The vulnerability of UAVs to cyber attacks - An approach to the risk assessment

2013 5th International Conference on Cyber Conflict
K. Podins, J. Stinissen, M. Maybaum (Eds.)
2013 © NATO CCD COE Publications, Tallinn

The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment

Kim Hartmann
Institute of Electronics, Signal Processing and Communication
Otto-von-Guericke-University
Magdeburg, Germany
kim.hartmann@ovgu.de

Christoph Steup
Department of Distributed Systems
Otto-von-Guericke-University
Magdeburg, Germany
steup@ovgu.de

Abstract: By 2012 the U.S. military had increased its investment in research and production of unmanned aerial vehicles (UAVs) from $2.3 billion in 2008 to $4.2 billion [1]. Currently UAVs are used for a wide range of missions such as border surveillance, reconnaissance, transportation and armed attacks. UAVs are presumed to provide their services at any time, be reliable, automated and autonomous. Based on these presumptions, governmental and military leaders expect UAVs to improve national security through surveillance or combat missions. To fulfill their missions, UAVs need to collect and process data. Therefore, UAVs may store a wide range of information from troop movements to environmental data and strategic operations. The amount and kind of information enclosed make UAVs an extremely interesting target for espionage and endangers UAVs of theft, manipulation and attacks.

Events such as the loss of an RQ-170 Sentinel to Iranian military forces on 4th December 2011 [2] or the “keylogging” virus that infected an U.S. UAV fleet at Creech Air Force Base in Nevada in September 2011 [3] show that the efforts of the past to identify risks and harden UAVs are insufficient. Due to the increasing governmental and military reliance on UAVs to protect national security, the necessity of a methodical and reliable analysis of the technical vulnerabilities becomes apparent.

We investigated recent attacks and developed a scheme for the risk assessment of UAVs based on the provided services and communication infrastructures. We provide a first approach to an UAV specific risk assessment and take into account the factors exposure, communication systems, storage media, sensor systems and fault handling mechanisms. We used this approach to assess the risk of some currently used UAVs: The “MQ-9 Reaper” and the “AR Drone”. A risk analysis of the “RQ-170 Sentinel” is discussed.

Keywords: *UAV, Risk assessment, Cyber attack, Security analysis*

1. INTRODUCTION

The targets of concern to cyber conflict researchers are often either civilian infrastructures or military computer systems. However, the increasing level of technology in modern warfare and the reliance on these technical devices enforces the investigation of the vulnerability of advanced military devices against technical attacks.

Unmanned aerial vehicles (UAVs) are currently reascending military aerial devices capable of operating without human pilots on board. Previously predominately used by military services, UAVs are becoming increasingly valuable to civil applications. UAVs may manoeuvre autonomously, relying on on-board-computers or be remotely controlled by pilots from ground stations.

Within the past 5 years several incidents concerning drones have been reported by the public news agencies, showing and increasing the public interest in military and civilian drone applications.

The U.S. military increased its investment in the research and production of UAVs from $2.3 billion in 2008 to $4.2 billion in 2012 [1]. UAVs are currently used for a wide range of operations such as border surveillance, reconnaissance, transport and armed attacks.

UAVs are presumed to be reliable, automated and autonomous machines, providing their services at any time. Based on these presumptions, governmental and military leaders hope that UAVs improve national security. However, reviewing UAVs from a technical point of view, UAVs must be classified as highly exposed, multiply linked, complex pieces of hardware with high strategic and economic value.

It is interesting and bizarre that there is more research done regarding the security of modern cars incorporating car-to-car- and car-to-infrastructure-communication than research regarding the security of UAVs. It is unclear whether this is an effect of the closed-source-politics due to UAVs military origins or if these devices are simply considered to be secure due to their original tasks.

System security should never be considered as a state, but rather as a process. In order to support this process, it is important to be capable of describing and judging the current security status. Furthermore, it is desirable to be able to compare system configurations in terms of security levels. In order to fulfil these tasks, we are confronted with the questions: What is security and how is it measured?

Focusing on the technical aspect of the questions, (information) security is defined in the 44 USC §3542 [4] as " … protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction … ”. Hence, security is a value describing how good a system is protected against the above named.

In order to determine how good a system is protected, it is important to know its vulnerabilities. Technically, the vulnerability of a system is an aspect of the system that heightens the probability of malfunction due to specific incidents. Depending of the severity of the malfunction, ranging from the complete loss of control/ destruction of the system to mere errors, the vulnerability may impose a threat to the systems security. In other words: A threat is a possible incident with a severe impact on the systems security. An incident may either be an attack or an event [5].

In terms of system security, a risk is a combination of the severity of the impact of an attack on the systems security, multiplied by its probability of occurrence. Hence, risk assessment quantifies the possible severity and likelihood of attacks. It is a crucial value for any high-level security system [6].

Interestingly, attackers searching for targets go the same way as system architects designing a secure system. An attacker is searching for a system vulnerability imposing a high threat, implying a high risk. A system architect is trying to eliminate vulnerabilities imposing high threats and hardens the system through the integration of coping mechanisms.

To heighten the systems security it is essential that the system designer finds vulnerabilities before attackers do. This is achieved by continuous risk analysis and assessment. Risk assessment schemes defined for most types of software- and hardware-components exist. However, none such risk assessment scheme or guideline for UAVs was found. Alarmingly, the reported incidents regarding UAVs indicate that the risk assessment – if used - for UAVs must be deficient. This paper aims at improving this situation through supplying a prototype scheme for the risk assessment of UAVs and the initiation of an academic discussion on the topic.

