VSTAR SYSTEMS INC.

UAV CYBER SECURITY

INCOSE

Andy von Stauffenberg

Agenda

VSTAR SYSTEMS INC.

- VStar Systems Overview
- What is Cyber Security?
- UAV Overview
- Broad types of Cyber Attacks
- Remote Attacks
- Subsystem Attacks
- Suggestions
- References

About VStar

VSTAR SYSTEMS INC.

What we do?

VStar Systems Inc. is an unmanned systems integrator that creates innovative and effective solutions for Government and Commercial Clients.

Areas of Expertise

- Unmanned/Autonomous Vehicles
- Intelligence, Surveillance, Reconnaissance (ISR)
- Data/Communication Systems
- Command and Control (C2) Systems/Ground Stations
- Remote Sensing
- System of Systems/Distributed Systems
- Storytelling & Problem Solving

What is Cyber Security?

VSTAR SYSTEMS INC.

Definition:

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Why UAV Cyber Security?

VSTAR SYSTEMS INC.

- They 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.
- In the future, could (and will) be used for nefarious purposes.

UAV Overview

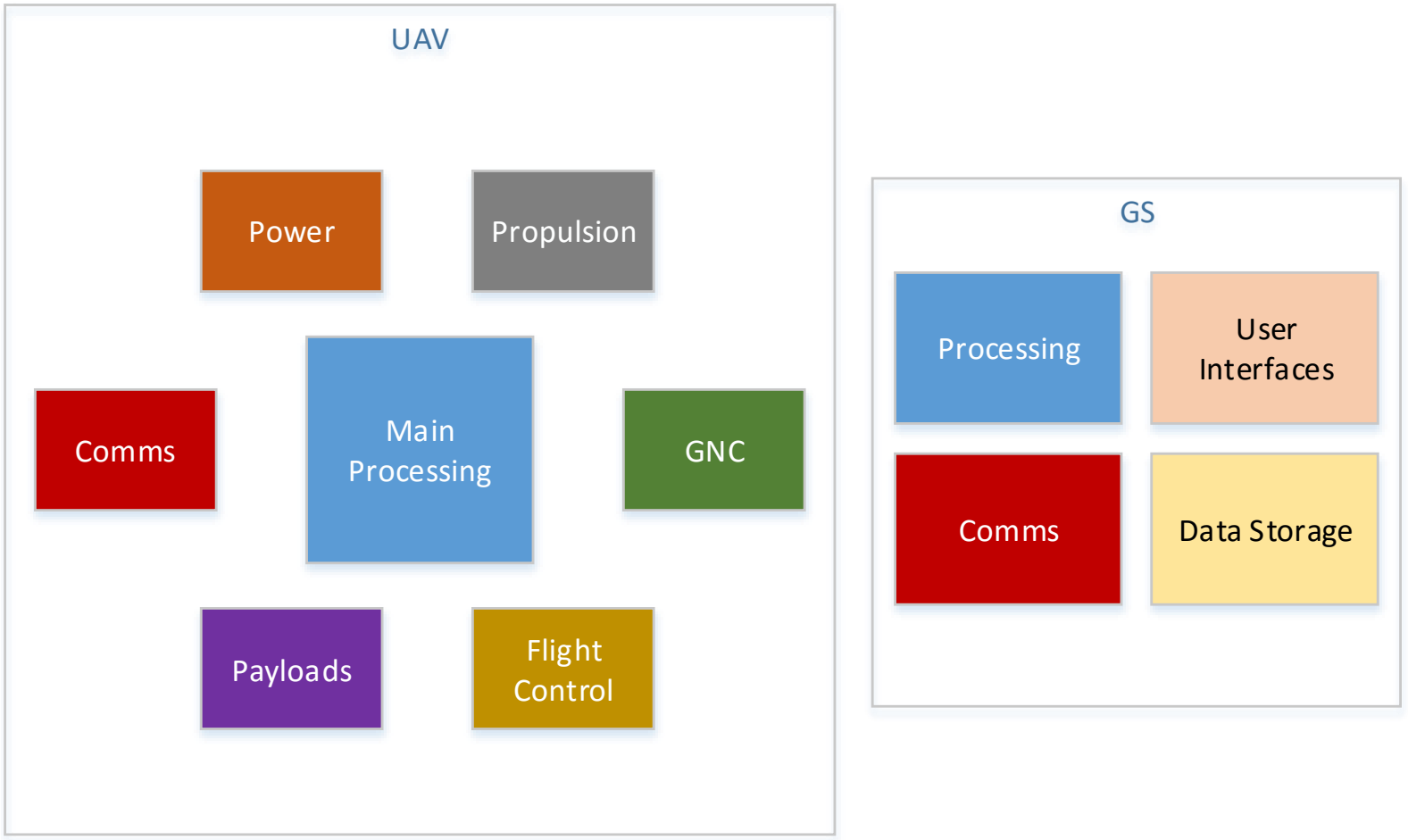
VSTAR SYSTEMS INC.

- Government
- Fire Fighting
- Energy Sector
- Transportation
- Agriculture, Forestry, Aquaculture
- Earth Observation
- Communication, Broadcasting
- Filmography, Photography

UAV's are becoming very common – need to think about Cybersecurity NOW!!

