Integral and Networked Home Automation Solution towards Indoor Ambient Intelligence

3^{nd} version

Miguel A. Zamora-Izquierdo, José Santa and Antonio F. Gómez-Skarmeta
Department of Information and Communications Engineering
Computer Science Faculty
University of Murcia, Spain

Submitted on 9 November 2009

***Abstract*—We have been listening for a long time to the wide functionality that home automation technologies can offer for improving our lives and adding security to our houses. However the price and an unstable domotics market have restricted the deployment of such systems. Nowadays, companies offer too technology-dependent solutions which do not cover user demands completely. Meanwhile, works in the literature focus on small innovations on specific parts of home automation systems, which do not consider integration and deployment issues in order to present practical designs. The system presented in this work considers user requirements, including novel advances, all in an integral home automation solution suitable for many services. The modular nature of the architecture allows direct adaptation to specific cases using standard domotic technologies, for managing in-house devices, and a proposal of an IP-based network for connecting the main home automation module with the rest of platform elements. A remote security system has been developed and managing tasks are enabled by in-home control panels and an advanced 3D application for local/remote homeowner access. The system has been deployed on a prototype house, where a wide set of domotic services have been tested. Moreover, the range of indoor pervasive applications has also been extended to eHealth, elderly adaptation, greenhouse automation and energy efficiency.**

***Index Terms*—Home Automation, Domotics, Service Gateway, In-home Networking, Ambient Intelligence.**

CONTEXT

There is limited knowledge about what home automation (or domotics) exactly is. People usually understand this concept as "a set of expensive gadgets which make the house smart", and a large part thinks that domotics is not essential. Probably they were right some years ago, but perhaps an up-to-date and whole explanation about what current technologies and home automation systems can offer could persuade them. Initial solutions which switched on the lights when the inhabitants were present, have given way to automated systems which are able to control the operation of most appliances, windows, lighting, blinds, locks, etc., and, what is more and more demanded, monitor the house state.

The main fields where home automation can be applied are security, entertainment, labour-saving white goods, environmental control, eHealth and remote control [1]. The potential customers of such systems are working adults who need to save time, an ageing population which needs assistance and users wanting a remote control of the house. Thus, the number of services offered and the wide variety of clients make the adaptation of commercial solutions a challenge for companies involved in the sector. Such adaptation must also take into account the usefulness of the system in the target environment. The boundary between a system which helps inhabitants with daily tasks, and a system which performs undesired automatic actions, is sometimes narrow [2]. And this is the reason why it is necessary to identify **user requirements** of home automation solutions. These generally fall into the following groups:

- Efficient automation of routine tasks.
- Security of automation systems.
- Easy to use.
- Local and remote access.
- Tele-monitoring.
- System cost and flexibility.

Probably obviating the previous requirements, the domotics world has been immersed in a competition of communication standards and specifications since early 90's [3]. Nowadays the state of wired domotics protocols, in Europe at least, is more established, and EIB (European Installation Bus) appears to be the most used specification; however, a similar problem has recently arisen in the field of wireless communication technologies, due to continuous advances in the area of in-home networking. Apart from initial radio-based solutions and the more recent Bluetooth, new wireless communication technologies are suitable for home automation [4]. ZigBee and Z-Wave are currently competing to become the in-home networking reference of future houses. The solution presented in this paper uses EIB and ZigBee as main technologies to communicate with in-home appliances, but proposes an IP-based communication protocol between the main controller of the house (home automation module) and the rest of local embedded computers and remote equipments.

BACKGROUND

The most common design approximation in home automation until now has been considering user's needs and current technologies to deploy ad-hoc solutions. This methodology has led to works which are too technology-dependant, even present in the research world. In [5] authors describe a home

automation system based on an Internet-accesible server. This hosts a Java application which manages a set of digital I/O lines connected to some appliances. A similar solution is described in [6]. However, communication with appliances is now carried out using a radio frequency (RF) link and a non standard management protocol. This requires slave nodes which supports the protocols over the RF link to be deployed in the house and wired to appliances. Our work, apart from supporting digital I/O (and other inherited communication technologies), is compliant with standardized protocols in domotics. The work presented in [7] is focused on the specification of the logical model of the house and appliances, in order to enable the implementation of IF/THEN sentences to manage the devices. Although the gateway has been developed, the work lacks integrating it in a whole automation solution. Furthermore, another issue which clearly differentiates that work of ours is the integration of critical automation tasks in a PC-based gateway. We bet on a high reliability solution based on an embedded home automation unit instead.

In these previous works researchers try to solve scalability issues and also offer different remote management capabilities through Internet. The previous works are mainly centered on the home automation unit, highly linked to a Web-based gateway. However, there are more elements to be considered in an integral home automation solution. A suitable HMI (human-machine interface), not only by means of a gateway, but also using local control panels, have also been developed in our solution. Likewise, a complete security system for the house involves the communication with more entities, such as the local security staff and the security company. Moreover, an insufficient security treatment for IP-based communications in current solutions is also noticeable. The platform presented in this work covers this lack by means of secure communication channels.

A concept which is gaining a gradual importance these days is ambient intelligence. The penetration of this idea in home automation is more and more evident in the literature, and proposals which offer context-awareness and ubiquity capabilities are being introduced on the automation basis in order to provide houses with real intelligence [8]. This work adapts ambient intelligence concepts to the special case of assisted living systems, field in which our platform has also been applied successfully [9]. In [10] authors present a research project where a house has been automated to offer pervasive services to inhabitants. Although interesting ubiquitous services are proposed in that work, thanks to the wide deployment of sensors, actuators and a pervasive middleware, the reliability of the system is not properly considered. Thus, services are offered by means of a software gateway, which communicates with deployed devices by means of RF. Also, the house security and the remote management and monitoring are not considered in the work. These services are supported by the networked home platform presented in [11]. Although the work only includes the logical model of the architecture, and it is specially focused on UPnP (Universal Plug and Play), the functionalities pretended in the solution are quite similar to the ones included in the architecture presented in the current paper.

