

# WSAN4CIP

## Deliverable 6.3

### Final Plan for using and disseminating knowledge

Editor:	Jens-Matthias Bohli, NEC
Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	PU
Contractual delivery date:	31/12/2011
Actual delivery date:	31/12/2011
Suggested readers:	Stakeholders in the Sensor and Critical Infrastructure Business
Version:	1.0
Total number of pages:	40
Keywords:	Dissemination, exploitation

---

#### *Abstract*

This document presents the final exploitation plans of the WSAN4CIP consortium. The main exploitable results of the project are presented and a path to their exploitation is described. Finally, a detailed per partner exploitation plan is listed, showing the concrete steps initiated by each member of the consortium. The exploitation plans are an update from Deliverable D6.2. The second part of the deliverable lists the dissemination activities by the consortium. Both internal dissemination to spread findings in order to ensure further exploitation of the results for business or research purposes, and dissemination to a broader public audience are covered. The dissemination activities are summarised in a dissemination table.

---

---

**Disclaimer**

---

This document contains material, which is the copyright of certain WSAN4CIP consortium parties, and may not be reproduced or copied without permission.

All WSAN4CIP consortium parties have agreed to full publication of this document.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the WSAN4CIP consortium as a whole, nor a certain party of the WSAN4CIP consortium warrant that the information contained in this document is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using this information.

**Impressum**

[Full project title] Wireless Sensor Networks for the Protection of Critical Infrastructures

[Short project title] WSAN4CIP

[Number and title of work-package] WP6 Dissemination and Exploitation

[Document title] Final Plan for using and disseminating knowledge

[Editor: Name, company] Jens-Matthias Bohli, NEC

[Work-package leader: Name, company] Jens-Matthias Bohli, NEC

[Estimation of PM spent on the Deliverable] 7 PM

**Copyright notice**

© 2011 Participants in project WSAN4CIP

## **Executive summary**

This document presents the final exploitation plans of the WSAN4CIP consortium. The main exploitable results of the project are presented and a path to their exploitation is described. Finally, a detailed per partner exploitation plan is listed, showing the concrete steps initiated by each member of the consortium. The exploitation plans are an update from deliverable D6.2. The second part of the deliverable lists the dissemination activities by the consortium. Both internal dissemination to spread findings in order to ensure further exploitation of the results for business or research purposes, and dissemination to a broader public audience are covered. The dissemination activities are summarised in a dissemination table.

## List of authors

Company	Author
BUTE	Levente Buttyan
IHP	Peter Langendörfer
INOV	Augusto Casaca
INRIA	Claude Castelluccia
LTU	Evgeny Osipov
NEC	Jens-Matthias Bohli
Sirrix	Marcel Selhorst
TECNATOM	Jose Luis Serrano
UMA	Daniel Garrido

## Table of Contents

Executive summary .....	3
List of authors.....	4
Table of Contents .....	5
1 Exploitation plan .....	7
1.1 General approach .....	7
1.2 Exploitation roadmap.....	10
1.3 WSAN4CIP Workshops .....	11
1.3.1 Lisbon 2010 .....	11
1.3.2 Grenoble 2011 .....	11
1.3.3 Lulea 2011 .....	12
1.4 Standardisation Activities .....	12
1.4.1 Relevant standardisation bodies.....	12
1.4.2 Activities of WSAN4CIP.....	14
2 Individual partner plans and exploitable items.....	16
2.1 Industrial / Solution providers.....	16
2.1.1 NEC .....	16
2.1.2 Sirrix .....	17
2.1.3 TECNATOM.....	17
2.2 Academic / Research institutes .....	18
2.2.1 INRIA .....	18
2.2.2 IHP.....	18
2.2.3 INOV .....	19
2.2.4 BME.....	19
2.2.5 LTU.....	20
2.2.6 UMA.....	20
2.3 End-users.....	20
2.3.1 FWA .....	20
2.3.2 EDP.....	21
2.4 Exploitable results and WSAN4CIP technology differentiator .....	21
2.4.1 Overview of exploitable results .....	21
2.4.2 Advanced node configuration.....	22
2.4.3 Key exchange for bootstrapping.....	22
2.4.4 Secure code update .....	22
2.4.5 Advances in MAC layer .....	23
2.4.6 Advances in routing protocols .....	23
2.4.7 Advances in transport protocols .....	23
2.4.8 Secure OS .....	24
2.4.9 Advances in service protection.....	25
2.4.10 CIP WSAN management.....	25
3 Dissemination activities .....	26
3.1 Website .....	26
3.2 Flyer .....	28
3.3 Media Releases .....	28
3.4 Project Presentations .....	28
3.5 Conference, Journal and Magazine Publications .....	30
3.6 Eurescom Mess@ge.....	35
3.7 Internal dissemination activities.....	35
3.8 Concertation and Clustering Activities .....	36
3.9 Summer School on Network and Information Security .....	36
Annex A .....	37
A.1 Media Releases .....	37
A.1.1 February 2010.....	37
EU researchers develop cost-effective infrastructure protection - Press release, 2 February 2010 -.....	37
A.1.2 December 2011 .....	38

EU research project WSAN4CIP has demonstrated a cost-effective solution for protecting electricity and water networks ..... 38

A.2 WSAN4CIP Flyer ..... 40

# 1 Exploitation plan

In this section, we introduce the consortium exploitation plan. After introducing our methodology, we present an exploitation plan by partner type, such as academic or research institute. We then list the exploitable technological items of WSAN4CIP, as well as a few approaches how to ensure their exploitation, such as standardisation or dissemination of our result.

## 1.1 General approach

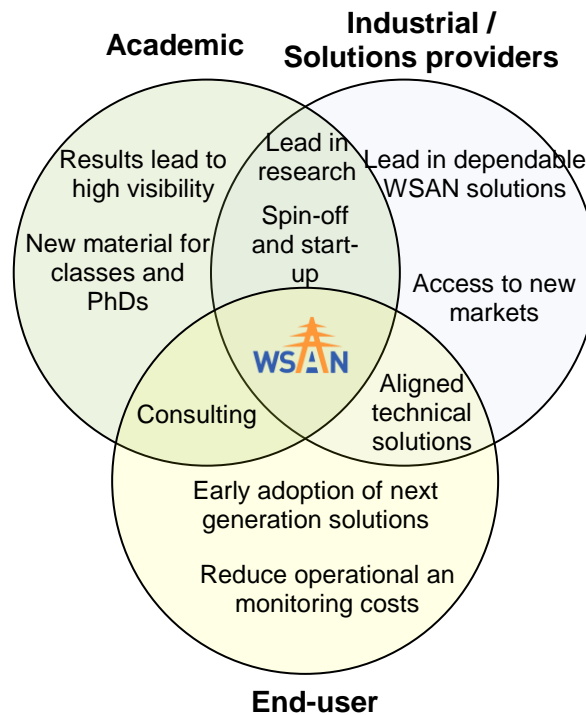
An exploitation plan contains partners' ideas about how to use the project results at local, regional, national, European, and/or international levels. When talking about results, we mean all the productions from the WSAN4CIP project, whether they are tangible or intangible.

We followed a mixed approach for developing the exploitation strategy. Thus we:

- Asked partners about their ideas and individual plans for the exploitation of the WSAN4CIP products or results. Each partner was asked to evaluate the possible exploitation of the projects results, and provide means to achieve their exploitation plan.
- Identified some differentiators in the sector/topic that WSAN4CIP is dealing with. This sector is the use of wireless embedded system for monitoring large scale infrastructures. WSAN4CIP made further innovations for protocols and software compared to the prior art. Those differentiators and exploitable results are discussed later.
- Investigated other sectors where results of WSAN4CIP could have a significant impact. For example, automation industry is keen on dependable sensor technologies.
- Studied the missing gaps between our demonstrator prototypes and a commercial product. These gaps are keys to understand what an end-user still needs to adopt WSAN technologies for monitoring their critical infrastructure.

We adopted an active approach by identifying the most attractive opportunities for exploitation and then planning to investigate these opportunities.

We can qualify the partners of the projects into 3 categories: academic, industrial/research institute, and end-users. Each of those partners has different interests in the exploitation of the results of the project. We describe in the figure below the general interests of those actors.



**Figure 1: Overview of the WSAN4CIP actors and their exploitation.**

#### ***Academic / Research Institutes:***

The goals of academic partners (i.e., universities and research institutes) aim at keeping a leading edge in technical developments. Those developments will be integrated quickly into the teaching curricula and research agendas, giving themselves as well as their graduates a competitive edge. Academic partners will also make sure that these developments are carried into future national and international research projects, deeply rooting WSAN4CIP results in research and development activities. By publishing high-quality papers about the WSAN4CIP results, academic partners will obtain improved international visibility and improve their position in attracting the best international PhD, Master and graduate level students to their institutions. To spread WSAN4CIP approaches widely among the academic and engineering networking community, academic partners will also exploit the project results to organise tutorial-style and research seminar-style summer schools of high academic standing. The academic exploitation of strategic guidelines naturally has a longer time horizon. We will prepare the future research agenda based on the WSAN4CIP results and identify new problems which have to be solved to strengthen the WSAN4CIP impact even more. Academic partners are also tasked with preparing the workforce for the future technological landscape, both for direct work in industry and for research – this development will be particularly important for SMEs who are often not themselves able to train personnel in these new networking technologies.

#### ***Industrial/ Solutions providers:***

Our industrial partners can exploit direct technical improvements internally. The reliability and security solutions developed in WSAN4CIP can be integrated into current and new products. A manufacturer can use the acquired know-how to shorten turn-around times from the project results to products –to reduce time to market and improve its business position or to outperform competitors through the quality of immediately forthcoming new products. Manufacturers can introduce a range of next generation monitoring solutions, automation and security applications faster than their competitors. We will ensure this by transferring results from the research departments of our industrial partners directly to development, products, marketing, and maintenance departments. The right of a partner to decide to protect some of its results before any kind of dissemination of such result and the mostly open source based dissemination of other results will be a strong support for the industrial partner's internal exploitation.



Industrial partners can also exploit direct technical improvements externally. The prime objective here is to create new products and services for already existing or currently incipient markets. WSAN4CIP partners will be better prepared for new markets, products, and services and can position themselves early on. To achieve this, tutorials can be organised at specialised fairs such as SPS in Nuremberg. We achieve these exploitation goals by educating the customers and business relations of our industrial partners about the new technical possibilities and by developing attractive offerings. We also intend to provide our results to forthcoming test-bed projects to ensure early adoption of our approaches within the CIP research community as a solid foundation for future European and world-wide research.

The project will also influence internal strategic guidelines, which will allow our partners to advance preparation for new business models and business roles and is a key strategic opportunity for the longer-term development of their business both in Europe and globally. For example, there will be a huge deployment of sensor related technologies in the near future, with the commoditisation of M2M and Internet of Things products. WSAN4CIP partners will be well-prepared to exploit these opportunities – for example, by becoming solutions provider, combining operation and design expertise. It will also become possible for our partners to start up dedicated companies for such new business models. In addition, training for sales personnel, field engineers, etc., can be started early, thus bringing an advantage over the competition. Overall, being aware of future strategic developments allows our consortium partners to embrace new usage scenarios and to prepare technical solutions, rather than being overwhelmed by them. In the long run, this will lead to new business opportunities for our partners. The manufacturers will be well positioned for serving this new demand in a market that is not only shifted but also enlarged.

In line with these exploitation activities, we will use strategic results to create new markets and new business opportunities, foster new customer relationships, and create new, competition-friendly, highly efficient, unbundled technological structures. We will present those results to external industrial partners, by demonstrating our results in fairs and technical conferences. To ensure deep dissemination of our projects, we have organised vendor workshops during our meeting with targeted companies, which can pick up results of WSAN4CIP or create new business relationships with partners of WSAN4CIP to create new solutions. Those vendors furthermore provide feedback to the project partners, thus the consortium can react quickly to new trends.

#### ***End-users:***

By being a lead user in the adoption of WSAN technologies, our end-user partners can participate in the requirements and design of solutions that are adapted to their need. WSANs offer to reduce operational costs, allowing utilities to become more competitive, while ensuring a better availability of their infrastructure. Utilities have to face new challenges, such as new business like smart grids, while facing new dangers, e.g. new forms of vandalism and terrorist threats. WSANs are part of the solution to address those future challenges.

WSAN4CIP can let the end -users evaluate the benefits of the technology on a small scale, thanks to the two demonstrators. Based on the results, the next steps of exploitation can be drawn. The gaps identified in the demonstrators can be filled, such that larger deployments of WSAN technology can be made. Finally, once the technology is mature enough, the technology can be deployed in a production environment. WSAN4CIP also allows end-users to create strong relationships with partners of the projects, which may useful for further development of products and concepts. Furthermore, through the organisation of vendor workshops, new business contacts can be made.

