# 1 iCS2 – iseg Communication Server

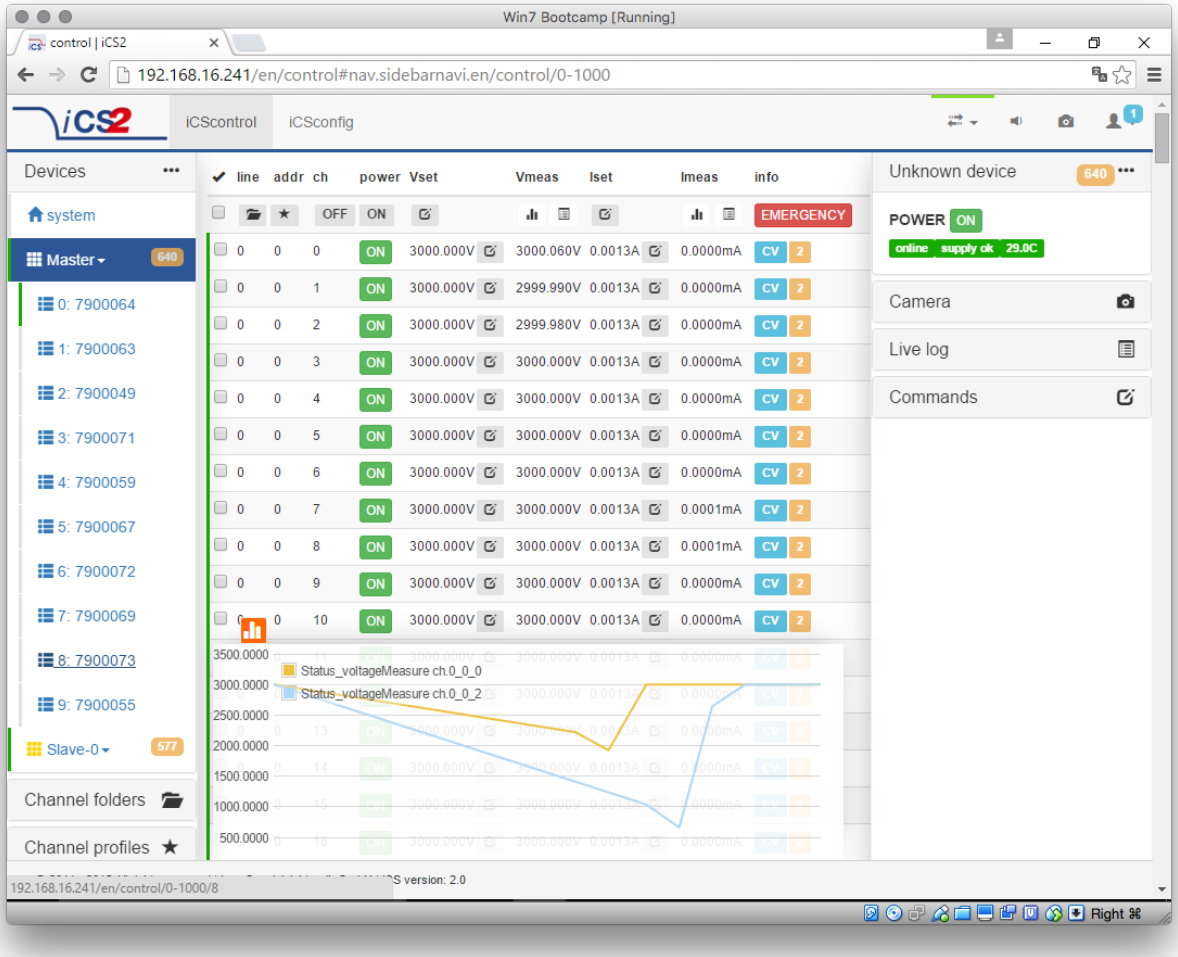


*Figure 1: iseg Communication Server*

## 1.1 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<br>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<br>TCP/UDP 5064, 5065 |
| OPC/UA | OPC / UA server | |
| SNMP | Simple Network Management Protocol | UDP 161 |

