IoT Standards Enable Interoperability

By Kenton Williston, Roving Reporter (Intel Contractor), Intel® Internet of Things Alliance

The Internet of Things (IoT) promises a future where everything is online. But today, a lack of standards makes it difficult to connect. To learn how developers can solve this problem, I spoke with three industry experts:

- Jens Wiegand, CTO of Kontron, a Premier member of the Intel® Internet of Things Alliance (Intel® IoT Solutions Alliance)
- Ido Sarig, Vice President and General of IoT Solutions Group at Wind River, an Associate member of the Alliance
- Tony Magallanez, OEM Systems Engineer at McAfee, an Associate member of the Alliance

Below are key excerpts from my interviews. For more information, see my full interviews with Kontron, Wind River, and McAfee.

What are the biggest challenges to deploying IoT solutions?

Jens Wiegand, Kontron: Currently the market is fragmented and characterized by incompatible systems and stovepiped solutions. IoT concepts like predictive maintenance, big data, and analytics require a holistic approach, but there is a lack of cooperation between hardware and software suppliers, service providers, and communication infrastructure vendors.

Ido Sarig, Wind River: Much of the industry's effort is focused on connecting legacy or "brownfield" devices that were not designed to be connected and even designed to make connectivity difficult in order to protect them from network-borne threats. Developers must figure out not only how to connect brownfield devices but how to safely connect them.

Another challenge is the lack of a single standard for connecting to networks. Many brownfield devices use proprietary protocols and will require gateways to connect with IP-based networks. And if they are already IP-based, they may be using a wide variety of protocols. Developers will need to be able to build gateways that support virtually any communication protocol.

Tony Magallanez, McAfee: The major problem we see is the security of these devices. These devices tend to be not manned but often handle personally identifiable information. The question is how you protect the data both while it's on the system and while it's being transmitted between devices.

How can developers address these issues? In particular, how do standards and multi-vendor solutions help?

Jens Wiegand, Kontron: Developers should strive to build on solutions that adhere to industry standards on all levels, from communications protocols to cloud connectors. In particular, they should seek standards that are supported by multiple industry leaders in form of application-ready concepts. Such standards can reduce complexity and risk, and provide a time to market advantage.

Ido Sarig, Wind River: Delivering secure and reliable IoT solutions requires an end-to-end view that encompasses the endpoint device, the connectivity layer, the gateway, and the application running in the cloud. For example, security challenges need to be factored in at every level. Virtually every known type of hardware and software security measure comes into play in IoT. Secure booting at the device level, access control and authentication, application whitelisting, and firewalls and intrusion prevention systems are just some of the tools at hand to respond to security threats.

The benefits of the IoT have been thus far constrained by the complexity of issues like this. As standards coalesce, market needs and business cases become more sharply defined, and operators and device manufacturers are freed to focus on the true value they can deliver: innovative new services and applications.

What role do you see for standards bodies like the new Industrial Internet Consortium (IIC)?

Jens Wiegand, Kontron: The IIC as well as Industry 4.0 are good examples where a consortium of industry leaders drives towards a common goal: enabling business value for end customers by implementing standards and by developing the ecosystem to enable solutions.

Ido Sarig, Wind River: Organizations such as the IIC bring together expertise and the tools to bring smart connectivity, high security, and manageability to the market. These consortia will help expedite the realization of the IoT through specialized skills and expertise required to build intelligent devices which typically reside outside the core competency of operators and device manufacturers.

Tony Magallanez, McAfee: Most people understand that they need security, but in many cases they lack expertise –and in far too many cases they end up doing nothing if they don't have to. That's where I see consortiums or standards-based organizations driving security.

Talking specifically about IIC, its recommendations are likely to overlap with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) recommendations. But one of the great things about these consortiums is that they go further than the regulations require. For example,

they may recommend things like application whitelisting. In the regulatory bodies, whitelisting is still a bit of an outlying technology. So these standards bodies can help developers not only achieve compliance but also true security.

So how do you comply with these regulations? Typically, OEMs or ODMS have taken a buy or build mentality. However, it's very difficult to build your own security infrastructure. So it's wise to get help from vendors who are experts in security, and ask these security solution vendors to make sure the systems are secure.

What role do you see for ecosystems like the Intel® IoT Solutions Alliance?

Jens Wiegand, Kontron: The Alliance is a great example of a large scale ecosystem that enables rapid deployment with IoT solutions that are pre-integrated, verified, and validated by system integrators and solution providers like Kontron. The benefits for our customers are flexibility, choice, velocity, and the ability to focus on the development of innovative applications with less risk and pain.

Tony Magallanez, McAfee: Alliance members will help provide the components to meet regulatory recommendations or requirements. They will give you the building blocks to get you to compliance and beyond. Without these groups, you will have different OEMs/ODMs and device owners all struggling to define what the security should look like. Not being security experts, they can miss out on some of the security opportunities.

How you are using standards and ecosystem collaboration to create IoT solutions?

Ido Sarig, Wind River: As part of Intel IoT Group, Wind River is collaborating with Intel on solutions like the Intel® Gateway Solutions for the Internet of Things (Intel® Gateway Solutions for the IoT), which serves as the software backbone for intelligent gateways. It is a complete software development environment that provides pre-integrated and fully tested ready-to-use components to secure, manage, and connect intelligent gateways.

Tony Magallanez, McAfee: What we are doing with the Intel Gateway Solutions for the IoT is providing a platform that will allow OEMs/ODMs to establish a base level of security and functionality in the device without having to do a lot of the development on their own. In addition, the hardware that's built in gives them a starting point that is easier than taking a huge SKU sheet and picking out the components individually.

Jens Wiegand, Kontron: The Intel Gateway Solutions for the IoT is a good example of how Kontron builds on industry standards and capitalizes on the work of the Alliance by leveraging platform concepts to create IoT-enabled hardware and software stacks. [Editor's note: Kontron recently announced the Intel® Gateway Solutions for the IoT-based KBox A-201 mini.] But even more, we strive to develop standards further, grow the ecosystem, and offer more value to our customers with IoT solutions that enhance the reach of our application-ready platforms. We see solution- and application-readiness as well as software expertise as key differentiators and innovation enablers.

Kontron is a Premier member of the Intel® IoT Solutions Alliance. McAfee and Wind River Systems are Associate members of the Alliance.

This article first appeared in the Intel® Embedded Community, published by the Intel® Internet of Things Alliance.