



***Ръководство  
на  
потребителя***

*rev. 2.42 (отразява фърмуер v5.94)*

**08.04.2026**

---

## СЪДЪРЖАНИЕ

1. Въведение.....	7
1.1. Основен панел (за стандартен ABS корпус). Възстановяване на фабричните настройки.....	8
1.2. Корпус за DIN шина.....	9
2. Достъп до устройството.....	10
2.1. Достъп през облачната платформа на <a href="http://domo.ipnetcontrol.net">domo.ipnetcontrol.net</a> .....	10
2.2. Достъп чрез Web браузер.....	10
2.3. Достъп чрез HTTP URL команди.....	11
2.4. Достъп чрез SNMP протокол.....	11
2.5. Достъп през MQTT.....	11
2.6. Достъп през ModbusTCP (от v5.56).....	11
3. Управление/конфигуриране на устройството през Web.....	13
3.1. Управление/статус на входно-изходните вериги (меню „Status“).....	13
3.1.1 Управление/статус на входно-изходните вериги чрез URL команди (за интегриране към външно управление през скриптове и др.).....	13
3.2. Мрежови параметри и настройки (меню „IP Settings“).....	14
3.2.1 Секция „IP Configuration“.....	14
„Ethernet Settings“.....	17
„WiFi Settings“.....	17
3.2.2 Секция „SNMPv1 access settings“ и „SNMPv1 traps/remote IO settings,“.....	17
3.2.3 DHCP - динамично зареждане на основните мрежови параметри.....	18
3.2.4 Списък с имена на хостове, които могат да се ползват от различни услуги.....	19
3.2.5 Филтър по IP за сървърните услуги (SNMP, HTTP, ModBUS).....	20
3.3. Входно-изходните вериги. Режими на работа и параметри. (меню “IO Settings“).....	21
3.3.1 Цифрови входове-изходи („Digital I/O Channels“)......	21
3.3.2 Аналогови входове („Analog I/O Channels“)......	23
3.3.3 Други общи настройки за входовете.....	24
3.3.4 Виртуално входно-изходни канали (Virtual IO)......	24
3.4. Macros – последователности от действия на изходните вериги.....	25
3.4.1 „Remote IO/Macros Action“ - подаване на команда за действие към друг NetControl.....	28
3.5. Timers – стартиране на Macros по зададен час:минута, ден от седмицата и месец.....	28
3.5.1 Синхронизиране на часовника на NetControl по SNTP.....	29
3.5.2 Хардуерен часовник с батерия.....	30
3.5.3 Настройка на Timer.....	31
3.6. 8 (24)-канален “PING Monitor”.....	31
3.7. Автоматични задачи (меню „Automation“).....	33
3.7.1 Режим на диференциално измерване.....	36
3.7.2 Фабрична настройка за генериране на събития от алармени входове към външните услуги (MQTT, SmartSpaceCloud).....	38
3.7.3 Стартиране на макроси от цифрови входове.....	38
3.8. Рестартиране, обновяване на софтуера и др. (меню „Misc“).....	39
3.8.1 Потребители за Web достъпа.....	39

3.8.2	Възстановяване на фабрични настройки.....	39
3.8.3	Обновяване на системния софтуер по TFTP.....	39
3.8.4	Обновяване на системния софтуер през domo.ipnetcontrol.net.....	41
3.8.5	Обновяване на системния софтуер през Web.....	41
3.8.6	Запазване и възстановяване на конфигурацията във/от файл.....	41
3.8.7	“Events Log” - архив на последните IO събития.....	41
4.	Достъп през SNMPv1 протокол.....	42
4.1.	Достъп до I/O през SNMP.....	42
4.1.1	SNMP обекти за индивидуален достъп до входно-изходните вериги.....	42
4.1.2	Други (общи) SNMP обекти за достъп до входно-изходните вериги.....	43
4.1.3	Изчитане на температурата (от датчик TDS300) през SNMP.....	44
4.1.4	Изчитане на стойността за относителната влажност (от датчик HDS300) през SNMP.....	44
4.1.5	Вход за измерване на Unet (VIN), +Uin.....	44
4.1.6	Алармен вход.....	44
4.1.7	Вход измерване на DC ток чрез външен шунт (за 4RU1SH2S).....	45
4.1.8	Вход за NTC температурен сензор.....	45
4.1.9	Достъп до старите OID за достъп до I/O портовете.....	45
4.2.	Примерен PERL скрипт за изчисляване на температурата, Unet и алармения вход.....	45
5.	Управление през MQTT протокол.....	46
5.1.	Принцип на работа на MQTT протокола.....	47
5.2.	Настройки за MQTT.....	47
5.3.	Поддържани обекти.....	48
5.3.1	JSON формат на данните, които публикува NetControl.....	49
5.3.2	Формат на данните, подавани към NetControl.....	49
5.3.3	LWT обект.....	50
5.3.4	Други поддържани обекти.....	50
6.	WiFi модул.....	51
6.1.1	Настройки на WiFi в WEB интерфейса.....	51
7.	ПРИЛОЖЕНИЕ I Тип на канала 'type' в MQTT JSON данните; в ioModeXX.0 при SNMP и в ioreg.js масива 'PM' ( в HEX).....	54
8.	ПРИЛОЖЕНИЕ II Списък на кодовете за източник на събитието (“st” в MQTT).....	55
9.	ПРИЛОЖЕНИЕ III Бързо ръководство за работа с SNMP. Списък с наличните в NetControl обекти.....	56

## Легенда:



Текстът съдържа допълнителна и полезна информация, която разяснява специфични ситуации и особености.



Текстът съдържа информация от съществена важност, с която непременно трябва да се запознаете!

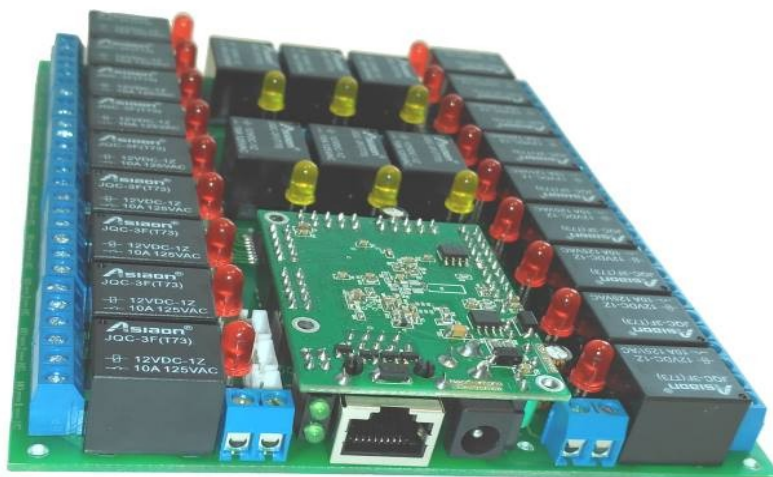
Версия	Дата	Кратко описание на въведените промени
2.42	08.04.2026	Добавено описание за нов MQTT обект „cfg_ts“ в 5.3.4 Добавено описание за „Remote Macros Action“ в 3.4 Разширен резултата от snmwalk в 9
2.41	05.02.2026	Добавено описание за хардуерен RTC. Други поправки в текстовете
2.40	07.10.2025	Променена е секцията за MQTT в частта за обектите и формата на данните
2.39	22.05.2025	Добавено описани на новият режим на работа в PingMonitor (от v5.74)
2.38	13.05.2025	Добавено описание към режима INTERVAL в Automation Корегирано описани на менюто Timers за DST функцията. Добавени информация в таблиците в раздели 7 и 8.
2.37	10.02.2025	Добавена бележка за адреса на устройството в ModBusTCP
2.36	15.01.2025	Промени в секциите за MQTT и Macros, отразяващи нововъведенията от v5.66
2.35	20.04.2024	Променено описание за точността на времевите периоди (3.3.1, 3.4) от v5.62 Променена структурата на документа – информацията за отделните модели е обособена в отделен документ. Добавена е секцията за WiFi модул.
2.32	03.11.2023	Добавени описания на новите стъпки в Macros, Circular Event Log, 'Virtual IO' и филтър на изходящите ON команди (v5.58 и 5.59)
2.31	03.08.2023	Добавено раздел за Modbus TCP от v5.56 Добаен раздел за новата функция „Services access list“ от v5.56
2.30	12.06.2023	Добавено описание на функцията „Events log“ от v5.55
2.29	10.03.2023	Добавено описание на модел 8CT1RS и 7R8A1RS
2.28	12.10.2022	Добавена забелжка към секцията „Remote IO Settings“
2.27	09.06.2022	Мнжество промени в секциите IO Settings и Automation, относно най-новите версии на фърмуера
2.26	09.11.2021	Корекции в 3.8.6 (MA филтър), в 3.2.1 - HTTP Disable, 4.1.1 - добавен ioValueFiltered и нов раздел 3.8.5.
2.25	10.09.2021	Добавен раздел 3.2.4 за списъка с имена хостове (от v5.37). Добавена информация и в секцията за DHCP.
2.24	05.07.2021	Преработени раздели 3.2.1 и 3.8.1 за втория Web потребител „IO User“ (от v5.35)
2.23	18.06.2021	Добавен раздел 3.8.6 за функцията за запазване/възстановяване на конфигурацията от файл (от v5.34)
2.22	29.01.2021	Добавено е описание на два нови модела за монтаж на DIN шина: 4R3OC7A и 4R6I2O Модифицирано е описанието на Macros – добавена е стъпка „Stop Macros“, въведена във фърмуер v5.31.
2.21	28.07.2020	Добавено е описание на функцията „Remote IO Action“ в Macros, въведена във фърмуер v5.22.
2.20	17.06.2020	Добавено е описание на функцията Timers, въведена във фърмуер v5.21.
2.19	22.05.2020	Добавено е описание (3.3.3) за дефиниране на до 26р. потребителски сензори; добавена е информация за стартиране на макрос през MQTT (фърмуер v5.19)
2.18	30.04.2020	Добавено описание на модел 6R8A.
2.17	07.02.2020	Добавено описание на модел 2R4A.
2.16	02.12.2019	Добавено описание на MQTT опцията „Mirror /in to /out“, въведена във версия 5.15
2.15	23.10.2019	Цялостна преработка, свързана с въвеждането на Macros във фърмуер v5.12.
2.14	04.06.2019	Добавено описание на модела 4R4S1A WiFi. Малки корекции по другите текстове.
2.13	18.01.2019	Добавени са разделите 1.5 и 2.1.1 с описание за HTTP URL команди за достъп
2.12	11.06.2018	Добавено описание за MQTT протокол, наличен от v5.7 Добавено е и приложение с описание на кодовете за режимите на работа на входовете/изходите
2.11	05.02.2018	Добавен модел 24R3S2A. Добавена бележка за опцията 'Last' на параметъра 'Default'
2.10	27.11.2017	Корекции в съдържанието във връзка с всички нови модели с увеличен брой входове за външни сензори.
2.9	16.11.2017	Добавени описания за новите функции от фърмуер v3.17: HTTP auth brute-force blocking, ACT LED mode, Ping data size
2.8	03.05.2017	Добавено описание за обекта ioPulseCfg[P].0, въведен с фърмуер 3.16
2.7	07.10.2016	Коригирано е описанието на режимите '>HIGH', '<LOW' и '>HIGH или <LOW' в раздел 2.5; нови модели
2.6	09.06.2016	Добавена е информация за 4RU1SH2S относно грешен знак на 'Cloud scale coefficient' за версии на фърмуера до 3.14 включително.
2.5	11.05.2015	Добавен е раздел за модел 4RU1SH2S
2.4	19.03.2015	Корекции, свързани с фирмуер v3.9: описание към 4PC2R; добавен е ioGauge обекта. Добаен е и раздел за модел 4PH1R
2.3	06.02.2015	Добавено е описание за датчика за влажност HDS300
2.2	07.2014	Въведено описание за новата опция за цифровите изходи „Invert Output“

		Добавено описание за DHCP режим на конфигуриране и опцията 'swap-server' налична от версия 3.3
2.1	07.2014	Въведен нов модел NetControl 8R1T1A
2.0	05.2014	Начална версия на документа за софтуер 3.xx

## 1. Въведение.

*NetControl* е мрежово устройство с 10/100Mbit Ethernet интерфейс, като ядрото му е изградено с популярния PicoIP модул на НЕОМОНТАНА ЕЛЕКТРОНИКС. За да бъдат реализирани оптимално всички особености на серията NetControl е разработена специална, унифицирана за всички модели на устройството, версия на софтуерът му (версия 5.xx).

В зависимост от модела в устройството са вградени различни входно изходни вериги: релейни изходи, входове за датчици за температура, алармени входове за контактни датчици, захранващ модул с широк диапазон на входното напрежение.



Като мрежово устройство NetControl поддържа следните протоколи и функционалност:

- Задължителните мрежови протоколи ARP, IP, ICMP (ping), DHCP
- 802.1q VLAN поддръжка с възможност за работа в пълния 12bit VLAN обхват;
- SNMPv1 протокол за достъп до всички параметри и функции на модула;
- MQTT протокол за автоматизация и IoT решения
- Генериране на SNMP-Trap съобщения при промяна на входове
- ModbusTCP достъп до IO
- Генериране на изходни сигнали при промяна на аналоговите входове
- TCP/IP стек с Web Server за достъп до всички параметри и функции на модула;
- Режим на оторизация на Web достъпа
- Възможност за забрана на достъпа по SNMP за конфигуриране
- Възможност за забрана на достъпа по SNMP/Web по мрежа (IP/Mask)
- Възможност за спиране на Web достъпа;
- TFTP клиент за обновяване на системния софтуер (firmware update)
- Достъп до устройството през облачната платформа на [domo.ipnetcontrol.net](http://domo.ipnetcontrol.net)
- 8(24) канален „ping“ монитор
- SNTP клиент за синхронизиране на вътрешния часовник и изпълнение на таймери
- и много други функции (също и по клиентска поръчка)

С помощта на *NetControl* успешно се решават следните задачи:

- Активен мониторинг и контрол на мрежови сегменти и трасета
- IP охрана на телекомуникационни шкафове и други обекти
- Следене на температура
- Измерване на аналогови величини – напрежения, токове и др. (в зависимост от модела)
- Smart Home / Home Automation
- Отдалечено управление на отоплителни и други системи през Интернет
- и много други ...

### 1.1. Основен панел (за стандартен ABS корпус). Възстановяване на фабричните настройки.

Всички устройства от серията *NetControl* разполагат с 10Mbit Ethernet (10/100 за фърмуер 5.x/PicoIPv2) интерфейс RJ-45 конектор, разположен на основния панел. Установяването на връзка с отсрещното устройство се индицира от светодиода на основния панел „Link”. При входно/изходен трафик светодиодът премигва.

Фабричните IP настройки са:

**IP address:** 192.168.1.100  
**NetMask:** 255.255.255.0  
**Gateway:** 192.168.1.1

Преди да опитате достъп до устройството проверете дали имате нормален мрежов достъп до IP адресът му. За целта може да използвате командата „ping 192.168.1.100”. В случай, че не получавате отговор от устройството вероятно имате проблем с мрежовите настройки на самото устройство, на мрежата, в която го използвате или на компютъра от който се свързвате!

	<b>POWER</b>	Захранващо гнездо 5.5x2.1 12VDC +/-10%. Консумираната мощност зависи от модела!
	<b>ETHERNET</b>	RJ45-F, AutoMDIX 10/100 (10Mbit без AutoMDIX за фърмуер 3.xx) със защита от диференциално пренапрежение (10V)
	<b>RESET</b>	Задържане на бутона при включване на захранването води до възстановяване на фабричните настройки. Светодиода „ACT” потвърждава операцията с премигване 5 пъти. При версия 5.11+: пуснете бутона, щом светодиодът започва да премигва (данните са заредени).
	<b>LINK Led</b>	Свети при установена Ethernet връзка. Премигва при преминаване на трафик.
	<b>ACT Led</b>	По подразбиране свети постоянно при подадено захранване. Софтуерно могат да му се зададат други функции.

Устройството е с габаритни размери 118x72x35mm. На дъното му са предвидени отвори за окачване на стена посредством два винта. Разстоянието между винтовете трябва да е 70mm.



## 1.2. Корпус за DIN шина

Някои модели са оборудвани с корпус за DIN шина с размери 105x65x90mm и изработен от ABS V0 (UL94V-0) материал.

В зависимост от модела се предлагат различни конфигурации от входно-изходни терминали, като на долният ред винаги са достъпни RJ45 и Reset бутона.



## 2. Достъп до устройството

### 2.1. Достъп през облачната платформа на [domo.ipnetcontrol.net](http://domo.ipnetcontrol.net)

„SmartSpace Cloud” представлява сървърна платформа за комуникация с NetControl устройствата. Тя е снабдена с модерен WEB интерфейс и е достъпна 24/7 от компютър, таблет или телефон. Специално за мобилни устройства е налична и „Lite” версия на интерфейса с достъп само до основните функции и изключително компактна визия.

