



Alarm Receiving Centres: A Central Function in the European Security Landscape

Today and Tomorrow

White Paper by CoESS
And its Working Committee Electronic Surveillance

September 2009

CoESS – Confederation of European Security Services
Jan Bogemansstraat | Rue Jan Bogemans 249
B-1780 Wemmel, Belgium
T +32 2 462 07 73 | F +32 2 460 14 31
E-mail: apeg-bvbo@i-b-s.be | Web: www.coess.eu





Responsible publisher

CoESS General Secretariat:

Ms. Hilde De Clerck (Secretary-General of CoESS)

Jan Bogemansstraat | Rue Jan Bogemans 249

B-1780 Wemmel, Belgium

T + 32 2 462 07 73 | F +32 2 460 14 31

E-mail: apeg-bvbo@i-b-s.be | Web: www.coess.eu

CoESS Registered Office:

8, rue de Milan, F-75009 Paris, France

Copyright disclaimer

Unless stated to the contrary, all materials and information (studies, position papers, white papers, surveys and their future results) are copyrighted materials owned by CoESS (Confederation of European Security Services). All rights are reserved. Duplication or sale of all or any part of it is not permitted. Electronic or print copies may not be offered, whether for sale or otherwise, to any third party. Permission for any other use must be obtained from CoESS. Any unauthorised use of any materials may violate copyright laws, trademark laws, the laws of privacy and publicity, and communications regulations and statutes.



Introduction & Acknowledgement

Introduction

This document serves as a *White Paper* to describe the history and the current and future issues of the Alarm Receiving Centre (ARC) activity in the European private security landscape.

Its purpose is to give a better understanding to security industry players and national and European policymakers of this manned guarding activity, which is a full part of private security services, the needs for its development and the conditions of collaboration with Law Enforcement Agencies (LEAs).

The White Paper explains the viewpoint of CoESS as a European Confederation that tries to harmonise the interests of the industry, policymakers, governments and law enforcement agencies as well as end users/customers and tries to contribute to an improved security environment.

Acknowledgement

CoESS wishes to thank all CoESS Working Committee Electronic Surveillance members for devoting their time and effort to the development of this White Paper as part of the CoESS Working Committee Electronic Surveillance Working Programme 2008-2009.



Table of Contents

Introduction & Acknowledgement.....	3
Introduction.....	3
Acknowledgement.....	3
Table of Contents	4
Executive Summary	6
1. Alarm Receiving Centres?.....	7
1.1. Definition	7
1.2. Historical overview	7
1.3. The role of an ARC today	8
2. Current working practices/functionality	10
2.1. Introduction.....	10
2.2. The process of alarm handling and intervention on security alarms.....	10
2.2.1. Receiving the data (input)	10
2.2.2. Filtering.....	11
2.2.3. Operator analysis and verification	11
2.2.4. Justified response.....	12
2.2.5. Feedback	13
2.2.6. Other security-related activities.....	13
2.3. Other activities	14
2.3.1. Technical alarms.....	14
2.3.2. Safety alarms	14
2.3.2.1. Social alarms	14
2.3.2.2. Medical alarms.....	14
2.3.2.3. Elevators.....	14
2.3.2.4. e-Call	14
2.3.2.5. Fire alarms.....	14
3. Towards a European norm for ARCs	15
4. European legal and social framework.....	16
4.1. Legal provisions	16
4.1.1. Legal position in relation to monitoring.....	16
4.1.2. National ARC standards.....	17
4.1.3. Police policies	17
4.1.4. Fines or loss of response to systems by the police	17
4.2. Training requirements	17



5. Cooperation with public authorities	18
6. Future trends and challenges.....	19
Annexes	21
Belgian best practice	22
United Kingdom (UK) best practice	24
Italian best practice	26



Executive Summary

This White Paper describes the functioning of Alarm Receiving Centres (ARCs) and their contribution to overall security. ARC activities are a full part of private security services, whereby human intervention by the ARC operator is of paramount importance to the accuracy and quality of the service provided. The use of ARC services should be seen in the total security chain. This way, the highest degree of efficiency can be guaranteed as documented in this White Paper.

A degree of standardisation, a correct legal framework for the activities of the operators manning these centres and a correct level of information to end users and other stakeholders concerned increases overall quality via a controlled process of verification at the ARC. This results in high accuracy and short reaction times. On top of correctly described rules and regulations, a legal framework should define additional requirements (e.g. on training). This will increase the professionalism of ARC activities and positively impact the security of the end users.

A maximum of alarms should be verified by ARCs, because this will dramatically discharge the Law Enforcement Agencies (LEAs) in having to treat false alarms. The LEAs can thus much better prioritise and concentrate on urgent alarm response. Moreover, they can intervene towards real and verified alarms with a maximum of useful information. To achieve this, the right levels of communication and collaboration between ARCs and LEAs have to be officially agreed. Governments should thus promote the widest possible use of ARCs.

The current European private security landscape offers some cases of good practice in the different domains as the annexed cases from Belgium, the United Kingdom and Italy will show.

There is an important task for industry players in the different countries (through their national organisations) and for policymakers (governments at national level and the European Commission at European level) to correctly develop the necessary supporting frameworks. Not only the security industry will benefit from this, but even more so the customers, companies and organisations that aspire the best levels of security; and the respective governments who, through their LEAs, can benefit from an increased efficiency.

