



# INNOVATIVE SOLUTIONS FOR SECURITY



## Protection for Industrial Control Systems



United States Patent claim № US 13458662

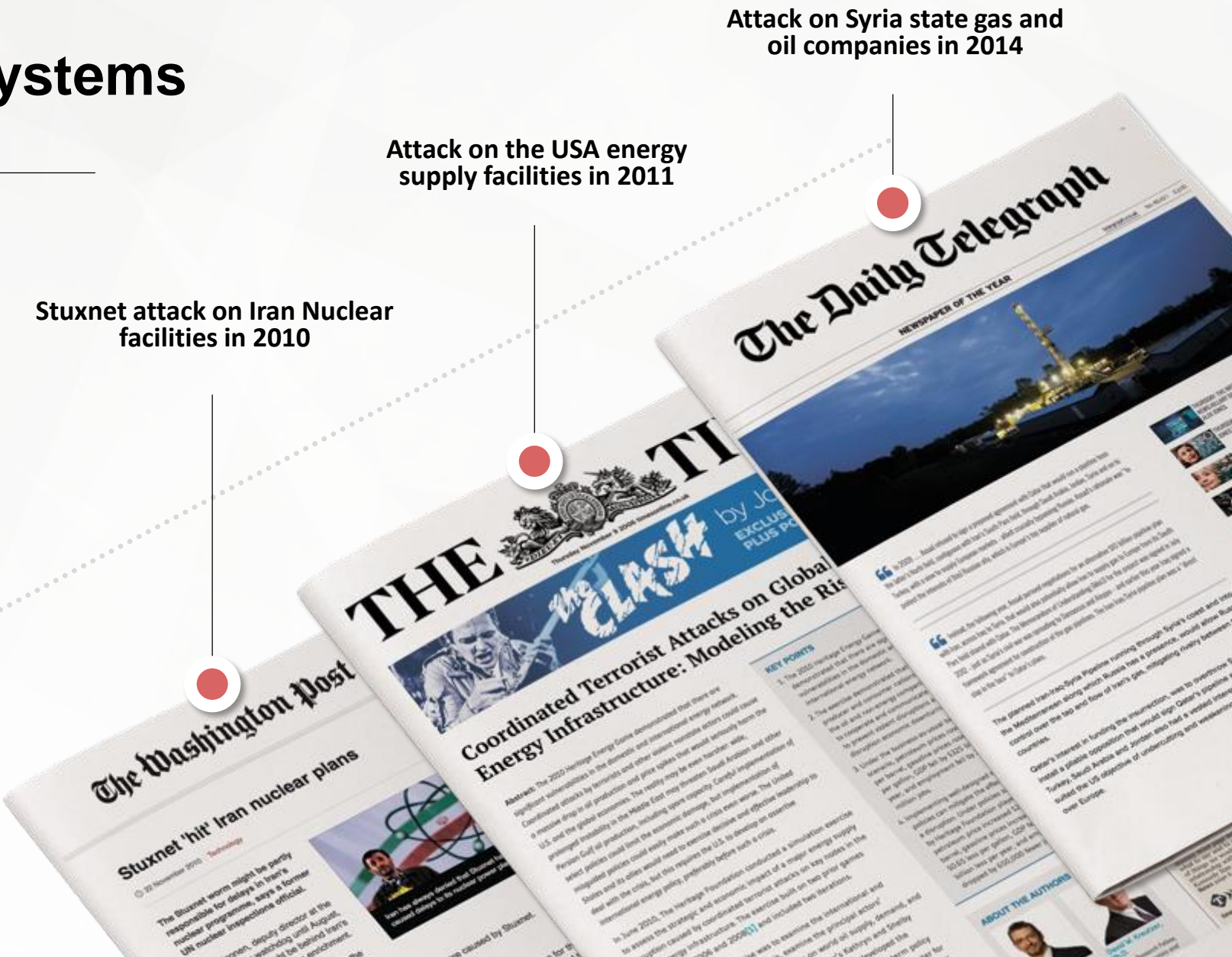
METHOD AND SYSTEM FOR PROTECTION OF AUTOMATED  
CONTROL SYSTEMS FOR SMART BUILDINGS

