Security @ CERN

Ll. Miralles. SMB

Security: the combination of human, technical and organisational methods designed to forestall, avert or reduce the risk of occurrence of a malicious act*.

*The term "**Malicious act**" refers to risks of human origin, caused either deliberately or through voluntary lack of action, with the intent to harm a person, organization or property.

Summary

- CERN security framework
- Legal basis
- CERN security strategy
- Video Surveillance
- Examples
- Guards
- Conclusions

World security framework today

- The worldwide security situation has changed significantly over the last few years :
  - Risks have evolved
  - Threats have become more widespread
  - Risk analysis has become more difficult
  - Security has become one of the public's primary concerns
- Organizations take all these factors into consideration and integrate them into their strategies.

CERN’s security principles

- CERN's primary security objective is to ensure the protection and safety of all persons on site.
- CERN does not want to give up its fundamental principles established by its Convention:
  - It wishes to preserve the freedom of movement and a campus ‘spirit’ that promotes creativity,
  - It needs to take into account the particularity and diversity of the site, as e.g. industrial aspects of its activities.
- CERN is the custodian of the financial contributions of the Member States and must protect all the investments made.
- CERN security strategy is fundamentally influenced by its relations with the Host States on security matters.

CERN's today security challenges

- Security considerations of CERN context.
  - CERN has the distinctive features
    - established on 2 Host States across the border, distributed on 16 sites, covering a fenced area of 200 hectares with a perimeter of 22 km.
    - around 26 000 people hold an access card and 22 000 vehicles are registered to enter the sites.
    - more than 130 000 visitors every year.
  - To enable CERN population to enter the sites, CERN has:
    - 20 site entrances that handle 20 000 entries a day
    - 855 card readers that control 13 000 entries a day
  - With the exception of the Prevessin and Meyrin site, most of CERN's sites are far apart and located in rural areas that are
    - rarely frequented,
    - often at some distance from residential areas.
  - the increase in user numbers and its impact on the security facilities,
  - the obsolescence of certain facilities,
  - the need to intensify and coordinate collaboration with the security forces of Host States.
- This makes the sites particularly vulnerable to intrusions and thefts.
- It is important that all this is taken into consideration when determining CERN's security policy, in terms of both equipment and human means.

The nature of the threat

- Characteristics of the risk of malicious acts
  - Like any organisation, CERN is obliged to contend with different types of risks in its daily functioning.
  - CERN takes account of intentional and calculated actions to define the risk of malicious acts (theft of property, theft of information, vandalism, damage or destruction, physical aggression, etc.)
  - The security measures will therefore cover many aspects, seeking above all to protect the values of the Organization. These values may be :
    - human (protection of people),
    - material (protection of property), or
    - immaterial (protection of image or reputation).
- *N.B.: Terrorist threats are handled by the specialised services in the Host States, who inform CERN in the event of an increased threat. CERN is then responsible, by activating CMT (Crisis Management Team), for proposing additional measures to be adopted.*

General overview of the legal framework

- General principle of Public International Law under which a Host State must provide assistance to IGOs seated on its territory. The 1955 Accord de siège allows the Swiss authorities to take measures in the interest of the security of Switzerland and, in agreement with the organization, the latter's security .

- The 1965 Franco-Swiss Convention contains several provisions on actions that may be undertaken by Host States in the field of security.

- The Swiss Federal Act on the Maintenance of Internal Security of 1997 and the Host State Act of 2007 contain provisions on the protection of intergovernmental organizations located in Switzerland.

- The 1972 Status Agreement with France includes provisions which are similar to those of the 1955 Headquarters Agreement with Switzerland but also stipulates, in particular, that the French authorities may be called upon to ensure the protection of the Organization's sites and the maintenance of order in its immediate neighbourhood.

Legal framework

- While CERN must assume its responsibilities for the protection of its sites, protection obligations are incumbent upon its Host States under existing agreements and public international law, and the parties concerned collaborate in this effect.

Regulatory framework

- Operational Circular N°2: Conditions of access to the fenced parts of the CERN site,
- Operational Circular N°10: Principles and procedures governing investigation of fraud,
- Implementation measures for Operational Circular N°2,
- Contractors and their staff: access to and activities on the CERN site,
- Rules for the use of Gate E,
- Rules for use of the tunnel “intersite”,

CERN security strategy

- CERN security strategy
  - **Close collaboration** with the security services of the Host States (CH and FR)
  - **Physical security** protection measures aligned with the organization geographical environment.
  - **Preparation and training** for security events. Crisis management.
  - **Resilience** of the organization on security events.

Collaboration with the Host States

- In order to increase reactivity CERN has:
  - developed institutional and operational relations,
  - professionalized the security function,
  - developed bilateral operational relationships,
  - actively collaborate with the authorities in the handling of infringements,
  - formalized relationships through validated procedures.
- The result is:
  - better monitoring of cases by the authorities,
  - a recognized quality of investigations conducted by CERN,
  - faster on-call interventions,
  - skills recognized by our interlocutors,
  - increased confidence.

Physical Protection

- Measures established to get a level of physical security aligned with CERN geographical environment:
  - invested in the renovation of access points,
  - improved the quality and speed of access controls,
  - standardized some equipment
  - renovated the perimeter protection when opportunities arises
  - diversify guards contract activities,
  - developed optimization tools for guards (electronic log book, GIS supported patrolling, ….)
  - badge wearing
  - invested in video surveillance and analytics

Physical Protection

Implementation of measures as the mandatory CERN card-wearing or video surveillance follows the recommendation emanating from the two Host States, with the aim to improve security within the Organisation.

It must also be reminded that, even though CERN is responsible of its own site-security, the Organisation is located on the national territory of France and Switzerland, both remaining responsible for the security on their own territory.

This recommendation does not refer to specific security threats but reflects the global trend in both France and Switzerland.

CERN shall be able to demonstrate that has taken reasonable security measures

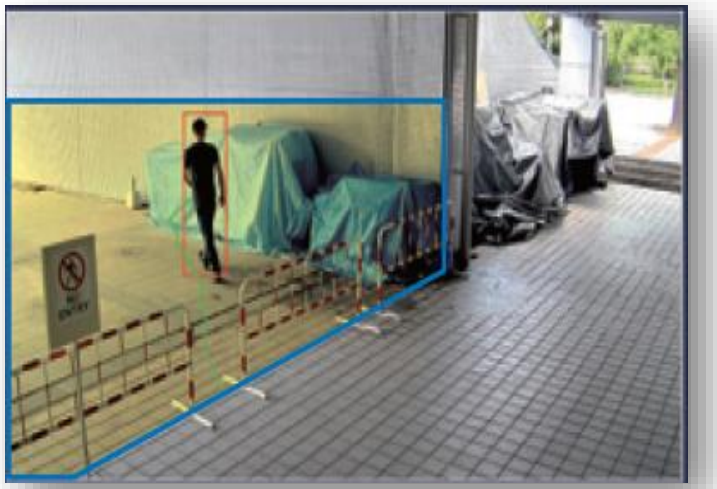
Measures as the badge wearing and video surveillance:

- are considered as good practise security measures
- protect CERN as organization
- contribute to the safety in case of incident/accident

