Embedded Intel® Solutions

Fall 2018

AI Power Tool

Tackling Sophisticated Cyberattacks

Digital Signs Evolve to Energize Engagement

www.embeddedinteln.com

Gold Sponsors
Unparalleled processing power. Rugged and secure.

Embedded Intel® single board computers designed, tested, manufactured, and supported in the USA for use in the most extreme environments on Earth.
conga-TC175
Low consumption COM Express Compact

Technology for brilliant imaging
- 7th Generation Intel® Core™ SOC processor
- Intel® Gen9 HD Graphics with HEVC support
- Intel® Optane™ memory
- Low consumption for passive cooling

Embedded in your Success.
Supermicro celebrates 25 years of industry leading growth and Green Computing innovation by delivering highest quality, First-To-Market server and storage technologies. These resource-saving computing offerings can help us to preserve our precious Earth for an even brighter future.
FROM THE EDITOR

A More Convenient World

More options for sharing experiences at events, faster shopping, and eliminating steps at check out

By Lynnette Reese, Editor-in-Chief, Embedded Intel® Solutions

Amazon, an online behemoth, is making it increasingly difficult for brick-and-mortar stores to compete. Shopping online has 24/7 convenience, makes comparing products easy, and saves your shopping cart forever. Customers expect online stores to track their preferences and personalize the shopping experience with suggestions based on past choices. The same kind of personalization is difficult for traditional stores. However, with smart digital signage, smartphone apps, and a little creativity, traditional stores are working to customize the shopping experience, too.

A few years ago, I put a store app called Cartwheel on my smartphone. It saved me money, time, and made shopping more informative. I could check a price using my smartphone as a barcode reader. I could mark e-coupons anytime, which the app collected. Later, the cashier scanned a single barcode on my phone that applied all the coupons; no scissors required.

Digital signage can make shopping more informative and convenient for shoppers in brick-and-mortar stores. Personalizing the shopping experience can be a good thing for customers, saving them money, time, and frustration. For retailers, information from digital signs on how long people linger in front of a display can translate into products that better fit the demographic local to the store. Smart digital signage means less wait time at a restaurant. Table-top payment kiosks in restaurants mean that customers don’t have to wait for the check; it’s on the touch-pad kiosk. Customers can close their ticket, securely swipe their credit card in the kiosk, and leave a busy restaurant without wait staff ever handling their credit card.

Remember Pokémon Go? Augmented reality apps can assist customers in finding an item. A customer can find the correct aisle for a specific item by searching for it on her phone. When she reaches the right aisle, she can hold up her smartphone, and a digital overlay identifies the area or bin with the item. Digital signage can save time for customers and store labor costs.

Stadium games are more fun with digital signage. You can leave the game to get snacks or go to the restroom without missing a play since large displays feed the live action along the way. Moderated, scrolling twitter feeds allow fans to contribute to the social experience with commentary. Voting by smartphone enables concertgoers to influence the encore song. Processors all around us fuel engagement, create convenience, and offer a richer experience.

Lynnette Reese is Editor-in-Chief, Embedded Intel® Solutions and Embedded Systems Engineering, and has been working in various roles as an electrical engineer for over two decades. She is interested in open source software and hardware, the maker movement, and in increasing the number of women working in STEM so she has a greater chance of talking about something other than football at the water cooler.
Embed Security in Every Application

We live on the sensory edge of what’s happening, where the flood of critical data originates. Leveraging security advances in the latest generation of Intel® Atom® processors, WinSystems’ line of Intel-powered embedded computer systems are designed to safely and reliably acquire and facilitate the flow of essential data. Our resilient single board computers can process a vast array of data to support application solutions for the ever-expanding world of industrial IoT.

From standard components to full custom solutions, WinSystems delivers world-class engineering, quality and unrivaled technical support. Our full line of embedded computers, I/O cards, and accessories help you design smarter projects offering faster time to market, improved reliability, durability, and longer product life cycles.

EBC-C413
EBX-compatible SBC with latest generation Intel® Atom™ E3800 Series Processor

EPX-C414
EPIC-compatible SBC with latest generation Intel® Atom™ E3800 Series Processor

PX1-C415
PC/104 Form Factor SBC with PCIe/104™ OneBank™ expansion and latest generation Intel® Atom™ E3900 Series processor
A More Convenient World  
By Lynnette Reese, Editor-in-Chief, Embedded Intel® Solutions

Comparing Hardware for Artificial Intelligence: FPGAs vs. GPUs vs. ASICs  
By Lynnette Reese, Editor-in-Chief, Embedded Intel® Solutions

“Zero Touch” IoT Security Is Key to Continued Growth  
By John Blyler, Senior Editor

Tackling Sophisticated Cyberattacks Head On  
By Qizhi Zhang, ADLINK Technology

Take a Look at the New-Look Signage  
By Caroline Hayes, Senior Editor

Trends in Digital Signage: Interview with Intel’s Jose Avalos  
By Lynnette Reese, Editor-in-Chief, Embedded Intel® Solutions

Intel’s New Tool for Programming FPGAs…for Artificial Intelligence  
By Lynnette Reese, Editor-in-Chief, Embedded Intel® Solutions

On the Cover:  
Accelerate AI inference. The OpenVINO tool optimizes a DNN model (TensorFlow or Caffe) for running on an Intel CPU, GPU, Movidius, or FPGA. The single-shot command line utility can also convert the model from any Intel AI-suitable platform to another, enabling quick experimentation among platforms. And it’s free.  
Page 23
Empowering the Connected World

Boosting IoT Designs from Edge to Cloud

- Scalable module, IoT gateway, network appliance
- Energy-efficient embedded solution
- Industrial operating temperature
- Extended product longevity
- High reliability

Enable Your Design Today
www.portwell.com
info@portwell.com
1-877-278-8899

Portwell
ISO 9001, ISO 13485, ISO 14001, TL 9000

Intel IoT Solutions Alliance
Comparing Hardware for Artificial Intelligence: FPGAs vs. GPUs vs. ASICs

Compare the general pros and cons of hardware commonly used for AI applications. FPGAs are looking good: a free command-line tool makes FPGAs that much easier to work with and dramatically lowers the size of an inference model, all in one go.

By Lynnette Reese, Editor-in-Chief, Embedded Intel® Solutions

The Artificial Intelligence (AI) deep learning chipset market will reach $66.3 billion by 2025¹. Although Graphics Processing Units (GPUs) and Central Processing Units (CPUs) lead in AI sockets today, Application Specific Integrated Chips (ASICs), Field Programmable Gate Arrays (FPGAs), and System-on-Chip (SoC) accelerators are also part of the expanding AI hardware market. Deep Neural Networks (DNNs), a special subset of machine learning, are all about completing repetitive math algorithms or functions on a massive scale at blazing speeds. Hardware accelerators like CPUs, GPUs, ASICs, FPGAs, and even SoCs have various advantages and design trade-offs.

Latency Comparison
FPGAs offer lower latency than GPUs or CPUs. All else being equal, FPGAs and ASICs are faster than GPUs and CPUs because they run on "bare metal," as the saying goes; there is no Operating System (OS). Both logic transistors and software programs can complete instructions. ASICs and FPGAs can provide lower latencies, which is better for applications that require real-time AI.

Panch Chandrasekaran, FPGA Marketing Director, Programmable Solutions Group at Intel®, places an emphasis on latency, where FPGAs outperform GPUs. "For applications that require real-time performance, like streaming video object detection and identification, for example, latency matters. For example, if an application has to perform image classification in an automotive setting, or if there’s a large venue where stress profiling is the goal, latency can be critical. For real-time, low latency requirements, FPGAs are the more suitable strategy. GPUs, being software in nature, can accommodate changes, but when the application is also performance-, power-, and latency-critical, FPGAs really shine versus GPUs.”

Power Comparison
Another area where FPGAs outperform GPUs (and CPUs) is for those applications with a constrained power envelope. It takes less to run on bare metal.

Flexibility: FPGAs vs. ASICs
FPGAs are similar to ASICs except that FPGAs are notoriously difficult to program and ASICs have a typical production cycle time of 12 – 18 months. Changing a design on an ASIC takes much longer, whereas a design change on an FPGA requires reprogramming that can take anywhere from several hours to several weeks. FPGAs have been steadily growing more competitive with ASICs on price, as well.

FPGAs are superior in terms of flexibility and proving especially useful in rapidly growing and changing AI applications. Neural networks can improve significantly over the course of months. For instance, their architectures, also referred to as topologies, can undergo changes. As more and/or different data comes in, companies want the ability to retrain or tune neural nets as their applications develop. For cases requiring maximum flexibility, or where neural networks are still evolving, FPGAs make sense.
Tony Kau, Marketing Director, Artificial Intelligence, Software and IP solutions at Intel, states, “So much is changing in the wildly evolving space of AI. There are many hundreds of existing topologies for various industries and use cases and the [AI] industry is constantly adding new ones. The neural networks vary in precision from 32-bit to binary. And FPGAs can accommodate all of that.”

Kau goes on to add, “To give an idea of how fast AI is evolving, consider that the original GoogleNet and ResNet versions were created back in 2015. There were some follow-on versions of both networks, but these topologies are now considered “old” and almost “classical.” We currently have 150+ different topologies in our benchmark. FPGAs allow data centers to process workloads on a hyper-scale for real-time AI. For example, a system of FPGAs can run 8 billion calculations that are required for ResNet 50 (an industry-standard DNN) without having to batch or queue loads.”

**Parallel Computing**

DNNs can employ parallel computing on a massive scale. But parallel computing has introduced execution complexities as programs running through one of several pipelines must be coordinated across cores. Computational hardware imbalances can occur if irregular parallelisms evolve. FPGAs are also better than GPUs wherever custom data types exist or irregular parallelism tends to develop.

