



## DELIVERABLE D3.1

# Current status of Security in Mass Transport

November 2009

*Author(s): Ana C. Sáez (INECO), Álvaro Urech (INECO), Jaime Pereira (TIFSA)*

*Reviewed by: Ilpo Kumala (VTT), Raija Koivisto (VTT)*

**PUBLIC**

<b>Grant Agreement number :</b>	<b>218264</b>
<b>Project acronym :</b>	<b>DEMAsST</b>
<b>Project title :</b>	<b>Demo for mass transportation security: roadmapping study</b>
<b>Partners:</b>	FOI (SE, coordinator), Ansaldo STS (IT), CEA (FR), Diehl (DE), EADS Astrium (FR), FFI (NO), Fraunhofer (DE), INECO-TIFSA (ES), SINTEF (NO), TECNALIA-INASMET (ES), THALES Security Systems (FR), TNO (NL), and VTT (FI).

## **Revision table**

<b>Version</b>	<b>Date</b>	<b>Modified Pages</b>	<b>Modified Sections</b>	<b>Comments</b>
0.1	30/06/09	All	All	Creation
1.0	30/07/09	All	All	All graphics included
2.0	28/08/09	All	All	Conclusions and final review
3.0	09/09/09	All	All	Comments from partners included
4.0	06/10/09	All	All	Comments from the Commission included

**Table of contents**

1 LIST of ACRONYMS. ....4

2 INTRODUCTION AND SCOPE. ....5

3 CURRENT STATUS OF SECURITY IN MASS TRANSPORT. ....7

4 ANNEX A: QUESTIONNAIRE. ....14

5 ANNEX B: STATISTICAL ANALYSIS OF STAKEHOLDERS' FEEDBACK.....25

## **1 LIST of ACRONYMS.**

ARC: Alarm Reception Centre.

CBRN: Chemical Biological Radiological & Nuclear.

CCTV: Closed Circuit Television.

CPS: Centre for Protection (of citizens) and Security. It is a synonym of Control Centre.

ICT: Information and Communication Technologies.

K9: Canine (patrols).

PA: Passenger Announcement.

## **2 INTRODUCTION AND SCOPE.**

Within the scope of DEMASST WP3, this document gathers all the information collected from key stakeholders all around Europe with the aim of drawing a map of the current status in mass transportation security.

The main inputs for this document have been the answers to a questionnaire distributed among the different entities involved.

The model of questionnaire used is included as Annex A whereas the raw data stemming from these answers are included as Annex B.

While performing the interviews to get the answers from the stakeholders, they also transmitted to us some extra information about mass transportation security not directly linked to the questionnaire. In this direction, we were addressed to an exercise performed in Oslo in 2006, where a large-scale real-time exercise on terror attacks against the transport systems was hosted. The exercise lasted 24 hours, and included the following scenarios:

- An explosion in a subway carriage at an underground train station
- An explosion in a train carriage parked at the central train station
- An explosion in a bus
- A train stopping in a tunnel, possibly linked to the previous explosions.

After the exercise, a rather substantial and public evaluation report was produced. It is called "Øvelse Oslo 2006 – Evalueringsrapport", and was produced by The Directorate for Civil Protection and Emergency Planning in 2007.

It describes in some detail what happened during the exercise, points at possible improvements, not least based on the requirements from first responders and involved preparedness departments.

Although it's been three years since the exercise was held, and some of the identified challenges have been solved (at least partially), the stakeholder interviewed felt the report still showed an accurate picture of the most relevant security challenges for handling such a massive crisis.

The most interesting for this report might be their recommendations for the future regarding emergency preparedness, also related to transport security. These recommendations are included in the next chapter.

60% of questionnaires were filled in by conducting face-to-face interviews with the people in charge of security issues, while 40% were answered by email.

Codification keys used to represent the different answers is listed below:

Y: Yes.

N: No.

N/A: No Answer.

The report aims not only to list what tasks every specific entity develops, but also to sketch how the different entities cooperate in the different aspects of mass transportation security.

This report is based on the information provided by 18 different entities. The following table shows the split of these organisations according to their nature:

Type of organisation	Number of representatives
First responders	4
Aviation	1
Multimodal operator	6
Rail operator / Infrastructure manager	7

These organisations are spread all around Europe. For confidentiality reasons their exact location is not revealed, but they have been classified in three different areas: Southern Europe (representing 35% of stakeholders), Central Europe (30%) and Northern Europe (45%).

Regarding exclusively mass transportation entities (operators, infrastructure managers), one relevant factor is the size of each operator domain, namely the population of the city/area where each entity operates in.

In this direction, the mass transportation entities who have participated in this survey can be divided in two different categories:

- Companies that operate (or manage) in regional/national transport networks, with several transport nodes and always covering highly-populated areas (always over one million inhabitants). They represent 54% of the mass transportation entities interviewed.
- Transport entities that operate in one city and its metropolitan area (in all cases over one million inhabitants). They make 46% of the mass transportation entities interviewed.

The conclusions are made upon eleven main security areas namely:

- Security Management System.
- Comprehensive threat detection.
- Risk assessment-based command and control.
- Intelligence.
- Cyber defence.
- Passive protection systems.
- Preventive and early intervention.
- Post-incident intervention and restoration of services.
- Forensics.
- Learning and training.
- Interoperability and information interfaces.
- Implementation of security technologies.
- Security perception/ Future Situation.

### **3 CURRENT STATUS OF SECURITY IN MASS TRANSPORT.**

Regarding security organizational aspects, most of the mass transportation entities have specific departments for security issues with dedicated resources. The only exception are relatively small local transport operators.

The above mentioned security department is in close contact with Local or National Authorities with responsibility in security issues (e.g. councils), police forces, and in some cases other transport entities.

At the same time, there is a lack of a formal, based on national or European standards security management system.

Threat analysis is performed by most of the operators since it is considered as one of the most important parts of the security process. It is commonly performed through a collaborative framework between operators and intelligence services.

Threat scenarios may include up to fifty threats, such as spread of pandemics, threats to water supply, IT failures, terrorism and even natural catastrophes.

When detecting and classifying potential threats for mass transportation assets, low severity acts (robbery, assaults, vandalism) are commonly prioritized than other threats such as terrorism or fire damage since they are much more frequent and transport entities must face them daily.

Although some entities coming from Northern Europe mention some web pages where information is publicly available or their own (publicly available as well) preparedness plan, threat databases are generally kept as confidential.

A list of threat open sources mentioned is included:

[www.securityservice.se](http://www.securityservice.se) (Swedish Security Service)

[www.brs.dk](http://www.brs.dk) (Danish Emergency Management Agency)

[www.pet.dk](http://www.pet.dk) (Danish Security and Intelligence Service)

<http://fe-ddis.dk> (Danish Defence Intelligence Service)

The vulnerability analysis is commonly performed in conjunction with the corresponding National Security Authority in order to study the consequences of eventual malicious attacks. In this task, antagonistic threats are not a primary focus.

This task includes ICT vulnerabilities in order to prevent cyberattacks. The usual ICT vulnerability is the one associated to a complete disruption of IT systems.

In general, it is a weakly-standardised process in mass transportation security. In some cases, entities can lean on some national security rules, but vulnerability analysis is mostly developed based on the background experience.

The only formal method mentioned is the so-called “MVA-method” (Multi-dimensional work analysis), which is a process-based method for analysing organisational vulnerabilities. The method has been developed by Human Geography researchers (Per Olof Hallin and Jerry Nilsson) at the universities of Lund and Malmö. More information can be found at [mva-metoden.se](http://mva-metoden.se).

Stakeholders currently implement procedures for detecting, tracking and tracing abnormal behaviour. The usual method consists merely in surveillance through CCTV from the Control Centres by security staff.

Recognition techniques are not implemented by the majority of the mass transportation entities. Those who perform it, only rely on the security staff (both private companies and police forces) to recognize people who are already in their own records.

Mass transportation companies monitorize their own transport network for security purposes, this task usually involve their own staff joined by private security staff. The technologies used are CCTV joined by detection systems and access control devices.

It is also important to remark that monitoring is also performed with other purposes in mind (e.g., ticket control). Depending on the transport entity, the resources to be committed may be insufficient to perform extensive monitoring exclusively for the purpose of security.

Video surveillance is an increasing security measure in the mass transportation networks. Starting from the major stations, it is also being implemented in a increasing number of facilities and also trains and buses.

Transport entities also implement detection and identification of unwanted entities in the surroundings of the transport critical infrastructures. They rely on police forces to perform this task.

The technological tools used for this task are CCTV, detection systems (such as volumetric sensors in electrical substations or infrared detection systems for detecting falling objects in the entrance of tunnels), image processing and K9 patrols.

Entry points are commonly supervised by transport operators, although in some cases it is only performed in the major stations. Multimodal operators are even less strict regarding this issue, since most of them admit not to supervise entry points.

CCTV is again the technology chosen to perform this task by the mass transportation entities, in some cases it is used with detection systems. The use of screening checkpoints is limited to air transport.

The detection of abandoned luggage is developed in most of the mass transportation assets, combining security agents assisted by K9 patrols and CCTV surveillance. Nevertheless, in most cases it is only performed in major stations.

Multimodal operators show a wide variety of answers on this issue: while some admit not implement detection procedures for abandon luggage others declare they even perform it inside the buses.

CBRN is labelled as a threat for most of the mass transportation entities, although it is not considered as one of the priorities of mass transportation operators in terms of security. In some cases CBRN protection procedures are only applied in specific periods of time following instructions from the intelligence services. One multimodal operator denied answering this issue considering it as classified information.

In contrast, it turns to be a more important issue for first responders, especially Fire Brigades. Some of them coming from Northern Europe even have a special unit trained for CBRN threats. In case of CBRN-related crisis they manage and perform operations although they have are not responsible for the detection. More precisely, fire and rescue services are primarily concerned with chemical threats. For this issue, they use a portable container with a full set of equipment, including equipment for detection.

Command and control centres are considered as the key tool for security purposes. In general, they are managed by both public and private security entities together with personnel from the corresponding operator /infrastructure manager. In some cases they may be joined by workers belonging to the ICT service provider which developed the Control Centre.

These centres are conceived mainly as Alarm Reception Centres (ARC) working in conjunction with CCTVs and detection systems (such as intrusion detection systems). Most of the operators (both multimodal and specific rail ones) implement risk assessment in the daily operation of their control centres, checking regularly the received alarms and evaluating carefully each situation before intervention.

Some stakeholders from northern and southern Europe implement a network consisting on local control centres combined with a central control centre providing an overview.

Transport entities in charge of medium-sized metropolitan areas state that surveillance centres are not exclusively dedicated to security since resources are not sufficient for this activity.

The information gathered from the stakeholders mirrors that there is a constant communication between public transport entities and intelligence service.

Cyber-protection is a field yet to be completely covered by mass transportation operators, and it mainly lies on the intrinsic protection provided by the corresponding communication system (GSM-r, TETRA, etc). This task (when performed) is developed exclusively by the operator's personnel.

In the very few cases where robust encoding is performed, the methods mentioned are:

- Radio based communication.
- Encrypted text+radio based communication systems following national standards.
- Northern Europe first responders use a encrypted system for their communication called "Raket". This system is currently being tested by mass transport operators, but not yet implemented.

To have a digital communication network is mentioned as a protection measure itself since protection is part of the standard.

Fire protection is one of the highly considered areas in terms of security by the mass transportation actors, and therefore is well covered by them.

The responsibility for fire protection implementation belongs to the operator / infrastructure manager. To some extent, passive fire prevention is regulated or imposed by law, although is the mass transportation company who decides the equipment and systems to be installed.

One measure mentioned by a Northern Europe multimodal operator is to implement fireproofing materials. This is especially significant on busses, especially buses using natural gas.

Person access control is implemented by the vast majority of the operators. Access control is generally performed by the operator's personnel together with outsourced security companies and it is focused on access to both facilities and control centres.

Resilience criteria are generally taken into account by rail entities, but it only applies to relatively new facilities. In some countries, building technical norms already provide specific requirements for critical transport infrastructures. The most likely to intervene in this task are fire experts in order to ensure that the infrastructure is properly protected against potential damage effects. For instance, a fire expert coming from northern Europe affirms that tunnels are not adequately constructed for withstanding explosions.

Although some of the representatives interviewed weren't sure of the meaning/scope of the question and consequently didn't answer it, the majority of mass transportation

stakeholders stated clearly that they have specific protocols to achieve a quick response if needed.

In this area first responders feedback is very relevant.

In best cases, all the first responders (police, fire brigade and ambulance services) are notified at the same time by a “triple-alarm” whenever an incident is reported. Once in the incident scene is the police who decides the steps to be taken by the rest of the entities.

Some of the inquired did not mention external organization regarding this task. Those who did named police and national security forces in conjunction with internal personnel. Some also listed national or regional security authorities, therefore it seems that this task is managed by a higher security level.

A first responder from Northern Europe states that there is no specific model for mass transport systems since the intervention model is prepared for specific types of situations, including metro and commuter train fires. At the same time there is a system belonging to the Metropolitan Area Emergency and Rescue Service where information from service operators, as well as updated information from cameras, is processed together with databases containing procedures for specific situations.

Neutralisation measures are implemented by most of the stakeholders. The basic scheme is internal personnel plus first responders (police, firemen, health assistance depending on the services needed) and outsourced security companies.

More than half of the interviewed stakeholders decided not to specify their neutralisation measures. Those who did mentioned:

- Coordinated intervention of police and internal personnel to isolate the affected area.
- Panic avoidance.
- The existence of crisis managers who validates every step taken. Those steps should come from a previously designed checklist.
- The final aim of this task should be the normalisation of traffic.
- Measures against CBRN threats, only for neutralising chemical substances performed by fire brigade.
- Ambulance services mention evacuation, first aid to injured passengers, emergency procedures in connection with life-threatening conditions.
- Fire fighters' from Northern Europe mentions that it is part of the fire fighters' obligations to salvage what remains of assets that have been damaged, and to take adequate measures for this purpose. When such measures are acute, the fire and rescue service is authorised to acquire resources for this. More information can be found at [www.rvr.nu](http://www.rvr.nu).

Regarding formal rescue procedures, the idea of specific procedures for specific events comes again. In this case, there are “building blocks” of procedures for specific situations (e.g. emergencies on auto busses).

In any case, the responsibility is on the operator. Metro and commuter trains are constructed in order to facilitate self-evacuation. There are specific systems, such as smoke-repelling fan systems, that are implemented in order to rescue passengers. But most of these systems are still under evaluation.

Formal rescue procedures are applied extensively in the mass transportation domain. The police have procedures for management of an accident scene in the case of major accidents/catastrophes.

Taking into account that restoration of services is a basic part in every response model and in light of the answers collected from multimodal operators, the existence of a gap regarding this issue can be inferred. In contrast, the majority of rail /metro entities declare to have a restoration of services protocol implemented.

Anyway, all depends on the magnitude of the damage. Services can be restored after a relatively minor damage, such as an isolated fire, by remedying procedures. But existent models are not adequate for situations comparable to the London or Madrid bombings.

One real example are the procedures used to remove smoke and moisture in the tunnels, at the acute stage of the situation, in order to make transport operations possible again.

Damages are thoroughly evaluated after suffering an attack, including not only direct damages but also indirect ones (due to service or systems disruption).

This is a significant responsibility of fire brigades, in conjunction with insurance companies.

Post-event data analysis is performed by the vast majority of the operators. The common scenario drawn by the stakeholders consulted is made of internal personnel cooperating with police forces or outsourced security companies. Sometimes it is only based in workshops.

Most of the stakeholders have this kind of database. Alternatively, some of them include security issues within a more general incident register which also covers safety issues, namely an alarm reporting system that allows for information search.

Information on emergency operations is stored in databases, but general investigations are not systematically registered or archived.

Mass transportation stakeholders not only confirm that they perform learning and training programmes, but also remark the importance of creating a security culture among their employees. This way, the cooperation between their own staff and security entities (so common in light of the results provided by this report) becomes more efficient.

There are several different trainings and exercises on location, both with personnel from the corresponding stakeholder and with personnel from other organisations, and both during the construction phase and during the operating phase of the transport system.

The training programs (which include also online educational programs in some cases) cover aspects such as awareness about security protocols and prevention.

Training programs are performed by human resources departments and also security experts coming from training centres and security companies.

It is clear that communication and data sharing between security and operational areas is performed by most of the stakeholders inquired. Not only that, stakeholders also are in contact with different kinds of entities such as meteorological institutes providing data to warn against floodings or potential natural disasters.

Public transport (in contrast with the aeronautical side) suffers a lack of security standards that limits interoperability and pushes operators to develop their own security protocols bases only on experience and their own needs.

The decision about the resources to be dedicated to security are based both on economic factors and the national security regulation.

Furthermore, stakeholders analyze carefully the maturity of the technology to be implemented.

Also it is important to have "Sufficient human resources" meaning both that there is competence and manpower to adequately use new technologies. The technology in

question, as well as the organisation, must be mature; the management is risk-averse when it comes to implementing new technologies.

While Multimodal operators mention the next issues as the top requisites to fulfil:

- The flow through / normal operation should be hindered as less as possible.
- Minimize the cost and the interruption of services and maximize the ease of implementation and use.

Rail metro operators /infrastructure managers prioritize the following aspects:

- To have easily available information on current threats together with a set of plans adapted to the current threats.
- Develop actions to promote a safe, secure and comfortable trip for the passengers.
- To ensure that measures implemented have been properly tested and therefore provide enough reliability.
- To increase the number of communication devices between passengers and security personnel, CCTVs and also the information given to the passengers through screens and PA systems.
- The development and implementation of new security systems shall not affect the daily transport operations.

Police forces demand more resources assigned to Control Centres, which should be 24/365, allowing an immediate and continuous communication between police and operators involved.

In general, people are positive to increased security, but video surveillance is a controversial issue.

The desirable situation for the future regarding mass transportation security in general can be summarized as an increase in human resources combined with adequate technology, subject to economic constraints.

Another aspect to improve is to increase both the participation and competence in case of an emergency. In particular, this applies to the technical systems; since people in general have too much confidence in the systems that their security depends on, are often ignorant of the limitations of such systems, and can rarely deal adequately with situations where such systems fail.

Furthermore, security should be considered more at the design stage. Mass transportation security should rely less on cheap and automated systems, but more on human competence. Fire fighters cannot rely on improvised solutions in their work; emergency procedures must include adequate information and participation from the transport operators or authorities.

First responders mention another goal, which is to create a “security culture”, and to ensure that key decision-makers acknowledge the importance of security. Key decision-makers, including directors/managers of both transport companies and authorities, are more interested in making money, and attracting passengers. To avoid this, security must be marketed where such interests are dominating. The management must be made more attentive to security issues, especially threats with major consequences.

They also mention the need for more research and technological development in order to increase confidence in and awareness of existing capabilities. A specific example concerns work in tunnels; where information management systems must be more

adapted to rescue operations; since fire fighting requires “holistic” information management providing the whole picture of each situation.

The police forces insist in their idea of improving control centres as much as possible and also suggest the idea of creating a specific police body for mass transportation due to its singular characteristics.

The input from the aeronautical side is focused on increasing the awareness regarding security issues of their passengers.

Multimodal operators (only 50% of them gave recommendations) mentioned the need of realistic simulation (namely serious gaming) since exercising is not enough and expensive. They also propose to improve the security in the public transport context by design. Last but not least, to provide a safer environment for bus drivers is also desired.

Operators mentioned the following recommendations:

- Develop simple security analysis procedures as an addition to safety analyses.
- Centralize both safety and security incidents, combining this with the creation of specific security bodies for mass transportation.
- Provide better detection systems for preventing trespassing on tracks.
- Implement identification techniques in entrance areas, and develop better ways of fighting vandalism.
- The development of European rules and directives in the frame of mass transportation.

As it was mentioned in the introduction chapter, we were given some recommendations based on the experiences from and follow-up work after the exercise held in Oslo, 2006.

These recommendations are summarized as follows:

- Establishing a common situational picture for all involved in the crisis is important, but it's also important to consider who will need the information such a situational picture provides. Not to keep things confidential, but to avoid that strategic crisis managers will get bogged down by endless amount of “trivial” information. Sit-picture solutions that also establish roles and aggregate different information sets would be beneficial.
- It is generally important to differentiate between the needs of the operational/tactical personnel on-site, and the strategic level of command, during a crisis.
- The layout and design of crisis command centres is a subject worthy of research. Not least, someone should look at what kind of services and systems does the staff need in order to be efficient.
- Realistic table-top exercises are necessary, since real-time exercises are costly. Solutions for simulation-based exercises, based on simple GIS visualisations, could be helpful.
- Good technological solutions are needed to help transfer of knowledge between staffers for crises that last long (for instance during watch changes).
- A general recommendation is to acknowledge that not all problems and challenges related to mass transport security can be solved by technology. For the most part, procedures for coordination are just as important.

## 4 ANNEX A: QUESTIONNAIRE.

### Part 1: Stakeholder identification.

- Stakeholder's name:
- Stakeholder's category:
- Stakeholder's security role:
- Stakeholder's resources:
- Modes of transport involved:
- General characteristics:

### Part 2: Security questions.

#### Capability 0: Security Management system.

##### *Function 0.1: Security organizational roles.*

Question 0.1.1: Do you have any specific body/division/department in charge of security issues?.

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 0.1.2: Do you interact with other bodies/companies regarding security issues?.

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 0.1.3: Do you have a formal Security Management System (including treatment of documents) based on national or European standards?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

#### Capability 1: Comprehensive threat detection.

##### *Function 1.1: Threat analysis.*

Question 1.1.1: Do you consider threat analysis in the security planning?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 1.1.2: Which entities have been involved in this task?

**Answer:**

Question 1.1.3: What kind of threat scenarios do you use in your planning regarding mass transportation?

Yes

No

**Additional info:**

Question 1.1.4: Are there open national threat descriptions of relevance to urban transportation where closer information can be got (e.g., published studies, reports, literature, databases and other open sources)?

Yes

No

**Additional info:**

*Function 1.2: Vulnerability analysis.*

Question 1.2.1: Has vulnerability analysis been performed regarding mass transportation assets in order to evaluate the impact in the event of malicious acts?.

Yes

No

**Additional info:**

Question 1.2.2: Which entities have been involved in this task?

**Answer:**

Question 1.2.3: Do these analyses include specific ICT vulnerabilities?.

Yes

No

**Additional info:**

Question 1.2.4: Are the vulnerability analyses performed against any national or European standard or formal methodology?

Yes

No

**Additional info:**

*Function 1.3: Detecting, tracking and tracing of abnormal behaviour of individuals.*

Question 1.3.1: Are procedures for detecting, tracking and tracing abnormal behaviour implemented?.

Yes

No

**Additional info:**

Question 1.3.2: Which entities are involved in this task?.

**Answer:**

Question 1.3.3: Which are the systems and technologies being used to meet this function?.

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

*Function 1.4: Recognition techniques.*

Question 1.4.1: Are recognition techniques implemented?.

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 1.4.2: Which entities are involved in this task?.

<b>Answer:</b>
----------------

Question 1.4.3: Which are the systems and technologies being used to meet this function?.

<b>Answer:</b>
----------------

*Function 1.5: Monitoring of network traffic.*

Question 1.5.1: Is your traffic network monitored with security purposes?.

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 1.5.2: Which entities are involved in this task?.

<b>Answer:</b>
----------------

Question 1.5.3: Which are the systems and technologies being used to meet this function?.

<b>Answer:</b>
----------------

*Function 1.6: Detection and identification of unwanted entities in close proximity to critical infrastructures.*

Question 1.6.1: Is any procedure for detection and identification of unwanted entities in close proximity to critical infrastructures implemented?.

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 1.6.2: Which entities are involved in this task?.

<b>Answer:</b>
----------------

Question 1.6.3: Which are the systems and technologies being used to meet this function?.

<b>Answer:</b>
----------------

*Function 1.7: Monitoring of entry points.*

Question 1.7.1: Are entry points monitored?.

Yes

No

**Additional info:**

Question 1.7.2: Which entities are involved in this task?.

**Answer:**

Question 1.7.3: Which are the systems and technologies being used to meet this function?.

**Answer:**

*Function 1.8: Detection of unattended luggage.*

Question 1.8.1: Are procedures for detection of unattended luggage implemented?.

Yes

No

**Additional info:**

Question 1.8.2: Which entities are involved in this task?.

**Answer:**

Question 1.8.3: Which are the systems and technologies being used to meet this function?.

**Answer:**

*Function 1.9: Surveillance*

Question 1.9.1: Is surveillance implemented in mass transportation assets (namely infrastructure and vehicles)?.

Yes

No

**Additional info:**

Question 1.9.2: Which entities are involved in this task?.

**Answer:**

Question 1.9.3: Which are the systems and technologies being used to meet this function?.

**Answer:**

*Function 1.10: CBRN detection.*

Question 1.10.1: Is CBRN (Chemical Biological Radiological & Nuclear) labelled as a threat for mass transportation?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 1.10.2: Is CBRN detection implemented?.

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 1.10.3: Which entities are involved in this task?.

<b>Answer:</b>
----------------

Question 1.10.4: Which are the systems and technologies being used to meet this function?.

<b>Answer:</b>
----------------

**Capability 2: Risk assessment-based command and control.**

*Function 2.1: Command and Control.*

Question 2.1.1: Is there a command and control centre used for security purposes (alternatively: Are security issues implemented in your command and control centres?).

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 2.1.2: Which entities participate in its daily operation?.

<b>Answer:</b>
----------------

Question 2.1.3: Which are the systems and technologies being used to meet this function?.

<b>Answer:</b>
----------------

Question 2.1.4: Do these control centres consider risk assessment?.

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

**Capability 3: Intelligence.**

*Function 3.1: Information management.*

Question 3.1.1: Do you cooperate with the intelligence services, either to get updated threat pictures they can use themselves, or to provide data that can be helpful to other entities?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

**Capability 4: Cyber defence.**

*Function 4.1: Robust encoding.*

Question 4.1.1: Are the communication systems belonging to your transport assets robustly encoded?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 4.1.2: Which entities are involved in this task?.

<b>Answer:</b>
----------------

*Function 4.2: Resilience of communication network from jamming.*

Question 4.2.1: Are jamming resilience measures implemented in the communication network? Which entities are involved in this task?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 4.2.2: Which entities are involved in this task?.

<b>Answer:</b>
----------------

*Function 4.3: Resilience of communication network from heavy noise signals.*

Question 4.3.1: Are any heavy noise signals protection measures implemented in the communication network?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 4.3.2: Which entities are involved in this task?.

<b>Answer:</b>
----------------

*Function 4.4: Resilience of communication network from power Microwave attacks.*

Question 4.4.1: Is the communication network's resilience tested from Microwave attacks?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 4.4.2: Which entities are involved in this task?.

**Answer:**

**Capability 5: Passive protection systems.**

*Function 5.1: Fire protection.*

Question 5.1.1: Is passive fire protection implemented within transport infrastructures? Which entities are involved in this task?

<b>Yes</b> <input type="checkbox"/>	<b>No</b> <input type="checkbox"/>
-------------------------------------	------------------------------------

**Additional info:**

*Function 5.2: Person access control.*

Question 5.2.1: Is person access control implemented?

<b>Yes</b> <input type="checkbox"/>	<b>No</b> <input type="checkbox"/>
-------------------------------------	------------------------------------

**Additional info:**

Question 5.2.2: Which entities are involved in this task?

**Answer:**

*Function 5.3: Design of resilient buildings.*

Question 5.3.1: Have resilience criteria been taken into account in the design of mass transportation infrastructures?

<b>Yes</b> <input type="checkbox"/>	<b>No</b> <input type="checkbox"/>
-------------------------------------	------------------------------------

**Additional info:**

Question 5.3.2: Which entities have been involved in this task?

**Answer:**

**Capability 6: Preventive and early intervention.**

*Function 6.1 Early intervention.*

Question 6.1.1: Do you have an early intervention model in order to avoid propagation?

<b>Yes</b> <input type="checkbox"/>	<b>No</b> <input type="checkbox"/>
-------------------------------------	------------------------------------

**Additional info:**

Question 6.1.2: Which entities have been involved in this task?

**Answer:**

**Capability 7: Post-incident intervention.**

*Function 7.1: Neutralisation.*

Question 7.1.1: Are neutralisation measures implemented in the event of malicious acts?.

<b>Yes</b> <input type="checkbox"/>	<b>No</b> <input type="checkbox"/>
<b>Additional info:</b>	

Question 7.1.2: Which entities are involved in this task?

<b>Answer:</b>
----------------

Question 7.1.3: What do these measures consist on?

<b>Answer:</b>
----------------

*Function 7.2: Rescue.*

Question 7.2.1: Is there a formal passenger rescue procedure implemented in the whole security system?.

<b>Yes</b> <input type="checkbox"/>	<b>No</b> <input type="checkbox"/>
<b>Additional info:</b>	

*Function 7.3: Restoration of services.*

Question 7.3.1: Does your incident response model contain a restoration of services procedure to be implemented in the event of malicious acts?

<b>Yes</b> <input type="checkbox"/>	<b>No</b> <input type="checkbox"/>
<b>Additional info:</b>	

Question 7.3.2: Which entities have been involved in its definition?

<b>Answer:</b>
----------------

**Capability 8: Forensics.**

*Function 8.1: Damage assessment.*

Question 8.1.1: Is damage assessment systematically performed after suffering an attack?

<b>Yes</b> <input type="checkbox"/>	<b>No</b> <input type="checkbox"/>
<b>Additional info:</b>	

Question 8.1.2: Which entities are involved in this task?

<b>Answer:</b>
----------------

*Function 8.2: Post -event data analysis.*

Question 8.2.1: Are post-event situation analysis systems used in order to re-enact the sequence of a malicious event?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 8.2.2: Which entities are involved in this task?

<b>Answer:</b>
----------------

Question 8.2.3: Do you have a database collecting information from previous malicious acts?.

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 8.2.4: Is this used as an input to be included in your security systems?.

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 8.2.5: Which entities are involved in this task?.

<b>Answer:</b>
----------------

**Capability 9: Learning and training.**

*Function 9.1: Learning and training procedures.*

Question 9.1.1: Does your entity develop crew learning and training programmes?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 9.1.2: What do they consist of?

<b>Answer:</b>
----------------

Question 9.1.3: Which other entities are involved in this task?

<b>Answer:</b>
----------------

**Capability 10: Interoperability and information interfaces.**

*Function 10.1: Information interfaces.*

Question 10.1.1: Do your entity's security systems interface with other internal systems (such as operational)?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 10.1.2: Does your entity's security system architecture and its interfaces follow any technical standard?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

*Function 10.2: External interoperability.*

Question 10.2.1: Are security systems implemented following any technical standard, national or European Regulation? Which entities have been involved in this task?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 10.2.2: Are your security systems interconnected with security systems belonging to similar entities within the European Framework?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

Question 10.2.3: Are your security systems interoperable with other similar entities in the European Framework?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Additional info:</b>	

**Capability 11: Implementation of security technologies.**

*Function 11.1: Decision-making in mass transportation security systems.*

Question 11.1.1: What are the main user requirements for security measures to be taken?

<b>Answer:</b>
----------------

Question 11.1.2: Which are the key decision factors to implement new technologies within your security system?

<b>Answer:</b>
----------------

Question 11.1.3: Are societal/ethical aspects taken into account before implementing a new security system or technology?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

**Additional info:**

**Capability 12: Security perception/ Future Situation**

*Function 12.1: Security perception*

Question 12.1.1: Do you think passengers have a positive perception regarding security measures implemented in mass transportation?

Yes

No

**Additional info:**

*Function 12.2 Desirable situation of mass transportation security in the near future*

Question 12.2.1: What are your recommendations or demands for the near future in the frame of mass transportation security?

**Answer:**

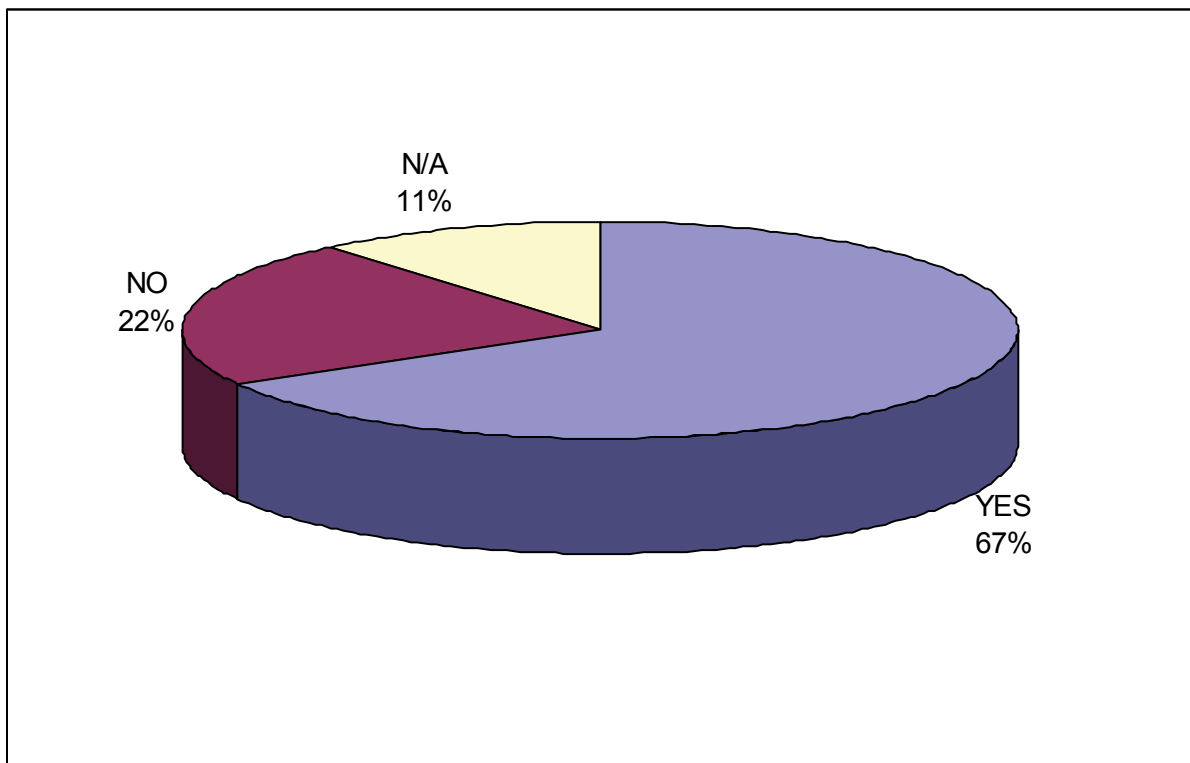
## 5 ANNEX B: STATISTICAL ANALYSIS OF STAKEHOLDERS' FEEDBACK.

