Hardware-based solutions secure machine identities in smart factories

Dr. Josef Haid, Infineon

Security is a cornerstone of Industry 4.0. Secure cryptographic identification of machines and devices protects smart factories against manipulation and data theft. Hardware trust anchors implemented with dedicated security chips provide robust protection for security keys while lowering overall security expenses for device manufacturers.

Figure 1. Manufacturers need powerful, reliable security technologies to secure communication between devices and machines within heavily networked infrastructures.

The Internet of Things (IoT) is connecting more and more smart devices and machines to create smart factories (known as Industry 4.0 or Industrial Internet). Although these highly automated, decentralized factories promise greater efficiency and flexibility across production processes, they are also exposed to attacks from cyberspace as they rely on Internet connectivity. Software measures alone do not generally provide sufficient protection against these attacks. Hardware-based trust anchors are required to effectively protect smart factories. Infineon OPTIGA security controllers provide scalable security for embedded systems, thus protecting machines, data and intellectual property in smart factories.

Smart factories and connected supply chains are presenting many manufacturing companies with new security challenges. Malware, manipulation, sabotage, faulty firmware updates and counterfeit components are examples of digital threats that can bring entire production lines to a halt and may lead to significant costs and loss of image. The tiniest security gap in a company infrastructure can lead to theft of data, intellectual property (IP) and process know-how. Safeguarding this sensitive information calls for tailored solutions that deliver end-to-end protection yet also strike the right balance between security performance requirements and financial constraints. Manufacturers need powerful, reliable and scalable security technologies to safeguard communication between devices and machines within heavily networked infrastructures.

In this context, secured identities for machines provide the anchor for implementing any measures to protect electronic exchange and storage of data. As known from daily life where ID cards or passports are used for identification of humans, secured identities are used by machines to reliably identify each other. But even these secured IDs digitally stored on machines could become the subject of attacks and theft. Hardware-based security solutions based on security chips are the best way to efficiently protect machine identities as well as data and communication. Security controllers provide a greater level of security than concepts that are purely software-based as it is relatively simple to read and overwrite software.

Integrating security chips into all critical nodes helps to prevent unauthorized access to production networks and smart factories. Security chips continuously check component authenticity as well as data and system integrity to prevent manipulation. They are capable of verifying the authenticity of software updates and enable protection of remote access activities. Last but not least they offer robust protection against low-quality, counterfeit spare parts and repair tools. Chip solutions also provide cryptographic functionality such as public key cryptography and key management. Although these functions could be implemented in both software and hardware, for industrial applications, a hardware-based solution such as a dedicated security chip has clear benefits and can add real value for manufacturers.

Silicon manufacturers such as Infineon Technologies use highly secured, certified processes to personalize hardware trust anchors, i.e. to provide a secure identity to each security chip. This often includes a set of keys and certificates stored on the chip in order to allow other devices in the industry automation system to securely authenticate a remote device, to build up a secured connection, and exchange data in a protected way. Proper hardware anchors are security-certified components that are also equipped with measures to protect them against physical attacks. As such they offer protection during transit. In other words, a hardware anchor protection is so robust that it does not need special security measures to be shipped using cost-efficient logistics channels. This not only applies to shipping the security chip itself but, more

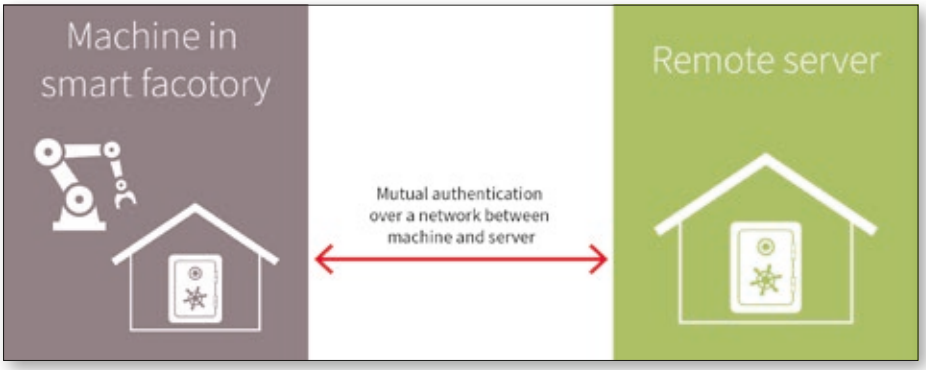

Figure 2. Mutual authentication of machines over a network

importantly, also to shipping devices that contain a hardware anchor with customer-specific keys. These physical protection capabilities can reduce costs particularly during installation and delivery processes.

