

Technical documentation
Last changed on: 2025-02-12

CSmmc

3U Controller with embedded Linux server

- Ethernet connectivity
- Embedded Linux Server with iCS control system
- USB-C connector
- Controls CPS, DPS or EPS modules in connection with MICC controller
- Included services: EPICS, SNMP, HTTP, Websocket, SCPI
- Webbrowser based control and configuration system
- Easy configuration and firmware updates of connected hardware



Document history

VERSION	DATE	MAJOR CHANGES
1.0	2025-02-12	Initial release

Disclaimer / Copyright

Copyright © 2025 by iseg Spezialelektronik GmbH / Germany. All Rights Reserved.

This document is under copyright of iseg Spezialelektronik GmbH, Germany. It is forbidden to copy, extract parts, duplicate for any kind of publication without a written permission of iseg Spezialelektronik GmbH. This information has been prepared for assisting operation and maintenance personnel to enable efficient use.

The information in this manual is subject to change without notice. We take no responsibility for any mistake in the document. We reserve the right to make changes in the product design without reservation and without notification to the users. We decline all responsibility for damages and injuries caused by an improper use of the device.

Safety

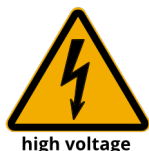
This section contains important security information for the installation and operation of the device. Failure to follow safety instructions and warnings can result in serious injury or death and property damage.

Safety and operating instructions must be read carefully before starting any operation.

We decline all responsibility for damages and injuries caused which may arise from improper use of our equipment.

Depiction of the safety instructions

DANGER



“Danger” indicates a severe injury hazard. The non-observance of safety instructions marked as “Danger” will lead to possible injury or death.

WARNING



“Warning” indicates an injury hazard. The non-observance of safety instructions marked as “Warning” could lead to possible injury or death.

CAUTION



Advices marked as “Caution” describe actions to avoid possible damages to property.

INFORMATION



Advices marked as “Information” give important information.

Description of the symbols



Warning of dangerous high voltage



Read the manual



Warning of danger spots



Connect the earth connection on the appliance to the ground



The crossed bin symbol indicates that the device shall not be disposed with regular.



CE marking. The product fulfils the requirements of the applicable EU directives.

Description of the symbols on the product



Read the manual.



Important information.



Attention high voltage!



CE marking. The product fulfils the requirements of the applicable EU directives.

Intended Use

The device may only be operated within the limits specified in the data sheet. The permissible ambient conditions (temperature, humidity) must be observed. The device is designed exclusively for the control of iseg high voltage modules as specified in the data sheet. Any other use not specified by the manufacturer is not intended. The manufacturer is not liable for any damage resulting from improper use.

Qualification of personnel

A qualified person is someone who is able to assess the work assigned to him, recognize possible dangers and take suitable safety measures on the basis of his technical training, his knowledge and experience as well as his knowledge of the relevant regulations.

General safety instructions

- Observe the valid regulations for accident prevention and environmental protection.
- Observe the safety regulations of the country in which the product is used.
- Observe the technical data and environmental conditions specified in the product documentation.
- You may only put the product into operation after it has been established that the high-voltage device complies with the country-specific regulations, safety regulations and standards of the application.
- The high-voltage power supply unit may only be installed by qualified personnel.

Important safety instructions

DANGER



This device is part of a high voltage supplying systems. High voltages are dangerous and may be fatal.

USE CAUTION WHILE WORKING WITH THIS EQUIPMENT. BE AWARE OF ELECTRICAL HAZARDS.

Always follow at the minimum these provisions:

- High voltages must always be grounded
- Do not touch wiring or connectors without securing
- Never remove covers or equipment
- Always observe humidity conditions
- Service must be done by qualified personnel only

WARNING



To avoid injury of users it is not allowed to open the unit. There are no parts which can be maintained by users inside of the unit. Opening the unit will void the warranty.

WARNING



Do not operate the unit in wet or damp conditions.

WARNING



Do not operate the unit in an explosive atmosphere.

WARNING



Do not operate the unit if you suspect the unit or the connected equipment to be damaged.

WARNING



RAMP DOWN VOLTAGES!

Before insertion or removal of crate controller, please make sure, that all voltages are ramped down, modules are switched off and power cord is disconnected.

WARNING



Particularly while remote controlling high voltage systems, make sure that nobody is near the high voltage or can be injured.

CAUTION



When installing the units, make sure that an air flow through the corresponding air inlet and outlet openings is possible.

INFORMATION



Please check the compatibility with the devices used.

Table of Contents

Document history	2
Disclaimer / Copyright	2
Safety	3
Depiction of the safety instructions	3
Description of the symbols	4
Description of the symbols on the product	4
Intended Use	4
Qualification of personnel	4
General safety instructions	4
Important safety instructions	5
1. General description	9
2. Overview	9
3. Technical data	10
3.1. Specifications	10
3.2. Compatibility	11
4. Package contents	11
5. First start-up	11
5.1. Installation and connection of the unit	11
5.2. Location requirements	12
5.3. Forced cooling	12
5.4. Configuration for initial start-up	12
6. Handling	13
6.1. RESET Button	13
6.2. USB-C interface	13
6.3. Ethernet	13
6.4. CONTROL connection	14
6.5. LED	14
7. iCS2 – iseg Communication Server	14
Document history	15
Disclaimer / Copyright	15
7.1. System description	16
7.2. Software architecture	17
7.2.1. How to connect via WiFi	18
7.2.2. How to connect via Ethernet	18
7.2.3. iCSconfig: manage hardware, service and preferences	19
7.3. Hardware	20
7.3.1. Ethernet configuration	21
7.3.2. (Re)set / ethernet configuration	22
7.3.3. WiFi configuration	22
7.4. Users / roles configuration	23
7.4.1. Access Control Lists (ACL)	23
7.4.2. SSH access	23
7.4.3. (Re)set SSH access	24
7.4.4. iCS Factory Reset Invocation	24
7.4.5. Instructions:	24
7.5. iCSservice configuration	25
7.5.1. HTTP interface	26
7.5.2. Examples	26
7.5.3. EPICS	27
7.5.4. HALservice	28
7.5.5. SNMP	28

7.5.6. Updates	29
7.5.7. Custom scripts	30
7.6. iScontrol software overview	31
7.6.1. Left bar: Hardware Explorer	32
7.6.2. Left bar: Channel folders	33
7.6.3. Left bar: Channel profiles	33
7.6.4. Center bar: Channel list	33
7.6.5. Right bar: Device information	33
7.6.6. Right bar: Camera	34
7.6.7. Right bar: Live log	34
7.6.8. Right bar: Commands	34
8. Dimensional drawing	35
9. Connectors assignments	36
10. PIN assignments	37
10.1. Control connector	37
11. References	38
12. Glossary	39
13. Warranty & service	41
14. Disposal	41
15. Conformity	41
16. Manufacturer contact	41

1. General description

The iseg CSmmc is an intelligent internal MICC add-on controller with an embedded Linux Server system and preinstalled iseg Communication Server (iCS). The iCS comes with a large set of services as EPICS, Web-Control, SNMP, Websocket, OPC/UA¹, isegHAL and HTTP-API. The iCS also delivers two main web based user applications. **iCScontrol** provides a quick and smart control interface of the connected hardware by using web-browser without software installation. **iCSconfig** is used for hardware and service configuration and firmware upgrades. Both can also be used on mobile devices like tablets or smartphones.

For native application control several software solutions are available:

- iseg**Control** (Linux, Windows, Mac)
- isegHalRemote-Library

2. Overview



Figure 1: Sample of MCC controller

NUMBER		DESCRIPTION	DETAILED EXPLANATION IN CHAPTER
[1]	LED	Status LED	6.5 LED
[2]	ETHERNET	Interface	6.3 Ethernet
[3]	USB-C	Interface	6.2 USB-C interface
[4]	RESET	Hard-Reset	6.1 RESET Button
[5]	CONTROL	connector with configurable digital I/O	6.4 CONTROL connection
[6]	CONNECTOR	System connector	3 Technical data

Table 1: Description of the elements

¹ Expected available middle of 2025

3. Technical data

3.1. Specifications

SYSTEM		
Module System		MMC
Type		MICC add-on controller
System Connector		96-pin MMC connector, DIN 41612
INTERFACES		
Universal Serial Bus	USB-C	default
Ethernet	ETH	default
Control connector	Control	default
HARDWARE		
CPU		NXP/Freescale iMX6 Quad-Core 996 MHz
RAM		1 GB DDR3 onboard
Flash Memory		4 GB onboard
CASE		
Form factor		Euro cassette
Dimensions	L x W x H	160mm x 4HP x 3U, MMC
Weight		0.2 kg
Cooling		Force cooling required
ENVIRONMENTAL		
Operating parameters	Temperature	0°C – 50°C
	Humidity	20% – 80%, non-condensing
Storage parameters	Temperature	-20°C – 70°C
	Humidity	20% – 80%, non-condensing

Table 2: Technical data

3.2. Compatibility

HARDWARE	REQUIRED	
ECH 14A ²	free MMS 3U Slot	
MICC or MICCETH	Firmware version: MICC_428 or higher	

Table 3: compatibility

4. Package contents

HARDWARE	INCLUDED	
CSmmc	Plug-in controller card	

Table 4: Package contents

5. First start-up

CAUTION



Before plugging the power supply of CSmmc in or out, please make sure, all voltages are ramped down, connected crates or AC/DC supplies are switched off.

