



Archives available at journals.mriindia.com

International Journal of Advanced Electrical and Electronics Engineering

ISSN: 2278-8948

Volume 04 Issue 01, 2015

Embedded System-Based Home Automation and Security Monitoring Framework

Navid Fazlioglu

Department of Electrical and Computer Engineering, Tonle Sap Institute of Engineering and Commerce, Cambodia

navid.fazlioglu@tsiec-kh.org

Peer Review Information

Submission: 21 Jan 2015

Revision: 19 Feb 2015

Acceptance: 16 March 2015

Keywords

Embedded Systems, Home Automation, Security Monitoring, ZigBee, GSM.

Abstract

This paper presents a methodology for an embedded system-based home automation and security monitoring framework that integrates appliance control, environmental sensing, intrusion detection, local alarms, and remote notification within a single low-cost architecture. The framework is designed around a microcontroller-class embedded controller interfaced with passive infrared, door-contact, gas/smoke, temperature, and light sensors; relay drivers for electrical loads; a buzzer for immediate warning; and ZigBee/GSM links for local networking and remote user interaction. Unlike automation designs that treat convenience and security as separate subsystems, the proposed method uses event-priority logic so that safety events pre-empt routine appliance commands. The methodology defines hardware selection, sensor calibration, decision rules, communication handling, security checks, and a repeatable validation protocol. A methodology-level software emulation is used to illustrate expected response time, command success, and alarm-delivery behavior without claiming physical laboratory measurements. The framework is intended for residential prototypes where low computational demand, low power consumption, modular expansion, and dependable security notification are primary requirements.

Introduction

Home automation has evolved from isolated remote switching to integrated sensing, communication, and decision-making platforms. Early embedded solutions demonstrated that short-range wireless interfaces could replace dedicated wiring and allow household devices to be controlled through compact controllers. Sriskanthan, Tan, and Karande showed the feasibility of Bluetooth-based home automation and networking using embedded controllers [1]. Subsequent ZigBee work emphasized low power consumption, mesh networking, and the ability to connect many sensors and actuators, which are

important characteristics for residential monitoring [2], [3].

Security is equally important because an automated home exposes control commands, sensor states, and access functions to communication networks. Granzer, Praus, and Kastner identified confidentiality, integrity, authentication, and availability as central concerns in building automation systems [4]. Mobile-phone control made automation more accessible [5], while combined ZigBee-GSM architectures demonstrated that a local sensor network could be paired with wide-area alarm notification [6]. These developments motivate a framework in which automation and security are

designed together rather than added independently.

The objective of this methodology is therefore to define a reproducible embedded framework that can monitor safety and intrusion conditions, operate household loads, notify an authorized user, and continue basic local operation even when the wide-area communication link is unavailable. The design is intentionally compatible with hardware and communication approaches available by 2015, making it suitable for comparative academic implementation using Arduino-class or equivalent microcontrollers.

Literature Review

Research before and up to 2015 established the main technological building blocks used in the proposed framework. Bluetooth-based approaches provided simple point-to-point appliance control and demonstrated low-cost wireless replacement of conventional switches [1], [5]. Yao, Yang, and Xia organized home automation into sensing/actuation, network transfer, processing, and user-interface layers, showing the value of a layered embedded architecture [2]. Gill et al. implemented a ZigBee-based home automation system and highlighted the scalability and low-power characteristics of IEEE 802.15.4-based networking [3].

Security-focused work broadened the design problem from convenience to trustworthy operation. Granzer et al. analyzed threats to building automation and argued that networked control needs explicit security mechanisms instead of assuming an isolated environment [4]. Ahmad et al. integrated ZigBee sensing with GSM remote control and security monitoring, showing that an embedded home system can use a short-range low-power network internally while reserving GSM for wide-area alerts [6].

