WIRELESS SENSORS FOR AEROSPACE – SMART WAY OF ENABLING WIRELESS REMOTE INSPECTIONS

M. Sessinghaus and T. Wollweber
SILVER ATENA Electronic Systems Engineering GmbH,
Hein-Saß-Weg 36, D-21129 Hamburg, Germany

Abstract

Novel wireless remote inspection methods for identifying structural damages or system conditions have evolved over the last years motivated by new lightweight parts made of composite materials and with increasing system complexity. One smart way of enabling remote inspections can be performed through the use of Wireless Sensor Networks. This energy-efficient wireless technology has reached a maturity level that brings the industry in the position to advertise COTS products based on standardized communication protocols. The IEEE 802.15.4 is such a well-established communication standard already used in many control and monitoring applications beyond aerospace.

This paper aims to provide the reader with a case study about wireless remote inspection of aircraft systems in order to understand the wireless communication and operational performance limits of the CSMA/CA protocol as part of IEEE 802.15.4. This paper provides also a brief overview about some aerospace applications, expected benefits as well as future challenges for designing wireless remote inspection applications using Wireless Sensor Networks.

1. INTRODUCTION

Safety by inspection is indispensable for ensuring airworthiness of aircraft vehicles. Efficient inspection of aircraft systems is of increasing concern to airlines in order to reduce total operating costs. The ICAO has determined in 2001 that direct maintenance costs add up to 11 % of the total operating costs. Inspection as part of the maintenance process has evolved during the last years from manual inspections with check sheets towards automatic inspections. Fact is that inspection data on check sheets are highly error-prone meaning entries are indecisive, illegible and thus difficult to understand if those results are required to be entered into a database [1]. Automatic inspection methods reduce or eliminate the drawbacks of sheets-based manual inspections. Automatic means that the use of a portable inspection tool (e.g. PDA) allows for electronic capture of the data. Such automatic inspection tools often use probes to directly inspect the system. Some drawbacks of these tools are that cables and connectors come along with practical limitations like tool flexibility, data handling, and usage in hazardous areas or user mobility. Being smarter to mitigate or eliminate these drawbacks could be provided with wireless sensors embedded into structures (e.g. wings, fuselage) and systems (e.g. engines, landing gear) to support automatic and cable-free remote inspection tools. These tools implicate wireless sensors which are smart devices providing low-power processing and wireless communication capabilities.

This paper is organized as follows. Chapter 2 motivates the use of wireless sensors for aerospace applications such as structural health and condition-based systems monitoring.
Chapter 3 introduces the Wireless Sensor Network technology with a brief survey on hardware properties and commercially available platforms. Then, the crucial benefits and challenges will be described to keep in mind when designing WSN based communication systems for aircraft inspection or other aerospace applications. Furthermore, an overview about low power radio standards and energy-saving strategies will be given for the IEEE 802.15.4 standard.
Chapter 4 describes our case study about wireless remote inspection of aircraft systems. Furthermore, the CSMA/CA protocol as part of the IEEE 802.15.4 will be analyzed for this case study in order to evaluate the wireless communication performance and operational lifetime limits.
Finally, Chapter 5 concludes with a summary.

2. WIRELESS SENSORS FOR AEROSPACE

Novel wireless remote inspection methods for identifying structural damages or system conditions have evolved over the last years motivated by new lightweight parts made of composite materials and with increasing system complexity. Structural or systems health monitoring refers to continuous monitoring in order to reliably detect damages or system failures. In the following, some aerospace applications for structural and system health monitoring will be presented which already benefit from using Wireless Sensor Networks.

