ПЪЛНО ОПИСАНИЕ И ТЕХНИЧЕСКИ ИЗИСКВАНИЯ

ПРЕДМЕТ: **„Инженеринг - проектиране, авторски надзор и изпълнение на Главната командно-контролна система за сигурност по част от периметъра на северната дъга и прилежащите й обекти“**

ПЪРВО: ОПИСАНИЕ НА ВИДОВЕТЕ РАБОТИ

Концептуалното решение за сигурността на “ТЕЦ Марица Изток 2” ЕАД включва два съществени елемента:

- функционалното и физическото разполагане на съоръженията и отделите на територията на централата;
- физическа, техническа и кибер защита.

За да се намали до минимум заплахата от проникване в централата на лица без разрешен достъп, да се попречи на тези лица да достигнат до зони с ограничен достъп, а също така да се ограничи риска хора с ниско равнище на достъп да влязат в зони, за които се иска по-висока степен на достъп е наложително да се изградят технически системи за сигурност и безопасност.

Концепцията на Системата за сигурост на “ТЕЦ Марица Изток 2” ЕАД включва следните основни равнища на защита:

- **предварителен прием** - достъп до външни услуги преди “Главния портал”;
- **първо равнище** - защита на външния периметър на централата от нежелано навлизане в обособената територия на централата;
- **второ равнище** - защита на специфични критични (стратегически) зони и обекти, разположени вътре в периметъра на централата.

ИНФРАСТРУКТУРА И ОБЩИ ИЗИСКВАНИЯ

В топлоелектрическата централа трябва да се изгради подходяща инфраструктурна система за подпомагане на решенията за безопасността. Тя следва да включва: строителство, правила за движение, електричество, комуникации, охранително осветление, както и функции за безопасност.

Инфраструктурните системи трябва да се проектират и конструират според местните стандарти, закони и разпоредби, като се вземат предвид следните аспекти:

- модулност (необходима е за поетапното осъществяване);
- дублиране на източници и маршрути за доставки;

- гъвкавост (необходима е за свързването на различни системи);
- резерви за бъдещо разширение;
- ремонтопригодност.

1. НОВ ГЛАВЕН КОМАНДЕН И КОНТРОЛЕН ЦЕНТЪР ЗА СИГУРНОСТ

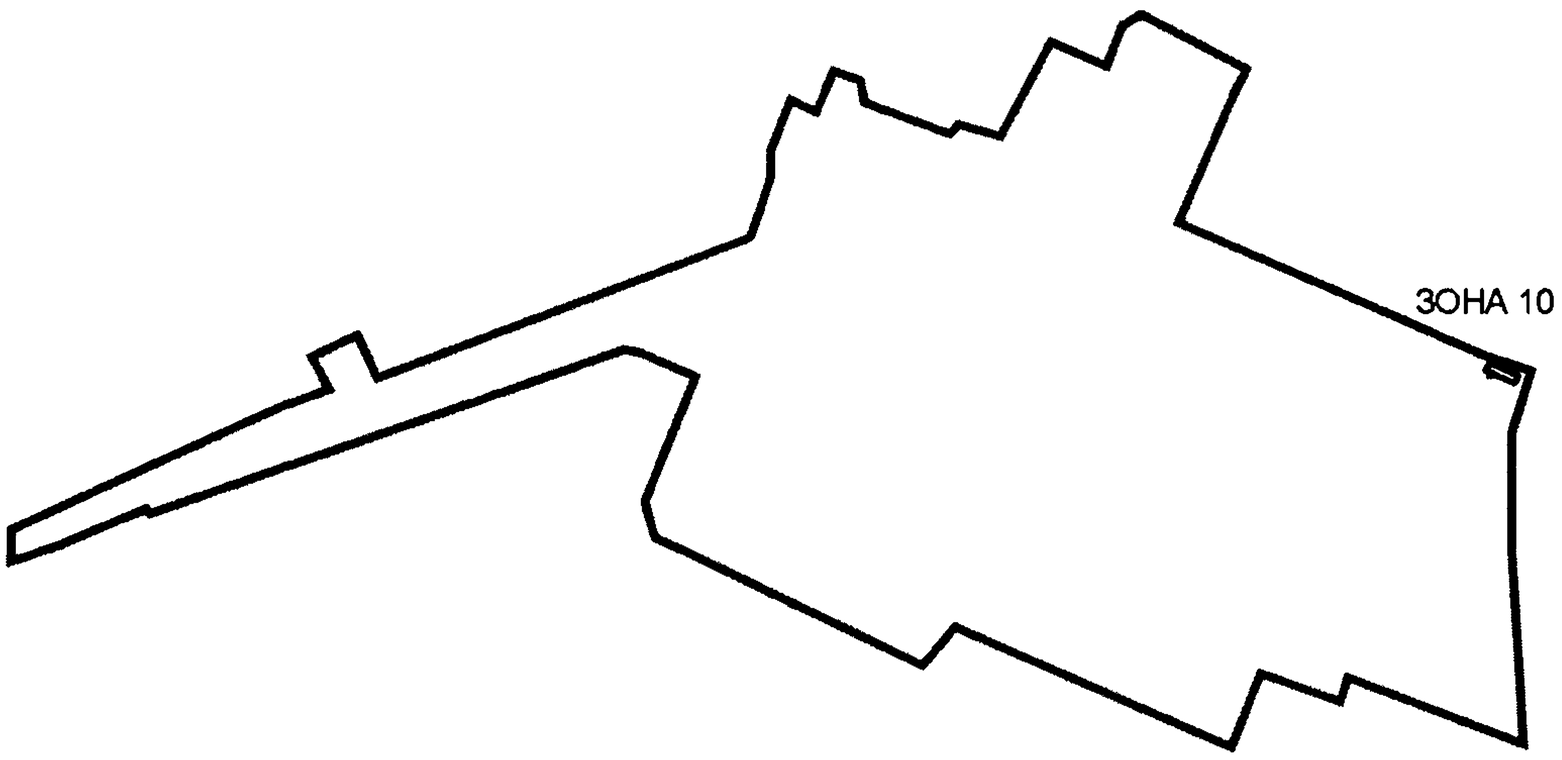
Съществуващият комплекс за контрол на сигурността на централата не отговаря на съвременните изисквания за подобен център.

Равнището на съществуващите мерки за сигурност е ниско.

За да отговори на настоящите и бъдещите изисквания за сигурност на централата, трябва да се изгради нов Главен команден и контролен център за сигурност.

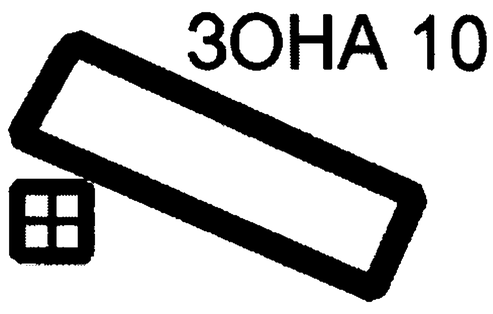
Местоположението на Главния команден и контролен център за сигурност ще бъде на мястото на съществуващите стари временни постройки на МТС, както е посочено на приложената по-долу скица за ориентация.

Разполагането на Главния команден и контролен център за сигурност спрямо външния периметър и конкретния контур на зоната са показани на фигура № 1 - 1.



фигура № 1 - 1

За зона № 10 трябва да се обособи 1 (една) входно / изходна точка за преминаване само на хора. Местоположението й е показано на фигура № 1 - 2.

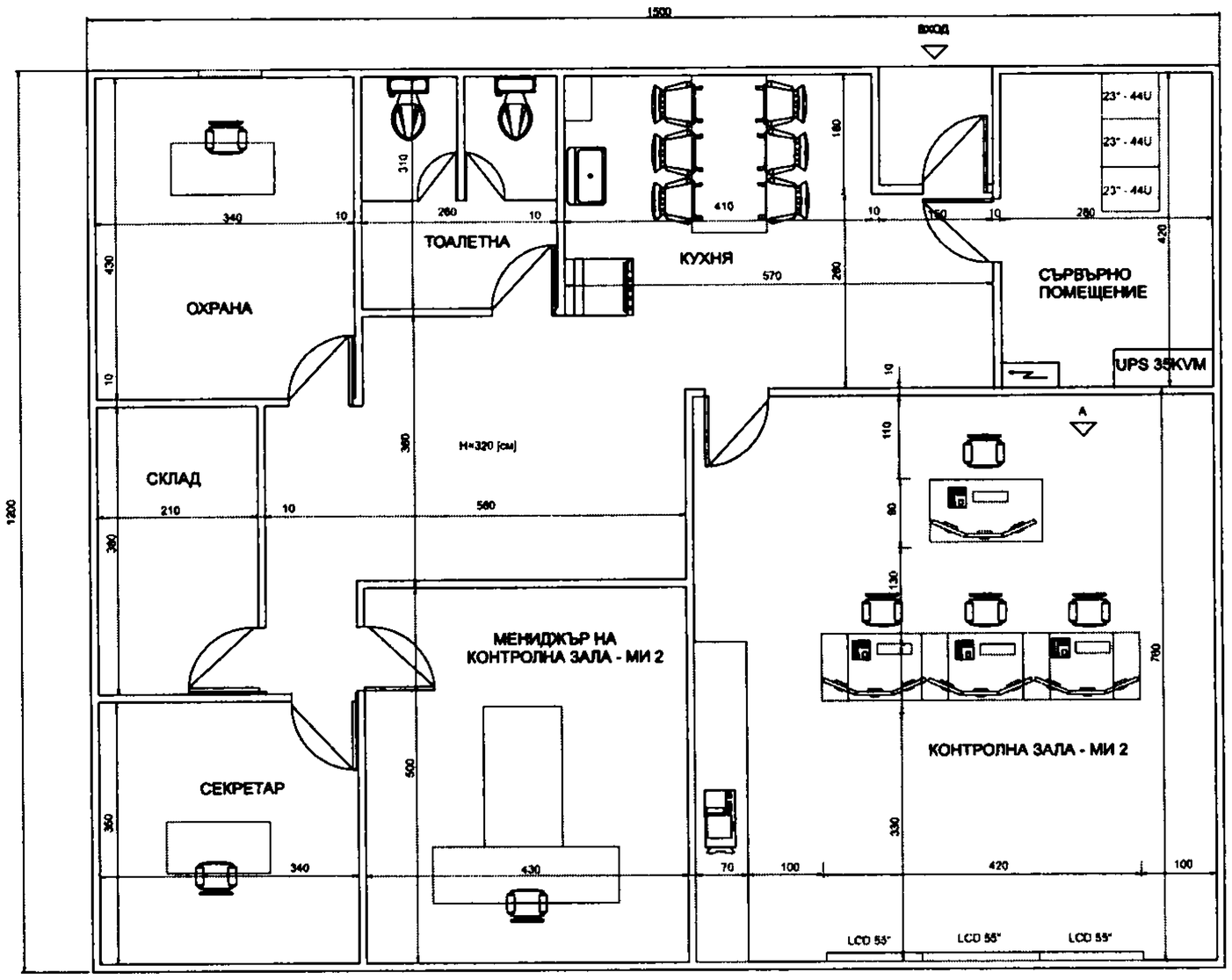


фигура № 1 - 2

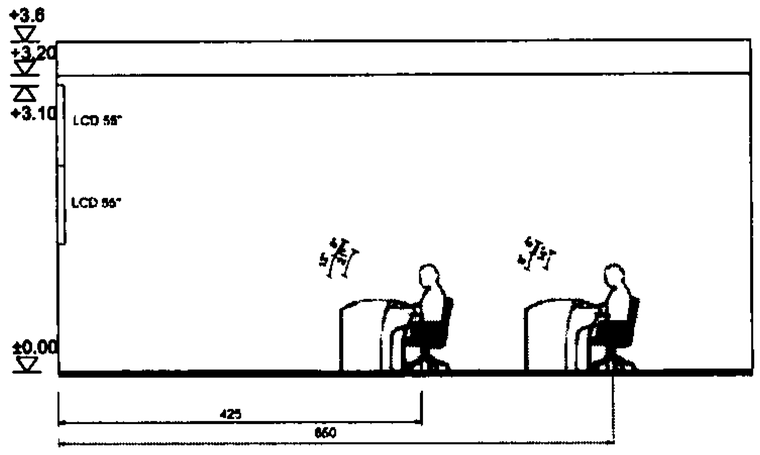
Трябва да се създаде нов Главен команден и контролен център за сигурност, който задължително ще се състои от:

- **оперативна / контролна зала** - включва 2 (две) работни места за оператори и 1 (едно) работно място за контрольор (супервайзор);
- **помещение с оборудването на системите за сигурност и комуникация / сървърно помещение** - включва необходимия брой ракове с оборудване и централна UPS система;
- **помещение за поддържане и съхраняване на резервни части** - включва място за софтуерно и хардуерно поддържане и подходящо място за резервни части;
- **битови помещения** - включва съблекални и санитарни възли;
- **други помещения** - по преценка.

Примерното архитектурно разпределение на помещенията в бъдещия Главен команден и контролен център за сигурност е показано на фигура № 1 - 3.



Изглед - А



фигура № 1 - 3

ГЛАВЕН КОМАНДЕН И КОНТРОЛЕН ЦЕНТЪР НА СИГУРНОСТ - ОБЩИ ИЗИСКВАНИЯ

Центърът трябва да се организира така, че да се съобразява с изискванията на Главната командно - контролна система, включително строителни, електрически и други изисквания по отношение на инфраструктурата.

Очакваната застроена площ, необходима за командния контролен център е не по-малко от 180 [m^2].

Изискванията по отношение на инфраструктурата трябва да включват:

- повдигнат под;
- окачен / звукоизолиран таван;
- звукоизолирани вътрешни стени;
- кабелни канали и кабелни скари за различни цели;

- подходящи охранителни врати;
- пожароизвестителна система;
- пожарогасителна система;
- електрически инсталации, включително UPS и архивираща система;
- осветление, включително аварийно;
- електрическо и електронно заземяване;
- отоплителна, вентилационна и климатична инсталация с пълно дублиране;
- комуникации.

2. ПЕРИМЕТЪРНА СИГУРНОСТ

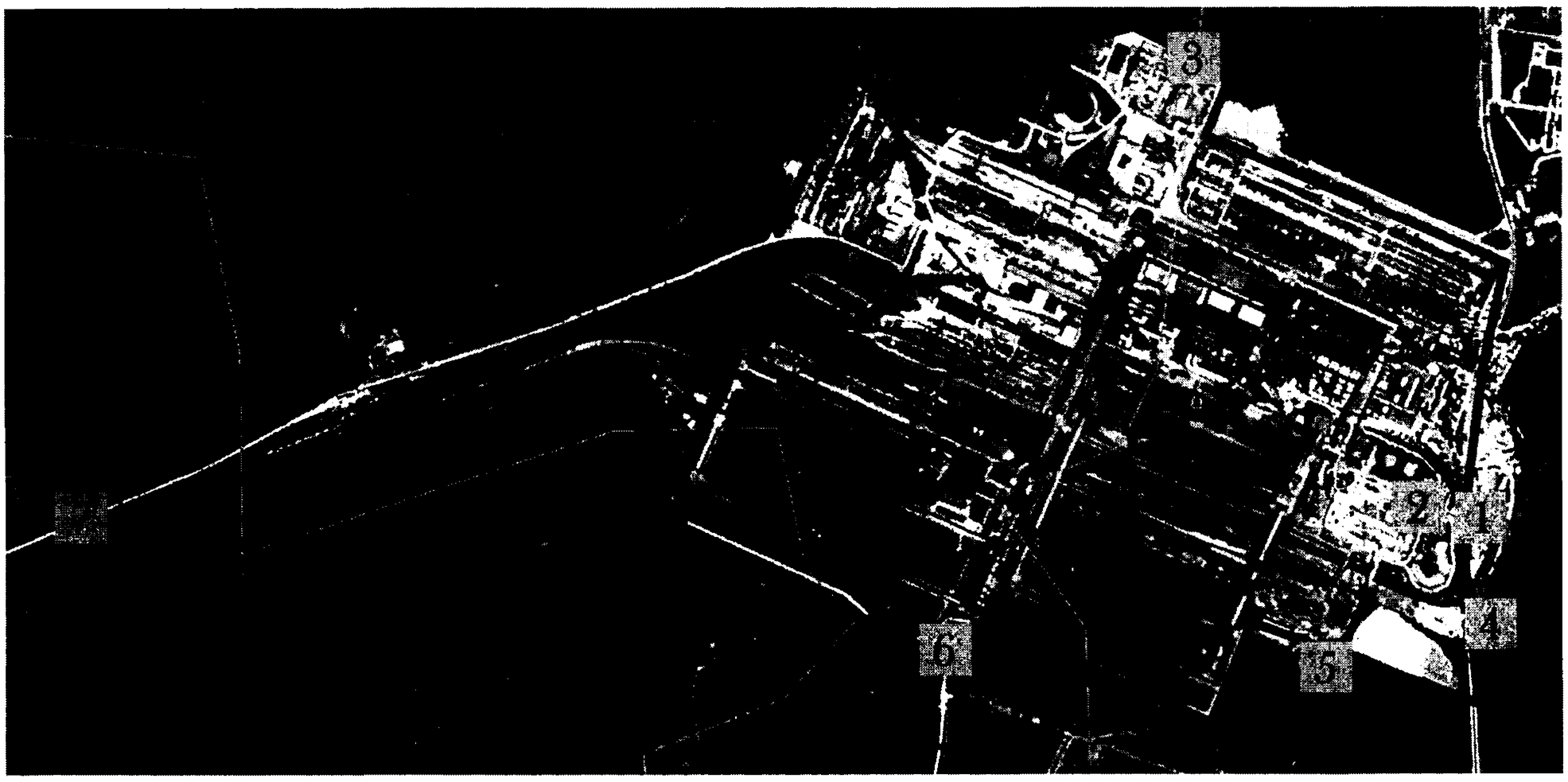
Съществуващата територия на "ТЕЦ Марица изток 2" ЕАД трябва да се огради по периметъра. Целият външен периметър на централата е около 9 500 [m] и обхваща следните участъци:

- от съществуващия временен портал на железопътната линия по североизточната страна на територията на централата, през електрическата подстанция „Изгрев", охладителната кула и новата административна сграда до северния портал;
- от северния портал през съществуващата външна ограда на електрическата подстанция (открита разпределителна уредба) - до буферния и главния портали;
- от буферния портал по външната оградата на паркинга пред киносалона и бензиностанцията - до товарния портал;
- от товарния портал покрай междуселищния път № 55 през гористата местност - до портала „Гипсоотвал";
- от портала „Гипсоотвал" покрай старото въглищно стопанство - до портала „Черно езеро";
- от портала „Черно езеро" покрай новото въглищно стопанство и успоредно на железопътния път от южната му страна - до портал „Железопътна гара".

Поради размера и топографията на обекта, решението за периметърна сигурност се основава на интегриран подход, който включва:

- периметърна физическа ограда (бетонов фундамент, ограда и кльон);
- портали (контролно - пропускателни пунктове);
- охранително осветление;
- патрулни пътища от вътрешната страна на оградата;
- полоса за наблюдение от външната страна на оградата;
- системи за откриване, наблюдение и проверка.

Периметърът на оградата, заедно с порталите са показани схематично на фигура № 2 - 1.



фигура № 2 - 1

Първият етап от изграждането на периметърната сигурност на централата, включва частта:

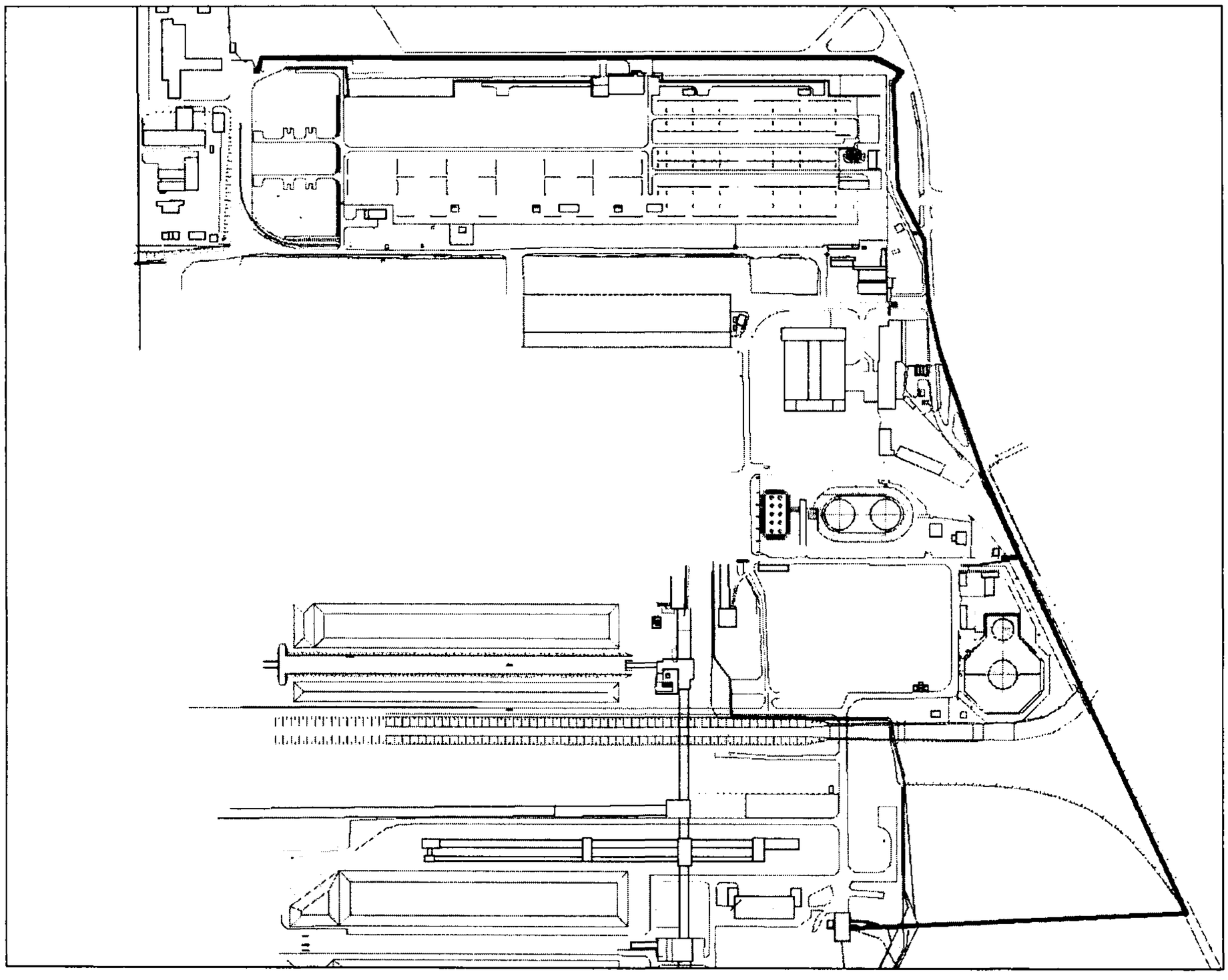
- от северния портал през съществуващата външна ограда на електрическата подстанция (открита разпределителна уредба) - до буферния и главния портали;
- от буферния портал по външната оградата на паркинга пред киносалона и бензиностанцията - до товарния портал;
- от товарния портал покрай междуселищния път № 55 през гористата местност - до портала „Гипсоотвал";

За да се отговори на приетата концепция за сигурност, трябва да се изпълнят следните мерки за сигурност:

№	предлагани мерки	кратко описание
1	2	3
1.	периметърната ограда с електронно оборудване	• физическа ограда с електронно оборудване; • портали; • патрулни пътища.
2.	охранително осветление	районът на оградата и заобикалящата я среда трябва да се осветят добре

3.	затворена система за телевизионно наблюдение	подвижни управляеми и стационарни камери - трябва да се инсталират, за да се наблюдава и контролира движението на хора и превозни средства

Ориентировъчната дължина на оградата по частта от северната дъга на периметъра, предмет на първия етап е около 1 300 [m], показани схематично на фигура фигура **№ 2 - 2**.



фигура № 2 - 2

2.1. ПЕРИМЕТЪРНА СИГУРНОСТ - ФИЗИЧЕСКА ОГРАДА

По външния периметър трябва да се изгради допълнително ограда на нови места и най-вече в разширената зона, която обхваща районите на сгуроотвала, гипсоотвала, железопътните трасета и други в съответствие с изискванията на техническото задание.

Новата ограда по периметъра на обекта ще включва три основни елемента:

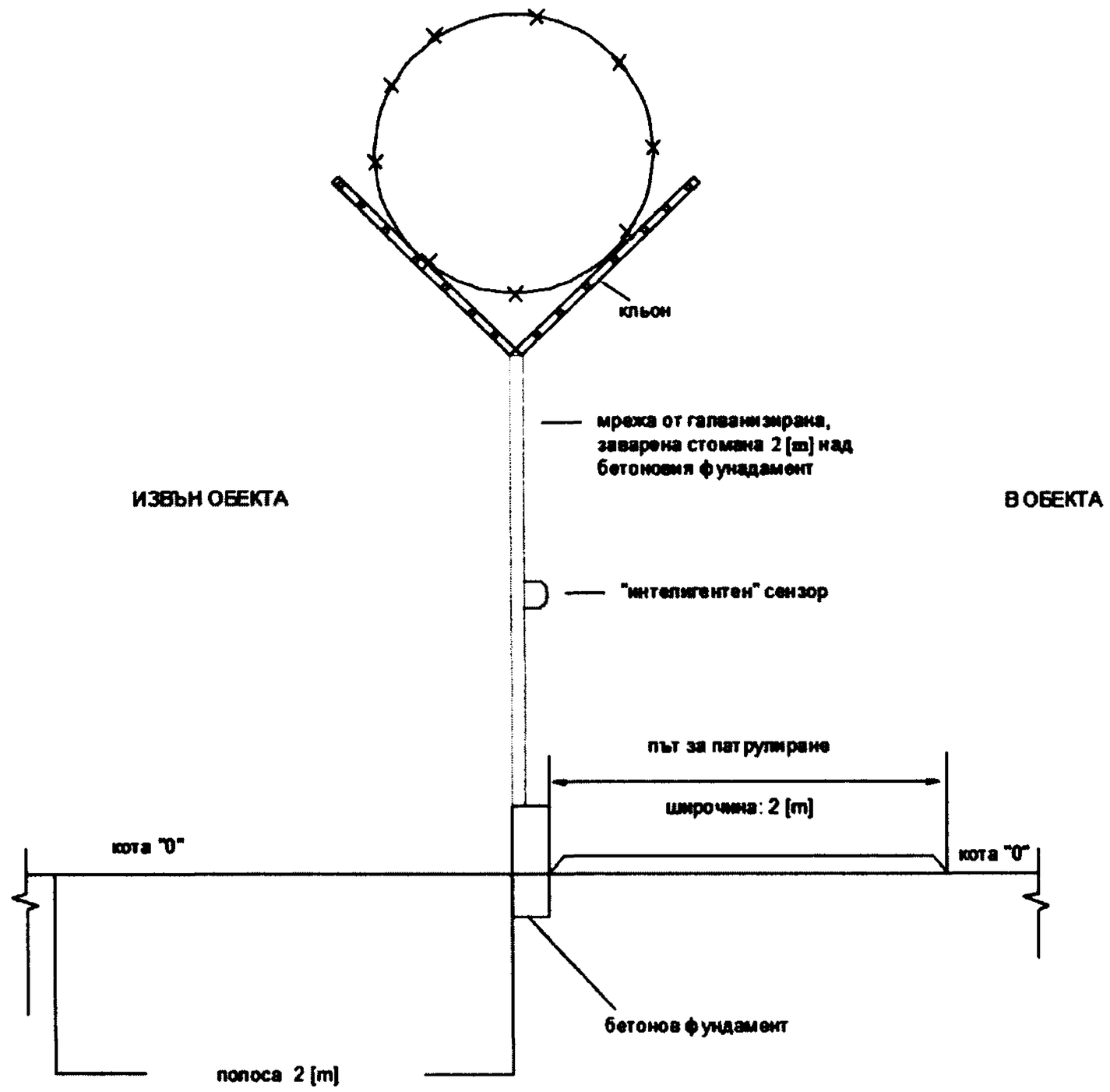
№	предлагани мерки	кратко описание
1	2	3
1.	бетонов фундамент	с височина минимум 70 [cm] и дебелина 20 [cm]. 50 [cm] от височината на оградата са под кота “0” и 20 [cm] са над кота “0”. Отворите и тръбите в бетоновата основа, използвани за дренаж и оттичане на водите през нея, трябва да се подсигурят с мрежа от галванизирана стомана с дебелина на металните пръчки най-малко Ø 12 [mm] и с размер на отворите на мрежата, не по-голям от 100 [mm] x 100 [mm]
2.	мрежа от галванизирана заварена стомана	с максимален размер на отворите 50 [mm] x 150 [mm] - минималната дебелина на стоманената тел трябва да бъде Ø 4,5 [mm]. Минималната изисквана обща височина от върха на оградата до бетоновате основа е 2 000 [mm]. Мрежата следва да бъде свързана към вертикални стоманени колони през не повече от 3 000 [mm]. Вертикалните колони трябва да бъдат закрепени неподвижно за бетоновата основа
3.	кльон	от заварена мрежа с дължина 800 [mm]. Той от своя страна следва да бъдат закрепен към наклонени стоманени греди с дължина от 600 [mm], които са част от вертикалните, носещи колони. Наклонът на гредите трябва да бъде 60^0 спрямо равнището на хоризонта. Кльонът и вертикалната мрежа трябва да бъдат здраво свързани. Препоръчва се и добавянето на серпентина с остри режещи краища върху кльона

Забележка: Тъй като част от периметъра е вече оградена, препоръката за тези части от оградата е да се запази и реновира съществуващия бетонов фундамент.

Точната линия, по която ще минава оградата, особено за новооградените зони следва да се определи по време на детайлното проектиране.

Съществуващата ограда, заедно с кльона следва да се демонтира, ремонтира и подобри, така че да отговаря на съответните технически изисквания.

Примерният вид на оградата е показан на фигура № 2.1. - 1.



фигура № 2.1. - 1

2.2. ПЕРИМЕТЪРНА СИГУРНОСТ - АЛАРМЕНА СИСТЕМА СРЕЩУ ПРОНИКВАНЕ ЗА ПЕРИМЕТЪРНАТА ОХРАНА

Сензорна система за откриване на нарушители трябва да се инсталира по целия периметър на централата. Необходимо е тя да се свърже към оградната мрежа и кльона. Сензорни линии следва да се инсталират и на крилата на работните / аварийните портали. Тези сензори подават сигнал, когато нарушител се опита да премине (пробие) оградата чрез разрязване или прескачане на оградата или портала.

Сензорните линии трябва да са с дължина не по-голяма от 100 [m]. Сензорната линия (вибрационна система) трябва да е подходяща и невлияеща се от електромагнитните излъчвания. В някои специални случаи (при необходимост) може да се използва и комбинирана инфрачервена и микровълнова система. Точното решение за всеки участък следва да се дефинира на етап проектиране.

2.3. ПЕРИМЕТЪРНА СИГУРНОСТ - МАГНИТНИ КОНТАКТНИ ДЕТЕКТОРИ, КОИТО СЛЕДЯТ ПОЛОЖЕНИЕТО НА ВРАТИТЕ НА ПОРТАЛИТЕ

Свръхмощни магнитни контактни детектори от висок клас за „външно“ използване (позиционни превключватели) следва да се инсталират на работните / аварийните портали, които обичайно са затворени, така че да подават алармен сигнал при опит за неразрешено отваряне на вратите.

2.4. ПЕРИМЕТЪРНА СИГУРНОСТ - ЗАТВОРЕНА СИСТЕМА ЗА ТЕЛЕВИЗИОННО НАБЛЮДЕНИЕ ПО ПЕРИМЕТЪРА

Затворена система за телевизионно наблюдение, базирана на цифрови стационарни и подвижни управляеми камери трябва да се инсталира по дължината на периметърната ограда, за да позволи идентифициране и наблюдаване по периметъра и в околното му пространство, и за проверяване на причините за алармите, подадени от сензорните линии в реално време.

Всяка стационарна камера трябва да обхваща част от периметъра с дължина до 50 [m], а подвижните управляеми камери може да покриват участъци от периметъра с дължина до 200 [m]. В допълнение, подвижните управляеми камери трябва да се разположат на специфични места, така че да осигуряват наблюдение и контрол на критични точки, а също и за общо наблюдение. При разполагането на камерите трябва да се предвиди 10 % (десет на сто) припокриване на съседните зони. В случай на аларма от сензорна линия или магнитен сензор, камерата, която покрива съответната секция, трябва автоматично да се насочи в съответната посока. Видеизображението от съответната камера трябва да се появи автоматично на монитор в командния център. Точното разположение на камерите, както и тяхното количество и вид, трябва да се определят на етап детайлно проектиране (тази задача е свързана и с решението за охранително осветление, което следва да се вземе за централата).

Необходимо е да бъдат разчистени растенията от зоните на видеонаблюдение, за да се елиминират “слепите” петна в наблюдаваните участъци от системата за видеонаблюдение.

2.5. ПЕРИМЕТЪРНА СИГУРНОСТ - ПЪТИЩА ЗА ПАТРУЛИРАНЕ

Трябва да се изгради непрекъснат патрулен път по целия периметър в непосредствена близост от вътрешната страна на оградата и полоса за наблюдение от външната. Този път дава възможност на патрулните сили да достигнат всяка една точка от периметъра по най-лесния и бърз начин, така че да проверят, реагират и се справят с различни събития в сферата на защитата и безопасността. Също така, този път следва да се използва за техническо поддържане на оградата с електронно оборудване и на други елементи на системата за сигурност.

Ако се налага, в определени участъци местоположението на оградата може да се промени в процеса на проектиране на патрулния път, за да се осигурят необходимите условия за работа на охранителите и за ревизия на техническите системи за сигурност.

2.6. ПЕРИМЕТЪРНА СИГУРНОСТ - ОХРАНИТЕЛНО ОСВЕТЛЕНИЕ

Целият периметър трябва да се освети с бяла светлина с подходяща интензивност.

Охранителното осветление е от критично значение за идентифицирането и проверяването на подозрителни дейности.

Същевременно то осигурява нормалната работа през нощта на системата за телевизионно видеонаблюдение.

3. ПЕРИМЕТЪРНА СИГУРНОСТ - ПОРТАЛИ

Порталите по външния периметър на централата са критични зони по отношение на сигурността - заради постоянното придвижване на хора, превозни средства и материали. Мерките за сигурност на порталите трябва да се разглеждат като съществена част от мерките за сигурност по периметъра и следва да получават същото внимание (по отношение на сигурността), както останалата част от периметъра.

Първият етап от изпълнението на проекта включва изграждането и реконструкцията на следните портали:

1. Портал “Главен - 1” - нов (буферна зона).
2. Портал “Главен - 2” (основен).
3. Портал “Север”.
4. Портал “Товарен”.

3.1. ПОРТАЛ “ГЛАВЕН - 1” (буферна зона)

Непосредствено пред съществуващия главен портал на отклонението от главния път към централата следва да се изгради нов портал със специфични функции. В пространството между новия портал и съществуващия трябва да се обособи буферна зона за предварителен прием на външни лица. Необходимо е посетителите да имат достъп до съществуващата сграда с киносалона за ползване на различни търговски, финансови и други услуги, свързани с тяхната дейност в “ТЕЦ Марица Изток 2” ЕАД.

За да се отговори на концепцията за сигурност, трябва да се изпълнят следните мерки за сигурност:

№	предлагани мерки	кратко описание
1	2	3
1.	отделни платна	трафикът на моторни превозни средства при портала трябва да се организира в 2 (две) отделни платна - едно за „входящи“ и едно за „изходящи“. Двете платна трябва да бъдат разделени с ръчно управляеми боларди (стандарт К - 8). Порталът обслужва само леки коли и моторни превозни средства със специално предназначение

2.	антитерористични бариери - „боларди” (стандарт K - 8)	за предотвратяване влизането на скорост (с взлом) в централата на превозни средства без разрешен достъп
3.	система за наблюдение под шаситата на моторните превозни средства	сканира автомобилите отдолу - за откриване на бомби, експлозиви и други подозрителни материали. Трябва да се инсталира самостоятелна система за наблюдение на входното платно с подходящи технически характеристики за съответните моторни превозни средства
4.	система за разпознаване на регистрационните номера (2 броя)	идентифицира превозните средства и потвърждава разрешението за достъп
5.	елементи за безопасност и контрол на трафика	за забавяне на трафика при порталите (неравност - изпъкналост за забавяне на скоростта), за функционално подпомагане на елементите от системата за сигурност и за контрол на трафика (предупредителни светлинни сигнали)
6.	неподвижни боларди	за предотвратяване на странично влизане на превозни средства (между двата портала) на буферната зона
7.	прозорец на охранителния пост	външните прозорци на охранителните постове следва да се усилят със защитни решетки или с бронирано стъкло
8.	затворена система за телевизионно видеонаблюдение	подвижни управляеми и стационарни камери - следва да се инсталират, за да се наблюдава и контролира движението на хора и превозни средства през портала
9.	комуникационно оборудване	безжично, мобилни телефони, стационарна телефонна система и кибермрежи, трябва да се използват за докладване и осигуряване на непрекъсната връзка
10.	охранително осветление	районът на портала и заобикалящата го среда трябва да са добре осветени

3.2. ПОРТАЛ “ГЛАВЕН - 2” (основен)

Съществуващият главен портал се използва предимно за преминаване на:

- пешеходци - служители и посетители;
- превозни средства - вход за VIP - коли, специални доставки (поради големия размер на внасяните съоръжения и материали) и моторни превозни

средства със специално предназначение.

