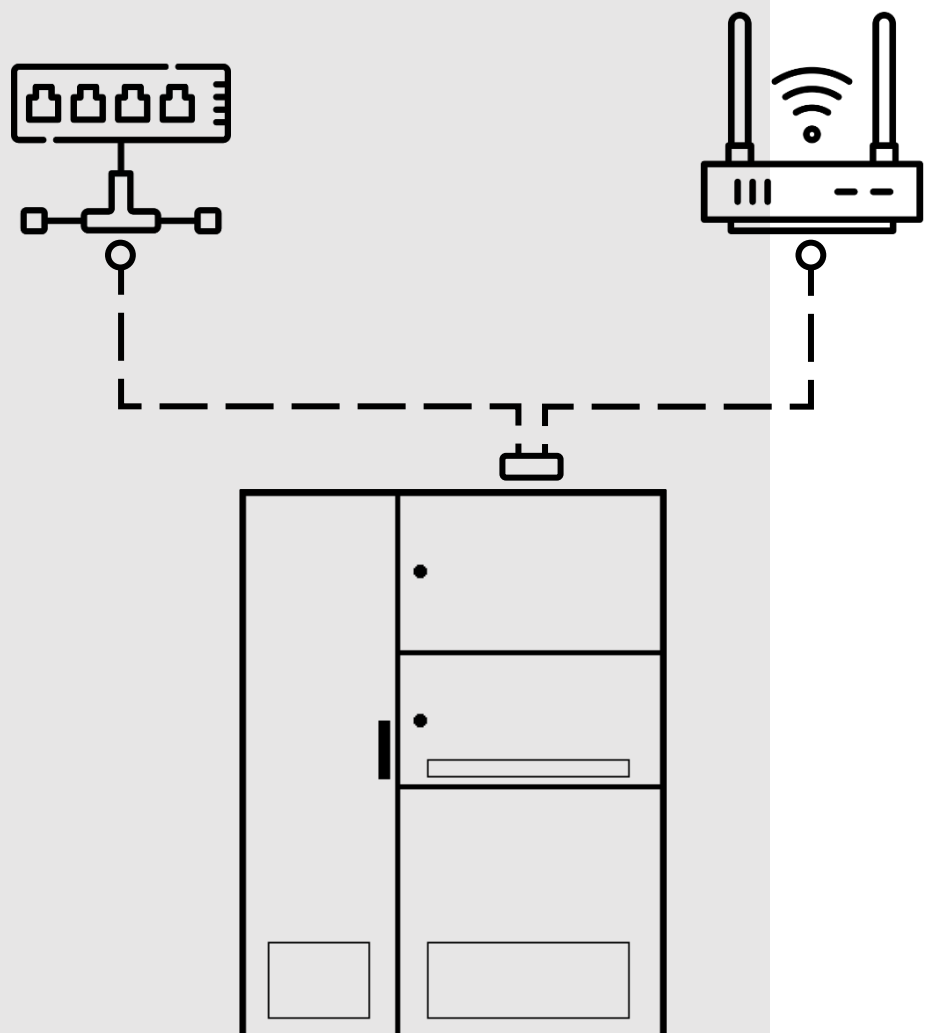


Datenverbindung

Anleitung / Leitfaden





Willkommen bei LIVARSA

bei jedem neuen Projekt versuchen wir stets den Bedürfnissen unserer Kunden gerecht zu werden und möchten sie bei ihren Projekten bestmöglich unterstützen. Jeden Tag sind wir bestrebt unsere Kunden, die sich für unsere Produkte und Dienstleistungen entschieden haben, mit höchster Qualität und großem Engagement zu unterstützen.

Es ist unsere Priorität, die Effizienz und die Firmenabläufe jedes Kunden mit unseren Produkten zu verbessern.

Danke, dass Sie sich für uns entschieden haben!

Die in diesem Dokument enthaltenen Informationen sind zum Zeitpunkt der Drucklegung auf dem neuesten Stand, können jedoch im Rahmen unserer Zielsetzung einer kontinuierlichen Produktentwicklung und -verbesserung ohne Vorankündigung oder Benachrichtigungspflicht geändert werden.

Dieses Dokument wird mit der Anlage geliefert und ist ein integraler Bestandteil des LIVARSA-Systems. Es ist zu beachten, dass bei unterschiedlichen Anweisungen in den Handbüchern die sicherste und restriktivste befolgt und angewendet werden sollte.

Die beiliegende Dokumentation ist für die beteiligten Fachpersonen bestimmt und muss daher stets aufbewahrt und dem Benutzer und Fachpersonal zugänglich gemacht werden.

Die Anlage darf nur installiert und benutzt werden, nachdem die gesamte Dokumentation vollständig gelesen und die darin enthaltenen Anweisungen befolgt wurden.



ZUSAMMENFASSUNG

1. SICHERHEITSINFORMATIONEN	4
1.1. SICHERHEITSHINWEISE & -EINRICHTUNGEN	4
1.2. PERSÖNLICHE SCHUTZAUSRÜSTUNG (PSA)	4
2. EINFÜHRUNG	5
3. BESCHREIBUNG E-CONTROLLER	5
3.1. HARDWARE	5
3.2. TASTEN	FEHLER! TEXTMARKE NICHT DEFINIERT.
3.3. LCD-DISPLAY	5
3.4. USB-ANSCHLUSS	5
3.5. ANSCHLÜSSE	5
3.6. ETHERNET ANSCHLUSS	5
4. VOR DEM START	6
4.1. ROUTER TELTONIKA RUT950	6
5. VORSCHLÄGE ZUR KONNEKTIVITÄT	7
5.1. STANDARD-KONNEKTIVITÄTSLÖSUNG	7
5.2. ISA99 BEREIT	10
5.3. VPN	12
6. INTEGRATION IN DRITTSYSTEME	13
6.1. API	13
6.2. MIDDLEWARE	13
6.3. MODBUS-REGISTERTABELLE	15
6.4. OPC UA	16
7. UNTERSTÜTZUNG	16
7.1. HILFEERSUCHEN	FEHLER! TEXTMARKE NICHT DEFINIERT.



1. SICHERHEITSINFORMATIONEN

Lesen Sie die Anweisungen in diesem Dokument sorgfältig durch und beachten Sie insbesondere die Hinweise zum Schutz vor elektrischen Gefahren.

Das Personal, das Arbeiten jeglicher Art am LIVARSA- System durchführt, muss über genaue technische Kompetenzen, besondere Fähigkeiten und Erfahrungen verfügen, die in dem jeweiligen Bereich erworben und anerkannt wurden; es muss außerdem mit den erforderlichen Arbeitswerkzeugen und angemessenem Sicherheitsschutz (PSA) gemäß den geltenden Vorschriften ausgestattet sein, um die Sicherheit und Gesundheit von Personen zu gewährleisten.

Dieses Dokument ist ein Leitfaden für die Nutzung des LIVARSA-Systems. Es darf nur für die vom Hersteller vorgesehenen Zwecke verwendet werden. Bei unsachgemäßer Verwendung können Gefahren für die Sicherheit und Gesundheit von Personen sowie wirtschaftliche Schäden entstehen.

1.1. SICHERHEITSHINWEISE & -EINRICHTUNGEN

Das System verfügt über eine Beschilderung der Schalttafel in Form von Text und Warnpiktogrammen. Beachten Sie die Warnhinweise auf der Vorderseite und den Seitenflächen des Systems.

Die nebenstehende Abbildung zeigt den Standort und die Form der verwendeten Beschilderung.

