Sensors and Materials, Vol. 29, No. 7 (2017) 1069–1080
MYU Tokyo

S & M 1400

Fusion-Algorithm-Based Security System with Multiple Sensors

Kuo-Hsien Hsia and Jr-Hung Guo[1*]

Department of Electrical Engineering, Far East University,
No. 49, Chung Hua Rd., Hsin-Shih. Tainan County 744, Taiwan, R.O.C.
[1]Department of Electrical Engineering, National Yunlin University of Science & Technology,
123 University Road, Section 3, Douliou, Yunlin 64002, Taiwan, R.O.C.

(Received March 1, 2016; accepted May 15, 2017)

Keywords: multisensor fusion, adaptive fusion method, fuzzy-AHP, security system, IoT

People seek a comfortable and safe living environment, but accidents such as home invasions, gas leaks, and fire often occur in our environment. Thus, a security system for disaster prevention and detection is very important. However, current common security systems are either too simple to function or too complicated to be installed and used. Hence, in this study, we developed a security system with a multi-agent architecture, which has multiple sensors and multiple communication interfaces. In the event of a disaster, this system can not only provide early warning, but also safely and quickly guide people to leave the scene of the accident. Our security system is composed of a variety of modules with different functions. Multiple sensors may be connected on one module. Every module can operate independently. Multisensor fusion and adaptive fusion methods make the modules more accurate in detecting events. The modules communicate via Wi-Fi, Ethernet, RF, power line communication, or other interfaces. At least two communication interfaces are active between modules to form a group with multi-agent architecture. When an event occurs, each group communicates with the others to find a safe escape route and then guides people safely and quickly away from the scene of the accident via light or sound from each module. In addition, these modules can connect to a monitoring system through the communication interfaces. The monitoring system, operating on a computer or a handheld device, can confirm that an incident occurred using fuzzy analytic hierarchy process (fuzzy-AHP) by these data and establish accident models for earlier warning. These models can be transmitted to the modules making them more intelligent. Since each module developed in this paper has the function of network communication, it can be an Internet of Things (IoT) node, and the monitoring system can form a regional disaster prevention system.

1. Introduction

The definition of quality of life, in addition to anti-theft protection, prevention of fire and gas leaks, and other disasters, also includes the abilities to prevent disasters or provide guidance for escape. In other words, one can use various security modules and modes of communication to monitor the home environment, such as ambient temperature, humidity, and illumination. However, these are just functional enhancements; how to enhance the stability and intelligence of a

*Corresponding author: e-mail: g9710801@yuntech.edu.tw
http://dx.doi.org/10.18494/SAM.2017.1597

ISSN 0914-4935

security system is a key issue in quality of life research. This means that security modules have a higher degree of accuracy and convenience and can be monitored by smart phones, personal digital assistants (PDAs), or other devices on the network. A system can prevent the occurrence of a disaster, or can provide a safe escape route when a disaster occurs. Such a system can be regarded as a system that provides for quality of life.

In the past, many studies of intelligent safety systems have been carried out. Kujuro and Yasuda described how to evaluate a system in a smart building and the importance of information updating and communication capabilities in the building automation system.[1] Fu *et al.* designed standard interfaces for intelligent building systems to be used in the control of appliances and communication.[2,3] In the area of fire hazard detection, Cheong *et al.* used ultraviolet (UV) sensors and ZigBee wireless sensor networks to detect the sources of fire.[4] Budi *et al.* combined machine vision and image recognition algorithms to identify fire sources.[5] Wang *et al.* used a single chip with three complementary sensors (temperature, smoke, and carbon monoxide) to detect fire sources and designed a fire detection module using the multiple sensing fusion theory.[6] It can be seen from the previous literature that an intelligent security system is quite complex and large, but many features can be implemented independently, so Agent[7] technology is very suitable for a security system. Agent, a key research topic in artificial intelligence, means that when a node fails, its function can be completed by other nodes.