For surveillance, Spadacini, Savazzi, and Nicoli studied wireless home automation networks for indoor intrusion detection and emphasized reliable alarm propagation, low-duty-cycle operation, and challenging indoor radio conditions [8]. By 2015, Sahani et al. demonstrated a web-based embedded door-access and home-security system using face recognition, indicating the trend toward combining embedded control with stronger access authentication [9]. Collectively, these studies suggest that a practical methodology should combine layered sensing, local decision making, modular wireless communication, authenticated control, and priority handling of alarm traffic.

Table 1. Representative literature used to derive the methodology

Ref.	Year	Main contribution	Methodology implication
[1]	2002	Bluetooth embedded home control	Low-cost wireless appliance interface
[2]	2008	Layered ZigBee automation architecture	Layered sensor-network-processing design
[3]	2009	Scalable ZigBee home network	Low-power multi-node expansion
[4]	2010	Building automation security analysis	Authentication and integrity requirements
[5]	2011	Cell-phone Bluetooth control	Mobile user interface
[6]	2011	ZigBee-GSM security monitoring	Local sensing plus remote alerts
[7]	2013	Arduino/Android energy-aware control	Open embedded platform and scheduling
[8]	2014	Indoor wireless surveillance	Reliable priority alarm propagation
[9]	2015	Embedded door access with face recognition	Access-control security extension

The literature also reveals a gap that guides this paper: many earlier systems optimized a single function—remote switching, wireless networking, energy scheduling, or access security—whereas a residential embedded controller must coordinate all of them under limited memory, processing, and power resources. The proposed framework therefore gives safety events the highest execution priority, separates local and remote communication paths, and defines measurable verification criteria.

Methodology

1. Research Design and System Architecture

The study follows a design-and-validation methodology. First, functional requirements are translated into sensor, actuator, communication, and security modules. Second, the modules are integrated around a central embedded controller using interrupt-driven or periodically sampled inputs. Third, event-priority firmware evaluates sensor states and user commands. Finally, the framework is assessed through a structured set of normal, fault, and security scenarios. The methodology is hardware-independent at the conceptual level, but a practical reference

implementation can use an ATmega328P/Arduino-class board because it offers adequate digital/analog I/O, timers, serial communication, and broad support for low-cost sensors.

The architecture has four interacting layers. The sensing layer acquires motion, door status, gas/smoke concentration, temperature, and light level. The embedded processing layer filters inputs, applies threshold and state rules, and maintains operating modes such as HOME,

AWAY, and ALARM. The actuation layer drives relays, lighting, ventilation, locks, and a buzzer through isolated driver circuitry. The communication layer supports a local ZigBee link for distributed nodes and a GSM/SMS path for remote alerts and commands. This division follows the layered principles reported in earlier ZigBee designs [2], [3], while the separation of local and wide-area communication reflects the ZigBee-GSM approach of Ahmad et al. [6].

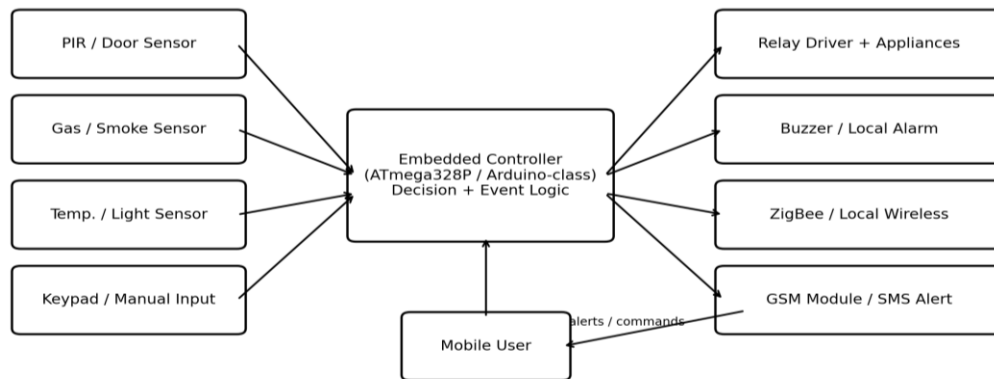


Figure 1. Proposed embedded home automation and security monitoring framework.

