Dell Technologies Video Analytics Reference Architecture with ISS

Video Analytics for Urban Mobility and Intelligent Situational Awareness for Cities

October 2021

H18943

White Paper

Abstract

This white paper describes the urban mobility solutions driven by ISS video analytics applications on Dell Technologies infrastructure. It provides an overview of the reference architecture of the solution and the various technologies used. The document also explains the various city challenges that can be addressed using the solution and the differentiating product capabilities.

Dell Technologies Solutions

Copyright

The information in this publication is provided as is. Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Chapter 1 Executive Summary

This chapter presents the following topics:

Overview

Dell Technologies helps reduce risks for customers by validating and ensuring compatibility of end-to-end partner solutions with Dell Technologies infrastructure for common use cases. The pre-validated lab solution reduces system disruption and increases customer speed-to-outcome. This white paper outlines the use of video analytics (VA) to address the challenges with urban mobility and citizen safety. It provides an overview of the reference architecture for the Intelligent Security Systems (ISS) SecurOS on Dell Technologies infrastructure solution including the scenarios where this solution can be used.

Terminology

The following table provides definitions for some of the terms that are used in this document.

Table 1. Terminology

Term	Definition
ANPR	Automatic number plate recognition
HCI	Hyperconverged Infrastructure
IOC	Integrated operations center
ITS	Intelligent transportation system
LPR	License plate recognition
MCC	Monitoring and control center
NAS	Network attached storage
PSIM	Physical security information management
RTSP	Real time streaming protocol
SDK	Software development kit
VA	Video analytics
VMS	Video management system

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on the solution and the solution documentation. Contact the Dell Technologies Digital Cities team by email.

Author: Vijay Gadwal: Solutions Architect, Dell Technologies <Vijay.Gadwal@Dell.com>, Eugene Beytenbrod: Director of Engineering, ISS <eugene@issivs.com>

Contributors: Eric Wong: Technical Content Developer, Dell Technologies <Eric.Wong3@Dell.com>

Chapter 2 Challenges Faced by Cities

This chapter presents the following topics:

Urban mobility challenges

Urbanization is continuing to progress at a rapid clip. By 2030, the United Nations estimates that megacities (metropolises with at least 10 million residents) will be home to more than 750 million people, a 35% increase from today. Meanwhile, cities with over 1 million inhabitants are projected to have an aggregate population of 2.3 billion people, with much of that population concentrated in developing countries.

Growing populations, aging and inefficient transport systems, and rising car ownership in these cities are increasing congestion and reducing productivity. According to the World Economic Forum, the number of cars worldwide is set to soar in the decades ahead, climbing from 1.1 billion in 2019 to 2.0 billion by 2040. Inadequate transport systems are also a significant driver of poor health (from emissions and road accidents) and exacerbate social inequality in cities by restricting access to education, jobs, and health care.

Digital cities (smart cities) emerged as a response to these growing trends as an attempt to address these challenges with better data and technology. Today, as some of the key technologies like edge processing, 5G, data management, artificial intelligence (AI), cybersecurity, and modern, agile application architectures converge, create an unprecedented possibility for cities to develop powerful, new capabilities towards delivering citizen outcomes more efficiently and effectively.

Urban mobility solutions are one of the key areas of focus that most cities are focusing on as part of their transformation strategies.

Some of the key urban mobility challenges faced by cities can be categorized into the following:

Transportation and citizen safety

- Most big cities are stuck in traffic jams that paralyze city life.
- The number of traffic incidents growing from year to year.
- Traffic incidents, along with roadside deaths and injuries, are growing every year.
- An increase in traffic incidents and traffic violations leads to even more traffic jams.
- Traffic jams tend to increase pollution and worsen the ecological situation in cities.

City management process and technologies

- City traffic management systems do not meet modern challenges and cannot cope with traffic problems.
- Most cities do not have the necessary modern digital infrastructure for effective monitoring and managing of road infrastructure.
- Operators of city control centers are no longer able to cope with the huge number of events that must be responded to.
- Most urban city management systems do not scale efficiently.

- Urban infrastructure is not integrated and cannot be effectively managed.
- Most city management systems are outdated and do not meet cybersecurity requirements.

Challenges for city IT administrators

In the same way as urban transportation problems pose challenges in ensuring seamless utilization of city resources, lack of a robust and agile city IT infrastructure limits the capabilities of city administrators to leverage the full potential of the various solutions being implemented. Smart city initiatives involve multiple technology providers and system integrators. The IT infrastructure must be able to cater to the demands of all kinds of applications. Some of the challenges that IT administrators face in a smart city implementation include:

Scalability

Scalability is defined as the ability to seamlessly scale applications from a pilot to city-wide deployments.

Infrastructure solutions that are not scalable would limit the city from realizing the outcomes at the larger scale. Cities usually start implementing newer solutions as pilots catering to a smaller area, however, as these pilots generate outcomes, these solution deployments should be able to be rapidly expanded to cater city-wide. This expansion would result in generating enormous amounts of data and the need for compute capability also increases. The infrastructure supporting these solutions would have to be capable of scaling up vertically and horizontally while maintaining efficiency.

Security

Security is the ability to secure the data at motion and at rest, also ensuring controlled access to data.

In a digital city context, security and privacy are among the most important aspects to consider while designing newer solutions. It is of paramount importance to the city to secure and protect the data related to its citizens. Thus, the infrastructure driving these solutions must have an intrinsic security capability to support various levels of data protection. Support for encryption, secure boot, signed firmware upgrades, audit logging, and alerts are some of the key security features needed at the infrastructure layer.

Data storage and processing

Data storage and processing involves optimally storing collected data and running efficient analytics on it.

As cities continue to implement newer smart solutions, the amount of data being generated increases enormously. Therefore, it is critical to have a robust and scalable data storage solution that could support multiple types of data that must be processed and stored at varying scale and speed. Many of the digital city solutions would be governed by regulations and policies related to the storage and processing of the data, so it is critical for the data systems to be able to support capabilities like long-term archival, role-based access, geographic distribution, and encryption.

Integration

Integration is the ability to integrate multiple solutions to create an end-to-end outcome.

It is common for cities to have several siloed applications deployed independently of each other. This type of infrastructure limits the ability of the city administrators to realize additional value from combining insights from multiple solutions. There are tremendous possibilities in bringing data and insights from multiple solutions together, which opens a whole new dimension of the value of city data. A centralized view of everything happening across the city gives seamless situational awareness and helps prepare city services to be in a better position to respond to incidents happening on the ground. This needs a strong integration capability, both at the application layer and the infrastructure layer. The ability to deploy multiple types of workloads on the same infrastructure makes integration efforts smoother and quicker to achieve.

Dell Technologies helps address each of these challenges through the wide range of infrastructure products in our portfolio, complementing it with predefined reference architectures and lab validated solutions.

Chapter 3 Video Analytics

This chapter presents the following topics:

The role of video analytics in intelligent systems

Why video analytics is needed

Modern city management and monitoring systems cannot achieve their full potential without the wide use of video analytics (VA), which replaces a significant number of personnel and provides a state of total monitoring and management of business processes.

VA eliminates unnecessary time spent on manual video archive review and provides system operators intelligent data in the form of real-time alarms when incidents happen.

Video analytics capabilities

Modern VA can perform almost any task, and the list of possibilities is constantly expanding. The following list details a few of its capabilities:

- Track and classify objects, such as vehicles, people, animals, and others.
- Detect various situations and implement behavioral analytics, such as crowd, intrusion, loitering, and others.
- Train the AI engine to look for specific behaviors, such as hand sanitation, falling, fighting, and more.
- Monitor business processes (synchronize video and business processes metadata)
- Recognize license plate numbers of vehicles, railway wagons, containers, and other identification plates.
- Detect and recognize faces

State-of-the-art video analytics

A state-of-the-art VA requires a combination of artificial intelligence (AI), deep learning (DL) technologies, and neural network (NN) algorithms.

The use of traditional VA in real conditions is not effective without the use of advanced and robust AI algorithms, which filter out false alarms and provide operators more intelligent data.

Modern AI solutions allow for the setup and customization of VA by operators using natural human language without the use of complex programming languages.

Modern VA allows not only to accumulate important day-to-day data, but also to provide the ability to predict the behavior of various objects in business processes.

The complexity of modern business systems is constantly growing. Simultaneously, there is a growing demand to monitor a huge number of systems, which is impossible to do without the use of modern VA.

For sophisticated VA solutions, seeking technologies from a single supplier plays an important role, as the efforts of integrating technologies from different vendors is proven to be a cumbersome task and does not always guarantee the ultimate success.

VA is crucial to VMS

In the modern world, there is a huge array of information being collected in the form of video recordings. Using only the traditional video management systems (VMS) to process and extract insights from the videos becomes ineffective because of their limited capability to identify details within the videos automatically. Therefore, implementing video analytics (VA) for such scenarios makes it possible to identify important events from the video repository and extract additional metadata effectively.

In today's digital era, data is growing rapidly and humans are becoming the bottleneck in modern business management and monitoring systems. In these conditions, it is the use of VA that makes it possible to automatically process a huge amount of information and allow a person to make decisions only where they are required.

Thus, the role of VA in the modern world is important. As without it, it is no longer possible to imagine any effective system without it.

Application of video analytics in ITS

Scenarios for video analytics

Modern intelligent transportation system (ITS) is impossible without modern VA. Traffic monitoring, automatic incident detection, detection of traffic violations, parking, and E-toll management are some of the tasks in which VA are the primary sensors that power the upper-level ITS subsystems.