Both GPUs and FPGAs can process in parallel on a massive scale. However, FPGAs also surpass GPUs for efficiency in parallel processing. Using the analogy of a bottling factory, we can compare FPGAs and GPUs on the concept of parallelism. Imagine that a soda bottling factory has a three-step process of filling up a bottle, capping it, and then labeling it. You could do one bottle at a time in a long series, but to dramatically expand capacity you would process rows of several bottles, in parallel. CPUs, GPUs, FPGAs and ASICs are all able to process in parallel on a massive scale (some better than others).

The bottle factory as run by a GPU might fill a row of one hundred million bottles every clock cycle. Then the whole row would get capped, then labelled, before the next massive row of bottles is advanced to be filled, capped, and labelled. An FPGA would also process in parallel on a massive scale, but several steps are performed at each cycle. The FPGA does not waste bandwidth in its one hundred million-wide (108) pipeline of bottles. By the time the first row of 108 bottles is getting labeled, the second row of 108 bottles is being capped, and the third row in the FPGA bottling factory is filling bottles at the same time. The 108-wide FPGA pipeline is fully utilized. GPUs can only do one row at a time before moving on to the next row of bottles to perform the same set of repetitive operations. Yes, both FPGAs and GPUs can operate in parallel on a massive scale, but FPGAs are inherently more efficient (with a full pipeline), faster (running an algorithm on bare metal), and are more flexible than GPUs in terms of architecture and programming changes.

**Flexibility: FPGAs vs. GPUs**

FPGAs can be programmed to add different steps or outputs altogether, allowing growth beyond existing GPU support without physically changing the way the GPUs are architected. If the bottles need to be cleaned before they are filled, the FPGA can be programmed to add that step. FPGAs go even further in flexibility, however. Assume that the owner of the bottling factory wants to make bicycles as well. The factory running on the FPGA needs to be re-programmed to add bicycle-making steps, and it can be running within hours or weeks, depending on the complexity of the bicycle. The GPU-run factory would need additional GPUs as well as programming. The ASIC-run factory would not be able to add bicycles to the manufacturing line for 12 - 18 months but would require little programming upon release.

---

As Kau points out, “FPGAs are massively programmable in a way that enables different outputs. And with GPUs you can only do one thing at a time. That is why there have been talks within the industry that a GPU is great for looking at training data or unstructured data. But once the data is trained, the GPU goes through a very deterministic inference model, and this is where the FPGA brings tremendous value.” The inference model is the resulting model from all that training and what AI uses to make decisions once it’s up and running.

One the most important features of the OpenVINO toolkit is a “model zoo,” which contains public and free optimized models. One can use these models for rapid prototyping as well as to expedite development and production of applications without having to search for or train your own models.

Conclusion
AI opens an untapped frontier for technology to solve problems, provide extreme productivity boosts, entertain us, and so much more. As AI rapidly grows and changes, FPGAs offer flexibility, performance, and extensibility in comparison to other accelerators. Although historically complex to program, FPGAs are carving out their own space in AI technology, with new tools that make programming AI applications that much easier.

Lynnette Reese is Editor-in-Chief, Embedded Intel® Solutions and Embedded Systems Engineering, and has been working in various roles as an electrical engineer for over two decades. She is interested in open source software and hardware, the maker movement, and in increasing the number of women working in STEM so she has a greater chance of talking about something other than football at the water cooler.
By now it’s clear that the IoT will miss the much-touted target of 50B connected devices by 2020. The problem? Security.

IT managers are so worried about security issues that they are requiring manual provisioning of IoT devices. This is leading to a slowdown in installation that cuts into revenues for OEMs, ODMs, and cloud platform providers.

The solution lies in IoT Identity Access Management (IAM). IoT IAM has become so important that MarketsandMarkets predicts the market will grow from $1.1B in 2016 to $4.97B by 2021.

In this article, we will explore:

- How IoT device deployments differ from IT approaches
- Why slow device provisioning decreases revenue
- How a new “Zero Touch” onboarding platform satisfies IT while meeting IoT requirements

Scalability or Security

Early IoT devices relied on self-discovery when installed on a network. This approach was easy for installers but gave IT departments headaches. No IT professional likes to see unsecured devices appear on the network without warning.

IT departments responded by forcing operations departments to secure each device before bringing it online. This improved security of the devices but put the brakes on rapid deployment of IoT systems.

To ensure each IoT device was secure, IT departments have explored a number of solutions—all with serious drawbacks. One option was to stage all IoT devices with uniform images, so that all devices used a known configuration. While this solution works great for generic PCs, it doesn’t work well for the highly diverse world of IoT devices.

The second approach was to have the operations person contact IT for a unique key for each IoT device. This manual provisioning was extremely error-prone and time-consuming—often taking an hour per device (Figure 1).

The third solution was to encourage IoT device OEMs and ODMs to pre-configure their IoT devices for specific cloud platform providers. This way, the provisioning burden could be outsourced to cloud providers.

The problem is that there are many cloud providers, including Amazon, Microsoft, IBM, and Honeywell, to name a few. Thus, this approach placed a heavy burden on OEMs/ODMs, which now had to validate, document, and track a unique SKU for each cloud platform.

Motivations: Lost Revenue and Data Protection

Slow rollout of IoT devices means lost revenue for the entire IoT ecosystem.

That includes cloud platform providers. “If the IoT devices aren’t getting onboarded, then their monetization is suffering,” explains Jen Gilburg, senior director of IoT security at Intel’s Internet of Things Group (IoTG). “[That’s true] regardless of whether the platform providers monetize on the volume of data or the number of devices under their management.”

For OEMs and ODMs, the problem is unpredictable sales. Gilburg illustrates the point with a typical scenario: Suppose...
a customer requests 100,000 devices. The OEM/ODM gears up for production, but after the first 5,000 devices are delivered, the remainder of the order is delayed due to the slowdown imposed by security concerns. This can throw production schedules into chaos.

**Ecosystem-Based Solution**
Since the original problem was that the IoT deployment model was different from IT models, it makes sense that a new solution is needed – one that combines greater scalability with automated security.

Enter Intel® Secure Device Onboard (Intel® SDO). This onboarding service is designed for rapid, platform-neutral provisioning, and offers:

- Zero-touch onboarding with automatic discovery and provisioning
- Only seconds to run at power-on
- Password-free authentication with Intel® Enhanced Privacy ID (Intel® EPID)
- Ability to support multiple cloud platforms with a single SKU
- Digital ownership traceability from manufacturer to customer

With this new platform, OEMs and ODMs need create only a single image for their devices. Then the device will become fully provisioned on initial power-up by the installer and ready for handoff to a back-end platform provider for operation (Figure 2).

Here’s how the platform works:

- **Silicon Provider** – Embeds an Intel EPID identity in the silicon’s trusted execution environment (TEE) at manufacturing, using an Intel EPID 2.0 open source SDK.
- **Gateway/Device Manufacturer** – Uses a toolkit to insert client software into boot code to support a direct anonymous attestation communication channel to the IoT platform, which passes the device GUID, Intel SDO service URL, and digital ownership credential.
- **Device Owner** – After the distribution change of ownership, the final owner can automatically load its digital ownership receipt into the IoT Platform.
- **IoT Platform** – Uses an API to enable the platform or VM marketplace containers to register the device to the owner’s account and enable rendezvous protocols that share the destination IP address.
- **Device Activation** – The powered-on device contacts the Intel SDO service to prove authenticity, and it receives the URL where it meets the new owner for provisioning.

To create the platform, Intel worked with numerous silicon, equipment, and platform providers (Figure 3). The first equipment to support the platform is expected to come from members of the Intel® Internet of Things Solutions Alliance such as Nexcom.

![Figure 2: Intel® Secure Device Onboard (Intel® SDO) streamlines provisioning.](image-url)
Further, Intel is working with the Open Connectivity Foundation (OCF), the IoTivity project, and other IoT standards organizations to contribute concepts and toolkits based on their real-world experiences with onboarding devices.

In addition to security, the global ecosystem-based approach must also adhere to privacy concerns. For anyone dealing with the European Union, this means adhering to the upcoming General Data Protection Regulation (GDPR). This regulation requires that any company collecting any type of data must ensure its protection and security.

That’s one reason Intel SDO uses Intel EPID. This authentication method allows devices to access a system based on their approved level of access and not any identity information like a MACID. In other words, if 100 authentic signatures are verified, the verifier would not be able to determine whether 100 devices were authenticated, or if the same device was authenticated 100 times.

Traditional digital certification and authentication techniques like public key infrastructure (PKI) cannot remain anonymous while granting access (Figure 4). A given public certificate contains the key owner’s name and information, thus making the ownership of the secured information known. If the same device is verified multiple times, its activity could be tracked, which would allow hackers to create a threat map from which denial-of-service attacks could be launched – among other things.

Intel EPID, on the other hand, collects no such identity data. Aside from dissuading hackers, the lack of identity data means Intel EPID is not affected by the GDPR initiative.

“As the industry moves to address the privacy of data with regulations like the GDPR, Intel EPID will gain a lot of additional use cases,” says Gilburg. “It will then become more of an industry standard beyond just Intel and our partners.”

From Fab to End Product Provisioning
To see how this all fits together, consider the scenario illustrated in Figure 5. The Intel EPID identity is burned into the trusted execution environment during chip fabrication.

The chips then go to the OEM/ODM, which stores a unique identifier known as a GUID and a public key in its board. The public key contains the chain of signatures that establishes device ownership.

Once the board is built into a product (say, a smart light bulb with GUID 123), it ships through various channels, eventually reaching the end customer. At each step, the signature chain grows.
Finally, the IoT device is installed. At this point, Intel SDO provides a broker service – really just a rendezvous point that is typically a URL, where the device can discover the owner’s IP address. At this point, both the device and the owner prove themselves to each other.