5.1. Installation and connection of the unit

Installation is only intended in the ECH 14A. Switch off the device and disconnect the mains cable from the device. Unscrew the existing slot covers. Slide the controller into the marked (with number “one”) slot. Carefully insert the card into the slot and lock it.

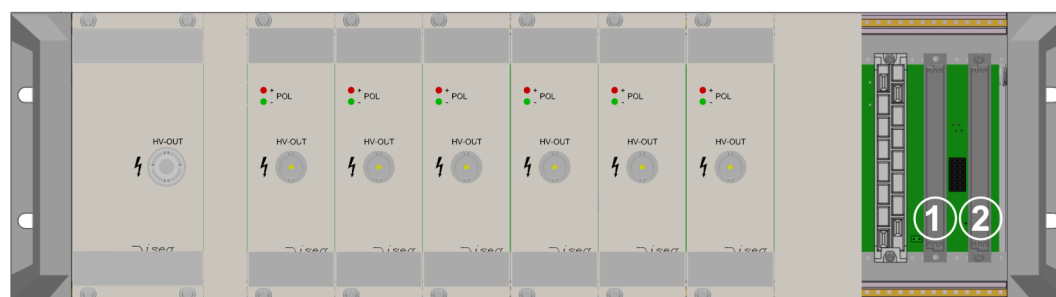
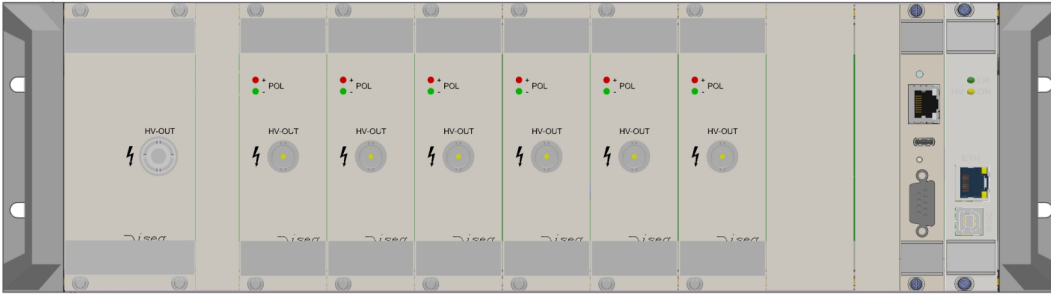


Figure 2: free Slot for CSmmc

² The CSmmc can only be operated together with a MICC controller



Close any unused slots. The necessary covers are available separately.

5.2. Location requirements

The product is for indoor use only. The climatic conditions must be observed (see chapter 3 Technical data). To ensure optimum operation, the ambient temperature should be maintained.

5.3. Forced cooling

The module generates heat from its internal components during operation. To ensure that the temperature is kept constant during operation, the enclosure should be forcibly ventilated.

5.4. Configuration for initial start-up

Connect the Ethernet cable to the RJ-45 connector of the CSmmc. Connect the other end of the Ethernet cable to a switch which is also connected to the control computer. The module is set to DHCP at the factory. To find the specific IP address, contact your IT department or use the iseg software iCSfinder. The link to iCSfinder can be found in the chapter 11 References. Use a web browser and enter the iCSmmc's IP address in the address field and press Enter. A log-in webpage is loaded. The user name and password for the are "admin" and "password". Use only lower case letters. After the log-in, the user interface of the iseg Communication Server appears.



Figure 3: iseg Communication Server

The hardware can be managed in the user interface. Activate the required protocols for communication in the user interface. A detailed description can be found in the chapter 7 iCS2 – iseg Communication Server.

6. Handling

6.1. RESET Button

Pressing the button restarts the device. A short press of the reset button sends a signal to the micro controller to restart. The CSmmc controller restarts. All configuration are retained.

6.2. USB-C interface

Access via SCPI commands is possible via the USB-C interface. The command set is described in the SCPI manual "[SCPI Programmers Guide en.pdf](#)". The link can be found under chapter 11 References.

The commands are described in the chapters:

- 2.3. Syntax extension for iCS based systems
- 4 Common instruction set
- 6 EHS, NHR, SHR, NHS and MICC

6.3. Ethernet

The Ethernet interface enables the module system to be controlled via:

- isegHAL,
- SCPI,
- iCS webcontrol,
- EPICS,
- HALservice or
- SNMP.

The description of the commands or software is listed in the chapter 11 References.

RJ-45 Ethernet network connector (10/100/1000MBit) indicates the following modes with its status LEDs.

Upper LED – speed indicator

Amber on	Operating as a Gigabit connection
Green on	Operating as a 100 Mbit/s connection
Off	Operating as a 10 Mbit/s connection

Lower LED – link indicator

Blinking	There is activity on this port
Off	No link is established

6.4. CONTROL connection

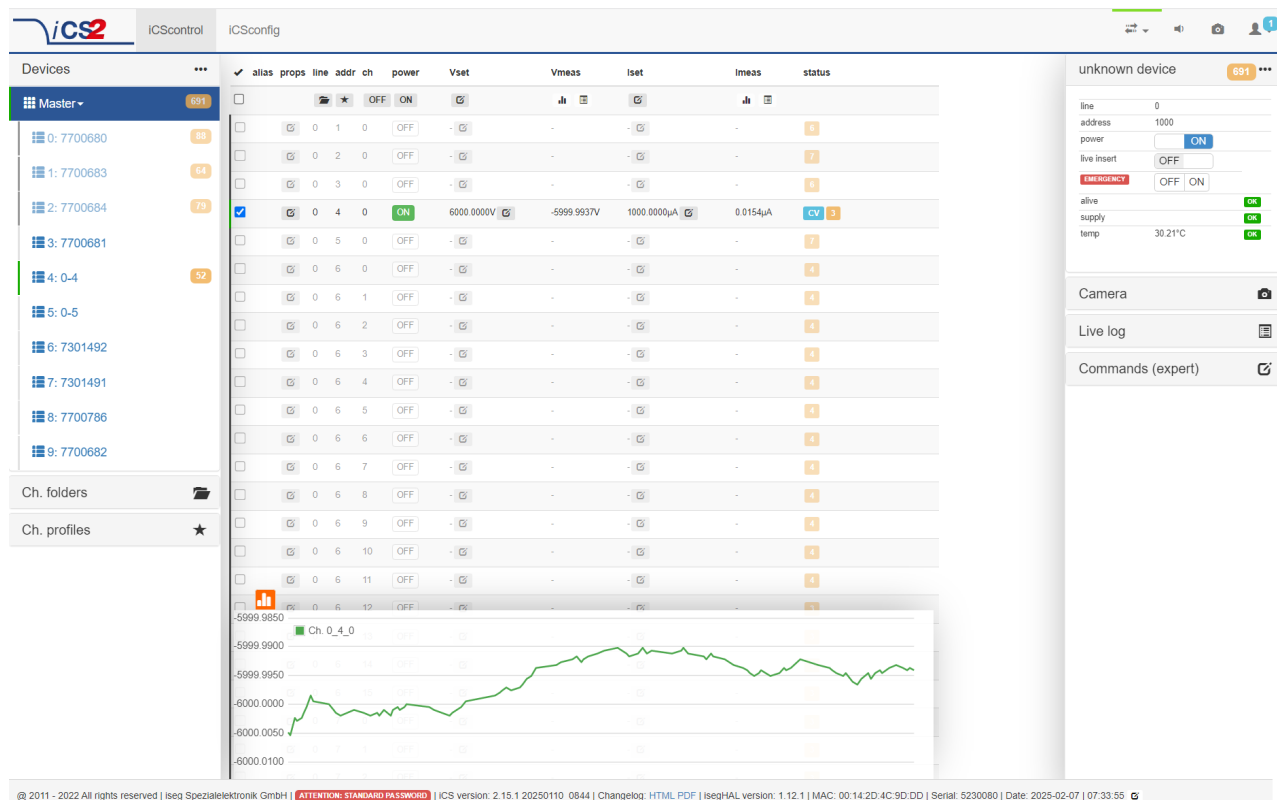
This function will be implemented shortly.

6.5. LED

The LED on the front of the controller signals the following states:

- LED is off CSmmc off, no power
- LED is lighting green CSmmc powered on

7. iCS2 – iseg Communication Server



Document history

VERSION	DATE	MAJOR CHANGES
1.3	2025-02-04	Update figures, Changing the default configuration of the services As of iCS version 2.15.1, the services isegSnmp and isegloc (EPICS) are switched off by default. This results in the following standard configuration: Ethernet: DHCP WiFi hotspot: active (with existing hardware) Websocket: active isegHalRemote: active EPICS: deactivated SCPI: active OPC: deactivated (available from iCS v3.2) SNMP: deactivated
1.2	2024-06-20	Safety instructions revised
1.1	2023-04-13	Labeling of tables, small layout adjustments
1.0	2023-01-03	Modification log for the document, 7.4.2 SSH access, 7.4.3 (Re)set SSH access

Disclaimer / Copyright

Copyright © 2025 by iseg Spezialelektronik GmbH / Germany. All Rights Reserved.

