Solution Brief

Manufacturing Plants and Critical Infrastructure Facilities

Vaelsys and Intel Advance Intelligent, Cost-Effective Security at the Edge

Open V4 delivers precise, cost-effective computer vision intelligence for mission-critical security and safety applications, powered by Intel® Core™ Ultra processors and enabled by Metro AI Suite

At critical facilities across the world, companies are transitioning their video surveillance systems from passive recording to active, AI-based and real-time situational analysis.

Advances in AI-driven video analytics allow computer vision security systems to enable security teams to move from reactive incident investigation to proactive threat detection and operational awareness.

Real-time analytics can identify security issues such as:

- Unauthorized access to restricted areas
- Unsafe worker behavior in industrial environments
- Overcrowding at events or transit hubs
- Suspicious activity in retail and public spaces

Beyond security, intelligent video analytics are increasingly used to improve operational efficiency and safety.

Vaelsys, an Intel® Industry Solution Builders ecosystem partner, has doubled the channel density and substantially reduced the false alarm rate of its Open V4 AI-powered safety and perimeter protection edge solution using Intel® technologies.

Key Intel Technologies

- Intel® Core™ Ultra processor
- Metro AI Suite, including OpenVINO™ toolkit and Deep Learning Streamer (DL Streamer)

Open V4 Brings Intelligence to Cameras

Open V4 is an AI-based video analytics framework that serves as the orchestration and integration layer for multi-camera deployments, enabling centralized management, metadata aggregation, rule configuration, and event handling across distributed sites.

Responsible AI Deployment

Data collection, retention, and sharing policies are defined and governed by the end user in compliance with applicable regulations such as GDPR and relevant AI governance frameworks.

Vaelsys does not create or maintain biometric databases and supports configurable retention policies, role-based access controls, and secure audit capabilities. The company is committed to responsible AI deployment, ensuring transparency, proportionality, cybersecurity, and data protection by design.

Open V4 Ecosystem Creates Unique Solutions

All the tools provided in Open V4 work both with Vaelsys analytics, and also with third-party analytics and AI models. This allows security integrators to create custom solutions that leverage Open V4 using the built-in APIs, an SDK, and other tools to make the model work with any camera, AI model or analytics software package.

Vaelsys has created several complete solutions that add workload-specific functionality to the Open V4 foundation for a targeted application. One example is DeepWall which delivers perimeter security functionality. Figure 1 shows how DeepWall works using an Intel® Core™ Ultra processor-based small form factor server.

Metro AI Suite Enables AI Solutions at the Edge

Vaelsys has developed Open V4 using the Metro AI Suite, part of the Intel Edge AI Portfolio, which provides an application framework with libraries, tools, and reference implementations to help organizations build AI solutions for mission-critical safety, security, transportation, and smart infrastructure use cases at the edge.

Within this framework, Vaelsys leverages the OpenVINO® toolkit to optimize and accelerate AI inference on Intel® processors. In Open V4, the OpenVINO toolkit enables efficient hybrid workload execution across the CPU, GPU, and neural processing unit (NPU)— the dedicated integrated AI accelerator in Intel Core Ultra processors— and supports low-latency, cost-efficient inference without the need for discrete GPUs.

As part of the Open V4 visual AI pipeline, Vaelsys integrates with Deep Learning Streamer (DL Streamer) for video decoding and media stream processing. DL Streamer is a streaming media analytics framework built on GStreamer and included in the OpenVINO toolkit. In Open V4, DL Streamer handles efficient ingestion and preprocessing of video streams, enabling OpenVINO toolkit optimized inference to be applied within Vaelsys' real time perimeter security analytics pipeline across Intel® CPU, GPU, and NPU resources.

Figure 1. This image shows a DeepWall perimeter protection application.

Open V4's Growing Ecosystem

In addition to DeepWall, Vaelsys has a growing ecosystem of Open V4-based solutions that address different applications. Open V4 offers both APIs and an SDK that integrators can use to add their own analytics. Vaelsys also has developed customized solutions for a wide range of industries, including:

- Drone detection for airports
- Bird detection for wind farms and airports
- Manufacturing computer vision for product quality, employee safety, and equipment monitoring
- Retail computer vision for customer behavior analytics
- Logistics computer vision for operational efficiency
- Transport computer vision for optimizing public and private transportation
- Overhead crane safety zone management
- License plate recognition using contextual camera
- Personal protection equipment for employee safety
- EV charging station protection

In most cases, the ecosystem solution adds intelligence to existing camera installations extending the hardware investment already made.