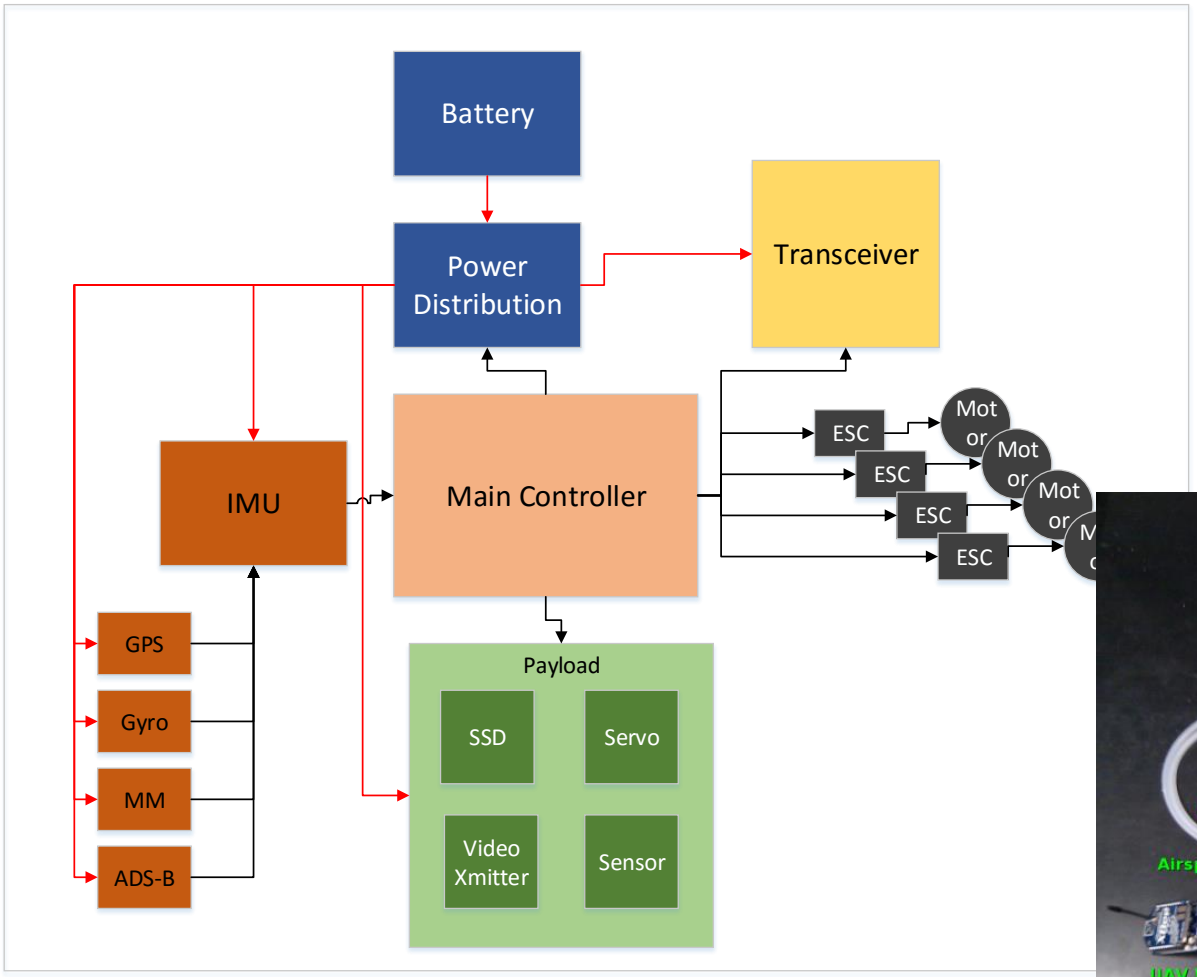
UAV System Overview

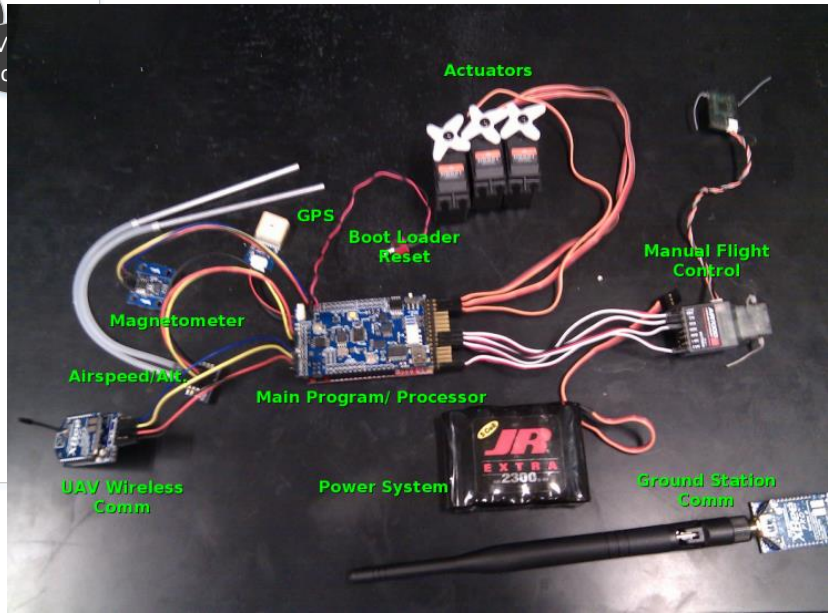
VSTAR SYSTEMS INC.



sUAV System Architecture

VSTAR SYSTEMS INC.



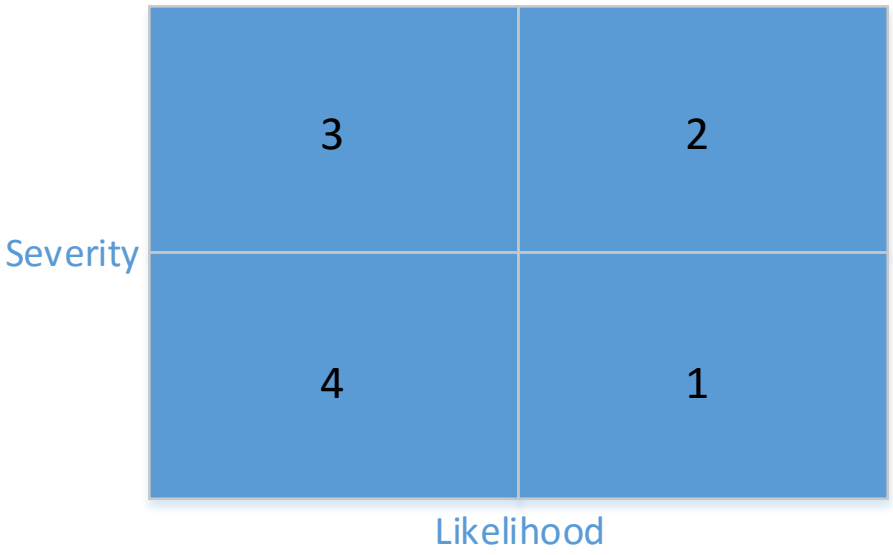


General Attacks

VSTAR SYSTEMS INC.

- Remote Attack (Wireless Attack or Sensor Jamming/Spoofing)
  - Attack through one of the sensor or comms channels
  - Easy, but single system infiltration
- Hardware Attack
  - Access to components directly
  - Harder to accomplish, but effect greater

