



SITEMANAGER

USER MANUAL

DE



Inhalt

Willkommen	8
<i>Funktionsumfang der Managementsysteme</i>	9
Stromanschluss	10
Einbindung in das Netzwerk	10
<i>Erstkonfiguration über den Konfigurationsmodus 10.10.10.10</i>	11
<i>Vorbereitungen am PC</i>	11
<i>Der DHCP-Modus</i>	12
<i>Benötigte Informationen im DHCP-Modus</i>	13
<i>Netfinder: IP-Adressen suchen und auslesen</i>	13
Betriebsmodi der Manager	14
<i>Der Konfigurationsmodus</i>	14
<i>Der reguläre Betriebsmodus</i>	14
<i>Der manuelle Modus</i>	14
<i>Der DHCP-Modus</i>	14
Der Rettungsmodus	15
Bevor Sie mit der Konfiguration beginnen	15
<i>Installationsbeispiele</i>	15
<i>Benötigte Ports</i>	18
Erster Login: Vordefinierte Benutzer	18
Der Setup Wizard	19
<i>General</i>	19
<i>Network</i>	19
<i>Date & Time</i>	20
<i>UPS-Setup</i>	20
<i>Review</i>	20
Grundlegende Einstellung im Konfigurationsmodus	20
<i>Wired LAN und Wi-Fi</i>	20
<i>Besonderheit Erstkonfiguration im DHCP-Modus</i>	21
<i>WLAN – Die Wi-Fi Schnittstelle</i>	21
Weitere Grundeinstellungen	21
<i>Eingabe der Kontakt- und Standortdaten</i>	21
<i>Angabe von Region und Maßeinheit der Temperatur</i>	22
<i>Unterschied Fahrenheit / Celsius</i>	22
Dienste	23
<i>Webserver</i>	23
<i>SNMP</i>	24
<i>Modbus</i>	24
<i>BACnet Server</i>	24
<i>Serial Trace</i>	24
<i>UNMS & RCCMD Trap Service</i>	24
<i>RSyslog Client</i>	24
<i>BACS Viewer</i>	25
Datum und Uhrzeit	25
<i>Automatische Korrektur der Uhr</i>	25
Erweiterte Nutzerverwaltung	26

Nutzerrollen.....	26
Verfügbare Nutzer.....	26
Der Administrator.....	26
Der Techniker.....	26
Der Kunde.....	26
Gastzugang.....	26
Nutzermanagement unter RADIUS.....	27
Systemübersicht: Die About-Seite	28
Das System und die Firmware.....	28
Reboot und Kaltstart	29
Kaltstart.....	29
Warmstart - Reboot Der Neustart-Button.....	29
Konfiguration der Systembenachrichtigungen	29
E-Mail - Einstellungen.....	29
Mailserver.....	30
SMTP-Port.....	30
Connection Security.....	30
Sender Email Address.....	30
Email Authentifizierung verwenden, Nutzer und Passwort.....	30
Advanced Options.....	30
Format.....	30
Log.....	30
Automatically send an EMail.....	30
Testen der Maileinstellungen.....	31
Connection refused - Die häufigste Fehlermeldung:.....	31
Email-Traps.....	31
Modbus	31
Modbus in Geräten.....	32
Modbus als Single-Master-Protokoll.....	32
Modbus über RS232 und Modbus over IP.....	32
Modbus Funktionscodes.....	32
Modbus Fehlercodes.....	32
Konfiguration von Modbus.....	33
Enable Modbus Slave.....	33
TCP Port 502.....	33
Slave Address.....	34
Baud Rate.....	34
Parity.....	34
Stop Bit.....	34
Übernehmen / Abbrechen.....	35
Weiterführende Dokumente und Modbus-Listen.....	35
SNMP Agent	35
Der SITEMANAGER 7 unterstützt die SNMP v2 und SNMP v3.....	36
Einrichten von SNMP V2.....	36
IP-Adresse.....	36
Permission.....	36

Einrichten von Trap Empfängern	36
Konfigurieren von Trap-Empfängern auf dem SITEMANAGER 7	36
Test der Trap Empfänger.....	37
Einrichten von SNMP v3.....	37
User Definition.....	38
Authentication.....	38
Einrichten von TRAP Empfängern unter SNMP v3	38
Test der Trap Einstellungen.....	39
Allgemeine Interfaceeinstellung der COM-Ports.....	39
COM 1.....	39
COM 2 – Sensor	39
COM 3.....	39
USB – Port.....	39
Einstellen der USV	40
Übersicht der Einstellungen.....	41
Model	41
Leistung (VA).....	42
Last (VA)	42
Haltezeit (Min)	42
Akkuladezeit	42
Baud Rate	42
Kabeltyp	42
Batterieinstallationsdatum.....	42
Batterie veraltet nach.....	42
System Shutdown Zeit.....	42
UPS-ID.....	42
Übernehmen / Abbrechen.....	42
Besonderheit: Die RFC1628 USV Schnittstelle.....	43
Einrichten der Zielkarte unter SNMP v2	44
Modell.....	44
SNMP-Version.....	44
SNMP Community	44
Übernehmen/Abbrechen.....	44
Einrichten der Zielkarte unter SNMP v3.....	44
USV-Monitor: Überprüfen der Einstellungen	45
Die USV Funktionen	45
Funktionserklärung.....	45
Custom Test.....	46
Battery Test.....	46
Full Test	46
Selftest	46
UPS Control settings	46
Schaltbare Ausgänge	46
Einstellen der Systemereignisse.....	47
Definition eines Jobs für ein Ereignis	48
Jobs verwalten	48

Symbole mit eindeutiger Funktion.....	48
Symbole mit Doppelfunktion:	48
Einrichten eines Jobs	48
Verfügbare Jobs.....	49
Besonderheiten beim Job UPS Shutdown	49
Definition eines UPS Shutdowns	50
Zeit zum Ausschalten in Sekunden.....	50
Zeit zum Anschalten in Sekunden.....	50
Type	50
Verwendung des Jobs UPS Shutdown	50
Jobs suchen und anzeigen.....	50
Ereignis: contains	50
Jobs	50
Job Defintion: Auswählbare Zeitfenster:	51
Zeitmanagement der Jobs in Relation zur USV	51
Multiple Jobs hinzufügen	52
Löschen von Jobs	52
Gegenereignissen Jobs zuweisen	53
Custom Thresholds	54
Unterschied zwischen Warning und Alarm Levels	54
Beispielkonfiguration: UPS Temperature	54
Einstellen der Alarm Levels	55
Exemplarischer Auszug: Custom Thresholds	56
Beispielszenario: Custom Thresholds.....	57
RCCMD	58
Was ist RCCMD.....	58
Konfiguration von RCCMD	58
Einstellen eines RCCMD-Jobs	59
Einstellen der IP-Adresse für RCCMD.....	59
Broadcast.....	59
Eingrenzen auf IP-Adressen.....	59
Port	60
Zeitpunkt für RCCMD definieren.....	60
Die RCCMD-Kommandos	61
Der RCCMD Shutdown.....	61
Die RCCMD Message	61
Konfiguration eines RCCMD Executes	61
Die RCCMD Traps	62
SITEMANAGER 7 - spezifische Geräte und Sensoren	63
Der Kabelkamm	63
Sensoren und Geräte	63
Konfiguration der Sensoren im SITEMANAGER 7.....	64
Anschluss der Sensoren.....	64
Verwendung der analogen und digitalen Anschlüsse.....	65
Analoge Sensoren.....	65
Definition der Alarmschwellenwerte	66

Sensor Bereich.....	66
Voralarm und Alarm.....	66
Die digitalen Inputs.....	67
Name	67
NC Kontakt.....	67
Aktiv	67
Sitemanager 7 Outputs.....	67
Name	68
Anschalten	68
Delay.....	68
Erweitertes Monitoring	68
Digital Output	68
Analog Alarms.....	68
Die System Status LEDs	68
Besonderheit: Power LED	68
SITEMANAGER 7: Sensoren ein Ereignis zuweisen	69
Analogen Inputs Systemereignisse zuweisen	69
Digitalen Inputs Systemereignisse zuweisen	70
Besonderheit beim JOB AUX:	70
Scheduler.....	71
Webserver.....	72
Aktivieren / Deaktivieren der Weboberfläche	72
Konfiguration des Webzugriffs.....	72
Übersicht der Grundeinstellungen.....	72
HTTP Port	73
HTTPs Port.....	73
Force HTTPs.....	73
HTTP Aktualisierungszeit	73
Verwende einfachen Monitor	73
Automatischer Logout.....	74
Zertifikatsverwaltung / https – Zugriff	74
Diagnose: Statusleiste und LED's	74
Logfiles	75
Das Eventlog.....	75
Das Datalog	76
Datalog Chart – Grafische Darstellung	77
Übersicht	77
Kalenderfunktion.....	78
Zoom – Funktion.....	78
Toolbox.....	79
Reboot / Kaltstart.....	79
Tracer	79
COM 1/ UPS.....	79
COM 2 / GSM-Modem.....	79
COM 3 / AUX.....	79
Network-Scan.....	80

<i>Netzwerkscan: Auswertung der Daten</i>	80
<i>Löschen von Logfiles</i>	81
<i>Logo austauschen</i>	81
<i>Datensicherung und Updates</i>	82
<i>Wenn gar nichts mehr geht – das Rettungssystem</i>	85
<i>FAQ – Frequently Asked Questions</i>	87
<i>Anhang: Hardware Layout und Anschlüsse CS141 / SITEMANAGER 7</i>	89
<i>Urheberrechts-Erklärung zum geistigen Eigentum und Umgang mit vertraulichen Informationen</i>	96

Willkommen

Wir bedanken uns für das Vertrauen in die umfangreiche Produktfamilie der CS141 Webmanager – die zuverlässige Lösung im kritischen Ressourcenmanagement.

Die CS141 wurde speziell für den Einsatz im kritischen Ressourcenmanagement entwickelt. Da der CS141 als vollwertiger und eigenständiger Manager entwickelt wurde, ist seine Aufgabe nicht auf das Sammeln und Weitergeben von Informationen beschränkt, sondern erfüllt zahlreiche Aufgaben in der Mess-, Regel- und Steuertechnik im Bereich des kritischen Ressourcenmanagements. Eine weitere Kernfunktion liegt in Nachrichtenmanagement:

Der CS141 kann nicht nur Anfragen von übergeordneten Systemen beantworten, sondern im Notfall auch eigenständig Verantwortliches Personal informieren und auf Basis vorherbestimmter Parameter Notfallmaßnahmen einleiten. Der CS141 kann im selbstständig Notfallsysteme aktivieren, Server und Arbeitsstationen herunterfahren und zu vorbestimmten Bedingungen wieder starten. Neben Standardtechnologien wie SNMP und Modbus greift der CS141 dabei exklusiv auf die leistungsfähige RCCMD Softwarelösung zurück, mit der selbst das Notfallverhalten komplexer, voll virtualisierter Serverlandschaften realisiert werden kann.

Noch mehr Flexibilität dank RFC1628

Dank der neuen RFC1628 konformen USV-Schnittstelle können Sie den CS141 nutzen, um jede USV, die diesen Standard unterstützt, über das bestehende LAN abzufragen und den aktuellen Status nativ anzeigen lassen. Sollten Sie also eine USV im Einsatz haben, dessen Schnittstellen wider Erwarten mit dem CS141 nicht kompatibel ist, Sie können über diese Funktion mit wenig Aufwand und Kosten eine Kompatibilität herstellen und damit auf die leistungsfähigen und zuverlässigen GENEREX-Produkte wie das von GENEREX entwickelte RCCMD zurückgreifen.

Tipp:

Da der CS141 Webmanager als eigenständiger Manager agieren kann, ist er flexibel in sehr vielen Bereichen auch außerhalb der in diesem Handbuch beschriebenen Funktionalität einsetzbar. Dieses Handbuch beschreibt daher die grundsätzlich implementierte Funktionalität in Verbindung mit USV-Systemen. Die enorme Flexibilität und die Möglichkeit, mit über- und untergeordneten Systemen in Echtzeit zu kommunizieren.

So individuell wie Ihr Netzwerk

Der SITEMANAGER 7 passt sich flexibel an Ihre speziellen Netzwerkanforderungen an. Dieses Handbuch beschreibt alle Menüs, die Ihnen bei der Konfiguration der folgenden Geräte begegnen können:

- SITEMANAGER 7

Bitte beachten Sie, dass – obwohl es viele Überschneidungen – aus technischen Gründen nicht alle Zubehörteile vollständig kreuzkompatibel sind, auch wenn die äußere Steckerkonfiguration passen würde.

Darunter fallen zum Beispiel:

- Zusätzliche Sensoren und Geräte

Hierunter fallen zum Beispiel das GSM-Modem, analoge Sensoren sowie der Sensormanager II oder das Relayboard CON_R_AUX / 4 bzw. die BACS-Version GX_R_AUX

- AUX-Geräte und BACS-Aufrüstbarkeit

Der SITEMANAGER 7 bietet neben schaltbaren Ausgängen Analoge und digitale Inputs, wahlweise über die Klemmleiste oder die analogen Sensoreingänge sowie die vollständige BACS-Funktionalität

Das Herz des SITEMANAGER 7 ist der leistungsfähige CS141 verwendet:

Anders als beim CS141 ist der COM-Port 1 hier die Schnittstelle zur USV und kann nicht für Sensoren verwendet werden. Die Menüs weichen hierbei von der CS141 – Standardoberfläche ab, und einige Funktionalitäten sind anders.

Wenn Ihr Gerät ein Hardwarelayout nicht anbietet, werden Ihnen die entsprechenden Menüs innerhalb der Software nicht angeboten.

Funktionsumfang der Managementsysteme

Hardware:

Der SITEMANAGER und SITEMONITOR sind speziell in der Bauform für den Einsatz in Standard Server Racks konzipiert. Zubehörteile können je nach Bedarf zum Beispiel über genormte DIN-RAILS entsprechend in der Nähe befestigt werden. Der SITEMANAGER und der SITEMONITOR bieten die Möglichkeit, als SNMP – Adapter direkt mit einer RS-232 – Schnittstelle oder über die RFC1628 smart UPS-Schnittstelle über LAN mit der USV zu kommunizieren und als vollwertiger Webmanager zu agieren.

Das beinhaltet:

-SNMP und SNMP-Traps:

Das SNMP (Simple Network Management Protocol) ist ein Internet-Standard-Protokoll, um Anlagen über IP-Netzwerke zu überwachen. Das Protokoll ist definiert und standardisiert in RFC-Spezifikationen. USV-Systeme verwenden im Allgemeinen als MIB die RFC 1628-Spezifikation, die USV-spezifische Geräte definiert. Daher ist es meist nicht notwendig eine eigene MIB in die SNMP-Software einzufügen.

SITEMANAGER und SITEMONITOR können zahlreiche Aufgaben erfüllen. Beispielsweise können Spannungsversorgung und der Batteriezustand einer USV von einer SNMP-Managementstation überwacht werden, Türkontakte, oder Zugriffskontrollen aktiv geschaltet werden, etc. Die aktuellen Schaltzustände können sowohl zeitlich gesteuert als auch und reaktiv in Form von Schaltketten inklusive eines Feedbacks geschaltet werden. Zu jedem Schaltzustand kann eine speziell definierte Nachricht automatisch versendet werden.

-Fernbedienung von USV-Systemen:

Über diese Funktion kann die USV beispielsweise auf Bypass geschaltet werden (herstellerabhängig); ausgelöst wird dieses durch ein entsprechendes Kommando über die Network Management Station oder durch die zur USV gehörige USV Management Software für das Web.

-Multipler Shutdown per RCCMD:

Der CS141 kann mit allen RCCMD Modulen der UPS-Management Software einen Netzwerk-Shut-Down einleiten. Ein auf TCP/IP basierendes RCCMD Sendesignal wird an alle konfigurierten RCCMD-Clients versendet. Damit kann auch Shutdown auf unbegrenzt vielen Computern ausgelöst werden, unabhängig von deren Betriebssystem. RCCMD ist optionaler Bestandteil der USV Management Software. USV-Management Software und RCCMD Lizenzen sind beim USV Fachhändler erhältlich.

-Zeitgenaues Logfile:

Sowohl SITEMONITOR als auch SITEMANAGER besitzen eine Reihe eigener Logfiles, um Ereignisse und Alarmer genau zu protokollieren. Dieses Logfile ist per UNMS, UPSMAN, WebGUI sowie FTP zugänglich. Der Export als CSV-Datei erlaubt hierbei ein leichtes Archivieren für spätere Diagnosen

-Kommunikation über E-Mail:

Die CS141 Modelle besitzen einen Simple Mail Transfer Protokoll (SMTP) kompatiblen E-Mail-Client, der automatisch Emails bei Ereignissen versenden kann.

-Integration in Network Management Systeme

Der SNMP-Adapter ist mit allen gebräuchlichen Networks Management Systemen kompatibel. Alle SNMP-Systeme, die das Kompilieren einer MIB erlauben – oder bereits die Management Information Base (MIB) / Request for Comment 1628 (RFC) für USV Systeme enthalten, können mit dem Adapter betrieben werden. Über potentialfreie Kontakte kann zudem mit Über- und Untergeordneten Monitoring- und Managementsystem interagiert werden.

-Moderne Webtechnologie für leichte Konfiguration:

Die Modelle der CS141 Produktfamilie besitzen einen Webserver, der alle Informationen des Gerätes anzeigt. Mit dem UPSView kann eine grafische Darstellung der Daten angezeigt werden. Der Zugriff auf das Webinterface ist mit einem gängigen Webbrowser möglich.

-Modbus-Unterstützung

Sowohl der SITEMANAGER als auch der SITE-MONITOR bieten standardmäßig mit Modbus over IP eine Anbindung an bestehende Modbus-Infrastrukturen an.

-RS-232 / Pipe-through:

Der SNMP Adapter Typ CS141 kann das USV-Protokoll, welches über COM1 gelesen wird, direkt auf COM2 wieder ausgeben. Damit ergibt sich die Möglichkeit weitere Software / Hardware an die USV anzuschließen ohne zusätzliche Verteiler-Hardware (RS-232 Multiplexer) einzusetzen.

- UPSTCP:

Der gängigste Weg, um mit dem CS141-Adapter zu kommunizieren ist TCP. Der CS141 beinhaltet UPSTCP, welches ihnen eine komplette API-Schnittstelle bietet, um ihren Adapter in das Netzwerk zu integrieren. Diese Schnittstelle wird auf Wunsch an Hersteller von Software geliefert, um eine eigene Einbindung zu ermöglichen. Alle anderen Anwender verwenden TCP für den Zugriff über ein Webinterface (UPSVIEW, UPSMON, UNMS) oder SNMP oder MODBUS over IP.

Stromanschluss



Der SITEMANAGER und SITE-MONITOR 6 bieten Ihnen Flexibilität bei der Anbindung an das Stromnetz:

Standardmäßig werden beide Geräte mit einem 24V /1,5A - Netzteil geliefert. Die Anschlussklemme ist kodiert, um ein Verpolen zu verhindern.

Unter bestimmten Bedingungen kann es notwendig oder sinnvoll sein, eine alternative Stromquelle zu verwenden.



Aus diesem Grund ist der Verbindungsstecker modular konzipiert. Der Sitemanager 6 passt sich dynamisch an die Eingangsspannung an:

Minimum: 18 VDC

Maximum: 75 VDC

Bitte beachten Sie beim Anschluss eigener Spannungsquellen die korrekte Polung, um Schäden am Gerät zu vermeiden.

Einbindung in das Netzwerk

Alle Modelle der CS141-Familie werden ausschließlich über die speziell entwickelte Weboberfläche des Adapters konfiguriert. Um die Erstkonfiguration oder einen schnellen Eingriff vor Ort zu erleichtern, ist Webmanager der CS141-Familie hardwareseitig auf die IP-Adresse 10.10.10.10 voreingestellt:



Sie erkennen diese Voreinstellung, wenn der Schiebeschalter auf der Stirnseite in der Mittelstellung steht. Die einzige Ausnahme bildet hier der CS141 MINI, welcher auf Grund seiner kompakteren Bauform auf der Platine Dip-Schalter verwendet. Die Mittelstellung bzw. beide Dip-Schalter auf off aktiviert den sog. Konfigurationsmodus. In diesem Modus einige Funktionen wie zum Beispiel die Eingabe der IP-Adressdaten konfigurierbar, sind jedoch erst verfügbar, sobald Sie in den regulären Betriebsmodus wechseln.

Die folgende Tabelle zeigt die Möglichkeiten der regulären Betriebsmodi im Standard-Betrieb:

<p>Schalterknopf mittig: versetzt das Gerät in den Konfigurationsmodus und aktiviert die Standard IP-Adresse 10.10.10.10. nach einem Kaltstart.</p>	
<p>Schalterknopf rechts: Automatische IP-Adressierung: DHCP ist aktiviert und eine IP-Adresse wird automatisch gesetzt. Prüfen Sie die MAC-Adresse von Ihrem Gerät, um die IP- Adresse in der DHCP-Server-Tabelle identifizieren zu können.</p>	
<p>Schalterknopf links: Verwendung der im HTTP-Interface konfigurierten Werte. Mit gesonderter Einstellung auch DHCP möglich.</p>	

[Erstkonfiguration über den Konfigurationsmodus 10.10.10.10](#)

Vorbereitung am SITEMANAGER 7

Bringen Sie vor der Inbetriebnahme den Schiebeschalter auf der Rückseite in Mittelstellung Nach dem Bootvorgang befindet sich der Manager im Konfigurationsmodus und ist auf der hardwareseitig voreingestellten IP-Adresse 10.10.10.10 erreichbar.

Tipp:

Der Moduswechsel über die Hardwareschalter erfordert einen Reboot. Den Neustart können Sie über zwei Wege durchführen:

- Durch kurzes Entfernen der Stromversorgung (Hardware Reset)
- Über die Neustartfunktion im Menü Tools (Software Reset)

Dieser Vorgang bezieht sich nicht auf die angeschlossene USV – diese läuft unabhängig von dem Webmanager weiter.

Vorbereitungen am PC

Nach dem Systemstart im Konfigurationsmodus ist der Webmanager physikalisch in folgendem Netzwerk zu finden:

IP – Adresse 10.10.10.10
Subnetzmaske: 255.255.255.0

Die empfohlenen Netzwerkeinstellungen für den Client-PC zur Einrichtung sind:

IP-Adresse 10.10.10.11
Subnetzmaske 255.255.255.0
Gateway 10.10.10.11 (wird dann automatisch ausgeblendet)
DNS leer

Kontrollieren Sie die Einstellungen Ihres Service-Computers, indem Sie eine Konsole öffnen und den Befehl `PING 10.10.10.10` eingeben. Wenn die Einstellungen richtig sind, wird der CS141 auf entsprechend antworten:

```
C:\Users\Gunnar>ping 10.10.10.10

Ping wird ausgeführt für 10.10.10.10 mit 32 Bytes Daten:
Antwort von 10.10.10.10: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 10.10.10.10:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (<0% Verlust>),
    Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms

C:\Users\Gunnar>
```

Im Anschluss können Sie einen Webbrowser öffnen und das Webinterface des SITEMANAGER 7 über die Anfrage `http://10.10.10.10` direkt erreichen und mit der Konfiguration beginnen.

Eine Route hinzufügen

Innerhalb größerer Installationen mit fest definierten Domänenbeitritten kann es hilfreich sein, temporär eine Route zu verwenden.

In diesem Fall muss sichergestellt sein, dass der SITEMANAGER 7 innerhalb sich im selben Netzwerksegment befindet und dem entsprechend direkt erreichbar ist.

Beispiel: Route bei einem Windows-PC hinzufügen:

1. Öffnen Sie die Kommandokonsole cmd als *Administrator*
Dieser Schritt ist deshalb wichtig, weil Windows einen Nutzer mit lokalen Administrationsrechten benötigt, um eine Route hinzufügen zu können.
2. Geben Sie folgenden Befehl ein: `route add 10.10.10.10 <Ihre IP-Adresse>`
Windows antwortet in diesem Fall mit OK

```
C:\Windows\system32>route add 10.10.10.10 192.168.200.17
OK!
```

Um die neu angelegte Route zu überprüfen, geben Sie den Befehl `route print` ein:

```
Pv4-Routentabelle
=====
Aktive Routen:
  Netzwerkziel    Netzwerkmaske    Gateway          Schnittstelle    Metrik
  0.0.0.0         0.0.0.0         192.168.200.1   192.168.200.17   20
  10.10.10.10    255.255.255.255  Auf Verbindung  192.168.200.17   21
  127.0.0.0      255.0.0.0       Auf Verbindung  127.0.0.1        306
  127.0.0.1      255.255.255.255  Auf Verbindung  127.0.0.1        306
  127.255.255.255 255.255.255.255  Auf Verbindung  127.0.0.1        306
  192.168.200.0  255.255.255.0   Auf Verbindung  192.168.200.17   276
```

Den Eintrag 10.10.10.10 finden Sie unter *Aktive Routen*. Als Zusätzlichen Test können Sie mit dem Befehl `ping 10.10.10.10` kontrollieren, ob der Webmanager erwartungsgemäß antwortet.

Tipp:

Im Konfigurationsmodus können immer nur einen CS141 mit der voreingestellten IP-Adresse 10.10.10.10 betreiben. Sollten Sie mehrere Geräte gleichzeitig anschließen wollen, gibt es im Konfigurationsmodus einen Netzwerkkonflikt.

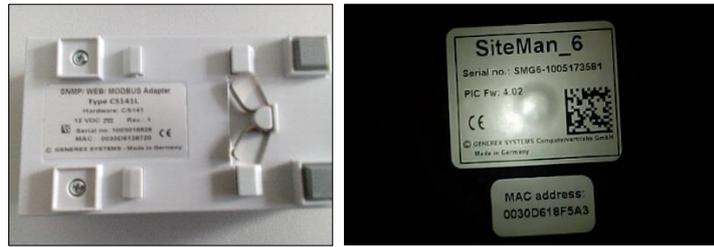
Der DHCP-Modus

Da die Modelle der CS141 – Familie auf Grund ihrer Flexibilität sehr viele Funktionen erfüllen können, ist es ein durchaus realistisches Szenario, dass Sie innerhalb einer Installation mehrere Geräte gleichzeitig in Betrieb nehmen müssen und vorläufig keine feste IP-Adresse vergeben werden kann.

Um den DHCP-Modus zu aktivieren, schieben Sie den Schiebeschalter nach rechts, also zur Außenkante des CS141. Bei dem CS141 Mini lassen Sie den Dip-Schalter 1 auf OFF und bewegen den Dip-Schalter 2 auf ON. Beim Nächsten Neustart wird der Webmanager entsprechend der Hardwarekonfiguration im DHCP-Modus booten und sich eine IP-Adresse aus Ihrem Netzwerk beziehen

Benötigte Informationen im DHCP-Modus

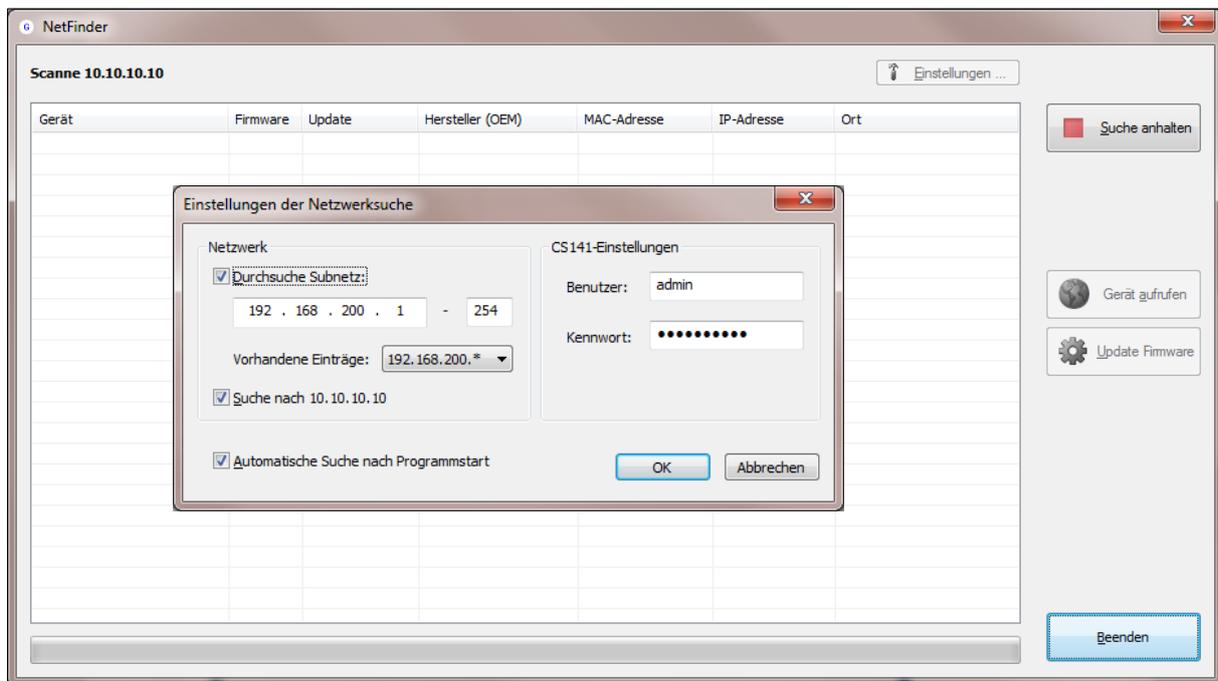
Um die Geräte nach der hardwareseitigen Installation eindeutig zuordnen zu können, notieren Sie sich vor der Installation die MAC-Adresse und den Installationsort, welche auf jedem Webmanager der CS141-Familie als Aufkleber zu finden ist:



Stellen Sie sicher, dass für diesen Betriebsmodus ein passender DHCP-Server zur Verfügung steht, da ansonsten der automatische Bezug der IP-Adressdaten nicht möglich ist.

Netfinder: IP-Adressen suchen und auslesen

Um die IP-Adressen auszulesen, nutzen Sie das Tool Netfinder, welches auf der Support-CD sowie unter www.generex.de zum Download bereit steht. Der Netfinder ist ein nützliches Softwaretool, welches alle in einem Netzwerk erreichbaren CS141 und SITEMANAGER 7 – Geräte anzeigen kann.



Die Standard-Suche bezieht sich immer auf das Netzwerksegment, in dem sich der Service-Computer befindet. Um andere Netzwerke und Subnetze CS121 oder CS141-Installationen zu scannen, geben Sie die entsprechenden IP Adressräume an.

Netzwerk von 192.168.222.1 bis 192.168.222.254 - scanne 192.168.222.168

Gerät	Firmware	Update	Hersteller (OEM)	MAC-Adresse	IP-Adresse	Ort
CS141L	1.61	Nicht nötig	ABB (36)	00-30-d6-16-1d-e7	192.168.222.106	
CS141BSC	1.60	Nicht nötig	Online (4)	00-30-d6-13-3d-eb	192.168.222.104	
CS141R_2	1.60	Nicht nötig	Piller (3)	00-30-d6-12-6e-c7	192.168.222.107	
CS141L	1.56	Verfügbar (1.58)	ABB (36)	00-30-d6-12-60-70	192.168.222.108	
CS141LM	1.60	Nicht nötig	AMG Accent Monitorin...	00-30-d6-12-0f-2b	192.168.222.110	
CS141SC	1.60	Nicht nötig	Salicru (82)	00-30-d6-16-bb-f3	192.168.222.112	
BACSKIT_B4	1.60	Nicht nötig	Generex (12)	00-30-d6-12-60-61	192.168.222.114	
BACS II Webmanager BUDGET	5.62	Nicht nötig	UPS LTD (84)	00-03-05-18-77-6A	192.168.222.113	
BACS II Webmanager BUDGET	5.62	Nicht nötig	Hoppecke (91)	00-03-05-18-59-7A	192.168.222.103	
CS131 16MB	5.62	Nicht nötig	ALTERVAC (92)	00-03-05-18-6A-A4	192.168.222.111	GENEREX Hamburg Garage
CS141BSC	1.60	Nicht nötig	CET (81)	00-30-d6-12-6f-9d	192.168.222.119	
CS131 16MB	5.34	Verfügbar (5.62)	Generex (12)	00-03-05-18-96-A2	192.168.222.123	

Der Netfinder gibt Ihnen einen detaillierten Überblick aller im Netzwerk abgebildeten Geräte und erlaubt einen schnellen und einfachen Zugriff auf die Webkonsole des entsprechenden Managers.

Tipp:

Im DHCP-Modus kann sich je nach Netzwerkkonfiguration die IP-Adresse sporadisch ändern. Webmanager, die von einem übergeordneten System wie z.B. die UNMS II überwacht werden sollen, sollten daher eine feste IP-Adresse erhalten. Ist dies nicht der Fall, kann man mit dem Netfinder alle Geräte wiederfinden.

Betriebsmodi der Manager

Unterschied zwischen, Konfigurations-, Rettungs- und Betriebsmodus

Alle Modelle der CS141 Familie werden ausschließlich über eine intuitive Weboberfläche konfiguriert. Dabei bieten die Webmanager fünf gültige Betriebszustände an, welche sich grundlegend voneinander unterscheiden.

Der Konfigurationsmodus

Der Schiebeschalter ist in diesem Fall in der Mittelposition.



Der Konfigurationsmodus ist der Modus, in dem der Manager standardmäßig ausgeliefert wird. In diesem Modus ist der Webmanager über eine hardwareseitig voreingestellte IP-Adresse 10.10.10.10 erreichbar und erlaubt alle systemrelevanten Einstellungen.

Da der Manager im Konfigurationsmodus generell die voreingestellte IP-Adresse verwendet, können Sie hier auch Datenbackups einspielen und nach dem Neustart anpassen.

Der reguläre Betriebsmodus

Der Schiebeschalter ist je nach Einstellung in der linken oder der rechten Position.

Je nach Einstellung befindet sich der CS141 im DHCP-Modus oder im manuellen Modus.

Der manuelle Modus



Im manuellen Modus legen Sie die IP-Adressdaten fest: Beachten Sie bitte, dass es bei falschen Einstellungen zu Adresskonflikten im Netzwerk kommen kann bzw. die getätigten Einstellungen nicht funktionieren. Die für den manuellen Modus notwendigen Daten können beim lokalen Administrator bezogen werden.

Tipp:

Im Manuellen Modus werden die Daten „von Hand“ eingetragen und damit fest vergeben: Der CS141 wird diese Daten benutzen, um sich im Netzwerk bekanntzumachen. Sollte es zu einem IP-Adresskonflikt kommen, weil die IP-Adresse doppelt vergeben wurde, können Sie jederzeit zurück in den Konfigurationsmodus wechseln und erreichen den Webmanager unter der voreingestellten IP-Adresse 10.10.10.10

Der DHCP-Modus



Im DHCP-Modus übernimmt der CS141 von einem Server zugewiesene Einstellungen automatisch und verwendet diese für die IP-Adresseinstellungen. Dabei übernimmt der Webserver die Verwaltung der IP-Adressdaten. Nach dem Startvorgang kann der Webmanager mit dem Tool *Netfinder* gefunden werden.

Tipp:

In der Regel werden per DHCP zugeteilte IP-Adressen nur für bestimmte Zeitfenster vergeben. DHCP Clients fragen daher nach 50% dieses Zeitfensters, ob die IP-Adresse noch gültig ist oder eine andere zugeteilt wurde. Wie statisch der DHCP-Server hier IP-Adressen vergibt, ist dabei eine Entscheidung, die der Systemadministrator trifft. Es kann daher passieren, dass bereits durch einen Neustart bereits eine andere IP-Adresse zugeteilt wird.

Bei der Wahl des Betriebsmodus sollte die Funktion des CS141 innerhalb des Netzwerks beachtet werden:

Wenn der Webmanager ein aktives Element innerhalb von Shutdown-Lösungen oder in Verbindung mit übergeordneten Monitoring-Strukturen sein soll, ist eine manuell vergebene IP-Adresse sinnvoll, da eine authentifizierte IP-Adresse konfiguriert werden muss. Ein weiterer Vorteil ist, dass der Webmanager durch vorkonfigurierte IP-Adressen im Notfall auch ohne einen vorhandenen DHCP-Server autonom startet.

Der Rettungsmodus

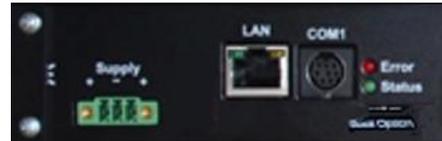
Bei diesem Modus ist ein zusätzlicher Jumper gesetzt und der Schiebeschalter in der mittleren Position:

Jeder Webmanager besitzt zwei ROMs, von denen gebootet werden kann. Vorgehalten werden hierbei die aktuelle Firmware sowie der letzte Zustand vor dem Firmwareupdate inklusive der Konfigurationsdatei. Wenn der Webmanager in den Rettungsmodus gesetzt wird, startet der Logik folgend von dem letzten bekannten Status und ist zunächst wieder voll einsatzbereit, zeigt jedoch in den allgemeinen Systeminformationen einen Vermerk, dass der Webmanager sich im Rettungsmodus befindet.

Der Rettungsmodus stellt einen Notfallbetrieb dar und ist dafür gedacht, z.B. einen fehlerhaften Flashvorgang zu wiederholen.