*Table 1*

## 1.2 Software architecture

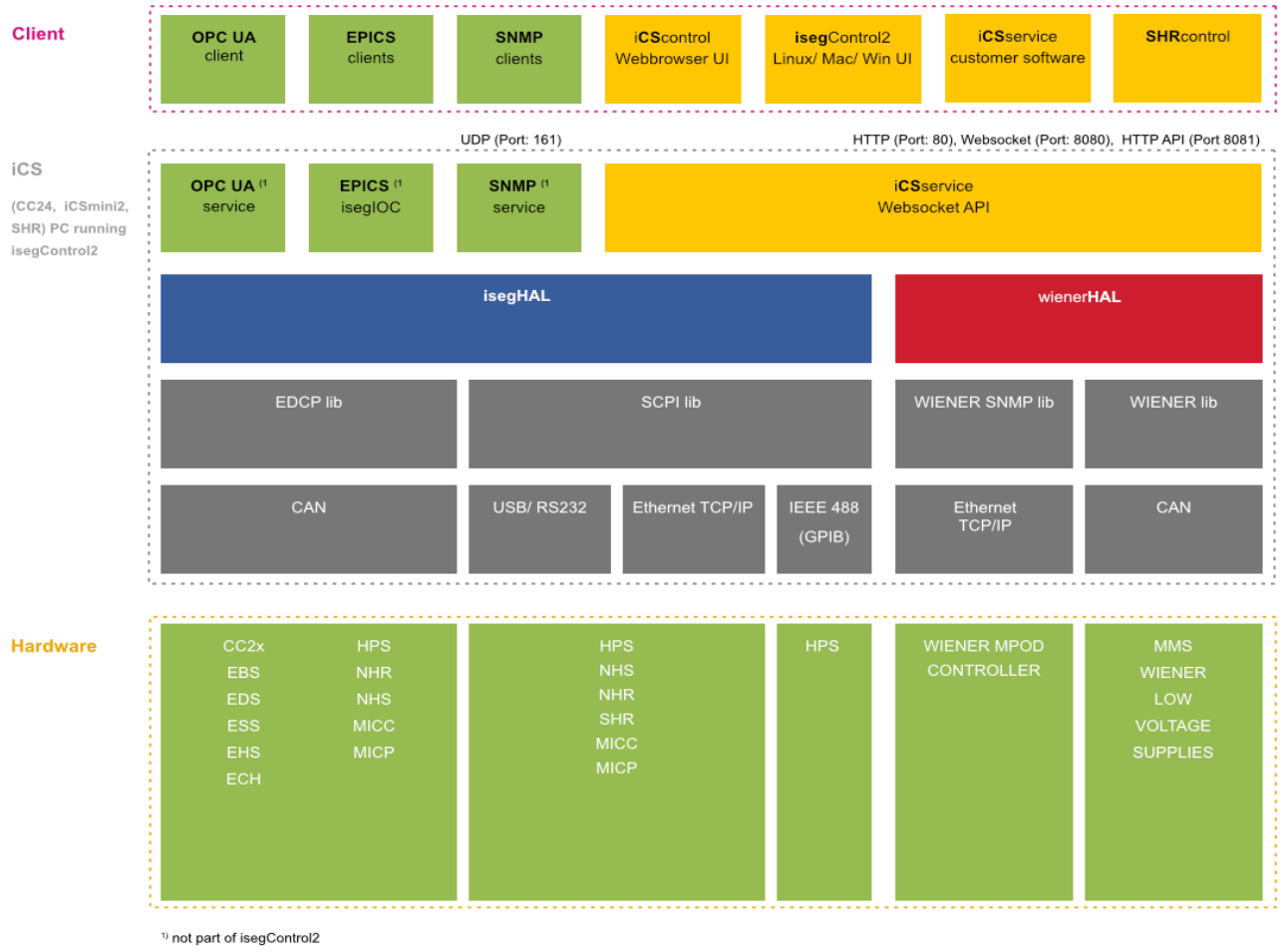


*Figure 2: Software architecture*

### 1.2.1 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 „iseg-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**

INFORMATION

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

### 1.2.2 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**

INFORMATION

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

It can be downloaded here: https://iseg-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 1.3.1 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).

