

Evolutions in CCTV systems

Programmatic document

12/03/2018

CARBONI Marco

www.linkedin.com/in/marcocarboni32



~~CONFIDENCIAL~~

Sommario

Description	2
A. Plant Documentation & Privacy	3
B. CCTV - new feature	8
C. Firmware Management.....	9
D. COMSEC (Communications Security).....	10
E. Identity & Access Management System	11

Description

This programmatic document lists and describes some features that could be development and implemented in CCVT systems, without having to analyze new specific features of the CCTV.

The intervention points are listed below by area of interest:

- A. Plant Documentation & Privacy
- B. CCTV new feature
- C. Firmware Management
- D. COMSEC
- E. Identity & Access Management System

A. Plant Documentation & Privacy

Among the various problems that can be found in the management of a small or large plant is the documentation part of the plant itself, that is all the information that during the upgrade or maintenance phase we would all like to have in place.

I have identified the following tools that could help a TVCC plant manager:

1. Tool and Plant Manuals - an instrument that describes the system with the following chapters:
 - First page customizable with logo and company writings (owner) logo and writings installer
 - Map position cameras with angle of view (hypertext icons) better if in 3D
 - System cameras list (hypertext list)
 - Screen-shot of every single camera with the operating parameters:
 - date installation
 - date retention
 - resolution
 - frame-rate
 - compression
 - time and method of registration,
 - optical data (focal, angle of view, etc.)
 - PTZ brakers
 - penultimate level measurement degradation (Rotakin test)
 - displacement (in case the camera has been moved from the initial resume point)
 - etc.

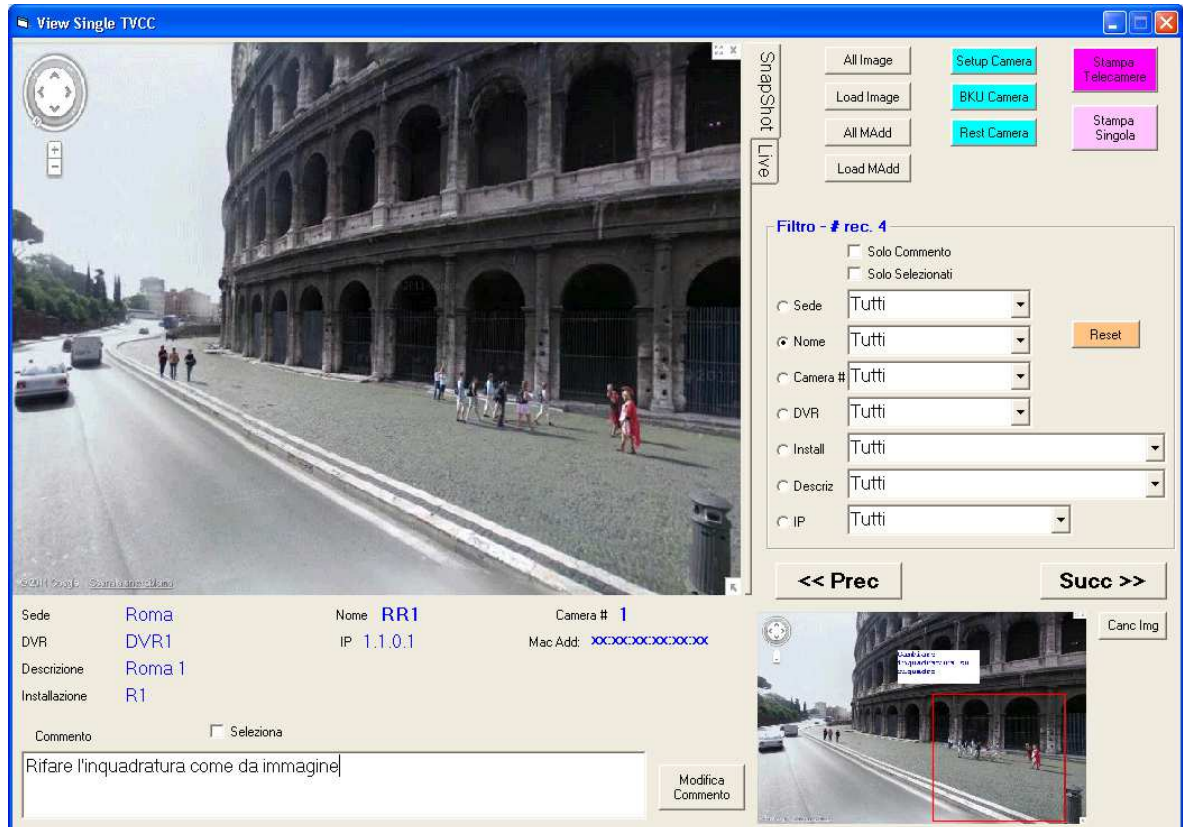
(in case of shooting a people, the automatic system eliminates the faces for management the privacy problems)

- For each camera, the result is a degradation measurement with a measurement screen shot (Rotakin test or electronic measurement)
- Datasheet of every single camera
- Index for system mnemonic code, for mac-address, for IP
- List of people can access to CCTV system
- Digital signature of the installer
- Digital signature of the document / manual


This on-demand tool must automatically extract this information, and retrieve it from the individual cameras or from the supervision platform.

The final product will be a PDF file to be delivered to the owner of the plant or Security Manager, as well as to the Data Privacy Officer.

