Research into the Radio Interference Risks of Drones

version 1.01, May 2016

Strict b.v. Lange Dreef 11-f Postbus 12 4130 EA Vianen T. 088 55 55 800 F. 088 55 55 801 info@strict.nl www.strict.nl IBAN NL20 RABO 0138 1585 41 BIC RABONL2U KvK 30205458 BTW NL814370925B01

Colophon

Document name	Research into Radio Interference Risks of Drones v1.0
Title	Research into the Radio Interference Risks of Drones
Reference number	16003
Version, date	version 1.01, May 2016
Reference	
Written by	Ir. Gerton de Goeij (Strict), ir. Eildert H. van Dijken (Strict) and ir. Frank Brouwer (FIGO)
Project	100-1050703

Contactdetails for this publication

Strict b.v.
Lange Dreef 11-f
4131 NJ Vianen
T. 088 5555 800
F. 088 5555 801
KvK number: 30205458
http://www.strict.nl

Report Colophon

Overview of Changes

Date	Description	Status
February 2016	V0.4 for review by Agentschap Telecom	Draft
April 2016	V0.9 for review by Agentschap Telecom	Concept
May 2016	V1.0	Final

Reviewers

Name	Organisation
Aart Ballast	Agentschap Telecom
Frans Hofsommer	Agentschap Telecom
Antoine van der Sijs	Strict Consultancy

CONTENTS

ABBREVIATIONS

BVI	Bewijs Van Inschrijving in het luchtvaartregister
CSMA	Carrier Sense Multiple Access
CTR	Control Region around airports
dBm	Decibel-milli watts
DSSS	Direct-sequence spread spectrum
DARPAS	Dutch Association for Remotely Piloted Aircraft Systems
ETSI	European Telecommunications Standards Institute
FAA	Federal Aviation Administration
FPV	First Person View
FM	Frequency Modulation
FHSS	Frequency-hopping spread spectrum
GPS	Global Positioning System
ISM	Industrial, Scientific and Medical
ILT	Inspectie Leefomgeving en Transport
ICAO	International Civil Aviation Organization
LAA	License Assisted Access
LTE	Long Term Evolution
LPWAN	Low-Power Wide-Area Network
NTCV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NLR	Nederlands Lucht- en Ruimtevaartcentrum
OSD	On Screen Display
OFDM	Orthogonal frequency-division multiplexing
RFID	Radio-frequency identification
RC	Remote Control
RPAS	Remotely Piloted Aircraft System
RPA	Remotely Piloted Aircraft System
ROC	RPAS Operator Certificate
STBC	Space Time Block Code
S-BVL	Speciaal Bewijs Van Luchtwaardigheid
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
VNV	Vereniging Nederlandse Verkeersvliegers
VTOL	Vertical Take-Off and Landing
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum
WRC	World Radio Conference

ABSTRACT

Telecom Agency requested Strict and FIGO to conduct a study on the risks of drones using unlicensed spectrum. The goal of the study is to gain insight in the risk of interference between drones and other users of unlicensed spectrum.

The number of drones in the Netherlands still increases substantially. This study looked at micro and mini drones, which are drones up to 4 kilos, for both professional and recreational use. At present, there are an estimated 150,000 of these types of drones in the Netherlands. Exact figures are difficult to obtain because there is no registration of drones required in the Netherlands. DJI is market leader with about 50% of the market. A strong emerging brand is Yuneec.

Research by ILT shows that the number of incidents involving drones doubles each year. The press increasingly reports incidents involving drones. These incidents are not frequency-related. Both ILT and (interviewed) users report that no frequency-related incidents are known. It appears that many users suffer from so-called "fly-aways". In this cases drones fly away for unknowns reasons. There are also reports of uncontrolled landings. This should be seen as an indication of a potential problem, there is no proof that these fly-aways and uncontrolled landings were caused by interference, exact details are not available.

The reference drone architecture is first investigated to understand for which types of communication unlicensed spectrum bands are used and what technologies are used. For the control of the drone the 2.4 GHz is used in most cases, with a combination of FHSS and DSSS technology to make the control channel as robust as possible. Each supplier has its own proprietary implementation of the control channel protocol and these are not compatible. For the video downlink the 5 GHz is widely used with OFDM technology (often Wi-Fi). FM is also used for example by FPV (first person view) race drones. For the telemetry link there are several options, sometimes a separate 2.4 GHz channel, sometimes via on-screen display (OSD) of the video channel and sometimes via Zigbee at 868 MHz.

As part of this assignment we have measured the influence of a drone control on a Wi-Fi connection and vice versa. It was found that the data transfer of a Wi-Fi connection is cut in halve when a drone operates nearby. The other way around the effect is less pronounced, only in one case the drone control was lost shortly. The video link from a DJI appeared to disrupt a Wi-Fi connection considerably

The results of this research have been used in two scenarios. The first scenario is an inspection of a tall office building (with Wi-Fi) by a drone. The second scenario is a drone that is used for crowd control during an event, Wi-Fi is offered to visitors of the event and other users in the neighborhood use Wi-Fi. The conclusion of the first scenario that a drone controller or video transmitter might disrupt Wi-Fi in the office building. The video of the drone connection can be disturbed by Wi-Fi. In the second scenario, drone control can significantly disturb Wi-Fi of end users. Also the reception of video of the drone can be disturbed by the Wi-Fi signals.

Also remarkable is that the market leader DJI seems to cause the most disruption. This is even more remarkable because unlike some other controllers they comply with all regulations, for example the latest

ETSI standard, which is designed to improve cooperation between different users of the spectrum. It is not clear what will happen when other drone controllers are also going to meet this ETSI standard.

We also encountered lot of illegal equipment available via online stores during the investigation, which is actually used in the Netherlands. Because this was not part of the scope of the investigation this was not incorporated in the results.

It can be concluded that there is a significant chance of disruption of Wi-Fi traffic by both drone control and drone video. Conversely, there appears to be little risk of interference of Wi-Fi on drones. It should be noted that this could change if all controllers comply with the latest ETSI standard. Furthermore, little information is available about numbers of drones, frequency related incidents and technical architecture of drones.

1 INTRODUCTION

1.1 Background

Remotely Piloted Aircraft Systems (RPAS) – commonly known as drones – are developing at an incredible speed. There are some huge opportunities for unmanned aviation, new applications and innovations are regularly on the news. The use of drones offers new opportunities for sectors like Public Protection, Disaster Relief, Security, Inspection, Mapping, Building, Journalism and Agriculture.

Drones can quickly and in an easy way deliver measurements and pictures which give valuable information on the actual situation on the ground. But there are also risks to this explosive growth, and these risks are not always clear. One of these risks is the use of license exempt spectrum by drones. Most drones can be considered robots. They are capable of flying autonomous based on their GPS. More capabilities are added like 'detect and avoid' by mapping the area around them, just like robots on the ground. Even though most drones can be considered to be robots it is essential for a ground operator to have a robust radio connection to control the drone. It is required by law to always have visual contact with the drone and being able to control it manually.

Radio connections are also needed to relay the information gathered by the payload. This is in most cased a real time video stream from a camera, but also measurement data or sensor data and sound can be transferred real time. At this moment most drones are using the license exempt frequencies, like the 868 MHz, 2.4 GHz and 5.8 GHz bands. These frequencies are also used for a large number of applications on the ground, like Wi-Fi, home automation and parking sensors. Earlier research by Strict and FIGO showed that many end users currently already experience problems with the use of Wi-Fi in the unlicensed 2.4 GHz band caused by the large number of users.[1] The use of the same license exempt bands by these applications can have an effect on

[1] Van Dijken, E.H., Brouwer, F. en Lippman, T. (2015), *Research into the License Exempt Spectrum of the Netherlands*, FIGO and Strict.

drones and vice versa. This can happen especially when different technologies are mixed, like Wi-Fi and frequency hopping remote control. Drones flying high in the air can impact a large area on the ground which can potentially have a large effect on these applications.

In a previous research project by Agentschap Telecom in 2014[2] it was already mentioned that the usage of the 2.4 GHz band should be further investigated. License exempt applications must obey certain (technical) criteria to minimalize interference to other users. Even when the criteria are met (according to the Nordic Telecom Agency this is almost never the case[3]), drones use a different technology than most applications on the ground to like Wi-Fi and LoRaWAN, which makes it possible to control the drone even at a large distance (more than 500 meters). It is not clear that the license exempt criteria can still be useful and stay useful for drones or what the consequences are for the other applications in the license exempt domain. For example: the great height of the antenna of a flying drone is not a criteria. The results of this project research can be an indication whether additional regulation is needed with regards to the license exempt frequency spectrum and what the contribution of Agentschap Telecom can be in international discussions.

1.2 Assignment

Agentschap Telecom has assigned Strict and FIGO to investigate the impact of the increased usage of license exempt spectrum by drones.

The main research question is:
"To what extent occurs (mutual) interference between drones and other unlicensed use and what are the consequences of the usage of these bands by drones?"

<u>In scope:</u>
The following sub questions were formulated:

- What is the risk of interference with the use of unlicensed frequencies by drones and what measures will solve this?
- To what extent will interference occur with other users of unlicensed frequencies when drones are used in close proximity and which measures will solve this?

The following aspects of drones are investigated:

- The reliability of the radio interface;
- Current and expected future use of drones, assuming provisioning for drones will be permitted in new aviation regulations;
- The different radio applications used by drones and their payload, the relevant technical data (such as frequency, transmission power, bandwidth and modulation technique, etc.),

---

[2] Projectgroep Mobiel in de lucht, *Mobiel in de Lucht*, 10 juni 2014
[3] http://www.telecompaper.com/news/growing-drone-use-could-interfere-with-radio-spectrum--1114252, consulted April 2016

the usage (e.g. what is their flight duration) and a realistic picture of the practical range of wireless communication;

- The effects of disruption on the reliability of the existing radio applications by flying drones and an indication what countermeasures can be taken by users of drones;
- An overview of frequency-related incidents or near-incidents with drones (a level of disturbance which made it impossible to fly, flights had to be cancelled, drones crashed or video connections failed);
- Other relevant studies which have been carried out and describes the relationship to this investigation.

Out of scope:
This study does not address the possible resulting effects for the drone when the radio link is lost. For example, drones with GPS will probably have a "return to home" (RTH) function which will be activated when the radio link is lost. GPS in the drones are out of scope of this report.

The research focuses on license exempt spectrum only. The 2.3 GHz band was made available in the Netherlands for professional drone users[4]. A license is needed to use this frequency, so it is considered out of scope. Part of the 5 GHz band has been specially allocated for controlling unmanned aircraft weighing over 150 kg during WRC-12 (World Radio Conference 2012). This concerns the 5030 – 5091 MHz band. A band plan by ICAO needs to be established first. Until then, only temporary licenses can be issued in this band. This is also out of scope.

1.3 Research Parties

This research assignment was performed in a joint effort by a team of specialists from Strict and FIGO.

1.3.1 Strict

Strict Consultancy provides independent ICT advice with the focus on communication technology. Strict advises, organises and implements communication applications that optimise primary processes and service delivery. Strict has extensive practical experience in the field of radio network analysis, especially related to the way it is used in business processes.

Strict and FIGO have recently performed research into the current use 2.4 GHz and 5 GHz license exempt bands[1] and also market research[5] into the future use of the licence exempt spectrum in the 433 MHz, 868 MHz, 2.4 GHz, 5 GHz and 60 GHz for the Ministry of Economic Affairs, both projects commissioned by Agentschap Telecom.

---

[4] https://www.internetconsultatie.nl/nfp_wijzigingspakket_2015_1 (consulted april 2016)
[5] De Goeij, G.A., Van Dijken, E.H., Achterberg, E.H., Hötte, W, Brouwer (2016), *Research into Market Usage of License-Exempt Equipment in the Netherlands,* Strict, Telecompaper and FIGO

1.3.2 FIGO

FIGO is a high-tech product organisation with a strong focus on open innovation. Radio communications, in particular through radio technologies using License Exempt frequencies, are the core of FIGO's solutions, and as a result are the core of the FIGO's knowledge.

FIGO is actively involved in research projects with national and international partners. FIGO's knowledge and experience bridge theory and practice with a strong view on state-of-the-art radio technology and foresight into its future. Both this knowledge of current day technology and a vision on its developments form the basis of the created applications, concurring the challenges such as communications in heavily occupied spectrum.

1.4 Report Structure

This report starts with a description of the background and the assignment in Chapter 1. The research method is briefly described in chapter 2. Chapter 3 contains the results of (desk) research divided into drone definition, regulation, market volumes. Chapter 4 describes the drone architecture, modulation technologies, overview of the used license exempt spectrum and the focus of this research. Chapter 5 contains the results of the measurements, which are used in chapter 6 which describes the mutual interference scenarios. Finally, conclusions and recommendations can be found in chapter 7 and 8.

2 RESEARCH METHOD

The project started with a kick-off participated by Agentschap Telecom, Strict and Figo. The project approach was defined in detail and the planning was determined.

The agreed project approach contains:

- Gathering information phase
  - Desk research
    - Definitions, Types of drones, Suppliers, Market volumes, Regulations
    - Applications of drones
    - International sources, experiences and regulations
    - Known incidents, especially radio frequency related
  - Interviews and visits
    - Suppliers
    - Users; professional, consumer, interest groups
    - Conferences
- Modelling phase
  - Developing interference scenario's
    - Expecting interference level
    - Define test scenarios
- Test phase
  - Execute the test scenarios
  - Report the test results
- Analyse phase
  - Analyse the gathered information and test results in relation to the project goals

The research subsequently started with desk research on the different type of drones, current and expected future use of drones and their applications (public order and safety, security, inspection work, etc.). All recreational and professional drones which are encountered, are put in a list and updated whenever new information becomes available. The key parameters for this research are noted per drone, like frequency (e.g. 2.4 GHz, 5.8 GHz or 868 MHz) and technology used for control, video and telemetry (e.g. Wi-Fi, GFSK, FHSS, DSSS). Other characteristics like flight time, weight, size and speed are also noted.

Research sources from outside the Netherlands are also used, especially on the use and technical characteristics of drones. In the US, all drones are required to be registered and the registration information is publicly available. On the site of the FCC test reports of popular types of drones are available. This information was valuable input for the project.

Other information is obtained by contacting model flying organizations, suppliers of drones and a visit to the TUSexpo (Unmanned Systems) conferences in The Hague. Interviews were performed with the Dutch Police and the Twente Fire Department. Both organizations started to use drones in their professional tasks. The frequency-related incidents are investigated by contacting ILT (inspection agency for the Infrastructure and the Environment Department) for a search through their database.

The interference scenarios are developed in the modelling phase, where distances, radio propagation models, capabilities, etc. are processed. The expected interference levels and the test scenarios are determined this phase. In the test phase the interference scenarios are tested. This was executed together with the helpful support from the Twente Fire Department on their testing facility – Twente Safety Campus[6] – on the premises of Airport Twente with support of Clear Flight solutions[7].

With the results of the tests a better prediction can be made about the occurrence of interference and its consequences. The results were analyzed and based on this, conclusions were drawn and incorporated into this report.

[6] https://www.twentesafetyandsecurity.com/drone-ontwikkel-opleiding-en-testcentrum-op-airport-twente/ (April 2016)

[7] http://clearflightsolutions.com/ (April 2016)

3 RESEARCH DRONE MARKET

3.1 Terminology: drone, UAV, UAS or RPAS?

Drone is the common name for all devices which are remotely controlled and fly without a human pilot in the aircraft. This can be an ultralight device of a few grams up to the most complex and heavy devices like the MQ-1 predator used by the US army. Other terms in use are:

- UAS – Unmanned Aerial System
- UAV – Unmanned Aerial Vehicle
- RPAS – Remotely Piloted Aircraft System, this includes aircraft and ground station

In the military the term UAV is used the most. They distinguish between mini, tactical, strategic and special task UAV's.[8] Agentschap Telecom mentions both the term drone and RPAS in the research assignment.

According to a recent definition of the International Civil Aviation Organization (ICAO[9]), RPAS can be distinguished from other UAS by not being autonomous. This means that a RPAS is always under control of a pilot on the ground.

In this document the term "drone" is used. The reasons are also mentioned in a WODC report about drones[10], because:

- The use of terms which include only certain classes of unmanned aircrafts is not advised. The term RPAS cannot be used because future autonomous systems should not be excluded. Current systems can already fly autonomous by setting waypoints, the manual control is only needed by law;
- The term drone is recognized and well known with the general public and drone manufacturers.

3.2 Regulation and classification of drones

The European Union has developed a strategy to support innovative applications of drones which is supported by the aviation industry in the Riga Declaration. It refers to a number of drones applications that are made possible and that will populate the airspace in the future as can be seen in Figure 1.

