An OPC UA based approach for dynamic-configuration of security credentials and integrating a vendor independent digital product memory

Marco Blume[1], Nils Koch[2], Jahanzaib Imtiaz[2], Dr. Holger Flatt[2], Prof. Dr. Jürgen Jasperneite[2],

Dr.-Ing. Miriam Schleipen[3], Dr.-Ing. Olaf Sauer[3], and Steffen Dosch[4]

[1] WIBU-Systems AG, Rüppurrer Str. 52-54, 76137 Karlsruhe, Germany

marco.blume@wibu.com

[2] Fraunhofer IOSB-INA, Application Center Industrial Automation, Langenbruch 6, 32657 Lemgo, Germany

{nils.koch, jahanzaib.imtiaz, holger.flatt, juergen.jasperneite}@iosb-ina.fraunhofer.de

[3] Fraunhofer IOSB, Information Management and Production Control, Fraunhoferstr. 1, 76131 Karlsruhe, Germany

{miriam.schleipen, olaf.sauer}@iosb.fraunhofer.de

[4] wbk Institute of Production Science, Kaiserstr. 12 , 76131 Karlsruhe, Germany

steffen.dosch@kit.edu

Abstract: This paper presents an approach to securely integrate industrial devices into automation systems with a minimal engineering effort. A special specific focus is on the needed communication architecture that is based on the platform independent and vendor neutral technology OPC UA. The paper also describes the need of a digital product memory besides a life cycle data harvesting to facilitate such seamless integration; this is by means of presenting semantics of operations to an external system. As part of the work, a case study has been identified; different architectural aspects are evaluated and essential system components are realized/implemented/integrated as a proof of concept. Principle results include the implementation of a BeagleBone Black-based Secure Plug & Work I/O field device with an extended real-time industrial communication interface and a semantically enriched OPC UA server that provides vendor neutral configuration and an I/O data service interface. Furthermore, the result provides a platform independent and standardized way to represent a field device to external systems, to enable intelligent technical systems to communicate and orchestrate a seamless and secure integration.

1 Introduction

Due to shorter product lifecycles and changing market conditions, current production systems must become more flexible. Industry 4.0 carries the vision of intelligent, self-configuring plants, which adapt automatically to changes, leading to reduced administration times [SF12]. In order to offer Plug & Work capabilities, adaption to industrial devices at multiple levels is required and various technological challenges have to be addressed [SH12]. Typically, when integrating a new device into a plant, the plant needs to know the type and the skills of the device in order to handle it accordingly. In addition to that, a digital product memory (DPM) embedded in the device provides a digital diary of the complete product life cycle [BB11]. Such information in the DPM allows offline diagnosis but often requires a vendor specific communication protocol for information exchange [SC10]. Since this data may be confidential, it has to be protected or even encrypted and only be accessible to certain users. Also, when a new device is plugged into a plant, security credentials have to be exchanged.

In order to integrate such a device into a heterogeneous environment, there is a need to express and exchange the description of functionalities, services, properties, skills, and security credentials for that device in a vendor neutral manner. OPC UA is seen as a de facto standard to model and securely exchange device specific complex information, platform/vendor independently [JI13].

This paper is organized as follows: section 2 provides a state of the art analysis along with some technological background. In section 3, a proposed communication architecture for a Secure Plug & Work device is presented. Section 4 describes a case study based on an exemplary application. Finally, section 5 concludes this paper.

In: Jasperneite, Jürgen; Jumar, Ulrich (Hrsg.): Jahreskolloquium Kommunikation in der Automation (KommA 2014). Lemgo, Nov 2014, ISBN 978-3-9814062-4-5

2 State of the art

Intelligent networks and self-configuration were already the objective of some research projects in order to provide Plug & Play (PnP) functionalities to arbitrary nodes and modules of a system. In “SOCRADES”, a service oriented architecture (SOA) on device level was developed [CW10]. The project proposed a framework for flexible service orchestration based on petri nets. However, every reconfiguration step results in manual effort. In order to achieve the objective of PnP, the system must react autonomously to changes. The EU project “Internet of Things at Work” (IoT@Work) [HM12] specified a Secure Plug & Work communication infrastructure taking industrial automation requirements into account and supporting autonomous network configuration and optimization. However, the project focused only on the lower layers of the communication system. Finally, the project “AutoPnP” [PNP14] dealt with automatically adding and configuring new components in automation systems, based on artificial intelligence concepts and algorithms. However, the project focused on the control level including manufacturing execution systems (MES) with decreased temporal requirements. Besides, several individual research works were directed towards self-configuration covering various relevant topics in this area. A semantic self-description is in most cases the basis to implement self-configuration of intelligent technical systems. In [OJ13], the communication between different manufacturing modules is analyzed and, based on the findings, a lightweight taxonomy to solve the problem of signal identification is introduced. The taxonomy is evaluated with a real implementation based on industrial standards such as OPC UA [MD09]. Another important aspect of self-configuration is the automatic configuration of real-time communication networks which usually require numerous manual configuration steps. A promising approach is presented in [LD12], [LD13] based on Profinet and in [GR08] based on Powerlink. Both works divide the configuration in different steps and have in common that they need an ad hoc channel for the configuration [MU14].