### 1.2.3 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 2*

## 1.3 Hardware

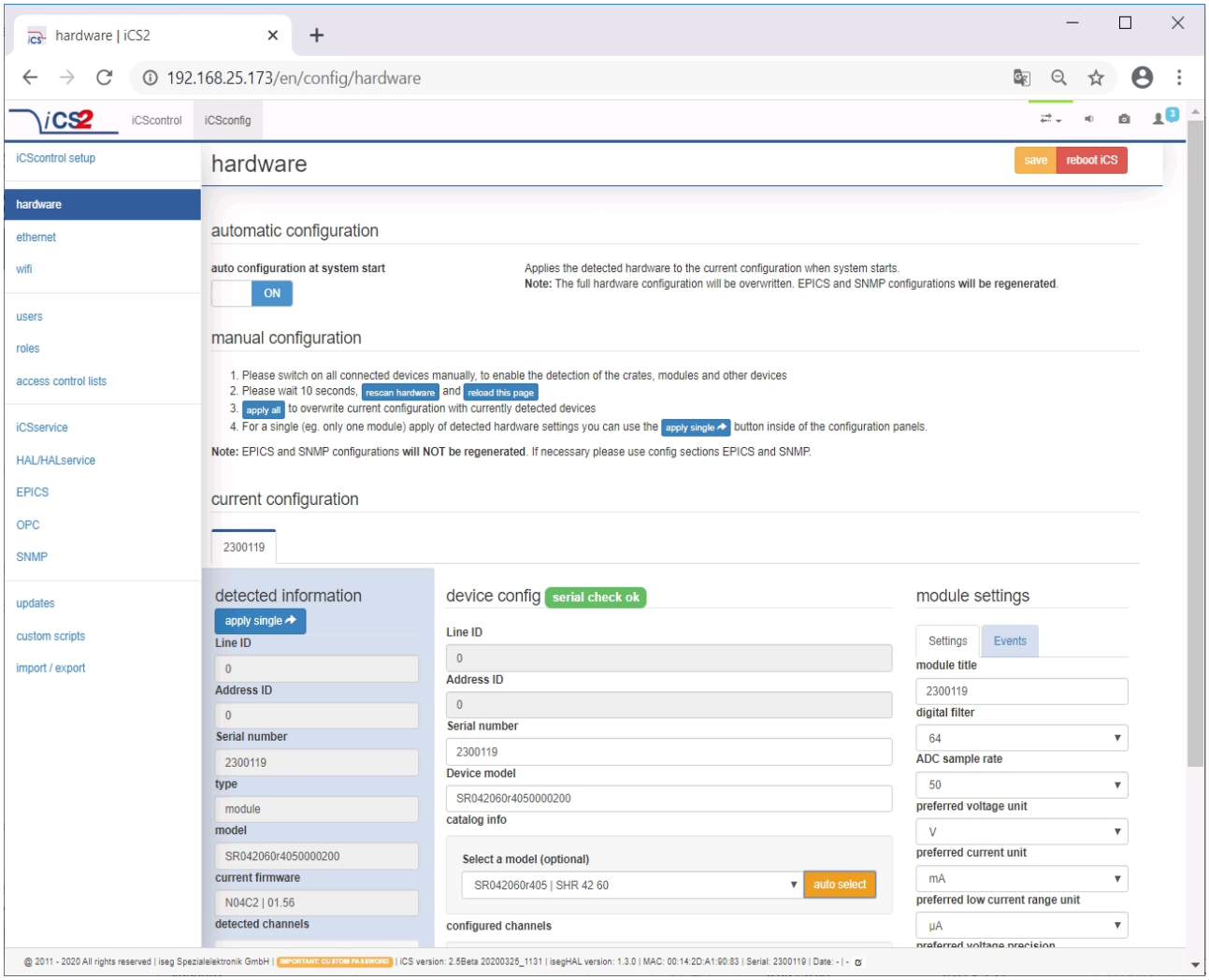


*Figure 3: Hardware*

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 3: 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.

### 1.3.1 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 4: 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.

