

Tables of contents

1.	General.	6
1.1	Power supply.	6
1.2	Power LED.	6
1.3	Status A LED.	7
1,4	Status B LED.	7
1.5	GSM LED.	7
1.6	Connect LED.	7
1.7	SD Card.	7
1.8	Communication ports.	7
1.9	CAN port.	8
1.10	10/100BaseT connection.	9
1.11	Button.	9
1.12	RTC.	9
1.13	I/O.	9
2.	Getting started.	11
2.1	Installation.	11
2.2	Connect to the iCex.	12
2.3	iCex setting, monitoring and tracing.	14
3.	Configure and Monitor the iCex.	18
3.1	Setting.	21
3.1.1	iCex.	21
3.1.2	Modem.	25
3.1.3	Drivers.	29
3.1.4	Serial Communication.	33
3.1.5	Counters.	34
3.2	Remote access.	35
3.2.1	OpenVPN	35
3.2.2	NAT.	37
3.2.3	Com-server.	39
3.3.	iCex maintenance.	41
3.3.1	Security.	41
3.3.2	Autoexec.	42

3.3.3	Files.	43
3.4	Monitor.	45
3.4.1	Trace.	45
3.4.2	Tree.	46

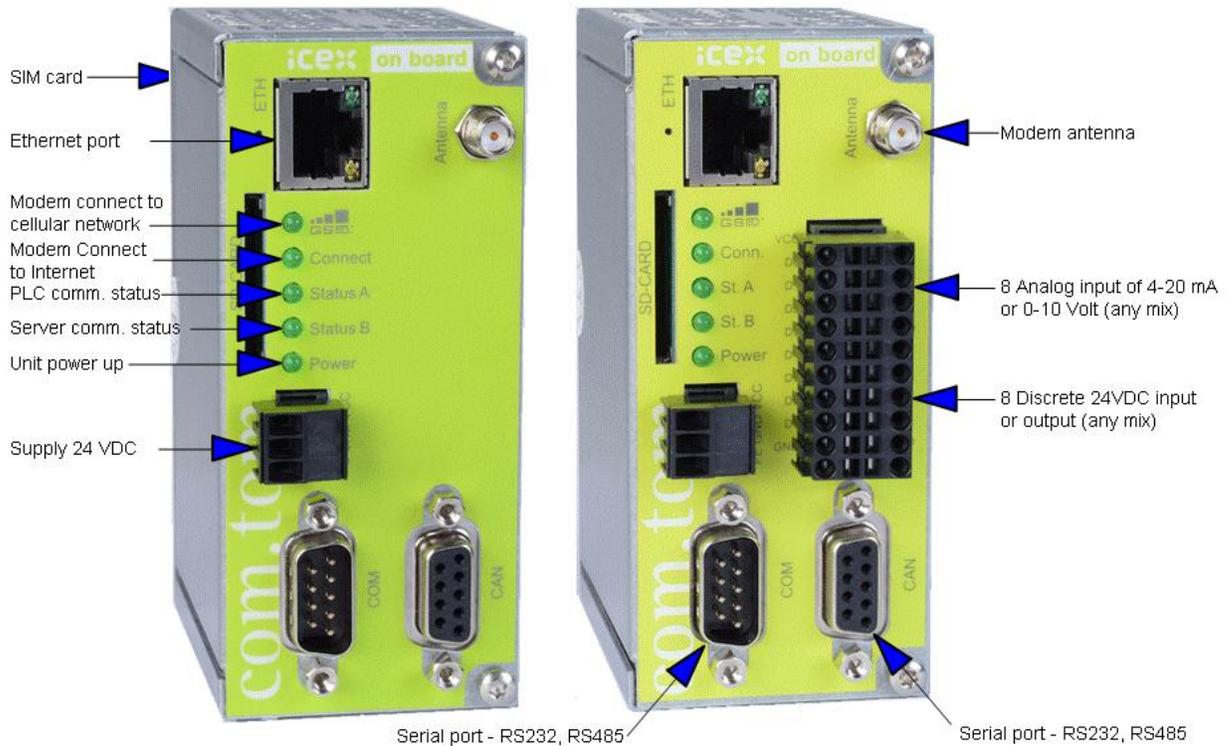
Appendix

1.	Address space	47
2.	Filter	51
3.	Chip.ini	52
5	Security	55
6.	OpenVPN remote configure and monitor	62

Revisions history

Rev	Date	Revision details
1	01.06.2016	First draft. Version 2.0.0.1
2	01.02.2017	Updates to version 2.0.1.6

1. General



1.1 Power supply

Supply voltage 24 VDC (-15% / +15%), maximum current 200 mA.

Connector assignment

VCC – 24VDC (+)

GND – 24VDC (-)

Include circuitry to protect against reverse-polarity connections.

1.2 Power LED

Power LED indicates iCex power supply status.

1.3 "Status A" LED

"Status A" LED indicates the status of the connection to the monitor/control systems:

Off - The initial LED status (after power up) is off. If it remains off it indicates that the iCex has no requests for communication with the monitor/control systems.

On - Communication ok to all monitor/control systems.

Blinking - iCex has a communication problem with at least one of the monitor/control systems.

The LED starts blinking after three (3) unsuccessful retries.

1.4 "Status B" LED

"Status B" LED indicates the status of the communication to the RealiteQ-COMP (Central Online Management Portal).

Off – The initial LED status (after power up) is off.

On - iCex is connected to the COMP and functioning normally.

Blinking - iCex has a communication problem with the server.

1.5 GSM LED

"GSM" LED indicates the status of the cellular modem connection to the cellular operator

Off – The initial LED status (after power up) is off.

On – The modem is power-on and connected to the Cellular network.

Blinking – The modem is in power-up and connection to the Cellular network (GSM) procedures.

1.6 Connect LED

"Connect" LED indicates the status of the cellular modem connection to the Internet.

Off – The initial LED status (after power up) is off.

On – The modem is connected to the Internet and functioning normally.

Blinking – The modem is in sign-in and connection procedures.

1.7 SD card

Not used.

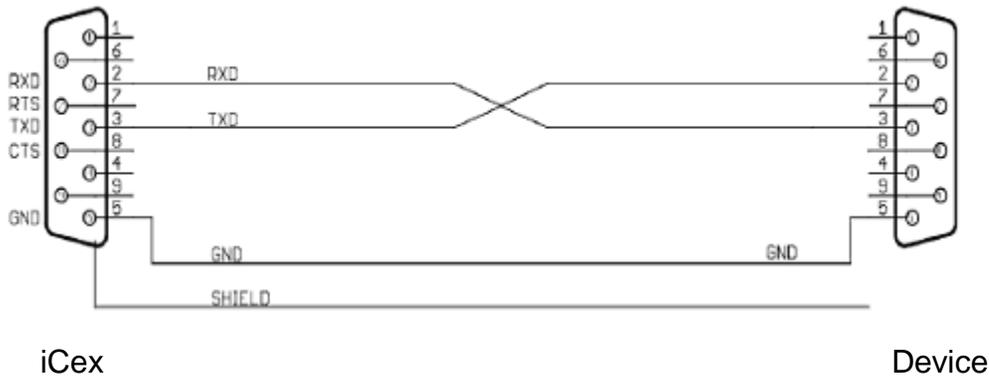
1.8 Communication Port

Combined RS232/RS485 interface D sub plug 9 pins (male). The COM interface can be used alternatively as RS232 or RS485. A suitable cable should be used for the selected interface. The RS485/RS232 interface is not galvanic isolated. The maximum transmission rate for the RS232 interface is 115k baud and 230k baud for the RS485 interface. The RS485 interface is setup for half duplex operation. Pull-up, pull-down and termination resistors for the RS485 interface are recommended in the connection cable.

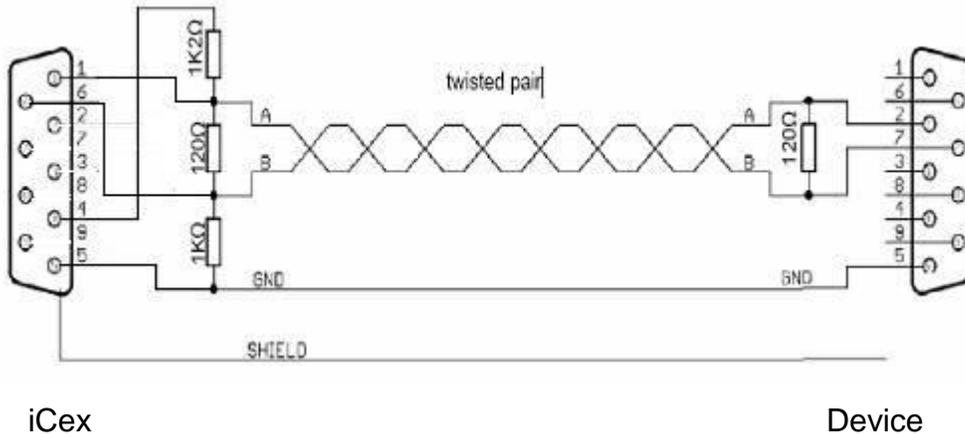
Communication pins assignment:

	RS232	RS485	RS422
Pin 1	NC	Y	A
Pin 2	RxD	NC	NC
Pin 3	TxD	NC	NC
Pin 4	NC	NC	A'
Pin 5	GND	GND	GND
Pin 6	NC	Z	B
Pin 7	RTS	NC	NC
Pin 8	CTS	NC	NC
Pin 9	NC	NC	B'
Housing	Connected with operational earth		

RS 232 Cable



RS 485 Cable



Pull-up resistors are optional.

1.9 CAN Port

Not used

1.10 10/100BaseT connection

Standard 10/100BaseT RJ45 connector with 2 status LEDs:

Yellow LED - Activity status: **On** - activity, **Off** - no activity. On in normal operation.

Green LED - Link status: **On** – link on, **Off** - no link. Blinking in normal operation.

1.11 Button

Internal button to restoring factory settings. Externally accessible with a pointed object such as a straightened out paper clip.

1.12 RTC

Real-time clock. Not battery power, the clock power consumption is very low and is powered with an external high capacity capacitor. The clock can continue to run up 3 weeks without external power. iCex synchronizes the RTC time with the server on power up and every 24 hours.

1.13 I/O

iCex model R10 with I/O has 8 analogs input current / voltage and 8 discrete 24 volt DC input / output. I/O pin assignment

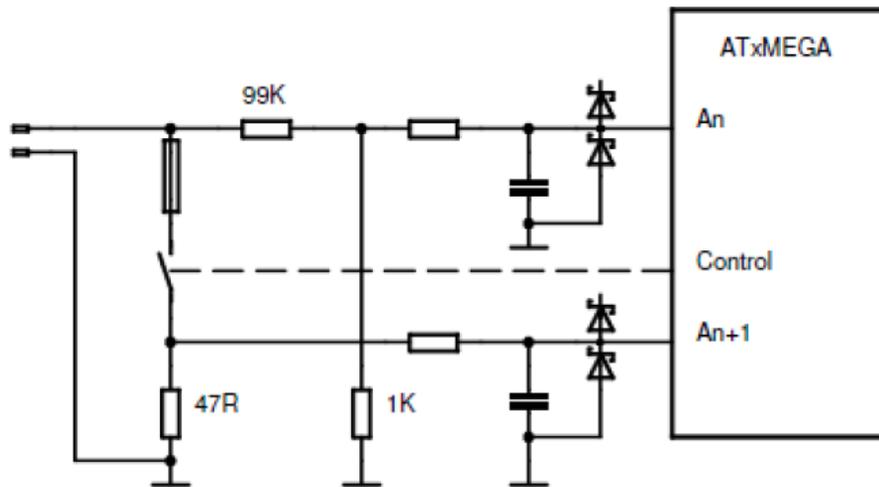
PIN	Description	Description	PIN
D-VCC	Power Supply for Digital I/O	Analog In 0	A0
D0	Digital I/O 0	Analog In 1	A1
D1	Digital I/O 1	Analog In 2	A2
D2	Digital I/O 2	Analog In 3	A3
D3	Digital I/O 3	GND for Analog In	A-GND
D4	Digital I/O 4	Analog In 4	A4
D5	Digital I/O 5	Analog In 5	A5
D6	Digital I/O 6	Analog In 6	A6
D7	Digital I/O 7	Analog In 7	A7
D-GND	GND for Digital I/O	GND for Analog In	A-GND

Analog in detail:

“GND for Analog In” is galvanic isolated from “GND for Digital I/O”. The Analog I/O signals are not galvanic isolated among themselves.

Technical data:

Analog Inputs: voltage input 0-10.1V or current input 0-25mA. Any analog input can be used as a voltage input or current input.



Digital in detail:

Digital I/O x can be used as an input or output. By using as an output, the signal status can be read back via the input function. In both applications, the signals refer to "GND for digital I/O" which is galvanic isolated from "GND for analog in". The digital I/O x signals are not galvanic isolated among themselves.

Technical data:

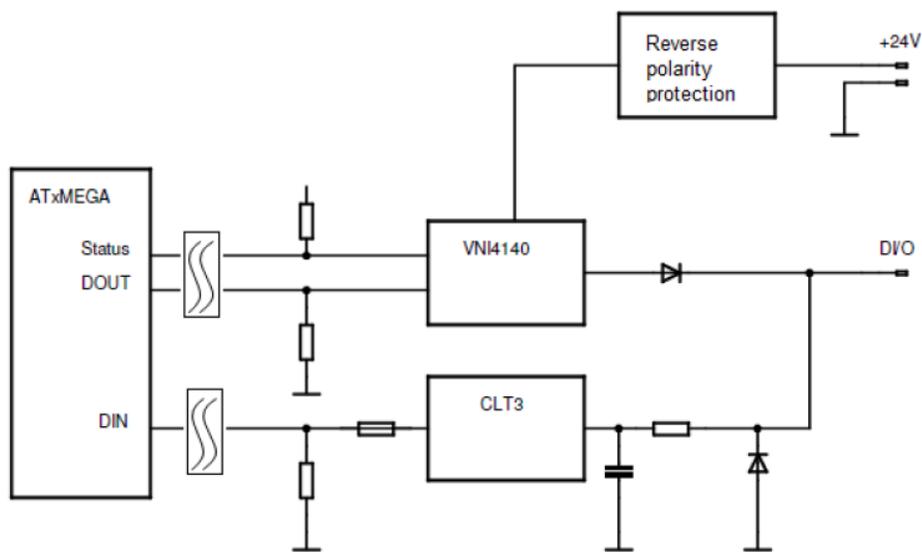
Digital Inputs: Sink, 24 V DC type 5 mA;

The nominal value for TRUE: 15 V DC min

The nominal value for FALSE: 5 V DC max

Digital Outputs: Transistor, 24 V DC, max 500 mA

Short-circuit and overload resistant.