Danny Vandormael

President of the CoESS Working Committee Electronic Surveillance



1. Alarm Receiving Centres?

1.1. Definition

An Alarm Receiving Centre (ARC) activity is an activity where the operator is electronically supported to collect data from various sources, to analyse this data and adequately interpret them. The operator will then organise a correct response (e.g. specialised intervention guard, video verification etc.), will follow-up this response and will eventually close the incident, thereby informing all parties concerned. The human factor in these procedures is of paramount importance. As such, ARC activities are a full part of private security services; a fact that, in most countries, is confirmed by the inclusion of ARC activities in national private security legislation.

1.2. Historical overview

The remote monitoring of signals originating from alarm systems has been practised for many years in one form or another. This service was initially provided using telephone wire networks, and largely relied on simple mechanical dialling mechanisms calling a keyholder, a private security company and in many cases the Law Enforcement Agency (LEA). In most cases, these dialling mechanisms were known as 'autodiallers', which evolved in time as 'digital communicators'.

Autodiallers were the forefathers of remote signalling alarm systems. They were relatively inexpensive to install and became a very popular method of 'calling for help' following an alarm activation. The autodialler traditionally used any existing telephone line merely dialling the LEA and reciting a recorded message giving address details and calling for assistance. In the early 1960s, these systems were largely used for higher risk premises, banks, jewellers, cash depots etc. During the later 1960s, they began to be popular for higher value domestic systems and, finally, in the early 1970s, they were being installed across all risk sites.

This chapter aims to give an insight as to why ARCs were eventually to become the primary calling point for intruder alarm signals from the 1970s to today. Some reasons for this evolution were as follows:

- Increasing popularity in the use of autodiallers to control rooms resulted in a significant demand on the LEA;
- The clarity and quality of messages being sent by autodiallers became unreliable in many cases and alarms were often triggered for no genuine reason (false alarms);
- It soon became known that creating a mere telephone line fault prevented the signal from reaching its destination;



- Insurers and consumers lost confidence and sought higher security connections, usually via direct communication lines from protected premises. This method partly solved some of the security issues, but still gave rise to growing demands on the LEA.

This is a shortlist of early experiences of an immature solution to getting a signal from one area to another in a relatively secure way; however, cost and the LEA pressure on the industry gave rise to the birth of the ARC of today.

During the early transition period, ARCs were generally operated from existing security control rooms, which were able to double as alarm signal receiving centres at the same time. As the popularity of signal monitoring grew, monitoring centres began to mature both in standards and quality of services offered.

During the 1970s, the LEA began to enjoy the benefit of the commercial interception of alarm signals prior to them being passed to the LEA, but there was still the problem of growing demand on the LEA from both growth and false alarm signals being received.

With the emerging popularity both by the end user and alarm installers, the growth of privately monitored intruder alarm systems grew year on year for a considerable period of time. This growth was to create a large industry of Alarm Receiving Centres whose numbers were also growing at an impressive rate. This spectacular growth caused by market demand finally resulted in an effect which now raised LEA concerns. What had previously been perceived as a benefit to all, fast became a strain on LEA resource. It was clear that most signals being passed to the LEA were in fact still false alarms. This problem was being experienced throughout Europe and on both sides of the Atlantic. Things had to change and change they did.

ARCs and end users operating throughout Europe had restrictions imposed upon them as to how many signals would be tolerated from any system. Some countries opted out of attending altogether unless a high degree of evidence that the call was genuine could be proved. A new era began in what was to become a blueprint for alarm monitoring across all EU countries. The word 'confirmation' became a minimum requirement and European Standards were being consolidated as far as they could.

1.3. The role of an ARC today

The ARC of today now plays a vital role in the chain of security protecting homes and businesses alike. The ARC monitors its clients' security systems 24/7 and thus ensures they know that if there are any problems with the system or if the system activates, the ARC will carry out mutually agreed upon procedures and make sure the correct response is sent to the protected premises.



An ARC has day-to-day contact with customers, installers of security systems and with the emergency response services:

- By sending them daily reports on the activations that have occurred over a 24-hour period;
- By talking to customers who have accidentally set off their security system (this may include problems with their monitored alarm and the customer will contact the ARC for assistance);
- By talking to the emergency response services informing them of activations from installed systems;
- Or by dealing with emergency services requests for more information about activation incidents.

The ARC can therefore be perceived to be the ‘face’ of the industry by customers and emergency response services. These groups can form their opinion on the professionalism of the security industry by the actions of the ARC.

The ARC is also important to other organisations, such as insurers who rely on the ARC to monitor the systems of those insured by them. National retailers utilise ARCs to monitor their systems to not only protect their premises and assets, but also their staff, who are their most important asset. Monitored alarms not only protect buildings, persons and mobile objects, they also deter criminals who know that the activation of the alarm will bring an emergency response and a high likelihood that they will be caught.

Today’s ARC can monitor different types of systems, including, but not limited to:

- Intruder alarm systems
- Hold-up alarm systems
- CCTV systems
- Fire alarm systems
- Social and medical alarm systems
- Technical alarm systems
- Vehicle tracking systems

This list is not exhaustive as the ARC has the ability to not only monitor remote systems, but to also perform a number of additional functions, such as acting as the remote access control for sites using audio or CCTV technology, e.g. responding to door entry systems, or even carrying out a remote access patrol function by utilising the site’s CCTV system to view the perimeter.