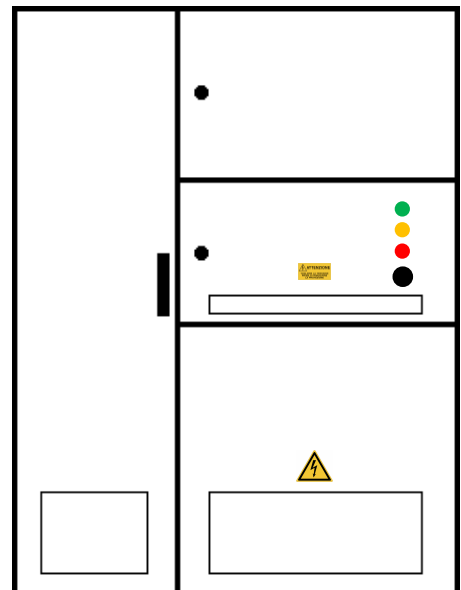
Die wichtigsten Hinweise sind im Folgenden aufgeführt.



Sie weisen auf die elektrische Gefahr hin und identifizieren mögliche stromführende Teile im Schaltschrank.

In der Mitte des LIVARSA-SYSTEMS befindet sich eine schwarzer Pilztaster. Er schaltet das System nicht stromlos und darf daher nicht als "Notaus-Knopf" oder "Stopptaster" verwendet werden.

Die Bedienung der Schalttafel muss unter Beachtung der Anweisungen in den entsprechenden Betriebshandbüchern erfolgen.



1.2. PERSÖNLICHE SCHUTZAUSRÜSTUNG (PSA)

Bei Arbeiten in der Nähe des LIVARSA-Systems muss ein geeigneter Schutz getragen werden. Bei Arbeiten an der Datenverbindung des Systems ist elektrisch isolierendes Schuhwerk nach EN ISO 20345:2011 mit der Schutzklasse S1P SRC ESD zu tragen.



2. EINFÜHRUNG

Dieses Dokument enthält alle Informationen, die für die korrekte Konfiguration des LIVARSA-Systems erforderlich sind, damit stabile Bedingungen zur Kommunikation mit dem Energia Europa-Server hergestellt werden können. Es enthält wichtige Informationen zu den relevanten Netzregeln und technische Informationen zur Implementierung und Aufbau der Datenkommunikation durch Fachpersonal.

Bevor Sie Arbeiten an dem Gerät durchführen, müssen Sie die in der "EPX LIVARSA-SYSTEM" enthaltenen Anweisungen sorgfältig lesen und verstehen. Wenden Sie sich im Zweifel an LIVARSA.

3. BESCHREIBUNG E-CONTROLLER

Der E-Controller, der im LIVARSA-System eingebaut wird, bietet die Möglichkeit, Daten zu überwachen und aufzuzeichnen, Energieberichte zu erstellen und ergänzende Analysen durchzuführen.

Der E-Controller ist eine webbasierte, programmierbare elektronische Steuerung zur Überwachung und Verwaltung automatischer Vorgänge in der Industrie.

Über eine RS485-Verbindung ist das Gerät mit den Messeinrichtungen und den Schutz- und Steuerungseinheiten der Anlage verbunden. Über eine gesicherte Internetverbindung ist die Fernwartung und -steuerung des Systems möglich.

Energia Europa hat eine Webschnittstelle entwickelt, über die der Nutzer die mit dem E-Controller ausgestatteten Anlagen direkt von einem PC aus (ferngesteuert oder lokal) verwalten kann. In diesem Fall kann der Nutzer das Verhalten und die Leistung der Systeme einsehen, Parameter zur Stromqualität überwachen oder Befehle direkt vom PC aus tätigen.

Ausführliche Informationen zur Verwendung des E-Controllers finden Sie im "EPX-Handbuch".

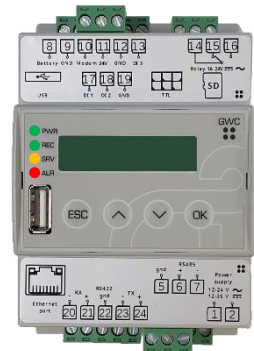
3.1. HARDWARE

Der E-Controller (Higeco, GWC 4DIN) ist die Anlagenkomponente, die für die Aufzeichnung und Datenkommunikation verwendet wird - dieses Gerät ermöglicht dem Nutzer die Interaktion mit dem LIVARSA-System.

Der E-Controller besteht aus Polymermaterial und ist für die Montage auf einer DIN-Hutschiene vorbereitet.

An der Vorderseite befinden sich LED-Leuchten, die den aktuellen Betriebsstatus visuell anzeigen.

- PWR- POWER-gespeistes Gerät;
- REC- ACTIVE Gerät ist eingeschaltet;
- SRV- SERVER Gerät, das mit dem Server verbunden ist;
- ALR- ALARM Gerät im Alarmzustand.



3.2. TASTEN

Auf der Vorderseite des E-Controllers befinden sich vier Folientaster, mit denen Sie durch das Menü navigieren und das Gerät konfigurieren können.

3.3. LCD-DISPLAY

Das LCD-Display befindet sich auf der Vorderseite des Geräts. So kann der Nutzer die Schritte nachvollziehen, die er bei der Konfiguration des Geräts durchführen muss. Es zeigt im Normalbetrieb den Geräte-Typ sowie das aktuelle Datum und die aktuelle Uhrzeit an.

3.4. USB-ANSCHLUSS

Das Gerät ist mit einem USB-2.0-Eingang vom Typ A ausgestattet, über den Upgrades des Geräts vor Ort möglich sind, die jedoch nur von spezialisiertem und autorisiertem Personal durchgeführt werden dürfen.

3.5. ANSCHLÜSSE

An der Ober- und Unterseite des E-Controllers befinden sich Phoenix Contact-Klemmenblöcke. Diese werden für die Datenübertragung von Peripheriegeräten und für die Übertragung von Signalen/Befehlen und zur Datenkommunikation verwendet.

3.6. ETHERNET ANSCHLUSS

Das Gerät ist mit einem Ethernet-Anschluss ausgestattet, an den ein Ethernet-Kabel mit RJ45-Steckern angeschlossen werden kann. Es dient zur Kommunikation über das TCP/IP-Protokoll.



4. VOR DEM EINSCHALTEN

LIVARSA empfiehlt, das LIVARSA - System über ein vorhandenes Kundennetzwerk mit dem Internet zu verbinden. Dies garantiert niedrigere Kosten, höhere Zuverlässigkeit und höhere Datenraten als eine Modem-Verbindung über einen Mobilfunkbetreiber (SIM). Sofern vom Kunden nicht anders angegeben, wird das LIVARSA-System mit aktiviertem DHCP-Client geliefert. Dies erleichtert dem Techniker des Kunden die Identifizierung im internen Netz, und bei künftigen Änderungen des internen Netzes ist es nicht erforderlich, mit LIVARSA in Kontakt zu treten, um Systemparameter zu ändern.

In diesem Abschnitt werden die Konnektivitätsoptionen und die dazu notwendigen Schritte zur Verbindung des E-Controllers mit der Energy Europe Cloud erläutert. Da es mehrere Konfigurationsmöglichkeiten gibt, wird empfohlen, dass Sie vor der Installation des LIVARSA-Systems Ihren Netzwerkadministrator mit diesem Leitfaden konsultieren, um die am besten geeignete Anschlusskonfiguration zu bestimmen.

4.1. ROUTER TELTONIKA RUT950

Im Laufe der Jahre hat LIVARSA mit dem Einsatz unterschiedlicher Verbindungsarten auseinandergesetzt. Ziel ist, den Anschluss zu erleichtern und gleichzeitig ein hohes Maß an Sicherheit zu gewährleisten.