На този портал има 24 - часова охрана.

Съществуващите мерки за сигурност не са достатъчни.

За да се отговори на концепцията за сигурност, трябва да се изпълнят следните мерки за сигурност:

№	предлагани мерки	кратко описание
1	2	3
1.	метални детектори рамки - 3 броя	тези устройства осигуряват недопускането на оръжия, експлозиви и други неразрешени предмети през пешеходните входове. На този етап и съобразно с идентифицираните заплахи, не съществува непосредствена необходимост от използването на устройства, различни от металдетекторните рамки. Необходимо е, на етап проектиране да се направи съответната подготовка по отношение на инфраструктурата и потребното пространство, за последващо инсталиране на тези устройства
2.	антитерористична бариера с вертикално рамо	за предотвратяване на нерегламентирано влизане на превозни средства в централата
3.	прозорец на охранителния пост	съществуващите външни прозорци на охранителните постове следва да се усилят със защитни решетки или с бронирано стъкло
4.	затворена система за телевизионно видеонаблюдение	подвижни управляеми и стационарни камери - следва да се инсталират, за да се наблюдава и контролира движението на хора и превозни средства през портала
5.	въртящи се врати „цял ръст" (турникети) с четци на картите за достъп (3 броя)	позволява само на лица с разрешен достъп валидни (карти за достъп) да влизат в централата. Някои от експлоатационни въпроси, които трябва да се вземат предвид са: • посетителите трабва да се снабдяват с временни карти за достъп и задължително трябва да се придружават от упълномощени лица; • посетителите може да преминават само през определени турникети, които може да се контролират и ръчно от охранителя, отговорен за портала;

		• турникетната система трябва да се използва и за контрол на изхода на пешеходци; • системата за контрол на достъпа следва да блокира влизането на всеки, за когото не е регистрирано предишно излизане; • порталният комплекс трябва да се обслужва едновременно най-малко от толкова охранители, колкото е броят на турникетните линии; • охранителите трябва да контролират придвижването в зоната на портала и да идентифицират всяка подозрителна дейност, за да осигурят спазването на правилата за сигурност от всички пешеходци; • контролиращ охранител / супервайзор трябва да присъства на портала, за да контролира всички дейности в тази зона
6.	комуникационно оборудване	безжично, мобилни телефони, стационарна телефонна система и кибермрежи, трябва да се използват за докладване и осигуряване на непрекъсната връзка
7.	охранително осветление	районът на портала и заобикалящата го среда трябва да са добре осветени

Забележка: Всички дейности при двата главни портала, независимо от това дали са отворени или не и цялата буферна зона, трябва да се наблюдават от Главната командно - контролна система за сигурност.

3.3. ПОРТАЛ "СЕВЕР"

Съществуващият северен портал се използва предимно за преминаване на:

- пешеходци - служители, посетители, доставчици, шофьори и други лица с разрешен достъп;
- превозни средства - леки коли и камиони за доставяне на различни материали и суровини за производствения процес.

На този портал има 24 - часова охрана.

Съществуващите мерки за сигурност не са достатъчни.

За да се отговори на концепцията за сигурност, трябва да се изпълнят следните мерки за сигурност:

№	предлагани мерки	кратко описание
1	2	3
1.	отделни платна	трафикът на моторни превозни средства при портала трябва да се организира в 2 (две) отделни платна - 1 (едно) за „входящи“ и 1 (едно) за „изходящи“. Необходимо е ръчно управляеми боларди (стандарт K - 8) да разделят “входящото” от “изходящото” платна.
2.	елементи за безопасност и контрол на трафика (на входа и на изхода)	за забавяне на трафика при порталите (неравност - изпъкналост за забавяне на скоростта), за функционално подпомагане на елементите от системата за сигурност и за контрол на трафика (предупредителни светлинни сигнали)
3.	антитерористични бариери - „боларди” (стандарт K - 8)	за предотвратяване влизането на скорост (с взлом) в централата на превозни средства без разрешен достъп
4.	бариера тип “вертикално рамо” (2 броя)	позволява проверяване на водачите и моторните превозни средства преди влизането / излизането и дава възможност за контрол на движението
5.	система за разпознаване на регистрационните номера (2 броя)	идентифицира превозните средства и потвърждава разрешението за достъп
6.	система за наблюдение под шаситата на моторните превозни средства	сканира автомобилите отдолу за откриване на бомби, експлозиви и други подозрителни материали. Трябва да се инсталират 1 (една) система за наблюдение на „входното“ платно с подходящите технически характеристики за съответните моторни превозни средства
7.	рентгенов скенер за багаж, сниферн и метални детектори (метални детектори рамки - 3 броя)	тези устройства осигуряват недопускането на оръжия, експлозиви и други неразрешени предмети през пешеходните входове. На този етап и съобразно с идентифицираните заплахи, не съществува непосредствена необходимост от използването на устройства, различни от металдетекторните рамки. Необходимо е, на етап проектиране да се направи съответната подготовка по отношение на инфраструктурата и потребното пространство, за

		последващо инсталиране на тези устройства
8.	четци на идентификационни карти (на две нива, съответно за коли и за камиони)	трябва да се инсталират на стойки, за да се идентифицират водачите и да се потвърди разрешението за тяхното влизане с камионите и леките коли. Подобни стойки с четци на карти трябва да се инсталират и на изхода, за да регистрира излизането на водачите от територията на централата
9.	процес на контрол на сигурността за камиони и други моторни превозни средства	концепцията за сигурност при влизане на камиони и други моторни превозни средства се основава на следните принципи: • само на камиони и водачи с разрешен достъп се позволява да влизат през портала; • камиони без разрешен достъп не може да влизат в централата; • водачи без разрешен достъп също не може да влизат през портала; • на пешеходци или други лица - като например асистенти (съпровождащи) на водачите или велосипедисти, не трябва да се разрешава да преминават през входа / изхода за камиони; • всички камиони и водачи, които имат разрешен достъп, трябва да преминават проверка за сигурност на влизане; • трябва да се осигури поне по1 (един) охранител за „входното“ и 1 (един) охранител за „изходното“ платно на входа за товарни камиони
10.	въртящи се врати „цял ръст” (турникети) с четци на картите за достъп - 3 броя	те позволяват само на лица с разрешен достъп - пешеходци да влизат в централата. Предлаганите мерки включват: • най-малко 1 (един) отделен турникет трябва да се използва за асистентите (съпровождащи) на водачите. Входът за посетители и лица с временен достъп - като сервизни работници и техници (група № 1) трябва да е отделен с парапети от турникетите (най-малко 2 (два)), които се използват от служителите и други лица с разрешен постоянен достъп (група № 2); • турникети за пешеходци трябва да се използват за контрол на изхода за всички лица; • системата за контрол на достъпа следва да блокира влизането на всеки, за когото не е регистрирано предишно излизане; • трябва да има поне по 1 (един) охранител

		на всеки турникет на портала; • контролиращ охранител / супервайзор трябва да присъства на портала, за да контролира всички дейности в тази зона; • охранителите трябва да контролират придвижването в зоната на портала и да идентифицират всяка подозрителна дейност, за да се осигури спазването на правилата за сигурност от всички пешеходци: Група1 - трябва да се инспектира и идентифицира лично от охранителите чрез проверяване на валидността на картите за достъп на всяко от влизащите лица. Посетителите трябва да имат временни карти за достъп и трябва да се придружават от упълномощени лица;
		Група2 - трябва да се проверява на случаен принцип от охранителите
11.	прозорец на охранителния пост	съществуващите външни прозорци на охранителните постове следва да се усилят със защитни решетки или с бронирано стъкло
12.	затворена система за телевизионно видеонаблюдение	подвижни управляеми и стационарни камери - следва да се инсталират, за да се наблюдава и контролира движението на хора и превозни средства през портала. Два броя стационарни камери, които да бъдат монтирани на високи пилони, за наблюдение на каросериите на камионите
13.	комуникационно оборудване	безжично, мобилни телефони, стационарна телефонна система и кибермрежи, трябва да се използват за докладване и осигуряване на непрекъсната връзка
14.	охранително осветление	районът на портала и заобикалящата го среда трябва да са добре осветени

Забележка: Всички дейности при този портала, независимо от това дали е отворен или не, трябва да се наблюдават от Главната командно - контролна система за сигурност.

3.4. ПОРТАЛ "ТОВАРЕН"

Съществуващият товарен портал трябва да се реконструира и да се използва предимно за преминава на:

- пешеходци - не се предвижда да преминават;
- превозни средства - камиони за доставяне на различни материали, предимно на варовик.

На този портал има 24 - часова охрана.

Съществуващите мерки за сигурност не са достатъчни.

За да се отговори на концепцията за сигурност, трябва да се изпълнят следните мерки за сигурност:

№	предлагани мерки	кратко описание
1	2	3
1.	едно широко платно	трафикът на моторни превозни средства при портала трябва да се организиран в 1 (едно) платно за „входящи“ за „изходящи“)
2.	елементи за безопасност и контрол на трафика	за забавяне на трафика при порталите (неравност - изпъкналост за забавяне на скоростта), за функционално подпомагане на елементите от системата за сигурност и за контрол на трафика (предупредителни светлинни сигнали и светофари)
3.	антитерористични бариери - „боларди” (стандарт K - 8)	за предотвратяване влизането на скорост (с взлом) в централата на превозни средства без разрешен достъп
4.	бариера тип “вертикално рамо” - 2 броя	позволява проверяване на водачите и моторните превозни средства преди влизането / излизането и дава възможност за контрол на движението
5.	система за разпознаване на регистрационните номера на влизане и излизане (2 броя)	идентифицира превозните средства и потвърждава разрешението за достъп
6.	система за наблюдение под шаситата на моторните превозни средства	сканира автомобилите отдолу за откриване на бомби, експлозиви и други подозрителни материали. Трябва да се инсталира самостоятелна система за наблюдение с подходящите технически характеристики за съответните моторни превозни средства (в случая камиони)
7.	четци на идентификационни карти (на две нива за коли и	трябва да се инсталират на стойки, за да се идентифицират водачите и да се потвърди

	камиони)	разрешението за тяхното влизане с камионите. Подобна стойка с четец на карти трябва да се инсталира и на изхода, за да регистрира излизането на водачите от територията на централата
8.	процес на контрол на сигурността за камионите	концепцията за сигурност при влизане на камионите се основава на следните принципи: • само на камиони и водачи с разрешен достъп се позволява да влизат през портала; • камиони без разрешен достъп не може да влизат в централата; • водачи без разрешен достъп също не може да влизат; • на пешеходци или други лица - като например асистенти (съпровождащи) на водачите или велосипедисти, не трябва да се разрешава да преминават през този портал; • всички камиони и водачи, които имат разрешен достъп, трябва да преминават проверка за сигурност на влизане;
9.	прозорец на охранителния пост	съществуващите външни прозорци на охранителните постове следва да се усилят със защитни решетки или с бронирано стъкло
10.	затворена система за телевизионно видеонаблюдение	подвижни управляеми и стационарни камери - следва да се инсталират, за да се наблюдава и контролира движението на хора и превозни средства през портала. Два броя стационарни камери, които да бъдат монтирани на високи пилони, за наблюдение на каросериите на камионите
11.	комуникационно оборудване	безжично, мобилни телефони, стационарна телефонна система и кибермрежи, трябва да се използват за докладване и осигуряване на непрекъсната връзка
12.	охранително осветление	районът на портала и заобикалящата го среда трябва да са добре осветени

Забележка: Всички дейности при този портала, независимо от това дали е отворен или не, трябва да се наблюдават от Главната командно - контролна система за сигурност.

4. “ТЕЦ МАРИЦА ИЗТОК 2” ЕАД - ОБЕКТИ

В централата трябва да се структурират защитени зони - единични или комплекси от различни обекти обособени в една зона. Всяка една от тях следва да се оборудва с необходимите технически средства за сигурност, които трябва да осигурят желаното равнище на сигурност и безопасност.

Подходящото техническо решение, което включва разполагането на различни технически средства по видове и количества, трябва да се изберае на етап проектиране, като част от цялостния инженерингов проект.

Топлоелектрическата централата има 16 (шестнадесет) комплекса от обекти (активи, оперативни процеси или цели), които са обособени като отделни части (зони) в рамките на съответната специфична област в централата. В тези 16 (шестнадесет) функционални комплекса са включени 8 (осем) външни комплекса от обекти, разположени на външния периметър и 8 (осем) вътрешни комплекса от обекти, които са във вътрешния периметър на централата.

През първия етап от реализацията на проекта външните обекти, които ще бъдат ремонтирани и оборудвани с технически средства са:

1. Паркинг за камиони и зони за изчакване при северния портал;
2. Паркинг за служители и VIP - паркинг - главен портал;

4.1. ПАРКИНГ ЗА КАМИОНИ И ЗОНИ ЗА ИЗЧАКВАНЕ ПРИ СЕВЕРЕН ПОРТАЛ

Зоната за временно паркиране и зоната за изчакване на камионите за доставка са в обществената зона - извън територията на централата - в близост до северния портал.

Няма съществуващи мерки за сигурност.

За да се отговори на концепцията за сигурност, трябва да се изпълнят следните мерки за сигурност:

№	предлагани мерки	кратко описание
1	2	3
1.	затворена система за телевизионно видеонаблюдение	наблюдението в зоната към подхода за "северния" портал следва да се осигури чрез подвижни управляеми камери, които трябва да осигуряват общо наблюдение и разследване в случай на проблем със сигурността
2.	охранително осветление	целият обект и околностите трябва да имат подходящо охранително осветление

4.2. ПАРКИНГ ЗА СЛУЖИТЕЛИ И VIP - ПАРКИНГ - ГЛАВЕН ПОРТАЛ

Паркинг зоната за служители и VIP - паркинга са разположени извън периметъра на централата до главния портал и битовата сграда (киносалона). Паркингът за посетители и подизпълнители е разположена в обществената зона в близост до главния портал и се намира извън периметъра на централата.

Няма съществуващи мерки за сигурност.

VIP - паркингът следва да се премести на мястото на сегашния паркинг за служители и да се вкара в периметъра на общата ограда.

За да се отговори на концепцията за сигурност, трябва да се изпълнят следните мерки за сигурност:

№	предлагани мерки	кратко описание
1	2	3
1.	физическа ограда	цялата зона следва да се загради с физическа ограда за вътрешен периметър със специално определените вътрешни контролно - пропускателни пунктове по периметъра на зоната. Едната от страните на паркинга съвпада с външната ограда на централата
2.	затворена система за телевизионно видеонаблюдение	да се монтират стационарни камери за следене и контрол на преминаващите хора и трафика на превозни средства през пунктовете на зоната и подвижни камери за панорамно наблюдение на периметъра на зоната
3.	система за контрол на достъпа	системата за контрол на достъпа трябва да се монтирана на обособените контролно - пропускателни пунктове за пропускане на хора и моторни превозни средства. Контролът за достъп трябва да включва: управляеми изпълнителни механизми (въртящи се врати в пълен размер "турникети" и бариери с вертикално рамо) и електронни модули (двустранни четеци на идентификационни карти за влизане и излизане, детектор, следящ положението на изпълнителния механизъм; възможност за дистанционно управление на бариерата от Главния командно - контролен център за сигурност
4.	охранително осветление	цялата зона, пропускателните пунктове и околностите трябва да са осветени подходящо
5.	дистанционно наблюдение от Главния командно - контролен център за сигурност	всички движения на коли и хора в зоната (независимо дали са в светлата или тъмната части от деня) трябва да са под непрекъснат видеоконтрол

5. ПРЕУСТРОЙСТВО НА СГРАДА „СТОЛОВА И КИНОСАЛОН“ С ПРОМЯНА НА ФУНКЦИОНАЛНОТО ПРЕДНАЗНАЧЕНИЕ - ОТ КИНОСАЛОН В АДМИНИСТРАТИВНИ ОФИСИ.

5.1. ОБЩИ СВЕДЕНИЯ.

Сградата, в която са разположени столовата и киносалона се намира в непосредствена близост до Главна административна сграда на централата и контролно-пропускателен пункт при главен портал.

Същата е построена през 1964 - 1965 година. Състои се от високо тяло и две по-ниски тела. В ниската част са разположени складовете, кухнята, стола за ИТР и стая за персонала. Високата част се състои от 3 етажни нива.

В 1-во етажно ниво е разположена столова с достъп от запад през ниското тяло и зала за първоначален инструктаж с независим достъп от изток.

Във II-ро етажно ниво са разположени - киносалонът, офис помещения, тоалетни и други.

В III-то етажно ниво са разположени - кинокабина, складови помещения, тоалетни и други.

II-ро и III-то етажно ниво са със самостоятелен вход от изток, не изискващ преминаване през Главния КПП на централата.

Сутерен има само под половината от ниското тяло. Там е разположена абонатната станция и бойлерна уредба. От там тръгват и тръбните разводки за водоснабдяване и отопление на цялата сграда.

Високото тяло, предмет на настоящото преустройство е с масивна, скелетно-гредова конструкция (сглобяема). Външните и вътрешните ограждения са от тухлена зидария. Източната фасада е с алуминиеви витрини; северната фасада - бетонова декоративна решетка (допълнително зазидана); западна и южна - без особености.

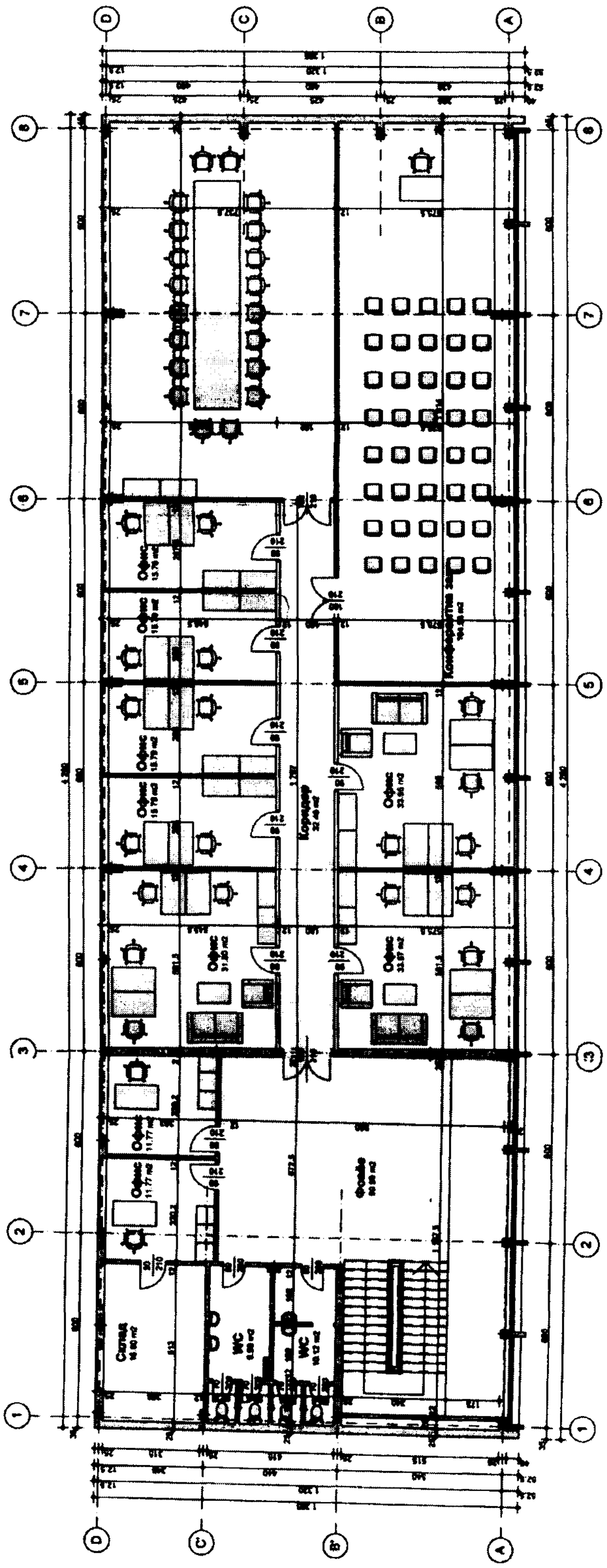
Покривът е едноскатен, с наклон от изток към запад. Изпълнен е с покривно покритие от битумни мембрани. Водоотвеждането е външно посредством улуци и водосточни тръби.

Идеята на настоящото преустройство е разделяне на високия обем на киносалона с междинна етажна плоча и обособяване на две офис - административни нива.

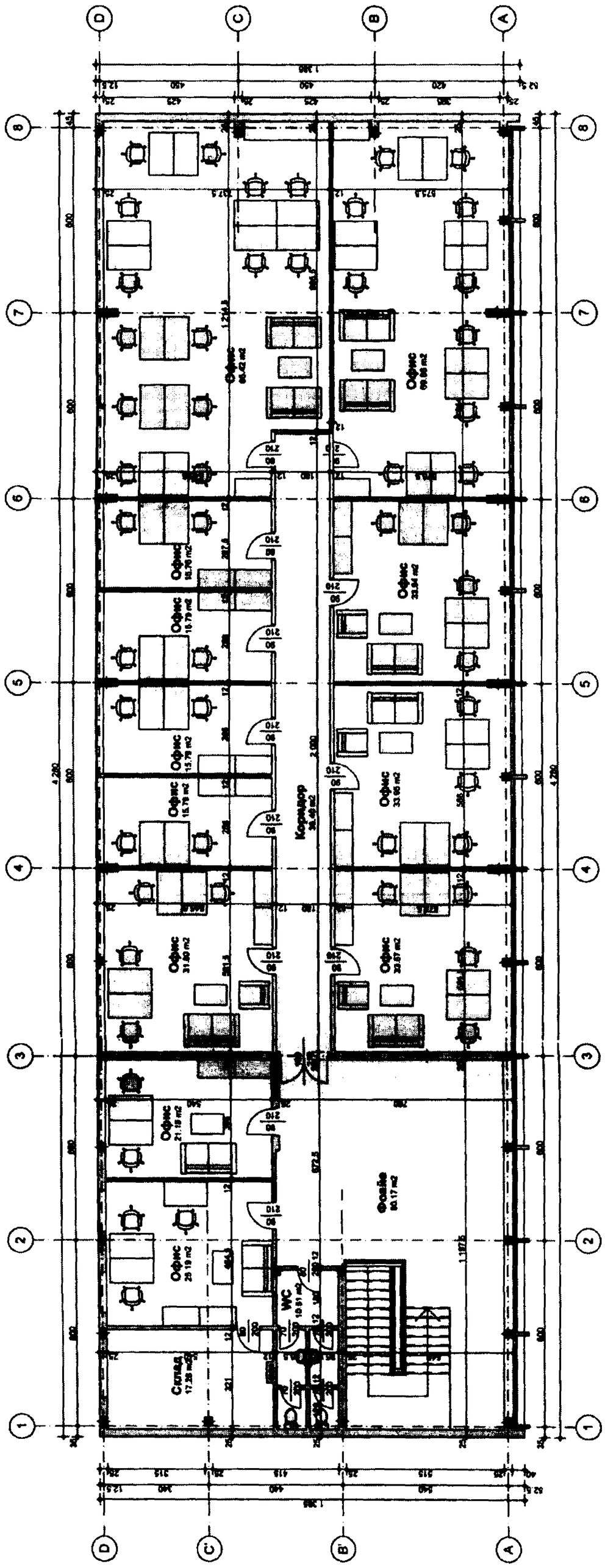
В тях ще се разположи външният административен кръг, включващ онези отдели и звена, на които се налага да работят с физически лица и с представители на юридически лица, извършващи съвместна административна дейност с „ТЕЦ Марица изток 2” ЕАД без необходимост от пропускателен режим за промишлената площадка.

Възложителят разполага с примерни архитектурни проекти, които желае да бъдат изпълнени. Примерните проекти са приложени като неразделна част настоящето описание и са приложени на фигура № 5.1. - 2 (първо ниво) и на фигура № 5.1. - 3 (второ ниво).

В архивната документация на централата не беше открит строително - конструктивен проект, което означава, че изпълнителят ще трябва сам да заснеме необходимите му изходни данни.



фигура № 5.1. - 2



фигура № 5.1. - 3

5.2. ИЗИСКВАНИЯ КЪМ ПРОЕКТА.

При разработването на работния проект всички части следва да са придружени с обяснителни записки и технически изчисления, както следва:

№	части на проекта	съдържание
01	02	03
1.	Архитектурна	Архитектурни разпределения; План на покрива; Фасади; Разрези; специфични архитектурни детайли; спецификации
2.	Топлотехническа ефективност	Технически изчисления; детайли
3.	Конструктивна	Инженерно геоложко проучване; Обследване на съществуващата канализацияция, включващо: визуален оглед; конструктивно заснемане; обектово замерване, свързано с разкривки на конструктивните елементи; контрол и оценка на вложения в к-циите бетон и армировка; лабораторни изследвания и други; моделно изследване; конструктивна експертиза; Мероприятия по усилване на съществуващи конструктивни елементи в случай на необходимост. Разработване на нови конструктивни елементи / фундаменти, греди, колони, връзки / с оглед поемане на натоварвания от допълнителното етажно ниво. Кофражни и армировъчни планове (при монолитно изпълнение); Монтажни планове; КМД чертежи при сглобяеми и метални к-ции; спецификации; статически изчисления и други.
4.	Водоснабдяване и канализация	Вътрешни В и К мрежи; Външни В и К - подвързване към присъединителните т-ки; Технически изчисления
5.	Електро	Вътрешни електроинсталации: силова, осветителна, заземителна, мълниезащитна, структурно окабеляване (компютърни и телефонни връзки); Контрол за достъп; Районно осветление; Пожароизвестителна. Технически изчисления.

6.	ОВК	Отопление: изпълняват се два инсталации: - Въздушноохлаждаем водоохлаждащ агрегат (охладителна + отоплителна мощност); - мрежова вода от централно захранване. Осигурена принудителна вентилация за помещенията.
7.	Част пожарна безопасност	Съгласно ПСТН2 и Наредба № Із-1971 от 29 октомври 2009 година за строително-техническите правила и норми за осигуряване на безопасност при пожар.
8.	План за беозпасност и здраве	ПБЗ да бъде изготвен в съответствие с изискванията на Наредба № 2 от 22.03.2004 година на МТСП и МРРБ за минималните изисквания за здравословни и безопасни условия на труд при извършване на строителни и монтажни работи.

ЗАБЕЛЕЖКИ:

- Възложителят ще предостави на Изпълните всички изходни данни с които разполага;
- Категоризиране на строежа - I-ва категория по чл. 137 от ЗУТ;
- Гарантиран срок - съгласно Рамковото споразумение;
- Присъединителните точки ще бъдат заснети от изпълнителя;
- Предварителният оглед е задължителен;
- Всички части на проекта да бъдат взаимосъгласувани;
- Част конструктивна проверена и съгласувана от Технически контрол съгласно чл. 139 от ЗУТ.

5.2.1. ИЗИСКВАНИЯ КЪМ ПРОЕКТА ПО ЧАСТ „АРХИТЕКТУРА“

За база на проектирането ще служат приложените по-горе архитектурни разпределения на двете нива. Преградните стени между офисите и коридорите, както и между самите офиси да бъдат от лек тип (щендерни) от гипсокартон - 2 пласта. Стените са с дебелина минимум 12 [sm] и пълнеж от минерална вата за изолация. Външните оградни стени се обшиват от вътрешна страна с гипсокартон върху конструкцията и се топлоизолират с необходимия брой слоеве от минерална вата. Пакетите от инсталационни тръби се скриват с обшивка от влагоустойчив гипсокартон на конструкцията. Стените се шпакловат и боядисват с акрилна боя с цвят по мостра.

Дограмата е алуминиева с прекъснат термомост и прозрачен стъклопакет от нискоемисионно стъкло. Помещенията трябва да бъдат добре осветени, съобразно с нормативните наредби. Източната фасада да бъде акцент на сградата, да се изпълни със структурно окачено фасадно

остъкление, двубариерни структурни стъклопакети, достатъчен като брой и размери отваряеми елементи. Вратите на помещенията към коридорите са алуминиеви с остъклена надстройка за осигуряване индиректно осветяване на коридорите.

Всички зидове на санитарно-битовите помещения са от тухлена зидария. Стенните облицовки в санитарните и санитарно-битовите помещения са от фаянс.

Подовите настилки в офис помещенията и коридорите са от гранитогрес. Теракот се предвижда за санитарните помещения, а фоайетата, стълбищните стъпала и площадки се облицоват с гранит. За постигане на едно ниво в преходите между настилките се ползват компенсационни лайсни, ако се налага.

Фасадите на сградите да бъдат изпълнени в съответствие със система XPS (екструдиран пенополистирен) на BAUMIT или еквивалентна система. Поради агресивния характер на средата мазилката да бъде силиконова.

Цокълът на сградата и външното стълбище при главния вход се облицова с камък. За стълбищната клетка да се предвидят алуминиеви парапети.

Покривното покритие да се изпълни с ЛТ стоманени листове с PVC покритие.

Водоотвеждаща покривна система (улуци, водосточни тръби) да бъде от PVC с UV добавки, гарантиращи дългосрочна експлоатация.

5.2.2. ИЗИСКВАНИЯ КЪМ ПРОЕКТА ПО ЧАСТ „КОНСТРУКТИВНА“

Разработва се въз основа на предварително одобрен архитектурен проект от страна на Възложителя, съобразно новите натоварвания от преустройството и съгласно действуващата нормативна база.

5.2.3. ИЗИСКВАНИЯ КЪМ ПРОЕКТА ПО ЧАСТ „В И К“

Предвижда се самостоятелно захранване, чрез директно сградно отклонение към площадкови колектори за питейна и противопожарна вода. В точките на присъединяване да се предвиди необходимата изолираща арматура, разклонения и други. Сградното отклонение за питейна вода се изпълнява от вкопани, полиетиленови тръби. Вътрешните водопроводни инсталации за топла и студена вода се изпълняват чрез скрит монтаж от полипропиленови тръби (изолирани). Фитингите и арматурите да са съвместими с тази система. Преминаването на всички вертикални клонове през етажните плочи се изпълнява чрез ползване на гилзи от шумо и водоизолиращ материал (пенополиетилен).

Затоплянето на водата за мивките ще се извършва чрез електрически бойлер/и.

Канализационните тръби и съединения се изпълняват от твърд PVC (БДС 12996-75). Ще се ползва съществуващото сградно отклонение. При констатирана необходимост същото се ревизира.

5.2.4. ИЗИСКВАНИЯ КЪМ ПРОЕКТА ПО ЧАСТ „ЕЛЕКТРИЧЕСКА“

Проектът и изпълнението по част електрическа да включва:

- **Силова инсталация и ел. контакти**

Главното ел. захранване да се вземе от съществуващо табло ТНН намиращо се в столовата (ниската част на сградата) със захранващ кабел неразпространяващ горенето. В помещението на ТНН да се проектира извод за ел. захранване на новата част от сградата в ново силово табло монтирано на стената и оборудвано с прекъсвач и самостоятелен трифазен електромер за измерване на консумираната активна и реактивна енергия. В сградата да се предвидят главно разпределително табло офиси и минимум 4 броя етажни ел. табла за захранване на отделните групи консуматори, включително вентилаторни конвектори за отопление и охлаждане, рекуператори, както и машинно табло за управление на 2 броя помпи използувани за климатизацията в офисите. В ГРТ офиси да се проектира извод за въздухоохлаждаем водоохлаждащ агрегат с минимум 40÷45 [kW] електрическа мощност. Магистралните кабели да бъдат монтирани и положени в метални поцинковани кабелни скари от типа на „Обо Бетерман“ или такива с еквивалентно качество. Разклонителните кутии да са с подходящ размер за комутация и изходните радиалните кабели зад гипсокартон или в стена да са положени в цели гофрирани шлаухи с подходяш диаметър за лесно изтегляне. Избраната инсталационна схема да бъде **/TN-S/.** ГРТ офиси да бъде монтирано в отделно помещение преградено с негорима преграда (врата). Използуваната апаратура и материали да бъдат от реномирани фирми и качество (например Schneider, legrand, GE или други с еквивалентно качество). При проектирането **и** изпълнението да се предвиди блокировка на приходната вентилация при сигнал за пожар.

Да се предвидят предмети за първоначално обзавеждане.

- **Осветителна инсталация**

Осветителната инсталация да включва вътрешна осветителна инсталация, външна осветителна инсталация (районно осветление включващо паркинга, централния портал и стола) и евакуационно осветление. Външната осветителна инсталация да има ръчно и автоматично управление посредством часовник или реле програматор, а вътрешната в коридорите да се управлява посредством импулсни релета и ключове осигуряващи дежурно и работно осветление. Осветителните тела да бъдат с електронно запалване ЕПРА. Използуваната апаратура, осветителни тела и материали да бъдат от реномирани фирми и качество.

- **Пожароизвестителна инсталация**

Пожароизвестителната инсталация да бъде от адресируем тип и да отговяря на изискванията от Техническото задание. Пожароизвестителната инсталация да съдържа необходимите компоненти и софтуер и да бъде включена към съществуващата централизирана система за мониторинг на „ТЕЦ Марица изток 2” ЕАД. При проектирането и изпълнението да се предвидят допълнителни изходи за блокиране на приходната вентилация при сигнал за пожар.

- **Структурно окабеляване (компютърни и телефонни връзки)**

Да бъде проектирано структурно окабеляване, като за всяко работно място бъде предвидена двойна розетка RJ45 (PC/Tel). Да се предвиди нов шкаф RACK с размери осигуряващи окабеляването на всички работни места, конферентната и заседателна зала. Активното и пасивно оборудване в RACK да бъде до окомплектовано за осигуряване на по големия брой потребители в новите офиси. Да се включи телефонен панел раково изпълнение за развиване на 50 чифтов телефонен кабел Всички кабели от структурното окабеляване да бъдат положени по

отделни метални поцинковани кабелни скари от типа на „Обо Бетерман“ или такива с еквивалентно качество. Вертикалните спусъци да са изтеглени в цели гофрирани шлаухи с подходящ диаметър за лесно изтегляне. Използуваната апаратура и материали да бъдат от реномирани фирми и качество.

- **Мълниезащитна инсталация**

Да се проектира и изпълни мълниезащитна инсталация с мълниеприемник с изпреварващо действие с време на изпреварване ≥60 [ms].

- **Заземителна инсталация**

Да се проектира и изпълни нова заземителна инсталация, която да се свърже към съществуващата.

5.2.4. ИЗИСКВАНИЯ КЪМ ПРОЕКТА ПО ЧАСТ „ОВК“

- **Отопление -** 2 инсталации:

1. Въздушноохлаждаем водоохлаждащ агрегат (охладителна + отоплителна мощност);
2. Мрежова вода централно захранване tвх = 85°C; tвх= 65°C – ал. радиатори, колектор, пластинчат топлообменник, отделен (самостоятелен) кръг само за сградата.

- **Вентилация**

Да се предвиди нагнетателна и смукателна вентилация, за конферентни зали, коридори, фоайета, санитарни възли. Изходите от смукателната вентилация да се изведат към съществуващите въздуховоди, а където липсват да се изградят нови. Да се предвиди и присъединяване към пожароизвестителна инсталация.

За цялостното обслужване на ОВК да се предвидят тръбна разводка, носеща конструкция, фасони части, разпределителни колектори, помпи, кранове, изолация за тръби, въздуховоди гъвкави, фасони части за гъвкави въздуховоди, топлоизолация за въздуховоди, ел. табла и елементи за автоматично регулиране.

5.3. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

По време на изпълнението Изпълнителят стриктно спазва действуващия правилник за извършване на СМР (ПИПСМР). Процесът на изпълнение е осигурен с постоянен авторски надзор.

Изменения по проекта се допускат само след предварително съгласуване от страна на Възложителя и след запис в заповедната книга от проектанта по съответната част. Всяко изменение се оформя като екзекутив, който се прилага към досието на строежа. В процеса на строителство изпълнителят изготвя изискваните документи съгласно Наредба № 3 от 31 юли 2003 година за съставяне на актове и протоколи по време на строителството.

ЗАБЕЛЕЖКА:

Демонтажът на съществуващото оборудване, инсталации и други (театрална сцена, седалки за зрители в киносалон; окачени тавани; стенни облицовки; подови настилки; врати и прозорци; обзавеждане на санитарни помещения; демонтаж на зидария) влиза в обемът от задължения на Изпълнителя.

5.4. БЕЗОПАСНОСТ, ХИГИЕ НА ТРУДА И ПРОТИВОПОЖАРНА ОХРАНА

За допускане до работа Изпълнителят изготвя необходимия пакет документи съгласно регламента и Правилника за вътрешния ред в централата, които се предоставят от ОБЗР и организира издаването на пропуск за достъп и работа в централата.

Преди започване на работа Изпълнителят е дръжен да разработи План за безопасност и здраве съгласно изискванията на Наредба №2 от 22.03.2004 година. При нужда го актуализира, подписва и осигурява необходимите по плана длъжностни лица за контрол.

Изпълнителят е длъжен да използва по време на строителството само изправни и отговарящи на техническите изисквания съоръжения и инструменти.

Изпълнителските кадри да имат необходимата квалификация и правоспособност. Преминаването на същите през първоначален инструктаж от отдел "Безопасност и здраве" към централата е задължителен и предшествува началото на изпълнение на подготвителни и същински строително-монтажни работи.

Изпълнителя се задължава да организира разработване и спазване на план за предотвратяване и ликвидиране на аварии.

