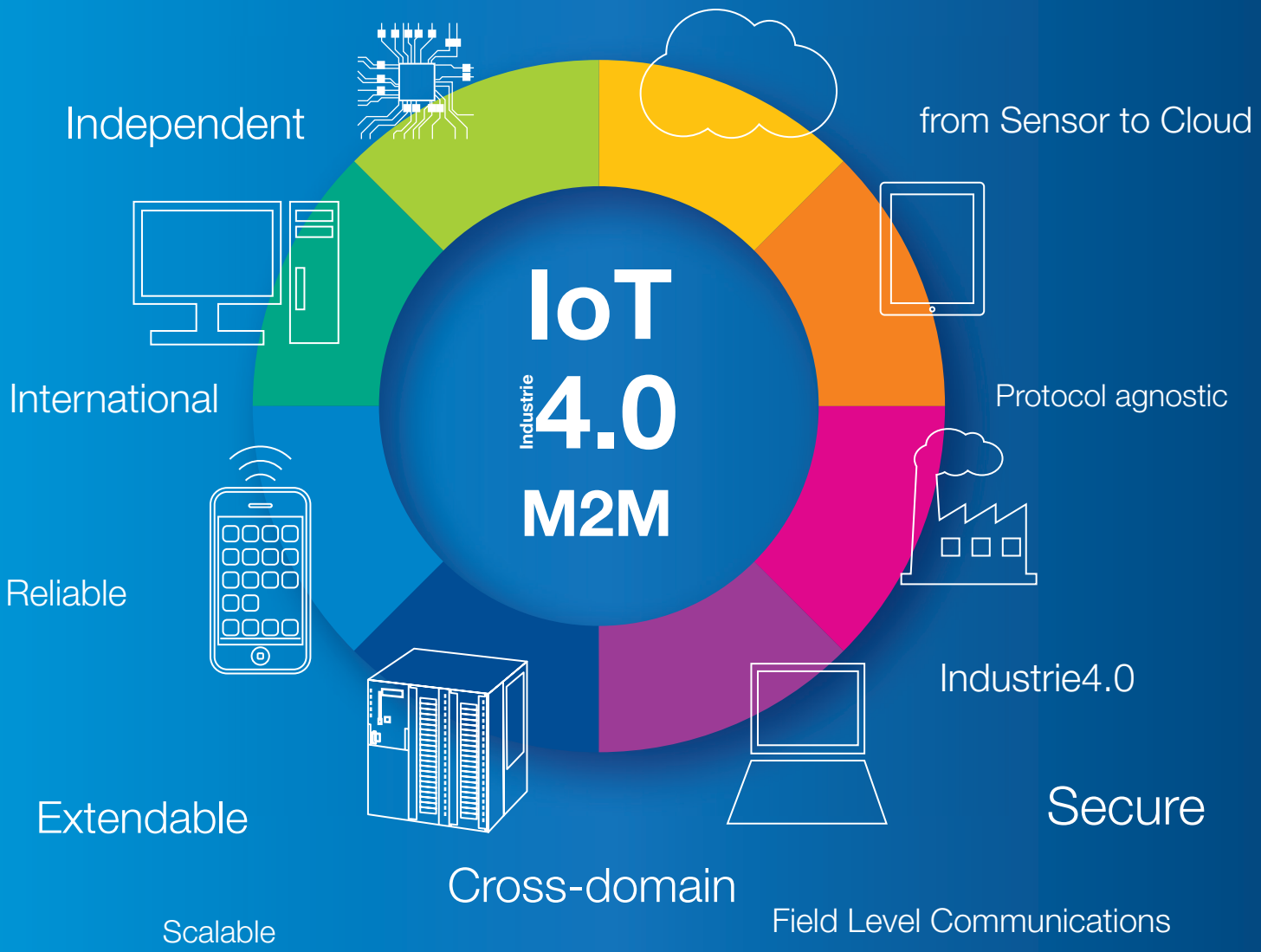
The Industrial Interoperability Standard

OPC UA Users and Experts – Conveying Knowledge and Experience

Third Edition
September 2021

The OPC Foundation publishes a series of interviews with experts, market leaders and think tanks in communication, automation and industrial IT to highlight the benefits and the potential of the OPC UA technology for end users, system integrators, operators in the world of industrial IoT.



Contents

OPC EXPERTS PODCAST

OPC Foundation Podcasts are available on different distribution channels like …

Spotify **iTunes** **Google** **your computer**

For any further questions please send an email to office@opcfoundation.org and let's stay in touch.

OPC FOUNDATION

www.opcfoundation.org

SPS 23 – 25.11.2021
OPC Booth Hall 5 – 140

NEW – NOW AVAILABLE
OPC UA FOR FLC BROCHURE
www.opcfoundation.org/FLC

Factory Automation

First Live Demo: November 2021

OPC UA for Field eXchange

A Sole OPC UA Solution for Factory and Process Automation

Process Automation

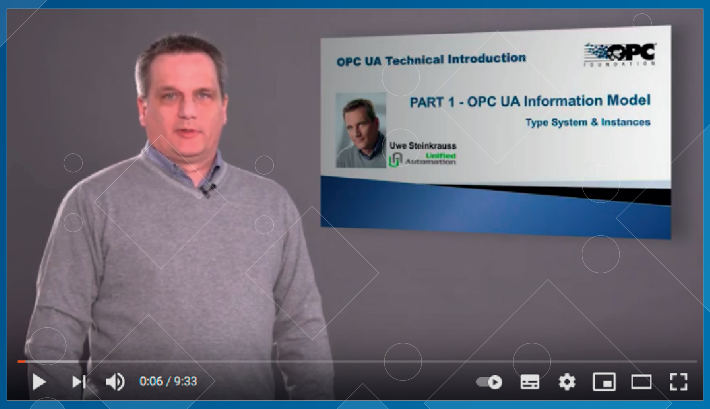
© metamorworks – shutterstock.com

ABB · BECKHOFF · rexroth A Bosch Company · B&R · CISCO · EMERSON · FESTO
hilscher COMPETENCE IN COMMUNICATION · HIRSCHMANN A BELDEN BRAND · HUAWEI · intel. · kalycito creating a difference · KUKA · Lenze
MITSUBISHI ELECTRIC · molex · MOXA · MURR ELEKTRONIK stay connected · OMRON · PHOENIX CONTACT
PILZ THE SPIRIT OF SAFETY · Rockwell Automation · Schneider Electric · SIEMENS Ingenuity for life · TTTech industrial · WAGO · YOKOGAWA

OPCFoundation YouTube Channel

https://www.youtube.com/user/TheOPCfoundation/videos

Learn more about OPC technology with these free webinars and videos provided by the OPC Foundation and its members.

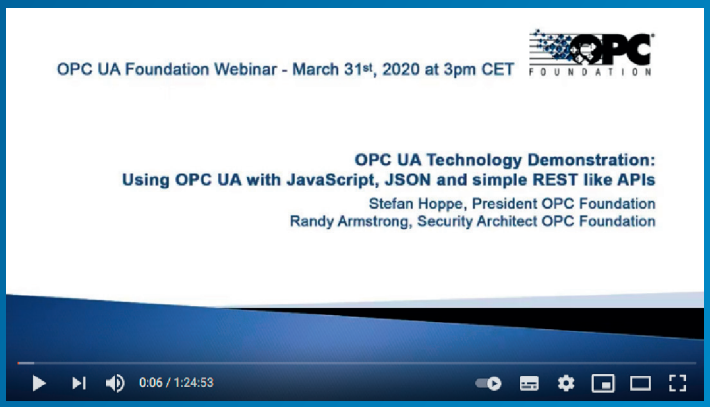


Listen to short technical OPC UA explanation videos by **Uwe Steinkrauss,** CEO of Unified Automation

- OPC UA Concept **https://youtu.be/E2XJfmAEdqw**
- OPC UA Transport **https://youtu.be/E2XJfmAEdqw**
- OPC UA Security **https://youtu.be/z4zNgNdauLY**
- OPC UA Profiles **https://youtu.be/CCvlLASACjE**
- OPC UA Discovery **https://youtu.be/1NlbUAlOdcA**

Security is a key requirement in a digitalized world. OPC UA is not only “secure by promise” instead the open source framework has been rewieved by international security experts.
Listen to **Randy Armstrong,** chairman OPC UA Security team about the multiple built-in by design security concepts and features.

- **https://youtu.be/pa82WydVtPY**



Did you know that OPC UA already has built in REST-like API? Remember OPC UA is not just a protocol – instead OPC UA is transporting standardized information via different protocols like UDP, TCP, MQTT, AMQP, … and will be extended with APL, TSN, 5G, WiFi6 and more. Follow Randy Armstrong and his hand on lab demo how to handle (get/put) data via REST API inside OPC UA

- **https://youtu.be/fiuamY0DzLM**

Welcome to new edition

OPC UA, MQTT, and Information Interoperability

By Randy Armstrong and Michael Clark

In earlier times, OPC learned a hard lesson that tying a specification to a specific wire protocol leads to obsolescence as technology evolves. This is why OPC UA has layered architecture, which makes it possible to create mappings for any number of transports like JSON HTTP or UA TCP for Client/Server and MQTT or UA UDP for Pub/Sub. When OPC releases a specification, they try to provide mappings for what the market has initially indicated they want, only to find that sometimes the uptake may be diminished (e.g., AMQP). The power of OPC UA is that these mappings can be quickly modified to implement new mappings that better match market needs (e.g., MQTT). When a future technology emerges, a such as QUIC/HTTP3, OPC UA is ready.

The reason protocols can be added as needed is because the value of OPC UA comes from information interoperability, which exists no matter what protocol is used to communicate. OPC UA provides a standard framework for describing information that can be accessed by Client/Server or Pub/Sub. This enables a level of plug-and-play between applications from different vendors that cannot be achieved by simply standardizing the message format and topic tree. This is particularly true for cloud-based applications that need to integrate data from many sources.

This is why Erich Barnstedt, Chief Architect, Standards & Consortia, Azure IoT at Microsoft, shared that, “One of the questions I get quite a lot is “should I use OPC UA or MQTT to send industrial data to the cloud?” My answer is always the same: Use both! OPC UA for the payload and MQTT for the transport. Let me explain:”

“First of all, comparing the two technologies is an apples-to-oranges comparison, as OPC UA is an application while MQTT is a protocol. It is like asking: “Should I use web pages or the Internet Protocol for my website?” I think you get my point...”

The emphasis on the need for information interoperability was also why the OPC Foundation and CESMII joined forces to create the OPC UA Cloud Library, which enables the publishing and discovery of standardized OPC UA Information Models as a component of the Smart Manufacturing Innovation Platform and Profiles. In their July 2021 press release, CESMII stated, “The key to new levels of innovation and performance will only be achieved when information, and associated context, can flow freely in the enterprise, to users and applications that need that information.” Delivering reusable Information Models is a strategic component of the Cloud Library.