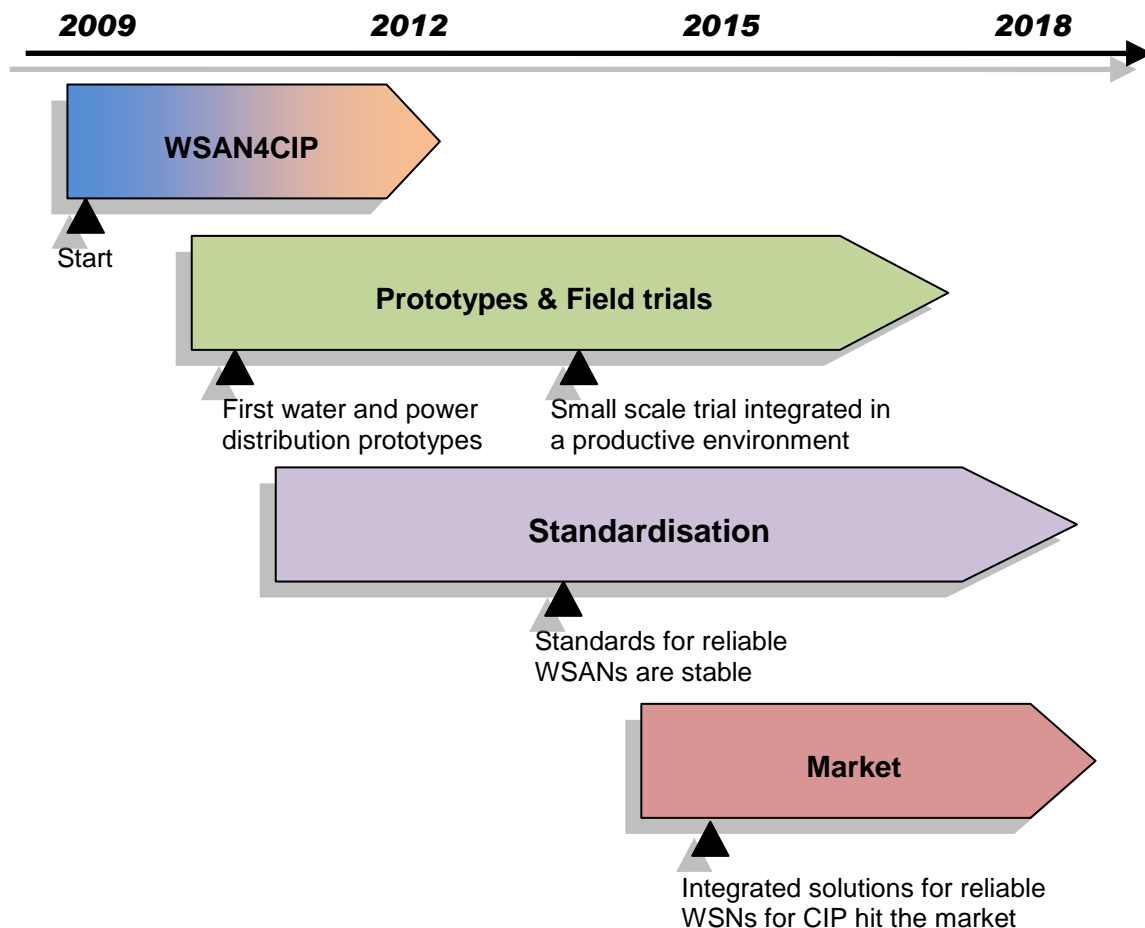
The internal exploitation also consists to train and raise awareness of WSAN4CIP of the key personnel of the companies. Hence, the WSAN4CIP end-users will have a competitive advantage by having adopted early WSANs solutions, and have already adapted their operations and business strategies to successfully integrate them.

## 1.2 Exploitation roadmap

WSAN4CIP started in 2009 with the objective of advancing the state of the art in reliability and availability of wireless sensor networks. A first important milestone for exploitation is the deployment of sensors in the field mid-2011, which can help to identify gaps to real products.

Further projects will improve over the results of WSAN4CIP and close those gaps over the next coming years. The lessons learned in WSAN4CIP will be a great basis for those future prototypes.

Once the standards are established and stable, the market can move from a very specialized and fragmented market to more interoperable and off-the-shelf solutions, where the end-users could truly profit from competition.



The standardisation activities of partners that are related to WSAN4CIP are listed in Section 1.4. WSAN4CIP results are already influencing products of WSAN4CIP partners. Sirrix' TURAYA security kernel will be improved based on WSAN4CIP results. TECNATOM is also continuing development of a monitoring solution that is building on the SCADA integration and security components from WSAN4CIP. IHP is planning a spin-off company in the domain of wireless systems for water infrastructure, which will strongly exploit the experiences and results of WSAN4CIP.

## 1.3 WSAN4CIP Workshops

WSAN4CIP has organised since the second half of the project small workshops with vendors, solutions providers, end-users and academia in order to disseminate results from the project and get valuable feedback from market players. WSANs are recognised as a valid approach to reduce cost of operations while increasing the amount of data collected from the monitored infrastructure. Those meetings also allow creating or reinforcing business contacts, which can be useful for future collaboration.

### 1.3.1 Lisbon 2010

The first workshop was held in Lisbon in November 2010 with the following companies: Tecnilab, Efacec, and Siemens. Short notice apologies were received from ABB who had already confirmed participation. The agenda included

- WSAN4CIP project overview
- Trustworthy code execution in Embedded Devices
- Presentations from Tecnilab, Efacec and Siemens regarding their product portfolio and current R&D activities
- Overview of the WSAN4CIP field demonstrators.
- Node protection with large scale support based on the TURAYA security kernel.
- Secure multi-hop networking in constrained environments with Routing Protocol for Low power and Lossy Networks.



**Figure 2: Participants at the Lisbon Workshop.**

### 1.3.2 Grenoble 2011

The second vendor workshop was held in Grenoble in conjunction with the WSAN4CIP general meeting on 19 May 2011. The vendor workshop had the topic "Security and Privacy for Embedded Devices in Critical Systems" and guest from CEA, SorinGroup and Laboratoire d'Informatique de Grenoble attended and contributed. WSAN4CIP partners demonstrated and presented project results to the guests, followed by presentations of the guests to learn about their ideas and needs. The detailed agenda was as follows:

- 13:00-13:30 WSAN4CIP Project presentation
- 13:30-15:00 WSAN4CIP Project Results
- 15:30:17:00 Invited talks

### 1.3.3 Luleå 2011

The third workshop of the WSAN4CIP project was organized by LTU, Luleå University of Technology on September 14th, 2011.

Amongst the invited guests were present a head of water distribution department at Luleå municipality, representatives from the Swedish railroads authority responsible for technical operation of IT infrastructure, the head of CDT, the research and Development center at Luleå University of Technology, a chief Technical Officer at BahavioSec AB.



**Figure 3: Guests at the Luleå Workshop**

The workshop was organized in a form of panel on topic "Large Scale Trustworthy Distributed IT Systems: Academy and Industry perspectives". with demonstrations of project's research results from WSAN4CIP. The workshop continued in an open and productive atmosphere. The invited guests presented the needs for secure solutions in the respective operation domains. They also pointed out a clear need in more intensive knowledge transfer between the research projects and the industry which would supply integrated solutions to the final customers. As results of the workshop several contacts between the invited industry and the project's partners were established. Luleå University of Technology thank all the attendees of the workshop for open and productive discussions.

As result of this third workshop a dialogue could be established between the Luleå water distribution department and IHP, which eventually contributed to a first business plan for a spin-off company planned at IHP.



**Figure 4: Discussions at the Luleå Workshop.**

## 1.4 Standardisation Activities

### 1.4.1 Relevant standardisation bodies

There is a large number of standards which are relevant to the WSAN4CIP project. With the rise of the Internet of Things, new standards and working groups have been established to define future WSANs interfaces. There is an evolution from rather closed, application oriented standards (e.g. Z-Wave) to fully open and large-scale standards such as IETF 6lowpan and IETF ROLL.

As the requirements for the WSNs applications can be extremely diverse, there is obviously no standard that will win the overall WSN market. For each of the market segments, one of the standards will stand out in front of its competitors. For example, in personal area networks, Low-Energy Bluetooth has a strong advantage because of the widespread usage of Bluetooth enabled handhelds. Adopting Bluetooth sensors can be therefore seen as more efficient, due to an easier market penetration. In other scenarios, requirements such as reliability or transmission delay might rule out generic standards. Critical infrastructures are probably going to adopt similar standards as the ones for wireless factories. However, even in that sector, many standards are competing, such as: WiFi, Bluetooth, ZigBee, WirelessHART, and ISA100.11a.

In standards related to protocols for communication within the WSNs, there are mainly three standardization bodies: IEEE, ZigBee Alliance and IETF. IEEE specifies physical and MAC layers for low-power devices in the 802.15.4 WG. Also, there is interest in the 802.11 group in getting a part of the M2M market by bringing low-power WiFi nodes. In WSN4CIP, this is an interesting evolution, 802.11 platforms are used in the EDP demonstrator. The higher radio power and wider bandwidth allows application like video streaming on a large distance.

The ZigBee Alliance is specifying the network by providing a ZigBee stack on top of the 802.15.4 layers. There are several ZigBee profiles, which are adapted to the application requirements. To name a few, there are the Smart Energy profile which relates to smart metering applications, home automation profile, or the telecommunication profile, which aims at bringing ZigBee on mobile personal devices. At first, ZigBee did not consider bringing the IP protocol to the WSNs itself, but recently ZigBee announced the desire to adopt IP protocols into future ZigBee specifications, adopting IETF ROLL and 6lowpan standards. Those IETF working groups focus on the adaptation of IPv6 over networks of low-power embedded devices, such as IEEE802.15.4 nodes. One can also note the recent working group CoRE, which develops an application layer to expose a RESTful interface at the sensor nodes. The goal is to let the resources of WSNs universally accessible from the World Wide Web. Last but not least, ISA100.11a and WirelessHART are two important standards developed by industrial consortia, and will have a definitive place in the industry of automation and wireless factories.

NEC is a member of the ZigBee alliance. It participated actively in the Over-the-Air Upgrade working group, which defined the requirements and interfaces for a reprogramming tool for ZigBee nodes. The contribution of WSN4CIP consisted in defining the security requirements.

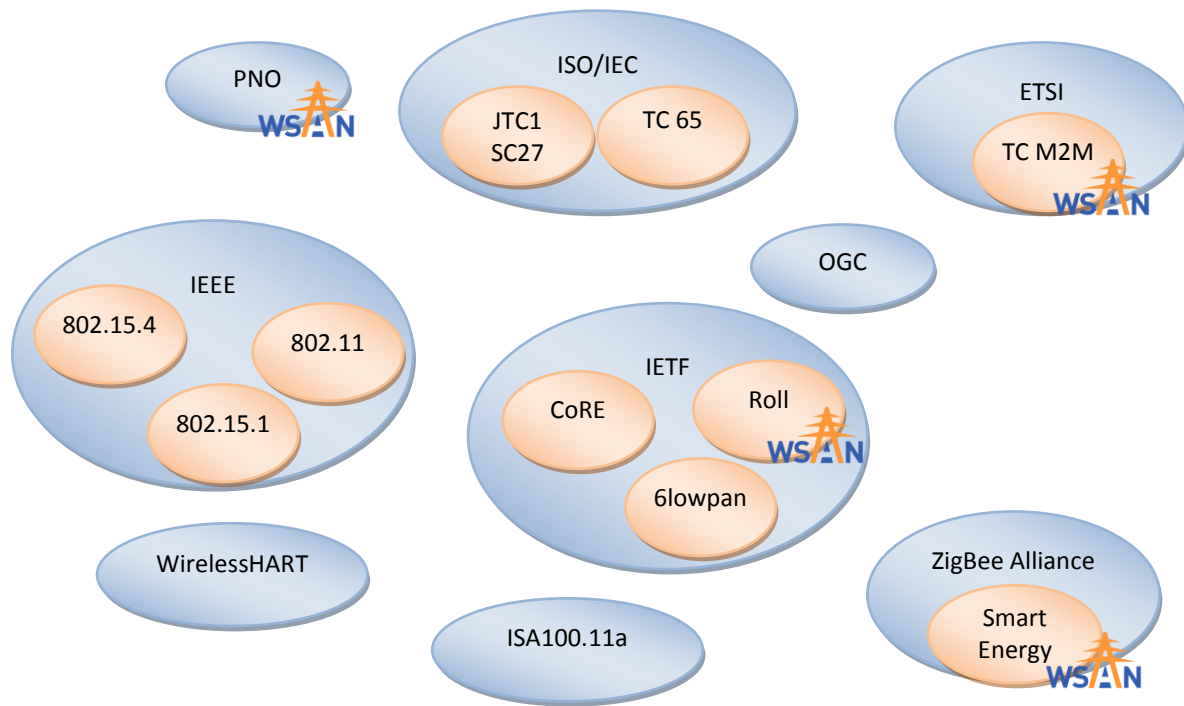
It is expected that RPL will be an important protocol in the future Internet of Things landscape. It might become the standard routing protocol for low-energy mesh networks. As we see it as strategically important, BME is contributing with a draft to provide security extensions to RPL. By also adopting early the standard, we make sure that WSN4CIP solutions are built upon protocols of tomorrow, and thus will not be outdated before soon.