From previous studies, it can be seen that a stable and correct security system requires the integration of hardware and software, including sensors, communication technology, software technology, and a variety of algorithms. This makes a security system expensive or complicated to install. With the design concept of "operating independently and monitoring centrally," we used in this study the 8051 as the master controller with a modular design to reduce the cost of the security system and to make the resulting system convenient to use. For communication, we integrated wireless RF, RS232/422/485, wireless network, wired network, and other communication interfaces, and up to three communication interfaces were used at the same time. Because the security module has wireless and wired network communication interfaces, it also has the function of the Internet of Things (IoT). This design allows each module to have a powerful ability to communicate and a more complete monitoring function. It also prevents message sending failure due to communication interface problems.

Each module of the security system has four sensor signal inputs. Users can install 1 to 4 sensors, which may be the same or different, as required. To determine the accuracy of the sensor signal to reduce the chances of a miscarriage of justice, we use the fuzzy analytic hierarchy process (fuzzy-AHP) and the adaptive fusion method[8] on each module of the security system to process the sensor signals and events. This ensures the correctness of the sensor signals and enables the grouping of events into classes. These data on the class of events and the accuracy of sensors can also be used to assess the correctness and stability of the security system modules and make the entire security system more intelligent.

In a security system module, we use micro IP (μIP), which is an implementation of the transmission control protocol/Internet protocol (TCP/IP) network protocol stack developed by Dunkels.[9] Owing to the small code size, μIP makes an 8/16bit single-chip system having functions of TCP, user datagram protocol (UDP), simple mail transfer protocol (SMTP), telnet server/client, an HTTP server and web client, domain name system (DNS), and others. Our security system modules have Wi-Fi and Ethernet functions. With these two functions together, the developed security system modules will be more convenient to use and can be linked to form an IoT system.

2. System Architecture

The security system module developed in this study is based on the 8051 series single chip as the main control chip with a sensor signal processing circuit, communication interface, and other peripheral circuits. A block diagram of the module is shown in Fig. 1. Up to four sensors can be connected to this module. Before being calculated or processed, each sensor signal goes through a signal processing circuit for signal amplification, zeroing, filtering, and other processing, and then is sent to the single chip A/D for digitization.

In the communication interface, the security system module can be connected to the RF wireless module, Wi-Fi, Ethernet, power-line communication (PLC), or wired universal asynchronous receiver/transmitter (UART). The security system module can use three different communication interfaces at the same time. Through the communication interfaces, processed sensor data or calculated results can be returned to the host computer, and the host computer can receive the sensor threshold, module data or parameters, communication settings, or other parameters. Because there are many communication interfaces, it is simpler and more convenient to apply the security system module, and it can be ensured that an event message is sent immediately at the time of an incident.

The module can be used alone or to form a sensor network by connecting multiple modules via the communication interfaces. In the case of multiple modules, the user can adjust the number and types of sensors used by each module according to the requirements, so that the entire monitoring system can generate more accurate results.

For data communication, a well-defined data packet structure produces the following benefits:[10]

(1) The source of any information can be easily identified and the data can be easily analyzed.
(2) The leading code and the check sum can ensure the correctness of the information.
(3) The length of the data packet can be estimated, and the receiver can confirm the data integrity.
(4) The required transmission time can be predetermined, and the communication efficiency can be improved.

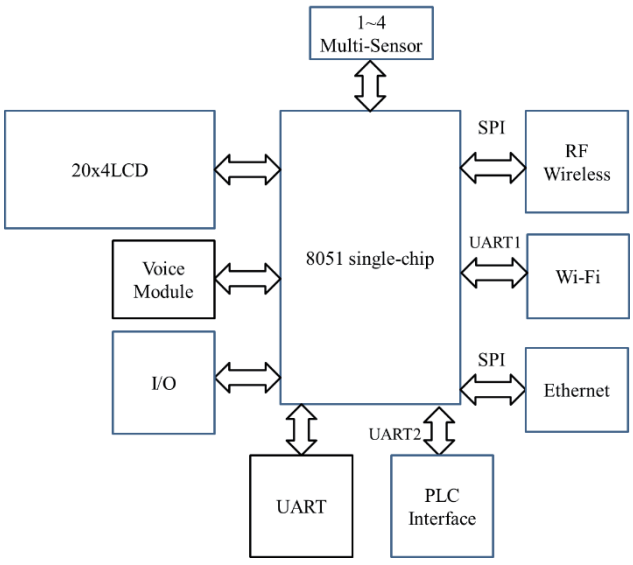


Fig. 1. System architecture.

