usually an incorrect F-device address.



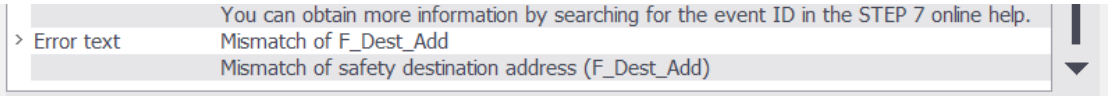
Further information may be found by selecting the device and clicking the ➟ button



This shows that that safety inputs and outputs in the apexDRIVE are not communicating - select the line highlighted in red (“F-Module I/O..”) and click the ➟ button for further information.



Scroll down to see further information – here the screen shows a mismatch of the F-device address (or “F_Dest_Add”)



Press the ⬅ button to move back up one level. Press the 🏠 button above the PLC diagnostic display to return to the top level of the diagnostics tree. Press any of the menu buttons at the bottom of the screen to exit the PLC diagnostic display and return to one of the Mentor display screens.

Also see “Uploading Service Data for Analysis” on page 89.

7.2 Power Supply Protection

7.2.1 Mains Input (AC Supply)

The mains input to the Mentor is protected by a 2A thermal magnetic circuit breaker mounted on the rear panel above the mains inlet.

When tripped the circuit breaker actuator will pop out and reveal a white indicator. Press the actuator to reset the circuit breaker; it may be necessary to wait for up to 3 minutes to allow the circuit breaker to cool before resetting is permitted.

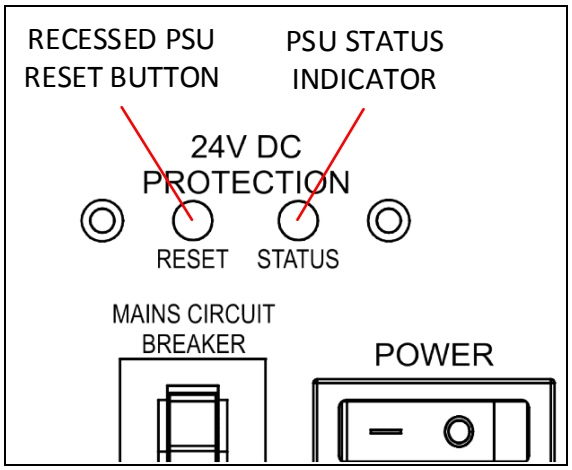
If the circuit breaker trips repeatedly contact Kinesys or your local distributor for support.

7.2.2 DC Circuit Protection

Mentor incorporates an electronic protection system for the 24V DC control circuits. The protection is split into four circuit groups:

1. Programmable Logic Controller, Ethernet switch (internal)
2. Touchscreen display, fans (internal)
3. Emergency stop switch power supplies and indicators
   Beacon and siren outputs
   1A total load maximum
4. Console / Pendant output
   2A maximum

An overloaded circuit will trip while leaving other circuits operational.



Status of the protection system is shown by the “STATUS” indicator on the rear panel above the mains input.

Green:	supply OK
Yellow flashing:	warning – one or more outputs operating at > 80% capacity
Off:	alarm – one or more outputs tripped

Gently press the recessed “RESET” button with a pen or screwdriver to reset the power supply alarm or trip.

If the power supply trips repeatedly disconnect all external devices (pendant or console, emergency stop switches). If the power supply trips with no external devices connected contact Kinesys or your local distributor for support. If the power supply does not trip then reconnect the external devices and cables one at a time to identify the device or cable with a fault.

7.3 Maintenance & Repair

Your Mentor 401 is designed for long service in a demanding professional environment. In normal use no user maintenance should be required beyond periodic functional and safety testing, and basic cleaning.

Mentor 401 contains no user-serviceable parts. In the event of damage or premature failure please contact Kinesys or your local distributor to arrange service or repair.

7.3.1 Cleaning the Enclosure

Warning! Turn off power to the Mentor 401 before cleaning.

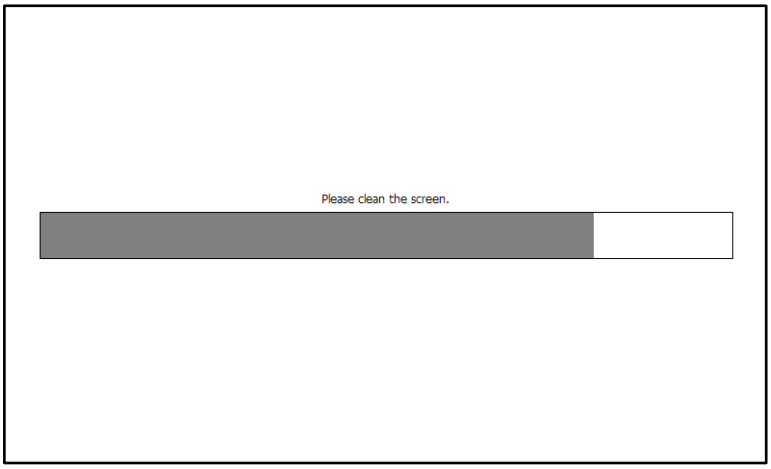
The enclosure should be kept clean and dust free by periodically wiping down with a soft cloth. A clean, dry brush or vacuum cleaner brush attachment may be used to remove dirt from cooling grilles and around controls.

Light dirt or finger marks may be removed using a slightly dampened cloth if necessary. To avoid damaging the surface finishes of the Mentor 401 do NOT use harsh chemicals or abrasive materials when cleaning.

7.3.2 Cleaning the Touchscreen

Warning! If you clean the touch screen when it is switched on, you may cause incorrect operator inputs.

Switch the Mentor 401 off prior to cleaning or activate the clean screen mode by pressing the “Clean Touchscreen” button on the TOOLS menu. Once the clean screen is activated, touch screen operation is locked for 30 seconds. The time remaining for the lockout is indicated by a progress bar.



Clean the touchscreen using a cleaning cloth dampened with a cleaning agent. Only use water with a little liquid detergent or a screen cleaning foam. Do not use solvents or abrasive cleaners. Do not spray cleaning agent directly onto the screen. When cleaning the display, wipe inwards from the edge of the screen.

7.3.3 Periodic Inspection

Visually inspect all connectors and controls. If damage is noted then contact Kinesys, or your local distributor to arrange repair.

7.3.4 Electrical testing

The Mentor 401 is safety tested during manufacture:

Earth Bond 25A
500V DC Insulation Resistance

Periodic safety testing should be carried out in accordance with local electrical equipment safety regulations.

Warning! To avoid damage to internal electronics, do NOT flash (Hi-Pot) test Mentor 401.

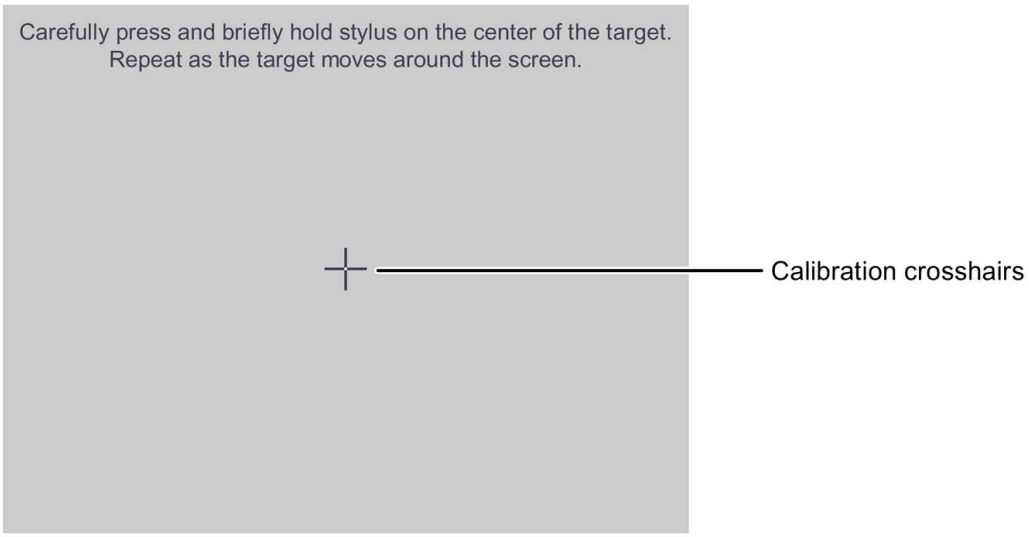
7.3.5 Safety System Testing

Mentor 401 tests all safety inputs during operation by using pulsed signals to determine the presence of short-circuits between safety signals, or to power supply rails. Additionally two-circuit safety devices such as emergency stop switches and enabling switches are tested to ensure that both circuits make and break simultaneously when operated. No additional tests need to be performed on the safety system other than the complete, documented functional tests performed following each installation or reconfiguration of the system and regularly thereafter.

7.3.6 Recalibrating the Touchscreen

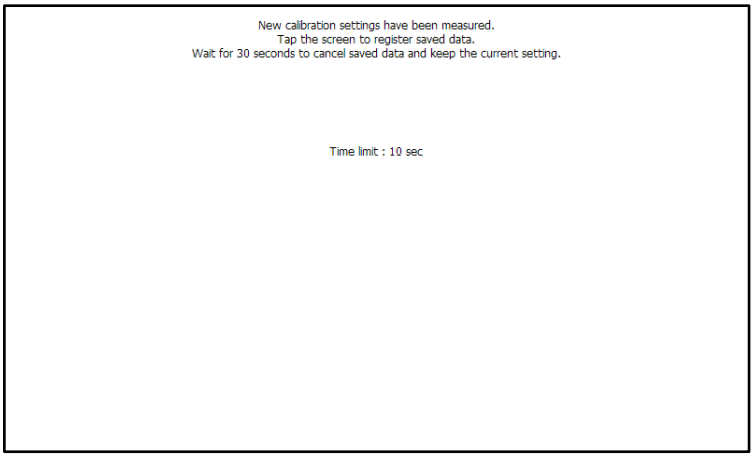
The display touchscreen is factory calibrated and should not normally require recalibration.

If calibration is required enter the touchscreen calibration page by touching the “Calibrate Touchscreen” button from the TOOLS menu. The following dialog is displayed:



Touch the centre of the calibration cross until it is shown at the next position. The calibration cross appears at four other positions. Use only a touchscreen stylus to calibrate the touchscreen. Do not use pens, screwdrivers or other sharp objects as these may cause permanent damage to the touchscreen.

Once you have touched the calibration cross at all five positions, the following dialog appears:

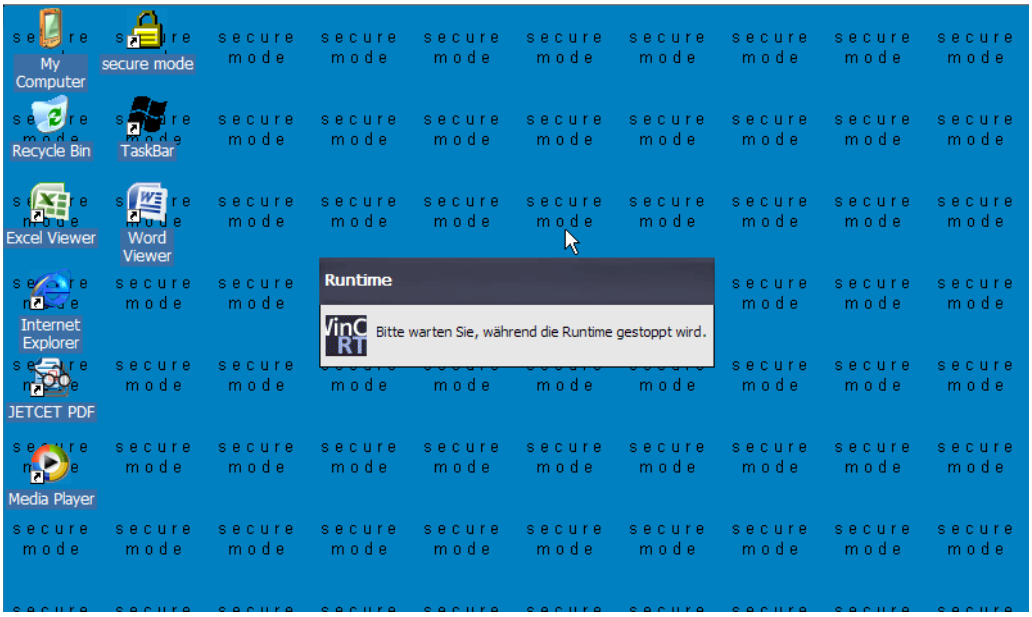


7.3.7 Accessing the Windows CE Control Panel

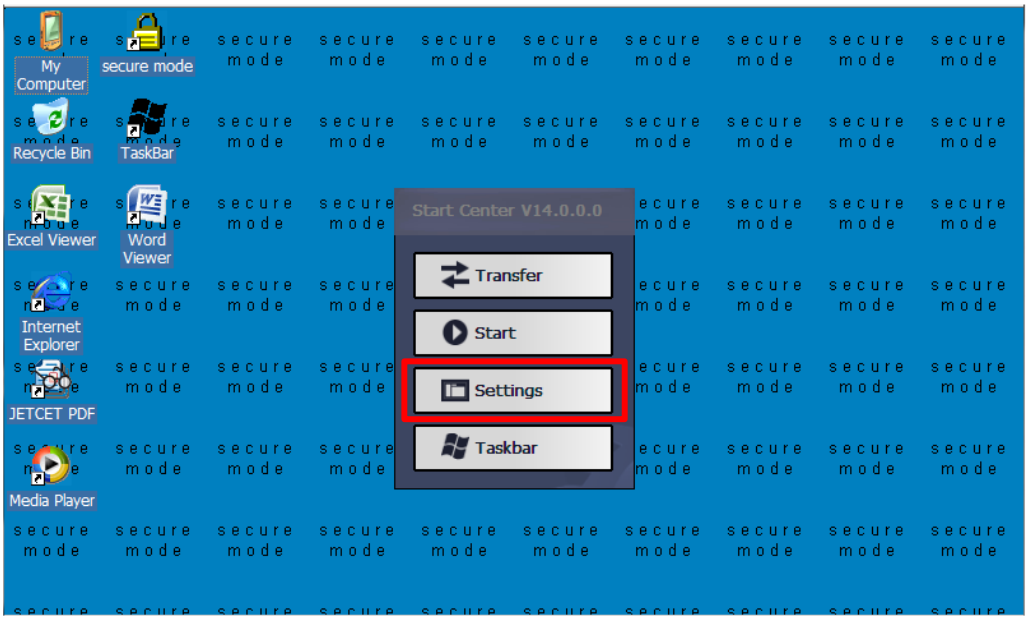
On occasions it may be necessary to access the Windows CE control panel to perform various maintenance or diagnostic functions.

Changing settings in the Windows CE control panel may render the Mentor display inoperable! Only access menus and settings as directed by Kinesys support personnel.

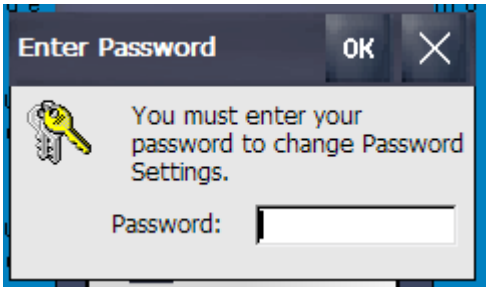
1. Select the tools menu by pressing
2. Touch “Exit Program”. If not already logged in, a user login with basic configuration rights will be required
3. Wait for the runtime operating system to close



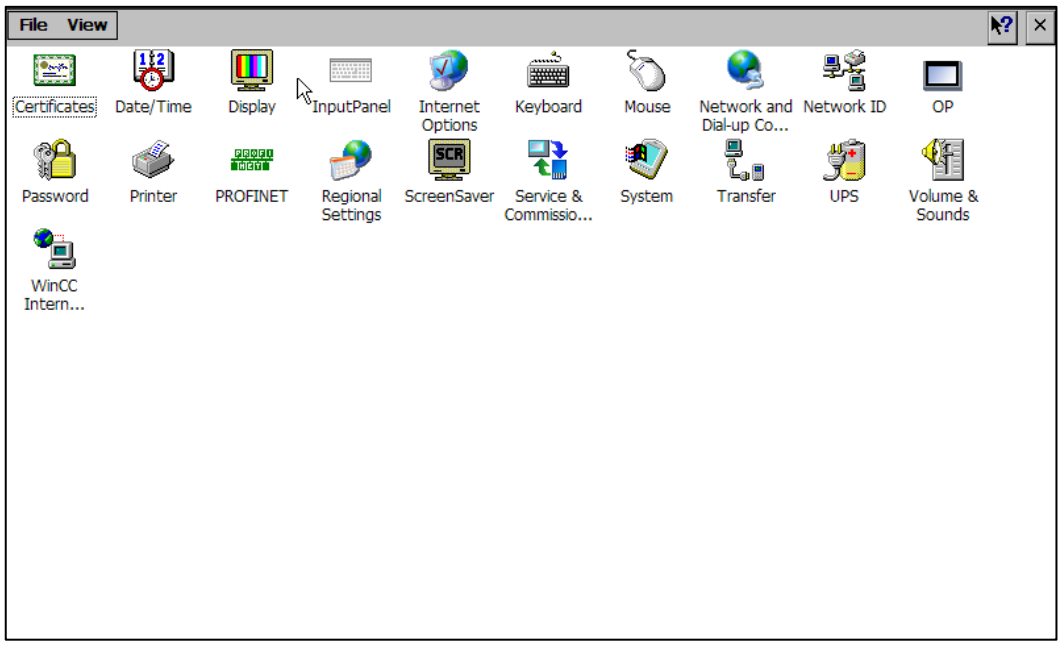
4. Click the “Settings” button



5. Enter the Windows Secure Mode password as advised by Kinesys

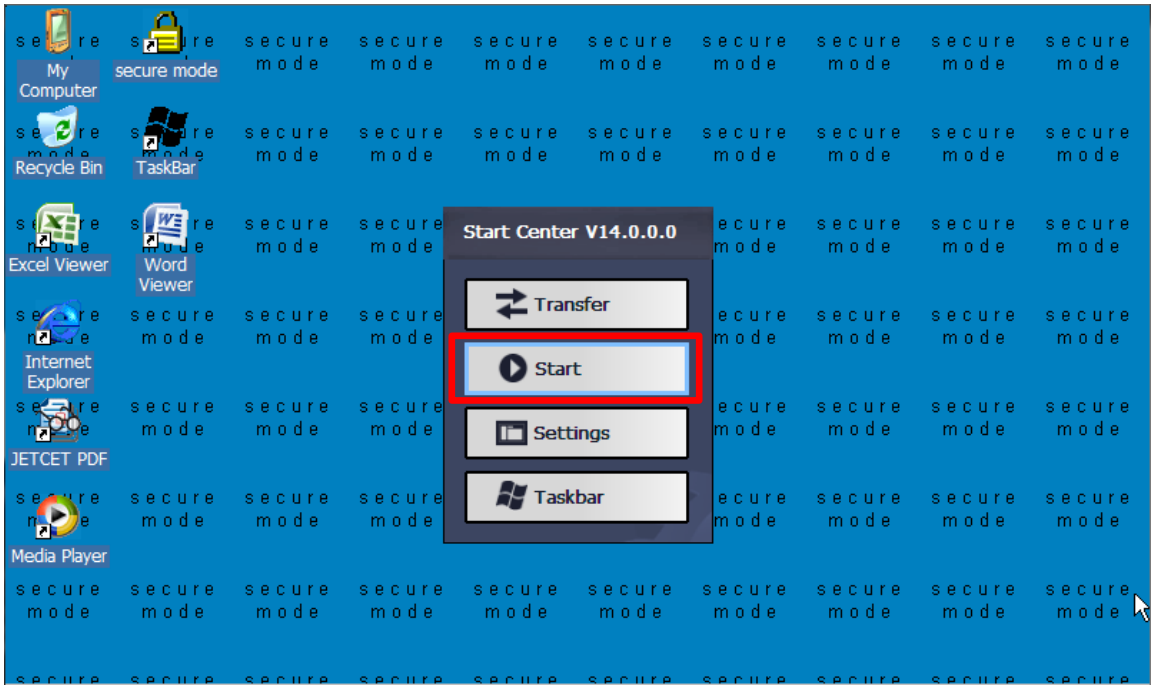


6. The control panel is displayed. Use the tools only as directed by Kinesys support personnel. Do not make any other changes as this may render the Mentor display inoperable.



7. When finished, close the control panel using the  button

8. Press the “Start” button on the Start Center to return to the Mentor display screens.



7.3.8 Spare parts

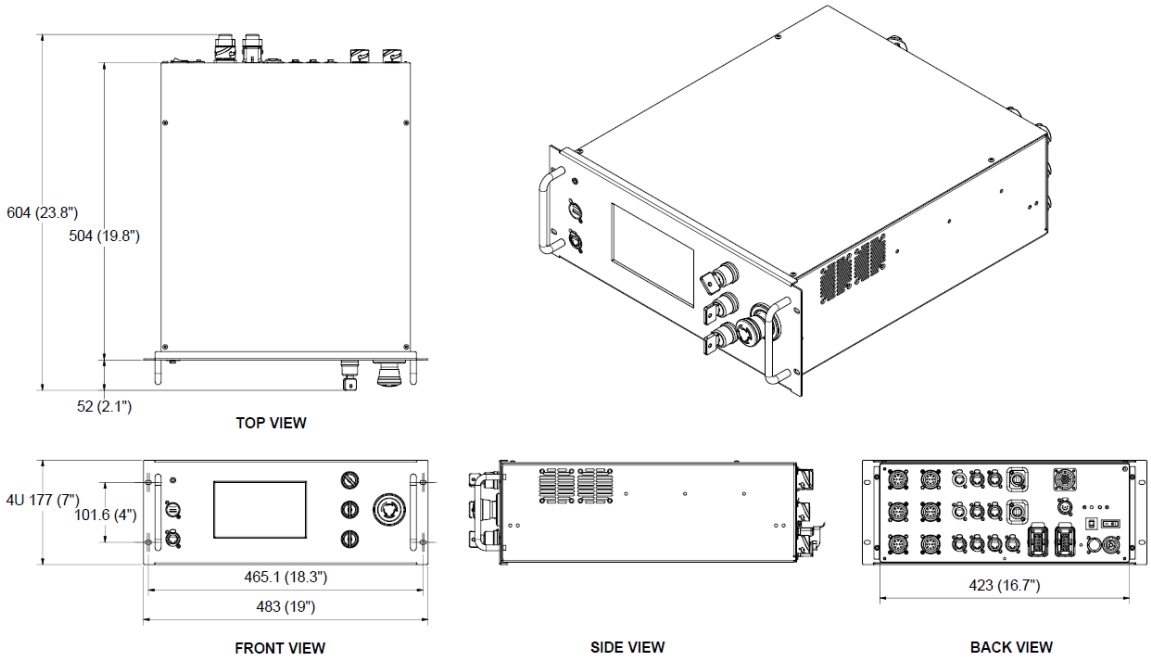
For continued service and long working life it is recommended to contact Kinesys or your local distributor to obtain original spare parts for your Mentor 401. See the spare parts list on page 58.

8 Technical Information

8.1 Specifications

Feature	Specification
Environmental	*Operating Temperature Range* - 5C to 40C *Storage & Transportation Temperature Range* - -25C to + 55C *Humidity* - RH <50% at maximum 40C *Altitude* - 1000m **For indoor use only!**
Mains power supply	85-264V 50-60Hz 130W Protected by 2A thermal magnetic circuit breaker
Enclosure	Steel enclosure, zinc plated finish Steel front panel, blue stove enamel finish Ingress Protection IP30
Cooling	Force air cooled (2 x internal DC fan) Air intakes at left side of enclosure Air exhausts to right side of enclosure
Dimensions	483mm x 177mm x 504mm (excluding handles, connectors, cabling and mounting hardware)
Weight	
Rack mounting	19” rack mount 4U x 500mm (19.6”) deep (excluding handles and connectors)
Maximum achievable safety level	SIL3 (according to EN 62061) PLe (according to EN 13849-1)

8.2 Dimensions



Mentor 401: Overall Dimensions

8.3 Declaration of Conformity

kinesys

CE

ORIGINAL

EC Declaration of Conformity

manufacturer: **Kinesys Projects Limited**
address: **Unit 2 Kempton Gate, Oldfield Road, Hampton, Middlesex. TW12 2AF**

in accordance with the following EC directives:

Low Voltage Directive 2014/35/EU
EMC Directive 2014/30/EU

declares that the products:
description: **Mentor M401 Safety Controller**
part numbers: **MEN-04-0010**

are in conformity with the applicable requirements of the following standards:

EN 60204-1	**Safety of machinery - Electrical equipment of machines -- Part 1: General requirements**
EN 62061	**Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems** Mentor M401 may be used in applications up to SIL3 in conjunction with suitable safety switches, operator controls, data distribution and output devices
EN 61000-6-1	**Electromagnetic compatibility (EMC). Generic standards. Immunity for residential, commercial and light-industrial environments**
EN 61000-6-3	**Electromagnetic compatibility (EMC). Generic standards. Emission standard for residential, commercial and light-industrial environments**

The manufacturer hereby declares that the products named above have been designed to comply with the relevant sections of the above referenced standards. The units comply with all applicable Essential Requirements of the Directives.