Das LIVARSA-System wird seit August 2022 ist mit einem ROUTER ausgestattet, der auch als 4G-Dual-SIM-Modem fungiert (siehe nebenstehende Abbildung) und im SIM1-Steckplatz die firmeneigene Daten-SIM von LIVARSA enthält, die den Zugriff auf das LIVARSA-System und dessen Konfiguration aus der Ferne ermöglicht.

Vorbehaltlich des bestehenden Vertrages wird die LIVARSA-SIM-Karte aktiviert, sobald der vom Kunden festgelegte Verbindungsmodus eingestellt wurde, kann diese aus der Ferne deaktiviert werden. Diese kann von LIVARSA nur bei außerordentlichen Eingriffen aufgrund der fehlenden Anschlussmöglichkeit des Kunden aktiviert werden. LIVARSA behält sich daher das Recht vor, seine SIM-Karte zu aktivieren, um eine Störungsbeseitigung vorzunehmen, wenn die vom Kunden gewählte Verbindung nicht ordnungsgemäß funktioniert oder nicht stabil genug ist, um einen Fernzugriff zu ermöglichen.

Alle LIVARSA-Systeme sind mit einem E-Controller ausgestattet, der zur Fernsteuerung der Anlage dient. Die Anlage wird mit Weiterleitungsregeln für die im erworbenen LIVARSA-System enthaltenen Geräte ausgeliefert. Nachfolgend finden Sie eine Tabelle mit den Port-Spezifikationen und Protokollen, die verwendet werden, um Geräte aus Ihrem LAN entweder über den WAN RJ45- oder WiFi-Verbindungstyp zu erreichen. Auf Wunsch des Kunden ist es möglich, diese Weiterleitungsregeln zu ändern oder sie für eine höhere Sicherheit zu deaktivieren, falls das Gerät nicht über die RJ45- oder WiFi-Schnittstelle des WAN erreicht werden muss.

WEITERLEITUNGSREGELN:

INKOMMEN	PORT	PROTOKOLL	NAT	PRIVATE IP	PORT	PROTOKOLL
WAN/WiFi IP-Schnittstelle	443/TCP	HTTPS	AN	Teltonika	443/TCP	HTTPS
WAN/WiFi IP-Schnittstelle	8001/TCP	HTTPS		E-Controller	8001/TCP	HTTPS
WAN/WiFi IP-Schnittstelle	502/TCP	Modbus TCP		HMI	502/TCP	Modbus TCP
Zusätzliche Regeln für das Beispiel Janitza UMG 605-PRO				Zusätzliche Regeln für das Beispiel Janitza UMG 605-PRO		
WAN/WiFi IP-Schnittstelle	1024/TCP	FTP-Daten		Janitza	1024/TCP	FTP-Daten
WAN/WiFi IP-Schnittstelle	1025/TCP	FTP-Daten		Janitza	1025/TCP	FTP-Daten
WAN/WiFi IP-Schnittstelle	1026/TCP	FTP-Daten		Janitza	1026/TCP	FTP-Daten
WAN/WiFi IP-Schnittstelle	1027/TCP	FTP-Daten		Janitza	1027/TCP	FTP-Daten
WAN/WiFi IP-Schnittstelle	21/TCP	FTP		Janitza	21/TCP	FTP
WAN/WiFi IP-Schnittstelle	1502/TCP	Modbus TCP		Janitza	502/TCP	Modbus TCP
WAN/WiFi IP-Schnittstelle	8000/TCP	Modbus über Ethernet		Janitza	8000/TCP	Modbus über Ethernet



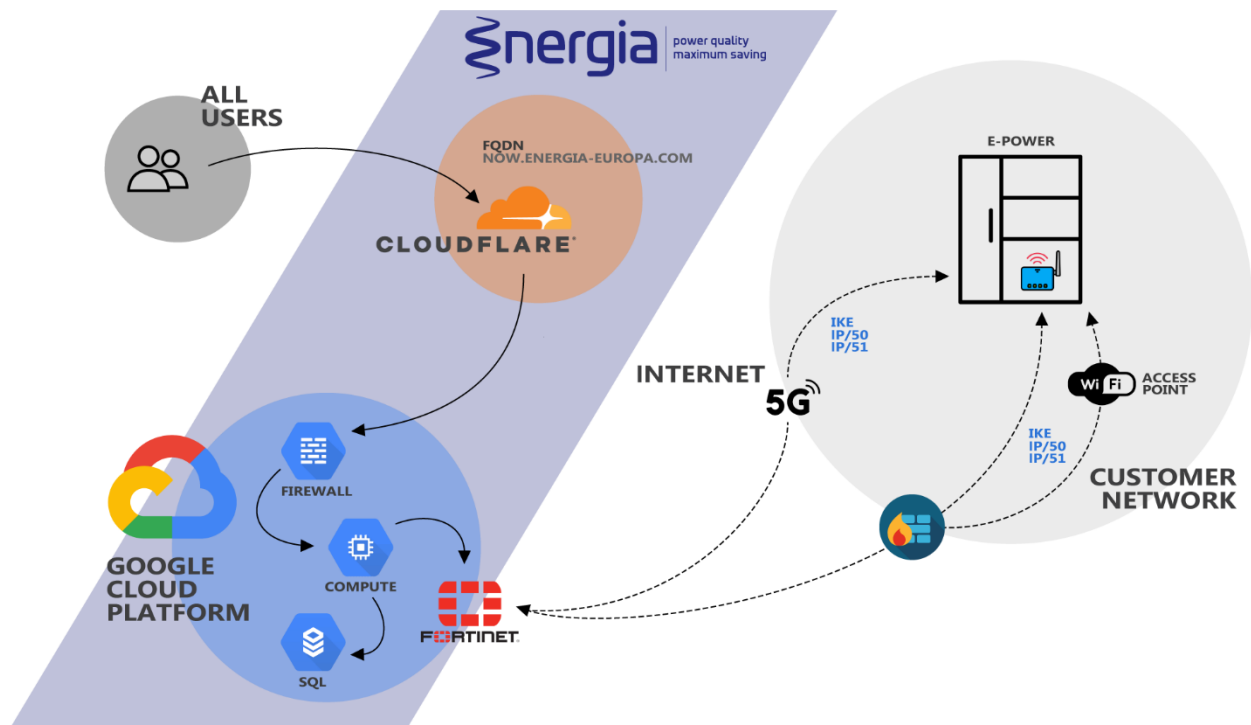
5. KONEKTIVITÄTSLÖSUNGEN

LIVARSA gemeinsam mit Energia Europa stellt den Überwachungsdienst über die Oberfläche e-powernow und den NOW-Datendienst zur Verfügung. Um diese Dienste zu ermöglichen und sie auf einem hohen Betriebsstandard zu halten, muss das LIVARSA-System in der Lage sein, mit unserer Cloud zu kommunizieren.

Im Folgenden werden alle möglichen Lösungen beschrieben, die es dem E-Controller-Gerät ermöglichen, Daten sicher an den Server zu senden. Sobald die Verbindung korrekt konfiguriert ist, kann der Nutzer über <https://now.energia-europa.com> die Daten ferngesteuert anzeigen und das LIVARSA-System steuern.

Die genannten Vorschläge beziehen sich auf eine Vielzahl von Verbindungsarten. Das Dokument gibt eine Übersicht aller von uns bereit gestellten Lösungen und ist als Leitfaden für den IT-Netzmanager zur Auswahl, der am besten geeigneten Option für Livarsa-System konzipiert. Für jede Option wird eine kurze allgemeine Beschreibung angegeben. Für IT-Fachpersonal werden in *grau unterlegter Schrift* die Optionen noch detaillierter beschrieben.