The protocol independent architecture of OPC UA also allows for synergies between applications that would not necessarily have anything in common. For example, all of the major automation vendors are investing heavily in OPC Foundation’s Field Level Communication (FLC) initiative, which is based entirely on UA Pub/Sub using UDP. For these applications, MQTT simply cannot provide the capabilities that the controller-to-controller FLC applications require. On the other hand, the UA Pub/Sub infrastructure developed for FLC will enable connectivity to the cloud via UA Pub/Sub over MQTT because the overall architecture and configuration model is the same. This, in turn, will mean a lot of OPC UA commercial off-the-shelf (COTS) products will be available that can push data to the cloud via UA Pub/Sub over MQTT. In the long term this means a much greater selection of products will be available to factory owners that need to connect their factories to the cloud.

This emphasis on information interoperability and protocol adaptability makes OPC UA the best long-term solution for any factory owner looking to leverage MQTT and a means to connect their factories to the cloud.

JIM LUTH,
System Architect for Schneider-Electric and the CTO of the OPC Foundation.
jim.luth@se.com

OPC UA: THE PAST AND THE FUTURE

IN THIS SECTION: Learn from an interview with Jim Luth who is a System Architect in Process Automation R&D at Schneider Electric and is the CTO of the OPC Foundation. He will discuss the past and the future of OPC UA and his role as OPC Foundation CTO. We'll have conversations about OPC UA revisions and versioning, about MQTT, about big-data, and where he sees OPC UA becoming adopted.

Jim, please introduce yourself to our readers. Tell us about your role at Schneider Electric and your role at the OPC Foundation.

LUTH: I'm currently a System Architect at Schneider Electric and, although most system architects work largely on products, I'm more focused on standards, with OPC being one of the big standards in which I participate.

My role at the OPC Foundation is that I'm currently the Chairman of the OPC UA Working Group. In addition to my title is as CTO, I'm also a member of both the Technical Advisory Council and the Technical Control Board.

My career started in the 70s. It's been entirely focused on automation; first with General Motors and then later with Taylor Instruments, which is now ABB; then for the Foxboro Company, which became Invensys and Schneider Electric; I participated in a bunch of small startups; I worked for ICONICS, which is now part of Mitsubishi Electric; and along the way, I focused mostly on software.

I taught myself, object-oriented programming and became a free-lance consultant, bringing object-oriented programming into many different organizations. You'll actually see a lot of object-oriented concepts in OPC UA.

CLARK: Sounds great. So, how does one get a title of CTO?

LUTH: Well, yeah, that's an interesting one and it is really very much a title. Such a title is bestowed by the Board of Directors of the OPC Foundation and, essentially, I gained that title by being a consistent volunteer over many, many years. Since 1997, I've been active in working groups, writing sample code, and driving the vision forward for the OPC Foundation – and that continues today.

You know, part of my work is getting other volunteers to help share the load – I certainly don't do it alone, although I've been called by others, "the father of OPC UA" for my role in bringing this all together.

CLARK: So, you've been the chair since 1997 and had, perhaps, even some involvement before then. With OPC UA now being at revision 1.04, when might we anticipate seeing version 2.0?

LUTH: Well, hopefully never!

One of the things that we've done with OPC UA is that we've tried to make it so that we wouldn't have any breaking changes. The day we decide we're going to create Version 2.0, by our own rules, it would mean that there's a discontinuity – or a breaking change – between version 1.x and version 2.0. Over the 17 years of existence of OPC UA, we haven't had any of those kinds of breaking changes. Instead, we work on incremental changes. We work on different underlying protocols or security enhancements or features. But we do this all in a way that the oldest versions of version 1.0 of OPC UA can connect to the version 1.04 and vice versa. Except for the difference in functionality, they all work correctly.

CLARK: So, those companies that jumped on the bandwagon at the very beginning – using Version 1.0 – they can still use that first implementation today with, as you said, the exception of any additional features that have come along since the beginning?

LUTH: That's right; although we, of course, hope that our vendors, incrementally improve their products and adopt the newer versions. They can do so on their own schedule, without being impacted by

external pressures. The OPC Foundation will never say that, “if you don’t make this fix by next month, nothing is going to work and your products won’t work with other, newer products.” We’ve never hit those kinds of walls with OPC UA. It’s made it very acceptable to the marketplace. The last thing vendors want is to be on some hamster-wheel, trying to keep up with changes for the sake of change.

CLARK: So, Version 1.xx will never be finished?

LUTH: Yeah, that’s my plan, or at least until I retire. You know, UA was really designed in a layered way, knowing that technology would change. We wanted to produce the specs in a way that we could adopt newer, underlying technologies, without breaking the outer design of UA. We’ve been quite successful with that.

A good example is security algorithms. We knew from the get-go that we’d have to put them into the spec; but we know that security algorithms get cracked over time. We deliberately created a way to incrementally enhance security algorithms and deprecate old ones without breaking anything.

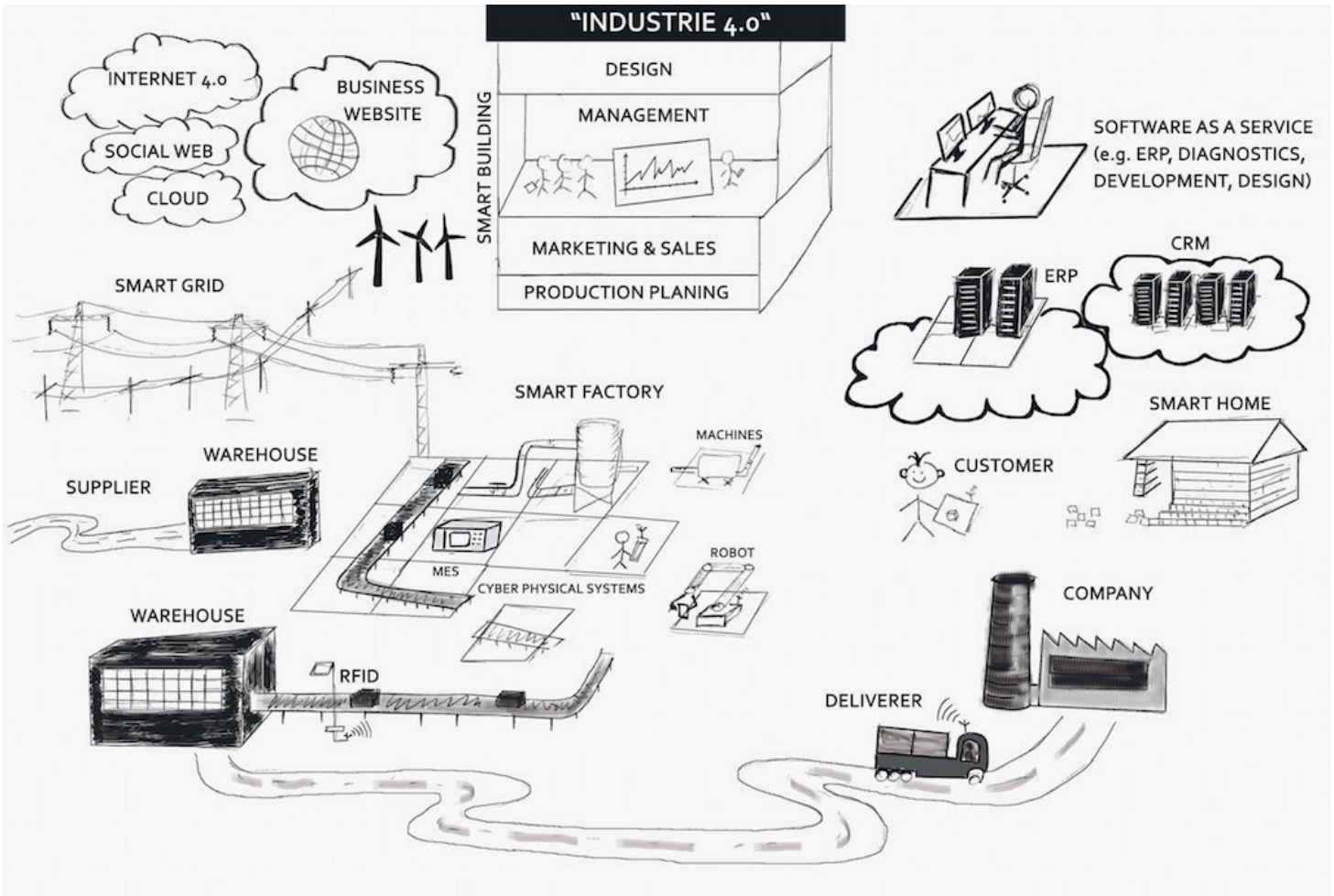
And then, with respect to features, in version 1.04, we added the Publish/Subscribe communication pattern to augment the longstanding request/response pattern that was in UA. These kinds of features stand side-by-side with the original functionality, and again, the older products can still use client/server; they just can’t use publish/subscribe until they modify their code. Notwithstanding, this allows a nice smooth path to the future.

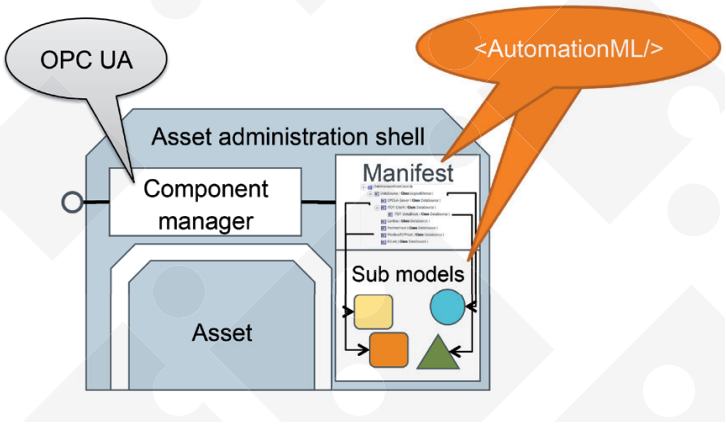
Over time, we add different communication protocols that underlie OPC UA. The basis of the client/server work is simply based on TCP, which is, of course, the most well-known internet protocol; however, with publish/subscribe, we’re adding UDP. Raw Ethernet is being added along the way, and the support of message brokers, including AMQP and MQTT, has become important – it’s all part of the publish/subscribe pattern.

CLARK: So, major UA versions have been 1.03, 1.04, 1.05, and so on. How about the concept of amendments being published in-between?

LUTH: TWe’ve been on a cycle of releasing a major update about every three years, which, to us, is not a major version because that would mean a breaking change. Instead, we increment from 1.03 to 1.04 to 1.05.