Hence, for our application, we define a data packet structure as shown in Table 1. Each data set starts with 35H (Byte 0). Definitions of other bytes are as follows:

(1) ID (Byte 1): This byte defines the type of packet and the length of the receiving/transmission. The format of this byte is shown in Table 2. Bit 7 indicates the direction of data flow: "0" means requiring information from the host, and "1" means transferring from the module. Bits 4–6 indicate data packet as shown in Table 3. Bits 3–0 indicate the data length. For example, "0001" means that the data length is 1. The maximum data length is 16 with bits 3–0 being "1111". The default data length is 4 B.

(2) Sensor Kind (Byte 2): This byte defines the details of the sensor or module and is called the group number. Table 4 lists several types of sensors. By expanding this table, modules with other sensing functions can be used in the system.

Table 1
Protocol format.

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4
35H	ID	Sensor kind	Module	State
	$4N$ (N = 1–16)			Checksum
	Data/Parameter			SUM (all byte)

Table 2
ID Byte format.

bit 7	bit 6	bit 5	bit 4
Rx/Tx	Packet type		
bit 3	bit 2	bit 1	bit 0
Data length (N: 1–16)			

Table 3
Packet type.

bit 6	bit 5	bit 4	Packet type
0	0	0	wireless sensor
0	0	1	wired sensor
0	1	0	other sensor
0	1	1	security parameter
1	0	0	net parameter
1	0	1	location
1	1	0	module parameter
1	1	1	system used

Table 4
Sensor kind definition.

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0	Sensor kind
0	0	0	0	0	0	0	0	Sensor_Reed_A
0	0	0	0	0	0	0	1	Sensor_Reed_B
0	0	0	0	0	0	1	0	Sensor_Glass
0	0	0	0	0	0	1	1	Sensor_IR
0	0	0	0	0	1	0	0	Sensor_Fire
0	0	0	0	0	1	0	1	Sensor_Body
0	0	0	0	0	1	1	0	Sensor_Appliances1
0	0	0	0	0	1	1	1	Sensor_Appliances2
0	0	0	0	1	0	0	0	Sensor_Temperature
0	0	0	0	1	0	0	1	Sensor_Humidity
0	0	0	0	1	0	1	0	Sensor_Illumination
0	0	0	0	1	0	1	1	Sensor_Pressure
0	0	0	0	1	1	0	0	Sensor_Noise
0	0	0	0	1	1	0	1	Sensor_Gas
0	0	0	0	1	1	1	0	Sensor_Smoke
0	0	0	0	1	1	1	1	Sensor_AC
0	0	0	1	0	0	0	0	Sensor_Air
0	0	0	1	0	0	0	1	Sensor_CO
0	0	0	1	0	0	1	0	
				⋮				For future use
1	1	1	1	1	1	1	1	

(3) Module (Byte 3): This byte is used to define the module ID between 0 and 255 (00H–FFH). Each group can contain a maximum of 255 modules. By combining the bytes of Sensor Kind and Module, there can be a maximum of 65,535 modules or devices in the security network.
(4) State (Byte 4): For a smart sensor module, it describes the state of the module/sensor. It means that this byte can be used for diagnostics. Consider a current-sensing module as an example. If one sensor has malfunctioned, it will be isolated and marked by this byte after the data on the sensor is processed.
(5) Data: The data length is defined from bits 3–0 of Byte 1. Thus, the data length can be defined according to the sensor number or speed of the communications interface, and the longest data length is 64 B. It can also be used for setting parameters on the modules for the monitoring software.
(6) Check Sum: This byte is used to check if there is any error in the transmission data. It simply takes the lowest byte of the addition of all bytes including the starting byte 35H as the check sum. One reason for this definition is the limited computation power of a single chip.

By using single-chip architecture and modular design coupled with a sound communication protocol, the security system and the module are very flexible and convenient to use.

