54. IWK

Internationales Wissenschaftliches Kolloquium
International Scientific Colloquium

Information Technology and Electrical Engineering - Devices and Systems, Materials and Technologies for the Future

Faculty of Electrical Engineering and Information Technology

Startseite / Index:
http://www.db-thueringen.de/servlets/DocumentServlet?id=14089

TECHNISCHE UNIVERSITÄT
ILMENAU

Impressum

Herausgeber: Der Rektor der Technischen Universität Ilmenau
Univ.-Prof. Dr. rer. nat. habil. Dr. h. c. Prof. h. c.
Peter Scharff

Redaktion: Referat Marketing
Andrea Schneider

Fakultät für Elektrotechnik und Informationstechnik
Univ.-Prof. Dr.-Ing. Frank Berger

Redaktionsschluss: 17. August 2009

Technische Realisierung (USB-Flash-Ausgabe):
Institut für Medientechnik an der TU Ilmenau
Dipl.-Ing. Christian Weigel
Dipl.-Ing. Helge Drumm

Technische Realisierung (Online-Ausgabe):
Universitätsbibliothek Ilmenau
ilmedia
Postfach 10 05 65
98684 Ilmenau

Verlag:
Verlag ISLE, Betriebsstätte des ISLE e.V.
Werner-von-Siemens-Str. 16
98693 Ilmenau

ISBN (USB-Flash-Ausgabe): 978-3-938843-45-1
ISBN (Druckausgabe der Kurzfassungen): 978-3-938843-44-4

Startseite / Index:
http://www.db-thueringen.de/servlets/DocumentServlet?id=14089

ABSTRACTION OF WIRELESS COMMUNICATION BY A CONVERGENCE MIDDLEWARE IN CONJUNCTION WITH A XML-CONFIGURATION

Peter Buschkuehle

Volker Schuermann

Joerg F. Wollert

Department of Electrical Engineering and Computer Science, Bochum University of Applied Sciences
Bochum, 44801, Germany

ABSTRACT

Today the meaning of wireless technologies constantly increases. That is not only of interest in the consumer area, but also for office solutions or the control and regulation of machines within the automation technology. In the different fields of applications the requirements varying against the radio technologies. In the past it turns out that there is not the one wireless technology that fulfills all requirements in every situation. For this reason different radio technologies in the automation technology were established. Here for example WLAN, Bluetooth and IEEE 802.15.4 are to mention. Therefore the individual wireless technologies offer strong differences. For example the parameterization of the specific communication solutions, or the topologies, in which the wireless networks are organized, are mentioned. It is obvious, that a uniform interface must be created to abstract the wireless technologies, that a commercial long run success is guaranteed.

Index Terms - XML, ZigBee, Bluetooth, nanoNet, WLan, middleware, convergence, configuration

1. INTRODUCTION

In automation cable-bound systems dominate sensor and actor networks. But wired networks represent a weak point, because the industrial environment can be raw. The wires have a high wear, because they are pretty often subject to physical or chemical demands. In addition cable-bound system can be very expensive. Because of these cases radio technologies become more and more accepted in automation. They use the air as transmitting medium, which logical does not have any wear. Also the individual radio modules can be built in such a way that they can withstand the demands. A further point is that there is no special radio technology for the automation industry. Therefore increasingly radio technologies from other areas like e.g. the consumer market are used and/or modified for automation. To mention here are technologies like e.g. Bluetooth [1], IEEE 802.15.4/ZigBee [2] or WLAN (Wireless Local Area Network) [3]. Technologies like these using the royalty-free 2,4 GHz ISM band. Because of this they have the advantage that thereby no further costs would arise. Furthermore these technologies are applicable worldwide.

Meanwhile there are many standards, which are usually more or less well suitable for different tasks [4]. The application scenarios of wireless technologies are often found in mobile environments. That results in participants moving out of range of the hotspots of high dynamic networks. In addition the start-up and maintenance of networks are often a not trivial task, which is still made more difficult by vanishing or joining participants. It suggests itself that this procedure is to automate and to arrange for the user transparency as far as possible.

