SocioBrains
ISSN 2367-5721, JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
INTERNATIONAL SCIENTIFIC REFEREED ONLINE JOURNAL WITH IMPACT FACTOR
ISSUE 63, NOVEMBER 2019

DEVELOPMENT OF INTEGRATED SYSTEMS FOR SECURITY AND COMMUNICATION

Abstract: Integrated security and communication systems enable them to be managed and observed states of all security systems in an organization from one platform (single control center). In this way, organizations have the opportunity to maintain an integrated system quality management, the environment, Information Security health and safety at work of its employees.
In this regard, the report examines new developments in construction Integrated Security System and communication.

Author information:

Donika Dimanova
Assoc. Prof. PhD in Management of Security Systems
Department at Konstantin Preslavky University of Shumen
✉ d.dimanova@shu.com
Bulgaria

Zdravko Kuzmanov
Chief assist. prof. PhD in Management of Security Systems
Department at Konstantin Preslavky University of Shumen
✉ z.kuzmanov@shu.bg
Bulgaria

Keywords:
integrated systems, security, communication, development.

Въведение

Интегрираните системи за сигурност и комуникация дават възможност да бъдат управлявани и наблюдавани състоянията на всички системи за сигурност в една организация от една платформа (единен контролен център). По такъв начин организациите имат възможност да поддържат интегрирана система за управление на качеството, околната среда, сигурността на информацията, здравето и безопасността при работа на своите служители.

В тази връзка доклада разглежда новостите при изграждането на интегрирана система за сигурност и комуникация.

Изложение

Голяма част от българските фирми решават проблемите със сигурността „на парче". Много от ръководителите организират „фирмената сигурност" чрез електронни системи за сигурност и жива охрана или договор с фирма за охрана с технически средства. Мениджърите не си дават сметка, че това са само елементи на сигурността и предназначението им е да сигнализират нарушения, когато не са сработили другите системи. Масово се подценяват другите видове заплахи, от където идват и повечето проблеми свързани със сигурността.

Концепцията за сигурност трябва да дава отговор на въпросите:

- Какъв е типа на обектът на защита?
- От кои рискови трябва да се защитава обектът?
- и Как трябва да се защитава обектът?

В тази връзка „сигурността на организацията“ може да се разглежда като комплекс от взаимно свързани мероприятия и дейности, отнасящи се до физическата и информационната защита на хора и обекти, финансовите средства, материалната и интелектуална собственост, имащи задачата да осигурят устойчиво функциониране и създаване на условия за продължителна и успешна работа. Поради това е необходимо да се извършва цялостен инженеринг на системите за сигурност, а именно: алармени системи, видеонаблюдение, контрол на достъп, пожароизвестяване и пожарогасене, системи за детекция на вода и газ, системи за периметрова охрана, комуникационни системи, системи за централизирана охрана и предаване на данни, системи против кражби, специализирани системи за банкова сигурност и оповестяване, структурно кабелни системи и други [2].

Концепцията за сигурност трябва да е насочена към съвременните изисквания за сигурност, висококачествени продукти от най-ново поколение и решения базирани на последните достижения на техническите системи за сигурност.

Системна интеграция. Системната интеграция е бъдещето на системите за сигурност. Интеграцията е ключ към успеха т. к. спестява време и разходи, извършва се лесен контрол и мониторинг, и съществува възможност за бъдещо надграждане на системите. За изграждане на интегрирана система за сигурност са необходими [6]:

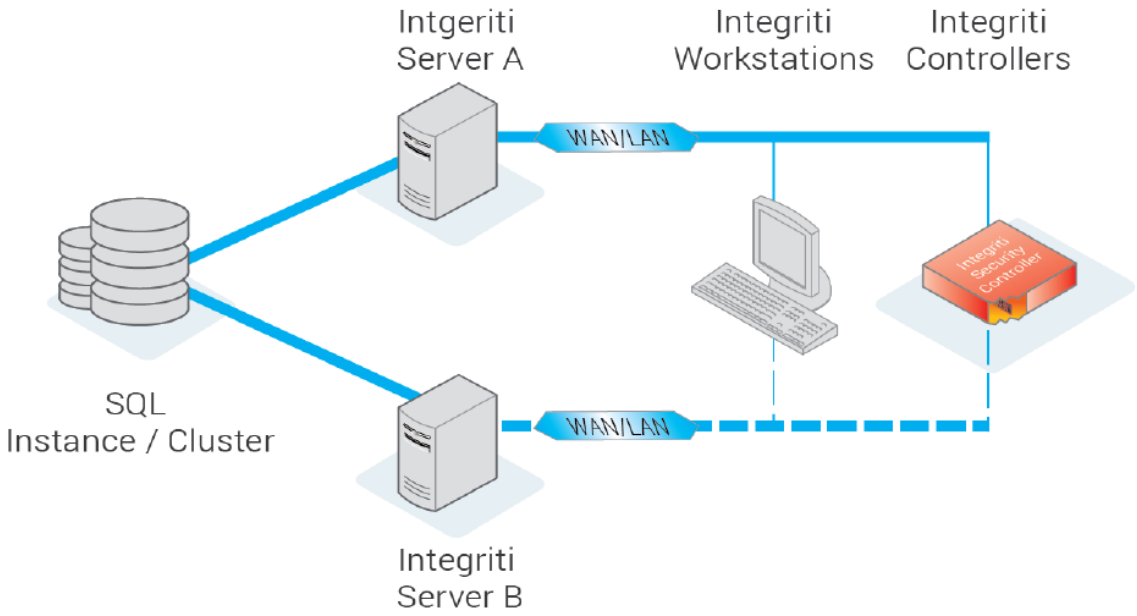
- Решения за сигурност, изградени от различни технически продукти и системи;
- Мощен софтуер, обединяващ системите с общ контрол и мониторинг;
- Работа с различни компании за ефективна интеграция с външни системи.

С развитието на технологиите през последните години непрекъснато се търсят нови инженерни решения, осигуряващи максимална степен на защита. Като новости при интегрирани системи за сигурност Inner Range могат да се отбележат:

- Използването на паралелен сървър за по-голяма сигурност;
- Векторно базираните схематични карти;
- Интеграция за разпознаване на регистрационни номера;
- Подобрения в модула за преглед на събития (Review).

Използването на паралелен сървър цели резервиране на системата. Ако по някаква причина хардуерът на сървъра се повреди или се нуждае от профилактика (или друга причина), сайтовете да не претърпят загуба на връзка на контролерите и клиентите. Когато има опасност от отпадане на критични системи на ниво корпоративен бизнес, това може да нанесе огромни загуби за организацията. В повечето случаи се практикува сървърите Integriti да бъдат инсталирани на различни физически места, за да бъдат минимизирани възможните проблеми свързани, например с прекъсване на мрежата, захранването, природни бедствия и др.

На фигура 1 е показано използването на втори Integriti сървър, който работи паралелно с първия и предполага висока надеждност на приложения слой. Като решение за редуване на корпоративно ниво, високото наличие на слой на приложение на Integriti може да се комбинира с SQL Clustering, за да се премахне още една точка на неуспех. Съкращаването на приложенията SQL и Integriti осигурява най-доброто време за работа [1].



Фиг. 1. Висока надеждност на приложения слой

Има развитие и във векторно базирани схематични карти, етажни планове и икони на сгради и населени места. Схематичните карти могат да бъдат мащабирани и увеличени без загуба на качество или пикселиране, което позволява да се използва една детайлна и подробна карта. Възможностите на динамичната видимост и мащабиране позволяват иконите и етикетите да се показват само при определени нива на мащабиране. Това позволява създаването на карта без примеси, където приоритетните елементи се виждат по всяко време и размера на иконите е с нормална големина.

Интеграцията за разпознаване на регистрационни номера се извършва чрез заснемане от система за видеонаблюдение, което дава пълномощия на потребителите за осигуряване на достъп до паркинги, входни врати и др. След като потребителя поднесе стандартна безконтактна карта към четец от системата, идентичността на виртуалната карта се обработва. Регистрационния номер на автомобила е зададен на потребителя като идентификационен номер, което дава възможност на системата за видеонаблюдение да изпрати аларми за разпознаване на регистрационните номера и заснемане от камерата за видеонаблюдение. Така се използват усъвършенстваните функции за контрол на достъпа, като например, контрол на зоната, потвърждение за достъп от страна на оператора, разрешения на потребителите и условен достъп до регистрационните номера на превозните средства.

