

Temasek Defence Systems Institute

Feasibility Assessment for Secured Vehicle Teleoperation via the Public Cellular Network

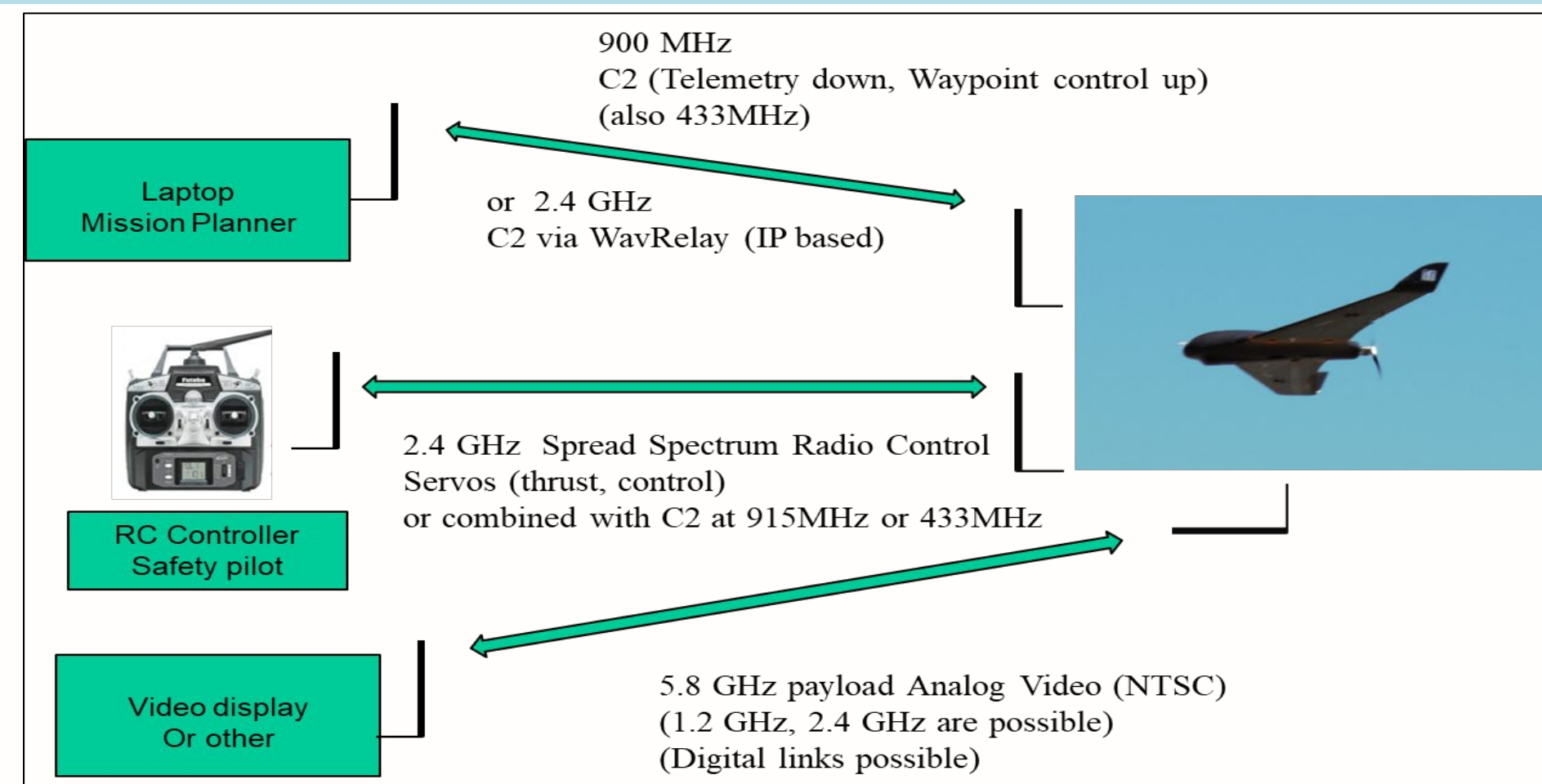
Author: ME5 Siritape Teo, Republic of Singapore Air Force (RSAF)

