Electronic Specifier design

June 2013 / Volume 3, Issue 6

www.electronicspecifier.com

Auto Alliances

Why the move from mechanical to electrical in-car systems is prompting industry collaboration

Reader Offer!
Win a Microchip PICDEM 4 Demo Board!

In this issue:

Speaking the same language

As industrial automation systems become more complex, Sally Ward-Foxton asks how do we make sure that all the machines can talk to each other in a secure and reliable way?

Ten years ago, it was common for industrial control system integrators to subscribe to the 'buy everything from one vendor' school of thought. Today, the picture is a lot more complex. Multi-vendor platforms have become much more common as people begin to question the idea of buying everything from a single vendor, partially due to significant technology advances, partially down to expectations driven by the world of consumer electronics and the expectations of engineers leaving university.

The increase in brand new systems that use hardware and software from multiple vendors is not the only factor – older systems are being upgraded in this way too.

"We're starting to see a trend of existing automation systems being retooled with additional hardware and software applications to extend the life of the systems, that come from different vendors," observes Thomas J. Burke, President and Executive Director of the OPC Foundation. Burke says that the proliferation of smartphones is also playing a part.

"Many of the end-users in factory automation and process automation are starting to use smartphones and tablets as part of their daily lives, as they monitor their corresponding facilities," he says. "Although we are still in a Microsoft world, we are seeing quite a trend for using non-Microsoft applications and devices to be integrated into the total infrastructure and systems."

Interoperability

Interoperability is obviously a key requirement to make all the components work in a cohesive system, and that's where the OPC Foundation comes in. The non-profit organisation has developed an open standard, recognised by the IEC, which specifies communication of real-time data from the plant between control devices from different manufacturers. It has also become the de-facto standard for connecting factory control and process automation devices to HMIs (human-machine interfaces) and SCADA systems (supervisory control and data acquisition – a type of industrial control system typically used in infrastructure and large-scale automated facilities). Today, the standard has evolved to facilitate alarm processing and notifications, as well as services for historical data retrieval.

"The whole concept of islands of automation is going to be a thing of the past," Burke says. "There is a need to bridge and connect all of the disconnected systems together to lower cost and increase revenue through increased automation. It's become very important to be able to connect up many of the embedded devices already developed as well as future embedded devices into a cohesive integrated system."

"End-users and system integrators want to be able to choose best-of-breed products from multiple vendors and expect that all of these products interoperate

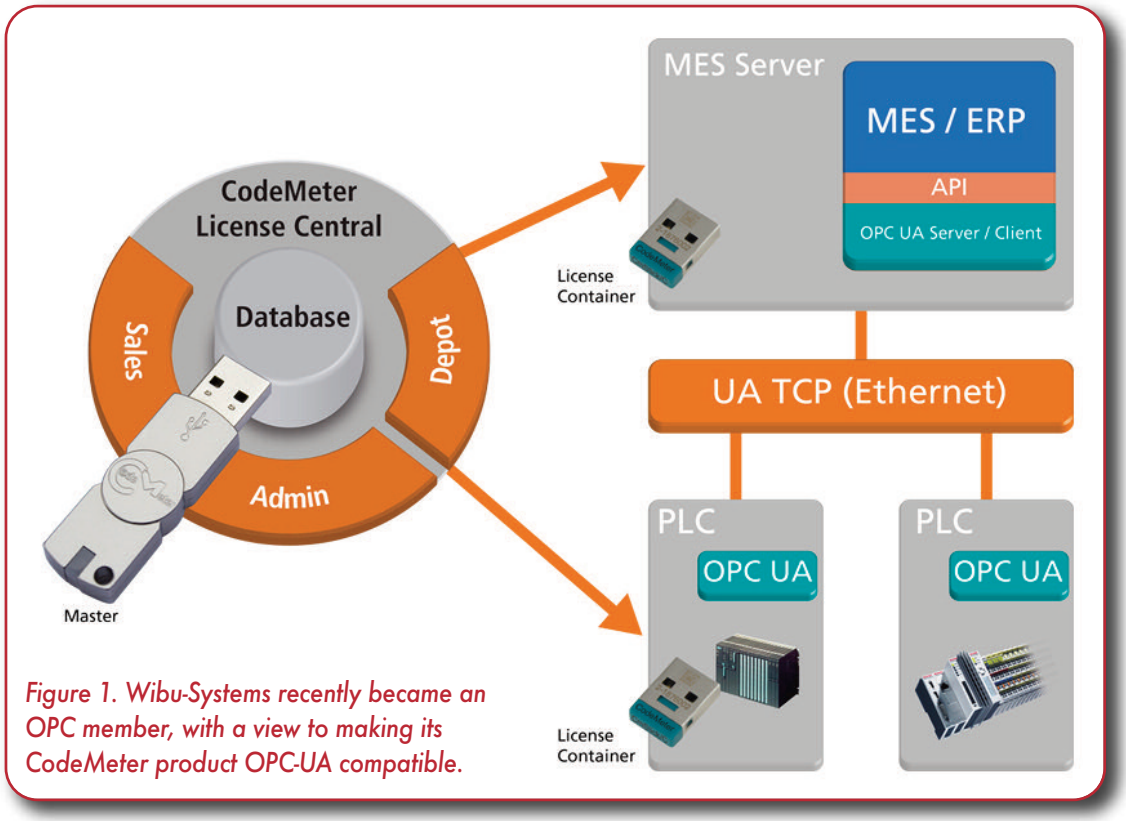


Figure 1. Wibu-Systems recently became an OPC member, with a view to making its CodeMeter product OPC-UA compatible.

together," he adds. "The OPC is all about collaboration – we are working on collaborating with vendors and consortiums for total interoperability."

