A Cyber-Physical System Design Approach

Miroslav Sveda
Faculty of Information Technology
Brno University of Technology
Brno, Czech Republic
e-mail: sveda@fit.vutbr.cz

Radimir Vrba
Faculty of Electrical Engineering and Communication
Brno University of Technology
Brno, Czech Republic
e-mail: vrbar@feec.vutbr.cz

***Abstract*— This paper exemplifies principles of cyber-physical systems design using original smart data acquisition systems capable to store and present measured data wirelessly. The presented temperature data logger stands for an example of flexible, mobile and intelligent appliances fitting various industrial or medical applications. Similarly, the discussed sensor network represents a system architecture stemming from wireless smart pressure sensors connected by Bluetooth and from a network concentrator, which is based either on PDA personal digital assistant or on GSM SmartPhone. Two pilot software implementations were developed for IPAQ PDA 5450 and Nokia 3650 SmartPhone. The paper describes a cyber-physical system design approach using novel data acquisition systems, which can serve as components of public or technological process monitoring systems and allow collecting data also from locations difficult to reach, e.g., from sensors located on rotating parts.**

Keywords- Embedded system design, smart sensor, wireless communication, temperature and pressure measurement.

I. INTRODUCTION

The charter for the CPS (Cyber-Physical System) Summit in April 2008 [6] introduced the following: “The integration of physical systems and processes with networked computing has led to the emergence of a new generation of engineered systems: cyber-physical systems. Such systems use computations and communication deeply embedded in and interacting with physical processes to add new capabilities to physical systems. These cyber-physical systems range from miniscule (pacemakers) to large-scale (the national power grid). Because computer-augmented devices are everywhere, they are a huge source of economic leverage. … it is a profound revolution that turns entire industrial sectors into producers of cyber-physical systems. This is not about adding computing and communication equipment to conventional products where both sides maintain separate identities. This is about merging computing and networking with physical systems to create new revolutionary science, technical capabilities and products.” Embedded computers allow designers to add capabilities to physical systems that they could not feasibly add in any other way. By merging computing and communication with physical processes and mediating the way we interact with the physical world, cyber-physical systems bring many benefits: they make systems safer and more efficient; they reduce the cost of building and operating these systems; and they allow individual machines to work together to form complex systems that provide new capabilities.

The kernel of this paper consists of a general part, covered by Section II, of case studies presenting the real-world applications discussed in Sections III and IV, and of conclusions. The general part is devoted to the review of state of the art in frame of CPS design. The first introduced application discusses a new mobile temperature data logger with RFID (Radio Frequency Identification) capabilities. The second application deals with a developed sensor network that embodies the pressure sensing system consisting of wireless smart pressure sensors connected by the Bluetooth, and of a network concentrator, which is based either on PDA personal digital assistant or on GSM SmartPhone.

II. CYBER-PHYSICAL SYSTEMS DESICN

Many of the embedded systems-related studies and efforts in the past have focused on the challenges the physical environment brings to the scientific foundations of networking and information technology, see [2] and [4]. However, the full scope of the change enabled by introducing CPS as a new branch of science and technology provides much more than restructuring inside this domain. The new approach can turn entire industrial sectors into producers of CPS. Actually, CPS is about merging computing and networking with physical systems to create new capabilities and improve product quality [9].

Cyber-physical systems denote a new modeling paradigm that promotes a holistic view on real-world – and therefore complex – systems. These systems have been studied before from various particular perspectives using paradigms like ubiquitous and distributed computing or embedded and hybrid systems. The above mentioned facts require also another approach to the design of such systems respecting from the beginning of design process the application domain that influences quality-of-service requirements such as real-time behavior, safety and security [12], [13] and [14], but also precision, reliability and other non-functional properties and contentment affecting attributes specified usually by official standards [8].