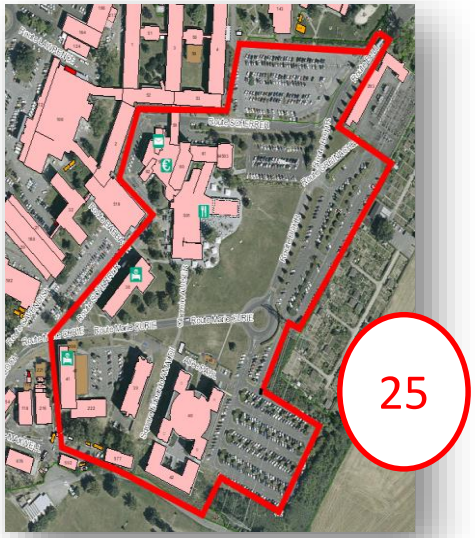
Video surveillance project cameras

Camera type	N° camera
Outdoor	284
Indoor	62
Specific	59
TOTAL	405

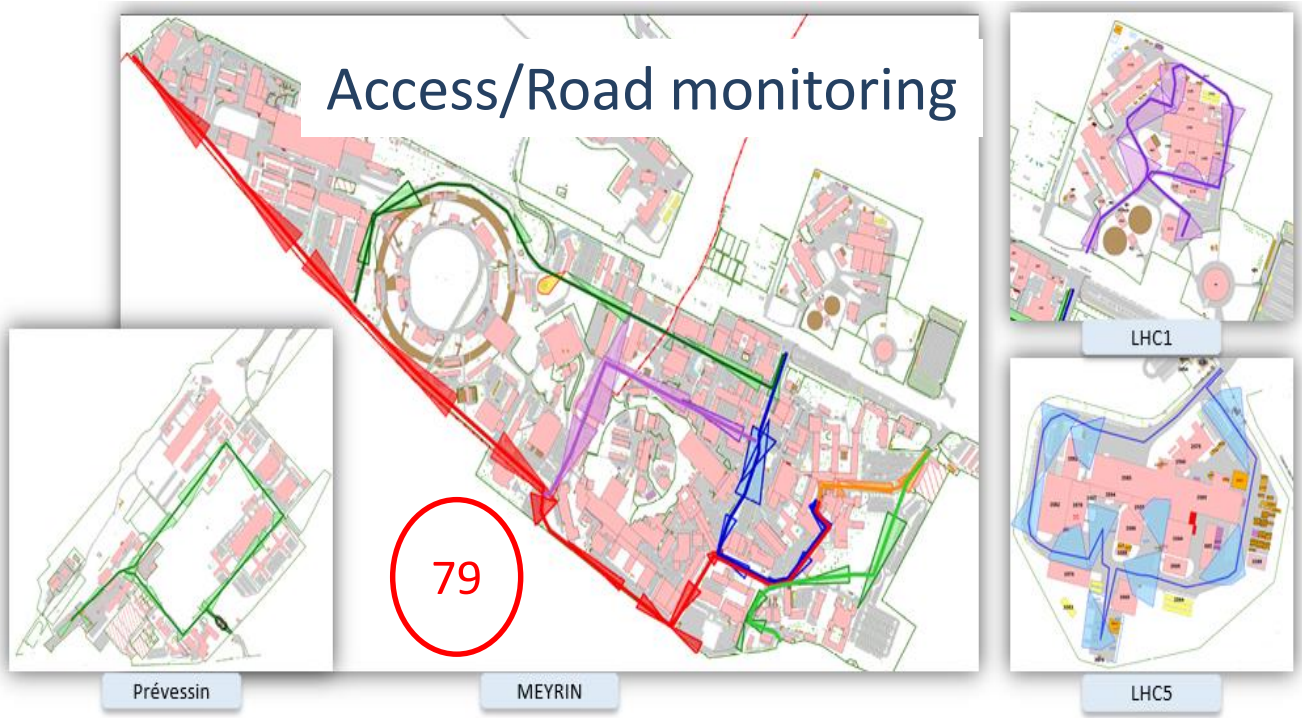
Specific camera



General surveillance outdoor cameras



Campus area

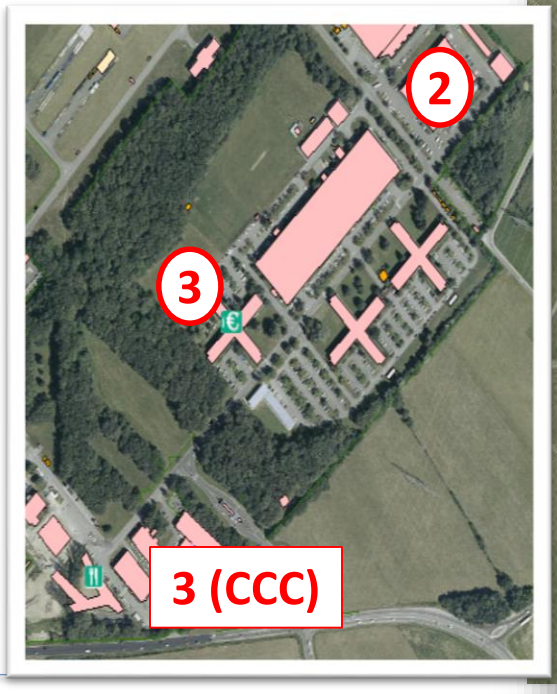


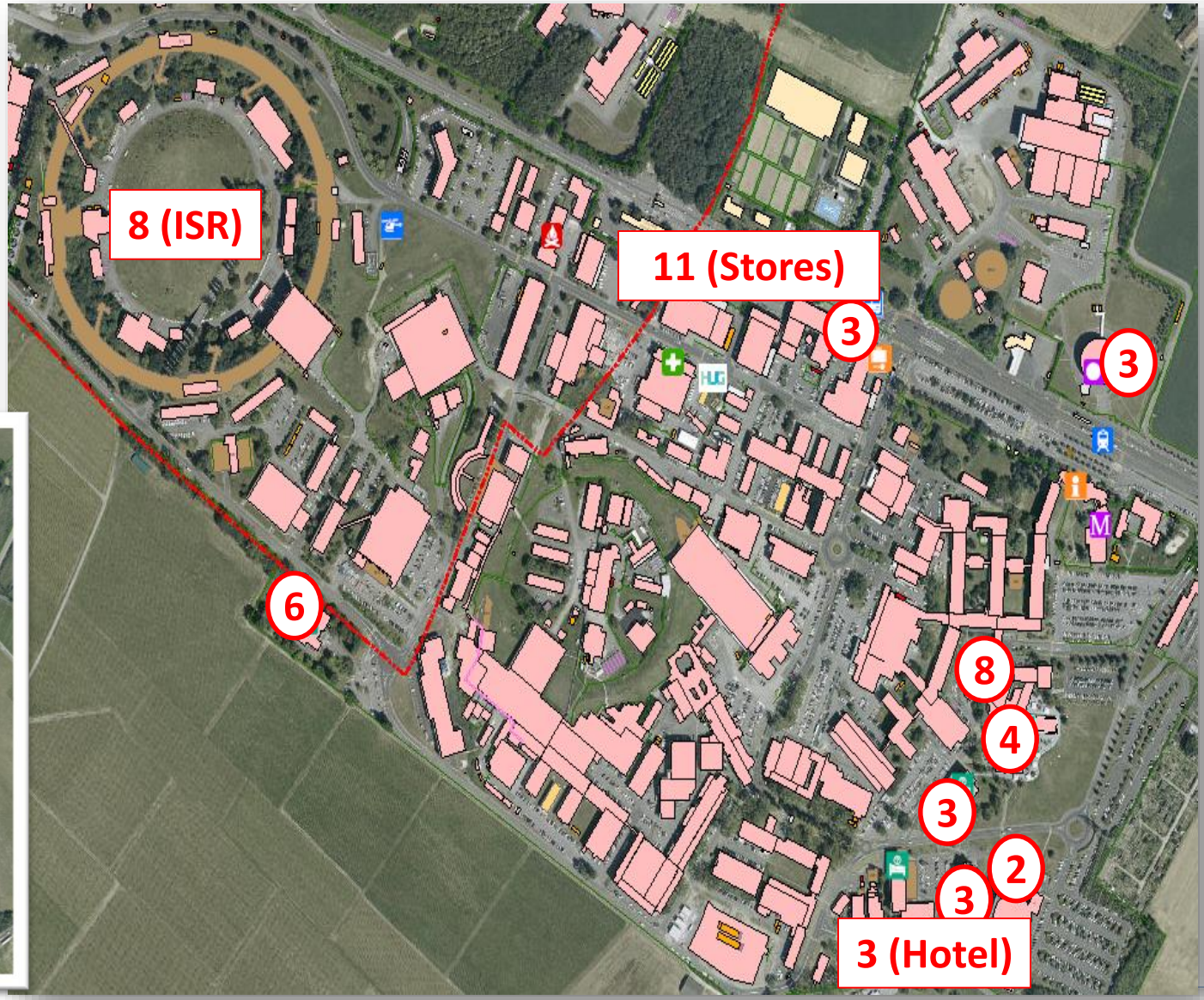
CERN sites

Total n° cameras : 284

Sensitive Sites indoor cameras

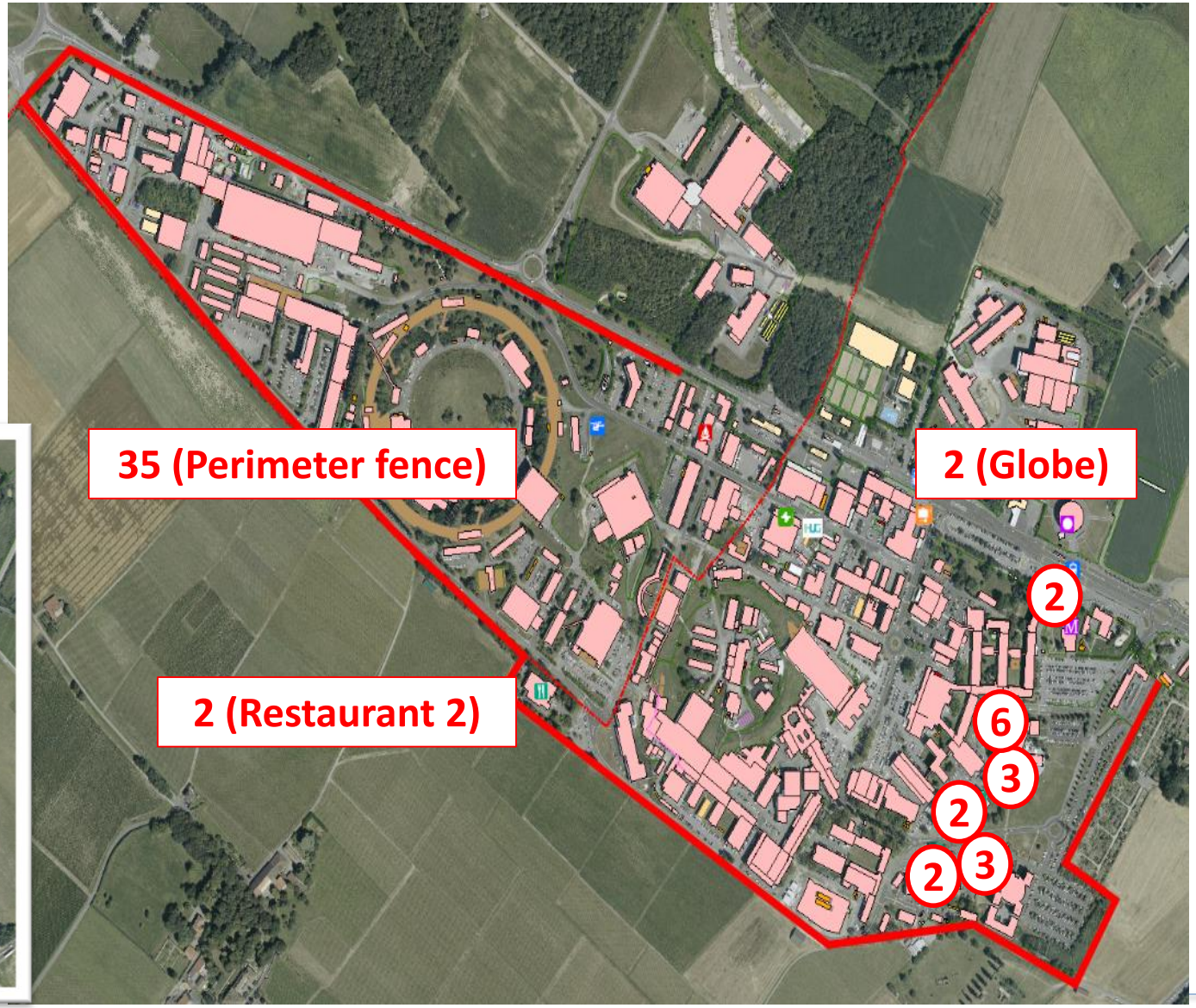
Total of cameras : 62





Specific surveillance

Total of cameras : 59



Video surveillance Principles

- Task: ***"Provide, through analysis of data (video footage, access control logs, vehicle locations, etc.) technical details in response to a request, while observing the <u>strictest confidentiality</u>",***
- Based on "Need to know principle". "Black screen" approach, no continuous watch.
- CCTV retention period maximum 1 year
- Since last year there is a dedicated part time staff position for video analysis
- Video workstation and software – Access only granted to Video Data Analyst

Video Extraction – How it works?

Home > Functions by Unit: SMB-DI > Video surveillance and access logs

CERN Service Portal
easy access to services at CERN

Home News Service Information Navigate Catalogue Contacts About

Also in SMB-DI:

- Contractors' personnel and Biometrics Registration
- CSA Actions
- CSA Control Room
- CSA Evt exceptionnels
- CSA Manager
- CSA Parking
- CSA Patrouilleurs
- CSA Reception 33
- CSA Service
- CSA Statiques

Show more

Go to functions by unit page

Supported Services

Important for:

Guards Service

Video surveillance and access logs (SMB-DI)

Extraction, video, access log, accès, accident, theft, degradation, vol, vols, agression, incivility, incivilité

