

W&T

www.WuT.de

Anleitung

Inbetriebnahme und Anwendung

Web-IO Digital 4.0 Relais

gültig für folgende Web-IO 4.0 Modelle:

#57150	Web-IO 4.0 Digital 2xIn, 2xRelay Out
#57151	Web-IO 4.0 Digital 4xRelay Out
#57738	Web-IO 4.0 Digital 12xIn, 8xRelay Out

Release 1.72 05/2025

© 05/2025 by Wiesemann und Theis GmbH

Microsoft und Windows sind eingetragene Warenzeichen der Microsoft Corporation.

Irrtum und Änderung vorbehalten:

Da wir Fehler machen können, darf keine unserer Aussagen ungeprüft verwendet werden. Bitte melden Sie uns alle Ihnen bekannt gewordenen Irrtümer oder Missverständlichkeiten, damit wir diese so schnell wie möglich erkennen und beseitigen können.

Führen Sie Arbeiten an bzw. mit W&T Produkten nur aus, wenn sie hier beschrieben sind und Sie die Anleitung vollständig gelesen und verstanden haben. Eigenmächtiges Handeln kann Gefahren verursachen. Wir haften nicht für die Folgen eigenmächtigen Handelns. Fragen Sie im Zweifel lieber noch einmal bei uns bzw. bei Ihrem Händler nach!

Inhalt

1. Rechtliche Hinweise.....	5
Warnhinweiskonzept	5
Qualifiziertes Personal.....	5
Entsorgung.....	6
Symbole auf dem Produkt	6
2. Sicherheitshinweise.....	7
Allgemeine Hinweise.....	7
Elektrische Sicherheit	7
Batterien.....	9
3. Schnellinbetriebnahme.....	11
Netzwerkanschluss	11
Stromversorgung	11
IP-Adressvergabe	11
Funktionstest	11
4. Produktvorstellung	12
Hardware-Ausstattung	12
Netzwerksicherheit	13
Zugriffsrechte.....	14
Anwendungs- und Zugriffsmöglichkeiten.....	15
Aktionen	16
5. Montage und Verdrahtung.....	17
#57750 - Web-IO Digital 2xIn, 2xRelay Out.....	17
#57751 - Web-IO Digital 4xRelay Out.....	21
#57738 - Web-IO Digital 12xIn, 8xRelais Out.....	24
6. Inbetriebnahme	30
Vergabe der IP-Adresse	30

Ändern der eingestellten IP-Parameter	31
7. Grundeinstellungen.....	32
Inputs und Outputs konfigurieren.....	32
Datum / Uhrzeit.....	33
Sprache / Infos.....	33
Passwort	33
Zertifikate.....	34
8. Basisanwendungen	35
Browser-Zugriff	35
E-Mail-Versand.....	37
Box-to-Box.....	38
9. Integration in bestehende Systeme.....	39
MQTT.....	39
REST 41	
OPC DA.....	45
OPC UA.....	46
SNMP	48
Modbus -TCP	49
10. Aktionen	55
Auslöser	55
Aktionen	57
11. Zugriff aus eigenen Anwendungen.....	62
Zugriff über TCP/IP-Sockets	62
12. Anhang.....	65
Alternativen bei der IP-Adressvergabe	65
Firmware-Update.....	66
Security-Hinweise.....	66
Notzugang.....	73
Bedeutung der Status-LEDs	74
13. Technische Daten	75

1. Rechtliche Hinweise

Warnhinweiskonzept

Diese Anleitung enthält Hinweise, die zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachtet werden müssen. Die Hinweise sind durch ein Warndreieck hervorgehoben. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt:

GEFAHR

kennzeichnet eine Gefährdung, die Tod oder schwere Körperverletzung zur Folge hat, wenn keine entsprechende Vorsichtsmaßnahmen getroffen werden.

WARNUNG

kennzeichnet eine Gefährdung, die Tod oder schwere Körperverletzung zur Folge haben kann, wenn keine entsprechende Vorsichtsmaßnahmen getroffen werden.

VORSICHT

kennzeichnet eine Gefährdung, die eine leichte Körperverletzung zur Folge haben kann, wenn keine entsprechende Vorsichtsmaßnahmen getroffen werden.

ACHTUNG

kennzeichnet eine Gefährdung, die Sachschaden zur Folge haben kann, wenn keine entsprechenden Vorsichtsmaßnahmen getroffen werden.

Bei Vorliegen mehrerer Gefährdungsstufen wird immer der Warnhinweis der jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das in dieser Anleitung beschriebene Produkt darf nur von Personal installiert und in Betrieb genommen werden, das für die jeweilige Aufgabenstellung qualifiziert ist.




Dabei muss die für die jeweilige Aufgabenstellung zugehörige Dokumentation beachtet werden, insbesondere die darin enthaltenen Sicherheits- und Warnhinweise.

Qualifiziertes Personal ist aufgrund seiner Ausbildung und Erfahrung befähigt, im Umgang mit den beschriebenen Produkten Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Entsorgung

Elektronische Geräte dürfen nicht über den Hausmüll entsorgt werden, sondern müssen einer fachgerechten Elektroschrott-Entsorgung zugeführt werden. Die im Gerät eingebaute Lithium-Mangandioxid-Knopfzelle muss getrennt entsorgt werden. *Siehe Abschnitt Batterien*

Symbole auf dem Produkt

Symbol	Erklärung
	CE-Kennzeichnung Das Produkt entspricht den Anforderungen der zutreffenden EU-Richtlinien.
	UKCA-Kennzeichnung Das Produkt entspricht den Anforderungen der zutreffenden Richtlinien des Vereinigten Königreichs (GB)
	WEEE-Kennzeichnung Das Produkt darf nicht über den Hausmüll, sondern muss gemäß den am Installations-ort gültigen Entsorgungsvorschriften für Elektroschrott entsorgt werden.

2. Sicherheitshinweise

Allgemeine Hinweise

Diese Anleitung richtet sich an den Installateur der im Handbuch beschriebenen Web-IOs und muss vor Beginn der Arbeiten gelesen und verstanden werden. Die Geräte dürfen ausschließlich durch qualifiziertes Personal installiert und in Betrieb genommen werden.

Bestimmungsgemäßer Gebrauch

GEFAHR

Die Digitalen Web-IOs von Wiesemann & Theis sind Netzwerkfernschalter mit integriertem Webserver und digitalen Ein- und Ausgängen. Sie dienen als dezentrale Schalt- und Überwachungseinheit, ansprechbar über TCP/IP-Ethernet mittels diverser Web- und Netzwerkprotokolle gemäß der vorliegenden Anleitung.

Nicht bestimmungsgemäß ist jegliche andere Verwendung oder eine Modifizierung der beschriebenen Geräte.

Elektrische Sicherheit

WARNUNG

Vor Beginn jeglicher Arbeiten am Web-IO muss die Stromzufuhr durch geeignete Maßnahmen vollständig getrennt werden. Achten Sie darauf, dass das Gerät nicht versehentlich wieder eingeschaltet werden kann!

Das Web-IO darf nur in geschlossenen und trockenen Räumen eingesetzt werden.

Das Gerät sollte keinen hohen Umgebungstemperaturen und keiner direkten Sonnenbestrahlung ausgesetzt werden, sowie nicht in der Nähe von Wärmequellen betrieben werden. Bitte beachten Sie hierzu die Einschränkungen in Hinblick auf die maximale Umgebungstemperatur.

Lüftungsöffnungen müssen frei von jeglichen Hindernissen sein. Es sollte ein Abstand von 10-15 cm des Web-IO zu benachbarten Wärmequellen eingehalten werden.

Eingangsspannung und Ausgangsströme dürfen die Nennwerte der Spezifikation nicht überschreiten.

Bei der Installation ist darauf zu achten, dass keine vagabundierende Drähte durch die Lüftungsschlitze des Web-IOs ins Innere des Gehäuses ragen. Stellen Sie sicher, dass keine einzelnen Drähte von Litzen abstehen, sich die komplette Litze in der Klemme befindet und die Schrauben der Anschlussklemmen fest angeschraubt sind. Ziehen Sie die Schrauben von unbenutzten Anschlussklemmen fest.

Das zur Versorgung der Web-IOs verwendete Netzteil muss zwingend eine sichere Trennung der Niederspannungsseite gegen das Versorgungsnetz gemäß EN62368-1 gewährleisten und „LPS“-Eigenschaft besitzen.

EMV

ACHTUNG

Zum Netzwerkanschluss der Web-IOs dürfen ausschließlich geschirmte Netzkabel verwendet werden.

Die Web-IOs erfüllen in diesem Fall die industriellen Störfestigkeits-Grenzwerte und die strengeren Emissions-Grenzwerte für Haushalt und Kleingewerbe. Daher gibt es keine EMV-begründeten Einschränkungen in Hinblick auf die Verwendbarkeit der Geräte in diesen Umgebungen.

Die vollständigen Konformitätserklärungen zu den in der Anleitung beschriebenen Geräten finden Sie über die jeweilige Internet-Datenblattseite auf der W&T-Homepage unter <http://www.wut.de>.

Batterien

Das Web-IO Digital 4.0 beinhaltet eine 3V Lithium-Mangandioxid-Knopfzelle des Typs CR 1632 zur Pufferung der internen Uhr. Diese Batterie hat eine Lebensdauer von ca. 10 Jahren und darf ausschließlich durch eine Batterie gleichen Typs ersetzt werden.

Bei Betrieb des Web-IO Digital 4.0 in einer Netzwerkumgebung mit Zugriff auf einen Time-Server ist die Batterie für die korrekte Funktion des Gerätes nicht zwingend erforderlich und kann entfernt werden.

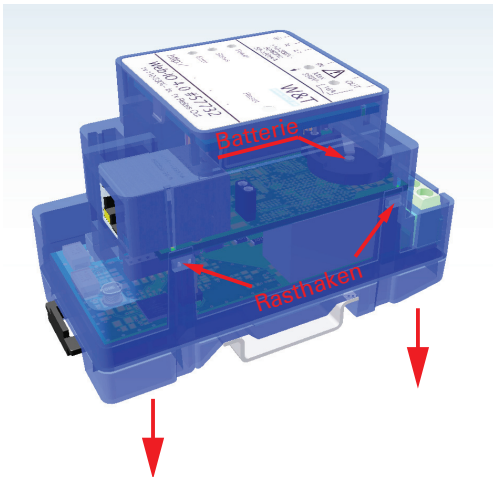
⚠ ACHTUNG

Die Batterie darf ausschließlich durch eine elektrotechnische Fachkraft ausgetauscht oder entfernt werden.

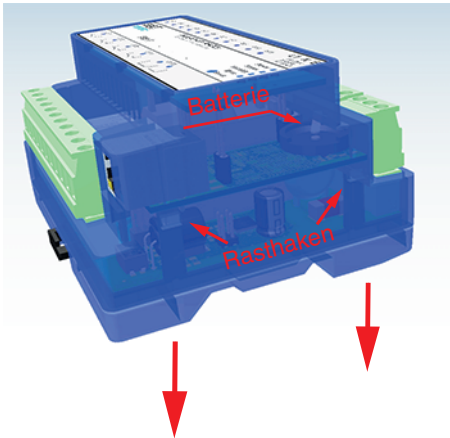
Drücken Sie mit einem spitzen Gegenstand auf die seitlichen Rasthaken der Gehäuses und ziehen Sie zeitgleich den Gehäuseboden aus der Oberschale.

Entnehmen Sie anschließend den Leiterkarten-Stapel nach unten aus dem Gehäuse.

#57150 / #57151



#57738



Auf der oberen Leiterkarte befindet sich in einer Halterung die Pufferbatterie für den Uhrenbaustein.

Nach Tausch / Entnahme der Batterie erfolgt der Zusammenbau des Gerätes in umgekehrter Reihenfolge.

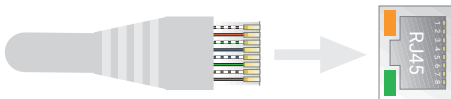
Hinweis nach dem Batteriegesetz (BattG):

Batterien und Akkus dürfen nicht im Hausmüll entsorgt werden, sondern Sie sind zur Rückgabe gebrauchter Batterien und Akkus gesetzlich verpflichtet. Altbatterien können Schadstoffe enthalten, die bei nicht sachgemäßer Lagerung oder Entsorgung die Umwelt oder Ihre Gesundheit schädigen können.

Batterien enthalten aber auch wichtige Rohstoffe wie z.B. Eisen, Zink, Mangan oder Nickel und werden wiederverwertet. Sie können die Batterien nach Gebrauch entweder an uns zurücksenden oder in unmittelbarer Nähe (z.B. im Handel oder in kommunalen Sammelstellen) unentgeltlich zurückgeben. Die Abgabe in Verkaufsstellen ist dabei auf für Endnutzer für die Entsorgung übliche Mengen sowie solche Altbatterien beschränkt, die der Vertreiber als Neubatterien in seinem Sortiment führt oder geführt hat.

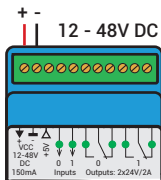
3. Schnellinbetriebnahme

Netzwerkanschluss

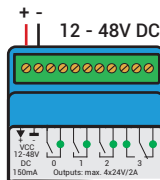


Stromversorgung

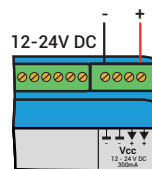
#57150



#57151



#57738



Für den ersten Test lassen Sie die Inputs und Outputs unbeschaltet.

IP-Adressvergabe

Utility-Tool installieren (Download: <https://wut.de/wutility>).

Nach dem Start von Wutility erscheint Ihr Web-IO in der Liste. Wenn mehrere Geräte angezeigt werden, identifizieren Sie Ihr Gerät über die Mac-Adresse (weißer Geräteaufkleber „EN = 00c0:3d.....“)

Befindet sich in Ihrem Netzwerk ein DHCP-Server, können Sie für einen ersten Test die zugeteilte IP-Adresse nutzen. Über das IP-Adress-Icon im WuTility können Sie dem Web-IO alternativ eine freie statische IP-Adresse zuteilen.

Funktionstest

Öffnen Sie im Browser die Webseite des Web-IO über die Adresse <http://<IP-Adresse des Web-IO>>.

4. Produktvorstellung

Hardware-Ausstattung

Die Web-IO-Geräte unterscheiden sich je nach Typ in ihrer mechanischen Ausführung und der Hardware-Ausstattung:

#57150 - Web-IO 4.0 Digital 2xIn/2xRelay Out



Netzwerkschnittstelle:

RJ45 10/100BaseT

Stromversorgung:

12 .. 48V DC oder PoE (Power over Ethernet)

Inputs:

2x Input zur Überwachung potentialfreier Kontakte

Outputs:

2x Relais. CO (Wechsler) max. 24V/2A, 48V/0,5A DC

Anzeige LEDs:

Netzwerkstatus
Gerätestatus und Fehlerstatus
Status der Inputs und Outputs

#57151 - Web-IO 4.0 Digital 4xRelay Out



Netzwerkschnittstelle:

RJ45 10/100BaseT

Stromversorgung:

12 .. 48V DC oder PoE (Power over Ethernet)

Outputs:

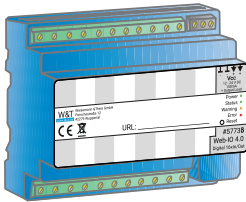
3x Relais. NO (Schließer) max. 24V/2A, 48V/0,5A DC

1x Relais. CO (Wechsler) max. 24V/2A, 48V/0,5A DC

Anzeige LEDs:

Netzwerkstatus
Gerätestatus und Fehlerstatus
Status der Inputs und Outputs

#57738 - Web-IO 4.0 Digital 12xIn, 8xRelais Out



Netzwerkschnittstelle:

RJ45 10/100BaseT

Stromversorgung:

12 .. 24V DC oder PoE (Power over Ethernet)

Inputs:

12x Inputs -30 .. +30V DC Schaltschwelle ca. +2,5V

Outputs:

4x Relais NO (Schließer) max. 24V/2A 48V/0,5A DC

4x Relais CO (Wechsler) max. 24V/2A 48V/0,5A DC

Anzeige LEDs:

Netzwerkstatus

Gerätestatus und Fehlerstatus

Status der Inputs und Outputs

Netzwerksicherheit

Das Web-IO verfügt über eine interne Firewall. Alle verfügbaren Netzwerkzugänge sind konfigurierbar und müssen vom Administrator zunächst aktiviert werden. Ab Werk sind nur der Browser-Zugang, die Inventarisierung per Wutility und der Port für die Initialisierung von Firmware-Updates freigegeben. Außerdem ist DHCP aktiviert.

