DOI: 10.24427/978-83-65596-71-0_6

6. INTELLIGENT BUILDINGS AND AUTOMATIC CONTROL

6.1. Introduction

Automation systems can be classified according to an array of criteria, which includes length, complexity, application and integration. The application of these systems to the field of habitability defines a specific use of equal or greater complexity to industrial automation. The integration of automation and control systems into buildings improves its operating characteristics, providing them with better services and operations easy to use.

Considering the scope of application, the automation of processes can be classified into three degrees of automation called:

The **monitoring** of the magnitudes of the system to determine the technical and economic aspects.

The **control mode** by the user completes the monitoring and provides information on actions to control the installations in accordance with pre-established criteria.

The **automatic control** has a structure of a closed loop. It includes the acquisition of information and its treatment to provide the actions on the process. The user is still required for the monitoring work. The classic elements of this system are sensors, control system and actuators (Huidobro & Miller, 2004).

Considering the scope of application, the automation of processes is called:
- Domotics (automation of houses),
- Immotics (automation of buildings),
- Urban domotics (automation of cities),
- Macromatics (greater scope automation).

DOMOTICS refers to housing control and automation applied to:

Energy Management: Optimization of services, real time consumption control adapted to energy prices, strategic disconnections, optimal air conditioning, blinds and awnings, among others.

Comfort: Inside and outside lighting, remote communications control, remote sound/music control, voice and special sound recognition, remote door/window operation, remote lighting operation, air conditioning remote control, heating storage, real time scenarios, cleaning and maintenance.

Gardening: Valve control, watering control, water consumption optimization, remote fertilization, environmental monitoring.

Security: Medical alarm, theft alarm, gas alarm, water alarm, CO_2 alarm, fire alarm, smoke alarm, fire service and police communication, presence control and simulation, access control, access restrictions, CCTV surveillance, safety deposit boxes, anti-sabotage systems, security maintenance.

Communication: Internet, preventive maintenance, fax, email, databases, video-conference, events communications, TV, remote communication, print services, telemarketing, advertising time slots, GSM, GPRS, radio.

IMMOTICS refers to the automation processes applied to other buildings, such as schools, universities, museums, hotels or offices.

URBAN DOMOTICS applies to traffic control, temperature, urban transport, suburban transport, emergency resources, pollution, control of utilities (electricity, water, gas, steam). Its application to the generation, transport and consumption of electric energy is a developing area called SMARTGRIDs.

MACROMATICS: by GPRS and satellites (weather, ozone layer, natural disasters, ecological disasters, navigation aid, air control, border control).

6.2 Connectivity and protocols

6.2.1. Automation architecture

Automation structures oriented towards the control of buildings are composed of different layers of integration with physical components (hardware) and logical and programming systems (software), which interact according to different design architectures. The operation of the systems depends on the load on either its physical or its logical structure, allowing the designer to develop levels of automation under digital, combinational or sequential systems.

Digital systems: Physical systems modeled by logical relationships among the output variables (actions) and input variables (data), in a series of predetermined discrete states.

Combinatorial system: A logical system in which the output variables are only functions of the input variables.

Sequential system: The output variables depend on the input variables and also on the order in which they change. Sequential systems are similar to systems with memory.

The systems described above can be implemented under wired or programmed technology based on factors such as scope, complexity, cost, construction integration, expansion flexibility, etc.

Wired technology: The automation is done through modules (electromagnetic relays, pneumatic logical modules or electronic cards) connected by wires or cables. The desired operation of the automation is achieved as a result of the choice of these modules and inter-connection by wiring. All partial logical operations are executed any time giving the results, at the same time, depending on the entries.

Programmed technology: The automation is carried out through the programming of devices (electronic cards, microprocessors, computers and PLCs). The desired operation is achieved by both electronic devices (hardware) and by the logical schema translated into a list of instructions stored in the memory of the program (software). The program written in the memory replaces the choice of elementary functions and the wiring, which would require the automatic version, called "wired technology".

Depending on where the intelligence of the domotic system resides, there are several different architectures:

Centralized architecture: a centralized controller receives information from multiple sensors and, once the information is processed, it generates the appropriate commands for the actuators.

Distributed architecture: the intelligence of the system is distributed through all the modules (sensors or actuators). It is typical of the systems of wiring, either in bus or wireless networks.

Mixed architecture: the decentralized architecture of computers with several small devices is able to acquire and process the information from multiple sensors and transmit them to the rest of devices distributed throughout the house.

The main needs that appear in the building control could be summarized in 5 functions:

- search/scan,

- alarm,
- register,
- display of states,
- automatic regulation (control).