More Performance with Intel Core Ultra Processors

To highlight solution optimization and deployment, Vaelsys developed and optimized its DeepWall AI-powered perimeter security solution on the Open V4 platform, running on a server powered by an Intel® Core™ Ultra X7 processor 368H (see Figure 2). DeepWall's analytics support real-time perimeter intrusion detection, unauthorized access monitoring, and continuous tracking of individuals across sensitive zones.

Figure 2. Vaelsys server powered by Intel® Core™ Ultra processors.

In optimizing its solution, Vaelsys updated and tuned the Open V4 and DeepWall software to make the models more powerful so they can take advantage of the Intel® Core™ Ultra Series 3 platform[i]. The result is improved detection accuracy and system efficiency (see Figure 3). As implemented on the System under Test (SUT) based on the Intel Core Ultra X7 processor 368H ("Series 3 SUT"), DeepWall reduced false alarms by up to 40% compared to the SUT based on the Intel®

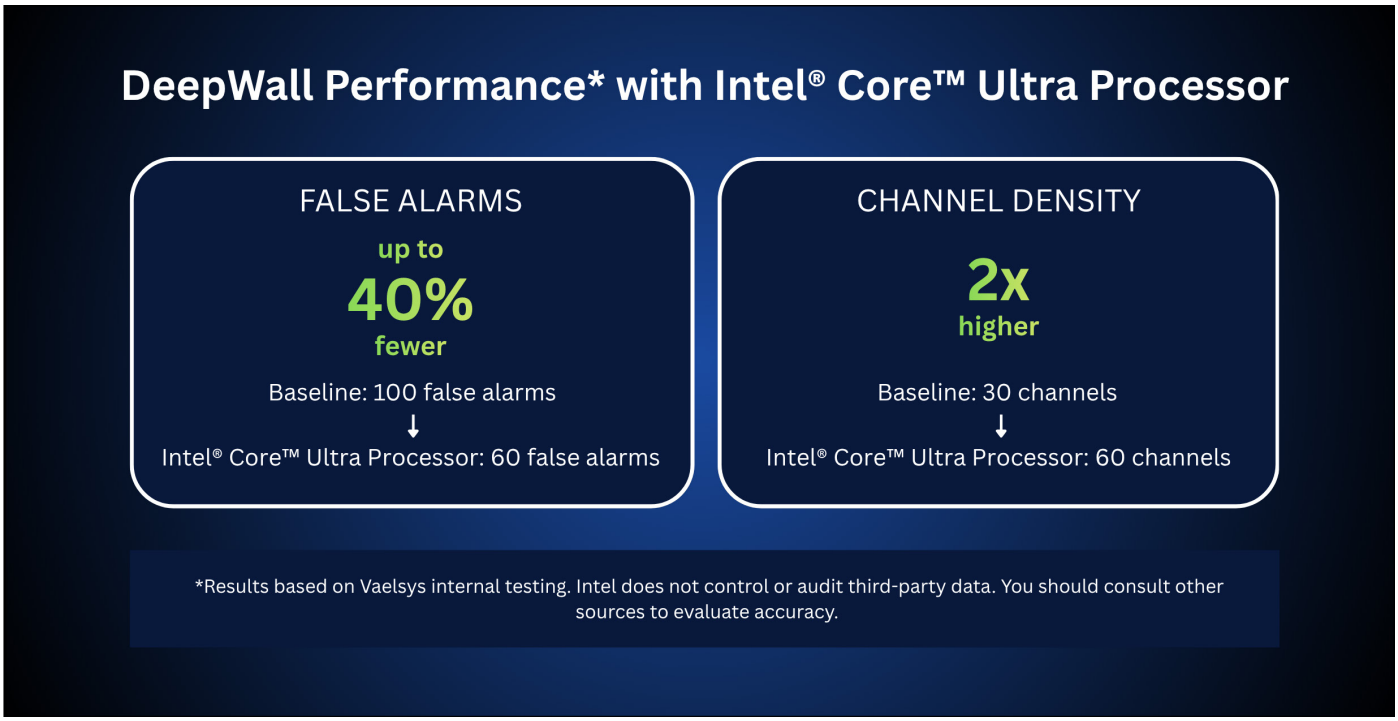

Figure 3. When powered by Intel Core Ultra processor, Open V4 shows significant performance improvements in both detection accuracy and camera stream density.

Test Criteria	Performance
Median number of alarms per thermal spectrum camera per day. (Using a thermal camera with 25mm sensor with 384x288 resolution and 12um)	Series 3 SUT Between 0.1 and 0.3 alarms at a range of 284m Series 2 SUT Between 0.2 and 0.4 alarms at a range of 241m
Maximum distance using thermal spectrum camera (Using a thermal camera with 60mm sensors, 384x288 resolution and 17um)	529 meters

Figure 4. Results from a test of DeepWall using Series 2 SUT and Series 3 SUT with both HD and thermal cameras. Data from both of these systems was sent to a video management system (VMS).