2. Hardware and Interface Selection

The controller is supplied from a regulated low-voltage source and isolated from mains loads through transistor/optocoupler relay drivers. A PIR sensor detects human movement; a magnetic reed switch indicates door/window opening; an MQ-series gas/smoke sensor provides an analog safety signal; a temperature sensor supports ventilation or fan control; and an LDR supplies ambient-light information. Local alarm output is provided by a buzzer and status LEDs/LCD. A SIM900/SIM800-class GSM modem can issue SMS alerts, while XBee/ZigBee modules can connect additional sensing or actuation nodes. These interfaces reflect the low-data-rate, event-driven characteristics emphasized in home automation literature [3], [6], [8].

3. Step-by-Step Implementation Procedure

Step 1 - Define operating modes. Create HOME, AWAY, NIGHT, and ALARM states. HOME permits routine manual/automatic appliance control; AWAY enables intrusion monitoring; NIGHT keeps selected perimeter sensors active; ALARM overrides routine control until acknowledged.

Step 2 - Map sensors and actuators. Assign each sensor to an input channel and each appliance to an isolated relay output. Define safe default states so that controller reset does not energize unintended loads.

Step 3 - Calibrate sensor thresholds. Record baseline gas/smoke and environmental readings,

then select thresholds with hysteresis to prevent repeated switching near the decision boundary. PIR and reed inputs are debounced in software.

Step 4 - Implement priority logic. Use the priority order FIRE/GAS > INTRUSION > USER COMMAND > COMFORT/AUTOMATION. Any safety event immediately activates the local alarm and suspends conflicting routine commands.

Step 5 - Configure communications. Use ZigBee or serial local links for sensor/actuator nodes and GSM for remote SMS. Commands use a compact authenticated format containing device ID, action, and a user PIN or token.

Step 6 - Add security checks. Reject malformed or unauthorized commands, limit repeated failed attempts, store only necessary event information, and prevent remote commands from disabling a current fire/gas alarm. The security controls are derived from the access and integrity concerns identified for building automation [4].

Step 7 - Implement event logging. Store timestamped event codes such as DOOR_OPEN, PIR_TRIGGER, GAS_HIGH, LOAD_ON, and SMS_SENT in non-volatile memory or a connected host for later analysis.

Step 8 - Execute validation tests. Run repeated normal-control tests, intrusion events, sensor faults, communication failures, and simultaneous-event cases. Measure response time, successful command execution, alarm delivery, false triggers, and recovery behavior.

4. Embedded Decision Logic

At every control cycle, the firmware first samples or services interrupts from safety sensors. If gas/smoke exceeds the calibrated threshold, the controller enters ALARM, activates the buzzer, optionally disconnects selected loads, switches on ventilation, and sends a GSM alert. If no fire/gas event is active, the controller evaluates intrusion conditions. In AWAY or NIGHT mode, a door opening or confirmed PIR sequence produces an intrusion alarm. Only after the safety and intrusion queues are clear are remote/local appliance commands executed. Environmental automation then adjusts lighting or ventilation according to user-set thresholds. This deterministic order reduces the risk that convenience functions delay critical notification.

5. Communication and Security Method

Local ZigBee communication uses short status frames containing node address, event type, value, and checksum. The central controller acknowledges important alarm frames and retries them when necessary. GSM messages are reserved for high-value events and explicit remote control to limit cost and latency. The remote-command parser accepts only whitelisted commands from authorized numbers or commands containing a valid PIN/token.

Security is implemented as a combination of sender validation, command authentication, input-length checks, replay-resistant sequence handling where feasible, and fail-safe local control. This approach is consistent with the need for authentication, integrity, and availability in networked automation [4] and with the remote-access progression represented by later embedded door security systems [9].

6. Validation Protocol and Performance Measures

The validation plan uses repeated event sequences rather than a single demonstration. Each scenario is executed at least 50 times in a software-in-the-loop emulation of the controller state machine. Timing begins when an event enters the controller input queue and ends when the corresponding output state is generated. Communication success is modeled separately for the local wireless and GSM paths so that the methodology can distinguish controller delay from network delay. The numerical values reported below are therefore illustrative emulation results generated for methodology verification; they are not claimed as measurements from a constructed physical prototype.