The aerospace industry has recognized the beneficial use of WSN for space habitats, spacecraft and ground testing equipment [2]. Integrated vehicle health monitoring (IVHM) of aerospace vehicles is absolutely required for safety. But before WSN will proliferate in IVHM applications, power, volume, and mass must be reduced as well as issues like electromagnetic interference, thermal dissipation, or shock must be addressed.
Future spaceflight applications [3] could also benefit from WSN, particularly when robust and reliable sensor hardware and software (e.g. communication protocols) is available which meets the special mission-critical requirements (e.g. power, radiation, years-long service lifetimes, etc.). In [3], the IEEE 802.15.4 standard has been evaluated in a Lunar Habitat Wireless Testbed. Wireless accelerometer sensors were connected to monitor the habitat hull and results were collected at a base station. Concurrent WLAN transmissions took place in the same 2.4 GHz frequency band and disrupt the IEEE 802.15.4 connections. The author criticized the communication reliability of IEEE 802.15.4 due to the lack of frequency agility. But co-existence between wireless systems can be ensured reactively per system design (e.g. channel adaptation) or proactively by standardization bodies, e.g. defining a dedicated frequency spectrum to protect wireless transmissions. Then, WSN could be successful for mission-critical spaceflight applications.
In [4], a distributed aircraft engine control application was presented. Heavily shielded analog wire harnesses (network bus) are used to connect sensors with the engine controller. Thermal as well as mechanical shielding imparts a heavy weight penalty. Using wireless sensors can help to simplify the design of such a safety-critical system but provide challenges (see section 3.1) to develop a reliable and secure engine control function. Wireless communication constraints like delay, data loss or bit rate limitations have to be analyzed to evaluate the overall systems performance.
A revolutionary new concept was presented with a “fly-by-wireless” flight control system. This visionary concept aims to replace the current “fly-by-wire” flight control with integrated wireless sensors/ actuators e.g. for unmanned aerial vehicles (UAVs) without substantial increase in weight and complexity. Such wireless safety-critical flight control design requires definitely a dedicated frequency spectrum for operability. Other non-safety critical applications [4] which can benefit from wireless sensors are the environmental control system (ECS), anti-icing systems or hydraulic leaks monitoring.
In [5], a RFID-based sensor approach was integrated for landing gear system health (condition-based) monitoring because today’s operational data provide indirect information. RFID-based sensors allow in situ wireless monitoring of e.g. hard landings providing enhanced information. Implementing such an Integrated System Health Management process (ISHM) could enable predictive-based maintenance, optimized levels of spares, reduction in turnaround time, and so on. Finally, the use of ISHM for the landing gear system provide long-term condition monitoring of life-limited parts which will lead to an improved design and maintenance quality.
Having read WSN-based applications from the aerospace sector, the next chapter will briefly introduce the WSN technology [6], [7] expected benefits and challenges.

3. WIRELESS SENSOR NETWORKS

At the turn of the millennium, technical advances in microelectronics and radio transceiver design, particularly the production of miniaturized, energy-efficient and powerful integrated circuits, promote the evolution of Wireless Sensor Networks. A wireless sensor node is a small, battery-operated device with the capability to capture physical or environmental conditions like pressure, temperature, vibration and to process and wirelessly transmit these sensor data through a network [6]. The main components of a wireless sensor node are [7] (see Figure 1):

- Sensor(s)/actuator(s): These pluggable devices are able to convert analog readings into digital data; as integral part of the sensor node or attached as extension supporting different digital serial interfaces like I2C or SPI.
- Controller: A microcontroller is used to operate energy-efficiently with a low clock frequency in the order of MHz and low memory footprint in the order of kilobytes.
- Transceiver: A radio device that handles data messages for transmitting/receiving over the antenna. The gross data rate and dissipated power are very low compared to WLAN (802.11b: 11Mbps, 20 dBm). Ultra-low power radio standards like IEEE802.15.4 [8] have approximately 250 kbps@+3 dBm.
- Memory: It is used to store data using volatile (e.g. RAM) and non-volatile memory (e.g.

Flash). Only non-volatile memory keeps data without power supply.

- Power supply: Supplying all attached node components needs a small power supply integrated in a single housing. The most widely used types are batteries like primary or rechargeable cells. A totally different type of autonomous power supply provides energy harvesting which captures energy from the environment (e.g. solar, vibration, temperature, rotation). For example, the rotation energy from the landing gear wheels can be captured to supply a wireless sensor node for tire pressure monitoring.

Innovative circuit designs had led to wireless sensor node packaging as System-on-Chip (SoC), i.e. all components except the power supply and sensors are fully integrated on a single chip as illustrated in Figure 1.