Cable-bound automation systems likewise have multiplicity at communication technologies, which differs more or less strongly.

All these Problems should be solved in the DANA-Project (Dynamic Ad-hoc networks in automation) [5] at the Bochum University of Applied Sciences. This article presents a solution. In chapter 2 the state of the art is figured out. Chapter 3 will present a convergence middleware and chapter 4 describes a configuration tool. These two chapters represent the solution of the problems addressed above. Chapter 5 will examine the solution critically. The last chapter gives a conclusion.

2. STATE OF THE ART

This chapter has its focus on automation. More precisely the state of the art of radio technologies in automation and device description languages will be described.

2.1. **Device description languages**

Device description languages exist since automation devices are available. They serve among other things the description of network and communication characteristics, containing information of the equipment assembly, for the diagnosis and some more. Software tools use device descriptions for the automatic production of the configuration, as well as the adjustment of specific characteristics of the field devices. However there are no solutions, which describe complete networks. From the historical development different languages for different use cases [6] resulted. Apart from text-based description languages such as EDDL [7], also several XML dialects are developed [8]. In the ISO 15745 [9] some device description languages are described and standardized. The ISO 15745 has the title „Industrial automation systems and integration - Open systems application integration framework“ and consists of the following parts:

- Part 1: Generic reference description
- Part 2: Reference description for ISO 11898-based control systems
- Part 3: Reference description for IEC 61158-based control systems
- Part 4: Reference description for Ethernet-based control systems

The fundamental mechanisms of a device description language obtain part 1, while in the other parts; the fieldbus specific device description languages are described. In this article a special focus lies on XML based device description languages. For this reason the article only goes on detail on ISO 14745-3.

FDCML (Field Device Configuration Markup Language) offers the possibility to describe the device in its details. A device is not completely out-modeled, but only the structures for representation of certain types of devices are defined, because XML generally defines only the structure of a document. It is an advantage that the devices without knowledge of automation and communication system can be described. Rather information about identification, communication, functionality, diagnostic information and mechanical details should be given. Beside the multilingualness fulfills FDCML the following requirements completely:

- Network independence
- Expandability is given

Further a description of groups of devices or individual components within devices are possible because FDCML offers a structure, to let appear a group of devices as unit.

2.2. **Wireless in automation**

Radio technologies are often used in office environments or private domains. For this reason the automation industry wants to use wireless communication and participate from the advantages. Meanwhile there are numerous of different radio technologies, which transmit usually in the same ISM band, but they differ hardly in their technology and its level of maturity. The two technologies, which are probably most developed are Bluetooth and WLan (Wireless Local area network). But the requirements in automation are so different that more and more radio technologies come to existence. To mention at this point are among others IEEE 802.15.4/ZigBee, nanoNet and RFID.

The general requirements at radio technologies in the automatic control engineering are now represented briefly [10]:

- The Quality of connection can vary strongly by different influences. So monitoring mechanisms are essential.
- If it should come to connection interruptions and one or more devices are not connected any longer, a mechanism is necessary that the connection repairs.
- Security mechanisms like authentication or encryption are extremely important, because radio is an open medium.

All these technologies have different function modes, which bring pro and cons with itself and cope with different application scenarios. Often Consumer technologies are special modified. To mention here for example are IWLAN (Industrial Wireless Local Area Network) of the company Siemens und WISA (Wireless Interface for Sensors and Actors) of the company ABB.

WLAN is often used for a radio-based extension of the existing cable-bound networks, because it has the highest affinity for such networks of all the radio technologies. In addition also a high range and high data rates are characteristics of WLAN.

Bluetooth should bridge short ranges and is used among other things to parameterize or configure machines by the use of mobiles. Notice, that the transmission rates are moderate and only a small number of participants can be realized.

ZigBee is a relative new technology, which has very small energy consumption. The data rate is rather small. ZigBee is suitable for networking on sensor level; because the data volume is small in this case. At the same time these sensors are not cable-bound, since they can be operated due to their small energy consumption with a battery. A promising application type is offered e.g. within building automation.