It seems that the current scope of ARC monitoring is only limited by the current technology that is used or the lack of end user knowledge of how much added benefit an ARC can bring to the security and safety of their homes and businesses.



2. Current working practices/functionalities

2.1. Introduction

ARCs have also expanded their tasks and responsibilities from the filtration of incoming intruder alerts from fixed premises (buildings) to include responsive action on alerts from persons and mobile objects and from signals of a technical, fire or health and safety nature.

In order to adequately fulfil its role in case of a security alert, which is to maximise both the security of the customer and the efficiency of the corrective or preventive action taken either by the authorities or by private intervention, the ARC will always perform the following steps in a controlled and secured filtering process:

- Automatically receive data from a multitude of sources and technologies;
- Filter away those data signals not requiring operator attention;
- Let the operator perform an analysis and verification of the data received so that he/she can classify the alert into a specific alarm category;
- On the basis of this classification, the ARC will start a procedure for further action (response) or decide against any further procedures;
- The ARC operator will then close the incident by providing feedback as mutually agreed upon with the customer.

Over the last decades, thanks to a series of technical and organisational developments, ARCs have been able to improve their filtering performance, i.e. the identification and consequent elimination, from the process, of alarms that do not require intervention, often referred to as 'false alarms'.

New ICT technology provides the ARC with additional resources and means; however, in order to keep up with these rapid developments, continuous investments from the ARC are required on all levels. Nonetheless, the ARC needs to remain critical on the added value of new technology in order to maintain a controlled process with proper filtering, to keep the process itself secured from outside attacks and loss of control, and to ensure proper training of its operators.

2.2. The process of alarm handling and intervention on security alarms

2.2.1. Receiving the data (input)

The era of analogue data transmission and a fairly simple technical structure has long gone.



The ARC now deals with incoming data from a multitude of sources and technologies:

- High volume: an average customer will send approximately 60 signals per month to the ARC;
- Multiple network technologies: PSTN, ISDN, GSM (voice), GSM/GPRS, internet, direct lines and specific networks;
- Different network providers with different levels of performance and warranties;
- Data which is formatted along different protocols for which the ARC will operate a selection of specific or multiprotocol receivers, from analogue signals, via PSTN to IP.

On a monthly basis, a 'typical' ARC with around 50,000 customers will receive approximately 3 million data signals from its customer base, all of which require adequate processing via the ARC's operational servers.

2.2.2. Filtering

The ARC's servers will provide an initial filtering of data on the basis of whether they are alarm-related or to be treated as background information for further reference. More than 90% of incoming data is filtered away to the data storage. The servers will also automatically process a certain number of incidents via reporting, voice messages or SMS, thus reducing the amount of incidents requiring operator intervention on site to less than 5% of incoming signals. These incidents can be referred to as 'security alerts'.

2.2.3. Operator analysis and verification

Historically, the ARC operator could use call-back on site, i.e. private intervention as a means of verification. Over the last decades, technology has provided new and additional tools for ARC operators, a trend that will no doubt continue. This resulted in the development of verification procedures, which are, in most countries, in the process of becoming some form of legislation or a covenant between the ARCs and the national authorities. These covenants determine the procedures, exchange of information, priorities and performance targets that are applicable at this stage, e.g. the Dutch VEBON/VPB 'Covenant with the Supervisory Board (Raad van Commissarissen)', and specific legislation in the United Kingdom and Belgium.

In a 'typical' ARC with around 50,000 customers, ARC operators will be presented with about 100,000 incidents per month (or an average of 2 incidents per customer per month). After selection and information, less than 50% of these incidents will be qualified as security alerts. The remaining incidents will be identified and responded to as organisational or technical incidents.



The full verification process is applied to security alerts according to mutually agreed upon procedures with the customer and using all available verification means:

- Audio verification: the establishment of a direct verbal contact with the site and/or the customer and the customer's contact persons, either by call-back or via an automated connection to listen-in and/or via two-way communication;
- Sequential verification: evaluation of the sequence of incoming data, confirming the original incident by a repetitive pattern and/or a confirmation from (a) different detection point(s) and/or a general pattern;
- Video verification: the establishment of a direct visual link with the site using images, video clips or live feeds, allowing for confirmation of the data received;
- Site visit: on site situation check either by a designated person or via intervention by specialised private guard forces.

If one or more of these verification elements confirm a suspicious situation, the ARC will catalogue the alert as a security alarm and proceed to the next phase of justified response.

2.2.4. Justified response

The response towards the site can be organised either via a specialised intervention guard and/or via the police, depending on local legislation and circumstances. The intervention team will evaluate and consolidate the situation on site and request additional assistance if required. In order to keep the ARC operator fully informed of the progress of the intervention and to complete and automate the information flow towards the intervention team, technical and organisational improvements have already been made and will continue to be introduced in the future. By using tracking and tracing devices, PDAs and other tools, real-time information can be dispatched to the intervention team.

Avoiding unnecessary interventions offers several advantages to:

- The customer:
 - Less distressing situations
 - Fewer costs
 - No compromise on security
- The intervention team:
 - Decreased workload resulting in fewer costs and shorter intervention times
 - Improved information regarding the situation on site reduces security risks
 - In some countries, projects are being deployed in order to automate and standardise the exchange of information with the national authorities



2.2.5. Feedback

The process of verification is closed by providing feedback to the customer and other stakeholders such as installers, intervention teams etc. Technology now allows the operator to provide instant and online information:

- Messaging technology: voice calls, automated messages, visual information on PDAs or other devices etc.;
- Online access to secured servers where further information on the incident is made available.