Всяко *NetControl* устройство се свързва автоматично към платформата (ако е разрешен 'SPC mode') и за това не са необходими абсолютно никакви специфични мрежови настройки, освен стандартните настройки за мрежа IP/MASK/GATEWAY и Интернет връзка през зададения GATEWAY.

В нея имате неограничен и постоянен достъп до:

1. Всички налични входно/изходни вериги на NetControl - релейни изходи, измервателни вериги за напрежение, температура и т.н., алармен вход и др.
2. История и отчети за всички данни от и към устройството
3. Отчитане на разход на енергия и изчисляване на стойността по тарифи.
4. Известяване (по е-мейл, опционално по SMS) по зададени от потребителя сценарии
5. Мощен модул за описване на автоматични задачи/сценарии (Macros): тук дефинирате условия (комбинация от време и/или информация от Вашите устройства) при настъпването на които да бъде стартирана зададена от Вас последователност от действия. Самата последователност от действия също може да съдържа условия за състояние на уреди или време, според които действията да поемат по един или друг, определен от Вас път.

Всичко, което Ви е необходимо за да "влезете" в облака е:

1. Устройство *NetControl* (версия 3.00/5.xx и по-нова)
2. Достъп до Интернет за устройството
3. Безплатна регистрация на [domo.ipnetcontrol.net](http://domo.ipnetcontrol.net)

### 2.2. Достъп чрез Web браузер

*NetControl* има вграден HTTP сървър, който отговаря на стандартния 80-и порт TCP.

За да достъпите устройството просто заредете адресът му в браузър (Firefox, IE, Chrome ...), например <http://192.168.1.100>. Ще Ви бъдат поискани потребителско име и парола. Фабричните им стойности са:

**User=admin, Password=admin.**

WEB сървърът, вграден в устройството, разполага с режим на блокиране (HTTP auth brute-force blocking) на множество опити за brute-force атакуване на потребителското име и паролата. При последователни 10 опита с грешни потребител/парола се блокира изцяло достъпа до WEB съдържанието (извежда се грешка '503 Service Unavailable'). Блокирането продължава за период от 5 минути и след това отново се разрешава. IP адресът на последното валидно влизане с потребител и парола не се блокира от описания механизъм. Функцията е включена по подразбиране, а от версия 3.17 тя може да се активира/деактивира в менюто „IP Settings”.

### 2.3. Достъп чрез HTTP URL команди

За интегрирането в автоматизирани системи, скриптове и т.н. често се налага директното подаване на команди към устройството през HTTP. Информация за формата на данните ще намерите в раздел 3.1.1.

### 2.4. Достъп чрез SNMP протокол

В *NetControl* е заложена поддръжка на основните за SNMPv1 команди: *snmpget* и *snmpset*. С тяхна помощ могат да бъдат прочетени или променени стойностите на конфигурационните параметри. Те са описани детайлно в специален MIB файл, който е достъпен за сваляне от сайта [www.ipnetcontrol.net](http://www.ipnetcontrol.net).

За достъп през SNMP се използват две пароли (community string): Read-Only Community String и Read-Write Community String. С първата е възможно само четене на параметрите, а с втората и тяхната промяна.

Фабричните стойности на паролите са: **Read-Only=public, Read-Write=private**

За повече информация и примери за използване на SNMP командите отидете на стр. 55.



*При използване на SNMP за достъп, да се използват snmpget и snmpset само към един OID, а не към група от OID-е. Други команди (snmpwalk например) не се поддържат!*

### 2.5. Достъп през MQTT

От версия 5.7 на системния софтуер се предлага възможност входно-изходните вериги на *NetControl* да са достъпни за контрол през [MQTT](#) – олекотен комуникационен протокол за централизирано управление и мониторинг на мрежови устройства за IoT.

MQTT комуникацията е реализирана, като алтернатива на връзката със SmartSpace Cloud и потребителят трябва да избере кой от двата начина на управление да използва (или да деактивира изцяло външното управление).

По-подробна информация ще намерите в раздел 5.

### 2.6. Достъп през ModbusTCP (от v5.56)

От тази версия е добавен достъп до входно-изходните вериги на *NetControl* през [ModbusTCP](#) протокол. Протоколът е разпространен при PLC системите, в соларните инвертори и други системи за автоматизация.

Вграденият ModbusTCP сървър е на стандартния порт 502 (TCP).

Тъй-като протоколът няма вградени средства за авторизация и сигурност е препоръчително да комбинирате използването му с функцията за ограничаване на достъпа до сървърните услуги по IP адрес (вижте 3.2.5). По подразбиране ModbusTCP е забранен във фабричните настройки на IP филтъра.

В следващата таблица са посочени всички поддържани адреси за достъп, както и типа команди, с които могат да се достъпват.



*Сървърът поддържа само една TCP сесия!*

*Устройството отговаря на фиксиран адрес 0x01 (Unit Identifier/Device ID)!*

Достъп (FuncCode)	Адреси	Описание
ReadCoils (1) WriteSingleCoil (5) WriteMultipleCoils (15)	0 ... 23	За 1bit достъп до цифровите входно-изходни канали (ON=1, OFF=0)
ReadHoldingRegisters (03) ReadInputRegister (04) WriteSingleRegister (06) WriteMultipleRegisters (16)	0 ... 31	16bit достъп до всички входно-изходни вериги. За цифровите ON=0x0001, OFF=0x0000; за аналоговите (сензори) – 10bit стойност (0...1023) на АЦП (може само да се чете).
ReadInputRegister (04)	1000 ... 1063  и  1064 ... 1079 (v5.59)	32bit (BigEndian) достъп (регистрите са по двойки, напр. 1000-1001, 1062-1063 за всеки IO канал) до всички 32бр. входно-изходни вериги. За цифровите стойността е отново 0/1 за OFF/ON. За аналоговите/сензорни – стойността е 32bit float, който съответства на стойността на зададения сензор за входа (напр. за TDS300 стойността ще 23.5 градуса). За входове тип брояч на импулси – стойността на брояча (той е 32bit). За Virtual IO (от v5.59) се използва обхвата 1064...1079 (на практика виртуалните портове се явяват след 32-те броя хардуерни такива).
ReadDeviceIdentification (43)		Отговорът на тази заявка съдържа само данните от Basic категорията: (0)VendorName="Neomontana Electronics" (1)ProductCode="NetControl MOD=xx" (2)MajorMinorRevision="V5.56" / 'xx' е код за конкретния модел NetControl /

Опит за четене на адреси извън посочените ще доведе до връщане на съобщение за грешка „IllegalAddress“. Може да се подават команди за запис към адресите на аналоговите входове – не се третират като грешка, но няма да се изпълни нищо.

Регистрите от обхвата 1000 ...1061 трябва да се изчитат винаги по двойки (или четен общ брой) и стартовият адрес също трябва да е четен! В противен случай ще се върне съобщение за грешка от типа „IllegalAddress“.

32 (24)-те адреса за достъп до входно-изходните вериги съответстват на SNMP „Номер [P]“ на наличните за всеки модел канали (вижте описанието на конкретния модел в раздела му „Връзка между каналите и SNMP обектите за достъп“). Единствената разлика, е че при SNMP първият канал е с номер 1, а при ModbusTCP – 0 (т.е. трябва да се извади 1 от 'Номер [P]' за да се получи адреса в ModbusTCP).

Допустимо е (за унифициране) винаги да се четат всички адреси, като на тези, на които няма реални входове-изходи за даден модел ще се връща нулева стойност.

### 3. Управление/конфигуриране на устройството през Web

#### 3.1. Управление/статус на входно-изходните вериги (меню „Status”)

Началната страница, която се зарежда при успешна авторизация на Web адреса на устройството изглежда така (според модела ще се виждат различен брой входове/изходи). До нея се достига и чрез менюто „Status”.

При избор на името на устройството „My NetControl” се влиза в частта с настройки му (там са разположени изброените по-долу менюта).

В горният край на статус страницата са аналоговите входове (температура, напрежение и т.н.) с техните имена и текуща стойност.

Следват макроси, дефинирани от потребителя и настроени да се виждат на централната страница. От тук те могат да бъдат ръчно стартирани.

Следващата група са цифровите вериги, които могат да са входове или изходи според устройството. Чрез бутоните се променя състоянието им (ако са изходи), както и се вижда текущото им състояние. Под името на канала е описан и избраният в момента режим на работа.

Налични са и бутоните „All On/All OFF”, чрез които могат с един клик да се включат или изключат всички релейни изходи (не важи за макросите).

Можете да зададете време за автоматично презареждане на тази страница ако искате да следите автоматично стойностите на каналите.

The screenshot shows the 'My NetControl' web interface. At the top, it displays '18.1°C Temperature', '0.5VAC Unet', and 'OPEN Alarm'. Below this is a 'Macro 01' section with a 'Start MACRO' button. There are four 'Line' sections (Line 1 to Line 4), each with a 'Switch ON' button and the text 'Manual Output, Initial=Off'. At the bottom, there are 'All OFF' and 'All ON' buttons, and an 'Auto refresh' dropdown menu set to '10s'.

##### 3.1.1 Управление/статус на входно-изходните вериги чрез URL команди (за интегриране към външно управление през скриптове и др.)

Ако е необходимо да подадете команда през URL адрес за включване или изключване на даден изход (например през скрипт) трябва да използвате HTTP GET заявка към следния адрес:

```
http://<NetControl IP address>/iochange.cgi?ref=ioreg.js&PP=VV
```

, където

- PP е номера на канала P на *NetControl* (във формат двуцифрено HEX число с водеща нула). За конкретен модел номерата на каналите може да видите в описанието на SNMP обектите, **като тук се използва стойността на [P]от SNMP минус 1**. Например за NetControl 8Rxxxx Line1 е с PP=08, Line2 PP=09, Line3 PP=0A ... Line8 PP=0F; Можете да използвате PP=FF -тогава подадената команда ще се приложи на ВСИЧКИ изходни канали (релета). Това е равносилно на командите AllOn/AllOff от Web интерфейса
- VV е стойността, която да се подаде към изхода: възможни са стойности '00' = изключи релето и '01' – включи.

```
>curl -u admin:admin "http://<NetControl IP address>/iochange.cgi?ref=ioreg.js&09=01"
```

На заявката *NetControl* отговаря с JavaScript файла `ioreg.js` (ако не Ви интересуват данните от файла, може да замените `'ioreg.js'` със `'re-done'` във заявката и тогава ще се връща малък HTML файл). JS файла съдържа стринга IO, в който са текущите статуси на всички входно-изходни вериги:

```
IO="00,00,00,00,00,00,00,00,01,00,00,01,00,00,00,00,00,01,01,00,00,00,00,00,01C  
B,0015,000C,005A,005A,0068,03FD,0145"
```

Първото число се отнася за канал с  $[P]=1$ , второто за  $[P]=2$  .... и така за всичките 24 цифрови входно-изходни вериги (не всички от тях са достъпни в конкретния *NetControl* модел). И тук стойност 00 отговаря на изключено, а 01 – на включено състояние.

Последните 8 числа, са стойностите за 8-те входа на аналогово-цифровия преобразовател (стойност от 0 до 1023), като връзката със сензорите на конкретния *NetControl* е отново през номера на канала  $[P]$  от SNMP обектите за достъп.

Всички числа в IO са шестнадесетични!

С изчитане директно на „`http://<NetControl IP address>/ioreg.js`” винаги имате достъп до моментното състояние на входовете и изходите.

За улеснение на потребителите сме публикували на [www.ipnetcontrol.net](http://www.ipnetcontrol.net) примерен PHP код за достъп до входно-изходните вериги през HTTP URL, както и през SNMP.




## 3.2. Мрежови параметри и настройки (меню „IP Settings”)




**ВАЖНО!!!** Поради спецификата на SNMP протокола, който се поддържа от устройството (невъзможност за едновременен достъп до няколко OID), първоначалната настройка на IP/Mask/Gateway е желателно да се направи през Web. В противен случай може да се окаже невъзможно задаването на желаните настройки, поради ограничението за промяната им поединично.

### 3.2.1 Секция „IP Configuration“

Software Version	Текуща версия на софтуера в устройството
Hardware	Показва хардуерната версия на IP ядрото (последно 2.2)
Ext.Flash	Информация за наличие и обем на допълнителна флаш памет
System Uptime	Време (d:h:m) от последното включване контролера
PHY (Uptime)	<p>Време (d:h:m) от последното рестартиране на PHY трансивъра.</p> <p> Ако двете времена се различават, това означава, че е PHY чипа е рестартиран от функцията "Restart PHY if no RX frames in XX seconds". Това може да е сигнал за наличие на силни електромагнитни смущения, които нарушават работата на чипа!</p>
Last power off (v5.90)	Време на последното изключване на устройството от захранването (софтуерно рестартиране на устройството НЕ обновява тази информация). За да работи тази функция е необходимо да има валиден SNTP сървър или сверен хардуерен RTC.
MAC address	MAC адрес на устройството
Ethernet Settings	Връзка към страница за настройка на физическите параметри на Ethernet връзката. За повече информация вижте след таблицата.
WiFi enable mode	<p>Режим на работа на WiFi модула (достъпно е само за модели с допълнителен WiFi модул).</p> <p>Достъпни са два режима:</p> <p><b>'When Ethernet Down':</b> WiFi се активира при отпадане на Ethernet връзката (т.е. физическо премахване на кабела или спиране на отсрещното устройство). WiFi се деактивира при възстановяване на Ethernet връзката.</p> <p><b>'Never':</b> WiFi модулът е деактивиран</p>
IP address, Subnet mask, Default gateway	Стандартните мрежови настройки за адрес, маска и шлюз за достъп от/до Интернет/външни мрежи
Primary/Secondary DNS server	IP адреси на DNS сървъри, които се използват за намиране на IP адресите на имената от „DNS names cache“. Първо се използва Primary сървъра – ако се получи код за грешка или липса на отговор се прави опит с Secondary сървъра. Ако и двата не дадат резултат – след 15 минути се започва отначало.
DHCP client	Определя дали параметрите адрес, маска и шлюз са статично зададени или се получават динамично през DHCP протокол
Tagged VLAN mode	Активира режим на тагнат VLAN (802.1q)
VLAN ID	Таг (ID) на VLAN в режим „Tagged VLAN mode=Enable“
Access MAC address 1 and 2 / Global access filters/	Ограничаване на достъпа до устройството към до два MAC адреса. Нулева стойност на адрес не се взема в предвид (съответно и двете нулеви = без ограничаване на достъпа).

	 <p>При използване на защита по MAC адрес, да се има предвид, че при достъп от външни мрежи, към модула пристигат пакети с MAC адреса на Default Gateway. В такъв случай той трябва да бъде винаги зададен като един от двата адреса с достъп.</p>
Network IP/MASK / Global access filters/	<p>Заклучване на достъпа до устройството само от зададената мрежа/маска. Маска 0.0.0.0=без заключване. Изходящи услуги (като SPC, MQTT) не се влияят от този филтър.</p> <p> <i>Защитата по MAC адрес е с ПО-ВИСОК приоритет от тази по IP/MASK!</i></p> <p> <i>Ако Ви се наложи да промените през SNMP параметрите на мрежата за достъп първо настройвайте IP адреса при отворена маска (0.0.0.0), а след това маската. В противен случай (при смяна първо на IP адреса, при някаква зададена маска) може да се получи нежелана комбинация от IP/MASK и да се блокира достъпа.</i></p>
External managing service	<p>От тук може да се зададе по какъв протокол да се управлява устройството отдалечено: SmartSpaceCloud (domo.ipnetcontrol.net), MQTT или без външно управление. Под тази настройка се изписва и статуса на връзката ONLINE/OFFLINE.</p>
TFTP client	<p>Разрешава/забранява обновяването през TFTP</p>
TFTP server IP address	<p>IP адрес на сървъра, съдържащ имиджа за обновяване. За повече информация относно обновяване през TFTP отидете на стр. 38.</p>
SNTP server IP address	<p>IP адрес на NTP/SNTP Time сървър за синхронизиране на часовника (необходим е за работа на модула Timers). Стойност 0.0.0.0 – деактивира синхронизирането и модула Timers.</p>
HTTP service	<p>Деактивиране на достъпа през Web. Удачно е с цел сигурност: при вече конфигуриран и инсталиран модул, който използва други комуникационни протоколи (SNMP, MQTT, SPC).</p>
HTTP listening port	<p>Дава възможност за задаване номер на TCP порт, на който да „слуша“ WEB сървъра. Допустими стойност от 1024 ... 65535. Стандартно е 80.</p>
HTTP auth brute-force blocking	<p>От тук можете да активирате/деактивирате функцията за защита от brute-force атака на Web сървъра. За повече информация за функцията вижте 2.2.</p>
Reboot if no RX frames in	<p>Настройка за софтуерен Watchdog, който следи за постъпващи Ethernet фреймове. Ако няма входящи фреймове за зададеният период от време – <b>NetControl</b> се саморестартира. Функцията се деактивира при задаване на стойност 0 на времето.</p>
ACT LED mode	<p>Задава режима на работа на ACT LED индикатора на устройството. Достъпни са следните режими:</p> <ul style="list-style-type: none"> <li>-“Power ON”: свети постоянно при захранено устройство</li> <li>-“Incoming PING request”: премигва на всеки постъпил „ICMP Echo request“ към IP адреса на устройството</li> <li>-“Incoming PING reply”: премигва на всеки постъпил „ICMP</li> </ul>

	<p>Echo reply“ към IP адреса на устройството. Типично това ще отговор от отдалечено устройство, настроено в „PNIG Monitor“.</p> <p>-“Incoming PING Any”: премигва и за двата предни случая</p> <p>-“DHCP Valid IP”: Когато използвате модула в DHCP режим, индикаторът светва при получен валиден IP адрес. При режим на статични настройки, индикаторът ще работи като "Power ON".</p> <p>-“WiFi Link/Rx”: При режим на работа WiFi светодиода свети постоянно при установена връзка с AP и премигва при входящ трафик. При WiFi светодиода Link/ACT не функционира.</p>
<p>IO User web account</p>	<p>Настройки за вторият (неадминистративен) потребител за Web достъп. Може да се активира или деактивира, както и да му се определи режим на достъп до заглавната страница: Read Only или Action.</p> <p><i>Фабрично (или след ъпдейт на по-стара версия) вторият потребител не е дефиниран и за да функционира е необходимо след като е в режим Enabled, да се зададат име и парола от менюто „Misc“.</i></p> <p> <i>Поставянето на настройката в Disabled деактивира потребителя, но не му изтрива зададените име/парола. При ново активиране с Enabled ще са валидни последните име и парола.</i></p>

### „Ethernet Settings”

От това подменю можете да настроите физическите параметри и режим на Ethernet връзката. Можете да зададете ръчен режим на скоростта и дуплекса на връзката и да деактивирате автоматичното разпознаване на RX/TX усуканите двойки. Имате достъп до информация в какъв режим е установена текущата връзка.