5.1. STANDARD-KONNEKTIVITÄTSLÖSUNG



Alle LIVARSA-Systeme sind über einen Standard-IPsec-Tunnel mit der Energia Europa Cloud verbunden. Jedes System besitzt seine eigene IPsec-Konfiguration welche nicht mit der eines anderen LIVARSA-Systems austauschbar ist. Diese Lösung besteht auf Hardware-Ebene aus dem Teltonika RUT950 ROUTER.

Das Gerät wird von LIVARSA standardmäßig mit einer vorkonfigurierten und betriebsbereiten SIM-Karte in dem als SIM1 bezeichneten Steckplatz geliefert:

- WAN RJ45 (Ethernet-Kabel);
- Mobilfunkbetreiber (SWISSCOM Schweiz) (SIM-Karte);
- WiFi.

Diese Konfiguration bietet mehrere Möglichkeiten, sich mit dem Internet zu verbinden und unsere Cloud zu erreichen. Je nach den Bedürfnissen des Kunden können eine oder mehrere Verbindungen gleichzeitig konfiguriert werden, wobei die Schnittstellen in der von Energia Europa verwalteten und programmierten Failover-Konfiguration nach den Vorgaben des Kunden priorisiert werden.

5.1.1. SIM

Im LIVARSA-System befindet sich ein ROUTER mit integriertem Mobilfunk-Modem, in den Sie die SIM-Karte in Steckplatz SIM1 einlegen, um die Hauptverbindung zur Energia Europa Cloud aufbauen zu können.

Der SIM-Karte muss auf der Seite, an der die Antennen mit den SMA-Steckern angeschlossen sind, in den Steckplatz SIM1 eingesetzt werden. Um den SIM-Kartenhalter bestücken zu können, muss dieser mit einem geeigneten Werkzeug (Stift mit 1 mm Breite und 10 mm Länge) zunächst geöffnet werden.



Die SIM-Karte des Kunden muss die folgenden Merkmale aufweist:

- Mindestens 500 MB Datenverkehr pro Monat.
Wenn Sie Ihre durch einen PIN-Code geschützte SIM-Karte einsetzen möchten, müssen Sie sich per E-Mail mit LIVARSA in Verbindung setzen und die folgenden Informationen angeben:
 - Die Seriennummer auf dem ROUTER, Beispiel: 201-000-001-128;
 - Der Name des Zugangspunkts (APN), der eingestellt werden soll, Beispiel: internet.com;
 - Der PIN-Code der SIM-Karte, die in den SIM1-Steckplatz eingelegt ist.

Informieren Sie sich bei Ihrem Mobilfunkbetreibers welcher Eintrag für den APN einzugeben ist.

Energia Europa stellt seinen Kunden eine Anwendung zur Verfügung, mit der sie den APN für den SIM1-Slot in einfachen Schritten konfigurieren und die relative Signalqualität (angegeben in DBm), überwachen können.

Laden Sie die E-Modem-App aus dem Play Store herunter (für iOS-Geräte ist die App noch nicht verfügbar); die entsprechende Bedienungsanleitung können Sie über den QR-Code rechts herunterladen.



5.1.2. ETHERNET RJ-45

Das LIVARSA-System ist mit der Funktion ausgestattet, eine LAN-Verbindung über das Firmennetz des Kunden auszuhandeln, unabhängig davon, welche Verbindung als Hauptverbindung für die Datenübertragung gewählt wird.

Die für diese Konfiguration anzuschließende Schnittstelle ist in der Komponente ROUTER als WAN angegeben. In diesem Fall kann festgelegt werden, ob diese Verbindung als Hauptverbindung zur Energia Europa Cloud oder nur als sekundäre Verbindung für die Verbindung mit dem Verwaltungssystem des Kunden genutzt werden soll.

Wenn der direkte LAN-Anschluss als Standard-Verbindungsmethode zur Energia Europa Cloud definiert ist, ist es wichtig, dass die Firewall die folgenden Protokolle in der Tabelle unten zulässt.

AUSGEHENDE REGELN:

SOURCE	PROTOKOLL	DESTINATION	PORT
IP-WAN-Schnittstelle	IKE	FQDN: be.firewall.energia-europa.com	4500/UDP
IP-WAN-Schnittstelle	IKE	FQDN: be.firewall.eneria-europa.com	500/UDP
IP-WAN-Schnittstelle	IP/50 (ESP)	FQDN: be.firewall.energia-europa.com	
IP-WAN-Schnittstelle	IP/51 (AH)	FQDN: be.firewall.energia-europa.com	

Bevor Sie den E-Controller über ein RJ45-Kabel anschließen, muss gewährleistet sein, dass sich im angeschlossenen LAN ein DHCP-Server vorhanden ist - dies erleichtert die Konfiguration. Der Vorteil dieser Konfiguration besteht darin, dass die Netzwerkparameter jederzeit von Ihrem Netzwerkadministrator geändert werden können, ohne dass ein Eingriff seitens Energia Europa erfolgen muss.

Unverzichtbare Netzparameter:

- IP-Adresse;
- Netzmaske;
- Gateway;
- DNS.

Der Kunde muss die entsprechende Verkabelung von den Netzwerkgeräten zum LIVARSA-System mittels eines Ethernetkabels mit RJ45-Steckern selbst vornehmen. Wir empfehlen eine maximale Länge von 50 Metern.

Wenn es im LAN keinen DHCP-Server gibt, muss LIVARSA eingreifen, um die Schnittstelle korrekt zu konfigurieren; teilen Sie in diesem Fall die oben aufgelisteten Parameter per E-Mail mit.

5.1.3. WIFI

Der im LIVARSA-System installierte ROUTER ist außerdem mit WiFi-Antennen ausgestattet, über die er mit dem WLAN des Kunden verbunden werden kann, unabhängig davon, welche Verbindung als Hauptverbindung für die Datenübertragung gewählt wird. Diese Konfiguration schließt die Möglichkeit aus, den Status der in Steckplatz SIM1 eingelegten SIM-Karte über die mobile Anwendung zu konfigurieren und anzuzeigen. Um diese Art der Verbindung zu konfigurieren, muss ein WiFi-Netz eingerichtet werden, welches vom LIVARSA-System aus erreichbar ist. Es wird empfohlen, dass ein Techniker nach der Einrichtung des Netzes die Qualität der Abdeckung am Installationsort des Systems mit einem mobilen Gerät misst.

Das Personal von Energia Europa kann diese Verbindung aus der Ferne konfigurieren, allerdings muss der Kunde Energia Europa die folgenden Parameter per E-Mail mitteilen:

- SSID;
- Kennwort.

Bei der oben erwähnten Ethernet-Verbindung kann festgelegt werden, ob diese Art von Verbindung als Hauptverbindung oder als Dienstverbindung verwendet werden soll, die dem Kunden für die Verbindung mit seinem eigenen Verwaltungssystem zur Verfügung steht.



Wenn diese Lösung als Standard-Verbindungsmethode zur Energia Europa Cloud definiert ist, ist es wichtig, dass die Firewall die folgenden Protokolle zulässt.

