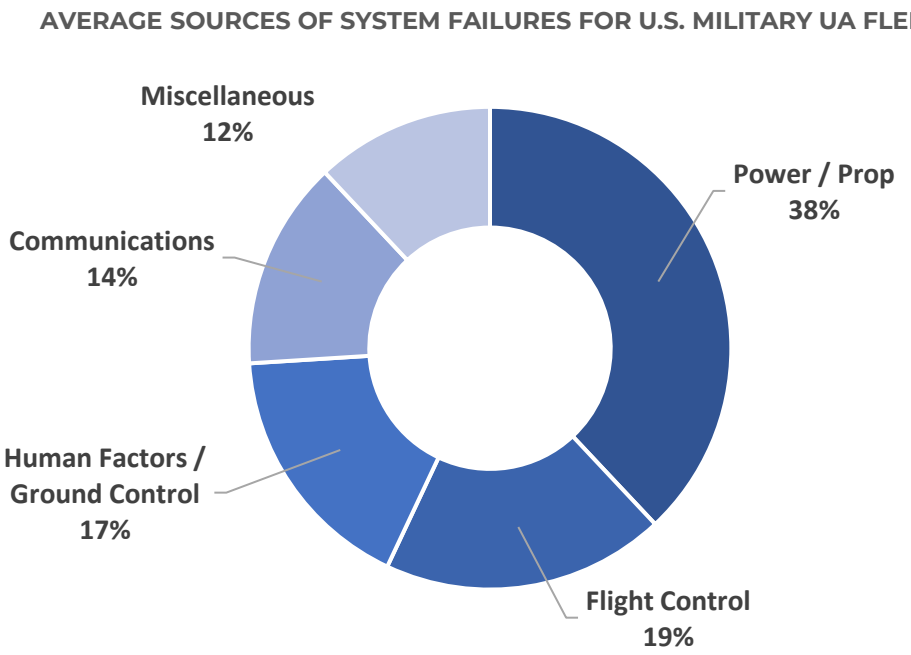
RELIABILITY SERIES 4 OF 5
DRONE CRASH CAUSES
#4 COMMS

In our last blog entry “Causes of UAV Loss” we explained what are the main causes of UAV losses and their relative occurrence.

The US Department of Defense document “Unmanned Aircraft Systems Roadmap 2005-2030” uses the following definitions to categorize areas of a system failure leading to mission aborts or cancellations.



- **Power/Propulsion (P&P)**.
- **Flight Control**.
- **Human Factors/Ground Control**.
- **Communications**. They consider only the data link between the aircraft and the ground
- **Miscellaneous**.

Now, let’s talk about cause #4, Communications

Cause #4: Communications

There are internal and external factors that cause a comms failure in a UAV

INTERNAL

Hardware-related

Radio
Failure

Antenna
Failure

Connectors
Failure

Electrical Power Source
Failure

EXTERNAL

Solar Flares
Solar flares are large explosions from the surface of the sun that emit intense bursts of electromagnetic radiation. They can disrupt Earth's magnetosphere and result in geomagnetic storms. Such geomagnetic storms can lead to auroras closer to the equator than is possible during calm conditions.

In 1989, a large solar flare accompanied a coronal mass ejection and hit Earth, plunging the entire province of Quebec, Canada, into an electrical blackout that lasted 12 hours, according to a NASA statement(opens in new tab). The solar eruption triggered a geomagnetic storm on Earth, resulting in aurora borealis, or northern lights, that could be seen as far south as Florida and Cuba. (https://www.space.com/solar-flares-effects-classification-formation)

Radio interference
From other radio transmitters or sources of electromagnetic disturbances nearby, like electric motors and powerlines.

Lightning
Lightning is a naturally occurring electrostatic discharge during which two electrically charged regions, both in the atmosphere or with one on the ground, temporarily neutralize themselves, causing the instantaneous release of an average of one gigajoule of energy. This discharge may produce a wide range of electromagnetic radiation. Lightning occurs commonly during thunderstorms as well as other types of energetic weather systems, but volcanic lightning can also occur during volcanic eruptions. Lightning discharges generate radio-frequency pulses which can be received thousands of kilometers from their source as radio atmospheric signals and whistlers, disrupting radio communications. (https://en.wikipedia.org/wiki/Lightning)

Jamming
Jammers work by blasting electromagnetic noise at the radio frequencies that drones use to operate and emit information. Effectively, they drown out the signal between a drone and its operator. This is usually either 2.4Ghz or 5.8Ghz, which are non-assigned, public frequencies. This

prevents jammers from interfering with manned aircraft, cell phones, public broadcasts, or other dedicated radio bands.

