



# MOBILE VIDEO SURVEILLANCE IN CITY AND NATIONWIDE VIDEO SURVEILLANCE SYSTEMS

Sami Marjoniemi

**TELESTE**



## TABLE OF CONTENTS

1	Mobile video surveillance in city and nationwide video surveillance systems	3
2	Introduction to mobile video sources, clients and storages	4
3	Your use case and needs	5
4	Availability of video from vehicle, bodycams and drones	6
5	User interfaces optimised for different client types	7
6	Decide whether to go to the cloud or not	8
7	Ensure sufficient network capacity and security	9
8	Pros and cons of each video offload method	10
9	Consider who you can trust	11



## MOBILE VIDEO SURVEILLANCE IN CITY AND NATIONWIDE VIDEO SURVEILLANCE SYSTEMS

In the realm of city and nationwide video surveillance systems, there is an ever-increasing demand for seamless integration of mobile video surveillance sources as well as mobile clients. These systems must effectively receive surveillance video from mobile devices deployed in the field, while also transmitting surveillance video to moving patrols.

This guide aims to present key insights and practical knowledge on achieving efficient, safe and secure mobile surveillance operations. Furthermore, it provides guidance on seamlessly connecting mobile video sources as well as mobile clients to the main Video Management System. By following these recommendations, organisations can enhance their mobile surveillance capabilities as part of their security operations and infrastructure.

# Introduction to mobile video sources, clients and storages

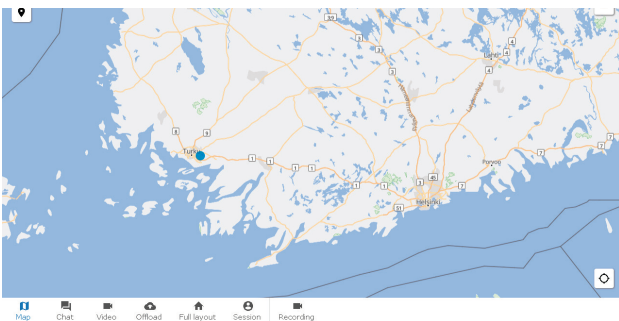
When adding mobile surveillance to your infrastructure, having a unified system for accessing and controlling all surveillance cameras, whether they are normal video surveillance cameras, body cameras, vehicle cameras or drone cameras, offers clear benefits. It is also highly advantageous to ensure that surveillance video can be viewed on all required clients, provided that the necessary user rights are granted.

## Mobile video sources

**Body cameras** are cameras that are worn by police officers, security guards, firefighters, etc., while on duty. Body cameras can either record video locally inside the body camera or stream it wirelessly to a central surveillance centre. The locally recorded videos can be offloaded in the surveillance or dispatch centre to Offload Network Video Recorders also known as storage hotels.

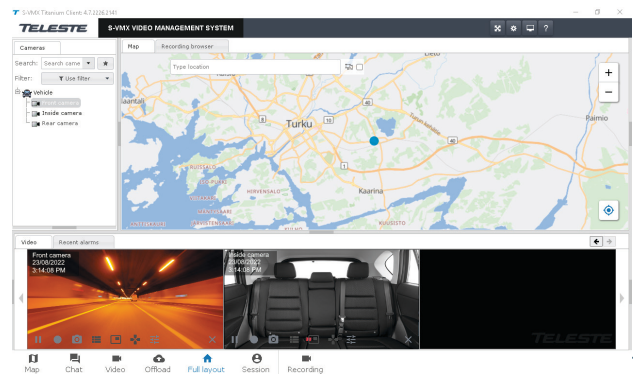
**Vehicle cameras** are primarily installed inside various types of vehicles, including cars (especially police cars), trains, subway trains, trams and other similar vehicles. These cameras are commonly utilised to capture video footage of the vehicle's surroundings and also inside a vehicle. Typically, the recorded video streams from these cameras are stored within the vehicle itself. The live view of these video streams can be accessed within the vehicle, streamed directly to a surveillance centre or both.