В общия случай (настройката е Link=Auto, Auto MDIX=Enabled) не е необходимо да се правят промени, освен ако не възникват проблеми с връзката с отсрещното устройство.

### „WiFi Settings”

Това меню е достъпно само при наличието на WiFi модул. За повече информация вижте раздел 6.

### 3.2.2Секция „SNMPv1 access settings” и „SNMPv1 traps/remote IO settings,,

В тази секция са всички необходими настройки за достъпване на устройството по SNMP протокол.

<p>SNMP protocol</p>	<p>Указва глобалното разрешаване или забраняване на SNMP протокола</p>
<p>Listen on UDP port</p>	<p>Определя UDP порта, на който „слуша“ SNMP сървър в устройството. Валидни стойност 161 (стандартно) или 1024...65535.</p>
<p>Access to IP configuration</p>	<p>Определя дали през SNMP могат да се променят параметри от IP настройките на устройството. Не влияе на команди за четене/запис от входно-изходните портове.</p>
<p>RO community</p>	<p>Парола за четене (4-13 символа на латиница)</p>

string	
RW community string	Парола за четене и запис (4-13 символа на латиница)

В следващата секция са настройките свързани с генерирането на SNMP автоматични "trap" съобщения от *NetControl*. За да се използва тази функционалност е необходим специален сървър, който да обработва тези съобщения.

Настройката е комбинирана с настройката за друго устройство *NetControl*, което да го командвате през Macros. За повече информация вижте раздел 3.4.1.

Target IP	IP адрес на SNMP trap сървър, към който да се изпращат генерирани SNMP traps. Съобщенията се изпращат към стандартния порт 162 (UDP). Този IP адрес се използва и за „Remote IO” - изпращане на команди (през Macros) към друго NetControl устройство.
Community string	Парола за TRAP сървъра (4-13 символа на латиница) и същевременно за „Remote IO”.
UDP port for remote IO	Определя UDP порта, на който ще се изпращат SNMP съобщенията за „Remote IO”. Стандартно SNMP ползва порт 161 (UDP), но може да се зададат и други стойности.

### 3.2.3 DHCP - динамично зареждане на основните мрежови параметри

Устройството поддържа протокола DHCP, който позволява да се заредят динамично (при наличие на DHCP сървър в мрежата) следните параметри:

- IP адрес (IP address)
- мрежова маска (Network mask)
- шлюз по подразбиране (Default Gateway)
- DNS сървъри (**option domain-name-servers**) – 2бр. (от v5.37)
- TFTP сървър (**option swap-server**) за обновяване (след v3.3)
- SNTP сървър (**option ntp-servers**) – взема са само първият IP адрес

Първите три параметъра IP/Mask/Gateway са задължителния минимум за да функционира нормално устройството. Останалите параметри, ако не се подадат през DHCP протокола, използват последно зададените статични стойности от настройките.

През DHCP също можете да изберете и от имената на хостове само за TFTP и SNTP независимо, че DHCP директно не позволява това. За целта като IP адрес трябва да зададете **0.0.1.D**, където D=[1..10] съответства на номера на името на хоста от списъка „DNS names cache” (виж 3.2.4).



*NetControl* съхранява в енергонезависима (FLASH) памет всички свои настройки, включително и мрежовите такива. Заредените през DHCP параметри НЕ водят до обновяване на тези в FLASH паметта (освен ако в режим на DHCP не са използвани Web страницата с настройките и се натисне „Apply Settings” – тогава текущите стойности от DHCP ще бъдат записани в паметта). За това при изключване на опцията DHCP устройството възприема последно записаните в паметта настройки.



Разрешаването на DHCP клиента при липса на работещ сървър (или наличие на мрежов проблем) може да доведе до невъзможност на *NetControl* да зареди мрежовите си параметри и по този начин достъпът до него да се загуби. За да се предотврати това *NetControl* изчаква определен период от време (до около 40s след рестартирането си) за да получи мрежовите си настройки. В случай, че не успее, *NetControl* зарежда последно настроените си статични параметри и започва да работи с тях, като същевременно

продължава да търси DHCP сървър. Ако се получи отговор от сървър NetControl мигновено възприема новите си динамични параметри.



При достъп през Web и разрешен DHCP режим в полетата на съответните параметри се изписват данните, получени от DHCP сървъра, а не статично зададените такива! Ако искате да видите какви са в момента заредените му статични настройки изключете опцията (без да потвърждавате с „Apply Settings“) и те автоматично ще се покажат в полетата.

Следния пример накратко илюстрира примерни настройките в dhcpd.conf (Linux) за динамично конфигуриране в мрежа 192.168.1.0, като на определено устройство (pico\_test, разграничава се по даден MAC адрес) са индивидуално фиксирани IP/Mask/Gateway, TFTP и SNTP.

File: dhcpd.conf (partial content)

```
#
# Sample configuration file for ISC dhcpd for Debian
#
# $Id: dhcpd.conf,v 1.4.2.2 2002/07/10 03:50:33 peloy Exp $
#
# option definitions common to all supported networks...

option subnet-mask 255.255.255.0;
default-lease-time 600;
max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.160 192.168.1.175;
    option domain-name-servers 192.168.1.1, 8.8.8.8;
    option routers 192.168.1.1;
    option subnet-mask 255.255.255.0;
    default-lease-time 3600;
    max-lease-time 7200;
}

host pico_test {
    hardware ethernet ec:f2:36:00:0b:db;
    fixed-address 192.168.1.158;
    option swap-server 192.168.1.104;
    option ntp-servers 192.168.1.1;
    #Use the second host name from user cache as SNTP server (e.g. 0.bg.pool.ntp.org)
    #option ntp-servers 0.0.1.2;
}
```

### 3.2.4 Списък с имена на хостове, които могат да се ползват от различни услуги

От v5.37 на системния софтуер е добавен списък от 10 имена на хостове, които могат да бъдат избирани като адреси за услугите TFTP, SNTP, SNMP, MQTT и Ping Monitor. За всяка услуга, потребителят избира дали да използва име от DNS списъка или IP адрес. До списъка се достига от линка „Manage DNS names cache“ в менюто „IP Settings“.

За всеки от 10-те броя записи е налично поле за въвеждане на името на хоста (напр. 'yahoo.com'); всеки нововъведен хост трябва да бъде потвърден със съответния бутон „Change“.

В полето „IP address“ ще се изпише IP адресът, който са върнали DNS сървърите или съобщение за грешка с нейният RCODE. Най-честите грешки, които ще видите са **NXDOMAIN** – такъв домейн/име не съществува или **NOIP** – името съществува, но няма IP адрес. В скоби ще видите и (P) или (S) – това ще Ви покаже кой от DNS сървърите (Primary/Secondary) са върнали съответния резултат.

Бутонът „Pruge DNS cache“ Ви дава възможност да изчистите наличната информация за IP адресите и отново да се направи запитване към DNS сървърите.

Ако искате да използвате IDN имена (напр. съдържащи кирилица и други символи) е необходимо първо да ги преобразувате до ASCII (през дадения в страницата [линк](#)).



Използването на имена на хостовете дава по-голямо удобство, но трябва да се има предвид, че процесът на превръщане на името към IP (с което реално се работи в TCP/IP стека) добавя допълнителна латентност в процесите. При Ping Monitor това би могло да доведе до некоректен timeout.

Status	IP Settings	I/O Settings	Macros	Timers	PING Monitor	Automation	Misc
Domain names database ( <a href="#">Refresh page</a> )							
No.	Name (max. 63 chars)	IP address					
1	<input type="text" value="www.google.bg"/>	<input type="text" value="172.217.17.227 (P)"/>	<input type="button" value="Change"/>				
2	<input type="text" value="0.bg.pool.ntp.org"/>	<input type="text" value="46.40.123.212 (P)"/>	<input type="button" value="Change"/>				
3	<input type="text" value="www.google1.bg"/>	<input type="text" value="NXDOMAIN(3) (S)"/>	<input type="button" value="Change"/>				
4	<input type="text"/>	<input type="text"/>	<input type="button" value="Change"/>				
5	<input type="text"/>	<input type="text"/>	<input type="button" value="Change"/>				
6	<input type="text"/>	<input type="text"/>	<input type="button" value="Change"/>				
7	<input type="text"/>	<input type="text"/>	<input type="button" value="Change"/>				
8	<input type="text"/>	<input type="text"/>	<input type="button" value="Change"/>				
9	<input type="text"/>	<input type="text"/>	<input type="button" value="Change"/>				
10	<input type="text"/>	<input type="text"/>	<input type="button" value="Change"/>				
* International Domain Names (IDN) must be converted to ASCII from <a href="#">here</a>							
<input type="button" value="Purge DNS cache"/>							

### 3.2.5 Филтър по IP за сървърните услуги (SNMP, HTTP, ModBUS)

Във версия 5.56 е разширена базовата функционалност („Global access filters”) за ограничаване на достъпа до **Services access list** предоставяните от него услуги: „IP settings” → „Services access list“.

Този нов филтър позволява описване на до 3 IP адреса, с индивидуални настройки за това, към кои услуги се разрешава или забранява достъпа. Услугите са само такива, които са в режим “listen”, например SNMP, HTTP (съответно тези филтри нямат влияние върху изходящи услуги като MQTT, SPC и т.н.).

Clients not in list access	SNMP	HTTP	MBUS
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Client 1 IP	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="1"/>
	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="102"/>
Client 1 access	SNMP	HTTP	MBUS
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Client 2 IP	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="0"/>
Client 2 access	SNMP	HTTP	MBUS
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Client 3 IP	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="0"/>
Client 3 access	SNMP	HTTP	MBUS
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Освен индивидуалните настройки за услугите на всеки филтър има и една глобална група с настройки („Clients not in list access“), която е валидна за тези IP адреси, които не са намерили съвпадение в списъка. Задаването на IP адрес 0.0.0.0 на практика деактивира реда от списъка.

В посочения пример за IP адрес 192.168.1.102 са разрешени само HTTP и MBUS достъп, а този по SNMP е забранен. За всякакви други клиентски IP адреси са разрешени SNMP и HTTP, но MBUS е забранен.

### 3.3. Входно-изходните вериги. Режими на работа и параметри. (меню “IO Settings”)

В това меню са събрани всички настройки, касаещи наличните в устройството входно-изходни вериги: релета, входове за температура, напрежение и др.

В най-горният край на страницата можете да поставите свое име на устройството „**Host name**“. От информацията за модела, която също е изписана до името на устройството, ще бъдете директно препратени към страницата с описанието на съответния модел.


Също така можете да поставите Ваши имена и на всеки един от наличните вериги. Името ще се вижда, както в началната страница, така и може да бъде получено чрез SNMP заявка.



*Потвърждаването на имената става с отделен бутон: „Change Names“. Ако преди да го изберете първо потвърдите други настройки с бутона „Change Parameters“, то имената няма да се запазят. Двата бутона работят независимо един от друг!!!*

#### 3.3.1 Цифрови входове-изходи („Digital I/O Channels“)

В зависимост от модела *NetControl* разполага с различни цифрови входно-изходни вериги – релета, цифрови входове и др. Всички те са налични за конфигуриране в този раздел.

Visible	Определя дали каналът да бъде видим в началната страница. Не влияе на достъпа през SNMP; не спира действието на командите All ON/All Off.
Name	Име на канала (промяна в имената се потвърждава с бутона „Change Names“)
Default	Задава началното състояние на изхода/входа след подаване на захранване на устройството: ON, OFF, Last В 'Last' последното състояние се помни в енергонезависима памет и при рестартиране се зарежда запазената последна стойност. <b>Този режим не функционира за режим на изхода „Impulse“</b> За повече информация вижте обясненията след таблицата!
Mode	Задава режима на работа на канала. За по-подробна информация виж обясненията след таблицата!
Delay[s] Impulse[s] Filter[ms]	Задава времето на импулса в секунди за изходи с Mode=Impulse Output. Максимална стойност 16383s.   <i>Времето 'Impulse' е с точност [-100ms;0], т.е. реалното време е по-малко с до 100ms или равно на зададеното (от v5.62).</i>  За цифрови входове – задава стойността на цифровия филтър, който филтрира генерирането на събития при промяна на състоянието му. В този случай стойността е в ms, като е на стъпка

	<p>20ms. Максимално допустима стойност 65535.</p> <p><i>Препоръчително е да се използват стойност от няколкостотин ms, когато става дума за механични контакти, свързани към входа – така се гарантира, че няма да има множество събития в следствие на механичното трептене на контактите преди да заемат стабилно състояние.</i></p> <p>(от v5.59) За изходите в Mode=Manual/Toggle се задава закъснение (Delay) в секунди на изпълнението на командите за включване. Стойност „0“ (по подразбиране) деактивира забавянето и командите се изпълняват директно.</p> <p><i>Закъснението е полезно при автоматични процеси и дистанционно управление, където е възможно поради различни причини да се струпат бързи ON-OFF-ON-OFF последователности. За някои типове товари това не е полезно. Закъснението на практика елиминира междинните изключения и оставя само последното включване (след като изтече времето на закъснение). Командите за изключение ВИНАГИ се изпълняват мигновено!</i></p>
Invert Output	<p>Поставянето на тази отметка води до „обръщане“ на подаваните към релето команди. Използвайте я, когато товарът е свързан към нормално затворения контакт на релето – така състоянието ON в интерфейса и в SNMP ще отговаря на „ВКЛЮЧЕН“ товар.</p>

Стойността от полето „Default“ има различно значение според това дали каналът е вход или изход. Ако става дума за изход (напр. реле) това определя състоянието на релето след включване на захранването. В този случай от значение е и стойността на параметъра „Invert Output“.

**За улеснение може да използвате правилото: когато товарът е свързан през нормално затворен (Н.З.) контакт, включете „Invert Output“. Това е задължително и ако искате облачната платформа правилно да отчита състоянията включено/изключено на товара (респ. да калкулира изразходвана енергия)**

Състояние (“Default”)	“Invert Output”	ТОВАР през Н.О. контакт	ТОВАР през Н.З. контакт	Бобина на релето под напрежение
OFF	НЕ	ИЗКЛЮЧЕН (OFF)	ВКЛЮЧЕН (ON)	НЕ
ON	НЕ	ВКЛЮЧЕН (ON)	ИЗКЛЮЧЕН (OFF)	ДА
OFF	ДА	ВКЛЮЧЕН (ON)	ИЗКЛЮЧЕН (OFF)	ДА
ON	ДА	ИЗКЛЮЧЕН (OFF)	ВКЛЮЧЕН (ON)	НЕ

Когато става дума за цифров вход параметърът „Default“ определя какъв потенциал да се подаде вътрешно към входа, така че бидейки оставен несвързан (отворен) да има определено стабилно състояние.

Въпросният потенциал се получава в следствие на вътрешно „свързване“ на pull-up или pull-down резистор (~50kOhm) към +3.3V или 0V. Тази функционалност позволява на такъв вход директно да се свърже механичен контакт (от бутон, рид-ампула и др.) към 0V (при Default=HIGH/ON) или към +3.3V (при Default=LOW/OFF). В този случай настройката „Invert Output“ не оказва влияние на това, към кой

потенциал да бъде вътрешно свързан входа. Но ще инвертира стойността, която се изчита от входа.

