

Industrial Plant Monitoring

TRAN Trung Duc

October 20, 2020

Contents

| | | |
|----------|---|----------|
| 1 | Introduction | 3 |
| 2 | Summary | 3 |
| 3 | Operation description | 3 |
| 3.1 | Organization overview | 3 |
| 3.1.1 | Safety and Cyber-security | 3 |
| 3.1.2 | Design and Production | 3 |
| 3.1.3 | Screw Training | 3 |
| 3.1.4 | Maintenance | 4 |
| 3.1.5 | Crew | 4 |
| 3.1.6 | UAS Configuration Management | 4 |
| 3.2 | Operational procedure description | 5 |
| 3.2.1 | Standard operating procedures | 5 |
| 3.2.2 | Abnormal operation and emergency procedures | 6 |
| 4 | UAS description | 7 |
| 4.1 | Ground Station | 7 |
| 4.1.1 | Ground control station computer | 7 |
| 4.1.2 | Joystick 1 | 7 |
| 4.1.3 | Fail-safe button | 7 |
| 4.1.4 | Module Com 1 & Com 2 module | 8 |
| 4.1.5 | Package | 8 |
| 4.1.6 | Video screen | 8 |
| 4.1.7 | Joystick 2 | 8 |
| 4.1.8 | Com 3 module | 8 |
| 4.2 | Aircraft | 8 |
| 4.2.1 | Autopilot | 8 |
| 4.2.2 | Fail-safe module | 8 |
| 4.2.3 | GPS modules | 8 |
| 4.2.4 | Com 1 & Com 2 modules | 9 |
| 4.2.5 | Package | 9 |
| 4.2.6 | Power board | 9 |
| 4.3 | Communication | 9 |
| 4.3.1 | Com 1 & Com 2 | 9 |
| 4.3.2 | Com 3 | 9 |
| 4.4 | Supplemental Cybersecurity features | 9 |
| 4.4.1 | Autopilot software integrity | 9 |

1 Introduction

2 Summary

a Modifier - add image- shorter

In order to monitor a nuclear power plant, the electricity company will use a UAS equipped with a thermal camera. The UAS will be deployed to make flights around the plant which locates in a rural zone. The drone does not fly across the plant and keep the distance of 200m from the plant. There is not any airport near the inspected area. The drones is 30 kg with the maximum dimension of 2m is designed to fly automatically and beyond visual line of pilot during the whole operation at 30m above the ground.

During the flight, the pilot observes the status of the drone and the highway in real time via the GCS computer. The pilot needs to carry out only three simple actions: start the flight, end the flight (back to stand by mode), go home. The data exchanged between the GCS and the aircraft is transmitted via a wireless communication system.

The aircraft is equipped with a video camera with the characteristics as follows:

- Resolution: 1920 x 1080
- Min. Angle of view: 140 degree.

The aircraft is equipped with a thermal camera with the resolution of 640 x 640 px

3 Operation description

3.1 Organization overview

a Modifier - add management for security The highway company is the operator of the UAS operation. In the company, the UAS will be operated by a team of 2 people:

- A pilot is in charge of observing and controlling the flight via the GCS computers.
- The second pilot is in charge of carrying out vehicle preparation before the flight, visual observation during takeoff and landing moment. During the flight, the she/he observes the nuclear power plant via the GCS computers.

3.1.1 Safety and Cyber-security

a Modifier

The Safety Management System have not been integrated into the the organization.

3.1.2 Design and Production

The highway company is not responsible for the design and/production of the UAS. The UAS is designed and produced by SOGILIS company and its partners.

3.1.3 Screw Training

- The two crews are trained by the manufactures to operate the system in the normal, abnormal and emergency situation.
- The two crews have training in general knowledge and competence adequate for the operation (UAS regulation, UAS airspace operating principles, Airmanship and aviation safety, Meteorology, Navigation/Charts, UA knowledge, operating procedures).

3.1.4 Maintenance

- The maintenance of the system is carried out by the manufacturer - SOGILIS.
- The maintenance instructions, maintenance schedules and maintenance procedures are defined and documented by the manufacturers.
- The maintenance log system is used to record all maintenance activities conducted.
- All maintenance staff have undergone a training program defined by the manufacturers.