Specific Attacks



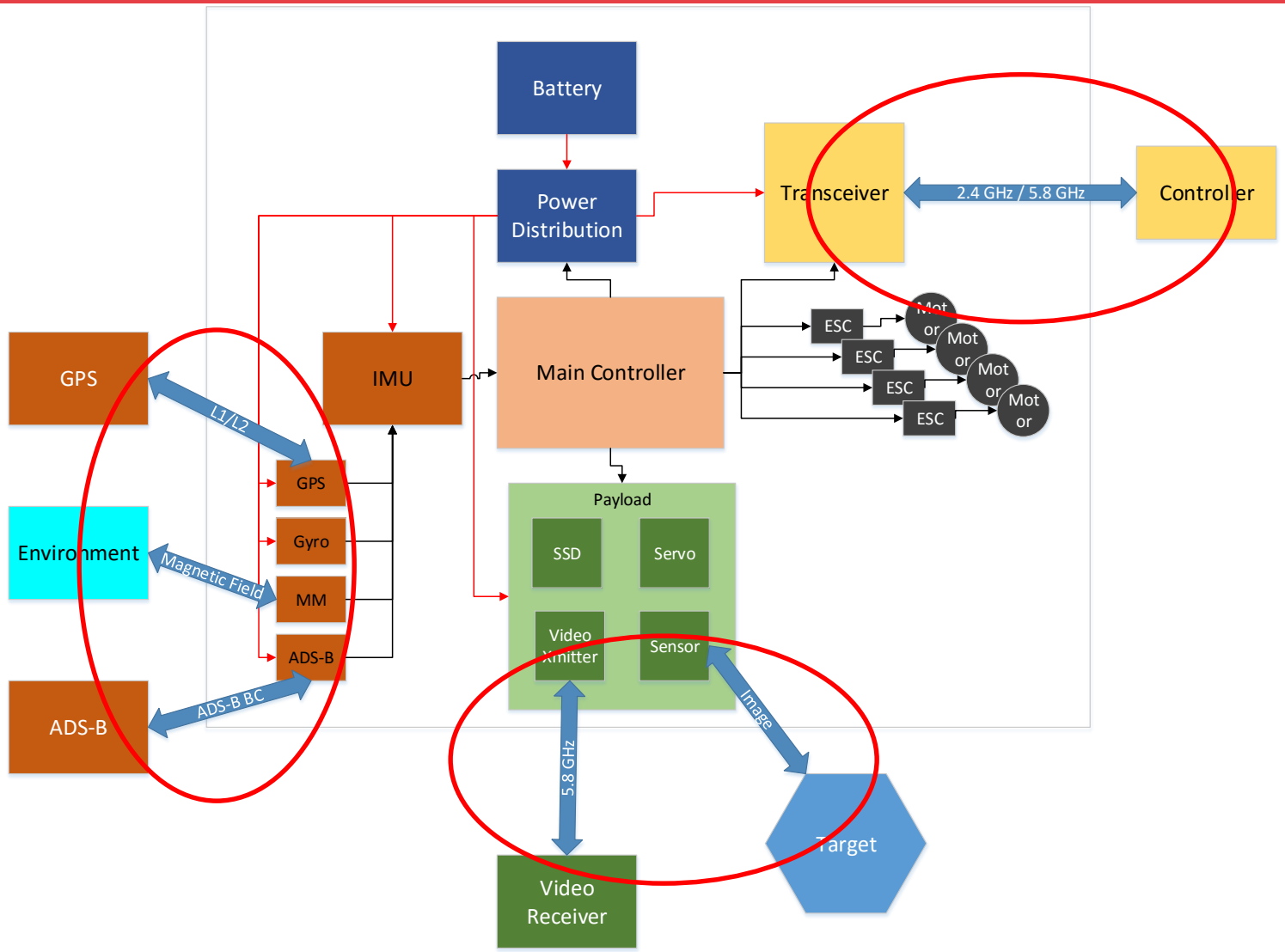
1. Payload/C2 Data Attack
   - “Stealing” Sensor Data
2. Direct Payload Attack
   - Temporary or Permanent damage to Payload
3. Control System Attack
   - Attacking the Control System SW or HW
4. Application Logic Attack
   - Altering data to the Control System

VSTAR
SYSTEMS INC.

Remote Attacks

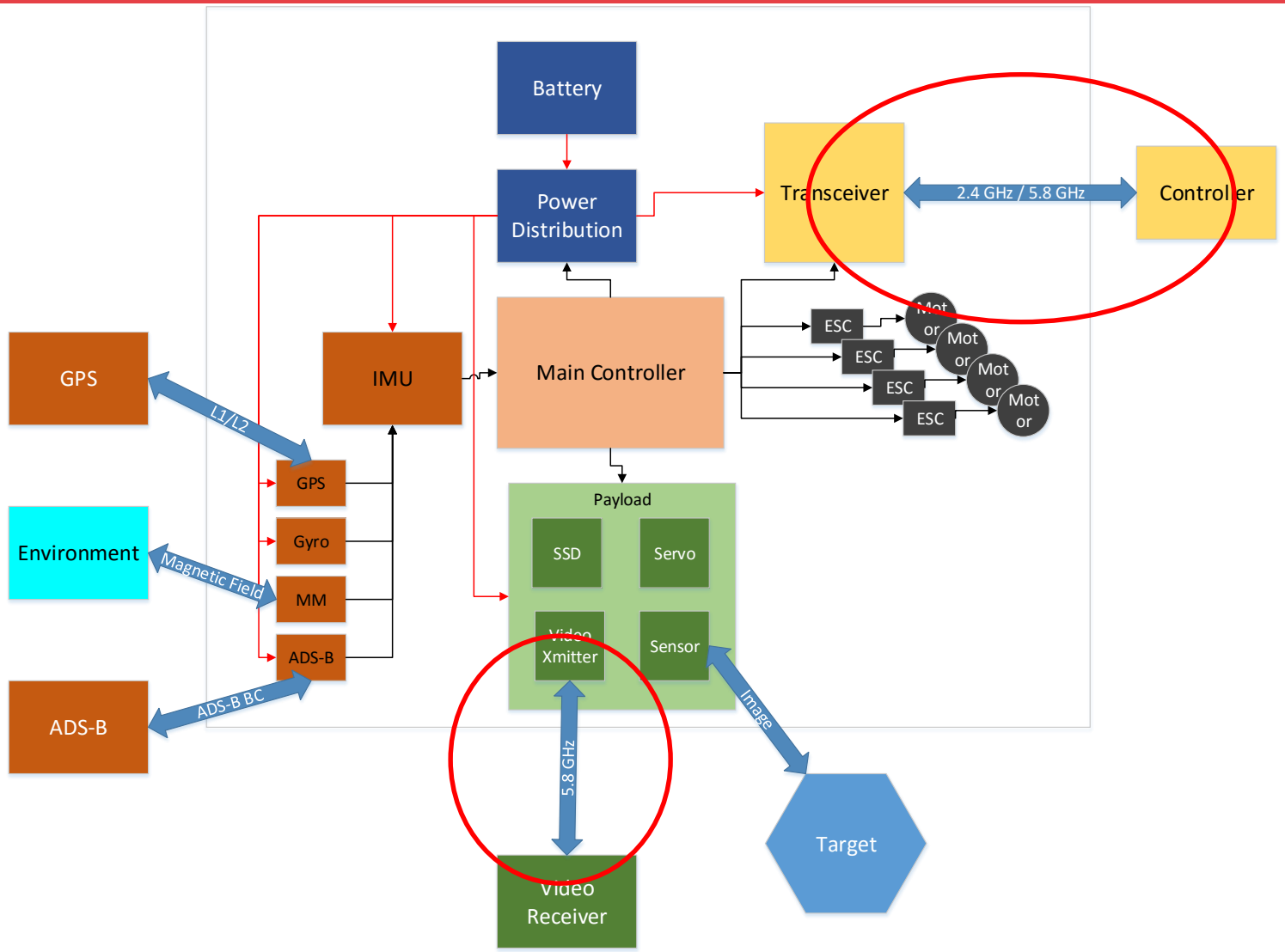
UAV External Interfaces

VSTAR SYSTEMS INC.