2. Getting start

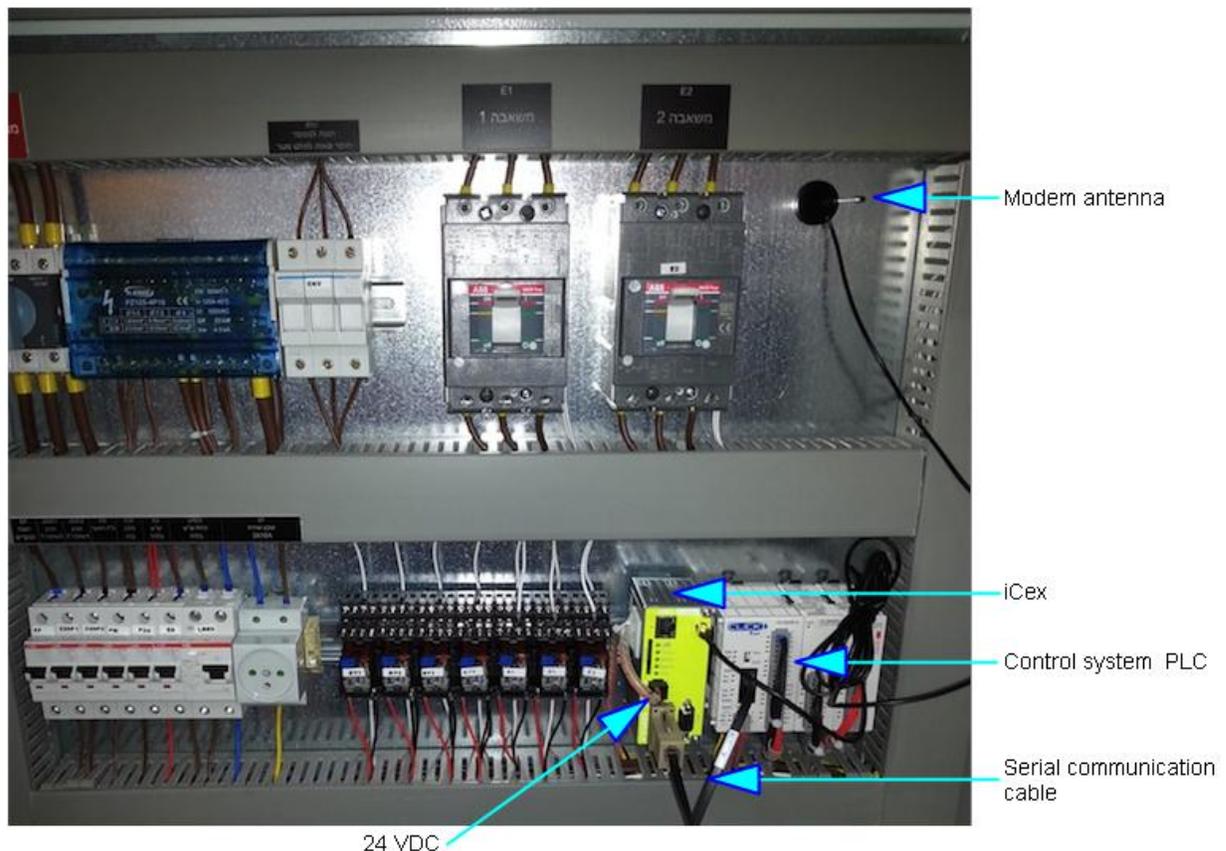
1. iCex installation.
2. Connect your PC to the iCex.
3. iCex setting, monitoring and tracing.

2.1 Installation

Follow the steps below to install the iCex.

1. Connect the Ethernet cable.
2. Connect the PLC communication cable.
3. Connect the antenna, and insert the SIM card (on the rear of the iCex)
4. Connect the iCex to a 24 VDC power source and check that the Power LED is on.

Typical iCex installation

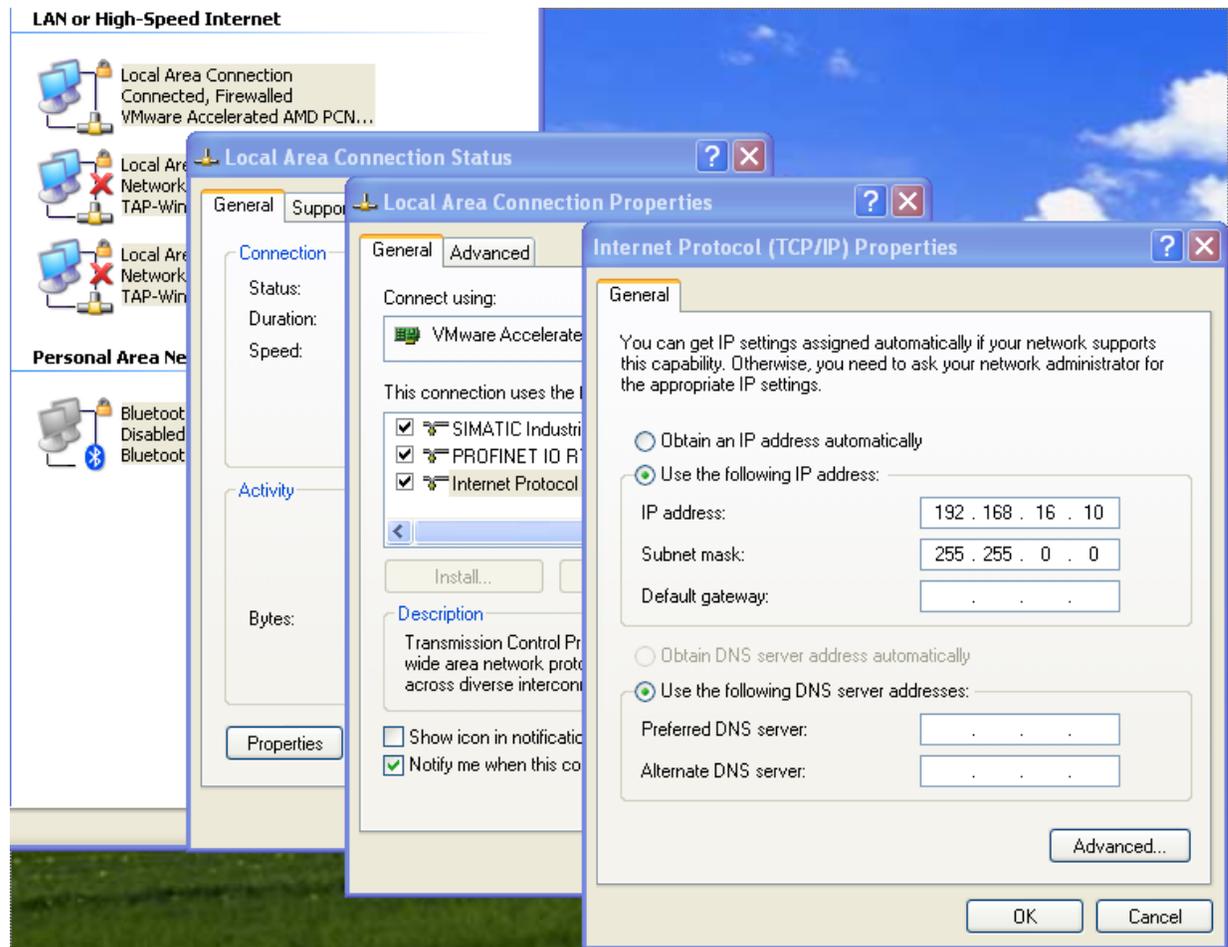


2.2 Connect your PC to iCex

Connect the iCex directly to your computer with a standard or twisted network cable or through a common switch. Check that the yellow link LED in the iCex Ethernet plug is on.

The iCex is shipped as standard with the IP address 192.168.16.201 and subnet mask: 255.255.0.0

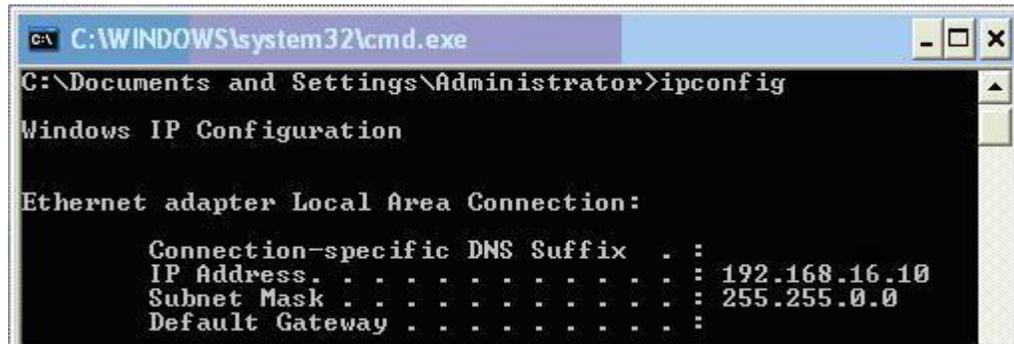
For initial commissioning, we recommend a separate direct PC to the iCex connection. Change your PC network setting to iCex network setting range:



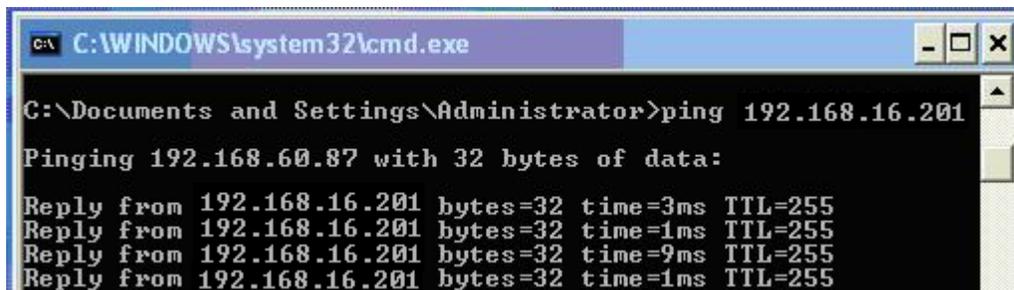
Follow the steps below to connect your PC to iCex

1. Select "PC network setting",
2. Select edit "Local Area Connection Properties" by right click on the local area connection icon and selecting "Properties" option.
3. Select "Internet Protocol (TCP/IP)" and click "Properties" button.
4. Select "Use the following IP address" option and fill the IP address and the Subnet mask to be in the same range of the iCex IP.

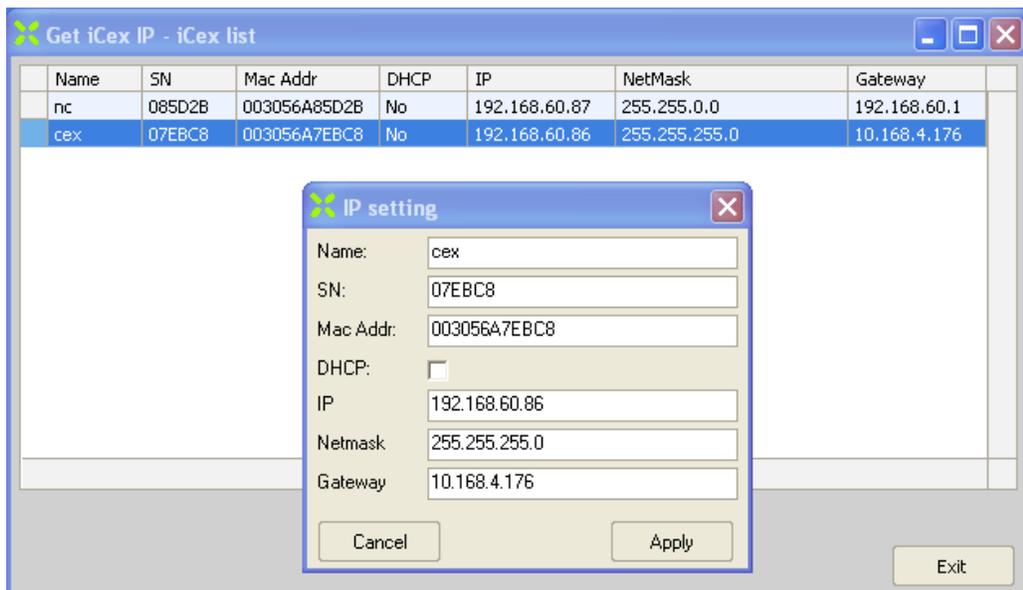
- Close all windows with OK buttons. Check your PC LAN configuration by typing "IPconfig" command in the "CMD" window



- Ping the iCex by typing "ping" command



- If you get a replay, you are ready to browse the iCex for the setting.
- If you do not know the iCex IP or you want to change it, run the GetIcexIP utility (you can download this program from <http://realiteq.com>)



A list of all connected iCex's will appear in the GetiCexIP main window.

Double click the iCex row to open the IP setting form, set the IP, Network mask, Gateway addresses or select DHCP to retrieve automatically the network settings from your server. The setting of these parameters affects the CHIP.INI file.