Um den Notfallmodus zu aktivieren:

1. Öffnen Sie das Gerät und suchen Sie die kleine Platine mit der Netzwerkschnittstelle – da die Platine selber nicht entfernt werden muss, können Sie sich an der Rückfront des Webmanagers orientieren:
2. Auf der geschraubten kleinen Platine finden Sie ein Flachband-Datenkabel und direkt darunter befindet sich ein geöffneter Jumper. Schließen Sie diesen Jumper und schließen den Stromadapter wieder an:



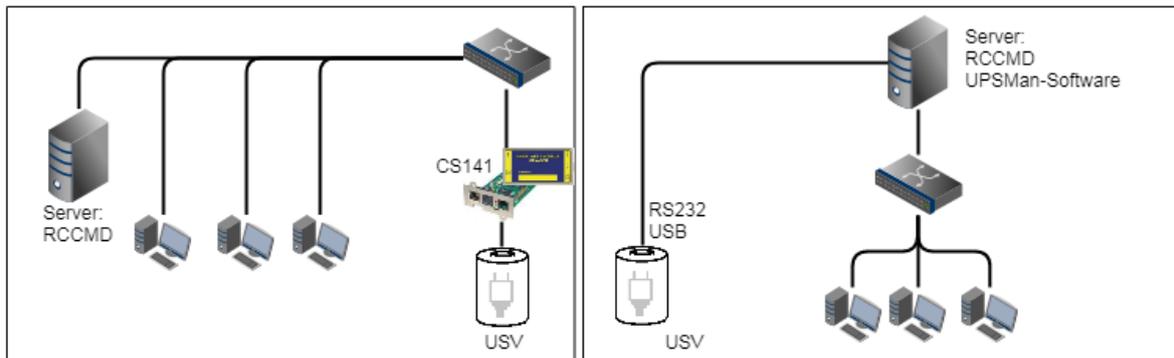
Der Webmanager wird automatisch im Rettungsmodus starten.

Bevor Sie mit der Konfiguration beginnen ...

Installationsbeispiele

Der CS141 wurde als Webmanager speziell darauf ausgelegt, Ihnen bei der Installation maximale Handlungsfreiheit zu geben, um dem stetig wachsenden Anspruch und die daraus resultierende zentrale Rolle moderner USV-Anlagen innerhalb der allgemeinen Stromversorgung gerecht zu werden:

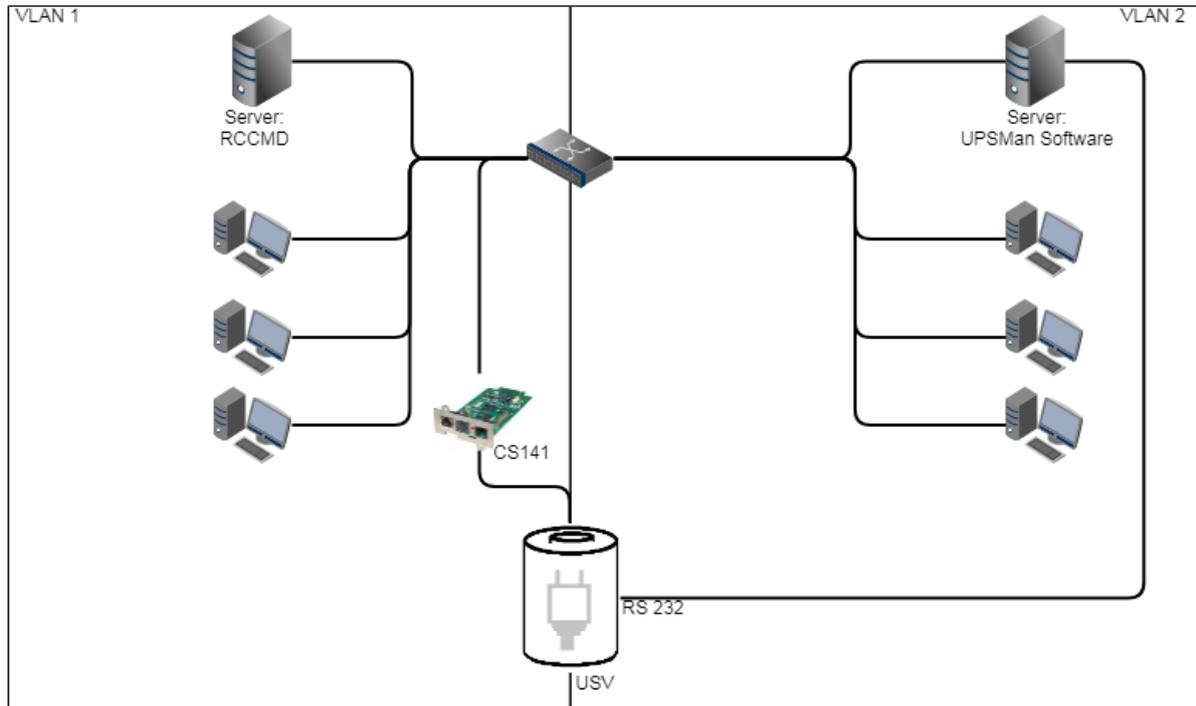
Der einfache Fall:



Die USV soll den Server absichern, bis dieser heruntergefahren wurde. Die vollständige Shutdown-Routine wird hierbei von dem CS141 gesteuert, da dieser ein vollwertiger Manager ist, welcher eigenständig handeln kann. Alternativ zum CS141 kann auch über die UPSMan-Software die Shutdown-Routine eingeleitet werden. Weitere Stationen und Server benötigen hier lediglich eine weitere RCCMD-Lizenz.

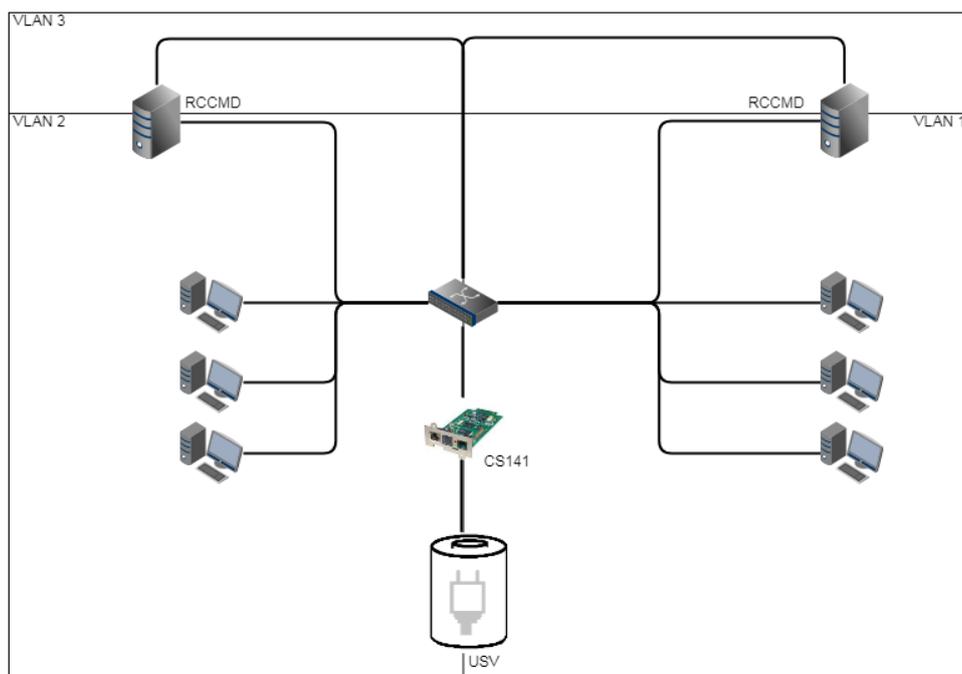
Zwei getrennte Netzwerke

Schwieriger wird es, sobald zwei Server über getrennte Netzwerke angebunden werden sollen, welche über dieselbe USV abgesichert werden:



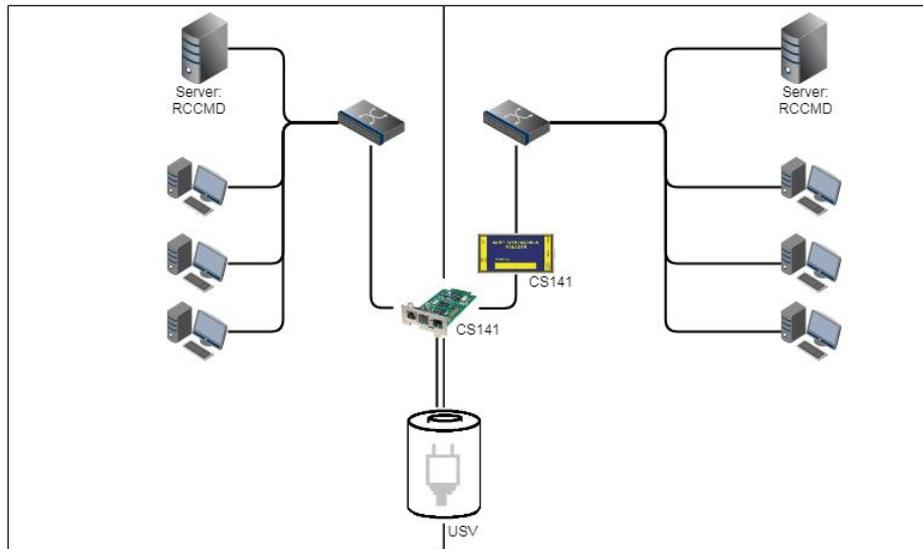
Die USV ist als zentraler Bestandteil von existenzieller Bedeutung. Da die VLANS physikalisch getrennt sind, kann lediglich in einem LAN der Server über den CS141 versorgt werden. Einfache Abhilfe schafft hier die UPSMan-Software, welche über den COM-Port des Servers mit der USV kommunizieren kann und dieselbe Funktionalität bietet wie der CS141 und beherrscht zusätzlich RCCMD. VLAN 2 repräsentiert hierbei eine „Software only“ – Lösung, bei der kein CS141 als zusätzliche Hardware benötigt wird.

Sollte dieser RS232 – Anschluss nicht zur Verfügung stehen, benötigen Sie lediglich Server mit jeweils 2 Netzwerkkarten:



Wenn Sie eine freie RS232-Schnittstelle haben, können Sie bei dieser Lösung die Schnittstelle für das nächste unabhängige Netzwerk nutzen, sofern die USV den Parallelbetrieb von Slot und RS232 unterstützt.

Pipe Through



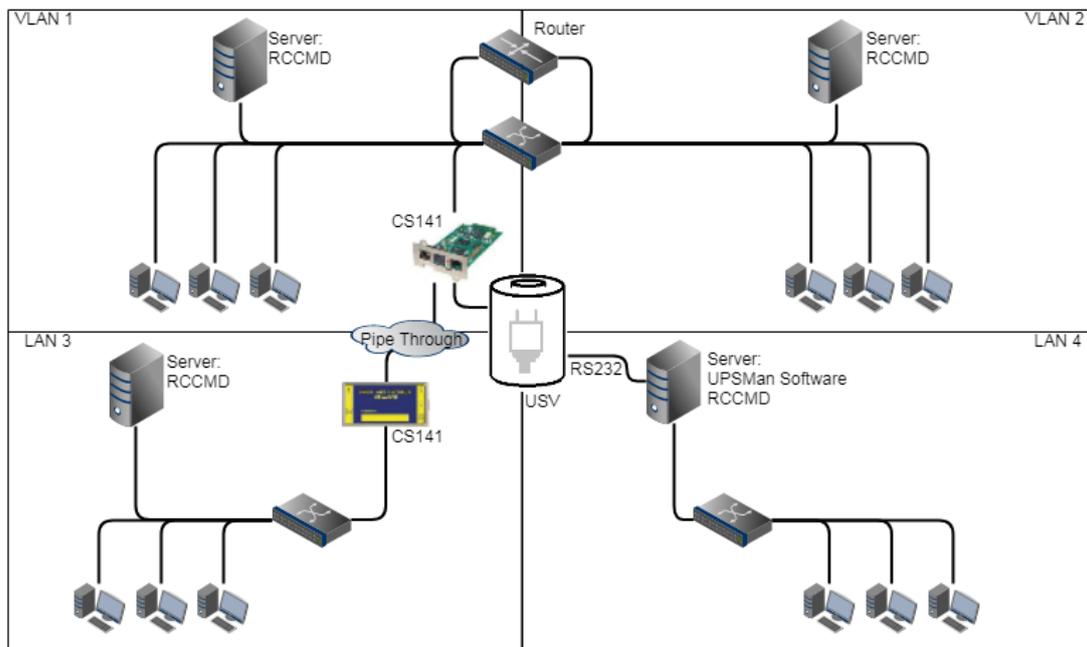
In einigen Unternehmen ist eine physikalische Trennung der Netzwerke unumgänglich, aber die USV bietet nicht die Option, RS232 und Slot parallel zu betreiben. In diesem Fall kann über die Pipe-Through – Funktion das Signal 1:1 durchgeschliffen werden, so dass zwei CS141 gemeinsam dieselbe Funktion ausfüllen können. Dabei können die unterschiedlichen CS141 – Versionen beliebig kombiniert werden. Auch die Kombination CS141/UPSMAN-Software ist möglich.

Technische Besonderheit SITEMANAGER 7

Der SITEMANAGER 6 verwendet als USV-Anschluss COM1 einen Mini-Din Anschluss an. Daraus ergibt sich, dass die Pipe-Through-Funktion generell unterstützt wird, jedoch technisch bedingt der SITEMANAGER 6 lediglich als letztes Gerät in der Pipe- Through -Kette verwendet werden kann.



Komplexe Strukturen



In diesem Beispiel wurden VLAN 1 und VLAN 2 mit einem Router logisch verknüpft, damit ein CS141 sowohl in VLAN 1 als auch in VLAN2 RCCMD-Kommandos an die Server übergeben kann. Die Pipe Through – Funktion ermöglicht gleichzeitig, dasselbe Signal an ein unabhängiges LAN 3 zu senden, in dem in weiterer CS141 als Manager dieselben Informationen über

den USV-Status bekommt. Über die RS232-Schnittstelle ist das LAN 4 mit der UPSMan-Software verbunden. Sie erhalten in diesem Beispiel zwei verbundene und zwei physikalisch isolierte Netzwerke, welche sich eine zentrale Stromversorgung teilen und zu jeder Zeit über den genauen Status der USV informiert sind.

TIPP:

Die UPSMan- Software beherrscht auch die Kommunikation über USB – Sollte Ihre USV den parallelen Betrieb unterstützen, können Sie einzelne Server mit installierter UPSMan-Software auch USB mit der USV verbinden.

Bitte beachten Sie bei der Installation:

Der SITEMANAGER 7 unterliegt bei verschachtelten Netzwerkstrukturen technisch bedingt einer Limitierung:

Sie können bei einer Installation, die Pipe Through voraussetzt, ausschließlich als zweites Gerät eingebunden werden, da der COM-Port-Port, der zum Durchschleifen von USV-Signalen benötigt wird, bereits ist.

Eine Möglichkeit, dies zu Umgehen wäre die gezielte Nutzung der RFC 1628 – USV Schnittstelle in Verbindung mit definiertem Routing.

Benötigte Ports

Der CS141 benötigt eine Reihe von Ports, welche offen bzw. verfügbar sein müssen. Einige Ports sind Standard Ports innerhalb Ihrer EDV, andere müssen exklusiv für den CS141 geöffnet oder verfügbar gemacht werden. Bitte überprüfen Sie vor Ort, ob die folgenden Ports verfügbar oder geöffnet sind:

Echo	7/tcp
echo	7/udp
WOL	9/udp
ftp-data	20/tcp
ftp	21/tcp
telnet	23/tcp
smtp	25/tcp
http	80/tcp
snmp	161/udp
snmptrap	162/udp
time (rfc868)	37/tcp
time (sntp)	123/tcp
rccmd	6003
Upsmon	5769
Modbus over IP	502/tcp

Tipp:

Dieses Benutzerhandbuch behandelt *alle* Menüs, welche Ihnen bei der Konfiguration eines CS141 begegnen können. Dabei ist die Grundlage dieser Dokumentation die Firmware 2.22 sowie nachfolgende Versionen. Wenn Sie ein Menü nicht finden, kann das mehrere Gründe haben:

Der von Ihnen verwendete CS141 bietet diese Funktion nicht an

Die Firmwareversion, die Sie verwenden, ist älter und das Feature ist daher noch nicht verfügbar

Das Menü ist vorhanden, hat sich jedoch durch den fortlaufenden Entwicklungsprozess verschoben

Erster Login: Vordefinierte Benutzer

Nachdem Sie die IP-Adresse eingegeben haben, meldet sich der CS141 mit seiner Weboberfläche und erwartet die Eingabe eines Passworts:

Nutzer: admin	Passwort: cs141-snmp	... Systemadministrator, volles Menü
Nutzer: engineer	Passwort: engineer	... Techniker, administrative Menüs gesperrt
Nutzer: customer	Passwort: customer	... Kunde, Zugang beschränkt auf Logfiles und Screens
Nutzer: guest	Passwort: guest	... Gastzugang, nur Statusanzeigen sichtbar

Wichtig: Bei der Ersteinrichtung ist nur der Benutzer „admin“ freigeschaltet! Weitere Nutzer müssen exklusiv zugelassen bzw. eingerichtet werden.

Um mit der Erstkonfiguration zu beginnen, melden Sie sich mit dem Nutzer admin und dem Standardpasswort cs141-snmp an:

Tipp:

Moderne Webbrowser sind darauf ausgerichtet, Webseiten möglichst schnell anzuzeigen. Dabei werden unter anderem Techniken verwendet, welche Bilder, Seiten und Abfragemasken in einen Zwischenspeicher geladen werden, um sie später noch einmal direkt anzeigen zu können. Das kann unter Umständen dazu führen, dass es zu einem Anzeige- oder Darstellungsfehler kommt, oder bestimmte Menüs augenscheinlich nicht mehr funktionieren:

Sollten diese Phänomene auftreten, aktualisieren Sie die Browseranzeige mit STRG + F5 oder löschen Sie den Cache des verwendeten Webbrowsers und deaktivieren Sie zusätzlich installierte Tools und Addons, welche die Darstellung behindern könnten.

Der Setup Wizard

Für diesen Konfigurationsschritt benötigen Sie das folgende Menü:



Wenn Sie den CS141 das erste Mal in Betrieb nehmen, startet automatisch der Willkommensschirm mit dem Wizard:

Folgende Grundeinstellungen können vorgenommen werden:

General

Geben Sie grundlegende Angaben über Ort, Kontaktperson, Ansprechpartner, Systemsprache und Temperaturskala an.

Network

Geben Sie die Netzwerkkonfiguration an – Die notwendigen Daten sind beim lokalen Administrator zu bekommen.

Date & Time

Geben Sie grundlegende Angaben über Datum, Uhrzeit und Zeitserver an.

UPS-Setup

Geben Sie die USV an, an die der CS141 angeschlossen und betrieben werden soll.

Review

Überprüfen Sie noch einmal alle Daten, bevor Sie mit Finish den Konfigurationsprozess beenden und der CS141 die Konfiguration übernimmt.

Tipp:

Der Setup Wizard fasst lediglich grundlegende Einstellungen zusammen und bietet eine schnelle und komfortable Lösung, über die grundlegende Einstellungen für eine schnelle Inbetriebnahme CS141 vorgenommen oder geändert werden können. Sollten Sie die Konfiguration vollständig manuell durchführen wollen, betätigen Sie hier *Cancel* – Sie können jederzeit den Setup Wizard im Konfigurationsmenü neu starten.

Grundlegende Einstellung im Konfigurationsmodus

Für diesen Konfigurationsschritt benötigen Sie das folgende Menü:



Wired LAN und Wi-Fi

Die meisten Einstellungen lassen sich im Konfigurationsmodus vornehmen, jedoch sind Tests sowie Weiterleitungsfunktionen oftmals nicht möglich, da der Webmanager hardwareseitig auf die IP-Adresse 10.10.10.10 eingestellt ist. Daher ist es empfehlenswert, die Grundeinstellungen im Konfigurationsmodus durchzuführen und danach in den manuellen Betriebsmodus zu wechseln. Um den Webmanager in Ihr Netzwerk einzubinden, öffnen Sie das Menü *Netzwerk*:

Configure	Active
IP-Adresse: 192.168.0.200	IP-Adresse: 10.10.10.10
Subnetzmaske: 255.255.255.0	Subnetzmaske: 255.255.255.0
Standard Gateway: 192.168.0.100	Standard Gateway: 0.0.0.0
DNS Server: 192.168.200.1	DNS Server:

Die linke Seite ist hierbei die Konfiguration, die sie eingeben, die rechte Seite zeigt die aktuell eingestellte aktive Konfiguration.

Folgende Einstellungen können Sie vornehmen:

MAC: 00-30-d6-13-87-20	→ Die MAC-Adresse des Systems
Hostname: cs141	→ Hostname
IPv4	
Local Address: 10.10.10.10	→ Lokale IP-Adresse
Subnet Mask: 255.255.255.0	→ Subnetzmaske
Default Gateway: 10.10.10.1	→ Gateway
DNS Server: 10.10.10.1	→ DNS-Server

Für die benötigten Einstellungen setzen Sie sich bitte mit dem verantwortlichen Netzwerkadministrator in Verbindung. Mit *Übernehmen* werden die Einstellungen gespeichert. Wenn Sie das Gerät zum ersten Mal in Betrieb nehmen, stehen hier hardwareseitig voreingestellte Werte.

Tipp:

Der Webbrowser wird Sie an dieser Stelle auf eine andere IP-Adresse umleiten wollen. Da der CS141 sich noch im Konfigurationsmodus befindet, werden Sie im Anschluss eine Fehlermeldung von Ihrem Webbrowser erhalten. Drücken Sie in diesem Fall STRG F5, um die Webanzeige zu aktualisieren.

Bei einer kompletten Neukonfiguration ist das Menü *Netzwerk* die einzige Einstellung, die Sie aktuell im Konfigurationsmodus durchführen müssen. Alle weiteren Einstellungen können Sie auch im regulären Betriebsmodus durchführen.

Besonderheit Erstkonfiguration im DHCP-Modus

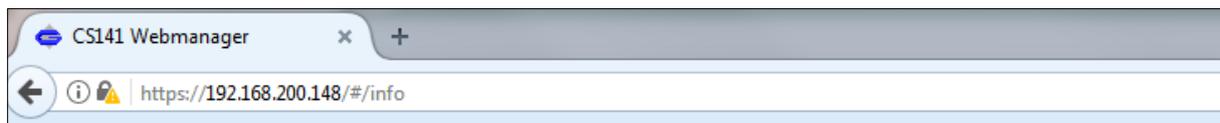
Wenn Sie den CS141 im DHCP-Modus starten, wird von einem DHCP-Server eine IP-Adresse zugewiesen. Diese können Sie mit dem kostenlosen Tool *Netfinder* anzeigen lassen. Wenn Sie mehrere Webmanager im Einsatz haben, ist das Gerät an Hand der MAC-Adresse und dem Adressaufkleber leicht zu identifizieren.

CS141L	1.61	Nicht nötig	Generex (12)	d0-39-72-3b-df-f8	192.168.200.142	
BACSKIT_B4	1.60	Nicht nötig	Generex (12)	00-30-d6-16-b3-4b	192.168.200.148	
CS141BL	1.61	Nicht nötig	ALTERVAC (92)	00-30-d6-12-6f-56	192.168.200.224	
BACSKIT_B4	1.61	Nicht nötig	Generex (12)	00-30-d6-12-60-42	192.168.200.225	
CS131	5.58	Verfügbar (5.62)	Generex (12)	00-03-05-0E-2F-49	192.168.200.227	FB Office



Die Funktion *Gerät aufrufen* öffnet einen Webbrowser mit der richtigen IP-Adresse. Sie können jetzt unter *Netzwerk* Ihre IP-Adresseinstellungen vornehmen und anschließend in den manuellen Modus wechseln:

Im DHCP-Modus werden diese Einstellungen komplett ignoriert und ausschließlich die vom Server zugewiesene Adresse verwendet:



Der Vorteil ist, dass Sie ohne viel Aufwand beliebig viele CS141 gleichzeitig ins Netzwerk bringen können, die sofort erreichbar sind. Der Nachteil liegt in der Tatsache, dass sich im DHCP-Modus die IP-Adressen dynamisch ändern können, wodurch übergeordnete oder angedockte Shutdown-Lösungen eventuell nicht mehr greifen können oder Fehler ausgeben.

WLAN – Die Wi-Fi Schnittstelle

Unabhängig zu den LAN-Einstellungen verfügen SITEMANAGER 7 und SITEMONITOR 7 über ein vorinstalliertes Wi-Fi -Modul, welches mit einem beliebigen WLAN verbunden werden kann:

Configured

IP Configuration:

Network Name:

Password:

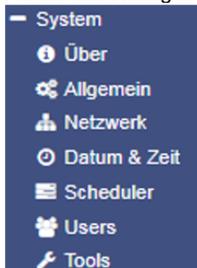
Security:

- ➔ Einschalten / Ausschalten des Wi-Fi – Moduls
- ➔ Definition der SSID
- ➔ WLAN-Passwort
- ➔ Verschlüsselungsart

Weitere Grundeinstellungen

Eingabe der Kontakt- und Standortdaten

Für diesen Konfigurationsschritt benötigen Sie das folgende Menü:



➔ **Standorteinstellungen und Kontaktdaten**

Standortdaten können von einer Software, die diese Option unterstützt, ausgelesen werden. Wenn Sie viele Standorte mit multiplen Installationen überwachen, können Sie über diese Funktion die Zuordnung von installierten Geräten erleichtern.

Standort	<input type="text" value="Allgemeine Anlage 3"/>	→ Geben Sie hier den Ort ein, wo das Gerät steht
System Kontakt	<input type="text" value="Mustermann"/>	→ Geben Sie einen zuständigen Namen an
Customer Signature	<input type="text"/>	
Check Firmware Update	<input checked="" type="checkbox"/>	→ Auf Wunsch wird automatisch auf Firmware geprüft

Mit Übernehmen werden die aktuellen Einstellungen übernommen und im Menü Über entsprechend angezeigt. Das Freeware Tool *Netfinder* wird Ihnen die Standortdaten mit angeben, was die Suche nach einem bestimmten Gerät erleichtert:

CS141L	1.61	Nicht nötig	Generex (12)	d0-39-72-3b-df-f8	192.168.200.142	Allgemeine Anlage 3	
BACSKIT_B4	1.60	Nicht nötig	Generex (12)	00-30-d6-16-b3-4b	192.168.200.204		
CS141BL	1.61	Nicht nötig	ALTERVAC (92)	00-30-d6-12-6f-56	192.168.200.224		
BACSKIT_B4	1.61	Nicht nötig	Generex (12)	00-30-d6-12-60-42	192.168.200.225		
CS141L	1.61	Nicht nötig	Generex (12)	00-30-d6-12-70-36	192.168.200.231		
CS141L	1.60	Nicht nötig	Generex (12)	00-30-d6-14-21-3c	192.168.200.232		

Angabe von Region und Maßeinheit der Temperatur

Sprache	<input type="text" value="Deutsch"/>	→ Auswahl der Menüsprache
Temperature:	<input checked="" type="radio"/> Celsius <input type="radio"/> Fahrenheit	→ Auswahl der Maßeinheit für Temperaturen

Wählen Sie unter *Sprache* ihre bevorzugte Systemsprache aus. Folgende Sprachen werden unterstützt:

Deutsch, Englisch, Chinesisch (Simple), Französisch, Spanisch, Polnisch, Portugiesisch

Wählen Sie unter Temperaturen die Maßeinheit aus, in der die Temperaturen angezeigt werden sollen.

Unterschied Fahrenheit / Celsius

Obwohl anfangs durch den Gefrierpunkt von Wasser (und später Schmelzpunkt des Eises) definiert, ist die Celsius-Skala offiziell abgeleitet von der Kelvin-Skala.

Null auf der Celsius-Skala (0 °C) entspricht 273,15 K, mit einer Temperaturdifferenz von 1 °C äquivalent zu einer Differenz von 1 K, so dass die Größe der Einheit in jeder Skala gleich ist. Dies bedeutet, dass 100 °C, die zuvor als Siedetemperatur von Wasser definiert wurden, nun 373,15 K entsprechen.

Die Celsius-Skala ist ein Intervall-System, nicht aber ein Verhältnis-System, was bedeutet, dass es einer relativen, jedoch nicht absoluten Skala folgt. Dies ist daran zu erkennen, da ein Temperaturintervall zwischen 20 °C und 30 °C gleich ist wie zwischen 30 °C und 40 °C, aber 40 °C nicht über die doppelte Luftwärmeenergie wie 20 °C verfügt.

Eine Temperaturdifferenz von 1 °C entspricht einer Temperaturdifferenz von 1,8 °F.

Da beide Skalen weltweit Anwendung finden, ist es vor der Konfiguration wichtig, vorher zu wissen, welche Skala zu verwenden ist.

Tipp:

Der CS141 berechnet die Werte beim Umstellen der Skala neu und passt die Einstellungen automatisch an – ein übergeordnetes System, welches auf Fahrenheit konfiguriert ist, wird jedoch von einem Webmanager, der auf Celsius eingestellt ist, zwangsläufig falsche Angaben bekommen.

Dieses kleine Problem kann große Auswirkungen haben, vor allem wenn man in einem internationalen Team arbeitet:

Zum Beispiel hat am 11.12.1998 der Mars Climate Orbiter gemäß Programmierung in die Umlaufbahn des Planeten eingeschwenkt, jedoch 170 Kilometer tiefer als geplant. Die Ursache war, dass zwei unterschiedliche Gruppen der NASA die Flugbahnberechnungen durchführten – eine in Inch und eine in Metern:

„The ‘root cause’ was the failed translation of English units into metric units in a segment of ground-based, navigation-related mission software ...“

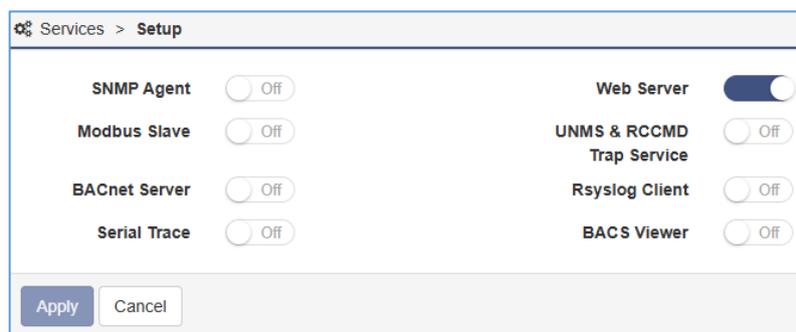
Dienste

Für diese Einstellung benötigen Sie folgendes Menü:



Hinweis: Die Dienste und ihre Einrichtung inklusive aller notwendigen Tabellen (z.B. für die Einrichtung von Modbus) werden ausführlich in der CS141 Benutzerdokumentation erörtert. Die CS141 Gesamtdokumentation finden Sie unter www.generex.de im Downloadbereich.

Standardmäßig sind bis auf der Webserver aus Sicherheitsgründen deaktiviert, und müssen bei Bedarf einzeln aktiviert werden.



Der SITEMANAGER 7 verwendet zur Kommunikation diverse, voneinander unabhängige Systemdienste. Das erlaubt ein Aktivieren und Deaktivieren der Funktionen, ohne dass die Geräte komplett neu gestartet werden müssen.

Tipp: Doktrin Wechsel mit der Firmware 2.14 – Cybersecurity Enhanced!

Nach Best Practice waren die Default-Einstellungen so gewählt, dass eine schnelle und unkomplizierte Einbindung in bestehende Systeme, die auf Standards setzen, möglich war. Mit Blick auf Cybersecurity wurde dieses nun geändert. Alle Dienste, die für die Ersteinrichtung nicht benötigt werden, sind künftig bei der Werkseinstellung standardmäßig auf „OFF“ – Administratoren müssen Funktionen wie SNMP oder Remote Syslog künftig manuell und bewusst aktivieren, bevor diese genutzt werden können.

Webserver

Der Webserver– Dienst ist die lokale Webschnittstelle des CS14. Dabei wird über Port 80 mittels eines Webbrowsers eine Verbindung aufgebaut, über die der CS141 konfiguriert werden kann.

In einigen Hochsicherheitsbereichen kann es notwendig sein, nach der Konfiguration diesen Zugriff auf die Weboberfläche permanent zu verbieten, ohne dass die konfigurierte Funktionalität eingeschränkt wird.



Da der Webzugriff vollständig unterbunden wird, kann diese Option nicht mehr rückgängig gemacht werden – hierzu ist ein Booten über das Rettungssystem mit Wiederherstellung des Auslieferungszustands notwendig. Eine Datensicherung (Backup) ist möglich, da dieses als letzter Schritt vor dem Deaktivieren der Webschnittstelle erfolgen muss.

Tipp:

Das Rettungssystem auf dem CS141 hat nicht nur die letzte Firmware gespeichert, sondern auch die letzte Konfiguration vor Ihrem Update. Sollten Sie versehentlich oder bewusst diese Funktion deaktiviert haben und später aktivieren wollen, empfiehlt es sich, vor den aktivieren ein Firmware-Update durchzuführen.

Auf diese Weise wird gewährleistet, auch später noch auf das System zugreifen zu können, ohne die allgemeine Konfiguration zu verlieren.

SNMP

Das Simple Network Management Protocol SNMP oder auch einfaches Netzwerkverwaltungsprotokoll, ist ein Netzwerkprotokoll, das von der IETF entwickelt wurde, um Netzwerkelemente von einer zentralen Station aus überwachen und steuern zu können.

Das Protokoll regelt dabei die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. SNMP beschreibt hierbei sowohl den Aufbau der Datenpakete, die gesendet werden können, als auch den Kommunikationsablauf.

Es wurde dabei so ausgelegt, dass jedes netzwerkfähige Gerät mit in die Überwachung aufgenommen werden kann. Zu den Aufgaben des Netzwerkmanagements, die mit SNMP möglich sind, zählen:

- Überwachung von Netzwerkkomponenten,
- Fernsteuerung und Fernkonfiguration von Netzwerkkomponenten,
- Fehlererkennung und Fehlerbenachrichtigung.

Durch seine Einfachheit, Modularität und Vielseitigkeit hat sich SNMP zum Standard entwickelt, der sowohl von den meisten Managementprogrammen als auch von Endgeräten unterstützt wird.

Wenn Sie in Ihrem Netzwerk SNMP verwenden möchten, lassen Sie das Häkchen bei dieser Funktion aktiv.

Modbus

Feldbusse sind Bussysteme, über die einzelnen Geräte wie Sensoren oder Aktuatoren miteinander verbunden werden können und ermöglichen eine geordnete Kommunikation zu einem entsprechenden vollautomatisierten Managementsystem.

Wenn mehrere Kommunikationspartner ihre Informationen über dieselbe Leitung senden, muss für die Kommunikation feste Regeln aufgestellt werden

- wer (Kennung)
- was (Maß, Befehl) und
- wann (Initiative)

senden darf. Hierzu wird auf standardisierte Protokolle zurückgegriffen.

Modbus ist hierbei nicht neu:

Das Modbus-Protokoll wurde 1979 von Gould-Modicon zur Kommunikation mit seinen speicherprogrammierbaren Steuerungen eingeführt und ist aufgrund seines offenen Protokollstandards zu einem inoffiziellen Standard für die industrielle Nutzung geworden.

Seit 1999 sind Feldbusse weltweit in der Norm IEC 61158 (Digitale Datenkommunikation für Mess- und Regeltechnik - Feldbus für den Einsatz in industriellen Steuerungssystemen) standardisiert. Die zweite Generation der Feldbustechnologie basiert auf Echtzeit-Ethernet.

Nähere Informationen über die Möglichkeiten erfahren Sie im Kapitel „Modbus“ in diesem Handbuch, die notwendigen Modbus-Listen finden Sie im Anhang.

BACnet Server

BACnet (Building Automation and Control Networks) ist ein Netzwerkprotokoll, das von der ASHRAE, ANSI und ISO 16484-5 standardisiert wurde für die Gebäudeautomations. Näheres über die Möglichkeiten und Konfiguration erfahren Sie im Kapitel „BACnet“ in diesem Handbuch.

Serial Trace

Der CS141 bietet unter Tools einen Systemtracer an, mit dem Sie die Kommunikation zwischen dem CS141 und der USV beobachten und mitschneiden können. Diese Kommunikation findet über den Port 4000 statt. Mit diesem Schieberegler können Sie gezielt den Port 4000 öffnen (an) oder schließen (aus)

UNMS & RCCMD Trap Service

Der UNMS & RCCMD Trap Service wurde speziell für die Kommunikation mit der universellen Netzwerkmanagementsoftware von GENEREX entwickelt. Der leistungsfähige Nachfolger UNMS 2 kommuniziert mit dem CS141 über UPSTCP an Port 5769. Der USV-Serverdienst aktiviert oder deaktiviert die Verfügbarkeit über diesen Port.

RSyslog Client

Remote Syslog ist eine beliebte Methode, um lokal gespeicherte Logfiles unabhängig vom Gerät oder Hersteller in einem normierten Format an einen zentralen Netzwerkknoten, einem sog. Syslog Receiver, zu senden.

BACS Viewer

Wenn Sie ein BACS-System betreiben, können Sie mit der BACS Viewer Software die Daten der betreuten Batterien herunterladen. Diese Funktion öffnet den dafür notwendigen SFTP-Port und schaltet den Agenten frei, über den sich der BACS-Viewer mit dem CS141 / BACS WEBMANAGER verbinden kann.