Für alle Kommunikationswege kann explizit festgelegt werden, ob auf die Outputs zugegriffen werden darf.

Eine Liste der aktuell offenen TCP- und UDP-Ports finden Sie im Navigationsbaum unter *Port-Liste*.

Zugriffsrechte

Konfiguration und Bedienung des Web-IO erfolgen im Browser. Für den Zugang gibt es drei Berechtigungsstufen:

Gast

Der Gast kann ohne Login den Status von Inputs, Countern und Outputs lesend verfolgen.

Benutzer

Der Benutzer kann nach Anmeldung mit Passwort die Outputs schalten, wenn diese für den Zugriff per Browser freigegeben sind.

Administrator

Der Administrator verfügt nach Anmeldung mit Passwort über uneingeschränkte Konfigurations- und Zugriffsrechte.

Ab Werk sind beim Web-IO keine Passwörter vergeben. Es reicht ein Klick auf den Anmelde-Button.

Nach der Anmeldung können die freigegebenen Konfigurationsbereiche über den Navigationsbaum auf der linken Seite aufgerufen werden. Hilfe und Informationen zu den jeweiligen Konfigurationsmöglichkeiten bekommen Sie über die Info-Buttons auf der rechten Seite.

Über einen Klick auf den Anwenden-Button werden die vorgenommenen Einstellungen sofort wirksam.

Bei allen weiteren, die Konfiguration betreffenden Beschreibungen, wird der Zugriff mit Administratorlogin vorausgesetzt.

Anwendungs- und Zugriffsmöglichkeiten

Browser-Zugriff

Über einen passwortgeschützten Zugang können auf der Home-Seite die Zustände von Inputs, Countern und Outputs im Browser überwacht werden. Außerdem lassen sich mit den erforderlichen Zugriffsrechten die Outputs schalten.

Darüber hinaus kann eine komplett nach eigenen Bedürfnissen erstellte Webseite ins Gerät hochgeladen und gespeichert werden.

E-Mail-Versand

Das Web-IO bietet die Möglichkeit, in Abhängig von IO-Zuständen oder nach festem Intervall E-Mail-Meldungen zu versenden. Dabei unterstützt das Web-IO auch die von den öffentlichen Providern vorgeschriebenen Authentifizierungsverfahren.

Box-to-Box

Zwei Web-IOs lassen sich so konfigurieren, dass die Outputs des ersten Web-IO den Inputs des zweiten folgen. Das funktioniert bei entsprechender Konfiguration in beide Richtungen.

Integration in bestehende Systeme

Für die Integration in bestehende Systeme unterstützt das Web-IO bei entsprechender Konfiguration, die Kommunikation über einige ausgewählte Standardprotokolle.

MQTT

Im Umfeld von Industrie 4.0 und dem „Internet of Things“ ist MQTT ein innovativer Kommunikationsweg. Das Web-IO kann den Status der IOs per MQTT-Publish an einen MQTT-Broker übermitteln und per MQTT-Subscribe die Aufforderung zum Schalten entgegen nehmen.

REST

REST (Representational State Transfer) ist ein weiteres Web-basierendes Protokoll, mit dem das Web-IO optimal in das Umfeld von Industrie 4.0 und dem „Internet of Things“ integrierbar ist.

Web-API - HTTP-Requests/AJAX

Der Status von Inputs, Countern und Outputs kann über HTTP-Requests abgefragt werden. Darüber hinaus lassen sich auch die Outputs über HTTP-Requests direkt steuern.

OPC DA/OPC UA

In Verbindung mit dem W&T OPC-Server kann das Web-IO aus beliebigen OPC-Client-Anwendungen angesprochen werden.

SNMP

Sowohl der Zustand der Inputs, Counter und Outputs als auch die Konfiguration und der Fehlerstatus können über SNMP abgerufen werden. Zur einfachen Einbindung in SNMP-Systeme steht eine Private MIB zum direkten Download aus dem Gerät zur Verfügung.

Modbus-TCP

Mit Modbus-TCP unterstützt das Web-IO eines der gängigsten Industrie-Protokolle. Über das Lesen und Schreiben der entsprechenden Register können beliebige Modbus-TCP Master auf die IOs zugreifen.

Eigene Anwendungen

Für den Zugriff aus eigenen Anwendungen bietet das Web-IO TCP- und UDP-Socket-Zugänge. In beiden Fällen unterstützt das Web-IO die Ansprache mit lesbaren Kommando-Strings oder den Austausch von Binär-Strukturen.

Durch die Unterstützung von HTTP-Requests, können auch eigene Web-Anwendungen (z.B. mit PHP oder JavaScript) auf das Web-IO zugreifen.

Aktionen

Abhängig von vordefinierten Ereignissen an den IOs, kann das Web-IO Aktionen wie z.B. den Versand einer E-Mail-Meldung auslösen. Weitere Aktionen sind das Versenden von Syslog-Meldungen, SNMP-Traps oder MQTT-Publishes, das Schreiben in eine Datei via FTP, das Versenden von Daten per TCP oder UDP, bis hin zum Schalten der eigenen Outputs.

5. Montage und Verdrahtung

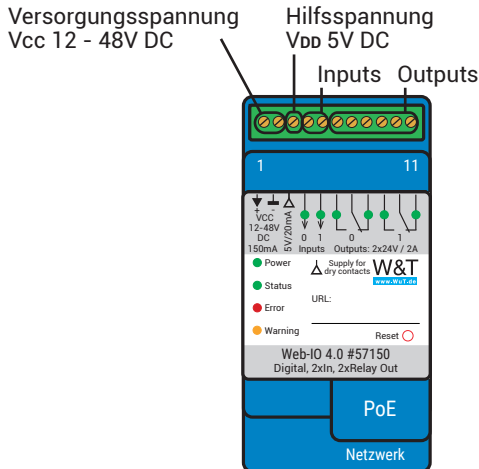
Die Montage und Verdrahtung des Web-IO sollte durch qualifiziertes Fachpersonal erfolgen. Dabei sind die allgemein gültigen Regeln der Technik und die jeweils gültigen Vorschriften und Normen zu beachten.

#57150 - Web-IO Digital 2xIn, 2xRelay Out

Montage

Das Web-IO Digital 2xIn, 2xOut ist für die Montage in Schaltschrank oder Unterverteilung vorgesehen. Zur mechanischen Fixierung sollte das Web-IO auf eine 35mm Hutschiene nach DIN EN 50022 aufgeschnappt werden. Dabei nimmt das Web-IO 46mm Breite in Anspruch.

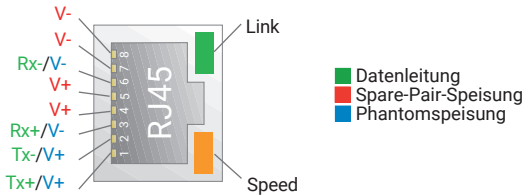
Anschlüsse



Netzwerkanschluss

Für den Netzwerkanschluss kann ein gewöhnliches Ethernet-Patchkabel (min. CAT5) mit RJ45-Steckern genutzt werden.

Bei PoE-fähiger (Power over Ethernet) Infrastruktur kann das Web-IO über den Netzwerkanschluss versorgt werden.



Anschluss der Versorgungsspannung

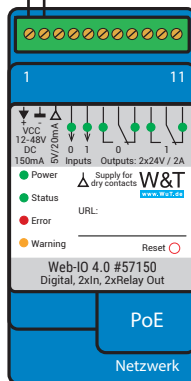
Das Web-IO wird entweder über PoE (Power over Ethernet Class 2) oder mit einer Gleichspannung zwischen 12 und 48V versorgt. Die Versorgungsspannung wird über die Klemmen 1 (+) und 2 (-) angeschlossen.

Für die externe Versorgung des Web-IO #57150 dürfen ausschließlich potentialfreie Netzteile verwendet werden. Deren Bezugsmasse für die Ausgangsspannung darf keine direkte Anbindung an den Schutzleiter haben.

Der gleichzeitige Anschluss einer externen Versorgung und einer PoE-Infrastruktur ist nicht zulässig.



Die gleichzeitige Versorgung mit einem externen Netzteil und PoE ist nicht zulässig!

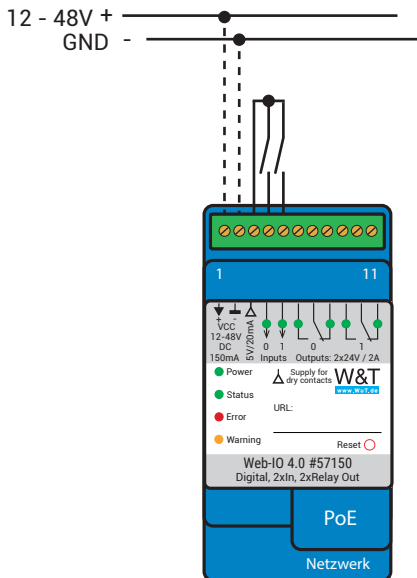


Bei einer in der Industrie typischen Spannungsversorgung von 24V nimmt das Web-IO ca. 100mA Strom auf.

Input-Verdrahtung

Die Inputs des Web-IO #57150 sind ausschließlich für die Ansteuerung über potentialfreie Kontakte ausgelegt. Dazu liefert das Web-IO auf Klemme 3 eine Hilfsspannung, die über die potentialfreien Kontakte auf die Klemmen 4 und 5 geschaltet werden kann.

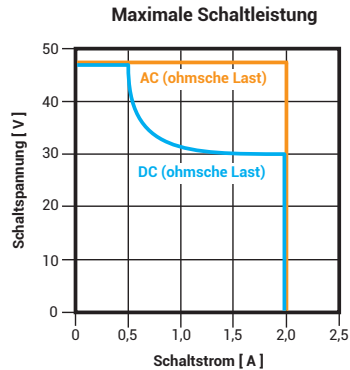
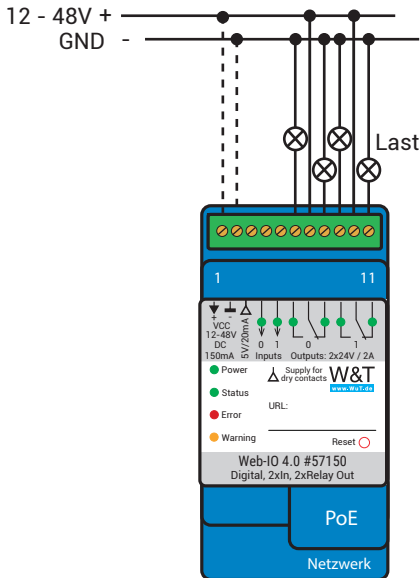
Das Ansteuern der Inputs mit Fremdspannungen ist nicht zulässig und kann das Web-IO beschädigen.



Output-Verdrahtung

Die Outputs arbeiten intern über Relais und schalten mittels potentialfreier Kontakte. Dafür stellt jeder der beiden Outputs einen Wechslerkontakt (CO) zur Verfügung.

Bei 24V können bis zu 2A AC oder DC geschaltet werden. Bei 48V beträgt der maximale Schaltstrom 500mA DC oder 2A AC.



Klemmenbelegung

Klemme	Bezeichnung / Funktion
1	+ Vcc / Geräte-Versorgung
2	- GND / Geräte-Versorgung
3	+ VDD / Hilfsspannung für Input-Ansteuerung
4	Input 0
5	Input 1
6	Output 0 NO
7	Output 0 COM
8	Output 0 NC
9	Output 1 NO
10	Output 1 COM
11	Output 1 NC

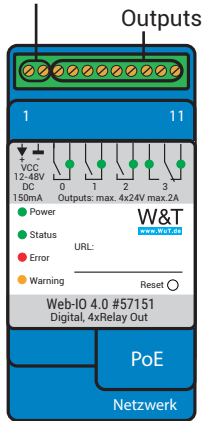
#57151 - Web-IO Digital 4xRelay Out

Montage

Das Web-IO Digital 4xRelay Out ist für die Montage in Schaltschrank oder Unterverteilung vorgesehen. Zur mechanischen Fixierung sollte das Web-IO auf eine 35mm Hutschiene nach DIN EN 50022 aufgeschnappt werden. Dabei nimmt das Web-IO 46mm Breite in Anspruch.

Anschlüsse

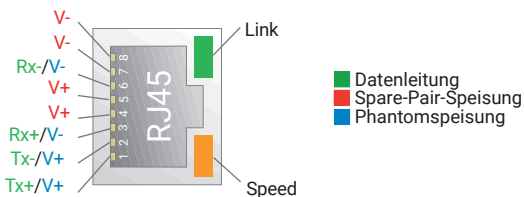
Versorgungsspannung
Vcc 12 - 48V DC



Netzwerkanschluss

Für den Netzwerkanschluss kann ein gewöhnliches Ethernet-Patchkabel (min. CAT5) mit RJ45-Steckern genutzt werden.

Bei PoE-fähiger (Power over Ethernet) Infrastruktur kann das Web-IO über den Netzwerkanschluss versorgt werden.

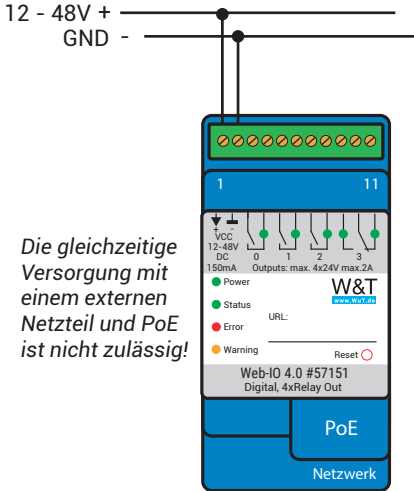


Anschluss der Versorgungsspannung

Das Web-IO wird entweder über PoE (Power over Ethernet Class 2) oder mit einer Gleichspannung zwischen 12 und 48V versorgt. Die Versorgungsspannung wird über die Klemmen 1 (+) und 2 (-) angeschlossen.

Für die externe Versorgung des Web-IO #57150 dürfen ausschließlich potentialfreie Netzteile verwendet werden. Deren Bezugsmasse für die Ausgangsspannung darf keine direkte Anbindung an den Schutzleiter haben.

Der gleichzeitige Anschluss einer externen Versorgung und einer PoE-Infrastruktur ist nicht zulässig.

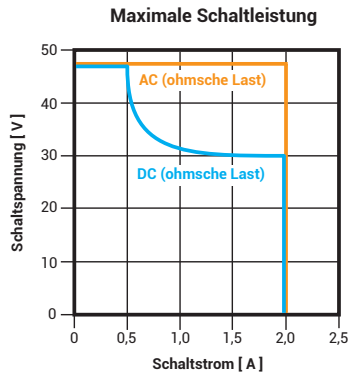
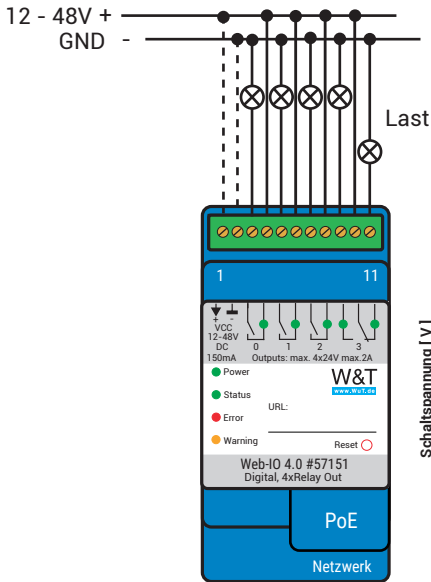


Bei einer in der Industrie typischen Spannungsversorgung von 24V nimmt das Web-IO ca. 100mA Strom auf.