“Intel isn't actually authenticating trust in the cloud,” explains Gilburg. “Instead, we are simply rerouting devices to their intended new owner, where authentication will occur via the original Intel EPID signature. Once both agree, then an encrypted secure tunnel can be established between the device and the platform from which operational provisioning can occur.”

Provisioning is an important step that balances the security with the constraints of the device. For example, if the device is an embedded system with an RTOS, then the IoT platform management system might use a simple RSA key. If the device is a full gateway with greater memory and processing power, then a more secure image of the gateway can be used. Whatever is needed for that device to be operational, the platform management service makes that determination.

Scalable Security
This “zero touch” onboarding concept allows installers to simply plug in the device and verify its location. From there, network administrators can then take control of the device.

Authentication and security are established by a cloud-based proxy service connected to one of many IoT cloud-based platform providers. Once securely connected, the device is automatically provisioned by the user’s account in the cloud service – users don’t need to configure passwords, keys, or unique identifiers.

This last point is an important differentiator for Intel’s approach, as it ensures privacy of the device. Potential hackers cannot create an attack map by tracing devices from owner to owner. Intel EPID technology establishes an anonymous secure channel where endpoint authentication is hidden, unlike traditional public key methods (like PKI) where ownership is traceable.

In short, Intel’s approach to onboarding of IoT devices is both secure and easily scalable to the quick deployment of millions upon millions of devices.

Not a problem at all.

© 2018 insight.tech All rights reserved. Celeron, Intel, the Intel logo, Intel Atom, Intel Core, Intel Quark, Intel vPro, and Intel Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Other names and brands may be claimed as property of others.

John covers today’s latest high-tech, science and even science fiction in blogs, magazine articles, books and videos. He is an experienced physicist, engineer, journalist, author and professor who continues to speak at major conferences and before the camera on Chipestimate.com TV.
Meeting New Challenges for Detection and Prevention
As network protection increasingly demands more sophisticated and diversified capabilities, intrusion detection systems (IDS) and intrusion prevention systems (IPS) are becoming indispensable components for effective network security systems. An IDS monitors network operations security by gathering and analyzing network-wide information in order to instruct the operator on the required security rules adjustments, while an IPS blocks intrusions by executing security rules in real time after in-depth analysis of network data.

To enhance detection rates and minimize error rates, both IDS and IPS come with comprehensive detection technologies including feature matching, protocol analysis, and anomaly detection.

• Feature matching is by far the most commonly used due to its high accuracy and speed. Maximum feature matching efficiency depends on the accuracy of the overall feature library and the equipment’s feature matching capacity.

• By discerning protocol operating principles (usually based on Request for Comments or RFC standards), protocol analysis searches for suspicious visit behaviors to detect overflow and denial of service (DoS) attacks. Effective use of this technology enables a high detection rate and a near-zero error rate.

• Anomaly detection discovers unexpected abnormal traffic by learning and adjusting to a specific network environment’s normal traffic criteria, sending an alarm when the traffic statistics exceed the threshold value for a given traffic criterion.

Despite their advantages, each technology has its flaws. For example, feature matching requires regular updates of the feature library to avoid omissions. Due to the wide variances in each protocol’s implementation and unavailability of complete details for proprietary protocols, protocol analysis can usually only be realized for common protocols such as HTTP, FTP, and SMTP. When threshold values are set improperly, anomaly detection can result in false positives. As the number of web-based networks and advanced persistent threats (APTs) continues to increase, relying on traditional technologies when deploying IDS/IPS will be inadequate.

Challenges of Protecting Web-based Networks
HTTP is by far the most common source of network traffic. According to the TCP port traffic ranking statistics of the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT), the traffic on port 80 is far higher than that of other ports. Under such circumstances, increasing numbers of viruses, Trojans, and botnets will naturally launch attacks via HTTP. New-generation web threats and cyberattacks are increasingly covert as a result of interest orientation.

Enterprises are often prone to attacks hidden in legitimate traffic on the web due to enterprises’ dependency on the Internet for routine operations.

A built-in web reputation mechanism allows IDS and IPS to send timely warnings (IDS) or to block attacks (IPS) when users visit a webpage on which a Trojan has been implemented in order to effectively prevent infiltration of network security threats into the corporate intranet, leakage of sensitive data, and other information security incidents.

Application of Deep Packet Inspection Technology
Unlike a traditional firewall, an IPS can perform deep packet inspection (DPI) of packet contents. If a hacker launches attacks through the vulnerability in Layers 2-7, an IPS can detect and then block such attacks from the data flow. By contrast, the traditional firewall can only detect the quintuple of a data packet (source IP address, source port, target IP address, target port, and protocol at the transmission layer), without detecting the contents at the application layer or individual bytes, thus overlooking many attacks. As an IPS checks each byte of data traffic, it identifies most mainstream application protocols based on its protocol recognition framework. Then, through nuanced management of the identified information, it can detect the security vulnerabilities in these applications and take the initiative to prevent web attacks.

Tackling Sophisticated Cyberattacks Head On
How open hardware architecture and platform scalability are bringing 100G+ detection and prevention into the IoT era.

By Qizhi Zhang, ADLINK Technology
Application identification using DPI generally requires equipment with large-scale parallel computing ability to filter and detect tens of thousands of packets per second, as well as being able to perform IP defragmentation, TCP stream aggregation, and data flow status tracking.

**User-based Behavioral Analysis**

With the mobile network becoming an important infrastructure for enterprises, the number of intranet infiltration incidents via wireless networks is growing. In wireless network deployment, open Wi-Fi hotspots for visitors, allowing unauthenticated access to the corporate network, have become increasingly popular. In addition, employees working off-site may access the company network from their homes, airports, and customer premises. These wireless networks often lack effective management, allowing hackers to easily bypass the company’s firewalls, making wireless networks a stepping stone into the company’s intranet.

As the second security gateway after the firewall, IDS/IPS offers user identity and user access control to resolve broken access control (BAC) problems brought about by the roaming of unauthenticated equipment and employees. Statistical analysis of a company's employee network visit activities can establish a normal web visit pattern based on user identity, geographical location, operating time, visit contents, and visit frequency. The system can accurately detect abnormal behavior deviating from the normal visit pattern and send alarms (IDS) or block the activity (IPS).

**Advanced Persistent Threats**

Stealing core data is often the goal of APTs. Web attacks and intrusions launched on corporate users are often premeditated over a long period of time and highly concealed. APT attacks are like a special forces team equipped with comprehensive and sophisticated weapons that can paralyze the defensive power of the corporate web environment’s traditional firewalls and antivirus programs.

IDS/IPS bring better probability for successfully dealing with APTs. By performing network traffic visualization, an IDS will send alarms after detecting traffic anomalies to minimize the losses caused by APTs. Through collaboration with the local threat analysis system and based on the APT sample, behavior analysis, and virtual execution technologies, an IPS can discover advanced malicious codes hidden in the traffic and dynamically adjust its protection strategy to block malicious traffic in real time.

**How Hardware Platform Characteristics Support Advanced IDS and IPS**

New IDS and IPS solutions are coming online, including from NSFOCUS, enabling customers to monitor for, detect, and prevent attacks (Figure 2).

- In addition to a having an advanced attack rule feature library for detecting known security threats, NSFOCUS’ NIDS has a continually updated reputation feature library that can reduce hazards brought by unknown malware and prevent persistent intranet infiltration with its intranet security function, thus minimizing sensitive data leaks and abnormal external connections to servers.

- NSFOCUS’ NIPS is equipped with an attack feature library and real-time reputation library. To respond to advanced threats, an integrated sandbox detection capability offers 3D protection for both known and unknown threats. Flow virus detection technology captures hotspot viruses to maximally enhance antivirus capacity. The integrated mobile phone housekeeper makes secure enquiry push and secure status real-time monitoring possible, cutting maintenance and operation workloads.

**High Throughput Capacity and I/O Density**

To better meet the demands of core networks, cloud computing centers, large enterprises, and IDC outlets, NSFOCUS sought support of the 100GB interface on computing platforms for its
IDS/IPS products, with each piece of equipment supporting a minimum of 800G traffic connection and a minimum of 64x 10GB ports. The network ports must support upstream and downstream port consistency and RSS.

“The 4U space supports four dual Intel® Xeon® Processor E5-2600 v3/v4 boards or Intel® Xeon® Scalable Processor compute nodes to provide industry-leading processing performance and density.”

Parallel Computing and Computing Density
Parallel processing capability to support deep packet inspection and other detection methods also needed to be part of the feature set. In particular, network packet processing platforms needed wire speed transceiving capability, the maximum possible computing density per rack unit, and a zero packet loss rate for small packets of 64 bytes.

Load Balancing, Same Source and Same Host
In NSFOCUS’ NIDS/NIPS, all data traffic is connected by means of a switch board, which balances the traffic load to individual processor boards. When processor board errors are detected, the switch board can redirect the traffic. To ensure processing of the same conversation at the same CPU node, the switch board must support the same source and the same host to automatically merge the data flow of the same conversation.

Carrier-grade High Availability
As a NIPS platform must be incorporated into the traffic path, the modularization of computing platforms in a carrier-grade industrial design provides uninterrupted services for users with hot swap capability for faulty components (compute, switch, PSU, fan, and storage).

Support for Standardized API Management
Support for standardized API management of hardware platforms with a set of standardized APIs for traffic and hardware management of all components on the rack, port and VLAN management, commonly used L2/L3 switch protocol stacks, and remote reboot reduces low-level development burdens.

