W&T

www.WuT.de

Manual

Installation, Startup and Application

Web-IO Digital 4.0

valid for:

#57732	Web-IO Digital, 1x 230V In,1x Relais Out
#57832	Web-IO Digital, 230V Relais 1xNO, 1xCO
#57838	Web-IO Digital, 230V Relais 4xNO, 4xCO

Release 1.63 APR. 2023

Subject to error and alteration:
Since it is posssible that we make mistakes, you mustn't use any of our statements without verification. Please, inform us of any error or misunderstanding you come about, so we can identify and eliminate it as soon as possible.

Carry out your work on or with W&T products only to the extent that they are described here and after you have completely read and understood the manual or guide. We are not liable for unauthorized repairs or tampering. When in doubt, check first with us or with your dealer.

Content

1. Legal notices

Warning notice system

This manual contains notices that must be observed for your personal safety as well as to prevent damage to equipment. The notices are emphasized using a warning sign. Depending on the hazard level the warning notices are shown in decreasing severity as follows.

⚠DANGER

Indicates a hazard which results in death or severe injury if no appropriate preventive actions are taken.

⚠WARNING

Indicates a hazard which can result in death or severe injury if no appropriate preventive actions are taken.

⚠CAUTION

Indicates a hazard that can result in slight injury if no appropriate preventive actions are taken.

⚠NOTE

Indicates a hazard which can result in equipment damage if no appropriate preventive actions are taken.

If more than one hazard level pertains, the highest level of warning is always used. If the warning sign is used in a warning notice to warn of personal injury, the same warning notice may have an additional warning of equipment damage appended.

Qualified personnel

The product described in this manual may be installed and placed in operation only by personnel who are qualified for the respective task.

The documentation associated with the respective task must be followed,

especially the safety and warning notices contained therein.

Qualified personnel are defined as those who are qualified by their training and experience to recognize risks when handling the described products and to avoid possible hazards.

Disposal

Electronic equipment may not be disposed of with normal waste, but rather must be brought to a proper electrical scrap processing facility. The lithium manganese dioxide battery installed in the devices must be disposed of separately. See Batteries section

The complete declarations of conformity for the devices described in this manual can be found on the respective Internet data sheet page on the W&T homepage at http://www.wut.de

Symbols on the product

Symbol	Explanation
	CE Mark The product conforms to the requirements of the relevant EU Directives.
	WEEE Mark The product may not be disposed of with normal waste, but rather in accordance with local disposal regulations for electrical scrap
	PE marking Terminals with this marking must be connected to the protective conductor or protective ground.

2. Safety notices

General notices

This manual is intended for the installer of the Web-IOs described in the manual and must be read and understood before starting work. The devices are to be installed and put in operation only by qualified personnel.

Web-IO 4.0 Relay device are not suitable for use in locations where children may be present.

⚠DANGER

Before starting any work on the devices, the power supply must be completely disconnected by taking suitable measures.

The Web IOs are open operating devices that may only be put into operation after they have been firmly and securely installed in a housing or control cabinet. Access to the housings or cabinets may only be possible with a key or with tools and may only be permitted to instructed or authorized personnel.

The protection of the operating personnel and the plant is only guaranteed if the device is used in accordance with its intended use. Operation other than that described in the manuals calls into question the safety and function of the Web IOs and the connected systems.

If faults cannot be eliminated, the devices must be put out of operation and protected against accidental start-up.

There are no user-serviceable parts inside the housing.

Tampering with the devices and modifications to the equipment are life-threatening and therefore not permitted.

The operator is responsible for complying with the locally applicable safety regulations.

Intended use

⚠DANGER

The Digital Web-IOs manufactured by Wiesemann & Theis are network remote switches with integrated web server and digital in- and outputs. They are used as a remote switching and monitoring unit, accessible via TCP/IP-Ethernet using various web and network protocols in accordance with the present manual.

Non-intended use is any other use or any modification to the described devices.

Electrical safety

⚠DANGER

The devices meet the requirements for overvoltage category II environments. When operating in a Cat. III environment, the installer must ensure that suitable protective devices are used to ensure that the Cat. II limits for transient overvoltages at the connections of the devices are not exceeded.

For the Web-IO #57832, it is mandatory that the supply terminal and the switching contacts are connected to the same phase or the same phase conductor. Switching a SELV circuit or another phase is not permitted.

An all-pole supply circuit breaker with a rated current of 16A must be connected upstream of the Web-IO #57832. For the Web-IO #57838, the rated current is 10A.

An easily accessible disconnect device must be provided near the devices during installation.

If the Web-IOs are connected to an inter-building network, this must be protected against transients whose amplitude exceeds a value of 2500 V by overvoltage-limiting measures.

If the Web IOs are supplied with power from an isolated network (so-called “IT” supply network), insulation monitoring must be provided.

EMC

⚠NOTE

Only shielded network cables may be used for connecting the Web-IOs to the network.

In this case the Web-IOs meet the noise immunity limits for industrial applications and the stricter emissions limits for households and small businesses. Therefore there are no EMC-related limitations with respect to the usability of the devices in such environments.

The complete Declarations of Conformity for the devices described in the manual can be found on the corresponding Internet page at the W&T homepage: http://www.wut.de.

Batteries

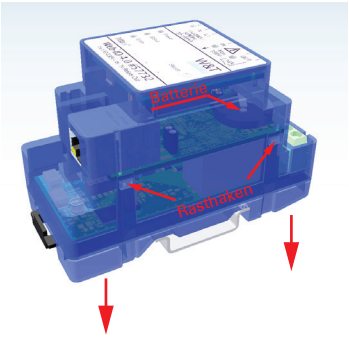
The Web-IO Digital 4.0 relays contain a 3V Lithium-Manganese dioxide battery cell type CR 1632 for buffering the internal clock. This battery has a lifetime of 10 years and may only be replaced by a battery of the same type.

If the Web-IO Digital 4.0 is operated in a network environment with access to a time server, the battery is not absolutely necessary for the correct functioning of the device and can be removed.

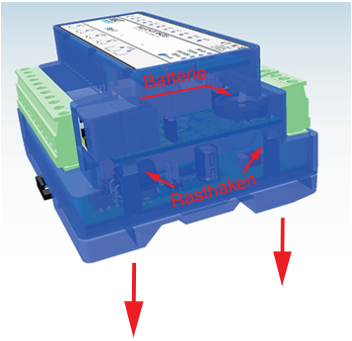
⚠ CAUTION
The battery may be removed or replaced only by an electronic specialist.

To remove the battery, open the housing as follows:

#57732, 57832



#57838



Press a pointed object against the side latch hook of the housing while pulling the base of the housing out of the top shell.

Remove the circuit board stack from the bottom of the housing.

The battery for the clock module is located in a holder on the top circuit board.

After removing/replacing the battery, reassemble in reverse order.

Note re: the Battery Law (BattG):

Batteries and rechargeables must not be disposed of with normal waste, recycling of used batteries and rechargeables is required by law. Used batteries may contain harmful substances which can damage the environment or your health if not disposed of properly.

Batteries also contain important raw materials such iron, zinc, manganese or nickel and are recycled. You can either send the batteries back to us or you can return them free of charge to the local retailer or to the communal collecting point. The return of batteries of the end user to the local retailer is restricted to a reasonable amount of batteries and is restricted to only the batteries that the local retailer offers in his product range.

The full Declaration of Conformity for the described device can be found on the Internet data sheet page on the W&T homepage at www.wut.de/57732, www.wut.de/57832 bzw. www.wut.de/57838.

3. Installation and Wiring

Installation #57732

Installation of the Web-IO 4.0 Digital 1x In, 1xRelay Out must for reasons of contact protection be in an enclosed housing, a sub-distribution unit or a control cabinet. The 45mm (2.5 TE) wide device is then fastened to a 35mm DIN rail.

Wiring #57732

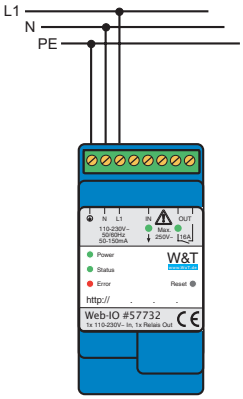
The power and I/O cables are connected to the Web-IO using an 8-pin screw terminal strip with 5mm spacing.

Solid wire with a maximum cross-section of 4.0 mm2 may be used, or stranded conductors with a maximum cross-section of 2.5 mm2.

Please use a 3mm flat screwdriver to tighten the terminal screws. Do not exceed a tightening torque of 0.6 Nm.

Connecting the supply voltage

The Web-IO 4.0 can be operated at an AC voltage of between 110V and 230V and a frequency between 50 and 60Hz. The Power LED indicates the presence of supply voltage.



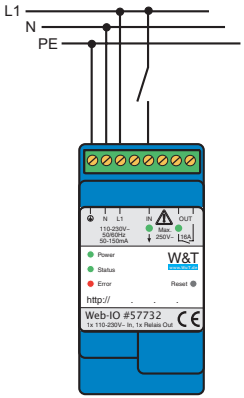
The external lead must be connected to the terminal labeled “L1“, and the neutral conductor to terminal “N“.

⚠ WARNING

Since the described Web-IO 4.0 is a Protection Class I device, the protection ground must always be connected to “PE”.

Input wiring

The digital input signal of the Web-IO 4.0 is connected to the terminal labeled “In”.



Voltages above approx. 80Veff referenced to the “N” terminal are recognized as an “ON” signal and indicated by the green “IN” LED. A switching state must be present for at least 50ms to be reliably detected.

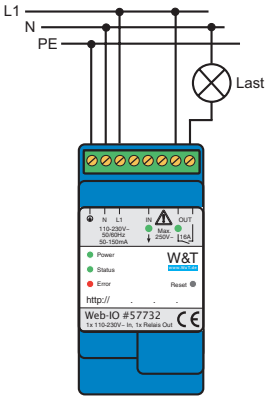
In the example above the outer conductor for the supply is connected to the digital input of the Web-IO using a potential-free contact.