## Importance of industrial control systems protection

### Consequences of the attacks on the industrial control systems

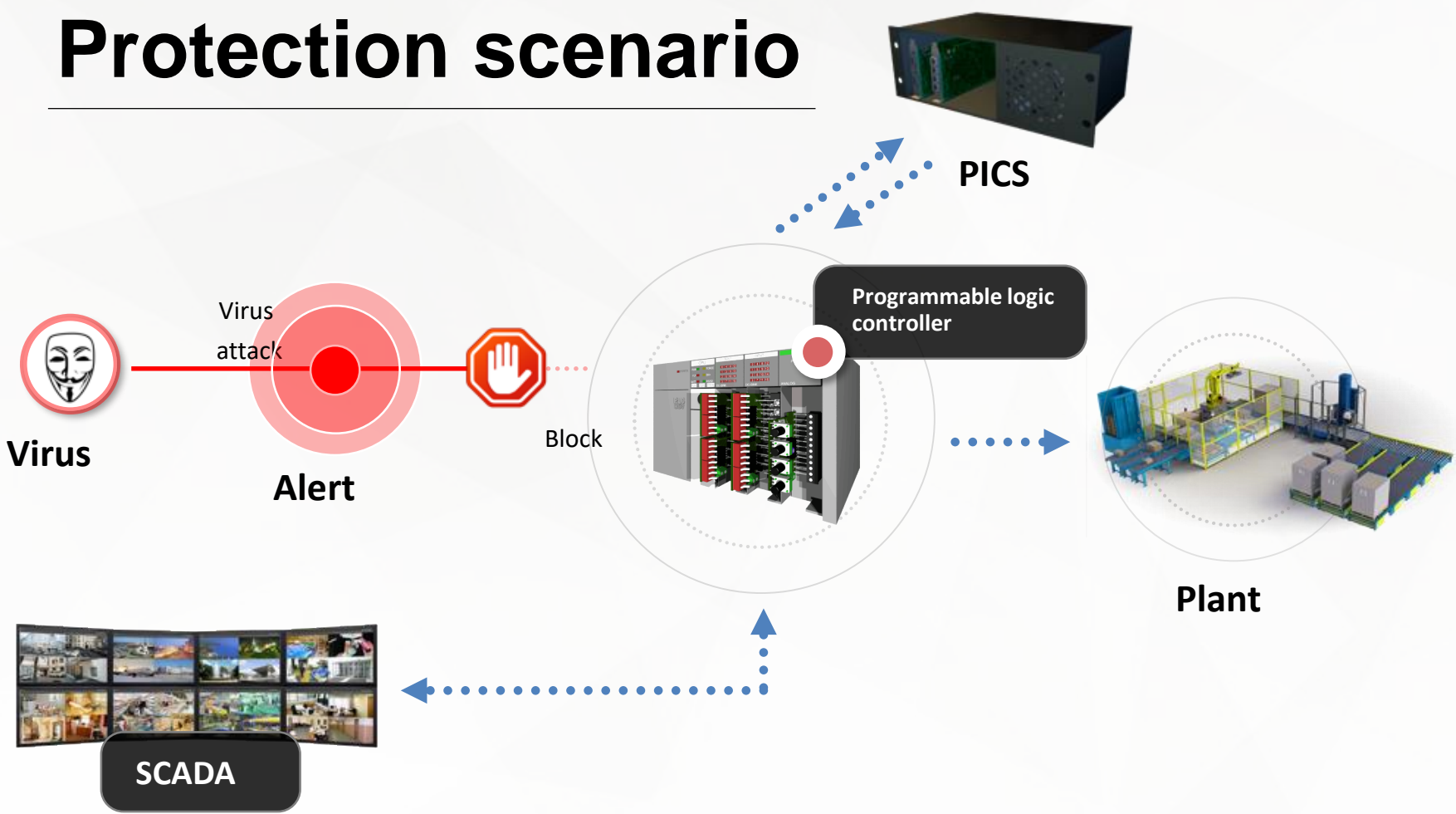
- ❖ Infringement of working capacity of the key systems at the enterprise
- ❖ Technological disasters
- ❖ Data leakage

### Known Worldwide attacks on the industrial control systems



## OUR SOLUTION

### Protection scenario



**PICS** is the unique patented hardware/software solution and the first **Intrusion Prevention System (IPS)** for industrial process control systems, which detects, prevents or blocks malware in information infrastructure systems of automatic control for various production and technological processes:

-  **Highest level**  
SCADA, MES
-  **Middle level**  
PLC, HMI
-  **Field level**  
Sensors, Devices

# PROTECTION FOR INDUSTRIAL CONTROL SYSTEMS

ГОТОВЫЙ  
БИЗНЕС



## APPLICATION



Fire-protection system



Perimeter defense

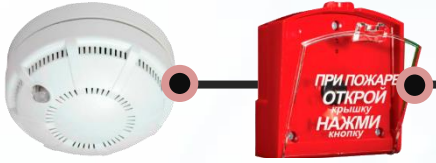


Security systems



CCTV

### Fire-protection system



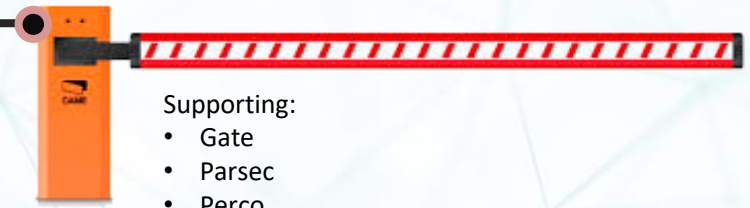
- Supporting:
- System sensor
  - Argus-Spectr
  - Arsenal bezopasnosti
  - Arton
  - VERS etc.

### CCTV system



- Supporting:
- CheckTV
  - Line
  - Bolid
  - BiteERG etc.

