

Sensor Network in Czech General Aviation

Jakub Kraus

Department of Air Transport,
Department of Air Transport, Faculty of Transportation Sciences, Czech Technical University
Horská 3, Praha 2, 128 03, Czech Republic
e-mail: krausjak@fd.cvut.cz

Abstract – This article focuses on possible use of sensor network in general aviation in Czech Republic for ensuring safety and security at small aerodromes.

Keywords – Sensor network, WSN, GA, security, aerodromes

I. INTRODUCTION

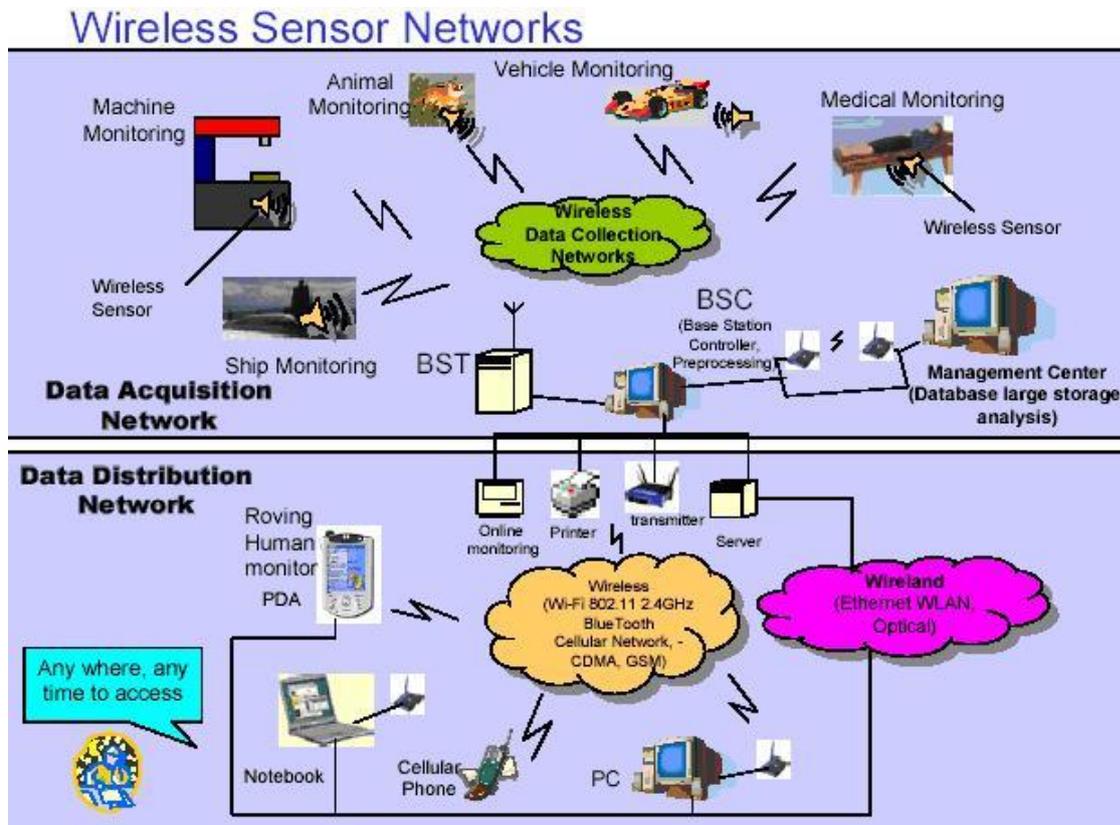
Protection of the aerodrome and its surroundings in terms of security and safety is very important and today is at major airports at a very high level. Despite the high level of protection and the latest X-ray equipment there are still cases where passenger can somehow trick the security system and carry prohibited thing or substance to the board where it could endanger the health or even the lives of passengers. Therefore, the development of new and more sophisticated systems continues, to try to prevent similar situations.

Protection of the aerodrome is at a level at which the effectiveness of the weakest part is. For this reason it is very

important not to underestimate and neglect security of less used or even unused areas. To protect these areas is good to use the technology of wireless sensor networks. Securing such a place with a few thermal imaging cameras can perfectly replace the guards with a view for saving the company considerable amount of money. Unfortunately, the cost could be much higher compared with employee salaries and so it is important to analyze whether the technology could secure the space in the same or better way and how much differ the financing of both types.

From the perspective of general aviation (GA), the situation is even more complicated by the lack of funding for small aerodromes, which sometimes do not even have basic security, which every airport should have.

FIGURE I – GENERAL PRINCIPLE OF WIRELESS SENSOR NETWORKS [1]



II. WIRELESS SENSOR NETWORK

Sensory networks consist of variously spaced separate sensors that monitor some physical properties and send this information over the network to the master server.

Sensor itself converts non-electric value into a numeric value. For the actual operation, however, requires the transmitter with antenna, the control unit and an energy source, which is usually the battery, respectively in combination with other sources of renewable energy (solar cell). That, what affects the possible use of sensor networks are the types of sensors and their ability to capture a certain variable.

