ЕВРОПЕЙСКИ СЪЮЗ
Европейки фонд
за регионално развитие
Инвестираме във вашето бъдеще

ОПЕРАТИВНА ПРОГРАМА
„Развитие на конкурентоспособността
на българската икономика" 2007-2013
www.opcompetitiveness.bg

"ОСОБЕНОСТИ НА ИНТЕГРИРАНИТЕ СИСТЕМИ ЗА СИГУРНОСТ И БЕЗОПАСНОСТ"

инж.Евгени Янков, инж. Михаил Аврамов

РЕЗЮМЕ:

Широкото разпространение на системи за сигурност и безопасност се дължи едновременно на регулаторни разпоредби и на осъзната необходимост. Задължителен компонент на обществени сгради е система за известяване при пожар, а за обекти като гари, летища, МОЛ-ове системата за публично оповестяване е неразделна част. Множество компании разчитат на защита чрез системи за видео-наблюдение, сигнално-охранителна техника СОТ и контролиране на достъпа. Интегрираните системи за сигурност и безопасност ИССБ предлагат централизиран контрол върху всички подсистеми за подобряване на оперативната ефективност и оптимизиране на разходите. Имплементирането на подобна система зависи от множество фактори като очакван обхват на системата, включително съществуващи системи, които да бъдат интегрирани под управлението на ИССБ, избор на подходяща ИССБ и респективно интегратор, промяна в организационно и оперативно отношение, отчитане на ползи и не на последно място цена, ROI, и TCO. Проведеното изследване върху водещи в бранша интегрирани системи представя характеристики, които са основни и значими за потребителите, както и недостатъци, които е необходимо да се имат предвид.

ЗА ИЗСЛЕДВАНЕТО

След бурното развитие на системите за сигурност и безопасност през последните години започна да се говори и да се развива интеграцията между отделните системи на един или на различни производители твърде често профилирани в определен сегмент. Вече тази интеграция се разглежда като необходимост [22]. Което поражда допълнителни въпроси, които се нуждаят от отговори, както и ясно определяне на проблемите, с които ще се сблъскват инвеститорите, и начините за тяхното преодоляване.

Проведеното изследване на интегрирани системи за сигурност и безопасност е основано на публична информация, предоставена от компаниите производители, маркетингови материали, публикации в периодични издания, конференции и др. Изследвани са интегрирани системи за сигурност и безопасност в необходимия обхват, за да могат да се постигнат целите за определяне на техните характеристики, които са важни за потребителите и влияят върху вземане на решение за имплементиране (внедряване).

ТИПОВЕ СИСТЕМИ

Интегрираните системи за сигурност и безопасност ИССБ могат да се класифицират по няколко критерия: обхват на поддържаните подсистеми, функционални характеристики, зависимост от специфичен хардуер или специфичен софтуер, възможности за интеграция с подсистеми на трети страни..

Относно обхвата на поддържаните подсистеми ИССБ се делят на две основни групи: с пълно или частично покритие на следните подсистеми:

1. Видео-наблюдение
2. Контрол на физическия достъп (контрол на достъпа)
3. Бариери и гаражи (автоматизирани врати) – може да се разглежда като по-вид на контрола на достъпа
4. Периметрова охрана
5. СОТ (сигнално-охранителна техника)
6. Пожаробезопасност и пожарогасене;
7. Оповестяване (звукова сигнализация и гласови съобщения)

Някои ИССБ са ориентирани само към системите за сигурност, докато други – върху системите за безопасност. В зависимост от очаквания обхват може да се избере компромисен вариант на система с частично покритие, като трябва да се предвиди какво ще бъде развитието на ИССБ и прилагането в компанията на допълнителни подсистеми, които биха оказали влияние в дългосрочен план.

