# Smart object design for active security management of hazardous products

Dragos Dobre, Eddy Bajic

DIPSO 2007 1st International Workshop on Design and Integration Principles for Smart Objects In Conjunction with the Ninth International Conference on Ubiquitous Computing (Ubicomp 2007) September 16, 2007. Innsbruck, Austria

**Dragoş DOBRE · Eddy BAJIC**

# Smart Objects Design for Active Security Management of Hazardous Products

Received: June 14, 2007 / Accepted: July 18, 2007

**Abstract** Hazardous substances are products that need special attention from the personnel which manipulates them, therefore, there is an increased need for better security management of goods and people in chemical industries. In this paper we propose the design of the Smart Object capable to survey its own environment according to its own security rules and to cooperate with others surounding equiped products to manage the security level in acceptable boundaries. By this way, an Active Security Environment is created, in which, hazardous products transformed into Smart Objects monitor, notify and alarm when security conditions are inappropriate.

**Keywords** Smart Object · WSN · Active Security · Chemical Product · RSSI

## 1 Introduction

Nowadays, security is one of the most important problems. Even if we speak about security in everyday life, security in working environment, the concern about our security or the security of others makes this one of our top interests.

Sometimes, without our concern, we trust our lives to others as we depend on security measures that others take for us in environments that are out of our control. Such examples are storage and transport environments of chemical substances. Without a high security level, industrial companies and workers are exposed to big risks on both economical and human aspects. That is a good reason to develop a security management policy of hazardous products based on rules and constraints associated to individual products and to products interactions.

Basically when we have a barrel that contains a chemical substance, a security system must be implemented that considers all the factors that can increase the intrinsic risk level of that substance, potentially explosive, toxic or harmful for its environment. One of the main European Union law concerning chemical safety is the Council Directive 67/548/EEC describing regulations relating to the classification, packaging and labelling of dangerous substances. For a warehouse application scenario, we must consider the safety data sheets of each substance as described in the Merck catalog according to european directives 67/548/EEC and 91/155/EEC and then implement a set of rules to monitor and control the product security level.

As the overall security level is the matter of each individual product and of its interaction with its vicinity, an efficient security management needs to be based on a distributed security model approach supported by individual products. Thus each product is an active brick of the whole security system by means of product embedded security functions as monitoring, controlling, decision making and alarm. Ambiant and communication technologies bring a new vision to create reliable security systems where products are transformed into smart products. In our concept, a product (chemical container) can be aware of the conditions it is stored in, of the environment changes and of other products situated in its proximity. So product can have a reactive behavior to all the changes or inappropriate storage conditions based on the security rules whose it is constrained. By using WSN[1], attached to barrels, we create a network of interactive Smart Objects to implement an Active Security system.

This article describes the concept and realization of an Active Security System for security management of warehousing and transportation of chemical substances. It is divided into five sections: the second section introduces the Active Security concept relying on a Smart Object approach. In the third section we describe the pParticle technology used for the smart product design. The other two sections describe the methodology and the

Dragoş DOBRE · Eddy BAJIC
CRAN Laboratory - CNRS UMR 7039
Nancy University, France
E-mail: {dragos.dobre; eddy.bajic}@cran.uhp-nancy.fr

[1] Wireless Sensor Network

implementation of the Active Security system. Then we close this article with conclusions and a vision for future developments.

## 2 Smart Objects for Active Security Management

Along with the passing of time, as technology becomes more and more interweaved with everyday activities a new era arises, one that has been assigned the name of "ubiquitous computing" [7]. This newborn concept relies heavily on the use of smart objects in order to manage the correct handling of sensitive information.

Smart objects were introduced for the first time in Neil Gershefelds article "When Things Start to Think" which designated them as having the following major characteristics: owning an unique identity and being able to communicate with other objects and to detect the nature of their environment [3].

For instance a research group at Lancaster University UK is studying a smart object approach towards assuring the correct storing and handling of hazardous chemicals [6]. They have identified a number of scenarios leading to dangerous situations that can occur in a variety of working environments: at a chemical plant, in an external warehouse or during transport. Moreover, these environments are not under uniform control but involve diverse ownerships. Thus they argue in favor of Cooperative Artifacts, communicating standalone devices that do not rely on exterior supervision and that are implemented through barrels equipped with Smart-its Particles. These are able to collect data from the outside, process it and transform it into knowledge that is then used in order to generate an action according to the situation. The key point of their concept is that the knowledge associated with the artifact is stored and processed within the artifact itself. Therefore a barrel is able to know its own status but needs to communicate with the others in order to reason on a changing environment. The distributed knowledge base is a good way to solve the problem of variable surroundings appearing in the cycle of life of the chemical wastes. However this might lead to a difficult decision when it comes to delimiting the information that should be stored in each object and to over flooding with messages from one artifact to another.