This document is under copyright of iseg Spezialelektronik GmbH, Germany. It is forbidden to copy, extract parts, duplicate for any kind of publication without a written permission of iseg Spezialelektronik GmbH. This information has been prepared for assisting operation and maintenance personnel to enable efficient use.

The information in this manual is subject to change without notice. We take no responsibility for any mistake in the document. We reserve the right to make changes in the product design without reservation and without notification to the users. We decline all responsibility for damages and injuries caused by an improper use of the device.

7.1. System description

The iseg Communication Server iCS is a software solution to control iseg high voltage hardware from multiple devices over wired or wireless network. iCS is a manufacturer specific Linux OS, which runs on iseg hardware, like iCSmini2, CC24 crate controller series or SHR Desktop High Voltage Power Supply.

The iCS front end is based on browser technology to keep installation and maintenance effort low, to enable a quick start for configuration independently from the user's software platform, even on mobile devices.

iCS is equipped with an integrated role and user management, and delivers important software services right out of the box, like EPICS IOC, OPC server, SNMP interface, HTTP and webservices to give a quick access to iseg hardware.

iCS also delivers configuration utilities and straight forwarded tools for firmware upgrading process.

The installed iCS2 libraries and services licenses files are located on the system under:

/usr/share/common-licences/[library or service module]

ICS SOFTWARE COMPONENTS	DESCRIPTION	PORT / PROTOCOL
iCSconfig	Configuration section for iCS software services, restorable hardware configurations, and firmware updates, documentation access and more...	TCP 80 / HTTP
iCScontrol	Multi-user browser based device control, surveillance cam support	TCP 80 / HTTP
iCSservice	Internal websocket based server, JSON objects, with clients Push (websocket) or pull (HTTP polling) technology	TCP 8080 / Websocket TCP 8081 / HTTP API
isegHALservice	iseg hardware abstraction layer service, simple hardware access	TCP 1454 / isegHAL Socket
EPICS IOC	EPICS Input / Output controller, autoconfiguring to hardware setup, customizable by file upload#	EPICS Base R3.15.7 TCP/UDP 5064, 5065
OPC/UA	OPC / UA server	
SNMP	Simple Network Management Protocol	UDP 161

Table 5: software components

7.2. Software architecture



Figure 4: Software architecture

7.2.1. How to connect via WiFi

- 1) Make sure to have the WiFi adapter onboard or external installed, all modules are plugged in and CAN connections (if used) are attached. Start the crate or device.
- 2) Use your mobile device or computer to search for existing WiFi networks and select „iseq-iCS_XXXX“ (XXXX is the iCS serial number).
Enter the factory default WiFi password (password).
- 3) Open a recommended web-browser like Google Chrome and enter the factory default IP address (192.168.1.1)
- 4) Enter the factory default username (admin) and password (password)

INFORMATION



WiFi support can be turned off in iCSconfig → WiFi. The default WiFi password can be changed there also.

7.2.2. How to connect via Ethernet

For Ethernet connections with the use of factory defaults, it is necessary to know the IP address of the iCS server first.

By default the iCS is configured to obtain the IP automatically by DHCP. To discover the IP address of the iCS, a small software application iCSfinder can be used. It scans the local network for running iCS services. More details are in the INFORMATION box below. iCS also provides UPnP messages, which can be discovered, e.g. in Windows using „Network“ environment. For Linux and MAC, Zeroconf/Bonjour can be used to find the iCS.

INFORMATION



To discover iCS installations on the local network, a small utility iCSfinder can be used.

It can be downloaded here: <https://iseq-hv.com/download/?dir=SOFTWARE/iCS/iCSfinder/>

Note: If you wish to set a fixed address without preconnecting via DHCP, please use a (temporarily) WiFi connection to setup OR follow the instructions of (re)setting the ethernet settings (see chapter 7.3.1 Ethernet configuration)

Hint: If you experience problems using iCSfinder, please try using free software tools like “IP SCANNER” / MAC or “ADVANCED IP SCANNER” (Windows)

- 1) Make sure to have the network cable, all modules plugged in and all CAN connections if used attached. Start the crate.
- 2) Open a recommended web-browser and enter the current IP address (see preparations before).
- 3) Enter the factory default username (admin) and password (password).

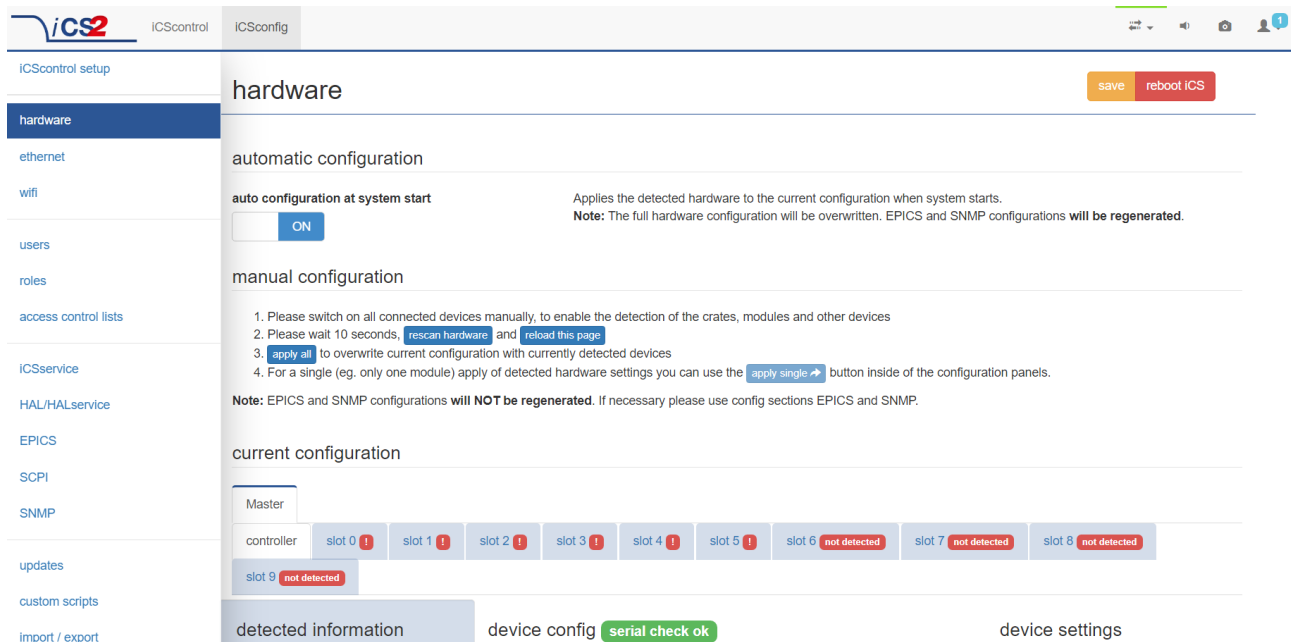
7.2.3. iCSconfig: manage hardware, service and preferences

iCS has a comprehensive set of configurable properties. All of them are stored in an XML file, to keep configuration flexible. This enables the possibility to have multiple configuration setups stored and restored using the import / export utility.

ICS CONFIG SECTIONS	
iCScontrol Setup	Manage preferences of iCS web control application
Hardware	Manage connected hardware, set configurations, auto configure, start firmware updates
Ethernet	Manage Ethernet port settings of the iCS
Wifi	Manage wireless access point of the iCS
Users	Create / edit / delete iCS users
Roles	Create / edit / delete iCS roles
Access Control Lists	Grant / deny rights on user / group / channel / item base
iCSService	Configure iCSService API / HTTP API
HAL/HALservice	Configure HAL logging and HALservice credentials
EPICS	Configure the embedded EPICS Input/Output controller (IOC)
OPC	Configure the embedded OPC/UA server
SNMP	Configure the embedded SNMP server
Updates	Download updates (System, Product database, firmware) from internet
Custom Scripts	Configure the custom Python3 scripts
Import / Export	Save and restore complete iCS configuration to backup hardware setup

Table 6: ics config section

7.3. Hardware



The screenshot shows the iCS2 hardware configuration page. The left sidebar contains a menu with options: hardware (selected), ethernet, wifi, users, roles, access control lists, ICSservice, HAL/HALservice, EPICS, SCPI, SNMP, updates, custom scripts, and import / export. The main content area is titled 'hardware' and has 'save' and 'reboot ICS' buttons. It is divided into three sections: 'automatic configuration', 'manual configuration', and 'current configuration'. The 'automatic configuration' section has a toggle for 'auto configuration at system start' set to 'ON' and a note: 'Note: The full hardware configuration will be overwritten. EPICS and SNMP configurations will be regenerated.' The 'manual configuration' section contains instructions and a note: 'Note: EPICS and SNMP configurations will NOT be regenerated. If necessary please use config sections EPICS and SNMP.' The 'current configuration' section shows a table of hardware slots. The 'detected information' tab is active, showing a table with columns for 'detected information', 'device config', and 'device settings'. The table lists slots 0 through 9, with slots 0-5 and 9 marked as 'not detected' and slots 6-8 marked as 'not detected'.