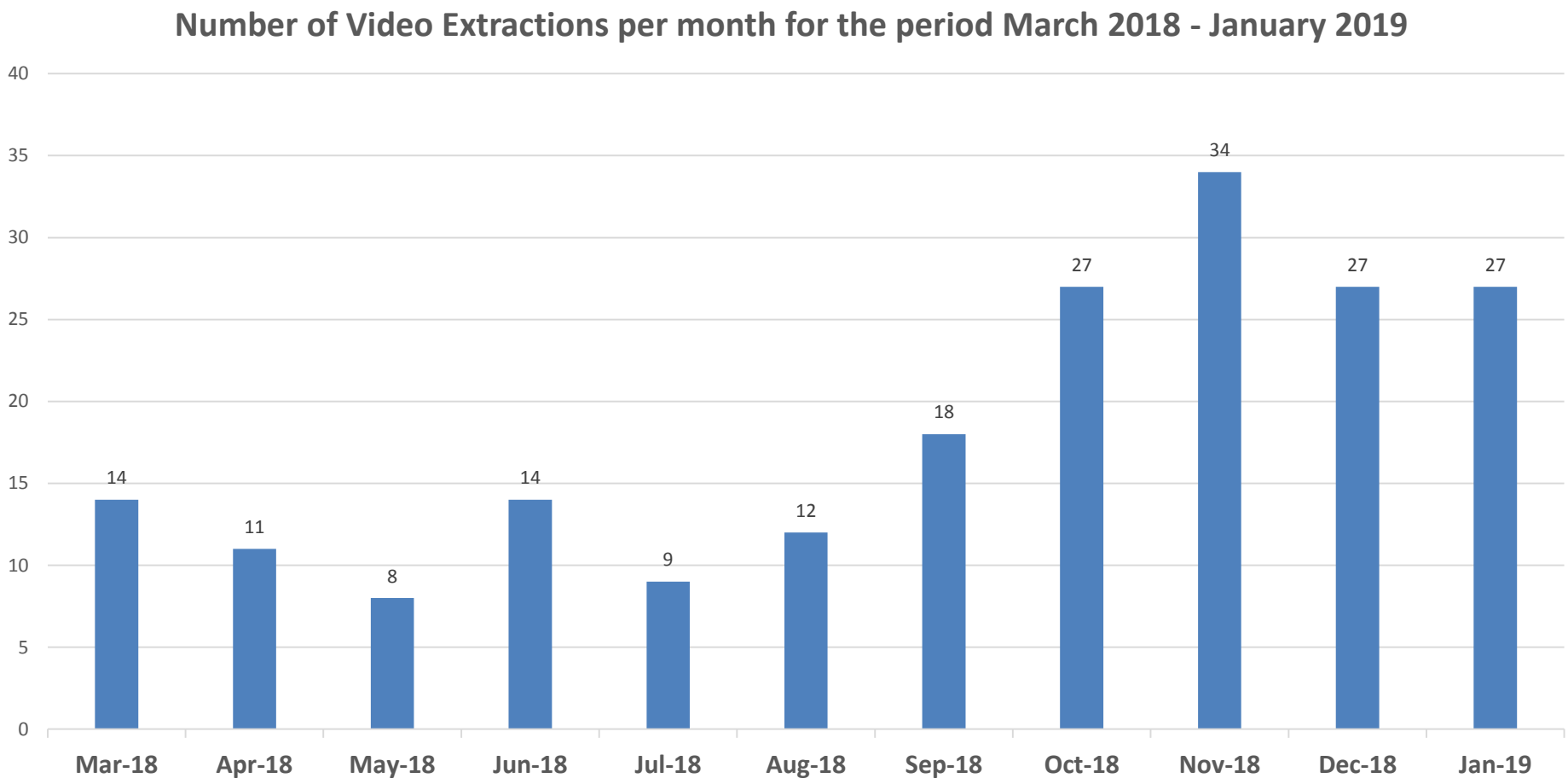
Actions

Report issue	Report an incident
Request	Submit a request
Request	Video surveillance / access logs extraction request

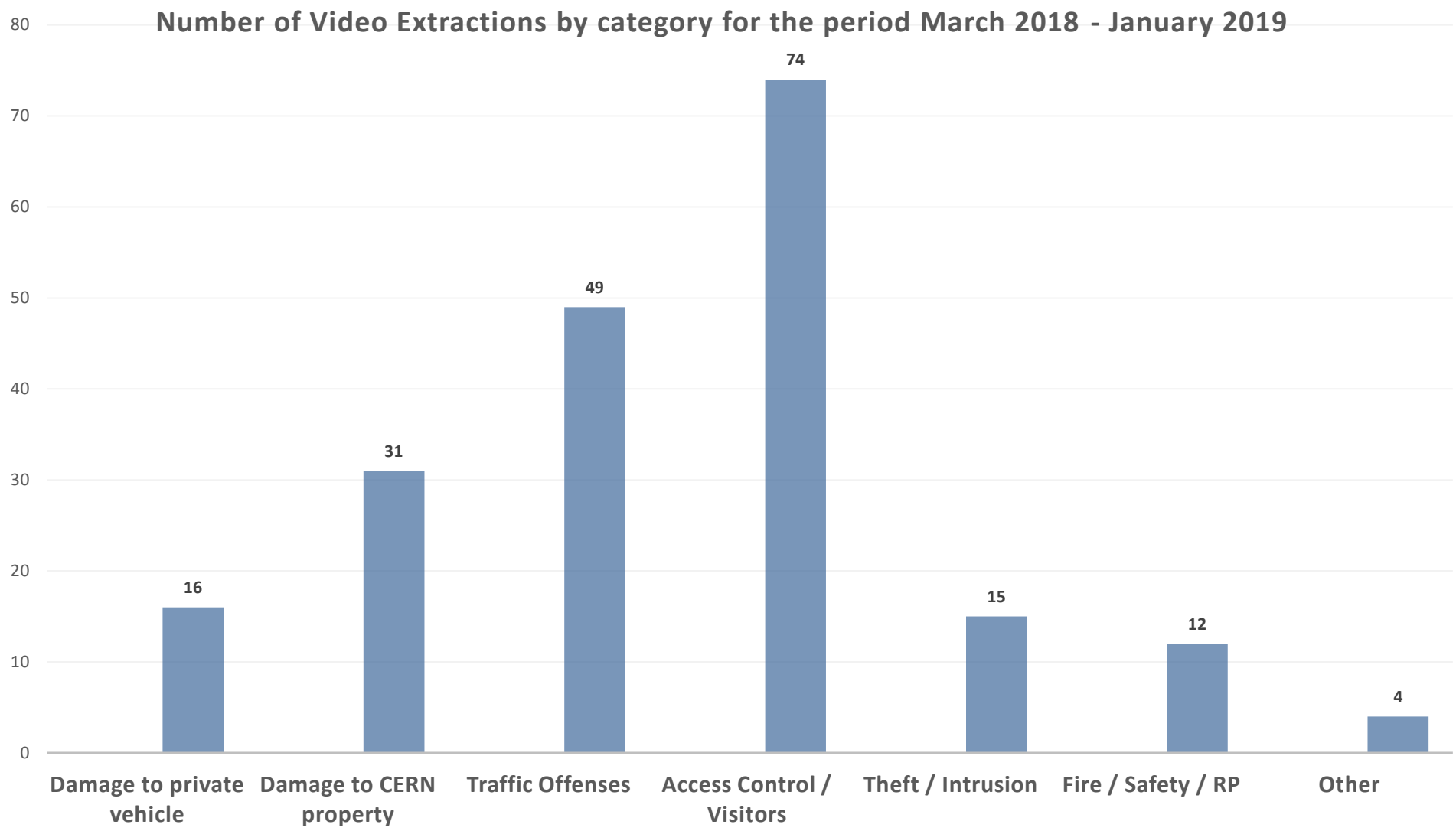
*Cannot find what you need here? Do you simply need advice or assistance? The **Service Desk** is here to help.*
*Call the Service Desk on: **77777** (07:30 - 18:30 work days, Geneva time)*