The work of WSN4CIP focuses intensively on the “last mile”, where we defined the protocols and services running at the WSNs. However, if a robust system integration of the resources represented by the WSNs is desired, it is worth considering the following standardisation bodies.

To handle sensor data, the Open Geospatial Consortium (OGC) defines the mark-up language SensorML to describe sensor resources and processes. It also defines a family of specifications regrouped in SWE (Sensor Web Enablement) that enables the query of sensor networks distributed on a large scale.

WSN4CIP applications can also be seen as a machine-to-machine (M2M) use case, and therefore the ETSI M2M standardization committee is of relevance. It aims at developing an end-to-end *M2M architecture, filling the gaps of existing standards*. NEC is active in ETSI M2M, and will work on context processing in that standardisation body.

To conclude, most standardisation bodies have a 2-3 year lifecycle from the first consideration of a work item to a finalised specification, the identification of relevant bodies is a continuous process of monitoring and adaptation. Figure 5 shows the bodies that WSN4CIP is monitoring or has been active.



**Figure 5: Standardisation bodies relevant to WSAN4CIP. Active participation of WSAN4CIP is indicated by a logo.**

## 1.4.2 Activities of WSAN4CIP

### 1.4.2.1 IETF

In January 2011, the Internet-draft “Extension of Security Services” has been submitted to the IETF working group Routing Over Low power and Lossy networks (RoLL). The draft is written by A. Dvir, T. Holczer, L. Dora and L. Buttyan from the Budapest University of Technology and Economics (BME):

- Dvir, T. Holczer, L. Dora, L. Buttyan,  
Version Number Authentication and Local Key Agreement,  
Internet Draft, January 14, 2011

The draft describes security improvements for the Routing Protocol for Low power and Lossy Networks (RPL) that were developed in WSAN4CIP. The draft has been presented at IETF #80 in Prague and received a positive feedback from the workinggroup. Based on the feedback, a new draft has been submitted. The new draft focuses on the routing specific security extensions Version Number and Rank Authentication:

- Dvir, T. Holczer, L. Dora, L. Buttyan,  
Version Number and Rank Authentication for RPL,  
Internet Draft, July 14, 2011.

The updated draft will be presented will be presented at IETF-83 which takes place in Paris March 2012.

### 1.4.2.2 ZigBee Alliance

Participation to the ZigBee Alliance plenary meeting, Dublin, February 2009

WSAN4CIP contributed to the Market Requirement Document of the Over-The-Air Upgrade task group in the ZigBee Alliance. It was made a requirement that code images sent to the WSAN must be signed in order to be successfully verified by the individual node.

### 1.4.2.3 ETSI M2M TC

WSAN4CIP applications can also be seen as a machine-to-machine (M2M) use case, and therefore the ETSI M2M standardization technical committee is of relevance. It aims at developing an end-to-end M2M

architecture, filling the gaps of existing standards. NEC is active in ETSI M2M, and will work on sensor data processing in that standardisation body.

#### **1.4.2.4 PNO**

Presentation by Steffen Peter, IHP, on Wireless sensor networks for factory and process automation including security issue to PNO (Profibus Nutzer Organisation), July 2009

We presented security requirements related to the application of WSANs for automating critical processes at a meeting of the German standardisation body PNO.



## 2 Individual partner plans and exploitable items

We list the individual exploitation plans of the WSAN4CIP partners. They are an update of the exploitation plans presented in the description of work of the project. Since the time of the proposal, the partners have a better understanding of which result can have a significant impact for their internal strategy. Thus, their plan can change accordingly to their analysis of the results.

### 2.1 Industrial / Solution providers

#### 2.1.1 NEC

NEC has the unique advantage to be both an advanced communication solution and IT solution provider. Its strategy focuses on providing cloud solutions for the future, as an enabler for various applications. NEC has stakes in all the parts of the M2M value chain: from sensor hardware to service platforms via IT servers and middleware platforms. Hence, developing the sensor sector and acquiring IPR on it is of strategic value for NEC. NEC Laboratories Europe (NLE) is NEC's European R&D laboratory and focuses on the needs of NEC's European customers. NLE is active in research, technology development and standardisation.

Wireless Sensor and Actuator Networks are a key technology in the next decade for numerous services especially in M2M related areas. NEC is a supplier of security systems for the protection of infrastructures. This includes broadcasting systems, artificial satellites and integrated CCTV surveillance systems for airports and governments, as well as other security-related systems that enhance public safety and security. These systems clearly benefit from the integration of reliable WSANs. Besides critical infrastructures, other promising application areas are found in a smart city environment: eHealth including Ambient Assisted Living, smart grids and energy management, or intelligent transport systems, to name just a few of them. Reliability of WSANs will play a key role and WSAN4CIP results are expected to contribute to the development of reliable system solutions. In the following we give a short qualitative analysis how WSAN4CIP results can be exploited for NEC and its subsidiary.

NEC as provider of WSAN hardware and solutions

NEC group company, NEC Engineering Ltd., develops the ZB24FM-Z family of embedded modules, which are certified by the ZigBee Alliance. The modules can be equipped with sensors and integrated in various solutions such as facility management or energy management in conjunction with smart meters. WSAN4CIP solutions for node protection, e.g. code attestation or secure code update, will improve the management tools that are regularly distributed with hardware packages. The code update solution developed at WSAN4CIP offers clear advantage in dense and lossy environment, such as in the building automation sector. The fountain code can transmit the code fast, which can in turn provide the end-user a higher level of satisfaction. The distributed data storage has interesting applications, especially when it comes to auditing. If sensors had to be used in critical applications, it can provide an interesting tool for post-accident investigation, and more remarkably if there are important network failures in the CI, or in any other WSN related applications. Concealed network coding provides additional confidentiality for free in a scenario where network coding is used.

NEC as provider of management and service platforms

While it is not the main focus of WSAN4CIP to connect the WSAN to a broader architecture, progress in that direction has however been made in Task 4.4. NEC believes that the project results can be used for various M2M scenarios, where the requirements on the WSAN are set high. NEC's BitGate cloud service platform does currently integrate data from RFIDs, but in the long long-term an extension to WSANs will be important. Also NEC has been involving in a number of energy-related projects making use of WSAN. Acquiring reliable and secure data will be key in most applications in the future.

Other advances in WSAN4CIP offer interesting perspective for the future. The incorporation of WSAN management in the M2M framework, the incorporation of RPL routing in the prototypes, the secure micro-kernel on embedded systems, are all interesting elements that can foster future research at NLE. Although NEC did not contribute to those advances in WSAN4CIP, monitoring and understanding those technologies can be of great value for further development in wireless embedded systems.



NEC is participating in M2M standardisation, e.g. in ETSI M2M and 3GPP SA3. The focus is on areas where product development is already further advanced than on WSAN4CIP related technologies.

### **2.1.2 Sirrix**

Sirrix is one of the technology leaders in trustworthy operating systems. While operating systems for safety critical applications, such as in avionics and defence systems, are subject to in-depth analyses regarding security and safety considerations (e.g., based on the Common Criteria), current operating systems for WSAN lack in providing essential security properties and functions. On the other side, Sirrix expects these security properties to be crucial for providing reliable services within a WSAN infrastructure and especially with regard to the scalability of the systems. Therefore, Sirrix will strongly push the exploitation of the gathered results. Sirrix plans to publish an adapted version of the TURAYA™.embedded security kernel that is based on the results of WSAN4CIP and thus, addressing WSANs requirements and providing industrial support.

Sirrix sees many future application areas for the gathered WSAN4CIP results, e.g., in the area of Trusted Grid, Home Automation, and Internet of Things (IoT). Currently, all these application fields do not provide adequate solutions for trustworthy sensor nodes that are offered by the TURAYA security kernel. Therefore, Sirrix will fill these gaps with the results of WSAN4CIP in addition to own developments for the implemented secure TURAYA kernel.

One exemplary key market Sirrix is currently striving into is Smart Metering where 40 million private households will be connected to the Smart Grid within the next decades. The TURAYA.embedded security kernel will be used to build secure embedded sensors for gathering sensor measurements (e.g., energy and heat consumption). The measurement data will then be transmitted wirelessly to a Secure Gateway. The SCADA-developments within WSAN4CIP will help realising such a Secure Gateway. The exploitable results of WSAN4CIP are currently under application to the latest German legal requirements with respect to communication protocols and security objectives.

Additionally, due to the recent dissemination activities (conferences and vendor workshop), Sirrix received several contacts of potential customers and is currently in the negotiation phase.

### **2.1.3 TECNATOM**

TECNATOM has analyzed the potential market for the WSAN4CIP technology in its main area of activity (Services for Nuclear Power Plants - NPP). TECNATOM expects this technology is incorporated into the services portfolio if it is successful. TECNATOM has great potential, considering that around 50% of TECNATOM sales are in these markets, and at present, this technology is not commercially mature in this sector due to the security and reliability problems which are being solved during the project. Additionally, added-value synergy services, such as emergency procedures, human factors studies, etc. will benefit from this initiative, especially taking into account the current market position of TECNATOM in these fields. This technology will also lead to more efficient and robust Information Systems for Critical Infrastructures. TECNATOM strategy on exploitation will be based on several related R&D initiatives to open up new areas of business and industry lines that can benefit from WSAN4CIP results.

Additionally, TECNATOM intends to exploit WSAN4CIP results in the following way:

- Improvement of current products/services: TECNATOM is interested in studying the viability of applying the SCADA interface to WSANs in their training material for Nuclear Power Plant operators. TECNATOM supplies full-scope simulators and other learning tools for plant crew.
- New products/services: TECNATOM is developing a business line of security and monitoring for Nuclear Installations. Clearly, WSAN4CIP results will be of high interest to this business line to offer new monitoring and control systems with improved capabilities regarding security and information from remote, difficult-access locations. Nuclear power plants and other critical infrastructures related to power generation and distribution are on the focus of TECNATOM activities.
- Further R&D: TECNATOM has been awarded a national R&D project from the Spanish Ministry of Industry to develop new technologies for wireless monitoring of critical infrastructures and emergencies that clearly matches with the goals of WSAN4CIP. Results from WSAN4CIP will be a key input for this project.

The main outcome of this project will be a wireless monitoring device for radiological monitoring in emergencies. Additionally, TECNATOM is preparing a proposal for an ICT project for a middleware for wireless embedded systems that also will benefit from know-how obtained in WSAN4CIP.

## **2.2 Academic / Research institutes**

### **2.2.1 INRIA**

INRIA focuses its activities into research, development and technology transfer in the areas of computers and communications. One of INRIA's priorities is computer and network security in general and security of critical infrastructure in particular.

Thanks to this project, INRIA improved its know-how and expertise in the area of critical infrastructure protection. More specifically, INRIA improved its expertise in OS security, code attestation, and key exchange protocols. We showed some very important and fundamental results. For example, we demonstrate that software code attestation is not possible without minimal hardware support.

These results were also used to enrich our teaching materials. The WSAN4CIP project provided the context and partial funding for 2Phd students (D. Perito and S. Ben Hamida), a post-doc (Gergely Acs) and few diploma projects.

INRIA filed 2 patents on wireless key establishment and relay attack detection as a result of this project. These patents are valuable results that will possibly help technology transfer.

We also published several articles in top conferences (such as ACM CCS, Information Hiding, ...) and participated to the visibility and dissemination of European research results and excellence.

This project strengthened INRIA's scientific relations with other European companies and R&D groups in Europe and outside of Europe (in particular with UC Irvine, PARC and UB Berkeley).

It allows us to develop other collaborations in the area of trusted embedded systems, smart grid and smart metering.

