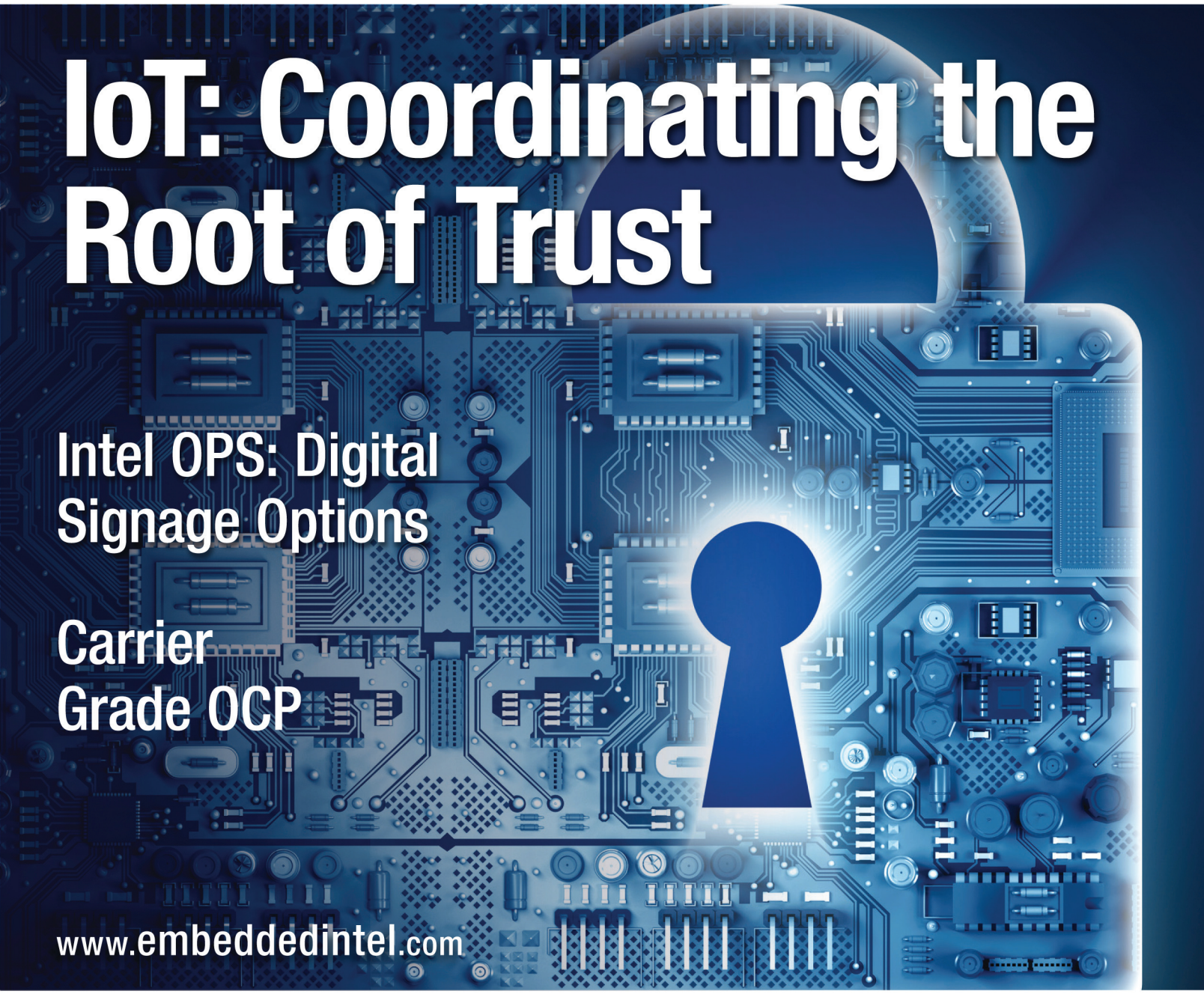
Extension MEDIA

Embedded Intel® Solutions

Fall 2017



IoT: Coordinating the Root of Trust

Intel OPS: Digital Signage Options

Carrier Grade OCP

www.embeddedintel.com

Gold Sponsors

congatec

Portwell

SUPERMICRO

WinSystems® The Embedded Systems Authority

X-ES

"We have to coordinate that root of trust": Q&A with WinSystems

Why right sizing is a part of securing the IoT

By Anne Fisher, Managing Editor

Editor's Note: This spring saw publication of the Industrial Internet Connectivity Framework by the Industrial Internet Consortium (IIC), of which Intel® is a founding and contributing member. Intel's involvement at that level in an organization striding purposefully toward "a trustworthy IIoT in which the world's systems and devices are securely connected and controlled....[1]" is a role well understood by WinSystems, with roots firmly in industrial computing, and now branched to the MIL-COTS, energy, transportation, and automation verticals as well.