The nanoNET technology has for the most part the same application type like ZigBee, but has a

completely different transmission method and should be more fail-safe for this reason.

The development of wire-bound communication systems has led to nearby similarly heterogeneous mixture of fieldbus standards. For manufacturers of industrial radio solutions this means a directly additional expenditure, because no uniform integration interfaces for wireless communication systems are defined for fieldbus systems. The results are isolated solutions and proprietary beginnings, which in both sides are laid out radio and/or product specific. For operators of industrial machines an uniform representation of wireless systems is missing. The re-use of assigned concepts for the integration of new radio technologies is hardly possible.

The Bochum University of Applied Sciences deals with this problem within the research project DANA (Dynamic Ad-hoc networks in automation). The goal of the project was the structure of a Framework for the uniform integration of radio technologies into automation systems. Principal item of DANA is the convergence middleware presented in this contribution. Contrary to other middleware solutions, like described in e.g. [11] [12] [13] [14], the focus is not on the support of self organization of wireless networks and their high dynamics regarding of the number of participants and routing properties. Rather more the supported services correspond to the typical views on industrial communication systems with regards to wireless communications. Particularly, these include the configuration and commissioning, the maintenance and a reliable and deterministic operation with diagnosis and error detection. So the middleware presented here corresponds as far as possible to the application driven approaches like in [11].

3. CONVERGENCE MIDDLEWARE

The antecedent chapter shows, that radio technologies differ very much. For this reason a convergence middleware has to be created.

3.1. **Requirements of the Middleware**

Before the structure of a convergence middleware for the integration of wireless networks is build up the existing basic conditions has to be identified. These result from the requirements of industrial communications, the characteristics of wireless technologies and the communication channels [4] the data are transported over.

3.1.1. General requirements

- In automation strict defaults exists for the observance of latency, answer and cycle times. The operating time and the Overhead of the convergence middleware may make only a negligible contribution for the increase of these times.
- The communication may load the CPU of the superordinate control only lowly, because its major task is the treatment of the control program.
- A general trend is to offer services and remote procedure calls over web services, how you can see in the OPC specification [15]. These are based on extensive XML messages, which are transferred over SOAP between the different systems. Against this trend the protocol should be very slim, because the exchanged data are only a few bytes per cycle.
- Services for synchronous data exchange of real time systems and asynchronous data exchange for configuration, parameterization, diagnostics and status information are the basic structure of an industrial communication system.

3.1.2. Requirement regarding wireless technologies

- Apart from general services to configure and parameterize wireless networks, extended properties for the installation and start-up are necessary, because of the variable topologies.
- The connection quality can vary strongly due to various factors like multi-path propagation fading interference and inter symbol interference. For this reason services represent a substantial requirement characteristic for the monitoring of the transmission quality to the convergence middleware.
- If it comes to a break of the connection several participants can be concerned. Self Healing mechanisms and finding new routes, as far as these are present, can last after present state of the art up to several seconds. In this case parameter-driven functions for the treatment of these exceptional conditions can limit the risk on sides of the radio nodes only previously.
- Radio channels are very easily accessible and physically speaking hardly tap-proof. Therefore suitable authentication and security procedures are needed, in order to cope with security policies for the data security of companies.

3.2. **General middleware architecture**

Derived from the requirements specified above the middleware was developed like in Figure 1 illustrated.

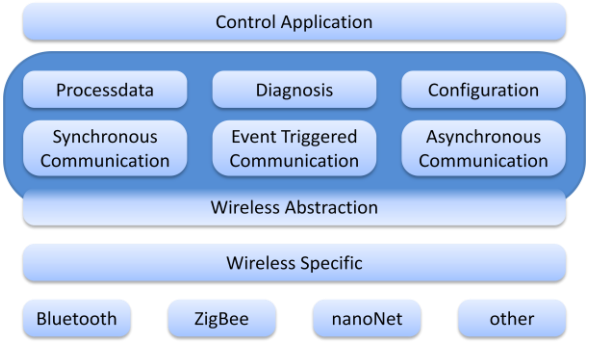

Figure 1: architecture of the convergence middleware in principle

3.2.1. Communication model

The data exchange between the WSAN and the superimposed control system happens via synchronous process images of the inputs and outputs. Depending on the control system or the integration of the wireless network interface only a limited amount of data can be exchanged per cycle. For this reason the middleware supports the segmented exchange of the process data over several cycles. It is important to note that each segmentation involving a direct increase of the latency of the system.

