Технически изисквания
към система за предварителен подбор на изпълнители
№ С-14-НМ-Д-123, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

Техническа спецификация:

I. Technical requirements, regarding the Head End System

1. Description

1.1 Functional description:

All data, collected until 00:00 a.m., must be received by the grid operator not later than 12:00 a.m. on the next calendar day.

Reading of the load profile must be possible, by setting periods – multiple times within a day. Any and all data, collected by 00:00 a.m. are stored, and in all future reading requests, only the values, which have not been read previously, are to be read.

The invoicing data readings and the logbooks are not subject to the requirement for daily reading and therefore the grid operator can plan an individual reading as well as various fixed reading requests.

For reading modes the grid operator allows both reading methods: PUSH (initialized by the meter) and PULL (initialized by the central system)

For this purpose a time schedule is to be established and configured, for individual reading of the PUSH /data transmission/ and PULL / data reception/ modes.

In the PUSH mode, it should be possible to configure the time schedule for reading in the electricity meter.

In the PULL mode, the reading schedule is controlled by the Head End System. The reading schedule must specify the precise time of reading of each of the electricity meters.

1.2 Initiator:

For reading the electricity meters; according to the reading schedule

For configuration of the reading schedule:

The grid operator needs the data and for that purpose he determines the time schedule (if necessary the schedule is transferred to subordinate levels in the hierarchy).

1.3 Result:

For the reading of the electricity meters:

The grid operator has received all requested data.

For configuration:

A reading schedule is preset in the necessary system components.

1.4 Service level:

When starting the reading of the values, at 00:05 a.m., 98 % of all electricity meters must be read within 12 hours.

2. Ad hoc- reading

2.1. Name: Spontaneous reading of the electricity meters or Immediate reading of electricity meters

2.2. Function description: The purpose is to obtain up-to-date electricity metering data upon the request by authorized participants (following the rules and provisions for data protection). This request is sent by the grid operator to the respective electricity meter in the form of a reading command. The scope of data may be defined (e.g. logbooks, invoicing data, load portfile data)

In case the ad hoc-reading has been completed unsuccessfully several times, an on-site reading should be

I. Технически изисквания към Система за дистанционно отчитане

1. Описание

1.1 Функционално описание:

Всички данни, които са събрани до 00:00 ч., трябва да са при мрежовия оператор най-късно до 12:00 ч. на следващия календарен ден.

Товаровият профил трябва да може да се отчита посредством задаване на периоди - многократно в рамките на деня. Всички събирани до 00:00 ч. се съхраняват, при следващи заявки за отчитане това трябва да се отчетат само липсващи стойности.

Отчитанията на данните за фактуриране и дневниците не подлежат на изискването за ежедневно отчитане и затова мрежовият оператор може да планира индивидуално отчитане а така също и различни фиксирани заявки за отчитане.

За режим на отчитане възложителят допуска методи на отчитане: PUSH (инициализирано от електромера) и PULL (инициализирано от централната система).

За целта е необходимо да се определи респективно да се конфигурира времеви график за отчитане поотделно за режимите PUSH /предаване на данни/ и PULL /приемане на данни/.

При режим PUSH времевият график за отчитане трябва да може да се конфигурира в електромера.

При режим PULL графикът за отчитане се управлява от централната система. В графика за отчитане трябва да е определено кои електромери кога трябва да се отчетат.

1.2 Инициатор:

За отчитането на електромери: съгласно графика за отчитане

За конфигуриране на графика за отчитане:

Мрежовият оператор се нуждаеот данните и за целта определя времеви график (при необходимост графикът се пренасочва към подчинени йерархични нива).

1.3 Резултат:

За отчитането на електромери:

Мрежовият оператор е получил всички изискани данни

За конфигуриране:

В необходимите системни компоненти е заложен график за отчитане.

1.4 Ниво на поддръжка:

При стартиране на отчитането на стойностите към 00:05 ч. в рамките на около 12 часа трябва да са отчетени 98 % от всички електромери

2. Ad hoc- отчитане

2.1. Наименование:Спонтанно отчитане на електромери или Незабавно отчитане на електромери

2.2. Описание на функцията: Целта е получаване на актуални електромерни данни при запитване от страна на оторизирани участници (спазване на правата и на разпоредбите за защита на данните). Това запитване мрежовият оператор изпраща на съответния електромер под формата на команда за отчитане. Обхватът на данните може да се дефинира (напр. дневници, данни за фактуриране, данни за товаров профил).

В случай, че ad hoc-отчитането многократно е завършило без успех, следва да има възможност за

available.
The following applies to the combined methods:
2.3. Initiator:
a) Change of client (differentiation when invoicing)

b) If the planned periodic reading (multiple) has been unsuccessful
c) Client complaints (inspection of authenticity)

d) Maintaining the security of operation of the network
e) During installation
2.4. Result:
The required electricity meter data is received at the Head End System.
2.5. Service level:
In 99 % of the cases <= 5 min.

3. On-Site Reading
3.1. Name:
On-Site Reading
3.2. Function description:
In general there must be an opportunity for reading the electricity meter on-site by means of a mobile terminal through the maintenance interface P0. In order to meet the strict provisions, regarding the data protection, an individual key/password is to be entered in the mobile terminal, which enables the reading of the respective electricity meter.
The data obtained in this manner, should be transferrable to the Head End System. Each reading must be incorporated in the access protocol.
The requirements in the area of security must be met.

3.3. Initiator:
- unsuccessful planning reading
- (De-)installation

3.4. Result:
The data is read and can be sent to the Head End System.
3.5. Sevice level:
In 99% of the cases.
4. Deactivation
For the deactivation, no group, or mass command (broadcast) must be used.

4.1 In case of client change
4.1.1 Name:
Power supply interruption, due to the fact, that the client leaves the real estate, which becomes uninhabited
4.1.2 Function description
The purpose is, the power supply of a certain site or facility, to be disconnected remotely (from the Head End System of the grid operator), because the property remains uninhabited. The deactivation takes place by opening the switch /Breaker/, situated in the electricity meter.
The Head End System of the grid operator sends to the respective electricity meter a command for deactivation. The intelligent electricity meter fulfills the command and sends a status back to the Head End System. This status must be clearly shown on the display of the electricity meter (e.g. OFF).

4.1.3 Initiator:
Erasing of an existing client
4.1.4 Result:
The power supply has been disconnected and the status "disconnected" is displayed on the electricity meter and in

отчитане на място.

2.3. Инициатор:
a) Смяна на клиент (разграничаване при фактуриране)
b) Когато планираното периодично отчитане (многократно) е било неуспешно
c) Рекламация от клиента (проверка на верността)
d) Поддържане на сигурността на експлоатацията на мрежата
e) По време на монтаж
2.4. Резултат:
Необходимите електромерни данни са получени в централната системата.
2.5. Ниво на поддръжка:
В 99 % от случаите <= 5 мин.

3. Отчитане на място
3.1. Наименование:
Отчитане на място
3.2. Описание на функцията:
Принципно трябва да има възможност за отчитане на електромера на място посредством мобилен терминал през интерфейса за поддръжка P0. За да бъдат спазени строгите разпоредби относно защитата на данните, в мобилния терминал трябва да се въведе индивидуален ключ/ парола, който дава право да се отчете съответния електромер. Така получените данни трябва да могат да се предадат на централната система. Всяко отчитане трябва да се отбелязва в протокола за достъп.
Трябва да се спазват изискванията в областта на сигурността.
3.3. Инициатор:
- неуспешно планирано отчитане
- (Де-)монтаж

3.4. Резултат:
Данните са отчетени и могат да се изпратят до централната системата.
3.5. Ниво на поддръжка:
В 99 % от случаите
4. Изключване
За изключванията не трябва да се използва групова респ. масова команда (Broadcast).

4.1. При смяна на клиент
4.1.1. Наименование:
Прекъсване поради това, че клиентът напуска имота, без да се нанесе нов клиент
4.1.2. Описание на функцията:
Целта е, електрозахранването на даден обект да бъде изключено дистанционно (от централната системата на мрежовия оператор), тъй като в обекта не се нанася друг клиент. Изключването се извършва чрез отваряне на прекъсвача /Breaker/, намиращ се в електромера.
Централната система на мрежовия оператор изпраща до желания електромер команда за изключване.
Интелигентният електромер изпълнява подадената от централната системата команда и изпраща обратно към централната системата статус. Този статус трябва също така да бъде ясно изобразен на дисплея на електромера (напр. OFF).
4.1.3 Инициатор:
Отписване на съществуващ клиент
4.1.4 Резултат:
Електрозахранването е прекъснато и статусът "прекъснат" е визуализиран на електромера и в

the Head End System.
4.1.5 Service level:
In 99 % of the cases<= 15 min
4.2 Payment-related disconnection

4.2.1 Name:
Disconnection within the payment collection process

4.2.2 Function description:
The grid operator may disconnect the facilities of clients with overdue payments.
The Head End System sends to the respective electricity meter a deactivation command. The electricity meter executes the respective command (the internal switch interrupts the power supply to the client facility) and sends back to the Head End System the relevant information, regarding the disconnection status. This status must be clearly shown on the display of the electricity meter.

After disconnection, there is no option for immediate reconnection on-site by the client.
4.2.3 Initiator:
The client fails to make a payment.
4.2.4 Result:
The switch in the electricity meter has disconnected the facility, visualized that on the display and has sent a message to the Head End System. The electricity meter IS NOT ready for immediate on-site reconnection.

4.2.5 Service level:
In 99 % of the cases<= 15 min.

4.3 On-site through the servicing interface
4.3.1. Name:
Deactivation on-site through the servicing interface (P0)

4.3.2 Function description:
The electricity meter is switched of on-site by means of a mobile terminal through the servicing interface. In order to meet the strict provisions, regarding data protection, an individual key/password must be entered in the mobile terminal, enabling the disconnection of the respective electricity meter. Therefore, it should not be possible to deactivate several or all electricity meters by means of a single key. The key control must correspond to the security concept.

4.3.3 Initiator:
Working on the maintenance/ servicing of the client facility
Disconnection, related to the collection of payments
4.3.4 Result:
The switch in the electricity meter has disconnected the facility, visualized that on the display and has sent a message about the changed status to the Head End System
4.3.5 Service level:
Immediately, upon sending a command by the mobile terminal
5. Switching on
5.1 Connection-related with payment

5.1.1 Name:
On-site switching on
5.1.2 Function description:
The electricity meter receives from the Head End System or through the maintenance interface, a command, activating

централната системата.
4.1.5 Ниво на поддръжка:
В 99 % от случаите <= 15 мин
4.2 Прекъсване по причини, свързани с плащания
4.2.1 Наименование:
Прекъсване в рамките на процеса по събиране на плащания
4.2.2 Описание на функцията:
Мрежовият оператор може да изключи съоръженията на клиенти с просрочени задължения.
Централната системата изпраща до съответния електромер команда за изключване. Електромерът изпълнява подадената от централната системата команда (вътрешният прекъсвач изключва електрозахранването на клиентското съоръжение) и изпраща обратно до централната системата информация за статуса на изключването. Този статус трябва да бъде ясно изобразен на дисплея на електромера.
След прекъсване няма възможност за незабавно повторно включване на място от страна на клиента.
4.2.3 Инициатор:
Клиентът не извършва заплащане.
4.2.4 Резултат:
Прекъсвачът на електромера е изключил съоръжението, визуализирал е това на дисплея и е изпратил съобщение до централната системата.
Електромерът НЕ е готов за незабавно повторно включване на място.
4.2.5 Ниво на поддръжка:
В 99 % от случаите <= 15 мин.

4.3 На място през интерфейса за обслужване
4.3.1. Наименование:
Изключване на място през интерфейса за обслужване (P0)
4.3.2 Описание на функцията:
Електромерът се изключва на място посредством мобилен терминал чрез интерфейса за обслужване. За да бъдат спазени строгите разпоредби относно защитата на данните, в мобилния терминал трябва да се въведе индивидуален ключ/ парола, който дава право да се изключи съответния електромер. Следователно не трябва да е възможно изключване на няколко или на всички електромери от електромерното стопанство посредством един ключ. Управлението на ключовете трябва да съответства на концепцията за сигурност.
4.3.3 Инициатор:
Работи по поддръжка/ обслужване в клиентското съоръжение
Прекъсване свързано със събиране на плащания
4.3.4 Резултат:
Прекъсвачът на електромера е изключил съоръжението, визуализирал е това на дисплея и променениият статус е отразен в централната системата.
4.3.5 Ниво на поддръжка:
Веднага, при подаване на командата от мобилния терминал
5. Включване
5.1 Включване по причини, свързани с плащания
5.1.1 Наименование:
Включване на място
5.1.2 Описание на функцията:
Електромерът получава от централната системата или чрез интерфейса за поддръжка, команда, активираща

(again) the on-site switching on. The switching on takes place in the following manner:
5.1.2.1 From the Head End System or through the maintenance interface an activation command is sent to the electricity meter. The electricity meter visualizes that status on the display. This status is reported to the Head End System.
5.1.3 Initiator:
5.1.3.1 The client enters into possession in a facility with interrupted power supply and wants it to be reactivated.
5.1.3.2 The outstanding debts have been paid.
5.1.4 Result:
The electricity meter is activated and this is visualized on the display. The status of the electricity can be shown in the Head End System.
5.1.5 Service level:
In 99 % of the cases<= 15 min. for activation
6. Date and time synchronization
6.1 Name:
Ensuring accurate system time for all end-devices

6.2 Function description:
Checking the actual time.
Behaviour in case of deviation in the time settings.
If the respective deviation is up to 2 seconds, no actions are required.
If the deviation is between 2 and 9 seconds, the time must be synchronized, no entry is made in the event logbook.
If the deviation exceeds 9 seconds, the time must be set and an entry in the event logbook must be made, as well as in the load profile if it is configured (displaying the date and time and an entry for the status).

The chronology ("numeration") of the metering activities must be stored.
The synchronization is performed from the Head End System through a WAN-interface. It must be possible to carry that out on-site through the servicing interface. The synchronization cycle must be capable of parameterization.
6.3 Initiator:
Parameterization cycle (Schedule)
6.4 Result:
The system time of all the end-devices is the same.

6.5 Service level:
99,9 % of the end devices have proper system time.

7. Firmware Download
7.1 Part, not subject to metrological inspection

7.1.1 Name:
Update of the firmware of a part, NOT subject to metrological inspection
7.1.2 Function description:
As with the electricity meter, the Head End System must support updates and, respectively, upgrades of a part, NOT subject to metrological inspection (the non-metrological part). Upon issuing a command, given by the grid operator, the updated software is loaded to the electricity meter. After loading, the electricity meter checks if the software has been fully downloaded and without any errors. After that the installation starts in the electricity meter. After the software is installed, the electricity meter must perform a self-check, which ensures the flawless functioning of the new software. Failing that, the previous version of the software will be restored automatically. The electricity meter

(повторно) включване на място. Включването протича по следния начин:
5.1.2.1 От централната системата или чрез интерфейса за поддръжка се изпраща команда за включване на електромера. Електромерът визуализира това състояние на дисплея. Това състояние се съобщава в централната системата.
5.1.3 Инициатор:
5.1.3.1 Клиентът се нанася в обект с прекъснато съоръжение и желае то да бъде активирано.
5.1.3.2 Отворените задължения са заплатени.
5.1.4 Резултат:
Електромерът е включен и това е визуализирано на дисплея. Статусът на електромера може да се види също и в централната системата.
5.1.5 Ниво на поддръжка:
В 99 % от случаите <= 15 мин. за активиране
6. Синхронизиране на дата и час
6.1 Наименование:
Осигуряване на точно системно време на всички крайни устройства
6.2 Описание на функцията:
Проверява се актуалното време.
Поведение при отклонения в часа.
Ако констатираното отклонение е до 2 секунди, не трябва да се предприемат действия.
Ако отклонението е между 2 и 9 секунди, времето трябва да се синхронизира, не се предприема вписване в дневника на събитията.
Ако отклонението е по-голямо от 9 секунди, времето трябва да се определи и да се предприеме вписване в дневника на събитията и в товаровия профил ако е конфигуриран (показание с дата и час и вписване за статуса).
Трябва да се запази хронологията ("номерацията") на измервателните стойности.
Синхронизирането се извършва от централната системата през WAN-интерфейс. Трябва да е възможно да се извърши също и на място чрез интерфейс за сервизно обслужване. Цикълът на синхронизиране трябва да може да се параметрира.
6.3 Инициатор:
Параметриран цикъл (Schedule)
6.4 Резултат:
Системното време на всички крайни устройства е еднакво.
6.5 Ниво на поддръжка:
99,9 % от крайните устройства имат правилно системно време.
7. Firmware Download
7.1 Част, Неподлежаща на метрологична проверка
7.1.1 Наименование:
Актуализация на фърмуера на НЕподлежащата на метрологична проверка част
7.1.2 Описание на функцията:
Както електромерът, така също и централната система трябва да поддържат ъпдейт респ. ъпгрейт на НЕподлежащата на метрологична проверка част (неметрологичната част). По команда, дадена от мрежовия оператор, актуализираният софтуер се зарежда в електромера. След зареждане, електромерът проверява дали софтуерът е прехвърлен изцяло и без грешки. След това стартира инсталирането в електромера. След като софтуерът бъде инсталиран в електромера трябва да се извърши самопроверка, която гарантира безпроблемното функциониране на

sends to the Head End System an error message, indicating the failing attempt in the event logbook.

The previous version is restored automatically, when the electricity meter fails to establish contact with the Head End System within 72 hours.
An entry in the event logbook must also be made in case of successfully installed software.

7.1.3 Initiator:
The electricity meter manufacturer provides a new firmware for the part, NOT subject to metrological inspection. Using a Head End System the grid operator sends through the concentrator, an update to the electricity meter.
7.1.4 Result:
The firmware in the electricity meter has been successfully updated. The electricity meter communicates that to the Head End System and makes an entry in its logbook.
7.1.5 Service level:
99 % of all affected electricity meters within 30 days.

8. Sending an ALARM signal
8.1 Name:
sending an ALARM
8.2 Function description:
The electricity meters, data concentrator, may be exposed to tampering attempts, damages and technical issues. The alarms are events, defined by the grid operator. They must be sent spontaneously by the electricity meter to the Head End System. The alarm always results in certain actions (direct or indirect).

8.3 Initiator:
A decentralized system component (electricity meter, Data Concentrator) identifies an event, configured as an alarm. Then the system component generates a clear alarm message and sends it independently and directly to the Head End System.

8.4 Result:
The Head End System receives a clear alarm message and displays it to the grid operator in the respective form.
8.5 Service level:
99 % within 6 hours.

9. EVENTS /events/
9.1 Name:
EVENT creation and transfer
9.2 Function description:
Unlike alarms, the events must be reported in an appropriate form by the respective system components, but these are not transmitted immediately to the Head End System. The Events are used to ensure the quality and are specified by the grid operator.

The components create clear event messages (event type; moment of occurrence and duration; moment of transmission ,…), they record them in the events memory, /in the event logbook and transfer them to the Head End System during the periodic reading of the electricity meters or upon request.

9.3 Initiator:
A decentralized system component (electricity meter, Data Concentrator) finds an occurrence, defined as an event.

новия софтуер. Ако не е така, предходната версия на софтуера трябва да се върне автоматично.
Електромерът изпраща до централната система съобщение за грешка и отбелязва неуспешния опит в дневника на събитията.
Предишната версия се връща автоматично също и тогава, когато електромерът не успее да се свърже с централната система в рамките на 72 часа.
Вписване в дневника на събитията трябва да се направи също и при успешно инсталиране на софтуера.
7.1.3 Инициатор:
Производителят на електромера предоставя нов фърмуер за НЕподлежащата на метрологична проверка част. Чрез централна система мрежовият оператор изпраща през концентратора ъпдейт към електромера.
7.1.4 Резултат:
Фърмуерът в електромера е успешно актуализиран. Електромерът съобщава това на централната системата и прави вписване в дневника на събитията си.
7.1.5 Ниво на поддръжка:
99 % от всички засегнати електромери в рамките на 30 дни.
8. Изпращане на АЛАРМА
8.1 Наименование:
изпращане на АЛАРМА
8.2 Описание на функцията:
Електромерите, Концентраторите на данни, могат да са изложени на опити за манипулация, повреди и технически проблеми. Алармите са събития, дефинирани от мрежовия оператор. Те трябва да се изпращат спонтанно от електромера към централната система. Алармата задължително води след себе си действие респ. намеса (индиректна или директна).
8.3 Инициатор:
Децентрална системна компонента (електромер, концентратор на данни) открива събитие, конфигурирано като аларма. След това системната компонента генерира еднозначно съобщение за аларма и го изпраща независимо и директно до централната система.
8.4 Резултат:
Централната система получава еднозначното съобщение за аларма и го показва на мрежовия оператор в съответната форма.
8.5 Ниво на поддръжка:
99% в рамките на 6 часа

9. СЪБИТИЯ / events /
9.1 Наименование:
Създаване и пренасяне на СЪБИТИЯ
9.2 Описание на функцията:
За разлика от алармите, събитията трябва да бъдат протоколирани в подходяща форма от съответните системни компоненти, но не се предават незабавно към централната система. Събитията служат за гарантиране на качеството и се специфицират от мрежовия оператор.
Компонентите създават еднозначни съобщения за събитие (вид на събитието; момент на поява и продължителност; момент на предаване ,…), записват ги в паметта, предназначена за събития, / в дневника на събитията и ги прехвърлят към централната система по време на периодичното отчитане на електромерите или при поискване.
9.3 Инициатор:
Децентрална системна компонента (електромер,

Then the system component generates a clear message of an event, records it and sends it to the Head End System during the respective reading.

9.4 Result:
The Head End System receives a clear message about the event and displays it to the grid operator in the respective form.
9.5 Service level:
99 % within 6 hours
Any additional functionality which is not defined in the current requirements must be defined in the offer.

Definition for Alarms and Events

Event	Alarm> spontaneous message	Event-> In the readout dadata set	logbook / Event memory record
Terminal cover opening	Option: Yes	Yes	Yes
Meter main cover opening	Option: Yes	Yes	Yes
Voltage interruptions (all 3 phases) U <5%	-		Time and duration
Phase failure detection U <5%		Yes	Yes
access Log			Yes
Unauthorized access attempt	Option: Yes	-	Yes
Critical Error (FF)	Option: Yes	-	Yes
External magnetic field detection > 400 mT	Option: Yes	-	Yes
Current limit exceeded (per phase)	-	Yes	Yes
Overload	-	-	Yes
Disconnected device; Detected current flow	-	-	Yes
Last accepted command	-	-	Yes

концентратор на данни) открива случка, дефинирана като събитие. След това системната компонента генерира еднозначно съобщение за събитие, записва го и го изпраща към централната система по време на съответното отчитане.
9.4 Резултат:
Централната система получава еднозначното съобщение за събитие го показва на мрежовия оператор в съответната форма.
9.5 Ниво на поддръжка:
99 % в рамките на 6 часа
Всяка допълнителна функционалност, която не е дефинирана в настоящите изисквания следва да бъде описана в офертата
Определяне на Аларми и Събития

Събитие	Аларма-> спонтанно съобщение	Събитие-> по време на отчтитане	logbook / запис в паметта на събитията
Отваряне на клемна капачка	Опция: Да	Да	Да
Отваряне на основната капачка на електромера	Опция: Да	Да	Да
Отпадане на напрежение (всички 3 фази) U <5%	-		Време и продължителност
Отпадане на фазно напрежение U <5%		Да	Да
Осъществен достъп			Да
Опит за неоторизиран достъп	Опция: Да	-	Да
Критична грешка (FF)	Опция: Да	-	Да
Разпознаванена външно магнитно поле > 400 mT	Опция: Да	-	Да
Превишен лимит по ток (пофазно)	-	Да	Да
Претоварване	-	-	Да
Прекъснато устройство; Наличие на ток	-	-	Да
Последна приета команда	-	-	Да

II. System Requirements

1. Communication

1.1 Data transfer requirements

The system must support the following simultaneous processes:

1. Sending consumption data
2. Automation of the client processes (e.g.

II. Изисквания към системата

1. Комуникация

1.1 Изисквания към преноса на данни

Системата трябва да се поддържат паралелно следните процеси:

1. Изпращане на данни за потреблението
2. Автоматизиране на клиентски процеси (напр.

disconnection and reconnection of the power-supply)
3. Automatic logging and identification of the end-devices
4. Online commuting commands
5. Remote configuration of system components

6. Spontaneous alarm transfer
7. Transfer of events and operational data upon request
8. Control of remote Firmwaredownload (from Data Concentrator), by means of the network of a mobile operator, end-devices,…)
9. For the various applications in system, the following priorities must be set:
9.1 The configurations of the system components must take place successfully within 5 minutes.

9.2 The performance of mass readings within the legally established timeframe must be guaranteed.

9.3 Not later than 24 hours after their installation (usually 15 minutes later) the end devices must be automatically registered in the Head End System.

9.4 In case of remote Firmwaredownload it must be ensured that the new firmware will be rolled out to all system components within 30 days.It must be ensured that all of the above applications may work in parallel and be processed according to the current priorities.

Detailed requirements regarding:
1.1.1. Remote reading of consumption data
The entire system must be dimensioned in such a manner that is met in all modes of operation. More specifically, the following is required:

1.1.1.1 Daily reading of all daily consumption values (all registeres for active energy in both directions) not later than 12:00 a.m. (the reading starts at 0:05 a.m.)

1.1.1.2 Additional daily reading every 15 minutes of load profiles for electricity meter readings (active energy in both directions) of electricity meters,

1.1.1.2.1 which are required for billing purposes,
1.1.1.2.2 which are required for the operation of the network;
1.1.1.2.3 which are required for statistical purposes.
100 % transmission of the load profiles of all electricity meters is to be ensured. Within the aforesaid timeframe, 99 % of all the necessary data must be transmitted.

1.1.2. Client processes: Disconnection, reconnection and cash collection
The Client processes for disconnection and reconnection of the power-supply of client facilities (activation of the circuit breakers in the electricity meters), must take place successfully within 5 minutes and be confirmed in the Head End System (at least 99 % of all commands).

1.1.3. Registration and identification of end-devices
First of all, in the installation of electricity meters, but also in the replacement for metrological inspection, covering a vast territory, it must be possible to employ automatic

прекъсване и възстановяване на захранването)
3. Автоматично регистриране и идентифициране на крайни устройства
4. Online-команди за комутиране
5. Дистанционно конфигуриране на системни компоненти
6. Спонтанен пренос на аларми
7. Пренос на събития и оперативни данни при поискване
8. Управление на отдалечен Firmwaredownload (от концентратор на данни), посредством мрежата на мобилния оператор, крайни устройства,…)
9. За различните приложения в системата трябва да се зададат следните приоритети:
9.1. Конфигурациите на системните компоненти трябва да се извършат успешно в рамките на 5 минути.
9.2. Трябва да е гарантирано извършването на масови отчитания в рамките на законово определените срокове.
9.3. Най-късно 24 часа след инсталирането им (обикновено след 15 минути) крайните устройства трябва автоматично да се регистрират в централната система.
9.4. При отдалечен Firmwaredownload трябва да се гарантира, че новия фърмуер в рамките на 30 дни ще бъде зареден във всички системни компоненти. Трябва да се гарантира, че всички от гореспоменатите приложения ще работят едновременно и ще бъдат обработвани по приоритет.
Детайлни изисквания към:
1.1.1. Дистанционно отчитане на данни за потреблението
Цялата система следва да се оразмери така, че да бъдат изпълнени при всички режими на работа. По-специално се изисква:
1.1.1.1 Ежедневно отчитане на всички дневни стойности на потреблението (всички регистри за активна енергия в двете посоки) най-късно до 12:00 ч. (начало на отчитането в 0:05 ч.)
1.1.1.2 Допълнително ежедневно отчитане на всеки 15 минути на товарови профили за електромерни показания (активна енергия в двете посоки) на електромери,
1.1.1.2.1които са необходими за фактурирането,
1.1.1.2.2които са необходими за експлоатацията на мрежата,
1.1.1.2.3които са необходими за статистически цели.
Трябва да се гарантира пренасяне на 100 % от товаровите профили на всички електромери. В рамките на горепосочения времеви интервал следва да се пренесат 98 % от необходимите данни.
1.1.2. Клиентски процеси: Прекъсване, възстановяване и инкасо
Клиентските процеси за прекъсване и възстановяване на клиентски съоръжения (задействане на прекъсвачите в електромерите), трябва да се извършат успешно в рамките на 5 минути и да се потвърдят в централната система (най-малко 98 % от всички команди).
1.1.3. Регистриране и идентифициране на крайни устройства
Преди всичко при монтаж на електромери, но също така и при подмяна за метрологична проверка, обхващаща голяма територия, трябва да е възможно автоматичното идентифициране и регистриране в системата на минимум 1 000 крайни устройства дневно. Крайните устройства по принцип трябва да се

identification and registration in the system of at least 1 000 end-devices per day. The end devices have to register at the Head End System within 15 minutes. It must be guaranteed that the maximum time for registration shall be 24 hours (for at least 99% of the end devices).