COTS DPI and Network Security Platform
As a next-generation high-performance telecommunications COTS DPI and network security platform, the CSA-7400, built on ADLINK’s Open Compute Carrier-grade Edge Reference Architecture (OCCERA), achieves high-speed interconnection of compute nodes with dual-redundant switch nodes to offer front panel I/O up to 800G. The CSA-7400 supports hot swapping of major chassis components to protect uninterrupted business, making it suitable for the next-generation high-performance IDS/IPS. The main features of the CSA-7400 are summarized as follows:

- Up to four compute nodes with dual Intel® Xeon® Processor E5-2600 v3/v4 or Intel® Xeon® Scalable Processors with support for single sled upgrade or hybrid deployment.
- Dual-redundant switch design with bandwidth of 4x 50GB per node for internal interconnection of four compute nodes, including 4x 100GB or 36x 10G upstream panel I/O.
- Switch supports accelerated processing of NVGRE/VXLAN tunneling protocols to meet the needs of Layer 2 network in cloud computing.
- ADLINK PacketManager software that provides commonly used Layer 2, Layer 3 switch protocol stacks and flow-based strategic control API, load balancing, same source and same host functions to accelerate application development.
- Supports smart system management using IPMI-based specifications for remote system diagnosis, redirection, shutdown, and startup.

Table 1 lists the requirements for the NSFOCUS next-generation NIDS/NIPS computing platforms, with the corresponding features of the CSA-7400 from ADLINK shown in the right column.

According to NSFOCUS, with our expertise in attack prevention developed over the years, this in-depth collaboration with ADLINK enables both parties to build IDS/IPS products meeting the demands of high-end application scenarios such as core networks for operations, cloud computing, large enterprises, and data centers. The interconnected redundant module design and hot swap support for both computing nodes and switches of the OCCERA-based CSA-7400 platform from ADLINK offer users uninterrupted delivery service.

NSFOCUS’ NIPS products are equipped with various advanced technologies, such as the NSFOCUS global threat intelligence system, and NSFOCUS unknown threat detection can demonstrate better protection on the CSA-7400. In the future, NSFOCUS will continue close collaboration with ADLINK for its IDS/IPS products to maximize the effectiveness of the excellent features of NSFOCUS’ NIDS/NIPS products on CSA-7400 platform for the network security market.

Figure 3: CSA-7400, next-gen high-performance telecommunications COTS
Meeting Network Security Requirements

| Supports ultra-high throughput interface and equipped with 100GB, 40GB and 10GB interfaces. | Modular I/O designed for scalable bandwidth according to actual needs. Supports high speed 100GB/40GB interfaces and provides up to 72x 10GB interfaces. Compared to currently popular 2U network security equipment, which supports a maximum of 64 x 10GB interfaces in the same 4U rack space. |
| Supports high-density parallel processing and is equipped with higher data packet processing performance; 64-byte small packet processing. | The 4U space supports four dual Intel® Xeon® Processor E5-2600 v3/v4 boards or Intel® Xeon® Scalable Processor compute nodes to provide industry-leading processing performance and density. Compared to currently popular 2U network security equipment supporting only one dual Intel® Xeon® processor board, the CSA-7400 4U space supports two dual Intel® Xeon® processor boards with the addition of excellent small packet (64 bytes) performance. Each compute node can process over 50GB of data with zero packet loss rate. |
| Load balancing, same source and same host | In addition to the load balance function for users to set different load weights for individual compute nodes, the switch board supports automatic elimination of faulty nodes in the load balancing process to ensure reliable processing of data flow. The switch board also supports same source and same host realized by hardware to efficiently merge network conversations. |
| High availability and full protection for hardware stability | Carrier grade high availability is achieved by design, including PSU redundancy and component hot swap. These designs also support real-time out-of-band monitoring of module operation through IPMI. Stringent QC enables product stability and reliability |
| Standardized API management interface for packaged inter-change and traffic and hardware control. | The ADLINK PacketManager equipped on the CSA-7400 platform offers port and VLAN management and protocol stacks for LACP, LLDP, RSTP, and VRRP. In addition, the CSA-7400 achieves high-performance smart forwarding of traffic via ACL as well as remote monitoring and reboot. |

Table 1: The CSA-7400’s high bandwidth, high density, high performance, and high reliability features meet the overall high computing capability requirements of today’s network security products.

Other Applications for Network Security and Telecommunications
ADLINK further integrates the latest virtual machine (VM) technology for information and communications into the hardware platform to provide the requisite features for developing security application products. In addition to IDS/IPS computing platforms, the CSA-7400 can be used for next-generation firewalls, telecommunications DPI and network virtualization, and mobile edge computing (MEC).

Conclusion
The CSA-7400 is a next-generation, high performance, carrier grade COTS network security platform built on the Open Compute Carrier-grade Edge Reference Architecture (OCCERA) by ADLINK, integrating network interfaces, switches, and overall computing capacity. The open hardware architecture and platform scalability of the CSA-7400 support NSFOCUS’ next-generation 100G+ ISD/IPS solutions, allowing NSFOCUS to launch its high-performance NIDS/NIPS products for the network security market. The CSA-7400’s flexibility and configurability enables cross-business product deployment and easy integration to other high-end network security markets, such as next-generation firewalls, telecommunications, and mobile edge computing. In addition to hardware features, the API library provided by ADLINK allows security solution providers focus on their core competence, enhance business migration increase product efficiency, and shorten product launch and delivery cycles.

Qizhi Zhang is System Architect for the Network & Communication Business Center, ADLINK Technology, where he is responsible for product definition, architectural design, and technical consulting for the enterprise’s Network & Communication platforms. Dr. Zhang received his Ph.D. in Automation from Shanghai Jiao Tong University. With 10+ years’ working experience in telecom industry, he is equipped with solid expertise in system management, high availability systems, and network security devices.
Take a Look at the New-Look Signage

There are not many examples where technology makes an original product bigger, but advances in display manufacture are proving to be the exception to the rule.

By Caroline Hayes, Senior Editor

Digital signage has revitalized hanging around at airports and train stations. The static information boards are now screens displaying timely information alongside adverts for ways to while away the time that are in the immediate vicinity. Sited in other public areas, they can make adverts more interesting, with video advertisements catching the eye of passers-by as the video plays. Digital signage is also found in private spaces, such as the doctor’s or dentist’s waiting rooms and also in companies, where a video wall can welcome, inform, and entertain visitors. More importantly, the screens can send targeted messages and create an impression of the company or brand as soon as someone enters the building.

Globally, the digital signage market is estimated to enjoy a Compound Annual Growth Rate (CAGR) of around seven to eight percent over the next few years to achieve a worldwide worth of over $30 billion by 2023.

Much of this growth is expected to come from retail and healthcare where digital signage is used for promotional material. An advantage that it offers is that content can be uploaded and displayed with little outlay and can be changed to meet changing market needs. There is also likely to be an increase in use in the corporate hospitality and corporate sectors, as content is created and distributed via screens that are 52-inch and above, according to Grand View Research.

Display Technology

Thin and flexible displays enable them to be used in more locations, such as on the curved walls of the London Underground (Figure 1). Other drivers will be 4K technology, which will be used for sharp images. 4K technology is expected to be exploited in advertising content, while LED-backlit panels will result in energy savings for the always-on signage and encourage enterprises to adopt digital signage in more locations.

Software extends beyond streaming content but can also be used to monitor and control both the content and the display’s operation. Analytics can provide data on footfall past a static location and also provide feedback on how content is viewed, re-posted on social media platforms, and shared.

Research by Orbis Research shows that advances in display technology, such as organic light emitting diodes (OLEDs), electronic paper display (EPD), and quantum dot LED (QLED) are also driving the market.

Innovation is bringing slim, lightweight, and inexpensive screens to market, making multiple displays in one location a cost-effective option. Taking a lead from smartphones, many of the displays used are borderless and capacitive touch screens, bringing interactivity to the display.

Figure 1: Curved screens mean digital signage can appear in more places, like the London Underground. (Picture credit: NEC Displays)
It is the rise of social media platforms, data analytics, and advances in display technology that have created a perfect storm. A combination of these three factors means that digital signage can be used more widely and with greater effect—for both the viewer and the owner/operator—than ever before.

**Customized Displays**

Although hardware plays a significant role, exploiting the thin format, high resolution display technology, it is software that is shaping the future of digital signage.

Dallas-based Lucid Networks builds cloud-based applications and services for video walls and displays which are used in corporate and retail spaces. Using Intel® NUC media players, NEC displays, and the company’s own LAVA Controls management and monitoring software, it builds, compiles, and ships cloud-based applications for digital signage.

The company takes an Intel NUC, a mini PC that measures four inches square, and embellishes it with customized functions for digital signage applications around the world. “We put 16-Gbyte of memory in it, to cache the internet content on it so that it is faster, especially on slower connections like an LTE connection,” explains Stephen Loeckle, CEO of Lucid Networks. Although the NUC box is off-the-shelf, the operating system is a version of Debian Linux and also runs the Chrome browser. It is the browser that displays all the content. The proprietary software performs a lot of self-healing functions. “If Chrome has any issues, the system will automatically perform a number of self-healing functions like restarting Chrome, clearing cache, rebooting the box. It is designed to be hands-off and to run 24/7 for years on end,” says Loeckle. It is a maintenance-free system, continues Loeckle, as the company provides all software updates and security updates, without burdening the IT department. He lets us in on a secret: “[The system] has generally been purchased by the marketing department and IT doesn’t want to have anything to do with digital signage if they can help it, it was purposely built to make it easy for everyone, including us and the end user,” he reveals.

“**The company takes an Intel® NUC, a mini PC that measures four inches square, and embellishes it with customized functions for digital signage applications around the world.**”

The light version of the NUC media player is equipped with 4Gbyte RAM and an Intel i3 processor. It is designed for slide displays, whereas the full version has 16Gbyte of RAM and an Intel i5 processor. This model is designed for end-users to show 4K video and social media content. “Some of the graphics in social media analytics can be very large and processor-intensive,” concedes Loeckle, requiring the enhanced processor capability, adding “It is likely that we will release a high-end version with 32Gbyte of RAM and an Intel i7 processor, for people that need the extra horsepower.”

