NEXCOM
The Intelligent Systems

White Paper

Increase Transportation Security with Video-based Intelligence

Commonly used in the transport sector, computer vision has been used to produce video evidence or render visual assistance on buses, commercial fleets, and patrol vehicles. For concerns over transportation security, computer vision can have more active uses to allow precautionary measures to be imposed or immediate response taken on the spot. To this end, computer vision is increasingly inseparable from video analysis.

In this article, we show how NEXCOM's In-vehicle Computers VTC 7230 and 7240 leverage the 5th generation Intel® Core™ processors to generate video-based security intelligence. The article looks at how the VTCs provide a flexible approach to not only delivering video analysis but also providing consistent performance regardless of evolving analysis techniques. The article also gives consideration to the size and power design of the VTCs, and illustrates how these design enhancements give users mobility to adapt to highly dynamic mobile environments. The article moves on to potential security risks and introduces security tools to create a safe operating environment for video analysis to run.

The Need for Intelligence

Security is a common concern shared among the overall transport sector and law enforcement agencies such as border patrols. Buses and metro transit systems are equipped with mobile surveillance systems to clarify liabilities after a criminal offense or incident takes place. Truck drivers count on cameras providing a view of blind spots for the purpose of gaining situation awareness. Border patrols also deploy camera-equipped trucks to help monitor borders.

However, these systems often compel drivers to divert their eyes from roads to view video, posing road risks from distracted driving. A new paradigm is needed where mobile computing systems can automatically convert video images into actionable information and alert drivers only when necessary (Figure 1).

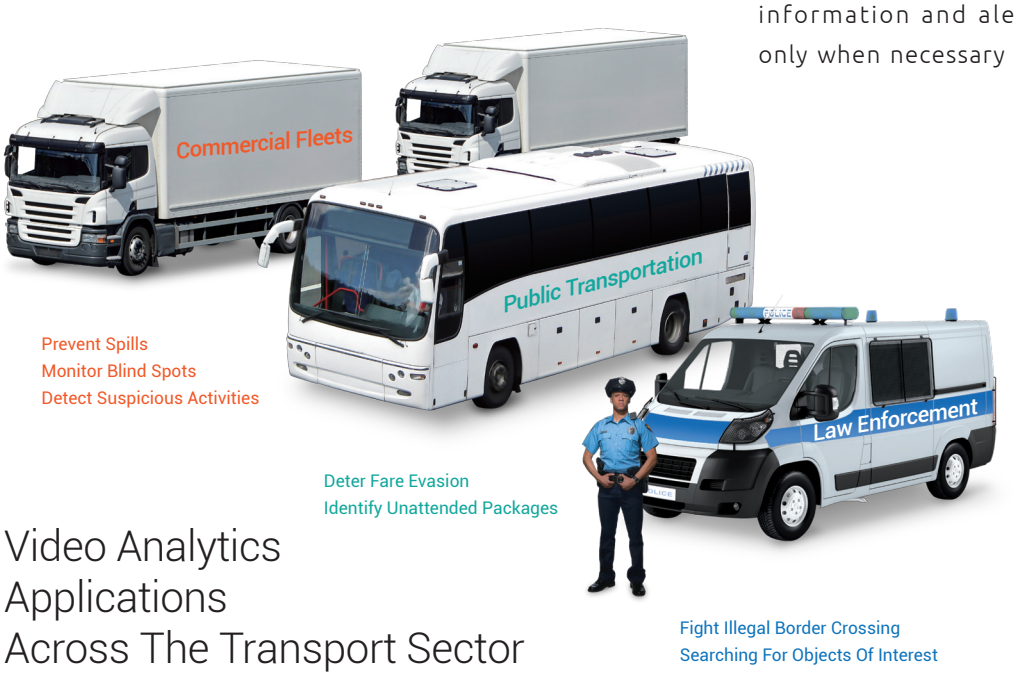

Figure 1. A new paradigm is needed where video images can be converted into actionable information.