When transferring low-voltage lines (e.g. to another transformer station/ Data Concentrator) all the affected electricity meters must be automatically disconnected from the already inaccessible Data Concentrator within 24 hours and register with a new Data Concentrator (at least 99% of all affected electricity
meters).

1.1.4. Remote configuration of system components

This remote configuration must be completed successfully within 5 minutes and confirmed in the Head End System. The system must be so dimensioned that 3% of all end-devices can be configured every month (at least 99% within the specified timeframe).

1.1.5. Transfer of alarms, events and messages

The meters alarms must be transferred to the data concentrator, so as not to be overwritten by subsequent alarms/events, but this time should not be greater than 6 hours. The frequency of alarms transmission from the data concentrators to the central system must be possible to be set by the network operator (requirement: minimum 5% of all the terminal devices per month).

The events and messages must be capable of spontaneous reading (individual reading). The operating modes must also be subject to remote reading. This transmission must take place successfully within 5 minutes (minimum 10% of all end-devices per month, 99 % within the specified time).

In case of mass readings, a maximum period of reading of 24 hours must be observed (at least 99% of all end-devices must be read within the specified time). E.g. the following data must be read from time to time, in the form of mass reading:

1.1.5.1. Power-supply interruptions
1.1.5.2. Error log
1.1.5.3. Access protocol
1.1.5.4. Logbooks for all end-devices

In order to maintain the operating control, as well as for the purposes of planning the development of the grid, for 99,9% of all infrastructure elements by 7:00 a.m. every day data of the communication status must be submitted and recorded in the Head End System in 15 minute intervals.

1.1.6. Remote Firmwaredownload

The proposed system must enable the remote change of the firmware of all the system components. This Remote Firmwaredownload must be completed successfully within 30 days, which means that in the Head End System feedback, regarding the successful update of the firmware must have been received (requirement: minimum 99 % of all affected system components).

1.1.7. Additional system requirements

1.1.7.1 At least once a day the system must check the system time. In case of deviations > 9 seconds, the system

регистрират в централната система в рамките на 15 минути. Трябва да се гарантира, че максималното време за регистрация е 24 часа (за най-малко 99% от крайните устройства).

При прехвърляне на изводи НН (напр. към друг трафопост/концентратор на данни) всички засегнати електромери трябва в рамките на 24 часа автоматично да се изключат от вече недостъпния концентратор на данни и да се регистрират в новия концентратор на данни (най-малко 99% от всички засегнати електромери).

1.1.4. Дистанционно конфигуриране на системни компоненти

Дистанционното конфигуриране трябва да е успешно извършено в рамките на 5 минути и да бъде потвърдено в централната система. Системата трябва да е така оразмерена, че месечно да могат да бъдат преконфигурирани 3% от всички крайни устройства (най-малко 99% в рамките на зададеното време).

1.1.5. Пренос на аларми, събития и съобщения

Алармите от електромерите трябва да бъдат пренесени до концетратора, така че да не бъдат презаписани от последващи аларми/събития, но това времетраене не трябва да бъде по-голямо от 6 часа. Честотата на преноса на аларми и данни от концентраторите до централната система трябва да може да се настройва от мрежовия оператор (изискване: минимум 5% от всички крайни устройства месечно)

Събитията и съобщенията трябва да могат да бъдат спонтанно отчетени (индивидуално отчитане). Режимите на работа също трябва да могат да бъдат отчетени дистанционно. Този пренос трябва да бъде успешно извършен в рамките на 5 минути (минимум 10% от всички крайни устройства месечно, 99 % в рамките на зададеното време).

При масови отчитания трябва да се спазва максимално време за отчитане от 24 часа (най-малко 99% от всички крайни устройства трябва да бъдат отчетени в рамките на зададеното време). Напр. следните данни трябва да бъдат отчитани периодично под формата на масово отчитане:

1.1.5.1 Прекъсвания на напрежението
1.1.5.2 Регистър на грешките
1.1.5.3 Протокол за достъп
1.1.5.4 Дневници за всички крайни устройства

С цел поддържане на оперативното управление, както и на планирането на развитието на мрежата, за 99,9% от всички инфраструктурни елементи трябва до 7:00 всеки ден да се предават и записват в централната система данни за комуникационния статус през интервал от 15 минути.

1.1.6. Отдалечен Firmwaredownload

Предложената система трябва да предоставя възможност за дистанционно променяне на фърмуера на всички системни компоненти. Този отдалечен Firmwaredownload трябва да приключи успешно в рамките на 30 дни, това означава, че в централната система трябва да е получена обратна информация за успешната актуализация на фърмуера (изискване: минимум 99 % от всички засегнати системни компоненти).

1.1.7. Допълнителни изисквания към системата

1.1.7.1 Системата трябва поне веднъж на ден да проверява системното време. Ако има отклонения > 9

must set the time. Any and all processes of time setting must be registered in the logbook and transmitted to the Head End System.

1.1.7.2 The PLC-communication, must be protected, against the neighboring systems, so that in the operation of the neighboring systems it would be guaranteed that the above data will be transmitted to the requested availability.
1.1.7.3 For the PLC communication the possibility for changing the carrying frequency for communication or another fixed frequency must be declared, conforming to the available frequency for the modulation of the existing system and sufficiently different from the available system so that the communication sessions of the separate systems do not affect each other, so that the operation of two systems in a single grid is ensured.
1.1.7.4 The bandwidths of the system components must be dimensioned so that the additional requirements are met, in accordance with the security concept:

1.1.7.4.1Encryption and authorization
1.1.7.4.2Necessary changes to the keys (e.g. Session-Keys) according to the level of the equipment.
1.1.7.4.3Changes in the symmetrical keys of the interfaces at the electricity meter (in accordance with the level of equipment, always in case of change of residence
1.1.8. Quantities
When hierarchic systems are concerned - Head End System - Data Concentrator- end-devices (electricity meters), the dimensioning of the entire system must take place, based on the following quantities/ numbers:

Depending on the size of the grid operator:

i. At least 10 000 data concentrators to the Head End System.
ii. At least 1 000 electricity meters per data concentrator

1.1.9. Requirements, regarding the monitoring of the availability and time for execution the processes
The execution time (the time between the assignment of the order by the legacy systems and the transmission of a positive feedback to the legacy system of each separate command must be measured and recorded in the Head End System. The results from that monitoring must be presented on the interface for presentation of information (Webservice).

1.1.10. Special requirements when using hierarchic systems
Communication link between the Head End System and the data concentrator
The requested reaction and availability times throughout the system must be strictly observed also when using systems with Data Concentrator. The communication links of the Data Concentrator must be dimensioned so that all the reaction times are observed and the required availability is achieved.

In order to be able to discover the reason for errors in case of failure to observe the required values in the entire system, the availability of the separate connections for data transfer between the electricity metering portals and the Head End System must be metered and recorded, by means of functions for grid control and it must be made available

секунди, системата трябва да настрои времето. Всички процеси за настройване на времето трябва да се впишат в дневника и да се предадат към централната система.
1.1.7.2 PLC-комуникацията трябва да е защитена срещу съседните й системи, така че при експлоатация на съседните системи да бъде гарантирано, че горепосочените данни ще бъдат пренесени с изисканата разполагаемост.
1.1.7.3 При PLC комуникация следва да се декларира възможността за промяна на носещата честота за комуникация или друга фиксирана честота съобразена с наличната честота за модулация на съществуваща система и отстояща от честота на наличната система така че комуникационните сесии на отделните системи да не влияят една на друга, за да се гарантира работа на две системи в една мрежа.
1.1.7.4 Широчините на честотните ленти на системните компоненти трябва да са така оразмерени, че да гарантират изпълнението на допълнително необходимите изисквания съгл. концепцията за сигурност:
1.1.7.4.1 Кодиране и оторизация
1.1.7.4.2 Необходими промени на ключовете (напр. Session-Keys) според техническото ниво.
1.1.7.4.3 Промяна на симетричните ключове на интерфейсите при електромера (в съответствие с нивото на техниката, винаги при смяна на жилище)

1.1.8. Количества
Когато се касае за йерархични системи - централна система - Концентратор на данни- крайни устройства (електромери), оразмеряването на цялата система трябва да се извърши въз основа на следните количества/ бройки:
В зависимост от това, колко голям е мрежовият оператор:
i. Най-малко 10 000 концентратори към централната система.
ii. Най-малко 1 000 електромери към един Концентратор на данни
1.1.9. Изисквания към мониторинга на разполагаемостта и на времената за изпълнение на процесите
Времето за изпълнение (времето между възлагането на поръчката от водещите системи и предаването на положителна обратна информация до водещата система, на всяка отделна команда трябва да се измери и запише в централната система. Резултатите от този мониторинг трябва да се извеждат на интерфейс за предоставяне на информация (Webservice).
1.1.10. Специални изисквания при използване на йерархични системи
Комуникационна връзка между централната система и Концентратор на данни
Изисканите времена на реакция и разполагаемости в цялата система трябва да бъдат спазени и когато се използват системи с концентратор на данни.
Комуникационната свързаност на концентратор на данните трябва да е така оразмерена, че да се спазват времената за реакция и да е гарантирана изисканата разполагаемост.
За да може да бъде открита причината за грешка в случай на неспазване на изисканите стойности в цялата система, разполагаемостта на отделните връзки за пренос на данни между електромерните портали и

through the information provision interface (Webservice).

When using public grids (e.g. ADSL, GPRS) the offer of the Head End System must specify the level of services, provided by the public providers, which is necessary for achieving the total availability.

When using landline communication connections (e.g. cables, optical cables), owned by the grid operator, the system components, specified by the grid operator must be allowed and – if necessary –requirements are to be defined, to be applicable to the provision of the total availability.

Furthermore the mass methods, which are to be applied to this evidence, must be specified.
Note: The requirements, regarding planning, construction, commissioning and operation of telecommunication grids do not form part of this tender procedure.
Communication connections between the data concentrator and the end devices
1.1.11. PLC
The PLC-system must be dimensioned so that with the aforesaid end-devices per one data concentrator and with simultaneous maximum data transfers, the required availability and certain reaction are observed. Particular attention is to be paid to the outlines for transformer stations with a total length of up to 1,5 km., as well as lines with up to 5 transfers from overhead line to another overhead line, consisting of several conductors with equal potentials or to a cable in a tube. The PLC system must be resistant to false signals, so that, despite the temporary reverse effects on the grid by the client facilities, the required availability and the specified reaction times are observed.

In case of interferences from electric appliances at the client facilities, it is necessary to ensure appropriate filters for reducing such interferences.

1.2. Events and alarms
The integration in the Head End Systems for the control of alarms and events must be possible.
The respective event must be characterized by at least the following information:
a. Clear identification of the origin
b. Type of the event and information in clearly presented text
c. Date/time of the event
d. Time of transfer /of the central registration (if applicable)
e. Event/Error category e.g
  i. Informative
  ii. Critical error: not removed,
  iii. it is possible that other devices are also affected by that error,
  iv. The error has not been ultimately validated.
All the readings of the electricity meters and events of all the system levels must be recorded in protocols and time-stamped (both for the original time of occurrence and the actual duration of the event). The time-stamp must always be combined with the report command and the information on the event.
The events/alarms must be recorded in all the decentralized components (electricity meters, circuit breakers, gates) as

централната система трябва да се измери и запише посредством функционалност за управление на мрежата и да се предостави на разположение чрез интерфейс за предоставяне на информация (Webservice).
При използване на обществени мрежи (напр. ADSL, GPRS) оферента на централната система трябва да посочи нивото на обслужване от страна на обществените провайдъри, което е необходимо за постигане на общата разполагаемост.
При използване на линейни комуникационни връзки (напр. кабели, оптична връзка), които са собственост на мрежовия оператор, трябва да се разрешат зададените от мрежовия оператор системни компоненти и при необходимост да се дефинират изисквания, които са необходими за изпълнение на общата разполагаемост.
Освен това следва са се посочат масовите методи, с които трябва да се приложи това доказателство.
Забележка: Изискванията към планирането, изграждането, въвеждането в експлоатация и експлоатацията на телекомуникационни мрежи не са част от настоящата тръжна процедура.
Комуникационни връзки между Концентратор на данни и крайните устройства
1.1.11. PLC
PLC-системата трябва да е оразмерена така, че с по-горе упоменатия брой крайни устройства за един онцентратор на данни при едновременни, максимални трансфери на данни да бъдат спазени необходимата разполагаемост и определените времена за реакция По специално трябва да бъдат разглеждани изводи на трафопостове с дължина до 1,5 км., както и линии с до 5 прехода от въздушна линия към друга въздушна линия, състояща се от няколко проводника с еднакъв потенциал, или към кабел в една тръба. Системата PLC трябва да е устойчива срещу погрешни сигнали, така че въпреки временни обратни въздействия върху мрежата от страна на клиентски съоръжения, да се спазят необходимата разполагаемост и определените времена за реакция.
В случай на смущения от електрически уреди в клиентски съоръжения е необходимо да бъдат осигурени подходящи филтри за намаляване на тези смущения.
1.2 Събития и аларми
Интеграцията в централни системи за управление на аларми и събития трябва да е възможна.
Дадено събитие трябва да се характеризира поне със следната информация:
a. Еднозначна идентификация на произхода
b. Тип на събитието респективно информация в ясно формулиран текст
c. Дата/Час на събитието
d. Час на прехвърлянето/на централното регистриране (ако е приложимо)
e. Събитие/Категория на грешката например:
  i. Информативна
  ii. Критична грешка: не премахната,
  iii. възможно е и други уреди да бъдат засегнати от тази грешка,
  iv. Грешката не е окончателно валидирана.
Всички отчитания на електромери и събития на всички системни нива трябва да се протоколират и да им се добавят времеви печати (както за час така и за продължителност на събитието). Времевият печат трябва винаги да се комбинира с командата за отчет и с

well as in the centralized system for a period of time, variable and specified for the respective Alarms and Events Group, as the minimum number of entries to be stored is 100.

Error analysis and optimization

1.2.1. Information, regarding the events and the alarms

In order to process the critical situations, it is necessary that the centralized system is capable of interpreting events and alarms as well as to generate filters in order to prepare reports. The contents of such reports must be accessible for the users or to be stored in a recommended file format (e.g. *.csv, .txt, .xls …).

1.2.2. Configuration for the processing of events and alarms

The centralized system must document each and every event/alarm received, as for this purpose, it is possible that the relevant rules are freely selected (e.g. only to file protocols, create tickets etc.) doing that, a temporary link between events/alarms is to be established

1.2.3. Report on the assets and the checked events and alarms

The centralized system must provide functionality for retrieving information regarding the active events and alarms and the history of various events/alarms.

There must be a capability for the events/ alarms to be sorted by different criteria, such as time roles, event/alarm type, electricity meter, electricity meter groups, etc. The centralized system must offer functionality for manual and automatic erasing of events/alarms.

1.2.4. Configuration of filters for various events/alarms

In order to determine which events/alarms must be referred to the centralized system, it should be possible to configure different filters.

It must be possible to make configurations for a single electricity meter, for a group of electricity meters as well as for all electricity meters.

These capabilities must also be available for the Data Concentrator.

The objective of the filter is to protect the centralized system against "overloading" through events/alarms.

The contractor must detail in the specification the filters, which can be defined.

The following reports must be provided for as a minimum:

a. Automatically, according to the specified calendar schedule, reports are to be generated on the communication devices, lacking data or having no connection.

b. Automatically, according to the specified calendar schedule for reading, reports are to be generated for the end devices, which lack data.

c. Automatic, according to the specified calendar schedule,

d. Analysis of the energy balance: The system must be capable of calculating the balance, based on parts of the network, defined by the operator – the amount of the reported energy, according to the commercial electricity meters with a similar or identical calendar schedule for reading and balancing electricity meter with the same schedule. Automatically, according to the specified calendar

информацията за събитието.

Събитията/Алармите трябва да се запаметяват във всички децентрализирани компоненти (електромери, прекъсвачи, гейтове) както и в централизираната система за период от време, променлив и настройван за дадена Група Аларми и Събития, но да се запаметят минимум 100 записа.

Анализ на грешки и оптимизация

1.2.1. Информация относно събитията и алармите

За обработването на критични ситуации е необходимо централизираната система да е в състояние да интерпретира събития и аларми както и да генерира филтри с цел изготвяне на справки. Съдържанието на справките трябва да е достъпно за потребителите или да се съхранява в желан файлов формат (например *.csv, .txt, .xls …).

1.2.2. Конфигурация за обработването на събития и аларми

В централизираната система е необходимо всяко прието събитие/аларма да се документира, като за целта е възможно правилата за това свободно да се изберат (напр. само да се протоколират, създаване на тикети, и др.) При това трябва да се създаде времева връзка между събития/аларми

1.2.3. Справка за активните и проверените събития и аларми

Централизираната система трябва да предлага функционалност за извеждане на информация относно активни събития и аларми и историята на различни събития/аларми.

Трябва да е налице възможност събитията/алармите да се сортират по различни критерии, като времеви период, тип на събитие/аларма, електромер, група от електромери, и др. Централизираната система трябва да предлага функционалност за ръчно и автоматично изтриване на събития/аларми.

1.2.4. Конфигурация на филтри за различни събития/аларми

За да се установи, кои събития/аларми трябва да се сигнализират към централизираната система, трябва да е възможно конфигуриране на филтри.

Трябва да е възможно да се правят конфигурации за един електромер, за група електромери както и за всички електромери.

Тези възможности трябва да са налични и за Концентратор на данни.

Целта на филтъра е да се предпази централизираната система от "препълване" чрез събития/аларми.

Изпълнителят трябва да опише в спецификацията филтрите, които могат да бъдат дефинирани.

Следните справки следва минимално да бъдат възможни за изпълнение:

a. Автоматично, съгласно зададения календарен график, да се генерират справки за комуникационните устройства, от които липсват данни или с които няма връзка.

b. Автоматично, съгласно зададения календарен график за отчитане, да се генерират справки за крайните устройства, за които липсват данни.

c. Автоматично, съгласно зададения календарен график,

d. Анализ на енергийния баланс: Системата да има възможност за изчисляване на баланс по участъци от мрежата, дефинирани от оператор – сума от

schedule, to generate files with the sections of the grid (outlets), where a disbalance of energy – outside the limits, preset by the operator.

e. Metering data – for a period, latest data, automatic and manual generation of files, templates for formatting of files (data, time, serial number of the device, transformer station, outlet, address, data1, data2, data3 etc.), standard formats CSV,XLS

1.2.5. Report on events/alarms and assigned filters

The centralized system must provide the capability of retrieving information regarding the relevant active filters, applicable to certain events/alarms. The capabilities for analyzing the filters, which, at a certain moment in time, were active, must be clearly detailed.

The centralized system must provide the capability for tracing the relevant filters, assigned to certain events/alarms. There should be a capability for preparing reports on the history of the active filters.

отчетената енергия от търговски електромери с еднакъв календарен график за отчитане и балансов електромер със същия график. Автоматично, съгласно зададения календарен график, да се генерират файлове с участъците от мрежата (изводи), където е измерен дебаланс на енергията – извън предварително зададени от оператора граници.

е. Измервателни данни – за период, последни данни, автоматично и ръчно генериране на файлове, шаблони за форматиране на файловете (дата, час, сер.ном.на устройството, ТП, извод, адрес, данни1, данни2, данни3 и т.н.), стандартни формати CSV,XLS

1.2.5. Справка за събития/аларми и причислени филтри

В централизираната система трябва да е възможно да се извежда информация относно това към кои събития/аларми какви активни филтри са причислени. Възможностите за анализиране относно филтрите, които в даден период от време са били активни, трябва да бъдат описани.

В централизираната система трябва да е възможно проследяването на това какви събития/аларми и какви филтри за били зададени. Трябва да е налице възможността да се изготвят справки за историята на активни филтри.

III. Fully electronic electricity meter with manipulations recognition, an integrated modem and a load management relay

1. Technical details

Position 1: Single-phase electricity meter
Position 2: Three-phase electricity meter for direct connection
Position 3: Three-phase electricity meter for indirect connection

Consumption type:	Active and reactive power – A+, A-, Option: QI, QII, QIII, QIV
Current strength:	Positions 1 and 2: 5(60)A or 10(60)A Position 3: 5(10)A
Rated voltage:	Position 1: 230V Positions 2 and 3: 3x230/400V
Rated frequency:	50 Hz
Precision class:	Positions 1 and 2: 2 (MID A, according IEC Class 2) Position 3: 1 (MID B, according IEC Class 1)
Types of tariffs:	multi-tariff (at least 4 tariffs), currently preset with 2 tariffs, cyclical displaying of the data on a LCD-display. The stored billing values from previous periods must not be visualized on the display.
Tariff management:	by means of a built-in clock (with summer/winter switching)
Billing:	The billing, caused by the built-in clock, takes place at 00.00 a.m. on the date, defined by the system. There should be an option for remote defining of the date of the billing period

III. Напълно електронен електромер с разпознаване на манипулации, интегриран модем и реле за управление на товара

1. Технически данни

Позиция 1: Еднофазен електромер
Позиция 2: Трифазен електромер за директно свързване
Позиция 3: Трифазен електромер за индиректно свързване

Вид консумация:	Активна и реактивна енергия – A+, A-, Опция: QI, QII, QIII, QIV
Сила на тока:	Позиции 1 и 2: 5(60)A или 10(60)A, Позиция 3: 5(10)A
Номинално напрежение:	Позиция 1: 230V Позиции 2 и 3:
Номинална честота:	50 Hz
Клас на точност:	Позиции 1 и 2: 2 (MID A, съгласно IEC клас 2) Позиция 3: 1 (MID B, съгласно IEC клас 1)
Видове тарифи:	многотарифен (най-малко 4 тарифи), в момента параметризиран с 2 тарифи, с циклично показване на данните на LCD-дисплея. Запаметените самоотчети (билинг стойности) от минали периоди не трябва да се визуализират на дисплея.
Управление на тарифите:	посредством вътрешен часовник (с лятно/зимно превключване)
Самоотчет (билинг):	Самоотчетът (билингът), предизвикан от вътрешния часовник, се извършва в 00.00 на дефинирана от системата дата. Дефинирането на дата за край на билинг период следва да може да се задава дистанционно

Data exchange channel:	IR - data exchange, PowerLine or GSM/GPRS – defining the interfaces, according to the block diagram
Control output:	Positions 1 and 2: Recommended 1000 Imp./kWh Position 3: Recommended 10000 Imp./kWh

Канал за обмен на данни:	IR - обмен на данни, PowerLine или GSM/GPRS – дефиниране на интерфейсите според блоковата схема
Контролен изход:	Позиции 1 и 2: Препоръчително 1000 Imp./kWh , Позиция 3: Препоръчително 10000 Imp./kWh.

2. General Requirements

The electricity meters must meet, in terms of technical specifications, the legal requirements, regarding metering in the Republic of Bulgaria.

Electricity meters, registered with the Governmental Register of Metering Devices, Approved for use in Bulgaria, may be used. A copy of the registration certificate (a type approval certificate) must be submitted.

Electricity meters, certified by the Measuring Instruments Directive (MID) may be used. A copy of the MID certificate, together with the type testing certificate, must be submitted.

A requisite precondition is the presence of a valid manufacturer's certificate, according to EN ISO 9001 or equivalent.

The electricity meters must be structurally designed and produced that no hazards would occur in fixed operational and normal conditions of work. More specifically, the following must be ensured:

a) - safety of people against electric shock
b) - safety of people against the effects of high temperatures
c) - security and resistance to heat and fire
d) - protection of the housing of the electricity meter against the penetration of hard objects, dust and water (at least IP51 or higher)
e)- protection of people, against events, being health hazards (vapours, sharp edges, ...).

Furthermore, the electricity meters (including the interfaces) must be protected against mechanical and electrical tampering.

In normal operating conditions, all parts of the electricity meters must be efficiently protected against corrosion. The protective layer must be strong enough, so that they cannot be damaged by weather conditions, under certain operating conditions.

2.1. Housing

Three openings on the box are required for the installation of the electricity meter on the installation panel, according to DIN 43857 part 1 for Position 1 and DIN 43857 part 2 for Positions 2 and 3. The dimensions must be met, irrespective of whether it is a fully integrated or modular solution.

The basic dimensions of the electricity meters, as well as the type and position of the fixtures must be recorded in tenderer's application, in case of deviations from the DIN requirements.

It must not be possible to open the housing without breaking it (e.g. it must be glued or welded), it is recommended that a sealing option is provided.

If the electricity meter can be opened without damaging it, there should be a contact, registering each and every opening of electricity meter's housing and it must be sealable.

2. Общи изисквания

Електромерите трябва да отговарят в техническото си изпълнение на законовите предписания за измерванията в Р. България.

Допускат се електромери, вписани в Държавния регистър на одобрените за използване в страната средства за измерване. Следва да се представи копие от вписването в държавния регистър – свидетелство за одобрен тип.

Допускат се електромери, сертифицирани съгласно Директива за измервателните уреди (MID). Следва да се представи копие от MID сертификат, заедно с типовото изпитание.

Необходимо е наличието на валиден сертификат на производителя по EN ISO 9001 или еквивалентен.

Електромерите трябва да са структурно проектирани и произведение така че при фиксирани експлоатационни и нормални условия на работа, да не възникват опасности. По-специално трябва да се осигури:
a) безопасността на хората срещу токов удар
b) безопасността на хората срещу ефектите на повишена температура
c) сигурност и устойчивост на топлина и огън
d) защитата на корпуса на електромера срещу проникване на твърди предмети, прах и вода (най-малко IP51 или по-висока)
e) защита на хората срещу събития, засягащи здравето (изпарения, остри ръбове, ...).

В допълнение електромерите (включително и интерфейсите) трябва да имат защита срещу механични и електрически опити за манипулиране.

При нормална работа всички части на електромерите трябва да бъдат ефективно защитени от корозия. Защитните слоеве трябва да бъдат достатъчно здрави, така че да не могат да бъдат повредени от атмосферните влияния, при определените условия на работа .

2.1. Корпус

За монтирането на електромера към таблото за монтаж са необходими три отвора на кутията съгласно DIN 43857 част 1 за Позиция 1 и DIN 43857 част 2 за Позиции 2 и 3. Размерите трябва да се спазват, независимо от това дали е напълно интегрирано или модулно решение.

Основните размери на електромерите, а също и вида и разположението на закрепващите елементи трябва да се запишат в заявлението за участие на кандидата, ако е налице отклонение от изискванията на DIN.

Отварянето на корпуса не трябва да е възможно без неговото разбиване (например да е залепен или заварен), желателно е да е налице възможност за пломбиране.

Ако електромерът може да се отваря без да се увреждa, то трябва да е налице контакт, регистриращ отварянията на корпуса на електромера и задължително да има възможност за пломбиране.

The housing must be sealable in such a manner that the internal parts of the electricity meter must only be accessible, after breaking the seal/s.
The cover of the housing must only be removable with the use of tools.
The housing must be designed and positioned in such a manner, that in case of temporary deformation, the reliable operation of the electricity meter must not be affected.
It is recommended that the housings are made of reusable insulating material, in accordance with protection class II.
Any and all bolts must be made of metal and combined with a metal threaded bushing. Furthermore, the plate for the sealing wire must be cast together with the box or the terminal cover.

2.2. Terminals, connection block

Whenever the terminals are arranged in one or more connection blocks, they must have sufficient insulation and mechanical strength. In order to ensure that, the insulating material, designed for the production of the connecting terminals, must be checked, following the applicable rules.
The electricity meter must not have any calibration links on the connection block.
The material of the connection block must withstand the ISO 75-2 tests at a temperature of 135°C and pressure of 1,8 MPa (method A).
The inlets in the insulating material, leading to the terminals, must be large enough, so that the insulation of the conductor can also pass through them.

The method of fixing of the conductor in the terminals must ensure sufficient and proper contact. No loosening of the connection or overheating of the conductor must be possible. Screw terminals, used for the electric contact and the screws, which may be unscrewed and screwed multiple times, during operation of the electricity meter, must be supplied with a metal threaded bushing. The main connections must be designed as box couplings or frame terminals with one or two terminal with straight or Philips screws Pozidriv 2 for Positions 1 and 2 and Pozidriv 1 for Position 3. The respective screws must be Pozidriv-Kombi 2 for Positions 1 and 2 and Pozidriv 1 for Position 3.