3.1.5 Crew

The UAS is operated by a team of 2 crews: pilot and support staff. The duties and responsibilities of each crew are described as follows:

Pre-flight

- In the pre-flight phrase, the pilot is in charge of starting the system and checking for any anomaly of GCS, autopilot, communication, sensors values, batteries, aviation chart via GCS and verifying the weather condition. The checking is logged in a document
- In the pre-flight phrase, the second pilot is in charge of visually checking for any damages, wears or tears; deploying the system in the takeoff area; verifying that the takeoff area is clear. The checking is logged in a document.

Flight

- After checking for any anomalies via the GCS, the pilot starts the flight by sending taking-off command to UAV via GCS. The pilot observes the status of flight and the feedback video. In case of emergency situation, the pilot is in charge of deciding whether or not to continue the flight (by getting UAV back to the pre-determined site or letting the UAV drop).
- In the flight phrase, the second pilot is in charge of observing the nuclear power plant. In case of an emergency situation, the second pilot in charge of carrying out any necessary actions on the field to ensure the safety of the plant and revoke the equipment (e.g call the guardians).

Post - flight

- After the flight, the pilot turns off the UAV. The pilot is in charge of carrying out the post analyses of the data stored on the GCS.
- After the flight, the second pilot checks for any damage, wear or tear before taking the UAV back to store. The support staff is in charge of carrying out the post analyses of the data stored on the UAV.
- Both the pilot and the second pilot are in charge of completing the post analysis report and report any technical anomalies to the manufacturer.

3.1.6 UAS Configuration Management

a Modifier

Any changes to the hardware and the software(parameter configuration, flight plan modification, software update) are designed or created by the manufacturer.

Any changes to the UAS are carried out by the manufacturer. The instructions and equipment for this task are defined and documented by the manufacturer.

The log system is used to record all changes conducted on UAS.

3.2 Operational procedure description

a Modifier

To observe the nuclear power plant, the owner company deploy a unmanned aircraft. The aircraft will fly around the plant.

The drone of 30kg is designed to fly automatically and beyond visual line of pilot during the whole operation at 30m above the ground. The flights is made inside a predefined geographic zone of 100 large around the plant (geo-fencing). The distance between the flight zone and the plant is 200m. **a Modifier-** add image

During the flight, the pilots could observe the status of the drone and the plant via the GCS computers. The pilot could perform only three simple actions: start the flight, end the flight (back to stand by mode), go home.

3.2.1 Standard operating procedures

Pre-flight procedures

Operating site location : The flight area (sky and land) is checked in order to ensure that a safety flight could be carried out:

- Other aircraft operations: Check to see if there are any other aircraft operations within the immediate vicinity such as local aerodromes, sky diving sites etc.
- Public Access: Is there any public access to the site and surrounding areas? What is the likelihood of encountering a member of the public?
- Weather conditions: The weather will be checked on the day of the flight as well as when the pilot arrives on site. If at any time the pilot feels that the weather could jeopardise the safety of the flight he has the right to cancel/abort the operation.
- Pre-notification: it will be necessary to notify any nearby Aerodrome and aircraft operating sites or the local police of any operations that we are undertaking. If the flight is being conducted in or near Aerodrome traffic then notification must be given before the event to ensure that the flight won't have an impact on the operations of said Aerodrome.

Preparation and correct assembly of UAV : the UAVs are unpacked from the store and set up in accordance to the manufacturer's instructions.

Pre-flight checks on UAS and equipment Once the UAV has been unpacked and assembled, the support staff will give the device one final check before the flight to confirm that there are no defects that were missed or that were caused during transit or conservation. Then the pilot starts the GCS and checks the value of displayed parameters, flight map for any anomalies. These checks are defined in a checklist provided by manufacturer.

Flight procedures

Take-off

Once all the pre-flight checks have been completed, the pilot starts the flight by pushing the 'takeoff' button on GCS. Receiving the command of the pilot, the UAV automatically takes off and fly up to the altitude of 30m.

During takeoff, the UAV is observed by both the pilot and the support staff.

In-flight

After reaching up the 30m altitude, the UAV follows the predefined trajectory in order to capture the video of highway.