3. Algorithms

To ensure that the modules can correctly classify the state of the events, we use fuzzy-AHP algorithms on the modules for assistance in analysis and judgement. The results are transmitted to the monitoring system via the communication interfaces and processed by the adaptive fusion method in the monitoring system. Such a process can prevent the system from making a wrong decision when an error occurs in the security system module in an area. In addition, the results of adaptive fusion theory can also be used to analyze the error rate of each security system module. This mechanism can reduce the rate of false positive events, and can provide for the early detection of the possible failure of a security system module. Finally, the monitoring system sends the results processed by the adaptive fusion method to the security system modules to enhance the accuracy and intelligence of each module.

3.1 Fuzzy-AHP methods

Because there may be different numbers of sensors on different modules and different types of sensors on one module, there are three ways to deal with fuzzy-AHP.
(l) Using a single sensor: This is the most commonly used model and the cheapest method. However, since only one sensor is used, it is easy to produce erroneous event messages due to sensor problems. To reduce the chance of sensor error, a number of sensor data are continuously read. The total number of sensor data (measurements) j can be set by the monitoring system. A threshold h is set in the module for data comparison for sensors. Comparing the measured value v of the sensor to the threshold h, we can get S using the following equation.

$$\begin{cases} \text{If } v_k > h \text{ then } S_k = 1 \\ \text{If } v_k \leq h \text{ then } S_k = 0 \end{cases} \tag{1}$$

Since the results obtained by multiple measurements using a single sensor are a one-dimensional array, whether an event has occurred or not can be evaluated using Eqs. (2)–(6). Summarizing

the 1's in the array and then dividing the sum by the number of samples represents the fuzzy severity of the event. As defined in Eq. (4), the event severities E = 1–5 mean safety, possible, warning, danger, and emergency, respectively. While transmitting the event data, the security system module transmits results of the fuzzy-AHP evaluations and the severity information to the monitoring system at the same time. The monitoring system uses this information to evaluate the accuracy and stability of the security system module.

$$C = \sum_{k=1}^{j} S_k \tag{2}$$

$$e = C / j \tag{3}$$

$$\begin{cases} \text{If } e \geq 90\% \text{ then } E = 5 \\ \text{If } e \geq 70\% \text{ then } E = 4 \\ \text{If } e \geq 50\% \text{ then } E = 3 \\ \text{If } e \geq 30\% \text{ then } E = 2 \\ \text{If } e < 30\% \text{ then } E = 1 \end{cases} \tag{4}$$

$$\begin{cases} \text{If } E \geq 3 \text{ then } M = 1 \\ \text{If } E < 3 \text{ then } M = 0 \end{cases} \tag{5}$$

$$\begin{cases} \text{If } M = 1 \text{ then } T = true \\ \text{If } M = 0 \text{ then } T = false \end{cases} \tag{6}$$

(2) Using duplicate sensors: This is an advanced way to ensure that event judgments do not fail due to sensor failure. We set i as the number of the sensor, j as the total number of measurement by a sensor, h as the threshold value, and v as the value measurement by a sensor. If the measured value v is less than or equal to the sensor threshold, then $S_k = 0$. Otherwise, $S_k = 1$. Continuously reading the sensor data can reduce the chance of sensor error. The number j can be set in the monitoring system. The value of each sensor is read and compared with the threshold; we can rewrite Eq. (1) as

$$\begin{cases} \text{If } v_{ki} > h \text{ then } S_{ki} = 1, \\ \text{If } v_{ki} \leq h \text{ then } S_{ki} = 0. \end{cases} \tag{7}$$

The following results can be obtained after finishing all of the comparisons:

$$A = \begin{bmatrix} S_{11} & S_{12} & S_{13} & S_{14} \\ S_{21} & S_{22} & S_{23} & S_{24} \\ S_{31} & S_{32} & S_{33} & S_{34} \\ \vdots & \vdots & \ddots & \vdots \\ S_{j1} & S_{j2} & S_{j3} & S_{j4} \end{bmatrix}. \tag{8}$$

Summarizing the 1's of each column, we have

$$C_i = \sum_{k=1}^{j} S_{ki},\ i = 1, ..., 4. \tag{9}$$

Then, we can write

$$a = \begin{bmatrix} C_1 & C_2 & C_3 & C_4 \end{bmatrix}. \tag{10}$$

Dividing each element of Eq. (10) by the number of measurements, we have

$$e_i = C_i / j. \tag{11}$$

Applying the results of Eq. (11) into Eq. (4), the following equations confirm the occurrence of the event.

$$\begin{cases} \text{If } E_i \geq 3 \text{ then } r_i = 1 \\ \text{If } E_i < 3 \text{ then } r_i = 0 \end{cases} \tag{12}$$

$$M = \sum [r_1, r_2, r_3, r_4] \tag{13}$$

$$\begin{cases} \text{If } M \geq 2 \text{ then } T = true \\ \text{If } M < 2 \text{ then } T = false \end{cases} \tag{14}$$

Using duplicate sensors avoids false event messages due to sensor problems, but it is costly and computationally expensive.