Each electricity meter or connection block cover must have a label with standard symbols, indicating the electric connection diagram. The Employer will include a connection diagram. The precise connection method shall be determined by the Employer, by means of a sample.
The possibility for corrosion, as a result of the use of various conductive materials, must be minimized by means of proper selection of these work pieces.

The electric connections must ensure that the contact pressure is not transferred through the insulating material.
The terminal connections must ensure a permanent contact for the entire lifetime of the electricity meter.

Any dubious terminals of various potentials, arranged close to each other, must be secured against accidental short circuit.

2.3. Terminal cover

The terminals of the electricity meter, if placed in a connection block and not protected otherwise, must have a separate terminal cover, which can be sealed, independently from the main cover. The terminal cover must enclose the terminals, screws and connecting conductors, as well as

Корпусът трябва така да се пломбира, че вътрешните части на електромера да станат достъпни едва след счупване на пломбата/пломбите.
Отстраняватнето на капака на корпуса не бива да е възможно без използване на инструменти.
Корпусът трябва да е конструиран и разположен така, че при временна деформация да не се наруши надеждната работа на електромера.

Препоръчително е корпусите да се изработват от годен за повторна употреба изолационен материал в съответствие с клас на защита II.
Всички болтове трябва да са изработени от метал и да се комбинират с метална втулка с резба. Освен това пластината за телта на пломбата трябва да е отливка с кутията или с клемния капак.

2.2. Клеми, клемен блок

Когато клемите са подредени в един или повече клемни блокове, те трябва да имат достатъчно добра изолация и механична здравина. За да се гарантира това, изолационният материал, предвиден за производството на съединителните клеми, трябва да бъде проверен по съответния ред.
На клемния блок електромерът не трябва да има връзки за калибриране.
Материалът на клемния блок трябва да издържи изпитванията по ISO 75-2 при температура от 135°C и налягане от 1,8 MPa (метод A).
Входящите отвори в изолационния материал, които водят до клемите, трябва да бъдат достатъчно големи, че през тях да може да премине и изолацията на проводника.
Начинът на закрепване на проводника в клемите трябва да гарантира достатъчно добър и траен контакт. Не трябва да се допуска разхлабване на връзката или прекомерното загряване на проводника. Винтови свръзки, които осъществяват електрически контакт, и винтове, които могат да бъдат развивани и завивани многократно по време на експлоатацията на електромера, трябва да имат резбова втулка от метал.
Основните клеми трябва да бъдат изработени като втулкови клеми или рамкови клеми с по един или два клемови винта за използването на прави и кръстати отвертки Pozidriv 2 за Позиции 1 и 2 и Pozidriv 1 за Позиция 3. Като винтове трябва да се използват Pozidriv-Kombi 2 за Позиции 1 и 2 и Pozidriv 1 за Позиция 3.
На всеки електромер или капак на клемния блок трябва със стандартни символи да е трайно обозначена електрическата схема за свързване. Възложителят ще приложи образец на схемата за свързване. Точния начин на закрепване ще се определи от Възложителя с помощта на мострата.
Възможността за корозиране в следствие използването на различни проводникови материали трябва да се снижи до минимум с подходящ подбор на тези заготовки.
Електрическите свръзки трябва да са направени така, че контактното налягане да не се провежда през изолационния материал.
Клемните връзки трябва така да са изпълнени, че да се гарантира траен контакт за времето на експлоатационния срок на електромера.
Съединителните клеми с различен потенциал, които са подредени гъсто една до друга, трябва да са обезопасени срещу случайно късо съединение.

their insulation at a proper length.

There must be no access to the terminals without breaking the seal of the terminal cover. The screws on the terminal cover must have the same heads, as those on the terminal screws.
The sealing option must be designed so that using more than one seal is possible, as long as the seals are permitted by the Bulgarian Metrology Institute.

It is recommended that the terminal cover is made of recyclable insulating material with protection class II.

The terminal cover must meet the provisions of DIN 43857.

2.4. Protection class

Solely electricity meters with insulated housing (incl. the connection block cover) with protection class II must be delivered. These electricity meters must have strong and durable housings and terminal covers, made of insulating material. The materials must have mechanical resistance and color resistance against ultraviolet radiation.

The housing must enclose all metal parts of the electricity meter, with the exception of small parts, such as the plate, bolts, rivets and other fasteners.
If such small parts outside the housing are accessible during installation or testing, in accordance with IEC 60529 they must be properly insulated, so that they cannot become energized in case of a failure in the main insulation.
Insulation paint, enamel, ordinary paper, cotton, oxide film on the metal parts, self-adhesive foil or similar unstable materials, are insufficient for such additional insulation.

Reinforced insulation is required for the connection block and the terminal cover.
When sealing the meter, the sealing wire must not get in contact with energized parts.

2.5. Protection against penetration of dust and water

According to EN 60529 +A1 of 2000-10-01 the electricity meters must have the following protection, as a minimum:

2.6. Technical data plate

If the electricity meter is installed in the grid, the plate and the metrological seal must be clearly visible on the front.
If the meters are certified according to the requirements of Regulation of measuring instruments subject of metrological control nameplate must comply with the relevant requirements of the Ordinance.

If the meters are certified according to MID nameplate must meet the relevant requirements of MID

Each electricity meter must have the following labeling:

2.6.1. any and all labeling, as required by the MID

2.6.2. any and all warning signs, as required on national level

2.6.3. any and all labeling, required approvals and certificates

1) Manufacturer's name or logo

2) Type labels and sign for admission to operation. For MID electricity meters, the respective number of the notified body is also included.

3) Number of phases and number of conductors, for which the electricity meter is designed (single- or three-phase). This data may be indicated, with the help of graphical symbols, in accordance with EN 62053-52 of 2006-10-01.

2.3. Клемен капак

Клемите на електромера, ако те са в клемен блок и не са защитени по друг начин, трябва да имат отделен клемен капак, който да може да бъде пломбиран независимо от основния капак. Клемният капак трябва да обхваща клемите, винтовете и присъединителните проводници, както и тяхната изолация на подходяща дължина.
Не трябва да има достъп до клемите без да бъде разпломбиран клемния капак. Винтовете на клемния капак трябва да бъдат изпълнени за същите глави като клемните винтове.
Възможността за пломбиране трябва да бъде проектирана така, че да е възможно пломбиране с една или повече пломби, разрешени от Българския Институт по Метрология.
Препоръчително е клемният капак да бъде произведен от рециклируем изолационен материал с клас на защита II.
Клемният капак трябва да отговаря на DIN 43857.

2.4. Клас на защита

Трябва да се доставят изключително и само електромери с изолиран корпус (вкл. капака на клемния блок) от клас на защита II. Тези електромери трябва да имат здрави и издръжливи корпуси и клемни капаци от изолационен материал. Материалите трябва да имат механична устойчивост и устойчивост на оцветяването срещу ултравиолетови лъчи.
Корпусът трябва да покрива всички метални части на електромера, с изключение на малки части като табелка, болтове, нитове и др. крепежни елементи.
Ако такива малки части извън корпуса са достъпни по време на монтаж или изпитване съгласно IEC 60529 те трябва да са подходящо изолирани срещу попадане под напрежение в случай на дефект на основната изолация. Изолационна боя, емайл, обикновена хартия, памук, оксид филм върху метални части, самозалепващо фолио или подобни нестабилни материали, не са достатъчни за тази допълнителна изолация.
За клемния блок и клемния капак се изисква подсилена изолация.
При пломбиране пломбажната тел не трябва да докосва части под напрежение.

2.5. Защита срещу проникване на прах и вода

Електромерите трябва да разполагат със защита съгласно EN 60529 +A1 издание 2000-10-01: IP51

2.6. Табелка с технически данни

Когато електромера е монтиран в мрежата табелката и метрологичната пломба/стикер трябва ясно да се виждат от предната страна.
В случай че електромерите, са сертифицирани съгласно изискванията на Наредба за средствата за измерване подлежащи на метрологичен контрол, табелката с техническите данни трябва да отговаря на съответните предписания на Наредбата.
В случай че електромерите, са сертифицирани съгласно MID табелката с техническите данни трябва да отговаря на съответните предписания на MID
Всеки електромер трябва да има следните означения:

2.6.1. всички маркировки, изисквани от MID

2.6.2. всички необходими предупредителни знаци изисквани на национално ниво

2.6.3. всички маркировки, необходими одобрения и

4) Factory number and year of manufacturing. The factory number, as seen on the plate, must also be programmed in the software of the electricity meter. Whenever the technical data plate is a part of the cover of the housing, the factory number, specified on the plate must also be inscribed durably on the inside of the electricity meter. The plate cannot be placed on the terminal cover.
5) Rated voltage: number of metered systems and voltage at the terminals.

6) Rated current and maximum admissible current (e.g.: 0,5-10(60)A).
7) Rated frequency: in Hz.
8) Constant of the electricity meter, e.g. in Imp/kWh.
9) Metering precision class 2 (MID A) for active and 2 for reactive values for Positions 1 and 2, metering precision class 1 (MID B) for active and 2 for reactive values in Position 3.
10) Temperature range, in accordance with MID (-25°C to +55°C).
11) Double protective insulation mark.
12) Barcode
At Employer's request, a barcode is also to be affixed. The precise type of the barcode and its exact place on the technical data plate are determined, based on the sample.
13) Ownership labeling:

14) MID labeling (for MID-electricity meters).

15) CE – Labeling with the year of the MID calibration (e.g. M14) and notified body.
16) The counters, visualized on the display of the electricity meter, must be detailed on the technical data plate.
The entire information, specified above, must be specified on an UV-resistant plate, which must be durable, clear and readable from the outside.
It is permitted to use standardized symbols, according to CENELEC EN 60387, on the plate.
The plate design is agreed individually with the Employer.
2.7. Weather conditions – temperature range
Temperature range in operating mode:
- 25°C to +55°C
Temperature range during storage or transport: - 25°C to +70°C
The precision class must be preserved in the entire scope of the operating temperature.

3. Power supply
3.1. Consumed power in the voltage and current circuits
The power, consumed by each voltage and current circuit of the electricity meter, as well as the additional modules at the rated voltage, the rated temperature and rated frequency, including the consumption of the metering systems for active and complete power must not exceed the values, set out in EN 62053-21. This refers to both the fully integrated version and the modular version, as an aggregate of all modules, including the electricity meter.
The own consumption with and without active

сертификати
1) Име на производителя или фирмен знак
2) Означение на типа и знак за допускане за експлоатация. При MID електромери, се изобразява съответния номер на нотифицираният орган.
3) Брой на фазите и брой на проводниците, за които е предвиден електромерът (едно- или трифазен). Тези данни могат да са означени с помощта на графични символи съгласно EN 62053-52 издание 2006-10-01.
4) Заводски номер и година на производство.
Заводският номер, както се вижда на табелката трябва да е програмиран и софтуерно в електромера. Когато табелката с техническите данни е част от капака на корпуса, отбелязаният върху табелката заводски номер трябва да е нанесен трайно и във вътрешната част на електромера. Поставянето на табелка върху клемния капак не е разрешено.
5) Номинално напрежение: брой на измервателните системи и на напрежение на клемите.
6) Номинален ток и максимално допустим ток (например: 0,5-10(60)A).
7) Номинална честота: в Hz.
8) Константа на електромера, напр. в Imp/kWh.
9) Клас на измервателна точност 2 (MID A) за активни и 2 за реактивни величини за Позиции 1 и 2, клас на измервателна точност 1 (MID B) за активни и 2 за реактивни величини при Позиция 3.
10) Температурен обхват съгласно MID (-25°C до +55°C).
11) Знак за двойна защитна изолация.
12) Баркод
Изискване на възложителя е поставяне на баркод. Точният тип на баркода и мястото му на поставяне на табелката с техническите данни се определят чрез мострата.
13) Маркировка за собственост:

14) Означаване според MID (при MID-електромери).
15) CE – Маркировка с година на MID калибриране (напр. M14) и нотифициран орган.
16) Броячите, които се визуализират на дисплея на електромера, трябва да са описани върху табелката с техническите данни.
Цялата информация, посочена по-горе, трябва да се съдържа върху UV - устойчива табелка, която трябва да бъде издръжлива, ясна и четлива отвън.
Разрешава се използването на стандартизирани символи според CENELEC EN 60387 на табелката.
Дизайнът на табелката е индивидуално договорена с Възложителя.
2.7. Климатични условия – температурен диапазон
Температурен диапазон при режим на работа:
- 25°C до +55°C
Температурен диапазон при съхранение и транспорт: - 25°C до +70°C
В целия диапазон на работната температура класът на точност трябва да се запази.
3. Захранване
3.1. Консумирана мощност в напреженовите и токовите вериги
Мощността, консумирана от всяка напреженова и

communication of the electricity meter must be specified in the technical documentation of the product, enclosed to the application for participation.

3.2. Supply voltage
3.2.1. Grid voltage allowance range
The power supply of the electricity meter must be designed so that it can function properly in the following ranges:
a) rated voltage Un=230V
b) normal operating range: 0,9Un to 1,10Un
c) operating range limits: 0,8Un to 1,15Un
The tender must specify the minimum voltages, at which the electricity meter starts metering.

3.2.2. Rated voltages
Rated voltage: Position 1: 230V
Rated voltage: Positions 2 and 3: 3x230/400V
3.2.3. Frequency
The meters must be designed for a rated frequency of 50Hz. They must be capable of working flawlessly in a two-pole field of ± 2% of the rated frequency.

3.3. Reverse effects on the grid
The supply grid block may be designed so that it does not allow any reverse effect by high-frequency oscillations in the grid.
The observation of EN 61000-3-2 +A2 edition 2005-11-01 must be guaranteed.
3.4. Protection against overvoltage
The test is conducted in accordance with EN 62052-11, chapter 7.3.2 pulse voltage test.
Pulse wave shape 1,2/50 microseconds, according to EN 60060-1.
Source impedance: 500Ohm + 50Ohm
Peak voltage value - 6kV.
3.5. Checking the resistance against pulse voltage

The products must meet the EN 61000-4-5 pulse effect test with a wave of 1,2/50 microseconds.

Pulse wave shape1,2/50 microseconds, according to EN 60060-1.
Source impedance: 2 Ohm ± 10%
Peak voltage value - 4 kV.
3.6. Electromagnetic compatibility
The products must not be affected by any interference, according to CENELEC EN 55011 and CENELEC EN 55014.
The power supply must be resistant to external electric and magnetic field interference at the specified installation locations for the electricity meters.
The electricity meter must not be affected by GSM cell phones with a transmission power of up to 2Watt.

3.7. Resistance against transitive interference (Burst)
In this respect, the requirements of EN 61000-4-4 (test precision 4) must be met.
3.8. Magnetic interference by permanent magnets
If a permanent magnet, with a residual magnetization of 400mT is placed at the electricity meter, this should not result in either a metrical-technical or functional errors.

In case of higher fields (>400mT) and the meter is not protected against magnetic influences the electricity meter must record their occurrence. These must always be recorded in the Logbook. Sending an alarm signal to the system is optional.

токова верига на електромера, както и от допълнителните модули при номинално напрежение, номинална температурата и номинална честота, включително консумацията на измервателните системи за активна и пълна мощност не трябва да надвишава стойностите, определени в EN 62053-21. Това се отнася както за напълно интегрирана версия, така и за модулна версия като сбор от всички модули, включително електромера.
Собствената консумация с и без активна комуникация на електромера трябва да се посочат в техническата документация на изделието към заявлението за участие.
3.2. Захранващо напрежение
3.2.1. Допусково поле на мрежовото напрежение
Захранването на електромера трябва да бъде проектирано така, че да може да функционира правилно в следните диапазони:
a) номинално напрежение Un=230V
b) нормален работен обхват: 0,9Un до 1,10Un
c) граничен работен обхват: 0,8Un до 1,15Un
В офертата трябва да се посочват минималните напрежения, при която електромерът започва да измерва.
3.2.2. Нормирани номинални напрежения
Номинално напрежение: Позиция 1: 230V
Номинално напрежение: Позиции 2 и 3: 3x230/400V
3.2.3. Честота
Уредите трябва да са предназначени за номинална честота от 50Hz. Те трябва да могат да работят безпроблемно в допусково поле от ± 2% от номиналната честота.
3.3. Обратни въздействия върху мрежата
Захранващият мрежови блок трябва да е оформен така, че да не допуска обратни въздействия от високочестотни трептения по мрежата.
Трябва да се гарантира спазването на EN 61000-3-2 +A2 издание 2005-11-01.
3.4. Защита срещу пренапрежение
Тестът се извършва съгласно EN 62052-11, глава 7.3.2 тест импулсно напрежение.
Форма на вълната на импулса 1,2/50 микросекунди, съгласно EN 60060-1.
Импеданс на източника: 500Ohm + 50Ohm
Пикова стойност на напрежението от 6kV
3.5. Проверка на устойчивостта срещу импулсно напрежение
Изделията трябва да са в съответствие с EN 61000-4-5 тест при импулсно въздействие с вълна 1,2/50 микросекунди.
Форма на вълната на импулса 1,2/50 микросекунди, съгласно EN 60060-1.
Импеданс на източника: 2 Ohm ± 10%
Пикова стойност на напрежението - 4 kV.
3.6. Електромагнитна съвместимост
Изделията не трябва да бъдат повлиявани от смущения съгласно CENELEC EN 55011 и CENELEC EN 55014. Не трябва е възможно повлияване на захранванията от външни електрически и магнитни полета на предвидените места за монтаж на електромерите.
Електромерът не трябва да се повлиява от GSM мобилни апарати с мощност на излъчване до 2Watt.
3.7. Устойчивост срещу преходни смущения (Burst).
Тук трябва да се спазват изискванията по EN 61000-4-4 (точност на изпитването 4).
3.8. Магнитно повлияване от постоянни магнити

3.9. Electromagnetic fields
In this respect the requirements as per EN 61000-4-3 must be met. According to chapter 5 a test precision of 4 is required. This corresponds to a test field strength of 30V/m.
3.10. Electrostatic discharge
In this respect, the requirements of EN 61000-4-2 must be met, test precision 4:
Contact discharge: 8kV
Aerial discharge: 15kV
3.11. Resistance to heat and fire
The connection block, the terminal cover and the housing of the electricity meter must be made of a non-combustible material, ensuring sufficient protection against the distribution of fire.
The members of the personnel must not get burned when touching thermally overloaded parts. The standard tests, according to EN 62052-11 and IEC 60695-2-11, designed for this purpose must be observed.

3.12. Behavior in case of grid power failure and restoration
The supply of the three-phase electricity meter must, consists of three phases and in case of failure of one or two phases of the grid power supply, the electricity meter must preserve its complete functionality, of at least one phase amounts to UN $\pm$ 10%.In case of failure of the neutral conductor, the electricity meter must not be damaged permanently and no general data loss must occur. When the grid power supply is resumed, whether it is single-, double- or triple-phase, the electricity meter must resume its complete functionality within not more than 5 sec.

In case of power failure for within one metering period, no data is to be stored in the load profile, but it is necessary to identify the failure with an appropriate status. In case of longer power interruptions, the last (incomplete) data, regarding the load profile must be stored with an appropriate status (Power down). The first data after the restoration of the power supply must also be identified with an appropriate status (Power up).

4. Technical requirements
4.1. Rated and maximum current

Values (EN 50470-1)	Position 1	Position 2	Position 3
I_{Ref} Referent current	5 or 10A	5 or 10A	5A
I_{max} (maximum current for the respective precision class)	60A	60A	6A
Maximum current, which the electricity meter can withstand without any damages	80A	80A	10A

I_{st} and I_{min} must be specified by the manufacturer.
The minimum commutating current of the control relay must be at least I_{max}.
4.2. Metered values
4.2.1. Metering and storage of active energy:
a) Total active energy +A (kWh)

При поставянето на постоянен магнит с остатъчна намагнитеност 400mT електромерът не трябва да отчита нито измервателно-техническа, нито функционална грешка.
При по-високи полета (>400mT) електромерът трябва да регистрира поява им. Задължително е вписването им в дневника на събитията (LogBook). По желание, да се изпрати алармен сигнал към системата.

3.9. Електромагнитни радиочестотни полета
Тук трябва да се изпълнят изискванията по EN 61000-4-3. Съгласно глава 5 се изисква точност на изпитването 4. Това съответства на сила на тестовото поле от 30V/m.
3.10. Електростатично разреждане
Тук трябва да се изпълнят изискванията по EN 61000-4-2, точност на изпитването 4:
Контактен разряд: 8kV
Въздушен разряд: 15kV
3.11. Устойчивост на топлина и огън
Клемният блок, клемният капак и корпусът на електромера трябва да са изработени от самогасящ се материал, осигуряващ достатъчна защита срещу разпространението на огън.
Не трябва да се стигне до опарване на персонала при докосване до термично претоварени части. Стандартни тестове според EN 62052-11 и IEC 60695-2-11, предвидени в това отношение трябва да бъдат изпълнени.
3.12. Поведение при отпадане и възстановяване на напрежението в мрежата
Захранването на трифазния електромер трябва да е трифазно изпълнено и при отпадането на една респективно на две фази на мрежовото напрежение електромерът трябва да запази пълната си функционална годност, ако поне едното фазово напрежение възлиза на UN $\pm$ 10%.При прекъсване на нулевия проводник електромерът не бива да се увреди трайно и не бива настъпи генерална загуба на данни. При възстановяване на мрежовото напрежение, независимо дали ще е едно-, дву- или трифазно, електромерът трябва най-късно след 5 сек. да е изцяло годен за функциониране.
При отпадане на напрежението за един период на измерване не трябва да се запаметяват данни в товаровия профил, но е необходимо да се идентифицира отпадането с подходящ статус. При по-дълги прекъсвания последните (непълни) данни за товаровия профил трябва да бъдат запаметени с подходящ статус (Power down). Първите данни след възстановяване на напрежението трябва да бъдат идентифицирани с подходящ статус (Power up).

4. Технически изисквания
4.1. Номинален и максимален ток

Величини (EN 50470-1)	Позиция 1	Позиция 2	Позиция 3
I_{Ref} Референтен ток	5 или 10A	5 или 10A	5A
I_{max} (макс. ток за класа на точност)	60A	60A	6A
Максимален ток, който електромера може да понесе без да се повреди	80A	80A	10A

b) Total active energy –A (kWh)
c) Load profile 15 min. +A: Generation of metered data (kWh) with date/time and status (e.g. power restoration)

d) Load profile 15 min. –A: Generation of the metered data (kWh) with date/time and status (e.g. power restoration)
4.2.2. Option: Metering and storage of reactive energy:

a) Total reactive power QI (kVArh)
b) Total reactive power QII (kVArh)
c) Total reactive power QIII (kVArh)
d) Total reactive power QIV (kVArh)
e) Load profile 15 min. QI: Generation of the metered data (kVArh) with date/time and status (e.g. power restoration)
f) Load profile 15 min. QII: Generation of the metered data (kVArh) with date/time and status (e.g. power restoration)
g) Load profile 15 min. QIII: Generation of the metered data (kVArh) with date/time and status (e.g. power restoration)
h) Load profile 15 min. QIV: Generation of the metered data (kVArh) with date/time and status (e.g. power restoration)
4.2.3. Option: tariff registers
Apart from the aggregate logs (total energy) the electricity meter must also have at least four tariff registers for: +A, –A, Option: QI, QII, QIII, and QIV.

The activation of these logs must take place by means of an internal tariff table with hourly/daily/weekly/monthly/yearly and holiday programs, which may be configured from both the remote reading interface and the service port of the electricity meter.

Any and all changes to the tariff table must be registered with their actual date and time, in the event logbook.
4.3. Identification of the metered values
For clear identification of the metered values, the OBIS code may be used (according to EN 62056-01: Object Identification System - OBIS).
To determine which values to be included in the data list shall be configured by the grid operator. *It is recommended for the readings to be with leading zeroes in position 1 and 2.

I_{st} и I_{min} трябва да се обявят от производителя.
Минималният комутиращ ток на релето за управление трябва да е най-малко I_{max}.
4.2. Измервани величини
4.2.1. Измерване и съхранение на активна енергия:
a) Обща активна енергия +A (kWh)
b) Обща активна енергия –A (kWh)
c) Товаров профил 15 мин. +A: Формиране на измерените данни (kWh) с дата/час и статус (например възстановяване на напрежението)
d) Товаров профил 15 мин. –A: Формиране на измерените данни (kWh) с дата/час и статус (например възстановяване на напрежението)
4.2.2. Опция: Измерване и съхранение на реактивна енергия:
a) Обща реактивна енергия QI (kVArh)
b) Обща реактивна енергия QII (kVArh)
c) Обща реактивна енергия QIII (kVArh)
d) Обща реактивна енергия QIV (kVArh)
e) Товаров профил 15 мин. QI: Формиране на измерените данни (kVArh) с дата/час и статус (например възстановяване на напрежението)
f) Товаров профил 15 мин. QII: Формиране на измерените данни (kVArh) с дата/час и статус (например възстановяване на напрежението)
g) Товаров профил 15 мин. QIII: Формиране на измерените данни (kVArh) с дата/час и статус (например възстановяване на напрежението)
h) Товаров профил 15 мин. QIV: Формиране на измерените данни (kVArh) с дата/час и статус (например възстановяване на напрежението)
4.2.3. Опция: тарифни регистри
Електромерът трябва да притежава освен сумарните регистри (обща енергия) и най-малко четири тарифни регистри за: +A, –A; Опция: QI, QII, QIII, и QIV.
Активирането на тези регистри трябва да бъде направено чрез вътрешна тарифна таблица с часови/дневни/седмични/месечни/годишни и празнични програми, които да могат да се конфигурират както от интерфейса за дистанционно отчитане, така и през сервизния порт на електромера.
Всякакви промени в тарифната таблица, трябва да се регистрират с дата и час в дневника на събитията.
4.3. Идентификация на измерваните величини
За недвусмислено идентифициране на измерените стойности може да се използва OBIS код (според EN 62056-01: система OBIS – Object Identification System).
Определянето кои величини да бъдат включени в списъка с данните трябва да може да се конфигурира от мрежовия оператор. *Препоръчително е показанията да бъдат с водещи нули за позиция 1 и 2

OBIS	Definition	Display/presentation of register	Interface P0 (IR)/ presentation of register	Interface P1 (PLC)/ presentation of register
*	Device ID, provided by the manufacturer	-	*	*
0.0.0	ID Number (Device serial No.)	-	20/0	20/0
F.F	Error register	Max. 8/0	Max.8/0	Max. 8/0
0.1.0	Reset counter	2/0	2/0	2/0
1.6.0	15min maximum demand (P+)	-	2/2 с 4 historical values	2/2 с 4 historical values
2.6.0	15min maximum power (P-)	-	2/2 с 4 historical values	2/2 с 4 historical values
1.8.0	Active energy register (A+)	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
1.8.T	Active energy register (A+) T=1-4 – tariffs from 1 to 4	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
2.8.0	Active energy register (A–)	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
**5.8.0	Register reactive energy (QI)	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
**6.8.0	Register reactive energy (QII)	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
**7.8.0	Register reactive energy (QII)	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
**8.8.0	Register reactive energy (QIV)	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
0.9.1	Current time [hh:mm:ss]	Hh:mm:ss	Hh:mm:ss	Hh:mm:ss
0.9.2	Current date [YYYY-MM-DD]	yy-mm-dd	yy-mm-dd	yy-mm-dd
31.25 (31.7)	Current L1	-	2/2	2/2
51.25 (51.7)	Current L2	-	2/2	2/2
71.25 (71.7)	Current L3	-	2/2	2/2
32.25 (32.7)	Voltage L1	-	3	3
52.25 (52.7)	Voltage L2	-	3	3
72.25 (72.7)	Voltage L3	-	3	3
*	Hardware identification	-	*	*
*	Firmware identification (under metrological seal)	-	*	*
*	Firmware identification (outside metrological seal)	-	*	*
*	Parameterization code (tariff table, ...)	-	*	*
*	Time and date of last parameterization	-	*	*
Load profile data				
1.8.0	Energy profile (A+) with date and time, units of measurement and status	-	*	*
2.8.0	Energy profile (A-) with date and time, units of measurement and status	-	*	*
**5.8.0	Energy profile (QI) with date and time, units of measurement and status	-	*	*

**6.8.0	Energy profile (QII) with date and time, units of measurement and status	-	*	*
**7.8.0	Energy profile (QIII) with date and time, units of measurement and status	-	*	*
**8.8.0	Energy profile (QIV) with date and time, units of measurement and status	-	*	*
P.98	Event Logbook	-	*	*

* To be approved by the grid operator.
** Option

4.4. Memory capacity
The electricity meter must store a load profile for each of the parameterized values (including information regarding the status, date and time) the last minimum 40 days.
The memory of the event logbook must be capable of storing at least 100 events.
4.5. Software architecture of the electricity meter
4.5.1. General requirements
The structure must generally conform to the recommendations of the WELMEC Software Guide 7.2 (Measuring Instruments Directive 2004 / 22 / EC). In particular, it should be noted that a mandatory minimum requirement is that the firmware is separated into metrological (approved) and non-metrological (non-approvable). The metrological part of the firmware may only include the functions, detailed in 4.5.2. Any and all other functions may only be implemented in the non-approvable part.
4.5.2. Metrological firmware
The metrological firmware must only include functions, which are directly required for metering purposes. The supplier must specify which are the metrological functions and sub-functions of the firmware.