We’ve been following the IEC rules for updating specs. This means that in-between each major publication, we publish two other types of documents. One type is called “amendments”, which is where we add new functionality; the other one is called “errata”, wherein we





Localization of OPC UA and AutomationML in the Industrie 4.0 component administration shell.

make corrections to any mistakes found in the specification itself. These documents, per the IEC rules, are published as separate, physical documents, leaving the original specs untouched.

But, after living with the amendments and errata process now for a few years, beginning with Version 1.05, we're going to be changing these procedures; we're going to drop the errata and amendment documents and, instead, we'll be releasing point releases or sub point releases to the physical documents themselves as need be. Now you'll see a 1.05.1 and 1.05.2, and so on, in order to implement those same changes along the way. We're not changing the functionality that we're implementing; we're not changing the speed at which we're releasing those changes; we're just using a different system that we think will be smoother for our users.

In our world, all the specs are free, and they're instantly downloadable on the Internet so, we want to make the documents more easily updatable and more "live", like you would expect in this digital era.

CLARK: Earlier, you mentioned that you work as a system architect and that you work on standards. OPC UA is one, and maybe the most important; however, other standards do exist which you implicitly suggested. I've got a question about MQTT. Would MQTT be considered a competitor to OPC UA?

LUTH: Well, sure it is; but I think it's one of those cases where it's a competitor AND a part of OPC UA.

As I said, when describing the pub/sub features, OPC supports the MQTT protocol; and we use it as a viable way to move the physical bytes from one point to another. But, at the same time, MQTT is used by some as a raw technology to move the data outside of the scope of OPC UA.

This is nothing new. For example, back in the day when OPC UA client/server was first coming onto the scene, it was the heyday of web services. When speaking of client/server work, we would say, "you should be using OPC UA"; but others would argue, "but I can write web services, instead... they're really easy. Microsoft and others provide all the tools. It's really simple."

It's true; It can be simple to use some of those other standards if your job is to just simply get it done – to be able to move data from one point to another; but OPC UA is way more than a protocol for moving data.

Once you realize that you're better off implementing the whole ecosystem, which includes the data, the metadata, the security algorithms, the interoperability testing, the compliance testing, and so forth, as a long-term vehicle for something you're going to build into a product – something you can live with for years and years – using OPC UA is a much smarter way to do that, even if you decide you want to move the data with MQTT.

These point-to-point connections, as I like to call them, where some programmer impulsively wrote both sides of it – and then pats himself on the back because he successfully moved the data that he was asked to move – is missing that bigger context. And, as we move more and more into cloud systems and big-data, the context is now equally as important as the data itself. In those cases, losing the metadata that surrounds the data in UA is crazy! At some point, if not already, it's going to become more and more important to have that data.

CLARK: You just mentioned how context is particularly important in big-data scenarios. Can you share with our readers a big-data example and what you mean by context?

LUTH: Let's say I was able to have services and temperature sensors all around the world measuring temperature; then I decided to put a bunch of MQTT publishers out there to send out each temperature every minute, or every hour, or whatever. Now I've gathered a bunch of numbers in the cloud that represent temperatures. Well, that's great, but without the context, what am I going to do with that data?

Context could be as simple as the engineering units. If I don't know whether the temperature units are in degrees Celsius or degrees Fahrenheit, the values themselves are actually useless. Even if I knew the engineering units, if I don't have any idea of the physical location, the Geo location, of the temperatures, or whether I'm measuring the temperature under the sea, in the air, or of a device, a tank, or something else, again, what good is the data itself?

One could argue that, when making a point-to-point connection, they already know exactly what their application is. They could even provide just the right amount of metadata to the cloud. But one of the profound advantages of big-data analytics comes when tying information together in ways that the original implementors never envisioned. There's value that's being gained from big-data analytics; it's the imaginative correlation of datasets that seemingly would have no precedent of direct correlation.

And so, if today I cannot forecast what those correlations might be; if I don't even know which metadata I would absolutely need – or which ones I don't – the idea of capturing and maintaining all of that context is going to be super, super important as time goes on.

Unfortunately, when that point-to-point solution I spoke about earlier has its data moved to another location, typically, most of the context is lost.

CLARK: So, does that mean that OPC UA would need to be adopted everywhere – in sensors, in factories, but also in cars, buildings, even the cloud – so we can have full data, in context, as you've just explained?

LUTH: Well, that's often the way it can be viewed. I mean, if you're someone like me, who works almost exclusively with OPC UA, it's like walking around with a hammer, realizing everything looks like a nail.

The reality is, there are places and times where OPC UA, as a technology, as a whole, as we know it today – that is the metadata plus the data; the aspect of moving that data in real time – isn't necessarily the most appropriate application of the technology.

One of the things that we're starting to try to figure out now is how to move the richness of the OPC UA information model in ways that don't necessarily conform to the current OPC UA standards, with respect to the underlying protocols and the movement of data.

Currently, the OPC Foundation has a Joint Working Group for what's called Cloud Library and its purpose is to be able to publish OPC UA information models in the cloud for ease of reuse. Having a place to go, recognizing that this data came from OPC UA somewhere, that it's using this information model, and now, without going back to that location of the data, I can go to the cloud to get the context of the information model and metadata surrounding it. So that's one example of how we're trying to move information, outside of the normal space of OPC UA, including OPC UA clients and servers and publishers and subscribers.

Another example rests with FLC, which is OPC Foundation's Field Level Communication initiative. We're working on creating what, ultimately, will be the uber-replacement fieldbus in factory and process automation. As is true of all of the existing fieldbus technology, the ability to do offline engineering of devices and systems is very important; we have to have a way to effectively configure what will be an OPC UA system, without actually having the OPC system available at the time of configuration. For this, we're using another specification called AutomationML, which was specifically built for the purpose of exchanging engineering data among tools; not among live systems. So, we're working on effectively implementing OPC UA information models in an alternate tool, AutomationML.

Yet another example that I can share is a working group we have working on semantic validation. This is the idea that, right now, a lot of what we write in our compliance tests is written in English. The goal is to be able to have a way to validate these things in a more precise way than English allows. This has to do with validating the information model and the constructs within said information model.

One of the things the working group did was to convert the UA information model to the Web Ontology Language (OWL). They did this in order to make use of other tools available within that environment. In this case, they used SHACL, short for, Shapes Constraint Language, which allows them to do advanced processing of the information model in order to do validation. Since the OPC UA information model didn't have the necessary tools to do this, it made sense to convert this to a different form.

The last example I'll give is that within the Industry 4.0 initiatives, there's a concept called Asset Administration Shell. This similarly wraps a concept and an information model around anything and everything that could be an asset. Throughout the asset work that the Working Group is doing, they've tied this to runtime OPC UA information models but, much like our earlier FLC example, they need this information available in the static offline form. It'll be important to maintain the fidelity of the information model as it moves from an offline representation to an online representation within OPC UA.

CLARK: As a final question, is there any development you've experienced lately or any final thought that you would like to share with our readers?

LUTH: I think, in keeping with my last comments, the idea to extend OPC UA both down to the field level and as we go up to the cloud, we find things that OPC UA is really good at; however, there are other places where we have to reach out to other technologies. There's a lot of important concepts in OPC UA that need to be maintained, which are useful, but we're constantly challenged to find different ways to express it. I think, over time, we'll be better off if we don't look at everything as a nail, as we walk around with our hammer. •

ABOUT ABOUT THE INTERVIEW PARTNER – JIM LUTH:

Jim Luth is currently a System Architect for Schneider-Electric and the CTO of the OPC Foundation. Jim has been deeply involved in the development of OPC technologies for the past 25 years, originally representing ICONICS in OPC working groups and chairing the Technical Steering Committee. Later Jim became the full time Technical Director of the OPC Foundation and has served as Chairman of the Unified Architecture working group since its inception in 2003.

Jim has over 30 years of experience in factory automation and software development having previously worked for such organizations as General Motors, Taylor Instruments and The Foxboro Company. Jim received a Bachelor of Science degree in Electrical Engineering from Rensselaer Polytechnic Institute.

RANDY ARMSTRONG,
Chief Software Architect at Sparhawk Software and Director, IT Operations, Chair of the OPC UA Security Working Group
randy.armstrong@opcfoundation.org

OPC UA SECURITY

IN THIS SECTION: Learn from an interview with Randy Armstrong, Chief Software Architect at Sparhawk Software and Director, IT Operations. He is also Chair of the OPC UA Security Working Group. He will discuss the duties of the Security Working Group and why it was created, the companies involved, and the process of handling security vulnerabilities.

Randy, please introduce yourself to our readers; where you are from; what you were doing before OPC UA, and what has been your involvement with OPC UA and the OPC Foundation to date?

ARMSTRONG: Well, I've been involved in OPC pretty much full time since 1997. Prior to that I worked at a company doing embedded systems development and so I have long experience working with OPC. I've been following its evolution over time, having learned about how all of our security issues came up with DCOM, and trying to come up with solutions that would allow people to address these issues in a holistic way.

CLARK: Let's talk about OPC UA and security for starters. For some readers, security may be a relatively new topic. What is security and what should we think of regarding OPC UA security? Also, who are the members of the UA Security Working Group and what do they do?

ARMSTRONG: Well, security is something that has multiple aspects to it. The one that people are most familiar with is the notion that a hacker can sort of come in remotely and somehow connect to your software, take it over, or otherwise get information from your system. Sometimes that's achievable by taking advantage of bugs in software that allowed them to get in.

In general, what we think about it in OPC UA is we try to take a very structured approach where we have transport security at the bottom layer. In other words, how do you ensure that the information that you're sending over the network is confidential? How do you make sure that you know it hasn't been altered?

The next level is authorization. How do you make sure that any communication is coming from somebody who's authorized to send it; and you're sending information back to only someone who's authorized to receive it?

The final aspect of security has to do with access control. So, you know who you're talking too, that's great, but what are they allowed to do and how do you keep track of what they're allowed to do? How do you prove what they're allowed to do? I guess authorization is the correct term here.

What we've done in UA is that we've incorporated every aspect of the specification. Whenever we deal with any feature, the first question we always ask ourselves is, "what are the security implications"? We write out the requirements, we set out APIs, and we tie it into the other more generic framework we've put in place.

CLARK: So, there's a wide variety of aspects, as you said, that goes wider than just a hacker trying to get into your system. Tell us about the UA Security Working Group and what they do for the OPC Foundation.

ARMSTRONG: We realized several years ago that, as the number of people getting involved in the UA Working Group started to expand, we weren't getting the people in the working group that were necessarily the security experts within their companies. Primarily because these security experts tend to have many, many jobs and they couldn't prioritize being involved in every OPC UA meeting. So, we set up the Security Working Group with the idea that this group will only talk about security issues. We specifically invited all OPC Foundation member companies to send their security experts to join this particular group. This allowed us to benefit from all of the security expertise from all of our members as we're dealing with different is-

sues related to the UA Specification. This has worked extremely well. We've gotten very talented security researchers involved in the group that have really helped identify issues and solve problems.