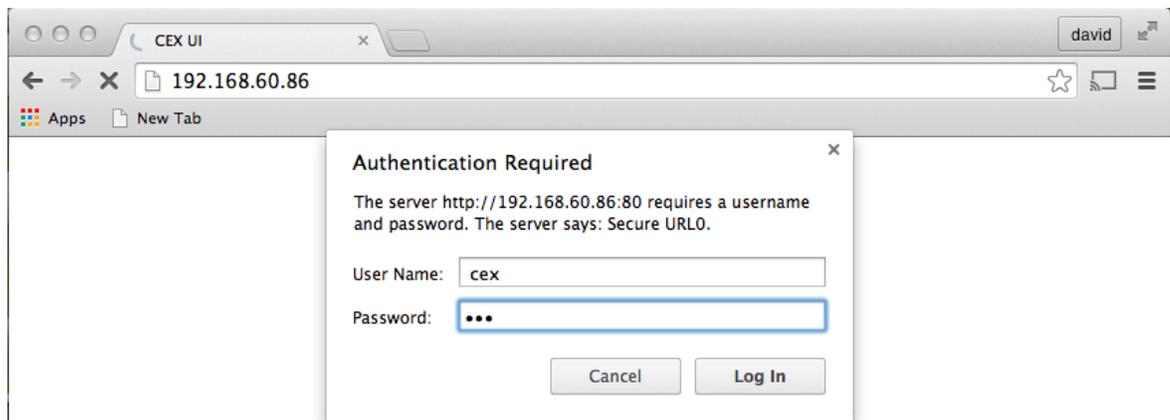
Only IP and Network mask settings are needed for iCex setting communication.

Note that the GetIcexIP program uses UDP broadcast to explore the network and to discover the connected iCex. Some PC blocks such communication for security reasons. Consult with the IT staff how to disable this restriction. The setting web interface uses standard HTTP communication on the standard Internet port 80.

2.3 iCex setting, monitoring and tracing.

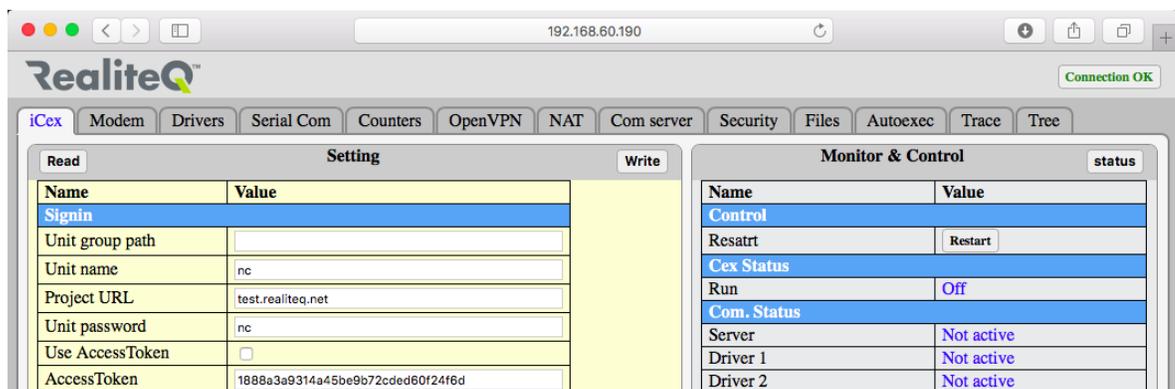
Follow the steps below to set iCex:

1. Start your browser and input the following URL in the address line: `http://192.168.16.201` or the new iCex IP.
2. Input the username and password (pay attention to uppercase and lowercase). Default login data: username = "cex" and password = "cex"



Note: Username and password should be changed for better security.

3. After successful login, you will get the setting monitor and control forms

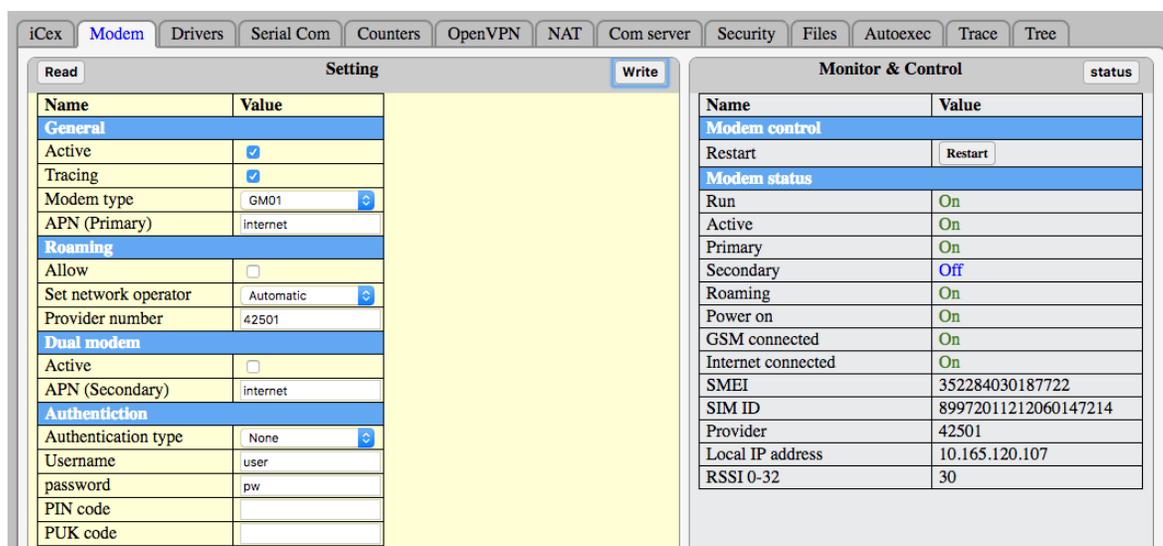


4. Make sure that the Web and iCex programs are running and if you are going to use a Cellular connection check the modem program too.



Write the new setting to the iCex and then reboot.

5. Connect to the cellular network and internet
Follow the steps below to connect your iCex to the cellular network and internet.



1. Insert the SIM card in the right direction to the slot on the back of the iCex.
2. Connect the antenna cord.
3. Choose "Modem" tab in the UI iCex setting.
4. Select "Use modem".
5. Select "Modem type":
GM01 – iCex version below 4.0, GPRS modem type.
GM02 – iCex version 4.0 and above, UMTS modem type.
GM04 – iCex version 4.0 and above, GPRS modem type.
6. Select "Tracing" for startup stage. On the right side of the screen, you can monitor the modem state or trace the modem activities in the Tracing tab. Later, you can deselect this option.
7. Enter the "APN" Access Point Name. Very common APN name is "internet". Consult with your network operator for the right APN.

8. Set the "Authentication" details. In most of the cases, the "Authentication type" has to set to "none" and rest of the fields to remain empty. Consult your network operator for the right authentication details.
9. After setting the connection details, make sure that the modem program is running, on the left side "Running" status = "On". If the status:
 - On – restart the modem run.
 - Off - go to "Autoexec" tab, check the "Modem" field, click "Write" button and then reboot the iCex.
 Watch the connection status on the right side of the "Modem" tab screen or the connection log in the "Tracing" tab.

iCex		Modem	Drivers	Serial Com	Counters	OpenVPN	NAT	Com s
iCex		Driver	Modem					
Message								
2017/01/23 10:05:56 : Set primary								
2017/01/23 10:05:56 : Modem Ver 1.0.0.5								
2017/01/23 10:05:56 : Power on								
2017/01/23 10:06:21 : Init GSM successfully								
2017/01/23 10:06:36 : Operator: IL ORANGE, No: 42501 Status: Current								
2017/01/23 10:06:36 : Operator: , No: 42506 Status: Available								
2017/01/23 10:06:36 : Operator: JAWWAL-PALESTINE, No: 42505 Status: Available								
2017/01/23 10:06:36 : Operator: IL Cellcom, No: 42502 Status: Forbidden								
2017/01/23 10:06:36 : Wait to network registration								
2017/01/23 10:06:37 : Registered to home network								
2017/01/23 10:06:37 : GPRS Network Registration successfully								
2017/01/23 10:06:38 : IMEI= 352284030187722								
2017/01/23 10:06:38 : SIM ID= 89972011212060147214								
2017/01/23 10:06:38 : RSSI (signal)= 30								
2017/01/23 10:06:38 : Link to Internet								
2017/01/23 10:06:43 : Link establish local IP= 10.165.120.107								
-								
-								

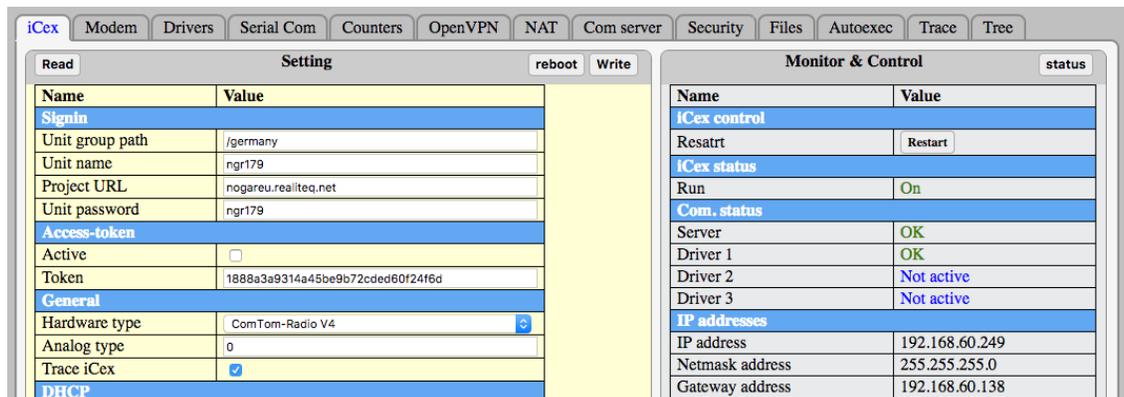
10. If the iCex modem failed to connect, correct the setting, restart the modem and monitor the results.
6. Connect iCex to RealiteQ-COMP

Before start trying to connect the iCex to the project in the RealiteQ-COMP, make sure that the iCex node with at least one communication node is appeared in your project also make sure that the project administrator created a user with the right permissions to connect the iCex.

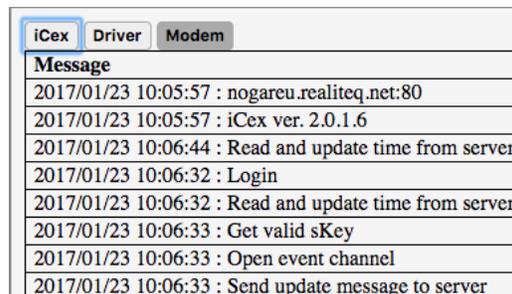


Follow the steps below to connect iCex to -COMP

1. Open the "Cex" tab.



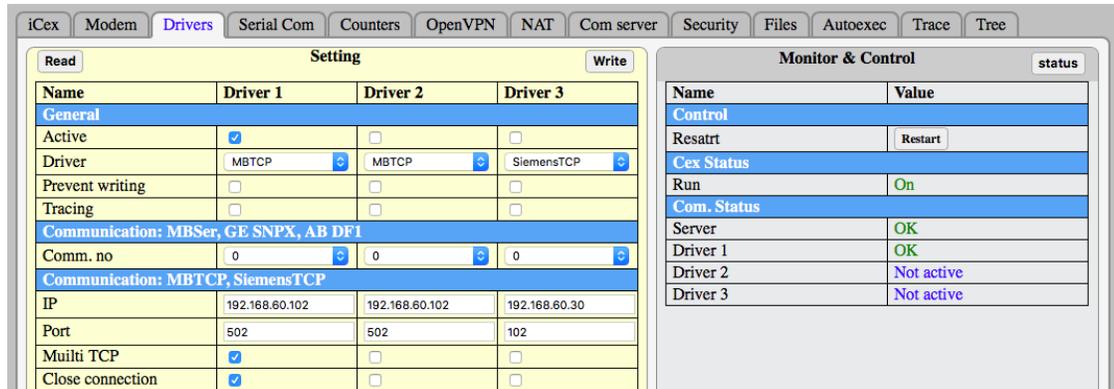
2. Edit the "Sign in" fields: "Unit name", "Project URL" and "Unit password".
3. Restart the iCex program, if iCex program not running, go to "Autoexec" tab, check iCex field, click "Write" button and reboot.
4. Watch the connection status on the right side of the "Cex" tab screen or the connection log in the "Tracing" tab. If the iCex failed to connect to RealiteQ-COMP, correct the setting, restart the iCex and monitor the result.



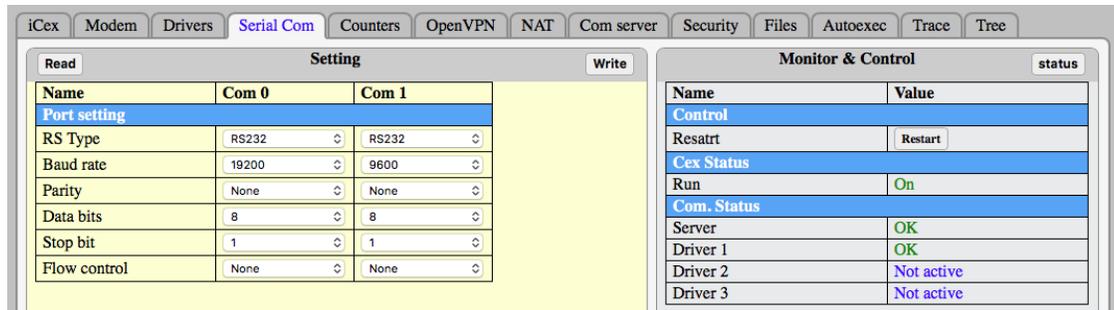
7. Connect iCex to system PLC.

Follow the steps below to connect iCex to system PLC.

1. Open the "Drivers" tab.



2. Activate drive 1, select "Driver" type and set the communication details. For network drivers set the "IP" and the "Port" fields, for serial drivers set the "Comm.no" field and switch to the "Serial Com" tab for the serial port setting.



3. Restart the iCex program to adopt the new setting.
4. Watch the connection status on the right side of the "Cex" tab screen or the connection log in the "Tracing" tab. If the iCex failed to connect to PLC, correct the setting, restart the iCex and monitor the result.