5.5. ДРУГИ УСЛОВИЯ

Преди започване на всякакви дейности Изпълнителят огражда строежа с временна ограда с естетичен вид. След завършване на строежа оградата се демонтира и нейните елементи се изнасят от обекта.

Необходимите в процеса на изпълнение ел. енергия и производствена вода се осигуряват от и за сметка на Възложителя.

За временни помещения по време на строителството като съблекални, складове за дребен инвентар и други подобни, Изпълнителя може да използва подвижни фургони, които се монтират на място, съгласувано с Възложителя.

Изпълнителят е задължен ежедневно след привършване на работата да оставя строителната прощадка подредена и чиста.

За битови отпадъци Изпълнителя следва да си осигури контейнер, а строителните да извозва на депо за строителни отпадъци, находящо се на около 30 [km] от местостроежа (сметище в град Нова Загора). Товарните коли преминават през електронната везна при Северен портал на централата за отчет на всеки курс пълен/празен. Таксите на депото са за сметка на централата.

Демонтираното оборудване се транспортира на определени за целта площадки и складове на централата - разстояние от местостроежа до 1.5 [km].

5.6. ТЕХНИЧЕСКИ СИСТЕМИ ЗА СИГУРНОСТ

За да се отговори на концепцията за сигурност, трябва да се изпълнят следните мерки за сигурност:

- пожароизвестителна система;
- пожарогасителна система;
- осветление, включително аварийно;
- електрическо и електронно заземяване;
- отоплителна, вентилационна и климатична инсталация с пълно дублиране;
- комуникации.

№	предлагани мерки	кратко описание
1	2	3
1.	въртящи се врати „цял ръст" (турникети) с четци на картите за достъп	те позволяват само на лица с разрешен достъп - пешеходци да имат достъп до административните офиси. Предлаганите мерки включват: • 1 (един) отделен турникет трябва да се използва за посетители. Входът за посетители и лица с временен достъп - като сервизни работници и техници (група № 1) трябва да е отделен от турникетите (най-малко 2 (два)), които се използват от служителите и други лица с разрешен постоянен достъп (група № 2); • турникети трябва да се използват за контрол на изхода за всички лица; • системата за контрол на достъпа следва да блокира влизането на всеки, за когото не е регистрирано предишно излизане; • трябва да има поне 1 един охранител на входа на сградата; • охранителите трябва да контролират придвижването в зоната на входа на сградата и да идентифицират всяка подозрителна дейност, за да се осигури спазването на правилата за сигурност от всички пешеходци:
2.	рентгенов скенер за багаж, и метални детектори	тези устройства осигуряват недопускането на оръжия, експлозиви и други неразрешени предмети през пешеходния вход. На този етап и съобразно с идентифицираните заплахи, не съществува непосредствена необходимост от използването на

		устройства, различни от металдетекторните рамки. Необходимо е, на етап проектиране да се направи съответната подготовка по отношение на инфраструктурата и потребното пространство, за последващо инсталиране на тези устройства
3.	четци на идентификационни карти	трябва да се инсталират до вртатите на помещенията с ограничен достъп за посетители. От вътрешната страна на помещенията трябва да се инсталират бутони „ИЗХОД“, които да отварят вратите при излизане от помещенията
4.	затворена система за телевизионно видеонаблюдение	стационарни камери - следва да се инсталират, за да се наблюдава и контролира движението на хора при входа на сградата, във фоайетата и коридорите ѝ и фасада
5.	комуникационно оборудване	безжично, мобилни телефони, стационарна телефонна система и кибермрежи, трябва да се използват за докладване и осигуряване на непрекъсната връзка
6.	пожароизвестителна инсталация	трябва да осигурява пожарната безопасност на всички помещения в сградата.
7.	пожарогасителна инсталация	трябва да осигурява пожарната безопасност на помещението, предвидено за инсталиране на комуникационното оборудване и новия шкаф RACK.

ЗАБЕЛЕЖКА: Участниците имат възможност да направят оглед на обекта, за да уточнят с Възложителя конкретното местоположение на отделните подобекти, порталите, трасетата на оградата, обходните пътища и полосата за наблюдение, особеностите на сградата за преустройство, комуникационните трасета и други въпроси.

ВТОРО: ТЕХНИЧЕСКИ ИЗИСКВАНИЯ

СЪДЪРЖАНИЕ

1. Увод

1.1. Основни положения
1.2. Основни характеристики
1.3. Принципи на решението за сигурността

2. Мерки за сигурност
2.1. Равнища на сигурност и защита
2.2. Етапи на изпълнение

3. Съдържание на мерките за сигурност
3.1. Концептуална блок - схема
3.2. Интегрирани системи за сигурност

4. Система за контрол на достъпа (СКД)

4.1. Основни положения

4.2. Компоненти

4.3. Технически изисквания
4.3.1. Безконтактна (Proximity) карта
4.3.2. Картови четци
4.3.3. Геометрия на ръка или пръстов отпечатък
4.3.4. Контролери за контрол на достъпа
4.3.5. Електрически и магнитни ключалки
4.3.6. Плъзгаща се врата
4.3.7. Турникет (пълен размер)
4.3.8. Турникет (триножник)
4.3.9. Антитерористични бариери (АТБ)
4.3.10. Бариери с вертикално рамо (БВР)
4.3.11. Свръхмощни бариери с вертикално рамо (СБВР)
4.3.12. Помощни елементи за трафика и безопасността
4.3.13. Металдетекторна рамка (врата)
4.3.14. Рентгенов скенер за идентифициране и проверяване на багажа

4.3.15. Превключватели на позициите на вратите
4.3.16. Бутони за отваряне на вратите
4.4. Система за управление на контрола на достъпа (СУКД)
4.4.1. Основни характеристики
4.5. Илюстрирана блок - схема

5. Алармена система срещу проникване за периметърна охрана (АССППО)
5.1. Основни положения
5.2. Характеристики и компоненти
5.3. Физическа стоманена ограда и структура - основни изисквания
5.4. Физическа стоманена ограда и структура - технически изисквания
5.4.1. Физическа стоманена ограда - бетонов фундамент / бетонови стъпки и вкопана стаманена мрежа
5.4.2. Физическа стоманена ограда - мрежа от галванизирана стомана
5.4.3. Физическа стоманена ограда - „външен“ кльон
5.4.4. Физическа стоманена ограда - режеща серпентина
5.5. Нова ограда за критичните обекти (зони) във вътрешния периметър
5.5.1. Мрежа от поцинкована заварена стомана за критичните обекти (зони) във вътрешния периметър
5.5.2. „Вътрешен“ кльон за критичните обекти (зони) във вътрешния периметър
5.6. Алармена система срещу проникване за периметърна охрана - електронна алармена система срещу проникване (ЕАССП)
5.6.1. Основни характеристики
5.6.2. Компоненти
5.6.3. Общи изисквания за изпълнение
5.6.4. Свойства на детектиране
5.6.5. Лъжливи аларми
5.6.6. Характеристики на сензорите
5.7. Спецификации на сигналните процесори
5.7.1. Описание на сигнален процесор
5.7.2. Работа на сигналния процесор
5.7.3. Обща дължина на оградата, защитена от системата
5.7.4. Алармени изходи
5.7.5. Мрежов транспордер и централен контролер
5.7.6. Работен диапазон в зависимост от околната среда
5.7.7. Изисквания към елктрическото захранване

5.7.8. Надеждност / ремонтопригодност
5.7.9. Критерии за инсталиране
5.7.10. Калибриране на сензорите
5.7.11. Параметри за калибрирането

5.8. Системно поддържане и ремонт
5.8.1. Изисквания за рекалибриране
5.8.2. Ремонт на сензорна линия
5.8.3. Интегриране с Главната командно - контролна система

5.9. Алармена система срещу проникване за периметърна охрана - комбинирана инфрачервена и микровълнова система (КИМС)
5.9.1. Комбинирана инфрачервена и микровълнова система - технически изисквания
5.9.2. Технически изисквания към микровълновите сензори
5.9.3. Технически изисквания към инфрачервените сензори

5.10. Алармена система срещу проникване за периметърна охрана - детектиращи решетки
5.10.1. Технически изисквания към детектиращите решетки
5.10.2. Време на отказите и време за ремонт

5.11. Алармена система срещу проникване за периметърна охрана - свръхмощни охранителни магнитни сензори за външните портали
5.11.1. Общо описание
5.11.2. Технически изисквания към магнитните сензори

5.12. Алармена система срещу проникване за периметърна охрана - Интегриране с Главната командно - контролна система

6. Система за разпознаване на регистрационните номера (СРРН)

6.1. Основни положения
6.1.1. Технически изисквания към камерата

7. Система за наблюдение под шаситата на моторни превозни средства (СНПШ - МПС)

7.1. Основни положения
7.2. Технически изисквания

8. Система за наблюдение под влаково композиции (СНПВК)
8.1. Основни положения

8.2. Основни положения
8.3. Технически изисквания

9. Затворена система за телевизионно видеонаблюдение (CCTV)
9.1. Основни положения
9.2. Компоненти
9.3. Техническа спецификаация на камерите
9.3.1. Фиксирани IP камери за външно използване
9.3.2. PTZ камери за външно използване
9.3.3. IP PTZ скоростна куполна камера
9.3.4. Фиксирана куполна камера за вътрешно използване
9.3.5. Кожух за камера
9.3.6. Обектив
9.4. Видеоенкодери
9.4.1. Видеоенкодер - едноканален
9.4.2. Видеоенкодер - дванадесетканален
9.4.3. Видеоенкодер - четиридесетканален
9.5. Система за управление, наблюдение и записване на IP базирано видеонаблюдение (СУНЗ)
9.5.1. Основни положения
9.5.2. Описание на системата за управление, наблюдение и записване на IP базирано видеонаблюдение
9.5.3. Мрежова преносна система
9.5.4. Система от мрежови видеорекодери
9.5.5. Декомпресиране и възпроизвеждане на клипове от архива
9.6. Използване на видеоматрицата и PTZ контрол
9.6.1. Инструкции за „плаващ“ вход на записващо устройство
9.7. Възможности на софтуера на системата за видеонаблюдение да управлява останалите ситеми за безопасност и охрана
9.8. Разширяване на системата
9.9. Архивиране (Bask - up)
9.10. Хардуер на системата от мрежови видеорекодери

Системни изисквания

9.11. Разпределена верижна архитектура на системата от мрежови сървъри

10. Видеосистема за откриване на движение / “интелегентен” видеоанализ (ВОД / ИВА)

10.1. Основни положения

10.2. Основни характеристики
10.2.1. Типове “интелегентен” видеоанализ
10.2.2. Филтри на “интелегентен” видеоанализ
10.2.3. Метод на действие на “интелегентния” видеоанализ

11. Електрооптични сензори / термични камери (ЕОС / ТК)

11.1. Основни положения
11.2. Технически изисквания
11.2.1. Термичен сензор
11.2.2. CCD - сензор
11.2.3. Механични

12. Инфрачервени осветители и осветители с бяла светлина

12.1. Инфрачервени осветители - технически изисквания

12.2. Осветители с бяла светлина - технически изисквания

13. Алармена система срещу проникване (АССП)

13.1. Основни положения

13.2. Компоненти

13.3. Технически изисквания
13.3.1. Основни положения
13.3.2. Алармен контролер
13.3.3. Алармен контролер - I / O устройства
13.3.4. Алармен контролер - комуникационни възможности
13.3.5. Алармен контролер - технически характеристики
13.3.6. Детектори с двойна технология - комбинирани детектори (PIR + MW) за използване в промишлени обекти
13.3.7. Магнитни контакти

13.3.8. Активен инфрачервен детектор
13.3.9. Електрическо захранване - технически изисквания
13.3.10. Пасивен инфрачервен детектор
13.3.11. Детектори с двойна технология - комбинирани детектори (PIR + MW) за монтиране на таван и използване в промишлени обекти
13.3.12. Акустичен детектор, регистриращ счупване на стъкло

14. Система за пожарна безопасност (СБП)

14.1. Пожароизвестителна инсталация (ПИИ)
14.1.1. Адресируема управляваща централа
14.1.2. Адресируем димен пожароизвестител
14.1.3. Адресируем топлинен пожароизвестител
14.1.4. Изолатор
14.1.5. Сирена
14.1.6. Монтажна основа
14.1.7. Ръчен пожароизвестител
14.1.8. Сензорен кабел
14.1.9. Специализиран адресируем топлинен пожароизвестител
14.1.10. Лъчев пожароизвестител

14.2. Пожарогасителна инсталация (ПГИ)

14.3. Централизирана система за мониторинг

15. Автоматична система за публично оповестяване (АСПО) и интерком - система

15.1. Основни положения

15.2. Основни изисквания и функции

15.3. Технически изисквания към аудиосървъра

15.4. Технически изисквания към усилвателя

15.5. Технически изисквания към IP високоговорителя за тавана

15.6. Технически изисквания към високоговорителя на сирената

15.7. Технически изисквания към аналоговия високоговорител за тавана

15.8. Технически изисквания към аналоговия високоговорител на сирената за стена

15.9. IP сигурност / подстанция за авариен интерком

15.10. IP главна работна станция

15.11. IP устройство за автоматичен тест и контрол на озвучителните тела

16. Комуникационна инфраструктура / мрежа

16.1. Основни положения

16.2. Технически изисквания към превключвателя
16.2.1. Превключватели от “трети” слой
16.2.2. Превключватели от “втори” слой

17. Главна командно - контролна система (ГККС)

17.1. Основни положения
17.1.1. Преглед
17.1.2. Архитектура на системата
17.1.3. Допълнителни функции
17.1.4. Конфигуриране на сървъра

17.2. Основни системни функции
17.2.1. Главна командно - контролна система - таблица на взаимните връзки
17.2.2. Графичен потребителски интерфейс (GUI)
17.2.3 Дисплеи
17.2.4. Географска информационна система - интерактивна карта
17.2.5. Възможности за видеоуправление
17.2.6. Администриране и доклади

17.3. Мултимедия
17.3.1. Основни положения
17.3.2. Матрица и мултимедиен контролер с „тъч скрийн“
17.3.3. Мултимедиен контролер
17.3.4. „Тъч скрийн“
17.3.5. Видеоматрица с 12 (дванадесет) входа и 8 (осем) изхода

17.4. Контролер за клавиатура, мишка и монитор

17.5. Превключвател за клавиатура, мишка и монитор

17.6. Сплитер за монитори

17.7. Хардуер на системата

17.8. Ракове с оборудване

18. Изисквания към инфраструктурата и специализираните строително - монтажни дейности

18.1. Основни положения

18.2. Нов Главен командно - контролен център
18.2.1. Основни положения
18.2.2. Изисквания

18.3. Концепция / типов дизайн - електрическо захранване
18.3.1. Основни положения
18.3.2. Електрическо захранване
18.3.3. Захранващи кабели

18.4. Заземяване

18.5. Мълниезащита

18.6. Непрекъснато електрическо захранване (UPS)

18.7. Стълбове за камери

18.8. Подсилване на прозорците

18.9. Благоустройство на обекта и разни строителни работи
18.9.1. Отстраняване на растителност и изравняване на земната повърхност
18.9.2. Пътно - строителни дейности
18.9.3. Разни инфраструктурни дейности

19. Изисквания за осигуряване на безопасни условия за работа

20. Изисквания към строително - монтажните работи

21. Съдържание на инженеринга

1. Увод

1.1. Основни положения

В резултат от извършения анализ и оценка на риска са определени заплахите и щетите от неоторизиран достъп, терористична дейност или саботаж, а също така и последиците от евентуални атаки; формулирани са препоръки за подобряване на системата от организационни, физически и технически мерки за физическа и информационна защита на „ТЕЦ Марица Изток 2“ ЕАД като стратегически обект със значение за националната сигурност.

Новото комплексно решение за сигурността трябва да осигури възпирането, откриването и предотвратяването на атаки, извършвани от терористични и престъпни организации, както и да предотвратява незаконни дейности, като кражби на материали, продукти и саботаж, извършвани от криминални елементи.

Системата за сигурност на „ТЕЦ Марица Изток 2“ ЕАД следва да гарантира цялостно решение за справяне със заплахите и уязвимостите, като бъдат отстранени всички съществуващи пропуски.

1.2. Основни характеристики

При проектирането и изграждането на техническите системи за сигурност е необходимо да се предвидят следните основни характеристики:

- **модулност** (дава възможност изграждането на системите за сигурност да се извърши на етапи, съобразно предвидените ежегодни бюджети);
- **гъвкавост** (позволява разширяване, усъвършенстване и надграждане на съществуващите системи за сигурност в съответствие с промените на бизнес - средата и съответните заплахи);
- **самостоятелност** (може да се изграждат паралелно със съществуващите системи за сигурност);
- **непрекъснатост** (прекъсването на технологичния процес ще се сведе до минимум).

1.3. Принципи на решението за сигурността

Решението за сигурността трябва да се основава на цялостни, комплексни интегрирани системи, като се вземат предвид следните принципи:

- **Откриване**

Необходимо е системата да включва подходящи съвременни сензори и видеоаналитични модули, които покриват целия периметър на електроцентралата, заедно с критичните (стратегически) външни и вътрешни зони. Тези сензори трябва да позволяват откриването в реално време на всички проникванията или нежелани дейности и събития вътре и извън защитените зони.

- **Проверяване**

Нужно е системата да позволява бързо и точно проверяване на подозрителни обекти и събития, „забелязани“ от сензорите за сигурност и видеокамерите.

- **Идентифициране**

Потребно е системата да предоставя възможности за идентифициране на всички служители, доставчици, посетители, превозни средства, материали и продукти и да контролира движението през входно / изходните портали с помощта на специални мерки за достъп.

- **Наблюдение**

Необходимо е системата да позволява непрекъснатото наблюдаване на всички събития и дейности във външните и вътрешните рискови зони чрез съответната специализирана система за видеонаблюдение.

- **Тактическа информация**

Главната командно - контролна система трябва да дава пълна „тактическа картина“, като включва цялата информация, получена от всички сензори и системи за сигурност на обекта. Обобщените тактически данни следва да осигуряват в реално време ясно и лесно идентифициране и оценяване на състоянието на обекта по отношение на местоположението на „приятелските сили“ и „потенциалните мишени“. Също така, тази информация трябва да позволява на операторите да предприемат действия в съответствие с предварително разработените планове и оперативни процедури.

- **Търсене и разследване**

Потребно е системата да включва усъвършенствана подсистема за цифров запис, която да позволява по всяко време и без намеса в дейността на работещите в реално време отделни системи за сигурност, разследване на различни предишни събития за целите на изследването, обучението и извличането на поуки.

2. Мерки за сигурност

2.1. Равнища на сигурност и защита

Решението за сигурността трябва да осигурява 2 (две) основни равнища на защита:

- **първото равнище** представлява защита на външния периметър на централата от нежелано или незаконно проникване;
- **второто равнище** включва защитата на специфичните критични (стратегически) зони вътре в централата.

2.2. Етапи на изпълнение

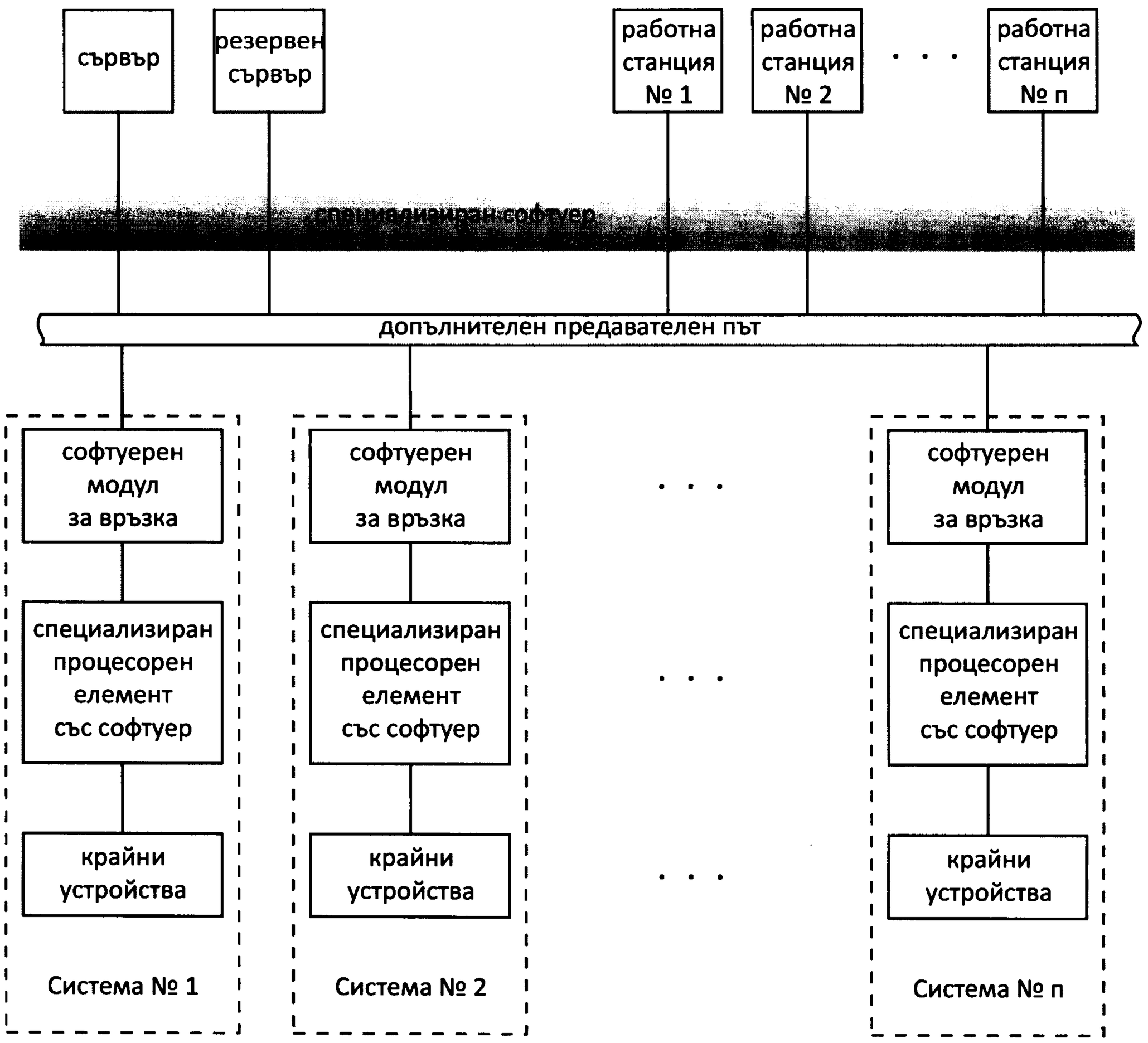
Необходимо е решението за сигурността да се изпълнява поетапно, като съдържанието (обема от видовете работи) на всеки етап се определя в Плана за изпълнение.

Настоящият Документ определя Техническите изисквания на цялостната система за сигурност (в съответствие с препоръчаните мерки за сигурност и независимо от етапа за изпълнение).

3. Съдържание на мерките за сигурност

3.1. Концептуална блок - схема

Концептуалната блок - схема на Главната командно - контролна система за сигурност на „ТЕЦ Марица Изток 2“ ЕАД следва да се разработи на основата на Европейския стандарт за комбинирани и интегрирани алармени системи за сигурност CLC_TS_50398 (съответства на българския стандарт СД_CLC_TS_50398). Тя трябва да има следния вид:



3.2. Интегрирани системи за сигурност

Потребно е мерките за сигурност да включват интегрирани физически и технически системи и елементи, както следва:

- Система за контрол на достъпа (СКД);
- Алармена система срещу проникване за периметърна охрана (АССППО);
- Система за разпознаване на регистрационни номера (СРРН);
- Система за наблюдение под шаситата на моторни превозни средства (СНПШ - МПС);
- Система за наблюдение под влакови композиции (СНПВК);
- Затворена система за телевизионно видеонаблюдение (CCTV);
- Система за видеоанализ (Видеосистема за откриване на движение (ВОД));
- Термични камери (ТК);
- Охранително осветление (инфрачервени и бели прожектори);
- Алармена система срещу проникване (АССП);
- Системи за пожарна безопасност - пожароизвестителни и пожарогасителни системи (СПБ);
- Автоматична система за оповестяване (АСО);
- Комуникационна / мрежова инфраструктура;
- Главна командно - контролна система (ГККС);
- Изисквания към инфраструктурата и строително-монтажните дейности.

4. Система за контрол на достъпа (СКД)

Предназначението на Системата за контрол на достъпа е да контролира лицата и превозните средства, които влизат на територията на „ТЕЦ Марица Изток 2“ ЕАД, както и придвижването им между отделните зони за сигурност в централата.

4.1. Основни положения

Територията на „ТЕЦ Марица Изток 2“ ЕАД е разделена на няколко класифицирани стратегически зони с различни равнища на сигурност, определени от съответната критичност, значение за производствения процес, равнище на въздействие и необходимо време за възстановяване.

Всички лица, в това число постоянен и временен персонал, служители, изпълнители, подизпълнители, посетители и доставчици, които влизат в централата трябва да носят в баджове и на видно място лични идентификационни карти, съответстващи на определеното равнище на сигурност. Картите за сигурност трябва да съдържат подробна информация и снимки за идентифициране на самоличността на лицето, което я притежава.

Придвижването на лицата от една зона в друга следва да се извършва само с тези карти. Класифицираните зони и определените критични обекти, трябва да бъдат защитени със специални и подходящи за тях мерки за сигурност.

4.2. Компоненти

Системата за контрол на достъпа трябва да включва следните компоненти:

- четци на карти, създадени на основата на безконтактна (proximity) и биометрична технология;
- централни и локални контролери;
- електрически и магнитни ключалки;
- плъзгащи се врати;
- управляеми въртящи се врати „цял ръст” и триножници „турникети“;
- антитерористични бариери - боларди (АТБ);
- бариери с вертикално рамо (БВР);
- антитерористични бариери с вертикално рамо (АБВР);
- елементи за забавяне на скоростта на движение и за безопасност на движението на МПС;
- метални детектори;
- рентгенов скенер за идентифициране и скрининг на багажи;
- детектори, които следят положението на вратите;

- бутони за отваряне на вратите;
- централна софтуерна система, която включва софтуерни модули за включване и интегриране към Главната командно - контролна система за сигурност.

4.3. Технически изисквания

4.3.1. Безконтактна (proximity) карта

Системата за контрол на достъпа трябва да осигурява възможност за достъп на потребителите до различните обекти на централата, ползвайки 1 (една) безконтактна идентификационна карта.

Картата трябва да:

- се изработи от PVC материал;
- съответства на изискванията на ISO 7810;
- разполага с антена за електрическо зареждане с обхват до 60 [cm];
- е пасивна и да не използва батерия;
- се проектира за продължителна употреба;
- осигурява възможност за сигурно прочитане - дори при засенчване с тяло или при наличие на метални предмети (ключове, монети и други) в съседство с картата;
- разполага с възможности за изобразяване на графики, директно отпечатване на изображение, магнитни ленти и бар кодове.

4.3.2. Картови четци

Картовите четци трябва да се инсталират на определените за специален достъп места - бариери, врати и други (въртящи се врати „цял ръст“, триножници, стълбове за четци).

Картовите четци трябва да:

- съответстват на стандарта CE;
- имат обхват на прочитане: не по - малко от 10 [cm];
- имат светодиоден индикатор;
- осъществяват специализирана комуникация с контролера;
- имат възможност за „външно“ и „вътрешно“ инсталиране;
- работят при температура: от -20 [^{0}C] до +60 [^{0}C];
- имат защита от фактори на околната среда: IP55;
- работят при относителна влажност: до 95 [% RH].

4.3.3. Геометрия на ръка или пръстов отпечатък

Модулите на системата за биометрична идентификация трябва да може да се свързват помежду си за трансфер на данни с кабел тип „усукана двойка“ (за RS - 485).

Биометричните четци трябва да:

- съответстват на стандарта CE;
- четат със скорост: не повече от 2 [sec];
- имат време за проверяване на биометричните данни: не повече от 2 [sec];
- имат времеви интервал между две последователни прочитания: не повече от 2 [sec];
- имат вътрешна памет: не по - малко от 1000 потребители;
- имат размери на четящия сензор: не по - малко от 20 x 14 [mm];
- имат разрешаваща способност на сканиране: не по - малко от 500 [dpi];
- имат светодиоден индикатор;
- осъществяват специализирана комуникация с контролера;
- имат възможност за „външно“ и „вътрешно“ инсталиране;
- работят при температура: от -10 [^{0}C] до +50 [^{0}C];
- имат защита от фактори на околната среда: IP65;
- работят при относителна влажност: до 95 [% RH];
- имат възможност за присвояване на повече от един вид биометрични данни за един потребител.

4.3.4. Контролери за контрол на достъпа

Контролерите от системата за контрол на достъпа трябва да следят състоянието („отворено“ или „затворено“) на наблюдаваните контролни точки (врати, турникети и други). Също така е необходимо те да управляват алармените сигнали и в онлайн режим да обменят информация със сървъра на СКД. Контролерите трябва да се инсталират на закрито или в случаите, когато е небходимо инсталиране на открито, те следва да се поставят в шкафове за оборудване, предназначени за външно монтиране. В случай на прекратяване на връзката с контролния център, всеки контролер трябва да продължи да управлява своите свързани точки за достъп, като използва своята вътрешна памет и резервно захранване.

Контролерите трябва да:

- имат 4 (четири) четеца за 2 (две) врати („вход“ и „изход“) или 4 (четири) четеца за 4 (четири) врати („вход“);
- може да управляват светлинната и звуковата сигнализация на използваните четци;
- имат не по-малко от 8 (осем) информационни входа и 2 (два) технически

входа за прекъсване на захранването и откриване на саботаж;

- имат не по - малко от 4 (четири) изхода;
- обслужват не по-малко от 100000 картодържатели, с динамично разпределение на RAM;
- съхраняват в паметта не по-малко от 250000 събития, с динамично разпределение на RAM;
- имат 2 [MB] флаш - памет за фърмуера (свален от PC);
- имат 4 [MB] RAM памет за база данни и буфер за събития;
- имат вграден TCP порт;
- имат 3 (три) серийни порта (два RS232 / RS485 и един RS485);
- обработват протоколи, поддържани от TCP / IP, ARP, UDP, TCP, Telnet, ICMP, SNMP, DHCP, BOOTP, IP, HTTP, TFTP, HTTPS, SSH, SSI, FTP, PPP;
- поддържат скорост на обмен на данни: от 4 800 [baud] до 115 200 [baud];
- имат сменяеми конектори;
- поддържат не по-малко от 250 дневни програми;
- имат възможности за поддържане на не по-малко от 120 седмични програми;
- позволяват автономни решения на локално равнище, без да се влошава работа на системата;
- включват мултитехнология за работа с: биометрични, смарт, “proximity”, магнитни и други карти;
- имат AntiPassBack без необходимост от компютър;
- работят при температура: от 0 [^{0}C] до +50 [^{0}C];
- работят при относителна влажност: до 95 [% RH];
- съответстветстват на стандарта CE.

4.3.5. Електрически и магнитни ключалки

Електрическите и магнитните ключалки трябва да отговарят на следните технически изисквания:

- конструкция - изцяло от неръждаема стомана, устойчива на корозия, непропусклива и високоиздръжлива конструкция;
- метод на заключване - чрез електромагнит;
- инсталиране - за „вътрешно“ и „външно“ използване;
- сигурност (Fail Safe);
- продължителност на експлоатация - неограничени брой задействания, без електрическа умора или механично разбиване;
- задържаща сила: не по - малко от 250 [kg];
- магнитен контакт - интегриран в ключалката;
- работно напрежение: 12 [V] DC, 24 [V] DC;

- работна температура: от -20 [^{0}C] до + 40 [^{0}C];
- защита от фактори на околната среда: IP65;
- относителна влажност: до 95 [% RH].

4.3.6. Плъзгаща се врата

Плъзгащите се врати трябва да са в съответствие със следните технически изисквания:

- задвижване - електромотор със зъбни предавки или пневматично / хидравлично;
- дистанционно и кабелно управление;
- пълно интегриране със системата за контрол на достъпа;
- тип - конзола без релси или колела;
- дължина на крилото - спрямо съответния обект;
- материал за изработване на вратата - галванизирана стомана с PVC покритие;
- скорост на придвижване: не по - малко от 1 [m / sec];
- устойчивост на удар: 6,8 [t] / 65 [km / h];
- операции (отваряне / затваряне): над 200 броя за 1 [h];
- работна температура: от -20 [^{0}C] до +60 [^{0}C];
- относителна влажност: до 95 [% RH].

4.3.7. Турникет (пълен размер)

Въртящите се врати пълен размер (или „цял ръст") трябва да са в съответствие със следните технически изисквания:

- въртяща се врата - от висок клас;
- възможност за „външно" и „вътрешно" инсталиране;
- две посоки на въртене;
- оперативен контрол - картов четец, електрически бутон;
- препоръчителна височина - 2300 [mm];
- материал - полирана стомана;
- брой рамена - 3 x 120^0;
- безопасен режим на работа - свободно въртене за безопасно преминаване на потребителите, в случай на повреда в захранването;
- работна температура: от -20 [^{0}C] до +60 [^{0}C];
- относителна влажност: до 95 [% RH].

4.3.8. Турникет (триножник)

Охранителните триножници от висок клас, турникетен тип трябва да са в

съответствие със следните технически изисквания:

- възможност за „външно“ и „вътрешно“ инсталиране;
- две посоки на въртене;
- оперативен контрол - картов четец, електрически бутон;
- материал за изработване - полирана стомана;
- брой рамена: три броя, разположени на 120^0 пространствени градуса;
- безопасен режим на работа - спускане на рамената и осигуряване на свободно преминаване в случай на повреда в захранването;
- работна температура: от -20 [^{0}C] до +60 [^{0}C];
- относителна влажност: до 95 [% RH].

4.3.9. Антитерористични бариери (АТБ)

Антитерористичните бариери „боларди” трябва да са в съответствие със следните технически изисквания:

- съответствие със стандарт K - 8;
- височина - минимум 700 [mm];
- диаметър - минимум 250 [mm];
- материал - безшевна стомана ST42 / 52;
- скорост на излизане: не повече от 5 [sec];
- устойчивост на удар: 6,8 [t] / 65 [km / h];
- задвижване - пневматично / хидравлично;
- работна температура: от -15 [^{0}C] до +50 [^{0}C];
- възможност за увеличаване на работния температурен диапазон, чрез използването на нагревател;
- защита от фактори на околната среда: IP65.

4.3.10. Бариери с вертикално рамо (БВР)

Бариерите с вертикално рамо трябва да са в съответствие със следните технически изисквания:

- задвижване - пневматично / хидравлично;
- дистанционно и кабелно управление;
- дължина - спрямо съответния обект;
- материал за изработване на рамото - алуминий;
- скорост на издигане / спускане: не повече от 6 [sec];
- операции: над 200 броя за 1 [h];
- работна температура: от -20 [^{0}C] до +60 [^{0}C];
- относителна влажност: до 95 [% RH].

4.3.11. Свръхмощни бариери с вертикално рамо (СБВР)

Свръхмощните бариери с вертикално рамо трябва да са в съответствие със следните технически изисквания:

- задвижване - пневматично / хидравлично;
- дистанционно и кабелно управление;
- дължина - спрямо съответния обект;
- материал за изработване на рамото - алуминиево двойно рамо;
- допълнителен специализиран стоманен кабел;
- скорост на издигане / спускане: не повече от 8 [sec];
- операции: над 200 броя за 1 [h];
- устойчивост на удар: 6,8 [t] / 65 [km / h];
- работна температура: от -20 [^{0}C] до +60 [^{0}C];
- относителна влажност: до 95 [% RH].

4.3.12. Помощни елементи за трафика и безопасността

Допълнителни помощни елементи за подобряване безопасността на трафика са светофарните уредби, които трябва:

- да се инсталират на порталите;
- да са свързвани към контролерите на бариерите;
- да работят автоматично.

4.3.13. Металдетекторна рамка (тип „врата”)

Металдетекторната рамка трябва да отговаря на следните технически изисквания:

- способност за детектиране на метални оръжия от магнитни, немагнитни и смесени сплави;
- транзитен поток: кратко време за нулиране и бърза скорост на преминаващия поток;
- скорост на детектиране: до 15 [m / s];
- програмиране: вградени клавиатура и дисплей, дистанционно управление и работа в компютърна мрежа;
- защита от достъп до програмиране с парола, механична ключалка или с друг способ;
- визуални сигнали - многозонов дисплей, локализиран на височината на човешкия ръст;
- светлинна сигнализация за масата на откритията обект;
- интензивни звукови алармени сигнали;
- програмируеми сила и тон на алармите;

- мултиинсталации: автоматично синхронизиране между два и повече метални детектора с минимално разстояние между тях от 5 [cm];
- работна температура: от -15 [^{0}C] до +60 [^{0}C];
- относителна влажност: до 95 [% RH];
- съответствие с правилата и нормите на ЕС и международните стандарти, свързани с електрическата безопасност и електромагнитното съответствие.

