Active product modeling for chemical security management based on smart object concept

Dragos Dobre, Eddy Bajic

7e *Conférence Francophone de MOdélisation et SIMulation - MOSIM'08 - du* 31 *mars au* 2 *avril* 2008 *- Paris - France*
«Modélisation, Optimisation et Simulation des Systèmes : Communication, Coopération et Coordination»

ACTIVE PRODUCT MODELING FOR CHEMICAL SECURITY MANAGEMENT BASED ON SMART OBJECT CONCEPT

Dragoş DOBRE, Eddy BAJIC
Research Center for Automatic Control (CRAN), Nancy - Université, CNRS UMR 7039,
BP 239, F-54506 Vandœuvre-lès-Nancy Cedex, France,
Dragos.Dobre;Eddy.Bajic@cran.uhp-nancy.fr

ABSTRACT: *Nowadays the management of the security of goods and persons is a stake mattering in industries. In general, product's security level is the matter of each individual product and it often depends on products' interactions within vicinity. An efficient security management needs to be based on distributed security model supported by each individual products. Ambient and communication technologies bring new visions in creating reliable security systems, where products are transformed into smart products. Thus, each product acts as an active brick of the whole security system by means of embedded security functions as monitoring, controlling, decision making and alarming actions according to security and dependency rules. We propose the Active Product concept that provides product reactive behaviors to changes and inappropriate storage conditions, based on the security rules it is compelled. In our approach a product as for example a chemical container can be aware of its handling and storage conditions, and of changes in its environment and can be sensitive to products which surround it. Using wireless sensors attached to products, we create a network of interactive and communicating products to manage an Active Security System in an Ambient Intelligent Environment where human operators and hazardous chemical products are interacting securily in warehoursing and handling area. This article describes the concept Active Product by mean of smart object functionalities applied to hazardous industrial product and it proposes an internal structure model and associated capabilities of Active Product entity dedicated to security management.*

KEYWORDS: *Smart Object, Active Security, Wireless Sensor Network, Chemical Product, Ambient Intelligence.*

1. INTRODUCTION

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. This is a fact in industrial application cases as storage and transport management 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.

A security system must be implemented each time we work with barrels containing chemical substances. This system considers all factors that can increase the intrinsic risk level of the substance, potentially explosive, toxic or harmful for its environment and the personal manipulating it. One main European Union laws concerning chemical safety is the Council Directive 67/548/EEC, describing regulations for classification, packaging and labeling of dangerous substances.

In a warehouse application scenario, we must consider safety data sheets for each substance in according to European Directives 67/548/EEC (European-Community 1967) and 91/155/EEC (European-Community 1991). Chemical data sheets can be found in Merck[1] catalog. One can use these to implement a set of rules to monitor and control the product security level.

This article describes the concept and realization of an Active Security System (ASS) for security management for warehousing and transportation of hazardous chemical products. 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 Particle Computer technology used for the smart product implementation. The next two sections describe the methodology, design and implementation of the ASS. The last chapter will conclude and give a vision for future developments.

2. AMBIENT INTELLIGENCE AND SMART OBJECTS

As technology becomes more and more interweaved with everyday activities, a new era arises, one that

[1] http://www.merck.de

has been assigned to Ubiquitous Computing (Weiser 1991). This newborn concept relies heavily on the use of Smart Objects in order to manage the correct handling of sensitive information.

The Smart Object concept was introduced for the first time in (Gershenfeld 1999). Also referred as inteligent product by (McFarlane, Sarma, Lung, Wong & Ashton 2002) it is commonly accepted in the research community on automated manufacturing systems as the merging of physical and informational objects characterized by the following elementary features enriched several times :

- possesses a unique identification (Wong, McFarlane, Zaharudin & Agarwal 2002);
- is able to communicate effectively with its environment (Kintzig, Poulain, Privat & Favennec 2002);
- can retain or store data about itself;
- is capable of taking part or making decisions relevant to its destiny;
- develops interactions between products and their environment;
- offers objects advanced services along its life cycle (Bajic 2005).

The Ambient Intelligence (AmI) is the domain of research for many companies and research centers. According to (Remagnino & Foresti 2005), AmI is based on a distributed layered architecture enabling ubiquitous communication and advanced human - machine communication protocol, allowing persons to be assisted by the surroundings' objects which are sensitive to people's presence and respond to their needs. The key technologies used to deploy AmI (Alcañiz & Rey 2005) are Ubiquitous Computing, Ubiquitous Communication and Intelligent User Interfaces. Ubiquitous Computing refers to integration of microprocessors in everyday objects. Ubiquitous Communication enables objects to communicate with each other, with the environment and with persons that are present in their proximity.