AUSGEHENDE REGELN:

SOURCE	PROTOKOLL	DESTINATION	PORT
IP-WAN-Schnittstelle	IKE	FQDN: be.firewall.energia-europa.com	4500/UDP
IP-WAN-Schnittstelle	IKE	FQDN: be.firewall.energia-europa.com	500/UDP
IP-WAN-Schnittstelle	IP/50 (ESP)	FQDN: be.firewall.energia-europa.com	
IP-WAN-Schnittstelle	IP/51 (AH)	FQDN: be.firewall.energia-europa.com	

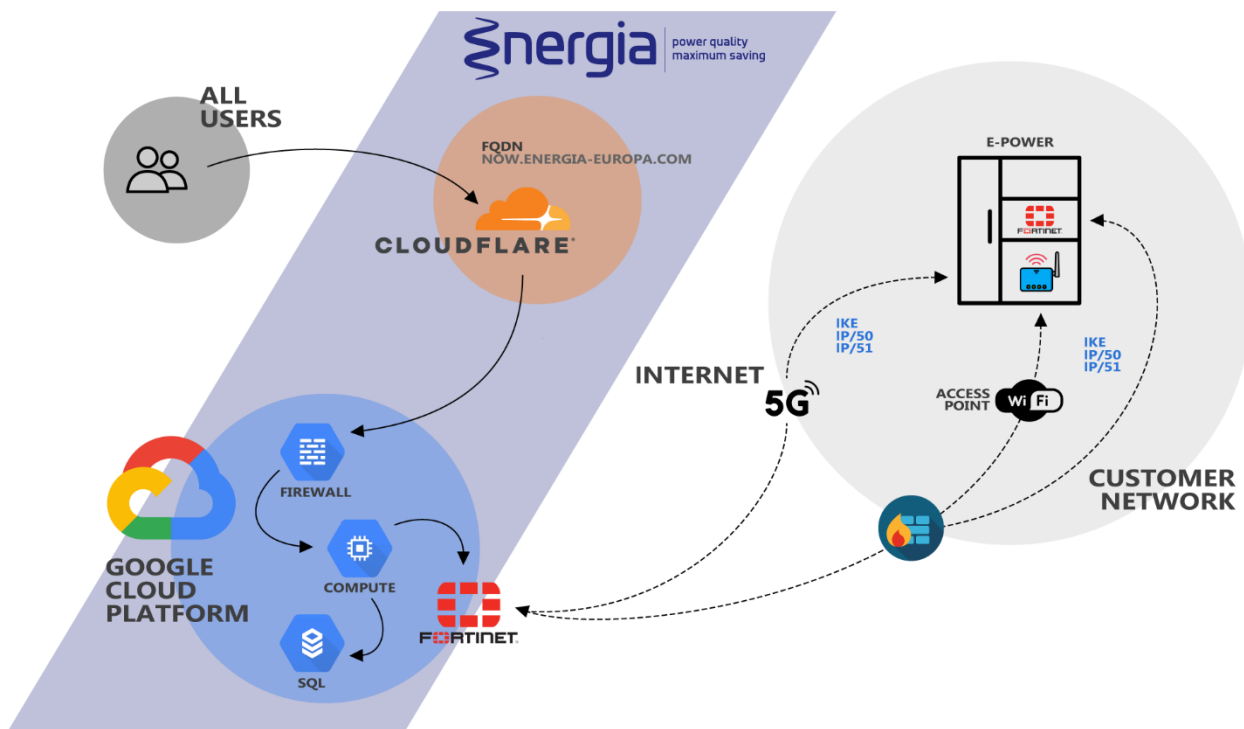
Diese Arten von Verbindungen können von Energia Europas Team mittels Fernzugriff konfiguriert werden. Alle Schnittstellen sind mit DHCP-Clients ausgestattet, um den Anschluss am LIVARSA-System durch externe Netzwerktechniker zu erleichtern. Wenn jedoch kein DHCP-Server im Netzwerk vorhanden ist, können die Parameter auch manuell konfiguriert werden, indem eine E-Mail an Energia Europa mit folgenden Informationengesendet wird:

1. IP;
2. Netzmaske;
3. Gateway;
4. DNS.

Die gesamte Konfiguration des LIVARSA-Systems in Bezug auf die Konnektivität des E-Controllers wird ausschließlich von LIVARSA verwaltet. Es ist möglich, die Art des Anschlusses und/oder die Konfiguration zu einem späteren Zeitpunkt zu ändern, indem Sie eine E-Mail an den technischen Kundendienst an LIVARSA senden.

Wie oben beschrieben, ist es möglich, mehrere Konnektivitäten gleichzeitig zu verwalten, indem festgelegt wird, auf welcher Schnittstelle die IPsec-Verbindung primär verwendet werden soll; die anderen Konnektivitäten werden möglicherweise als Failover-Verbindungen beibehalten.

5.2. ISA99 READY



Diese Lösung wird vorwiegend von den Kunden gewählt, die ein hohes Maß an IT-Sicherheit benötigen. Sie entspricht dem ISA99-Standard und ist vorbereitet für die ISA99-Zertifizierung.

Die Norm IEC62443, auch bekannt als ISA99, sie dient als Leitlinie für den Aufbau einer ICS-Infrastruktur (Industrial Control Systems), die vor den ständig zunehmenden Cyber-Bedrohungen sicher ist. So wie die Datenschutz-Grundverordnung zu einem Standard geworden ist, den alle Unternehmen einhalten müssen, ist zu hoffen, dass auch ISA99 zu einem verbindlichen Standard wird, der in allen ICS-Einrichtungen angewendet werden muss bei denen potenzielle Bedrohungen bestehen:

- Gefährdung der öffentlichen Sicherheit oder der Mitarbeiter;
- Verlust des öffentlichen Vertrauens;
- Verstoß gegen die gesetzlichen Bestimmungen;
- Verlust von geschützten oder vertraulichen Informationen;
- Wirtschaftlicher Schaden;
- Auswirkungen auf die nationale Sicherheit.

Diese Konfiguration ist die sicherste Variante und auch einfach zu installieren, da die bordeigene Firewall (Fortinet 40F) bereits vollständig konfiguriert und eingerichtet mitgeliefert wird. Mit ihr wird ein Standard-IPsec-Tunnel mit der Energia Europa Cloud aufgebaut.

Das Fortinet 40F wird, sofern im Vertrag nicht anders angegeben, ohne Lizenzen geliefert, da diese mit monatlichen Kosten verbunden sind. In der Praxis ist es oft so, dass das Gerät bereits hinter der Firewall des Kunden mit genau definierten Betriebsregeln installiert ist und auch häufig ohne Lizenzvertrag betrieben wird. Wenn die Firewall nicht lizenziert ist, beeinträchtigt dies keine der in diesem Handbuch beschriebenen Funktionen. Der einzige Unterschied besteht darin, dass der IPS- und Antivirus-Filter nicht auf den Datenverkehr angewendet wird, der von den physischen Schnittstellen des Geräts selbst kommt, während die Verbindungen, die durch den IPsec-Tunnel laufen, durch die auf der Cloud installierte Energia Europa-Lizenz geschützt werden.

Die Lizenzen können jederzeit aktiviert werden, danach werden die Kosten hierfür jährlich und im Voraus in Rechnung gestellt. Die Firewall ist immer bereit, sich über eine WAN-Schnittstelle mit dem Netz des Kunden oder über Port A mit der Cloud zu verbinden, wobei der von Energia Europa verkaufte Fortinet-ROUTER als Failover-Schnittstelle angeschlossen wird. Diese Lösung besteht auf der Hardware-Ebene aus dem Model Fortinet 40F.

Kurze Beschreibung der Schnittstellenkonfiguration:

- **WAN:** Verbindung zum Netz des Kunden;
- **A:** Anschluss an ROUTER Energia Europa;
- **1:** Dient zum Anschluss des in Abschnitt 3 dieses Handbuchs beschriebenen E-Controller-Geräts;
- **2:** Dient zum Anschluss eines beliebigen Netzanalysators mit RJ-45-Schnittstelle, z. B. zur Messung der Netzqualität direkt aus dem Kundensystem;
- **3:** Dient zum Anschluss des E-Power HMI-Geräts (Touch-Display).



Standardmäßig werden die folgenden NAT-Regeln vom WAN-Port auf die mit der Firewall verbundenen Geräte angewendet.