CLARK: So, who are these people? Not the persons themselves, but what are the types of companies, the types of parties involved in the Security Working Group?

ARMSTRONG: It's basically the same interested parties who are involved in the UA Working Group but it's just different individuals that happened have expertise in security. So, all of the big control system vendors are represented: Siemens, ABB, Rockwell, those kinds of companies. You could basically go down the OPC Foundation membership roster and you'll find a complete cross section of the different companies that are involved in UA who are also involved in OPC UA security.

CLARK: Right, so they would be more typically the larger companies as they would have easier access and security experts represented in their environments rather than the smaller companies.

ARMSTRONG: Yeah, that is definitely a trend we see, where a larger company will have somebody on staff whose job is to do standards-related security, so they're more likely to have somebody that they would contribute to the effort. But, of course, we also have smaller companies participating. Obviously, all of the SDK vendors are represented in one form or another. The cloud vendors are represented as well, like Amazon and Microsoft – SAP is also involved. They all need to deal with security in order to get the OPC data into their infrastructure.

CLARK: You say that toolkit providers are involved; Is that so they can quickly correct and update new vulnerabilities? Is that a two-way benefit that they bring to the party?

ARMSTRONG: Well, you're kind of jumping into the next topic of identifying what the UA Security Working Group does, and that has to do with vulnerabilities.

OPC UA has garnered huge interest, especially now that there's a lot of development going on. We're also attracting keen interest from security researchers. The good thing is that this interest means that people find vulnerabilities. You might find it perplexing to suggest that finding vulnerabilities could ever be a good thing; but what it really means is that people are seriously looking at OPC UA, trying to find issues.

For the most part, what happens is that these vulnerabilities are brought to our attention, we discuss it as a group, and we decide how we want to deal with it.

But do we need to publish a public notice of the vulnerability? Well, before doing so, we coordinate with the SDK vendors and software vendors to make sure that their software gets updated to fix the vulnerability before we make anything public.

So that's a glimpse into the formal process that we follow anytime something gets reported. It could be reported from government bodies, it could come as a private report from a corporation, or it could even be published in research papers.

CLARK: Respecting that you are dealing with sensitive security topics, is there anything you can share with our readers regarding the things the UA Security Working Group is currently tackling?

ARMSTRONG: Well, the big thing that we're looking at right now is something that we realized fairly early on. With OPC UA, it's not enough to simply define all the security primitives in the specification, since what ends up happening is that the device becomes very complicated to set up and configure.

So, what we've done is that we've provided a mechanism for configuring and managing security. Moreover, we're continuing to look at ways to further enhance these capabilities - to cover the complete lifecycle of a device from the moment that it's shipped from the manufacturer, to when it's installed on the factory floor - identifying what steps are involved and how we can assure that this device has not been modified or tampered with throughout the supply-chain.

Additionally, we are constantly looking at developments in either new security algorithms and/or incorporating new protocols as they come up.

We recently incorporated the Elliptic-curve Cryptography (ECC) algorithms into the UA umbrella because these are very important for small embedded systems.

And, with respect to protocols, we have an effort underway where we're looking at HTTP 3.0, which is coming down the pipe. We will be trying to decide how best to incorporate those capabilities into the UA specification.

CLARK: I suppose it's safe to assume that security is an ongoing effort and that you will likely never be able to say that you're finished.

ARMSTRONG: Right, but we are now at the point where we've got, I believe, a critical mass of infrastructure that will allow people to build and deploy secure UA systems where we can now settle into a state where we're simply maintaining the existing infrastructure. But, yes, there's always new stuff that comes along; there is always a risk that somebody will find a flaw that we need to address.

The good thing is that UA has been around for over 15 years and we've had lots and lots of security people - and hackers - working on it, trying to find exploits, and, for the most part, it's held up! We haven't had to revise the protocol at all, especially since the issues we've addressed tend to be related to configuration or software implementation.

Perhaps our readers may not be familiar with a contest called Pwn2Own. This is a contest where large sums of money are offered to hackers to find vulnerabilities in products. This has been going on for years and their focus has historically been on consumer electronics, like mobile phones and home-based routers and those kinds of things.

The organizers recently expanded the contest to include industrial automation systems. The targets are published and then all the contestants will spend a fair amount of time trying to find ways to exploit or to hack into those targets. If they are successful, they get a specific sum of money for every exploit they find.

So, at the contest in 2020, in Miami, OPC UA applications were put on the block and they came out looking pretty good. There were a couple of minor issues but, for the most part, they couldn't find any exploits.

CLARK: The topic of open-source comes up frequently. What role does open-source play in relationship to OPC UA and security.

ARMSTRONG: Open-source is a key part of all software development nowadays; you can't have a solution without some open-source solutions so the OPC Foundation and Microsoft have been sponsoring a .NET open-source project.

There are a number of other open-source projects in different languages such as Java, ANSI C, and Node.js. Within all of these projects, security has to be implemented and this is where the challenge lies - they need to implement security properly.

To help with this, the OPC Foundation has its certification program. We try to encourage vendors who are using these open-source libraries to go through our certification program and, thereby, verify that the libraries they're using are, in fact, implementing OPC UA security correctly. In some cases, these open-source projects have sponsors who will go through the certification process just to make sure that they've done things right.

The relationship between OPC Foundation and open-source is that we provide the link to certification - getting the certification done. If people are looking at open-source – and there's lots of projects out there – we are encouraging them to focus on ones that have actually gone through this certification process because that's the only way they can have any assurance that they've implemented security properly.

CLARK: As far as security and OPC UA are concerned, can you share with our readers one or two features that you will be working on in the near future?

ARMSTRONG: Sure. As I mentioned before, we're working on device provisioning, which is the full lifecycle security model, to try to come up with a solution that allows device manufacturers to produce devices that can then be verified when they're plugged into their network. This is something that we're doing in conjunction with our Field Level Communication (FLC) initiative because there are plans to produce UA devices where there's an opportunity to put some standards in place in order to promote adherence to certification.

CLARK: Thanks for participating Randy. In conclusion, are there any developments you've experienced lately; any activity that may be coming up in these times of COVID-19; or any final thought that you would like to share with our readers?

ARMSTRONG: The COVID-19 Pandemic had zero impact on the work of the Security Working Group because it was operating remotely to start with. Thankfully, we've been moving forward uninhibited.

I'd like to reiterate the importance of security within any industrial automation application and how people – end users or factory owners – can't ignore it. They need to have a solution for it, even within their local networks because you never know where a compromise is going to come from and that's where UA is part of the solution. •

ABOUT ABOUT THE INTERVIEW PARTNER – RANDY ARMSTRONG:

Randy Armstrong is the Lead Security Architect for the OPC Foundation.

He is also the Chair of the OPC UA Security Working Group which is responsible for making decisions on all aspects of the OPC UA specifications related to cyber security.

Randy has been contributing as an expert and editor to OPC Foundation working groups since 1997.

Randy is also the Chief Architect for Sparhawk where he has developed OPC applications for many different automation software vendors.

FABIAN ANZMANN,
Technical Advisor in the area of digitalization for the Industrial Association of House, Heating, and Kitchen Technology (HKI)
anzmann@hki-online.de

HOLGER BURGTORF,
Industrial Association of House, Heating, and Kitchen Technology (HKI)
holger.burgtorf@phoeniks.eu

COMMERCIAL KITCHEN EQUIPMENT

IN THIS SECTION: Learn from an interview with Fabian Anzmann and Holger Burgtorf about the OPC UA Companion Specification for Commercial Kitchen Equipment. They will tell us about the Industrial Association of House, Heating, and Kitchen technology, and what the company, Küppersbusch, does. They will also give us an introduction to commercial kitchens and explain what role the Internet of Things may play in the concept of the connected kitchen.

MICHAEL CLARK: Fabian, please introduce yourself to our readers. Tell us about the Industrial Association of House, Heating, and Kitchen Technology, and Küppersbusch, including your involvement with OPC technology and the OPC Foundation.

ANZMANN: My name is Fabian and I'm working for the industrial Association of House, Heating, and Kitchen technology. In that Association, I am responsible for most of the digitalization topics, that is why I was involved in the manufacturer-neutral communication standard.

I can imagine that many people do not know the HKI due to the fact that, in comparison to bigger Associations like the VDMA, we are rather small. We have quite a history, because we are now more than 70 years old. We're representing the manufacturers of commercial kitchen equipment and domestic heating and cooking appliances. In total, we have about 230 members. Even though we are a national association, we are well connected on an international level. So, we interact with the European association that deals with commercial kitchens, but also with our American association counterparts. When establishing international standards, this is very important.

You also asked about the HKI. First of all, as with most industrial associations, we serve as a dialogue partner for politics and authorities. We represent the industry with one voice by providing assistance, advice and services. One very important role for the HKI is the development of technical rules, standards, and norms for the benefit of our manufacturers. This is very important, because we work together with the OPC Foundation to create communication standards within commercial kitchens.

CLARK: Same for you, Holger. Please introduce yourself to our readers and tell us who and what is Küppersbusch

BURGTORF: My name is Holger Burgtorf, and I'm the head of innovation and product management within Küppersbusch. I joined the company in 2006. Küppersbusch was founded in 1875 in Gelsenkirchen by Friedrich Küppersbusch. Today Küppersbusch Großküchentechnik is in the business of producing professional kitchen appliances in Gelsenkirchen, Germany.

Where might you find professional kitchen appliances from Küppersbusch? We serve small restaurants, five-star hotels, institutional catering from hospitals to universities, and even in-flight catering.

Whether it's 50 or even 10,000 meals a day, you will find Küppersbusch equipment.

CLARK: Please give our readers an introduction to commercial kitchens. What are the main differences between these and domestic kitchens?

ANZMANN: Professional kitchens are normally seen in the gastronomy and catering sector. The main difference when comparing to domestic kitchens, is that professional kitchens have much higher production rates. Since we are talking about two-hundred meals or more per day these kitchens have more in common with a production area than with normal cooking at home.

Due to the fact that there are such large quantities of food, and the high production rates, there are different requirements for these kitchens, including food monitoring by officials from public health authorities. It is important to mention that professional kitchen operators have responsibility for food safety. Since they usually operate under licensing from a public health authority, they are required to store data regarding food safety and have to demonstrate that they are in compliance with regulations.

It is important to mention the HACCP system. HACCP is short for hazard analysis and critical control points. The HACCP system deals specifically with potential hazards during food processing. Therefore, kitchen operators are required to document a system that mitigates potential hazards during their food processing operations. Inspection is usually done at critical control points during food processing. For example, at one such control point, the operator observes a temperature at this particular stage of production. So, in this example, if you are cooling stuff, it may be required to chill to a certain temperature. If the measured temperature is above the required value, the written procedures describe what action to take.