For any of the previous architectures, the control scheme has reference and feedback signals, affected by the corresponding perturbations according to the control diagram shown in Fig. 6.1.

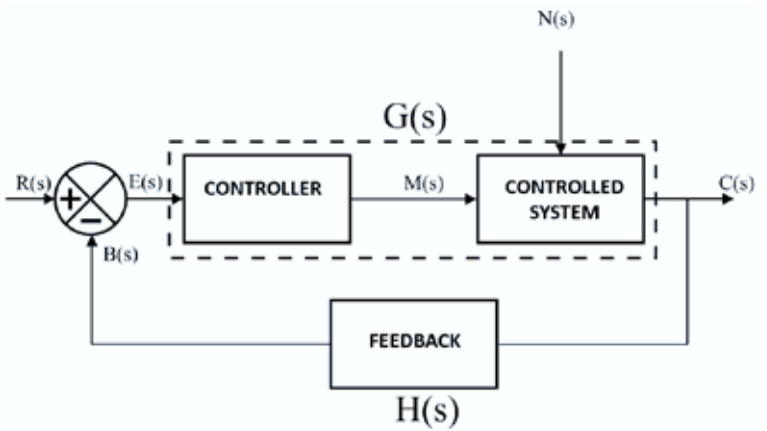

Fig. 6.1. Control standard structure (Source: own elaboration)

6.2.2. I/O devices

The devices responsible for detecting the parameter to be controlled, as well as the ones dedicated to interacting with the system (input/output devices), operate through elements accountable for converting and conditioning physical signals into electrical ones and vice versa, as shown in Fig. 6.2. The elements of the sensor/actuator chain are described below.

Transductor: It is a device that receives the information input as a physical magnitude and then converts this information into another physical magnitude.

Sensor: It is an electric signal transductor. It converts a physical magnitude signal into an electrical signal.

Transmission: It is a "conditioner" that transforms the signal from the transducer into a standard signal.

Analog: 4-20 mA DC # 10-50 mA # 0-20 mA # 1-5 V

Digital: 24v DC # 48v DC # 220v AC.

Signal converter: It is a device that changes the normalized signal into another standard sign with the same physical nature as the input.

Fig. 6.2. Standard signal transformation (Source: own elaboration)

Classifications of input and output devices in automation systems are presented in tables 6.1-6.2.

Table 6.1. Classification of input devices in automation systems (Source: own elaboration)

INPUT DEVICES		
Position	Mechanical devices	limit switch (lever, rod, piston); network switch
	Electronic devices	optical, inductive and capacitive proximity detectors
	Angular position	incremental and absolute encoders
Force/strength/pressure	Sensor	force/strength to deformity
	Transductor	strain gauges, piezoelectric, inductive, tactile sensors
	Transmitter	variable resistor, Wheatstone bridge
Temperature	Sensor	thermocouple, resistance thermometer, thermistor, optic fiber, pyrometer
	Transductor	variable resistor, Wheatstone bridge
Level	Sensor	float, rotate vanes, pressure, conductivity, capacity, ultrasounds, optical, radar

Table 6.2. Classification of output devices in automation systems (Source: own elaboration)

OUTPUT DEVICES		
Actuators	They are usually power receptors that convert the electrical input signal into a mechanical action	motors: electric (rotation or linear), pneumatic, hydraulic
		cylinders: electric, pneumatic, hydraulic
		servo valves
Pre-actuator	It is a part of the controlled system, as well as of the control equipment because it receives the order from the control device and then it executes such order on the corresponding actuator	contactors
		electro valves

6.2.3. Home networking technologies and protocols

The automation and control systems must connect devices that work with diverse levels of electrical signals, different speeds of process, and physical or wireless media. Such adaptation of communications and interaction with external media is produced through different protocols, which establish the standardized procedure to assign priorities, define functionality and optimize the automation. These protocols also establish rules for the operation of control networks, data networks, and interconnection of devices. Below are shown the main protocols used in automation systems in the field of Domotics, as well as a description of its main characteristics.

Interconnection of devices: IEEE 1394 (FireWire), Bluetooth, USB, IrDA

Control and automation networks: KNX, LonWorks, X10, ZigBee, Z-Wave, Bus SCS, LCN

Data networks: Ethernet, HomePlug, HomePNA, Wi-Fi

Table 6.3. Main protocols for Domotics and their characteristics (Source: own elaboration)

PROTOCOL	POWER NET	RADIO FREQUENCY	OPEN SOURCE
C-BUS	NO	YES	NO
IN-BUS	NO	YES	NO
INSTEON	YES	YES	YES
KNX	YES	YES	NO
UPB	YES	NO	NO
X10	YES	YES	NO
Z-WAVE	NO	NO	YES
ZIGBEE	NO	YES	NO

InBus: It is a protocol of communication among different electronic modules, not only for home automation functions.