### Barriers



- Supporting:
- Gate
  - Parsec
  - Perco
  - Bolid etc

### ACS and turnstiles



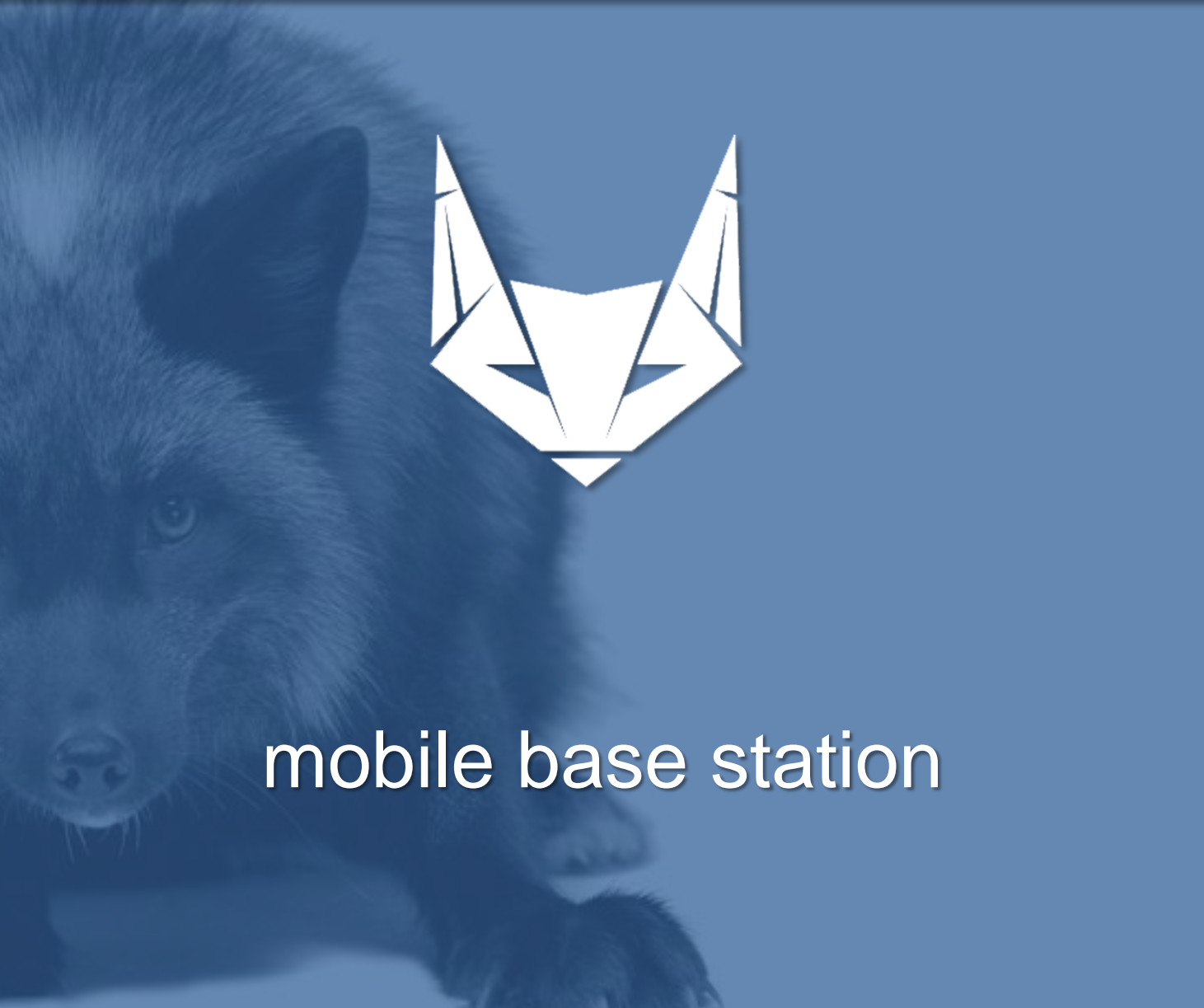
- Supporting:
- Aler
  - IronLogic
  - Promix
  - Elix etc



### **CYBERPHYSICAL PROTECTION SYSTEM**

Information log for object's cybersecurity





mobile base station

## Implementation Methods



**Industrial case**



**Office case**



**Mobile case**

## Mobile base station Black Fox

**Black Fox** – a virtual mobile base station that allows to build a local GSM-network with the following functionality:

- ★ Real time mobile phones tracking in the local area (IMSI, IMEI, activity).
- ★ Local calls and local text messages to phones in the area.
- ★ Local calls between phones in the area without bounding to real mobile operators.
- ★ Selective mobile phones blocking in the area according to white list/black list policy.



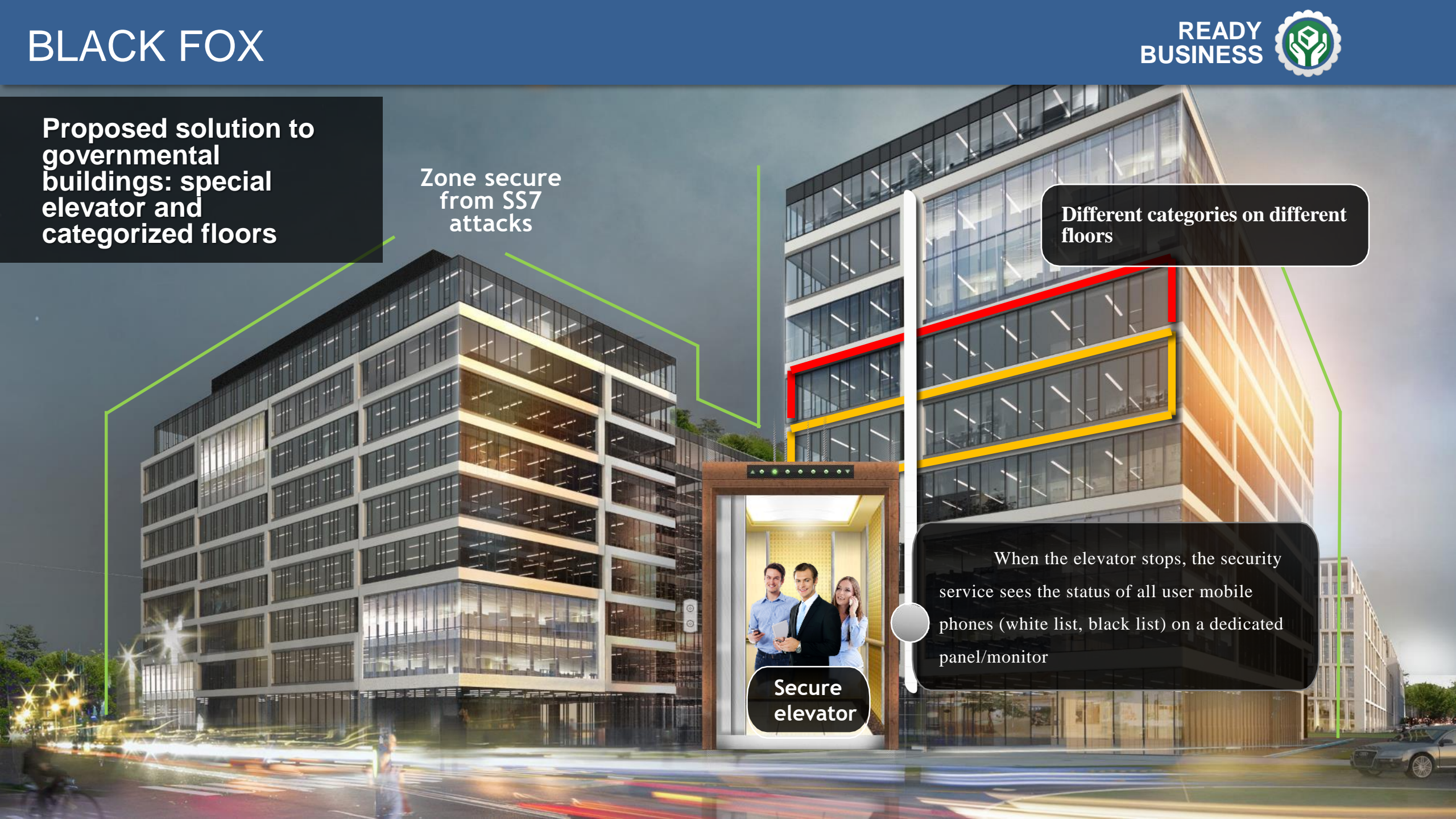
Proposed solution to governmental buildings: special elevator and categorized floors