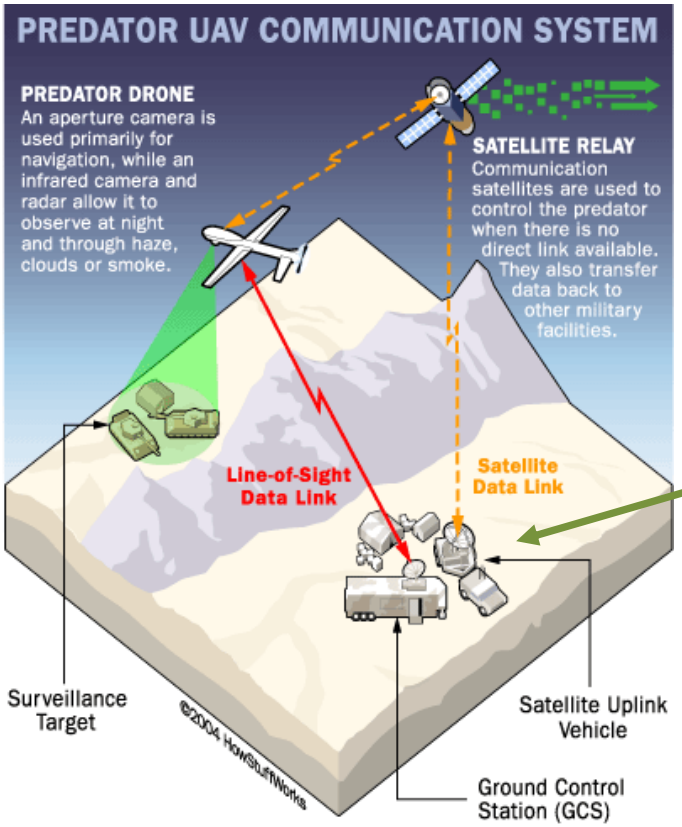


Payload/C2 Data Attacks

VSTAR SYSTEMS INC.



UAV Comms Architecture



DCGS

Difficult because different comms paths have different owners/stakeholders

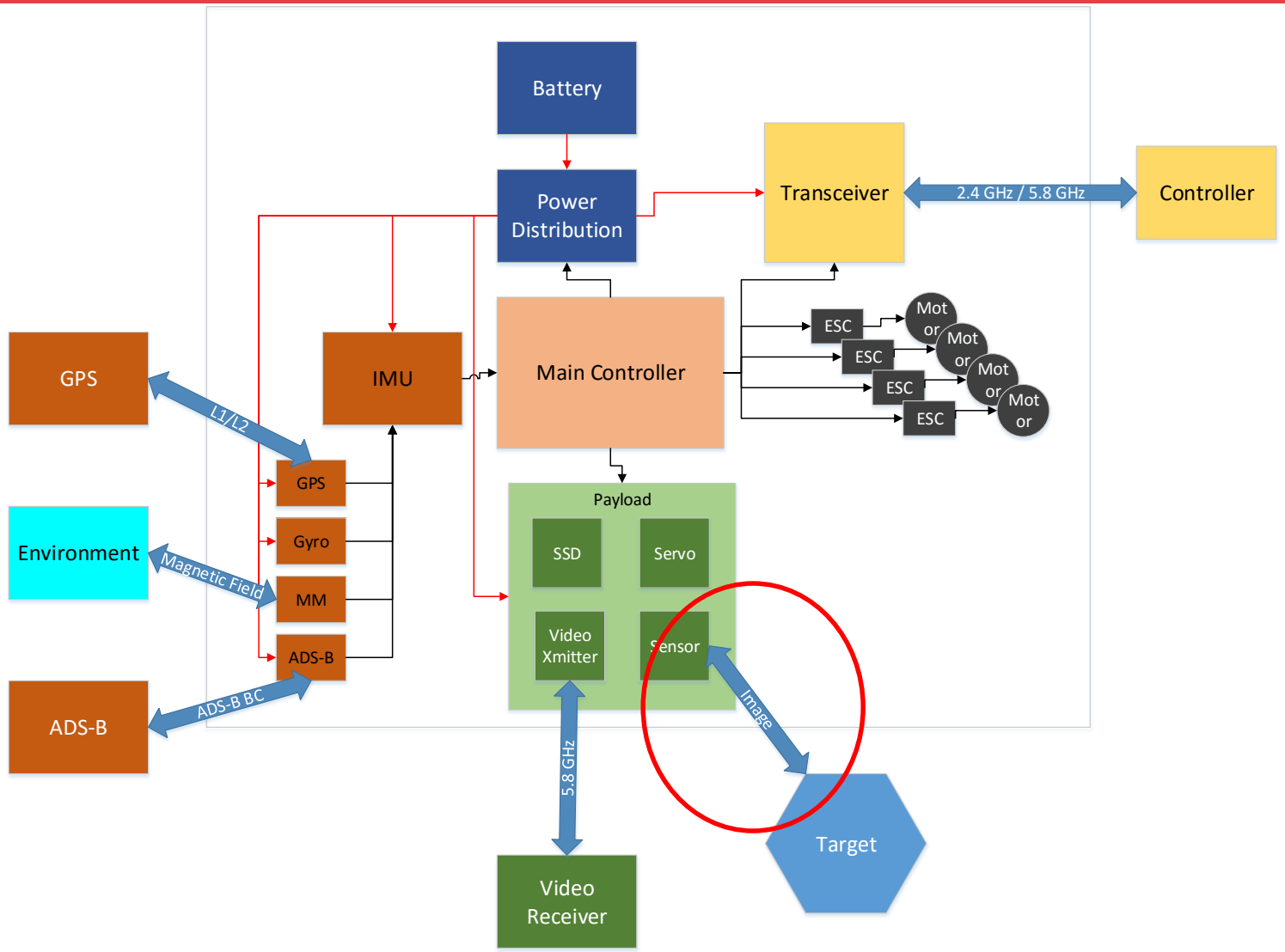
Payload/C2 Data Attacks

VSTAR SYSTEMS INC.

- Prevalent type of Attack – very easy to do
- Gaining Access to the Datastream in order to get “free” intelligence
  - Most streams poorly, or not at all encrypted
- Reports of wide range of U.S. UAV’s hacked by Iraqi Insurgents
  - Rovers widely used – Video Streams intercepted or jammed
- Typically “annoying”, but could also reveal critical intelligence

Direct Payload Attacks

VSTAR SYSTEMS INC.