(3) Using several different sensors: This approach uses multiple sensors associated with the detection event to detect the occurrence of an event. In this way, the characteristics of the different sensors can be used to identify and distinguish the event in more detail. For example, when we want to detect fire, we can use the flame sensor, carbon monoxide sensor, smoke sensor, and a temperature sensor. When there is a fire, the sensors listed can detect some of the characteristics of the fire. However, there may not be a clear flame at the beginning of a fire; there may be only smoke or an increase in temperature. Therefore, using a variety of different sensors enables early warning for fires, and it may be possible to clearly indicate the status of a fire.

Similar to the use of duplicate sensors, we set i as the number of the sensor, j as the total number of measurements by a sensor, h_i as the threshold value of the ith sensor, and v as the value measured by the sensor. If the measured value v is less than or equal to the sensor threshold, then $S_k = 0$. Otherwise, $S_k = 1$. Continuously reading the sensor data can reduce the chance of sensor error. The number j can also be set in the monitoring system. The measured value of each sensor is read and compared with the threshold, and we can rewrite Eq. (1) as

$$\begin{cases} \text{If } v_{ki} > h_i \text{ then } S_{ki} = 1, \\ \text{If } v_{ki} \leq h_i \text{ then } S_{ki} = 0. \end{cases} \tag{15}$$

The following results can be obtained after finishing the comparisons:

$$A = \begin{bmatrix} S_{11} & S_{12} & S_{13} & S_{14} \\ S_{21} & S_{22} & S_{23} & S_{24} \\ S_{31} & S_{32} & S_{33} & S_{34} \\ \vdots & \vdots & \ddots & \vdots \\ S_{j1} & S_{j2} & S_{j3} & S_{j4} \end{bmatrix}. \tag{16}$$

Summarizing the 1's of each column, we have

$$C_i = \sum_{k=1}^{j} S_{ki},\ i = 1, ..., 4. \tag{17}$$

Then, we can write

$$a = \begin{bmatrix} C_1 & C_2 & C_3 & C_4 \end{bmatrix}. \tag{18}$$

Dividing each element of Eq. (18) by the number of measurements results in

$$e_i = C_i / j. \tag{19}$$

Because different sensors are used; we can not only confirm the occurrence of the event but also distinguish the state of the event. For example, security system modules with flame, smoke, carbon monoxide, and temperature sensors for fire detection may have severity values of E_{flame} = 2, E_{smoke} = 4, E_{CO} = 3, and $E_{temperature}$ = 3. Because each sensor has a different relationship to the fire, we can set a weighting factor g for each sensor in the monitoring system. Thus, we have the fuzzy assessment equation

$$u_0 = \sum_{i=1}^{4} \left(E_i * g_i \right). \tag{20}$$

With this fuzzy assessment equation, we can assess how likely it is that a fire occurred. Moreover, as the previous example, we can describe the incident as "a possible fire; some smoke has been generated; we must pay attention to carbon monoxide and temperature". Thus, we can accurately describe the status of an event, and the description can be a reference for handling the event or escaping the area.

3.2 Adaptive fusion method

Although we use fuzzy-AHP in the sensor module to reduce the rate of false alarms, to analyze each sensor more accurately and reduce the misjudgment rate, we used the adaptive fusion method in the monitoring system. This algorithm is very suitable for digital detection signals, and the module sensor data after fuzzy-AHP processing are all digital. We can analyze the data using the adaptive fusion method.

Consider a binary hypothesizing-and-testing system with n area detecting points in which each detecting point employs a predetermined decision rule. The two hypotheses are H_0 and H_1, where H_0 means that the event does not occur and H_1 means that the event does occur. The hypotheses have a priori probabilities $P_0 = P(H_0)$ and $P_1 = P(H_1)$. Figure 2 shows the system architecture.