Understood too is embedded designers' ongoing need for information as threats to IIoT security persist. "We have a strong relationship with Intel, and can help our customers understand the security measures that exist and Intel's security roadmap for the IoT on all the device levels that are available," T.J. Smith, WinSystems' Technology and Engineering Director, tells EECatalog.

"On a regular basis, we help customers understand what is coming, what the timeline is, and how to implement toward their needs as well as enabling all of the broad features that Intel has brought to the table—because every chip that Intel brings to the table has new IoT features and improved security," Smith adds.

EECatalog *spoke with Smith and George T. Hilliard, Director of Technical Sales, WinSystems, about the Industrial IoT and security recently. Edited excerpts of the interview follow.*

EECatalog: What's important for someone targeting Industrial IoT applications to know about the elements supporting "Secure and Trusted Data" in a product like WinSystems' PX1-C415 SBC? [Figure 1]

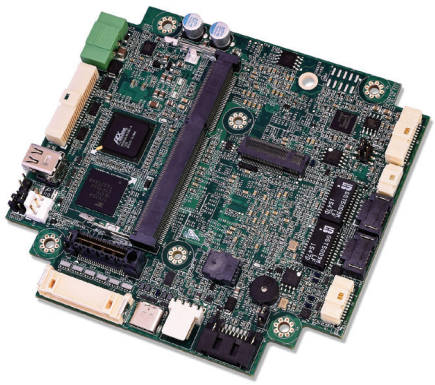


Figure 1: A PC/104 form factor SBC with PCIe/104™ OneBank™ expansion, the PX1-C415 single board computer from WinSystems includes the latest generation Intel® Apollo Lake-I E3900 SOC processor.

George T. Hilliard, WinSystems

George T. Hilliard, WinSystems: From a systems-level perspective, it's key to design and plan for security upfront. I still often see that folks will look at the feature set first and then get down the road before they start thinking about how they are going to secure the system. Then they have to do some redesign. That's sometimes a missing element

1. https://lwn.net/Articles/506761/

out there. A secure way to start is with the root of trust and the platform itself. And that's where we come in as an embedded systems provider. We give customers a hardware platform where they can create that root of trust using Intel or other CPU products and have that space as a starting point for the security. Addressing security in parallel with application development and design speaks to the customer's bottom line. By using this approach, he can minimize risks and control costs rather than going back at some point and having to redesign.

T.J. Smith, WinSystems

T.J. Smith, WinSystems: As soon as you realize that your product has value, you need to understand how you are going to protect that value. So, you have to do an assessment very early on in the product life cycle.

It's also possible to oversize or overdevelop on security. One of the things we target with our customers is how to right size their security. You need to understand the value of what is being protected and put the appropriate measures in place to address that security now and into the future. What will need to be monitored? What will need to be adapted 10 years down the road?

EECatalog: How have some of the actions taken by Intel in the past couple of years, including licensing decisions, affected the solutions WinSystems is developing for its customers?

Smith, WinSystems: Longevity is very important. Intel has been strongly promoting its longevity and has been making licensing decisions based on that. When you go into deployment, you have to understand not just security today, but security tomorrow. How are you going to make sure that two years down the road the millions of the products you've deployed into the field don't suddenly become vulnerable with no cost-effective way to repair them? The advanced decisions involve understanding what a proven framework can do and how WinSystems and Intel and the different software and security layers play together to give you a secure yet flexible, adaptable, solution for your IoT products without going through the roof on costs.

Hilliard, WinSystems: In the embedded space, which has now morphed into what everybody is calling the IIoT, Intel's acquisition of McAfee and VxWorks shows its commitment to embedded systems platforms. We are seeing these technologies picked up into the consumer products, which is encouraging in that it can flow back into our area as well. And I think the fact that Intel has focused on including more of the hardware security into its chipsets is also a positive sign and helps us to set the platform for the root of trust.

EECatalog: How do you assure various security elements complement one another in an SBC?