INBOUND REGELN:

INKOMMEN	PORT	PROTOKOLL	NAT	PRIVATE IP	PORT	PROTOKOLL
IP-WAN-Schnittstelle	8001/TCP	HTTPS	AN	E-Controller	443/TCP	HTTPS
IP-WAN-Schnittstelle	8443/TCP	HTTPS		ROUTER	443/TCP	HTTPS
IP-WAN-Schnittstelle	502/TCP	Modbus TCP		HMI	502/TCP	Modbus TCP
IP-WAN-Schnittstelle	4840/TCP	OPC UA		HMI	4840/TCP	OPC UA
Zusätzliche Regeln für das Beispiel Janitza UMG 605-PRO				Zusätzliche Regeln für das Beispiel Janitza UMG 605-PRO		
IP-WAN-Schnittstelle	1024/TCP	FTP-Daten		Janitza	1024/TCP	FTP-Daten
IP-WAN-Schnittstelle	1025/TCP	FTP-Daten		Janitza	1025/TCP	FTP-Daten
IP-WAN-Schnittstelle	1026/TCP	FTP-Daten		Janitza	1026/TCP	FTP-Daten
IP-WAN-Schnittstelle	1027/TCP	FTP-Daten		Janitza	1027/TCP	FTP-Daten
IP-WAN-Schnittstelle	21/TCP	FTP		Janitza	21/TCP	FTP
IP-WAN-Schnittstelle	1502/TCP	Modbus TCP		Janitza	502/TCP	Modbus TCP
IP-WAN-Schnittstelle	8000/TCP	Modbus über Ethernet		Janitza	8000/TCP	Modbus über Ethernet

Dieses Anschlusssystem ermöglicht sowohl dem Techniker von LIVARSA als auch dem Kunden den direkten Zugriff auf die Konfiguration jedes angeschlossenen E-Controller-Geräts über die zugeordneten Protokolle; wichtig hierbei ist auch die Möglichkeit, die APN des ROUTERS zu ändern ohne dabei den Schaltschrank öffnen zu müssen.

Um die Verbindung mit der Energia Europa Cloud ordnungsgemäß herzustellen, müssen die in der nachstehenden Tabelle aufgeführten Protokolle und Ports zugelassen werden.

AUSGEHENDE REGELN:

SOURCE	PROTOKOLL	DESTINATION	PORT
IP-WAN-Schnittstelle	IKE	FQDN: be.firewall.energia-europa.com	4500/UDP
IP-WAN-Schnittstelle	IKE	FQDN: be.firewall.energia-europa.com	500/UDP
IP-WAN-Schnittstelle	IP/50 (ESP)	FQDN: be.firewall.energia-europa.com	
IP-WAN-Schnittstelle	IP/51 (AH)	FQDN: be.firewall.energia-europa.com	

Energia Europa verpflichtet sich, mit der angegebenen Kontaktperson die für die korrekte Herstellung der Verbindung erforderlichen Informationen auszutauschen und wird keine Einstellungen in der Firewall des Kunden ändern. Für die Konfiguration der Firewall empfiehlt Energia Europa gegebenenfalls einen externen Partner, der sich auf die Konfiguration von Computernetzen spezialisiert hat.

Falls erforderlich, installiert Energia Europa den Netzanalysator des Kunden zum Zeitpunkt des Baus der Maschine und konfiguriert die WAN-Schnittstelle und ihre NAT-Regeln entsprechend, um die Interoperabilität zu ermöglichen.

Es kann vorkommen, dass die IT-Abteilung selbst auf die Firewall zugreifen möchte, um NAT-Regeln und Richtlinien zu ändern, um beispielsweise Sicherheitsniveau zu ändern/erhöhen. In diesem Fall stellt Energia Europa ein lokales Konto oder eine RADIUS-Konfiguration des Kunden zur Verfügung, um die Umsetzung der Anpassungen/Änderungen zu erleichtern.

Im VLAN, an das die WAN-Schnittstelle der Firewall angeschlossen werden soll ist ein DHCP-Server empfohlen, um die Konfiguration zu erleichtern. Wir möchten darauf hinweisen, dass der Vorteil dieser Konfiguration darin besteht, dass die Netzwerkparameter jederzeit von Ihrem Netzwerkadministrator geändert werden können, ohne dass Energia Europa oder eine autorisierte Person am Gerät eingreifen muss.

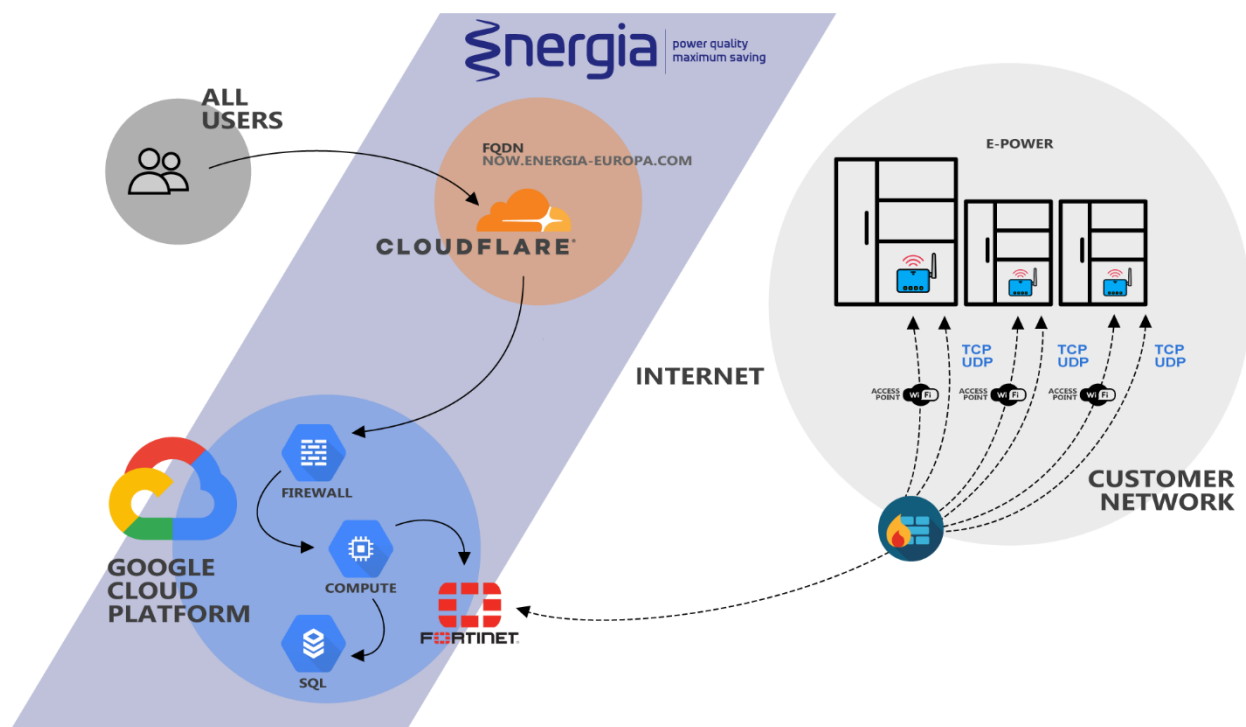
Alternativ können Sie die Netzwerkparameter auch manuell in der Firewall konfigurieren (statische Adressen); allerdings müssen Sie sich an den technischen Support von Energia Europa wenden, um sie später zu ändern.

Benötigte Netzparameter:

- IP-Adresse;
- Netzmaske;
- Gateway.

Sofern vom Kunden nicht anders angegeben, liefert Energia Europa die Firewall mit der im DHCP-Modus konfigurierten WAN-Schnittstelle aus, um so die Konfiguration zu erleichtern.