X10: It is a communication protocol for remote control of electrical devices through the use of electrical outlets without new wiring. It is the most common protocol developed in open source software. This protocol is unreliable with electrical noise.

KNX/EIB: Bus from European installation with more than 20 years and more than 100 manufacturers of products that are compatible with one another. It uses its own wiring and gateways to be applied in wireless systems or even to package the information over the internet or other TCP/IP network.

ZigBee: It is a standard protocol, with reference to protocol IEEE 802.15.4 of wireless communications.

OSGi: It stands for Open Services Gateway Initiative. Open specifications for software that enables designing supporting platforms which can provide multiple services.

LonWorks Protocol: It is an open standard ISO 14908-3 for the distributed control of buildings, housing, industry and transport.

Universal Plug and Play (UPnP): It is an open architecture and software that allows the exchange of information and data with the devices connected to a network.

Modbus: It is an open protocol which allows communication through RS-485 (Modbus RTU) or via Ethernet (Modbus TCP). It is an open source protocol that has been in the market for the longest time and whose devices are manufactured by a large number of companies. Manufacturers are continuously using this protocol device.

BUSing: It is a distributed automation technology, where each of the connected devices has its own autonomy. It is 'useful' by itself.

INSTEON: It is a protocol of communication by double band through current carrier and radio frequency.

6.3. Smartgrids

From a global context, the intelligent electrical network (SMARTGRID) can be defined as the dynamic integration of the developments in electrical engineering, energy storage and the advances in information and communication technologies in the field of electricity and distributed energy resources (generation, transmission, distribution, storage and marketing, including alternative energies). The SMARTGRID allows for

the coordination of areas of protection, control, instrumentation, measurement, quality and administration of energy, etc., by a single management system with the primary objective of performing an efficient and rational use of energy in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply (Source: WEB-1).

Fig. 6.3. Real time SMARTGRID control and monitoring (Source: NASA archive)

According to the previous concept, other actors could also be integrated into the field of the measurement and control, such as gas sources and water service. Thus, smart grids would be a part of intelligent cities (Fig. 6.3).

The efficiency of the intelligent electrical grid is based on the optimization of the production and distribution of electricity to achieve a better balance of supply and demand between producers and consumers. Using smart meters, this network enables consumers to choose best hourly rates, as well as discern between the hours of consumption, which would allow for a better use of the network. This system also allows the user to map and anticipate the energy consumption with more precision.

The irruption of the renewable energies in the energy landscape has changed dramatically the energy flows in the electricity grid. Nowadays users not only consume, but also produce electricity through the same network. So, the flow of energy is now bidirectional. A smart network sends electricity from vendors to consumers using bidirectional digital technology to control consumer needs.

A common element of these networks is the application of digital processing and communication to the electrical network for the management of the essential information from the intelligent network.

Some main characteristics of the Smartgrids are:

Flexibility
- adaptable to the changing needs of the system,
- bidirectional.

Safety
- intensive in the use of infrastructures,
- able to operate in a protected way with simplicity and security,
- providing the necessary information in real time.

Efficiency
- allowing the grid to satisfy the energy needs by minimizing the needs for new infrastructures.

Open development
- allowing safe integration of renewable energies,
- facilitating the development of the electric markets,
- creating new business opportunities.

Sustainability
- respectful of the environment,
- socially accepted.

6.4. The Internet of Things

The Internet of Things (IoT) refers to the digital interconnection of everyday objects with the Internet. It was initiated through research in the field of Radiofrequency Identification in Network (RFID) and sensor technologies.

The Internet of Things should codify about 100 billion objects and follow their movement (it is estimated that every human being is surrounded by at least 1000 objects). With the latest generation of Internet applications (IPV6 protocol), this system can instantly identify any type of object.

The connection of the device to the network through low-power radio signals is the most active field of study on the Internet of Things. The main reason for this fact is that the signals of this type need neither Wi-Fi nor Bluetooth. However, different alternatives that need less energy and that are more economical are being investigated under the name of "CHIRP Networks".

Currently, the term Internet of Things is used for the advanced connection of devices, systems and services that go beyond the traditional M2M (machine-to-machine) and cover a wide variety of protocols, domains and applications. Applications for the

Internet-connected devices can be divided into three main branches: consumption, business, and infrastructure.