⚠ WARNING

The input signal must always originate from the same outer conductor as the supply voltage.

Output wiring

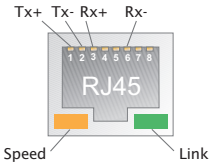
The digital output of the Web-IO is a potential-free contact and can switch loads of up to max. 16A current draw.



The “OUT” LED comes on when the contact is closed. Details about the load capacity of the relay contact can be found in the technical data for the Web-IO.

Network connection

A normal Ethernet patch cable (min. CAT5) with RJ45 plugs can be used for the network connection.



Installation and wiring of the Web-IO should be performed by qualified specialists. Good engineering practice and the corresponding prevailing regulations and standards must be observed.

Installation #57832

Installation of the Web-IO 4.0 Digital 230V Relais 1xNO, 1xCO, must for reasons of contact protection be in an enclosed housing, a sub-distribution unit or a control cabinet. The 45mm (2.5 TE) wide device is then fastened to a 35mm DIN rail.

Wiring #57832

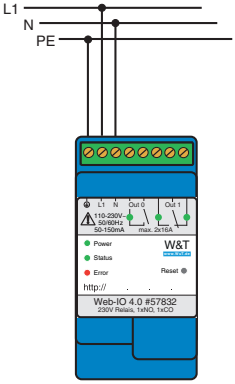
The power and I/O cables are connected to the Web-IO using an 8-pin screw terminal strip with 5mm spacing.

Solid wire with a maximum cross-section of 4.0 mm2 may be used, or stranded conductors with a maximum cross-section of 2.5 mm2.

Please use a 3mm flat screwdriver to tighten the terminal screws. Do not exceed a tightening torque of 0.6 Nm.

Connecting the supply voltage

The Web-IO 4.0 can be operated at an AC voltage of between 110V and 230V and a frequency between 50 and 60Hz. The Power LED indicates the presence of supply voltage.



The external lead must be connected to the terminal labeled “L1“, and the neutral conductor to terminal “N“.

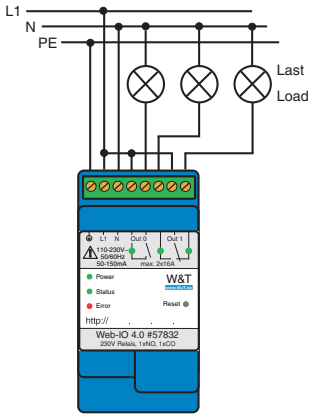
⚠ WARNING

Since the described Web-IO 4.0 is a Protection Class I device, the protection ground must always be connected to “PE”.

Output wiring

The digital outputs of the Web-IO are potential-free contacts and can switch loads of up to max. 16A current draw.

Output 0 is designed as a normally open contact (NO), Output 1 operates as a changeover contact (CO).



⚠ DANGER

Switching voltage and supply voltage must be supplied from the same phase or outer conductor.

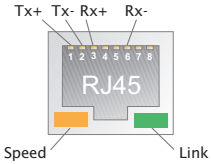
The “OUT” LEDs indicate whether and how a contact is closed. For details on the load capacity of the relay contacts, please refer to the technical data for Web-IO 4.0.

⚠ CAUTION

If the supply voltage is interrupted, the relay contacts retain their current switching state. Only when the power supply is restored or the Web-IO is restarted do the relays revert to the idle state indicated on the device label.

Network connection

A normal Ethernet patch cable (min. CAT5) with RJ45 plugs can be used for the network connection.



Installation and wiring of the Web-IO should be performed by qualified specialists. Good engineering practice and the corresponding prevailing regulations and standards must be observed.

Installation #57838

Installation of the Web-IO 4.0 Digital 230V Relais 4xNO, 4xCO, must for reasons of contact protection be in an enclosed housing, a sub-distribution unit or a control cabinet. The 108mm (6 TE) wide device is then fastened to a 35mm DIN rail.

Wiring #57838

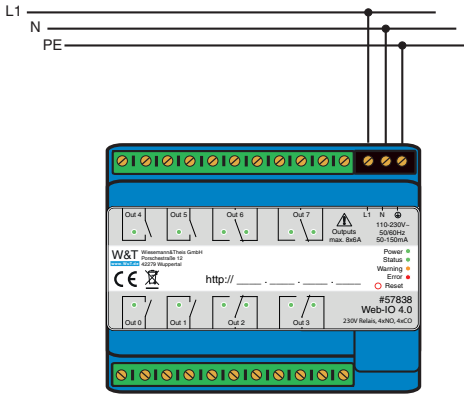
The supply voltage is connected to the Web-IO 4.0 #57838 via the 3-pole, pluggable screw terminal.

The device provides two green, 11-pin, pluggable screw terminals for connecting the outputs. Solid wire or stranded wire with a maximum cross-section of 2.5qmm may be used for the wiring.

Please use a 3mm flat screwdriver to tighten the terminal screws. Do not exceed a tightening torque of 0.6 Nm.

Connecting the supply voltage

The Web-IO 4.0 can be operated at an AC voltage of between 110V and 230V and a frequency between 50 and 60Hz. The Power LED indicates the presence of supply voltage.



The external lead must be connected to the terminal labeled “L1“, and the neutral

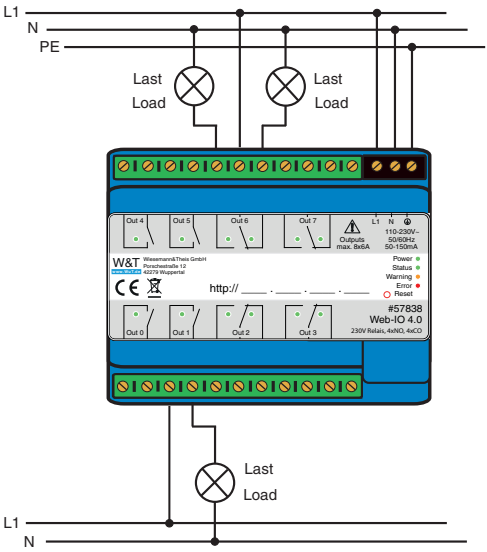
conductor to terminal “N“.

⚠ WARNING
Since the described Web-IO 4.0 is a Protection Class I device, the protection ground must always be connected to “PE”.

Output wiring

The digital outputs of the Web-IO are potential-free contacts and can switch loads of up to max. 6A current draw.

Output 0, Output 1, Output 4 und Output 5 are designed as normally open contacts (NO), Output 2, Output 3, Output 6 und Output 7 operates as a changeover contact (CO).



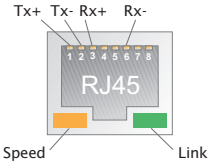
⚠ DANGER
Switching voltage and supply voltage must be supplied from the same phase or outer conductor.

The “OUT” LEDs indicate whether and how a contact is closed. For details on the load capacity of the relay contacts, please refer to the technical data for Web-IO 4.0.

⚠ CAUTION
If the supply voltage is interrupted, the relay contacts retain their current switching state. Only when the power supply is restored or the Web-IO is restarted do the relays revert to the idle state indicated on the device label.

Network connection

A normal Ethernet patch cable (min. CAT5) with RJ45 plugs can be used for the network connection.



Installation and wiring of the Web-IO should be performed by qualified specialists. Good engineering practice and the corresponding prevailing regulations and standards must be observed.

Connection or switching of inductive loads

When switching inductive loads, interference can occur in the phase conductor at the moment of disconnection. If applications have problems switching such loads, there are several ways to reduce or prevent interference:

Contactor as intermediate switch
Instead of operating the load directly via an output of the Web IO, the control line of a contactor is switched by the Web IO and the load is operated through the switching side of the contactor. The utilization category of the contactor must be taken into account here.

Example:

- Finder Series 22 for use category AC-7a/b/c

Line filter

Mains filters suppress interference from electrical devices in supply networks. To reduce wired interference caused by switching inductive loads, a mains filter can be connected in front of the load.Mögliche Netzfilter für Hutschienenmontage:

- NF-1ph-DIN1 von EPA
- NEF 1-10 – 2788977 Phoenix Contact
- FN2412-32-33 Schaffner

RC element

The combination of an electrical resistor and a capacitor can serve as an attenuator for high-frequency interference. For example, in parallel with the inductive load.

RC element for top-hat rail mounting:

- RC12 Eltako

4. Product Introduction

Hardware Features #57732

The Web-IO 4.0 Digital 1x110-230V In, 1xRelay Out (hereinafter referred to simply as Web-IO) is powered with 230V, can monitor a 230V signal and switch a 230V load. Connections are made via screw terminals.

For communication the Web-IO has an RJ45 female for connecting to TCP/IP Ethernet networks.

The device status, error status and status of the inputs/outputs is indicated by corresponding LEDs.

The Web-IO has a battery-backed clock.

A recessed reset switch allows restarting, releasing an emergency access, or resetting to factory defaults, depending on how it is actuated.

Hardware Features #57832

The Web-IO 4.0 230V Relais 1xNO, 1xCO (hereinafter referred to simply as Web-IO) is powered with 230V, can monitor a 230V signal and switch a 230V load. Connections are made via screw terminals.

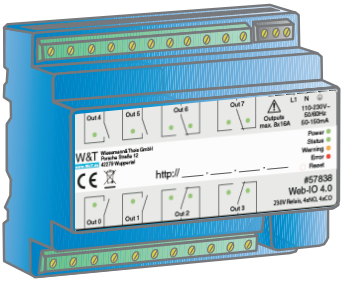
For communication the Web-IO has an RJ45 female for connecting to TCP/IP Ethernet networks.

The device status, error status and status of the inputs/outputs is indicated by corresponding LEDs.

The Web-IO has a battery-backed clock.

