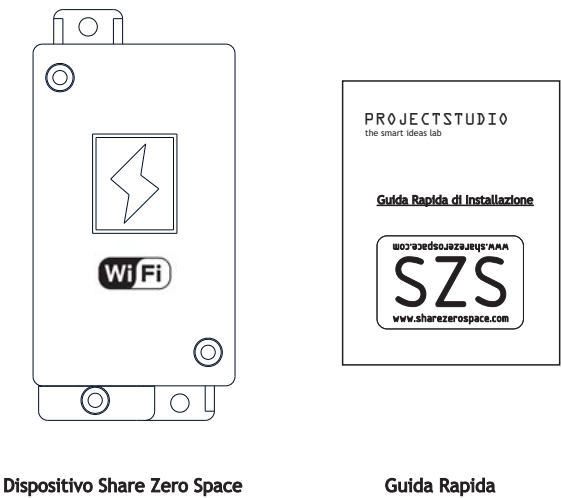


Guida Rapida di Installazione
Sistema globale per la gestione degli eventi



model one

Contenuto della confezione



Requisiti per l'uso

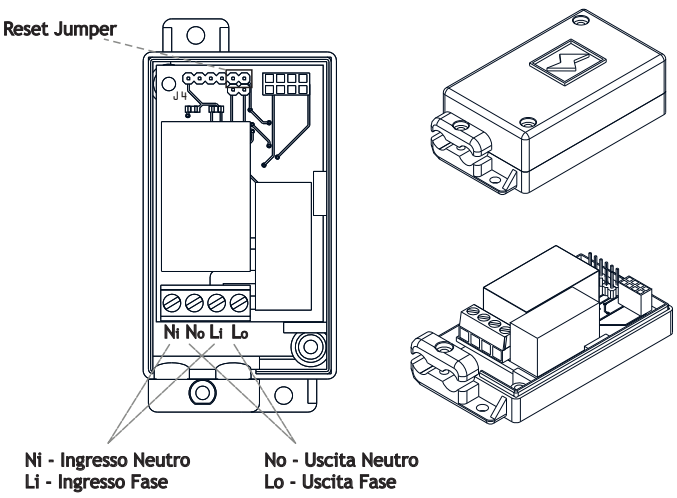
Requisiti minimi di sistema per la configurazione

- Dispositivo in grado di navigare la rete Internet dotato di connessione Wi-Fi : Smartphone, Tablet, Personal Computer, ecc.

Requisiti minimi per l'uso

- Disposito in grado di navigare la rete internet quale: Smartphone, Tablet, Personal Computer, ecc.

1 Collegamento fisico



Modello One (100x50x30) con alimentatore integrato a tensione di rete (230 / 110 Volt AC)

Connessione alla fonte di alimentazione

Concordemente al modello acquistato, il device **SZS®** viene alimentato a tensione di rete (230/110 VAC) mediante il cordone a spina o cavo idoneo collegando i morsetti indicati nel disegno direttamente dentro alla scatola. Il dispositivo è costruito per essere interposto tra alimentazione e carico in modo che lo stesso carico venga alimentato e commutato dallo stesso dispositivo SZS. La capacità di commutazione è di 16A@230V mentre il consumo massimo del dispositivo SZS in funzione è di 0.5W/h.

Porte di comunicazione e collegamento

SZS® comunica con la rete internet mediante la sola rete WiFi. **SZS®** comunica con gli eventi ad esso collegati mediante le seguenti porte.

Connessioni eventi da controllare e comandare

n°1 uscita a relè commutata (16A@230V)
n°1 Ingressi digitali non opto-isolati*
con contatto in chiusura verso massa con funzione di ingresso/contatore con funzione NA/NC programmabile (predisposizione attivabile con accessorio)

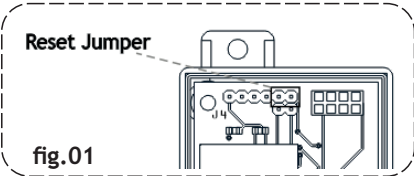
* Sono disponibili quali accessori, adattatori opto-isolati con diverse funzioni (presenza rete, opto-isolamento a tensioni diverse, ecc).