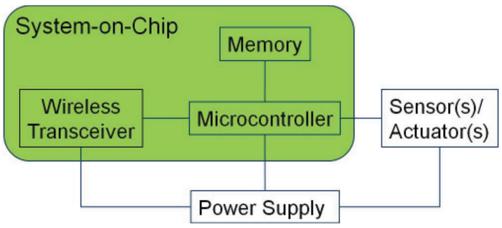

Figure 1: Main Components of a Wireless Sensor Node

The SoC design aims to further improve the power consumption, packaging, and weight compared to System-in-Package (SiP) solutions. SiP designs contain all integrated circuits on a single package or module. The appendix shows the specification of three commercially available (COTS) WSN platforms in SoC design.

3.1. Benefits and Challenges

The use of WSN technology for remote inspection (maintenance) of aircraft systems and structures provides large benefits and challenges.
The usage of WSN provides the following crucial benefits:

- Cable- and connector-free: No need of signal cables, harness or connectors to perform remote inspections. This implicates overall system weight reduction.
- Mobility awareness: Wireless provides user mobility, i.e. inspections can be performed more flexible from the distance.
- Energy efficiency: Wireless sensor nodes provide ultra-low power operation due to the hardware and communication protocol design. This favors the development of miniaturized, lightweight and powerful systems for various applications in the aerospace sector.
- Wireless data loading: Thanks to the use of a wireless interface, data loading like firmware or configuration updates can be transferred over-the-air.
- Efficient maintenance: For example, predictive-based maintenance methods (by performing continuous monitoring to predict failures) can be installed and performed more efficiently because wireless enables automatic remote inspections.
- Localization: Providing localization capabilities could give better orientation for the maintenance staff to find the system/sub-system to be investigated. The localization accuracy depends mainly on the used frequency, propagation environment and the underlying localization algorithm (e.g. at 2.4 GHz, ca. 1-2 m accuracy).
- Retrofit: A wireless upgrade of existing maintenance procedures and aircraft systems is desirable to enhance inspection services and system design to save costs.

There are some challenges to address when using WSN technology for remote inspection applications:

- Radio frequency: The radio frequency usage for wireless inspections shall be regulated and harmonized worldwide to ensure failure-free, reliable and secure inspection operation. For instance, the 2.4 GHz band is licensed-free and worldwide available. But WLAN, Bluetooth and ZigBee (IEEE 802.15.4) use similar frequency bands (channels) and can cause interferences.
- Wireless reliability: Everyone perceives wireless communication sometimes unreliable in daily life with using mobile phones or WLAN. Wireless systems shall operate reliable; particularly in case of safety-critical applications. Redundant communication and dedicated protected frequency spectrum could be two solutions to ensure wireless reliability.
- Wireless security: In principle, any wireless communication is vulnerable due to the shared medium (as opposed to a dedicated wire). Security mechanisms are required to protect it against unauthorized access, disruption or any other threats [9]. For example, the ZigBee protocol [10] defines a security layer with a 128-bit AES encryption/decryption engine.

Wireless now becomes indispensable to provide a flexible and cost-effective remote inspection solution. Certainly, the seamless WSN technology integration into the maintenance process makes it valuable and productive for maintenance shops. Aspects like integration and processes will not be addressed in this paper.
The next chapter presents existing wireless radio standards where the IEEE 802.15.4 provides a low power (energy-efficient) standard.

3.2. Low Power Wireless Communication

Until now, many wireless radio standards have been developed to satisfy different user needs from short-range towards mid-range communication. The continuous increase of data rate becomes as important as the decrease of power consumption. Figure 2 and 3 show existing radio standards with details about transmit power and data rate vs. range. It can be seen that for short-range communication (up to 100 m in outdoor) Bluetooth, Ultra-Wide Band (UWB) and ZigBee/802.15.4, the transmit power varies from 100 µW up to 100 mW. It has to be mentioned that UWB provides the best low-power footprint but commercial systems are not available today. In this paper, we evaluate the IEEE 802.15.4 radio standard [8], [10] because it has been designed for energy-efficient wireless control and sensor monitoring applications.