Equipment referred to in this Declaration of Conformity was first manufactured in 2017

A M Cave

Technical Director

Hampton, 17 May 2017

The attention of the specifier, purchaser, installer, or user is drawn to special measures and limitations to use which must be observed when these products are taken into service to maintain compliance with the above directives.

Details of these special measures and limitations to use are available on request, and are also contained in the product manuals.

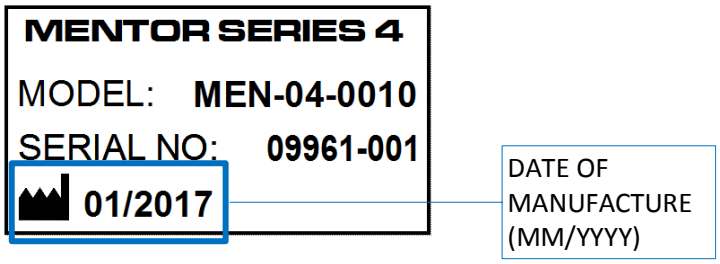
+44 (0)20 8481 9850 kinesys.co.uk info@kinesys.co.uk Kinesys, Unit 2 Kempton Gate, Oldfield Road, Hampton, Middlesex, TW12 2AF, UK

Kinesys Projects Ltd, Registered in England & Wales No. 04620583 **Registered Office** as above **VAT Number** GB 805 2763 38

8.4 Service Life (Mission Time)

The safety system is designed based on a service life (“proof test interval” according to EN 62061; “mission time” according to EN 13849-1) of 20 years from the date of manufacture. After this time the safety related parts of the control system must be replaced.

The system manufacturing date is shown on the serial number label on the rear panel above the mains input connector. Mentor must be taken out of service and the safety related elements of the control system replaced no later than 20 years after the date of manufacture.



8.5 End of Life

In the event of a product reaching the end of its usable service life or being considered beyond economic repair it should be disposed of with care and in line with local legislation on the disposal of Waste Electrical and Electronic Equipment (WEEE).

In Europe WEEE shall be disposed of in accordance with European Union Directive 2012/19/EU.

In most regions of the world similar legislation exists to ensure that WEEE is handled separately to maximise reuse of materials and avoidance of landfill.

8.6 Spare parts

The following table shows common spare parts and accessories for the Mentor 401. This is not an exhaustive list. Please contact Kinesys, or your local distributor for any component that is not listed.

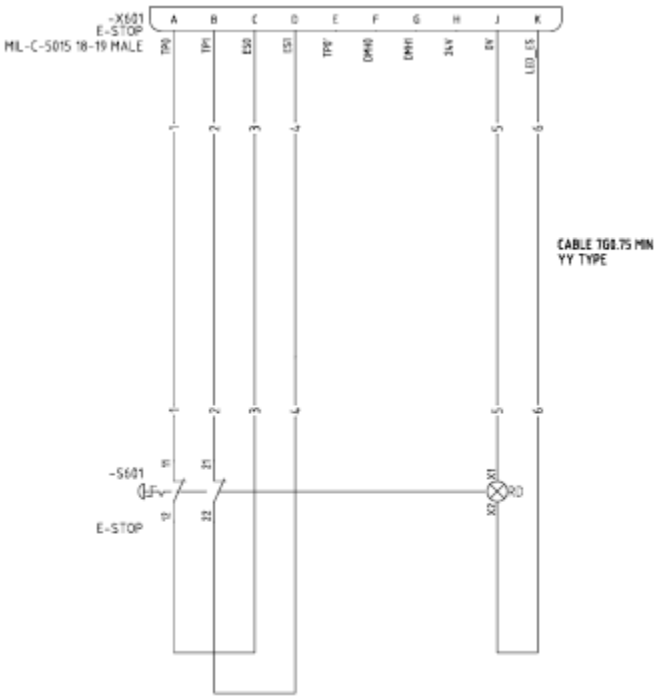
Item	Kinesys Part number
Reset key, yellow, OMR 73033	5303099
Configuration key, black, OMR 73034	5303098
Maintenance key, blue, OMR 73038	5303096
Slide rail kit, Accuride 3307 20”	
Power cable, powerCON TRUE1 – bare ends, 2m	
E-stop input shorting plug	MEN-98-2010
Console input shorting plug	MEN-98-2020
Universal device interface shorting plug	MEN-98-2040

Table 1 Mentor 401 spare parts

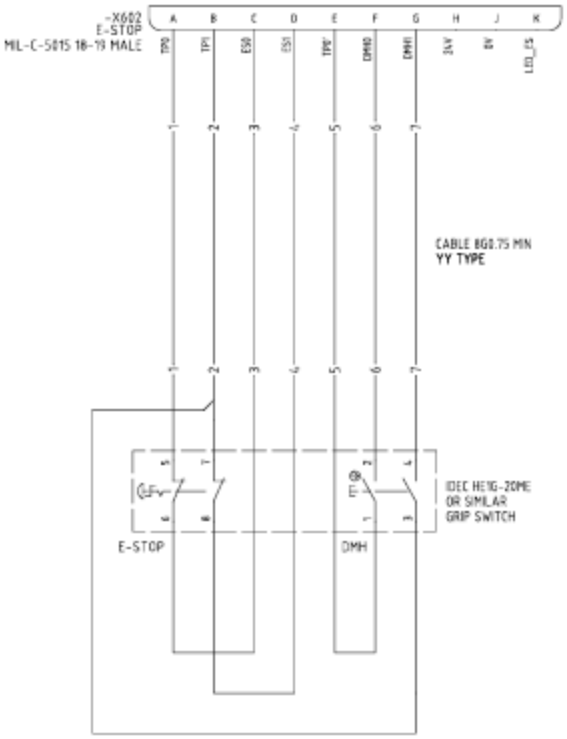
9 Appendix A: Schematic Diagrams

9.1 Example Device Schematics

9.1.1 Emergency Stop Switch

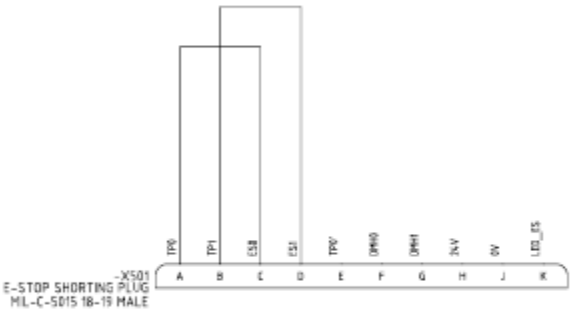


9.1.2 Emergency Stop Switch / Dead Man's Handle

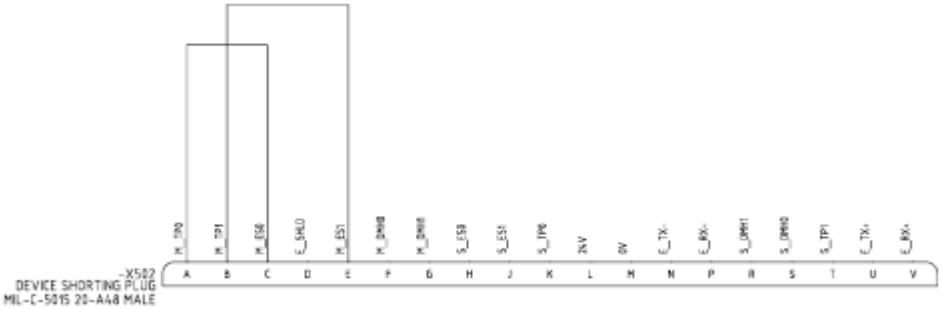


9.2 Shorting Plug Schematics

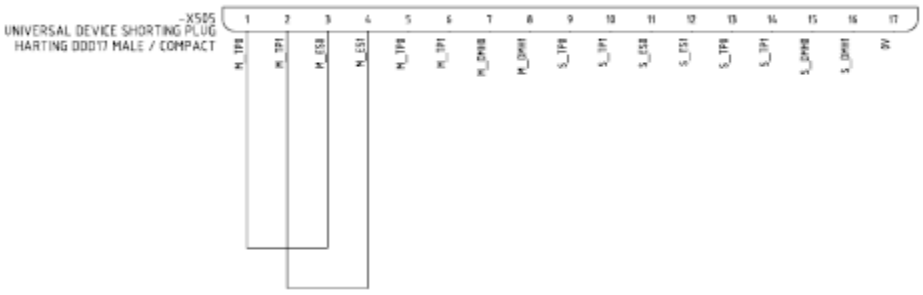
9.2.1 Emergency Stop Shorting Plug



9.2.2 Console / Pendant Input Shorting Plug

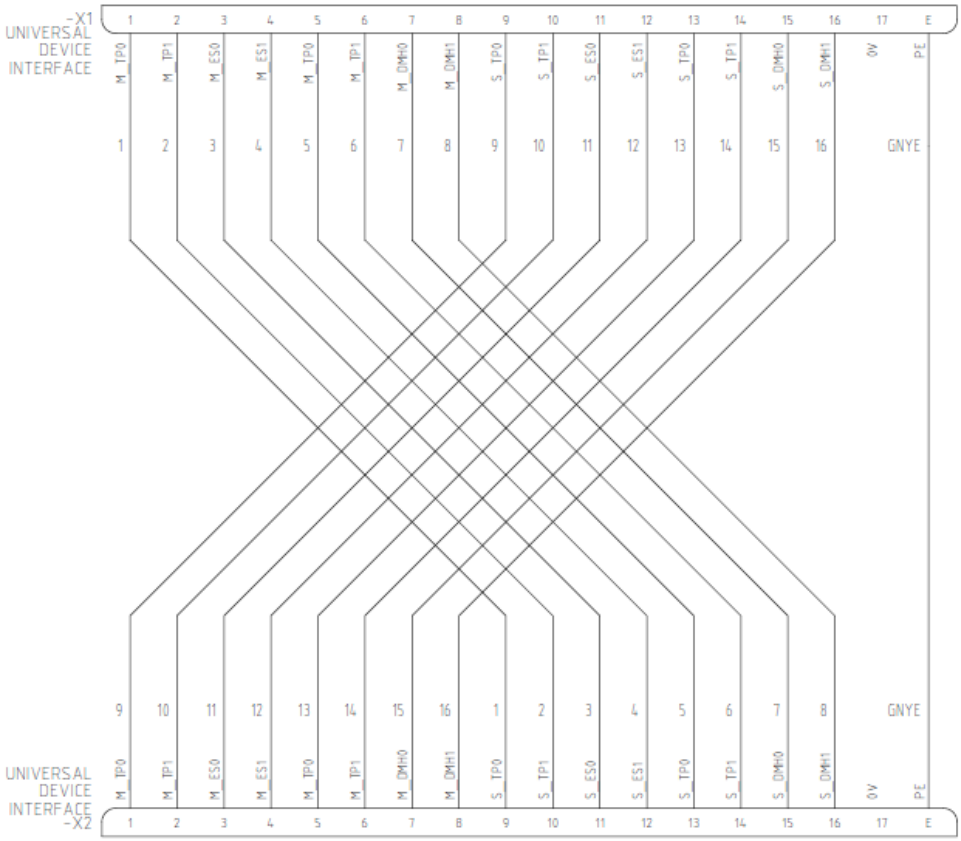


9.2.3 Universal Device Interface Shorting Plug



9.3 Interconnecting Cables

9.3.1 UDI-UDI Link Cable for Master-Slave Operation



10 Appendix B: Safety Performance Achievable with Array PD-ES Systems

The safety connections of Elevation 1+ systems using Array PD-ES distribution may be connected to the Universal Device Interface connectors on the Mentor 401 using Kinesys cable assembly MEN-98-2130. Where motion data uses the same network as that connected to the Mentor an additional Ethernet connection must be made between one of the Mentor Ethernet sockets and the Ethernet connection on the Array PD-ES

The Array PDES contains a safety relay and mains line contactor(s) which control the power output to Elevation 1+ controllers, providing a Category 0 stop according to EN 60204-1:2006 – "a stopping by immediate removal of power to the machine actuators". In addition, the line contactor and the drive enable signal in the Elevation 1+ controller are switched off via control lines in the Elevation data cable.