4.5.3. Software update/upgrade of the non-approvable part
Software update/upgrade in the non-metrological part must be possible to perform from the electricity meter and from the Head End System. After removing the electricity meter it should be checked if the entire software has been transferred. Only then can its installation begin. After the installation, the electricity meter carries out a self-check and checks if the new software has been properly installed, recording the relevant data in the event logbook.
If the update fails, the software is automatically restored to the previous version. The respective error must be recorded in the event logbook.

The procedure must take place in accordance with the requirements for "security of the electricity meter".
The firmware update of non-approvable part should not affect in any way of the current values of energy registers.
4.6. Display
For displaying the data, using the external buttons of the electricity meter, displays, ensuring easy reading are to be used, as the delay in case of an environmental temperature of -25°C should not exceed 1 second.

For confidentiality purposes, displaying data for the load

* Трябва да се съгласуват от мрежовия оператор.
** Опция

4.4. Обем на паметта
Електромерът трябва да съхранява за всяка от параметризираните стойности товаров профил (включително информация за състоянието, дата и час) за последните минимум 40 дни.
Паметта на дневника на събитията трябва да бъде най-малко 100 събития.
4.5. Софтуерна архитектура на електромера
4.5.1. Общи изисквания
Структурата по принцип трябва да се съобразява с препоръките на WELMEC Software Guide 7.2 (Measuring Instruments Directive 2004 / 22 / EC). По-специално следва да се отбележи, че като задължително минимално изискване е фърмуера да се раздели на метрологичен (одобрен) и неметрологичен (неодобряем). Метрологичната част на фърмуера може да включва само тези функции, които са описани в 4.5.2. Всички други функции могат да бъдат реализирани само в неодобряема част.
4.5.2. Метрологичен фърмуер
Метрологичният фърмуер трябва да включва само тези функции, които са пряко необходими за измерване. Доставчикът трябва да уточни кои са метрологичните функции и под-функции на фърмуера.
4.5.3. Софтуерно обновяване/надграждане на неодобряемата част
Софтуерна актуализация/надстройка в неметрологичната част трябва да бъде изпълнима от електромера и централната система. След свалянето електромера трябва да провери дали пълният софтуер е бил прехвърлен. Само тогава може да започне инсталацията му. След инсталирането електромерът извършва самопроверка и проверка дали новият софтуер е правилно инсталиран, като записва съответните данни в дневника на събитията.
Ако актуализацията не е успешна трябва да се извърши автоматично връщане към предишната версия на софтуера. Трябва да се регистрира съответната грешка в дневника на събитията.
Процедурата трябва да бъде направена съгласно изискванията за "сигурност на електромера".
Промяната на неодобряемата част на фърмуера не трябва по никакъв начин да променя текущите стойности на енергийните регистри
4.6. Дисплей
За изобразяване на данните, които се извикват с външните бутони на електромера, трябва да се използват дисплеи, с които лесно се отчита, като при температура на околната среда до -25°C забавянето

profile on the display, using the call button, is only allowed in special cases, this indicator is to be activated and deactivated additionally, using the WAN interface P1 for remote reading and through the service port (inperface P0) for servicing and maintenance of the electricity meter (default setting – no data on the load profile is shown on the display).

The opening of the terminal cover must be shown on the display.
The electronic display must meet the following minimum requirements:
(Back)light
Capacity to display the following values:
4.6.1. Direct electricity meters
4.6.1.1 8 digits with two digits after the decimal point (6/2) Minimum dimensions 8x3mm.
4.6.1.2 Power with 8 digits and 3 digits after the decimal point (5/3)
4.6.2 Indirect electricity meters
4.6.2.1 8 digits with three digits after the decimal point (5/3) Minimum dimensions 8x3mm.
4.6.2.2 Power with 8 digits with 3 digits after the decimal point (5/3)
4.6.3 Main functions
4.6.3.1 Units of measurement
4.6.3.2 Code of the metered value (OBIS or another code)
4.6.3.3 Energy indicator for +A, –A (Option: +R, –R), an arrow or a square diagram
4.6.3.4 Phase indicators: Showing the presence of phase voltage and the direction of rotation of the field (e.g. blinking in case of reserve movement)
4.6.3.5 Indicator for the absence of consumption
4.6.3.6 Error code
4.6.3.7 Status of the control relay
4.6.3.8 Version of the firmware (approved and non-approvable)
4.6.3.9 Firmware checksums
4.6.3.10 Date and time
4.6.3.11 Displaying current values at request (e.g. current, voltage, power factor etc.)

4.6.3.12 Option: Status indicators (freely adjustable) for:

4.6.3.12.1 Connection of the device to the interface for external meters
4.6.3.12.2 Active data transfer
4.6.3.12.3 Status of the communication module
4.6.3.12.4 Status of the control relay (e.g. OFF, stand-by…)
4.6.3.12.5 Operating mode (Normal, Settings, Parameterization)
4.6.3.12.6 Tampering status
4.6.4 Additional functions
4.6.4.1 Showing the active tariff
4.6.4.2 Tariff table number
4.6.4.3 Readings, regarding the aggregate reactive energy QI, QII, QIII and QIV
4.6.4.4 Readings of all tariff registers
4.7 Additional functions
The activation of the tariff regisers (and their readings on the display) must be possible through the configuration table.
The electricity meter must be calibrated for the full range of metrological functions. It must always meter and store all the metered values.

трябва да е под 1 секунда.
Поради съображения за поверителност показването на данни за товаровия профил на дисплея чрез бутона за повикване е разрешено само в специални случаи, този показател трябва да се активира и деактивира допълнително чрез WAN интерфейса за дистанционно отчитане P1 и посредством сервизния порт (интерфейс P0) за обслужване на електромера (настройка по подразбиране - да няма данни за товаровия профил на дисплея).
Отварянето на клемния капак трябва да се изобрази на дисплея.
Електронният дисплей трябва да отговаря на следните минимални изисквания:
(Фоново) осветление
Възможност за изобразяване на следните величини:
4.6.1. Директни електромери
4.6.1.1 8 цифри с два знака след десетичната запетая (6/2) Минимален размер 8x3mm.
4.6.1.2 Мощност с 8 цифри с 3 знака след десетичната запетая (5/3)
4.6.2 Индиректни електромери
4.6.2.1. 8 цифри с два знака след десетичната запетая (5/3) Минимален размер 8x3mm.
4.6.2.2. Мощност с 8 цифри с 3 знака след десетичната запетая (5/3)
4.6.3. Основни функции
4.6.3.1. Мерни единици
4.6.3.2. Код на измерваната величина (OBIS или друг код)
4.6.3.3. Енергиен индикатор за +A, –A (Опция: +R, –R), стрелка или квадрантна диаграма
4.6.3.4. Фазови индикатори: Показват наличието на фазните напрежения и посоката на въртене на полето (например мигане при обратна посока)
4.6.3.5. Индикатор за липса на консумация
4.6.3.6. Код за грешка
4.6.3.7. Статус на релето за управление
4.6.3.8. Версия на фърмуера (одобрен и неодобряем)

4.6.3.9. Контролни суми на фърмуера
4.6.3.10.Дата и час
4.6.3.11.Показване на моментни величини по желание (напр. ток, напрежение, фактор на мощността и др.)
4.6.3.12.Опция: Статусни индикатори (свободно настройваеми) за:
4.6.3.12.1. Свързване на устройство към интерфейса за външни измервателни устройства
4.6.3.12.2. Активен трансфер на данни
4.6.3.12.3. Статус на комуникационния модул
4.6.3.12.4. Статус на релето за управление (напр. ИЗКЛ., готов за включване…)
4.6.3.12.5. Режим на работа (Нормален, Настройка, Параметризиране,)
4.6.3.12.6. Манипулационен статус
4.6.4. Допълнителни функции:
4.6.4.1. Показване на активната тарифа
4.6.4.2. Номер на тарифната таблица
4.6.4.3. Показания за сумарна реактивна енергия QI, QII, QIII и QIV
4.6.4.4. Показания на всички тарифни регистри
4.7. Допълнителни функции
Активирането на тарифните регистри (и показанията им на дисплея) трябва да бъде възможно чрез конфигурационната таблица.
Електромерът трябва да бъде калибриран за пълен

In order to ensure the efficiency and usability, only the required tariff registers should be activated and displayed (e.g. single-tariff schedule with a single log).

The following parameters must be determined:
→ Allowing the reactive logs (5.8.0/6.8.0/7.8.0/8.8.0), as well as their displaying on screen.

4.8 Built-in clock and calendar
The built-in clock must meet the requirements of EN 62054-21 and EN 62052-21.
The control of the built-in clock must be quartz.

The built-in clock switch must have a complete calendar (date and time) with a summer/winter time switch and weekend and holidays switch.
Setting/synchronization of the date and time should be possible, using the WAN interface of the Head End System, as well as through the service interface on-site. The settings of the date and time, using the buttons on the electricity meter is forbidden for IT security reasons.

The change of summer/winter time (DST) must be parameterized, in accordance with the European standards. The switching times, valid in Bulgaria (UTC+2) must be taken into consideration, as well as all the leap years until 2050.
DST should be performed according next table:

DST time	DST:
Summer -> Winter	4:00 => 3:00 o'clock
Winter -> Summer	3:00 => 4:00 o'clock

The switching of the tariffs takes place in accordance with Regulator's Decision No.Ц–002/ 29.03.2002.

Tariff program	Tariff program active from:
Summer	00:00 01.04
Winter	00:00 01.11

The lifetime of the clock switch must be at least 20 years.

The precision must be within ± 5ppm (a maximum daily deviation of 0,5 seconds per day).
Apart from that the clock switch must incorporate temperature compensation.
The switching of tariffs must take place in accordance with the following table:

Metered value	Tariff counter	Winter time	Summer time
P+	1.8.1 (nightly)	22:00 to 06:00	23:00 to 07:00
	1.8.2 (daily)	06:00 to 22:00	07:00 to 23:00

4.9 Load control relay (Position 1 and 2)
There is a requirement for the presence of a switching off device, integrated in the electricity meter. The switching-off device must be capable of interpreting the following commands – both through the local interface, and remotely

- SWITCHING-ON RELAYS

набор от метрологични функции. Той винаги трябва да измерва и съхранява всички измервани величини.
За да се гарантира работоспособността и използваемостта само необходимите тарифни регистри трябва да бъдат активирани и показани на дисплея (напр. еднотарифен план с един регистър).
Трябва да се определят следните параметри:
→ Разрешаване на реактивните регистри (5.8.0/6.8.0/7.8.0/8.8.0), както и показването им на дисплея.
4.8. Вътрешен часовник и календар
Вътрешният часовник трябва да отговаря на изискванията на EN 62054-21 и EN 62052-21.
Управлението на вътрешния часовник трябва де е кварцово.
Вътрешният часовников превключвател да разполага с пълен календар (дата и час) с превключване на лятно/зимно време и за почивните дни.
Настройка/синхронизиране на датата и часа трябва да са възможни чрез интерфейс WAN интерфейса на централната системата, както и чрез сервизния интерфейс на място. Настройката на дата и час чрез бутони на електромера не е позволено поради съображения за IT сигурност.
Смяната лятно/зимно време трябва да бъде параметризирана, съгласно европейския стандарт. Да се вземат предвид времената за превключване, валидни за България (UTC+2), както и всички високосни години до 2050.
Лятното часово време трябва да се извършва съгласно следващата таблица:

DST time	DST:
Лято -> Зима	4:00 => 3:00 o'clock
Зима-> Лято	3:00 => 4:00 o'clock

Превключването на тарифите се извършва съгл. Решение на Регулатора №Ц–002/ 29.03.2002.

Тарифна програма	Тарифна програма валидна от:
Лято	00:00 01.04
Зима	00:00 01.11

Продължителността на живот на часовниковия превключвател трябва да бъде най-малко 20 години.
Точността трябва да е в рамките ± 5ppm (максимално дневно отклонение 0,5 секунди на ден).
Освен това часовниковият превключвател трябва да е с компенсиране на температурата.
Превключването на тарифите трябва да се извършва съгласно следната таблица:

Измервател на величина	Тарифен брояч	Зимно часово време	Лятно часово време
P+	1.8.1 (нощна)	22:00 до 06:00	23:00 до 07:00
	1.8.2 (дневна)	06:00 до 22:00	07:00 до 23:00

4.9. Реле за управление на товара (Позиция 1 и 2)
Има изискване за наличие на интегрирано в електромера устройство за изключване. Устройството за изключване трябва да може да интерпретира следните команди – както през локален интерфейс,

- SWITCHING-OFF RELAYS

The formatted commands must be provided.

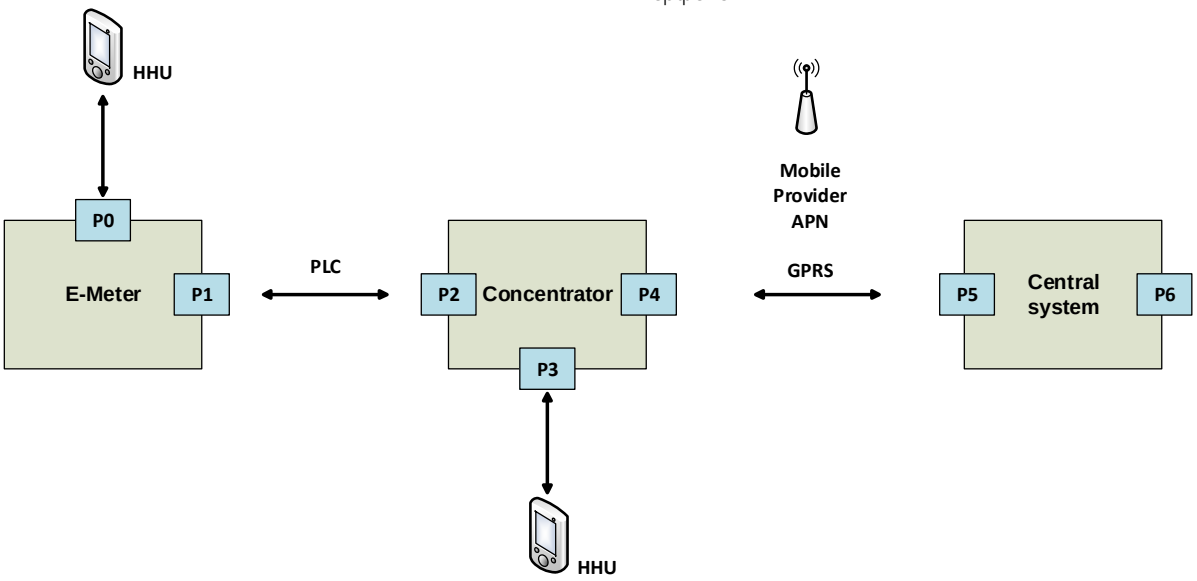
Technical details
The switching-off device must meet the following minimum requirements:
Mechanical useful lifetime: 100 000 commutations
Mechanical useful lifetime, according to EN 62055-31, annex C: 10 000 commutations at 100 A, cosφ=1
Maximum commutation voltage: 400 V (AC)
Maximum commutation current: 80 A
Short circuit < 10 ms as per EN 62053-21: 3 kA
Maximum commutation power: 25 kVA
Insulation capability: 4 kV with duration 1 minute

5 Interfaces. Interface related Requirements
Interfaces:

така и дистанционно:
- ВКЛЮЧВАНЕ НА РЕЛЕТАТА
- ИЗКЛЮЧВАНЕ НА РЕЛЕТАТА

Форматираните команди трябва да бъдат предоставени.
Технически данни
Устройството за изключване трябва да покрива следните минимални изисквания:
Механичен полезен живот: 100 000 комутации
Механичен полезен живот съгл. EN 62055-31, анекс C: 10 000 комутации при 100 A, cosφ=1
Максимално напрежение на комутиране: 400 V (AC)
Максимален комутиран ток: 80 A
Късо съединение < 10 ms според EN 62053-21: 3 kA
Максимална мощност на комутиране: 25 kVA
Изолационна способност: 4 kV с продължителност от 1 минута

5. Интерфейси. Изисквания към интерфейсите
Интерфейси:



Interfaces description

Interface	Description
P0	Infrared (IR) interface through which external maintenance tasks can be performed of E-Meter with external device (HHU).
P1	WAN interface of the meter must be able to handle PLC communication
P2	PLC interface between data Concentrator and E-Meter.
P3	Interface through which external maintenance tasks can be performed of Concentrator with external device (HHU).
P4	Interface between data Concentrator and Head End System using GPRS communication environment.
P5	WAN interface of Head End System for

Описание на интерфейсите:

Интерфейс	Описание
P0	Инфрачервен (IR) интерфейс, чрез който външни дейности по поддръжка могат да бъдат извършвани с Е-електромера, с помощта на външно устройство (Преносим терминал).
P1	WAN интерфейса на електромера трябва да може да се справи с PLC комуникацията
P2	PLC интерфейсът между Концентратора на данни и Е-електромера.
P3	Интерфейс, чрез който могат да бъдат извършвани външни дейности по поддръжка с Концентратор с помощта на външно устройство (Преносим терминал).
P4	Интерфейс между Концентратора на данни и Централната система чрез използване на GPRS комуникация.

	communication with Concentrators.
P6	Interfaces for data exchange between Head End System and existing legacy systems or third party applications.

Electronic electricity meter
In general, the electricity meters must be designed, in a manner ensuring that any requests, sent to one interface cannot be retranslated through another interface (port insulation). This means that a single unauthorized access through the service interface cannot be used for burglary access to the WAN-interface, enabling the use of the WAN.

5.1. Service interface (P0)
Physical layer
The service interface must be executed as an optical interface.
The communication speed must be at least 9600 boud.

Protocol layer
The service access to the electricity meter must be provided through DLMS/COSEM, IEC 62056-21 or another standard protocol. The eligible option must be determined by the grid operator.
Security
The security must be provided within the framework of the assignments of "Security of the electricity meter".
The access control must be provided by individual passwords. It is not necessary to code the data transmission, due to the exclusively local access

5.2. WAN Interface (P1)
In order to ensure the quality of the communication channels data, such as signal level, signal-to-noise ratio and bit errors must be provided.
Optionally, the electricity meter must be designed integrated or modular.
The electricity meter/module must be supplied with indicators showing the communication status by means of LEDs:
i. Presence of communication for PLC
ii. Status (normal operation status or error status))

5.2.1. Intergrated WAN Interface PLC (C)
Physical layer
The connection of the meters and the communication equipment to the grid must take place in accordance with the technical instructions of the manufacturer.

The manufacturer must propose a technical solution (e.g. interference suppression filter), in order to eliminate any possible interferences in the client equipment, caused by electric devices.
Application layer
Own protocols of the electricity meters are allowed.
Security
The security must be provided within the assignments of "Security of the electricity meter".
6. Permission for commissioning, initial and follow-up inspection
6.1. Type approval and MID certification
For the MID electricity meters it is necessary to specify the place of manufacturing, the certifying body and the notified body for monitoring the inspection. The offer must contain

P5	WAN интерфейс на Централната система за комуникация с Концентраторите.
P6	Интерфейси за обмен на данни между Централната система и съществуващите системи или приложения на трети страни.

Електронен електромер
По принцип електромерите трябва да се конструират така, че заявки до един интерфейс да не могат да се препредават чрез друг интерфейс (изолация на портовете). Това означава, че даден неоправомощен достъп през сервизния интерфейс да не може да бъде използван за взломен достъп във WAN-интерфейса и по този начин да може да се използва WAN-мрежата.
5.1. Сервизен интерфейс (P0)
Физически слой
Сервизният интерфейс трябва да се изпълни като оптичен интерфейс.
Скоростта на комуникация трябва да е минимум на 9600 бода.
Протоколен слой
Сервизният достъп до електромера трябва да се осигури чрез DLMS/COSEM, IEC 62056-21 или друг стандартен протокол. Допустимата опция трябва да се определи от оператора на мрежата.
Сигурност
Сигурността трябва да се осъществи в рамките на заданията на „Сигурност на електромера".
Контролът на достъпа трябва да се осъществява чрез индивидуални пароли. Не е необходимо кодирането на предаването на данни поради изключително локалния достъп
5.2. WAN Интерфейс (P1)
За осигуряване на качеството на комуникационните канали трябва да се предоставят данни като ниво на сигнала, отношение сигнал-шум и грешки на битове.
Опционално, електромерът трябва да се изгради интегриран или модулен.
Електромерът/модулът трябва да разполага с индикатори показващи комуникационния статус посредством LED:
i. Наличие на комуникация при PLC
ii. Статус (нормално работно състояние лили състояние на грешка)
5.2.1. Интегриран WAN Интерфейс PLC (C)
Физически слой
Свързването на измервателните уреди и комуникационното оборудване към мрежата трябва да бъде съгласно техническите предписания на фиармата производител.
Фирмата-производител трябва да предложи техническо решение (напр. филтър за подтискане на смущенията), за да се отстранят евентуални влияния в съоръженията на клиента от електроуреди.
Приложен слой
Допускат се собствени протоколи на електромерите.
Сигурност
Сигурността трябва да се осъществи в рамките на заданията в „Сигурност на електромера".
6. Допускане в експлоатация, първоначална и последваща проверка
6.1. Одобрение на типа и MID сертифициране
При MID електромери е нужно да се посочат мястото на производство, акредитиращият орган и

a certificate from a type test, including temperature correlation of the metrological errors and a declaration of conformity, both for each delivery and in case of a change in the version of the product of the manufacturer.
The electricity meter may also be approved for use in Bulgaria, by means of registration in the commercial meters logs.

6.2. Parameterization software

A license is required for the parameterization software, supplied with all the available functions of the proposed electricity meter. When supplying the electricity meter, it must be accompanied by the parameterization software, in order to ensure full compatibility and functionality with the various parameter options. The license must include all the software updates for the lifetime of the electricity meter.

The media, containing the installation files can be freely selected (CD, USB etc.).
If necessary, the supply shall include all due training in working with the software, setting the parameters and the necessary data processing.
A contact person must be specified.
The parameterization software must be designed in a manner, ensuring the access to the electricity meter through the service interface. Therefore attention is to be paid to the option for encryption of the connection with the electricity meters.

6.3. *Option for entering the test mode

The status of the test mode (ON or OFF) for the calibration must be clearly displayed on the electricity meter by means of the service interface and the display.
The following commands, which may be transmitted by the test device through the service interface and executed by the electricity meter, must be available:

a) Test mode ON
b) Test mode OFF
c) Settings the time/date
d) Increasing the LED constant (for the metrological inspection)
e) Display test (optional)
f) Switching the LED for active/reactive energy (optional)

g) Billing (optional).
h Switching the tariffs for metering energy and power (optional)
i) Control relay ON (Except option)
g) Control relay OFF (Except option)

6.3.1. LED

A standard optical head should enable the reading of pulses at any time.
It is preferable to use red and green LEDs. The execution of the LED must ensure the flawless reading of pulses with optical heads, which can be activated from a distance of 30mm. This function must be guaranteed in case of referenced (closed) electricity meters. If there is only a single LED on the electricity meter, it should be possible to switch the pulses between active and reactive power and back through an IR command. Alternatively, there may be two LEDs (for active/reactive energy).

6.3.2. Position of the LEDs and the IR-interface.

In order to ensure the flawless automatic calibration of the

нотифицираният орган за наблюдение на проверката. В офертата трябва да се представят сертификат от типово изпитание, включително температурната зависимост на метрологичните грешки и декларация за съответствие, както с всяка доставка така и при промяна на версията на продукта от производителя.
Електромерът може да бъде и одобрен за ползване в България посредством списване в регистъра на средствата за търговско измерване .

6.2. Параметризиращ софтуер

Нужен е лиценз за параметризиращ софтуер, снабден с всички налични функции на предложения електромер. Със закупуването на електромера е нужно да се предостави и параметризиращия софтуер, така че да е възможна пълна съвместимост и функционалност с различните версии на параметрите. Лицензът трябва да включва всички софтуерни актуализации за времето на живот на електромера.
Носителят на инсталационните файлове може да е свободно избран (CD, USB и др.)носител.
При необходимост трябва да се проведе обучение относно работата със софтуера, задаване на параметрите и необходимата обработка на данните.
Необходимо е да се посочи лице за контакт.
Параметризиращият софтуер трябва да бъде проектирана така, че достъпът до електромера през сервизния интерфейс да е възможен. Следователно да се обърне внимание на възможността на криптиране на връзката с електромерите.

6.3. *Възможност за влизане в тестов режим

Статус на тестовия режим (вкл. или изкл.) за калибриране трябва да бъде видимо показан на електромера чрез сервизния интерфейс и дисплея.
Необходими са следните команди, които да могат да бъдат подадени от тестовото устройство чрез сервизния интерфейс и изпълнени от електромера:
a) Тестов режим ВКЛЮЧЕН
b) Тестов режим ИЗКЛЮЧЕН
c) Настройка на час/дата
d) Увеличаване на константата на светодиода (за метрологична проверката)
e) Тест на дисплея (опционално)
f) Превключване на светодиода за активна/реактивна енергия (по желание)
g) Самоотчет (по желание)
h) Превключване на тарифи за измерване на енергия и мощност (по желание)
i) Реле за управление ВКЛЮЧЕНО (Без Позиция 3)
g) Реле за управление ИЗКЛЮЧЕНО (Без Позиция 3)

6.3.1. Светодиод

Със стандартна оптична глава трябва да е възможно снемането на импулси по всяко време.
За предпочитане е използването на червени и зелени светодиоди. LED-изпълнението трябва да гарантира безпроблемното снемане на импулси с оптични глави, които могат да бъдат задействани на разстояние от 30mm. Тази функция трябва да е гарантирана при еталонирани (затворени) електромери. Ако налице е само един светодиод върху електромера трябва да е възможно превключването на импулсите между активна и реактивна енергия и обратно чрез IR команда. Алтернативно, възможно е наличието на два светодиода (за активна/реактивна енергия).

6.3.2. Разположение на светодиодите и IR-интерфейса.

electricity meter, the LED to be calibrated and the IR-interface must be positioned in such a manner, as to enable the simultaneous inspection, respectively calibration of the electricity meter using these two elements.

6.3.3. Sensitivity requirements and error allowances

The requirements, regarding the warm-up times, the values for the effects and the error allowances are determined in accordance with the requirements of the BMI on the inspection of Electricity Meters.
The additional errors in case of a temperature rise must be specified in the test report.

The electricity meters must meet these requirements, especially with respect to adhering to the admissible error allowances.
The electricity meters must be manufactured in such a manner that to enable the automatic inspection of metering points with standard test equipment.

