## WIFI

- PalmH / TicketBreedProfession


# Lecture One

## Course Overview &

## Intro to Space

# Meet the instructors!

# Jacob Oakley

# Michael Butler






Current Job: Principal Engineer, Cybersecurity and Advanced Platforms Subdivision (CAPS), at The Aerospace Corporation

- Developing cyber labs for training, perform penetration testing & vulnerability assessments {Ethical Hacking!}
- Performing cybersecurity research on ground systems and spacecraft systems to better position the federal government with respect to protection of our critical space infrastructure.

FINAL FRONTIER SECURITY

**2005** — B.S. Electrical Engineering West Virginia University

**2009** — Lockheed Martin Supporting National Geospatial Intelligence Agency

NASA's Independent Verification and Validation Program

Working for Small Business in West Virginia doing Spacecraft and Ground Simulation/Emulation

**2013** — Transitioned to NASA Government Employee GS-13

Began "Hacking" Space Systems

**2018** — Left the Government as GS-15 to become Chief Technology Officer (CTO) for small business in West Virginia

- Supported NASA part-time as contractor

**2019** — Left Job as CTO to join Aerospace Corporation Federally Funded and Development Center

**2024**

## Pen-tested / "Ethically Hacked" Space Systems 2013-2024

- Mars' Rovers (MER & MSL) & Deep Space Network (DSN) at JPL
- Hubble Space Telescope (HST) at GSFC
- Closed IONet (CIONet) within NASCOM at GSFC
- Space Network (SN) at the White Sands Complex (WSC)
- KSC Ground Systems Development and Operations (GSDO) Kennedy Ground Control
- System (KGCS) and Launch Control System (LCS)
- James Web Space Telescope (JWST) Ground System at the Space Telescope Science Institute (STScI) in Baltimore
- Huntsville Operations Support Center (HOSC) at Marshall Space Flight Center
- Near Earth Network (NEN) at Wallops Flight Facility
- ISS Mission Control Center (MCC) at Johnson Space Center
- Wind tunnels at Glenn Research Center
- Hypersonic Environment at Langley Research Center
- NOAA's Joint Polar Satellite System (JPSS)

***NASA's Exceptional Service Medal (2019) for "groundbreaking" cyber work***

## 2019-2024

- DefCON Presentations:
  - DEF CON 2020: Exploiting Spacecraft
  - DEF CON 2021: Unboxing the Spacecraft Software BlackBox Hunting for Vulnerabilities
  - DEF CON 2022: Hunting for Spacecraft Zero Days using Digital Twins
  - DEF CON 2023: Building Space Attack Chains using SPARTA
- Papers/Articles:
  - 2019: Defending Spacecraft in the Cyber Domain
  - 2020: Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices
  - 2021: Cybersecurity Protections for Spacecraft: A Threat Based Approach
  - 2021: Translating Space Cybersecurity Policy into Actionable Guidance for Space Vehicles
  - 2022: Protecting Space Systems from Cyber Attack
  - 2024: Space Segment Cybersecurity Profile for NSS
- July 2022 Congressional Testimony:
  - Video: https://science.house.gov/hearings?ID=996438A6-A93E-4469-8618-C1B59BC5A964
  - Written Testimony: https://republicans-science.house.gov/_cache/files/2/9/29fff6d3-0176-48bd-9c04-00390b826aed/A8F54300A11D55BEA5AF2CE305C015BA.2022-07-28-bailey-testimony.pdf
- SPARTA Launched
  - https://sparta.aerospace.org

SPARTA — SPACE ATTACK RESEARCH & TACTIC ANALYSIS

# Class Day 1

- 0900 – 1000 Lecture 1: Lecture 1: 60m Intro to course & Understanding the attack surface
- 1000 – 1030 Lab 1: 30m NOS3 and ground control system operations
- 1030 - Break: 15m
- 1045 – 1130 Lab 1: 45m NOS3 and ground control system operations continued
- 1130-1230 Lecture 2: 60m Adversarial Perspective
- 1230-1345 Lunch
- 1400-1500 – Lab 2: 1hr insider threat, malicious tasks
- 1500 - 1600 – Lab 3: 1hr Exploiting ground to space without using ground SW (garak command sende
- 1600-1615 Coffee Break
- 1615 – 1700 Lab 4: 45m IOCs and cleaning up after yourself
- 1700 – 1800 FFA