4.3.14. Рентгенов скенер за идентифициране и проверяване на багажа

Рентгеновият скенер за идентифициране и проверяване на багажа трябва да отговаря на следните технически изисквания:

- проникване през стомана с дебелина не по-малко от 25 [mm];
- откриване на жици с диаметър по - голям от 0,1 [mm];
- безопасност и вредни емисии:
  - не трябва да повреждa магнитни ленти, компютърни харддискове, CD, DVD, видеокасети, лични идентификационни карти и кредитни карти;
  - максимално изтичане на радиация: до 0,1 [mR / h];
  - радиация - трябва да отговаря на всички публикувани международни регламенти;
- размери на светлия отвор на тунела: минимум 550 [mm] x 350 [mm];
- максимален товар за обработване: не по - малко от 150 [kg];
- скорост на движение на конвейера: не по-малко от 0,20 [m / sec];
- мрежови връзки - да позволяват много рентгенови устройства да се свързват към отдалечена зона за допълнителен преглед;
- здраве и безопасност - в съответствие с приложимите международни регулации за здраве и безопасност;
- захранващо напрежение: 230 [V AC], 50 [Hz];
- работна температура: от 0 [^{0}C] до +40 [^{0}C];
- относителна влажност: до 95 [% RH].

4.3.15. Превключватели на позициите на вратите

- конструкция, позволяваща монтиране върху стомана;
- защита от саботаж;
- защита - екран, който предпазва от магнитен поток;
- контакти - дизайн с висока надеждност;
- работна температура: от -20 [^{0}C] до +60 [^{0}C];
- относителна влажност: до 95 [% RH].

4.3.16. Бутони за отваряне на вратите

Бутоните за отваряне на вратите трябва да:

- са лесни за употреба - да се активират само с лек натиск;
- може да се монтират навсякъде (за удобство при работа с тях);
- разполагат с голям светлинен червен бутон за лесно визуално разпознаване, дори в аварийни условия;
- работят с всички системи за контрол на достъпа;
- са разработени за високи натоварвания, специално предназначени за зони с натоварен трафик;
- може да се конфигурират - първоначално „отворени“ или „затворени“;
- имат захранващо напрежение: 12 [V DC] / 24 [V DC];
- имат работна температура: от -5 [^{0}C] до +40 [^{0}C].

4.4. Система за управление на контрола на достъпа (СУКД)

4.4.1. Основни характеристики

Системата за управление на контрола на достъпа трябва да отговаря на следните изисквания:

- софтуерът за контрол на достъп трябва да може да функционира в 2 (два) операторски режима:
  - мониторингов режим;
  - команден режим;
- когато е в мониторингов режим, системата трябва да изпълнява следните основни операции, при представяне на идентификационна карта пред четеца на карти:
  - проверяване на кода на картата;
  - проверяване на равнището на достъп за съответната времева зона;
  - проверяване с цел предотвратяване на повторно влизане с една и съща карта, без предхождащо го излизане от охраняваната зона („Anti pass -back“);
  - показване и разпечатване на информация, включително персонален код, име на картопритежателя, време, идентификационен номер на четеца на карти, валидно или невалидно прочитане;
  - при разрешаване на достъп трябва да се задейства електрическото заключващо устройство за предварително зададено време;
  - при отказ на достъп трябва да се генерира системно съобщение, което да се отпечатва или показва;
- командният режим трябва да предоставя следните функции за управление:
  - добавяне на персонални идентификационни карти в паметта с възможност

да се определи къде и кога картопритежателят може да използва картата. Въз основа на принципа „от врата до врата“, трябва да е възможно дефинирането на валидни времена и дни на достъп;

- групово зареждане на персонални карти с еднакви права, при използване на който и да е картов четец;
- изтриване на персонални карти от паметта;
- промяна на правата за достъпа на избрани картопритежатели;
- избиране на персонални карти за проследяване;
- дефиниране на вратата(ите), през които излизането ще се осъществява чрез бутон, вместо чрез картов четец;
- дефиниране на зони, в които повторното влизане е забранено без предхождащо го излизане („Anti pass - back“);
- ръчно отключване на врати от главния работен терминал;
- определяне на минимум от 100 (сто) кода за достъп;
- определяне на минимум 20 (двадесет) празнични дни;
- автоматично отключване и заключване на избрани врати;
- избиране на картови четци, които ще генерират предупредително съобщение, когато се използват съответни персонални карти, избрани за проследяване;
- получаване на хартиен носител на доклади за моментния статус на системата;
- избор на съобщенията за достъп и на съобщенията от наблюдаваните входовете, които трябва да се отпечатват от системния принтер;
- определяне на това дали да се изпращат съобщения за валиден достъп от избрани врати, в определени часове и дни от седмицата;
- приемане и потвърждение на алармените събития;
- избиране на точки от системата, които трябва да се наблюдават по всяко време и такива, които трябва да се наблюдават само през избрани периоди от време;
- избиране на зони, контролирани от картови четци, които да се наблюдават за „принудително отваряне“ на вратите и за „задържане на отворена врата“ и определяне дали тези аларми се генерират по всяко време или само, когато системата е в „нощен“ режим;

- системата трябва да е защитена с парола;
- всеки оператор трябва да има собствена парола, за да получи достъп до командния режим на системата;
- всички команди на операторите трябва да се управляват от меню;
- трябва да има възможност за системни разпечатки;
- по желание на оператора, работещата система, трябва да има възможност да разпечатва всички съобщения за събития или само тези за действията на операторите. Разпечатките трябва да съдържат следното:

- списъци (на хартиен носител) с персонални карти във всички възможни комбинации на равнище на достъп, времеви код, местоположение („вън“ или „вътре“) и статус на проследяване;
- списъци (на хартиен носител) със зададените определения за всяка врата и / или наблюдавана точка;
- списъци (на хартиен носител) за всеки тип доклад;
- операторът трябва да има възможност да избира типа на съобщенията, които трябва да се разпечатат;
- системата трябва да позволява генериране на съобщения най-малко за:
- валиден достъп;
- невалиден достъп;
- действия в наблюдавани точки;
- действия на операторите;
- обновявания на базата данни;
- всички системни съобщения трябва да са в еднакъв или подобен формат и да съдържат най-малко следната информация:
- избрани картови четци;
- дата и час на събитието;
- описание на събитието;
- буквено-цифорви данни, определящи местоположението, оператора и код за съответните команди за всяко събитие;
- определени от потребителя наименования, където е приложимо;
- времеви и присъствени характеристики:
- разпределението за почивните и празнични дни трябва да бъде на човек, по часове и дни;
- трябва да има 4 (четири) брояча за работа в извънработно време;
- трябва да има възможност за изчисляване на работата в извънработно време по отделни фактори;
- времето, добавено като извънработно, трябва да се включва в общ баланс за положения труд в извънработно време;
- трябва да има възможност за показване на отсъствията по часове и дни;
- трябва да е разрешено изготвянето на статистики;
- трябва да има възможност за ограничаване на извънработното време за определени дни;
- трябва да има възможност всеки работник да прочита определена избрана информация и да въвежда необходими данни през лесен за употреба терминал.
- трябва да има „онлайн“ и „офлайн“ работни режими;
- трябва да има възможност за автоматично и ръчно управление;
- гъвкавост - възможност за комбиниране в една инсталация на различни технологии за идентифициране;

- управление на контрола на достъпа и присъствието чрез едно приложение и единна потребителска база данни.
- възможност за централизиран контрол чрез TCP / IP мрежа от разпределени устройства (дори и на различни места) и контрол на устройствата от различни точки (много потребители);
- мощна, стабилна, сигурна и надеждна база данни чрез използване на SQL технология. Възможност за адаптиране към други системи за бази данни (Oracle, SQL Server, Access и други);
- минимално използване на компютърни ресурси и възможност за управление от всяка операционна система: Windows, Linux и Unix (MAC). Драйвер за сървър с операционна система Windows;
- системата трябва да работи на български език;
- възможност за многоезичен интерфейс (приспособим към всеки език);
- възможност за използване на различни филтри с цел генериране на конкретни доклади;
- ефективна и адаптирана към реалните нужди на обекта;
- интуитивен графичен потребителски интерфейс;
- брой потребители: не по - малко от 20000.
- капацитет на контролирани четци: не по-малко от 5000;
- контрол на времеви графици;
- възможност за въвеждане на подробни лични данни, включително и снимка;
- поддържане на функция за предотвратяване на повторно влизане, без излизане от охранявания обект („Anti pass - back“);
- възможност за генериране на доклади за историята на събитията в системата и създаване на log файл.

Забележка: **Всеки участник трябва да представи подробна функционална блок - схема, илюстрираща работата на системата за контрол на достъпа, връзките между отделните модули и видовете крайни устройства, които смята да използва.**

5. Алармена система срещу проникване за периметърна охрана (АССППО)

5.1. Основни положения

Алармената система срещу проникване за периметърна охрана трябва да се инсталира на физическите огради, за да открива нарушители при опити за проникване в защитените оградени зони.

Избраната система е необходимо да отговаря на настоящите Технически изисквания, общите изисквания на поръчката и условията на околната среда, характерни за охранявания обект.

5.2. Характеристики и компоненти

Алармената система срещу проникване за периметърна охрана е нужно да изпълнява 2 (две) основни функции:

- физическа функция - обозначава линията на периметъра на охранявания обект;
- техническа функция - технически средства, инсталирани по границата на охранявания периметър, които разрешават достъп на упълномощени лица и разкриват неупълномощени нарушители.

Алармената система срещу проникване включва изграждането на:

- физическа стоманена ограда и фундамент;
- електронна алармена система срещу проникване (ЕАССП), включваща следните подсистеми:
  - сензорни линии, базирани на вибрационни сензори;
  - инфрачервени и микровълнови детектори за периметърна охрана;
  - свръхмощни охранителни магнитни детектори за външните портали;
  - детектиращи решетки;
  - локални и централни контролери;
  - централна софтуерна система, включваща софтуерни модули за включване и интегриране към Главната командна и контролна система за сигурност.

5.3. Физическа стоманена ограда - основни изисквания

Точното трасе на външната ограда по периметъра на територията на централата следва да се определи на етап проектиране.

Съществуващата конструкция на оградата, включително кльона, трябва да се ремонтират, обновят или изградят отново, за да отговорят на новите изисквания за

сигурност на съоръжението. Секторите от оградата, които не подлежат на обновяване трябва да се подменят.

При проектирането на новата и реконструирането на съществуващата стоманобетонна и стоманена конструкция е необходимо да се вземат предвид:

- условията на околната среда;
- геотехническите резултати от почвените тестове;
- вятърното натоварване, което трябва да бъде в съответствие с българските и международните стандарти, но не по-малко от 100 [kg] хоризонтална сила и 300 [kg] теглителна сила за всяка част на цялата структура.

5.4. Физическа стоманена ограда - технически изисквания

Новата ограда трябва да включва 4 (четири) основни елемента (този тип ограда ще се използва за обезопасяване на външния периметър на централата), както следва:

5.4.1. Физическа стоманена ограда - бетонов фундамент / бетонни стъпки и вкопана стоманена мрежа

Фундаментът следва да отговаря на следните изисквания:

- подсилен бетон висок клас;
- минимални размери - височина 70 [cm]; дебелина 20 [cm]; „вкопана част“ (под кота „0“) - 50 [cm]; „надземна част“ (над кота „0“) 20 [cm];
- отворите и тръбите в бетоновата основа, използвани за дренаж и оттичане на водите през нея, трябва да са подсигурени с мрежа от галванизирана стомана или с плъзгащи се капаци от галванизирана стомана;
- дебелина на металните пръчки на мрежата трябва да е не по-малко Ø 12 [mm], а размера на отворите на мрежата, не по-голям от 100 [mm] x 100 [mm].
- СМР - новите стоманобетонови фундаменти е необходимо да се проектират и изпълнят от бетон клас В 30 и армировъчна стомана. При проектирането им е нужно да се спазват действащите строителни норми и правила към момента на изграждането. Фундирането да се осъществява в здрав почвен слой. При необходимост, да се предвиждат подложки от бетон , или уплътнени инертни материали. При ремонта на съществуващите стоманобетонови фундаменти е необходимо да се отстранят всички компрометирани участъци, след което да се анкерира допълнителна армировка и се възстанови цялостта на фундамента.
  Върху фундамента се монтират вертикални стоманени колони през не повече от 3 (три) метра разстояние.

5.4.2. Физическа стоманена ограда - мрежа от галванизирана заварена

стомана

Мрежата от галванизирана заварена стомана следва да отговаря на следните изисквания:

- максимален размер на отворите: 150 [mm] x 50 [mm];
- минимална дебелина на стоманената тел: не по-малко от Ø 4,5 [mm];
- минимална изисквана височина на мрежата - 2000 [mm] над бетоновия фундамент / бетоновите стъпки / надземното равнище;
- мрежата следва да бъде свързана (опъната) към подходящи вертикални стоманени стълбове, разположени един от друг на не повече от 3000 [mm];
- за допълнителна стабилност на всеки 24 [m], както и на завоите, трябва да се добавят укрепващи двойни диагонални стоманени стълбове;
- вертикалните стълбове трябва да бъдат закрепени неподвижно (изляти или фиксирани по друг начин в) бетоновия фундамент или бетоновите стъпки;
- структурата на оградата трябва да се проектира така, че да издържа на екстремни метеорологични условия.

5.4.3. Физическа стоманена ограда - „външен“ кльон

Кльонът от галванизирана заварена стомана следва да отговаря на следните изисквания:

- дължина на кльона - 800 [mm];
- максимален размер на отворите: 150 [mm] x 50 [mm];
- минимална дебелина на стоманената тел: не по-малко от Ø 4,5 [mm];
- кльонът трябва да се закрепи към наклонени стоманени греди с дължина от 600 [mm], които са част от вертикалните колони, носещи мрежата.
- наклонът на гредите, носещи кльона трябва да бъде 60^0 спрямо равнището на хоризонта;
- кльонът и вертикалната мрежа трябва да са здраво свързани помежду си с подходящи за целта клипсове.

5.4.4. Физическа стоманена ограда - режеща серпентина

Серпентината с остри режещи краища, следва да отговаря на следните изисквания:

- място на разполагане - в горната част на кльона;
- диаметър на серпентината - 1000 [mm];
- кльонът и серпентината трябва да са здраво свързани помежду си с подходящи за целта клипсове.

5.5. Нова ограда за критичните обекти (зони) във вътрешния периметър

Новата ограда за критичните обекти (зони) във вътрешния периметър трябва да включва 3 (три) основни сектора, както следва:

Бетоновият фундамент следва да отговаря на същите изисквания, както за външния периметър, съгласно точка 5.4.1.

5.5.1. Мрежа от поцинкована заварена стомана за критичните обекти (зони) във вътрешния периметър

Мрежата от поцинкована заварена стомана следва да отговаря на следните изисквания:

- максимален размер на отворите: 50 [mm] x 50 [mm];
- минимална дебелина на стоманената тел: не по-малко от Ø 3 [mm];
- минимална изисквана височина на мрежата - 2000 [mm] над бетоновия фундамент / бетоновите стъпки / над земното равнище;
- мрежата трябва да се свърже с обтягане към вертикални стоманени колони (или към съществуващата ограда), разположени един от друг на не повече от 3000 [mm];
- за допълнителна стабилност на всеки 24 [m], както и на завоите, трябва да се добавят укрепващи двойни диагонални стоманени стълбове;
- вертикалните стълбове трябва да са закрепени неподвижно (изляти или фиксирани по друг начин в) бетоновия фундамент или бетоновите стъпки;
- структурата на оградата трябва да се проектира така, че да издържа на екстремни метеорологични условия.

5.5.2. „Вътрешен“ кльон за критичните обекти (зони) във вътрешния периметър

Физическа стоманена ограда - кльон за критичните обекти (зони) във вътрешния периметър на централата, следва да се предвиди само на особено специални (опасни) места, които ще се уточнят по време на проектирането на системата.

- дължина - 800 [mm];
- наклон - 60^0 спрямо хоризонта;
- кльонът трябва да е част от / или заварен за вертикалните стоманени колони.

5.6. Алармена система срещу проникване за периметърна охрана - електронна алармена система срещу проникване (ЕАССП)

5.6.1. Основни характеристики

Електронната алармена система срещу проникване (ЕАССП) за периметърна защита, трябва да притежава следните основни характеристики:

- на оградата на целия външен периметър на „ТЕЦ Марица Изток 2“ ЕАД трябва да се инсталира електронна система с подходящи висококачествени технически средства, използващи технология за откриване на вибрации (нужно е системата да се свърже с монтираната стоманената мрежа и кльона на оградата);
- необходимо е да се инсталират сензорни вибрационни линии и на „работните“ и „аварийните“ портали (в затворено положение порталите следва да са част от периметърната система за сигурност);
- тези сензорни линии трябва да подават алармен сигнал, ако нарушител се опитва да проникне през оградата (чрез прерязване или изкачване на оградата, или на някой от порталите);
- на места или сектори от периметъра, където поради работни изисквания или изисквания за безопасност, не може да има физическа ограда, трябва да се използват многолъчеви инфрачервени и микровълнови детектори, монтирани в специални корпуси;
- конкретното подходящо техническо решение за всеки отделен сектор трябва да се определи в етапа на проектиране.

5.6.2. Компоненти

Електронната алармена система срещу проникване (ЕАССП) за периметърна защита, трябва да включва:

- сензорни линии, базирани на вибрационни сензори;
- инфрачервени и микровълнови детектори за периметърна охрана;
- свръхмощни охранителни магнитни детектори за инсталиране на открито;
- детектиращи решетки;
- локални и централни контролери;
- централна софтуерна система, включваща софтуерни модули за включване и интегриране към Главната командно - контролна система за сигурност.

5.6.3. Общи изисквания за изпълнение

5.6.3.1. Описание на системата

Върху оградата по периметъра на охранявания обект трябва да се инсталира електронна алармена система срещу проникване с голяма чувствителност, базирана на вибрационни сензори и микропроцерно управление. Заедно с физическата ограда тази система трябва да охранява периметъра на централата.

Системата трябва да е в състояние да наблюдава огради, изградени с различни видове мрежа - плетена, телена или заварена.

Използваните сензори трябва да откриват нарушители, които се опитват да срежат, деформират или повдигнат оградата, а също и при опит да се покатерят през нея.

Системата трябва да бъде високотехнологична, с голяма разделителна способност, позволяваща определяне на точното местоположение на всеки опит за проникване по протежение на оградата. Задължително условие за системата е тя да е в състояние да определи местоположението на даден опит за проникване с точност до 3 [m].

Системата трябва да е в състояние да функционира като самостоятелна система или като неразделна част от Главната командно - контролна система за сигурност.

5.6.3.2. Сигнален процесор

Сигналният процесор е необходимо да анализира сигналите от вибрационните детектори, които трябва да откриват незначителни вибрации по оградата. Процесорът трябва да използва адаптивни алгоритми, за да прави разлика между действителните и лъжливите аларми.

5.6.3.3. Вибрационни сензори

Вибрационните сензори трябва да са от механичен тип и да са чувствителни към движение / вибрации. Всеки от тях трябва да включва метални топки в херметически запечатана кутия. Всяка топка трябва да се поддържа от контактна система. Препоръчително е контактната система да има позлатени контакти. Когато метална топка се премести вследствие на вибрации по оградата, топката трябва да направи нов контакт и да прекъсне съществуващ контакт в контактната система, за да генерира сигнали, които да се анализират.

На оградата трябва да се закрепят много вибрационни сензори, на интервали не по-голями от 3 [m]. Трябва да има по един сензор на всеки панел от оградата, ако същата е изградена от панели. Вибрационните сензори трябва да са свързани с комуникационен кабел, който да е прикрепен към оградата с помощта на кабелни връзки, устойчиви на ултравиолетово лъчение. Сензорите трябва да генерират сигнали при опит да се среже, деформира или повдигне оградата, а също и при опит за покатерване през нея. Сигналите от сензорите трябва да се предават към сигнален процесор, който да ги анализира и да реши дали трябва да се генерира аларма или не.

5.6.3.3. Алгоритми за обработване на сигнали

Системата трябва да използва цифрови технологии за обработване на сигнали,

които да включват адаптивни алгоритми, способни да се адаптират към специфични видове ограда и условия на околната среда.

5.6.4. Свойства на детектиране

5.6.4.1. Чувствителност при детектиране

Системата трябва да открива нарушители, които се катерят, повдигат или режат оградата, като същевременно отхвърля други вибрации, които са резултат на промени в околната среда. Системата трябва да бъде в състояние да определи мястото, където оградата вибрира, с точност до 3 [ш]. Коефициентът на откриване трябва да бъде над 99 % (деветдесет и девет на сто).

5.6.4.1. Характеристики на филтриране

Сензорите за откриване трябва да работят като инерционен лентов филтър, който да отхвърля тези вибрации по оградата, които не отговарят на човешки проникванията.

5.6.5. Лъжливи аларми

5.6.5.1. Системно генерирани аларми (лъжливи аларми)

Максималният дял на лъжливите аларми, генерирани от вътрешни електронни процеси (кабелите са изключение) трябва да е по-малък от 1 % (едно на сто) на секция, на година (усреднено за общия брой секции в системата).

5.6.5.2. Аларми, предизвикани от околната среда (нежелани аларми)

Системата трябва да е предназначена за работа на открито и инсталирана в съответствие с препоръките на производителя, за да се сведе до минимум вероятността от аларми от следните фактори:

- валежи - включително дъжд, сняг, градушка и мъгла;
- изгрев / залез на слънцето;
- ветрове със скорост до 60 [km / h];
- резки температурни промени;
- движение на обекти близо оградата (превозни средства и други);
- движение на повърхностнтта или подпочвените води;
- наличие на растителност в близост до сензорите - с височина до 30 [cm];
- наличие на източници на радиочестотпи и електромагнитни смущения в близост до сензорите;
- сеизмични вибрации;
- допълнителни акустични или магнитни ефекти,

като същевременно се запази пълната работоспособност на системата за откриване за реални нарушители.

5.6.6. Характеристики на сензорите

Вибрационният сензор трябва да е поставен в херметически запечатана кутия, която да съответства на стандарта EN / IEC 60068 (US MIL STD 810C) за устойчивост на атмосферни влияния. Сензорите трябва да са свързани на равни интервали по протежението на кабела.

Една дължина на сензорния кабел или една сензорна линия, трябва да може да включва не по-малко от 33 (тридесет и три) броя вибрационни сензора, така че, ако е инсталирана към оградата и сензорите са на интервали от 3 [m], една сензорна линия ще бъде достатъчна за покриването на 100 [m] от оградата. Към всеки от сигналните процесори на системата трябва да може да се свързват не по-малко от 4 (четири) такива сензорни линии.

Вибрационните сензори трябва да са здраво монтирани от вътрешната страна на оградата със скоби, по един сензор на едно платно от оградата (т. е. между една двойка стълбове на оградата) и така, че един сензор да се намира на около 3 [ш] от следващия сензор. Сензорният кабел трябва да бъде прикрепен здраво към вътрешната страна на оградата с помощта на кабелни връзки, устойчиви на ултравиолетово лъчение.

5.7. Спецификации на сигналните процесори

5.7.1. Описание на сигнален процесор

Всеки сигнален процесор трябва да свързва до 4 (четири) сензорни линии и да е в състояние да наблюдава 4 (четири) секции по 100 [m] от оградата. Процесорът трябва да може да работи като самостоятелна единица със собствени алармени релета и като неразделна част от Главната командно - контролна система за сигурност. Процесорът трябва да включва вътрешни схеми за защита срещу мълнии и промени в напрежението.

5.7.2. Работа на сигналния процесор

Сигналните процесори, разположени по периметъра, трябва да получават и обработват сигналите от сензорната линия, като същевременно осигуряват безотказна работа на системата. Срив на един процесор не трябва да засяга обработването на сигнала от другите процесори по периметъра.

5.7.3. Обща дължина на оградата, защитена от системата

Общата дължината на оградата, защитавана от системата трябва може да се

променя (увеличава или намалява): от ограда, използваща един сигнален процесор, до ограда с неограничена дължина и много на брой процесори. Покритието на детектиране трябва да бъде непрекъснато и еднообразно и не трябва да има пролука между защитените секции на оградата.

5.7.4. Алармени изходи

Сигналният процесор трябва да може да работи самостоятелно, като генерира локални алармени сигнали чрез собствени релейни контакти.

Аларми, причинени от катерене, рязане, деформиране или повдигане на оградата, трябва да се идентифицират като аларми, предизвикани от опит за проникване.

Аларми, предизвикани от отварянето на външната кутия, спиране на тока, ниско напрежение, неизправност на кабел, или вътрешна електронна грешка, трябва да се идентифицират като повреди. Сигналите за повреда трябва да се различават и разграничават от алармите, предизвикани от опит за проникване.

Локалните алармени изходи трябва да са формирани от отделни релета с нормално затворени [NC] и / или нормално отворени [NO] контакти.

Локалните релейни алармените изходи трябва да осигуряват алармена резолюция с точност до една секция от 100 [m].

5.7.5. Мрежов транспондер и централен контролер

Всеки сигнален процесор трябва да може да се интегрира с Главната командно - контролна система за сигурност. Сигналният процесор трябва да функционира като мрежов транспондер, способен да изпраща алармени сигнали и диагностична информация към централния контролер.

Присъединяването към централен контролер трябва да осигурява алармена резолюция с точност до най-близкия сензор - 3 [m].

5.7.6. Работен диапазон в зависимост от околната среда

Системата трябва да може да функционира при следните условия на околната среда:

- работна температура: от -40 [^{0}C] до +70 [^{0}C];
- относителна влажност: от 20 [% RH] до 95 [% RH].

5.7.7. Изисквания към електрическото захранване

Процесорът трябва да работи с ниско напрежение: от 12 [V DC] до 30 [V DC].

5.7.8. Надеждност и ремонтопригодност

Сигналният процесор трябва да има средно време между отказите по-голямо от 20000 [h] и средно време за подмяна по-малко от 10 [min]. Вибрационният детектор трябва да има средно време между отказите по-голямо от 2000000 [h].

5.7.9. Критерии за инсталиране

При работа на открито, сигналният процесор трябва да се монтира в устойчив на атмосферни влияния корпус, с клас на защита IP 66. Корпусът трябва да включва капак с най-малко четири скрепителни елементи, тяло от неръждаема стомана и тампер - контакт за защита от саботаж. Корпусът трябва да се инсталира на оградата или на стълб, отделно от оградата, на която са монтирани сензорните кабели, от охраняваната страна на периметъра. Процесорът може да се инсталира и на закрито. За всеки процесор трябва да се осигури подходящо заземяване.

5.7.10. Калибриране на сензорите

Всички функции за калибриране трябва да може да се изпълняват от централния контролер.

Като алтернатива, всяка сензорна линия трябва да е в състояние да се калибрира от съответния сигнален процесор. Калибрирането на сензорите трябва да може да се извършва с помощта на преносим компютър, което ще позволява на техническите лица да настройват и да наблюдават реагирането на всеки отделен сензор.

5.7.11. Параметри за калибрирането

Техническите лица, които извършват обслужването на системата, трябва да може да настройват следните системни параметри:

- **дефиниране на условия за подаване на сигнал**: необходима продължителност на сигнала, за да може да се изпрати сигнал за настъпило събитие;
- **брой на събития**: брой на настъпилите събития, преди да се обяви аларма;
- **времеви прозорец**: време, през което трябва да се случат предварително дефинирания брой събития;
- **времеви прозорец за повреда**: времезакъснение до обявяването на повреда.

5.8. Системно поддръжане и ремонт

5.8.1. Изисквания за рекалибриране

След първоначалното калибриране, системата не трябва да има нужда от рекалибриране, с изключение на влошаване на състоянието на оградата

(разхлабени оградни елементи или проводници и други).

5.8.2. Ремонт на сензорна линия

Ако даден сензор е отрязан или повреден, той трябва да може да се ремонтира (с използване на допълнителен кабел, ако е необходимо, и с подходящ комплект за съединяване). Комплектът за съединяване трябва да изисква използването само на стандартни инструменти. Индивидуалните сензори трябва да може да се сменяват на място от техническо лице, което извършва сервизната обслужване.

5.8.3. Интегриране с Главната командно - контролна система за сигурност

Системата от вибрационни сензори трябва да се интегрира напълно в Главната командно - контролна система за сигурност на централата.

Всички сензори, контролери и други устройства трябва да се появяват на картата на графичния потребителски интерфейс. Главната командно - контролна система трябва да получава и да показва състоянието на сензорите и комуникационния статус, както и алармените сигнали. В случай на отказ на комуникацията, системата трябва да може да показва точното място на възникналия проблем, а визуална и звукова аларма от оградата трябва да показват точното местоположение на проникване с точност до 3 [m]. Системата трябва да позволява конфигуриране на контролерите и активиране / деактивиране на отделни сектори като порталите например.

5.9. Алармена система срещу проникване за периметърна охрана - комбинирана инфрачервена и микровълнова система (КИМС)

5.9.1. Комбинирана инфрачервена и микровълнова система - технически изисквания

На места или сектори от периметъра, където не може да се инсталира ограда, трябва да се предвидят многолъчеви, активни, инфрачервени и микровълнови сензори, които напълно да се интегрират с вибрационната система по останалата част на периметъра. Тези сензори трябва да отговарят на следните изисквания:

- интегриране на 2 (две) технологии в 1 (едно) решение;
- детекторите, които използват 2 (две) различни технологии трябва да са инсталирани в 1 (един) корпус;
- мониторинг на алармите - аларменият статус трябва да се съобщава чрез релейни изходи или интерфейс за връзка със сензорната мрежа. За да се намали окабеляването, предавателят трябва да изпраща информация за състоянието си на приемника през Tx - Rx комуникационна връзка чрез модулиране на микровълновия сигнал;

- възможности на сензорната мрежа - сензорът трябва да има възможност да изпраща съобщения за аларми, информация за състоянието си и конфигурацията си към 1 (една) централна контролна точка през мрежата, както и да се конфигурира от нея;
- конфигуриране и отстраняване на неизправности - конфигурирането и отстраняването на неизправности на сензора трябва да е възможно да се извършва директно на място, чрез USB - връзка към микровълновия сензор или през сензорната мрежа от 1 (една) централна точка.

5.9.2. Технически изисквания към микровълновите сензори

- диапазон на детектиране:
  - ходеща цел: от 5 [m] до 200 [m];
  - пълзяща цел: от 5 [m] до 150 [m];
  - специално обучени: от 5 [m] до 100 [m];
- диаграма - 13^0 хоризонтална и вертикална;
- процент на откриване - по-висок от 99 % (деветдесет и девет на сто);
- защита от мълнии - всички входове и изходи;
- околна среда:
  - работна температура: от -30 [^{0}C] до +60 [^{0}C];
  - относителна влажност: до 95 [% RH], без конденз;
- входове и изходи за:
  - захранване;
  - не по-малко от 2 (два) релейни изхода;
  - 1 (един) вход;
  - USB за конфигуриране.
- изисквания към захранването: от 12 [V DC] до 30 [V DC] за предавателя и приемника;
- релета:
  - релетата трябва да са програмируеми според конкретните изисквания;
  - функциите, които трябва да може да се програмират, трябва да включват аларма, антисаботажен контакт, срив във входното захранване.
- помощен вход за връзка по мрежата;
- спазване на регулаторните изисквания:
  - FCC - в съответствие с FCC част 15, подчаст C, раздел 15.245; 10 (десет) канала с избираеми полета в обхвата от 24.075 [GHz] до 24.175 [GHz]; изход - 24 [DAm];
  - CE - в съответствие с ETSI EN 300 440-1 v1.5.1, ETSI EN 301 489-3 и EN 50130-4, 10 (десет) канала с избираеми полета в хармонизирания обхват от 24.150 [GHz] до 24.250 [GHz]; изход - 20 [DBm].

5.9.3. Технически изисквания към инфрачервените сензори

- фотоелектричен лъчев сензор с 4 (четири) синхронизирани лъчи;
- двойно честотно модулиране;
- възможност за работа при лошо време (мъгла, сняг или силен дъжд и т. н.);
- защита срещу влияние на външна светлина с поносимост към слънчева светлина, живачна светлина и флуоресцентна светлина;
- за да се задейства алармената система трябва задължително да има прекъсване и на 4 (четирите) лъча, с цел елиминиране на най-честите причини за лъжливи аларми (дребни животни, птици и падащи листа);
- лесно настройване на на лъча;
- защита от попадане на насекоми в оптичната система;
- защита от електромагнитни и радиочестотни смущения;
- регулируем обхват при настройване на лъча;
- защита от саботаж - антисаботажен сух контакт.
- време за реагиране: < 60 [msec];
- алармен сигнал: релеен изход със сух контакт;
- антисаботажен сух контакт;
- захранващо напрежение: от 12 [V DC] до 30 [V DC];
- консумация: < 80 [mA] (при 12 [V DC]);
- работна температура: от -30 [^{0}C] до +60 [^{0}C];
- относителна влажност: до 95 [% RH].

5.10. Алармена система срещу проникване за периметърна охрана - детектиращи решетки

Детектиращите решетки трябва да се инсталират на водни пътища (канали), канализации и други места, където няма възможност да се постави ограда. Решетките трябва да блокират входните точки и физически да предотвратяват проникването на нарушители в обекта. Решетките трябва да съдържат вградена алармена система, която да се свърже с алармената система срещу проникване на оградата (периметъра) и да предупреждава при опит за проникване в обекта през решетката. Сигнал за аларма от решетките трябва да се подава в следните ситуации:

- в случай, че нарушител отвори решетката;
- в случай, че нарушител се опитва да увреди структурата на решетката.

Трябва да има възможност за подаване на различна алармата, при опит за рязане на решетката или когато има опит за отстраняване на решетката.
За предпочитане е всички стоманени профили да бъдат от поцинкована стомана тип SAE 1020.

5.10.1. Технически изисквания към детектиращите решетки

- раборна температура: от -30 [^{0}C] до +60 [^{0}C];
- относителна влажност: до 100 [% RH], без конденз;
- скорост на водата: до и включително 40 [km / h] без влошаване на експлоатационните качества.
- средното време за ремонт на една решетка: по-малко от 1 [h].

5.10.2. Време на отказите и време за ремонт

- средното време между отказите (MTBF) на сигналния процесор и системата от решетки трябва да бъде по-голямо от 80000 [h];
- средното време за ремонт (MTTR) трябва да бъде по-малко от 30 [min].

5.11. Алармена система срещу проникване за периметърна охрана - свръхмощни охранителни магнитни сензори за външните портали

5.11.1. Общо описание

На вратите и решетките трябва да се инсталират магнитни сензори за сигнализиране при отваряне и затваряне на вратите. Магнитните сензори трябва да са свързани към алармената система срещу проникване за периметърна защита и да предоставят контакт, който да показва състоянието на наблюдаваната врата (отворена / затворена).

5.11.2. Технически изисквания към магнитите сензори

- магнитните сензори трябва да са устойчиви на поразяване от външни магнити.
- за повишаване на сигурността на тяхната работа трябва да притежават антисаботажна защита от магнитно поле и допълнителни мерки против разбиване / отлепване.
- магнитните контакти трябва да са предназначени за инсталиране на метални врати и да може да се настройват така, че да компенсират ефектите от стоманата;
- магнитните контакти трябва да са в съответствие с изискванията на списъка DIAM 50 - 3 за използване в обезопасени отделения за архивиране на информация (SCIFs).

5.12. Алармена система срещу проникване за периметърна охрана - интегриране с Главната командно - контролна система

Различните сензори на алармената система срещу проникване за периметърна защита, включително: електронната алармена система срещу проникване, базирана на вибрационни сензори, системата от детектиращи решетки,

комбинираната инфрачервена и микровълнова система и магнитите сензори, трябва изцяло да се интегрират в Главната командно - контролна система за сигурност.

Всички сензори, контролери и други устройства трябва да се появяват на картата на графичния потребителски интерфейс. Главната командно - контролна система трябва да получава информация и да показва състоянието на сензорите и връзките (комуникационния статус), както и алармените сигнали. В случай на отказ на комуникацията, системата трябва да показва точното място на проблема. Алармените сигнали от оградата трябва да предизвикват визуално и звуково сигнализиране в Главната командно - контролна система, като точното местоположение на проникване се показва с точност до 3 [m]. Системата трябва да позволява конфигуриране на контролерите и активиране / деактивиране на отделни сектори (например порталите).

Забележка: **Всеки участник трябва да представи подробна функционална блок - схема, илюстрираща работата на алармената системата срещу проникване за периметърна охрана, връзките между отделните модули и видовете крайни устройства, които смята да използва.**

6. Система за разпознаване на регистрационни номера (СРРН)

6.1. Основни положения

Системата за разпознаване на регистрационни номера трябва да е част от цялостната Система за контрол на достъпа. Необходимо е тя да осигурява управление и контрол на достъпа на оторизирани превозни средства в защитените зони и да идентифицира и отказва достъпа на неоторизирани превозни средства.

- системата за разпознаване на регистрационни номера трябва да се инсталира, за да идентифицира превозните средства (регистрационен номер, тип на превозното средство и идентифициране на шофьора) и да потвърждава дневните и нощните разрешителни за влизане;
- нужно е системата за разпознаване на регистрационни номера да е идентификационна система, работеща със стационарна видеокамера, която трябва автоматично да разчита регистрационния номер на превозното средство;
- потребно е тази система за обработване на изображения да проследява регистрационния номер на превозното средство, да го разчита и идентифицира;
- нужно е системата да използва висококачествен софтуер, който да е интегриран с централната затворена телевизионна система за наблюдение (CCTV). В затворената телевизионна система за наблюдение трябва да има вградени специални алгоритми за разпознаване на регистрационните номера, които да извършват идентифициране и разпознаване на регистрационни номера, без необходимост от допълнителен хардуер като контролери например;
- системата за разпознаване на регистрационни номера трябва да е в състояние да работи безотказно при скорост на движение на превозните средства < 30 [km / h].