During inspections by the public health authorities, the producer needs to show that the HACCP system is properly documented.

CLARK: Holger, would you like to add your thoughts from the perspective of a manufacturer?

BURGTORF: Thank you, Fabian. There is something more I can add. For example, guest expectations, when visiting a restaurant. Guests have a certain expectation, a certain food quality, and a consistent food quality. This should be totally independent from who is preparing and cooking the food. In a professional kitchen, you need more standardized recipes, and even standardized preparation processes, to guarantee consistent food quality and to support the restaurant concept of competition.

Another important issue for professional kitchens is the availability of service for the appliances. Meaning, if there's a failure of one of the appliances, professional operations need urgent service to repair the appliance, to get back online to return to serving meals. It's not like in domestic kitchens, where you might wait a few days for a service technician to come by to repair your oven. A quick service response is an important differentiator between professional and domestic kitchens.

CLARK: What are the major challenges in the area of commercial kitchens?

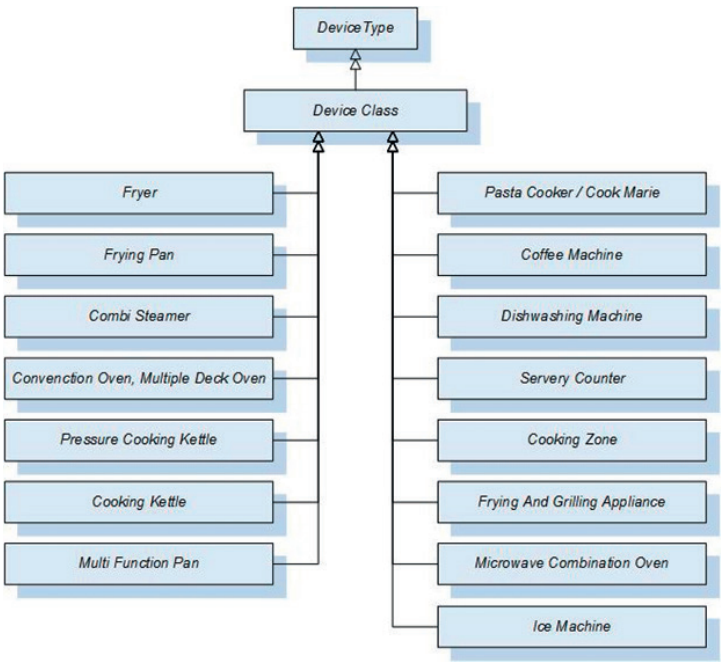
ANZMANN: I think there are quite a few different challenges that we face. First of all, there is a shortage in staff due to the working conditions in professional kitchens. Since conditions are not always the best, not very many people like to work there.

Today, there is higher demand for restaurants and canteens, which can be traced to societal changes over the course of several decades. If you look at today's modern families, they tend to eat out or get their meals through home delivery. This results in greater need for a higher degree of automation within commercial kitchens.

We hear in the news a growing effort to promote sustainability; of course, this impacts the commercial kitchen as well. We have to find solutions for the efficient use of food and addressing food waste. This is definitely something with which that IoT can help.

Another big topic is energy consumption. The devices that are normally found in commercial kitchens have really high energy consumption. There is lots of potential to optimize energy consumption. This is also something where IoT, in my opinion, can help.

Lastly, I want to mention the challenge of IT security, because in kitchens, it's important to have high data protection requirements. It may surprise your readers to learn that we have sensitive systems here. For example, if intruders manipulate a temperature control system, one which maintains the temperature of stored food, in a worst-case outcome, it could spoil the food and, subsequently, harm people. We promote high IT security standards so that such a thing cannot occur.



CLARK: Holger, do you also want to add something here?

BURGTORF: Yes, thank you Fabian. There's something to add in reference to IoT. IoT integration of appliances into kitchen management systems is something of a challenge so far. Looking at the market today, there are many proprietary solutions for appliance connectivity. In addition to that, there are many different kinds of appliances – dishwashers, fryers, kettles, coffee machines, fridges – all from different manufacturers. It's difficult to create common integration across kitchen management systems. The industry has been begging for a standardized solution, cries which came primarily from the kitchen operators. Before the creation of the OPC UA Companion Specification, there was no clear standardization of the requirements for connected kitchens. No easy or sufficient communication was guaranteed. Now, looking to the companion specification, there is a real, cost-efficient, and safe integration into kitchen management systems, which was not possible before. Furthermore, it is manufacturer-independent.

What are some other threats to professional kitchens, specifically looking at restaurants and business canteens and even hospitals? Delivery services have become the new competition for these kitchens, forcing them to become very competitive. On the other hand, there is still rising demand for restaurants and canteens due to the out-of-home clientele as a growing market, as was mentioned before.

Another issue is the rising complexity in production processes. As mentioned by Fabian, we have to ensure food safety through requirements outlined in respective HACCP documents. This means that you have to control, monitor, and do a proper documentation of all critical control points. All of this requires resources, since someone has to do it. On the other hand, staff shortages are not helping the situation at all. This calls for an IoT solution.

CLARK: How can digital services and IoT help in that context?

ANZMANN: Frankly, we can automate more processes. This is better for the kitchen operators, since this will provide more time for important tasks, including creativeness and interacting with restaurant guests. Furthermore, process monitoring is something on which IoT can have valuable influence. In many cases, legal requirements stipulate that operators monitor their food production processes. Remote services for appliances can further support the kitchen operator, and when you look at sustainability for energy and resource management, artificial intelligence can easily consume this standardized data to bring greater optimization to the operator. These are just a few examples of how IoT can help, but this is almost impossible to achieve without some sort of standard. That's why we are engaged in this great undertaking.

CLARK: Why is a manufacturer-independent communication standard so important for commercial kitchens?

ANZMANN: If you look into professional kitchens, you see a lot of different appliances and devices from several different manufacturers. It's quite the heterogeneous system. Consequently, if there is no

standard, every manufacturer is left to invent their own solution. This means that the kitchen operator has to have several apps to monitor everything, which can't be the solution.
Imagine the enormous task that a kitchen operator would have to undertake if attempting to integrate all of these disparate devices. Now, imagine a scenario where one of those devices fails, and they are forced to replace it with something that doesn't conform to the system they had created. It is so very important to have a standard; a prerequisite for the integration of a professional kitchen management system.

CLARK: Holger, do you want to add something here?
BURGTORF: Yes, there is something I can add.
Coming back to the initial set up of a new kitchen; what are the rules? Meaning, what are the rules when issuing public tenders? In accordance with the specified requirements, consultants will describe functions and applications, and then identify appliances pertaining to those functions. Then, in order to comply with the rules for public tenders, it's necessary to have more than one brand per product available in the market. If only one proprietary, manufacturer-specific solution for IoT was offered, then it creates a problem for public tendering, because only one brand could fulfill the specification. It's clear why it is very helpful to have a manufacturer-independent standard for communication interfaces.

CLARK: Why did the working group decide to go with OPC UA?
ANZMANN: There are several reasons for that. One very important one is data security, which is important for the professional kitchen. The BSI, the Federal Office for Information Security here in Germany, did a comprehensive analysis of OPC UA, which confirmed that OPC UA does not contain any systematic security gaps, which was very important for us.
Another point which we want to mention is that OPC UA is very versatile in its application; it is more than just a protocol; it delivers the whole infrastructure for communications. Even if a new technology pops up, it will be integrated into the OPC UA standard. It was critical that we were not getting into a methodology which wasn't future-proof. We are quite optimistic with OPC UA. We looked at other associations, like the VDMA, seeing that they were advocating for OPC UA. This strengthened our opinion that we had made the right decision to go with OPC UA.

BURGTORF: May I add something to this as well. Another important issue for us was that the solution needed to be open source. Thankfully, it allows easy adaptations, as required, by manufacturers or operators. Another important issue for us was that the documentation needed to be open to everyone. Nobody has to pay for OPC Standards. Furthermore, there are no licensing fees required, neither by the manufacturer nor by the operator later on.
The vending machine industry is another sector closely associated to professional kitchens, and they are also considering using OPC UA; it's easy, quick, and can directly connect to the cloud. This is helpful if you're looking into Microsoft Azure, or SAP connectivity. Most of all, there is no vendor lock-in with OPC UA.
Another appreciated outcome for us was the excellent support we received from the OPC Foundation when we were creating the companion spec within the working group of the HKI.

CLARK: I understand that the OPC UA Companion Specification for Commercial Kitchen Equipment was launched in July of 2019. Can you please share with us how long it took to create this document and how the process worked?
ANZMANN: This took two or three years. Most of our time was spent doing market research, finding the appropriate solution for the standard. When we finally made the decision to go with OPC UA, the work began to accelerate. We worked together with 30 manufacturers in our association and, of course, they are all now part of the OPC Foundation.
Within the companion specification, we defined fifteen device-type information models, describing the data for those devices which will be transported via OPC UA. For example, we have defined, fryer, combi-steamer, cooking kettle, dishwashing machines, and microwave combination ovens. In those information models, we defined the data that will be transported with meta information, like the NodeClass, BrowseName, the data type or the type definitions, as well as the modeling rule.
This companion specification serves as a basis, but it has room for individual data for each manufacturer. It is very important for us that this is the case.

CLARK: What does the implementation of OPC UA look like from the perspective of a manufacturer? Do any challenges remain?
BURGTORF: So, for Küppersbusch, we wanted to become a first-implementer for this OPC UA standard. We successfully introduced an OPC UA interface with our new KCI controller. Since IoT is a new field for Küppersbusch, we took on a partner that has special skills in IoT.
Another challenge for us is that we are pushing an open standard, unlike bigger competitors in the market who tried to push their own proprietary systems, pressuring us to get on board with their systems, which is not in our favor at all.

CLARK: Have other manufacturers of commercial kitchen equipment, besides Küppersbusch, implemented OPC UA into their devices as a manufacturer-neutral communication standard?
BURGTORF: Starting out was not as easy as we thought; there were only a few brands, including Küppersbusch, who were the first to push this standard into the market. We presented our equipment at international trade fairs, making the concept of IoT integration more and more public. It was reassuring to see more and more customers come to us welcoming the idea of easy IoT integration. Because of this push and pull effect, we now have many more manufacturers implementing the standard, and offering interfaces in accordance to the OPC UA standard.

CLARK: What can we expect to happen with regards to extending the OPC UA Companion Standard for Commercial Kitchen Equipment into the market? What are the next steps?

ANZMANN: With the companion specification released, we are now promoting the standard and building awareness that such a standard exists. We are very happy to be highlighted in this article, allowing us to do some promotion. We are also speaking with other associations, including the American association, to promote this standard worldwide; we are pushing it strongly on an international level.