**Drone cameras** refer to drones equipped with one or more cameras. The captured video can be streamed to the ground to allow real-time viewing and recording. Additionally / alternatively, it can be stored inside the drone.



## Mobile clients and mobile video storages

**Clients**, in general, are designed to allow a single operator to watch and control video using a single operator station. They can be located both in surveillance centres and individual locations, such as vehicles and personal work desks. **Mobile Clients** are clients optimised for mobile devices and to be used in the mobile environment. These include web clients that are used from mobile devices, dedicated mobile applications optimised for smartphones and tablets, as well as touchscreen clients optimised for touchscreen PCs. These touchscreen clients are used especially inside vehicles together with a vehicle PC. \*



**Local video storage** options include local NVRs (Network Video Recorders), mNVRs (Mobile Network Video Recorders) located inside vehicles, and SD cards that are utilised as storage devices within cameras. MNVRs as well as body cameras and drones equipped with SD cards serve as mobile video storages. \*\*

**Centralised video storages** consist of NVRs or Offloading NVRs designed to store the recorded video footage. The locally stored recordings are offloaded to the centralised video storages when the person or vehicle returns to the base. \*\*

## Your use case and needs

---

Your specific use case and needs should provide the foundation for your video surveillance system. Taking into account the essential topics outlined below ensures that the system will be easily built to accommodate and meet your requirements.

---

**1** **The system should be modular.** Whether your primary focus lies in mobile surveillance, traditional video surveillance, or both, a modular system can be readily adopted and tailored to your specific needs and requirements.

---

**2** **The system should be built as federated from multiple smaller systems.** In such systems, the main video management system at the surveillance centre can act as an umbrella, integrating all subsystems under a unified user interface. This allows efficient monitoring and management of the entire ecosystem – **regardless of whether the subsystems are stationary city or region-wide systems or mobile vehicle systems.**

---

**3** **Your use cases and needs should be communicated directly** to a video surveillance system manufacturer or their premium value-added reseller. Direct communication ensures that your system will be built using suitable and optimal modules that meet your needs and requirements.

---

Compared to single native systems, the modular system structure offers several advantages. Modular systems provide more options for separating different parts of the system regarding, for example, cost sharing, maintenance, security and user privileges. They also allow you to flexibly share resources between different organisations and scale up by integrating third-party systems.

*\*Teleste offers all these types of Clients as part of the Teleste S-VMX product family.*

*\*\* Teleste offers NVRs, mNVRs and Offloading NVRs as part of the Teleste S-VMX product family to extend the S-VMX video management system also to mobile applications.*

## Availability of video from vehicle, bodycams and drones

---

Ensuring the availability of video to all necessary stakeholders is an essential feature of your video surveillance system, regardless of whether the video sources are stationary or mobile, or whether users are on the move or at the surveillance centre.

---

### Inside the vehicle

If Teleste S-VMX mNVRs are used together with vehicle cameras and a local touchscreen in the vehicle, video footage can be viewed and controlled inside the vehicle with the touchscreen optimised S-VMX Titanium Client.

### Vehicles and the surveillance centre

- Users at the central surveillance centre can access both the live and recorded surveillance video from the vehicles.
- Vehicle locations are visible on a map if the Teleste S-VMX Central System is in use and a GPS signal is available.
- Users at the central surveillance centre can engage in real-time chat and effortlessly share snapshots with users who are situated in a vehicle.
- Vehicle recordings can be offloaded at vehicle depots to Teleste Offload NVRs for later inspection and evidence.
- All of the above functions can be performed while maintaining a high level of cyber security, and they are available in addition to the normal video surveillance system functions for stationary cameras.
- Note: Some of the functions above require the use of Teleste VTT-series Secure Access locks and the federation of Teleste S-VMX mNVR to a surveillance centre's Teleste S-VMX system.