Contact Service Desk SMoD Site Guide

Video Extraction Statistics

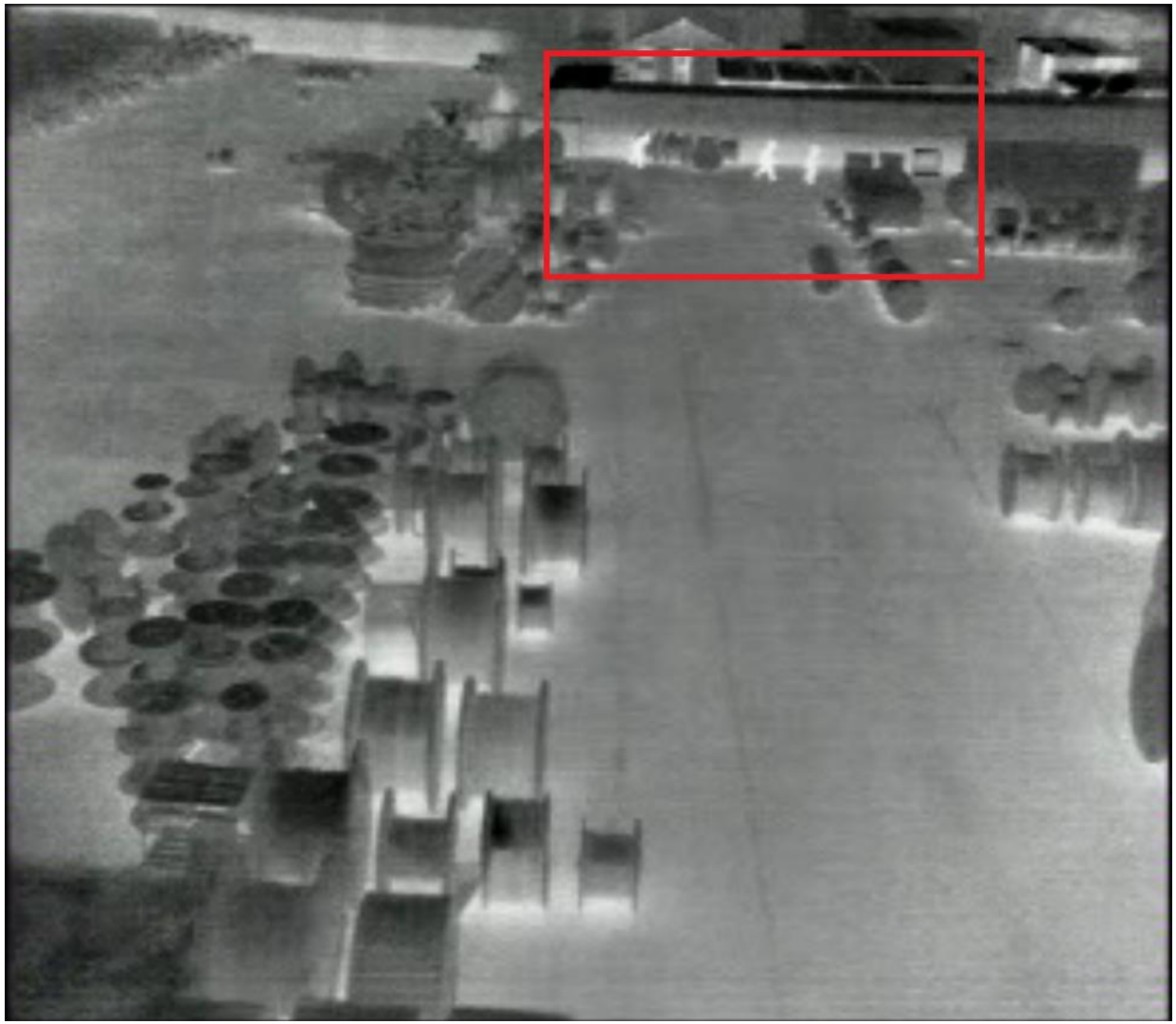


Video Extraction Statistics

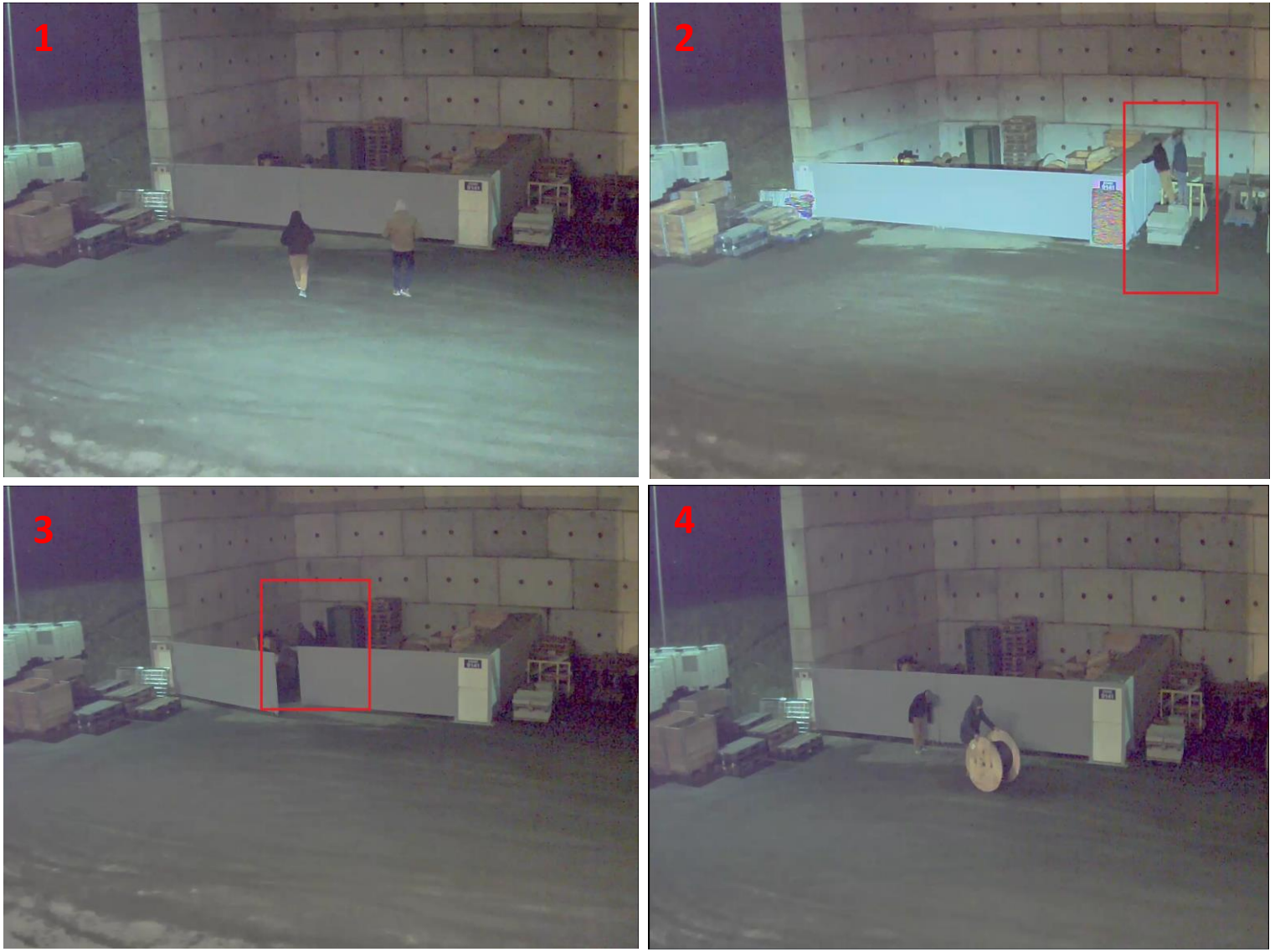


Some examples

Intrusion Zone Tourets Prevessin 13 January 2018

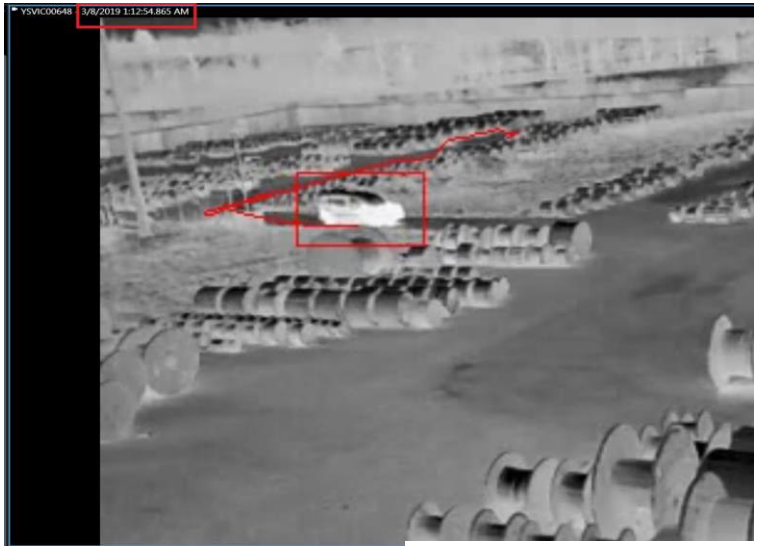


Intrusion / Theft at BA4 8 February 2018

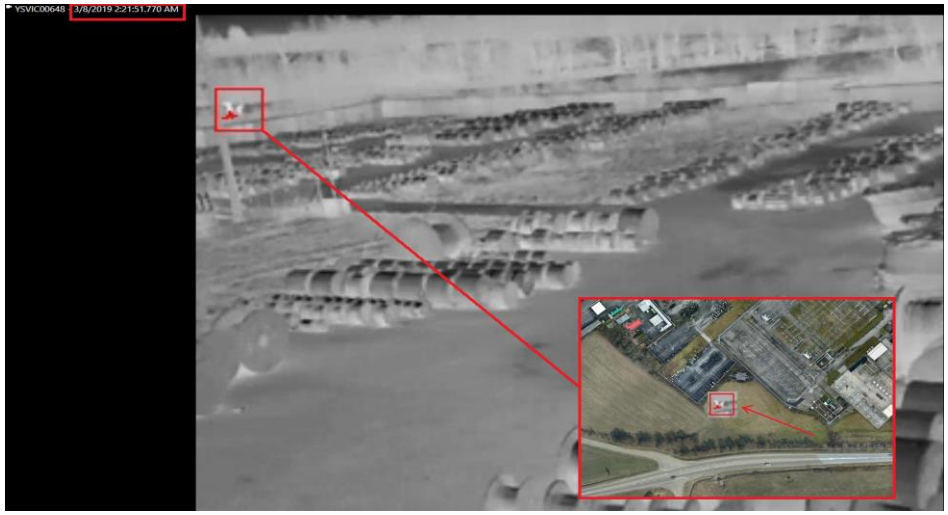


Zone Tourets Prevessin on 8 March 2019

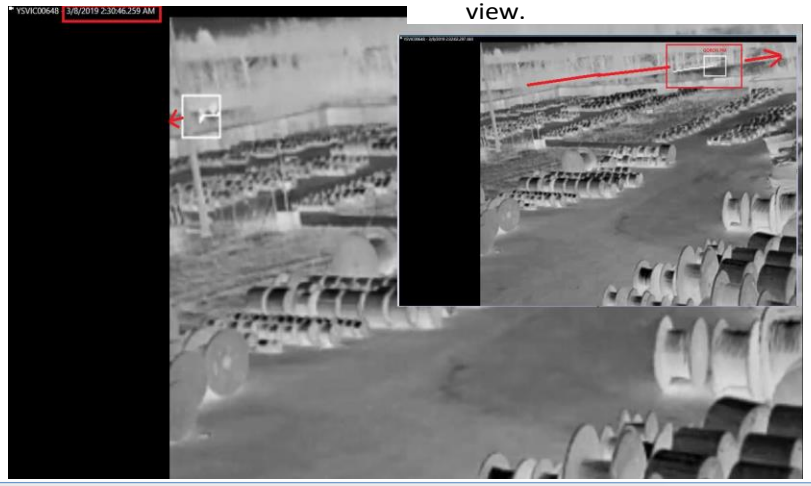
1. At 01:12 a.m. on 08 March 2019, GORON PM is patrolling inside Zone Tourests.