For example, video analytics in integrated ITS solutions for traffic monitoring and automatic incident detection can assist with the following tasks:

- Traffic jam detection
- Vehicle stopped in a traffic flow or in a traffic jam
- Vehicle stopped in a prohibited area (exceeding the time limit)
- Vehicle driving in a controlled area
- Vehicle driving on the side of the road
- Driving in a prohibited direction
- Road traffic accidents
- Pedestrians in the roadway
- Animals in the roadway
- Pedestrians moving in a control area
- Counting the number of people in the control area
- Vehicle classification and counting
- License plate recognition

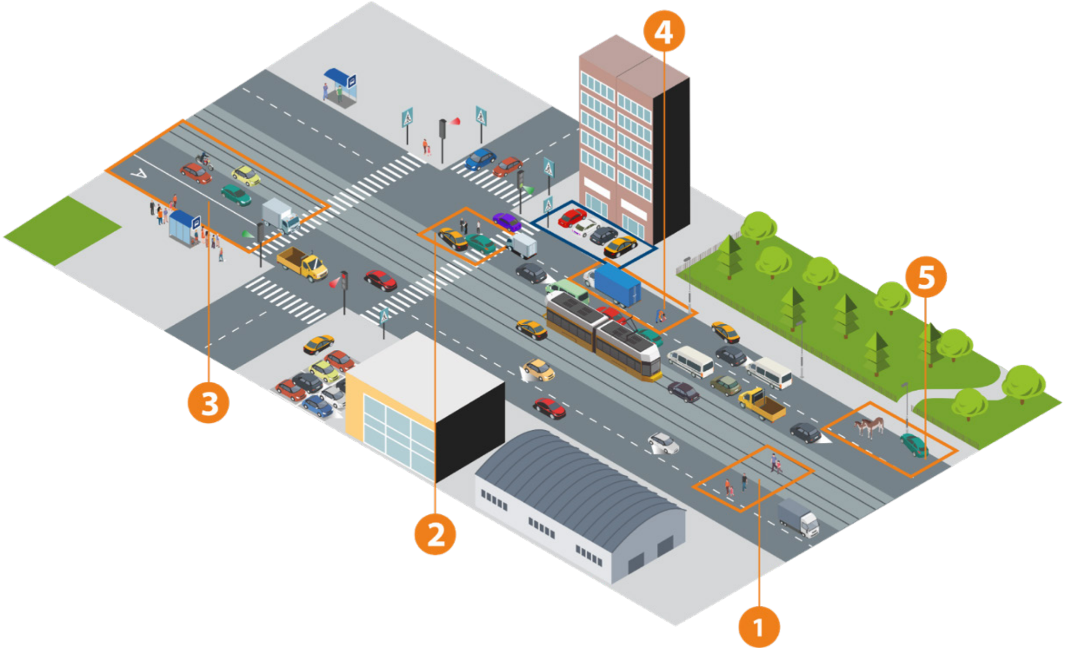

Figure 1. Video analytics scenarios in ITS

Examples of incidents:

- Pedestrians on the road outside the pedestrian crossing
- Road traffic accident—vehicle collision
- Vehicle counting
- Emergency stop
- Animal in the roadway

Advantages of native analytics

The efficiency of modern integrated systems depends on a seamless VA operation. Using native VA from ISS provides tremendous benefits such as guarantees of technical performance and high-quality support.

In addition, ISS offers unique processing of VA events, which is based on the natural language programming. This approach does not require complex programming logic and customization of the VA for specific incidents in each location. Processing works by defining the control area, selecting one or more events that must be detected, and setting the response time for each event.

Advantages of natural language processing for VA

The processing logic is similar to that of regular language and allows you to combine several conditions into a single linguistic process. Thus, complex VA code at the machine level is present to the city traffic operators in simple language, allowing them to understand and adapt the code without any programming or configuration knowledge.

Unique event processing algorithms

Unique event processing algorithms can be implemented to handle various incident scenarios occurring in a city.

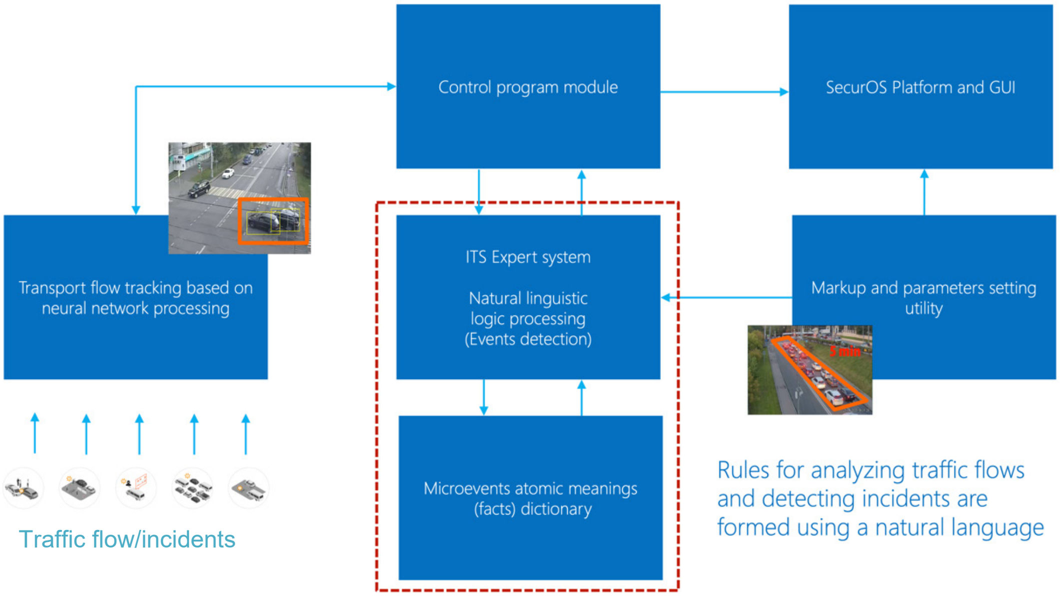
Control program module
SecurOS Platform and GUI
Transport flow tracking based on neural network processing
ITS Expert system
Natural linguistic logic processing (Events detection)
Markup and parameters setting utility
Microevents atomic meanings (facts) dictionary
Traffic flow/incidents
Rules for analyzing traffic flows and detecting incidents are formed using a natural language

Figure 2. ITS event processing algorithms

Chapter 4 SecurOS Use Cases

This chapter presents the following topics:

SecurOS ITS—Traffic violation detection and processing

Traffic violation detection and fine ticketing system is one of the most important parts of ISS comprehensive integrated SecurOS ITS solution. To solve these problems, ISS has a special integrated solution—SecurOS TrafficScanner.

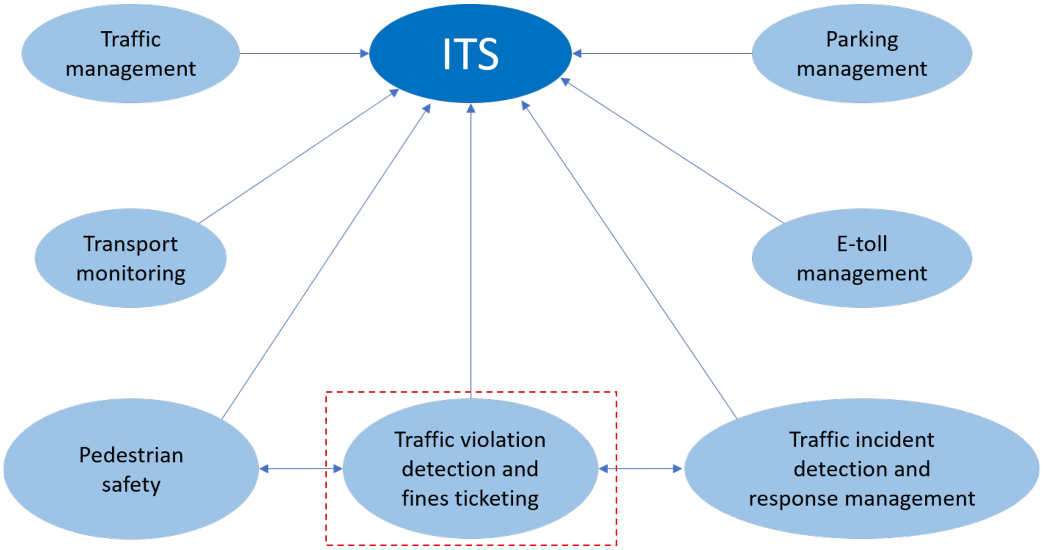
Traffic management
ITS
Parking management
Transport monitoring
E-toll management
Pedestrian safety
Traffic violation detection and fines ticketing
Traffic incident detection and response management

Figure 3. ITS traffic violation detection and processing

Note: Traffic violation detection and fine ticketing systems are government-regulated and require local certification. The implementation of these solutions should be carried out according to a special business process in compliance with local regulations and in consultation with ISS expert teams.

SecurOS TrafficScanner key features

The following are the key features of the SecurOS TrafficScanner solution**:**

- Detection of traffic violations
- Automatic license plate recognition of violator vehicle
- Round-the-clock video recording and storage during a specified time for a subsequent analysis
- Reports on the passage of vehicles
- Detecting vehicles on the wanted list (subject to provision of the respective database)
- Traffic overview video surveillance

Major traffic violations that can be detected

The following types of traffic violations can be detected:

- Running red lights
- Crossing a stop-line when red traffic light is on
- Bypass of closed or closing railroad crossing gates or entrance to railway crossings during prohibitory signals (typically red flashing lights); crossing the railway track outside the permitted zone

- Driving in lanes designated for public transportation, bicycle lanes or pedestrian paths, and sidewalks
- Driving against traffic or driving in prohibited areas
- Turn or U-turn violations of the traffic signs or markings on the speedway
- Movement in the opposite direction on one-way roads
- Failure to let pedestrians cross the road on a crossing
- Exceeding vehicle speed limit

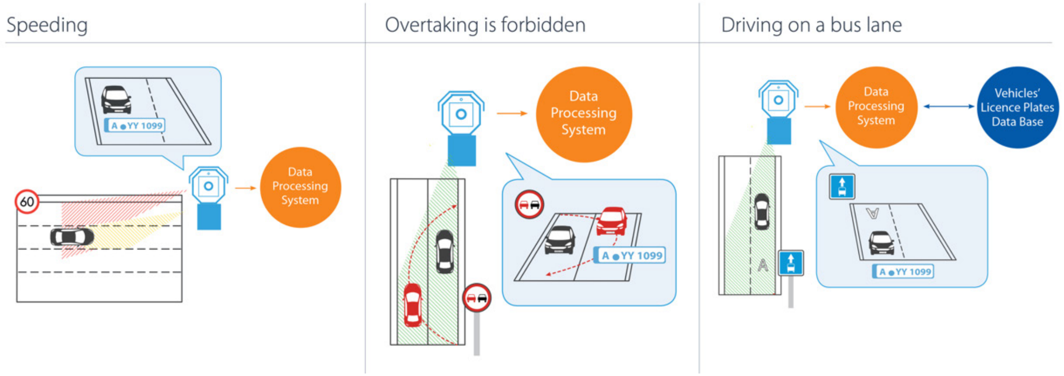

Figure 4. Traffic violation detections

SecurOS Crossroad key features

SecurOS Crossroad is an edge-to-edge solution for traffic violations detection. It combines custom ruggedized hardware components and software for high precision detection and automatic license plate recognition (ANPR).

