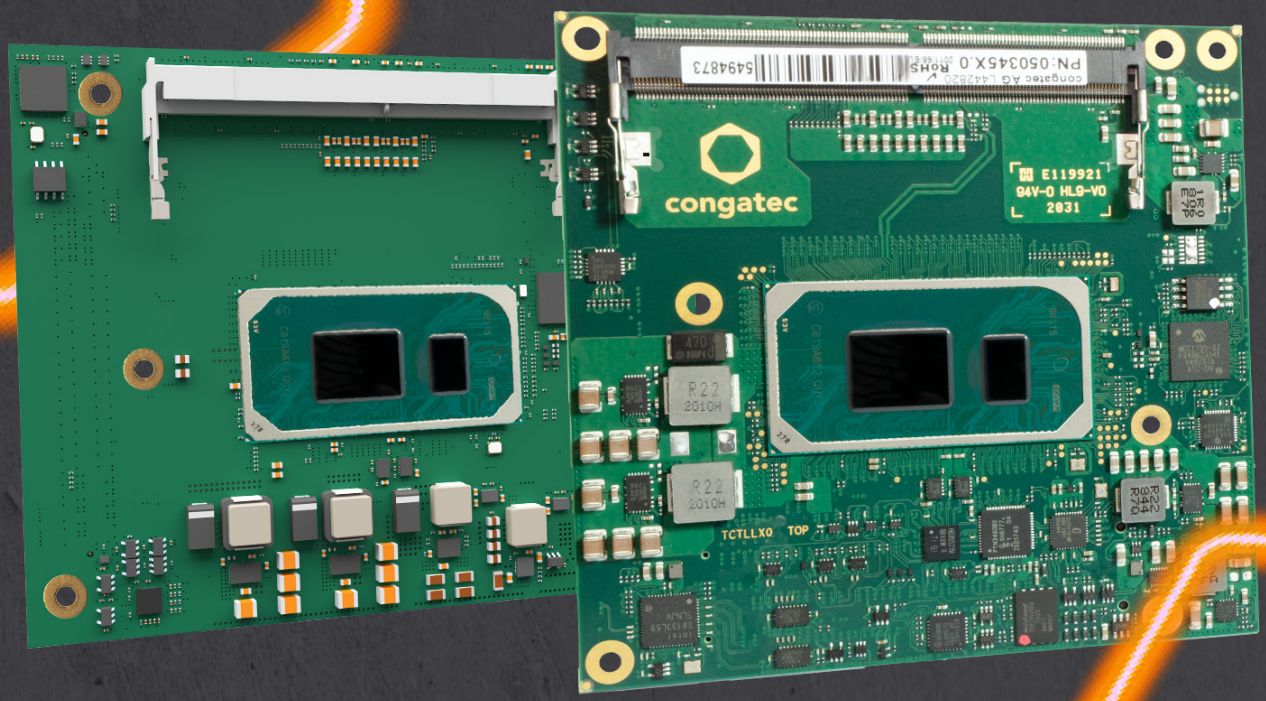
V. 08/21

congatec



Whitepaper

11 good reasons for the 11th generation

Why 11th Gen Intel® Core™ processors will conquer the market

Alcom electronics
Singel 3 | B-2550 Kontich | Belgium | Tel. +32 (0)3 458 30 33 | info@alcom.be | www.alcom.be
Rivium 1e straat 52 | 2909 LE Capelle aan den Ijssel | The Netherlands | Tel. +31 (0)10 288 25 00 | info@alcom.nl | www.alcom.nl

11 good reasons for the 11th generation

In parallel with the launch of the 11th Intel® Core™ processor generation (codenamed Tiger Lake), congatec has made the new processors available on COM-HPC Size A and COM Express Compact Computer-on-Modules. What does the new Intel® Core™ processor generation offer? This whitepaper spells out the 11 most important reasons why OEMs should rely on congatec modules with 11th generation Intel® Core™ processors.

The embedded and edge computing markets are hungry for more performance within the given thermal budgets. Any performance increase that can be achieved without an active processor fan is welcomed with open arms. The goal is to develop even more powerful systems, characterized by robust, durable, and maintenance-free designs and capable of communicating securely and in real-time with increasing bandwidth via the Internet of Things (IoT). These requirements apply across the entire spectrum of high-performance embedded computing applications – from embedded systems and edge computing nodes, network hubs and local fog data centers, to infrastructure appliances in the core network, and robust central cloud data centers for critical government applications. The low-power, high-density variants of the 11th generation Intel® Core™ processors (aka Tiger Lake) will therefore rapidly conquer the embedded market and become the new flagship of fanless high-speed embedded computing. There are 11 good reasons for this.