Another smart object application is looked into by a team of researchers from TecO in cooperation with Karlsruhe University, Germany, and Massachusetts Institute of Technology, USA [2]. They are trying to coordinate the integrity of paper written documents, to enforce access restrictions and to keep track of changes in both the physical and the electronic document. Their solution, named DigiClip, is an electronically enhanced paperclip built on the basis of Smart-its Particles. It can ensure the proper use of the documents within its grasp by monitoring their whereabouts through a location tracking system. This is a graphical interface that displays all the rooms in a certain area. The Smart-its Particles communicate with the computer program over the air, thus sending their address and their location. In this manner the particle can not only know where it is situated but also hold an archive of all the former places where it's been. A combination of an accelerometer and a light sensor enables the detection of a document that is being put into or taken out of a bag, further extending the tracking capabilities. In addition, the smart paperclip can ensure the integrity of a document by "counting" the number of pages. It does so by making use of a sine wave generator and a resistor measuring the capacity of the stack of paper. It has proven itself to be accurate for up to 20 pages.

A different type of smart object is being employed by the CHAOS project from CalTech to secure the information exchange in distributed systems [5]. CHAOS integrates security policies in data objects as active nodes in order to form active objects. In this case the active objects are represented by a special type of XML objects that encompass data elements as well as active elements. Each one of the latter contains one active node by mean of a Java class that must be interpreted by a runtime environment. When a query is passed to one of the active objects its active node is dynamically loaded and executed by the security mediator. The mediator is the system component that parses and filters all the information requests, and then leads to the enforcement of the security policies that lie within the active nodes. It is these policies that modify the content as well as the structure of the data elements according to the user's permissions.

## 3 Particle Platform

The development of a Smart Object needs some characteristics to be fulfilled: it can memorize its state, it has the ability to sense its environment, to communicate with its surrounding and to react after taking a decision on its own. One technology that gives us the desired functionalities is the WSN with embedded computing capabilities. One node can survey its near environment

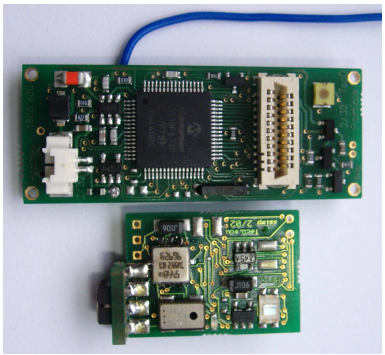

**Fig. 1** The pParticle 2/32 with SSimp 2/02

and communicate with other nodes. Also, it can take decisions based on algorithmic computation accordingly to perceived information.

In our project we use the pParticle ver. 2/32 with the full sensor circuit SSimp ver. 2/02, produced by *Teco* and commercialized by *Particle Computer*. This WSN platform has been chosen for its capabilities, which help us to detect all factors that influence the level of security. Also, in order to communicate within a wireless network, we used the wireless bridge, WBride.

In this section we present the Particle platform by means of hardware devices and their capabilities.

### 3.1 Particle device

One Particle device is composed by the Particle base and the sensor module. In fig. 1 we present the two components. The Particle base is the core of the device, whose characteristics are presented in table 1. The interesting points are the microcontroller, especially for its frequency, the flash memory, in which the smart object can save security information and rules, and the communication capabilities.

The Particle device include several sensors:

- temperature (TC74) can sense the temperature from 0℃ to 125℃;
- light (TSL2550), that can sense normal and infrared light;
- two 2D accelerometer (ADXL210) to create one 3 axis accelerometer;
- audio (MAX8261 OP);
- voltage on the board.

We use these sensors in order to create an image of the environment. By this way, the product can actively verify its intrinsic security state in order to react to changes that can affect its normal storage or handling conditions.