Hilliard, WinSystems: We give the choice to the customer. For example, customers can add a Trusted Platform Module (TPM) and take advantage of secure boot and other features, such as the integrated Intel security engine and ECC memory, which gives you a more reliable RAM for your device, and helps you protect it from a forced reset vulnerability, for instance. As Jack [T.J.] notes, they can right size that security solution for the application, and that is where their planning and expertise are going to come in.

Smith, WinSystems: Exactly. The platform is designed from the start to enable, but not require, all levels of encryption and security. A strong level of security requires a good root of trust. And where that root of trust resides is an important decision between us, the designer and manufacturer of the hardware, and the consumer, the integrator, and their development of their application. We have to coordinate that root of trust. Our hardware is capable of providing a hardware root of trust. We can also enable any of the variety of layers that are well integrated with the Intel platform. The Apollo Lake platform provides a generous helping of security capabilities. The application author and system integrator have an awful lot of options for developing security. We support them through that decision process; we support them through that implementation process. And we definitely support them through the production and manufacturing ramp into volume.

EECatalog: Please comment on the Industrial Internet Connectivity Framework (IICF).

Smith, WinSystems: I like the direction the IICF is headed. It's reached critical mass at this point and will be effective. The IICF defines a wonderful selection of reference architectures and frameworks to apply to basically any IIOT application. They are helping drive interoperability in the space so that developers can integrate layers even if they are from different vendors. This is particularly helpful to WinSystems and our IIOT ecosystem partners as we help our customers get their products to market.

Hilliard, WinSystems: The [Industrial Internet Consortium] IIC is involved in the standards, but they are not trying to set the standards so much as to get individual standards to talk to each other. With all these big installed bases for industrial control—there are so many different protocols on industrial Ethernet, for example—they are trying to find ways for all of these platforms to talk to each other and then be able to transfer that data at different layers at a higher level. It's going to be beneficial long term, but I don't think we're really seeing the structure around it yet, although publishing the Industrial Internet Security Framework[2] is going to go a long way toward that.

2. Industrial Internet of Things Volume G4: Security Framework IIC:PUB:G4:V1.0:PB:20160926. Published in 2016

EECatalog: With regard to IIoT security as well as for other elements, the model referenced is often that of layers—will this model continue to work?

Smith, WinSystems: Yes, the layered model has been shown to be effective and beneficial for over 30 years in the networking arena. Applying this model to security and the IIOT provides a similar abstraction from the complications and details that each layer provides. This allows customers to quickly integrate security features from trusted partners while maintaining focus on their own special requirements.

For example, if we integrate a security layer from a trusted partner like Intel McAfee, the system security will be improved without much extra complexity or burden to the customer.

WinSystems has a very similar role. We build very trustable hardware. We put on top of that very trustable BIOS; we put on top of that very trustable security layers, network layers, and Board Support Packages [BSPs] and Operating Systems all the way up into where the user runs their specific application. One of the benefits the layers model gives us is that users can almost be a la carte with what they do and don't need. If they don't need a secure network layer from us, then that can be provided through their own existing capabilities. Depending on whether they need, for example, a unique identification key for each board or a shared key for each board or for their family of boards, we can abstract that in a different layer of security. Yet the layers above and below don't have to change dramatically.

The layered models give you the flexibility to adapt to the various needs of a customer without having to start over and redevelop everything. There are substantial benefits there in terms of speed of execution, speed of production, re-using tested code, and cost efficiency.

EECatalog: What tools and practices need to be developed today to keep the "things" of the Industrial Internet of Things secure?

Smith, WinSystems: One of them is system management. When you have devices in the field you have to have a way to manage them. Depending upon the requirements, this could be aggregated to a single pane of glass cloud-based solution or it might have to be an on-site hands-on management-based solution.

We know that the closer you have to get to a device, the more it costs. If you have to go up and service the device at the top of the windmill, it costs more than if you can do it from your browser, so remote system management is very important.

Security detection is also very important. You need to have some level of monitoring to understand when an attack or breach has occurred. There is a tremendous amount of malware in the world, detection of that is going to be an ongoing problem for decades to come.

Finally, once you detect an issue, you have to be adaptable enough to correct the problem. You have to be able to correct problems and restore the system to a trusted state. That can be something as simple as changing passwords or as complicated as pushing a complete new software image, a more secure, not corrupted software image into the device remotely.

Security needs to be included early, right-sized, and cost-efficient because it will require attention for the life of your product. If you deploy security measures and think you're done and out the door, and you're forever secure—Well, there's no such thing as forever secure.