Output-Verdrahtung

Die Outputs arbeiten intern über Relais und schalten mittels potentialfreier Kontakte. Dafür stellen die Outputs 0 - 2 jeweils einen Schließkontakt (NO) und Output 3 einen Wechslerkontakt (CO) zur Verfügung.

Bei 24V können bis zu 2A AC oder DC geschaltet werden. Bei 48V beträgt der maximale Schaltstrom 500mA DC oder 2A AC.



Klemmenbelegung

Klemme	Bezeichnung / Funktion
1	+ Vcc / Geräte-Versorgung
2	- GND / Geräte-Versorgung
3	Output 0 COM
4	Output 0 NO
5	Output 1 COM
6	Output 1 NO
7	Output 2 COM
8	Output 2 NO
9	Output 3 NO
10	Output 3 COM

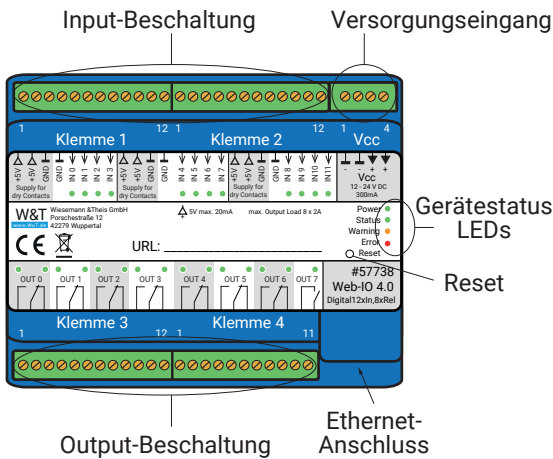
Klemme	Bezeichnung / Funktion
11	Output 3 NC

#57738 - Web-IO Digital 12xIn, 8xRelais Out

Montage

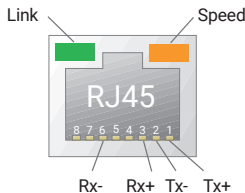
Das Web-IO Digital 12xIn, 8xRelais Out ist für die Montage im Schaltschrank vorgesehen. Zur mechanischen Fixierung sollte das Web-IO auf eine 35mm Hutschiene aufgeschnappt werden. Dabei nimmt das Web-IO 107mm Breite in Anspruch.

Anschlüsse



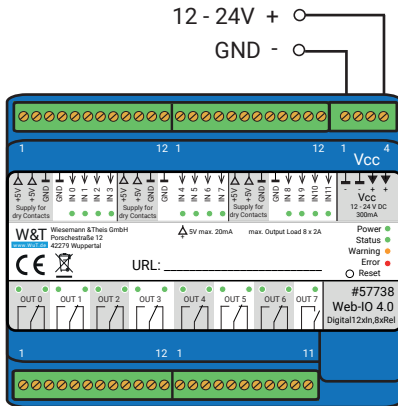
Netzwerkanschluss

Für den Netzwerkanschluss kann ein gewöhnliches Ethernet-Patchkabel (min. CAT5) mit RJ45-Steckern genutzt werden.



Anschluss der Versorgungsspannung

Das Web-IO wird über die Klemmen 1 (- GND) und 2 (+ Vcc) mit einer Gleichspannung zwischen 12 und 24V versorgt.



Versorgung wahlweise
extern über Vcc oder PoE

PoE
Power over
Ethernet



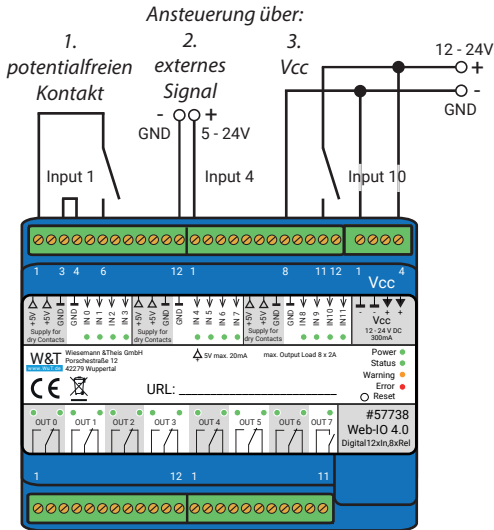
Bei einer in der Industrie typischen Spannungsversorgung von 24V nimmt das Web-IO ca. 150mA Strom auf.

Für die externe Versorgung des Web-IO #57738 dürfen ausschließlich potentialfreie Netzteile verwendet werden. Deren Bezugsmasse für die Ausgangsspannung darf keine direkte Anbindung an den Schutzleiter haben.

Der gleichzeitige Anschluss einer externen Versorgung und einer PoE-Infrastruktur ist nicht zulässig.

Input-Verdrahtung

Die 12 Inputs des Web-IO sind in 3 Gruppen a 4 Inputs angelegt. Jede der Gruppen hat eine eigene Bezugsmasse (GND). Die Gruppen sind untereinander und gegen die Innenbeschaltung des Web-IO mit 1kV galvanisch getrennt.



Die Inputs sind für Spannungen zwischen -30V und +30V ausgelegt. Positive Spannungen über +3V, bezogen auf die entsprechenden Klemmen - GND, werden als ON Signal erkannt und über die entsprechende LED signalisiert.

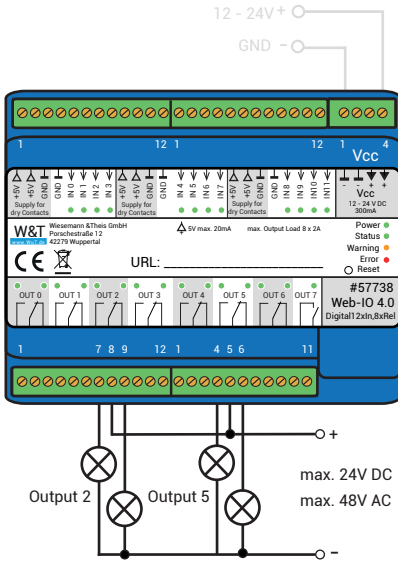
Für die Ansteuerung gibt es drei Varianten:

1. Potentialfreier Kontakt
Vdd wird über den Kontakt auf den gewünschten Input geschaltet.
Der Gruppen-GND wird mit dem internen Versorgungs-GND gebrückt.
2. Externes Spannungssignal
Spannungen größer 3V (+/-1V) bezogen auf den Gruppen-GND = ON
- 3 Vcc als Steuersignal
Vcc wird über einen Kontakt auf den gewünschten Input geschaltet.
Der Gruppen-GND wird mit dem Versorgungs-GND gebrückt.

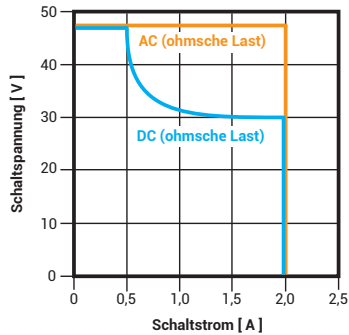
Innerhalb einer Input-Gruppe sollte nur eine Variante genutzt werden.

Output-Verdrahtung

Die Outputs sind als potentialfreie Kontakte (Schließer) realisiert und über jeweils zwei Klemmen nach außen geführt. Es können max. 24V DC oder 48V AC mit einer Last von 2A geschaltet werden.



Maximale Schaltleistung



Die Kontakte sind nicht für das Schalten von 230V ausgelegt!

Klemmenbelegung

Klemme Vcc	Bezeichnung / Funktion
1	GND / Geräte-Versorgung
2	GND / Geräte-Versorgung
3	+ Vcc - Geräte-Versorgung 12-24V 300mA@12V
4	+ Vcc - Geräte-Versorgung 12-24V 300mA@12V

Klemme 1	Bezeichnung / Funktion
1	+ Vdd - Hilfsspannung 5V 20mA für Input-Ansteuerung
2	+ Vdd - Hilfsspannung 5V 20mA für Input-Ansteuerung
3	GND / Bezugsmasse für +Vdd
4	GND / Bezugsmasse für Input-Gruppe 1
5	Input 0 - Schaltschwelle +4V
6	Input 1 - Schaltschwelle +4V

Klemme 1	Bezeichnung / Funktion
7	Input 2 - Schaltschwelle +4V
8	Input 3 - Schaltschwelle +4V
9	+ Vdd - Hilfsspannung 5V 20mA für Input-Ansteuerung
10	+ Vdd - Hilfsspannung 5V 20mA für Input-Ansteuerung
11	GND / Bezugsmasse für +Vdd
12	GND / Bezugsmasse für Input-Gruppe 2

Klemme 2	Bezeichnung / Funktion
1	Input 4 - Schaltschwelle +4V
2	Input 5 - Schaltschwelle +4V
3	Input 6 - Schaltschwelle +4V
4	Input 7 - Schaltschwelle +4V
5	+ Vdd - Hilfsspannung 5V 20mA für Input-Ansteuerung
6	+ Vdd - Hilfsspannung 5V 20mA für Input-Ansteuerung
7	GND / Bezugsmasse für +Vdd
8	GND / Bezugsmasse für Input-Gruppe 3
9	Input 8 - Schaltschwelle +4V
10	Input 9 - Schaltschwelle +4V
11	Input 10 - Schaltschwelle +4V
12	Input 11 - Schaltschwelle +4V

Klemme 3	Bezeichnung / Funktion
1	Relais Output 0 - NO
2	Relais Output 0 - COM
3	Relais Output 0 - NC
4	Relais Output 1 - NO
5	Relais Output 1 - COM
6	Relais Output 1 - NC
7	Relais Output 2 - NO
8	Relais Output 2 - COM
9	Relais Output 2 - NC
10	Relais Output 3 - NO
11	Relais Output 3 - COM
12	Relais Output 3 - NC

Klemme 4	Bezeichnung / Funktion
1	Relais Output 4 - NO
2	Relais Output 4 - COM
3	Relais Output 4 - NC
4	Relais Output 5 - NO

Klemme 4	Bezeichnung / Funktion
5	Relais Output 5 - COM
6	Relais Output 5 - NC
7	Relais Output 6 - NO
8	Relais Output 6 - COM
9	Relais Output 6 - NC
10	Relais Output 7 - NO
11	Relais Output 7 - COM

6. Inbetriebnahme

Nachdem das Web-IO ordnungsgemäß montiert und verdrahtet wurde, kann die Versorgungsspannung eingeschaltet werden. Es sollten alle drei Status-LEDs kurz aufleuchten. Nach ca. 5 Sekunden sollte nur noch die Power-LED leuchten. Die Status-LED kann ggf. blinken. Wenn an einem der Input ein gültiges Signal erkannt wird, leuchtet auch die entsprechende LED.

Bei einer funktionierenden Netzwerkverbindung signalisiert die grüne LED in der Netzwerkbuchse einen vorhandenen Link. Die orange LED gibt Auskunft über die Netzwerkgeschwindigkeit.

Ein = 100MBit/s

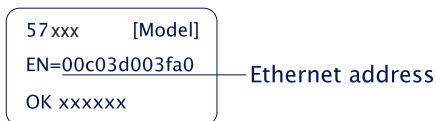
Aus = 10MBit/s

Vergabe der IP-Adresse

Im Auslieferungszustand hat das Web-IO die IP-Adresse 0.0.0.0 und DHCP ist aktiviert.

Netzwerke mit DHCP

Ist in dem Netzwerk, in dem das Web-IO angeschlossen wird, ein DHCP-Server aktiv, sollte dem Web-IO automatisch eine IP-Adresse zugeteilt werden. Um das Web-IO gezielt ansprechen zu können, sollten Sie eine Reservierung im DHCP-Server konfigurieren, damit das Web-IO immer unter derselben Adresse erreichbar ist. Die dazu benötigte Ethernet-Adresse finden Sie auf dem weißen Aufkleber am Gerät.



Fragen Sie im Zweifel den zuständigen Netzwerkadministrator

Netzwerke ohne DHCP

Installieren Sie auf einem Windows-PC das Programm WuTility (Download unter <https://www.WuT.de>). Wenn Ihnen kein Windows-PC zur Verfügung steht, lesen Sie im Anhang das Unterkapitel **Alternativen zur IP-Adressvergabe**.

Beim Start von WuTility wird das lokale Subnet durchsucht und alle gefundenen W&T-Netzwerkkomponenten werden aufgelistet. Markieren Sie Ihr Web-IO und klicken Sie das *IP-Adresse* Icon. WuTility schlägt Ihnen die Netzwerkparameter (Subnet-Mask, Gateway, DNS-Server) vor, die auch für den PC gelten. Wenn das Web-IO im gleichen Subnet arbeiten soll, wie der PC, müssen Sie lediglich die IP-Adresse anpassen.

Wenn Sie unter *Adressbereich > beliebiges Netzwerk* wählen, können Sie auch von Ihrem lokalen Netzwerk abweichende Parameter eingeben, z.B. um das Web-IO für ein anderes Netzwerk vorzukonfigurieren.

Ändern der eingestellten IP-Parameter

Um IP-Adresse, Subnet-Mask, Gateway oder DNS-Server nachträglich zu verändern, können Sie entweder erneut WuTility nutzen oder die Parameter im Browser unter *Grundeinstellungen » Netzwerk* anpassen.

7. Grundeinstellungen

Die weitere Konfiguration des Web-IO findet im Browser statt. Geben Sie als Adresse die IP-Adresse des Web-IO ein. Klicken Sie im Navigationsbaum auf *Anmelden* und wählen Sie als Benutzer Administrator. Ab Werk ist kein Passwort vergeben und es genügt ein Klick auf den Anmelde-Button, um das Web-IO mit Administratorrechten zu konfigurieren.

Inputs und Outputs konfigurieren

Im Bereich *Grundeinstellungen* » *Inputs/Outputs* können Sie den Inputs und den Outputs individuelle Benennungen. Diese Namen ersetzen dann die ab Werk vergebenen Bezeichnungen *Input n* und *Output n* in der Visualisierung und in etwaigen Meldetexten.

Erweiterte Einstellungen der Inputs

Für spezielle Anwendungen können einige Eigenschaften der Inputs angepasst werden:

Input-Filter

Ein Signalzustand muss mindestens für die hier in Millisekunden eingetragene Zeit anliegen, damit es vom Web-IO verarbeitet wird. So kann z.B. das Prellen von mechanischen Kontakten abgefangen werden.

Signal-Invertierung

Im Normalfall werden anliegende Signale mit einer Spannung über 8V als ON verarbeitet. Durch Aktivierung der Invertierung werden Spannungen unter 8V als ON und darüber liegende als OFF gewertet.

Erweiterte Einstellungen der Outputs

Für spezielle Anwendungen können einige Eigenschaften der Outputs angepasst werden:

Output invertiert schalten

Im Normalfall sind die Outputs im OFF-Zustand ausgeschaltet (also ohne Signal) und im ON-Zustand eingeschaltet. Durch Aktivierung der Invertierung, verhält sich der so konfigurierte Output genau umgekehrt.

Puls-Modus

Durch Aktivierung des *Puls* Modus fällt der Output, wenn er in den Zustand ON geschaltet wird, automatisch nach der eingestellten Pulsdauer zurück in den OFF-Zustand. Bei erneutem Einschalten während des Pulses beginnt die Pulsdauer erneut zu zählen. Mit *Rücksetzen erlaubt* wird festgelegt, dass der Output auch während eines laufenden Pulses in den OFF-Zustand geschaltet werden darf.

Datum / Uhrzeit

Im Bereich *Datum / Uhrzeit* kann festgelegt werden, ob ein zyklischer Abgleich mit einem Time-Server erfolgen soll. Darüber hinaus können Datum und Uhrzeit auch manuell eingestellt werden. Auch die Konfiguration einer Zeitzone und der Sommer-/Winterzeitvorgaben lässt sich hier vornehmen.

Sprache / Infos

Neben der Sprachauswahl Deutsch oder Englisch können hier weitere Anzeigeelemente, bis hin zum Logo, angepasst werden.