Technology also facilitates the provision of improved feedback from authorities regarding the incident itself, the incident rate in particular geographies or the types of incidents encountered. Again, ARCs are well-positioned to disseminate such information to customers if requested and justified.

2.2.6. Other security-related activities

The described filtering and verification process is in place in most ARCs in order to adequately deal with security alarms from fixed premises (buildings). Since 2000, however, ARCs have gradually expanded their tasks and responsibilities to include the following functions:

- Tracking and tracing activities. As carjacking and homejacking reached a critical level, ARCs proposed to install a device which allows for real-time transmission of data and GPS coordinates. This device is installed in mobile objects such as cars, trucks, equipment etc. The signals are processed according to the aforementioned filtering and verification process, but the nature of the equipment allows for additional localisation services, controlled immobilisation and additional services as per the customer's request and as authorised by law. The collaboration between ARCs and national authorities resulted in tangible achievements with respect to the reduction of false alarms, vehicle recovery (over 90%) and criminal arrests.
- As regards the monitoring of persons, a similar ARC service is currently being developed in order to address security risks to which lone workers and other staff are exposed. A mobile tool, similar to a GSM, provides for the transmission of data and location coordinates via LBS or GPS. The signals are processed according to the aforementioned filtering and verification process.
- CCTV systems are used by ARCs not only for video verification, but also to perform a video surveillance function via virtual patrols or systematic reviews of image material. There is often no specific signal triggering the ARC's action, with the exception of an incoming image, which the ARC judges to be anomalous.



2.3. Other activities

In the previous subchapters, the filtering and verification process of security alerts and alarms coming from alarm systems in buildings, persons or mobile objects was described in detail. Next to purely security-related activities, the ARC also touches the technical and safety domain.

2.3.1. Technical alarms

Similar filtering and verification procedures for security alerts/alarms are applicable to alarms coming from a technical device indicating a technical malfunction, e.g. temperature control, power drop etc.

2.3.2. Safety alarms

2.3.2.1. Social alarms

The ARC provides for assistance services for certain demographics requiring a localisation verification, e.g. elderly people, prisoners etc.

2.3.2.2. Medical alarms

The ARC provides for first-line interaction with persons in need of medical care.

2.3.2.3. Elevators

The ARC processes signals and calls from elevators and organises the response.

2.3.2.4. e-Call

The ARC responds to signals coming from vehicles 'in distress', e.g. exploding airbag, collision indicator etc. by verifying localisation and the need for help and assistance. Please refer to the European Commission Communication COM(2009) 434 on 'eCall: Time for Deployment' for further information.

2.3.2.5. Fire alarms

Similar filtering and verification procedures for security alerts/alarms are applicable to fire alarms, but with tailored procedures and the fire brigade as the designated intervention team.



3. Towards a European norm for ARCs

In 2000, the idea was launched to prepare a European initiative on the standardisation of monitoring and electronic surveillance activities. The initiative took concrete form when CoESS' Working Committee Electronic Surveillance and Euralarm's Standing Committee n° 7 decided to join forces in order to draft a common proposal concerning Monitoring and Alarm Receiving Centres. The aim was to define a number of criteria with which ARCs throughout Europe should comply.

In June 2005, after four and a half years of intensive work, a joint 'Code of Practice for Monitoring and Alarm Receiving Centre Requirements' was finalised. Both Committees agreed to introduce the document to their respective Boards. Upon official approval, the Code of Practice was to be transmitted to the relevant European standardisation bodies as a discussion paper for the development of a European norm.

The draft document was intended to be discussed within CENELEC, the European Committee for Electrotechnical Standardisation. CENELEC launched a new Working Group (n° 14) according to the standard format: national standardisation organisations appoint experts at national level to sit in the European Working Group. The necessary preparations were made mid 2006, when the Working Group officially commenced its activities.

A total of 20 national experts participate in the Working Group's bi-monthly or quarterly meetings. It is worth mentioning that several participants from the former CoESS-Euralarm taskforce are again present in the CENELEC Working Group, thereby representing many of the same countries.

The CENELEC Working Group proceeds essentially in the same way the CoESS-Euralarm taskforce did in the sense that all relevant topics, issues and questions are discussed in detail. The CENELEC specifications for ARCs will be threefold:

- European Standard EN 50518-1 – Part 1: Location and construction requirements
- European Standard EN 50518-2 – Part 2: Requirements for technical facilities
- European Standard EN 50518-3 – Part 3: Procedures and requirements for operation

The entire preparatory process and the definite specifications are expected to be finalised in the course of 2010.

The future CENELEC norm is an example of a European harmonisation initiative, driven by technical experts and spread over a fairly lengthy period of time, starting with a joint CoESS-Euralarm taskforce preparing a draft document that is reviewed within the CENELEC structure with the aim of becoming a European norm.



Currently the security technical committee (IEC TC/79) belonging to the world standards body, the International Electrotechnical Commission (IEC) is looking at writing an international ARC standard. It is expected that the CENELEC work will be used as part of the base documents for this work.

4. European legal and social framework

4.1. Legal provisions

In early 2007 and towards the beginning of the development of the 'European Standard (EN50518) for Monitoring Centres', CoESS undertook a survey across the wider European monitoring market to determine the existence or otherwise of specific regulation in the region. This survey was updated at the beginning of 2009.