Sensors can be divided into:

a) Active - radiate energy into their surroundings. Active sensors generate their working environment by active intervention into the surrounding space (transmit electromagnetic waves). Subsequently, the input signals are compared with pre-defined criteria.

b) Passive - these sensors only observes their surroundings and responds to physical changes (change in temperature, position...). Passive sensors are unlike the active ones harder to identified and thus for the intruder more dangerous and for the entire security system more efficient.

According to the character of the area guarded by active sensors they can also be divided into:

a) Space sensors - sensors react to any disturbance of the protected area. They are suitable for the monitoring of rooms and smaller spaces.

b) Directional sensors - sensors reacting only in a certain desired direction. These sensors are ideal for monitoring in areas that are poorly visible from the current location of space sensors. They are used to monitor poorly visible corners, where they are placed windows, doors, outputs from the ventilation shafts and other potential opportunities for an illegal intrusion.

c) Barrier sensors - the sensor response to distortion in every place of the entire barrier, which is created by the radiation or sensory characteristics or the sensor. They are used as the overall security system for facility or monitored area. Barrier sensors are one of the most commonly used systems for buildings.

d) Positional sensors - sensors reacting to change of the position of the sensor itself or the object which is guarded. This is for securing small or movable objects, for example aircraft.

TABLE I – SENSOR TYPES (I.E.)

Components of outdoor perimeter protection	- Microphone, Geophone
	- Infrared barriers
	- Microwave barriers
	- Slotted cable
	- Ground pressure hoses
Components of surface protection	- Perimeter passive infrared sensors
	- Contact
	- Destructive
	- Destructive symptoms
Components of space protection	- Acoustic pressure
	- Barrier sensors
	- Passive infrared sensors
	- Active infrared sensors
Components of subject protection	- Ultrasound sensors
	- Microwave sensors
	- Combined dual sensor
Control devices	- Shake sensor (Seismometer)
	- Sensor to protect hung objects
	- Capacity sensors
Special sensors	- Acoustic pressure
	- Blocking locks
	- Switch and release locks
	- Code keypads
	- Control and display components
Special sensors	- Card control
	- pressure sensors
	- Foot mats

Using electrical and electronic networks consisting of sensors with different object can provide the following ways:

a) Perimeter protection - protection signalling disruption of aerodrome perimeter, for example shake sensors, microphone wires, lights etc.

b) Shell protection - signals aerodrome building envelope distortion. This is the installation of sensors to the input units, such as windows, doors, but also exterior walls, ceilings, roofs, etc.

c) Spatial protection - provides the protection of the reference area and any abnormal movement or activity triggers a signal. It uses sensors with sensing movement or thermal imaging.

d) Subject Protection - this protection is used to protect the specific subject. These include detecting or improper manipulation of guarded object.

e) Multistage protection - the best. This means that for one protected object or building is used multiple types of protection.

III. COMPARISON OF SENSOR NETWORKS AND CLASSICAL SECURITY

Applying sensor networks in aerodrome security has undoubtedly huge potential. But if we want to get the most out of the available options and technologies, the best solution, as in many other cases, is a combination of classic security and new electrical and electronic systems. Many classical security elements can be replaced by new technology which may often have more varied options. But nobody can easily replace all the classic elements using sensor network. If we really want to do this, it would lead to unnecessarily complex structure and huge costs. Still, we cannot completely get rid of staff, since sensor network will require repair and maintenance.

The best level of security is achieved, if we fully apply both security options. As traditional security, or sensory network itself could ensure security alone. By taking advantage of both, all systems will be duplicated. Whole process, however, becomes too complex and the costs of creating and maintaining it are too high. Very high level of security for very high price is not economically feasible, and therefore we must find another solution.

Purely classical security has got from the historical development good standards and processes. However, we had to occupy all the places that we wanted to actually directly monitor by security personnel. This would require a large number of employees, which is very expensive. Ensuring such security system would mean more jobs for management and organization of security personnel and all associated activities. In addition to this we have to consider the construction of costly solid barriers that would prevent entry of unauthorized persons. Therefore, the use of classical elements of security today would mean an unnecessary anachronism and a return to the now outdated and unsatisfactory trends. The overall level of security would be not today satisfactory, although the advantage would be high speed of response to adverse event.

Creating a fully complex electronic sensory network seems to be a very good solution on one side; minimize the need for employees, maximum automation, and high level of reliability thanks to new technologies. Despite the relatively higher costs of construction the running costs are relatively low with little less complexity of operation. Sensory Network also has an additional advantage that one of its main characteristics is predictive capabilities and reveals hidden threats. And predictive protection is the direction of today's security philosophy. Additionally indisputable advantage of sensory networks can be found in the possibility of their connection with other systems. The sensory network is ideal for the monitoring of large areas, especially at night or in poor visibility, and also smaller areas without staff on site to monitor situation.