Passwort

Hier können die Passwörter für Administrator und Benutzer festgelegt werden.

Bitte beachten Sie, dass für Administrator und Operator nicht dasselbe Passwort vergeben werden darf.

Vermeiden Sie bei der Passwortvergabe die Zeichen &, ?, # sowie Umlaute und länderspezifische Sonderzeichen.

Wenn das Administrator-Passwort nicht mehr bekannt ist, wird physischer Zugriff auf das Web-IO benötigt, um die Passwörter ggf. zurückzusetzen. Siehe hierzu das Kapitel *Notzugang* im Anhang dieser Anleitung.

Zertifikate

Protokolle wie HTTPS oder OPC UA basieren auf dem TLS-Protokoll. Die Verschlüsselung der Kommunikation und die Authentifizierung der Kommunikationspartner ist hierbei über Zertifikate realisiert.

Ab Werk identifiziert sich das Web-IO mit einem selbstsignierten Zertifikat. Solche Zertifikate werden von vielen Anwendungen als Sicherheitsrisiko bewertet. Erfordert die Anwendung eine sichere Authentifizierung, muss das Web-IO mit einem individuellen, von einer vertrauenswürdigen Zertifizierungsstelle signierten Zertifikat ausgestattet werden.

Zertifikat-Signierungsanforderung (CSR)

Hier besteht die Möglichkeit ein CSR (Certificate Signing Request) mit einem neuen Schlüsselpaar und individuellem Inhalt zu erzeugen.

Mit Klick auf den Button *Überprüfen*, werden die eingegeben Werte formal geprüft und der neue Schlüssel generiert. Das neue CSR kann über den Button *CSR herunterladen* heruntergeladen werden.

Selbstsigniertes Zertifikat

Ein zuvor erzeugter individueller CSR kann durch das Gerät mit dem zum CSR gehörenden Private-Key selbst- signiert werden.

Zertifikat hochladen/Zertifikatskette hochladen

Ein zuvor erzeugter und heruntergeladener CSR kann nach der Signatur durch eine externe Zertifizierungsstelle als Zertifikat in das Gerät geladen werden. Sollte eine zum Zertifikat gehörende Zertifikatskette nicht bereits Bestandteil der Zertifikats-Datei sein, kann diese anschließend separat hochgeladen werden. Die Dateien können im PEM- oder DER-Format vorliegen.

Zertifikat/Zertifikatskette installieren

Ein zuvor hochgeladenes Zertifikat inkl. zugehöriger Zertifikatskette wird im Gerät installiert und nach dem Speichern als Zertifikat innerhalb von TLS-Verbindungen verwendet.

8. Basisanwendungen

Das Web-IO verfügt über eine Fülle verschiedener Kommunikationswege und unterstützt diverse Standardprotokolle. Wir empfehlen, nur die Kommunikationswege freizugeben, die in Ihrer Anwendung auch wirklich benötigt werden. Damit begrenzen Sie die Möglichkeit von ungewolltem Fremdzugriff und Manipulation.

Zunächst wollen wir die drei meist genutzten Kommunikationswege vorstellen:

Browser-Zugriff

Der Zugriff über den Browser hat die Besonderheit, dass neben der Überwachung und Bedienung der IOs, bei entsprechendem Login, auch die Konfiguration des Web-IO auf diesem Weg abgewickelt wird.

Dabei hat der Administrator die Berechtigung auf die gesamte Konfiguration zuzugreifen. Über den ebenfalls passwortgeschützten Benutzerzugriff können alle die IOs betreffenden Einstellungen und die Aktionen angepasst werden.

Ohne Login können nur die Zustände von Input und Output beobachtet werden.

HTTP oder HTTPS

Ab Werk ist der Browser-Zugang für HTTP über Port 80 freigegeben. Um den Zugang auf HTTPS umzustellen oder den Port zu ändern, wählen Sie im Navigationsbaum *Grundeinstellungen* » *Netzwerk* und dann im Bereich *Zugang für Webdienste* den Punkt *Protokoll*. Alle weiteren, die Anzeige im Browser betreffenden Einstellungen, können unter *Webseiten* vorgenommen werden.

Menübaum ausblenden

Wenn die Konfiguration abgeschlossen ist, kann die Anzeige im Browser auf den IO-Zugriff reduziert werden. Dazu muss unter *Webseiten* >> *Browser-Zugang* die Option *Menübaum ausblenden* aktiviert werden. Über: `http://<URL/IP des Web-IO>/index` kann der Menübaum vorübergehend eingeblendet und dann über o.g. Option auch wieder dauerhaft zugeschaltet werden.

IO-Zugriff

Für den Zugriff auf die Inputs, Counter und Outputs bietet das Web-IO zwei vorbereitete Webseiten:

Home

Die Home-Seite gibt eine Übersicht über alle IOs und die konfigurierten Aktionen. Bei entsprechendem Login können die Outputs geschaltet und der Counter gelöscht werden. Beides muss dazu zunächst unter *Webseiten » Home* freigegeben werden. Im Auslieferungszustand ist dieser verändernde Zugriff deaktiviert.

Direkter Aufruf der Home-Seite ohne Anzeige des Navigationsbaums über: *http://<URL/IP des Web-IO>/home*

Wenn die Option *Menübaum ausblenden* aktiviert ist, erscheint auf der Home-Seite ein Passworteingabefeld. Nach Klick auf den Anwenden-Button können Outputs und Counter bedient werden, bis die Home-Seite wieder verlassen wird. Durch Aktivieren der Option *Webseiten >> Home > Passwort zum Schalten im Browser speichern* wird das Passwort im Browser als Cookie gespeichert und nach Aufruf der Home-Seite im gleichen Browser ist die Bedienung sofort freigeschaltet.

Meine Webseite

Die im Web-IO vorgeladene Webseite bietet eine kompakte Übersicht der IO-Zustände.

Unter *Webseiten » Meine Webseite* kann die Original-Webseite gegen eine selbst gestaltete ausgetauscht werden.

Damit diese Webseite die Zustände von Inputs, Countern und Outputs dynamisch aktualisiert, muss unter Kommunikationswege » Web-API der Punkt HTTP-Requests erlauben aktiviert sein. Hier wird auch festgelegt, ob die Outputs über HTTP-Requests geschaltet werden dürfen.

Direkter Aufruf der eigenen Webseite ohne Anzeige des Navigationsbaums über: *http://<URL/IP des Web-IO>/user*

Weitere Details zur Programmierung eigener Webseiten finden Sie im Programmier-Handbuch zum Web-IO. (Download unter: *http://www.WuT.de* - geben Sie einfach im Suchfeld die Artikelnummer Ihres Web-IO ein und wählen Sie *Anleitung*.)

E-Mail-Versand

Um E-Mail-Meldungen zu verschicken, sind zunächst einige Grundeinstellungen nötig.

Netzwerkparameter

Wenn der Versand über einen Mailserver im Internet erfolgen soll, ist es wichtig, dass die Netzwerkgrundeinstellungen korrekt sind. Kontrollieren Sie unter *Grundeinstellungen* » *Netzwerk* insbesondere ob *Gateway* und *DNS-Server* richtig angegeben sind.

Mailserver-Zugang

Alle Mailserver-spezifischen Einstellungen können Sie unter *Kommunikationswege* » *Mail* vornehmen. Das heute übliche Authentifikationsverfahren ist SSL/TLS. Weitere Tipps zu den spezifischen Einstellungen für die gängigsten E-Mail-Anbieter finden Sie im Infobereich unter *Mail*.

E-Mail-Meldung anlegen

Um eine neue E-Mail-Meldung anzulegen, klicken Sie unter *Aktionen* den Button *Hinzufügen*. Es erscheint die Eingabemaske für eine neue Aktion.

Hier können Sie bestimmen, welchen Namen die Aktion hat und was der Auslöser sein soll, z.B. der ON-Zustand eines Inputs. Eine detaillierte Beschreibung der Möglichkeiten finden Sie im Kapitel *Aktionen*.

Als Aktion wählen Sie *E-Mail-Meldung*. In der zugehörigen Eingabemaske haben Sie die Möglichkeit, eine individuelle E-Mail-Meldung zu verfassen. Nutzen Sie hierbei die im folgenden beschriebenen Platzhalter, die beim Versand der E-Mail gegen die gerade vorliegenden IO-Zustände, Counter-Werte usw. ersetzt werden.

Platzhalter	Beschreibung
<i>x</i>	Zustand des Inputs Nr. x (ON/OFF)
<o>x</o>	Zustand des Outputs Nr. x (ON/OFF)
<c>x</c>	Zählerstand des Counters Nr. x
<i></i>	Zustand aller Inputs als hex. Bitmuster
<o></o>	Zustand aller Outputs als in hex. Bitmuster
<dn>	Device Name
<inx>	Name des Inputs Nr. x

Platzhalter	Beschreibung
<onx>	Name des Outputs Nr. x
<t>	Zeitstempel mit Datum und Uhrzeit
<\$y>	Jahr im Format "JJJJ"
<\$m>	Monat im Format "MM"
<\$d>	Tag im Format "TT"
<\$h>	Stunde im Format "hh"
<\$i>	Minuten im Format "mm"
<\$s>	Sekunden im Format "ss"
<hex: xx xx>	Beliege Bytes als hexadezimale Eingabe
<rxxxx>	Modbus-Registerwert (Kapitel Modbus-TCP)

Box-to-Box

Der Box-to-Box-Betrieb verbindet zwei Web-IOs über das Netzwerk so miteinander, dass die Outputs des einen den Inputs des anderen folgen (ON an Input 0 von Web-IO A schaltet Output 0 von Web-IO B auf ON).

Im Box-to-Box-Betrieb gilt es, ein Web-IO als Master und das andere als Slave zu konfigurieren. Das Master-Web-IO (Client) übernimmt den Verbindungsaufbau zum Slave-Web-IO (Server). Nach erfolgreichem Verbindungsaufbau, arbeiten beide Web-IOs gleichberechtigt und bei entsprechender Konfiguration werden die Schalt-signale in beide Richtungen übertragen.

9. Integration in bestehende Systeme

Das Web-IO unterstützt einige gängige Standards und Protokolle und lässt sich so einfach in viele bestehende Systeme integrieren.

MQTT

Nach Aktivierung von MQTT und Konfiguration im Menüzugriff *Kommunikationswege* » *MQTT* unterstützt das Web-IO zwei grundsätzliche Möglichkeiten:

1. MQTT mit individuellen Topics über Aktionen
2. MQTT mit W&T-Standardtopics

MQTT mit individuellen Topics

Durch Anlegen einer entsprechenden Aktion kann zum einen der Zustand von Inputs, Outputs und Countern per MQTT-Publish an einen MQTT-Broker weitergegeben werden, zum anderen kann durch MQTT-Subscribe auf konfigurierbare Topic-Inhalte das Schalten von Outputs ausgelöst werden.

Publish von IO-Zuständen

Um ein neues MQTT-Publish anzulegen, klicken Sie unter *Aktionen* den Button *Hinzufügen*. Es erscheint die Eingabemaske für eine neue Aktion.

Hier können Sie bestimmen, welchen Namen die Aktion hat und was der Auslöser sein soll.

Bestimmen Sie z.B. als Auslöser *Input0* und als Trigger *ON*.

Als Aktion wählen Sie *MQTT-Publish*. Im Folgemenü tragen Sie den Pfad ein, auf den das Topic beim Broker geschrieben werden soll.

Den textlichen Inhalt (Payload) des Topics können Sie frei bestimmen, wobei die im Infotext beschriebenen Platzhalter benutzt werden können.

Schalten von Outputs über Subscribe

Auch für diesen Fall müssen Sie eine neue Aktion hinzufügen. Als Auslöser wählen Sie *MQTT-Subscribe*. Geben Sie nun den Pfad an, über den das Topic übergeben wird, das das Schlüsselwort zum Schalten enthält. Als Aktion konfigurieren

Sie *Output schalten* » *Output dieses Web-IO schalten*. Dann bestimmen Sie noch, in welchen Zustand der Output geschaltet werden soll bzw. ob der Zustand wechseln soll.

Beispiel:

Ein beliebiges Gerät schreibt beim im Web-IO angegebenen Broker in den Pfad *wut/webio123/set0* als Topic das Schlüsselwort ON. Dieser Pfad und das Topic werden beim Web-IO als Auslöser unter *MQTT Subscribe* angegeben. Als Aktion wird das Schalten des Outputs auf *ON* bestimmt.

Mit jedem Schreiben von ON wird der Output eingeschaltet. Mit einer zweiten Aktion kann festgelegt werden, wodurch der Output wieder ausgeschaltet werden soll.

Das Web-IO als MQTT-Gateway

Durch die flexiblen Möglichkeiten, die das Web-IO bei der Konfiguration von Aktionen bietet, können abhängig vom Inhalt bestimmter Topics auch E-Mails, SNMP-Traps oder Meldungen über andere Kommunikationswege verschickt werden. Mehr dazu im Kapitel **Aktionen**.

MQTT mit W&T-Standardtopics

Für eine schnelle Integration ohne großen Konfigurationsaufwand bietet das Web-IO die Möglichkeit, von W&T vordefinierte Topics zu nutzen.

Um mit W&T-Standardtopics zu arbeiten, muss unter *Kommunikationswege* » *MQTT* grundsätzlich *MQTT* aktiviert und konfiguriert sein. Außerdem muss der Punkt *Publish und Subscribe mit W&T-Standard-Topics* aktiviert werden.

Darüber hinaus kann ausgewählt werden, welche IO-Zustände das Web-IO per *Publish* an den konfigurierten Broker senden soll und ob das Schalten der Outputs per *Subscribe* erlaubt sein soll.

Aufbau der Standardtopics

Der Aufbau des Topic-Pfades folgt immer dem gleichen Schema und setzt sich zusammen aus:

```
<Gerätenamen>/<Funktionsrichtung>/<Funktion>/<IO-Nummer>
```

Der Geräte name ist ab Werk ist so aufgebaut:

```
wut-<letzte 6 Stellen der MAC-Adresse>
```

Als Funktionsrichtung stehen *get* (für *Publish* von Änderungen an Input, Output

oder Counter) und `set` für das Schalten eines Outputs oder Löschen eines Counters zur Verfügung.

Mögliche Funktion sind `input`, `counter` oder `output`

Über die IO-Nummer, ist beginnend bei 0 vorgegeben, um welchen IO es geht.

Publish von IO-Zuständen

Beispiel für das Publish einer Zustandsänderung an Input 1:

```
wut-0a4711/get/input/1
```

Als Payload wird je nach Zustand `ON` oder `OFF` mitgesendet.

Schalten von Outputs über Subscribe

Beispiel für das Setzen von Output 5 mittels Subscribe:

```
wut-0a4711/set/output/5
```

Als Payload kann `ON`, `OFF` oder `TOGGLE` zum Umschalten des Zustands genutzt werden.

Für das Lesen und Setzen von Countern werden die entsprechenden Ziffern als Payload übertragen. Zum löschen z.B. 0.

Sowohl bei den Topics als auch beim Payload ist auf Groß-/Kleinschreibung zu achten.

REST

Mit REST (Representational State Transfer) stellen die Web-IO einen weiteren, web-basierenden Kommunikationsweg zur Verfügung.

Die Kommunikation erfolgt über Web-IO spezifische HTTP-Requests über den unter *Grundeinstellungen* » *Netzwerk* » *Zugang für Web-Dienste* eingetragenen HTTP- bzw. HTTPS-Port.

Um REST Daten austauschen zu können, muss der Zugriff zunächst über *Kommunikationswege* » *Rest* aktiviert werden.

Wenn der REST-Zugang gegen unberechtigten Zugang geschützt werden soll, haben Sie die Möglichkeit, die Digest-Authentifizierung zu aktivieren. Die Requests müssen dann als User „admin“ mit dem Administratorpasswort oder als User „opera-

tor“ mit dem Benutzerpasswort erfolgen.

Es kann darüber hinaus festgelegt werden, ob die Outputs über REST geschaltet werden dürfen.