Datum und Uhrzeit

Für diesen Konfigurationsschritt benötigen Sie das folgende Menü:



Für einige systemkritische Einstellungen wie z.B. Ereignisprotokolle oder wiederkehrende Aufgaben ist eine exakte Zeitangabe notwendig. Der CS141 verfügt aus diesem Grund neben einer eigenen Systemuhr auch über die Möglichkeit, externe NTP-Server abzufragen.

Darüber hinaus kann – sofern von der USV unterstützt – im Notfall die USV-interne Uhr gestellt und wieder ausgelesen werden für den Fall, dass keine externe Möglichkeit zur Verfügung steht, die Zeit selbst zu kontrollieren.

Automatische Korrektur der Uhr

Die aktuelle Systemzeit

- Zeitserverns → Eingabe des ersten
- Zeitserverns → Eingabe des zweiten
- Zeitserverns → Eingabe des dritten
- Zeitserverns → Zeitzone auswählen
- synchronisieren → System mit Zeitserver
- Eingabe übernehmen

Wenn die Netzwerkeinstellungen richtig gesetzt sind und eine Verbindung zum Internet besteht, können Sie die voreingestellten Server verwenden. Über die Test-Funktion können Sie die Verfügbarkeit testen. Sollten Sie in Ihrem Netzwerk einen eigenen lokalen Zeitserver verwenden, können Sie an dieser Stelle auch die IP-Adresse Ihres internen Zeitservers angeben.

Tipp:

Ein Zeitserver gibt eine vorformatierte Uhrzeit aus, welche u.a. auch die verwendete Zeitzone enthält. Der CS141 berechnet aus der Einstellung der Zeitzone die reale Systemzeit selber. Sollten Sie einen eigenen Zeitserver betreiben, muss diese Zeitzone entsprechend angeglichen werden.

Durch Übernehmen werden die Einstellungen übernommen und der Zeitserverdienst neu gestartet und eine erste Zeitsynchronisation durchgeführt.

Erweiterte Nutzerverwaltung

Für diesen Konfigurationsschritt benötigen Sie das folgende Menü:



Nutzerrollen

Nutzerrollen haben großen Einfluss auf die Verfügbarkeit der Menüs. Nur Benutzer mit der Nutzerrolle „Administrator“ haben Vollzugriff auf alle Funktionen. Andere Nutzerrollen bekommen dynamisch basierend auf ihrer Funktion entsprechende Menüs eingeblendet.

- Lock the Engineer Role
- Lock the Customer Role
- Lock the Guest Role

Um die jeweilige Nutzerrolle verwenden zu können, entfernen Sie den jeweiligen Haken, und klicken Sie auf Apply. Die Nutzerrolle wird hierdurch verfügbar und der entsprechende Nutzer kann verwendet werden. Ausnahmen bilden hier die Nutzerrolle „Administrator“ und den „Super User“ admin.

Verfügbare Nutzer

Als Voreinstellung sind 4 Nutzer vorgegeben.

Der Administrator

User: *admin*
Default-Passwort: *cs141-snmp*

Der Administrator hat bedingt durch seine Funktion den vollen Umfang der Konfigurationsmöglichkeiten zur Verfügung. Der Administrator verwaltet Netzwerk- und Maleinstellungen und ist der einzige Nutzer mit der Berechtigung, die Landschaft der angeschlossenen Geräte zu ändern. Dieser Nutzer kann weder gelöscht noch deaktiviert werden. Der Nutzer „admin“ hat zudem Vollzugriff auf das Usermanagement, und kann jeden selbst angelegte Nutzer mit der Nutzerrolle „Administrator“ verwalten. Der Nutzer „admin“ ist der einzige Benutzer, der im Konfigurationsmodus (Schiebeschalter mitig) verwendet werden kann.

Der Techniker

User: *engineer*
Default Passwort: *engineer*

Der Techniker hat ein auf sein Aufgabengebiet eingeschränktes Nutzerkonto. Er hat Zugriff auf die Funktionen, die das technische Handeln betreffen. Er hat kann die verfügbaren Geräte anpassen, konfigurieren und die entsprechend notwendigen Anpassungen vornehmen. Dieser Nutzer ist frei editier- und löschar, und die Nutzerrolle deaktiviert.

Der Kunde

User: *customer*
Default Passwort: *customer*

Der Kunde ist eine weitere Abstufung zum Techniker. Er hat Zugriff auf System- und Statusmonitore und deren Funktionen, und kann zudem alle Logdateien herunterladen. Dieser Nutzer ist frei editier- und löschar, und die Nutzerrolle deaktiviert.

Gastzugang

User: *guest*
Default Passwort: *guest*

Der Gastzugang ermöglicht das reine Betrachten der Systemmonitore, ohne weitere Funktionen auslösen zu dürfen. Dieser Nutzer ist für Unterfunktionen essenziell und kann deaktiviert, aber nicht umbenannt oder gelöscht werden.

Anonymous Guest

Der Anonymous Guest ist eine Zusatzfunktion des regulären Gastzugangs, und direkt an diesen gebunden:

Mit dem Anonymous Guest ist es möglich, auf Basis einer Session die Statusscreens ohne wiederholte Eingabe eines Passworts abzurufen bzw. einzusehen und ist nur verfügbar, wenn der Benutzer „guest“ nicht gesperrt ist.

Zu beachten ist hierbei, dass der Anonymous Guest kein eigenes Passwort verwendet, sondern das Benutzerpasswort des regulären Gastzugangs übernimmt.

Weitere Administratoren anlegen

Jeder Benutzer mit der Nutzerrolle „Administrator“ kann unter „local Users“ in Freitext Benutzer anlegen und eine entsprechende Nutzerrolle zuweisen. Das Menü wird entsprechend der Nutzerrolle dynamisch die verfügbaren Menüs einblenden. Die einzige Ausnahme ist der Zugriff auf den Benutzer „admin“.

Nutzermanagement unter RADIUS

Vorbedingung ist, dass ein RADIUS-Server erfolgreich eingerichtet und getestet wurde.

Die Einstellung überschreibt teilweise die lokale Nutzerdatenbank:

RADIUS Servers	
	IP Address
<input checked="" type="checkbox"/>	Primary 127.0.0.1
<input checked="" type="checkbox"/>	Secondary 127.0.0.1

Local Authentication Only
 RADIUS, then Local Authentication
 RADIUS Only

1. Benutzer / Freigabeebene

Der RADIUS-Nutzer und seine Freigaben werden verwendet, um das jeweilige Menü einzublenden.

Ausnahmen:

- Die Nutzerrolle ist lokal gesperrt.
- Das Gerät befindet sich im Konfigurationsmodus, in dem Fall ist der Zugang auf den SuperUser „admin“ beschränkt.

Folgende Möglichkeiten bietet das RADIUS-Setup:

- Local only: der RADIUS-Server wird ignoriert und es gelten ausschließlich die Vorgaben der lokalen Nutzerdatenbank
- RADIUS, then Local: Es wird zuerst versucht, den RADIUS – Server zu erreichen. Sollte dieser nicht verfügbar sein, wird mit der lokalen Nutzerdatenbank abgeglichen. Wichtig: Sollte der RADIUS-Server erreichbar sein, aber nicht antworten, ist der Login nicht möglich.
- RADIUS only: Restriktiver Betriebsmodus – Es gelten exklusiv die Vorgaben des RADIUS-Servers. Sollte dieser nicht erreichbar sein, ist ein Zugang nicht möglich.

Tipp:

Eine vollständige und detaillierte Konfigurationsanleitung des RADIUS Servers finden Sie in der offiziellen CS141 Benutzerdokumentation im Downloadbereich unter www.generex.de

Systemübersicht: Die About-Seite

Für die Systemübersicht klicken Sie auf den folgenden Menüpunkt:



Wenn Sie alle Grundeinstellungen ausgeführt haben, können Sie unter *Über* die allgemeinen Systeminformationen aufrufen und in einer Gesamtübersicht anzeigen lassen:

Das System und die Firmware

Die folgende Liste enthält die wichtigsten Informationen über Ihren SITEMANAGER 7

Name CS141LM	→ Der verwendete Adapter
Version 2.23.12.250220	→ Die aktuelle Firmware
License Pro Edition	→ USV-Lizenz Key
Manufacturer Generex	→ Der OEM-Hersteller
UPS Model No UPS model defined	→ Das verwendete USV-Modell
Location	→ Standort des Geräts
System Contact	→ Kontaktdaten des Systembetreuers
Time 2025-02-20 16:18:10 (UTC+01:00, DST) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	→ Systemzeit und Zeitzone
Uptime 0 days, 1 hours, 11 minutes, 33 seconds	→ Betriebszeit seit letztem Start
Serial No. 1016909336	→ Seriennummer des Geräts
Features hw161	→ Die Hardware-Revision des Geräts
MAC Address 00-30-d6-38-4d-a4	→ Die MAC-Adresse des Geräts
Hostname cs141	→ Hostname
Domain localdomain	→ Domain-Einstellungen
Timeserver Address 1 0.pool.ntp.org	→ Definierte Zeitserver
Timeserver Address 2 1.pool.ntp.org	→ IP-Modus (DHCP/statisch)
Network Configuration Mode Static IP address	→ Aktuelle IP-Adresse
IPv4 Address 10.10.10.10	→ Subnetzmaske
IPv4 Subnet Mask 255.255.255.0	→ Gateway
IPv4 Gateway 10.10.10.1	→ DNS-Einstellungen
IPv4 DNS Server 1 10.10.10.1	

Sollten Sie technischen Support benötigen, benötigt unser technischer Support mindestens folgende Angaben von Ihnen:

- Firmwareversion
- Das verwendete USV-Modell
- Betriebszeit seit letztem Start
- Seriennummer des Geräts
- Die unter Features ausgewiesene Hardware-Revision

Reboot und Kaltstart

Unter Umständen kann es notwendig sein, dass der SITEMANAGER 7 neu gestartet werden muss, wobei je nach Einsatzszenario 2 unterschiedliche Möglichkeiten existieren:

Kaltstart

Unterbrechen Sie kurz die Stromzufuhr, indem Sie den Stromstecker ziehen oder die Karte aus dem Slot entfernen. Das Gerät wird anschließend mit der neuen hardwareseitigen Einstellung in den entsprechenden Betriebszustand booten.

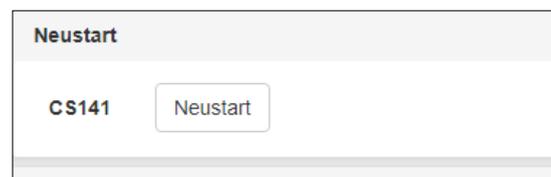
Warmstart - Reboot Der Neustart-Button

Für diesen Vorgang benötigen Sie das folgende Menü:



Geben Sie bei der Passwortabfrage den Standardnutzer *admin* und das Passwort für Ihren Administratorzugang ein. Wenn Sie kein Passwort vergeben haben, gilt das Standardpasswort *cs141-snm*

Im Anschluss können Sie mit der Funktion *Neustart* den CS141 mit einem softwareseitig gesteuerten Neustart in den Betriebsmodus booten. Für Welche Bootmethode Sie sich auch entscheiden, in beiden Fällen wird nicht die USV neu gestartet, sondern es betrifft lediglich den CS141 – Ihre Stromversorgung ist zu jedem Zeitpunkt sichergestellt.



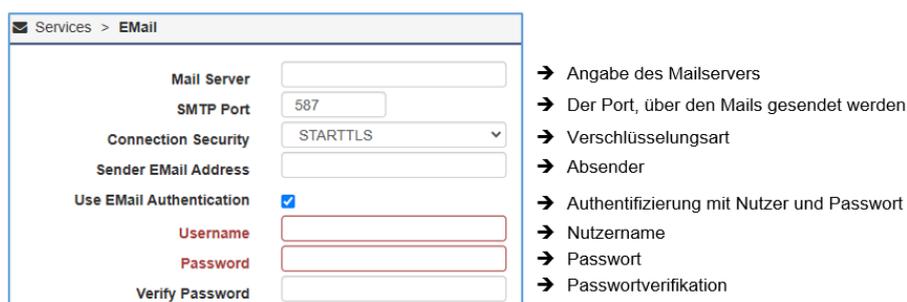
Konfiguration der Systembenachrichtigungen

E-Mail - Einstellungen

Für diesen Konfigurationsschritt benötigen Sie das folgende Menü:



Der SITEMANAGER 7 verfügt über unterschiedliche Möglichkeiten, um mit der Umwelt, angeschlossenen Geräten und Netzwerken zu interagieren. Eine der Grundfunktionen ist die automatische Benachrichtigung über E-Mail und E-Mail-Traps. Für diese Funktionalität muss jedoch ein gültiges E-Mail-Konto hinterlegt werden:



Mailservers

Tragen Sie hier den Mailserver ein, der verwendet werden soll. Dabei ist sowohl die Eingabe eines Mailservers als auch die Eingabe der entsprechenden IP-Adresse möglich. Es kann sowohl ein eigener interner Mailserver als auch ein externer Serviceanbieter via Internetanbindung verwendet werden.

Tipp:

Das SITEMANAGER 7 eine Verbindung zum Internet hat, um auf externe Konten großer Mailanbieter zuzugreifen, bedeutet nicht, dass der externe Anbieter Service-Mails als solche zulässt oder zu einem späteren Zeitpunkt ohne Angabe von Gründen derartige E-Mails unterbindet. Wenden Sie sich im Zweifelsfall an Ihren Serviceanbieter.

SMTP-Port

Definiert den Port, über den ein Mailclient mit dem Mailserver kommuniziert. Grundsätzlich sind die Ports genormt, es besteht jedoch immer die Möglichkeit, eigene Ports für die Kommunikation zu verwenden. Die notwendigen Zugangsdaten sind daher von dem lokalen Administrator in Erfahrung zu bringen.

Connection Security

Wählen Sie die Verschlüsselungsart aus, mit dem der CS141 die Emails an den Mailserver übertragen soll:

None	Keine Verschlüsselung
STARTTLS	If available
TLS /SSL	Force Encryption

Sender Email Address

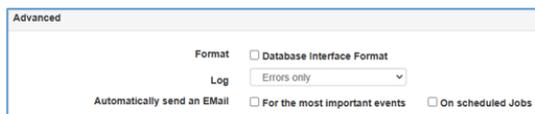
Geben Sie die Mailadresse ein, über die eine Mail versendet werden soll. Dieser wird dann im „Von“ – Feld des jeweiligen Empfängers angezeigt.

Email Authentifizierung verwenden, Nutzer und Passwort

Je nach Konfiguration verwenden Emailserver als Nutzernamen entweder die Mailadresse oder eine eigene Benutzerkennung mit Passwort, um Mails zum Versenden entgegenzunehmen.

Für die gültigen Zugangsdaten setzen Sie sich bitte mit dem entsprechenden Netzwerkbetreuer vor Ort in Verbindung.

Advanced Options



- Datenbank konformes Mailformat
- Protokollierung des E-Mail-Versands
- Automatisches Senden von E-Mails

Format

Sollten E-Mails automatisch in einer Datenbank erfasst werden, kann das Format der E-Mail entsprechend vorgeformatiert werden.

Log

Definiert die Bedingungen, unter denen das Senden einer E-Mail im Ereignisprotokoll erfasst wird.

Folgende Möglichkeiten stehen zur Auswahl:

- Errors only** Mails, die auf Störungen hinweisen, werden im Ereignisprotokoll erfasst
- Always** Jede Mail wird als „gesendet“ im Ereignisprotokoll erfasst
- Never** Die Mails werden gesendet, jedoch nicht im Ereignisprotokoll erfasst.

Automatically send an EMail

Angelehnt an die im Eventmanagement eingetragenen RCCMD-Traps. Wenn ausgewählt, sendet der Der SITEMANAGER 7 unabhängig von der sonstigen Konfiguration eine E-Mail

<input checked="" type="checkbox"/> For the most important events	Ein vordefiniertes Set an Systemereignissen – Die genaue Liste richtet sich nach Funktionsumfang, Ausbaustufe und angeschlossener USV.
<input checked="" type="checkbox"/> On scheduled Jobs	Für alle über den Scheduler geplanten Aufgaben.

Tipp:

Je nach Konfiguration kann diese globale Einstellung für viele Systemereignisse eine zweite E-Mail absetzen. Wenn Sie gezielt im Event-Management eigene E-Mails definieren, kann es sinnvoll sein, diese Funktion zu deaktivieren.

Gleiches gilt für die Funktion *Log*:

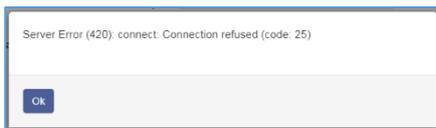
Zu viele Einträge im Ereignisprotokoll sorgen schnell für unübersichtliche Datenbestände, sobald man spezielle Einträge innerhalb eines Zeitfensters sucht.

Mit Übernehmen werden die Einstellungen in die Konfiguration übernommen und der Dienst zum Versenden von Mails neu gestartet.

Testen der Maileinstellungen

Beachten Sie bitte, dass diese Funktion erst zur Verfügung steht, nachdem Sie auf Übernehmen geklickt und damit die Daten in die Konfiguration des SITEMANAGER 7 übernommen wurden.

Über diese Funktion können Sie an eine Mailadresse Ihrer Wahl eine entsprechende Nachricht schicken, um die Funktion zu überprüfen.

Connection refused - Die häufigste Fehlermeldung:

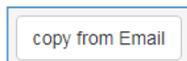
Dieser Fehler bedeutet, dass keine Verbindung zum Mailserver aufgebaut werden konnte.

Die Gründe hierfür können vielfältig sein, und reichen vom falschen oder nicht freigeschalteten Port bis hin zu der Tatsache, dass ein externer Mailanbieter diese Art von Mailübertragung unterbindet.

Email-Traps

Mail-Traps sind von industriellen Systemen automatisch generierte Status- und Informationsmeldungen, welche von einem entsprechenden Empfänger abgeholt und ausgewertet werden können. Der Unterschied zu einer E-Mail ist, dass Sie weder einen Text eingeben noch einen abweichenden Empfänger definieren können.

Näheres erfahren Sie im Kapitel **Konfiguration der USV**



Wenn es dasselbe Konto verwenden möchten, dass Sie unter *E-Mail* eingerichtet haben können Sie mit *copy from Email* die Daten direkt übernehmen:

Die Funktion *copy from Email* kopiert die bereits eingegebenen Daten. Sie müssen lediglich noch einmal unter *Verify Password* die Passworteingabe bestätigen. Wenn Sie ein abweichendes E-Mail-Konto oder einen anderen Mailserver geben Sie die entsprechenden Zugangsdaten ein.

Modbus

Für diesen Konfigurationsschritt benötigen Sie folgendes Menü:



Feldbusse sind Bussysteme, die in einer Anlage Feldgeräte wie Messfühler (Sensoren) und Stellglieder (Aktoren) zur Kommunikation mit einem Automatisierungsgerät verbindet. Wenn mehrere Kommunikationsteilnehmer ihre Informationen über dieselbe Leitung senden, dann muss festgelegt sein, wer (Kennung) was (Messwert, Befehl) wann (Initiative) übermitteln kann und darf. Um diese Kommunikation sicher zu stellen, gibt es genormte Protokolle.

Das Modbus-Protokoll wurde im Zuge dessen 1979 von Gould-Modicon für die Kommunikation mit seinen speicherprogrammierbaren Steuerungen ins Leben gerufen und hat sich in der Industrie inzwischen zu einem inoffiziellen Standard entwickelt, da es sich um ein offenes Protokoll handelt.

Seit 1999 werden Feldbusse in der Norm IEC 61158 (Digital data communication for measurement and control - Fieldbus for use in industrial control systems) weltweit standardisiert. Die zweite Generation der Feldbustechnik basiert auf Echtzeit-Ethernet.

Tipp:

Weitere Informationen entnehmen Sie bitte dem Handbuch für Modbus, welches Sie im Downloadbereich unseres Webauftritts unter www.generex.de beziehen können.

[Modbus in Geräten](#)

Modbus ist ein Protokoll für die serielle Kommunikation. Daten werden in Form von 16-Bit-Registern (Integer) oder Datenbyte-Statusinformationen übertragen. Dabei hat MODBUS viele Vorzüge:

- Die grundlegende Struktur von MODBUS hat sich aus Kompatibilitätsgründen nie wirklich geändert. Die Menge an einheitlichen Geräten ermöglicht eine stabile Basis für Integration und Wartung und Konfiguration.
- Dieses offene Protokoll hat sich als Quasi-Standard bei vielen Industriemaschinen weltweit etabliert. Sobald ein Gerät Modbus unterstützt, kann es in der Regel in einen bestehenden Verbund integriert werden.

[Modbus als Single-Master-Protokoll](#)

Der Master steuert die gesamte Übertragung und überwacht mögliche auftretende Zeitüberschreitungen. Die angeschlossenen Geräte dürfen nur dann Telegramme senden, wenn der Master dies anfordert.

Zur Fernsteuerung und Überwachung von Geräten kann die Modbus-Schnittstelle in jedem CS141 Messwerte, Ereignisse, Status und andere Informationen innerhalb des Master-Slave - Protokolls auslesen.

Tipp:

Wenn Sie bestimmte Messwerte vermissen, ist das nicht unbedingt Fehler – Gerade dann, wenn es um Sonderfunktionen handelt, kann es sein, dass die USV dieses dem CS141 über SNMP mitteilt, denen jedoch herstellerbedingt keine Modbus-Adresse hinterlegt wurde. In dem Fall würde der CS141 im Webinterface auf eine Funktion wie z.B. Batterie niedrig reagieren und gemäß Konfiguration Nachrichten, RCCMD-Kommandos, etc. versenden, jedoch ist dieser Status nicht über Modbus abfragbar.

[Modbus über RS232 und Modbus over IP](#)

Wie bereits erwähnt, können beherrschen alle Geräte der CS141 – Familie MODBUS - der Unterschied liegt im Detail. Während der CS141 Modbus Adapter mit der RS485 – Schnittstelle in einen Bus integriert werden kann, verwenden SITEMANAGER und SITEMONITOR mit Modbus über RS232 und Modbus over IP eine Point-to-Point – Verbindung. Der RS232-Modbus-Anschluss wird üblicherweise verwendet, wenn man Modbus-Daten der USV in ein anderes System oder eine spezielle Überwachungssoftware überführen möchte.

Dabei halten sich beide Geräte hierbei an den RFC1628 Standard. Bei Bedarf kann die MIB unter www.generex.de im Downloadbereich heruntergeladen werden.

[Modbus Funktionscodes](#)

Die Geräte der CS141 Produktfamilie unterstützt folgende Funktionscodes:

01H	-	Read Coils
02H	-	Read Discrete Inputs
03H	-	Read Holding Registers
04H	-	Read Input Registers
05H	-	Write Single Coil

Bitte beachten Sie, dass die tatsächlich verfügbaren Funktionscodes von der jeweils angeschlossenen USV abhängen, da die USV-Kommandos dieser Art unterstützen muss. In der Regel stehen bei Standard USV Anlagen die Funktionen 03H und 04H zur Verfügung, wobei der CS141 keinen Unterschied zwischen diesen beiden Funktionen macht. Da der CS141 Abfragegeschwindigkeiten von bis zu 38400 Baud unterstützt, lässt sich der CS141 flexibel in ein bestehendes System integrieren.

[Modbus Fehlercodes](#)

Mit Ausnahme von Broadcast Nachrichten, wobei das Master Gerät eine Anfrage zu dem Slave Gerät sendet, wird von dem Master eine eindeutige und gültige Antwort vom Slave erwartet. Sollte die Antwort nicht den Vorgaben entsprechen, wird das Packet mit einem entsprechenden Fehler verworfen.

Folge möglichen Ereignisse können bei der Anfrage durch ein Mastergerät eintreten:

1. Der Slave antwortet entsprechend mit einem passenden Datenpaket.

Der Master wird entsprechend reagieren.

2. Die Slave Einheit bekommt die Anfrage durch den Master nicht

Dieses Ereignis tritt zum Beispiel bei einem Kommunikationsfehler ein. Da als Konsequenz aus Sicht des Masters die Anfrage nicht beantwortet wurde, reagiert dieser mit einem entsprechenden timeout.

3. Master oder Slave senden ungültige die Nachrichten

Ein solches Phänomen kann ein treten, wenn zum Beispiel die Abschlusswiderstände nicht gesetzt wurden. Es werden zwar Daten gesendet, jedoch bestehen innerhalb des Datenpackets eindeutig Fehler bei der Parität, dem LRC oder CRC. Da ungültige Pakete verworfen werden, wird der Slave üblicherweise bei so einer Anfrage nicht antworten. Der Master reagiert bei einer fehlerhaften Antwort generell mit einer entsprechenden timeout Meldung.

4. Der Slave erhält eine gültige Anfrage, die nicht beantwortet werden kann

Wenn die Slave-Einheit eine Anfrage ohne einen Kommunikatonsfehler erhält, jedoch ein Auslesen aufgrund z.B. eines nicht-existenten Register nicht möglich ist, antwortet die Slave-Einheit mit einer spezifischen Ausnahmemeldung, die Master-Einheit über den Grund de Fehlers informiert

Folgende Fehlercodes sind beim CS141 möglich:

- 02H Illegal Data Address

Die Datenadresse, welche mit der gültigen Anfrage erhalten wurde, ist keine zulässige Adresse, die der Slave bedienen kann

- 03H Illegal Data Value

Ein Wert, welcher in der Anfrage enthalten war, ist kein zulässiger Wert für den Slave.

- 06H Slave device busy

Der Slave hat eine gültige Anfrage erhalten, ist jedoch aktuell mit einem zeitintensiven oder zeitkritischen Prozess beschäftigt, wodurch er den Master gegenwertig nicht bedienen kann. Der Master wird in dem Fall nicht mit einem timeout reagieren, sondern die Anfrage zu einem späteren Zeitpunkt wiederholen.

Konfiguration von Modbus

Da Modbus auf Standards setzt, ist die grundsätzliche Konfiguration relativ einfach. Öffnen Sie hierzu unter Dienste den Reiter Modbus, um das Menü für die entsprechenden Einstellungen zu öffnen:

TCP Port	502
Max Connections	10
Slave Address	1
COM2 (RS232 / RS485)	
Baud Rate	38400
Parity	n
Stop Bit	1
Übernehmen Abbrechen	

- Port 502: Standard Modbus Adresse
- Maximale gleichzeitige Gerätezugriffe
- Modbus-ID des Geräts

- Übertragungsrate
- Paritäts-Bit
- Stop-Bit

- Speichern / Abbrechen

Enable Modbus Slave

Diese Funktion aktiviert die Modbusabfrage. direkt aus diesem Menü heraus. Bitte beachten Sie, dass andere, übergeordnete Menüs diese Funktion ebenfalls enthalten können – Sollten Sie dort Modbus deaktivieren, wird dieser Haken automatisch mit aus dem System entfernt.

TCP Port 502

Der TCP Port 502 ist im Rahmen des Modbus-Standards eine generelle Einstellung, die nicht geändert oder angepasst werden kann. Der CS141 beantwortet generell alle Modbusanfragen auf exakt diesem Port.

Slave Address

Der Modbus Slave ist die ID, unter der sich ein Gerät angesprochen fühlt und im Rahmen dessen auch tatsächlich antworten wird. Diese ID darf frei vergeben werden, jedoch im Netzwerk lediglich nur einmal vorhanden sein.

Tipp:

Wenn Sie eine Modbus Slave Address doppelt vergeben, führt dies nicht zu einem sogenannten Netzwerkkurzschluss – in dem Fall würden beide angesprochenen Geräte antworten, wodurch der Modbus-Master entsprechend irreführende Daten anzeigen wird.

Überprüfen Sie in diesem Fall die Eindeutigkeit der Slave Address und vergeben Sie ggfs. eine entsprechend freie Adresse.

Baud Rate

Die Baud Rate definiert die Übertragungsrate – die Geschwindigkeit, mit der Modbusabfragen entgegengenommen und beantwortet werden können. Beachten Sie in diesem Zusammenhang, dass die Abfragegeschwindigkeit durch den Master identisch mit der Einstellung im Slave sein muss, da ansonsten eine Kommunikation nicht zu Stande kommen kann.

Parity

Bei der Übermittlung von Daten in Form eines Bitstroms bildet das Paritätsbits eine Sicherheitsinstanz, mit der eine Fehlererkennung durchgeführt werden kann. Der Wert des Paritätsbits wird hierbei von dem Sender berechnet und dem Empfänger entsprechend mitgeteilt. Dieser kann dann mit demselben mathematischen Algorithmus überprüfen, ob die Daten beschädigt sind.

Die Berechnung der Parität kann für dabei auf gerade oder ungerade ausgelegt werden.

Sender und Empfänger müssen sich daher vorher einigen, ob sie eine gerade oder ungerade Paritätsberechnung durchführen.

Beispiel: Gerade Parität

Bei Einigung auf die Berechnung einer geraden Parität wird die Anzahl aller 1-Bits in den abzusichernden Daten gezählt. Die Aufgabe des Paritätsbits ist es, bei Bedarf das Ergebnis auf eine ungerade Zahl zu erweitern.

Wenn die Anzahl der zu überprüfenden Bits demnach gerade ist, muss das Paritätsbit als 0 übertragen werden, da ansonsten der Gesamtwert nicht stimmt.

Der CS141 bieten in diesem Zusammenhang folgende Optionen an:

n	Keine Paritätskontrolle
o	Ungerade Paritätskontrolle
e	Gerade Paritätskontrolle

Standardmäßig wird der CS141 mit dem Wert n für keine Paritätskontrolle ausgeliefert.

Stop Bit

Das Stoppbit definiert das Ende eines Datenworts innerhalb eines Datenstroms und findet in der asynchronen Datenübertragung Verwendung:

Üblicherweise wird vor dem Beginn eines Datenwortes ein entsprechendes Start-Bit gesendet, damit das empfangene Gerät den Beginn in der Zeichenfolge erkennen kann. Es handelt sich im Prinzip auch um ein High-Signal, jedoch ist der Pegel anders als bei dem nachfolgenden Datenwort.

Am Ende erfolgen je nach Konfiguration ein bis zwei Stoppbits, die das ausdrückliche Ende des Datenworts festlegen. Als Konsequenz kann zwischen Stoppbits und dem nächsten Start Bit kein gültiges Datenwort vorhanden sein und dem entsprechend verworfen werden.

Wenn durch Probleme innerhalb der Datenübertragung Daten verloren gehen oder unvollständig sind, kann über diese vordefinierte Kette zwischen Start und Stopp unterschieden werden, wodurch eine erneute Synchronisation möglich wird.

Tipp:

Wenn mehrere Modbusgeräte auf derselben ID liegen, senden bei einer entsprechenden Anfrage genau diese Geräte ihren Datenstrom entsprechend hinaus. Dabei überschneiden sich unter anderem die Start- und Stoppbits innerhalb des Verbunds, so dass es zu Problemen bei der Zuordnung von gültigen und ungültigen Datenpaketen kommt.

Mit der Funktion *Stop Bit* definieren Sie, ob der SITEMANAGER oder SITEMONITOR einen oder zwei entsprechende Stop Bits senden soll.

Übernehmen / Abbrechen

Mit dieser Funktion werden die eingegebenen Daten gespeichert und die entsprechenden Dienste bei Bedarf neu gestartet. Ein kompletter Reboot des CS411 ist nicht notwendig.

Übernehmen - Speichert die eingegebenen Daten und startet die Dienste neu

Abbrechen - Verwirft die eingegebenen Daten und bricht den Konfigurationsdialog ab, ohne eine Änderung durchzuführen.

Beachten Sie bitte, dass einige Clients wie zum Beispiel MODBUS Poll „MODBUS Adressen“ wie der CS1451 einem gültigen Bereich von 0-65535 verwenden. Sollten Sie einen anderen Client verwenden, dessen „MODBUS Register“ mit einem gültigen Bereich von 1-65536 funktioniert, ist es erforderlich, eine 1 zur Adresse hinzuzuaddieren

Weiterführende Dokumente und Modbus-Listen

Weiterführende Systemdokumentationen sowie alle verfügbaren Modbus-Listen entnehmen Sie der offiziellen CS141 Anwenderdokumentation im Downloadbereich unter www.generex.de

SNMP Agent

Für diesen Konfigurationsschritt benötigen Sie folgendes Menü:



Das Simple Network Management Protocol ist ein Netzwerkprotokoll, das von der IETF entwickelt wurde, um Netzwerkelemente von einer zentralen Station aus überwachen und steuern zu können. Das Protokoll regelt dabei die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. SNMP beschreibt den Aufbau der Datenpakete, die gesendet werden können, und den Kommunikationsablauf.

Der SITEMANAGER 7 ist vollständig in ein Netzwerk mit SNMP-Überwachung integrierbar. Der SNMP-Agent übernimmt dabei die Aufgabe, entsprechende Anfragen zu empfangen und zu versenden.



- Versions-Nummer
- Nutzerberechtigungen
- Senden von Traps
- Bestätigen/Abbrechen
- SNMP-Funktionstest

Tipp:

SNMP V1.0 wird vom SITEMANAGER 7 offiziell nicht unterstützt. Wir empfehlen ausschließlich den Gebrauch ab Version 2.0. Da V1.0 aber in großen Bestandteilen von V2.0 enthalten ist, wird der SITEMANAGER 7 auf SNMP-V1 Anfragen antworten, jedoch erfolgt die Verwendung von V1.0 außerhalb des offiziellen Supports.

Der SITEMANAGER 7 unterstützt die SNMP v2 und SNMP v3

Der Unterschied besteht darin, dass SNMP v2 auf der Basis der berechtigten IP-Adresse während SNMP v3 auf der Basis direkter Nutzerberechtigungen mit Namen und Passwort arbeitet.

SNMP Version 2 3

Aktivieren Sie zunächst den SNMP-Agenten, um auf das Menü zugreifen zu können. Unter SNMP-Version wählen sie die gewünschte Version aus.

Einrichten von SNMP V2:

Die Übersicht zeigt alle bisher eingerichteten Nutzergruppen

SNMP Communities			
	Address	Community	Permission
+			

Um einen neuen Berechtigung zu konfigurieren, klicken Sie auf das +

Add Community

IP Address: IP address required

Community:

Permission:

- Die berechtigte IP-Adresse
- Die berechtigte Community
- Berechtigungen bei Datenzugriff

IP-Adresse

Geben Sie unter *IP-Adresse* die IP-Adresse des berechtigten Computers ein, welcher über SNMP v2 auf den CS141 zugreifen darf. Die *Community* definiert die Berechtigungsgruppe.

Permission

Diese Einstellung definiert die direkte Berechtigung, mit der ein Gerät auf den CS141 zugreifen darf:

Read only Geräte in dieser Berechtigungsgruppe haben reine Leserechte
Read/Write Geräte in dieser Berechtigungsgruppe besitzen Lese- und Schreibrechte.

Einrichten von Trap EmpfängernWofür sind SNMP-Traps da?

Grundsätzlich kann ein Agent, der ein System überwacht, unaufgefordert ein sogenanntes Trap-Paket an seine Management-Station senden, sollte dies erforderlich sein. Dabei wird unter anderem der Status des überwachten Geräts mitgeteilt. Der Agent kann im Anfragen wiederum von seinem Manager erhalten und bedienen. Dabei werden standardmäßig zwei Ports benötigt:

Port 161 Wird vom Agenten auf dem Gerät zum Empfangen der Anfragen benötigt
Port 162 Wird von der Managementstation zum Empfangen von Nachrichten benötigt

Sind diese Ports in der Firewall oder auf Switchen blockiert, funktioniert die Kommunikation nicht.

Konfigurieren von Trap-Empfängern auf dem SITEMANAGER 7

Der Vorteil der Trap-Nachrichten, ist, dass der SITEMANAGER 7 automatisch über Änderungen bei der USV informieren kann. Hierzu muss dem System jedoch mitgeteilt werden, wohin die Nachrichten geschickt werden sollen:

SNMP Trap-Empfänger		
+	Adresse	SNMP Community
<input type="button" value="Übernehmen"/> <input type="button" value="Abbrechen"/>		

Klicken Sie auf das +, um einen neuen Trap Receiver anzulegen.

Da Trapnachrichten ausschließlich gesendet werden und über Statusänderungen informieren, entfällt das Eingabefeld für die Schreib/Lesevorgänge.

Geben Sie die IP-Adresse des Empfängers sowie die gültige Community ein.

Mit Save übernimmt der SITEMANAGER 7 die Einstellungen und startet den SNMP-Agenten neu. Der SITEMANAGER 7 muss hier nicht komplett neu gebootet werden.

Add Trap Receiver	
IP Address:	<input type="text" value="10.10.10.10"/> IP address required
SNMP Community	<input type="text" value="public"/>
<input type="button" value="Save"/> <input type="button" value="Abbrechen"/>	

Test der Trap Empfänger

SNMP-Traps testen

Sie können einen Stromausfall und einen Strom wiederhergestellt Trap an die u. g. Empfänger senden.

Bitte beachten Sie: Um die neu hinzugefügten Empfänger zu testen, ist es erforderlich, die Konfiguration zu speichern.

192.168.200.17	public	<input type="button" value="Test"/>
----------------	--------	-------------------------------------

Die neu eingerichteten Trao Empfänger können im Anschluss getestet werden, indem Sie den Test-Button betätigen. Die entsprechende Testnachricht wird abgesetzt und sollte direkt in Ihrem Programm angezeigt werden.

Tipp:

Trap-Nachrichten sind automatisch generierte Nachrichten, welche *keine* Bestätigung anfordern – ein Gerät, welches Trapnachrichten versendet, weiß generell nicht, ob die Nachrichten angekommen sind. Folglich werden auch keine Informationen über einen Empfang protokolliert werden können.