Synchronous data communication serves for the change of the real time data. It is essential to exchange the data as efficiently as possible among the wireless node and the control system. The wireless network itself constitutes a separate subbussystem through, which an independent sub-process image is held. Each data exchange with the control system is served immediately from this sub-process image. The exchange of configuration and diagnostic data is done asynchronously through reserved areas of the process image.

Both for reasons of energy consumption as well as the deliberate use of the frequency band are differentiated within the wireless network between the cyclic communication for critical data and event-driven communications e.g. sensor data battery radio nodes. Furthermore event-controlled alarms and diagnostic functions can be registered.

3.2.2. Abstraction layer

The abstraction layer contains similarly as [14] two sub layers. The lower layer illustrates the radio-specific characteristics on a uniform interface, the upper layer implements functions which is not supported by the protocol stack like packet repetition. For example, the service for configuration of the interval time can be mapped by the abstraction layer to the Sniff Interval [16] of Bluetooth Slaves or the Beacon Interval [17] of IEEE 802.15.4 networks. Dealing with all service mappings the scope of this document would exceed.

It should be noted that the possible range of values of the parameters and services depends significantly on the functional scope and the technological properties of the wireless technology, which is used concretely. With Bluetooth for example no multi hop networks can be developed and there is only one channel, which hops through the entire frequency band. At this point is referred on [18] for a concise description of the characteristics of appropriated radio technologies for automation.

3.2.3. Device model

For the view on the radio networks the middleware differentiates three types of device:

- Master/Coordinator:
  This device starts and coordinates the wireless network. The coordinator represents usually also the physical interface to the control system. This device manages the process data of the entire wireless network.
- Router:
  This device can have local process data or serve only as Relay node in a network, in order to stretch Multihop networks of higher range. It is important to note, that not every radio technology supports the device type router. The implementation of routing functionality solely by the middleware is not supported.
- Slave/Enddevice:
  This device has a local process data. It is at least connected over a router or a coordinator to the radio network.

For the view on the control system the superordinate control is called master. The radio network is globally described as a slave. The asynchronous communication is initiated by the master in use of request-response procedures. The synchronous communication to exchange the process data is cyclically triggered by the master.

4. THE CONFIGURATION SOFTWARE

The configuration and start-up of wireless networks differs substantially from cable-bound communication systems, therefore a special qualification of the personnel is necessary. To automate the configuration and start-up of wireless networks the radio technology and the existing communication solution of automation has to be abstracted. So it is possible to communicate with the devices over uniform interfaces. Apart from the simplification and/or the automation of start-up, the whole solution should be as flexible as possible in the reference to new technologies and parameterization. Therefore configuration software has to be created, which can abstract several wireless networks at the same time. Likewise it should be possible to manipulate the determined data if necessary. In order to arrange start-up as simple as possible, it has to be possible to provide software modules from the determined data.

These should be loaded after some manipulations directly on the programmable logic controller (PLC).

4.1. **Program sequence in principle**

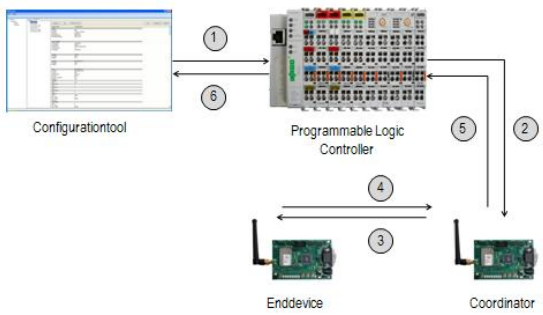

Figure 2: Example of a program sequence

1. A request is sent by the configuration software to the PLC.
2. The request is passed through the PLC to the Coordinator of the wireless network.
3. If the inquiry is not intended for the Coordinator, it is passed on the correct receiver.
4. The receiver sends an appropriate response back.
5. The coordinator passes the response on to the PLC.
6. The configuration software downloads the information of the PLC.