Core™ Ultra 5 processor 225H ("Series 2 SUT"), improving event reliability and reducing unnecessary operator intervention, under a real time perimeter security analytics workload using multi camera video streams and rule based detection.[1]

The testing also showed that when Vaelsys updated its software to take advantage of the Intel technology video channel density doubled enabling the system to process up to 60 camera streams on a single compact edge server without discrete GPUs.[1] The increased channel density allows customers to consolidate hardware, reduce infrastructure footprint and energy consumption, and significantly lower total cost of ownership while maintaining real-time performance and detection accuracy across industrial, retail, and critical infrastructure deployments.

Effective at Long Distances

Vaelsys also optimized DeepWall to improve detection accuracy at long distances by updating its analytics to use a larger, higher-fidelity model designed for extended-range perimeter detection.

[1]Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy. See backup for workloads and configurations. Results may vary.

As part of this optimization, Vaelsys evaluated DeepWall at a maximum surveillance distance of up to 529 meters. The company also compared the number of alarms per day at various distances to show the performance of the Open V4 model. Figure 4 shows that the Series 3 SUT recorded a median of between 0.01 and 0.03 alarms per camera at 284 meters. These results mean a typical 100-camera installation would generate between 10 and 30 alarms per day.

The Series 2 SUT's performance was between 0.2 and 0.4 alarms at 241 meters. The increase in accuracy and range is enabled by the increased AI processing capability available in Intel Core Ultra processors and supported by the Metro AI Suite framework. Together, these technologies allow more demanding models to run efficiently at the edge.

Based on these results, moving to an Intel Core Ultra processor-based platform with the latest Vaelsys model would deliver a median decrease in alarms of 40%.[1]

The tests show that Vaelsys is able to both run a more powerful model and process more simultaneous streams due to the performance of the Intel® Core™ Ultra X7 processor 368H.

In real-world applications, this performance translates into fewer nuisance alerts for security teams, faster response to genuine threats, lower operational workload, and improved trust in automated perimeter detection.

Conclusion

Intelligent cameras and AI-enhanced analytics are becoming essential physical security infrastructure for critical facilities of all kinds. Vaelsys, working with Intel, is helping organizations move from passive surveillance to more intelligent, cost effective security operations.

This intelligence delivers the ability to detect bad actors and send alerts in real-time. By enabling more accurate detection, fewer false alarms, and higher camera density on compact edge systems, organizations can achieve stronger security outcomes while reducing hardware, energy, and operational costs. Vaelsys' Open V4 system brings this intelligence to a surveillance network offering advanced analytics and an ability to customize these analytics for different applications. Powered by Intel Core Ultra processors and Metro AI Suite, Open V4 delivers a scalable, high-performance foundation that allows customers to deploy more effective security with lower total cost of ownership (TCO) across a wide range of security environments.

Learn More

Vaelsys Website – Perimeter Analytics Overview

Open V4 Home Page

DeepWall – Perimeter Protection Solution

Intel® Core™ Ultra Series 3 Processors

Metro AI Suite

OpenVINO™ Toolkit

Deep Learning Streamer (DL Streamer)

Trusted Platform Module (TPM 2.0)

Intel® Industry Solution Builders

[i] Series 3 SUT: Using Intel® Cloud Based Remote Debug (Intel® CBRD) infrastructure, Vaelsys accessed and provisioned a single node, single socket Intel® Core™ Ultra X7 processor 368H with 16 cores. Total DDR memory was 16 GB (2 slots/ 8GB). Software: OS was Ubuntu 24.04; kernel was 6.7.11. Workload software: SafeGear (13.3.0). Test conducted by Vaelsys in January 2026.

Series 2 SUT: Using Intel® Cloud Based Remote Debug (Intel® CBRD) infrastructure, Vaelsys accessed and provisioned a single node, single socket Intel® Core™ Ultra 5 processor 225H with 16 cores. Total DDR memory was 16 GB (2 slots/ 8GB). Software: OS was Ubuntu 24.04; kernel was 6.7.0. Workload software: SafeGear (13.3.0). Test conducted by Vaelsys in January 2026.

Notices & Disclaimers

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See configuration disclosure for details. No product or component can be absolutely secure.

Intel optimizations, for Intel compilers or other products, may not optimize to the same degree for non-Intel products.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

See our complete legal Notices and Disclaimers.

Intel is committed to respecting human rights and avoiding causing or contributing to adverse impacts on human rights. See Intel's Global Human Rights Principles. Intel's products and software are intended only to be used in applications that do not cause or contribute to adverse impacts on human rights.

0326/CG/DJA/PDF Please Recycle 368570-001US