Direct Payload Attack

VSTAR SYSTEMS INC.

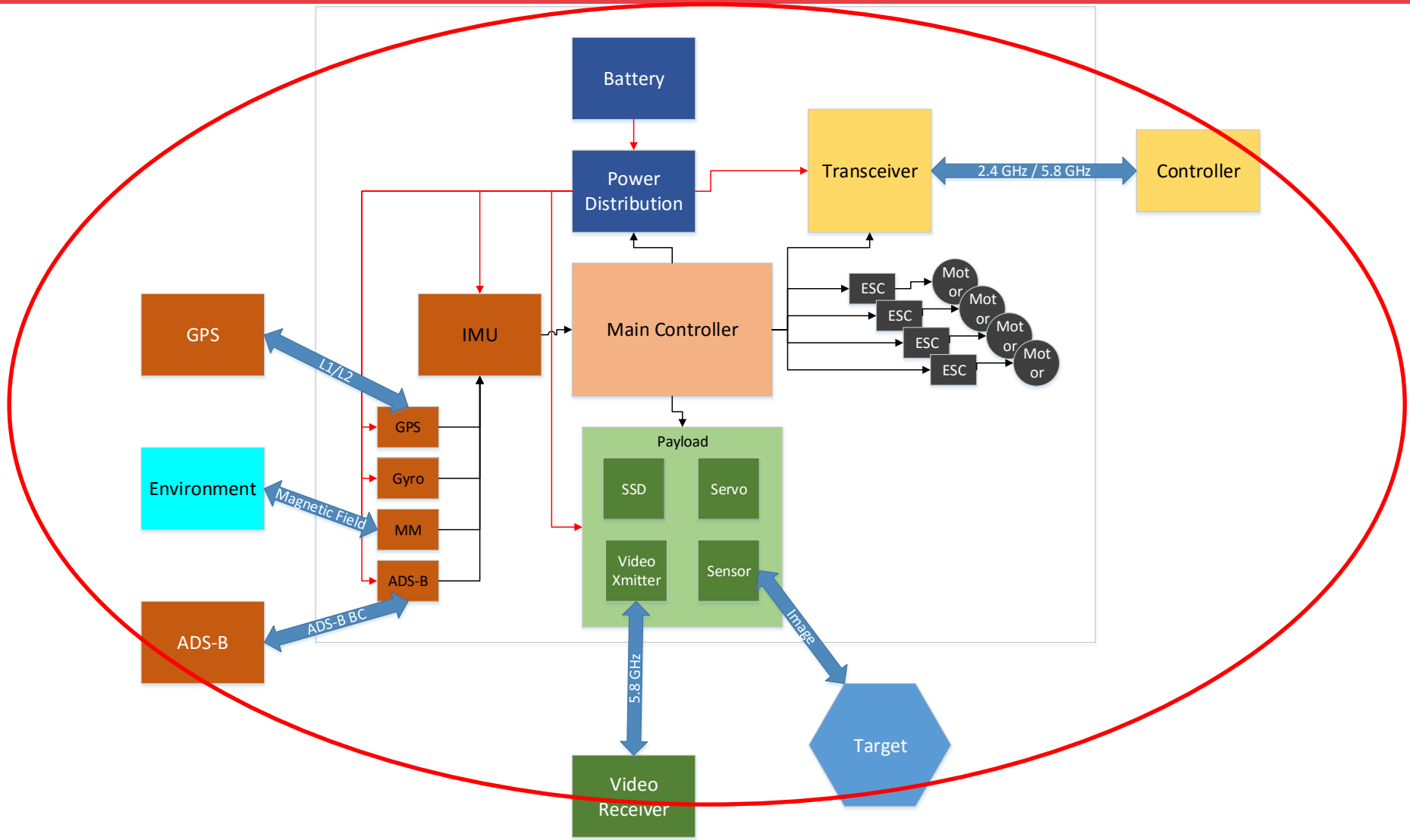
- Bit more difficult, but could seriously interrupt operations
- Disrupting or destroying the Payload
- EO/IR Cameras, SIGINT/EW Systems, etc.

VSTAR
SYSTEMS INC.

Subsystem Attacks

Subsystem Attack

VSTAR SYSTEMS INC.



UAV Subsystem Attacks

VSTAR SYSTEMS INC.

- Difficult to do, but great impact if accomplished.

- Control System Attack
  - Prevent H/W or CPU from behaving as programmed.
    - Buffer Overflow Exploits
    - Forced Resets to load malicious code
    - H/W Changes or additions

- Application Logic Attack
  - Manipulation of sensors or the environment to provide false data.
    - Sensor Data Manipulation
    - Vehicle/Component State Manipulation
    - Nav Data Manipulation
    - C2 data communication

Example of Attacks

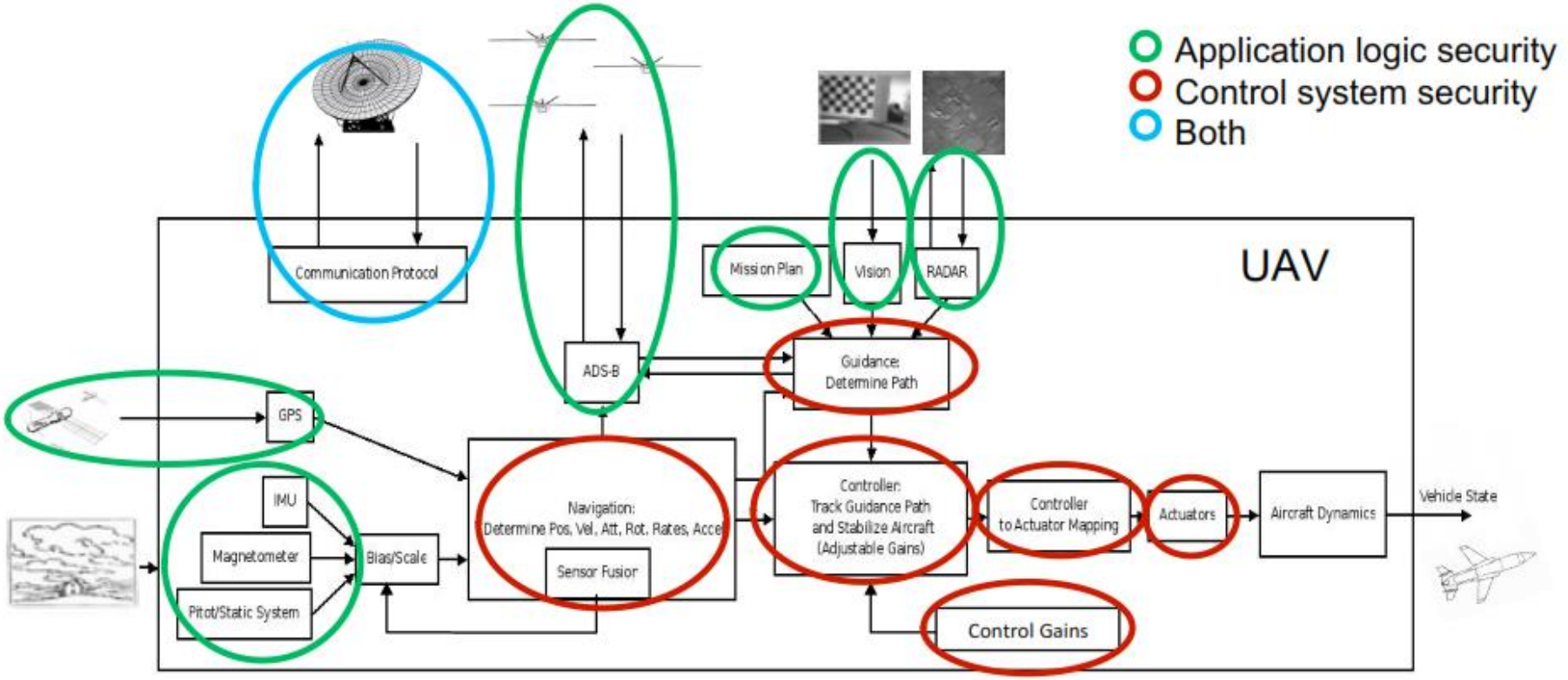
VSTAR SYSTEMS INC.