2. At 02:21 a.m. on 08 March 2019, Thermal Camera YSVIC-000648 is detecting the 2 x individuals, who are outside CERN Fence, and initiates an Alarm on Milestone.

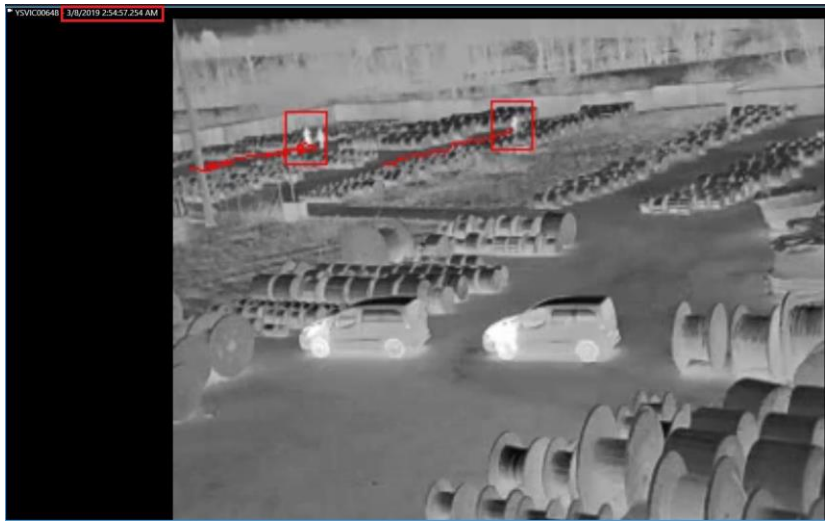


3. At 02:30 a.m., just 2 minutes before the GORON PM Vehicle arrives and heads on the Decheteri road (02:32 a.m.) , the 2 x individuals are leaving the area, going out of the thermal camera`s view.

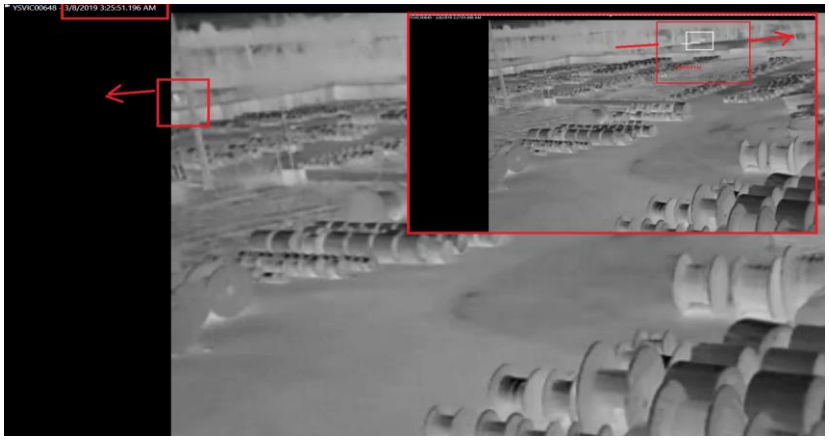


Zone Tourets Prevessin on 8 March 2019

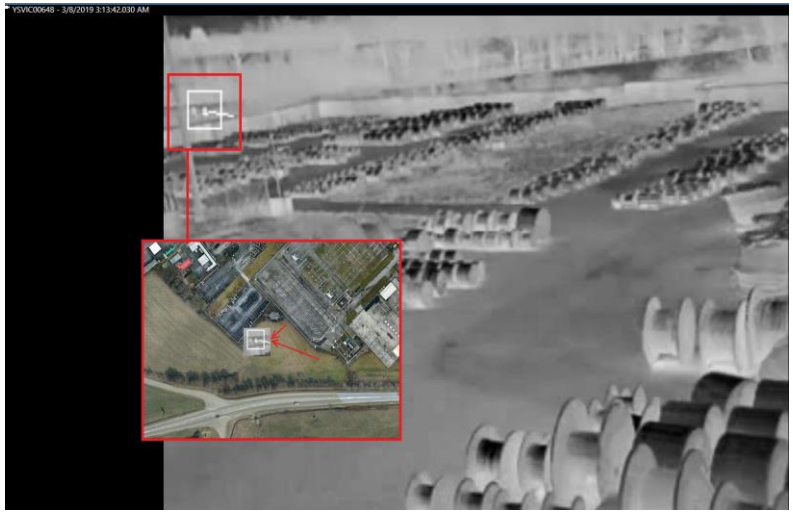
5. At 02:54, GORON PMs are patrolling inside Zone Tourests.