Zone secure from SS7 attacks

Different categories on different floors

When the elevator stops, the security service sees the status of all user mobile phones (white list, black list) on a dedicated panel/monitor

Secure elevator



## ANTI-TERRORIST SECURITY

Criminal  
is detected

 JOHN  
TRAVOLTA

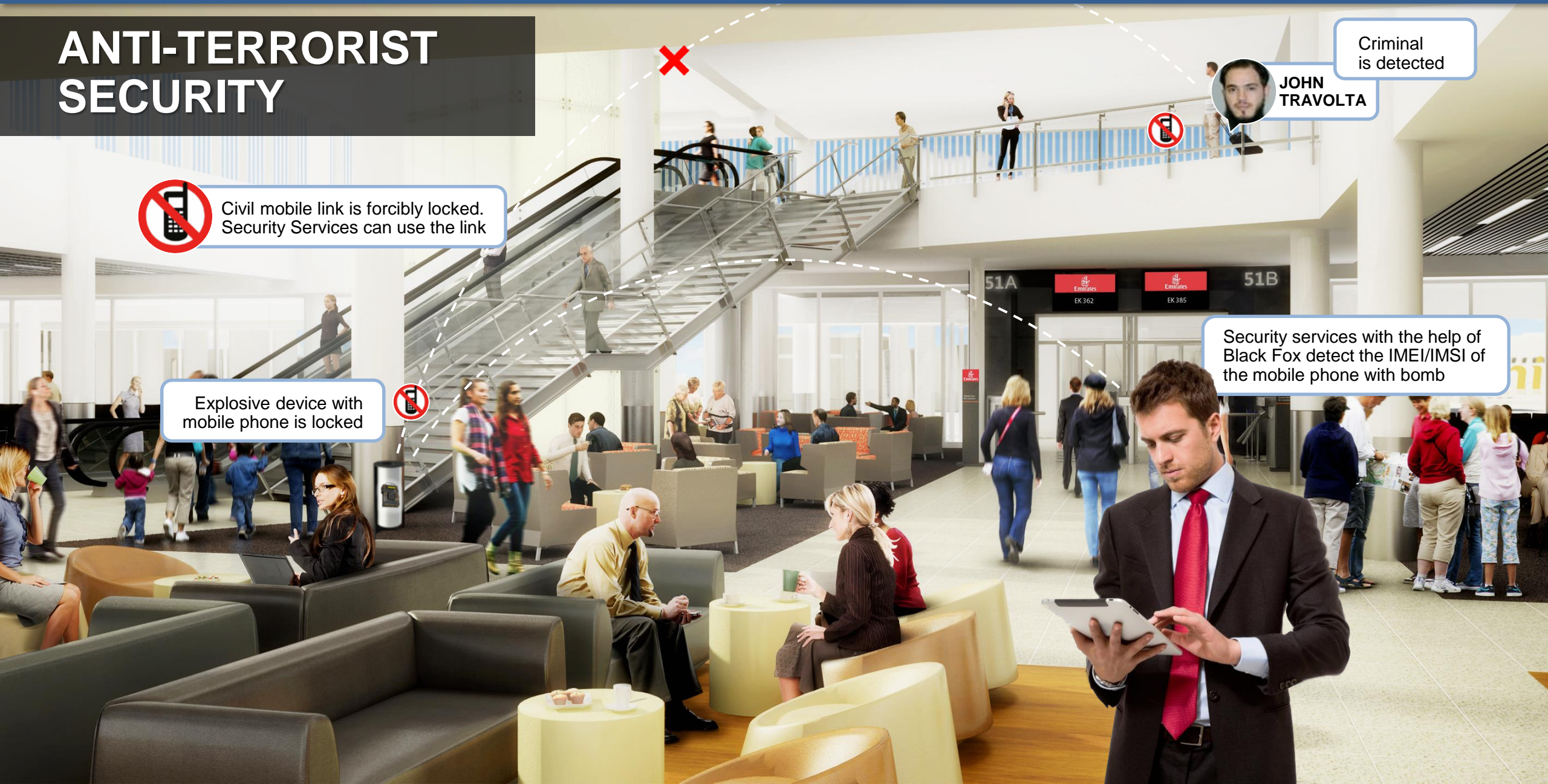


Civil mobile link is forcibly locked.  
Security Services can use the link

Explosive device with  
mobile phone is locked



Security services with the help of  
Black Fox detect the IMEI/MSI of  
the mobile phone with bomb