---

[8] M. de Fátima Bento. Unmanned Aerial Vehicles. An Overview. 2008. url: http://www.insidegnss.com/auto/janfeb08-wp.pdf (Retrieved april 2016).
[9] http://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf
[10] B.H.M. Custers, J.J. Oerlemans, S.J. Vergouw, "Het gebruik van drones", WODC, 2015

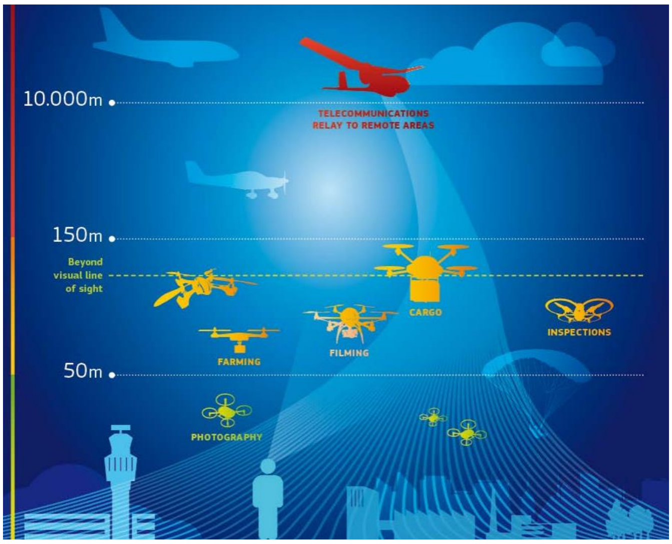


Figure 1: Future use of airspace by drones[11]

In Europe, the national authorities are responsible for drones operations with a weight of 150 kg or less. This leads to different rules from state to state. The Dutch aviation regulation makes a distinction between model aircrafts and RPAs:

- A model aircraft is an aircraft unable to carry a human being, and used exclusively for air shows, recreation or sports. Private/recreational users have to comply with the regulation for model aircrafts. A model aircraft weighs less than 25 kg. The rules for these aircrafts are described in the "regeling modelvliegen"[12]. No license is needed to fly model aircrafts as long as they comply to the law;

- A RPA is a Remotely Piloted Aircraft other than a model aircraft and unmanned. Professional users of drones have to comply to the regulation "Luchtvaart Dronevliegers - RPAS"[13, 14]. A license is needed to fly the drone. Drones with a weight of up to 150 kg do not need to take off from an airport, but have to be in VLOS (visual line of sight) of a drone operator. BVLOS (beyond visual line of sight) flights are not granted in the Netherlands.

The ILT (Inspectie Leefomgeving en Transport) is responsible for the enforcement of drone legislation in the Netherlands. For professional usage, permits are needed from ILT for:

- The pilot: RPA-L, a license to fly;
- The aircraft and ground station:

---

[11] http://ec.europa.eu/transport/modes/air/aviation-strategy/images/infographics/aviation_strategy_innovation_proposal_phase.pdf (April 2016)
[12] https://www.ilent.nl/onderwerpen/transport/luchtvaart/modelvliegers/ (March 2016)
[13] https://www.ilent.nl/onderwerpen/transport/luchtvaart/dronevliegers/ (March 2016)
[14] http://wetten.overheid.nl/BWBR0019147/2015-11-07 (March 2016)

- BVI, Proof of registration in the aircraft register;
- S-BVL, Special Certificate of Airworthiness;

- The company providing RPAS services: ROC, RPAS Operator Certificate;
- Flight school: Registration as RPAS flight school with both a Theory Exam and Practical Exam;
- The organization which carries out individual technical inspections: individual design and construction assessment.

The result of this distinction between professional use and recreational use is that for the same drone a license is needed with a lot of restrictions for professional use but when it is used recreationally the drone can be used without license and with less restrictions. For example, when a DJI Phantom 4 is used for recreational use and pictures are taken, this is legal. When money is earned by selling these pictures, it is considered a professional flight and a license is required.

To solve this a further distinction was proposed in a new proposed regulation which is known as "the mini drone regeling"[15]. In this new regulation no license is needed for all drones less than 4 kg, equal for all types of use, professional or recreational. This new regulation was supposed to become into effect in October 2015 and would be good news for professional users like photographers, journalists and farmers. But it was withdrawn for unknown reasons.

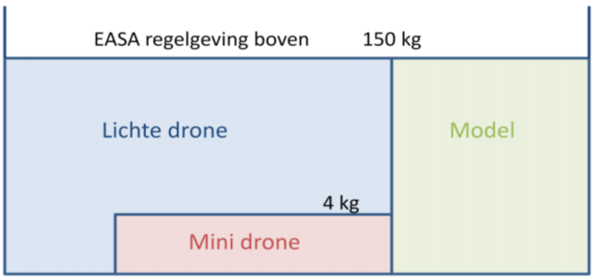


Figure 2. Proposed drone classification in mini-drone regeling of oktober 2015

In response to several drone incidents at Schiphol airport[16], the state secretary recently answered several parliamentary questions[17]. At the same time the new draft rules for mini drones were published. In this draft regulation professional drone flyers will be given dispensation for RPA L, S-BVL and BVI provided that the flight complies with stricter conditions:

- The maximum distance from the pilot is 100 meters;
- The maximum flying height is 50 meters and in civilian military low flying areas 40 meters
- Drones are not allowed in the control zone around airports and within three kilometers around an uncontrolled airport

---

[15] https://www.internetconsultatie.nl/veiligheidsregelgeving_drones/document/1645 (April 2016)
[16] http://www.nrc.nl/nieuws/2016/04/02/baan-schiphol-tijdelijk-dicht-na-melding-van-drone (April 2016)
[17] https://www.rijksoverheid.nl/documenten/kamerstukken/2016/04/22/beantwoording-vragen-schriftelijke-overleg-drones (April 2016)

Pilot of drones from 1 to 4 kilograms must be able to demonstrate that they have sufficient theoretical knowledge to participate safely in the air traffic with the drone. This requirement does not apply for drones up to 1 kg (micro drone). Pilots are still obliged to have an ROC, but this is eased considerably. Flights do not need to be reported to the mayor and a NOTAM (notice to airmen) does not need to be published 48hrs beforehand.

As can be seen in the regulations mentioned above the classification used depends on usage (professional or recreational) and weight. In this research drones are distinguished based on the current and proposed regulation for drones, mini drones and large drones:

- **Micro drones** are simple and light drones, less than 1 kg, for recreational use and do not have GPS. The risks that these drones cause harm are very low. Examples of micro drones are Dromida Ominus and Syma X5C which weigh around 100g and should be considered toys.
- **Mini drones** are drones weighing more than 1 kg and less than 4 kg for recreational or professional use and in most cases with GPS. This is a popular and rapidly increasing group of drones. Examples of popular mini drones are the DJI Phantom, Yuneec Typhoon H and Walkera. The upper limit of 4 kg was taken from the earlier mentioned “mini drone regeling”.
- **Large Drones** are more than 4 kg and less than 25 kg and are mostly used by professionals. Examples are the Aerialtronics Altura and the recently introduced DJI Matrice M600[18]. The limit of 25 kg is used because of the upper limit in the “regeling modelvliegen”.

Based on estimations from interviews with market parties, the total number of drones in the Netherlands is about 150.000 of which the majority are micro- and mini drones. The number of large drones is probably not more than one thousand, but because drones do not need to be registered unlike in the US, exact figures are not available. The majority is used for recreational usage, while a minority of about 3000 is used professionally.

Figure 3 depicts the classification and numbers of drones and their usage by the professional and recreational market.

[18] http://tweakers.net/nieuws/110421/dji-presenteert-matrice-600-drone-die-tot-zes-kilogram-kan-dragen.html (April 2016)

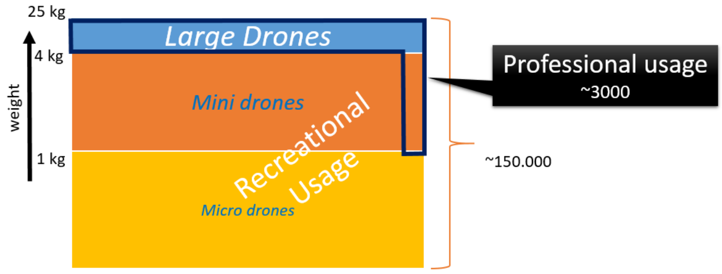


Figure 3. Classification of drones used in this report, estimated numbers in the Netherlands and their usage by the professional and recreational market (april 2016)

3.3 Types of drones

Most people associate drones with the quadcopter systems, which are the most commonly known types of drones for the recreational market. Figure 4 shows the DJI phantom 4 which is popular in both the professional and the recreational market. The **multirotor** is the most commonly used type of drone. This type of system is characterized by using multiple rotors which lift the aircraft. This can be 4 rotors (quadcopter), 6 rotors (hexacopter) or 8 rotors (octocopter). An advantage of this type of drone is that it does not need an airstrip or launch installation to take off, unlike a fixed wing drone.

Figure 4. Example of a multirotor drone, the DJI phantom 4.
This is one of the most popular types of drones for professional and for recreational use.

Fixed wing drones have fixed wings, like most regular aircrafts, for example the SenseFly eBee which is a professional mapping drone. The shape of the wings in combination with speed generates the lift for the aircraft. This type of drone needs a launch system or can be launched by hand. Most model airplanes are fixed wing systems. Recently Google plans to deliver high-speed internet (5G) with solar-powered fixed wing drones from the air[19]. These are currently tested in Spaceport America in New Mexico. Another type of fixed wing drone is a glider.

---

[19] http://www.nu.nl/gadgets/4206524/google-maakt-drone-zonne-energie-5g-internet-verspreiden.html (March 2016)

Figure 5. Example of a fixed wing drone, the SenseFly eBee, mostly used for mapping

The hybrid drone is a combination of a fixed wing drone and a multirotor drone. This drone can take off vertically, once it is in the air the system will use wings to stay in the air. This is also called a VTOL (vertical take-off and landing). An example of a hybrid system is the Prime Air tested by Amazon in the USA[20].

Figure 6. Example of a hybrid VTOL drone, the Amazon Prime Air

The helicopter drone is a helicopter controlled via the ground. One or two rotors generate the lift for the aircraft. This type of drone is are used for private use, like the Syma 107G. But also for professional use, like the Dutch High Eye HEF30[21].

---

[20] https://www.youtube.com/watch?v=MXo_d6tNWuY
[21] http://higheye.nl/hef-30/

Figure 7. Example of a helicopter drone, the high eye HEF30.

A special type of drone is the ornithopter. This uses bird-like flapping wings to generate lift. An example of this type of drone is the Delfly explorer[22].

Figure 8. Example of an Ornithopter

Balloons are not considered to be a drone in this research project, as well as a rockets.

The development of new types of drones is going into new territories. Some companies are busy with drones which can even transport humans. Examples are the Dutch "one man drone" project which won the 2016 ESEF award[23] and the Ehang 184 which was shown at the CES 2016 in Las Vegas[24]. Figure 9 shows the Ehang 184. One can argue if this is really a drone because it is not unmanned although the passenger cannot control it. The question is if the passenger can be considered a "payload" in order to fly without a pilot's license. If so, BVLOS flights are not allowed

[22] http://www.delfly.nl/explorer.html
[23] http://onemandrone.com/we-were-awarded-for-our-inovation/ consulted in april 2016
[24] http://www.ft.com/cms/s/0/a6dede66-b499-11e5-8358-9a82b43f6b2f.html#axzz45WRHCHtQ consulted in april 2016

in the Netherlands now. Lots of questions have to be answered before this type of drones will be allowed in Europe.

Figure 9. The Ehang 184 can transport passengers

This research focuses on drones using license-free bands. License-free bands have a limited power and should not be used over long distances. License free is suited for most drones with limited range. This applies in particular to multicopters. Also battery powered fixed wing drones can use license-free bands as long as they stay within visual contact. VTOL drones have a long range and fly BVLOS. Because BVLOS is not permitted in the Netherlands this is not a problem.

3.4 Drone sizes, weights and other technical data

Drones come in all types of sizes and weights. For example the Cheerson CX-10 mini quadcopter measures only 40x40 mm. Drones which can carry humans like the previously mentioned Ehang 184 weighs 200 kg and can carry up to 100 kg, but is not legal[25]. An average drone like the best-selling DJI Phantom measures 590 mm (diagonal) and weighs 1280 grams. The popular Dutch professional drone Aerialtronics Altura Zenith weights about 6650 grams with a payload of up to 2900 grams. Based on different sources which includes sites like Specout[26], the averages and differences in size, weight and technical data are summarized below in Table 1: Key parameters from drones.

[25] http://www.uavexpertnews.com/ehang-184-personal-mini-copter/
[26] http://drones.specout.com/

		Min	Average	Max
weight	grams	7	2.030	20.000
max payload	grams	-	2.468	99.000
size	mm (diagonal)	30	475	3.401
max speed	m/s	5	16	33
battery	mAh	80	3.424	52.000
flight time	minutes	3	15	120
max altitude	meters	4	1.708	6.100

Table 1: Key parameters from drones

3.5 Expected market volume of drone

Estimations for the global growth of the drone market show a huge variation. According to BusinessInsider, the market for professional and recreational drones will grow at a compound annual growth rate (CAGR) of 19% between 2015 and 2020[27], from about 1 billion in 2015 to about 2 billion in 2020. According to market research reports (MRR), the smart professional drones market, valued at $3.4 billion in 2014, is expected to jump to $27.1 billion by 2021, an increase of nearly 800%. Market research firm Tractica predicts that worldwide shipments of professional drones will increase from 80,000 units in 2015 to nearly 2.7 million units in 2025. Tractica sees drone hardware sales rising from $283 million in 2015 to nearly $4 billion in 2025.

It is very hard to get clear figures for the number of drones in the Netherlands. Drones do not need to be registered and manufacturers and distributors are not willing to disclose sensitive data on their sales of drones to their competitors or the figures are not available. Even if all the figures of Dutch distributors were available it would only give a partial impression, due to the parallel import via Chinese web shops and other European countries.

According to DARPAS, the number of drones in the Netherlands is estimated at 100,000 (according to an interview with Rob van Nieuwland, chairman of DARPAS, published in Slash, Technical University Eindhoven, December 2015). Of these drones 97% are used for recreational purposes and are comparable to a DJI Phantom. The number of drones used for professional purposes is estimated at approximately 3,000.

After a round of calling several distributors in the Netherlands, the general impression is that at the moment of writing (March 2016) there are about 150.000 drones in the Netherlands. Sales are around 20-30.000 drones per year rising with 20-30% per year.

[27] BusinessInssider US Drone Report, May 25, 2015

According to an estimate by Goldman Sachs in 2014 the global drone market is doubling each year, from around $600 mln in 2014 to around $4800 mln in 2017. This would mean that in the Netherlands, there will be almost 200.000 drones by the end of 2016.

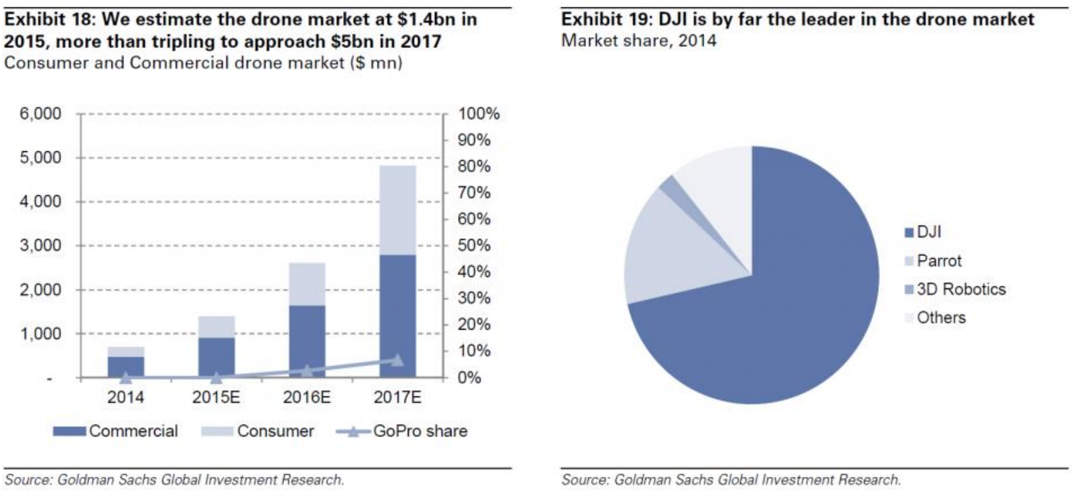


Figure 10. Drone Market and market share of drone manufacturers estimated by Goldman Sachs in 2014. The market is doubling each year and DJI is by far the leader in the drone market.

3.5.1 Market share of drone manufacturers

As can be seen in Figure 10, DJI was estimated to be the biggest drone manufacturer in 2014. Until 2016 it was very difficult to verify this figure, because DJI does not disclose any sales figures. Thanks to new FAA legislation in the US, drones heavier than 250 gram have to be registered and these are published regularly. This gives a more accurate estimate of the market share of drone manufacturers. As can be seen in Figure 11, more than 45% of registered drones owned in the USA are manufactured by DJI. DJI is the most popular drone manufacturer with the Phantom series as their flagship.

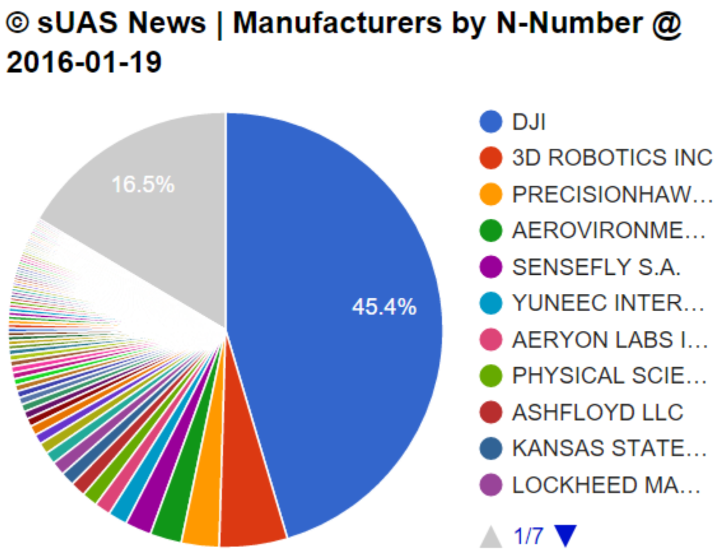


Figure 11. Market share of manufacturers in the US, based on FAA registered drones database (status 19 January 19, 2016)[28]

Information from Dutch drone suppliers confirm that DJI is market leader, contributing to about 50% of all drone sales. The market figures of 2014 with a high market share of 3Drobotics and Parrot could not be confirmed. One of the suppliers with a large growth is Yuneec, another Chinese company. It is estimated that they currently contribute to around 30% of all sales. Other popular semi-professional drones are from suppliers like Xiro, Walkera and Blade Chroma. Figure 12 shows the estimated share of current drone sales.