A recessed reset switch allows restarting, releasing an emergency access, or resetting to factory defaults, depending on how it is actuated.

Hardware Features #57838



Das Web-IO 4.0 230V Relais 4xNO, 4xCO (hereinafter referred to simply as Web-IO) is powered with 230V, can monitor a 230V signal and switch a 230V load. Connections are made via screw terminals.

For communication the Web-IO has an RJ45 female for connecting to TCP/IP Ethernet networks.

The device status, error status and status of the inputs/outputs is indicated by corresponding LEDs.

The Web-IO has a battery-backed clock.

A recessed reset switch allows restarting, releasing an emergency access, or resetting to factory defaults, depending on how it is actuated.

Network security

The Web-IO has an internal firewall. All available network accesses are configurable and must first be enabled by the administrator. By default only browser access, inventorying via Wutility, and the port for initializing firmware updates are enabled. DHCP is also enabled.

You can explicitly specify for all communication paths whether the outputs may be accessed.

A list of the currently open TCP and UDP ports can be found in the navigation tree under Port list.

Access rights

The Web-IO is configured and operated from the browser. There are three authorization levels for access:

Guest
The guest has read-access to the status of Input, Counter and Output without logging in.

User
A user can switch the output after logging in with a password if it is enabled for access via the browser.

Administrator
After logging in with a password the administrator has unrestricted configuration and access rights.

By default no passwords are assigned for the Web-IO. Simply click on the Login button.

After login the navigation tree on the left side can be used to open the enabled configuration areas. For help and information about the respective configuration possibilities click on the Info buttons on the right side.

Clicking on the Apply button makes the settings immediately effective.

For all other descriptions affecting the configuration, access with Administrator login is required.

Application and access possibilities

Browser access

With password protected access the status of Input, Counter and Output can be monitored in the browser. You can also switch the output with the required access rights.

It is also possible to upload and save a Web page created entirely according to your own needs to the device.

Email sending

The Web-IO offers the option of sending email messages depending on IO states or at fixed intervals. The Web-IO also supports authentication procedures prescribed by public providers.

Box-to-Box

Two Web-IOs can be configured so that the output of the first Web-IO follows the input of the second. This works in both directions when configured accordingly.

Integration into existing system

The Web-IO allows communication using several selected protocols for integration into existing systems when configured accordingly.

MQTT

In Industry 4.0 and the “Internet of Things” MQTT is an innovative communication path. The Web-IO can determine the status of the IOs via MQTT Publish to an MQTT Broker and even accept the request to perform a switching action via MQTT Subscribe.

REST

REST (Representational State Transfer) is another Web-based protocol that can be used to integrate the Web-IO into the environment of Industry 4.0 and the Internet of Things.

Web-API - HTTP-Requests/AJAX

The status of Input, Counter and Output can be queried using HTTP requests. In addition the outputs can be directly controlled using HTTP requests.

OPC

Together with the W&T OPC Server the Web-IO can be accessed from any OPC client applications.

SNMP

The status of Input, Counter and Output as well as the configuration and error status can be obtained via SNMP. A private MIB for direct download from the device is available for easy incorporation into SNMP systems.

Modbus-TCP

With Modbus-TCP the Web-IO supports one of the most common industry protocols. By reading and writing the corresponding registers any Modbus-TCP master can access the IOs.

In-house applications

The Web-IO offers TCP and UDP socket accesses for access from your own applications. In both cases the Web-IO supports addressing using command strings, but also by exchanging binary structures.

With the support of HTTP requests your own Web applications (e.g. with PHP or JavaScript) can also access the Web-IO.

Actions

Depending on predefined events on the IOs, the Web-IO can initiate actions such as sending an email message. Other actions include sensing syslog messages or SNMP traps, writing to a file via FTP, sending data via TCP or UDP, or switching its own output.

5. Initial start-up

Once the Web-IO has been properly installed and wired, the power can be turned on. All three status LEDs should come on briefly. After approx. 5 seconds only the Power LED should remain on. The Status LED may flash. If a valid signal is detected on one of the inputs, the corresponding LED will come on.

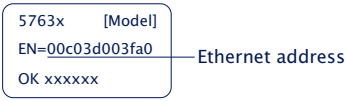
When a network is connected the green LED in the network socket will indicate an existing link. The orange LED provides information about the network speed.

On = 100MBit/s
Off = 10MBit/s

Assigning the IP address

IBy default IP address 0.0.0.0 and DHCP is activated on the Web-IO.

Networks with DHCP
If a DHCP server is active in the network in which the Web-IO is connected, an IP address should be automatically assigned to the Web-IO. To be able to specifically access the Web-IO, you should configure a reservation in the DHCP server so that the Web-IO is always accessible under the same address. The required Ethernet address can be found on the white sticker on the device.



(If in doubt ask your network administrator)

Netzwerke ohne DHCP
Install the Wutility Windows PC program (download at http://www.WuT.de). If no Windows PC is available, see the Appendix, sub-section Alternatives to IP Address Assignment.

When Wutility is started the local subnet is searched and all found W&T network

components are listed. Highlight your Web-IO and click on the IP Address icon. Wutility suggests the network parameters (subnet mask, gateway, DNS server) which also apply to the PC. If the Web-IO will run in the same subnet, you must only modify the IP address.

If you select Address range > any network, you can also enter parameters which are different from your local network, for example to pre-configure the Web-IO for a different network.

Changing the set IP parameters

To later change the IP address, subnet mask, gateway or DNS server, you can either use Wutility again or modify the parameters in the browser under Basic settings » Network.

6. Basic Settings

The rest of the Web-IO configuration is done in the browser. As an address enter the IP address of the Web-IO. Click on Login in the navigation tree and select Administrator as the user. By default no password is assigned, you need only click on the Login button to configure the Web-IO with Administrator rights.

Configuring Input and Output

In Basic settings » Input/Output you can give individual names to the Input and Output. These names replace the factory default names Input and Output in the visualization and any message texts.

Expanded Input settings

For special applications some Input properties can be modified:

Input filters

A signal state must be present for the time in milliseconds entered here for it to be processed by the Web-IO. This can for example filter out bouncing of mechanical contacts.

Signal inversion

Normally signals of over 80V are reliably detected as ON. Enabling inversion means voltages over 80V are considered OFF.

Expanded Output settings

For special applications some Output properties can be modified:

Switch Output inverted

Normally the Output is turned off in the OFF state, i.e. turned on with no signal and in the ON state. Enabling inversion means the Output behaves in exactly the reverse.

Pulse mode

By enabling Pulse mode, when the Output is switched to the ON state it reverts automatically back to the OFF state after the set pulse duration. When turned on again during the pulse, the pulse duration begins to count over again. Reset allowed means the Output may also be switched to the OFF state during a pulse.

Date / Time

In the Date / Time area you can specify whether there is a cyclical synchronization with a time server. In addition the date and time can be manually set. Here you can also configure a time zone and summer/winter time changes.

Language / Info

In addition to selecting German or English, you can also modify other display elements including the logo.

Password

Here you can specify passwords for Administrators and Users.

Please note that the same password should not be used for Administrators and Operators.

If the Administrator password has been forgotten, physical intervention in the Web-IO is required to reset the passwords. See section Emergency access in the appendix to this manual.

Certificates

Protocols such as HTTPS or OPC UA are based on the TLS protocol. The encryption of the communication and the authentication of the communication partners is realized via certificates.

The Web IO identifies itself ex works with a self-signed certificate. Many applications consider such certificates to be a security risk. If the application requires secure authentication, the Web IO must be equipped with an individual certificate signed by a trusted certification authority.

Certificate Signing Request (CSR)

Here it is possible to generate a CSR with a new key pair and individual content.

By clicking the *Verify* button, the entered values are formally checked and the new key is generated. The new CSR can be downloaded via the *Download CSR* button.

Self signed certificate

A previously generated inidividual CSR can be self-signed by the device with the private key belonging to the CSR.

Upload certificate/upload certificate chain

A previously generated and downloaded CSR can be loaded into the device as a certificate after signature by an external certification authority. If a certificate chain belonging to the certificate is not already part of the certificate file, it can be uploaded separately afterwards. The files can be in PEM or DER format.

Install certificate/certificate chain

A previously uploaded certificate incl. associated certificate chain is installed in the device and used as a certificate within TLS connections after saving.

7. Basic Applications

The Web-IO features a variety of different communication options and supports various standard protocols. We recommend enabling only the communication paths actually required in your application. This limits the possibility of unauthorized access and manipulation.

First we will introduce the most commonly used communication methods:

Browser access

Access from a browser is special in that in addition to monitoring and operating the IOs, if a user is logged in he can also configure the Web-IO from here.

The Administrator has authorization to access the entire configuration. Using the likewise password protected user access all the IOs can be adapted to the respective settings.

Without a login only the states of Input and Output can be observed.

HTTP or HTTPS

By default browser access for HTTP is enabled using Port 80. To change access to HTTPS or change the port, select Basic settings >> Network in the navigation tree and then Protocol under Access for Web services. All other settings applicable in the browser can be made under Web sites.

Hide menu tree

Once configuration is finished, browser display can be restricted in the browser to IO access. To do this go to Web sites >> Browser access and select the option Hide navigation tree. Use: http://<URL/IP of Web-IO>/index to temporarily show the menu tree and then permanently turn it off a gain using the option above.

IO access

The Web-IO provides two pre-prepared Web pages for access to Input, Counter and Output:

Home

The Home page provides an overview of Input, Output and the configured actions. When appropriately logged in the output can be switches and the counter cleared. Both must first be enabled under Web sites >> Home. Be default this is disabled.

The menu point Web sites >> Home offers several other display options for the Home page.

Direct opening of the Home page without display of the navigation tree at: http://<URL/IP of Web-IO>/home

If Hide menu tree is enabled, a password entry field appears on the Home page. After clicking on the Apply button the Output and Counter can be operated until the Home page is exited. Enabling Web sites >> Home > Save password for switching in browser saves the password in the browser as a cookie and operation is immediately enabled again after opening the Home page in the same browser.