Lesender Zugriff

Für lesende Zugriffe verwendet REST das HTTP-Kommando GET.

Dabei unterstützt das Web-IO für Antworten auf REST-Anfragen drei Formate:

- JSON
- XML
- Text

In welchem Format geantwortet wird, kann über die Anfrage bestimmt werden. Mit

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

kann z.B. das gesamte Prozessabbild des Web-IO im JSON-Format abgerufen werden. Die Antwort sieht dann so aus:

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

```

        "state" : 0
    }
],
"counter" : [
    {
        "number" : 0,
        "state" : 0
    },
    {
        "number" : 1,
        "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"
        }
    ]
}
}
}

```

Um nur einzelne Bereiche oder Punkte abzufragen, kann die Anfrage detaillierter formuliert werden:

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

Das veranlasst das Web-IO dazu, den Status aller Inputs zurückzugeben:

```

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

```

Mit

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

kann gezielt der Zustand von Input 0 abgefragt werden.

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

Verändernder Zugriff

Bei Zugriffen, die den Schaltzustand der Outputs verändern oder die Counter löschen, wird mit POST gearbeitet.

Um z.B. Output 1 auf ON zu setzen, wird ein POST auf folgende URL gesendet:

`http://<ip-adresse>/rest/json/iostate/output/1`

Dabei werden die folgenden Parameter als Payload übergeben:

Set=ON

Das Web-IO antwortet mit

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

Über die gleiche URL kann der Output mit dem Parameter Set=OFF ausgeschaltet werden.

Das Löschen, z.B. von Counter1, erfolgt über ein POST auf folgende URL:

```
http://<ip-adresse>/rest/json/iostate/counterclear/1
```

Das Web-IO antwortet mit

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

Um die Antworten in einem der anderen Formate zu erhalten, muss einfach das Schlüsselwort `json` durch `xml` oder `text` ersetzt werden.

Eine detaillierte Beschreibung der unterstützten REST-Requests und dem Aufbau der Antworten finden Sie im Web-IO-Programmier-Handbuch. (Download unter <https://www.WuT.de>). Folgen Sie von der Datenblattseite Ihres Web-IO dem Link Anleitung.

OPC DA

Das Web-IO ist ab Werk bereits für den OPC-Betrieb voreingestellt. Wenn Sie OPC nutzen möchten, müssen Sie unter *Kommunikationswege* » *OPC* lediglich den OPC-Zugriff aktivieren und bei Bedarf das Schalten der Outputs freigeben.

Damit Ihr OPC-Client mit dem Web-IO kommunizieren kann, muss der W&T OPC-Server installiert sein. Der Zugriff über OPC-Server von Drittanbietern ist nicht vorgesehen.

Im OPC-Server wählen Sie den Menüpunkt *Geräte* » *Neues E/A Gerät*. Geben Sie IP-Adresse und Passwort Ihres Web-IO ein und wählen Sie den Gerätetyp aus. Bestätigen Sie mit *OK*. Abschließend müssen Sie über den Menüpunkt *Datei* » *Speichern als aktive Konfiguration* die neuen Eingaben übernehmen.

OPC UA

Neben dem klassischen OPC-Zugriff über den W&T OPC-Server, kann das Web-IO auch direkt über OPC UA angesprochen werden.

Das Gerät stellt Ihnen OPC UA über ein binäres TCP-Protokoll zur Verfügung. Der voreingestellte Port des Server-Dienstes entspricht dem Standard-Port für diese Anwendung: 4840. Der Verbindungsaufbau Ihres Clients erfolgt entsprechend mit dem Aufruf:

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

Authentifizierung

Das Gerät stellt mehrere Authentifikationsverfahren, mit entsprechenden Sicherheitsrichtlinien, zur Verfügung. Sie haben die Wahl zwischen:

- Keine Authentifizierung Keine Sicherheitsrichtlinie
- Sign
Sicherheitsrichtlinien:
Basic128 - RSA15
Basic265
Basic265-SHA256
AES128-SHA256 RsaOaep
- Sign & Encrypt
Sicherheitsrichtlinien:
Basic128 - RSA15
Basic265
Basic265-SHA256
AES128-SHA256 RsaOaep

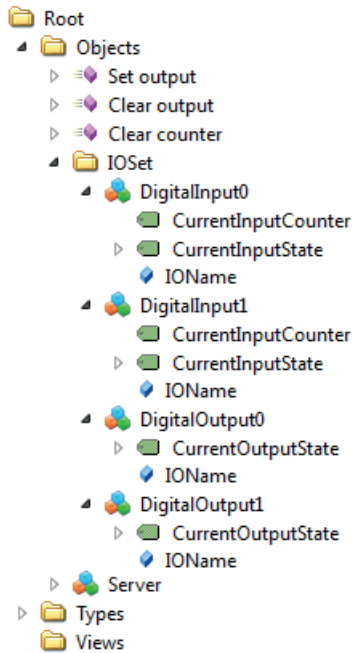
Konfigurieren Sie außerdem einen OPC UA Benutzernamen und ein Passwort. Sofern Sie „Keine Authentifizierung“ auswählen, ist dies nicht notwendig.

Nodes und NodeIDs

Die wichtigsten Nodes, mit denen die Zustände der IO-Endpunkte abgerufen werden können sind:

- CurrentInputCounter - Zählerwert der am Input erkannten Impulse
- CurrentInputState - Schaltzustand des Inputs (ON oder OFF)
- CurrentoutputState - Schaltzustand des Outputs (ON oder OFF)

Das Gerät liefert Ihnen den im Folgenden dargestellten OPC UA Baum (hier am Beispiel des Web-IO #57150).



Eine Liste der wichtigsten Nodes und der zugehörigen NodeIDs können Sie im Browser über http://<ip-adresse>/opcua_nodes?PW=<passwort> abrufen.

Wenn Sie die ab Werk voreingestellten NodeIDs gegen eigene ersetzen möchten, laden Sie im Menüweig *Kommunikationswege* >> *OPC UA* die node-Konfiguration herunter. Tragen Sie in der JSON-Datei hinter den gegebenen IDs die gewünschten IDs ein. Laden Sie die modifizierte Datei wieder Hoch und klicken Sie aus *Anwenden*.

Das Verändern der Output-Schaltzustände und das Löschen der Counter erfolgt über das Schreiben der entsprechenden Nodes mit true bzw. false oder über folgende Methoden:

- Set output - setzt den über den Index-Parameter definierten Output auf ON
- Clear output - setzt den über den Index-Parameter definierten Output auf OFF
- Clear counter - setzt den über den Index-Parameter definierten Counter auf 0

SNMP

Über SNMP kann sowohl auf die IOs als auch auf die Konfiguration des Web-IO zugegriffen werden. Welcher Parameter, welcher Status, welcher Wert unter welcher OID abgerufen werden kann, ist in der Private-MIB hinterlegt, die direkt aus dem Web-IO *Kommunikationswege* » *SNMP* heruntergeladen werden kann (alternativer Download unter <https://www.WuT.de>).

Die MIB kann bequem mit einem der gängigen MIB-Browser eingesehen werden. So bekommen Sie am schnellsten einen Überblick über die Zuordnung der OIDs. Alle SNMP betreffenden Einstellungen können Sie unter *Kommunikationswege* » *SNMP* vornehmen. Wenn die Outputs über SNMP schaltbar sein sollen, muss hier die Freigabe dafür erfolgen.

Herstellen einer SNMP-Session

Ein lesender Zugriff ist nach Aktivierung von SNMP unter *Kommunikationswege* » *SNMP* sofort per SNMP-GET möglich. Für einen schreibenden/verändernden Zugriff muss zunächst ein Session Login mit Übergabe des Systempasswortes erfolgen. Das geschieht mittels SNMP-SET über die OID, die Sie im MIB-Zweig Ihres Web-IO unter

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

finden.

Ob eine gültige Session besteht, kann über über eine GET-Abfrage auf die OID

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

abgefragt werden.

(Rückgabe 1 = gültige Session, 0 = keine Session.)

Eine bestehende Session kann über SET auf die OID

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

beendet werden.

Während einer SNMP-Session werden Login-Versuche über den Browser abgewie-

sen.

Zugriff auf die Inputs und Outputs

Das Lesen von Inputs, Countern und Outputs ist durch GET-Abfrage der entsprechenden OID immer möglich.

Im OID-Bereich

```
wtWebioEA...InOut
```

gibt es dafür entsprechende Tabellen.

Die MIB ist für die verschiedenen Web-IO Modelle symmetrisch aufgebaut. Es werden Input- und Output-Tabellen geführt, die je nach Web-IO Type eine unterschiedliche Anzahl von Einträgen haben. So bleibt die MIB geräteübergreifend kompatibel.

Beispiel: Abfrage des Schaltzustands von Input0

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

Bei den Tabelleneinträgen wird für die einzelnen IOs ein Index angehängt. Für Input 0 z.B. „.1“ (Rückgabe ist 0 = OFF und 1 = ON.)

Für das Schalten der Outputs ist zwingend eine gültige Session erforderlich. Auch für die Output gibt es eine entsprechende Tabelle:

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

Die Indizierung funktioniert genau wie bei den Inputs. Wird über SNMP-SET eine 1 übergeben schaltet der Output auf ON - durch Übergabe einer 0 auf OFF.

Modbus -TCP

Über den Menüpunkt *Kommunikationswege* » *Modbus-TCP* kann das Web-IO für den Modbus-Slave-Betrieb aktiviert werden. Hier können Sie auch festlegen, ob die Outputs über Modbus-TCP geschaltet werden dürfen. Zu dem bereitgestellten Server-Port (502) kann normalerweise zu einer Zeit nur eine Verbindung aufgebaut werden. Falls benötigt, kann über die Checkbox Zweite Verbindung erlauben ein

weitere Verbindung zugelassen werden.

Die folgenden Tabellen zeigen welche Funktionscodes und Registeradressen vom Web-IO unterstützt werden.

Modbus-Speicheraufteilung

Bitte beachten Sie, dass die Anzahl der unterstützten Inputs, Outputs, Counter oder Alarmer je nach Web-IO-Modell variiert.

Bit-Bereich:

Beschreibung	Adresse (dezimal)	Adresse (hexadez.)	Speichermodell	Länge (Byte)	Bit lesen mit FC (dezimal)	Bit lesen mit FC (hexadezimal)	Bit schreiben mit FC (dezimal)	Bit schreiben mit FC (hexadezimal)
Input 0	4096	0x1000	Bit	1	1, 2	0x01, 0x02		
Input 1	4097	0x1001	Bit	1	1, 2	0x01, 0x02		
Input 2	4098	0x1002	Bit	1	1, 2	0x01, 0x02		
Input 3	4099	0x1003	Bit	1	1, 2	0x01, 0x02		
Input 4	4100	0x1004	Bit	1	1, 2	0x01, 0x02		
Input 5	4101	0x1005	Bit	1	1, 2	0x01, 0x02		
Input 6	4102	0x1006	Bit	1	1, 2	0x01, 0x02		
Input 7	4103	0x1007	Bit	1	1, 2	0x01, 0x02		
Input 8	4104	0x1008	Bit	1	1, 2	0x01, 0x02		
Input 9	4105	0x1009	Bit	1	1, 2	0x01, 0x02		
Input 10	4106	0x100A	Bit	1	1, 2	0x01, 0x02		
Input 11	4107	0x100B	Bit	1	1, 2	0x01, 0x02		
Input 12	4108	0x100C	Bit	1	1, 2	0x01, 0x02		
Input 13	4109	0x100D	Bit	1	1, 2	0x01, 0x02		
Input 14	4110	0x100E	Bit	1	1, 2	0x01, 0x02		
Input 15	4111	0x100F	Bit	1	1, 2	0x01, 0x02		
Output 0	4128	0x1020	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 1	4129	0x1021	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 2	4130	0x1022	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 3	4131	0x1023	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 4	4132	0x1024	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 5	4133	0x1025	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 6	4134	0x1026	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 7	4135	0x1027	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 8	4136	0x1028	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 9	4137	0x1029	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 10	4138	0x102A	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 11	4139	0x102B	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 12	4140	0x102C	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F

Beschreibung	Adresse (dezimal)	Adresse (hexadez.)	Speichermodell	Länge (Byte)	Bit lesen mit FC (dezimal)	Bit lesen mit FC (hexadezimal)	Bit schreiben mit FC (dezimal)	Bit schreiben mit FC (hexadezimal)
Output 13	4141	0x102D	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 14	4142	0x102E	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Output 15	4143	0x102F	Bit	1	1, 2	0x01, 0x02	5, 15	0x05, 0x0F
Aktion 1 Status	4160	0x1040	Bit	1	1, 2	0x01, 0x02		
Aktion 2 Status	4161	0x1041	Bit	1	1, 2	0x01, 0x02		
Aktion 3 Status	4162	0x1042	Bit	1	1, 2	0x01, 0x02		
.....								
Aktion 28 Status	4187	0x105B	Bit	1	1, 2	0x01, 0x02		
Aktion 29 Status	4188	0x105C	Bit	1	1, 2	0x01, 0x02		
Aktion 30 Status	4189	0x105D	Bit	1	1, 2	0x01, 0x02		
Exception State	4192	0x1060	Bit	1	1, 2	0x01, 0x02		
Config. state	4200	0x1068	Bit	1	1, 2	0x01, 0x02		
Aktion 1 Trigger	4160	0x1800	Bit	1	1, 2	0x01, 0x02		
Aktion 2 Trigger	4161	0x1801	Bit	1	1, 2	0x01, 0x02		
Aktion 3 Trigger	4162	0x1802	Bit	1	1, 2	0x01, 0x02		
.....								
Aktion 28 Trigger	4187	0x105B	Bit	1	1, 2	0x01, 0x02		
Aktion 29 Trigger	4188	0x105C	Bit	1	1, 2	0x01, 0x02		
Aktion 30 Trigger	4189	0x105D	Bit	1	1, 2	0x01, 0x02		

16-Bereich:

Beschreibung	Adresse (dezimal)	Adresse (hexadez.)	Speichermodell	Länge (Byte)	Register lesen mit FC (dezimal)	Register lesen mit FC (hexadezimal)	Register schreiben mit FC (dezimal)	Register schreiben mit FC (hexadezimal)
Inputs 0 - 15	8192	0x2000	16-Bit	2	3, 4	0x03, 0x04		
Outputs 0 - 15	8194	0x2002	16-Bit	2	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Alarm state 1 - 16	8196	0x2004	16-Bit	2	3, 4	0x03, 0x04		
Diagn. Error count	8198	0x2006	16-Bit	2	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Diagn state 0 - 15	8199	0x2007	16-Bit	2	3, 4	0x03, 0x04		
Diagn state 16 - 31	8200	0x2008	16-Bit	2	3, 4	0x03, 0x04		
Diagn state 32 - 47	8201	0x2009	16-Bit	2	3, 4	0x03, 0x04		
Diagn state 48 - 63	8202	0x200A	16-Bit	2	3, 4	0x03, 0x04		
Diagn state 64 - 79	8203	0x200B	16-Bit	2	3, 4	0x03, 0x04		
Diagn state 80 - 95	8204	0x200C	16-Bit	2	3, 4	0x03, 0x04		
Except./Conf.-State	8205	0x200D	16-Bit	2	3, 4	0x03, 0x04		

32-Bit-Bereich:

Beschreibung	Adresse (dezimal)	Adresse (hexadez.)	Speichermodell	Länge (Byte)	Register lesen mit FC (dezimal)	Register lesen mit FC (hexadezimal)	Register schreiben mit FC (dezimal)	Register schreiben mit FC (hexadezimal)
Inputs 0 - 15	20480	0x5000	32-Bit	4	3, 4	0x03, 0x04		
Outputs 0 - 15	20482	0x5002	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Alarm state 1 - 15	20484	0x5004	32-Bit	4	3, 4	0x03, 0x04		
Counter 0	20486	0x5006	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 1	20488	0x5008	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 2	20490	0x500A	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 3	20492	0x500C	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 4	20494	0x500E	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 5	20496	0x5010	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 6	20498	0x5012	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 7	20500	0x5014	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 8	20502	0x5016	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 9	20504	0x5018	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 10	20506	0x501A	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 11	20508	0x501C	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 12	20510	0x501E	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 13	20512	0x5020	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 14	20514	0x5022	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Counter 15	20516	0x5024	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Diagn. Error count	20554	0x504A	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Diagn state 0 - 31	20556	0x504C	32-Bit	4	3, 4	0x03, 0x04		
Diagn state 32 - 63	20558	0x504E	32-Bit	4	3, 4	0x03, 0x04		
Diagn state 64 - 95	20560	0x5050	32-Bit	4	3, 4	0x03, 0x04		
Diagn state 96 - 127	20562	0x5052	32-Bit	4	3, 4	0x03, 0x04		
Diag state 128 - 159	20564	0x5054	32-Bit	4	3, 4	0x03, 0x04		
Diag state 160 - 191	20566	0x5056	32-Bit	4	3, 4	0x03, 0x04		
Seriennummer	24576	0x6000	32-Bit	8	3, 4	0x03, 0x04		
Ethernet-Adresse	24580	0x6004	32-Bit	8	3, 4	0x03, 0x04		
Virtual Register 0	28672	0x7000	32-Bit	4	3, 4	0x03, 0x04	6, 16	0x06, 0x10
Virtual Register 1	28674	0x7002	32-Bit		3, 4	0x03, 0x04	6, 16	0x06, 0x10
Virtual Register 2	28676	0x7004	32-Bit		3, 4	0x03, 0x04	6, 16	0x06, 0x10
Virtual Register 3	28678	0x7006	32-Bit		3, 4	0x03, 0x04	6, 16	0x06, 0x10
Virtual Register 4	28680	0x7008	32-Bit		3, 4	0x03, 0x04	6, 16	0x06, 0x10
Virtual Register 5	28682	0x700A	32-Bit		3, 4	0x03, 0x04	6, 16	0x06, 0x10
Virtual Register ..								
Virtual Register 28	28728	0x7038	32-Bit		3, 4	0x03, 0x04	6, 16	0x06, 0x10
Virtual Register 29	28730	0x703A	32-Bit		3, 4	0x03, 0x04	6, 16	0x06, 0x10
Virtual Register 30	28732	0x703C	32-Bit		3, 4	0x03, 0x04	6, 16	0x06, 0x10
Virtual Register 31	28734	0x703E	32-Bit		3, 4	0x03, 0x04	6, 16	0x06, 0x10

Register-Funktionen

Alle Adress-Angaben sind hexadezimal zu verstehen.

Beim Web-IO gibt es verschiedene Modbus-Speicherbereiche:

- Bit-Bereich (ab Adresse 0x1000),
- 16Bit-Bereich (ab Adresse 0x2000)
- 32-Bit-Bereich bzw. 2x16-Bit-Bereich (ab Adresse 0x5000)

Die Adressierung erfolgt im Bit-Bereich bitweise, d.h. 1 Bit benötigt eine Adresse. Im 16-Bit- und im 32-Bit-Bereich findet die Adressierung wortweise (2 Byte) statt.

Hier nochmal die wichtigsten Register im Überblick:

Die Inputs

finden sich:

- im Bit-Bereich ab 0x1000
- im 16-Bit-Bereich ab 0x2000
- im 32-Bit-Bereich ab 0x5000

Die Outputs

finden sich

- im Bit-Bereich ab 0x1020
- im 16-Bit-Bereich ab 0x2002.
- im 32-Bit-Bereich ab 0x5002.

Die Counter

finden sich im 32-Bit-Bereich ab Adresse 0x5004

Counter-Werte schreiben: Counter können auf beliebige Werte gesetzt werden.

Modbus - virtuelle Register

Das Web-IO stellt 64 virtuelle 16-Bit Register zur Verfügung, in die vom Modbus Master beliebige Werte geschrieben werden können (High Byte first). Das Schreiben in diese Register löst im Web-IO keine speziellen Aktionen aus. Der virtuelle Speicher dient vielmehr zur Übergabe von Modbus- Prozessdaten an Web-Anwendungen.

Der Adressraum für die Virtuellen Register beginnt bei 0x7000.

Virtuelle Register in Web-Anwendungen

Über einen HTTP Request

```
modbusreg?PW=<password>&
```

können die 64 Register (128Byte) von Web-Anwendungen abgerufen werden.

Das Web-IO antwortet mit

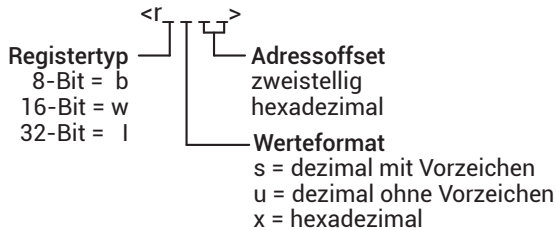
```
modbus;<High Byte1>;<Low Byte1>;<High Byte2>;<Low Byte2>;<High Byte3>;...
```

Das heißt, alle 64 Register (128Byte) werden Byte für Byte mit Semikolon getrennt hinter dem Wort „modbus“ ausgegeben.

Über JavaScript und Programmieretechniken wie AJAX kann so eine Prozessvisualisierung im Browser realisiert werden. Im einfachsten Fall können die virtuellen Register auf der werksseitig vorhandenen User-Seite des Web-IO tabellarisch angezeigt werden (nur wenn die Betriebsart Modbus im WebIO aktiviert wurde).

Virtuelle Register in Aktionen

Über die Inhalte der virtuellen Register lassen sich zwar keine Aktionen auslösen, allerdings können die dort gespeicherten Werte mittels Platzhalter (Tag) in die übermittelnden Nachrichten integriert werden.



Eine detailliertere Beschreibung der unterstützten Funktionscodes und Registeradressen finden Sie im Web-IO-Programmierhandbuch.

10. Aktionen

Mit dem Aktionsprinzip bietet das Web-IO die Möglichkeit, individuelle Alarmer und Meldungen abzusetzen und auch Outputs zu schalten. Das geschieht in Abhängigkeit definierter IO-Zustände oder anderer Ereignisse.

Bis zu 30 Aktionen können angelegt und verwaltet werden, wobei für jede Aktion ein individueller Name festgelegt werden kann.

Auslöser

Input

Es kann einer der Inputs als Auslöser bestimmt werden. Für den Input kann festgelegt werden, ob ein Wechsel von OFF nach ON, ein Wechsel von ON nach OFF oder jeder Zustandswechsel eine Aktion auslösen soll.

Output

Es kann einer der Outputs als Auslöser bestimmt werden. Für den Output kann festgelegt werden, ob ein Wechsel von OFF nach ON, ein Wechsel von ON nach OFF oder jeder Zustandswechsel eine Aktion auslösen soll.

Counter

Es kann einer der Counter als Auslöser bestimmt werden. Für den Counter muss festgelegt werden, bei welchem Zählstand eine Aktion ausgelöst soll. Ferner können Sie bestimmen, ob der Counter nach Auslösen der Aktion auf Null zurückgesetzt wird.

I/O-Kombination

Es können auch Inputs und Outputs in Kombination eine Aktion auslösen. Hierbei können Sie festlegen, ob die einzelnen Zustände UND- bzw. ODER-verknüpft ausgewertet werden.

Intervall-Timer

Durch entsprechende Konfiguration kann das Web-IO Aktionen zu vorgegebenen Zeiten ausführen. Die Eingabe der Zeiten erfolgt im „Cron-Format“.

Gültige Zeichen sind:

- * steht für alle gültigen Werte im jeweiligen Eingabefeld (z.B. alle Minuten oder alle Stunden)
- L Letzter Tag eines Monats
- gibt einen Bereich von..bis an (z.B. Wochentag „2-4“ steht für Dienstag bis Donnerstag, während die Eingabe von „*“ an allen Wochentagen den Timer auslöst). In Verbindung mit „L“ gilt „-“ als Minuszeichen um z.B. den vorletzten Tag des Monats („L-1“) zu definieren.
- / Intervall innerhalb des eingegebenen Bereichs (z.B. Minute „0-45/2“ löst den Timer im Bereich zwischen der 0. und 45. Minute alle zwei Minuten aus (0, 2, 4, 6, 8, 10, ..., 44)).
- , Gibt einen absoluten Wert an (z.B.: Minute „0, 15, 30“ löst den Timer zur vollen Stunde, zur 15. Minute und zur 30. Minute aus.).

Beispiel:

eine Aktion soll in den Monaten April bis Oktober immer Montags um 8:00 Uhr ausgeführt werden.

Minute:	0
Stunde:	8
Monatstag:	*
Monat:	4-10
Wochentag:	1

Geräte Neustart

Wenn ein Neustart eine Aktion auslösen soll, unterscheidet das Web-IO zwei Varianten:

- Kaltstart

Wird der Neustart durch Hardwarezugriff ausgelöst (Zuführung bzw. Unterbrechung der Versorgungsspannung oder Betätigen der Reset Taste) wertet das Web-IO das als Kaltstart.

- Warmstart

Ein Warmstart kann über die Webseite unter *Wartung* mit dem Neustart-Button

ausgelöst werden. Des Weiteren wird über das Verbinden auf Port 8888 TCP und die Übergabe des Systempasswortes ein Neustart herbeigeführt, wenn der Reset-Port freigegeben ist.

MQTT-Subscribe

Empfängt das Web-IO auf dem unter Topic Pfad eingetragenen Pfad das als Topic konfigurierte Schlüsselwort, wird die Aktion ausgeführt. Dazu muss unter *Kommunikationswege* » *MQTT* die MQTT-Unterstützung aktiviert, ferner müssen alle nötigen Angaben zum Broker konfiguriert sein.

Aktionen

Bei den Aktionen, die das Versenden von Alarm-, Melde- und sonstigen Texten erlauben, können innerhalb des Textes Platzhalter genutzt werden, die beim Ausführen einer Aktion gegen tatsächliche Inhalte, wie IO-Zustände, Uhrzeit usw. ersetzt werden.

Platzhalter	Beschreibung
<ix>	Zustand des Inputs Nr. x (ON/OFF)
<ox>	Zustand des Outputs Nr. x (ON/OFF)
<cx>	Zählerstand des Counters Nr. x
<i>	Zustand aller Inputs als hex. Bitmuster
<o>	Zustand aller Outputs als hex. Bitmuster
<dn>	Device Name <inx> Name des Inputs Nr. x
<inx>	Name des Inputs Nr. x
<onx>	Name des Outputs Nr. x
<t>	Zeitstempel mit Datum und Uhrzeit
<\$y>	Jahr im Format "JJJJ"
<\$m>	Monat im Format "MM"
<\$d>	Tag im Format "TT"
<\$h>	Stunde im Format "hh"
<\$i>	Minuten im Format "mm"
<\$s>	Sekunden im Format "ss"
<hex: xx xx>	Beliege Bytes als hexadezimale Eingabe
<rxxxx>	Modbus-Registerwert (Kapitel Modbus-TCP)

Bei den Textmeldungen lässt sich neben der eigentlichen Meldung, die beim Auslösen versendet wird, zusätzlich eine Clear-Meldung hinterlegen. Die Clear-Meldung wird versendet, wenn der Auslöser für die Aktion nicht mehr gegeben ist - also der Normalzustand zurückkehrt. Das Versenden von Meldungen nimmt je nach Protokoll unterschiedlich viel Zeit in Anspruch. Sollte der auslösende Zustand nur so kurz anliegen, dass die entsprechende Meldung noch gar nicht versendet werden konnte, wird nur die Clear-Meldung versandt.

E-Mail-Meldung

Empfänger, Betreff und Inhalte der E-Mail können frei konfiguriert werden.

Um E-Mail-Meldungen verschicken zu können, muss der Zugang zum Mailserver konfiguriert werden und *Mail* als Kommunikationsweg aktiviert sein. Alle notwendigen Einstellungen können Sie unter *Kommunikationswege* » *Mail* vornehmen. Im Infobereich finden Sie die allgemeinen Zugangsdaten der gängigsten E-Mail-Anbieter.

SNMP-Trap

IP-Adresse bzw. Host-Name des SNMP-Servers, sowie die Meldetexte können frei konfiguriert werden.

Um SNMP-Traps versenden zu können, muss *SNMP* unter *Kommunikationswege* » *SNMP* aktiviert sein. Alle anderen dort einstellbaren Parameter sind für den Versand von SNMP-Traps nicht relevant.

MQTT-Publish

Das Web-IO kann beliebige Informationen als MQTT-Topic in einen zu konfigurierenden Pfad auf einen MQTT Broker schreiben.

Dazu muss unter *Kommunikationswege* » *MQTT* der Zugang zum MQTT-Broker konfiguriert werden.

HTTP-Request

Eine weitere mögliche Aktion ist das Versenden eines HTTP-Request, wie er von einigen Geräten, wie z.B. Kameras, benötigt wird, um bestimmte Funktionen anzustoßen.

Geben Sie als HTTP-Request die komplette URL mit allen vom empfangendem Gerät erwarteten Parametern ein.

Format:

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

Bei solchen Geräten, die eine Authentifizierung mit Username und Passwort benötigen, wählen Sie aus, welche Art der Authentifizierung angewendet werden soll und füllen Sie die entsprechenden Felder aus.

Bei der Request-Methode haben Sie die Möglichkeit einer GET-Anfrage oder mittels POST weitere Daten mitzusenden.

TCP-Meldungen

Beim Versenden von TCP-Meldungen arbeitet das Web-IO als TCP-Client. Es baut beim Auslösen der Aktion eine TCP-Verbindung zur angegebenen TCP-Server-Adresse auf den angegebenen Port auf, übermittelt den Melde- bzw. Clear-Text und baut dann die Verbindung wieder ab. Etwaige Antworten vom Server werden ignoriert und verworfen.

UDP-Meldungen

Um UDP-Meldungen versenden zu können, muss unter *Kommunikationswege* » *Socket-API* im Bereich *UDP-Sockets ASCII-Mode UDP-Sockets* aktiviert sein.

Beim Versenden von UDP-Meldungen arbeitet das Web-IO als UDP-Peer. Die Meldung wird in Form eines UDP-Datagramms zur angegebenen UDP-Peer-Adresse auf den angegebenen Port übermittelt. Etwaige Antworten von der Gegenseite werden ignoriert und verworfen.

Syslog-Meldungen

IP-Adresse bzw. Host-Name des Syslog-Servers, sowie die Meldetexte können frei konfiguriert werden.

Um Syslog-Meldungen versenden zu können, muss *Syslog* unter *Kommunikationswege* » *Syslog* aktiviert sein. Alle anderen dort einstellbaren Parameter sind für den Versand von Syslog-Meldungen nicht relevant.

FTP-Meldungen

Das Web-IO kann Meldetexte per FTP in eine Datei speichern.

Dazu muss unter *Kommunikationswege* » *FTP* die FTP-Unterstützung zunächst aktiviert und der Zugang zum FTP-Server konfiguriert werden.

Der Dateiname, Melde- und Clear-Texte können frei formuliert werden.

Über die Optionen wird unterschieden, ob mit *STOR* die Datei bei jeder ausgelösten Aktion komplett überschrieben wird oder ob mit *APPEND* die Melde- und Clear-Texte kontinuierlich an die Datei angehängt werden.

Outputs schalten

Beim Schalten von Outputs unterscheidet das Web-IO zwischen dem Schalten der eigenen Outputs oder dem Schalten der Outputs eines anderen Web-IO.

Eigene Outputs schalten

Bei Auswahl eines einzelnen Outputs kann dieser auf ON oder auf OFF geschaltet werden. Als weitere Möglichkeit kann der bestehende Zustand gewechselt werden.

Alternativ können mehrere Outputs gleichzeitig geschaltet werden. Dabei kann für jeden ausgewählten Output festgelegt werden, ob dieser auf ON oder OFF gesetzt werden soll.

Outputs eines anderen Web-IO schalten

Auch hier können entweder ein bestimmter oder mehrere Outputs geschaltet werden.