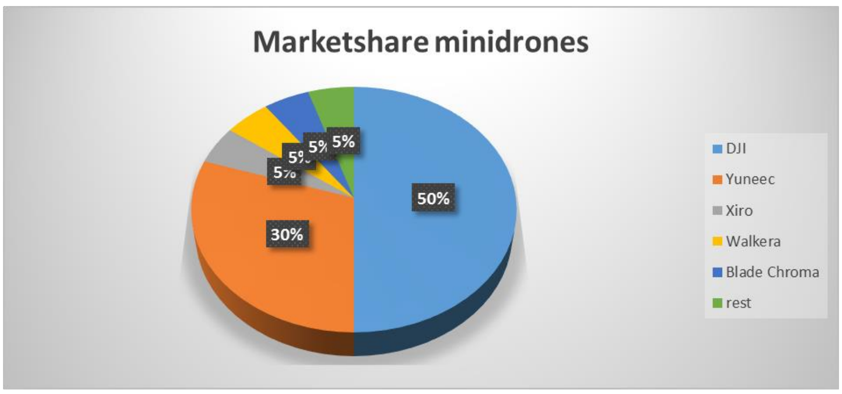


Figure 12. Estimated market share of (semi) professional drones in the Netherlands in number of drones sold per year.

[28] http://www.suasnews.com/2015/12/faa-registered-drones-a-yuletide-update/

For the micro drone market (category less than 1 kg, simple and light drones without GPS or even a camera) an estimation was also given, but this is changing even more rapidly.

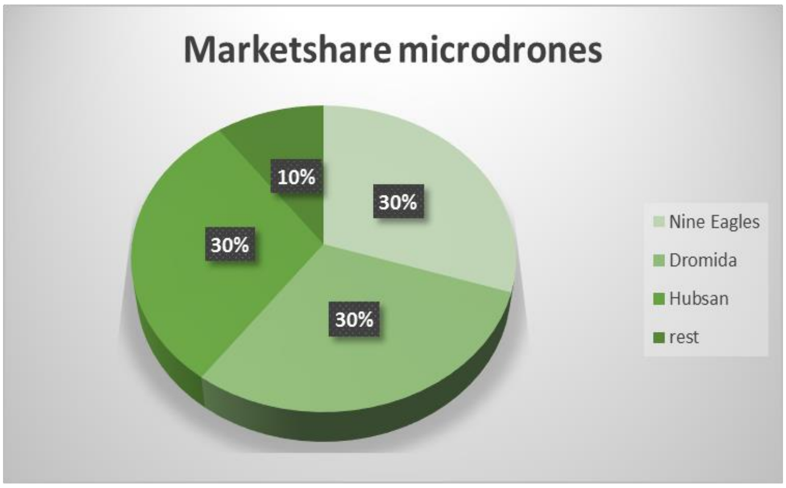


Figure 13. Market share of micro drones. These are small drones without GPS and sometimes even without camera

3.5.2 Market for large drones

Most Dutch companies offering professional services like inspection, mapping or video use drones from DJI or Aerialtronics. DJI is also market leader in the professional market with popular models like the DJI Inspire and the Spreading Wings Series. Dutch company Aerialtronics also has a substantial market share, with the Altura Zenith used by many professional companies or institutions. The Twente Fire department is a user of the Aerialtronics Altura.

3.6 Application of drones

Drones are used for recreational, professional and military purposes. For this research the military use is excluded. An exhaustive description of the possibilities are described in the WODC report[10]. The most common professional and recreational use of drones is described below.

3.6.1 Professional use

Key industries that will drive the adoption of professional drones include film, media, agriculture and oil and gas. Professional drones are also used in the public sectors like law enforcement search, surveillance and rescue, high altitude imaging, emergency response, forest fire monitoring, humanitarian aid, flood mapping. In addition, drones are also being used for environmental monitoring and mapping, hyper spectral imaging, soil moisture imaging, plume dispersion and tracking, in-situ atmospheric monitoring and aerosol source determination among others.

3.6.2 *Recreational use*

The largest number of drones are in use for recreational purposes. Making photographs and videos is the number one application. Drones like the Lily[29] have follow me functionality which makes “selfie action movies” possible. With continuously new developing technology like detect and avoid[30], this will also be possible in the future in forests or other environments.

Drone racing is the sport of the future where drones race against each other with speeds of up to 100 km/h. These drones are controlled by pilots on the ground with FPV (First Person View) helmets which show the live video feed of the drone.

3.7 Incidents with drones

In their position paper on drones[31] the Dutch Airline Pilots Association VNV is concerned about “a degradation of the existing high level of safety for the existing professional airspace users. This is due to the limitations and properties of drones and their pilots and especially the widespread lack of knowledge about the manned low level operations.”

This is supported by the increasingly mentioned close encounters between commercial flights and drones in the news[32, 33]. VNV (Vereniging Nederlandse Verkeersvliegers) is even more concerned about the effect of drones on helicopters, like ambulance, firefighting and police[34]. Several bird strikes have demonstrated that even impact with small birds (below 200 g) can have catastrophic consequences for a helicopter. Drones, even light ones below 1 kg, will cause significant or even catastrophic damage to helicopters in case of a collision due to the number of vulnerable, critical components, such as the tail rotor or main rotor head. The more advanced drones have software to make flying near airports impossible, this is called "geo-fencing". With geo fencing a drone cannot be used in the control zone (CTR) around airports.

Ambulance helicopters are not designed to withstand any bird strikes. Due to the type of the operations (ambulance) helicopters often fly low, away from aerodromes and outside controlled airspace. Despite the limitation to the height a drone can legally be in the same airspace.

The number of incidents caused by *interference* in unlicensed bands is difficult to estimate.

---

29 https://www.youtube.com/watch?v=4vGcH0Bk3hg, consulted April 2016
30 http://geekly.nl/11388/skydio-een-drone-die-obstakels-kan-ontwijken/, consulted April 2016
31 VNV: *Airborne threats of low level Remotely Piloted Aircraft System (RPAS),* June 2015
32 http://www.nu.nl/gadgets/4233225/weer-drone-vlak-langs-passagierstoestel.html (March 2016)
33 http://nos.nl/artikel/2096703-drone-rakelings-langs-landende-vliegtuigen-op-schiphol.html (April 2016)
34 Vereniging Nederlandse Verkeersvliegers, “Airborne threats oflow level Remotely Piloted Aircraft System (RPAS)”, June 2015

In the ILT report on drones[35] the conclusion is that the number of incidents with drones doubles each year. We contacted ILT to receive information on what incidents are frequency-related. It was concluded that there were incidents with uncontrollable drones, but it is not possible to determine if these incidents are related to radio interference. A note was made that not all incidents are reported, because recreational users are not required to report incidents. Recreational users typically do not know the ILT or know how to report an incident.

During our visit of the TUSexpo[36] in The Hague we asked (professional) drone users on their experience with frequency related incidents or problems. All requested participants assured us that, to their knowledge, license exempt spectrum has not created any problems. One of the participants of the TUSexpo was the NLR. NLR offers test facilities for drone manufacturer and is qualified to train drone pilots. Their observation was that most drone users are not required and do not scan the interference levels before take-off. That means that the opinion of drone users is not based on facts.

Despite that the users are not recognizing interference problems, there are a lot of unexplained incidents which were never investigated. One type of incidents reported with drones concern “fly-aways”, where the drone flies away uncontrolled. A survey showed almost half (!) of all DJI Phantom owners have experienced a fly-away, see Figure 14. A Facebook page was even created to help the DJI Phantom owners with the psychological impact of a fly-away.

It is not clear what causes the fly-aways. In some forums the Wi-Fi connection of the GoPro is blamed, but also loss of GPS signal is mentioned many times. Fly-away due to interference with other license spectrum was not reported, but is also probably never properly investigated.

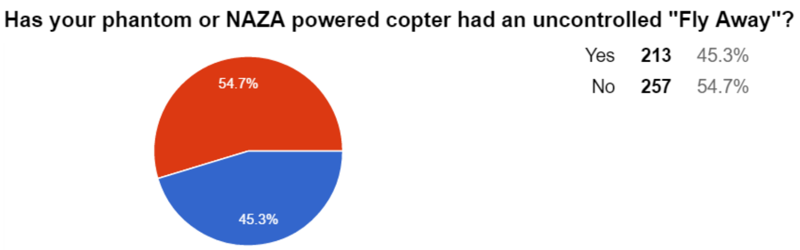


Figure 14. Almost half of DJI Phantom owners experienced a fly away[37]

Interference between drones can also occur, although not likely. The DJI manual recommends not to use more than three Phantom 3's at the same time. The use of more than three Phantom 3’s may lead to mutual blocking of the FPV application, so a limitation on the amount of traffic in the

[35] Informatieblad ABL, Incidentmeldingen drones, Inspectie Leefomgeving en Transport (Jun 2015)
[36] http://tusexpo.com/
[37] https://nl.ifixit.com/Wiki/Drone_DJI_Phantom_FlyAway (April 2016)

downlink. The limitation of three simultaneous users does not seem to relate to any risk of interference in the remote control.

Adding this all up the total number of uncontrolled flights which probably should be registered as incident alt ILT is much higher than the reported number of 27 in 2014. According to the magazine of the NTCV[38] more than 70% of drone flights have an uncontrolled ending. In almost all cases it is impossible to discover if the reason is radio interference, but it can also not be excluded.

[38] Magazine "Nationale veiligheid en crisisbeheersing" 13e jaargang 2015 nr. 5, page 7

4 DRONE ARCHITECTURE

4.1 Basic architecture

The technology behind a visual line of sight controlled drone can be explained with the technical and functional architecture and design. The basic architecture of a drone is shown in Figure 15.

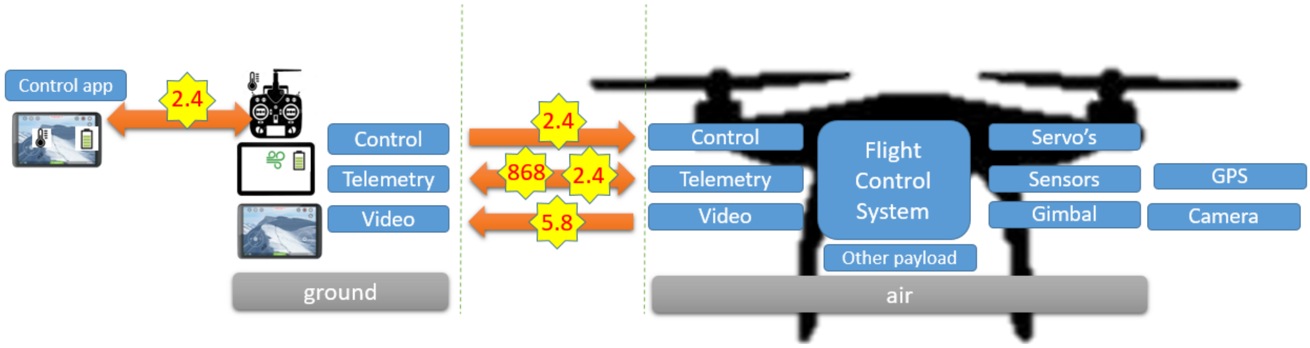


Figure 15. Basic components which (can be) part of a drone.

The focus of this research is on the ground to air communication in license exempt bands, most commonly used, are shown in the picture.

A drone can be controlled directly with a RC controller. The receiver in the drone controls the servo's in the drone directly and/or connects to a flight control system which controls the drone. When the drone can fly a preprogrammed path via waypoints, these are programmed in the flight control system via the telemetry receiver. The GPS provides information to the flight control system on the actual position of the drone. Sensors and system collect data like wind speed, temperature, battery status, etc. This information is sent via the telemetry link to the ground. The payload information, which is in most cases video, is sent to the ground. In case of video, the camera can be independently controlled and kept stable via a gimbal. Some drones are provided with an additional control app for tablets or phones. These tablets or phones connect via Wi-Fi or Bluetooth to the controller or ground station. An example is the DJI Go app.

The functions described in Figure 15 are not necessarily separate recognizable modules in a drone. Hobbyists which build their own drone can buy these components separately and integrate them into a drone. Mass produced drones often integrate components both in the drone and on the ground. For example, Lightbridge from DJI provides a ground station which combines control, video and telemetry[39]. The A2 flight controller from DJI which can be used for the spreading wings series has an inbuilt receiver.

This investigation focuses on the wireless connections used for control, telemetry and video because these are using the license exempt bands. The bands are described in more detail below. GPS is not investigated because this was not in scope of this research.

4.2 Control

Manual drone control is mandatory by Dutch law for all professional and recreational drones. The controller on the ground controls the drone via the receiver. Model aircraft builders use generic controllers.

Popular generic controllers are Futaba, Spektrum, JR, and Hitec. New on the market is Jeti with dual transmitters. Popular mini drones like the DJI Phantom use customized controls compatible with Futuba.

The controller sends information to the receiver in the drone. The receiver has several outputs (or channels) which can be connected to servos in the drone (for example throttle, aileron, elevator, rudder for a fixed wing drone), and or can be connected to the flight controller. The receiver can also be integrated in the flight controller.

When a generic remote control is used, a matching receiver must be used. A Futaba radio does not work with a Spektrum receiver. Customized controllers seem to re-use existing control systems, but it is not always clear which type. For example, the DJI A2 flight controller has a receiver built in that will pair with several Futaba transmitters/controllers[40].

A scan was performed on most used drones, controllers and modulation schemes. Extensive desk research was done to accomplish this in combination with expert knowledge on drones and model airplanes which was available in our team. An excerpt of this research for controllers is shown in Table 2.

The majority of controllers use the 2.4 GHz spectrum with a proprietary FHSS modulation. FHSS is used to maximize robustness and controlling distance.

By exception Wi-Fi with OFDM modulation can be used in either the 2.4 GHz or the 5.8 GHz band and is used to control a drone. This is for example the case for the Parrot AR2 on the 2.4 GHz band. The advantage is that the drone can be controlled via a smartphone or tablet, making a separate controller unnecessary. A big disadvantage is the limited range and sensitivity for other Wi-Fi bands.

[39] http://www.dji.com/product/lightbridge-2/info
[40] http://www.phantompilots.com/threads/spreading-wings-s1000.21319/

Another exception is Yuneec which seems to use Zigbee[41] for control (DSSS modulation).

In some rare cases drones use the 5.8 GHz band. An example is the DJI controller for the Phantom 2 Vision plus, which uses the 5.8 GHz for control[42] and the Xiro controller[43].
Another rare case is the use of the 433 MHz band. It is used by the Immersion EzUHF module. This module uses 2 MHz of spectrum with a 500mW transmitter, which means it can only be operated by someone with a ham radio license[44].

Chipsets in controllers are originating from a few suppliers:[45]

- Micro Linear ML2724 used by Futaba FASST;
- Cypress CRYF6936 used by JR/Spektrum's DSM, DSM2 and DSMX;
- Texas Instruments CC2500 used by HiTec, Co-rona, FrSky, Tactic, Futaba S-FHSS;
- Texas Instruments CC2520 used for JR's DMSS.

Brand	Frequency	Modulation	Technology
DJI Phantom	2.4 GHz /5.8 GHz	FHSS/DSSS	FASST/Lightbridge
Futaba	2.4 GHz	FHSS/DSSS	FASST
Spektrum	2.4 GHz	FHSS/DSSS	DSMX
JR	2.4 GHz	FHSS/DSSS	DMSS
Hitec	2.4 GHz	FHSS/DSSS	AFHSS
Graupner	2.4 GHz	FHSS/DSSS	HOTT
Yuneec	2.4 GHz	DSSS	ZigBee
Parrot AR2	2.4 GHz	OFDM	Wi-Fi
Immersion*	433 MHz	FHSS	EzUHF

* Does not comply to European regulation

Table 2. Popular controls used by drones, frequencies they operate on and the used modulation technique and technology

4.3 Telemetry

Information on the health, position and speed of the drone is send via a telemetry link. Information which is often send is:

---

41 https://fccid.io/2ACS5-ST16 (march 2016)
42 https://store.dji.com/product/phantom-3-remote-controller-5-8g-sta
43 http://xiro.auroragroup.eu/ see menu option " comparison" (march 2016)
44 http://www.immersionrc.com/fpv-products/ezuhf-500mw-transmitter/ (march 2016)
45 http://www.rchelicopterfun.com/RC-Spread-Spectrum.html (april 2016)

- Air unit power capacity
- Transmission status
- GPS satellite count
- Air craft nose orientation
- Aircraft altitude
- Aircraft flight distance
- Vertical speed of the aircraft
- Horizontal speed of the aircraft

The current method to show this information on the on-screen display (OSD) in the controller is to send overlaid telemetry information over the video link, or to use a separate radio channel. In most cases the 868 MHz is used, in some cases the 433 MHz or the 2.4 GHz band.

As separate radio channel the ZigBee protocol is often used in the 868 MHz band. This ZigBee link can also be used for setting waypoints and control the drone. Research has shown that it is possible to hack a professional drone via a ZigBee link[46].

Another communication channel which can be used for telemetry is 4G. This has been demonstrated by Uavia[47] in France. Uavia envisions a world with an "internet of drones" which can be deployed anywhere in the world and controlled from any place in the world. However, in the Netherlands control beyond visual line of sight (BVLOS) is not allowed for drone operators.