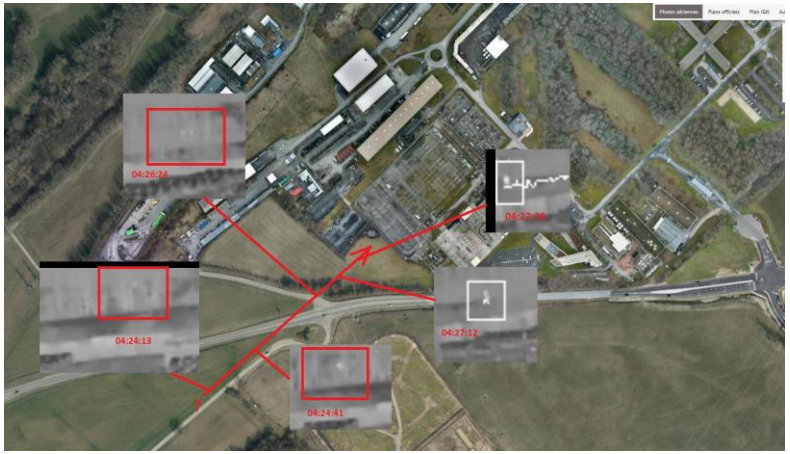
7. At 03:25 a.m., again just 2 minutes before GORON PM Vehicle arrives (03:27 a.m.), the 2 x individuals are leaving the area, back to the direction from where they came.



6. At 03:13 a.m., the 2 x unknown individuals are again detected by the thermal camera, coming from the same direction (please see map and Video 2)

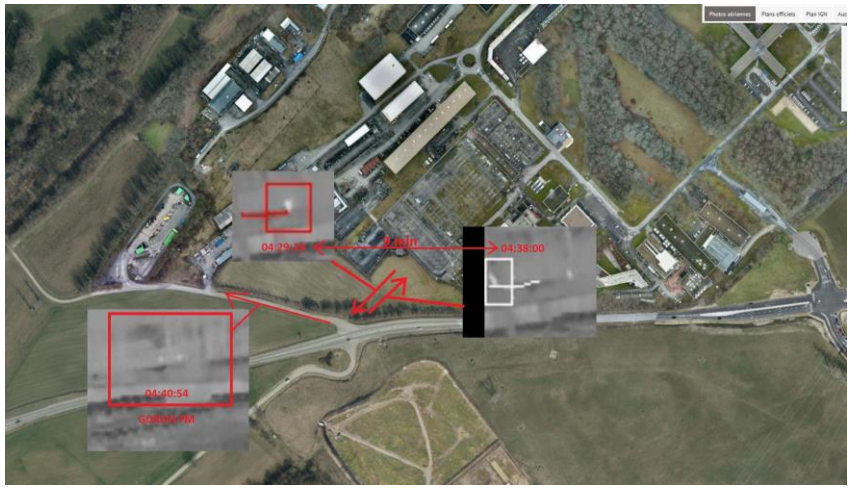


10. Between 04:24 to 04:38 – the heat signatures of the 2 x individuals are detected, outside of the CERN`fence, moving back and forward during this time. The Alarm on Milestone initiates at 04:29 a.m.

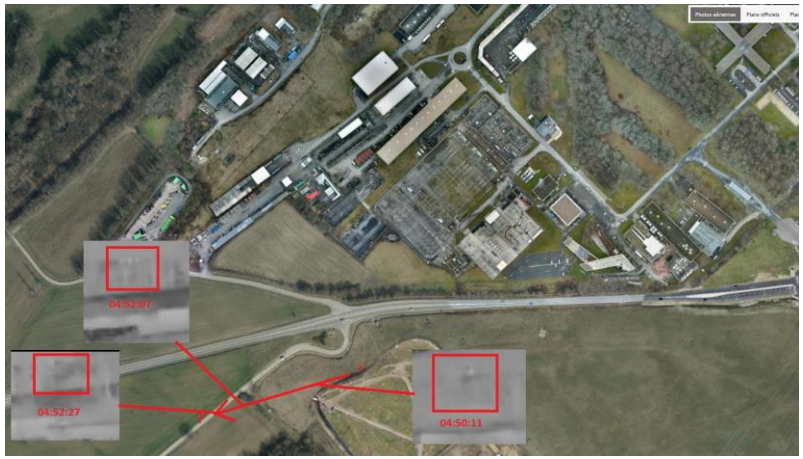


Zone Tourets Prevessin on 8 March 2019

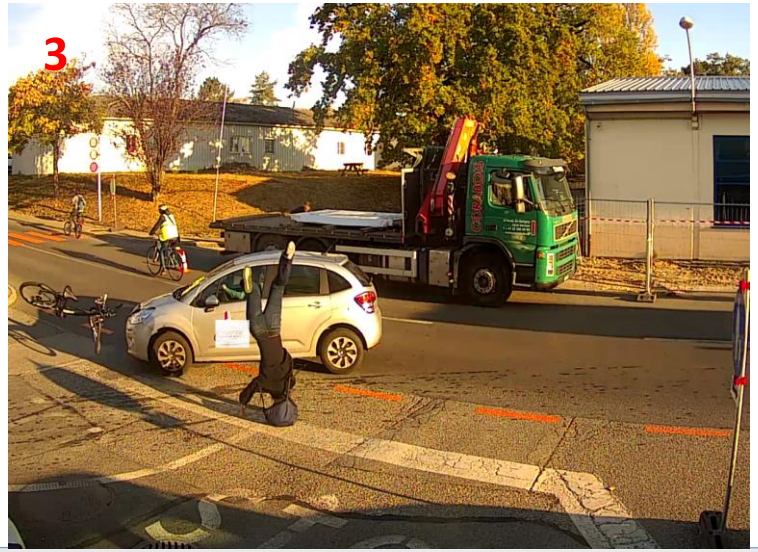
11. At 04:38 a.m. the 2 x individuals are running away, in opposite direction from where they have come. At 04:40 a.m., GORON PMs arrives on the decheterie road.

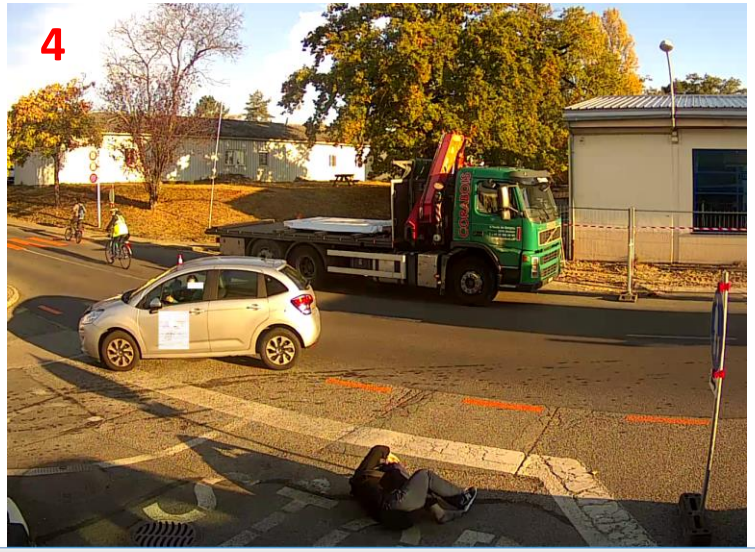


12. At 04:50 a.m. the heat signatures of the 2 x individuals are detected by the thermal camera. They are on the other side of the Saint Genis to Ferney road, heading back to direction of BA2 road / Camp Gens de Voyage.