Legen Sie durch Eingabe der IP-Adresse fest, bei welchem Web-IO die Outputs geschaltet werden sollen. Als TCP-Port geben Sie den Port an, der beim Ziel-Web-IO als Zugang für den Browser eingestellt ist. Wenn das Ziel-Web-IO mit einem Passwort geschützt ist, muss dieses ebenfalls eingetragen werden.

Beim Ziel-Web-IO muss der Zugriff für AJAX bzw. HTTP-Requests aktiviert sein (*Kommunikationswege* » *Web-API*) und es müssen die angesteuerten Outputs für das Schalten über HTTP-Requests freigegeben sein.

Es können auch die Outputs von Web-IOs älterer Bauart (#57630, #57631, #57634 und #57637) geschaltet werden. In diesem Fall muss als TCP-Port der HTTP-Port des Web-IO angegeben werden. Im *Output Mode Menü* müssen die Outputs auf

HTTP gesetzt werden.

Das Schalten von Outputs bietet als Aktion viele interessante Anwendungsmöglichkeiten.

IO-Logik

Durch entsprechendes Kombinieren von Input-Zuständen als Auslöser und dem Schalten der eigenen Outputs lassen sich logische Verknüpfungen realisieren.

Point-to-Point-Verbindung

Ähnlich der Box-to-Box-Verbindungen, bei denen die Inputs von Web-IO A 1:1 auf die Outputs von Web-IO B abgebildet werden, kann der Schaltzustand eines beliebigen Inputs auf einen beliebigen Output eines anderen Web-IO abgebildet werden.

Point-to-Multipoint

Durch Anlegen mehrerer Aktionen, die den selben Input als Auslöser verwenden, lassen sich entsprechend mehrere Outputs an verschiedenen Web-IOs steuern.

11. Zugriff aus eigenen Anwendungen

Neben den zahlreichen standardisierten Zugriffsmöglichkeiten bietet das Web-IO auch die Option, es aus einer eigenen Anwendung anzusprechen.

Das kann über TCP/IP-Sockets aus den gängigen Hochsprachen erfolgen. Es ist aber auch möglich, gängige Web-Techniken wie AJAX oder PHP zu nutzen, um mit dem Web-IO zu kommunizieren.

Zugriff über TCP/IP-Sockets

Für den Zugriff über TCP/IP-Sockets bietet das Web-IO drei Zugänge.

Zugriff über:

- Kommandostrings ASCII
- Binärstrukturen BINARY
- HTTP-Requests AJAX

Kommandostrings ASCII

Durch den Austausch einfacher Kommandostrings können die Inputs und Counter gelesen bzw. die Outputs gesetzt werden.

Je nach Konfiguration arbeitet das Web-IO in diesem Modus als TCP-Server oder als UDP-Peer.

Eine Liste der unterstützten Kommandos und weitere Details zum Zugriff über ASCII-Sockets finden Sie im Web-IO-Programmierhandbuch. (Download unter <https://www.WuT.de>). Folgen Sie von der Datenblattseite Ihres Web-IO dem Link Anleitung.

TCP-Server

Um das Web-IO über ASCII-Sockets als TCP-Server anzusprechen, aktivieren Sie *TCP ASCII-Sockets* unter *Kommunikationswege* » *Socket-API*. Geben Sie an, auf welchem Server-Port das Web-IO Verbindungen entgegennehmen soll. Das Web-IO kann zeitgleich bis zu vier TCP-Verbindungen über den angegebenen Port bereitstellen - jeder weitere Verbindungsversuch wird abgewiesen.

Empfängt das Web-IO innerhalb von 30 Sekunden kein gültiges Kommando,

schließt es die Verbindung und ist danach wieder frei für einen neuen Verbindungsaufbau. In gleicher Weise verhält sich das Web-IO, wenn ein fehlerhaftes oder unbekanntes Kommando empfangen wird.

Das Lesen der Inputs geschieht im Regelfall im Pollingverfahren. Eine ereignisgesteuerte Auswertung ist nur nach entsprechender Konfiguration der Input-Trigger möglich.

UDP-Peer

Um das Web-IO mittels ASCII-Sockets über UDP anzusprechen, aktivieren Sie *UDP ASCII-Sockets* unter *Kommunikationswege* » *Socket-API*. Geben Sie an, auf welchem lokalen UDP-Port das Web-IO Datagramme entgegennehmen soll.

Über *Remote UDP-Port* kann festgelegt werden, an welchen UDP-Port des Anfragers die Antworten des Web-IO gesendet werden. Der Eintrag *AUTO* legt fest, dass die Antworten an den Port zurückgehen, der im empfangenen Datagramm als Absende-Port eingetragen ist.

Das Lesen der Inputs ist ausschließlich im Pollingverfahren möglich. Eine ereignisgesteuerte Auswertung kann durch Hinzufügen einer entsprechenden Aktion erreicht werden (siehe Kapitel **Aktionen**).

Binärstrukturen BINARY

Für die verschiedenen Funktionen wie Lesen der Inputs, Setzen der Outputs usw. gibt das Web-IO binäre Strukturen vor. Der Zugriff erfolgt ausschließlich durch Austausch dieser Strukturen.

In diesem Modus kann das Web-IO als TCP-Client, TCP-Server oder UDP-Peer arbeiten. Der Zugriff kann über ein Passwort geschützt werden.

Es stehen vier Binary-Zugänge zur Verfügung, die unabhängig von einander unter *Kommunikationswege* » *Socket-API* aktiviert und konfiguriert werden können.

In der Betriebsart TCP-Server kann sich zu einer Zeit nur ein Client auf den entsprechenden Binary-Zugang verbinden. Jeder weitere Verbindungsversuch wird abgewiesen.

Eine ausführliche Beschreibung der unterstützten Binärstrukturen und weitere Details zum Zugriff über BINARY-Sockets finden Sie im Web-IO-Programmierhandbuch (Download unter <https://www.WuT.de>).

Folgen Sie von der Datenblattseite Ihres Web-IO dem Link Anleitung.

HTTP-Request

Neben den klassischen Socket-Zugängen kann das Web-IO auch über den HTTP-Zugang direkt mittels HTTP-Requests angesprochen werden

Ab Werk ist dieser Zugang gesperrt und muss zunächst über den Menüweig *Kommunikationswege* » *Web-API* aktiviert werden.

Eine ausführliche Beschreibung der unterstützten HTTP-Requests und weitere Details zum Zugriff mit Web-Techniken wie AJAX oder PHP finden Sie im Web-IO-Programmierhandbuch (Download unter <https://www.WuT.de>). Folgen Sie von der Datenblattseite Ihres Web-IO dem Link Anleitung.

12. Anhang

Alternativen bei der IP-Adressvergabe

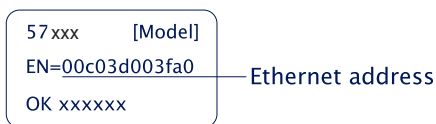
Für die Fälle, in denen die IP-Adressvergabe nicht per DHCP oder mit dem Wutility Tool erfolgen kann, bietet das Web-IO zwei weitere Möglichkeiten:

- Vergabe mit Hilfe des ARP-Kommandos
- Vergabe über die serielle Schnittstelle

Vergabe der IP-Adr. mit Hilfe des ARP-Kommandos

Diese Methode ist ausführbar, wenn das Web-IO noch keine IP-Adresse hat, der Eintrag also 0.0.0.0 lautet. Eine weitere Voraussetzung ist, dass sich Web-IO und Computer im gleichen Netzwerksegment befinden.

Lesen Sie die Ethernet-Adresse des Web-IO von dem Aufkleber an der Gehäuseseite ab:



Fügen Sie jetzt mit der folgenden Befehlszeile der ARP-Tabelle des Rechners einen statischen Eintrag hinzu:

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

Beispiel unter Windows:

```
arp -s 10.40.72.15 00-C0-3-00-3F-A0
```

Beispiel unter SCO UNIX:

```
arp -s 10.40.72.15 00:C0:3D:00:3F:A0
```

Starten Sie abschließend den Web-Browser und geben Sie

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



In Windows-Umgebungen darf die Eingabe von IPAdressen nur ohne führende Nullen erfolgen.

Das Web-IO übernimmt die IP-Adresse des ersten, an seine Ethernet-Adresse gesendeten Netzwerkpaketes als seine eigene und speichert diese nichtflüchtig ab. Die Webseite des Web-IO wird daraufhin geladen und alle weiteren Einstellungen können nun bequem per Web-based Management vorgenommen werden

Firmware-Update

Die Firmware der Web-IOs wird kontinuierlich weiterentwickelt, um den immer wieder neuen Anforderungen wachsender Netzwerke gerecht zu werden.

Aktuelle Firmware für Ihr Web-IO finden Sie unter <https://www.WuT.de> wenn Sie in der Suche die Artikel-Nr. Ihres Web-IO eingeben und Firmware wählen.

Um das Firmware-Update einzuspielen, benötigen Sie einen Windows-PC mit installiertem WuTility-Tool (im Firmware-Archiv enthalten) und ungehinderten Netzwerkzugriff auf das Web-IO.

Starten Sie WuTility, markieren Sie Ihr Web-IO in der Inventarliste und klicken Sie in der Icon-Leiste auf *Firmware*. Wählen Sie die entsprechende UHD-Datei aus. WuTility führt Sie durch den Update-Prozess.

Unterbrechen Sie während des Updates weder die Stromzufuhr noch die Netzwerkverbindung.

Alle Einstellungen im Web-IO bleiben erhalten und das Web-IO sollte nach dem Update sofort wieder betriebsbereit sein.

Security-Hinweise

Die folgenden Abschnitte enthalten aus Sicht der IT-Sicherheit relevante Hinweise und Empfehlungen für Inbetriebnahme, Konfiguration, Betrieb und Wartung der in dieser Anleitung beschriebenen Web-IO Modelle.

Funktion und typische Anwendung

Web-IOs bieten die Möglichkeit, die Zustände elektrischer Schaltsignale über einen Ethernet-Anschluss innerhalb höherer Protokoll-Instanzen zu übermitteln oder anzusteuern.

Alle Web-IO Modelle basieren auf einem W&T-eigenen Betriebssystem und sind im Kern frei von Open-Source-Bestandteilen und Drittanbieter-Software.

Ab Werk sind die Web-IOs für den Betrieb in einer sicheren Netzwerkumgebung konzeptioniert. Der Schwerpunkt der Werkeinstellungen liegt auf einem möglichst latenzarmen und deshalb ungesicherten Konfigurationszugang über HTTP.

In unsicheren Netzwerkumgebungen und/oder bei erhöhten Sicherheitsanforderungen müssen zusätzliche Maßnahmen getroffen werden, um unauthorisierte Zugriffe zu vermeiden.

Mit Ausnahme der Anzeige im Browser sind alle anderen Zugriffsmöglichkeiten auf die Inputs, Outputs und die Konfiguration deaktiviert.

Anforderungen an Integratoren und Betreiber

Abhängig von der individuellen Netzwerkumgebung und den Security-Anforderungen müssen die Werkeinstellungen für den operativen Betrieb aus Sicht der Security überprüft werden. Es können Änderungen und/oder zusätzliche Maßnahmen durch den Integrator oder Betreiber erforderlich sein.

Hierzu zählen insbesondere:

- Wahl eines sicheren Passwortes hinsichtlich Länge und Zusammensetzung
- Deaktivierung nicht benötigter Dienste und/oder Zugriffsbeschränkungen durch eine vorgeschaltete, externe Firewall.
- Installation eines individuellen Gerätezertifikats innerhalb einer PKI-Umgebung
- Schutz der Web-IOs vor unauthorisiertem physischen Zugriff

Weitere Details hierzu finden Sie in der Folge dieses Kapitels sowie auch in den vorhergehenden Beschreibungen der einzelnen Betriebsarten

Installationsort

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

- Außerbetriebnahme des Gerätes (Entfernen des Netzkabels, Spannungsversorgung ...) und Verlust aller Verbindungen zu Kommunikationspartnern.
- Je nach Modell Rücksetzen auf Werkseinstellungen durch langes drücken des

Resettasters.

Inbetriebnahme

Die Inbetriebnahme des Web-IOs unterteilt sich in die Vergabe der IP-Adresse (DHCP, WuTility, statischer ARP-Eintrag, je nach Modell serieller Port) und der anschließenden weiteren Konfiguration über das Web-Based-Management. Mit der Werkseinstellung sind alle Konfigurationsdienste frei zugänglich. Die Inbetriebnahme muss daher so erfolgen, dass bis zur Vergabe des System-Passwortes und einer sicheren Konfiguration keine unauthorisierten Zugriffe erfolgen können.

Eine geeignete Maßnahme ist zum Beispiel die Inbetriebnahme über eine Punkt-zu-Punkt-Verbindung mit dem konfigurierenden Rechner durchzuführen. Erst anschließend wird das Web-IO mit dem eigentlichen Zielnetzwerk verbunden.

Passwort

Der operative Einsatz des Web-IOs ohne Passwort sollte nicht erfolgen. Das Passwort ist der zentrale Schutz vor unauthorisierten Zugriffen auf die Konfiguration und das Management des Web-IOs. Je nach gewähltem Kommunikationsweg schützt das Passwort auch den Zugriff auf die Inputs und Outputs

Wir empfehlen die Verwendung eines sicheren Passwortes mit einer Länge von mindestens 15 Zeichen, bestehend aus Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen (nicht erlaubt sind &, # und /)

Die Übertragung des System-Passwortes an das Web-IO erfolgt beim WBM-Zugriff über HTTP im Klartext. Nur bei Konfiguration über HTTPS erfolgt die Übertragung verschlüsselt.

Bei Passwort geschützten Zugriffen aus unsicheren oder öffentlichen Netzwerken sind zusätzliche Maßnahmen, wie z.B. die Nutzung eines VPN-Tunnels, zu treffen.

Registrierung für sicherheitsrelevante Informationen

Über das Inventarisierungstool WuTility können Geräte bei W&T registriert werden. Im Fall von sicherheitsrelevanten Updates und/oder Informationen werden sie von uns sofort per Email benachrichtigt.

Neben den angegebenen persönlichen Daten werden bei einer Registrierung auch die gerätespezifischen Daten gespeichert.

Betrieb und Konfiguration

Ab Werk sind alle Zugänge bzw. Kommunikationswege bis auf den Browserzugang deaktiviert.

Wir empfehlen nur die Kommunikationswege und Dienste zu aktivieren, die für den Betrieb tatsächlich benötigt werden.

Eine Übersicht der möglichen Kommunikationswege finden Sie in der folgenden Tabelle.