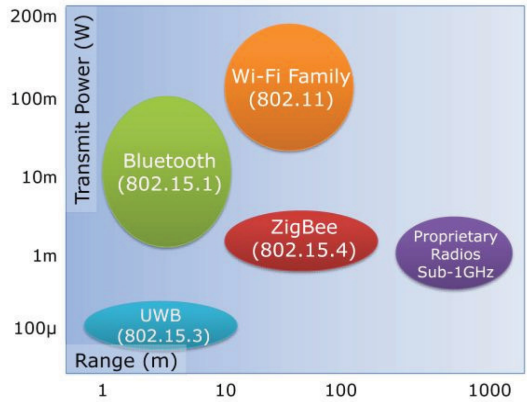

Figure 2: Wireless Radio Standards – Transmit Power vs. Communication Range

Consider now the data rate for the different wireless radio standards in Figure 4.

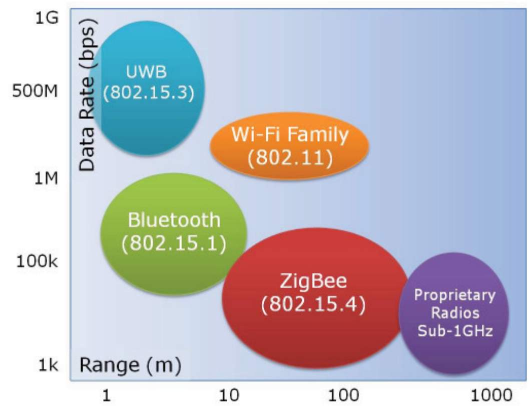

Figure 3: Wireless Radio Standards – Data Rate vs. Communication Range

UWB supports up to 1 Gbps on very short distances below of 10 m. UWB operates in the frequency band from 57-64 GHz (802.15.3c standard) which results in higher signal attenuation and thus shorter range compared to the other standards. ZigBee/802.15.4 operates in the lower frequency band 2400-2483.5 MHz and provides ranges at about 100 m. Generally, the communication range depends mainly on factors like used frequency band (channel bandwidth), antenna, transmission power, receiver sensitivity, and RF propagation effects (e.g. loss in signal strength). The gross data rate describes a raw bit rate (including signaling overhead) and was defined to 250 kbps in IEEE 802.15.4 at a bandwidth of 2 MHz per channel for ideal conditions.

But in real communication scenarios we may expect signal degradations due to the multipath environment (resulting in direct and reflected signals) and interferences by other signal transmissions in the same frequency band (channel). This leads in worst case to a corrupted signal which cannot be reconstructed at the receiver site. Then, a signal retransmission can be immediately initiated to have a transmission success. If this will be done several times, the transmission time until the data is received successfully will increase to a maximum number of retries. This leads to an achievable data rate which is quite lower than the gross data rate of 250 kbps.

Before we evaluate this relationship in Chapter 4, we will first describe the communication protocol stack of the IEEE 802.15.4 standard [8], [10] and explains the major sources of energy consumption [7].

3.3. IEEE 802.15.4 & Energy-Saving Strategies

IEEE 802.15.4 is a well-established wireless radio standard widely used for many WSN applications: Lighting control, smoke and fire detection, tire pressure monitoring, gaseous detection, etc. This standard defines a protocol stack, a set of communication rules implemented in two layers namely the Physical (PHY) and the Media Access Control (MAC) layer as shown in Figure 4. The PHY layer specifies different frequency bands whereas the 2.4 GHz frequency band is regulated and harmonized worldwide. The de-facto ZigBee (www.zigbee.org) standard specifies additional layers with the network, security, and API layer. Finally, the user defines on top its customized application. For more details the reader is referred to [10].