Furthermore, the cross-sectional project "Intelligent networking" within the Leading-Edge Technology Cluster ”Intelligent Technical Systems OstWestfalenLippe” (it’s OWL) aims to enable Plug & Play functionalities for intelligent devices by developing a reference architecture. Thereby, various interaction scenarios in dynamic and cooperative networks can be supported [IN14].

However, since most of above approaches are focused on automatic configuration of industrial components, little work [FK12] has been done in the direction of secure connectivity of such autonomous components. One of the key objectives of this work is to investigate possible techniques to enable a secure connectivity between distributed control systems by enabling security credential management using a digital product memory.

2.1 OPC Unified Architecture

OPC UA is a platform-independent industrial standard through which various kinds of systems and devices can communicate by sending messages between clients and servers over various types of networks. It fundamentally is about data modelling and transport. It uses object-oriented techniques, including type hierarchies and inheritance, to model information. An OPC UA address space allows information to be connected in various ways. The base OPC UA specifications provide only the infrastructure to model information, and encourage additional, industry specific information model specifications to be defined by vendors and standards organizations [JI13]. OPC UA can be mapped onto a variety of communication protocols and data can be encoded in various ways to trade off portability and efficiency. Furthermore, the OPC UA systems architecture models the OPC UA clients and servers as interacting partners. Each system may contain multiple clients and servers (see figure 1). Each client may interact concurrently with one or more servers, and each server may interact concurrently with one or more clients. An application may combine server and client components to allow interaction with other servers and clients at various levels in automation hierarchy for seamless vertical integration.

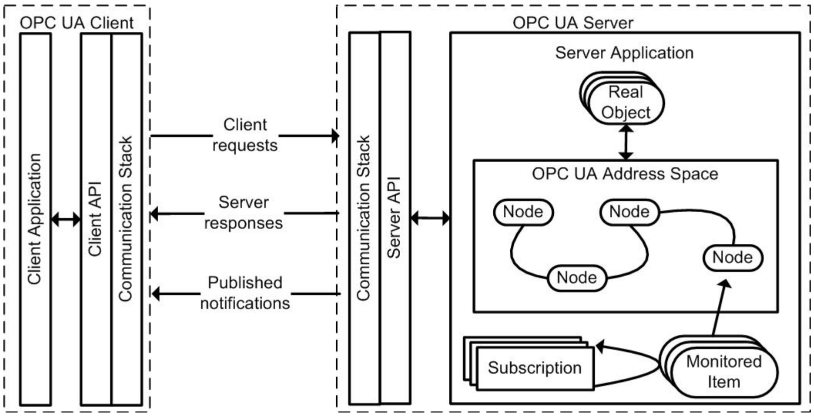


Fig 1: OPC Unified Architecture

OPC UA is designed in a way that individual implementations do not need to support all features and can be therefore downscaled to a limited scope, if desired. A service-based OPC UA implementation can be tailored to be just as complex as needed for the underlying application.

2.2 Digital Product Memory

A digital product memory (DPM) is used to provide better diagnosis during the life cycle of a product and to enable an optimized seamless production. A DPM is realized by either placing an active electrical memory or a passive identifier such as a QR code or an RFID- or NFC-tag directly at the product. An active DPM in the form of a small embedded system has the advantage of enabling direct access to it, whereas passive DPMs need a combination with centralized data storage, such as the cloud. On the other hand, passive elements can be much smaller. In either way, during the life cycle of the product, all relevant data (for example of the product's sensors) is collected and stored, such as temperature or driving speed. This enables monitoring whether the product was handled incorrectly. A product might warn about critical incidents such as increased temperature or pressure, or provide information regarding its carbon footprint that is calculated from its actual logistics and production emissions [BB11]. Another example would be supplying the product with GPS modules to track the position and to find it in case of a loss. Using digital product memories also makes the products smarter. They know in which state the production process they are. So, the intelligence is moved from the controller layer to the product itself. In terms of auto configuration, a DPM is not only used for diagnosis purposes, but also to store the initial configuration data of the different components.

For example a module in a production plant stores a model of its capabilities in the DPM and communicates it to a higher level instance when plugged in. This procedure is described in detail in chapter 3. A key role for the use of DPMs play semantic technologies [SC10], [YZ07] which are based upon that the meaning of information is coded in machine-readable data. They enable the data exchange of DPMs with intelligent environments and the user-friendly graphical interface with a DPM itself. OPC UA can be an enabler as a vendor neutral interface to represent and exchange contents of the DPM. Within well-defined smart spaces it becomes feasible to access and utilize real-world information from all kinds of different sources for the potential benefit of various stakeholders such as consumers, retailers, or manufacturers. By means of a link to digital data, physical artefacts - including products - may become “smart items” integrated into this novel information structure [SP10].