4.2. **Inquiry of the wireless networks**

The device description, which is located on each device of the ZigBee network, must first be loaded into the configuration software. Particularly for this reason a request-response protocol was created, which is called ACP (Asynchronous Communication Protocol). It has different function codes and serves the communication of the ZigBee devices among themselves as well as to the configuration software.
The three different devicetypes Coordinator (C), Router (R) and Enddevice (E) support different function codes, like shown in table 1. The rights of access are reading (R), writing (W) and reading and writing (RW).

Code	Function	Access	Device
0x01	Device Description	RW	C/R/E
0x02	Name	RW	C/R/E
0x03	Max Nodes Per Hops	RW	C/R
0x04	Max Hops	RW	C/R
0x05	Time Out	RW	C/R/E
0x06	Interval Time	RW	C/R/E
0x07	Remote Outputs	RW	R/E
0x08	Security Mode	RW	C/R/E
0x09	Security Key	RW	C/R/E
0x0A	Channel Scan	W	C/R
0x0B	Channel Selection	W	C/R
0x0C	Start Network	W	C/R
0x0D	Parent Device	R	C/R/E
0x0E	Connected Devices	R	C/R/E
0x0F	Bind/Pair	W	C/R
0x10	unBind/Disconnect	W	C/R
0x11	Mode	RW	C/R/E
0x12	Sync	W	C/R/E

Table 1: ACP-Function-Codes

4.3. **Binary XML**

A largest disadvantage of XML is the large memory usage. Other formats, which are not a XML dialect, have not an overhead like XML because of its structure. A fact is that XML documents are text formats, which not only use a lot of memory, but complex string operations are required for their processing, too. The processing and memory usage of large files give no more problems with modern PC systems practically. But if one would save the device description on a field device, it can be a problem. On devices of a sensor and actor network the limits of memory, processing power and transmission band width are reached very fast. The solution of this problem exists in the use of a binary representation of the XML document, which is transparent for the program with application of an appropriate XML Parser.

One of the first Binary XML formats was the WAP Binary XML (WBXML) [11]. It was supported by the W3C and came to the market in 1999. Later further formats followed. For example VTD-XML [12] or Efficient XML Interchange (EXI) [13] should be mentioned at this point. Test results [14][15] show that EXI can be used for very small XML documents (< 100 Kbyte) , but although the created binary documents are more than 100 times smaller than the original XML documents.

The FDCML device descriptions used in this project usually have the size of 25-30 Kbyte. Tests resulted that these files could be compressed on an approximate size of 3 Kbyte. Comparably large FDCML or GSDML files for the description of Interbus and PROFINET components could be compressed to 5-9 Kbyte. Table 2 shows an excerpt of the test results. It shows, that the FDCML files from the project could be compressed on approximately 10% of their original size. So the compressed device descriptions come into regions of less than 3 Kbyte. Compared with typical protocol stack sizes of approximate 30 Kbyte and more at ZigBee Coordinators and Routers, binary XML device

descriptions with a size of 3-10 Kbyte can be classified suitable for many embedded platforms.

File	Original [Byte]	EXI [Byte]	GZIP [Byte]	EXI + GZIP [Byte]
FDCML DANA	27899	3211	3153	2782
FDCML Interbus	25209	8833	4532	7169
FDCML Interbus	28322	8907	4711	7168
GSDML PROFINET	36574	7626	3390	5475

Table 2: Compression of Device Descriptions

5. DISCUSSION

It is to be pointed out that the configuration software could support further radio technologies, as it was already done via Bluetooth and nanoNet ZigBee. So a middleware would be created, which different wireless technologies abstracted. This makes it possible, that devices with different radio technologies can interoperate with each other.

The program could support several device description languages, to expand extremely the subsequent processing in extern software tools. The export in the PLCopen format could be possible, too. PLCopen has targeted, to create producer-independently a XML format, which can exchange all kind of textual and graphical information between all development environments [17].