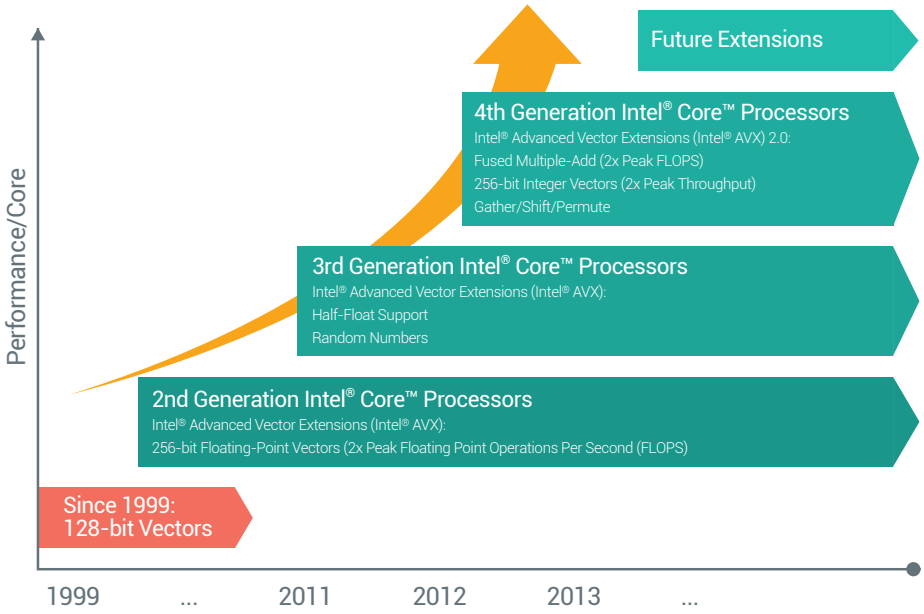

Figure 2. Intel® Core™ processors deliver an upgraded vector-processing technology for signal and image processing.

Turn Images into Intelligence

The new systems must aggregate multiple video streams and data feeds from video cameras and in-vehicle sensors, and perform video analysis based on existing, newly emerged, and yet to be discovered behavioral patterns. Bringing these server-like capabilities onto a mobile system is taxing. NEXCOM in-vehicle computers VTC 7230 and 7240 based on Intel® Core™ i3-5010U and i7-5650U processors respectively can fulfill the requirements by providing outstanding video analytics performance for detecting, identifying, and tracking suspicious activities and objects shown in video images.

These Intel® Core™ processors include the Intel® Advanced Vector Extensions 2 (Intel® AVX2) instruction set, an upgraded vector-processing technology from Intel® Advanced Vector Extensions (Intel® AVX). Intel® AVX 2.0 extends most of integer instructions to 256 bits, doubles the number of floating-point operations per second (FLOPS) per clock cycle, and adds instructions for floating-point fused multiply-add (FMA), vector gather, shift, and permute operations. These improvements enable higher integer, fixed- and floating-point arithmetic throughput to allow for more vector processing operations (Figure 2). The processors also support graphics programmability features like OpenCL 2.0 so developers can utilize the integrated graphics processing units (GPUs) to further boost video analysis performance.

In-vehicle computers like NEXCOM VTCs benefit from using these processors, achieving higher precision and speed in signal and image processing. Take for example unattended package detection. On transit systems, an unattended package is typically regarded as suspicious and a potential security threat. To enhance transport safety, NEXCOM VTCs can apply image sharpening, image segmentation, and object extraction algorithms—compute-intensive workloads usually handled by servers—to identify a static object on real-time surveillance footage.

On discovering a possibly abandoned object, the VTC 7230 and 7240 can send alarm signals to metro conductors and drivers. If necessary, NEXCOM VTCs can report the incident to metro control centers and metro police, transferring the metro train's GPS location, video footage, and other details over cellular or wireless broadband networks (Figure 3).

Reinforce Mobile Task Forces

The signal and image processing capabilities offered by Intel Core processors also enable in-vehicle computers to ease workloads for commercial drivers. The VTC 7230 and 7240 integrate a wide variety of interfaces including controller area network (CAN) and on-board diagnostics-II (OBD-II) protocols to connect to in-vehicle electronic systems. By consolidating information from multiple sources such as dashboard cameras, proximity radars, and tank level gauges, in-vehicle computers can evaluate a traffic situation ahead, calculate minimum stopping distance, and suggest drivers slow down to a safe speed to obviate the need to slam on the brake. Taking such preventive precautions can avoid a potential rollover crash and spill, increasing road safety, and even protecting the environment when goods in transit are flammable materials or hazardous chemicals.