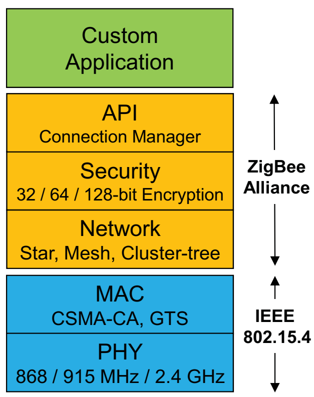

Figure 4: Communication Layers (IEEE 802.15.4/ZigBee)

The focus in this paper is on the MAC layer because Chapter 4 evaluates the CSMA/CA (IEEE 802.15.4) performance. The MAC function is to control the shared medium access of each anticipated wireless sensor node in an energy-efficient manner. It has to be noted that a bad MAC design can lead to dramatic communication reliability and energy limitations. In practice, the MAC functions should be configurable software which can be adapted to the applications need, for example, configuration of parameters like back off timer, clear channel assessment, etc. [10].

The major sources of energy consumption are idle listening, overhearing, data collisions, and protocol overhead [7].
Idle listening means that the transceiver being in idle is ready to exchange data but is not currently receiving anything. The active (idle) state still consumes a significant amount of energy. Switching off the transceiver to an inactive (sleep) state can help to reduce energy consumption. But state changes also cost energy; their frequency should be kept as small as possible. This relation is known as transceiver duty cycle and can be affected by the MAC design. Figure 5 shows the duty cycle which is determined by the portion of time spent for the active state to the total time (transmission cycle).

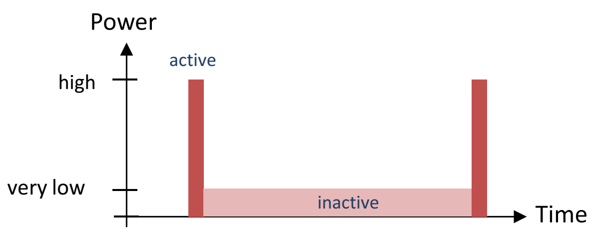

Figure 5: Principle of the Duty Cycle with the Transceiver States Active and Inactive

The transceiver consumes much more power in the active state which might be factor 1000 larger than in inactive state (see appendix). Generally, send fast (with a high data rate) and immediately going to sleep is the rule to save energy.
Overhearing leads to waste of energy and occurs due to the fact that all nodes in transmission range to each other hear a data packet and drop it when it is not addressed to them; these nodes overhear the data packet.
Data collisions implicate useless transmit and receive costs. Hence, collisions should be avoided by the MAC design, for example, fixed assignment of time slots in GTS or collision avoidance procedures defined in CSMA/CA of IEEE 802.15.4. However, if the network load or duty cycle is always sufficiently low then data collisions are not a problem.
Protocol overhead is induced by message signaling e.g. by request packets. This overhead should be kept as small as possible. For example, a kind of signaling is time synchronization in order to perform a time-slotted MAC protocol (e.g. GTS) which introduces additional overhead but ensures no data collisions (only if synchronization is accurate).

Back to the MAC layer of IEEE 802.15.4 which defines two medium access strategies termed as GTS (Guaranteed Time Slots) and CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). The CSMA/CA protocol works as follows: Each node transmits only if the medium is free (by carrier sense). If the medium is busy, the node falls into a back off (collision avoidance) and chooses a random time to restart its transmission. This strategy is simple because no explicit coordination by a master is required and the protocol overhead is low compared to time-slotted MAC strategies like GTS. But if the number of transmitting nodes is too large then data collisions (data loss) increase and data throughput decreases for each node.
The next chapter will evaluate the CSMA/CA performance motivated by a case study about wireless remote inspection of aircraft systems.

4. WIRELESS REMOTE INSPECTION OF AIRCRAFT SYSTEMS

Imagine that maintenance staff stays in front of a parked aircraft and wants to perform a pre-check flight inspection of many systems at different locations (e.g. landing gear, engines, leading/trailing edge, or tail plane) as illustrated in Figure 6.