## EVACUATION SCENARIO

Send SMS with evacuation  
plan with the help of Black Fox

Mobile complex  
is fixed up in the  
vehicle



Fire in the building,  
people are trapped inside



## ESTABLISHING COMMUNICATION LINK IN DISASTER AREA



Mobile Black Fox unit  
establishes local cell link  
when GSM link is  
unavailable



Able to call people with cell  
phones in the area of action



# AutoVisor

A new generation of car protection against  
cyber threats



United States Patent № US 8955130

METHOD FOR PROTECTING VEHICLE DATA  
TRANSMISSION SYSTEM FROM INTRUSIONS

## HOW CAN YOUR VEHICLE BE ATTACKED?

Methods of malware penetration in your car's system are similar to those that are used for normal computers.



Wireless  
connection



Troubleshooting  
systems




External data  
carriers



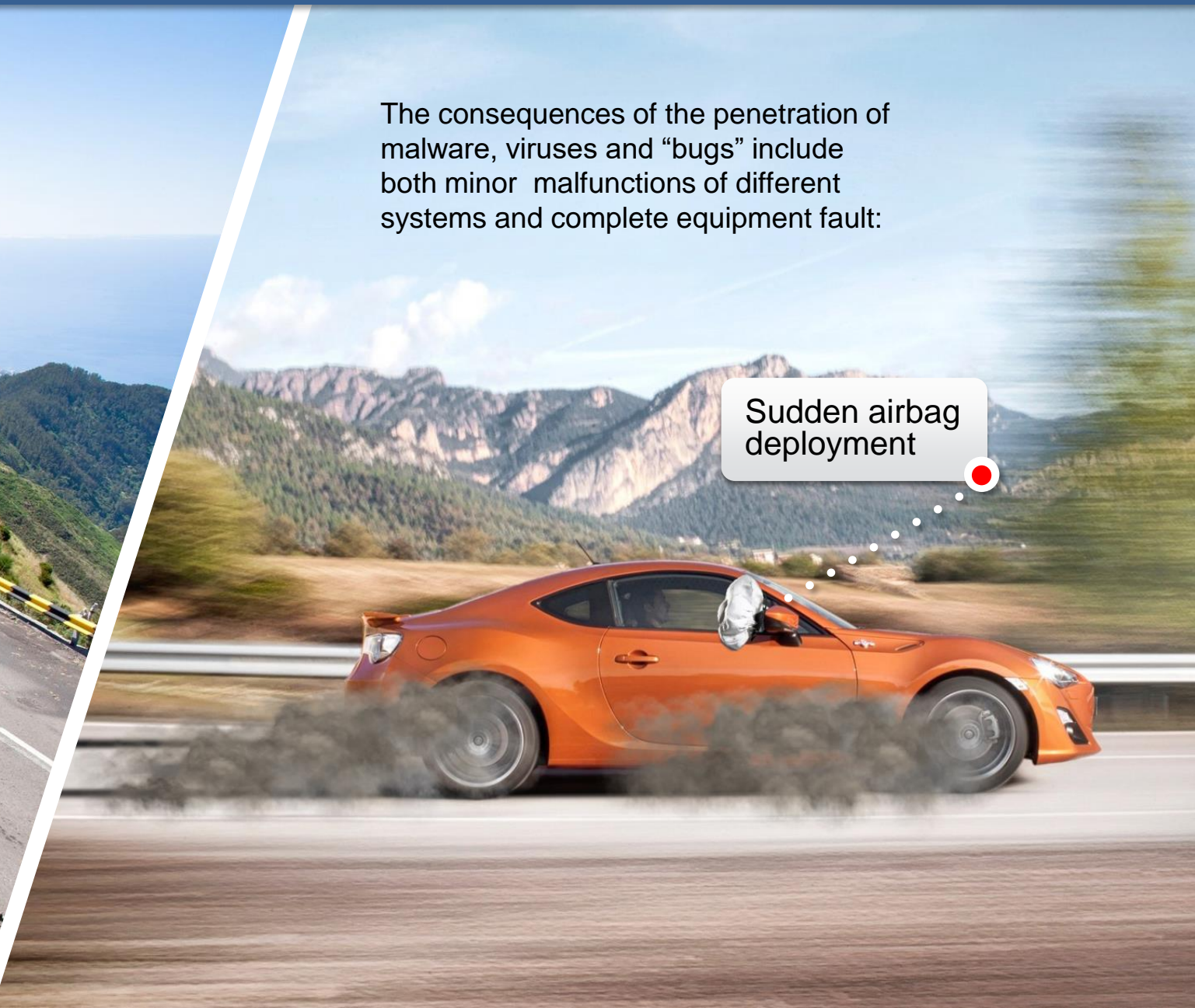
Exposure during  
service  
maintenance

## AFTERMATH



Wheel lockup

The consequences of the penetration of malware, viruses and “bugs” include both minor malfunctions of different systems and complete equipment fault:



Sudden airbag deployment

# AFTERMATH

Disabling  
headlights at  
night



Disabling the  
brake system





AutoVisor provides maximum protection from unexpected consequences of attacks on the vehicle's CAN-bus

AutoVisor is the only tool that enables the car owner to control the parameters of the vehicle operation independently. It also provides automatic blocking of threats.