THE DOMOSEC ARCHITECTURE

The DOMOSEC (DOMotics and SECurity) platform gives a home automation solution which covers current and future necessities in the indoor domotics field. It avoids a tight dependence on technologies, considering successful experiences, and proposing innovative subsystems. All of this thanks to an analysis, design, implementation and deployment of an entire home automation, management and monitoring architecture. This underlying architecture is used to provide common domotic capabilities, but taking into account the design of an integral platform to offer novel pervasive services.

The whole architecture of the DOMOSEC system is showed in Fig. 1. As can be seen, the platform is divided into the in-home system, the supporting security infrastructure and the homeowner remote access subsystem. External entities communicate with in-home subsystems by means of Internet. Two different methods of external connection are provided. First, the local gateway enables homeowners to monitor/manage their houses by means of an authenticated HTTP (Web-based) channel. Second, the home automation module communicates with security modules and remote gateways using a secure UDP protocol later explained.

Although the diagram showed in Fig. 1 considers all the possible elements of a complete configuration for automating a building, the system is completely modular and only the home automation module is mandatory. Moreover, the generic nature of the system enables us to apply the automation architecture not only in houses, but also in offices, schools, shopping centers, hospitals, resorts and, in general, any other domain where domotics and indoor automation take place.

Home Monitoring and Control

The main element of the architecture is the **Home Automation Module** (HAM). This comprises an embedded computer which is connected with all appliances, sensors and actuators. In this way, the HAM centralises the "intelligence" of the house, since it contains the configuration used to control all installed devices.

The HAM module includes an optional human-machine interface, as explained later. In addition, several **Control Panels** can be spread in the house in order to control specific parts of the building. These comprise an embedded solution with an HMI adapted to the controlled devices. For example, in a three-storey office building, each floor could have a control panel, in order to set the automatic opening of windows, switch on the air conditioning to set the desired temperature, or close/open the blinds according to the desired light intensity before using artificial lighting. These examples are developed cases of study which diminish the power consumption and contribute to environmental preservation.

The **Local Gateway** offers value-added services for management and monitoring tasks, but it is not in charge of

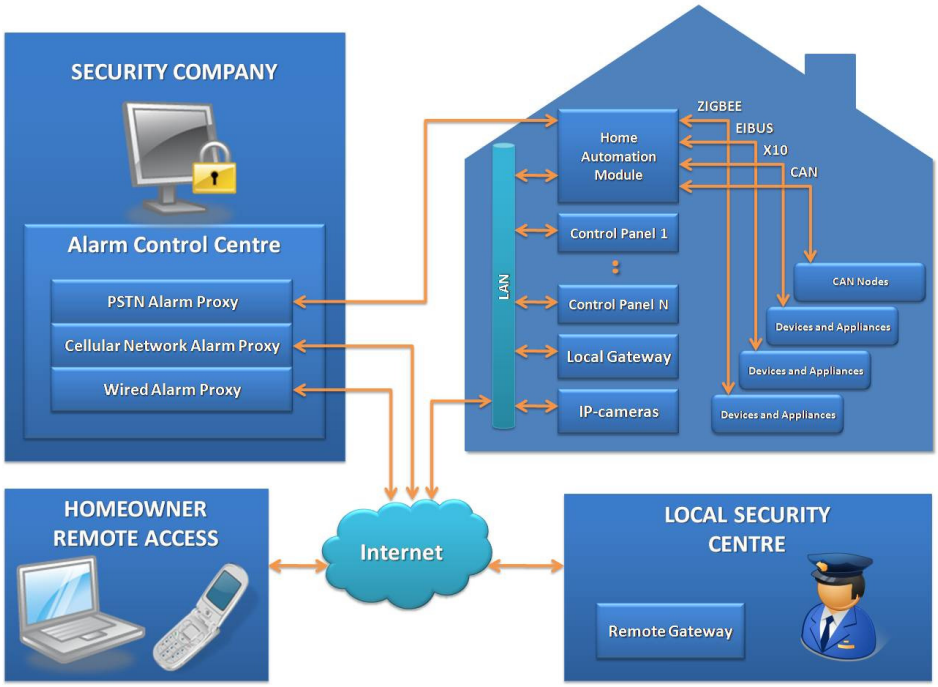


Figure 1. Overall home automation system provided by DOMOSEC.

performing any control over appliances or actuators directly. Instead, this gateway communicates with the HAM using a UDP-based protocol later explained. Some other solutions leave these tasks to a PC-based gateway, which is understood as a not appropriate strategy. In [12] a software implementation of a gateway is also used as automation station, which is executed over a common PC/Java platform. The embedded solution used in our HAM proposal offers a fault-tolerant architecture and assures the correct operation of devices. A PC-based gateway is used in our architecture to give extra services to inhabitants, and perform networking tasks from the transport to the application layer in the OSI stack, as described in [13]. The OSGi (Open Services Gateway initiative) framework is used in the gateway to manage the life cycle of services which cover these features. Thus, a service which implements the underlying UDP protocol to connect with the HAM enables the implementation of more complex applications; and the HTTP service offered by the OSGi framework is used by a Web application to provide local/remote management capabilities through a 3D interface. Additionally, the homeowner can also use an SMS-based remote control strategy, in the case the wired Internet access being out of service.