The data collected come from four different stakeholders' categories, namely first responders (represented on this report only by police forces operating within mass transportation scope), multimodal operators, rail infrastructure managers/ rail operators (labelled as operators in the document) and aeronautical companies. This last category has been included as a specific input from the aeronautical side into the public transport, since some security aspects are further developed in the aeronautical domain.

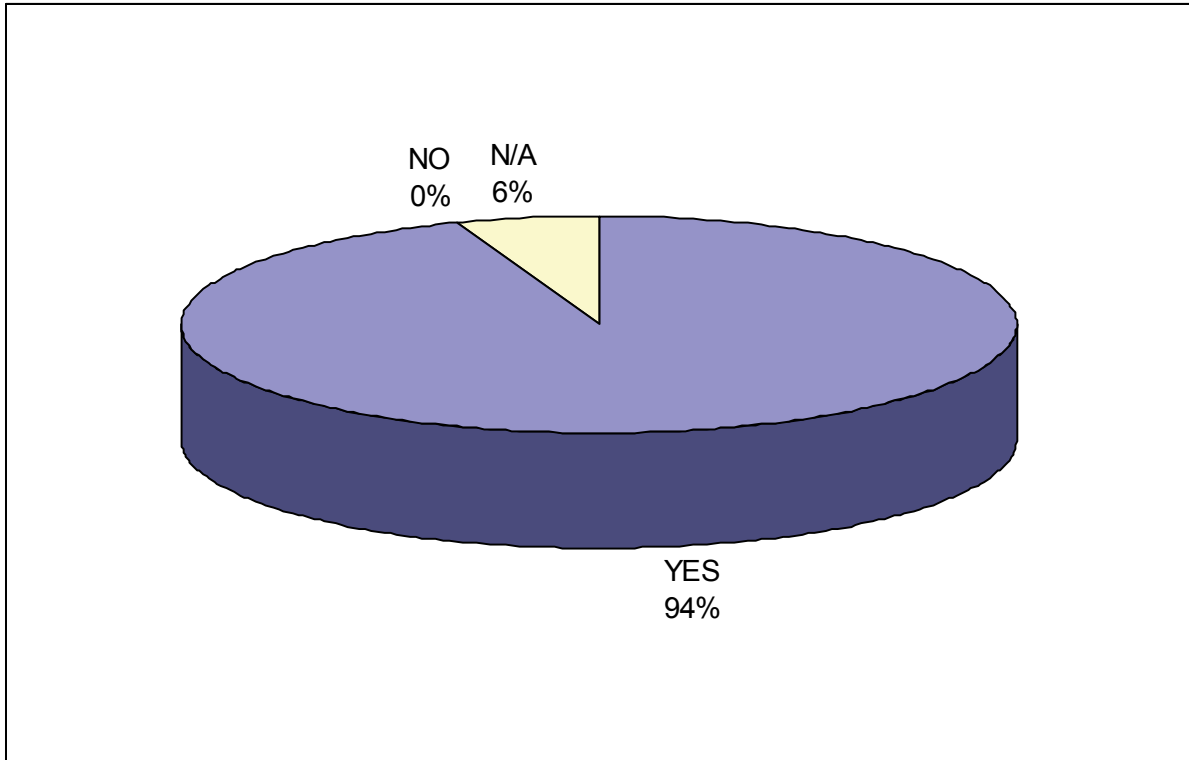
### 5.1 Security Management system.

#### 5.1.1 Security organizational roles.

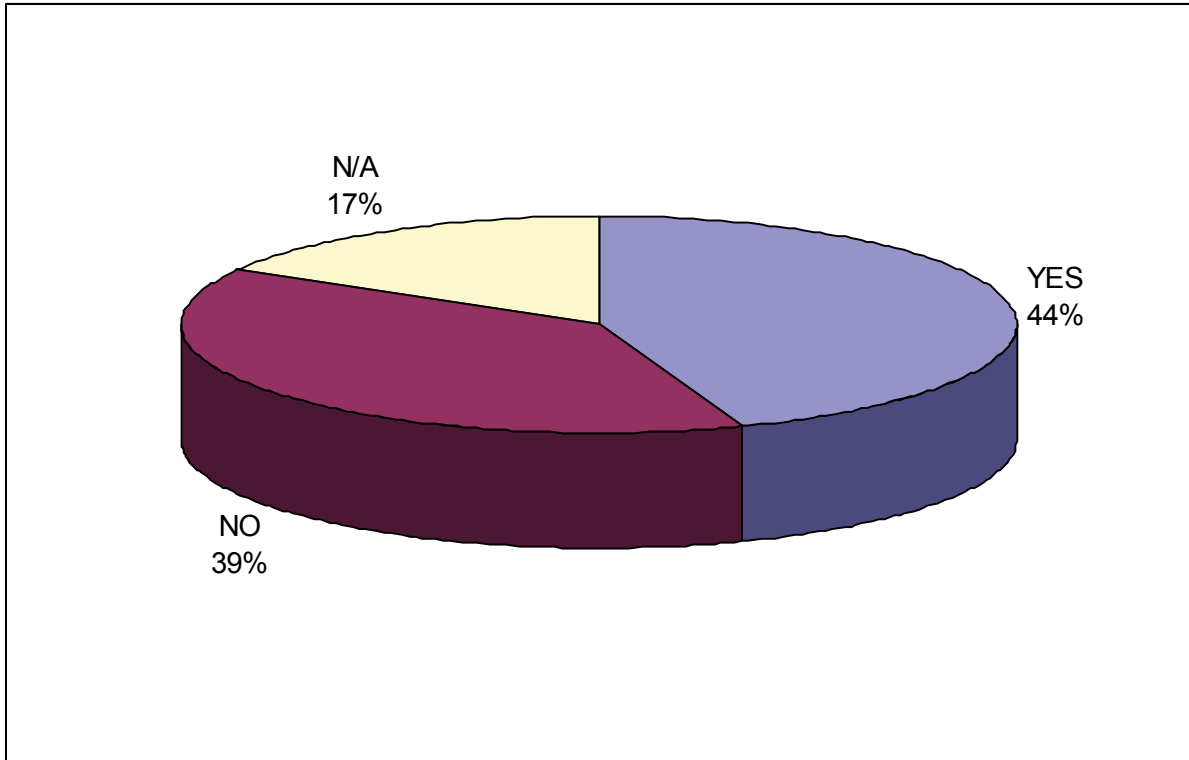
Do you have any specific body/division/department in charge of security issues?



Do you interact with other bodies/companies regarding security issues?



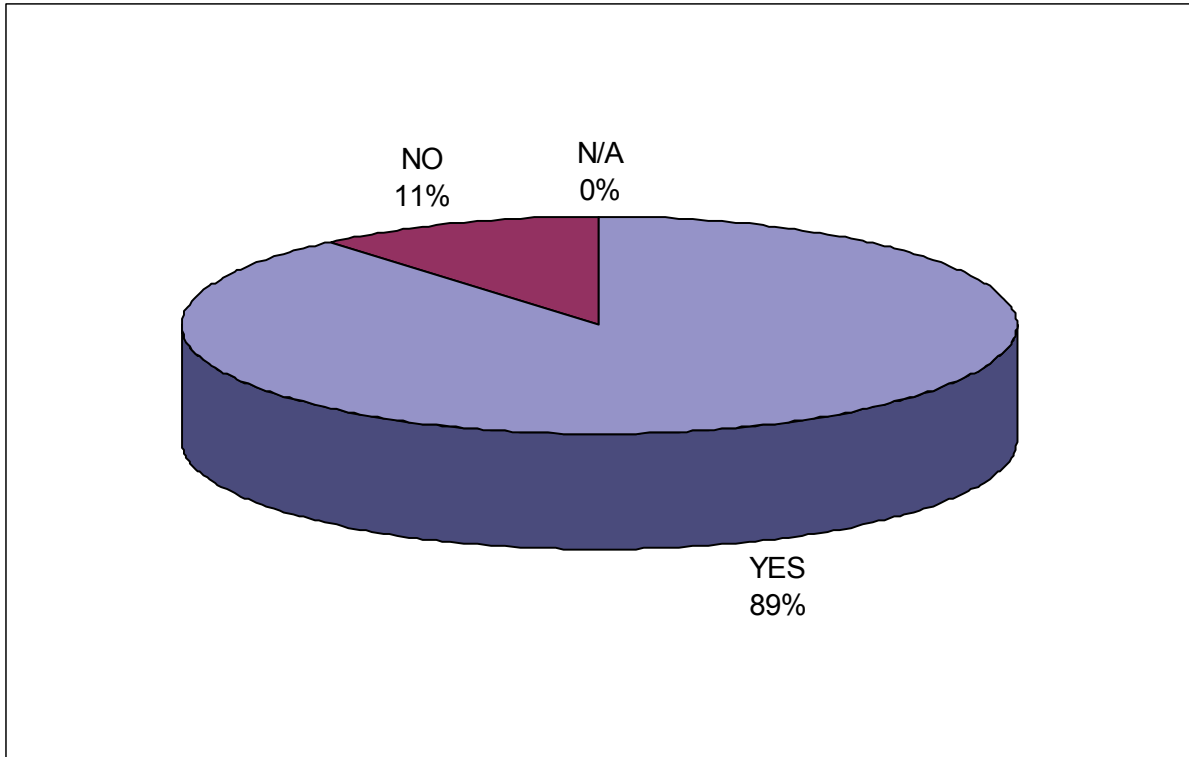
Do you have a formal Security Management System (including treatment of documents) based on national or European standards?



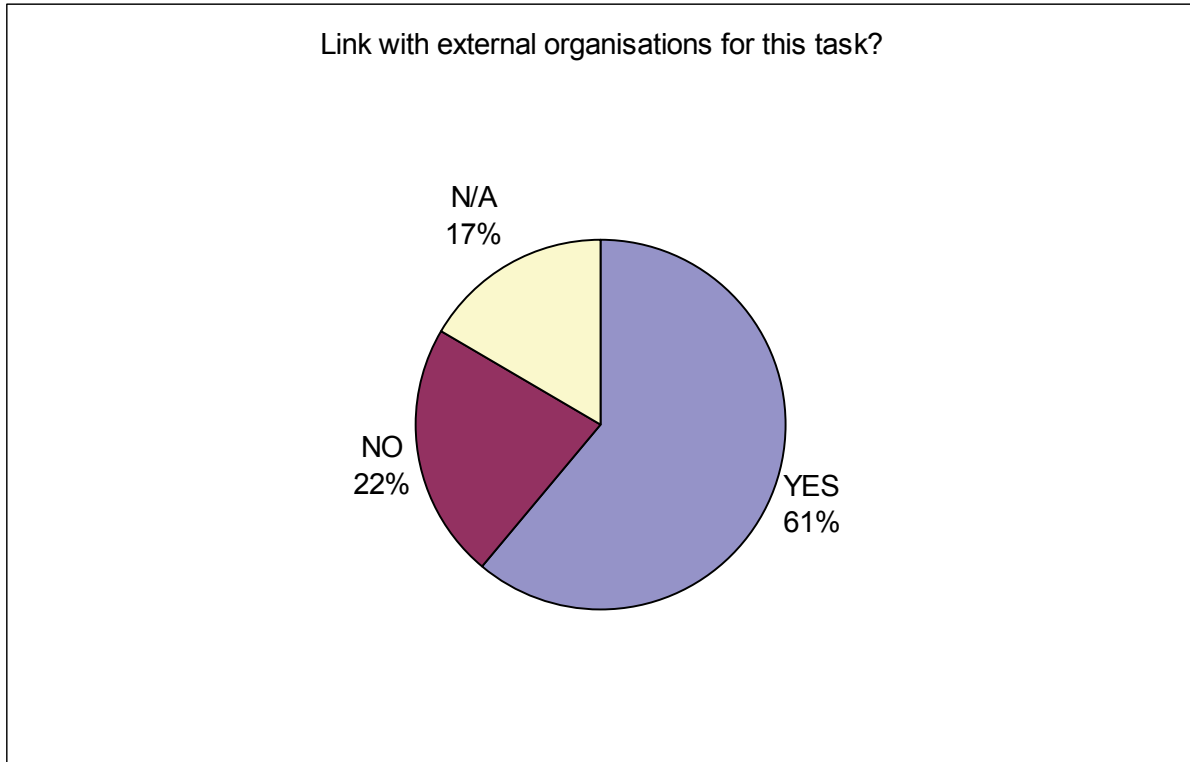
Comprehensive threat detection.

5.1.2 Threat analysis.

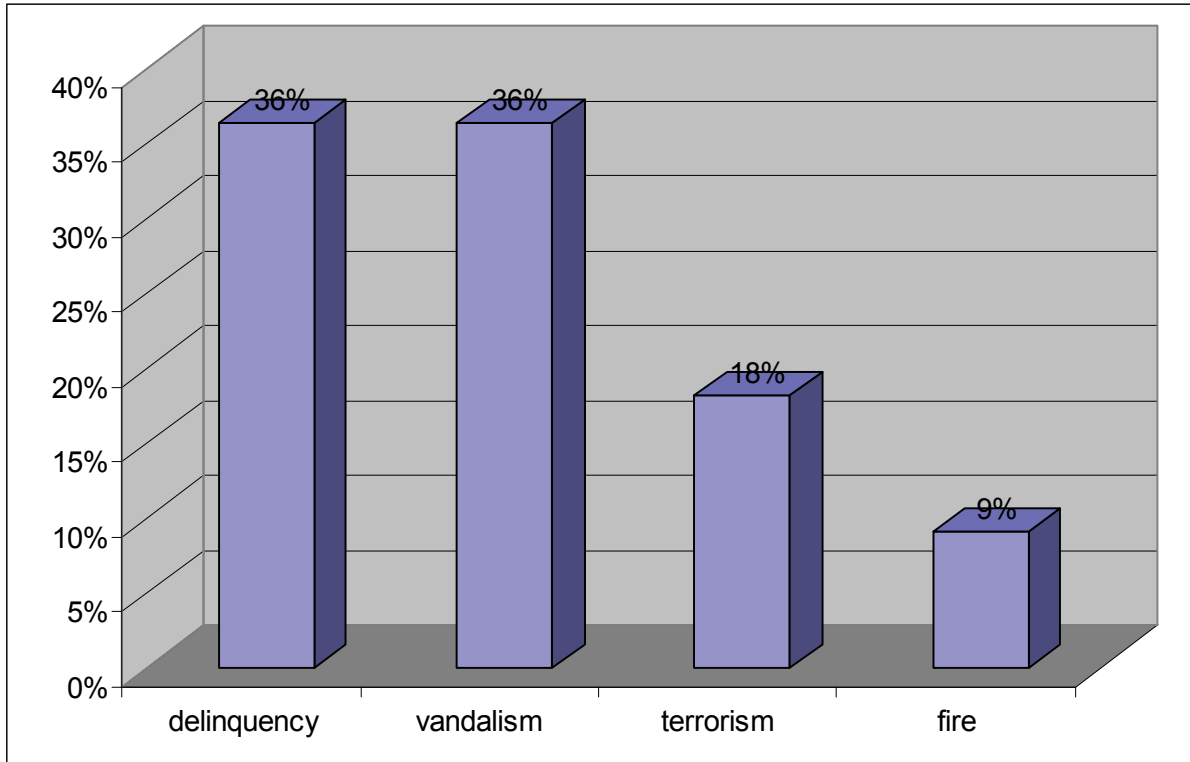
Do you consider threat analysis in the security planning?



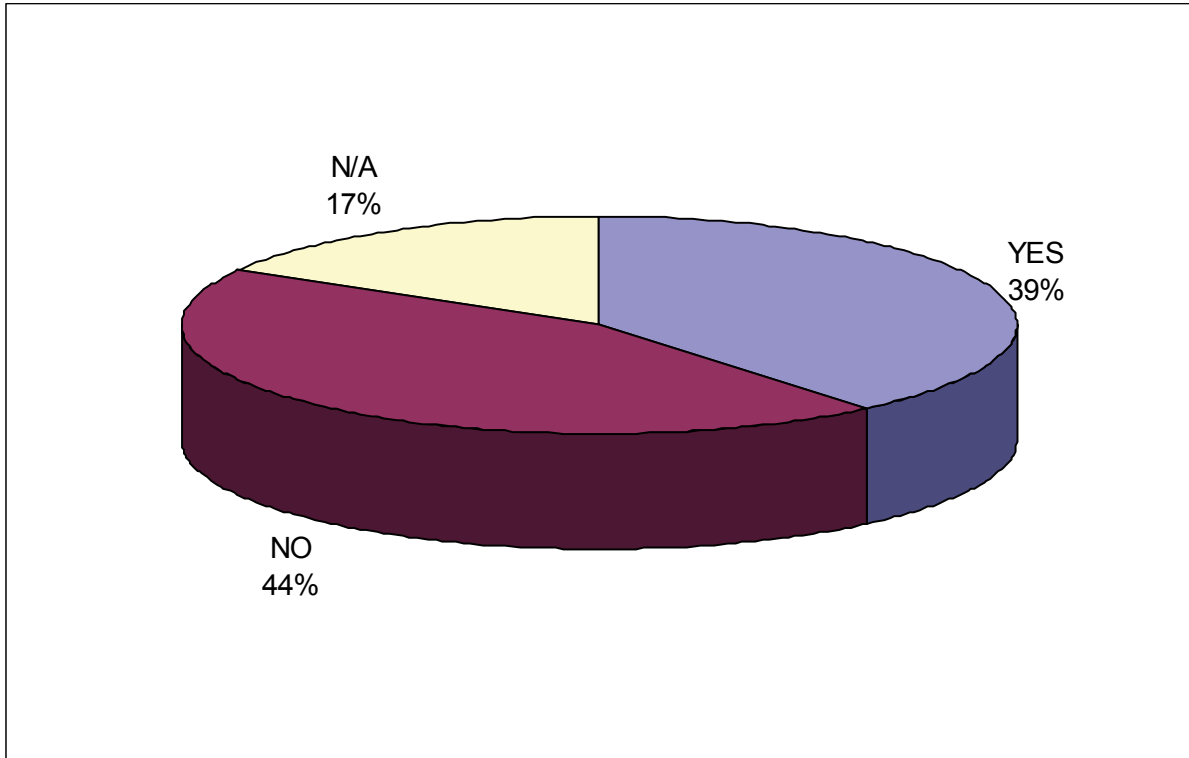
Which entities have been involved in this task?



What kind of threat scenarios do you use in your planning regarding mass transportation?

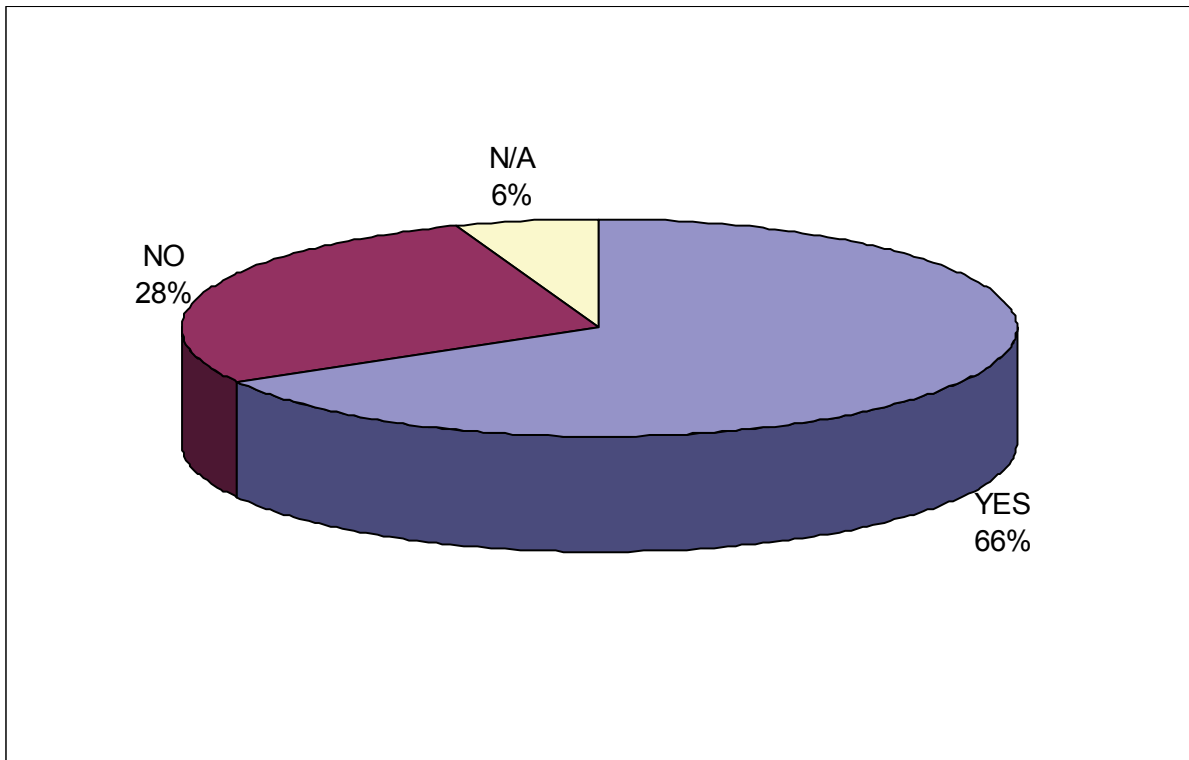


Are there open national threat descriptions of relevance to urban transportation where closer information can be got (e.g., published studies, reports, literature, databases and other open sources)?

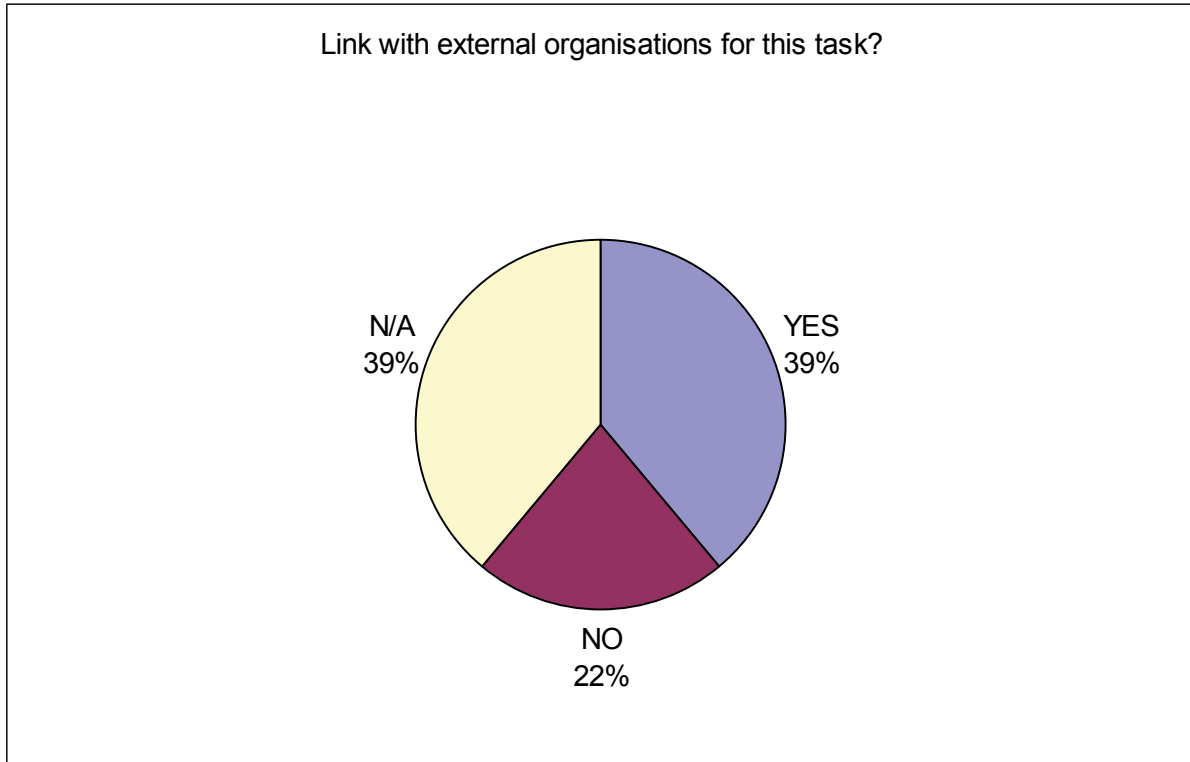


5.1.3 Vulnerability analysis.

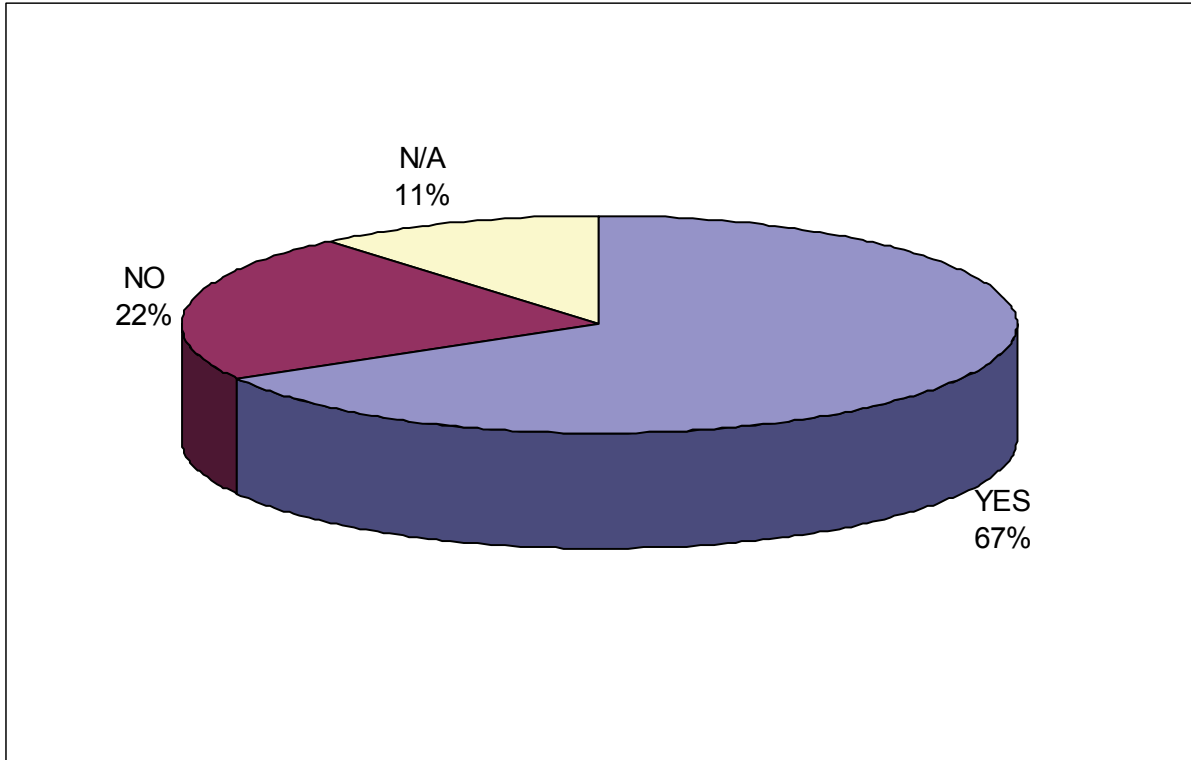
Has vulnerability analysis been performed regarding mass transportation assets in order to evaluate the impact in the event of malicious acts?.



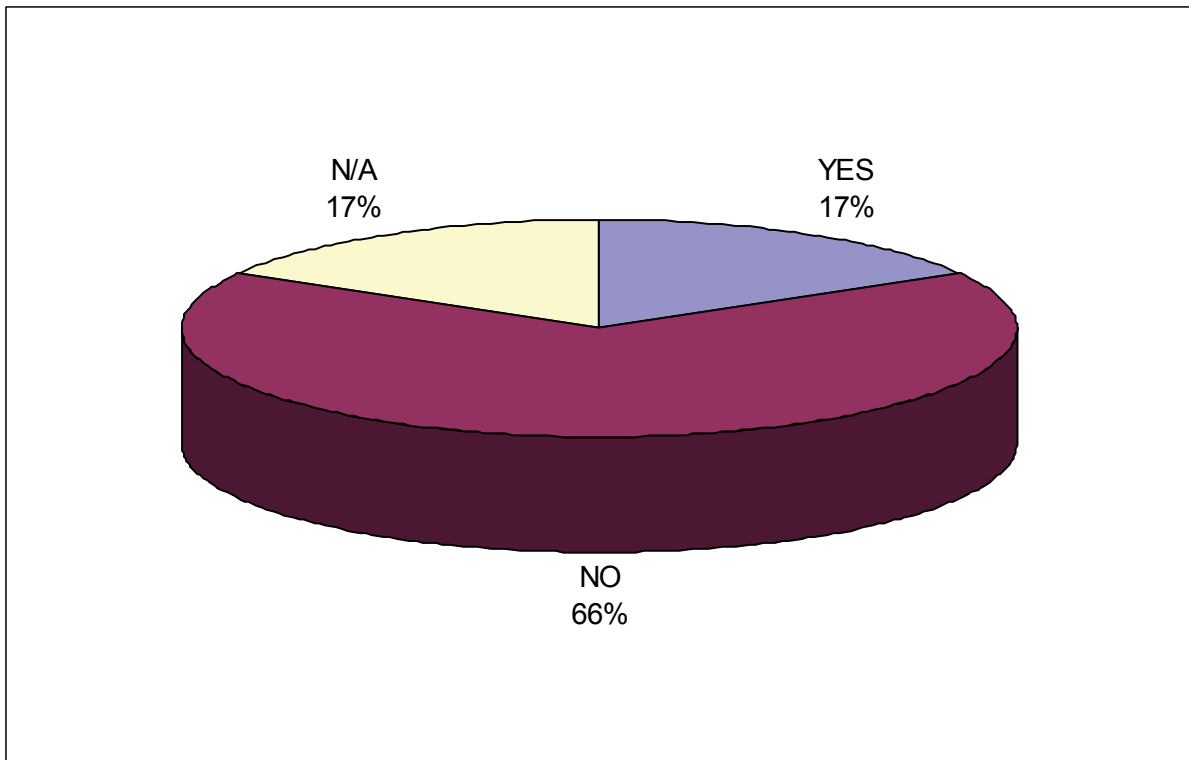
Which entities have been involved in this task?



Do these analyses include specific ICT vulnerabilities?

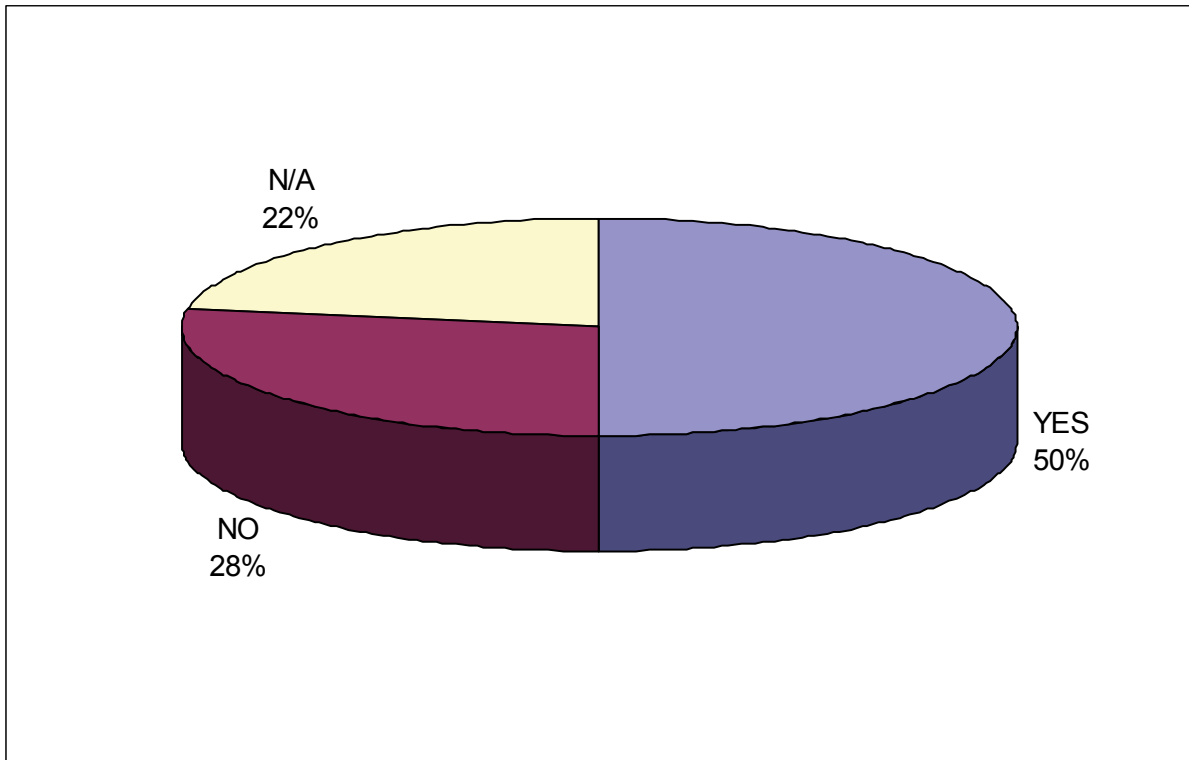


Are the vulnerability analyses performed against any national or European standard or formal methodology?