Adding so smart capabilities to real-world objects is a common goal in Ubiquitous Computing community. Then two important decisions, needed to be made when designing smart objects, are whether they will be able to function without any infrastructure support (this means as fully autonomous objects) and whether they advertise and propagate their individual functionalities and properties.

Research activities in Smart Object community are mainly focused on service infrastructures specification and prototyping of Smart Objects which are functionally autonomous, in the fact that they can operate with and without any infrastructure. A survey can be found in (Bajic, Cea-Ramirez & Dobre 2008). In the manufacturing system community, we can identify the holonic approach, promoted by IMS/HMS research project. The holon-product concept is similar to Smart Object definition, but it is often physically distributed and dependent on hierarchical system architecture to fulfill its objectives. Multi Agent Systems programming techniques is an implementation technology mainly used to test and evaluate distributed models of holons' collaborative interactions (Fisher 1999). Our approach is closer to the Smart Object community to assume a fully autonomous product behavior by itself.

"Smart-its" projects community (Holmquist, Gellersen, Schmidt, Strobach, KOrtuem & Beigl 2004) creates autonomous smart objects by attaching small computational devices (smart-it devices) to physical object, thus, they argue in favor of Cooperative Artifacts as communicating standalone devices that do not rely on exterior supervision.

In the aim of managing the security level of goods and people in the activities of storing and handling of hazardous chemicals products, we can identify 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, handling or moving between companies. Moreover, these environments are not under uniform control, but involve diverse ownerships and somehow diverse system infrastructures or organizations.

So, smart products can be a way to achieve interoperability among companies or infrastructures as they can rely very weakly on the hosting system without denying their intrinsic capabilities for their self-monitoring or cross-regulation.

Thus, autonomous active products, implemented through containers equipped with Smart-its Particles, are able to collect data from the outside, process it and transform it into knowledge that is used in order to generate an action according to the situation (Strohbach, Kortuem & Gellersen 2005).

The key point of our approach is that the knowledge associated within the active product is stored and processed within the product itself. Therefore a container is able to know its own status and can perform communication with other containers to make decision on a changing environment or product intrusion. The distributed knowledge base is a good way to solve the problem of variable surroundings appearing in the lifecycle of the chemical products. 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 product to another.

The presented paradigms and research objectives are obviously close to industrial practical needs mainly within the scope of security management covered by the present paper and which is the center topic of the European project FP6 Cobis (Cobis 2008). This pinpoints the need to spend research efforts on both conceptual research activities on concepts and methodologies enhancements and also on development, implementation and testing of artifact solutions, feasibility demonstration and large scale evaluation.

We need a better understanding of the smart objects' capabilities and opportunities to face the research and industrial challenges and we urgently need to define and assess an internal smart object's model and associated implementation structures for evaluation and validation aspects.

The following sections detail our conceptual contribution and practical implementation and evaluation of Active Product concept.

3. SMART OBJECTS PLATFORM

Smart Object development needs some characteristics to be fulfilled. It can memorize its state; it has the ability to sense its environment, to communicate with the surrounding and to react, after taking a decision on its own.

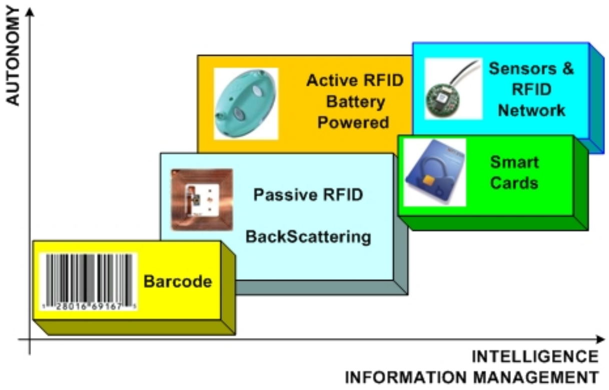

Figure 1: Technologies used to implement a Smart Object

There exist several technologies that present capabilities requested by a Smart Object. In fig. 1 we illustrate our view in the ubiquitous technologies evolution (Bajic et al. 2008). As the Barcode is used to identify the type of a product, using an optical lecture in direct view, the technology has been improved, offering the possibility to save proprietary information in non-volatile memory inside one RFID[2] tag. At present, we dispose of computational and communication capabilities to deliver automatic treatment of the exchanged information by SmartCards and WSN[3].