# Space

# Purpose

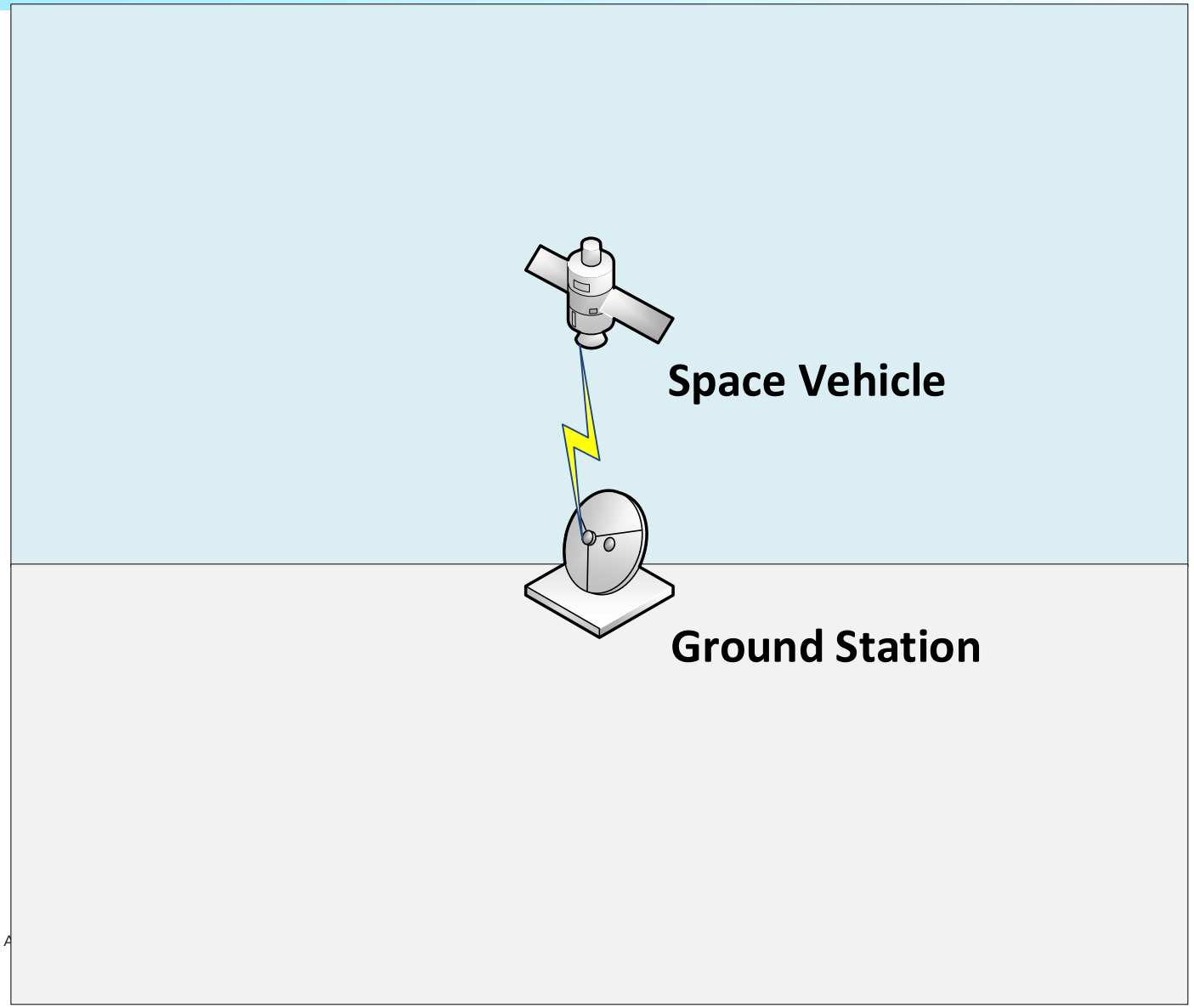
- Space Systems have unique constraints, challenges, technologies, missions and CONOPS
- These aspects dictate adversary tradecraft
- Understanding how malicious actors will operate within these systems is key to figuring out how to stop them

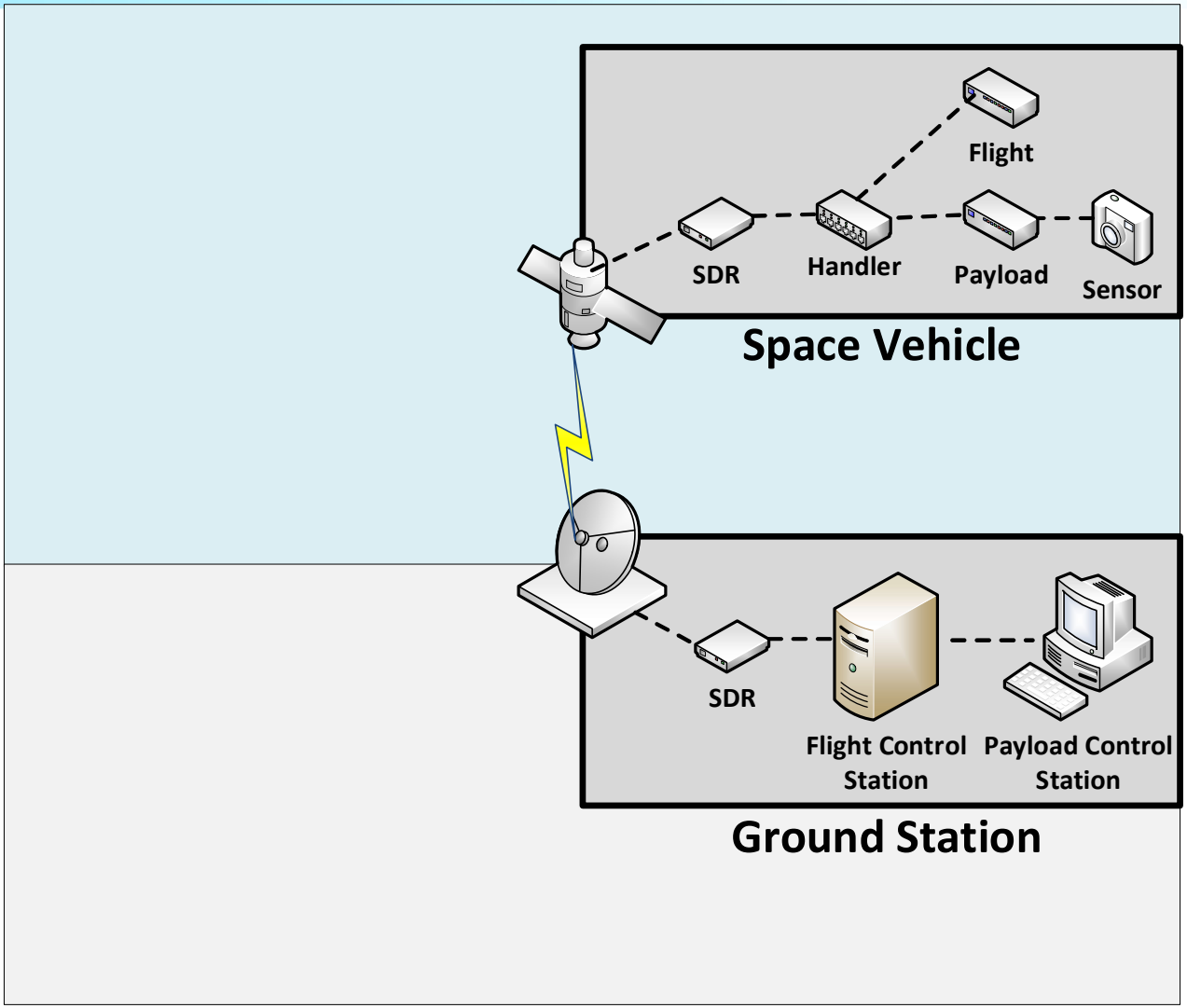
# So What?