The latest is always the best

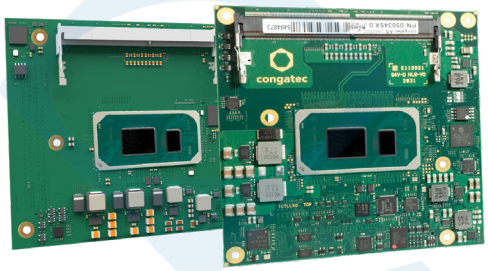
The first and perhaps most important reason to rely on the low-power high-density processors of the 11th Intel Core processor generation is the fact that end customers always want the very latest. Even if they cannot take full advantage of the improvements, they still want to be sure that they have chosen the best available solution on the market. For this reason, it is often almost impossible for OEMs to skip a launch to save NRE costs and increase ROI. As soon as a competitor appears who aims to exploit the advantages of the new processor, customers will quickly start to question the innovative strength of their own OEM. Any attempts to justify the omission of a development cycle solely for efficiency reasons will not counterweight the argument that the latest processor also offers more innovative features and that the competitor offers exactly these functions and you do not.

Therefore, it is generally advisable to follow the design cycles of the processor manufacturers as closely as possible – especially since this strategy also enables you to claim innovation leadership for yourself. The most efficient way to meet this customer expectation, which is not based on technical facts but more emotionally motivated, is to use Computer-on-Modules. As a rule, they do not require any additional engineering effort on the hardware side and offer numerous other advantages, as shown in Figure 1.

COM and carrier designs offer numerous advantages over full-custom designs. For new processor launches such as the 11th Intel Core processor generation, the most significant benefit is a very short time-to-market.

If the Computer-on-Modules come from embedded suppliers such as congatec, who are able to bring them to market the moment the new processors are launched, OEMs can optimize their time-to-market and create the necessary competitive advantage that can never be achieved with a dedicated full-custom design.

COM Express and COM-HPC Size A



The latest is always the best is a principle that also applies to Computer-on-Modules. However, with congatec offering two extremely attractive new options – for COM-HPC and next-gen COM Express – it's not easy to decide whether designs for the 11th Intel Core processor generation are best implemented with COM-HPC Client Size A or COM Express Compact. The congatec design decision guide 'COM-HPC vs COM Express', which is available at congatec's landing page for the current processor launch, helps to steer developers through the evaluation process.

Processor performance has vastly increased

The second reason is the significant performance boost. With up to 4 cores, the 11th Intel Core UP3 processor generation boosts performance up to 23 percent in single-thread applications and 19 percent in multi-thread applications compared to Intel Core Embedded processors of the 8th generation. Changes to the new core microarchitecture (Willow Cove microarchitecture) that affects performance includes a redesign of the cache and the optimization of the transistors compared to the direct predecessor (Sunny Cove microarchitecture). Even more important for embedded applications is the fact that high-speed Intel SoC processor technology is now for the first time available in Intel's SuperFin technology. Admittedly, it is generally argued that this is already the third Intel Core generation that has been developed based on 10nm transistors. In fact, the last two generations (SoCs codenamed Ice Lake and Cannon Lake) have not been equipped with Computer-on-Modules – at least not by the leading Computer-on-Module supplier congatec. Embedded users of Intel architecture who will be migrating from the 6th, 7th or 8th generation to the new UP3 variants of the 11th generation can therefore benefit for the first time from two distinct advantages offered by 10nm technology: Higher packing density; and lower power consumption at equal performance, or higher performance at equal TDP. Both aspects are key in embedded designs. By comparison, the new designs – which are available in 12, 15, and 28-Watt versions – bring significant performance increases to users.

Intel has also introduced a new L1 cache to further improve performance. It significantly lowers latency during data access and reduces the load on the L2 cache, which grew from 256 kB per core to 1.25 MB, and the L3 cache, which now has 50% more capacity with 12 MB. This significantly accelerates memory accesses to RAM shared with the GPU, bringing us to the third good reason for the new Intel SoCs – the GPU.