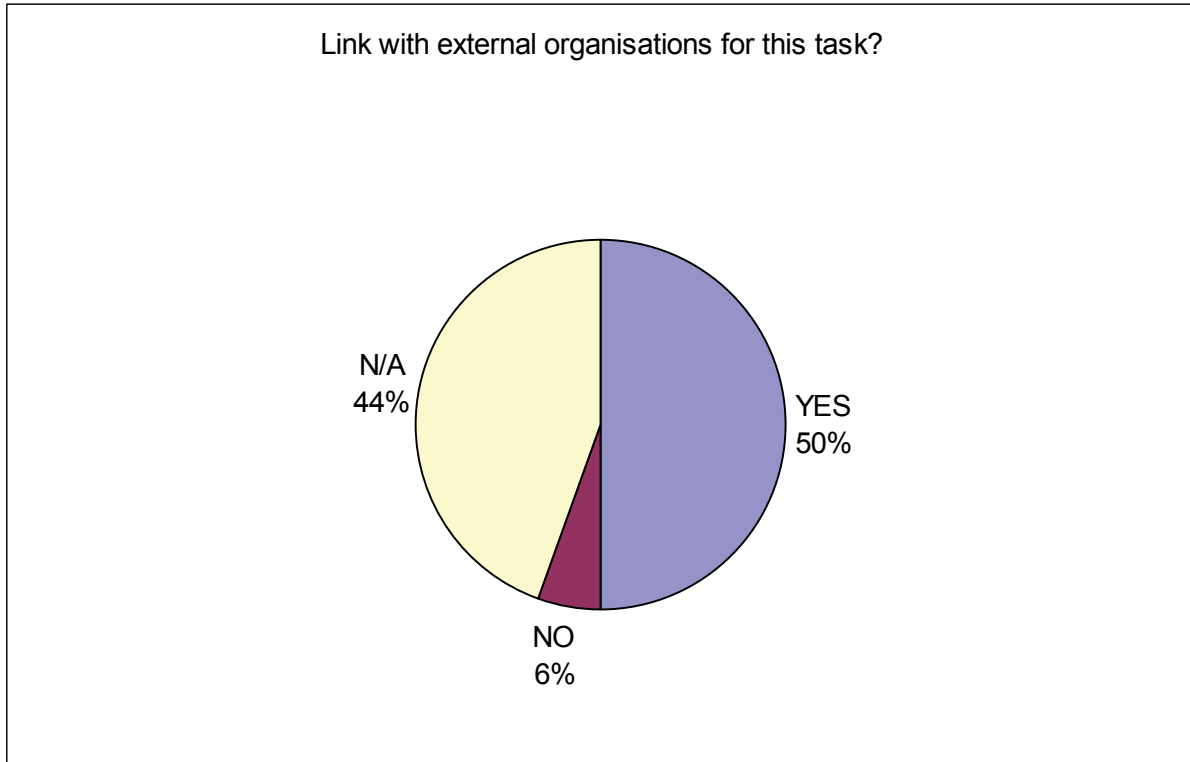


5.1.4 Detecting, tracking and tracing of abnormal behaviour of individuals.

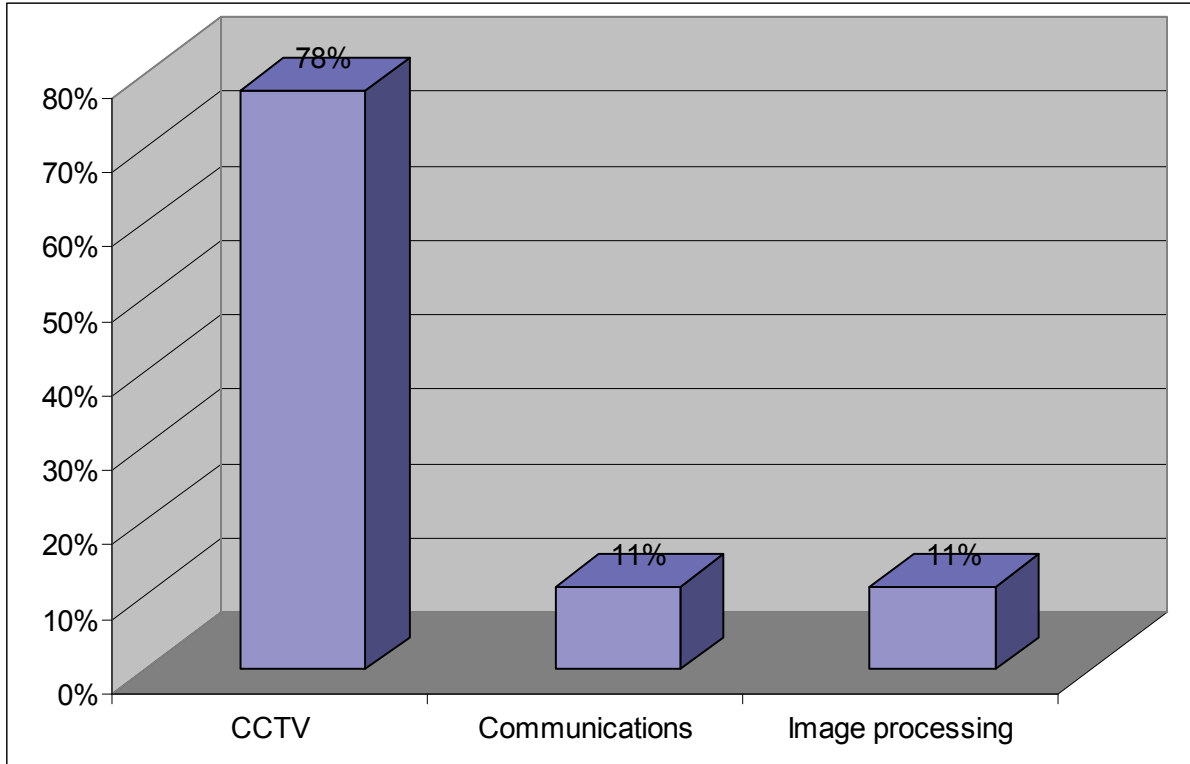
Are procedures for detecting, tracking and tracing abnormal behaviour implemented?



Which entities are involved in this task?

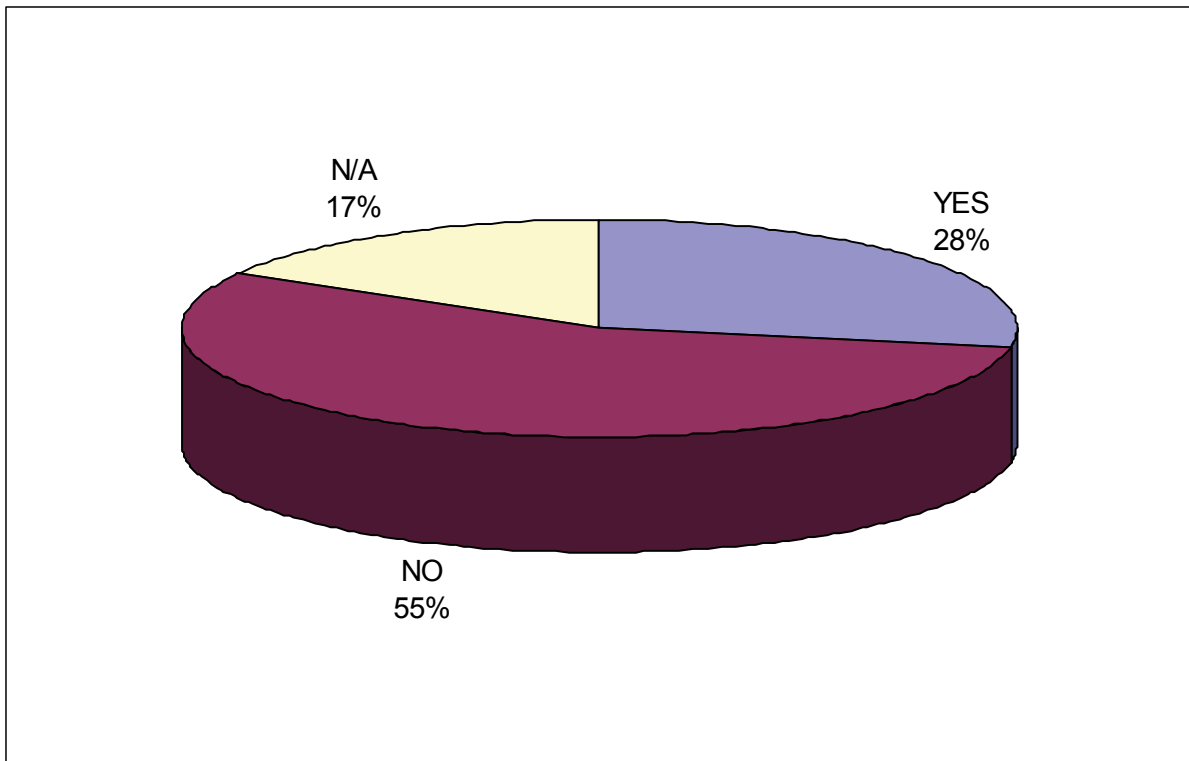


Which are the systems and technologies being used to meet this function?



5.1.5 Recognition techniques.

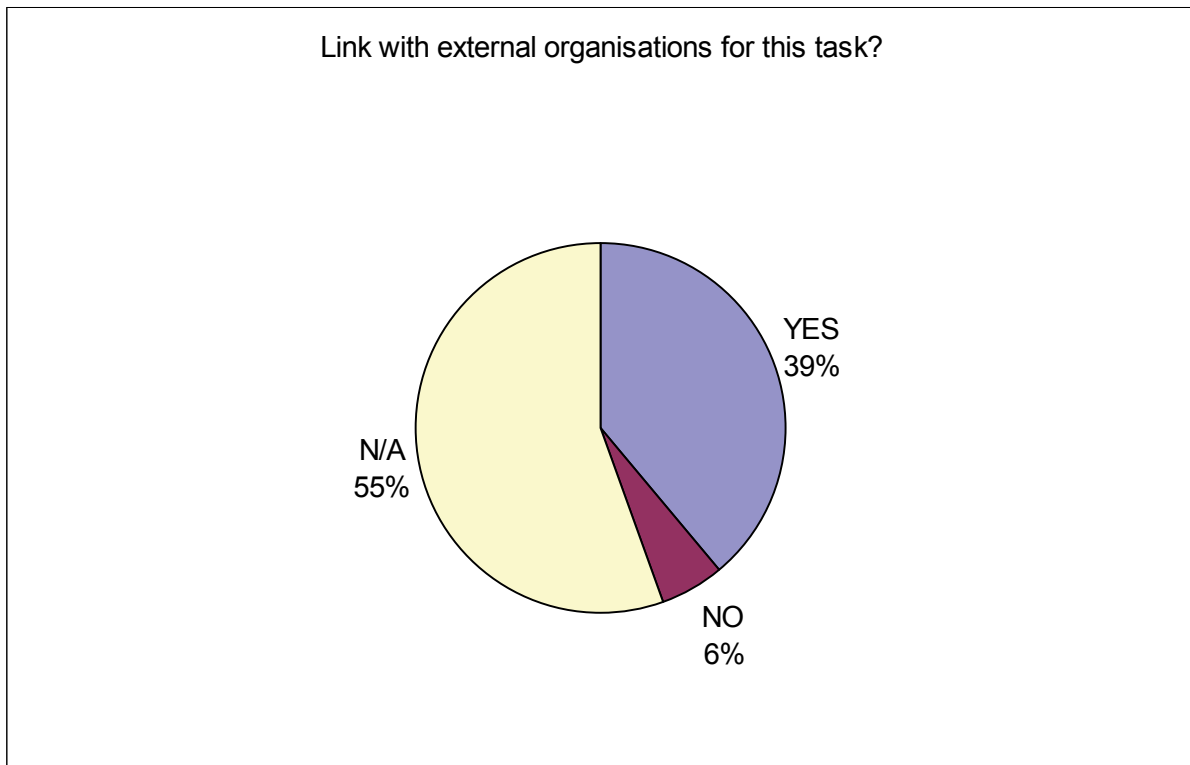
Are recognition techniques implemented?



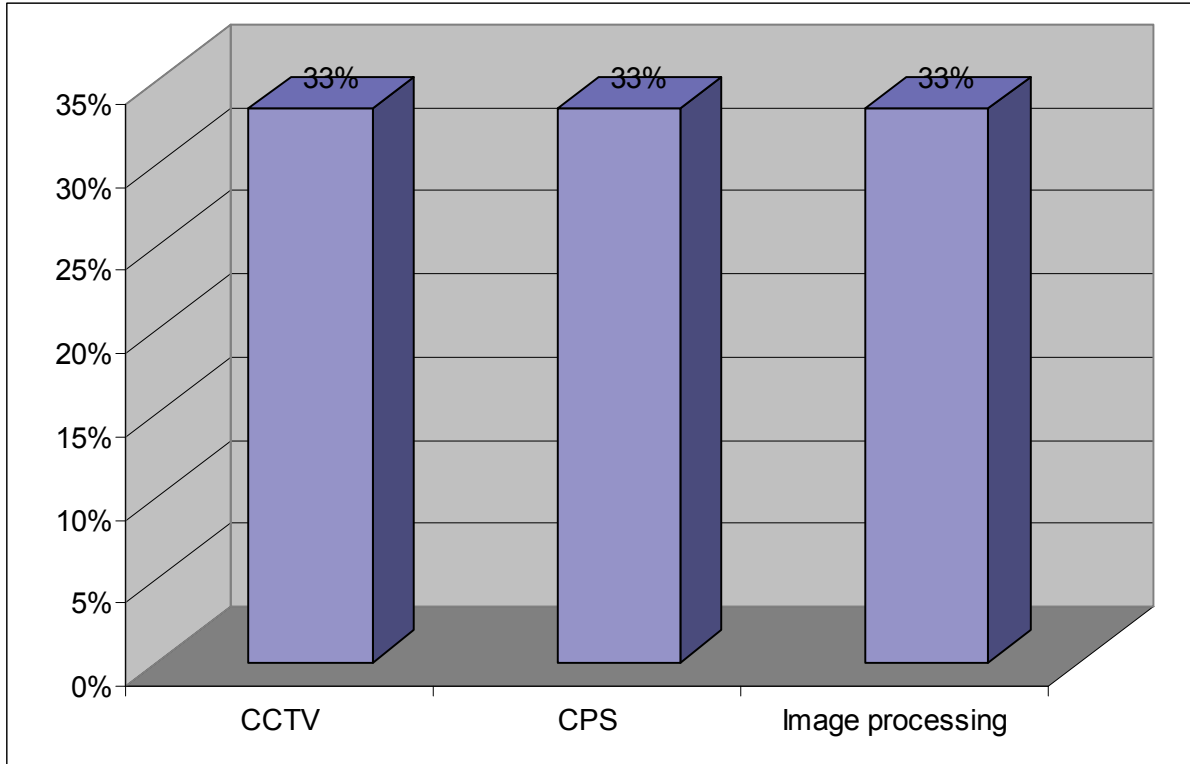
Which entities are involved in this task?

**Conclusions:**

Although some entities (50% approximately) did not answer this question, those who did, affirmed that in most of the cases security forces (both public and private) are in charge.

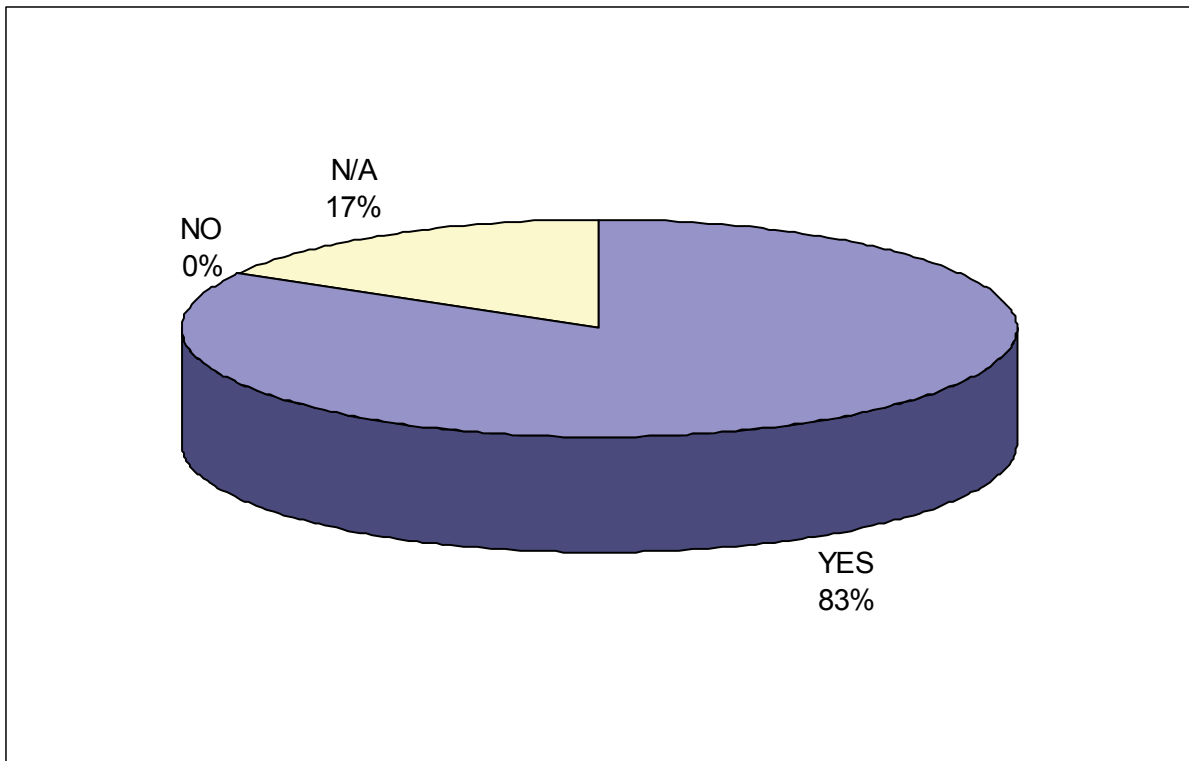


Which are the systems and technologies being used to meet this function?



5.1.6 Monitoring of network traffic.

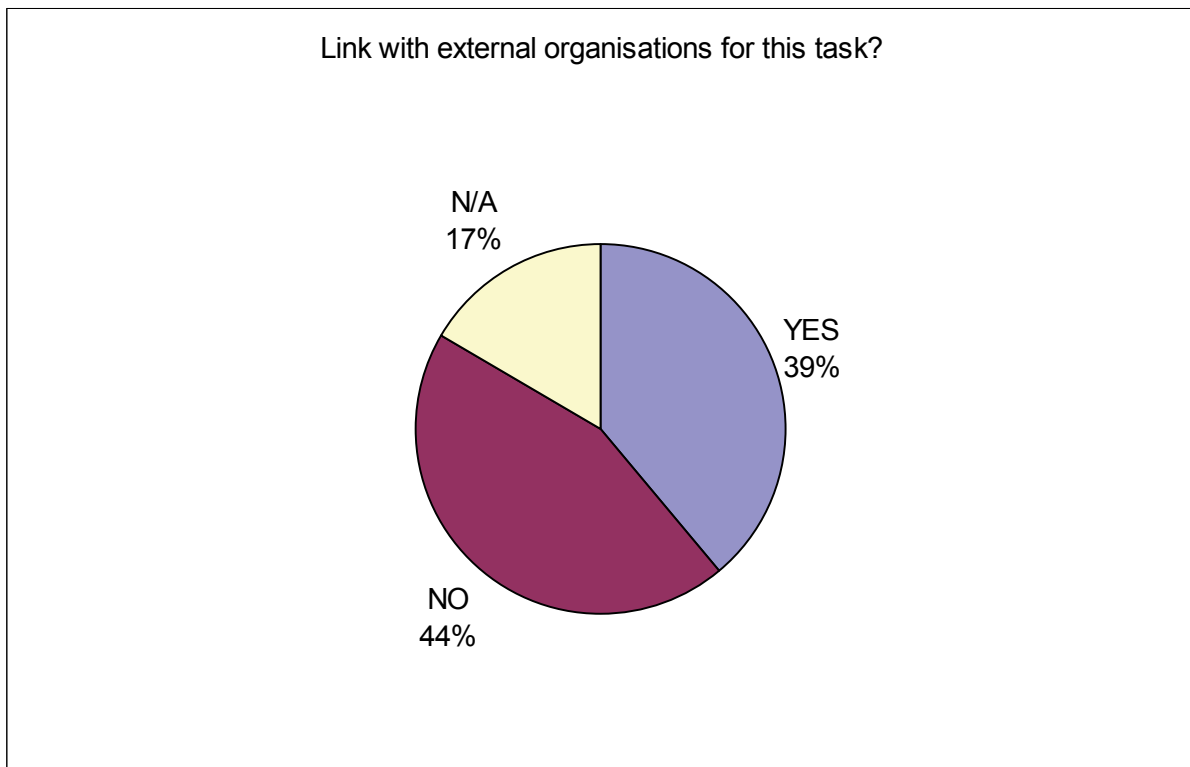
Is your traffic network monitored with security purposes?



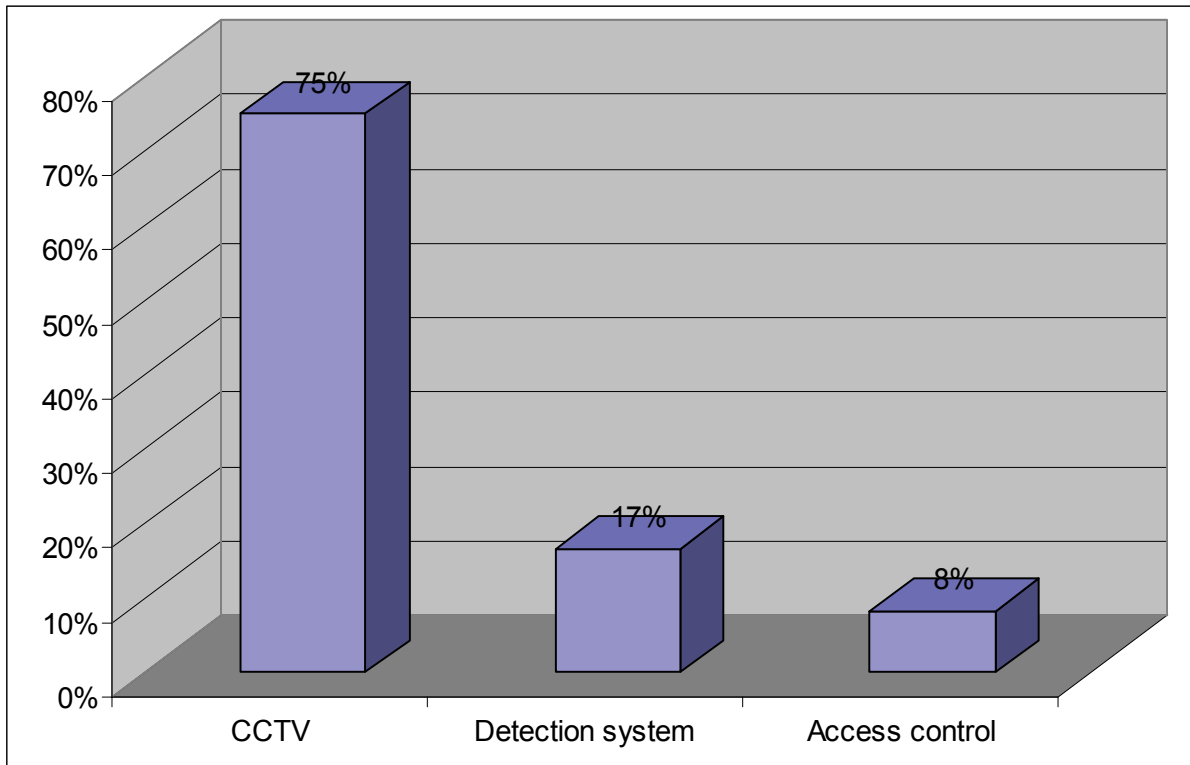
Which entities are involved in this task?

**Conclusions:**

This task is mainly performed by own personnel coming from the operators, who in case of having external help work in conjunction with police and private security entities.

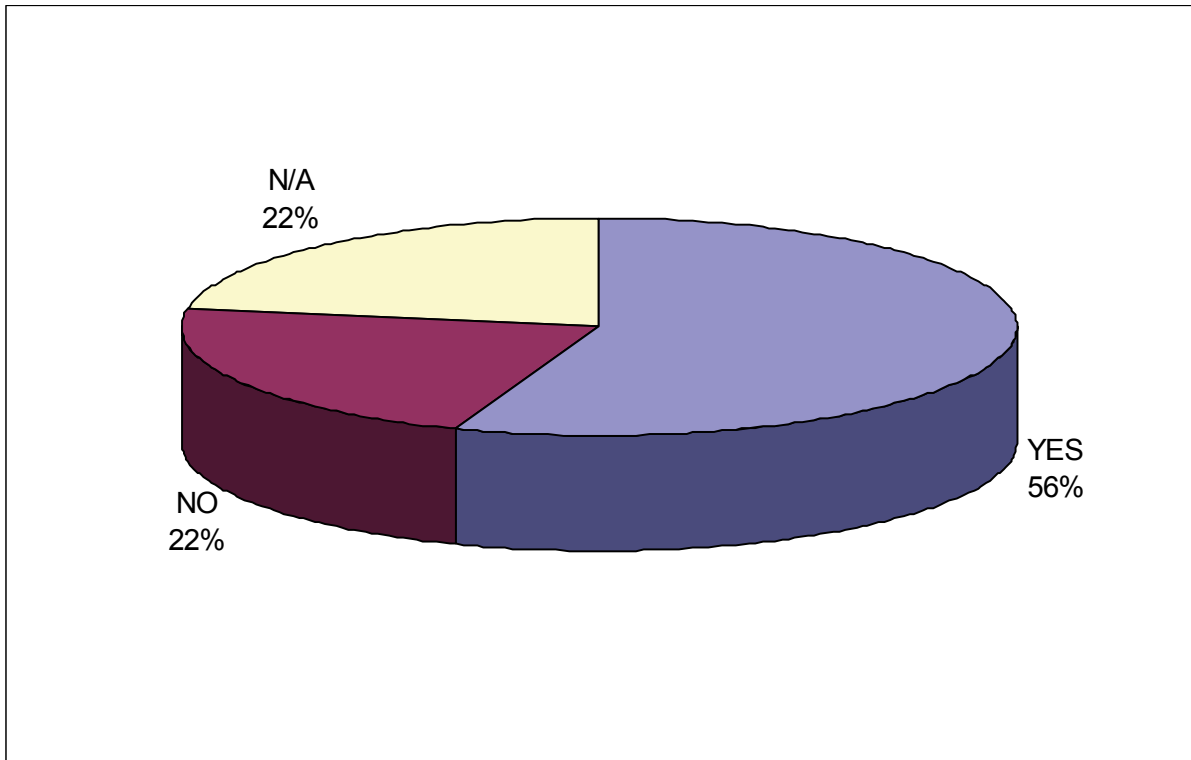


Which are the systems and technologies being used to meet this function?

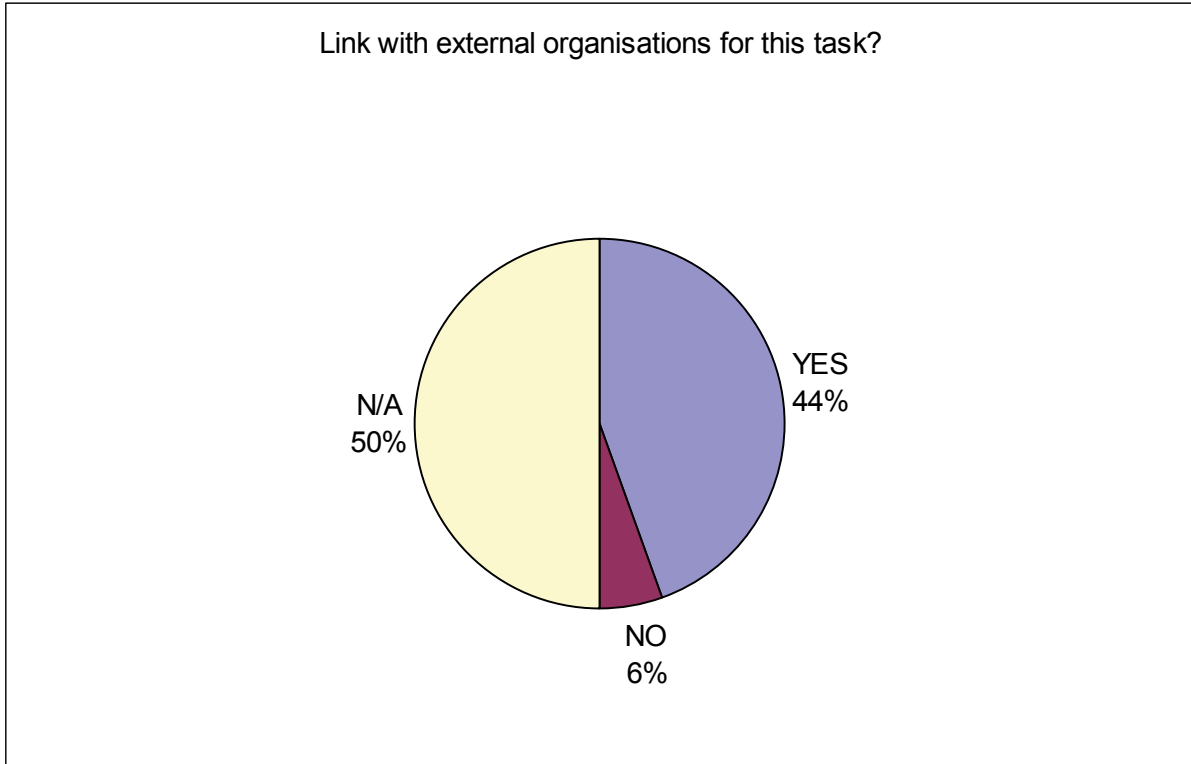


5.1.7 Detection and identification of unwanted entities in close proximity to critical infrastructures.

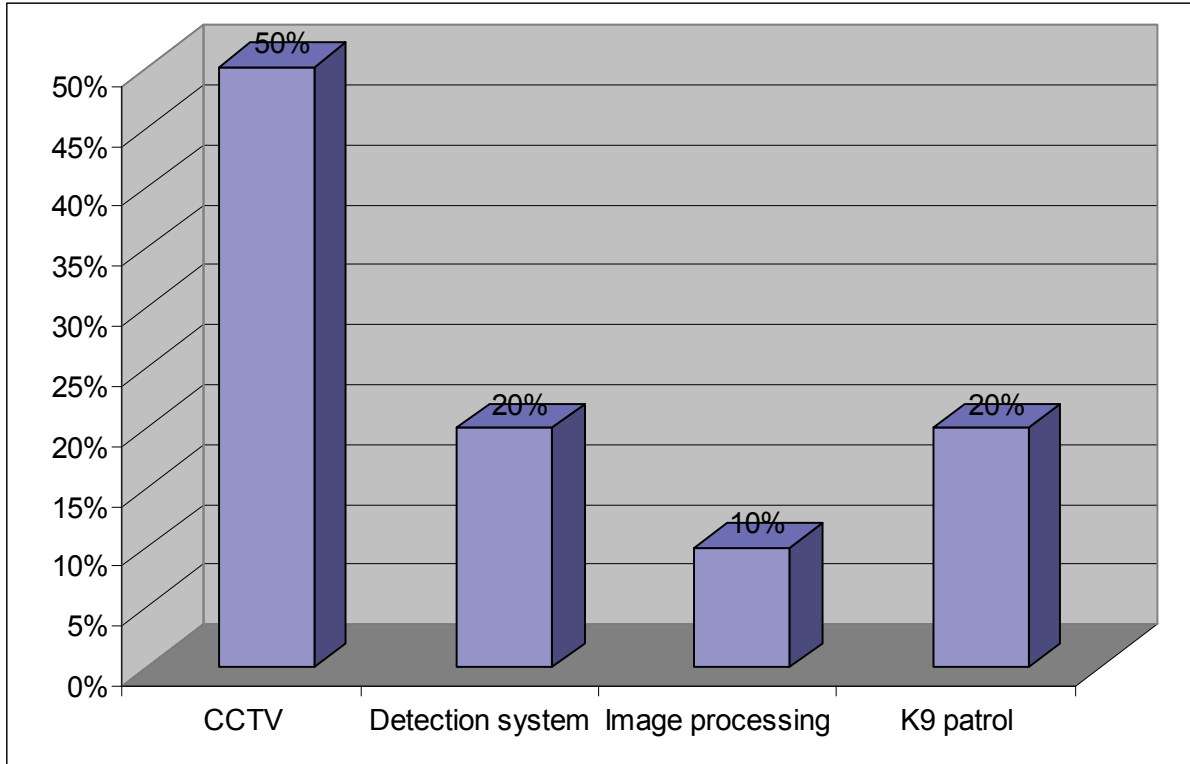
Is any procedure for detection and identification of unwanted entities in close proximity to critical infrastructures implemented?



Which entities are involved in this task?