2.3 Security aspects of Plug & Work Systems

Self-configuring components, DPMs and vertical communication through the automation pyramid require a new view on the security of the transported information. Real-time information from sensor level is sent to the MES layer or cloud services. Information is transported offline with the component from the user to the manufacturer in a DPM. After connecting a new component to a machine or plant, the configuration data is downloaded to the component automatically from a PLC or SCADA system. All this is part of the Secure Plug & Work approach. This bidirectional communication flow opens new attack vectors to the component, the communication or the transported information. This is also known as Cyber Physical Attacks. Motivation for an attack is versatile. The user might manipulate logged data to claim warranty. A displeased employee might manipulate sensor values to disturb or sabotage the plant or production. A competitor might be interested in the parameters set in the component. This scenarios compromise the objectives Data Integrity and IP protection. This can be achieved by the use of signatures and encryption.

3 Proposal of a Communication Architecture for Secure Plug & Work Automation Systems

This section presents an OPC UA-based architecture solution that enables a dynamic configuration of security credentials (licensing, user access, etc.) for a device, as well as a vendor neutral exchange of information from a digital product memory [KA10]. The architectural design is a result of the joint research project SecurePLUGandWORK. The project is funded by the Federal Ministry of Education and Research (BMBF) in the context of call for proposals "Intelligent Networking in Production – A Contribution to the Future Project 'Industry 4.0'" (funding number 02PJ2590 ff). It tries to enable Plug & Work-capability in production-related software components integrated, based on the skills [JP13] of the production components, and across the different levels of automation. The project relies on standards which are already used in industry today, e.g. OPC UA and AutomationML [RH14].

In principle, two questions must be answered: 'What is communicated?' and 'How are the contents transmitted?' The first question concerns the transmitted contents including a domain model. Each component, machine or even IT system involved in the automation system must provide its own description containing aspects such as an object description with attributes and interfaces, the component's production skills, geometry, kinematics, logic and behavior, and relations to other components. A possible standard for this task is AutomationML, an upcoming open standard series (IEC 62714) as described in [SD09]. Furthermore, the component, machine, or IT system must be able to communicate this information to other partners (components, machine, or IT systems) of the production system. OPC UA is one possible platform-independent standard series (IEC 62541) to solve this problem because it can be used on each level of the automation hierarchy (from the field sensor up to ERP systems). OPC UA can even be used in combination with IT tools of the production planning phase as described in [SS11]. To this end, an architecture based on both standards – AutomationML and OPC UA – was defined.

Every component, machine, or IT system is equipped with an OPC UA interface, either with an own OPC UA server or via a converter or gateway with a representation in an aggregated OPC UA server. If a standard OPC UA server, e.g. for a controller, is chosen and it does not provide the possibility to secure its communication, a gateway as aggregated OPC UA server can integrate this server. Legacy OPC servers can be wrapped and integrated via the gateway into the aggregated OPC UA server. If the component, machine, or IT system does not provide feasible communication components and interfaces for the extension with OPC UA, it is expanded by an additional secure automation device which includes the OPC UA server. Every component, machine, or IT system has its own model based on AutomationML. This AutomationML model is included in the OCP UA server address space (see [RH14]), based on a common AutomationML information model. In addition, the services (provided by the component, machine, or IT system) are realized by means of standard OPC UA services (e.g. a valued read) or individual methods provided for the objects of the OPC UA server address space.

The descriptions of each component, machine, or IT system are then fusioned into the AutomationML model for the production situation in focus. This integration or fusion task (see also [MG12]) is realized by the change management which is implemented as aggregating OPC UA server including an integrated OPC UA client. The change management also undertakes the task of a global discovery server where all other OPC UA server must 'register' with their possibilities in terms of profiles. Moreover, this OPC UA server contains methods for version and rights management as well as the possibility for providing notifications on model changes, and features for secure communication. The security server manages amongst others all necessary security keys and ensures that they are available on the components, machines, or IT systems if necessary.

In: Jasperneite, Jürgen; Jumar, Ulrich (Hrsg.): Jahreskolloquium Kommunikation in der Automation (KommA 2014). Lemgo, Nov 2014, ISBN 978-3-9814062-4-5

4 A Prototype Secure Plug & Work I/O field device as a Case Study

Figure 2 shows the core system components of a proposed Secure Plug & Work I/O field device that is implemented as a proof of concept. Furthermore, figure 3 describes the hardware components involved in the developed prototype. The device consists of a security dongle (CodeMeter [WB14]) which holds the keys and certificates used for the OPC UA communication process. It acts as a key for a device to become part of the plant. The BeagleBone Black [BBB] is used to run an OPC UA server, which provides the configuration data needed at the beginning of operation of the device. In addition, it provides live and recorded sensor data and represents the DPM, which is permanent and can be used by the manufacturer of the component during the lifecycle process. The OPC UA-based interface to the DPM allows the flexibility to connect devices with any vendor neutral diagnostic system.

