NEXCOM

Committed to Customer Success

Solution Brief

AI Integration for Enhanced Private Network Protection

DNA 140 is designed for intelligent security applications

The Trend

Building a private network allows companies greater flexibility and implementation of enhanced cybersecurity, ensuring corporate digital domains remain invulnerable. A significant trend in cybersecurity is the utilization of AI against cyberattacks. While hackers innovate new techniques to breach private networks and steal valuable assets, IT teams leverage AI's power to construct robust digital security walls.

AI systems are adept at identifying and classifying sensitive information, inspecting packets and patterns, monitoring data flows across the network, detecting anomalies, and responding to potential threats. By implementing AI in cybersecurity, critical information can be safeguarded with less IT/OT staff intervention.

Data encryption and decryption is inevitably needed during transmission across the network, but to strike a balance between crypto and computing performance is an art in itself. By incorporating the latest software-driven crypto acceleration techniques, private network sites can protect sensitive data, ensuring that proprietary information and operational data remain secure against potential breaches without hindering manufacturing operations.

In addition, OS's resilience to faults in operations or upgrades and/or booting is crucial for the entire network infrastructure, especially in the manufacturing framework, where prevention of downtime is the top priority of the facilities.

The Challenge

However, implementing sound cybersecurity measures in private networks is not easy. It involves integrating sophisticated technologies and policies across different protocols and resources.

In manufacturing settings, data such as operational metrics, machine performance logs, and real-time sensor readings must be constantly monitored. This data comes in various formats from multiple sources, including IoT devices, industrial control systems, and enterprise resource planning software.

Seamless connection and integration of IT/OT infrastructure with data efficiently collected, transported and cleansing is critical for enabling a smart factory, and even more so when AI training models and business intelligent applications are called upon to assist decision making.

Another challenge is the tradeoff between security measures and operational efficiency, especially in environments like smart manufacturing where uptime and performance are crucial. The implementation of software-driven crypto acceleration techniques must be optimized to ensure there is no latency or bottlenecks in the network.

NEXCOM Solution

NEXCOM's DNA 140 is a compact AI-in-a-Box network appliance, built on the newest Intel Atom® x7433RE processor (Codenamed Amston Lake) optimized for Edge computing and software-defined network. It unlocks smarter cloud-based security services, ensuring consistent policy enforcement and access control across users, devices, applications, and IoT.

DNA 140 features four 2.5GbE LAN ports to fulfill the demand for multi-media or

DNA 140 enables AI inferencing for cybersecurity IoT applications

small-to-mid business data transmission. Two ports feature PoE+ capability with up to 30W (802.3at) per port, significantly simplifying the installation and management of connected devices. By delivering both power and data over a single Ethernet cable, DNA 140 enhances flexibility, allowing devices like sensors, cameras, and access points to be easily relocated without requiring additional power source, improving overall energy efficiency and reliability in manufacturing environments.

In cybersecurity, the DNA 140, driven by Intel® technologies, including Intel® AES New Instructions, Intel® OS Guard, Intel® Boot Guard, Intel® Virtualization Technology (VT-x), Intel® Virtualization Technology for Directed I/O (VT-d), and more, to deliver advanced technology and processing capabilities for outstanding connectivity, performance, and high availability.

Intel Atom® x7433RE features software-driven Intel® QuickAssist Technology (Intel® QAT) that offers greater flexibility compared to hardware-based Intel® QAT in legacy processors. It can be easily updated, configured, and scaled according to the specific needs of the network or application without requiring physical changes to the hardware: security patches, performance enhancements, and new features can be rolled out promptly through software updates.

NEXBOOT is NEXCOM's proprietary failover mechanism with additional capabilities for OS rotation (Round Robin), OS recovery, and hardware/software diagnostics. OS failover is implemented using separate physical storage locations, including onboard eMMC and M.2 storage. DNA 140 offers two modes to choose from: **Dynamic Mode**, which dynamically switches to the Golden OS when the Primary OS fails, and **Force Mode**, which forcefully reboots to the Golden OS using a latch switch for recovery or diagnostics.

Enabling the **NEXBOOT** function on DNA 140 allows uninterrupted services and prevents downtime, establishing a secure foundation for operations. This value-added feature enhances the overall stability of private networks in factory settings, where accessing physical devices can be challenging, and ensures a resilient and trustworthy operational environment.

In terms of memory DNA 140 leverages a single DDR5 4800 slot, enhancing performance and efficiency. In addition, multiple expansion slots are reserved for dual 5G and single Wi-Fi modules to bring additional wireless routes for mass IoT connectivity, and a slot for AI card for better fit into smart environments.

AI Integration

DNA 140 adopts a power-efficient Hailo-8 edge AI processor through a mini-PCIe slot to enable real-time, low latency, and high-efficiency AI inferencing at the Edge. To prove AI performance on DNA 140, NEXCOM runs a few versions of YOLO (You Only Look Once) computer vision models. YOLO uses PyTorch for object detection and operates at a higher inference speed, making it effective for real-time applications. YOLO acts as a good object detector to detect small objects. It is one of the fastest models among similar models and is particularly well-suited for cybersecurity IoT applications in manufacturing settings, where rapid and precise detection is crucial. Detailed test configuration is shown in TABLE I.