Traffic Accident Gas Station 15 October 2018





Guards

- Resources
  - Access control (15 guards)
  - Patrol (7 guards),
- Main tasks :
  - Alarm intervention (5 000 events/year)
  - Safety signalisation (1 000 events/year)
  - Parking management (1 500 events/year)
  - VIP visits (200 events/year)

GUARDS

- **Access control**
- **Traffic regulation**
- **Alarm intervention**

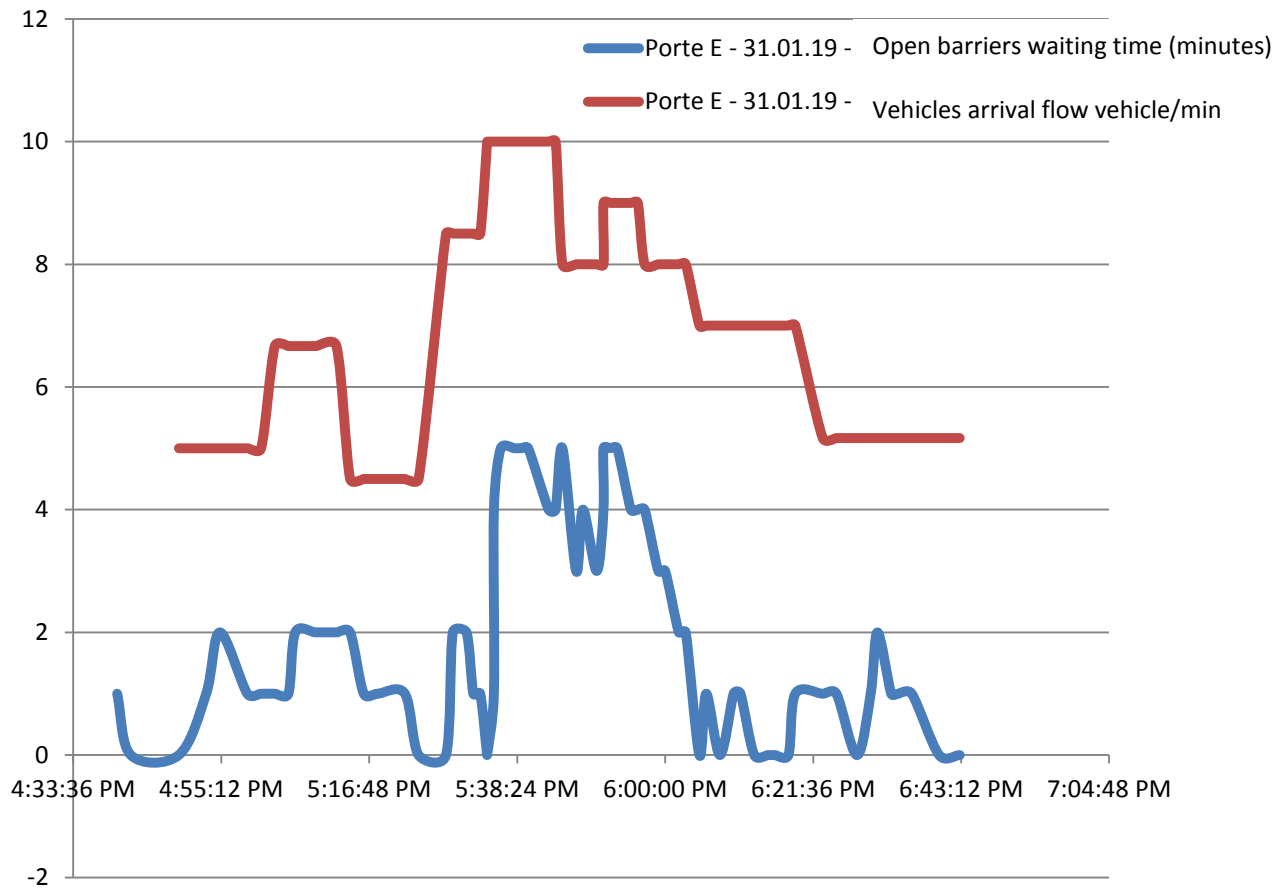
GUARDS

Mobility

- Traffic
- Road signalling
- …

Security

- Access control
- Patrol
- …



CONCLUSIONS

- CERN's security strategy is based on a realistic framework and a sound legal basis
- However, to protect the complexity of the CERN sites is a big challenge
- The strong collaboration with the Host States authorities is a key ingredient into this framework
- Whilst personal perception plays a significant role on such a delicate matter, your understanding and support is key to achieve CERN's security objectives
- A safe and secure workplace for all persons on the CERN sites is in our highest interest

THANK YOU VERY MUCH FOR YOUR ATTENTION

Security events. Crisis management

- Security events added to the Crisis Management framework
  - in the event of an increase in the level of threat by Host States
  - in the event of a site incident
- Tools and procedures have been developed to support crisis management events. GIS support, site evacuation plan.

Security events. Resilience

- In order to increase resilience after security event
  - new control room
  - preserved the old room as back-up
  - introduced provisions in the guards contract in order to be able to quickly increase the number of resources (x2)
  - Communication equipment. 4G + wifi and tetra radios

Theft statistics

Count of Task	Column Labels							
Row Labels	2013	2014	2015	2016	2017	2018	2019	Grand Total
Vélo CERN / CERN bike	51	19	18	21	38	43	4	194
CERN Carte d'accès / CERN access cards	1	8	24	21	23	14	7	98
Matériel informatique (ordinateurs et périphériques) and Hardware	15	30	18	7	15	8		93
Téléphone portable	1	8	7	11	6	8		41
Câbles, cuivre, métaux divers / Cables, copper, various metals	12	11	3	5	6	2	1	40
Autre / Other	9	5	6	4	1	6		31
Matériel, outil / Equipment, tool	4	5	7	3	5	4	1	29
Clés CERN / CERN keys		2	3	2	8	8	2	25
Affaires personnelles (sac, argent, portefeuille...) / Personal Belongings		4	2	3	3	5		17
Legitimation documents: Swiss and French cards / Documents de légitimation		1	4		1	3		9
Official vehicles (belonging to or rented by CERN) / Véhicules officiels			4	2		2		8
Matériel hightech (projecteur, écran plasma, appareil photo/ High-tech equipment	1	1	1	1		1		5
Dosimètre CERN / CERN dosimeter				1		1		2
Grand Total	**94**	**94**	**97**	**81**	**106**	**105**	**15**	**592**

Sum of Estimated value (CHF)	Column Labels							
Row Labels	2013	2014	2015	2016	2017	2018	2019	Grand Total
Câbles, cuivre, métaux divers / Cables, copper, various metals	49,697	61,573	24,367	129,695	53,280	4,400	35,878	358,890
Matériel informatique (ordinateurs et périphériques) and Hardware	63,610	41,706	124,247	8,246	23,733	9,707		271,248
Vélo CERN / CERN bike	21,904	5,779	4,929	6,244	7,011	17,200	1,600	64,667
Matériel, outil / Equipment, tool	4,104	3,215	23,715	813	5,117	9,690	462	47,117
Autre / Other	9,176	3,760	2,285	8,120	399	3,625		27,365
Matériel hightech (projecteur, écran plasma, appareil photo/ High-tech equipment	5,781	4,000	203	10,406		348		20,738
Téléphone portable	800	2,939	3,419	7,856	2,243	3,229		20,487
Affaires personnelles (sac, argent, portefeuille...) / Personal Belongings		3,040	2,067	1,894	2,165	2,400		11,566
Official vehicles (belonging to or rented by CERN) / Véhicules officiels			1,466	20		739		2,225
CERN Carte d'accès / CERN access cards	5	40	120	105	107	417	35	829
Dosimètre CERN / CERN dosimeter				350		350		700
Clés CERN / CERN keys		20	30	20	86	410	20	586
Legitimation documents: Swiss and French cards / Documents de légitimation		10	40		10	360		420
Grand Total	**155,077**	**126,081**	**186,889**	**173,769**	**94,150**	**52,876**	**37,995**	**826,838**

OC2 enforcing

- Art 18 : all persons present on the site shall submit to the checks carried out by the site guards in pursuance of the tasks entrusted to them by the Director-General
- Art 18.1 : General check
  - The task of the site guards is to check, throughout the site, the identities of persons and vehicles, their access permits and the goods they are transporting. To this end, they are authorised to:
    - a) request the presentation of an identity document, a CERN card, ….
    - b) inspect a vehicle,…;
    - c) seize goods likely belonging to the Organization that are being transported without the appropriate accompanying documentation…;
    - d) stop a vehicle for as long as required to carry out the necessary checks;
    - e) refuse access to persons or vehicles not complying with the Circular. Persons entering or leaving the site must facilitate the smooth completion of these checks.