Our first architecture of Smart Object concept implementation (Cea, Dobre & Bajic 2006) used RFID technologies, to save proprietary information, and UPnP services architecture[4], to attach a bunch of customized services to each physical product that can be requested from any place in the networked architecture as a service-based virtual image of the physical object. The need of a Middleware computer to interact continuously with the RFID tagged object is one inconvenience of the proposed architecture. Also, the computer needs network connection to allow communication between objects. So, the Smart Object represents a virtual representation of the physical object, an informational entity (UPnP Device) able to communicate, interact and to take decisions regarding its state. Using a specialized UPnP Control Point, the user can interact and exchange information to survey and control the Smart Object.

From the five technologies, the one which gives us all desired functionalities is the WSN. One node can survey its near environment, communicate with other nodes and have computational algorithmic behaviors according to perceived information. Examples of WSN nodes are Mica2 produced by Crossbow[5] and pParticle produces by Teco[6] and commercialized by Particle Computer[7].

The project uses the pParticle ver. 2/32 wireless sensor with the full sensor circuit SSimp ver. 2/02. This WSN has been chosen for its capabilities (sensors, computational power, communication speed), which help us to detect all factors influencing the security level. One barrel contains a chemical product and has attached one pParticle device. Within the WSN, the Smart Objects can interact freely, exchanging object-to-object information.

The user-to-object interaction is implemented with Teco's wireless bridge, WBride. The user is exchanging information using a simply PDA with appropriate application.

Next section presents Particle platform by means of hardware devices and communication capabilities.

3.1. Particle device

One Particle device is composed by the Particle base and the sensor module. In fig. 2 we present the two components. The Particle base is the core of the de-

[2] Radio Frequency Identification

[3] Wireless Sensor Network

[4] Universal Plug and Play

[5] http://www.xbow.com

[6] http://particle.teco.edu

[7] http://www.particle-computer.de

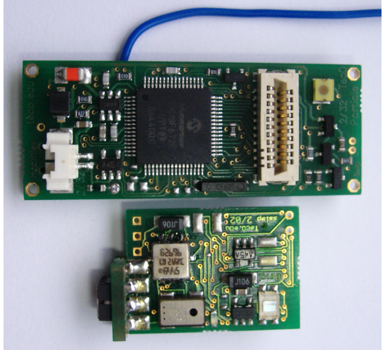

Figure 2: The pParticle 2/32 with SSimp 2/02

vice. Characteristics are presented in table 1. The motivating points are the microcontroller (especially the computational power), the flash memory capacity, in which the Smart Object save security information and rules, and the communication capabilities.

As sensors, the Particle device includes:

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

We use these sensors to create an image of the ambient environment. This way, the product can actively verify its intrinsic security state, reacting to changes affecting its normal storage or handling conditions. Moreover, the voltage sensor surveys the battery life, one of the major problems in WSN.

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 connector
Power regulation	0.9 to 3.3 V
Board core voltage	3.3V
Size	45x18 mm (no battery)
Code	in C, OTAP

In addition, the device includes a RSSI[8] sensor to be used for distance measurement between two devices. 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 the wireless ad hoc customized protocol AwareCon (Beigl, Krohn, Zimmer, Decker & Robinson 2003). Its design follows the fundamentals of the established OSI/ISO layered approach. AwareCon (fig. 3) 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 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 WLAN, 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.

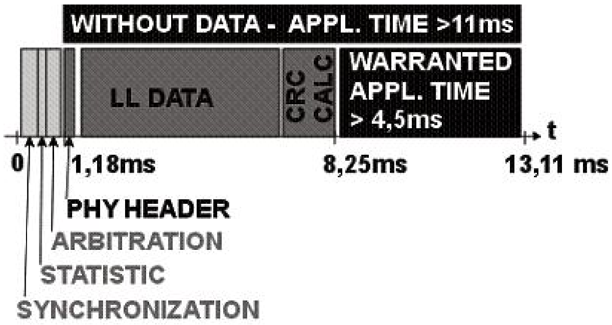

Figure 3: The AwareCon frame structure

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 en-

[8] Received Signal Strength Indicator

able the information exchange between nodes. In the Particle System, the proposed approach is ConCom (Krohn, Beigl, Decker, Robinson & Zimmer 2004), an approach to represent transmitted data as tuples. A tuple is a byte sequence that starts with a type identifier (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, collects data from the environment and process it. Its natural reaction to an environmental threat is an audible and/or visual alarm, in order to alert and announce of an immediate threat the afferent personnel manipulating it. Other reaction can be alarm messages sent to notify the security personnel, with detailed information concerning the cause.