6.1.1. Технически изисквания към камерата Основни положения

- цифрова камера от тип IP;
- работа при минимална осветеност от 0 [lux];
- вградени мощни високоефективни инфрачервени светодиоди;
- инфрачервено осветяване на разстояние до 30 [m];
- вграден вентилатор;
- козирка;

- вандалоустойчив корпус;
- корпус за монтиране на стълб;
- защита от фактори на околната среда: IP66;
- осветление на ъгъла на виждане на камерата - 30^0;
- работна температура: от -30 [^{0}C] до +60 [^{0}C];
- относителна влажност: до 95 [% RH].

7. Система за наблюдение под шаситата на моторни превозни средства (СНПШ - МПС)

7.1. Основни положения

Системата за наблюдение под шаситата на моторните превозни средства трябва да се инсталира на основните портали по външния периметър на централата, за да сканира долната част на превозните средства и да даде възможност за откриване в реално време на скрити хора, материали и стоки. С тази система се препятства неразрешен достъп - влизане / внасяне или излизане / изнасяне от защитения периметър на „ТЕЦ Марица Изток 2“ ЕАД. Тя позволява откриване на бомби, експлозиви и съмнителни материали. Системата следва да работи денонощно.

Необходимо е системата да позволява лесно и удобно използване. Потребно е управлението на системата да включва 4 (четири) режима на работа: включен / изключен / ръчен / автоматичен. Резултатите трябва да се запазват във видеоархива на системата за сигурност.

7.1. Технически изисквания

Системата трябва да:

- извършва сканиране на напълно спряло превозно средство;
- има възможност за увеличаване / намаляване („зуум”);
- възможности за сканиране от всички страни под различни ъгли;
- разполага с контролер за избор между „ръчно“ и „автоматично“ управление;
- позволява сканиране, както през деня, така и през нощта и да разполага със собствено независимо осветление;
- работи с цветни IP камери с висока разрешаваща способност;
- осигурява видеопоток при 25 [fps];
- има разрешаваща способност на камерата не по-малко от 530 [TVL] и минимум 345000 ефективни пиксела;
- поддържа минимум оптично увеличение („зуум”) от 24 пъти;
- поддържа инфрачервено осветяване с висок интензитет;
- разполага с обектив, защитен със сапфирен кристал, предпазващ от надраскване;
- предлага стационарно инсталиране;
- има свръхустойчива рампа от галванизирана стомана;
- има водоустойчив и устойчив на атмосферни влияния корпус;
- предлага защита от фактори на околната среда: IP66;
- поддържа работна температура: от -15 [^{0}C] до +60 [^{0}C];

- работи при относителна влажност: до 95 [% RH];
- работи 24 [h] в денонощието, 365 дни в годината, във / през всички сезони, при всякакви метеорологични условия;
- извършва маркиране на дата и час върху записа на събитието;
- позволява (мрежов / цифров) видеозапис;
- се интегрира напълно с другите системи за контрол на достъпа и CCTV;
- използва монитор с минимален размер 21";
- има следните режими на работа:
  - „автоматичен“ - системата се включва автоматично и следва автоматична програма за сканиране, като позволява програмирането на специфични зони за сканиране;
  - „ръчен“ - позволява на оператора да сканира ръчно и да включва режим на търсене. Операторът трябва да може да контролира PAN, TILT, ZOOM (PTZ) функциите, както и повдигането и придвижване на оптичната система по дъното на превозното средство.

8. Система за наблюдение под влакови композиции (СНПВК)

8.1. Основни положения

Системата за наблюдение под влакови композиции трябва да се инсталира на предварително определени железопътни линии, за да сканира долната част на влаковите композиции при тяхното влизане / излизане в / от централата. Сканирането трябва да даде възможност за откриване в реално време на скрити хора, материали и стоки. С тази система се препятства неразрешен достъп - влизане / внасяне или излизане / изнасяне от защитения периметър на „ТЕЦ Марица Изток 2“ ЕАД. Тя трябва да позволява откриване на бомби, експлозиви и съмнителни материали. Системата следва да работи денонощно.

Системата трябва да открива внасяне или контрабанда на незаконни предмети, 24 часа в денонощието, 7 дни в седмицата, при всякакви климатични условия.

Системата трябва да:

- позволява онлайн сканиране на дъното на влака, докато влакът се движи бавно;
- предоставя видеообраз с висока разделителна способност на сканираните резултати;
- запазва резултатите във видеоархива на системата за сигурност.

8.1. Технически изисквания

Системата трябва да:

- извършва сканиране на много бавно движещи се влакове - до 20 [km / h];
- позволява дневно и нощно сканиране;
- разполага със собствено независимо осветление;
- работи с цветни и черно / бели IP камери с висока разделителна способност;
- осигурява видеопоток при 25 [fps];
- има разрешаваща способност на камерите не по-малко от 530 [TVL] и минимум 345000 ефективни пиксела;
- поддържа инфрачервено осветяване с висок интензитет;
- разполага с обектив, защитен със сапфирен кристал, предпазващ от надраскване;
- предлага стационарно инсталиране;
- има водоустойчив и устойчив на атмосферни влияния корпус със специална защита от вибрации;
- предлага защита от фактори на околната среда: IP66;

- има работна температура: от -30 [^{0}C] до +60 [^{0}C];
- работи при относителна влажност: до 95 [% RH];
- работи 24 часа в денонощието, 365 дни в годината, във / през всички сезони, при всякакви метеорологични условия;
- извършва маркиране на дата и час върху записа на събитието;
- позволява мрежов / цифров видеозапис;
- се интегрира напълно с другите системи за контрол на достъпа и CCTV;
- използва монитор с минимален размер 21";
- има автоматичен режим на работа - изпраща сигнал на операторския терминал при откриване на чужд обект;
- има възможност за:
  - самостоятелно независимо инсталиране;
  - работи в мрежа.

9. Затворена система за телевизионно наблюдение (CCTV)

9.1. Основни положения

Необходимо е системата за телевизионно видеонаблюдение да покрива всички „важни“ точки от територията „ТЕЦ Марица Изток **2**“ ЕАД, за да може служителите по сигурността да получават в реално време актуална информация за състоянието на сигурността на обекта. Камерите трябва да се инсталират по периметъра от вътрешната страна и на определени места в рамките на централата, особено при порталите и критичните точки (зони), за да наблюдават подозрителни събития и възпират извършителите на потенциални заплахи.

Системата за видеонаблюдение трябва да работи на открито и закрито с възможности за идентифициране и проверяване на събития и общо наблюдение.

Видеонаблюдението трябва да се интегрира със системите за периметърна защита и системите срещу проникване, чрез приложение за управление и контрол. Необходимо е видеоизображение от съответната камера да се показва автоматично в контролната зала, когато е генериран алармен сигнал от някоя от интегрираните системи (алармената система срещу проникване, видеосистемата за откриване на движение, системата за контрол на достъпа и периметърната защита), като най - близката подвижна камера автоматично трябва да се позиционира в съответното предварително дефинирано положение.

9.2. Компоненти

Затворената система за телевизионно наблюдение следва да се изгради с нови IP камери.

Новата система за видеонаблюдение трябва да включва:

- различни типове камери:
  - фиксирани цветни IP камери за работа на открито;
  - подвижни (PTZ) IP камери за работа на открито;
  - фиксирани IP куполни камери за работа на закрито;
  - подвижни (PTZ) скоростни куполни камери за работа на закрито;
  - термични камери (виж детайли в точка 11.).
- енкодери;
- сървъри на системата за видеонаблюдение (мрежови видеорекордери);
- виртуална видеоматрица;
- клавиатура с контролери за мишка и джойстик;
- цветни видеомонитори;

- приложен софтуер.

Необходимо е системата за видеозапис да се основава на мрежа от сървъри с инсталиран специализиран софтуер, като всички камери трябва да се записват 24 часа в денонощието, 7 дни в седмицата; за период от 30 дни. Записите трябва да поддържат постоянно 12 [fps] и 25 [fps] при генерирана аларма и предварителна аларма.

Архитектурата на системата от мрежови видеорекордери трябва да се основава на принципа n + 1 сървър. Ако някой от сървърите на системата претърпи срив (по каквато и да е причина), камерите, които са свързани към този сървър трябва да се превключват автоматично към резервен сървър. Камерите трябва да се превключат автоматично към оригиналния сървър в момента, в който сървърът се възстанови.

9.3. Техническа спецификация на камерите

Предпочитани производители на различните видове видеокамери: Pelco, Bosch, Panasonic, Axis или техен еквивалент.

9.3.1. Фиксирани IP камери за външно използване

Фиксираните IP камери за външно използване трябва да са в съответствие със следните технически изисквания:

- минимум 1 / 3” CCD / CMOS;
- ден / нощ;
- разрешаваща способност: 720 x 576;
- баланс на белия цвят;
- широк динамичен обхват - минимум 60 [dB];
- обектив от полирано стъкло с регулируемо фокусно разстояние (не се допуска използването на пластмасови обективи);
- отношение сигнал / шум минимум 50 [dB], при изключено автоматично регулиране на усилването;
- автоматичен ирис контрол;
- автоматичен обратен фокус;
- автоматично превключване между дневен и нощен режим;
- чувствителност: минималнна при цветно - 0,5 [lx]; черно / бяло - 0,06 [lx];
- изходи:
  - мрежов порт RJ45;
  - алармено реле минимум 1 / 1;
  - аудио вход / изход;
- 25 [fps] при максимална разрешаваща способност;
- възможност за извършване на настройване през Web браузър;

- видеокомпресиране - H.264;
- възможност за захранване по Ethernet мрежата (Power Over Ethernet) - при включен нагревател;
- работна температура: от -10 [^{0}C] до +50 [^{0}C] без нагревател; от -40 [^{0}C] до +50 [^{0}C] с нагревател;
- относителна влажност: до 95 [% RH];
- вандалоустойчив кожух.

9.3.2. PTZ за външно използване

Подвижните IP камери за външно използване трябва да са в съответствие със следните технически изисквания:

- минимум 1 / 3" CCD / CMOS;
- ден / нощ;
- разрешаваща способност - 550 [TVL];
- оптично увеличение („зуум") - 36 пъти;
- баланс на белия цвят;
- широк динамичен обхват - минимум 60 [dB]
- обектив от полирано стъкло (не се допуска използването на пластмасови обективи);
- отношение сигнал / шум минимум 50 [dB], при изключено автоматично регулиране на усилването;
- обектив с фокусно разстояние: минимално 3,5 [mm] - 122 [mm];
- автоматичен ирис контрол;
- автоматичен обратен фокус;
- автоматично превключване между дневен и нощен режим;
- чувствителност: минималнна при цветно - 0,1 [lx]; при черно / бяло - 0,01 [lx];
- изходи:
  - мрежов порт RJ45;
  - алармено реле минимум 1 / 1;
  - аудио вход / изход.
- възможност за инсталиране по 3 (три) оси: на таван, на стена или на връха на ограден стълб;
- възможност за предварително дефиниране на минимум 64 позиции;
- 25 [fps] при максимална разрешаваща способност;
- работна температура: от -10 [^{0}C] до +50 [^{0}C] без нагревател; от -40 [^{0}C] до +50 [^{0}C] с нагревател;
- относителна влажност: до 95 [% RH];
- вандалоустойчив кожух по стандарт IK10;

- защита от фактори на околната среда: IP66;
- възможност за захранване по Ethernet - мрежата на камерата и PTZ модула (Power Over Ethernet) при включен нагревател;
- хоризонтално движение - въртене (Пап): непрекъснато въртене 360^0, с променлива скорост до 100^0 в секунда;
- вертикално движение (Tilt) в обхват 90^0 - 40^0, с променлива скорост до 40^0 в секунда;
- моторизирани обективи;
- да е възможно монтирането на два инфрачервени прожектора, директно на системата за позициониране (PT).
  - всеки инфрачервен прожектор трябва да осветява различно разстояние и поле с различна широчина (конус с различен ъгъл);
  - ъгълът и разстоянието на осветяване трябва да се определят в зависимост от терена;
  - инфрачервеният прожектор трябва да започва да работи автоматично, когато интензитетът на светлината е нисък;
  - средното време между отказите (MTBF) трябва да бъде най-малко 30000 [h];
  - дължина на инфрачервената вълна: не по-малко от 840 [nm];

9.3.3. IP PTZ скоростна куполна камера

Подвижните IP камери за външна употреба трябва да са в съответствие със следните технически изисквания:

- минимум 1 / 3" CCD / CMOS;
- ден / нощ;
- разрешаваща способност: 720 x 576;
- оптично увеличение („зуум") - x 36;
- баланс на белия цвят;
- скорост:
  - въртене: от $0,5^0$ до 100^0 в секунда при ръчно управление и до 300^0 в секунда при предварително програмирани позиции;
  - накланяне: от $0,5^0$ до 100^0 в секунда при ръчно управление и до 100^0 в секунда при предварително програмирани позиции;
  - скоростта трябва да е регулируема.
- широк динамичен обхват: минимум 52 [dB];
- отношение сигнал / шум: минимум 50 [dB], при изключено автоматично регулиране на усилването;
- обектив с фокусно разстояние: от 5 [mm] до 84 [mm];
- автоматичен ирис контрол;
- автоматичен фокус;
- автоматично превключване между дневен и нощен режим;

- възможност за извършване на настройване през Web - браузър;
- чувствителност: минималнна при цветно - 0,5 [lx]; при черно-бяло - 0,06 [lx];
- скорост на електронния затвор: 1 - 1 / 10000;
- изходи:
  - мрежов порт RJ45;
  - минимум 1 алармен изход;
  - аудио вход / изход.
- възможност за инсталиране по 3 (три) оси: на таван, на стена или на връх на ограден стълб;
- възможност за предварително дефиниране на минимум 64 позиции;
- 25 [fps] при максимална разрешаваща способност;
- H.264 видеокомпресиране;
- работна температура: от -30 [^{0}C] до +50 [^{0}C];
- относителна влажност: до 90 [% RH];
- вандалоустойчив корпус;
- защита от фактори на околната среда: IP66;
- възможност за захранване по Ethernet мрежата (POE).

9.3.4. Фиксирана куполна камера за вътрешно използване

Фиксираните куполни камери за вътрешна употреба трябва да са в съответствие със следните технически изисквания:

- минимум 1 / 3” CCD / CMOS;
- ден / нощ;
- разрешаваща способност 720 x 576;
- баланс на белия цвят;
- вариообектив, минимум 3 [mm] - 9 [mm];
- обектив от полирано стъкло (не се допуска използването на пластмасови обективи);
- отношение сигнал / шум 50 [dB], при изключено автоматично регулиране на усилването;
- автоматичен ирис контрол;
- автоматичен обратен фокус;
- автоматично превключване между дневен и нощен режим;
- възможност за извършване на настройване през Web - браузър;
- чувствителност: минималнна при цветно - 0,5 [lx]; при черно / бяло - 0,06 [lx];
- изходи:
  - мрежов порт RJ45;
  - алармено реле минимум 1 / 1;

- аудио вход / изход.
- 25 [fps] при максимална резолюция;
- H.264 видеокомпресиране;
- работна температура: от -10 [^{0}C] до +50 [^{0}C];
- относителна влажност: до 80 [% RH].

9.3.5. Кожух за камера

Кожусите трябва да са в съответствие със следните технически изисквания:

- корпусът трябва да е изработен от неръждаема стомана или алуминий;
- корпусът трябва да е вандалоустойчив;
- корпусът трябва да разполага с място за камера, обектив и захранване;
- трябва да има сенник за защита срещу отблясъци и за да се намали температурата в корпуса;
- корпусът трябва да включва нагревател и вентилатор;
- нагревателят и вентилаторът трябва да са контролирани от термостат;
- защита от фактори на околната среда: IP66;
- предният прозорец трябва да е направен от стъкло, без оптично изкривяване;
- трябва да е осигурен лесен достъп за инсталиране и поддръжка.

9.3.6. Обектив

Обективите за камерите трябва да са в съответствие със следните технически изисквания:

- обективът трябва да подхожда на сензора (CCD / CMOS 1 / 2", 1 / 3" и т. н.);
- тялото на обектива трябва да е изработено от метал;
- монтаж - C / CS;
- фокусното разстояние трябва да се определя за всяка камера;
- автоматичен ирис контрол;
- ръчното или автоматично мащабиране трябва да се определят за всяка камера;
- ръчно или автоматично фокусиране трябва да се определят за всяка камера;
- работна температура: от -10 [^{0}C] до +50 [^{0}C] без нагревател и вентилатор.

9.3.6. Обектив

9.4. Видеоенкодери

9.4.1. Видеоенкодер - едноканален

- разрешаваща способност 720 x 576;
- разрешаващата способност трябва да може да се променя - 1CIF, 2CIF, 4CIF

и D1;
- конектор - RS232 или RS485;
- PTZ поддържащи протоколи: за предпочитане Pelco D, Pelco C, Bosch или друг;
- 25 [fps] за всички разрешаващи способности;
- скоростта на кадрите трябва да може да се променя;
- H.264 видеокомпресиране;
- BNC конектор - 75 [Ohm];
- мрежов порт RJ45;
- мрежовият порт трябва да може да се настройва за различни режими;
- аудио вход / изход;
- битрейтът трябва да може да се променя;
- алармено реле минимум 1 / 1;
- възможност за захранване по Ethernet мрежата (POE);
- автоматичен ирис контрол;
- автоматичен обратен фокус;
- енкодерът трябва да може да се настройва през браузър.

9.4.2. Видеоенкодер - дванадесетканален

- разрешаваща способност 720 x 576 за всеки канал;
- разрешаващата способност трябва да може да се променя - 1CIF, 2CIF, 4CIF и D1;
- монтиране в рак 1U;
- да включва охлаждащ вентилатор;
- минимум 1 (един) конектор - RS232 или RS485;
- PTZ поддържащи протоколи: за предпочитане Pelco D, Pelco C, Bosch или друг;
- 25 [fps] за всички разрешаващи способности;
- скоростта на кадрите трябва да може да се променя;
- H.264 видеокомпресиране;
- BNC конектор - 75 [Ohm];
- мрежов порт RJ45;
- мрежовият порт трябва да може да се настройва за различни режими;
- аудио вход / изход;
- битрейтът трябва да може да се променя;
- алармен вход - по 1 (един) за всеки канал;
- релеен изход: минимум по 1 (един) на всеки 4 (четири) канала;
- енкодерът трябва да може да се настройва през браузър.

9.4.3. Видеоенкодер - четиридесетканален

- разрешаваща способност 720 x 576 за всеки канал;
- разрешаващата способност трябва да може да се променя - 1CIF, 2CIF, 4CIF и D1;
- монтиране в рак 4U;
- да включва охлаждащ вентилатор;
- минимум 1 (един) конектор - RS232 или RS485;
- PTZ поддържащи протоколи: за предпочитане Pelco D, Pelco C, Bosch или друг;
- 25 [fps] за всички разрешаващи способности;
- скоростта на кадрите трябва да може да се променя;
- H.264 видеокомпресиране;
- BNC конектор - 75 [Ohm];
- мрежов порт RJ45 - по 1 (един) на всеки 4 (четири) канала;
- мрежовият порт трябва да може да се настройва за различни режими;
- аудио вход / изход;
- битрейтът трябва да може да се променя;
- алармен вход - по 1 (един) за всеки канал;
- релеен изход - минимум по 1 (един) на всеки 4 (четири) канала;
- енкодерът трябва да може да се настройва през браузър.

9.5. Система за управление, наблюдение и записване на IP базирано видеонаблюдение (СУНЗ)

9.5.1. Основни положения

Системата за управление, наблюдение и записване трябва да обединява софтуера за аудио и видеомениджмънт със системата за видеоанализ, оптимизирана за работа на открито. Базовият софтуер трябва да може да работи на всеки стандартен компютър (компютри) и трябва да може да поддържа аналогови и IP видеокамери от различни производители и технологии, включително HD / мегапикселови камери.

Всеки мрежов видеорекордер (сървър) трябва да може да получава видеопотоци през IP. Необходимо е всички сървъри сда може да споделят информация помежду си. Обменът на информация трябва да дава възможност на отделните устройства да извършват в реално време предаване, отговор, записване, възпроизвеждане на видеоклип, синхронизирано възпроизвеждане на няколко клипа, управление и архивиране на всички IP потоци, които са свързани към устройството, едновременно с тези между устройствата, с променливи формат на кодиране, честота на кадрите и разрешаваща способност. Обменът на информация също така трябва да позволява на отделните сървъри да извършат „интелигентен“

видеоанализ в реално време.

Цялата функционалност на системата трябва да се осигурява от едно софтуерно приложение, което може да се инсталира на 1 (един) или повече компютри, споделящи ресурси помежду си, без да се изисква централен сървър.

Отделните сървъри на системата може да се групират заедно в едно и също помещение или да са разпределени на територията на централата.

9.5.2. Описание на системата за управление, наблюдение и записване на IP базирано видеонаблюдение

9.5.2.1. Функционално управление на системата

А. Софтуерът за видеомениджмънт трябва да изпълнява следните функции:

- обмен - комуникация и управление на видеопотоците между твърдите дискове и мрежовите входове от други източници (ако се използват такива);
- потребителски интерфейс - получаване на информация от базите данни, от въведени данни от потребители, от входове от външни системи чрез XML API и показване на информация във вид на карти, слайдове, икони, бутони, падащи менюта и видеопрозорци с графични слоеве, в зависимост от предварително дефиниран достъп за дадения обект и потребител;
- изпращане на съобщения - предаване на вътрешни съобщения между процесорите и между устройствата - всички промени, настъпили в дадено устройство трябва да се изпращат до всички други устройства в мрежата по такъв начин, че състоянието на всеки обект, който принадлежи към дадено устройство, трябва да може да се управлява от всяко друго еднакво устройство в мрежата;
- обикаляне (Touring) - автоматични връзки, създаване на графици и зареждане на автоматични параметри;
- разпространение - осигурява еднаквост на информацията във всички устройства;
- предпазване (watchdog) - следене на всички процеси, предварително информиране за евентуален срив и иницииране за рестартиране, включително хардуерни тестове за устройствата.

Б. Софтуерът трябва да изпраща за записване, информация за източниците на аларма, които се управляват от него, включително видеодетектиране на движение, както и за загуба на видеосигнал, било то в резултат на сигнал от устройство за получаване на видеоинформация или в резултат на анализ на получаваните образи.

В. Конфигурацията за източниците на аларма трябва да има възможност да бъде променяна на базата на график, определен в настройката на системата. Устройството трябва да наблюдава алармените графици и да изпраща нови инструкции за записване при необходимост.

Г. На всички оператори трябва да се присвоят равнища на достъп. Равнището на достъп трябва да определя функциите, които са достъпни за съответния оператор. Всеки оператор трябва да вижда само функциите, за които има достъп. Достъпът на потребителя трябва да може да се актуализира в съответствие с предварително зададен график и в резултат на настъпило събитие.

Д. Системата трябва да предоставя следната информация за алармите:

- състояние на алармата:
  - активна;
  - приета;
  - нулирана;
- показване на предварително конфигурирани инструкции за действия, които трябва да се предприемат при аларма;
- възпроизвеждане на различни звукови сигнали за всеки тип сензор и за всеки вид аларма;
- представяне на всеки вид аларма чрез икона, предварително определена от потребителя;
- уведомяване на отговорния персонал чрез изпращане на текстово съобщение.

Е. Системата трябва да:

- определя броя и местоположението на мониторите, на които да се изобразяват алармите;
- възпроизвежда видеоинформация от определен момент преди и до определен момент след сигнала за аларма от всяко устройство и архив;
- променя всички характеристики на обекти от системата в реално време чрез стандартния работен софтуер, без необходимост от използване на специален софтуер за настройване. Обектите на системата за видеоанализ може да се настройват разширено чрез специален софтуер;
- дава възможност за наслагване на цвят върху текст, за показване на местоположението на нарушител и идентификационния номер на дадена камера върху видеодисплея. Слоят с тази информация трябва да може да се показва на цял екран и / или на четворен дисплей. Мястото на полетата от този слой трябва да е динамично и програмируемо. Разрешаващата способност и броят на символите в него не трябва да

бъде по-малък от 200 x 200 пиксела.

Ж. Системата трябва да има възможност за изпращане на аларми към различни работни станции. Тази функция трябва да може да се дефинира в зависимост от часа в денонощието и деня от седмицата. При необходимост трябва да има възможност за изпращане на аларми към повече от една потребителска работна станция.

9.5.2.2. Потребителска работна станция

А. Потребителската работна станция трябва да предоставя на оператора контрол върху всички устройства, свързани към мрежата. Всеки сървър в мрежата трябва да може да изпълнява функциите на работна станция.

Б. Всеки системен оператор трябва да има потребителско име и парола, които може да се променят по време, дата и възникнали аларми.

В. Работното място трябва да предоставя следните екрани:

- карти и слайдове;
- таблици;
- динамични бутони за управление на отделните елементи (които се появяват и променят при избиране на съответния елемент);
- оперативни менюта;
- потребителски инструкции;
- програмируем симулатор за отделните устройства;
- видеопрозорци за изобразяване на картина в релно време;
- меню за настройване на отделни елементи;
- икони.

Г. Потребителската работна станция трябва да предоставя на оператора менюта за състоянието и контролните функции:

- падащи менюта;
- преглед на менюто по начин, определен от администратора;
- състояние на всички сензори.

Д. Потребителската работна станция трябва да позволява на голям брой потребители да комуникират, настройват, контролират и преглеждат данни. Трябва да се осигури незабавен достъп за получаване на информация от съответното устройство, или от което и да е друго устройство в мрежата (всички или тези, определени от програмата) а именно:

- камери, монитори (VGA и композитно видео);

- PTZ контролери;
- „интелигентен“ видеоанализ;
- записващи устройства, възпроизвеждащи устройства;
- аналогови входове и изходи;
- потребители (характеристики и профили);
- работни станции;
- мрежови видеорекордери;
- управление на мрежата (състояние на мрежата и контрол на параметрите);
- външни устройства (системи, които са свързани към устройството);
- местоположение на алармата или нарушителя с калибрирани параметри.

Е. Потребителската работна станция трябва да осигури динамично графично наслояване, без да се изисква повторно логване в системата.

Ж. Трябва да се показват избрани икони, които имат общи черти на картите.

З. Трябва да има филтър за иконите, за да се позволи лесно опериране с голям брой икони.

И. Графичният потребителски интерфейс трябва да показва географското местоположение и състоянието на всяка избрана аларма.

Й. Графичното представяне трябва да се конфигурира така, че алармените икони да се появяват автоматично („изскачайки“) на картите на предварително определено и програмируемо място.

К. Трябва да е възможно графичният потребителски интерфейс да се конфигурира за всеки отделен оператор. Различните равнища на достъп на отделните оператори трябва да предоставят различен потребителски интерфейс.

Л. Всяка работна станция трябва да е в състояние да работи на всеки език, поддържан от Windows и да има възможност отделните работни станции да работят на различен език по едно и също време.

М. Всеки алармен сигнал трябва да може да се свърже с отделни и различни гласови съобщения.

Н. Работната станция трябва да е в състояние да представя самостоятелно или интегрирано видеоизображение в реално време по мрежата.

О. Всяка работна станция трябва да има възможност да контролира и определя видеокартината, която да се показва на всяка друга работна станция, както и на мониторите, използващи композитен сигнал.

П. Всеки оторизиран потребител трябва да е в състояние да контролира дистанционно (от всяка работна станция) другите работни станции в мрежата. Това трябва да включва изключване (log out) на потребители, изключване на станции и рестартиране на устройства.

Р. Всички функции, които са достъпни от главната контролна зала и от нейните работни станции трябва да са достъпни, след определено оторизиране, от всеки друг сървър в мрежата.

С. Всяка работна станция трябва да е в състояние да създава и да приема виртуални аларми въз основа на логически връзки между съобщенията (и, или, нито едно, което и да е, но не и двете заедно).

Т. Всяка работна станция трябва да е в състояние да работи в друг часови пояс, в рамките на една и съща база данни.

9.5.3. Мрежова преносна система

А. Ситемата трябва да поддържа TCP / IP, UDP и RTP протоколи през Ethernet - мрежа. Тя трябва да работи в уникаст, мултикаст и броудкаст режими за данни и видеопотоци.

Б. Устройствата трябва да се настроят, за да работят при постоянна скорост на предаване (CBR). Битрейтът трябва да се определя за всяка камера спрямо алармата и графика.

В. Системата трябва да може да се разширява чрез даване на възможност за пълно дуплекс комуникиране между много устройства.

Г. Системата трябва да е в състояние да насочва видео- и аудиосигналите към различни места.

Д. Системата трябва да поддържа скорост на комуникация минимум 100 [Mbps].

Е. Системата трябва да поддържа много мрежови топологии, включително топологии от типа затворена верига.

Ж. Мрежата трябва да е защитена срещу неоторизирана физическа връзка чрез регистриране на разрешените за ползване в нея MAC адреси.

9.5.4. Система от мрежови видеорекодери

А. Мрежовият видеорекордер трябва да предоставя за запис 32 видеоканала,

използващи MPEG4 или H.264 компресиране при 1 [fps] - 25 [fps] с променлива разрешаваща способност на камерата.

Б. Трябва да се осигурят следните възможности:

- едновременно записване и преглеждане на видеокартина на живо или записан видеоклип;
- самостоятелно конфигуриране на условията за записване за всяка камера;
- записване на видеосигнала от всяка камера на много мрежови видеорекордери и върху присъединени към мрежата масиви от твърди дискове с различни параметри;
- разделяне и обединяване на процесори, масиви от твърди дискове и бази данни през мрежата;
- експлоатационни качества: възможност за записване на видеопотоци и показване на най-малко 3 (три) видеопотока при 25 [fps], HD разрешаваща способност и 6 [Mbps] скорост на потока. Видеопотокът може да е от локални или отдалечени устройства.

В. Записващата система трябва да поддържа следните режими на работа:

- ръчен - записване от оператора. Всеки ръчно записан клип трябва да има максимално предварително зададено време (размер на клипа). Всеки канал за записване трябва да има максимална квота (брой на клипове);
- циклично записване - записване на група изображения през определени периоди от време. Дефинираното време за записване от всяка камера трябва да представлява един цикъл. (метод FIFO (първи записан - първи изтрит) за управление на квотите за записване);
- събитие - предварително определени алармени и системни събития, трябва да предизвикат запиване на клип с предварително зададена продължителност. Броят на клиповете трябва да е определен и да се управлява по метода FIFO. Системата трябва да заснема клиповете последоватеелно, в един цикъл. Когато дадено събитие се приеме, системата трябва да продължи да записва за предварително определен следалармен период. Системата трябва да може да започне да записва нов клип с приключването на следалармения период.

Г. Системата трябва да позволява показване на записаните видеоклипове.

Д. Позицията на показване върху монитора трябва да е програмируема.

Е. Системата трябва да е в състояние да показва едновременно най-малко 4 (четири) видеоизображения на всеки монитор.

Ж. Форматът за записване трябва да бъде кадър по кадър, позволявайки

хомогенно използване на мрежата и гладко показване на записания клип.

З. Трябва да има възможност даден запис да се възпроизвежда в затворен цикъл.

И. Всички възможности на системата за дадено устройство трябва да са достъпни по мрежата от всички останали устройства.

9.5.5. Декомпресиране и възпроизвеждане на клипове от архива

А. Възпроизвеждащото устройство трябва да позволява показване на записани клипове на монитора.

Б. Позицията на показване върху монитора трябва да се определя по настройки, които са направени от потребителя.

В. Възпроизвеждащото устройство трябва да позволява декомпресиране и възпроизвеждане на клипове от всяко устройство в мрежата, при използване на постоянна скорост (CBR) и гладко показване. Прехвърлянето на клипове между устройствата трябва да се извършва чрез RTP (Real Time) протокол.

Г. Буферът на възпроизвеждащото устройство не трябва да надвишава 50 кадъра. Възпроизвеждането на всеки избран кадър от даден клип трябва да започне в рамките на 2 [sec] след избиране на съответната команда. Трябва да има пълен контрол върху режима на декомпресиране: преместване „напред“ и „назад“ с различни скорости (до 32 пъти по - големи от оригиналната скорост), „стоп“ и „пауза“ (без „вибриране“ на изображението на екрана).

Д. Декомпресирането на записите трябва да се основава на някой от следните критерии:

- дата и час;
- камера;
- записващо устройство;
- вид на алармата;
- тип на сензора;
- тип на записа.

Е. Декомпресирането (разархивирането) трябва да предоставя списък с клипове, съдържащ най-малко един кадър от търсените час и дата.

Ж. Възпроизвеждащото устройство трябва да поддържа команда „отиди в“ („Go To“) за осигуряване на достъп и възпроизвеждане на определено

време и дата в рамките на даден клип.

З. Трябва да е възможно различни едновременно работещи възпроизвеждащи устройства да получават едни и същи или различни клипове по едно и също време от едно или няколко устройства.

И. Възпроизвеждащото устройство трябва да позволява копиране на определена част от клип (монтиране).

Й. Възпроизвеждащото устройство трябва да е в състояние да се свързва с друго записващо устройство.

9.6. Използване на видеоматрицата и PTZ контрол

А. Видеоматрицата трябва да има възможност за свързване на източника на видеосигнал (камерата и / или записващото устройство) към монитора. Всяко устройство трябва да има уникален IP адрес.

Б. Устройството трябва да има възможност да изпраща команди към PTZ камерите и да получават „отговори“ от тях, локално или чрез мрежата, с ограничени закъснения (до 250 [ms]).

В. Софтуерната видеоматрица трябва да позволява свързването на всеки видеосигнал към всеки видеоизход. Видеоизображението от една и съща камера може да се програмира за едновременно показване на няколко монитора и да се записва на няколко записващи устройства. Броят на комбинациите за свързване трябва да е неограничен. Това трябва да се извършва чрез мултикастинг по мрежата, за да се оптимизира нейното натоварване.

Г. Системата трябва да предоставя програмируеми последователности за превключване между камери, цветни наслагвания върху VGA дисплеи, а така също и показване на образа върху цял или разделен на 4 екран.

Д. Ръчният контрол на **PTZ** камерите трябва да има следните характеристики:

- възможност за дефиниране на икони, при настройване на системата, за управление на PTZ камерите директно от екрана, върху който се изобразява картина от камерата в реално време;
- възможност за „кликване“ върху видеоизображението, получавано в реално време, за да се контролират PTZ характеристиките на камерата.

Е. Системата трябва да може да поддържа PTZ камерите в режим

„сканиране“. Потребителят трябва да има възможност да конфигурира: наклона, увеличението / намалението, фокуса, настройването на ириса, обхвата на движение и скоростта на въртене на камерата в режим „сканиране“.

Ж. Предварително определени позиции на камерата трябва да може да се дефинират при системното настройване. Системата трябва да е в състояние да свързва иконите от 3D картите и алармите с настройките на съответната неподвижна камера или настройките за предварително дефинираната позиция на PTZ камерата, включително увеличение, фокус и настройка на ириса за съответната позиция.

З. Системата трябва да поддържа следното предварително зададено функционално настройване на камерата:

- потребителят трябва да определя настройките на камерата, които да се използват при записване по график или записване при алармена ситуация;
- „отговорът“ на дадена аларма трябва да включва команди, за насочване на определени камери към съответните видеоизходи (VGA монитор, композитен монитор и записващо устройство) и „извикване“ на предварително дефинирани настройки на камерата;
- записване по график, записване при аларма и извършване на няколко предварително дефинирани действия в „отговор“ на дадена аларма;
- проследяване на „обръщанията“ към предварително дефинирани настройки на камерата за дадена задача и приоритетите на различните задачи - ако задача с по-висок приоритет, „прерди“ задача с по-нисък приоритет, системата трябва да „върне“ камерата към нейните настройки за задачата с по-нисък приоритет след приключване на задачата с по-висок приоритет.
- възможност за показване на образа от една и съща камера няколко пъти - всеки път с различна предварително дефинирана настройка.

И. Матрицата трябва да има възможност за създаване на един или повече маршрути - обиколки. Всеки образ от дадена камера трябва да съдържа поредния номер на входа на камерата и номера на съответната предварителна настройка.

- възможност за настройване на продължителността на задържане в определена позиция за всяка отделна камера;
- възможност за извикване на определен маршрут, съставен от няколко предварително дефинирани позиции и настройки за една и съща камера.

Й. Системата трябва да има възможност да прилага „интелигентни“

решения при обхождането на определен маршрут, които да съчетават видеодетектирането на движение с движението по маршрута. При този тип обиколка, времето на задържане на обиколката във всяка предварително дефинирана позиция, трябва да зависи от това дали камерата засича дейност в полето на наблюдение. Ако няма дейност, камерата трябва да премине към следващата позиция от маршрута по-бързо. Потребителят трябва да може да настрои камерата, да се върне към режим на сканиране, когато тя не се използва за друга цел.

9.6.1. Инструкции за „плаващ“ вход на записващо устройство

А. Системата трябва да има възможност да свързва и да управлява видеовходове, да свързва видеоизходи за монитори, да изпраща инструкции за записване, да свързва всяка камера към всяко устройство в мрежата.

Б. Инструкциите за „плаващ“ вход на записващо устройство трябва да дават възможност на системата да поддържа: записване при срив, записващи устройства за специални аларми и запис при поискване.

В. Системата трябва да позволява записване при срив, като даде възможност на потребителя да дефинира едно или малък брой записващи устройства с инструкции за „плаващ“ вход, които може да служат като „Back - up“ за всяко друго записващо устройство в системата.

9.7. Възможности на софтуера на системата за видеонаблюдение да управлява останалите ситеми за безопасност и охрана

А. Софтуерът на системата за видеонаблюдение трябва да има възможности да управлява и наблюдава останалите системи за сигурност на територията на централата, като същесвременно е независим по отношение на основната система за управление на сигурността на центалата. Алармите, постъпващи от другите системи (АССПО, АССП, СКД, СПБ и т. н.), трябва да се показват на работните станции на затворената система за телевизионно видеонаблюдение, като се представят на оператора приоритетно. Това позволява на системите за сигурност и безопасност на територията на централата да продължат да функционират дори в случай на отказ на Главната командно - контролна система за управление на сигурността.