Параметърът „**Mode**” определя режима на работа на канала. За изходите са налични три режима:

- „**Manual Output**” - ръчно управление на канала. Промяната на състоянието му ON/OFF става с ръчно подадена команда през Web/SNMP/SmartSpaceCloud/MQTT и др.
- „**Impulse Output**” - Импулсен изход, който след команда сменя състоянието си за определено време (зададено в полето **Impulse[s]**) и след това се връща в изходното (т.е. зададеното „Default”) състояние.



Когато командата се подава през SNMP или от Macros трябва да се има предвид, че запускането на импулса (независимо дали „Default” на изхода е Low или High) става със подаване на състояние ON=1.

През времето на импулса е допустимо да се подаде команда OFF=0 - тя ще доведе до форсирано връщане на изхода в начално състояние.



Повторно подаване на команда за стартиране на импулса, докато той вече е стартиран води до започване на ново отмерване на времето на импулса, т.е. той се запуска отначало (удължава се).

- „**Toggle Output**” - подаването на каквато и да е команда (ON или OFF) води до преобръщане на текущото състояние на изхода. Този режим може да се използва за по-високоскоростно обръщане на изхода за генериране на периодични сигнали (не е подходящ за релейни изходи).

### 3.3.2 Аналогови входове („Analog I/O Channels“)

Различните видове измервателни канали (температура, напрежение, ток и др.) се подават на вградения аналогово-цифров преобразовател (ADC). Той преобразува напрежението, генерирано от датчика в цифров код и след това се изчислява първичната величина по съответните формули.

Както и при другите канали може да зададете име на всеки канал (**Name**) и дали да е видим в „Status” страницата (**Visible**).

Падащото меню „**Mode**” определя зависимостта по която се преобразува измереното от входа напрежение в съответната физична величина.

Тъй-като един и същи канали могат да измерват различни величини (според сензора, който е поставен на тях), то на всеки от тях може да се избере която и да е величина, но това не означава, че реално устройството може да я измерва.

За моделите, които имат канал за измерване на магистрално напрежение от тук трябва да се зададе дали се измерва VDC или VAC.

„**MA Filter Points**“ полето определя броя измервания на вградения [Moving Average](#) филтър (от v5.39) за аналоговите входове: от 1 (няма филтриране) до 256 измервания. Филтърът усреднява зададения брой измервания и така ефективно премахва шума от тях (за сметка на бързодействието). **За разлика от стария метод на филтриране, тук то се прилага за всички модули, които имат достъп до аналоговите входове – Automation, Web, MQTT, SNMP, SPC!!! Само в SNMP има достъп и директно до аналоговия вход преди филтъра.**

Времето на реакция на филтъра, т.е. времето между промяната на входната величина и стартирането на Automation например, се определя по формулата:

$$T_f = N * ScanInterval,$$

където N е броя на измерванията на филтъра (1, 2 ... 256)

ScanInterval – преиода на сканиране на аналоговите входове (виж 3.3.3)

*В по-старите фърмуерни версии вместо MA филтъра има примитивен филтър, аналогичен на този при цифровите канали: „**Filter [ms]**”. Тук е свързан само с*

функционирането на **Automation** частта: определя колко ms трябва измерената стойност да е стабилно под/над зададения праг преди да се изпълни Automation. Това филтриране е изключително важно за стабилната работа на **Automation** режимите, тъй-като без него (или при много малки стойности на филтъра) може да се получи „осцилация“ около зададения праг, което да води до генерирането на много изходящи команди.

### 3.3.3 Други общи настройки за входовете

От v5.46 е въведен раздел „Miscellaneous parameters“, в който са поставени общи настройки за всички входове.

Наличните настройки към момента са:

Analog inputs scan interval	Определя честотата на сканиране (ScanInterval) на аналоговите входове. Стъпката е през 20ms, фабрично е 20ms, но може да се увеличи до 2000ms.
"Toggle" only with 1 (0=Off)	За цифровите изходи, които са в режим „Mode = Toggle Output“, тази отметка определя дали обръщането на състоянието да става само с подаване на 1/On (при поставена отметка) или да става и с двете стойности 0 и 1 (Off и On). В първия случай подаването на 0/Off действа като стандартна команда и изхода заема това състояние.

От v5.19 на фърмуера е добавена нова възможност потребителя сам да дефинира до 2 специфични сензори, които са свързани към аналоговите входове. Това позволява към да се използват всякакъв тип сензори с напреженов изход в диапазона 0...3.3VDC.

Двата потребителски сензора се появяват в падащото меню 'Mode' като 'User defined 1, 2'. За да ги редактирате е необходимо да влезете в линка „*Edit user defined sensors*„.

За настройката е необходимо да познавате функцията на преобразуване на сензора, която трябва да може да се опише като:

$$U[V] = a + b * \text{'Sensor physical value'}$$

, където U е напрежението на изхода на сензора (във волтове);

a и b са коефициенти (реални числа с плаваща запетая)

'Sensor physical value' – е стойността на физическата величина, която измерва сензора (напр. градуси, Bar, скорост на вятъра и т.н.)

Да вземем за пример сензор за налягане 0..16Bar с изход по стандарта 0..10V. Лесно можем да установим, че функцията му на преобразуване в напрежение е:

$$U[V] = 10/16 * P[Bar] \Rightarrow a = 0.0, b = 0.625$$

Дименсията на измерваната величина от Вашия сензор въведете в полето 'Dimension' (допускат се до 4 символа) – тя ще се използва при визуализацията на стойностите в основната страница, в Automation блока и в MQTT JSON съобщенията. Можете да оставите дименсията и празна.

Данните от сензора се закръгляват до два знака след десетичната запетая. Ако Ви е нужна по-голяма точност може да преработите формулата и да изобразявате мили-, микро-, кило-, мега- и т.н. от физическата величина.

### 3.3.4 Виртуално входно-изходни канали (Virtual IO)

Във v5.59 са въведени 8бр. виртуално входно-изходни – това са софтуерни регистри, на които могат да се присвояват стойности [0..255]. На тях не отговарят реални хардуерни входове или изходи. Стойността им не се запазва при рестартиране на устройството и те се нулират.

Основното им предназначение е да разширят възможностите на функциите Automation, Macros, Timers. А в някои специализирани модели ще се ползват за достъп до информация, получена от външни устройства (напр. през RS-485).

До тях има достъп през MQTT (запис/четене) и по ModbusTCP (само четене като 32bit двойки)

В менюто „IO Settings“ през линка „Virtual Ports“ имате достъп до моментните стойности на Virtual IO портовете, както и да променят тяхната стойност.



*Всяка промяна на стойността на Virtual IO порт предизвиква проверка в Automation блоковете, в които той участва като източник на данни ('Main Sensor').*

### 3.4. Macros – последователности от действия на изходните вериги

Това е нов функционален модул, който позволява на потребителя да дефинира групи от действия с изходните вериги, комбинирани с времеви закъснения. Например:

**“Включи Line1 → Изчакай 10s -> Включи Line 2 → Изчакай 5s -> Изключи Line1 → Изключи Line 2 → КРАЙ“**

Тези групи от действия (Macros) могат да се стартират ръчно (през Web, SNMP, MQTT), от друг макрос, от автоматичните задачи ('Automation'), от таймери („Timers“) или от 'Ping Monitor' модула. **Тези макроси НЕ се поддържат в облачната платформа (тя има собствен Automation модул за тази цел).**


Модулът за Macros (достъпен от менюто 'Macros' в Web интерфейса) съдържа 24 блока за дефиниране на последователности от действия като всеки блок съдържа 8 реда/клетки.

Status	IP Settings	I/O Settings	Macros	Timers	PING Monitor	Automation	Misc
<div style="display: flex; justify-content: space-around;"> <span>Show macros 1...8</span> <span>Show macros 9...16</span> <span>Show macros 17...24</span> </div>							
<div style="border: 1px solid #ccc; padding: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span><b>abcdef_Macro01</b></span> <span>Start Stop</span> </div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Visible <input checked="" type="checkbox"/> Restart <input checked="" type="checkbox"/> Auto Start         </div> <div style="margin-top: 5px;"> <div style="display: flex; justify-content: space-between;"> <span>IO Action</span> <span>Pin Name 00001</span> <span>ON</span> </div> <div style="margin-top: 5px;"> <span>Sleep</span> <input type="text" value="1"/> s         </div> <div style="display: flex; justify-content: space-between;"> <span>IO Action</span> <span>Pin Name 00001</span> <span>OFF</span> </div> <div style="margin-top: 5px;"> <span>Sleep</span> <input type="text" value="2"/> s         </div> <div style="display: flex; justify-content: space-between;"> <span>IO Action</span> <span>Pin Name 00001</span> <span>ON</span> </div> <div style="margin-top: 5px;"> <span>Sleep</span> <input type="text" value="3"/> s         </div> <div style="display: flex; justify-content: space-between;"> <span>IO Action</span> <span>Pin Name 00001</span> <span>OFF</span> </div> <div style="margin-top: 5px;"> <span>Start Macro</span> <span>abcdef_Macro01</span> </div> </div> </div>							
<div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span><b>abcdef_Macro02</b></span> <span>Start Stop</span> </div> <div style="margin-top: 5px;"> <input type="checkbox"/> Visible <input checked="" type="checkbox"/> Restart <input type="checkbox"/> Auto Start         </div> <div style="margin-top: 5px;"> <div style="display: flex; justify-content: space-between;"> <span>IO Action</span> <span>Pin Name 00003</span> <span>ON</span> </div> <div style="margin-top: 5px;"> <span>Sleep</span> <input type="text" value="2"/> s         </div> <div style="display: flex; justify-content: space-between;"> <span>IO Action</span> <span>Pin Name 00003</span> <span>OFF</span> </div> <div style="margin-top: 5px;"> <span>EXIT</span> </div> </div> </div>							

Макросите са разделени на групи от по 8 бр. за по-голяма прегледност. **Моля, имайте предвид, че бутона „Apply changes” записва промените само в текущата група макроси, която е показана в браузера!**

В следващата таблица са описани достъпните параметри за настройка на всеки макрос:

Име на макроса	Свободен текст за име на макроса. Максимум 15 символа.
Start / Stop	Бутони за ръчно стартиране или спиране на макрос. Спирането е полезно при работа с циклични макроси.
Visible	Определя дали на заглавната страница ('Status') да се показва бутон за ръчното стартиране/спиране на макроса
Restart	Макросите, с отметната тази опция, започват изпълнението си от начало, всеки път щом дойде команда/събитие за това, независимо дали макросът се изпълнява в момента или не. Макросите без тази отметка – не се запускат повторно от начало, ако в момента се изпълняват. <b>Този параметър не влияе на случая, когато макрос запуска отново самия себе си и такова самозапускане е винаги разрешено.</b>

Auto Start	В този режим макросът се стартира автоматично със стартирането на <b>NetControl</b> .
Редове/клетки	<p>Всяка клетка (8бр. за всеки макрос) може да бъде:</p> <ul style="list-style-type: none"> <li>- 'EXIT': край на текущия макрос (текущият макрос се приключва и след изпълнение на 8-мата клетка)</li> <li>- 'IO Action': действие към изходен канал (напр. Line1 = ON). <b>Изходи в режим „Impulse” се запускат винаги с ON!</b></li> <li>- 'Sleep': времезакъснение в секунди (1...65535)</li> <li>- 'Start Macro': стартиране на макрос (вкл. и на самия себе си) и продължаване на текущия. <b>Първо се приключва текущия макрос и тогава ще се започне стартирания.</b></li> <li>- 'Stop Macro': спиране на макрос и продължаване на текущия</li> <li>- „Remote IO Action” (v5.22+): подаване на команда към друго устройство (през SNMP). Трябва да уточните валидните канали на отсрещното устройство ([P])</li> <li>- „Remote Macros Action” (v5.94+): стартиране/спиране на макрос на друго устройство (през SNMP).</li> <li>- 'EXIT IF' – приключване на макроса, ако даден вход/изход/виртуален канал има определена стойност в момента на проверката.</li> <li>- 'Skip next step IF' – прескачане на следващата стъпка от макроса, ако даден вход/изход/виртуален канал има определена стойност в момента на проверката.</li> <li>- 'IF Value' – не е достъпна за избор от потребителя, активира се автоматично в комбинация с предните два вида стъпки и чрез нея се задава стойността за сравняване.</li> <li>- 'Invert State': (v5.66) действие към изходен канал/VirtualIO, което обръща текущото му състояние (напр. от ON към OFF). Резултатът от инвертирането е винаги 0 или 1, а за изходите с PWM(аналогови) 0%/100%</li> </ul> <p> Времето 'Sleep' се задава в секунди, като отклонението от зададената стойност е (-100ms;0], т.е. реалното време е по-кратко с до 100ms или равно на зададеното (от v5.62).</p>

Възможността един макрос да стартира друг, позволява произволно количество (или дори всички) макроси да се свържат верижно като един макрос с повече на брой клетки.

Също е възможно макрос да стартира отново себе си: така се получава безкрайно циклично изпълнение на макроса или група от макроси (докато не се промени конфигурацията им или не се спре ръчно). Комбинацията на цикличен макрос с режим '**Auto Start**' дава възможност **NetControl** да изпълнява винаги дадена последователност от действия.

'Stop Macros' позволява прекъсване на макроси по команда или дори в следствие на Automation, Timer или Ping Monitor (тъй-като тези модули имат само настройката за стартиране на макрос, то ще е необходимо да се направят междинни макроси, през които да се реализира Stop). Спирането на макрос е много полезно при управление на циклични макроси: например, превключване от един към друг цикличен режим.



Използването на циклична група от макроси да се планира много внимателно, тъй-като се създават много различни ситуации на действия, особено ако се комбинира с Automation, Timers или Ping Monitor.



Ръчното спиране на циклична група от верижни макроси ще бъде доста трудно практически, поради липсата на информация кой макрос е активен, за да се подаде на него команда 'Stop'. Вариант е да се подаде Stop последователно на всички участващи макроси или да се премахне временно samozапускането и да се изчака да приключи последователността от действията.

През SNMP макросите не могат да се конфигурират, но могат да бъдат ръчно стартирани или спирани с командите:

```
Start: >snmpset -v1 -c private 192.168.1.100 .1.3.6.1.4.1.19865.2.3.6.M.0 i 1
Stop: >snmpset -v1 -c private 192.168.1.100 .1.3.6.1.4.1.19865.2.3.6.M.0 i 0
```

където M=[1..24] е номера на макроса за стартиране

Макросите могат да се стартират/спират и през MQTT – виж 5.3.2.

Можете да комбинирате Macros с изходи в режим „Impulse Output” - така ще получите още по-широки възможности за комбиниране и получаване на различни последователности от действия.

### 3.4.1 „Remote IO/Macros Action” - подаване на команда за действие към друг NetControl

„Remote IO Action” Ви дава много интересна възможност да пренесете дадена автоматика през мрежовата връзка и да управлявате друго *NetControl* устройство. Разбира се, това е лесно постижимо с облачната платформа, но тази функция ви позволява „peer-to-peer” комуникация между две устройства, без наличие на междинни системи.

Според модела на другото устройство трябва да уточните, кои номера [P] канали са налични в него и да ги изберете в макроса (показват се всички възможни 24 изходни канала, но при всеки модел е реализирана различна част от тях). За управление на макрос – просто задайте номера на отдалечения макрос и типа команда.

Настройката за командването устройство е в раздела IP Settings->SNMPv1 traps/remote IO settings. Тези настройки трябва да кореспондират на настройките за SNMP на другото устройство (паролата трябва да съвпада).



Когато използвате „Remote IO Action” в Macros, който е с опция „Auto Start” (стартиране с включване на устройството) винаги оставайте преди него Sleep от 5-10 секунди. В противен случай командата „Remote IO Action” се изпълнява в много ранен етап, в който мрежовите протоколи (напр. ARP) все още не са се инициализирали и командата няма как да бъде изпратена.



Имайте предвид, че командите се подават по UDP посредством SNMPv1 протокола. При съвременното ниво на мрежовите комуникации загубите на пакети са изключително ниски, дори пренебрежими. Но теоретично е възможно загуба на данни и съответно неизпълнение на подадената команда. За по-голяма надеждност можете да дублирате изпращането на командата след някакво време, например: „Remote IO XX” -> Sleep 10s -> „Remote IO XX”

### 3.5. Timers – стартиране на Macros по зададен час:минута, ден от седмицата и месец

Менюто 'Timers' (от v5.21) Ви позволява да дефинирате 16 различни времена (час:минута) на стартиране на даден макрос. Допълнително може да се окаже и в кои дни от седмицата и кои месеци да се изпълнява таймера.