Il morsetto di connessione per l'alimentazione in uscita destinata ala carico è contraddistinta dalle indicazioni No-Lo alla quale deve essere collegato il carico. Il conduttore di terra è continuo ed il sisntema non necessita di connessione terra in quanto risulta in doppio isolamento. La porta di connessione per l'ingresso è utilizzabile solo con accessorio specifico. Le corrispondenze dei morsetti sono: **Ni - Li ingresso 230V - No Lo uscita carico 230V**. Il sistema SZS possiede protezione elettronica per lo stesso dispositivo (elettronica) mentre la protezione del carico deve essere garantita dal dispositivo di protezione della linea di alimentazione entrante con caratteristiche di corrente massima non superiore a 16A e concordemente con il carico applicato

2 Configurazione collegamento con il Cloud SZS®

Configurazione di rete del dispositivo

Per mettere in collegamento il dispositivo **SZS®** con il cloud è necessario configurare la rete. Il dispositivo **SZS®** viene configurato di fabbrica sull'indirizzo di rete 192.168.0.110, porta dati: 502 e porta web: 80 . Il dispositivo **SZS®** genererà quando alimentato un rete WiFi (SSID: szsdevice password: szsdevice) alla quale è necessario collegarsi con un dispositivo in grado di navigare (esempio uno smartphone). Compare quindi una finestra all'indirizzo http://192.168.0.110 in cui è possibile inserire le seguenti informazioni: indirizzo ip del dispositivo (default: 192.168.0.110) porta comunicazione (default: 502) quindi SSID e Passowrd della rete Wi-Fi a cui **SZS®** si deve collegare per accedere al cloud. Inseriti i dati è possibile confermare con il tasto **[save]**. Viene quindi mostrato un riepilogo che è possibile confermare con il tasto **[save and reboot]** oppure modificare e rimemorizzare utilizzando ancora il tasto **[save]**. L'operazione termina con il tasto **[save and reboot]** che riavvia il dispositivo con la nuova configurazione. Se tutto è statao configurato correttamente è possibile passare alla configurazione del cloud. Questa procedura è ripetibile e necessaria quando il dispositivo **SZS®** deve essere collegato ad un'altra rete Wi-Fi. Quando è necessario reimpostare i parametri di fabbrica si deve installare il ponticello sul contatto di reset (fig.01) quindi fornire alimentazione dopo almeno 2 secondi il jumper deve essere rimosso perché l'operazione di reset ai parametri di fabbrica è avvenuta.



Collegamento con il cloud

Appena configurato **SZS®** con l'indirizzo di rete desiderato è necessario configurare nella propria rete (router) la porta di comunicazione che deve essere vista, ovvero pubblicata all'esterno (internet).

Per fare ciò, seguendo le istruzioni del router presente aprire la porta 502 (successivamente è possibile cambiarla) indirizzando la connessione esterna proveniente dal cloud verso l'indirizzo ip configurato nel dispositivo **SZS®**. Ciò permetterà al server cloud di 'vedere' il dispositivo.

Qualora la rete internet a cui fisicamente è collegato il dispositivo **SZS®** non disponga di un indirizzo pubblico di tipo statico si utilizzi un servizio anche gratuito di DNS dinamico quale per esempio DynDns (www.dyndns.com) oppure un servizio che sia supportato dal router. Questa azione completa la configurazione di rete lato dispositivo.

A questo punto è necessario accedere al cloud di sharezerospace mediante un browser da qualunque dispositivo si possa connettere alla rete internet (pc,tablet,smartphone) navigando all'indirizzo sicuro **https://cloud.sharezerospace.com**, quindi mediante il proprio account (se non lo si possiede è possibile crearlo immediatamente) si acceda al menu [Dispositivi].

Usando la funzione [Nuovo dispositivo] si inserisca il numero seriale del dispositivo **SZS®** che si trova sull'etichetta* applicata nel coperchio interno dello stesso dispositivo.