Thesis advisor: Dr David R. Jacques, Air Force Institute of Technology (AFIT)

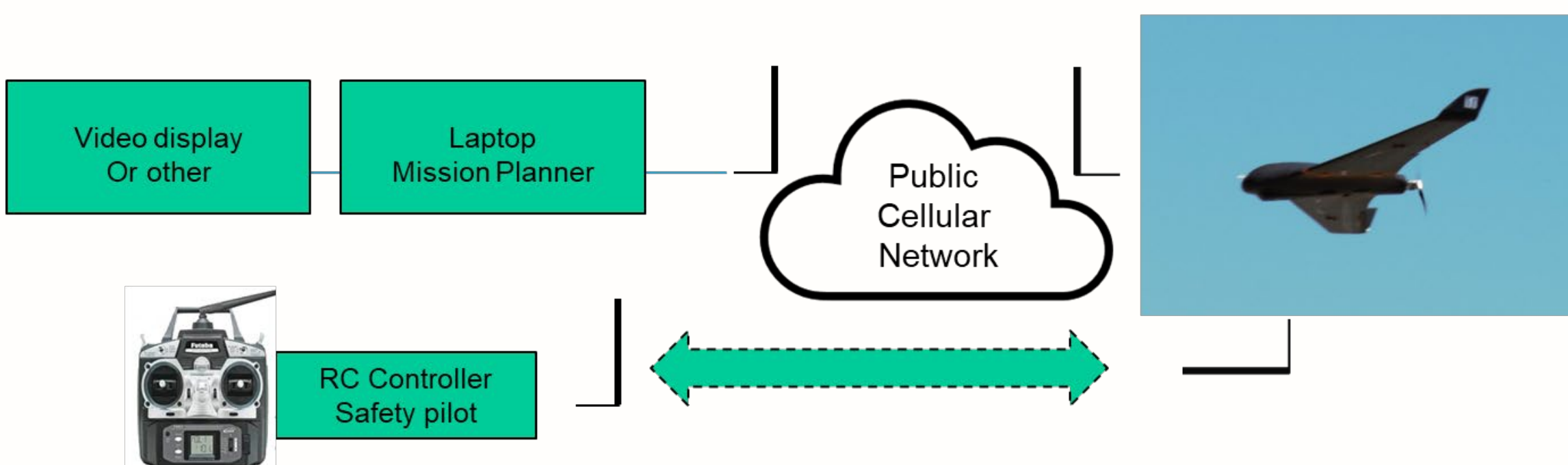
Background

In United States Air Force (USAF), Unmanned Aircraft System (UAS) uses dedicated radio-frequency communications systems to transmit and receive data wirelessly between the air vehicle and ground station, for cyber security reasons. UAS's operating range depends on considerations such as:

- Competition for radio-frequency bands;
- Datalink Interferences and Losses;
- Communications hardware's Size, Weight & Power (SWaP).