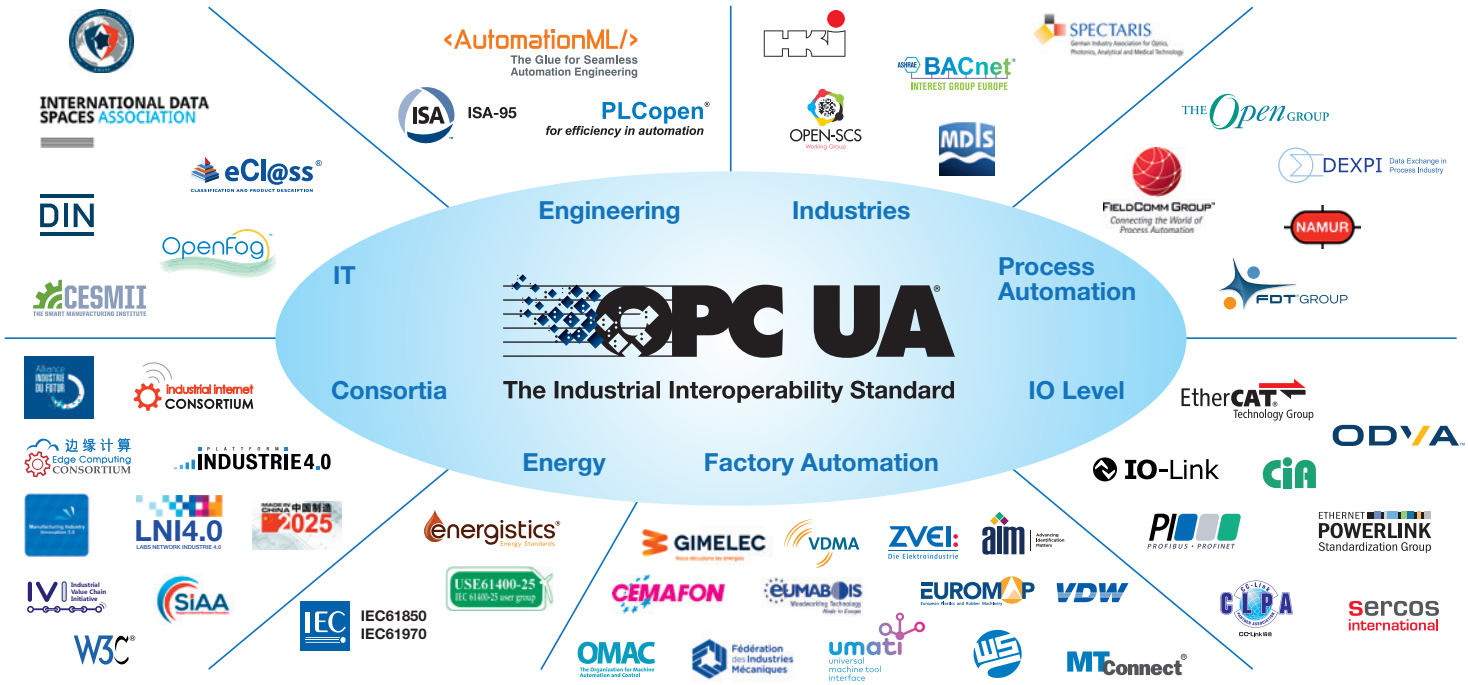
There is more to add to the standard. We continue our work on another chapter for cooling appliances, as they are not yet included in the companion specification. We're working on those information models for this device type, and we're looking forward to having it integrated into this companion specification very soon. We believe this companion specification has high potential, especially since there is nothing comparable on the market. It's our goal to produce an international standard in professional kitchens.

CLARK: In closing, are there any final thoughts you would like to share with our readers?

ANZMANN: We want to say thank you to the OPC Foundation for all the support they have given. We're very grateful for their help. •

ABOUT ABOUT THE INTERVIEW PARTNER – FABIAN ANZMANN:

Since 2018, Fabian Anzmann has been working as a Technical Advisor in the area of digitalization for the Industrial Association of House, Heating, and Kitchen Technology (HKI). He has a Master's Degree in Food Technology from the University of Bonn and Bachelor of Food Technology from Hochschule Fulda.



OLAF WILMSMEIER,
Founder & Owner, Wilmsmeier Solutions, Freelance consultant specializing in auto-ID and digitization.
info@wilmsmeier-solutions.com

PETER ALTES,
Managing Director of AIM-D e.V.
peter.altes@aim-d.de

AUTOID COMPANION SPECIFICATION

IN THIS SECTION: Learn from an interview with Olaf Wilmsmeier from Wilmsmeier Solutions and Peter Altes from AIM about the OPC UA Companion Specification for AutoID Devices. They will introduce the AIM organization, identify the role of AutoID in the context of Industrial IoT, why they chose OPC UA as their basis, and the status and synergies between wireless sensor networks and AutoID.

MICHAEL CLARK: Olaf, please introduce yourself to our readers and tell us about your company, and your involvement with OPC technology and the OPC Foundation.
WILMSMEIER: My name is Olaf Wilmsmeier founder and owner of Wilmsmeier Solutions. I have 25 years of experience in the automation machinery market. For the last 10 years, I've been focusing on the AutoID and RFID business.
I support digitization and AutoID solutions. At the SPS Exhibition 2013 I set up the first technical demonstration of an RFID device communicating via OPC UA.

CLARK: Peter, please introduce yourself and give our readers a quick introduction to AIM.
ALTES: My name is Peter Altes and I've been the managing director of AIM, Germany since 2016. AIM is the association for the AutoID industry, providing technical solutions, systems integration, and software solutions for all AutoID technologies. This includes optical technologies like barcode and RFID products. Being in Germany, we are integrated into a global network of national chapters and organisations, like AIM global and AIM Europe, where we cooperate with several partners in different organizational or technical areas. One of our major partners is the OPC Foundation, whom we're talking about today. We are involved in each other's working groups, joint exhibitions, speaker exchange, and joint marketing campaigns.

CLARK: Since we will be talking about the OPC UA Companion Specification for AutoID Devices, please tell us what AutoID devices are, and what they do.
ALTES: AutoID means automatic identification. Identification is a step in all industrial processes, whether it's a physical process performed by a person or an automatic process performed by machines. It means two objects have to identify each other, and this works with AutoID devices like readers, RFID gates, or barcode scanners, with which anybody who has ever gone to a supermarket is quite familiar. Additional systems may include sensors that detect parameters like pressure or other variables.
In addition to identification devices, there is a second group of devices, like printers and technical definitions for interfaces. AutoID devices collect and exchange data as part of the identification processes. This data is provided to the IT systems for either logistical

processes or production processes. The data can then be brought to the cloud, into a company's manufacturing execution systems, or an ERP system.

CLARK: Since AIM has been one of the drivers behind the OPC UA Companion Specification for AutoID Devic es, can you tell us about their goals?

ALTES: From AIM's point of view, we believe that we are the driving force behind AutoID, since we are the association for this industry; however, without the OPC Foundation, we couldn't succeed. In this relationship, we are the two organizations who are on top of development. We are an association, driven by small and medium sized companies, but also by global players. To name just a few, Olaf Wilmsmeier's company, is one of our major contributors, not only in our association, but also as a contributor to the OPC UA companion specification. We have other well-known companies like Kampmann, medium size companies like Balluff and Turck, automation partners like Leuze and Sick, others like Logopak and ascolab. We also have research and development partners including Fraunhofer Institute, among several others. That's a brief overview of a small list of partners who are driving AIM and the OPC UA Companion Specification.

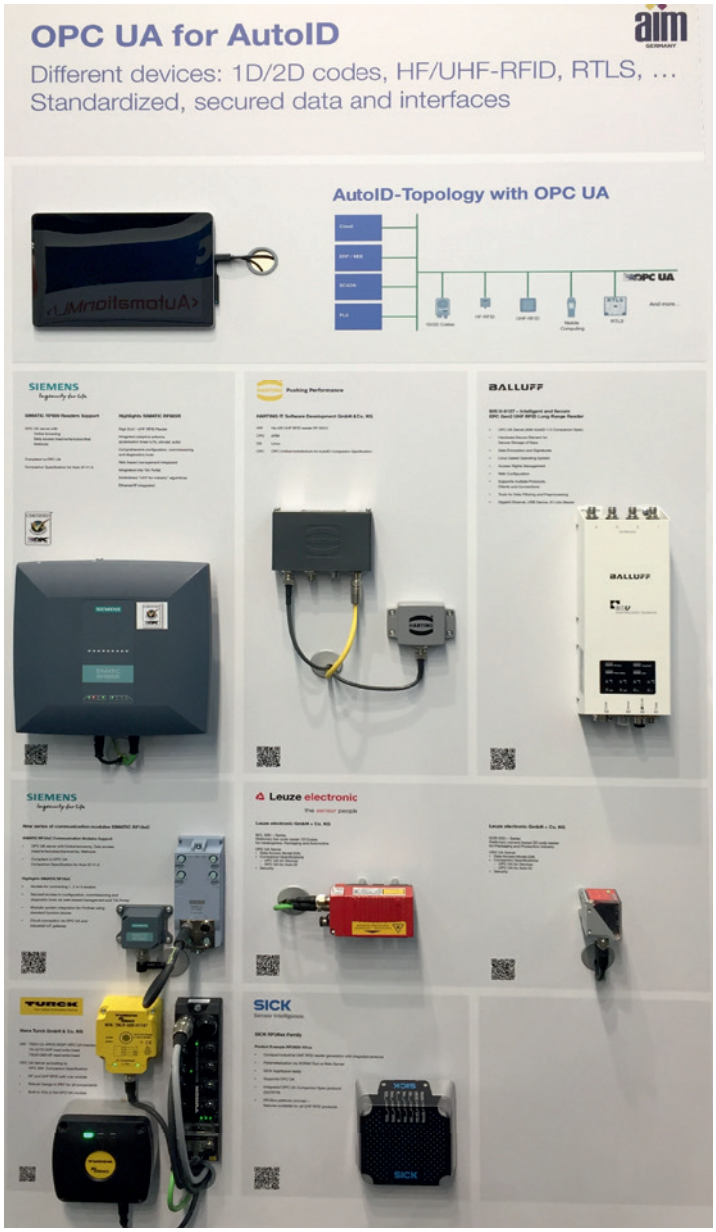
CLARK: Is AIM typically involved in global standardization?

ALTES: Yes, for sure. Standardization is a key focus for AIM. AIM (The Association for Automatic Identification and Mobility) was founded in Pennsylvania about 40 years ago as an organization which was allowed to allocate number systems, you might know them from GS1. AIM is also providing input on ISO standards and is working with CEN and CENELEC.

WILMSMEIER: One of the more important topics, where AIM is working with Brussels and other European countries, is the standardization of a common radio frequency range across the entire world.