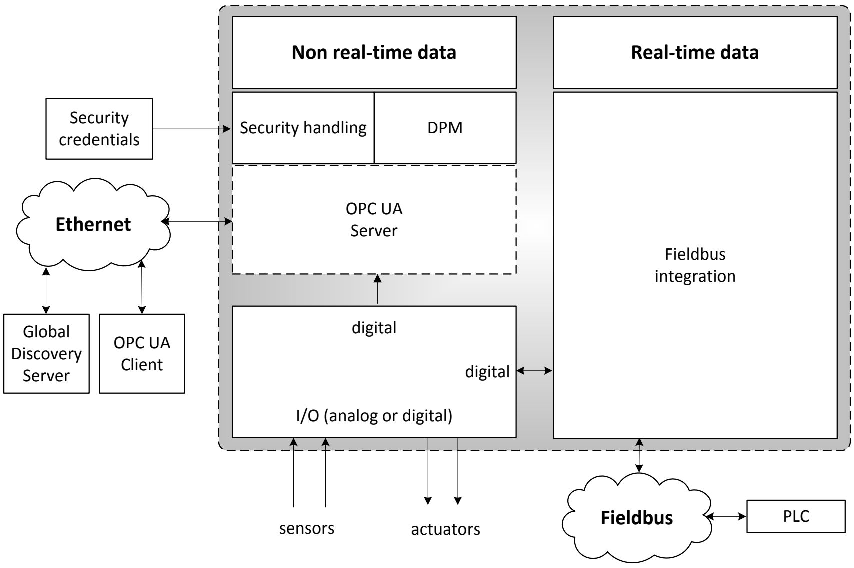


Fig 2: System Components

This new developed, intelligent I/O device is used to be able to flexibly plug components in and out of a system, for example the Lemgo Smart Factory (LMF). The LMF consists of six separate modules, which transport bulk goods (corn) and produce packaging material (popcorn). At one of these modules, namely the production module, the corn is heated and the hereby formed popcorn is then filled. In this case study, this production module is equipped with the Secure Plug & Work I/O device. Because the plant can be run with or without the production module, in this way the functionality can be optimally demonstrated. To integrate this Secure Plug & Work I/O device at the production module, all the sensors and actors are connected to the BeagleBone Black instead of the traditional bus terminal. On the BeagleBone Black, the data is processed and passed to the digital product memory. Furthermore, the sensor data has to be deterministically exchanged with the controller as well. Therefore, a real-time communication channel is needed; for the case study this is done by the TPS-1 [RH12], which provides PROFINET-based real-time communication. Besides that, the TPS-1 can also be used as a virtual Ethernet interface on the BeagleBone Black, to provide network access to the digital product memory. For this purpose, the network traffic is transferred between the two via SPI.

Furthermore, the system consists of a Secure Plug & Work I/O field device and infrastructure services, which are essential to orchestrate the dynamic configuration and seamless integration. Core system components can be split between hardware and software components. The Following subsection provides more detailed information about those components.

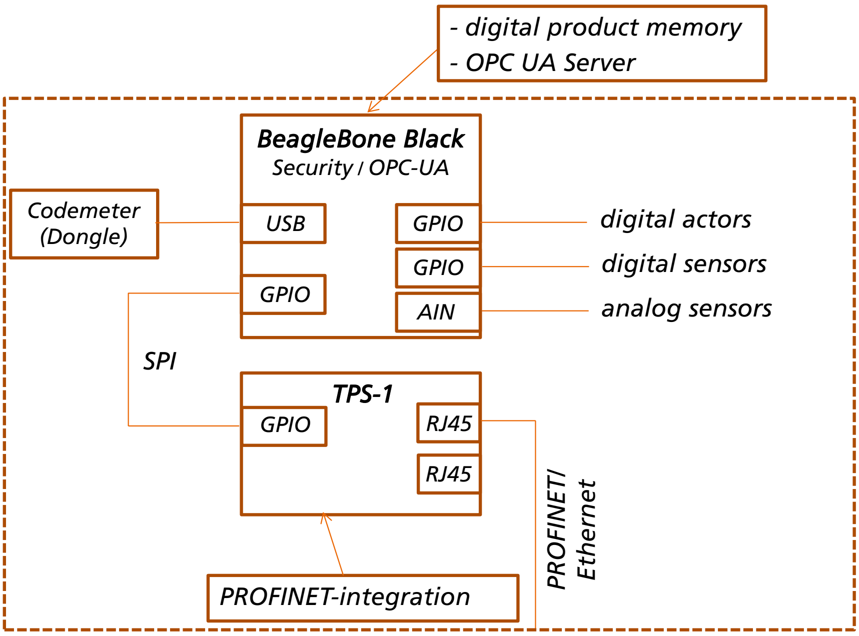


Fig 3: Secure Plug & Work I/O field device

4.1 Codemeter Dongle / Security

The implicit need for a security system within the Plug & Work environment is described in chapter 2.1. The OPC UA standard allows the use of different SSL implementations based on the security architecture used in web services. All this implementations do not cover two important factors which often makes the use of encryption complicated: the secure rollout and distribution of keys and certificates as well as the secure storage of those.

Latter is solved by the CodeMeter dongle with its integrated smart card chip. It is able to store the keys and certificates in a secure memory. All cryptographic operations are done inside this chip, so the secret key does never leave the secure memory. The technology is placed beside the SSL implementation which is specified today. So the OPC UA standard is kept but reinforced by the use of a state of the art cryptographic implementation. The needed CodeMeter hardware can either be an USB, (µ)SD or ASIC form factor (see figure 4).