Б. Софтуерът на системата за видеонаблюдение трябва да предоставя следната информация за алармите:

- състояние на алармата;

- активна;
- приета;
- нулирана;

- показване на предварително конфигурирани инструкции за действия, които трябва да се предприемат при аларма;
- възпроизвеждане на различни звукови сигнали за всеки вид аларма;
- представяне на всеки вид аларма в цвят, определен от потребителя;

В. Софтуерът на системата за видеонаблюдение трябва да обработва алармени събития от различни източници, включително:

- видеодетектиране на движение / отсъствие на движение;
- откриване на загуба на видеосигнал, или чрез сигнал от източника на видеосигнал или чрез анализ на заснетите изображения;
- всяка промяна в статуса на дадено устройство трябва да генерира алармено съобщение в системата;
- старт / край на активност плюс всички промени в статуса - генериране на алармено съобщение, съответстващо на всяка отделна промяна в статуса.

Г. Софтуерът на системата за видеонаблюдение трябва да позволява на потребителя да дефинира как да се следи състоянието на алармените източници и да изпраща алармени съобщения към потребителската работна станция въз основа на промени в статуса им. Броят и видът на алармените съобщения, които трябва да се генерират за даден алармен източник, трябва да се определят от конфигурирането на източника.

Д. Софтуерът на системата за видеонаблюдение трябва да изпраща информация за записване, за конфигурирането на алармените източници, които се управляват от него, включително алармени контакти, детектиране на видеодейност, както и за детектиране на загуба на видеосигнал. Конфигурирането на алармените източници трябва да може да се променя на базата на график, определен в настройка на системата. Софтуерът трябва да наблюдава алармените графици и да изпраща необходимите нови инструкции към записващите устройства.

Е. Администраторът трябва да определя реакцията на системата на всяко алармено съобщение.

Ж. Операторът трябва да бъде отговорен за:

- четенето на информацията за реагирането на дадена аларма;
- получаването на алармени съобщения от алармените източници;
- проверяването на историята на алармените събития;
- организирането на „отговор“ на всяко алармено съобщение.

З. Конфигурациите на алармените източници и алармените „отговори“ трябва да може да се сменят съобразно съответния график.

И. При получаване на сигнал за аларма, софтуерът на системата за видеонаблюдение трябва да предостави инструкции за действия, които да се изпълнят в „отговор“ на съобщението за аларма:

- инструкции за записване - старт на записването или промяна в режима на записване за една или повече камери, свързани с едно или повече устройства;
- инструкции за видеоматрицата - извикване на предварителни настройки за камерите и показване на определени камери на мониторите за гледане на видеоизображения в релно време - на живо, свързани с алармено събитие;
- инструкции за дисплея - уточняване как алармите трябва да се показват на мониторите, включително цветове, които да се използват за обозначаване спешността на алармата, всички съобщения, които да се показват, дали видеоизображението трябва да се показва автоматично на алармения монитор и т. н.

Й. Софтуерът на системата за видеонаблюдение трябва да има възможност да направлява аларми към специфични потребителски работни станции в рамките на системата. Изпращането на алармени съобщения трябва да е възможно да се променя по предварително зададен график. Също така, софтуерът трябва да осигурява възможност за едновременно насочване на аларми към повече от една потребителска работна станция (при необходимост).

К. Системата трябва да е в състояние да дефинира софтуерни модули, които да контролират поведението на други елементи. Тези елементи трябва да може да се комбинират в неограничен брой логически връзки. За всяка система броят на логическите връзки между елементите й трябва да е неограничен.

Л. Системата трябва да предоставя списък от инструкции, които да включват всички елементи, определени в рамките на системата. Въз основа на тези инструкции, системата трябва да може да създаде неограничен брой макросценарии. Макросценариите трябва да може да се активират въз основата на график, ръчна намеса, обект в системата или статус на устройство. Всеки макросценарий може да има специфични закъснения, свързани с него.

М. Системата трябва да може да съхранява и извлича данни за историята на

събитията - локално, както и в цялата система. Това включва алармена дейност, видеоклипове, изображения и информация за оператора.

Н. Софтуерът на системата за видеонаблюдение трябва да позволява дефинирането на графици, които автоматично да изпълняват следното:

- да разпознават специалните почивни дни;
- да правят разлика между пълен и непълен почивен ден;
- да включват много видове почивни дни;
- да сигнализира на системния оператор за предстоящи почивни дни, една седмица предварително, за да се осигури проверяване на валидността на съответните дати.

9.8. Разширяване на системата

Системата трябва да има неограничени възможности за разширяване.

9.9. Архивиране („Back - up“)

Архивирането трябва да се извършва в реално време, за да се предотврати възможността за загуба на информация. Архивирането трябва да се извършва върху дисков масив организиран в RAID-5.

9.10. Хардуер на на системата от мрежови видеорекордери

Хардуерът на сървърите и работните станции трябва да е от водещи производители, като например DELL, IBM, HP или друг.

Системни изисквания

обект	технически спецификации
1	2
процесор	Intel i7 / Xeon E5 2600 или по-висок клас
оперативна памет	минимум 8 [GB] D3 RAM
харддиск устройство	Минимум 2 [TB] с RAID поддържане
DVD записващо устройство	Външно DVD +16, RW, +8x, CDW 48x, Blue ray
мрежов адаптер	двоен TCP / IP,интегриран 10 / 100 / 1000 base - T

звукова карта	вградена
видеокарта	минимум1 [GB] DDR 5
записваща скорост	25 [fps] / канал (за 32 канала)
USB 3.0	2 на предния панел
клавиатура	PS / 2
мишка	Оптична мишка със скрол бутон
монитор	22”
операционна система	MS Windows последна версия - към момента на провеждане на търга
антивирусна програма	последна версия на антивирусен софтуер към момента на провеждане на търга

9.11. Разпределена верижна архитектура на системата от мрежови сървъри

Системата от сървъри на системата за видеонаблюдение трябва да е проектирана и организирана като разпределена мрежа.

А. Всички сървъри трябва да комуникират един с друг, да „споделят“ една и съща база данни, права на потребителите и други.

Б. Всички сървъри трябва да може да „споделят“ и архивират данни (видеоклипове) и да може да се конфигурират едновременно.

В. Всеки компютър трябва да може да функционира пълноценно като сървър, работна станция и процесор за „интелигентен“ видеоанализ.

Г. Не трябва да има централен сървър.

Д. Системата трябва да е с висока надеждност (no single point of failure).

Забележка: Всеки участник трябва да представи подробна функционална блок - схема, илюстрираща работата на затворената система за телевизионно видеонаблюдение, връзките между отделните модули и видовете крайни устройства, които смята да използва.

10. Видеосистема за откриване на движение / „интелигентен“ видео анализ (ВОД / ИВА)

10.1. Основни положения

Видеосистемата за откриване на движение трябва да се интегрира със затворената системата за видеонаблюдение (CCTV) и да е приложена на определени фиксирани камери - като вграден алгоритъм в камерата или като отделно оборудване.

10.2. Основни характеристики

Видеосистемата за откриване на движение трябва да осигурява чрез персонален компютър съвременно цифрово видеодетектиране на движение и проследяване при проникване.

Системата трябва да работи с широк набор от камери, произведени от известни производители, които са разположени на стратегически места в охранявания обект.

Системата трябва да осигурява надеждно откриване на нарушители при различни атмосферни условия, като същевременно се запазят ниски стойности за броя на лъжливите и нежеланите аларми.

Системата трябва да осигурява: цялостно алармено оповестяване, коректно реагиране на видеоматрицата за изпращане на образ от алармено събитие на правилно избран монитор, цветни графики, свързани с видеоизображението и запис на възникналите събития.

Системата трябва да се проектира за работа на открито и да е в състояние да открива и проследява няколко цели с 1 (една) камера.

Всеки първоначален видеокадър, от всяка възникнала аларма при неразрешено проникване, трябва да се записва на системния твърд диск за по-късно разследване.

Видеосистемата за интелигентен видеоанализ трябва да позволява автоматично откриване на подозрителни движения на предмети или хора във видеоизображенията от всяка камера в мрежата, като същевременно превръща всяка камера в усъвършенстван сензор.

10.2.1. Типове „интелигентен“ видеоанализ

Софтуерът на системата за видеонаблюдение трябва да има вградени алгоритми за „интелигентен“ видеоанализ, които трябва да предоставят следните възможности,

приложими както за камери за използване на открито, така и на закрито:

- видеодетектиране на движение по подразбиране - използва се като виртуална разделителна ивица / виртуална ограда (предварително определена и със заводско калибриране), при пресичане на която се подава сигнал;
- „интелегентен“ видеоанализ / поведенчески анализ - анализира поведението на движещи се обекти чрез:
  - модел и скорост на движение;
  - забавяне (разтакаване) във времето или в определени зони;
  - ограничени / забранени зони и други.
- „интелегентен“ видеоанализ / детектиране на липса на движение - открива изоставени предмети;
- екстремен „интелегентен“ видеоанализ - приспособени алгоритми, конфигурирани на място, приложими за сложни сценарии, като: усъвършенствани модели на проникване / трикове за проникване, сложна среда (например огледални стени);
- „интелегентен“ видеоанализ за PTZ камера - прави се анализ на всяка запаметена позиция, като на отделна камера;
- автоматично проследяване с PTZ камера - поддържа следения обект в рамките на зрителното поле на камерата;
- детектиране на тълпи - нетипично събиране на група хора на едно място;
- разпознаване на лица - да може да категоризира лица, с променлива степен на доверие (достъп) като: „черен“ списък (забранени), „бял“ списък (позволени), „сив“ списък (неразпознати);
- преброяване на хора;
- разпознаване на регистрационни номера - да може да категоризира регистрационни номера: „черен“ списък (забранени), „бял“ списък (позволени), „сив“ списък (неразпознати).

10.2.2. Филтри на „интелигентен“ видеоанализ

Системата за „интелегентен“ видеоанализ трябва да има специални алгоритми за тежки външни условия, включително разширени филтри за:

- дъжд;
- движение на стълба на камерата;
- сенки;
- облачно време;
- движение на дървета и растителност;
- птици и дребни животни.

10.2.3. Метод на действие на „интелигентния“ видеоанализ

А. Системата за „интелегентен“ видеоанализ трябва да се интегрира в софтуера на системата за видеонаблюдение и да предоставя актуален „интелигентен“ видеоанализ за „външни“ / „вътрешни“ приложения, без необходимост от добавяне на допълнителен хардуер / софтуер. Приложението трябва да обработва целия видеосигнал при пълна скорост на кадрите и на всички видеовходове.

Б. Системата за „интелегентен“ видеоанализ трябва да има възможност за обработване на видеосигналите и идентифициране на целите, като същевременно изчислява реалния размер на обекта в цялата зона на детектиране.

В. Системата за „интелегентен“ видеоанализ трябва да има възможност за изчисляване на промени в размера на обекта в съответствие с 3D (топографска карта), както и по отношение на разположението на камерата и полето на видимост, включително равнинни промени като хълмове, сгради и изкачвания.

Г. Системата за „интелегентен“ видеоанализ трябва да има възможност да дефинира промени в терена (като склонове, хълмове, постройки), маскиране и перспективно компенсиране.

Д. Приложението за „интелегентен“ видеоанализ трябва да предоставя най-малко 25000 детектиращи клетки за всяка камера и трябва да е в състояние да използва 100 % (сто на сто) от зрителното поле на камерата.

Е. Зоната на детектиране на всяка камера трябва да е най-малко 3000 [m^2] (например 30 [m] x 100 [ш]).

Ж. Системата за „интелегентен“ видеоанализ трябва да има разработени алгоритми за компенсиране на влиянието на неблагоприятни условия на околната среда, включително филтри за:

- дъжд;
- движение на пилона на камерата;
- сенки;
- облаци;
- движение на дървета и друга растителност;
- птици и малки животни.

З. Системата за „интелегентен“ видеоанализ трябва да позволява няколко

зони едновременно да са обект на проследяване и интерес. В тези зони на някои или на всички детектиращи клетки трябва да може да се зададат следните критерии за детектиране или липса на детектиране:

- детектиране на всякакъв вид движение;
- обекти със специфичен размер;
- обекти със специфичен праг на чувствителност;
- скорост на движение на обекти;
- посока на движение на обекти;
- едновременно откриване и проследяване (чрез изобразяване на пътя в различни цветове) на най-малко 6 (шест) нарушители за всяка камера;
- филтриране на постоянни движения в изображението.

И. Системата за „интелегентен“ видеоанализ трябва да съхранява всички настройки на детектиране и настройките на камерите в база данни и да има възможност за зареждане или промяна на тези настройки при желание от потребителя - по предварително определен таймер, или при системно събитие (аларма или други).

Й. Системата за „интелегентен“ видеоанализ трябва да съхранява висококачествени изображения на точния момент на алармата за последващ разбор.

К. Системата за „интелегентен“ видеоанализ трябва да е в състояние да изпълнява дейността си като предоставя аналогово видеоизображение в реално време, записан клип или цифров видеообраз, който да се предава по мрежата.

Л. Системата за „интелегентен“ видеоанализ трябва да включва аналитична програма, която да има способността за наблюдаване в детайли на работата на алгоритъма по време на детектирането на движение. Програмата трябва да позволява активиране на алгоритъма за всеки образ поотделно, за по-внимателно анализиране на резултатите от детектирането.

М. Софтуерът на системата за „интелегентен“ видеоанализ трябва да генерира аларма при загуба на картината от дадена камера.

Н. Системата за „интелегентен“ видеоанализ трябва да генерира аларма при външна намеса в някоя от камерите, като например блокиране.

О. Софтуерът на системата за „интелегентен“ видеоанализ трябва да включва алгоритъм, чрез който да се компенсират облаците. При разпознаване на такова събитие, „засегнатата“ зона трябва да обмени

информация за движението на облаците с всички други зони на „интелегентния“ видеоанализ в съответното устройство.

П. Системата за „интелегентен“ видеоанализ трябва да е снабдена с цифрово записващо устройство, за да се даде възможност за последващо обработване, като се използват всички възможности.

Р. При аларма за наличие на движение / липса на движение, системата трябва да дава инструкции, които да се изпълнят в „отговор“ на съобщението за аларма:

- инструкции за записване - старт на записване или промяна на режима на записване за една или повече камери, свързани с едно или повече устройства;
- инструкции за превключвателя на видеоматрицата - „извикване“ на предварителните настройки на камерите и „извикване“ на камерите на монитори за гледане на видеоизображения в реално време, свързани с аларменото събитие;
- инструкции за мониторите - уточняване как алармите трябва да се показват на мониторите, включително цветовете, които ще се използват за обозначаване спешността на алармата, всички съобщения, които трябва да се показват, дали видеото трябва да се показва автоматично на алармения монитор и т. н.;
- инструкции за приключване - довеждат до спиране на други инструкции.

11. Електрооптични сензори / термични камери (ЕОС / ТК)

11.1. Основни положения

Електрооптичните сензори са интегрирана система, ползваща **2** (две) технологии (термична и CCD) за наблюдаване на открито за дневно и нощно виждане.

Системата от електрооптчини сензори трябва да съчетава термични и CCD сензори за откриване на движение и идентифициране на движещият се обект.

Неохлаждаемата PTZ термична инфрачервена камера и CCD камерата с висока разделителна способност трябва да се затворят в общ корпус и да се монтират на обща стойка със свръхмощен и точен мотор за въртене и накланяне с променлива скорост.

Системата трябва да се инсталира на високи стълбове за камери, за да покрива големи неосветени зони.

Видеосигналите от системата от електрооптчини сензори трябва да се предават към системата от мрежови видеорекордери като част от системата за видеонаблюдение.

Системата електрооптчини сензори трябва да се контролира и от системата за контрол на видеонаблюдението.

11.2. Технически изисквания

11.2.1 Термичен сензор

- спектрален диапазон: 8 [μm] - 14 [μm];
- видеоразрешаваща способност: 384 x 288;
- P / T протокол: за предпочитане на Pelco D или друг;
- защита от фактори на околната среда: минимум IP65;
- две зрителни полета: 135 [mm] / 45 [mm];
- обхват на детектиране: минимум (2500 [m] / 800 [m]) обхват на детектиране на хора;
- обхват на разпознаване: минимум (800 [m] / 250 [m]);
- термична чувствителност: < 85 [mK] NEdT (шумоеквивалентна температурна делта (noise equivalent delta temperature)) при f / 1.6;
- фокус - моторизиран;
- обръщане на поляритета - „черен горещ“ или „бял горещ“.

11.2.2 CCD - сензор

- оптично увеличение („зуум”): до 36 пъти;
- разрешаваща способност: 540 [TVL];
- P / T протокол: за предпочитане на Pelco D или друг;
- CCD - сензор: минимум 1 / 4”;
- ефективни пиксели: над 400000;
- автоматично регулиране на усилването;
- отношение на сигнал / шум 50 [dB];
- широк динамичен обхват;
- компенсиране на задно осветяване;
- работна температура: от -40 [^{0}C] до +60 [^{0}C].

11.2.3 Механични

- задвижващо устройство: неделим задвижващ мотор за въртене / накланяне (pan / tilt) - със задвижващи се стоманени предавки;
- ъгъл на въртене: 360^0 непрекъснато въртене;
- скорост на въртене: променлива скорост до 40^0 в секунда;
- ъгъл на накланяне: минимум от -45 [^{0} C] до +45 [^{0}C];
- скорост на накланяне: променлива скорост: от 0,1^0 до 10^0 в секунда;
- точност при позициониране в предварително зададени позиции: по-добра от 0,02^0;
- задължително пропорционално P / T спрямо позицията на увеличение („зуум”).

12. Инфрачервени осветители и осветители с бяла светлина

12.1. Инфрачервени осветители - технически изисквания

- изградени на основата на LED - технология, с използване на свръхмощни светодиоди, за постигане на осветеността, необходима за работата на системата за телевизионно видеонаблюдение;
- инсталирани, като част от конструкцията за видеокамерите, вградени в корпуса на камерите или инсталирани в самостоятелен корпус, на отделна конструкция, за разширяване на възможностите за наблюдение с видеокамерите;
- разстояние на осветяване - късо, средно и далечно в рамките от 30 [ш] до 150 [m];
- далечното разстояние на осветяване се отнася за PTZ видеокамерите и обикновено се интегрира с късо и средно разстояние на осветяване;
- ниска консумация на електрическа енергия;
- чувствителност: от 10 [lx] до 20 [lx];
- вградена фотоклетка;
- средно време между отказите (MTBF): минимум 30000 [h];
- защита от фактори на околната среда: минимум IP65;
- дължина на инфрачервената вълна: 840 [nm];
- ъгълът и разстоянието на осветяване трябва да се определят спрямо терена;
- инфрачервеният осветител трябва да започне да работи автоматично, когато интензивността на светлината е ниска.

12.2. Осветители с бяла светлина - технически изисквания

- осветление с бяла светлина, на основата на PL - технология или флуоресцентна технология трябва да се инсталира на порталите, за да се повиши равнището на осветеността, както и за да се подпомогне осъществяването на проверки, мониторинг и управление, във връзка със сигурността;
- осветителните тела трябва да са с ниска консумация на електрическа енергия и висока ефективност;
- осветлението следва да се инсталира на нови стоманени конструкции / стълбове или на съществуващи стълботе, отчитащи характерните особености на обекта и поставените изисквания;
- равнището на осветеността трябва да е не по-малко от 50 [lx];
- осветителите трябва да са от тип, предназначен за инсталиране на открито;

- **степен на защита от фактори на околната среда: IP65.**

13. Алармена система срещу проникване (АССП)

13.1. Основни положения

Алармената система срещу проникване трябва да открива опити за проникване в закрити и открити места и своевременно да подава аларма към Главния контролен и команден център по сигурността.

Модули на АССП трябва да се монтират в чувствителни и критични места в централата, като:

- административните сгради;
- работни помещения, помпени зали и електрозалата на генераторите;
- охранителното оборудване;
- IT помещенията;
- други.

13.2. Компоненти

Алармената система срещу проникване трябва да съдържа следните компоненти:

- локален алармен контролер (ЛАК), включващ:
  - централен процесор;
  - I / O устройства;
  - комуникационен модул;
  - електрическо захранване.
- буквено - цифрови клавиатури за включване и изключване на системата;
- детектори / сензори за проникване;
- комбинирани детектори;
- магнитни контакти;
- паник - бутони.

13.3. Технически изисквания

13.3.1. Основни положения

Алармите, генерирани от различните детектори трябва да се предават на локален алармен контролер, който е необходимо да има напълно програмируем алармен панел, съдържащ входни / изходни контакти и необходимите интерфейси за интегриране с други системи. Контролерът следва да е от модулен тип, позволяващ разширяване чрез добавяне на необходимия брой разширители за входни / изходни точки.

АССП трябва да се интегрира с Главната командно - контролна система за сигурност чрез сървърите на системата за контрол на достъпа. СКД (респективно АССП) трябва да изпраща алармите, получени от детекторите към сървъра на Главния център. Алармите трябва да се анализират и да се показват на работните компютърни станции на операторите по сигурността в Главния команден и контролен център по сигурността.

13.3.2. Алармен контролер

- аларменият контролер трябва да е микропроцесорно програмируемо устройство, което се състои от локална енергонезависима памет, I / O модули, захранване и комуникационен интерфейс;
- аларменият контролер трябва да е с модулен дизайн и да използва "BUS" технология за разширение.
- аларменият контролер трябва да има възможност за разширяване чрез използване на разширителни платки и с допълнителни алармени панели в мрежата.
- конфигурационните и програмируемите параметри на алармения контролер трябва да може да се въвеждат локално от персонален компютър или по мрежата от Главната командно - контролна система.
- входно / изходните модули трябва да може да се инсталират вътре в алармения контролер и външно на различни места в охранявания обект;
- аларменият контролер трябва да поддържа комуникация с външни модули.
- комуникационният интерфейс между алармения контролер и външните (отдалечени) устройства трябва да се основава на мрежови връзки или "BUS" топология.
- аларменият контролер трябва да „докладва" за следните видове повреди:
  - антисаботажен контакт на задния капак на контролера;
  - антисаботажен контакт на вратата на контролера;
  - повреда в комуникацията с Главната система;
  - повреда в главното електрическо захранване;
  - повреда на батерията;
  - изтощена батерия;
  - повреда в клавиатурата;
- всички съобщения трябва да се показват на дисплея на клавиатурите на локалните контролери и на екраните на работните станции на Главната командно - контролна система, както всички други събития.
- в нормално състояние, алармените контролери трябва да се наблюдават и контролират от Главната командно - контролна система чрез сървърите на системата за контрол на достъпа. Алармените съобщения трябва да се показват на екраните в Главния команден и контролен център. При

изчистване на алармено съобщение от екрана на компютъра, не трябва да се изчиства алармата в локалния контролер.

- изчистването на алармата от алармения контролер трябва да може да се извършва само от неговата клавиатурата след използване на валидна потребителска парола.
- всички съобщения, получени от алармения контролер и всички действия, извършвани от операторите и на клавиатурите на контролерите трябва да се предават към Главната командно - контролна система и да се записват в паметта на панелите.
- в случай на неизправност в Главната командно - контролна система или липса на комуникация между нея и панела, алармения контролер трябва да може да функционира самостоятелно. Всички функции, като например включване / изключване, активиране / дезактивиране на зони и други, трябва да се извършват от клавиатурите на контролерите.
- при възстановяване на връзката с централния компютър, алармения контролер трябва да предаде всички записани съобщения в локалната си памет към централния компютър. Предаваните съобщения трябва да съдържат времева отметка, в съответствие с която те трябва да се архивират в централната компютърна система.
- аларменият контролер трябва да е в състояние да съхранява минимум 250 съобщения. Ако комуникацията не е възстановена преди паметта на алармения контролер да се запълни, новите съобщения ще се съхраняват по метода FIFO.
- продължителността от време между получаването на съобщението (задействане на контакта на входната точка) и предаването на съобщението до основната система трябва да не надвишава 2 [sec].
- аларменият контролер трябва да работи в независими зони. Всяка зона трябва да може напълно да се конфигурира софтуерно като:
  - 24 часова;
  - ден / нощ;
  - изход;
  - достъп;
  - паника;
  - принуда.
- аларменият контролер трябва да позволява обособяване най-малко на 8 (осем) дяла с различен брой зони. Всеки дял трябва да може да се активира / дезактивира отделно и независимо от другите дялове;
- включването / изключването на дялове трябва да може да се извършва от клавиатурите на алармения контролер, както и от работните станции на Главната командно - контролна система.
- за всеки дял трябва да може да се определи специална клавиатура за

включване / изключване или да може да се активира / дезактивира от централната клавиатура.

- състоянието на дялове и зоните, определени към съответните дялове, трябва да се показва на динамични дисплеи с графичен потребителски интерфейс на станциите на Главната командно - контролна система.
- на дисплея трябва да се представя състоянието на елементите на алармената система в реално време.
- процесор:
  - алармения контролер трябва да се проектира така, че работния софтуер и работните параметри трябва да се намират в енергонезависима памет;
  - когато се наложи актуализиране на софтуера или промяна на версията на софтуера, новата версия на софтуера трябва да се изтегли на алармения контролер от Главната командно - контролна система или от преносим компютър, свързан локално към алармения контролер чрез един от неговите комуникационни портове;
  - зареждането на нова версия на софтуера трябва да се разреши, по време на нормалното функциониране на алармения контролер и процеса на зареждане не трябва да пречи на работата на устройството. След приключване на процеса на зареждане, алармения контролер трябва ръчно да се превключи към новата версия на софтуера;
  - запазване на параметрите: алармения контролер трябва да съхранява конфигурационните си параметри във файл или файлове. Тези файлове трябва да може да се прехвърлят по мрежата от алармения контролер на Главната командно - контролна система или на преносим компютър за резервно съхраняване.
- захранване:
  - работното напрежение на алармения контролер трябва да е между 12 [V DC] и 24 [V DC]. Захранването към алармения контролер, I / O модулите и детекторите, трябва да е доставено от наблюдаван източник на захранване;
  - електрозахранването трябва непрекъснато да се наблюдава от алармения контролер и да се докладват следните съобщения за повреда (като минимум):
    - повреда в главното захранване;
    - повреда в зарядно устройство;
    - повреда в батерия;
    - изтощена батерия.
  - захранването трябва да съдържа резервна батерия, която да поддържа непрекъснато електрозахранване в случай на отпадане на главното електрозахранване, за продължителност не по-малко от 8 [h];
  - батерията трябва да бъде акумулаторна, от „гел“ тип, запечатана и без

необходимост от специално поддържане;

- захранването трябва да се състои от бързо зарядно устройство, което да позволява пълно зареждане на батерията за кратко време след възстановяване на захранването;
- след достигане на пълния капацитет на зареждане, зарядното устройство трябва да намалява зарядния ток, за да се избегне повреда на батерията;
- захранването към клавиатурите, външните входно / изходни модули и детекторите трябва да е доставено чрез силови линии в комуникационния кабел между алармения контролер и модулите, или от захранванията, монтирани в близост до входно / изходните модули.

13.3.3. Алармен контролер - I / O устройства

- аларменият контролер трябва да се състои от следните модули:
  - I / O платки (входове и изходи);
  - сериен интерфейсен модул.
- I / O модулът трябва да може да се монтира в алармения контролер или във външна кутия.
- комуникационният канал между алармения контролер и външните модули трябва да е двупосочен.
- комуникационният канал трябва да е под постоянен надзор. Линията между алармения контролер и външните модули трябва да е напълно контролирана и всеки опит за саботаж по линията трябва да подаде незабавна аларма в алармения контролер, която трябва незабавно да бъде препратена към Главната командно - контролна система чрез сървърите на системата за контрол на достъпа.
- каналът трябва да осигурява комуникация на минимално разстояние от 300 [m].
- комуникационният канал трябва да поддържа “BUS” топология.
- адресирането на външните модули, трябва да се извършва автоматично от алармения контролер, в съответствие с местоположението на устройството по линията, или чрез използването на конфигурационни превключватели на самите външни модули.
- комуникационният канал трябва да има възможност за самостоятелно възстановяване след повреда в комуникацията или прекъсване на електрозахранването.
- комуникацията трябва да се основава на протокол за проверяване през определен интервал.
- корпусите на външните модули трябва да са оборудвани с антисаботажни контакти. Отварянето на корпуса трябва да предизвиква аларма в алармения контролер, който изпраща доклад за съобщението към Главната командно - контролна система.

- входен модул:
  - 8 (осем) или 16 (шестнадесет) зонови разширители, които използват кабелна връзка;
  - наблюдаване на зони с норамално затворени контакти (NC), нормално отворени контакти (NO), с крайни резистори (EOL) или с двойни крайни резистори (DEOL);
  - превключваем допълнителен изход „захранване";
  - програмируемо време за „отговор" по линията: 10 [ms], 500 [ms], 1 [ms].
- изходен модул:
  - 4 (четири) модула с релета за високо напрежение (3 [A]);
  - 8 (осем) изходни модула с отворени колектори (70 [mA]);
  - всеки изход трябва да има възможност да се активира в резултат на редица събития, свързани със системата или съответен дял, зона или потребител.

13.3.4. Алармен контролер - комуникационни възможности

- аларменият контролер трябва да съдържа необходимите серийни интерфейси за комуникация с отдалечени входни / изходни модули, клавиатури и външни системи.
- аларменият контролер трябва да съдържа следните интерфейси:
  - сериен интерфейс за комуникация с външни I / O модули и клавиатури - минимум 2 (два) броя;
  - USB - интерфейс за комуникиране с локален компютър за конфигуриране на параметрите на алармения контролер, и качване / сваляне на информация - минимум 2 (два) броя;
  - LAN интерфейс - Ethernet 100 Base T.
- хардуерът и софтуерът на алармения контролер трябва да позволяват дистанционно качване / сваляне на софтуер.
- аларменият контролер трябва да съдържа диагностични светодиоди, които да показват комуникационния статус на контролера.
- аларменият контролер трябва да комуникира със сървъра на Главната командно - контролна система чрез специализирана комуникационна мрежа за предаване на данни.
- комутаторите, чрез които се осигурява връзка на елементите на алармената система срещу проникване с общата мрежа на системите за сигурност, трябва да бъдат разположени в защитени зони.

13.3.5. Алармен контролер - технически характеристики

зони	8 броя ÷ 128 броя
възможност за разширяване на зони (с кабели или безжично)	120 броя
модули на разширените зони (с кабели или безжично)	(1 x 8) + (7 x 16)
“BUS” линии за разширение	2 броя
дялове / зони	8 броя
групи в един дял	4 броя
потребителски кодове	99 броя
програмируеми изходи	6 броя ÷ 70 броя
контролирани, наблюдавани електрически захранвания	8 броя
клавиатури	16 броя
акаунти	12 броя
седмични времеви графици	32 броя
списък със събития	250 броя, разширяеми до 999 броя
IP комуникация	
мрежова съвместимост	Ethernet 10BaseT или 100BaseT TCP / IP протокол по LAN или WAN
сигурност	256bit AES криптиране, оторизация и защита срещу заместване и спам, шифровъчния ключ трябва да може да се сменя често
проверяване на връзката	конфигурируем пулс на всеки 10 [sec]

IP адрес	статичен или динамичен (DHCP)
IP ъплоуд / даунлоуд от множество канали	едновременно IP докладване и ъплоуд / даунлоуд от множество канали през TCP / IP при локална скорост от 9600 [bits / sec]
GSM / GPRS комуникация	
канали за доклади и комуникация	GSM гласов канал, GPRS или SMS
криптиране за GPRS и SMS доклади	128bit AES криптиране, оторизация и защита срещу заместване
SMS съобщения	да се създават от контролера при възникнване на събитие
e - mail съобщения	да се създават от контролера при възникнване на събитие
SMS операции	всички команди към панела трябва да бъдат потвърдени с обратен SMS
предплатени SIM карти	трябва да се поддържат
ъплоуд / даунлоуд	през GSM канал за данни
IP / GSM приемник	
входове	TCP / IP събития от мрежата GPRS събития от GSM / GPRS модула SMS събития от GSM / GPRS модула
изходи	ID контакти през COM портове
интегриране	XML протокол за интегриране с външни приложения
сигурност	съвременна оторизация и защита срещу заместване и спам
проверяване на връзката	конфигурируем пулс на всеки 10 [sec]

13.3.6. Детектори с двойна технология - комбинирани детектори (PIR + MW) за използване в промишлени обекти

вид	двойна технология, по два микровълнови и пасивни инфрачервени канали
покритие	25 [m]
ъгъл на наблюдение	90^0
защита от фактори на околната среда	минимум IP65
чувствителност	1,6 [^{0}C] / 0,6 [m] / 12 [m]
скорост на детектиране	0,3 [m / sec] ÷ 1,5 [m / sec]
продължителност на алармен цикъл	2 [sec]
алармен изход	NC сух контакт
антисаботажен контакт	задейства се при отстраняване на капака
LED индикатори (примерно)	червен - аларма, проблем жълт - MW, проблем зелен - PIR, проблем
захранване	9 [V DC] ÷ 16 [V DC]
защита срещу маскиране	активна IR
RFI	да не се генерира аларма при 30 [V / m]
работна температура	от -20 [^{0}C] до +55 [^{0}C]
относителна влажност	до 95 [% RH]

13.3.7. Магнитни контакти

Магнитните контакти трябва да са специално предназначени за използване със стоманени врати с приложения за промишени обекти.

Характеристики:

- специален дизайн за монтиране на метални врати;
- кабел със стандартна дължина 2 [m];
- тампер линия.

Технически спецификации:

тип	външен или вътрешен с максимална сигурност
тип на вратата за монтаж	метална
защита	вградена защита срещу магнитен поток екран с тройна оплетка тампер срещу магнитно поле
контакти	дизайн с висока сигурност
размер на пролуката (отвора)	от 1 / **8**” до 1 / 2”
работна температура	от -5 [^{0}C] до +50 [^{0}C]
относителна влажност	до 100 [% RH]

13.3.8. Активен инфрачервен детектор

Инфрачервените детектори трябва да са с далечен обсег за „вътрешно“ и „външно“ използване. Необходимо е да са лесни за инсталиране и поддържане.

Лъчите на инфрачервените детектори трябва да са подходящи за „външно“ използване, като поддържат обхват от 60 [m] на открито. Също така трябва да имат 2 (два) инфрачервени предавателя и приемника за намаляване на вероятността от аларми от малки животни, остатъци, носени от вятъра и падащи листа.

Лъчите трябва да задействат аларма, само когато и двата лъча са прекъснати едновременно.

Входните напрежения на сензора трябва да позволяват лесното му интегриране в нови или съществуващи системи.

Характеристики:

- защита от светкавици и пренапрежение;
- 99 % стабилност при блокиране на лъчи;

- регулируемо време за прекъсване на лъча;
- наобходимост от прекъсване на двата лъча за подаване на алармен сигнал;
- лесно инсталиране и настройване;
- закрита оптика, за да се предотврати навлизането на насекоми и прах;
- автоматично управление на усилването;
- дизайн против замръзване.

Обхвати:

- 120 [m] при „вътрешно“ използване и 60 [m] при „външно“ използзване;

Технически спецификации:

тип	пулсов инфрачервен фотоелектрически
обхват на детектиране	60 [m]
лъчи	двойни инфрачервени
време на прекъсване за генериране на аларма	50 [msec]
ъгъл на лъча	±90° хоризонтален, ±5° вертикален
елиминиране на фалшиви аларми	EMI / RFI защита лъч с висока мощност автоматично регулиране на усилването двойно синхронизирани лъчи избираеми честоти на лъчите защита срещу кондензация при мъгла
напрежение	12 [V DC] ÷ 28 [V DC]
продължителност на алармен цикъл	2 [sec]
защита от саботаж	антисаботажен контакт на предавателя и приемника
защита	срещу удари от светкавици и пикове в напрежението
работно напрежение	12 [V DC]
работна температура	от 5 [^{0}C] до 55 [^{0}C]

относителна влажност	до 95 [% RH]
инсталиране	монтиране на стена или стълб

13.3.9. Електрическо захранване - технически изисквания

конструкция	кутия от монолитен поликарбонат
околна среда	за монтиране на открито
работна температура	от -5 [^{0}C] до +70 [^{0}C]
относителна влажност	до 100 [% RH]
кутия	IP67 - прахо и водоустойчиво устойчиво на продължителен контакт със сол, бензин, дизелово гориво и масла устойчиво на кратък контакт с киселина, алкални разтвори, обезмасляващи агенти и хидравлични течности

13.3.10. Пасивен инфрачервен детектор

PIR - сензор	пасивни инфрачервени с два двойни PIR елемента
покритие	15 [m]
ъгъл на наблюдение	90^0
алармен изход	NC сух контакт
антисаботажен контакт	да се задейства при отстраняване на капака
защита срещу маскиране	активна IR
LED индикатори (примерно)	червен - аларма, проблем

	жълт - MW, проблем зелен - PIR, проблем
захранване	9 [V DC] ÷ 16 [V DC]
работна температура	от -20 [^{0}C] до +55 [^{0}C]
относителна влажност	до 95 [% RH]

13.3.11. Детектори с двойна технология - комбинирани детектори (PIR + MW) за монтиране на таван и използване в промишлени обекти

тип	двойна технология, 1 микровълнов и 3 пасивни инфрачервени канала
покритие	18 [m] диаметър
ъгъл на наблюдение	360^0
височина на монтиране	от 2,7 [m] до 8 [m]
алармен изход	NC сух контакт
антисаботажен контакт	да се задейства при отстраняване на капака
LED индикатори (примерно)	червен - аларма, проблем жълт - MW, проблем зелен - PIR, проблем
захранване	9 [V DC] ÷ 16 [V DC]
защита срещу маскиране	активна IR
RFI	да не се генерира аларма при 30 [V / m]
работна температура	от -20 [^{0}C] до +55 [^{0}C]
относителна влажност	до 95 [% RH]
възможност за изключване на микровълновия сензор в режим UNSET	

13.3.12. Акустичен детектор, регистриращ счупване на стъкло

тип	**действащ във всички посоки микрофон с микропроцесорно обработване на сигнала**
покритие	9 [m] радиус
алармен изход	NC сух контакт
антисаботажен контакт	**да се задейства при отстраняване на капака**
захранване	9 [V DC] ÷ 16 [V DC]
работна температура	от -20 [^{0}C] до +55 [^{0}C]
относителна влажност	до 95 [% RH]

Забележка: **Всеки участник трябва да представи подробна функционална блок - схема, илюстрираща работата на алармената системата срещу проникване, връзките между отделните модули и видовете крайни устройства, които смята да използва.**

14. Система за пожарна безопасност (СБП)

Съществуващата система за пожарна безопасност осигурява най-ранното възможно предупреждение, при възникване на пожар в голяма част от важните за електроцентралата зони, както и автоматичо пожарогасене в сектори, които са критични за работата на електроцентралата.