### **2.2.2 IHP**

IHP is a research organization which is devoted to innovation. IHP will try to sell Intellectual Property (IP) acquired in the dependability and security area directly to interested parties. Due to the fact that IHP is currently leading a consortium working on real time wireless systems for automation and process control networks (RealFlex), we think that there is a market for such IP and we are already in touch with global players such as Phoenix Contact Electronics GmbH and the Sick AG. In this area IHP is currently preparing a new project proposal that is dedicated to allow for further developing research results into the direction of pre-products. This is an essentially needed step towards a spin off working in the mentioned area.

IHP has conducted a small market analysis including interviews with critical infrastructure owners and software providers for control systems. The result was included in a project proposal submitted to the program Forschung für den Markt im Team (research for the market in a team) run by the German ministry for research and education (BMBF). The research idea is an extension of investigations started in WSAN4CIP and the project proposal was successful. IHP will retrieve 1.6 million € funding to further research intrusion detection systems and tools to set up those systems for critical infrastructures and automation systems. Part of the working items is developing a business plan for a spin-off commercializing the project results. Such spin-off is not essentially required but more than highly welcome and recommended from the BMBF. For IHP this additional project provides a unique opportunity to continue working on topics addressed in WSAN4CIP while collaborating with companies in the field. First user workshop was conducted and the feedback from vendors providing software for control systems for critical infrastructure was positive. Here IHP will continue working on strategies form commercialization especially in cooperation with the software vendors consulted during this workshop.

Currently IHP is planning a spin-off company in the area of wireless communication networks in the application area of water distribution networks, which will apply and further exploit the knowledge of the project. During the preparation of this spin-off contacts from the WSAN4CIP project could be interviewed to tailor the requirements of a potential market. The interviewees include the partner FWA as well as guests at the vendor workshops, i.e. the representative of the water distribution department at Luleå municipality. Both

pose target customers for the planned spin-off. Spin-offs have already been done successfully in the past, i.e. IHP founded two spin-offs namely lesswire AG and Silicon radar GmbH.

Besides commercial exploitation IHP will use the WSAN4CIP results for further research in the security/privacy area. The WSAN4CIP results will partly be used for teaching purposes in lectures which are given at the Technical University of Cottbus and will also be integrated into a new master program with a focus on security which is currently under development at Technical University of Cottbus.

### **2.2.3 INOV**

INOV is a non-profit R&D company focussing its activity into research and development in the areas of computers, communications and electronics. The key participants in this project are also Professors at the Technical University of Lisbon, which is one of the INOV owners. The exploitation of results from the project will therefore be connected not only to the exploitation of the achieved results, but also to academic objectives, namely education and research advancement.

The involvement of INOV in the WSAN4CIP project allowed the achievement of the following:

- Development of novel applications towards protection of substation equipments, protection of medium/ low voltage power distribution lines, premises protection at substation and power transformer cabinets.
- Research progress in the areas of “WSAN protocols”, “Web services for WSAN representation in SCADA systems” and “Increase of security and reliability for communication protocols in Smart Grid environments”. In this area the DTSN protocol has been specified and developed (see table above).

Based on these results INOV considers that:

- Improved its technological position within the community of research establishments
- Enhanced the knowledge base of the research groups involved
- Published research results and improved scientific relations with other European companies and R&D groups.
- The INOV researchers connected to University included in their lectures some of the WSAN4CIP results, namely in “WSAN” lectures and “Computer Networks and Security” lectures.

Additionally, through the development of the novel applications reported above in close cooperation with EDP, and also through the contact with the main equipment suppliers to EDP in the WSAN4CIP vendor’s Workshop, in future, cooperation towards integration of the developed technology into existing products or creation of new products can be achieved.

The results obtained in the current project allowed a more consistent intervention in the area of Smart Grid, which is already instantiated in a new proposal for Call 8 in the Smart Grid area and also in a narrower collaboration with EDP in that domain.

### **2.2.4 BME**

BME enriched its teaching activity with the knowledge generated within the project. This has been achieved, on the one hand, by integrating the generated knowledge in our course on Security Protocols (BMEVIHIM132), a large part of which covers wireless sensor network security. In particular, the application scenarios are used as motivating examples for useful applications of wireless sensor networking technology, the requirement analysis are used to highlight security and dependability aspects of these systems, and the architecture and the mechanisms developed in the project, especially those on secure routing and transport, as well as private aggregation give useful insights into the general design principles of security and dependability mechanisms for wireless networked embedded systems. On the other hand, the project provided the context for several semester and diploma projects, and there were 5 PhD students that worked on it and can use the generated results in their dissertations. The project also served as the vehicle for the participation of BME’s CrySyS Lab in the National Technology Platform called ARTEMIS (Advanced Research and Technology for Embedded Intelligence and Systems) in Hungary. As a follow-up of this, we

leveraged our WSAN4CIP partnership to join a large integrated project (IP) called CHIRON in the ARTEMIS program. In the CHIRON project, we work on security and privacy in body area sensor networks.

We tried to exploit some of the results on dependable networking in the forestry domain, and for this, we established connections with relevant industry partners. We developed a prototype sensor network for detecting animals approaching new plantations, and another prototype sensor network for measuring light intensity in forests. These prototypes were delivered to one of our industry partners, and they used them as a proof of concept to justify the setup of a new project on developing sensor network based solutions in the forestry domains. We also tried to apply our know-how to establish another project with Hungarian industry partners on sensor network based monitoring of fences in forests and near highways. However, this attempt failed due to lack of business interest. Yet, all in all, we believe that our attempts will foster the adoption of sensor technology in the domain of forestry.

We also had plans to apply some of the results in the field of industrial automation, but those have not been realized yet.

One of the main exploitable outcome of the project for BME is our RPL implementation, which has been extensively tested, and which is now in a stable state such that it could even be commercialized. However, this RPL implementation alone is not sufficient for creating a start-up company, because other RPL implementations exist, and they are available for free. So our strategy for exploitation rather aims at teaming up with some industry partner that develops sensor network based solutions and that can leverage our existing RPL implementation and our know-how necessary in customizing this implementation for particular application domains. We are currently exploring the possibilities for such a collaboration; tentative partners include evopro, a Hungarian SME active in the field of industrial automation.

#### **2.2.5 LTU**

LTU will use principles of developing MAC protocol in the iRoad project. It is a Swedish national project which will deploy on-road sensor to monitor traffic and road conditions. The university has an advanced course in WSN where the results of the project are visible. The project results will be exploited for further establishment of the research competence of the group in the area of embedded systems networking on the international academic arena. Specifically, the results will be published on international conferences and workshops, will become a ground for formulation of Master projects and be subject for deeper investigation of selected areas. The output of the project will also be actively used in the education process by significantly extending the content of existing and developing communication courses.

#### **2.2.6 UMA**

UMA will exploit the results of the project with three different goals. From the technology transfer point of view, its strong relationship with critical infrastructure companies, such as TECNATOM, will allow to provide these companies with leading edge technologies that will improve their position in this market. UMA will have continuous collaboration with TECNATOM, developing further WSAN solutions. UMA will aim at contacting companies interested in using SCADA systems and their interaction with WSAN. If the interest is high, potentially a spin-off could be created, following the example set by Softcrits ([www.softcrits.es](http://www.softcrits.es)), a spin-off created from a previous project called SMEPP.

From the point of view of collaboration with other EU funded projects, the participation of UMA in different projects related to security and software development in critical environments as SMEPP, SEEDS, SERENITY, UBISENS and CARLINK will ensure a proper knowledge of related work that is being carried out in other projects.

From the scientific dissemination point of view the group regularly publishes in the main related conferences and journals. Finally, a PhD degree course on Software Development and Security for Sensor Networks is included in the PhD program of the university for the last three years.

### **2.3 End-users**

#### **2.3.1 FWA**

Upon successful reliability and performance field tests, FWA intends to integrate the WSAN4CIP architecture in the control loop of the drinking water distribution network. FWA also plans to use WSAN

enabled mobile measurement stations for quality monitoring. FWA is willing to act as a lead customer for technologies developed in the WSAN4CIP project, thus acting as a seed in order to attract first customers in the drinkable water distribution sector.

### 2.3.2 EDP

EDP wishes to improve the remote monitoring of its substations through the local deployment of wireless sensor networks. It wishes also to improve the remote monitoring of the structural health of the poles supporting distribution energy lines by using the same technology. Therefore, the results of the project and, especially the results of the field test, will be exploited by the company to further deploy WSANs in other substations and poles to enlarge the real-time supervision of the energy distribution network. This deployment will result also in an increased security level of the daily operation of the network. Additionally, EDP intends, during 2012, to continue exploiting the wireless sensor infrastructure, gateway and SCADA system deployed by WSAN4CIP at the substation, power lines and secondary substation.

## 2.4 Exploitable results and WSAN4CIP technology differentiator

By bringing WSANs technology to Critical Infrastructure Protection, WSAN4CIP will be a step ahead in comparison to competitors. By providing theoretical advances in wireless and embedded security and making them practical by integrating them in long-lasting prototypes, it ensures the exploitation of advanced protocols for future products.

### 2.4.1 Overview of exploitable results

The main exploitable results are first listed in an overview table, and then discussed in details.

Exploitable Knowledge (description)	Exploitable product(s)	Short description	Patents or other IPR protection	Owner & Other Partner(s) involved
Advanced node configuration	ConfigKit	Security engineering for WSNs	Licensed SW	IHP
Security bootstrapping	Key exchange over wireless reciprocal channels	Easy bootstrapping for wireless node in scattering environments	Licensed SW	INRIA
Secure Code Update	Over-the-air reprogramming	Secure code update based on in-network coding	Licensed SW	NEC
Advances in MAC layer	Multichannel MAC layer	Reliable and tuneable multichannel MAC layer	Licensed SW	LTU
Advances in routing	RPL implementation with security extensions	Routing for sensor networks	Licensed SW	BME
Advances in network protocols	DTSN	Transport protocol for WSNs	Licensed SW	INOV
Advances in service protection	DDS, tinyDSM	Security products for WSAN Increase data dependability	Licensed SW	NEC, IHP

CIP management	WSAN	SCADA2WSAN Gateway Management middleware	Gateways between WSAN and SCADA. End-to-end communication and logic between SCADA and WSAN.	Licensed SW	UMA, TECNATOM, INOV
Secure kernel for wireless sensor platform		TURAYA security kernel	Secure OS for embedded systems	Licensed SW	Sirrix

### 2.4.2 Advanced node configuration

Configuration of sensor nodes includes the selection of hardware, composition of software and parameterization of the components. It is a complex task which has to be performed before deployment of the system. Fixing errors made in this phase - if possible at all - is connected with high costs. That is why it is mandatory to support system developers and end users in reducing the probability of errors in this phase as much as possible. ConfigKit, a tool that has been developed in WSAN4CIP project, realises an approach to map application requirements to a sensor node system, which eventually can be implemented and finally tested against the requirements. The tool relies on a repository that contains information of available software and hardware modules and their properties and relations described in a XML-based meta-language. The requirements definition interface is meant to be accessible and understood even by non-experts in the domain of sensor networks. By this ConfigKit can reduce the perceived complexity of the node configuration and increase the acceptance of the sensor node technology. That is why we are convinced that such a tool is important to market sensor node system solutions to end users.

Beside the support of the systems developed within the WSAN4CIP project, the exploitation of ConfigKit aims to licensing the technology to third party commercial vendors of wireless sensor network systems and components. Disseminating aspects of the tool in conferences, journals and magazines is primordial to gain the required publicity. To further increase its visibility, a demo of the tool will be made publicly available online at [www.configkit.org](http://www.configkit.org) in 2011.

### 2.4.3 Key exchange for bootstrapping

Bootstrapping is the phase in the life-cycle of a network, where a node joins an existing network. In some scenarios, it might be that the new node does not possess key material prior to entering the network. We devised a new method based on the reciprocity of the wireless channel to securely establish a key between two nodes. More important, we have shown that an attacker in the vicinity of the nodes cannot capture by eavesdropping due to the physical properties of the wireless medium. However, in order to have enough entropy to exchange keys, the environment should offer enough scattering, as it offers variations in the wireless channel. Hence, the key exchange protocol has a lot of potential in indoor environment, and thus the exploitation this invention could also reach consumer markets. For example, wireless personal area networks or buildings automation could benefit from it, as they are generally in environments offering scattering of wireless signal.

### 2.4.4 Secure code update

The secure code update (SCU) is both a protocol to disseminate large files securely among a large sensor network and a program that locally manages on the node the code images, which can be written from external memory to the program memory. The secure code update is a powerful management tool, as it allows reprogramming sensors deployed in the field in a matter of minutes. It is seen as an optional requirement in the smart energy profile of ZigBee Alliance, which is a standard adopted for smart metering in the USA.