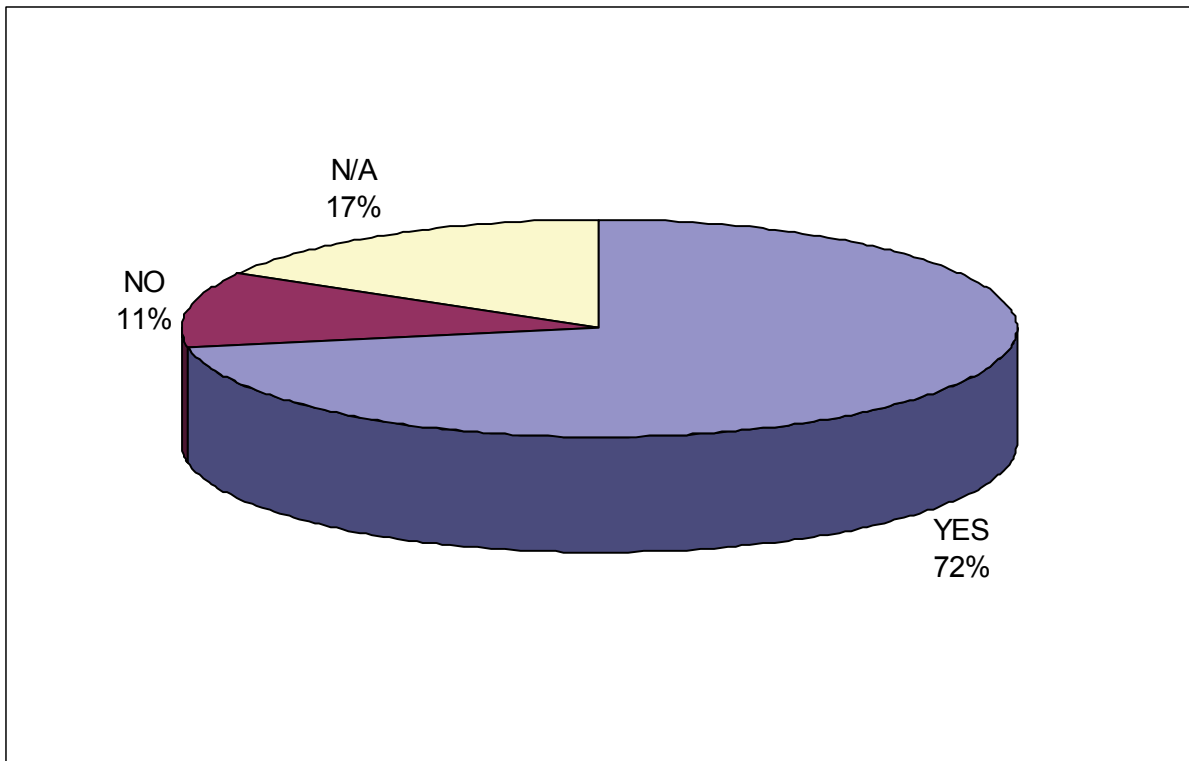


Which are the systems and technologies being used to meet this function?

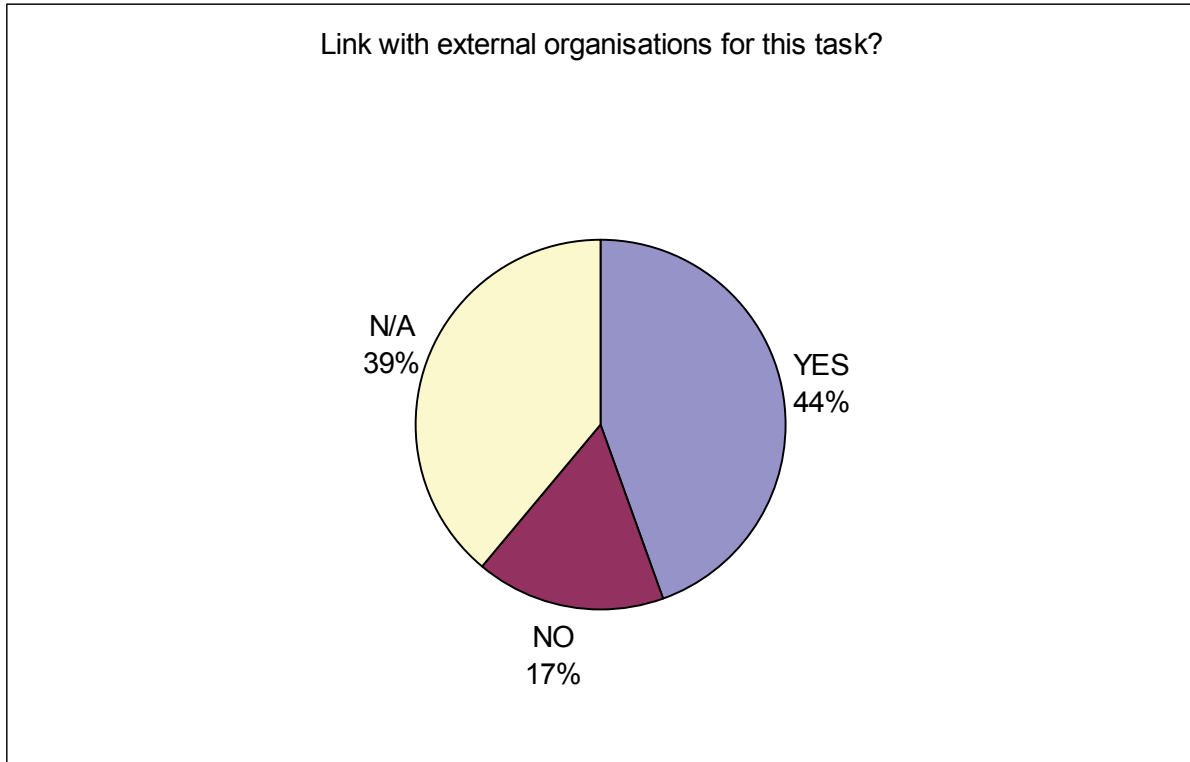


5.1.8 Monitoring of entry points.

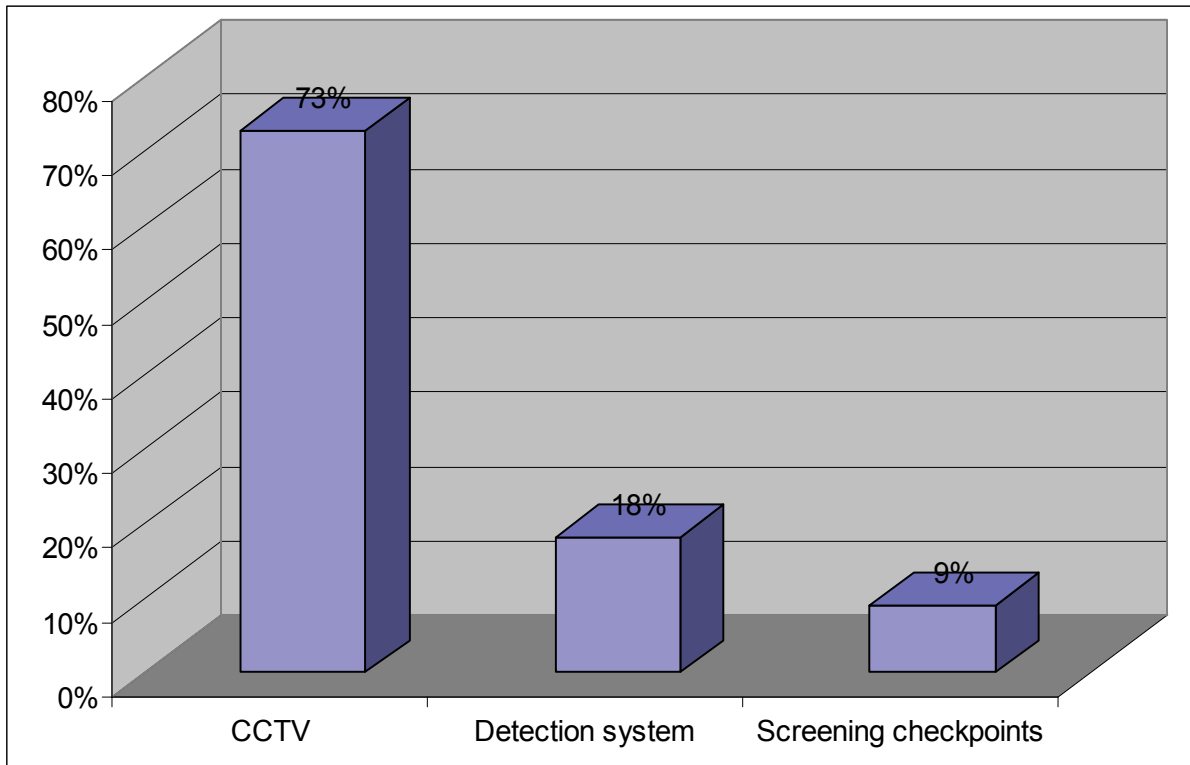
Are entry points monitored?



Which entities are involved in this task?

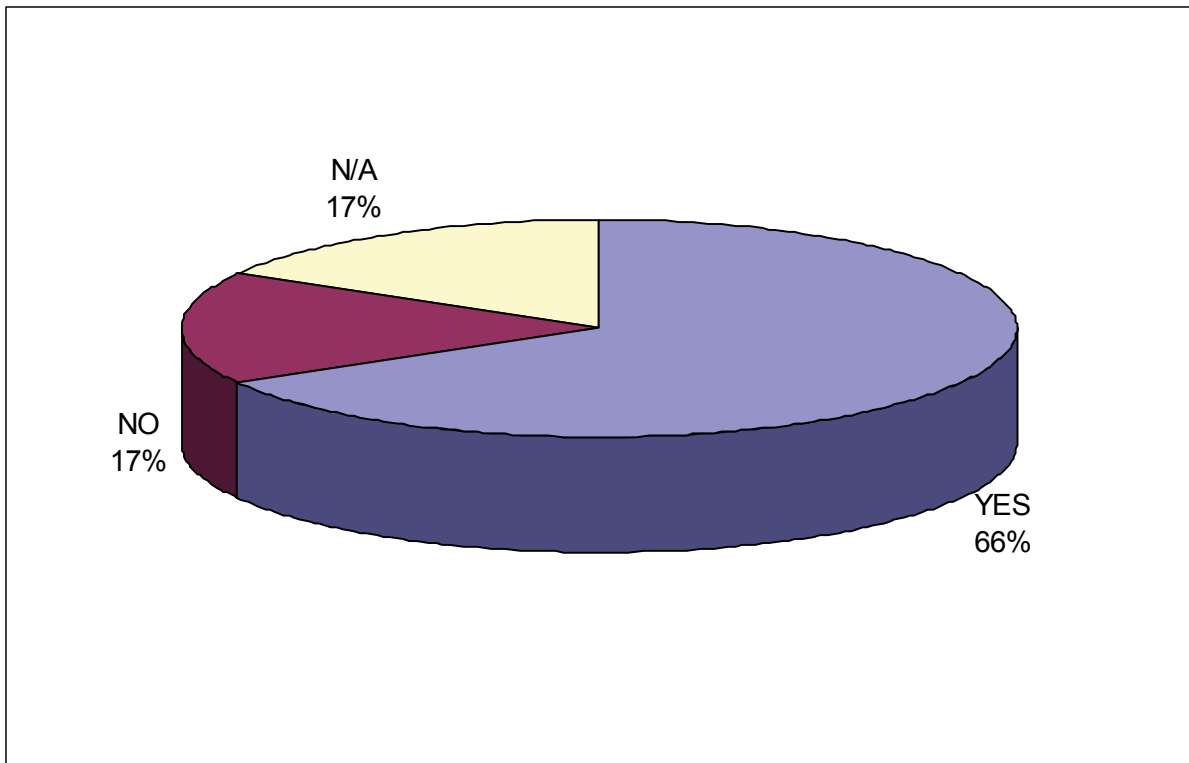


Which are the systems and technologies being used to meet this function?

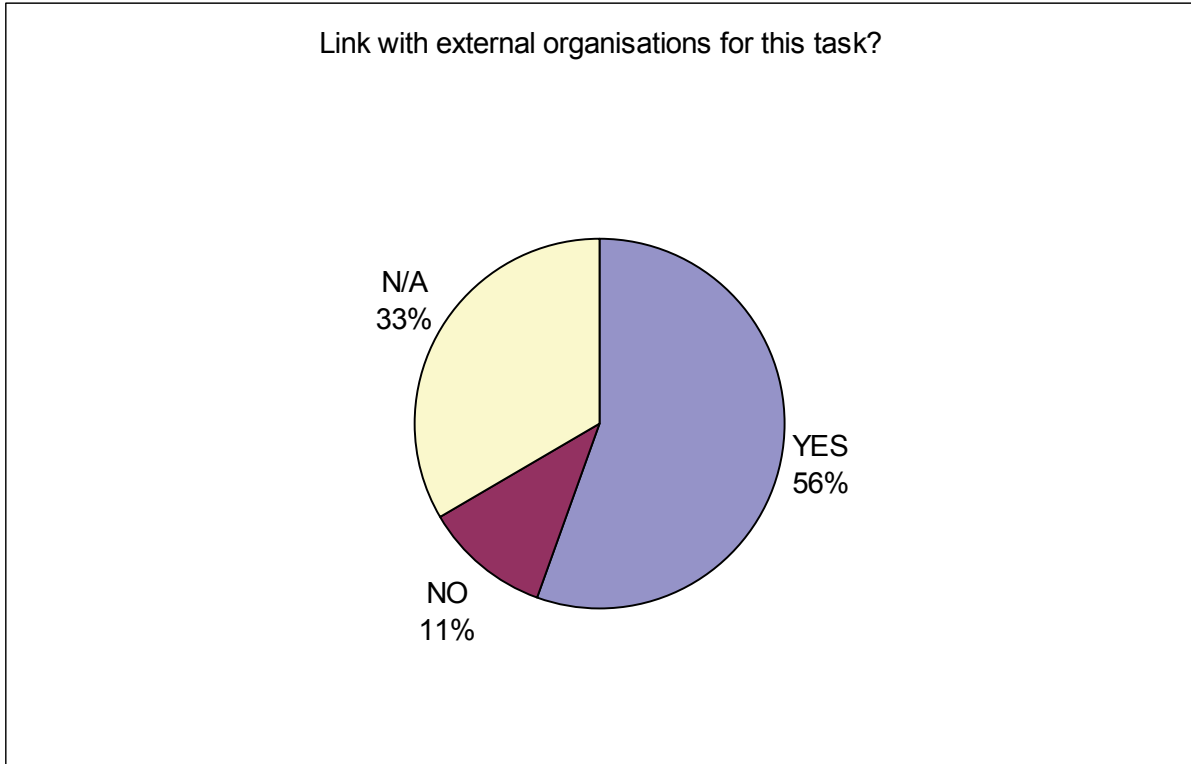


5.1.9 Detection of unattended luggage.

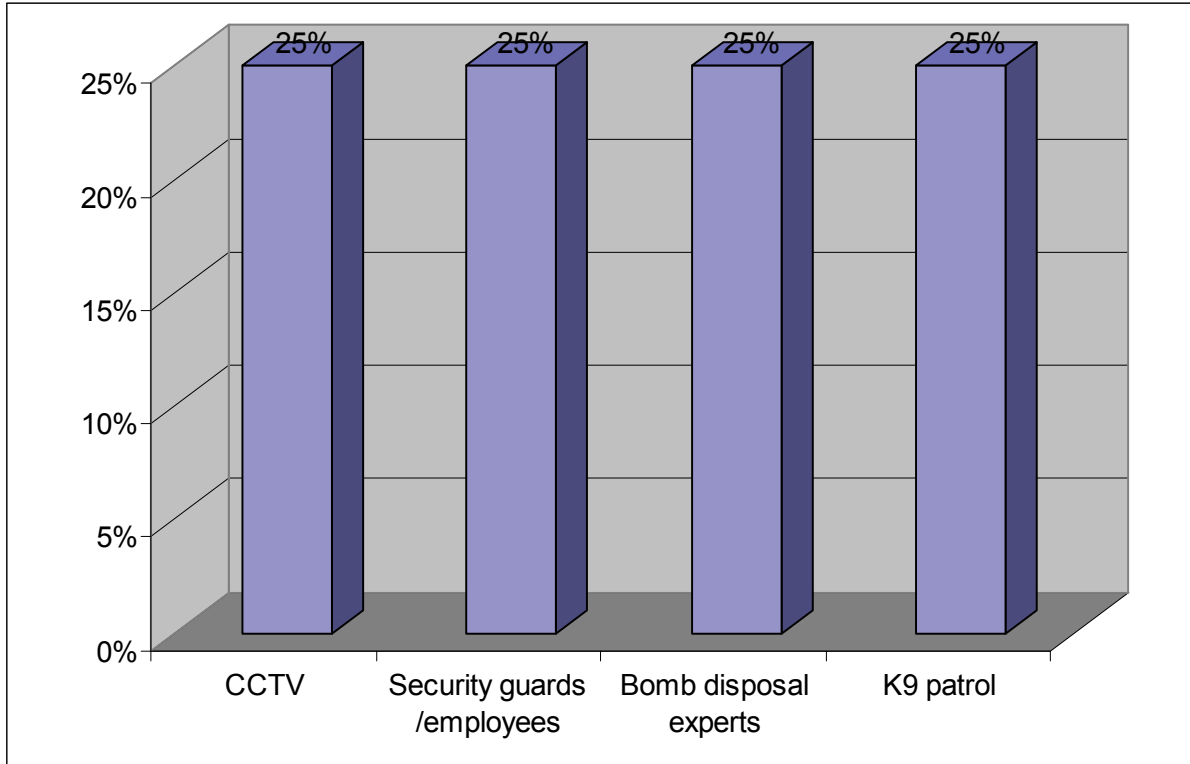
Are procedures for detection of unattended luggage implemented?



Which entities are involved in this task?

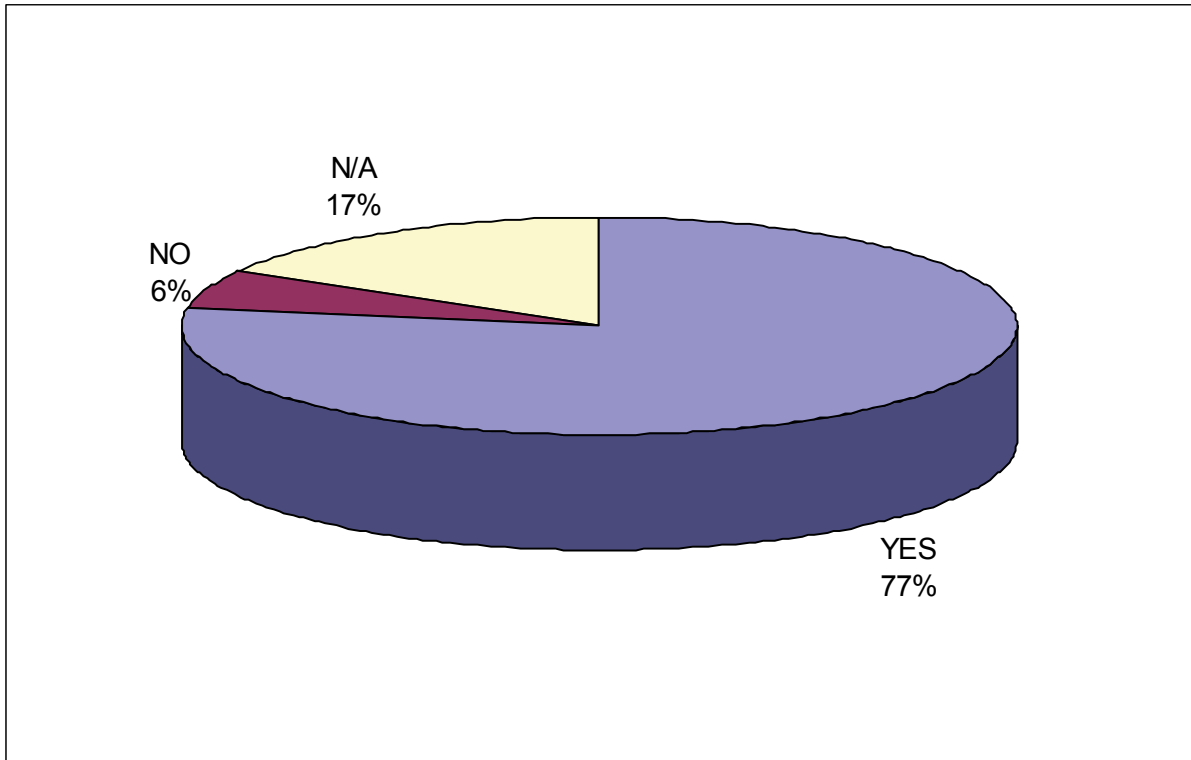


Which are the systems and technologies being used to meet this function?

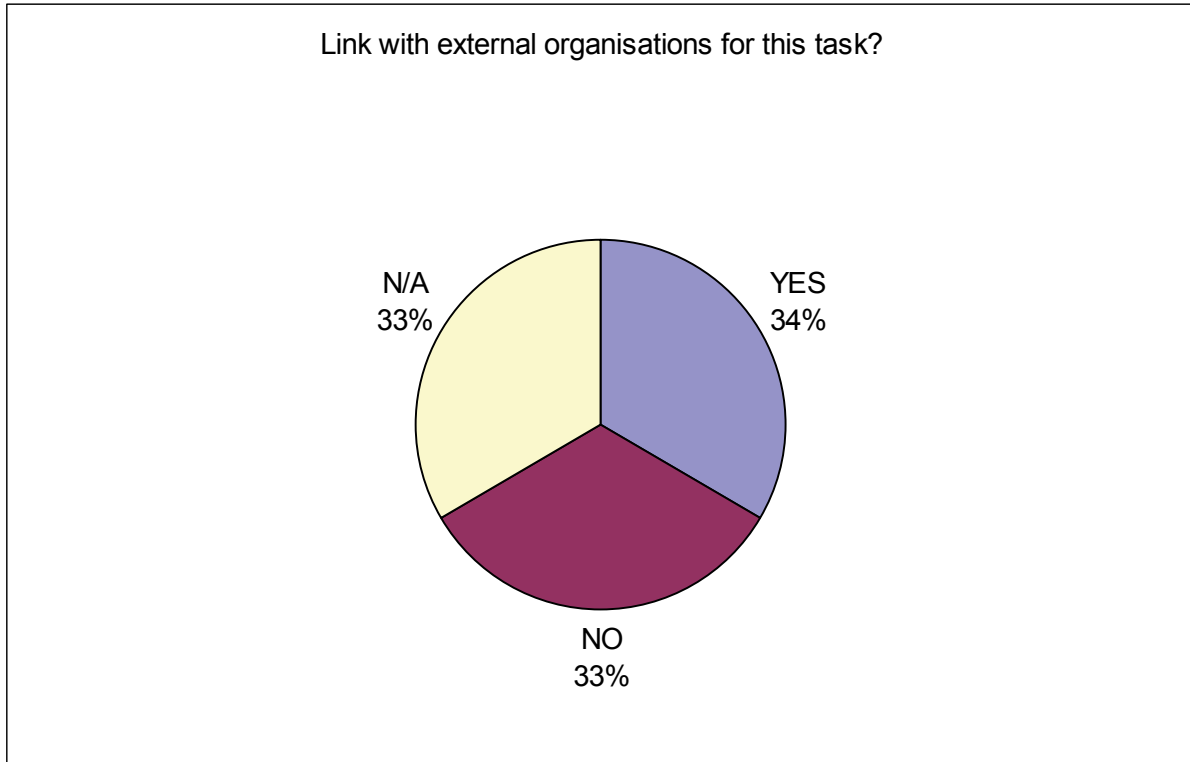


5.1.10 Surveillance

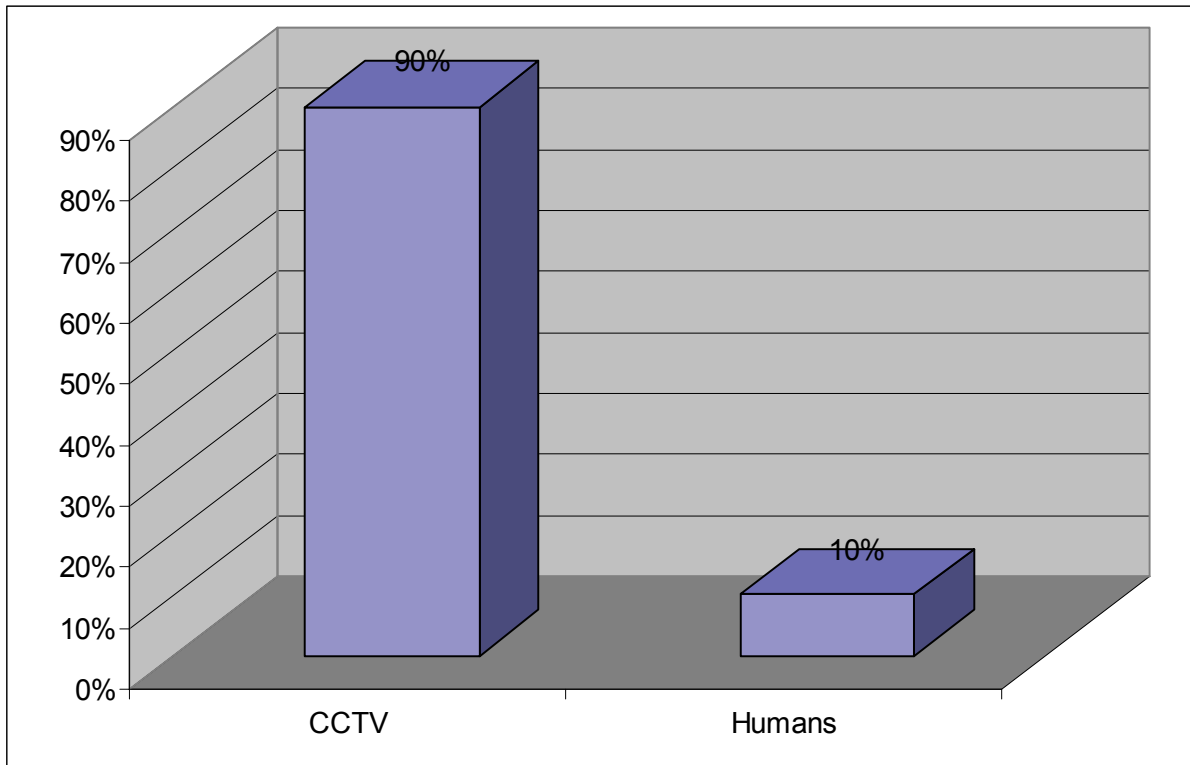
Is surveillance implemented in mass transportation assets (namely infrastructure and vehicles)?



Which entities are involved in this task?

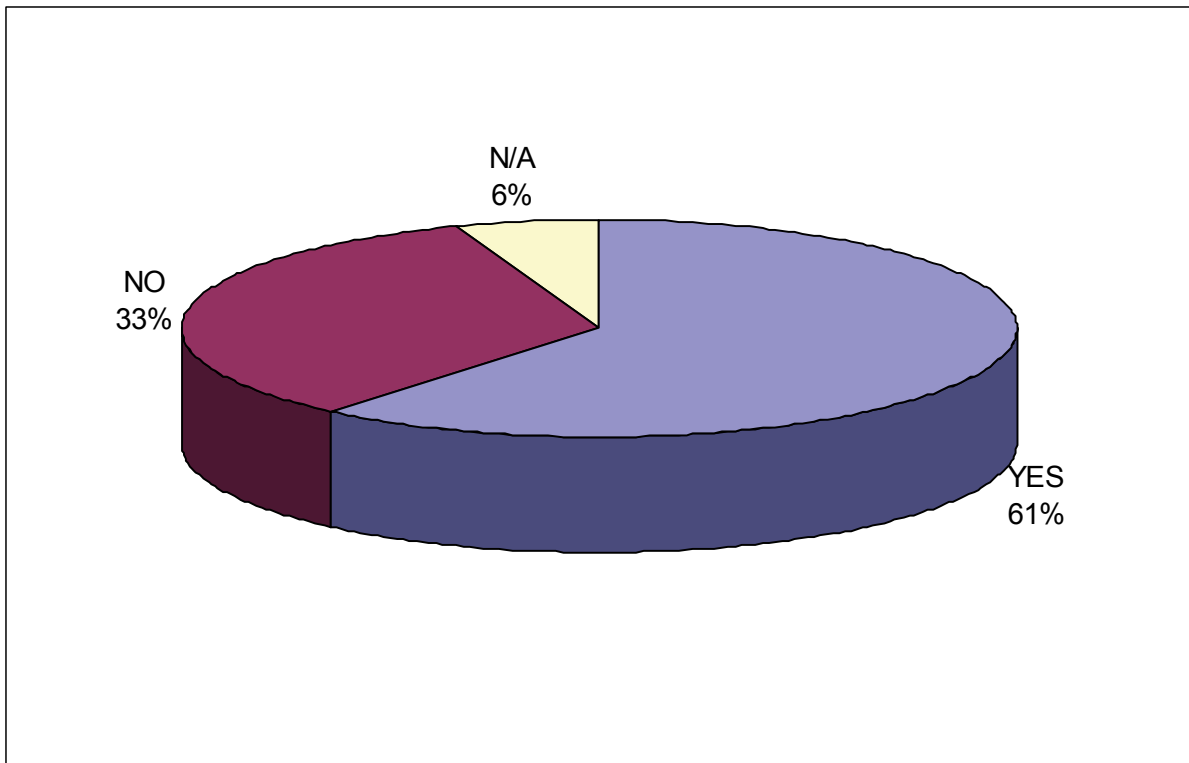


Which are the systems and technologies being used to meet this function?

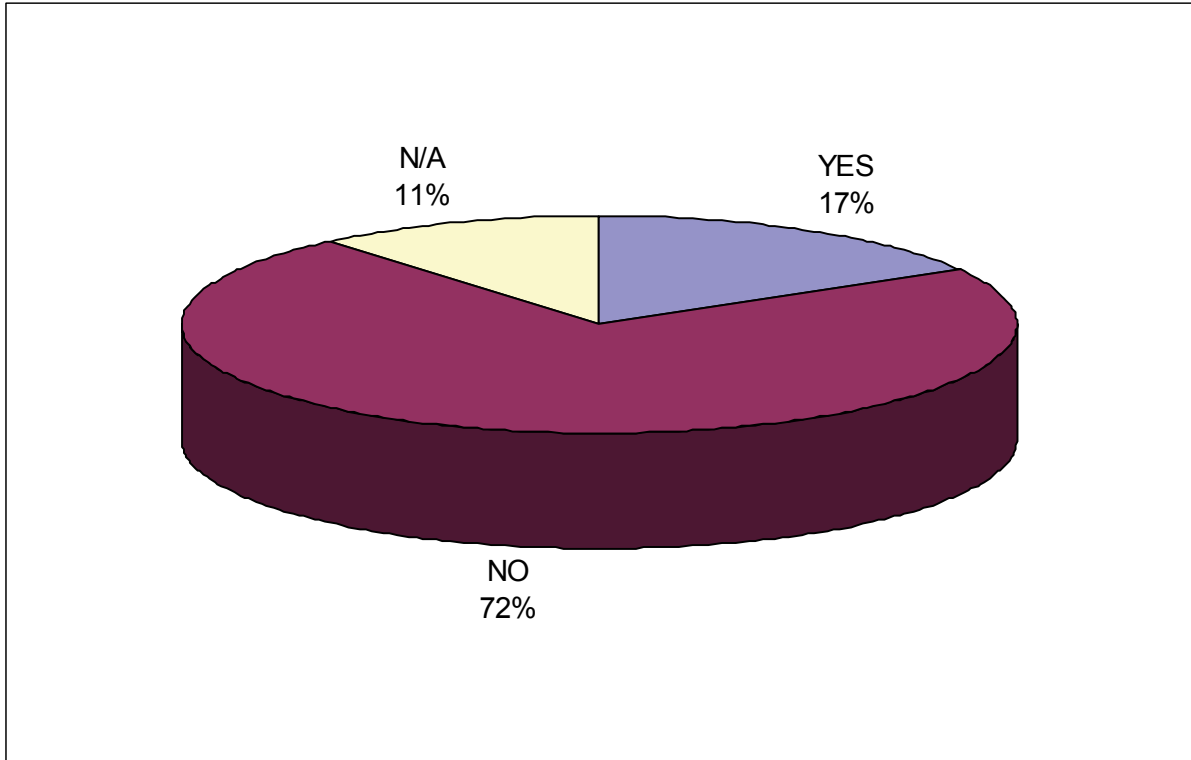


5.1.11 CBRN detection.

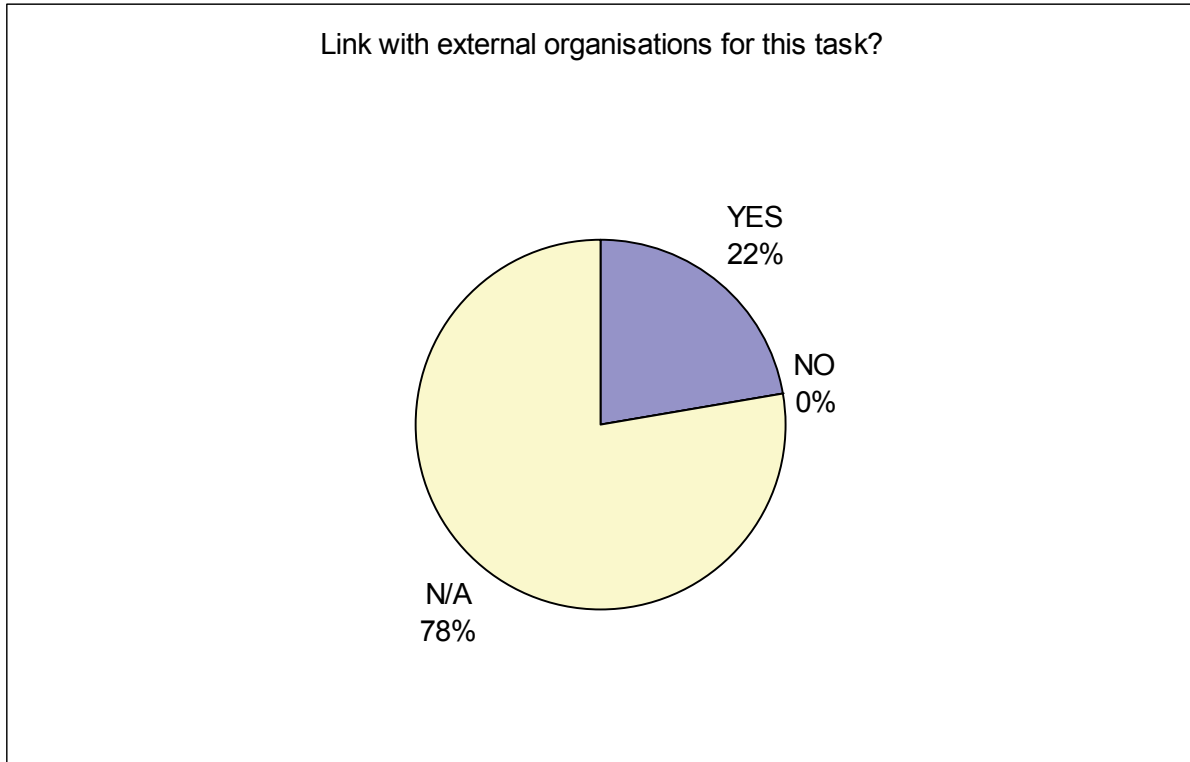
Is CBRN labelled as a threat for mass transportation?