### 1.3.2 (Re)set / ethernet configuration

You can reset the ethernet configuration and also set to fixed IP adress 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 5*

**INFORMATION**

INFORMATION

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

### 1.3.3 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 6*

## 1.4 Users / roles configuration

Users of iCScontrol 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 |

### 1.4.1 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.

**INFORMATION**

INFORMATION

Note: Users, roles and ACL are only applied for user authentication for applications and services, which are based on iCSservice. These are iCScontrol, iCSconfig, isegControl, and HTTP API.
isegHAL based services should implement their own security mechanisms.

### 1.4.2 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 user to install own services or freely configure e.g. EPICS plugins etc. The setup of a custom password will be described in the next chapter 1.4.3 (Re)set SSH access.

**INFORMATION**

INFORMATION

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.

### 1.4.3 (Re)set SSH access

**INFORMATION**

INFORMATION

To protect your iCS system we strongly advice to change the standard factory password into a new user defined one. Keep this password secret!

For security reasons this is only possible with direct hardware access using the following procedure:

1) Create a file RESET_SSH.txt with your new root Passwort 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.

### 1.4.4 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!**

CAUTION!

After factory reset all hardware configurations will get lost!

### 1.4.5 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.

## 1.5 iCSservice configuration

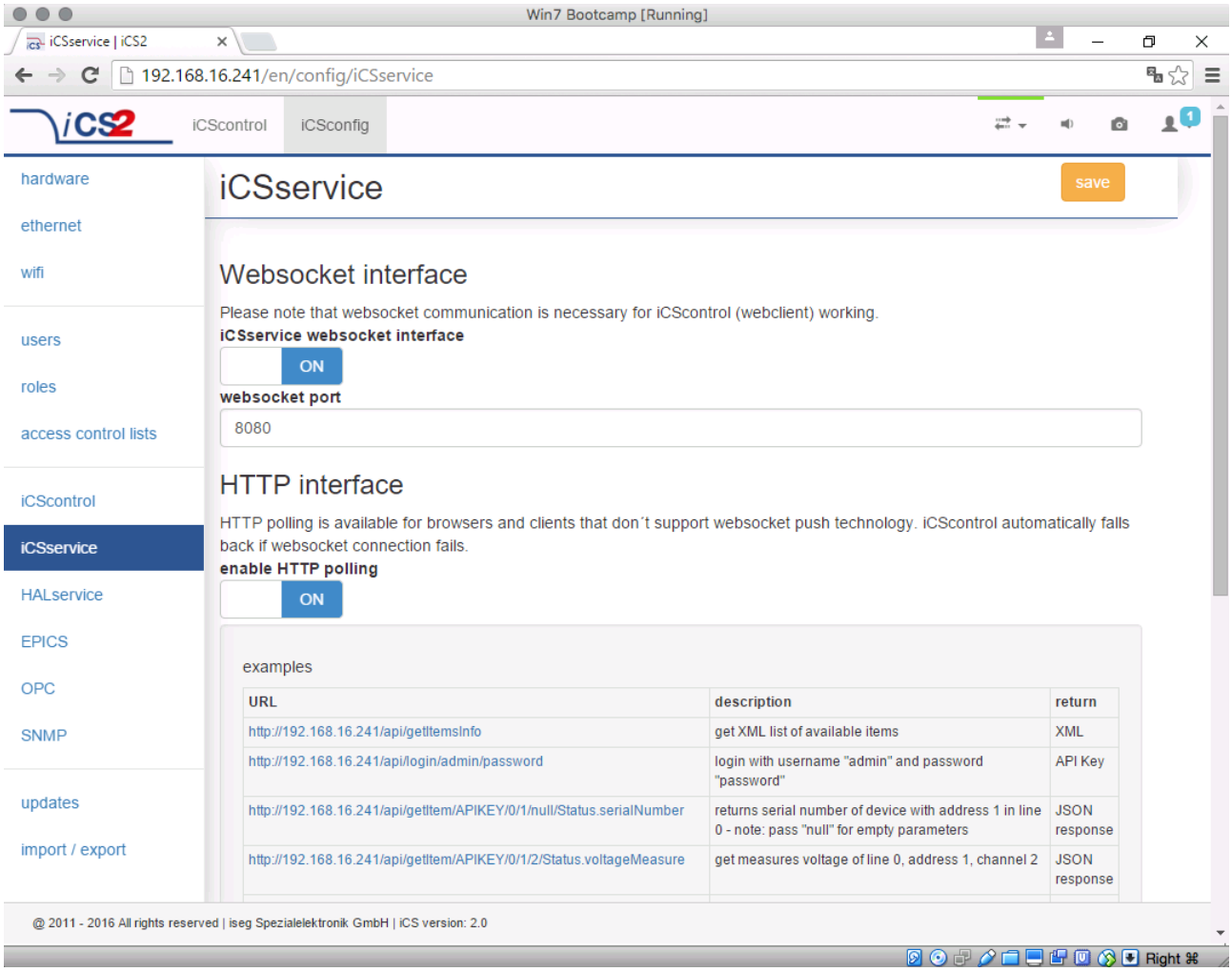


*Figure 4: iCSservice configuration*

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/ |

**INFORMATION**

INFORMATION

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/

### 1.5.1 HTTP interface

This interface gives quick access to iCSservice 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<br>$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<br>$line, $address, $channel can be set by wildcard '*' |
| http://<IP-of-ICS>:8081/api/getUpdate/$apikey/ | JSON Object | returns all changes collected by iCSservice since last getUpdate call for this client session |
| Notes:<br>Use “*” as wildcard, e.g. to set or get items on multiple channels at once.<br>Use “null” as empty set identifier, e.g. to obtain module specific objects without channel declaration. | | |

*Table 7*

| **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 8: Examples*

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

*Table 9*

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**

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/

### 1.5.3 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 [1].

**INFORMATION**

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

### 1.5.4 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 (substition 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**

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

1 

### 1.5.5 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.) |

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.