The set pieces are the Intel NUC, NEC displays and video walls. For Internet of Things (IoT) devices, the company also offers LTE systems and Sierra Wireless routers for internet connectivity. The alchemy is in the operating system (OS) that the company puts on the NUC. There are many versions of the NUC, including the NUC8i7HYK and NUC8i7HNK released in January (Figure 2), based on the 8th Gen Intel Core processor, targeting gamers and virtual reality (VR) content creators.

**The Role of Software**

“We heavily embrace open source software, in operation and in deployment of the equipment,” says Loeckle. “We use Fog [the free, open source network computer cloning and management software] for imaging, whether local or remote.” He adds that the company also uses Debian Linux, another open source operating system (OS). The open source software is integrated with Lucid Networks’ own, custom software.

Lucid Networks uses a light and full version into which standard and Open Pluggable Specification (OPS) cards can be used. The OPS was launched by Intel in 2010 to standardize system architecture between displays and media players. Adding Kingston memory, with Crucial as a secondary source, the NUC is assembled in either Dallas, Texas, or Manchester, England for installation by local teams in Argentina, Mexico, Canada, South Korea, Australia, Japan, UK, and Poland. “We have boxes and video installations on every continent except Antarctica,” declares Loeckle. Nowhere, however, should be off limits, with remote control and monitoring; there must be a need for displaying environmental data at the McMurdo Station (the US research center) soon!

“For deployment it is more about people than the software,” Loeckle asserts. The boxes are pre-configured in house, “We know exactly where they are going to be deployed, so they are
appropriately labelled and configured for any particular video wall or deployment throughout an organization," Loeckle explains. "Every box is labelled for a purpose and location, so you know which box you are talking to when you get into our web interface." The web interface is global, controlling all the boxes and sending content. "You can send content to a box in the UK from the US, see what is running on that box, and check the status of the box, all managed through proprietary software," he adds.

Loeckle cites the example of video walls: "With the global interface someone in the US can completely control or monitor a video wall or display clear across the world. We can schedule tiling where images can span across the entire wall, we can have images pop or images move from monitor to monitor for a dynamic show on a video wall," he enthuses.

Adding Intelligence
A close relationship with NEC allows part of the software that runs on some of the boxes to be display control software. "We control the display from a power perspective, from an input perspective, we can schedule power on, power off, we can schedule input changes and we also report it back to the cloud," says Loeckle. He gives an example of remote monitoring. If the temperature of a monitor starts rising quickly, it is generally an indicator that there is a problem, maybe with the monitor, or air-conditioning or the power supply. "We can alert the customer before the monitor dies and they can get a replacement/call tech support and take care of the problem before it becomes an issue," Loeckle points out. "The thing we like to prevent are the monitors going out or the boxes not working. Probably the most embarrassing things for a digital signage company is to have no content running or a monitor that has gone out and nobody knows about it for days, or weeks," he adds. Building the monitoring and control features into the system, to provide an understanding of the health of the media player and the monitor are believed to be unique to Lucid Networks. "What no one has done before is combine those two together so that you know what your entire kit is doing. You need to know what the entire kit is doing to have a successful deployment," confirms Loeckle.

With these innovations in both hardware and software, where next for digital signage? Loeckle sees the possibilities as endless: "We started displaying social media content, and then it started going to lobbies for large corporations, now it is going into retail. The marketplace for digital signage as we currently call it, isn’t necessarily really digital signage any more. It is displaying content that is on the internet, no matter what that content is. It could be a birthday message, it could be social media analytics, so a large company can understand how their brand is doing on the internet, it could be YouTube videos, sales material, and it could be employee notices. It is so wide ranging that it amazes us how corporations are using our technology to send a message. And that can be any sort of still messages—or any message—to be conveyed."

Caroline Hayes has been a journalist covering the electronics sector for more than 20 years. She has worked on several European titles, reporting on a variety of industries, including communications, broadcast and automotive.
Trends in Digital Signage: Interview with Intel’s Jose Avalos

Mobile devices and social networks are making digital signage more interactive. Information adapts in real time based on location, time of day, online information feeds, and audience demographics. The possibilities for enhanced engagement are nearly endless.

By Lynnette Reese, Editor-in-Chief, Embedded Intel® Solutions

Many brick-and-mortar stores are fighting to stay ahead while battling on-line stores with global reach. Amazon is a prime example of an online store that has grown into a serious competitor to stores with a physical retail presence. Online stores like Amazon have overhead costs that are quite different from those at a brick-and-mortar, with no showrooms to maintain, no retail staff at a cash register, a fluid ability to change prices globally in an instant, and consumers who freely labor to post product reviews without compensation. Online stores have an automatic advantage when creating personalized experiences for customers. The online retailers can easily track visits and what customers shop for, as well as obtaining customer data when customers establish an account to make payment easier.

Although consumers can see and touch products in brick-and-mortar stores, this is not new. It’s no wonder that brick-and-mortar stores, in addition to maintaining an online presence, are bringing technology into stores to personalize the shopping experience and maintain continuity between customer visits (both in store and online). One of these tools is digital signage, which covers several other areas in addition to physical signs. Digital signage brings aspects of the online experience to consumers, be it in a department store or a sports arena.

Analysts report that around the world, about 70% of the visual experiences include Intel-based digital signage media players as an ingredient. These experiences include traditional digital signage, menu boards, video walls, interactive kiosks, interactive whiteboards, visual data devices, automated retail, intelligent shelves, smart lockers, digital jukeboxes, and more.

Reese: Are you seeing any trends in how digital signs and kiosks are being adopted in various venues?

Avalos: Intel-based digital signage and kiosk applications span across a wide range of verticals including retail, quick service restaurant (QSR), hospitality, transportation, healthcare, education, corporate, banking, entertainment, stadiums, and outdoors. The highest growth is in the retail, banking, QSRs, and transportation verticals; it varies by geography as well. For example, in Southeast Asia, banking is the fastest growing vertical at the moment.

Reese: What are retailers doing to blend the online and in-store experiences?

Avalos: When shopping online, today’s customers want all the personalization of an in-store experience. When they walk into a brick-and-mortar store, they want continuity from this online experience, based on the choices they made across all other touchpoints. Savvy retailers have met these expectations by pulling in incredible amounts of data for highly personalized cross-channel offerings. Online, they’re performing advanced real-time analytics on customer behavior to deliver digital experiences tailored to customers’ interests and needs. In the store, they’re using cutting-edge software to understand who’s looking at displays and to engage, entice, interact, and motivate action. This level of relevant personalization uses artificial intelligence (AI) for facial analytics. It is an essential tool for any retailer who aims to keep up with the changing expectations of digital consumers and find more effective ways to generate revenue.

By Lynnette Reese, Editor-in-Chief, Embedded Intel® Solutions

Embedded Intel magazine’s Editor-in-Chief, Lynnette Reese, interviewed Intel’s Jose A. Avalos, IoT Group Vice President and Visual Retail General Manager, about the role of technology in enhancing the consumer experience.

Lynnette Reese: How do you define digital signage, and where is Intel within that market space?

Jose Avalos: Intel® defines Digital Signage as a remotely managed interactive compute-driven display for advertising and information sharing.
Reese: Smart signs can display information for a customer that is tailored to their interests and needs. What is the role of Artificial Intelligence (AI) in digital signage?

Avalos: AI and facial detection enable a deeper understanding of customers and create a more curated experience. A certain level of personalization can be provided by using AI for facial analytics. Digital and interactive displays go beyond facial detection. They can detect a certain level of demographic information for each customer, the time they spent shopping, the locations where they lingered, and much more. With all of this information, it’s possible to create an in-store personalization that can deliver experiences that are individually tailored. The latest digital displays can collect analytics and deliver content as precisely as what customers experience online, which leads to a better understanding of the customer, greater insight and personalization, and an improvement in overall customer experience. Data shows that interactive digital signage gets more than twice the engagement rate of top social networks. But to actively engage the power of how this works you need to learn about the customer, so you can deliver customized content that reaches them at the right time. Good salesmanship is about helping a customer solve a problem by offering the right solutions, and smart signage can pick up on the kind of clues that can deliver the right content at the right time without being intrusive.

Reese: Privacy is always of interest; does Intel have any involvement in maintaining the privacy of consumers in digital signage applications? Or is maintaining an individual’s privacy completely up to the developer?

Avalos: Intel strives to protect consumer privacy related to our interface with digital signage under the Intel privacy policy. All offerings from Intel for the digital signage industry adhere to this policy. The policy starts out by saying, “Intel’s business brings technology to businesses, consumers and, society in a way that makes amazing experiences possible but doesn’t come at the expense of your privacy.” In addition, we advocate and influence our partner solutions to adhere to collecting and anonymizing data, so information doesn’t even register as belonging to any particular individual. However, in some cases, our end-customers such as retailers, for example, want to utilize detection analytics data for loyalty programs. In these cases, businesses and brands need to adhere to government opt-in laws. Ultimately, it is the solution provider’s privacy policies that apply in digital deployments.

Reese: How is Intel working with mobile integration to digital signage?

Avalos: Today, consumers are engaging with brands in a different way, merging in-person and online experiences as they take their interactions on the go and shop how they wish. A significant change affecting consumers is the shift to mobile, as now most consumers use their phone to research, browse, compare products, and order from anywhere. Digital signs provide an almost infinite number of ways to do this. Digital signs can be interactive, and they can sync up with mobile devices and social networks. They can take the form of a simple one-way flow of information like a classic sign, or the information can adapt in real time based on location, time of day, online information feeds, and the demographics of the audience. The possibilities for enhanced engagement are nearly endless. Intel enables unified commerce-ready digital signage and kiosk solutions so end customers (e.g., retailers) can grab and hold their audience’s attention and make their business stand out.