Jammers can either be stationary, mounted devices, or built into highly mobile, gun-like devices. (https://www.911security.com/knowledge-hub/counter-drone-technology/jammers-and-spoofers)

Spoofing
While jammers work by blocking RF frequencies, spoofers send fake GPS signals that mimic legitimate ones. Spoofers hijack a drone's communication link by emitting a counterfeit signal that the device reads as valid because it is the same frequency as the real signal.

The spoofer works by emitting a stronger counterfeit signal. The spoofer can cause a small delay between drone and controller; then, the spoofer emits a stronger false signal. The spoofer now has control over the device and can pilot the drone. The spoofer deceives the GPS receiver

GPS spoofing is hard to defend against if your UAS device is using GPS for flight control. GPS is a signal broadcasted from satellites. You can't add standard protection tools such as encryption and certificates to GPS satellite signals. (https://www.911security.com/knowledge-hub/counter-drone-technology/jammers-and-spoofers)

Signal Bounce
It creates an echo signal that confuses the autopilot.

Here are some examples of crashes due to comms failure (lost link)

Nov 11, 2011 Germany Heron-1 Mid-flight (lost link) Afghanistan

Afghanistan
In the political discussion about the purchase of armed drones, a large reconnaissance model of the Bundeswehr crashed. In Afghanistan, an unmanned Heron drone crashed into a mountain.

The connection with the ground station in Mazar-i-Sharif had previously been lost. "The reasons for the disconnection are still unknown and are now being investigated by specialists," said a spokesman for the Bundeswehr on request.

The incident happened on November 8th. A day later, the remains of the drone were sighted.

Full report at:
https://www.welt.de/wirtschaft/article121775327/Bundeswehr-Drohne-Heron-zerschellt-in-Afghanistan.html

Sept 18 2012 US Air Force MQ-1 Predator Mid-flight (lost link) Iraq

EXECUTIVE SUMMARY
ABBREVIATED AIRCRAFT INCIDENT INVESTIGATION
MQ-1B, T/N 03-0111
CENTCOM AOR
18 SEPTEMBER 2012

On 18 September 2012, at approximately 0926 Zulu (Z), the mishap remotely piloted aircraft (MRPA), an MQ-1B Predator, tail number 03-0111, operated by the 20th Reconnaissance Squadron (RS) at Whiteman Airforce Base (AFB), Missouri, crashed and was destroyed on impact in the Central Command Area of Responsibility. The 20th RS is assigned to the 432d Wing, Creech AFB, Nevada. At the time of the crash, the Mishap Crew (MC) was controlling the MRPA from Whiteman AFB. The MRPA was destroyed at an estimated loss of $4.4 million. There were no casualties, and there was no reported damage to any property at the crash site other than the MRPA itself.

The MRPA took off from a forward operating base at 0102Z. Prior to the MC taking control of the MRPA, there was difficulty with the satellite data link that allows the MRPA to communicate with its crew. However, the issue was resolved by resetting the connection to the MRPA and the mission proceeded. At approximately 0919Z the primary navigation system began to diverge from the secondary navigation system by approximately 0.1 Nautical Mile (NM), to a maximum divergence of 0.25 NM. Normally, these systems record the same or approximately the same, location for the MRPA. At 0921:53Z the MRPA satellite data link disconnected (known as “lost link”). In response, The Mishap Pilot ran the appropriate checklist but was unsuccessful in reestablishing the satellite link. At approximately 0926Z the MRPA impacted about 3.25 NM south-southwest from the point of “lost link”.

Full report at:
https://www.airforcemag.com/PDF/AircraftAccidentReports/Documents/2013/091812_MQ-1B_CENTCOM_AOR_full.pdf

Library:

We have found very illustrative the following documents or web pages:

US Department of Defense: Unmanned Aircraft Systems Roadmap 2005-2030.
Although old, this document shows an in-depth understanding of how drones started to become a core element in military operations, the implications of UAV reliability, the regulatory framework, and the future of UAV development. The full document can be found at:
https://irp.fas.org/program/collect/uav_roadmap2005.pdf

Drone Wars UK: Accidents Will Happen
Drone Wars published a dataset of just over 250 large military drone crashes that have taken place over the past decade (2009-2018). You can find the links and document here:
https://dronewars.net/2019/06/09/accidents-will-happen-a-dataset-of-military-drone-crashes/

Dedrone: Worldwide Drone Incidents
This page keeps a log of all reported drone-related incidents worldwide, from a small drone invading airport airspace to a drone trying to deliver drugs and phones into a prison yard. Here is the info:
https://www.dedrone.com/resources/incidents/all

George Slensky: Analysis of UAV Military Aircraft Mishaps
Mr. Slensky analyses the main causes of US military aircraft both, manned and unmanned.
https://www.researchgate.net/publication/327135551_Analysis_of_UAV_Military_Aircraft_Mishaps