Appena confermato il dispositivo **SZS®** viene registrato di proprietà dell'utente e lo si ritroverà nel proprio account con nuovo nome di default **'New Device'** nella lista sottostante con la scritta in colore grigio. E' necessario ora configurare il dispositivo nel cloud mediante l'inserimento di alcuni semplici parametri più avanti descritti.



*Codice Seriale

Configurazione Cloud

Entrare nella configurazione di **New Device** da [Dispositivi] e quindi appena allargata la finestra nuovamente su **New Device**. Completare i campi [description] con la descrizione (nome) del dispositivo, la [position] con la posizione geolocalizzata o con l'indirizzo del luogo fisico in cui è installato il dispositivo nella forma (Città, Via e n°civico, Nazione) se lo si desidera, quindi il fuso orario (la dicitura DST indica l'uso dell'ora legale).

Inserire con attenzione l'indirizzo IP pubblico della rete che ospita il dispositivo **SZS®** ovvero l'url DNS anche dinamico qualora sia disponibile, uguale sia per la voce [localaddr] e [remoteaddr]. Lasciare inalterata per ora la voce [encr.code] e le voci [localport] e [remoteport]. Questi parametri avanzati sarà possibile cambiarli qualora occorra in seguito. Appena eseguito, si attualizza con il pulsante [Aggiorna] al fondo della pagina e si preme sull'ingranaggio arancione al fianco della scritta [remoteport].

Parametri Firmware SZS Device

Nella pagina appena aperta e premendo sulla chiave inglese ed il cacciavite è possibile interrogare il dispositivo di campo **SZS®** verificandone la connessione e la funzionalità. Atteso il tempo di chiamata a video compariranno tutti i parametri configurati nel firmware del dispositivo. Nella maggior parte delle installazioni tutto può essere lasciato com'è. Qualora si desideri configurare o cambiare un parametro lo si selezioni nel menu [Campo da programmare] indi si scriva il relativo valore nella casella [Valore] (attenzione ai parametri binari ed esadecimali). Quindi premendo l'icona a dischetto si memorizzi il parametro. Se tutto è andato a buon fine se ne avrà avviso mediante indicazione. Al termine delle operazioni si preme ulteriormente la chiave inglese ed in cacciavite quindi si preme sull'icona di interruttore al fianco della dicitura [Pulsante per Riavviare...]. Il dispositivo sarà riavviato anche se remoto e saranno operativi i parametri configurati.

3 Configurazione Eventi

Porta di Uscita ed Ingresso (opzionale)

Sotto ai campi dei parametri di descrizione, posizione e rete, sono elencate in ordine le [Porte di Uscita] (per questo dispositivo una), le [Porte di Ingresso] (per questo dispositivo una). Il numero e l'esistenza delle stesse dipende dal tipo di dispositivo. Ogni porta, numerata con la corrispondenza fisica sul dispositivo **SZS®**, dispone di un campo Nome (al fianco della indicazione Tipo di porta X) nel quale è possibile scrivere il nome della porta o la funzione. A seguire sulla stessa riga è disponibile il campo codice di sicurezza relativo alla stessa porta. Nella riga sotto è disponibile l'indicazione icona a menu dal quale è possibile scegliere l'icona dello stato che in modo automatico genererà il messaggio di avviso (es. lampada spenta, messaggio spento, acceso). Indi il check-box Avvisami che se spuntato esprimerà la volontà di ricevere un messaggio mail (o sms) al cambio di stato (per le uscite e gli ingressi digitali).

E' poi presente un campo webcam nel quale si può inserire l'indirizzo completo che punti alla pagina video di una camera IP. Si noti che se inserito, nella consultazione dell'evento comparirà l'icona camera che, se utilizzata, aprirà una finestra integrata nella pagina controllo evento, con la visualizzazione dello stream della camera. Questa funzione non interagisce con il software della camera quindi se la stessa necessità di autenticazione verrà richiesta dalla camera stessa.

Nelle porte di ingresso è presente un campo [Conteggio dal numero] che permette, se la porta è stata configurata come contatore di inserire un numero parziale (trip) dal quale cominciare a contare permettendo l'azzeramento parziale (virtuale) del contatore di porta. Il contatore di porta si azzerà solo resettando completamente (parametri di fabbrica) il dispositivo. Ciò a contrasto con qualsivoglia manomissione del conteggio.