**Table 1** pParticle base characteristics

| Feature | Description |
|---|---|
| Microcontroller | PIC 18F6720 at 20 MHz |
| Internal Memory | 128kbyte program Flash |
| RAM | 4kbyte |
| EEPROM | 1kbyte |
| Additional Memory | 512 kbyte FLASH |
| Communication | RF through RFM TR1001 |
| Bandwidth | 125kbit |
| RF Power | <1mV |
| Interface | 21 pin multi purpose connector |
| Power regulation | 0.9 to 3.3 V |
| Board core voltage | 3.3V |
| Working temperature | -40 to +85C |
| Size | 45x18 mm (no battery) |
| Programmable | in C, Over-the-Air-Programming |

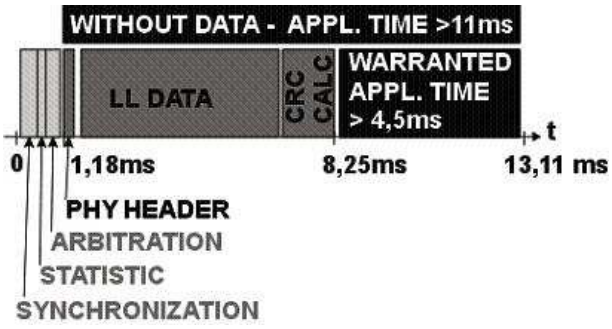


**Fig. 2** The AwareCon frame structure

The device include also a RSSI[2] sensor to be used for distance measurement between two devices. This way, the smart objects can automatically detect incompatibilities between them. RSSI is discussed in section 5.1.

### 3.2 Particle communication

The pParticle devices are equipped with a 125 kBit TR 1001 radio frequency module functioning at 868.35 MHz. The RF communication protocol is based on AwareCon [1], the wireless ad hoc customized protocol for the particle computer. Its design follows the fundamentals of the established OSI/ISO layered approach. AwareCon (fig. 2) is composed of three layers: the physical radio frequency layer (RF), the Link Layer (LL) and the Application Convergence Layer (ACL). One of the most important aspects in designing a communication protocol for a distributed networked sensor systems is mobility. As a result, AwareCon is able to handle a high mobility of the particle nodes, the main delay for the synchronization with another partner being around 40 ms.

The design of AwareCon also reflects the concept of a fully distributed system. All nodes have equal responsibilities to establish time slots, exchange synchronization signals and keep an established timing scheme alive. There are no access points or master devices like in W-LAN, Bluetooth or many other known protocols. The channel access uses a nondestructive bit wise arbitration known from wired networks such as the CAN field bus. This access method achieves low collision rates especially for a high number of concurrent nodes and can also handle priorities.

The data traffic is organized in packets of 64 data Bytes. To allow multiple nodes to use the same frequency channel the signal is divided into time slots. Each time slot of AwareCon can carry one packet of data.

A common communication language is required to be able to exchange information between nodes. In the Particle System the proposed approach is ConCom [4], a mode to represent transmitted data as tuples. A tuple is a byte sequence that starts with a type identifier

[2] Received Signal Strength Indicator

(2 bytes), followed by a length statement (1 byte) and then the number of data bytes specified by the length. The first tuple is referred to as the subject and it is used to enable application specific data processing within the system. An application subscribes itself to a subject and filters thereafter all received information, while the procedure for sending from the application uses the subject as the prescript of the outgoing message.

## 4 An Active Security Environment

As a standalone device, the hazardous product acting as a smart object can collect data from the environment and process it. Its reaction to an environmental threat can be an audible/visual alarm or alarm messaging to notify the security personnel. When more products are close to each other, smart objects can also react to each other by requesting information or responding to another. In both cases the reactive behavior of the hazardous products creates an active security environment.

At a product configuration stage, static information is stored on each product by a central monitoring software or a handheld PDA: substance name, substance ID from Merck catalog international chemical products numbering, Product's electronic product code (EPC), security phrases and security symbols according to european directives 67/548/EEC (toxic, inflammable, explosive, oxidant, dangerous for the environment, radioactive, corrosive, irritant). This is the static core information of the product to uniqually identify it as an hazardous and commercial item. Supply chain traceability and manufacturer's information are supported by EPC numbering schema and internet information services support.