In a CPS application, the function of a computation is defined by its effect on the physical world, which is in this case not only a system environment, but evidently also a component of the designed application system. Therefore, proper design environments should be used to improve or at

ISBN:978-1-61208-114-4

least to enable efficiency of the design process. In cyber-physical systems the passage of time becomes a central feature — in fact, it is this key constraint that distinguishes these systems from distributed computing in general. Time is central to predicting, measuring, and controlling properties of the physical world: given a (deterministic) physical model, the initial state, the inputs, and the amount of time elapsed, one can compute the current state of the plant. This principle provides the foundations of control theory. However, for current mainstream programming paradigms, given the source code, the program's initial state, and the amount of time elapsed, we cannot reliably predict future program state. When that program is integrated into a system with physical dynamics, this makes principled design of the entire system difficult. Instead, engineers are stuck with a prototype-and-test style of design, which leads to brittle systems that do not easily evolve to handle small changes in operating conditions and hardware platforms. Moreover, the disparity between the dynamics of the physical plant and the program seeking to control it potentially leads to errors, some of which can be catastrophic.

III. Wireless temperature data logger

Knowledge of temperature course during a certain time is needed in scientific, medical and industrial applications. In some applications, however, the recorded temperature course should be read wirelessly. This section describes main principles applied in a set of mobile temperature data logger and portable reader/writer with wireless transfer of digitized temperature values. The pilot concepts of the system were originally introduced in [7].

A. *Application basics*

A mobile temperature data logger with RFID features was designed for applications, where portability and wireless data transfer is inevitable. Communicating reader/writer can be mounted on the wall or can also be portable.

Two main modes of operation during temperature data logging may be remotely chosen for a tag:

- Mode 1 - normal data collecting method in preprogrammed regular acquisition time intervals (100 milliseconds up to 2 hours) with number of samples limited only by a data EEPROM memory size.
- Mode 2 - more memory size reducing method, when only breaking lower and upper temperature limits initiates storing the date and time stamp.

In mode 2, the following date and time stamp is stored only when the temperature returns back into the temperature band between lower and upper temperature predefined limits. Also enhanced mode can be set when the maximum or minimum temperature between breaking and returning points of a sampling temperature course is stored, too. This is a typical example for monitoring of food transport, where the time stamp and maximum temperature after breaking the limit help to identify that offender who damaged the transported goods.