The ability to connect embedded devices with limited CPU, memory, and power capabilities enables the IoT to have applications in almost any area. These systems can be responsible for collecting information in different environments, from natural ecosystems to buildings and factories, so they can be used for environmental monitoring and urban planning.

There are other applications of the IoT: in the automatic heating, water supply, electricity, the management of energy, and even in intelligent transport systems. Other examples of consumer applications include entertainment, home automation and household appliances (washing machines, dryers, robotic vacuum cleaners, air purifiers, ovens, refrigerators) that use Wi-Fi for remote control (Nordrum, 2016).

The monitoring and control of operations of urban and rural infrastructure such as bridges, railways and wind farms is a key application for the IoT. It can be used for the surveillance of any event or change in the structural conditions that may compromise safety. This solution can improve the handling of incidents, the coordination of the response to emergency situations, the quality and availability of services, and additionally, it can reduce the cost of operation in all areas related to infrastructure.

6.5. Friendly environment in automation

The previous systems need an interface that allows easy and intuitive communication with a user who is not familiar with programming languages or electronic systems. To this end, the SCADA system (Supervisory Control and Data Acquisition) has been designed. It is a series of software applications specially designed to be used in computers that control and supervise the processes. Main characteristics of the SCADA system are, on the one hand, quick and easy access to the house/building control system and, on the other, the representation of variables.

It is necessary to emphasize its comfortable and friendly environment, which is achieved through its graphical interface where the process of control and supervision is represented. This interface can be displayed on different devices, as required in each case (monitors, touchscreens, etc.).

SCADA systems allow for communication with different devices (e.g. regulators or PLCs) to control any process from the display device (the computer monitor). In addition, control can be modified by the user through SCADA in a simple way. The use of this device can also modify the control variables in real time in a very intuitive

way, because the interface generated with the SCADA is graphic, which makes it simple to understand. Therefore, the SCADA not only shows the different problems generated in the system, but it also gives guidance on the procedures to solve them.

Fig. 6.4. Friendly environment graphical scale examples (Source: own elaboration)

Usually, the term SCADA can be confused with HMI (human-machine interface). All SCADA systems have a GUI user-PC, but not all control systems with HMI belong to the SCADA type. The difference between these two types of devices is the monitoring function that SCADA can perform through its interface. The main supervisory functions are:

- acquisition and storage of data,
- graphic representation of variables,
- performing action control,
- open and flexible architecture with adaptation,
- connectivity with other applications,
- supervision of variables through a monitor,
- transmission of information with field devices,
- databases: management of data in low access times,
- presentation, graphical representation of the data via interface,
- exploitation of data acquired by quality management,
- alert to the user for detected changes.

6.6. Security

The automation and control systems, including the domestic sphere, in addition to providing functionality, must be secure and robust. To achieve this, common risks that may affect the system must be known, so that they can be evaluated.

Therefore, the following items must be ensured:

- protection of electricity supply,
- protection against viruses or malware,
- protection against unauthorized access.

PROTECTION OF ELECTRICITY SUPPLY

The stable electrical current must be maintained, as well as the correct distribution of the electrical fluid and the balance between phases. Continuity of supply can be guaranteed by:

- the UPS in direct mode (from the power net to the UPS, and from the UPS to the installation),
- the UPS in reserve mode (it works only in case of fault of the power net).

Table 6.4. shows electricity supply faults and their effects on installations, whereas Fig. 6.5-6.6 present the UPS operation for electricity protection (conversion AC/DC/Ac or direct supply).

Table 6.4. Electricity supply faults and their effects on installations (Source: own elaboration)

Characteristics UNE-EN 50160	Automation and control effects	
	Severity	Probability
Frequency	MEDIUM	VERY LOW
Voltage variation	MEDIUM	MEDIUM
Quick variations	LOW	LOW
Voltage hollow	MEDIUM	VERY HIGH
Short breaks	HIGH	HIGH
Long breaks	VERY HIGH	MEDIUM
Overvoltage	MEDIUM	MEDIUM
Imbalance in voltage	LOW	VERY LOW
Harmonics	MEDIUM	VERY LOW

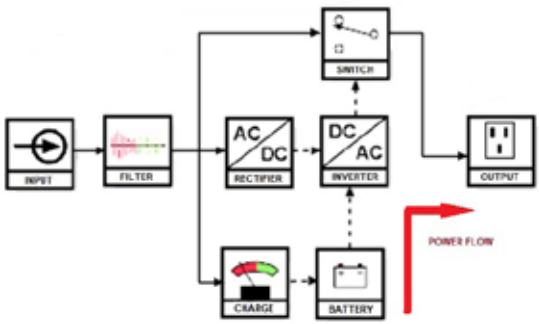

Fig. 6.5. UPS operation for electricity protection by AC/DC/AC conversion (Source: own elaboration)

The most frequent input electrical signal defects are:

Transients or peaks: by network discharges, such as lightning or start/stop of high power machines. They cause damage to electronic devices and a loss of computer data.