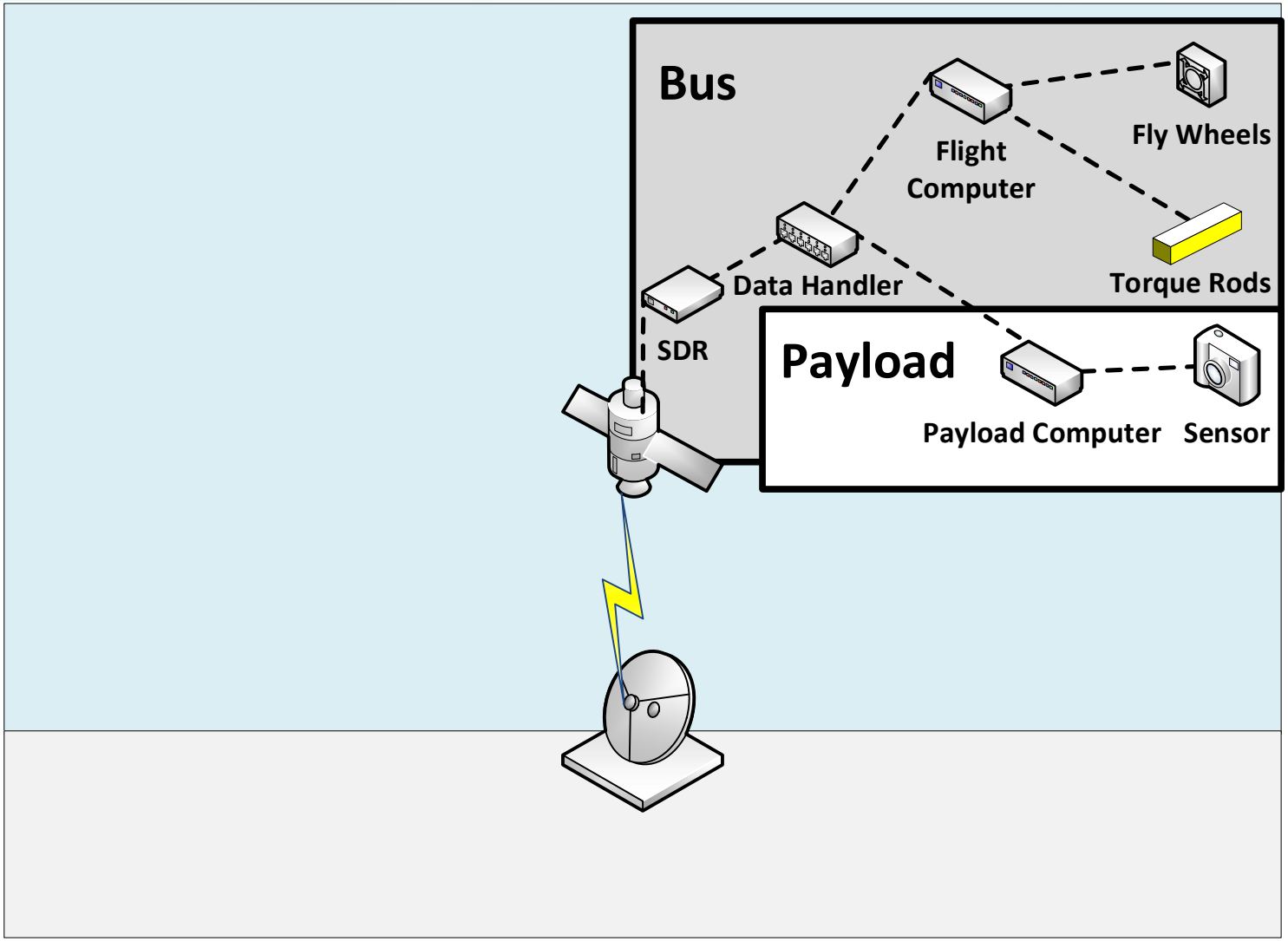
- Very limited international communication
- No weather forecasting
- No PNT
  - Flights grounded, ships lost at sea, inability for most people to navigate
- No time
  - Encryption
  - Financial transactions
  - Network protocol failures
- A bit hyperbolic, but illustrative of how important space has become