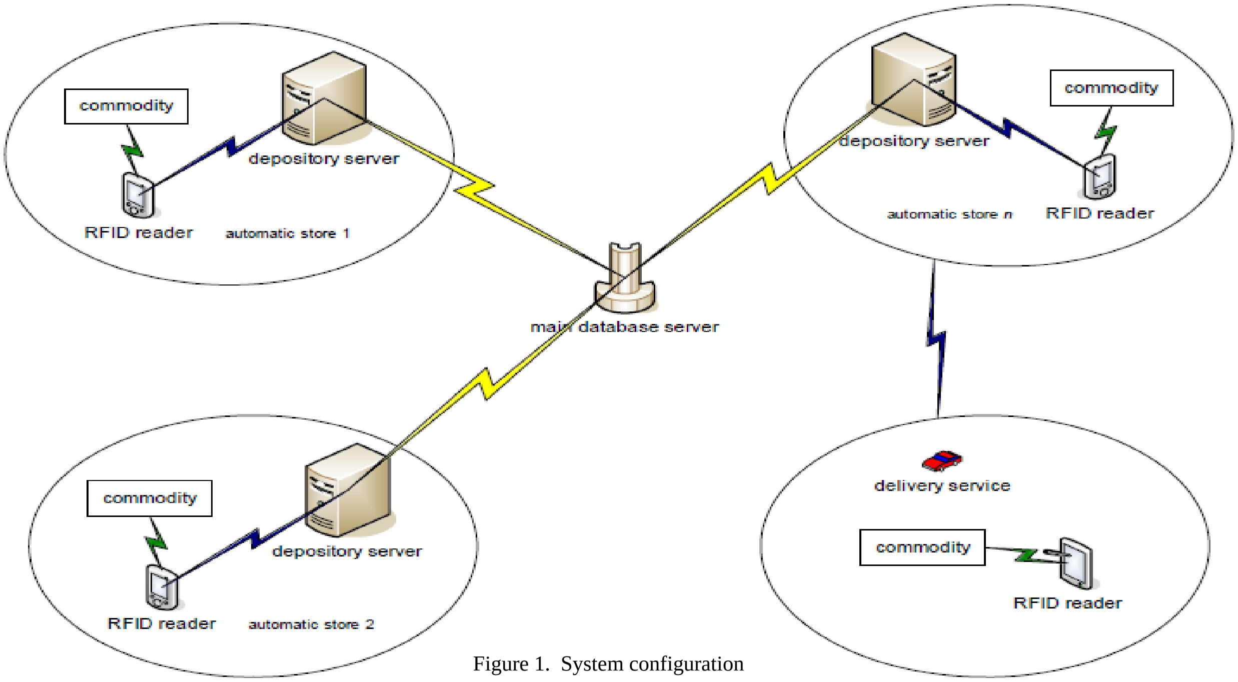

Figure 1. System configuration

Wireless RFID systems generate and radiate electromagnetic waves. This is the reason why those systems are legally classified as radio systems. The function of other radio services must under no circumstances be disrupted or impaired by the operation of RFID systems. For this reason, it is usually only possible to use frequency ranges that have been dedicated specifically for industrial, scientific or medical applications. These are the frequencies classified for worldwide as ISM (Industrial – Scientific – Medical), and they can also be used for RFID applications. The most important frequency ranges for RFID systems are therefore 135 kHz, 27.125 MHz, 40.68 MHz, 433.92 MHz, 869.0 MHz, 915.0 MHz, 2.45 GHz, 5.8 GHz and 24.125 GHz.

B. *Application constraints*

The range below 135 kHz is heavily used by other radio services because it has not been reserved as an ISM frequency range. The propagation conditions in this long wave frequency range permit the radio services that occupy this range to reach wide areas at a low technical cost. In order to prevent collisions, the future Licensing Act for Inductive Radio Systems in Europe, 220 ZV 122, will define a protected zone of between 70 and 119 kHz, which will no longer be allocated to RFID systems. The main block diagram of designed tag and reader/writer system is shown in Fig. 1.

Preferences for frequency range below 135 kHz allow reaching large ranges with low cost transponders. High level of power is available to the transponder. The transponder has low power consumption due to its lower clock frequency and often sleeping a standby mode of operation. Miniaturized transponder formats can be achieved due to the use of ferrite coils in transponder. Low absorption rate or high penetration depth in nonmetallic materials and water are available due to lower frequencies. Basic block diagram is shown in Fig. 2.

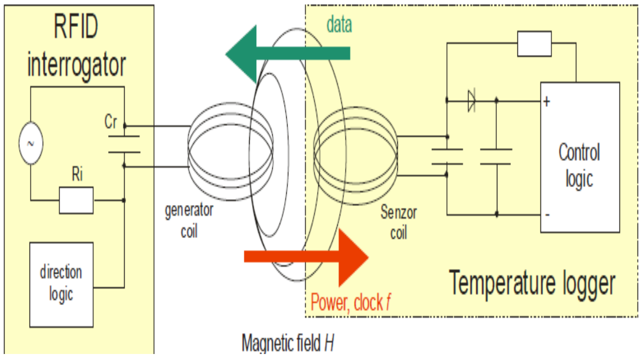

Figure 2. Basic block diagram

An inductively coupled data logger comprises an electronic data-logging device and a large area coil that functions as an antenna. Inductively coupled logger is almost always operated in passive mode of data transmitting between an RFID tag and reader. This means that all the energy needed for the data transfer to the temperature logger has been provided by the reader. For this purpose, the reader’s antenna coil generates a strong, high frequency electromagnetic field, which penetrates the cross-section of the coil area and the area around the coil.

C. *Data-logger design*

Temperature is recorded using a temperature tag at user defined time intervals. The temperature tag can be programmed so that when the memory is full it either stops further recording or continues recording by overwriting the earliest of the previously recorded data. Typical stored information contains: date and time stamp, temperature, temperature tag unique ID. Recorded information can be transferred to a reader/writer and then to a PC or a PDA with wired or wireless connection to a reader/writer. Temperature can be displayed graphically and the zoom functions allow focus on time periods where the temperature exceeds parameters.