In general terms, the survey addressed three specific areas:

1. What is the current legal position in relation to monitoring in each European country?
2. Does a national standard exist to which ARCs must confirm?
3. Is there a specific policy set by the police that must be followed in order for them to offer a response service to the ARC?

All 27 EU Member States were invited to participate in the survey. The following countries did not contribute: Cyprus, Denmark, Latvia, Lithuania, Luxembourg, Malta, Portugal and Sweden. The following non-EU countries also took part in the survey, i.e. Bosnia & Herzegovina, Norway, Serbia, Switzerland and Turkey.

4.1.1. Legal position in relation to monitoring

All participating EU countries indicated that, next to standard business laws, there are specific laws in existence relating to the operating of an ARC in their country.

Of the non-EU countries, both Norway and Bosnia & Herzegovina have laws, while Switzerland reported that, other than standard business legislation, they have no specific laws.



4.1.2. National ARC standards

Here the answers were very different with only the following countries confirming the existence of a current national standard: Austria, Belgium, France, Germany, Ireland, Italy, Spain, Slovenia, The Netherlands and the United Kingdom.

The following countries have not confirmed that they have a national standard: Bulgaria, Czech Republic, Estonia, Finland, Greece, Hungary, Poland, Romania and Slovakia.

As regards the non-EU countries, Serbia, Switzerland and Turkey do not have a national standard, while Bosnia & Herzegovina confirmed they have.

4.1.3. Police policies

The following countries confirmed the existence of local police rules in order for their ARCs to receive a response from the police: Austria, Belgium, Czech Republic, France, Germany, Ireland, The Netherlands, Slovenia and the United Kingdom.

The following countries do not have any specific police rules determining requirements in order to respond to alarm events from ARCs: Bulgaria, Estonia, Finland, Greece, Hungary, Italy, Poland, Romania, Slovakia and Spain.

All three non-EU countries, i.e. Norway, Switzerland and Bosnia & Herzegovina, do have specific police policies.

4.1.4. Fines or loss of response to systems by the police

In Europe, the police deal with false alarms in many different ways. In some countries, fines are imposed on the ARC or the installer or the end user. In other countries, there are no fines, but the police will not respond to alarm systems after the alarm system has had a small number of false alarms in a defined period.

4.2. Training requirements

The same countries responded to the question as to whether a formal training programme exists or is mandatory for ARC operators.

In most countries, e.g. Belgium, Finland, France, Italy, Poland, The Netherlands and many others, ARC operators, being part of private security, have to be qualified private security guards.



This means they need official approval by the competent authority in their country and have the obligation to follow the basic training for private security guards.

On top of this basic training, a number of countries have introduced additional requirements for ARC operators, mandatory by law or otherwise (e.g. in Belgium there is a legal requirement to carry out 70 hours of specialised training (in addition to the basic training of 132 hours) and to pass through a governmental test examination centre; after this, operators are issued with a licence), or a specific training organised by specialised training institutes; e.g. Nordic Training Centre for Alarm Technique (NUSA), Inspectorate of the United Kingdom, Security Institute of Ireland, etc.

5. Cooperation with public authorities

The key factor, but even more the bridge between private security and public authorities is formed by ARCs.

In many countries, public authorities are rather apprehensive about their connection with private guarding and even with the possibilities offered by security devices such as cameras, CCTV equipment and access control systems. These suspicions are often caused by a lack of know-how of the nowadays reality and/or by short-sighted political dogmatism. Security and safety are still believed to be reserved exclusively to the public authority domain.

Nonetheless, the ARC market is perceived as the most trustworthy segment of the private security industry. The reasons thereof are multiple. ARCs enjoy the impression of technical neutrality and benefit from the perception of quality and professionalism. Authorities are collaborating with ARCs on an increasingly regular basis.

It is indeed near impossible and too costly for the police and fire brigades to be connected to the millions of homes, businesses and public buildings in their respective areas.

The fact that ARCs are often the first to be notified of an intrusion, theft or fire is a very convenient feature to the authorities.

The situation as it presents itself e.g. in Belgium, The Netherlands and the United Kingdom is in many respects a best practice for the future. It is important that authorities sign written covenants with ARCs stipulating respective tasks and responsibilities. It remains crucial for the ARC to commit itself to strict procedures, privacy policies and an immediate response to alerts. Authorities (both the police and fire brigades) in turn must engage themselves to intervene in a timely manner. All too often, only the ARCs have service and quality agreements towards their end customers.



Equally important is the necessity for the police and fire brigades to provide feedback to the ARC following an intervention. This will not only reassure the customer in question, but will improve corrective and/or preventive measures and will increase overall security.

By closely cooperating with ARCs, there is no need for authorities to invest in costly hardware and software, neither are they obliged to remunerate ARC personnel 24/7, but more importantly, authorities can shift the responsibility onto the ARC in case of failure or error.

These are just some of the reasons why the cooperation between authorities and ARCs needs to be strengthened and officially recognised in national and supranational legislation.

A close cooperation necessitates a good balance between public interest and the interests of the ARC's end customers. Given the enhanced risks, globalisation and continuous democratisation the world is facing today, cooperation between all security stakeholders (public authorities, customers and ARCs) will continue to increase. Authorities and ARCs will evolve towards a junior partnership, where the junior partner, the ARC, performs its security operations and the authorities create the legal framework within which the ARC can operate. In order to avoid an unbalanced partnership, it is imperative to put in place European legislation based on the democratic values of the Member States, the knowledge of private security stakeholders and a positive outlook on the future.