The best solution will thus be a combination of both systems. By taking an advantage from both sensory network and classical security we get excellent predictive capabilities and sufficient flexibility and speed of response. In the case of small aerodromes that means at least provide some security.

IV. GENERAL AVIATION AIRPORT SECURITY

In this chapter I would like to show the practical use of security technologies to smaller aerodromes for general aviation. The main issue, already mentioned above, is finance; therefore the security design must satisfy the condition of low prices. Therefore we must use only suitable technologies that are economically reasonable.

If there were a sufficient amount of funding, the ideal structure would be solid fence supplemented by CCTV. The fencing could be replaced by the motion sensor. All objects will be secured with CCTV and motion sensors, together with other various sensors. All information and especially sudden changes would be forwarded to the security service. According to the size of the aerodrome would be chosen number of security personnel. At minimum, however, one employee had to monitor systems directly from the headquarters and decide on action and solutions. In extreme cases, it may be sufficient to have just this one employee to address individual situations flexibly.

The whole complex system must be designed directly to a specific aerodrome according to current needs. Structure of the network will depend on the disposition of the buildings, the area, traffic density, the probability of security risk and security requirement. Sensory network structure will be different at each aerodrome, though all will depend on the same basic philosophy.

A. *Securing the perimeter*

Fence is used for security perimeter, which is relatively expensive or is used appropriately placed CCTV to scan the most vulnerable part of the aerodrome. With this technology, it is necessary to have an employee who would sit at the monitor and watched outputs from cameras. Another option is laser barriers to guard the aerodrome area disruption. In the event of disruption, there is again the need for CCTV which could detect intruders. Although none of the technologies guarantee perfect security of aerodrome perimeter, lower cost of laser sensors prefers them before the fence.

B. *Person Monitoring*

For monitoring of persons at the aerodrome we cannot use technology like screening points, pre-screening, X-ray and other from the big aviation, because of their high costs. At smaller aerodromes, the designation used for persons monitoring within the guarded area are ID cards provided with photos and information about its owner. Anybody is able to get one after successfully passing security training. Although this technology is less secure than others, it is used because of its affordability. Therefore every ID card could contain position transmitter to ensure monitoring of

employees and visitors to the airport. If every ID card had the green and red areas for movement, it would not be a problem to detect the intruder using smart software for ID cards movement evaluation.

C. Hangars security

The only thing the owner want strongly guard is his fleet stored in a hangar. Here should everybody invest in security equipment specializing in the protection of larger objects. These technologies work on the principle of sensing movement and distortions of entrance doors and windows. Price of such security system is not that astronomical and is very accessible to all small general aviation aerodromes. This security system is a good feature to protect the fleet and its efficiency is at a very high level.

V. CONCLUSION

In this article, I described a general introduction to sensor networks and their potential application to secure GA aerodromes. Sensory networks are becoming an increasingly attractive security option and if the system is properly designed then it has excellent results. Last but not least, sensor network are cheaper to purchase and operate than other types of security measures.

The use of sensory networks for aviation has a very large scope and it is advisable to focus attention on it, because it is small airports, which lacks security.

VI. ACKNOWLEDGEMENTS

This paper was supported by the Grant Agency of the Czech Technical University in Prague, grant No. SGS12/165/OHK2/2T/16.

REFERENCES

- [1] Wireless Sensor Networks - A Market Research Report. The Dolcera Blog. [online]. Available at <<http://blogs.dolcera.com/blog/2009/08/02/wireless-sensor-networks-a-report/>>
- [2] Frank, Randy: Understanding Smart Sensors / Randy Frank. -- Norwood : Artech House, 1996. -- xvi, 269 s., ISBN 0-89006-824-0
- [3] Handbook of sensor networks : algorithms and architectures / edited by Ivan Stojmenović.. -- Hoboken : Wiley-Interscience, c2005.. -- xvii, 531 s. : il., ISBN 0-471-68472-4
- [4] European Workshop on Wireless Sensor Networks (3. : 2006 : Curych, Švýcarsko): Wireless sensor networks : third European workshop, EWSN 2006, Zurich, Switzerland, February 13-15, 2006 : proceedings / Kay Römer, Holger Karl, Friedemann Mattern (eds.).. -- Berlin : Springer, c2006.. -- xi, 341 s. : il.. -- (Lecture notes in computer science, ISSN 0302-9743 ; 3868), ISBN 3-540-32158-6
- [5] Callaway, Edgar H., jr., 1958-: Wireless sensor networks : architectures and protocols / Edgar H. Callaway, Jr.. --

Boca Raton : Auerbach, c2004. -- xvi, 342 s. : il. ISBN 0-8493-1823-8

- [6] Sensor technology handbook / editor-in-chief Jon S. Wilson. -- Burlington : Newnes, c2005. -- ix, 691 s. : il. + 1 CD ROM, ISBN 0-7506-7729-5

- [7] ICAO Annex 14 / Předpis L 14