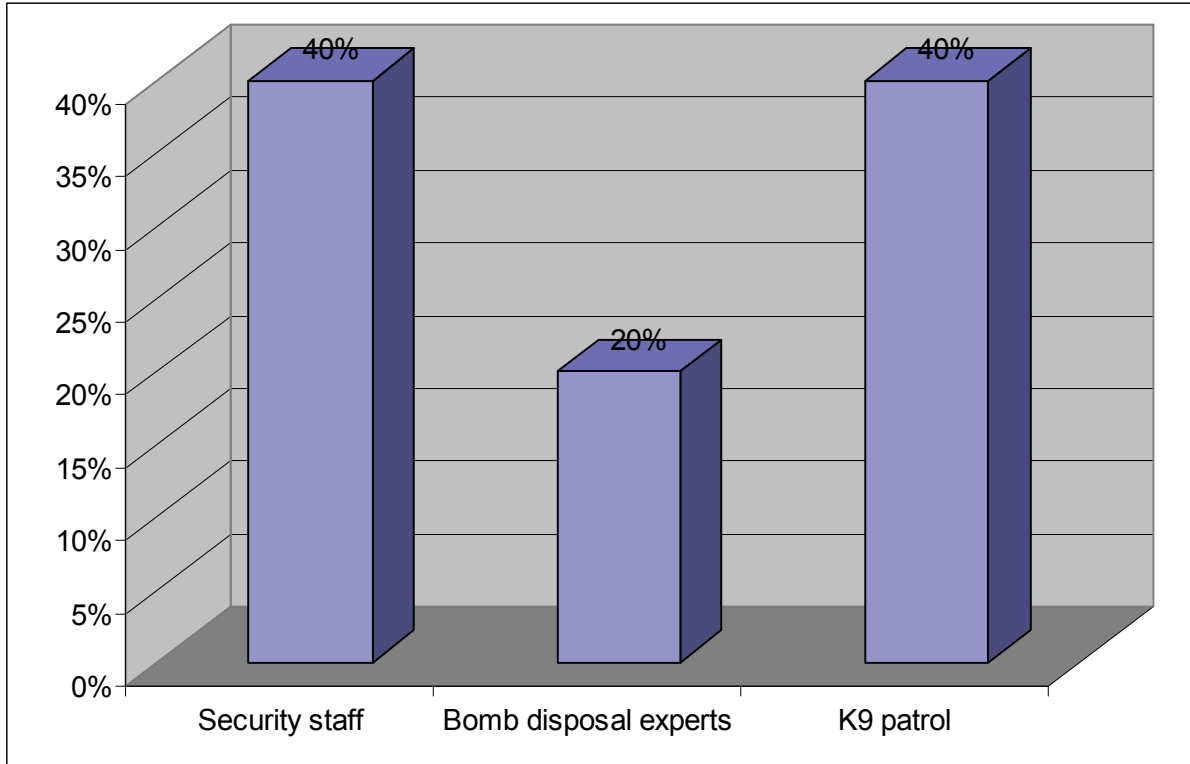
Is CBRN detection implemented?



Which entities are involved in this task?



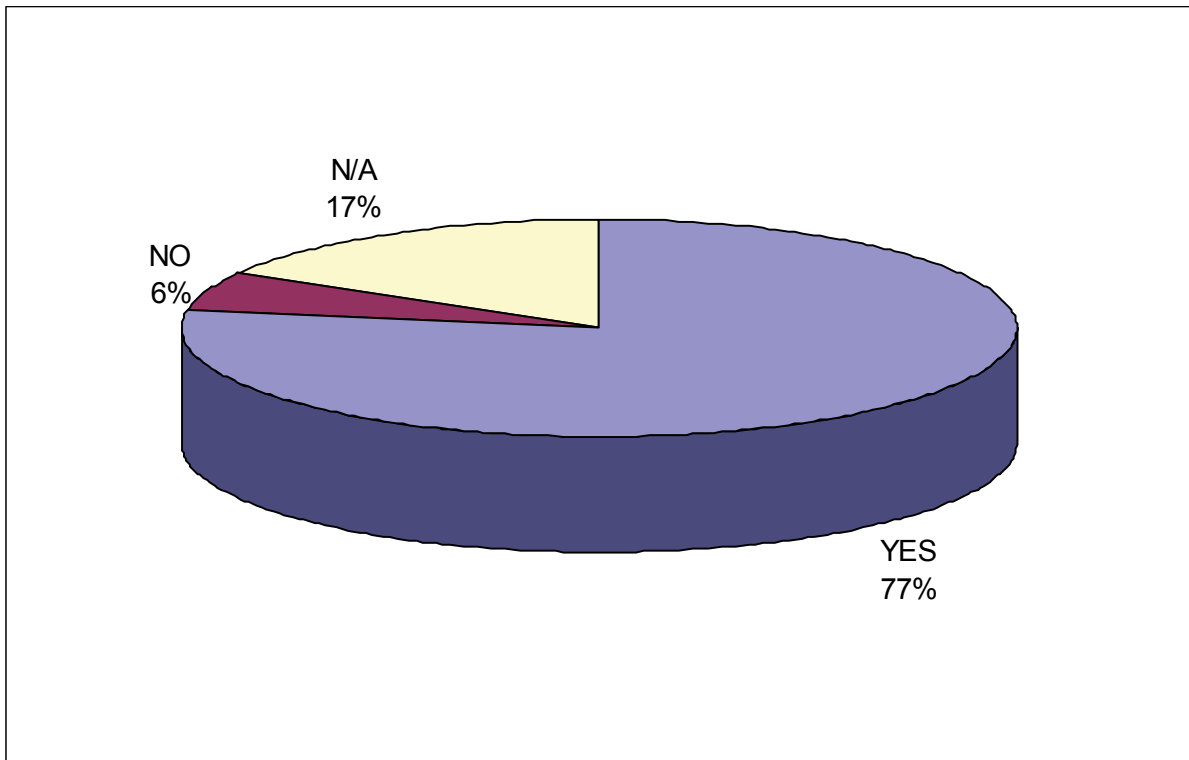
Which are the systems and technologies being used to meet this function?



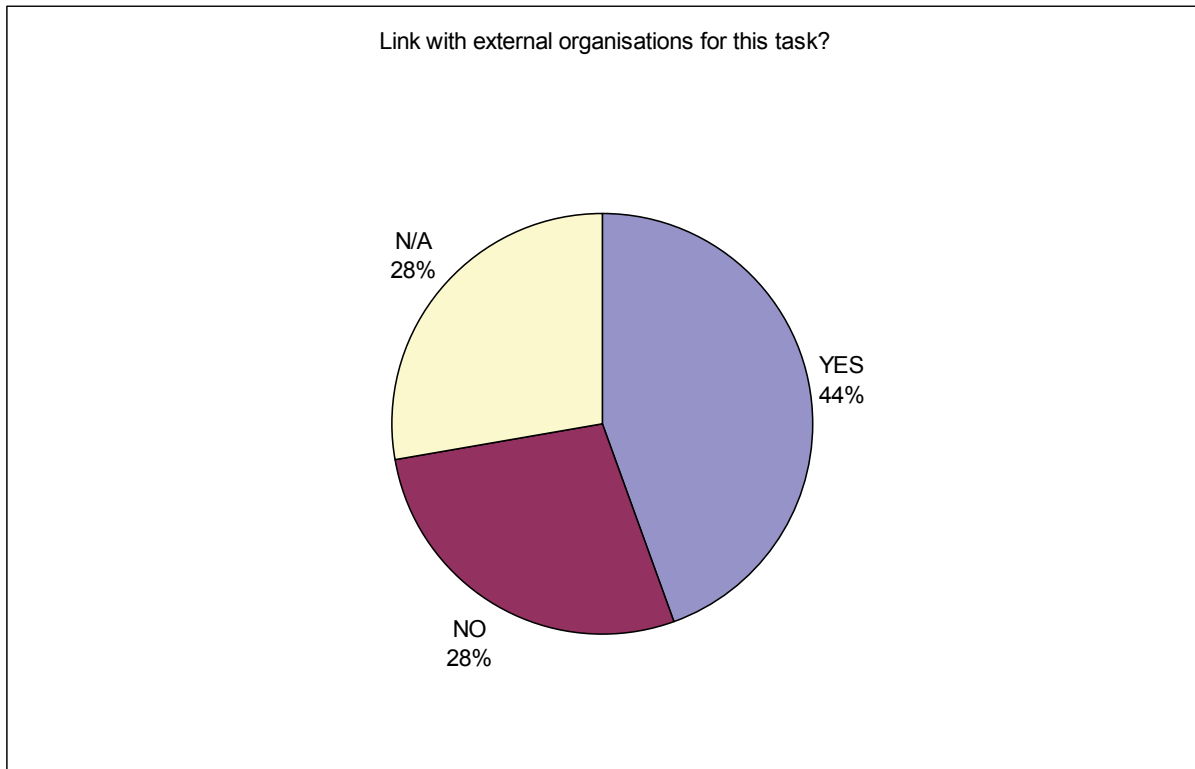
## 5.2 Risk assessment-based command and control.

### 5.2.1 Command and Control.

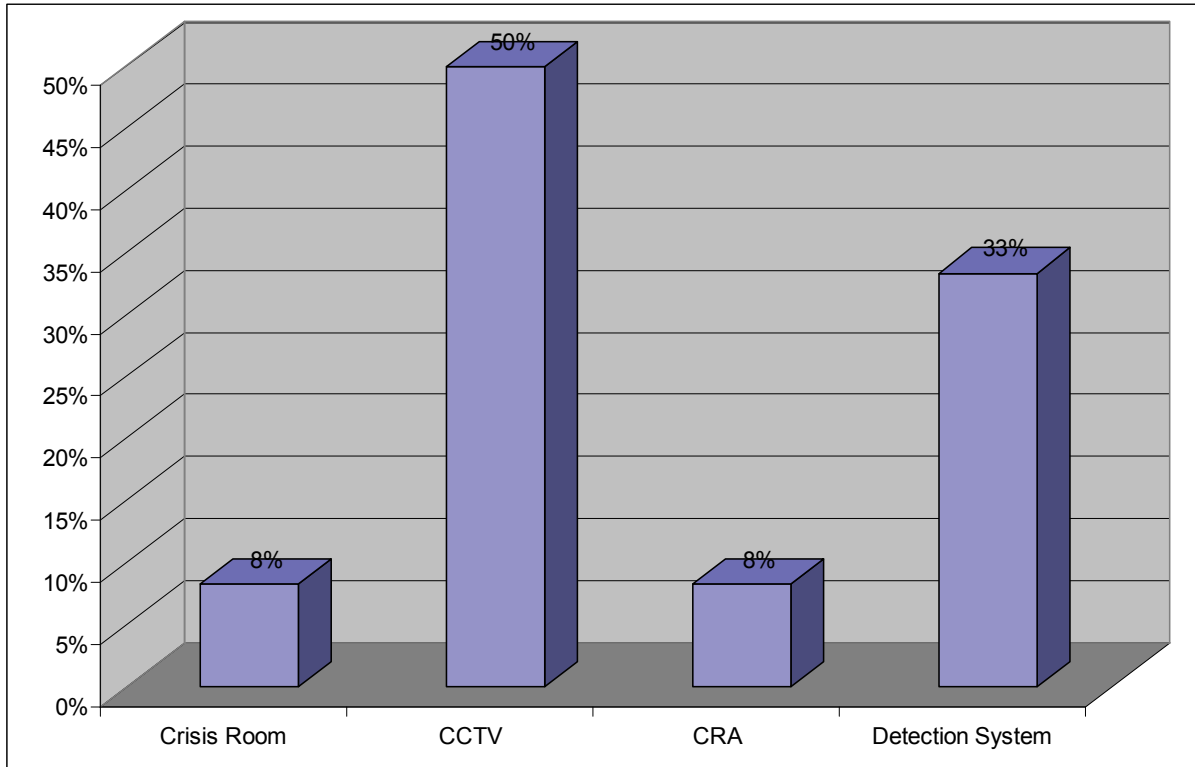
Is there a command and control centre used for security purposes (alternatively: Are security issues implemented in your command and control centres?)



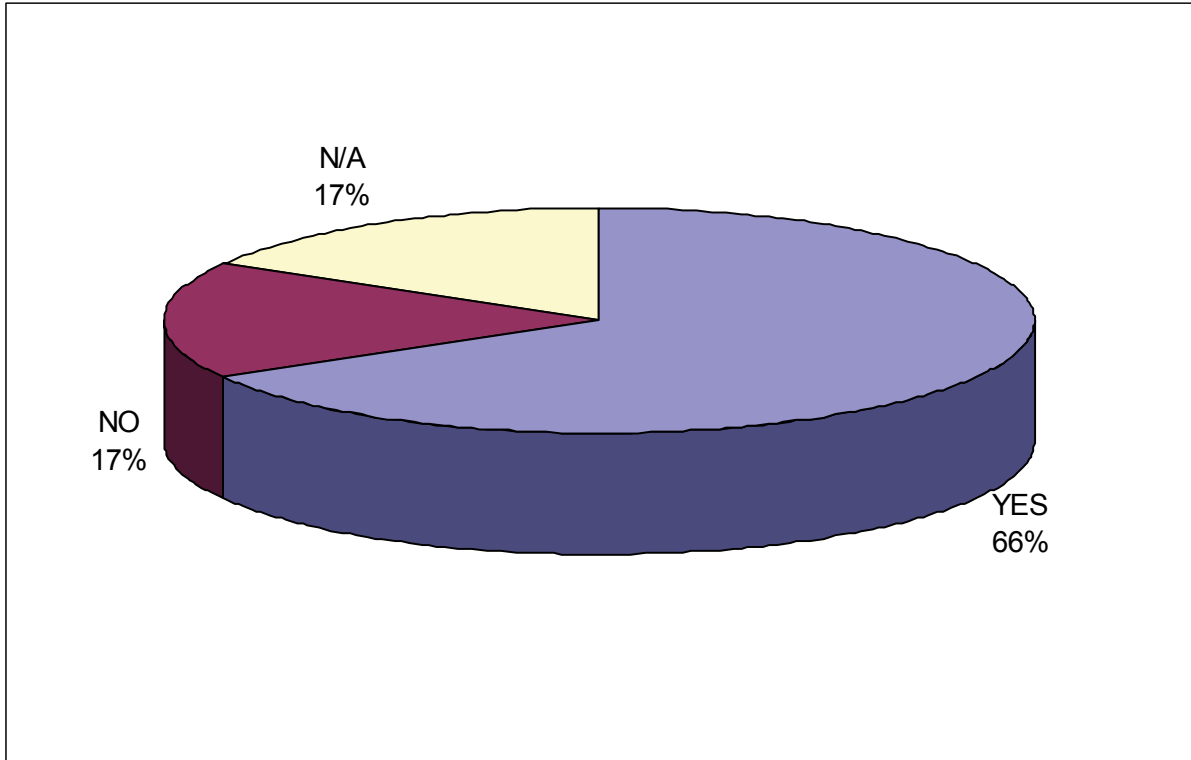
Which entities participate in its daily operation?



Which are the systems and technologies being used to meet this function?



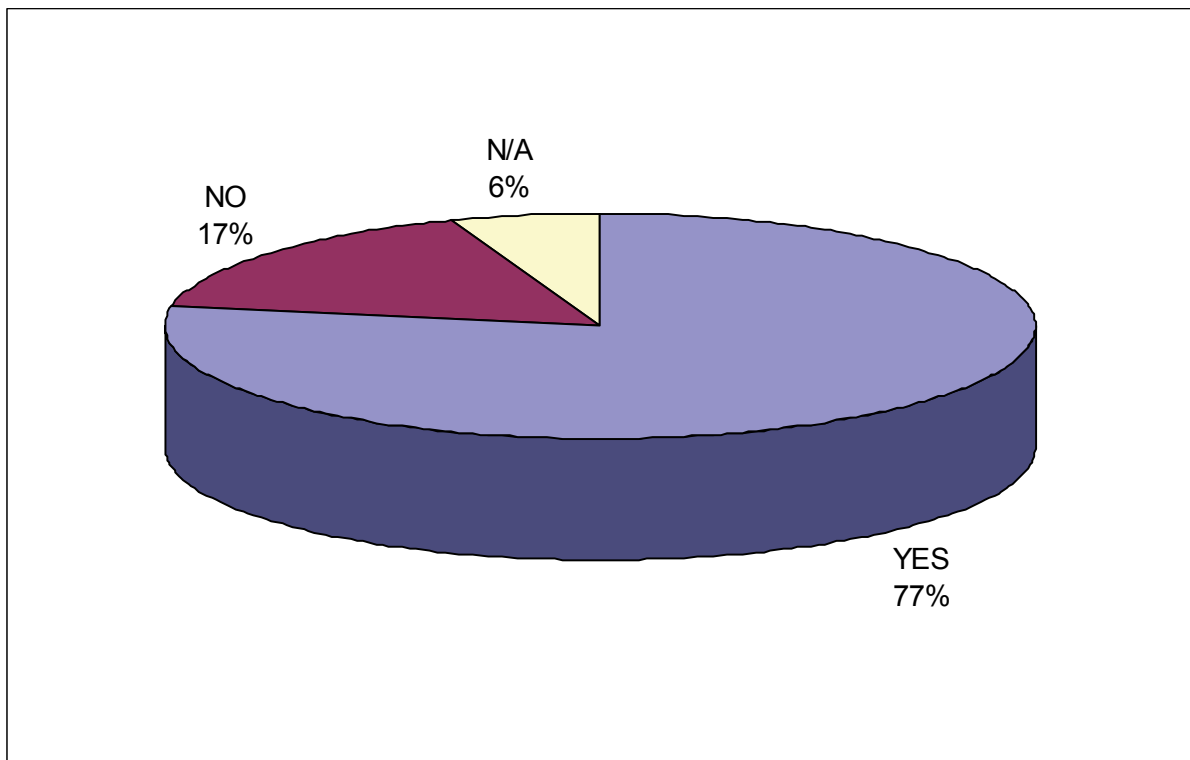
Do these control centres consider risk assessment?



### 5.3 Intelligence.

#### 5.3.1 Information management.

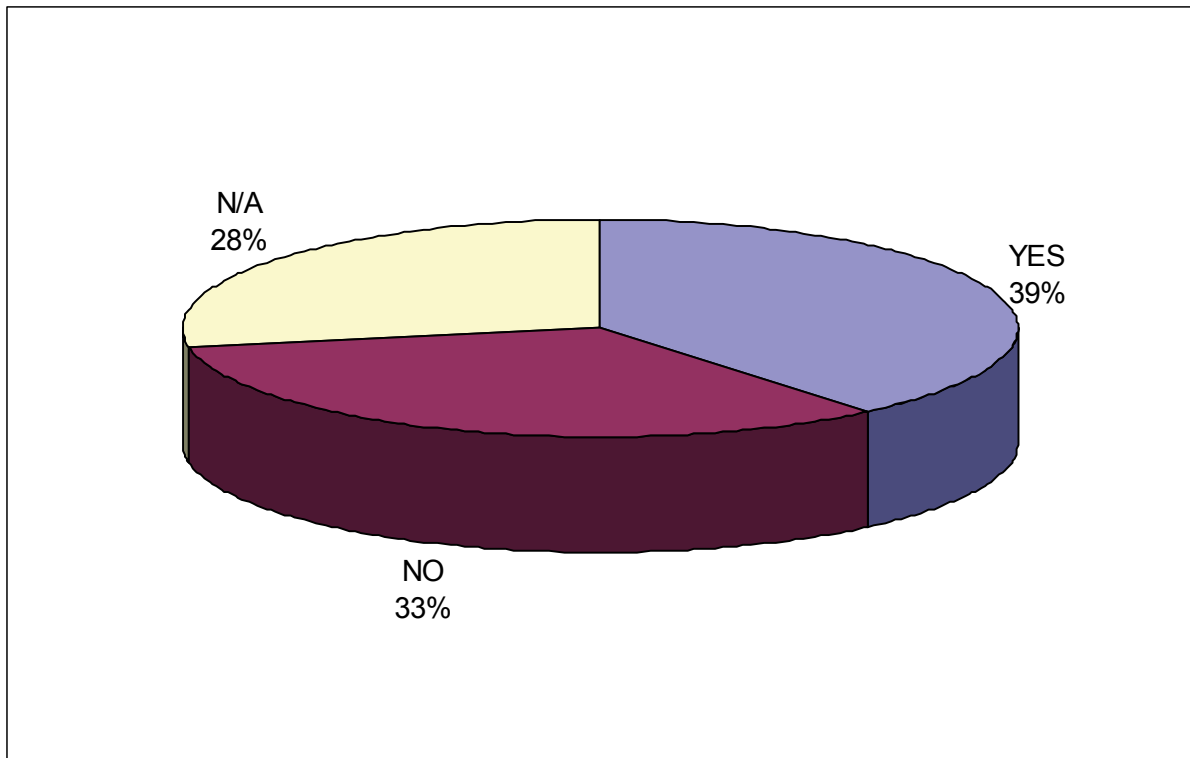
Do you cooperate with the intelligence services, either to get updated threat pictures they can use themselves, or to provide data that can be helpful to other entities?



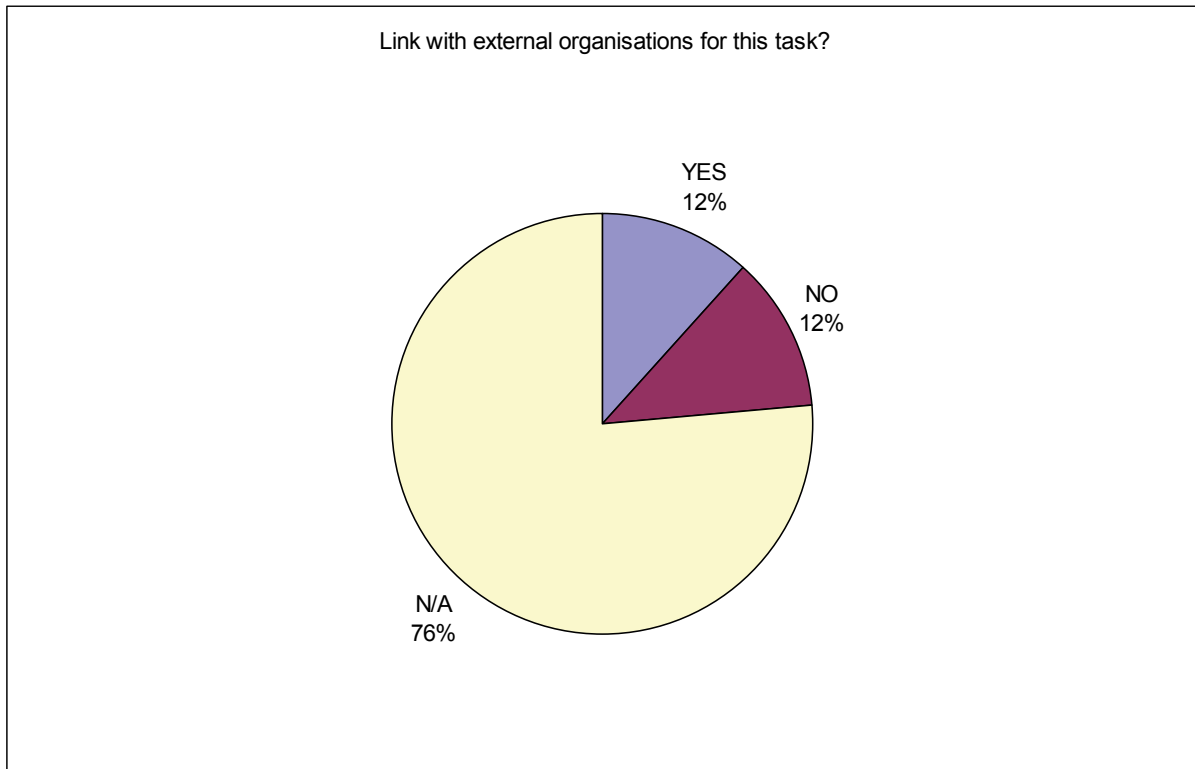
## 5.4 Cyber defence.

### 5.4.1 Robust encoding.

Are the communication systems belonging to your transport assets robustly encoded?

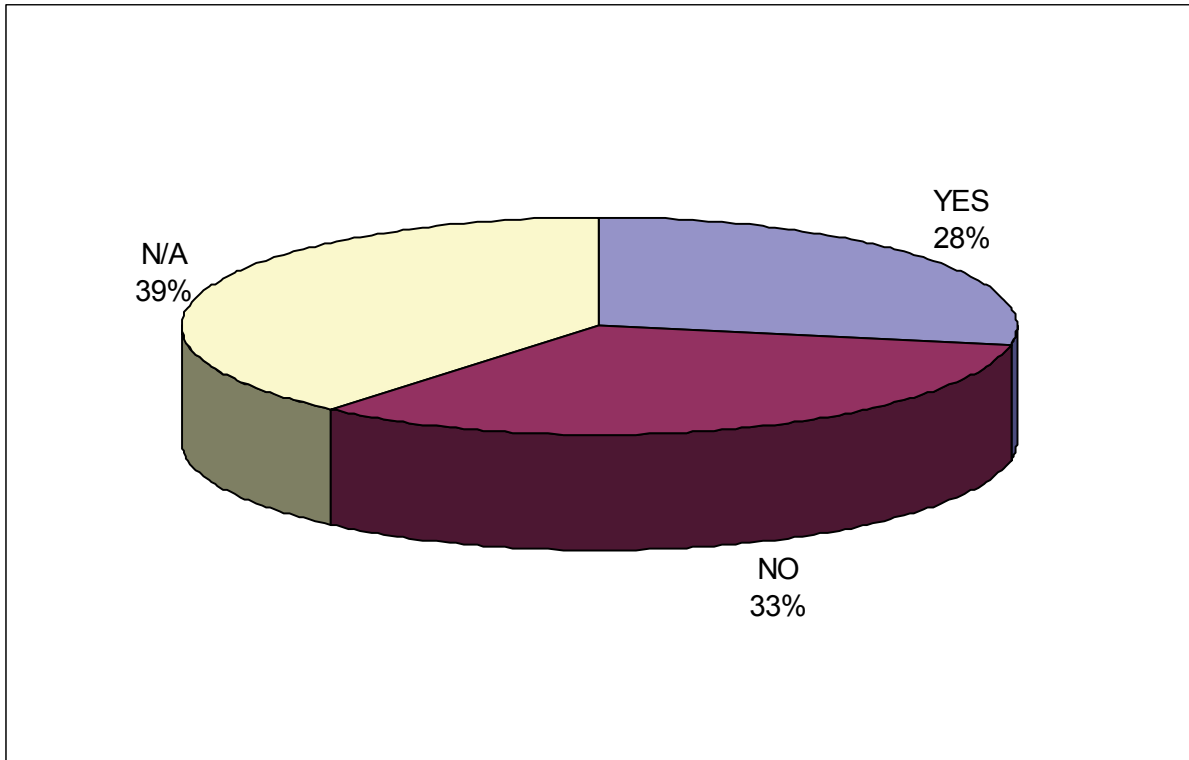


Which entities are involved in this task?

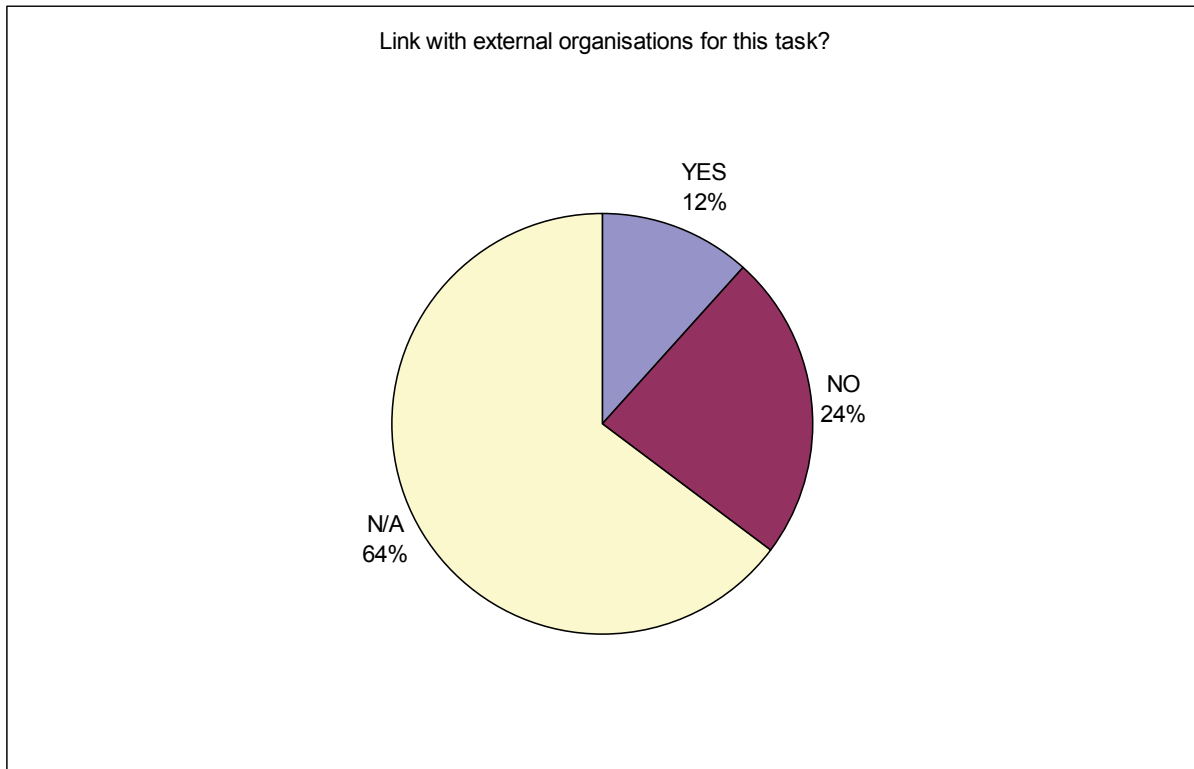


5.4.2 Function 4.2: Resilience of communication network from jamming.

Are jamming resilience measures implemented in the communication network? Which entities are involved in this task?

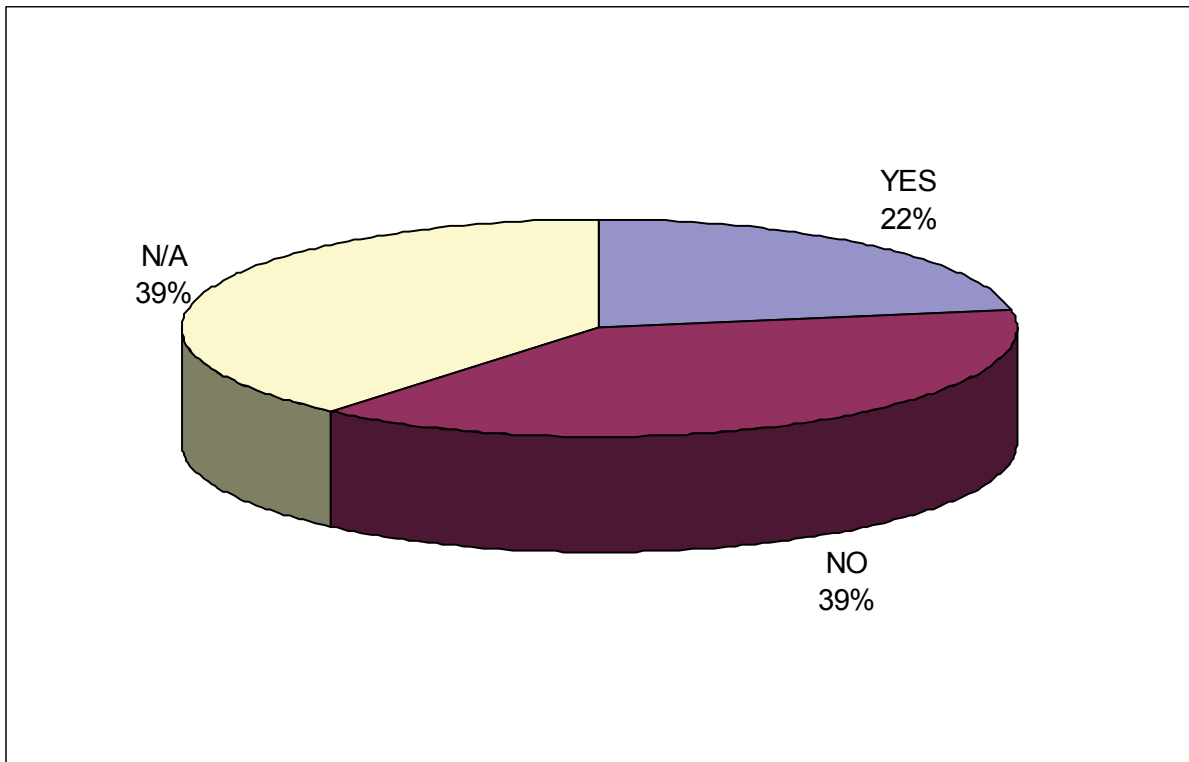


Which entities are involved in this task?