**INFORMATION**

INFORMATION

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

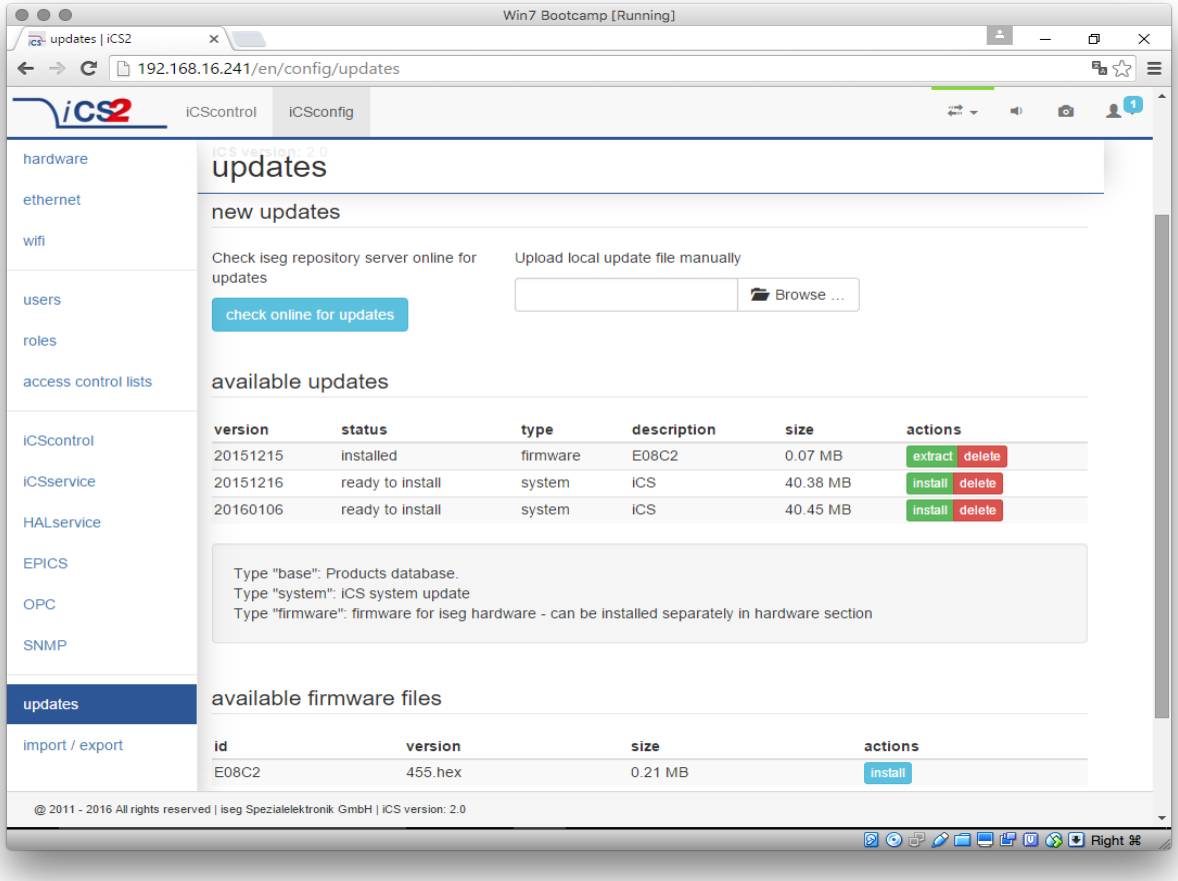


*Figure 5: Updates*

### 1.5.6 Custom scripts

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

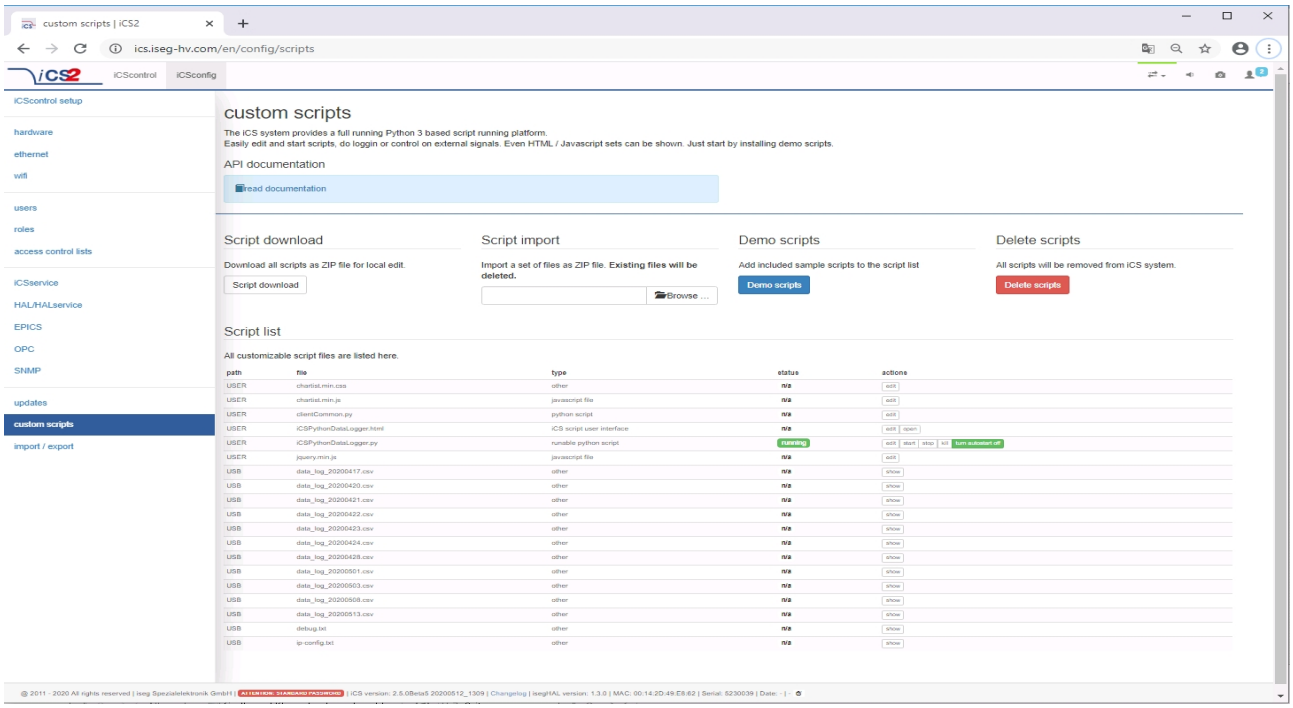


*Figure 6: Custom scripts setup*

| Custom scripts | |
|---|---|
| Script download | Load a copy of all installed files from iseg hardware */mnt/user/data/scripts* as ZIP file to your local download directory |
| Script import | Import a ZIP file to iseg hardware and extract it to */mnt/user/data/scripts*. Existing files will be overwritten. |
| Demo scripts | Add included sample scripts to */mnt/user/data/scripts 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 10: Custom script*