[Einrichten von SNMP v3](#)

Die Übersicht zeigt alle bisher eingerichteten Nutzer

SNMP User		
+	User	Access
<input type="button" value="Übernehmen"/> <input type="button" value="Abbrechen"/>		

Da SNMP v3 auf Benutzerbasis arbeitet, können Sie hier keine Benutzergruppen anlegen. Klicken Sie auf das +, um einen neuen Nutzer zu konfigurieren:

User Definition:

Standardmäßig hat jeder Nutzer die Berechtigung zum Lesen und Schreiben. Wenn Sie einen Nutzer gezielt das Schreibrecht verweigern wollen, aktivieren Sie die Option *Read only*

Authentication

Definieren Sie den Sicherheitslevel, mit dem ein Nutzer zugreifen kann:

No security	Kein Passwort benötigt
Authenticity	Ein Passwort wird abgefragt.
Authentication and Privacy	Die Verbindung wird zusätzlich verschlüsselt, zwei Passworte werden benötigt.

Tipp:

Bitte beachten Sie, dass neben den richtigen Zugangsdaten auch der Verschlüsselungstyp identisch sein muss, ansonsten kommt keine Verbindung zu Stande.

Einrichten von TRAP Empfängern unter SNMP v3

Um unter SNMP v3 einen Trap Empfänger einrichten zu können, müssen Sie zunächst einen passenden User anlegen. Diesen User können Sie bei SNMP v3 anschließend als Trap-Empfänger auswählen.

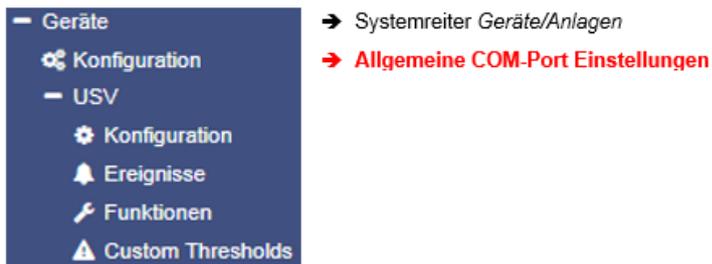
Test der Trap Einstellungen

Im Anschluss können Sie über die Testfunktion den SNMP v3 Trapempfänger testen:

SNMP-Traps testen			
Sie können einen Stromausfall und einen Strom wiederhergestellt Trap an die u. g. Empfänger senden.			
Bitte beachten Sie: Um die neu hinzugefügten Empfänger zu testen, ist es erforderlich, die Konfiguration zu speichern.			
192.168.200.17	My_User		Test

Allgemeine Interfaceeinstellung der COM-Ports

Für diesen Konfigurationsschritt benötigen Sie folgendes Menü:



Je nach Bauart und Modell besitzen die Geräte der CS141-Familie bis zu drei hardwareseitige COM-Anschlüsse, welche unterschiedliche Funktionen erfüllen können.

Sowohl der SITEMANAGER als auch der SITEMONITOR sind hier technisch weitgehend vorkonfiguriert:

COM 1

Dieser Anschluss ist für den Anschluss der USV reserviert

COM 2 – Sensor

Type: Sitemonitor / Sitemanager

Der SITEMANAGER 6verfügt über interne Relais sowie die Option, analoge Sensoren und digitale inputs zu verwalten.

Der SITEMONITOR 6 besitzt bis 64 digitale Eingänge sowie zwei AUX-Ports, über die extern speziell entwickelte Relaisboards angeschlossen werden können.

Der integrierte CS141 kommuniziert intern der bereits vorinstallierten Hardware.

COM 3

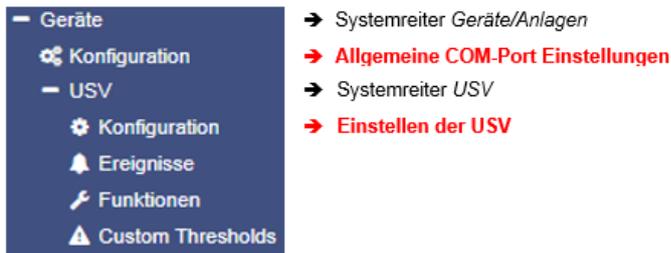
Der SITEMANAGER 7 verwendet die COM-Schnittstelle, um mit dem BACS-System zu kommunizieren.

USB – Port

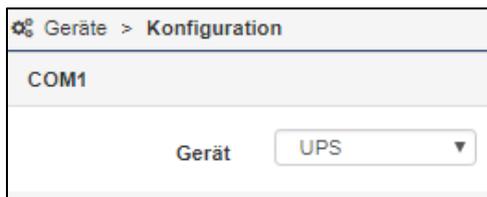
Der SITEMANAGER 7 kommuniziert über den internen USB-Port mit dem WLAN-Modul

Einstellen der USV

Für diesen Konfigurationsschritt benötigen Sie folgende Menüs:



Kontrollieren zunächst die allgemeinen COM-Port Einstellungen:



Standardmäßig ist für COM1 das Gerät UPS ausgewählt. Ist dies nicht der Fall, öffnen Sie das Auswahlmennü und wählen Sie UPS aus.

Mit Übernehmen wird die neue Einstellung gespeichert und der CS141 startet die entsprechenden Dienste, die notwendig sind, eine USV ansprechen zu können. Mit der Aktivierung dieser Funktion wird zunächst ein allgemeiner Dummy gesetzt, über den Sie Zugriff auf die entsprechenden Menüs erhalten.

Sie können die Erfolgreiche Aktivierung in der oberen Leiste deutlich erkennen



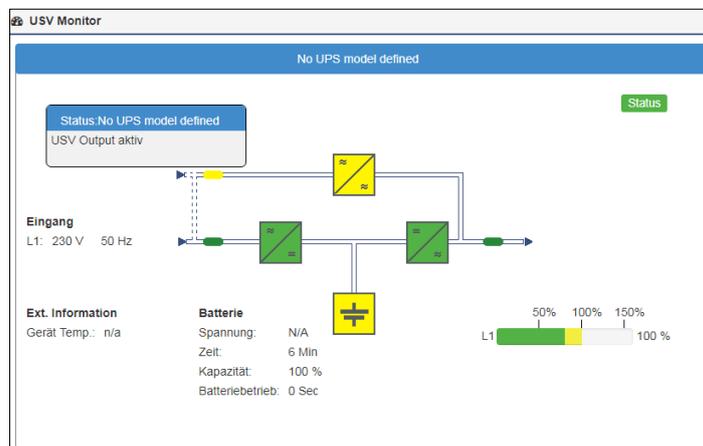
→ Das System startet die USV-Funktion



betriebsbereit

→ Der Dummy und das USV-Menü sind

Beachten Sie bitte, dass an dieser Stelle lediglich ein Dummy ohne eine Funktion gestartet wurde, auch wenn scheinbar eine USV angeschlossen und in Betrieb ist:



Tipp

Sollten Sie keine USV verwenden wollen bzw. angeschlossen haben, können Sie den COM 1 auf none stellen. In dem Fall werden die zuständigen Dienste deaktiviert und die weiterführenden Konfigurationsmenüs automatisch ausgeblendet.

Nachdem Sie auf COM1 für die USV bereitgestellt haben, gehen Sie auf das Untermenü *USV* und dort auf *Konfiguration*

- Auswahl des USV-Modells
- Die von der USV zur Verfügung gestellte Leistung
- Maximale Last, die an der USV anliegen darf
- Maximale Dauer, die die USV bei maximaler Last hält
- Zeit, bis die Akkus wieder aufgeladen sind.
- Geschwindigkeit der Datenübertragung
- Zu verwendendes Kabel
- UPS ID
- Datum, wann die Batterien installiert wurden
- Hinweis, wann die Batterien getauscht werden sollten

- Dauer, ab wann die USV sich selber abschaltet
- Speichern / Abbrechen

Übersicht der Einstellungen

Diese Werte werden interessant, sobald das Protokoll der USV keine entsprechenden Daten liefert. In diesem Fall ist der CS141 an Hand der Datenlage im Stande, selbstständig die entsprechende Laufzeit im Batteriemodus zu berechnen. In Regel muss an diesen Einstellungen nichts geändert werden, wenn Sie ein USV-Modell auswählen können – die für das Modell optimale Konfiguration wurde bereits hinterlegt.

Wenn Sie eine vom Standardmodell abweichende Konfiguration einstellen möchten oder ein Modell, bei dem diese Daten nicht über das Protokoll von der USV geliefert werden, setzen Sie sich mit dem Hersteller der USV in Verbindung, um die korrekten Werte in Erfahrung zu bringen.

Tipp:

Standardmäßig ist die OEM ID 12 für GENEREX SYSTEMS eingestellt. Sollten Sie eine USV von einem anderen Hersteller verwenden wollen, lohnt sich ein Blick in den Downloadbereich von www.generex.de – suchen Sie sich die Firmware zu Ihrer USV aus installieren Sie dieses als reguläres Firmwareupdate.

Im Anschluss stehen Ihnen die entsprechenden USV-Modelle zur Verfügung.

Folgende Informationen können angepasst werden:

Modell

Definiert die Voreinstellung der USV mit dem entsprechend hinterlegten Protokoll. Wenn Ihre USV aufgelistet ist und eine Kommunikation hergestellt wurde, liefert die Telemetrie der USV in der Regel alle notwendigen Daten, die der CS141 für die Berechnung und Anzeige der realen Autonomiezeiten benötigt.

Beachten Sie bitte, dass beim Wechsel des USV-Modells auch die Konfiguration der USV-Ereignisse zurückgesetzt. Der CS141 bietet an daher die Möglichkeit, vorher ein entsprechendes Backup der Ereigniskonfiguration zu erstellen.

- Don't save: Weiter ohne Backup
- Save: Backup erstellen
- Abbrechen: Keine Änderungen am System durchführen

Leistung (VA)

Definiert die Leistung der USV in VA, die eine USV Verfügung stellen kann. Wenn dieser Wert überschritten wird, kann die USV nachhaltig beschädigt oder sogar zerstört werden.

Last (VA)

Definiert die maximale Last, die real angeschlossen werden soll. Dieser Wert sollte niemals höher als der unter Leistung stehende Wert sein. Bitte beachten Sie, dass die Last maximal gleich dem Wert Leistung sein kann.

Haltezeit (Min)

Dieser Wert wird in Minuten angegeben und definiert die maximale Laufzeit bei 100% angeschlossener Last.

Akkuladezeit

Die geschätzte Zeit, die ein vollständiger Ladezyklus benötigt.

Tipp:

Hinter den Werten *Leistung (VA)*, *Last (VA)*, *Haltezeit* und *Akkuladezeit* ist eine mathematische Formel hinterlegt, über die der CS141 selbstständig errechnen kann, wie lange die Batterien der USV im Autonomiefall reichen müsste und daraus die entsprechenden Systemereignisse auslösen. Diese Werte kommen nur dann zum Tragen, wenn das Protokoll der USV keine Werte liefern kann – zum Beispiel, wenn eine USV ausschließlich über schaltbare Kontakte kommuniziert und lediglich grundlegende Betriebszustände erfasst werden können

Baud Rate

Unterschiedliche Protokolle unterstützen unterschiedliche Geschwindigkeiten bei der Datenübertragung. Die Baudrate definiert die Geschwindigkeit, mit der Daten gesendet und empfangen werden können. Eine falsche Baud Rate kann zu Kommunikationsstörungen zwischen dem CS141 und der USV führen.

Kabeltyp

USV-Hersteller verwenden für Ihre Modelle teilweise speziell konfektionierte Kabel. Neben diesen speziellen Eigenentwicklungen gibt es noch standardisierte Kabeltypen, durch deren Beschaltung unterschiedliche Funktionen und Schaltzustände abgebildet werden können.

Batterieinstallationsdatum

Batterien in einer USV haben eine begrenzte Lebensdauer – zu den regelmäßigen Wartungsarbeiten gehört daher auch der Tausch der Batterien. Um in größeren Installationen den Überblick zu behalten, können Sie hier das Datum eintragen, wann Sie die Batterien in Betrieb genommen bzw. zuletzt getauscht haben.

Batterie veraltet nach

Der CS141 kann automatisch Hinweise geben, wann der reguläre Betriebszeitraum für die installierten Batterien abgelaufen ist. Standardmäßig meldet sich der CS141 mit entsprechenden Systemhinweisen nach 48 Monaten. Sie können den Zeitraum in Monaten verlängern oder verkürzen

System Shutdown Zeit

Über die System Shutdown Zeit wird die letzte Notabschaltung des Netzwerks definiert, das unter Geräte/Anlagen>USV>Ereignisse zu finden ist. Über diesen Wert kann prinzipiell die letzte Notabschaltung des gesamten Netzwerks definiert werden.

UPS-ID

Große USV-Anlagen können mehr als ein USV-Modul beinhalten, welche über eine eindeutige ID abgefragt werden. Die 0 ist dabei eine Form von Broadcast, bei der der CS141 die Anzahl der USV-Module selber erkennen und verwalten kann, was im Normalfall die optimale Einstellung darstellt. Wenn Sie diesen Wert ändern, bekommen Sie auch nur noch exakt das Modul mit dieser speziellen ID angezeigt.

Übernehmen / Abbrechen

Diese Funktion erlaubt das Speichern und den Neustart des USV-Dienstes auf dem CS141.

Anschluss der USV an den SITEMANAGER 7

Auf der Rückseite des Geräts befindet sich neben dem Netzwerkanschluss ein mit COM 1 beschrifteter MINI-DIN – Anschluss:

Schließen Sie das im Lieferumfang erhaltene Adapterkabel MINIDIN / RS232 an und verbinden Sie anschließend das im Lieferumfang Ihrer USV enthaltene Standard Datenkabel mit dem Adapterkabel:



Um den korrekten Halt zu gewährleisten setzen Sie zwischen die kleinen beiden Arretierungen die im Lieferumfang enthaltenen Schraubmuttern.

Der SITEMANAGER bzw. SITEMONITOR zeigt nach einer kurzen Synchronisationsphase die Daten der USV im USV-Monitor an:

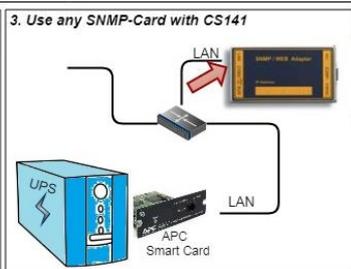
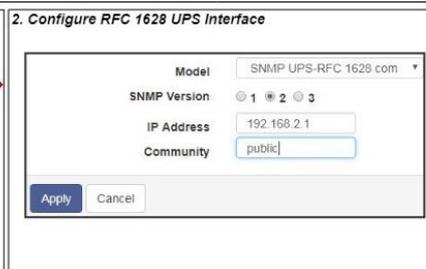
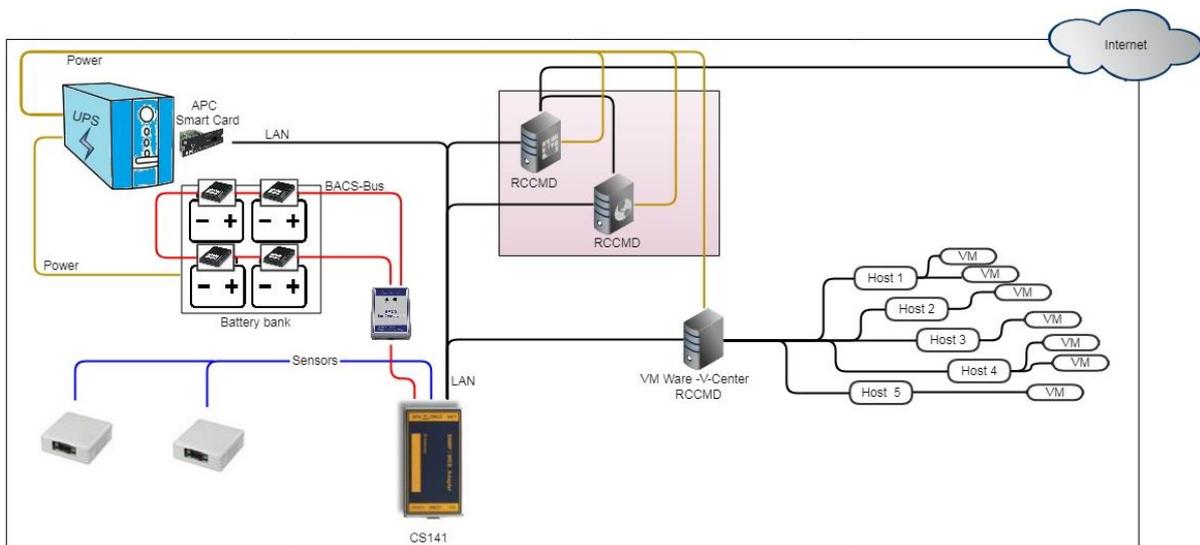
Die Status-LED blinkt langsam und gleichmäßig grün

Besonderheit: Die RFC1628 USV Schnittstelle

In einigen Fällen liefern USV-Hersteller Anlagen aus, mit denen der CS141 nicht direkt kommunizieren kann – oftmals liegt es dann an dem Problem, dass die Karte zum Beispiel nicht in den Slot passt, oder dass die von USV gesendeten Daten nicht kompatibel sind.

USV-Hersteller haben in dem Fall eine eigene SNMP-Karte verbaut, welche ähnliche Funktionen bietet, jedoch zu Ihrer GENEREX-Softwarelandschaft nicht kompatibel sein kann. Um dennoch eine Kompatibilität zu gewährleisten bietet der CS141 Webmanager die Möglichkeit, mittels SNMP mit einer beliebigen Karte zu verbinden. Die einzige Bedingung ist hier, dass die RFC 1628 MIB von der Zielkarte unterstützt wird.

Um diese Funktion nutzen zu können, ist es notwendig, zunächst auf der Zielkarte eine entsprechende SNMP-Freigabe zu konfigurieren. Anschließend können Sie im CS141 die Zugangsdaten eingeben und eine Verbindung zur Zielkarte aufbauen.



Einrichten der Zielkarte unter SNMP v2

Modell	SNMP UPS-RFC 1628 com
SNMP Version	<input type="radio"/> 1 <input checked="" type="radio"/> 2 <input type="radio"/> 3
IP Address	192.168.222.116
SNMP Community	public
<input type="button" value="Übernehmen"/> <input type="button" value="Abbrechen"/>	

- ➔ Auswahl USV-Modell
- ➔ SNMP Version
- ➔ IP-Adresse des Zielsystems
- ➔ SNMP Community
- ➔ Speichern/Abbrechen

Modell

Wählen Sie hier das Modell SNMP UPS-RFC 128 com aus

SNMP-Version

Je nach Konfiguration der Zielkarte stellen Sie hier SNMP-Version v1 oder v2 ein.

SNMP Community

Geben Sie die SNMP Community an, unter der die Zielkarte erreichbar ist.

Übernehmen/Abbrechen

Mit Übernehmen wird die Konfiguration übernommen der CS141 baut eine Verbindung zur anderen SNMP-Karte auf. Wenn die Kommunikation hergestellt ist, können Sie im oberen Bereich einen grünen Marker bei UPS sehen.

Tipp:

Was ist der Unterschied zwischen der RF1628 USV Schnittstelle und dem APC Smart Network?

Im Prinzip kann die APC-Karte auch mit dem RFC1628 Standard umgehen – Sie werden grundsätzliche Informationen über die USV abfragen können. Die APC Karte verwendet an vielen Stellen jedoch eigene OID's, welche für APC spezifisch und daher mit dem RFC1628 - Standard nicht vereinbar sind.

Für den vollen Funktionsumfang empfiehlt es sich daher, bei APC-USV Anlagen in diesem Anwendungsfall nicht auf die RFC1628 – Schnittstelle zurück zu greifen, sondern die APC-spezifische Einstellung APC Smart Network zu verwenden.

Einrichten der Zielkarte unter SNMP v3

Modell	SNMP UPS-RFC 1628 com
SNMP Version	<input type="radio"/> 1 <input checked="" type="radio"/> 2 <input type="radio"/> 3
IP Address	192.168.222.116
User	cs141
Security Level	Authentication and Privacy
Auth Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Auth Password
Privacy Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Privacy Password
<input type="button" value="Übernehmen"/> <input type="button" value="Abbrechen"/>	

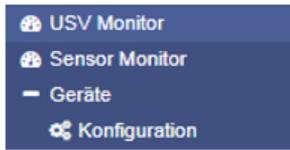
Version

- ➔ Auswahl des USV-Modells
- ➔ Bestimmen Sie die SNMP
- ➔ IP-Adresse des Zielsystems
- ➔ SNMP User
- ➔ Verschlüsselungsart
- ➔ Passwordeingabe MD5/SHA
- ➔ Passwordeingabe DES/AES
- ➔ Übernehmen/Abbrechen

Der CS141 unterstützt in diesem Betriebsmodus die SNMP Version v1, v2 und v3
Geben Sie die Zugangsdaten zu der Zielkarte gemäß Ihrer Konfiguration ein und betätigen Sie übernehmen.

USV-Monitor: Überprüfen der Einstellungen

Zum Überprüfen der Einstellungen wechseln Sie in das folgende Menü:



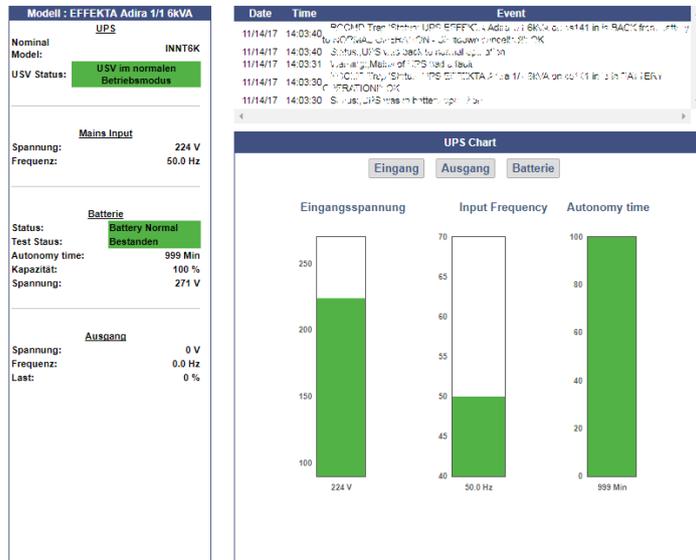
➔ Überprüfen der Einstellungen: USV-Einrichtung

Wenn alle Einstellungen korrekt eingegeben wurden, können Sie im USV-Monitor den aktuellen Status der USV in Echtzeit überprüfen. Auch wenn die Darstellung je nach Hersteller und Modell stark variieren kann, werden einige Daten wie das ausgewählte Modell immer angezeigt.

Deutlich zu erkennen ist:

- Modell
- Hersteller
- Leistungsdaten

Der genaue Umfang und die Darstellung variieren je nach Hersteller und Modell.



Die USV Funktionen

Für diesen Konfigurationsschritt benötigen Sie folgendes Menü:



➔ Systemreiter Geräte/Anlagen

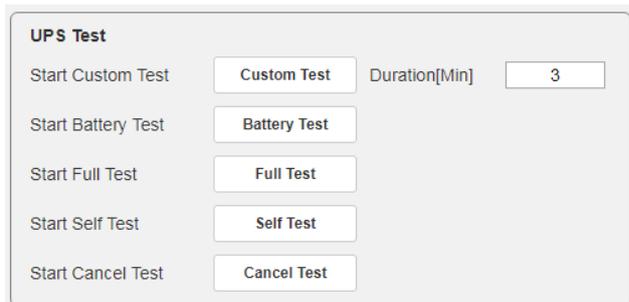
➔ Systemreiter USV

➔ Steuermenu für die ausgewählte USV

Funktionserklärung

Das Menü *USV Funktionen* enthält Möglichkeiten, USV-Test- und Kontrollszenarien wie Batterietests etc. durchzuführen. Die für diesen Menüpunkt angezeigten Masken können daher sehr unterschiedlich sein. Sie sind auf das verwendete USV-Modell zugeschnitten, um dessen Funktionsumfang darstellen zu können. Manche USVs lassen lediglich den An-/Aus-Zustand zu, andere bieten mehr Funktionen.

Typische Testfunktionen wären zum Beispiel:



definiertes Laufzeit ➔ USV-Test mit selbst

➔ Batterietest

➔ Volltest

➔ Selbsttest

➔ Abbruch von laufenden

Tests

Custom Test

Der Custom Test ist ein Funktionstest über eine selbst definierte Zeit in Minuten.

Battery Test

Der Battery Test überprüft, ob im Zweifelsfall die Batterien richtig übernehmen und arbeiten. Dieser Test dauert in der Regel etwa 15 Sekunden.

Full Test

Der Full Test überprüft die Batterien bis zur Erschöpfung. Dieser Test kann in Abhängigkeit zu Leistung und Last sehr lange dauern. Dabei wird vom CS141 auch die Laufzeit unter Last genau gemessen und ermittelt. Bitte beachten Sie, dass USV-Systeme für einen Full Test eine angeschlossene Last von mindestens 25% benötigen.

Selftest

Mit diesem Test überprüft die USV seine eigene Funktionalität als Ganzes

Tipp:

In einigen Fällen kann es vorkommen, dass ein USV-Befehl scheinbar nicht ausgeführt wird oder eine Fehlermeldung erscheint. Hintergrund ist, dass die USV zwar den Befehl entgegennimmt und bestätigt, jedoch selber entscheidet, ob und wann dieser Befehl ausgeführt werden kann oder wird – Je nach USV-Modell kann durchaus passieren, dass zum Beispiel für einen bestimmten Batterietest eine minimale Ladung vorhanden sein muss, ansonsten gibt die USV als Resultat eine Fehlermeldung zurück. Diese wird dann entsprechend als „Fehler“ protokolliert.

Im Umgekehrten Fall kann es auch sein, dass die USV trotz Fehler ein positives Feedback sendet, aber an der Stirnseite selber einen Fehler anzeigt.

UPS Control settings

Je nach Bauart und Modell unterstützen einige USV-Anlagen zusätzliche Funktionen, über die das Betriebsverhalten der USV überprüft werden kann. Der genaue Funktions- und Konfigurationsumfang ist sehr unterschiedlich und hängt stark sowohl vom Hersteller als auch vom verwendeten Modell ab.

Typische Testfunktionen sind zum Beispiel:

The screenshot shows a control panel titled "UPS Control" with the following elements:

- A button labeled "Shutdown Restore".
- Input fields for "Shutdown[Sec]" with the value "60" and "Restore[Sec]" with the value "120".
- A button labeled "Shutdown with Duration".
- An input field for "Shutdown[Sec]" with the value "60".
- A button labeled "Switch off UPS".
- A button labeled "Cancel Shutdown".
- A button labeled "Toggle Buzzer".

Schaltbare Ausgänge

Je nach Bauart unterstützen einige USV-Anlagen das AN- und Abschalten der Ausgänge.

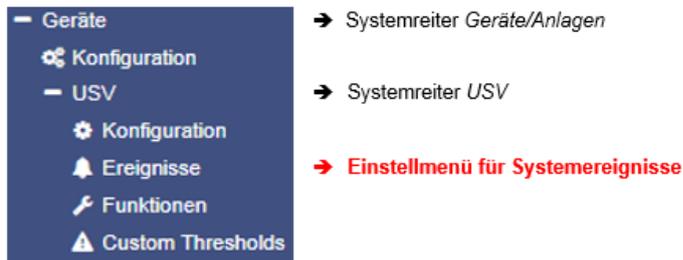
The screenshot shows a control panel titled "Toggle the outlets" with two green buttons labeled "1" and "2".

Tipp

Die USV-Anlagen sind je nach Leistungsklasse, Hersteller und Modell unterschiedlich ausgestattet. Dabei variiert sowohl das Layout als auch der Funktionsumfang.

Einstellen der Systemereignisse

Für diesen Konfigurationsschritt benötigen Sie folgendes Menü:



Es gibt immer wieder Vorfälle, die den Betrieb einer USV erforderlich machen oder die USV und die angeschlossenen Geräte hinter der USV betreffen - darunter fällt zum Beispiel das Versagen der Hauptstromversorgung, das Wiederherstellen der Hauptstromversorgung, ein Defekt an der USV, die das Umschalten in den autonomen Batteriemodus verhindert, etc.

Der CS141 kann als vollwertiger Manager im Vergleich zu anderen sogenannten Systemen auf diese Vorfälle mit einem Systemereignis reagieren, informieren und selbstständig vollständige Ereignisketten verwalten: Er bietet die Möglichkeit, eine komplette Shutdownlösung für ein komplexes Netzwerk mit gegenseitigen Abhängigkeiten zu realisieren.

Definition eines Jobs für ein Ereignis

Systemereignisse sind stark von dem verwendeten USV-Modell abhängig und variieren sowohl in der Bezeichnung als auch an der Fülle von Möglichkeiten. Einer der größten Probleme hier stellt das Zusammenspiel von Ereignissen und Gegenereignissen dar:

Einem Ereignis wird eine Handlung, - ein sogenannter Job - zugewiesen, welcher nur dann ausgeführt wird, wenn das Ereignis eintritt. Dabei unterscheiden sich die Jobs in ihrer Funktion und Art:

- Information

Diese Jobs können beliebig oft ausgeführt werden und erfüllen lediglich den Zweck der Information. Je nach Konfiguration kann dabei der Inhalt einmalig oder zyklisch wiederholt werden, solange ein Ereignis ansteht – dabei ist die Art des Ereignisses grundsätzlich egal. Ändert sich die Gegebenheit und das Ereignis kommt nicht mehr zum Tragen, wird dieser Job einfach nicht weiter ausgeführt.

- Aktion

Diese Jobs sind darauf ausgelegt, etwas zu schalten, auszulösen, anzustoßen, etc. Diese Jobs werden ausgelöst, sobald ein Ereignis eintritt. Der Unterschied ist, dass sie mit einem entsprechenden gegenläufigen Job wieder beendet oder Anweisungen wieder zurückgenommen werden müssen.

Tipp:

Warum ist es wichtig, diesen Unterschied zu verstehen?

Solange ein Stromausfall ist, soll alle 5 Minuten gezielt eine Mail geschrieben werden, die Logdateien versendet. Sobald der Stromausfall beseitigt ist, wird keine E-Mail mehr geschrieben. Ein Job, der einen potentialfreien Kontakt schließt, sobald ein Stromausfall festgestellt wird, wird einmalig ausgeführt und ist damit beendet. Auch wenn der Stromausfall beseitigt wurde, bleibt der Kontakt geschlossen. Ist über den Kontakt eine Warnlampe geschaltet, würde diese so lange leuchten, bis dieser Kontakt wieder bewusst geöffnet wird.

Das *warum* wird an folgendem Beispiel sichtbar:

Wenn ein Temperaturfühler ab einer bestimmten Temperatur den CS141 veranlasst, eine Mail mit einer Warnung auszugeben und den Kontakt für eine Klimaanlage zu schließen, wird dies gemäß der Konfiguration durchgeführt. Sobald die Temperatur unter den kritischen Wert sinkt, wird keine weitere Mail mit einer Warnung über kritische Temperaturen verschickt - aber die Klimaanlage muss zwangsläufig weiterlaufen, bis sich die Temperatur vollständig normalisiert hat. Genau das würde nämlich nicht funktionieren, wenn sich der Kontakt in dem Moment automatisch öffnet, weil das Ereignis für zu hohe Temperaturen nicht mehr gegeben ist. Man benötigt einen aktiven Job, um die Klimaanlage gezielt abzuschalten, sobald eine bestimmte Temperatur unterschritten wurde.

Problematisch wird es, wenn auf Grund eines Stromausfalls zwei USV-Anlagen, die über getrennte Stromkreise laufen, einen Befehl zum Shutdown geben müssen: Sobald beide Anlagen einen gültigen Shutdown angeordnet haben, fährt der Server sofort runter - Auch dann, wenn beide USV-Systeme zeitlich getrennt jeweils einen Stromausfall meldeten, und den Shutdownbefehl nicht zurückgenommen haben, nachdem ihre jeweiligen Einzelprobleme beseitigt wurden.

Definition eines Jobs für ein Ereignis

Die Jobs können jederzeit konfiguriert werden. Getestet werden können Sie jedoch nur unter zwei Bedingungen:

1. Jobs in Verbindung mit einem Mailkonto benötigen gültige Zugangsdaten
2. Jobs auf Basis der TCP/IP – Einstellungen benötigen eine gültige Netzwerkkonfiguration

Kontrollieren Sie vor dem nächsten Konfigurationsschritt, dass alle Zugangsdaten hinterlegt sind, die Netzwerkeinstellungen richtig sind und sich der CS141 im regulären Betriebsmodus in Ihrem Netzwerk befindet.

Jobs verwalten

Klicken Sie im Untermenü *USV* auf Ereignisse, um die verfügbaren Systemereignisse einsehen zu können. Beachten Sie bitte, dass sowohl die Anzahl und als auch Bezeichnung der Ereignisse zwischen unterschiedlichen USV-Modellen abweichen können.

Symbole mit eindeutiger Funktion:

	→ Öffnen und Schließen der Tabelle
	
	→ Editieren eines vorhandenen Jobs
	→ Testen eines vorhandenen Jobs

Symbole mit Doppelfunktion:

	→ Löschen
	→ Checkbox zum Auswählen von mehreren Jobs oder Ereignissen
	→ Hinzufügen eines Jobs

Tipp:

Symbole mit Doppelfunktionen haben zwei unterschiedliche Bedeutungen. Je nachdem, wo man sie bedient, beziehen sie sich auf ALLE Ereignisse oder auf ein spezielles Ereignis beziehungsweise eingestelltes Event. Diese doppelte Funktionalität erlaubt, ein bestimmtes Event zu bestimmten oder allen Systemereignissen hinzuzufügen, ohne es jedes Mal einzeln einzugeben.

Einrichten eines Jobs

Das Verwalten von Jobs zu einem Systemereignis erfolgt immer nach denselben Regeln - für dieses Beispiel wurden folgende Systemereignisse ausgewählt:

	<input type="checkbox"/>			Stromausfall	3	1	0	1	0
	<input type="checkbox"/>			Power restored	3	1	0	1	0

Klicken Sie auf , um eine allgemeine Übersicht über bereits vorhandenen Jobs zu erhalten:

		Stromausfall	3	1	0	1	0	0
		Job Typ	Wann	Parameter				
		Log	Periodisch alle 100s, sofort	{\"text\":\"Powerfail\"}				
		RCCMD Trap	Einmal, sofort	{\"text\":\"Powerfail on #MODEL . Autonomietime #AUTONOMTIME min.\"}				
		E-Mail Trap	Einmal, sofort	{}				

Für das Ereignis Stromausfall sind also insgesamt 3 Jobs bereits konfiguriert. Diese Jobs wurden bei der Auswahl der USV als eine empfohlene Standard-Konfiguration geladen. Wenn Sie diese Ändern oder entfernen möchten, klicken Sie auf das entsprechende Symbol.

Wenn Sie innerhalb eines Systemereignisses alle Job löschen möchten, aktivieren Sie die Checkbox in der Zeile für Stromausfall und drücken auf das Löschsymbolsymbol. In diesem Fall werden alle diesem einen Ereignis zugeordneten Jobs aus der Liste gelöscht. Bei sehr vielen Jobs ist diese Option sehr nützlich.



Tip:

Gelöschte Jobs können nicht zurückgeholt werden, sie müssen in dem Fall neu angelegt oder über ein Backup wieder eingespielt werden. Um ein versehentliches Löschen zu verhindern, muss diese Eingabe über eine Sicherheitsabfrage noch einmal bestätigt werden.

Um ein Job dem Ereignis Stromausfall hinzuzufügen, betätigen Sie in der Ereigniszeile das +. Diese Funktion startet das Konfigurationsmenü zur Einrichtung von Jobs.

Verfügbare Jobs:

Log	Es wird in das Eventlog ein Eintrag gemacht.
Email	Eine E-Mail wird versendet.
Email Trap	Eine Trapnachricht wird versendet.
RCCMD Shutdown	Ein Shutdownsignal wird an einen oder mehrere RCCMD-Clients übermittelt.
RCCMD Message	Eine RCCMD-Nachricht wird an einen oder mehrere RCCMD-Clients übermittelt.
RCCMD Execute	Es wird ein Kommando via RCCMD gesendet, wodurch ein RCCMD-Client eine Datei ausführt.
UPS Shutdown**	Auswechseln der USV
AUX*	Schaltet externe Relais an bzw. aus.
Buzzer*	Sollte ein Alarmgeber angeschlossen sein, kann er mit diesem Kommando aktiviert werden.
RCCMD Trap	Eine RCCMD Trap Nachricht wird übermittelt
Send WOL	Ein Wake On LAN – ein sog. <i>magic packet</i> – wird an einen Netzwerkgerät übermittelt.
Remote Command*	Steuern Sie einen CON_R_AUX4, oder ein GSM-Modem an einem anderen Gerät
Send SMS*	Wenn ein GSM-Modem angeschlossen ist, kann eine SMS versendet werden*

* Für die Nutzung dieser Funktionen sind eventuell zusätzliche Ausrüstung und Zubehörteile notwendig bzw. werden von Ihrem Gerät nicht unterstützt

** Diese Funktion steht nur bedingt zur Verfügung: Einige USV-Anlagen unterstützen zwar grundlegend die Funktionalität, reagieren jedoch sehr unterschiedlich auf diesen Job.