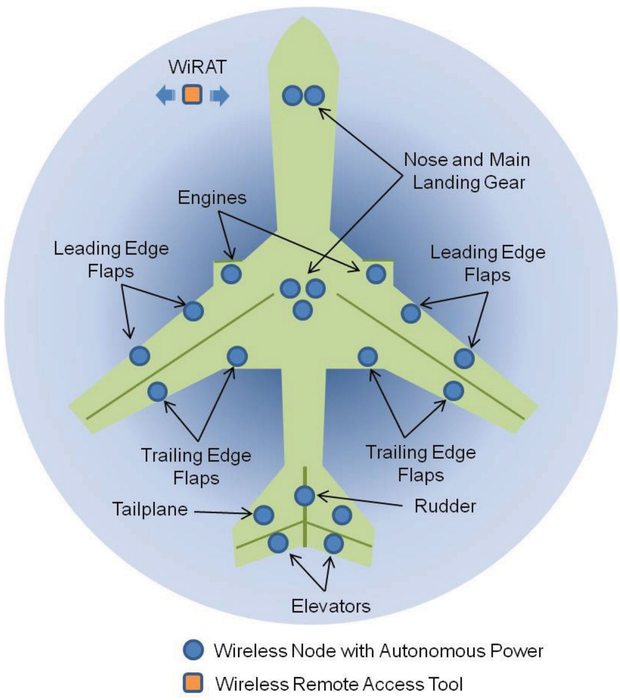

Figure 6: Wireless Remote Inspection Scenario with Distributed Wireless Nodes at different Aircraft Locations

No visual inspection is required; that saves valuable inspection time and leads to improved aircraft turn-around time. Because the way of doing inspections now is different thanks to the use of a wireless remote access tool called WiRAT (e.g. PDA, netbook) to get automatically the system status. It is therefore necessary that each system integrates the WSN features, particularly a wireless communication interface and battery supply because the aircraft power is usually shut down. Then, the maintenance staff initiates a status request from its WiRAT to the end systems. These end systems wake up and reply immediately with their status data. The maintenance staff collects all data in a few seconds. This is how wireless remote inspection might look like – easy and fast.

Now, we ask ourselves how long the aircraft systems (e.g. landing gears' tire pressure monitoring subsystem) can operate without changing batteries. Essentially for airlines who might like almost maintenance-free systems to save costs. The second question could be interesting for the system engineer who specifies the wireless communication protocol and battery capacity of the WSN based end system. System engineers may ask whether the end system is sufficiently designed to provide status data reliably for a long operational lifetime (until batteries must be changed).
The next two sections describe the case study setup and settings as well as the CSMA/CA performance results.

4.1. Case Study Setup

The following model assumptions were made to evaluate the wireless remote inspection scenario: Let us assume that the data (e.g. temperature or pressure signal) has a sample width of 16 bit (2 byte) and a transmit interval from 0.5 to 2 seconds.
The transceiver settings were chosen according to Atmel's ATmega128RFA1: Transmit current (active state) of 14 mA, power output of +3 dBm, a sleep current of 0.2 µA (inactive state) and a wake-up time (including TX/RX switching) of 400 µs. The gross data rate was selected to 250 kbps at 2.4 GHz with an occupied bandwidth of 2 MHz. To simulate the reliability of the wireless data transmissions, we have assumed a Packet Error Rate (PER) of 1 %. The used battery capacity for each system was chosen to be 1200 mAh. Of course, larger battery capacities can be chosen and impacts the results linearly.

Assume that no wireless aircraft network infrastructure is in service because the onboard power supply is off. The battery-operated wireless sensor nodes shall be able to communicate energy-efficiently and without centralized coordination. Sensor data are wirelessly exchanged only within a network domain. The network domain is defined as radio coverage where all nodes are in transmission range to each other as shown in Figure 6. Furthermore, the maintenance staff requires no knowledge about the type and number of systems to be inspected. This will be, for example, automatically registered during the wireless remote inspection procedure.

4.2. Performance Results

To evaluate the communication performance and power consumption using CSMA/CA for the given inspection scenario, we have defined two metrics: (1) maximum achievable data rate and (2) battery lifetime.
In practice, the achievable data rate within the network domain is lower than 250 kbps as defined by the IEEE 802.15.4 standard. It is limited mainly by the carrier sensing and collision avoidance strategy of CSMA/CA and the transceiver timing constraints of the used hardware (ATmega128RFA1).
The maximum achievable data rate is 127 kbps per frequency channel [11]. This is the case when the channel is free and the packet error rate is zero; thus no retransmissions are required to transmit a maximum data payload of 114 bytes (equals to 57 sensor samples) as shown in Figure 7. In reality, packet errors exist and thus retransmissions are required to transmit data successfully with a data rate smaller than 127 kbps.