Working or surrounded with hazardous products creates dangerous space where certain ambiant and environmental parameters influence the intrinsic security level of each product. Variation of the ambiant factors can disturb the normal and balanced state of the chemical substance inside a barrel. We consider the following environmental factors are capital for intrinsic security monitoring of each hazardous product (a radioactive sensor should be also of great interest) :

- *temperature* : substance reacts violently changing its structure, and stability, ending with an explosion;
- *acceleration* : substance has reaction to shocks and movement handlings;
- *light and infrared light* : substance reacts and alters with light;
- *audio level* : substance reacts to frequencies stimulation or audio levels.

The Intrinsic Security level of hazardous product is processing from internal sensors data relating to a set of rules that we describe as a set of boundaries limits for parameters values. For the temperature value we have implemented a high and low limit. For light, infrared light, audio and acceleration values we have implemented only high limits. Using the safety data sheet of each chemical substance we can establish what are the specific values for each limit and store them in static information of the smart product at configuration stage. Therefore, the smart product determines its internal security level with reasoning by inference on the sensor's values and boundaries limits. A fuzzy logic quantification of individual parameter security level is proposed : Level 1 or Good when value is within +/- 90% of the boundaries; Level 2 or Bad when value is above +/- 90% and Level 3 or Dangerous when value is 100% and above. The global intrinsic security level of a hazardous product is an aggregation of all individual parameters security levels.

In addition, the extrinsic product security level depends on the nature and the compatibility agreements of other products located in the vicinity. A compatibility relationship can be derived from the security symbols coded in each product in its static information at configuration stage. We have designed compatibility rules by means of a compatibility matrix with cross-relation of security symbols then coded in static information on the smart product. Based on the compatibility matrix, some security symbols are incompatible with others so every substance has compatible and incompatible symbols. The extrinsic security level of a hazardous product is Good when all producs in the vicinity are compatible, and Dangerous in all other cases.

In an active security environment a smart object sends information about the substance inside the barrel: the substance ID and the security symbols. Any other smart object receives this information, calculates the RSSI value of the message, and sends that value with its own security symbols. The first product receives this message, reads the RSSI value, verifies the compatibility with the second product and calculates its extrinsic security level.

The global security level for the hazardous product is a logical combination of intrinsic and extrinsic security levels with alphabet {G,B,D} where B and D are absorbant states.

## 5 Smart Object's behavior for security management

Each hazardous product when equipped with pParticle device is tranformed into a smart object dedicated to security management activity based on product's characteristics and limitations rules coded in static information and also on security symbols and compatibility matrix. Hazardous product has the ability to monitor its environment and ccommunicates with other hazardous products or systems. Fig. 3 illustrates the algorithmic behavior of a smart object, built on three main loops : not configured loop, new message received loop and internal check loop.

In a default application case scenario, a new barrel enters the warehouse, and sends periodically to the su-