Besonderheiten beim Job UPS Shutdown

Eine USV führt einen UPS Shutdown aus, um die Batterien vor einer Tiefenentladung zu schützen. Dabei wird die USV physikalisch heruntergefahren und ausgeschaltet. Der Zeitpunkt, wann eine USV diese Funktion ausführt, variiert dabei bereits zwischen den Modellen innerhalb eines Herstellers – hinzukommt, dass jeder Hersteller zudem auch eigene Definitionen zum Schutz der Batterien verwendet.

Da die USV ausgeschaltet wird, können hier in der Konsequenz nur schwer Gegebenheiten konfiguriert werden.

Definition eines UPS Shutdowns

Job	UPS Shutdown
Parameter	
Shutdown Time	<input type="text"/>
Restore Time	<input type="text"/>
Type	1

➔ Auswahl des Jobs

Sekunden

➔ Zeit zum Ausschalten in

Sekunden

➔ Zeit zum Anschalten in

➔ Ausschaltmodus

Zeit zum Ausschalten in Sekunden

Definieren Sie, wie lange die USV den Betrieb aufrechterhalten soll, bevor sie sich selbst herunterfährt.

Zeit zum Anschalten in Sekunden

Wenn die Hauptstromversorgung wiederhergestellt ist, wartet die USV den voreingestellten Wert in Sekunden, bis sie wieder hochfährt.

Type

Diese Einstellung definiert, was die USV genau ausschalten bzw. anschalten soll. Dabei gibt es zwei unterschiedliche Einstellungen:

- 1 Die USV schaltet die Ausgänge aus, bleibt aber selbst autonom in Betrieb.
- 2 Die USV schaltet sich komplett aus und wartet, bis der Hauptstrom wiederhergestellt ist

Verwendung des Jobs UPS Shutdown

Dieser Job kann nicht beide Einstellungen in Einem abbilden, es sind je nach gewünschtem Ziel mindestens zwei Jobs notwendig. Sie können über zwei unterschiedliche Jobs zum Beispiel folgende Sequenz realisieren:

- Ausgänge nach 3 Minuten ausschalten
- USV nach 4 Minuten herunterfahren
- USV 2 Minuten nach Wiederherstellung der Hauptstromzufuhr anschalten
- 15 Minuten später die Ausgänge freischalten

Beachten Sie, dass die Shutdown-Time und die Restore-Time entsprechend verschachtelt für beide Jobs korrekt wiedergegeben werden müssen. Tragen Sie in diesem Fall je nach gewünschtem Ereignis entweder eine 1 oder eine 2 ein.

Jobs suchen und anzeigen

>	<input type="checkbox"/>	+	Ereignis	Jobs	Log	E-Mail	E-Mail Trap	RCCMD Shutdown	RCCMD Nachricht
			contains...	<input type="text"/>					

Die Suchfunktion ist eine schnelle und einfache Möglichkeit, innerhalb der Ereignisse konfigurierte Jobs zu finden. Dabei haben Sie zwei grundlegende Möglichkeiten:

Ereignis: contains...

Wenn Sie ein bestimmtes Ereignis suchen, können Sie über diese Leiste durch Eingabe eines Wortes oder Wortfragments alle passenden Ereignisse anzeigen lassen.

Jobs

Geben Sie hier die Anzahl konfigurierter Jobs ein, und es werden alle Ereignisse mit dieser Jobanzahl aufgelistet.

Bei der Einrichtung ändern sich einige Parameter, je nachdem welcher Job ausgewählt wurde.

Job	Log
------------	-----

Die Auswahl des Jobs definiert, welche Parameter angezeigt werden:

Beispiel 1: Logdateien - welcher Text soll im Eventlog erscheinen?

Parameter	
Text	<input type="text"/>

Beispiel 2: RCCMD - Welche IP-Adresse soll die Nachricht empfangen und auf welchem Port wird gelauscht?

Parameter	
IP	<input type="checkbox"/> Broadcast <input type="text"/>
Port	<input type="text" value="6003"/>
Command	<input type="text"/>

Die Parameter unterscheiden sich, je nachdem, welcher Job im Einzelnen ausgewählt wurde.

Job Definition: Auswählbare Zeitfenster:

Der CS141 bietet viele Systemereignisse, welchen ein Job zugewiesen werden kann. Einige Systemereignisse können klare Bedingungen zugewiesen werden, wobei jeweils unterschiedliche Zeitrechnungen verwendet werden:

Zeitpunkt	
<input checked="" type="radio"/>	Sofort, einmalige Ausführung
<input type="radio"/>	Nach <input type="text"/> Sekunden
<input type="radio"/>	Nach <input type="text"/> Sekunden, wiederhole alle <input type="text"/> Sekunden
<input type="radio"/>	Nach <input type="text"/> Sekunden auf Batterie
<input type="radio"/>	Bei <input type="text"/> Sekunden Restlaufzeit

Sofort, einmalige Ausführung:	Sobald das Ereignis eintrifft, wird dieser Job genau ein Mal ausgeführt.
Nach XXX Sekunden:	Sobald das Ereignis eintrifft, wird bei der Ausführung des Jobs die eingestellte Zeit in Sekunden gewartet. Ist das Ereignis vorher beendet, wird der Job nicht ausgeführt.
Wiederhole alle XXX Sekunden:	Der Job wird zyklisch wiederholt, bis das Ereignis nicht mehr existiert.
Nach XXX Sekunden auf Batterie:	Das Ereignis muss eintreten und die USV eine voreingestellte Zeit im autonomen Modus laufen. Wenn zum Beispiel 300 Sekunden eingestellt wird, wird dieser Job nur ausgeführt, wenn die USV mindestens seit 300 Sekunden sich im autonomen Modus befindet.
Bei XXX Sekunden Restlaufzeit:	Der Job wird ausgeführt, wenn die Restlaufzeit der USV basierend auf der tatsächlich angehängten Last erreicht oder unterschritten wird.

Zeitmanagement der Jobs in Relation zur USV

Das Zeitmanagement bei auszuführenden Jobs ist schwierig, da man hier konzeptionell zwischen zwei unterschiedlichen Betrachtungsweisen unterscheiden muss. Am Beispiel des Ereignisses *Stromausfall* wird dieser Unterschied deutlich:

Bei einem Stromausfall übernimmt die USV die Stromversorgung und sichert den Betrieb der Server ab, bis einer von beiden Ereignissen eintrifft:

1. Die Batterien sind erschöpft
2. Die Hauptstromversorgung wurde wiederhergestellt.

Wenn die USV in den sogenannten *autonomen Modus* wechselt, laufen zwei unterschiedliche Zeitmesser:

Eine linear vorwärtslaufende Uhr in Sekunden, die bei 0 Beginnt.

Soll ein Job nach 45 Sekunden ausgeführt werden, wird er nur ausgeführt, wenn das Ereignis mindestens 45 Sekunden ansteht. Wird das Ereignis vorher beendet, wird der Job in der Konsequenz nicht ausgelöst.

Eine relative Uhr, die in Abhängigkeit zur angeschlossenen Last rückwärts zählt.

Diese Zeitmessung basiert auf einem relativen Wert, der die angeschlossene Last berücksichtigt. Wenn die USV zum Beispiel zu 100 % unter Last 7 Minuten den autonomen Betrieb zulässt, würde sie bei 50% entsprechend 50% länger halten, also 10,5 Minuten funktionieren:

Werden demnach der Logik folgend nach 3 Minuten Geräte ausgeschaltet und die Last auf 50% sinken, würde die Uhr von 4 Minuten auf 7,5 Minuten springen.

Beide Zählweisen haben ihre spezifischen Vor- und Nachteile:

Der eine Zähler gibt eine klare Vorgaben über eine zeitliche Abfolge und ignoriert dabei die tatsächliche vorhandene Restlaufzeit. Gibt es mehrere kleine Stromausfälle nacheinander, würde ein Servershutdown nach exakt 7 Minuten nicht greifen, wenn nur noch für 6 Minuten genug Strom zur Verfügung steht.

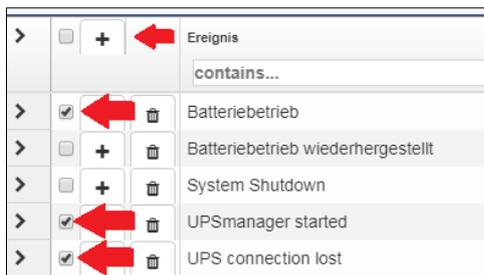
Der andere Zähler lässt sich schwer berechnen und es kommt zu einem zeitlichen Versatz von ausgeführten Aufgaben. 5 Minuten Restlaufzeit können auch über einen längeren Zeitraum nicht erreicht werden, wenn die Rahmenbedingungen die Restlaufzeit erhöhen, bzw. eine vorgegebene Abfolge von Ereignissen kann durcheinander kommen, sobald die Gegebenheiten diese Zeit nach unten korrigieren.

Tipp:

Grundsätzlich ist der Shutdown über die Restlaufzeit sinnvoll, da hier die tatsächlich vorhandene Batterieladung in die Berechnung mit eingeplant werden kann. Wenn hingegen bei anderen Jobs eine spezielle Reihenfolge einhalten muss, ist es sinnvoll, die linear vorwärtslaufende Uhr zur Zeitplanung zu verwenden.

Multiple Jobs hinzufügen

Unter Umständen kann eine Konfiguration es notwendig machen, dass mehreren Ereignissen der selbe Job zugewiesen werden muss. Um diese Jobs einem Ereignis zuzuweisen gibt es die Möglichkeit, jedes Ereignis einzeln anzuwählen und einen Job zu definieren.



Der schnellere Weg ist, dass Sie die Ereignisse auswählen, die den selben Job erhalten sollen und anschließend auf das abgelegene obere + klicken.

In diesem Fall wird der selbe Job bei jedem angewählten Ereignis angelegt.



Aktivieren Sie den Haken in der obersten Reihe, wenn ein Event allen Ereignissen zugeordnet werden soll – Es werden alle Ereignisse ausgewählt.

Um einen Job zuzuweisen, betätigen Sie anschließend das + in genau dieser Zeile.

Löschen von Jobs

Wenn bestimmte Systemereignisse für die Konfiguration nicht mehr relevant sind, besteht die Möglichkeit, diese Jobs aus der Systemkonfiguration zu entfernen:

- Einen Job löschen

Klappen Sie mit > den gewünschten Reiter auf:



Wählen Sie den gewünschten Job aus und betätigen Sie das kleine Papierkorb-Icon, um den ob sofort und dauerhaft aus der Konfiguration zu entfernen.

- Alle Jobs innerhalb eines Ereignisses löschen

-		<input checked="" type="checkbox"/>	+	🗑️	Batteriebetrieb
		↑		↑	
		✎	🗑️	▶	Job Typ
					Log
					Einmal, sofort
					RCCMD Trap
					Einmal, sofort

Wählen Sie die Checkbox bei dem Ereignis aus, um alle Jobs innerhalb dieses Ereignisses zusammen zu löschen.

Tipp:

Sie können jeden Job innerhalb eines Ereignisses löschen, anlegen oder bearbeiten. Das Ereignis selber wird vom System vorgegeben und kann nicht gelöscht werden.

Gegenereignissen Jobs zuweisen

Einige Jobs müssen explizit wieder zurückgenommen werden, sobald ein gegenläufiges Ereignis eintrifft:

- Information von Verantwortlichen / „Entwarnungen“
- Weiterführende Aktionen
- Angestoßene Servershutdowns
- ...

Die Konfiguration eines Gegenjobs erfolgt nach demselben Schema wie das Erstellen eines Jobs. Wichtig ist in diesem Zusammenhang das oben beschriebene Zeitmanagement, da die USV im autonomen Modus war und eine gewisse Zeit benötigt, um die Batterien aufzuladen.

Beispielszenario:

Die USV hat durch einen Stromausfall in den autonomen Modus geschaltet und kann bei 100% Last 60 Minuten alle angeschlossenen Geräte halten. Bei 30 Minuten Restlaufzeit werden viele Computer automatisch heruntergefahren, wodurch sich die Last auf 20% verringert. Die Restlaufzeit wird entsprechend nach oben korrigiert. Da erst bei 5 Minuten Restlaufzeit alle Systeme heruntergefahren werden, jedoch der Stromausfall bei 6 Minuten beseitigt wurde, stellt sich die Normalität ein.

Der CS141 kann in diesem Fall via Wake on LAN (WOL) alle zum Schutz der Restlaufzeit heruntergefahrenen Computer wieder starten – eine Tatsache, die absolut gewünscht ist.

Würde man in diesem Szenario sofort alle angeschlossenen Computer wieder automatisch starten, bedeutet das rechnerisch, dass die USV mit 20% Last 6 Minuten beim nächsten Stromausfall durchhalten könnte – allerdings 100% Last liefern muss. Da das nicht funktionieren kann, muss das WOL-Paket zeitlich verzögert abgesetzt werden, um der USV die Möglichkeit zu geben, eine Mindestladung der Batterien durchzuführen.

Tipp:

Es können bis zu 50 Jobs pro Systemereignis angelegt werden. Beachten Sie in diesem Zusammenhang, dass sich hier einzelne Jobs durchaus widersprechen bzw. gewünschte Jobs mit Gegenjobs rückgängig gemacht werden können.

Custom Thresholds

Für diesen Konfigurationsschritt benötigen Sie folgendes Menü:



Manche USV-Modelle erlauben Ihnen, die Grenzwerte für einige USV-spezifische Ereignisse selbst individuell festzulegen.

Der CS141 unterstützt diese Funktionen, wenn die USV diese Option zur Verfügung stellt. Sollte dies nicht der Fall sein, werden Sie über eine entsprechende Systemnachricht informiert.

Die Konfiguration erfolgt über zwei unterschiedliche Menüs:

- In den Custom Thresholds definieren Sie, welche Messwerte ausgelesen werden, und
- Unter USV > Ereignisse weisen Sie zu den Ereignissen entsprechend Jobs zu

Warning Levels				
		Min		Max
<input type="checkbox"/> Battery Voltage	out of range	<input type="text" value="0"/>	V	<input type="text" value="0"/>
<input type="checkbox"/> Input voltage P-N	out of range	<input type="text" value="0"/>	V	<input type="text" value="0"/>
<input type="checkbox"/> UPS Temperature	out of range	<input type="text" value="0"/>	°C	<input type="text" value="0"/>
<input type="checkbox"/> UPS Autonomy	less than	<input type="text" value="0"/>	m	
<input type="checkbox"/> Battery Charge	less than	<input type="text" value="0"/>	%	
<input type="checkbox"/> Output Load	less than	<input type="text" value="0"/>	%	
<input type="checkbox"/> Seconds on Battery	greater than	<input type="text" value="0"/>	s	

Unterschied zwischen Warning und Alarm Levels

Die Custom Thresholds sind für Warning und Alarm Levels identisch – Sie werden jedoch in den USV-Ereignissen getrennt aufgeführt und können unterschiedliche Werte enthalten und werden in den Logdateien als Warning bzw. Alarm aufgelistet. Das ist notwendig, um sowohl das Warn- als auch das Alarmverhalten unterschiedlich konfigurieren zu können.

Folgende Bedingungen können erfüllt werden:

- out of range* Das Ereignis – unabhängig ob Alarm oder Warnung – wird ausgelöst, wenn der Messwert die eingetragenen Werte unter- bzw. überschreitet.
- less than* Das Ereignis – unabhängig ob Alarm oder Warnung – wird ausgelöst, wenn der Messwert den eingetragenen Wert unterschreitet.
- greater than* Das Ereignis – unabhängig ob Alarm oder Warnung – wird ausgelöst, wenn der Messwert den eingetragenen Wert übersteigt.

Beispielkonfiguration: UPS Temperature:

Alle elektrischen Geräte haben eine minimale und eine maximale Temperatur, innerhalb der sie gefahrlos betrieben werden dürfen. Werden diese Temperaturen unter- bzw. überschritten, kann von einfachen Defekten bis hin zur akuten Brandgefahr alles passieren. Um rechtzeitig eingreifen zu können, muss demnach ein vorgegebener Temperaturwert mit den gemessenen Temperaturen verglichen werden:

Wird zum Beispiel die „sichere Betriebstemperatur“ vom Hersteller zwischen +5°C und +39°C angegeben, könnte auf diese Weise sowohl ab +5°C als auch ab +39°C eine Warnung ausgegeben werden:

Durch die Bedingung *out of range* wird zunächst definiert, was außerhalb dieses Bereichs liegt.

Die Konfiguration erfolgt in zwei separaten Menüs:

- Custom Thresholds:

Die erste Einstellung wird unter Custom Thresholds vorgenommen, wo die entsprechenden Werte festgelegt werden.

Warning Levels					
		Min		Max	
<input type="checkbox"/> Battery Voltage	out of range	<input type="text" value="0"/>	V	<input type="text" value="0"/>	V
<input type="checkbox"/> Input voltage P-N	out of range	<input type="text" value="0"/>	V	<input type="text" value="0"/>	V
<input checked="" type="checkbox"/> UPS Temperature	out of range	<input type="text" value="10"/>	°C	<input type="text" value="34"/>	°C
<input type="checkbox"/> UPS Autonomy	less than	<input type="text" value="0"/>	m		

Aktivieren Sie die Check-Box, um diesen Eintrag in die USV-Ereignisse einzubeziehen. Bei dem Argument *out of range* geben Sie bei *Min* die niedrigste und bei *Max* die höchste Zulässige Temperatur ein.

Tipp:

Da es sich hierbei um die Warnung handelt, sollte diese vor dem Erreichen der kritischen Werte abgesetzt werden, die in diesem Fall bei +5°C bzw. +39°C liegen. Deshalb müssen die Werte entsprechend korrigiert werden. In diesem Beispiel wurde die Warnung mit +10°C und +34°C jeweils um 5°C korrigiert.

Mit *Übernehmen* speichern Sie die Konfiguration.

- USV-Ereignisse

Suchen Sie in den USV-Ereignissen die notwendigen Einträge. Anders als im *Custom Thresholds* Menü werden die einzelnen Thresholds wie reguläre Systemereignisse angezeigt, um alle Zustände abbilden zu können:

>	<input type="checkbox"/>	+	🗑️	UPS Temperature Threshold Warning Low On	1	1	0	0	0
>	<input type="checkbox"/>	+	🗑️	UPS Temperature Threshold Warning Low Off	1	1	0	0	0
>	<input type="checkbox"/>	+	🗑️	UPS Temperature Threshold Warning High On	1	1	0	0	0
>	<input type="checkbox"/>	+	🗑️	UPS Temperature Threshold Warning High Off	1	1	0	0	0

Da die Custom Thresholds wie reguläre USV-Ereignisse konfiguriert werden können, sind sämtliche Jobs verfügbar.

[Einstellen der Alarm Levels](#)

Alarm Levels					
		Min		Max	
<input type="checkbox"/> Battery Voltage	out of range	<input type="text" value="0"/>	V	<input type="text" value="0"/>	V
<input type="checkbox"/> Input voltage P-N	out of range	<input type="text" value="0"/>	V	<input type="text" value="0"/>	V
<input checked="" type="checkbox"/> UPS Temperature	out of range	<input type="text" value="6"/>	°C	<input type="text" value="38"/>	°C
<input type="checkbox"/> UPS Autonomy	less than	<input type="text" value="0"/>	m		

Die Alarm-Levels bilden die Eskalationsstufe der Warning-Levels und werden gesondert in den USV-Ereignissen mit allen 4 möglichen Status angezeigt:

>	<input type="checkbox"/>	+	🗑️	UPS Temperature Threshold Alarm Low On	1	1	0	0	0
>	<input type="checkbox"/>	+	🗑️	UPS Temperature Threshold Alarm Low Off	1	1	0	0	0
>	<input type="checkbox"/>	+	🗑️	UPS Temperature Threshold Alarm High On	1	1	0	0	0
>	<input type="checkbox"/>	+	🗑️	UPS Temperature Threshold Alarm High Off	1	1	0	0	0

Da die Alarmlevel eine Eskalationsstufe darstellen und ggfs. Notfallmaßnahmen auslösen sollen, müssen die Werte entsprechend angepasst werden. Da die Bedingung für einen Alarm zusätzlich zu der Warnung erfüllt ist, können sich unglücklich konfigurierte Jobs ggfs. parallel ausgeführt werden, sich überschneiden oder sogar widersprechen bzw. gegenseitig aufheben.

Exemplarischer Auszug: Custom Thresholds

Diese Liste stellt ein Beispiel dar, je nach USV-Modell und Hersteller kann diese Liste sowohl in der Bezeichnung als auch im Funktionsumfang variieren. Die hier dargestellte Beispielliste stammt von einer XANTO 2000R des Herstellers Online:

		Min		Max	
<input type="checkbox"/> Battery Voltage	out of range	0	V	0	V
<input type="checkbox"/> Input voltage P-N	out of range	0	V	0	V
<input type="checkbox"/> UPS Temperature	out of range	0	°C	0	°C
<input type="checkbox"/> UPS Autonomy	less than	0	m		
<input type="checkbox"/> Battery Charge	less than	0	%		
<input type="checkbox"/> Output Load	less than	0	%		
<input type="checkbox"/> Battery Symmetry Pos./Neg.	greater than	0	V		
<input type="checkbox"/> Seconds on Battery	greater than	0	s		

Battery Voltage *out of range* XX V – XX V

Batterien reagieren empfindlich auf Spannungen, zu hohe Spannungen und Tiefentladungen können sie dauerhaft beschädigen. Über diesen Wert kann rechtzeitig vor derartigen Ereignissen gewarnt werden, sobald der eingegebene Bereich in Volt verlassen wird.

Input voltage P-N *out of range* XX V – XX V

Einige USV-Anlagen bieten auf Wunsch die Messdaten der Eingangsspannung an. Über diesen Wert kann ein Alarmverhalten bei Spannungseinbrüchen oder Überspannung im Stromnetz realisiert werden.

UPS Temperature *out of range* XX°C – XX °C

Einige USV-Anlagen haben interne Temperaturfühler. Über diesen Wert kann ein zusätzliches Alarmverhalten definiert werden basierend aus den Temperaturwerten, welche die USV in dem Fall liefert.

UPS Autonomy *less than* XX m

In einigen Fällen kann es sinnvoll sein, über die Zeit, die eine USV im autonomen Modus in Minuten zur Verfügung hat, ein zusätzliches Alarmverhalten zu definieren – etwa, wenn Jobs mit einer vorwärtslaufenden Zeitverzögerung versehen sind, und durch mehrere kurze Stromausfälle in Folge nicht genug Zeit zur Verfügung steht: Es könnte ein Notfallverhalten definiert werden, zum Beispiel eine Alarmabschaltung.

Battery Charge *less than* XX %

Nachdem eine USV im autonomen Betrieb war, werden die Batterien automatisch wieder aufgeladen. Wenn zum Beispiel mehrere kurze Stromausfälle in Folge waren, kann über diesen Wert ein zusätzliches Frühwarnverhalten definiert werden.

Output Load *less than* XX %

einige USV-Anlagen bieten einen Messwert an, bei dem die tatsächlich angelegte Last in Echtzeit angezeigt wird. Wenn im Autonomiefall nicht relevante Systeme heruntergefahren werden, könnte über diesen Wert ein Bestätigungs- oder Hinweisverhalten realisiert werden.

Battery Symmetry Pos./Neg. *greater than*

Einige USV-Anlagen nutzen bei Wechselstrom sowohl die positive als auch die negative Halbwelle aus. Diese Einstellung definiert das Alarmverhalten, wenn der positive Batteriestrang und der Negative Batteriestrang nicht gleichmäßig geladen werden.

Seconds on Battery *greater than* XX s

In manchen Fällen wird lediglich ein Spannungseinbruch verzeichnet, etwa, wenn große Industrieanlagen in Betrieb genommen werden. Dabei kann es vorkommen, dass eine USV in den autonomen Modus springt. Über diesen Wert in Sekunden könnte eine zusätzliche Warnung realisiert werden, die den „echten Autonomiefall“ verifiziert.

Tipp:

Beachten Sie genau die Argumente, die mit den Thresholds verknüpft sind:

Greater than, less than, in range, out of range – da Argumente werden wörtlich als Bedingung genommen werden, wird das Warn- und Alarmverhalten auch entsprechend interpretiert. So wird zum Beispiel bei Output Load less than 67% auch eine Warnung ausgegeben, wenn der Wert auf 43% fällt, während bei 68% entsprechend keine Warnung ausgegeben wird.

Beispielszenario: Custom ThresholdsDas Problem:

Der SITEMANAGER 7 erkennt zwar die USV erkennt korrekt, jedoch sollen in Abhängigkeit zueinander über potentialfreie Kontakte Schütze angesteuert werden, welche externe Geräte abschalten, sobald die Ladung der Batterien unter einen gewissen Wert in Prozent fallen.

Diese Konfiguration ist möglich, jedoch nur indirekt:

Wenn ein CON_R_AUX4 angeschlossen ist, können die potentialfreien Ausgänge benutzt werden, um die Schütze anzusteuern – Sie können durchschalten (ON) und blockieren (OFF). Damit ist die Ansteuerung der Schütze relativ einfach zu realisieren.

Schwierig wird es, wenn die USV derartige Events nicht hergibt:

Diese werden in der Konsequenz dann auch nicht unter Geräte/Anlagen>USV>Ereignisse angezeigt. Eine Möglichkeit, die Konfiguration dennoch zu realisieren finden Sie im USV-Menü im Punkt *Custom Thresholds*:

Der entscheidende Punkt ist, dass diese Funktion einen frei definierbaren Job als USV-Ereignis abbildet:

Wenn Sie hier bei Warning Levels 71% und bei Alarm Levels 61% einstellen, können Sie hinterher in den USV-Ereignissen ein entsprechendes Verhalten zuordnen:

- Wenn in diesem Fall die Battery charge auf 70% fällt, werden die ersten Geräte ausgeschaltet.
- Wenn die Battery charge auf 60% fällt, werden die nächsten Geräte ausgeschaltet.

Die Gegenevents werden dann entsprechend auf Warning OFF bzw. Alarm Off gelegt.

Da die Batterien ja geladen werden, werden die Geräte über den Wert der Battery Charge gestartet:

- > Ab 61% werden die Geräte wieder zugeschaltet,
- > Ab 71% die zweiten Geräte wieder zugeschaltet

Da es keine UND-Verknüpfung zum Power Fail gibt, werden diese Events je nach Einstellung sooft wiederholt, bis der eingestellte Wert in Prozent erreicht ist, oder einmalig ausgeführt. Sollten also Geräte bei 70% abgeschaltet und bei 61% angeschaltet werden, könnte es hier zu Konflikten zwischen den Events kommen, die Geräte sollten also konsequent auf einen Wert konfiguriert werden.

Sollte zwischen 0% und 71% ein weiterer Power Fail eintreffen, würden die Geräte demnach entweder aus bleiben oder kurze Zeit später wieder ausgeschaltet werden.

Weitere Geräte könnten dann unabhängig als Job über die Restlaufzeit über die Ereignisse *Power Fail* und *Power Restored* getriggert werden:

Da die Restlaufzeit sich dynamisch der Last anpasst, würden diese Geräte erst dann ausgeschaltet werden, sobald diese tatsächlich den Wert X in Minuten erreicht hat. Bei *Power restored* wird dann das entsprechende Gegenevent konfiguriert.

Warning Levels			
		Min	Max
<input type="checkbox"/> Battery Voltage	out of range	0 V	0 V
<input type="checkbox"/> Input voltage P-N	out of range	0 V	0 V
<input type="checkbox"/> UPS Temperature	out of range	0 °C	0 °C
<input type="checkbox"/> UPS Autonomy	less than	0 m	
<input checked="" type="checkbox"/> Battery Charge	less than	0 %	
<input type="checkbox"/> Output Load	less than	0 %	
<input type="checkbox"/> Battery Symmetry Pos./Neg.	greater than	0 V	
<input type="checkbox"/> Seconds on Battery	greater than	0 s	

Alarm Levels			
		Min	Max
<input type="checkbox"/> Battery Voltage	out of range	0 V	0 V
<input type="checkbox"/> Input voltage P-N	out of range	0 V	0 V
<input type="checkbox"/> UPS Temperature	out of range	0 °C	0 °C
<input type="checkbox"/> UPS Autonomy	less than	0 m	
<input checked="" type="checkbox"/> Battery Charge	less than	0 %	
<input type="checkbox"/> Output Load	less than	0 %	
<input type="checkbox"/> Battery Symmetry Pos./Neg.	greater than	0 V	
<input type="checkbox"/> Seconds on Battery	greater than	0 s	

Übernehmen Abbrechen

Tipp:

Eine Beschreibung des CON_R_AUX4 finden Sie im Kapitel *Sensoren und Geräte*

RCCMD

Was ist RCCMD

RCCMD (Remote Console Command) ist der weltweit erfolgreichste Shutdown-Client für heterogene Netzwerke und ist der sicherste Weg, vielfältige Meldungen und Shutdown-Sequenzen aus der USV einzuleiten. Die RCCMD Clients lauschen hierbei auf Port 6003 nach einen RCCMD Server, der im Allgemeinen Bestandteil einer UPSMAN-Software, einem CS141 oder RCCMD-lizenzierte USV-Manager

Ein RCCMD Server steuert die im Netzwerk befindlichen RCCMD Clients im Falle eines USV-Alarms an. Der Funktionsumfang geht von Hinweisen und Benachrichtigungen bis hin zu einem geordneten Shutdown einer multiplen Serverumgebung, bei der gegenseitige Abhängigkeiten berücksichtigt werden müssen.

Tipp:

Der RCCMD-Client ist keine Freeware, es wird eine separate Lizenz benötigt, welche Sie weltweit bei lizenzierten Resellern, OEM-Partnern oder über den Webshop auf www.generex.de beziehen können. Die Lizenz selber ist dabei unbegrenzt gültig, im Serviceumfang enthalten sind 2 Jahre kostenlose Updates ab Kaufdatum.

Konfiguration von RCCMD

Auf dem RCCMD Server werden RCCMD- Kommandos über die Systemereignisse als Jobs definiert. Dabei stehen drei unterschiedliche Kategorien als Job zur Verfügung:

RCCMD Shutdown

Der RCCMD – Shutdown sendet an einen RCCMD-Client ein Signal, das den Client veranlasst, den Computer entsprechend seiner Konfiguration geordnet herunterzufahren.

RCCMD Message

Eine RCCMD-Message ist ein Hinweistext, welcher an ein RCCMD Empfänger gesendet werden kann und dort über eine Message Box auf dem Bildschirm angezeigt wird.

RCCMD Execute

Sollten Skripte im Vorfeld zu einem Shutdown ausgeführt werden müssen, können diese über einen Execute ausgeführt werden. Dabei bietet RCCMD neben vorgefertigten-Kommandos die Möglichkeit, eigene Skripte zu starten.

RCCMD Trap

Trapnachrichten sind reine Informationsmeldungen, welche an einen RCCMD-Client gesendet werden können. Der Client empfängt diese Textnachrichten und zeigt sie in einer Message Box an.

Tipp:

Ein angestoßener RCCMD Shutdown kann nicht wieder zurückgenommen werden. Sie können jedoch innerhalb des RCCMD-Clients auch sog. Redundanzen definieren und IP-Adressen eingrenzen, welche berechtigt sind, einen RCCMD Shutdown zu senden.

Einstellen eines RCCMD-Jobs

RCCMD funktioniert auf der Basis der IP-Adressen, um Geräte innerhalb eines Netzwerks oder Netzwerksegments anzusteuern.

Während einige Parameter für alle RCCMD-Jobs gültig sind, gibt es je nach Job einige Unterschiede in den Parametern.

- Sende Signal als Broadcast (UDP)
- IP-Adresse des Clients
- Der verwendete Port

- Timing des Jobs

Einstellen der IP-Adresse für RCCMD

Broadcast

Wenn Sie diese Checkbox aktivieren, wird ein sog. Broadcast in Ihr Netzwerksegment gesendet. Jeder RCCMD-Client, der in diesem Netzwerksegment installiert ist, wird hierbei angesprochen und reagiert mit dem Herunterfahren und Ausschalten des Computers. Dabei wird nicht zwischen Host, virtueller Maschine, Einzelservers oder Arbeitsstation unterschieden.

Eingrenzen auf IP-Adressen

Wenn Sie eine bestimmte Maschine innerhalb Ihres Netzwerks ansprechen möchten, geben Sie hier die direkte IP-Adresse an. Dabei wird ausschließlich der angesprochene Computer – egal ob physikalisch oder als virtuelle Maschine – angesprochen. Dabei können Sie für jeden RCCMD-Client einen einzelnen Job anlegen oder mehrere IP-Adressen mit einem Job zusammenfassen:

... ein Job pro IP-Adresse ...

... mehrere IP-Adressen mit einem Sammeljob

Bei mehreren IP-Adressen beachten Sie bitte genau die Syntax: 192.168.3.1,192.168.3.18 ...

Es dürfen keine Leerzeichen zwischen den einzelnen Einträgen und dem Komma sein, ansonsten erhalten Sie einen entsprechenden Fehlerhinweis.

Tipp:

Broadcast und einzelne IP-Adressen bzw. Sammeladressen schließen sich einander aus. Wenn Sie zuerst Geräte und Gerätegruppen herunterfahren möchten, und danach einen Broadcast senden, legen Sie einen weiteren Job mit einer entsprechenden Verzögerung an.

Port

Der Standard-Port für RCCMD-Kommandos ist der Port 6003 – der RCCMD-Client lauscht auf diesem Port nach einem RCCMD-Kommando. Wenn Ihr RCCMD-Client bei der Installation und Konfiguration einen anderen Port zugewiesen wurde, gleichen Sie bitte die Daten an, damit Sender und Empfänger sich auf demselben Port befinden.

Parameter	
IP	<input type="checkbox"/> Broadcast <input type="text" value="192.168.3.1"/>
Port	<input type="text" value="6003"/>

[Zeitpunkt für RCCMD definieren](#)

Bestimmen Sie unter Zeitpunkt das Timing des Jobs. Dabei steht zur Auswahl:

Zeitpunkt	
<input checked="" type="radio"/>	Sofort, einmalige Ausführung
<input type="radio"/>	Nach <input type="text" value="1"/> Sekunden
<input type="radio"/>	Nach <input type="text"/> Sekunden, wiederhole alle <input type="text"/> Sekunden
<input type="radio"/>	Nach <input type="text"/> Sekunden auf Batterie
<input type="radio"/>	Bei <input type="text"/> Sekunden Restlaufzeit

- *Sofort, einmalige Ausführung*

Der Job unmittelbar ausgeführt, wenn das Ereignis vorliegt.

- *Nach XXX Sekunden*

Der CS141 wartet eine voreingestellte Zeit, bevor er den Job ausführt. Ändern sich die Gegebenheiten und der Job wäre dann obsolet, wird dieser auch nicht mehr ausgeführt

- *Nach XXX Sekunden, wiederhole alle XXX Sekunden*

Der Job wird nach einer voreingestellten Zeit gestartet und dann zyklisch wiederholt, bis das Ereignis nicht mehr ansteht oder die Gegebenheiten das Ausführen unmöglich machen –wenn zum Beispiel die USV-Batterien erschöpft sind und die USV sich selbst ausgeschaltet hat, um eine Tiefentladung zu verhindern.

- *Nach XXX Sekunden auf Batterie*

Der Job wird nur ausgeführt, wenn die USV einen voreingestellten Wert in Sekunden im autonomen Modus auf Batterie läuft.

- *Bei XXX Sekunden Restlaufzeit*

Der CS141 führt diesen Job nur aus, wenn die allgemeine Restlaufzeit einen bestimmten Wert in Sekunden erreicht hat. Da der Wert sich mit real angehängten Last verschieben kann, ist es möglich, dass diese Kondition mehrfach erreicht werden kann. Dies geschieht zum Beispiel, wenn zum Beispiel durch das Herunterfahren einer Maschine die allgemeine Last sinkt und die Restlaufzeit wieder oberhalb des eingestellten Wertes liegt.

Die RCCMD-Kommandos

Der RCCMD Shutdown

Parameter	
IP	<input type="checkbox"/> Broadcast 192.168.3.1
Port	6003

Der RCCMD- Shutdown ist vordefiniert und veranlasst, dass der angesprochene RCCMD Client das Betriebssystem herunterfährt und das Gerät ausschaltet.

Die RCCMD Message

Parameter	
Text	Am Brunnen, vor dem Tore, da steht ein...
IP	<input type="checkbox"/> Broadcast 192.168.3.15
Port	6003

Die RCCMD Message ist eine Textnachricht, die Sie frei definieren können. Das Textfeld verschiebt sich automatisch mit den eingegebenen Texten, sobald Sie an den rechten Rand gelangen. Diese Nachricht wird anschließend als Hinweis auf einem Computer mit installiertem RCCMD-Client in einer Alarmbox erscheinen. RCCMD gibt zudem auf der Taskleiste ein Feld mit Warnhinweis wieder.

Konfiguration eines RCCMD Executes

Parameter	
IP	<input type="checkbox"/> Broadcast 192.168.3.1
Port	6003
Command	hallowelt.bat

Eine umfangreiche Funktion innerhalb von RCCMD ist, dass Sie direkt eigene ausführbare Dateien und Batchfiles auf einem Ziel-Gerät ausführen können. Diese Funktion ist nützlich, wenn zum Beispiel noch Skripte vor einem Shutdown durchlaufen müssen. Legen Sie hierzu die auszuführende Datei im Client im Verzeichnis von RCCMD ab. Im Anschluss können Sie als RCCMD Execute die Datei direkt benennen, die ausgeführt werden soll.

Tipp:

Im Screenshot sehen Sie, dass unter Command hallowelt.bat eingetragen wurde. In diesem Fall würde der RCCMD – Client auf dem PC mit der IP-Adresse 192.168.3.1 versuchen, die Datei hallowelt.bat direkt zu starten.