The tag is a self-powered facility working like a wireless temperature sensor. It consists of a temperature probe and an active part with active RFID technology powered by an internal battery. The tag transmits an RF signal on demand at a pre-set time-interval. Tag life is estimated at several months depending on pre-set period of a transmission, where the related transmission interval can be configured via wireless connection by a reader/writer node. Each lifespan of the tag ends when the battery life is exhausted. Battery status can be inferred by interrogating the tag’s internal status value. The lifespan of the tag can be increased by delayed switch on by the first communication attempt of a reader/writer. A portion of this tag is used to measure actual temperature, to store measured data and to implement real time clock for timing. Distinct temperature values are acquired in pre-set intervals. The discussed tag can work in two basic modes as Data Logger and Out-of-Limit-Values Logger:

- Data Logger - Temperature is measured in pre-set intervals. All data is stored into the internal memory. In this mode there is stored only a start time. Number of measurements depends on memory size. Data logging principle is shown in Fig. 3.
- Out-of-Limit-Values Logger - If temperature is out of range, time stamp and temperature data are stored into the internal memory. Needless to say that the number of stored values depends on memory size.

This temperature tag is designed for usage in shipping containers, dairy industry, medical applications, fuel industry, refrigerated loads, agricultural industry, refrigeration monitoring, dangerous goods areas or anywhere, when temperature monitoring is required. Of course, the collection of possible applications is currently increasing for the reason that temperature is a critical process and quality assurance factor for many industries.