# Key Terms & Definitions

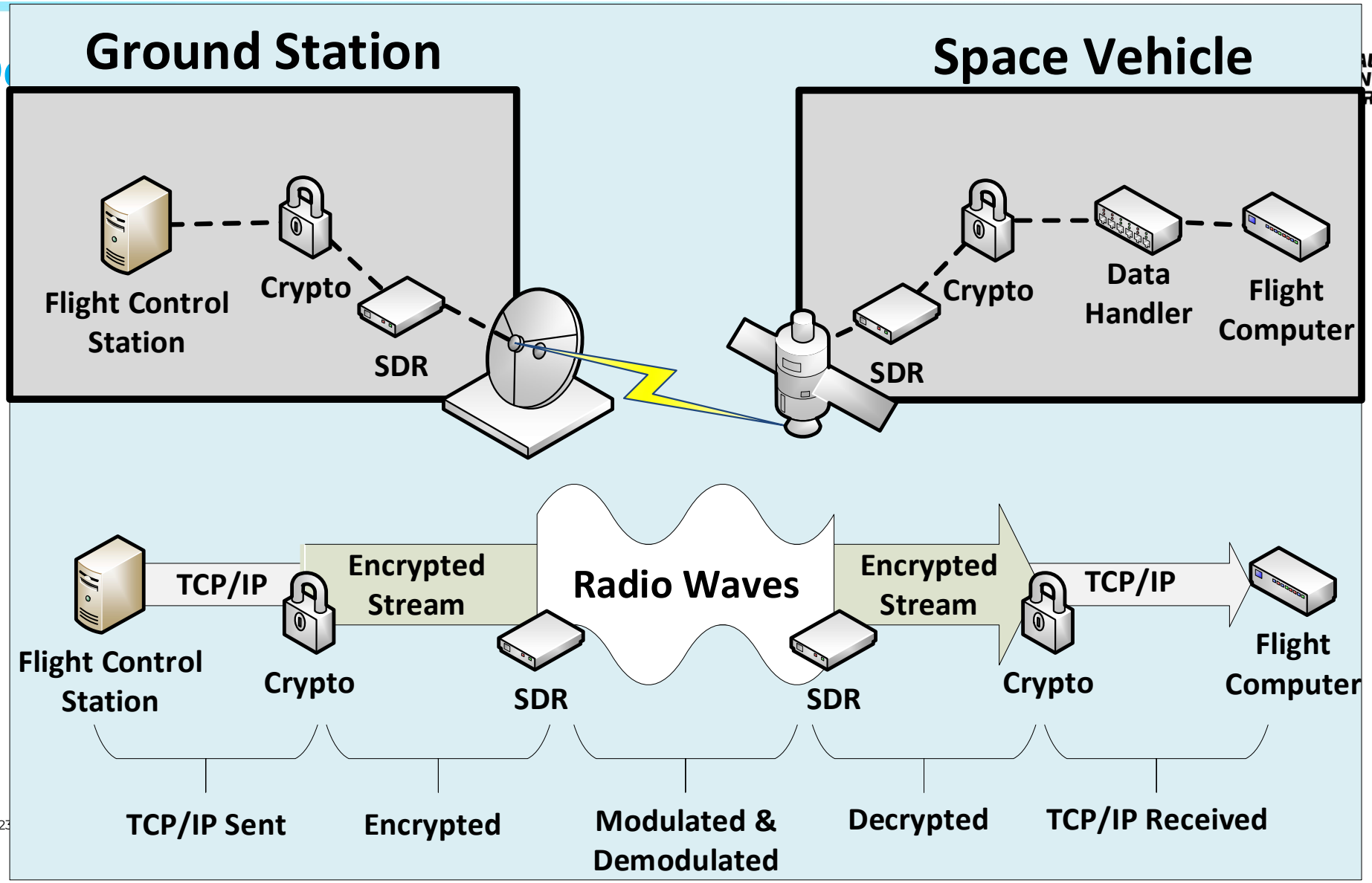
- SDR: Software defined radio capable of reprogramming RF communications characteristics
- Modem: modulates and demodulates RF signals
- Telemetry (TLM): Data from a spacecraft is telemetry, engineering (housekeeping) or science data
- Command / Task: request made to the satellite or payload to do or report something
- ADCS: Attitude determination and control system turns commands into execution
- Flight software: suite of SW and framework running on the flight computer (ADCS + comms, data management, storage etc)
- Satellite Bus: components responsible for flight
- Payload: components responsible for mission
- Software Bus: pub-sub mechanism for flight computer and ADCS to communicate to things like propulsion, PNT receiver, star tracker, sun sensor, solar panels battery etc.