Figure 5: Hardware

In the hardware section, all iCS connected devices like connected crates, controllers and modules are listed and configurable. Each device is represented by a tab, modules and controllers are nested into their responding crates. The CAN lines of the crates are presented with a yellow or green upper tab border (corresponding to yellow or green CAN line), master crates and modules in legacy crates with a blue upper tab border. The configuration is stored independently from the current hardware setup or connected states. This gives the opportunity to detect misconfigurations and recent hardware setups can easily be restored. The feature auto configuration at system start supports automatically take over of the detected to the configured hardware, generation of EPICS and SNMP configuration. Auto configuration will be executed one time after iCS system start when master crate backplane is on or when iCS is running on a iCSmini. To apply the complete detected hardware state into the configuration use the apply all button after triggering a rescan using the rescan hardware button. To apply the detected config of just one device (controller or module) use the apply single button under each single tab. The devices information is stored with the information of "module/device config" column. Here the line and address ID are shown and a serial number can be entered (or applied by using auto configuration / apply). If the model of the hardware device could be detected automatically, a model is selected in the dropdown list, otherwise it should be selected manually. Here a FIND buttons checks the list and helps prefiltering the list.

HARDWARE TYPES	
Device	Standalone High Voltage Power Supply
Crate	Case / Bin for a modular HV-supply (module), which supplies power and provides slots for the modules
Controller	Special controller card used in a crate to control, monitors and manages nested modules and crate functions, like switch ON/OFF of crate power supply, monitor temperatures, fans, UPS and more
Module	Modular High Voltage Power Supply, plugged in a slot of a crate, supplied by a CRATE, communication and management by CRATE CONTROLLER, no own POWER ON feature

Table 7: Hardware Types

Information in the row „module settings /device settings“ are module / device specific settings and are stored into the XML configuration file. These settings will get lost when using auto configuration at system start, apply all or apply single functionality.

7.3.1. Ethernet configuration

The ethernet settings of the iCS server hardware (CC2x Crate Controller, iCSmini) can be changed under the ethernet tab. By turning DHCP Client to enabled the iCS will try to obtain an IP address from the local networks DHCP server. Otherwise the IP can be set fixed. Therefore DHCP client must be disabled and IPv4 settings can be entered manually.

ETHERNET FACTORY DEFAULTS	
IP	DHCP
GATEWAY	empty
NAMESERVER	empty
DNS	empty
TIMESERVER	empty

Table 8: Ethernet Defaults

The Ethernet settings will be stored automatically to the USB flash memory, directory iseg-ICS as file ip-config.txt whenever an USB flash memory is plugged in. This allows retrieving the current IP configuration from an iCS system.

7.3.2. (Re)set / ethernet configuration

You can reset the ethernet configuration and also set to fixed IP address e.g. cause of problems with DHCP IP relay using the following procedure:

- 1) Shut down all modules/devices and turn off the iCS System by unplugging mains.
- 2) Create an empty file called "RESET_NET.txt" on a USB flash memory drive (FAT32 format)
- 3) Now edit the file. It should contain the following entries, separated by new lines.
- 4) Plug USB flash memory drive into the USB slot at the front panel of the device (CC24, iCSmini2, SHR)
- 5) Plug in mains
- 6) Please wait about 20 seconds until iCS has started completely
- 7) Optional: Plug off the USB flash memory drive and check on a computer if the file created on step 2 was renamed to RESET_NET.txt.done. If it was not renamed, then something went wrong.

CONTENT OF RESET_NET.TXT			
LINE	PARAMETER	EXAMPLE	DEFAULT-VALUE
0	IP address / DHCP	192.168.0.10	DHCP
1	NET MASK	255.255.255.0	255.255.255.0
2	GATEWAY	192.168.0.1	192.168.0.1
3	NAMESERVER	192.168.0.1	192.168.0.1

Table 9: reset content

INFORMATION	
	Use quality USB flash memory drives, otherwise the drive might not be detected by the iCS. Also make sure, the flash memory has no file system problems.

7.3.3. WiFi configuration

The WiFi configuration sets the wireless network properties provided by the iCS hardware access point (optional). Generally the WiFi function can be disabled using the WiFi support switch. The IP address of the WiFi is fixed, so once connected with a iCS WiFi the IP address always stays the same.

WIFI FACTORY DEFAULTS	
IP (fixed)	192.168.1.1
SSID	iseg-iCS2_[HARDWARE SERIAL-NUMBER]
Channel	5
Password	password

Table 10: wifi configurations

7.4. Users / roles configuration

Users of iCScntrl can be added, edited and removed in the users section. Users can be assigned roles, such like admin, user etc. One or more users can be selected by editing a role.

USER DEFAULTS	
User	admin
Password	password
Role	admin

Table 11: user configurations

7.4.1. Access Control Lists (ACL)

With the access control list rights to grant or forbid control on special objects for principals (roles or users) is managed. This gives a powerful tool for very detailed rights mechanism.



Note: Users, roles and ACL are only applied for user authentication for applications and services, which are based on iCSservice. These are iCScntrl, iCSconfig, isegControl, and HTTP API.

isegHAL based services should implement their own security mechanisms.

7.4.2. SSH access

The ICS2 Linux host system can be fully accessed as root user using an encrypted SSH shell access over port 22.

This enables the user to install own services or freely configure e.g. EPICS plugins etc.

From factory side, the user account root is enabled, but protected with a secret password. To use the SSH access, you need to setup a custom password. This is described in the next chapter 7.4.3 (Re)set SSH access.

Afterwards, you can use any SSH client, e.g. PuTTY (<https://putty.org>) to log in as root with your custom password.



The local file system is divided into a system and a user data partition. To make changes on the read-only mounted system part use the following command: `mount-rw /` and `mount-ro /` switches the root file system back to read-only.

7.4.3. (Re)set SSH access

INFORMATION



To protect your iCS system, we strongly advise to change the factory SSH password into a custom password. This password allows full system access, so keep this password secret!

For security reasons, changing the SSH password is only possible with direct hardware access using the following procedure:

- 1) Create a file RESET_SSH.txt with your new root Password as content in the first line and save it to an USB flash memory drive (FAT32 format). Note: if the file is empty, the iCS root password will be reset to factory default.
- 2) Plug the USB flash into iCS hardware and reboot iCS.
- 3) The iCS changes the password during the boot process. In case of success the file will be renamed into RESET_SSH.txt.done.

7.4.4. iCS Factory Reset Invocation

In case the user has forgotten his password or simply wants to get back to factory default configuration, it is possible to invoke a factory reset. For factory reset an USB flash drive (USB stick) with a FAT32/FAT16 partition is needed.

CAUTION!

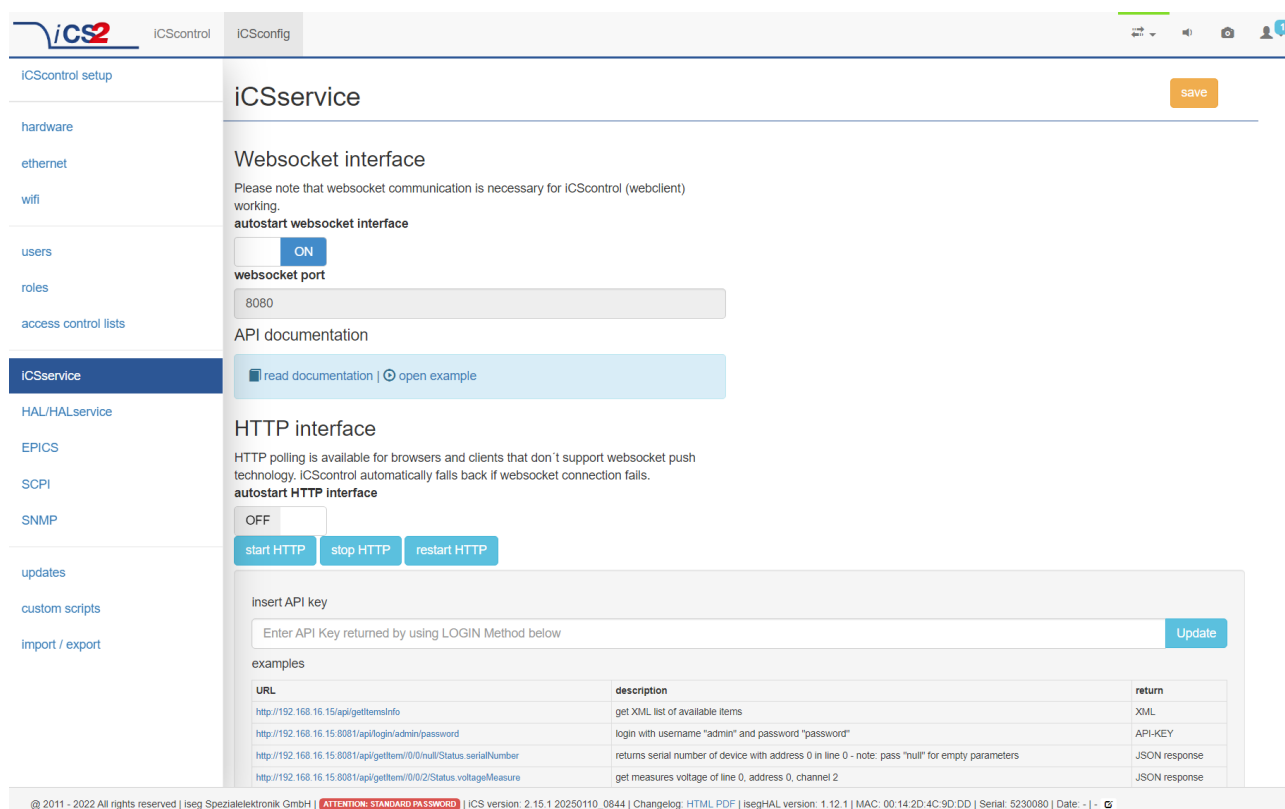


After factory reset all hardware configurations will get lost!