Figure 7 shows the gross data rate over the number of supported nodes within the network domain. This number ranges from 1 to 30 limited by the payload size (number of samples) and the maximum achievable data rate of 127 kbps.
These performance limits could be relaxed with e.g. using multi-channels to increase both the payload size and number of supported nodes for each sub-network. But this introduces additional protocol complexity to allocate a free channel for each group of nodes.

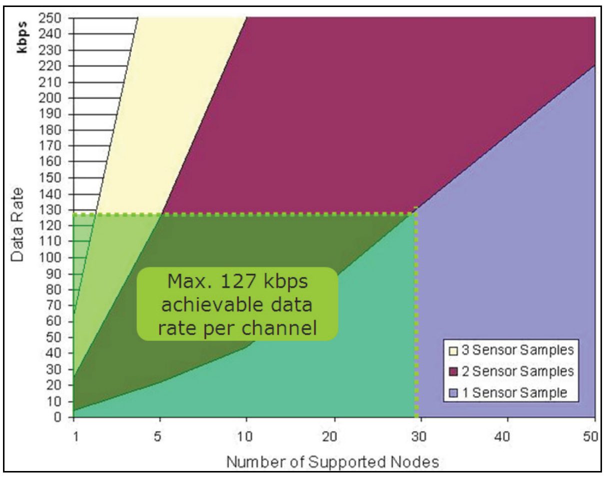

Figure 7: Gross Data Rate vs. Number of Supported Nodes per Channel using CSMA/CA

The transceiver duty cycle determines mainly the battery lifetime as shown in Figure 8. The battery capacity is 1200 mAh; transmission interval starting from 0.5 to 2 seconds for different sensor data payloads varying from one to a maximum of 57 samples (114 bytes) is given. In the best case, the battery lifetime is 6.6 months assuming a payload size of one sample (2 bytes) and a low transmission interval of 2 seconds. The worst case is 0.8 months with the highest duty cycle of 0.014 %.

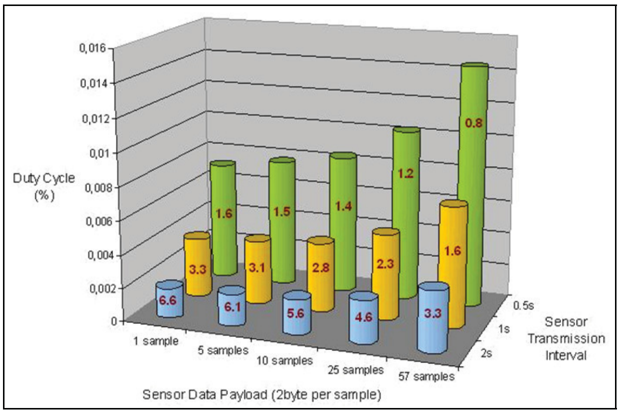

Figure 8: Duty Cycle vs. Sensor Data Payload/Transmit Interval resulting in Operational/Battery Lifetime

Using larger batteries can improve the lifetime. In practice, self-discharge, retransmissions due to poor conditions (interferences, multipath) result in lower operability and finally earlier change of batteries.
The real CSMA/CA communication performance and operational lifetime (using batteries) have shown that this MAC protocol is useful for wireless remote inspections when sensor transmissions are not so frequently and data rates are below of 127 kbps.

5. CONCLUSION

The conclusion to be drawn is that WSN provides not only reducing cables and weight but rather simplification of inspection procedures for structures and systems through the use of energy-efficient wireless communication solutions. Our case study of wireless remote inspection for aircraft systems has shown that the CSMA/CA protocol of IEEE 802.15.4 provides an energy-efficient and reliable remote inspection solution with acceptable communication and operational performances without changing batteries for a long time.