4 December 2011 - RQ-170 Sentinel downed by Iran

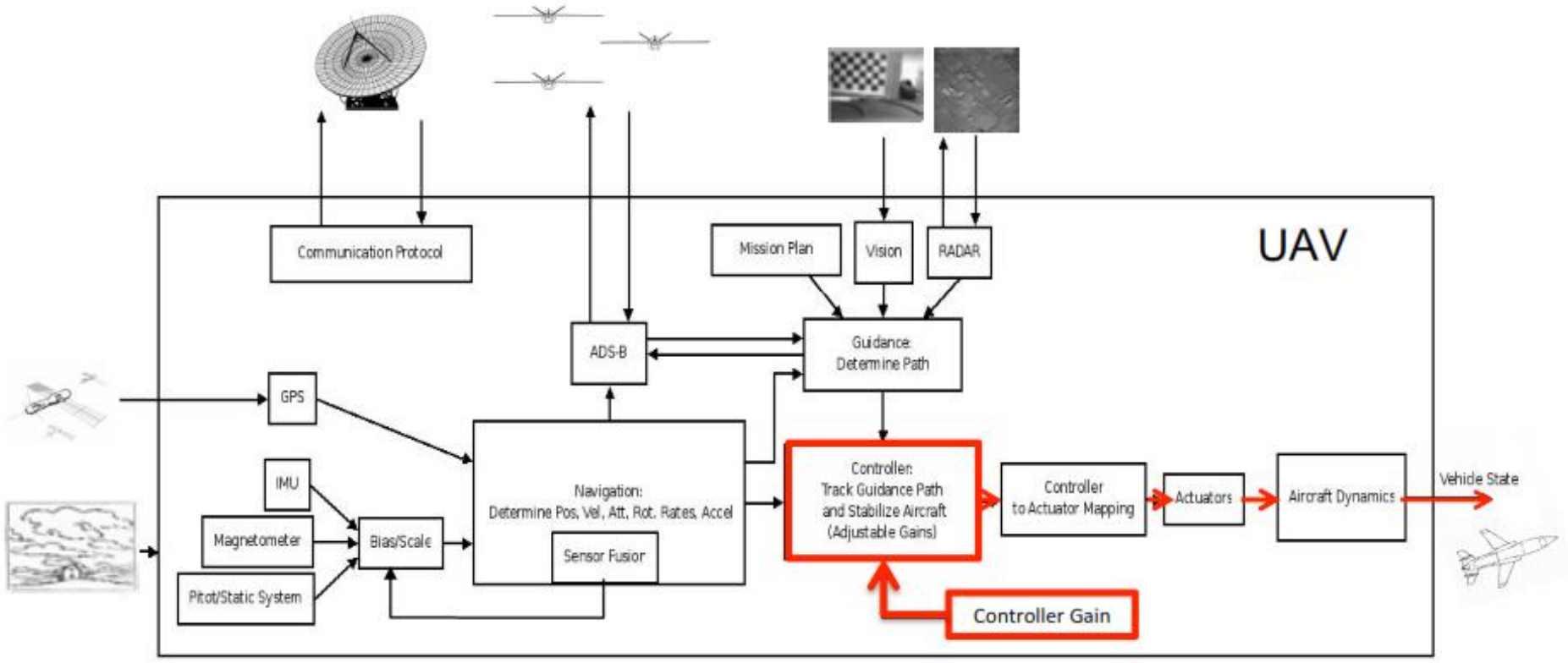
Accomplished through GPS Spoofing (according to Iran)

System Attack Scenarios

VSTAR SYSTEMS INC.