6.3.4. Inspection of the behaviour in operating mode
In operating mode the electricity meter must meet EN 62053-21 and the relevant requirements established in the Bulgarian Metering and Measurement Act.
The electricity meters must be designed and manufactured so that it is possible to perform both automatic inspection of the operating mode (by means of a LED) with the respective testing equipment, as well as inspection by means of visual control (e.g. the arrow indicating the power flow direction on the display).
The LED constant must be designed so that during a start-up test, at least 2 pulses can be registered in 10 minutes.
6.3.5. Inspection of the behavior of the electricity meter in idle mode
In idle mode, the electricity meter must meet EN 62053-21 and the relevant requirements, set out in the Bulgarian Metering and Measurement Act.
The minimum duration of the test is calculated, applying the formula below.
During that test, at the output of the electricity meter not more than one pulse is to be registered.

$$\Delta t \geq \frac{600*10^6}{k*m*Un*\mathrm{Im}ax} = [\mathrm{min}]\,forClass1$$

$$\Delta t \geq \frac{480*10^6}{k*m*Un*\mathrm{Im}ax} = [\mathrm{min}]ForClass2$$

k = Constant of the pulse output
m = Number of metering systems
Un = Rated voltage
Imax = Rated current

The electricity meter must be designed and manufactured so that it is possible to perform both automatic inspection of the idling (by means of a LED), as well as inspection by means of visual control of the electricity meter. The LED must always be on, when the electricity meter has no load.
6.3.6. Stability of the pulses of the LED
The calibration of the electricity meters requires pulses, proportional to the power.
6.3.7. *Test mode
The electricity meter must have a calibration mode. In this mode, the energy counters must have 3 digits after the

За да се създаде възможност, за безпроблемно автоматично калибриране на електромера, предвиденият за калибрирането светодиод от една страна и IR-интерфейса от друга страна трябва да бъдат така разположени, че да може да се извърши едновременна проверка, респективно калибриране на електромера чрез двата елемента.
6.3.3. Изисквания за чувствителност и допустими граници на грешката
Изискванията към времената на затопляне, величините на влияние и допустими граници на грешките се определят съгласно изискванията на БИМ за проверка на СИ
Допълнителните грешки при краткотрайно затопляне трябва да бъдат посочени в протокола от изпитанието.
Електромерите трябва да отговарят на тези изисквания, особено на спазването на допустимите граници на грешките.
Електромерите трябва да бъдат изработени така, че да е възможна автоматична проверка на измервателни точки със стандарни средства за проверка.
6.3.4. Проверка на поведението в режим на работа
В режим на работа електромерът трябва да отговаря на EN 62053-21 и съответно на утвърдените изисквания в българския Закон за Измерванията.
Електромерите трябва да са така изработени, че да е възможна, както автоматична проверка на режима на работа (посредством LED) със съответна изпитвателна техника, така и проверка чрез визуален контрол (напр. на стрелката за посоката на енергията върху дисплея).
Константата на светодиода трябва да бъде такава, че при стартов тест да е възможно регистрирането на минимум 2 импулса за 10 минути.
6.3.5. Проверка на поведението на електромера в режим на самоход (празен ход)
В режим на самоход електромерът трябва да отговаря на EN 62053-21 и съответно на утвърдените в българския Изисквания на Закон за Измерванията.
Минималната продължителност на теста се изчислява по долупосочената формула. По време на този тест на изхода на електромера не трябва да се регистрира повече от един импулс.

$$\Delta t \geq \frac{600*10^6}{k*m*Un*\mathrm{Im}ax} = [\mathrm{min}]заКлас1$$

$$\Delta t \geq \frac{480*10^6}{k*m*Un*\mathrm{Im}ax} = [\mathrm{min}]заКлас2$$

k = Константа на импулсния изход
m = Брой на измервателните системи
Un = Номинално напрежение
Imax = Номинален ток

Електромерът трябва да бъде изработен така, че да е възможна, както автоматична проверка на самохода (посредством LED), така и проверка чрез визуален контрол на електромера. LED-диодът трябва да свети винаги когато електромерът няма товар.

6.3.6. Стабилност на импулсите на светодиода
За калибриране на електромерите са нужни импулси, пропорционални на мощността
6.3.7. *Тестов режим
Електромерът трябва да има режим за калибриране. В

decimal point (for indirect electricity meters – 4 digits), and when reading the data, the increased resolution of the energy counters must be taken into consideration.)
The increased resolution in the test/calibration mode is required in order to ensure the increased efficiency of the inspection.

6.4. Metering, grid connection

6.4.1. Precision class

Direct connection: at least MID Class A
Indirect connection: at least MID Class B
Optional: for reactive energy Class 2

6.4.2. Two-way metering

It is necessary that the forward and reverse energy is recorded in separate energy logs (as an aggregate and according to tariffs). This applies to both the active, and the reactive power.

6.4.3. Metering, irrespective of the direction of the field

The metering cannot be affected by fields with different rotation directions, which sometimes occur in the grid.

6.4.4. Functionality monitoring (self-diagnostics, watchdog)

The watchdog function is designed to avoid damages to the electricity meter due to software failures. Such damages are avoided as the software notifies from time to time the watchdog function, that it still functions properly. At watchdog's command, the software is restarted. If the precision of the energy logs is disturbed, it is necessary to restore the values from the last 15 minute period before the error. Each restart of the watchdog timer must be recorded in the event logbook. The restarting must not take more than 10 seconds.

IV. Data Concentrator

1. General requirements

1.1. Definition

The data concentrator is a compact device, which performs two-way data communication through PLC resp. wireless connection (interface P1) and the transfer of data stored, through remote interface (interface P4). These interfaces are used to transfer all data, commands and signals between the Head End System and the end devices.

Apart from that the data concentrator has a local interface for maintenance (P3) for setting the parameters, configurations and reading data.

Table 1: General requirements regarding Data Concentrator

Technical details	Minimum requirements
Installation	• Capabilities for installation through a DIN-bus or a three-point connection to the connection block of the electricity meter
External antenna	• Connection of the external antenna by means of a SMA-connector
Protection	• Minimum IP 40 (according to EN 60529)
Air humidity	• 5% to 90% relative humidity (without condensate)

този режим енергийните броячи трябва да имат 3 знака след запетаята (при индиректни електромери – 4 знака), и при отчитането на данните, увеличената резолюция на енергийните броячи трябва да се отчита.)
Увеличената резолюция в режим на тест/калибриране е нужна с цел по ефективна проверка.

6.4. Измерване, свързване към мрежата

6.4.1. Клас на точност

Директно свързване: най-малко MID Клас A
Индиректно свързване: най-малко MID Клас B
По желание: за реактивна енергия Клас 2

6.4.2. Двупосочно измерване

Нужно е енергията в права и обратна посока да се отчита в отделни енергийни регистри (сумарно и по тарифи). Това е валидно както за активната, така и за реактивната енергия.

6.4.3. Измерване, независимо от посоката на въртене на полето

Измерването не трябва да се влияе от полета с различни посоки на въртене, които понякога се появяват с мрежата.

6.4.4. Мониторинг на функционалността (самодиагностика, watchdog)

Чрез използването на watchdog функцията трябва да се предотврати повреда на електромера чрез отказ на софтуера. Тази повреда се избягва като софтуера периодично уведомява watchdog функцията, че все още работи правилно. По команда на watchdog функцията е необходимо да се направи рестарт на софтуера. Ако точността на енергийните регистри е нарушена е нужно да се върнат стойностите от последният 15 минутен период преди грешката. Всеки рестарт на watchdog таймера трябва да се запише в дневника на събитията. Рестартирането не трябва да трае повече от 10 секунди.

IV. Концентратор на данни

1. Общи изисквания

1.1. Дефиниция

Концентратор на данниа е компактно устройство, което осъществява двупосочна комуникация на данни чрез PLC респ. безжична връзка (интерфейс P1) и прехвърлянето на съхранените данни чрез дистанционен интерфейс (интерфейс G4). Чрез тези интерфейси се трансферират всички данни, команди и сигнали между централната система и крайните устройства.

Освен това Концентратор на данниа има локален интерфейс за поддръжка (P3) за настройка на параметрите, конфигурации и отчитане на данни.

Таблица 1: Общи изисквания към Концентратор на данни

Технически данни	Минимални изисквания
Монтаж	• Възможности за монтаж през DIN-шина или триточково закрепване за клемния блок на електромера
Външна антена	• Свързване на външна антена посредством SMA-конектор
Защита	• Минимум IP 40 (съгласно EN 60529)
Влажност на въздуха	• 5% до 90% относителна влажност (без конденз)

Power supply	• 3 x 230/400 V (wide range: 140 V to max 260 V) • Safety with a max. 16 A-fuse • Connection up to max 2,5 mm^2 cross section of the conductor
PLC - communication method	• Transfer method, compatible with CENELEC volume A • Connection of up to 1.000 end devices
Software	• Firmware upgrade can be performed both through the remote, as well as through the local interface.
Temperature range	• Operating range: - 25°C to 55°C • Storage and transfer range: - 25°C to 70°C •
Device Interfaces	• P2: PLC, • P3: RS 232, Ethernet • P4: RS 232, Ethernet, interface to a modular GSM/GPRS/UMTS-modem (SMA – connector for connection of the external antennas) • Optional S: RS 232, Ethernet
Conformity with standards	• CE-certification • EN 61000-6-4 • EN 50065-1
Network protocols	• TCP/IP, HTTP, FTP, SCP
Built-in clock module / Time base	• Possible synchronization with NTP (Network Time Protocol) server • Alternative: synchronization with the Head End System

Захранване с напрежение	• 3 x 230/400 V (широк диапазон: 140 V до макс. 260 V) • Обезопасяване с макс. 16 А-предпазител • Свързване до макс. 2,5 mm^2 напречно сечение на проводника
PLC - метод за комуникация	• Метод за прехвърляне, съвместим с CENELEC том А • Подвързване на до 1.000 крайни устройства
Софтуер	• Промяна на фърмуера може да се извърша както през дистанционния, така и през локалния интерфейс.
Температурен диапазон	• Работен диапазон: - 25°C до 55°C • Граничен диапазон за съхранение и трансфер: - 25°C до 70°C
Интерфейси на устройството	• P2: PLC, • P3: RS 232, Ethernet • P4: RS 232, Ethernet, интерфейс към модулен GSM/GPRS/UMTS-модем (SMA – конектор за свързване на външни антени) • Опционално S: RS 232, Ethernet
Съответствие със стандарти	• CE-сертифициране • EN 61000-6-4 • EN 50065-1
Мрежови протоколи	• TCP/IP, HTTP, FTP, SCP
Вътрешен часовников модул / Часова база	• Възможна синхронизация с NTP (Network Time Protocol) сървър • Алтернативно: синхронизация с централната система

1.2 Constructive requirements

1.2.1. General provisions

Based on its structural design and manufacturing, the data concentrator must be designed so that under specific operating and normal conditions of use, no hazards can occur. The following is to be provided in particular:

a) safety of people in case of energizing voltage(the current conducting parts must be properly insulated)

b) safety of people under the effect of high temperature

c) safety and resistance to heat and fire
d) protection against the penetration of solids, dust and water.
All parts, exposed to corrosion under normal operating conditions, must be efficiently protected. The protective layers must have sufficient strength, so that under the specific operating conditions, cannot be damaged by the weather conditions. These requirements are of decisive

1.2. Конструктивни изисквания

1.2.1. Общо положение

Въз основа на своя конструктивен дизайн и производство Концентратор на данни трябва да бъде така проектиран, че при определени експлоатационни и нормални условия на употреба да не могат да възникнат опасности. По-специално трябва да се подсигури следното:
а) безопасност на лицата от попадане под напрежение(тоководещите части да са надежно изолирани)
b) безопасност на лицата при въздействия от повишена температура
c) безопасност и устойчивост на топлина и огън
d) защита срещу проникване на твърди тела, прах и вода.
Всички части, изложени на корозия при нормални условия на употреба, трябва да бъдат ефективно защитени. Защитните слоеве трябва да бъдат толкова

significance for the selection of the protection class.

1.2.2 Housing
Optional: housing, which may be sealed, so that the internal parts of the device are only accessible after breaking the seal(s). The removal of the cover of the housing should not be possible without using tools.

1.2.3 Protection class
It is preferable that the housings are made of recyclable insulating material (resistant to UV-radiation, resistant to the vapours from solvents), corresponding to protection class II.
Protection against the penetration of dust and water.
The concentrator must be of protection class at least IP 51 according to IEC 60529:
1.2.3.1 Weather conditions
The operating temperature and the environmental temperature must be between -20 °C to + 60 °C.
The temperature range during storage must be between -25 °C and + 65 °C.
1.2.3.2 Power supply
Standardized rated voltage: 3x230/400 V; 50 Hz

Range of the allowances of the power supply: The grid part with rated voltage Un = 230 V is to be designed in such a manner that it can operate flawlessly in the following voltage range:

230 +/- 20% Volts; 50 Hz
3-phase power supply with a maximum cross section of the conductor 2,5 mm^2.
The power supply connections are also used to ensure PLC-communication with all 3 phases.
The type of connection of the conductors at the terminals must ensure sufficient and permanent contact. The loosening of the conductors or their excessive heating are to be prevented. Bolted connections, ensuring electric contact, and screws, which can be tightened and loosened many times, during the useful life of the data concentrator, must have a threaded metal bushing.

The risk of corrosion, due to the different contact materials, must be minimized by means of a proper selection of these materials.
The electric connections must be performed in such a manner that the contact pressure is not determined by the insulation material.
1.2.4 Frequency
The concentrator must be designed for rated frequency 50 Hz. They must operate flawlessly in the range of the allowances of ±2% of the rated frequency.

When connecting terminals with various potentials, near each other, these are to be secured against accidental short circuit.

1.2.5 Reverse effects within the grid
The data concentrator (incl. network device and modem) must be designed so that no excessive reverse effects may occur in the grid as higher harmonics. The observation of EN 61000-3-2 must be ensured.

1.2.6 Protection against power surges
The data concentrator must be inspected using a surge of peak voltage 1,2/50 µs according to EN 61000-4-5 Control level of sensitivity 3 with a maximum value of 2 kV (the

устойчиви, че при определените условия на работа да не могат да бъдат повредени от атмосферните условия. Тези изисквания са от решаващо значение за избора на клас на защита.
1.2.2 Корпус
Опционално: корпус, който може да се пломбира, така че вътрешните части на уреда да са достъпни само след счупване на пломбата(ите). Отстраняване на капачката на корпуса не бива да бъде възможно без използването на инструмент.
1.2.3 Клас на защита
За предпочитане е корпусите да бъдат изработени от рециклируем изолационен материал (устойчив на UV-светлина, устойчив на изпаренията от разворителите), съответстващ на клас на защита II.
Защита срещу проникване на прах и вода.
Концентраторът трябва да разполага с най-малко IP 51 клас на защита съгл. IEC 60529:
1.2.3.1 Климатични условия
Работната температура и температурата на околната среда трябва да бъдат между -20 °C до +6 0 °C.
Диапазонът на температурата при съхранение трябва да е между -25 °C до + 65 °C.
1.2.3.2 Захранване
Стандартизирано номинално напрежение: 3x230/400 V; 50 Hz
Диапазони на допустимо отклонение на захранването:
Мрежовата част с номиналното напрежение Un = 230 V за предпочитане трябва да бъде така проектирана, че да може да се експлоатира безупречно в следния диапазон на напрежение:
230 +/- 20% Волта; 50 Hz
3-фазно захранване с максимум 2,5 mm^2 напречно сечение на проводника.
Захранващите връзки служат и затова, PLC-комуникация да се осъществява във всички 3 фази.
Видът на закрепване на проводниците в клемите трябва да осигури достатъчен и постоянен контакт. Трябва да е предотвратено разхлабването на проводниците или прекомерното им загряване. Болтови връзки, които правят електрически контакт, и винтове, които могат да бъдат многократно затягани и разхлабвани по време на полезния живот на Концентратор на данниа трябва да имат втулка (букса) с резба от метал.
Опасността от корозия поради различни контактни материали следва да бъде сведена до минимум чрез правилен подбор на тези материали.
Електрическите връзки трябва да бъдат изпълнени така, че контактното налягане да не се определя от материала на изолацията.
1.2.4 Честота
Концентраторът трябва да бъде конструиран за номинална честота 50 Hz. Трябва да могат да се експлоатират безупречно в диапазона на допустимо отклонение от ±2% от номиналната честота.
Присъединителни клеми с различни потенциали, които са поставени близо една до друга, трябва да бъдат обезопасени против случайно късо съединение.
1.2.5 Мрежови обратни въздействия
Концентратор на данниа (вкл. Мрежови уред и модем) трябва да бъде така проектиран, че в мрежата да не възникват недопустимо високи обратни въздействия под формата на висши хармоници. Следва да се гарантира спазването на EN 61000-3-2.
1.2.6 Защита от ударно напрежение
Концентраторът трябва да се проверява с вълна на

preferred sensitivity level is 4 at 4 kV).

1.2.7 Electromagnetic compatibility
Must meet the requirements according to EN 61000-4-3. The data concentrator must be capable of suppressing radio interferences. It must not affect the grid parts by external electric and magnetic fields, which can usually be expected at the operating locations.

1.2.8 Technical data plate
At least the following information must be included, clearly visible when the device is installed – without the use of any other auxiliary devices:

1.2.8.1. Unique device number
1.2.8.2. Barcode in accordance with the grid operator's specifications
1.2.8.3. Labeling the manufacturer and type
1.2.8.4. Description of LEDs with statuses
1.2.8.5. Manufacturing year
1.2.8.6. Connection diagram
1.3 Interfaces
1.3.1. WAN interface (P5)
1.3.1.1. GSM/GPRS/UMTS - modem
The GSM/GPRS/UMTS-modem is an integrated or modular replaceable communication unit. In general the modular/replaceable solution is preferred.

TABLE 2: MINIMUM REQUIREMENTS - MOBILE RADIO-MODEMS

Technical details	Minimum requirements
Operating voltage	230 +/- 20% Volts; 50 Hz
Functionality	GSM/GPRS/UMTS-module for GSM-grids

THE GSM/GPRS/UMTS-MODEM MUST AT LEAST HAVE THE FOLLOWING INDICATIONS:
a) Unique device number
b) Barcode in accordance with the grid operator's specifications
c) Labeling the manufacturer and type
d) Manufacturing year
1.3.1.1.1. Modem functionality
The GSM/GPRS/UMTS-module must be suitable for all the GPRS-grids, currently in operation in Bulgaria. The output power must be at least 2W. The sensitivity must be -108 dBm the data transfer through the GSM-grid, must take place, using a minimum of 9600 Baud (V.32bis). The data must be compressed.

1.3.1.1.2. SMA – connector
It is preferable to provide a SMA-coupling for connection of the external antennas to the data concentrator, resp. the GSM/GPRS/UMTS-modem.
1.3.1.1.3. Selection of the operator of the mobile network
In the borderline areas, where several operators of mobile radio networks intersect, it is necessary to select the operator of the mobile radio network (blocking international roaming). However, in general, the modem must select the operator of the mobile radio network with the strongest signal in the region.

ударно напрежение 1,2/50 μs съгл. EN 61000-4-5 Контролна степен на чувствителност 3 при максимална стойност от 2 kV (за предпочитане степен на чувствителност 4 при 4 kV).
1.2.7 Електромагнитна съвместимост
Трябва да отговаря на изискванията съгласно EN 61000-4-3. Концентратор на данни трябва да може да подтиска радиосмущенията. Не бива да оказва влияние върху мрежовите части чрез външни електрически и магнитни полета, които обикновено могат да се очакват в местата на експлоатация.
1.2.8 Фирмена табелка за технически данни
Върху уреда трябва да се нанесат минимум следните обозначения, които да бъдат добре четливи и в монтирано състояние на уреда - без използването на други помощни средства:
1.2.8.1. Уникален номер на уреда
1.2.8.2. Баркод в съответствие със спецификациите на мрежовия оператор
1.2.8.3. Обозначаване от производителя и типа
1.2.8.4. Описание на LEDs със статуси
1.2.8.5. Година на производство
1.2.8.6. Схема на свързване
1.3 Интерфейси
1.3.1 WAN интерфейс (P5)
1.3.1.1 GSM/GPRS/UMTS - модем
Под GSM/GPRS/UMTS-модем се разбира интегрирана или модулно заменяема комуникационна единица. Принципно се предпочита модулно/ заменяемо решение.

ТАБЛИЦА 2: МИНИМАЛНИ ИЗИСКВАНИЯ МОБИЛНИ РАДИОМОДЕМИ

Технически данни	Минимални изисквания
Оперативно напрежение	230 +/- 20% Volts; 50 Hz
Функционалност	GSM/GPRS/UMTS-модул за GSM-мрежи

GSM/GPRS/UMTS-МОДЕМЪТ ТРЯБВА ДА ИМАТ ПОНЕ СЛЕДНИТЕ ОБОЗНАЧЕНИЯ:
a) Уникален номер на уреда
b) Баркод в съответствие със спецификациите на мрежовия оператор
c) Обозначаване от производителя и типа
d) Година на производство
1.3.1.1.1 Функционалност на модема
GSM/GPRS/UMTS-модулът трябва да е подходящ за всички GPRS-мрежи, намиращи се в експлоатация в България. Изходната мощност трябва да бъде максимум 2W. Чувствителността трябва да бъде -108dBm. Прехвърлянето на данни чрез GSM-мрежата трябва да се извърши с минимум 9600 Baud (V.32bis). Трябва да се извърши компресиране на данните.
1.3.1.1.2 SMA – конектор
За предпочитане е да се предостави SMA-букса за свързване на външни антени към Концентратор на данниа съотв. GSM/GPRS/UMTS-модем.
1.3.1.1.3 Избор на оператора на мобилната мрежа
В граничните райони, където се пресичат няколко оператора на мобилни радиомрежи, е необходимо да се избере операторът на мобилната радиомрежа (блокиране на международен роуминг). По принцип

1.3.1.1.4. Parameterization

The modem must be provide software parameterization settings or a terminal program. The respective adjustments must be accessible remotely. The parameterization must not be lost in case of power failure or loss of voltage. It must be possible to configure minimum 2 different APN settings.

1.3.1.1.5. Resetting

The modem must also perform an automatic reset of the GSM/GPRS/UMTS- module after certain time, preset by the user, so that in case of failure of the modem, the connection can be established again. If there are other options, these must be specified in the tender.

1.3.2. Interface to end devices - Last Mile (C)F

In order to ensure the communication channels, data regarding the remote reading must be provided, such as signal level, signal-to-noise ratio, noise level, bit errors ratio, table of routes, non-reading electricity meters, at what phase a certain electricity meter is installed.

1.3.2.1. PLC

Communications technique using high frequency signals to transmit data over. Typical interface technologies are narrowband PLC communication networks, local wired networks. Regardless of the network paths of the specific implementation, special care on the security of the C interface is necessary to prevent unauthorized monitoring or intervention (see also Clause 5 Privacy and Data security).

1.3.3. Service interface (P3)

The data concentrator must have an interface, allowing, in case of inactive remote interface (due to an issued with a supplier or technical problems), taking into consideration preset access rights, the following commands/actions to be performed on the data concentrator, as well as on the connected end devices:

a) Reading data
b) Setting the clocks of the subordinate devices - according to those of the data concentrator
c) Configuring the devices
d) Firmware update

1.3.3.1. Ethernet interface
1.3.3.1.1. 10/100 Base-T standard.
1.3.3.1.2. LAN RJ-45 standard jack
1.3.3.1.3. For a connection of category 5 cables
1.4. Execution
1.4.1 Commissioning

In general, after establishing the communication, the data concentrator must initialize and carry out self-identification and automated inspection of the authenticity with the Head End System, in accordance with the framework security conditions. The time for establishing the communication with the remote interface must not exceed one hour.

1.4.2 On-site operational inspection

The data concentrator must have indication capabilities, displaying the most important operating conditions of the electricity transmission line and remote communication by means of LED indicators. The plate must clearly differentiate, by using symbols or names, the PLC and the

обаче модемът трябва да избере оператора на мобилна радиомрежа с най-силен сигнал в региона.

1.3.1.1.4 Параметризация

Модемът трябва да може се настройва със софтуер за параметризация или терминална програма. Това трябва да бъде възможно и от разстояние. Параметризацията не трябва да се загубва в случай на отпадане на напрежението или прекъсване на захранването. Трябва да бъде възможно конфигуриране едновременно на минимум 2 различни APN настройки.

1.3.1.1.5 Reset (нулиране)

Модемът също така трябва да извърши автоматичен Reset на GSM/GPRS/UMTS-модула след зададено от потребителя време, така че при срив на модема след това отново да може да се осъществи връзка. Ако има други възможности, те трябва да бъдат посочени и описани в офертата.

1.3.2. Интерфейс към крайни устойства Last Mile (C)

За гарантиране качеството на комуникационните канали трябва да се осигурят за дистанционно отчитане данни като например ниво на сигнала, съотношение сигнал-шум, ниво на шума, коефициент грешки в битове, таблици за маршрути,не отчитащи се електромери, на коя фаза е монтиран даден електромер.

1.3.2.1. PLC

Комуникационии техники използващи високочестотни сигнали за пренос на данни. Типични технологии за интерфейс са теснолентова PLC комуникационни мрежи. Независимо от мрежови пътища на конкретното изпълнение следва да се осигури специално внимание върху сигурността за превенция върху неоторизиран мониторинг или интервенция (виж също клауза 5 от част Сигурност и защита на данните).

1.3.3. Сервизен интерфейс (P3)

Концентраторът на данни трябва да разполага с интерфейс, който да позволява, при неактивен дистанционен интерфейс (поради проблем с доставчик или технически проблем), като се вземат предвид предварително зададени права за достъп, да се извършват следните команди/действия върху Концентратор на данни, както и на присъединените крайни устройства:

a) Отчитатане на данни
b) Сверяване на часовниците на подчинените устройства- според тези на Концентратор на данни
c) Конфигуриране на устройства
d) Промяна фърмуера

1.3.3.1. Ethernet интерфейс
1.3.3.1.1. 10/100 Base-T стандарт.
1.3.3.1.2. LAN RJ-45 стандартна букса
1.3.3.1.3. За връзка с кабели категория 5
1.4. Изпълнение
1.4.1 Въвеждане в експлоатация

По принцип Концентратор на данниа след създаване на комуникационна връзка трябва да инициализира и извърши самоидентификация и автоматизирана проверка на автентичността с централната система в съответствие с рамковите условия за сигурност. Времето за създаване на комуникация на дистанционния интерфейс трябва да се извърши в рамките на един час.

1.4.2 Оперативна проверка на място

Концентратор на данни трябва да разполага с възможности за индикация, които могат да указват най-

status displayed as a result of the remote communication, in order to avoid any confusion.

In case of GSM/GPRS/UMTS-communication the level of the signal and any error messages are to be displayed.

1.4.3 Execution
The PLC network is organized independently, according to the framework conditions, set by the respective PLC system. It is possible to carry out both the PUSH and PULL commands automatically or manually.
In order to reduce the online time of communication between the data concentrator and the Head End System, the order of execution of the requests must be, as follows:
1.4.3.1. Establishment of a communication link between the Head End System and the data concentrator.
1.4.3.2. Transmission of the reading command to all the electricity meters, connected to the data concentrator

1.4.3.3. Closing the communication link between the Head End System and the data concentrator
1.4.3.4. The data concentrator establishes a communication link with the Head End System
1.4.3.5. Transfer of all data from the data concentrator to the Head End System. After the successful transfer, the data is erased from the memory of the Data concentrator.
1.4.4. Firmware update
By means of a remote interface it is possible to replace some parts of the software or the firmware. This process must be fully transparent. The safety aspect and the related volume of the keys must function even during firmware download.

The acceptance of new firmwares shall take place after the automatic inspection, whether the hardware components are compatible with the planned download. The control processes and automatic tests are to be provided. Routine inspections for damages and self-tests are provided.
The restoration of the system to the previous software must take place automatically in case of errors. In this case the newly installed firmwares must be deleted. This is to be communicated to the central control system.

V. IT security requirements for distant meter reading and control system for EVN EP (EVN Bulgaria Elektrorazpredelenie EAD)/Contracting Authority

Definitions of expressions:
E-Meter – Intelligent electricity meter, which is connected to the distribution grid and uses communication technologies for data exchange with central software platform. This is technical device which is measuring energy consumption and uses latest modern technologies for remote data transfer in both directions.

Central system - It is an aggregation expression for software of all systems which are responsible for the

важните експлоатационни състояния на електропровода и дистанционна комуникация посредством LED индикатори. На табелката трябва да има ясно разделение чрез символи или наименования между PLC и статуса показания от дистанционната комуникация, за да се избегнат объркванията.
В случай на GSM/GPRS/UMTS-комуникация трябва да бъдат показани нивото на сигнала и съобщения за грешки.
1.4.3 Изпълнение
PLC мрежата се организира самостоятелно според рамковите условия, които задава съответната PLC система. Възможно е автоматично или ръчно да се извършват както PUSH, така и PULL команди.
За да се намали онлайн-времето за комуникация между Концентратор на данни и централната система, редът на изпълнение на заявките трябва да бъде както следва:
1.4.3.1. Изграждане на комуникационна връзка между централната система и Концентратор на данни
1.4.3.2. Предаване на командата за отчитане към всички електромери, присъединени към Концентратор на данни
1.4.3.3. Приключване на комуникационната връзка между централната система и Концентратор на данни
1.4.3.4. Концентратор на данниа изгражда комуникационна връзка към централната система
1.4.3.5. Прехвърляне на всички данни от Концентратор на данниа към централната система. След успешно прехвърляне, данните се изтриват от паметта на Концентратор на данни.
1.4.4. Смяна на фърмуера
Посредством дистанционния интерфейс е възможно да се заменят някои части на софтуера или фърмуера.Този процес трябва да бъде напълно прозрачен. Аспектът на безопасност и с това свързания обмен на ключове трябва да функционират дори и при фърмуер даунлоуд.
Приемането на новия фърмуер става само след автоматична проверка дали хардуерните компоненти са съвместими за планирания даунлоуд. Трябва да бъдат осигурени рутинни процедури за проверки и самостоятелни тестове.

Връщане към предишния софтуер трябва да се извършва автоматично в случай на грешка. В този случай новоинсталираният фърмуер трябва да бъде изтрит.Всяка грешка при промяна на фърмуера трябва да се отрази в централната системата.