6. ACKNOWLEDGMENT

We would like to thank all reviewers for their suggestions to improve this paper. And we believe that our contribution is valuable for those engaged not only in research and development but also in maintenance and operations.

7. REFERENCES

[1] S. Reilly, Aviation Maintenance Technician Handbook, FAA, Online Handbook, 2008

[2] W. Wilson, G. Atkinson, Wireless Sensing Opportunities for Aerospace Applications, Sensors & Transducers Journal, Vol. 94, Issue 7, July 2008

[3] R. S. Wagner, Standards-Based Wireless Networking Protocols for Spaceflight Applications, IEEE Aerospace Conference 2010, 6-3 March 2010

[4] R. K. Yedavalli, R. K. Belapurkar, Application of wireless sensor networks to aircraft control and health management systems, Journal of Control Theory and Applications, Springer, January 2011

[5] B. Pátkai et al., Requirements for RFID-based Sensor Integration in Landing Gear Monitoring – A Case Study, Auto-ID Lab, UK, 16 July 2007

[6] I. F. Akyildiz et al., Wireless sensor networks: a survey, Computer Networks, Vol. 38, Elsevier, 2002

[7] H. Karl, A. Willig, Protocols and Architectures for Wireless Sensor Networks, Wiley & Sons, 2005

[8] The IEEE Standards Publications, IEEE Part 15.4: Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks, http://standards.ieee.org, 2006

[9] K. Sampigethaya, M. Li et al., Secure Wireless Collection and Distribution of Commercial Airplane Health Data, Third IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'07), 25-26 September 2007

[10] S. Farahani, ZigBee Wireless Networks and Transceivers, Newnes, Elsevier, 2008

[11] Jennic Inc., Calculating 802.15.4 Data Rates, Application Note: JN-AN-1035, 15 August 2006

APPENDIX

The following table presents three WSN COTS platforms in SoC design which are specifically tailored to IEEE 802.15.4 operating in 2400-2483.5 MHz.

Manufacturer	Atmel Corporation	NXP Semiconductors (former Jennic)	Texas Instruments
Product release	Q1/2011	Q3/2010	Q1/2010
Size	9x9 mm	8x8 mm	6x6 mm
Transceiver	ATmega128RFA1	JN5148-001	CC2530
Data rate modes	250 kbps, 1,2 Mbps	250-667 kbps	250 kbps
Receiver sensitivity	-104 dBm	-95 dBm	-97 dBm
Output power /TX	3.5 dBm (2.24 mW)	2.5 dBm (1.78 mW)	4.5 dBm (2.82 mW)
Active/RX	16.6 mA	17.5 mA	24 mA
Active/TX	18.6 mA	15 mA	29 mA
Inactive (sleep)	0.25 µA	0.1 µA	0.4 µA
Microcontroller	RISC (8-bit)	RISC (32-bit)	8051 (8-bit)
Clock frequency	16 MHz	4-8 MHz	< 32 MHz
RAM	16 KB	128 KB	8 KB
Flash	128 KB	1 Mbit (opt.)	256 KB
Power supply	1.8-3.6 V	2-3.6 V	2-3.6 V
Sleep-to-active	240 µs	840 µs	120 µs
Active-to-TX/RX	126 µs	290 µs	192 µs

ABBREVIATIONS

AES	Advanced Encryption Standard
API	Application Programming Interface
COTS	Components-Of-The-Shelf
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
ECS	Environmental Control System
GTS	Guaranteed Time Slot
I2C	Inter Integrated Circuit
ICAO	International Civil Aviation Organization
IEEE	Institute of Electrical and Electronics Engineers
ISHM	Integrated System Health Management
IVHM	Integrated Vehicle Health Monitoring
MAC	Media Access Control
PDA	Personal Digital Assistant
PER	Packet Error Rate
RAM	Random Access Memory
RFID	Radio Frequency Identification
SHM	Structural Health Monitoring
SPI	Serial Peripheral Interface
UAV	Unmanned Aerial Vehicle
WiRAT	Wireless Remote Access Tool
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network