Possible Future for UAS Operation



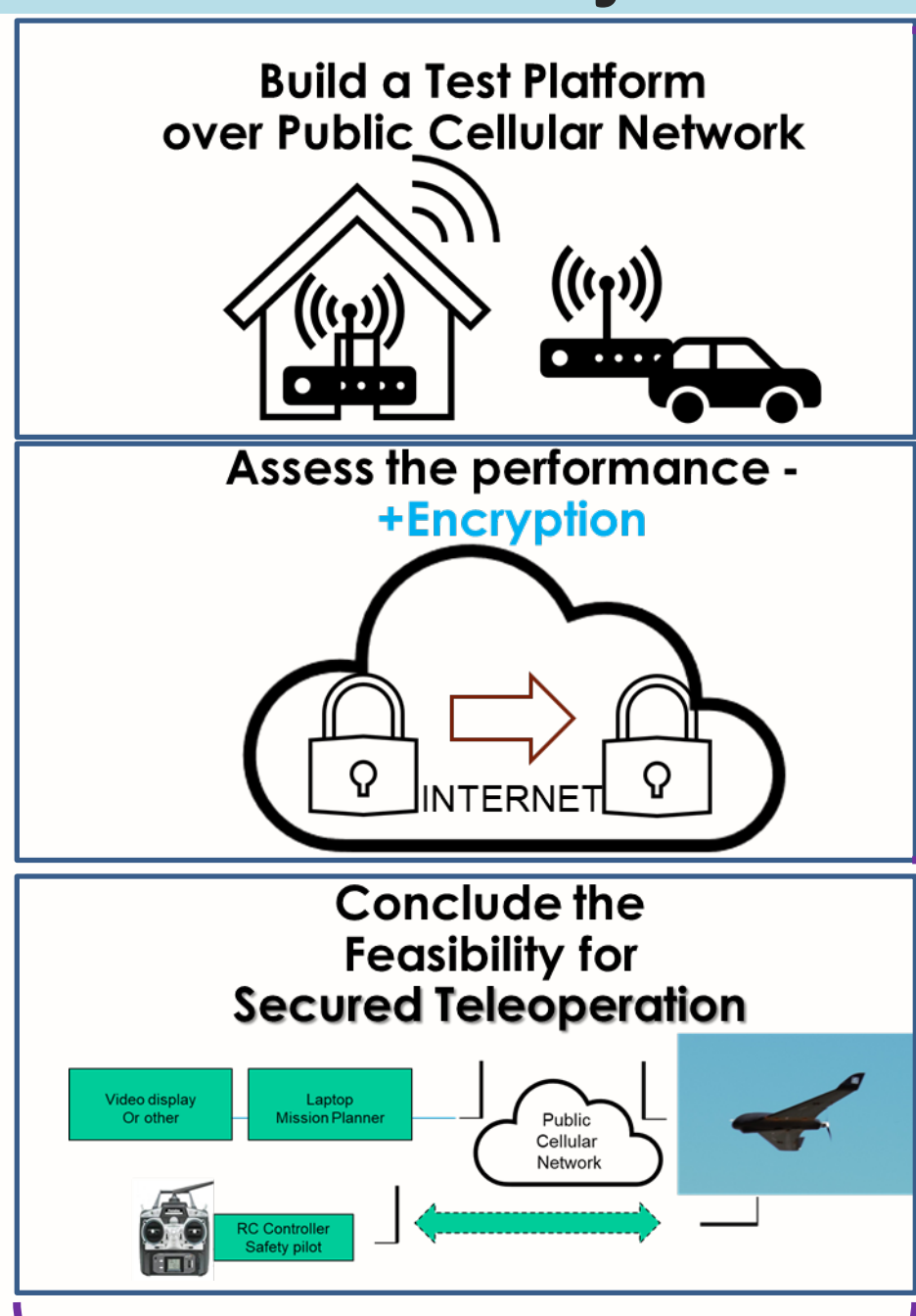
Problems

- Cyber Security on Datalink
- Latency over transmission

Commercial unmanned systems have realised Teleoperation via the 4G/5G network.

For feasibility over defence/homeland security applications: (1) Cyber Security on datalink; and (2) Latency, has to be thoroughly investigated.

Research Objectives



Key Interpretations

- True Teleoperation not feasible with secured datalink.
- > Video is useful for beyond Line-of-Sight (LOS) situational awareness - Latency <500msec via Web Real-Time Communications (WebRTC)
- > Telemetry Latency is near real-time if using 5G network
- Limited use of cell network for secured datalink still possible.

Test & Instrumentation Set-ups