### 3.5.1 Синхронизиране на часовника на NetControl по SNTP

Повечето модели *NetControl* не разполагат с батерийно резервиран часовник за реално време, за това отмерването на време изисква синхронизация на софтуерния му часовник през мрежовия SNTP протокол (това е под-клас на протокола NTP, UDP порт 123). Този протокол се поддържа от всички публични NTP TimeServers, който можете да видите на <https://www.pool.ntp.org>. Други известни NTP сървъри са time.google.com, time.microsoft.com. Изпълнете PING към избраният от Вас сървър и полученият IP адрес въведете в менюто „IP Settings“->SNTP server IP address.

Най-добрият вариант е да използвате локален NTP/SNTP сървър за синхронизиране на Вашите *NetControl* устройства, тъй-като така не сте зависими от външните услуги и Internet свързаността. Освен това междинен сървър Ви дава възможност за резервираност на източника на време, тъй-като обикновено могат да ползват няколко публични сървъра. NTP сървър има вграден в Windows 10 (но не е активиран по подразбиране), лесно достъпен е и за Linux операционните системи (ntpd).

При всяко рестартиране на *NetControl*, на всеки 2 часа и при изпълнение на командата „Sync Now“ или „Apply Settings“ от менюто „Timers“ се прави заявка за текущото време, към зададения сървър. Ако не се получи веднага отговор от него заявката започва да се повтаря периодични (в началото по-бързо, а при трайна липса на отговор на всеки 5 минути).

Status	IP Settings	I/O Settings	Macros	Timers	PING Monitor	Automation	Misc
<b>Time settings</b>							
Current internal clock time		Tue, 13 May 2025 16:48:46					
Last synchronization		Tue, 13 May 2025 15:59:55					<input type="button" value="Sync now"/>
Timezone offset		<input type="text" value="180"/> minutes					
Daylight saving		<input type="text" value="Europe"/>					
<b>Timer No. 1</b>							
<input type="text" value="Enabled"/>							
Start macro		<input type="text" value="Macro01"/> at <input type="text" value="8"/> : <input type="text" value="10"/>					
every		<input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thr <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat					
in		<input checked="" type="checkbox"/> Jan <input checked="" type="checkbox"/> Feb <input checked="" type="checkbox"/> Mar <input checked="" type="checkbox"/> Apr <input checked="" type="checkbox"/> May <input checked="" type="checkbox"/> Jun <input checked="" type="checkbox"/> Jul <input checked="" type="checkbox"/> Aug <input checked="" type="checkbox"/> Sep <input checked="" type="checkbox"/> Oct <input checked="" type="checkbox"/> Nov <input checked="" type="checkbox"/> Dec					

Часовникът на *NetControl* поддържа зимно/лятно часово време за Европа (от v5.71). От потребителя са изисква да определи стандартното отместване спрямо UTC на часовата си зона и да го въведе в полето „Timezone offset“ (стойността е в минути и може да е положителна или отрицателна стойност). Смяната на лятно/зимно часово време става автоматично, ако е активирано „Daylight saving=Europe“.

При правилно настроени мрежови и времеви параметри, в полето „Current internal clock time,“ ще се визуализира Вашето текущо време.

При използване на DHCP може да използвате параметъра „option ntp-servers“ за да зададете динамично адреса на NTP/SNTP сървъра. Имайте предвид, че DHCP позволява да се зададат няколко IP адреса, но *NetControl* взема само първия.



*Точността на софтуерния часовник не е голяма и не е гарантирана. За това е добре да сте сигурни, че сте задали адрес на достъпен и стабилен NTP сървър. NetControl може да работи неограничено време след едно единствено сверяване на часовника му, но ще се натрупва бързо грешка в измерването (може да се очакват десетки секунди отместване на денонощие).*



При синхронизиране на времето след дълга пауза (липса на връзка, неработещ сървър и т.н.) има заложен алгоритъм за проследяване на изпуснати/дублирани събития (в следствие на скоковото отместване на часовника напред/назад). Поради това е възможно няколко Time-ра да се стартират накуп при новото синхронизиране.

При разлика в текущото и новото време повече от 1 час – вътрешният модул за следене на таймерите се ре-инициализира и започва от начало. В такъв случай, събития, които са били в „дупката“ от 1 час ще се загубят или ще се дублират (зависи от това дали вътрешният часовник изостава или избързва).



Модулът Timers реално започва да функционира след първото синхронизиране на времето. Ако такова изобщо не се случи – модулът няма да изработи нито едно събитие. Синхронизира ли се обаче веднъж – ще работи неограничено дълго време, независимо дали има или не нови синхронизации по SNTP (респ. ще се натрупва и неограничена грешка в часовника). Задаването на IP адрес 0.0.0.0 за SNTP сървъра е равносилно на деактивиране на целия модул с Timers (зададените настройки на отделните таймери ще се запазят). При деактивиране или липсата на връзка със сървъра се изписва „Not synchronized“ в полето за „Current internal clock time“.

### 3.5.2 Хардуерен часовник с батерия

При някои модели е вграден допълнителен часовник за реално време (RTC) с батерийно захранване. Той позволява работата на таймерите, както и на други функции, базирани на време да работят с голяма точност и без да е необходим достъп до SNTP сървър (т.е. може контролерът да няма достъп до интернет).

**Time settings**

Current internal time Thu, 05 Feb 2026 09:55:54

Last SNTP synchronization Not synchronized

Hardware RTC Present, valid date

Timezone offset  minutes

Daylight saving

В случай, че Вашият модел разполага и с хардуерен RTC модул, в полето “Hardware RTC” ще видите надпис “Present”. Ако имате и съобщението “valid date” – това означава, че след стартирането на контролера са намерени коректни данни за време и те се заредени във вътрешния софтуерен часовник.

Двата модула: RTC и SNTP работят паралелно, така че ако имате SNTP данни, то сверяването на софтуерния, както и на RTC, ще се стават през SNTP на определен период от време (около 2 часа).

Ако нямате SNTP данни, то остава да работи само RTC, който също ще поддържа точен вътрешния софтуерен часовник през същия интервал от време.



Ако RTC не е сверяван нито веднъж (“invalid date”), то при първото включване на контролера е необходимо да се свери. Ако имате валиден SNTP сървър – това ще стане автоматично при първото получаване на данните от него. Ако нямате – кликнете бутона “Sync now” – това ще вземе системното време на браузера, с който достъпвате контролера. Този бутон форсира и сверяване по SNTP: ако има SNTP данни, те ще останат последните валидни, ако не – ще остане системното време на компютъра.



За да сте сигурни, че RTC модула е коректно настроен: рестартирайте контролера и се уверете, че получавате съобщение “Present, valid date” в полето “Hardware RTC”.



Ако получите съобщение “BATTERY LOW!” след полето “Hardware RTC” това означава, че е засечено ниско напрежение на батерията и тя е разреждана. В този случай ще получите и съобщение “invalid date”. При това положение RTC модулът вече не работи коректно и неговите данни вече не се ползват от контролера (остава само SNTP като източник на

точно време). Имайте предвид, че нивото на батерията реално се анализира само в момента, в който няма основното захранване на контролера и RTC модула остава захранен само от нея. Следователно реалният статус на батерията може да се провери само след като е било изключено захранването на контролера.


### 3.5.3 Настройка на Timer

За да активирате някой от 16-те таймера е необходимо да зададете час:минута на стартиране на даден макрос, както и в кои дни от седмицата ще бъде активен. Ако не маркирате нито един ден – таймерът автоматично се деактивира (става Disabled). Същото важи и за месеците от годината.

### 3.6. 8 (24)-канален “PING Monitor”

Тъй-като едно от основните приложения на серията *NetControl* е активен мониторинг на мрежови трасета и рестартиране на блокирало оборудване е разработен многоканален софтуерен модул за PING към до 8 IP адреса. За модела 24R3S2A броят на каналите е увеличен на 24. При загуба на PING може да се стартира макрос, който да рестартира оборудването, през което преминава отпадналата връзка.

В менюто „PING Monitor” имате достъп до 8-те „**Monitoring Group No.**”. Те имат едни и същи параметри за настройка:

Enabled/ Disabled	Определя дали групата е активирана или не. Деактивирането на група реално е еквивалентно на задаване на нулева стойност на „ <b>If no response within,</b> ”
IP address	Адрес към, който ще се изпращат 'ICMP Echo Request' заявките
If no response within	Определя времето, за което ако трайно няма отговор от IP адреса се счита, че няма връзка. Допустимите стойности са от 40s до 16383s. <b>Не е предвидено активно действие при възстановяване на връзката!</b>
Start macros	Кой номер макрос да се стартира при загубена връзка към IP адреса. Може да се избере и „None” - няма да се изработва действие при загуба на връзката, но при комбиниране с 'ACT Led mode' може да се ползва за визуална диагностика. <b>Имайте предвид, че макросът ще се стартира периодично (през периода на „If no response within“ при трайна загуба на връзката до IP адреса.</b>
Will start macros after	Това поле показва след колко време ще изтече периода, в който считаме връзката за прекъснала и ще се стартира макроса. Тъй-като заявките на всяка група се подават през около 10-16s е нормално тук да се достига до стойности с толкова по-малки от зададеното в „If no response within“ време и след това броенето пак да започва от максимума.  Това поле може да се използва за обратна връзка дали има PING до даден адрес: може да се избере to=Nothing и да се следи дали „Will timeout after“ се възстановява на всеки 10-16 секунди. Ако не се възстановява и постоянно намалява към 0 – то устройството не получава ICMP Echo отговори, т.е. „Няма PING към зададения адрес“. Страницата не се презарежда автоматично; трябва периодично да избирате менюто „PING Monitor” за да виждате актуалната стойност на това поле.

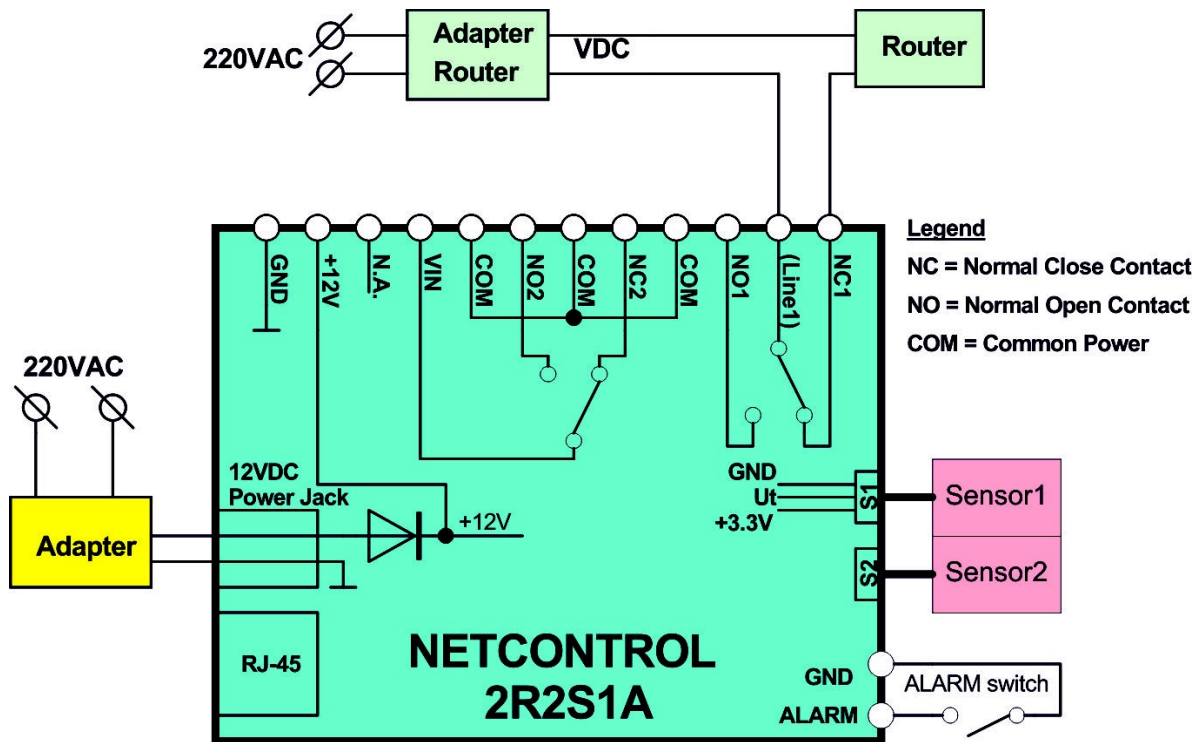
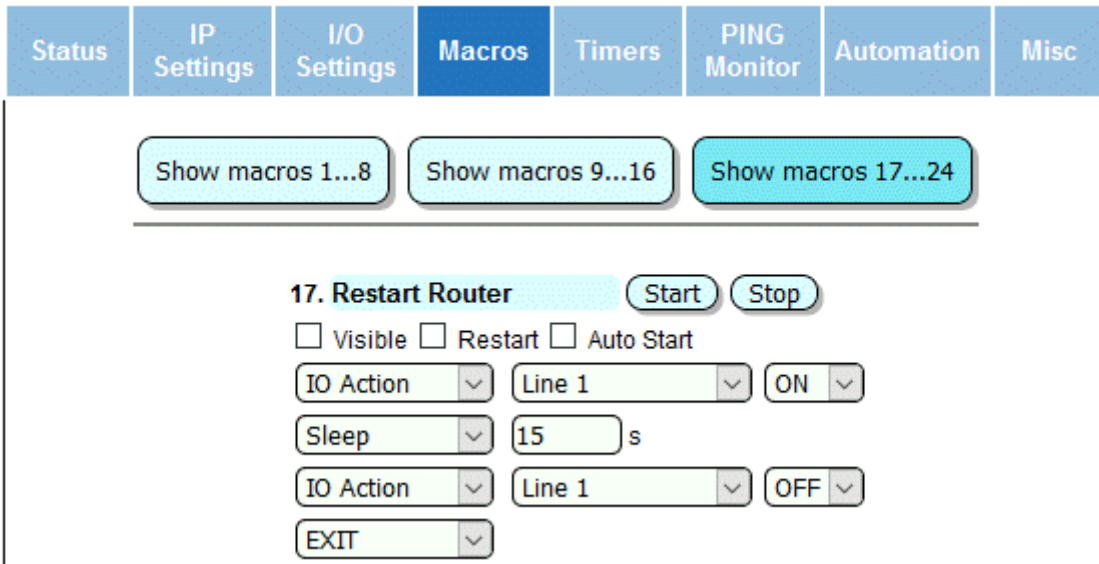
Limit consecutive restarts to	При трайна загуба на връзка от тук може да се ограничи броя на последователно подадените команди за стартиране на макрос (напр. ако няма нужда безкрайно да се рестартира оборудване, в което не е проблема).
Ping data size	Определя големината на данните на ICMP Echo request. Допустими стойности 32..1472 байта.
Start macro when ping restored (v5.86)	При „Disabled“ – функционирането е по стандартния начин, описан в предните параметри. При „Enabled“ – следващият макрос след основния се стартира еднократно при възстановяване на PING до зададения адрес, но само ако преди това е била регистрирана загубата му (по стандартния механизъм). Може да използвате този режим за локализиране на устройства (напр. мобилен телефон) в локалната мрежа и изработване на действие при появата му.

Възможно е да се получи ситуация, при която периода на PING мониторинга да е по-къс от този на времето на изпълнение макроса (или група от макроси). Тогава може да се генерира ново стартиране на макроса, докато още не е приключил предишното стартиране, и поведението ще зависи от настройките на самия макрос (Restart опцията му дали е включена или не).

На следващите две изображения са показани примерни настройки на Ping Monitor и Macros, с които да може да рестартираме Line1 за 15s при загуба на Ping за над 300s към адрес 1.2.3.4.

След това е показано и как да свържете нормално затворения контакт на реле от *NetControl* към захранването на рутера за да можете да го рестартирате.


Status	IP Settings	I/O Settings	Macros	Timers	PING Monitor	Automation	Misc
<b>Monitor Group No.1</b>							
					Enabled		
	IP address	1	2	3	4	<a href="#">IP Whois</a>	
	If no response within	300	s, start macros	Restart Router			
	Will start macros after	297	s (each ICMP ECHO reply reloads timer)				
	Limit consecutive restarts to	255	+1 (255=unlimited)				
	Ping data size	32	[32 to 1472] bytes				




### 3.7. Автоматични задачи (меню „Automation“)

Имате достъп до 8 отделни автоматични задачи, които най-общо Ви дават възможност да стартирате макроси (и да се изпрати SNMP Trap съобщение), при промяна на някой от аналоговите входове извън предварително зададени граници. Няма ограничение колко пъти даден вход или изход ще участва в автоматични задачи, но от потребителя зависи да не се получат взаимно изключващи се действия.