### Bodycams and the surveillance centre

The accessibility of bodycams for central surveillance centre users depends heavily on the specific model of the bodycam:

- When using recording-only bodycams, users at the central surveillance centre can access recordings only after they are offloaded from bodycams to offload NVRs. In Teleste S-VMX, offloaded material can be searched, accessed and exported in the same way as normal recordings from stationary video surveillance cameras.
- If the bodycams in use have the capability to provide both live stream and recordings, central surveillance centre users can access both the live surveillance video feed and recorded footage from the bodycams.
- If the bodycams in use come with both live stream and GPS capability, officer locations can also be shown on a map (in Teleste S-VMX Central system).
- Note: When utilising live stream bodycams, it is crucial to give special consideration to cyber security measures.

### Drones and the surveillance centre

From a video surveillance standpoint, drones are almost like bodycams, with the main distinction being that, in certain cases, drones and their flight path can be controlled also from the surveillance centre. It is also worth noting that in some jurisdictions the operation of drones is only permitted if they remain within the physical visibility range of the individual controlling the drone, and other regulations may also apply. In certain situations, the requirement for physical visibility would naturally also arise from other needs and requirements.

# User interfaces optimised for different client types

---

In your video surveillance system, the user interface should also be optimised on the basis of your specific needs and the terminal devices used. The user interface should be designed to support optimisation for at least three different terminal device types and use cases to ensure high system functionality.

---

1

**Normal operator station use** at a surveillance centre or in other office-type location: In these setups, users typically utilise a regular PC or laptop equipped with one or more displays. This setup displays a variety of information using the standard client user interface and allows users to simultaneously view multiple video streams.

---

2

**Vehicle use:** It is essential to have a dedicated and optimised client user interface designed specifically for small touchscreen displays. It should feature dedicated views for main use cases, including displaying videos, map, chat and video offloading. In addition, accessing the complete operator station-type UI in special and administration cases should be possible.

---

3

**Mobile phones or tablets** should also have an optimised user interface specifically designed for these devices. The user interface should feature simple and clear screens that efficiently handle various use cases.

---

All of the aforementioned interfaces should provide an easy-to-use user interface including functionalities such as selecting and viewing live and recorded video, chat functionality and accessing map views. In the mobile and vehicle user interfaces, the map view should also display the user's own location, while in the central surveillance centre UIs, the map should indicate the locations of fixed cameras and moving objects such as vehicles and patrols.



# Decide whether to go to the cloud or not

---

Whether or not to go to the cloud is one of the most frequently asked questions in the field of video surveillance. Despite the hype, it is important to recognise that the cloud is not a magical solution capable of addressing all needs. In fact, a modular video management system (VMS) provides most of the advantages familiar to cloud-based solutions but without their drawbacks.

---

## Advantages of a modular VMS

- **Videos can be accessed from different locations** in the network within certain limits mainly related to issues such as user rights and bandwidth. In other words, the location of cameras and network video recorders is entirely independent of the location where the video is displayed.
- **Reliability is improved** compared to cloud-based solutions as both local and central units can be used to maintain operations in case network connections are lost between the sites.
- Even when it comes to **mobile video surveillance**, there are several situations in which cloud applications do not provide the optimal solution. It is true that when seeking live access to mobile video sources in the field, or communicating in real-time with mobile clients, the video data or information often needs to be transmitted over public networks. The cloud might sound like an obvious solution for these cases, but the points mentioned above and below remain valid. Additionally, the route between mobile client and central system - or central system (incl. clients) and mobile sources - should be as direct as possible to guarantee lowest latency and smallest number of potential points of failure. Nonetheless, it is worth noting that there are instances where cloud solutions can be advantageous and should be considered as a viable option.

From **the legality** point of view, a modular VMS is also a safer solution, at least when considered from the point of view of the European Union's General Data Protection Regulation (GDPR) and also many national laws and regulations.

For example, as an owner of all the data produced and stored in your VMS, you might be required to erase specific personal information and all its copies from your data, and you should also be able to prove that you have done so. This task is considerably easier to perform within a modular VMS than in any cloud-based solution.