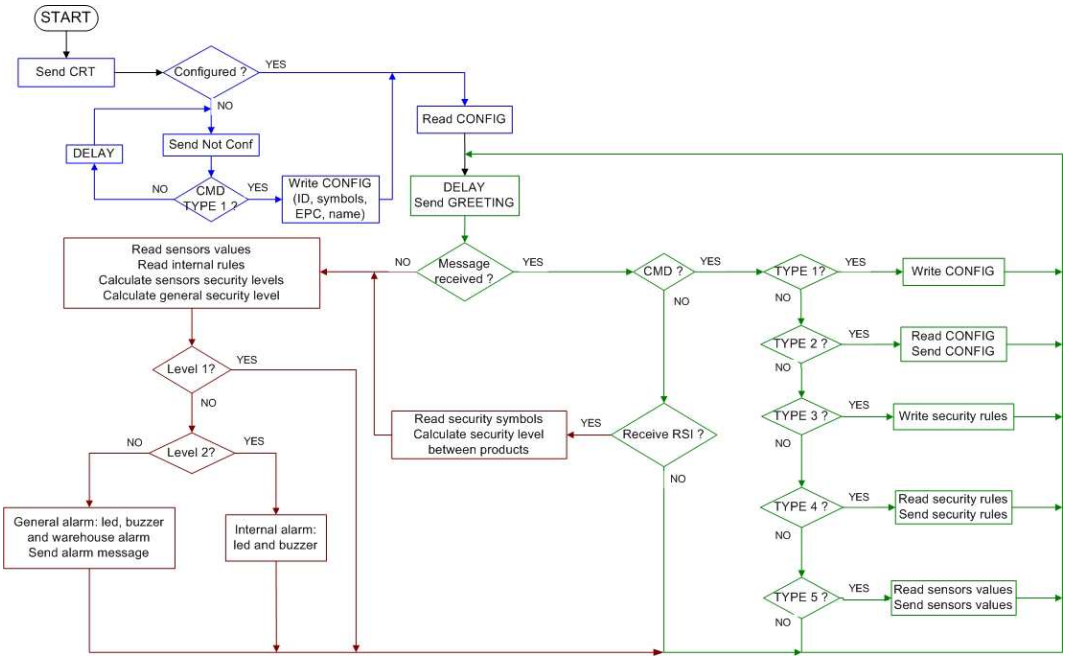


**Fig. 3** The algorithmic behavior for security management on a Smart Product

pervisor system not-configured messages until it receives a configuration. Qualified personnel remotely configure the smart product with related to the substance inside the barrel. This can be done at automatically at manufacturing stage in a M2M approach.

After receiving the configuration, the smart object enters IDLE state by sending greeting messages. In IDLE state the smart object reads all sensors values, calculates the RSSI values for each smart object in the proximity and then calculates a product global security level. Each greeting message is sent in broadcast and contains the substance ID inside the barrel and the product global security level. If no changes in conditions monitoring the smart object remains in that state.

If any sensor value reaches 90% of the internal security limit the smart object records the value and enters a state of warning or security level 2. If he succeeds 100% of that limit he enters in security level 3 or alarm. In both cases the smart product sounds an audible alarm and sends alarm messages with the level of security. Alarm message indicates the sensors out of range or the ID of incompatible barrels close to him. Hazardous product informs the vicinity of a danger like does a blackbird with its cry when predators are close to the nest. It returns to IDLE state when the threat has disappeared. All messages are broadcasted (greeting, command and RSSI) and used to communicate either between smart objects or between smart object and supervisor. The command messages are mainly used by the supervision application to configure the smart objects (type 1 and 3), to read the configuration (type 2 and 4) and to monitor the value of the sensors (type 5).

### 5.1 RSSI for extrinsic security level determination

For extrinsic security level calculation of hazardous product, RSSI method is used to estimate the distance with other hazardous products that could worsen the global security level by way of their incompatibility. We integrated the pParticles devices in conductive ABS plastic boxes to be affixed on industrial chemical containers. Particle's antenna is left on the outside so it can be freely tilted to any position. After conducting experiments with and without the packaging we concluded that it has no influence on the message transmission quality.

Many other factors, mostly controllable, affect the values indicated by the RSSI. One of them is the orientation of the particle's antenna. During our experiments we noticed that the indications vary as follows: when the antenna is pointed upwards the RSSI value is smaller than when it is positioned horizontally.

Yet another factor that influences the measurements is the place where the particles are positioned. When they are situated on the floor of a room the signal strength is quite inferior to that when particles are positioned on top of the barrel. This can limit the detection of barrel fallen on the ground.

RSSI level is obviously conditioned by the Batteries charge level so therefore transmission signal strength must be accorded consequently. More over the signal strength becomes a real problem when obstacles are positioned between the smart products. Paperborad boxes for exemple extend the interval between consecutive RSSI measurements but the electronic devices act like a screen and distrub the sending of the messages completely.