Value compare mode	Определя режима на сравнение на входната стойност. За повече информация вижте обясненията след таблицата.
Thresholds	Долен (LOW) и горен (HIGH) праг за функциите за сравняване на

	<p>входната величина. Стойностите, които се задават съответстват директно на дименсията на избрания 'Main sensor' канал (и на обхвата на измерваната от него величина)</p> <p> Въведените от потребителя стойности се преизчисляват спрямо разделителната способност на аналого-цифровият преобразувател и за това е възможно да бъдат коригирани автоматично до най-близката дискретна стойност.</p>
Main sensor	<p>Входен аналогов канал, чиято стойност ще се сравнява. Каналите се показват с техните имена и дименсията им.</p> <p>(от v5.59) В допълнение към аналоговите канали може да избирате и от Virtual IO каналите като източник на информация. Тези канали се „проверяват“ за Automation събития ПРИ ВСЯКА ПРОМЯНА НА СТОЙНОСТТА ИМ.</p>
Diff. sensor	<p>Втори аналогов канал при диференциален режим на работа. Реално се сравнява стойността на (Main – Diff. Sensor). Не може да се комбинира с Virtual IO канали</p> <p><b>Диференциалният режим се деактивира като се избере 'Not used' в това поле.</b></p>
On Event	<p>Кой макрос да бъде стартиран при удовлетворяване на зададения „Value compare mode” режим. ВИНАГИ се генерира и SNMP trap съобщение, като може да се избере и само това да остане единствената реакция.</p> <p>Разрешени за избор са CAMO макроси от 1 до 8 (включително)</p>
On Restore	<p>Тук е показан макроса, който ще се стартира при възстановяване на стойността при режим на работа Hysteresis(ACC).</p> <p>Макросите при възстановяване са от 9 до 16 (вкл.) и не могат да се избират от потребителя.</p>

Достъпни са следните режими на работа („Value compare mode„) по отношение на следенето на входната аналогова величина:

Disabled	Задачата е деактивирана
<LOW	Макросът 'On event' се стартира ЕДНОКРАТНО при спадане на измерваната величина под зададения долен праг (Low Threshold). Нищо не се случва при възстановяване, освен че се дава ново разрешение за стартиране на 'On Event'.
>HIGH	Макросът 'On event' се стартира ЕДНОКРАТНО при спадане на измерваната величина над зададения горен праг (High Threshold). Нищо не се случва при възстановяване, освен че се дава ново разрешение за стартиране на 'On Event'.
<LOW or >HIGH	Макросът 'On event' се стартира ЕДНОКРАТНО при надвишаване на зададения горен праг (High Threshold) или при спадане на измерваната величина под зададения долен праг (Low Threshold). Нищо не се случва при стойност в интервала [LOW; HIGH], освен че се дава ново разрешение за стартиране на 'On Event'.
Hysteresys (ACC)	Макросът 'On event' се стартира ЕДНОКРАТНО при надвишаване на зададения горен праг (High Threshold). При спадане на измерваната величина под зададения долен праг (Low Threshold) се стартира макросът 'On restore'. Нищо не се случва при стойност в интервала [LOW; HIGH]
Interval (INTRV) (от v 5.71)	<p>Макросът 'On event' се стартира ЕДНОКРАТНО при попадане на стойността в интервала [LOW; HIGH]. При излизане извън него се стартира ЕДНОКРАТНО макросът 'On restore'.</p> <p> Тъй-като този режим няма естествения хистерезис на предходния е заложен механизъм на времево филтриране на състоянието – “излизане” от интервала. Филтрирането е зависимо от настройката “MA filter points” за “Main Source”, така че да се гарантира, че събитията няма да се генерират по-често от на 1 секунда. При “по-бавни” настройки на входа – допълнителното филтриране се деактивира, тъй-като тогава филтърът гарантира по-ниската честота на събитията. Това филтриране не засяга събитията от попадане в интервала - те се генерират при първата попаднала стойност.</p>

Независимо от избрания режим на работа е необходимо входната величина да е имала стойност над/под зададените прагове за минимум времето на филтъра, който е зададен за аналоговия вход в менюто „**I/O Settings**”. Ако измерваната стойност се колебае около прага няма да се генерират събития докато тя трайно (поне за времето на филтъра) не удовлетвори неравенството.

Режимите „<LOW”, “>HIGH”, “<LOW or >HIGH” функционират по аналогичен начин. Изпълнението на неравенството и на филтъра на входа води до стартиране на макроса 'On Event'. Това става ЕДНОКРАТНО и неговото повторно стартиране е възможно само след като е имало неудовлетворяване на неравенството. Режимите са подходящи за ситуации, изискващи действие тип „аларма“.

Генерирането на SNMP trap съобщение в тези режими работи по следния начин: съобщение със стойността на входа се изпраща при първото удовлетворяване на неравенството и филтъра. Ако неравенството продължи трайно да бъде удовлетворено, няма да се изпращат нови съобщения. Ако в следващ момент стойността на аналоговия вход престане да удовлетворява неравенството

(дори и еднократно) се дава разрешение за ново изпращане на съобщението със стойността на входа (след като пак се удовлетвори неравенството и филтъра).

**Всичко до тук казано доказва, че изборът на стойност за филтъра на аналоговия вход много важна за получаване на оптимални резултати! Правилото е: Колкото по-голяма е стойността – толкова по-стабилна ще е работата на автоматичните алгоритми, но за сметка на бързодействието им.**

Режимът „**Hysteresys (ACC)**” работи на принципа стартиране на макрос ('On Event') при надвишаване на горния праг и стартиране на друг макрос ('On Restore') при преминаване под долния праг. Подходящ е за изходи в режим „Manual Output”. Това е практически най-често приложимият начин на работа за реализиране на:

- **терморегулатор с нагревател:** релеен изход се включва при спадане на температура под зададен праг и се изключва след достигане на зададена температура
- **терморегулация с вентилация** – аналогично на нагревателя, но с обратен статус на изходната верига (релето).
- **Управление на заряд на акумулатор** – включване на зарядната верига при напрежение на акумулатора под зададен праг (разреден) и изключване на заряда при достигане на 14.4V (зареден)

Тук SNMP Trap съобщение се изпраща еднократно при преминаване на стойността над прага HIGH за времето на филтъра. След това съобщение се генерира при спадане на стойността под прага LOW. В неутралната зона (LOW; HIGH) не се случва нищо.



*Във всеки SNMP trap се съдържа стойността на аналоговия вход (като 12bit цяло число) при която е било удовлетворено неравенството.*



*Да се има предвид, че SNMP traps се обработват през период от 2s, т.е. ако аналоговите филтри са с малки стойности може събитията да се генерират по-бързо, от колкото да се обработят и изпратят като SNMP trap. В такива случаи новите събития презаписват старите и се изпраща, това което последно е останало в момента на обработката на информацията.*



*За аналогови входове в режим „ContactSwitch(Alarm)”, освен SNMP trap, се генерира съобщение и в MQTT/SPC канала за да се предаде информация за промяната.*

*Automation блокове с Virtual IO като източник не генерират SNMP trap съобщения!*

Интересна комбинация се получава ако се използва този режим с изход в режим „Impulse Output” или макрос имитиращ същото - тогава изходът ще се възстанови (след като изтече времето на импулсния изход) дори и ако входната величина не спадне под „LOW”, а е в неутралната зона. Така ще се получи „защитно време“ и няма да се позволява на изхода да стои в зададения статус неограничено дълго време.

### 3.7.1 Режим на диференциално измерване

Много често в практиката се налага да се следи не стойността на един сензор (напр. за температура), а разликата между стойностите на два сензора. Такъв пример имаме при задачата за включване на циркулационната помпа в системите за топла вода със слънчеви колектори: помпата се активира само когато разликата между температурата на колекторите и тази в буфера/бойлера надвиши зададена стойност; помпата спира при доближаване на температурата на водата в бойлера до тази в колекторите.

Нека да видим как може да се настрои такъв режим на работа на следващото изображение:

- 1) Очевидно, решението за такъв случай е режим на работа HYST, който ще даде най-стабилна работа на помпата.
- 2) Избираме двата сензора за температура: 'Main Sensor' и 'Diff. sensor'  
**Устройството вече използва разликата 'Main-Diff', като база за изчисленията.**
- 3) Задаваме горен (5.2°) и долен (1.9°) праг на разликата (положителни стойности, като LOW<HIGH), като алгоритъмът на работа следва следните неравенства:  
Ако (Main-Diff) > HIGH → 'On Event' macros  
Ако (Main-Diff) <= LOW → 'On Restore' macros
- 4) Избираме предварително настроените макроси, които включват и изключват помпата.

#### Event Group No.8

Value compare mode

Thresholds LOW  HIGH

Main Sensor

Diff. Sensor (=main-diff)

On Event

On Restore

На следващата таблица е проследен процеса стъпка по-стъпка: в изходно състояние бойлера е 35°, панелите 37° – няма достатъчно температурна разлика за да се включи помпата. След като панела достигне 41° постигаме над 5.2° разлика – помпата включва. От този момент започва увеличаването на температурата на водата в бойлера. Помпата работи докато разликата не стане твърда малка при температура на бойлера 40° (разликата вече е <=1.9°).

Може да се зададе LOW=0° и тогава помпата ще работи докато Tbuffer не се изравни или надмине Tcollector (в конкретния пример не е възможно надминаване на температурата на солара, но в други ситуации е възможно). Тъй-като равенството на два сензора е практически трудно за постигане (поради шумове, неточности в измерването и т.н.) е по-добре да не се разчита на чистото равенство, а да се използва стойност LOW>0 (практически циркулацията при нищожна температурна разлика може да е безсмислена, поради малката печалба на топлинна енергия за сметка на ел. ток).

Main, °C	Diff, °C	Main-Diff	Действие
37	35	2	няма
40	35	5	няма
41	35	6 (> 5.2)	'On Event' (вкл. помпа)
41	36	5	няма
41	38	3	няма
41	40	1 (<1.9)	'On Restore' (изкл. помпа)



**В менютата няма ограничение да се избират само един тип диференциални сензори (температура, влажност и т.н.). Дименсиите на праговете следват тази на 'Main sensor', като диференциалното измерване ще функционира и при смесени сензори, но е необходимо ръчно да се преизчислят праговете спрямо другите типове сензори.**



Диференциалният режим може да се използва и в режимите LOW, HIGH и LOW/HIGH.

### 3.7.2 Фабрична настройка за генериране на събития от алармени входове към външните услуги (MQTT, SmartSpaceCloud)

Фабрично във всеки *NetControl* е конфигурирана показаната по-долу автоматична задача. Нейното предназначение е да предизвика генериране на събития към облачната платформа или MQTT при промяната на състоянието на алармения вход на устройствата. Тъй-като за него се използва един от аналоговите входове той генерира данни към платформата периодично, но без тази автоматична задача няма да изпраща веднага данни при промяна на състоянието.

Value compare mode

Thresholds LOW  HIGH

Main Sensor

Diff. Sensor (=main-diff)

On Event

On Restore

### 3.7.3 Стартиране на макроси от цифрови входове

В някои модели освен стандартните аналогови входове са налични и цифрови такива (тип „Alarm“). За да може промяна на цифров вход да доведе до стартиране на макрос е предвидена секцията „Macro start from event on digital inputs“. Тази секция се показва само ако устройството има цифрови входове!

**Macro start from event on digital inputs**

Alarm 9 -> 9. Macro09

Alarm 10 -> 10. Macro10

Alarm 11 -> 11. Macro11

Alarm 12 -> 12. Macro12

Alarm 13 -> 13. Macro13

Alarm 14 -> 14. Macro14

Alarm 15 -> 15. Macro15

Alarm 16 -> 16. Macro16

Alarm 17 -> 17. Macro17

Alarm 18 -> 18. Macro18

Alarm 19 -> 19. Macro19

Alarm 20 -> 20. Macro20

Обърнете внимание, че връзката цифров вход – номер на макрос е фиксирана (не може да се избират произволно макросите), като единствено може да я активирате или не. Имайте предвид и, че макроси от 9 до 16 могат да участват в Automation блоковете и трябва така да се планират, че да няма дублиране с цифровите входове.

Ако е необходимо да се промени нивото на входния сигнал, който ще стартира макроса, трябва да използвате опцията „Invert” в настройките на входа.

### 3.8. Рестартиране, обновяване на софтуера и др. (меню „Misc”)

#### 3.8.1 Потребители за Web достъпа

От тук можете да зададете Ваши собствени стойности на потребителското име и паролата. Изискването е те да са с дължина от 4 до 12 символа на **ЛАТИНИЦА!**

От v5.35 има възможност за дефиниране на администраторски потребител и на „IO User” с достъп единствено до началната страница със състоянието на входно-изходните вериги и макроси. Ако „IO User” е в режим „Action” (от менюто „IP Settings->IO User web account”) с него може да се изпращат команди към изходите на устройството или да се стартират макроси. В противен случай, той може единствено да вижда текущите състояния.

За превключване между потребителите, в долната и част на основната страница има предвиден линк „Logout”.

#### 3.8.2 Възстановяване на фабрични настройки

Имате възможност отделно да направите нулиране на настройките към фабричните такива за IP частта, за настройките на входно-изходите вериги и за имената на каналите. Възстановяването към фабрични настройки от бутона за входно-изходните вериги (IO Settings) нулира и всички настройки в Macros, Timers, Automation, Ping Monitor.

#### 3.8.3 Обновяване на системния софтуер по TFTP

Устройството е снабдено с TFTP клиент, който при подаване на команда от бутона „**Start Firmware Update via TFTP**” (или през SNMP) се свързва към IP адреса на TFTP сървър и изтегля (ако е наличен) необходимия му файл със обновление. След приключване на обновяването то се саморестартира.



*Силно препоръчително е обновяването на системния софтуер да не се прави в реални условия (големи мрежи, дистанционно захранване и т.н.). Пропадането на захранването в момента на обновление на системния софтуер ще доведе до повреда в устройството!*



*Връщането на **по-стара версия** (т.нар. downgrade) в повечето случаи ще изисква еднократно последващо **зареждане на фабричните настройки**. Това също означава, че процесът не трябва да се прави в реални условия (отдалечено).*

За коректно протичане на процеса на обновяване трябва да се премине през следните стъпки:

1. Инсталирайте програмата '3CServer' (свали от [ТУК](#)) за Windows. Може да се използват и други програми, включително и вградените в Linux TFTP демони.

2. Стартирайте програмата, пуснете с бутона „TFTP” сървъра. На статус лентата на програмата трябва да е изписано TFTP: On



време на обновлението може да забележите нарушаване на действието на различните процеси в устройството.

### 3.8.4 Обновяване на системния софтуер през [domo.ipnetcontrol.net](http://domo.ipnetcontrol.net)

Предвидена е възможност автоматично да бъдат обновени всички устройства, които са регистрирани в облачната платформа. Така няма нужда потребителят да се грижи да следи за публикувани нови версии (да инсталира TFTP сървър и т.н.) – те автоматично ще бъдат качени в свързаните устройства (за това е необходимо устройството Ви да е ONLINE в платформата).

При публикуване на нова версия на софтуера ще бъдете известени в платформата за това и ще можете да потвърдите обновяването.

### 3.8.5 Обновяване на системния софтуер през Web

Системният софтуер на *NetControl* може да бъде обновен и чрез upload на \*.bin файла през страницата Misc на вградения Web интерфейс.

След стартиране на качването на файла, изчакайте извеждане на съобщение за успешно приключване на процеса (няма статус в реално време).



По този начин НЕ може да се обновява софтуера на WiFi модула – при него е възможно само през TFTP.

### 3.8.6 Запазване и възстановяване на конфигурацията във/от файл

В менюто „Misc” имате достъп и до раздел „Configuration” с бутони „Backup” и „Restore”. С тях можете да съхраните във файл цялата текуща конфигурация на *NetControl* устройството – това обхваща абсолютно всички настройки – IP, IO, Names, Macros, Ping Monitor, Automation, Timers. Създаденият файл след това може да го заредите на други устройства и така да си спестите задаването на еднотипни параметри във всяко едно от тях.

### 3.8.7 “Events Log” - архив на последните IO събития

Status	IP Settings	I/O Settings	Macros	Timers	PING Monitor	Automation	Misc	
History of 100 events								
				Refresh				Purge
No.	Time	Object name	Value	Event source				
1	12 Jun 2023 09:35:14	Line 2	0	'Macro01'				
2	12 Jun 2023 09:35:12	Line 2	1	'Macro01'				
3	12 Jun 2023 09:35:12	Macro01	Start	Web				
4	12 Jun 2023 09:34:38	Pin Name 00002	1	Web				
5	12 Jun 2023 09:34:37	Pin Name 00001	1	Web				

От тук можете да проследите всички изходящи IO събития, стартиране на макроси и таймери. При сверен часовник (по SNTP) се изписва и дата/час на събитието (в противен случай ще се изписва 'n/a'). В полето „Event Source” се показва информация за източника на събитието; например за релеен изход – Web, SNMP, MQTT, SPC.

Буферът е за 100 събития. След напълването му, нови събития не се регистрират, но с бутона „Purge” може да ги изчистите и автоматично ще започне да се записва всичко новопостъпило.