Mutual authentication refers to two parties authenticating (securely identifying) each other at the same time. In the context of smart factories, this could be a server and a machine authenticating each other before starting a critical remote maintenance task such as a firmware update or adaptation of critical parameters. In this scenario, the secure identity stored in the machine hardware anchor is verified by the server and vice-versa. The hardware anchor contains the secret keys and offers functionalities to verify the secured identities of the other parties. It usually does this using a public key infrastructure (PKI) scheme.

When an industrial automation system is set up, the computing and controlling components are equipped with a specific version of the relevant software package. After this point in time, the smart factory must be protected against unintended changes to the software as this could disrupt production, threaten plant safety and enable know-how to be stolen. At the same time, it must still be possible for software to be updated intentionally, for example, for maintenance purposes or to change certain features. Robust trust anchors also support this use case, for example by enabling a secured boot process. The underlying concept here is that code is only executed after its integrity has been verified in advance by the hardware anchor.

By using state-of-the-art microcontrollers and stand-alone security controllers such as the OPTIGA product family it is possible to implement a hardware-based trust anchor that protects the system software against attacks. The key to successful protection lies in the use of open industry standards that allow seamless connectivity across existing and new systems.

For many manufacturers, protecting their products against counterfeit is a top priority. With its OPTIGA Trust product family, Infineon offers a complete security solution comprising a chip and software for electronic accessories. The chip is based on asymmetric cryptography and is easily integrated into electronic accessories thanks to its compact package (2 mm x 3 mm) and turnkey set-up. In order to check whether or not a part is genuine, the host system sends a challenge (essentially a random number) to the chip in the accessory. The OPTIGA Trust subsequently generates a response using the chip-individual key. If successfully authenticated by the chip, the accessory or replacement part is accepted by the system and can be used without restrictions.

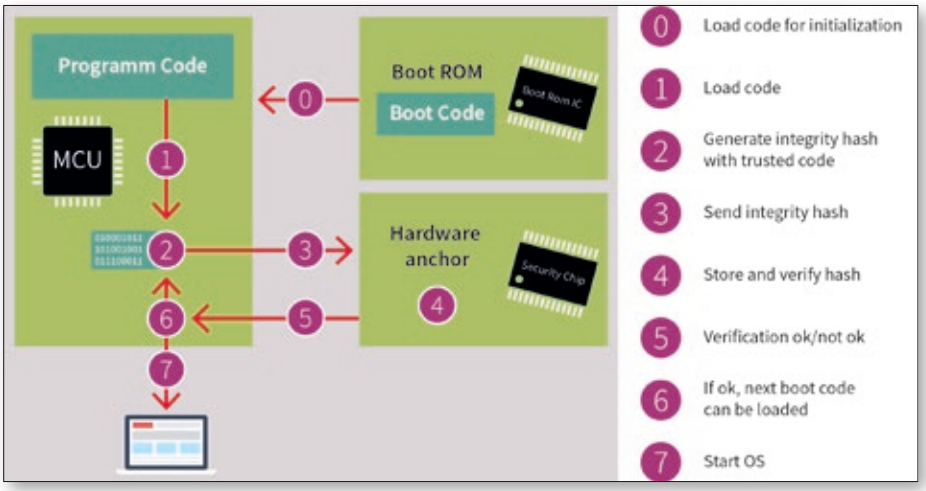

Figure 3. A secure boot process ensures platform integrity of computing and control systems in industrial environments.

Following the same principle, the OPTIGA Trust E was specifically developed for protection of high-value goods in industrial applications. It features an I2C interface as well as an extended temperature range (-40 to +85 °C). This would be of benefit to manufacturers of wind turbines, for example, who would want to avoid damage to the overall system caused by counterfeit replacement parts. Both the OPTIGA Trust and the OPTIGA Trust E are delivered with code to simplify integration of the chip into spare parts.

Preventing counterfeit through authentication is just the first step in the process of safeguarding the overall system. Further security functions are necessary to protect application-specific information (e.g. customer data and intellectual property) and the overall operating procedure. The OPTIGA Trust P security solution comes as a security controller with a Java Card operating system and can be flexibly programmed for a wide range of applications. This in turn allows the applications to be managed in the field as OPTIGA Trust P supports a Global Platform specification.