The solution is supplied with weatherproof processing units, environmentally protected ready-to-mount cases, and complementary illumination. The crossroad system is designed to monitor multiple vehicles and pedestrian behavior at crossroads or in potentially dangerous streets and automatically detect suspected traffic law violations.

Major traffic violations that can be detected

SecurOS Crossroad automatically detects a wide range of traffic violations at crossroads including a violation for failure to give way to pedestrians at zebra crosswalks.

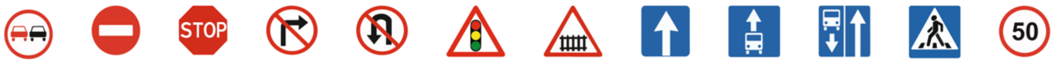

Figure 5. Crossroads violations

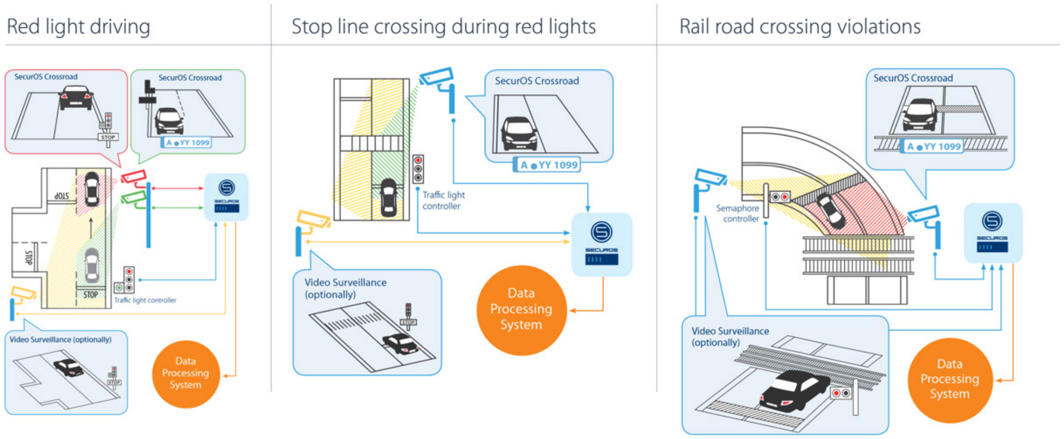

Figure 6. Crossroads traffic violation detections

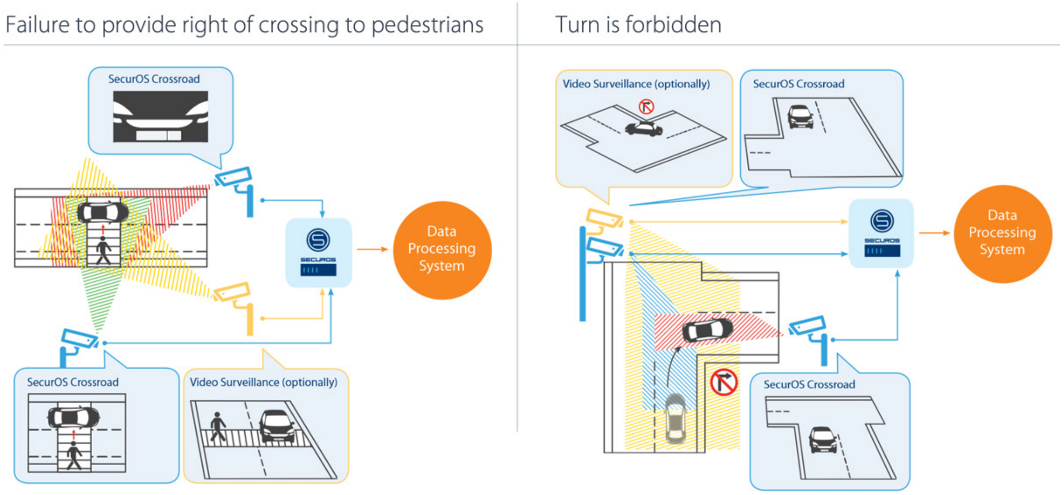

Figure 7. Crossroads traffic violation detections

SecurOS Crossroad solution advantages

The primary advantages to the introduction of video monitoring system for traffic offenses are:

- Monitors roads 24/7/365 by allowing operators to record all cases of offenses in the area of video monitoring.
- Increases efficiency by issuance of citations with minimal human interaction; allowing law enforcement to dedicate more time to more critical activities.
- Generates a high percentage of positive violation detection results: a minimum number of missed violations and a minimum number of false positive detections.
- Yields an exceptionally high-quality proof of violation under any weather conditions (due to the use of video data and specifically engineered hardware).
- Provides scalable solution suitable for every possible road configuration.
- Supports integration with violation processing software.
- Supports integration with external databases to enable automatic vehicle data search.
- Generates reports of vehicles which passed traffic check posts.

- Allows Internet Protocol (IP) cameras of SecurOS Crossroad to be used as a part of a safe city or an urban surveillance system.
- Records video 24/7 in automatic mode for further detailed analysis.
- Assesses the vehicle paths, vehicle speed changes, movement of pedestrians, possible obstacles in the frame/scene, such as foliage, snowing, and other weather events using the SecurOS Crossroad algorithms.
- Supports configuration of separate violation detection scenarios for each individual system.

How SecurOS Crossroad works

SecurOS Crossroad provides a highly accurate evaluation of the traffic situation and minimizes the number of undetected violations or false detection events.

SecurOS Crossroad algorithms assess the vehicle paths, vehicle speed changes, movement of pedestrians, and possible obstacles in the frame/scene, such as weather-related events like foliage or snow. Configuring separate violation detection scenarios for each individual system is supported.

Detection of traffic violations ends with the formation of a special packet of violations and is transferred to the fine ticketing processing system. Fine ticketing processing is an external system, which is under the control of the city transport authority.

The fine ticketing processing system generates the tickets in paper and electronic form and notifies the violator of the violation.

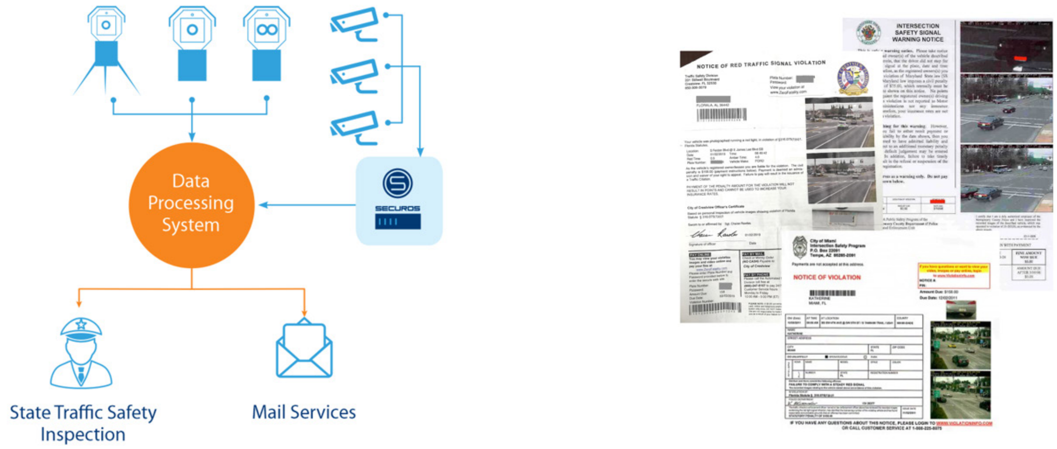
Data Processing System
SECUROS
State Traffic Safety Inspection
Mail Services
NOTICE OF RED TRAFFIC SIGNAL VIOLATION
INTERSECTION SAFETY SIGNAL WARNING NOTICE
NOTICE OF VIOLATION

Figure 8. Traffic violation processing and fine generation

SecurOS ITS—Pedestrian safety

Pedestrian safety is a problem

Ensuring pedestrian safety at unregulated pedestrian crossings is considered one of the most important tasks of modern integrated ITS systems around the world. Many pedestrians are killed or injured in such situations, especially at night.