V. Изисквания за сигурност за дистанционно отчитане на електромери и системи за управление за ЕВН ЕР (ЕВН България Електроразпределение ЕАД)/Възложителя

Дефиниции и изрази:
Е-електромер – Интелигентен електромер, свързан с разпределителната мрежа разпределителната мрежа и използващ комуникационни технологии за обмен на данни с централна софтуерна платформа. Това представлява техническо устройство, което измерва потреблението на електроенергия и ползва най-модерните технологии за дистанционен пренос на данни и в двете посоки.
Централна система – това е общ израз за софтуера, касаещ всички системи, които отговарят за администрирането и управлението на Е-електромерите.

administration and management of E-Meters. In that aspect it can include Head End System (HES) for control and provisioning of electrometers, module for management of collected meter information data, technology for data validation and reporting, interfaces with existing legacy application stack of the Contractor and adequate module (service) for managing the cryptographic techniques in order to guarantee the resistance towards the cyber-attacks in process of communication/data exchange with E-Meter and concentrator.

Concentrator – It is a device which is responsible for PLC (power line communication) with the E-Meter and supports the data transport through GPRS environment to the Central system in both directions.
HHU – Portable handheld unit which can be used for maintenance tasks of Concentrator or E-Meter.

PLC – Power line communication which is compatible with European regulations.(CELENEC)

End-To-End Security – means, that the whole communication between the endpoints (endpoints lay in the central system and the E-Meter) is secured. It must not be possible for an unauthorized person to read or manipulate the transferred information.

Cryptographic Service – Will be a part of the central system. The cryptographic service can be an additional application within the central system or the functionality can be provided by another application (e.g. by the HES). The cryptographic service should provide additional mechanism to support the end-to-end security within the distant meter reading and control system and should also provide mechanism for secure storing the used cryptographic keys.

Cryptographic key – is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. This key remains private and ensures secure communication. Cryptographic keys could be symmetric or asymmetric. Symmetric encryption requires only one key, which is used to encrypt and decrypt data. Asymmetric encryption uses two different keys: one for encryption and one for decryption.

1. General architecture of distant metering and control system:
1.1 The transfer environment of metering data from E-Meter must be realized with GPRS or PLC (power line communication). The technical module which is responsible for communication with E-Meter must be installed in the same corpus of E-Meter. In case of usage of PLC communication, a Concentrator must be a part of communication chain with the E-Meter which must be capable to transfer/collect data and communicate with many E-Meters and after that to transfer the data to the Central system. The Concentrator must be able to use GPRS communication environment or Ethernet connection for establishing transfer channel with the Central system. The Central system must provide a cryptographic service with which the data transfer to/from Concentrator and E-Meter to be encrypted. The central system must support the encrypted storage of the unique E-meter cryptographic

В тази връзка, терминът може да включва, Главна система /Head End System (HES)/ за управление и осигуряване на електромери, модул за управление на събраните данни с информация от електромерите, технология за валидиране и отчитане на данни, интерфейси със съществуващите системи на изпълнителя и подходящи модули (обслужващи) за управление на криптографските техники, за да се гарантира устойчивостта срещу кибер атаки в процеса на комуникация/обмен на данни с Е-електромера и концентратора.
Концентратор – Това е устройство, което отговаря за Комуникацията по силовия кабел /PLC/ с Е-електромера и подпомага преноса на данни чрез GPRS среда до Централната система в двете посоки.
Преносим терминал – преносим ръчен уред, който може да се използва за извършване на дейности, свързани с поддръжката на Концентратора или Е-електромера.
PLC – Комуникация по силовия кабел, която е съвместима с европейските регламенти и нормативни разпоредби.(CELENEC)
Безопасност от край до край – означава, че е обезопасена цялата комуникация между крайните точки (крайните точки са в централната система и електромера). Не трябва да е възможно неопълномощени лица да отчитат или да манипулират пренесената информация.
Криптографско обслужване – ще бъде част от централната система. Криптографското обслужване може да бъде допълнително приложение в централната система или функционалността може да се осигури от друго приложение (напр. от HES). Криптографското обслужване следва да предоставя допълнителен механизъм, който да поддържа сигурността от край до край в рамките на системата за дистанционно измерване и управление и също така следва да осигури механизъм за безопасно съхраняване на използваните криптографски ключове.
Криптографски ключ – е редица битове, използвани от криптографски алгоритъм за преобразуване на обикновен текст в шифрован и обратното. Този ключ остава таен и гарантира сигурна комуникация. Криптографските ключове могат да бъдат симетрични или асиметрични. Симетричното криптиране изисква само един ключ, който се използва за криптиране и декриптиране на данни. Асиметричното криптиране използва два различни ключа: един за критпиране и един за декриптиране.
1. Обща архитектура на системата за дистанционно измерване и управление:
1.1. Средата за пренос на данните от измерването, получени от Е-електромерите, трябва да се реализира посредством GPRS или PLC (комуникация по силов кабел). Техническият модул, който отговаря за комуникацията с Е-електромера, трябва да бъде монтиран в корпуса на Е-електромера. При използване на PLC комуникация, Концентраторът трябва да бъде част от комуникационната верига с Е-електромера, който трябва да може да пренася /събира данни и да комуникира с множество Е-електромери и след това да прехвърли данните до Централната система. Концентраторът трябва да може да използва комуникационната среда GPRS за установяване на канал за пренос на данни с Централната система. Централната система трябва да осигури

keys.

2. Description of logical interfaces (see pic.1):

Interface	Description
P0	Infrared (IR) interface through which external maintenance tasks can be performed of E-Meter with external device (HHU).
P1	WAN interface of the meter must be able to handle PLC communication or GPRS communication when a GPRS meter will be used.
P2	PLC interface between data Concentrator and E-Meter.
P3	Interface through which external maintenance tasks can be performed of Concentrator with external device (HHU).
P4	Interface between data Concentrator and Central system using GPRS communication environment or Ethernet.
P5	WAN interface of Central system for communication with Concentrators.
P6	Interfaces for data exchange between Central system and existing legacy systems or third party applications.

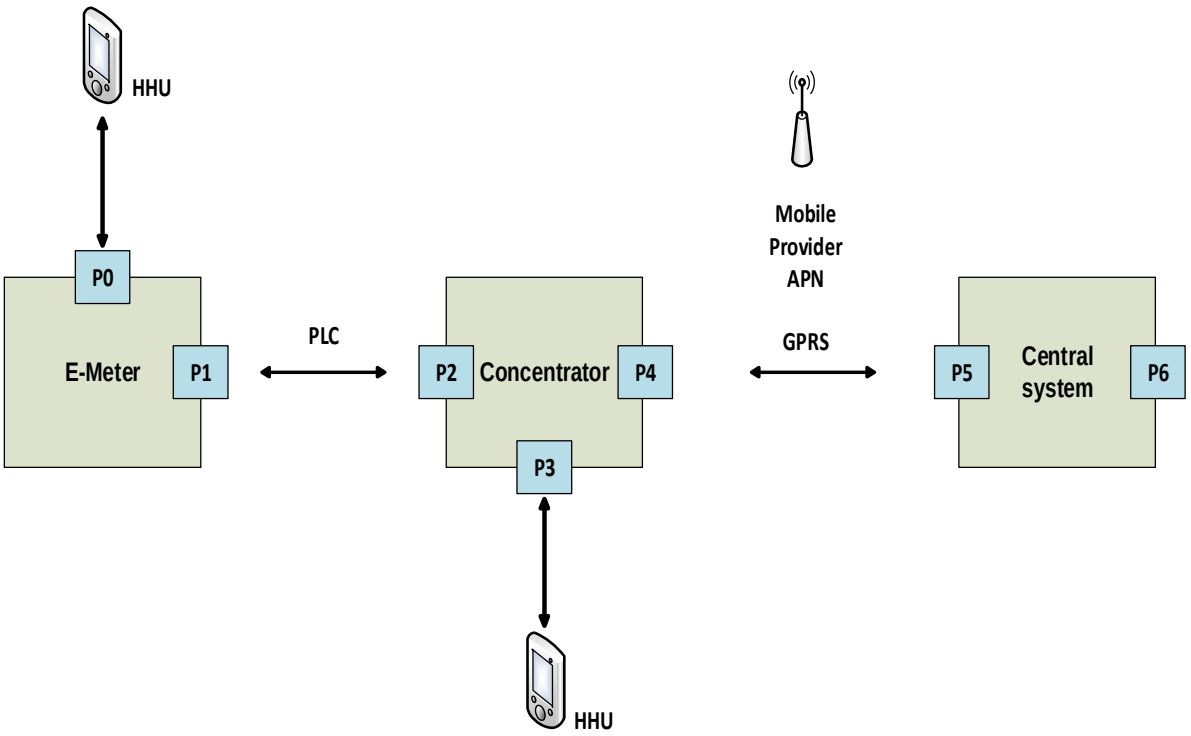
pic.1

криптографските услуги, чрез които преносът на данни до/от Концентратора и Е-електромера ще бъде криптиран. Централната система трябва да подпомага криптираното съхранение на уникалните ключове на Е-електромера.

2. Описание на логическите логически интерфейси (виж илюстрация 1):

Интерфейс	Описание
P0	Инфрачервен (IR) интерфейс, чрез който външни дейности по поддръжка могат да бъдат извършвани с Е-електромера, с помощта на външно устройство (Преносим терминал).
P1	WAN интерфейса на електромера трябва да може да се справи с PLC комуникацията или GPRS комуникация, когато се използва GPRS електромер.
P2	PLC интерфейсът между Концентратора на данни и Е-електромера.
P3	Интерфейс, чрез който могат да бъдат извършвани външни дейности по поддръжка с Концентратор с помощта на външно устройство (Преносим терминал).
P4	Интерфейс между Концентратора на данни и Централната система чрез използване на GPRS среда за комуникация или Ethernet.
P5	WAN интерфейс на Централната система за комуникация с Концентраторите.
P6	Интерфейси за обмен на данни между Централната система и съществуващите системи или приложения на трети страни.

Илюстрация 1



3. Processing sensitive / personal data and IT security.
3.1. Data information flow which is not needed must be not saved or recorded.
3.2. Saved information which is not anymore important / needed must be deleted.
3.3. Sensitive/personal data from E-Meter must be able maximum within 12 hours to be transferred and saved in Central system.
3.4. Without permission, the unauthorized access to the data flow must be strictly prohibited.
3.5. Unauthorized access to the protected channels (communication interfaces) must be not possible.

3.6. The E-Meter must deliver reading out information from its registers if it is requested, with exception of alarms and defined critical events.

3.7. In case of unexpected intervention in the data flow shown in pic.1 the grid operator must be alerted from a monitoring mechanism implemented in the central system.

3.8. Passwords and cryptographic keys must be unique for each E-Meter in the process of exploitation from Central system.

3.9. Commands for switch-off and switch-on for each E-Meter must be unique, encrypted and coded with the proper keys related to deployed cryptographic service.
3.10. IT security must be able to be managed from grid operator (distribution system operator).

3.11. The design and architecture of implemented IT security solution must be provided from bidder to EVN EP and also related processes in order to be able to be audited either from Contractor, or either from third party company. EVN EP will treat the received information with respected confidentiality.

4. The bidder (vendor) must support the audit of IT security of the whole system by EVN EP or by third party company in case of request from EVN EP.

4.1. In case of third party auditor, it must be independent from the bidder and will be chosen from EVN EP.
4.2. If necessary, the respective bidder must actively support the implementation of IT security audit by providing the necessary information and devices.

4.3. The bidder must provide human resources in the process of auditing the whole system from the contractor.

5. . The following sensitive information must be solely transmitted with secured encrypted connection:

5.1. Personal information such as measurement data, etc.
5.2. Firmware updates.
5.3. Control commands (Switch on/off, set the Power limitation - if available).

5.4. Device settings and configurations.

6. All cryptographic keys must be located (stored) into the Central system, but only within a protected

3. Обработване на деликатни/лични данни и IT сигурност.
3.1. Потокът на данни, които не са необходими, не трябва да бъде запазван или записван.
3.2. Запазената информация, която вече не е важна/необходима трябва да бъде изтривана.
3.3. Деликатни/лични данни от Е-електромер трябва да може в срок от не повече от 12 часа да се прехвърлят и запазват в Централната система.
3.4. Без разрешение, неоторизирания достъп до данните трябва да бъде строго забранен.
3.5. Всякакъв неоторизиран достъп до защитените канали (комуникационни интерфейси) трябва да е невъзможен.
3.6. Трябва да е невъзможно получаването на непоискана информация отчетена от Е-електромерите, освен ако не става въпрос за аларми и предварително определени критични събития.
3.7. В случай на неочаквана намеса в потока данни, както е показан на илюстрация 1 операторът на мрежата трябва да бъде предупреден чрез механизъм за контрол, вграден в Централната система.
3.8. Паролите и криптографския механизъм (ключове) трябва да бъдат уникални за всеки Е-електромер в процеса на експлоатация на Централната система.
3.9. Командите за изключване и включване на всеки Е-електромер трябва да бъдат уникални, криптирани и кодирани с надлежните ключове, свързани с въведените криптографски услуги.
3.10. IT сигурността трябва да може да бъде управлявана от оператора на мрежата (оператора на електроразпределител-ната мрежа).
3.11. Конструкцията и архитектурата на приложеното решение за сигурност трябва да бъде предоставено от Участника на EVN EP, както и свързаните процеси, за да може да бъде подложен на одит от страна на Изпълнителя, или от трета страна. EVN EP третира всяка получена информация строго конфиденциално.

4. Участникът (изпълнителя) трябва да съдейства за одита на IT сигурността на цялата система, осъществяван от EVN EP или от трета страна, в случай, че EVN EP го поиска.
4.1. В случай, че трета страна е одиторът, тя трябва да е независима от участника и се избира от EVN EP.
4.2. Ако е необходимо, съответният участник трябва активно да подпомага въвеждането на одит на IT сигурността като предостави необходимата информация и човешки ресурси.
4.3 Участникът трябва да осигури човешки ресурси в процеса на одитиране на цялата система от страна на Изпълнителя.

5. Посочената по-долу деликатна информация трябва да се изпраща единствено по сигурна криптирана връзка:
5.1. Лична информация, като данни от измервания и т.н.
5.2. Актуализация на Фърмуер.
5.3. Контролни команди (Включване/изключване, определяне на ограничението за мощността – ако има такива).
5.4. Настройки и конфигурации на Устройство.

encrypted area or unexportable.

7. The Concentrator can store in it the cryptographic keys only for communication chain with the Central system and assigned E-Meters behind it. The cryptographic keys must be stored within a protected encrypted area or unexportable.

8. Each command from Central system to the E-Meter must be encrypted and must be executed only once towards the E-meter (Protection from Reply Attacks). Messages are accepted only from authenticated parties.

9. Cryptographic service within the central system:

9.1. All cryptographic methods used within the framework of the security solution (service) must be based on open and public available standards and must be considered by international organizations (like ENISA Document Algorithms Key Sizes and Parameter.

9.2. All used cryptographic algorithms need minimum to have cryptographic strength comparable to AES 128 (the cryptographic strength of an algorithm, for example, can be improved by increasing key lengt

9.3. Unique cryptographic keys must be deployed in each E-Meter from the vendor.

9.4. For already installed E-meters the firmware update must be done in encrypted and secured communication channel. Guarantee must be available that firmware image was not manipulated and was issued by the vendor.

9.5. All passwords, which are implemented for E-Meter and data Concentrator, must meet the following minimum requirements:
9.5.1. Minimum length of 10 character
9.5.2. Composed of lowercase letters, uppercase letters and digit.
9.5.3. Randomly generated and not reproducible.

9.6. Passwords and cryptographic keys must be unique for each device (E-Meter or Concentrator), which are participating the process of encryption and decryption or messages for authentication.

9.7. Passwords and cryptographic keys, which can be used for encryption and decryption messages or for authentication of the communication data flow, must be generated with a cryptographically secure (pseudo) random number generator and not to be able to be reproduced. As an example of a possible implementation is made at this point to the following documents:

9.7.1. NIST Special Publication 800-90A - Recommendation for Random Number Generation Using Deterministic Random Bit Generators.
9.7.2. BSI TR-02102 - Cryptographic module: recommendations and key lengths
This requirement must be obeyed on one hand for the initial

6. Всички Криптографски ключове трябва да бъдат съхранявани в Централната система, но само в рамките на защитената зона и да бъдат криптирани или неподлежащи на извличане.

7. Концентраторът може да се използва за съхраняване на Криптографските ключове, единствено за осъществяване на комуникационна верига с Централната система и съответните Е-електромери към нея. Криптографските ключове трябва да се съхраняват в рамките на защитена зона, криптирани или неподлежащи на извличане.

8. Всяка команда от Централната система към Е-електромера трябва да бъде критпирана и да се изпълнява само веднъж в посока Е-електромера (Защита от атаки чрез повторение). Съобщенията се приемат единствено от удостоверени страни.

9. Криптографски услуги в рамките на Централната система:
9.1. Всички криптографски методи, използвани в рамките на системата за сигурност, трябва да се основават на открити и обществено достъпни стандарти и трябва да бъдат разгледани от международни организации (като Размерите на ключовете и параметрите на алгоритми при криптиране на документи към ENISA).
9.2. Всички използвани криптографски алгоритми трябва да имат най-малко криптографската сила, сравнима с AES 128 (криптографската сила на алгоритъм, напр. може да бъде подобрен чрез увеличаване на дължината на ключа).
9.3. Уникални главни и оперативни ключове трябва да бъдат включени от търговеца към всеки Е-електромер.
9.4. За вече монтираните Е-електромери, актуализацията на фърмуера трябва да се извършва чрез криптирани и сигурни комуникационни канали. Трябва да бъде дадена гаранция, че файлът с фърмуера не е манипулиран и е действително издаден от търговеца (дигитален подпис на файла с фърмуера, липса на неоторизирана промяна на ключа на търговеца в електромера).
9.5. Всички пароли, използвани за Е-електромер и Концентратора на данни, трябва да съответстват на следните минимални изисквания:
9.5.1. Минимална дължина - 10 символа.
9.5.2. Съставени от малки, главни букви и числа.

9.5.3. Генерирани произволно и не подлежащи на възпроизвеждане.
9.6. Паролите и Криптографските ключове трябва да бъдат уникални за всяко устройство (Е-електромер или Концентратор), което взема участие в критпирането и декриптирането или в съобщенията за валидиране.
9.7. Пароли и Криптографските ключове, които могат да бъдат използвани за съобщения за критпиране и декриптиране или за валидиране на комуникационните данни, трябва да бъдат генерирани произволно и да не подлежат на възпроизвеждане. Като пример за възможното използване, насочваме вниманието ви към следните документи:
9.7.1. NIST Специална публикация 800-90A – Препоръки за генериране на произволни числа, чрез използване на

installation and loading of E-Meters and on the other side in case of the regular exchange of keys that are in operation of already deployed E-Meters.

9.8. All passwords which are participating the communication chain from Central system, Concentrator to E-Meter must be possible to be remotely changed from central system. Optional: if necessary, all operational cryptographic keys in the E-Meters could be changed on demand.

9.9. After installing the appropriate component (E-Meter or Concentrator), the initial used passwords must be changed. Optional if necessary all operational cryptographic keys in the E-Meters could be replaced on demand.

9.10. Secure backup and restore of data stored in the cryptographic service in central system must be possible.

9.11. Reporting and monitoring functions and representation of the current operating state of the cryptographic service must be available.
9.12. The cryptographic service should provide the following key management functio
9.12.1. Import of the initial cryptographic keys from vendor, which for the operation of the cryptographic service are required.
9.12.2. Initial loading of cryptographic keys for encryption of communication for each E-meter in the central system database. All keys must be stored in encrypted and protected way into the environment of Central system.

9.12.3. Mutual authentication of E-Meter and Central System.
9.12.4. Encryption and decryption of messages.
9.12.5. Optional must be possible a process of renewing the operational cryptographic keys (key generation and distribution of operational cryptographic keys) from remote central system in case of necessity.

9.12.6 Support for a detailed investigation in case of defective E-Meters.
9.12.7 Operation and maintenance of cryptographic service.
9.12.8 Reporting and monitoring of system status.
9.12.9 Support a general key management procedure, which enables and supports safe operation of the Central system.

9.12.10 In case of successfully change of specific operational cryptographic key in E-Meter, all messages, news, commands which are secured with old key must no longer be accepted.

9.13 Transfer of cryptographic keys to the Concentrator and E-Meter must be done in a way that corresponds to the process of secured shipping (for example SSH,SCP,SFTP,HTTPS or other methods with minimum level of encryption AES 128). During the network communication between the Central system, concentrators and E-meters must be established under method of authentication – password or certificate or public key or symmetric key can be used.

9.14 The cryptographic keys must be incorporated

детерминистични генератори на произволни битове.
9.7.2. BSI TR-02102 - Криптографски модул: препоръки и дължина на ключовете
Това изискване трябва да бъде спазвано при първоначалната инсталация и зареждане на Е-електромерите, като при редовна промяна на ключовете, за вече работещи Е-електромери.
9.8. Всички пароли, които участват в кореспонденцията в рамките на Централната система, Концентратора и Е-електромера трябва да може да бъдат променяни дистанционно от централната система. Незадължителна характеристика: ако е необходимо, всички работни ключове в Е-електромерите могат да бъдат променени при поискване.
9.9. След монтаж на съответния елемент (Е-електромер или Концентратор), първоначално използваните пароли трябва да бъдат сменени. По желание, ако е необходимо, всички Криптографските ключове в Е-електромерите могат да бъдат заменени при поискване.
9.10. Трябва да е възможно сигурно съхранение на резервни копия и съответното възстановяване на данни, съхранявани криптографските части на централната система.
9.11. Трябва да има функции за докладване и контрол и представяне на текущото оперативно състояние на криптографските дейности.
9.12. Криптографската служба осигурява следните основни функции по управление на ключовете:
9.12.1. Въвеждане на първоначалните ключове, които се изискват за криптографските дейности.

9.12.2. Първоначално зареждане на основния и работните криптографски ключове за критпиране на комуникацията по всеки Е-електромер в базата данни на Централната система. Всички ключове трябва да се съхраняват в криптирана форма по защитен начин в базата данни на централната система.
9.12.3. Взаимно валидиране на Е-електромера и централната система.
9.12.4. Критпиране и декриптиране на съобщения.
9.12.5. По желание може да се включи и процес по подновяване на работните криптографски ключове (генериране на ключове и разпространение на работни Криптографските ключове) дистанционно от централната система при необходимост.
9.12.6 Съдействие за подробно разследване дефектни Е-електромери.
9.12.7 Работа с и поддръжка на криптографска услуга.

9.12.8 Отчитане и контрол на статуса на системата.
9.12.9 Съдействие за процедурите по общото управление на ключовете, което позволява и подпомага безопасната експлоатация на Централната система.
9.12.10 В случай, че успешно бъде променен конкретен експлоатационен криптографски ключ в Е-електромер, то не трябва повече да бъдат приемани никакви съобщения, новини, команди, обезопасени със стари ключове.
9.13 Прехвърлянето на Криптографските ключове в Концентратора и Е-електромера трябва да се осъществява по начин, който съответства на процеса по сигурното пазаруване (например SSH, SCP, SFTP ,HTTPS или други методи с минимално равнище на критпиране

(imported) into the cryptographic service in advance defined process in order to be guaranteed the secure management of the keys.

9.15 Each E-Meter must be produced with embedded unique cryptographic keys and in the process of delivery a shipment file (list) must be delivered to EVN EP. The shipment file must contain the list of production information of E-Meters (serial number and etc.) and appropriate cryptographic keys for each E-Meter. The electronic delivery must occur in a defined format and must be transmitted to EVN EP via a secured channel. This delivery will be securely processed subsequently by the cryptographic service of the central system. That shipment file must be encrypted and can be decrypted only from the cryptographic service of Central system. Throughout the delivery process, it must be ensured that no unauthorized third party has an access to the cryptographic keys.

9.16 Optionally after commissioning and deployment of E-Meter, some of the factory embedded cryptographic keys could be replaced with new operational keys which are issued dynamically from the cryptographic service of Central system. The newly deployed keys must be used for operational communication with the E-Meter.

9.17 Optionally the cryptographic service must provide appropriate functions, which must randomly enable a generation of new E-Meter specific cryptographic operational keys, which can be used in the process of exploatation of E-Meter. In case of necessity the Central system (Cryptographic service) must be able to repeat the process of renewing the operational cryptographic keys for each E-Meter.

9.18 The following reporting functions must be available from the cryptographic service:

9.18.1 Periodic reporting must be possible about which key have been changed due to certain criteria in case of dynamic exchange of operational cryptographic keys for E-Meters.

9.19 If E-Meter is deinstalled (decommissioned) and if E-Meter and cryptographic service support a replacement process of operational cryptographic keys, all stored operational cryptographic keys must also be destroyed. Only authorized employees may be able to initiate such a deletion. Unused cryptographic keys must be no longer stored in E-Meter or Concentrator.

9.20 If cryptographic service is allowing a replacement of operational cryptographic keys in the E-Meter, technical and organizational process measures must be possible to reduce the risk of accidental reset of cryptographic keys in E-Meter or Concentrator.

9.21 In case of availability of function for replacing of operational keys a unique process must be executed for deploying operational cryptographic key into a current E-

AES 128). По време на мрежовата комуникация между Централната система, концентраторите и Е-електромерите може да се използва метод на валидиране – парола, сертификат, публичен ключ или симетричен ключ.

9.14 Криптографските ключове трябва да бъдат вградени в криптографската система чрез предварително определен процес, за да може да се гарантира сигурното управление на ключовете.

9.15 Всеки Е-електромер трябва да бъде произведен с вградени уникални Криптографски ключове и в процеса на доставка на EVN EP следва да се представи пътен лист. В пътния лист се съдържа информация за производството на Е-електромерите (сериен номер и т.н.) и съответните Криптографски ключове за всеки Е-електромер. Електронната доставка следва да се осъществи в предварително определен формат и трябва да бъде изпратена на EVN EP по сигурен канал. Тази доставка след това се обработва безопасно от криптографската система на Централната система. Този пътен лист трябва да бъде криптиран и може да бъде декриптиран единствено от криптографската система към Централната система. В рамките на целия процес по доставка трябва да се гарантира, че неоторизирани трети страни няма да имат достъп до Криптографските ключове.

9.16 По желание, след въвеждането в експлоатация и монтажа на Е-електромерите, някои от фабричните Криптографски ключове могат да бъдат заменени с нови работни ключове, които се издават динамично от криптографската система към Централната система. Нововъведените ключове трябва да се използват за оперативната комуникация с Е-електромера.

9.17 По желание криптографската система трябва да осигури необходимите функции, които произволно да осигуряват генерирането на нови специфични криптографски работни ключове за Е-електромерите, като тези ключове могат да се използват в процеса на експлоатация на Е-електромерите. При необходимост Централната система (Криптографската система) трябва да може да повтори процеса по подновяване на работните Криптографски ключове за всеки Е-електромер.

9.18 Криптографската система трябва да има възможност за изготвяне на следните отчети и доклади:

9.18.1 Трябва да е възможно изготвяне на периодични отчети за това, кои ключове са променени, поради определени критерии в случай на динамичен обмен на работните криптографски ключове за Е-електромерите.

9.19 Ако Е-електромерите бъдат демонтирани (изведени от експлоатация) и ако Е-електромерът и Криптографската система предлагат възможност за прилагане на процес по замяна на работните Криптографски ключове, всички запазени работни Криптографски ключове също трябва а бъдат унищожени. Единствено оторизирани служители имат право да инициират подобно унищожаване. Неизползваните Криптографски ключове не трябва да се съхраняват в Е-електромерите или Концентратора.

9.20 Ако Криптографската система може да заменя работните Криптографски ключове в Е-електромера, трябва да съществуват мерки, свързани с техническия и организационен процес, чрез които да се намали риска от случайно анулиране на Криптографските ключове в Е-електромера или Концентратора.

9.21 При наличие на функция за замяна на работните

Meter.
9.22 Cryptographic service is very critical for operation of whole Central system. Cryptographic service must be deployed with high availability architecture. The central system must provide a secure backup and restore capabilities for all stored cryptographic keys.

9.23 Cryptographic service should autonomously work without user interaction. Any operation upon sensitive information or operation of cryptographic service must be done in cooperation of two different employees. Separation of duties must be obeyed. All login attempts and user interactions have to be logged and generated protocol information must be protected against unauthorized manipulation. The log entries must be traceable to a unique user. The cryptographic service must further enable the implementation of different user roles.

9.24 Cryptographic service must generate an alarm in case of unauthorized use. It should provide appropriate reporting and monitoring functionality, which allows monitoring of current operating state.

9.25 The cryptographic service must provide at least the following information:
9.25.1 Current state of cryptographic service – for example initial delivery state, operational information, synchronization with redundant cryptographic service, discovering critical and not critical errors, discovered manipulation attempts as a result of occurred possible security incident, ...)