The pilot concentrates on monitoring the flight status (attitude, altitude, batteries, position) and monitoring the high-way.

The support staff concentrate on visually monitoring the flight on the field.

Landing

Once the predefined trajectory is completed, the UAV goes back the landing site and hover over ground at 150m. Then it automatically lands on the ground. Once the landing is completed, the pilot pushes the 'dis-arm' button in order to turn off all the motors. Then the support staff turn off the power of the UAV.

During landing, the UAV is observed by both the pilot and the support staff.

Post-flight

Once a flight has been completed the time of flight must be logged. This will include the start and end times of the flight and the duration. Also any incidents must be noted and logged.

Then the UAV is inspected for signs of wear and tear or damage. If any is found it must be recorded.

All the flight data and video data stored on the UAV will be downloaded.

All flight data (store on the GCS and the UAV) will be analyzed by the pilot and the support staff. Any incidents must be noted, logged and reported to the manufacturer.

3.2.2 Abnormal operation and emergency procedures

Malfunctions

If any malfunction (communication, sensor, battery, controller,etc) is detected on the UAV then steps must be taken to immediately land the device safely at one of the designated landing sites. If the malfunction make a controlled landing is unavailable, the pilot must shutdown all motors and let the UAV drop within flight zone. In order to protect the people on the ground and the aircraft, the aircraft is equiped with a parachute which could be automatically or manually deployed.

A list of possible malfunction and necessary procedures are documented and provided by manufacturer.

Lost of control

In the case that the aircraft is totally lost of control and the auto fail-safe function is failed, the pilot could stop the operation manually by push the fail-safe button.

Change in Weather

During the flight the weather must be monitored at all times. If the pilot feels that rain or snow is imminent then he will take steps to return the UAV to the designated landing zone

Fire

In the event of smoke or fire coming from the UAV the pilot must immediately return to the landing zone to assess the cause and severity of the incident. In the case of damage or fire to the battery a fire blanket must be used to cover the UAV and control the fire

Designated Landing Area Compromised

In the event that the designated landing area is compromised the pilot will land the UAV at the secondary site. If both sites are compromised the support staff will try to clear the obstruction to allow the pilot to safely land

4 UAS description

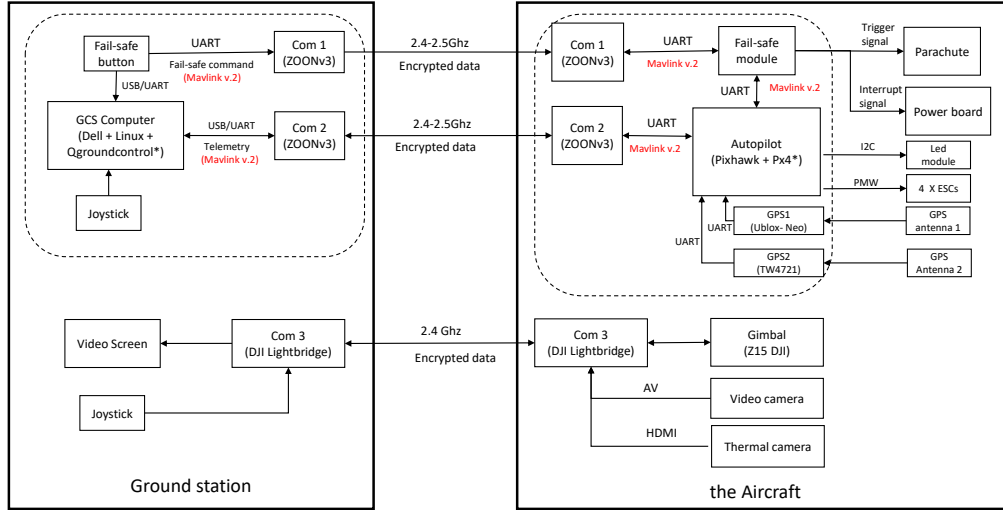


Figure 1: UAS Architecture

4.1 Ground Station

4.1.1 Ground control station computer

The GCS computer is a DELL laptop installed the Linux operation and the Qgroundcontrol. The Linux operation provide a basic **access control** service. To access to the computer, the pilot has to have a account (identification + password). The Qgroundcontrol is a open-source GCS software. This software provide a user interface that allow the pilot to control and monitoring the status of the aircraft. The Qgroundcontrol is set up with the mavlink v2 communication protocol. GCS computer communicate with the aircraft via the Telemetry communication link - Com 2 (see 4.3). The Qgroundcontrol software is modified to provide the supplemental cybersecurity functions presented in 4.4.