Относно функционалните характеристики ИССБ са насочени да отговорят на определена бизнес цел. Съществуват системи, чиято основна роля е да предоставят централизирано управление чрез едно софтуерно приложение на всички устройства от обслужваните подсистеми [7]. Други извеждат на първо място функция за управление на кризи [12]. От друга страна ИССБ се представят като част от системи за управление на сгради – Building Management Systems BMS [1],[6],[9]. При тези системи има две разновидности – ИССБ да има възможност за самостоятелно функциониране [6],[9] или да е модул от BMS, което не предполага такова [1]. Съществуват държави, където за подобни системи се прилагат стандарти.

Определено можем твърдим, че всички ИССБ зависят или от специфичен хардуер или от специфичен софтуер или от двете взети заедно. Типичен пример за зависимост от специфичен хардуер е BMS на Bosch [1], която чрез отделните си модули [2-5] управлява компоненти производство на същата компания. Като допълнение компоненти на трети страни се управляват чрез OPC Server, което в по-голяма степен се отнася за управление на устройства за сградна инсталация, а не за компоненти на подсистемите за сигурност и безопасност. Друг подход е приложен от Johnson Control [9], като тяхната система P2000 освен за собствените им компоненти предлага и управление за ограничен кръг видео-камери и контролери/четци за контрол на достъпа на трети производители, и в допълнение притежават софтуерни интерфейси към конкретни специфични подсистеми на трети производители. От CDC Group Holdings твърдят, че тяхната система „Security Manager" има свързаност с богата гама различни системи от различни производители [7], което е разновидност на зависимост от специфичен софтуер. Някои производители обявяват, че в своите системи използват конкретни географски информационни системи GIS [12], [15].

Отговорът на въпроса възможна ли е интеграция с подсистеми на трети страни се оказа ключов в проведеното изследване. Почти липсва конкретна информация при проучените системи, което ще ни позволи да изложим нашето виждане. Както по-горе посочихме съществуват системи от изцяло затворен тип, където всички компоненти и софтуер за подсистемите и самата ИССБ е от един производител например Bosch. За такъв тип системи едва ли ще бъде целесъобразна интеграцията с вече използвани подсистеми при клиента. Същото се отнася и до системите от типа на Johnson Control. Подходът на CDC Group Holdings изглежда се доближава максимално до визията за интеграция с подсистеми на трети страни. В случая очакваният подход е самата компания да „изработи" конкретен интерфейс към съществуваща подсистема. Съществува и друга тенденция, основана на взаимния интерес. Като пример ще посочим компании в различни сфери (например видео-наблюдение и контрол на достъпа), които влизат в партньорски взаимоотношения за обмен на информация за взаимна интеграция на техните продукти.

ХАРАКТЕРИСТИКИ НА ИССБ

Характеристиките на ИССБ могат да се разделят основно на два вида: системни и функционални.

Към системните характеристики спадат поддържането на конкретни операционни системи, отделни сървър за бази данни и приложен сървър, клиент-сървър архитектура, наличието на WEB интерфейс, използвани комуникационни канали. Списъкът с поддържаните хардуерни компоненти и софтуерни интерфейси към подсистеми на трети страни е от изключително значение за потребителя.

Систематизирането на основните функционални характеристики, които са водещи за интегрираните системи за сигурност и безопасност, установи, че наличието и възможностите на слените модули са от съществено значение при вземане на решение за внедряване:

- Административен модул с възможност за грануларен достъп до информация и делегирани права за действия, организиране на представителния модел на обекта;
- Графичен интерфейс за визуализация на обекти и компоненти на подсистемите;
- Регистриране и управление на аларми с възможност за определяне на ниво за автоматичен отговор;
- Модул за управление на реакциите чрез правила;
- Лесна интеграция с компоненти или подсистеми на трети производители.

Разбира се съществуват и други функционални характеристики, които влияят върху избора на платформа, които допълват възможностите на системите.

ПРЕДИ ДА ИЗБЕРЕМ

Изборът на интегрирана система за сигурност и безопасност е съпроводен с редица решения и предвиждания за развитие, които една фирма трябва да направи. Голяма част зависят от спецификата на дейността, организацията на сигурността, физическото разположение на инфраструктурните обекти, като сгради, помещения, пътища, паркинги и др. Има обаче някои въпроси, които са общи за всички.

