AUTOMATION TECHNOLOGIES

INTERNATIONAL ONLINE EDITION

5

October 2016

VEREINIGTE FACHVERLAGE

Industrial Automation

WORLDWIDE OFFICIAL PARTNER 2016

Secure communication for Industrie 4.0 systems

IAS INDUSTRIAL AUTOMATION SHOW

Shanghai's success
Automation plays a vital role

RFID solution
Safety supervision and tracking in the food industry

Energy chains
Highly flexible cables for every movement

Machine Vision
3D cameras in digital imaging applications

Security – The backbone of the global smart manufacturing revolution

Nicole Steinicke, Oliver Winzenried

Many companies are affected by product or brand piracy, hacking and cyber-attacks. This costs jobs, revenues and opportunities and results in an estimated damage. So there is a need for security.

The commercial history of mankind can be read as a history of more and more elaborate predatory acts: When the second industrial revolution introduced the world to electricity and specialized labor, piracy took the form of product counterfeiting. Once IT and electronics became part of the game, it was not just products, but their inherent qualities and functions that were copied. Now that cyber-physical systems are coming as part of Industrie 4.0, we are entering a new stage of piratical sophistication, where digital identities and business models are the top targets. Paradoxically, the rise of software piracy is powering the evolution of professional and regulated know-how protection, software license management, and security measures on a global scale.

Wibu-Systems is one of the leading suppliers in the digital rights management (DRM) anti-piracy industry. The company is a specialist in protection of software-, data-, and media-related intellectual property against piracy, license management and integrity protection for cyber-physical systems, IoT, M2M and connected control systems. But which possibilities do we exactly have to prevent software and product piracy? What kind of products can we use to provide effective protection against espionage and cyber-crimes?

Oliver Winzenried, founder and CEO of Wibu-Systems, *in conversation with Nicole Steinicke*

Wibu-Systems is one of the technology leaders in the global software license lifecycle management industry. What is your main expertise, and how does that translate into your offerings?

'Perfection in Protection, Licensing, and Security' is our company's vision. First, we provide solutions against counterfeiting and reverse engineering. This requires strong encryption of digital assets, associated with secure key storage. Second, we offer flexible licensing for a versatile configuration of machine and device features. This includes the integration of license entitlement directly into the business process, i.e. ERP systems or e-commerce platforms. Our third focus is security against tampering, cyber-attacks, and even unintentional manipulation.

About Wibu-Systems

The privately held company founded by Oliver Winzenried and Marcellus Buchheit in 1989, is an innovative security technology leader in the global software licensing market. Wibu-Systems' comprehensive and award winning solutions offer unique and internationally patented processes for protection, licensing and security of digital assets and know-how to software publishers and industrial manufacturers who distribute their applications through PC-, embedded-, mobile- and cloud-based models.

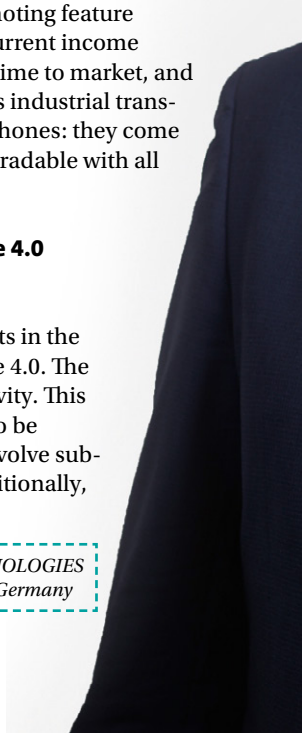
How can developers and manufacturers benefit from your products?

Industrie 4.0 subverts the traditional paradigms and, by transferring value from hardware to software, increases overall performance, from productivity to efficiency. The advantage is shared with customers, who can enjoy tailor-made products. It is software licensing that powers this fine-grained customization process. Intelligent device manufacturers and vendors can leverage these monetization opportunities by promoting feature on-demand business models that provide recurrent income streams with software upgrades, reduce their time to market, and reach new target groups. You can compare this industrial transformation with the trend in consumer smart phones: they come with a set of basic functions and are then upgradable with all sorts of features through an app store.