Модула за преглед на събития (Review) претърпява значителен брой промени. Целта е да се подобри цялостната ефективност на търсенето, филтрирането и изготвянето на отчети от операторите.

Както вече бе споменато, системната интеграция е бъдещето на системите за сигурност. Като предимства на системната интеграция за потребителите могат да се отчете управлението и мониторинга на всички системи в един софтуер и разширена функционалност.

Възможностите за допълнителни функции на интегрираните системи за сигурност и комуникации свързани с изкуствения интелект са [4]:

- Филтриране на аларми – спестява се време и ресурс чрез намаляване на фалшивите аларми чрез филтриране на фактори на смущения като промени в осветлението или движението на животни в зрителното поле. Благодарение на Deep Learning алгоритмите се подобрява

ефективността на наблюдение и детекция на незаконно проникване в охраняваният обект. Само действителните заплахи задействат аларми, което прави мерките за сигурност значително по-ефективни и предотвратява нежеланото влизане.

- Бизнес анализ – броене на посетители, Heatmap анализ, анализ на човекопотока;
- Достъп на хора и автомобили – извършва се лицево разпознаване и разпознаване на регистрационни номера на автомобили. За да се увеличи точността на разпознаване се инсталира LPR камера по правилния начин за заснемане на квалифицирани изображения;
- Управление на трафика – извършва се разпознаване на номера, детекция на посока, анализ на трафик, преброяване.

На фигура 2 е показана продуктовата гама на HikVision, които са технологичния гигант в областта на сигурността.

Фиг. 2. Продуктова гама на HikVision

През месец Октомври 2019 г. фирма Сектрон и технологичния гигант HIKVISION представиха в България най-новите интелигентни продукти за детекция и класификация на обекти, броене на хора, последните новости при системите за контрол на достъп, цветни изображения при видеонаблюдение в пълен мрак, термовизионни решения за видеонаблюдение и периметрова охрана, новото поколение модулни IP и двупроводни видео домофонни системи.

В демонстрираната интегрирана система за сигурност и комуникация бяха интегрирани следните продукти:

- Камери за разпознаване на автомобилни номера – достъп за автомобили чрез разпознаване на номера;
- Устройства за WI-FI/LAN звънец – повикване и преглед на видео през мобилен телефон (фиг. 3);
- Видео домофони – модулна IP система (фиг. 4);
- Контрол на достъпа – IP терминали, четци, видео интерком (фиг. 5);
- PTZ/PanoVu камери – панорамна камера 32MP/PTZ камера с Auto Tracking функция и бърз фокус (фиг. 6);
- 360° панорамна камера - 12MP, интелигентни функции, Heatmap (фиг. 7);

- TURBO HD технология – еволюция на аналоговата видеосистема, до 8MP, PoC, ColorVu, AcuSense, IoT PIR(фиг. 8);
- Терминал за лицево разпознаване (фиг. 9);
- Термовизионни камери с AI функции – решения за охрана на критична инфраструктура (фиг. 10);
- Серия Acusense с филтриране на аларми – класификация на обекти за минимизиране на фалшивите аларми (фиг. 12);
- Алармени продукти (фиг. 13);
- Софтуерна платформа HikCentral – централизиран алармен мениджмънт, видео център;
- Cloud платформа HikConnect – Push известяване, мобилен видео център.

Нововъведенията в домофонните системи са свързани с разширяване на функционалните им възможности, както следва: видео интерком функции, възможност за връзка (повикване) с други мониторни панели, дистанционно отваряне на врата, запис на гласови съобщения, автоматичен отговор и режим „Do not disturb“, микрофон и говорител, възможност за добавяне на IP камери, IR осветление за нощна работа, широкоъгълен обектив 120°, детекция на присъствие и автоматично заснемане, четец за карти за контрол на достъпа и слот за SD карта.

Фиг. 3. Устройства за WI-FI/LAN звънец

Фиг. 4. Видео домофони.

Фиг. 5. Контрол на достъпа - IP терминали, четци, видео интерком.

Фиг. 6. PTZ/PanoVu камери.