2. UAV – BASICS

UAVs are highly exposed technical systems. To analyse an UAVs vulnerabilities, it is important to understand what components an UAV is made of and how these components interact. In order to analyse UAVs on a common basis, we described UAVs in terms of component models.

Figure 1 shows a general component model of a standard UAV, without autonomous flight entity and weapons. The model in Figure 1 describes the basic components a UAV must incorporate.

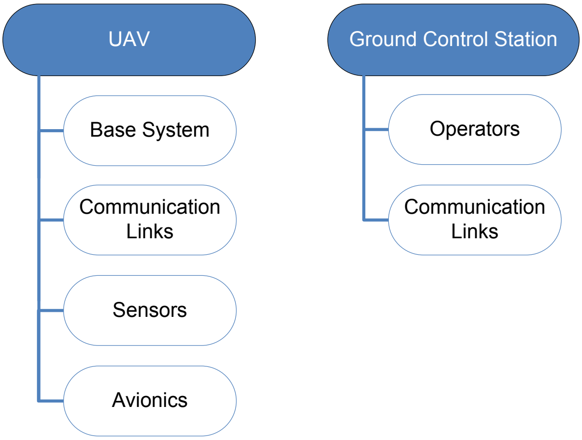


Figure 1. Right: General component model of a UAV. Left: Simple component model of a ground station

The “UAV base system” is the foundation of the UAV linking together the UAV components. It is needed to allow inter-component communication and controls the sensor, navigation, avionic and communication system. It may be considered as an UAV “operating system”. The base system also allows the integration of further optional components such as special sensors or weapon systems.

The UAV sensor system consists of the sensory equipment of the UAV together with integrated pre-processing functionalities. For common military UAVs these sensors are often cameras with different capabilities. UAVs may be equipped with further sensors, such as INS, GPS and radar.

The UAV avionic system is responsible for the conversion of received control commands to commands of the engine, flaps, rudder, stabilisers and spoilers.

The in-flight communication of UAVs is always wireless and may be divided into two types: a) direct, line-of-sight (LOS) communication and b) indirect – mostly – satellite communication (SATCOM).

Figure 2 displays the information flow between components of the UAV system.

Newer UAVs, such as the RQ170 Sentinel, are able to operate autonomously. They may be additionally capable of holding and operating weapons as well as weapon supporting systems (e.g. the MQ-9 Reaper).

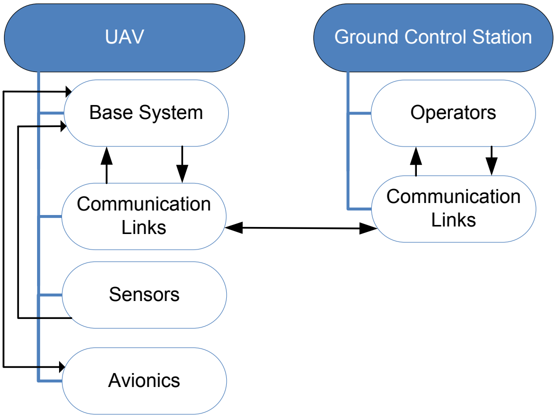


Figure 2. Information flow between the UAV components and the ground station

To account to the above adjustments, an extended UAV component model is given in Figure 3.

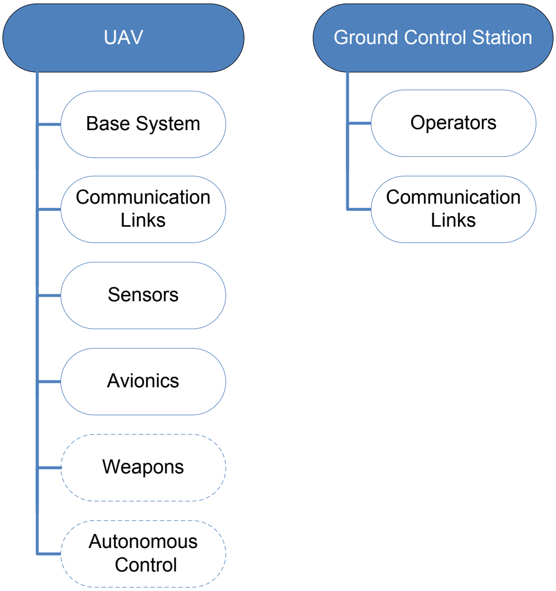


Figure 3. Extended UAV component model

The information flow within the extended UAV component model may differ, according to the UAV type. The exact internal communication may be relevant for an attacker, if the attacker already has access to the internals of the system. Otherwise it is not essential.

Unless physical access to the UAV is given, an attacker must access and influence the UAV externally. Luckily for an attacker, UAVs are highly dependent on external input and therefore provide multiple input channels. Due to the "wireless nature" of UAVs, these channels are wireless and hence difficult to harden.

There are several information flows between an UAV and its environment, as shown in Figure 4. The two most important operational connections are 1) the bidirectional information flow between the communications system and the ground control station (GCS) and 2) the information flow from the environment to the sensors.