When more products are close, Smart Objects can 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 (fig. 4).

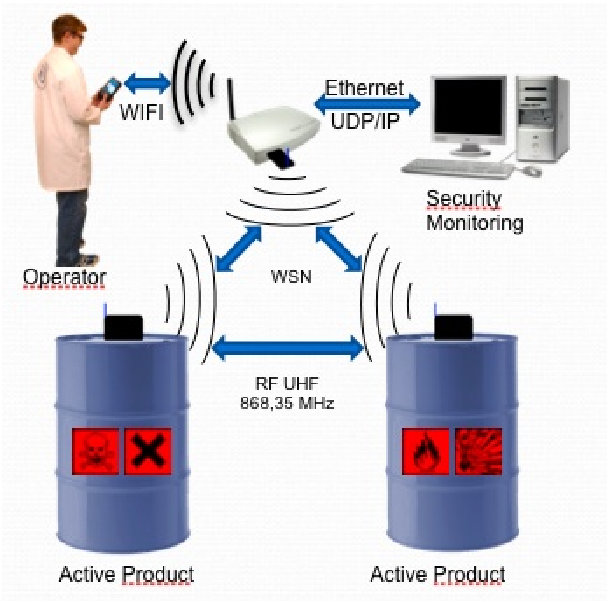

Figure 4: Active products in an Ambient intelligence environment

Object comportment is given by a series of information and rules. At a configuration stage, static information is stored on each product by central monitoring software: substance name, substance ID (from Merck international catalog for chemical products numbering), product's electronic product code (EPC), security phrases and security symbols according to European directives 67/548/EEC (fig. 5). This represents the core information, to uniquely identify the product as a hazardous and commercial item. Other useful information can be saved in product memory according to use case. Supply chain traceability and manufacturer's information are supported by EPC numbering schema and Internet information services support.

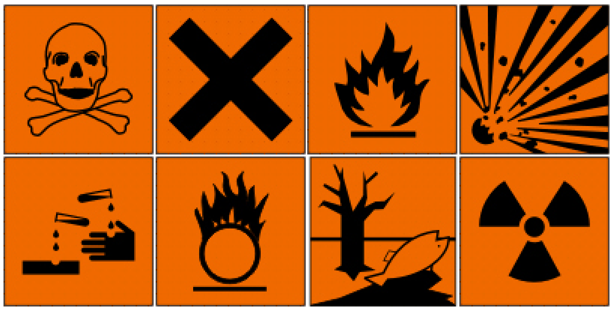

Figure 5: Chemical product security symbols: toxic, irritant, inflammable, explosive, corrosive, oxidant, dangerous for the environment, radioactive

Each product has two security levels: the intrinsic and the extrinsic. The intrinsic security level is dependent of environmental factors (temperature, shocks, etc.) that influence in a direct mode the product. The extrinsic security level is given by the compatibility between chemical substances.

Working or surrounded with hazardous products creates dangerous space where certain ambient and environmental parameters influence the intrinsic security level of each product. Variation of the ambient 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) (fig. 6):

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

The intrinsic security level is processed using sensors data, considering a set of boundaries limits for pa-

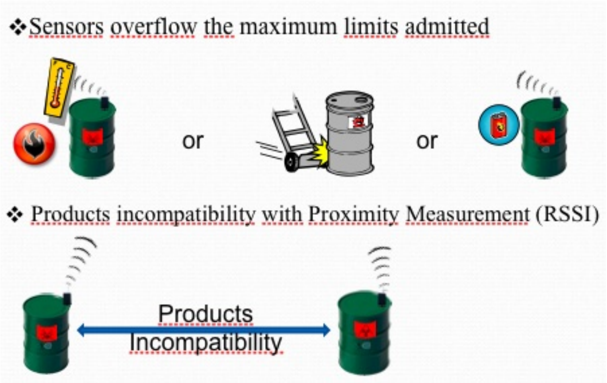
❖Sensors overflow the maximum limits admitted
or
or
❖ Products incompatibility with Proximity Measurement (RSSI)
Products
Incompatibility

Figure 6: Product sensitivity to Ambient characteristics

rameters values. These boundaries represent the security phrases registered in memory. For the temperature value we considered the upper and lower limit. For light, infrared light, audio and acceleration values we used only upper limits. Using the safety data sheet, we can establish the specific value for each limit. Therefore, the smart product determines its internal security level with reasoning, by inference on the sensor's values and boundaries limits.