My Web page

The preloaded Web page in the Web-IO provides a compact overview of the IO states.

Under Web sites >> My Web page the original Web page can be replaced with one you have programmed yourself.

For the Web page to be able to dynamically refresh the states of Input, Counters and Output, Allow HTTP requests must be enabled under Communication paths >> Web-API. *Here you also specify whether the output is allowed to be switched using HTTP requests used for AJAX.*

Direct opening of your own Web page without displaying the navigation tree at: http://<URL/IP of the Web-IO>/user

More details on programming your own Web pages can be found in the programming manual for the Web-IO. (Download at: http://www.WuT.de – simply enter the article number of your Web-IO in the search field and select Manual.)

The Smart Website

For access from a smartphone or other device with a limited screen size, the Web IO offers a very compact web page.

The smart website is not linked via the navigation tree and can only be accessed via

the direct URL entry *http://<URL/IP of the Web-IO>/smart*.

Sending email

A few basic settings are necessary in order to send email messages.

Network parameters

If you want to send via a mail server in the Internet, it is important that the network basic settings are correct. Check under Basic settings >> Network especially whether Gateway and DNS server are correctly specified.

Mail server access

All mail server-specific settings can be made under Communication paths >> Mail. The currently favored authentication procedure is SSL/TLS. For more tips about specific settings for the most common email providers see the info section under Mail.

⚠ Creating an email message

To create an email message, click the Add button under Actions. An input screen will appear for a new action.

Here you can determine the name for an action and what the initiator should be (e.g. the ON state of the input). A detailed description of the possibilities can be found in the Actions section.

For the action select Email message. In the associated input screen you can compose an individual email message. Use the placeholders described below which replace the current IO status, counter values etc. for sending the email.

Placeholder	Description
<ix>	State of the inputs No. x (ON/OFF)
<ox>	State of the outputs No. x (ON/OFF)
<cx>	Counter state No. x
<i>	State of all inputs as hex. bit pattern
<o>	State of all outputs as hex. bit pattern

Placeholder	Description
<dn>	Device Name
<inx>	Name of the input No. x
<onx>	Name of the output No. x
<t>	Time stamp with date and time
<$y>	Year in format „YYYY“
<$m>	Month in format „MM“
<$d>	Day in format „DD“
<$h>	Hour in format „hh“
<$i>	Minutes in format “mm“
<$s>	Seconds in format „ss“

Box-to-Box

Box-to-Box mode links two Web-IOs to each other over the same network so that the output of the one Web-IO follows the input of the other Web-IO (ON on the input of Web-IO A switches the output of Web-IO B to ON).

Box-to-Box mode the idea is to configure one Web-IO as the master and the other as a slave. The master Web-IO (Client) is responsible for opening the connection to the slave Web-IO (Server). After the connection has been opened, both Web-IOs work equally and when correspondingly configured send the switching signals in both directions.

8. Integration Into Existing Systems

The Web-IO supports several common standards and protocols and can therefore be integrated easily into many existing systems.

MQTT

After enabling MQTT and configuring in the menu branch Communication paths >> MQTT the Web-IO supports two basic possibilities:

1. Passing the individual IO states and the counter value as an MQTT Topic to an MQTT Broker via MQTT Publish.
2. Switching the output depending on Topic contents received via MQTT Subscribe.

Both cases are handled in the Web-IO as an Action. A detailed description of the Action philosophy used in the Web-IO can be found in the Actions section.

Publish IO states

To create a new MQTT Publish, click on the Add button under Actions. The input screen for a new action will appear.

Here you can specify a name for the action and what the initiator should be.

For example you can specify Input as the initiator and ON as the trigger.

For the action select MQTT-Publish. In the following menu enter the path through which the Topic should be written for the Broker.

You can freely determine the contents of the Topic, where the placeholders described in the infotext can be used.

Switching outputs using Subscribe

Here again you must add a new action. As initiator select MQTT-Subscribe. Then enter the path over which the Topic is send which contains the keyword for switching. For action use Switch output >> Switch this Web-IO output. Then specify to what state the output should be switches and if the state should change.

Example:
A device writes as a topic the keyword ON for the Broker specified in the Web-IO over the path wut/webio123/set0. This path and the Topic are specified for the Web-IO as initiator under MQTT Subscribe. Switching the output to ON is specified as the action.

Each time ON is written the output is switched. You can use a second action to specify what should be used to turn the output off again.

The Web-IO as MQTT gateway

The flexibility which the Web-IO allows in configuring act4ions means that depending on the contents of certain Topics you can also send emails, SNMP traps or messages over other communication paths. For more information see the Actions section.

REST

The Web-IO uses REST (Representational State Transfer) to provide another Web-based communication path.

Communication is via Web-IO specific HTTP requests using the HTTP or HTTPS port specified under Basic settings >> Network >> Access for Web services.

To be able to exchange data via REST, access via Communication paths >> Rest must first be enabled.

If you wish to protect REST access against unauthorized manipulation, you can enable digest authentication. The requests must then take place as “admin” user with the Administrator password or as “operator” using the user password.

Here you can also specify whether REST is permitted to switch the output.

Read access

For read access REST uses the HTTP command GET.

The Web-IO supports three formats for replies to REST requests:

- JSON
- XML
- Text

The format used for replies can be determined using the request. Using

```
http://<ip-adresse>/rest/json
```

for example opens the entire process image of the Web-IO in JSON format. The reply then looks as follows:

```
{
  "info" :
  {
    "request" : " / rest / json",
    "time" : "2016 - 09 - 09,
    09 : 42 : 54",
    "ip" : "10.40.22.227",
    "devicename" : "WEBIO - CAFE27"
  },
  "iostate" :
  {
    "input" : [
      {
        "number" : 0,
        "state" : 0
      }
    ],
    "output" : [
      {
        "number" : 0,
        "state" : 0
      }
    ],
    "counter" : [
      {
        "number" : 0,
        "state" : 0
      }
    ]
  },
  "system" :
  {
    "time" :
    {
      "time" : "2016 - 09 - 09,
      09 : 42 : 54"
    },
    "diagnosis" : [
      {
        "time" : "06.09.2016 09 : 42 : 54",
        "msg" : "Gerätestatus : OK"
      }
    ],
    "diagarchive" : [
      {
        "time" : "06.09.2016 09 : 42 : 54",
        "msg" : "Gerätestatus : OK"
      }
    ]
  }
}
```

To query individual areas or points, you can formulate the request in greater detail:

```
http://<ip-adresse>/rest/json/iostate/input
```

This causes the Web-IO to return the status of the inputs:

```
{
  "iostate" :
  {
    "input" : [
      {
        "number" : 0,
        "state" : 0
      }
    ]
  }
}
```

Changing access

The same URL can be used to turn the output off using the parameter Set=Off or to change its state using Set=TOGGLE.

Clearing counters for example is done by using a POST to the following URL:

```
http://<ip-adresse>/rest/json/iostate/output/0
```

To remain compatible with the Web-IO products which have more than one output, Index 0 must be specified for Output 0.

The following parameters are sent:

```
Set=ON
```

The Web-IO replies with

```
{
  "iostate" :
  {
    "output" : [
      {
        "number" : 0,
        "state" : 1
      }
    ]
  }
}
```

The same URL can be used to turn the output off using the parameter Set=Off or to change its state using Set=TOGGLE.

Clearing counters for example is done by using a POST to the following URL:

```
http://<ip-adresse>/rest/json/iostate/counterclear/0
```

No additional parameter needs to be sent.

The Web-IO replies with

```
{
  "iostate" :
  {
    "counter" : [
      {
        "number" : 0,
        "state" : 0
      }
    ]
  }
}
```

To receive the replies in one of the other formats, simply replace the keyword `json` with `xml` or `text`.

A detailed description of the supported REST requests and the structure of the replies can be found in the Web-IO Programming Manual (download at http://WuT.de*). Follow the* Manual *link from the data sheet page for your Web-IO.*

OPC DA

By default the Web-IO is set for OPC mode. To use OPC, you must simply enable OPC access under Communication paths >> OPC and as needed enable switching of the output.

For your OPC client to communicate with the Web-IO the W&T OPC server must be installed. Access via OPC servers from third parties is not possible.

In the OPC server select Devices >> New I/O device. Enter the IP address and password for your Web-IO and select the Web-IO model. Confirm with OK. Then you must use File >> Save as active configuration to apply the new entries.

OPC UA

In addition to the classic OPC access via the W&T OPC server, the Web IO can also be addressed directly via OPC UA.

The device provides OPC UA via a binary TCP protocol.

The preset port of the server service corresponds to the standard port for this application: 4840. The connection setup of your client is done accordingly with the call:

```
opc.tcp//<ip-adresse>:4840
```

Authentication

The device provides several authentication methods, with corresponding security policies. You have the choice between:

- No authentication — No security policy
- Sign — Security policy:
  Basic128 - RSA15
  Basic265
  Basic265-SHA256
  AES128-SHA256 RsaOaep
- Sign & Encrypt — Security policy:
  Basic128 - RSA15
  Basic265
  Basic265-SHA256
  AES128-SHA256 RsaOaep

Also configure a UPC UA user name and password. If you select „No authentication“, this is not necessary.