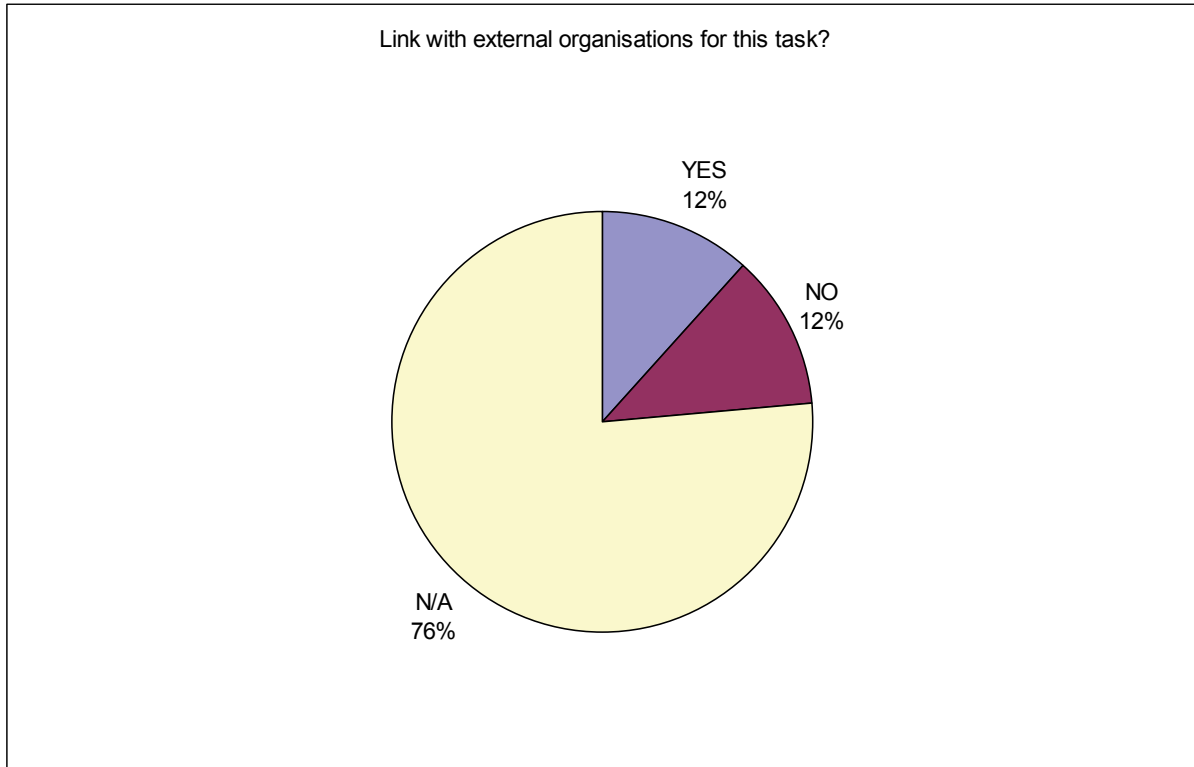


5.4.3 Resilience of communication network from heavy noise signals.

Are any heavy noise signals protection measures implemented in the communication network?

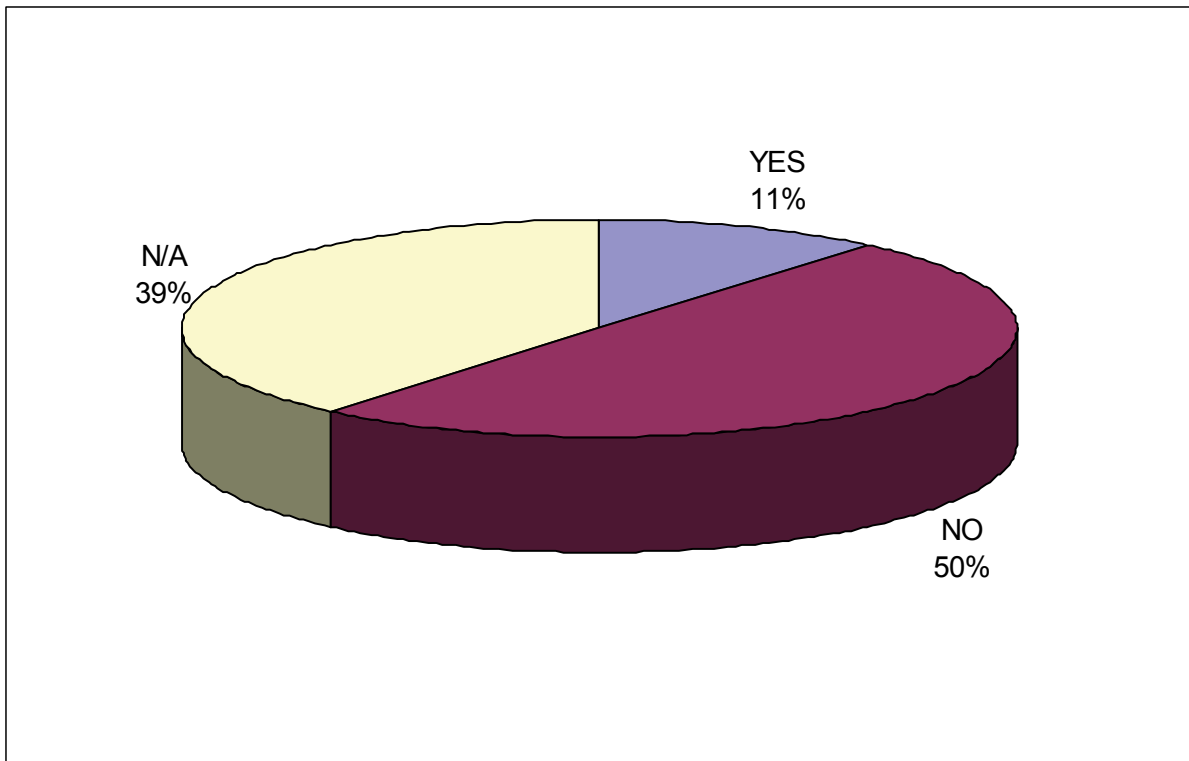


Which entities are involved in this task?

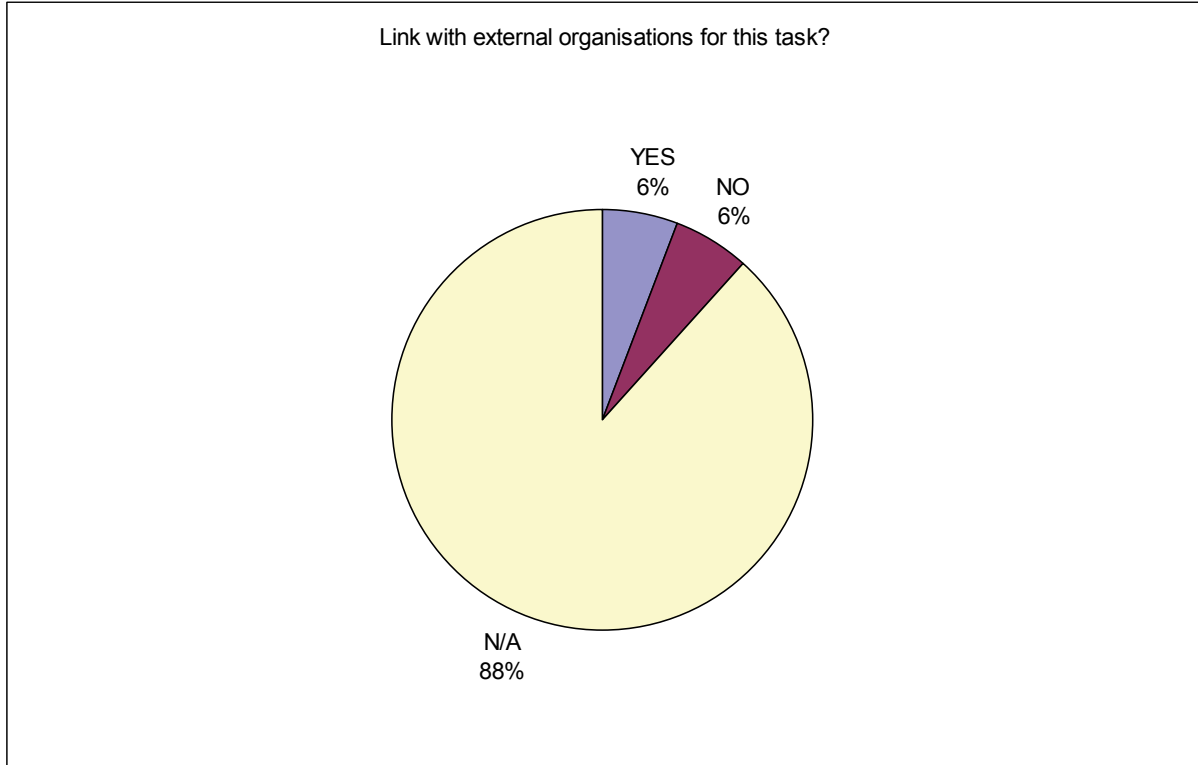


5.4.4 Resilience of communication network from power Microwave attacks.

Is the communication network's resilience tested from Microwave attacks?



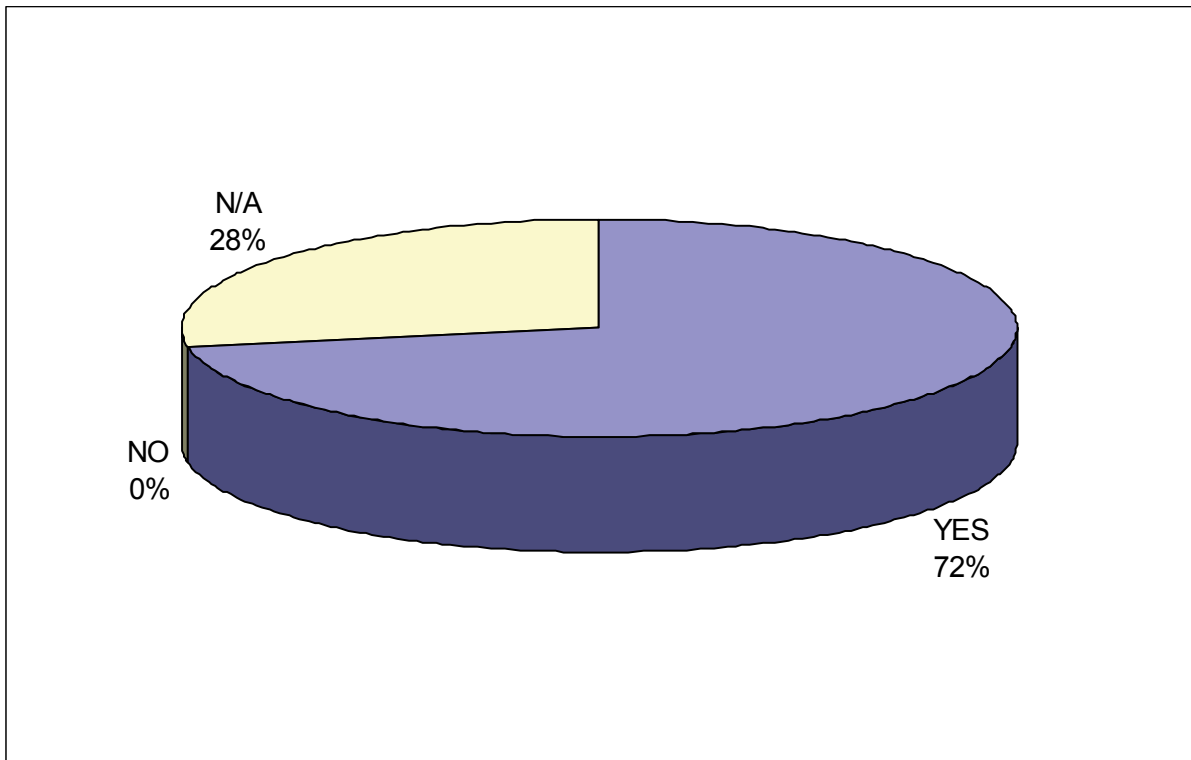
Which entities are involved in this task?



## 5.5 Passive protection systems.

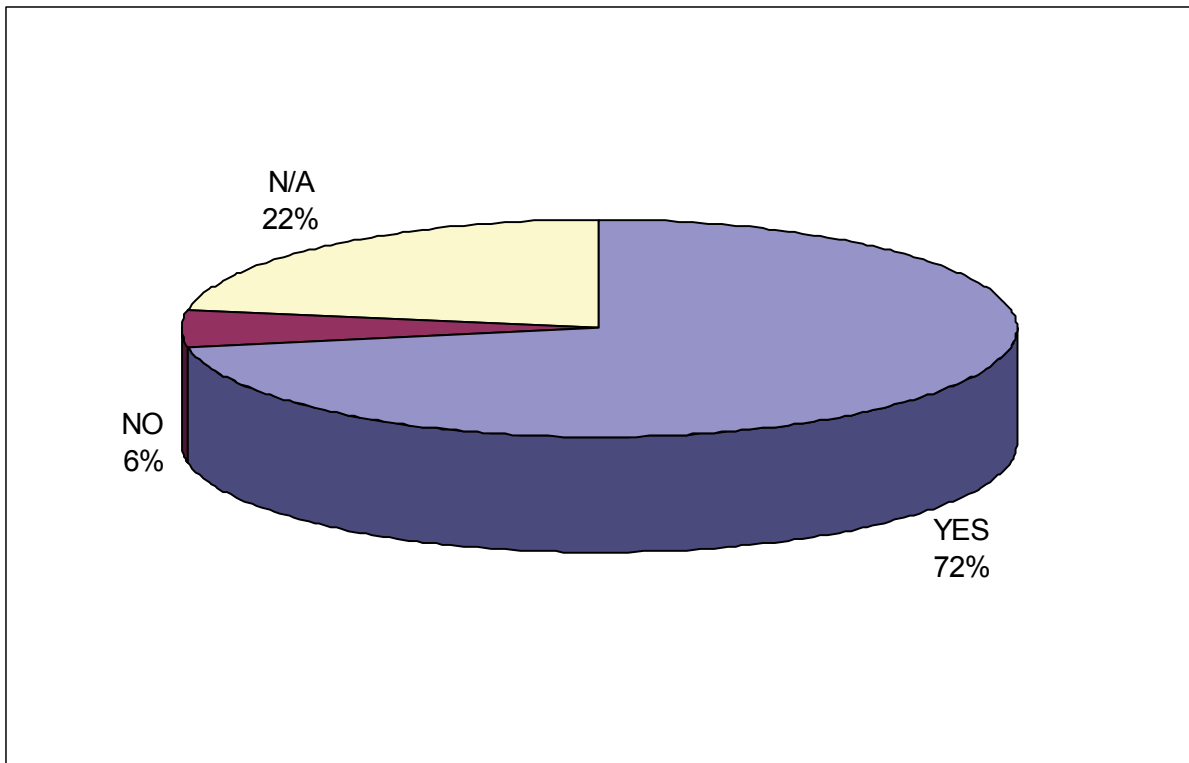
### 5.5.1 Fire protection.

Is passive fire protection implemented within transport infrastructures? Which entities are involved in this task?

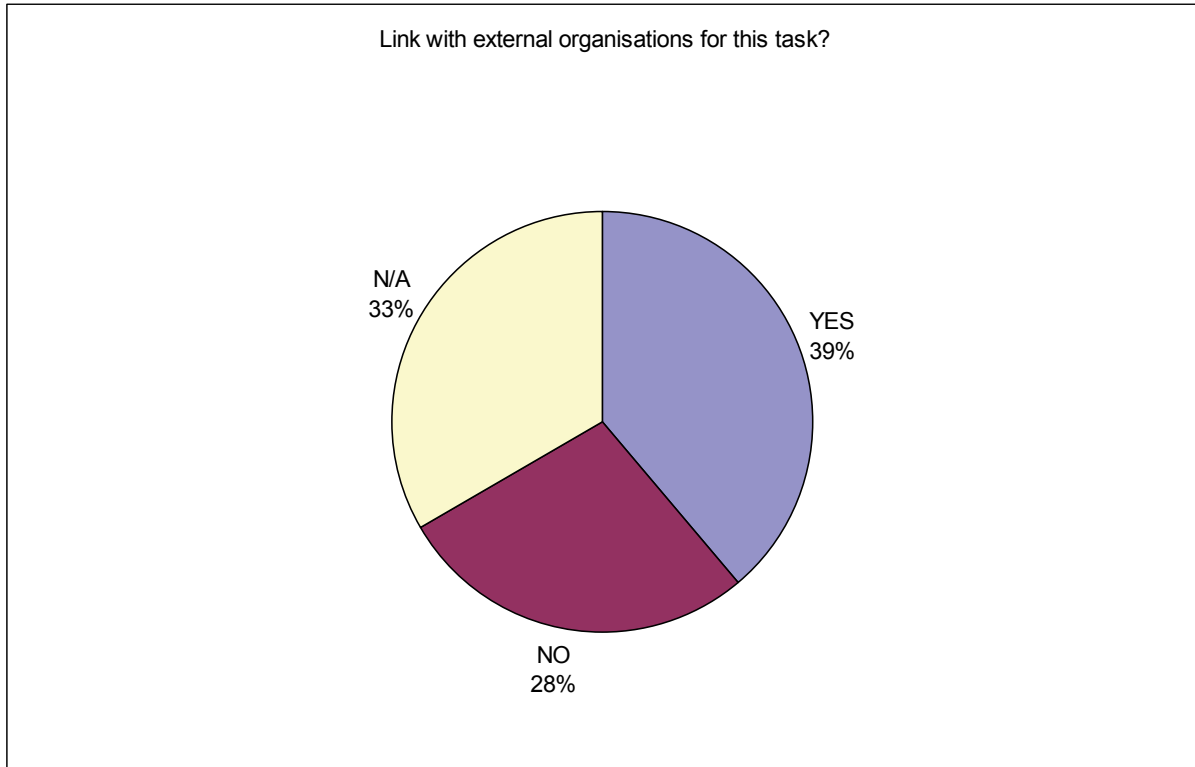


5.5.2 Person access control.

Is person access control implemented?

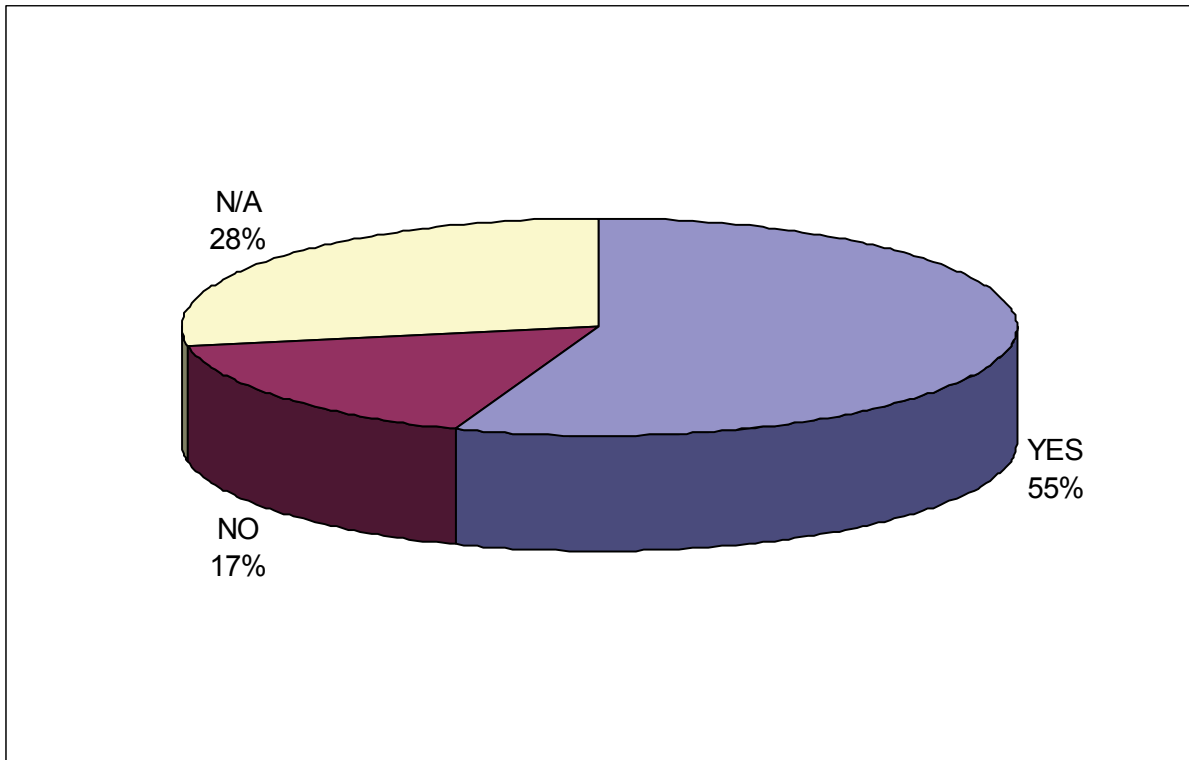


Which entities are involved in this task?

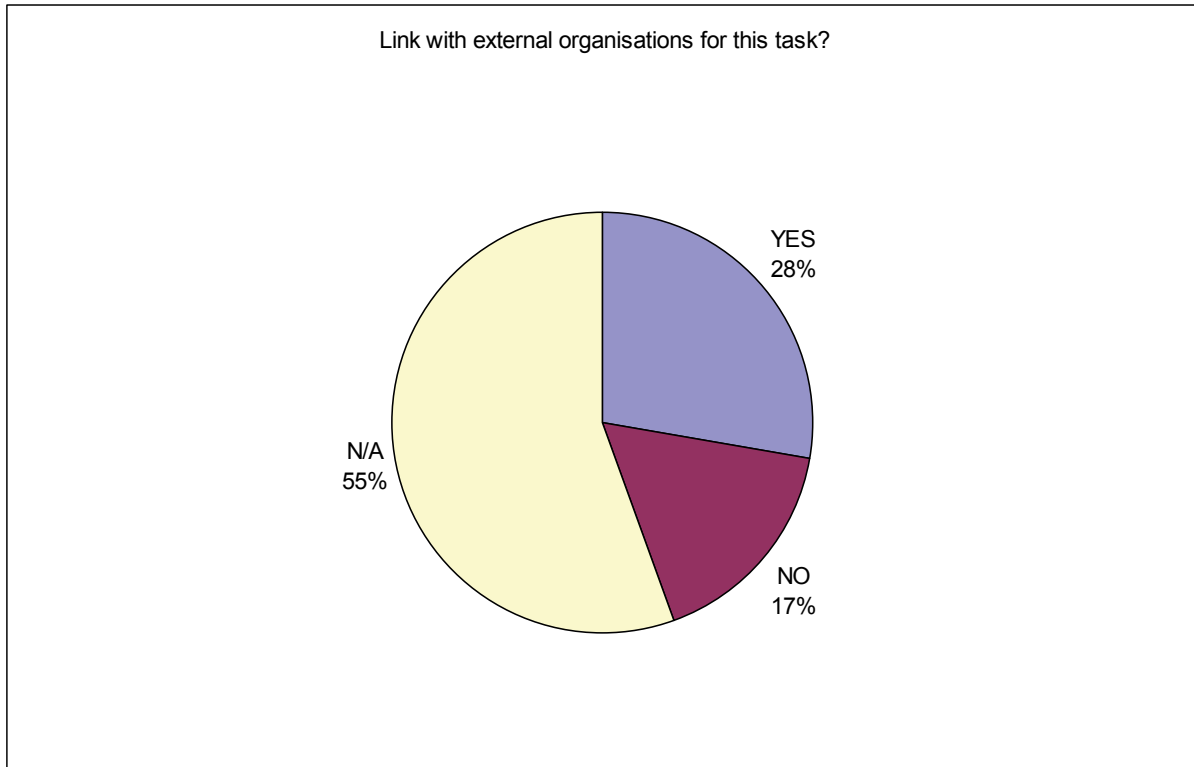


5.5.3 Design of resilient buildings.

Have resilience criteria been taken into account in the design of mass transportation infrastructures?



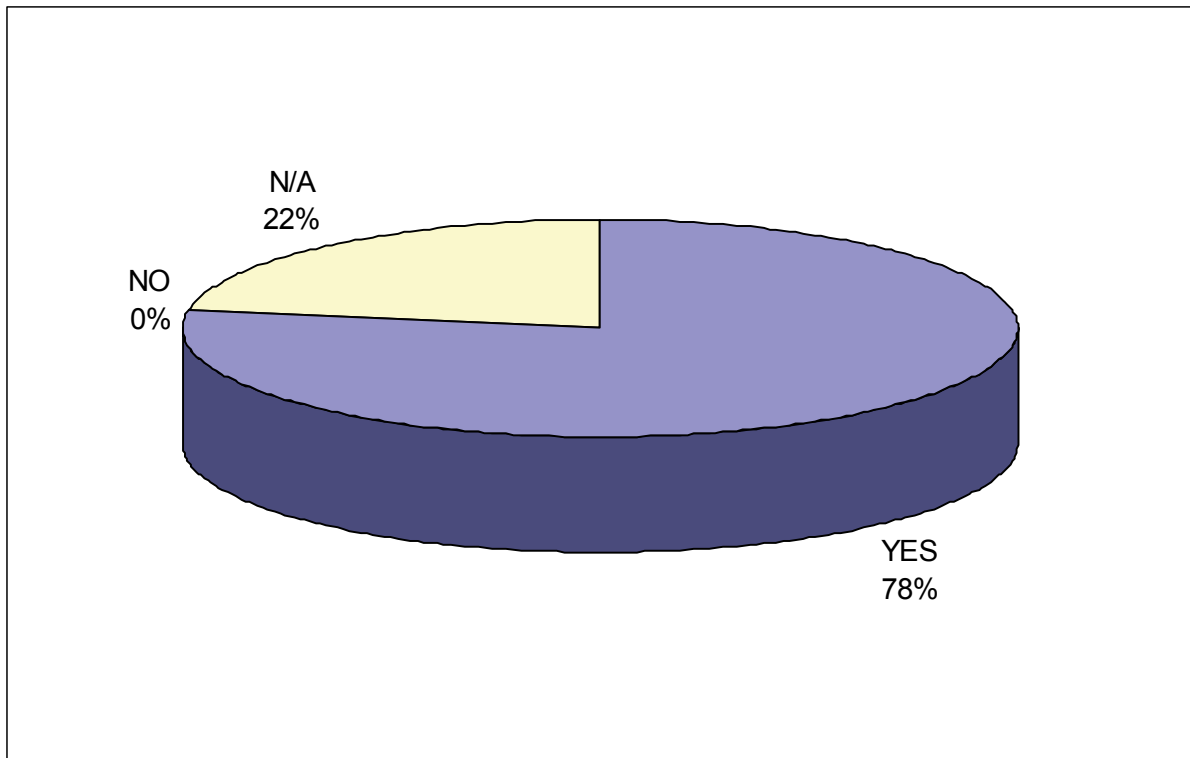
Which entities have been involved in this task?



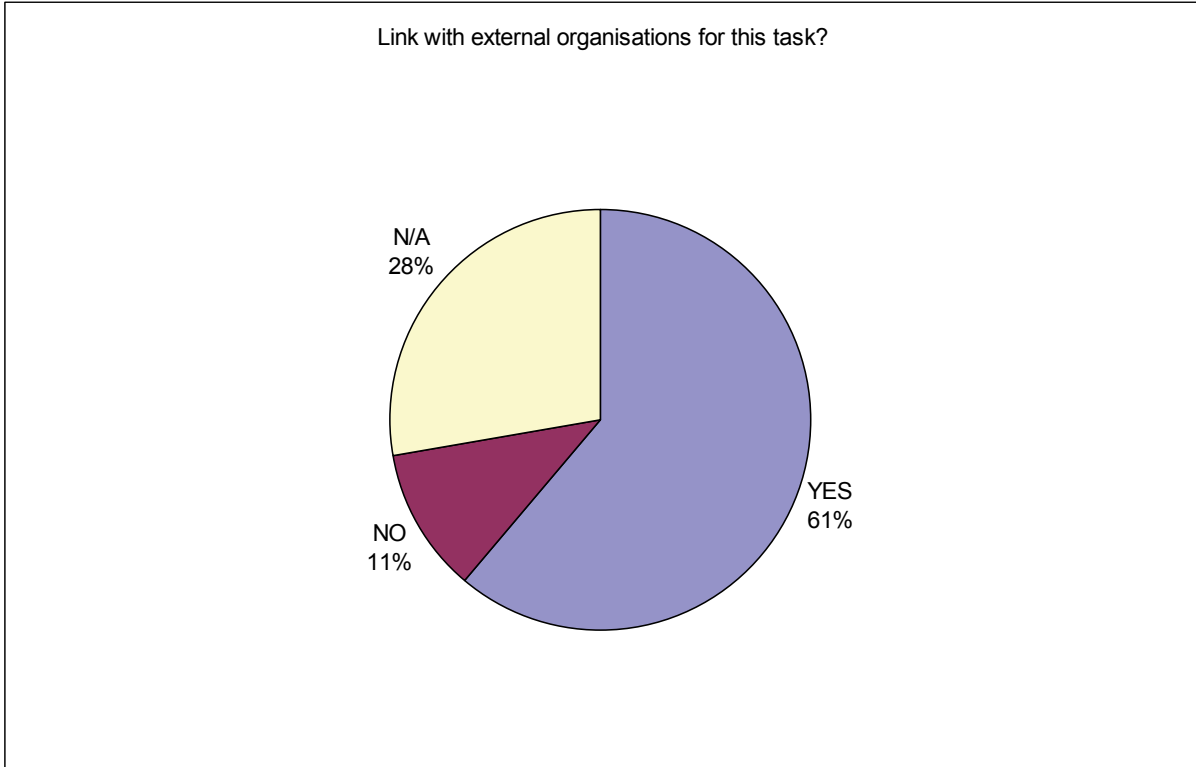
## 5.6 Preventive and early intervention.

### 5.6.1 Early intervention.

Do you have an early intervention model in order to avoid propagation?



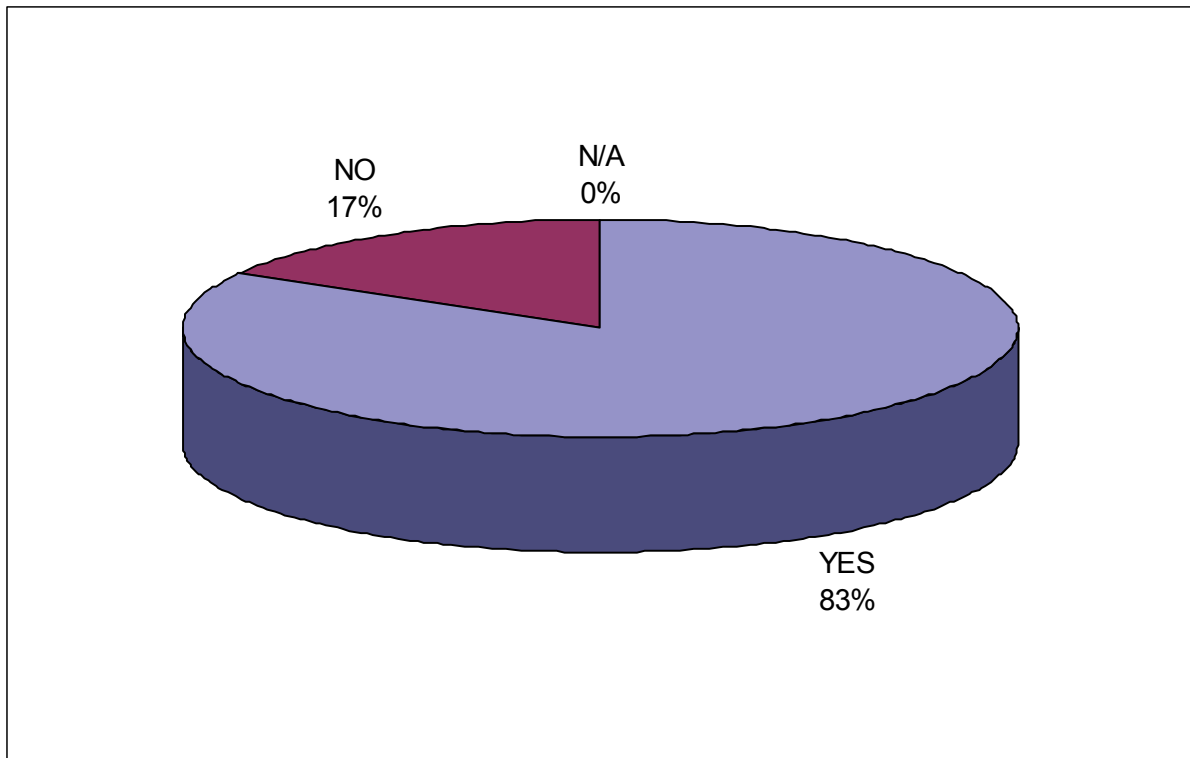
Which entities have been involved in this task?