4.4 Video

Drone can transport different types of payload depending on the purpose of a drone or flight. This is extensively described in a comprehensive WODC study[48]. In short these can be:

- Camera and microphone
- Sensors (chemical, biological, meteorological)
- Other, like packets or other objects to be delivered, agricultural objects, etc.

Most commonly used as payload is a camera for both the amateur and the professional market. Images are send directly to the ground via a video link. This is often done via the 5.8 GHz band, but also the 2.4 GHz is used. As can be seen in the overview of different video links in Table 3, OFDM is a popular modulation technique for video. The reason is that OFDM enables high bitrates which are needed for video streams.

Another modulation technique is FM, this is mostly used for FPV (first person view) applications, for example for drone racers with the Fat Shark headsets[49]. Brands which are selling this equipment are Fat Shark, Immersion and Boscam. The radiated power is very high, up to 2.5

---

[46] Nils Rodday, "Exploring security vulnerabilities of Unmanned Aerial Vehicles", Master Thesis, July 2015
[47] http://uavia.eu/en/ (March 2016)
[48] B.H.M. Custers, J.J. Oerlemans, S.J. Vergouw, "Het gebruik van drones", WODC, 2015
[49] http://www.fatshark.com/product-category/headsets/ (March 2016)

Watts[50]. In the product sheets there are warnings that local regulations must be checked before using the equipment and that a radio amateur license might be needed (!).

Brand	Frequency	Modulation	Technology
DJI	2.4 GHz	OFDM	Lightbridge/Wi-Fi
Immersion	2.4 GHz	FM	
Yuneec	5.8 GHz	OFDM	Wi-Fi
Connex	5.8 GHz	OFDM	
Immersion	5.8 GHz	FM	
Boscam	5.8 GHz	FM	

Table 3. Popular video systems used by drones. Most used types of modulation are OFDM and FM

Another communication channel which can be used for video is 4G, which has also been demonstrated by Uavia[51] in France. Skydrone is a company which delivers video over LTE[52]. The advantage of using 4G is the low latency, high reliability and low investment for the video connection.

4.5 Frequencies and modulation techniques used by drones

For remote control it has been possible to use the license exempt 27 MHz and 35 MHz bands for many years. The radio control equipment using these bands was very popular in the 80's and 90's. The 27 MHz systems were often used for toys, the 35 MHz systems for more serious remote control. Since several years the 2.4 GHz band has been the favorite frequency for remote control, also due to the move to digital technologies and cheaper solutions. There are several differences between the older 35 MHz and newer 2.4 GHz systems.

The 2.4 GHz systems often use Spread-Spectrum technologies, which are much less prone to interference. Transmitter and receiver are bonded, which eliminates the possibility that another transmitter connects to the receiver. In the 35 MHz band transmitters on the same channel can take control or cause interference to each other.

The following advantages are valid for 2.4 GHz systems:

- Worldwide allocated as license exempt
- Low cost for end user equipment
- Higher bitrates with less delay and more precise control
- Less prone to external interference than 35 MHz channels
- Lower energy consumption for the transmitter

---

50 http://www.iftrontech.com/product_info.php?products_id=210 (March 2016)
51 http://uavia.eu/en/ (March 2016)
52 http://www.skydrone.aero/fpv (March 2016)

- More users can work in parallel
- Antennas are much shorter for transmitter and receiving, making it easier to integrate
- Failsafe setting is possible when the signal is lost, this is not common on 35 MHz systems

As a result, the 35 MHz systems are not popular anymore. New transmitters are hardly available, only replacement receivers were found.

Especially for new drone systems, the 2.4 GHz band is the default choice. Other license exempt spectrum bands used by drones are the 433 MHz, 868 MHz and the 5.8 GHz. The 2.4 GHz band is most used for control, while the 5.8 is most used for video. The 433MHz and 868 MHz bands are mostly used for telemetry, besides the 2.4 GHz. Table 4 shows an overview of the different frequencies and modulation techniques used by drones.

	433 MHz	868 MHz	2.4 GHz	5 GHz
Control:	✗	✗	DSSS+FHSS DSSS OFDM	OFDM
Video:	✗	✗	OFDM	OFDM, FM
Telemetry:	Divers	DSSS	OFDM, DSSS	OFDM

4.5.1 Modulation techniques

Chapter 3.7 shows the different modulation techniques used for control, telemetry and video. This chapter will make clear what the advantages and disadvantages are and what the reasons are for choosing a modulation technology.

Most commonly used digital modulations technologies are:

- FHSS
- DSSS
- FHSS+DSSS
- OFDM

FHSS means Frequency Hopping Spread Spectrum. This technology divides a frequency band in several bands, for example 74 bands of 1.6 MHz width in the case of a Futaba controller. Both the transmitter and the receiver agree on a hopping sequence code and hop through the frequency band in the same sequence. This technique makes the connection very robust against interference, multipath reflections and other radio sources like Bluetooth. This technology is also very suitable for having several simultaneously active radios in the same area[53].

[53] S.M. Schwartz. “Frequency Hopping Spread Spectrum (FHSS) vs. Direct Sequence Spread Spectrum (DSSS) in the Broadband Wireless Access and WLAN Arenas.” In: white paper (2001).

There are two ways to determine the channel hop pattern:

1. During Binding the transmitter will share the channels to use and what the hopping sequence is. Some protocols send the channel numbers to use, others use a code that is used in a mathematical operation to determine the channels and hop pattern.
2. The channels used are always the same, but the hopping pattern changes. Once the receiver receives its first packet, the data from that packet determines the channel hop pattern for subsequent hops. This will stay the same until the transmitter is power-cycled.

A receiver does not know what channel the transmitter is transmitting on when powered up. To get the receiver and transmitter in sync it is listening onto any known channel that it hops on (with the channel list from either above method), and waits till it gets a data packet in. Once it has this data packet in, it knows what channel next the transmitter will hop to.

In Europe, transmitters have to comply ETSI 300 328-v1.8.1 starting from January 2015, which adds several sharing mechanisms like Listen Before Talk (LBT) or duty cycle. When LBT is implemented a transmitter hopping to the next channel will first listen if anything else is transmitting. If that is the case, it doesn't transmit and waits till the next time slot that it can hop to the next channel. Likewise, the receiver will be listening on that channel, no data is received and so it will then timeout and hop channel on the next time slot.

Protocols such as Bluetooth are also using frequency hopping as above, but if a channel is frequently congested, it will mark that down as not to use and then share that between both transmitter and receiver. This relies on the fact that Bluetooth has two way communication. Most remote controls for drones use one way communication.

DSSS means Direct Sequence Spread Spectrum. This technology uses a spreading code to spread the original (lower) bit rate into a higher bitrate which is then modulated onto a fixed carrier. The resulting signal can be received with very low SNR, sometimes even below the noise level. An example of DSSS is WCDMA used by UMTS (3G) and ZigBee for home automation purposes like Philips Hue.

FHSS+DSSS is a combination of the two technologies above and offers best of both worlds. This is used by most drone controllers, like Futaba, Spektrum and Jeti.

OFDM stands for Orthogonal Frequency Division Multiplexing, this divides a frequency band in a large number of closely spaced orthogonal subcarriers that are transmitted in parallel. This makes very high data rates possible. This technology is used by Wi-Fi (802.11g, n, ac) and LTE. Because of the high throughput this technology is very suitable for high bandwidth applications like video.

Another technology used is space time block code technology (**STBC**). With this technology the data is packaged with different codes, sent over different antennas and combined at the receiver antenna. This technology delivers more robustness and a somewhat better coverage.

4.5.2 Frequencies

As mentioned in Table 4 in this chapter, the license exempt spectrum used by drones is:

- 433 MHz
- 868 MHz
- 2.4 GHz
- 5 GHz

Not mentioned in this list is the 2.3 GHz which was made available in the Netherlands for professional drone users[54]. A license is needed to use this frequency, so it is considered out of scope.

Below is a more detailed description of the frequencies and applications which use these frequency bands.

4.5.2.1 433.05-434.79 MHz

The 433 MHz is an ISM frequency band, mostly used for SRDs such as key fobs for cars and garage door openers, but also for industrial use, applications outlined under the '*Regeling gebruik van frequentieruimte zonder vergunning en zonder meldingsplicht 2015'* [55] and weather stations. However, more and more home automation devices are adopting this band, including products such as sensors, smart lighting and switches[56]. Typical range for these devices is 3-50 m with a power of 10mW and duty cycles of 0,1-10%.

Drones can use this band for sending telemetry information to the receiver. This is for example the case for the Aerobotica Kratos[57]. Immersion also has a controller which works in this frequency band.

4.5.2.2 863.0-870.0 MHz

The 868 MHz Licence Exempt frequency band is used for a variety of applications and devices, such as (active) tags in RFID, (social) alarms and professional microphones. More home automation devices are also using this band, including sensors, smart lightning and switches. Another trend is the development and production of cheap Low-Power Wide-Area Network (LPWAN) devices. These allow long-range communications at a low bit rate among connected objects such as battery-operated sensors. KPN is busy rolling out a national network using

[54] https://www.internetconsultatie.nl/nfp_wijzigingspakket_2015_1 (consulted April 2016)
[55] Regeling gebruik van frequentieruimte zonder vergunning en zonder meldingsplicht 2015 bijlage 11 subcategorie 1 (March 2016)
[56] Website Homewizard, "compatible products" (consulted on 16/2/16)
[57] http://www.aerobotica.nl/, information received at the TUSexpo 2016

LoRaWAN in 2016[58]. Companies like Sigfox are already using this frequency for LPWAN. There are also other initiatives that have built IoT networks in this band. The 868 band can be used for sending telemetry data from the drone to the receiver. For example Aerialtronics uses ZigBee via 868 MHz to communicate telemetry.

4.5.2.3 2,400-2,483.5 MHz

The 2.4 GHz frequency spectrum is an ISM band and is well known for its use by wideband data through Wi-Fi and Bluetooth, but it is also used by home automation devices with protocols such as ZigBee and Z-Wave. It is further used by wireless analogue video and audio devices. The 2.4 GHz band is also used by almost all manufacturers for controlling the drone.

4.5.2.4 5,150-5,350; 5,470-5,725 MHz & 5,745-5,875 MHz

The 5 GHz frequency band is divided into three parts:

- 5,150-5,350 MHz – can only be used indoors
- 5,470-5,725 MHz – can be used outdoors with higher radiated power limits but with additional requirements like DFS
- 5,745-5,875 MHz – can only be used with lower power.

This band is mostly used for wideband data like Wi-Fi, and operators are also planning to use LTE technology in this band, through technologies such as LTE-LAA[59]. Another example of (outdoor) use is weather radar. For example, in the past a system in Smilde using this frequency caused problems with a weather radar across the border in Germany.

4.6 Focus of this research

When considering the used radio technologies, and their possible mutual interference with co-users of the spectrum, measurements should focus on those cases where a pre-dominant risk can be identified, and where model based analysis cannot fill in all relevant details. The license exempt frequencies drone pre-dominantly use 2.4 GHz and 5 GHz. No equipment with *legal* use of the 433 MHz was found during the study, and only scarce use of the 868 MHz could be found.

When considering the popular bands 2.4 and 5 GHz, some clear difference can be found. The 2.4 GHz band is much smaller than the 5 GHz band and building penetration of 5 GHz is much worse than 2.4 GHz. Both make that the 2.4 GHz band is much more crowded than the 5 GHz band. Additionally, the drone systems typically use the higher frequencies at 5.8 GHz, whereas most Wi-Fi systems operate at the lower 5 GHz frequencies. This all makes the risk of mutual interference in the 5 GHz band much lower than in the 2.4 GHz band.

A second aspect is the mix of technology. The 5 GHz band in most cases is used for wideband data transmission, mostly video, using OFDM based technology. An exception is video used for drone races, where FM technology is used, but these are not used professionally. The mutual

[58] http://corporate.kpn.com/pers/persberichten/lora-netwerk-van-kpn-live-in-de-randstad.htm (April 2016)
[59] "Wi-Fi alliance moves to defuse LTE-U tensions" (4/11/2015), Telecoms.com (consulted on 15/2/16)

interference between OFDM systems can be estimated relative simple. Mutual impact between systems using the same or similar technology can be estimated from basic radio parameters like power and sensitivity and a proper understanding of the protocol.

As mentioned the 868 MHz band is rarely used for telemetry. If used for telemetry, the used technology is Zigbee with a low duty cycle. Almost all applications in this band like Lora, RFID etc have low duty cycles, so the effect will be low.

The 2.4 GHz band however contains a mix of technologies. On the one hand, this band is used for remote control using the DSSS/FHSS technology, whereas other users typically are Wi-Fi systems using OFDM. The mutual interference between the low bitrate DSSS/FHSS and the high bitrate Wi-Fi systems are difficult to estimate directly.

For the drones a clear distinction can be made between remote control and payload. The remote control systems massively use DSSS/FHSS or likewise technologies, with a focus to create a robust low data rate link. The payload of most drones, in particular considering the scenarios of interest, is a video link, either purely Wi-Fi or OFDM based. Considering that Wi-Fi is OFDM based, this can be seen as a single technology interference scenario.

The measurements should therefore assist in estimating the mutual interference on 2.4 GHz between DSSS/FHSS remote control systems and OFDM based Wi-Fi systems.

The result is that two basic questions need to be answered:

1. what is the impact of a remote control sending control data on the achievable throughput of Wi-Fi;
2. what is the impact of heavy Wi-Fi traffic on the reception of remote control data. These questions are executed as separate measurements.

The measurements and the results will be described in the next two chapters.

5 MEASUREMENTS AND RESULTS

The measurements executed assist in estimating the mutual interference on 2.4 GHz between DSSS/FHSS remote control systems and OFDM based Wi-Fi systems. The result is two basic questions: 1) what is the impact of a remote control sending control data on the achievable throughput of Wi-Fi; and 2) what is the impact of heavy Wi-Fi traffic on the reception of remote control data. These questions are executed as separate measurements.

5.1 Remote control interfering Wi-Fi

In order to estimate the impact of remote control transmissions on the throughput of Wi-Fi, open field measurements were executed on a runway of the former Airport Twente. By doing so, it was guaranteed that no interference was present.

Figure 16 shows the measurement layout. The measurement set-up consists of a pair of Wi-Fi devices. One device is configured as Access Point, the other device as client. The client is running a throughput performance test by transmitting as much data as possible in TCP mode. The Access Point echoes the data, so it is a two way test. The remote control is continuously transmitting. In this measurement set-up, the remote control receiving end, i.e. the drone, is not present.

Both Wi-Fi devices are 802.11n radios, have around 17 dBm output power and are equipped with an external omnidirectional antenna. The Access Point signal was attenuated by 20 dB, so that the communication link had a moderate quality, representing an indoor AP and an outdoor client. The system uses a 20 MHz channel, configured on Wi-Fi channel 6.

The distance between the Wi-Fi devices is 40 m. Exactly halfway, at 20 m, the remote control is placed on an orthogonal line at different distances, 0 m, 12.5 m, 25 m or 50 m from the straight line between both Wi-Fi devices.

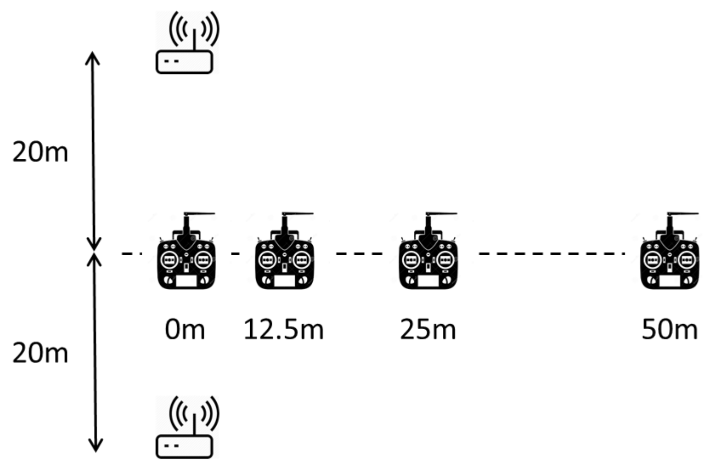


Figure 16 Measurement ground plan

The measurements are executed with seven different popular remote controls, of different manufacturers, including different technologies. As reference one test is executed without any remote control. The remote controls operate on 2.4 GHz, so all measurements are executed in this frequency band.

The test was executed with the following remote controls. As of January 1st 2015 there are new spectrum sharing rules. The test was executed with some pre-2015 and some post-2015 remote controls, so excluding and including these new regulations:

- Pre-2015 models:
  - Futaba SG14
  - Spektrum DX9 – DSMX mode
  - Graupner MX-20
  - Turnigy 9X
  - Multiplex Royal EVO
- Post-2015 models:
  - Jeti Duplex DS14
  - DJI Phantom 3 Advanced

Each measurement consists of a series of ten times ten measurements. So 100 measurements per remote control per position.

Figure 17 shows the effect of the transmissions of remote controls of various types of remote controls. The figure shows the median Wi-Fi throughput in the presence of remote controls of different manufacturers. The throughput is normalized to the median throughput for a case where no remote control is present.