SCU has two strong technological advantages over the state of the art. Firstly, it is based on fountain codes, which makes the dissemination of large code update (>2kB) faster in large multi-hop networks (>10 nodes). Secondly, the signature scheme used to authenticate the code image is based on Merkle's one time signature, which purely relies on hash functions. Hence, the cost for public key cryptography, either in program memory or in a hardware accelerator, can be saved. Also, this avoids issues with royalties for patents that are held on suitable elliptic curves algorithms.

As a first step to exploitation, the secure code update has been proposed to several business units of NEC, to equip sensors that are deployed in infrastructures such as buildings, bridges, and mines. It is also planned to incorporate it in home automation solutions, by coupling WSA capabilities with the NEC home gateway solution.

#### **2.4.5 Advances in MAC layer**

WSAN4CIP developed a novel MAC layer, which is designed to meet the stringent requirements of the use cases of critical infrastructure. The MAC protocol is a completely distributed multichannel TDMA scheme. It includes features such as security, prioritization, and frequency hopping. The MAC layer has two major advantages over the standard 802.15.4 MAC: First, the frequency hopping pattern is hard to predict for an attacker, and thus the novel MAC layer is more resilient to jamming issues. Second, the MAC layer can be configured specifically for the application and topology of the use case through the support of engineering methodologies. This approach allows adapting to the most stringent application requirements.

LTU sees applications of this MAC layer for numerous use cases. One of them is roadside sensors, which indeed have requirements and network topologies that are very similar to the ones of WSA4CIP. It is expected that the MAC layer will be reused in further projects, and possibly exploited by SME partners of LTU.

#### **2.4.6 Advances in routing protocols**

For the routing layer, WSA4CIP have been following closely the drafting of RPL, the chosen routing protocol by the IETF ROLL working group. WSA4CIP implemented it according to the latest draft and will integrate it in its two demonstrators. The implementation can be then used in further classes and projects, as RPL will probably be the routing protocol used for most of the WSANs applications. More importantly, BME developed in WSA4CIP a security extension for RPL, which might have a significant impact for the ROLL WG. At the time of writing, a draft is being elaborated to propose security extensions to RPL, which proposes solutions for local and cluster key agreements. Furthermore, mechanisms to provide authentication for the messages of the DODAG root node (a key node in RPL terminology, which may provide connectivity to Internet hosts) are provided, such that WSA nodes can verify the authenticity of routing messages. The security extension would complete the security framework of RPL, which tackles other issues such as payload encryption and authentication.

As RPL might become a ubiquitous solution for routing packets in WSANs, its early adoption by the project increases the chances to make our solution interoperable with future networks. BME can use its deep knowledge of the protocol to foster new projects, and possibly help existing and future local companies to develop WSANs products based on a secure RPL routing layer.

#### **2.4.7 Advances in transport protocols**

For the transport protocols, we extended the DTSN transport protocol with two significant features: buffering strategies and end-to-end security.

The first extension was based on extensive simulations of flows in the networks, with various wireless channel and MAC layers settings. It allowed defining strategies for buffering the packets in-network along the routing path of an end-to-end transmission. Hence, by looking at strategies such as uniform buffering, or alternative ones such as keeping more packets at the extremities of the path or in the middle of it, we observed significant performance increase in term of end-to-end transmission delay and throughput. Hence, with this enhanced DTSN, higher quality of service can be achieved for demanding applications such as video surveillance, a use case that is present in the EDP demo with the substation perimeter surveillance use case.

The security extension of DTSN ensures that the signalling packets of DTSN are protected against replay and forgery attacks. Hence, control packets such as ACK (acknowledgement packet) are provided with integrity and authenticity using efficient symmetric cryptography. An external attacker cannot disturb the network operations by sending bogus control packets, which could easily lead to a Denial of Service (DoS).

The extensions of DTSN made it more secure and reliable, which are the two properties we wanted to develop in WSAN4CIP. We believe it will provide an excellent transport layer for demanding applications. With the EDP demonstrator, we show it can fulfil both high throughput and low-latency requirements. With all those qualities, DTSN is a candidate for being integrated to WSANs solution, and could be licensed for that.

Also, WSAN4CIP developed a new metric to define the robustness of a network that can be evaluated in polynomial time. This metric could be a seed for further research and development of deployment tools for WSANs, where resistance to jamming and node failure. Such a tool could be used by WSANs operator to place sensors strategically such that resilience against faults and attacks is maximised.

#### **2.4.8 Secure OS**

Current WSANs are built using hardware and software with almost no implemented security or reliability features. However, the nature of a WSAN gives the possibility to significantly increase the strength and possibilities to observe and to react to incidents inside CIs. There is a high necessity of building such systems with respect to security techniques developed in the IT security environment. A reliable WSAN heavily depends on a secure and dependable operation of the nodes and, thus, relies on the used operating system. The modified OS should provide mechanisms for strong process isolation, in order to limit the effects of both, accidental errors as well as malicious modifications of the application software. Within the context of the WSAN4CIP project, we solve a significant number of the before mentioned issues, by providing the high-assurance security kernel called TURAYA.

The main aspect of the TURAYA security model and its high-secure kernel is to isolate critical parts of the operating system and encapsulate each of them in so called compartments. This is realised in such a way that no other compartment, running on the system, can access, interact, or influence without permission granted by the underlying TURAYA security kernel. This leads to a system, which still acts as expected, even if parts of the overall system are corrupted.

The secondary aspect of the TURAYA model is that there must be a trustworthy proof of the integrity of the system against the sensor node and the complete wireless sensor network. A solution for this is also provided by the TURAYA security kernel. Sensor nodes and its actuator network running TURAYA can fulfil all set requirements: to observe, to secure, and to react to incidents inside CIs.

Realising trustworthiness inside a WSAN is one of the most important aspects for protecting CIs, thus, the systems and sensor nodes have to be reliable so that every communicating party/entity can trust on the information flow coming out of the network. For example, in case of an incident, a WSAN network measuring a power grid should not behave like everything is in a normal state. All corresponding actuators or even persons behind the control panels should react in-time on an abnormal behaviour of the system. Since possibly cost-intensive or even life-threatening decisions are made based on the measured information of WSANs, these networks have to be fully trustworthy with regard to the data provided.

The TURAYA security kernel provides such a trustworthy platform for secure communication nodes. It is based on a microkernel system with a very small Trusted Computing Base (TCB). Compared to monolithic operating systems, such as Linux or Windows, the number of lines of code is very small so that it is much easier to prove the correct behaviour of such an operating system. On top of the microkernel, TURAYA offers the implementation of several security services, responsible for code-update, attestation, secure communication, and secure measurement of the sensor data. These security services are combined, using a strict isolation of each service in addition to a predefined access control to guaranty a trustworthy communication between each compartment. In parallel to the security relevant compartments, it is possible to run standard operating systems (e.g., Linux) so that even non-TURAYA-specific code can run on the system. Combining all these implemented aspects, the TURAYA security kernel offers a secure and trustworthy platform for sensor and communication nodes to be used in WSAN for the protection of critical infrastructures.



By applying microkernel technology and virtualization techniques, in order to enable strong separation properties, WSAN4CIP develops a new approach to a secure operating system for sensor nodes to be used inside WSNs.

#### **2.4.9 Advances in service protection**

In service protection, the middleware developed in WSAN4CIP to securely share data inside a network may have a large number of use cases. For example, tinyDSM is a middleware that allows a WSAN application to share variables among its neighbourhood, and keeping them consistent with every update. It can be used with any application which needs to share information among nodes. It can furthermore be used as a query system, allowing the base station to query the values of the variables. TinyDSM can be an enabler to develop more reliable and complex WSAN application, and use cases for its usage are virtually unlimited.

A distributed data storage based on network coding was also developed. Contrarily to tinyDSM, the goal is persistency. The idea is to store data for a long period, in order to retrieve it in case of accident or failure. It can also be used for audits, in order to look if the data stored by the WSAN is similar to the data reported to the base station during the operation. Hence, the distributed data storage offers an efficient and reliable long storage service for sensor nodes. It is meant to be exploited in mission critical environment, where no data should be lost, for example when the connection to the base station might be temporarily unavailable.

A QoS manager for the sensor node has also been developed, which allows a node to scale its level of service according to the service need, but also to the availability of resources, in particularly the amount of battery energy left on the node. The QoS manager allows WSANs application to scale its service quality according to the network conditions, hence extending the lifetime of the network.

#### **2.4.10 CIP WSAN management**

SCADA systems were generally constituted of wired devices, sometime in combination with point-to-point wireless backhaul. Nevertheless, the sensor and actuator network could be considered as static, with link failures being only occasional. In WSAN4CIP, the WSANs is much more dynamical than previously, with links that could come and go, immediately replaced by new routes establish by the ad-hoc routing protocol. Furthermore, some nodes may run on battery and thus add an extra dimension to the state of a monitoring node.

Hence, it is important to reflect the status of the WSANs network on the SCADA interface, such that the operator can keep an accurate overview of his system. To achieve this, a WSAN2SCADA gateway has been developed, which translate SCADA requests into WSAN messages. Based on the open-source SCADA system Mango, WSAN4CIP developed an interface which allows to query and manage the WSANs as if it were a usual SCADA system. Furthermore, new SCADA features that are specifically targeted for WSANs are added. For example, the video stream generated by a node may be scaled down automatically by the SCADA systems, if the battery reserve of that node becomes too low, in order to extend the lifetime of the network. This has a real market value, since it allows the infrastructure operator to get the maximum of its WSANs with interfaces for which employees are already trained for, thus requiring a minimum investment on training or communication infrastructure.

### 3 Dissemination activities

The success of this STREP finally depends on their ability to sell, internally in the participating organisations and the public, the results and knowledge they have obtained.

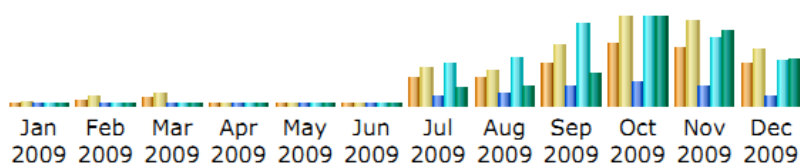
#### 3.1 Website

The WSAN4CIP webpage was set up at the end of March 2009 and is available at <http://www.wsan4cip.eu/>. During the project, the website was continuously updated giving information to publications by the project and listing important news and events. The website is of interest to visitors who work or research on critical infrastructure protection or in wireless sensor networks. Most of the publications and all public deliverables can be downloaded from the website, and generate most of the traffic.

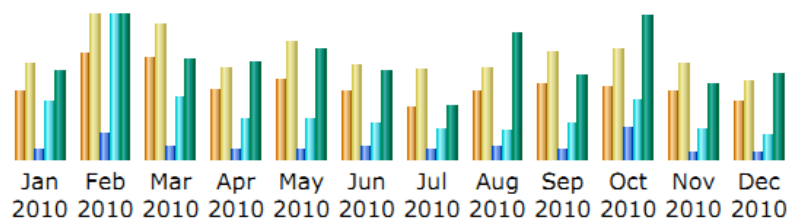
The website additionally contains a private area, accessible to the partners only. It mainly contains manuals for the individuals in how to access and use the different collaborative tools of the projects; for example, how to set up a phone conference or to use the project SVN repository.

The following tables depict statistics of number of visitors during the project runtime. Due to a technical problem, no logging of access information is available between January and July 2011. The website was online without downtime during this period and also frequently updated.