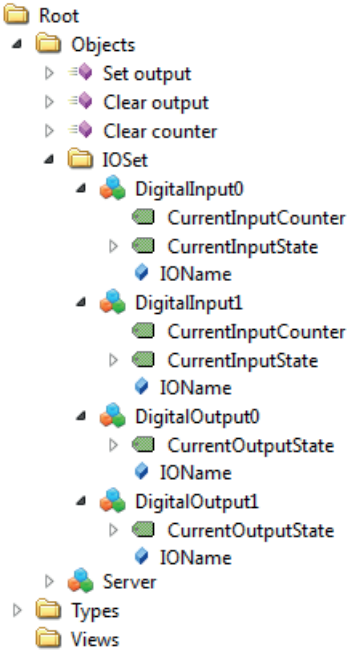
Nodes und NodeIDs

The main nodes that can be used to retrieve the states of the IO endpoints are:

- CurrentInputCounter - Counter value of the pulses detected at the input
- CurrentInputState - Switching state of the inputs (ON or OFF)
- CurrentoutputState - Switching state of the outputs (ON or OFF)

The device provides you with the OPC UA tree shown in the following (here at the

example of the Web-IO #57737).



A list of the most important nodes and the corresponding NodeIDs can be retrieved in the browser via `http://<ip-address>/opcua_nodes?PW=<password>&`.

If you want to replace the factory default NodeIDs with your own, download the node configuration in the menu branch *Communication paths >> OPC UA*. Enter the desired IDs behind the given IDs in the JSON file. Upload the modified file again and click *Apply*.

Changing the output switching states and clearing the counters is done by the following methods:

- Set output - sets the output defined by the index parameter to ON
- Clear output - sets the output defined by the index parameter toOFF
- Clear counter - sets the counter defined by the index parameter to 0

SNMP

SNMP can be used to access the IOs as well as the configuration of the Web-IO. Which parameter, what status, what value can be called under which OID is stored in the private MIB, which can be downloaded directly from the Web-IO Communication paths >> SNMP (or download from http://www.WuT.de).

The MIB can be conveniently viewed using the usual MIB browser. This gives you the quickest overview of the assigning of the OIDs.

All settings affecting SNMP can be made using Communication paths >> SNMP. To make the output switchable using SNMP, it must be enabled here.

Opening an SNMP session

Read access is possible using SNMP-Get requests after enabling SNMP under Communication paths >> SNMP. Write/altering access requires a session login with system password entry.

This is done using SNMP-SET via the OID which you can find in the MIB branch of your Web-IO under

```
wtWebioEA….SessCntrl » wtWebioEA….SessCntrlPassword
```

Whether there is a valid session open can be queried using a GET request to the OID

```
wtWebioEA….SessCntrl » wtWebioEA….SessCntrlConfigMode.
```

(Return 1 = valid session 0 = no session.)

A session can be ended using SET to the OID

```
wtWebioEA….SessCntrl » wtWebioEA….SessCntrlLogout
```

During an SNMP session login attempts from the browser are rejected.

Access to input and output

Reading the input, counter and output is always possible using GET requests to the corresponding OID.

In the OID area

```
wtWebioEA….InOut
```

there are corresponding tables.

The MIB is symmetrically structured for the various Web-IO models. Input and output tables are kept which have a different number of entries depending on the Web-IO model. In this way the MID remains compatible across different models.

Example: Querying the switching state of Input0

```
wtWebioEA….InOut » wtWebioEA….InputTable »
              wtWebioEA….InputEntry » wtWebioEA….InputState
```

An index is appended to the table entries for the individual IOs. For Input 0 for example „.1“ (return 0 = OFF and 1 = ON.)Switching the outputs requires a valid session. There is also a corresponding table for the outputs:

```
wtWebioEA….InOut » wtWebioEA….OutputTable »
            wtWebioEA….OutputEntry » wtWebioEA….OutputState
```

Indexing works just like for the outputs. If a 1 is sent via SNMP-SET, the output switches to ON – and sending a 0 turns it OFF.

Modbus-TCP

The menu point Communication paths >> Modbus-TCP can be used to enable the Web-IO for Modbus slave mode. Here you can also specify whether Modbus-TCP may be used to switch the outputs.

The following tables show which function codes and register addresses are supported by the Web-IO.

Modbus-Memory

Bit range:

addresse (hexadec.)	description	memory type	length (byte)	read bits with FC	read reg. with FC	Write bits with FC	write reg. with FC
1000	Input 0	bit	1	0x01, 0x02	-	-	-
1001	Input 1	bit	1	0x01, 0x02	-	-	-
1002	Input 2	bit	1	0x01, 0x02	-	-	-
1003	Input 3	bit	1	0x01, 0x02	-	-	-
1004	Input 4	bit	1	0x01, 0x02	-	-	-
1005	Input 5	bit	1	0x01, 0x02	-	-	-
1006	Input 6	bit	1	0x01, 0x02	-	-	-
1007	Input 7	bit	1	0x01, 0x02	-	-	-
1008	Input 8	bit	1	0x01, 0x02	-	-	-
1009	Input 9	bit	1	0x01, 0x02	-	-	-
100A	Input1 0	bit	1	0x01, 0x02	-	-	-
100B	Input 11	bit	1	0x01, 0x02	-	-	-
1020	Output 0	bit	1	0x01, 0x02	-	0x05	0x0F
1021	Output 1	bit	1	0x01, 0x02	-	0x05	0x0F
1022	Output 2	bit	1	0x01, 0x02	-	0x05	0x0F
1023	Output 3	bit	1	0x01, 0x02	-	0x05	0x0F
1024	Output 4	bit	1	0x01, 0x02	-	0x05	0x0F
1025	Output 5	bit	1	0x01, 0x02	-	0x05	0x0F
1026	Output 6	bit	1	0x01, 0x02	-	0x05	0x0F
1027	Output 7	bit	1	0x01, 0x02	-	0x05	0x0F
1028	Output 8	bit	1	0x01, 0x02	-	0x05	0x0F
1029	Output 9	bit	1	0x01, 0x02	-	0x05	0x0F
102A	Output 10	bit	1	0x01, 0x02	-	0x05	0x0F
102B	Output 11	bit	1	0x01, 0x02	-	0x05	0x0F
1040	Alarm state 1	bit	1	0x01, 0x02	-	-	-
1041	Alarm state 2	bit	1	0x01, 0x02	-	-	-
1042	Alarm state 3	bit	1	0x01, 0x02	-	-	-
1043	Alarm state 4	bit	1	0x01, 0x02	-	-	-
1044	Alarm state 5	bit	1	0x01, 0x02	-	-	-
1045	Alarm state 6	bit	1	0x01, 0x02	-	-	-
1046	Alarm state 7	bit	1	0x01, 0x02	-	-	-
1047	Alarm state 8	bit	1	0x01, 0x02	-	-	-
1048	Alarm state 9	bit	1	0x01, 0x02	-	-	-
1049	Alarm state 10	bit	1	0x01, 0x02	-	-	-
104A	Alarm state 11	bit	1	0x01, 0x02	-	-	-
104B	Alarm state 12	bit	1	0x01, 0x02	-	-	-
1060	Exception State	bit	1	0x01, 0x02	-	-	-
1068	Config. state	bit	1	0x01, 0x02	-	-	-
1800	Alarm trigger 1	bit	1	0x01, 0x02	-	0x05	0x0F
1801	Alarm trigger 2	bit	1	0x01, 0x02	-	0x05	0x0F
1802	Alarm trigger 3	bit	1	0x01, 0x02	-	0x05	0x0F
1803	Alarm trigger 4	bit	1	0x01, 0x02	-	0x05	0x0F
1804	Alarm trigger 5	bit	1	0x01, 0x02	-	0x05	0x0F
1805	Alarm trigger 6	bit	1	0x01, 0x02	-	0x05	0x0F
1806	Alarm trigger 7	bit	1	0x01, 0x02	-	0x05	0x0F
1807	Alarm trigger 8	bit	1	0x01, 0x02	-	0x05	0x0F
1808	Alarm trigger 9	bit	1	0x01, 0x02	-	0x05	0x0F
1809	Alarm trigger 10	bit	1	0x01, 0x02	-	0x05	0x0F
180A	Alarm trigger 11	bit	1	0x01, 0x02	-	0x05	0x0F
180B	Alarm trigger 12	bit	1	0x01, 0x02	-	0x05	0x0F

Please note that the number of supported inputs, outputs, counters or alarms varies depending on the Web-IO model.

16- and 32-bit range:

addresse (hexadec.)	description	memory type	length (byte)	read bits with FC	read reg. with FC	Write bits with FC	write reg. with FC
2000	Inputs 0 - 11	16-bit	2	-	0x03, 0x04	-	-
2002	Outputs 0 - 11	16-bit	2	-	0x03, 0x04	-	-
2004	Alarm state 1 - 12	16-bit	2	-	0x03, 0x04	-	-
2006	Diagnosis Error count	16-bit	2	-	0x03, 0x04	-	0x06, 0x10
2007	Diagnostic state 0 - 15	16-bit	2	-	0x03, 0x04	-	-
2008	Diagnostic state 16 - 31	16-bit	2	-	0x03, 0x04	-	-
2009	Diagnostic state 32 - 47	16-bit	2	-	0x03, 0x04	-	-
200A	Diagnostic state 48 - 63	16-bit	2	-	0x03, 0x04	-	-
200B	Diagnostic state 64 - 79	16-bit	2	-	0x03, 0x04	-	-
200C	Diagnostic state 80 - 95	16-bit	2	-	0x03, 0x04	-	-
200D	Exception/Conf.-State	16-bit	2	-	0x03, 0x04	-	-
5000	Inputs 0 - 11	32-bit	4	-	0x03, 0x04	-	-
5002	Outputs 0 - 11	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
5004	Alarm state 1 - 12	32-bit	4	-	0x03, 0x04	-	
5006	Counter 0	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
5008	Counter 1	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
500A	Counter 2	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
500C	Counter 3	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
500E	Counter 4	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
5010	Counter 5	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
5012	Counter 6	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
5014	Counter 7	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
5016	Counter 8	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
5018	Counter 9	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
501A	Counter 10	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
501C	Counter 11	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
504A	Diagnosis Error count	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
504C	Diagnostic state 0 - 31	32-bit	4	-	0x03, 0x04	-	-
504E	Diagnostic state 32 - 63	32-bit	4	-	0x03, 0x04	-	-
5050	Diagnostic state 64 - 95	32-bit	4	-	0x03, 0x04	-	-
7000	virtuel Register 0	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
7002	virtuel Register 1	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
7004	virtuel Register 2	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
7006	virtuel Register 3	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
7008	virtuel Register 4	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
700A	virtuel Register 5	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
700C	virtuel Register 6	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
700E	virtuel Register 7	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
7010	virtuel Register 8	32-bit	4	-	0x03, 0x04		0x06, 0x10
.....	virtuel Register 9 - 23	32-bit	4				
702E	virtuel Register 23	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
7030	virtuel Register 24	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
7032	virtuel Register 25	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
7034	virtuel Register 26	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
7036	virtuel Register 27	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
7038	virtuel Register 28	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
703A	virtuel Register 29	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
703C	virtuel Register 30	32-bit	4	-	0x03, 0x04	-	0x06, 0x10
703E	virtuel Register 31	32-bit	4	-	0x03, 0x04		0x06, 0x10

A detailed description of the supported function codes and register addresses can be found in the Web-IO programming manual.