6. Future trends and challenges

Over the years, the European ARC market has grown significantly in terms of customer base, and seems set to continue this trend in the future. Nevertheless, ARCs are continuously challenged and faced with new and important changes and technologies, some of which present interesting opportunities.

From a technological point of view, there are three key drivers which determine the development of the ARC market:

- ARCs used to connect their client's alarm systems via analogue telephone lines (PSTN), which are now being abandoned in favour of digital telephone lines (VOIP). This new set-up necessitates the replacement of a substantial number of devices by more secure and more capable TCP-enabled devices (ADSL or GPRS);
- The alarm information received by an ARC includes more and more video and/or audio data, which in turn provide for better quality verification, and enable the ARC operator to perform a remote and in-depth analysis of the situation on site. New monitoring features include full or partial arm/disarm controls, remote change of settings and firmware upgrades;



- The rapid deployment of machine-to-machine (M2M) security applications opens up completely new possibilities for an ARC, changing the monitoring target from fixed to a mobile environment and even to an individual's exact location. ARCs are still merely at the starting point of these exciting developments, which are expected to get a boost in the next few years in anticipation of upcoming regulations (e.g. the e-Call initiative) and the growing availability of GPS and other asset or personal tracking technologies.

ARCs throughout Europe are devoting considerable efforts to redefine their role in preparation of these changes, especially in terms of IT infrastructure, new procedures and adequate training programmes. This last element will improve the retention of skilled operators, which will become a growing concern for the industry as training requirements continue to increase.

The perception and added value of ARCs handling security alerts need to be addressed and improved in certain areas, such as the residential market, which demonstrates clear potential as market penetration in this particular segment is not always high in every country. New technologies enable the customer to benefit from more or less the same features that are available at the ARC, i.e. the customer can receive real-time alerts via SMS, MMS and e-mail, can view frames or live feeds, can listen-in and is able to manage his/her security system at home or at the office using a PC or smartphone. These useful features must, however, be used in parallel with the operations carried out by the ARC, as they do not substitute professional alarm handling and verification. A citizen is not trained to perform such operations, nor is he/she available 24/7. LEAs should therefore discourage the 'do-it-yourself' approach to security.

In this changing environment, it remains a challenging task for the private security industry to play a proactive role in defining new norms and protocols, including training manuals, thereby setting the highest possible industry quality standards. High quality entails recognised added value and mutual benefits for customers, authorities and the security industry.



Annexes



Belgian best practice

The Belgian best practice was provided by ACA¹ (Alarm Centrale Associatie/Association Centrale d'Alarme), the Belgian association of monitoring stations, who in turn is an active member of CoESS.

Public-private cooperation on improved verification leads to more efficient and safer intervention after alarm

The Belgian Ministry of the Interior has been an early and important factor in the regularisation of the Private Security Industry. After the creation of the legal framework for the Private Security Industry (and covering, amongst others, the ARC activity) on April 10, 1990 (the so-called “Law Tobback”), the Authorities have continued with clarifications and updates in the form of Royal Decrees. With respect to the role of ARCs, two specific Royal Decrees have played an important role.

The first one was published on May 17, 2002 and regulated the mandatory role of the ARC with respect to “Stolen Vehicle Tracking” (SVT). It was the first regulation of this type of activity in the EU. The operating principles laid down in this legislation are established in close cooperation with equipment manufacturers, insurers and ARCs. ARCs are now filtering the alarms from approximately 30,000 connected vehicles and have limited their request for Police intervention to less than 300 incidents per year. More than 70% of the requests turn out to be real thefts or attempted fraud. The recovery rate of stolen vehicles is well above 90%.

A second legislation was passed in the form of a Ministerial Decree on January 10, 2003 and covered communication between ARCs and the Police. This decree was followed by additional clarification documents covering a.o. verification of incoming alarms and communication thereof to the Police. These verification procedures were elaborated in close cooperation between the Authorities and the ARCs. The implementation of these allowed ARCs, by 2005, to better filter on the mass of incoming alarms (estimated at more than 4,000,000 per year) and to reduce the request for Police intervention to less than 25% of the 2002 level. During the Symposium on “Private Security on the Move!” on December 7, 2006, the Minister of the Interior acknowledged this result as a cutback of tens of thousands of unnecessary Police interventions per year. He also announced his strategy to further support the increased use of ARCs in the alarm verification process because of the increased accuracy of their information versus other sources. One of the outcomes has been a favourable fiscal treatment of the ARC service and related components, such as alarm installation, in the value chain.

¹ Please refer to the website of ACA for further information on the ACA organisation and its activities (the website is available in Dutch/French only): www.a-c-a.be.



Recent developments in Belgium are focusing on the quality of the information, and the way it gets transmitted from ARCs to specialised guarding personnel and to the Authorities. Again the aim is to further increase the efficiency and safety of interventions on site.



United Kingdom (UK) best practice

The United Kingdom (UK) best practice was provided by BSIA², the British Security Industry Association, who in turn is an active member of CoESS.

In the UK, if an Alarm Receiving Centre wishes to pass an alarm activation to the Police, it must meet the conditions set down in the UK Police security system policy³ and with the system installer/maintainer (who also has to meet the UK Police security systems policy requirements) to provide false alarm prevention/management.