## Ensure sufficient network capacity and security

---

Network capacity and security demands play a crucial role in large-scale video surveillance systems, and their importance is even more emphasised in mobile video surveillance systems. For a successful outcome, it is essential to keep a few basic considerations in mind.

---

First and foremost, you need to have **components** deployed at both ends of your system. This entails having equipment in the field where mobile (vehicle, drone and body) cameras are situated, as well as in the surveillance and dispatch centres and in other possible central equipment locations.

Secondly, you need to take into account that sharing real-time video and information between mobile video sources, mobile client and the central system requires sufficient **bandwidth**. Additionally, the video streams need to be protected from unauthorised access during the transmission, especially when using mobile video sources or mobile clients.

### Transmission

Video from or to mobile devices is typically transmitted from the field to the surveillance centres or mobile clients by using cellular (4G/5G) networks. Due to technical limitations or cost considerations, you might also need a lower bitrate video stream for remote live-viewing and downloading recordings.

The low bitrate video stream can be either sent directly from the camera over the network or it can be transcoded in the mNVR in the field before sending it over the network. Mobile clients can receive these streams directly or after stream conversion done in the central system. Stream conversion includes e.g., video transcoding, HLS streaming and multicast-to-unicast conversion. It is also worth noting that different type of IP networks may require stream conversions.

### Security

To safeguard video streams and other confidential information as well as video sources and clients from unauthorised access, the transmitted video and data should always be encrypted effectively. There are several methods to achieve this, ranging from software-based solutions to dedicated hardware devices establishing encrypted connections optimised for video surveillance. Both SW and HW-based methods are available as part of the Teleste S-VMX product family.

## Pros and cons of each video offload method

---

The collection of evidence and investigation material from mobile video sources typically involves offloading videos and related metadata from mobile devices and systems to central offload NVRs. Offloading the recorded video material in the dispatch centres can be achieved by utilising wireless connections, connecting the recorder via cables or utilising USB drives or bodycams equipped with SSDs and SDs specifically designed for offloading and uploading the material.

---

### Wireless offloading



Offloading can be fully automatised. There is no need to physically remove or connect devices.



Achieving reasonable offloading times usually requires a high transmission speed that might be challenging to achieve for a high number of vehicles in the same location at the same time. For this reason, an easy manual selection of the offloaded material is also needed, instead of just automatically offloading everything.

---

### Cabled offloading



Can be fully automated. High transmission speed is easier to achieve for offloading for a high number of vehicles in the same location and at the same time than in wireless offloading.



Laborious and very impractical to perform in real life field conditions.

---

### Offloading from USB drives and bodycams with SSDs and SDs



Exporting the material from vehicle, bodycam or drone is very easy.



Uploading the material to central offload NVRs is laborious. Losing material is easy.

---

All the above offloading methods have a role to play in how much bandwidth your system requires. Investing in thorough system design can help you tackle the challenge, and it is also absolutely important from a network security perspective.

From the security point of view, unauthorised access to video streams is a serious issue, but the most significant risk for your network security comes from unauthorised access to edge units. Changing passwords, disabling unneeded services and network connections (e.g. maintenance Wi-Fi from cameras), and placing units in hard-to-reach places are all necessary actions to minimise security threats, but you can also utilise dedicated network protection units for the protection of the edge units.

Protecting the central units follows this same protocol: change the default passwords, default ports of the services, limit the user and administration rights, and do not forget to also protect the system documentation.

## Consider who you can trust

---

Trust is one of the most important aspects of building a modern video surveillance system. Choose your system providers carefully and prefer those that have no ties to suspicious parties – whether companies, individuals, countries or anyone you cannot trust.