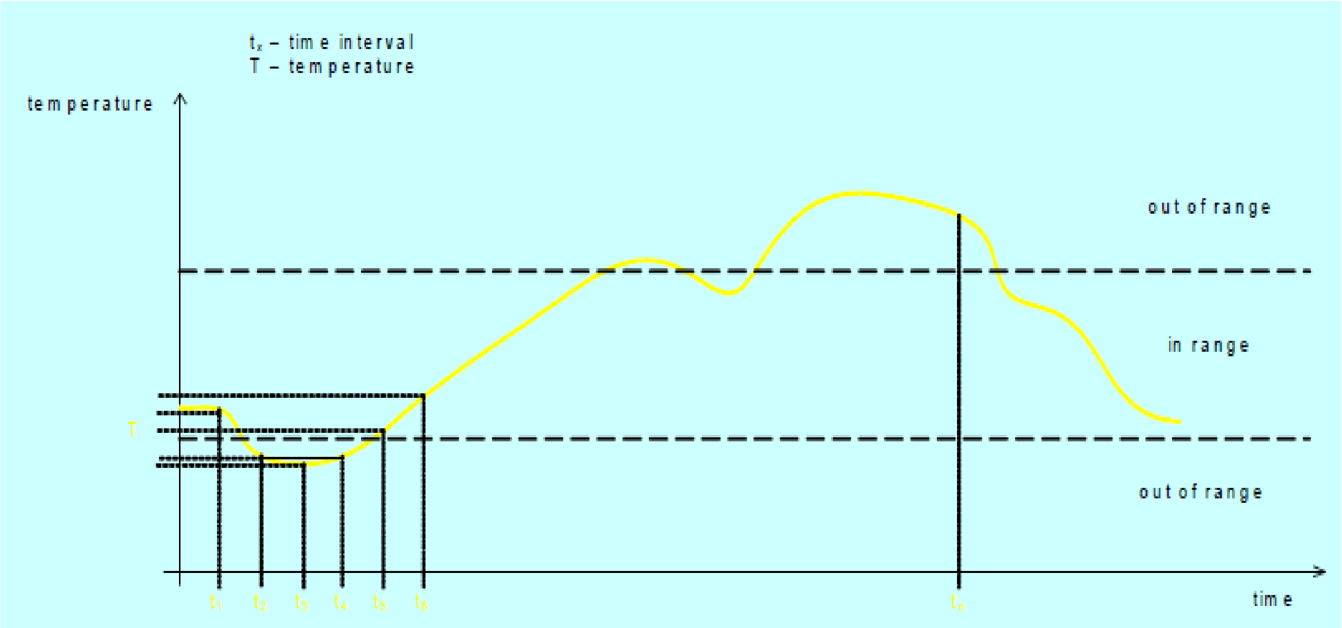

Figure 3. Data logging principle

IV. WIRELESS SMART SENSOR NETWORK

Many industrial systems cannot operate on cable connections among distributed components, which can be geographically remote, temporarily installed, allocated on rotating elements, etc. In such circumstances it is sometimes possible to connect smart sensors and actuators via RF wireless physical layer on ISM (Industrial, Scientific, and Medicine) band. For small range network with perimeter up to 100m the wireless connection standard Bluetooth can be used. This standard also enables to assure high safety and security of data by encryptions and related crypto-graphical techniques. The current section, which stems from partial results published earlier [15], proposes not only how to represent a system's solution as an application example, but also how to generalize reached research results.

The described novel wireless smart sensor network system represents the system architecture formed by a set of the wireless smart pressure IEEE 1451 sensors. This original prototype is connected using a Bluetooth and a network concentrator/controller is based on (see Fig. 4):

- A PDA personal digital assistant (IPAQ PDA 5450 in this case study) or
- A GSM SmartPhone (Nokia 3650 SmartPhone in this case study).

Particular software applications are developed for both IPAQ PDA 5450 and Nokia 3650 SmartPhone. Those SW applications fit system requirements for data monitoring, parameter setting and exploiting all embedded functions of the novel smart pressure sensor with Bluetooth wireless interface in the slave role mode. Another SW application for standard PC enables to process data in MS Office formats. Such wireless system virtual port enables to configure the related sensor, to sense and to record data by remote reading and/or writing via a Bluetooth SPP supported port by a PC, a PDA or a SmartPhone equipped with a Bluetooth standard access module.

A. *Application basics*

Many industrial systems may not use cable connection between components and blocks of the system. Components are geographically isolated, temporarily installed or allocated on rotating elements etc. However, it is appropriate in such case to realize interconnection between components by wireless communication network. The conclusions enable to connect smart sensors and actuators via RF wireless physical layer on ISM (Industrial, Scientific, and Medicine) band. For small range network with perimeter up to 100 m an industrial Bluetooth wireless connection standard can be used, where full Bluetooth stack and basic necessary functions have been defined.

This standard also accepts requirements to assure high safety and security of data by using encryptions and cryptography. Bluetooth stack and defined protocols are also compliant to Internet protocols.