DNA 140 is suitable for visual data processing and analysis

TABLE I
DNA 140 TEST CONFIGURATION

Item	DNA 140
CPU	Intel Atom® x7425RE, 4 cores
Memory	1 x 16GB DDR5 4800 SODIMM
SSD	1 x 64GB SATA III M.2 SSD
Storage	eMMC 32GB onboard
Extension	1 x Hailo-8R (in internal mPCIe slot)
Ubuntu	23.04
Kernel	6.2

YOLO model offers different versions tailored to different operational needs, and offers different level of detection speed, accuracy, and resource requirements, making them adaptable to different cybersecurity AI applications. NEXCOM has tested four YOLO versions on DNA 140:

- **YOLOv5s:** Best for speed and low-resource environments.
- **YOLOv5m:** Balances speed and accuracy, suitable for moderate resources.
- **YOLOv7_tiny:** Optimized for ultra-fast performance with minimal resources.
- **YOLOv7:** Highest accuracy, designed for more powerful systems.

Test results are shown in TABLE II in FPS (frames per second). With a higher FPS, the AI system can quickly identify and respond to potential threats or anomalies, minimizing the risk of missed detections and ensuring continuous, effective monitoring. Additionally, higher FPS reduces latency, enabling quicker responses to detected events, which is vital in maintaining the security and operational efficiency of the system.

For basic object detection tasks, an FPS of around 15-30 is considered the minimum, as it allows for reasonable accuracy in capturing movement and changes in the scene. For more demanding applications, such as real-time security monitoring or smart manufacturing, higher FPS—60 FPS or more—is preferred to ensure that fast-moving objects are accurately detected without motion blur or lag.

With its high frame rate (189.89 FPS), **YOLOv5s** is ideal for continuously monitoring entry points and restricted areas in a smart factory. It can detect unauthorized personnel or vehicles in real-time, instantly alerting security teams. This rapid response is crucial for maintaining the security of sensitive production areas. **Perfect for: Real-Time Object Detection**.

TABLE II
DNA 140 YOLO MODEL TEST RESULTS

Model	Resolution	DNA 140, FPS
YOLOv5s.hef	640 x 640	189.89
YOLOv5m.hef		78.47
YOLOv7_tiny.hef		186.68
YOLOv7.hef		19.17

DNA 140 proved its flexibility and adaptability to smart threat detection

With its lower frame rate (78.47 FPS), **YOLOv5m** is suitable detecting changes or anomalies in equipment behavior or positioning, which might indicate a cybersecurity threat, such as tampering, an attempt to alter machine settings remotely or introduce malware via compromised devices. **Perfect for: Equipment Tampering and Anomaly Detection**.

YOLOv7_tiny's high FPS (186.68 FPS) and lightweight design make it ideal for managing large-scale IoT environments in a smart factory. It can rapidly process data from numerous IoT devices, identifying any unusual patterns or unauthorized device connections. **Perfect for: Mass IoT Device Surveillance**.

YOLOv7, with its slowest result (19.17 FPS), is suitable for in-depth analysis of complex behaviors or detailed monitoring tasks. It can be used to detect advanced persistent threats (APTs) that require careful observation over time. **Perfect for: Detailed Threat Analysis and Complex Behavior Detection**.

Achieved test results proves DNA 140's ability to seamlessly integrate into various cybersecurity applications as a universal Edge device for addressing specific cybersecurity needs based on the factory's requirements. DNA 140 as an entry level desktop fits the best for low-resource cybersecurity tasks, such as object detection, access control, and IoT-related applications.

Conclusion

As the cybersecurity landscape evolves, the ongoing development and integration of AI and software-driven technologies will be pivotal in maintaining robust defenses and supporting the secure growth of smart environments. However, the complexity of implementing and managing these systems requires a strategic approach, balancing performance with security and ensuring comprehensive real-time coverage.

NEXCOM's DNA 140 deployed in private networks helps to keep digital domains secure and resilient. Its advanced AI extension capabilities offer flexibility and adaptability to smart threat detection in cybersecurity applications. Feature-rich design makes it ideal for businesses looking to integrate AI into 5G, SD-WAN, SASE, and other security applications.

DNA 140 shows exceptional performance across a variety of cybersecurity tasks, particularly those involving visual data processing and analysis, real-time monitoring, and object detection. Despite its positioning as an entry-level cybersecurity desktop, the tests have confirmed that the DNA 140 offers sufficient AI capabilities to enhance the overall security and resilience of private networks in diverse and dynamic environments.

Committed to Customer Success

NEXCOM, founded in 1992 and headquartered in Taiwan, stands as a distinguished global leader in edge computing and industrial IoT solutions. Demonstrating an unwavering commitment to excellence, NEXCOM provides integrated services encompassing SD-Edge Computing (software-defined edge computing) and cutting-edge MOM (manufacturing operations management) platforms. Its comprehensive solutions include network and communication, mobile computing, video surveillance, smart city and retail, digital healthcare, AIoT services, OT cybersecurity, industrial IoT and industrial robots—all developed based on open standards. As a trailblazer in the industry, NEXCOM continues to set the standard for innovation and reliability, meeting the diverse needs of its global clientele with precision and sophistication.

www.nexcom.com

intel partner Titanium

NEXCOM is a Titanium member of the Intel® Partner Alliance, as a top tier of the Alliance. Intel and more than 500 global IoT partners of the Intel® Partner Alliance provide scalable, interoperable Intel® -based technologies and 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 firstin-market solutions.

Learn more at: https://www.intel.com/content/www/us/en/partner-alliance/overview.html

Intel and Atom are registered trademarks of Intel Corporation in the United States and other countries.