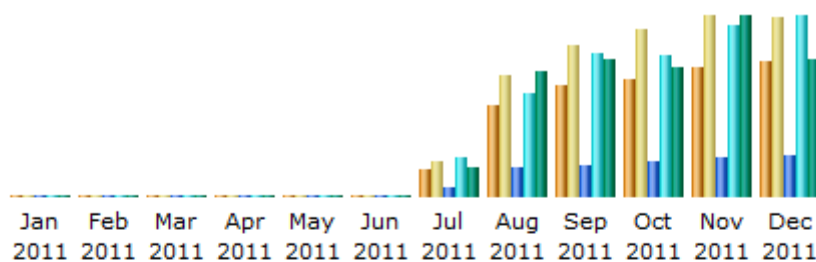
**Table 1: 2009.**



Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2009	11	13	16	32	96.56 KB
Feb 2009	25	46	61	100	234.61 KB
Mar 2009	44	58	69	123	300.12 KB
Apr 2009	6	6	7	12	25.02 KB
May 2009	0	0	0	0	0
Jun 2009	0	0	0	0	0
Jul 2009	150	219	719	3410	17.69 MB
Aug 2009	144	195	841	3922	19.97 MB
Sep 2009	238	341	1588	6641	34.75 MB
Oct 2009	347	496	1857	7204	92.49 MB
Nov 2009	327	484	1510	5540	78.38 MB
Dec 2009	234	318	785	3542	48.22 MB
Total	1526	2176	7453	30526	292.15 MB

**Table 2: 2010.**

Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2010	270	381	1876	9943	100.30 MB
Feb 2010	419	576	4206	24944	166.79 MB
Mar 2010	407	539	2062	10634	115.65 MB
Apr 2010	281	360	1455	6892	112.63 MB
May 2010	314	473	1880	6788	126.92 MB
Jun 2010	268	374	1981	5855	101.37 MB
Jul 2010	211	357	1667	5054	62.79 MB
Aug 2010	273	368	1958	4770	145.44 MB
Sep 2010	296	425	1836	5971	97.86 MB
Oct 2010	284	437	5501	10124	165.35 MB
Nov 2010	272	378	1080	5004	87.01 MB
Dec 2010	227	309	976	4071	99.77 MB
Total	3522	4977	26478	100050	1.35 GB

**Table 3: 2011.**

Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2011	0	0	0	0	0
Feb 2011	0	0	0	0	0
Mar 2011	0	0	0	0	0
Apr 2011	0	0	0	0	0
May 2011	0	0	0	0	0
Jun 2011	0	0	0	0	0
Jul 2011	66	81	318	1251	33.35 MB
Aug 2011	215	286	920	3382	142.61 MB
Sep 2011	263	357	992	4691	156.34 MB
Oct 2011	278	396	1149	4611	147.27 MB
Nov 2011	307	427	1306	5632	206.07 MB
Dec 2011	319	425	1340	5904	157.49 MB
Total	1448	1972	6025	25471	843.13 MB

## 3.2 Flyer

As part of the project dissemination support, a flyer was prepared and printed in February 2010. It presents WSAN4CIP in a two-sided threefold brochure, which can be handed out by the project partners to visitors of their organisation. It is also an excellent communication vector at conferences, and other fairs, to let people remember about the project. We expect people interested in the project to then visit the website if they need further information. The flyer can be found in the Annex.

## 3.3 Media Releases

Media Releases are an important tool to reach a broader public audience than by industrial and scientific dissemination.

A first press release was issued in January 2010 to communicate to the public the vision of WSAN4CIP, and to provide early information on the setup of the two demonstrators at EDP and FWA. The release has been translated to Portuguese and German.

A second press release has been issued in December 2011. The release reports from the two WSAN4CIP demonstrators that successfully demonstrated a wireless sensor-based solution for cost-effective monitoring of electricity distribution networks and water networks. The release has been translated to Portuguese and German for distribution through the end-users of the demonstrators, EDP and FWA.

The press release was well received, e.g. by

- “Wireless sensors effective in protecting critical infrastructure”, Wireless Homeland Security, 21 December 2011
- “Wireless sensors for infrastructure protection”, Cordis Wire, 20 December 2011
- „Drahtlose Sensoren für den Infrastrukturschutz“, inovations-report, 19 December 2011
- „Drahtlose Sensoren für den Infrastrukturschutz“, IDW Online, 19 December 2011
- “NETZE: Drahtlose Sensoren für den Infrastruktur-Schutz” in the German magazine “Energie und Management” including an interview with Uwe Herzog, 9. Januar 2012

The distribution of the press release by the end-users is still ongoing, so that additional local coverage in Germany and Portugal are expected.

Both press releases can be found in the appendix.

## 3.4 Project Presentations

WSAN4CIP has participated to three seminars / panels

- Panel discussion on Protection of Critical Infrastructure and its Design Implications on Mesh Network based Systems, organized at 9th International Symposium on Autonomous Decentralized Systems, 2009; further panellists from BSI and SMART (Artemis project)
- P. Langendoerfer, Wireless Sensor and Actuator networks chance or risk for critical infrastructure protection, at 4th German-Norwegian Security Conference, 2 December 2009, Berlin

As promised in the dissemination plans, BME also released a project summary in the Infocommunications Journal published by the Hungarian Scientific Association for Infocommunications, a sister society of the IEEE Communications Society. Levente Buttyán also gave invited talks at various places.

WSAN4CIP was presented at the following events:

Event/Location	Date	Title	Presenter	WP / Cooperation
Concertation Meeting on Wireless Sensor	5.3.09	WSAN4CIP Wireless Sensor and Actuator	P. Langendoerfer	IHP, WP6

Networks and Cooperating Objects, Brussels, Belgium		Networks for the Protection of Critical Infrastructures		
Verein der Brandenburgischen Ingenieure und Wirtschaftler e. V. (VBIW), IHP, Frankfurt Oder, Germany	6.5.09	WSAN4CIP Project	P. Langendoerfer	IHP, WP6
Seminar Series on Advances in Telecommunications, Networking and Computing, Budapest University of T..., Budapest, Hungary	25.6.09	Selected Security and Privacy Schemes for Wireless Sensor Networks: CDA and Secure Code Update	Dirk Westhoff	NEC, WP2, WP4
EU-Brazil R&D Collaboration Workshop, Sao Paulo, Brazil	8.9.09	Security, Privacy and Trust Research in the European Union	Jim Clarke	external, WP6
2nd Workshop of the IntelliCIS COST Action IC0806, Budapest, Hungary	17.5.10	The WSAN4CIP Project	Levente Butyan	BME, WP6
Seminar, University of Twente, The Netherlands	26.5.10	Dependable protocols for wireless sensor networks	Levente Butyan	BME, WP3,WP6
Keynote at IWSCN 2010, Karlstad, Sweden	27.5.10	Dependable protocols for wireless sensor networks	Levente Butyan	BME, WP3,WP6
4th Monitoring and Control Concertation Meeting, Brussels, Belgium	2.6.10	Wireless Sensor and Actuator Networks for Protection of Critical Infrastructures	Augusto Casaca	INOV, WP1, WP3
Workshop on Monitoring and Control for Full Water-Cycle Management co-organized with HD-MPC and EUCL..., Brussels	18.6.10	WSAN4CIP & IQLevel: Wireless Sensor Network for Water Management	Peter Langendörfer	IHP, WP6
IADIS Multi Conference on Computer Science and Information Systems 2010 , Freiburg, Germany	26.7.10	Keynote speech on "Selected Security and Dependability Solutions for Uplink and Downlink Traffic in Wireless Sensor Networks"	D. Westhoff	NEC, WP2, WP3
The second COST IC 0906 WiNEMO Workshop, University Pompeu Fabra, Barcelona, Spain	14.9.10	On Specification Process of Dependable MAC Protocols	Evgeny Osipov	LTU, WP1, WP3
The third COST IC 0806 IntelliCIS Workshop, University of Novy Sad, Serbia	23.9.10	On Specification Process of Dependable MAC Protocols	Evgeny Osipov	LTU, WP1, WP3
1st Effectsplus cluster meeting, Brussels, Belgium	29.3.11	WSAN4CIP in a nut shell	Peter Langendörfer	IHP, WP6

4th Summer School on Network and Information Security, Crete, Greece	27.6.11	WSAN4CIP - Wireless Sensor and Actuator Networks for the Protection of Critical Infrastructures (Poster)	Steffen Peter, Michaela Schreier, Peter Langendörfer	IHP, WP6
Effectsplus Clustering Event Amsterdam, Amsterdam, The Netherlands	4.7.11	Assessment models to improve the usability of security in Wireless Sensor Networks	Steffen Peter	IHP, WP2
FI Cluster Workshop, Future Internet Week, Poznan, Poland	27.10.11	Wireless sensor networks: a building block for tomorrow's smart cities	Peter Langendörfer	IHP, WP6

### 3.5 Conference, Journal and Magazine Publications

The WSAN4CIP project was very active in disseminating research results. The tables in Section 3.5 give a detailed list of the paper published by the project in Journals, Magazines, Conference Proceedings, and Book Chapters. In total WSAN4CIP published 11 Journal, 3 Magazine, 47 Workshop and Conference Articles and 1 Book Chapter. As recommended by the reviewers, WSAN4CIP worked towards joint publications. Many publications were also collaborations with external partners, spreading the ideas and securing additional knowledge for WSAN4CIP.

Conference	Date	Paper	Authors	WP / Cooperation
<b>Journal</b>				
Computer Networks, Elsevier	Apr. 2009	Distributed Latency-Energy Minimization and Interference Avoidance in TDMA Wireless Sensor Networks	M. Macedo, A. Grilo, M. S. Nunes	INOV, WP3
International Journal of Business Data Communications and Networks, IGI Global	Oct. 2009	Slot Allocation Algorithms for Minimizing Delay in Alarm-driven WSN Applications	M. Macedo, A. Grilo, M. Nunes	INOV, WP3
IEEE Wireless Communications Magazine, Special Issue on Security and Privacy in Emerging Wireless Networks	Oct. 2010	Application of Wireless Sensor Networks in Critical Infrastructure Protection: Challenges and Design Options	L. Buttyán, D. Gessner, A. Hessler, P. Langendoerfer	BME, SIRRIX, IHP, NEC, WP6
Computer Communications, Elsevier	Dec. 2010	Data Obfuscation with Network Coding	A. Hessler, T. Kakumaro, H. Perrey, D. Westhoff	NEC, WP3, WP4
it- Information Technology	Dec. 2010	Security Solutions for Uplink- and Downlink-Traffic in Wireless Sensor Networks	J.-M. Bohli, A. Hessler, O. Ugus, D. Westhoff	NEC, WP2, WP3, WP4
Springer Telecommunication Systems	Dec. 2010	On automating the verification of secure ad-hoc network routing protocols	T. V. Thong, L. Buttyan	BME, WP3
Ad Hoc & Sensor Wireless Networks	2011	Dependable Over-the-Air Programming	J.-M. Bohli, A. Hessler, K. Maier, O. Ugus, D. Westhoff	NEC, WP2
Journal of Network and Computer	July 2011	A survey on quality of service support in wireless	J. Chen, M. Díaz, L. Llopis, B. Rubio, J. M.	UMA, WP6

Applications		sensor and actor networks: Requirements and challenges in the context of critical infrastructure protection	Troya	
International Journal of Distributed Sensor Networks, Special Issue on Sensor Networks for High-Confidence Cyber-Physical Systems	2011	Anonymous Aggregator Election and Data Aggregation in Wireless Sensor Networks	T. Holczer, L. Buttyan	BME, WP3
IEEE Transactions on Dependable and Secure Computing	November/December 2011	Detection and Recovery From Pollution Attacks in Coding Based Distributed Storage Schemes	L. Buttyán, L. Czap, I. Vajda	BME, WP4
Elsevier, Performance Evaluation Journal	2011/2012	An Analytical Model for Transport Layer Caching in Wireless Sensor Networks	N. Tiglao, A. Grilo	INOV, WP3

Magazine				
Eurescom mess@ge	March 2011	Wireless sensor and actuator networks for critical infrastructure protection	P. Langendoerfer	IHP, WP6
Eurescom mess@ge	March 2011	Protection of electrical energy distribution infrastructures - The example of EDP	A. Casaca, C. Fortunato	INOV,EDP, WP1, WP5
Eurescom mess@ge	March 2011	Monitoring drinking water pipelines	S. Peter, G. Weber	IHP,FWA, WP7

Workshop/Conference				
9th International Symposium on Autonomous Decentralized Systems	23. Mar 2009	A Cross-Layer Approach for Data Replication and Gathering in Decentralized Long-Living Wireless Sensor Networks	M. Brzozowski, K. Piotrowski, P. Langendörfer	IHP, WP6
SNCNW + Adhoc 2009 : 6th Swedish National Computer Networking Workshop and 9th Scandinavian Workshop...	4. May 2009	Introduction to component based design of dependable protocols for wireless sensor networks	L. Riliskis, E. Osipov	LTU, WP1
The 2009 International Symposium on Collaborative Technologies and Systems (CTS 2009)	18. May 2009	tinyDSM: A Highly Reliable Cooperative Data Storage for Wireless Sensor Networks	K. Piotrowski, P. Langendörfer, S. Peter	IHP, WP4/WP6
7th International Conference on Wired / Wireless Internet Communications	27. May 2009	On Prolonging Sensor Node Gateway Lifetime by Adapting its Duty Cycle	M. Brzozowski, P. Langendoerfer	IHP, WP6
SENSORCOMM09	18. June	WSN Self-address Collision Detection and Solving	C. Ribeiro, I. Anastácio, A. Costa, M. Baptista	INOV, WP3