ISBN:978-1-61208-114-4

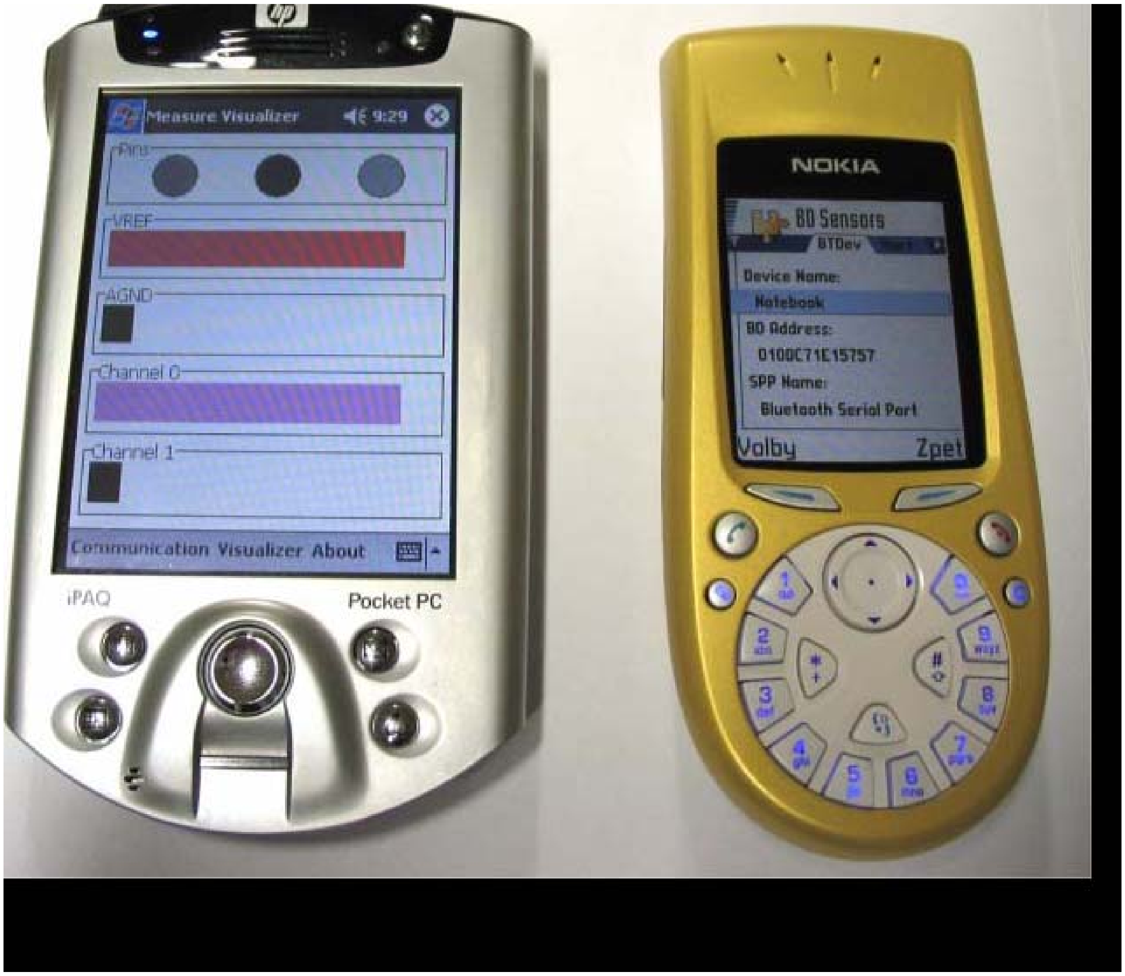

Figure 4. IPAQ PDA 5450 visualizing bar graphs of measured quantities
and GSM Nokia 3650 SmartPhone with a sample window for smart sensor parameter settings

Most of current control and measurement applications deploy galvanic connection of sensors and actuators to central control system. That scheme can cause some problems and limitations in cases, where it is not possible to use standard cable connection between control system (wiring station) and local sensors and actuators. Galvanic interconnection is possible in cases, when the configuration is permanent and it is possible to make cable interconnection between components.

This contribution, which stems from partial results published earlier, proposes not only how to represent a system's solution as an application example, but also how to generalize reached research results.

B. *Bluetooth*

The basic concept for connection of distributed smart sensor to the central data acquisition station is based on Bluetooth standard specification [1]. This standard defines data exchange among remote stations using RF wireless interface. The Bluetooth operates in the Industrial-Scientific-Medicine Band (ISM), which is in most countries defined as a band ranging from 2 400 MHz to 2 483.5 MHz.

In many countries, including the Czech Republic, the radio transmissions in the ISM band are not licensed. The Bluetooth standard defines 79 channels with the frequency width of 1 MHz in the ISM band. The position of any channel in the ISM band can be calculated as follows

$$f = 2402 + k,\ k = 0 \ldots 78 \text{ MHz}.$$

Devices corresponding to the Bluetooth standard are subdivided according to the transmitted power into three power classes: 100 mW, 2.5 mW and 1 mW.

Bluetooth based systems consist of the following components: radio transmitter (2.4 GHz Bluetooth radio), link controller (controls the transmitter), and link manager & I/O (provides terminal interface). The Bluetooth standard defines two different data transmission methods. The first one defines synchronous data channel (Synchronous Connection Oriented -SCO), which is intended mostly for audio transmission, while the second one defines asynchronous data channel (Asynchronous Connectionless - ACL). Both SCO and ACL utilize the same RF line.

The wireless network is built on the PICONET, which is the simplest interconnected Bluetooth network that can consist of up to eight nodes. In every PICONET one node acts as a MASTER, the rest as SLAVEs. More PICONETs can form a higher-level entity called as SCATERNET. The formation of SCATTERNET is permit for more PICONETs in the same location, of course, respecting some restrictions on transmission capacity.