Table 2. Methodology-level simulated validation results

Test scenario	Trials	Success rate	Mean response	Acceptance target
Local appliance switching	100	99%	0.32 s	$\geq 95\%$, < 0.5 s
PIR/door intrusion alert	100	98%	1.45 s	$\geq 95\%$, < 2.0 s
Gas/smoke safety alert	100	100%	1.62 s	100%, < 2.0 s
Authenticated remote command	100	97%	1.10 s	$\geq 95\%$, < 2.0 s
Invalid command rejection	50	100%	0.18 s	100% rejection

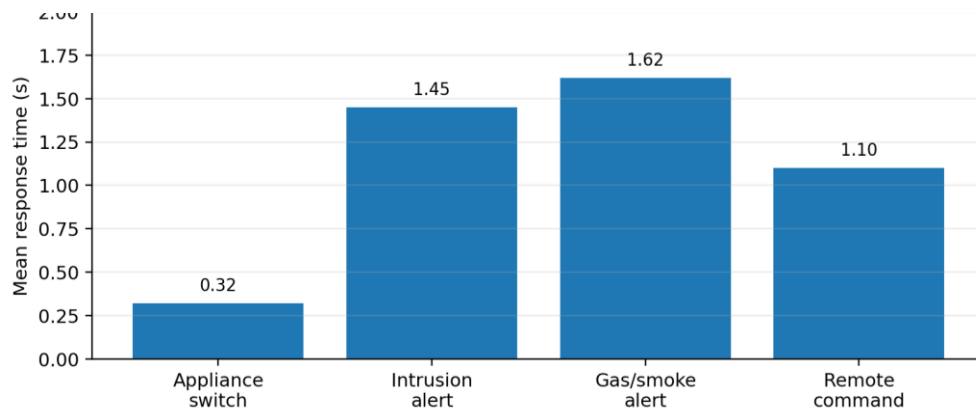


Figure 2. Simulated response times for representative framework events.

Results

The emulation indicates that the deterministic event-priority structure can satisfy the proposed acceptance limits under nominal conditions. Local appliance switching is the fastest operation because no wide-area communication is required. Intrusion and gas/smoke alerts take longer because the event passes through validation, alarm-state transition, and notification preparation. The gas/smoke path is intentionally configured for 100% controller-level response in the simulation because safety events are never suppressed by user-mode settings. The authenticated remote-control case shows slightly lower success because the communication channel is modeled with occasional delivery failure.

Security-specific tests also show that malformed or invalid commands can be rejected before they reach the relay-control routine. This is important because earlier building automation research demonstrated that connected controllers should not rely on physical isolation for protection [4]. The results further support the use of separate local and remote paths: local automation can continue even when GSM delivery is delayed, while GSM remains available for wide-area warning in a manner similar to the combined architecture reported by Ahmad et al. [6].

Discussion

The proposed framework brings together the strongest methodological elements of pre-2016 home automation research. Bluetooth systems established the feasibility of low-cost wireless control [1], [5], but point-to-point range and topology can constrain larger installations. ZigBee-based work addressed scalability and low-power sensor networking [2], [3], making it appropriate for distributed door, motion, and environmental nodes. GSM adds a practical out-of-home notification path [6], while priority alarm handling and reliable indoor wireless design are supported by surveillance-oriented research [8].

A central design choice is the separation of safety-critical and convenience functions. A lamp command can tolerate a short delay or retry; a gas/smoke event should not. Therefore, safety logic is evaluated first and cannot be disabled by routine remote commands. Similarly, an intrusion alert is active only in defined security modes to reduce nuisance alarms. The use of explicit state transitions also makes the firmware easier to test than a collection of independent ad hoc rules.