The second challenge of certificate and key distribution can be covered by the use of the License Central (LC). By using master keys in the dongles, the software is able to establish a secure communication channel between a central certificate authority (CA) and the secured components in the machine or plant. As an initial process, a new component sends a request to the LC and gets back the signed certificate. OPC UA will be the communication channel. The needed data is transported as encrypted bulk data in the OPC UA protocol. This ensures compatibility in heterogeneous environments. If the OPC UA protocol is working, the license transfer works, too. The License Central database (see figure 5) gives an overview of all CodeMeter secured knots within the plant.

CodeMeter and License Central are established products in the market. In this project the adaption to OPC UA client and server and the use of OPC UA as transport medium are realized.

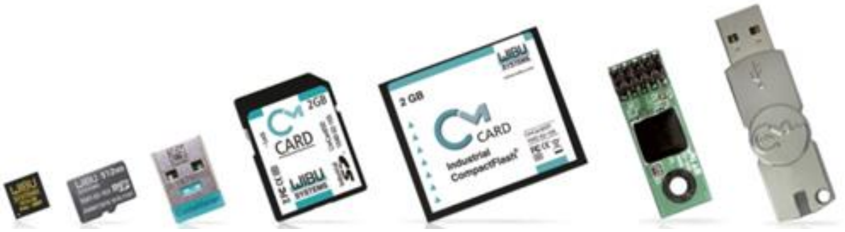


Fig 4: Form factors of the CodeMeter Dongle

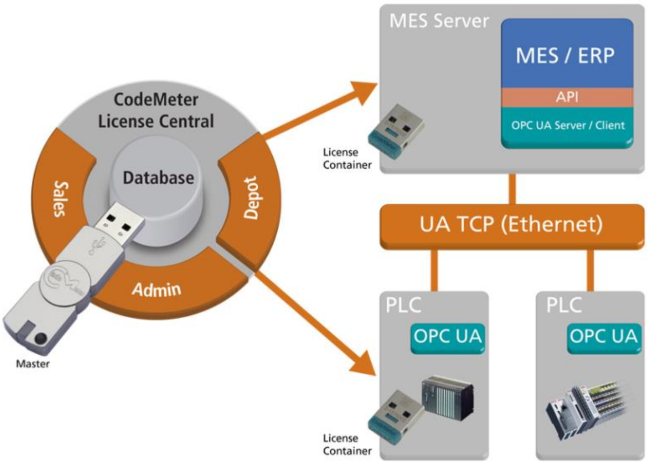
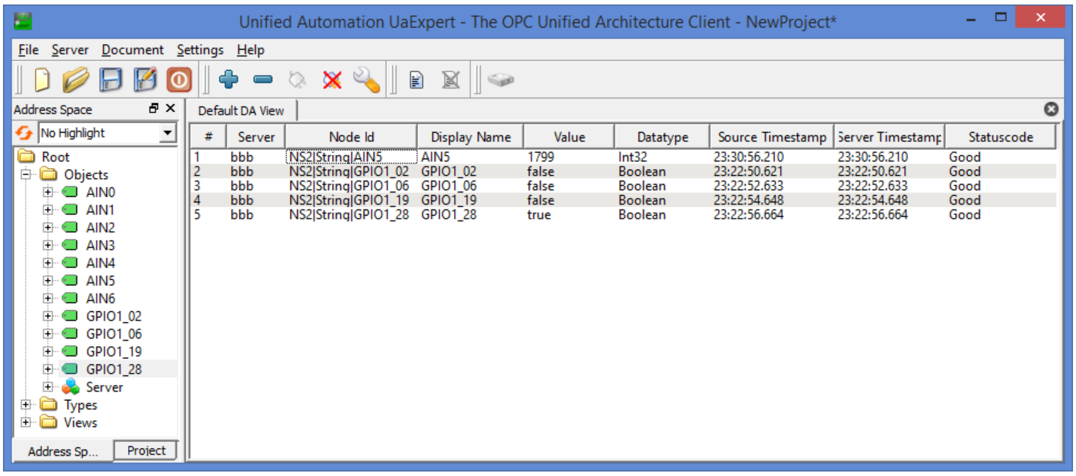


Fig 5: CodeMeter and License Central in an industrial environment

4.2 Beaglebone as development platform for Secure Plug & Work I/O field device

The BeagleBone Black is a small sized, flexible single-board computer running a 1 GHz ARM CPU. Many of the CPU's GPIO pins are directly accessible on the board's headers, which enables the possibility to use up to 65 digital I/Os. Furthermore, there are 7 analog inputs available, using the internal 12 bit analog digital converter. By using the headers on the board, it is possible to expand the BeagleBone Black with additional functionalities on further boards, the so called capes. Since the BeagleBone Black is based on the ARM architecture, it can run Linux as an operating system, which leads to some great opportunities. The community of the BeagleBone provides patches for the kernel to enable real-time scheduling, which makes it usable in time-critical industrial applications. With the 1 GHz CPU and 512 MB of RAM, the system has sufficient resources to run a complete Standard UA Server Profile. In this project the Unified Automation Server SDK is used to create and OPC UA-Server as shown in figure 6. Because the system runs on a SD card (in this case 8 GB), plenty of data can be stored in the digital product memory. The PROFINET integration is done via the single chip solution TPS-1 (ARM9@100MHz) [RH12]. It provides two Ethernet interfaces and all PROFINET related protocol handling is implemented in the hardware. Its corresponding software is based on the real-time OS "embOS". To be able to connect the TPS-1 to the BeagleBone Black, we designed a custom cape consisting of two printed circuit boards. This cape also provides the functionality to convert the voltages, since the GPIO pins of the BeagleBone Black only support 3.3V, whereas most industrial scale sensors and actors require 24V. This custom cape is described in detail in the next section. For the communication with the TPS-1, a loadable kernel module on the basis of the TPS-1-API delivered by KW-Software is used. Thus, within this application the inputs and outputs of the BeagleBone Black can be written according to the PROFINET data.