Reese: Do you have any examples that come to mind of campaigns that combine with people’s mobile technology (smartphones and the like) possible?

Avalos: We see mobile devices as an extension of the visual experiences delivered on digital touchpoints and extend the circle of influence on the consumer much beyond the point of sale into point of wait and point of transit. There are many end customers that have included mobile integration into their deployments for delivering experiences like product lookup, digital couponing, sharing shopping experiences on...
social media, and so on. We can’t name these end customers for confidentiality reasons, of course, but there’s a case study online [https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/awm-intelligent-shelving-solution-brief.pdf] and other proof points on www.intel.com/retail.

Reese: A trend in digital signage seems to be the blending of digital and physical worlds. What is Intel doing concerning VR/AR and digital signage?

Avalos: Augmented reality and virtual reality are certainly trends that are evolving in the digital signage and kiosk industry, enabling new use cases and applications. As part of our continued silicon technology innovation, we are adding additional compute and media performance to handle these workloads. Also, we are investing in enabling software that our VR and AR application developer ecosystem can leverage to unleash the hardware capabilities. Intel has also made several investments to offer AR and VR experiences into the sports experience, which are capabilities we can also extend into the digital signage and kiosk spaces.

Reese: What types of Intel processors are needed for smart (AI) digital signage?

Avalos: For seamless experiences and a wide range of applications for smart digital signage, Intel offerings range from Intel® Atom® class processors to Intel® Xeon® class processors and everything in between. This can be augmented by visual processing units such as Intel® Movidius™ and a wide range of programmable logic solutions (FPGAs) such as Cyclone®, Arria®, and Stratix®. To expedite the development of applications and differentiated solutions, Intel offers several development kits such as OpenVINO™ for Analytics, Intel® Media SDK for media and graphic-effects intense applications.

Reese: In general, what can we expect from digital signage in the future?

Avalos: Today digital signage is delivering more productive, engaging, and fun experiences across many industries such as retail, banking, and transportation. Digital signage coupled with other technologies such as AI, analytics, and computer vision is enabling brands to have a continuous dialogue with consumers. This continuity with customers is critical to brands, as today consumers not only want to communicate with brands, they also want to help shape the evolution of their favorite brands.

Reese: Well the future certainly looks bright for creating a better overall customer experience using technology. Thank you for your time.
Intel’s New Tool for Programming FPGAs…for Artificial Intelligence

Accelerate AI inference. The OpenVINO tool optimizes a DNN model (TensorFlow or Caffe) for running on an Intel CPU, GPU, Movidius, or FPGA. The single-shot command line utility can also convert the model from any Intel AI-suitable platform to another, enabling quick experimentation among platforms. And it’s free.

By Lynnette Reese, Editor-in-Chief, Embedded Intel® Solutions

Intel® has a toolkit called OpenVINO™ that can take a Dynamic Neural Network (DNN) model from TensorFlow™, Caffe, or MXNet to any Intel AI hardware platform in a few seconds. The command line tool optimizes the neural network model and converts it for use on any other AI hardware Intel platform, including Field Programmable Gate Arrays (FPGAs).

Various AI accelerators are available on the market today: GPUs, high performance processors, FPGAs, and custom chips (i.e., ASIcs). Accelerators help in AI by rapidly performing numerous calculations, off-loading the main processor. FPGAs hold several advantages, however, given that AI is changing rapidly and constant hardware optimization is a necessity in many areas.

Tony Kau, Marketing Director, Artificial Intelligence, Software and IP Solutions at Intel, states, “FPGAs bring a lot of value at the hardware performance level. FPGAs accommodate many new topologies and primitives in AI that are coming into the space today. FPGAs also bring the ability at a high level to do a lot of optimization around precision bit width and then to really achieve the power performance balance that a customer wants. FPGAs bring a low latency advantage combined with extraordinary flexibility.”

Historically, FPGAs have been complicated to program, with a steeper learning curve than traditional programming. However, the programming scene for FPGAs is improving. Recently, Intel® released a development tool that allows effective execution of a neural network model from several deep learning training frameworks to any Intel AI Hardware engine, including FPGAs. Open Visual Inference & Neural Network Optimization (OpenVINO™) toolkit performs a one-time, offline, seconds-long conversion. OpenVINO has a single API across all types of Intel standard HW targets and accelerators. You can use OpenVINO to convert a TensorFlow™, MXNet, or Caffe model to a format that works for Intel standard HW targets including CPUs and CPUs with integrated graphics as well as accelerators such as Vision Processing Units (VPUs) featuring Movidius, and FPGAs.

The OpenVINO tool, in a nutshell, provides a near-instant conversion of the AI training tools output (model) so it’s compatible to run on any Intel AI HW engine.

Adam Burns, Director of Computer Vision and Digital Surveillance at Intel Corporation, describes how OpenVINO works. “You can train a neural network using TensorFlow or one of the other frameworks, which produces a model. OpenVINO optimizes the model. The result allows you to target various Intel hardware engines that you can choose from to run the model on. OpenVINO optimizes the output for running on an Intel CPU, GPU, Movidius, or FPGA.” OpenVINO’s single API works across all Intel accelerators. Developers do not need to re-design applications for deployment on different targets, allowing for quick experimentation of best-case scenarios on the actual hardware. One of the most important features of the OpenVINO toolkit is the “model zoo,” which contains public and free optimized models. One can use these models for rapid prototyping as well as expediting development and production of applications without having to search for—or train—your own models.

The time required to pre-process a large model by OpenVINO is measured in seconds, not minutes. No model re-training is required. OpenVINO is continuously benchmarked on a wide array of deep learning models (150+ models). The outputs of OpenVINO are checked both for accuracy and functionality across all targets and accelerators. OpenVINO allows flexibility with customizations in C++ and OpenCL languages, and provides a comprehensive validation suite, as well. (See Figure 2.)

OpenVINO is a one-step, command-line driven process. Changes to a model are natural. If you need to change your model, you go back into your deep learning training framework.

Figure 1: Tony Kau, Marketing Director, Artificial Intelligence, Software and IP Solutions. Intel.
and change the model, then convert the new model using OpenVINO again. Importantly, OpenVINO does not require the original training framework in order to execute.

Neural networks come in different sizes, requiring different amounts of memory, so the OpenVINO tool makes it convenient to choose only as much hardware as you need, be it a CPU, an FPGA, or a Movidius processor. The Intel Movidius, for instance, is ideal for ultra-low-power consumption applications using smaller models and executing on a smaller footprint. Developers might find that their existing model, once it is optimized using OpenVINO, fits in a smaller accelerator, saving much in hardware cost.

**Optimizing for Power**

Optimizing models using OpenVINO is a snap. For example, by applying quantization and converting a model from 32-bit floating point (FP32) to 16-bit floating point (FP16) one can make the model smaller, lowering the required compute, and thus save a lot of power. In some cases, such optimization comes at the cost of less than 1% in accuracy. In future releases, optimization capabilities of OpenVINO will significantly expand, featuring many new functionalities around quantization/ternarization/binarization, pruning, and sparsity.

As Burns points out, “Developers can fit the compute they need into a relatively inexpensive and low-power device. That kind of conversion power in a free tool has generated high interest, so a lot of developers are looking at OpenVINO as a way to easily add capability to an existing system. OpenVINO opens up a whole new world of options to design around because you can just plug in that little low-power, low-cost device and add the benefit of an AI engine to your system.”

OpenVINO is a free tool offered by Intel under a mixture of licenses, including the Apache license, depending upon the model. Supported target platform (64 bit) operating systems include Windows 10 and the Yocto Project’s Poky Jethro v2.03, Ubuntu 16.04.3 LTS, and CentOS 7.4 Linux distributions.

Lynnette Reese is Editor-in-Chief, Embedded Intel® Solutions and Embedded Systems Engineering, and has been working in various roles as an electrical engineer for over two decades. She is interested in open source software and hardware, the maker movement, and in increasing the number of women working in STEM so she has a greater chance of talking about something other than football at the water cooler.
NEW! Compact, Modular and Fanless Industrial PC

Applications
- Industrial IoT (IIoT) Network and Cloud Computing
- Cyber Security Edge Devices for ICS and SCADA threat security
- Secure Networking (Secure Routing, Traffic Monitoring and Gateways)
- Intelligent Machinery and Equipment Controllers

The ADLEPC-1520 is a rugged, compact industrial-grade chassis constructed from 6063 aluminum, with thick-walled design and a fanless, conduction-cooled CPU for wider temperature operation. It features a durable anodized finish, flush-mounted screws, and flexible mounting options. At only 2.3” x 3.4” x 3.7”, it is ideal for a variety of industrial applications and environments...whether on the factory floor or in the external environments.

Features & Benefits
- Compact footprint: 2.3” x 3.4” x 3.7”
- Intel® E3800 -Series Atom processors
- Stackable Extension Connector
- Modular I/O Expansion
- Fanless Design
- Custom I/O and Power available to support specific application requirements
- Operating Temperature: -20C to +60C (optional extended temperature available)

Embedded Solutions
SMARTER BY DESIGN®

ADL Embedded Solutions
855-727-4200
sales@adl-usa.com

Designing with Intel® Embedded Processors?

Embedded Intel® Solutions delivers in-depth product, technology and design information to engineers and embedded developers who design with Intel® Embedded processors.