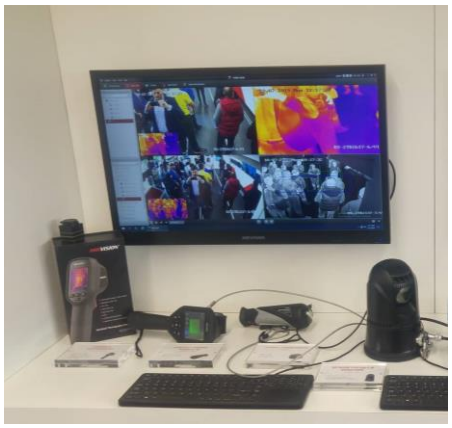
Фиг. 7. 360° панорамна камера.

Фиг. 8. TURBO HD.

Фиг. 9. Терминал за лицево разпознаване

TURBO HD технологията е базирана на революционната HD-TVI (High Definition Transport Video Interface) технология. Тя е нова технология, позволяваща пренос на видеосигнал с мегапикселова резолюция (720p/1080p) по стандартен коаксиален кабел на разстояние до 500 м. HD-TVI системите не изискват изграждането и конфигурирането на мрежова преносна среда, а използват традиционната схема на свързване с коаксиален кабел и BNC конектори между камерата и DVR устройството [4, 5]. Това дава възможност да се използват съществуващи коаксиални трасета, което е добро решение за надграждане на вече изградени аналогови системи. Като предимство на HD-TVI технологията може да отчете липсата на компресиране на сигнала в камерата, което позволява наблюдение с мегапикселова резолюция без закъснение и накъсване, и без сложно конфигуриране. Друг съществен момент е липсата на допълнителни мрежови устройства, сървъри и софтуер, което прави HD-TVI системата оптимално изгоден, надежден и опростен вариант за работа и преход към мегапикселово видеонаблюдение днес.

Термовизионните IP камери все повече навлизат в системите за сигурност и се използват за видеонаблюдение, периметрова охрана и детекция на пожари. Благодарение на Deep Learning алгоритъма, камерите поддържат детекция на пожар, пресичане на линия, навлизане/излизане в зона и температурна детекция (±8°C).



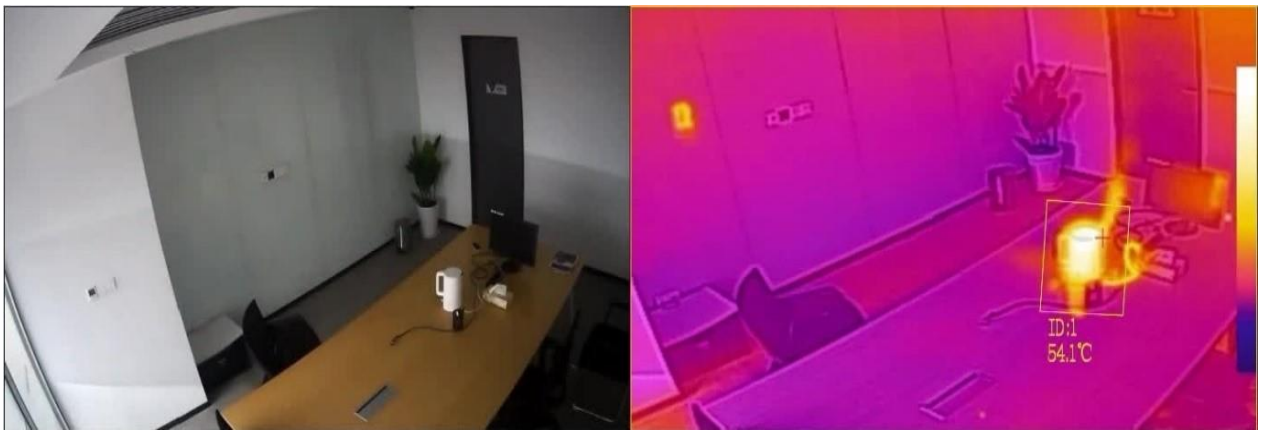
Фиг. 10. Термовизионни камери с AI функции и термални камери за видеонаблюдение.

Термалните IP камери са иновативни продукти и решения за видеонаблюдение. Те се използват и за целите на периметровата охрана и предотвратяването на пожари в критични инфраструктури като летища, железопътни линии, затвори, електроцентрали и т.н.

Новата куполна термокамера на Hikvision с Deep Learning алгоритъм предоставя подобрени възможности за откриване на пожар в закрити помещения, усъвършенствана аларма за температурна аномалия и визуално предупреждение. Предварителната алармена система помага незабавно да бъдат открити неочаквани събития и предпазва от загуба на собственост. Благодарение на тези възможности се намаляват рисковете от пожар и повреди.