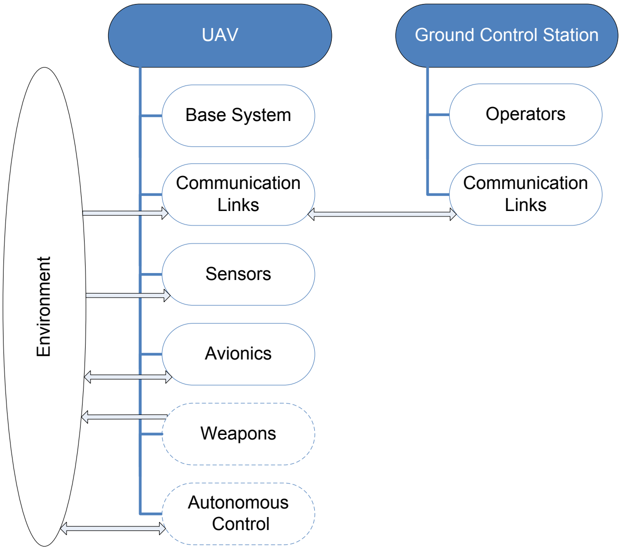


Figure 4. Extended UAV component model with information flow

However, additional influences between the environment and the UAV must be considered. These influences are the changes of the attitude of the UAV induced by the avionics, the result of weapons on the environment and the influence of the environment on the communication links.

The links are diverging in reliability and receptive to manipulation in different ways. While the reliability of sensors and system components are mostly investigated during system design, the consideration of the receptiveness of a sensor or system component to manipulation is not common.

The key to unauthorised control of an UAV is knowledge of the receptiveness of the system components to manipulation. To avoid third parties to take advantage of this knowledge, the receptiveness must be considered during system design.

3. RECENT ATTACKS

The incorporation of UAVs in military services was accompanied by a series of accidents having a broader impact on the overall security of UAVs.

One of the most recent and interesting incidents was the claimed theft an RQ-170 Sentinel by Iranian forces. It is widely accepted that Iranian forces are in the possession of the RQ-170 Sentinel. This claim was implicitly confirmed by a press statement of US-President Obama, asking for the return of the UAV [2] .

However, the circumstances under which the UAV came into the possession of the Iranian forces are controversial. Two popular theories exist that explain how the RQ-170 Sentinel may have been lost.

The first theory supposes that a vulnerability of the UAV sensor system with effects on the navigation system was used to attack the GPS system, discussed by Humphreys [7]. The attack uses details about the GPS functionality which make it easy to attack the GPS system of an UAV by a "GPS-spoofing"-attack. The GPS-satellite-signal is overlaid by a spoofed GPS-signal originating from a local transmitter with a stronger signal. The spoofed GPS-signal simulates the GPS-satellite-signal, leading to a falsified estimation of the UAVs current position. Supporter of this theory suppose that Iranian forces jammed the satellite communication of the drone and spoofed the GPS-signal to land the drone safely on an Iranian airfield.

Although the described attack is difficult to execute, it is not impossible [8]. If Iranian forces possess the knowledge and techniques to complete a GPS-spoofing attack remains and open question.

The second theory explains the loss of the UAV as a result of a technical malfunction. The theory postulates that the UAV may have landed on Iranian territory due to a technical malfunction. This may have allowed Iranian forces to recover the UAV.

Both theories indicate security problems. The GPS-Spoofing theory emphasises the necessity to include further and unusual components (e.g. sensors, input channels) in the risk assessment of UAVs. Partial autonomous systems as UAVs are dependent on their sensor systems in order to operate correctly. Furthermore, the sensor system must be reviewed as a continuously open input channel and may hence be prone to attacks.

Some reported incidents craved the destruction of the UAV to secure the confidentiality of sensitive data, [9], [10]. The technical malfunction theory claims that a self-destruction of the RQ-170 Sentinel was not possible. Regardless whether this theory is correct or not, it shows the necessity to examine the autonomous behaviour of UAVs regarding the security implications. An UAV must be capable of autonomously choosing the right strategy in case of a severe fault to uphold the systems security.

Another threat to UAVs is the exposure of the GCS to viruses as in the keylogging-virus attack [3]. The possible consequences may range from a loss of sensitive data to a loss of control of the assigned UAVs.

Another type of attack reported aimed directly at the communication link between the UAV and its GCS. During this attack live video feeds of an UAV were captured by Iraqian forces. The attack was possible due to a disabled encryption of the communication link. The software used to accomplish the attack was worth $26 [11].

4. PROACTIVE RISK ASSESSMENT SCHEME

We assessed the risk of security violations of UAVs based on our component models. Accordingly, the overall risk assessment of an UAV is the summation of its components risk assessment.

The risk assessment result of the provided scheme is multi-dimensional. It provides the risk assessment according to the type and intensity of security needed. It is a component-wise, probability-based evaluation of integrity, confidentiality and availability of the UAV [5]. A high score in the risk assessment scheme corresponds to a high risk regarding the loss of confidentiality, integrity or availability.

The scheme provides information on the susceptibility of components to attacks on the integrity, confidentiality or availability of the component, respectively of the UAV. According to the level of susceptibility, values between 0 and 1 are appointed to the component (0 meaning “not susceptible”, 1 corresponds to “highly susceptible”).

The values given by the scheme represent the susceptibility of the investigated component to attacks influencing integrity, confidentiality or availability. To calculate the risk, the specific probabilities of the occurrence of an attack are multiplied with the susceptibility value [12]. The result must be evaluated according to the severity of the loss of integrity, confidentiality or availability of the investigated component/UAV [6]. The aspects of security may be in conflict.

The multi-dimensional risk assessment considers the different requirements of UAVs. According to the general task of the UAV, different aspects of security play varying roles and must be weighted accordingly. Therefore, the risk assessment of UAVs is always mission-bound.