A channel is represented by a pseudo-random sequence defining change of used frequency (hop sequence). All PICONETs share the same RF band; however, each PICONET has its own hop sequence. Thus at one time each PICONET uses its own 1 MHz wide channel. For the actual data acquisition the capabilities of transmission lines are very important. Bluetooth standard defines two different transmission lines that provide different throughput: asynchronous ACL and synchronous SCO. According to the demanded transmission capacity, it is possible to select the required type of the transmission line on the fly; so, the type of the transmission line can be negotiated as needed.

The SCO line allows synchronous 64 Kbit/s transmission. The ACL line allows transmissions asynchronous and PICONET-wide broadcasts. As the ACL deploys multi-slot system, it is possible to achieve transmission speed of 721 Kbit/s in one direction and 57.6 Kbit/s in the opposite direction (presented transmission speed expects zero error corrections).

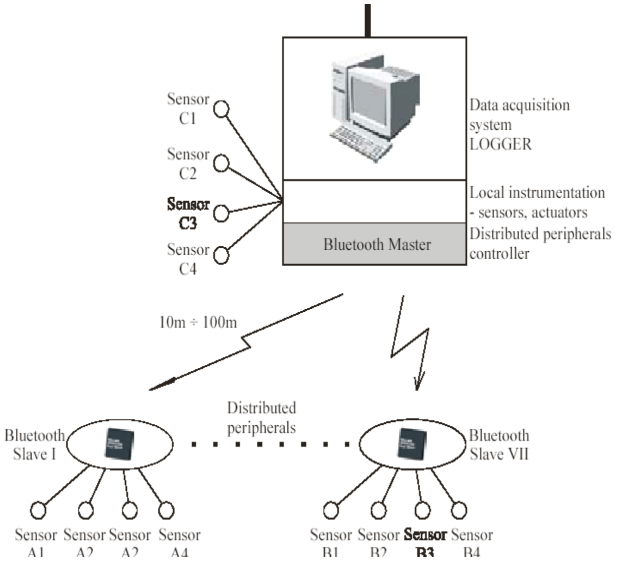

Figure 5. Structure of data acquisition system with data logger

Central data acquisition node (data logger) utilizes both integrated local sensory instrumentation, and distributed remote sensors connected to wireless Bluetooth network, see Fig.5. The data logger acts as a communication master, while the remote sensors act as slaves. In such network, there can be up to 7 distributed sensors. However, the distance between the master node and the slave cannot exceed 10/100 meters.

C. Data acquisition system

The number of possible Bluetooth masters in the central node defines the limitation of the entire distributed data acquisition system. The number of Bluetooth modules located in the same area is limited by the Bluetooth specification; hence, there should be guaranteed communication capacities that fit the application. The presented data acquisition system enables to include wide range of sensors with different requirements on their channel throughputs, e.g. simple temperature and humidity sensors as devices with narrow-band requirements, and CCD cameras as sensors with wide-band requirements on data throughput.

V. CONCLUSIONS

The paper, in its general part, is devoted to a brief review of state of the art of CPS domain, including important properties that can be implemented for applications, and to the typical features of CPS design, which are demonstrated in the rest of the paper. The presented real-world CPS applications deal with two designed sensory systems focusing on their physical design principles, system structures and communication architectures.

Our research group is currently launching a related continuation research that aims at the formal tools support of CPS design [11], [12], [13]. Evidently, this new research domain requires not only formal specification and verification techniques extensions and modifications, but also novel approaches and adaptations of such general methods as model checking and proving, see e.g., [1], [2], [3], [4], [8], [9] and [14].

ACKNOWLEDGMENT

The authors acknowledge contributions of their colleagues, namely Radek Kuchta, Pavel Steffan, Ondrej Sajdl and Zdenek Barton.