5.3. VPN



Diese Lösung wird von unseren Kunden mit vielen Filialen bevorzugt. Sie muss mit den jeweiligen IT-Abteilungen des Kunden und Energia Europa abgestimmt werden. Der Aufbau dieser Variante erfordert in der Regel eine enge Abstimmung und genaue Planung zusammen mit Energia Europa. Diese Konfiguration erfordert eine Erweiterung des VLANs innerhalb des **MPLS**-Netzes des Kunden. Der erweiterte VLAN-Bereich des Netzes umfasst dabei nur die Geräte von Energia Europa, so dass höchste Sicherheitsstandards gewährleistet sind. Diese IT-technisch aufwändige Konfiguration vereinfacht im Weiteren die Installation bei Folge-Aufträgen und dem über Jahre verteilten Ausbau mit LIVARSA-Systemen.

Nachstehend finden Sie eine Beispiel-Tabelle, die die erforderlichen Mindestangaben enthält. Alle Parameter können von den jeweiligen IT-Abteilungen ausgehandelt werden, um die am besten geeigneten Einstellungen zu finden. In diesem Fall muss sich der IT-Netzmanager des Kunden mit dem IT-Netzmanager von Energia Europa in Verbindung setzen.

IKE-Sitzung V2			
VPN-Peer	FQDN: be. firewall.energia-europa.com	Fern-Peer-VPN	IP-Firewall
Verschlüsselungsalgorithmus	AES (Schlüsselgröße 256)	Hashing-Algorithmus	SHA-1
Diffie-Hellman-Gruppe	Gruppe 2	Rekey-Zeitintervall	28800
Authentifizierungsmodus	Gemeinsam genutzte Schlüssel		gemeinsam definieren
IPSec-Sitzung			
IP LAN Energie Europa	gemeinsam definieren	IP LAN Kunde	gemeinsam definieren
Verschlüsselungsalgorithmus	AES (Schlüsselgröße 256)	Hashing-Algorithmus	SHA-1
Rekey-Zeitintervall	3600 Sekunden	Perfektes Vorwärtsgeheimnis	Ja
		Diffie-Hellman-Gruppe	Gruppe 2

Energia Europa verpflichtet sich, mit der angegebenen Kontaktperson die für die korrekte Herstellung der Verbindung erforderlichen Informationen auszutauschen und wird keine Einstellungen in der Firewall des Kunden ändern. Für die Konfiguration der Firewall empfiehlt Energia Europa gegebenenfalls einen externen Partner, der sich auf die Konfiguration von Computernetzen spezialisiert hat.



Die Implementierung dieser Lösung erfordert, dass beide Parteien die über den Tunnel auszutauschenden Netze definieren; die gesamte Kommunikation wird in dem geschaffenen Tunnel gekapselt und der gesamte Datenverkehr wird verschlüsselt, um die Kommunikation sicher zu machen.

Ein DNS-Server wird im Netz nicht benötigt, da keine Namensauflösung erforderlich ist; es wird eine Adresse aus dem definierten Pool gewählt, um den Server mit dem HTTPS-Protokoll über den Tunnel zu erreichen. Es wird empfohlen, das Netzwerk an der Firewall zu terminieren, damit alle E-Controller-Geräte zentral verwaltet werden können. Bei aktiviertem DHCP-Server-Dienst können so die Adressen der genannten E-Power-Systeme reserviert werden. Die Protokolle, die dem definierten Pool zur Kommunikation mit den E-Controller-Geräten erlaubt werden, sind immer SSH und HTTPS.

In Anbetracht des Sicherheitsniveaus des Netzes wird es daher immer notwendig sein, den Zugang über SSH durch das Cloud-System von Energia Europa zu ermöglichen.

Integration in DRITTSYSTEME

Die Daten in dem von Energia Europa betriebenen Portal <https://now.energia-europa.com/> können in vom Kunden genutzte Drittsysteme integriert werden.

5.4. API

Über einen API-Dienst (Application Programming Interface) besteht die Möglichkeit, die von den E-Power-Systemen gesammelten Daten in unterschiedlichste Verarbeitungs-/Visualisierungssysteme des Kunden zu integrieren.

Durch die Nutzung dieses Dienstes ist es ferner möglich, Software von Drittanbietern, wie z. B. ein Unternehmensmanagementsystem, einzubinden, um die vom E-Power-System gesammelten Daten vom Server herunterzuladen. Die Funktionsweise dieses Dienstes wird unter dem folgenden Link beschrieben, der alle erforderlichen Schritte aufzeigt:

<https://now.energia-europa.com/doc/>

Die zu verwendenden Anmeldeinformationen sind die gleichen wie die, die für den Zugang zum Portal <https://now.energia-europa.com/> verwendet werden.

Die für das Herunterladen historischer Daten erforderlichen Schritte sind nacheinander auszuführen. Für den Fall, dass die Software von Drittanbietern nicht in der Lage ist, HTTPS-Anfragen zu verarbeiten oder eine JSON-Datei zu analysieren, stellt Energia Europa eine in Bash geschriebene Open-Source-Software zur Verfügung, die die Daten über HTTPS-Anfragen entgegennimmt und die Ausgabe in eine angepasste csv-Datei umwandelt. Diese Software ist im öffentlichen Repository auf github.com unter <https://github.com/energia-source/higeco-integration-tool> verfügbar.

Es wurde Notwendigkeit, die Bash-Syntax für die Realisierung dieser Software zu verwenden, da sie die Basis zur Vereinfachung künftiger Installations- und Änderungsroutinen ist. Die Software kann in einem Docker oder in einem Linux-VPS in der Unternehmensinfrastruktur des Kunden ausgeführt werden, um so eine größere Sicherheit zu gewährleisten, da sie von anderen Systemen getrennt ist.

Wenden Sie sich an den technischen Kundendienst von Energia Europa, um weitere Einzelheiten zu erfahren und gegebenenfalls eine Betriebsvorführung anzufordern.

5.5. MIDDLEWARE

Für den Fall, dass der Kunde Daten direkt aus dem LIVARSA-System abrufen oder Programmierbefehle an das System senden möchte, hat Energia Europa ein Tool entwickelt, das eine einfache Schnittstelle zwischen LIVARSA-System und dem Fremdsystem über HTTPS-Aufrufe ermöglicht.

Dieses Tool ist in Bash geschrieben, um die Kompatibilität mit verschiedenen Betriebssystemen zu gewährleisten. Darüber hinaus kann es in einem Docker oder einem Linux-VPS in der Unternehmensinfrastruktur des Kunden ausgeführt werden, um eine größere Sicherheit zu gewährleisten, da es von anderen Systemen getrennt ist.

Wir raten davon ab, die Software zu ändern, da die von diesem Tool angezeigten Befehle diejenigen sind, die Energia Europa für die Fernausführung ausgewählt hat.

Um sich beim Host anzumelden und mit dem LIVARSA-System zu kommunizieren, benötigen Sie die korrekten Zugangsdaten, die Ihnen von Energia Europa zur Verfügung gestellt werden; diese sind nicht dieselben wie die, die für den Zugang zum Portal <https://now.energia-europa.com/> verwendet werden.

Das Netz des Kunden muss so konfiguriert werden, dass HTTPS-Anfragen an die E-Controller weitergeleitet werden können, mit denen sie interagieren möchten.

Mit diesem Tool ist das möglich:

- Sofortiger Daten-Download;
- Initiierung der Befehle Bypass und Speichern;
- Festlegen der Spannungsregeln.

Den vollständigen Leitfaden mit Beispielen finden Sie unter: <https://github.com/energia-source/higeco-gwc-connector>.



6.2.1. BEISPIEL FÜR DIE VERWENDUNG DES GWC-CONNECTORS

Nachfolgend finden Sie ein Beispiel für die Implementierung der GWC-Connector-Middleware in einem Managementsystem.