Die RCCMD Traps

RCCMD Traps sind reine Nachrichten, welche über den aktuellen Zustand der USV informieren sollen. Dabei wird ein spezielles Datenpaket generiert, welches von dem entsprechenden Programm empfangen, ausgelesen und interpretiert werden kann.

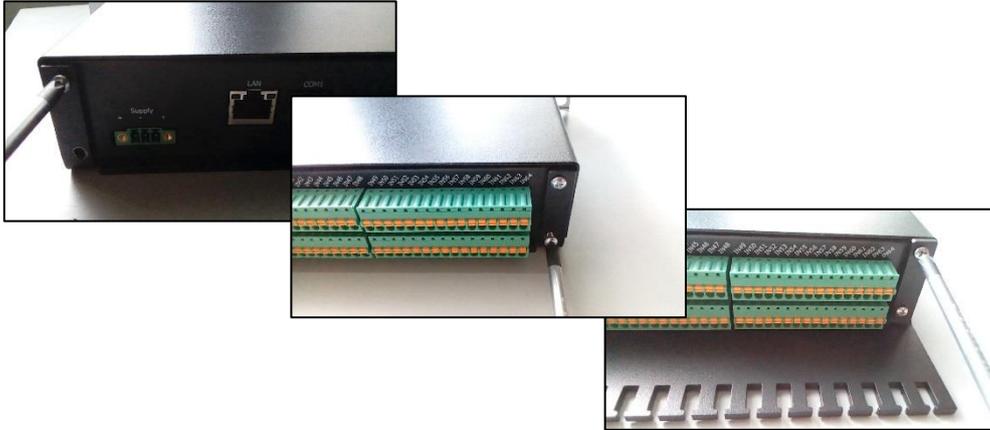
Die folgende Liste enthält mögliche Variablen, die sie zur Definition von RCCMD-Traps verwenden können:

#AGENTSOFTRREV	CS141 Firmware Version
#AUTONOMTIME	Autonomiezeit in Minuten
#BATT2OLD()	Zeit in Monate bis zum Event „Please check batteries“
#BATT2OLD_YEARS	Batteriealter Jahre
#BATTCAP	Batterie Kapazität in %
#BATTINSTDATE	Installationsdatum der Batterie
#BATTTESTDATE	Datum vom letzten Batterietest
#BATTVOLT	Batterie Spannung in V
#CHARGECURR	aktueller Ladestrom
#CNT_BL	Counter Battery Low
#CNT_PF	Counter Powerfail
#CNT_SA	Counter Active Shutdowns
#CNT_SD	Counter Shutdowns
#CNT_TF	Counter Testfehler
#DATE	aktuelles Datum
#EVENTSTATE	obstatus (idle, error, progress, success)
#FULLTESTDATE	Datum des letzten Fulltests
#GETLASTRESULT()	Ergebnisse vom letzten durchgeführten Test
#HOLDTIME	Laufzeit bei 100 Prozent Last
#IDENT_NAME	Name des SNMP Adapters
#INCURR0/1/2	Eingangstrom in V
#INFREQ0/1/2	Eingangsfrequenz in Hz
#INPHASES	Anzahl Eingangsphasen
#INPUTCURRENT0/1/2	aktuelle Eingangstrom in V
#INVOLT0/1/2	Eingangsspannung in V
#LASTERR	Letzter Fehler
#LOAD	aktuelle Last
#LOCATION	Standort
#MANUFACTURER	Hersteller der UPS
#MODEL	UPS Modell
#OUTFREQ0/1/2	Ausgangsfrequenz in Hz
#OUTPHASES	Anzahl Ausgangsphasen
#OUTPOWER0/1/2	Last in Prozent
#OUTPUT_VOLT0/1/2	
#OUTPUTCURRENT0/1/2	
#OVERLOAD	Überlast
#PHASES	Phasen
#POWER	Leistung
#RECHARGETIME	Zeit bis zur vollständigen Aufladung
#RESTORETIME	Wiederherstellungszeit
#RUNTIME	Laufzeit seit letzter Inbetriebnahme
#SECONBAT()	Sekunden auf Batteriebetrieb
#SELFTESTDATE	Datum des letzten Selbsttests
#SERVER	IP des SNMP Adapters
#STATUS	Systemstatus
#SYSDATE()	Systemdatum
#SYSTEMTIME()	Systemzeit
#TEMPDEG	Temperatur in °Celsius
#TIMEZONE	Zeitzone
#VOLTAVAI	USV bezogen, // USV hat eine Möglichkeit, die Inputvoltage abzufragen

SITEMANAGER 7 - spezifische Geräte und Sensoren

Der Kabelkamm

Auf der Rückseite des Geräts befinden sich 4 Schrauben – diese halten den Kabelkamm in der Lieferposition fest:



Tipp

Wenn Sie die Hold Funktion nicht aktiviert haben, und einen aktuellen Alarm mit ACK bestätigen, wird der dieses Alarmverhalten ebenfalls ausgelöst und der Zustand entsprechend gehalten

Der Unterschied ist, dass ohne die Hold-Funktion der Alarm optional bestätigt werden kann, wogegen der Alarm mit aktiver Hold-Funktion bestätigt werden muss.

Sensoren und Geräte

Der SITEMANAGER 7 verfügt über 8 analoge und 8 Digitale Eingänge, die wahlweise über reguläre Stecker oder über die Klemmleiste bedient werden können.

Hierbei ist zu beachten, dass Sie entweder vorkonfektionierte Kabel mit den entsprechenden analogen Sensoren verwenden oder die Anschlüsse über die Klemmleiste verwenden:



Dabei ist folgendes zu beachten:

AN 1 und AN 2	Sensor Input 1
AN 3 und AN 4	Sensor Input 2
AN 5 und AN 6	Sensor Input 3
AN 7 und AN 8	Sensor Input 4

Sie können also einen analogen Standalone Sensor über das Kabel an *Sensor Input 1* anschließen, besteht die Möglichkeit, und einen weiteren Sensor über die Klemmleiste an AN 2 zu befestigen. Wenn Sie zwei Sensoren an Sensor Input 1 anschließen, sind die beiden Anschlüsse AN1 und AN2 dem entsprechend belegt.

Hinzu kommen noch bis zu 8 digitale Inputs, welche über die Klemmleiste angeschlossen werden können:

Die untere Klemmleiste bietet über die Plus- und Minuspole eine 12 V Stromversorgung an, welche ähnlich wie der SITEMONITOR zu bedienen sind:

Möchten Sie den digitalen Input direkt mit einem externen Schalter oder Relais nutzen, wählen Sie den Minuspol als Bezugsquelle, um am Eingang einen entsprechendes High-Signal zu provozieren. Sollten Sie externe Sensoren oder Schaltgeräte zusätzlich mit einer Stromversorgung ausrüsten können Sie die notwendige Stromversorgung über die untere Klemmleiste abgreifen und dann den digitalen Kontakt auf den entsprechenden digitalen Eingang auflegen.

Der SITEMANAGER bietet zwar weniger digitale Eingänge als der SITEMONITOR, kann jedoch dafür 8 analoge Sensoren verwalten und verfügt über 8 bereits vorintegrierte Relais, um Ausgänge aktiv schalten zu können.

Konfiguration der Sensoren im SITEMANAGER 7

Für diesen Konfigurationsschritt benötigen Sie die folgenden Menüs:

<ul style="list-style-type: none"> 🏠 USV Monitor 🏠 Sensor Monitor — Geräte ⚙️ Konfiguration ➤ USV — Sensors ⚙️ Konfiguration ⚙️ Matrix 🔔 Ereignisse 	<ul style="list-style-type: none"> ➔ Allgemeine COM-Port Einstellungen ➔ Einstellung der Sensoren ➔ Sensorergebnisse logisch verknüpfen ➔ Einstellmenü für System- und Sensoreignisse
--	--

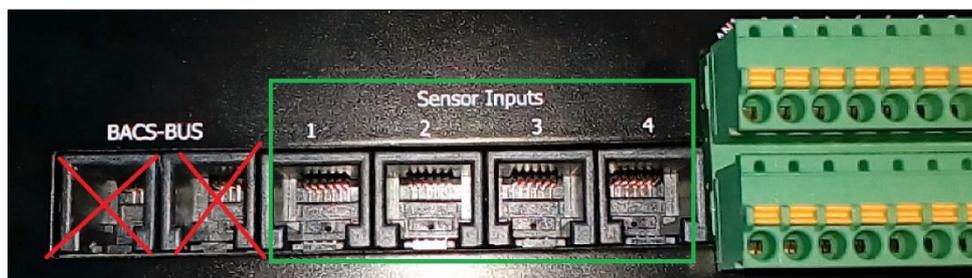
Eine signifikante Abweichung zum CS141 mit seinen optionalen Modulen bietet der SITEMANAGER 7. Anschlussbedingt ist die USV-Schnittstelle COM1 ein MINI-DIN – Anschluss, der serielle 9-polige SUB-D -Anschluss wird intern anderweitig verwendet, um die zusätzliche Funktionalität abzubilden.

Sensoren sind für den SITEMANAGER 7 wichtig, da sie über die Umgebung zahlreiche Informationen liefern, welche für den Betrieb von Anlagen relevant sein können. Darunter fallen unter anderem Luftfeuchtigkeit, Luftdruck, Temperaturen, etc. Wenn Anlagen außerhalb der regulären Betriebsumgebungen betrieben werden, können diese beschädigt oder im schlimmsten Fall zerstört werden.

Einer der Besonderheiten des SITEMANAGER 7 ist die Möglichkeit, bis zu 8 Sensoren, analoge und digitale Eingänge zu verwalten und mit spezifischen Systemereignissen zu belegen. Weiterhin bietet der SITEMANAGER 7 als einziges Gerät aus der CS141- Familie 4 Output Relais, um externe Systeme zu schalten oder Schaltzustände bei Zielgeräten zu definieren.

Anschluss der Sensoren

Der Anschluss der Sensoren erfolgt ähnlich wie bei dem GENEREX Sensormanager - auf der Rückseite des SITEMANAGER II/V6 finden Sie die entsprechenden Anschlüsse links von der Klemmleiste mit den analogen und digitalen Eingängen.



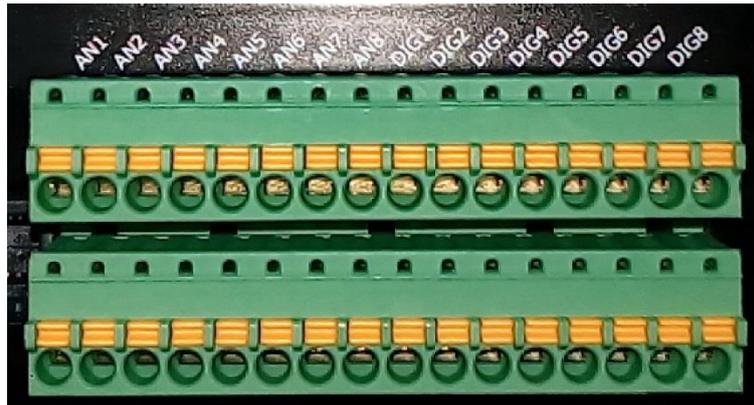
Verwechseln Sie beim Anschluss der Sensoren nicht die Sensor Inputs mit den Eingangsbuchsen des BACS-BUS – die Stecker der Sensorkabel sind anders konfektioniert und können daher die BACS – Bus – Buchsen mechanisch beschädigen

Insgesamt können Sie bis zu 8 Sensoren anschließen – dabei ist jedem Sensor Input 2 Kanäle zugeordnet. Grundsätzlich kann man zwischen zwei unterschiedlichen Sensoren unterscheiden:

- Der Single Sensor
Dieser Sensor bietet die Möglichkeit, einen zweiten Sensor in Reihe anzuschließen.
- Der Kombi-Sensor
Dieser Sensor besteht aus zwei unterschiedlichen Sensoren, welche zusammen in einem Gehäuse untergebracht sind. In diesem Fall werden beide Kanäle an einem Sensor Input für den Sensor belegt.

Bitte beachten Sie beim Anschluss, dass Sie die richtigen Sensoren in Reihe anschließen, da Ihnen ansonsten in der Konfiguration ein Sensor fehlen könnte.

Verwendung der analogen und digitalen Anschlüsse



Wenn Sie eigene Sensoren direkt anklennen möchten, bietet Ihnen der SITEMANAGER II/V6 die Möglichkeit, Klemmleiste zu benutzen. Dabei wird folgender Schlüssel verwendet:

- AN1 / AN2 Sensor Input 1
- AN3 / AN4 Sensor Input 2
- AN5 / AN6 Sensor Input 3
- AN7 AN8 Sensor Input 4

Die entsprechende Betriebsspannung oder die Bezugspunkte können aus der zweiten Klemmleiste darunter bezogen werden.

Der Konfigurationsbildschirm im SITEMANAGER ist dabei in 3 Teile unterteilt

Analoge Sensoren

Sensor	Standort	Sensortype	Einheit	Alarm (niedrig)	Vor-Alarm (niedrig)	Vor-Alarm (hoch)	Alarm (hoch)	Sensor Bereich	
1	Channel 1	Custom 0-10V		1 <input type="checkbox"/>	2 <input type="checkbox"/>	8 <input type="checkbox"/>	9 <input type="checkbox"/>	0 - 10	
2	Channel 2	Custom 0-10V		1 <input type="checkbox"/>	2 <input type="checkbox"/>	8 <input type="checkbox"/>	9 <input type="checkbox"/>	0 - 10	
3	Channel 3	Custom 0-10V		1 <input type="checkbox"/>	2 <input type="checkbox"/>	8 <input type="checkbox"/>	9 <input type="checkbox"/>	0 - 10	
4	Channel 4	Custom 0-10V		1 <input type="checkbox"/>	2 <input type="checkbox"/>	8 <input type="checkbox"/>	9 <input type="checkbox"/>	0 - 10	
5	Channel 5	SM_T_H_RevB	°C	1 <input type="checkbox"/>	2 <input type="checkbox"/>	8 <input type="checkbox"/>	9 <input type="checkbox"/>	0 - 100	
6	Channel 6	SM_T_H_RevB	% rel H	1 <input type="checkbox"/>	2 <input type="checkbox"/>	8 <input type="checkbox"/>	9 <input type="checkbox"/>	0 - 100	
7	Channel 7	SM_T_H_RevB	°C	1 <input type="checkbox"/>	2 <input type="checkbox"/>	8 <input type="checkbox"/>	9 <input type="checkbox"/>	0 - 100	
8	Channel 8	SM_T_H_RevB	% rel H	1 <input type="checkbox"/>	2 <input type="checkbox"/>	8 <input type="checkbox"/>	9 <input type="checkbox"/>	0 - 100	
Hysteresis		3							

Übernehmen

Nachdem Sie einen Sensor angeschlossen haben, definieren Sie mit Sensortype die Art des Sensors. Beachten Sie bitte, dass die einzelnen Kanäle in Pärchen nach außen geführt werden.

Die Sensoren 1 und 2 bilden ein Kanalpärrchen, die Sensoren 3 und 4 bilden eins, etc.

Wenn Sie einen Kombisensor bei einem Kanal einstellen, wird der dazugehörige Zwilling automatisch angepasst. Die entsprechende Einheit wird automatisch voreingestellt.

Definition der Alarmschwellenwerte

Die Sensoren bieten mehrere Möglichkeiten, an die Betriebsumgebung angepasst zu werden. Als Beispiel wird in diesem Fall ein Temperatursensor angepasst.

Alarm (niedrig)	Vor-Alarm (niedrig)	Vor-Alarm (hoch)	Alarm (hoch)	Sensor Bereich
1 <input type="checkbox"/>	2 <input type="checkbox"/>	8 <input type="checkbox"/>	9 <input type="checkbox"/>	0 - 100

Sensor Bereich

Der Sensorbereich definiert den Bereich, der gemessen wird. Die 0 definiert dabei 0°C und die 100°C – sollten Sie einen Tiefkühlraum betreiben, müssten Sie den Wert entsprechend nach unten korrigieren, wogegen in einem Generatorraum in der Wüste Temperaturen von bis zu 80°C durchaus ein realistischer Wert sein könnte. In diesem Beispiel soll ein Raum überwacht werden, deren Anlagen zwischen 5°C und 45°C betrieben werden dürfen.

Um die Skala an den realistischen Wert anzupassen, würde man die Skala also von 0°C bis 60°C etwa gestalten. Das sollte reichen.

Voralarm und Alarm

Der Voralarm stellt die Alarminstanz da, bei der erhöhten Wachsamkeit erforderlich ist. – In diesem Bereich kommt es zwar noch nicht zu Problemen, jedoch die Temperatur bedenklich. Alarm ist die Instanz, bei der eine sofortige Reaktion erfolgen sollte, da ansonsten die Anlagen beschädigt werden können.

In diesem Beispiel liegt die untere Grenze für den Betrieb bei 5°C – das wirft zwei interessante Fragen auf:

1. Wie ist die Durchschnittstemperatur im Betrieb
2. Wie sind Temperaturschwankungen durch Betrieb und Umwelteinflüsse zu bewerten.

Ein schlecht belüfteter oder beheizter Raum kann hie im Sommer durchaus die 50°C erreichen, während im Winter Temperaturen im den Gefrierpunkt herrschen. Liegt die allgemeine Temperatur im Durchschnitt bei 15°-20°C, kann man die unteren und oberen Werte sehr gut definieren:

Der Voralarm sollte in der Konsequenz VOR dem eigentlichen Alarm ausgelöst werden. Also bei etwa 10°C - Dort kann später als Ereignis zum Beispiel das Versenden von Emails als Job hinterlegt werden. Der Alarm hingegen wird bei 6°C ausgelöst. Hierbei kann dann zum Beispiel das Herunterfahren der Anlage definiert werden in Zusammenhang mit Alarm- und Hinweismails.

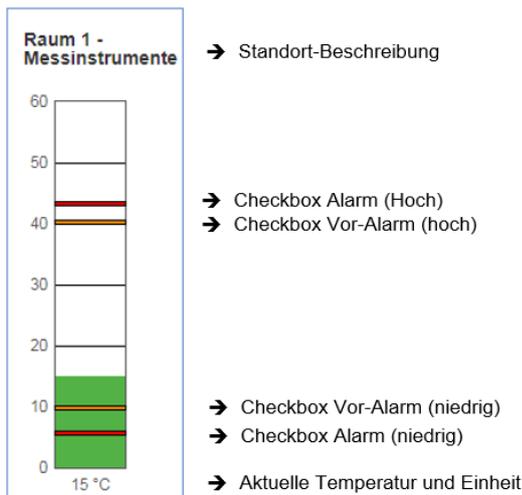
Der obere Bereich wird ähnlich definiert: Der VOR-Alarm wird auf 40°C gelegt, während der Alarm selber bei 43°C ausgelöst wird und entsprechende Notfallmaßnahmen einleitet. Die

Angepasst würde die Temperaturzeile so aussehen:

Sensor	Standort	Sensortype	Einheit	Alarm (niedrig)	Vor-Alarm (niedrig)	Vor-Alarm (hoch)	Alarm (hoch)	Sensor Bereich
1	Raum 1 - Messinstrumente	SM_T_H	°C	6 <input checked="" type="checkbox"/>	10 <input checked="" type="checkbox"/>	40 <input checked="" type="checkbox"/>	43 <input checked="" type="checkbox"/>	0 - 60

Die Checkbox definiert dabei, ob dieser Wert aktiv geschaltet ist oder entsprechend Ignoriert werden soll.

Im Sensor Monitor kann man im Anschluss das Ergebnis sehen:



Die digitalen Inputs

SiteManager Inputs							
Eingang	Name	NC-Kontakt	Aktiv	Eingang	Name	NC-Kontakt	Aktiv
1	<input type="text" value="Input 1"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	5	<input type="text" value="Input 5"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="text" value="Input 2"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	6	<input type="text" value="Input 6"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input type="text" value="Input 3"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	7	<input type="text" value="Input 7"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input type="text" value="Input 4"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	8	<input type="text" value="Input 8"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Die digitalen Inputs werden ähnlich wie die Sensoren konfiguriert.

Folgende Einstellungen sind möglich:

Name

Vergeben Sie im Freitext eine entsprechende eindeutige Bezeichnung für den Eingang. Da die dazugehörigen Systeme in anderen Gebäudeteilen stehen können, achten Sie auf eine eindeutige Benennung.

NC Kontakt

Diese Einstellung definiert, ob ein Kontakt normalerweise geschlossen oder offen sein sollte. Unterschiedliche Sensoren oder Systeme handhaben das sehr unterschiedlich. Da der digitale Input nur high/low-Signale erkennen kann, ist es wichtig zu wissen, welcher Wert den Normalzustand darstellt.

Aktiv

Diese Checkbox aktiviert oder deaktiviert den Kontakt entsprechend Ihrer Angabe.

SiteManager 7 Outputs

Die Outputs bieten die Möglichkeit, aktiv ein Relaiskontakt zu schalten. Diese werden später im Sensor Monitor und auf der Stirnseite des SITEMANAGER 7 bei der LED-Gruppe Digital Outputs angezeigt. In einigen Fällen ist es notwendig, dass beim Start automatisch Relaiskontakte geschaltet sein sollen.

In anderen Fällen müssen die Relaiskontakte zeitverzögert geschaltet werden oder werden über explizite Jobs verwendet.

SiteManager Outputs							
Ausgang	Name	Anschalten	Delay	Ausgang	Name	Anschalten	Delay
1	<input type="text" value="Output 1"/>	<input type="checkbox"/>	<input type="text" value="0"/>	5	<input type="text" value="Output 5"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text" value="Output 2"/>	<input type="checkbox"/>	<input type="text" value="0"/>	6	<input type="text" value="Output 6"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text" value="Output 3"/>	<input type="checkbox"/>	<input type="text" value="0"/>	7	<input type="text" value="Output 7"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text" value="Output 4"/>	<input type="checkbox"/>	<input type="text" value="0"/>	8	<input type="text" value="Output 8"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Name

Vergeben Sie einen eindeutigen Namen, welcher dem Output zugeordnet ist. Dieser wird später im Event Log und im Sensor Monitor angezeigt.

Anschalten

Definieren Sie, ob der SITEMANAGER beim Neustart automatisch diese Outputs schalten soll.

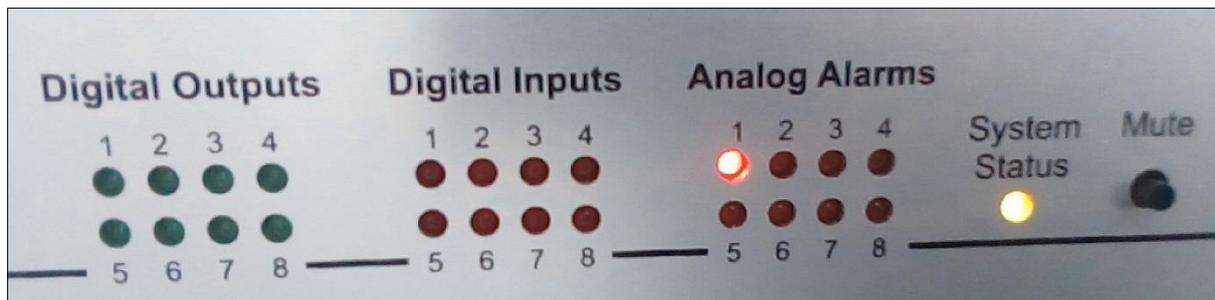
Delay

Definiert die Zeitverzögerung beim Schalten in Sekunden.

Erweitertes Monitoring

Der SITEMANAGER 7 kommuniziert über 2 Wege, Probleme mitzuteilen:

Auf der Frontseite befinden sind Status-LEDs zu allen möglichen Anschlüssen logisch zugeordnet:



Digital Output

LED-Farbe: grün

Diese LEDs leuchten auf, wenn Sie einen digitalen Output geschaltet haben

Digital Input

LED-Farbe: rot

Diese LEDs blinken, wenn ein Problem festgestellt wurde

Das Blinken wird ein statisches Leuchten, sobald im SITEMANAGER II/V6 der Fehler bestätigt wurde

Analog Alarms

LED-Farbe: rot

Diese LEDs blinken, wenn ein Problem festgestellt wurde.

Das Blinken wird ein statisches Leuchten, sobald im SITEMANAGER II/V6 der Fehler bestätigt wurde

Die System Status LEDs

Diese LED ist dem BACS-System zugeordnet, zu dem es ein eigenes Manual gibt.

Besonderheit: Power LED

LED-Farbe: grün

Die Power-LED liefert unterschiedliche Systemzustände:

Die LED...

- Leuchtet statisch grün, wenn das System intern richtig angeschlossen wurde und funktioniert.
- *Blinkt grün, wenn der BOOT-Vorgang eingeleitet wurde oder keine Verbindung zum CS141 besteht.*

Zu den LEDs können Sie den Sensor Monitor-Screen hinzuziehen, um genauere Informationen über die Schaltzustände zu erhalten. Eine schnelle Information bietet nach dem Anmelden die obere Statusleiste:

UPS: ● OK
 Sensor: ● Alarm Analog Input Low in Channel 1
 GX_R_AUX: ●

Sobald Sie im Sensor Monitor die bestätigen, wird sich die LED entsprechend verhalten:

Ack

Der Sensormonitor wird zunächst davon ausgehen, dass dieser Zustand in irgendeiner Weise gewollt ist:

UPS: ● OK
 Sensor: ● OK
 GX_R_AUX: ●

Die LED an der Frontleiste wird jedoch weiterhin statisch rot leuchten, um bei der nächsten Wartung auf einen entsprechenden Fehler hinzuweisen.

SITEMANAGER 7: Sensoren ein Ereignis zuweisen

Für diesen Konfigurationsschritt benötigen Sie die folgenden Menüs:

<ul style="list-style-type: none"> USV Monitor Sensor Monitor Geräte Konfiguration USV Sensors Konfiguration Matrix Ereignisse 	<ul style="list-style-type: none"> → Allgemeine COM-Port Einstellungen → Einstellung der Sensoren → Sensorergebnisse logisch verknüpfen → Einstellmenü für System- und Sensorereignisse
--	--

Für die Notfallmaßnahmen ist die Definition von Ereignissen wichtig. Beachten Sie bitte, dass sich diese Ereignisse auf das Alarm-Verhalten beziehen, nicht aber um die im Monitoring mit auftauchenden Vor-Alarme.

Suchen Sie folgende Events:

[Analogen Inputs Systemereignisse zuweisen](#)

Das Ereignis: Alarm Analog Input 1:

>	+	-	x	Alarm Analog Input 1	1	1	0	0	0	0	0	0	0	0	0	0	0
---	---	---	---	----------------------	---	---	---	---	---	---	---	---	---	---	---	---	---

Diesem Ereignis zugeordnete job bestimmen, was passieren soll, wenn ein Alarmzustand erreicht ist.

Das Gegenereignis: Alarm Analog Input 1 off

>	+	-	x	Alarm Analog Input 1 off	1	1	0	0	0	0	0	0	0	0	0	0	0
---	---	---	---	--------------------------	---	---	---	---	---	---	---	---	---	---	---	---	---

Diesem Ereignis zugeordnete Jobs bestimmen, was passieren soll, wenn der Alarmzustand wieder verlassen wurde.

Klicken Sie auf , um ein allgemeine Übersicht über bereits vorhandenen Jobs zu erhalten it > die Liste konfigurierter Events auf, um die entsprechend vorkonfigurierten Jobs zu sehen.

-	+	-	x	Alarm Analog Input 1	1	1	0	0	0	0	0	0	0	0	0	0	0
				Job Typ	Wann		Parameter										
				Log	Einmal, sofort		{"text":"Alarm Analog Input 1"}										

Mit **+** öffnen Sie den Konfigurationsdialog für die Jobdefinition.

Tipp:

Die ausführbaren Jobs sind dieselben, welche auch bei den USV-Ereignissen ausgelöst werden können. Das ermöglicht die volle Integration der Umweltkontrollsensoren in das Warn- und Alarmverhalten. Bitte beachten Sie, dass andere Sensoren je nach Funktion gegebenenfalls andere Einstellungsmöglichkeiten zur Verfügung stellen können.

[Digitalen Inputs Systemereignisse zuweisen](#)

Suchen Sie nach Alarm Digital Input



Mit **+** öffnen Sie den Konfigurationsdialog für die Jobdefinition.

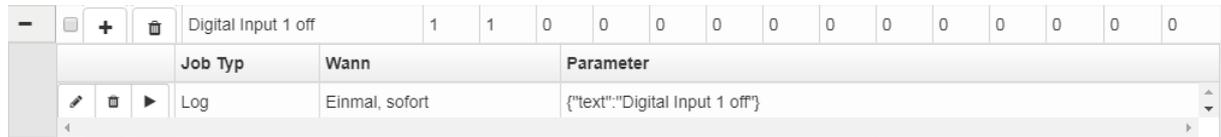
Sie können beliebig viele Jobs dem Event zuordnen – der SITEMANAGER II/V6 wird diese entsprechend der Konfiguration auslösen.

Das Gegevent einrichten:

Je nach Konfiguration des Ereignisses werden Jobs ausgeführt, solange ein Ereignis ansteht, oder angestoßen und bleiben aktiv, bis ein entsprechendes Gegevent ausgelöst wird.

Ein typisches Beispiel wäre hier ein RCCMD – Shutdown mit Redundanzverhalten. Der RCCMD-Client bekommt vom SITEMANAGER den Befehl, einen Shutdown auszulösen, wartet jedoch noch auf einen CS141, welcher das Kommando nicht ausgelöst hat. In diesem Fall muss als entsprechendes Gegenereignis der RCCMD Shutdown vom SITEMANAGER wieder zurückgenommen werden, da der RCCMD-Client sonst glaubt, dass die Anweisung zum Shutdown noch aktiv ist

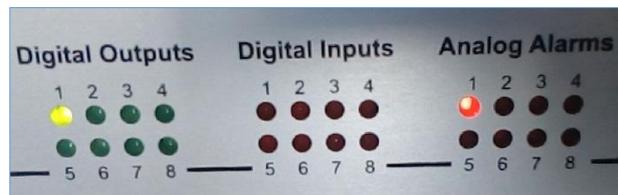
Sobald ein Ereignis nichtmehr ansteht, können auf diese Weise entsprechende A



[Besonderheit beim JOB AUX:](#)

Wenn Sie den CS141 mit einem CON_R_AUX4 betreiben, können Sie Outles schalten. Der SITEMANAGER II/V6 hat diese Funktion bereits fest integriert.

Wählen Sie als Job AUX aus. Anschließend stehen Ihnen unter Parameter die Site Manager Outlets Port 1 – 8 zur Verfügung, welche Sie frei schalten können. Geschaltete Outputs werden dem entsprechend an der Stirnseite unter *Ditigal Outputs* angezeigt.



Den Status können Sie sich im Sensor Monitor komfortabel anzeigen lassen und in Echtzeit ändern: Beachten Sie, dass die Beschriftung des Buttons den Zustand repräsentiert, den der Output einnehmen wird:

Ausgänge		
Name	Status	Anschalten
1 Output 1	●	Switch Off
2 Output 2	●	Switch On

Switch on / Switch Off wird entsprechend bei den Outputs auf der Stirnseite des SITEMANAGER 6 angezeigt. Schalten Sie den Ausgang auf off, werden beide Anzeigen ausgeschaltet. Bitte beachten Sie in diesem Zusammenhang das Caching-Problem der Webbrowser:

Wenn die Front-LED am Gerät ausgeschaltet wird, aber im Webinterface noch auf ansteht, aktualisieren Sie den Browsercache.

Einrichten eines Jobs

Tipp:

Die ausführbaren Jobs sind dieselben, welche auch bei den USV-Ereignissen ausgelöst werden können. Das ermöglicht die volle Integration der Umweltkontrollsensoren in das Warn- und Alarmverhalten. Bitte beachten Sie, dass andere Sensoren je nach Funktion gegebenenfalls andere Einstellungsmöglichkeiten zur Verfügung stellen können.

Die in diesem Menü verwendeten Symbole werden ausführlich im Kapitel *Einstellen der Systemereignisse* beschrieben.

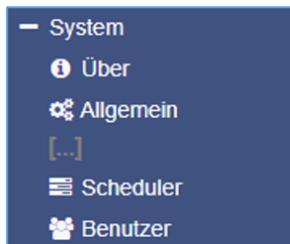
Klicken Sie auf , um eine allgemeine Übersicht über bereits vorhandenen Jobs zu erhalten

		SM_T_H_COM Temperature High	1	1	0	0
		Job Typ	Wann	Parameter		
		Log	Einmal, sofort	{"text": "SM_T_H_COM Temperature High"}		

Für das Ereignis einer zu hohen Temperatur ist demnach bereits ein Job konfiguriert.

Scheduler

Für diesen Konfigurationsschritt benötigen Sie die folgenden Menüs



→ Scheduler für geplante Aufgaben

Unabhängig von allen Systemereignissen bieten alle Modelle der CS141 Produktfamilie die Möglichkeit, Jobs zu frei definierbaren Zeitpunkten auszuführen. Diese sogenannten *scheduled Jobs* können dabei auf alle angeschlossenen Geräte gelegt werden. Diese Jobs können genutzt werden, um zum Beispiel über- oder untergeordnete Systeme anzusteuern, Computer neu zu starten, etc.

Das Konfigurationsmenü

In der Grundkonfiguration ist beim Scheduler kein Job als Werkseinstellung definiert – diese müssen bei Bedarf exklusiv definiert werden.

Um einen Job zu definieren, klicken Sie auf +:

Es öffnet sich die bereits bekannte Maske, welche alle Jobs beinhaltet, die zum Gegenwärtigen Zeitpunkt auswählbar sind.

Tipp:

Einige Jobs sind entsprechend der Konfiguration der angeschlossenen Geräte unterschiedlich einstellbar. Wenn Sie zum Beispiel in den allgemeinen Porteeinstellungen einen CON_AUX4 definiert haben, wird in den Jobs auch nur die Möglichkeit geboten, einen CON_AUX4 anzusteuern. Die erweiterte Funktionalität des CON_R_AUX4 wird ausgeblendet.

Webserver

Für diesen Konfigurationsschritt benötigen Sie die folgenden Menüs:

Aus Sicherheitsgründen wurde der Konsolenzugriff vollständig gesperrt. Alle Modelle der CS141-Produktfamilie wird ausschließlich über die Weboberfläche über http oder https konfiguriert.

[Aktivieren / Deaktivieren der Weboberfläche](#)

Der integrierte Webserver wird unter Dienste über den Schieberegler deaktiviert. Wichtig: Dies schaltet den integrierten Webserver im regulären Betriebsmodus aus, es ist kein Zugriff für die Konfiguration mehr möglich. Bevor Sie diesen Schieberegler auf OFF stellen, vergewissern Sie sich, dass ein aktuelles Systembackup (System>Update) angefertigt wurde.

[Konfiguration des Webzugriffs](#)

Übersicht der Grundeinstellungen

HTTP Port

Der internationale Standard für Webseiten jeglicher Art ist Port 80 – im Normalfall muss dieser Port nicht geändert werden. Sollten Sie in Ihrer IT-Infrastruktur für den Webmanager andere Ports vorgesehen haben, können Sie hier einen anderen Port eintragen. Beachten Sie bitte, dass Sie unter diesen Bedingungen auch den Port für die Web-Abfrage in Ihrem Webbrowser mit angeben müssen:

192.168.3.1:85

In diesem Fall wäre der Webmanager auf der IP 192.168.3.1 auf dem Port 85 erreichbar. Auf Port 80 hingegen würden Sie eine Fehlermeldung von Ihrem Webbrowser erhalten.

HTTPs Port

Sollten Sie HTTPs verwenden, wird standardmäßig der Port 443 verwendet. Bei Bedarf können Sie diesen Port Ihrem Netzwerk anpassen.

Tipp:

Sobald Sie force https aktiviert haben, müssen Sie https:// als Syntax in Ihrem Webbrowser verwenden. Ansonsten haben Sie zwei Möglichkeiten, wie ein Webbrowser auf diese Anfrage reagiert:

Connection Timeout

Da CS141 ausschließlich auf HTTPS antwortet, bekommt der Webbrowser keine Kommunikation.

Weiterleitung (Browserspezifisch)

Sollten Sie mehrere Geräte der CS141-Produktfamilie in Ihrem Netzwerk betreiben, kann es passieren, dass ein alternativer gültiger Eintrag bei Ihrem Webbrowser vorliegt – in dem Fall wird automatisch ein CS141 angezeigt.

Force HTTPs

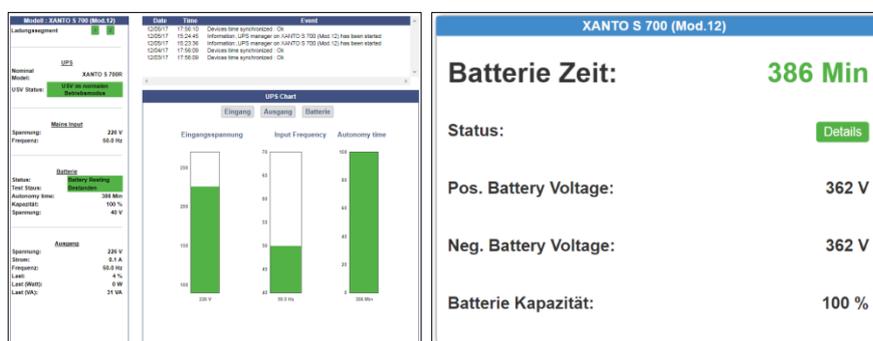
Eine standardmäßige HTTP-Verbindung im Internet kann sehr leicht von Unbefugten abgehört werden. Um dies zu vermeiden und damit eine sichere Datenübertragung zu gewährleisten, wird eine HTTPs-Verbindung genutzt. Es wird einerseits die Übertragung verschlüsselt und andererseits der Server authentifiziert. Der Vorteil liegt in der erhöhten Sicherheit, der Nachteil in der erhöhten Reaktionszeit, da die Daten verschlüsselt übertragen werden. Force HTTPs unterbindet den regulären HTTP-Verkehr und erzwingt die Nutzung von HTTPs

HTTP Aktualisierungszeit

Der CS141 liefert zyklisch automatisch eine aktualisierte Seite aus, über den unter anderem der Status von USV-Systemen oder anderen Statusmonitoren abgebildet wird. Dieser Wert definiert, wie oft eine automatische Seitenaktualisierung durchgeführt wird. Standardmäßig aktualisiert der CS141 diese Anzeigen alle 10 Sekunden.