In-home Networking

To date, most efforts in designing novel communication protocols in the home automation field have been focused on communicating a home automation controller with appliances. In [14], for instance, a bus-based protocol is defined over the power line. The DOMOSEC system, on the contrary, bets on current specifications to connect the HAM with appliances and the rest of devices, and it proposes a novel communication protocol which connects IP-based elements of the architecture through UDP. As IP-based elements are considered the local gateway, control panels and the architectural elements outside the house, such as the remote technical staff performing maintenance tasks and the remote gateway.

The HAM supports several communication controllers in order to connect with many devices. By complementing the direct digital and analog I/O through common wiring, a CAN (Controller Area Network) bus can be used to extend the operation range or provide a more distributed wiring solution. X-10 connections over the power line are also available for low-cost domotics installations, whereas the EIB controller offers a powerful solution for connecting with more complex appliances. Finally, ZigBee and Bluetooth can be used to avoid wiring in already built houses, for instance.

A LAN installation is used in the house to connect all IP-based elements with the HAM. The LAN technology currently used is Ethernet, but 802.11i is also being considered for future installations where wireless LAN communications are preferable. The in-home network is connected to the Internet by means of a non-fixed communication technology. Common ADSL, ISDN or cable-modem connections could be enough to offer remote monitoring/management and a basic security system.

The SHAP Protocol

We propose the Superior Home Automation Protocol (SHAP) to connect IP-based components of a home automa-

tion system over an IP network. In our architecture it connects the HAM with the in-home and remote IP-based entities, following a sliding window strategy with UDP packets to assure the data flow control.

Management messages are sent from control panels or gateways to the HAM by using the SHAP protocol. Moreover, the SHAP protocol includes a set of messages which are used to flash the microcontroller code memory remotely. We have developed an application which performs this task, which also enables specialists to update the HAM firmware by means of a local Ethernet connection or Internet. In this way, it is possible to reduce maintenance costs. This software is later explained in the paper.

Since home networks accessed from outside imply a number of security issues [15], the SHAP protocol implements an approach based on symmetric cryptography and hash algorithms to assure the authenticity and integrity of messages transmitted. Confidentiality is not directly provided for the packet payload because encryption is supposed to be included only in desired messages. For example, applying encryption to the payload is unnecessary for memory map messages, when the HAM memory is flashed, because decoding all packets would delay the process. Alarm messages, on the other hand, can offer encryption by themselves. At the service level, confidentially is offered by means of a secure HTTP access. In the same way, remote clients are authorised to access the 3D monitoring application by an authentication stage executed at the beginning of the session.

Distribution of Configuration Data

The HAM is in charge of maintaning the main database of the house configuration. A local non-volatile memory is used for this purpose. This database also saves the actions to be executed according to periodic or programmed tasks, or sensor-dependant conditions. In addition, each control panel and the local gateway include a local database synchronized with the main one in order to avoid the overload of the network. In this way, users can perform changes in the operation of automated devices using control panels, but these annotate changes in device status and update the interface only when they receive the confirmation of the action from the HAM. This communication is carried out by using SHAP messages and assures consistency of local databases. Communication between local and remote gateways with the HAM follows the same strategy. The database stored in the remote gateway is a part of the whole house state as well, because it is only related to security sensors. However, the database maintained by the local gateway is a complete copy of the one stored in the non-volatile memory of the HAM, since management capabilities included in it comprise a whole control over the house.

Securing the House

Due to the relevance of safety services in current home automation systems, the DOMOSEC architecture includes an integrated security system. Local sensors connected to the HAM, such as presence, noise and door opening detectors, are used as inputs for the security system. As it can be seen in Fig. 1, there are several entities, called **Alarm Proxies**, which are in charge of receiving security events from houses. These proxies are logical entities (i.e. software) which run on servers located at the security supplier. This security model, although it is not part of any standard or specification, it is common in the systems used by security companies. DOMOSEC interfaces with the software installed at the security company, called **Alarm Control Centre** in Fig. 1. All security events received by alarm proxies are forwarded to this software, this time using standardized alarm messages.

There are several types of alarm proxies. The wired one has been recently introduced by security suppliers, using a common Internet access. Nevertheless, the platform supports proxies which use cellular network (CN) or the public switched telephone network (PSTN). The CN-based solution requires a modem in the HAM, and the CN operator offers a direct access to Internet. Internet-based alarm proxies receive security notifications by means of alarm messages defined in the SHAP protocol. In the case of using the PSTN connection, a tone-based codification is used to send security events. This one is the most common among security companies. These three types of alarm proxies can be combined in our architecture and, in fact, more than one of the same type can be included to offer an extended reliability. Alarm events are simultaneously notified through all available alarm proxies and a "keep alive" strategy is used to receive periodic messages from the HAM. This mechanism prevents an attacker from blocking the security channel without being detected.

The payload of alarm messages are usually processed by security companies following a standardized format. The system currently supports Ademco Contact ID. However, it is envisaged to support other message formats, like 4+2. At the connection stage, the HAM negotiates the message format to be used in further security notifications with alarm proxies. This handshake is part of the SHAP protocol. The alarm proxy initiates the process and, after receiving a set of message formats supported by the HAM, replies with the selected one.

Sometimes, automated houses are included in an administrative domain (e.g. housing developments) and monitoring/securing tasks can be applied by local staff. The **Remote Gateway** is included in the architecture with this purpose. A remote gateway is used in these cases to receive security events from houses. This could be a preferable option for medium/small administrative domains, instead of using local gateways. The remote gateway contains a modified version of the software installed on local gateways, hence, it is able to connect with individual HAMs and attend to security events from all controlled houses. In some configurations, the remote gateway could be located in the same IP network as controlled houses, but Fig. 1 shows the general case.