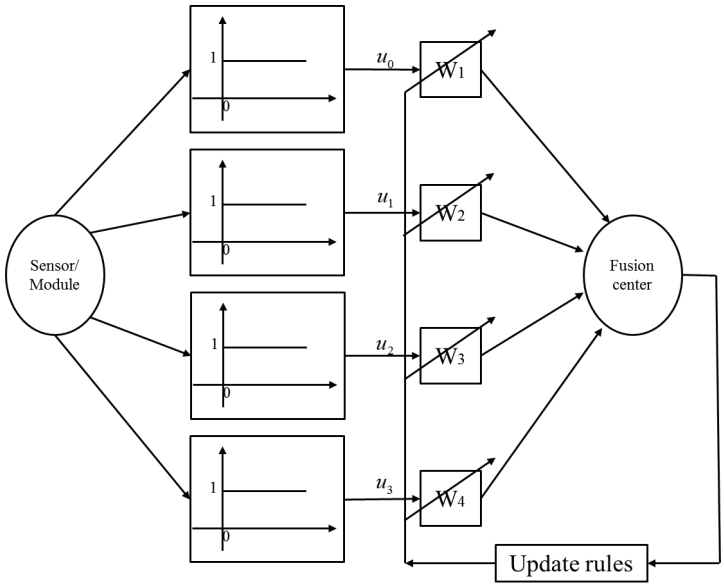


Fig. 2. Fusion architecture.

With some derivations,[11,12] we have the amended rule as follows.

The initial weight value is defined as

$$\hat{w}_0 = \log \frac{P_1}{P_0}. \tag{21}$$

Then we define the following parameters:

u_i: results of events detection by individual modules or sensors,
m: number of points indicating that the event has occurred
n: number of points indicating that the event has not occurred
m_{1i}: number of points for which $u_i = +1$ and H_1
m_{0i}: number of points for which $u_i = 0$ and H_0
n_{1i}: number of points for which $u_i = +1$ and H_0
n_{0i}: number of points for which $u_i = 0$ and H_1

Because the adaptive fusion method is a digital assessment method, we can derive the following equations for evaluation:

(1) If the module/sensor signal is reliable, then the weight change is (set $\Delta m_{1i} = 1$, $\Delta m_{0i} = 1$).

$$\Delta \hat{w}_i \approx \begin{cases} \dfrac{1}{m_{1i}} \Delta m_{1i} = \dfrac{1}{m_{1i}} & \text{if } u_i = +1 \text{ and } H_1 \\ \dfrac{1}{m_{0i}} \Delta m_{0i} = \dfrac{1}{m_{0i}} & \text{if } u_i = 0 \text{ and } H_0 \end{cases} \tag{22}$$

(2) If the module/sensor signal is not reliable, then the weight change is (set $\Delta n_{1i} = 1$, $\Delta n_{0i} = 1$).

$$\Delta \hat{w}_i \approx \begin{cases} -\dfrac{1}{n_{1i}} \Delta n_{1i} = \dfrac{1}{m_{1i}} e^{\hat{w}_i + \hat{w}_0} \cdot \Delta n_{1i} = \dfrac{1}{m_{1i}} e^{\hat{w}_i + \hat{w}_0} & \text{if } u_i = +1 \text{ and } H_1 \\ -\dfrac{1}{n_{0i}} \Delta n_{0i} = \dfrac{1}{m_{0i}} e^{\hat{w}_i + \hat{w}_0} \cdot \Delta n_{0i} = \dfrac{1}{m_{0i}} e^{\hat{w}_i + \hat{w}_0} & \text{if } u_i = 0 \text{ and } H_0 \end{cases} \tag{23}$$