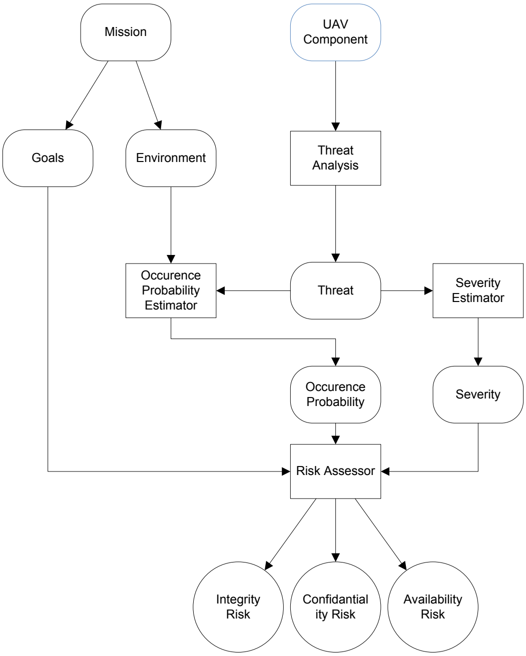


Figure 5. General overview of the proposed UAV risk assessment scheme.

A. ENVIRONMENT

As seen in the component model in Figure 1, the environment influences the UAVs sensors, its communication links and avionics. Hence, the environment must be considered in the UAV risk assessment. It is important to distinguish between political and physical factors of the environment, as these influence security aspects differently.

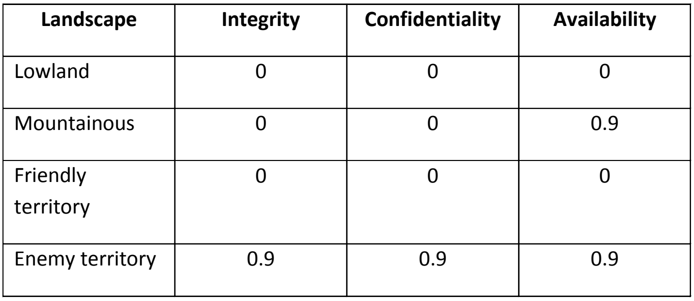
The landforms may be classified according to geomorphological categories. We considered two types of landscape (lowland and mountainous) and two political states (friend or enemy). This selection is only for demonstration purposes.

The influence of environmental factors on the UAVs security level in terms of availability, confidentiality and integrity is shown in Table I. The physical factors described are not capable of influencing the UAVs confidentiality or integrity.

However, other factors such as weather conditions, altitudes etc. may influence integrity.

The two political factors considered have influences on all aspects of the systems security. An UAV moving in enemy territory may lose its availability due to a heightened threat of destruction, takeover, signal disturbances etc.. Additionally, the UAV is exposed to the threat of confidentiality or integrity loss due to the risk of takeover, theft or manipulation.

Table I. Prototype environmental influence on UAV



Landscape	Integrity	Confidentiality	Availability
Lowland	0	0	0
Mountainous	0	0	0.9
Friendly territory	0	0	0
Enemy territory	0.9	0.9	0.9

B. COMMUNICATION LINKS

For the investigated UAVs, the satellite link tends to use the K_u-Band. The LOS-communication with the GCS is often based on the C-band or WiFi b-/g- or n-standard.

The following subsections give a short introduction on common communication types.

1) TCDL Ku-band communication

The TCDL (Tactical Common Data Link) is a secured data link developed by the U.S. military, capable of deriving data from different sources. It may furthermore route, encrypt, de-/multiplex, encode and transmit data at high speeds.

The TCDL uses a narrowband uplink at 15.15 GHz – 15.35 GHz and a wideband downlink at 14.40 GHz – 14.85 GHz. The TCDL may be operated both with directional and omnidirectional antennas and has ranges of 200 km at rates from 1.5 Mbit/s to 10.7 Mbit/s and low bit-error-rates. It may be used to transmit sensor data of any kind, especially radar, images and video signals.

One characteristic of K_u-band-based communication is that it is susceptible to rain/

snow fade. Due to the high frequencies used the signal may become disturbed by air humidity.

However, K_u-band-based communication is harder to overhear and hence harder to actively disturb than other comparable communication links, as required by [13].

2) LOS Communication: C-Band

Generally, the C-band describes the electromagnetic spectrum ranging from 4 GHz to 8 GHz. The C-band is used by a wide range of applications, such as weather radar systems, satellite communication, cordless phones and WiFi communication.

The frequencies relevant to uplink/downlink of the UAV communication systems investigated are 4.4 – 4.94 GHz and 5.25 – 5.85 GHz.

The C-band communication is less susceptible to air humidity than K_u-band communication. Nevertheless, due to the variety of applications, several COTS-devices exist that may interfere the radio signal and cause signal distortion.

UAVs tend to use omnidirectional antennas for C-Band communication, heightening the threat of interception by third parties.

3) LOS Communication: WiFi a/b/g/n

WiFi, synonymously described as "WLAN", refers to any communication based on the IEEE 802.11-standard. The frequencies used and the transmission rates differ according to the used standard. WiFi a, referring to the IEEE 802.11 a standard, ranges from 5.15 GHz – 5.75 GHz at transmission rates of 54 Mbit/s. The b and g standard operate in the frequency range of 2.4 GHz – 2.4835 GHz at 11 Mbit/s (b), respectively 54 Mbit/s (g). The WiFI n standard may operate both at 2.4 GHz as well as in the 5 GHz range. Due to the use of MIMO (Multiple Input Multiple Output), the n standard may transmit over longer distances and higher rates (up to 600 Mbit/s). To cover longer distances and achieve higher rates, the n standard uses multiple data streams and up to 4 antennas.