The OPTIGA TPM (Trusted Platform Module) portfolio covers the broadest range of security requirements. These security controllers are based on the international standard of the Trusted Computing Group, an association of leading manufacturers from the IT industry. TPMs have already successfully proven themselves in computer applications, and this technology is now making its way into new networked systems and devices such as routers, industrial facilities and cars.

The members of the OPTIGA TPM family have been validated and security-certified according to the Common Criteria certification process. To permit easy integration into a system, the OPTIGA TPM family supports commercial and open source code for Windows and Linux, including derivatives and Infineon tools. The OPTIGA TPM family comprises a broad range of security controllers complying with the standards TPM 1.2 and TPM 2.0, which, depending on the application area, are available for various temperature ranges and offer different interfaces such as SPI,I2C and LPC.

One area where OPTIGA TPMs can be used in industrial applications is secured data transmission or storage. In such an application, the key factor is the combination of

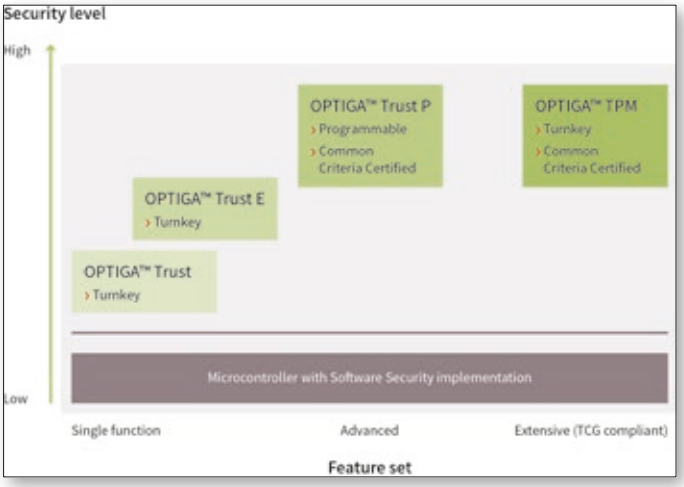

Figure 4. The OPTIGA product family offers scalable security solutions for a wide range of industries.

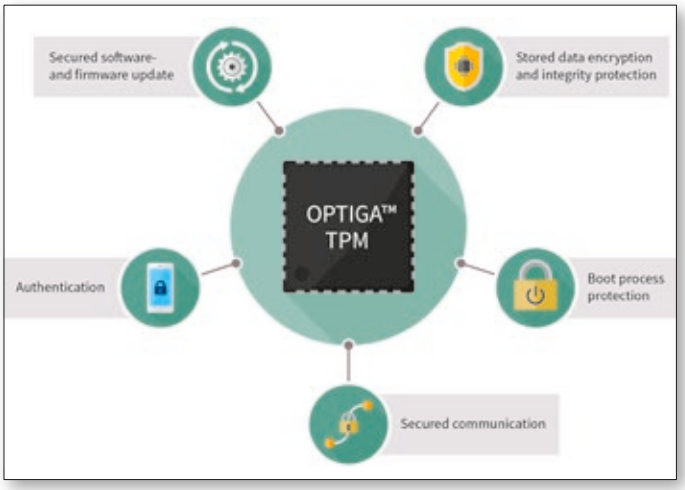

Figure 5.Typical use cases of OPTIGA TPM

secured hardware and software-based security mechanisms. The use of a TPM supports monitoring and/or protection of the system integrity. This security controller additionally permits reliable component identification, which only allows reliable and trustworthy components to communicate with each other.

For secured remote access, e.g. for system maintenance or software u pdates, t he T PM controls access to the system by means of device authentication. The OPTIGA TPM also provides secured storage for secret keys and protects cryptographic operations. For typical applications such as for the SSL/TLS protocol, keys are stored in the secured store of the TPM rather than in the memory of the main processor and are only processed internally. This offers the advantage that the secret keys are protected against external security risks. In conjunction with TPM and security mechanisms such as encryption, the system code is also protected against manipulation. As a standardized component, TPMs come with a rich ecosystem of available drivers and software stacks allowing customers to easily integrate security with limited integration effort. ■