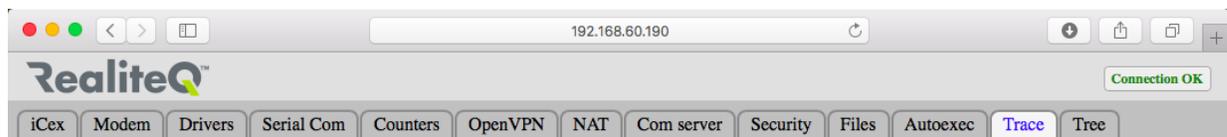
3. Configure and Monitor the iCex.

The iCex runs multiple programs simultaneously:

1. **Web** - Operates the web interface for configuring and monitor the iCex.
2. **Modem** - Operates and monitor the cellular modem.
3. **Cex** - Operates the communication to the COMP server and the communication to the connected equipment's like PLC.
4. **OpenVPN** - Allows (on demand) to establish and take care of the iCex in a secure OpenVPN connection.
5. **NAT** - Network Address Translation. Allows (on demand) the iCex to operate as a gateway to the global network. The NAT receives packets from the global network and forwards them to the relevant host in the local network; then receives host answer packets and forwards them to the global network. Working only under secure OpenVPN connection. Allows to reach, maintain, monitor and programming the connected equipment's
6. **Comserver** - Allows (on demand) the iCex to provide access to its serial ports from the global network. Working only under the secure OpenVPN connection. Allows to reach, maintain, monitor and programming the connected equipment's

All iCex settings saved in the chip.ini file. The auto executes programs list are saved in the autoexec.bat file. Both files configure with the web UI.

The configuration and monitor form includes several tabs:



1. Setting:

1. [iCex](#)
2. [Modem.](#)
3. [Drivers.](#)
4. [Serial Communication.](#)
5. [Counters.](#)

2. Remote access:

1. [OpenVPN.](#)
2. [NAT.](#)
3. [Com Server.](#)

3. iCex maintenance :

1. [Security.](#)

2. [Files.](#)
3. [Autoexec.](#)
4. **Monitoring:**
 1. [Trace.](#)
 2. [Tree.](#)

Each tab displays on the left side the current tab setting and on the right side monitors the operation status, at 5 seconds intervals.

Command buttons:

Read: Force to re-read and display the current setting.

Write: Update the iCex with the modified setting.

Reboot: Reboot the iCex. After reconfiguring the autoexec or in order to take care of some setting changes, the iCex must re-boot or re-power.

Status: Force to read and display iCex status.

Restart: Restart Modem or iCex program to adopt the new settings.

3.1 Setting

3.1.1 iCex.

✓ iCex - Setting:

Setting		reboot	Write
Name	Value		
Signin			
Unit group path	/germany		
Unit name	ngr179		
Project URL	nogareu.realiteq.net		
Unit password	ngr179		
Access-token			
Active	<input type="checkbox"/>		
Token	1888a3a9314a45be9b72cded60f24f6d		
General			
Hardware type	ComTom-Radio V4		
Analog type	0		
Trace iCex	<input checked="" type="checkbox"/>		
DHCP			
Use DHCP	<input checked="" type="checkbox"/>		
Manual IP addresses			
IP address	192.168.16.201		
Netmask address	255.255.255.0		
Gateway address	10.195.124.31		
DNS address	192.117.235.237		
Clock			
Time zone	Asia/Jerusalem		
Date & Time	2017-01-23 11:02:47		
Clock modify	<input type="button" value="Apply"/>		

Sign-in

Unit group path: Define the iCex group path. If iCex appears under project root, keep this field empty. If the iCex appears under group enter the iCex group path. Example: for iCex path */group/cex* set */group* in Unit group Path and *cex* in unit name.

Unit name: Define the name of the iCex. Limit to 20 characters. This name will show up with the software tool when the network is scanned, like GetiCexIP utility. The unit name is used as the iCex path and as the iCex username for login. Do not use any special characters and do not add / as a prefix.

Project URL: The URL is built from the project name as a prefix to the server URL (URL= projectname.realiteq.net). The URL is not case sensitive. Do not use special characters in the project name.

Unit password: Defines a password for the iCex for sign-in to RealiteQ-COMP. The password is case sensitive. Important notice: To avoid security leaks you must define a unique password to each ICex. The iCex will use unit name and password for sign-in (only when Use Access-Token is unchecked).

Access-Token: If Access-Token checked, the iCex would use the Access-Token for sign-in instead of using the username and password. An Access-Token is an opaque

string that identifies the user and its privileges that the iCex can use to sign-in to the server. The Access-Token is generated by the server and is attached to a specific path. For more details how to create user access token see in RealiteQ-UI setting.

General

Hardware type: Define the iCex hardware type:

1. ComTom-Basic - iCex basic (two serial port, no modem).
2. ComTom-Basic V4 - same as 1 but version 4 and above.
3. ComTom-Radio - iCex (one serial port, with a modem).
4. ComTom-Radio V4 - same as 3 but version 4 and above.

Analog type: For iCex with I/O. Mask to select whether the analog input measures voltage or current. Bits mask 0-7, bit = 1: voltage, bit = 0: current, for example: Analog = 0: all inputs set to measures current, Analog = 1: input 1 is set to measures voltage and the rest current, Analog = 5: inputs 1 and 3 set to voltage and the rest set to current.

Trace iCex: Generate trace messages for iCex activity via Telnet or SSH terminal.

DHCP

Use DHCP: When iCex attempts to connect to the network, the DHCP client software in iCex sends a broadcast query requesting necessary network IP's information.

Checked - The iCex gets its IP's configuration from the network server.

Unchecked – The iCex gets its IP's manually. See below.

Remark: To adopt the new setting, the iCex needs to reboot.

Manual IP address

Define the iCex network static IP's address (Relevant only when DHCP is unchecked):

IP address: iCex IP network address.

Netmask address: A Netmask is a 32 bits mask used to divide an IP address into subnets and specify the networks available connection, default: 255.255.255.0.

Gateway address: The gateway address (or default gateway) is the router IP address that iCex uses to forward packets to the Internet.

DNS address: DNS stands for Domain Name System, Domain name system servers match domain names to their associated IP.

Gateway and DNS are needed only when iCex is manually connected to the Internet via the Ethernet connection. Consult with your IT manager about all the manual IP's right values.

Remark: to adopt the new setting the iCex needs to reboot.

Clock

Time zone: The iCex has a RTC (Real Time Clock) with capacitor backup for about 3 weeks. When the iCex is connecting to the server and every 24 hours, the iCex asks for clock updates. The Time-zone needs to be set for right local time setting. For finding the right value, look at: [Time Zone website](#).

It is important to set the right Time zone to allow the iCex to adjust the clock according to the Zone and the daylight changes.

Examples:

+3 - Europe/Moscow

+2 - Asia/Jerusalem

+1 - Europe/Berlin

0 - Europe/London

-3 - America/Sao_Paulo

-4 - America/Halifax

-5 - America/New_York

-6 - America/Chicago

-7 - America/Phoenix

Date &Time: Display and setting the current iCex internal clock.

Modify: Manual clock setting.

✓ **iCex - Monitor & Control:**

Monitor & Control		status
Name	Value	
iCex control		
Resatrt	Restart	
iCex status		
Run	On	
Com. status		
Server	OK	
Driver 1	OK	
Driver 2	Not active	
Driver 3	Not active	
IP addresses		
IP address	192.168.60.190	
Netmask address	255.255.0.0	
Gateway address	192.168.60.1	

iCex control

Restart: Restart the iCex program. The iCex sign-out and then sign-in with the latest setting modification.

iCex status

Run: iCex-program run status.

Com. status

Server: iCex to RealiteQ-COMP communication status.

Driver's: iCex to connected equipment communication status: Not active, bad or OK.

IP addresses

IP, Netmask and Gateway addresses: Current iCex network interface IP's addresses.

✓ **iCex - tracing:**

iCex Driver Modem	
Message	
2017/01/23 10:05:57	: nogareu.realiteq.net:80
2017/01/23 10:05:57	: iCex ver. 2.0.1.6
2017/01/23 10:06:44	: Read and update time from server
2017/01/23 10:06:32	: Login
2017/01/23 10:06:32	: Read and update time from server
2017/01/23 10:06:33	: Get valid sKey
2017/01/23 10:06:33	: Open event channel
2017/01/23 10:06:33	: Send update message to server

Steps to initialize and connect the iCex to the COMP:

- Read from server and update iCex clock
- Login and get valid security key
- Open event channel to enable the option to get items list and write command.
- Update COMP server with nodes value / state.

3.1.2 Modem.

✓ iCex - Setting:

Name	Value
General	
Active	<input checked="" type="checkbox"/>
Tracing	<input checked="" type="checkbox"/>
Modem type	GM01
APN (Primary)	internet
Roaming	
Allow	<input type="checkbox"/>
Set network operator	Automatic
Provider number	42501
Dual modem	
Active	<input type="checkbox"/>
APN (Secondary)	internet
Authentication	
Authentication type	None
Username	user
password	pw
PIN code	
PUK code	

General

Use Modem: check to activate the modem for global communication.

Trace modem: check to activate modem activity.

Modem types:

1. GM01 – iCex ver. 1 to 3 with GPRS modem
2. GM02 – iCex version 4 and above with UMTS
3. GM03 – Edge Not available yet.
4. GM04 – iCex ver. 4 and above with GPRS modem support mux function.

APN (Primary): Access Point Name is the name of the gateway between the Cellular mobile network and the public Internet. The cellular modem needs the APN to make a data connection to the cellular operator. Very common APN name is "Internet". Consult with your cellular operator about the right APN. For APN and authentication details browse at [Operators APN website](#).

Roaming

Allow: Roaming service is the ability to get access to different operators as defined in the SIM. You should use this option only with an international SIM.

Set network operator: Set the Mode the iCex selects the current operator while in roaming mode:

Automatic – The iCex selects the first available operator.

Manual – The iCex selects the operator according to the setting of the operator number. Operator number must be one of the available operators that were queried with reading operators and appeared in the modem logs (appeared in the trace tab).

Manual/Automatic – If manual selection fails, use the automatic mode

Operator number: Set the preferred operator numeric name to work in the manual mode. An operator numeric name is a unique number assigned to every telecommunications operator in all countries of the world. You can find the available numbers in the modem trace or at [Operator codes website](#).

Dual Modem

Active: Enable the modem redundancy. Model R9 contains two modems; each modem has a separate antenna and a separate SIM card. The iCex switches to the secondary modem when there is a communication problem with the primary modem and vice versa.

APN (Secondary): Secondary Access Point Name APN.

Authentication

Authentication type:

1. None.
2. TAP
3. CHAP.

For the both authentication types, the iCex needs username and password to authenticate the connection to network.

Username: Authentication to data network username.

Password: Authentication to data network password.

Pin code: PIN (Personal Identification Number). The PIN acts like a password, prevents unauthorized use of the SIM. This is a numeric code, which must be entered for the modem to connect (unless the PIN security feature is turned off).

PUK code: PUK (PIN Unlock Key), is used to reset a PIN (Personal Identification Number) that has been lost or forgotten.

✓ **Modem - Monitor & Control:**

Monitor & Control		status
Name	Value	
Modem control		
Restart	<input type="button" value="Restart"/>	
Modem status		
Run	On	
Active	On	
Primary	On	
Secondary	Off	
Roaming	On	
Power on	On	
GSM connected	On	
Internet connected	On	
SMEI	352284030187722	
SIM ID	89972011212060147214	
Operator No	42501	
Local IP address	10.165.120.107	
RSSI 0-32	30	

Modem control

Restart: Restart the modem program. The modem re-powers and restarts use the latest setting modification.

Modem status

Run: Modem-program status. The Modem-program runs in two modes: Idle - "Active" unchecked or Active - "Active" checked.

Active: Status of modem activation for global communication option.

Primary: Communicate with the primary modem.

Secondary: Communicate with the secondary modem (Effective only in R9 model).

Roaming: Connect to a roaming network.

Power on: Modem power status.

GSM connected: iCex modem to cellular network connection status.

Internet connected: iCex modem to Internet connection status.

IMEI; Modem IEMI. The IEMI (International Mobile Station Equipment Identity) is a unique number given to mobile equipment.

SIM ID: SIM ID. The number that appears on the back of the SIM card.

Operator No: Current operator numeric name.

Local IP: iCex modem IP in the cellular network.

RSSI: The signal strength (RSSI) in a range of 0 to 31. -1: Not available, under 10: bad signal, change the antenna position. Above 24: Good signal. Be aware that the signal strength affects also the communication speed. The RSSI rate updates every one hour.

RSSI to dBm

RSSI 0 equal to -113 dBm or less

RSSI 1 equal to -111 dBm

RSSI 2...30 equal to -109...-53 dBm

RSSI 31 equal to -51 dBm or greater

RSSI 99, not detectable

✓ **Modem - tracing:**

iCex	Driver	Modem
Message		
2017/01/23	10:05:56	: Set primary
2017/01/23	10:05:56	: Modem Ver 1.0.0.5
2017/01/23	10:05:56	: Power on
2017/01/23	10:06:21	: Init GSM successfully
2017/01/23	10:06:36	: Operator: IL ORANGE, No: 42501 Status: Current
2017/01/23	10:06:36	: Operator: , No: 42506 Status: Available
2017/01/23	10:06:36	: Operator: JAWWAL-PALESTINE, No: 42505 Status: Available
2017/01/23	10:06:36	: Operator: IL Cellcom, No: 42502 Status: Forbidden
2017/01/23	10:06:36	: Wait to network registration
2017/01/23	10:06:37	: Registered to home network
2017/01/23	10:06:37	: GPRS Network Registration successfully
2017/01/23	10:06:38	: IMEI= 352284030187722
2017/01/23	10:06:38	: SIM ID= 89972011212060147214
2017/01/23	10:06:38	: RSSI (signal)= 30
2017/01/23	10:06:38	: Link to Internet
2017/01/23	10:06:43	: Link establish local IP= 10.165.120.107
-		

Steps to initialize and connect the iCex modem to the network:

- Modem power on
- Initialize GSM connection.
- Read network operators
- Register to GSM network.
- Read IMEI ID
- Read SIM ID
- Read RSSI
- Switch to data mode and link to Internet
- Get IP

3.1.3 Drivers.

✓ Drivers - Setting:

Setting			
Name	Driver 1	Driver 2	Driver 3
General			
Active	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Driver type	MBTCP	MBTCP	SiemensTCP
Prevent writing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Trace driver	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communication: MBSer, GE SNPX, AB DF1			
Comm. no	0	0	0
Communication: MBTCP, SiemensTCP			
IP address	192.168.60.102	192.168.60.102	192.168.60.30
Port	502	502	102
Muilti TCP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Close connection	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Timeout			
Timeout	2000	2000	2000
Sleep time	0	0	0
Swap			
Swap byte	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Swap word	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tasks			
Update clock	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start address	r1501	r1501	r1501
Update date	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start address	r1505	r1505	r1505
Block write	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Address	b10	b10	b10

General

iCex supports up to 3 drivers running simultaneously.