Verwende einfachen Monitor

Der CS141 bietet im USV-Monitor zwei unterschiedliche Anzeigen, die sich sowohl vom Layout als auch von den Inhalten stark unterscheiden:



Der einfache Monitor (Abb. rechts) enthält deutlich weniger Informationen, dafür jedoch eine bessere Lesbarkeit.

HTTP Tooltips aktivieren

Tooltips sind kontextbezogene Hinweifenster, die automatisch eingeblendet werden, sobald Sie die Maus über eine Einstelloption ziehen. Standardmäßig sind die Tooltips aktiviert, können jedoch über diese Option permanent deaktiviert werden.

Automatischer Logout

Das Zeitfenster zwischen zwei Konfigurationseingaben. Dabei reicht es nicht aus, die Maus zu bewegen, es muss ein Menü innerhalb des Zeitfensters geöffnet bzw. eine Konfigurationseingabe bestätigt werden - Das Eingeben eines Werts reicht für sich in ein Eingabefeld reicht nicht aus, es muss in dem Fall auch ausdrücklich mit Übernehmen ein Schreib/Lesevorgang ausgelöst werden. Sollte kein automatischer Logout bei Inaktivität gewünscht sein, aktivieren Sie die Checkbox bei „Kein Auto-Logout“

Zertifikatsverwaltung / https – Zugriff

Der SITEMANAGER 7 bietet bei Inbetriebnahme ein werkseigenes HTTPS-Zertifikat an, um die Verschlüsselung der Verbindung sicherzustellen.

Um das Zertifikat durch ein eigenes Zertifikat zu ersetzen, schieben Sie das neue Zertifikat als „PEM-File“ via Drag'n'Drop in die entsprechende Box, und klicken Sie auf Upload.

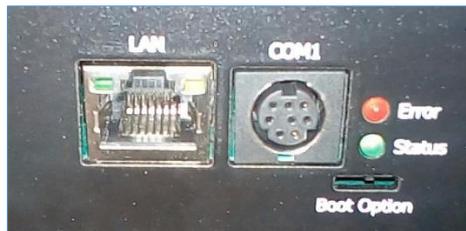
Hinweis:

Deaktivieren Sie für den Testlauf vorübergehend die Funktion „https erzwingen“, da ein fehlerhaftes / falsches Zertifikat den Zugriff via https verhindert. In dem Fall können Sie via http noch auf das Webinterface zugreifen, und ein neues Zertifikat hochladen.



Diagnose: Statusleiste und LED's

Der SITEMANAGER 7 bietet mehrere Möglichkeiten einer optischen Sichtkontrolle. Das erlaubt eine schnelle Vorabkontrolle, ob Handlungsbedarf besteht. Beim SITEMANAGER 6 befinden sich z.B. allgemeine Kontroll-LEDs direkt neben dem COM1 – Anschluss auf der Rückseite.



Grüne LED	Rote LED	Adapter
AUS	AUS	Keine Stromversorgung
AUS	AN	Bootvorgang
AUS	BLINKT LANGSAM	Updatevorgang
AUS	BLINKT SCHNELL	Updatevorgang fehlerhaft
AN	AN	Verbindung zur USV oder einem Externen Gerät verloren
BLINKT LANGSAM	AUS	Normalbetrieb, Verbindung aktiv

Detailliertere Informationen über den aktuellen Zustand finden Sie nach dem Login direkt in der oberen Statusleiste:

Zusätzlich zu dem physikalischen LED-Status existiert noch die Statusleiste. Hier werden die verschiedenen Zustände ebenfalls nähere Informationen über den aktuellen Zustand angezeigt:

UPS: ● Ready

Ein grüner Marker bedeutet, dass eine Kommunikation stattfindet und es keine Probleme gibt. Wenn Sie keine USV ausgewählt haben wird die LED ebenfalls grün leuchten.

UPS: ● Initializing

Ein Gelber Marker wird angezeigt, wenn:

- Das Gerät gerade initialisiert und die Kommunikation aufgebaut wird
- Ein Warnverhalten vorliegt, welches in naher Zukunft ein entsprechendes Eingreifen erfordern könnte.

UPS: ● Temperature Bad

Wenn der Marker rot leuchtet, liegt ein Alarm bzw. kritischer Zustand vor:

- Der CS141 hat die Kommunikation einem angeschlossenen Gerät verloren
- Es liegt ein Systemkritischer Zustand vor, welches ein zeitnahes Eingreifen erfordert.

Alle Arten von Alarmen werden hier detailliert angezeigt. Auch der Verlust der Kommunikation wird hier angezeigt.

UPS: ● Communications Lost

Ein blauer Marker bedeutet, dass das Gerät wahrscheinlich richtig konfiguriert wurde, jedoch noch keine Kommunikation stattfinden konnte.

Sensor: ● Disabled

Ein grauer Marker mit dem Hinweis *disabled* bedeutet, dass ein Gerät vollständig deaktiviert wurde und dem entsprechend keine Daten liefern kann.

Tipp

Auf der Frontseite befindet sich eine separierte Status-Anzeige, die den internen Status des Sitmanager 7 anzeigt. Wenn die Status-Anzeige blinkt, liegt ein internes Kommunikationsproblem bei den Anschlüssen vor.

Da das USV-Management sowie alle Jobs ausschließlich vom CS141 im Gerät betreut wird, werden USV-Management und entsprechend konfigurierte Systemdienste wie ein RCCMD Shutdown weiterhin ausgeführt, sofern die vorhandene Datenlage ausreicht.

Logfiles

Im Fall einer Fehlfunktion bieten die Protokolldateien zahlreiche Informationen an, die bei der nachfolgenden Ursachenforschung wertvolle Hinweise über die Ereigniskette und den Verlauf der Störung geben können.

Das Eventlog

- Logfile	
📄 EventLog	→ Das Ereignisprotokoll
📄 DataLog	→ Daten über Lade- und Entladezustände
📈 DataLog Diagramm	→ Grafische Darstellung

Logtime	Logtext
<input type="text" value="Logtime search"/>	<input type="text" value="Logtext search ..."/>
12/07/2017,09:38:01	time synchronization job : OK
12/07/2017,09:38:01	Restart NTP service: OK
12/07/2017,09:33:45	UPSMAN on No UPS model defined has started
12/07/2017,09:33:25	CS141L V1.63 - OEM 32

[Download als CSV Datei](#)

Im Eventlog werden neben den Systemereignissen alle Aktionen, die den CS141 und die USV betreffen, festgehalten. Der Eintrag wird dabei im Ereignismenü der USV-Einstellungen vorgenommen, Sie können individuelle Logdateien mit dem Job „Log“ erzeugen, oder die voreingestellte Konfiguration bestehen lassen.

Der Erste Eintrag nach einem Neustart ist immer der CS141 mit seiner OEM-ID:

12/07/2017,09:33:25	CS141L V1.63 - OEM 32
---------------------	-----------------------

Der älteste Eintrag ist dabei immer unten, der neueste Eintrag ganz oben in der Liste. Der Download als CSV-Datei erzeugt aus diesem Eventlog eine CSV-Datei und legt sie lokal auf Ihrer Festplatte ab:

DataLog	04.10.2017 13:45	MICROSOFT EXCEL-C...	400 KB
eventlog	07.12.2017 10:45	Microsoft Excel-C...	1 KB

Sie können diese Datei für spätere Analysen in einem Programm Ihrer Wahl öffnen:

A12			
A		B	
1	12/07/2017,09:33:25, CS141L V1.63 - OEM 32		
2	12/07/2017,09:33:45, UPSMAN on No UPS model defined has started		
3	12/07/2017,09:38:01, Restart NTP service: OK		
4	12/07/2017,09:38:01, time synchronization job : OK		
5			
6			

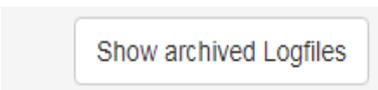
Ist der fortlaufende Speicher für Eventlogs erschöpft, wird sein Inhalt in eine Archivdatei verschoben, die auf dem CS141 abgelegt zur Anzeige und zum Download bereitsteht.

Tipp:

Je nach Konfiguration werden die Systemereignisse im Eventlog bis zu drei Monate vorgehalten. Sobald der fortlaufende Speicher für die aktuelle Eventlogdatei erschöpft ist, werden die Dateien abwechselnd in 2 Archivdateien gespeichert. Damit steht generell ein überwachter Zeitraum von bis zu 9 Monaten ab Erstinbetriebnahme zur Verfügung.

Zwischen den Logfiles navigieren

Standardmäßig wird das aktuelle Eventlog angezeigt.



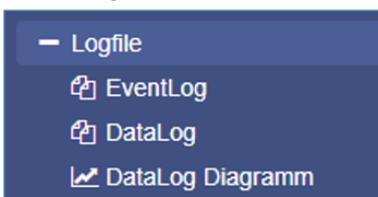
Sie können zwischen den beiden Logs umschalten, indem Sie in der oberen rechten Ecke den Button „Show archived Logfiles“ betätigen.

Beachten Sie, dass sich das Label des Buttons ändert:



Um zum aktiven Logfile zurück zu kehren, betätigen Sie den Button „Show active Logfile“

Das Datalog



→ Das Ereignisprotokoll

→ **Daten über Lade- und Entladezustände**

→ Grafische Darstellung

Logfile > DataLog																
Date,Time	InVolt1	InVolt2	InVolt3	InFreq	Load1	Load2	Load3	BattVolt	UPSTemp	BattCap	OutVolt1	OutVolt2	OutVolt3	OutFreq	AutonomTime	
01/01/2000,00:04:51	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	6.0
01/01/2000,00:07:59	230.0	230.0	230.0	50.0	100.0	n/a	n/a	n/a	n/a	100.0	n/a	n/a	n/a	n/a	n/a	6.0
01/01/2000,00:11:06	230.0	230.0	230.0	50.0	100.0	n/a	n/a	n/a	n/a	100.0	n/a	n/a	n/a	n/a	n/a	6.0
01/01/2000,00:14:16	230.0	230.0	230.0	50.0	100.0	n/a	n/a	n/a	n/a	100.0	n/a	n/a	n/a	n/a	n/a	6.0
01/01/2000,00:17:23	230.0	230.0	230.0	50.0	100.0	n/a	n/a	n/a	n/a	100.0	n/a	n/a	n/a	n/a	n/a	6.0
01/01/2000,00:20:31	230.0	230.0	230.0	50.0	100.0	n/a	n/a	n/a	n/a	100.0	n/a	n/a	n/a	n/a	n/a	6.0
01/01/2000,00:23:39	230.0	230.0	230.0	50.0	100.0	n/a	n/a	n/a	n/a	100.0	n/a	n/a	n/a	n/a	n/a	6.0

Im Datalog werden vorhandene Messdaten festgehalten. Da diese mit einem Zeitstempel versehen sind, können sie zusammen mit dem Eventlog Ereignisketten mit zusätzlichen Daten wie das Eventlog können diese Daten als CSV-Datei für spätere Analysen exportiert werden.

Das Datalog speichert hierbei die Einträge im 3-Minuten-Takt und hält die Einträge 8 Wochen als aktuelle Datalogdatei vor. Danach werden die Daten in eine Archivdatei verschoben und ein neues Datalog für die aktuellen Daten aufgemacht. Dabei können neben der aktuellen Datei 2 Archivdateien angelegt werden – es stehen also neben dem aktuellen Zeitraum bis zu 24 archivierte Wochen zur Verfügung. Nach Ablauf der Zeit wird die jeweils älteste Archivdatei ersetzt.

Wie beim Eventlog kann bei dem Datalog zwischen archivierten Dateien und der aktuellen Logdatei über die Funktion *Show archived Logfiles* und *Show active Logfiles* gewechselt und die Dateien im Format CSV über den Link am unteren Ende des Datalogs heruntergeladen werden.

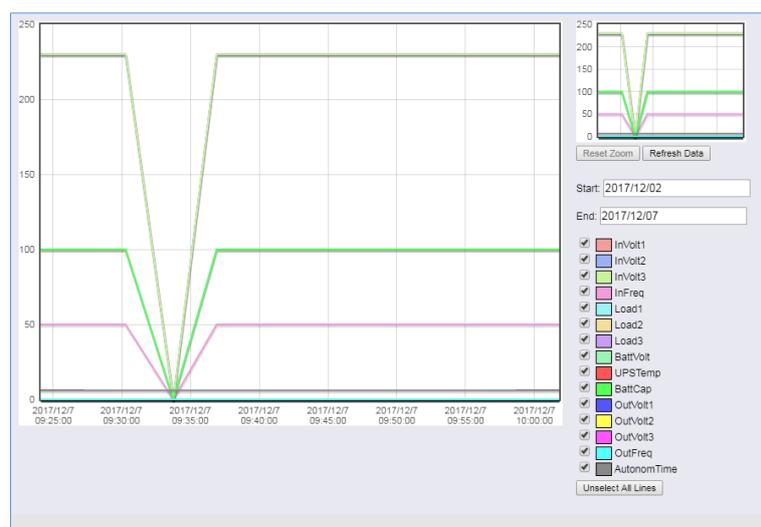
[Datalog Chart – Grafische Darstellung](#)



Übersicht

Der Datalog Chart ist eine grafische Aufbereitung des Datalogs:

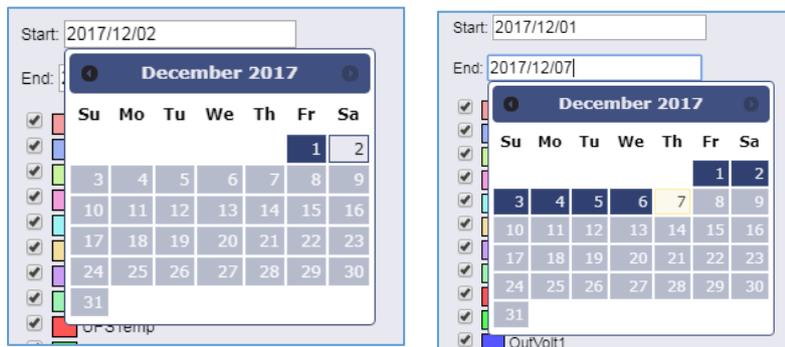
Dabei können über die Checkboxes alle Einträge innerhalb des Datalogs gezielt aus- bzw. abgewählt werden.



Sie haben die Möglichkeit, sich neben den aktuellen Werten auch gezielte Werte aus aktuellen Datenbeständen auszuwählen. Standardmäßig sind bei Aufruf alle Häkchen gesetzt. Über die Funktion *Unselect All Lines* können Sie diese entfernen und die relevanten Häkchen setzen.

Kalenderfunktion

Die Kalenderfunktion bietet einen schnellen Überblick vorhandener Zeitabschnitte, die Sie auswählen können. Klicken Sie

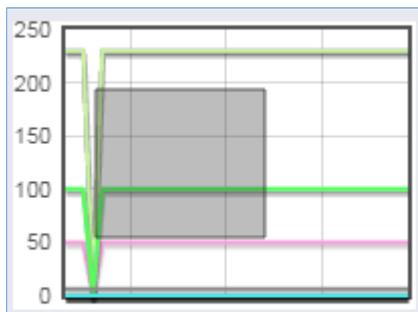


hierzu in das Datumsfeld, um den Kalender aufzurufen:

Die Daten des entsprechenden Zeitraums werden automatisch geladen und im Hauptfenster angezeigt.

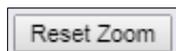
Zoom – Funktion

Der SITENANAGER 7 bietet die Möglichkeit, in die erhobenen Daten zu zoomen und so eine detaillierte Ansicht innerhalb der angezeigten Messdaten zu erhalten.

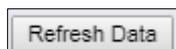


Um die Anzeige zu verfeinern ziehen Sie in dem kleinen Fenster einen Rahmen. Im Hauptfenster wird entsprechend automatisch eine Detailansicht mit angepasstem Zeitstrahl angezeigt:

Die Zoomfunktion erlaubt hierbei eine Vergrößerung des Zeitstrahls auf bis zu 2 Minuten.

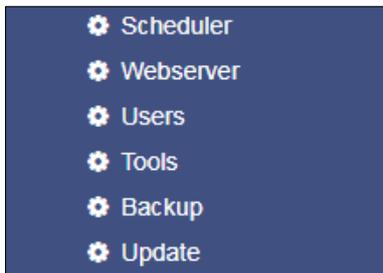


➔ Schaltet die Zoomtiefe auf Ausgangswert zurück



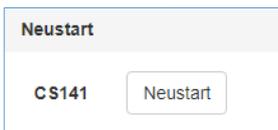
➔ Aktualisiert die aktuellen Daten und setzt den Fokus auf diese.

Toolbox



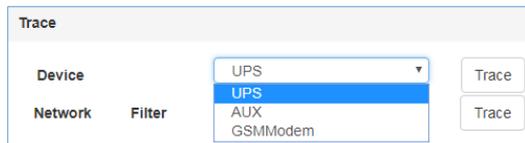
➔ **Toolbox mit der Rebootfunktion**

Reboot / Kaltstart



Da der CS141 die Konfigurationen in Echtzeit schreibt und die entsprechenden Systemdienste neu startet, ist ein kompletter Neustart nur in Ausnahmesituationen notwendig. Auch wenn der Neustart ausschließlich den CS141 betrifft und die USV in der Zeit regulär weiterläuft, fällt kurzfristig die Überwachung aus. Um ein versehentliches Neustarten zu verhindern, wurde diese Funktion bewusst unter Tools abgelegt.

Tracer



Der Tracer ist ein umfangreiches Diagnosetool zur Überprüfung der Kommunikation sowohl zwischen dem CS141 und den angeschlossenen Endgeräten als auch zur Identifizierung von Netzwerkproblemen, wenn Kommunikationsprobleme zwischen dem CS141 und einem Server nicht richtig funktioniert.

Unter Device werden Kommunikationsinformationen zwischen Endgerät und CS141 abgefragt. Dabei können die COM-Ports ausgewählt werden, bei denen es zu Problemen kommt. Um ein Gerät auszuwählen, öffnen Sie das Kontextmenü und wählen Sie das gewünschte Gerät aus, welches Sie überwachen möchten:

COM 1 / UPS

Dieser Tracer schneidet die USV-Kommunikation, die über den seriellen RS232 – Port läuft aktiv mit. Störungen oder fehlerhafte Kommunikation werden angezeigt und können zur späteren Auswertung gespeichert werden

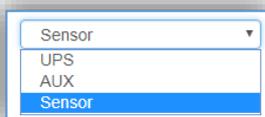
COM 2 / GSM-Modem

Der Tracer fragt die Kommunikation zwischen dem CS141 und dem GSM-Modem ab und zeigt diese in Echtzeit an. Fehler und Kommunikationsprobleme können auf diese Weise einfach gesammelt und für eine spätere Analyse gespeichert werden.

COM 3 / AUX

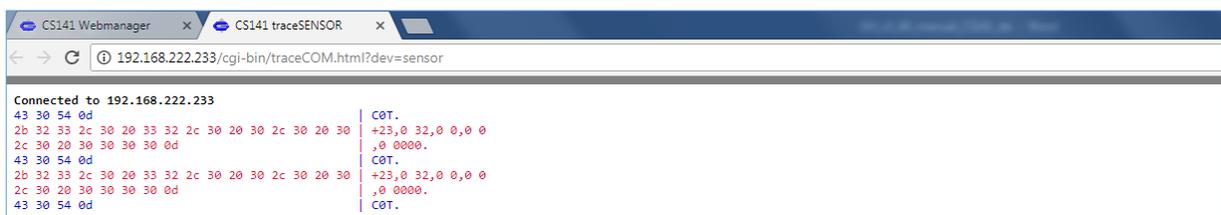
Über den AUX-Port kann ein CON_AUX4 bzw. CON_R_AUX4 angeschlossen werden. Der Tracer kann die Kommunikation mit dem Gerät in Echtzeit abfragen.

Tipp:



Der Tracer passt sich mit der Auswahl dem an, was Sie unter Geräte/Anlagen in der allgemeinen Porteeinstellungen konfiguriert haben. Wenn Sie statt dem GSM-Modem einen Sensormanager2 konfiguriert haben, wird im Tracer dem entsprechend nur Sensor angezeigt.

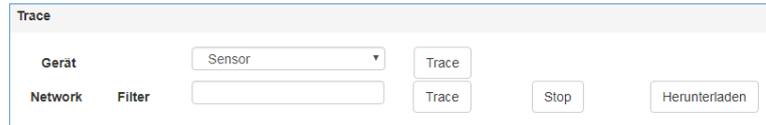
Mit dem Button Trace starten Sie den Vorgang, bei dem ein neuer Tab in Ihrem Webbrowser geöffnet wird, in der die Kommunikation zwischen dem Endgerät und dem CS141 gezeigt wird.:



Wenn Die dieses Fenster schließen, wird der Trace automatisch beendet und nicht gespeicherte Daten gehen verloren. Um die Daten zu speichern markieren Sie diese mit der linken Maustaste und kopieren Sie den Inhalt mit STRG + C, und fügen Sie die Information mit STRG + V in ein Dokument Ihrer Wahl ein.

Network-Scan

Eine Besonderheit des CS141 ist die Möglichkeit, mit einem integrierten Netzwerks scanner das LAN auf Fehlerquellen zu untersuchen. Der Netzwerks can liefert umfangreiche Informationen zur Auswertung über die Netzwerkkarte und den darin enthaltenen Datenverkehr in Ihrem LAN. Dabei werden alle Datenpakete in einer Protokolldatei gesammelt und kann für die spätere Auswertung heruntergeladen werden.



Datenschutzhinweis:

Da der Netzwerks can den gesamten Datenverkehr in diesem Netzwerksegment aufzeichnet, kann eine Auswertung mit einem entsprechenden Netzwerkt tool neben tiefen Einblicken in den Netzwerkverkehr auch verwendet werden, um z.B. das Nutzerverhalten zu protokollieren. Techniker sollten vor der Nutzung die jeweils notwendigen Verantwortlichen in Kenntnis setzen.

Um einen Netzwerks can durchzuführen, betätigen Sie in der Zeile Network den Button *Trace*:



Der Tracer bestätigt mit einem kurzen Einblenden, dass er gestartet wurde.

Der Tracer loggt alle Paketdaten innerhalb des LAN-Segments mit, und speichert diese lokal auf dem CS141. Dabei werden die erhobenen Daten in Echtzeit abgelegt und gespeichert – sollte der CS141 abstürzen, liegen die Daten bis zum Absturz anschließend vor können über den Button Herunterladen auf der lokalen Festplatte gespeichert werden. Der Tracer wird beendet, wenn zwei Bedingungen vorliegen:

1. Ein Neustart
2. Betätigen der *Stop*-Funktion

Nach dem Beenden werden die Daten in Form eines gepackten Archives zur späteren Auswertung heruntergeladen werden.



Tipp:

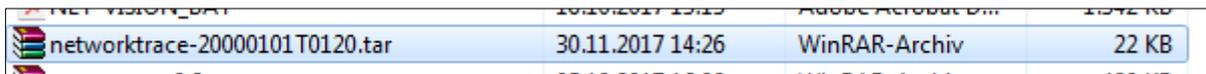
Der Netzwerkt racer wird In der Regel sehr selten benötigt, etwa, wenn der technische Support von GENEREX spezielle Informationen benötigt, die zur Eingrenzung eines Problems dienen. In diesem Fall empfiehlt es sich, den Tracer ohne einen besonderen Filter zu starten.

Diese Funktion kann noch mehr: Es verwandelt Ihren CS141 in ein Netzwerkd iagnosewerkzeug mit zahlreichen Funktionen, mit denen Sie Ihr lokales LAN untersuchen können:

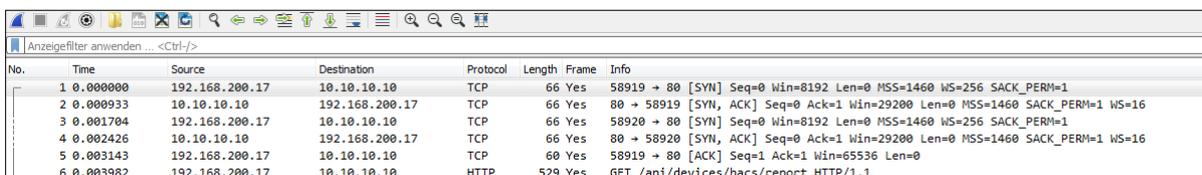
Unter www.tcpdump.org finden Sie umfangreiche Tutorials, wie Sie Filter definieren können, um das volle Potential des CS141 als Netzwerkd iagnosesystem nutzen zu können.

Netzwerks can: Auswertung der Daten

Die erhobenen Daten können über spezielle Diagnosetools wie *Wireshark** ausgelesen und analysiert werden:

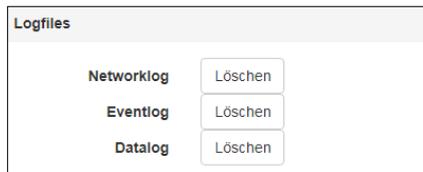


Entpacken Sie die Datei und Importieren Sie den Datensatz in *Wireshark*:



*Das Tool wireshark ist kein GENEREX-Produkt. Sie erhalten Sie unter www.wireshark.org

Löschen von Logfiles



Der CS141 sammelt und protokolliert große Mengen an Daten und speichert diese permanent in seinem eigenen Speicher. Diese Daten können anschließend über einen Webbrowser abgeholt und mittels Diagnosetools ausgewertet werden. Da die Logdateien sehr sensible Informationen über ein Netzwerk enthalten, können diese bei Bedarf vollständig und permanent gelöscht werden.

Netzwerklog

Mit dieser Funktion löschen Sie alle Aufzeichnungen, die der Netzwerkracer erhoben hat.

Eventlog

Mit dieser Funktion löschen Sie alle Aufzeichnungen, die Systemereignisse in der Logdatei vermerkt haben.

Datalog

Mit dieser Funktion löschen Sie alle Datenaufzeichnungen, die der CS141 protokolliert hat.

Logo austauschen

Es kann vorkommen, dass das original Logo innerhalb von Firmen Organisationen oder Konzernen letztendlich nicht gewünscht ist. Daher bietet der CS141 die Möglichkeit, das vorhandene Logo durch ein eigenes Logo zu ersetzen.

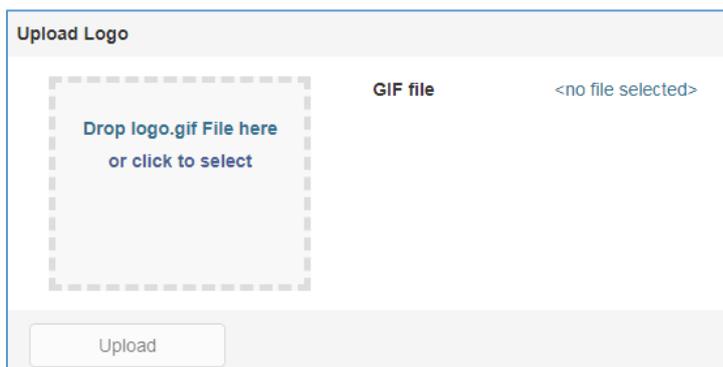
Kurzanleitung: Logo austauschen

1. Öffnen Sie ein verfügbares Grafikprogramm
2. Erstellen Sie zunächst ein neues Bild. Achten Sie auf die maximale Größe von 200x54 Pixel



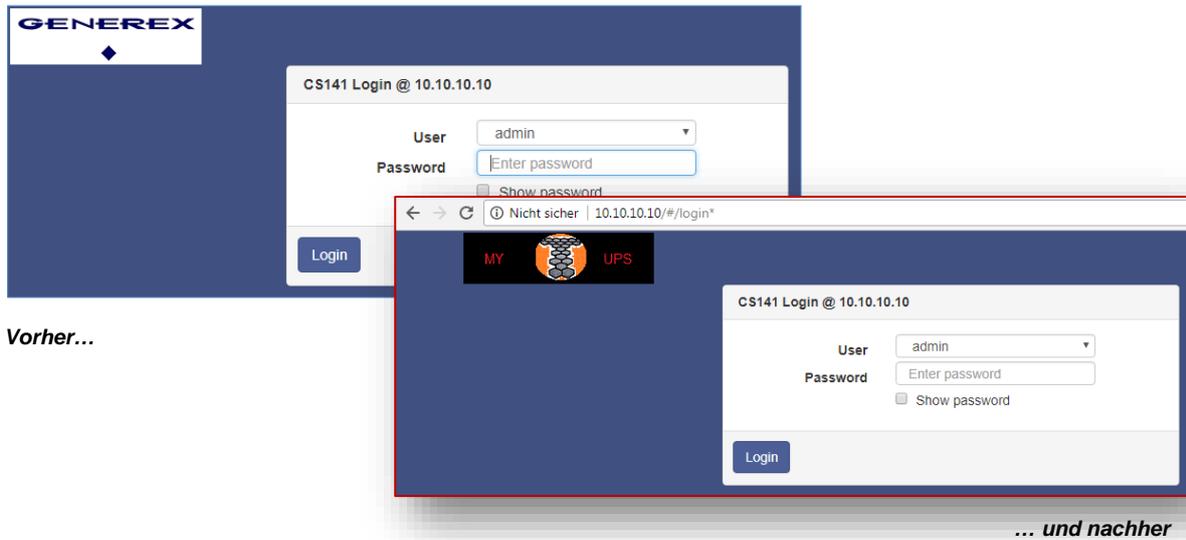
3. Editieren Sie das Bild und passen Sie den Inhalt nach Ihren Wünschen an.
4. Speichern Sie das Bild als *logo.gif* – ansonsten wird es nicht vom CS141 akzeptiert.
5. Öffnen Sie im CS141 die Tools.

Unter Tools finden Sie die folgende Option:



Nutzen Sie Drag and Drop, um das neue Logo in das vorgesehene Fenster zu schieben.

6. Mit Upload wird das neue Logo übernommen:



Datensicherung und Updates



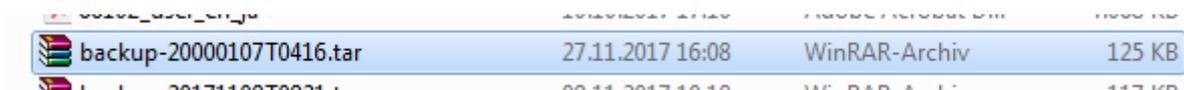
Die Datensicherung bietet die Möglichkeit, die aktuelle Systemkonfiguration komplett zu sichern, um im Notfall schnell wiederherstellen zu können.

Die Sicherung und Wiederherstellung erfolgen in zwei Schritten:

Schritt 1: Sichern der Daten



Wenn Sie im Menü *Backup* unter Konfiguration Speichern auf Backup klicken, wird eine gepackte Datei lokal auf Ihrem PC im Downloadverzeichnis abgelegt. Da die Backupfunktion systemkritisch ist, wird ausdrücklich noch einmal nach dem gültigen Administratorpasswort gefragt.



Dieses Datenbackup können Sie anschließend bei jedem CS141 mit derselben oder einer höheren Firmwareversion verwenden. Bitte beachten Sie, dass bei einer Änderung des Dateinamens die Backupdatei ihre Gültigkeit verliert und es zu einer Fehlermeldung kommt.

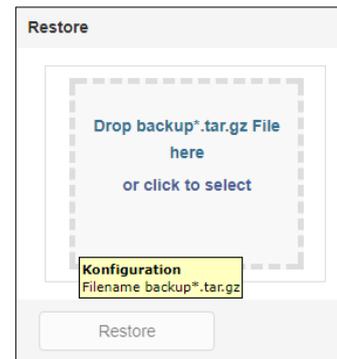
Schritt 2: Wiederherstellung der Daten

Das Einspielen eines Backups erfolgt in demselben Menü:

Ziehen Sie die gepackte Datei per Drag'n'Drop in die Box oder klicken Sie mit der linken Maustaste auf die Box, um einen Dateibrowser zu öffnen und wählen Sie mit einem Doppelklick die gewünschte Backupdatei aus.

Mit Restore stoßen Sie den Wiederherstellungsprozess an, welcher die Datei entpackt und automatisch als bestehende Konfiguration übernimmt. Nach Abschluss des Vorganges werden Sie automatisch ausgeloggt und müssen sich gemäß dem Backup mit den Anmeldedaten neu anmelden. Beachten Sie bitte, dass Backups von einem CS141 mit jedem CS141 derselben oder einer neueren Firmware kompatibel sind. Sollten Sie das Backup auf einem CS141 mit einer älteren Firmware verwenden, kann es zu Problemen kommen.

Ursache ist, dass mit einer neuen Firmwareversion neben allgemeinen Verbesserungen neue Features hinzukommen, deren Konfigurationsfiles auf älteren Firmwareversionen nicht richtig funktionieren können.



Firmwareupdates



Die Updates finden Sie unter www.generex.de im Downloadbereich.

Für Alle Geräte der CS141 Produktfamilie werden regelmäßig Systemupdates bereitgestellt. Neben allgemeinen Produktverbesserungen wie Erhöhung der Stabilität und Verbesserungen in der Betriebs- und Ausfallsicherheit bieten diese Updates regelmäßig auch neue Features, welche sich nahtlos in das bestehende System integrieren.

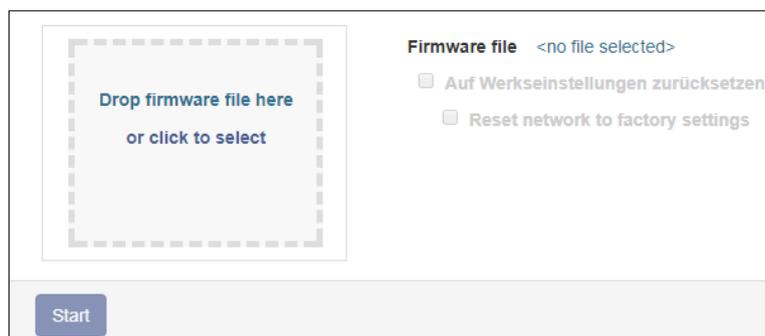
Standardmäßig ist die OEM ID 12 / GENEREX bei der Auslieferung vorinstalliert. Abweichungen ergeben sich, wenn Sie den Webmanager als Bestandteil einer USV von einem Hersteller erworben haben, für den ein OEM-Vertrag vorliegt.

Tipp:

Da der SITEMANAGER 7 technisch nicht gesperrt ist, Sie können jederzeit die OEM-Version eines anderen Herstellers installieren, sollte sich Ihre USV ändern.

Wählen Sie unter Firmware die von Ihnen gewünschte Version aus und laden sie diese auf ihren Computer herunter. Ein Entpacken der Datei ist nicht notwendig.

Nach dem Herunterladen öffnen Sie die Weboberfläche und gehen Sie unter System auf *Update*:



Ziehen Sie die heruntergeladene, gepackte Datei in das dafür vorgesehene Fenster. Mit Start beginnt der Updateprozess. Bevor Sie mit *Start* das Update beginnen, können folgende zusätzliche Optionen ausgewählt werden:

Auf Werkseinstellungen zurücksetzen

Diese Option löscht während des Updates sämtliche Konfigurationen und setzt das Gerät in den Auslieferungszustand zurück.

Reset network to factory settings

Diese Option setzt zusätzlich die Netzwerk- und IP-Einstellungen auf Auslieferungszustand zurück.

Tipp:

Diese beiden Optionen sind unabhängig voneinander, da ansonsten durch ein Update über einen Remote-Zugriff der CS141 die IP-Einstellungen mit verlieren würde. Sollten Sie Probleme haben, können Sie jederzeit über diese Funktion das Gerät ohne Änderung der IP-Adresse in den Auslieferungszustand zurücksetzen.

Die Updateroutine läuft automatisch, sie müssen nicht auf Seite bleiben. Sollten Sie zu früh auf das Webinterface zurückkehren, wird der CS141 die Verbindung automatisch ablehnen. Bitte beachten Sie in diesem Zusammenhang unbedingt das Cacheverhalten Ihres Browsers: Da einige Inhalte des Webinterfaces bereits im internen Speicher des Browsers vorliegen, kann es hier zu vermeintlichen Fehlermeldungen kommen, wenn der Bootvorgang noch nicht vollständig abgeschlossen ist.

Wechsel der OEM Firmware

Der CS141 Webmanager kommt in zwei unterschiedlichen Firmwareversionen:

- GENEREX – ID 12
- OEM-Version des Herstellers Ihrer USV

Sollten Sie Ihre USV nicht in der Liste der auswählbaren USV-Anlagen finden, kann es unter Umständen notwendig sein, eine andere Firmware zu installieren.