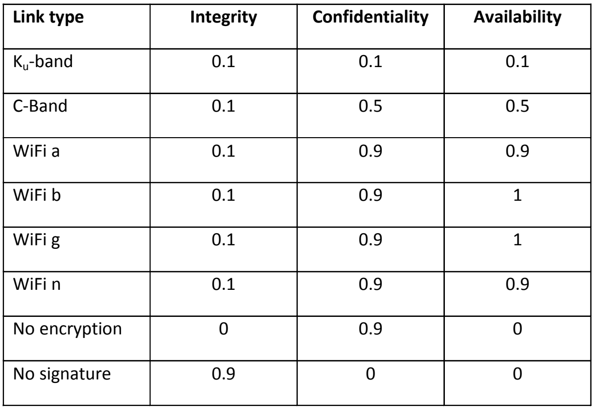
Due to its multiple applications and free usage, the b and g standard must expect signal interference. The frequencies above 5 GHz are restricted; hence interferences through civil applications are less likely. However, this may change in the near future (5-GHz-WLAN)

Because of the omnidirectional antennae used in the WiFi standards, WiFi is susceptible to eavesdropping. Precautions such as tunneling and encryption may be taken, but the general risk of eavesdropping – compared to other media – is still heightened as no knowledge of the signals direction is needed to tap the signal.

4) *Summary - Scheme for communication links*

The result of the general risk assessment scheme for communication links is shown in Table II. It is important to note that - although all communication links impose security threats to all aspects of security - the degree of susceptibility varies greatly. The overall risk depends on the specific task.

Table II. Risk assessment results for commonly used communication links



Link type	Integrity	Confidentiality	Availability
K_u-band	0.1	0.1	0.1
C-Band	0.1	0.5	0.5
WiFi a	0.1	0.9	0.9
WiFi b	0.1	0.9	1
WiFi g	0.1	0.9	1
WiFi n	0.1	0.9	0.9
No encryption	0	0.9	0
No signature	0.9	0	0

C. SENSORS

Sensors may be classified according to the type of reference used. References can be external or internal. An external reference is e.g. a GPS satellite. INS on the other hand relies only on internal references of physical parameters, such as acceleration or angular rates.

To determine the risks of the individual sensor systems, the characteristics of the sensor, the importance of the aspect observed and the mechanisms to detect spoofed or false sensor values must be considered.

Sensors with external references are more susceptible to jamming and spoofing than sensors with internal references. External references generally impose a risk to the integrity of the system.

Sensors relying on internal references must cope with value drifts, a certain deviation from the correct value over time. This phenomenon is due to the lack of external synchronisation and inherent errors. Reliable coping strategies exist and an external synchronisation may additionally take place when appropriate. It is widely accepted, that internal reference systems impose no additional risk.

Aspects of the environment that are crucial to the correct execution of the mission must be observed correctly and reliably. If such an aspect is observed solely by a sensor with an external reference, a risk for the integrity and the availability of the system may emerge. An UAV relying on GPS-based navigation is prone to attacks on the GPS-sensors, which may be jammed or spoofed. In this case, due to the reliance on the external reference and the lack of control and coping mechanisms, the correct autonomous behaviour of the UAV cannot be guaranteed [7].

However, sensors observing non-critical aspects of the environment may also impose security threats. If the values delivered by the sensors are incorrect and other components rely on these values, the implications may be severe. Hence, all sensor data needs to be checked before used. Consequently, only optional sensors with reliable failure and attack detection mechanisms impose no additional risk for the integrity.

The redundancy mechanisms used to compensate sensor values may additionally contribute to the systems security. If several - but different - sensors are used to observe one aspect of the environment, the acquired values are considered more reliable. It is less likely that multiple, different sensors are jammed or spoofed collectively. Therefore, it may be concluded that single sensor observations impose an additional threat for the systems integrity. If one sensor observes a crucial value, such as flight attitude, this imposes a threat to the availability* of the system, as jamming or spoofing of this sensor may lead to the loss of the UAV.

The above observations lead to the risk assessment according to Table III.

The risk assessment must be done for each sensor in the UAV system as well as every observed mission aspect. Since depending on the mission, different aspects need to be considered and different aspects are critical, a mission specific sensor setup will provide better options to lessen the risk for the UAV system. Also the application of sensor fusion mechanisms, as described in [14], for cross-checking and enhancement may lessen the risk of integrity or availability loss.

Commonly combined sensor systems as GPS, INS, camera and radar will now be discussed based on the results of the general analysis.

INS is a traditional sensor to observe positional data and flight attitude for planes. INS is often paired with GPS as an additional sensor to acquire absolute position data. GPS relies on external references, creating +1 for integrity. However, a navigation system based on an INS and a camera system are combined to observe optical feature - see [15] - it poses no immediate security risk, even though the increasing deviation is still present. If all three systems are combined, jammed/spoofed GPS values are overruled by the INS and the optical features. This combined sensor system poses no additional security risk.

Table III. General sensor risk assessment, overview

Sensor system property	Integrity	Confidentiality	Availability
Sensor with external reference	0.9	0	0
Mandatory sensor with external reference	0	0	0.9
Mandatory sensor without redundancy	0.9	0	(0.9)*
Optional sensor without attack or fault detection	0.9	0	0

To control an UAV, awareness of the UAVs current situation is needed. This accounts to autonomous and human control. In current UAVs the situation awareness is created by camera or radar systems. The multiple camera system MTS-B that is used in the MQ9-Reaper consists of infrared, daylight and light enhancing cameras, which are automatically fused to provide an optimal image. This heterogeneous setup decreases the risk of jammed or spoofed sensor data due to cross-checking and mutual enhancement. Although it is theoretically still possible to jam the cameras, the used light would need to cover a wide frequency spectrum, making it impractical and unlikely.