7.4.5. Instructions:

- 1) Shut down all modules / devices and turn off the iCS System by unplugging mains.
- 2) On the USB flash drive create an empty file called "RESET_ICS.txt"
- 3) Plug the USB flash memory drive into the USB slot at the front panel of the Crate-Controller
- 4) Plug in mains
- 5) Please wait about 20 seconds until iCS has started completely
- 6) In case of success the file will be renamed to RESET_ICS.txt.done.

7.5. iCSservice configuration



Websocket interface

Please note that websocket communication is necessary for iCScontrol (webclient) working.

autostart websocket interface

☐ ON

websocket port

8080

API documentation

[read documentation](#) | [open example](#)

HTTP interface

HTTP polling is available for browsers and clients that don't support websocket push technology. iCScontrol automatically falls back if websocket connection fails.

autostart HTTP interface

☐ OFF

[start HTTP](#) [stop HTTP](#) [restart HTTP](#)

Insert API key

Enter API Key returned by using LOGIN Method below [Update](#)

examples

URL	description	return
http://192.168.16.15/api/getItemsInfo	get XML list of available items	XML
http://192.168.16.15.8081/api/login/admin/password	login with username "admin" and password "password"	API-KEY
http://192.168.16.15.8081/api/getItems/0/0/null/Status.serialNumber	returns serial number of device with address 0 in line 0 - note: pass "null" for empty parameters	JSON response
http://192.168.16.15.8081/api/getItems/0/0/2/Status.voltageMeasure	get measures voltage of line 0, address 0, channel 2	JSON response

@ 2011 - 2022 All rights reserved | iseg Spezial Elektronik GmbH | **ATTENTION: STANDARD PASSWORD** | iCS version: 2.15.1 20250110_0844 | Changelog: [HTML](#) [PDF](#) | isegHAL version: 1.12.1 | MAC: 00:14:2D:4C:9D:DD | Serial: 5230080 | Date: - | -

Figure 6: iCSservice configuration

The iCSservice running on iCS hardware provides two interfaces, a websocket interface with push technology and a HTTP polling interface, which is fallback for browsers and clients, that do not support websocket technology. Both of them can be disabled, whereas at least one of them is necessary for the correct operation of iCScontrol.

ICSSERVICE DEFAULTS	
Websocket Port	8080
HTTP port	8081
HTTP URL BASE	<IP-of-iCS>:8081/api/

Table 12: iCSservice DEFAULTS



The documentation of iCSservice API, step by step connection guide to use Websocket / HTTP interface and an example Javascript is available on iCS directly (iCSconfig / iCSservice) or online on:

<https://iseg-hv.com/download/?dir=SOFTWARE/iCS/doc/iCSservice/>

7.5.1. HTTP interface

This interface gives quick access to iCService by simple HTTP queries.

ICSSERVICE HTTP FUNCTIONS		
URL, Parameters with leading \$, params not mandatory [\$param]	Response	Description
http://<IP-of-ICS>:8081/api/login/\$username/\$password	API Key	Returns API Key to be identified for session
http://<IP-of-ICS>:8081/api/logout/\$session-ID	TRUE / FALSE	
http://<IP-of-ICS>:8081/api/getItem/\$apikey/\$line/\$address/\$channel/\$item	JSON Object	Returns state of a specific item of a hardware path \$line, \$address, \$channel and \$item can be set by wildcard '*'
http://<IP-of-ICS>:8081/api/setItem/\$apikey/\$line/\$address/\$channel/\$item/\$value/[\$unit]	TRUE / FALSE	Sets state of a specific item of a hardware path \$line, \$address, \$channel can be set by wildcard '*'
http://<IP-of-ICS>:8081/api/getUpdate/\$apikey/	JSON Object	returns all changes collected by iCService since last getUpdate call for this client session
Notes: Use "*" as wildcard, e.g. to set or get items on multiple channels at once. Use "null" as empty set identifier, e.g. to obtain module specific objects without channel declaration.		

Table 13: iCService HTTP functions

7.5.2. Examples

EXAMPLES	
http://192.168.1.1:8081/api/getItem/123456-321/0/1/0/Status.voltageMeasure	Returns voltage value, unit and timestamp of channel 0 of module with address 1 of line 0
http://192.168.1.1:8081/api/setItem/123456-321/0/1/*/Control.voltageSet/1/kV	Set set voltages of all channels of module 1 in line 0 to 1,000 Volt
http://192.168.1.1:8081/api/setItem/123456-321/0/null/null/Control.power/1	Switch controller of line 0 (master) on

Table 14: Examples

7.5.3. EPICS

For the use of iseg hardware with Experimental Physics and Industrial Control System (EPICS), the iCS comes with a preinstalled integrated Input-Output-Controller (IOC). This service can be enabled or disabled using the switch enable EPICS input / output controller. To keep things straight forward, the iCS can generate IOC configuration files (.db and .sub) using the current hardware configuration. Both files can be downloaded to the local computer, edited manually, e.g. with a text editor and uploaded again. This gives a quick start to run an IOC out of the box. To get an overview on all available process variables (PV), which are generated at the start of IOC, the PV list can be downloaded using the respective button. The IOC script combines a process variable definition file (.db) with a substitution file (.sub), which contains hardware setup information and placeholders to create all accessible process variables at run time.

FILE	DESCRIPTION	SAMPLE CONTENT (EXTRACTION)
iseg_epics.db	Database file with definitions of PV	<pre>##### # ### Crate item values ### # ##### record(mbbiDirect, "ISEG:\${CONTROLLER_SN}:\${CAN_LINE}:\${ DEVICE_ID}:StatusLow") { field(DESC, "Lower 16 bit of module status register") field(DTYP, "isegHAL") field(INP, "@\${CAN_LINE}.\${DEVICE_ID}.Status can0") field(NOBT, "16") field(SHFT, "0") field(TSE, "-2") } ...</pre>
iseg_epics.sub	Substitution file contains a pattern that will be substituted by the following lines for each corresponding channel	<pre>{CONTROLLER_SN,CAN_LINE,DEVICE_ID,MODULE_ID,CHANNEL_ID} {5230003,0,1000,0,0,"AUTO"} {5230003,0,1000,0,1,"AUTO"} {5230003,0,1000,0,2,"AUTO"} ...</pre>
iseg_epics.pv	Text file with list of process variables generated	<pre>ISEG:5230003:0:0:0:CurrentMeasure ISEG:5230003:0:0:0:CurrentNominal ISEG:5230003:0:0:0:VoltageMeasure ISEG:5230003:0:0:0:VoltageNominal ...</pre>

Table 15: epic files

For more detailed information on EPICS, please visit: <https://epics.anl.gov/>, for sample libraries and test scripts, please contact support@iseg-hv.de.

INFORMATION



The documentation of iseg EPICS IOC and a sample scripts are available on iCS directly (iCSconfig / EPICS) or online on: <https://iseg-hv.com/download/?dir=SOFTWARE/iCS/doc/isegIOC/>

7.5.4. HALservice

The isegHALservice provides a secure sockets encrypted end-to-endpoint access to the iseg hardware layer running on iCS hardware. The isegHALservice API is similar to isegHAL API, with some specific extension. Please refer Appendix “isegHAL” for details. For an easy start a simple example program isegHalTerminal demonstrates the remote access. There are virtual instruments (VIs) which are based on the library isegHAL-remote in order to control iseg hardware via LabVIEW ³.

INFORMATION



The documentation of iseg HAL (service) is available on iCS directly (iCSconfig / HALservice) or online on: <https://iseg-hv.com/download/SOFTWARE/iCS/doc/isegHAL/index.html>

7.5.5. SNMP

For backward compatibility of the iCS2 to SNMP controlled systems like WIENER MPOD, iCS2 is able to communicate using the SNMP service.