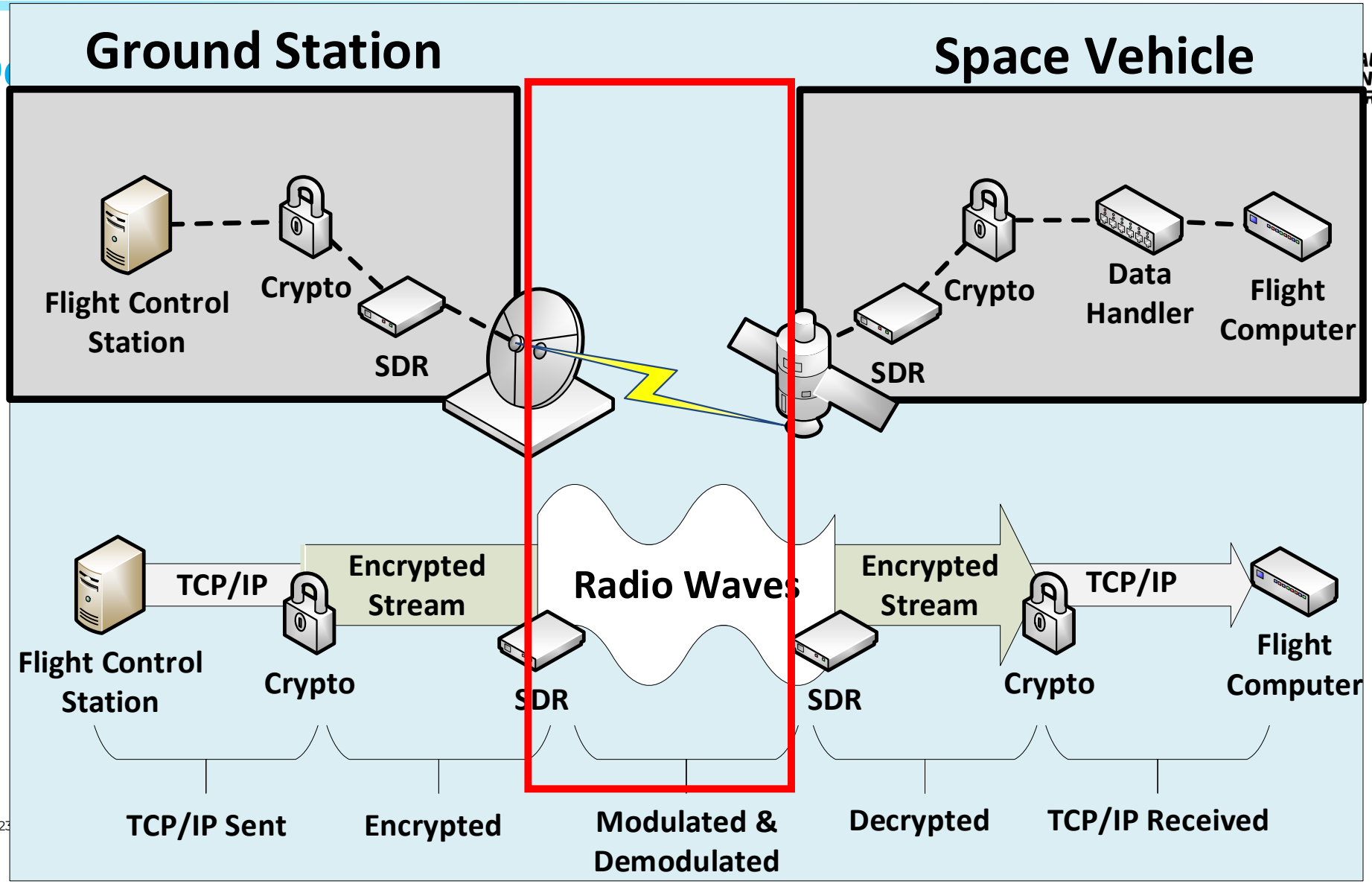


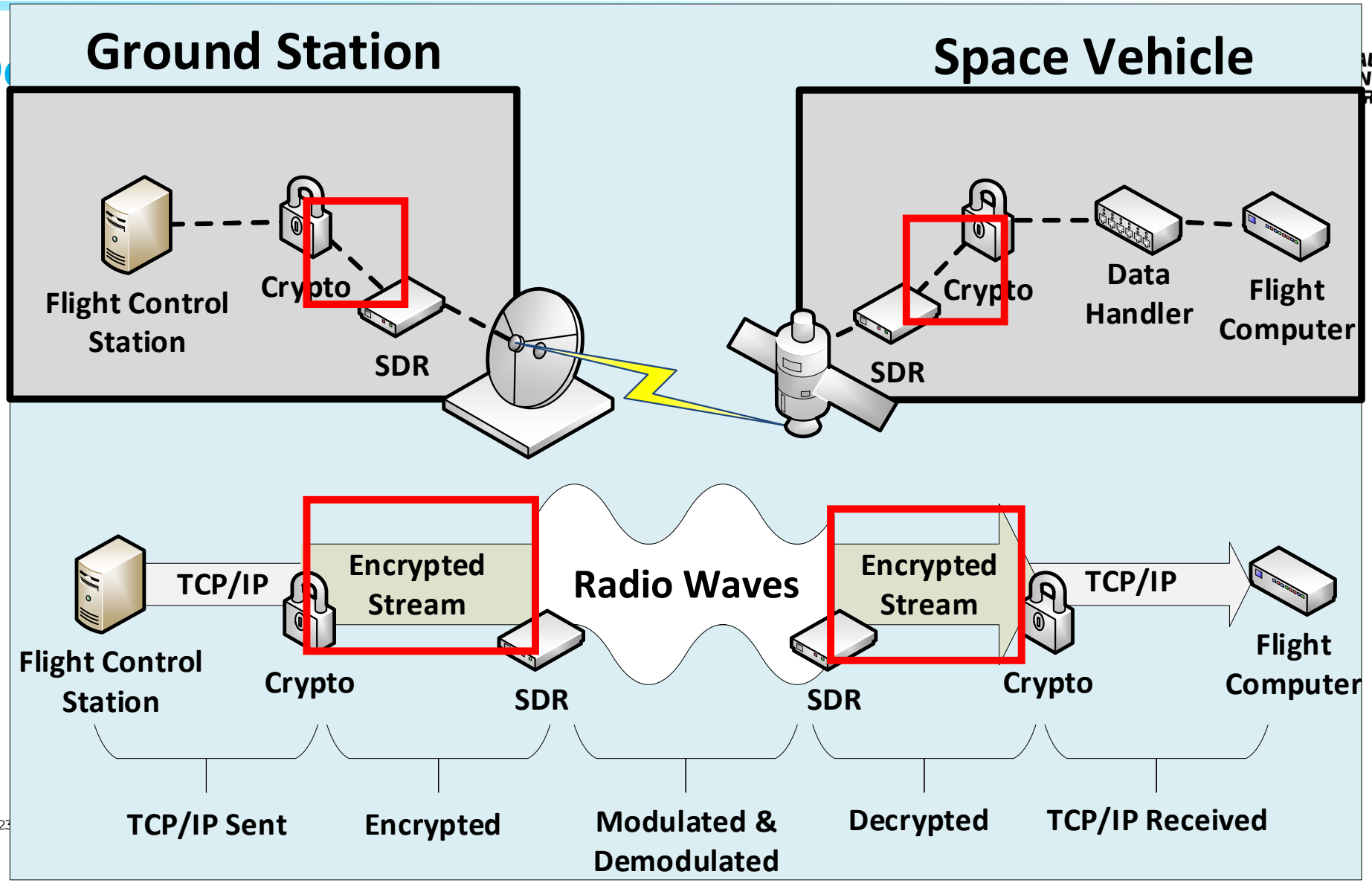


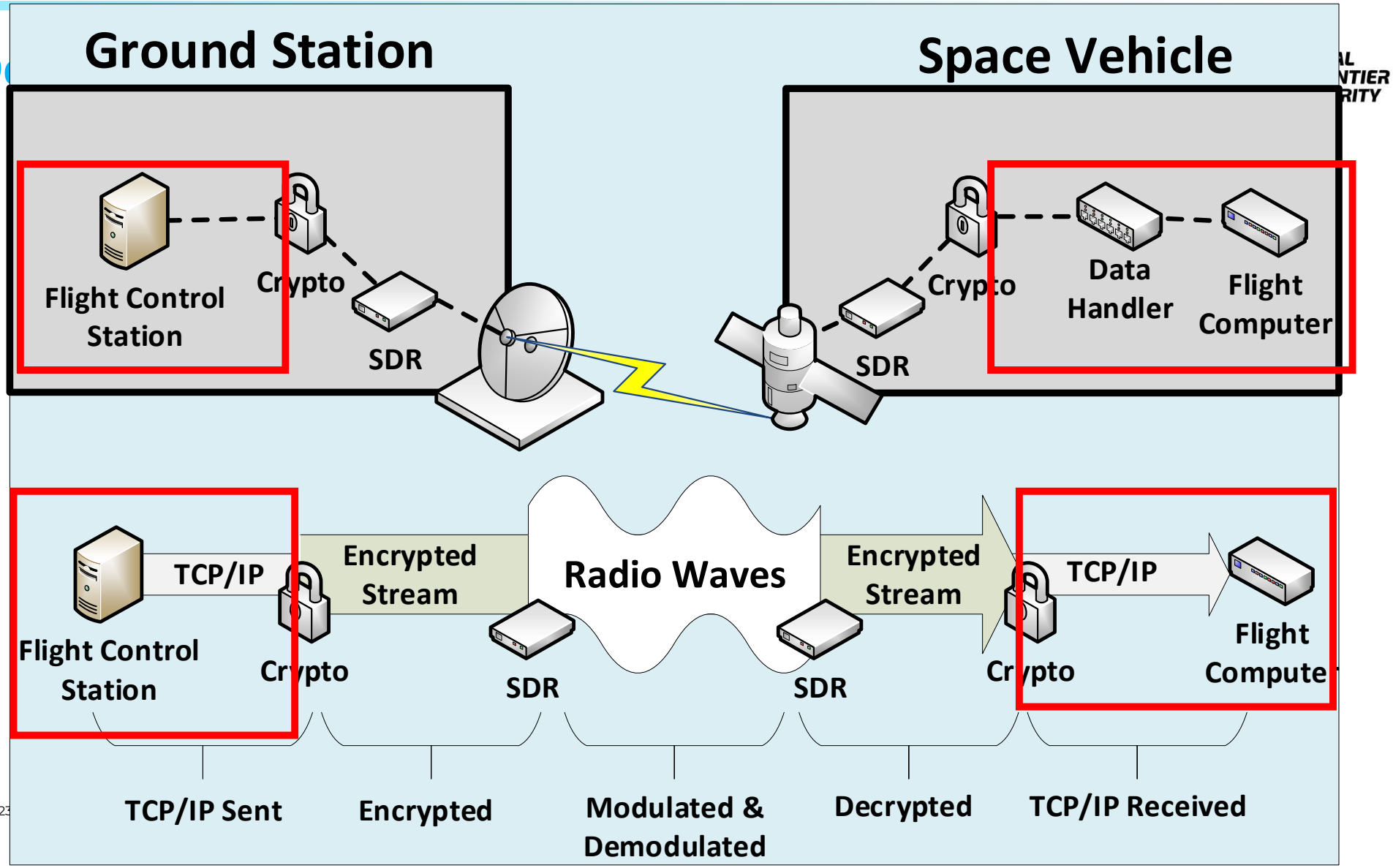


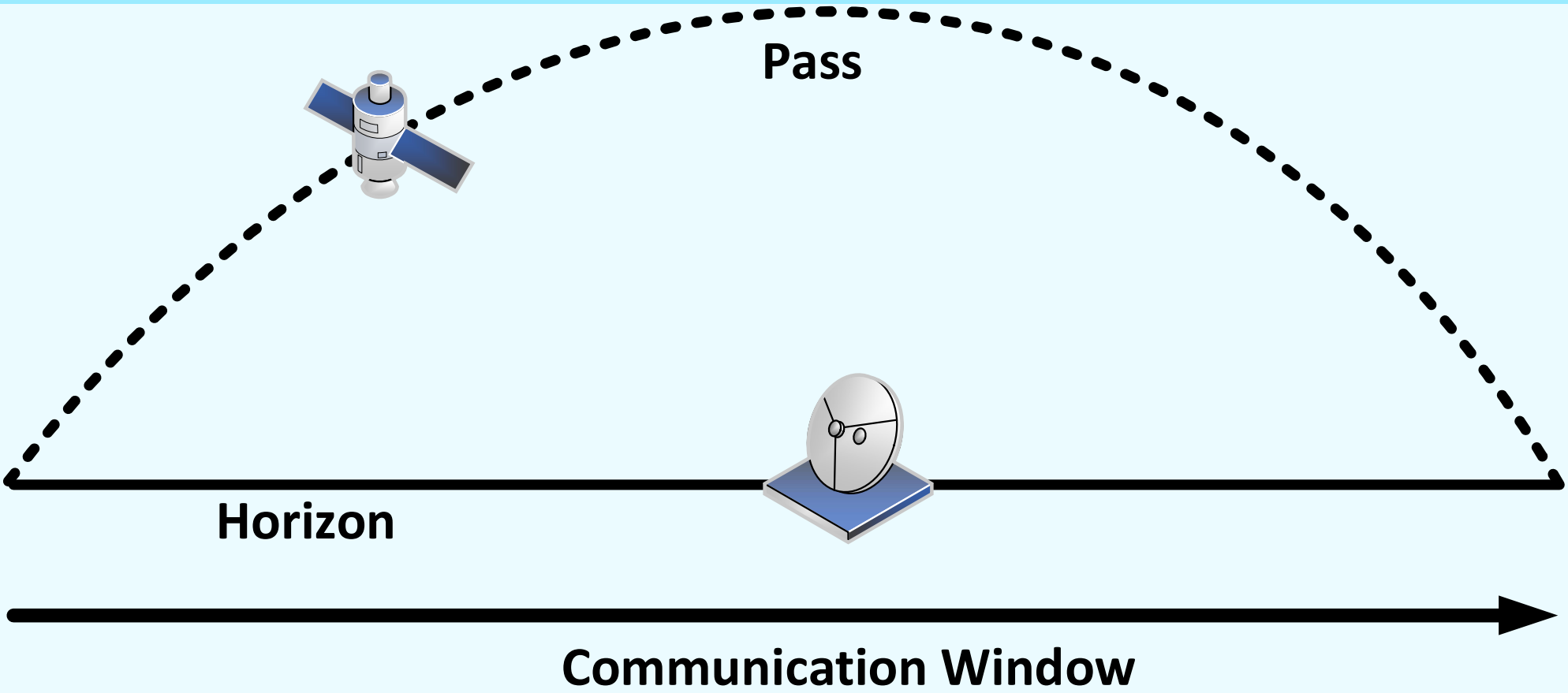

FINAL FRONTIER SECURITY


Ground Station
Space Vehicle
Flight Control Station
Crypto
SDR
Crypto
Data Handler
Flight Computer
SDR
TCP/IP
Encrypted Stream
Radio Waves
Encrypted Stream
TCP/IP
Flight Control Station
Crypto
SDR
SDR
Crypto
Flight Computer
TCP/IP Sent
Encrypted
Modulated & Demodulated
Decrypted
TCP/IP Received