The work the industry has undertaken to reduce false alarms from intruder alarm systems has been dramatic. In 2000, there were 949,062⁴ remote signalling intruder systems installed and these gave 921,649 false alarms (nearly 1 false alarm per system) and this was unacceptable to the Police service. In 2008, the number of remote signalling intruder alarms had grown to 1,152,475 systems installed and the false alarm rate had dropped to 277,873. The industry and the Police force are working together to continue this downward trend in false police alarm activations.

The main thrust of the police/industry proposals was to target those intruder alarm systems that had a number of false activations to which the Police responded. It was agreed that if an alarm system had 5 false alarms it would be removed from police response and could only regain police response if the intruder alarm system was upgraded to a “confirmed alarm system” (British Standard document DD 243 refers). This meant that the intruder alarm system had to send at least two separate alarm activations from at least two separate (and independent) detectors before the ARC could pass the activation to the police control room to gain a police response. This was a learning curve for the whole industry as the installer had to learn how to design and install confirmation systems and the ARC had to manage confirmation system activations.

Currently, the British Standard document for confirmation DD 243 is being upgraded to a British Standard BS 8243 and the Police now require “confirmed” activations for hold-up alarms. This has meant that when a hold-up alarm activation occurs, there must be some form of verification that the activation is genuine. This could be some form of audio or video confirmation or other method to reduce the possibility of a false activation.

² Please refer to the BSIA website for further information on the BSIA organisation and its activities (the website is available in English only): www.bsia.co.uk.

³ This document is entitled the ‘APCO Security Systems Policy 2009’ and is available from the following website: www.securedbydesign.com/professionals/pdfs/ssgpolicy.pdf.

⁴ The numbers stated in this clause are the official Association of Chief Police Officers (APCO) figures.



It is important to note that “confirmation systems” are only required for new intruder alarm installations and intruder alarm installations and hold-up alarm systems that caused false alarms. The Police force have not been retrospective and require all older intruder alarm systems to be upgraded as long as these older intruder alarm systems or hold-up alarm systems do not cause false alarms.

The work the industry is undertaking with the Police is proving what a partnership approach can accomplish. It is also dealing with the problems of false alarms and therefore giving the Police the confidence that when they attend a call from an ARC, there is a very high probability that a genuine burglary or hold-up situation is occurring and they can act accordingly.



Italian best practice

The Italian best practice was provided by FederSicurezza-A.N.S.S.A.T. FederSicurezza⁵ (Federazione del Settore della Vigilanza e Sicurezza Privata) is the Italian private security association, active member of CoESS. A.N.S.S.A.T.⁶ (Associazione Nazionale Servizi Satellitari e Telematici) is the Italian national association of satellite and telematic services, and in turn member of FederSicurezza-Confcommercio.

The original Italian text was provided by Mr. Romano Lovison, President of A.N.S.S.A.T. The present text is an excerpt of the English edition of FederSicurezza's 2009 Report and Outlook entitled '2009 Report from FederSicurezza: realities and scenarios in Italian private security in the European context'⁷.

⁵ Please refer to the FederSicurezza website for further information on the FederSicurezza organisation and its activities (the website is available in Italian only): www.federsicurezza.it.

⁶ Please refer to the A.N.S.S.A.T. website for further information on the A.N.S.S.A.T. organisation and its activities (the website is available in Italian only): www.anssat.it.

⁷ The '2009 Report from FederSicurezza: realities and scenarios in Italian private security in the European context' can be downloaded from the FederSicurezza website either in Italian (<http://www.federsicurezza.it/public/documenti/97200913365.pdf>) or in English (<http://www.federsicurezza.it/public/documenti/89200915934.pdf>).

The **advantages** of satellite **radiolocalization**

A.N.S.S.A.T. (the National Association of Satellite and Telematic Services), an adherent of FederSicurezza - Confcommercio, was founded in April 1997 and is an Association "not-for-profit, without ties to political parties and autonomous with respect to public powers, among companies, howsoever denominated or legally organized, which carry out, within the sphere of the laws that regulate the subject matter, security services and assistance on means of transport through operational centres and with the use of telematic and satellite localization systems, as well as the producer companies of hardware and software for radiolocalization".

A.N.S.S.A.T. represents the principal Italian companies that deal with the construction and/or distribution of remote-control services with professional satellite radiolocalization systems, which employ more than 400 highly specialized workers, with a global turnover in excess of 60,000,000 euro per annum. Some of these companies are business units of important national groups of the Private Security Sector which, globally, employ approximately 8,000 people with a turnover in excess of 600,000,000 euro. The associated companies provide advanced security services on more than 80% of heavy goods vehicles fitted with satellite systems, with a professional security service.

During the course of the last few years, the monitoring activity of vehicles carried out by the members of A.N.S.S.A.T. has produced a saving for insurance companies, or for the private firms or haulage companies or for the commissioners of the transport, of an annual average of 55 million Euro for thwarted thefts and robberies.