Hierzu ist es notwendig zu verstehen, woran Sie die aktuell installierte Firmware sowie die benötigte Firmware erkennen:

Die aktuelle Firmware

Sie erkennen die aktuelle Firmware an dem Logo oben links in der Ecke:



Je nach Hersteller werden Sie hier den entsprechenden Eintrag finden.

Die Firmware-Version

In den allgemeinen Systeminformationen finden Sie unter anderem diesen Eintrag:

Hardware	BACSKIT_B4
Firmware	CS141-SNMP V1.64.12 171213
Serial	1004211625 - 0030D6160377

Die Firmware gibt den OEM-Schlüssel wieder:

V1.64 die aktuelle Firmware
 .12 die aktuell installierte OEM-Version
 171213 das Erstellungsdatum rückwärts gelesen

Sollten Sie den CS141 in einer USV eines anderen Herstellers betreiben wollen, finden Sie die notwendige Firmware auf www.generex.de im Downloadbereich



Mit dem Link *Show Version info* können Sie überprüfen, ob es eine aktualisierte Firmware als Download erhältlich ist. Beachten Sie, dass – anders als bei einem Update innerhalb derselben OEM-Firmware – der Wechsel der OEM-Firmware das Zurücksetzen auf Werkseinstellungen notwendig ist, da sich unter anderem auch die Funktionen ändern.

Wenn gar nichts mehr geht – das Rettungssystem

Der SITEMANAGER 7 besitzt eine integrierte Schutz-Funktion, um bei Problemen selber automatisch neu zu initialisieren. Sollte dies nicht geschehen, verfügt der CS141 über zwei mögliche Optionen, mit denen Administratoren den Webmanager neu starten können.

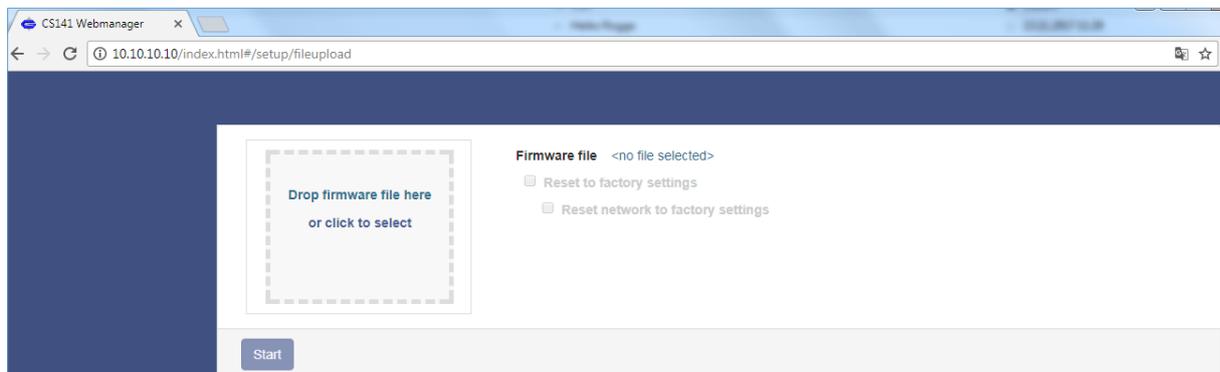
Sollte der CS141 keinen Login zulassen oder die Oberfläche eine fehlerhafte Darstellung anzeigen, jedoch noch regulär erreichbar sein, können Sie folgendes versuchen:

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

Über diese Option können Sie einen Neustart des CS141 in die Wege leiten, ohne dass Sie sich komplett anmelden müssen. Da der Neustart ein systemkritischer Vorgang ist, wird explizit nach dem Administratorpasswort gefragt.

`http://<Ip-Adresse>/update`

Diese Option ermöglicht es Administratoren, schnelle Systemupdates zu verteilen, da der Updatescreen direkt aufgerufen wird.



Nun können Sie das gewünschte Firmwarepaket per Drag&Drop oder durch klicken in die Schaltfläche auswählen. Bei Bedarf können Sie mit der Funktion Reset to factory defaults den CS141 auf Werkseinstellungen zurücksetzen. Dabei werden alle Konfigurationen gelöscht und das Gerät auf Startkonfiguration gesetzt.

Geben Sie nun das Kennwort für den Administrator ein. Der Vorgang startet und nach erfolgreichem Überspielen erscheint der Anmeldebildschirm.

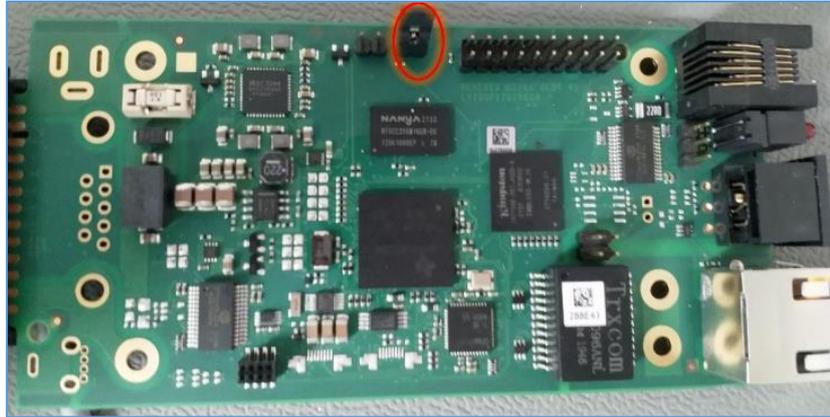
Tipp:

Netzwerkeinstellungen und Systemeinstellungen sind voneinander getrennt. Das erlaubt ein Flash-Update inklusive Löschen der Konfiguration, ohne dass die IP-Adresseinstellungen gelöscht werden.

Das Rettungssystem starten

Wenn diese Funktion nicht möglich ist, weil zum Beispiel das Update schiefgelaufen ist und der CS141 dadurch nicht mehr bootet, gibt es eine weitere Möglichkeit, das Gerät zu retten:

Der CS141 speichert bei jedem Updatevorgang eine komplette Sicherungskopie aller Logdateien und Konfigurationen der letzten als funktionierend bekannten Version. Diese Version kann durch setzen eines Jumpers aktiv geschaltet werden:



Wenn der Jumper gesetzt ist und der Adapter bootet, erkennen Sie das Rettungssystem anhand der Firmwareversion im *Über-Bildschirm* - Hinter der Firmware-Version finden Sie das Wort (*RESCUE*).
Appendix

FAQ – Frequently Asked Questions

Was bedeutet Fehler 500 / 503?

Dieser Fehler tritt auf, wenn der Webserver des CS141 nicht korrekt läuft. Sollte das Problem nach einem Neustart des Adapters weiterhin auftreten, muss die Firmware aktualisiert / neu eingespielt werden. Empfohlen wird dies dann in Verbindung mit einem Reset auf Werkseinstellungen.

Was bedeutet Fehler 422?

Dieser Fehler tritt auf, wenn versucht wird bei einer älteren Firmware die Konfiguration bestimmter Werte anzupassen. Aktualisieren Sie auf die neueste Version.

Was bedeutet Fehler 400 / 420/ 522?

Dieses Problem kann auftreten, wenn die Firmware aktualisiert wurde, der Browser aber noch alte Daten im Cache gespeichert hat. Drücken Sie STRG + F5 oder löschen Sie den Cache. Starten Sie den Adapter neu.

Der USV Status steht (kurzzeitig) auf „Paused“.

Wenn man über den Adapter auf die Alert History der USV zugreift, muss die normale Verbindung kurzzeitig angehalten werden. Wechseln Sie die Seite und drücken Sie F5 um den Anzeigestatus wiederherzustellen (sofern dies nicht automatisch geschieht).

Was bedeutet Fehler -1?

Dieser Fehler tritt auf, wenn keine Verbindung zum Adapter hergestellt ist (z.B. nach einem Neustart), vom Anwender aber die Konfigurationsseite des Adapters noch geöffnet ist. Warten Sie bis sich der Adapter wieder im normalen Betriebsmodus befindet und rufen Sie die IP des Adapters neu auf.

Ich habe mein Kennwort vergessen.

Schauen Sie in der Sektion „Rescue System“, dort ist beschrieben wie das Kennwort zurückgesetzt werden kann.

Warum werde ich ausgeloggt, wenn ich unter Dienste die http Tooltips deaktiviere?

Da die Tooltips mit dem http Service zusammenhängen und eine Änderung dieser Werte den Benutzer auf die neu konfigurierte Seite / den korrekten Port weiterleitet.

Der CON_R_AUX bekommt keine stabile Verbindung!

Dieses Gerät wird vom CS141 nicht unterstützt. Verwenden Sie hier den CON_R_AUX4.

Ich habe laufend Einträge im Logfile namens „UPSMAN started“.

Dieser Eintrag wird generiert bei Änderungen an der Eventkonfiguration. Dadurch dass die Änderungen sofort übernommen werden, muss der Dienst neu gestartet werden.

Beim Zugriff auf die Alert History bekomme ich nur einen Fehler angezeigt!

Die Funktion wird von der gewählten USV nicht unterstützt.

Ich erhalte den Fehler „Backend busy“ beim Versuch mich einzuloggen!

Warten Sie einen kurzen Moment und versuchen Sie es ggf. mit einem anderen Browser erneut. Sollte das Problem nach 5 Minuten weiterhin bestehen, verwenden Sie die /reboot Funktion.

Unterstützt der CS141 SNMP-Abfragen in der Version 1

Der CS141 hat eine SNMP-Abfragen v1.0 offiziell niemals unterstützt- was nicht bedeutet, dass er es nicht kann. Sollten Sie durch Ihr Abfragesystem gezwungen sein, eine v1-Abfrage durchzuführen, wird es funktionieren – jedoch wird es keinen offiziellen Bug fix geben, wenn Sie Probleme haben.

Ich habe Fragen, die nicht im Handbuch erklärt sind

Kein Problem, wir sind immer bestrebt, unsere Dokumentationen zu verbessern. Wenn Sie etwas haben, dass nicht oder unzureichend erklärt ist, schreiben Sie uns eine kurze Nachricht an support@generex.de – Wir helfen gerne weiter.

Ich will eine manuell eine abweichende Zeit einstellen, aber die verstellt sich immer auf den originalen Wert zurück

In 99% aller Anwendungsfälle sollte die Uhrzeit richtig eingestellt sein. Der CS141 löst das Problem, indem zunächst Zeitserver abgefragt werden – exakt in der Reihenfolge, wie sie eingetragen wurden. Dabei können sowohl eigene IP-Adressen als auch externe Zeitserver verwendet werden. Findet der CS141 den angegebenen Server nicht, nimmt er den nächsten Eintrag. Sobald kein Eintrag vorliegt, wird zunächst versucht, die Uhr der USV zu erreichen. Erst danach wird auf die interne Uhr zurückgegriffen.

Hier liegt das Problem:

Wenn die USV das setzen und auslesen über den CS141 unterstützt, wird bei *manueller Zeiteingabe* nicht die Systemuhr der USV überschrieben - umgekehrt jedoch kann der CS141 über die Systemuhr der USV die eigene Uhr korrigieren. Wenn Sie diese Uhr manuell setzen möchten, müssen Sie in dem Fall über das USV-Menü auch die USV-Uhr entsprechend den Einstellungen anpassen, da der CS141 sich mit der internen Uhr der USV synchronisiert.

Wieso kann ich den CS141 nicht in den NAGIOS Prozess mit einbinden?

Eine Sache, die vielleicht erwähnenswert ist: Nach dem Speichern der Datei in /usr/share/snmp/mibs sollte die Datei von *RFC1628-cs1x1.mib* in *UPS-MIB.txt* umbenannt werden, damit Centos sie erkennt und damit eine Interaktion möglich ist. Bitte beachten Sie, dass je nach Linux-Distribution die Verzeichnisse und Zugriffsrechte unterscheiden können.

Im Handbuch wird immer ein Blockdiagramm angezeigt, aber ich erhalte nur eine Balkenansicht, kann man das umstellen?

Die Ansicht ist je nach Hersteller unterschiedlich und kann nicht geändert werden, da diese vom Hersteller vorgegeben wird. Sie können jedoch im Auswahlmene *Webserver* zwischen einer einfachen und einer komplexen Darstellung des USV-Screens wählen.

Im Handbuch angegebene Links sind zwar inhaltlich richtig, aber die Position hat sich verschoben

Das passiert leider hin und wieder, besonders dann, wenn in letzter Sekunde noch eine Änderung am sog. „Release-Kandidaten“ vorgenommen werden, die letztendlich eine Fülle an Änderungen mit sich brachten. Diese Überschneidungen lassen sich leider nicht ganz ausschließen.

Warum kann ich nicht unter die 1.66.XX Firmware downgraden?

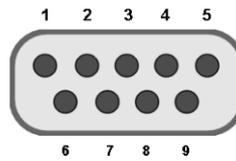
Ab 2018 gibt es eine neue Hardwarerevision der CS141 Boards. In der „About-Box“ unter System wird die Hardwarerevision unter Features angezeigt:

bch16 verwendet einen älteren Chip, welcher vor dem Jahr 2018 verbaut wurde. Dieser Chip ist voll auf- und abwärtskompatibel.

bch8 verwendet einen neueren Chip, welcher ab dem Jahr 2018 verbaut wird. Dieser Chip beginnt mit der Firmware 1.66.XX aufwärts und ist nicht zu älterer Firmware kompatibel

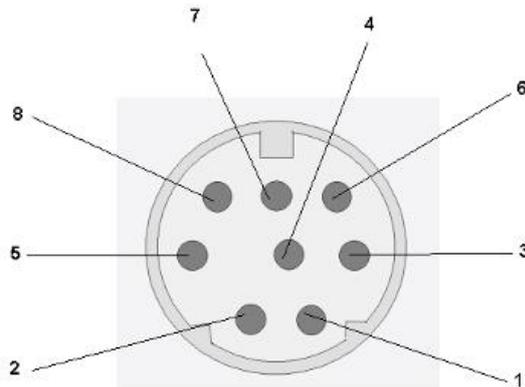
Da der CS141 ausschließlich mit der neuesten Firmware ausgeliefert wird, die zu dem Zeitpunkt aktuell ist, kann es sein, dass ältere Firmware als 1.66.XX aus diesem Gründen nicht lauffähig ist.

Für weitere Fragen kontaktieren Sie unseren Support unter support@generex.de !

Anhang: Hardware Layout und Anschlüsse CS141 / SITEMANAGER 7Schnittstellenbeschreibung

External D-SUB 9-polig male

Pin1: DCD	Pin6: DSR
Pin2: RxD	Pin7: RTS
Pin3: TxD	Pin8: CTS
Pin4: DTR	Pin9: RI
Pin5: GND	

Pin COM2 Mini-DIN 8 pol

Mini DIN 8 socket RS-232:

Pin1:	-> DCD
Pin2:	-> RxD
Pin3:	-> TxD
Pin4:	-> DTR
Pin5:	-> DSR
Pin6:	-> RTS
Pin7:	-> CTS
Pin8:	-> RI
Schirm	-> GND

RS-485 (optional):

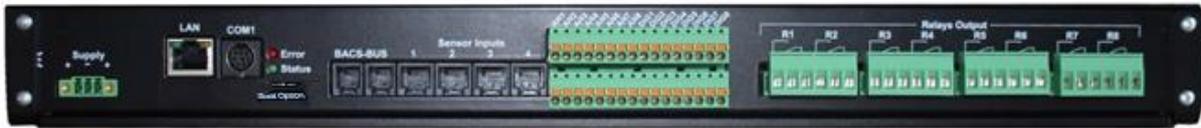
Pin1	→ GND
Pin2:	-> RS485/A
Pin3:	-> RS485/B(-)

Anschlussmöglichkeiten am SITEMANAGER 6

Die Abbildung zeigt eine typische Installation des Sitemanagers mit einer angeschlossenen USV. Es ist möglich, zahlreiche Arten von Sensoren mit dem Sitemanager zu verbinden und Stromkreise durch schalten der Relaiskontakte zu verwalten.

Anschlussbuchsen und Klemmleisten

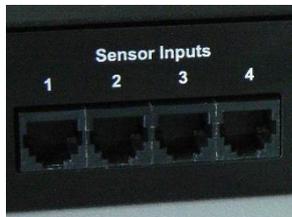
Die Rückseite des Sitemanagers ist mit folgenden Anschlusssteckern ausgestattet:



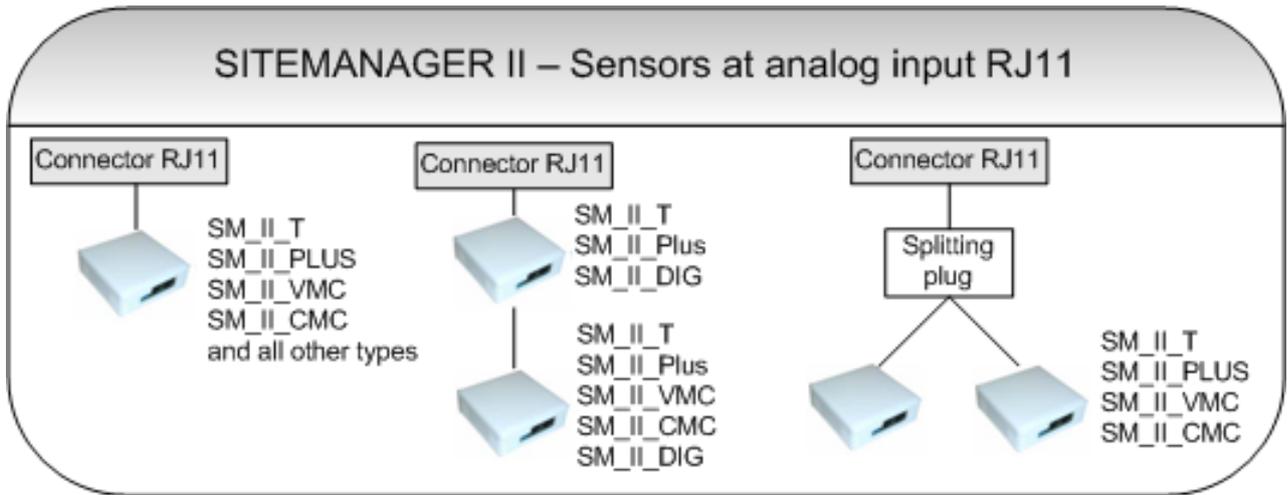
Rückseite des SITEMANAGER II/v6

- Stromversorgung: Verbinden Sie das mitgelieferte externe Netzteil (DC, 24V).
- Schnelle Umschaltung zwischen den Betriebsmodus dank Sliding Switch
- COM Port 1: RS232-Verbindung für USV, Sensor Manager oder sonstige RS232-Geräte.
- LAN-Buchse: Verbinden Sie den SITEMANAGER II/v6 durch ein RJ45-Kabel mit dem Netzwerk.
- 2 RJ10-Anschlüsse für den Anschluss eines BACS-Bus Systems
- 4 RJ12-Anschlüsse, Anschluss für 8 analoge Messeinheiten.
- Klemmleisten für 8 analoge- und 8 digitale Signale.
- 8 schaltbare Relaiskontakte (NO und NC).

Analoge Eingänge über RJ12-Anschlussbuchsen



Jede der 4 RJ12-Anschlussbuchsen kann 2 analoge Eingangssignale (0-10V o. 0/4-20mA) einlesen, damit ist es möglich 8 analoge Sensoren anzuschließen. Die folgende Abbildung zeigt wie die verschiedenen Sensoren an die RJ12-Anschlussbuchsen angeschlossen werden können. Für die PIN-Belegung schauen Sie bitte in den entsprechenden Anhang am Ende dieses Dokumentes.



Sensoren Anschlussmöglichkeiten am analogen RJ12 Input

1.1.1 Analoge Eingänge über Klemmleisten

Die 8 analogen Eingänge sind zusätzlich noch auf die obere Klemmleiste A01-A08 geführt. Dort können kundenspezifische Sensoren / Messwandler angeschlossen werden die ein Ausgangssignal von 0-10VDC liefern. Der Anschluss erfolgt über offene Leitungsenden (min.0,14mm² / max.1,5mm²) an den jeweiligen Federkraftanschluss der Klemmleiste.

Bitte darauf achten, dass Kanäle nicht doppelt über die RJ11-Buchse und Klemmleiste belegt werden!

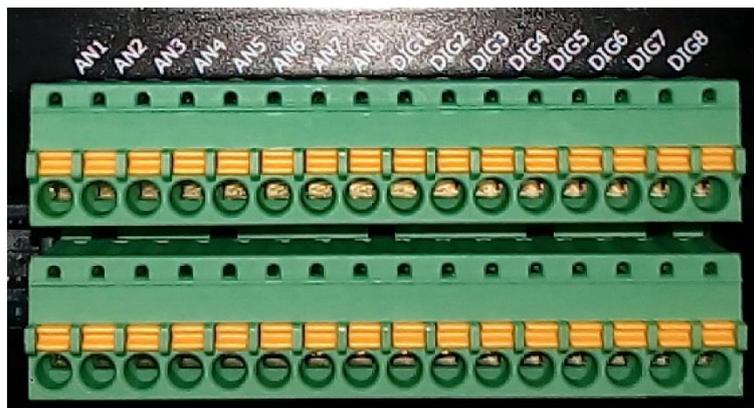
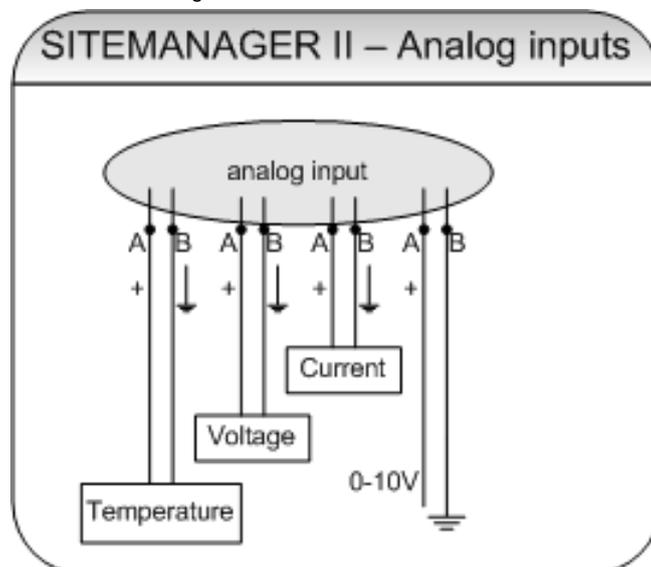


Abbildung: Auf der Klemmleiste sind die analogen Eingänge mit AN deutlich zu erkennen

Die folgende Abbildung zeigt die Anschlussbelegung der Klemmleiste für die Analogeingänge. Beachten Sie, dass das Eingangssignal in dem Bereich von 0-10V DC liegt.



Anschlussbelegung der Klemmleiste Analogeingänge

Konfiguration der SITEMANAGER II/v6 Analogeingänge

Jeder der 8 Analogeingänge des SITEMANAGER II/v6 bietet die Möglichkeit analoge Messwerte entweder von **0-10V (Auslieferungszustand)** oder **0-20mA bzw. 4-20mA** einzulesen.

Hierzu müssen auf der Hauptplatine die Jumper des jeweiligen Analogeinganges in der richtigen Position gesetzt sein.

Zum Ändern des Auslieferungszustandes bitte wie folgt vorgehen:

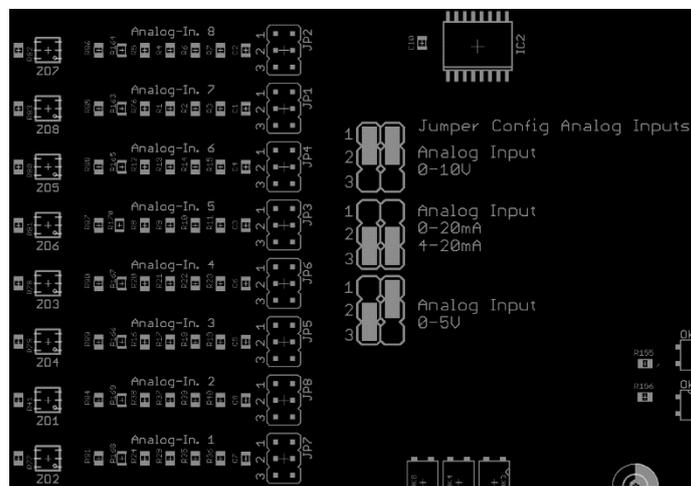
- Freischalten des SiteManagers II/v6 (Steckernetzteil ziehen)
- sämtliche Anschlussleitungen vom Gerät trennen (16/6-polige Phoenixstecker können bei Bedarf komplett vom Gerät abgezogen werden).
- Ausbau des Gerätes
- Gerät durch Lösen der 4 seitlichen Schrauben und Abziehen des Gehäusedeckels öffnen
- Jumper in der gewünschten Konfiguration setzen (siehe *Abb. 1/Abb.2*)
- In umgekehrter Reihenfolge Gerät wieder zusammenbauen/in Betrieb nehmen

Auslieferungszustand (Analog Inputs 0-10V)

Beide Jumper der Analog Inputs 1-8 (Channel 1-8) sind auf **PIN 1+2** gesetzt (*Abb. 1*)

In diesen Jumperstellungen dürfen nur folgende Sensoren an die Analog Inputs angeschlossen und innerhalb der Konfiguration der Sensor Type" in der SITEMANAGER II/v6 ausgewählt werden:

- **Custom 0-10V**
- **SM_II_T**
- **SM_II_T_H**
- **SM_II_T_Plus**
- **SM_II_VMC**
- **SM_II_CMC**

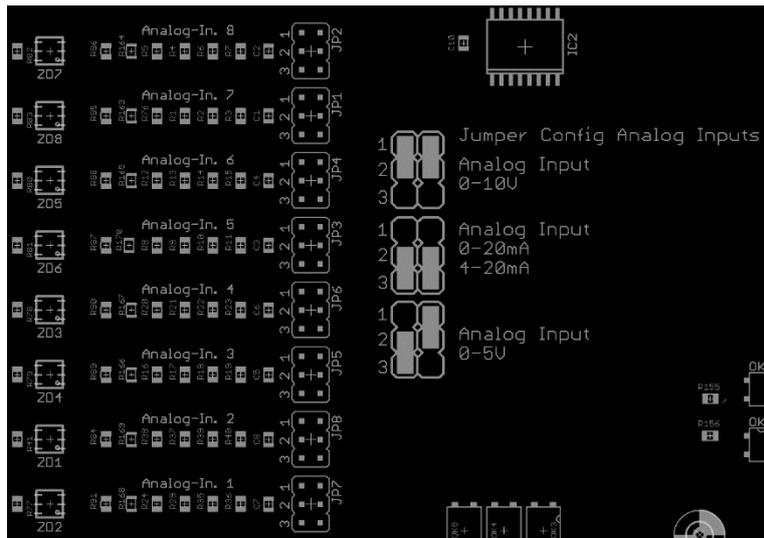


Jumperstellungen der Analog Eingänge 0-20mA bzw. 4-20mA

Beide Jumper der Analog Inputs 1-8 (Channel 1-8) sind auf **PIN 2+3** gesetzt (*Abb.2*)

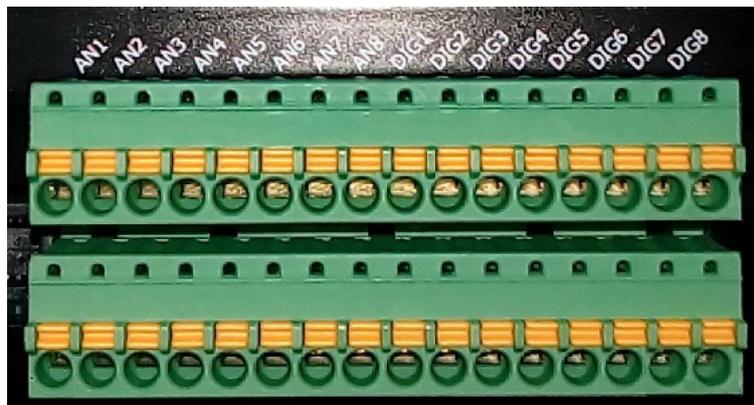
In diesen Jumperstellungen dürfen nur folgende Sensoren an die Analog Inputs angeschlossen und bei der Konfiguration des Sensor Type" in der SITEMANAGER II/v6 Configuration ausgewählt werden:

- **Custom 0-20mA**
- **Custom 4-20mA**



Digitale Eingänge über Klemmleisten

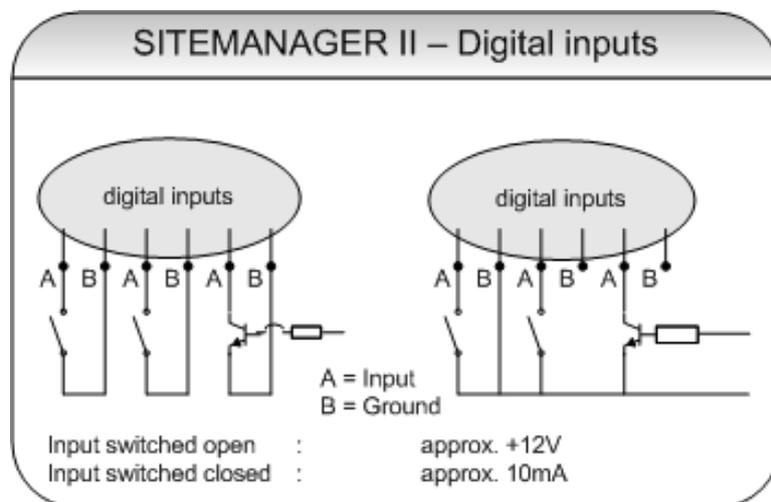
Unterhalb des analogen Inputs Anschlussbuchsen befindet sich die Klemmleiste für die 8 digitalen Eingänge.



Analogeingangsklemmleiste (A01-A08) und Digitaleingangsklemmleiste (D01-D08)

Die folgende Abbildung zeigt die Anschlussbelegung der Klemmleiste für die Digitaleingänge.

Anschlussbelegung der Klemmleiste Digitaleingänge



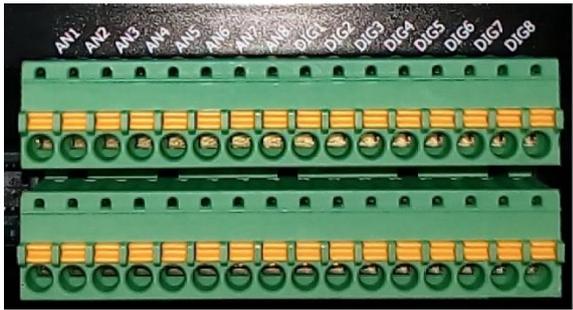


Abb.: Digital-/Analogeingänge SITEMANGER II/v6

Klemmenbezeichnung:	Anschluss:
X1 / 12V +	Betriebsspannung +12VDC
X1 / -	GND -
X2/A01	Analog Input 1
X2/A02	Analog Input 2
X2/A03	Analog Input 3
X2/A04	Analog Input 4
X2/A05	Analog Input 5
X2/A06	Analog Input 6
X2/A07	Analog Input 7
X2/A08	Analog Input 8
X2/D01	Digital Input 1
X2/D02	Digital Input 2
X2/D03	Digital Input 3
X2/D04	Digital Input 4
X2/D05	Digital Input 5
X2/D06	Digital Input 6
X2/D07	Digital Input 7
X2/D08	Digital Input 8

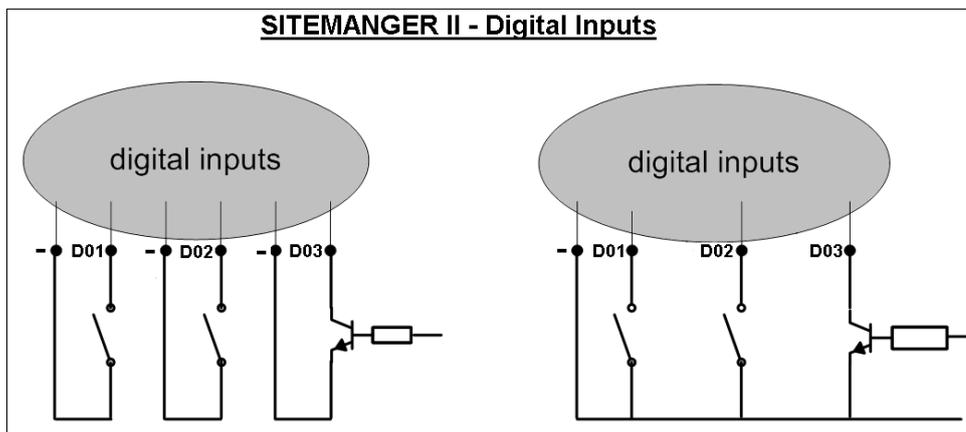
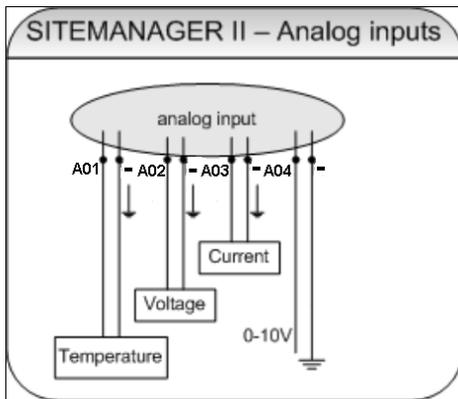
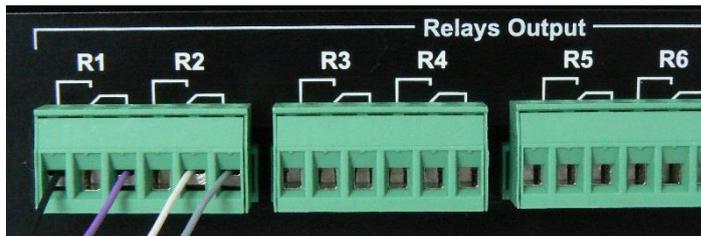
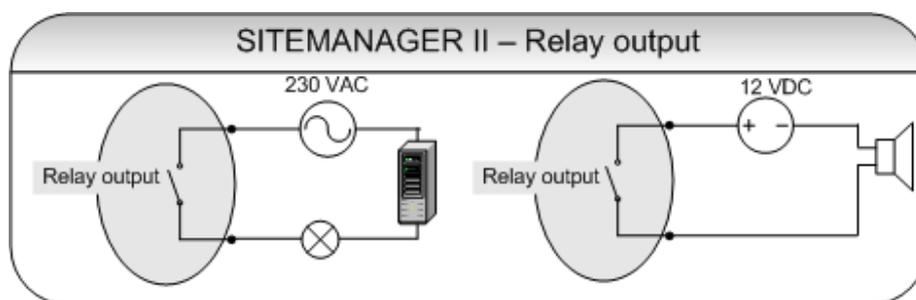


Abb.: Schaltbild Analogeingänge

Relaiskontakte über Schraubklemmen

Umschaltbare Relaiskontakte

Der SITEMANAGER II/v6 verfügt über 8 schaltbare Relaiskontakte, mit denen man Stromkreise von bis zu 250V/4A schalten kann. Jedes Relais verfügt je über einen Öffnerkontakt (NC) und einen Schließer kontakt (NO). Für Anschlussbeispiele bitte folgende Abbildung beachten.



Schaltbild: Relaiskontakt

Urheberrechts-Erklärung zum geistigen Eigentum und Umgang mit vertraulichen Informationen

Die Informationen in diesem Benutzerhandbuch sind nicht bedingte Anweisungen und können ohne Ankündigung verändert werden. Obwohl GENEREX versucht hat, präzise Informationen in diesem Dokument bereitzustellen, übernimmt GENEREX keine Verantwortung für die Genauigkeit dieser Informationen.

GENEREX ist nicht verantwortlich für jeden indirekten, speziellen, daraus folgenden oder unbeabsichtigten Schaden, ohne Einschränkungen, verlorener Gewinne oder Einkommen, Kosten von Austausch Gütern, Verlust oder Beschädigung von Daten, die sich durch den Gebrauch dieses Dokumentes oder das hier beschriebenen Produkt ergeben.

GENEREX als Hersteller der genannten Produkte, übernimmt keine Verpflichtungen mit diesen Informationen. Die Produkte, die in diesem Handbuch beschrieben werden, wurden auf der alleinigen Basis von Informationen für Geschäftspartner gegeben, damit diese ein besseres Verständnis für die GENEREX Produkte erhalten.

GENEREX erlaubt seinen Geschäftspartnern die Informationen, die in diesem Dokument enthalten sind, an Dritte weiterzugeben, ebenso an das Personal in deren Firma oder ihren eigenen Kunden, elektronisch, manuell, in Form von Fotokopien oder Ähnlichem. GENEREX gibt an, dass der Inhalt nicht verändert oder angepasst werden darf, ohne schriftliche Genehmigung von GENEREX.

Alle Rechte, Titel und Interessen am GENEREX Markenzeichen BACS oder Firmenzeichen (registriert oder nicht registriert) oder der Geschäftswert bzw. das geistige Eigentum von GENEREX, das Urheberrecht und die Produkt-Patente sind exklusiv und ohne Einschränkungen im Eigentum von GENEREX.

GENEREX wird jede Beanstandung über den Inhalt dieses Dokumentes zeitnah abwickeln. Kommentare oder Beanstandungen zu diesem Dokument sollten an die GENEREX Systems Vertriebsgesellschaft mbH adressiert werden.

Das Urheberrecht der Europäischen Union ist gültig (Copyright EU).
Copyright (c) 1995-2020 GENEREX GmbH, Hamburg, Deutschland.

Alle Rechte vorbehalten.