SYSTEM DEVELOPMENT

The DOMOSEC components described in the previous section have been developed. All prototypes presented here

are part of a real deployment of the system in a testbed house, although some hardware components are showed out of their installation point to make easier the explanation. Regarding application screenshots, they comprise real scenarios of usage.

Home Automation Module

The home automation module is based on the SIROCO (System for Integral contROl and COmmunications) hardware architecture, designed at the University of Murcia for automation purposes. The different modules which comprise the unit can be seen in Fig. 2. SIROCO is a modular system highly adaptable and compliant with current regulations (EN-50131 and EN-50136). Related works in the literature often plump for too simple and non-flexible architectures. In [16], for example, the automation module designed offers an embedded solution with basic I/O capabilities which needs the support a an external PC software. On the contrary, SIROCO gives a self-sufficient platform to perform management and monitoring tasks. It offers the option of installing a low-cost solution or a complex one, extending the base system with the required modules.

The heart of the HAM system is a 32-bit ARM microcontroller. The MPU (Main Processor Unit) Board is equipped with basic I/O capabilities through common serial and parallel interfaces, and an Ethernet connection to the IP network. The MPU board is the basis of both the HAM and control panels, and the display is connected by a serial interface. The HAM, however, is extended with more communication capabilities. Specific domotics communications are provided by the X10 module, connected through a serial interface, and an EIB controller, integrated in the MPU Board. The user interface (if needed) is a 5.6" colour touch screen. An alternative low-cost user interface can be integrated, by means of a 16-button touch pad plus a character LCD. The MPU board is extended with two additional boards: the communication and the I/O boards.

The Main I/O Board provides extra wired interfaces with appliances, sensors and actuators. It is possible to add up to 16 Lateral I/O Boards connected to the Main I/O Board. With this configuration, complex control schemes can be tackled. The Communication Board is equipped with ZigBee and Bluetooth interfaces and an extra wired connection through the CAN bus. Moreover, small CAN node boards with dimmers and additional remote I/O have been developed to provide connectivity with a wide range of home automation devices (lights, shutters, etc.). CAN bus offers an alternative to EIB when a more flexible communication channel with wired sensors (not necessary EIB-compliant) is needed. Finally, a cellular modem (GSM/GPRS/UMTS) and a phone interface (DTMF) are included to send security events to alarm proxies.

Fig. 3 shows a HAM with HMI capabilities, using the touch screen. This HAM has been installed on the back of the main entrance of the prototype house, near the electric panel, as can be seen in Fig. 3(a). Fig. 3(b) shows in detail the electronic components of the HAM prototype. On the left part, the Main I/O Board is fixed on the base of the plastic casing, connected to the MPU Board located above it. The Communication Board would be connected above the latter, but it has been removed for clarity. The rest of the hardware included in the prototype of the photo comprises the battery, provided to prevent system failures in power cuts, the power supply, near the top part of the battery, and, finally, an X10 module on the right.

Control Panels

Control panels are based on the MPU Board of the SIROCO architecture. They guarantee a familiar HMI, equivalent to that offered by the LCD-based HAM but limited to automated devices in the surroundings. Users can define configuration profiles, which contain a set of device states and actions to be performed under certain conditions. These can be saved using illustrative names, such as "At work" or "Sleeping". Moreover, the house alarm can be armed/disarmed by a defined control panel. Any panel, however, can be used to activate panic, security or fire alarms at any time. When an alarm is activated by the HAM (due to sensor measurements) or manually, control panels warn users via acoustic and visual messages.

The prototypes of developed control panels can be seen in Fig. 4. Fig. 4(a) shows two different versions, one based on a touchpad screen and the other mounted with a button pad and a character LCD. The last one has been recently replaced by the touchpad version in the prototype house, as can be seen in Fig. 4(b). In this case, the user is modifying the lighting intensity in the living room, where the control panel is installed. Fig. 4(c) shows a screenshot of the graphical application included in the touchpad-based control panel. The user is reviewing the configuration of blinds and awnings of the house. Two blinds are used, the first has been set-up to close and open automatically, depending on lighting conditions, whereas the behaviour of the second has been programmed at different times of day. Currently, they are opened at 50% and 60%, respectively. Another version of this application is also available for PDA platforms, to allow an in-home control over a wireless network. Finally, Fig. 4(d) illustrates another control panel designed for an energy-efficient building, project later explained in the paper.

House Setting-Up Software

The setting-up application allows specialists to locally or remotely access the house configuration by connecting with the HAM. The application can use a UDP/IP access, via the SHAP protocol, or a direct serial connection with the HAM. Fig. 5 shows a screenshot of the application while we were establishing the keys to be used in the communication with the HAM. The software also monitor X10, EIB and UDP communications with the HAM.