Във v5.58 е добавена възможност и за друг режим на работа на буфера на EventLog - 'Circular Buffer' (активира се от менюто 'IO Settings->Miscellaneous parameters'). В този режим буферът винаги съдържа последните 50 събития (новите изтриват най-старите) и не е нужно да се изчиства от потребителя.

## 4. Достъп през SNMPv1 протокол

### 4.1. Достъп до I/O през SNMP

Както вече стана дума устройството поддържа достъп до всичките си параметри и функции през SNMP. В SNMP всеки обект се характеризира със специфична поредица от числа (OID) или символно име (само ако коректно са инсталирани MIB файловете към SNMP клиента).

В този раздел са описани всички обекти, които са директно свързани с управлението/достъпа до входно-изходните вериги. Всички останали обекти можете да намерите в раздел 9, където е изобразена цялата дървовидна структура на обектите, заложи в устройството.

#### 4.1.1 SNMP обекти за индивидуален достъп до входно-изходните вериги.

В MIB структурата на *NetControl* е налична групата обекти „iop1” ... “iop32”, която съответства на всички системно налични за ядрото входно-изходни вериги. Не всички от тях са изведени в конкретен модел на устройството, но обектите са налични независимо от това.

Във всеки един от тези обекти, чиито OID се формира като .1.3.6.1.4.1.19865.2.3.1.P., където [P] е номера на канала от 1 до 32, са налични няколко подобекта, с които може да се извлича/записва информация на всеки канал:

MIB име	Цифров OID	Описание
ioNum[P]	.1.3.6.1.4.1.19865.2.3.1.[P].1.0	Номер на канала [1, 32]
ioName[P]	.1.3.6.1.4.1.19865.2.3.1.[P].2.0	Име (само за четене!). Промяната става само през WEB интерфейса
ioMode[P]	.1.3.6.1.4.1.19865.2.3.1.[P].3.0	Режим (виж 7)
ioDefault[P]	.1.3.6.1.4.1.19865.2.3.1.[P].4.0	Начална стойност
ioImpulseFilter[P]	.1.3.6.1.4.1.19865.2.3.1.[P].5.0	Импулс/Филтър
ioValue[P]	.1.3.6.1.4.1.19865.2.3.1.[P].6.0	Стойност (без филтриране)
ioReadAll[P]	.1.3.6.1.4.1.19865.2.3.1.[P].7.0	Изчитане на всичко за канала в HEX (данните са разделени със запетая)
ioInvert[P]	.1.3.6.1.4.1.19865.2.3.1.[P].8.0	Инвертиране на състоянията
ioGauge[P]	.1.3.6.1.4.1.19865.2.3.1.[P].9.0	Стойност като 32 бит цяло число без знак. Въведено е заради броячите на импулси, но може да се ползва и за другите канали за да се по-добра универсалност. Обектът е само за четене (read-only)!
ioPulseCfg[P]	.1.3.6.1.4.1.19865.2.3.1.[P].10.0	Виж раздел
ioValueFiltered[P]	.1.3.6.1.4.1.19865.2.3.1.[P].11.0	Стойност след MA филтър (v5.39)

Параметрите съответстват на достъпните за конфигуриране и вече описани в предните раздели параметри от WEB менюто „I/O settings”.



Умишлено по нататък в примерите използваме само цифровите представяния на OID, защото те работят винаги, независимо дали сте инсталирали MIB файла! Разбира се, ако файлът е правилно зареден в SNMP клиента ще може да се използва и достъп направо до `ioValue9.0` – стойността на канал 9 (т.е. Line1).

В следващата таблица е примерна връзка между релейните канали и и индекса [P] в SNMP структурата. За всеки модел ще намерите конкретна таблица за него в разделът, който го описва.

Релеен канал	Номер [P]	Достъп ioValue[P]	Бележки
Line1	9	R/W	0 (Low) = изключено реле (NC веригата е ЗАТВОРЕНА)  1 (High) = включено реле (NC веригата е ОТВОРЕНА)
Line2	10	R/W	
Line3	11	R/W	
Line4	12	R/W	
Line5	13	R/W	
Line6	14	R/W	
Line7	15	R/W	
Line8	16	R/W	

Например, ако искаме състоянието на изход Line4 да бъде ON трябва да изпълним SNMP команда, която в обекта `ioValue` на канал номер 12 да запише ON=1:

```
> snmpset -v1 -c private 192.168.1.100 .1.3.6.1.4.1.19865.2.3.1.12.6.0 i 1
```

#### 4.1.2 Други (общи) SNMP обекти за достъп до входно-изходните вериги

Освен описана група обекти, които имат една и съща структура за всички налични канали, има още една група, която е разположена под клона „`ioMisc`“.

MIB име	Цифров OID
<code>iomReadAllOld</code> .1.3.6.1.4.1.19865.2.3.2.1.0	<b>ВАЖНО: Да не се използва в нови приложения. Запазено е с цел обратна съвместимост.</b> Изчита стойностите на всички входно-изходни вериги във формата на PicoP устройството (по-старите фърмуери за NetControl). <b>Няма достъп до всичките 32 обекта!</b> Форматът е: 'P3,P5,P6,P6.1,P6.2,P6.3,P6.4,P6.5,P6.6,P6.7,P6.8' Всички стойности са шестнадесетични числа, например: 0x40,0x80,0x00,0x0055,0x00BD,0x00AA,0x008D,0x005C,0x0045,0x003E,0x0049
<code>iomReadAllHex</code> .1.3.6.1.4.1.19865.2.3.2.2.0	<b>Да не се използва за изчитане на броячи на импулси, тъй-като те са 32битови!</b> Изчитане на всички канали (32), като резултатът е шестнадесетичен масив (Hex-STRING) с по два байта на канал (MSB first). Например:

	00 01 00 01 00 00 00 00 00 00 00 00 00 00 00 D8 00 14 00 06 00 38 00 39 00 41 03 FD 01 7C
iomSetAll .1.3.6.1.4.1.19865.2.3.2.3.0	Записът на 0/1 (Off/On) в този обект води до прилагане на това състояние към ВСИЧКИ изходни канали. Еквивалентно е на командите „All On”, „All Off” в WEB интерфейса.

#### 4.1.3 Изчитане на температурата (от датчик TDS300) през SNMP

Обектът за температура не връща директно стойността на температурата, а стойността на аналогово-цифровия преобразовател (това е валидно за всички аналогови входове).

За изчитане на температурния вход на серията *NetControl* трябва да се използва командата:

```
> snmpget -v1 -c public 192.168.1.100 1.3.6.1.4.1.19865.2.3.1.25.6.0
```

Получената от стойност, например „INTEGER: 217“ трябва да се конвертира в градуси (Целзии) по формулата:

$$t[C^{\circ}] = ( 3300*(SNMPValue/1023) - 500 ) / 10$$

#### 4.1.4 Изчитане на стойността за относителната влажност (от датчик HDS300) през SNMP

Сензорът за влажност използва същият вход, като този температура. За това командата за изчитане е същата както в раздел 4.1.3.

Получената от стойност се конвертира в RH% по формулата:

$$RH[\%] = 125*(SNMPValue/1023) - 6$$

#### 4.1.5 Вход за измерване на Unet (VIN), +Uin

Командата за изчитане на напрежението Unet е:

```
> snmpget -v1 -c public 192.168.1.100 1.3.6.1.4.1.19865.2.3.1.26.6.0
```

Отново получената стойност трябва да се преобразува до напрежение по формула, като тя зависи от типа на напрежението и вида на захранването:

- при променливотоково (AC) Unet напрежение и захранване за 12V с директна връзка (SMPS K0C6P с грец изправител на входа):

$$Unet [V_{AC_{RMS}}] = 3.3*(SNMPValue/1023)*37.25 + 0.8;$$

- при променливотоково (AC) Unet напрежение и захранване за 12V с галванично разделяне (SMPS iK0C8P с грец изправител на входа):

$$Unet [V_{AC_{RMS}}] = 3.3*(SNMPValue/1023)*37.25 + 0.4;$$

- за DC напрежение:

$$Unet [V_{DC}] = 3.3*(SNMPValue/1023)*49+0.4;$$

- за DC напрежение (0...62VDC) при 4RU1SH2S:

$$+Uin[V_{DC}] = 3.3*(SNMPValue/1023)*19.2927;$$

#### 4.1.6 Алармен вход

Статуса на този вход се получава с:

```
> snmpget -v1 -c public 192.168.1.100 1.3.6.1.4.1.19865.2.3.1.31.6.0
```

При „отворен“ контакт на алармения вход връщаната стойност е близка до максимума 1023 (може да е с до 10-15 единици по-малка).

При затворен контакт на алармения вход стойността спада под 10 единици.

#### 4.1.7 Вход измерване на DC ток чрез външен шунт (за 4RU1SH2S)

Командата за изчитане на напрежението върху шунта Ush е:

```
> snmpget -v1 -c public 192.168.1.100 1.3.6.1.4.1.19865.2.3.1.29.6.0
```

Получената от стойност се конвертира в амperi по формулата:

$$I_{acc}[Adc] = (SHmA/SHmV) * (3300 * SNMPValue / 1023) - 1650 / 22000,$$

където 'SHmA' е номиналният ток на шунта в милиамperi (например 20A => 20000mA), 'SHmV' е номиналният напреженовия пад върху шунта – 60 или 75mV.

#### 4.1.8 Вход за NTC температурен сензор

Получената стойност се преобразува в градуси по формулата:

$$T[°C] = (SNMPValue - 32768) / 100$$

При липса на сензор на даден вход се връща стойност 27768, което съответства на -50.00°C.

#### 4.1.9 Достъп до старите OID за достъп до I/O портовете

За обратна съвместимост в *NetControl* е запазен достъпът до обектите, които се поддържат от *PicoIP* (и по старата фамилия версии (4.xx) на *NetControl*). Не се препоръчва използването им при нови разработки!

Основният обект е PicoIP.PortCTRL (1.3.6.1.4.1.19865.1.2.X.X.0), който поддържа групов достъп и индивидуален достъп до каналите на устройството. Концепцията там обаче е различна - каналите са обединени в бит маски и три групи. За повече информация можете да се обърнете към MIB файла за PicoIP (достъпен е на <http://lan.neomontana-bg.com>)



Ако използвате старите обекти няма да можете да ползвате режимите „Impulse“ на изходите, както и опцията „Invert Output“.

## 4.2. Примерен PERL скрипт за изчисляване на температурата, Unet и алармения вход

Посоченият примерен скрипт на Perl използва обекта за изчитане в HEX на всички входно-изходни канали (необходимо е да имате инсталиран и пакета 'net-snmp'). Извличат се само необходимите за температура, напрежение и алармен вход, който след съответното конвертиране се изписват на конзолата през 1 секунда:

```

#!/usr/bin/perl
#####
# PERL script testing the NetControl measurement inputs
#
#
# Created by Yassen Angelov, Neomontana Electronics, 2014
# Feel free to copy and modify
#####

$host_ip = $ARGV[0];

if ($host_ip == "") {
    printf ("Usage: ./demo_netcontrol4.pl host_ip\n");
    printf ("Using default IP=192.168.1.100\n");
    #exit();
    $host_ip="192.168.1.100";
}

$community = "public";

printf("Host: %s\nTime      \tVIN      \tTemperature \tAlarm\n", $host_ip);
printf("=====");
while (1)
{
    # Retrieve all IO port values with single SNMP request (the iomReadAllHex.0 object)
    $all_ports=`snmpget -v1 -t 1 -r 1 -Oqv -c $community $host_ip .1.3.6.1.4.1.19865.2.3.2.2.0`;

    # Convert HEX string to array ($words[])containing two byte value of every channel
    my @hexs = split(' ', $all_ports);
    my @words = ();
    for ($k=0;$k< $#hexs;$k +=2) {
        #printf ("%d = %d.%d\n", $k/2, hex($hexs[$k]), hex($hexs[$k+1]) );
        $words[$k/2] = 256*hex($hexs[$k]) + hex($hexs[$k+1]);
    }

    # Get needed channels for voltage, temperature, alarm
    $snmpV = $words[25];
    $snmpT = $words[24];
    $snmpA = $words[30];

    # Convert ADC value to physical quantity
    $VINac=3.3*($snmpV/1023)*37.25 + 0.4;
    $VINdc=3.3*($snmpV/1023)*49 + 0.4;
    $Temperature=(3300*($snmpT/1023) - 500)/10.0;
    if ($snmpA > 0.75*1023) {
        $Alarm="Open";
    }
    else {
        $Alarm="Closed";
    }

    # Print line with date, values
    $tm = `date +%k:%M:%S`;
    chomp($tm);
    printf("%s ", $tm);

    printf("\t%5.1fVAC/%5.1fVdc[%d] \t%1fC [%d]\t%s[%d]\n", $VINac, $VINdc, $snmpV, $Temperature, $snmpT,
$Alarm, $snmpA);
    sleep(1);
}

>[uesr@host]$ ./demo_netcontrol4.pl
Usage: ./demo_netcontrol4.pl host_ip
Using default IP=192.168.1.100
Host: 192.168.1.100
Time      VIN      Temperature Alarm
=====
15:47:33   2.8VAC/ 3.6Vdc[20] 19.4C [215] Open[1021]
15:47:34   2.8VAC/ 3.6Vdc[20] 19.4C [215] Open[1021]

```

## 5. Управление през MQTT протокол

## 5.1. Принцип на работа на MQTT протокола

В протокола се използват т.нар. теми или с други думи обекти, които може да бъдат променяни или изчитани. Например в *NetControl* използваме обекта „NetControl/in/ch9” за промяна на състоянието на релеен канал Но. 1 в моделите с 2, 4 или 8 релета; „NetControl/out/ch9” се използва, когато състоянието на релето се е променило (например ако му се смени състоянието през WEB интерфейса или SNMP)

След свързване към сървъра, клиентът се абонира за обектите, към които има интерес и така указва на сървъра да му препраща всички съобщения, касаещи тези обекти. В *NetControl* това са всички налични релейни канали, за това при всяка връзка към сървъра се изпращат SUBSCRIBE съобщение за всички такива обекти. Други клиенти, свързани към сървъра изпращат PUBLISH съобщение до обект и сървърът го препраща към абонираните устройства – така може да се превключи релето на NetControl чрез подаване на команда към сървъра от друг клиент (скрипт, Domoticz, OpenHab или друг софтуер с възможност за комуникация по MQTT)


Самият *NetControl* изпраща PUBLISH съобщение при всяка промяна на състоянието на изходите, както и периодичното изпраща данни за сензорните входове.

Много достъпно обяснение на принципите на MQTT протокола, можете да намерите на следния линк:

<https://www.hivemq.com/blog/mqtt-essentials/>

## 5.2. Настройки за MQTT

От менюто 'IP Settings' е необходимо да изберете режим „MQTT Server”, да потвърдите избора с бутона 'Apply Settings' и след това да изберете линка 'Settings'

Server IP address	IP адрес или DNS име на MQTT сървъра
Server Port	TCP порт на сървъра, стандартният порт за MQTT е 1883. Могат да се задават и други портове над 1024.  <i>MQTT стандартът използва и порт 8883 за „secure” комуникация, която <b>НЕ</b> се поддържа от NetControl.</i>
User name User password	Име и парола за връзка към сървъра. Максимум 32 символа.
MQTT QoS	Задава нивото на QoS (Quality of Service) на комуникацията със сървъра. <b>Не се поддържа QoS2!</b> QoS0 - (Получаване на данните „най-много веднъж”) – комуникацията със сървъра не се потвърждава в рамките на MQTT протокола. Теоретично е възможна загуба на данни, но практически е малко вероятна поради преноса на данни по TCP. QoS1 – (Получаване на данните „най-малко веднъж”) - получаването на всеки PUBLISH пакет се потвърждава от отсрещната страна. Възможно е дублиране на съобщенията.
Clean Session / v5.86+ /	Този флаг информира брокера, че при установяване на връзка, всякакви запазени данни се игнорират (това включва и неизпратени съобщения)
Retain Flag in PUBLISH	При всяко публикуване на данни от NetControl към брокера, може да се „вдигне“ този флаг, който указва на сървъра да запомни последното състояние на обекта. Други клиенти, свързвайки се със

	сървъра и абонирайки се за данни от въпросният обект, ще получат последното му състояние автоматично от сървъра.
PUBLISH value format	Поддържат се два формата: JSON и RAW.
Mirror /in events	Активира препращане на всички обработени входящи MQTT команди (към „/in“) към изходящите обекти.
Mirror to	Потребителят може да избере къде да се препратят командите: към стандартния „/out“ или към „/mrout“ (от v5.66).
Topic prefix	Определя префикса (първата част) от името на MQTT обектите. Използва се разграничаване на отделните контролери при връзка към един и същ брокер.
KeepAlive Period	Задава времето в секунди между изпращането на специални Keep Alive съобщение в MQTT връзката. Използват се за мониторинг на връзката. Възможно е да се зададе и стойност 0 (деактивиране на този механизъм, което е допустимо в MQTT протокола), но това е възможно да предизвика странични ефекти в TCP протокола и той да разпадне връзка при липса на друга предавана информация.
Inputs auto-send period	Всичко входове на NetControl (сензори, аларма, напреженов, ток и т.н.) могат с този параметър да се настройат колко често да изпращат информация за текущата си стойност към MQTT сървъра. Може да се деактивира тази функция със стойност 0. Това периодично изпращане на данни може да замени механизма на Keep-Alive. Бутонът „Send now“ позволява ръчно изпращане на данните от сензорите, което е удобно за диагностика.