Ground Station
Space Vehicle
Flight Control Station
Crypto
SDR
Crypto
Data Handler
Flight Computer
SDR
TCP/IP
Encrypted Stream
Radio Waves
Encrypted Stream
TCP/IP
Flight Control Station
Crypto
SDR
SDR
Crypto
Flight Computer
TCP/IP Sent
Encrypted
Modulated & Demodulated
Decrypted
TCP/IP Received


Ground Station
Space Vehicle
Flight Control Station
Crypto
SDR
Crypto
Data Handler
Flight Computer
SDR
TCP/IP
Encrypted Stream
Radio Waves
Encrypted Stream
TCP/IP
Flight Control Station
Crypto
SDR
SDR
Crypto
Flight Computer
TCP/IP Sent
Encrypted
Modulated & Demodulated
Decrypted
TCP/IP Received


Ground Station
Space Vehicle
Flight Control Station
Crypto
SDR
Crypto
Data Handler
Flight Computer
SDR
TCP/IP
Encrypted Stream
Radio Waves
Encrypted Stream
TCP/IP
Flight Control Station
Crypto
SDR
SDR
Crypto
Flight Computer
TCP/IP Sent
Encrypted
Modulated & Demodulated
Decrypted
TCP/IP Received



# Ground Station Functions

- Antennae movement
- Communication
- Tasking
  - Flight
  - Payload
- Dissemination

# Space Vehicle Functions

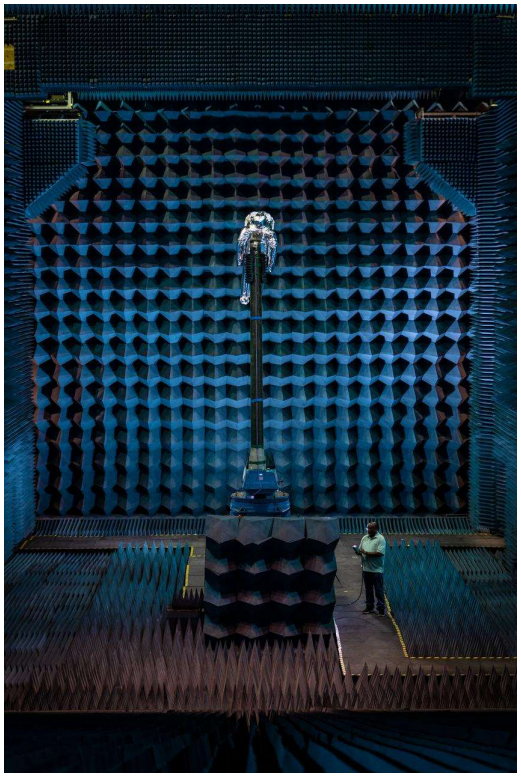
- Bus
  - Power
    - Generate, Store, Moderate
  - PNT
    - GPS, Star Tracker, Sun Sensor
  - Flight:
    - Propulsion & Attitude adjustment
  - Communication
- Payload
  - Tasking
  - Data storage and off load

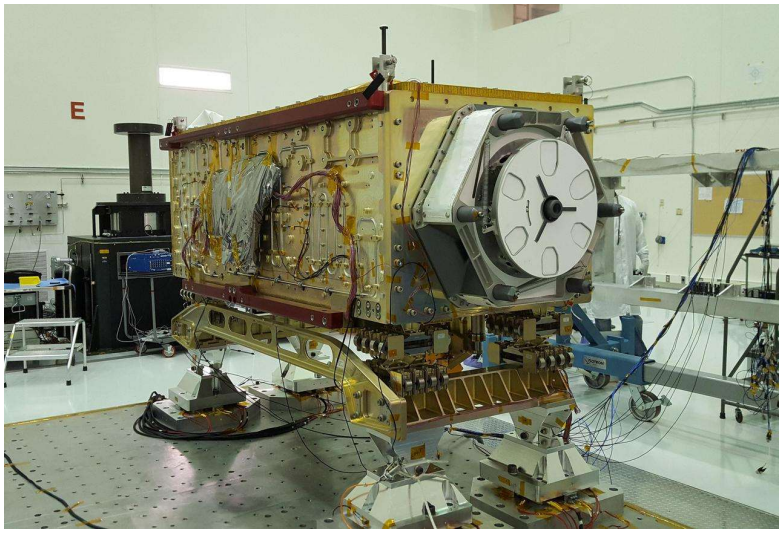
# Environmental Challenges

- Radiation
  - Single events
  - Accumulation
- Temperature extremes
- Vacuum
- Space objects
  - Junk
  - Others
- Vibration