The software, which was developed in context of this article, offers up where other development and configuration tools stop their function range. So integration would be quite meaningful in such tools. It would facilitate the work of the automation technician and save time and funds resources.

6. CONCLUSION

A large advantage is that the intermediate format, in which the radio networks are abstracted, is a standardized ISO 15745-3 conformal device description language. Other applications, which work with or on this format, are able to read the generated documents without any problem. An extern subsequent processing is possible without any efforts. Also applications, which do not rise directly from the automation technology, as e.g. a browser, which can present XML files, does not represent a problem, because FDCML is a XML dialect. Here you can refer to IO-Check, which offers an export function in a proprietary language [18].

The language represents also a XML dialect, but not a standardized language. Thus the associated disadvantages like interoperability lacking are directly taken over. All configuration tools stop exactly here, if they offer at all an export function.

Exactly at this point the developed software offers up. It uses the device description language for documenting, storing of network configurations. So the network can be easily set up after a break down. Further it is possible to add or remove participants of an older configuration without any problems before the network should be started up. That is in principle a complete new development and represents for the automation technician or PLC programmer a large simplification. He needs to think neither about the structure of the radio network, nor the function of a certain radio technology. He can setting up some few parameters, to which default values are given already. The software represents an one click solution, which takes over all steps of the configuration.

7. REFERENCES

[1] Bluetooth.com, “Bluetooth Specification” http://german.bluetooth.com/Bluetooth/Technology/Building/Specifications/Default.htm

[2] ZigBee Alliance, URL: http://www.zigbee.org/

[3] IEEE Standards Association, “Wireless LAN Specification” http://standards.ieee.org/getieee802/802.11.html

[4] Rappaport, T.S., „Wireless Communications“, 2nd Edition, Prentice Hall New Jersey, USA, 2002

[5] Buda A., Schuermann V., Wollert J.F.: Schlussbericht Dynamic Ad-hoc networks in automation (in german), 2009

[6] A. Braune, M. Wollschlaeger, “Jedem seine Sprache?”(in german), Weka Fachmedien, 2007

[7] IEC 61804, VDE Verlag, 2006

[8] M. Wollschlaeger, H. Kulzer, D. Nuebling, P. Wenzel, „A Common Model for XML Descriptions in Automation“, IFAC World Congress, 2005

[9] ISO 15745, Beuth Verlag, 2007

[10] Prof. Dr.-Ing Jörg F. Wollert, Volker Schürmann, Aurel Buda. *XML-based Middleware Approach for Industrial Wireless Communication Systems.*

[11] I. Chatzigiannnakis, G. Mylonas, S. Nikoletseas, “50 Ways to build your application; A Survey of Mid-

dleware and Systems for Wireless Sensor Networks" at AEOLUS Fall Workshop, September 2007

[12] P. Gil, I. Maza, A. Ollero, P.J. Marron, "Data centric middleware for the integration of wireless sensor networks and mobile robots", at ROBOTICA 2007, April 2007

[13] M. Diaz, D. Garrido, L. Llopis, B Rubio, J.M. Troya, "A Component Framework for Wireless Sensor and Actor Networks", in Emerging Technologies and Factory Automation, 2006. ETFA '06. IEEE Conference on

[14] V. Handziski, J. Polastre, J.H. Hauer, C. Sharp, A. Wolisz, D. Culler, „Flexible Hardware Abstraction for Wireless Sensor Networks", in Wireless Sensor Networks, 2005. Proceeedings of the Second European Workshop on

[15] OCP Specification,
URL: www.ocpfoundation.org

[16] IEEE 802.15.1 Spezifikation, URL: www.ieee802.org/15/pub/TG1.html

[17] IEEE 802.15.4 Spezifikation, URL: www.ieee802.org/15/pub/TG4.html

[18] A. Willig, K. Matheus, A. Wolisz, "Wireless Technology in Industrial Networks", in Proceedings of the IEEE, Vol. 93, No. 6, pp. 1130-1151, June 2005