The extrinsic security level is deducted using the nature and the compatibility agreements given by other products located in the vicinity. A compatibility relationship can be derived from the security symbols, coded in the product static information. Using a compatibility matrix that uses security symbols, we succeeded to determine if two products are compatible or not. 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 products in the vicinity are compatible, and Dangerous, in all other cases.

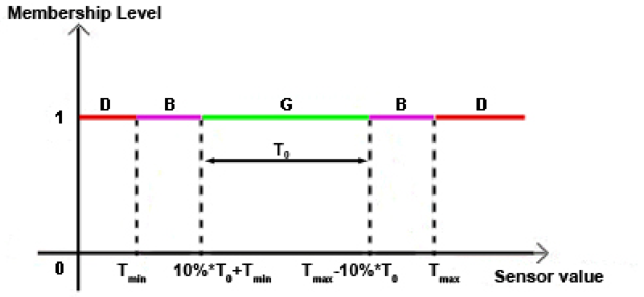

Figure 7: Chemical product security level: Good, Bad or Dangerous

In the active security environment, a Smart Object sends product information: the substance Merck ID and its security symbols. Other Smart Object, receiving the information, calculates the message RSSI value, verifies the compatibility with the first product, using its symbols, and determines 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 (Good), B (Bad), D (Dangerous) where B and D are absorbent states.

Manipulating the Smart Object, the worker receives security information from all barrels around him, allowing to know, in real-time, what is happening in the warehouse and to intervene in case of a problem.

5. SMART OBJECT'S BEHAVIOR FOR SECURITY MANAGEMENT

Each hazardous product, equipped with pParticle device, is transformed into a Smart Object. Its main activity is the security management, based on product's characteristics, limitations rules, security symbols and compatibility matrix, coded as static information. Hazardous product has the ability to monitor its near environment and communicates with other hazardous products or systems.

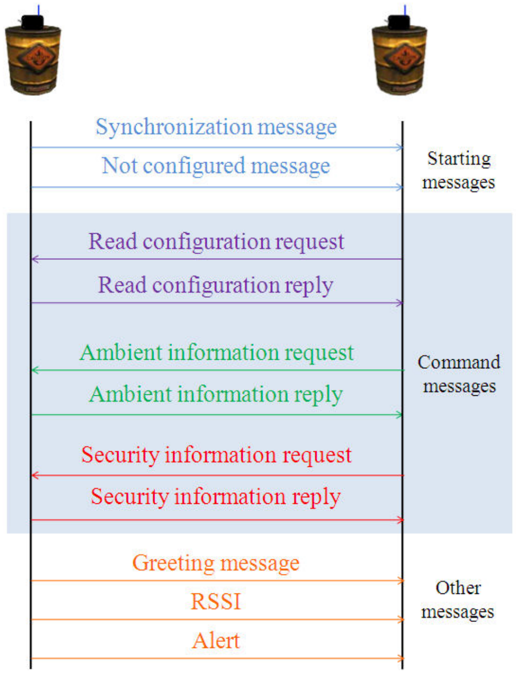

Figure 8: Messages exchanged between Smart Objects

In an AmI application, the main point is human-to-systems interaction. This is why one model must begin with use cases and with scenarios study. Within this study we propose messages that need to be exchanged between a Smart Object and another Smart Object or user application. In fig. 8 we present a sequence diagram containing messages exchanged in our environment.