The line contactor(s) in the Array PDES are monitored to prevent restarting of the system in the event of a fault; the control lines to the Elevation 1+ controller are not monitored, and a fault in these control circuits may lead to a loss of the safety function within the Elevation 1+ controller. To provide an increased level of safety dual line contactors are fitted to some Array PDES units.

All Array PDES distribution systems manufactured after August 2014 are fitted with dual mains contactors, units manufactured prior to this date may be modified by Kinesys as required. Units conforming to the new standard (dual contactors) are identified by the following:

A label on the front panel stating "EN 13849 CAT4 DUAL LINE CONTACTORS"

A label on the rear panel stating "EN 13849 CAT4 DUAL LINE CONTACTORS"

The presence of two contactors inside the unit – type LC1D80 identified as –KM1 and –KM3

The following table describes the emergency stop system safety performance which can be achieved with various configurations of Array PDES systems:

SYSTEM	SIL (According to EN 62061)	PL (According to EN 13849)
Array PDES – SINGLE CONTACTOR – all operation modes	SIL 1	PLc
Single Array PDES – DUAL CONTACTOR – with up to 2 additional external e-stop devices and front panel e-stop switch	SIL2	PLd
Single Array PDES – DUAL CONTACTOR – with one external e-stop device only, front panel e-stop covered*	SIL3	PLe
Array PDES – DUAL CONTACTOR – linked systems	SIL1	PLc
Array PDES – DUAL CONTACTOR – with Mentor master controller (multiple Array PDES if required)*	**SIL3**	**PLe**

* For SIL3 operation the emergency stop switch(es) on the Array PDES must be securely covered to prevent operation. Where a single stop switch only is connected this must be located adjacent to the system operator. Where multiple emergency stop switches are required all emergency stop switches must be connected to the inputs of a Mentor safety controller. An additional emergency stop switch may need to be connected to the Mentor in the vicinity of the Array PDES if required by the system risk assessment.

Note that the statement above applies only to full-size Array PDES with Powerlock or Camlok mains input, and not to Mini Array PDES (“Ceeform” input)

All emergency stop switches should be tested after each installation of a touring system, and regularly for a fixed installation.

The number of emergency stop switches and their location, and any additional safety requirements, must be determined following a risk assessment of the system to be controlled.

11 Appendix C: Using Sm@rtClient to View the Mentor Screen Remotely

Sm@rtClient allows the Mentor display screen to be viewed and operated on a desktop PC connected to the automation network.

11.1 Setting the PC IP Address

Your PC must have an IP address in the 10.0.0.0 / 8 subnet to connect to Mentor. An IP address structured as follows will not clash with any Kinesys equipment:

IP Address: **10.*x*.0.*y*** Subnet Mask: **255.0.0.0**
where *x* = 5 .. 10
where *y* = 1 .. 253

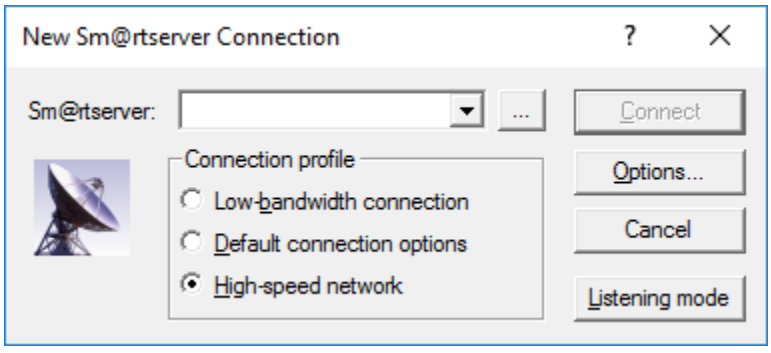
11.2 Installing Sm@rtClient

1. Download the Sm@rtClient application from the link supplied by Kinesys

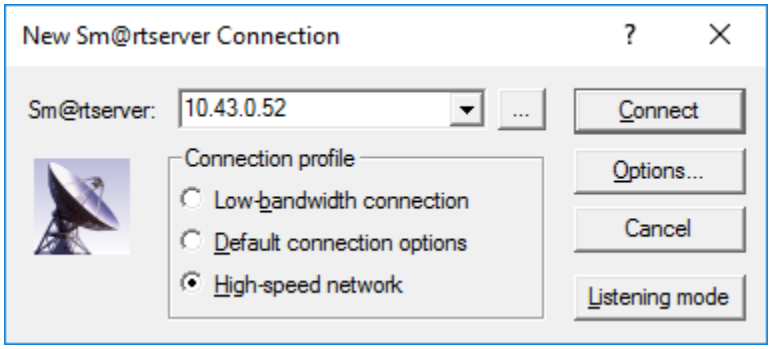
2. Copy the Sm@rtClient application to a folder on your PC hard disk, for example C:\Program Files (x86)\Kinesys. Create a shortcut to the program in the start menu or on the taskbar as required.

11.3 Connecting to the Mentor

1. Run the Sm@rtclient program. The “New Sm@rtserver Connection” dialog is opened.

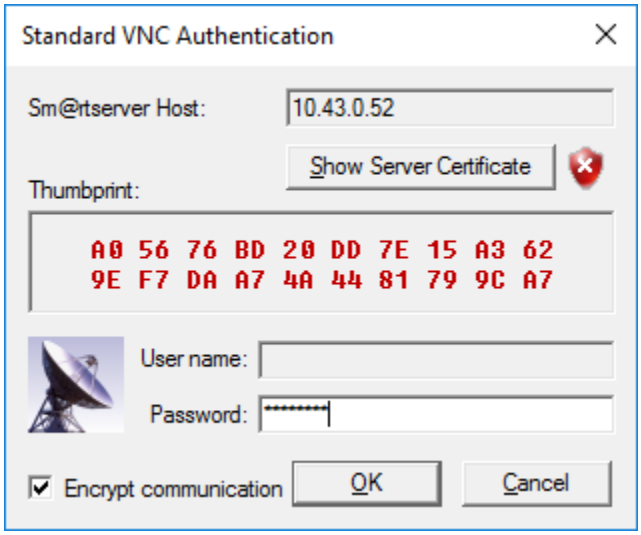


2. Enter the IP address of the Mentor display. This is in the format 10.43.0XX.0YY where XXYY are the last digits of the Mentor serial number, for instance serial number 09961-1234 will have an IP address of 10.43.12.34

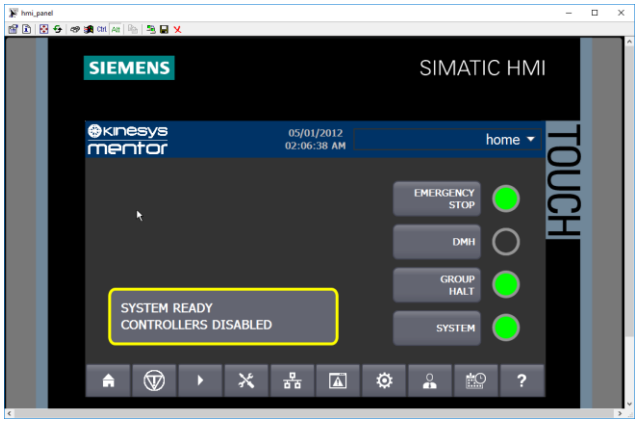


3. Press the “Connect” button to connect to the Mentor display

4. Enter the password in the authentication dialog. The User name should be left blank. Passwords are case sensitive.



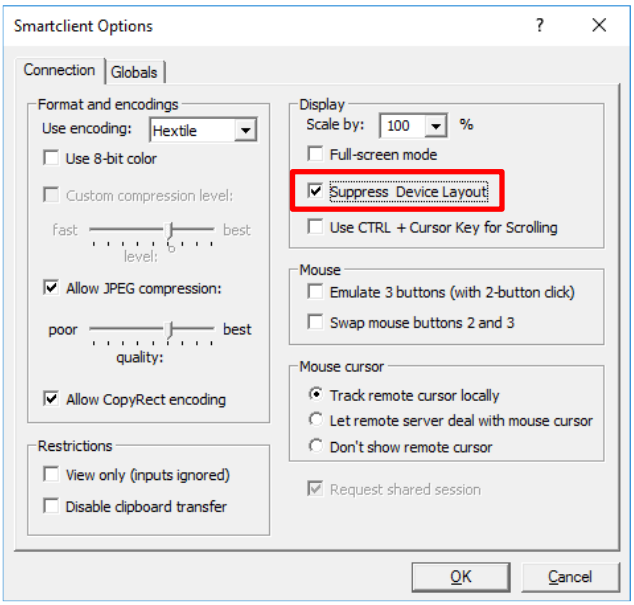
5. Press “OK” to log in. The Mentor display screen will be shown in a desktop window.

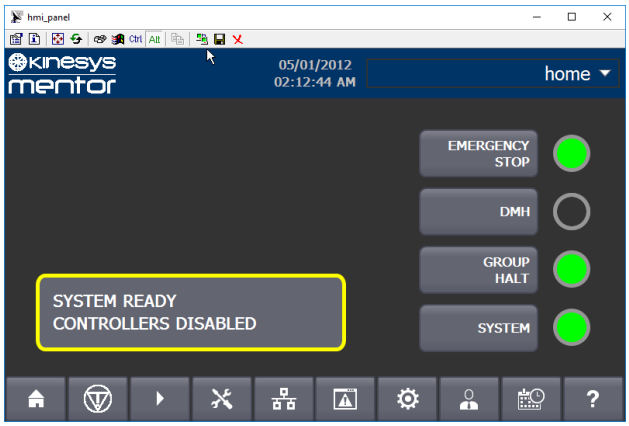


6. The mouse can be used to navigate the touch buttons.

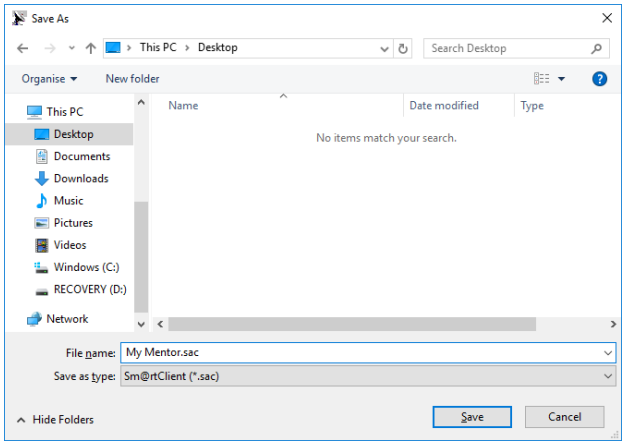
7. Press the “Connection Options” button  to open the options dialog.

8. Check the “Suppress Device Layout” box to hide the display frame and reduce the window size

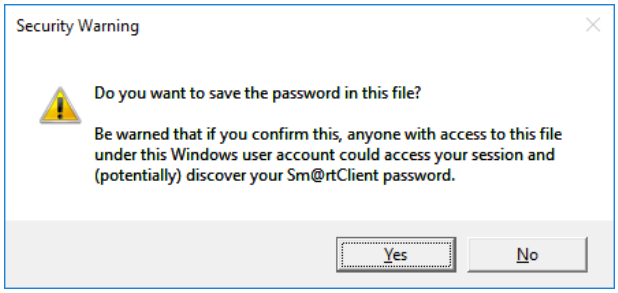




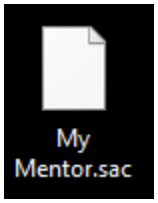
9. Click the “Save connection info as …” button  to save the connection data as a shortcut.



10. You may also save the connection password with the shortcut by clicking “Yes” in the security confirmation dialog. Observe the security warning.



11. The Sm@rtClient session may now be opened and logged in just by double-clicking the new shortcut.



12 Appendix D: Updating Mentor Program and Firmware

The Mentor program and firmware are updated using the Simatic Automation Tool, available from Kinesys Support. The Simatic Automation tool is used in the unlicensed mode so no license key is required.

Version 3.1.0.0 or later of the SIMATIC automation tool is required to upgrade the Mentor safety PLC.