In addition to providing a second set of eyes, in-vehicle computers can assist in fighting illegal border crossing. Temporary placement of in-vehicle computers on scope trucks enables law enforcement agencies to strategically complement surveillance cameras installed along borders. Tracking multiple suspect objects in motion and identifying a wanted suspect are some of practical uses of the VTC 7230 and 7240. They can also be used to apply analytics to thermal images, bringing potential incidents to the eyes of border patrol agents. The Intel® HD Graphics 5500 and 6000 built into these Intel Core processors enable NEXCOM VTCs to show a variety of information simultaneously on as many

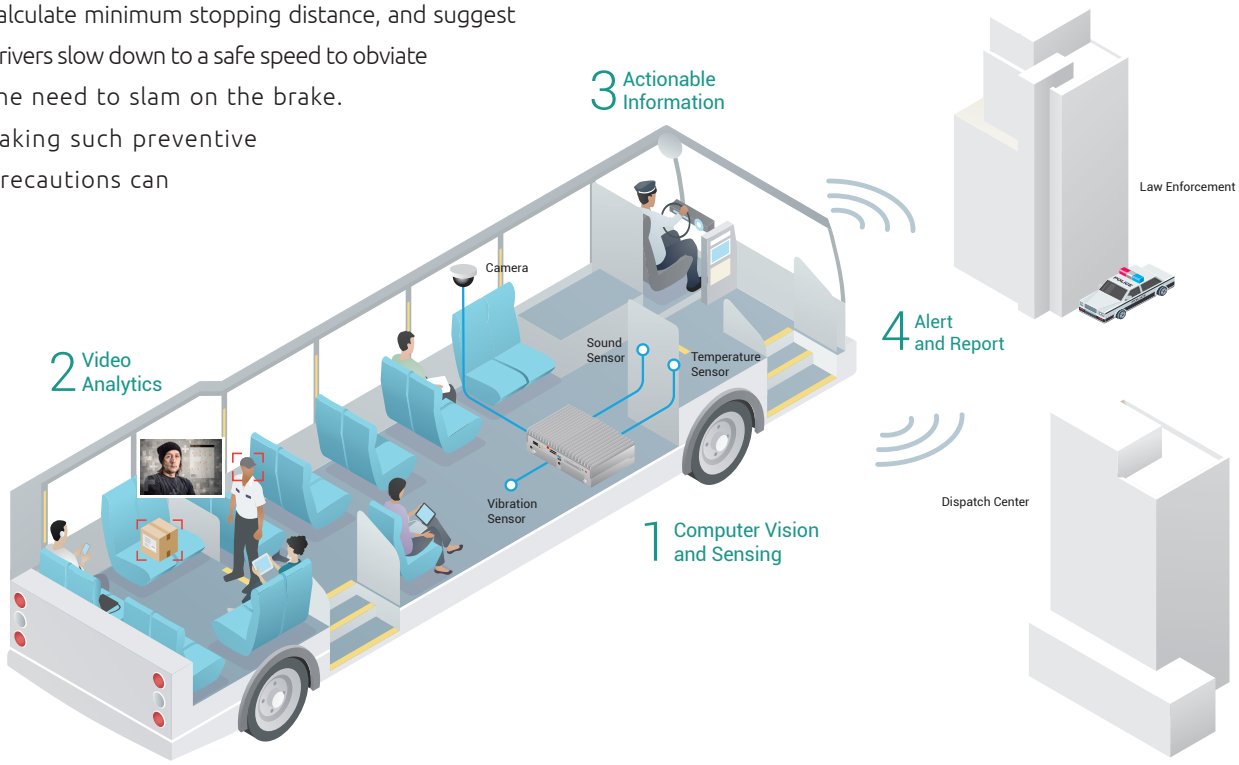

Figure 3. NEXCOM VTC 7230 and 7240 based on 5th generation Intel® Core™ processors provide server-like capabilities.

Figure 4. Temporary placement of in-vehicle computers on scope trucks enables law enforcement agencies to strategically complement surveillance cameras installed along borders.

as three displays with a maximum resolution of 4K (Figure 4).