9.25.2 Detailed listing of all occurred during operation errors (like failed logon attempt with username ABC time XYZ)

9.25.3 Representation of all active cryptographic keys together with appropriate identification description and subsequently comparing mechanism whether redundant crypto module contains all keys too.

9.25.4 Representation of all authorized usernames with the respective designated permissions.

9.26 The access to the user interface (GUI) of the crytographic service must be available only through defined and approved secure computers, if the cryptographic service is embeded as an additional system.
9.27 In the process of provisioning of new releases by the manufacturer (vendor) the following requirements must be fulfilled:
9.27.1 Support for all already used cryptographic methods also in the new release must be available;
9.27.2 Uninterrupted operation is secured in the process of update;
9.27.3 Delivery of documentation in which all new features and changes are documented.

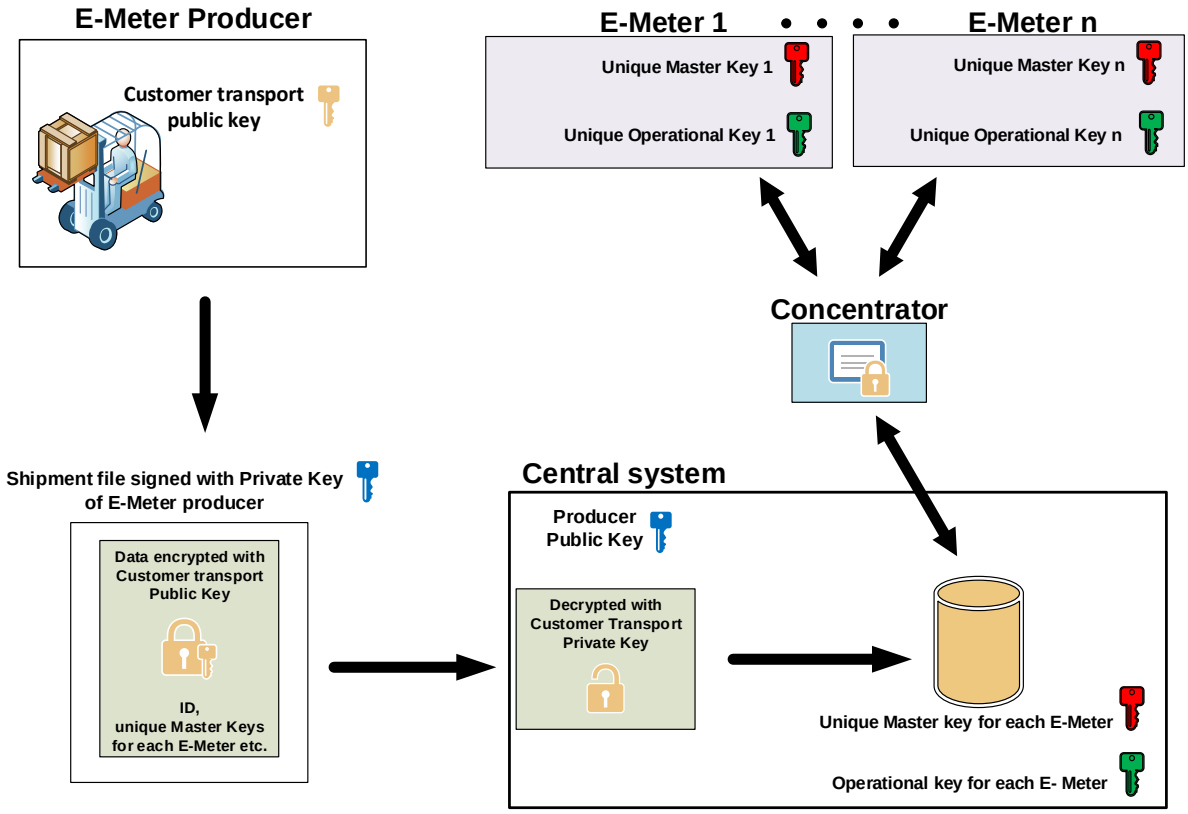
9.27.4 EVN EP itself can decide whether and when a new

ключове, трябва да бъде приложен уникален процес, за прилагане на работни криптографски ключове спрямо действащите Е-електромери.
9.22 Криптографската система е от жизненоважно значение за функционирането на цялата Централна система. Криптографската система трябва да бъде изградена с архитектура,позволяваща висока производителност и достъпност. Централната система трябва да осигури сигурни механизми за запазване и възстановяване на резервни копия за всички запазени Криптографски ключове.
9.23 Ако се въведе криптографска услуга като допълнителна система, то тогава криптографската услуга би следвало да работи самостоятелно, без намесата на потребителя. Всякаква работа, по отношение на чувствителна информация или работа на криптографската услуга, трябва да се извършва съвместно от двама различни служителя. Задължително трябва да се спазва споделянето на задълженията. При опити за влизане в системата и работа с нея трябва да се реализират записи и да се генерират протоколи, които следва да бъдат защитени от неоторизирано манипулиране. Направените записи трябва да бъдат проследяеми до уникален потребител.
Криптографската система трябва да позволява и прилагането на различни роли на потребителите.
9.24 Криптографската система трябва да генерира аларма в случай на неоторизирано използване. Тя трябва да предлага подходяща функционалност за отчетност и контрол, която да позволява контрол на текущото работно състояние.
9.25 Криптографската система трябва да осигурява най-малко следната информация:
9.25.1 Текущо състояние на криптографската система – например – състояние след първоначална доставка, оперативна информация, синхронизиране с допълнителни криптографски системи, откриване на критични и не-критични грешки, открити опити за манипулации в резултат на евентуален възникнал инцидент)
9.25.2 Подробен опис на всички възникнали грешки при работа (напр. успешно извършено запазване на резервно копие – час и дата XYZ, неуспешен опит за влизане в системата с потребителско име ABC – час и дата XYZ)
9.25.3 Представяне на всички активни Криптографски ключове, заедно със съответното описание за идентификация описание и последващо сравнение, за това дали резервния крипто модул също съдържа всички ключове.
9.25.4 Представяне на всички оторизирани потребителски имена със съответните им разрешителни и права.
9.26 Достъпът до потребителския интерфейс (GUI) на криптографската услуга трябва да е възможен единствено чрез определени и доказано сигурни компютри, ако криптографската услуга е внедрена като допълнителна система.
9.27 В процеса на прилагане на нови версии, предоставяни от производителя (продавача), трябва да бъдат изпълни следните изисквания:
9.27.1. Трябва да има поддръжка на всички вече използвани криптографски методи и в новата версия;
9.27.2. Непрекъснатото функциониране е обезпечено по време на процеса на актуализация;
9.27.3. Представяне на документация, в която са

release will be implemented or not.
9.27.5 Training must be provided for the new version

9.28 The Shipment file from the vendor, which must contain (master data of E-Meters, unique cryptographic keys for each E-Meter) must be signed with the private key of the meter manufacturer and encrypted. The received shipment file must be directly imported into the Central system and after that a decryption process to be started. See pic2.

описани всички нови елементи, характеристики и промени.
9.27.4 EVN EP само може да вземе решение дали и кога да приложи определена нова версия.
9.27.5 Трябва да бъде осигурено обучение за работа с новата версия
9.28 Пътният лист от продавача, който трябва да съдържа (основни данни за Е-електромерите, уникални Криптографски ключове за всеки Е-електромер) трябва да бъде подписан със собствения ключ на производителя на електромерите и да бъде криптиран. Получения пътен лист следва да бъде директно въведен в Централната система и след това трябва да започне процесът по декриптиране. Виж илюстрация(Фигура) 2.



Pic.2_Фигура.2

9.29 Optionally the cryptographic service of central system must support implementation of external Hardware Security Module (HSM) for storing cryptographic keys in a secured way.

9.29.По желание криптографската услуга на централната система трябва да поддържа въвеждането на външен Модул за Хардуерна Безопасност (HSM) за съхраняване на криптографски ключове по безопасен начин.

10. General requirements for Concentrator:
10.1 The Concentrator must have only one maintenance interface. (port P3)
10.2 The Concentrator must not be able to be configured through port P2. If there is a compromised E-Meter, it must be not possible to edit the configuration in the Concentrator based upon the credentials from the E-Meter.

10.3 The Concentrator must be able to be configured through port P4 from the central system.
10.4 The configuration of data Concentrator via a local interface port P3 must be adequately protected against attacks.

10. Общи изисквания за Концентратора:
10.1 Концентраторът трябва да разполага само с един интерфейс за поддръжка. (порт 3)
10.2 Концентраторът не трябва да може да бъде конфигуриран през порт P2. При Е-електромер с нарушена сигурност, трябва да не е възможно да се редактира конфигурацията на Концентратора, въз основа на правата и данните за достъп, получени от Е-електромера.
10.3 Концентраторът трябва да може да бъде конфигуриран чрез P4 от централната система.
10.4 Конфигурирането на Концентратора на данни чрез местния интерфейсен порт P3 трябва да бъде достатъчно надеждно защитено от атаки.

10.5 If the Concentrator has to use the local maintenance interface for reconfiguration or other maintenance activities, a unique combination of username and password must be possible for authentication, which corresponds to the defined password policy.(see point 9.5). Record of the event must be logged in it.

10.6 From maintenance port P3 of Concentrator must be not possible to reach protected area of cryptographic keys, which are eventually stored in it.

10.7 The unauthorized attempt for access to a data concentrator must be reported (viewed) by security measures from monitoring service of central system. Record of the event must be logged in it.

10.8 Each concentrator must be able to communicate over PLC technology with at least 1000 pieces of E-meters which are directly assigned to it.
10.9 The credentials for the automatic registration in a mobile network must be unique for every Concentrator. It is not permitted the usage of general login information contained by several units together.

10.10 The credentials for the automatic registration in mobile network may be saved only in Concentrator. The login Information must be not stored in the SIM card itself.

10.11 The mobile service provider will allow traffic only between central system and concentrator. Data traffic between concentrators will be prevented by appropriate routing rules.

10.12 If one data concentrator will be compromised by an attacker, the attacker should not be able to reach other data concentrators from the compromised data concentrator.

11. Performance requirements:
11.1 All installed E-Meters must be read out once per day. In case of E-Meters with load profile, 15 minutes load profile must be read with all 96 values for it. The reading activity has to start at 00:00h and finish till 12:00h at the same day and all read data to be transported in the central system. In addition, event information must be transported within that period to central system.

11.2 The architecture of the Central system must be able to be extended till 1500000 E-Meters with the same KPIs (key performance indicators) defined in point 11.1.

11.3 The success rate shall be minimum 98% of all active E-Meters registered in the central system as defined in point 11.1.

11.4 The cryptographic service is a highly critical component in the future of entire Central system infrastructure. The high availability requirements for the cryptographic service shall be like all components of the E-Meter infrastructure. The availability of the central system environment shall be not less than 99.99% for 24/7/365. (unplanned downtime shall be max. 53 minutes per year)

10.5 Ако се налага Концентраторът да използва местен интерфейс за поддръжка за преконфигуриране или други дейности по поддръжка, уникална комбинация от потребителско име и парола трябва да бъдат използвани за валидиране, като те трябва да съответстват на определената политика за паролите. (виж т. 9.5). Трябва да бъде извършен запис за съответното събитие.
10.6 От порт за поддръжка P3 на Концентратора не трябва да е възможен достъп до защитените зони на Криптографските ключове, които евентуално се съхраняват в него.
10.7 Неоторизирани опити за достъп до Концентратора на данни трябва да бъдат докладвани (разглеждани) чрез мерките за сигурност от направлението за контрол на централната система. Задължително се прави запис в архива за съответното събитие.
10.8 Всеки концентратор трябва да може да комуникира чрез технологията PLC с не по-малко от 1024 бр. Е-електромери, за които отговаря.
10.9 Данните за достъп при автоматична регистрация в мобилна мрежа трябва да бъдат уникални за всеки Концентратор. Не се допуска използване на обща информация за влизане в системата, едновременно от няколко единици.
10.10 Данните за достъп при автоматична регистрация в мобилна мрежа, могат да бъдат запазвани единствено в Концентратора. При използване на SIM карта, информацията за влизане в системата не трябва да бъде съхранявана на самата SIM карта.
10.11 Доставчикът на мобилни услуги следва да допуска трафик единствено между централна система и концентратора. Трафикът на данни между концентраторите се предотвратява чрез подходящи правила за маршрутизация.
10.12 Ако даден концентратор на данни е компроментиран от хакер, не би следвало хакерът да може да стига до други концентратори на данни от компроментирания концентратор на данни.

11. Изисквания относно работните характеристики:
11.1 Показанията от всички монтирани Е-електромери трябва да бъдат снемани веднъж дневно. В случай че Е-електромерите имат профил на товара, трябва да бъде отчетен профила на товара за 15 минути, заедно с всички 96 стойности. Дейностите по отчитането трябва да започват в 00:00 ч и да приключват в 12:00 ч. в същия ден, като всички отчетени данни се прехвърлят в Централната система. Освен това трябва да бъде прехвърлена в централната система информация за събитията през този период.
11.2 Архитектурата на Централната система трябва да може да бъде разширявана до достигане на 1 500 000 Е-електромера с едни и същи основни показатели за дейността (KPI), както е посочено в т. 11.1.
11.3 Процентът на успеваемост трябва да бъде минимум 98% от всички регистрирани в централната системата със статус активни Е-Електромери. както е посочено в т. 11.1
11.4 Криптографската услуга представлява жизненоважен компонент за бъдещето на инфраструктурата на цялата Централна система. Високите изисквания за достъпност, по отношение на криптографската услуга трябва да са като всички компоненти на инфраструктурата на Е-електромерите. Достъпността на средата на централната система

трябва да достига не по малко от 99.99% 24 часа в денонощието, 7 дни в седмицата, 365 дни в годината. (непланирано спиране на работата се допуска за не повече от 53 минути годишно).

11.5 A (geographical) redundant design and architecture as well as providing the relevant Fail Over functionality must be available of the central system.

11.5 (Географски) съкратената структура и архитектура, както и осигуряването на съответната функционалност Възстановяване след Срив трябва да са налични на централната система.

11.6 Cryptographic service must be so designed in a way that not only the productive instance of the central system, but also a test system (environment) can use its functionalities.

11.6 Криптографската система трябва да е разработена така, че не само продуктивната част на Централната система, а и тестовата система (среда) да могат да се възползват от нейната функционалност.

11.7 The Bidder must propose adequate IT architecture which refers to requirement in point 11.1 for productive environment of central system.

11.7 Участникът трябва да предложи съответната IT архитектура, която се отнася за изискването в т. 11.1 за продуктивна среда на централната система.

12. E-Meter:

12. Е-електромер:

12.1 Only physical interface P0 can be accessible without removing the cover of E-Meter.

12.1 Единствено физически интерфейс P0 може да се ползва да достъп без отстраняване на капака на Е-електромера.

12.2 The E-Meters must be able to automatically record the events related to the process of opening the meter housing (if not glued) or terminal cover is detected and to send notification to the corresponding central system and store it in the registry (memory) of E-Meter.

12.2 Е-електромерите трябва да могат автоматично да записват събитията, свързани с процесите по отваряне на корпуса на електромера (ако не е залепен) или капака на клемния блок, и да изпращат известия до съответната централна система и да ги съхраняват в регистъра (паметта) на Е-електромера.

12.3 The counter values and terminal cover must be suitable protected from unauthorized physical intrusion. Manipulation attempts upon the E-Meter itself or at the interfaces must be optically visible (for example, broken seals).

12.3 Насрещните стойности и капака на клемния блок трябва да бъдат надлежно защитени от неоторизирано физическо проникване. Опити за манипулации върху самия Е-електромер или върху интерфейсите трябва да се виждат оптически (напр. нарушени пломби).

12.4 The built-into E-Meter - microcontrollers, processors are usually with appropriate interfaces (like JTAG - IEEE 1149.1 Standard Test Access Port and Boundary-Scan Architecture) provided which are allowing programming or debugging of the respective components. These interfaces are required, for example in the process of production of E-Meter. All hardware interfaces, which can be used immediately for programming or debugging after the production of E-Meter must be disabled.

12.4 Вградените в Е-електромера елементи - микроконтролери, процесори обикновено разполагат с подходящи интерфейси (като JTAG - IEEE 1149.1 Стандартен порт за достъп при изпитване и и Архитектура за сканиране на граничните повърхности), които позволяват програмиране или проверка за неизправности и ремонт на съответните компоненти. Тези интерфейси са необходими, например в процеса на производство на Е-електромера. Всички хардуерни интерфейси, които могат да се използват непосредствено за програмиране или разрешаване на проблеми, след производството на Е-електромера трябва да бъдат изключени.

12.5 E-Meter must also preserve a secure state when errors and unwanted or unintended operating states (random or willfully) are caused.

12.5 Е-електромерът трябва да запазва сигурността си и при наличие на грешки или възникване на нежелани или неволно предизвикани работни състояния (случайно или злоумишлено причинени).

Examples of such errors are:
a) voltage loss
b) integrity error
c) self-test error of E-meter
d) error in the process of executing cryptographic functions

e) error in process of validating access permissions
f) error in data entry (wrong data formats, incorrect data field length, invalid commands, etc.)

g) error in the operation of the local cryptographic keys

Примери за подобни грешки са:
a) загуба на захранване
b) грешка, свързана с целостта електромера
c) грешка при самотестуване на Е-електромер
d) грешка в процеса на изпълнение на криптографски функции
e) грешка в процеса на валидиране на достъпа
f) грешка във въведените данни (грешен формат на данни, неправилна дължина на полето с данни, невалидни команди и т.н.)
g) грешка в ориентацията на локалните Криптографски ключове

12.6 The memory for the system log must be with adequate size, which ensures that no system log messages can be overwritten before they are read out by a central system. A minimum storage for minimum 100 events must be available in it.

12.6 Паметта за регистъра на системата трябва да бъде с достатъчна големина, което гарантира невъзможността за записване на нови съобщения за системния регистър, върху съществуващи такива, преди да бъдат прочетени от централната система. Минималната памет, която трябва да е налична е за

100 събития.

12.7 The cryptographic key(s) must be itself safely stored in the E-meter. It must be not possible to be read in plain text or exported.

12.7 Криптографските ключове трябва да бъдат съхранявани по сигурен начин в Е-електромера. Не трябва да е възможно да бъдат прочитани или записвани на друг носител.

12.8 The E-meter must have internal clock and at periodic intervals must be synchronized with the central system

12.8 Е-електромерите трябва да разполагат с вграден часовник и периодично трябва да бъдат синхронизирани с Централната система

12.9 The E-meter manufacturer must disclose (declare) before the first delivery, which components and types (like communication module or unit of measurement) are installed in E-meter as well as from which suppliers these components are coming. The configuration of the E-meter must be provided to EVN EP. Subsequent changes of the configuration (for example change of supplier of built-in chips and etc.) are only permitted if EVN EP previously was notified in written form and if EVN EP agrees.

12.9 Производителят на Е-електромерите трябва да разкрие (декларира) преди първата доставка, които компоненти и типове (като комуникационния модул или измерващия блок) са инсталирани в Е-електромер, както и от кои доставчици са набавени тези компоненти. Конфигурацията на Е-електромера трябва да бъде представена на EVN EP. Последващи промени в конгифурацията (напр. промяна на доставчика на вградените чипове и т.н.) се допускат единствено, ако EVN EP е било предварително уведомено в писмен вид и е приело промяната.

12.10 The communication on all interfaces of the E-Meter must be done in a way to guarantee and protect the confidentiality and integrity. The availability of the information from E-Meter must be guaranteed at all the time.

12.10 Комуникацията по всички интерфейси на Е-електромера трябва да се осъществява по начин, който гарантира и защитава конфиденциалността и почтеността. Достъпът до информацията в Е-електромера трябва да бъде гарантиран по всяко време.

12.11 At all bidirectional interfaces of E-Meter only messages must be accepted which are previously defined for each port from the vendor. Before a message is accepted, it must be validated and accuracy to be checked. Messages that do not pass this test must be discarded.

12.11 При всички двупосочни интерфейси на Е-електромера трябва да бъдат приемани единствено съобщения, които са предварително дефинирани за всеки порт, от страна на доставчика. Преди приемане на съобщение, то трябва да бъде валидирано и истинността му да бъде проверена. Съобщения, които не преминат тази проверка, не трябва да бъдат отваряни.

12.12 If E-Meter is installed (at its initial installation), but no communication link with the central system is established, the E-meter must operate as a standard electronic meter. Basic functions shall be possible such as:

12.12 Ако Е-електромерът е монтиран (при първоначалната му инсталация), но няма комуникационна връзка с Централната система, Е-електромерът трябва да работи като стандартен електронен електромер. Трябва да са възможно основни функции, като:

12.12.1 Unencrypted reading out of data stored in the counter register values and the load profiles. (port P0 can be used by HHU)

12.12.1 Некриптирано отчитане на данните, съхранявани в насрещните регистрирани стойности и профилите на товарите. (порт P0 може да бъде използван с Преносим терминал)

12.12.2 Unencrypted reading out of data stored in the counter event log entries (port P0 can be used by HHU)

12.12.2 Некриптирано отчитане на данните, съхранявани в записите в регистъра на събитията (порт P0 може да бъде използван с Преносим терминал)

12.12.3 Set the Date and Time. (port P0 can be used by HHU)

12.12.3 Настройване на датата и часа. (порт P0 може да бъде използван с Преносим терминал)

12.13 The E-Meter must be initially loaded with a firmware image in the process of its production from the vendor.

12.13 Е-електромерът трябва първоначално да бъде зареден с дигитално подписан фърмуер в процеса на своето производство от продавача.

12.14 Manipulation of a custom portion of the firmware or of the contained firmware settings must not be possible.

12.14 манипулирането на определена част от фърмуера или на настройките на фърмуер трябва да е невъзможно.

12.15 Firmware update must be possible from the central system and must not influence the metrological part of E-Meter. The integrity of the firmware updates must be protected at least by hash code of the downloadable file which is sent through a unicast (one to one) authenticated and encrypted message and the E-Meter must not activate downloading process without having received the authenticated hash code.

12.15 Трябва да е възможно и актуализиране на фърмуера чрез Централната система. Коректността на актуализациите на фърмуера и самоличността на подписалите актуализациите трябва да бъдат проверени чрез цифровия подпис. Ако новия фърмуер не е дигитално подписан, той не трябва да бъде ползван.

12.16 In case of corruption of the update firmware operation, the operation must not affect the respective component and E-Meter must continue to operate with old firmware.

12.16 В случай на повреда при инсталирането на актуализацията на фърмуера, започналата операция не трябва да влияе съответните компоненти и Е-електромера трябва да продължи да работи със стария

12.17 The metered data (stored data – counter values, events and configuration) are not allowed to be changed or deleted during the process of update of the firmware.

12.18 Unnecessary functions of the firmware of E-Meters must be explicitly disabled.
12.19 The vendor of E-meter must ensure that only a firmware image which is derived from the associated E-meter manufacturers has been released by a defined approval process.

12.20 The vendor during the research and development of components which are installed in E-Meter must have a detailed documentation. In case of discovery of vulnerabilities in firmware and software in context of internal quality checks they must be recorded. All measures taken into account for filling the gaps must be documented. That documentation must be provided to EVN EP in written form, if it is requested.

12.21 The manufacturer or supplier of the software or firmware has to confirm by a written agreement that measures have been taken that availability of backdoors in the firmware are strictly prohibited. Through these backdoors might unauthorized access to the components of the E-meter and Concentrator infrastructure to be possible. As a backdoor applies in that case, a remote maintenance function, which without knowledge of EVN EP could be put into operation from the vendor (manufacturer).

12.22 Manufacturer or supplier must cooperate in case of IT Security Audits.

13. Central system
13.1 The software of Central system must be compatible with x86 server architecture.
13.2. Productive and test environments must be deployed.

13.3 The Central system must be compatible with operating system Microsoft Windows 2008 server 64 bit or higher or Red Hat v. 6.3 / 64 bit or higher.

13.4 Graphical user interface of software of central system must be ergonomic and refer to EN ISO 9241 standardization.
13.5 The Central system must allow implementation of role-based authorization concept. User rights must be defined for each role with appropriate necessary permissions. The various users depending on their function must have assigned role corresponding to their duties. The implementation of a role-based authorization concept must allow maximum separation of functions.

13.6 Passwords corresponding to user rights must be kept in a way which correlates to the deployed secure encryption mechanism and must be not reproducible. Passwords must be managed centrally.

13.7 Software must assist 4-eyes principle for a critical central system functions. Critical system functions that need

фърмуер.
12.17 Измерените данни (съхранени данни – стойности от брояча, събития и конфигурация) не могат да бъдат променяни или трити в процеса на актуализация на фърмуера.
12.18 ненужните функции на фърмуера на Е-електромерите трябва изрично да бъдат деактивирани.
12.19 Фърмуерът на Е-електромера трябва да бъде цифрово подписан, така че автентичността и неприкосновеността на фърмуера гарантират, че той действително е разработка на производителите на Е-електромера и се предоставя след преминаване на обстоен процес по одобрение и след полагане на електронен подпис.
12.20 При научно-изследователската си дейност, свързана с компонентите, монтирани в Е-електромера, продавачът трябва да разполага с подробна документация. При разкриване на слабости във фърмуера и софтуера, в контекста на вътрешните проверки на качеството, същите трябва да бъдат регистрирани. Всички мерки, предвидени за запълване на непълноти, трябва да бъдат документирани. Тази документация трябва да се предоставя на EVN EP в писмен вид, при поискване.
12.21 Производителят или доставчика на софтуера или фърмуера трябва да потвърди с писмено известие, че са взети всички мерки да се предотврати наличието на всякакви „задни вратички" (средства за неоторизиран достъп) до фърмуера. Подобни „задни вратички" биха могли да осигурят неоторизиран достъп до компонентите на Е-електромера. Под „задна вратичка" в случая се разбира и функция за дистанционна поддръжка, която, без знанието на EVN EP, би могла да бъде активирана от доставчика (производителя).
12.22 Производителят или доставчика трябва да осигурят съдействие при Одити за ИТ сигурност.

13. Централна система
13.1 Софтуерът на Централна система трябва да е съвместим със сървърна архитектура x86.
13.2. Трябва да бъдат създадени продуктивна и тестова среда.
13.3 Централната система трябва да е съвместима с операционна система Microsoft Windows 2008 сървър 64 bit или следващи варианти или Red Hat v 6.3 64 битова или следващи версии.
13.4 Графичният потребителски интерфейс на софтуера на централната система трябва да бъде ергономичен и да съответства на стандарт EN ISO 9241.
13.5 Централната система трябва да дава възможност за реализация на концепцията за оторизация по роли. Правата на потребителите трябва да бъдат дефинирани за всяка отделна роля, заедно със съответните разрешителни. Различните потребители, в зависимост от своите функции, трябва да имат роли, съответстващи на задълженията им. Прилагането на ролева оторизация би трябвало да позволи максимално разделение на функциите.
13.6 Паролите, съответстващи на правата на потребителите, трябва да се съхраняват по начин отговарящ на въведения механизъм за сигурно криптиране и трябва да не подлежат на възпроизвеждане. Паролите трябва да бъдат управлявани на централно ниво.
13.7 При софтуера следва да се прилага принципа на 4-те очи за особено важните функции на централната

confirmation before execution must be configured in a way that requires at least 2 employees approve before the start of execution (example: process for switch off / switch on of electricity).

13.8 Commands for critical system functions for each E-Meters must be unique and their distribution must be not performed as a broadcast to all E-Meters.

13.9 Tamper-proof (secure) logging of all activities must be undertaken during the execution of critical commands towards the E-Meters.

13.10 Assignment of log entries must easily and uniquely identify employees' activities.

13.11 The Central system must provide the possibility of maximum number of daily activities towards the E-Meter. If the configurable limit is reached, the system must send an alert. The change of the daily limits must be possible from at least two employees of EVN EP (compliance with 4-eyes principle).

13.12 Due to the uniqueness of "switch off" command towards the circuit breaker for each E-Meter, a logical algorithm must be applied which regulates how many E-Meters can be switched off maximum per day. If the configurable limit is reached, the central system must stop the process of execution and generate an alert. The change of daily limits must be possible from at least two employees of EVN EP (compliance with 4-eyes principle and approving procedure).