	2009			
5th EuroNGI Conference on Next Generation Networks	1. July 2009	Multimedia Data Transport for Wireless Sensor Networks	J. Almeida, A. Grilo, P. R. Pereira	INOV, WP3
WOOT '09, 3rd USENIX Workshop on Offensive Technologies. USENIX Association	10. Aug. 2009	Half-Blind Attacks: Mask ROM Bootloaders are Dangerous	T. Goodspeed, A. Francillon	INRIA, WP2
The 7th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC09)	29. Aug. 2009	Completely distributed low duty cycle communication for long-living sensor networks	M. Brzozowski, H. Salomon and P. Langendoerfer	IHP, WP6
ETFA 2009 - 14th IEEE International Conference on Emerging Technologies and Factory Automation.	22. Sep 2009	An Engineering Approach for Secure and Safe Wireless Sensor and Actuator Networks for Industrial Automation Systems	S. Peter, O. Stecklina, P. Langendoerfer	IHP, WP6
IEEE Workshop on Wireless and Sensor Network Security (WSNS)	5. Oct 2009	Private Cluster Head Election in Wireless Sensor Networks	L. Buttyan, T. Holczer	BME, WP3
SOMSED'09, Self-Organising Wireless Sensor and Communication Networks	8. Oct 2009	Multi-Hop Over-The-Air Reprogramming of Wireless Sensor Networks using Fuzzy Control and Fountain Codes	K. Maier, A. Hessler, O. Ugus, J. Keller, D. Westhoff	NEC, WP2
SNE 2009	28. Oct 2009	Applications of the wireless sensor networks to the nuclear industry	J. Serrano, P. Piñeiro, E. Cabrera	TEC, WP6
SECUCODE'09: 1st ACM workshop on secure code execution	9. Nov 2009	Defending embedded systems against control flow attacks	A. Francillon, D. Perito, C. Castelluccia	INRIA, WP2
CCS'09: Proceedings of the 16th ACM conference on Computer and Communications Security	9. Nov 2009	On the Difficulty of Software-Based Attestation of Embedded Devices	C. Castelluccia, A. Francillon, C. Soriente, D. Perito	INRIA, WP2
Third IFIP International Conference on New Technologies, Mobility and Security (NTMS 09)	20. Dec 2009	An Adaptive Quantization Algorithm for Secret Key Generation using Radio Channel Measurements	S. Tmar, B. Hamida, J.-B. Pierrot, C. Castelluccia	INRIA, WP2
WNS3, Workshop on ns-3 in conjunction with the SIMUTools 2010	15. Mar. 2010	TOS-NS3 : a framework for emulating wireless sensor networks in the ns3 network simulator	L. Riliskis, E. Osipov, M. Maróti	LTU, WP3
IEEE Workshop on Sensor Networks and Systems for Pervasive Computing (PerSeNS)	29. Mar. 2010	Security Analysis of Reliable Transport Layer Protocols for Wireless Sensor Networks	L. Buttyán, L. Csik	BME, WP3
IEEE International Workshop on SECurity and SOCial Networking	2. Apr 2010	When Eco-IT meets Security: Concealed Network Coding for Multicast Traffic	A. Hessler, T. Kakumaru, D. Westhoff	NEC, WP3



(SESOC'10)				
7th GI/ASQF, Schloß-Steinhöfel-Seminar "Innovationen in Markt u. Forschung"	26. Apr. 2010	Towards Cyber Physical Systems Protection: Recent Achievements and Challenges Ahead	P. Langendörfer, L. Buttyan, A. Casaca, E. Osipov, D. Gessner	IHP,BME,INO V,LTU,SIRRIX , WP1
8th International Conference on Wired/Wireless Internet Communications (WWIC)	1. June 2010	ILA: Idle Listening Avoidance in Scheduled Wireless Sensor Networks	M. Brzozowski, H. Salomon, P. Langendoerfer	IHP, WP6
6th Euro-NF Conference on Next Generation Internet (NGI'2010)	2. June 2010	Efficient Multimedia Transmission in Wireless Sensor Networks	J. Mingorance-Puga, G. Maciá-Fernández, A. Grilo and N. Tiglao	INOV, WP3
IEEE Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC)	7. June 2010	Pollution Attack Defense for Coding Based Sensor Storage	L. Buttyán, L. Czap, I. Vajda	BME, WP4
IFIP WCC 2010 Critical Infrastructure Protection Conference	20. Sep 2010	Wireless Sensor Networks for the Protection of an Electrical Energy Distribution Infrastructure	A. Grilo, A. Casaca, M. Nunes, C. Fortunato	INOV,EDP, WP3, WP5
15th European Symposium on Research in Computer Security (ESORICS 2010)	20. Sep 2010	Secure Code Update for Embedded Devices via Proofs of Secure Erasure	D. Perito, G. Tsudik	INRIA, WP2
The 21th Personal, Indoor and Mobile Radio Conference (PIMRC 2010)	26. Sep. 2010	Empirical Analysis of UWB Channel Characteristics for Secret Key Generation in Indoor Environments	S. Ben Hamida, JB. Pierrot, C. Castelluccia	INRIA, WP2
8th ACM International Symposium on Mobility Management and Wireless Access (MobiWac 2010)	17. Oct. 2010	Limiting End-to-End Delays in Long-Lasting Sensor Networks	M. Brzozowski, H. Salomon, P. Langendoerfer	IHP, WP4
IEEE Workshop on Wireless and Sensor Network Security (WSNS)	8. Nov 2010	Perfectly Anonymous Data Aggregation in Wireless Sensor Networks	L. Buttyán, T. Holczer	BME, WP3
4th Workshop on Network Control and Optimization (NETCOOP'10)	29. Nov. 2010	Optimal Cache Partitioning in Reliable Data Transport for Wireless Sensor Networks	N. Tiglao, A. Grilo	INOV, WP3
The 2nd International ICST Conference on Sensor Systems and Software, S-Cube 2010	13. Dec. 2010	How secure are secure localization protocols in WSNs?	C. Boucetta, M. Ali Kaafar, M. Minier	INRIA, WP4
The 6th International Conference on Mobile Ad-hoc and Sensor Networks (MSN'10)	20. Dec. 2010	Inferring Technical Constraints of a Wireless Sensor Network Application from End-User Requirements	F. J. Oppermann, S. Peter	IHP, WP6
IEEE BCFIC 2011	16. Feb. 2011	On Synthesis of Dependable MAC Protocol for Two Real-world WSN applications	L. Riliskis, E. Osipov	LTU, WP1,WP3
IEEE Conference on Computer	10. Apr.	Backpressure approach for bypassing jamming attacks	A. Dvir, L. Buttyan	BME, WP3

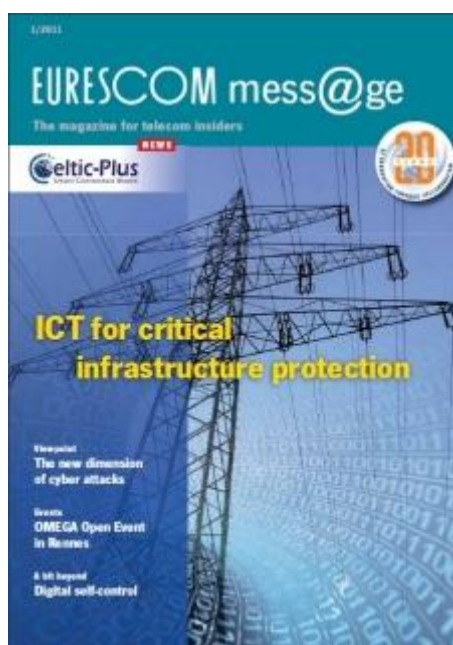
Communications (INFOCOM), poster session	2011	in wireless sensor networks		
The 13th Information Hiding Conference (IH)	18. May 2011	I have a DREAM! (Differentially Private smart Metering)	G. Acs, C. Castelluccia	INRIA, WP3
IEEE International Conference on Communications (ICC)	5. June 2011	A Secure Distributed Transport Protocol for Wireless Sensor Networks	L. Buttyan, A. M. Grilo	BME, INOV, WP3
11th International Conference on Innovative Internet Community Systems	15. June 2011	Code Attestation with Compressed Instruction Code	B. Vetter, D. Westhoff	NEC, WP2
ACM WiSec 2011	17. June 2011	Demonstrating self-contained on-node counter measures for various jamming attacks in Wireless Sensor Networks (Demo)	P. Langendoerfer, S. Ortmann, S. Kornemann	IHP, WP2
IEEE Workshop on Data Security and Privacy in Wireless Networks	20. June 2011	Optimal Selection of Sink Nodes in Wireless Sensor Networks in Adversarial Environments	A. Laszka, L. Buttyan, D. Szeszler	BME, WP3
7th Euro-NF Conference on Next Generation Networks	27. June 2011	A Transport Protocol for Real-time Streaming in Wireless Multimedia Sensor Networks	D. Meneses, A. Grilo, P. R. Pereira	INOV, WP3
Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2011)	7. July 2011	Self-contained detection of jamming attacks on Wireless Sensor Nodes (Poster)	S. Ortmann, S. Kornemann, P. Langendörfer, S. Peter	IHP, WP2
6th Future Security 2011	5. Sep. 2011	Realising a trustworthy sensor node with the idea of virtualisation	D. Gessner, M. Selhorst, C. Stübke, P. Langendoerfer	SIRRIX, NEC, IHP, WP2
6th IEEE International Workshop on Practical Issues in Building Sensor Network Applications (SenseApp 2011)	4. Oct. 2011	Resilient Data Aggregation for Unattended WSNs	J.-M. Bohli, P. Papadimitratos, D. Verardi, D. Westhoff	NEC, WP4
IEEE Workshop on Wireless and Sensor Network Security (WSNS)	17. Oct. 2011	VeRA - Version Number and Rank Authentication in RPL	A. Dvir, T. Holczer, L. Buttyan	BME, WP3
The 10th ACM Workshop on Privacy in the Electronic Society (WPES)	17. Nov. 2011	Protecting Against Physical Resource Wiretapping	G. Acs, C. Castelluccia and W. Lecat	INRIA, WP3
11a Conferência sobre Redes de Computadores (CRC'2011)	17. Nov. 2011	Energy and Quality of Service Management in Wireless Multimedia Sensor Networks	P. R. Pereira, J. Gonçalves, A. Grilo, C. Fortunato, M. S. Nunes, A. Casaca	EDP, INOV, WP4
11a Conferência sobre Redes de Computadores (CRC'2011)	17. Nov. 2011	A Multipath Extension to the Dynamic Source Routing Protocol for Wireless Multimedia Sensor Networks	N. Magaia, P. R. Pereira, A. Grilo	INOV, WP3
Network and	16.	SMART : Secure and	K. El Defrawy, A.	INRIA, WP2

Distributed Systems Security Symposium (NDSS)	Apr. 2012	Minimal Architecture for Establishing a Dynamic Root of Trust	Francillon, D. P. Perito, G. Tsudik	
---	-----------	---	-------------------------------------	--

Book Chapter				
Critical Infrastructure Security: Assessment, Prevention, Detection, Response, WIT Press	2011	<i>Wireless Sensor Networks for Critical Infrastructure Protection</i>	P. Langendoerfer, L. Buttyan, A. Hessler, C. Castelluccia, A. Casaca, A. Alkassar, E. Osipov	IHP, BME, NEC, INOV, SIRRIX, LTU

### 3.6 Eurescom Mess@ge

WSAN4CIP organised the cover theme of the Eurescom mess@ge 1/2011 "Critical Infrastructure protection" which was issued in March 2011. The issue highlights some of the latest solutions European research has to offer in making our critical infrastructures more secure.



WSAN4CIP contributed the following articles:

- Uwe Herzog "An overview on ICT and critical infrastructure protection"
- Peter Langendoerfer "Wireless sensor and actuator networks for critical infrastructure protection"
- Augusto Casaca, Carlos Fortunato "Protection of electrical energy distribution infrastructures - The example of EDP"
- ICT – The key for successful infrastructure protection. Interview with Aurelio Blanquet from Portuguese electricity operator EDP
- Steffen Peter, Gerd Weber, "Monitoring drinking water pipelines"

### 3.7 Internal dissemination activities

INOV contributed together with the EDP participants in the project towards the dissemination of the WSAN4CIP activities within the EDP Distribution company, which is directly interested in the results of this project

- UMA Organisation of courses which reuse and integrate WSAN4CIP research activities and results with a particular focus on security engineering, security patterns, ubiquitous, pervasive and mobile computing, ambient intelligence
- UMA Organisation of customised courses to industrial partners so as to show the WSAN4CIP's applicability and customisability on the marketplace

TECNATOM is an engineering company with more than 800 engineers working for industrial companies worldwide. The project is internally disseminated in several ways:

- 1) News item with presentation of the WSAN4CIP project in the intranet of the company. TECNATOM intranet is a daily resource for the staff of the company. News items about WSAN4CIP will be displayed on the intranet.
- 2) Presentation of WSAN4CIP to business units. Presentations about the project will be done to managers and engineers of the Division of Safety, Training and Operation, especially to the Emergency Management and Operation Support groups.