The software enables the installer to configure the different partitions and zones of the security system, set the devices connected to the system, and define the remote accesses allowed from outside. All this information is stored in the HAM database. The HMI allows the installation of initial profiles and actions to be performed under certain events detected by

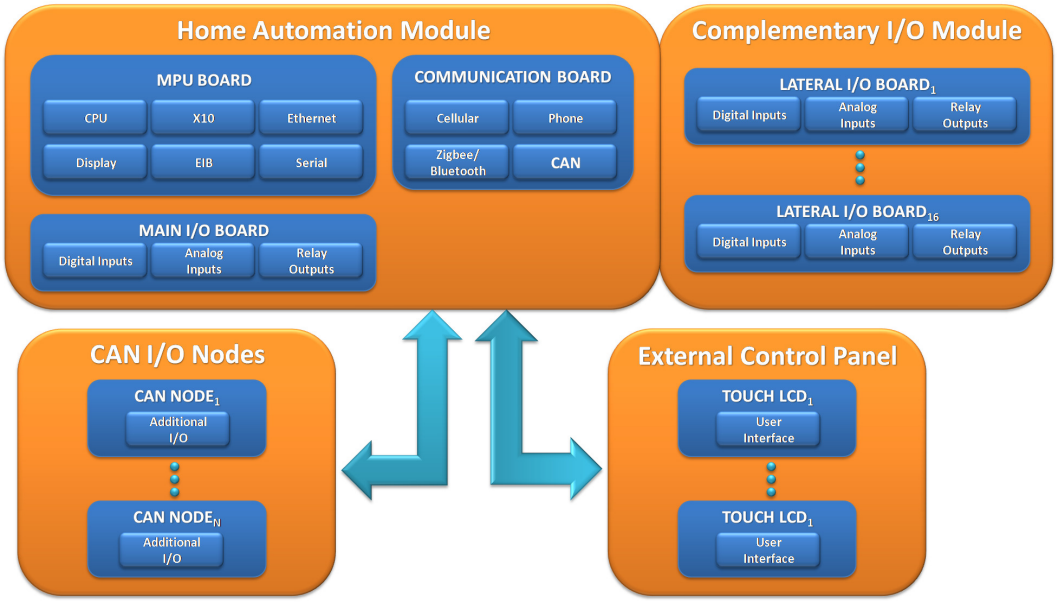
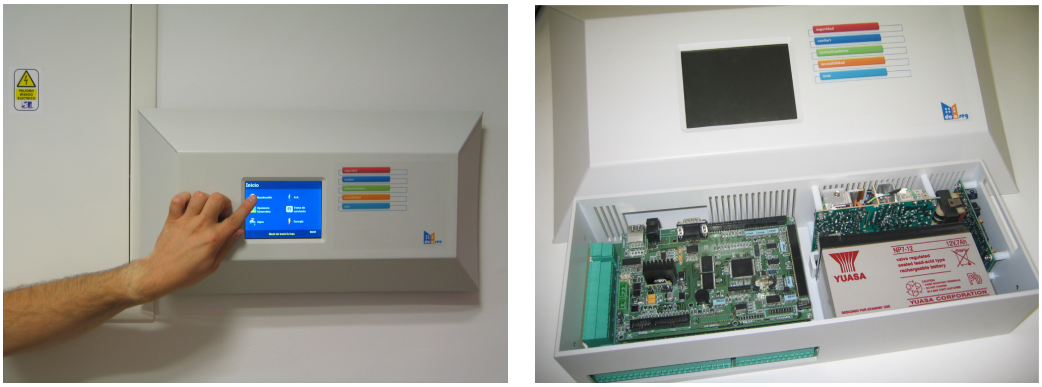


Figure 2. Logical diagram of the home automation module and its communication capabilities.



(a) HAM installed in the testbed house.

(b) Boards and electronics of the HAM.

Figure 3. Home automation module.

sensors. All settings can also be saved for application to other houses.

Home Management Application for Local/Remote Access

In addition to control panels and the optional HMI of the HAM, a local/remote management application offers users monitoring and control capabilities over the house. This application is hosted in a HTTP server at the local gateway. It includes a Flash program which is downloaded from the server to the client machine and gives an extended view of the whole house.

The homeowner, by using this application, has a 3D view of the house and can manage the automation system as if he/she were at home. An IP camera has been used in the prototype house to offer a real-time video monitoring of the house. Fig. 6(a) shows a screenshot of the application, where we are checking the state of the living room. The 3D map of the house is also visible in the screenshot. In Fig. 6(b) the user has rotated the view, and is currently modifying the lighting configuration to activate it automatically when the sunlight is poor.

The application has been designed as a module-based software, using graphical plug-ins for the desired parts of the house. Technical staff will be in charge of creating such modules according to house specifications. This task would be only performed once in the case of blocks of houses. Configuration of devices installed in the house is dynamically requested from the same local gateway, which maintains a local copy of the house settings. Thus, for example, the software can access the IP cameras using the URL provided by the local gateway.

A variant of this application, with security capabilities, has been designed to be installed on remote gateways. By means of this software, security staff in resorts or housing developments can monitor all automated houses. This version of the Flash application centralises the reception of alarms from houses

(a) Control panels with touch screen and button pad interfaces.

(b) Control panel installed in the testbed house.

(c) Touchpad version of the control panel software.

(d) Control panel for an energy-efficient building.

Figure 4. Control panel prototypes.

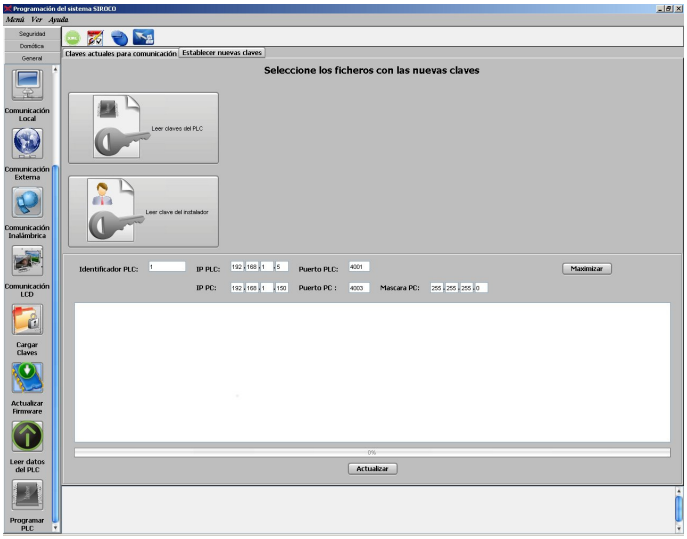


Figure 5. Screenshot of the house setting-up software.

and includes basic features to control certain devices, such as the hall lighting, security sensors and audible alarms. This scheme reduces the price of the system deployment for low-cost installations, because monitoring tasks can be left to security staff, and local gateways would not be necessary, for example.