CAUTION!
File operations involving the SIMATIC Automation Tool will place the Mentor PLC into STOP mode and will place any connected devices into a emergency stop / disabled state. Do not perform any file operations using the SIMATIC Automation Tool until all devices have been disconnected and are in a safe, disabled state.

CAUTION!
Interrupted file operations may leave Mentor in an unusable state. Ensure that Mentor is connected to a secure power supply before commencing any update or restore operations.

12.1 Installing the Simatic Automation Tool

12.1.1 System Requirements

- Windows 64-bit operating system
  - Windows 7 Home Premium SP1
  - Windows 7 Professional SP1
  - Windows 7 Ultimate SP1
  - Windows 10 Home Version 1607 or later
  - Windows 10 Pro Version 1607 or later
- 1.4GB free space on drive C:\ for system files
- Ethernet adapter for connection to Mentor
  The Ethernet adapter should have an IP address in the 10.5.0.x range with a subnet mask of 255.0.0.0

Software installation requires an account with administrator privileges

12.1.2 Installation

Save all your work in progress and close all applications before installing the SIMATIC Automation Tool.

Click on “Start.exe” in the SIMATIC automation tool folder to start the installation. Accept the default settings throughout the installation wizard. You may be prompted to restart your computer before and after installation.

12.1.3 Installation rules

You can only install one version of the SIMATIC Automation Tool on a PC. If you have installed a previous version, you must uninstall it first. The installation executable checks for a previous installation, and responds as follows:

- If no version of SIMATIC Automation Tool is found, the installation can proceed.
- If a version older than V3.0 of the SIMATIC Automation Tool is found, the setup informs you that you must uninstall the older version. The setup guides you through uninstalling the older version. You cannot proceed with the installation until you close and restart the installation.
- If version 3.0 is found, the installation process uninstalls the V3.0 version and installs V3.1.
- If an existing current version V3.1 of the SIMATIC Automation Tool is found, the setup presents options to modify/upgrade, repair, or uninstall the previous installation.

12.2 Starting the SIMATIC Automation Tool

Use one of the following methods to start the SIMATIC Automation Tool:

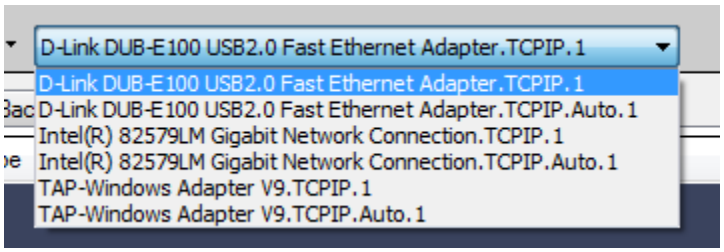
- Double-click the SIMATIC Automation Tool shortcut icon on your desktop.
- Use the Windows Start button:

– Click the Windows start button and "All Programs".

– Click the "Siemens Automation" folder, then the "SIMATIC Automation Tool" folder, and finally "SIMATIC Automation Tool".

12.2.1 Selecting the Network Interface

Before operations can commence you must select the network interface to which the Mentor is connected. Click the Network Interface card dropdown list in the toolbar and select the network interface connected to the Mentor.

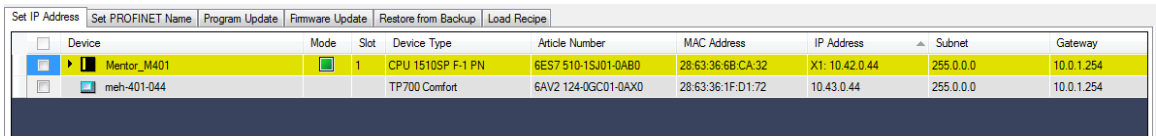


Always choose the device name without ".Auto". Note that the network interface will need a unique IP address in the 10.0.0.0 / 8 subnet.

12.2.2 Scan the Network

To scan the network, select the "Operations>Scan Network>Scan Entire Network" menu command. Alternatively, you can click the Scan button on the toolbar  and select "Scan Entire Network" from the button drop-down menu.

The network is scanned and at least two devices should be reported in the device table.



12.3 Backing up the Mentor Data

CAUTION!
File operations involving the SIMATIC Automation Tool will place the Mentor PLC into STOP mode and will place any connected devices into a emergency stop / disabled state. Do not perform any file operations using the SIMATIC Automation Tool until all devices have been disconnected and are in a safe, disabled state.

CAUTION!
Interrupted file operations may leave Mentor in an unusable state. Ensure that Mentor is connected to a secure power supply before commencing any update or restore operations.

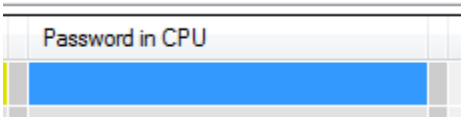
Taking a backup of the existing Mentor configuration will allow you to restore current operation should the software upgrade fail for any reason.

Two separate backups must be taken, one for the Mentor PLC (shown with the  icon in the device table) and one for the Mentor display (shown with the  icon).

To create a backup, follow the following steps:

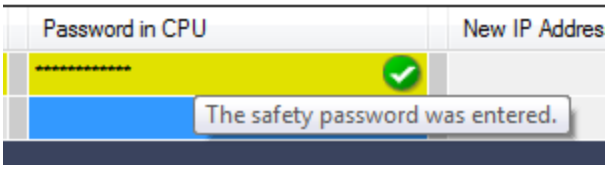
1. Select the Mentor PLC

2. Enter the PLC password in the “Password in CPU” field and click Enter.



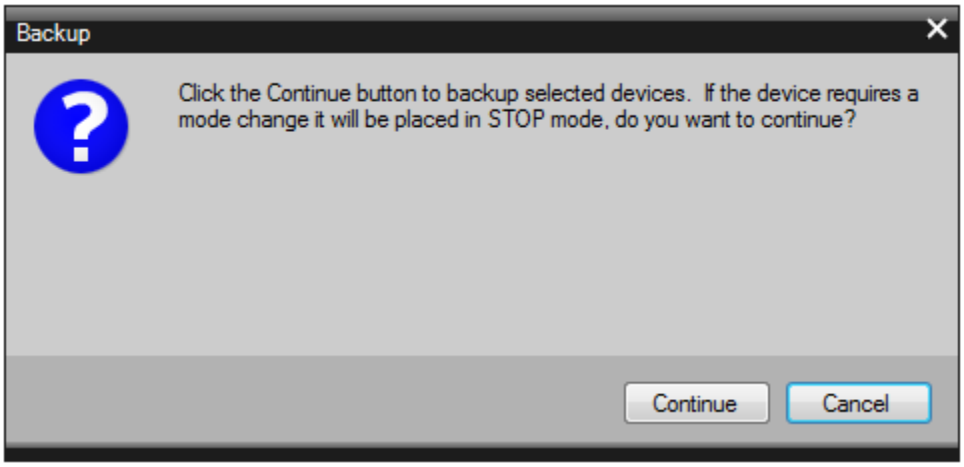
The password will be checked against the PLC password. A valid password, including access to the safety program, will be indicated by a green tick and a yellow highlight on the password dialog box. If a

password entry is valid, you can hover your mouse cursor over the password field to display a tool tip that shows the access level.

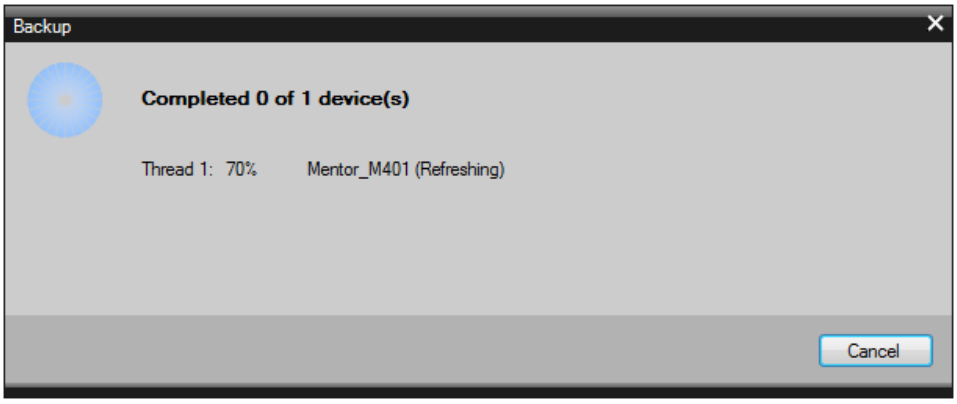


3. Select the "Backup/Restore > Backup Device to File" menu command from the Operations menu. Alternatively, click the Backup/Restore toolbar button  and select "Backup Device to File" from the button drop-down menu.

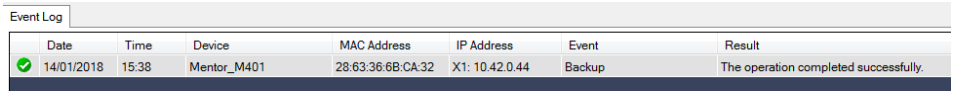
4. Click “Continue”. The Mentor PLC will be stopped and all connected devices will be placed into an emergency stop / disabled state.



5. The PLC contents will be backed up to the local hard drive.



Once finished, the Event Log window at the bottom of the screen will indicate a successful backup.



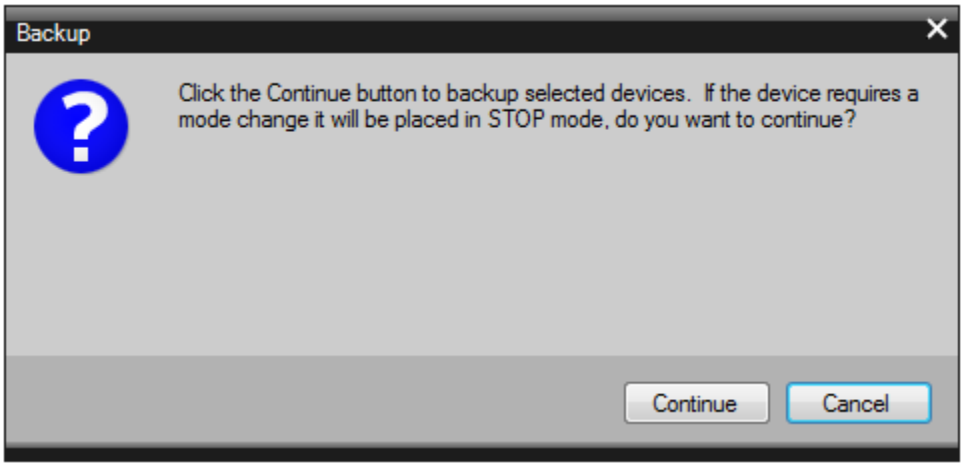
6. The PLC will remain in the Stop state after the backup is completed.

   Click the RUN mode button on the toolbar  and then click “Continue” or use the ”Start PLC” button on the Tools menu on the Mentor display to re-start the PLC.

7. De-select the Mentor PLC and select the Mentor display

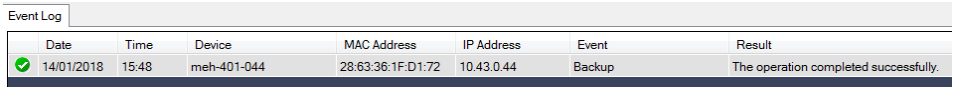
8. Select the "Backup/Restore > Backup Device to File" menu command from the Operations menu. Alternatively, click the Backup/Restore toolbar button  and select "Backup Device to File" from the button drop-down menu.

9. Click Continue. The Mentor display will exit to Windows and the contents will be automatically backed up to the local hard drive.