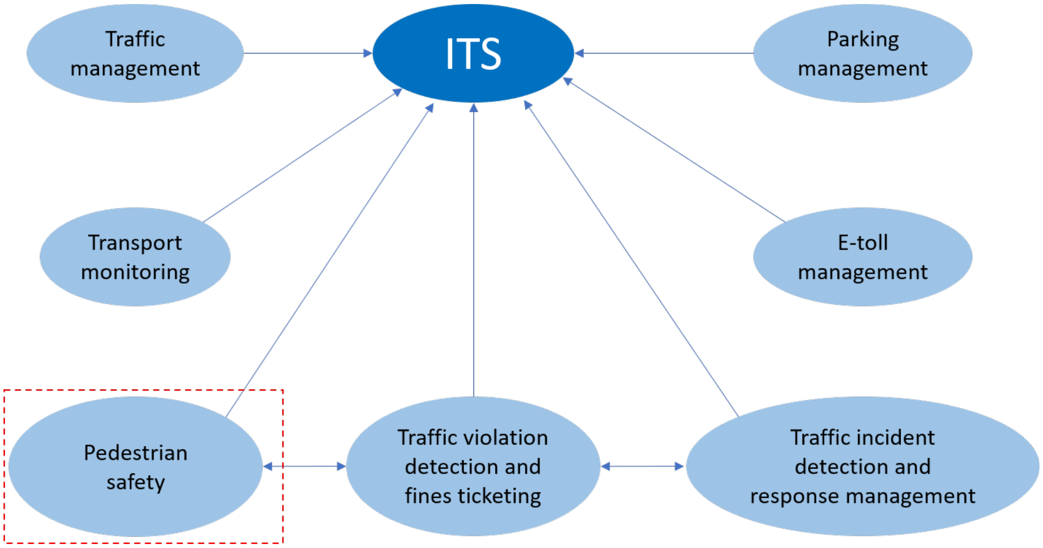
Traffic management
ITS
Parking management
Transport monitoring
E-toll management
Pedestrian safety
Traffic violation detection and fines ticketing
Traffic incident detection and response management

Figure 9. ITS pedestrian safety scenario

To provide pedestrian safety at unregulated pedestrian crossings, ISS has a unique special integrated solution—SecurOS Soffit.

SecurOS Soffit

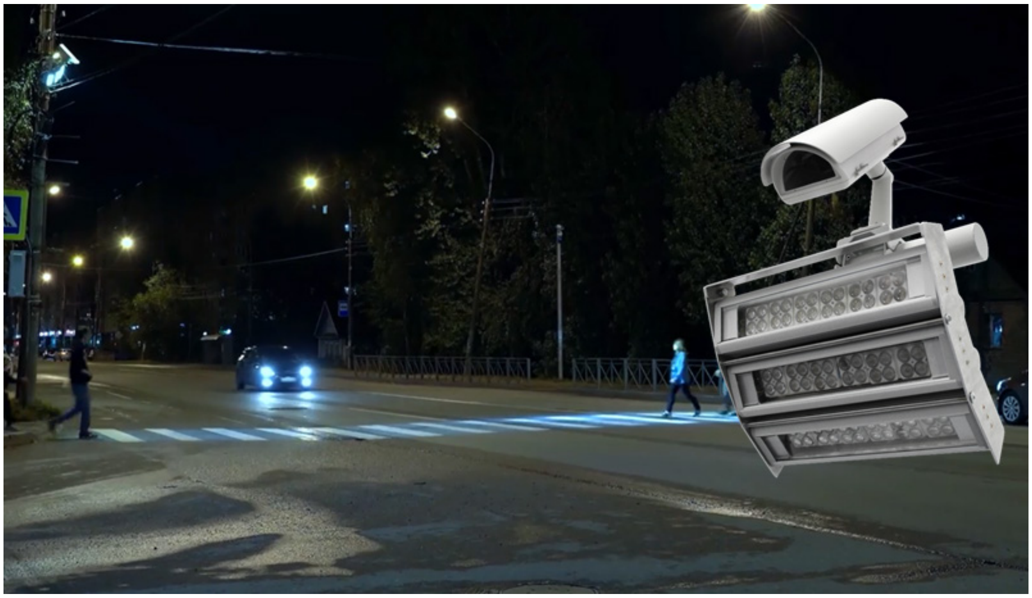

Figure 10. SecurOS Soffit solution

SecurOS Soffit know-how

SecurOS Soffit is an intelligent system which illuminates pedestrians at unregulated crosswalks after dark to prevent them from being involved in accidents. The system focuses the driver's attention on the pedestrian by highlighting the pedestrian with beams of light all the way through the crosswalk. The SecurOS Soffit dynamic lighting significantly improves the driver's awareness of the pedestrian, allowing drivers to slow down and stop in good time. This system is a comprehensive solution designed to improve pedestrian safety after dark and reduce the number of traffic violations and accidents.

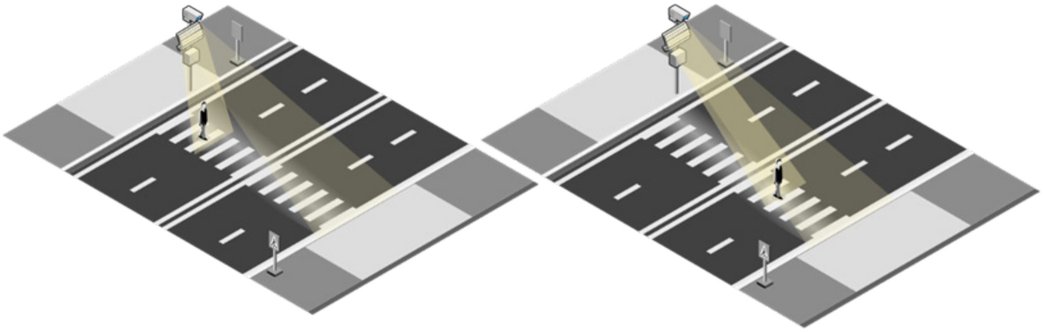

Figure 11. SecurOS Soffit dynamic lighting

How SecurOS Soffit works

The SecurOS Soffit focuses the driver's attention on the pedestrian by highlighting them with a beam of light all the way through the crosswalk.

The system's VA detectors, which are based on AI and computer vision technologies, process video from the IP video camera: detect and accurately classify objects—such as pedestrians, vehicles, and more—pinpoint their location at any given time, and track their trajectory, including changes in the speed of moving objects. The solution algorithms are not affected by possible interference in the frame, such as leaves, snowfall, shadows falling on the crosswalk from road signs or trees. The use of machine learning technology reduces the probability of the system being triggered by a non-human object down to a statistical margin of error.

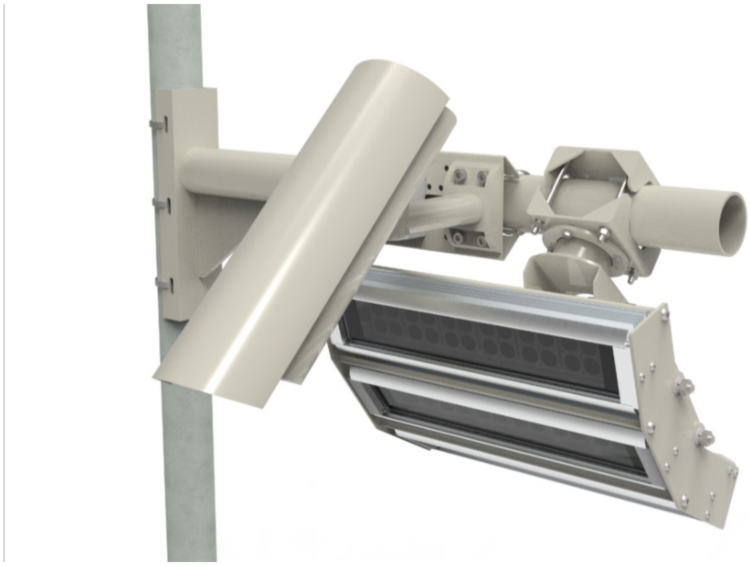

Figure 12. SecurOS Soffit equipment

Static and dynamic illumination of crosswalk

Unlike solutions that use static illumination of crosswalk signs or asphalt in the area of crosswalk markings, the SecurOS Soffit LED floodlight focuses the driver's attention entirely on pedestrians, without diverting it to other objects. This system element is designed so that each of the eight LED modules illuminates its own section of the crosswalk while people are on it. The brightness of the LED modules can be adjusted for the lighting conditions of the place where the system is installed.

The SecurOS Soffit works automatically around the clock, but the crosswalk is illuminated only after dark.

The dynamic lighting can provide constant or pulsing illumination. The pulsing lighting makes a pedestrian even more visible to the driver against the glare of streetlights, bright signs, advertising displays, and headlights of other vehicles.

Once the pedestrian leaves the control zone, the SecurOS Soffit system floodlight returns to standby mode.

SecurOS ITS—Incident processing and response management

The incident detection, processing, and response management system is one of the most important parts in integrated SecurOS ITS solutions.

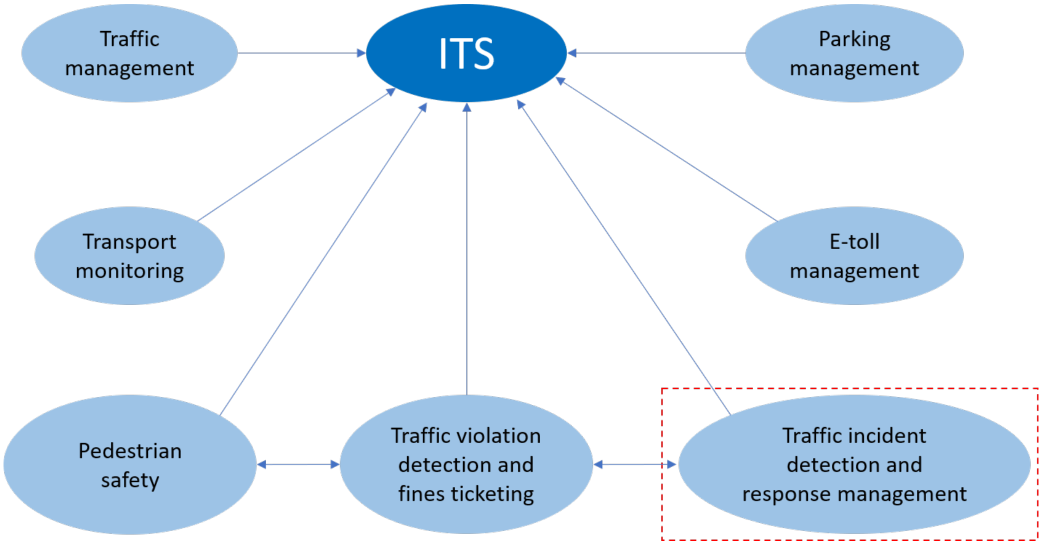
Traffic management
ITS
Parking management
Transport monitoring
E-toll management
Pedestrian safety
Traffic violation detection and fines ticketing
Traffic incident detection and response management

Figure 13. ITS Traffic incident detection and management

The architecture of such systems is inherently complex and integrated. The system uses an extensive network of IP cameras to monitor the road infrastructure and traffic flows. Traffic flows and traffic situation are analyzed using special NN trackers. Metadata from NN trackers goes into a special engine that processes them, classifies, and filters events according to the required criteria. ISS offers unique processing of these VA events, which is defined by natural language programming, see Application of video analytics in ITS.