Active: activate the driver

Driver type iCex supports 6 different drivers:

1. MBSER - Modbus RTU, serial.
2. MBTCP - Modbus TCP/IP, network.
3. RIOCard - iCex with I/O card, internal.
4. Siemens TCP - Siemens S7 profi-net, network.
5. SNPX - General-Electric GE 9030 serial.
6. DF1 - Allen Bradley DF1 serial

Prevent writing: iCex blocks write commands to PLC.

Trace driver: Display detailed driver activity via telnet terminal.

Communication (set for serial driver)

Com: Set the active serial com (communication) port: 0 or 1. iCex B2 has two serial ports. Relevant to drivers that use serial connection: MBSer, SNPX and DF1.

Communication (set for network driver)

IP: PLC IP address. Each driver can support up to 32 stations. For each station, you should set an IP address. You can enter from the UI only the IP address of the first PLC. If more stations are connected, you should add\edit their addresses directly to the chip.ini.

Port: The TCP port is common for all driver stations. Standard port for Modbus = 502 and for Siemens = 102.

MultiTCP: Checked - For working with several PLC's each one with different IP address. Unchecked - For working with ModbusTCP to Modbus RTU converter, in this mode the iCex communicates with one IP address for several stations.

Close Socket: Some PLC closes the TCP connection after an inactivity timeout. This behavior causes communication error when the iCex tries to re-poll the PLC. To avoid this situation, check this option.

Remark: Siemens driver needs another two parameters: rack and slot. For S7-300 set rack= 0 slot= 2 (default values) for S7-1200 and S7-1500 rack= 0 slot= 0, these parameters appear in the chip.ini for each driver.

Timeout

Timeout: The maximum time the iCex will wait to get the PLC answer. Default 1000 msec.

Sleep Mode: In milliseconds, for old slower PLC sometimes sleep time needed between messages to slow traffic.

Swap

Swap word: In Modbus driver, some PLC receives and transmits long and float data in a different word order. Swap word corrects this problem.

Swap byte: In Modbus driver, some PLC receives and transmits integer data in a different byte order. Swap byte corrects this problem.

Tasks

Update clock: iCex updates PLC every minute with clock and server communication status. 4 registers:

1. Day of week 1-7.
2. Hour.
3. Minute.
4. Communication to server status 1 - ok, -1 - fault.

Start address: start address in target PLC.

Update date: iCex updates PLC every hour with date status. 3 registers:

1. Day.
2. Week.
3. Year.

Start address: start address in target PLC.

Block write: iCex polls the PLC every 1 minutes and if block write address element is on, the iCex will block remote writes messages.

Address: block address in target PLC.

✓ **Drivers - Monitor & Control:**

Monitor & Control		status
Name	Value	
iCex control		
Resatrt	<input type="button" value="Restart"/>	
iCex status		
Run	On	
Com. status		
Server	OK	
Driver 1	OK	
Driver 2	Not active	
Driver 3	Not active	

Control

Restart: Restart the iCex program. The iCex restart and use the latest drivers setting modification.

Cex Status

Run: iCex-program run status.

Com. Status

Server: iCex to RealiteQ-COMP communication status.

Driver's: iCex to connected equipment's communication status: Not active, bad or OK.

3.1.4 Serial Communication.

✓ Serial Communication - Setting:

Setting		
Name	Com 0	Com 1
Port setting		
RS type	RS232	RS232
Baud rate	19200	9600
Parity	None	None
Data bits	8	8
Stop bit	1	1
Flow control	None	None

Port setting

RS Type: Communication type

1. .RS232.
2. RS422.

Baud: Speed:

1. 4800.
2. 9600.
3. 19200.
4. 38400.

Parity: Check sum:

1. None.
2. Odd.
3. Even.

Data bits: 7, 8.

Stop bits: 1, 2.

Flow control:

1. None.
2. XON/XOFF,
3. RTS/CTS.

✓ **Serial Communication - Monitor & Control:**

Monitor & Control		status
Name	Value	
iCex control		
Resatrt	<input type="button" value="Restart"/>	
iCex status		
Run	On	
Com. status		
Server	OK	
Driver 1	OK	
Driver 2	Not active	
Driver 3	Not active	

Control

Restart: Restart the iCex program. The iCex restarts and uses the latest drivers setting modification.

Cex Status

Run: iCex-program run status.

Com. Status

Server: iCex to RealiteQ-COMP communication status.

Driver's: iCex to connected equipment communication status: Not active, bad or OK.

3.1.5 Counters.

The iCex can run to each of his eight (8) digital inputs a counter. The counter can count pulses or working time (In seconds). Each input counter function handles three counters, each counter can configure to a different type of reset: none, reset daily, reset weekly and reset monthly. For pulses counter the iCex also calculates the flow rate. Each counter keeps the last value prior to reset and allow displaying the count of the previous day, the previous week or last month. Input counter function also calculates the flow by a number of pulses obtained at a specified time. The counter's values can be read/write with the I/O driver, for counter 1:

D1 to D3 - Accumulate counters

D4 to D6 - Previous counters counting.

F1 – Flow.

Counter 2 addresses: D11 to D16 and F11.

Do not forget to enable the PFI_ENABLE in the chip.ini for saving counters values in power failure.

✓ Counters - Setting:

Read		Setting						Write
General								
Active	<input type="checkbox"/>							
Counters								
Name	counter 1	counter 2	counter 3	counter 4	counter 5	counter 6		
Active	<input checked="" type="checkbox"/>	<input type="checkbox"/>						
Type	Pulse	Pulse	Pulse	Pulse	Pulse	Pulse		
flow base-time	60	60	60	60	60	60		
Reset type 1	None	None	None	None	None	None		
Reset type 2	Day	Hour	Day	Hour	Hour	Hour		
Reset type 3/td>	Month	Month	Week	Day	Day	Day		
Reset hour	0	0	0	0	0	0		
Reaset day	7	7	7	7	7	7		

General

Active: Activate the counters procedure.

Counters

Active: Activate the specific counter.

Flow base-time - In seconds, the iCex calculate the flow by (last count – previous count) * 3600 / (flow base-time). Flow base time is the difference in time between the tow counts.

Reset type 1, Reset type 2, Reset type 3 - The iCex runs three (3) counters, to each counter there are five options for reset:

1. None - Counts forever.

2. Hour.
3. Day.
4. Week
5. Month

Reset Hour: 0 - 23. The hour to counter reset. For "Day" and "Week" reset types.

Reset Day: 1 – 7. The day to counter reset. For "Week" reset type.

3.2 Remote access

3.2.1 OpenVPN

The iCex is designed to offer easy and secure remote access for setting and for remote programming of the connected PLCs. This allows the System integrators to troubleshoot the system remotely without going on the site, drastically reducing support costs.

A fully secure SSL-based VPN tunnel is used for all traffic. The information exchanged during the communication is encrypted via SSL allowing only authenticated users to connect to the iCex.

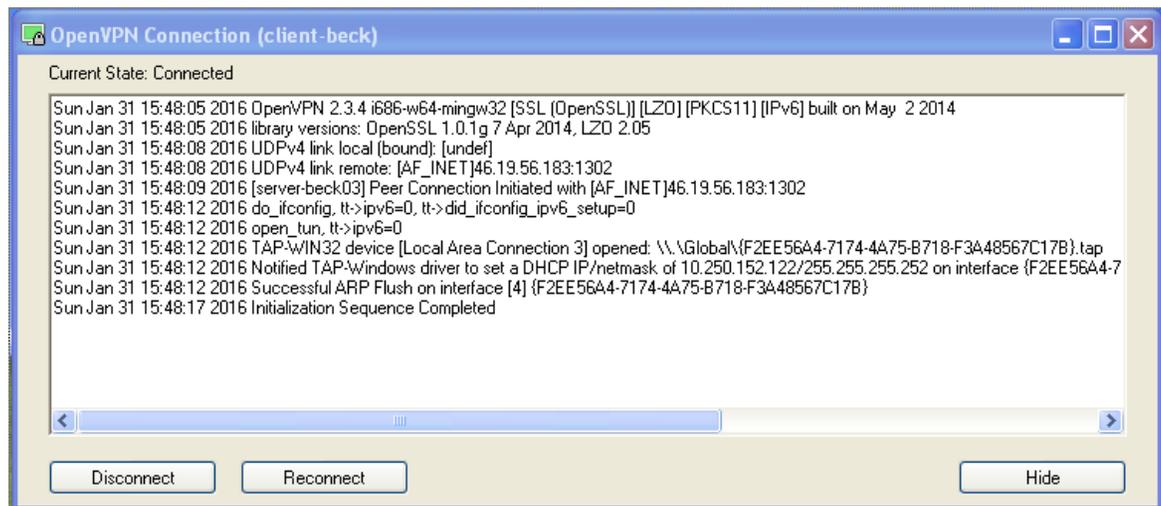
The VPN access can be controlled by a RealiteQ-UI (User Interface). The user can manually active / de-active the ICex VPN connection.

✓ PC installation and setting:

1. Download OpenVPN GUI at: openvpn.net.
2. Install OpenVPN. The installation adds TAP connection.
3. Ask RealiteQ for certificate, key and setting files: ca.crt, cert.crt, cer.key and client.ovpn. Copy files to C:\Program Files\OpenVPN\config.
4. Run OpenVPN, gray icon appears on window toolbars and after successful connection the icon change to green



Right click on the OpenVPN icon and select show status to verify the connection.



5. Do not forget to close the connection at the end of the use.

✓ **OpenVPN - Setting:**

Setting	
Name	Value
General	
Timeout (min)	10

General

Timeout (min): Timeout to OpenVPN operation.

✓ **OpenVPN - Monitor & Control (from local web UI):**

Monitor & Control	
Name	Value
OpenVPN control	
Launch & Start	<input type="button" value="Launch"/>
Stop & Remove	<input type="button" value="Remove"/>
OpenVPN status	
Run	On
Local OpenVPN IP	10.250.152.150

OpenVPN control

Launch & start: Start OpenVPN in iCex and connect the iCex to the tunnel server.

Stop & Remove: Disconnect iCex from tunnel server, stop and remove OpenVPN .exe program.

OpenVPN status

Run: OpenVPN program run.

Local VPN IP: iCex IP in OpenVPN network.

✓ **OpenVPN - Monitor & Control (From RealiteQ-UI):**



RealiteQ-UI allows to remotely controlling the iCex OpenVPN connection.

3.2.2 NAT

The iCex NAT (Network Address Translation) server is a gateway to connect a PC in the global network to the PLC's connected to the iCex local network. The NAT server forwards packets sent from the PC in the global network to the relevant PLC's in the local network and vice versa.

In order for a packet arriving from the global network to be uniquely assigned to the destination PLC's in the local network, a port address translation is required in addition to the conversion of the IP addresses. A local port of the NAT server is assigned to a combination of local IP addresses and port numbers. In this way, it is possible to specify uniquely the destination to which a packet is to be forwarded.

Remark: NAT can only forward communication from the OpenVPN connection.

✓ NAT - Setting:

Setting			
General			
Timeout (min)	10		
Map			
Name	Map 1	Map 2	Map 3
Protocol	TCP	UDP	TCP
Local port	502	28784	102
Remote IP address	192.168.60.102	192.168.60.102	192.168.60.30
Remote port	502	28784	102

General

Timeout (min): Timeout to NAT operation. Timeout counts start in NAT "no busy" status.

Map

Protocol: This entry specifies the protocol for which the mapping is valid. Possible values are "TCP" and "UDP".

Local port: This defines the port at which the packets come from the global network.

Remote IP address and Remote port: These two entries define the destination of the corresponding mapping.

Map 1: All TCP packets arriving from the global network in port 502 assigned uniquely to a client with IP 192.168.60.102 | port 502.

Remarks: Local port and remote port can be different. Each Local port of the three maps should be unique.

✓ **NAT - Monitor & Control (from local web UI):**

Monitor & Control		status
Name	Value	
NAT control		
Enable	<input type="button" value="Enable"/>	
Disable	<input type="button" value="Disable"/>	
NAT status		
Run	On	
Active	Off	
Busy	Off	

NAT control

NAT program should start in idle mode from the autoexec batch.

Enable: Enable NAT. Start routing packets from global network to local network and vice versa. iCex stops the normal communication with the PLC's via the network connection.

Disable: Disable NAT, stop routing and switch to idle mode. The NAT program switches automatically to idle mode after a timeout of inactivity. iCex returns to communicate normally with the PLC's.

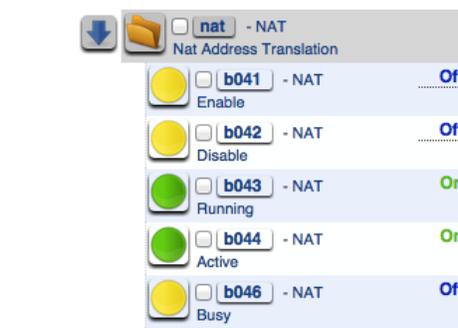
NAT status

Run: NAT program run.

Active: NAT program in routing mode.

Busy: NAT program busy routing messages from the global network to local network and vice versa.