3x greater graphics performance is truly impressive

The 11th generation Intel Core processor launch also includes new Intel graphics. A lot has changed here as well: The GPU architecture, which Intel calls Iris® Xe Graphics, now benefits from the 10nm++ manufacturing process, too. This has led to a 50% increase in packing density, making it possible to

implement twice as many floating point operations (FLOPs) in the given space. At the same time, the consumption per FLOP was also reduced compared to the previous Gen 11 graphics.

Intel's Core family on congatec board

Gen	Year	Process	Core	Graphic	SoC
	2006	65nm	Conroe	–	Core 2
	2008	45nm	Nehalem	–	Lynnfield
1 Gen Core	2010	32nm	Westmere	Gen5	Clarkdale
2 Gen Core	2011	32nm	Sandy Bridge	Gen6	Sandy Bridge
3 Gen Core	2012	22nm	Ivy Bridge	Gen7	Ivy Bridge
4 Gen Core	2013	22nm	Haswell	Gen7.5	Haswell
5 Gen Core	2015	14nm	Broadwell	Gen8	Broadwell
6 Gen Core	2015	14nm	Skylake	Gen9	Skylake
7 Gen Core	2017	14+	Kaby Lake	Gen9 LP	Kaby Lake
	2017	14++	Coffee Lake	Gen9 LP	Coffee Lake
8 Gen Core	2018	14++	Whiskey Lake	Gen9 LP	Whiskey Lake
9 Gen Core	2019	14++	Coffee Lake	Gen9 LP	Coffee Lake Refresh
11 Gen Core	2020	10SF	Willow Cove	Xe-LP	Tiger Lake

Depending on the processor, Intel Iris® Xe Graphics now offers between 48 and 96 execution units (EUs). With this developers will benefit from a 2.95x performance increase compared to the what the Intel® Core™ Embedded processors of the 8th generation deliver*.

But how does this performance gain translate into direct benefits? First, platforms with Intel Iris Xe Graphics can now simultaneously supply up to four 4k displays with video signals at 12-bit color depth. With 8k resolution, it is still possible to control two displays in parallel. In terms of video outputs, the 11th Intel Core processor generation supports 2x eDP 1.4b as well as 2x direct display interfaces (DDI), which can be configured as DisplayPort 1.4 or HDMI 2.1 with HDCP 2.3 support. Additionally, 1x DSI is supported, and a video output can be routed via USB 4.0.

As for the offered multimedia features, digital signage OEMs, in particular, will be impressed by the two video decode (VD) boxes, which allow up to 40 video streams to be decoded simultaneously in UHD resolution (1080 p at 30 fps). Moreover, the VD boxes support the latest codecs, such as ultra data-efficient and computationally intensive HEVC (H.265) and VP9, as well as the widely used predecessors AVC (H.264) and AV1. All this is ideal for high-performance media servers and AV headend systems.

As far as inputs are concerned, 11th generation Intel Core processors offer four MIPI 4k CSI camera inputs. The video encode box ensures efficient on-the-fly coding in HEVC, VP9 or AVC. Of course, it's also possible to feed still images. In this case, the maximum resolution is a massive 27 megapixels. The received video signals can then be forwarded to the computing cores via the new IPU 6 image processing unit. IPU 6 ensures hardware-accelerated automatic processing of video streams, for example for object or person recognition. This is an important feature for vision and AI applications, which are a separate reason for the 11th gen Intel Core processors and will be discussed in detail later.

4th generation PCI Express puts the pedal to the metal

For many developers, support of the 4th PCI Express generation is likely to be an even more important reason than the CPU and GPU improvements. The 11th generation provides the first embedded x86 processors with native PCIe Gen 4.0 support. It offers the same data rates over 4 lanes as PCIe Gen 3.0 over 8 lanes, which are also available via the platform controller hub for the connection of additional peripherals. PCIe Gen 4.0 allows the transfer of 2,048 MByte/s per lane and direction. Since PCIe is full-duplex capable, a total of 4,096 MByte/s can be transferred when the forward and return channels are added.

The clock rate has doubled from 8.0 GHz for PCIe 3.0 to 16 GHz for PCIe Gen 4.0. This increase has a major impact on the system design as it presents carrier board developers with new challenges, especially in terms of signal compliance. The COM/carrier board connectors must also meet these requirements. The new COM HPC connector is specifically designed to meet the compliance requirements of these latest high-speed interfaces; it is even already certified for PCIe Gen 5.0 at 32 GHz. Such a clock rate is not achievable with the current COM Express connector; it would require enabling the Gen3 compatible mode of the bus. However, congatec has already equipped its modules with a next-gen COM Express connector that is mechanically fully compatible and electronically more powerful. This connector is designed to ensure the future long-term availability of COM Express. congatec will release exact figures on how powerful it is after extensive testing.