The service can be enabled or disabled using the switch enable SNMP interface.

Using the current iCS2 hardware configuration a SNMP configuration can be automatically generated. To create a new SNMP configuration, which is compatible to WIENER Configuration file (.mib) please use button “generate configuration” under the SNMP tab in iCSconfig.

For user specific changes of configuration, the .mib (vendor specific definition of data points) and .sub (substitution information with list of hardware channels) files can be downloaded, locally modified and uploaded again.

Please note: local modifications will be overwritten every time the “generate configuration” function will be used.

INFORMATION



The documentation of iseg SNMPservice and sample scripts are available on iCS directly (iCSconfig / SNMP) or online on: https://iseg-hv.com/download/SOFTWARE/SNMPguide/SNMP_Programmers-Guide_en.pdf

³ © National Instruments Corporation. All rights reserved.

7.5.6. Updates

The following types of updates can be managed with iCS:

TYPE	DESCRIPTION
base	product database with information about iseg hardware specifications
system	update image of the iCS server operating system (CC, iCSmini)
firmware	firmware update files for iseg devices (like HV modules, crate controllers etc.)

Table 16: updates

All update files can be downloaded from iseg web repository using the CHECK ONLINE FOR UPDATES or using the update UPLOAD function to send a file from the local computer to the iCS server.

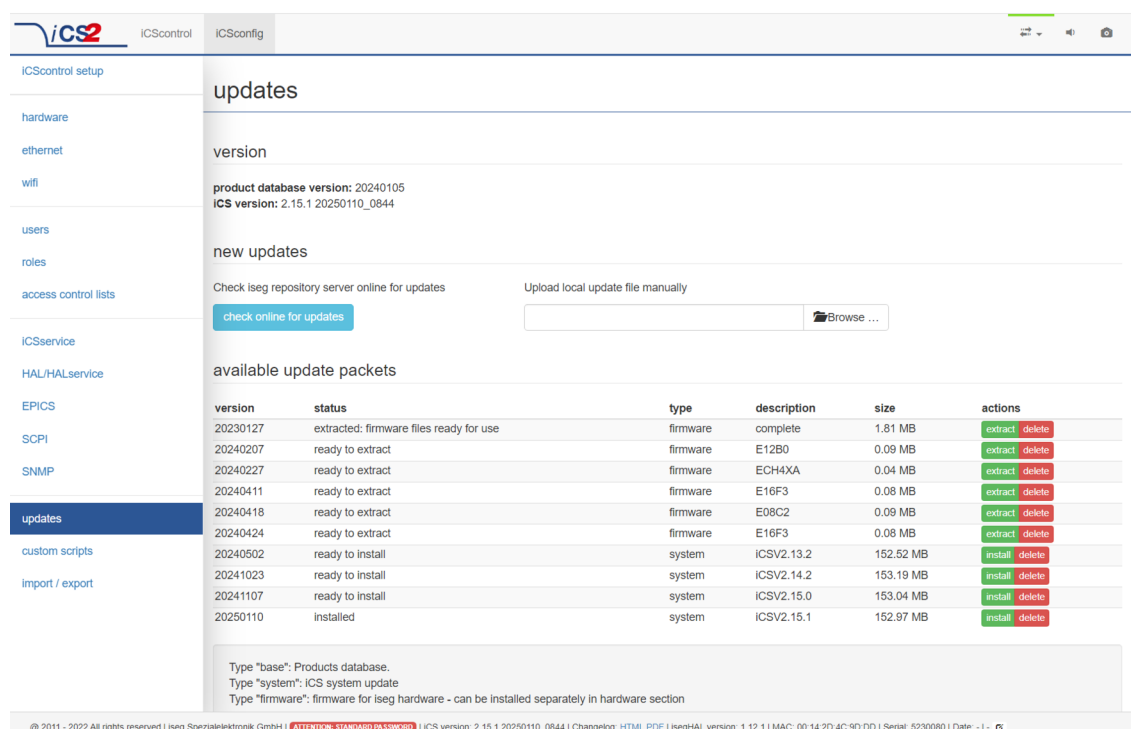
Once an update file is available on the iCS, it can be installed using INSTALL or removed by using DELETE Buttons. After using install, follow the instructions shown on the screen. Firmware files can be unzipped using EXTRACT. After extraction the available firmware files are shown in a list. By clicking INSTALL the iCS tries to apply the selected firmware to all connected devices, that are qualified for (matching item code, online, lower firmware version installed).

To update specific hardware devices please extract the firmware package first and then navigate in the hardware section to the corresponding device and use firmware update functionality individually.



Using the Check online for updates feature the iCS directly connects to iseg online software repository.

All update files can also be downloaded directly on <http://download.iseg-hv.com/?dir=SOFTWARE/iCS>



The screenshot shows the iCScontrol web interface. The left sidebar contains navigation links: hardware, ethernet, wifi, users, roles, access control lists, ICSService, HAL/HALservice, EPICS, SCPI, SNMP, updates (selected), custom scripts, and Import / export. The main content area is titled 'updates' and displays the following information:

- version**: product database version: 20240105, ICS version: 2.15.1 20250110_0844
- new updates**: Check iseg repository server online for updates (button: check online for updates) and Upload local update file manually (input field and Browse ... button).
- available update packets**: A table listing updates with columns: version, status, type, description, size, and actions.

version	status	type	description	size	actions
20230127	extracted: firmware files ready for use	firmware	complete	1.81 MB	extract delete
20240207	ready to extract	firmware	E12B0	0.09 MB	extract delete
20240227	ready to extract	firmware	ECH4XA	0.04 MB	extract delete
20240411	ready to extract	firmware	E16F3	0.08 MB	extract delete
20240418	ready to extract	firmware	E08C2	0.09 MB	extract delete
20240424	ready to extract	firmware	E16F3	0.08 MB	extract delete
20240502	ready to install	system	ICSV2.13.2	152.52 MB	install delete
20241023	ready to install	system	ICSV2.14.2	153.19 MB	install delete
20241107	ready to install	system	ICSV2.15.0	153.04 MB	install delete
20250110	installed	system	ICSV2.15.1	152.97 MB	install delete

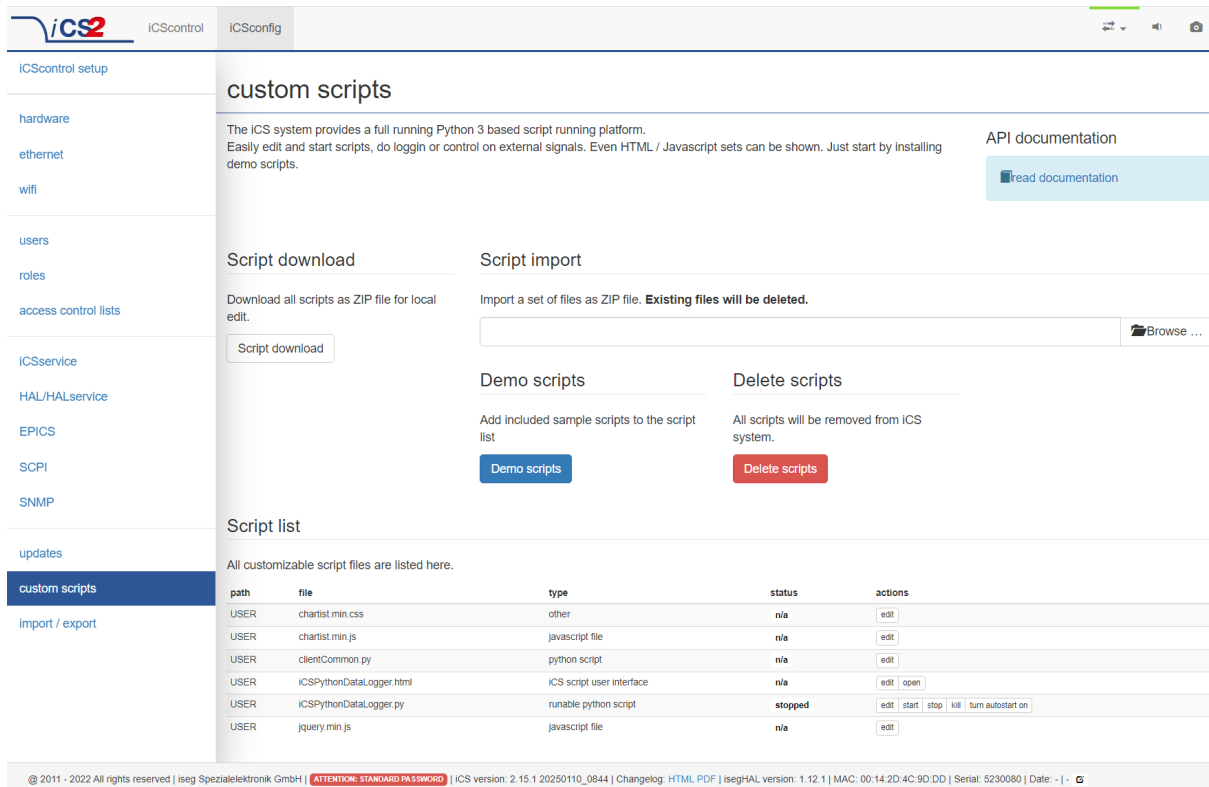
Below the table, there is a note: Type "base": Products database. Type "system": ICS system update. Type "firmware": firmware for iseg hardware - can be installed separately in hardware section.