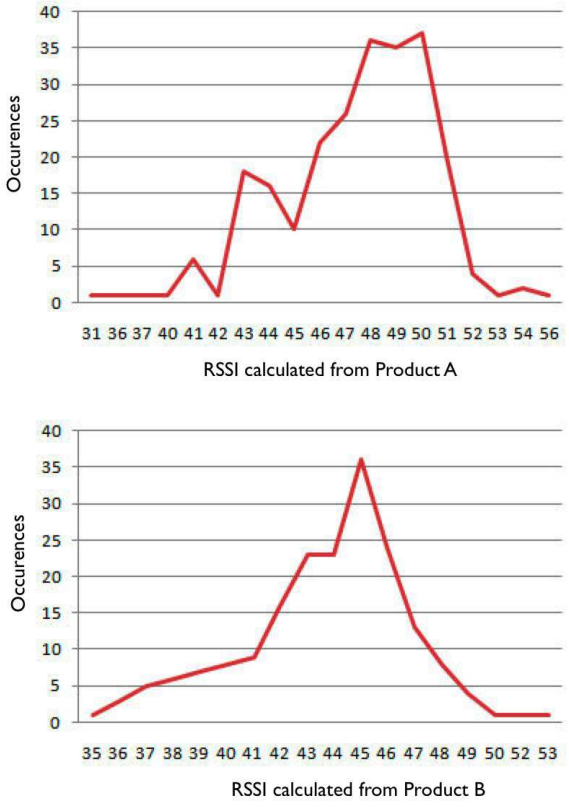


**Fig. 4** RSSI measurements distributions

An important issue to be taken into account is that not all particles send the same value for a given distance. Even though the circuitry is basically the same an experiment with two particles has shown that the average RSSI measurements over a period of time differs substantially for the two devices. Fig. 4 shows the distribution functions of RSSI measurements for two Smart products (A, B) facing at a distance of 1m. The measurement is asymetric as one particle indicates an average RSSI of 43,70 and the other 47,41.

During our experiments we have found relevant indications of the RSSI for distance up to 3 meters. This distance is appropriate to define a bubble of security around a product. For longer distances RSSI's messages were becoming either too scarce or completely absent. Fig. 5 reveals the RSSI indications at various distances and also the standard deviation tube.

## 6 Conclusion

The presented work proposes and demonstrates the feasibility of achieving Active Security management of chemical hazardous products by use of Smart Object's approach. By providing the product with capabilities for ambient sensing and monitoring, vicinity communication, and a rule-based decision making according to security compatibility regulation specifications, we grant to the hazardous products an autonomous and adaptative security-oriented behavior. Proactive alarm and preventive actions can be embodied in each hazardous product to prevent a catastrophic situation in hazardous chemical areas. With modeling of a smart product's behavior dedicated to security management of hazardous products, we define the concept of an Active Security Distributed Management System. Both theorical and technological points are still outstanding and must thus be investigated deeply like the monitoring of the product's extrinsic security by the co-operation of distant products, and robustness on a great scale of products.

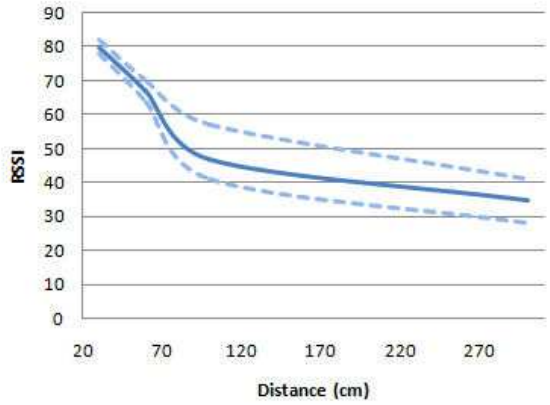


**Fig. 5** RSSI measurement for products distance evaluation

**Acknowledgements** The authors thank Iulia BUNU, Roxana FALCOS, Andrei MITRICA, Bogdan NICOLAE, Alexandru VELICU, for their involvement in this research work conducted in the framework of a Leonardo da Vinci program with University Polithenica Bucarest.

## References

1. M. Beigl, A. Krohn, T. Zimmer, Christian Decker and P. Robinson, "AwareCon: Situation Aware Context Communication", Ubicomp 2003, Oct. 12-15, Seattle, USA (2003)
2. Christian Decker, Michael Beigl, Adam Eames and Uwe Kubach, "DigiClip: Activating Physical Documents", ICDCSW'04, Tokyo, Japan (2004)
3. Gershenfeld N., "When Things Start to Think", Henry Holt & Company, 1st edition, USA (1999)
4. A. Krohn, Michael Beigl, Christian Decker, P. Robinson and T. Zimmer, "ConCom - A language and protocol for communication of context", Technical Report ISSN 1432-7864 2005/19 (2004)
5. David Liu, Kincho Law and Gio Wiederhold, "CHAOS: An Active Security Mediation System", Conference on Advanced Information Systems Engineering, Stockholm, Sweden (2000)
6. Martin Strohbach, Gerd Kortuem and Hans Gellersen, "Cooperative Artefacts - A Framework for Embedding Knowledge in Real World Objects", Smart Object Systems, 91 - 99. UbiComp 2005, Tokyo, Japan (2005)
7. Marc Weiser, "The computer for the 21st century", Scientific American 265, No. 3, pages 94 - 104 (1991)