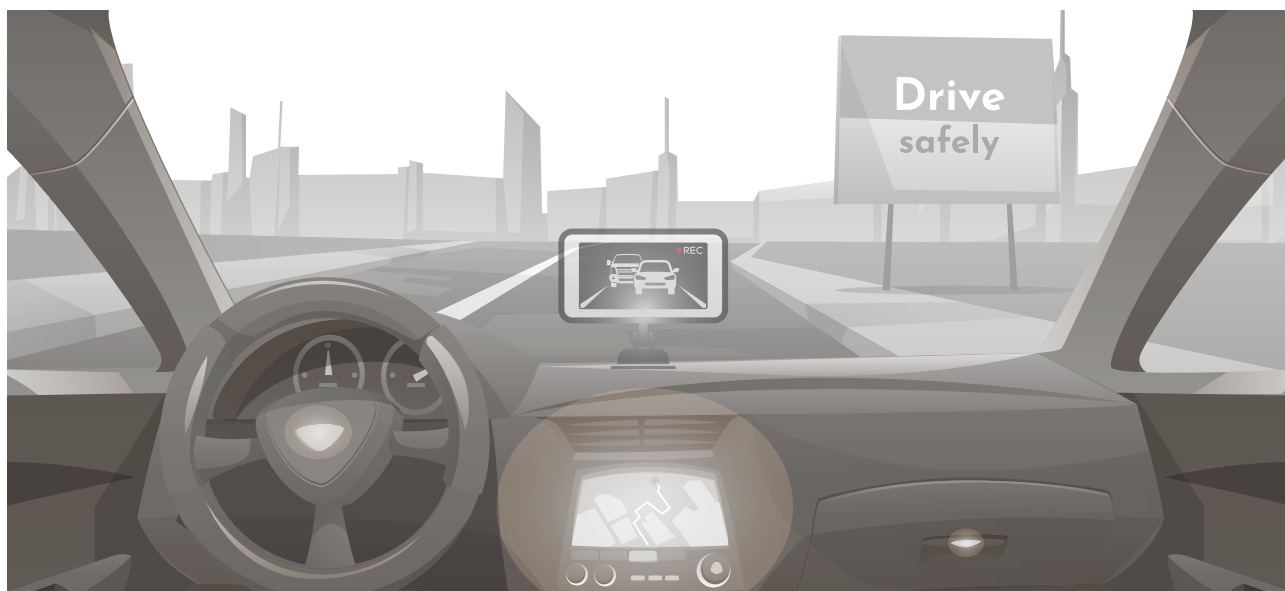
---

Your mobile video surveillance system provider and system integrator will learn a lot about your operating environment, and especially about your network. This information is needed to provide an optimal solution for you, in commissioning the system, as well as in support activities. Unfortunately, the same information can also be used to find weaknesses in the system and learn, for example, how to by-pass network protection.

Therefore, establishing trust is a paramount consideration when building a modern video surveillance system. It is crucial to exercise careful selection when choosing system providers, giving preference to those without any affiliations or connections to questionable parties. Opting for trustworthy and reliable partners ensures the integrity and security of your video surveillance system and your network, allowing you to have confidence in their operation.

All things considered, mobile video surveillance systems are highly powerful tools for public security under normal circumstances, and their relevance in the public sector grows tremendously during crises and disturbances. As technologies evolve, it is easy to get overwhelmed by the possibilities the systems offer, but it still pays to not give too much weight to all those nice-to-have features.

What matters the most is a comprehensive assessment of your current and future needs as well as the costs and benefits of the options available. A future-proof VMS with mobile video surveillance features fits seamlessly into your ecosystem, supports you in what you need to achieve, and is ready to evolve alongside your changing environment and requirements.





# TELESTE

**TELESTE CORPORATION**

P.O.Box 323

FI-20101 Turku, Finland

**[www.teleste.com](http://www.teleste.com)**

*P31\_Mobile video surveillance in city and nationwide video surveillance systems 2023*

*Copyright © 2023 Teleste Corporation. All rights reserved. Teleste and the Teleste logo are registered trademarks of Teleste Corporation.*

*Other product and service marks are property of their respective owners.*

*Teleste reserves the right to make changes to any features and specifications of the products without prior notice. Although the information in this document has been reproduced in good faith, the contents of this document are provided "as is". Teleste makes no warranties of any kind in relation to the accuracy, reliability or contents of this document, except as required by applicable law.*