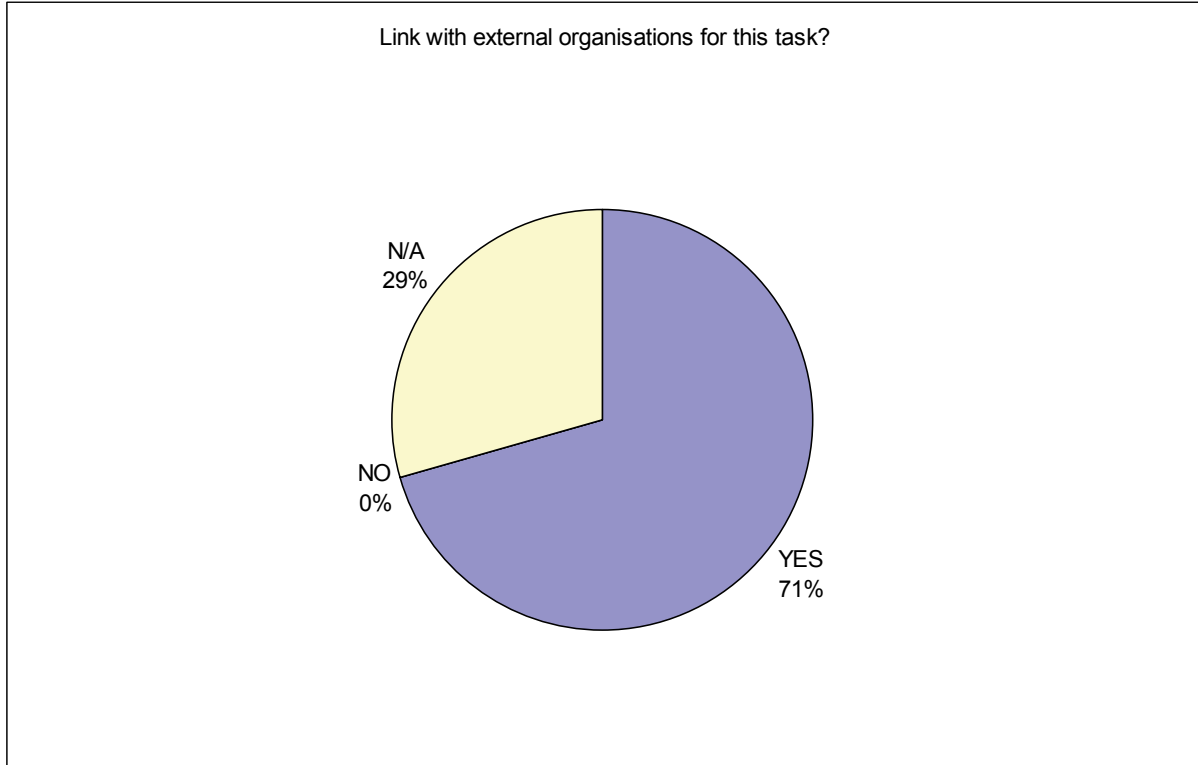
## 5.7 Post-incident intervention.

### 5.7.1 Neutralisation.

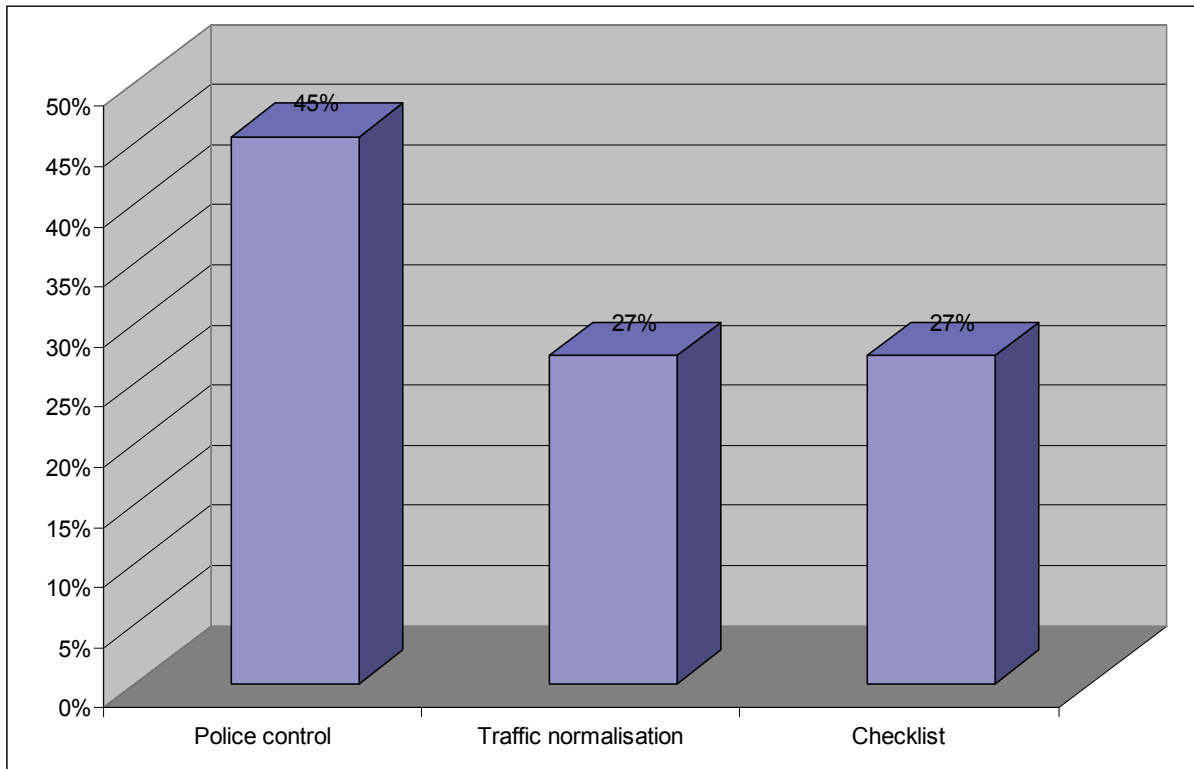
Are neutralisation measures implemented in the event of malicious acts?



Which entities are involved in this task?

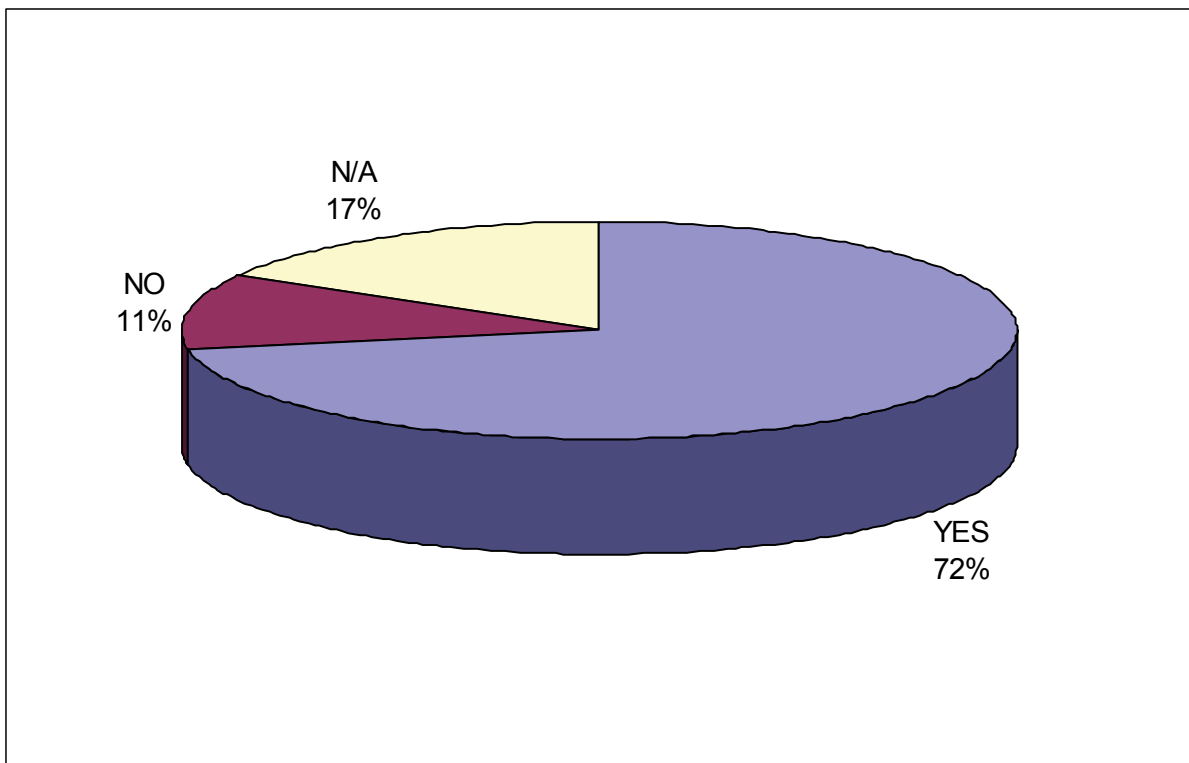


What do these measures consist on?



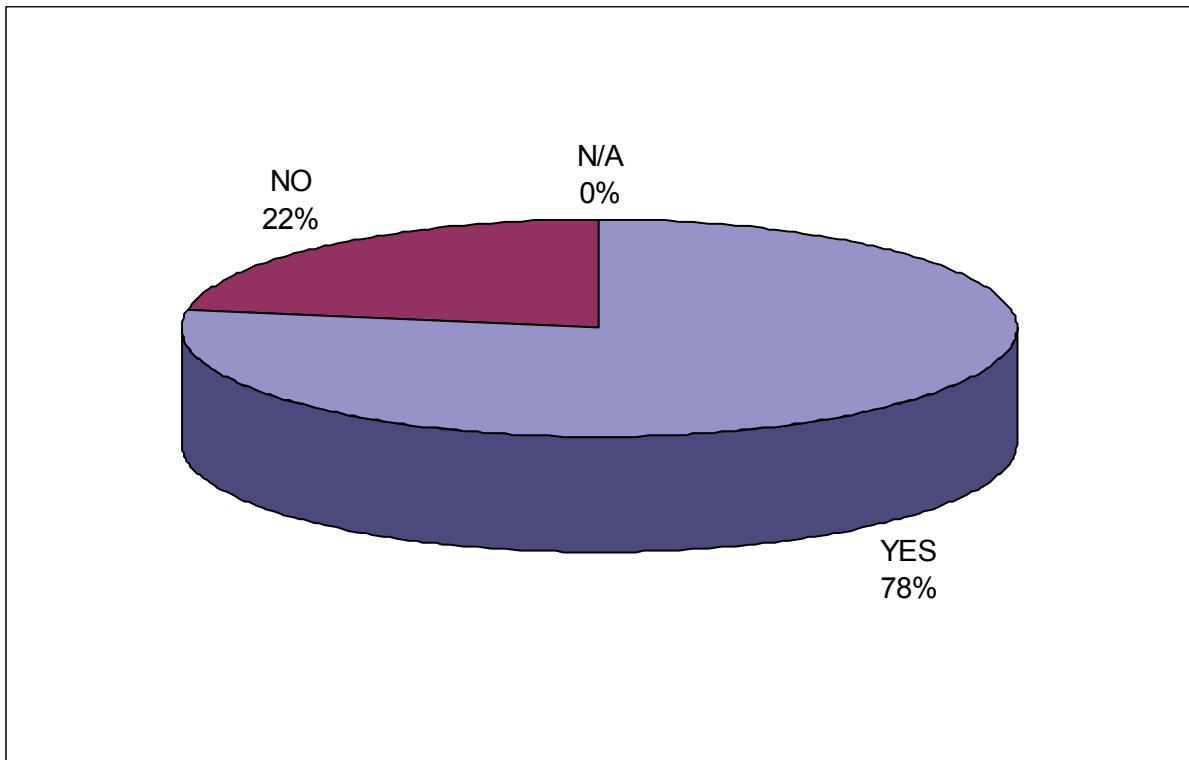
5.7.2 Rescue.

Is there a formal passenger rescue procedure implemented in the whole security system?

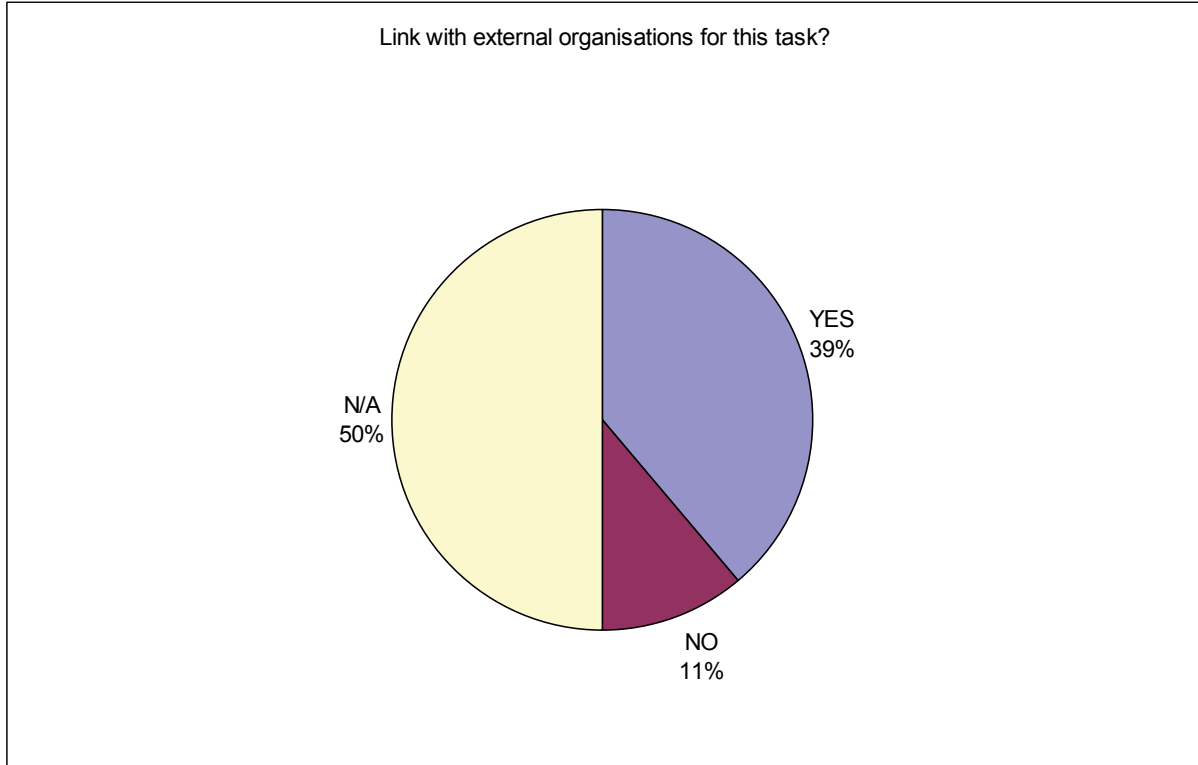


5.7.3 Restoration of services.

Does your incident response model contain a restoration of services procedure to be implemented in the event of malicious acts?



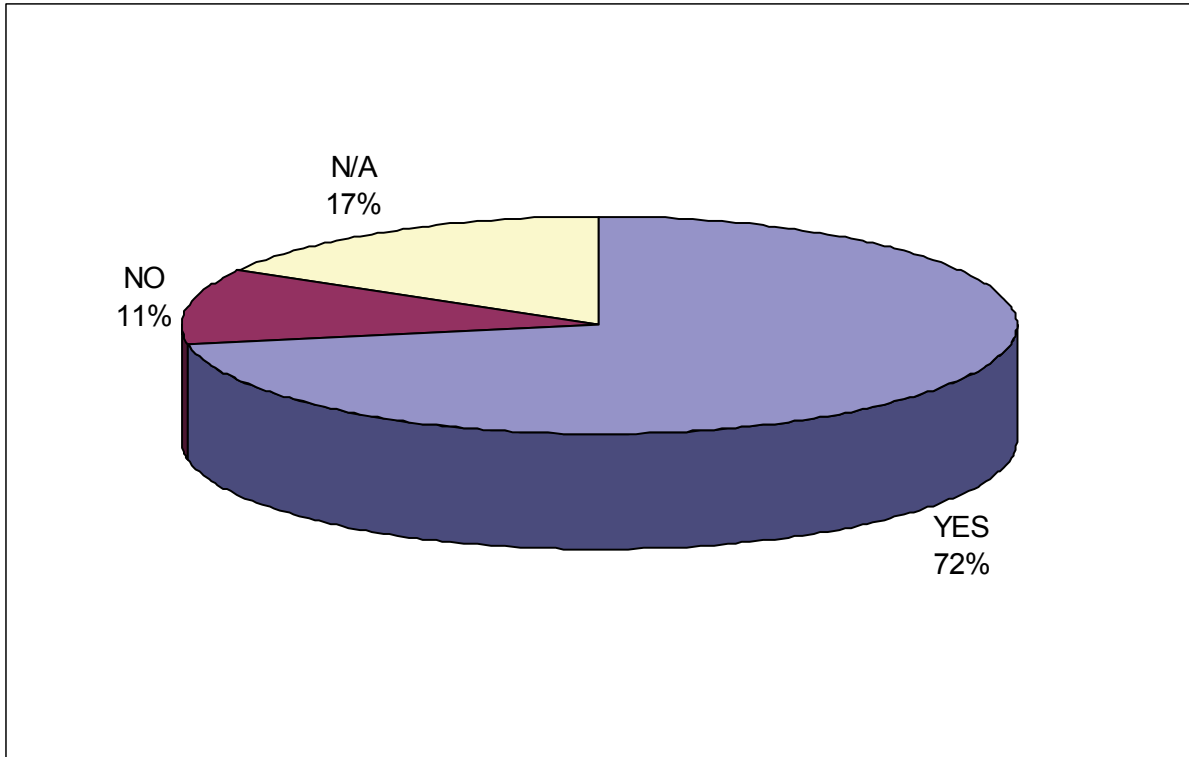
Which entities have been involved in its definition?



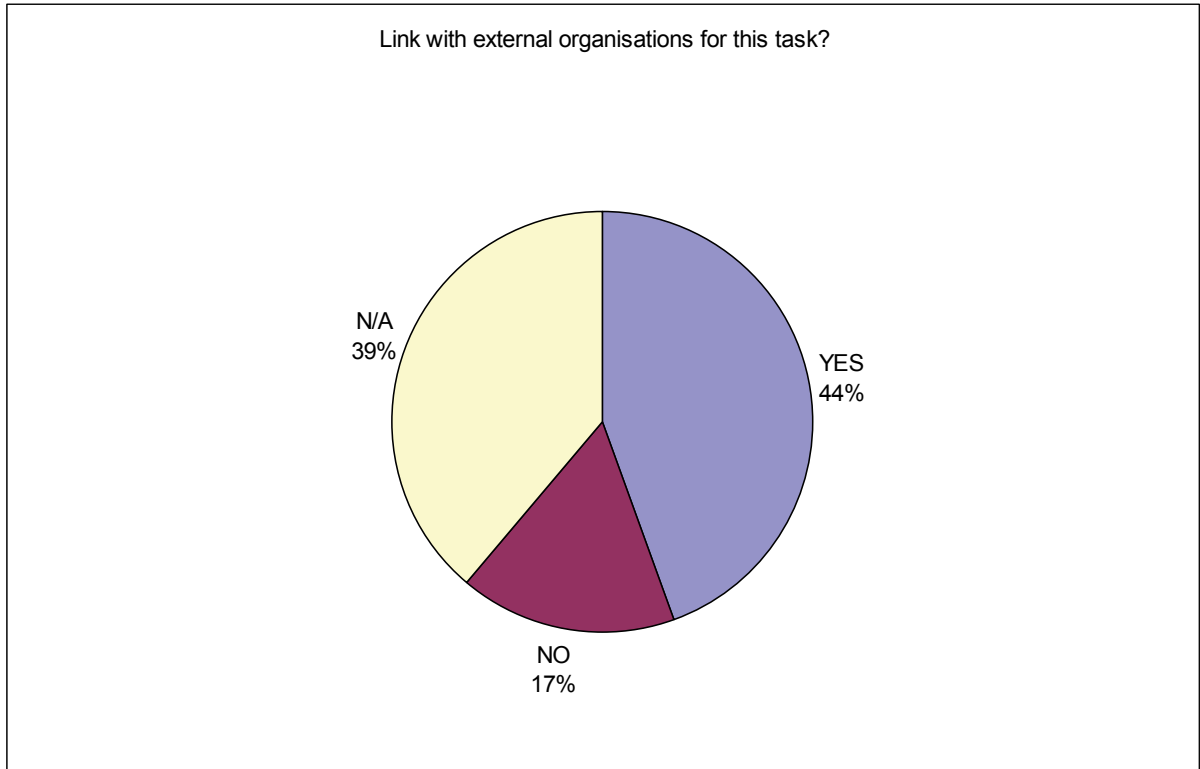
5.8 Forensics.

5.8.1 Damage assessment.

Is damage assessment systematically performed after suffering an attack?

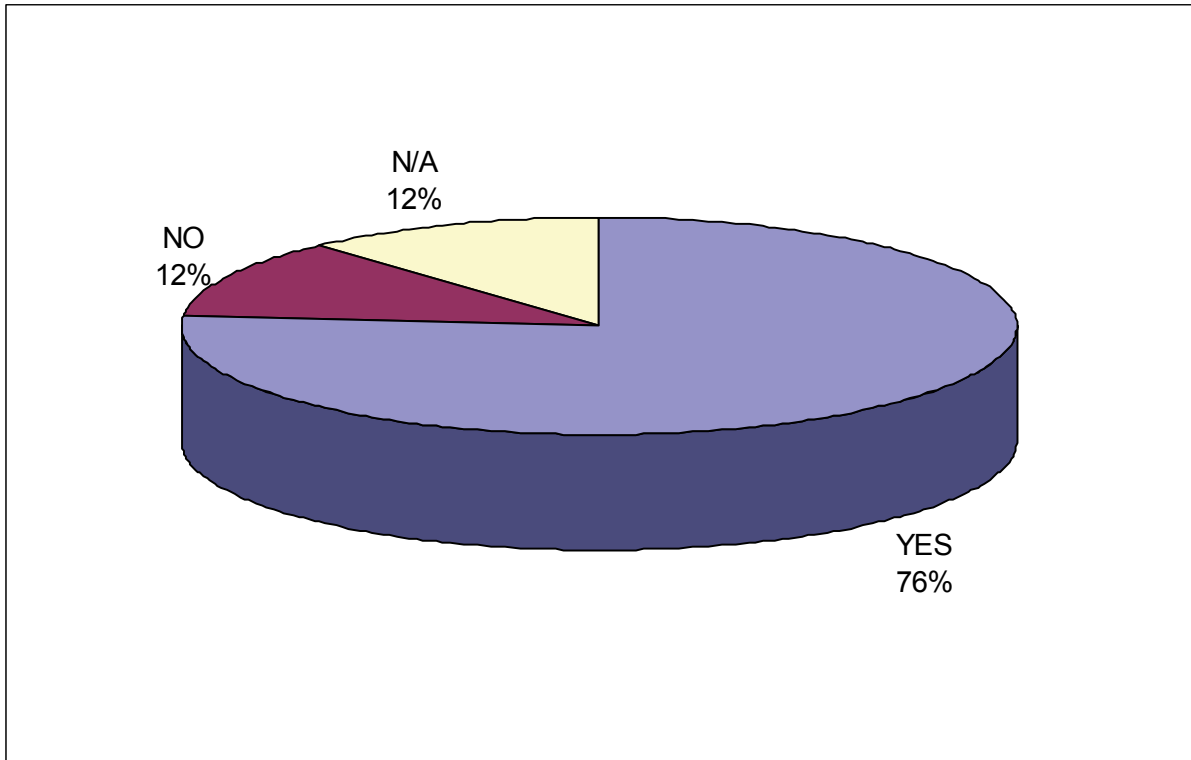


Which entities are involved in this task?

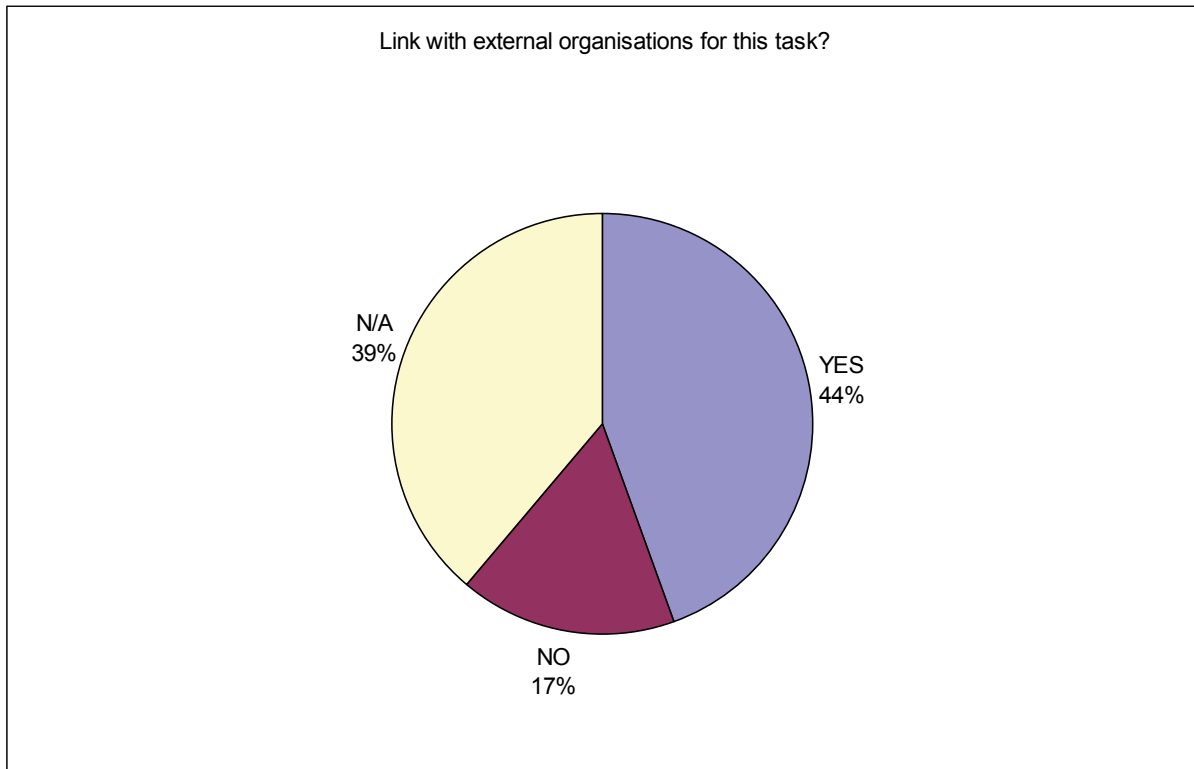


5.8.2 Post -event data analysis.

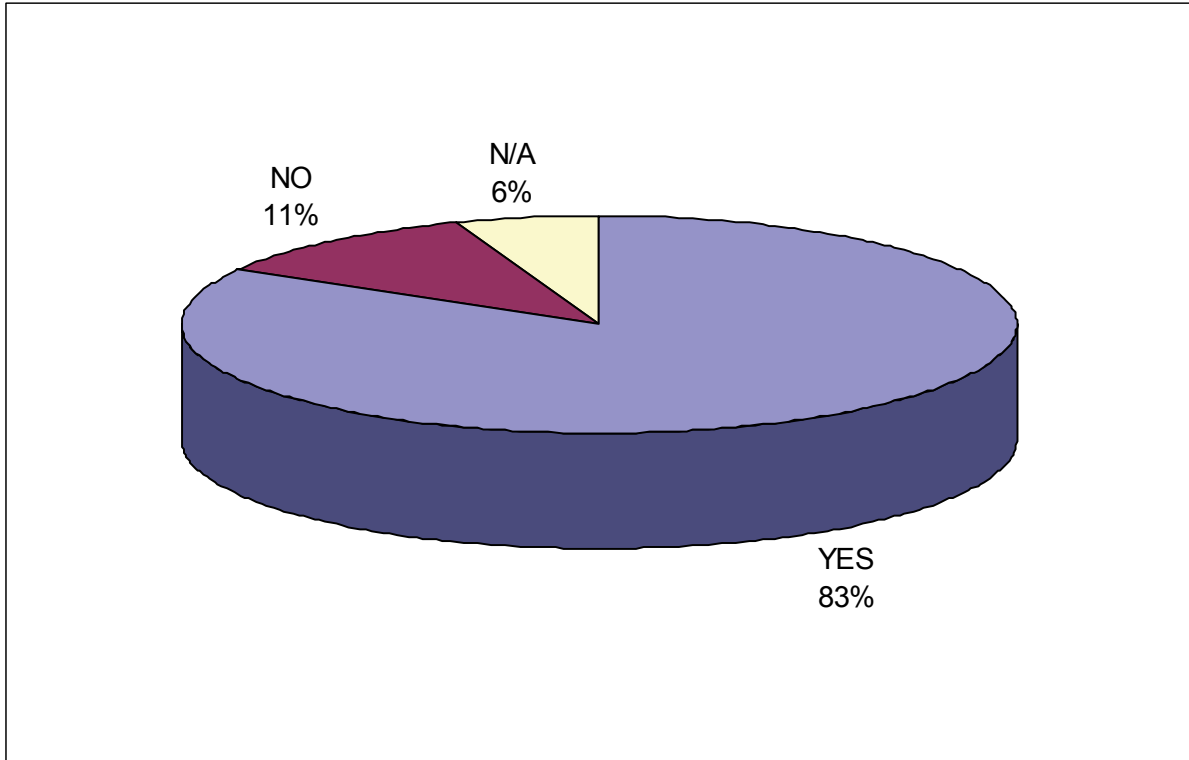
Are post-event situation analysis systems used in order to re-enact the sequence of a malicious event?



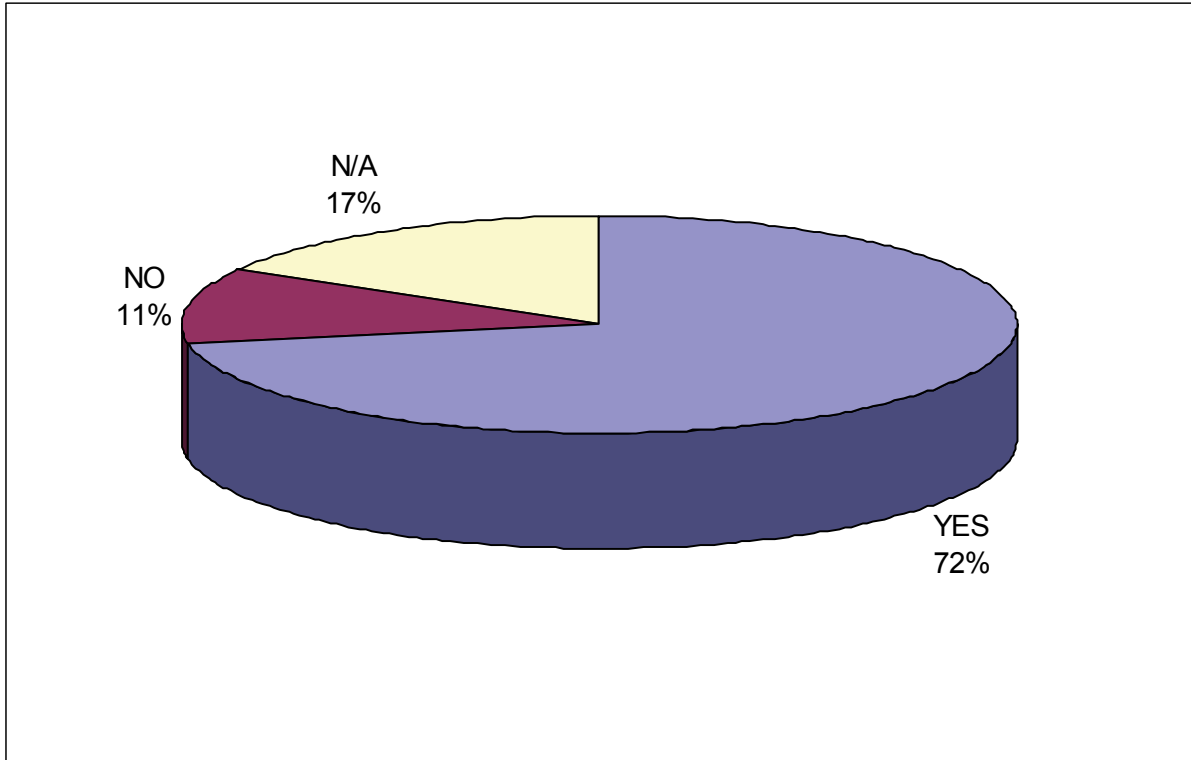
Which entities are involved in this task?



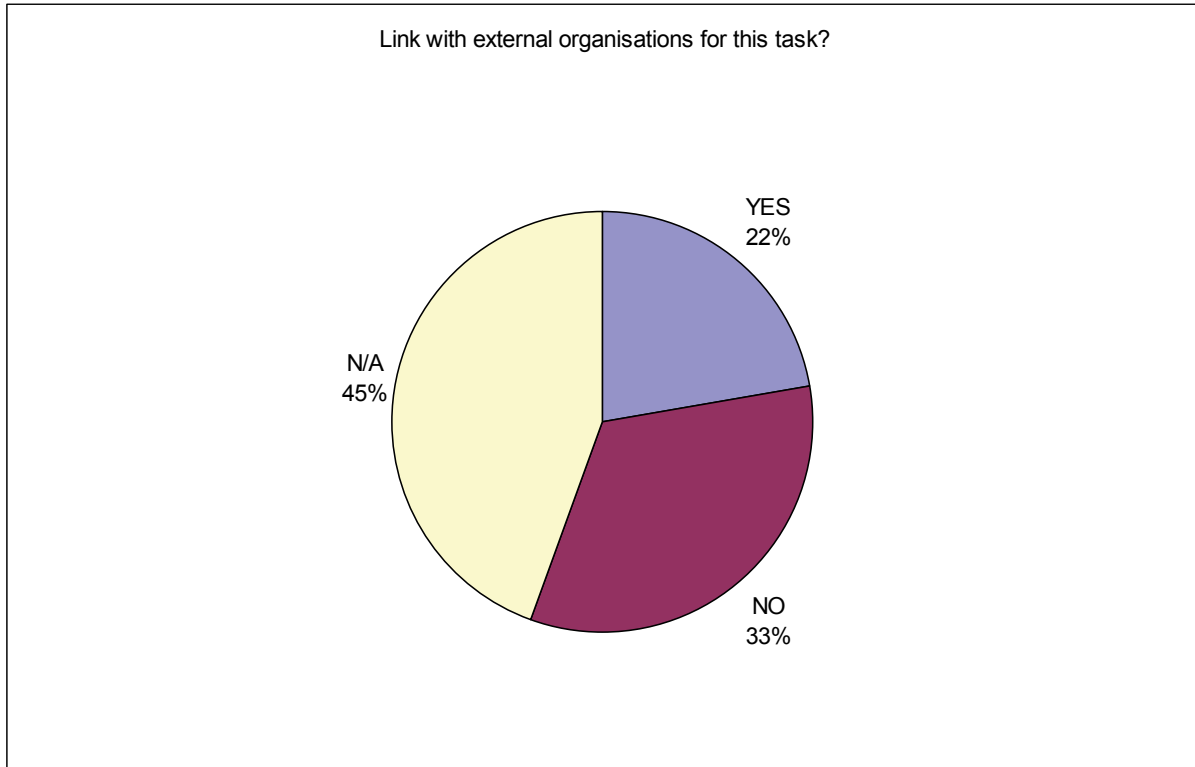
Do you have a database collecting information from previous malicious acts?