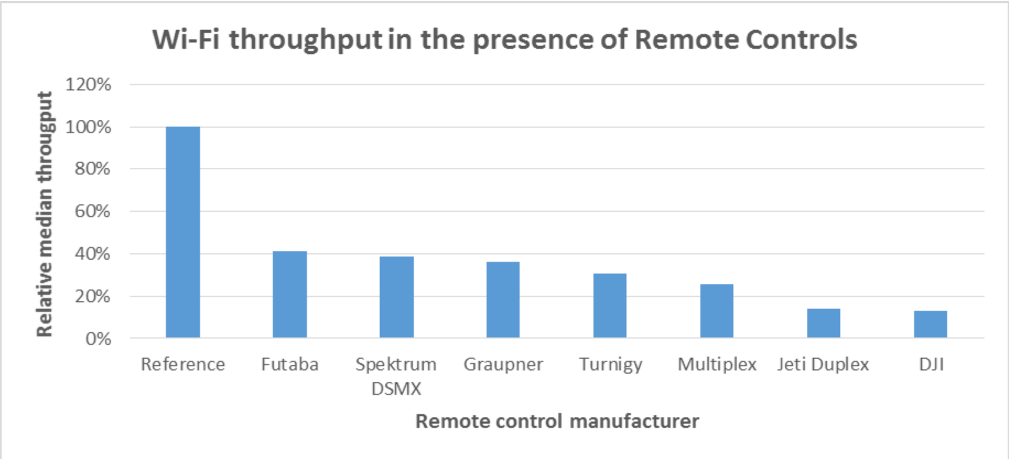


Figure 17. Median Wi-Fi throughput in the presence of different remote controls, relative to a reference case where no remote control is present

Figure 17 shows that turning on any remote control at the test location results in a drastic reduction in throughput in the Wi-Fi connection.

The figure shows from left to right the throughputs ordered to the median throughput. The figure shows that Futuba, Spectrum DSMX and Graupner cause the median Wi-Fi throughput to drop to around 40% and for Turnigy and Multiplex to around 30% of the reference throughput. Remarkably, the two models that include the latest standards regulations, Jeti Duplex and DJI, interfered the Wi-Fi connection most, resulting in a left-over throughput in Wi-Fi of less than 15% of the reference case. Whether this is a result of the new spectrum regulations or not cannot be concluded.

Also the difference between minimum and maximum Wi-Fi throughput increases significantly in the presence of interference of the remote controls. Figure 18 shows that in case no remote controller is active, the Wi-Fi throughput varies between -15% and +15% relative to the median. The measurements shows that the remote control can disrupt the Wi-Fi link completely (-100%). This is a typical behavior found when a remote control is near Wi-Fi. Too many consecutive packets fail, resulting in resynchronization of Wi-Fi. The figure also shows that the maximum throughput could be 50 to 150% higher than the median throughput for the same remote controls that can completely destroy the Wi-Fi link, so a large variability, being unstable.

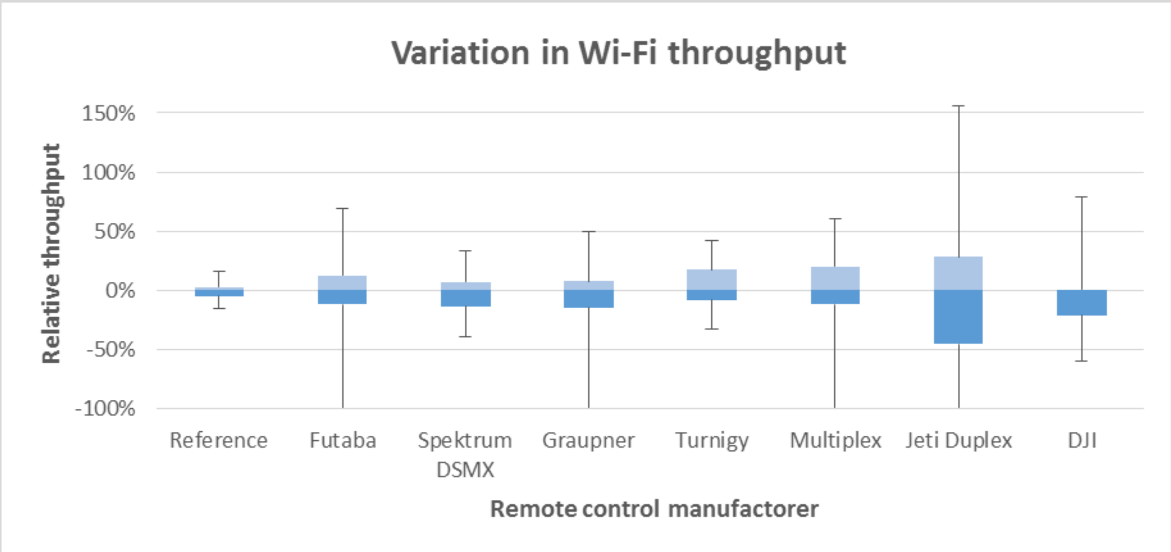
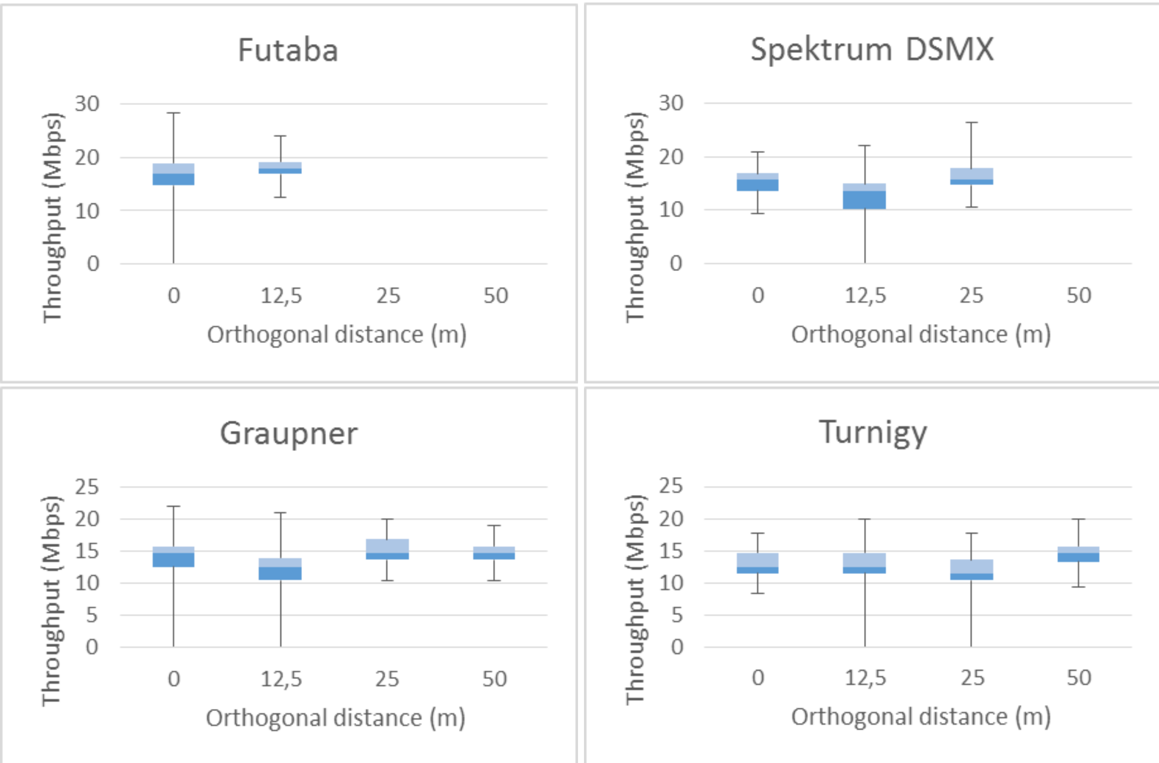


Figure 18. Wi-Fi throughput in the presence of different remote controls, relative to median throughput per case (box plot showing minimum, 25%, median, 75% and maximum relative throughput)

The Wi-Fi system occupies 20 MHz, which is ¼ of the 2.4 GHz band. It is remarkable that the presence of a remote control reduces the throughput of the Wi-Fi connection with a factor of 2.5 to 6. It is expected that this is due to the FHSS character of the remote control systems. FHSS spreads the signal over nearly the complete 2.4 GHz. The presence of the signal on each frequency is rather short, but by transmitting regularly at each frequency, the small amount of signal may cause a much larger number of times the Wi-Fi signal is either interfered, or the medium found occupied in CSMA.

The differences between the models can be found in a larger variety of parameters. Common to all models is the application of both DSSS and FHSS. The difference is that the DSSS bandwidth and the number of channels for FHSS differ. Probably the most significant difference to consider in relation to Wi-Fi is the FHSS hopping behavior, in particular the hop frequency. The bandwidth per FHSS channel may be of impact, but is expected to be secondary. To understand the effect in all aspects requires further study.

Figure 19 shows the measurement results for the various remote controls at the orthogonal distances 0, 12.5, 25 and 50 m. All results show only a marginal effect of the distance. The interference effect seems to reduce a bit for increasing distance, but this is too limited to consider in depth. The results show that a remote control transmitting at 50 m from a Wi-Fi device is interfering at the same level as when transmitting close-by.



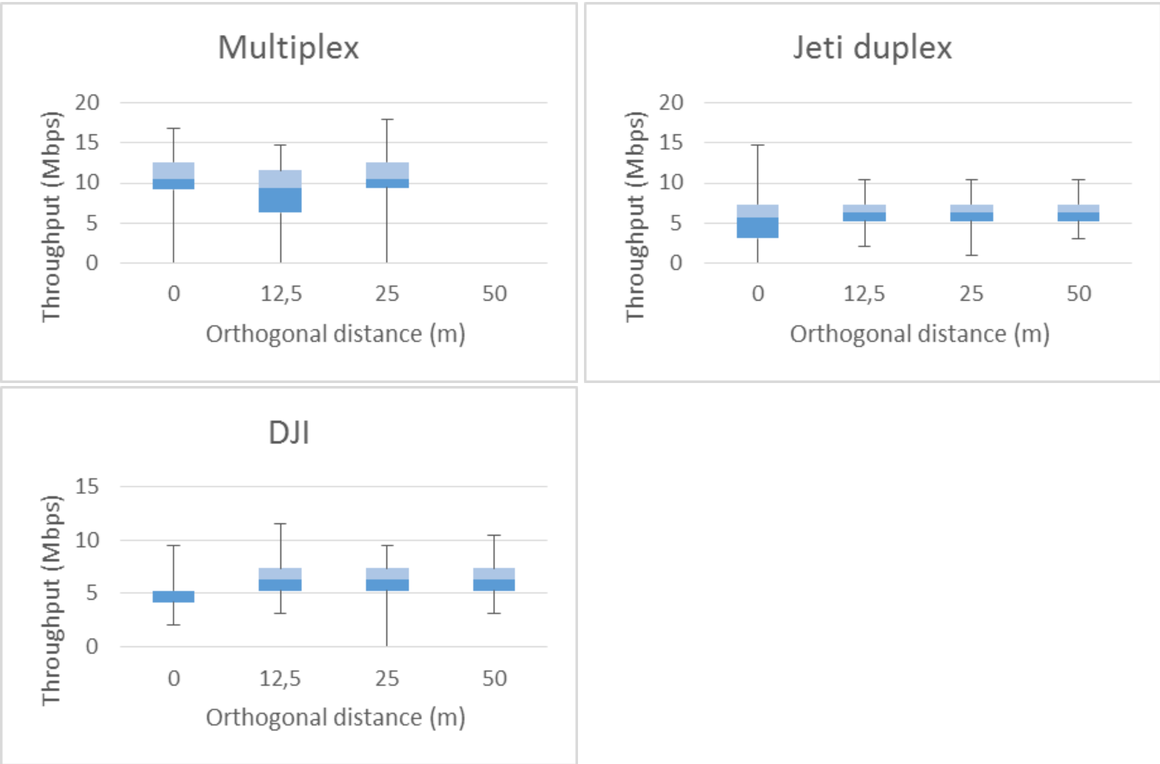


Figure 19 Wi-Fi throughput in the presence of different remote controls for different orthogonal distances

A second set of tests was examined the effect of a video link on Wi-Fi, using the DJI Lightbridge link. This video link was running on channels 1 through 3. The Wi-Fi connection was configured to either of the channels 2 or 11, so either on the same frequencies or on distinct frequencies. The Wi-Fi connection was running with or without a 20 dB attenuation.

Figure 20 compares the measured throughput of the Wi-Fi connection for the cases where communication was possible with the case of only the DJI remote control as reference. The figure shows that turning on the video link does lower the throughput in the Wi-Fi link, only in case the video link is running on the same channel as Wi-Fi. This is according to expectation. In order to have throughput on the same channel, the attenuation needed to be switched off. When the Lightbridge video link and the Wi-Fi link are configured to completely different channels, no interference from the video link is measured.

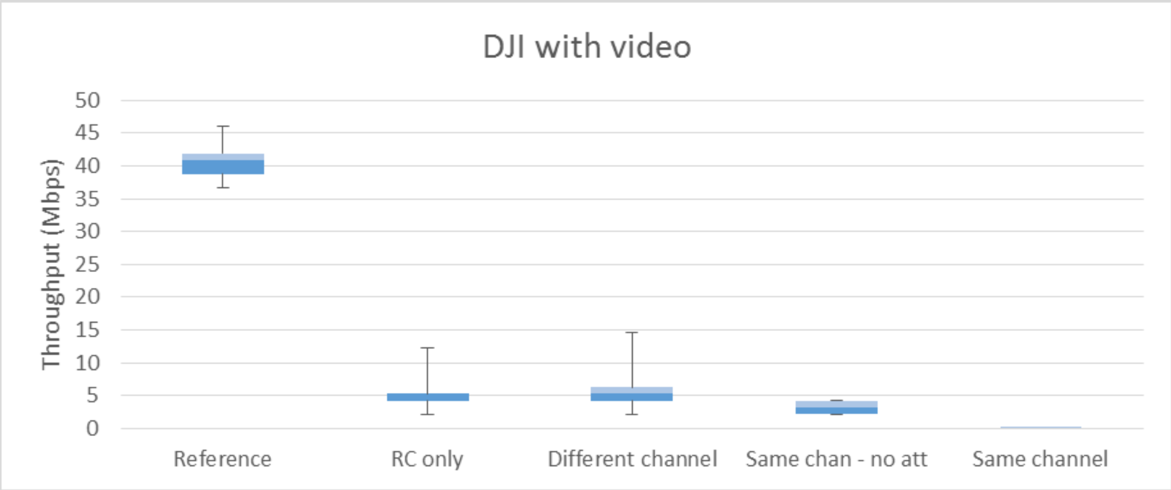


Figure 20 Wi-Fi throughput in the presence of DJI remote controls and video link

5.2 Wi-Fi interfering remote control

An additional set of measurements where performed to see if Wi-Fi could interfere a 2.4 GHz remote control. In this set-up three Wi-Fi Access Points where configured to channels 1, 6 and 11. All three Access Points where running a flooding script, i.e. sending as much data as possible. The Access Points operate according the CSMA rules, but do not require a counterpart for the transmissions.

The drone remote control link consisted of the remote control, and a receiver. The receiver was connected to a servo motor. In normal operation, the servo motor acts according to the commands it receives from the remote control. When interference starts to impact the link, remote control instructions will be missing. In normal operation, the system design can tolerate quite some loss, without losing control. In this test the failing of the remote control link is observed when the servo motor no longer acts correctly to the remote control instruction. This can be either a complete failure of the link, or a clear observation that the servo is no longer operating correctly.

The test was executed with the following remote controls. The older models do not comply to the new ETSI 300 328-v1.8.1 standard, while the newer models do:

- Compliant to ETSI 300 328-v1.8.1:
    - Spektrum DX9 - DSM2 mode
    - Spektrum DX9 – DSMX mode
    - Futaba
- Not Compliant to ETSI 300 328-v1.8.1:
    - Jeti Duplex DS14
    - DJI Phantom 3 Advanced

During these tests, interference of the remote control hardly occurred. Only the Futaba remote control did lose control due to the Wi-Fi interference. This however required full Wi-Fi traffic at close distance.

Before the test, is was expected that compliance to ETSI 300 328-v1.8.1 in the presence of very much Wi-Fi traffic would lead to a reduction in performance of the remote control. This effect was not observed in the measurements. A noticeable impact of ETSI 300 328-v1.8.1 compliance in the performance under all conditions cannot be excluded.

Interference of the remote control is feasible, but not very likely to occur.

6 ANALYSE MUTUAL INTERFERENCE SCENARIOS AND MODELS

The analysis of mutual interference between drones and other applications focuses on scenarios where a reasonable amount of drone usage is expected, and a realistic probability of interference is expected when drones are operated. E.g. inspection of a high-rise building in an urban environment is interference prone and will be studied, due to a high probability of close-by use of license exempt applications (e.g. Wi-Fi). A scenario where a drone is used for inspection of a windmill on an isolated place, is not expected to cause significant interference, and will hence be excluded.

As indicated in section 4.6 the 2.4 GHz band is the most interference prone license exempt band for drones. Therefore the scenarios and resulting analysis focusses on this band.

6.1 High-rise inspection scenario

This scenario is the inspection of a high-rise building in an urban environment. Figure 21 shows the layout of the scenario. In this situation a drone is used for the (visual) inspection of a high-rise building. The drone pilot is at the bottom of the building, while the drone is hovering at some limited distance from the building, streaming a video image of the building down to the drone pilot. A second high-rise building is located at some distance from the building being inspected.

6.1.1 Interference scenarios

Within this scenario, the following potential interference situations can be identified:

1. Remote control transmitter to indoor receiver
    a. The wanted signal is from an indoor transmitter in the same building.
    b. The receiver is an indoor device in the building
    c. The interfering signal is from the remote control outside
2. Indoor transmitter to remote control receiver
    a. The wanted signal is from the handheld remote control
    b. The receiver is the remote control receiver in the drone
    c. The interfering signal is from the indoor system
3. Drone payload transmitter to indoor receiver
    a. The wanted signal is from an indoor transmitter in the same building
    b. The receiver is an indoor device in the building
    c. The interfering signal is from the drone payload
4. Indoor transmitter to payload ground station
    a. The wanted signal is from the drone payload
    b. The receiver is the payload receiver on the ground
    c. The interfering signal is from the indoor system

These four interference conditions are applicable to the close-by building under inspection, and to the far-way “other” building. The only difference between both buildings is their distance to the remote control/ground station and the drone. In particular the drone will remain mostly very close to the building under inspection.