Visit www.embeddedintel.com

Subscribe Today at www.embeddedintel.com Free!
IOPS-602 OPS Slot-in Digital Signage Player

Compatible Operating Systems: Windows 10 / Linux Ubuntu

Supported Intel®: Intel® Core™ i7 Processor, Intel® Core™ i3 Processor, Intel® Core™ i5 Processor

IOPS-602 is a slot-in digital signage player built on the benefits and functionality of Intel’s Open Pluggable Specification (OPS). The OPS standard provides cableless and cost-effective deployment for more effective management and maintenance of media players. The IOPS-602 OPS signage player is powered by 7th Gen Intel® Core™ QC/DC processors and runs both Window 10 and Linux Ubuntu operating systems. It uses the processor-integrated, high-definition graphics for crisp content playback with up to 4K resolution.

In addition, advanced features to meet customer requirements include up to 32GB of DDR4 SO-DIMM support, four USB 3.0, one Gigabit LAN, an M.2 (KEY E) for optional WiFi/Bluetooth expansion cards, and Intel® AMT for remote system control, monitoring and troubleshooting. IBASE offers a comprehensive line of digital signage players with solutions from entry-level, low power systems for one or dual FHD displays, to high-end systems that feature advanced configurations for 4K/8K/12K multi-screen video walls, hardware/software EDID emulation and wireless communications expansion options.


FEATURES & BENEFITS
◆ Designed with Intel’s Open Pluggable Specification (OPS) standard
◆ Improved connection reliability between DS Player & display
◆ Allows cableless deployment and easy maintenance
◆ Supports 7th/6th Generation Intel® Core™ QC/DC Processors
◆ For crisp content playback with up to 4K resolution
◆ iAMT compliance for remote management
◆ 1x M.2 E-Key(2230) for Wi-Fi or Bluetooth options
◆ Supports Window 10 and Linux Ubuntu operating systems

TECHNICAL SPECS
◆ 7th Generation Intel® Core™ U-Series Processor
◆ 2x DDR4-2133 SO-DIMM, dual-channel, Max 32 GB
◆ 1x HDMI 1.4b, 4x USB 3.0 ports
◆ 1x RJ45 for Gigabit LAN, 1x RJ45 for RS232 serial port
◆ 1x Intel® I219LM LAN PHY for i5/i7
◆ 1x Intel® I219V LAN PHY for i3
◆ 1x M.2 E-Key(2230) for Wi-Fi or Bluetooth options
◆ 2x audio connectors for Line-in / Line-out
◆ 200mm(W) x 119mm(D) x 30mm(H)

APPLICATION AREAS
Embedded Computing; Digital Signage

AVAILABILITY
On the Shelf Now!
New! Flexible Configured 1U Network Appliance

Compatible Operating Systems: Microsoft Windows, Linux Kernel

Supported Intel®: Intel® Core™ i7 Processor, Intel® Core™ i3 Processor, Intel® Core™ i5 Processor, Intel® Pentium® Processor, Intel® Xeon® Processor D Series

Powered by Intel’s Xeon processor D family and Intel Core processors (7th and 8th generation), the new APTNS supports up to 17 LAN ports for a wide range of network appliances. The new APTNS 1U rackmount network communications appliance unit is designed to support primarily in the enterprise network security arena and deliver an outstanding combination of performance, flexibility and upgradeability in applications such as data center network server, firewall, access point control, unified threat management and as a software defined server.

“The APTNS" modularized design provides a greater selection of Intel processors, smooths the upgrade process. The COM Express design itself benefits customers by enabling them to select a variety of processor modules without re-inventing the wheel. Hot-swappable fan and optional redundant power supply unit not only support quick and easy field maintenance but also extend stability and reliability for enterprise applications. It also features rich I/O for versatile applications, dual-channel memory up to 96 GB and two 2.5” SATA HD.

FEATURES & BENEFITS
◆ Flexible configuration to support product from entry level to high-end level
◆ Scalable and up-gradable computing performance
◆ Easy expansion of high speed network interfaces up to 17 ports with copper/fiber/1GbE/10GbE/bypass
◆ Low power consumption enables power savings and supports energy conservation initiatives
◆ Faster time to market of next generation by upgrading with next generation processors

TECHNICAL SPECS
◆ Selection of Intel® Xeon® processor D series, Intel® Core™ processor series, or Intel® Pentium® processors
◆ Dual channel DDR3/4 ECC/non-ECC SDRAM up to 96 GB
◆ 2 x USB 2.0, 2 x USB 3.0, 1 x VGA, 1 x RS-232
◆ 3 x Hot swappable fan
◆ 300W single or redundant ATX power supply

APPLICATION AREAS

AVAILABILITY
Sample available now!
**Intel® Apollo Lake NANO-ITX Embedded Motherboard**

**Compatible Operating Systems:** Windows, Windows Embedded, Linux, VxWorks, and QNX

**Supported Intel®:** Intel® Atom™ Processor E3900

The Portwell NANO-6062 embedded motherboard built with Intel® Apollo Lake Atom™ E3900 series processor. The Intel® Atom™ E3900 series processor supports industrial grade wide temperature (-40°C~85°C) and also low power consumption (under 12W) for fan-less application. Additionally, NANO-6062 supports wide voltage of power input from DC 12V to 24V for rugged applications.

Portwell NANO-6062 supports two DDR3L 1866/1600 SODIMM slots up to 8GB RAM and four USB 3.0 ports, ensuring fast data transmission with low-power consumption. It also supports triple display with VGA, DP (Display Port) and onboard LVDS connector. One 5Gb/s PCI Express 2.0 Lane can be used as one full-size Mini PCIe for system expansion purpose. Two SATA 3.0 connectors (one of them is available as mSATA and the other for SATA) with up to 6 Gb/s allow quick and flexible system storage expansions. Intel I210-IT Gigabit Ethernet controller provides dual Gigabit Ethernet LAN access via two RJ45 ports. One audio jack on rear I/O with Line-out and onboard pin header with Line-in, Line-out and Mic-in.

Moreover, NANO-6062 integrates the M.2 socket (Type E) interface, which can provide wireless connectivity including Wi-Fi and Bluetooth, allowing ideal communication and connectivity for IoT edge or gateway devices.

The Portwell NANO-6062, with its ingenious design and superior performance with up to quad core processor with low thermal fan-less design, delivers the ability to execute an extensive array of application which requires wide operating temperature and robust reliability.

**FEATURES & BENEFITS**

- Supports two DDR3L 1866/1600 SODIMM slots up to 8GB RAM and four USB 3.0 ports
- Low-power consumption (Under 12W)
- Supports triple display with VGA, DP (Display Port) and onboard LVDS connector
- Integrates the M.2 socket (Type E) for wireless expansion
- Dual Gigabit Ethernet LAN access via two RJ45 ports
- 4.72”(L) x 4.72”(W)

**TECHNICAL SPECS**

- Intel® Atom™ processor E3900 series
- Supports DDR3L 1866/1600 SODIMM up to 8GB
- Supports triple display by VGA, Display Port and LVDS
- Supports one M.2 socket, SATA III port, Mini PCIe and mSATA socket, DC 12V-24V input
- Supports a wide -40°C to 85°C industrial temperature range

**APPLICATION AREAS**

Embedded Computing; Digital Security and Surveillance; Digital Signage; Gaming; Industrial Automation/Control; In-vehicle Infotainment; Medical; Military, Aerospace, and Government; Retail (POS/Kiosk/ATM); IP Services; Network Security Infrastructure; Networked Storage; IIoT Gateway; Wireless Infrastructure

**AVAILABILITY**

Sample available now! COTS modifications are also available.
Condor (VL-EPU-4460)

Compatible Operating Systems: Windows, Windows Embedded, Linux, VxWorks, and QNX

Supported Intel®: Intel® Core™ i7 Processor, Intel® Core™ i3 Processor, Intel® Core™ i5 Processor

The Condor is a compact, high-performance, embedded computer. It has been engineered and tested to meet evolving requirements for smaller, lighter, and lower power embedded systems while adhering to stringent regulatory standards. Designed around the COM “compact” form factor, the Condor is a member of the VersaLogic “EPU” family of ultra-rugged embedded computers, designed to withstand extreme temperature, impact, and vibration. The Condor’s on-board TPM security chip can lock out unauthorized hardware and software access. It provides a secure “Root of Trust.” Additional security is provided through built-in AES (Advanced Encryption Standard) instructions. The Condor features high-performance Skylake processors with dual-core CPUs and Hyper-Threading logic, allowing up to 4 simultaneous threads to be executed. Even with its outstanding performance and I/O features, the Condor’s typical power consumption is 15 to 17 watts, depending on the model. The Condor provides compatibility with a broad range of standard x86 application development tools for reduced development time.

VersaLogic’s newest embedded computer product is built around Intel’s powerful Skylake processor using the COM Compact form factor (95x95x37mm). It provides very high performance, small size, and a TPM security chip. It combines a processor board, I/O board, and heat plate, delivered as a fully assembled and tested computer.

FEATURES & BENEFITS

◆ 6th Generation Intel® Core™ “Skylake” processor --i7-6600U (dual core) or --i5-6300U (dual core) or --i3-6100U (dual core)

◆ -40° to +85°C operating temperature models

◆ TPM (Trusted Platform Module) security chip

◆ Shock and vibration per MIL-STD-202G

◆ On-board Power Management --8 to 30 volt DC input (12 and 24 volt system compatible) --Over- and reverse-voltage protection --RF noise filtering --Transient voltage protection

TECHNICAL SPECS


◆ Two Gigabit Ethernet (GbE). One port with remote boot support.

◆ SATA – 6 Gb/s SATA port. Supports rotating or solid state SATA drives.

◆ Mini PCIe Card Sockets – two full-sized sockets. Supports Wi-Fi modems, GPS, MIL-STD-1553, Ethernet, flash data storage with autodetect mSATA flash storage support, and other mini PCIe modules.

◆ Industrial I/O – includes two USB 3.0 ports and four USB 2.0 ports to support keyboard, mouse and other devices. Two RS-232/422/485 serial ports, three 8254 timer/counters, and I2C support.