Като предимства за използването на термалните камери могат да се отбележат [7, 3]:

- Оборудвани са с висококачествени хардуерни компоненти за обработка на изображенията, използвайки видима и инфрачервена светлина, или т.нар. „биспектърни изображения“;
- Може да заснеме причината за алармата и бързо да се провери ситуацията;
- Използват технологията за двуспектърно изображение, което създава визуализация на картина в картина и сливане на изображение;
- Камерите се наблюдава само по един канал, намалявайки честотната лента и опростявайки процедурата за предварителен преглед на живо, като се елиминира необходимостта да се превключва между термичния и оптичния канали;
- Камерите комбинират множество техники за обработка, за да създадат най-добрият резултат от термични и оптични изображения (фиг.11);
- Камерите използва „Температурна разлика еквивалентна на шума“ (NETD) по-малка от 40, т.е. колкото по-ниска е разликата в температурата, усетена от камерата, толкова по-малка е стойността и по-добро е изображението;
- Аларма за температурна аномалия – надеждно известяване за температурна аномалия, която ще задейства аларма, след като температурата надвиши границата, зададена от потребителя;
- Намаляване на фалшивите аларми. Това се осъществява благодарение на вградения графичен процесор (GPU) за подобряване ефективността на наблюдение и детекция на незаконно проникване в охраняваният обект. Технологията за интелигентен анализ на видео съдържание може да помогне за намаляване на фалшивите аларми чрез филтриране на фактори на смущения като промени в осветлението или движението на животни в зрителното поле. Само действителните заплахи задействат аларми, което прави мерките за сигурност значително по-ефективни и предотвратява нежеланото влизане [7].



Фиг. 11. Оптичен синтез на изображение

Фиг. 12. Серия AcuSense с филтриране на аларми

Фиг. 13. Алармени продукти

Заключение

В заключение можа да се отбележи, че към интегрираните системи за сигурност и комуникация се поставят все по-високи изисквания. Те са свързани с безопасността за населението и околната среда, защитата на целостта, конфиденциалността и достъпността на информацията, физическата защита на обекти, защитата на финансовите средства, материалната и интелектуална собственост.

В интегрираните решения за сигурност и комуникация задължително присъстват алармени системи, системи за видеонаблюдение, системи за контрол на достъп, системи за пожароизвестяване и пожарогасене, системи за детекция на вода и газ, системи за периметрова охрана, комуникационни системи, системи за централизирана охрана и предаване на данни, системи против кражби, специализирани системи за банкова сигурност и оповестяване, структурно кабелни системи и други [2]. За реализирането им се използва съществуващата или нова IT инфраструктура на обекта, която може да бъде конфигурирана за отдалечено наблюдение и управление. Отдалеченият контрол дава възможност в реално време да се наблюдават охраняваните зони на оторизирани потребители, намиращи се в различни части на сградата или извън нея. Гъвкавостта на системата позволява лесно да бъде разширена и надградена с допълнителни устройства и функции на по-късен етап.

Този доклад е подкрепен по Университетски проект № РД-21-236/28.02.2019 г., Усъвършенстване на способностите за съхранение на данни в интегрирана среда за информационна сигурност.

References:

1. Novosti pri integrirani sistemi za sigurnost, Inner Range, Tehnicheski biuletin, april 2018, http://www.sectron.com.
2. Politiki za sigurnost, http://www.sectron.com/en.
3. Chobanov, D. Integrated monitoring and control system. Conference proceedings MATTEX 2018. Information, Technical and Economical Problems of Security Systems, October 2018, Shumen, ISSN: 1314-3921, vol. 2, part. 1, pp. 68-73.
4. Chobanov, D. An algorithm for quick search of identifiers in an access control system. Conference proceedings MATTEX 2018. Information, Technical and Economical Problems of Security Systems, October 2018, Shumen, ISSN: 1314-3921, vol. 2, part. 1, pp. 74-78.
5. Hikvision_HD-TYI_News.pdf, http://www.sectron.com.
6. Sectron_Security2019_Integrated_Solutions_Presentation.pdf, http://www.sectron.com.
7. http://www.sectron.com/bg/news/termalni-kameri-hikvision-s-deep-learning-algoritym-za-analiz-veche-i-v-kupolen-variant