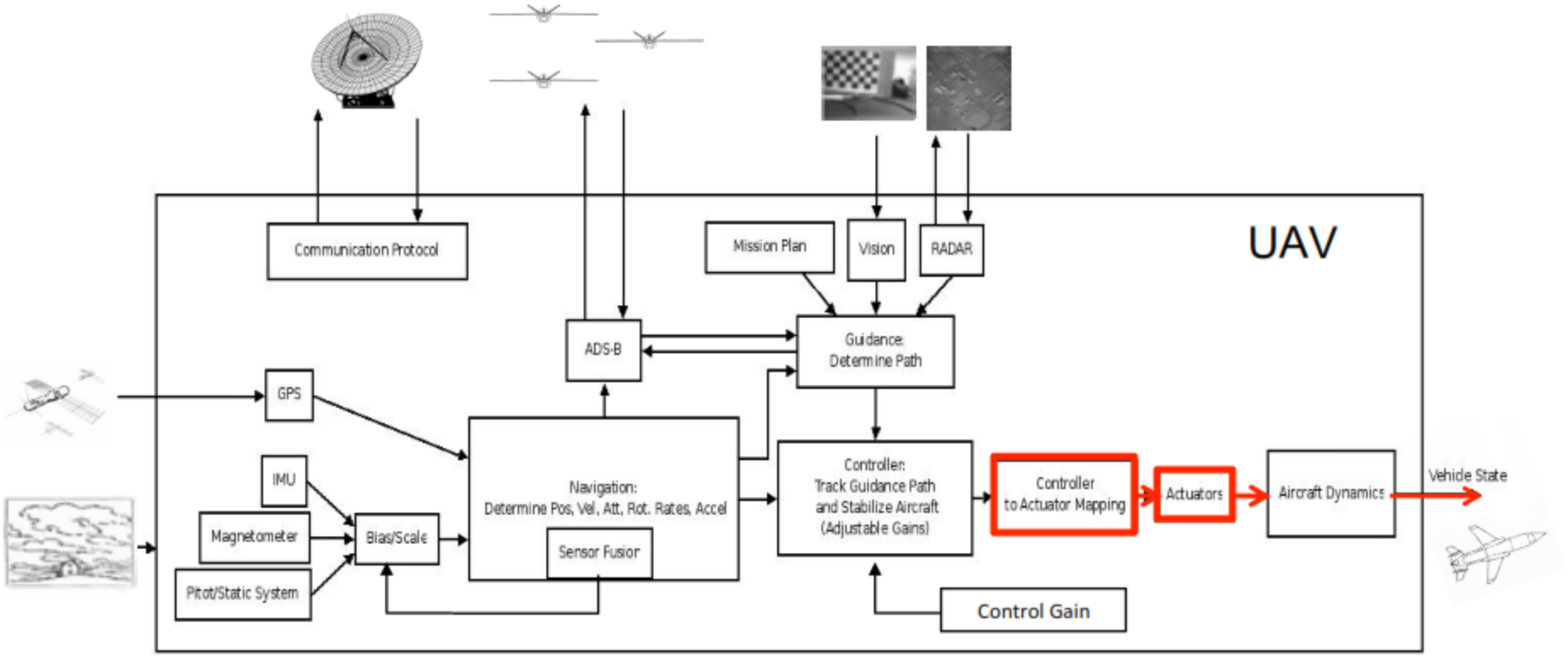


Gain Schedule Attack

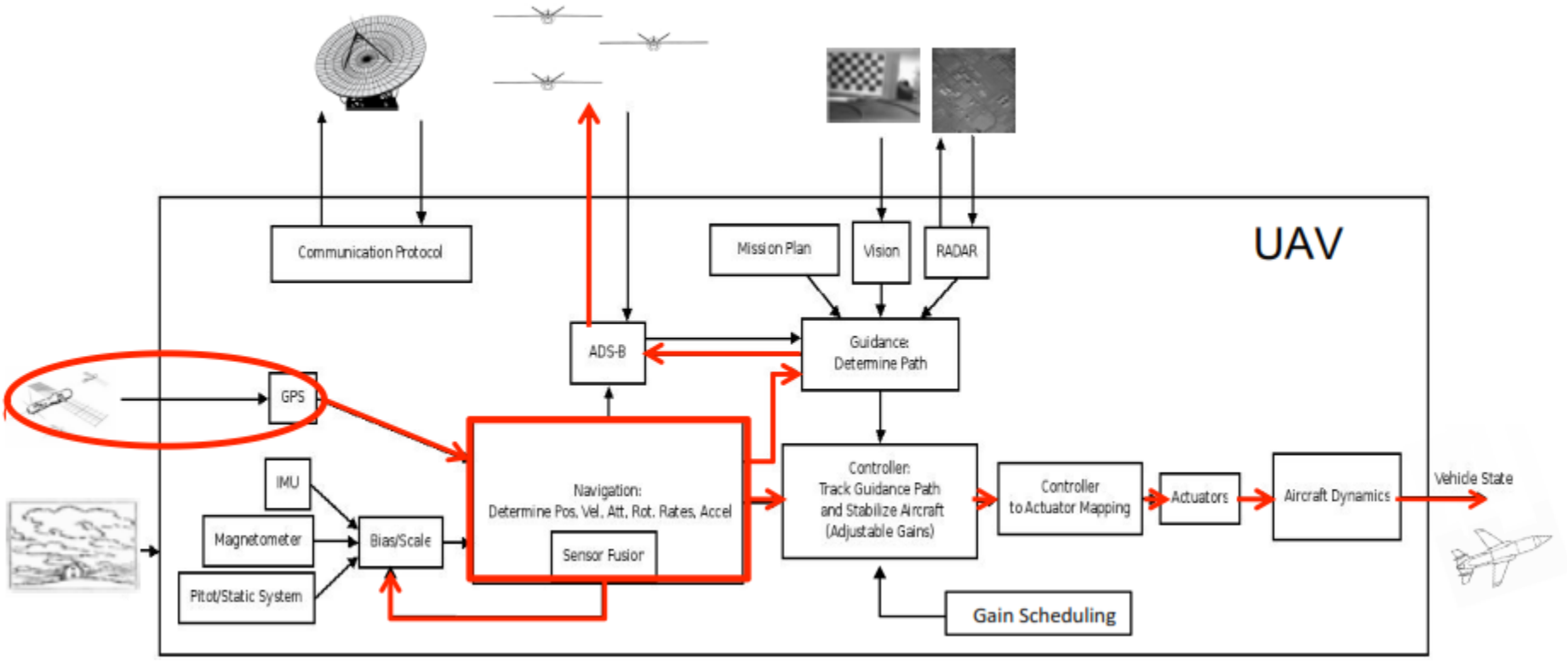


Actuator/Sensor Attack

VSTAR SYSTEMS INC.