At the bottom, there is a footer with copyright information: © 2011 - 2022 All rights reserved | iseg Spezialelektronik GmbH | ATTENTION: STANDARD PASSWORD | ICS version: 2.15.1 20250110_0844 | Changelog: HTML PDF | isegHAL version: 1.12.1 | MAC: 00:14:2D:4C:9D:DD | Serial: 5230080 | Date: - | -

Figure 7: Updates

7.5.7. Custom scripts

The custom script folder provides an access to the script setup. A list of installed scripts will be displayed here.



The screenshot shows the 'custom scripts' page in the iCS2 interface. The sidebar on the left contains various system configuration options. The main panel has a header 'custom scripts' and a brief description of the Python 3 based script running platform. Below this, there are four main sections: 'Script download' with a 'Script download' button; 'Script import' with a text input field and a 'Browse...' button; 'Demo scripts' with a 'Demo scripts' button; and 'Delete scripts' with a 'Delete scripts' button. At the bottom, there is a 'Script list' table with the following data:

path	file	type	status	actions
USER	chartist.min.css	other	n/a	edit
USER	chartist.min.js	javascript file	n/a	edit
USER	clientCommon.py	python script	n/a	edit
USER	iCSPythonDataLogger.html	iCS script user interface	n/a	edit open
USER	iCSPythonDataLogger.py	runable python script	stopped	edit start stop kill turn autostart on
USER	jquery.min.js	javascript file	n/a	edit

Figure 8: Custom scripts setup

CUSTOM SCRIPTS	
Script download	Load a copy of all installed files from iseg hardware <code>/mnt/user/data/scripts</code> as ZIP file to your local download directory
Script import	Import a ZIP file to iseg hardware and extract it to <code>/mnt/user/data/scripts</code> . Existing files will be overwritten.
Demo scripts	Add included sample scripts to <code>/mnt/user/data/scripts</code> on iCS hardware
Delete scripts	All scripts will be removed from iCS system
Edit	An editor window open the selected file to make changes or input additionally contents.
Open	Open iCSPythonDataLogger.html for graphical output of logging data.
Start	Start script execute a python3 process with the scrip
Stop	Send a stop command to the script in order to finish the execution.
Kill	Kill the script execution process
Turn on autostart on	Configure an autostart process for a script when the iCS system will be started.

Table 17: Custom script

7.6. iCScontrol software overview

The user interface of iCScontrol software is divided into three parts. The left bar contains the Devices, Ch folders channel folders and Ch profiles channel profiles. The center bar contains control elements, device and channel process variables with the possibility to output a graphical line plot. The right bar contains a device section, Camera access to an optional USB webcam, Live log for data logging and a field to input single Commands from a list.

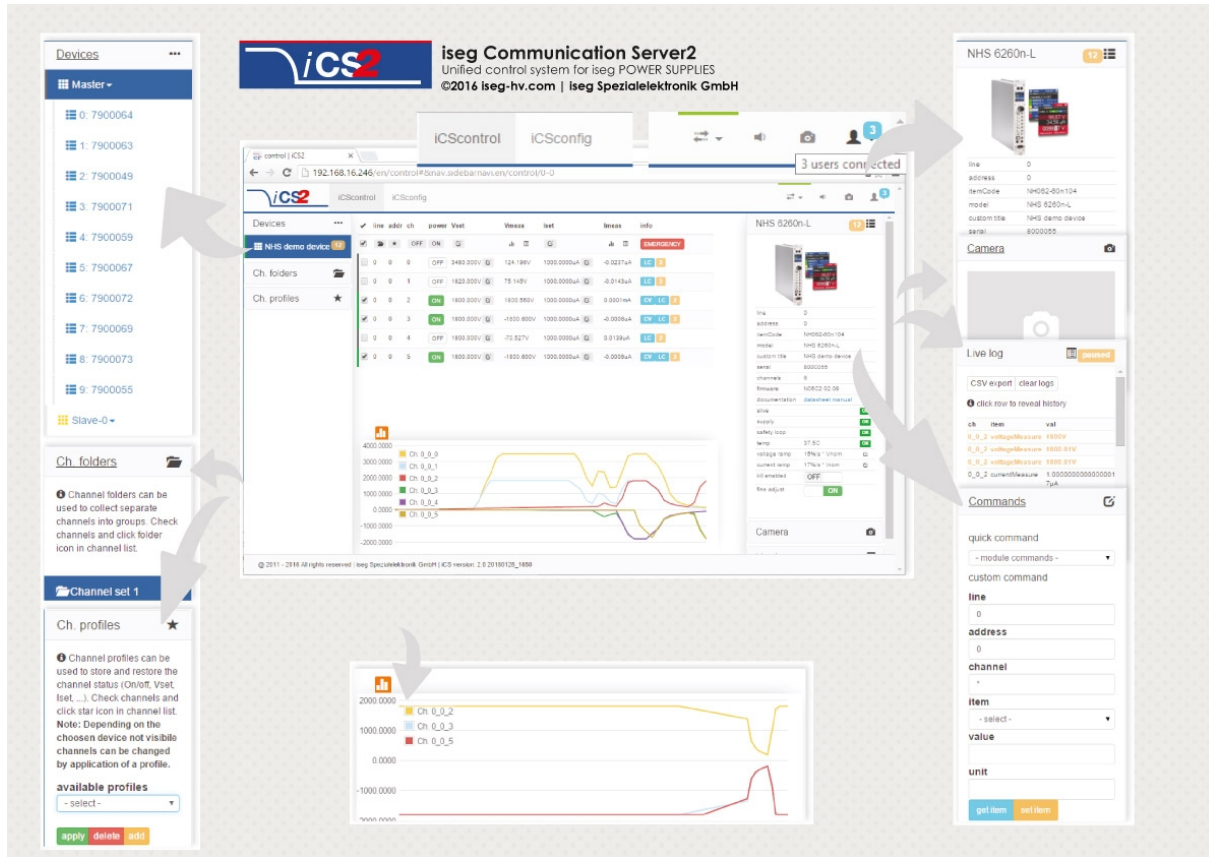


Figure 9: iCScontrol

7.6.1. Left bar: Hardware Explorer

The left column shows the configured hardware.

If connected with iseg CAN line management (starting with CC23) slaves are shown in yellow or green background, corresponding to the CAN line they are connected to. Every device has a colored left border showing the running state.

CRATE/DEVICE RUNNING STATES	
gray	all channels of the module are off
yellow	one channel of one of the nested channels is ramping to the desired voltage
red	the crate / device (or one of the nested modules/channels) has one or more errors (refer to the error/event badges)
green	the crate / device (and all of the nested modules) are in a good condition, at least one channel of a nested module is running high voltage

Table 18: Device running states

MODULE RUNNING STATES	
gray	not present, not connected or switched off
yellow	one channel of the module is ramping to the desired voltage
red	the module has one or more errors (refer to the error/event badges)
green	the device/module is in a good condition, at least one channel is running high voltage

Table 19: Module running states

CHANNEL RUNNING STATES	
blurred / faded out	Module is not detected (probably switched off)
gray	not present (configured module to current module mismatch), or switched off
yellow	channel is ramping to the desired set voltage
red	channel has at least one error (please inspect error counter badge)
green	channel is in good condition and switched on

Table 20: Channel running states

7.6.2. Left bar: Channel folders

Channel folders are shown in the section “channel folders” below the hardware section in the left application bar. Channel folders can be created and extended by selecting a set of channels and clicking the folders icon on top of the channel list.

Existing folders can be selected or removed in the folders section of the left bar.

7.6.3. Left bar: Channel profiles

Channel profiles store information about set values, on/off states, and Kill properties of channels. They can be created by selecting the channels that should be restored in the channel list and clicking the star-icon. Existing profiles can be selected, applied and removed in the channel profiles section of the left bar. A new option with the custom given title appears in the select box. By selecting a channel profile and clicking the APPLY button the stored state of the channel will be adjusted.

7.6.4. Center bar: Channel list

Once a device or channel folder has been selected, the channel list will update and show only the corresponding channels, with

- The topological location (line, address, channel),
- The running state,
- Set and measured values,
- Channel info, events and errors (displayed as clickable badges)

The list header has an ACTION ROW, where all channels can be selected with one click for more actions.

Each action in this row is located in top of its respective column.

Some examples:

- To create a new channel folder of specific channels, select these channels and click the folder-icon.
- To store the current setup of the specific channels (running state, set-values, kill enable etc.), select them and click on the star-icon. To enable or disable all selected channels, click the ON / OFF icons.
- Change the set voltages of all selected channels, click the edit-icon which is located in the V_{set} column.
- To display a graph of measured voltages of all selected channels, click on the graph-icon located in the V_{meas} column.
- To show a live log of measured voltages of all selected channels, click on the logtable icon located in the V_{meas} column.