EXPERIENCE

Prototype House

A diagram of the testbed house considered in the work can be seen in Fig. 7, including the deployment of most relevant sensors, actuators, automated appliances and management devices of DOMOSEC. By means of a set of automated switches, appliances located in the kitchen can be controlled by the HAM. The intensity of the lighting is also controlled independently for each room. The security system uses presence sensors and a robotic camera to receive information about the status of the house. As can be seen, the HAM has been installed at the entrance and a control panel is located in the living room. While the HMI of the HAM offers management capabilities over the whole house, the control panel is specially focused on the automation capabilities of the living room. Among these features, a smart management of lighting is performed, in order to automatically adjust its intensity, and the position of blinds and awnings, according to natural light. A PC-based local gateway has also been included in the testbed and it is connected to an LCD television. This gateway also hosts the 3D management software, which enables the homeowner to access the house remotely. The temperature of the house can also be adapted to user's preferences, au-

(a) Overall house view.

(b) Setting-up the lighting of the living room.

Figure 6. Flash application with 3D HMI for local/remote management.

tomatically switching on/off the centralized air conditioning and the heating. The power consumption is also monitored by the HAM, thanks to the adaptation of the electric panel.

Regarding the communication protocols used to connect the various devices with the HAM, we have covered a wide spectrum of the supported standards. Three inherited X10 switches, connected to the power line, have been installed in the kitchen. EIB has been used for communicating with the presence sensors installed in all the rooms. The most used communication technology is CAN. The lighting, heating, automated blinds and awnings, and light sensors are connected in this way, deploying CAN nodes in the house. Finally, a serial communication is used to connect the electric panel and the air conditioning with the HAM, using RS-485. IP-based devices are connected to the in-home network using Ethernet. These devices comprise the local gateway, the control panel and the IP camera.

Since most of the sensors are wired with the HAM, it has been found very useful to build the house considering the DOMOSEC installation. For devices installed during the system exploitation, which can not be easily connected to the deployed communication infrastructure (CAN, EIB or common I/O lines) or the Ethernet network, they can use a ZigBee or Bluetooth link. Some temperature sensors have been installed in this way, for example, using the Home Automation Profile of ZigBee.

The security system has also been deployed, supporting PSTN, cellular network and wired alarm proxies. Hence, a security company only need to include this software middleware in its system. For the wired connectivity, which is also used in the remote access, a common ISDN link has been used. The security middleware has been integrated in the information system of a security company. All the proxies has been installed at the company offices and a wide set of scenarios have been successfully tested. Thus, we have intentionally blocked one or two of the communication channels to check the operation of the system. Alarm messages, formated using Ademco Contact ID, have been decoded correctly by the private security software in all scenarios when, at least, one of the three security channels (PSTN, cellular or wire) is available.

Lessons Learned

During the last years of improving DOMOSEC, from a simple automation node to the current platform, we have identified the necessity of migrating from proprietary designs to open platforms. In this sense, common digital I/O wires have given way to EIB and CAN, for instance. A problem we are currently facing is the transition from standalone displays to panel PCs. The price of these devices is decreasing, in contrast to the high cost of independent touch screens, and they offer a more powerful platform to develop friendly interfaces. In the same way, the core processor of the HAM has evolved from a low-end PIC to the current 32-bit ARM. At the moment we are evaluating several x86 and new ARM processors, to migrate to a HAM based on an embedded operating system, like Familiar Linux. According to our experience, it is important to choose a robust processor with a secure manufacturer support, since ours is planed to be removed of the market soon and this imply a number of maintenance problems.

An important aim of our work has been to reach a useful and efficient solution for the remote components of the architecture. In that sense, we identified the alarm control centre as a key element to assure the correct reception of security events. Although our first versions of this software were installed in high-performance servers, we experimented some non-recoverable message loses when the system was tested in high stressful conditions (in the order of thousand houses being controlled and notifying security events). For this reason, we created two new software entities: the reception and attendance units. The first one only pre-processes security notifications quickly, and then passes the event to the attendance unit, where the event is entirely processed and finally passed to the alarm control centre. Although only a backend system exists, in this case the alarm control centre, both the reception and attendance units can be replicated, if needed, among different servers. This idea is being applied to remote gateways