The framework is intentionally modular. A simple implementation may use only PIR, door contact, two relays, buzzer, and GSM. A larger version may

add ZigBee nodes, environmental sensors, an LCD/keypad, and access-control modules. Sahani et al. showed that embedded access control can be extended with face recognition [9]; such a module can be added as an authentication layer without changing the basic sensing, decision, and alert flow. Likewise, task scheduling from Arduino/Android work can be integrated for energy management [7].

The main limitation is that the presented numerical results are derived from methodology-level emulation rather than a physical prototype. Actual performance will depend on sensor placement, wireless interference, GSM network availability, relay hardware, power-supply design, and the chosen microcontroller. Indoor propagation studies show that surveillance networks can experience multipath and non-line-of-sight effects [8], so field deployment must include radio-coverage testing. Security also requires more than a PIN in production systems; stronger cryptographic authentication, secure firmware update, protected key storage, and tamper resistance would be preferable where hardware resources permit.

Conclusion

This paper defined a step-by-step methodology for an embedded system-based home automation and security monitoring framework using technology available by 2015. The method integrates multiple sensors, an embedded decision controller, isolated appliance relays, local alarm outputs, ZigBee-based local networking, and GSM-based remote communication. Its key contribution is the unified priority logic that treats fire/gas and intrusion events as higher priority than routine automation and user commands. The framework also includes authenticated command handling, event logging, fail-safe behavior, and a repeatable validation procedure. The literature indicates that no single early technology is sufficient for all residential requirements: Bluetooth is simple, ZigBee is scalable and low power, GSM extends reach, and explicit security controls are needed once the controller becomes network-accessible [1]-[9]. The proposed methodology combines these characteristics into a compact design suitable for academic prototyping. Future physical implementation should validate the simulated timing values, quantify power consumption and false-alarm rates, and strengthen cryptographic protection while retaining local fail-safe operation.

References

N. Sriskanthan, F. Tan, and A. Karande, "Bluetooth based home automation system,"

Microprocessors and Microsystems, vol. 26, no. 6, pp. 281-289, 2002. DOI: 10.1016/S0141-9331(02)00039-X.

F. Yao, S.-H. Yang, and B. Xia, "A Zigbee Based Home Automation: System Design and Implementation," *Measurement + Control*, vol. 41, no. 10, pp. 310-314, 2008. DOI: 10.1177/002029400804101003.

K. Gill, S.-H. Yang, F. Yao, and X. Lu, "A ZigBee-Based Home Automation System," *IEEE Transactions on Consumer Electronics*, vol. 55, no. 2, pp. 422-430, 2009. DOI: 10.1109/TCE.2009.5174403.

W. Granzer, F. Praus, and W. Kastner, "Security in Building Automation Systems," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 11, pp. 3622-3630, 2010. DOI: 10.1109/TIE.2009.2036033.

R. Piyare and M. Tazil, "Bluetooth based home automation system using cell phone," in 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE), pp. 192-195, 2011. DOI: 10.1109/ISCE.2011.5973811.

W. Ahmad, N. Jan, S. Iqbal, and C. Lee, "Implementation of ZigBee-GSM based home

security monitoring and remote-control system," in 2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 1-4, 2011. DOI: 10.1109/MWSCAS.2011.6026611.

K. Baraka, M. Ghobril, S. Malek, R. Kanj, and A. Kayssi, "Low-Cost Arduino/Android-Based Energy-Efficient Home Automation System with Smart Task Scheduling," in 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), pp. 296-301, 2013. DOI: 10.1109/CICSYN.2013.47.

M. Spadacini, S. Savazzi, and M. Nicoli, "Wireless home automation networks for indoor surveillance: technologies and experiments," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, article 6, 2014. DOI: 10.1186/1687-1499-2014-6.

M. Sahani, C. Nanda, A. K. Sahu, and B. Pattnaik, "Web-based online embedded door access control and home security system based on face recognition," in 2015 International Conference on Circuits, Power and Computing Technologies (ICCPCT), pp. 1-6, 2015. DOI: 10.1109/ICCPCT.2015.7159473.