✓ **NAT - Monitor & Control (From RealiteQ-UI):**



RealiteQ-UI allows to remotely controlling the iCex NAT transfer.

3.2.3 Com-Server

Com-Server or terminal server is a serial port redirector that is compliant with the RFC 2217. This program lets you share a serial port through the network or to remotely connect to PLC's connected to iCex via the serial port.

Remark: Com-Server can only forward communication from the OpenVPN connection.

✓ **PC installation and setting:**

Serial to Ethernet connector is a program that will easily let you share serial port device over the network.

1. Download, install and run Serial to Ethernet connector for example from eltima.com

2. Create new serial port.

3. Set:

Virtual com number.

Remote IP address to iCex local OpenVpn IP address.

Remote port to 28.

Protocol to Telnet.

✓ **Com-Server - Setting:**

Setting	
Name	Value
General	
Timeout (min)	5
Listen port	28
Cisco compatible	<input checked="" type="checkbox"/>
HwVspV3 compatible	<input checked="" type="checkbox"/>

General

Timeout (min): Timeout to Com-Server operation. Timeout counts start in Com-Server "no busy" status.

Listen port: network port. 28 is standard for terminal sever.

Cisco compatible: Compatible with Cisco Serial to Ethernet driver software.

HW VSP V3 compatible: Compatible with HW VSP Serial to Ethernet driver software.

✓ **Com-Server - Monitor & Control (from local web UI):**

Monitor & Control		status
Name	Value	
ComServer control		
Start	Enable	
Stop & exit	Disable	
Comserver status		
Run	On	
Active	Off	
Connected	Off	
Busy	Off	

Com-Server control

Com-Server program runs in idle mode from auto exec.

Enable: Enable Com-Server. Start transfer packets from global network to local serial port and vice versa. Remark: iCex stops the normal communication via the serial port.

Disable: Disable Com-Server, stop transfer packets and switches to idle mode. The Com-Server program switches automatically to idle mode after a timeout of inactivity. iCex returns to communicate normally with the PLC's.

Com-Server status

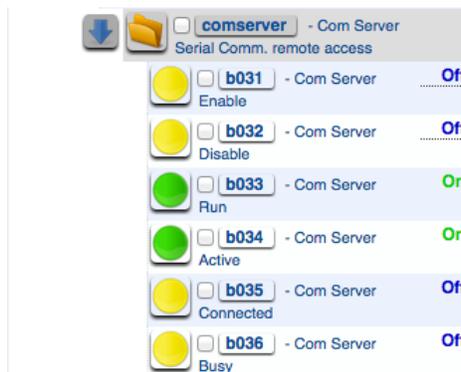
Run: Com-Server program run.

Active: Com-Server program in transfer mode.

Connected: PC Serial to Ethernet connector connects to Com-Server.

Busy: Com-Server program is busy transferring messages from the global network to local serial port and vice versa.

✓ **Com-Server - Monitor & Control (from local RealiteQ-UI):**



RealiteQ-UI allows to remotely controlling the iCex Com-Server transfer.

3.3 iCex maintenances.

3.3.1 Security.

List of different services that can work on the iCex, these services are needed only for maintaining and tracing the iCex to allow easy startup and not needed for normal operation.

- WEB server - Maintains the iCex configuration.
- TELNET server - Allows details trace and control of the iCex operation.
- FTP server - Allows uploading and downloading files to and from the iCex.
- UDP find service - UDP configuration server.
- SSH Server – Allows details trace and control of the iCex operation (like Telnet). Provide strong authentication and secure cryptographic connection.

Name	Value
Web server	
Enable	<input checked="" type="checkbox"/>
Main username	<input type="text" value="cex"/>
Main password	<input type="text" value="cex"/>
Upload username	<input type="text" value="upload"/>
Upload password	<input type="text" value="upload"/>
FTP server	
Enable	<input checked="" type="checkbox"/>
Username	<input type="text" value="ftp"/>
Password	<input type="text" value="ftp"/>
Telnet server	
Enable	<input checked="" type="checkbox"/>
Username	<input type="text" value="tel"/>
Password	<input type="text" value="tel"/>
UDP server	
Mask	<input type="text" value="0x13"/>
SSH server	
Enable	<input checked="" type="checkbox"/>
Secure communication - SSL	
Use SSL	<input type="checkbox"/>
Server URL	<input type="text" value="*.realiteq.net"/>

Passwords provide the first line of defense against unauthorized access to iCex. The stronger your password, the more protected your iCex will be from hackers and malicious software. You should make sure you have strong passwords for all utilities on your iCex. Remark: All usernames and passwords are not case sensitive.

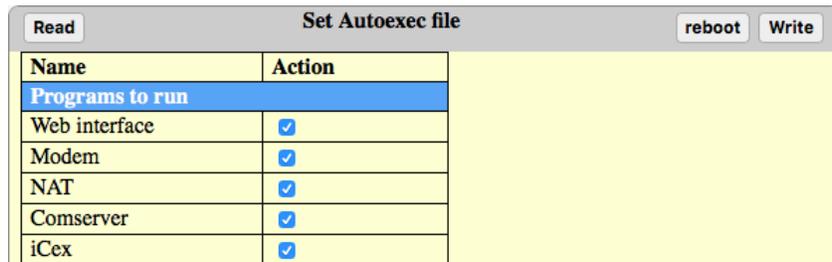
To avoid security leaks: it is better to disable unnecessary services and to leave only the SSH Server and to enable SSL communication between the iCex and the RealiteQ-COMP.

For more information about how to robust the iCex secure see appendix 3.

3.3.2 Autoexec.

iCex system includes 6 programs:

- WEB- Maintains the iCex configuration.
- Modem – Control the iCex cellular communications.
- iCex – Maintains the iCex communication to the PLC's and to the RealiteQ-COMP
- OpenVPN – Maintains the remote secure connection to the iCex. Not started by the iCex autoexec, runs on user demand.
- NAT – Routing communication from the global network to the local network to allow remote maintenance to connected PLC's. Start to run in idle mode. Activate/deactivate by user demand.
- Com-Server - Routing communication from the global network to local serial port to allow remote maintenance to connected PLC's. Start to run in idle mode. Activate/deactivate by on user demand.



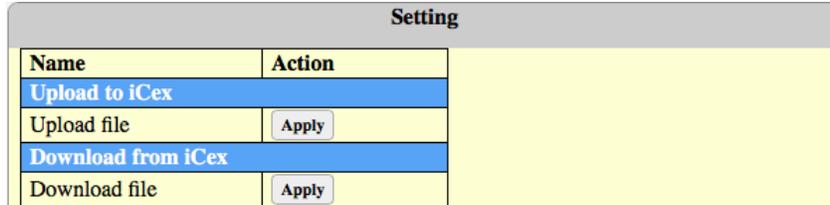
The screenshot shows a window titled "Set Autoexec file" with a "Read" button on the left and "reboot" and "Write" buttons on the right. The window contains a table with two columns: "Name" and "Action". The table lists six programs, each with a checked checkbox in the "Action" column.

Name	Action
Programs to run	
Web interface	<input checked="" type="checkbox"/>
Modem	<input checked="" type="checkbox"/>
NAT	<input checked="" type="checkbox"/>
Comserver	<input checked="" type="checkbox"/>
iCex	<input checked="" type="checkbox"/>

iCex should be re-booting in order that the new settings will take place.

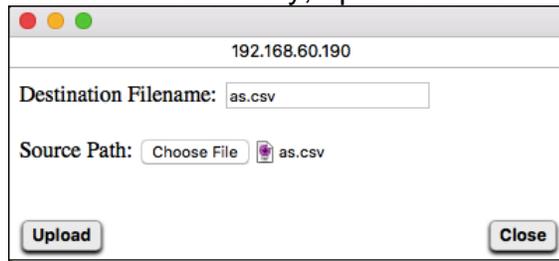
3.3.3 Files.

Allow to transfer file from and to ICex.



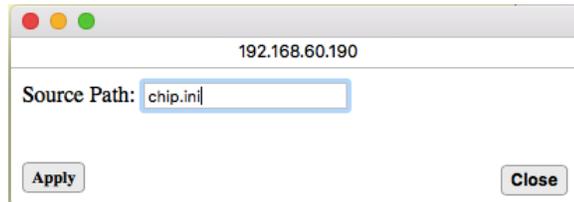
✓ Upload to iCex

Upload dialog: Open dialog box to upload files to iCex. Select the source file, if you want to upload the file to a different directory, update destination file.

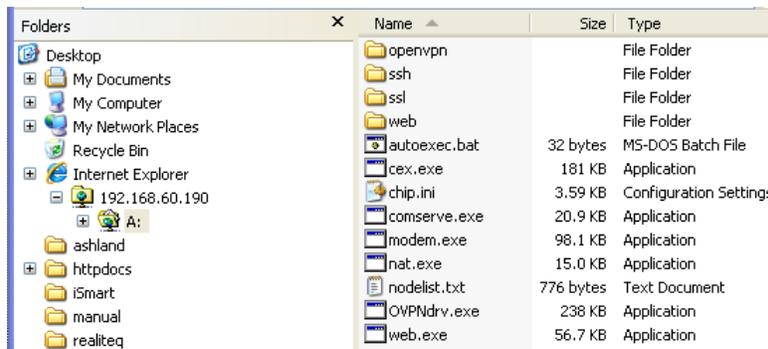


✓ Download from iCex

Download dialog: Open dialog box to download files from iCex.



Browse iCex with window explorer by typing ftp://iCex IP like ftp://192.168.16.201



iCex files system includes main directory "A:/" and several subdirectories. Files store in main directory:

- Six exe programs - Cex, Comserve, Modem, NAT,.OVPNdrv and web
- Autoexec.bat - iCex start up auto execute batch file.
- Chip.ini - iCex setting files.
- Nodelist.txt - Create and handle by the cex.exe program.

Subdirectories:

- OpenVPN - Certificate, key and setting OpenVPN files.
- SSH – Certificate and keys SSH files.
- SSL – Certificate and keys SSL files.
- Web - Web UI interface files.

3.4 Monitor.

3.4.1 Trace.

The iCex generates 3 type of tracing that shows all activities and message errors:

1. iCex - trace iCex communication to RealiteQ-COMP.

iCex	Driver	Modem
Message		
2015/08/11	10:18:57	iCex ver. 2.0.0.5
2015/08/11	10:19:17	Read and update time form server
2015/08/11	10:19:20	Login
2015/08/11	10:19:20	Read and update time form server
2015/08/11	10:19:21	Get valid sKey
2015/08/11	10:19:21	Open event channel
2015/08/11	10:19:21	Send update message to server
2015/08/11	10:19:24	Send update message to server
2015/08/11	10:19:35	Send update message to server

2. Driver – trace iCex communication to the PLC's.

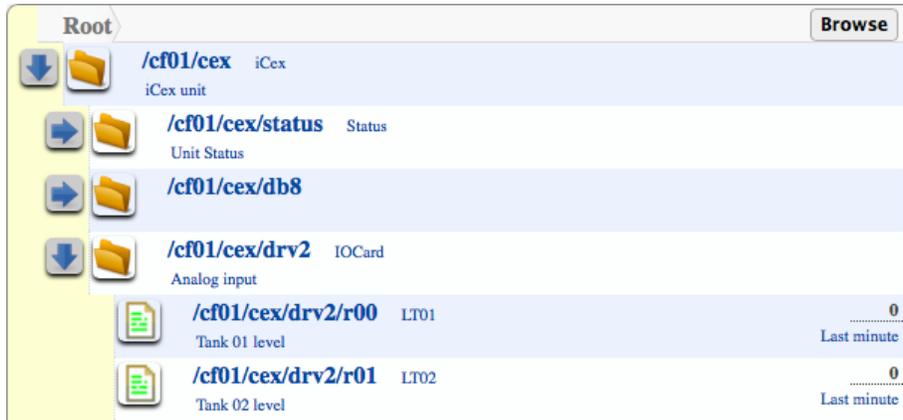
iCex	Driver	Modem
Message		
2015/08/11	10:27:09	Driver 1 - Station 1 Read block start db8/f10, size 29
2015/08/11	10:27:09	Driver 1 - Station 1 Read block start db8/f42, size 17
2015/08/11	10:28:00	Driver 1 - Update time start address r1501 = 3, 10, 28, 1
2015/08/11	10:28:09	Driver 1 - Station 1 Read block start db8/r0, size 7
2015/08/11	10:28:09	Driver 1 - Station 1 Read block start db8/f10, size 29
2015/08/11	10:28:09	Driver 1 - Station 1 Read block start db8/f42, size 17
2015/08/11	10:29:00	Driver 1 - Update time start address r1501 = 3, 10, 29, 1

3. Modem – Shows modem connect ion status.

iCex	Modem	Drivers	Serial Com	Counters	OpenVPN	NAT	Com s
Message							
2017/01/23	10:05:56	Set primary					
2017/01/23	10:05:56	Modem Ver 1.0.0.5					
2017/01/23	10:05:56	Power on					
2017/01/23	10:06:21	Init GSM successfully					
2017/01/23	10:06:36	Operator: IL ORANGE, No: 42501 Status: Current					
2017/01/23	10:06:36	Operator: , No: 42506 Status: Available					
2017/01/23	10:06:36	Operator: JAWWAL-PALESTINE, No: 42505 Status: Available					
2017/01/23	10:06:36	Operator: IL Cellcom, No: 42502 Status: Forbidden					
2017/01/23	10:06:36	Wait to network registration					
2017/01/23	10:06:37	Registered to home network					
2017/01/23	10:06:37	GPRS Network Registration successfully					
2017/01/23	10:06:38	IMEI= 352284030187722					
2017/01/23	10:06:38	SIM ID= 89972011212060147214					
2017/01/23	10:06:38	RSSI (signal)= 30					
2017/01/23	10:06:38	Link to Internet					
2017/01/23	10:06:43	Link establish local IP= 10.165.120.107					
-							
-							

3.4.2 Tree.

Allows local monitoring and control of iCex items list. After every modification to the items list, click Browse button to update the tree structure and documentation



Appendixes

1. Address space

The iCex supports a wide variety of data representations for PLC variables. The general address format recognized by the iCex is: <type><memory offset>. Memory offsets are in the range 0 to 65565. For individual bits the format changes to R<memory offset>.<bit offset>, where <bit offset> is a number between 1 and 16. for example R23.5, register 23 bit 5.