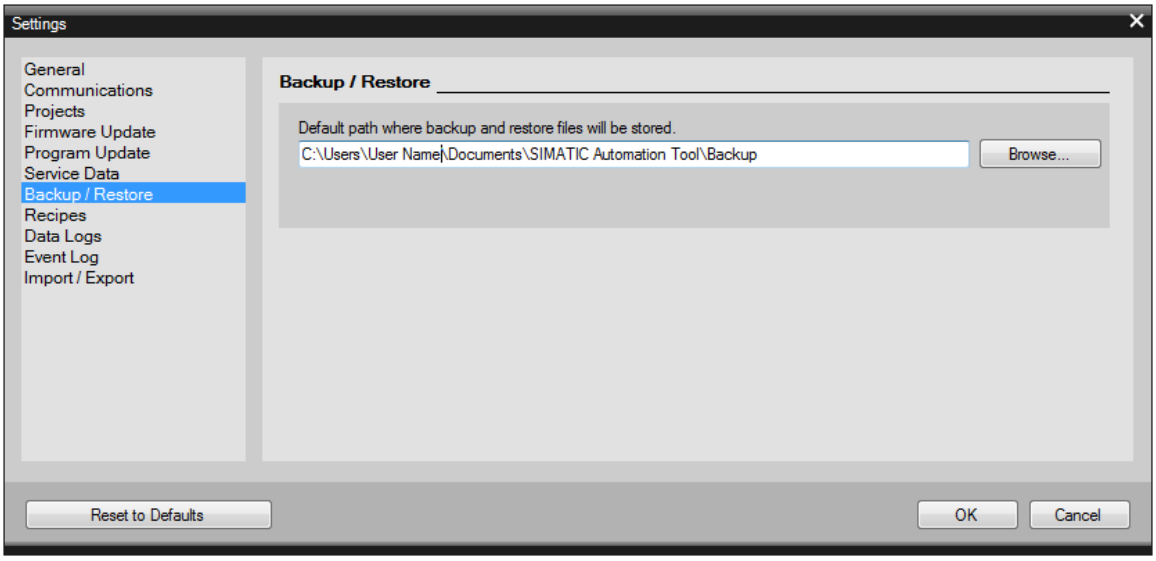


10. The HMI backup procedure may take several minutes to complete.

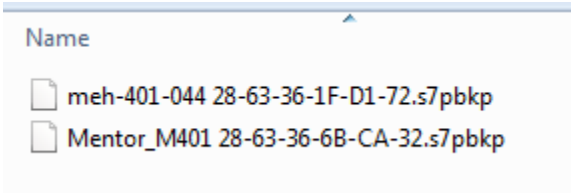
11. Once finished, the Event Log window at the bottom of the screen will indicate a successful backup.



Backups will be stored in the Backup and Restore folder, normally C:\Users\{UserName}\Documents\SIMATIC Automation Tool\Backup. The location of the Backup and Restore folder can be checked using the |Options |Settings menu and selecting the “Backup / Restore” option from the menu tree



The backup files will be identified by the device name and MAC address.



12.4 Updating the Mentor PLC Firmware

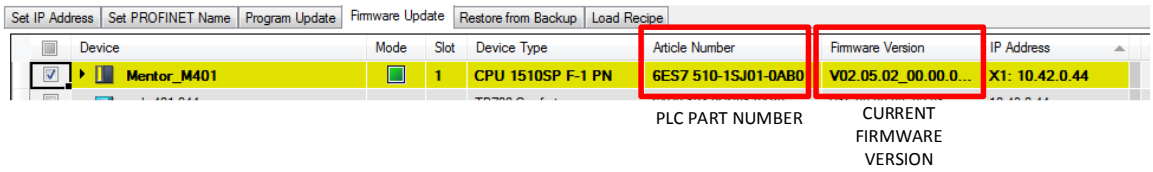
CAUTION!
File operations involving the SIMATIC Automation Tool will place the Mentor PLC into STOP mode and will place any connected devices into a emergency stop / disabled state. Do not perform any file operations using the SIMATIC Automation Tool until all devices have been disconnected and are in a safe, disabled state.

CAUTION!
Interrupted file operations may leave Mentor in an unusable state. Ensure that Mentor is connected to a secure power supply before commencing any update or restore operations.

New program features may require a PLC firmware update to function correctly. The minimum firmware version required will be advised when the PLC program update is made available. If necessary, request a firmware update file from Kinesys and follow the steps below to update the PLC firmware.

12.4.1 Checking the Current Firmware Version

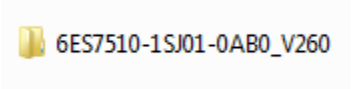
Scan the network as described in section 12.2.2. Select the Mentor PLC and click on the "Firmware Update" tab. The current firmware version and PLC part number are displayed as shown below.



12.4.2 Installing the New Firmware File

If the firmware needs to be updated request a firmware file from Kinesys support, advising the Mentor serial number, PLC part number and current firmware version.

The firmware will be supplied in a ZIP archive containing a single top level folder



The folder name will include the PLC part number and the new firmware version number in the form *{PLC PART NUMBER}_{VERSION}.*

1. Extract the contents of the folder to your computer's hard drive.

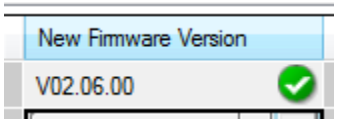
2. In the SIMATIC Automation Tool click the "…" icon on the Mentor PLC line in the "New Firmware Version" column

3. Browse to the folder where the extracted firmware files are located and open the “6ES7510-…” top level folder

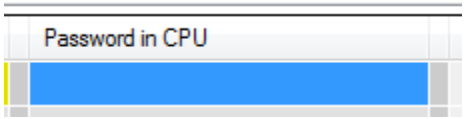
4. Open the “FWUPDATE.S7S” folder

5. Check that the file ending “.upd” matches the PLC part number and is the correct firmware version; select the file and press “Open”

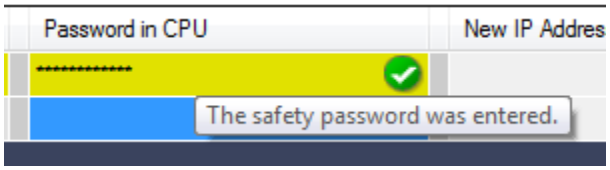
6. The firmware file is verified and loaded into the SIMATIC Automation Tool



7. Enter the PLC password in the “Password in CPU” field and click Enter.

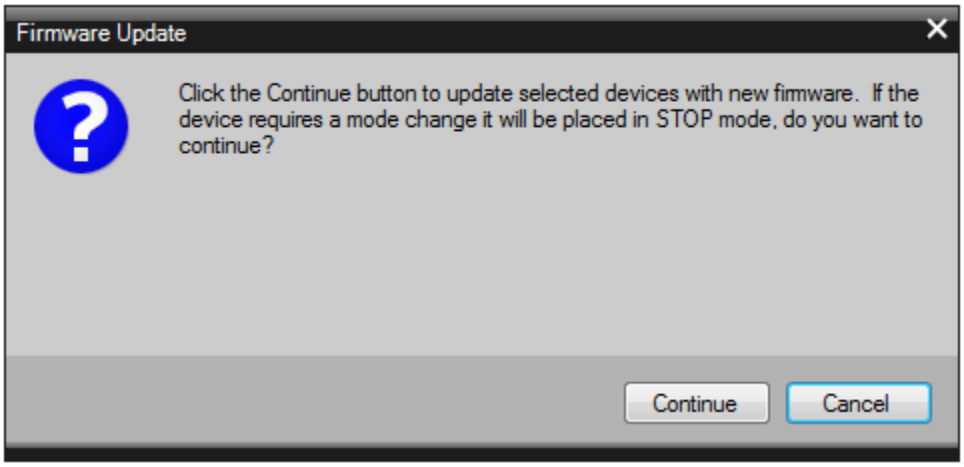


The password will be checked against the PLC password. A valid password, including access to the safety area of the PLC, will be indicated by a green tick and a yellow highlight on the password dialog box. If a password entry is valid, you can hover your mouse cursor over the password field to display a tool tip that shows the access level.

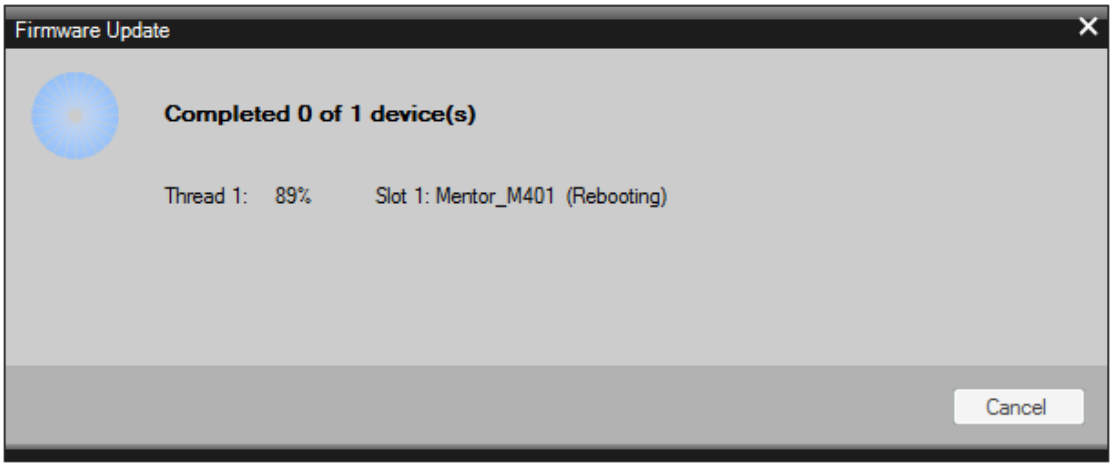


8. Once all the information has been entered select the "Operations > Update > Firmware Update" menu command to start the operation. Alternatively select the Update toolbar button  and select "Firmware Update" from the button drop-down menu.

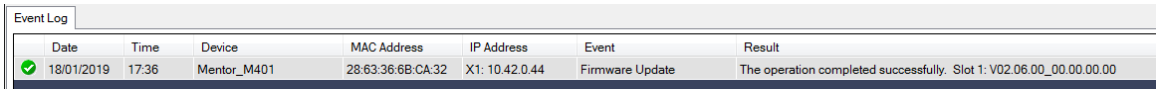
9. Click “Continue”. The Mentor PLC will be stopped and any connected devices will be placed into an emergency stop / disabled state.



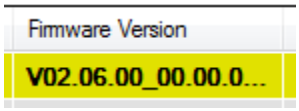
10. The PLC firmware is updated. The firmware update will take several minutes.



11. When the operation is complete the Event Log below the device table shows the results of this operation.



12. The device table will be updated showing the new firmware version.



13. The PLC will remain in the Stop state after the firmware update is completed.

    Click the RUN mode button on the toolbar  and then click “Continue” or use the ”Start PLC” button on the Tools menu on the Mentor display to re-start the PLC.

12.5 **Updating the Mentor PLC Program**

CAUTION!
File operations involving the SIMATIC Automation Tool will place the Mentor PLC into STOP mode and will place any connected devices into a emergency stop / disabled state. Do not perform any file operations using the SIMATIC Automation Tool until all devices have been disconnected and are in a safe, disabled state.

CAUTION!
Interrupted file operations may leave Mentor in an unusable state. Ensure that Mentor is connected to a secure power supply before commencing any update or restore operations.

The Mentor PLC program update will be supplied in a ZIP archive named as follows:

`M401_PLC-rel018_ser044_11101-11160.zip`

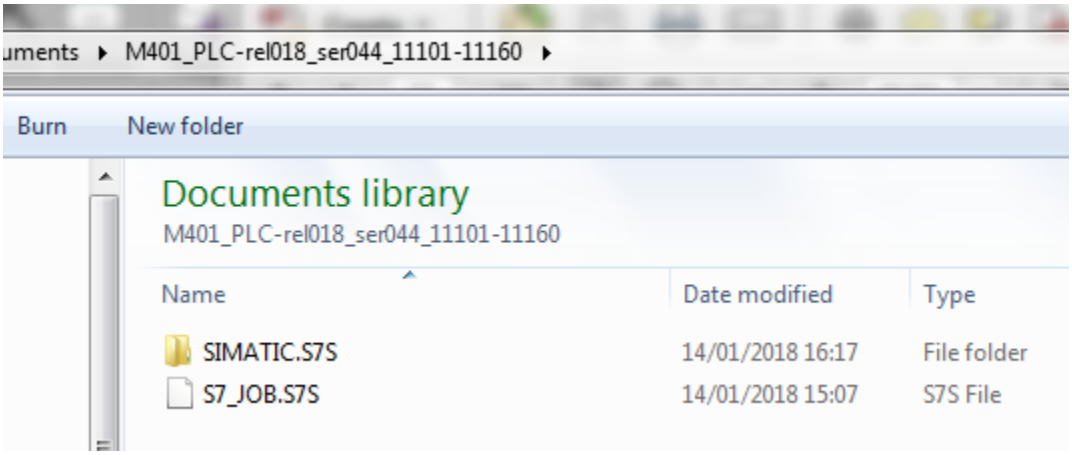
`M401_PLC` = Mentor 401 PLC program
`rel018` = release version number
`ser044` = Mentor serial number
`11101-11160` = device address range

Check the serial number in the received update file matches the serial number of the Mentor to be upgraded. Use of an upgrade file with the wrong serial number will render the Mentor inoperable.