Finally, we set the adaptive fusion rule of each sensor weight as

$$\hat{w}_i^+ = \hat{w}_i^- + \Delta\hat{w}_i, \tag{24}$$

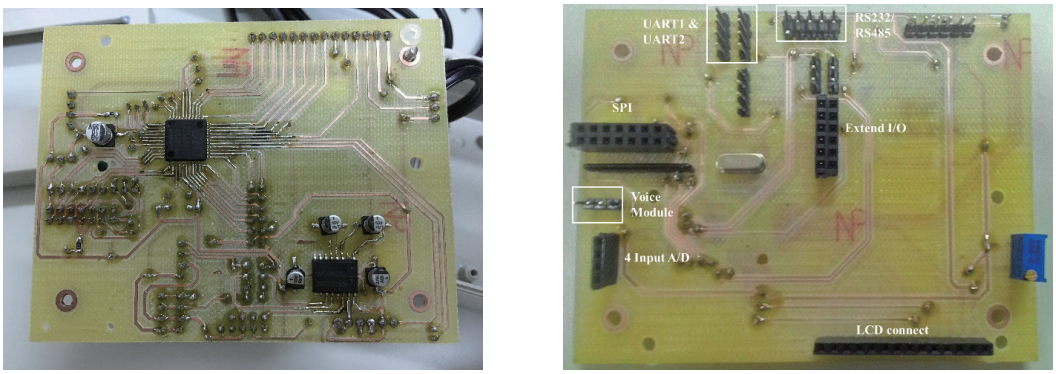
where $\hat{w}_i^+$ and $\hat{w}_i^-$ represent the weight after and before each updating. The criteria that $\hat{w}_i^+$ reach a stable value can be set by the monitoring system.

Using the fuzzy-AHP algorithm on the module and using the adaptive fusion method on the monitoring system reduces the possibility of false positives in the sensor or security system modules and makes the entire system more intelligent.

4. Experimental Results

In the completion of the design of the entire sensing module and the derivation of the algorithms, we completed the actual security system module as shown in Fig. 3. This module is based on the 8051 single chip as the main controller, taking into account considerations of moving freely and the ability to replace sensors or communication modules in accordance with the demand; the entire system is designed in modular fashion. Figure 3(a) is the front of the security system module board, and Fig. 3(b) is the back of the board with all connectors on this side. Figure 4 is the security system module with its outer casing. The user only needs to connect the power supply. Hence, it is very easy to use.

Because this security system module uses the µIP network protocol, we can use a browser to monitor it directly. Figure 5 shows the actual use of this module. The measured data can be



(a) (b)

Fig. 3. (Color online) Circuit board in the security system module: (a) front and (b) back.

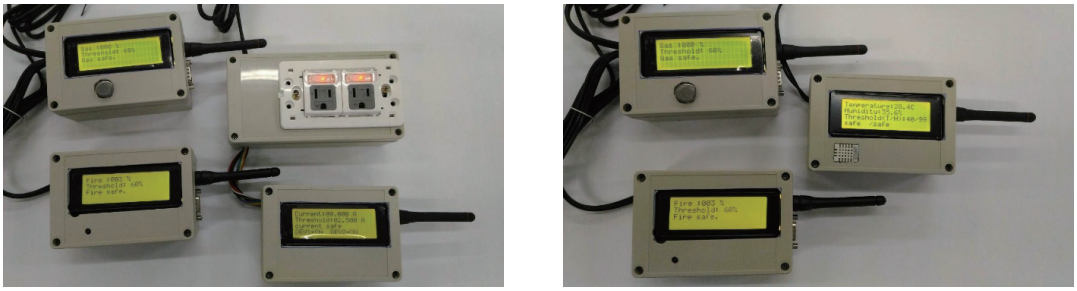
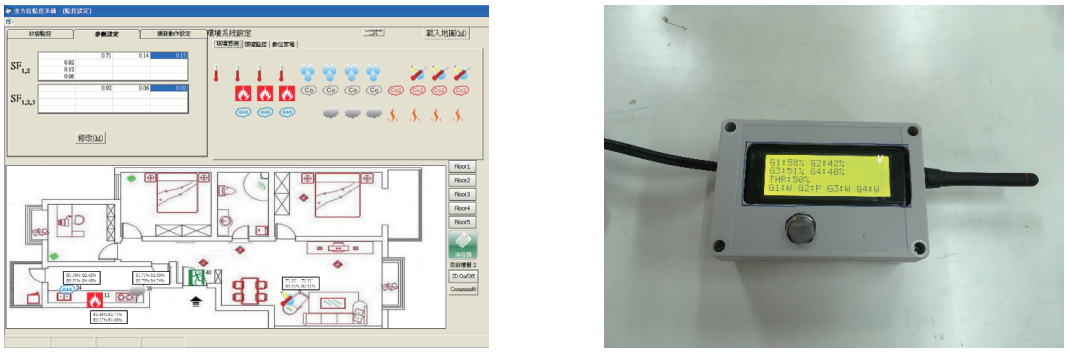


Fig. 4. (Color online) Security system module.