CLARK: What is the role of AutoID in the context of Industrial IoT?

ALTES: We here at AIM believe that AutoID technologies are the enabling technologies for all these processes, including industrial production processes or logistical processes, supply chain processes, machines, robots, containers, and even packaging systems.
In general terms, all of the objects I just mentioned (and more) need to communicate with each other, and communication starts with identification. In terms of the processes, the system might need to know, "is this object the right object for the next production process?" Or "Is this package the right package to be turned into loop A instead of loop B in the logistical system?"
This only works if there is proper identification, and identification is based on identification technologies. These are the optical technologies and the electronic technologies I spoke about earlier. Therefore, in all soberness, we say that these are the enabling technologies; there is neither digitalization nor the possibility of autonomous processes without AutoID technologies.
Looking towards the future, we're not only focused on object-to-object communication within autonomous processes, but we must



OPC UA for AutoID devices vendor and technology independent

concern ourselves that these communication pathways provide secure identification. Therefore, this sets the foundation of the digital transformation of economic processes. That's our perspective.

WILMSMEIER: So, to summarize this in a simple way, when we're talking about the next level of automation – how to speak with an object, how to interact with a carton, how to interact with a palette, how to interact with a metal pipe – these kinds of items are totally passive, they don't have an IP address, but that doesn't stop people from longing for automated processes. We need to find a way to communicate or, at a minimum, to identify, but maybe even hand over some data to such an object. This is what AutoID is about.

CLARK: What was the motivation for AIM to consider a common interface for AutoID devices?

ALTES: We have many AutoID devices like printers, gates, hand-

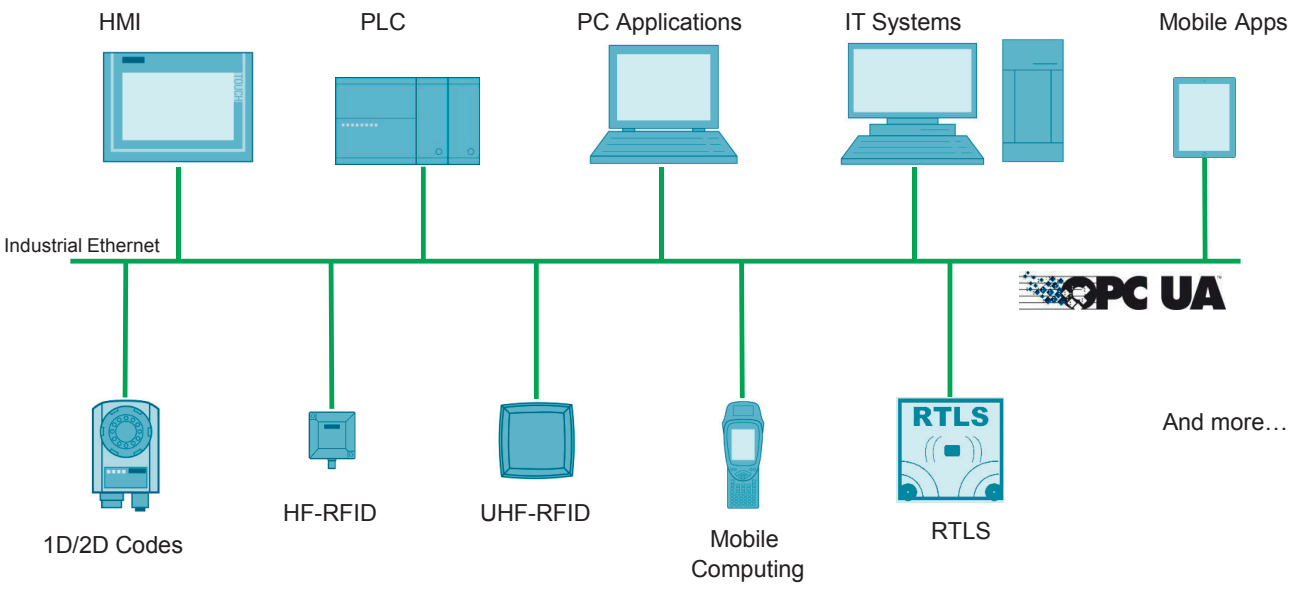
helds and so on. These different devices are provided by many different companies, and most of them have their own systems, which means software or “language systems”.
To harmonize all these devices with each other, and to harmonize these devices to the processes in which they are used – like production processes or logistical processes – they need a translator, they need a common language, and this means interoperability.
This leads to the question, “how can we achieve this kind of translation system, how can we achieve interoperability?” The answer was simple; we need a common language. There was only one option and it was OPC UA. Our goal was faster, easier, and more secure processes. Once again, it’s a question of standardization. If we want to feed a global internet of things or, in a narrower sense, an industrial internet of things, we need a common language.

CLARK: So, I guess you started answering the next question; why did you choose OPC UA as the basis for the common AutoID devices interface?

WILMSMEIER: Since we agree that AutoID is one of the base technologies to fulfill the next level of automation, then we had to find a method that is accessible for everybody and is common to all the different kinds of technologies, from an AutoID point of view. As is very common already, especially in the industrial world, AutoID and OPC UA mix together absolutely perfectly. OPC UA is the communication standard in the industrial automation world. The standard is already set; everybody is aware of it. Because of this, AIM was highly motivated to adopt OPC UA as a common interface.

SIEMENS

AutoID-Topologie mit OPC UA



Frei verwendbar / © Siemens AG 2014. Alle Rechte vorbehalten.

One for all: OPC UA is connecting AutoID devices with all other automation components – from sensor to cloud if needed

CLARK: Please tell us a bit about the development of the OPC UA Companion Specification for AutoID Devices. When did you start? Which companies have been involved?

WILMSMEIER: We started in 2014, where, in one of our first working group meetings, we discussed how to assure interoperability. We, again, came to the conclusion that OPC UA would be the ideal methodology. In 2015, we launched our first demos at the Hannover Fair.

The first companies involved were ICS, Siemens, and Harting. We had now shown that we were able to communicate between different devices, between different kinds of software, and up to a back-end Azure cloud from Microsoft. This was very easy, without much effort expended to perform the integration. This is what we're looking for, to make the base technologies fit together for all the integrators and software programmers.

CLARK: What is the status of the companion specification? Are you still actively improving the specification, or is it done?

WILMSMEIER: Of course, it's not done; you have to improve it all the time. As mentioned before, 2016 was the first release, but we have been working very actively since then, focusing on simplifying the companion specification to make it as easy as possible to use. For instance, we are working on sensor integration; a topic which we are actively pursuing on our agenda.

CLARK: What about wireless sensor networks and AutoID? Do any synergies exist between them?

WILMSMEIER: Yes, indeed. Everybody seems to be interested in wireless sensor networks to avoid nested cabling. Even though my company's history is a connector and cable assembly company, wireless technology is now in focus.

It's now possible to combine UHF RFID with existing sensor technology so that wireless sensor values, like humidity or temperature, can be transmitted "battery free." The energy to transmit is coming from the electromagnetic field of RFID communication. This is very interesting, especially for harsh environment industries. Battery free? Maintenance free? Of course, everybody loves it!

ALTES: I'd like to add to this point. You can see how important sensor systems and wireless sensor networks are for us. We recently founded a new working group within AIM, which is mainly focused on the relationship between AutoID technologies like UHF RFID and sensors. We are discussing, not only the interaction between RFID and sensor systems, but also how these systems work in common with the sensor tags.

CLARK: In closing, are there any final thoughts that you would like to share with our readers?

ALTES: Well, we try to update the companion specification as a kind of continuous improvement process; not day by day but month by month. We are planning new releases at least every two years. We also do interoperability workshops with automation partners. These workshops show us what works and what maybe does not work, so we have continuous input that help improve the companion specification.

WILMSMEIER: So, all the information for the new companion specification is available; feel free to contact us if you are interested in a copy. Of course, you will also find the information on the OPC Foundation website. In addition, I want to highlight that the AIM working group is active and we are more than open to new participants. Everybody who is willing to spend the time and effort to improve the overall companion specification is more than welcome to join us. •

ABOUT ABOUT THE INTERVIEW PARTNER – OLAF WILMSMEIER:

Olaf Wilmsmeier, Founder & Owner, Wilmsmeier Solutions | Olaf Wilmsmeier is a freelance consultant specializing in auto-ID and digitization. He brings around 25 years of professional experience in the field of mechanical engineering and automation to his work. Since 2010, Mr. Wilmsmeier has been leading digitization and in particular UHF RFID products and projects to success worldwide. After training and studying electrical engineering at the University of Applied Sciences in Osnabrück, Mr. Wilmsmeier worked as a developer, project manager, product and business development manager for various companies in Germany and abroad. As a board member of the German speaking chapter of AIM, Olaf Wilmsmeier is one of the initiators and drivers of the OPC Unified Architecture for AutoID Companion Specification, which the AIM Association defined in cooperation with the OPC Foundation.

ABOUT ABOUT THE INTERVIEW PARTNER – PETER ALTES:

Since 2016, Peter Altes has been the Managing Director of AIM-D e.V. and has been a consultant and project manager for various firms and research institutes in the event industry for nearly three decades. Peter has a Master's Degree in Philosophy, Political Sciences, Linguistics and National Economy.

CHRISTOPHER ANHALT,
Business Development Manager for
Softing Industrial Automation GmbH,
Senior Representative for the OPC Foundation
christopher.anhalt@softing.com

OPC UA USE CASES

IN THIS SECTION: Learn from an interview with Christopher Anhalt of Softing about markets, adoption drivers, competing standards, the horizontal and vertical integration of IT and OT, companion specification use cases, green-field and brown-field… and many other things relevant to use cases that have made OPC UA so successful.

MICHAEL CLARK: Christopher, please introduce yourself to our readers. Tell us a bit about yourself, your company, Softing, and your involvement to date with OPC technology and the OPC Foundation.

ANHALT: Sure, let me begin with Softing the company. Softing has specialized in industrial communication and embedded technology for over 30 years. We are headquartered just outside of Munich, in the town of Haar, Germany. We have several business units, one of which is called Industrial Automation, which focuses on developing and marketing industrial automation solutions.

Regarding the OPC Foundation, Softing has been a member since the early days in the 90s. We have a close cooperation with the OPC Foundation and have been actively involved in several technical working groups. For the past three years, I've worked as the business development manager in the Industrial Automation business unit and I'm also the marketing representative for the OPC Foundation for this internal group.

CLARK: Can you please give us an overview of the different markets in which OPC UA has been deployed successfully and comment on growth opportunities for the future?

ANHALT: Let me begin with vertical segments. The core vertical, where OPC is coming from, is industrial automation. This is the vertical where OPC UA has been deployed successfully, and where we expect growth in the near future and beyond. Of course, it is possible to use and to deploy OPC UA in other verticals, including building automation, transportation, and many other segments.