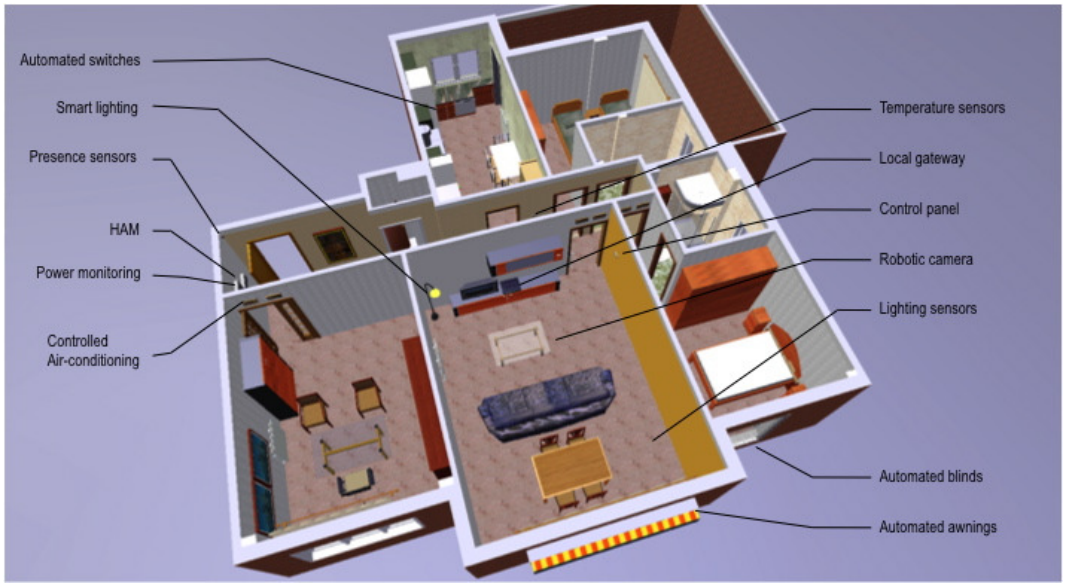


Figure 7. The prototype house used as testbed of the DOMOSEC platform.

as well, since they may be in charge of many houses or houses with many (security) sensors. Moreover, in order to improve monitoring and management tasks in such schemes, our next step is the development of a complementary SCADA (Supervisory Control and Data Acquisition) software, not as pretty as the 3D application, but more practical for security staff. Whereas Flash is a proprietary platform, our SCADA software will be based on a Java and Web basis.

When we started deploying the DOMOSEC system in the prototype house, we had to face several problems which were not identified at previous stages. One of the most important complications was the integration of DOMOSEC with the electric system. Apart from the extra connections needed for the HAM and the control panel, sensors and actuators also need a power supply. Moreover, since we manage the light intensity independently for each room of the house, it is necessary to adapt lighting circuits and wiring. Regarding the installation of components, a redesign of the cases was necessary to hold all necessary digital I/O wires, serial interfaces, Ethernet, etc. In any case, the modular nature of the system has been one of our major successes. The distribution of capabilities among the different elements of the platform has not diminished the robustness of the system, and since early stages the communication among components has worked properly.

Since the installation phase implies several tricky tasks, we have identified a testing protocol to assure the proper operation of the system. For automation platforms as distributed and integrated as the DOMOSEC one it is difficult to make sure that all is correctly set-up. The list of subsystems that must be checked in order of preference is:

1. Power supply of all devices.
2. Local digital I/O lines with HAM(s).
3. Communications via CAN bus and X10.
4. Serial communications.
5. EIB communications.
6. ZigBee and Bluetooth communications.
7. IP in-home communications via Ethernet.
8. IP remote communications via Internet and PSTN.
9. Software configuration of HAM(s).
10. Hierarchical communication of HAMs (in case more than one is considered).
11. Software configuration of control panels.
12. Communications between gateways and HAM(s).
13. Testing scenarios.

As can be noted, most critical devices are always checked first; hence, the set of sensors, appliances and actuators and their connection with the HAM are attended in first stages. Apart from this manual check, we have envisaged the implementation of self-checking software at the HAM and gateways, with the aim of making the installation phase easier. This middleware would also be useful to improve maintenance tasks and assure the robustness of the platform after the installation.

OTHER STUDY CASES

The DOMOSEC platform has been applied in more environments, exploiting its potential in other ambient intelligence scenarios. The most significant ones are briefly introduced next:

Greenhouses: The DOMOSEC system has been applied on automating greenhouses in a parallel research project at the University of Murcia. The main objective of the system lies in saving resources in ventilating and lighting. By processing information received from temperature, humidity and light sensors, it is possible to control several automated parts of the greenhouse, such as windows, lighting and cooling and heating systems. In this way, it is possible to save power consumption and take advantage of natural resources.

Elderly adaptation: Old people are potential users of the system, hence several of our research lines are addressed to make the control and management of the house easier. An intelligent remote control, for example, is being developed to learn current configurations of nearby devices and save reusable profiles. These remote controls are able to manage the closest device following a friendly design which includes only the most necessary buttons. In this manner, it is possible to open/close the blinds, turn up/down the air conditioning or open/close a window, just by walking towards the automated device.

eHealth: We have worked on an architecture to offer eHealth capabilities on the basis of the DOMOSEC platform [9]. A novel system has been designed using chronobiological algorithms to (tele) determinate several illness factors which imply tele-assistance. Complementing the base DOMOSEC system, a belt and a bracelet have been designed with a set of monitoring sensors: electrodes to capture the heart beat, stain gauges to estimate the corporal position, a temperature sensor and an accelerometer to detect inactivity or falls. The whole platform can also be applied to different care-delivering environments: public service providers (such as hospital, nursing homes or old people's homes), private entities (such as insurance companies or care institutions), and the patient's house itself, taking advantage of the platform flexibility.

Energy efficiency: DOMOSEC has also been applied in a new smart building project at the University of Murcia, whose main purpose is energy efficiency. The roof of the building is a big solar panel, and the interior has been automated to make the most of the power used. Each floor has a HAM to control all common areas, whereas each working zone has another one to monitor the water and power consumption, adapt the lighting according to natural light, detect fires and floods, or automatically switch on/off several devices. A control panel has been installed in each working zone to offer the HMI for these capabilities. This can be seen in Fig. 4(d), together with the adapted electric panel and the optional manual control of the air conditioning. All HAMs in the building have control access capabilities, by using smart cards, and a gateway has been set-up at the reception position to enable the remote management of all of them.