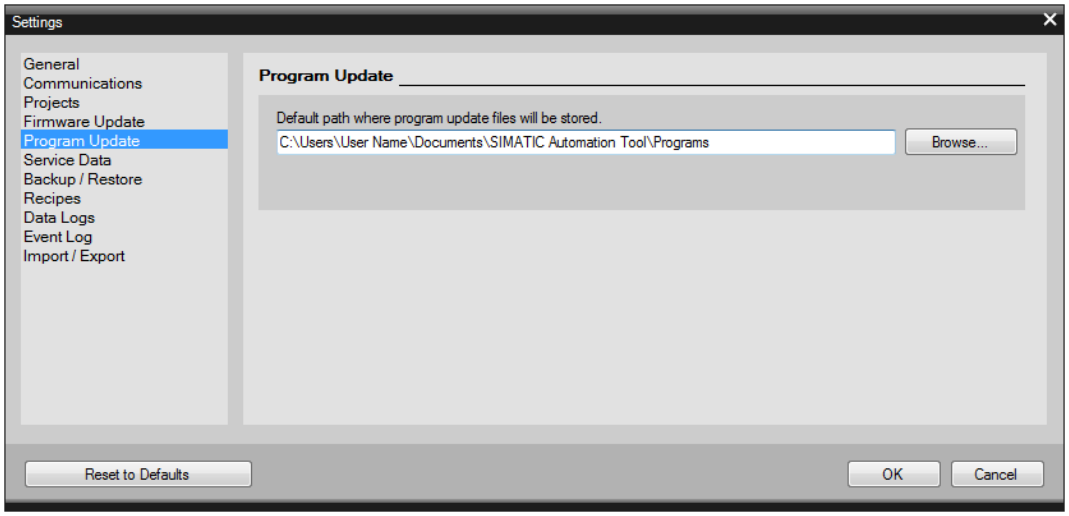
Backup the existing Mentor configuration as described in section 12.3 before installing the new program.

Follow the following steps to make the PLC program update accessible to the SIMATIC automation tool:

1. Use Windows Explorer to extract the ZIP archive to a folder of the same name by right-clicking the ZIP file and selecting “Extract All…”. The result will be a master update folder containing a SIMATIC.S7S folder and a S7_JOB.S7S file. Do not edit or rename any files or folders within the master update folder.

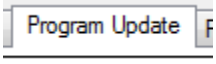


2. Copy or move the resulting folder, together with all its contents, to the SIMATIC Automation Tool Program Update folder, normally C:\Users\{UserName}\Documents\SIMATIC Automation Tool\Programs. The location of the Program Update folder can be determined using the |Options |Settings menu and selecting the “Program Update” option from the menu tree



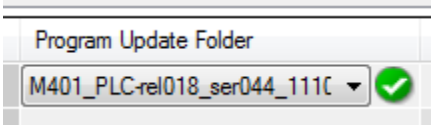
Once the program update has been transferred to the SIMATIC Automation Tool folder, follow the following steps to update the program in the PLC:

1. Click the “Program Update” tab

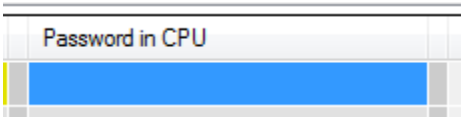


2. Select the Mentor PLC

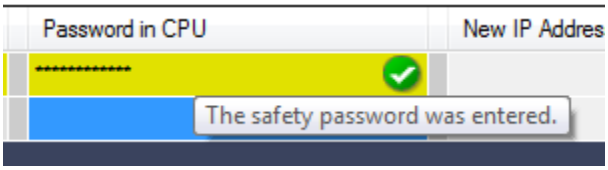
3. Use the "Program Update Folder" column drop-down list to select a folder name. The drop-down list shows the folders that you created in the program update path. You can also use the browse button and navigate to the folder where you have stored a program on your PC.



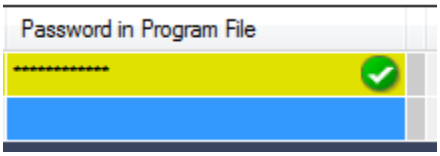
4. Enter the PLC password in the “Password in CPU” field and click Enter.



The password will be checked against the PLC password. A valid password, including access to the safety program, will be indicated by a green tick and a yellow highlight on the password dialog box. If a password entry is valid, you can hover your mouse cursor over the password field to display a tool tip that shows the access level.

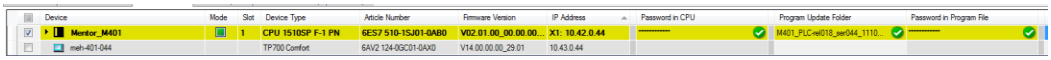


5. Enter the program password in the “Password in Program File” column and click Enter. (The program password may be the same as the PLC password, but it must still be entered again in the Program password dialog box). A valid password will be indicated by a green tick and a yellow highlight on the password dialog box.

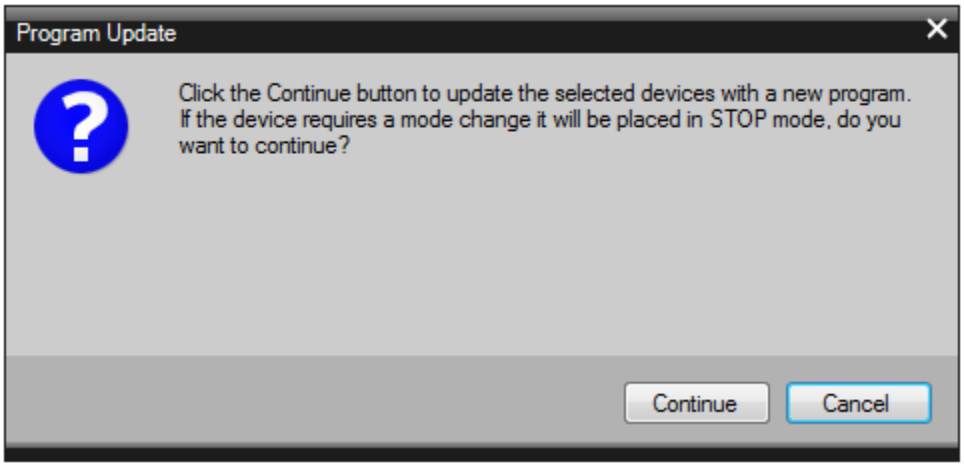


6. Once all the information has been entered select the "Operations > Update > Program Update" menu command to start the operation.

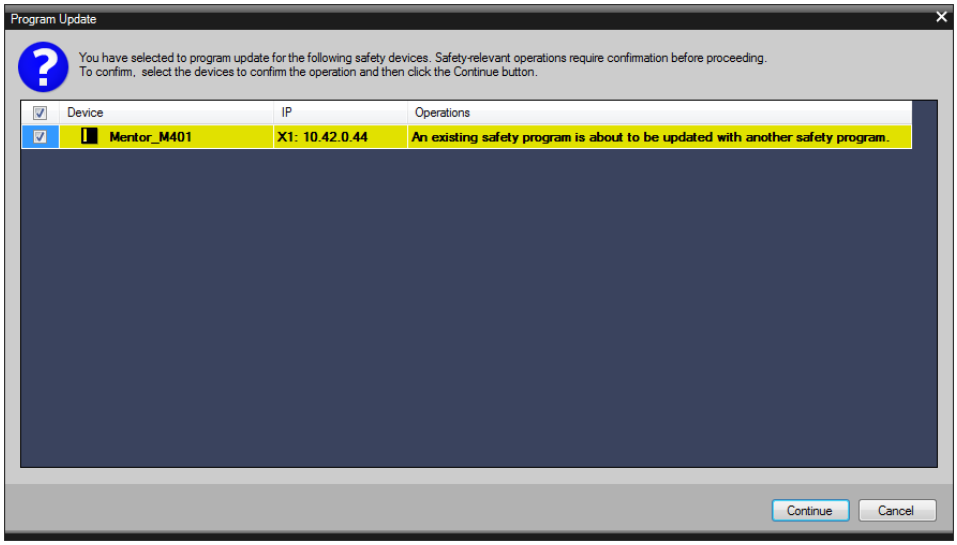
Alternatively select the Update toolbar button  and select "Program Update" from the button drop-down menu.



7. Click “Continue”. The Mentor PLC will be stopped and any connected devices will be placed into an emergency stop / disabled state.

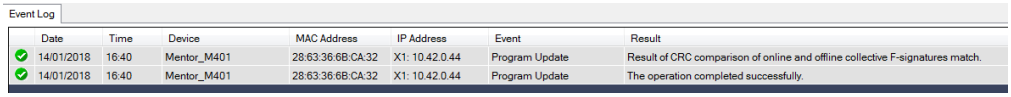


8. An additional confirmation dialog is presented to confirm an update of the safety system. Confirm that the correct Mentor device is shown, select the device and click “Continue”



9. The PLC program is updated.

10. The Event Log below the device table shows the results of this operation.



11. The PLC will remain in the Stop state after the program update is completed. Click the RUN mode button on the toolbar  and then click “Continue” or use the ”Start PLC” button on the Tools menu on the Mentor display to re-start the PLC.

12. Verify the program version and safety program checksum on the Help menu on the Mentor display.

12.6 **Updating the Mentor Display Program**

CAUTION!
File operations involving the SIMATIC Automation Tool will place the Mentor PLC into STOP mode and will place any connected devices into a emergency stop / disabled state. Do not perform any file operations using the SIMATIC Automation Tool until all devices have been disconnected and are in a safe, disabled state.

CAUTION!
Interrupted file operations may leave Mentor in an unusable state. Ensure that Mentor is connected to a secure power supply before commencing any update or restore operations.

The Mentor HMI (display) program update will be supplied in a ZIP archive named as follows:

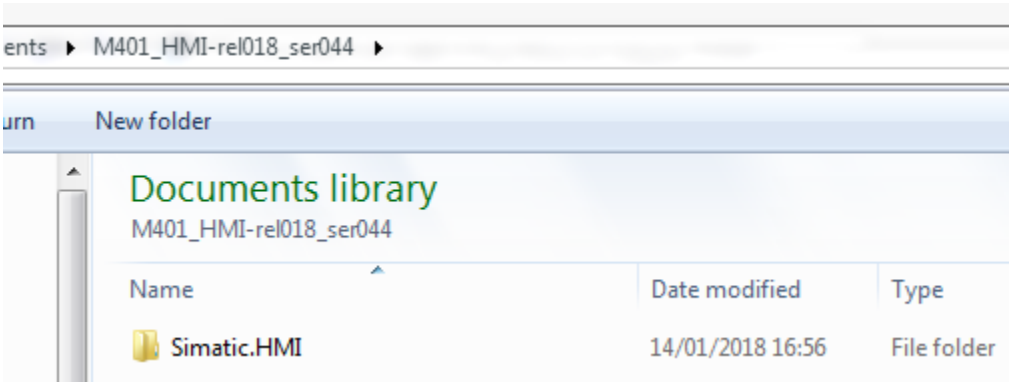
`M401_HMI-rel018_ser044.zip`

`M401_HMI` = Mentor 401 HMI program
`rel018` = release version number
`ser044` = Mentor serial number

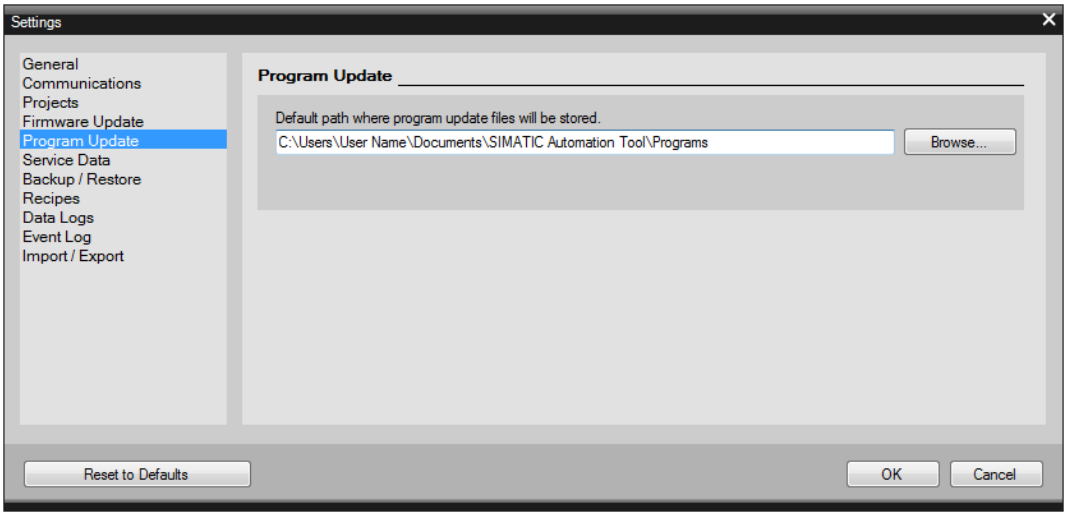
Check the serial number in the received update file matches the serial number of the Mentor to be upgraded. Use of an upgrade file with the wrong serial number will render the Mentor inoperable.