Besides the four potential interference paths, also the wanted signal path between remote control/ground station and drone exist. This covers two links, the remote control uplink and a payload downlink. Estimation of the interference requires an estimation of the path loss between the various transceivers. With the links mentioned three distinct paths are present, each covering two transmit and receive pairs:

1. Path between remote control/ground station and drone
2. Path between remote control/ground station and indoor transceiver
3. Path between drone and indoor transceiver

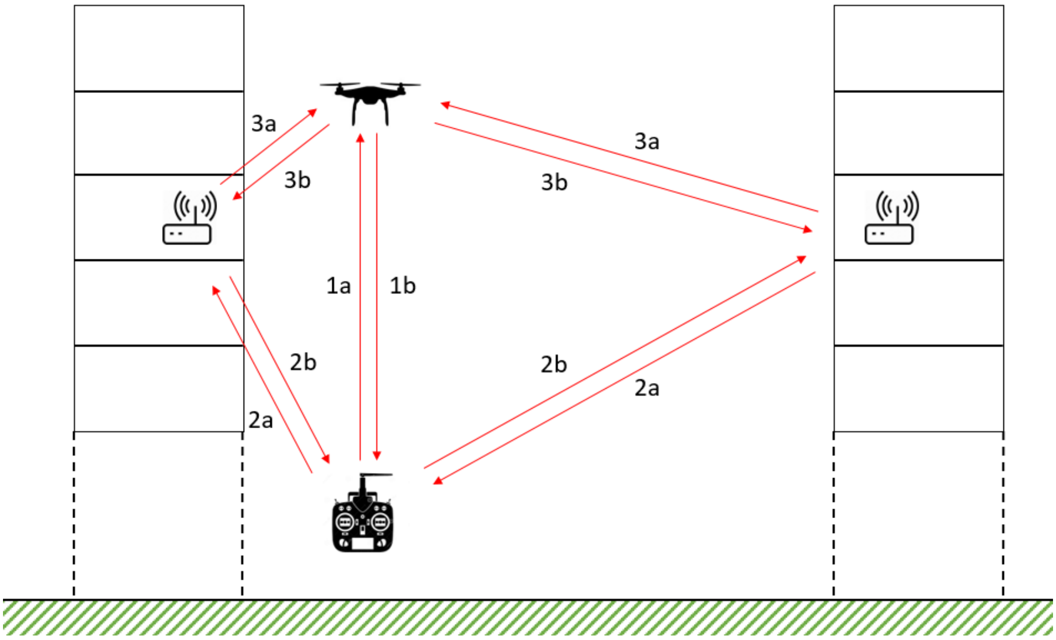


Figure 21 Transmission paths in high-rise building inspection scenario

The four potential interference conditions are analyzed pairwise according to the propagation paths in the next section:

path 2 Indoor – ground station:
   a. Remote control transmitter to indoor (Wi-Fi) receiver
   b. Indoor (Wi-Fi) transmitter to payload ground station

path 3 Indoor – drone:
   a. Indoor (Wi-Fi) system to remote control receiver
   b. Drone payload transmitter to indoor (Wi-Fi) receiver

6.1.2 *Estimation of interference*

6.1.2.1 *Indoor – ground station (path 2)*

There are two potential interference situations related to the propagation path "indoor – ground". Both the indoor Wi-Fi system and the drone remote control transmitter transmit near 20 dBm. So the signal strength of the remote control as received by the indoor Wi-Fi system, and the signal strength of the indoor Wi-Fi system received by the ground station are nearly equal, i.e. 20 dBm minus the propagation path. The impact on the receiver is however different:

- <u>Remote control transmitter to indoor Wi-Fi receiver</u>
  In the measurements in section 5 the interfering remote control signal was around -50 to -60 dBm. At the same time, the Wi-Fi signal was around -70 dBm. Seeing the large effect at this signal strength, interference is to be expected as long as the signal is over or equal to the Wi-Fi signal strength. The strength of a Wi-Fi signal will vary for any given scenario. In principle Wi-Fi could operate at sensitivity level, which is around -92 to -96 dBm, but most deployments lead to a signal strength of at least -70 dBm, and in most cases -50 to -60 dBm. Heavy interference from the remote control onto the Wi-Fi system is expected when the signal strength is over -60 dBm, and some interference when the signal is over -70 dBm.
- <u>Indoor (Wi-Fi) transmitter to payload ground station</u>
  The indoor Wi-Fi system applies OFDM, and the payload downlink applies mostly OFDM. Interference of both OFDM systems will only occur when both are operating on the same channel. On the 2.4 GHz band, three non-overlapping sub-bands exist. Considering that the building being inspected in this scenario is large, all three channels will be in use in some location of the building, so simultaneous use of the same channel is required.

  This simultaneous use can lead to interference. This will be the case when both systems transport a large amount of data. The video down certainly will. The indoor Wi-Fi system will typically be less active. Considering a video downlink transmitting at 20 dBm, and operating under line-of-sight conditions, the signal strength of the video transmission at the ground station will be around -50 dBm given the default scenario. Co-existence between the indoor Wi-Fi system and the video downlink will start to occur for a received signal strength of over -50 to -60 dBm. This effect will be strong when over -50 dBm, and limited when over -60 dBm.

Using these observations the following results are obtained.

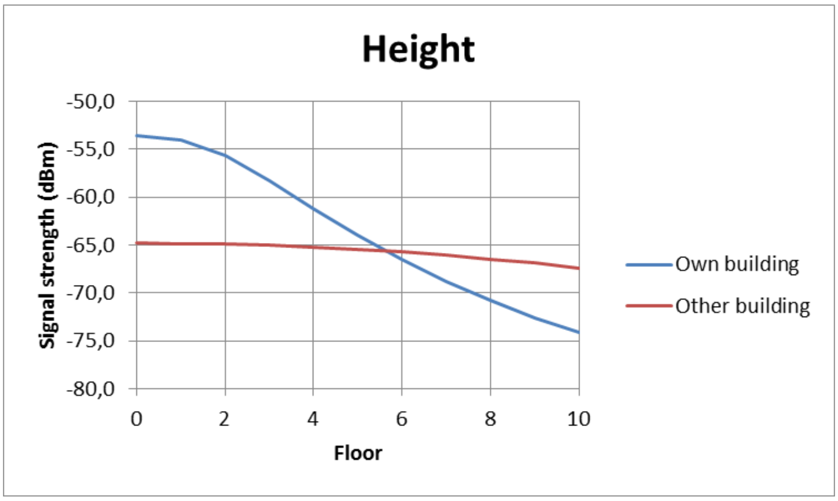


Figure 22 Received signal strength of interfering source for different heights in the high-rise building inspection scenario

Figure 22 shows the signal strength at the receiving victim (Wi-Fi signal strength received at ground station, or RC signal received at indoor Wi-Fi), varying the floor at which the indoor Wi-Fi system is being used. The figure shows the signal strength for the building under inspection (own building), and for a building at a distance of 50 m (other building).

The figure shows that heavy interference (> -60 dBm) is expected for the four lowest floors of the building under inspection, but is decreasing rapidly for increasing floors. Some more moderate interference (> -70 dBm) is expected in both the building under inspection and the remote building at 50 m.

With respect to interference of the indoor system onto the video ground station, only some limited effect is expected as the signal strength remains below -50 dBm. Some limited effect is interference is expect only when over -60 to -50 dBm. Some limited interference of Wi-Fi from the four lowest floors may be seen.

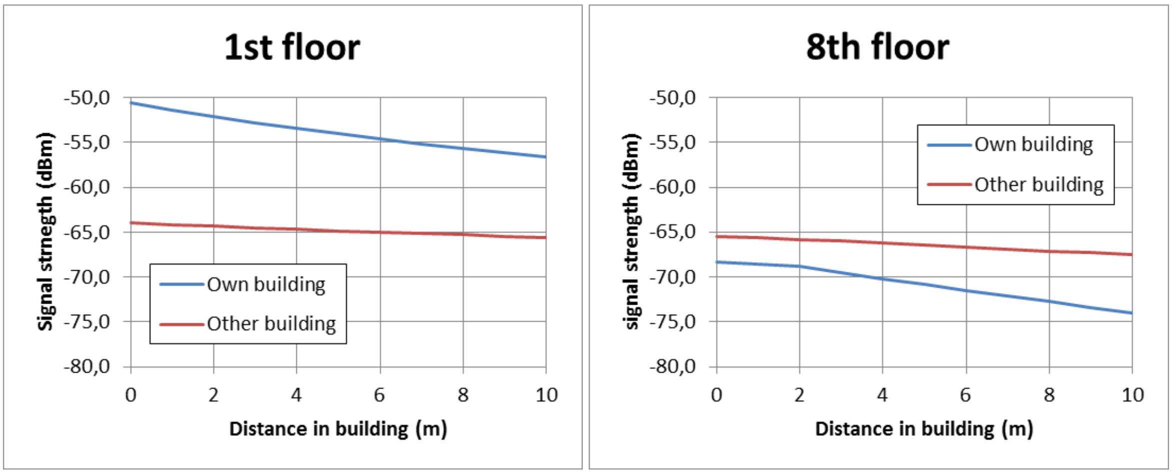


Figure 23 Received signal strength of interfering source for different distances in the building

Figure 23 shows the effect of the distance inside the building. Moving inside into the building will limit the amount of interference to some extent. This effect however is limited.

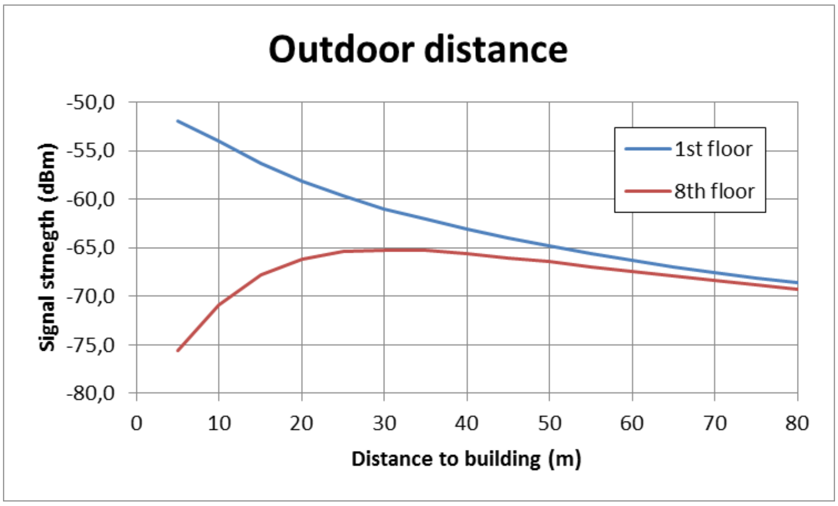


Figure 24 Received signal strength versus outdoor distance to building for 1st and 8th floor

Figure 24shows the effect of the outdoor distance. When considering a signal to or from the 1st floor, the signal strength drops with an increasing distance. For the 8th floor however the signal strength has a maximum at some distance from the building. For the lowest floors in a building, the risk of interference is realistic up to some tens of meters. For high floor some marginal probability exists, in particular when the remote control and ground station are at some tens of meter distance from the building. In all cases however, the risk of interference seems to be low to moderate.

6.1.2.2 Indoor – drone (path 3)

There are two potential interference situations related to the propagation path “indoor – drone”. Both the indoor Wi-Fi system and the drone video transmitter transmit near 20 dBm. So the signal strength of the video transmitter in the drone received by the indoor Wi-Fi system, and the signal strength of the indoor Wi-Fi system received by remote control receiver in the drone, are nearly equal, i.e. 20 dBm minus the propagation path. The impact on the receiver is however different:

- Drone payload transmitter to indoor (Wi-Fi) receiver
  The drone payload considered is an OFDM video transmitter. The interference or co-channel sharing situation for this case is comparable to two Wi-Fi systems operating in the same environment. As discussed in section 6.1.2.1, co-existence between the indoor Wi-Fi system and the video downlink will start to occur for a received signal strength of over -50 to -60 dBm. This effect will be strong when over -50 dBm (heavy interference), and limited when over -60 dBm (some interference).

- Indoor Wi-Fi system to remote control receiver
  The measurements in section 5 show that interference from Wi-Fi to a remote control receiver is only observed when Wi-Fi is dominant over the remote control signal. Assuming a drone height of around 30 m, and line-of-sight between remote control and drone, the signal strength of the remote control signal in the drone is around -50 dBm. So interference is expected when the Wi-Fi signal is well over -50 dBm (some interference), probably even over -40 dBm (heavy interference).

Using these observations the following results are obtained.

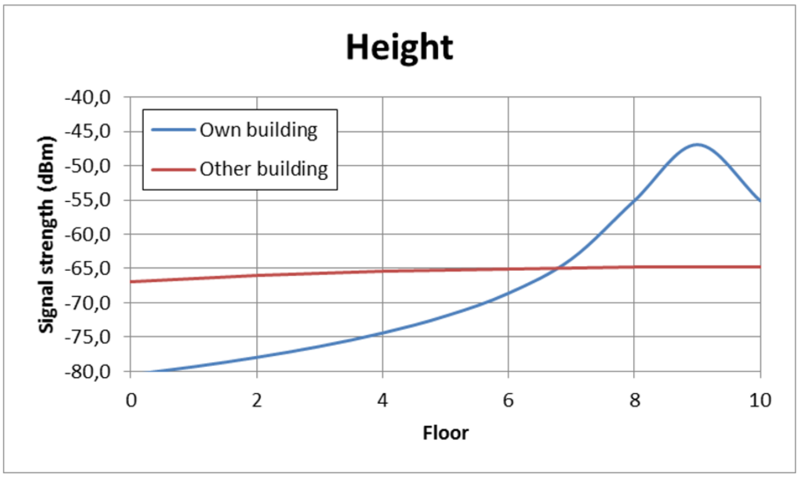


Figure 25 Received signal strength versus height (floor) indoor Wi-Fi system and drone inspecting 9th floor

Figure 25 shows the received signal strength of an indoor Wi-Fi system received at the drone, resp. the drone payload at the indoor Wi-Fi link. The figure shows the signal strength over different floors, where the drone is inspecting the 9th floor close-by (2 meters).

The figure clearly shows that the risk of interference is very much focused only on the floor under inspection, and the floors directly below or above. It is very likely that the drone payload will interfere the indoor Wi-Fi systems on the floor under inspection and the floors directly above and below, seeing signal strengths over -55 dBm. One floor lower or higher might still experience some effect. The signal strength is the remote building remains well below -60 dBm, so without noticeable interference.

The probability the indoor Wi-Fi system will cause interference on the drone remote control is however low. Only the signal from the floor under inspection will be over -50dBm, which is expected to cause some interference. But considering that it is only coming from one floor, it is very likely that this signal will not be active in the complete 2.4 GHz, so leaving space for the remote control FHSS system to communicate over a large part of the spectrum. So the risk of interference of the drone can be regarded negligible.

The default scenario assumes the drone to be flying at the 9th floor of the high-rise building. When assuming a drone flying a the maximum height of 120 meters, the remote control signal strength will drop by 10 dB to around -60 dBm. At such height interference of the indoor Wi-Fi system on the drone will become considerable. The signal strength of the indoor system will remain equal, but with the weaker remote control signal heavy interference is expected when the indoor signal strength is over -50 dBm, which includes the signal from at least the floor under inspection, but may include the floors just below and above. If the indoor Wi-Fi system is used intensely, the drone remote control may get disturbed.

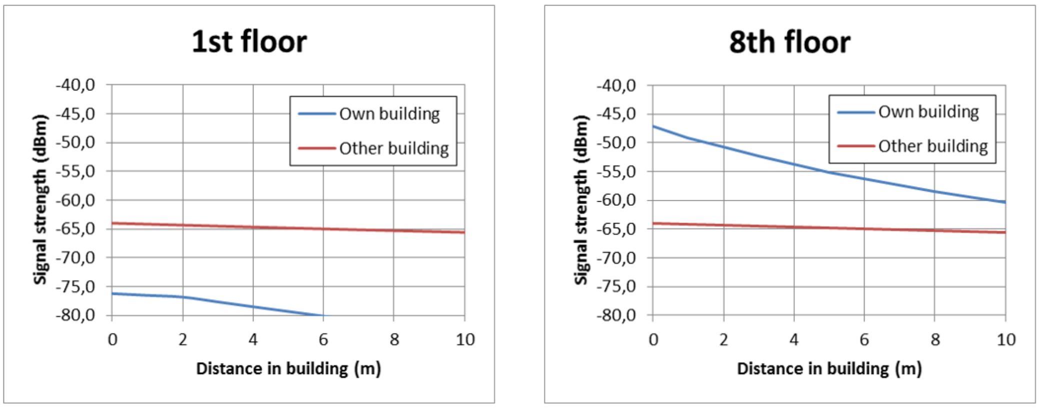


Figure 26 Received signal strength of interfering source for different distances in the building

Figure 26 shows the effect of the indoor distance. The effect of walking to or from the window is only of interest when being close to the drone, in this case being on the 8th floor. The probability the drone payload causes interference to the indoor Wi-Fi system or vice versa may become more apparent when people want to use Wi-Fi very close to the window. The heavy Wi-Fi usage is however likely not to occur this close to the window in most cases.

Figure 27 Received signal strength versus outdoor distance to building for 1st and 8th floor

Figure 27 shows the effect of the drone distance to the received signal strength. The figure shows that the signal strength has a maximum at some distance from the building under inspection, when this horizontal distance increases with the vertical distance to the drone. A very short distance of the drone to the building is beneficiary for the isolation between the radio signals of the drone and indoor systems, and limits the risk of interference.