**01** Has no analogues in the world

---

**02** Installation takes less than 2 hours at the service center

---

**03** All information about the protection system's operation is available in a mobile application (iOS, Android)





## Green Head

Protection of mobile devices from  
unauthorized wiretapping



United States Patent № US 8387141  
United States Patent № US 8732827  
SMARTPHONE SECURITY SYSTEM

## CURRENT PROBLEMS

Relevant threats for mobile devices and users



Unauthorized wiretapping of talks via cell phone



Unauthorized activation of microphone and camera of a device, data transmission to attackers



Access of unauthorized people to files containing business data



Locating a person by his mobile device



## OUR SOLUTION

Software for protection against wiretapping GREEN HEAD



Protection against wiretapping



Protection against data leakage

## Features



Detection of unauthorized activation of a mobile device's camera and microphone



The widget blocks the camera and microphone in one click and disables wireless communication: Wi-Fi, BT, NFC, mobile Internet, which can become data leakage channels



This application allows you to record a conversation in online mode for later playback



Widget on the screen of the mobile device notifies the user of unauthorized wiretapping.

For Android OS



## ADVANTAGES

HIGH  
SPEED



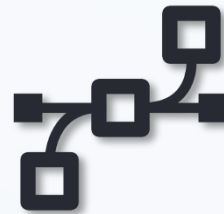
Green Head does not affect the speed of operation of your smartphone

SIMPLE  
IN USE

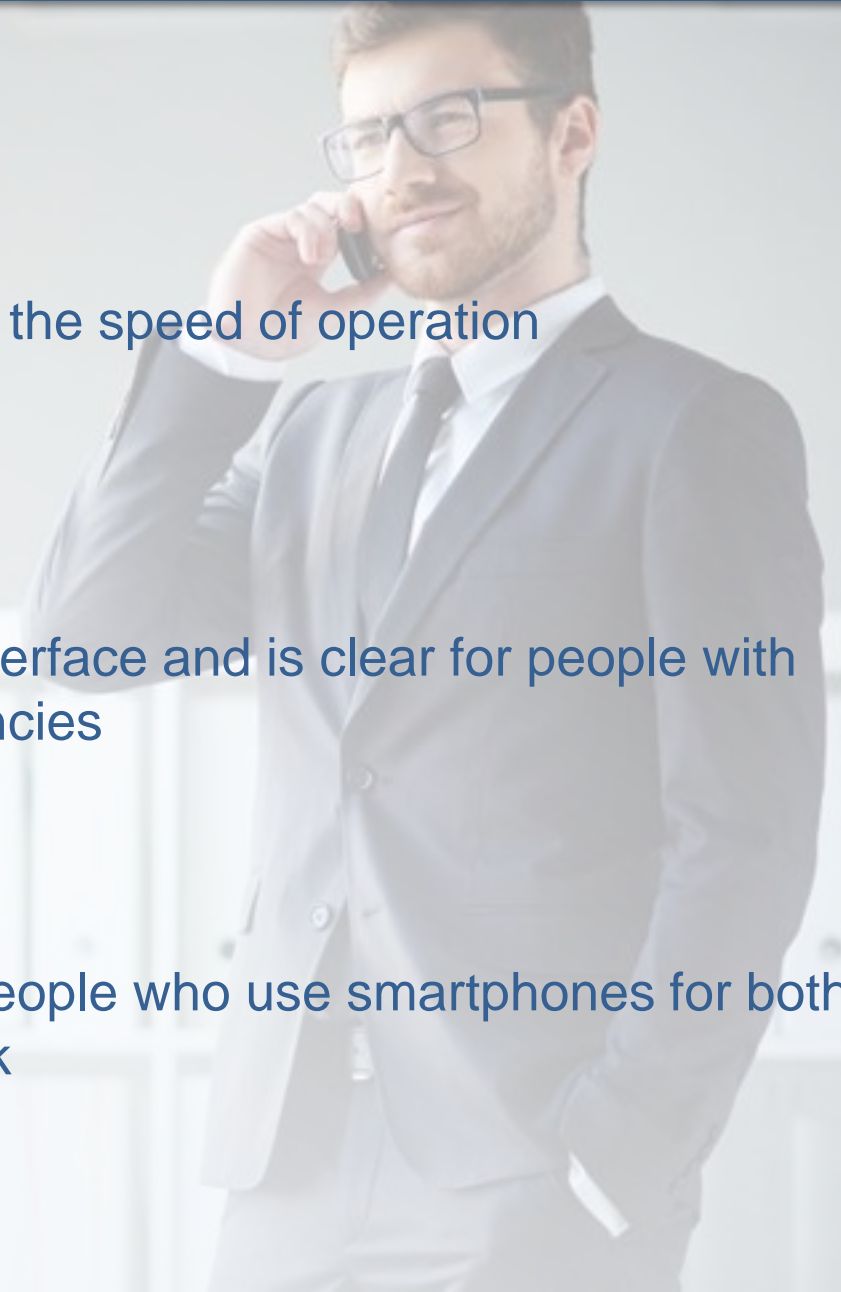


Green Head has intuitive interface and is clear for people with different technical competencies

MULTI-  
PURPOSE



Green Head is flexible for people who use smartphones for both personal purposes and work





# HONEYPOT

emulation of real industry or critical  
telecommunication infrastructure system  
on a server

# OPERATING PRINCIPLE

**HACKER**



**HONEYPOT**



**TARGET OBJECT**



HoneyPot simulates a target object. The hacker makes an attack, believing that he hit the target, and shows all his plans and tricks

# WHAT IS HONEYMOT?



## HONEYMOT

is the computer security mechanism set to **Detect**, **Deflect** and **Counteract** attempts at unauthorized use of information system.