USB4 – the wonder weapon for high-speed plug & play

Besides PCIe Gen 4.0, the 11th gen Intel Core processors provide another highly innovative and powerful interface that is a fifth good reason for choosing 11th generation Intel processors: USB4. This new interface is based on the Intel Thunderbolt 4 protocol, so it's not surprising that Intel speaks of CPU-integrated Thunderbolt with USB4 support.

But what exactly does this mean? Here are the details: 11th gen Intel Core processors support up to 4x Thunderbolt 4 for USB4 integration. Each Thunderbolt port provides 4 PCIe Gen 3.0 lanes with a data rate of 32 Gbps or 4,096 MB/s in each direction. In addition, two of these ports can tunnel DisplayPort signals for 1x 8k or 4x 4k video signals with 10-bit color depth and a refresh rate of 60 Hz.

For a complete USB4 interface with external USB-C connector, these lanes must also be combined with up to four USB 3.1 Gen2 ports for the full USB4 data rate of 40 Gbps. Developers can further choose to implement USB power delivery (PD) interfaces on the carrier board via the USB-C subsystem; in that case, external devices can be supplied with up to 100 Watts via the USB PD pins of the USB-C connector. Unlike the serial Thunderbolt interface, which only allows daisy chaining, a USB4 implementation must support the familiar hub tree structure. Since the implementation of USB-C is not trivial and higher clock rates present further challenges, customers can always contact congatec's technical support team for assistance in the form of training, design guides or even full schematics.

More real-time in real time

The increase in CPU, GPU and key interface performance is complemented by a range of qualitative features that significantly expand the application field of the new 11th generation. More comprehensive real-time processor support for IIoT/Industry 4.0 applications is a particularly good example. Although not all new processors support ECC, some have integrated this feature to support in-band error correction for critical real-time computing applications. The in-band error correction code (IBECC) provides single error correction, while double error detection (SECDED) is provided at the 64-byte cache line level.

However, these days real-time no longer stops at the field control level thanks to the ability to connect digital and analog I/Os as well as real-time field buses and all kinds of proprietary industrial Ethernet

variants, which OEMs often connect via PCIe. Time sensitive networking (TSN), which now also enables tactile Internet applications over IP, is another attractive feature. The 11th generation offers integrated MACs that support TSN via 1 GbE and 2.5 GbE ports. congatec has been supporting TSN for quite some time and already offers development platforms that combine TSN networking with real-time control. Another innovative feature is Intel's new time coordinated computing (TCC) technology, which orchestrates the TSN Ethernet standard based on Intel IP also towards I/Os to reduce latency and minimize jitter in synchronous processes. It can be adjusted as necessary via the Intel® TCC Software Toolkit provided in the extended temperature variants of the 11th generation. Of course, hardware virtualization also plays an important role in such connected real-time systems, which leads us to the next good reason for the 11th Intel Core generation.

Virtualization support embedded in hardware

Real-time multitasking is an important requirement for IoT and edge devices, which the 11th generation meets with hardware-based virtualization support. This is an attractive addition for real-time hypervisor technologies such as those offered by congatec with the RTS hypervisor. It integrates seamlessly with the hardware capabilities of 11th gen Intel Core processors to run critical real-time applications – without additional latency – in parallel to other multi-purpose operating systems such as Linux and Windows. The 11th Intel Core processor generation supports single root I/O virtualization (SR-IOV) for this purpose. This allows multiple apps hosted in virtual machines with general purpose operating systems (GPOS) to natively access an I/O interface, e.g. one of the 2.5 Gbps Ethernet interfaces. This is a rather attractive feature, especially because these interfaces are often in short supply.

The primary function of virtualization is the consolidation of numerous tasks on a single system. In next-generation industrial control systems, the number of tasks is multiplying rapidly today because on top of site control, they are now often also required to interact with each other in real time. In addition, IIoT-based data exchange is needed to monitor distributed machines, optimize the performance of assets, and introduce new business models with predictive maintenance and as-a-service offerings. Many applications also require the integration of vision-based artificial intelligence, which leads us to the next important reason for the 11th generation Intel Core processors.