9. Actions

The Action principle allows the Web-IO to issue individual alarms and messages – but also to switch the output. This is done based on defined IO states or other events.

Up to 12 actions can be stored and managed, where an individual name can be specified for each action.

Initiator

Input
The input can be specified as the initiator. For the input you can specify whether a change from OFF to ON, from ON to OFF, or any state change should initiate an action.

Output
The output can be specified as the initiator. For the output you can specify whether a change from OFF to ON, from ON to OFF, or any state change should initiate an action.

Counter
The counter can be specified as the initiator. For the counter you must specify for which count value an action should be initiated. You also need to determine whether the counter is reset to zero after the action is initiated.

I/O combination
A combination of input and output can also initiate an action. Here you can specify whether the individual states should have an AND or OR operation performed.

Interval Timer
The Web-IO can be configured to perform actions at specified times. The times are entered in Cron format.

Valid characters:

* Stands for all valid values in the respective entry field (e.g. all minutes or all hours)
- Specifies a range of from…to (e.g. weekday “2-4” stands for Tuesday to Thursday, whereas entering “*” triggers the timer on all weekdays).
/ Interval within the specified range (e.g. minute “0-45/2” triggers the timer in a range between the 0th and 45th minute every two minutes (0, 2, 4, 6 ,8, 10, ... , 44)).
, Specifies an absolute value (e.g.: minute „0, 15 ,30“ triggers the timer every full hour, every 15th minute and every 30th minute.).

Beispiel:
An action should be performed in the months of April to October every Monday at 8:00 a.m.

Minute:	0
Hour:	8
Date:	*
Month:	4-10
Day of week:	1

Device restart

The Web-IO distinguishes between two types when a restart is supposed to initiate an action:

- Cold start
  If the restart is initiated by hardware (applying/interrupting supply voltage or pressing the reset key) the Web-IO treats this as a cold start.

- Warm start
  A warm start can be initiated from the Web page under Maintenance by clicking on the Restart button. Connecting from Port 8888 and using the system password will also cause a reset if the reset port is enabled.

MQTT Subscribe

If the Web-IO receives the keyword configured as a Topic on the path entered as Topic path, the action is carried. Out. For this Communication paths >> MQTT must be used to enable MQTT support, and all the necessary Broker information must be

configured.

Actions

For actions which allow sending alarms, messages and other texts, placeholders can be used within the text which replace actual contents such as IO states, time etc. when performing an action.

Placeholder	Description
<ix>	State of the inputs No. x (ON/OFF)
<ox>	State of the outputs No. x (ON/OFF)
<cx>	Counter state No. x
<i>	State of all inputs as hex. bit pattern
<o>	State of all outputs as hex. bit pattern
<dn>	Device Name
<inx>	Name of the input No. x
<onx>	Name of the output No. x
<t>	Time stamp with date and time
<$y>	Year in format „YYYY“
<$m>	Month in format „MM“
<$d>	Day in format „DD“
<$h>	Hour in format „hh“
<$i>	Minutes in format “mm“
<$s>	Seconds in format „ss“

For text messages not only the actual message sent when initiating, but also a Clear message can be stored. The Clear message is sent when the initiator for the action is no longer active – i.e. the normal state is resumed. Sending of messages takes different amounts of time depending on the protocol. If the initiating state is only present for such a short time that the corresponding message could not be sent, only the Clear message is sent.

Email message

The recipient, subject and contents of the email can be freely configured.

To be able to send email messages access to the mail server must be configured and Mail enabled as the communication path. All necessary settings can be made under Communication paths >> Mail. In the info area you will find the general access data for the most common email providers.

SNMP trap

The IP address and host name of the SNMP server as well as the message texts can be freely configured.

To be able to send SNMP traps you must enable SNMP under Communication paths » SNMP. All other parameters which can be set there are not relevant to sending of SNMP traps.

MQTT publish

The Web-IO can write any information to an MQTT Broker over a configurable path as an MQTT Topic.

For this access to the MQTT Broker must be configured under Communication paths >> MQTT.

HTTP request

Another possible action is sending of an HTTP request, such as required by devices like cameras, in order to trigger certain functions.

As the HTTP request enter the complete URL with all parameters expected by the receiving device.

Format:
`http://<Ip/Hostname>/<request>?Parameter1&Parameter2&ParameterN`

For devices which require authentication with user name and password, enable User authentication and fill in the corresponding fields.

TCP messages

When sending TCP messages the Web-IO functions like a TCP client. When initiating the action it opens a TCP connection to the specified TCP server address on the specified port, transmits the message and clear text, and then immediately closes the connection. Any replies from the server are ignored and discarded.

UDP messages

To be able to send UDP messages UDP-Sockets must be enabled in UDP-Sockets ASCII-Mode under Communication paths >> Socket-API.

When sending UDP messages the Web-IO functions as a UDP peer. The message is transmitted in the form of a UDP datagram to the specified UDP peer address on the specified port. Any replies from the server are ignored and discarded.

Syslog messages

IP address and host name of the syslog server, as well as the message texts can be freely configured.

To be able to send syslog messages Syslog must be enabled under Communication paths >> Syslog. All other parameters set4table there are not relevant to sending of syslog messages.

FTP messages

The Web-IO can save message texts per FTP to a file.

To do this FTP support must first be enabled under Communication paths >> FTP and access to the FTP server must be configured.

The file name, message and clear texts can be freely formulated.

The options are used to distinguish whether STOR is used for each initiated action to completely overwrite the file or whether APPEND is used to append the message and clear texts continuously to the file.

Switching outputs

When switching outputs the Web-IO differentiates between switching its own outputs or switching the outputs on another Web-IO.

Switching the own outputs

The output can be switched to ON or OFF. Another possibility is to change the existing state.

Switching the outputs on another Web-IO

Here either a particular or multiple outputs can be switched.

Specify the IP address for which Web-IO should have its outputs switched. As TCP port specify the port which is set for the destination Web-IO as access for the browser. If the destination Web-IO is password protected, this must also be entered.

For the destination Web-IO Allow HTTP requests must be enabled (Communication paths >> Web-API) and the controlled outputs for switching from the browser and HTTP must be enabled.

The outputs on older model Web-IOs (#57630, #57631, #57634 und #57637) can also be switched. In this case the HTTP port of the Web-IO must be specified as the TCP port. The outputs must be set in Output Mode Menu.

Switching outputs as an action offers many interesting application possibilities.

Point-to-Point connection

Similar to box-to-box connections where the inputs on Web-IO A are mapped 1:1 to the outputs on Web-IO B, the switching state of the input can be mapped to any desired output on another Web-IO.

Point-to-Multipoint

By creating multiple actions which use the input as initiator, correspondingly more outputs on different Web-IOs can be controlled.

10. Access from your own applications

In addition to the numerous standardized access possibilities, the Web-IO also offers the option of accessing from your own application.

This can be done either using TCP/IP sockets from the common high-level languages – but it is also possible to use common Web techniques such as AJAX or PHO to communicate with the Web-IO.

Access using TCP/IP sockets

The Web-IO offers three ways to access using TCP/IP sockets:

- Command strings ASCII
- Binary structures BINARY
- HTTP requests AJAX

Command strings ASCII

The input and counter can be read and the output set by exchanging simple command strings.

Depending on the configuration the Web-IO operates in this mode as a TCP server or UDP peer.

A list of the supported commands and additional details on access via ASCII sockets can be found in the Web-IO programming manual. (download at http:www.WuT.de). Follow the Manual link on the data sheet page of your Web-IO.

TCP server

To access the Web-IO as a TCP server using ASCII sockets, enable TCP ASCII-Sockets under Communication paths >> Socket-API. Specify on which server port the Web-IO should accept connections. The Web-IO can provide up to four TCP connections on the specified port at the same time – any additional connection attempt is rejected.

If the Web-IO receives no valid command within 30 seconds, it closes the connection and is then free again to open a new connection. The Web-IO behaves the same way when a defective or unknown command is received.

Reading the input is generally done by polling. Event-driven processing is only possible after configuring the input trigger correspondingly.

UDP peer
To access the Web-IO via UDP using ASCII sockets, enable UDP ASCII-Sockets under Communication paths >> Socket-API. Specify on which local UDP port the Web-IO should accept datagrams.

Using Remote UDP-Port you can specify to which UDP port of the requestor the replies from the Web-IO should be sent. Entering AUTO means that the replies go to the port which is entered as the sending port in the received datagram.

Reading the inputs is possible only using polling. Event-driven processing can be achieved by adding a corresponding action (see Actions section).

Binary structures BINARY

The Web-IO provides for binary structures for various functions such as reading the input, setting the output etc. Access is only by exchanging these structures.

In this mode the Web-IO can work as a TCP client, TCP server or UDP peer. Access can be password protected.