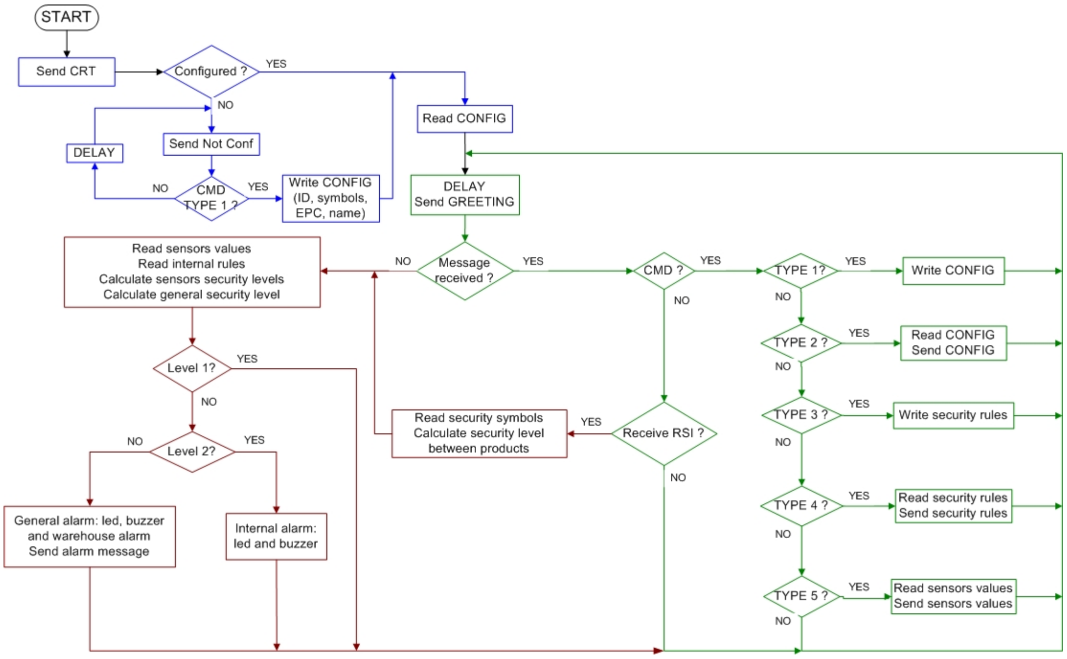
START
Send CRT
Configured ?
YES
NO
DELAY
Send Not Conf
NO
CMD TYPE 1 ?
YES
Write CONFIG (ID, symbols, EPC, name)
Read CONFIG
DELAY Send GREETING
Read sensors values
Read internal rules
Calculate sensors security levels
Calculate general security level
NO
Message received ?
YES
CMD ?
YES
NO
TYPE 1?
YES
NO
Write CONFIG
TYPE 2 ?
YES
NO
Read CONFIG Send CONFIG
TYPE 3 ?
YES
NO
Write security rules
TYPE 4 ?
YES
NO
Read security rules Send security rules
TYPE 5 ?
YES
NO
Read sensors values Send sensors values
Level 1?
YES
NO
Level 2?
NO
YES
General alarm: led, buzzer and warehouse alarm Send alarm message
Internal alarm: led and buzzer
Read security symbols Calculate security level between products
YES
Receive RSI ?
NO

Figure 9: The algorithmic behavior for security management on a Smart Product

There are three message types required to be implemented in our platform:

- Starting messages, used to create a synchronized wireless communication channel, when two or more Smart Objects are close together, or to announce the not configured state of the Smart Object (sent automatically);
- Command messages, used to interact with the Smart Object. These messages are sent in a request-response mode. It includes the reading/writing of configuration and the reading of object's sensor values;
- Other messages, sent automatically by the object, announcing its presence (greeting), to calculate the distance between two objects (RSSI) and to alert in case of a security problem (alert).

Using these messages, we created an internal algorithmic behavior of a Smart Object, illustrated in fig. 9. It is built on three main loops: not configured loop, new message received loop and internal check loop.

In our scenario, a new barrel enters the warehouse. Not being configured, it sends periodically not-configured messages to the supervisor system. This will stop as it receives a configuration. Qualified personnel remotely configure the smart product with suitable information related to the substance inside the barrel. The configuration is composed by product proprietary information and the security rules. This can be done automatically at manufacturing stage in a M2M[9] approach.

After receiving the configuration, the Smart Object enters IDLE state and sends greeting messages. In IDLE state the Smart Object reads all sensors values, calculates the RSSI values for each Smart Object in the proximity and calculates, using these values, a product global security level. The global security level can be good, warning or dangerous. The normal state is the good security level. A product is in this state if all sensors are in a limit of 90% of recorded security limits.

The greeting message is sent in broadcast. As information it contains the substance ID and the product global security level. As no condition monitoring is changing, the Smart Object remains in this state.

When a sensor records more than 90% of security limit, the Smart Object records the value and enters the warning state or security level 2. If it succeeds 100% of the limit, it enters in security level 3 or alarm. In both cases, the smart product sounds an audible alarm and sends alarm messages. Alarm message indicates the sensors out of range. In case of product incompatibility, the message contains the ID of the concerning barrel. As soon as the threat has disappeared, it returns to IDLE state.