<table>
<tr><th>#</th><th>Server</th><th>Node Id</th><th>Display Name</th><th>Value</th><th>Datatype</th><th>Source Timestamp</th><th>Server Timestamp</th><th>Statuscode</th></tr>
<tr><td>1</td><td>bbb</td><td>NS2|String|AIN5</td><td>AIN5</td><td>1799</td><td>Int32</td><td>23:30:56.210</td><td>23:30:56.210</td><td>Good</td></tr>
<tr><td>2</td><td>bbb</td><td>NS2|String|GPIO1_02</td><td>GPIO1_02</td><td>false</td><td>Boolean</td><td>23:22:50.621</td><td>23:22:50.621</td><td>Good</td></tr>
<tr><td>3</td><td>bbb</td><td>NS2|String|GPIO1_06</td><td>GPIO1_06</td><td>false</td><td>Boolean</td><td>23:22:52.633</td><td>23:22:52.633</td><td>Good</td></tr>
<tr><td>4</td><td>bbb</td><td>NS2|String|GPIO1_19</td><td>GPIO1_19</td><td>false</td><td>Boolean</td><td>23:22:54.648</td><td>23:22:54.648</td><td>Good</td></tr>
<tr><td>5</td><td>bbb</td><td>NS2|String|GPIO1_28</td><td>GPIO1_28</td><td>true</td><td>Boolean</td><td>23:22:56.664</td><td>23:22:56.664</td><td>Good</td></tr>
</table>

Fig 6: Address space of the BeagleBone’s UA Server in UaExpert

4.3 Enhanced Custom Cape for BeagleBone Black

Instead of using commercial off-the-shelf IO capes, which cumulated are able to supply the necessary performance and functionality needed, two unique capes have been created for this project (see figure 7a). One of the main design criteria has been the restriction of not surpassing the dimensions of the base plate of the BeagleBone Black (86x54mm) to ease implementation in the industrial environment. The provided function cluster contains respectively eight digital input and output channels, four high impedance analog measurement channels (up to 30VDC), an SPI and I2C connection, as well as a PROFINET expansion. The outputs are able to supply an output power of 30W at a level of 24VDC and are extensively secured for instance by galvanic separation. The digital inputs which are also securely designed, support CMOS, TTL, LV logic levels and can additionally be configured to support even the industry standard level of the 24VDC logic. Furthermore, an input supply range between 12 and 36VDC is supplied. EMV considerations at the design process are leading to a crosstalk factor of maximum 0.4% at switching frequencies of maximal 5 kHz.

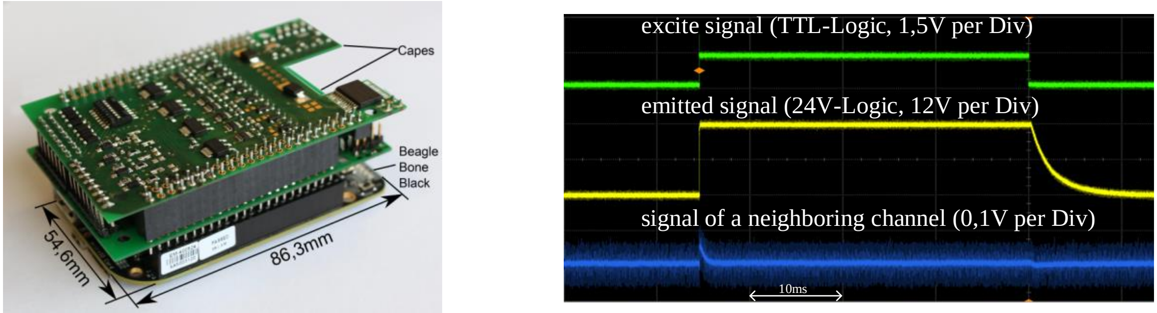

Capes
Beagle
Bone
Black
54,6mm
86,3mm
excite signal (TTL-Logic, 1,5V per Div)
emitted signal (24V-Logic, 12V per Div)
signal of a neighboring channel (0,1V per Div)
10ms

Fig 7: (a) BeagleBone Black with Enhanced Custom Capes, (b) Performance of the Digital Output Channels

As an example, figure 7b shows a performance of digital output channels (10ms per division) without further loads. The excite signal results in a certain emitted signal. Neighboring channels are affected by crosstalk on switching actions. To give an impression of the overall performance of the system, the slowest component shall be presented. The digital output channels shall be able to switch 24V as an impulse response of an excite signal. With no load on the channel, the capacitive discharge induces relatively high fall times of approximately 4.4ms. The alteration to a load of 12mA leads to a reduced fall time of approximately 0.05ms. Other characteristics of the impulse response vary in faster timing dimensions. Related to this, the rise time of 0.004ms varies minimal with the application of a load. The latency of rising and falling depends strongly on the flank and varies proportional from 2ms (no load) to 0.3ms with a 12mA load.