7.6.5. Right bar: Device information

The device section gives information on the currently selected hardware device of the hardware explorer. Depending on the device type, hardware status information are given (temperature, error, safety loop states), the device can be enabled / disabled. Device specific parameters can be set (ramps, kill parameters ...). To get a quick help, hardware documentation can be downloaded directly.

7.6.6. Right bar: Camera

The camera tab shows the captured image of the configured camera. It can be directly connected with the iCS hardware or an IP-Cam URL, configured in hardware / iCScontrol section.

7.6.7. Right bar: Live log

The live log collects information of the current session. The log data is only available until a reload of the iCScontrol web page occurs. The live log can be filtered to specific channels or value types, by selecting channels and clicking the corresponding log icon in the action row on top of the channel list. The log list shows the last value of an item. By clicking on it, previous log items are displayed.

All session log data can be exported as CSV file for ongoing work with spreadsheet applications, eg. Microsoft® Excel.

7.6.8. Right bar: Commands

Commands can be send directly to connected devices. Quick commands are mass operations that can be sent to more devices at one time. The commands tab prefills the input fields according to the selected hardware device (in hardware explorer).

8. Dimensional drawing

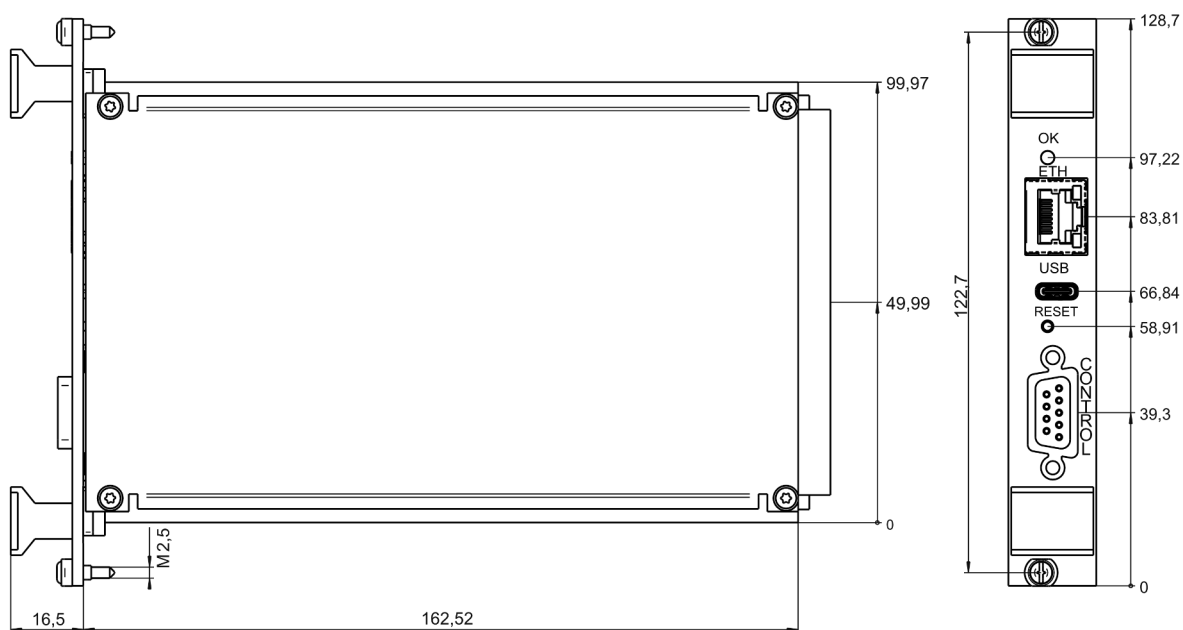


Figure 10: Dimension drawing

9. Connectors assignments

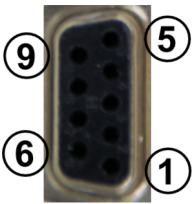
CONNECTORS		PART NUMBERS (manufacturer code / iseg accessory parts item code)	
USB-C		CABLE SIDE	
USB  Figure 11	connector	USB-C	
	manufacturer	different producers	
ETH RJ45		CABLE SIDE	
ETH  Figure 12	connector	RJ45	
	manufacturer	different producers	
Control connector D-SUB9 – female		CABLE SIDE	
 Figure 13	connector	D-SUD 9	
	manufacturer	different producers	
	iseg part number	Z592067 (male) + Z592146 (hood)	

Table 21: Connectors

10. PIN assignments

10.1. Control connector ⁴

Pin	Name	Description
1	Crate Enable	
2	Crate Fast Off	
3	User Input 0	
4	User Input 1	
5	Ground	
6	High Voltage On	
7	User Output 0	
8	User Output 1	
9	Logic High	

Table 22 Control connector

⁴ Implementation to follow soon

11. References

For more information please use the following download links:

This document
iseg_manual_CSmmc_en.pdf
Archive
Coming soon
Manual - ECH 124 and ECH 14A
https://iseg-hv.com/download/SYSTEMS/MMC/ECH/iseg_manual_ECH12x-14x_en.pdf
Iseg MMC System
https://iseg-hv.com/de#SYSTEM-MMC
isegControl2
https://iseg-hv.com/download/?dir=SOFTWARE/isegControl2/
iCSservice
https://iseg-hv.com/download/?dir=SOFTWARE/iCS/doc/iCSservice/
iCSFinder
https://iseg-hv.com/download/?dir=SOFTWARE/iCS/iCSfinder/
iseg EPICS IOC and a sample
https://iseg-hv.com/download/?dir=SOFTWARE/iCS/doc/isegIOC/
iseg HAL (service)
https://iseg-hv.com/download/SOFTWARE/iCS/doc/isegHAL/index.html
SCPI Programmers Guide
https://iseg-hv.com/download/SOFTWARE/isegSCPI/SCPI_Programmers_Guide_en.pdf
SNMP Guide
https://iseg-hv.com/download/SOFTWARE/SNMPguide/SNMP_Programmers-Guide_en.pdf

Table 23: References

12. Glossary

SHORTCUT	MEANING
0V	Supply ground
V_{nom}	nominal output voltage
V_{out}	output voltage
V_{set}	set value of output voltage
V_{mon}	monitor voltage of output voltage
V_{meas}	digital measured value of output voltage
V_{p-p}	peak to peak ripple voltage
V_{in}	input / supply voltage
$V_{in,s}$	$V_{in,s}$ Supply voltage
V_{type}	type of output voltage (AC, DC)
V_{ref}	internal reference voltage
V_{max}	limit (max.) value of output voltage
V_{limit}	voltage limit
$\Delta V_{out} - [\Delta V_{in}]$	deviation of V_{out} depending on variation of supply voltage
$\Delta V_{out} - [\Delta R_{load}]$	deviation of V_{out} depending on variation of output load
V_{bounds}	voltage bounds, a tolerance tube $V_{set} \pm V_{bounds}$ around V_{set}
I_{nom}	nominal output current
I_{out}	output current
I_{set}	set value of output current
I_{mon}	monitor voltage of output current
I_{meas}	digital measured value of current
I_{trip}	current limit to shut down the output voltage
I_{in}	input / supply current
I_{max}	limit (max.) value of output current
I_{limit}	current limit
I_{bounds}	current bounds, a tolerance tube $I_{set} \pm I_{bounds}$ around I_{set}
P_{nom}	nominal output power
P_{in}	input power
$P_{in,nom}$	nominal input power
T	temperature

SHORTCUT	MEANING
T _{REF}	reference temperature
ON	HV ON
OFF	HV OFF
CH	channel(s)
HV	high voltage
LV	low voltage
GND	signal ground
INH	Inhibit
POL	Polarity
KILL	KillEnable
CFG	Common Floating-GND https://iseg-hv.com/en/knowledge/floating
FG	Floating-GND https://iseg-hv.com/en/knowledge/floating
CG	Common-GND https://iseg-hv.com/en/knowledge/floating

13. Warranty & service

This device is made with high care and quality assurance methods. The standard factory warranty is 36 months. Please contact the iseg sales department if you wish to extend the warranty.

CAUTION



Repair and maintenance may only be performed by trained and authorized personnel.

For repair please follow the RMA instructions on our website: www.iseg-hv.com/en/support/rma

14. Disposal

INFORMATION



All high-voltage equipment and integrated components are largely made of recyclable materials. Do not dispose the device with regular residual waste. Please use the recycling and disposal facilities for electrical and electronic equipment available in your country.

This device is only intended for professional use or as an built-in component for devices in the research/development sector and is sold exclusively B2B (only to commercial end customers). The device may only be disposed of properly and not in normal household waste.

As an alternative to proper self-disposal, we offer a free disposal option for the device. Before sending in the device, please send an email to recycling@iseg-hv.de stating the device article and serial number to receive further information on the process.

15. Conformity

The declaration of the product is available on our website.

16. Manufacturer contact

iseg Spezialelektronik GmbH

Bautzner Landstr. 23

01454 Radeberg / OT Rossendorf

GERMANY

FON: +49 351 26996-0 | FAX: +49 351 26996-21