As opposed to platforms using proprietary video analytics integrated circuits, the Intel processor-based NEXCOM VTCs deliver excellent compute and visual performance, and most important of all the flexibility to run diverse algorithms for imaging analysis needed for specific circumstances and needs. Moreover, Intel Core processors manufactured by the 14nm production technology have a thermal envelope of as low as ten watts and support configurable thermal design power (TDP). As a result, the VTC 7230 and 7240 can carry out compute-intensive video analysis using Intel AVX2 and sidestep processors' TDP limits to assure optimal performance. The DI and DO channels in the VTC 7230 and 7240 can even operate when in-vehicle computers are in a power-off state and wake NEXCOM VTCs to tasks when devices sense vibrations, smoke, or other signals.

Keep Intelligence in Safe Hands

Due to the role played by the VTC 7230 and 7240, securing in-vehicle computers holds great significance. NEXCOM VTCs are armed with Intel® Platform Protection Technology, Intel® Data Protection Technology (Intel® DPT), and Intel® Identify Protection Technology (Intel® IPT) to address security challenges from system boot to application execution.

Intel Platform Protection Technology consists of Intel® BIOS Guard, Intel® Boot Guard, Intel® OS Guard, and Intel® Trusted Execution Technology (Intel® TXT), to help verify the integrity of basic input/output system (BIOS), operating systems (OS), and software. This verification is important since many security tools only offer OS-level protection and may leave in-vehicle computers exposed to attacks aimed at firmware or the OS kernel. Malware targeting a BIOS can persist after a system is rebooted or hard drive wiped, bypassing security mechanisms, and installing an invisible backdoor on a system. With Intel Platform Protection Technology, the BIOS is protected against unauthorized modification. If altered, the BIOS can be restored to a known good state while hardware-based authentication verifies a known and trusted BIOS is used for system boot.

Figure 5. Due to information sensitivity, layers of security protection are provided from system boot to application execution.

Intel DPT includes new Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI). Intel AES-NI allows faster data encryption and decryption for securing data and helping protect confidential intelligence and surveillance footage stored in the VTC 7230 and 7240 from loss. Moreover, Intel AES-NI uses hardware-based acceleration to achieve security enhancement without performance penalties.

In respect of information sensitivity, Intel IPT can add an additional security layer to restrict information access to authorized in-vehicle computers only. Using a combination of private keys, one-time password (OTP) tokens, and public key infrastructure (PKI) certificates, it is possible to examine the authentication of an in-vehicle computer before connecting it to a virtual private network (VPN) to retrieve intelligence stored in remote databases or servers (Figure 5).

Conclusion

Turning captured images into intelligence is an important prerequisite for a response to an incident. The VTC 7230 and 7240 relieve the need for security staff to constantly view surveillance video by enabling excellent performance of video analytics. Using these analytics to identify potential dangers in surroundings, can produce alerts to mobile task forces and provide information they can act on. Instead of documenting activities, NEXCOM VTCs are an active part of a joint mobile task force, searching for potential threats to public transport systems, catching ticket evaders and bus hooligans, and thwarting border trespassers. As more and more video analysis techniques and applications become available, NEXCOM's solutions provide high flexibility, allowing immediate implementation of the latest technology, making it an effective tool for managing and reducing security risks today and in the future.

NEXCOM
The Intelligent Systems

Founded in 1992, NEXCOM integrates its capabilities and operates six global businesses, which are Multi-Media Solutions, Mobile Computing Solutions, IoT Automation Solutions, Network and Communication Solutions, Intelligent Digital Security, and Medical and Healthcare Informatics. NEXCOM serves its customers worldwide through its subsidiaries in five major industrial countries. Under the IoT megatrend, NEXCOM expands its offerings with solutions in emerging applications including IoT, robot, connected cars, Industry 4.0, and industrial security.

www.nexcom.com

intel
IoT Solutions Alliance

NEXCOM is an Associate member of the Intel® Internet of Things Solutions Alliance. From modular components to market-ready systems, Intel and the 350+ global member companies of the Alliance provide scalable, interoperable solutions that accelerate deployment of intelligent devices and end-to-end analytics. Close collaboration with Intel and each other enables Alliance members to innovate with the latest technologies, helping developers deliver first-in-market solutions.

Intel and Core are trademarks or registered trademarks of Intel Corporation in the U.S. and/or other countries.