At the top level, this system displays digital maps, dashboards, and special interfaces that allow operators and response teams to receive, filter and process incidents until they are resolved and closed.

SecurOS ITS system software architecture

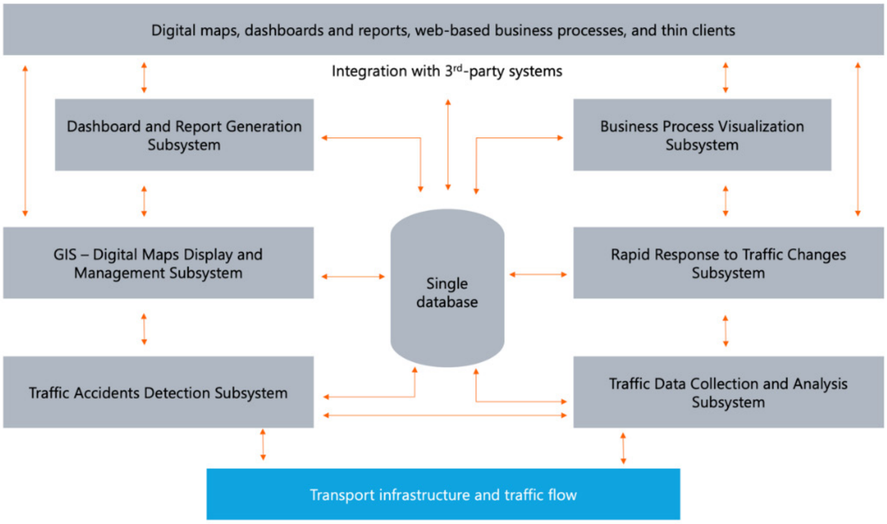
Digital maps, dashboards and reports, web-based business processes, and thin clients
Integration with 3rd-party systems
Dashboard and Report Generation Subsystem
Business Process Visualization Subsystem
GIS – Digital Maps Display and Management Subsystem
Single database
Rapid Response to Traffic Changes Subsystem
Traffic Accidents Detection Subsystem
Traffic Data Collection and Analysis Subsystem
Transport infrastructure and traffic flow

Figure 14. ITS system architecture

Scenarios for ITS VA processing

The geographic information system (GIS) subsystem works as a top-level system. All events from VA are displayed on a digital map and are displayed in a unified user interface. The operator's task is to check incidents, classify them, filter out false events, fill out a special incident form, and send it to the response system.

In the response system, all events are analyzed to ensure that the required responses are sent to the appropriate response teams. All business response processes are automated as much as possible. Typical incidents have a standard processing algorithm available to the response operator as prompts. After the initial processing by the response operator, the corresponding incident is sent to the appropriate team(s) for on-site response.

The onsite response team continues to work with the response system using mobile devices (smartphones, tablets, laptops, etc.). Once the incident has been cleared on site, a report is recorded in the system and the incident is sent to the responsible operator for review and final closure.

After confirming the incident, the information is sent to the GIS system, where it is removed from the active list and enters the event archive. Thus, the incident goes through a full cycle of processing from the moment it occurs, until it is processed and completely closed.

SecurOS ITS VA event processing

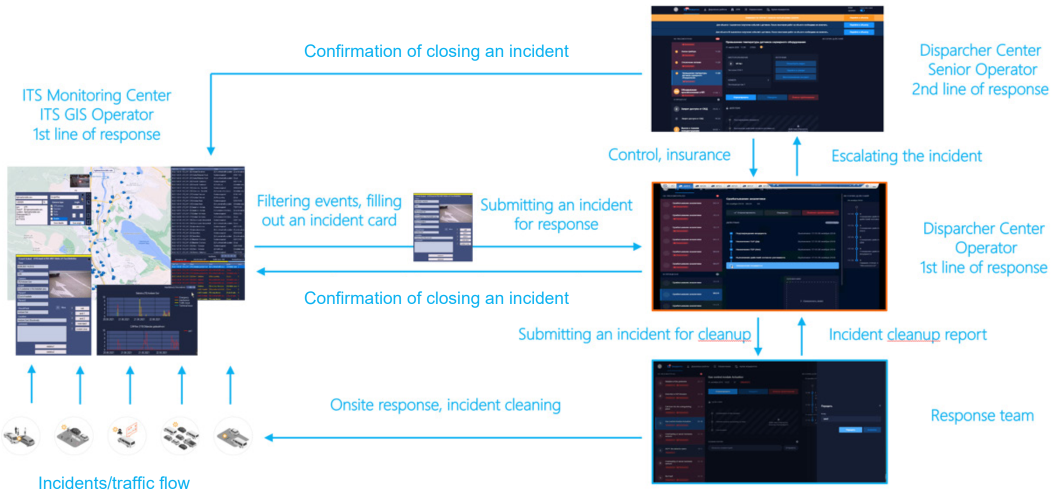

Figure 15. ITS event processing and management

SecurOS MCC for smart and safe cities

The importance of federated architecture

One of the biggest problems of modern VMS and VA systems is the task of combining remote isolated security or business monitoring systems into a single federated architecture with the possibility of their unlimited cascading and scaling.

To solve these problems, ISS has a unique integrated solution—SecurOS Monitoring and Control Center (MCC)—for any command centers in smart and safe cities.

SecurOS MCC as federated architecture

SecurOS MCC provides the global monitoring and management of the complete security infrastructure of all your local sites from a single command center. It is an excellent solution for customers with multiple geographically disparate sites or business facilities spread across a vast area.

SecurOS MCC allows for the federation of remote independent sites as if they were part of a single virtual system. This federation option allows for a more streamlined workflow and globalizes security operations to make security personnel more productive and better informed.

SecurOS MCC sample architecture

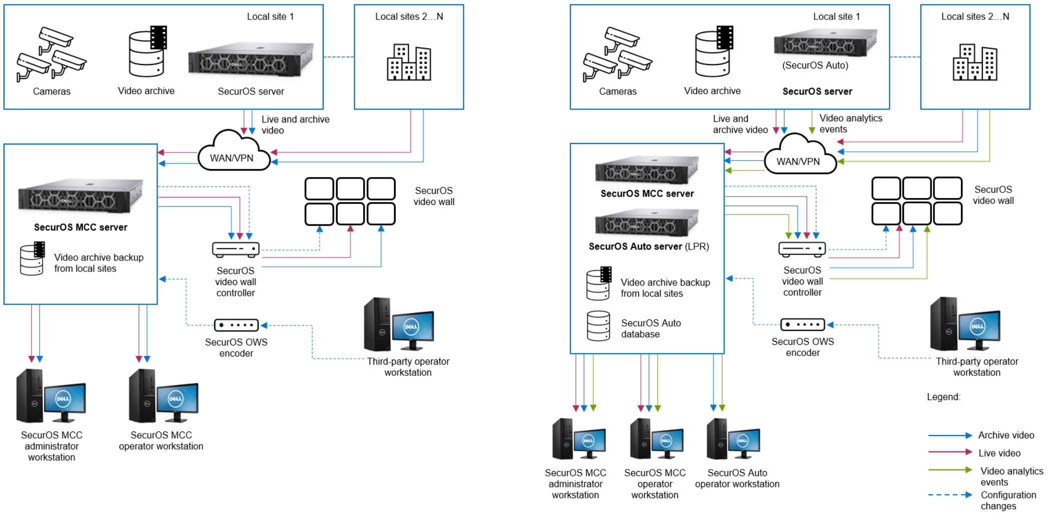

Figure 16. SecurOS MCC architecture

SecurOS MCC federation capability

The SecurOS MCC federation capability scales as required to tie together up to hundreds and thousands of globally disparate sites, and provides management of all SecurOS servers within the virtual network and visualization of all cameras and other devices which are connected to each individual SecurOS deployment.

It standardizes security procedures and automated alarms and actions across an organization’s complete security infrastructure.

The SecurOS MCC is ideal for installations with around-the-clock operation requirements. It also supports interoperability with professional failover data storage systems which provide continued access to live and uninterrupted video recordings.

MCC can be equipped with an integrated SecurOS VideoWall for operators demanding supreme situational awareness of any event.