6.1.3 Summary

The high-rise building inspection scenario shows that some risk of mutual interference between indoor (Wi-Fi) systems and the drone systems may occur. The analysis leads to the following conclusions.

1. Indoor (Wi-Fi) to drone interference:
    a. The probability indoor Wi-Fi will cause interference to the drone remote control is very low. Only when flying at large heights, when the remote control link weakens, some realistic risk of interference occurs. Even then the probability remains low.
    b. The probability indoor Wi-Fi will cause interference to the drone payload is realistic. This interference is caused by Wi-Fi systems operating close to the drone ground station.
2. Drone to indoor (Wi-Fi) interference:
    a. The probability the drone remote control will cause interference to an indoor Wi-Fi system is realistic. Such interference will exist for the lower three to five floors in the building.

b. The probability the drone video payload will cause interference to an indoor Wi-Fi system is likely for the floor under observation and probably for one floor lower and higher. This interference will limit the bandwidth of the indoor system, but not block it completely.

6.2 City park festival crowd observation scenario

In this scenario a large scale festival is organized in a city park. Examples may include the Parkpop festival in Zuiderpark - The Hague and the British Summer Time in Hyde Park - London. This scenario is not limited to concerts, but may be applicable to any large outdoor public event.

Figure 28 and Figure 29 show the layout of the scenario. In this situation, the drone is used for crowd control/crowd management. The drone is at some height, providing an overview image over the crowd. The drone pilot and video ground station are somewhere beside the event, but within the park, and in line-of-sight of the event.

The park is a city park, so it is close to residential areas. Typically terraced houses, or small apartment complexes. This can be characterized as an urban area.

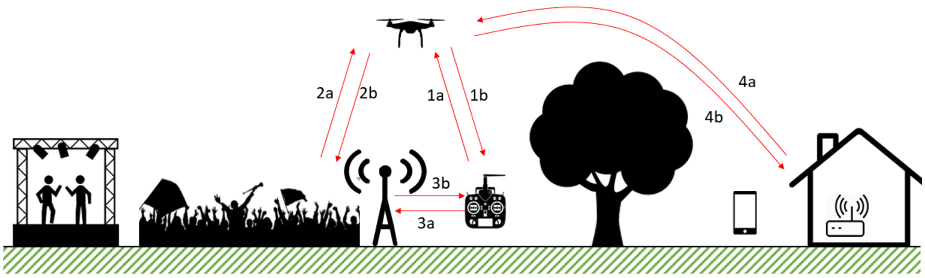


Figure 28 City park concert crowd observation scenario

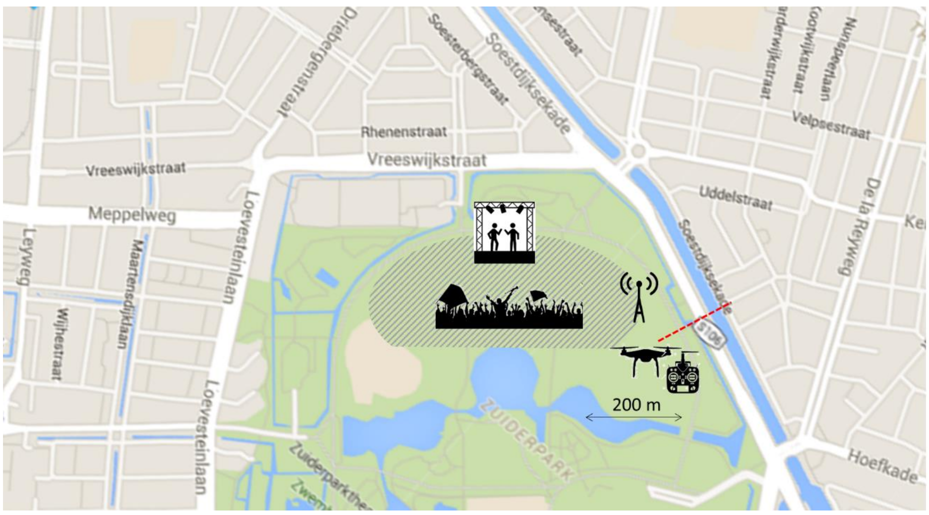


Figure 29 City park concert crowd observation scenario, top view

6.2.1 *Interference scenarios*

With respect to interference, two typical competing license exempt users are in the scenario:

1. The license exempt bands are used on site to provide wireless internet access (Wi-Fi) to visitors and/or staff.
2. A user may be using a Wi-Fi device in the garden of its home. As festivals are typically organized with good weather conditions and in weekends, the probability of user people being in their garden is rather high.

Within this scenario, the following potential interference situations can be identified:

At the park site

1. Remote control transmitter to visitor Wi-Fi system
    a. The wanted signal is from Wi-Fi smart phone to AP or vice versa
    b. The receiver is the counterpart, so Wi-Fi AP or smartphone
    c. The interfering signal is from the remote control (path 3a)
2. Visitor Wi-Fi system to remote control receiver
    a. The wanted signal is from the handheld remote control (path 1a)
    b. The receiver is the remote control receiver in the drone
    c. The interfering signal is from both visitor Wi-Fi AP and smartphones (path 2a)
3. Drone payload transmitter to visitor Wi-Fi system
    a. The wanted signal is from Wi-Fi smart phone to AP or vice versa
    b. The receiver is the counterpart, so Wi-Fi AP or smartphone
    c. The interfering signal is from the drone payload (path 2b)
4. Visitor Wi-Fi system to payload ground station
    a. The wanted signal is from the drone payload (path 1b)
    b. The receiver is the payload receiver on the ground
    c. The interfering signal is from both visitor Wi-Fi AP and smartphones (path 3b)

Around the park

5. Outdoor Wi-Fi smartphone used in the garden to remote control receiver
    a. The wanted signal is from the handheld remote control (path 1a)
    b. The receiver is the remote control receiver in the drone
    c. The interfering signal is a Wi-Fi smartphones used in a garden (path 4a)
6. Drone payload transmitter to Wi-Fi smartphone in garden
    a. The wanted signal is from an indoor Wi-Fi AP
    b. The receiver is a Wi-Fi smartphone used in the garden
    c. The interfering signal is from the drone payload (path 4b)

6.2.2 *Estimation of interference*

Section 6.2.1 identified two basic cases, in the park and around the park. The analysis is done accordingly.

6.2.2.1 Interference in the park

Figure 30 shows the signal strength of wireless devices received by a drone and vice versa versus the drone height (path 2). The potential interference from the drone to the users on site is the load of a video downlink. As indicated in section 6.1, the effect of sharing the same channel is expected to start to occur for a received signal strength of over -50 to -60 dBm. This effect will be strong when over -50 dBm (heavy interference), and limited when over -60 dBm (some interference).

Figure 30 shows that heavy interference of the drone payload on other applications is expected only when the drone is very close both horizontally (25 m) and vertically (< 25 m). As drones are not allowed to fly over crowds, it is likelier the distance is larger. The figure shows that a signal strength of over -60 dBm may realistically, so it is likely the drone payload will cause some interference to the users on site. The effect of the drone height is limited, so such situation will also occur when the drone is flying higher up.

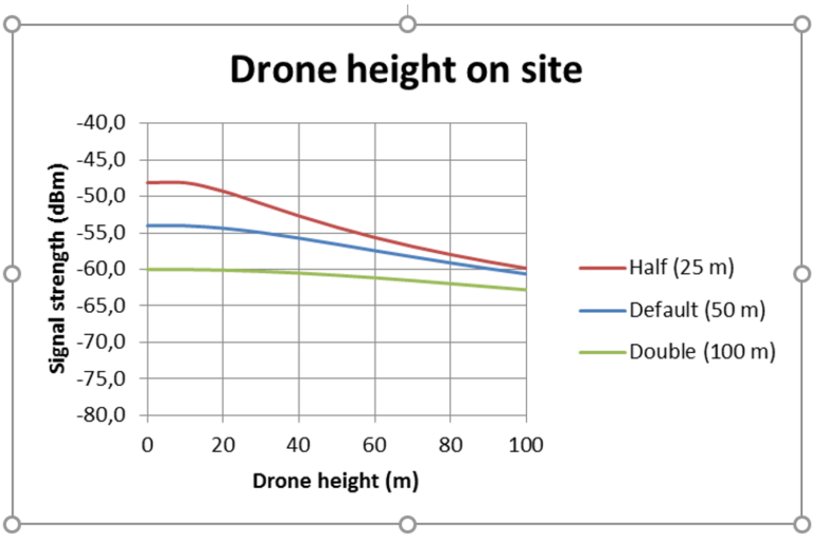


Figure 30 Signal strength of wireless applications at drone and vice versa

The values in the figure also hold for the signal strength of (Wi-Fi) systems on the ground as received by the remote control receiver in the drone.

Figure 31 shows the SNR of the remote control signal (path 1a compared to path 2a) for different horizontal distances between the drone and the remote control when varying the drone height. The horizontal distance between the drone and the interfering devices (path 2a) is 50 m, the default in this scenario.

As the remote control uses DSSS the SNR may become quite negative before losing the control. The exact value depends on the type of control, and is not publically known. It is estimated that control will not be interfered when the SNR remains over -3 to 0 dB. The figure shows that such situation can start to occur when the horizontal distance between drone and remote control is more than the vertical distance. Remind that the interfering source is also at 50 m from the drone.

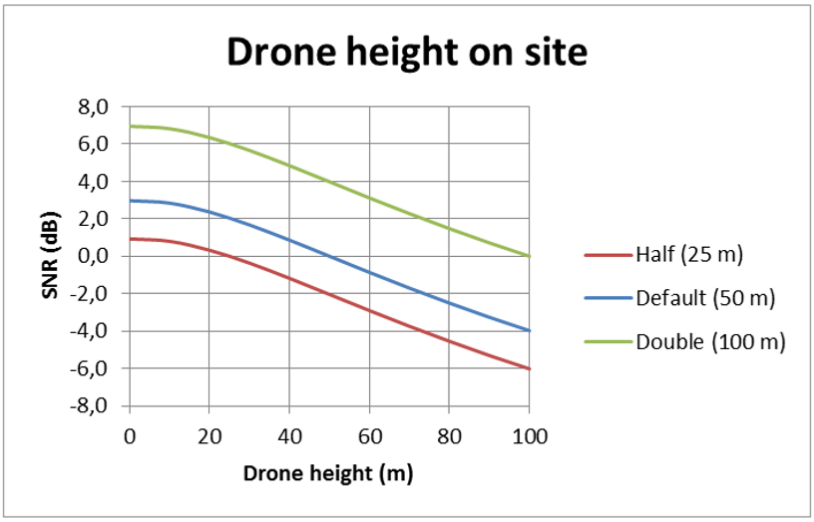


Figure 31 Signal to noise ratio for different drone heights versus the horizontal distance between remote control and drone

Figure 32 shows the signal strength of the remote control received by the Wi-Fi Access Point versus its distance (path 3). It is assumed the remote control and the Access Point are at line of sight with each other. The Wi-Fi Access Point will be higher up, in order to provide good coverage, whereas the remote control needs to have good coverage of the sky towards the drone, so will also be in an open place.

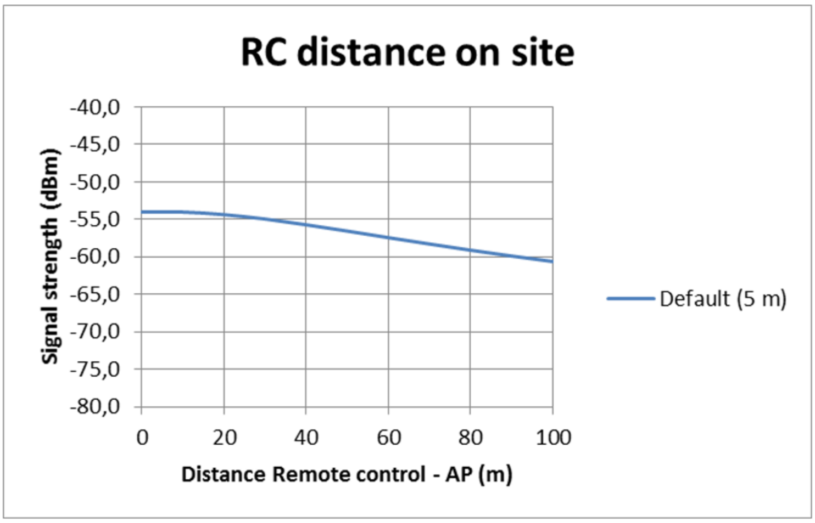


Figure 32 Signal strength of remote control at Wi-Fi Access Point

As discussed in section 6.1.2 heavy interference from the remote control onto the Wi-Fi system is expected when the signal strength is over -60 dBm, and some interference when the signal is over

-70 dBm. The figure clearly shows that it is more than likely the Wi-Fi system experiences heavy interference from the remote control.

The same signal strength also holds for the reception of the Wi-Fi Access Point signal received at the video ground station. As discussed in section 6.1.2 co-existence between the Wi-Fi system and the video downlink will start to occur for a received signal strength of over -50 to -60 dBm. This effect will be strong when over -50 dBm, and limited when over -60 dBm. The effect of the Wi-Fi Access Point onto the video ground station will be visible, but limited.

The reported signal strength applies under the assumption of direct line of site between the Wi-Fi Access Point and the remote control respectively the video ground station. The analysis shows that the interference is higher than wanted. Counter measures are possible through addition isolation between both systems. The simplest way to do so, is by adding requirements to the communication of the drone. Two possible measures:

1. By placing an isolating object (e.g. a wall or metal shield) between the drone remote control / ground station and the Wi-Fi Access Points.
2. By applying directional antennas on the remote control / ground station, pointing upward.

6.2.2.2 Interference around the park (path 4)

Interference around the park will only be between the drone in the air and other (Wi-Fi) users on the street or in the gardens of houses in a nearby residential area. The typical distance between the park and the closest houses is 200 m, whereas the default height of trees and houses is assumed to be 10 m. The distance between houses is 15 m, which is typical for urban terraced houses.

Figure 33 shows the signal strength versus drone height, for different distances between the drone and the location outside of the park. The figure shows that the signal strength increases with height until the drone is well over the tree/building height. At low heights the trees or buildings will block the signal.

The figure also shows that for the default distance (200 m) the signal strength remains very low. Recall that interference from the video downlink on other systems is expected when the signal strength is at least over -60 dBm, and that interference from other system on the remote control is expected for signal strengths at least over -50 dBm.

Given this analysis no interference is expected outside the park.

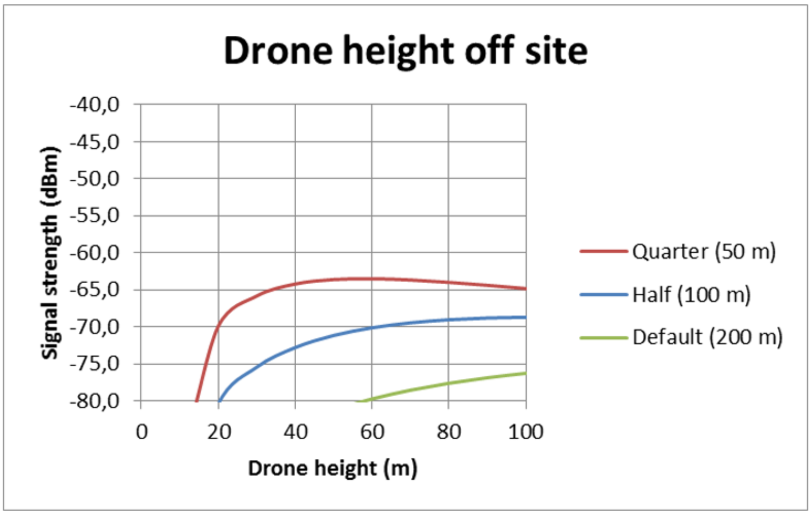


Figure 33 Signal strength of video downlink around the park and vice versa

6.2.3 Summary

The city park festival scenario relates to possible interference on the festival terrain as such and interference with the surrounding environment. The analysis shows that risk of interference is clearly limited to the city park. The probability surrounding residential areas are interfered or cause interference is negligible.

With respect to interference in the park four main cases lead to their own conclusions:

1. Drone payload to other (Wi-Fi) interference may occur. This however only in cases where a drone is flying at relative close distance to the other equipment (< 25 m) and at relative low altitude (< 25 m). At such distances the interference will remain moderate.
2. Disturbance of the drone remote control by other (Wi-Fi) interference, is unlikely in the vast majority of conditions. Though the SNR of the remote control signal may become low, the DSSS mechanism is expected to create sufficient performance even when the interferer is closer than the remote control. Of course the remote control range may be reduced due to this interference.
3. The other users in the park, in particular Wi-Fi Access Points positioned for coverage, may experience severe interference from a remote control. This may be the case even when the distance between one another is large. Providing additional isolation is important, being through isolating objects, or through directional antennas.
4. The video ground station may experience severe interference from other users, also in particular Wi-Fi Access Points being placed for coverage. In order to reduce interference, the same isolation measures as for the remote control apply.

7 CONCLUSIONS

Agentschap Telecom has assigned Strict and FIGO to investigate the impact of the increased usage of license exempt spectrum by drones. The main research question is:

“To what extent occurs (mutual) interference between drones and other unlicensed use and what are the consequences using these bands by drones?"

The research consisted of a market analysis, field measurements and analysis through scenarios, focusing on license expect spectrum.

The following use of license exempt spectrum is found:

- The 868 MHz band is used for telemetry in but not widespread;
- Nearly all drones use the 2.4 GHz band for remote control. The 2.4 GHz band is also popular for video downlinks, e.g. for FPV applications;
- Use of the 5 GHz band for drones is still low, but is increasing. This band is used for video downlinks. Most applications use the higher part of the band at 5.8 GHz.