This project has been carried out with a financial support from the Czech Republic state budget through the CEZ MMT projects no. MSM0021630528: *Security-Oriented Research in Information Technology* and no. MSM 0021630503: *MIKROSYN - New Trends in Microelectronic Systems and Nanotechnologies*, by the Grant Agency of the Czech Republic through the grant no. GACR 102/08/1429: *Safety and Security of Networked Embedded System Applications*, by the Ministry of Industry and Trade CR through the grant no. FR-TI1/037 of Ministry of Industry and Trade: *Automatic Attack Processing*, and by the Brno University of Technology, Faculty of Information Technology through the specific research grant no. FIT-10-S-1: *Secured, Reliable and Adaptive Computer Systems*.

REFERENCES

[1] R. Akella and B.M. McMillin, Model-checking BNDC Properties in Cyber-Physical Systems, *Proceedings of the33rd INternational Computer Software and Applications Conference COMPSAC 2009*, IEEE CS, New York, NY, US, 2009, pp. 660-663.

[2] Borzoo Bonakdarpour, Challenges in Transformation of Existing Real-Time Embedded Systems to Cyber-Physical Systems *IEEE Symposium on Real-Time Systems RTSS RTSS - Ph.D. Forum on Deeply Real-Time Embedded Systems*, Tucson, Arizona, 2007, 2pp.

[3] M.C. Bujorianu and H.Barringer, An Integrated Specification Logic for Cyber-Physical Systems, *Proceedings of the 14th IEEE International Conference on Engineering of Complex Computer Systems*, Potsdam, Germany, 2009, pp. 91-300.

[4] J. C. Eidson, E. A. Lee, S. Matic, S. A. Seshia, and J. Zou, Time-centric Models For Designing Embedded Cyber-physical Systems, EECS Department, University of California, Berkeley, *Technical Report No. UCB/EECS-2009-135*, October 9, 2009.

[5] J. Fraden, *Handbook of Modern Sensors.* New York, AIP Press, 1997.

[6] B.H. Krogh, E. Lee, I. Lee, A. Mok, R. Rajkumar, L.R. Sha, A.S. Vincentelli, K. Shin, J. Stankovic, J. Sztipanovits, W. Wolf, and W. Zhao, *Cyber-Physical Systems, Executive Summary*, CPS Steering Group, Washington D.C., March 6, 2008. [http://www.nsf.gov/pubs/2008/nsf08611/nsf08611.htm] [accessed: June 30, 2010]

[7] R. Kuchta, P. Steffan, Z. Barton, R Vrba, and M. Sveda, Wireless Temperature Data Logger, *Proceedings of the 2005 Asian Conference on Sensors, and International Conference on new Techniques in Pharmaceutical and Biomedical Research*, 5-7 Sept. 2005 pp. 208-212.

[8] E.A. Lee, Computing Needs Time, *Communications of the ACM*, Vol.52, No.5, pp. 70-79, May 2009.

[9] National Science Foundation, *Cyber-Physical Systems Program Solicitation, NSF 10-515*, Arlington, VA, US, March 11, 2010

[10] J.A. Stankovic, I. Lee, A. Mok, and R. Rajkumar, Opportunities and obligations for physical computing systems, *IEEE Computer*, November 2005, pp. 23-31.

[11] M. Sveda and R. Vrba, An Embedded Application Regarded as Cyber-Physical System, *Proceedings of the Fifth International Conference on Systems ICONS 2010*, Les Menuires, FR, IARIA, 2010, pp. 170-174.

[12] M. Sveda and R. Vrba, Meta-Design with Safe and Secure Embedded System Networking, *International Journal On Advances in Security*, Vol. 2, No. 1, 2009, US, pp. 8-15.

[13] M. Sveda and R. Vrba, Specifications of Secure and Safe Embedded System Networks, *8th International Conference on Networks Proceedings ICN 2009*, New York, NY, US, IARIA, IEEE CS, 2009, pp. 220-225.

[14] H. Tang and B.M. McMillin, Security Property Violation in CPS through Timing, *Proceedings of the 28th on Distributed Computing Systems IDCS 2008, Workshops*, IEEE CS, New York, NY, US, 2008, pp. 519-524.

[15] R. Vrba, O. Sajdl, O., R. Kuchta, and M. Sveda., Wireless Smart Sensor Network System. In Proceedings of the ICSE & INCOSE 2004 Conference. Las Vegas, Nevada: CRC Press LLC, 2004, pp. 104-109.