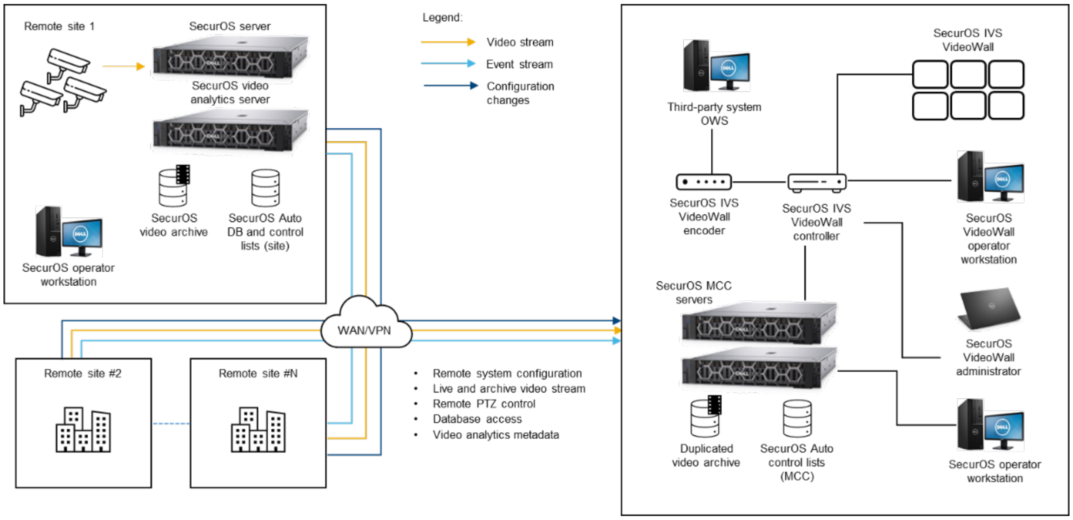
Remote site 1
SecurOS server
SecurOS video analytics server
SecurOS video archive
SecurOS Auto DB and control lists (site)
SecurOS operator workstation
Legend:
Video stream
Event stream
Configuration changes
Remote site #2
Remote site #N
WAN/VPN
Remote system configuration
Live and archive video stream
Remote PTZ control
Database access
Video analytics metadata
Third-party system OWS
SecurOS IVS VideoWall
SecurOS IVS VideoWall encoder
SecurOS IVS VideoWall controller
SecurOS VideoWall operator workstation
SecurOS MCC servers
SecurOS VideoWall administrator
Duplicated video archive
SecurOS Auto control lists (MCC)
SecurOS operator workstation

Figure 17. SecurOS MCC federation

How SecurOS MCC works

Top level system built on SecurOS MCC can unite geographically separated independent security systems running SecurOS Xpress, SecurOS Professional, SecurOS Premium, or SecurOS Enterprise.

SecurOS MCC can combine different versions of SecurOS VMS from different generations. This allows large systems to be deployed over time without having to update the entire SecurOS system to the latest version.

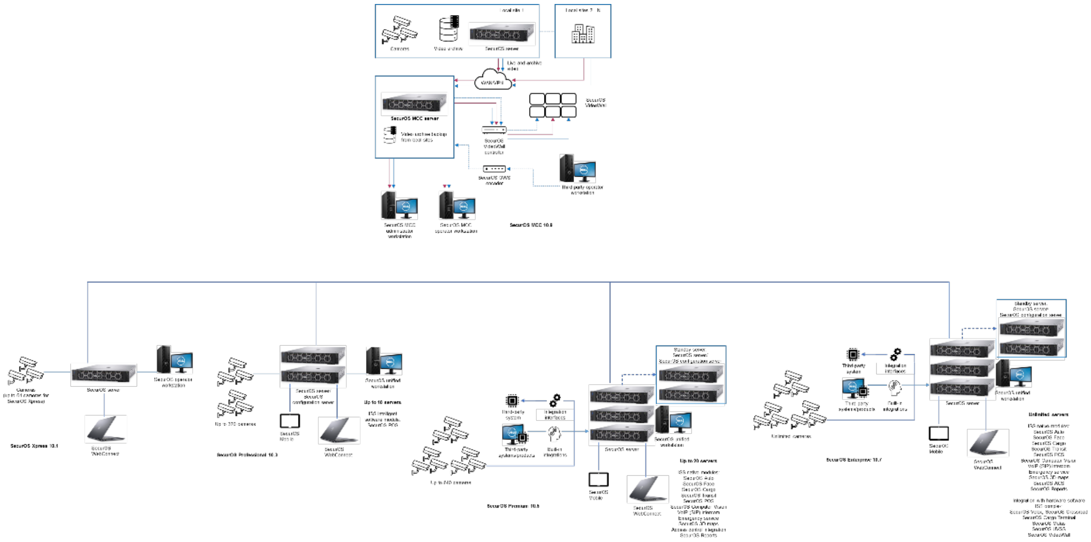

Figure 18. SecurOS MCC with combination of multiple SecurOS versions

The flexible SecurOS architecture allows the creation of a hierarchical structure across several monitoring and control centers. One MCC can be top-level to other MCCs or the responsibilities can be divided among several MCCs in accordance with customer needs.

SecurOS MCC aggregates geographically diverse sites into a centralized and integrated command and control infrastructure. It designed for large-scale and high-security installations: all your security systems based on SecurOS VMS products are under centralized control. The central management stations can receive, display, record video and manage events as well as all video analytics modules and externally integrated systems.

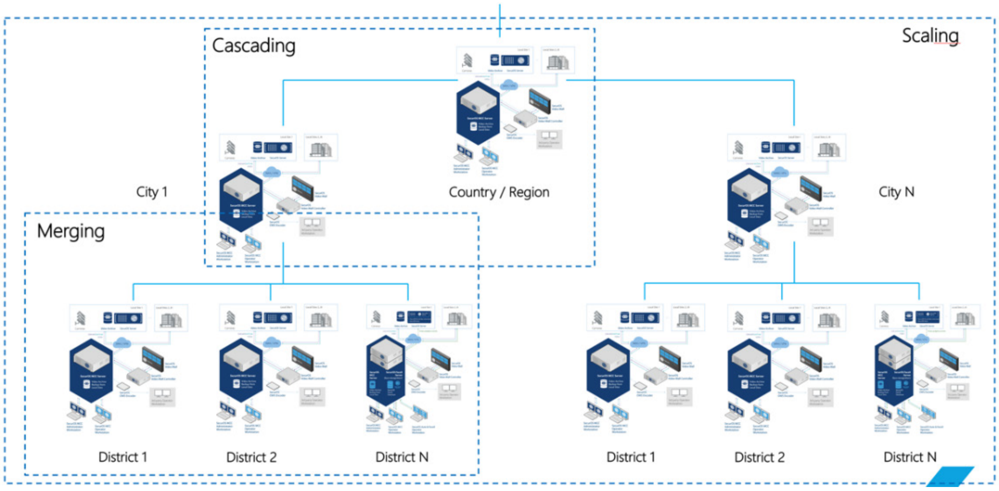

Figure 19. SecurOS MCC deployment models

Chapter 5 Dell Technologies Infrastructure

This chapter presents the following topics:

IT infrastructure components

The Dell Technologies portfolio includes a wide variety of infrastructure solutions that can be leveraged for the optimal implementation of VA-based solutions. This includes compute servers with flexible configuration options as well as hyperconverged solutions that help simplify the deployments. The following sections outline some of the infrastructure components that are well suited for deployment of a video analytics solutions like ISS SecurOS.

Dell EMC PowerEdge

Servers are the bedrock of the modern software-defined data center and the key to building a flexible, efficient, and cloud-enabled infrastructure. Dell EMC PowerEdge servers deliver a worry-free infrastructure that is secure and scalable, with no compromises.

Dell EMC PowerEdge servers provide a scalable business architecture, intelligent automation, and integrated security for your workloads from traditional applications and virtualization to cloud-native workloads. The Dell EMC PowerEdge difference is that we deliver the same user experience, and the same integrated management experience across all of our servers, so you have one way to patch, manage, update, refresh and retire servers across the entire data center. PowerEdge servers also incorporate the embedded efficiencies of OpenManage systems management that enable IT professionals to focus more time on strategic business objectives and spend less time on routine IT tasks. With open standards-based x86 platforms, the PowerEdge portfolio of rack, tower and modular server infrastructure can help you quickly scale from the data center to the cloud.

Figure 20. Dell EMC PowerEdge server

The Dell PowerEdge R740/R740xd is a general-purpose platform with highly expandable memory (up to 3 TB) and impressive I/O capability to match both read-intensive and write-intensive operations. It is well suited to handling demanding workloads and applications like VA.

The Dell EMC PowerEdge R740/R740xd is a two-socket, 2U rack server designed to run complex workloads using highly scalable memory, I/O capacity, and network options. The R740/R740xd features the Intel Xeon Processor scalable family, up to 24 DIMMs, PCI Express (PCIe) 3.0 enabled expansion slots, and a choice of network interface technologies to cover NIC and rNDC. In addition to the R740 capabilities, the R740xd adds unparalleled storage capacity options, making it well suited for data intensive applications that require greater storage, while not sacrificing I/O performance.

Dell EMC VxRail

Dell EMC VxRail, a jointly engineered hyperconverged infrastructure (HCI) system with VMware, is the easiest and fastest way to extend a VMware environment. Powered by VMware vSAN and managed through the VMware vCenter interface, VxRail provides a consistent operating experience. An HCI system includes, at a minimum, compute, software-defined storage, and virtualized networking and can run on commercial off-the-shelf servers. The underlying resources are abstracted and pooled together which allows them to be dynamically allocated to applications running in virtual machines (VMs) or containers.

Built on PowerEdge servers with a choice of Intel Xeon Scalable or AMD EPYC processors, VxRail is designed for today's mission-critical workloads and also delivers multiple compute, memory, storage, network, and graphics options to cover a wide variety of applications and workloads. VxRail supports the latest technologies such as Intel Optane persistent memory, NVMe cache and capacity drives, 100 Gb/s networking, and NVIDIA Data Center GPUs. And with redundancy built in at every opportunity—from the SATA M.2 RAID 1 "BOSS", high-efficiency redundant power supplies, and multiple networking ports—VxRail supports up to 99.9999% high availability.

Figure 21. Dell EMC VxRail

The components that make up a VxRail configuration are as follows:

- Compute—Dell EMC PowerEdge servers
- Storage—VMware vSAN
- Hypervisor—VMware vSphere
- VxRail Manager—Plug-in for VMware vCenter

The VxRail configuration is highly customizable and designed to meet any HCI requirements to appropriately size a VA-based workload like ISS SecurOS.