Съществуващите локални системи за пожарна безопасност са интегрирани от системата за централизиран мониторинг “WinGuard” на фирмата “ADVANCIS”, която е специално конфигурирана за използване в топлоелектрическата централа. Чрез нея сигналите за пожарна опасност се предават до локалното звено на ПБЗН.

Съществуващата централизирана система за мониторинг на системите за пожарна безопасност трябва да се интегрира със системата за управление и контрол на сигурността и безопасността.

Системата за пожарна безопасност включва автоматични сензори за откриване на пожар (пожароизвестителна инсталация), както и електрически и механични елементи, които осъществяват ефективно пожарогасене (пожарогасителна инсталация).

Новоизградените системи за пожарна безопасност трябва да се интегрират в съществуващата система за централизиран мониторинг “WinGuard”.

14.1. Пожароизвестителна инсталация (ПИИ)

14.1.1. Адресируема управляваща централа

А. Управляващата централа трябва да осигури:

- своевременна, пълна и точна информация от включените периферни устройства за пожарното състояние на охранявания обект - на място и в отдалечен пункт за реагиране на специализирани звена, в случай на пожар;
- управлението на всички модули, които са включени в пожароизвестителната (и пожарогасителната - ако има такава) инсталации;
- функционално действията на оторизираните служебни лица, които пряко отговарят за пожарната безопасност на охранявания обект;
- подаването на сигнал към автоматичната система за публично оповестяване, така че тя да излъчи подходящото предварително записано съобщение за конкретната ситуация;
- подаването на алармени звуков и светлинен сигнал за хората, които се намират в зоната на евентуален пожар.

- необходимите промени в работата на инженерните системи на охранявания обект, в случай на пожар.

Б. Структура:

Управляващата централа трябва да има възможност за разширяване на управляваните кръгове и охраняваните зони на модулен принцип и да включва:

- централен микропроцесор;
- интерфейсни модули за свързване на детекторните кръгове;
- самостоятелен микропроцесорен модул за всяка обособена зона;
- електрозахранващи модули с универсален вход, които позволяват работа със захранващо напрежение от 110 [V AC] до 255 [V AC] / 50 [Hz] или 60 [Hz] и изход 24 [V DC];
- електрическо табло със стопяеми предпазители;
- мрежов интерфейс, позволяващ свързването на TCP / IP мрежа;
- операторски контролен модул за осигуряване управлението на пожароизвестителните (и пожарогасителните - ако има такива) инсталации, който включва:
  - операторски LCD дисплей - модул на течни кристали, с не по-малко от 240 x 64 точки;
  - 0 - 9 цифрова клавиатура;
  - клавиши с посока на плъзгане „нагоре“ и „надолу“;
  - функционални бутони;
- светодиоден сигнализатор с индикатор за състоянието на различни зони;
- светодиодни индикатори на лицевия панел, които позволяват бързо разпознаване на състоянието на системата;
- входно / изходни допълнителни платки;
- модул с релеен интерфейс - програмира се за различни приложения, включително за изпращане на сигнал за противопожарното състояние в охранявания обект, за отделните модули, противопожарните изходи и охранителните системи;
- базов софтуер за управление;
- алармен брояч;
- резервно захранване от акумулаторни батерии, което осигурява не по-малко от 72 [h] автономна работа на инсталациите.

В. Технически изисквания:

брой на кръговете	не по-малко от 4 кръга

дължина на кръга	не по-малко от 1000 [m]
брой на модулите в един кръг	не повече от 128 броя
клас на защитеност	не по-ниска от IP30
програмируеми алармени изходи	не по-малко от 4 броя
сериен интерфейс	не по-малко от един
захранващо напрежение	220 [V AC] / 50 [Hz]
работна температура	от 0 [^{o}C] до +40 [^{o}C]
относителна влажност на въздуха	до 80 % [% RH]
европейски стандарти	EN 54, част № 2 EN 54, част № 4 EN12094, част № 1

14.1.2. Адресируем димен пожароизвестител

захранващо напрежение	от 15 [V DC] до 32 [V DC]
работна температура	от -10 [^{0}C] до +70 [^{0}C]
относителна влажност на въздуха	до 93 %, без конденз
клас на защитеност	не по-ниска от IP40
европейски стандарти	EN 54, част № 5

14.1.3. Адресируем топлинен пожароизвестител

захранващо напрежение	от 15 [V DC] до 32 [V DC]
работна температура	от -10 [^{0}C] до +70 [^{0}C]
относителна влажност на въздуха	до 93 % [% RH]
клас на защитеност	не по-ниска от IP40

европейски стандарти	EN 54, част № 5

14.1.4. Изолатор

Модулът трябва да изолира линията - да контролира състоянието на линията и при установяване на късо съединение да изолира повредения участък, като същевременно позволява на останалата част от кръга да функционира нормално.

захранващо напрежение	от 15 [V DC] до 32 [V DC]
работна температура	от -10 [^{0}C] до +60 [^{0}C]
относителна влажност на въздуха	до 93 % [% RH]
клас на защитеност	не по-ниска от IP40
европейски стандарти	VdS G297029

14.1.5. Сирена

захранващо напрежение	от 18 [V DC] до 28 [V DC]
максимален ток	30 [mA]
работна температура	от -25 [^{0}C] до +70 [^{0}C]
изход	105 [dB]
клас на защитеност	не по-ниска от IP54
европейски стандарти	EN 54, част № 3

14.1.6. Монтажна основа

работна температура	от -30 [^{0}C] до +70 [^{0}C]

клас на защитеност	не по-ниска от IP40
европейски стандарти	EN 54

14.1.7. Ръчен пожароизвестител

Ръчният пожароизвестител трябва да е с вградени изолатори за късо съединение.

захранващо напрежение	от 15 [V DC] до 30 [V DC]
работна температура	от -10 [^{0}C] до +60 [^{0}C]
относителна влажност на въздуха	до 93 % [% RH]
клас на защитеност	не по-ниска от IP42
европейски стандарти	VdS G 202035

14.1.8. Сензорен кабел

Сензорният кабел трябва да има регулируем праг на реагиране.

захранващо напрежение	от 10 [V DC] до 30 [V DC]
работна температура	от -20 [^{0}C] до +50 [^{0}C]
клас на защитеност	не по-ниска от IP65
европейски стандарти	EN 54, част № 5

14.1.9. Специализиран адресируем топлинен пожароизвестител

Специализираният адресируем топлинен пожароизвестител трябва да следи абсолютната стойност на температурата и да отчита скоростта на нейното нарастване.

захранващо напрежение	от 15 [V DC] до 32 [V DC]
работна температура	от 0 [^{0}C] до +50 [^{0}C]
клас на защитеност	не по-ниска от IP65
европейски стандарти	VdS G 205107

14.1.10. Лъчев пожароизвестител

Лъчевите димни пожароизвестители трябва да се инсталират в зони с високи тавани. Те трябва да се състоят от 2 (две) части (приемник и предавател), които се инсталират само на стабилни повърхности.

захранващо напрежение	от 12 [V DC] до 28 [V DC]
работна температура	от -10 [^{0}C] до +50 [^{0}C]
относителна влажност на въздуха	до 93 % [% RH]
разстояние между приемника и предавателя	от 5 [m] до 100 [m]
клас на защитеност	не по-ниска от IP54
европейски стандарти	БДС EN № 54 / 12: 2002

14.2. Пожарогасителна инсталация (ПГИ)

А. Ефективност:

- освобождаване на газообразния пожарогасителен агент - след получаване на алармен сигнал и времезакъснение от 30 [sec];
- максимално време за освобождаване на газообразния пожарогасителен агент - не повече от 60 [sec];
- време за потушаване на евентуален пожар - не повече от 60 [sec];
- продължителност на задържането на газообразния пожарогасителен агент в помещението след потушаване на пожар - не по-малко от 10 [min];
- влияние върху съоръженията - да не предизвиква вторични къси съединения и да не разрушава намиращите се в зоната съоръжения;

- влияние върху хората;
  - да се разработи за използване в обикновенно необитаеми зони;
  - след освобождаване на газообразния пожарогасителен агент да се гарантира нормална видимост по евакуационните трасета;
  - газообразният пожарогасителен агент да има близка до нулевата токсичност;
- влияние върху околната среда - да не предизвиква изменения.

Б. Изисквания към газообразния пожарогасителен агент**:**

- процентно съдържание на газообразния пожарогасителен агент в зоната на гасене след изпускането на газа:
  - съдържание на въглероден двуокис - от 3 % до 5 %;
  - съдържание на кислород - от 10 % до 15 %.
- въздействие върху материалните ценности:
  - корозионен риск - нулев, или близък до нулевия;
  - да не предизвиква влошаване на изолацията на кабелите и другите използвани материали в кабелните полуетажи;
  - минимален риск от натрупване на статично електричество;
  - максимално допустим спад на температурата, който определя минимален риск от термичен шок (топлинен удар) - от 10 [^{0}C] до 20 [^{0}C];
  - да не се налага специално почистване на охраняваните помещения след освобождаването на газообразния пожарогасителен агент;
  - минимален риск от непълно потушаване или от повторно възпламеняване на огъня след приключване на пожарогасенето;
- влияние върху хората - безвреден;
- въздействие върху околната среда:
  - химичен състав - газова смес от вещества с естествен произход, които се съдържат в атмосферата;
  - нулев, или близък до нулата потенциал за глобално затопляне на климата на Земята;
  - нулев, или близък до нулата потенциал за разрушаване на озоновия слой в Земната стратосфера;
  - нулева, или близка до нулата продължителност на съществуване в атмосферата.

В. Сертификати, с които се удостоверява, че газообразният пожарогасителен агент е преминал необходимите:

- изпитания за потвърждаване на посочените по-горе технически възможности, характеристики и параметри;
- медицински изследвания с участието на хора, които доказват, че използването на избрания газообразен пожарогасителен агент не оказва

някакво неблагоприятно въздействие върху човешкия живот и здраве.

Г. Изисквания към детектиращата част:

- да е централизирана;
- аларменият сигнал за освобождаване на пожарогасителния агент да се дублира от 2 (два) детектора;
- управляващата централа да позволява настройване (задаване на параметри) и обслужване (тестване и анализ) в диалогов режим;
- да се осигури резервно електрическо захранване от акумулаторни батерии;
- да има възможност за предаване на информация до персонален компютър за централизиран мониторинг.

Д. Изисквания към структурата и функционирането:

- при задействане, преди освобождаване на газообразния пожарогасителен агент, да се подават предупредителен звуков и светлинен сигнал, с които да се информират хората в помещенията;
- да има възможности за „автоматично“ и „ръчно“ освобождаване на газообразния пожарогасителен агент;
- да позволява използване на „секционни клапани“;
- пожарогасителният агент да се съхранява в газообразно състояние в бутилки, с налягане между 195 [bar] и 200 [bar] при температура 15 [^{0}C];
- да се осигури допълнително количество пожарогасителен агент, съгласно действащите европейски сатандарти, компенсиращо загубите от течове в охраняваните помещения;
- да се осигури резервиране на необходимото количество газообразен пожарогасителен агент за повторно гасене;
- за елиминиране на опасността от свръхналягане в охраняваните помещения, да се предвиди инсталирането на клапи за декомпресия.

Е. Изисквания към изпълнението на инсталационните работи:

- инсталацията да заема минимална част от пода;
- техническото обслужване и подържането в изправност да е лесно и удобно за служебните лица;
- времето за привеждане в състояние на „готовност за използване“ да е минимално;
- разходите за инсталиране да са минимални;
- за ефективното използване на газообразния пожарогасителен агент, да се осигури оптимално разпределение (ако се налага физическо разделяне) на защитаваните обеми.

14.3. Централизирана система за мониторинг

Централизираната система за мониторинг трябва да притежава графичен потребителски интерфейс, който осигурява пълното представяне на състоянието на всички елементи от системата за пожарна безопасност върху система от графични екрани, за:

- наблюдение и реакция в реално време;
- получаване на алармени съобщения в реално време;
- съхраняване на дневник на събитията;
- създаване на системни доклади;
- използване на двуизмерни планове за определяне на местоположението на устройствата, подали сигнал за промяна на текущото им състояние;
- управление на действията на персонала при произшествия - събира информация за рутинни и извънредни събития от съществуващата система и предоставя инструкции, съгласно предварително планирани стандартни работни процедури;

А Структура на системата:

- системата за мониторинг трябва да:
  - е с модулна структура от „отворен“ тип;
  - позволява визуализиране на информацията и управление на събития, които постъпват от различните модули на локалните пожароизвестителни и пожарогасителни инсталации;
  - позволява добавяне на нови интерфейсни и функционални модули.
- мрежовата комуникация на системата за мониторинг:
  - да се осъществява чрез обединяване на работата на отделните инсталации и работни станции;
  - да позволява работните станции и отделните инсталации за пожарна безопасност да се свържат в LAN - мрежа, изградена на базата на Windows приложения;
  - да дава възможност връзката между работните станции да се реализира на основата на мрежова карта за всички операторски станции и съответното окабеляване;
  - да позволява използване на TCP / IP протокол за обмен на информацията;
  - да позволява взаимозаменяемост на работните станции;
- обхват на системата:
  - броят на пожароизвестителните и пожарогасителните инсталации, които подлежат на общо наблюдение да не е по-малък от тридесет;
  - да се използват отделни комуникационен и файл сървъри, за гарантиране

непрекъсната работа на системата.

Б. Функционални възможности на системата:

- събитията (аларми, повреди и други), които възникват в свързаните инсталации да предизвикват изпращането на съответни съобщения в системата за мониторинг;
- всички възникнали съобщения трябва да се съхраняват по реда на тяхното постъпване и да се изобразяват под формата на списък, от който може да се избират за по-нататъшно обработване;
- всички възникнали съобщения в системата за мониторинг, след тяхното обработване, да се съхраняват заедно със съпътстващата ги графична и текстова информация върху твърдия диск на използвания файл сървър за период - не по-малък от една година;
- операторът да може да обработва постъпващата информация на всяка една от инсталираните работни станции;
- да се предоставя на оператора разширена информация за отделните съобщения и той да се подпомага при вземането на необходимите решения в конкретните случаи;
- на всяко съобщение да се присвоява графична и текстова информация с инструкции към оператора за възможните реакции;
- необходимите действия, които трябва да предприеме операторът (отпечатване на документи, набиране на телефонни номера, изпращане на информация чрез SMS и т. н.), следва да може да се извършват при поискване напълно „автоматично“ или „ръчно“;
- да се осигури възможност по всяко време данните от архива да се преглеждат с помощта на различни менюта и филтри, които позволяват достъп до информация за съобщенията;
- да се предвиди и т. нар. функция „паркиране“ (ако обработването на полученото съобщение не може да се извърши незабавно, да има възможност за довършване на обработването му на по-късен етап);
- програмното осигуряване да позволява да се отпечатват различни справки (за определен период от време и други);
- състоянието и местоположението на отделните групи детектори или на единични детектори, както в охраняваните помещения, така и на територията на централата да се изобразява ясно с помощта на отделни графики;
- да се осигури възможност отделните действия да се извършват при желание чрез използване на графика или текст с интерактивни символи.
- системата за мониторинг трябва да поддържа работата на отделните инсталации дори и извън процеса на обработването на постъпващите

съобщения;

- всички действия на оператора (като например приемане и обработване на съобщения, получени през използвания интерфейс) трябва да се протоколират от системата;
- да се осигури възможност отделните протоколи да се показват с помощта на уточняващи менюта и да може да се обобщават в свободно дефинирани справки заедно със съответната информация от архива;
- да се осигури възможност за симулиране на различни събития в системата за мониторинг, с цел обучение на персонала;
- специализираният приложен софтуер за работа със системата да е разработен на български език по най-съвременните методи, като се използват популярни изразни средства, да е достъпен и лесен за експлоатиране („приятелски настроен“).

В. Достъп за работа със системата:

- при стартиране на системата първо трябва да се появява един точно определен „прост“ прозорец, чрез който съответният оператор следва да:
  - се регистрира, със свой собствен код;
  - получи информация за самата система;
  - излезе от системата.
- достъпът до останалите функции на системата трябва да се разрешава само след регистриране на потребителя.

Забележка: Всеки участник трябва да представи подробна функционална блок - схема, илюстрираща работата на системите за пожарна безопасност, връзките между отделните модули и видовете крайни устройства, които смята да използва.

15. Автоматичната система за публично оповестяване (АСПО) и интерком - система

15.1. Основни положения

Автоматичната система за публично оповестяване трябва да осъществява масово оповестяване чрез гласови съобщениия и акустично сигнализиране в случай на различни производствени аварии, както и за ранно оповестяване, в случай на природни и други бедствия.

Системата трябва да е в състояние да осигурява акустично покритие с необходимата разбираемост на работните площадки и в рамките на помещенията на територията на електроцентралата.

Интерком - системата трябва да се използва за комуникация между командния и контролен център и обезопасени съоръжения като портали, зони на критични активи и други места.

Интеркомът и автоматичната система за публично оповестяване трябва да се основават на IP технология чрез използване на специализираната мрежа за IP комуникация на интегрираната система за сигурност за предаване и приемане на сигнали.

При необходимост от оповестяване на открити площи и помещения с големи обеми, трябва да се използват аналогови високоговорители, свързани към аналогови усилватели. Предаването на сигналите трябва да се извършва чрез използването на енкодери.

Конфигурирането на системата и разпределението на устройствата трябва да се определи на етап проектиране.

Акустичната система за оповестяване трябва да осигурява оповестяване на:

- целия обект, или на онези негови части, където има работен персонал;
- столовете, магазините, местата за реагиране и други, където се събират хора;
- порталите, местата за временно изчакване за посетители, автомобили и други моторни превозни средства;
- административните сгради;
- работните помещения;
- други зони и помещения.

Системата трябва да се състои от:

- електрически усилватели с резервно захранване;
- устройство (модул) за възпроизвеждане на предварително записани гласови

съобщения;

- устройство (модул) за записване на излъчваните съобщения;
- мрежов терминален контролер и аудиосървър за автоматичната система за публично оповестяване и интеркома;
- звукови излъчватели (IP и аналогови): стенни, таванни, прожекторни, тип Хорна и групи от излъчватели тип Хорна за озвучаване на големи пространства;
- интерфейсно устройство (модул) за получаване на сигнал от системите за мониторинг;
- подстанция за IP сигурност / аварийна;
- оперативна конзола / IP главна станция за интерком и гласови съобщения.

15.2. Основни изисквания и функции

- VOIP - технология;
- предаване на сигнали - чрез специално разработена за нуждите на сигурността TCP / IP мрежа;
- брой на зоните, в които трябва да се чува озвучаването - 100 (сто);
- оборудване за излъчване на повече от 30 (тридесет) предварително записани съобщения;
- програми за възпроизвеждане, които работят едновременно: повече от 20 (двадесет) броя;
- поддържане на MP3 формат.

15.3. Технически изисквания към аудиосървъра

оперативна памет	128 [MB] SDRAM, 1 [MB] NVRAM
капацитет на абонати	минимум 552 интерком станции на всеки сървър
аналогови станции	минимум 6 на всяка картова линия
аналогови телефони	минимум 12 на всяка картова линия
заето време на разговори	60000 BHCA
IP телефони	минимум 552 IP телефони на всеки сървър
проверка на целостта	MD5 (RFC 1321)

IP приоритет	DiffServ, IPTOS
IP сигурност	SSH, HTTPS, firewall
SIP	RFC 3261, SIPINFO, RE - Invite, RFC 2833, RFC 4733
VoIP вътрешна мрежа	30 канала
VoIP външна мрежа	30 канала
ISDN магистрала	ISDNPRI (30 канала)
аналогова магистрала	FXO (4 & 8 канала)
GSM магистрала	четирибандов GSM
мониторинг и регистриране	SNMP trap, SNMPMIB, системен лог, Web, e - mail, SQ Lite
дистанционни автоматични софтуерни актуализации	уеб, автоматични актуализации на IP станции
вътрешен аудио формат	1-bit (18,5 [KHz])
аналогови станции	18,5 [KHz] аудио
основен аудио интерфейс	18,5 [KHz] аудио
VoIP аудио	HD гласово - G.722 (7 [KHz]), телефонно аудио - G.711 (3,4 [KHz])
отваряне на конферентен дуплекс	20 конферентни канала, максимум 20 участника
Push - to - talk (PTT) конферентен разговор	50 конферентни канала, неограничен брой участници, приоритетни функции
групово повикване	250 групи, неограничен брой участници, приоритетни функции
режими на разговор	отворен режим, режим на звънене, режим “заявка за обаждане”, приоритетни функции

аудиосъобщения	АСПО излъчване, автопридружител, гласови указания (врати, асансьори), гласов отговор за сигурността
съответствие	CE; FCC, Част 15

15.4. Технически изисквания към усилвателя

- монтиране в рак;
- номнална изходна мощност - в зависимост от акустичния проект за обекта, но не по-малко от 350 [W];
- изходи за озвучителни тела - 70 [V], 100 [V] и 4 - 16 [Ω];
- наличие на изходен съгласуващ трансформатор;
- балансиран линеен вход тип XLR и небалансиран 1 / 4” TRS телефонен жак линеен вход;
- балансиран линеен изход тип XLR, който осигурява подаване на сигнал към друг електрически усилвател;
- надеждна защита от прегряване, претоварване, удар и късо съединение;
- съотношение сигнал / шум: по-високо от 80 [dB];
- честотна реакция: 50 [Hz] - 16 [kHz], (+1 [dB],-3 [dB]);
- изкривяване: по-малко от 0,1 %, при 1 [kHz]; при 1 / 3 номинална мощност;
- захранване: мрежово 230 [V AC] / 50 [Hz] или резервирано DC 24 [V DC].

15.5. Технически изисквания към IP високоговорителя за тавана

- доставяне на CCOIP - критична комуникация през IP;
- самостоятелно адресируема.

монтиране	с куки
препоръчителни размери (диаметър x дълбочина)	237 [mm] x 133 [mm]
max. SPL / 1 [m]	94 [dB]
max. SPL / 1 [kHz] / 1 [m]	84 [dB]
ефективен честотен обхват	200 [Hz] ÷ 7000 [Hz] (G.722 Codec)
дисперсия (-6 [db]) 1 [kHz] / 4 [KHz]	140 [^{0}C] / 50 [^{0}C]

защита от фактори на околната среда	IP54
температурен диапазон	от 0 [^{0}C] до 50 [^{0}C]
захранване	захранване през Ethernet, IEEE 802.3 a - f, Class 0, локално захранване 19 [V DC] ÷ 27 [V DC], при незаетост 2 [W], максимално 8 [W]
конектори	2 x RJ45 (Ethernet) 10 / 100 Mbps, сменяеми терминали (аудио и IO)
дистанционно управление	3 цифрови входа, 1 релеен изход и един логически изход
IP протоколи	IPv4 - TCP - UDP - HTTPS - TFTP- RTP - RTCP - DHCP - SNMP - DiffServ - TOS
LAN - протоколи	Power over Ethernet (IEEE 802.3 a - f), VLAN(IEEE 802.1pq), мрежови контрол на достъпа (IEEE 802.1x), STP(IEEE 802.1d), RSTP(IEEE 802.1d - 2004)
аудиотехнологии	широколентова 200 [Hz] - 7 [KHz] (G.722) телефония 3,4 [KHz] (G.711) адаптивен трептящ филтър аудиоизход 10 [W] високоговорител с импеданс 8 [Ω]
управление и експлоатиране	HTTPS (Web конфигурация) DHCP и статичен IP дистанционни автоматични софтуерни актуализации и централизирано наблюдение
разширени функции	превключвател за управление на данни с двоен порт, който поддържа VLAN и контрола на достъп до мрежата
съответствие	CE; FCC, Част 15

15.6. Технически изисквания към високоговорителя на сирената

- доставяне на CCOIP - критична комуникация през IP;
- самостоятелно адресируема.

монтиране	със скоби
препоръчителни размери (височина x широчина x дълбочина)	144 [mm] x 186 [mm] x 207 [mm]
max. SPL / 1 [m]	104 [dB]
max. SPL / 1 [kHz] / 1 [m]	94 [dB]
ефективен честотен обхват	330 [Hz] ÷ 7000 [Hz] (G.722 Codec)
дисперсия (-6 [db]) 1 [kHz] / 4 [KHz]	140 [^{0}C] / 40 [^{0}C]
фактор на насочване	1,8
защита от фактори на околната среда	IP67
температурен диапазон	от -20 [^{0}C] до 50 [^{0}C]
захранване	захранване през Ethernet, IEEE 802.3 a - f, Class 0, локално захранване 19 [V DC] ÷ 27 [V DC], при незаетост 2 [W], максимално 8 [W]
конектори	2 x RJ45 (Ethernet) 10 / 100 Mbps, сменяеми терминали (аудио и IO)
дистанционно управление	3 цифрови входа, 1 релеен изход и един логически изход
IP протоколи	IPv4 - TCP - UDP - HTTPS - TFTP - RTP - RTCP - DHCP - SNMP - DiffServ - TOS
LAN - протоколи	Power over Ethernet (IEEE 802.3 a - f), VLAN (IEEE 802.1pq), мрежови контрол на достъпа (IEEE 802.1x), STP (IEEE 802.1d), RSTP (IEEE 802.1d - 2004)

аудиотехнологии	широколентова 200 [Hz] - 7 [KHz] (G.722) телефония 3,4 [KHz] (G.711) адаптивен трептящ филтър аудиоизход 10 [W] високоговорител с импеданс 8 [Ω]
управление и експлоатиране	HTTPS (Web конфигурация) DHCP и статичен IP дистанционни автоматични софтуерни актуализации и централизирано наблюдение
разширени функции	превключвател за управление на данни с двоен порт, който поддържа VLAN и контрола на достъп до мрежата
съответствие	CE; FCC, Част 15
максимален капацитет на превключване	30 [W] DC
максимално напрежение в релейните контакти	60 [V DC]
максимален ток през релейни контакти	1 [A] DC

15.7. Технически изисквания към аналоговия високоговорител за тавана

- изводи на захранване: за 100 [V] - 20 [W] ÷ 40 [W];
- изводи на захранване: за 70 [V] - 10 [W] ÷ 20 [W].

монтиране	с куки
препоръчителни размери (диаметър x дълбочина)	237 [mm] x 133 [mm]
max. SPL / 1 [m]	94 [dB]
max. SPL / 1 [kHz] / 1 [m]	89 [dB] ±3 [dB]
ефективен честотен обхват	80 [Hz] ÷ 20 [KHz]

защита от фактори на околната среда	IP54
температурен диапазон	от 0 [^{0}C] до 50 [^{0}C]

15.8. Технически изисквания към аналоговия високоговорител на сирената за стена

- изводи на захранване: за 100 [V] - 10 [W] ÷ 50 [W];
- изводи на захранване: за 70 [V] - 5 [W] ÷ 25 [W].

монтиране	със скоби
препоръчителни размери (височина x широчина x дълбочина)	360 [mm] x 255 [mm] x 315 [mm]
max. SPL / 1 [m]	116 [dB]
max. SPL / 1 [kHz] / 1 [m]	99 [dB] ±3 [dB]
ефективен честотен обхват	90 [Hz] - 20 [KHz]
защита от фактори на околната среда	IP66
температурен диапазон	от -20 [^{0}C] до 60 [^{0}C]

15.9. IP сигурност / подстанция за авариен интерком

- трябва да е пригодена за „външно“ монтиране на врати или критични места;
- корпус от неръждаема стомана с дебелина минимум 2 [mm];
- 3” говорител, устойчив на атмосферни влияния;
- защитен електрически микрофон;
- 1 / 2” LED с висок интензитет;
- голям бутон за повикване, тип „гъба“;
- работна температура: от -20 [^{0}C] до +60 [^{0}C];
- оборудвана с двоен IP порт за евентуално последователно свързване на IP станции или устройства;
- вграден уеб сървър за програмиране;
- широколентово аудио (7 [kHz]);
- сух релеен контакт за отваряне на вратата или контрол на светлинните ефекти, като стандартни функции;

- IP станцията трябва да използва усъвършенстван алгоритъм за обработване на сигнала, за да се идентифицира и филтрира повтарящия се фонов аудиосигнал (шум);
- станцията трябва да е монтирана в стоманена кутия.

15.10. IP главна работна станция

- трябва да се използва за офиси и контролни зали;
- станцията трябва да включва голям дисплей с висок контраст със задно осветяване, който позволява да се показва важна информация за връзките;
- станцията трябва да е оборудвана с 10 (десет) DAK ключа за достъп с едно докосване до станциите, групови разговори и т. н., както и до телефонната слушалка за поверителни разговори;
- станцията трябва да се свързва директно към IP мрежите и да разполага с вграден уеб сървър за лесно конфигуриране, мониторинг и дистанционно автоматично софтуерно актуализиране;
- IP станцията трябва да използва усъвършенстван алгоритъм за обработване на сигнала, за да се идентифицира и филтрира повтарящия се фонов аудиосигнал (шум). Функцията трябва да е интегрирана в цифровия сигнален процесор (DSP), вграден в IP станцията и да се регулира софтуерно от IP интегрирания уеб сървър в станцията;
- станцията трябва да осигури широколентово аудио;
- свързването трябва да е към PoE комутатор или PoE инжектор за захранване.

15.11. IP устройство за автоматичен тест и контрол на озвучителните тела

Устройството за тест на рупорни високоговорители трябва да е IP базирано, за да извършва дистанционен контрол на работоспособността на рупорните високоговорители, които работят на труднодостъпни места, подложени на атмосферни влияния, в системи с изисквания за висока и много висока надеждност и непрекъснато експлоатиране. Трябва да е инсталирано между усилвателя и озвучителните тела.

Принципът на работата му, представлява подаване на кратък (2 [sec] ÷ 3 [sec]) пакет синусоидален сигнал с честота 10 [kHz] и максимална мощност, която зависи от типа на високоговорителя. На всеки високоговорител поотделно се измерва тока в линията и се прави оценка на импеданса на рупорния високоговорител и звуковия трансформатор.

Микропроцесорният блок трябва да притежава софтуер, който да: очаква команда от блока за дистанционен контрол; извършва превключване на изходите към високоговорителите в блока за измерване на ток; превключва входа на мощния усилвател към синус - генератора; стартира подаването на пакета измервателен

сигнал; отчита измерения импеданс на линиите към високоговорителите; подава информация към блока за дистанционен контрол; подава информация към панела за ръчен и визуален контрол. Микропроцесорният блок трябва да позволява извършване на измерване и след подаване на команда от панела за ръчен и визуален контрол. Трябва да притежава вход за връзка с компютър и протокол RS232.

брой дистрибутирани и тествани линии	8
входове:	
мощен усилвател	240 [W], max. 100 [V]
оповестяване	0 [dB] балансиран / небалансиран
сигнал тест	0 [dB] балансиран / небалансиран
тест	релеен
симулация	релеен
цифрови входове	като допълнителна възможност (по желание)
аналогови изходи:	
високоговорители	
статус на линиите	
индикация	
контрол	
сервизни входове и изходи за настройване	
тест : тип	

Забележка: **Всеки участник трябва да представи подробна функционална блок - схема, илюстрираща работата на системата за публично оповестяване, връзките между отделните модули и видовете крайни устройства, които смята да използва.**

16. Комуникационна инфраструктура / мрежа

16.1. Основни положения

Трябва да се изгради нова специализирана комуникационна система / мрежа за използване на интегрираната система за защита, безопасност и охрана.
Мрежата трябва да се основава на фиброоптична инфраструктура, която да свързва Главния команден и контролен център с всички локални комуникационни възли и разклонения, които трябва да се изградят и инсталират на различни места в електроцентралата.
Мрежата трябва да съдържа основни комутатори в контролния център и вторични комутатори за крайните устройства, разположени на различни места в електроцентралата.
Основните комутатори трябва да са "layer 3" превключватели, а вторичните трябва да са "layer 2" комутатори.
Комутатори трябва да се свържат в пръстен чрез оптичен кабел.
Точната архитектура на мрежата трябва да се определи на етапа на проектиране.
При определянето на дизайна на мрежата, особено на вида и капацитета на оптичните кабели, трябва да се вземе предвид необходимото разширяване на интегрираната система за сигурност и безопасност през следващия период, за да се гарантира изпълнението на всички етапи от препоръчаното цялостно решение за сигурността.

16.2. Тенически изисквания към превключвателя

16.2.1. Превключватели от „трети“ слой

- комутаторите трябва да са произвеени от Cisco, Juniper или еквивалентно;
- превключване от „третия“ слой (IP адрес);
- приложения за управление на комутаторите:
  - сериен кабел за директна връзка;
  - управление чрез браузър;
  - специално приложение за управление;
- трябва да поддържа минимум 16 броя VLAN's (виртуални мрежи);
- управлението на комутаторите трябва да е защитено с парола;
- надеждност на „третия“ слой: VRRP (Virtual Router Redundancy Protocol);
- възможност за специфично конфигуриране на всеки порт: например - 100 [Mb] пълен дуплекс;
- минимум 4 SFP модула за всеки комутатор;
- 2 (два) 10 [Gbit] порта;

- трябва да поддържа мултикаст IGMP (Internet Group Management Protocol) V2;
- „трети“ слой QoS (Quality of Service);
- минимум 8 порта трябва да поддържат POE +;
- работна температура: от -10 [^{0}C] до +50 [^{0}C].

16.2.1. Превключватели от „втори“ слой

- комутаторите трябва да са произведени от Cisco, Juniper или еквивалентно;
- превключване от „втория“ слой (MAC адрес);
- приложения за управление на комутаторите:
  - сериен кабел за директна връзка;
  - управление чрез браузер;
  - специално приложение за управление.
- управлението на комутаторите трябва да е защитено с парола;
- възможност за специфично конфигуриране на всеки порт: например - 100 [Mb] пълен дуплекс;
- минимум 4 SFP модула за всеки комутатор;
- 4 (четири) 1 [Gbit] порта;
- трябва да поддържа мултикаст IGMP (Internet Group Management Protocol) V2;
- „втори“ слой QoS (Quality of Service);
- минимум половината от портовете трябва да поддържат POE +;
- работна температура: от -10 [^{0}C] до +50 [^{0}C].

17. Главна командно - контролна система (ГККС)

17.1. Основни положения

17.1.1. Преглед

Главната командно - контролна система за сигурност трябва да осигурява интегрирано командване, контрол и комуникации, да обединява човешките и компютърните ресурси за физическо управление на информацията за сигурност. Системата трябва да се проектира така, че да осигури мониторинг, контрол и управление на всички технически системи за сигурност и взаимодействие на служителите, ангажирани в областта на сигурността, безопасността и свързаните с тях дейности в централата - като цяло или в дадена зона.

Главната командно - контролна система трябва да предлага добре построен, лесен за употреба графичен интерфейс, както за операторите, така и за мениджърите, който да позволи на организационно - структурното звено, отговарящо за сигурността да намали времето си за реагиране, да подобри своята ефективност и да опазва служителите и имуществото на централата.

Главната командно - контролна система трябва да има модулна, йерархична структура, която е в състояние да интегрира, както нови, така и наследени (предварително инсталирани) системи за сигурност и сензори на физическо равнище (от конфигурационно и логическо равнище до равнището на ситуационна осведоменост и управление).

17.1.2. Архитектура на системата

Главната командно - контролна система трябва да се разработи чрез използването на съвременни високотехнологични средства и да съчетава широка гама от технологии и интерфейси.

Главната командно - контролна система трябва да има отворена, модулна, йерархична архитектура и да използва софтуерни и хардуерни технологии, които позволяват бързо интегриране на новите и съществуващите сензори, които вече са инсталирани на обекта.