The results of the sensor system discussion are shown in Table IV.

Table IV. Risk assessment results for different sensor combinations and mission aspects

Aspect	Sensor System	Integrity	Availability
Navigation	INS	0	0.9
Navigation	GPS	1.8	0.9
Navigation	INS + GPS	0.9	0
Navigation	INS + Optical Flow	0	0
Navigation	INS + GPS + Optical Flow	0	0
Flight Attitude	INS	0	0.9
Flight Attitude	INS + Optical Flow	0	0
Situation Awareness	Single Camera	0.9	0
Situation Awareness	Multiple Cameras	0	0

D. DATA STORAGE

The risk assessment of data storage mechanisms considers three main aspects:

1. Volatility
2. Encryption
3. Signature

The usage of volatile storage imposes a risk to the availability of the stored data. If appropriate coping strategies are lacking, this may also lead to an inconsistent storage state and hence result in a loss of integrity of the stored data. However, the sole use of volatile storage does not impose an additional risk to the confidentiality of the stored data.

The use of encryption mechanisms may preserve the confidentiality of stored data. The lack of encryption generally heightens the risk of confidentiality loss. Encryption mechanisms do not prevent the stored date from being overwritten, which implies a risk for data integrity. To secure the integrity, mechanisms such as signatures or forgery detection must be integrated. These mechanisms have no influence on the confidentiality or availability of the data.

Using the above considerations, the resulting observations are:

- The availability of the data is based on the volatility of the storage medium.
- Solid state storage imposes no risk on the availability, as it is considered robust.
- Hard drive based storage and magnetic tapes are susceptible to force and magnetic fields, resulting in a higher risk of data loss.
- Volatile memory such as RAM is considered to impose no risk for the confidentiality but may impose a risk of availability and integrity loss.

We considered magnetic tapes, hard drive storage, solid state storage and temporary storage through RAM. The risk assessment for the considered storage media is shown in Table V.

Table V. Risk assessment of common data storage media

Storage type	Integrity	Confidentiality	Availability
Analog magnetic tape	0.9	0.9	0.9
Hard drive based storage	(0.9)	(0.9)	0.9
Solid state based storage	(0.9)	(0.9)	0
RAM	0.9	0	0.9

The numbers in brackets imply that the actual value depends on the encryption and signature used and may be 0. The values converge to zero if the data stored is signed and encrypted using strong encryption mechanisms.

E. FAULT HANDLING MECHANISMS

Fault handling mechanisms are difficult to assess regarding their "usefulness" in terms of security aspects. Although it is obvious that a "good fault handling mechanism" should improve the systems overall security, it is not obvious what good fault handling mechanisms for UAVs are. This is a common research problem of UAVs.

UAVs are technical systems and prone to faults in all of their components. Faults create errors, unhandled errors lead to malfunctions and disrupt the mission. To prevent this, the emerging of faults must be prohibited or faults must be masked by appropriate fault handling mechanisms [16].

Examples for fault handling mechanisms are "triple modular redundancy" or "fail-safe states". These mechanisms may cause restrictions on the functionality of the UAV, but enable the continuation of the mission. However, the fail-safe state may impose new threats to the security if the state is chosen unwisely.

Consider the following example: An UAV which is controlled remotely through a communication link must switch into a fail-safe state if the communication link is lost. One possible fail-safe state is to maintain the current position until the communication link is restored. In this case the UAV needs to aviate based on its on-board sensors, making the impact of manipulated sensor data tremendous. An example of this type of attack is the GPS-signal spoofing [7].

To assess the threats imposed by the fault handling mechanisms of an UAV it is necessary to categorise the possible faults. A fine grained categorisation is discussed in [17]. We categorise security threats by severity of the fault and fault type (transient or permanent).

Transient faults are often external temporary disturbances, such as communication interferences due to weather conditions. Permanent faults are mainly hardware damages.

The risk assessment of fault handling mechanisms in UAVs considers transient and permanent mission critical fault handling mechanisms and analyses their implications on integrity, confidentiality and availability.

Different fault-handling strategies for mission critical faults exist, examples are “self-destruct”, “automatic-return”, “land” and “hover”. Not all strategies may be equally appropriate for all faults [18].

The possible fault handling mechanisms for severe faults of general UAV components are shown in Table VI.

The “hover” strategy requires working avionics and navigation. For transient faults “hover” provides the ability to continue the mission after recovery. However, due to possibly limited sensor and communication facilities the UAV is more likely to be attacked through spoofed or manipulated data. This invokes threats to the integrity of the mission.

The “automatic-return” strategy provides the best chance of retrieving a functional UAV, but it imposes the same risks as the “hover” strategy.

Table VI. Component-dependent fail-safe states

Component	Fault handling mechanism
Base system	self-destruct
Data Storage	land, self-destruct, (automatic-return)
Sensors	hover, (automatic-return), land, self-destruct
Communication	hover, automatic-return, land, self-destruct
Avionics	Land, (automatic-return), self-destruct

The “land”-strategy needs a minimal set of working components and is also applicable in the case of engine failure. However, in enemy territory it imposes a risk on integrity and confidentiality.

The “self-destruct” strategy has the lowest risk of misuse or exposure of sensitive data, but it destroys the availability of any UAV component or data.

The deduced risk assessment values are shown in Table VII.