Per le porte di ingresso digitali è presente un campo [Decimali & Unità di misura] per permettere di valorizzare il dato nella forma decimale con unità di misura (es. 3Watt la lettura sarà con tre decimali e l'unità Watt - 0,000 Watt). Questa soluzione consente la visualizzazione del dato in modo fruibile dall'utente. Se non viene inserito nulla la visualizzazione è del tipo semplificato.

In questo dispositivo, per configurazione circuitale obbligatoria, i morsetti di uscita solo alimentati a 11/220 Vac quando attivati mediante il relativo comando. Per tanto non è possibile utilizzare i contatti di uscita per altri scopo se non alimentare un carico con la tensione in ingresso al dispositivo stesso.

La funzione è quella di presa comandata o condivisa dall'account cloud. In condizioni di default qualora venga a mancare la tensione di alimentazione al dispositivo al suo ritorno l'uscita sarà sempre senza tensione indipendentemente dallo stato assunto prima di tale mancanza. Mediante però la configurazione specifica dei parametri firmware (già descritti) sarà possibile configurare il dispositivo in modo che al ritorno della tensione l'uscita assuma lo stato che aveva prima di tale mancanza. In questo caso è necessario verificarne la compatibilità con l'eventuale carico alimentato accertandosi dei pericoli derivanti dall'alimentare un carico in maniera diretta al ritorno della tensione come nel caso di macchine o motori. Infine è possibile impostare l'ingresso (con il dispositivo di opzione ingresso) perché agisca sul relativo carico come in un relé passo-passo (bistabile).

5 Sicurezza

Impostazioni di base

Il dispositivo **SZS®** comunica con il cloud con un protocollo crittografato e sicuro. il codice di crittografazione che deve essere uguale nel firmware e nel cloud è memorizzato nel campo [encr.code] lato cloud e encryption code nel firmware. Diversamente non vi sarà comunicazione. Ogni **SZS®** possiede il proprio codice. L'accesso ai singoli eventi è regolato secondo quattro modelli. Nella configurazione cloud dal menù [Dispositivi] è presente il campo [device security] nel quale impostare l'eventuale codice valido per tutte le porte ,mentre per ogni porta è presente un campo (al destra della descrizione) che contiene il codice di sicurezza relativo alla porta della stessa riga.

Dalla prima selezione dispositivo menu [Dispositivi] è presente una casella di scelta rapida da cui impostare la modalità di sicurezza. Nella modalità [Nessuna password] l'utente e l'eventuale delegato può accedere al dispositivo ed ai relativi eventi in modo diretto semplicemente con il livello di sicurezza dell'autenticazione. Se viene selezionato [Password singola] ogni volta che l'utente o il delegato tenta di accedere all'evento desiderato viene richiesto un ulteriore codice di sicurezza [device security] uguale per tutti gli eventi del dispositivo selezionato. Se si desidera ulteriormente aumentare il grado di sicurezza [Password multipla] sarà necessario inserire per ogni evento il relativo codice di sicurezza memorizzato al lato della descrizione porta. Sia il master che ogni clone può avere proprio codice o codici diversi. Qualora invece non si desideri alcuna sicurezza ed invece si desideri condividere il dispositivo con tutta la comunità senza scegliere i delegati (evento virale social) è possibile utilizzare la scelta dispositivo pubblico. Il vantaggio dei codici di sicurezza diviene apprezzabile nell'uso di cloni e delegati a multiple porte per diversi utenti. Si ponderi bene l'uso di dispositivi pubblici.

Infine solo per i cloni è presente un check-box con indicazione locale. Questa funzione se applicata consente di condividere l'evento con il delegato ma evita che lo stesso compaia nella lista degli eventi, costringendo il delegato ad accedere a tale evento solo in modalità locale ovvero utilizzando il QR code applicato in prossimità dell'evento. Si consideri il fatto che delegando in modalità locale un evento il delegato non può selezionare tale evento sul dispositivo dal menu [Zone] e quindi non è possibile interagire da lontano. Per esempio il giardiniere delegato può aprire il cancello solo quando si trova davanti ad esso e con QR code.