Solution: the use of suppressor filter or a direct UPS.

Voltage short variations: by motor connections and stops, and other inductive loads. They cause resets in computers and electronic equipment.

Solution: the use of a line conditioner or a direct UPS.

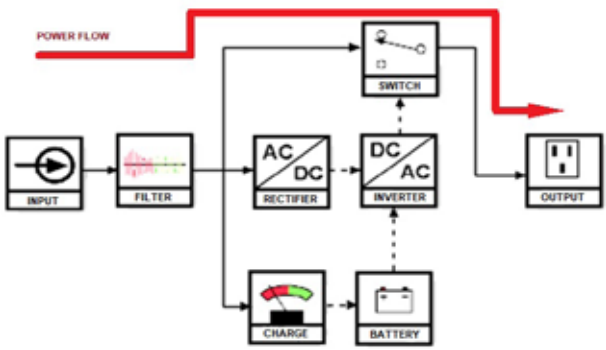

Fig. 6.6. UPS operation by direct supply (Source: own elaboration)

Overvoltages: for management of the electricity distribution network. They cause serious damages in electric and electronic devices.

Solution: the use of a line conditioner or a direct UPS.

Cuts and micro-breaks: failures in the distribution network, lightning and human factors. They cause damage to computers and electronic equipment.

Solution: the use of a direct UPS (on-line).

VIRUS PROTECTION

Industrial and domestic automation and control systems are exposed to the destructive action of external software such as viruses or worms, which can cause improper (even dangerous) operation of the system. An antivirus must be installed, which will slow down the system, but at the same time will improve its security.

In the field of Smartgrids, millions of new devices connected to these networks could become a potential target for hackers. In a sense, a dumb meter is a less hackable device, and therefore a safer one.

To solve the problem of a high number of new meters necessary for the Smart Grid, each of which will take an IP address, the IPV6 allows the new systems to accommodate in a relatively straightforward and secure way.

Smart switches will also be needed for the Smart Grid, which will have to be sturdier than the standard ones used in homes or offices, to operate in hostile environments.

UNAUTHORIZED ACCESS

The operating systems used in computerized automation equipment take measures to prevent or thwart undue connections to the network resources. To monitor and register the strength of systems against undue access, periodic audits should be done on the use of resources.

70% of the IoT devices have security vulnerabilities in their passwords. Thus, there is a problem with data encryption or access permissions and 50% of mobile device applications do not encrypt the communications. These security failures may allow for an interception of the video signal from a CCTV camera, or for revealing the password to the Wi-Fi network where a connected coffee machine transmits information without encryption. Data encryption before uploading the data to the cloud can help reduce this vulnerability.

References

Carvalho, M. C. (2013) Integration of Analytical Instruments with Computer Scripting. *Journal of Laboratory Automation*, ISSN 2211-0682, 328-333

Guarnieri, M. (2010) *The Roots of Automation Before Mechatronics*. IEEE Ind. Electron. M.: 42-43. doi:10.1109/MIE.2010.936772

Huidobro, J. M. & Millan, R. J. (2004) *Domótica. Edificios Inteligentes* Ed. Creaciones. Copyright

Jin, M., Jia, R. & Spanos, C. (2017) Virtual Occupancy Sensing: Using Smart Meters to Indicate Your Presence. IEEE Transactions on Mobile Computing. PP (99) ISSN 1536-1233

Kyriazis, D., Varvarigou, T., Rossi, A., White, D. & Cooper, J. (2013) Sustainable smart city IoT applications: Heat and electricity management & Eco-conscious cruise control for public transportation". *IEEE International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. ISBN 978-1-4673-5827-9

Li Rita, Yi Man, Li Herru, Ching Yu; Mak, Cho Kei, Tang & Tony Beiqi (2016) Sustainable Smart Home and Home Automation: Big Data Analytics Approach. *International Journal of Smart Home*, 177-198. doi:10.14257/ijsh.2016.10.8.18

Nordrum, A. (2016) Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. IEEE

Perera, C., Liu, C. H. & Jayawardena, S. (2015) The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey. IEEE *Transactions on Emerging Topics in Computing*. 3 (4), ISSN 2168-6750, 585-598

Vermesan, O. & Friess, P. (2013) *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. Aalborg, Denmark: River Publishers. ISBN 978-87-92982-96-4