1. Колко и кои подсистеми поддържа ИССБ? Важно е ИССБ да покрива като минимум съществуващите или планираните за управление подсистеми.
2. Коя е основната подсистема на производителя? Има системи, при които една подсистема е основна, и върху нея се надгражда ИССБ чрез връзки с други подсистеми или устройства. В този случай е важно внимателно да се прегледат

възможностите на другите подсистеми за покриване на вашите специфични изисквания. Може да се окаже, че именно определена подсистема, която за вас е от изключително значение, да е с ограничена функционалност.

3. Какви са възможностите за разширение? ИССБ трябва да позволява скалируемост с възможност за разширение и адаптиране към променящите се изисквания.

4. Кой отговаря за интеграция с други подсистеми? По принцип това е производителя или на ИССБ или на съответната подсистема. По-доброто решение е да е осигурена възможност на производителите на подсистеми да осигуряват интеграцията с ИССБ, тъй като познават своята специфика, и по този начин ИССБ може да разширява списъка с поддържани системи по-бързо в сравнение с другия вариант.

5. Отворена ли е системата? Чрез т.нар. API (Application Programing Interface) се предоставя възможност за разработване на специализирани функции и връзки с устройства на трети производители без участието на производителя на ИССБ.

6. Какви са отзивите от клиенти? Референциите от дългогодишни и доволни клиенти говорят най-добре за качествата на ИССБ и нейния производител.

БИБЛИОГРАФИЯ

1. Bosch Security Systems, "Building Integration System Building management – one platform for everything", 2008
2. Bosch Security Systems, "BIS - Automation Engine 2.3", v3, 01.07.2011
3. Bosch Security Systems, "BIS - Security Engine (SEE)", v2. 07.11.2012
4. Bosch Security Systems, "BIS - Video Engine (VIE)", v2. 07.11.2012
5. Bosch Security Systems, "BIS - Access Engine (ACE)", v6. 12.12.2012
6. CDC Group Holdings Ltd, „Welcome to CDC Integra the platform", 2010
7. CDC Group Holdings Ltd, „Welcome to CDC Security Manager", 2011
8. Dan Hebert, "Are Integrated Safety/Security Systems Secure?", Control Magazine, 30.10.2008
9. Johnson Controls Inc., "P2000 Security Management System", 2010
10. Johnson Controls Inc., James F. Dagley, Terry W. Hoffmann, "The Perfect Technology Storm", 2008
11. Integrated Security and Safety Systems LLC, "Security Integration", http://is3now.com/
12. Intergraph Corporation, "Incident Management Solution", 2010
13. Intergraph Corporation, "Incident Response Management", http://www.intergraph.com/learnmore/sgi/public-safety/incident-response-management.aspx
14. Intergraph Corporation, "All-hazards Security", 2012
15. Magal S3, "Integrated Solutions Fortis 4G"
16. Magal S3, "Even fences can be a bit friendlier to the environment"
17. Magal S3, "Focusing on the perimeter for Critical Infrastructure Protection (CIP)"
18. MessageNet Systems, "Fire, Safety, Security & Alerting Systems Integration — MESA", http://www.messagenetcommunicationsystems.com/home/products/safety-security-alerting-systems-integration-mesa
19. Robert Ward Fletcher, "The Next Step: A Fully Integrated Global Multi-Modal Security and Safety Management System"
20. Sobieski Life Safety, "Integrated Fire & Security Systems", http://www.sobieskilifesafety.com/integrated-systems.php
21. Spark Technologies, "Integrated Physical Security & Safety Systems", http://www.spark-techno.com/systems-technologies/safety-systems/
22. Тони Стойнов, „Тенденциите са към интеграция на системите за охрана и безопасност",http://tech-dom.com/statiieng.aspx?id=1506

Този документ е създаден с финансовата подкрепа на Оперативна програма „Развитие на конкурентността на българската икономика" 2007-2013, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието на документа се носи от „СИД ДП" ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Договарящия орган.