CONCLUDING REMARKS

The architecture presented gives an integral indoor automation solution suitable to deploy common domotic or novel pervasive services, as we have seen in the different projects where DOMOSEC has been applied. The evolution of the platform is directed now to assisted living scenarios, such as the elderly adaptation one, and environment preservation. A new project will exploit the idea of sustainable campus at the University of Murcia, reducing the energy consumption by means of novel techniques of tele-monitoring and management of resources. Moreover, we are currently defining a new research line to apply the HAM architecture in secure and mobile 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) communications. Sensor networks will be used to collect environmental information but, since the computational capabilities of these devices are quite restricted, due to consumption and size constraints, we propose to integrate SIROCO as a security and mobility proxy. In this way, by deploying these proxies as supporting infrastructure, the extra overload which supposes secure communications, ad-hoc mobile routing protocols, and even the data collection, would be quite reduced.

ACKNOWLEDGEMENTS

This work was supported by the Spanish Ministry of Industry, Tourism and Commerce, under the project Intelligent Beds TSI-020100-2008-536, the Spanish Program to Aid Groups of Excellence of the Séneca Foundation, under grant 04552/GERM/06, and partially by the Spanish Ministry of Education, under the project SEISCIENTOS TIN2008-06441-C02.

REFERENCES

[1] K. Sangani, "Home Automation - It's no place like home," *IET Engineering & Technology*, vol. 1, no. 9, 2006, pp. 46-48.

[2] S. S. Intille, "Designing a home of the future," *IEEE Pervasive Computing*, vol. 1, no. 2, 2002, pp. 76-82.

[3] K. Wacks, "Home systems standards: achievements and challenges," *IEEE Commun. Mag.*, vol. 40, no. 4, 2002, pp. 152-159.

[4] J. Walko, "Home control," *IET Computing & Control Engineering J.*, vol. 17, no. 5, 2006, pp. 16-19.

[5] A. R. Al-Ali and M. Al-Rousan, "Java-based home automation system," *IEEE Tran. Consumer Electronics*, vol. 50, no. 2, 2004, pp. 498-504.

[6] A. Z. Alkar and U. Buhur, "An internet based wireless home automation system for multifunctional devices," *IEEE Tran. Consumer Electronics*, vol. 51, no. 4, 2005, pp. 1169-1174.

[7] R. J. Caleira, "A web-based approach to the specification and programming of home automation systems," *Proc. 12th Mediterranean Electrotechnical Conf.*, 2004, pp. 693–696.

[8] J. Nehmer, M. Becker, A. Karshmer and R. Lamm, "Living assistance systems -An ambient intelligence approach-" *Proc. ACM Int'l Conf. Software Engineering*, 2006, pp. 43–50.

[9] A.J. Jara, M.A. Zamora and A.G. Skarmeta, "A wearable system for Telemonitoring and Tele-assistance of patients with integration of solutions from chronobiology for prediction of illness," *Ambient Intelligence Perspectives*, IOS Press, 2008, p. 221.

[10] S. Helal, W. Mann, H. El-Zabadani, J. King, Y. Kaddoura and E. Jansen, "The Gator Tech Smart House: A Programmable Pervasive Space," *Computer*, vol. 38, no. 3, 2005, pp. 50-60.

[11] A. Meliones, D. Economou, I. Grammatikakis, A. Kameas and C. Goumopoulos, "A Context Aware Connected Home Platform for Pervasive Applications," *Proc. Second IEEE Int'l Conf. Self-Adaptive and Self-Organizing Systems Workshops*, 2008, pp.120–125.

[12] P. Pellegrino et al., "Domotic house gateway," *Proc. ACM Symp. Applied Computing*, 2006, pp. 1915–1920.

[13] F. T. H. den Hartog et al., "Convergence of residential gateway technology," *IEEE Commun. Mag.*, vol. 42, no. 5, 2004, pp. 138–143.

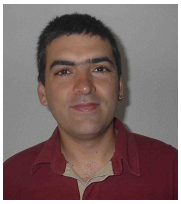
[14] K. Myoung et al., "Design and implementation of home network control protocol on OSGi for home automation system," *Proc. 7th Int'l Conf. Advanced Communication Technology*, 2005, pp. 1163–1168.

[15] P. Bergstrom, K. Driscoll and J. Kimball, "Making home automation communications secure," *Computer*, vol. 34, no. 10, 2001, pp. 50–56.

[16] J. Su, C. Lee and W. Wu, "The design and implementation of a low-cost and programmable home automation module," *IEEE Tran. Consumer Electronics*, vol. 52, no. 4, 2006, pp. 1239-1244.

Miguel A. Zamora-Izquierdo is an Associate Professor with the Department of Information and Communication Engineering, at the University of Murcia. His research interests comprise ubiquitous systems, sensor technologies, automation and control. He received his Ph.D. degree in computer science from the University of Murcia. Contact him at Universidad de Murcia, Campus de Espinardo, Facultad de Informática, 30100 Murcia, Spain; mzamora@um.es

José Santa is a researcher at the Department of Information and Communication Engineering at University of Murcia. His research interests include context awareness, location based services, intelligent transportation systems, and home automation and domotics. He received his MSc in Computer Science Engineering from the University of Murcia. Contact him at Universidad de Murcia, Campus de Espinardo, Facultad de Informática, 30100 Murcia, Spain; josesanta@um.es.



Antonio F. Gómez-Skarmeta is an Assistant Professor at the Department of Information and Communications Engineering at University of Murcia. His research includes mobile communications, pervasive systems, network security and ambient intelligence. He received his PhD in Computer Science from the University of Murcia. Contact him at Universidad de Murcia, Campus de Espinardo, Facultad de Informática, 30100 Murcia, Spain; skarmeta@um.es.