Table VII. Fail-safe state risk assessment results

Strategy	Integrity	Confidentiality	Availability
Hover	0.9	0	0
Land	0.9	0.9	0.9
Automatic-return	0.9	0	0
Self-destruct	0	0	0.9

The risk assessment shows that the security aspects are hardly compatible. This implies that fault handling mechanisms should be adapted to the preferred security aspect.

5. RESULTS

This section presents the results of applying the described scheme to modern UAVs.

A. AR.DRONE

The parrot AR.Drone is a remotely controlled quadrocopter originally designed for augmented reality video games. Meanwhile, the AR.Drone is commonly used as a research platform [19]. Apart from research institutions, the AR.Drone was also used during the "occupy wall street" actions to realise a robust police reconnaissance system [20].

The basic hardware setup incorporates a single IEEE 802.11b/g [21] compatible wireless communication link and an android or IOS based smartphone as GCS. The antenna is omnidirectional and the link is usually not encrypted.

Apart from RAM (used to buffer video streams), the AR.Drone does not possess any storage media. It contains two video cameras, an ultra-sonic range finder, a low-altitude altimeter and an INS as sensory equipment.

The fault handling mechanism in case of an error of the communication link is to enter the hover mode. Every other error results in instantaneous landing manoeuvres (land mode).

The results of our risk assessment for the AR.Drone are shown in Table VIII.

Table VIII. AR.Drone risk assessment results

Component	**Integrity**	**Confidentiality**	**Availability**
Communication links	1.1	2.7	2
Data storage	0.9	0	0.9
Sensors	2.7	0	0.9
Fault handling	1.8	0.9	0.9
Total	**6.5**	**2.6**	**4.7**

The sensor risk value results from the following observations: The used INS is accompanied by an optical flow measurement of the ground to track the position [15], which represents a checked mandatory sensor. The additional low-altitude distance sensor can be used to manipulate the flight height of the drone, which is a risk comparable to an unchecked mandatory aspect sensor with external reference. The cameras never overlap, prohibiting image cross-validation.

B. MQ-9-REAPER

The General Atomics MQ-9 Reaper is a remotely controlled UAV. It is the successor of the MQ-1 Predator. It uses the TCDL satellite communication system (SATCOM) as well as a direct LOS C-band communication.

The control of the UAV is done by a GCS. The default equipment of the UAV consists of several cameras bundled in a multi-spectral targeting system (MTS-B). These cameras detect infrared, daylight and intensive light. The data is automatically pre-processed and fused by the MTS-B. The navigational sensors are INS and GPS.

The MQ9-Reaper contains digital storage for video data. The encryption and signature mechanism are unknown.

The results of the risk assessment are shown in Table IX.

Table IX. MQ-9-Reaper Risk assessment results

Component	**Integrity**	**Confidentiality**	**Availability**
Communication links	0.2	0.6	0.6
Data storage	0.9	0.9	0
Sensors	0.9	0	0
Fault handling	0.9	0.9	0.9
Total	**2.9**	**2.4**	**1.5**

The communication system uses two independent links, which are both encrypted and signed.

The data storage is non-volatile, the encryption and signature methods used are unknown. For our calculations we presumed the worst-case-scenario; no encryption or signature methods.

The used camera system is redundant and uses fusion. The used combination of INS and GPS poses a risk for the integrity of the data as the GPS uses an external reference.

The accident described in [18] shows that the remote pilot must cope with permanent faults manually. Furthermore, the self-destruct mechanism is activated manually. This may lead to uncontrolled landings or flights and imposes threats to the availability, integrity and confidentiality of the system.

C. RQ-170 SENTINEL

Due to the current investigations of the Iranian claim to have attacked an RQ-170 Sentinel, publically available and reliable sources regarding the equipment of the RQ-170 are rare. The data available allows only a partial risk analysis of the UAV.

The sensory equipment of the UAV consists of infrared and daylight cameras as well as GPS and INS. The equipment is similar to the MQ-9-Reaper. The risk assessment of these sensors and the combinations are equal to the MQ-9. It is likely that the scores of the Sentinel are similar to the MQ-9-Reapers scores, if not better.

The data storage is non-volatile; the encryption and signature mechanisms are unknown. The communication link and the fault handling mechanisms are unknown.

6. CONCLUSIONS

The risk assessment of UAVs is a complex task consisting of vulnerability and threat analysis and is additionally dependent on mission details. The discussed UAV related incidents imply that risk assessment schemes for UAVs are lacking or insufficient.

The provided scheme is a first attempt to describe and formalise the risk assessment of UAVs. A component model of UAVs was designed to categorise and define a component-based risk assessment.

The components “communication system”, “data storage” and “sensor system” were analysed based on the used technology and known vulnerabilities. Environmental factors and fault handling mechanisms were additionally investigated. Security was defined following the definition in the 44 USC $ 3542.

The provided scheme was applied to the AR.Drone and MQ-9-Reaper. A brief risk analysis of the RQ-170 Sentinel was done, however the currently public available data is insufficient to draw any further conclusions. It appears that the RQ-170 Sentinel will at least score at the same rates as the MQ-9-Repear. However, depending on the further system setup, it is equally likely that this impression is false.

The calculated values give an indication of the susceptibility of the investigated UAV to attacks influencing availability, integrity or confidentiality.

Within this scope, risk was defined as the result of the susceptibility of an UAV multiplied by the probability of occurrence of a specific attack on a component's vulnerability, multiplied by the severity of the attack. It was shown that the risk assessment of an UAV is highly dependent on the assigned task/mission.