Four binary accesses are available which can be enabled and configured independently of each other under Communication paths >> Socket-API.

In TCP server mode only one client can connect to the corresponding binary access at a time. Any other connection attempt is rejected.

A detailed description of the supported HTTP binary structures and more details about access using BINARY sockets can be found in the Web-IO programming manual (download at http://www.WuT.de*). Follow the* Manual *link on the data sheet page of your Web-IO.*

HTTP request

In addition to traditional socket accesses the Web-IO can also be addressed directly via HTTP using HTTP requests.

By default this access is blocked and must first be enabled using Communication paths >> Web-API.

A detailed description of the supported HTTP requests and more details about access using Web techniques such as AJAX and PHP can be found in the Web-IO programming manual (download at http://www.WuT.de*). Follow the* Manual *link on the data sheet page of your Web-IO.*

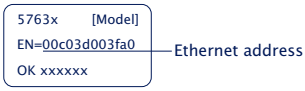
11. Appendix

Alternatives for IP address assignment

For cases where IP address assignment cannot be done via DHCP using the Wutility tool the Web-IO offers another possibility.

Assigning the IP address using the ARP command
This method can be used when the Web-IO does not yet have an IP address and the entry is 0.0.0.0. Another prerequisite is that the Web-IO and computer are in the same network segment.

Read the Ethernet address of the Web-IO from the sticker on the side of the housing:



Now use the following command line from the ARP table of the computer to enter a static entry:

```
arp -s [IP-Adresse]  [MAC-Adresse]
```

Example under Windows:
```
arp -s 10.40.72.15 00-C0-3-00-3F-A0
```

Example under SCO UNIX:
```
arp -s 10.40.72.15 00:C0:3D:00:3F:A0
```

Then start the Web browser and enter

```
http://<IP-Adresse>
```

In Windows environments IP addresses may only be entered without leading zeros.

The Web-IO accepts the IP address of the first network packet sent to its Ethernet address as its own and saves it in non-volatile memory. The Web page of the Web-IO is then loaded and all other settings can now be made conveniently using

Web-based Management.

Firmware update

The Web-IO firmware is continually improved to meet the new requirements of ever growing networks.

The current firmware for your Web-IO can be found at http://WuT.de by entering in your search the article number of your Web-IO and selecting Firmware.

To load the firmware update you need a Windows PC with the WuTility tool installed (found in the firmware archive) and unimpeded network access to the Web-IO.

Start Wutility, highlight your Web-IO in the inventory list and click on Firmware in the icon bar. Select the corresponding UHD file. WuTility will guide you through the update process.

Do not interrupt either power or the network connection during the update.

All the settings in the Web-IO are retained and the Web-IO should be immediately ready to use following the update.

Security advice

The following sections contain information and recommendations relevant from the point of view of IT security for commissioning, configuration, operation and maintenance of the Web IO models described in these instructions.

Function and typical application

Web-IOs offer the possibility to transmit or control the states of electrical switching signals via an Ethernet connection within higher protocol instances.

All Web-IO models are based on W&T's own operating system and ar free of open-source components and third-party software at their core. Out of the box, Web IOs are designed to operate in a secure network environment.

The factory settings focus on providing the lowest possible latency and therefore unsecured configuration access via HTTP.

In insecure network environments and/or with increased security requirements, ad-

ditional measures must be taken to prevent unauthorized access.

With the exception of the display in the browser, all other access options to the inputs and outputs are disabled.

Requirements for integrators and operators

Depending on the individual network environment and the security requirements, the factory settings for operational use must be checked from a security perspective. Changes and/or additional measures may be required by the integrator or operator.

These include in particular:

- Selection of a secure password in terms of length and composition
- Deactivation of unneeded services and/or access restrictions through an upstream external firewall.
- Installation of an individual device certificate within a PKI environment.
- Protection of the Web IOs against unauthorized physical access

Further details on this can be found in the following of this chapter as well as in the previous descriptions of the individual operating modes.

Installation location

Der Installationsort des Web-IOs muss gewährleisten, dass keine unauthorisierten physikalischen Zugriffe erfolgen können (z.B. geeignet gesicherter Raum, Schaltschrank etc.). Ein physikalischer Zugriff auf das Web-IO birgt z.B. folgende Risiken:

- Decommissioning of the device (removing network cable, power supply ...) and loss of all connections to communication partners.
- Depending on the model, reset to factory settings by pressing and holding the reset button.

Startup

The commissioning of the Web IO is divided into the assignment of the IP address (DHCP, WuTility, static ARP entry, depending on the model serial port) and the subsequent further configuration via Web-Based-Management. With the factory setting, all configuration services are freely accessible. Commissioning must therefore be carried out in such a way that no unauthorized access can take place until the sys-

tem password has been assigned and a secure configuration has been established.

A suitable measure is, for example, to perform commissioning via a point-to-point connection with the configuring computer. Only then is the Web IO then connected to the actual target network.

Password

Operational use of the Web IO without a password should not take place. The password is the central protection against unauthorized access to the configuration and management of the Web IO. Depending on the selected communication path, the password also protects access to the inputs and outputs

We recommend the use of a secure password with a length of at least 15 characters, consisting of upper and lower case letters, numbers and special characters (not allowed are &, # and /)

The system password is transferred to the Web IO in plain text for WBM access via HTTP. The transmission is only encrypted during configuration via HTTPS.

For password-protected access from supposedly insecure or public networks, additional measures such as the use of a VPN tunnel must be taken.

Registration for safety-related information

Devices can be registered with W&T via the WuTility inventory tool. In the event of security-relevant updates and/or information, we will notify you immediately by email.

In addition to the personal data provided, device-specific data is also stored during registration.

Operation and configuration

Ex works, all accesses or communication paths are deactivated except for browser access.

We recommend activating only those communication channels and services that are actually required for operation.

An overview of the possible communication channels can be found in the following

table.

Communication path / protocol	Connection type	Active in factory defaults	Local port	Configurable	Remoteport	Configurable	Password-protected	unencrypted transfer
Wutility Inventory	UDP	X	8513	X	dynamic			
Wutility IP Assignment	UDP	X	68		67		X	X
DHCP	UDP	X	68		67			
HTTP	TCP-Server	X	80	X	dynamic		X	X
HTTPS	TCP-Server		443	X	dynamic		X	
DNS	UDP	X	dynamic		53			
NTP	UDP	X	dynamic		123			
Geräte-Reset	TCP-Server	X	8888	X	dynamic		X	X
Device update initialization	TCP-Server		8002	X	dynamic		X	X
Device update firmware data	UDP		69		dynamic		X	X
Mail	TCP-Client		dynamic		587	X	X	
Box-to-Box 1 Master	TCP-Client		dynamic	X	49157	X	X	
Box-to-Box 1 Slave	TCP-Server		49157	X	dynamic		X	
Box-to-Box 2 Master	TCP-Client		dynamic	X	49158	X	X	
Box-to-Box 2 Slave	TCP-Server		49158	X	dynamic		X	
MQTT	TCP-Client		dynamic		1883	X	X	X
SMQTT	TCP-Client		dynamic		8883	X	X	
REST (HTTP)	TCP-Server		80	X	dynamic		X	X
REST (HTTPS)	TCP-Server		443	X	dynamic		X	
Web-API (HTTP)	TCP-Server		80	X	dynamic		X	X
Web-API (HTTPS)	TCP-Server		443	X	dynamic		X	
TCP-ASCII-Socket Server	TCP-Server		42280	X	dynamic		X	X
UDP-ASCII-Socket Peer	UDP-Peer		42279	X	dynamic	X	X	X
BINARY 1 TCP Sockets	TCP-Client		dynamic	X	49153	X	X	
BINARY 1 TCP Sockets	TCP-Server		49153	X	dynamic		X	
BINARY 1 TCP Sockets	UDP-Peer		45889	X	45889	X		
BINARY 2 TCP Sockets	TCP-Client		dynamic	X	49154	X	X	

Communication path / protocol	Connection type	Active in factory defaults	Local port	Configurable	Remoteport	Configurable	Password-protected	unencrypted transfer
BINARY 2 TCP Sockets	TCP-Server		49154	X	dynamic		X	
BINARY 2 TCP Sockets	UDP-Peer		45890	X	45890	X		
BINARY 3 TCP Sockets	TCP-Client		dynamic	X	49155	X	X	
BINARY 3 TCP Sockets	TCP-Server		49155	X	dynamic		X	
BINARY 3 TCP Sockets	UDP-Peer		45891	X	45891	X		
BINARY 4 TCP Sockets	TCP-Client		dynamic	X	49156	X	X	
BINARY 4 TCP Sockets	TCP-Server		49156	X	dynamic		X	
BINARY 4 TCP Sockets	UDP-Peer		45892	X	45892	X		
Modbus-TCP	TCP-Server		502	X	dynamic			
OPC DA	TCP-Server		49159	X	dynamic		X	
OPC UA	TCP-Server		4840	X	dynamic		X	
SNMP V1	UDP-Peer		161		dynamic			
SNMP V2	UDP-Peer		161		dynamic		X	X
SNMP V3	UDP-Peer		161		dynamic		X	
SNMP-Trap	UDP-Peer		161		162	X		
SYSLOG	UDP-Peer		dynamic		514	X		
FTP control connection	TCP-Client		dynamic		21	X	X	X
FTP data connection (active)	TCP-Server		dynamic		dynamic			
FTP data connection (passive)	TCP-Client		dynamic		dynamic			
HTTP-Request (Actions)	TCP-Client		dynamic		80	X	X	X
HTTPS-Request (Actions)	TCP-Client		dynamic		443	X	X	
TCP-Message (Actions)	TCP-Cleint		dynamic		8000	X		
UDP-Message (Actions)	UDO-Peer		dynamic		8500	X		
Accesses for the Com-Server function (only 57731)								
Com-Server configuration (Telnet)	TCP-Server	X	1111	X	dynamic		X	X
Socket access serial data	TCP-Server	X	8000	X	dynamic			
Control access serial port	TCP-Server	X	9094	*	dynamic		X	X
Port reset	TCP-Server	X	9084	X	dynamic			
Configuration download	TCP-Server	X	8003		dynamic		X	X
Configuration upload	TCP-Server	X	8004		dynamic		X	X

Communication path / protocol	Connection type	Active in factory defaults	Local port	Configurable	Remoteport	Configurable	Password-protected	unencrypted transfer
Telnet	TCP-Server		6000	X	dynamic			
Telnet	TCP-Client		dynamic		0	X		
FTP	TCP-Server		7000	X	dynamic			
FTP	TCP-Client		dynamic		0	X		
Socket Client serial data	TCP-Client		dynamic		0	X		
Socket UDP Peer serial data	UDP-Peer		8000	X	0	X		
Socket for InQueueCopy	TCP-Server		0	X	dynamic			

The control port for serial access must always be 1094 higher than the TCP port configured for serial socket access.