The screenshot displays the Livarsa management system interface. At the top, there's a header bar with the title 'Livarsa - Energie Europa SpA - Utente: MicroAdmin - Data operations: [11/04/2022]'. Below this, a sidebar on the left contains navigation icons for 'Home', 'Config', 'Data', 'Reports', 'Settings', and 'Help'. The main content area is divided into several sections:

- Configuration:** Includes fields for 'Username' (utente), 'Password' (masked), 'IP Address' (https://192.168.180.180:8078), 'Protocol' (HTTPS), 'E-Controller' (192.168.88.100), and 'Port' (8001).
- Command:** A section for sending commands, with a 'Value' field set to '0.00' and a 'Set' button.
- Data:** A section showing various data points and their status. It includes a table with columns: 'Line', 'Utc', 'threshold', 'Level', 'Percentage', 'total_saving_economic', 'total_saving_energy', 'total_saving_carbon_dioxide', 'total_saving_power_peak', 'v12n', and 'v12m'. The table contains 10 rows of data.
- Buttons:** A 'Data update' button is located at the bottom right of the data section.

The bottom status bar indicates 'Modificato: Genova 8/07/2021 11:05'.

Oben sehen Sie ein Beispiel, in dem die Parameter eingegeben werden, die erforderlich sind, um einen Authentifizierungs-Header (HTTP Basic Authentication Header) zu erhalten. Dieser ist notwendig, um alle Anfragen an das LIVARSA-System abzusetzen. Weiterhin sind die IP-Adresse mit Port vom LIVARSA-System und das Protokoll (HTTP/HTTPS), mit dem die Middleware Anfragen an den Rechner stellen wird dargestellt.

Darunter befindet sich ein Abschnitt, mit dem Befehle gesendet werden können, um das System in den Bypass bzw. Savings-Modus zu versetzen oder einen Mindestspannungsschwellenwert einzustellen (Spannungsregeln).

Im unteren Bereich gibt es einen Abschnitt, in dem die aktuellen System-Daten und deren Verlauf angezeigt werden - die Schaltfläche "Datenaktualisierung" bewirkt die Anzeige der Daten in Echtzeit.



5.6. MODBUS-REGISTERTABELLE

Beim LIVARSA-System, die mit einem HMI-Bildschirm ausgestattet sind, ist es möglich, durch Anschluss an den WAN-Port des ROUTERS oder Fortinet 40F die vom System gesammelten Daten über das Modbus/TCP-Protokoll abzufragen, um sie dann in Ihrem Datenverarbeitungssystem zu speichern. Nachfolgend finden Sie die Modbus-Tabellen aller Register innerhalb des HMI-Bildschirms. Für die Lesefunktionen gilt folgende Tabelle, sie gilt für alle Modbus-Funktionen 01

Adresse	Wörter zählen	Beschreibung	Datentyp
200	1	Vout-Kontrolle	Bool
202	1	Zugelassene Stufe 1	Bool
204	1	Zugelassene Stufe 2	Bool
206	1	Zugelassene Stufe 3	Bool
208	1	Zugelassene Stufe 4	Bool
210	1	Bypass	Bool
214	1	Sicherheits-Bypass	Bool
216	1	Bypass von e-power jetzt	Bool
218	1	Integrierter Bypass	Bool
220	1	Bypass-Alarm	Bool
222	1	Überstrom	Bool
224	1	Übertemperatur	Bool
226	1	Primärschutz des QS3-Filters	Bool
228	1	CM0	Bool
230	1	CPB	Bool
232	1	Verbindung zum Server unterbrochen	Bool

Die folgende Tabelle gilt sowohl für Modbus 03- als auch für Modbus 04-Funktionen

Adresse	Wörter zählen	Beschreibung	Einheit	Typ Daten
1000	2	V L1-N	Volt	IEEE 754
1002	2	V L2-N	Volt	IEEE 754
1004	2	V L3-N	Volt	IEEE 754
1006	2	A L1	Ampere	IEEE 754
1008	2	A L2	Ampere	IEEE 754
1010	2	A L3	Ampere	IEEE 754
1012	2	PF	Leistungsfaktor	IEEE 754
1014	2	W	Watts	IEEE 754
1016	2	Var	Var	IEEE 754
1018	2	kWh	KiloWatt pro Stunde	IEEE 754
1020	2	kVarh	KiloVar pro Stunde	IEEE 754
1022	1	Position*	Binär	UINT 16
1023	2	Vout lesen	Volt	IEEE 754
1025	2	Vout ändern	Volt	IEEE 754
1027	2	Warnungen**	Binär	UINT 32
1500	2	Sparen	Prozentsatz	IEEE 754
1502	2	Energieeinsparung	KiloWatt pro Stunde	IEEE 754
1504	2	CO2	Kilogramm	IEEE 754
1506	2	Photovoltaik-Äq.	kWp	IEEE 754
1508	2	Haus eq.	Abitation	IEEE 754

* Die nachstehende Tabelle wird für die Effizienzsteuerung der Anlage verwendet

** Bei Fehlern ist die Tabelle wie folgt aufgebaut, sie bezieht sich auf Bits und nicht auf ganze Register

BIT-Warnung	Modbus-Referenzregister 01	
1	200	Vout-Kontrolle
2	202	Zugelassene Stufe 1
3	204	Zugelassene Stufe 2
4	206	Zugelassene Stufe 3
5	208	Zugelassene Stufe 4
6	210	Bypass
7	214	Sicherheits-Bypass
8	216	Bypass von e-power jetzt
9	218	Integrierter Bypass
10	220	Bypass-Alarm
11	222	Überstrom
12	224	Übertemperatur
13	226	Primärschutz bei QS3
14	228	CM0

15	230	CPB
16	232	Verbindung zum Server unterbrochen
BIT-Position		Modbus-Referenzregister 03/04
1		Bypass
2		Stufe 1
3		Stufe 2
4		Stufe 3
5		Stufe 4
6		Antrag auf Umgehung
7		Ebene 1 Anfrage
8		Stufe 2 Antrag
9		Stufe 3 Antrag
10		Stufe 4 Antrag



Die einzig verfügbare Schreibfunktion ist nachfolgen aufgeführt und reagiert auf die Modbus-Funktion 06:

Adresse	Wörter zählen	Beschreibung	Einheit	Typ Daten
1025	2	Vout ändern	Volt	IEEE 754

5.7. OPC UA

Bei den LIVARSA-Systemen, die mit einem HMI-Bildschirm ausgestattet sind, ist es möglich, durch Anschluss an den WAN-Port des ROUTER oder Fortinet F40 des Systems die von der Maschine gesammelten Daten über das OPC UA-Protokoll abzufragen, um sie in Systemen von Drittanbietern anzeigen und weiterverarbeiten zu können.

6. UNTERSTÜTZUNG

Bei Bedarf oder zur Klärung der in diesem Dokument beschriebenen Punkte wenden Sie sich bitte an den technischen Kundendienst von Energia Europa. Sie werden dann mit einem, qualifizierten Mitarbeiter verbunden.

6.1. SUPPORT - SPRECHZEITEN

Den Support von Energia Europa ist von Montag bis Freitag von 09.00 bis 12.00 Uhr und von 14.00 bis 17.00 (CET) Uhr erreichbar.

LIVARSA GmbH
Tel. 0049 7835 6343792
E-Mail: info@livosar.com

Energia Europa
Tel. +39 0445 510156
E-Mail: service@energia-europa.com



Via Trieste, 222/B - 36010 Zanè (VI) - Italien



+39 0445 510156



+39 0445 518539



service@energia-europa.com



www.energia-europa.com



Energia Europa S.p.A.