The following address types are support in ModBus RTU and TCP drivers:

I	Inputs (ModBus opcode 02)
O,B	Outputs and internal flags (ModBus opcodes 01/05)
R	16-bits registers (ModBus opcodes 03/06)
D	32-bits registers (ModBus opcodes 03/0x10)
F	32-bits floating point registers (ModBus opcodes 03/0x10)
A	16-bits analog input registers (ModBus opcode 04)
L	32-bits analog input registers (ModBus opcode 04)
N	32-bits floating analog input registers (ModBus opcode 04)

The following address types are support in General Electric GE SNPX driver:

I	Inputs
O	Outputs
B	Internal flags
R	16-bits registers
D	32-bits registers
F	32-bits floating point registers

The following address types are support in Siemens driver:

I	Inputs in byte format, example /bi10.1
O	Outputs in byte format, example /bi12.5
B	Internal flags (M) in byte format, example /bb2.1
R	16-bits registers (DB), example /db10/r1

D	32-bits registers (DB), example /db12/d20
F	32-bits floating point registers (DB), example /db20/f0

The iCex recognizes subgroups formatted as db<db id>. For example, db2/r102 refers to r102 in db2. DB range from 1 to 255.

The following address types are supported in Allen Bradley AB DF1 driver.

Address format: Add type, file number 1 – 64 and offset 0 - 999. Example for PLC address N7:123 enter R70123.

I	Inputs file
O	Outputs file
B	Bits files, Example for PLC B3:15 enter B30015.
R	Integer files "N" for PLC address N7:123 enter R70123.
F	32-bits floating point registers. "F" for F8:321 enter F80321.

The following address types are supported in I\O driver:

I	Inputs 0 – 7
O	Outputs 0 – 7
B	Internal flags
A	Analog inputs 16-bits registers
D	32-bits register. Counters for more details see in counter section.
F	32-bits floating point registers. Flows for more details see in counter section.

The following address types are supported in status driver:

B	Internal flags
R	16-bits registers
S	String

Status items:

B1	PLC's communication status
B2	Server communication status

B11	Start OpenVPN
B12	Stop OpenVPN
B13	OpenVPN run
B22	Reset nodes list
B23	Reboot
B31	Enable Com-Server
B32	Disable Com-Server
B33	Com-Server program run
B34	Com-Server active, connect and control the iCex com port.
B35	Com-Server connected to the remote PC com driver
B36	Com-Server busy with the remote PC com driver
B41	Enable NAT
B42	Disable NAT
B43	NAT program run
B44	NAT active.
B45	NAT connected to the remote PC software
B46	NAT busy with the remote PC software.
R1	Version no. , read only.
R2	Modem signal RSSI, read only. Update every hour
R65	Total send byte, read only.
R66	Total receive bytes, read only.
S2	Start time, read only.
S3	SIM ID, read only.
S4	OpenVPN Remote IP Address (server), read only.
S5	OpenVPN Local IP address (iCex), read only.
S7	OpenVPN netmask address, read only.

The following prefixes can added before the type:

U	Unsigned value (by default integer values are signed)
X	Value is stored in BCD format

B	Value is byte
---	---------------

Examples:

1. R1000 - 16-bit signed integer at offset 1000.
2. XR1000 - 16-bit BCD integer at offset 1000.

Drivers

If multiple drivers are configured, they can access by creating groups for each driver. The iCex recognizes subgroups formatted as drv<station id>. For example, drv2/r101 refers to r101 in a PLC communicate with driver 2.

Stations

If multiple PLC's are connected to the same driver, using network or RS-485, they can access by creating groups for each station. The iCex recognizes subgroups formatted as st<station id>. For example, st4/r101 refers to a PLC with station id 4 or drv2/st3/101 refer to PLC with station ID communicate with driver 2.

Remark: address path without drv prefix refer to driver 1 and address path without st prefix refer to station 1.

2. Filter

The iCex supports a variety of dead-band types in order to provide a rich set of filters for unstable measurements:

Type	Example	Behavior
None	(empty)	Value is always transmitted to the server.
Never	never	Value is transmitted only when forced by status/b12
Value	2.5	Value is transmitted if the change is greater than the specified value.
Percentage	%3	Value is transmitted if the change is greater than the specified percentage.
Greater than	>10	Value is transmitted if it is greater than the specified value.
Greater than or equal	>=10	Value is transmitted if it is greater than or equal to the specified value.
Less than	<10	Value is transmitted if it is less than the specified value.
Less or than equal	<=10	Value is transmitted if it is less than or equal to the specified value.
In range	8<>12	Value is transmitted if it is within the specified value range.
Out of range	8><12	Value is transmitted if it is outside of the specified value range.
Equal	=8.5	Value is transmitted if it is equal to the specified value.
Out of range	<>8.6	Value is transmitted if it is not equal to the specified value.
Data log	Datalog	Send each sample without any filter with the iCex local time. In the case of communication loss with the RealiteQ-COMP. The iCex logs the samples and sends them when the communication re-establish. The sample time is normalizing.

3. Chip.ini

[Device]

Name=icex - Unit name.

;PFI_ENABLE=1 - for R10 iCex module working with counters remove the ";" to allow power fail automatic counters values.

[Reality]

path= /nc - iCex group name.

URL=test.realiteq.net - Project URL.

Password=pw - iCex password.

AccessTokenActive=0 - Use Access-token 0/1.

AccessToken=1888a3a9314a45be9b72cded60f24f6d - Access-token.

[General]

Hardware=4 - hardware type 1 – 4.

analogTypeMask=0 - Analog type.

Tracing=1 –Trace iCex activity 0/1.

ComTracing=0 – Trace drivers messages 0/1

UTCOffset=-7200 - For internal use.

TimeZone=Asia/Jerusalem - Time zone.

[IP]

DHCP=1 – Use DHCP. 0/1

DHCP_TRIALS=0 – for internal use, do not change.

TCPIPMEM=512 – for internal use, do not change.

ADDRESS=192.168.60.87 – IP address

NETMASK=255.255.0.0 – Netmask .address

GATEWAY=192.168.60.1 – Gateway address.

DNS=192.1.1.10 – DNS address.

[GM01]

Active=0 - Use Modem 0/1

Tracing=1 – Trace modem 0/1

Type=4 - Modem Types 1-4
APN=internet – Define primary APN name.
Roaming=0 – Allow roaming 0/1
SetMode=0 – Set network operator mode.
ProviderNo=42501 – The preferred operator numeric name for roaming.
Dual=0 – Working with dual modem 0/1
SecAPN=internet – Define secondary APN name in dual modem mode.
APN=internet - APN
PPPAUTH=0 - Authentication type.
PPPUSEr= Username - Authentication username
PPPPASSWORD= password - Authentication password
PUK=1234 - PUK
PIN= 5678 - PIN
PPPDIAL=ATD*99***1# - For internal use, do not change
PPPGPRSCONNECT=AT+CGDCONT=1,"IP","internet" - For internal use, do not change

[PLCDriver_1] - For driver 1, there are additional 2 sections for drive 2 and 3
Active=1 - Active driver
Driver=2 - Driver type 1- 6
PreventWriting=0 - Prevent writing 0/1
Tracing=0 - Trace driver
com=0 - Serial com.no 0,1
MultiTCP=1 - Multi PLC 0/1
CloseSocket=1 - Close socket 0/1
TCPPort=502 – TCP port
IPSt_1=192.168.60.101 - PLC IP address (set with web interface)
IPSt_2=192.168.60.102 - PLC station 2 IP address set manually
IPSt_3=192.168.60.103 - PLC station 3 IP address set manually
Timeout=2000 - Timeout
SleepTime=0 – Sleep mode
SwapByte=0 - Swap byte 0/1
SwapWord=0 - Swap word 0/1

UpdateClock=1 - Update clock 0/1
UpdateClockStartAddress=r1501 - Start address
UpdateDate=0 - Update date 0/1
UpdateDateStartAddress=r1505 - Start address
BlockWrite=0 - Block write 0/1
BlockWriteAddress=b10 - Address
rack= 0 - Manual enter for Siemens PLC's
slot= 0 – Manual enter for Siemens PLC's

[com0] - For com0

RSType=1 - RS type 1 - 2

Baud=19200 - Baud

Parity=0 - Parity 0 - 2

Databits=8 - Data bits 7 - 8

Stopbit=1 - Stop bit 1 - 2

FlowControl=0 - Control 0 - 2

[counter]

Active=0 - Active counters 0/1

count0_active=0 - counter 1 active

count0_type=0 – 0 for pulses, 1 for working time

count0_flowInterval=60 - Counter 1 flow base-time

count0_resetType1=0 - Counter 1 reset type 1

count0_resetType2=1 - Counter 1 reset type 2

count0_resetType3=2 - Counter 1 reset type 3

count0_resetHour=0 - Counter 1 reset hour

count0_resetDay=7 - Counter 1 reset day

Counter1 to counter7

4. Security

Notes about how to robust the iCex protection against unauthorized access.

List of different services that can work on the iCex that could allow unauthorized access, these services are needed only for maintaining and tracing the iCex to allow easy startup and not needed for normal operation.

1. **WEB server** - Maintains the iCex configuration.
2. **TELNET server** - Allows detail trace and control of the iCex operation.
3. **FTP server** - Allows uploading and downloading files to and from the iCex.
4. **TFTF server** - Allow uploading and downloading files to and from the iCex.
5. **PPP Server** - Running TCP/IP server over a cellular modem link.
6. **UDP find service** - UDP configuration server.

Remark: All iCex configurations kept in the chip.ini file.

1. **WEB server** - Maintains the iCex configuration.

Web section in chip.ini is [WEB].

By default Web Server set to run (Active=1). If activated, the Web server will run automatically on iCex startup.

Username=cex and password=cex for Web server login and username=upload, password=upload for Web server upload files to iCex. Both user name and password are case sensitive. Maximum user name size: 19 characters. Important notice: To avoid security leaks you must redefine both usernames and passwords.

Recommendation: Disable Web server after finish iCex setup or at least set "strong" username and password.

2. **TELNET server** - Allows detail trace and controlling of the iCex operation. Telnet server listens on port 23.

Telnet section in chip.ini is [TELNET].

By default Telnet Server set to run (Active=1). If activated, the Telnet server will run automatically on iCex startup.

To improve the protection of iCex against unauthorized access via Telnet server, the following definitions already exist in the chip.ini:

LOGINDELAY=1 – The active delay between login retries. The delay time starts with 0.4 seconds. After each following failed login, the delay time will be doubled until it reaches 20 seconds. After successful login, the delay time will be set back to 0.4 seconds. Remark: Telnet does not tell if the input of the username or the password input was wrong.

LOGINRETRIES=3 - Defines the number of login retries until Telnet session will be

closed.

Username0=tel and password0=tel for Telnet server login. Both user name and password are case sensitive. Maximum user name size: 19 characters. Important notice: To avoid security leaks you must redefine both username and password. Change also username1 and password1 in chip.ini.

Recommendation: Disable Telnet server after finish iCex setup or at least set "strong" username and password.

- 3. FTP server** - Allow upload download files and program to and from the iCex. FTP server listens in port 21.

FTP section in chip.ini is [FTP].

By default FTP Server set to run (Active=1). If activated, the FTP server will run automatically on iCex startup.

To improve the protection of iCex against unauthorized access via FTP server, the following definitions already exist in the chip.ini:

LOGINDELAY=0/1 - Delay between retries. For more details, see the above paragraph

Username0=ftp and password0=ftp for Telnet server login. Both user name and password are case sensitive. Maximum user name size: 19 characters. Important notice: To avoid security leaks you must redefine both username and password. Change also username1 and password1 in chip.ini.

Recommendation: Disable FTP server after finish iCex setup or at least set "strong" username and password.

- 4. TFTP server** - Allow upload download files and program to and from the iCex.

TFTP section in chip.ini is [TFTP].

By default TFTP Server disable (Active=0). Leave the TFTP server disable.

For download SFTP client look at: [FileZilla project web site](#)

- 5. PPP server** - PPP (Point to Point Protocol) is a mechanism for creating and running TCP/IP over a cellular modem link. The PPP server allows other computers to dial into the iCex. PPP server and communicate via the TCP/IP link using FTP, Telnet, Web, etc. in the same manner as with an Ethernet TCP/IP link. Remark: the iCex acts as a PPP client.

PPP server section in chip.ini is [PPPSERVER].

By default PPP Server - disable (Active=0). Leave the PPP server - disable.

6. **UDP find service** – UDP configuration server. The server is able to execute and reply incoming UDP protocol requests from external UDP clients. The UDP server allows the clients to get and set the iCex IP's.

UDP server section in chip.ini is [UDPCFG].

By default UDP Server set to run (Active=1). If activated, the UDP server will run automatically on iCex startup.

UDP default setting:

LEVEL=mask. Defines the supported functions of the UDP configuration server. LEVEL is a bit mask. Each bit represents one function. Setting the bit to 1 enables the function, setting it to 0 disables the function.

The bit assignment is as follows:

Bit 0: Detection of the iCex on the network.

Bit 1: IP configuration.

Bit 2: Keep "0".

Bit 3: Keep "0".

Bit 4: RTOS update.

Bits 5-15: Reserved for future use.

If the configuration level is set to 0x00, the configuration server task will not be started at all. The default value is 0x13

Recommendation: For better security, set the mask to 0x01, only keep the detection of iCex on the network by the GetIcexIP tool.

Rules to create "Strong" password, to keep your iCex safe:

- Use a unique password for each of your account.
- Use a mix of letters, number and symbols in your password, Password length should be longer than 8 figures
- Don't use personal information or common words in your password
- Keep your passwords secure.

SSH Server – Secure Shell connection, the goal of SSH is to replace the Telnet Server, which did not provide strong authentication or guarantee confidentiality. The SSH server allows secure detail tracing and control of the iCex operation.