## 1.6 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.

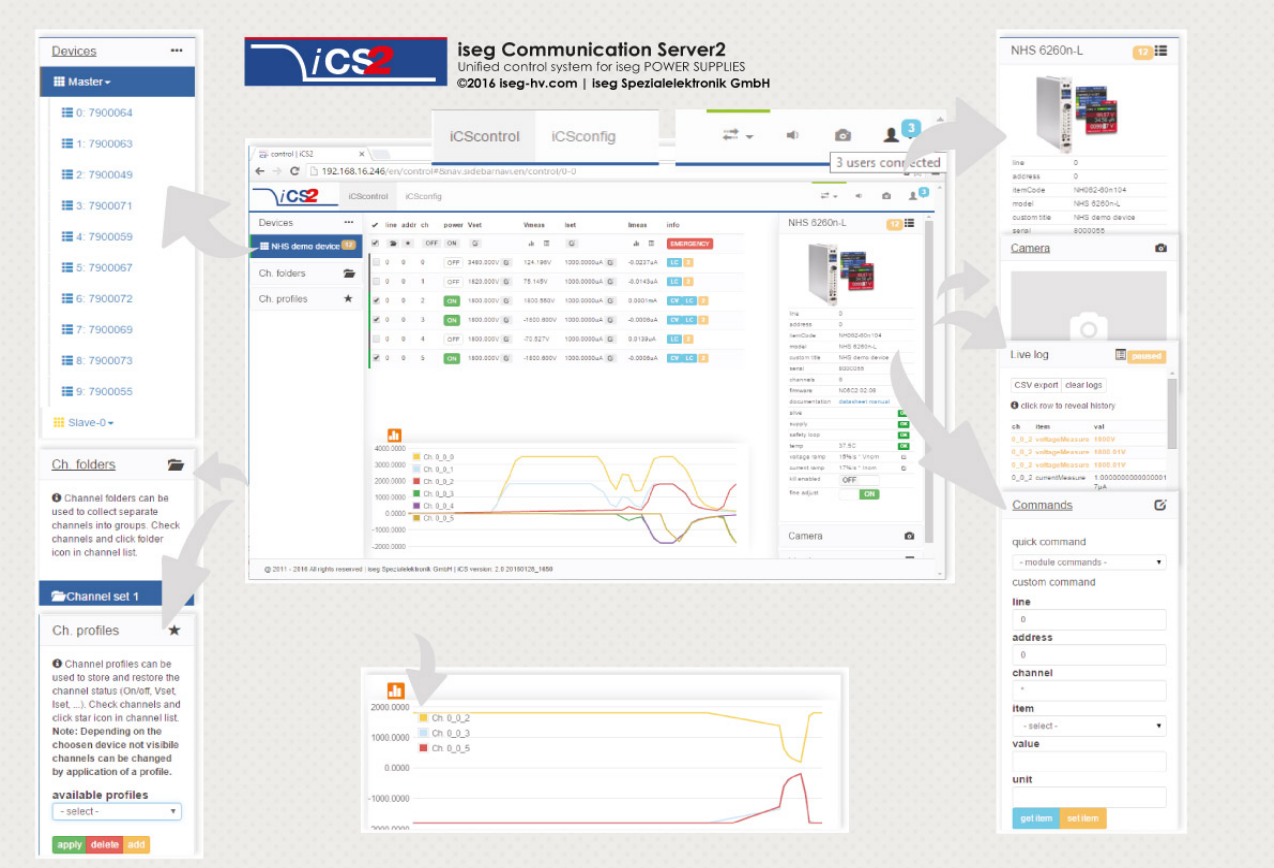


*Figure 7: iCScontrol*

### 1.6.1 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 |

| 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 |

| 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 |

### 1.6.2 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.

### 1.6.3 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.

### 1.6.4 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.

### 1.6.5 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.

### 1.6.6 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.

### 1.6.7 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.

### 1.6.8 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).