Configuration via HTTPS / PKI environments if possible

The TLS protocol used by HTTPS provides encrypted and authenticated access to the web interface of the web IO. This also applies to access via the Web API and the rest access. To protect the exchanged configuration data, commands and the system password, we recommend activating HTTPS especially in insecure network environments. As protection against man-inthe-middle attacks, the self-signed default certificate should also be replaced by an individual, own certificate.

Encrypted communication

The hardware platform of the Web-IO combines low latency with low power consumption. As a result, the key length of the possible certificates is limited to 1024 bits and the Web IO supports TLS1.2 at most. In applications with higher requirements, additional measures may have to be taken (e.g. VPN).

TLS encrypted communication is possible in the following operating modes:

- HTTPS (Browser)
- HTTPS (Web-API)
- HTTPS (REST)
- MQTT (SMQTT)
- Mailing
- OPC UA

The computationally intensive TLS encryption functions can have an impact on the latencies of data transmission. For time-critical switching and acquisition tasks, protocols should therefore be tested for their compatibility with HTTPS accesses. This includes, in particular, any security scans in the network. In some cases, these open a large number of TLS connections within a short time and can thus lead to interruptions or timeouts of the data traffic.

Islanding of the subnet via router/firewall

For applications that communicate unencrypted with the Web IO, the communication partners (e.g. Web IO and PC) should be isolated in a separate network segment via a firewall to protect against spying. For example, with the aid of a W&T Microwall, this also protects the communication partners from damaging events (broadcast storms, overloads, etc.) in the main network.

Appropriate firewall rules limit cross-network access to the minimum necessary.

Firmware updates

W&T publishes firmware updates for the Web IOs in order to eliminate functional errors, possibly discovered vulnerabilities or also to extend functions.

The upload to the device is done with the help of the WuTility management tool.

Update files always contain the entire firmware or the entire system of the Web IO. For this reason, firmware updates are always associated with a restart of the Web IO and thus also an interruption of the operational mode. Individual configuration data (IP parameters, firewall rules, etc.) are not affected by a firmware update and are retained.

The Web IOs are based on S&T's own operating system and do not contain any third-party components at their core (e.g. Linux, external TCP stacks, etc.). Compromise with common malicious code existing for these systems is therefore not possible.

The firmware is uploaded via TFTP (UDP) and the system password is transmitted in plain text on the network side during this process. In insecure networks or in environments with increased security requirements, additional external measures are therefore required (e.g. VPN).

For more details on a firmware update, refer to the Firmware Update chapter.

Service, maintenance and decommissioning

Despite high quality standards, electronics can fail at any time, e.g. due to external events. Depending on the availability requirements of the respective application, we recommend taking appropriate precautions.

- Backup/storage of the device configuration
- If necessary, provision of a replacement device
- Documentation of the procedure for device replacement

During decommissioning, all confidential information stored in the Web IO (IP ranges, external access data, etc.) should be reset to the factory settings to protect them. This can be done either via the web-based management or via hardware by pressing and holding the reset button or the device-internal jumper.

Emergency access

In case you have forgotten the passwords for the Web-IO or simply want to reset the device to its factory default settings, there are emergency accesses. In this case you need physical access to the device.

Deleting the password

Use a pointed object to press the reset button recessed in the housing front. Hold down the reset button until all the status LEDs begin to flash slowly. Now release the button.

By entering the IP address of the Web-IO as the URL in the browser you are taken to an emergency access Web page where you are offered the option of resetting the passwords.

Resetting to factory defaults

Use a pointed object to press the reset button recessed in the housing front. Hold down the reset button until all the status LEDs begin to flash slowly and after a while flash faster. Now release the button.

The Web-IO is now in its factory default state.

12. Technical Data

#57732

General data	
Housing:	Plastic enclosure 90 x 45 x 56 mm (LxWxH)
Weight:	approx. 140g
IP enclosure rating:	IP 20
Installation orientation:	any
Fastening / mounting:	DIN rail 35mm
Battery:	CR 1632
Battery life:	min. 10 years
Ambient conditions	
Working temperature range:	0°C - 40°C
Storage temperature range:	-25°C - 70°C
Relative humidity:	5..95% rH (non-condensing)
Pollution degree:	2
Operating altitude:	0 .. 2000m above sea level
Ventilation:	No external ventilation required

Electrical data	
Supply voltage:	110 - 230V AC, 50/60Hz
Current draw:	150 - 50 mA
Over-voltage category:	Category II
Protection class:	I
Galvanic isolation:	Digital output - Network: min. 2000 V Digital input - Network: min. 2000 V
Digital outputs:	One relay potential-free contact AC1: 16 A / 250 V AC AC15: 3 A / 120 V 1.5 A / 240 V AC3: 750 W max. 1800 switching cycles per hour
Digital inputs:	One digital input, max. input voltage 250V AC 50/60Hz Switching threshold 80V +/- 10V Integrated 32-bit pulse counter
Network:	10/100BaseT autosensing
Connections	
Network:	RJ45
IO and power:	8x screw terminal, 5mm spacing
Connectable wires:	Solid conductor: 0.2 – 4,0 mm2 Stranded: 0.2 – 2.5 mm2 Lead with end ferrule: 0.25 – 2.5 mm2 Only one conductor per clamp!
Screw tightening torque:	0,5 .. 0,6 Nm
Displays	
LED:	Power Network status Digital I/O states

#57832

General data	
Housing:	Plastic enclosure 90 x 45 x 56 mm (LxWxH)
Weight:	approx. 140g
IP enclosure rating:	IP 20
Installation orientation:	any
Fastening / mounting:	DIN rail 35mm
Battery:	CR 1632
Battery life:	min. 10 years
Ambient conditions	
Working temperature range:	0°C - 40°C
Storage temperature range:	-25°C - 70°C
Relative humidity:	5..95% rH (non-condensing)
Pollution degree:	2
Operating altitude:	0 .. 2000m above sea level
Ventilation:	No external ventilation required
Electrical data	
Supply voltage:	110 - 230V AC, 50/60Hz
Current draw:	150 - 50 mA
Over-voltage category:	Category II
Protection class:	I
Galvanic isolation:	Digital output - Network: min. 2000 V
Digital outputs:	One relay potential-free change over contact One relay potential-free normaly open contact AC1: 16 A / 250 V AC AC15: 3 A / 120 V 1.5 A / 240 V AC3: 750 W max. 1800 switching cycles per hour

Network:	10/100BaseT autosensing
Connections	
Network:	RJ45
IO and power:	8x screw terminal, 5mm spacing
Connectable wires:	Solid conductor: 0.2 – 4,0 mm2 Stranded: 0.2 – 2.5 mm2 Lead with end ferrule: 0.25 – 2.5 mm2 Only one conductor per clamp!
Screw tightening torque:	0,5 .. 0,6 Nm
Displays	
LED:	Power Network status Digital I/O states

#57838

General data	
Housing:	Plastic enclosure 90 x 116 x 56 mm (LxWxH)
Weight:	approx. 330g
IP enclosure rating:	IP 20
Installation orientation:	any
Fastening / mounting:	DIN rail 35mm
Battery:	CR 1632
Battery life:	min. 10 years
Ambient conditions	
Working temperature range:	0°C - 40°C
Storage temperature range:	-25°C - 70°C
Relative humidity:	5..95% rH (non-condensing)
Pollution degree:	2
Operating altitude:	0 .. 2000m above sea level
Ventilation:	No external ventilation required
Electrical data	
Supply voltage:	110 - 230V AC, 50/60Hz
Current draw:	150 - 50 mA
Over-voltage category:	Category II
Protection class:	I
Galvanic isolation:	Digital output - Network: min. 2000 V

Digital outputs:	Four relay potential-free change over contact Four relay potential-free normaly open contact AC1: 16 A / 250 V AC AC15: 3 A / 120 V 1.5 A / 240 V AC3: 750 W max. 1800 switching cycles per hour
Network:	10/100BaseT autosensing
Connections	
Network:	RJ45
IO and power:	one 3x screw terminal, 5mm spacing (Power) two 11x screw terminal, 7,5mm spacing (IOs)
Connectable wires:	Solid conductor: 0.2 – 2,5 mm2 Stranded: 0.2 – 2.5 mm2 Lead with end ferrule: 0.25 – 2.5 mm2 Only one conductor per clamp!
Screw tightening torque:	0,5 .. 0,6 Nm
Displays	
LED:	Power Network status Digital I/O states

General data

Data transmission:	
Protocols:	TCP- and UDP- Sockets, Client and Server SNMP incl. traps SMTP email sending OPC server Modbus-TCP Inventorying, group management
Response times:	Data and switching: typ. 40ms

Wiesemann & Theis GmbH
Porschestraße 12
D-42279 Wuppertal

Mail info@wut.de
Web www.wut.de

Tel. +49 (0)202 2680-110
Fax +49 (0)202 2680-265