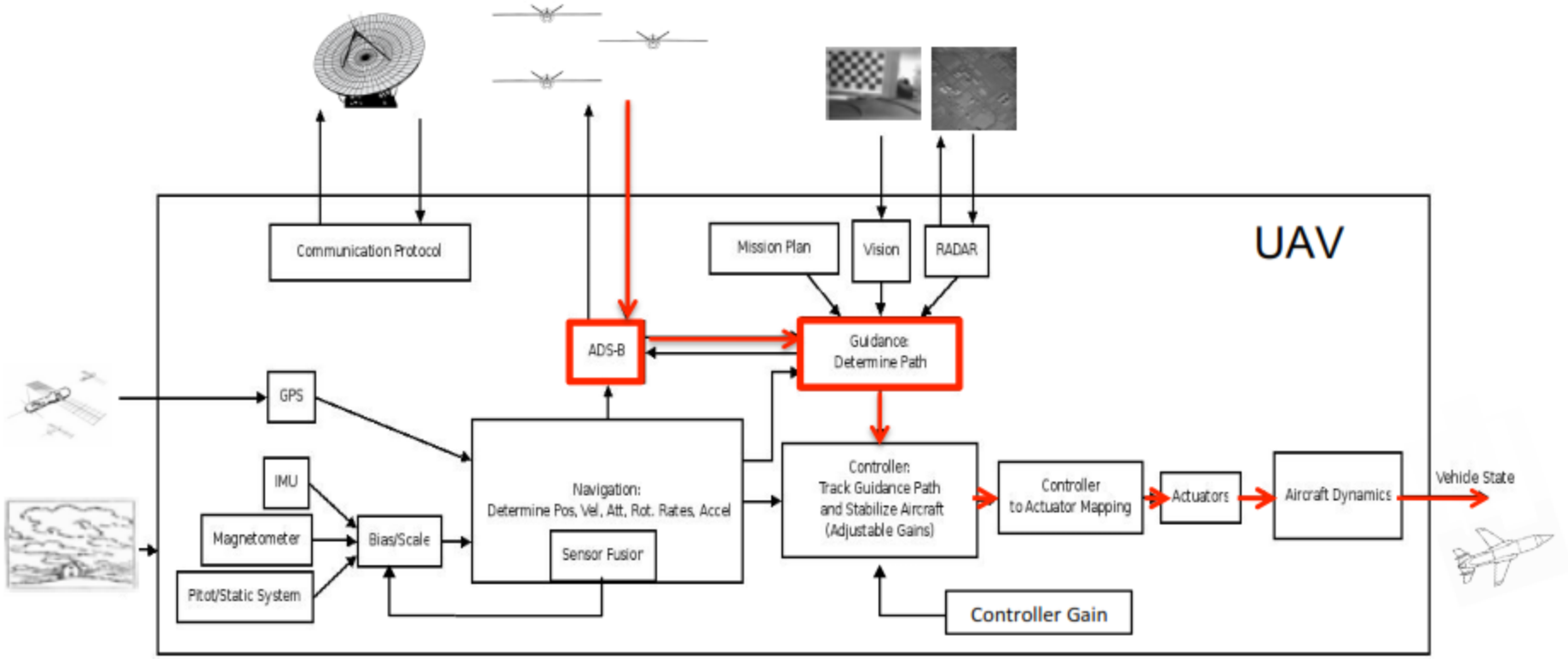


GPS Attack

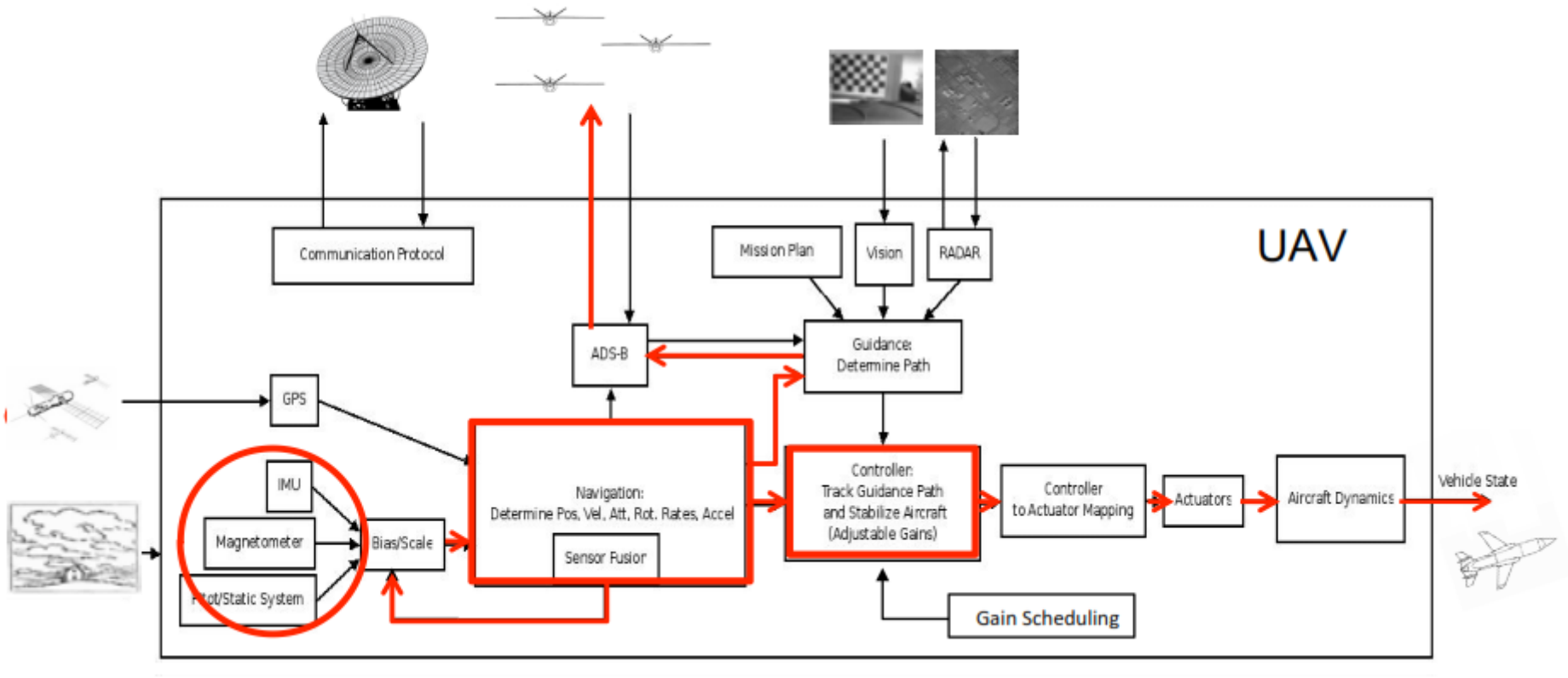

UAV
Communication Protocol
Mission Plan
Vision
RADAR
ADS-B
Guidance:
Determine Path
GPS
IMU
Magnetometer
Pitot/Static System
Bias/Scale
Navigation:
Determine Pos, Vel, Att, Rot. Rates, Accel
Sensor Fusion
Controller:
Track Guidance Path
and Stabilize Aircraft
(Adjustable Gains)
Controller
to Actuator Mapping
Actuators
Aircraft Dynamics
Vehicle State
Gain Scheduling

ADS-B Attack

VSTAR SYSTEMS INC.



Update Rate Attack



What to do about it?

VSTAR SYSTEMS INC.

- Keeping up with new Security Standards!
- Trusted Vendors
- Strong Quality Assurance Standards/Testing
- Strong Encryption
- Redundant subsystems
- Specific systems to counter external attacks
  - Receiver Autonomous Integrity Monitoring (RAIM)

UAV Cybersecurity is gaining traction – high costs associated!
BUT – Systems Engineering MUST think about it

References

- FAA Unmanned Aircraft Systems (UAS) Cyber Security Initiatives
  - Stephen George, FAA Airworthiness Manager
- Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles
  - Ian Kim, Brandon Wampler, James Goppert, Inseok Hwang
- The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment
  - Kim Hartmann, Christopher Steup
- A Study on Unmanned Vehicles and Cyber Security
  - Emy Rivera, Robert Baykov, Guofei Gu

VSTAR
SYSTEMS INC.

END TO END UNMANNED AND ROBOTIC SYSTEMS INTEGRATION