13.13 The central system must provide for all E-Meters and Concentrators time synchronization based upon international standard, like NTP protocol with an external timer or an already implemented in the internal network timers.
13.14 The time of central system can have difference of maximum of one second from the time of the external or internal timer.
13.15 The time from all installed E-Meters must be periodically checked and, if necessary, synchronized with the central system. Deviations of the time of installed E-Meters and Central system must be reported as an alarm message. (Excessive deviations could be a sign of a malfunctioning or manipulation of the E-Meter)

13.16 The central system must make an appropriate monitoring and reporting of all its functionalities. In case of malfunctions automatically a corresponding notification to the responsible personnel to be generated.
13.17 The assigned permissions and user rights of all employees which have an access in the Central system and to the respective components of E-Meter infrastructure should be checked periodically. For this review the provision of certain reports is necessary and they must contain:

13.17.1 List of all users with the date of definition, date of

система. Най-съществените функции на системата, които се нуждаят от потвърждение преди изпълнението си, трябва да бъдат конфигурирани по начин, който налага присъствието на поне 2 служители, които да одобрят съответните дейности, преди започване на тяхното изпълнение (пример: процес за прекъсване на електричеството).
13.8 Командите за функциите на критични системи функции за всеки от Е-електромерите трябва да бъдат уникални и разпространението им не трябва да се изпълнява като излъчване до всички Е-електромери.
13.9 Сигурно регистриране на всички дейности, защитено от посегателства трябва да се осъществява по време на изпълнението на особено важни команди по отношение на Е-електромерите.
13.10 Записите в регистъра трябва лесно и по уникален начин да идентифицират дейностите на служителите.
13.11 Централната система трябва да осигури възможност за максимален брой дневни дейности по отношение на Е-електромера. При достигане на подлежащия на конфигуриране максимален брой, системата трябва да изпрати предупреждение. Промяната в дневните лимити трябва да може да е извършва от поне двама служители на EVN EP (съответствие с принципа на 4те очи).
13.12 Поради уникалността на командата за прекъсване на захранването чрез главния прекъсвач за всеки Е-електромер, трябва да бъде приложен логически алгоритъм, който регулира колко Е-електромера максимално могат да бъдат изключени в рамките на един ден. При достигане на конфигурираната максимална стойност, Централната система трябва да спре процесът по изпълнение и генериране на предупреждение. Промяната на дневните максимални стойности трябва да е възможна единствено при участие на двама или повече служителя на EVN EP (спазване на принципа за 4-те очи и процедурата за одобряване).
13.13 Централната система трябва да осигурява за всички Е-електромери и Концентратори синхронизация на часа, въз основа на вътрешен стандарт, като NTP с външен таймер или вече приложен такъв във вътрешните мрежови таймери.
13.14 Часът според централна система може да се различава с максимум една секунда от часа на външния или вътрешния таймер.
13.15 Часът на монтираните Е-електромери трябва да бъде периодично проверяван и, ако е необходимо, синхронизиран с Централната система. Отклоненията в часа на инсталираните Е-Електромери и Централната система трябва да се съобщават под формата на алармено съобщение. (Прекомерните отклонения могат да са знак за неизправност или манипулация на Е-електромера)
13.16 Централната система трябва да осъществява надлежен контрол и отчетност на всичките си функции. При неизправност следва незабавно да се генерира и изпраща известие до отговорния персонал.
13.17 Дадените разрешения и потребителски права на всички служители, които имат достъп до Централната система и до съответните компоненти на Е-електромера, трябва да бъдат проверявани периодично. За тази проверка е необходимо изготвянето на определени доклади, които следва да съдържат следната информация:
13.17.1 Списък с всички потребители с дата на

first registration, date of last successful login, role membership of the user.

13.17.2 List of all permissions associated with a role in the central system.
13.17.3 List of evaluation according to various dimensions (for example- all users who are allowed to perform a certain action)
13.17.4 Identification of critical authorization combinations (for example, a user could run without the confirmation of another employee critical commands for a plurality of measurement points)
13.17.5 Historization of permissions of users (it should be comprehensible, about what permissions a user had at a particular time)

13.18 Any changes to the configuration of the central system have to be recorded. The stored log entries against subsequent change have to be protected. The log information must be clearly reported.

13.19 All changes in the central system (for example - manual manipulation of readings, replacement of values) must be logged, unique and assigned to a particular user. Historization of all user activities must be available.

13.20 If in the installed (deployed) E-Meters a critical system event is recognized then an appropriate alarm must be within 5 minutes sent to the central system.
13.21 During the periodic reading of the corresponding measured values from E-Meter, all stored in it event information must be able to be transported to central system.

13.22 For avoiding a re-recording possibility of encrypted commands towards the E-Meter from the central system or concentrator the Vendor has to implement an adequate mechanism to resist on it. (like framecounter of commands)
13.23 The application for maintenance tasks must be compatible with HHU operating system - Microsoft Windows mobile professional v.6.5 or libraries (SDK) for integration with existing legacy application. It is allowed for the applicant to provide software and hardware platform on a portable device, that fully meets the functionality and security requirements.

13.24 The client part of the central system application must be able to run on terminal server environment with Microsoft Windows 2008 server 64bit.

13.25 The central system must be able to be customized with modern technologies (interfaces) to exchange information with Contractor legacy systems in both directions. For example - billing and ERP system (kVASy) and meter data management environment.

13.26 In case of not successful execution of „switch on“ or „switch off“ function from central system towards the E-Meter in the timeframe within 4 hours, an automatic workorder must be created for maintenance task towards the HHU in order manually to perform the „switch on“ or “switch off” function for the E-Meter.
13.27 After manual execution of “switch on” or “switch off “ function by HHU from employee, the central system must

определяне на пълномощията, дата на първа регистрация, дата на последен успешен вход в системата, роля на потребителя.
13.17.2 Списък с всички разрешения, свързани с дадена роля в Централната система.
13.17.3 Списък с оценка, според различни показатели (напр. всички потребители, които имат право да осъществяват дадено действие)
13.17.4 Идентифициране на критични валидиращи комбинации (напр. даден потребител може да осъществява без потвърждение от друг служител критични команди за редица елементи от системата)
13.17.5 Исторически данни за разрешенията на потребителите (трябва да се съдържа подробна информация относно това кои потребители, какви права са имали в даден момент)
13.18 Всички промени в конгифурацията на Централната система трябва да бъдат регистрирани. Съхранените записи за съответните промени следва да бъдат защитени. Информацията в регистъра трябва да бъде ясна и точна.
13.19 Всички промени в Централната система (напр. – ръчно манипулиране на показания, замяна на стойности) трябва да бъдат регистрирани, уникални и обвързани със съответния потребител. Трябва да има налични хронологични данни за дейностите на всички потребители.
13.20 Ако в монтирани Е-електромери възникне критично системно събитие, съответната аларма трябва да бъде изпратена до Централната система.
13.21 По време на периодичното отчитане на съответните измерени стойности от Е-електромерите, цялата съхранена в тях информация за събития трябва да може да бъде прехвърлена в централната система.
13.22 За да се избегне повторен запис на криптирани команди към Е-електромерите от Централната система или концентратора, Доставчикът трябва да въведе подходящ механизъм за предпазване от подобно повтаряне. (брояч на команди)
13.23 Приложението за дейности по поддръжката трябва да е съвместимо с операционната система на Преносимия терминал - Microsoft Windows mobile professional v.6.5 или библиотеките (SDK) за интегриране в съществуващи приложения. Допуска се кандидатът да предостави софтуерна и хардуерна платформа на преносимо устройство, която напълно отговаря на изискванията за функционалност и сигурност.
13.24 Клиентската част от приложението на Централната система трябва да може да работи на терминален сървър с Microsoft Windows 2008 server 64bit.
13.25 Централната система трябва да подлежи на адаптация съобразно със съвременните технологии (интерфейси) за обмен на информация с предишните системи на Изпълнителя.

13.26 При неуспешно изпълнение на функцията по „включване“ от Централната система по отношение на даден Е-електромер в рамките на 12 часа, трябва да се генерира автоматична команда за задача по поддръжка към Преносимия терминал за да се осъществи ръчно „включването“ на Е-електромера.
13.27 След ръчното изпълнение на функцията „вкл.“ или „изкл.“ от HHU от страна на служител, централната

give possibility (interface) that HHU can report statuses of already executed workorders towards E-Meters.

13.28 Central system must support reporting mechanism with which the Contractor can create by itself adequate reports from the system.

14. Technical requirements for software maintenance of the central system.
14.1 Maintenance of an up-to-date program-license catalogue.
14.1.1 Initially the license catalogue shall be provided by the Contractor electronically or in paper after system insyallation;
14.1.2 The license catalogue shall contain name of license module/functionality, license price.
14.1.3 The license catalogue shall be updated after deployment of a new or removal of an existing license and not later than 1 month after deployment/removal a new license catalogue authorized by the Contractor shall be provided electronically or in paper.

14.3 Provision of software maintenance, covering the provision of communication service/Tickets, Hotline, maintenance at the site of the Contracting Authority, remote maintenance by the Contractor and others.,

14.4 Provision of communication service/Tickets and Hotline in the period from Monday to Friday and on the specified in Bulgaria working days in the period from 08:00-18:00 BG time without the Bulgarian public holidays.
14.5 Provision of communication service/Tickets and Hotline on weekend (Saturday/Sunday) and the Bulgarian holidays upon preliminary request by the Contracting Authority within the period giving 7 business days'notice.
14.6. The contractor shall provide the software maintenance, which consists of the following tasks:
14.6.1. Improvements: The Contractor shall remove all errors, ensuring its own quality of its product shall create new versions of the software and shall provide them to the Employer in the form of software packages for maintenance. The Employer is interested in any type of updates/upgrades, to be sure that he works with the latest version, although he is not bound.
All software updates and re-works shall be made available to the Employer in a current version with all the documentation for bringing the software into a working service and execution of operations with the software.

14.6.2 Error Management: The responsibility for debugging and troubleshooting is fundamental for the Contractor for the purpose of providing correctly running software to the Employer. The Contractor shall meet all the requirements after receiving error information from the Employer, by providing information how to avoid errors, self-removal of errors, errors specific for EVN, software re-works, future versions, packages, etc.

The type of delivery (information on the avoidance of errors, debugging of errors specific to EVN EP, software re-works, future versions, packages, etc.) depends on the class of the error. The delivery and implementation of an alternative solution for the management of the errors in an environment of the Employer (EVN EP) must be discussed in advance. These alternative solutions must be included in the

система трябва да дава възможност (интерфейс) HHU да може да отчита състоянията на вече изпълнените заявки за работа към Е-електромерите.
13.28 Централната система трябва да поддържа отчитащ механизъм, с който Изпълнителят да може сам да създава съответните доклади от системата.

14. Изисквания към софтуерната поддръжка на централната система.
14.1 Поддръжка на актуален програмно-лицензен каталог.
14.1.1. Първоначално лицензния каталог се предоставя от Изпълнителя в електронен вариант и на хартиено копие след инсталация на системата;
14.1.2. Лицензния каталог трябва да съдържа, име на лицензен модул/функционалнст, цена на лицензa.
14.1.3. Лицензния кататолог се актуализира при внедряване на нов или премахване на съществуващ лиценз, като не по късно от 1 месец след внедряването /премахването се предоставя актуализиран нов лицензен каталог в електронен вид и на хартиено копие оторизиран от Изпълнителя.
14.3 Осигуряване на софтуерна поддръжка, обхващаща предоставяне на служба за съобщения/Tickets, хотлайн/Hotline, поддръжка на място при Възложителя, поддръжка дистанционно при Изпълнителя и други.
14.4 Предоставяне на служба за съобщения/Tickets и хотлайн/Hotline в периода понеделник-петък и на определените в Република България работни дни в периода от 08:00-18:00 BG (българско време) без българските официални празници.
14.5. Предоставяне на служба за съобщения/Tickets и хотлайн/Hotline, в събота и неделя, както и на българските официални празници след предварително заявяване от Възложителя в периода с предизвестие от 7 работни дни.
14.6 Изпълнителят осигурява софтуерната поддръжка ,която се състои от следните задачи:
14.6.1 Подобрения: Изпълнителят премахва всички грешки, осигурявайки високо качество на продукта си, създава нови версии на софтуера и ги предоставя на Възложителя под формата на софтуерни пакети за инсталация. Възложителят е заинтересован за всякакъв тип актуализации/надстройки, за да е сигурен, че работи с последната версия, въпреки че не е задължен. Всички софтуерни актуализации и доработки се предоставят на Възложителя в съвременен вариант с цялата документация за привеждане на софтуера в работеща услуга и изпълняване на операции със софтуера.
14.6.2 Управление на грешките: Отговорността за отстраняване на грешки и проблеми е основна за Изпълнителя с цел предоставяне на коректно работещ софтуер на Възложителя. Изпълнителят изпълнява всички изисквания след информация за грешка от Възложителя, като предоставя информация за избягване на грешки, самостоятелно отстраняване на грешки, грешки специфични за ЕВН ЕР, софтуерни доработки, бъдещи версии, пакети и др.
Видът на доставката (информация за избягване на грешки, отстраняване на грешки специфични за ЕВН ЕР, софтуерни доработки, бъдещи версии, пакети и др.) зависи от класа на грешката. Доставката и имплементацията на алтернативно решение за управление на грешките в среда на Възложителя (ЕВНЕР) трябва да бъде предварително обсъдено. Тези

next package of services or in correctly and fully integrated system within half a year with the latest changes and amendments. All required tasks for solving problems and alternative solutions are without additional and separate prices. EVN EP shall give permission in case of troubleshooting or an alternative solution to be implemented, because the Employer undertakes additional installations, implementations or other changes of the software or its functionalities.

14.6.3. Exchange of information on current re-works and status: The Contractor shall provide estimated information at a neutral price at least once a year on current technical and commercial affairs, planned and ordered functionalities of the software (such as changes in technical matters, licenses, contact persons, owner, etc.)

14.7. Removal of failures

14.7.1 Classification of the failures:
14.7.1.1. Damage of category 1 - the Central system is not functioning and/or false data arise or the meter reading system does not function or the operation in at least one module is not possible or separate functions of the mass data processing, which shall be implemented without time delay (meter reading, electric meter switch-on, etc.), may not be carried out.

14.7.1.2. Damage of category 2 - individual functions of the Central system do not work or work incorrectly. The functionalities necessary for the daily work are not, or are partially available. There are alternative options. The operation of individual functions of one module is not possible and it can be resumed only with extraordinary spending of time and funds, wherein is concerned an essential function of the module, which must constantly be used. It is not possible to carry out a service, which must be immediately carried out for individual electric meter or it is not possible the immediate required preparation of meter reading. The work in a module or of one major feature of the module is seriously obstructed, as far as this affects the entire availability of the data base.

14.7.1.3 Damage of category 3 - one or more functions do not work optimally, but there is no severe obstruction of the daily work.
14.8. Response times is 4 hours after registering the problem into the ticketing system of contractor. Repair time is defined as follow based upon the categories of failures.

14.8.1 For category 1 - after registration should be started with identification of the cause of damage and the troubleshooting must be done latest within the working day in case the signal is registered until 12:00 a.m. and on the next working day if the signal is reported after 12:00 a.m. in the Republic of Bulgaria.

14.8.2 For category 2 - after registration should be started with identification of the cause of damage, and the troubleshooting must be done within the next three working days in the Republic of Bulgaria.
14.8.3 For category 3 - one day after registration should be started with identification of the cause of damage, and the

алтернативни решения трябва да бъдат включени в следващия пакет услуги или в коректно и напълно интегрирана система в рамките на половин година с последните промени и изменения. Всички задължителни задачи за разрешаване на проблеми и алтернативни решения са без допълнителни и отделни цени. Разрешението при отстранен проблем или алтернативно решение да се имплементира е на ЕВН ЕР, защото Възложителят поема допълнителни инсталации, имплементации или други промени на софтуера или функционалностите му.
14.6.3 Обмяна на информация за текущи разработки и статус: Изпълнителят предоставя прогнозна информация на необвързваща цена поне веднъж годишно за текущи технически и функционални въпроси, планирани и заявени функционалности на софтуера (като промени по технически теми, лицензи, лица за контакт, собственик и т.н.)
14.7 Отстраняване на повреди, осъществяват се на място при Възложителя или дистанционно при Изпълнителя
14.7.1 Класифициране на повредите
14.7.1.1 Повреда от категория 1 – Централната система не функционира и/или възникват грешни данни или Системата за отчет не функционира или Работата най-малко в един модул е невъзможна или Отделни функции от масовата обработка на данни, които трябва да бъдат реализирани без времево закъснение (отчет на електромери, включване на електромери и др.), не могат да бъдат извършени.
14.7.1.2 Повреда от категория 2 - отделни функции на Централната система не работят или работят грешно. Необходимите за ежедневната работа функционалности не са или отчасти са на разположение. Съществуват алтернативни възможности. Работата на отделни функции на един модул не е възможна и тя може да бъде възстановена само с извънреден разход на време и средства, при което се касае за съществена функция от модула, която трябва постоянно да бъде използвана. Не е възможно да се извърши услуга, която трябва незабавно да се извърши за отделен електромер или не е възможно незабавно необходимото изготвяне на отчет. Работата в един модул или на една основна функция от модула е сериозно възпрепятствана, доколкото от това е засегната цялата наличност на базата от данни.
14.7.1.3 Повреда от категория 3 - не работят оптимално една или повече функции, но няма сериозно възпрепятстване на дневната работа.
14.8. Времена на реакция 4 часа след регистриране на проблема чрез система за съобщения на Изпълнителя и време за отстраняване на проблема както следва по категории:
14.8.1 За категория 1 - след регистриране се започва с идентифициране на причината за повредата, а отстраняването трябва да стане в рамките най-късно на отстраняване в рамките на работния ден, в случай, че сигнала е регистриран до 12:00 часа и, ако сигнала е подаден след 12:00 часа, до 12:00 часа на следващия работен ден. в Република България.
14.8.2 За категория 2 - след регистриране се започва с идентифициране на причината за повредата, а отстраняването трябва да стане в рамките на следващите три работни дни в Република България.
14.8.3 За категория 3 - един ден след регистриране се започва с идентифициране на причината за повредата,

troubleshooting must be done within a deadline agreed between the two parties, but not later than 15 working days in the Republic of Bulgaria.
14.9 Transmitting the status of troubleshooting must be assured by the Contractor, the status containg information on details of troubleshooting within the response time.

14.10 The damage shall be considered removed after making tests and after the approval of EVN EP.
14.11 The Contractor must provide the following process for debugging the software:
14.11.1 The Contracting Authority shall send a message with the required information to the support team (Helpdesk) indicated by the Contractor for available errors through communication service/Tickets and/or Hotline for issues registration. Such message shall contain also the error class.
14.11.2 The error is logged in the issues registration system (ticket system) and response shall be returned within the specified response time.
14.11.3 After finding a solution the Employer shall be notified and asked to carry out a test in the test system, and the required documentation shall be sent.
14.11.4 After approval shall be made an installation in the test system.
14.11.5 Test and confirmation of the decision.

14.11.6 Approval for installation in a productive system.

14.11.7 Installation make in a productive system and official confirmation. The procedure is carried out in accordance with the agreed hours for each error class.

14.12. There must be guaranteed assistance in the case of installations, making a connection to databases, interfaces, reports, additions, technical problems or errors that have occurred during the use of the software, etc
14.13. There must be provided documentation for standard and configured / specific to the software functionalities according to the current version in use. For each implementation the Contractor shall provide documentation about the changes performed in the programming code prior the installation of the test system.
14.14 The Contractor must notify the Contracting Authority at least once a year for all committed changes and additions on components of the central system. The information should contain at least the date of issue, description of the functionality, the change request number to the software and any other changes made, if any. The Contractor shall provide this information at the latest within 1 calendar month upon EVN's EP request.

14.15. The option remote control must be possible for the central system through desktop sharing and VPN connection through EVN EP network whenever debugging is needed and/or software updates and upgrades. The method will be chosen by the Contracting Authority after contract signing.

14.16 Supply of new program versions
14.16.1 EVN EP must receive information for the availability

а отстраняването да стане в срок договорен между двете страни, не по късно от 15 работни дни в Република България.
14.9. Да се осигури предаване на статуса на отстраняване на повредата от страна на Изпълнителя съдържащ информация относно – детайли за дейностите свързани с отстраняването на повредата в рамките на времето за реакция.
14.10 Повредата се счита за отстранена след тестове и потвърждение от страна на ЕВН ЕР.
14.11 Изпълнителят трябва да осигури следния процес за отстраняване на грешки в софтуера:
14.11.1 Възложителят изпраща съобщение с необходимата информация към екипа за поддръжка (Helpdesk) посочен от Изпълнителя, за наличие на грешка чрез служба за съобщения/Tickets и/или хотлайн/Hotline за регистриране на проблеми. Съобщението съдържа и класа грешка.
14.11.2 Грешката се въвежда в системата за регистриране на проблеми и се връща отговор в определеното време за реакция.
14.11.3 След намиране на решение Възложителят бива уведомен и запитан за извършване на тест в тестовата система, а нужната документация бива изпратена.
14.11.4 След одобрение се извършва инсталация в тестовата система.
14.11.5 Тест и потвърждение за отстраняването на повредата от страна на Възложителя.
14.11.6 Съгласуване от страна на Изпълнителя за инсталация в продуктивна система с Възложителя, чрез службата за съобщенията.
14.11.7 Извършване на инсталация от Изпълнителя в продуктивна система и официално потвърждение. Процедурата се осъществява съгласно договорените часове за всеки клас грешка.
14.12. Трябва да бъде гарантирана помощ в случай на инсталации, осъществяване на връзка с бази данни, интерфейси, доклади, допълнения, технически проблеми или грешки, появили се по време на употреба на софтуера и т.н.
14.13 Трябва да бъде предоставена документация за стандартни и конфигурирани / специфични за софтуера функционалности според текущата версия, която е в употреба. За всяка една имплементация Изпълнителя предоставя документация за извършените в програмния код промени преди инсталирането в тестовата система.
14.14. Изпълнителят трябва да уведомява Възложителя поне веднъж годишно за всички извършени промени и допълнения върху компоненти на централната система. Информацията трябва да съдържа поне дата на издаване, описание на функционалността, номера изискване от системата за съобщения към софтуера и извършени други промени в случай на наличие на такива. Изпълнителя трябва да предостави тази информация не по късно от 1 календарен месец при заявка от страна на ЕВН ЕР.
14.15. Централната система трябва да има възможност, при нужда от отстраняване на грешки и/или софтуерни актуализации и надстройки за отдалечен достъп и контрол,чрез използване на споделен екран (desktop sharing) и VPN връзка през ЕВН ЕР мрежа. Методът ще бъде избран от Възложителя след подписването на договора
14.16. Доставка на нови програмни версии.
14.16.1 EVN EP да получава информация за наличие на

of new software versions.
14.16.2 EVN EP must approve the methods and the time window for installation.
14.16.3 New versions must be controlled with antivirus programs

нови програмни версии.
14.16.2 EVN EP да съгласува начините и времената за инсталация.
14.16.3 Новите версии трябва да са контролирани с антивирусни програми

VI. Standards

References to relevant standards and other technical regulations and recommendations to be followed.
Es gelten die jeweils aktuellsten Fassungen zum Zeitpunkt der Erstellung dieses Dokuments.

IEC/ISO	
IEC Publ. 60529	Degree of protection provided by enclosures (IP-CODE)
ISO Publ. 75	Plastics and ebonite, determination of temperature of deflection under load.
Europe Standards	Designation
EN 62052-11	Electricity metering equipment (AC) – General Part 11: Metering equipment
EN 62053-21	Electricity metering equipment (a.c.) – Particular requirements – Part 21:Static meters for active energy (classes 1 and 2)
EN 62056-21	Electricity metering – Data exchange for meter reading, tariff and load control – Part 21: Direct local data exchange
EN 62056-61	Electricity metering.Data exchange for meter reading, tariff and load control Part 61:Object identification system (OBIS)
EN 55011	Industrial, scientific and medical equipment. Radio-frequency disturbance characteristics. Limits and methods of measurement (Basisdocument CISPR 11)
EN 55014	Electromagnetic compatibility. Requirements for household appliances, electric tools and similar apparatus Emission (Basisdokument CISPR 14)
EN 62053-52	Electricity metering equipment (AC) – Particular requirements – Part 52: Symbols
EN 61000-3-2 + A2	Electromagnetic compatibility (EMC). Limits. Part 3-2 Limits for harmonic current emissions
EN 61000-4-4	Electromagnetic compatibility (EMC) -- Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test (Burst) (Basisdokument IEC 801-4)

VI. Стандарти

Изискванията на съответните технически стандарти и препоръки трябва да бъде спазено.
Es gelten die jeweils aktuellsten Fassungen zum Zeitpunkt der Erstellung dieses Dokuments.

IEC/ISO	Предназначение
IEC Publ. 60529	Степени на защита, осигурени от обвивката (IP код)
ISO Publ. 75	Пластмаси и ебонит, определяне на температурата на деформация при натоварване.
Европ. стандарти	Предназначение
EN 62052-11	Променливотокови уреди за измерване на електрическа енергия. Общи изисквания, изпитвания и условия на изпитване. Част 11: Уреди за измерване (електромери)
EN 62053-21	Променливотокови уреди за измерване на електрическа енергия. Специфични изисквания. Част 21: Статични електромери за активна енергия (класове 1 и 2)
EN 62056-21	Измерване на електрическа енергия. Обмен на данни за измервателни уреди за отчитане, управление на тарифи и товар. Част 21: Директен локален обмен на данни
EN 62056-61	Измерване на електрическа енергия. Обмен на данните за показанията на електромера, управление на тарифите и товарите. Част 61: Система за идентификация на обекти
EN 55011	Промишлени, научни и медицински (ПНМ) радиочестотни устройства. Характеристики на радиочестотните смущаващи въздействия. Гранични стойности и методи за измерване(CISPR 11)
EN 55014	Електромагнитна съвместимост. Изисквания за електрически уреди, електрически инструменти и подобни на тях уреди. (CISPR 14)
EN 62053-52	Променливотокови уреди за измерване на електрическа енергия. Специфични изисквания. Част 52: Символи за променливотокови електромери
EN 61000-3-2 + A2	Електромагнитна съвместимост (EMC). Част 3: Норми. Раздел 2: Норми за излъчвания на хармонични съставящи на тока
EN 61000-4-4	Електромагнитна съвместимост (EMC). Част 4-4: Методи за изпитване и измерване. Изпитване на устойчивост на електрически бърз преходен процес/пакет импулси (Burst) (Basisdokument IEC 801-4)

EN 61000-4-5	Electromagnetic compatibility (EMC) -- Part 4-5: Testing and measurement techniques - Surge immunity test (Surge)
EN 62052-11 of 2003-02-12	Alternating current electricity metering equipment. General requirements, tests and testing conditions. Part 11: Metering equipment (electricity meters)
EN 62053-21 of 2003-01-28	Alternating current electricity metering equipment. Specific requirements. Part 21: Static active energy electricity meters (classes 1 and 2)
EN 62054-21 edition 2005-08-01	Alternating current electricity metering devices. Tariff and load control Part 21: Specific requirements applicable to switching timers
DIN/DIN-VDE Standards	Designation
DIN 43859 6.77	Watthour meters for instrument-transformer connection; main dimensions for three-phase meters
DIN VDE 0160 05.88	Electronic equipment for use in power installations (with change A1/04.89 and A2/10.88)
Common	Designation
IEC 13 (SEC) 1022	Reliability requirements for static meters
OIML 11	General requirements for measuring instruments
OIML 12	Fields of use of measuring instruments subject to verification

TABLE - STANDARDS

EN 61000-4-5	Електромагнитна съвместимост (EMC). Част 4-5: Методи за изпитване и измерване. Изпитване на устойчивост на отскок
EN 62052-11 издание: 2003-02-12	Променливотокови уреди за измерване на електрическа енергия. Общи изисквания, изпитвания и условия на изпитване. Част 11: Уреди за измерване (електромери)
EN 62053-21 издание 2003-01-28	Променливотокови уреди за измерване на електрическа енергия. Специфични изисквания. Част 21: Статични електромери за активна енергия (класове 1 и 2)
EN 62054-21 издание 2005-08-01	Променливотокови уреди за измерване на електрическа енергия. Управление на тарифите и товара Част 21: Специфични изисквания към превключващи часовници
DIN/DIN-VDE Стандарти	Предназначение
DIN 43859 6.77	Електромери за индиректно свързване; основни размери за трифазни електромери
DIN VDE 0160 05.88	Електронно оборудване за използване в електрически инсталации (с промяна A1/04.89 и A2/10.88)
Общи	Предназначение
IEC 13 (SEC) 1022	Изисквания за надеждност за статични електромери
OIML 11	Общи изисквания за измервателните уреди
OIML 12	Области на употреба на измервателни уреди, подлежащи на проверка

ТАБЛИЦА - СТАНДАРТИ

*Посочените изисквания са пожелателни/незадължителни!

С подписването на настоящите Технически изисквания, Изпълнителят гарантира за тяхното приемане, спазване и точно изпълнение.

Дата …….

Подпис и печат: .....