4.1.2 Joystick 1

The Joystick 1 provides pilot a measure to control manually the aircraft. The output of the joystick is sent to the aircraft via the GCS computer. The joystick connects to the GCS commputer via a USB port.

4.1.3 Fail-safe button

In the case that:

- the aircraft fail to trigger automatically the fail-safe function
- and the pilot could not also trigger manually this function via the joystick/ GCS computer

The fail-safe button provide the pilot the final measure to trigger the fail-safe button. The output of the fail-safe button is sent to the aircraft via a emergency communication link - Com 1 (see 4.3)

4.1.4 Module Com 1 & Com 2 module

See more detail in (see 4.3)

4.1.5 Package

The GCS computer, joystick and fail-safe button and 2 communication module is packaged in a solid box to hide every unused connection ports.

4.1.6 Video screen

A screen is used to display the video recored by on-board camera.

4.1.7 Joystick 2

The joystick 2 provides the pilot a measure to control the cameras

4.1.8 Com 3 module

This module is a part of the communication link to stream the video from the aircraft to the ground. (see 4.3)

4.2 Aircraft

4.2.1 Autopilot

The autopilot includes the a pixhawk-based autopilot hardware and a Px4-based autopilot software. The autopilot hardware includes:

- Main FMU Processor: STM32F765 32 Bit Arm Cortex-M7, 216MHz, 2MB memory, 512KB RAM
- IO Processor: STM32F100 32 Bit Arm Cortex-M3, 24MHz, 8KB SRAM
- On-board sensors: 2 x Accel/Gyro: ICM-20689 & BMI055
- Magnetometer: IST8310
- Barometer: MS5611

The autopilot software provides the aircraft the capacity of flying at auto mode and all required fail-safe functions.

In comparison with the original version, the autopilot is modified to provide the supplemental cybersecurity functions presented in 4.4.

4.2.2 Fail-safe module

The fail-safe module is used to trigger the parachute and the cut-off the motor power in case of emergency.

In the fail-safe case, the fail-safe module shall receive the command from

- Autopilot
- or the fail-safe button on the ground via Com1

When receiving the fail-safe command, the fail-safe module shall send :

- “Trigger” signal to the parachute
- “Interrupt” signal to the power board (see ??) to cut off motor power.

4.2.3 GPS modules

The aircraft is equipped with two different GPS modules : Ublox Neo and TW4721. This configuration create a redundancy for the safety of flight.

4.2.4 Com 1 & Com 2 modules

See more detail in (see 4.3)

4.2.5 Package

The Autopilot, 2 communication modules, the fail-safe module and 2 GPS modules is packaged in a solid metal box to hide every unused connection ports.

4.2.6 Power board

It distributes the electricity power from the battery to the motors and the electronic components.

In the fail-safe case, it shall cut-off the motor power.

4.3 Communication

4.3.1 Com 1 & Com 2

The communication link 1 (Com 1) is used to send only the fail-safe command to the aircraft. The communication link 2 (Com 2) is for telemetry data. For these communication links, the ZOONv3 modules is used. The specification of these module is described as follows:

- Range: 6km - 21km
- Frequencies: 2.4-2.5Ghz
- Dataspeed: 0.5-256Kbps
- Encryption: ChaCha2.0
- Mavlink compatibility
- Tolerance to the decrease of the ommunication performance

4.3.2 Com 3

The communication link 3 is used for streaming video. The DJI Lightbridge is used for this link.

4.4 Supplemental Cybersecurity features

4.4.1 Autopilot software integrity

For each time the parameters of autopilot or the source code of the autopilot are changed, the autopilot will create a encrypted hash of the source code and the parameters. This hash will be sent and stored in the GCS.

When started, the autopilot generate a encrypted hash of the current source code and the current parameters. This hash shall be sent to GCS and compared with the hash stored in the GCS.