Dell EMC PowerScale

Dell EMC PowerScale, the world's most flexible scale-out NAS solution, is designed to be flexible and reliable at any scale. Regardless of the type of data, where it lives, or how big it gets, your data lake always stays simple to manage, simple to grow, simple to protect, and simple enough to handle the most demanding workloads of today and tomorrow.

PowerScale NAS was designed and developed for storing, managing, and accessing digital content and other unstructured data. A PowerScale clustered storage system is composed of three or more nodes. Each node is a self-contained, rack-mountable device that contains industry-standard hardware such as disk drives, CPUs, memory, and network interfaces. These nodes are integrated with the proprietary OneFS operating system, which is a distributed networked file system that unifies a cluster of nodes into a single shared resource.

Figure 22. Dell EMC PowerScale

Dell EMC PowerScale is uniquely differentiated from traditional storage to enable organizations to manage high volumes of video data with greater reliability and scalability. With traditional NAS solutions, the larger the data environment becomes, the more complex and time-consuming it is to manage the growing number of storage silos. And at some point, system performance begins to degrade. The PowerScale OneFS is a single file system with single namespace, which enables a single volume to be shared by all the camera streams—thus saving enormous amounts of time in initial set-up. Isilon enables organizations to build a scale-out data lake where they can store their video data at lower management costs and eliminate islands or silos of storage.

Dell EMC ECS

Dell EMC ECS is a complete software-defined cloud storage platform that supports the storage, manipulation, and analysis of video security and unstructured data at massive scale on commodity hardware. ECS is designed to support the mobile, cloud, and big data workloads that are similar to large-scale video management workloads.

Figure 23. Dell EMC ECS

ECS provides multiprotocol access where data ingested through one protocol can be accessed through others. Data can be ingested through S3 and modified through NFSv3 or Swift, or you can choose from many other protocol options as needed.

Dell EMC GeoDrive provides a local file system interface through which we can store and retrieve files on a Dell EMC ECS. GeoDrive provides fast and transparent access to ECS. It does not require complicated shares, mount points, or API development. Since GeoDrive presents an ECS bucket as a local drive in Windows, users and applications can store content in the cloud using existing applications written for Windows, with no additional IT or infrastructure cost. This architecture is used widely to leverage Dell EMC ECS as a tier-2 storage system for video management systems.

Chapter 6 Reference Architecture

This chapter presents the following topics:

Joint reference architecture

The ISS VA on Dell Technologies reference architecture consists of the compute infrastructure as well as the software components to implement the VA algorithms.

Architecture

The following figure outlines the high-level reference architecture of the solution.

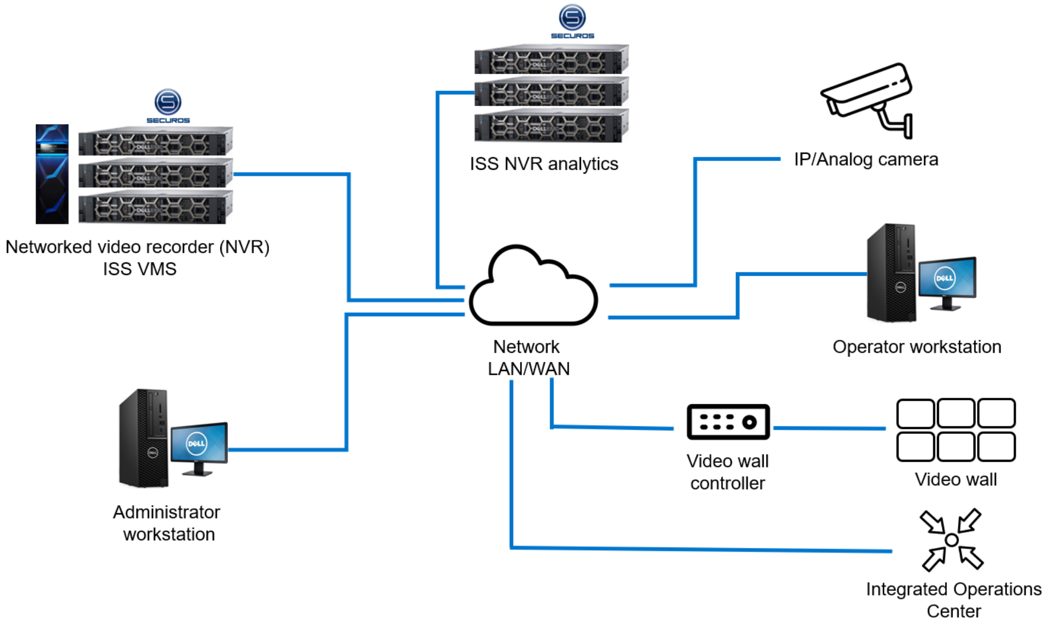

Figure 24. Dell Technologies VA reference architecture with ISS

The various components of the architecture include:

- Compute infrastructure for VA
    - Accelerator cards for performance enhancement
- ISS SecurOS analytics modules
- ISS SecurOS VMS module (optional)
- Operator workstations

The overall solution is a combination of the VMS and the VA modules that run on a dedicated compute environment. The VMS is validated to use external storage systems to persist the recorded videos. The analytics modules can be either deployed directly on the bare-metal servers or run on a VMware-based virtualized environment. The servers are designed for small to large installations, with large camera and bandwidth requirements. Additionally, the servers are engineered to efficiently run ISS VA modules, and support SAN/NAS expansions. Operator workstations are used to run the client applications for the video playback and incident response capabilities.

In addition to the VA use case outcomes mentioned earlier, the solution also enables the integration of the results into other applications like an integrated operations center (IOC) to help provide seamless situational awareness. This integration leverages the APIs provided by SecurOS to share real-time results with other applications.

The next sections describe the key features that distinguish the solution.

Modular architecture

The scalable architecture of the solution allows operators to easily upgrade to other SecurOS editions and include more modules at any point in time. It is seamless to add new functionalities and capabilities with minimal software management. Expanding to a larger scale of operation is also a straightforward process involving addition of compute servers and leveraging a centralized storage system to store the recordings.

Native failover clustering

Modern IT-systems require the implementation of cluster architectures for flexibility and fault tolerance. SecurOS Native Cluster technology allows operators to build flexible, resilient IT systems. In case of hardware failures, the system's functionality is restored automatically, and the recovery process is transparent for video surveillance operators.

A resilient server architecture is key to the continuous availability of video recording. If any physical server fails, the virtual SecurOS video server automatically migrates to the standby physical server. SecurOS Cluster supports various configurations, starting with "2+1" configuration (and even "1+1") and ending with more complicated configurations that may include hundreds of servers. SecurOS Cluster allows operators to create a solution with the required level of redundancy by allocating the right number of cluster servers for backup servers. This eliminates any data loss, security management process shutdown, or video archive loss during the period of work on replacing a failed server.

The failover capabilities include:

- Support of simple "2+1" (2 video servers+1 failover server) to complex configurations, consisting of dozens of servers
- Failover of all ISS features including analytics modules
- Failover operation under 30 seconds
- The ability to assign any SecurOS virtual video server to any physical server.

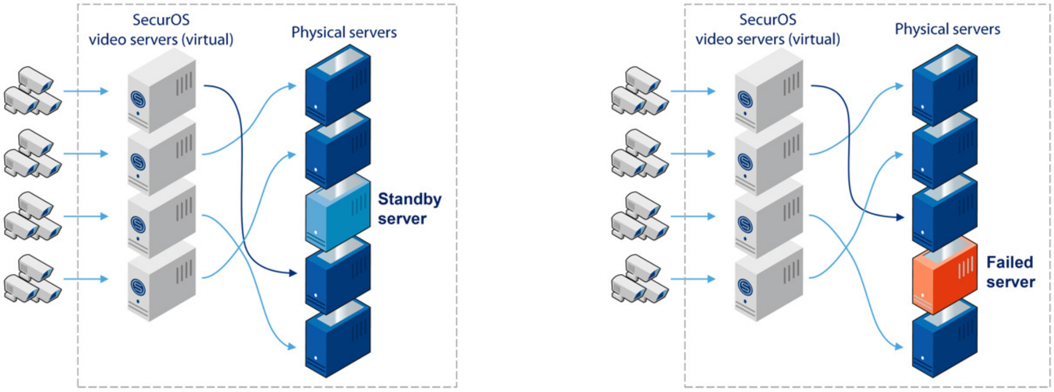

Figure 25. SecurOS failover clustering

Federation

The SecurOS federation capability scales as required to tie together as few as a handful of sites, up to hundreds or even thousands of globally disparate sites, and provides management of all SecurOS servers within the virtual network and visualization of all cameras and other devices which are connected to each individual SecurOS deployment. It further standardizes security procedures and automates alarms and actions across an organization's complete security infrastructure for a more streamlined workflow and globalization of security operations. This automation helps make security personnel more productive and better informed.