SSH server Features:

- Support SSH-2 protocol
- OpenSSH compatible key format

- Public key user authentication
- Cryptographic algorithms: RSA

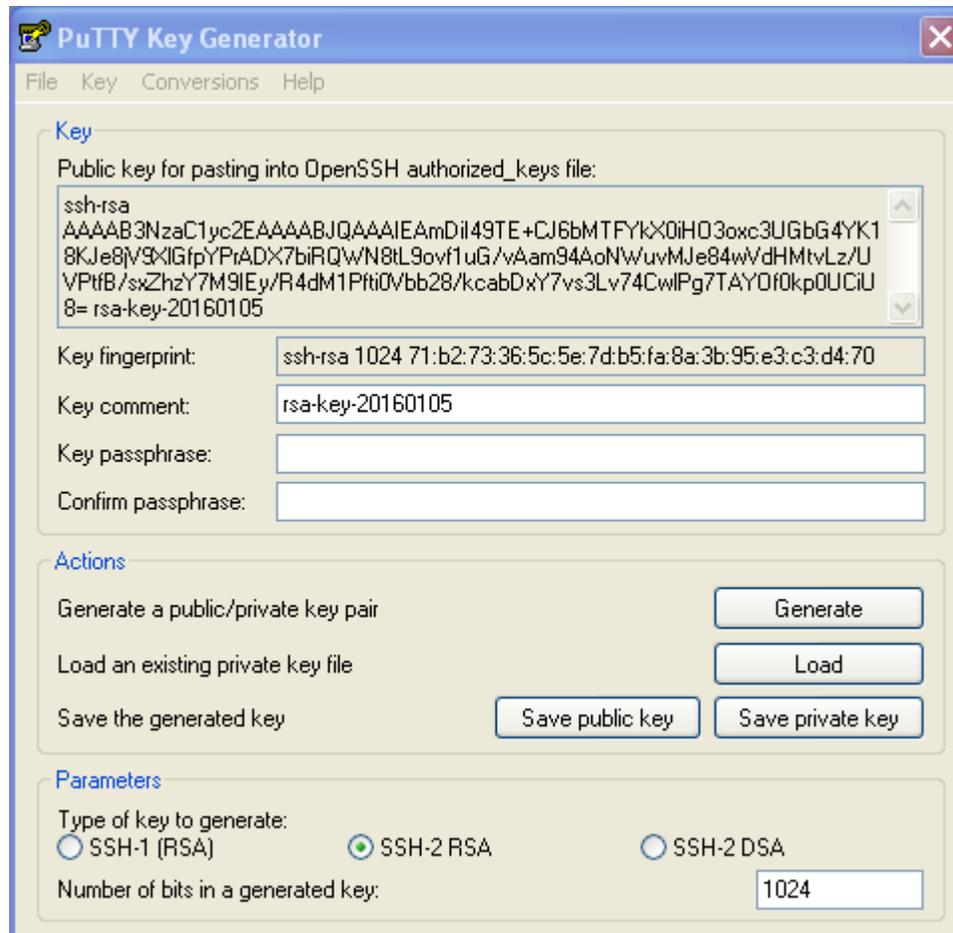
By default, the SSH server is enabled with a preload RSA key and user authentication key. Leave the SSH running all the time, if all the other software's will be disabled the SSH is the only means remain that will be used to solve problems in the iCex.

For monitoring the iCex via the SSH server we recommend to use the well known SSH client program PuTTY. PuTTY is an SSH telnet client for Windows platform. PuTTY is open source software and can free download at <http://www.putty.org>.

For better security, we recommend replacing the preload key user authentication. For this purpose, we recommend using the PuTTYgen a RSA key generation utility. . PuTTYgen is open source software and can free download.

Step by step how to create the server key for server authentication:

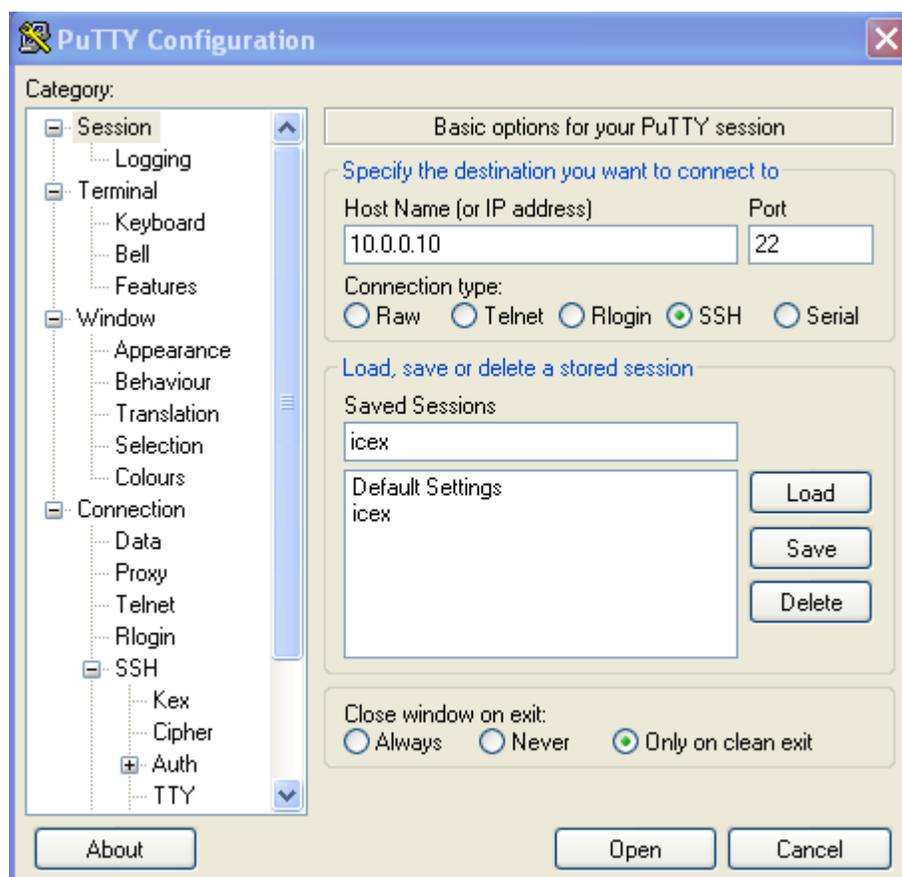
- Open 'puttygen.exe'.
- Select SSH-2 RSA and size = 1024 from the parameters field.
- Click the generate button.
- Do not enter a passphrase. Server keys with passphrase are not supported.
- Export the key in the OpenSSH format with filename "RSAkeyfile" without any extension.
- Transfer this key to the iCex to a:/ssh directory, use upload option in the Web configuration.



Step by step how to create key for user public key authentication:

- Open 'puttygen.exe' again.
- Select SSH-2 RSA and size = 1024 from the parameters field.
- Click the generate button.
- Save the private key.
- Copy the text from the dialog 'Public key for pasting into OpenSSH authorized_keys file.
- Paste the text into a new text file. Use Notepad to create, edit and save this file.
- Make sure that there are no line breaks.
- If you like, you can add other keys to this file. Each key must be in his own line.
- Save the file with filename "userkeyfile" without any extension.
- Transfer this file to the iCex a:/ssh directory.

Start working with PuTTY:



- Set in category connection/ssh/Auth the private key file for authentication
- Set in category session the iCex IP and port = 22. You can then save these setting for future uses.
- To start the SSH session after setting or setting load click the Open button.

Working with PuTTY terminal:

- The terminal display got three modes:
 1. User - Displaying programs trace messages. and allows program control.
 2. Shell - Displaying iCex Operating System (OS) message and allows iCex OS control.
 3. Both – Displaying user and shell messages and allow control on the iCex programs and OS

Use Ctrl-F to switch between modes.

- To enable temporarily the FTP, Telnet or Web configuration tools type: server arg1, agr2. Where arg1 is the server type: 1 - FTP, 2 - Telnet and 3 - Web and arg2 is the command: 0 - close and 1 - run. For example to run Web server click: server 3 1. After finishing the iCex maintenance, do not forget to close the opened server or to reboot the iCex in order to return to a secure mode.

- Reboot the iCex – type reboot in system mode. The connection will lose and you should reconnect to the iCex.

SSL TCPIP protocol - Protocol used for communication between the iCex and the RealiteQ-COMP. By default, the iCex uses the standard HTTP protocol, for better security, it is recommended to switch to HTTPS safe, secure and encrypted protocol (SSL).

Steps to be taken to improve iCex security and to prevent unauthorized access:

1. Change all predefines username and password.
Passwords provide the first line of defense against unauthorized access to iCex. The stronger your password, the more protected your iCex will be from hackers and malicious software. You should make sure you have strong passwords for all utilities on your iCex.
2. Disable the Telnet, FTP and Web servers and change the UDP server mask setting. By doing this, you block all the available options of unauthorized access to iCex.
3. Leave enable, only the SSH server but change the SSH server user private key. The SSH connection provides a secure channel over an unsecured network to the iCex for setting and troubleshooting.
4. Change the protocol that the iCex communicates to the RealiteQ-COMP to a secure and encrypt SSL TCP/IP protocol.

5. OpenVPN remote configure and monitor

iCex monitor and configure

Preparation during the iCex installation:

1. Install the OpenVPN certificates, keys and setting files.
2. Test the iCex to connect to the OpenVPN server and getting local OpenVPN IP.

Preparation in PC:

1. Install OpenVPN GUI.
2. Install the OpenVPN certificates, keys and setting files.
3. Test the PC to connect to the OpenVPN server and getting local OpenVPN IP.

Preparation in RealiteQ-UI

1. Create OpenVPN monitor and control UI

Monitor and configure:

1. Enter to project RealiteQ-UI.
 - Launch the OpenVPN and wait to iCex to connect to the OpenVPN server and get local IP.
2. Run PC OpenVPN GUI and connect to the OpenVPN server.
3. Run web browser, enter the local iCex OpenVPN IP and sign in to the iCex.
4. Do not forget after finishing to disconnect the PC and the iCex from the OpenVPN server

PLC programming – serial connection using OpenVPN and Com-Server programs.

Preparation during the installation:

1. Install the OpenVPN certificates, keys and setting files.
2. Test the iCex to connect to the OpenVPN server and getting local OpenVPN IP.
3. Check that Com-Server program enables in the autoexec file.

Preparation in PC:

1. Install OpenVPN GUI.
2. Install the OpenVPN certificates, keys and setting files.
3. Test the PC to connect to the OpenVPN server and getting local OpenVPN IP.
4. Install and set Serial to Ethernet connector.

Preparation in RealiteQ-UI.

1. Create OpenVPN monitor and control UI.
2. Create Com-Server monitor and control UI.

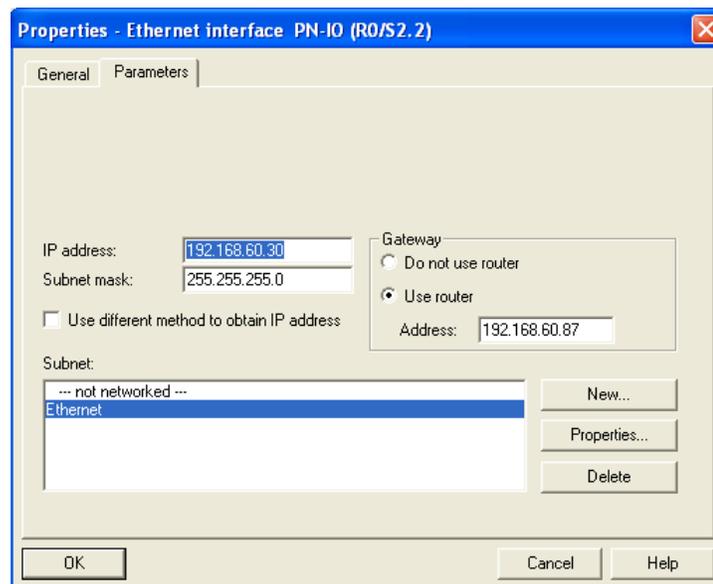
Programming:

1. Enter to project RealiteQ-UI.
 - Launch the OpenVPN and wait to iCex to connect to the OpenVPN server and get local IP.
 - Start Com-Server.
2. Run PC OpenVPN GUI and connect to the OpenVPN server.
3. You are ready to Run Step7 online.
4. Do not forget to disconnect the PC and the iCex from the OpenVPN server after finishing.

Siemens PLC - network connection using OpenVPN and NAT programs.

Preparation during the installation:

- 1 Install the OpenVPN certificates, keys and setting files.
- 2 Test the iCex to connect to the OpenVPN server and getting local OpenVPN IP.
- 3 Open Step 7 and set the PLC configuration:



- IP address - As you set in Drivers tab.
 - Subnet mask - Leave 255.255.255.0
 - Gateway – Select user router and set address to iCex IP address as you monitor in the iCex tab.
4. Download the configuration to the PLC and check the communication.
 5. Check that NAT program enables in the autoexec file.
 6. Set one map to

- Protocol - TCP.
- Local port - 102.
- Remote IP - PLC IP address.
- Remote port - 102.

Preparation in PC:

1. Install OpenVPN GUI.
2. Install the OpenVPN certificates, keys and setting files.
3. Test the PC to connect to the OpenVPN server and getting local OpenVPN IP.
4. Open Step 7 and set the PLC configuration:
 - IP address – iCex local OpenVPN IP.
 - Subnet mask - Leave 255.255.255.0
 - Gateway – Select "Do not use router".
5. Save the configuration.

Preparation in RealiteQ-UI

1. Create OpenVPN monitor and control UI
2. Create NAT monitor and control UI .

Programming :

1. Enter to project RealiteQ-UI.
2. Launch the OpenVPN and wait to iCex to connect to the OpenVPN server and get local IP.
3. Start NAT.
4. Run PC OpenVPN GUI and connect to the OpenVPN server.
5. You are ready to Run Step7 online.
6. Do not forget to disconnect the PC and the iCex from the OpenVPN server after finishing.