Most customers and partners of TECNATOM are involved in the decision-making process for procurement of equipment related to industrial monitoring and maintenance. All of them are potential users of results from WSAN4CIP. Therefore, results and progress of the project will be shown to them in several ways:

- 1) Presentation to Spanish Nuclear Society. This is a yearly meeting of the Spanish Nuclear Sector, including utilities, power plants, and engineering companies. TECNATOM presented a paper based on WSAN4CIP project that is the most downloaded file in the WSAN4CIP website.
- 2) News item in AGORA bulletin. This monthly bulletin is sent to national customers and partners of TECNATOM.
- 3) News item in TECNOTICIAS bulletin. This quarterly bulletin is created for international customers of TECNATOM.
- 4) Presentation in events in the nuclear sector. Information about the project will be presented at some key events of the European and world nuclear sector.

### **3.8 Concertation and Clustering Activities**

In 2009, INOV presented, in one of the European Commission concertation meetings, the rationale and the design for the WSAN4CIP demonstrator at the EDP premises.

WSAN4CIP took twice part in Effectsplus workshops. Effectsplus is a FP7 funded Coordination & Support Action across a large spectrum of R&D activity in trust and security. Peter Langendörfer attended the 1st Effectsplus cluster meeting. The meeting took place on 29 and 30 March in Brussels, Belgium. The report of this event is available from

<http://www.effectsplus.eu/files/2011/04/Effectsplus-March-event-report-Final.pdf>

Steffen Peter attended the 2nd Effectsplus Clustering Event that took place on 4 and 5 July in Amsterdam. WSAN4CIP joined the Special Interest Group on Monitoring. Current members of this group are the projects VIS-SENSE, MASSIF, COMIFIN, SYSSEC, WSAN4CIP, ANIKETOS, DEMONS, and TWISNET.

### **3.9 Summer School on Network and Information Security**

WSAN4CIP proactively made the effort to be present at the 4th Summer School on Network and Information Security. The summer school took place in Crete, Greece from 27 June to 1 July 2011. 2011's theme was "The Challenge of the Changing Risk Landscape" which fits well for WSAN4CIP's focus on critical infrastructure protection. Steffen Peter presented the WSAN4CIP poster "Wireless Sensor and Actuator Networks for the Protection of Critical Infrastructures". The summer school is annually co-organised by ENISA and FORTH-ICS.

## Annex A

### A.1 Media Releases

#### A.1.1 February 2010

#### ***EU researchers develop cost-effective infrastructure protection - Press release, 2 February 2010 -***

**Distribution networks for water and electricity are critical infrastructures for the functioning of our society. But what, if they are disrupted? How quickly do you notice? The European research project WSAN4CIP has developed a wireless sensor-based solution for cost-effective monitoring of critical infrastructures, which will increase their security.**

Today, critical infrastructures are either monitored and protected at very high cost, or their protection is neglected due to lack of money. WSAN4CIP, a European research consortium of twelve industrial and academic partners, is developing a solution which enables the cost-effective and reliable protection of such infrastructures. The solution is based on a secure communication network of wireless sensors.

"For monitoring critical infrastructures, you need sensor networks that are reliable. The current solutions don't offer the necessary security and dependability. Our project will make critical infrastructures more secure by setting up the first reliable wireless sensor network," says Peter Langendörfer from IHP, the technical manager of WSAN4CIP.

Two use cases, one in the energy sector and one in the water utilities sector, have been selected to prove the feasibility of the project's solution. In February 2010, the test phase will begin.

In the first use case, the project will implement a network of wireless sensors and actuators in a part of the power distribution network of EDP Distribuição Energia, a major energy distribution company in Portugal. The purpose is to get fast and reliable information on disruptions in the power distribution network and where they have occurred. "The WSAN4CIP solution will enable us to localise the point of failure immediately," explains Carlos Fortunato, senior technical expert of EDP.

In the second use case, the project will implement a network of wireless sensors and actuators in the drinking water network of FWA (Frankfurter Wasser- und Abwassergesellschaft), a regional drinking water and waste water management company in Frankfurt/Oder, Germany.

The wireless sensors in the network measure the water pressure and communicate data in case a sudden decrease of water pressure occurs, which may be an indicator of a disruption. The cause of a disruption could be, for instance, an accidentally damaged water pipe or a terrorist attack.

Gerd Weber, CEO of FWA, regards WSAN4CIP as an important step forward. "The project's wireless sensor solution will enable us to set up a monitoring network with a much higher density of measuring points. The current wire-based solutions would be simply too expensive for us," says Mr. Weber.

Uwe Herzog, coordinator of the WSAN4CIP project, summarises the benefits as follows: "The added value of WSAN4CIP, compared to current solutions, is that it provides secure

communication between the sensors so that measured information is highly reliable - a key requirement for operators of critical infrastructures."

## About WSAN4CIP

The goal of WSAN4CIP is to advance the technology of Wireless Sensor and Actuator Networks (WSANs) beyond the current state of the art, in order to improve the protection of Critical Infrastructures (CIs). WSAN4CIP is a Specific Targeted Research Project (STREP), which is partly funded by the European Commission in the ICT security area of the Seventh Framework Programme (FP7) under Objective 1.7: "Critical Infrastructure Protection". The project started on 1 January 2009 and has a duration of three years.

Project coordinator: Uwe Herzog, Eurescom

WSAN4CIP website including list of partners: [www.wsan4cip.eu](http://www.wsan4cip.eu)

### A.1.2 December 2011

Wireless sensors for infrastructure protection

#### ***EU research project WSAN4CIP has demonstrated a cost-effective solution for protecting electricity and water networks***

**Critical infrastructures are increasingly exposed to hacker attacks and other risks. Reducing these risks by making critical infrastructures more secure is a major societal challenge. A key element to achieve this is infrastructure monitoring. The European research project WSAN4CIP has now successfully demonstrated a wireless sensor-based solution for cost-effective monitoring of electricity distribution networks and water networks.**

The WSAN4CIP solution is based on a secure communication network of wireless sensors. Since February 2010 it has been successfully implemented and tested in two use cases, one in the energy sector and one in the water utilities sector.

## Energy

In the first use case, the project implements a network of wireless sensors and actuators (WSAN) in a part of the power distribution network of EDP Distribuição Energias de Portugal, a major energy distribution company in Portugal. The WSAN4CIP solution enables a fast and reliable information on disruptions in the power distribution network and where they have occurred. If, for example, an intruder enters a power substation, a camera is automatically switched on, the intruder is filmed, and the video is sent with an intrusion alert to a control center. An alert is also sent, if sensors measure a too high temperature in substation equipment.

The WSAN4CIP solution allows the remote active monitoring of several safety and security-related parameters. This includes circuit breaker trip coil status and power transformer oil temperature as well as medium and low voltage power line activity in all three phases to detect location of power line failures. Furthermore the sensors allow remote detection of medium- and low-voltage power transformer hotspots, through an infrared camera, to identify an emerging malfunction. All the monitored parameters will be visualized via the SCADA (supervisory control and data acquisition) system through a special-purpose interface and a graphical user interface.

## **Water**

In the second use case, the project implemented a network of wireless sensors and actuators in the drinking water network of FWA (Frankfurter Wasser- und Abwassergesellschaft), a regional drinking water and waste water management company in Frankfurt/Oder, Germany.

The wireless sensors in the network monitor physical access to the infrastructure and measure the water pressure. Data is communicated in case a sudden decrease of water pressure occurs, which may be an indicator of a disruption. The cause of a disruption could be, for instance, an accidentally damaged water pipe or a malicious attack.

In order to make the wireless sensor and actuator network robust and resilient, the WSAN4CIP project team created a novel, improved transport protocol, which enables a more secure wireless data transmission. WSAN4CIP has proven that a high level of critical infrastructure protection can be achieved through its wireless sensor and actuator solution while the implementation is much easier, faster and less expensive than a wired solution.

## **About WSAN4CIP**


The goal of WSAN4CIP is to advance the technology of Wireless Sensor and Actuator Networks (WSANs) beyond the current state of the art, in order to improve the protection of Critical Infrastructures (CIs). WSAN4CIP is a Specific Targeted Research Project (STREP), which is partly funded by the European Commission in the ICT security area of the Seventh Framework Programme (FP7) under Objective 1.7: "Critical Infrastructure Protection". The project started on 1 January 2009 and has a duration of three years.



## A.2 WSAN4CIP Flyer

Reliable data anytime,  
anywhere for secure

### Critical Infrastructures



Today, Critical Infrastructures, like power and water distribution networks, have become difficult to protect, due to growing complexity and increased threats.


The rapid development of wireless sensor technologies offers now cost-effective ICT solutions to enhance the dependability of Critical Infrastructures (CIs).

The WSAN4CIP project aims to demonstrate the benefits of wireless sensor technology for the protection of Critical Infrastructures. This shall build the necessary trust for utilities to deploy WSNs for CI protection.

Better protection for


### Critical Infrastructures

Visit [www.wsan4cip.eu](http://www.wsan4cip.eu)  
for further information



# WSAN<sup>4CIP</sup>

Wireless Sensor and Actuator  
Networks for the Protection of  
Critical Infrastructures



[www.wsan4cip.eu](http://www.wsan4cip.eu)

SEVENTH FRAMEWORK PROGRAMME

**Project Manager:** Uwe Herzog  
herzog@eurescom.eu  
+49 6221 989 132

**Technical Manager:** Peter Langendörfer  
langendoerfer@ihp-microelectronics.com  
+49 335 5625 350

### Building trust and dependability for WSAN Technology



WSAN4CIP aims at substantially advancing the technology of Wireless Sensor and Actuator Networks (WSANs) beyond the current state of the art and to apply this technology to Critical Infrastructure Protection (CIP).

#### Objectives of the project:

- Enhance the reliability of critical infrastructures by providing reliable and trustworthy data to the control center of the CI.
- Increase the dependability of critical infrastructures security, by providing selfhealing and dependability modules for WSN.
- Provide a dependability engineering methodology and appropriate tool support.
- Demonstrate the feasibility of our approach using: I) energy generation and distribution, and II) drinking water distribution, as representatives of critical infrastructures.

#### Challenges addressed by WSAN4CIP:

##### WSAN methodology and design

Engineering of dependable WSN applications will be assisted by a service composer tool applying formal descriptions of the application requirements and of the software modules of the WSAN4CIP library.

##### Sensor node protection

We will increase the dependability of current sensor platforms by developing innovative virtualization techniques for the operating system. The detection of compromised nodes will be performed through enhanced software attestation. Moreover, WSAN4CIP will reprogram deployed nodes with over-the-air upgrade mechanisms.

##### Dependable sensor networking

To increase the reliability of all networked services, we will develop MAC, routing and transport protocols with tuneable security, QoS and energy efficiency parameters. We will also look at network coding techniques to enhance transport and storage in WSNs.

##### Dependable sensor service

WSAN4CIP will develop intelligent middleware to enhance fault detection and fault resiliency beyond the state of the art. It will take advantage of the nodes redundancy to build fault-tolerant, self-organizing services that meet the application needs, ensuring service QoS and lifetime.

##### On-site demonstrators

In 2011, two comprehensive demonstrators in energy and drinking water distribution scenarios will show the applicability of the developed WSN modules for the protection of CIs. Moreover, they will meet the requirements of the utilities partners and interface to their SCADA management system.



#### Consortium:

<b>EURESCOM</b>	Germany
<b>IHP Microelectronics</b>	Germany
<b>NEC Europe Ltd.</b>	U.K.
<b>INESC Inovação – Instituto de Novas Tecnologias</b>	Portugal
<b>Energias de Portugal Distribuição</b>	Portugal
<b>Budapest University of Technology and Economics</b>	Hungary
<b>INRIA</b>	France
<b>Luleå University of Technology</b>	Sweden
<b>SIRRIX</b>	Germany
<b>Tecnatom S.A.</b>	Spain
<b>Universidad de Malaga</b>	Spain
<b>Frankfurter Wasser- und Abwassergesellschaft</b>	Germany

WSAN4CIP is an FP7 STREP project, which is partly funded by the European Commission. It started on 1 January 2009 with a duration of 3 years and a total budget of 4 million euro. This flyer expresses the views of the WSAN4CIP consortium; the European Commission has no responsibility for its content.