All messages are broadcasted (greeting, command and RSSI). They are used for object-to-object or object-to-supervisor communication. The command messages are mainly used by the supervision application to write the Smart Objects configuration, to read the configuration and to monitor the sensors values. The monitoring is the only message sent to a unique object.

[9] Machine to Machine

5.1. RSSI for extrinsic security level determination

For extrinsic security level calculation, RSSI method is used. We estimate the distance with other hazardous products that could worsen the global security level by way of their incompatibility. To easily attach the pParticles devices on industrial chemical containers, we integrated them in conductive ABS plastic boxes. Particle's antenna is left on the outside, so it can be freely tilted to any position. After conducting experiments, with and without 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 particle's antenna orientation. During our experiments we noticed the variation of indications 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 room floor, the signal strength is quite inferior to that when particles are positioned on top of the barrel. This can limit the detection of one barrel fallen on the ground.

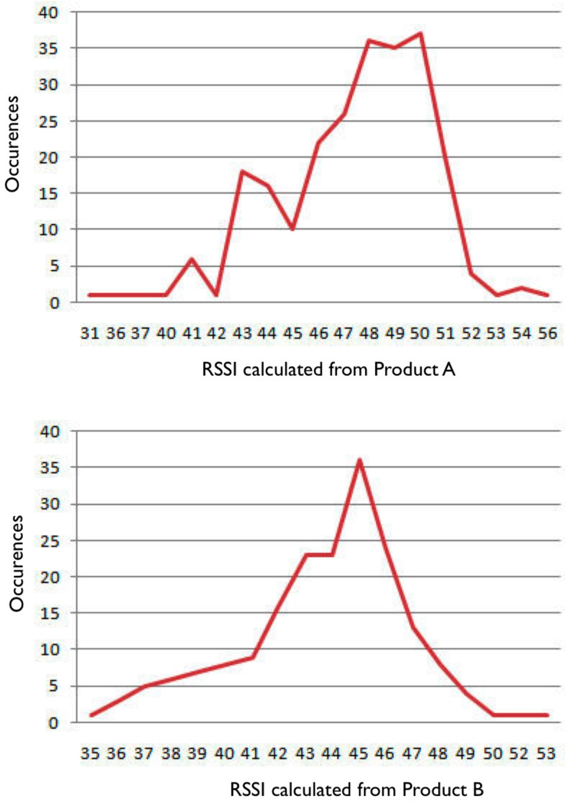

Figure 10: RSSI measurements distributions

RSSI level is obviously conditioned by the batteries charge level. Therefore, transmission signal strength must be accorded consequently. Moreover, the signal strength becomes a real problem when obstacles are positioned between the smart products. For example, paperboard boxes extend the interval between consecutive RSSI measurements, but the electronic devices act like a screen and disturb completely the communication.

An important issue is that not all particles receive the same RSSI value for a given distance. Even though the circuit is the same, an experiment with two particles has shown that the average RSSI measurements over a period of time differ substantially for the two devices. Fig. 10 shows the distribution functions of RSSI measurements for two Smart products A and B, at a distance of 1m from each other. The measurement is asymmetric, as one particle indicates an average RSSI of 43.70 and the other 47.41.

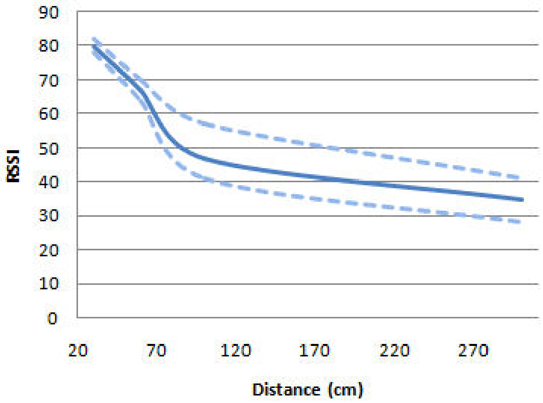

Figure 11: RSSI measurement for products distance evaluation

During our experiments, we have found relevant indications of the RSSI for distances up to 3 meters. This distance is appropriate to define a security bubble around a product. For longer distances, RSSI messages were becoming either too scarce or completely absent. Fig. 11 reveals the RSSI indications at various distances and the standard deviation tube.