With respect to the current and expected future use of drones, the following is observed:

- The current number of drones in the Netherlands is about 150.000;
- Most are for recreational use, only about 3000 for professional use;
- The exact numbers are unclear, unlike in the US where owners have to register their drone;
- The sales of drones are still increasing with 20-30% per year;
- Market leader in the Netherlands is DJI, but Yuneec is a strong contender.

With respect to the technical data, the average drone:

- Is a quadcopter;
- Weighs 1-2 kg;
- Has a diagonal size of ~500 mm;
- Has a maximum speed of 16 m/s (more than 50 kmph);
- Has a range of about 900m;
- Has a flight time of around 15 minutes;
- Uplink uses 2.4 GHz with FHSS+DSSS modulation for remote control ;
- Downlink uses 2.4 GHz or 5 GHz with OFDM modulation for video;
- Downlink uses 2.4 GHz or 5 GHz with OFDM modulation for the telemetry data.

With respect to frequency-related incidents or near-incidents

- Most incidents are related to users lacking knowledge about the risks and legislation;
- Problems with interference due to using license exempt spectrum is not recognized by all drone operators;
- However, the number of uncontrolled drone flights like fly-aways is very high, up to 50% of users have experienced this.

With respect to applied technology, the following is observed:

- Remote control is mostly implemented using proprietary technology. There is little compatibility among vendors. The technology however has many commonalities.
- The vast majority of remote control systems apply DSSS/FHSS technology. The differences can be found is the exact parameters. The focus of all manufacturers is providing a robust remote control link.
- A limited set of manufacturers use standard technology. ZigBee is used by Yuneec. ZigBee also uses DSSS, and should be comparable to the other systems. Wi-Fi is used only in toy-like drones, for very short range.
- FPV is very popular in consumer drones. This is implemented using Wi-Fi or FM in the case of drone racing. The geographical range of these applications is limited.
- (Semi) professional users make use special video links. State-of-the-art system use OFDM. Such systems can be found in both the 2.4 and 5 GHz bands.

With respect to the risk of interference of the remote control, the following is observed:

- Nearly all remote control systems use DSSS/FHSS. The technology focusses on robustness.
- No reported incidents were found where interference has caused the drone link to fail.
- The measurements indicate that remote control links are robust. When the drone is well in range of the remote control signal, the remote control link can handle a large amount of interference without noticeable performance impact.

With respect to the risk of interference by the remote control, the following is observed:

- The frequency hopping character of the remote controls causes significant interference on wideband applications like Wi-Fi, in case the signal strength is noticeable. Wi-Fi systems break down even when the signal hops to the frequency in intervals.
- Interference of the remote control signal is apparent when the remote control is near. So in cases where the distance between the remote control and the Wi-Fi system is in the same order of magnitude as the distances in the Wi-Fi system, Wi-Fi can fail completely.

With respect to the risk of interference of the video downlink, the following is observed:

- The probability a video downlink is disturbed on the 2.4 GHz band is realistic. This is however very scenario specific. The probability depends on the amount of Wi-Fi traffic near the ground station.
- The probability of interference in case the video uses 5 GHz is low. Most video downlinks use 5.8 GHz, which is not used by indoor Wi-Fi or other applications. In addition, the radio penetration through objects at 5 GHz is bad, resulting in small coverage areas. The potential interference is low in these small areas.

With respect to the risk of interference by the video downlink, the following is observed:

- The probability a video downlink disturbs Wi-Fi on the 2.4 GHz band exists, but is limited to very specific scenarios. E.g. in case of a high-rise building inspection, the interference is mainly limited to the floor under inspection.
- The probability of interference in case the video uses 5 GHz is low.

8 RECOMMENDATIONS

A mandatory examination by the drone user how busy the license-free bands are before the flight will decrease the risk of interference.

If an accessible reporting system is created for recreational drone users, include information if the incident is frequency related thus creating a better understanding of the real magnitude of the problem.

Inform recreational drone users about the risk of using unlicensed bands by drones, specifically when flying near buildings.

It is unclear what effect is of the more stringent ETSI 300 328-v1.8.1 requirements on drone equipment. Investigate whether this can make the drone control less reliable.

Several times we encountered equipment during this research for which was unclear the European standards were met. More strict monitoring and enforcing of equipment is required.

Once drone registration is required also include information on the used transmitter. This makes it easier to examine if an incident was frequency related.

Investigate whether it is possible establish at the international level a frequency for the use of drones, for example at 7 GHz.

Onderzoek of het mogelijk is in internationaal verband een frequentie vast te stellen voor het gebruik van drones.

9 ACKNOWLEDGEMENTS

We would like to thank the following persons and parties for their support with tests, sharing information and ideas:

- Justin Ma, FIGO, RC Racing
- Martijn Zagwijn, Brandweer Twente
- Casper Steenstra, Politie Nederland
- Ramon Wind, Clearflight Solutions
- Barend Houtsmuller, Strict
- Niels Bergervoet, Strict

10 ANNEX A: PROPAGATION MODELS

10.1 Path loss models for high-rise scenario

Figure 34 shows the layout of the high-rise building inspection scenario. The figure shows the parameter definitions in the scenario.

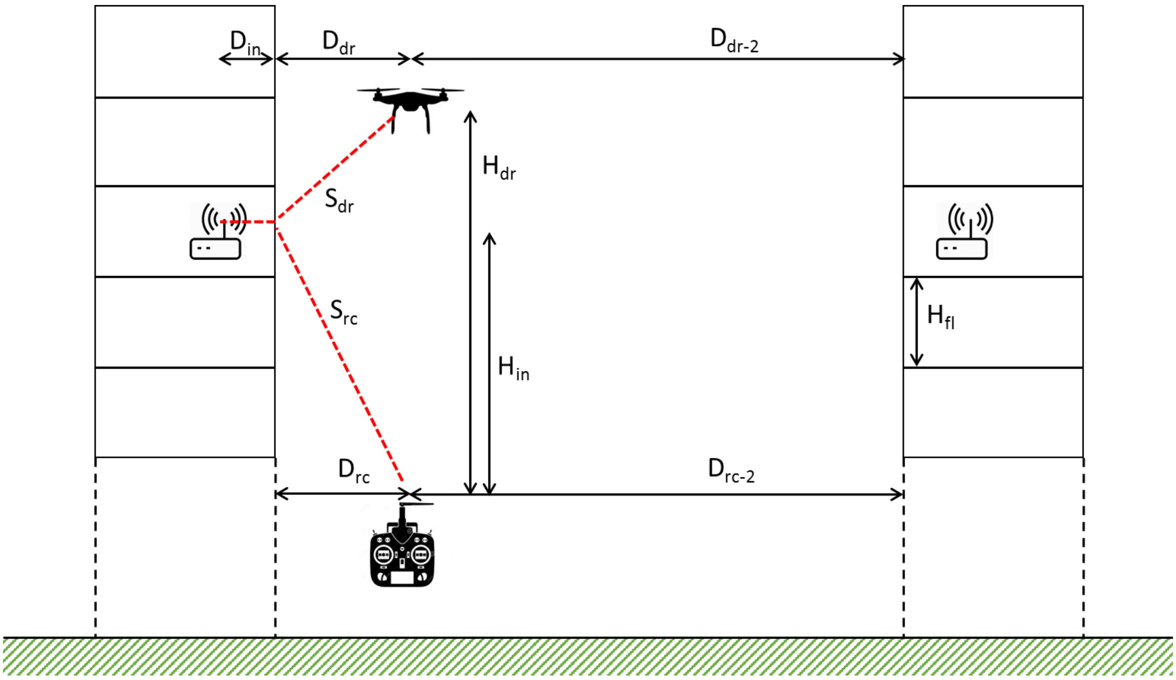


Figure 34 High-rise building inspection scenario

The interference in this scenario depends on the distances. The following distances are relevant:

- H_{dr} Height of drone to the remote control
- H_{in} Height of indoor transceiver to the remote control
- D_{rc} Horizontal distance between remote control handheld and building (D_{rc-2} for second building)
- S_{rc} Diagonal distance between remote control handheld and window closest to indoor transceiver: $S_{rc} = \sqrt{(D_{rc}^2 + H_{in}^2)}$
- D_{dr} Horizontal distance between drone and building (D_{dr-2} for second building)
- S_{dr} Diagonal distance between drone and window closest to indoor transceiver: $S_{dr} = \sqrt{(D_{dr}^2 + (H_{dr}-H_{in})^2)}$
- D_{in} Distance between window and indoor transceiver
- H_{fl} Height of one floor

Estimation of the interference requires an estimation of the path loss between the various transceivers. Within the high rise inspection scenario, three distinct paths are present:

1. Path between remote control/ground station and drone
2. Path between remote control/ground station and indoor transceiver
3. Path between drone and indoor transceiver

Path 1 is assumed to be free space. Paths 2 and 3 contain three parts: a free space outdoor component, a wall penetration part, and an indoor path. A similar situation is modelled by COST 231 as the "building penetration model for line-of-sight conditions"[60]. This model is designed for estimating the propagation loss for radio signals penetrating from an outdoor micro-cellular base station into a building on street level. The model is based on measurements in the frequency range from 900-1800 MHz and at distances up to 500 m. The height of high-rise buildings fits nicely within this model. Applying the model to the 2.4 GHz band should pose little restrictions. Validity of the model in the 5 GHz band is assumed.

The model assumes the direct path to be dominant, the effect on reflections from surrounding buildings are considered to be of secondary influence on the signal strength. The model further assumes free space propagation path loss between the external antenna and the illuminated wall. The wall penetration strongly depends on the angle of incidence, where propagation loss increases with a reduction of the angle of incidence. The indoor propagation path is modelled as free space plus the option for additional loss per wall being penetrated. This wall penetration is not taken into consideration for this model.

With the building penetration model as starting point, the various (reciprocal) paths are modelled as:

Path 1: $L = 32.4 + 20\log f + 20\log H_{dr}$

Path 2: $L = 32.4 + 20\log f + 20\log(S_{rc} + D_{in}) + W_e + \left(WG_e + \alpha(D_{in} - 2)\right) \cdot \left(1 - \frac{H_{in}}{S_{rc}}\right)^2$

Path 3: $L = 32.4 + 20\log f + 20\log(S_{dr} + D_{in}) + W_e + \left(WG_e + \alpha(D_{in} - 2)\right) \cdot \left(1 - \frac{|H_{dr} - H_{in}|}{S_{dr}}\right)^2$

All distances in this model are as defined above (in meters). The additional parameters are:

f	Carrier frequency (GHz)
W_e	Loss of the external wall at perpendicular penetration (dB)
WG_e	Additional loss of the external wall at a grazing angle (dB)
α	linear indoor attenuation factor (dB/m)

[60] "Digital mobile radio towards future generation systems – Final report", COST 231 Action, EUR 18957, Directorate-General Telecommunications, Information society, Information Market, and Exploitation of Research, ISBN 92-828-5416-7, EU 1999

The COST 231 report suggests the following setting for these parameters, which are also used in this report:

W_e ±7 dB for concrete buildings with normal windows
WG_e ±20 dB for distance up to 150m
α ±0.6 dB/m

Table 5shows the default set of parameters in the scenario.

Table 5 Default parameters fort the high-rise building inspection scenario

Scenario parameters			
Frequency	GHz	2,4	f
External wall loss	dB	10	W_e
Add wall loss	dB	20	WG_e
Indoor linear dist loss	dB/m	0,6	α
Default distance parameters			
Floor height	m	3,5	H_{fl}
Floor indoor	#	8	
Height indoor	m	28,0	H_{in}
Distance in building	m	5,0	D_{in}
Height drone	m	31,5	H_{dr}
Distance drone - building	m	2,0	D_{dr}
External distance drone	m	4,0	S_{dr}
Distance RC - building	m	10,0	D_{rc}
External distance rc	m	29,7	S_{rc}
Distance to other building	m	50	D_{dr-2}
External distance drone 2	m	50,1	S_{dr-2}
External distance rc 2	m	57,3	S_{rc-2}

10.2 Path loss models for city park festival scenario

Figure 35 shows the layout of the City park festival scenario.

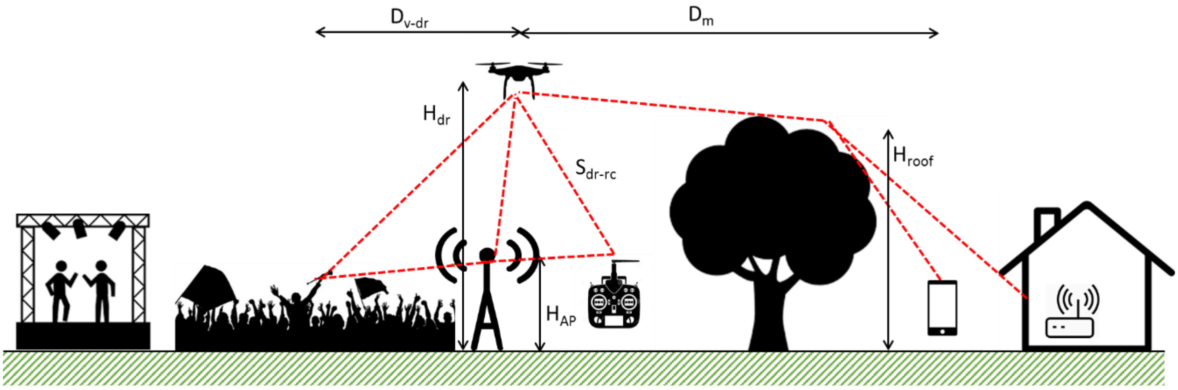


Figure 35 City park concert crowd observation scenario

The interference in this scenario depends on the distances. The following distances are relevant (mostly, but not all shows in Figure 35):

H_{dr}	Height of drone over the ground
H_{AP}	Height of Wi-Fi AP
H_{roof}	Height of rooftops/trees between park and houses
D_{rc-dr}	Horizontal distance between drone and remote control/ground station
D_{v-AP}	Horizontal distance between visitor (person in crowd using Wi-Fi) and Wi-Fi AP
D_{v-dr}	Horizontal distance between visitor (person in crowd using Wi-Fi) and drone
D_{v-rc}	Horizontal distance between visitor (person in crowd using Wi-Fi) and remote control/ground station
D_{rc-AP}	Horizontal distance between remote control/ground station and Wi-Fi AP
D_{dr-AP}	Horizontal distance between drone and Wi-Fi AP
D_m	Horizontal distance between drone and a mobile device in the garden or house

Estimation of the interference requires an estimation of the path loss between the various transceivers. Within the city park festival scenario, three distinct sets of paths are present:

1. Free space paths at the park site
   a. Drone – remote control/ground station
   b. Drone – Wi-Fi Access Point
   c. Drone – visitor
2. Line-of-site paths on the ground in the park
   a. Remote control/ground station – Wi-Fi Access Point
   b. Remote control/ground station – visitor
   c. Wi-Fi Access Point – visitor
3. Path between drone garden/indoor mobile devices (of site)

All paths under the first bullet are assumed to experience free space loss (FSL) radio propagation:

FSL: $L = 32.4 + 20 \log f + 20 \log d$

where:

d distance drone – mobile (m)

f carrier frequency (GHz)

The model for the second bullet is based on the COST231 – linear model[Fout! Bladwijzer niet gedefinieerd.]. This model adds a distance dependent linear loss. The model defines a variation of environments. The festival could be characterized as a "dense" environment, resulting in the following model for the analysis:

LOS: $L = 32.4 + 20 \log f + 20 \log d + 0.62\ d$

where:

d distance drone – mobile (m)

f carrier frequency (GHz)

The model for the third bullet is based on the COST231 – Walfish-Ikagami model[60]. This model is developed for predicting cell coverage in (sub)urban environments, for frequencies between 800 and 2000 MHz, transmitter heights of 4 to 50 meter and distances between 20 and 5000 meters. Applying this model to the 2.4 GHz band should not be of influence on the conclusions found.

The Walfish-Ikagami model distinguishes between line-of-sight (LOS) and non-line-of-sight (NLOS) situations. The LOS and NLOS conditions in this report fit well with the Walfish-Ikagami model. The model contains a large number of parameters, some of which are fixed for this study, to keep the complexity of the model realistic in the scope of this study. The following parameters are set fixed:

w 15 m (street width = distance between facades)

b 30 m (distance between rooftops)

φ 90° (street orientation)

The analysis will be further limited to cases where the drone is above the roofs, the mobile device is on ground level, and the scenario is urban, excluding a metropolitan area. The propagation models for the festival scenario are:

NLOS: $L = 6.4 + (25.3 + 0{,}757 f) \log f + 38 \log d + 2.27 f + 20 \log h_r - 18 \log(h_d - h_r)$

where:

d distance drone – mobile (m)

f carrier frequency (GHz)

h_r height of rooftops (m)
h_d height of drone (m)

Table 6 shows the default parameters used in the analysis of the City park festival scenario.

Table 6 Default parameters for the City park festival scenario

Scenario parameters			
Frequency	GHz	2,4	f
Default height parameters			
Height drone	m	50	H_{dr}
Height AP	m	5	H_{AP}
Height of roofs/trees	m	10	H_{roof}
Default horizontal distances			
Remote control - drone	m	50	$D_{rc\text{-}dr}$
Remote control - AP	m	20	$D_{rc\text{-}AP}$
Visitor - drone	m	100	$D_{v\text{-}dr}$
Visitor - AP	m	25	$D_{v\text{-}AP}$
Visitor - remote control	m	200	$D_{v\text{-}rc}$
Drone - AP	m	50	$D_{v\text{-}rc}$
Drone - mobile	m	100	D_m