17.1.3. Допълнителни функции

Главната командно - контролна система трябва да разполага със следните допълнителни функции:

- да осъществява пълно интегриране на текстова, картова и видеоинформация;

- всеки запис да е свързан с място, събитие и време;
- високотехнологичен „интуитивен“ графичен потребителски интерфейс (GUI);
- да позволява „влачене“ и „пускане“ на всички данни на всеки един от мониторите;
- да поддръжа многофункционален „тъч скрийн“ монитор;
- да ползва мощна 3D географска информационна система;
- да използва вградено изчисляване на зрителната линия за камерите, разположени по периметъра;
- да има вградена възможност за показване на видеообраз от дадена камера и зрителното й поле върху 3D картата на обекта;
- да разполага с вградена възможност за ясно визуализиране на настъпилите във времето алармени събития (заедно с видообраз от зоната на събитието), за да се анализират причините за появата им и за превенция;
- да има вградени мощни приложения за „интелигентен“ видеоанализ, оптимизирани за външна употреба;
- да осъществява лесно интегриране на новите камери и сензори;
- да има гъвкав интерфейс, който да позволи лесен импорт / експорт на външни данни;
- да е мащабируема и гъвкава.

17.1.4. Конфигуриране на сървъра

Главната командно - контролна система трябва да функционира в съответствие с конфигурирането клиент - сървър, позволяващо инсталиране на неограничен брой мрежови станции, които са необходими, за да се разпредели натоварването между различните оператори по време на алармени събития.

За постигане на максимална надеждност Главната командно - контролна система трябва да използва резервен сървър, който да може да функционира и като основен.

Главната командно - контролна система трябва да работи под операционна система Windows, като използва една от стандартните бази данни на Microsoft: Access или SQL.

Главната командно - контролна система трябва да включва съвременни решения за управление на правата на нейните потребители, които позволяват прецизно дефиниране на упълномощаването за достъп на основа на съответната роля на служебните лица в централата.

Системата трябва да се основава на съвременни модули, които позволяват разпределението на информация чрез жични и безжични комуникации до някои или всички от изброените по-долу:

- отдалечени работни станции за управление;
- бизнес - мрежата в обекта (например: да докладва за пристигане / заминаване на персонала);
- патрулни превозни средства, които са оборудвани с мобилни компютри;
- преносими Windows смартфони и други мобилни устройства, за показване на текстови съобщения, цифрови карти, видеообрази, списъци с процедури и други.

17.2. Основни системни функции

Главната командно - контролна система трябва да има следните възможности:

1. **Управление** - да осигури единна система за управление на ежедневните операции, инциденти и кризи.

2. **Идентифициране** - бързо и точно да определя единичните заплахи и съвкупността от аларми и да локализира проблемите, като предоставя пълна информация за ситуацията.

3. **Реагиране** - в реално време да предоставя на персонала оптимизирани процедури и директиви за действия при различни видове ситуации, като осигурява синхронизиран поглед и реакция.

4. **Комуникация** - да осигури един канал с много изображения, които може да се видят от много места. В реално време да изпраща съобщения, доклади и директиви за всички лица в рамките на централата, като им дава възможност да реагират бързо и правилно.

Тези възможности трябва да се постигнат чрез интегрирано управление на следните компоненти на Главната командно - контролна система:

- интерфейс за връзка със системи за сигурност;
- интерфейс за връзка с жични / безжични комуникационни системи;
- показване на информация от системите за сигурност (видеоизображения, аларми и други);
- графичен потребителски интерфейс (GUI) с карта на зоната в обекта от географската информационна система;
- връзки между различни операторски и управленски равнища.

17.2.1. Главна командно - контролна система - таблица на взаимните връзки

Таблицата по-долу показва как Главната командно - контролна система трябва да взаимодейства с отделните системи, които са интегрирани в нея. Системата следва да се програмира така, че да приспособява екраните и функциите, към изискванията на различните потребители.

техническа система за сигурност	изобразяване в Главната командно - контролна система	автоматична или операторска реакция
сигурност на портали / врати	състояние на портал / врата (отворена / затворена) на картата;	отваряне на вратата / портала за оторизирано превозно средство / лице (с идентификационна карта)
	насилване на портал / врата > показва се като алармен сигнал на картата	затваряне на всички врати / портали докато трае аларменото събитие
система за контрол на достъпа	насилване на врата или оставена отворена врата > показва се като алармен сигнал върху плана на сградата	изглед от камера към вратата, подала алармения сигнал отваряне на вратата за оторизирано лице докладване за пристигане / заминаване на персонала към бизнес - мрежата на обекта
затворена система за телевизионно видеонаблюдение	рутинни - автоматични обиколки или ръчен избор алармено събитие - изглед на вратата или частта от оградата, подали алармения сигнал	операторът наблюдава алармата на монитора
видеосистема за откриване на движение	изглед от камера, открила подозрително движение	автоматично / операторско сигнализиране към патрулно превозно средство по безжичен път

система от мрежови видеорекордери	преглед на записано събитие, видяно от камера, избрана от картата	операторът / мениджър разследва записаните събития систематично
алармена система за периметърна охрана	откриване на проникване - поглед на частта от оградата от най-близката камера, се показва на картата като алармен монитор	операторът оглежда частта от оградата, подала аларма автоматично / операторско сигнализиране към патрулно превозно средство по безжичен път
алармена система	пожарна аларма / аларма от паник бутон зоната на алармата се показва на картата поглед на зоната от най-близката камера	излъчва се предварително записано съобщение за опасност от системата за публично оповестяване аварийните изходи се отварят от системата за контрол на достъпа изпраща се текстово съобщение до мениджърите на обекта
система за проследяване	отбелязване на лица, които напускат разрешена зона / влизат в забранена зона	изпраща се текстово съобщение до охранителните патрули / мениджърите на обекта
рутинни дейности в обекта	рутинни - автоматични обиколки или ръчен избор GPS локализиране на патрулите работен график на охранителните патрули	мениджър: разследване на записани минали системни събития оператор: проверяване на състоянието на системата и сензорите
дейности, свързани с алармени събития	зоната на алармата се показва на картата на картата се показват алармените точки, място - положението на превозни - те средства списък с аварийни процедури	заключват се порталите и вратите алармени съобщения / звуци чрез системата за публично оповестяване автоматични обаждания към местните полицейски сили и

		аварийни служби

17.2.2. Графичен потребителски интерфейс (GUI)

Главната командно - контролна система трябва да има модулен, лесен за конфигуриране графичен потребителски интерфейс, като основен компонент на командния и контролен интерфейс.

Графичният потребителски интерфейс трябва да включва следните елементи на дисплея:

- географска информационна система - интерактивна карта на обекта;
- възможност на дисплея да показва 3D карта на обекта;
- възпроизвеждане на видео (на живо или на запис) от камерите на системата за телевизионно видеонаблюдение;
- единичен или разделен на части видеоекран;
- доклади за състоянието на системата и алармените сензори;
- инструкции и протоколи за управление на сигурността.

17.2.3. Дисплеи

Главната командно - контролна система трябва да показва графичните елементи на различни екрани, в съответствие с променящите се оперативни изисквания:

- на операторските екрани на работните станции;
- на големи екрани, монтирани на стена - главно за картата на обекта и видеоклипове;
- на видеостени, изградени от масиви от големи екрани - за гледане на дадени зони на екран с размер на стена;
- на екрани на мениджъри - предимно за отделни елементи за управление на сигурността;
- като използва „тъч скрийн“, позволяващ всички елементи да се избират / преместят и т. н. чрез докосване или с мишка;
- възможност за едновременно показване на видеообрази, системни данни и карта на един екран или на отделни екрани.

17.2.4. Географска информационна система - интерактивна карта

Интерактивната карта на обекта трябва да се основава на приложенията за географски карти от географската информационна система, които са независими от конкретни фирми - производители. Системата трябва да позволява бързо и свободно движение и приближаване / отдалечаване на изображения от картата. Географската информационна система трябва да включва следните

характеристики:

17.2.4.1. Интерактивна карта - създаване и формат

Главната командно - контролна система трябва да разполага с:

- възможности за използване на изготвени карти, въздушни снимки, векторни карти и допълнителни карти в различни мащаби (1 : 50000, 1 : 400000 или конкретно определен мащаб за обекта);
- възможност за активиране от дисплея на изображения на строителните планове на сградите, показващи входните врати, евакуационните пътища и други;
- възможност за показване на 3D карти;
- възможност главната системна карта да е едновременно разделена на 4 (четири) различни карти:
  - независими - които да предоставят възможност за свободно движение по всяка карта поотделно и едновременно управление на 4 (четири) различни места (или зони от един обект) с различни мащаби, от един екран;
  - синхронизирани - които да предоставят възможност за синхронизиране на картите за едно място (локация), избрано от администратора;
- възможност за създаване и поставяне на маркировка или икони на картата, включително: маркиране на области (обхват на стрелба, враждебни райони и т. н.), маркиране на маршрути (маршрут на патрулните превозни средства, пешеходни патрули, неасфалтирани пътища и други), отбелязване на местни забележителности (антена, портал, и т. н.);
- възможност да показва всички системни сигнали, незабавно и в реално време, с координати и подходящо маркиране (икона);
- всички картови елементи, икони и т. н. да може да се преместват / избират чрез докосване на екрана или с мишка.

17.2.4.2. Интерактивна карта - слоеве

Главната командно - контролна система трябва да има възможност да използва няколко картови слоя, които да се показват отделно, за да се запази картата ясна и подредена, без да се губят най-важните детайли, например:

- слоят от картата с аварийните маршрути за евакуиране, трябва да се появява само по време на пожарна аларма;
- системните слоеве показват трасетата на електрическите кабели, позициите на сензорите, местоположенията на патрулиращите превозни средства и т. н.;
- административни слоеве;

- слой с маршрутите на движение.

17.2.4.3. Интерактивна карта - интегриране на алармената система срещу проникване за периметърна охрана

Линията на оградата на алармената система срещу проникване за периметърна защита трябва да се обозначи на картата от географската информационна система. На картата трябва да се появяват като алармени икони всички аларми от системата (в зависимост от типа система), включително:

- единично докосване на оградата;
- продължително докосване на оградата;
- срязване на оградата;
- изключване на електрическото захранване;
- нарушаване на целостта на сензорните контролери;
- спад на напрежението при сензорите.

От екрана на графичния потребителски интерфейс, операторът трябва да може да включва / изключва сензори и да извършва преглед на историята на сензора.

Електронната ограда трябва да се свърже чрез затворена верига като „кръг“, така че да се осигури възможност за комуникация, дори ако някоя от комуникационните линии до сензорите на оградата е срязана. Главната командно - контролна система трябва да е в състояние да контролира неограничен брой сензори и контролери за оградата.

17.2.4.4. Интерактивна карта - интегриране на CCTV

Главната командно - контролна система трябва да е в състояние да:

- показва местоположението, ориентирането и зрителното поле на всяка фиксирана или PTZ камера;
- избира всяка камера директно от картата, за да прегледа видеопотока от нея (на отделен екран или на насложен върху картата екран);
- избира, ориентира, посочва и приближава / отдалечава образа от всяка PTZ камера директно от картата;
- избира точка или обект от картата, за да се покаже видеокартина от / за тази точка от най-близката камера;
- анализира зрителната линия на всички средства за наблюдение (например камера или радар) между две произволни точки на картата;
- симулира възможност за промяна на височината на инсталиране на камерата и да показва ефекта от предложената промяна, спрямо зрителните линии.

17.2.4.5. Интерактивна карта - интегриране на патрулните коли

Главната командно - контролна система трябва да е в състояние да следи патрулните автомобили, снабдени с GPS мобилни компютри или с преносими таблети в района на обекта, като следва да:

- получава и показва в реално време местоположението на всяко превозно средство с точност до 5 [m];
- избира скоростта на актуализиране на местоположението на превозното средство (на всеки няколко секунди, минути и т. н.);
- ограничава района на патрулиране на дадено превозно средство чрез маркиране на желания патрул на картата. Ако превозното средство напусне маркираната област, системата трябва да предупреждава оператора или ръководителя по сигурността;
- контролира и прави разбор за придвижването на дадено патрулно превозно средство по маршрута за патрулиране и показва изчисленото закъснение за целия маршрут с течение на времето;
- предава аларми от обекта към патрулните автомобили - или към патрулното превозно средство, което е най-близо до събитието или към всички патрулни превозни средства. Видеоизображенията и мястото на събитието трябва да може да се изпратят на екраните на мобилните компютри.

17.2.4.6. Интерактивна карта - възможности за охраняваните зони

Главната командно - контролна система трябва да се конфигурира за координиране на сигурността в рамките на централата. В тази връзка, тя трябва да:

- позволява намиране на мястото на извънредната ситуация на картата по местоположението (координатите), посочено по телефона от обаждащия се;
- дава възможност на оператора да сигнализира на най-близкия патрул, като се използва системната база данни с мобилни телефонни номера;
- дава възможност на оператора да помага в координирането на силите за реагиране, като използва информация от затворената система за телевизионно видеонаблюдение.

Когато се използва т. нар. „DTM” карта (включително с данни за надморската височина на терена), Главната командно - контролна система трябва да може да:

- измери реалното земно / пътно разстояние между две точки, взето от техните позиции на картата;
- измери височината, на която и да е точка на картата.

17.2.5. Възможности за видеоуправление

В допълнение към вече описаните възможности за видеоконтрол, Главната командно - контролна система трябва да предоставя възможност за лесен достъп до записаните архиви на системата зателевизионно видеонаблюдение и за търсене на видеозаписи, свързани с конкретни камери, места, дати, часове, сензори или събития, подбрани от системните списъци или от интерактивната карта.

Главната командно - контролна система трябва да разполага с интерфейси за камери от водещите световни производители.

Главната командно - контролна система трябва да е в състояние да изготви интерфейс за всякакъв вид камера, когато се предостави подходящ протокол за обмяна на данни за нея.

17.2.6. Администриране и доклади

Главната командно - контролна система трябва да предоставя специфични потребителски права на мениджърите и да се даде възможност за:

- показване на екран на протоколи и процедури за справяне с рутинни задачи или алармени събития, които да подтикват операторите да изпълняват задачите си в правилния ред;
- създаване на системни доклади, според типа на събитието, времето, мястото и т. н.;
- генериране на отчети, за да се следи времето за реагиране на служителите по сигурността и операторите;
- контрол на периодичните проверки и тестове за поддържане на системата в изправност.

17.3. Мултимедия

17.3.1. Основни положения

Мултимедията следва да се изгради като тази част, която контролира взаимодействието между основния екран (мониторите) и командната и контролна система в командния и контролен център.

Потребителят трябва да може да избира чрез мултимедиен контролер картината на екраните / мониторите и оформлението на представяната информация.

Контролерът трябва да е свързан с видеоматрица и с потребителите на командната и контролна система.

17.3.2. Матрица и мултимедиен контролер с „тъч скрийн“

- контролерът трябва да може да наблюдава и контролира всички мултимедийни устройства (високоговорители, монитори, екрани и

други);
- „тъч скрийн“ - овете трябва да може да се се използват чрез мултимедиен контролер.

17.3.3. Мултимедиен контролер

- монтиране и инсталиране в ракове - максимум 4U;
- минимум 6 (шест) RS232 / RS485;
- минимум 8 (осем) IR;
- минимум 8 (осем) I / O сухи контакта;
- минимум 1 (един) RJ45.

17.3.4. „Тъч скрийн“

- трябва да е възможно използването на таблети (lenovo, iPad, Samsung Galaxy или друг);
- минимален размер 7”;
- минимална разрешаваща способност: 800 x 480;
- 16 [Bit] цвят;
- комуникация с контролера: RS232 или TCP / IP или IR.

17.3.5. Видеоматрица с 12 (дванадесет) входа и 8 (осем) изхода

Матрицата трябва да превключва между входовете и изходите (12 x 8):

- 12 (дванадесет) видеовхода DVI / HDMI;
- 8 (осем) видеоизхода DVI / HDMI;
- монтиране и инсталиране в ракове максимум 3U;
- 12 (дванадесет) аудиовхода;
- 8 (осем) аудиоизхода;
- комуникация на данни: RS232 / 485.

17.4. Контролер за клавиатура, мишка и монитор

Компютрите на работните станции трябва да се инсталират в помещението, в което е разположено цялото централно оборудване за Главната командно - контролна система. Операторите и супервайзорите трябва да работят само с контролерите за клавиатура, мишка и монитор.

Контролерът за клавиатура, мишка и монитор трябва да се инсталира за свързване между компютрите и операторските бюра в командната зала. Контролерът за клавиатура, мишка и монитор трябва да включва 2 (две) активни устройства - предавател и приемник. Връзката между устройствата трябва да се извършва чрез кабели CAT 5e:

- конектор между устройствата (предавател и приемник);
- USB - конектор за мишка и клавиатура;
- 2 (два) входа за монитор (DVI или VGA) за всяко устройство;
- конектор RJ45.

17.5. Превключвател за клавиатура, мишка и монитор

- 1 (един) изход за монитор VGA / DVI;
- 1 (един) USB - изход за мишка и клавиатура (може да бъде 1 (един) USB за мишка и 1 (един) USB за клавиатура);
- 1 (един) стереоизход;
- 4 (четири) входа за монитор VGA / DVI;
- 4 (четири) USB - входа за мишка и клавиатура;
- 4 (четири) стереовхода;
- разрешаваща способност: до 1920 x 1200.

17.6. Сплитер за монитори

- разрешаваща способност: до 1920 x 1200;
- 1 (един) вход за монитор (DVI / VGA);
- 2 (два) изхода за монитор (DVI / VGA).

17.7. Хардуер на системата

- сървърите, устройствата за съхраняване на информация и работните станции, инсталирани в контролната зала или на друго място (например портал) трябва да са от следните утвърдени производители - IBM, Dell, HP, LENOVO или друг производител;
- всички сървъри трябва да са оригинално произведени за инсталиране в 19” рак;
- всички устройствата за съхраняване на инофрмация (харддискове) трябва да са от професионален клас, подходящи за непрекъснат видеозапис;
- всички монитори трябва да са минимум 25” LCD или LED от водещи производители;
- дължината на диагоналите на екраните за монтиране на стена, трябва да са не по-малки от 50”;
- екраните трябва да са LCD или LED и също да са произведени от водещи производители.

17.8. Ракове с оборудване

В помещението с оборудването трябва да има до 5 (пет) 19” стандартни ракове за

оборудване с височина от 44U и дълбочина 100 [cm]. Материалът, от който са произведени раковете трябва да е от високоиздръжлива алуминиева сплав.

Всеки рак трябва да включва най-малко следните аксесоари:

- 19” тава за вентилатор, монтирана на върха на рака;
- задна врата - алуминиева;
- предна врата - стъклена;
- вертикални и хоризонтални кабелни скари, монтирани за инсталиране на кабели;
- изходи към главната електрическа мрежа, монтирани на рака.

18. Изисквания към инфраструктурата и специализираните строително - монтажни дейности

18.1. Основни положения

В топлоелектрическата централа трябва да се изгради подходяща инфраструктура за подпомагане на решенията за сигурността, както и за да се реализират всички мерки и системи за сигурност, като част от решението за сигурността. Подобряването на инфраструктурата трябва да включва: определено строителство, организация на движението, осигуряване на електрическо захранване, комуникации, охранително осветление и безопасност.

Инфраструктурните системи трябва да се проектират и конструират според националните стандарти, закони и разпоредби, като се вземат предвид следните аспекти:

- модулност (необходима е за поетапното осъществяване);
- дублиране на източниците на електрическо захранване и на маршрутите за доставяне;
- гъвкавост, необходима за свързването на различните системи;
- резерви за бъдещо разширение;
- ремонтопригодност.

18.2. Нов Главен командно - контролен център

18.2.1. Основни положения

Трябва да се изгради нов Главен командно - контролен център за сигурност, който да се състои от:

- оперативна / контролна зала - да включва 2 (две) работни места за оператори и 1 (едно) за супервайзор;
- помещение с оборудването на системите за сигурност и комуникация / сървърно помещение - да включва до 5 (пет) 19” рака с оборудване и централен UPS;
- помещение за резервни части и ремонт - да включва работно място за софтуерно и хардуерно поддържане и подходящо място за резервни части;
- строително - монтажни работи - необходимо е новият контролен център да се проектира и изгради като масивна монолитна стоманобетонна постройка със скелетно - гредова система, едноетажна без сутерен. Пълнежните стени трябва да са надеждно свързани към основната

носеща конструкция. При проектирането да се спазват действащите към момента на реализирането строителни норми и правила.

18.2.2. Изисквания

Центърът трябва да се организира така, че да се съобрази с изискванията на Главната командно - контролна система, включително строителни, електрически и други изисквания по отношение на инфраструктурата.

Очакваната площ, необходима за Главния командно - контролен център е не по-малко от 60 [m^2].

Изискванията по отношение на инфраструктурата трябва да включват:

- повдигнат под;
- работно място за супервайзор;
- окачен / звукоизолиран таван;
- звукоизолирани вътрешни стени;
- кабелни канали и кабелни скари за различни цели;
- подходящи охранителни врати;
- пожароизвестителна инсталация;
- пожарогасителна инсталация;
- електрически инсталации, включително UPS и архивираща система;
- осветление, включително аварийно;
- електрическо и електронно заземяване;
- отоплителна, вентилационна и климатична инсталация с пълно дублиране;
- комуникации;
- специализирано оборудване и бюра за операторите.

18.3. Концепция / типов дизайн - електричество

18.3.1. Основни положения

Захранването за всички системи за сигурност и осветление трябва да е 220 ± 5 % [V AC] / 50 [Hz] монофазно, или 400 ± 5 % [V AC] / 50 [Hz] трифазно, или 12 [V DC] - 24 [V DC] постоянно токово.

Проектът на системата за електрозахранване трябва да е съобразен с българските закони, правила и стандарти. Когато няма местни стандарти, се прилагат международни или европейски стандарти.

Строително - монтажни работи - Трябва да се изградят кабелни трасета - подземни и надземни. Подземните трябва да включват ревизионни шахти, надеждно изградени от бетонови елементи и / или монолитен стоманобетон, покрити със стоманобетонни капаци. Между шахтите трябва да се развие тръбна мрежа , като в

местата на преминаване под пътища следва да се оформят защитни „кожуси” - от стоманобетон, или друг вид допълнителна защита.

Надземните трасета трябва да включват кабелни скари със защитни капаци и отделно преминаващи по съществуващите конструкции „обсадни” тръби от подходящи материали.

Необходимо е да се предвидят трасета за: специализирана комуникационна система, периметърно и районно (охранително) осветление, електрозахранване на системите за сигурност и за резерв. Кабелите на специализираната комуникационна система трябва да са отделени от силовите, захранващи кабели. Пред всяка кабелна касета да се предвиди кабелна шахта със стандартен размер 60 [cm] x 90 [цm] или 120 [cm] x 90 [cm] - в зависиомост от натовареността на трасето. Връзката между кабелните шахти да се осъществи с PVC тръби ϕ50 / 1.8 [mm]; ϕ75 / 2.2 [mm] и ϕ110 / 3.2 [mm] SN4. Връзката към уличните стълбове да се изпълни с гъвкави гофрирани тръби тип kopoflex или други с размер ϕ40 / 32 [mm] или ϕ50 / 41 [mm].

За да се намалят финансовите средства и за безопасност и гъвкавост - кабелите за районното и периметърното охранително осветление трябва да са петжилни, а там където позволява и трижилни, със сечение, съгласно проектните изчисления.

Необходимо е да се предвиди разпределително електрическо табло за районното и периметърното осветление, което да захранва кабелните касети. Нужно е да се предвидят кабелни касети, които да управляват определен брой улични осветителни тела в определена зона. За всяка касета трябва да се предвиди програмируем контролер с календар и часовник, на които може да се задават различни програми или да се използва програма, съобразена с изгрева или залеза на слънцето (например контролер Schneider Electric IC Astro). Зонирането и вида на осветлението да се съгласува с ръководството на „ТЕЦ Марица Изток 2“ ЕАД.

Осветителните стълбове трябва да са горещопоцинковани, с вградена в тях заключваема вратичка и предпазител 1P 6A за монтиране върху фундамент. Всеки 5 (пети), краен или разклонителен стълб трябва да се заземи като съпротивлението на заземлението не трябва да превишава нормативните изисквания. Външните улични осветителни тела трябва да са със светодиодни източници, като тяхната мощност и светлинен поток трябва да се определят от проектанта съгласно светотехническите норми и изчисления. Използването на светодиодни осветителни тела е икономически обосновано поради следните причини:

- използването на захранващи кабели с по-малко сечение заради значително по-малката електрическа мощност на светодиодните лампи в сравнение със стандартните металхалогенни лампи;
- бъдещи по-малки сметки за плащане на електрическа енергия.

Светодиодните осветителни тела да се свържат чрез редуване на фазите.

Цялото оборудване трябва да е напълно сертифицирано за употреба в Република България и трябва да отговаря на всички най-нови изисквания и разпоредби.

При изготвянето на подходящия конкретен работен проект, трябва да се оценят внимателно следните аспекти:

- безопасност;
- надеждност;
- гъвкавост;
- ремонтопригодност;
- ефективност на разходите;
- енергийна ефективност;
- отговорност за опазването на околната среда.

Електрическото захранване на техническите системи за защита, безопасност и охрана трябва да се основава на съществуващата електрическа мрежа. Захранването, особено за Главния командно - контролен център за сигурност, следва да се извърши от електрическата мрежа на централата, като се предвиди пълно резервиране от няколко източника, включително и от съществуващия дизелов генератор за резервно захранване.

18.3.2. Електрическо захранване

- електрическата мрежа трябва да се състои от специални електрически разпределителни табла, напълно отделени от всички други съществуващи разпределителни табла;
- разпределителните табла трябва да се захранват от най-близката точка с резервирано електрическо захранване и е за предпочитане да се инсталират в защитени места, обикновено в помещенията на главните електрически табла и в помещенията на охранителите, в близост до охраняваните врати;
- всеки портал в централата или критичен обект трябва да се захранва от отделно електрическо табло, което да захранва всички системи за сигурност на това място. Точното местоположение и техническите параметри на електрическите табла следва да се определят по време на етапа на проектиране.

18.3.3. Захранващи кабели

- захранващите кабели трябва да са годни за използване според местните правила и стандартите на електроцентралата;
- за външни инсталации, където няма кабелни скари или канали, кабелите може да се положат под земята в подходящи тръби;

- подземните трасета може да се използват и за полагане на комуникационни оптични кабели, които може да са разположени до силови кабели;
- за вътрешни инсталации, или когато има кабелни канали, кабелите може да се полагат до съществуващите кабели;
- в Главния командно - контролен център, кабелите трябва да се положат в кабелни скари в повдигнатия под или над окачения таван;
- изчисленията на сеченията на кабелите трябва да съответстват на местните правила и на инструкциите на производителя на кабела;
- при изчисляването на захранващия кабел трябва да се вземат под внимание следните параметри:
  - пад на напрежението;
  - De - рейтинг фактор на стайната температура;
  - De - рейтинг фактор за групирането на кабели;
  - увеличено напрежение, вследствие използването на различно оборудване.

18.4. Заземяване

Заземителната система трябва да се проектира в съответствие с местните правила и норми.

Всеки елемент от системите за сигурност трябва да е заземен и свързан към същото заземяване, към което е свързано и разпределителното, електрическо табло, захранващо съответния елемент.

Строително - монтажни работи - необходимо е изграждането на заземителна инсталация от поцинковани заземителни колове и шини.

18.5. Мълниезащита

Мълниезащитата трябва да са изгради съгласно местните правила и норми.

Всички стълбове, на които има инсталирани камери трябва да са предпазени с комплект за мълниезащита.

Строително - монтажни работи - необходимо е изграждането на мълниезащита от поцинковани колове и шини.

18.6. Непрекъснато електрическо захранване (UPS)

- всяко разпределително електрическо табло на системата за сигурност трябва да е свързано с локален UPS, за да се осигури необходимото електричество захранване на системите за сигурност;
- UPS - ът трябва да се свърже към LAN - мрежата, използвана от системите за сигурност чрез RJ45 конектор, за да се контролира и получава информация за грешки и повреди.

Капацитетът на UPS - а трябва да се изчисли като част от изчислението на електрическия баланс по време на етапа на детайлното проектиране. UPS - ът трябва да може да поддържа непрекъснато електрозахранване за не по-малко от 30 [min]. За командния контролен център резервното време трбва да е не по-малко от 1 [h].

Максималното натоварване на UPS - а не трябва да надвишава 85 % (осемдесет и пет на сто) от номиналната му мощност.

UPS - ът трябва да е в състояние да работи при натоварване от 125 % (сто двадесет и пет на сто).

Към веригата на UPS - а трябва да се прибави и външен ръчен байпас (за поддръжане).

18.7. Стълбове за камери

- повечето от външните камери трябва да се монтират върху метални стълбове;
- точното местоположение и височината на стълбовете трябва да се определят по време на етапа на детайното проектиране в съответствие с изискванията на всяко място;
- стандартната височина на стълбовете трябва да е 4 [m] ÷ 8 [m], в зависимост от местоположението и целта.
- стълбовете трябва да се инсталират на подходящи основи и съответно разклонителните кутии трябва да се монтират на или интегрират във всеки стълб.
- на всеки стълб трябва да се монтира специална разпределителна кутия за свързване на камерите към комуникационните кабели и електрическото захранване.
- всички захранващи и комуникационни кабели, трябва да са монтирани във вътрешността на стълбовете. Забранено е външно инсталиране на кабели.
- в стълбовете трябва да се направят специални отвори със запечатани капаци за направляване на кабели през стълбовете към или от кутията. В допълнение трябва да се направят 3 (три) кръгли отвора с диаметър 40 [mm] с щуцери в горната част на стълба за прокарване на кабелите между стълба и камерите.
- стълбовете трябва да са горещо поцинковани, с не по-малко от 300 [g / m^2], съгласно EN ISO - 1461;
- формата и структурата на стълбовете следва да се адаптират, за да отговорят на изискванията за натоварване и деформация;
- максимално допустимата деформация на стълбовете на мястото, където е

монтирана камерата не трябва да е повече от $0,2^0$, при динамична скорост на вятъра - 80 [km / h];

- стълбовете не трябва да се повреждат дори и при екстремни условия на околната среда;
- всички стълбове трябва да са оборудвани с шипове против катерене, тип "пола".

Строително - монтажни работи - всички стълбове трябва да се проектират и изпълнят върху стоманобетонни основи с подходящи размери и дълбочина на фундиране - предвид статичните и динамичните сили и натоварвания, влияещи на стълбовете (включително условията на околната среда), в съответствие с местните действащи строителни правила и норми.

Когато не съществуват местни стандарти, трябва да се използват признати международни такива.

При изчисленията и оразмеряването, трябва да се отчете и възможността за монтаж на повече от една камера на стълб.

Необходимо е заземление на стълбовете.

18.8. Подсилване на прозорците

Стъклопакетите на външните прозорци на 3 (трите) главни портала (главен портал, северен портал и товарен портал) трябва да се заменят с бронирани стъкла тип BR3, в съответствие с EN 1063.

В допълнение - на всички прозорци на охранителните контролно - пропускателни пункктове трябва да се монтират поцинковани стоманени пръти, с дебелина не по-малко от 12 [mm].

Строително - монтажни работи - необходимо е оформянето на защитни решетки от пръти, образуващи карета с размери не по-големи от 15 [cm] x15 [cm]. Защитните решетки трябва да са надеждно анкерирани по контура си към прозоречните рамки.

18.9. Благоустройство на обекта и разни строителни работи

18.9.1. Отстраняване на растителност и изравняване на земната повърхност

За да се осигури чисто зрително поле на камерите за телевизионно видеонаблюдение и да се минимализират лъжливите аларми от алармената система срещу проникване за периметърна защита, цялата периферия на централата трябва да се почисти от растителност и трябва да се подравни земната повърхност.

Строително - монтажни работи - необходимо е трайно да се премахнат (изкоренят) съществуващите дървета и храсти и да се предприемат мерки, които възпрепятстват бързото им възстановяване.

По гореописания начин трябва да се третира ивицата с широчина най-малко **2** [ш] от всяка страна на оградата.

18.9.2. Пътно - строителни дейности

За да се изпълнят всички определени мерки за сигурност, и най-вече тези на порталите трябва да се извърши благоустройството на обекта и съответните необходими пътно - строителните дейности.

Строително - монтажни работи - около новообособените портали (и около съществуващите портали) трябва да се изгради трайна пътна настилка с подходящи подложни пластове, осигуряващи трафик на движение с ниска и средна интензивност. Основите на всички монтирани защитни съоръжения трябва да се изпълнят като отделни стоманобетонни, фундирани минимум на 80 [cm] под терена. При тяхното проектиране трябва да се спазят действащите към момента на реализирането им строителни норми и правила.

При проектирането на строително - монтажните дейности, свързани с мерките за сигурност трябва да се предвиди изграждането на елементи за организация на движението и безопасност на трафика.

18.9.3. Разни инфраструктурни дейности

Съществуващите портали трябва да се ремонтират, като се изпълнят всички строителни, електрически, комуникационни, вентилационни и други изисквания, необходими за пълното инсталиране и експлоатиране на мерките за сигурност.

Строително - монтажни работи - необходимо е извършването на ремонтно - възстановителни работи по съществуващите сгради на порталите. като за „северния“ и „товарния“ портали се проектират и изградят метални платформи за инспектиране на товарите. При проектирането им следва да се спазят действащите към момента на реализирането строителни норми и правила. За изграждането на нови портали - да се предвидят основи от монолитен стоманобетон за сградите и съоръженията.

19. Изисквания за осигуряване на безопасни условия за работа

При извършване на отделните видове работа трябва да се спазват изискванията на „Правилника за безопасност на труда при строително - монтажни работи“ и „Правилника за безопасност на труда при експлоатирането на електрически уредби и съоръжения“.

Всички инсталатори да се инструктират по техниката на безопасност и да им се направи инструктаж за безопасна работа непосредствено на работното място.

Преди започване на работа, инсталаторите да се снабдят с лични предпазни средства, съобразени с наличните на обекта предупредителни и указателни табели.

Работите за изпълнение на поръчката да започнат с писмено нареждане на наблюдаващото от страна на Възложителя лице, съгласно Правилника за техническа безопасност.

Всички съоръжения да са заземени. Забранява се работата с неизправни инструменти, както и дейности, които противоречат на изискванията за охрана и безопасност на труда.

Обслужването на електрооборудването да се извършва само след изключване на устройството от електрическата мрежа.

Забранява се извършването на огневи работи и на други дейности, свързани с отделянето на топлина в близост до съоръженията.

Забранява се извършването на монтажни и на други работи от неправоспособни лица.

20. Изисквания към строително - монтажните работи

Изпълнителят трябва да вземе всички необходими мерки за опазване на околната среда (на строителните площадки и на временните си строителни бази), както и за недопускане на щети и отрицателно въздействие върху хора и имущество, вследствие на замърсяване, лъчения, шум и други вредни последици от работите по предмета на поръчката.

Изпълнителят трябва да ограничи действията на своя персонал и механизация до границите от предоставените му от Възложителя строителни площадки и прилежащи терени.

Изпълнителят трябва да осигури охрана на строежите от кражби и повреди до завършването и приемането на ремонтите и строително - монтежните работи по тях.

По време на строително - монтажните работи Изпълнителят трябва да премахва всички ненужни препятствия, отпадъци, излишни материали и механизация от строителните площадки, като ги складира на определени и съгласувани с Възложителя места или се освободи от тях.

При демонтажните и строително - монтажните работи на строежите трябва да се спазват изискванията на Наредба № 2 / 31.07.2003 година за въвеждане в експлоатация на строежите в Република България и минимални гаранционни срокове са изпълнени строителни и монтежни работи, съоръжения и строителни обекти и на Наредба № 3 / 31.07.2003 година за съставяне на актове и протоколи по време на строителството.

Всички работници на обектите, включително и тези работещи с механизация, трябва да се инструктират за условията и изискванията за изпълнение на строително - монтажните работи в непосредствена близост до постоянно действащи на 24 - часов режим съоръжения в експлоатация за производство на електрическа енергия, както и за условията и изискванията за изпълнение на Правилника за безопсността на труда и експлоатацията на електрическите уредби и съоръжения и други.

След приключване на строителството Изпълнителят е длъжен да възстанови строителните площадки в първоначалния им вид - да изтегли цялата си механизация и невложените матариали и да остави площадките чисти от отпадъци

При формиране на офертната си цена, участниците следва да предвидят съответните средства за:

- осигуряване на нормативно определените безопасни условия на труд на

строителната площадка по време на изграждането на строежите, както и за охрана на изпълняваните от тях работи, до завършването и приемането им.

- възстановяването на строителната площадка в първоначалния и / или проектен вид и освобождаването й от отпадъци.
- Необходимите за изграждането на строежите помощни видове строително - монтажните работи, като:
  - вътрешни и външни подпорни и / или работни скелета и площадки;
  - товарене, разтоварване (ръчно и / или механизирано), както и хоризонтално и вертикално пренасяне на материали, оборудване, строителни отпадъци и други подобни;
  - текущо и окончателно почистване на обекта от строителни отпадъци.

Приемането на работите следва да се извърши с подписването на Протокол за установяване на годността за ползване на строежа (Протокол - образец 16) и издаване на Разрешение за ползване за всеки от етапите на строежите.

Всички възникнали въпроси по време на строителството ще се решават в присъствието на упълномощени представители на „ТЕЦ Марица Изток 2“ ЕАД.

При строителството Изпълнителят трябва да спазва изискванията на всички Правила за изпълнение и приемане на строително - монтажните работи, засягащи строежите, както и фирмените технологии на фирмите - доставчици.

21. Съдържание на инженеринга

А. Предпроектно проучване.

Б. Проектиране.

В. Извършване на строително - монтажни дейности.

Г. Доставяне на технически средства и софтуер.

Д. Монтиране, инсталиране и тестване.

Е. Въвеждане в експлоатация.

Ж. Обучение на специалистите за работа със системите.

З. Изработване на съпровождаща документация.

И. Гаранционно поддържане.

Й. Следгаранционно поддържане.