This research examined the activity of approximately 800 vehicles that transported goods of similar types and uniform routes in the territory of Italy. This was so as to provide a framework of the importance, for the security of transports, of the adoption of radiolocalization systems on heavy goods vehicles. The comparison is made by comparing journeys

fig.7 **TREND OF THE EVENTS**



figure 7

fig. 8 **EVENTS IN THE PERIOD 2005-2008**

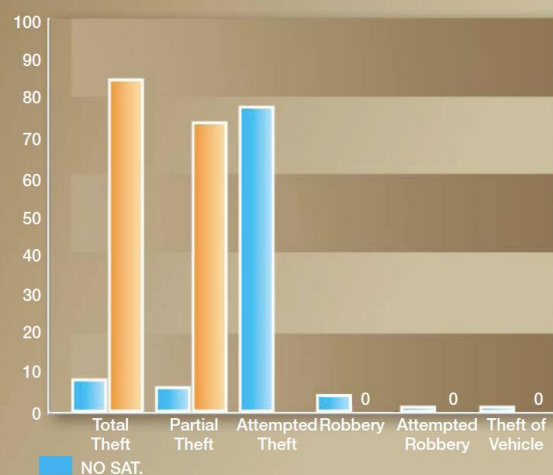


figure 8

between roughly 50% of vehicles equipped with professional security systems and around 50% of vehicles with no security systems fitted. *Figure 7* represents the global number of the events that occurred with vehicles fitted and not fitted with satellite radiolocalization systems. As can be seen, there was a noteworthy reduction of events in 2008 due to

an increasing number of counter actions, owing to both the organization of transport security and also to the actions implemented by the police forces which, thanks to the use of data provided by the surveillance systems, were often able to implement significant activities of repression of the phenomenon.

Figure 8 shows the events by type.

As can be seen, most of the events take place on vehicles that are not equipped with satellite radiolocalization systems.

In particular, it is possible to observe the large number of vehicles that have suffered the theft of all the goods they were carrying. As far as partial theft is concerned, it is important to note how the entity of the partially stolen goods is different. In the case of a vehicle fitted with a satellite radiolocalization system, the quantity of stolen goods is relatively small (a few packages) in that the activation of acoustic alarm systems disturbs the criminal activity, whereas in vehicles without satellite radiolocalization systems, the damage is greater. There were four robberies carried out, with one being only attempted, thanks to the bravura of the driver who managed to foil it. The theft of the vehicle occurred in a workshop, while it was undergoing maintenance, but the presence of the system made its recovery possible.

Figure 9 indicates, by percentage, the type of event to which the vehicles fitted with satellite radiolocalization systems were subject to.

In 86%, damage was avoided totally (80%) or partially (6%) thanks to the presence and operation of the satellite radiolocalization system. Only in 12% of the cases (total theft 8% and robberies 4%) was the damage complete.

Analyzing these cases one by one, it is revealed that this occurrence was due to the driver's failure to observe the measures imparted: the most frequent cause was parking in unsafe areas.

Figure 10 shows how, in the event of an occurrence, there is always an economic damage. In 53% of the cases, there is a significant event with theft of the totality of the goods, and in 47% of the cases there is partial

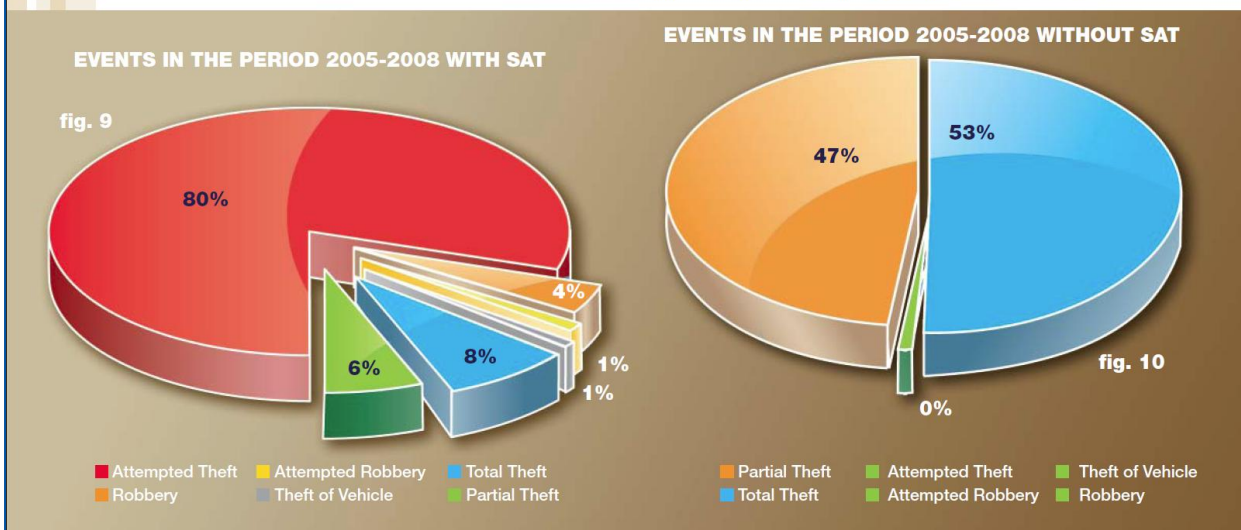


figure 9

figure 10

damage. In this last case, as was previously observed, the partial damage is of a greater entity with respect to the similar partial damage suffered by vehicles equipped with satellite radiolocalization systems.

Romano Lovison



**Alarm Receiving Centres:
A central function in the European security landscape
today and tomorrow**

White Paper by CoESS – Confederation of European Security Services
© September 2009

CoESS – Confederation of European Security Services
Jan Bogemansstraat | Rue Jan Bogemans 249
B-1780 Wemmel, Belgium
T +32 2 462 07 73 | F +32 2 460 14 31
E-mail: apeg-bvbo@i-b-s.be | Web: www.coess.eu