What are the new requirements of Industrie 4.0 and the Industrial Internet of Things (IIoT)?

Industrial IoT devices will be basic components in the machines and factories that make up Industrie 4.0. The underlying common denominator is connectivity. This makes it essential for each connected device to be assigned a tamperproof identity, which will involve substantial use of hardware secure elements. Additionally,

Author: *Nicole Steinicke, editor AUTOMATION TECHNOLOGIES and Oliver Winzenried, CEO Wibu-Systems Karlsruhe, Germany*



data is becoming much more relevant in production processes. In additive manufacturing, for instance, the product is completely defined by its production data. Protecting the intellectual property of such data and its integrity is business critical for manufacturers.

Would you say that the industry as a whole has the same focus on security, or is it something that needs to be pushed more?

We are currently only in the infancy of the IIoT, and more effort is needed to propagate this model. When new technologies start to be deployed on a larger scale and delivered in terms of features and convenience, everyone will be jumping on this bandwagon. At the moment, however, there are concerns about security; usually, security measures are implemented when incidents happen; with smart manufacturing, we see security frameworks being implemented at an early stage, so that security is already present by design or by default. Security by design means that devices are equipped with security configurable options, while security by default means that the user will receive the device configured in a way that a certain security level is preserved, regardless of the user's setup or preferences.

Looking towards Industrie 4.0, what are the obstacles to its successful implementation?

First of all, I believe that the message of flexible production needs to reach all manufacturing stakeholders. The next obstacle is the considerable lifespan of production machines, which usually stretches to twenty years or more. Any IIoT solution and the related security enhancements therefore need to be applicable in the brownfield and greenfield alike.

Where would you see the role of national governments? Can the public sector support the private sector?

It is my understanding that governments of all major world economic powers have already included connected manufacturing in their digital agendas, are supporting research and development projects, creating a legal framework to bolster Industrie 4.0, and promoting standardization as a means of igniting international cooperation and free trade. Looking specifically at Germany, we are directly involved in several projects that are funded by national institutions.

At which points are you actively involved in research and development?

I would like to mention two projects: "IUNO", funded by the German Ministry of Research & Development, BMBF, is the German national reference project for IT security in Industrie 4.0. It brings 21 parties to the table - 14 companies and 7 research institutes focusing on 4 use cases defined by Bosch, VW, Trumpf and Homag. Wibu-Systems is mainly working on secure remote access and the development of a technology data marketplace. The former uses our sophisticated industrial grade secure elements with different form factors, like USB sticks or SD cards; and the latter will be based on CodeMeter, our multi-vendor digital rights management solution. A second R&D project we are currently working on is "Secure Plug & Work", which resembles the concept of Plug&Play for USB devices in that it makes it easier to replace parts and components in machines with automatic configuration, and adds a layer of security to the process. Our CodeMeter technology provides secure key storage and certificate deployment via and for OPC UA communication.

There seems to be a lot of competing companies in these projects — how does that work? Is everyone pulling together at the moment?

When you are working on standards, you have no option but to work with all of the global titans, including competitors. Smaller, medium, and even large companies need to rely on a certain level of interoperability, and standards are the way to ensure flawless and secure communication when a large group of machines is brought together. Competing companies have an advantage when it comes to collaborating on the shared underpinnings, that is, the standards. They can then show their unique strengths and advantages individually when it comes to implementing these standards and developing the factors that distinguish them. This is the point where competition is at its strongest.

Why does Wibu-Systems take part in these industry initiatives?

Even though we are taking part in many industry initiatives, we only focus on those that concern our core technological values: protection, licensing, and security. The opportunity to work in markets as diverse as industrial automation or medical technology, each with its own requirements and customers' needs, allows us to understand the real market demands, enrich our solution, and fulfill the expectations of our users.

MULTIMEDIA CONTENT

In conversation with Oliver Winzenried at the Industrial Automation Show Beijing

https://youtu.be/6g8tn6k3kNg

www.wibu.com