Is this used as an input to be included in your security systems?



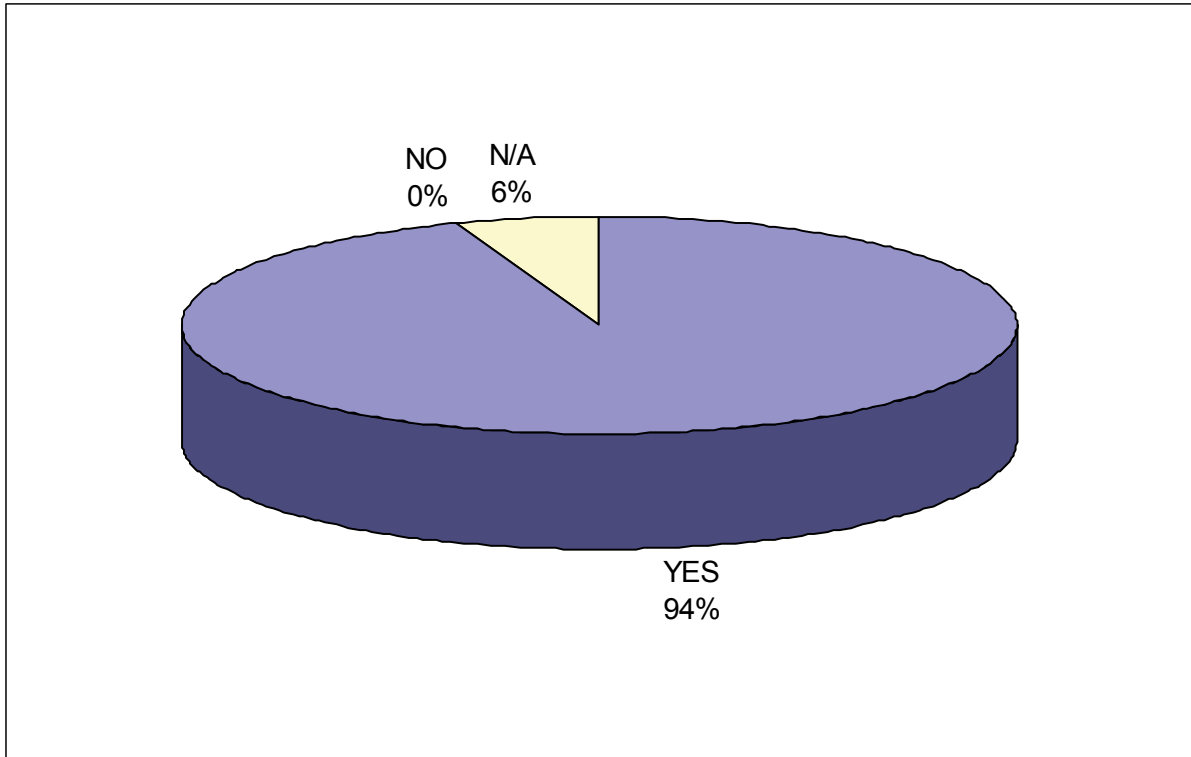
Which entities are involved in this task?



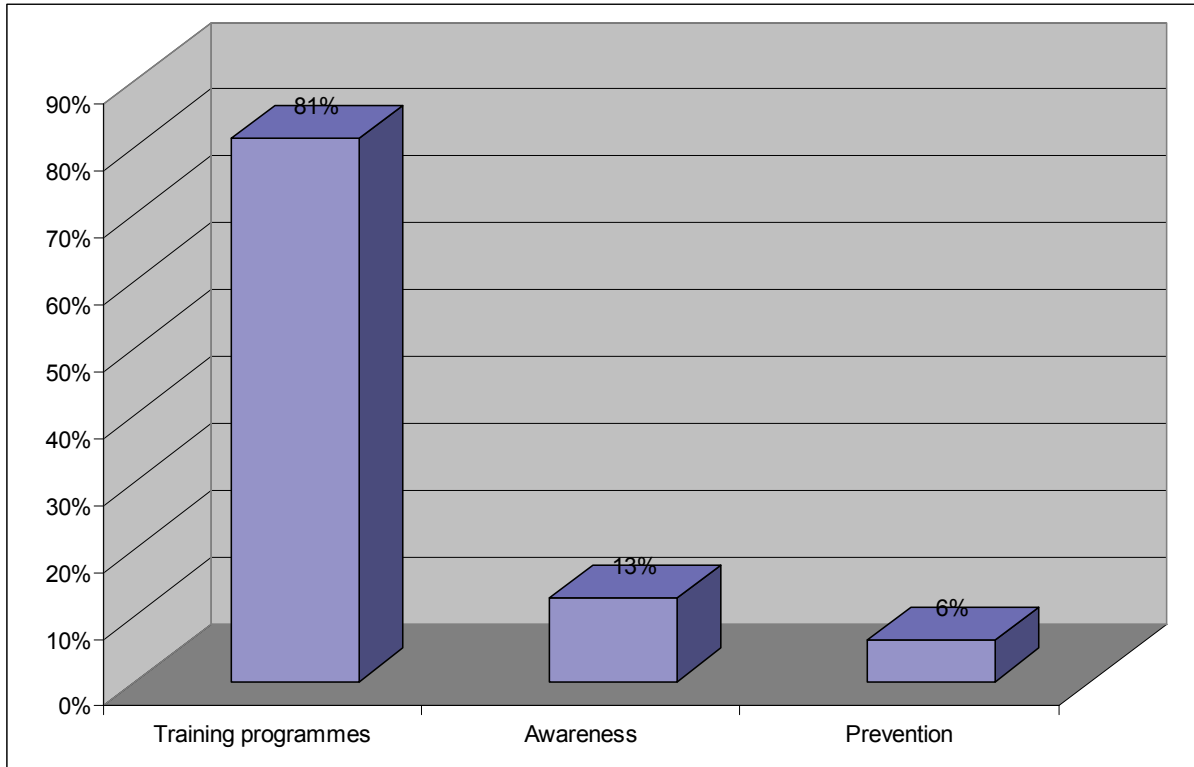
5.9 Learning and training.

5.9.1 Learning and training procedures.

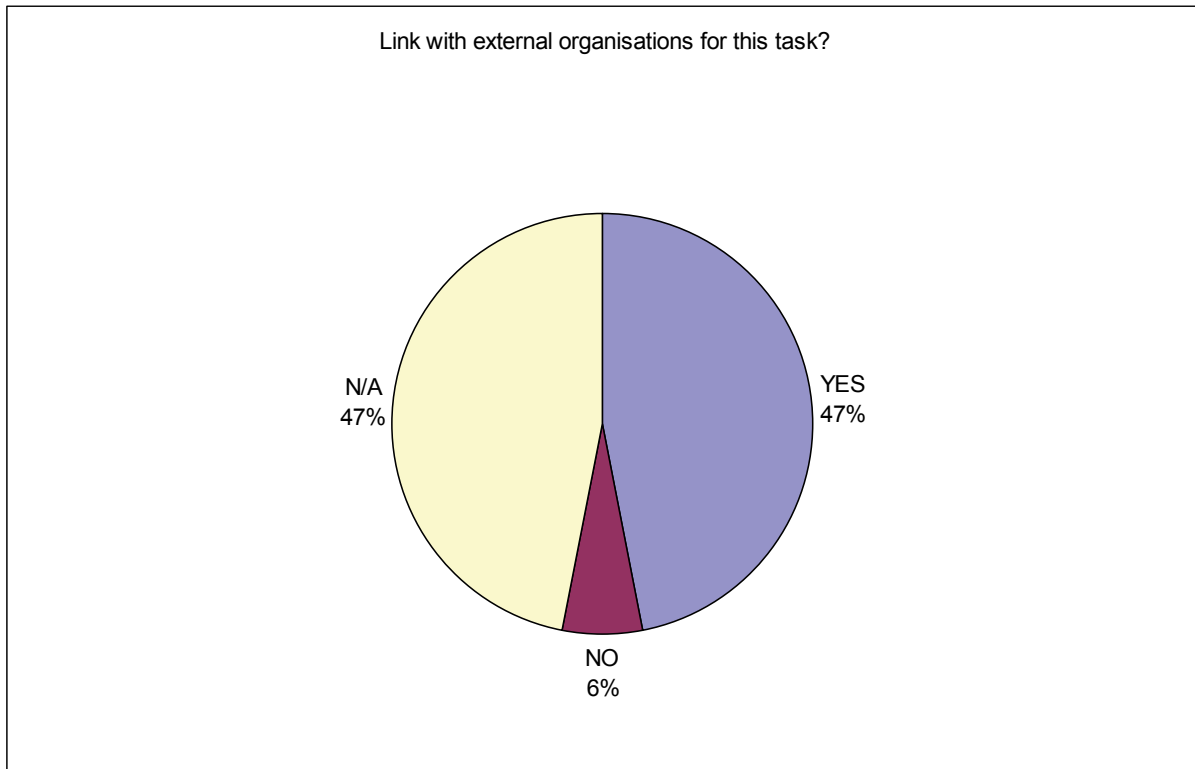
Does your entity develop crew learning and training programmes?



What do they consist of?



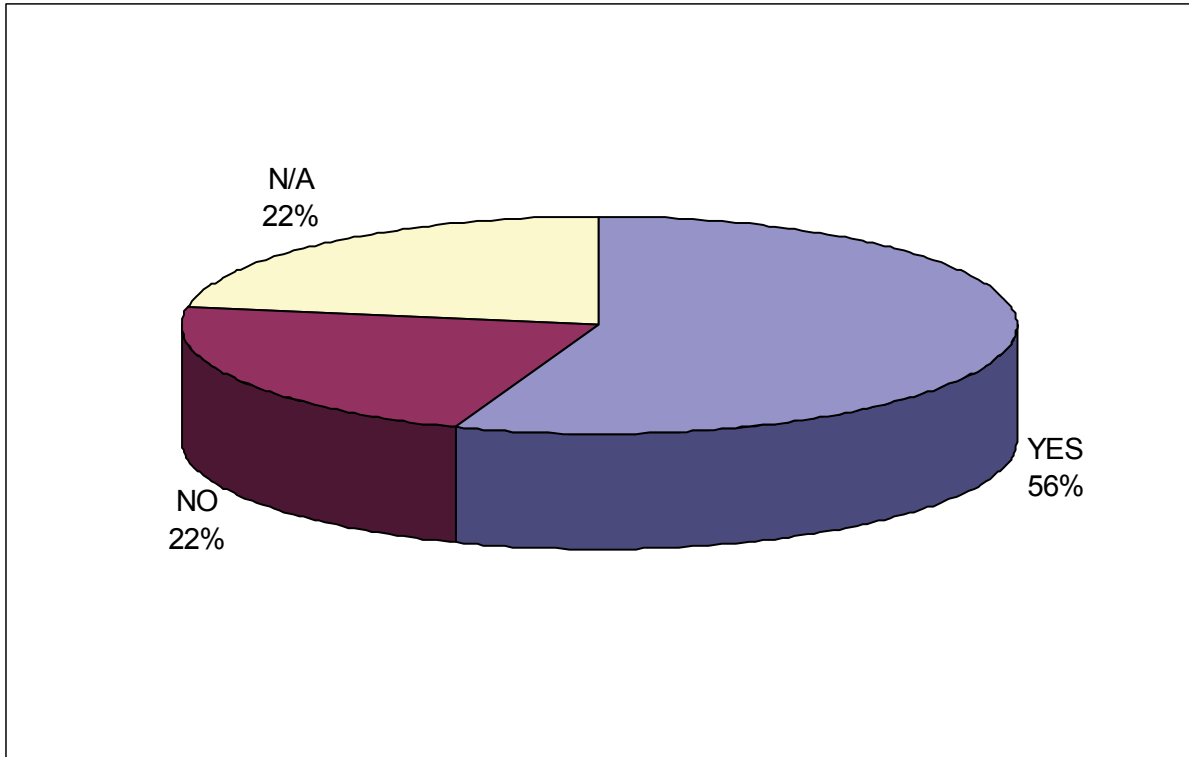
Which entities are involved in this task?



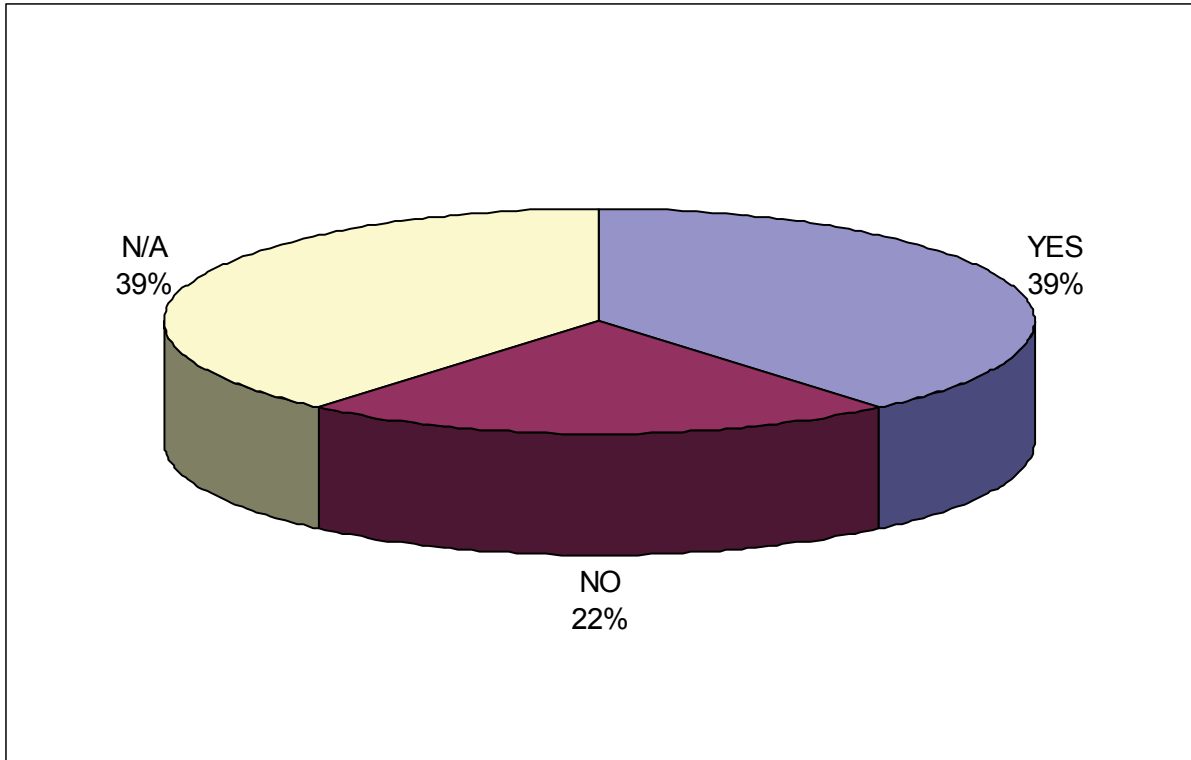
5.10 Interoperability and information interfaces.

5.10.1 Information interfaces.

Do your entity's security systems interface with other internal systems (such as operational)?

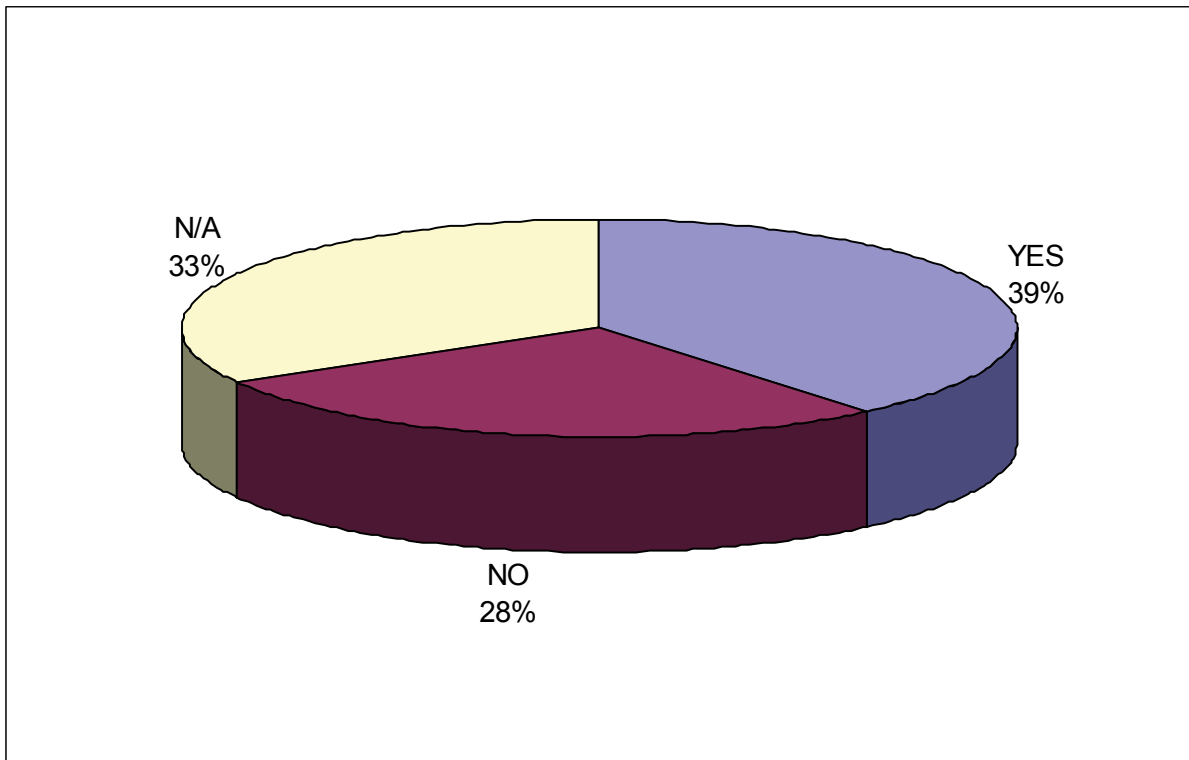


Does your entity's security system architecture and its interfaces follow any technical standard?

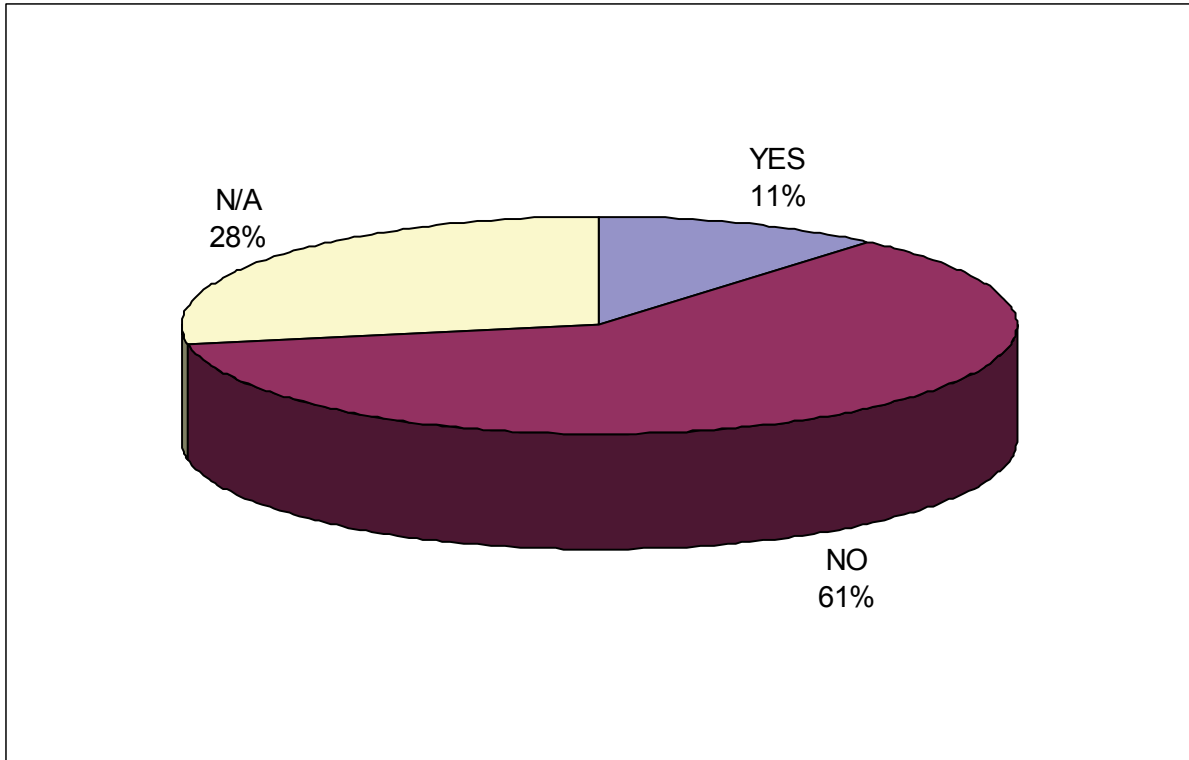


5.10.2 External interoperability.

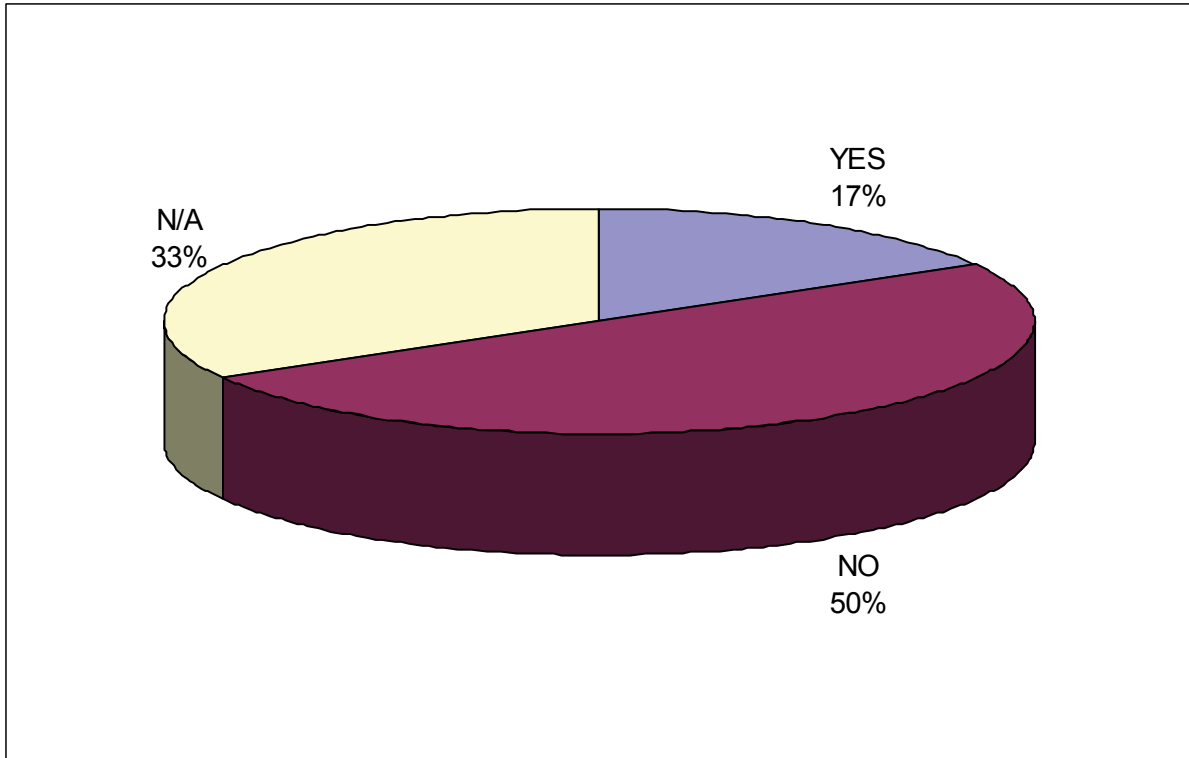
Are security systems implemented following any technical standard, national or European Regulation?



Are your security systems interconnected with security systems belonging to similar entities within the European Framework?



Are your security systems interoperable with other similar entities in the European Framework?



## 5.11 Implementation of security technologies.

### 5.11.1 Decision-making in mass transportation security systems.

Feedback from the stakeholders' regarding this issue cannot be depicted in charts since it is not based on Y/N answers. Therefore, this information is mirrored in the conclusions.

Which are the key decision factors to implement new technologies within your security system?

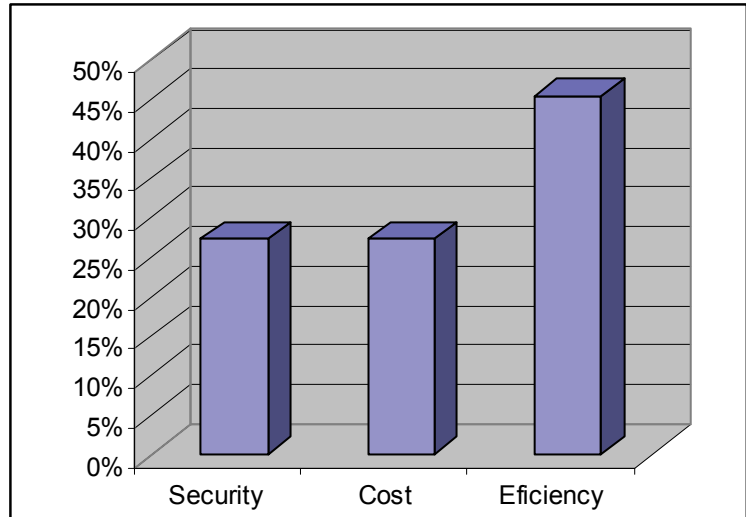
**Conclusions:**

Some lessons learned from answers given to the previous question can also be applied here.

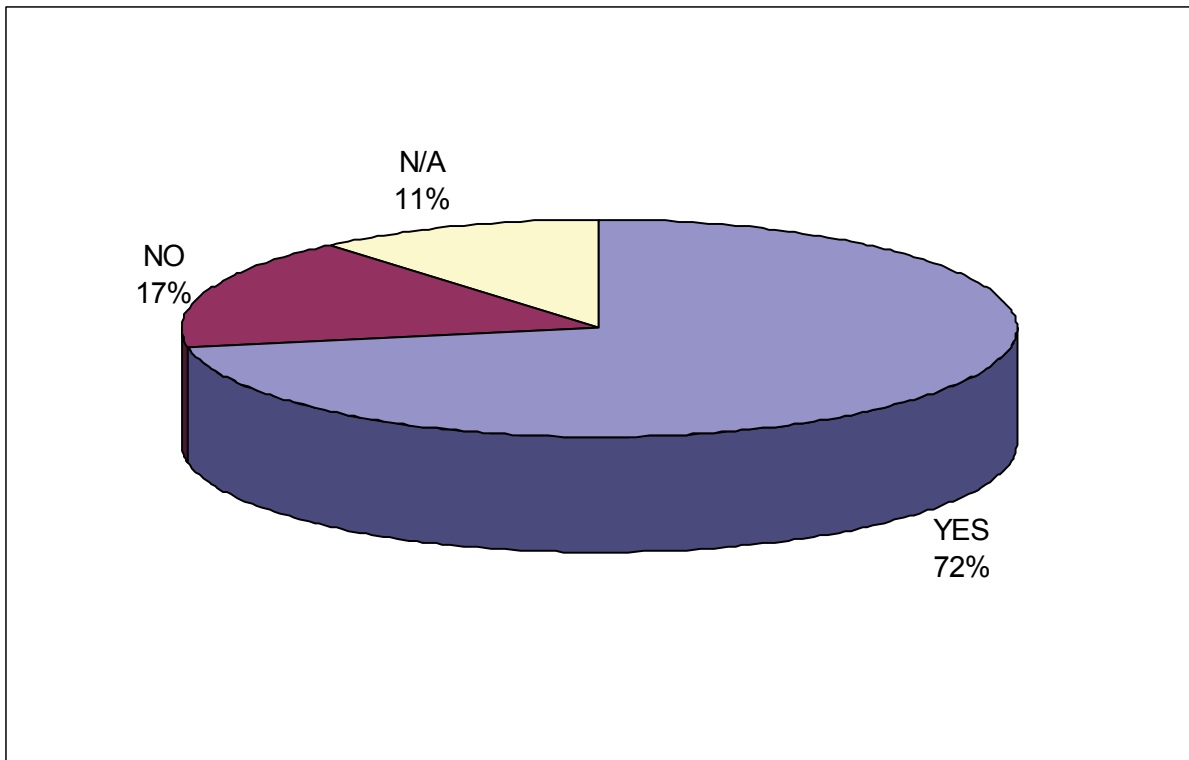
Stakeholders insist on being very cost-sensitive with regard to security measures, probably due to its nature of tax-subsidized entities and also taking into account that from their point of view improved security does not necessarily mean bigger incomes.

Rail metro operators /infrastructure managers priorities the following areas:

- Efficiency in the sense of investing the resources needed to respond exclusively to the existent threats, remarking that technologies chosen need not necessarily be the newest and most expensive solutions. In summary, aiming at solutions that are "good enough, robust, and not too expensive".
- Since new security solutions imply investment, they should be efficient solutions that bring added value in terms of security. The decision of increasing security resources should be provoked by increasing threats detected.
- New security systems can be incorporated to avoid potential human failures.



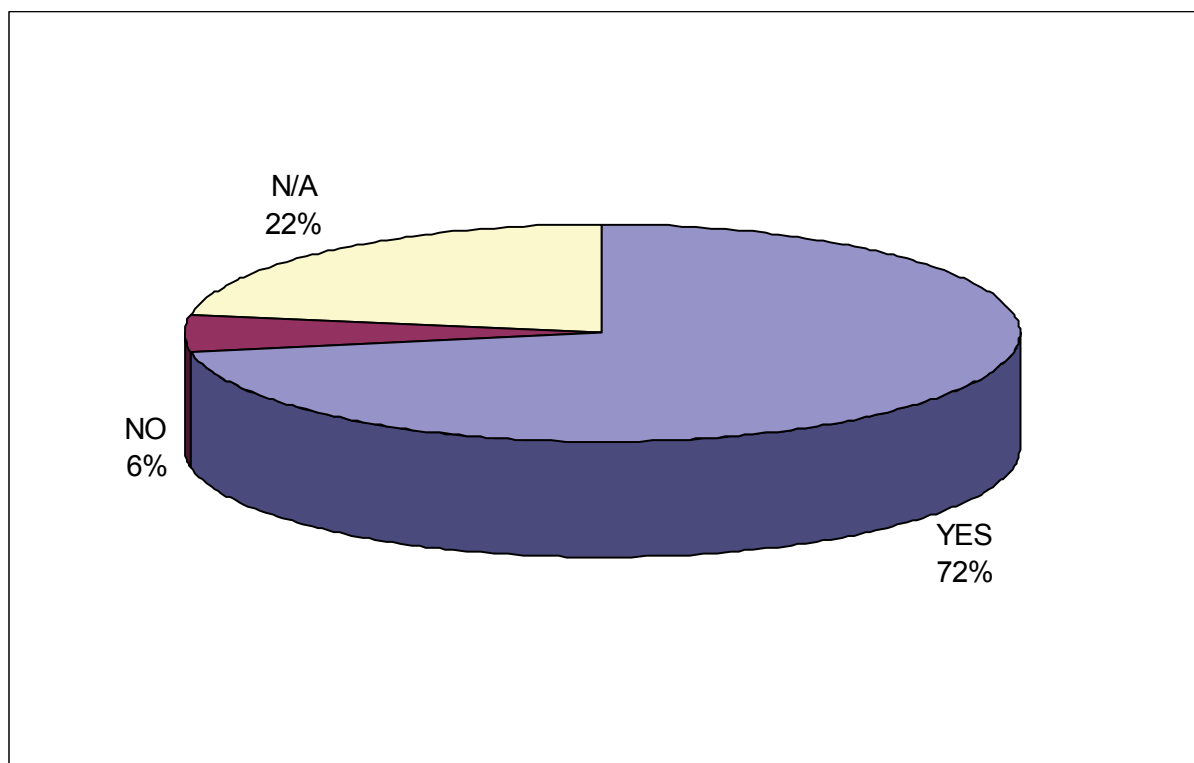
Are societal/ethical aspects taken into account before implementing a new security system or technology?



## 5.12 Security perception/ Future Situation

### 5.12.1 Security perception

Do you think passengers have a positive perception regarding security measures implemented in mass transportation?



### 5.12.2 Desirable situation of mass transportation security in the near future

What are your recommendations or demands for the near future in the frame of mass transportation security?

The huge variety in the answers received makes impossible to group them in charts.

END OF DOCUMENT.