Machine vision and artificial intelligence

Machine vision and learning will become even faster, more efficient, and easier to implement with the new Intel Core architecture. Faster simply because of the significantly greater number of graphics EUs. The Intel UHD 620 graphics of the comparable Intel® Core™ i7-8665UE processor from the Whiskey Lake family, for instance, achieves 441.6 GFLOPs at a maximum clock speed of 1.150 MHz

The workload consolidation kit for vision-based situational awareness applications from congatec, which is Intel-qualified as a production-ready Intel® IoT RFP Ready Kit, demonstrates the efficiency benefits of virtualization. It offers three virtual machines (VMs) for workload consolidation of vision applications based on hypervisor technology from Real-Time Systems (RTS). One VM runs a vision-based AI application using Intel® OpenVino® software for situational awareness. The second VM is real-time capable and operates deterministic control software, while the third VM acts as IIoT/Industry 4.0 gateway. The congatec kit, which was developed in cooperation with Intel® and RTS and can also be made available with the 11th Intel® Core™ processor generation, targets the next generation of vision-based collaborative robotics, machine controls and autonomous vehicles that need to perform multiple tasks in parallel, including situational awareness based on deep learning based AI algorithms.

with simple accuracy (8bit*2 per clock * 24 EUs * 1.150 GHz = 446 GHz). The new Intel graphics offers a lot more; since two generations were left out, the performance leap is considerable. The Intel Iris Xe Graphics of the 11th generation Intel Core processor family offers AI applications a full 1996.8 GFLOPs thanks to its 96 EUs and a higher possible clock rate of 1.3 GHz.

AI and deep learning inferencing are also executed significantly faster on CPU cores of the 11th gen Intel Core processors. That is because the new processors support the highly efficient AVX-512 instruction set for powerful 512-bit vector operations. Thanks to additional vector neural network instruction (VNNI) support, there are now four new instructions available for AVX 512, with VPDPBUSD/S for INT8 and VPDPWSSD/S for INT16. VNNI combines three instructions into one, and INT8 operations are massively accelerated to 128 executions per clock and core.

OEMs can easily exploit these performance gains for machine vision and deep learning information with the OpenVINO™ toolkit. It includes the Intel® Deep Learning Deployment toolkit, optimized OpenCV and media encoding/decoding routines, as well as 20 pre-trained models and code samples. An efficient way to get started with computer vision and OpenVINO is the congatec workload consolidation kit for vision-based situational awareness applications, which was introduced in the previous reason.

Better safe than sorry

IIoT connected edge devices are not complete without effective security features. Ideally, the foundations are already anchored in the hardware. Here too, 11th generation Intel Core processors offer a clear advantage. The additional security features are therefore the ninth reason why OEMs should choose the 11th generation for their distributed and mostly unattended IoT devices.

The three most important truly new hardware-based security measures are: total memory encryption (TME), control-flow enforcement technology (CET) and key locker. They help protect systems and system data in the event of hardware and network vulnerability attacks or physical theft.

- **Total memory encryption (TME):** TME uses a hardware-based, highly secure AES XTS encryption engine that sits in the direct data path between the processor and the external memory busses. This enables on-the-fly decryption and encryption of all incoming and outgoing data to the System-on-Chip – including the graphics unit –with a 128-bit key. Even if attackers remove storage media and install them on another system to read their contents, they will only see scrambled data.
- **Control-flow enforcement (CET):** Some 90% of all software-based attacks use techniques such as return oriented programming (ROP) or jump oriented programming (JOP) to capture data via browsers or malicious software applications. CET offers two security functions to prevent this: First, CET detects and prevents data flow triggered by malicious code execution. Second, CET detects and prevents malicious indirect jump calls or jump oriented programming in the executed software. This prevents the execution of malicious code, which – for example – has infiltrated the computer via manipulated emails.
- **Key locker**: This hardware-based micro handler protects encryption keys with the new AES-NI command 'ENCODEKEY' and offers faster encryption and decryption than previously available technologies. Data can only be decrypted with the key locker and application key. This way, even encryption keys that are held in memory by the application software are effectively protected against malicious attacks.

Industrial and IoT

The tenth reason for 11th generation Intel Core processors is absolutely key for most embedded applications: It concerns the industrial (0°C to 100°C TJMax) and extended temperature range.