From the beginning, OPC technologies have had a global presence, enhanced by collaborations with both international and regional standards bodies. The very diverse membership of OPC Foundation adds to its global presence.

It is remarkable how deeply OPC technologies have been adopted, especially in recent years, and we expect that growth to continue, especially in the Asian region. I mean, we see growth globally, but it has been particularly strong in Asia, where we now count China, Japan, South Korea, and Thailand as key markets; each are contributing to the rapid growth of OPC UA.

Regarding technology use cases, I will speak about vertical integration. This is the integration between OT devices and IT software applications, which count for the clear majority of deployments, driving additional growth in the future.

MICHAEL CLARK: What have been the drivers for adoption of OPC UA in various market segments and will they change as OPC UA moves into new markets?

ANHALT: Well, to summarize, the primary driver is the need for interoperability between devices, PLCs, and machines; interoperability between devices and software; and, finally, interoperability between software components. Interoperability throughout industrial solutions has been, and continues to be, the founding principle of the OPC Foundation. Users face questions about how to integrate these different components (hardware and software) efficiently; how to move data efficiently or securely; how to keep solutions flexible so they can be changed to take advantage of new solutions in the future.

When we talk about new markets, we need to look at what we now call IoT or Industrie 4.0. It's fundamentally the same need – the need for interoperability – but, what differs is scale and time-to-market pressures. Scale, with respect to hardware and the growing number

of devices. Innovation in IT is now happening with short development cycles and increasing time-to-market pressures. These new pressures will only further increase the adoption of OPC UA because it's designed to address exactly those needs.

CLARK: What about other interoperability standards competing with OPC UA? Do they exist, on perhaps an architectural level or even on a protocol level?

ANHALT: Well, that's a good question. The short and simple answer is, no.

First, there is no competing standard on the architecture level. When one looks at the combination of technologies or features that OPC UA integrates – information models, namespaces, semantic information, multiprotocol support, and security – the mixture of these, and other elements of OPC UA, is unique and there is just no other standard that combines and integrates all that.

Secondly, when you mention protocol level, it's true that OPC UA will sometimes be compared, and is often miscategorized, as a protocol. That's not to say that there may be scenarios and use cases where our goal can be achieved easily by implementing a protocol. But that's not really interoperability. A protocol is a different thing than an interoperability standard. It's not a correct comparison to liken OPC UA to a protocol.

CLARK: Can you comment on adoption of OPC UA as the interoperability standard within the automation industry versus adoption within IT? Has it not been the case since the introduction of IoT, that folks working in either world have had a hard time understanding each other? Has OPC UA been able to bring these two worlds together?

ANHALT: Well, another good question and it's certainly true that there is an adoption gap between IT and OT, including a cultural gap. I would also add that there is an administrative gap between OT and IT in some organizations. I certainly believe that OPC UA has helped to bring these two worlds together. For example, when we look at technology, there is a deep similarity between information models, which I've already mentioned, and object-oriented design, which is a well-known, established concept in IT. So, the information modeling, based on the OPC UA standard, is not foreign to people experienced in IT.

The same is true for security standards; OPC UA is using, or leveraging, what has been implemented successfully in the IT industry for many years. Elements like TLS encryption or X509 certificates, to give a couple of examples. Within OPC UA, there are technological elements that help bring these two worlds together.

Let's observe what the big IT players are doing; those who have entered the IoT market. Microsoft Azure and Amazon AWS for example; SAP with their Go to Market strategy and associated reference architectures; they all include OPC UA.

There is a third element, which I've observed in several meetings recently. I see that there's increasing knowledge about OPC UA among the IT systems integrators. For example, historically, companies have engaged in enterprise IT system integration projects but, now, they are starting to expand their portfolios and move into the industrial IoT market. What I now realize is that they have knowledge about OPC UA and their position now is, "please give us an OT interface that supports OPC UA and we know how to integrate our solution using that interface". So, the short answer is yes; OPC UA has been able to bring these worlds together.

CLARK: Let's stay with the integration of IT and OT for a bit. Can you please share an overview of typical IT/OT use cases with our readers?

ANHALT: Yes, although, may I point out that the term "use case" is sometimes used broadly and can mean many different things. Perhaps some readers would expect me to explain, in some detail, different applications like OEE [overall equipment effectiveness], predictive maintenance, quality assurance or typical industrial IoT applications that require IT/ OT integration. These are interesting topics, but I don't want to focus on them. Instead, I would prefer to briefly outline some ways that OPC UA can be used to handle the interoperability problem. You may prefer to categorize these as data integration use cases; therefore, I'll try to outline the benefits and the relevance of OPC UA regarding these particular use cases.

The first group of use cases could be summarized as "implementing a basic interface". Perhaps your company is a machine vendor or maybe a PLC vendor and you want to add an interface to your device that can be used for integration. Here is where OPC UA can be used. The same is true at the basic interface-to-software application – HMI's, SCADA, or perhaps an MES system – A vendor may be looking for an interface that can be used for integration. OPC UA is a perfect choice.

A second use case deals with "data aggregation". You may want to add an OPC UA aggregation server to your solution. This means that an aggregation server is used to collect data from many different data sources, which could be OPC UA data sources or perhaps others. The aggregation server integrates those data into one OPC UA server. This application has quite a few benefits. It may make communication between OT and IT applications more efficient by reducing communication overhead and communication cost. It may make configuration simpler. Aggregation servers help users build better-performing and easier-to-maintain applications.

I call the third use case, "interface abstraction". This is the most abstract use case; by that I mean that OPC UA can be used to shield away differences in OT in order to provide a unified interface to IT. Using an interface abstraction strategy could help segregate various machines or perhaps, if we think about corporate level exchanges, it could be used to isolate locations.

CLARK: What further details can you share with us regarding the three sub-categories you've just identified? Let's start with vertical communication between OT and IT.

ANHALT: There are many details I could talk about, so let me pick just two. The first one is the feature I mentioned earlier regarding multiprotocol support. Users have a choice between different protocols that are supported by OPC UA. These fall into two broad categories. One is called the Pub-Sub [publisher/subscriber] model and the other is called Client-Server. Each model has its pros and cons and it's helpful to be able to choose. For example, if you have a scenario where scalability is key – a lot of data points which need to be communicated every time data changes – it is best handled by a Pub-Sub protocol.

Whereas, a use case where you want to read out a certain value only occasionally – perhaps based on interaction with a human-being during configuration – this type of scenario is where the Client-Server protocol comes in handy.
Another aspect, which I mentioned earlier, deals with security. We all agree, as soon as we start talking about cloud applications, security becomes a crucial element. By adopting proven standards and by making security configurable, OPC UA helps users set up secure OT and IT communications. For example, OPC UA makes it possible to implement roles and configure role-based access rights to OT data. Another example is preventing access to "secret" process data from a maintenance person, one who uses a certain application to access the system for maintenance purposes; this person may even be an external user. These are a few simple examples of something you can do with OPC UA; you configure security to model certain roles and give role-based access for IT applications to OT.

CLARK: And how about horizontal communication between OT and IT… so, between devices?
ANHALT: Again, I'll pick two examples. The first, relevant scenario describes communication between sensors and supervisory controllers. OPC UA Pub-Sub can be implemented on devices with limited resources. For example, there are basic OPC UA server implementations that support Pub-Sub requiring only 200 kilobytes of code, or even less. When implementations are that small, they certainly do not include full-blown security. I mean, a cryptographic algorithm certainly requires more resources than that. However, in reality, security may not be needed at that level – it is certainly relevant for IT/ OT integration – but since this particular application is within the OT domain, it may be acceptable to relax some of these strict security requirements.
The second use case I want to mention, only briefly, is PLC to PLC communication. Here, OPC UA can also help, in combination with deterministic IP communications, but I guess that's a broader topic that potentially deserves separate treatment.

CLARK: And last, but not least, what about use cases of OPC UA within IT… so, within the upper layers of IoT solutions?
ANHALT: I guess one might ask a clarifying question, like, "what do you really mean by upper layers?" IT certainly is expanding; and it's coming closer and closer to the machine. Let me begin to answer this question by addressing OT at the edge.
When referring to the extension of on-prem, central platforms, or cloud platforms, designers are using OPC UA between various software components running at the edge. This could include a component for edge analytics and a separate gateway component that translates data from a central PLC into OPC UA. Then, these two components talk between each other, in terms of OPC UA data models within the IT realm. That's what I mean by "edge".
Now, when we think about the other "upper layers" such as MES systems or applications for predictive maintenance, OPC UA can certainly be used there. Having semantic information available can be very interesting for analytics, especially since the application is using OPC UA in its standardized data format. This is extremely attractive for end users. Think about not having a proprietary data format that requires a lot of migration effort, especially if the user ever decides to move to another platform.

CLARK: So, as a final question on the topic of use cases, is OPC UA only relevant for green-field plants and factories? What about integrating OPC UA into my existing, brown-field production line?
ANHALT: Well, it's probably true that OPC UA has a reputation that it's only relevant for greenfield plants, especially where OPC UA has been integrated into the devices and the controllers that are deployed in a new plant. Indeed, if that's the case, it's easier to use OPC UA to integrate with IT.
However, when you look at solutions and products that have been available for many years, it's amazingly easy to deploy gateways or data integration solutions into brown-field applications that acquire data from non OPC UA data sources. You then simply add an OPC UA interface to these data sources and integrate these data sources into OPC UA-centric architectures and solutions. •

ABOUT ABOUT THE INTERVIEW PARTNER – CHRISTOPHER ANHALT:

Dr. Christopher Anhalt works as Business Development Manager for Softing Industrial Automation GmbH in Haar near Munich, Germany. Dr. Anhalt as a 20-year-track record of engaging with Enterprise IT and Industrial Automation, at organizational culture- as well as technology levels, enabling him with sensitivity and knowledge to develop solutions for the Industrial IoT market.

Dr. Anhalt has been an active member of standardization groups in VDI and PNO organizations, and acts as Senior Representative for the OPC Foundation. He studied Mathematics, Computer Science and Electrical Engineering, and holds a PhD degree in Mathematics from Bonn University.

OPC FOUNDATION HEADQUARTERS
OPC Foundation
16101 N. 82nd Street, Suite 3B
Scottsdale, AZ 85260-1868 USA
Phone: 480 483-6644
office@opcfoundation.org

OPC FOUNDATION EUROPE
opceurope@opcfoundation.org

OPC FOUNDATION CHINA
opcchina@opcfoundation.org

OPC FOUNDATION JAPAN
opcjapan@opcfoundation.org

OPC FOUNDATION KOREA
opckorea@opcfoundation.org

OPC FOUNDATION ASEAN
asean@opcfoundation.org

OPC FOUNDATION INDIA
opcindia@opcfoundation.org

www.opcfoundation.org