5 Conclusion

This work shows that a hybrid approach using a real-time channel for the control loop and an OPC UA-based best effort channel is possible. The OPC UA channel can be used for a seamless communication from a sensor to the Internet in order to configure and exchange security related digital certificates and to provide a vendor neutral interface for a digital product memory as well as a live view at the sensor data without interfering the real-time part of the system.

Furthermore, this work has presented a concept of semantic product memories that goes beyond traditional digital product memories, since it provides a machine-understandable meaning and description of its contents based on OPC UA. If a product memory has no explicit semantic markup, only propriety software can exploit the information stored in the memory. In contrast, semantic product memories can be interpreted by any software that has access to the semantic description of the epistemological primitives (OPC UA in this case) and the ontologies used for capturing memory contents. Since data security is a topic of major concern in the industrial data communication networks, in this work, a secure data communication architecture is proposed that tries to leverage the integration of distributed and active components to existing centralized structures in the field of industry and manufacturing.

Shortcomings of the proposed approach are that it needs pre-configured infrastructure components such as a security credentials management portal and an embedded system with more processing power/memory resources. It requires a range of features that existing embedded platforms for industrial components not fully support. Therefore, a custom solution is needed that could provide a functionality of real-time communication beside secure exchange of semantics and allows to perform complex calculation related to semantic data modelling and security verification/validation.

A BeagleBone Black based-evaluation system allowed us to implement all important features efficiently. Being an open source embedded system, an adequate support from community is available. Also, it is readily extensible and real-time features are added on the same platform by means of a custom cape. A proof of concept implementation of the secure communication architecture demonstrated the viability of the concept with promising results. In the next step, performance aspects of the architecture should be evaluated in more detail together with an integration of the implemented Secure Plug & Work I/O field device into a smart factory.

One of the challenges of the Industry 4.0-IT-architecture is the ability to adapt to changes - whether that new systems or production processes are introduced into the system or existing production systems are changed. An OPC UA-based architecture would be an enabler for a flexible, scalable, secure and standards-based integration of distributed automation system components.

6 Acknowledgment

This research and development project is funded by the German Federal Ministry of Education and Research (BMBF) within the "Framework Concept 'Research for Tomorrow's Production'" (funding number 02PJ2590 ff) and managed by the Project Management Agency Karlsruhe (PTKA). The author is responsible for the contents of this publication.

7 References

[SF12] Stefan Ferber. "Industry 4.0 – Germany takes first steps toward the next industrial revolution." http://blog.bosch-si.com/, Oct 2012.

[SH12] S. Hodek and J. Schlick. Ad hoc field device integration using device profiles, concepts for automated configuration and web service technologies: Plug and Play field device integration concepts for industrial production processes. In Systems, Signals and Devices (SSD), 2012 9th International Multi-Conference on, pages 1 –6, march 2012.

[BB11] Brandherm, B.; Kroner, A., "Digital Product Memories and Product Life Cycle," Intelligent Environments (IE), 2011 7th International Conference on , vol., no., pp.374,377, 25-28 July 2011

[SC10] Seitz, C.; Legat, C.; Ziyuan Liu, "Flexible manufacturing control with autonomous product memories," Emerging Technologies and Factory Automation (ETFA), 2010 IEEE Conference on , vol., no., pp.1,8, 13-16 Sept.

[JI13] Imtiaz, J.; Jasperneite, J., "Scalability of OPC-UA down to the chip level enables "Internet of Things"," Industrial Informatics (INDIN), 2013 11th IEEE International Conference on , vol., no., pp.500,505, 29-31 July 2013

[KA10] Kroner, A.; Meixner, G.; Jacobs, O., "Digital Product Memories: Perspective of Users and System Architects," Intelligent Environments (IE), 2010 Sixth International Conference on , vol., no., pp.265,270, 19-21 July 2010

[WB14] WIBU, "CodeMeter encrypts and signs the software and data on embedded systems. The keys are stored on an external device "CmDongle". This dongle can be a SD card or an USB device. " www.wibu.com

[RH12] Roland Hess, Andreas Steinmetz, Sebastian Schriegel, and Markus Schumacher. "Profinet und Power-over-Ethernet: Simple networking of distributed sensors." In Industrial Ethernet Journal III/2012, pages 902–904, August 2012.

[JP13] Julius Pfrommer, Miriam Schleipen, Jürgen Beyerer: PPRS: Production skills and their relation to product, process, and resource. In: Proceedings of the 2013 IEEE 18th Conference on Emerging Technologies & Factory Automation (ETFA), September 2013.