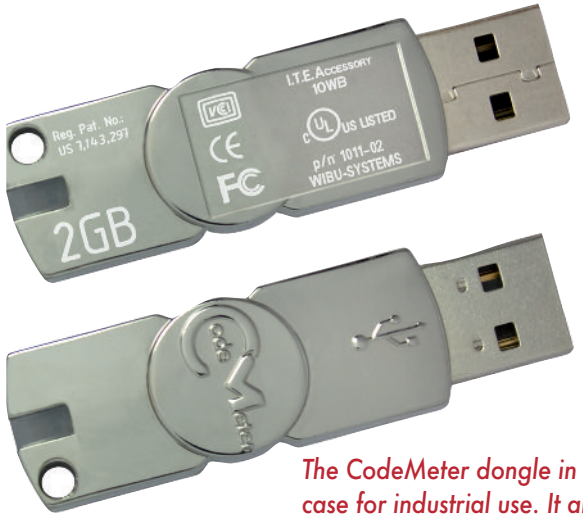
The Technical Advisory Council of the OPC Foundation includes members from all the major automation players, and they are actively part of the Foundation's working groups. The Foundation's most recent development is OPC-Unified Architecture, an infrastructure for multi-vendor, multi-platform secure reliable interoperability. This architecture provides a mechanism for data integration from embedded devices all the way up to the enterprise, or as Burke puts it; "complete connectivity from the shop floor to the top floor".

OPC-UA provides the infrastructure to take data/information from multiple vendors' equipment and be able to model it in an intelligent way; this allows generic applications to view and operate on the data and the information, so that intelligent decisions can be made to streamline operations.

Here's an example. In the oil and gas industry, a master control station in a central location controls and receives data from all the subsea equipment, in what's called a master control system (MCS). Each master control station is proprietary, and the subsea control modules have to come from the same vendor, to be able to communicate. Meanwhile, the oil platforms themselves use a distributed control system (DCS), where each subsystem or piece of equipment has its own controller. The master control station is the link between the MCS and DCS (between the subsea equipment and the platform). OPC-UA has been selected by the MCS and DCS Interface Standardisation network (MDIS), an organisation which is working to standardise the interface between MCS and DCS systems by simplifying data communication links while increasing the data quality. Eventually, devices in the subsea will be able to directly connect with DCS systems, as well as providing data to the enterprise. Essentially, OPC-UA will make data, and information about the data, available to generic applications that have no required knowledge of the applications or devices. Previously, only very high-level data from these devices was available.

Safety and Security

While interoperability is critical in getting industrial automation equipment to communicate,



The CodeMeter dongle in its metal case for industrial use. It also comes as a smart card.

there are other factors to consider – safety and security are also very important.

"Safety protects the people and the environment against the malfunctions of a machine, whereas security protects the machine against human errors or attacks from the outside," explains Oliver Winzenried, CEO of Wibu-Systems, a company that specialises in digital asset, intellectual property and integrity protection against piracy, reverse-engineering and code tampering.

Winzenried says that many different types of security threat exist in the industrial automation world, citing the top ten security threats to industrial control systems (see box).

"Honestly though, we come across even more types of attacks," he says. "In the realm of Integrated Industry or Industry 4.0, control devices are more connected than ever before. Data related to both the production process and the customer's product to be manufactured are shared along with the intellectual property and the know-how that come along with it."

Wibu's CodeMeter licensing and protection technology is designed to guard against all these security risks. It includes software development tools and a wide range of hardware form factors to securely store license information and cryptographic keys either in a license file or in a smart card based device. CodeMeter dongles are designed for the industrial world, with extended operating temperature range and EMC protection. CodeMeter includes solutions to protect embedded software from copying, reverse engineering and manipulation, using a digital certificate chain of trust. It also comes with CodeMeter License Central for generating, managing and rolling out licenses.

CodeMeter and OPC-UA

Wibu recently joined the OPC, with a view to making its CodeMeter range OPC-UA compatible (Figure 1). OPC-UA on its own does provide security; security mechanisms authenticate and validate the secure operation between applications and devices, and security can be configured right down to the finest levels of granularity, to say which users are authenticated and allowed to read and write data from a given device. Wibu are aiming to simplify this security process by adding CodeMeter, and provide additional levels of security for applications which require it.

"The OPC-UA standard features built-in communication encryption and network device authentication of its own," Winzenried says. "Wibu-Systems is currently cooperating with the OPC Foundation in order to integrate CodeMeter with the OPC infrastructure at both server and client level."

The outcome will result in the ability to transfer software licenses using the OPC-UA communications protocol, storing certificates in accordance with OPC-UA directives and deploying licenses and certificates in an OPC-UA compatible way.

In summary, industrial automation equipment now increasingly speaks the same language, no matter what vendor it's from, as a result of a collaboration between the major players via the OPC Foundation. The Foundation's architecture for interoperability, OPC Unified Architecture, is a mechanism for integrating data from every level of an industrial facility and bringing it to the enterprise level so that intelligent decisions can be made. It's being rolled out in the oil and gas industry, amongst others. While OPC-UA includes a good level of security, third party add-ons, like Wibu-Systems' CodeMeter, can help simplify this and increase security levels in particularly sensitive applications.

The top ten security threats to industrial control systems, as identified by the Federal Office for Information Security in Germany:

- Unauthorised remote service access
- Online attacks using office IT networks
- Attacks to commercial off-the-shelf systems, COTS in ICS, like OS or networks
- Distributed Denial of Service Attacks (DDOS)
- Human mistakes and sabotage
- Intrusion of malware using USB sticks or other hardware
- Reading and Writing of messages in ICS
- Unauthorised access to resources
- Attacks to Networks
- Failures and external events

Visit www.opcfoundation.org
Return to contents page.