Il QR code specifico per ogni evento è stampabile ed inviabile (con esclusione della modalità locale) a qualunque delegato mediante e-mail direttamente dal menu di configurazione dispositivo semplicemente cliccando l'icona codice in blu. La mail di avviso contiene anche informazioni sulla condivisione (con lingua a scelta) per la comodità del delegato. L'allegato grafico della mail contiene anche l'immagine del QR code che può essere stampata. Anche per le altre modalità comunque il QR code è perfettamente funzionante.

Si consiglia attenzione nella scelta del sistema di sicurezza, soprattutto per le modalità pubblico e locale. Qualora invece si ritenga utile cambiare il codice di crittografazione è necessario prima sostituirlo nel firmware del dispositivo e quindi solo dopo il riavvio lo si cambi nella configurazione cloud del dispositivo. Se qualcosa non dovesse andare per il giusto verso è possibile ripristinare tutti i parametri del dispositivo procedendo all'inizializzazione tenendo premuto il pulsante P1 sul dispositivo prima e durante (due secondi) l'operazione di alimentazione.

4 Cloni e Deleghe

Le Funzioni Social

Quanto sino a qui fatto consente all'utente proprietario del device (master), di disporre di tutte le funzioni di controllo e gestione degli eventi in modo personale e direttamente dal menu [Zone]. E' possibile o desiderato che l'utente master voglia condividere (delegare) il controllo e la gestione di uno o più eventi a chi lo desideri (famigliare, amico, collega, ecc.). Per fare ciò, e necessario dapprima creare un clone ovvero una copia esatta (se ne possono creare infinite) che contenga almeno una porta collegata ad un'evento (che si desidera condividere). Per fare ciò dal menu [Dispositivi] si entri nella configurazione dello stesso (click sul nome e quindi click sul nome a finestra aperta). Indi in fondo alla pagina si usi il pulsante [Clone]. Alla pressione del pulsante, la pagina viene aggiornata e al fianco sinistro di ogni porta compare un check-box. Si spuntano quindi tutte le porte che il clone deve contenere, quindi si preme al fondo della pagina il pulsante [Crea Clone]. In questa fase e nelle successive è possibile riassegnare e riconfigurare tutti i parametri e le voci di descrizione del dispositivo con esclusione dei parametri di collegamento e del codice di cifratura, variabili, solo se si voglia cambiare parametri nel firmware de dispositivo stesso. In quest' ultimo caso si ricordi dell'influenza di variazioni per altri cloni che siano derivati dallo stesso master.

Nel menu principale [Dispositivi] comparirà un nuovo dispositivo con colore arancione. Esso è il clone. Entrando nella configurazione si troverà un dispositivo clone che conterrà solo lo porte selezionate. Questa volta in alto compare il campo [Nome utente condiviso] nel quale è possibile inserire il nome utente (email di registrazione) dell'utente al quale si desidera concedere l'uso di questo clone e delle relative porte. Non è possibile condividere tale clone con un utente non registrato al cloud share zero space. Inserito il nome e premuto [Aggiorna] l'utente scelto ritroverà un dispositivo (in rosso) nella sua [Zona] e potrà eseguire le operazioni concesse. Tale utente però non avrà nessuna possibilità di delegare a sua volta il dispositivo e gli eventi, né potrà operare alcuna configurazione sul dispositivo e sui parametri della sicurezza (avanti descritti) che resteranno solo ed esclusivamente gestibili dall'utente proprietario del dispositivo, o utente master (l'utente che lo ha registrato inizialmente).Mediante il crono calendario con data di inizio e fine, giorni della settimana ed orari facilitati l'utente master potrà concedere al delegato o ai delegati (le condivisioni possibili sono con infiniti utenti) l'uso del dispositivo secondo volontà crono-temporali. Quando non condiviso secondo tale sistema il dispositivo sparisce dalla Zona dell'utente a cui si è concesso. Mediante questa funzione è possibile anche condividere per il futuro il dispositivo (si pensi all'accesso programmato). Sempre nel menu [Dispositivi] all'interno della programmazione del dispositivo e solo naturalmente per i cloni, è possibile rimuovere immediatamente la condivisione usando la funzione [Rimuovi] al fianco del nome dell'utente condiviso che si intende rimuovere. Sul lato destro è presente la funzione [Calendario] da cui impostare il crono-condivisore. Il colore di questo pulsante cambia temporalmente; se rosso la condivisione non è attiva perchè scaduta, se verde, condivisione attiva, se blu, condivisione attiva ma in questo momento sospesa (in funzione di ora e giorno), infine se arancio-giallo, condivisione effettuata ma non attiva a causa del fatto che la data di inizio non è ancora giunta.