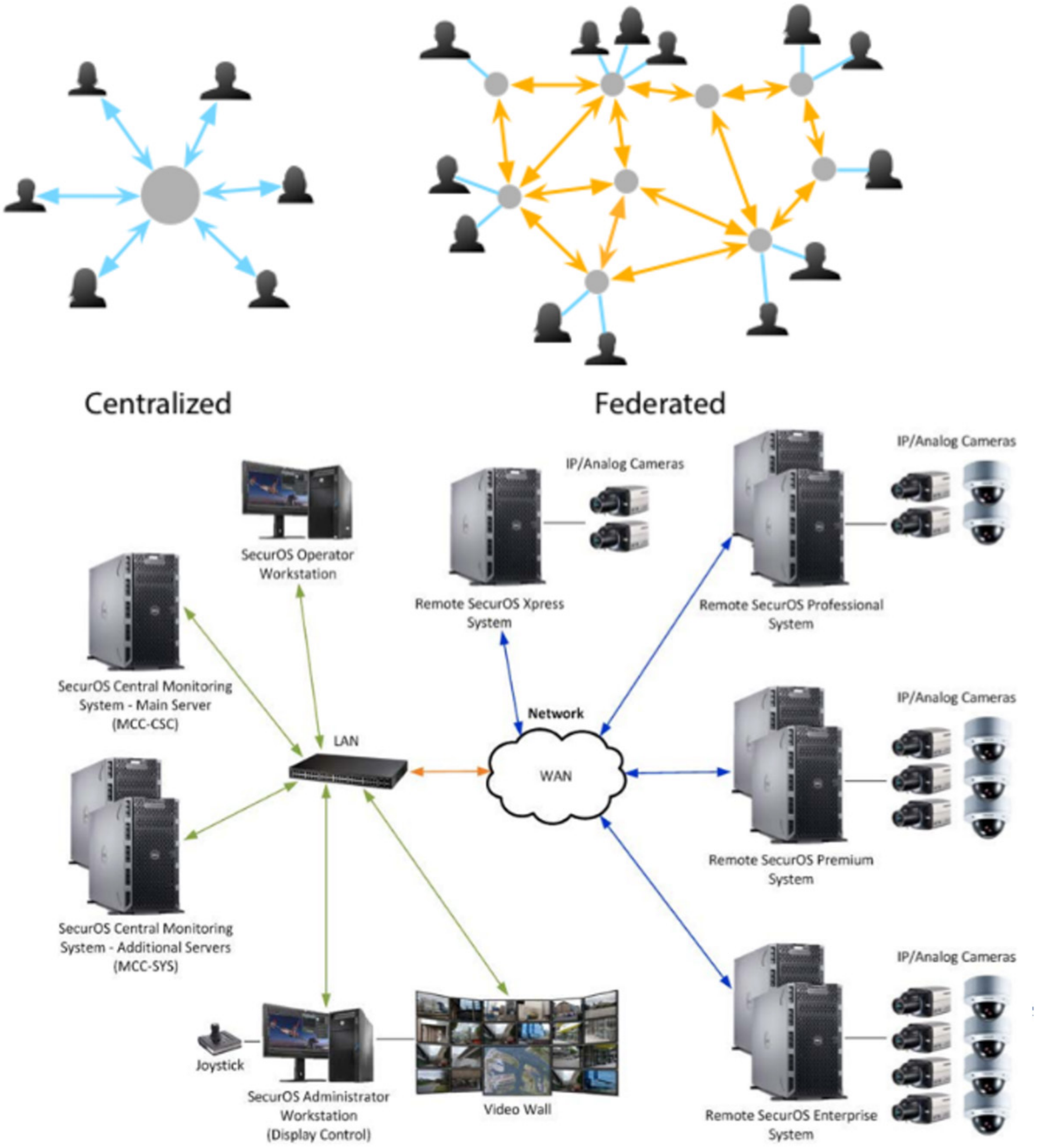
Centralized
Federated
SecurOS Operator Workstation
IP/Analog Cameras
Remote SecurOS Xpress System
IP/Analog Cameras
Remote SecurOS Professional System
SecurOS Central Monitoring System - Main Server (MCC-CSC)
LAN
Network
WAN
IP/Analog Cameras
Remote SecurOS Premium System
SecurOS Central Monitoring System - Additional Servers (MCC-SYS)
IP/Analog Cameras
Joystick
SecurOS Administrator Workstation (Display Control)
Video Wall
Remote SecurOS Enterprise System

Figure 26. SecurOS Federation

The flexible SecurOS architecture allows operators to create a hierarchical structure from several MCCs. One MCC can be top-level to other MCCs, or the responsibilities can be divided among several MCCs in accordance with the customer's needs.

Integration

The SecurOS solution is built as an open architecture platform that allows integration with third-party systems and devices, providing operators with a complete monitoring system. The solution provides an extensive API/SDK toolkit for easy third-party platform integration. Through these integrations, SecurOS can easily share alerts and insights with other applications as well as consume insights and data from external systems.

SecurOS integrates a multitude of ISS and third-party systems into one network and creates a unified command and control capability. All devices, objects, cameras, systems, and even users, macros, and scripts can be individually managed and have multi-level permissions based on login. Each object can be controlled manually or automated using scripts and macros.

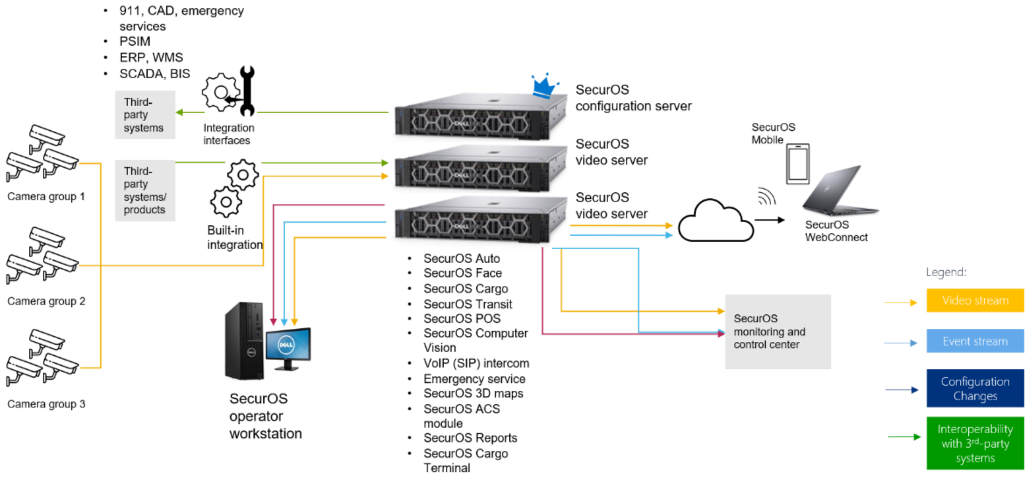

Figure 27. SecurOS Integration Structure

The ability to connect the equipment according to ONVIF and RTSP standards expands the list of integrated devices. SecurOS also provides interaction with software products like:

- ERP-systems, PSIMs, other third-party systems including custom-made corporate systems
- Geographic information system (GIS)
- Emergency Service (911)
- Application-dependent software

Chapter 7 Dell Technologies Lab Validation

This chapter presents the following topics:

Video analytics validation

Dell Technologies helps reduce risks for customers by validating and ensuring compatibility of end-to-end solutions with Dell Technologies infrastructure for common use cases. This pre-validated lab solution reduces system disruption and increases customer speed-to-outcome.

The key objectives of the validation are the following:

- Basic functional testing
- Performance testing
- Measuring the needs of specific system requirements to correctly size an implementation and match the appropriate Dell Technologies products to customer requirements.
- High availability configuration

The ISS SecurOS VA solution has been validated on Dell Technologies hardware components to document the performance characteristics and sizing guidelines for the joint solution.

Methodology

The validation process for the VA solution is based on the following Dell Technologies components:

- Dell EMC PowerEdge server
- Dell EMC VxRail Hyperconverged Infrastructure
- VMware vSphere

The ISS SecurOS modules considered for the validation are:

- SecurOS Auto
- SecurOS Cargo
- SecurOS Tracking Kit

Findings

The following are some of the key findings from the validation:

- The resource utilization is optimal when the SecurOS solution is deployed on a bare-metal Dell PowerEdge server.
- The use of additional GPUs enhances the performance of the algorithms consistently and helps support more channels per server. Some algorithms like the LPR use case support NN processing which can efficiently use GPUs to offload some processing from CPUs.
- The Dell EMC VxRail hyperconverged environment is a good solution choice when virtualization is preferred, however the sizing guidelines are on the higher side and would be different compared to bare metal environment.

The results and key findings from the VA modules validation are captured in the validation guide document titled, ISS SecurOS Video Analytics Solution on Dell Technologies Infrastructure. If you need to see specific validation results and sizing guidelines, do reach out to us using the contact information specified in Feedback.

VMS validation

Validating VMS solutions for hardware and software performance within the customer environment can be complex and time consuming. Dell EMC Safety and Security Labs are outfitted with leading technology from all major safety and security vendors, allowing us to validate all best-of-breed physical security applications with Dell EMC's portfolio of products and solutions. These proven lab validations with key partners accompany extensive documentation to simplify deployment and reduce risk of video loss for our customers.

Methodology

The VMS validation process involves extensive testing simulations with a broad portfolio of hardware and software to uncover data loss issues and provide remediation measures that improve deployment and speed of adoption.

The SecurOS VMS validation was performed using Dell PowerEdge R740xd servers, VMware VSAN for storage, Dell EMC ECS and Dell EMC PowerScale storage systems.

Findings

The validation results conclude that the ISS SecurOS architecture and product suite allows extreme scaling, from a few cameras to up to tens of thousands of cameras, by using Dell Technologies servers and storage systems.

The sizing results also document the optimal bandwidth that needs to be considered in designing the SecurOS video server configuration when using various Dell EMC storage systems like VNX, PowerScale, or ECS. The detailed findings can be seen in the document, Dell EMC Storage with ISS SecurOS Sizing Guide.

Chapter 8 References

This chapter presents the following topics:

Dell Technologies documentation

The following Dell Technologies documentation provides additional relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- Sizing Guide—Dell Technologies Safety & Security Solution with ISS SecurOS
- Technical White Paper: Cyber Resilient Security in Dell EMC PowerEdge Servers
- Running Modern Applications with VMware vSphere with Tanzu on Dell EMC VxRail

ISS documentation

The following ISS documentation provides additional and relevant information:

- The SecurOS Auto Datasheet
- SecurOS Velox—Speed Limit Violations Detection System Datasheet
- SecurOS Crossroad—Complex Traffic Violations Detection Datasheet
- SecurOS Soffit—Intelligent Pedestrian Crossing System Datasheet
- ISS SecurOS Cyber Security Guide
- ISS GDPR Compliance White Paper