Tool interface



T1DP6T08



19/12/2017 12:57:55

Dati telecamera

Sede	Milano
CameraNumber	1608
IP	[REDACTED]
Mac-Address	Null
Camera Name	T1DP6T08
Description	[REDACTED]
Location	[REDACTED]
DVR	[REDACTED]
LiveVideoQuality	5 frames per second
Resolution	768 x 576 (4 CIF-Expanded)
Event	-
Scheduled	-
Background	Y
BackgrVideoQuality	5 frames per second
MotionDetection	-


Commento

11 19 dic 2017

Es. of the manuals

INDICE

Nome TVCC	IP	Pagina
E	16	2
Pl	16	3
T	16	4
T	16	5
T	16	6
T	16	7
T	16	8
T	16	9
T	16	10
T	16	11
T	16	12
T	16	13
T	16	14
T	16	15
T	16	16
T	16	17
T	16	18
T	16	19
T	16	20
T	16	21
T	16	22
T	16	23
T	16	24
T	16	25
T	16	26
T	16	27
T	16	28
T	16	29
T	16	30
T	16	31
T	16	32
T	16	33
T	16	34
T	16	35
T	16	36
T	16	37
T	16	38
T	16	39
T	16	40
T	16	41
T	16	42
T	16	43
T	16	44
T	16	45

 19 dic 2017

2. Tool for the production of the employment document for union (RSU) or Ispettorato del Lavoro Italiano for the whole plant or part based on filtering, as documentation of privacy management.

In this document there must be:

- Progressive number of the document
- description of the system aimed at the agreement with the union (RSU)
- camera positioning map related to the agreement
- screen-shot of the cameras
- cameras technical data sheet

~~CONFIDENCIAL~~

Marco Carboni

- list of employee can access to CCTV system

ATTENTION: this tool can not reside on the cloud or web server, but must necessarily be at the PC client (app to download on PC) for privacy and security reasons.

~~CONFIDENTIAL~~

Marco Carboni

B. CCTV - new feature

Here are the new features for the cameras:

1. **RFID** - drowned in the camera body from which to take or store camera information (also maintenance info)
2. **INFO** – visualization, on request, of the data configuration of the camera in overlay at video (es. Frame-rate, resolution, etc.)
3. **Memory** - Greater functionality / flexibility in using local memory to store the video
4. **Manuals** - Put the user manuals and product datasheets on board the camera memory
5. **Meter** - Analysis of UTP cable length, voltage / power available, power consumed, real connection speed
6. **SMTP** - More extensive use of SMTP functionality to be supervised by Management System (such as HP OpenView, or other open source systems)
7. **RF** - HotSpot functionality:
 - WiFi repeater to replace internal building antennas (wiring costs recovery)
 - BLE for the Building Management functions (space management, smart office, indoor geolocation, etc.) here I see well agreements with companies that are very active in this regard (Honeywell, Durante, etc.)

C. Firmware Management

One of the big problems is the firmware management, currently the camera exits the factory with the latest firmware, but it could also take a long time before it is mounted and as a result may have been released many firmware.

It can also happen that the supervision system is not able to manage the latest firmware, as they may have also received major releases, which often happens when you are fixing security problems.

The availability of firmware on the public site makes it also lends itself to reverse engineering aimed at identifying any weak spots and the launch pad for hacker attacks.

So much attention must be paid to the availability of firmware and therefore to its deployment on the systems.

The Blockchain technology helps us, that is to use this technology to manage the *life* of the firmware that goes from the supply, installation on the camera and any recall, all under complete tracking and inability to modify them.

This technology could also be useful for any commercial revamping operations as the direct owner would be known.

D. COMSEC (Communications Security)

Another problem, perhaps bound in those environments of high interest, is the encryption of communication and the certainty that it is that camera and not the other.

To solve this problem, the communication encryption features must be activated, obviously with public keys no less than 256bit, between the supervision platform and the camera, this also to avoid problems of man in the middle.

Here we would find a system that allows you to choose the level of encryption based on the needs and performance that you want to achieve, and can be installed as a plug-in or optional even later.

Obviously this functionality must be developed in close contact with the developer of the supervision platform or implemented in the native drivers installed on the latter (change the place where the encryption level is set).

Here too, the use of BlockChain technology can be convenient for managing activation keys.

At the same time the ability to activate and configure the firewall on board cameras, as well as to be expected that the Firewall can be integrated with the company Firewall management systems.

E. Identity & Access Management System

The problem of the login will be the problem of the imminent future in the field of IoT, but also in the CCTV field, even if obviously the numbers are different.

Here we have two aspects:

- login for system configuration
- login for system operation (login on board supervisor)
- login for maintainer

So a system must be used that is placed between the user of the login, which is human or an application, and the CCTV.

One thing is certain, even after the last note of the Garante Privacy and the Ispettorato del Lavoro Italiano in which they are asking for more wise use, the login of the security systems cannot be left in the hands of the installer or maintenance technician.

It is also essential that the PCs, laptops, tablets and mobile phones that are used to install and maintain Security systems cannot be left to the technical staff and at least made to take them out of the company.

It is therefore necessary to implement an Identity Management system that is integrated on the supervisory platform or external to the system (see CyberArck) and in any case integrated with the management system of the corporate Domain Name (it must also comply with the Company Login and Password policies).

This system will be responsible for managing the login life as well as the various authorizations that can be temporary or even One-Shot.

Here I see two developments in this regard for TOP Security environments:

- development of an armored laptop / tablet that recognizes and is only recognized by the cameras of a given system (Samsung Knox)
- implementation of an Identity Management System (I highly recommend agreements with companies like CyberArck) in this way we could eliminate the concept of Login, to move to a concept of *interpenetration* (ie: *the systems recognize each other*)