В настройките на MQTT брокера препоръчваме да се използва опцията „max\_inflight\_messages=1“ – налична е в брокера Mosquitto. Тя гарантира, че към контролера ще се изпращат съобщенията едно по едно (MQTT протокола позволява в един фрейм да има няколко PUBLISH съобщения, но NetControl не поддържа този вариант и обработва само първото съобщение). Това има ефект върху съобщенията, които брокера е запазил като непотвърдени (особено при QoS=1) и те се подават към NetControl при установяването на нова връзка.

### 5.3. Поддържани обекти

Всички команди КЪМ NetControl се подават към следния обект:

**NetControl/subgroup/in/**

*NetControl* прави SUBSCRIBE към „NetControl/subgroup/in/#“ при всяко установяване на връзка с брокера.

Изходящи от *NetControl* събития (данни от сензори, променено състояние на реле през Web или SNMP) генерират PUBLISH към обект:

**NetControl/subgroup/out/**

,а при активирана опцията за копиране на входните събития се използва и публикуване към обект:

**NetControl/subgroup/mrout/**

### 5.3.1 JSON формат на данните, които публикува NetControl

Изходящи от *NetControl* събития се публикуват към посочените в предния раздел обекти, като се добавя номера на канала, например:

**NetControl/subgroup/out/chXX**

където:

'**chXX**' е канала на *NetControl*, където **XX** е номерът му (1, 2...32) и отговаря на номерата на каналите [P] в описанието за връзка между SNMP и номера на канала. „Virtual IO” каналите се намират на 'ch33' до 'ch40'.

При RAW формат, данните са аналогични на тези при достъп през SNMP и описанието в разделите за SNMP важи и тук (изходите връщат 0 или 1, аналоговите/сензорни входове стойност 0..1023).

Доста по-удобен и съдържащ повече информация е JSON форматът на данни, най-вече поради по-добрата съвместимост с външни клиенти за автоматизация ([Node-RED](#), [Domoticz](#), [OpenHab](#) и др.). Например данните от алармен вход изглеждат така:

```
{
  "device": "MyNetControl",
  "name": "Channel X",
  "value": { "real": "OPEN", "raw": 1 },
  "channel": 32,
  "type": 38,
  "ts": 1734092367,
  "source": "auto",
  "st": 6
}
```

, където:

„**device**” е името на устройството Host name, което сте въвели в менюто „I/O Settings”

„**name**” е името на канала (въведен от менюто „I/O Settings”)

„**value**” е стойността на канала, има я в два варианта: *real* и *raw*. Предимството на `real` е, че отговаря на зададения от потребителя сензор (TDS300, HDS300 и т.н.) и е градуси, проценти и т.н. Това позволява директно да се ползва стойността, без да се преобразува допълнително. `raw` съдържа първичната числова стойност като число (напр. стойност на АЦП).

„**channel**” е номера на канала (реално дублира номера от обекта за достъп)

„**type**” е типа на канала (TDS300, HDS300 и т.н.). Списък на типовете на каналите ще намерите в раздел 7

„**source**” показва източника на данни: 'auto' е когато данните са в следствие на периодичното изпращане на данни за сензорите; 'event' е когато данните са в следствие на външна команда (например при релейните изходи) или 'Macro'.

„**ts**” (от v5.66) съдържа TIMESTAMP на времето, в което събитието е постъпило в буферите на устройството (може да се разминава с времето на изпращане на събитието, ако е имало прекъсване в мрежовата връзка към брокера). Необходимо е да имате коректно настроен SNTP сървър за сверяване на софтуерния часовник (в противен случай в това поле ще има 0)

„**st**” (от v5.66) съдържа код, описващ кой е източника на събитието (както в Event Log). Списък с кодовете ще намерите в раздел 8.

### 5.3.2 Формат на данните, подавани към NetControl

При подаване на команди към *NetControl* се работи единствено с данни в RAW формат – данните са цяло число, като 0=изключено, 1=включено (поддържат се и текстовите варианти ON/OFF, true/false, start/stop без оглед на малки/главни букви).

Например (примерите използват клиент [mosquitto](#), който е достъпен за Linux, Windows, MAC):

Включи реле на канал 9 (Line 1):

```
> mosquitto_pub -h 192.168.1.102 -t 'NetControl/subgroup/in/ch9' -m 1
```

Изключи реле на канал 9 (Line 1):

```
> mosquitto_pub -h 192.168.1.102 -t 'NetControl/subgroup/in/ch9' -m 0
```

С подобна команда може да се стартира или спре макрос:

```
> mosquitto_pub -h 192.168.1.102 -t 'NetControl/subgroup/in/macro1' -m 1
```

, като валидните стойности са 1 или START и 0 или STOP.

### 5.3.3 LWT обект

*NetControl* използва още един обект (Will Topic), който е само изходящ за устройството:

**NetControl/subgroup/out/status**

При свързване към сървъра винаги се изпраща PUBLISH към този обект със стойност „online”, а сървърът генерира PUBLISH към същия обект със стойност „offline” при загуба на връзката с устройството. Този механизъм Ви позволява да следите дали устройството е свързано или не към сървъра. Подробно обяснение на функционирането на този механизъм може да прочетете на следния линк:

<https://www.hivemq.com/blog/mqtt-essentials-part-9-last-will-and-testament>

### 5.3.4 Други поддържани обекти

От v5.86 се поддържа следният обект (може да се запише 0,1,on,off,true,false):

**NetControl/subgroup/in/cfg\_http**

PUBLISH към този обект позволява временно активиране/деактивиране на Web сървъра на *NetControl*. След рестарт винаги се взема конфигурационната стойност от „IP Settings -> HTTP service“.

Идеята на тази функция е при контролери, които работят изцяло с MQTT канал, да се забрани глобално достъпа през HTTP с цел сигурност (след направата на първоначалните му настройки): „IP Settings -> HTTP service=Disable“. Но в случаи на необходимост от промяна в настройките на контролера да може през наличния MQTT канал да се разреши временно достъпа и след това да се забрани отново.

От v5.94 е добавен обект:

**NetControl/subgroup/in/cfg\_ts**

PUBLISH (задължително без „Retain“ флаг!!!) към този обект с UNIX TIMESTAMP (32bit цяло число, напр. 1775647843) позволява сверяване на софтуерния (и хардуерния, ако е наличен) часовеник за реално време.

Очаква се стойност за времето по UTC (както идва по SNTP протокола), като след това вътрешно се корегира със зададената стойност от „Timers->Timezone offset“.

Сверяването по MQTT и това по SNTP могат да работят едновременно, като при SNTP то става с периодични заявки от контролера, а при MQTT само по изрична заявка (PUBLISH).



**ВАЖНО!!!** Никога не публикувайте към тази тема с вдигнат „Retain“ флаг в клиента! Това ще запази в брокера последната стойност и при нов свързване по MQTT, брокерът автоматично ще му я изпрати и тя няма да отговаря на текущото време!!!

## 6. WiFi модул

Някои модели са снабдени с допълнителен WiFi модул на 2.4GHz, работещ по стандартите [802.11 b/g/n](#). За по-добро ниво на сигнала е използвана външна (3dBi) антена на RP-SMA конектор.

Устройството може да работи в даден момент само с един от комуникационните си интерфейси: Ethernet или WiFi. По-подразбиране устройството е в режим на активиране на WiFi при загуба на Ethernet връзката (физическа загуба на връзка – т.е. изключен кабел). Мрежовите настройки от „IP Settings” са общи за двата режима на връзка.

WiFi и Ethernet използват един и същ MAC адрес. За това, при превключване между WiFi/Ethernet е възможно връзката до устройството да не са появи веднага, поради прехвърлянето на MAC адреса на устройството между различни портове на суичтове/рутери.

### 6.1.1 Настройки на WiFi в WEB интерфейса

За осъществяване на WiFi свързаност е необходимо само задаване на SSID и SecurityKey (останалите параметри, като режим на сигурност и др. се избират автоматично).

Първата настройка е в менюто „IP Settings” - „WiFi Enable Mode”. Възможните режими са два „When Ethernet Down” (активиране на WiFi при липса на физическа връзка на Ethernet порта; по подразбиране) и „Disabled” (изцяло деактивиран WiFi).

Status	I/O Settings	IP Settings	PING Monitor	Automation	Misc
<b>IP configuration</b>					
Software Version	5.11				
MAC address	ECF2360040BE			<a href="#">Ethernet Settings</a>	
WiFi enable mode	When Ethernet down			<a href="#">WiFi Settings</a>	
IP address	192	. 168	. 1	. 100	

От линка „WiFi Settings” се отваря страницата със статус и настройки за WiFi интерфейса:

Status	I/O Settings	IP Settings	PING Monitor	Automation	Misc
<b>WiFi status</b>					
WiFi Active Yes					
AP MAC 00:0C:20:01:41:1E					
Auth mode WPA2_PSK					
AP WiFi mode b/g/n					
Radio Channel 6					
RSSI -42 dBm					
Software version 1.1					
<b>WiFi station parameters</b>					
SSID <input type="text" value="wifi_ssid"/>					
Security key <input type="password" value="*****"/>					
AP MAC address <input type="text" value="FF:FF:FF:FF:FF:FF"/>					
<small>(use <a href="#">FF:FF:FF:FF:FF:FF</a> to disable AP MAC lock)</small>					
<input type="button" value="Save parameters"/>					

WiFi Active	Показва дали WiFi интерфейса е активният в момента. Когато е активен, в следващите полета се зарежда информация за връзката. Може да се наложи да се презареди страницата, ако не са заредени данните.
AP MAC	MAC адресът на точката за достъп, към която е свързано устройството.
Auth mode	Текущ режим на сигурност на връзката (Open, WEP, WPA_PSK, WPA2_PSK, WPA_WPA2_PSK)
AP WiFi mode	Поддържани режими на комуникация/скорост от точката за достъп. Избира се режимът с най-високи параметри.
Radio Channel	Радио канал, на който е осъществена връзката
RSSI	Индикатор за силата на сигнала (по-голямо стойност -> по-силен сигнал)
Software version	Версия на софтуера на WiFi модула

В групата „WiFi station parameters” трябва да настроите необходимите параметри за осъществяване на връзката:

SSID	Име на безжичната мрежа, към която искате да се свържете. Фабричната стойност на това поле е: <b>wifi_ssid</b>
Security key	Парола (ключ) за свързване към тази мрежа. (звездичките не отговарят на реалния брой символи на паролата) Ако желаете да смените само някои от другите параметри, не попълвайте нищо в това поле и ще се запази текущата стойност на паролата. Фабричната стойност на това поле е: <b>wifi_secret</b>
AP MAC address	Задаването на стойност, различна от FF:FF:FF:FF:FF:FF, води до разрешаване на свързване само към точка за достъп със зададения MAC адрес (и съответното SSID).



Режимът 802.1Q (VLAN) не работи в режим WiFi. Използването на тази настройка при WiFi ще доведе до загуба на връзката до устройството.



WiFi модульт поддържа обновяване на фърмуера му по TFTP (в менюто „Misc” има бутон „Start Firmware Update of WiFi module via TFTP”). Файлът с ъпдейта трябва да се намира в главната директория на TFTP сървъра и е с име „rpfw5\_wifi.bin”. За повече информация относно обновяване по TFTP вижте раздел 3.8.3. По време на започнал процес на TFTP ъпдейт на WiFi модула се блокира превключването между WiFi и Ethernet – процесът на ъпдейт трябва да започне и завърши на един и същ комуникационен канал.

## 7. ПРИЛОЖЕНИЕ I Тип на канала 'type' в MQTT JSON данните; в ioModeXX.0 при SNMP и в ioreg.js масива 'PM' ( в HEX)

Номер	Тип/описание
0	Изход Manual
1	Изход Toggle
2	Изход Impulse
16	Изход фазов регулатор
17	Вход фазов регулатор (ZC)
18	Вход брояч импулси
19	Аналогов изход 0..100%
20	Температурен сензор NTC
32	Voltage (0-3.3Vdc)
33	Температура TDS300
34	Температура LM35Z
35	Voltage (0-33Vdc)
36	Voltage (0-110Vac)
37	Voltage (0-160Vdc)
38	Сух контакт (Alarm) или VDS300, WDS300
39	Външен 75(60)mV шунт
40	Влажност HDS300
41	Voltage (0-62Vdc)
42	User Defined 1 (виж 3.3.3)
43	User Defined 2 (виж 3.3.3)
44	Voltage (0-10Vdc)
45	Voltage (0-22Vdc)
	<i>'Virtual IO' канали</i>
256	Регистър с общо предназначение
257	-
258	Цена на ел. енергия
259	Температура (NTC)

## 8. ПРИЛОЖЕНИЕ II Списък на кодовете за източник на събитието (“st” в MQTT)

WEB	0
MACROS	1
SNMP	2
MQTT	3
SPC	4
AUTOMATION	5
SYSTEM	6
PINGMON	7
TIMER	8
MODBUS	9
WIEGAND	10
MODBUS_MASTER	11
ELECTRICITY PRICE	12

## 9. ПРИЛОЖЕНИЕ III Бързо ръководство за работа с SNMP. Списък с наличните в *NetControl* обекти

SNMP протокола дефинира отделни обекти във всяко устройство, които могат да се изчитат или записват според типа им. Тези обекти имат т.нар. OID – (object id), който ги характеризира еднозначно. Въпросните обекти се описват на специален синтаксис в текстов файл (MIB файл), който позволява вместо трудните за запомняне цифрови еквиваленти на OID-овете да се ползват имена.

OID-овете представляват дървовидна структура от типа .1.2.3.4.5..... и така се формира уникален номер за всеки обект. Тази структура е описани в съответния MIB файл. Неомонтана Електроникс има регистриран „клон“ в тази структура, който е **1.3.6.1.4.1.19865**.

За достъп до параметрите на *NetControl* се използват командите `snmpget` и `snmpset`. Синтаксисът е аналогичен:

```
>snmpget -v1 -c <парола read-only> <IP> <OID>
>snmpset -v1 -c <парола read-write> <IP> <OID> <тип данни> <стойност>
```

Командата `snmpset` изисква точното указване на типа данни, които ще се подадат на съответния OID. Допустимите типове са:

*i*: INTEGER, *u*: unsigned INTEGER, *t*: TIMETICKS, *a*: IPADDRESS  
*o*: OBJID, *s*: STRING, *x*: HEX STRING, *d*: DECIMAL STRING, *b*: BITS  
*U*: unsigned int64, *I*: signed int64, *F*: float, *D*: double

За изчитане на IP адреса се използва:

```
> snmpget -v1 -c public 192.168.1.100 netIP.0
```

При липса на MIB файл или недобре конфигуриран SNMP клиент горната команда няма да сработи и ще даде грешка. В такъв случай или трябва да се изчисти проблема около MIB файла или да се използва цифровия еквивалент (този вариант е универсален и ще работи винаги при всякакви SNMP клиенти):

```
>snmpget -v1 -c public 192.168.1.100 .1.3.6.1.4.1.19865.2.2.1.0
```

В „превод“ цифровият еквивалент означава:

(1.3.6.1.4.1.19865)	.2	.2	.1	.0
Neomontana	.NetControl	.network	.netIP	.0

Други примерни команди:

- изчитане на състоянието на изход „Line1”  
 > snmpget -v1 -c public 192.168.1.100 ioValue9.0  
 или  
 > snmpget -v1 -c public 192.168.1.100 .1.3.6.1.4.1.19865.2.3.1.9.6.0
- задаване на нивото на изход „Line2”  
 > snmpset -v1 -c private 192.168.1.100 ioValue10.0 i 1  
 или  
 > snmpset -v1 -c private 192.168.1.100 .1.3.6.1.4.1.19865.2.3.1.10.6.0 i 1
- задаване на нов IP адрес  
 > snmpset -v1 -c private 192.168.1.100 netIP.0 a 192.168.1.145
- рестартиране: snmpget -v1 -c public 192.168.1.100 .1.3.6.1.4.1.19865.2.1.3.0

По долу е поместени резултата от командата 'snmptranslate', която съставя дървовидна структура с имената и номерата на обектите и подобектите. От нея лесно може да се извлече цифровият еквивалент на всеки обект като се премине по разклоненията на дървото. От дървото добре се вижда и типа данни които ще изисква при запис всеки обект, както и дали е само за четене или за четене/запис.

Повтарящите се групи `ior2...ior31`, `ipMon2...ipMon7`, `auto2...auto7` се скрити за да се съкрати списъка, но достъпът до тях е налице.