The described method is a first approach to a general scheme for the risk assessment of UAVs. The risk analysis and assessment of each of the named components describes an individual research area. This paper understands itself as a basic but crucial introduction to the risk assessment of UAVs in terms of structure, tactics and analysis.

REFERENCES

[1] Lolita C. Baldor, «Flashy drone strikes raise status of remote pilots,» *The Boston Globe*, pp. online at 01.11.2012: http://www.bostonglobe.com/news/nation/2012/08/11/air-force-works-fill-need-for-drone-pilots/ScoF70NqiiOnv3bD3smSXI/story.html, 2012.

[2] CNN Wire Staff, «Obama says U.S. has asked Iran to return drone aircraft,» 2011.

[3] Noah Shachtman, «Computer Virus Hits U.S. Drone Fleet,» *Wired*, pp. online at 01.11.2012: http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet, 2011.

[4] Cornell University Law School. [Online]. http://www.law.cornell.edu/uscode/text/44/3542

[5] Matt Bishop, *Introduction to Computer Security*, 1st ed., Addison-Wesley, Ed. Boston, USA: Pearson Education, 2004.

[6] Andrew Jaquith, *Security Metrics: replacing Fear, Uncertainty, and Doubt*, 1st ed., Addison-Wesley, Ed. Boston, USA: Pearson Education, Inc., 2010.

[7] Todd Humphreys, «Statement on the vulnerability of civil unmanned aerial vehicles and other systemes to civil gps spoofing,» Austin, 2012.

[8] David Cenciotti. (2011, December) The Aviationist. [Online]. http://theaviationist.com/category/captured-stealth-drone/page/2/

[9] US Air Force. (2007, November) United States Air Force. [Online]. http://usaf.aib.law.af.mil/ExecSum2008/MQ-1L_AOR_29Nov07.pdf

[10] US Air Force. (2007, December) United States Air Force. [Online]. http://usaf.aib.law.af.mil/ExecSum2008/MQ-1B_AOR_17Dec07.pdf

[11] British Broadcasting Corporation. (2009, December) BBC News. [Online]. BBC News: online at http://news.bbc.co.uk/2/hi/world/middle_east/8419147.stm

[12] Carl Young, *Metrics and Methods for Security Risk Management.*: Syngress Media, 2010.

[13] Erdal Torun, «UAV Requirements and Design Consideration,» in *RTO-MP-44*, Ankara, Turkey, 2000, pp. B4-1 - B4-8.

[14] D.L. Hall and J. Llinas, «An introduction to multisensor data fusion,» in *Proceedings of the IEEE*, 1997, pp. 6 -23.

[15] Pierre-Jean Bristeau, François Callou, David Vissière, and Nicolas Petit, «The Navigation and Control Technology Inside the AR.Drone Micro UAV,» in *18th IFAC World Congress*, Milano, Italy, 2011, pp. 1477-1484.

[16] Jane W. S. Liu, *Real-Time Systems*, 1st ed., Prentice Hall, Ed., 2000.

[17] Algirdas Avizienis, Jean-Claude Laprie, and Brian Randell, «Fundamental Concepts of Dependability,» Newcastle, 2001.

[18] US Air Force. (2009, March) United States Air Force. [Online]. http://usaf.aib.law.af.mil/ExecSum2009/MQ-9_FortIrwin_20Mar09.pdf

[19] Vojtěch Vonásek,Daniel Fišer,Jan Faigl Tomáš Krajník, «AR-Drone as a Platform for Robotic Research and Education,» in *Research and Education in Robotics - EUROBOT 2011*, Prague, Czech Republic, 2011, pp. 172-186.

[20] N. Sharkey and S. Knuckey. (2011, December) The Guardian. [Online]. http://www.guardian.co.uk/commentisfree/cifamerica/2011/dec/21/occupy-wall-street-occucopter-tim-pool

[21] IEEE, «IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,» *IEEE Std 802.11-2012*, pp. 1-2793, Mar 2012.

[22] Laurence R. Newcome, *Unmanned aviation: a brief history of unmanned aerial vehicles*. Michigan, USA: American Institute of Aeronautics and Astronautics, 2004.

[23] P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century.*: Penguin Books, 2009.

[24] Bill Yenne, *Birds of Prey: Predators, Reapers and America's Newest UAVs in Combat*. Pasadena, CA, United States: Specialty Pr, 2010.

[25] Ian Palmer, *Unmanned Aerial Vehicles: Robotic Air Warfare 1917-2007*. Essex, United Kingdom: Osprey Publishing, 2008.

[26] Kimon P. Valavanis, *Advances in Unmanned Aerial Vehicles*. Dordrecht, The Netherlands: Springer Netherland, 2008.

[27] Army UAS CoE Staff, «»Eyes of the Army» U.S. Army Roadmap for Unmanned Aircraft Systems 2010-2035,» U.S: Army UAS Center of Excellence, Fort Rucker, Alabama United States, 2010.

[28] J. R. Wilson, «A new generation,» *Aerospace America*, pp. 28-32, January 2007.

[29] T. J. Nugent and Kare J.T., «Laser Power for UAVs,» LaserMotive, Kent, WA United States, White Paper.

[30] Secretary of Defense, «Unmanned Systems Roadmap 2007 - 2032,» U.S. Department of Defense, Washington D.C., USA, Roadmap December 2007.

[31] John R. Vacca, *Computer and Information Security Handbook.*: Morgan Kaufman, 2009.

[32] Douglas L. Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments.*: Crc Pr Inc, 2011.