### TYPES OF HONEYMOT

- Malware honeypots
- Spam versions
- Email trap
- Database honeypot

HoneyMOT consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually **isolated** and **monitored**, and that seems to contain information or a resource of value to attackers, who are then blocked





# WHY DO YOU NEED HONEYPOT?

**HoneyPot** is an emulation of real industry objects or core systems of a telecommunication structure on the server. Such server is connected to the Internet and attracts hackers as an easy target.



Attract hackers to the fake system



Monitor and control the attack



Analyze the methods of the attack



Defend the real system



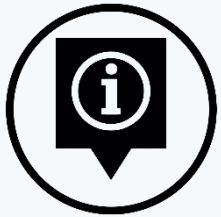
Avoid damage to the real system

# Photon

Digital Forensic Software

# PhotoN

is a software complex which allows to detect frauds of any level automatically and reliably.



## Metadata analysis.

Every image has hidden parameters (metadata) which are changed (deleted) after image is edited



## Deep digital analysis.

Assumes imposing different kinds of «filters» on the image which allows to identify the edited areas.



## PhotoN provides reliable fraud detection

PhotoN analyses the code of images instead of applying popular recognition algorithms.



## Fraud examples

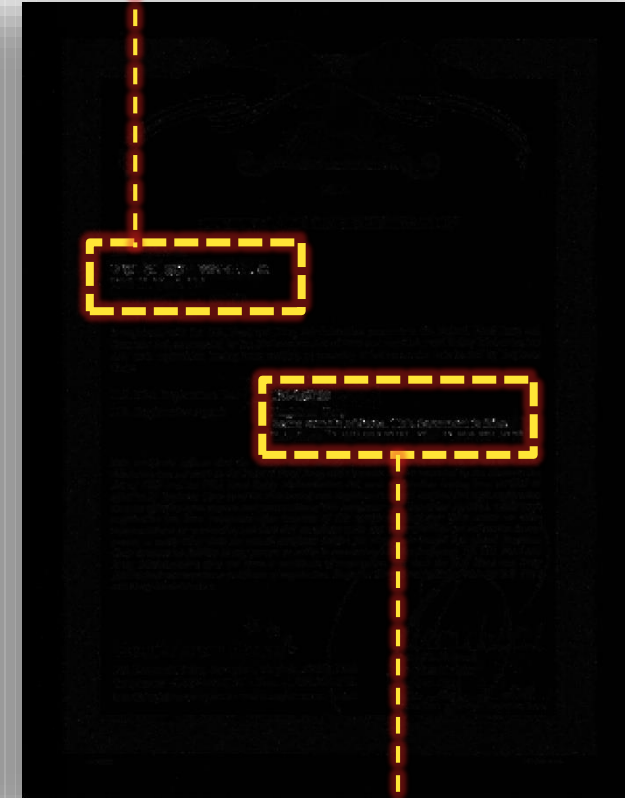
Fake passport photo

The result of digital analysis



Fake document scan

The result of digital analysis



# WOW!Mirror

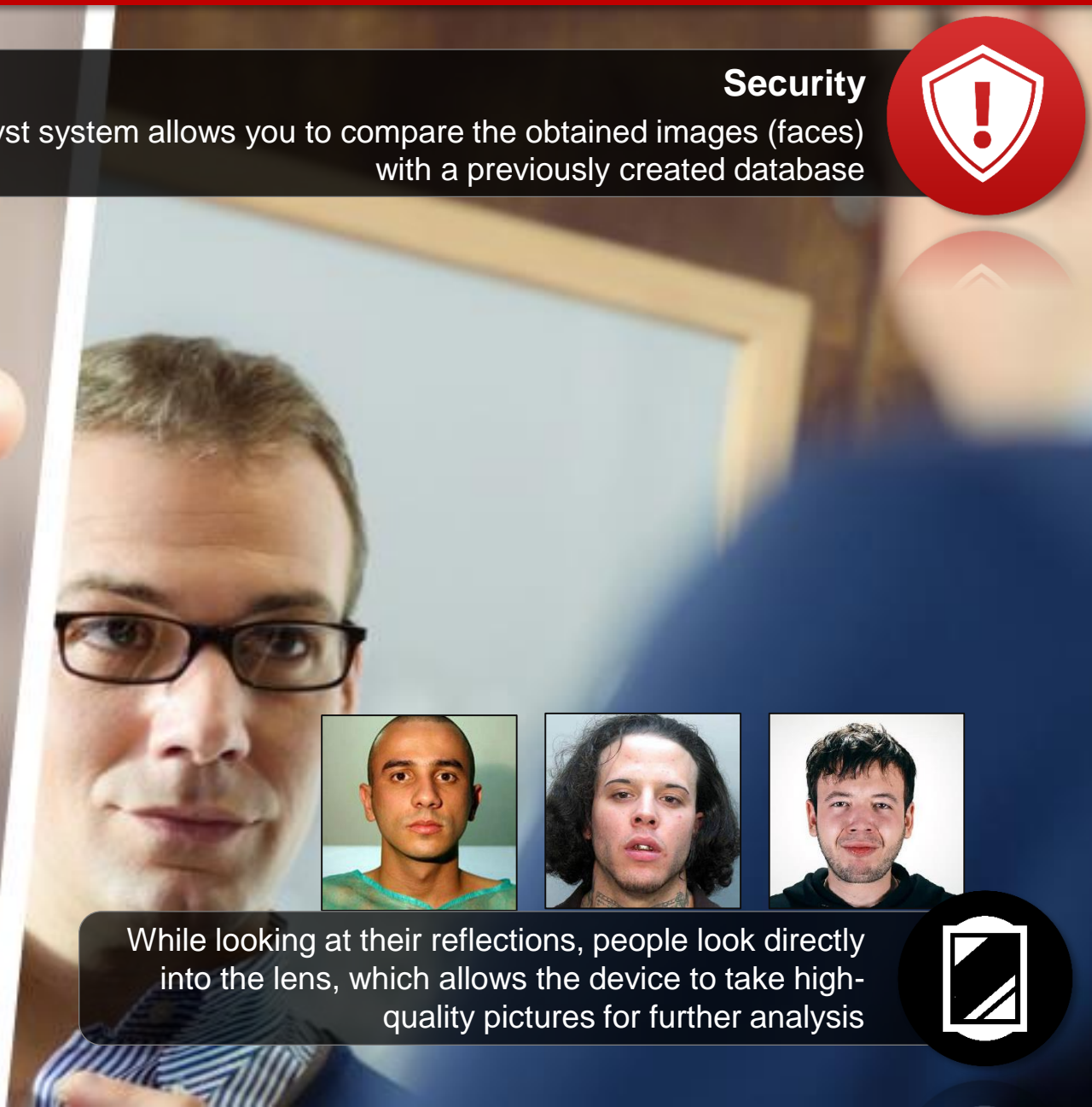
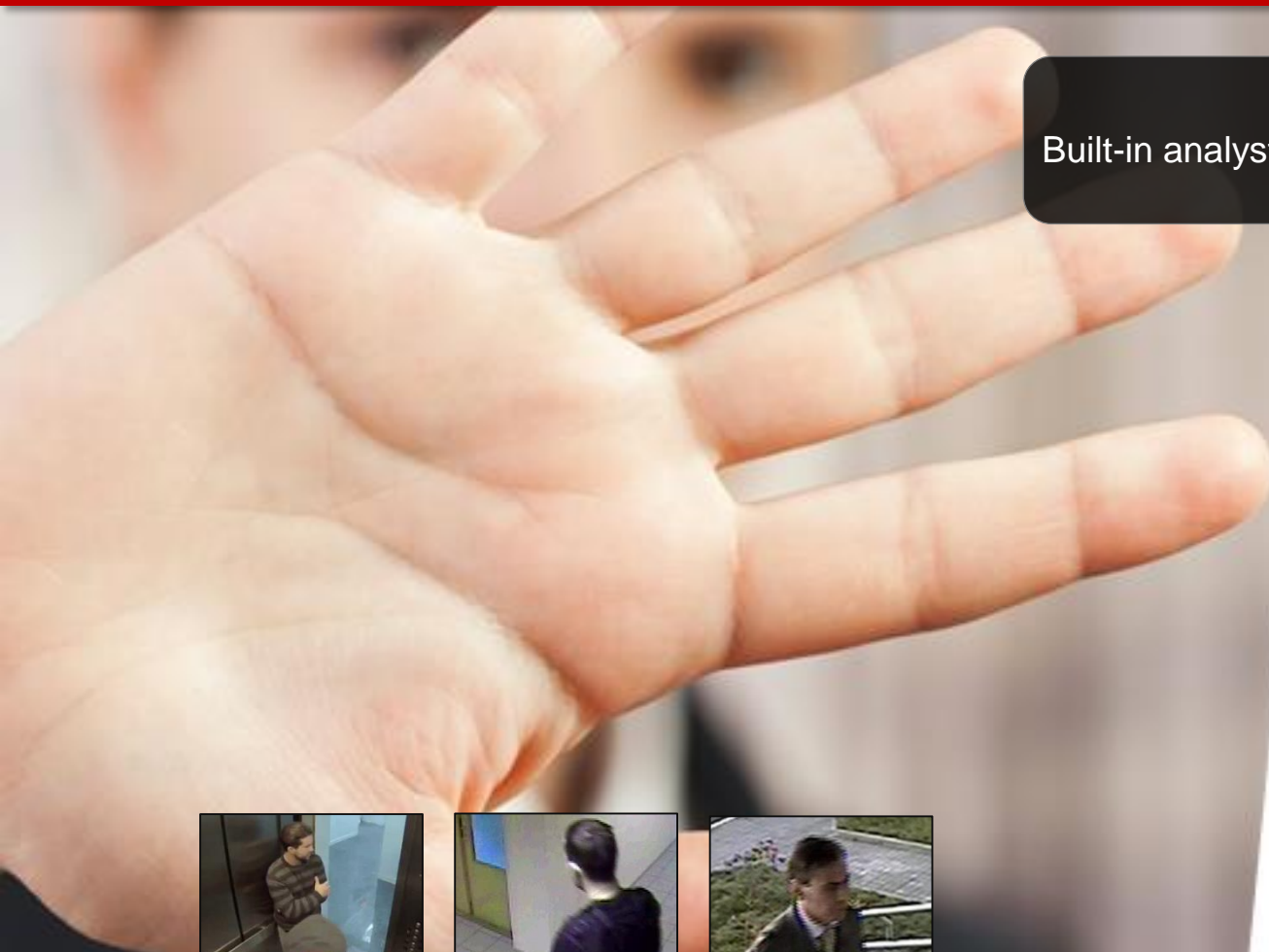
Innovative advertisement tool



Singapore Patent claim № SG 10201702912S  
METHOD AND SYSTEM FOR TARGETED ADVERTISING  
BASED ON PERSONAL PHYSICAL CHARACTERISTICS

## Security

Built-in analyst system allows you to compare the obtained images (faces) with a previously created database



Nobody purposefully looks at surveillance cameras. It is very difficult to register the face image using cameras.

While looking at their reflections, people look directly into the lens, which allows the device to take high-quality pictures for further analysis





Hotels, Beauty salons



Fitness clubs, Spa centers



Business centers, Airports



Restaurants, Night clubs