Kommunikationsweg /Protokoll	Verbindungstyp	Ab Werk aktiv	Lokaler Port	Konfigurierbar	Remoteport	Konfigurierbar	Passwort-geschützt	Klartext-übertragung
Wutility-Inventarisierung	UDP	X	8513	X	dynamisch			
Wutility-IP-Vergabe	UDP	X	68		67		X	X
DHCP	UDP	X	68		67			
HTTP	TCP-Server	X	80	X	dynamisch		X	X
HTTPS	TCP-Server		443	X	dynamisch		X	
DNS	UDP	X	dynamisch		53			
NTP	UDP	X	dynamisch		123			
Geräte-Reset	TCP-Server	X	8888	X	dynamisch		X	X
Geräte-Update Initialisierung	TCP-Server	X	8002	X	dynamisch		X	X
Geräte-Update Firmwaredaten	UDP		69		dynamisch		X	X
Mail	TCP-Client		dynamisch		587	X	X	
Box-to-Box 1 Master	TCP-Client		dynamisch	X	49157	X	X	
Box-to-Box 1 Slave	TCP-Server		49157	X	dynamisch		X	
Box-to-Box 2 Master	TCP-Client		dynamisch	X	49158	X	X	
Box-to-Box 2 Slave	TCP-Server		49158	X	dynamisch		X	
MQTT	TCP-Client		dynamisch		1883	X	X	X
SMQTT	TCP-Client		dynamisch		8883	X	X	
REST (HTTP)	TCP-Server		80	X	dynamisch		X	X
REST (HTTPS)	TCP-Server		443	X	dynamisch		X	
Web-API (HTTP)	TCP-Server		80	X	dynamisch		X	X
Web-API (HTTPS)	TCP-Server		443	X	dynamisch		X	
TCP-ASCII-Socket Server	TCP-Server		42280	X	dynamisch		X	X
UDP-ASCII-Socket Peer	UDP-Peer		42279	X	dynamisch	X	X	X

Kommunikationsweg / Protokoll	Verbindungstyp	Ab Werk aktiv	Lokaler Port	Konfigurierbar	Remoteport	Konfigurierbar	Passwort-geschützt	Klartext-übertragung
BINARY 1 TCP Sockets	TCP-Client		dynamisch	X	49153	X	X	
BINARY 1 TCP Sockets	TCP-Server		49153	X	dynamisch		X	
BINARY 1 TCP Sockets	UDP-Peer		45889	X	45889	X		
BINARY 2 TCP Sockets	TCP-Client		dynamisch	X	49154	X	X	
BINARY 2 TCP Sockets	TCP-Server		49154	X	dynamisch		X	
BINARY 2 TCP Sockets	UDP-Peer		45890	X	45890	X		
BINARY 3 TCP Sockets	TCP-Client		dynamisch	X	49155	X	X	
BINARY 3 TCP Sockets	TCP-Server		49155	X	dynamisch		X	
BINARY 3 TCP Sockets	UDP-Peer		45891	X	45891	X		
BINARY 4 TCP Sockets	TCP-Client		dynamisch	X	49156	X	X	
BINARY 4 TCP Sockets	TCP-Server		49156	X	dynamisch		X	
BINARY 4 TCP Sockets	UDP-Peer		45892	X	45892	X		
Modbus-TCP	TCP-Server		502	X	dynamisch			
OPC DA	TCP-Server		49159	X	dynamisch		X	
OPC UA	TCP-Server		4840	X	dynamisch		X	
SNMP V1	UDP-Peer		161		dynamisch		X	X
SNMP V2	UDP-Peer		161		dynamisch		X	X
SNMP V3	UDP-Peer		161		dynamisch		X	
SNMP-Trap	UDP-Peer		161		162	X		
SYSLOG	UDP-Peer		dynamisch		514	X		
FTP-Steuerverbindung	TCP-Client		dynamisch		21	X	X	X
FTP-Datenverbindung (activ)	TCP-Server		dynamisch		dynamisch			
FTP-Datenverbindung (passiv)	TCP-Client		dynamisch		dynamisch			
HTTP-Request (Aktion)	TCP-Client		dynamisch		80	X	X	X
HTTPS-Request (Aktion)	TCP-Client		dynamisch		443	X	X	
TCP-Meldung (Aktion)	TCP-Cleint		dynamisch		8000	X		
UDP-Meldung (Aktion)	UDO-Peer		dynamisch		8500	X		
Zugänge für die Com-Server Funktion (nur 57731)								
Com-Server Konfiguration (Telnet)	TCP-Server	X	1111	X	dynamisch		X	X
Socket-Zugang serielle Daten	TCP-Server	X	8000	X	dynamisch			
Kontrollzugang serieller Port	TCP-Server	X	9094	X	dynamisch		X	X
Port-Reset	TCP-Server	X	9084	X	dynamisch			
Konfigurations-Download	TCP-Server	X	8003		dynamisch		X	X

Kommunikationsweg / Protokoll	Verbindungstyp	Ab Werk aktiv	Lokaler Port	Konfigurierbar	Remoteport	Konfigurierbar	Passwort-geschützt	Klartext-übertragung
Konfigurations-Upload	TCP-Server	X	8004		dynamisch		X	X
Telnet	TCP-Server		6000	X	dynamisch			
Telnet	TCP-Client		dynamisch		0	X		
FTP	TCP-Server		7000	X	dynamisch			
FTP	TCP-Client		dynamisch		0	X		
Socket-Client serielle Daten	TCP-Client		dynamisch		0	X		
Socket-UDP-Peer serielle Daten	UDP-Peer		8000	X	0	X		
Socket für InQueueCopy	TCP-Server		0	X	dynamisch			

Der Kontrollport für den seriellen Zugang muss immer 1094 höher sein, als der den seriellen Socket-Zugang konfigurierte TCP-Port.

Konfiguration möglichst per HTTPS / PKI-Umgebungen

Das von HTTPS verwendete TLS-Protokoll bietet einen verschlüsselten und authentifizierten Zugriff auf die Weboberfläche des Web-IO. Das gilt auch für den Zugriff über die Web-API und den Rest-Zugang. Zum Schutz der ausgetauschten Konfigurationsdaten, Kommandos und des System-Passwortes empfehlen wir die Aktivierung von HTTPS besonders in unsicheren Netzwerkumgebungen. Als Schutz vor Man-in-the-Middle-Angriffen, sollte darüber hinaus auch das selbst signierte Default-Zertifikat durch ein individuelles, eigenes Zertifikat ersetzt werden.

Verschlüsselte Kommunikation

Die Hardwareplattform des Web-IO verbindet geringe Latenzzeiten mit einem niedrigen Stromverbrauch. Hierdurch ist die Schlüssellänge der möglichen Zertifikate auf 2048 Bit (1024 bei #57738) begrenzt und das Web-IO unterstützt maximal TLS1.2.. In Anwendungen mit höheren Anforderungen müssen ggf. zusätzliche Maßnahmen erfolgen (z.B. VPN).

Eine TLS-verschlüsselte Kommunikation ist in den folgenden Betriebsarten möglich:

- HTTPS (Browser)
- HTTPS (Web-API)
- HTTPS (REST)
- MQTT (SMQTT)

- Mailversand
- OPC UA

Die rechenintensiven TLS-Verschlüsselungs-Funktionen können Einfluss auf die Latenzen der Datenübertragung haben. Bei zeitkritische Schalt- und Erfassungsaufgaben sollte daher auf ihre Verträglichkeit mit HTTPS-Zugriffen getestet werden. Hierunter fallen besonders auch eventuelle Security-Scans im Netzwerk. Diese öffnen teilweise sehr viele TLS-Verbindungen innerhalb kurzer Zeit und können somit zu Unterbrechungen oder Timeouts des Datenverkehrs führen.

Verinselung des Teilnetzes über Router/Firewall

Bei Anwendungen, die unverschlüsselt mit dem Web-IO kommunizieren, sollten die Kommunikationspartner (z.B. Web-IO und PC) zum Schutz vor Ausspähung über eine Firewall in einem eigenen Netzwerksegment isoliert werden. Zum Beispiel mit Hilfe einer W&T Microwall werden die Kommunikationspartner hierdurch auch vor schädlichen Ereignissen (Broadcaststürme, Überlast etc.) im Hauptnetzwerk geschützt.

Geeignete Firewall-Regeln beschränken netzwerkübergreifende Zugriffe auf das erforderliche Mindestmaß.

Aktualisierung der Firmware

Zur Behebung funktionaler Fehler, eventuell entdeckter Schwachstellen oder auch zur Funktions-Erweiterung veröffentlicht W&T Firmware-Updates für die Web-IOs.

Der Upload in das Gerät erfolgt mit Hilfe des Management-Tools WuTility.

Update-Dateien beinhalten immer die gesamte Firmware bzw. das gesamte System des Web-IOs. Aus diesem Grund sind Firmware-Updates immer mit einem Neustart des Web-IO und somit auch einer Unterbrechung des operativen Betriebes verbunden. Individuelle Konfigurationsdaten (IP-Parameter, Firewall-Regeln etc.) werden von einem Firmware-Update nicht beeinflusst und bleiben erhalten.

Die Web-IO basieren auf einem W&T-eigenen Betriebssystem und beinhalten im Kern keine Komponenten von Drittanbietern (z.B. Linux, externe TCP-Stacks etc.). Eine Kompromittierung mit üblichem, für diese Systeme existierenden Schadcode, ist daher nicht möglich.

Der Upload der Firmware erfolgt per TFTP (UDP) und das System-Passwort wird in diesem Zuge netzwerkseitig im Klartext übertragen. In unsicheren Netzwerken oder in Umgebungen mit erhöhten Sicherheitsanforderungen sind daher zusätzliche externe Maßnahmen erforderlich (z.B. VPN).

Weitere Details zu einem Firmware-Update enthält das Kapitel Firmware-Update.

Service, Wartung und Außerbetriebnahme

Trotz hoher Qualitätsstandards kann Elektronik jederzeit z.B. durch externe Ereignisse ausfallen. Abhängig von den Anforderungen an die Verfügbarkeit der jeweiligen Anwendung empfehlen wir geeignete Vorkehrungen zu treffen.

- Sicherung/Speicherung der Gerätekonfiguration
- Ggf. Vorhaltung eines Ersatzgerätes
- Dokumentation der Vorgehensweise bei Gerätetausch

Bei der Außerbetriebnahme sollte das Web-IO zum Schutz aller im Gerät gespeicherten vertraulichen Informationen (IP-Bereiche, externe Zugangsdaten etc.) auf die Werkseinstellungen zurückgesetzt werden. Das kann entweder über das Web-Based-Management oder per Hardware über langes Drücken des Resetassers erfolgen.

Notzugang

Für den Fall, dass Sie die Passwörter des Web-IO vergessen haben oder das Gerät ohne Netzwerkzugriff auf Werkseinstellungen zurücksetzen wollen, benötigen Sie physischen Zugriff auf das Web-IO.

Über das mit Reset beschriftete Loch in der Frontblende kann mit Hilfe eines spitzen Gegenstands der versenkte Reset-Taster betätigt werden, um folgende Funktionen einzuleiten.

Geräteneustart

Durch kurzes Betätigen des Reset-Tasters startet das Web-IO neu. Alle bestehenden Netzwerkverbindungen werden dabei abgeworfen. Die Konfiguration des Web-IO bleibt aber vollständig erhalten. Wenn keine statische

IP-Adresse vergeben wurde, startet das Web-IO eine DHCP-Anfrage, was je nach Netzwerkumfeld zur Zuteilung einer neuen IP-Adresse führen kann.

Passwörter löschen

Durch langes Drücken (Zeitfenster 3 - 7 Sekunden der Reset-Tasters fällt das Web-IO in den Notzugangsmodus. Beenden Sie das Drücken des Reset-Taste, wenn die LEDs in der Frontblende anfangen langsam zu blinken. Für ca 5 Minuten kann nun bei Aufruf der Web-IO IP-Adresse über den Browser eine Notseite aufgerufen werden. Hier können über einen Button alle Passwörter gelöscht werden.

Rücksetzen auf Werkseinstellungen

Wird der Reset-Taster sehr lange gedrückt (mehr als 7 Sekunden) beginnen die LEDs unterhalb des Tasters schnell an zu blinken. Der Auslieferungszustand wird wieder hergestellt. Nach ca. 30 Sekunden muss der Reset-Taster dann erneut einmal kurz gedrückt werden, um das Web-IO mit Werkseinstellungen neu zu starten.

Bedeutung der Status-LEDs

In der Frontblende befinden sich neben den LEDs die den Schaltzustand der Inputs bzw. Outputs anzeigen vier weitere Status-LEDs

Power

Die Power-LED zeigt an, dass eine externe Versorgungsspannung oder PoE das Web-IO mit Strom versorgen.

Status

Durch zyklisches Blinken wird angezeigt, dass eine Netzwerk-Verbindung besteht bzw. versucht wird eine konfigurierte Verbindung aufzubauen. Zusätzlich wird durch Aufblitzen Netzwerkverkehr signalisiert.

Error

Die Error-LED zeigt Systemfehler an, die in aller Regel vom Anwender nicht ohne weiteres zu beheben sind (z.B. Checksummenfehler im Flash durch missglücktes Firmware-Update).

Warning

Fehler im Sinne einer Betriebsstörung werden durch die Warning-LED signalisiert. Die genaue Ursache können Sie als Administrator auf der Weboberfläche unter dem Menüpunkt „Diagnose“ sehen. Fehler dieser Kategorie treten meist durch Probleme in der Infrastruktur (z.B. Kommunikationspartner oder Dienst nicht erreichbar) oder eine fehlerhafte Konfiguration auf.

13. Technische Daten

Allgemeine technische Daten

Galvanische Trennung:	Digital-Ausgänge - Netzwerk: min. 1000V Digital-Eingänge - Netzwerk: min. 2000V Digital-Eingänge - Ausgänge: min. 1000V
Protokolle:	HTTP, HTTPS, REST TCP- und UDP-Sockets, Client und Server SNMP inkl. Traps SMTP E-Mail-Versand OPC- DA / OPC UA / Modbus-TCP Inventarisierung, Gruppenmanagement
Antwortzeiten:	Daten- und Schaltverkehr: typ. 40ms
Schutzklasse:	IP20
Lagertemperatur:	-25°C .. 70°C
Betriebstemperatur:	0°C .. 60°C
Zulässige Luftfeuchtigkeit:	5..95% relative Feuchte (nicht kondensierend)

Web-IO #57150

Anschlüsse, Anzeigen und Bedienelemente:

Digitale Ausgänge:	2 potentialfreie Kontakte in Relais-technik CO für 24V/2A DC für 48V/0,5A DC für 48V/2A AC max. 1800 Schaltzyklen pro Stunde
Digitale Eingänge:	2 x Digital Input für die Überwachung potentialfreier Kontakte integrierter 32-Bit Impulszähler
Netzwerk:	10/100BaseT autosensing
Stromversorgung:	12-48V DC (ca. 100mA@24V) PoE - Power over Ethernet
Anschlüsse:	1 x 11-fach Schraubklemme für IOs und Vcc 1 x RJ45 für Netzwerk

Anzeigen: Status-LEDs Netzwerk
Status-LEDs für Fehler- und Betriebszustände
LEDs für digitale Schaltzustände

Gehäuse und sonstige Daten:

Gehäuse: Kunststoff-Gehäuse
zur Hutschienen-Montage
90x46x56 mm (lxbxh)

Gewicht: ca. 200 g

Web-IO #57151

Anschlüsse, Anzeigen und Bedienelemente:

Digitale Ausgänge: 3 potentialfreie Kontakte in Relais-technik NO
1 potentialfreier Kontakt in Relais-technik CO
für 24V/2A DC
für 48V/0,5A DC
für 48V/2A AC
max. 1800 Schaltzyklen pro Stunde

Netzwerk: 10/100BaseT autosensing

Stromversorgung: 12-48V DC (ca. 100mA@24V)
PoE - Power over Ethernet

Anschlüsse: 1 x 11-fach Schraubklemme für IOs und Vcc
1 x RJ45 für Netzwerk

Anzeigen: Status-LEDs Netzwerk
Status-LEDs für Fehler- und Betriebszustände
LEDs für digitale Schaltzustände

Gehäuse und sonstige Daten:

Gehäuse: Kunststoff-Gehäuse
zur Hutschienen-Montage
90x46x56 mm (lxbxh)

Gewicht: ca. 200 g

Web-IO #57738

Anschlüsse, Anzeigen und Bedienelemente:

Digitale Ausgänge:	7 potentialfreie Kontakte in Relaischnik CO 1 potentialfreie Kontakte in Relaischnik NO für 24V/2A DC für 48V/0,5A DC für 48V/2A AC max. 1800 Schaltzyklen pro Stunde
Digitale Eingänge:	12 x Digital In, max. Eingangsspannung +/-30V verpolungssicher innerhalb dieses Bereichs Schwelle 8V +/- 1,5V „Ein“-Strom = 2,2 mA integrierter 32-Bit Impulszähler
Netzwerk:	10/100BaseT autosensing
Stromversorgung:	12-24V DC (ca. 100mA@24V) PoE - Power over Ethernet
Anschlüsse:	3 x 12-fach Schraubklemme für IOs 1 x 11-fach Schraubklemme für IOs 1 x RJ45 für Netzwerk
Anzeigen:	Status-LEDs Netzwerk Status-LEDs für Fehler- und Betriebszustände LEDs für digitale Schaltzustände

Gehäuse und sonstige Daten:

Gehäuse:	Kunststoff-Gehäuse zur Hutschienen-Montage 90x116x56 mm (lxbxh)
Gewicht:	ca. 310 g



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