Depending on the design, the 11th generation supports temperatures from -40°C to +100°C TJMax, which enables outdoor applications and serves a maximum spectrum of applications. The industrial-grade processors are robust enough for a long service life, even if systems are in full 24/7 operation for years. Another feature that is inseparably linked with embedded is the long-term support of the processors, with Intel currently promising 15 years of availability. Because the company has control over its own production, it cannot be surprised by other companies discontinuing a specific transistor size.

Management system for distributed applications

The 11th and for the time being the final reason for the new 11th generation are the more advanced remote management functions that will become available with the launch of the new congatec modules. Such functions are becoming increasingly important for IIoT-connected applications. congatec offers dedicated APIs and a board management controller that can be integrated on the carrier board. This functionality is complemented by integrated Intel vPro functions such as active management technology, which enables end-to-end out-of-band management independent of the operating system (OS). It allows a wide variety of system problems to be resolved even if a system's OS is not working. For example, IT administrators can remotely repair drivers, application software or the OS of unresponsive or unbootable systems, or use KVM control features for OS upgrades or BIOS startup. Of course, they can also remotely isolate compromised systems from the network to help contain the spread of infection.

The upcoming COM-HPC launches will also deliver an enhanced remote management interface based on the PICMG specifications. This interface is currently being developed in the PICMG Remote Management Subcommittee. The goal is to make a reduced portion of the complex intelligent platform management interface (IPMI) feature set available for the remote management of edge server modules. Like the PCI Express slave function, COM-HPC will also provide extended standardized remote management functions to communicate with the modules. OEMs and users will be able to easily ensure the reliability, availability, maintainability, and security (RAMS) that is common to servers. This functionality is individually expandable via the board management controller to be implemented on the carrier board. This provides OEMs with a consistent basis for remote management, which they can modify as required.

COM-HPC and COM Express processor configurations

congatec now offers this impressive feature set for the new Intel Core i7, i5 and i3 processors in two attractive options: COM-HPC Size A and COM Express Compact. All relevant industrial and embedded computing processor variants are supported by congatec. All are BGA variants and compatible with commercial motherboard technology. Also handy is the configurable TDP of 12, 15 to 28 Watts, which allows strict thermal limits to be met with very little configuration effort.

Processor	Cores/ Threads	Frequency at 28/15/12W TDP, (Max Turbo) [GHz]	Cache [MB]	Graphics Execution Units	Ext. Temperature range
Intel® Core™ i7-1185G7E	4/8	2.8/1.8/1.2 (4.4)	12	96	-
Intel® Core™ i7-1185GRE	4/8	2.8/1.8/1.2 (4.4)	12	96	yes
Intel® Core™ i5-1145G7E	4/8	2.6/1.5/1.1 (4.1)	8	80	-
Intel® Core™ i5-1145GRE	4/8	2.6/1.5/1.1 (4.1)	8	80	yes
Intel® Core™ i3-1115G4E	2/4	3.0/2.2/1.7 (3.9)	6	48	-
Intel® Core™ i3-1115GRE	2/4	3.0/2.2/1.7 (3.9)	6	48	yes

The feature set in detail

The conga-HPC/cTLU COM-HPC Client Size A module and the conga-TC570 COM Express Compact module are available with various Intel® Core™ processors from the 11th Gen Intel Core processor roadmap. They are the first to support PCIe x4 Gen 4 for connecting external peripherals with the highest bandwidth. In addition, developers can also use 8x PCIe 3.01 lanes. The COM-HPC module offers 2x USB 4.0, 2x USB 3.2 Gen 2 and 8x USB 2.0 interfaces; the COM Express module offers 4x USB 3.2 Gen 2 and 8x USB 2.0, compliant to the PICMG specification. COM HPC provides 2x 2.5 GbE, COM Express 1x GbE; both offer TSN support. Sound is provided via I2S and SoundWire in the COM-HPC version, and HDA in the COM Express modules. Comprehensive board support packages are provided for all leading RTOSes, including hypervisor support from Real-Time Systems as well as Linux, Windows, and Chrome.

For more information please visit congatec's 11th Gen Intel Core processors page: https://congatec.com/11th-gen-intel-core/

More information about the new conga-HPC/cTLU COM-HPC Client module is available at www.congatec.com/en/products/com-hpc/conga-hpcctlu/

More details about the conga-TC570 COM Express Compact module can be found at www.congatec.com/en/products/com-express-type-6/conga-tc570

Author:

Andreas Bergbauer,
Product Line Manager at congatec