Follow the following steps to make the HMI program update accessible to the SIMATIC automation tool:

1. Use Windows Explorer to extract the ZIP archive to a folder of the same name by right-clicking the ZIP file and selecting “Extract All…”. The result will be a master update folder containing a SIMATIC.HMI folder. Do not edit or rename any files or folders within the master update folder.

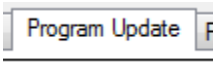


2. Copy or move the resulting folder, together with all its contents, to the SIMATIC Automation Tool Program Update folder, normally C:\Users\{UserName}\Documents\SIMATIC Automation Tool\Programs. The location of the Program Update folder can be determined using the |Options |Settings menu and selecting the “Program Update” option from the menu tree

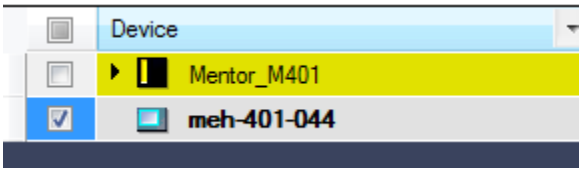


Once the program update has been transferred to the SIMATIC Automation Tool folder, follow the following steps to update the program in the HMI:

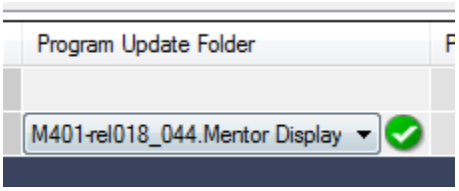
1. Click the “Program Update” tab



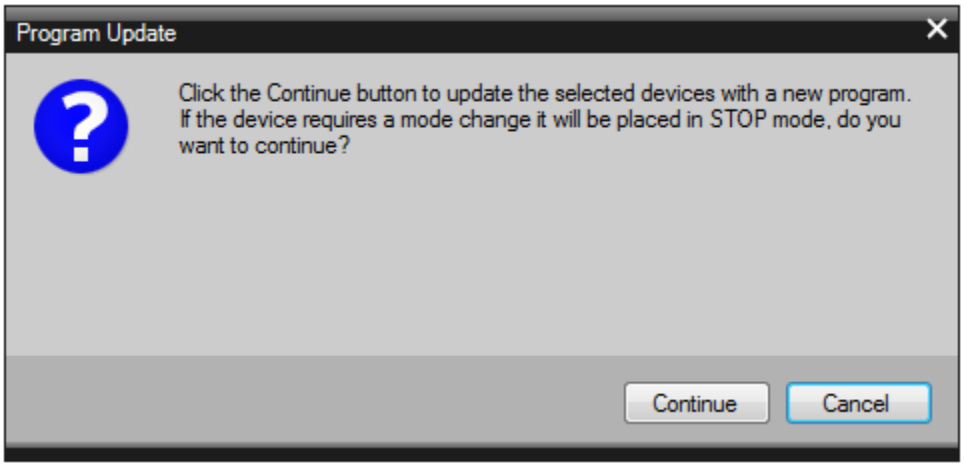
2. Select the Mentor display



3. Select the update file from the drop down list in the “Program Update Folder” column. Note that the displayed filename may differ slightly from the folder name or ZIP file name, but will still contain “M401 .. {release} …{serial number}”.



4. Select the "Operations > Update > Program Update" menu command to start the operation. Alternatively select the Update toolbar button  and select "Program Update" from the button drop-down menu. Click “Continue” in the Program Update confirmation dialog box.



5. The display exits to Windows and the operating system and program are updated. This process may take several minutes.

6. When complete the display will automatically load the Mentor display program. The Event Log below the device table shows the results of the update operation.

7. Check the display program version on the Help menu on the Mentor display.

13 Appendix E: Obtaining Diagnostic Data

The PLC log data may be downloaded to assist with diagnosing and resolving system faults. Log files are downloaded using the Simatic Automation Tool. Refer to section 12.1 on page 70 for information on installing the Simatic Automation Tool.

13.1 Starting the SIMATIC Automation Tool

Use one of the following methods to start the SIMATIC Automation Tool:

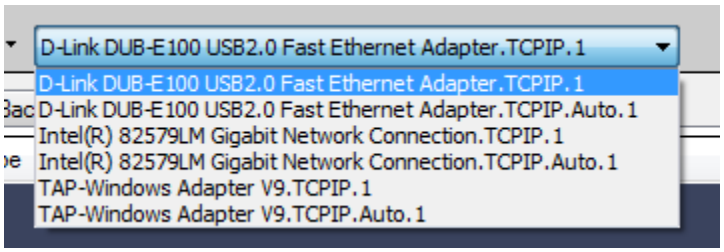
- Double-click the SIMATIC Automation Tool shortcut icon on your desktop.
- Use the Windows Start button:

– Click the Windows start button and "All Programs".

– Click the "Siemens Automation" folder, then the "SIMATIC Automation Tool" folder, and finally "SIMATIC Automation Tool".

13.1.1 Selecting the Network Interface

Before operations can commence you must select the network interface to which the Mentor is connected. Click the Network Interface card dropdown list in the toolbar and select the network interface connected to the Mentor.

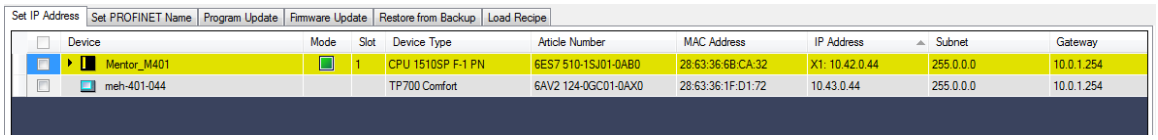


Always choose the device name without ".Auto". Note that the network interface will need a unique IP address in the 10.0.0.0 / 8 subnet.

13.1.2 Scan the Network

To scan the network, select the "Operations>Scan Network>Scan Entire Network" menu command. Alternatively, you can click the Scan button on the toolbar  and select "Scan Entire Network" from the button drop-down menu.

The network is scanned and at least two devices should be reported in the device table.



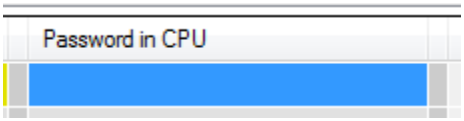
13.2 Displaying the Diagnostic Log

1. Select the Mentor PLC.

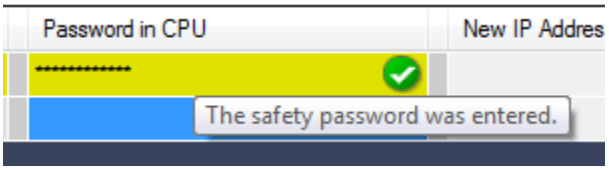
If the PLC is password protected this will displayed as “S7-1500”

If there are multiple Mentor systems in the network verify the device’s IP address

2. Enter the PLC password in the “Password in CPU” field and click Enter.



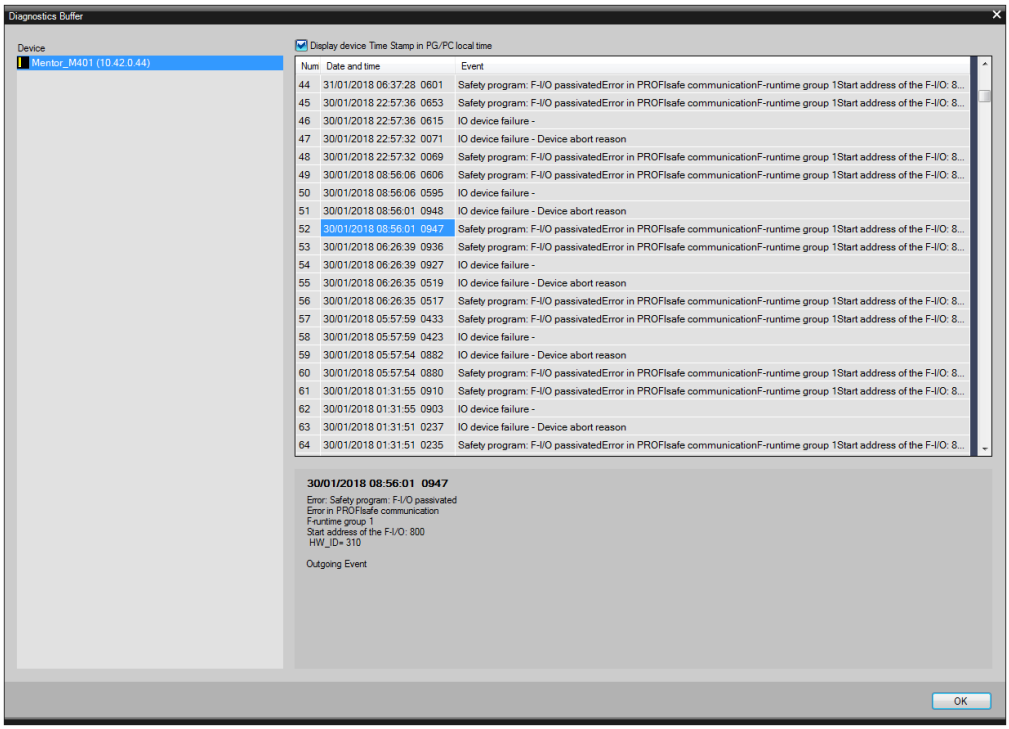
The password will be checked against the PLC password. A valid password, including access to the safety program. will be indicated by a green tick and a yellow highlight on the password dialog box. If a password entry is valid, you can hover your mouse cursor over the password field to display a tool tip that shows the access level.



3. Make sure the Mentor PLC is selected

4. Show the diagnostic log by selecting “Operations > Diagnostics > Show CPU Diagnostics” or by selecting the  button on the toolbar and then selecting “Show CPU Diagnostics” from the drop-down menu.

5. The diagnostic window opens



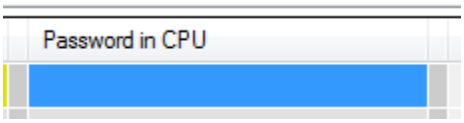
13.3 Uploading Service Data for Analysis

1. Select the Mentor PLC.

If the PLC is password protected this will displayed as “S7-1500”

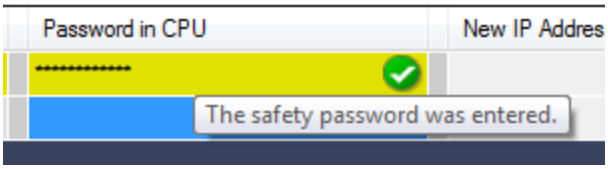
If there are multiple Mentor systems in the network verify the device’s IP address

2. Enter the PLC password in the “Password in CPU” field and click Enter.



The password will be checked against the PLC password. A valid password, including access to the safety program. will be indicated by a green tick and a yellow highlight on the password dialog box. If a

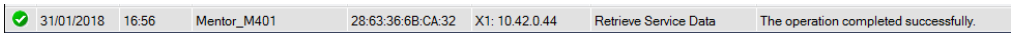
password entry is valid, you can hover your mouse cursor over the password field to display a tool tip that shows the access level.



3. Make sure the Mentor PLC is selected

4. Upload the log files by selecting “Operations > Diagnostics > Retrieve Service Data” or by selecting the button on the toolbar and then selecting “Retrieve Service Data” from the drop-down menu.

5. The log file is uploaded to the PC. When finished, a line will appear in the event log window at the bottom of the screen.



6. The uploaded log data will be stored in the Service Data folder, usually C:\Users\{username}\Documents\SIMATIC Automation Tool\Service Data. The location of the Service Data folder can be checked using the |Options |Settings menu and selecting the “Service Data” option from the menu tree