APPLICATION AREAS

Embedded Computing; Medical; Military; Aerospace; Industrial Automation/Control; and Government

AVAILABILITY

On the Shelf Now!
Getting a Grip on Robotics

How powerful software modules and high-performance embedded systems can drive the widespread adoption of autonomous, cooperative, and collaborative robots.

By Zeljko Loncaric, congatec and Prof. Dr. Christian Schlegel, Service Robotics Research Group, Ulm University of Applied Sciences

The Service Robotics Research Center of Ulm University of Applied Sciences is developing a modular software framework to make it easier to program robots. The goal is to provide software modules that can be used universally, for instance to swap robotic gripping arms from different manufacturers as required to generate new robotics solutions via plug and play. The team at Ulm University relies on congatec for highly scalable and standardized embedded computing hardware.

Today’s modern robots are highly complex constructions with numerous subsystems. They use manipulators with various axes and drive units, at the ends of which specific tools, gripper systems or measuring instruments are installed. Controlling the kinematics takes additional sensor systems, as does object and position recognition in pick-and-place applications for example. With the advent of autonomous and collaborative robots—sharing the same workspace with humans—many more tasks and building blocks are added. Examples include localizing and navigating mobile robots in industrial settings and safe human machine interaction (HMI). Industry 4.0 environments also need an M2M interface to the surrounding machines and systems. The goal is mutual task coordination. All of these different robot types—from autonomous to cooperative to collaborative—require powerful software modules and high-performance embedded systems.

**High Market Demand for Smart Robots**

Market demand for smart robots will grow rapidly in the coming years. For example, the market for autonomous robot systems is expected to grow at a CAGR of 23.7% until 2023, while the new market segment of collaborative robots is due to grow twice as much at an average 59% per annum. OEMs are under immense pressure to develop and to bring such new systems to market maturity as quickly as possible in order to participate in this high market growth. But the software development is a particularly great challenge for OEMs, system integrators, and users: More subsystems have to be integrated into the already complex autonomous robotics solutions if they are to become collaborative and/or cooperative.

**Figure 1:** Collaborative robotics needs hardware and software modules that can be modularly assembled to suit their task. There should be minimal to no programming effort; it should be enough for the modules to be parameterized.

**Figure 2:** The SmartMDSD Toolchain allows component developers to develop software modules for individual functional units that can be combined as required and reused in new robot designs. The underlying hardware should therefore be flexibly scalable.

**Why the Closed System Approach Isn’t Working**

Today, the software for robots is frequently still implemented as a closed system—usually with individually tailored x86 or other hardware including ASICS or FPGAs. Often, the software is even individually tailored for each robot, making reuse difficult. All tasks such as manipulator control, navigation, machine vision, task coordination, and HMI are programmed as a unit. It is therefore currently nearly impossible to exchange software components even for the most frequently required functions or to use them on another hardware platform. This means that for every new design, the robotics software has to be re-implemented. This is both error-prone and time-consuming and can significantly delay the rollout of much-needed innovative solutions—not to mention the hassle this causes operators who have to program each robot initially for its specific task.

---

Modular and Reusable
The development team of the Service Robotics Research Center of Ulm University of Applied Sciences under Professor Schlegel is now replacing this closed system approach, which burdens system integrators and users with additional work, with a modular software approach. Adopting this approach divides the complex overall robot system into several independent functional units. In a second step, it specifies the interaction between the individual units via fully and transparently defined interfaces.

This concept, SmartSoft, is now being expanded and widely marketed at the European level (EU H2020 project “RobMoSys - Composable Models and Software for Robotic Systems”) and national level (BMWi PAiCE project “SeRoNet - a platform for the joint development of service robot solutions”) in cooperation with partners from industry and research. Essentially, this approach aims to make it possible to assemble robotic systems from fully developed and tested modular software building blocks. This allows software developers to focus on individual function modules without having to consider the internals of the other components. More importantly, it makes it possible to combine functions such as the cooperative or collaborative elements as well as the logic for specific manipulators and a lot more in a modular way—even across manufacturers. Ultimately, this also reduces the effort required for system integrators and end users to make customer-specific adaptations and will significantly drive the widespread adoption of robotics.

So, let’s assume you have a manipulator from company A, combined with a chassis from manufacturer B, and a stereoscopic machine vision system from manufacturer C. The dedicated control software, like that in intralogistics applications for instance, is then easily assembled from the ready-made software components thanks to the high level of abstraction. Only minor adjustments are needed. No pipe dream, this application is already being tested in the real world. For example, the Ulm team has implemented the service robotics duo Larry and Robotino, which, in a pharmaceutical intralogistics application for Transpharm Logistik GmbH, assembles drug packages from individual trays completely autonomously and takes them to a specified delivery point.

In a slightly different configuration, the two robots have autonomously taken coffee orders and delivered them to the customer’s table. Thanks to the ready-made, freely combinable software components, the redesign took only a few hours. The video to see the two robots in action can be found at https://www.youtube.com/watch?v=Zz66I4NVtNU.

Containers with Clearly Defined Interfaces
To enable virtually any assembly of elements, the team from the Service Robotics Research Center of Ulm University of Applied Sciences has developed a software model with individual service-oriented components and a model-driven open-source software toolchain for the Eclipse development environment. This environment provides component developers with tools that they can use to build their own code for each functional unit and then secure those algorithms by automatically generated component containers. These containers communicate with other containers based on uniform communication interfaces. In addition, the wrapping also protects the component developer’s IP. The team has already developed several such functional modules and makes them available for use in their own projects. These include navigation modules, machine vision, HMI, manipulator control and task coordination, to name just a few examples. As a unifying communication interface, SmartSoft also relies on OPC UA. This allows manufacturers to focus on specific containers and build their core competencies here. Customers benefit from a much more flexible offering.

Generic Embedded Hardware Over Proprietary Designs
For the logic hardware, the Ulm team uses Intel® x86 technology to decouple the software development as far as possible from any specific hardware. With the appropriate glue logic, such an approach is also particularly easy to implement with x86 technology as far as the later migration of such systems is concerned.
Embedded x86 hardware is also particularly apt in this context because of the high standardization and comprehensive documentation. The form factors are standardized not only as regards dimensions, but also with regard to the application programming interface. Standardization facilitates replacement of hardware provided the boards comply with the EAPI specification of the PICMG or SGET UIC standard. Under those circumstances, it is even possible to vary freely between different form factors such as motherboards and Computer-on-Modules, depending on the requirements of the application, without having to significantly change how hardware is accessed during the migration. One supplier who attaches great importance to this standardization and its documentation as well as the simplest possible hardware integration is congatec, whose products the Service Robotics Research Center of Ulm University of Applied Sciences uses in its projects.

“Next to basic requirements such as maximum computing power, energy efficiency, and reliability, we also attach great importance to high standardization and the capability to migrate universally,” explains Matthias Lutz from Ulm University of Applied Sciences. “Every additional abstraction level in the software requires additional computing performance, so we’re currently working with powerful dual-core technology. A standardized approach to board components and GPIOs to control the robotics modules also gives us the abstraction required for independence at the embedded computing level.”

The choice ultimately fell on the fully industrial Mini-ITX carrier board conga-IC175. That’s because the standardized Mini-ITX form factor offers many advantages for developing the prototypes of the innovative software modules into real systems: It already integrates all interfaces on a standardized board, and the power supply is via standard ATX power supplies, industrial 12V feed-in, or SMART batteries, which is essential for mobile robots such as Robotino and Larry. Using PCIe expansion cards make implementing extensions quick and efficient. The board is highly energy efficient and uses robust embedded components, so it can be operated without expensive cooling.

Future commercial robot designs from Ulm will be implemented on Computer-on-Modules. But regardless of whether it’s a Mini-ITX motherboard, module with standard Mini-ITX carrier, module and individual carrier, or full-custom design: It is the Total cost of Ownership (TCO) that ultimately matters to OEMs, and when using modular software this is also determined by the software support of the hardware. To make it even easier to integrate more functionalities in the future, comprehensive support for real-time hypervisor technology can bring added benefits. This will give customers the option to integrate additional functionalities, such as their own IoT gateway, without having to use a dedicated hardware platform, which saves hardware costs.

“We see clear benefits in such modular approaches as they mirror the modular approach of our software. In this respect, it is very interesting to see that with the acquisition of Real-Time Systems congatec now has virtually direct access to the hypervisor technology of these robotics and automation experts,” concludes Lutz.

Coupled with the Technical Solution Center (TSC), in which congatec consolidates all its OEM services, this results in a complete package for customers such as the Service Robotics Research Center of Ulm University of Applied Sciences or Transpharm Logistik GmbH.

Use Case: Pharmacy Intralogistics
Picking tasks are performed by a heterogeneous robot fleet in an intralogistics application at congatec’s industrial partner Transpharm Logistik GmbH. The autonomous picking robot Larry is equipped with a UR5 manipulator module and uses a Segway chassis. The transport robot Robotino has a conveyor belt instead of a manipulator to take the picking robot to any point. Orders are received directly from the warehouse management system via WLAN. The fleet management system selects two picking robots, which then execute the order. The application is based on results from the BMBF project “LogiRob - Multi-Robot Transport System in a Shared Human-Machine Workspace” and “ZAFH Intralogistics - Collaborative Systems to Increase Intralogistics Flexibility” (Baden-Württemberg and EU ERDF 2014-2020).
INTERNET OF THINGS DEVELOPERS CONFERENCE
WWW.IOT-DEVCON.COM

JUNE 5-6, 2019
SANTA CLARA CONVENTION CENTER

The Premier Conference Devoted To Implementing IoT Technology in Embedded Systems - PLAN NOW TO ATTEND!
Unparalleled processing power. Rugged and secure.

Embedded Intel® single board computers designed, tested, manufactured, and supported in the USA for use in the most extreme environments on Earth.