[RH14] Robert Henssen, Miriam Schleipen: Interoperability between OPC-UA and AutomationML.Disruptive Innovation in Manufacturing Engineering towards the 4th Industrial Revolution, Proceedings of the 8th International CIRP Conference on Digital Enterprise Technology - DET 2014 mit CD-ROM, Hrsg.: Wilhelm Bauer, Carmen Constantinescu, Olaf Sauer, Paul Maropoulos, Jody Muelaner; Fraunhofer IAO, Stuttgart;

2014, Sprache: Englisch, Fraunhofer Verlag, ISBN 978-3-8396-0697-1, 2014.

[BB11] Brandherm, B.; Kroner, A, "Digital Product Memories and Product Life Cycle," Intelligent Environments (IE), 2011 7th International Conference on , vol., no., pp.374,377, 25-28 July 2011.

[MU14] Mönks, Uwe; Trsek, Henning; Dürkop, Lars; Geneiß, Volker; Lohweg, Volker: Assisting the Design of Sensor and Information Fusion Systems. In: 2nd International Conference on System-integrated Intelligence Bremen, Jul 2014.

[CW10] Colombo A W, Karnouskos S, Mendes J M. Factory of the Future: A Service-oriented System of Modular, Dynamic Reconfigurable and Collaborative Systems. In: Artificial Intelligence Techniques for Networked Manuf Enterprises Management, pp. 459–481. Springer, 2010.

[HM12] Houyou A M, Huth H P, Kloukinas C, Trsek H, Rotondi D. Agile Manufacturing: General Challenges and an IoT@Work Perspective. In: 17th IEEE Int Conference on Emerging Technologies and Factory Automation (ETFA 2012); Kraków, Poland, 2012.

[PNP14] AutoPNP consortium. AutoPNP – Plug and Play for Automation Systems 2014 [cited 2014 Feb 20] Available from: http://www.autopnp.com/.

[OJ13] Otto J, Böttcher B, Niggemann O. Plug-and-Produce: Semantic Module Profile. In: Dagstuhl-Workshop MBEES: Modellbasierte Entwicklung eingebetteter Systeme IV; 2013.

[MD09] Damm M, Leitner S, Mahnke W. OPC Unified Architecture. Springer-Verlag Berlin Heidelberg, 2009.

[LD12] Dürkop L, Trsek H, Jasperneite J, Wisniewski L. Towards Autoconfiguration of Industrial Automation Systems: A Case Study Using PROFINET IO. In: 17th IEEE Int Conference on Emerging Technologies and Factory Automation (ETFA 2012); Kraków, Poland, 2012.

[GR08] Reinhart G, Krug S, Huttner S, Mari Z, Riedelbauch F, Schlogel M. Automatic configuration (plug & produce) of industrial ethernet networks. In 9th IEEE/IAS International Conference on Industry Applications (INDUSCON), pages 1 – 6, 2008.

[LD13] Dürkop L, Imtiaz J, Trsek H, Wisniewski L, Jasperneite J. Using OPC-UA for the Autoconfiguration of Real-time Ethernet Systems. In: 11th International IEEE Conference on Industrial Informatics (INDIN 2013); Bochum, Germany, 2013.

[RH12] Roland Hess, Andreas Steinmetz, Sebastian Schriegel, and Markus Schumacher. Profinet und Power-over-Ethernet: Einfache Vernetzung dezentraler Sensorik. In Industrial Ethernet Journal III/2012, pages 902–904, August 2012.

[BBB] http://beagleboard.org/black

[SC10] Seitz, C.; Legat, C.; Neidig, J., "Embedding Semantic Product Memories in the web of things," Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on , vol., no., pp.708,713, March 29 2010-April 2 2010

[YZ07] Yanhe Zhang; Ying Yang; Tian Lei, "Product Semantics Evaluation Based on User Memory," Natural Computation, 2007. ICNC 2007. Third International Conference on , vol.4, no., pp.558,562, 24-27 Aug. 2007

[SP10] Stephan, P.; Meixner, G.; Koessling, H.; Floerchinger, F.; Ollinger, L., "Product-mediated communication through digital object memories in heterogeneous value chains," Pervasive Computing and Communications (PerCom), 2010 IEEE International Conference on , vol., no., pp.199,207, March 29 2010-April 2 2010

[FK12] Fischer, K.; Gessner, J.; Fries, S., "Secure Identifiers and Initial Credential Bootstrapping for IoT@Work," Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on , vol., no., pp.781,786, 4-6 July 2012

[SD09] Miriam Schleipen, Rainer Drath: Three-View-Concept for modeling process or manufacturing plants with AutomationML. 13th IEEE International Conference on Emerging Technologies and Factory Automation. 22.-25.9.2009, Palma de Mallorca.

[MG12] Miriam Schleipen, Dirk Gutting, Franziska Sauerwein: Domain dependant matching of MES knowledge and domain independent mapping of AutomationML models. IEEE conference on Emerging Technologies and Factory Automation ETFA 2012, September 17-21, Krakow, Poland, 2012.

[SS11] Miriam Schleipen, Manfred Schenk:Intelligent environment for mechatronic, cross-discipline plant engineering. IEEE conference on Emerging Technologies and Factory Automation ETFA 2011, September 5-9, 2011, Toulouse, France, 2011.

[IN14] it’s OWL, Cross-sectional project: Intelligent networking (Plug-and-play). http://www.its-owl.com/