6. CONCLUSION

Our contribution in the presented work aims at responding to both conceptual and practical objectives of Active Security Management supported by interactive Smart Products. Conceptual aspect is covered with the proposal of the Active Product concept along with smart objects interaction architecture. An internal behavior model of an Active Product, supported by a generic algorithm, is proposed to perform security management over a surrounding community of products. Practical contribution is given with the implementation and evaluation of Smart-its platform for validation of Active Product capabilities, which show the limits and current uncertainties of the Ambient Intelligence technology.

Providing 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 adaptive security-oriented behavior. Proactive alarm and preventive actions can be embodied in each hazardous product to prevent a catastrophic situation in chemical areas.

Our model for a smart product's internal behavior, dedicated to security management, defines the concept of an Active Security Distributed Management System. Both theoretical and technological gaps are still outstanding: product on-board energy saving, robustness of product's behavior in large scale community, refinement of internal product behavior model to allow adaptability and reconfigurability in different use case scenarios, outside security domain. We will deeply investigate the monitoring of the product's extrinsic security by the cooperation with distant products.

References

Alcañiz, M. & Rey, B. (2005). New technologies for ambient intelligence, *in* G. Riva, F. Vatalaro, F. Davide & M. Alcañiz (eds), *Ambient Intelligence*, IOS Press, pp. 3–15.

Bajic, E. (2005). Ambient services modelling framework for intelligent products, *Smart Object Systems, UbiComp 2005*, Tokyo, Japan, pp. 83–90.

Bajic, E., Cea-Ramirez, A. & Dobre, D. (2008). Service modeling for smart objects in the supply chain using rfid and upnp technologies, *in* T. Blecker & G. Q. Huang (eds), *RFID in Operation and Supply Chain Management*, Vol. 6 of *Operations and Technology Management*, ESV, pp. 91 – 118.

Beigl, M., Krohn, A., Zimmer, T., Decker, C. & Robinson, P. (2003). Awarecon: Situation aware context communication, *Ubicomp 2003*, Seattle, USA.

Cea, A., Dobre, D. & Bajic, E. (2006). Ambient services interactions for smart objects in the supply chain, *IEEE Service Systems and Service Management*, Troyes, France.

Cobis (2008). Collaborative business items, *Technical report*, www.cobis-online.de.

European-Community (1967). Council directive 67/548/eec on the approximation of laws, regulations and administrative provisions relating to the classification, packaging and labelling of dangerous substances, *Official Journal of the European Communities*, Council Of The European Economic Community, pp. 196–199.

European-Community (1991). Commission directive 91/155/eec defining and laying down the detailed arrangements for the system of specific information relating to dangerous preparations in implementation of article 10 of directive 88/379/eec, *Official Journal of the European Communities*, Council Of The European Economic Community, pp. 35–41.

Fisher, K. (1999). Agent based design of holonic manufacturing systems, *Robotics and Autonomous Systems*, Vol. 27, Elsevier Science, pp. 3 – 13.

Gershenfeld, N. (1999). *When Things Start to Think*, Henry Holt & Company.

Holmquist, L., Gellersen, H., Schmidt, A., Strobach, M., KOrtuem, G. & Beigl, M. (2004). Building intelligent environments with smart-its, *IEEE Computer graphics and applications*, Vol. 24, pp. 56–64.

Kintzig, G., Poulain, G., Privat, G. & Favennec, P. (2002). *Objets Communicants*, Hermès, France.

Krohn, A., Beigl, M., Decker, C., Robinson, P. & Zimmer, T. (2004). Concom - a language and protocol for communication of context, *Technical report*, TecO. ISSN 1432-7864 2005/19.

McFarlane, D., Sarma, S., Lung, C. J., Wong, C. & Ashton, K. (2002). The intelligent product in manufacturing control and management, *15th Triennial IFAC World Congress*, Barcelona, Spain.

Remagnino, P. & Foresti, G. (2005). Ambient intelligence: A new multidisciplinary paradigm, *IEEE Transactions on Systems, Man and Cybernetics, Part A*, pp. 1– 6.

Strohbach, M., Kortuem, G. & Gellersen, H. (2005). Cooperative artefacts - a framework for embedding knowledge in real world objects, *Smart Object Systems, UbiComp 2005*, Tokyo, Japan, pp. 91 – 99.

Weiser, M. (1991). The computer for the 21st century, *Scientific American 265* **3**: 94 – 104.

Wong, C., McFarlane, D., Zaharudin, A. A. & Agarwal, V. (2002). The intelligent product driven supply chain, *IEEE SMC*, Hammamet.