Per motivi pratici è possibile escludere la visualizzazione nel menù [Zone] di ogni tipo di dispositivo; master, clone, condiviso e pubblico in modo temporaneo utilizzando al funzione [Dispositivi Visibili] in [Zone] oppure in modo permenete mediante le relative caselle di selezione nella funzione [Account]. Naturalmente tutte le funzioni di visualizzazione sono reversibili.

6 Problemi

Inizializzazione

- Ricordare che è possibile ripristinare i parametri di fabbrica mediante la procedura di inizializzazione.
- Prima di configurare la rete WiFi e prima dell'alimentazione dello stesso accertarsi che il jumper reset sia installato.
- Accertarsi che la classe dell'indirizzo IP sia la stessa di quella della rete che connette fisicamente il dispositivo, diversamente si provveda con il browser a configurare il nuovo indirizzo.
- Ricordarsi di aprire e configurare la porta di comunicazione (default:502) instradandola all'indirizzo Ip assegnato al dispositivo SZS all'interno del proprio router internet (salvo che non si utilizzi l'accessoprio SZS VPN microbox.

Configurazione cloud

- Ricordarsi che i cambiamenti avvengono solo dopo la pressione del tasto [Aggiorna].
- Non è possibile creare un clone senza porte.
- Non è possibile registrare un dispositivo a più di un master.
- L'utente senza master può cancellare l'account, mentre se è disponibile uno o più master prima è necessario cancellarli e solo dopo sarà possibile cancellare l'account l'utente.

Alimentazione e collegamenti

Prima di dare tensione verificare bene i collegamenti. Non sovraccaricare le uscite a relè. Il sistema elettronico è protetto da cortocircuito ma comunque curare bene le connessioni ai morsetti Ricordarsi che il dispositivo ha collegamenti ai morsetti con tensioni pericolose (110/230Vac).

7 Informazioni

Project Studio® vi ringrazia per aver scelto un suo prodotto. Ogni cura è stata applicata per ottenere il miglior sistema per la gestione degli eventi al mondo e tutto viene sempre migliorato ed evoluto. Share Zero Space® è una tecnologia coperta da brevetto internazionale ed a marchio registrato. Ogni ulteriore informazione può essere richiesta all'indirizzo e-mail. E' anche possibile ottenere qualunque personalizzazione del dispositivo, delle funzioni o del cloud, quest'ultimo può essere anche realizzato ad hoc per l'esigenza del cliente o creato per specifiche comunità social, quali; aziende pubbliche o private, club, alberghi, centri sportivi, porti, campeggi e sistemi gestione impianti o macchinari anche per la manutenzione predittiva.

Dati Tecnici Dispositivo

Alimentazione: 110/220 Volt (versione con alimentatore entro-contenuto o esterno) oppure **9-12 Volt AC/DC** e consumo massimo con modulo Wifi di 0.8 A.

n°1 uscita a relè deviate (16A@230V)
n°1 Ingresso digitale non opto-isolato*
con contatto in chiusura verso massa con funzione di ingresso/contatore con funzione NA/NC programmabile

***Operativo con accessorio dedicato ed opzionale**

PROJECTSTUDIO
the smart ideas lab

Narva maantee 5
10177 Tallinn - Eesti
Tel. +372 602 7617
http://www.projectstudio.ee
e-mail : info@projectstudio.ee

Via Roma, 146
18038 Sanremo (IM) - ITALY
Tel. +39 0184 501913
http://www.projectstudio.eu
e-mail : info@projectstudio.eu