Fig. 5. (Color online) Web-based security system.



(a) (b)

(c) (d)

Fig. 6. (Color online) Integrated modules experimental results: (a) surveillance system, (b) gas module, (c) fire module, and (d) smoke module.

displayed on the module and the web page simultaneously. This allows us to monitor the security system modules via a browser anytime and anywhere. We also developed a central monitoring system. All of the security system modules can be monitored through this system. All data from security system modules are analyzed by the adaptive fusion method. The results are stored in a database. Users can use the monitoring system to send the results or other parameters to a security system module. This makes the whole system more intelligent. Figure 6 shows the integration of the security system modules and the monitoring system.

5. Conclusions

Using a low-cost MCS-51 series single chip, we have designed an "independent operation, central monitoring" security system. We used a variety of communication interfaces and network functions in each security system module at the same time. We used the fuzzy-AHP algorithm in the module to enhance the accuracy of judgment about events, and we used the adaptive fusion method for each analysis in a security system module in the event of incidents in the monitoring system so that the security system module could be more intelligent.

This system is very simple to use. Users only need to connect the security system module to a power supply. The user can determine the current state of the security system module from the LCD and voice module on the unit. Users can also use a browser to monitor the security system modules. In addition, we have also designed a monitoring system that allows the user to monitor or configure the security system module very simply.

We continue to develop a variety of sensor modules for the system so that the system is not limited for use in the home and can be applied to various fields. We will also increase the number of sensors that can be connected to the module and enhance the computing power of the module so that the module has the distributed computing ability. Indeed, this system is already an IoT system. Therefore, we will also strengthen the information security of the modules, so that this system can become a smart sensor network system for industrial applications as well as other applications.

References

1 A. Kujuro and H. Yasuda: IEEE Commun. Mag. **31** (1993) 22.
2 W. Y. Chung, L. C. Fu, and S. S. Hung: Proc. 2001 IEEE Int. Conf. Robotics and Automation (IEEE, Seoul, Korea, 2001) pp. 1981–1987.
3 L. C. Fu and T. J. Shih: Proc. 2000 IEEE Int. Conf. Robotics and Automation (IEEE, San Francisco, California, 2000) pp. 2641–2646.
4 P. Cheong, K. F. Chang, Y. H. Lai, S. K. Ho, I. K. Sou, and K. W. Tam: IEEE Trans. Ind. Electr. **58** (2011) 5271.
5 W. T. A. Budi and I. S. Suwardi: Proc. 2011 Int. Conf. Electrical Engineering and Informatics (Bandung, Indonesia, 2011) pp. 1–7.
6 H. Wang, Y. Zhang, L. Meng, and Z. Chen: Proc. 2011 Int. Conf. Electronic and Mechanical Engineering and Information Technology (Harbin, China, 2011) pp. 3678–3681.
7 J. C. Moon and S. J. Kang: IEEE Trans. Consumer Electr. **46** (2000) 791.
8 R. C. Luo, K. L. Su, and K. H. Tsai: Proc. 2002 IEEE Int. Conf. Robotics and Automation (IEEE, Washington, D.C., 2002) pp. 1777-1781.
9 A. Dunkels: Proc. 1st Int. Conf. Mobile Systems, Applications and Services (ACM: San Francisco, California, 2003) pp. 85–98.
10 J. H. Guo and K. L. Su: ICIC Express Letters, Part B: Applications **8** (2017) 289.
11 N. Ansari, J. G. Chen, and Y. Z. Zhang: IEE Proc. Radar, Sonar and Navigation **144** (1997) 105.
12 N. Ansari, E. S. H. Hou, B.O. Zhu, and J. G. Chen: IEEE Trans. Aerospace Electr. Syst. **32** (1996) 524.