# Operational Challenges

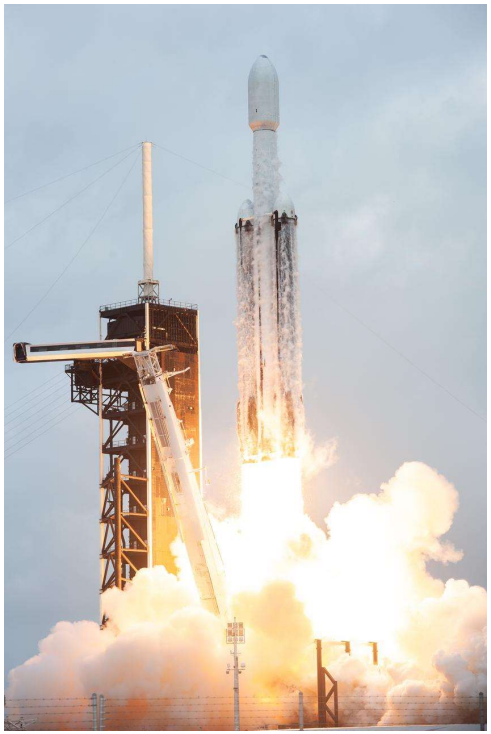
- Testing

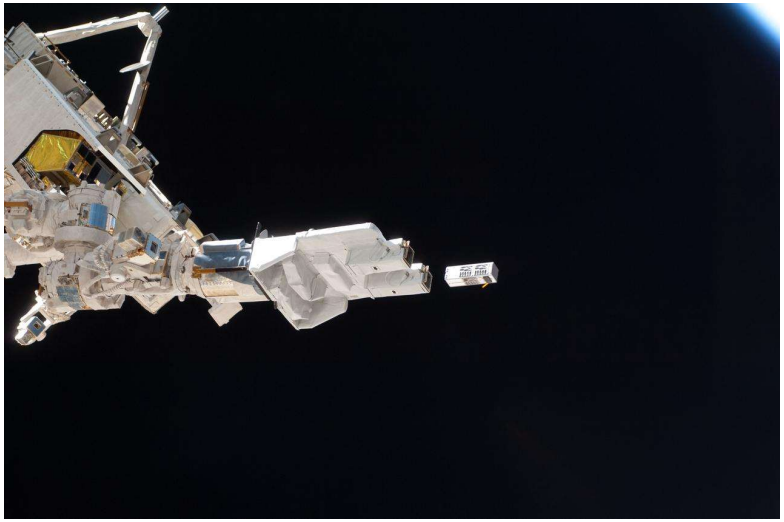




# Operational Challenges

- Launch
- Deployment
- Stabilization
  - De-tumble
  - Orbit





# Operational Challenges

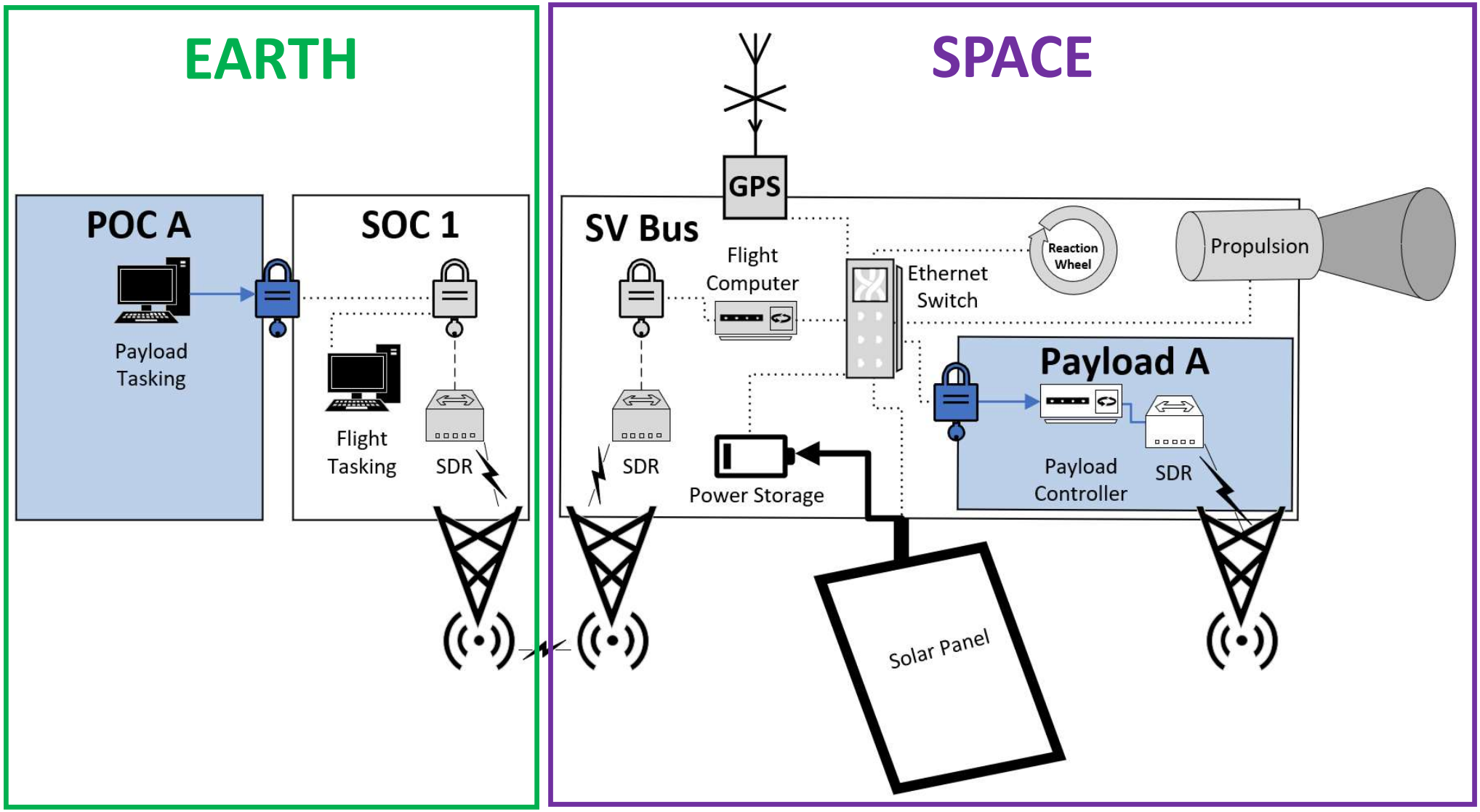
- Power
- Emanations interference (self inflicted and otherwise)
- De-Orbit

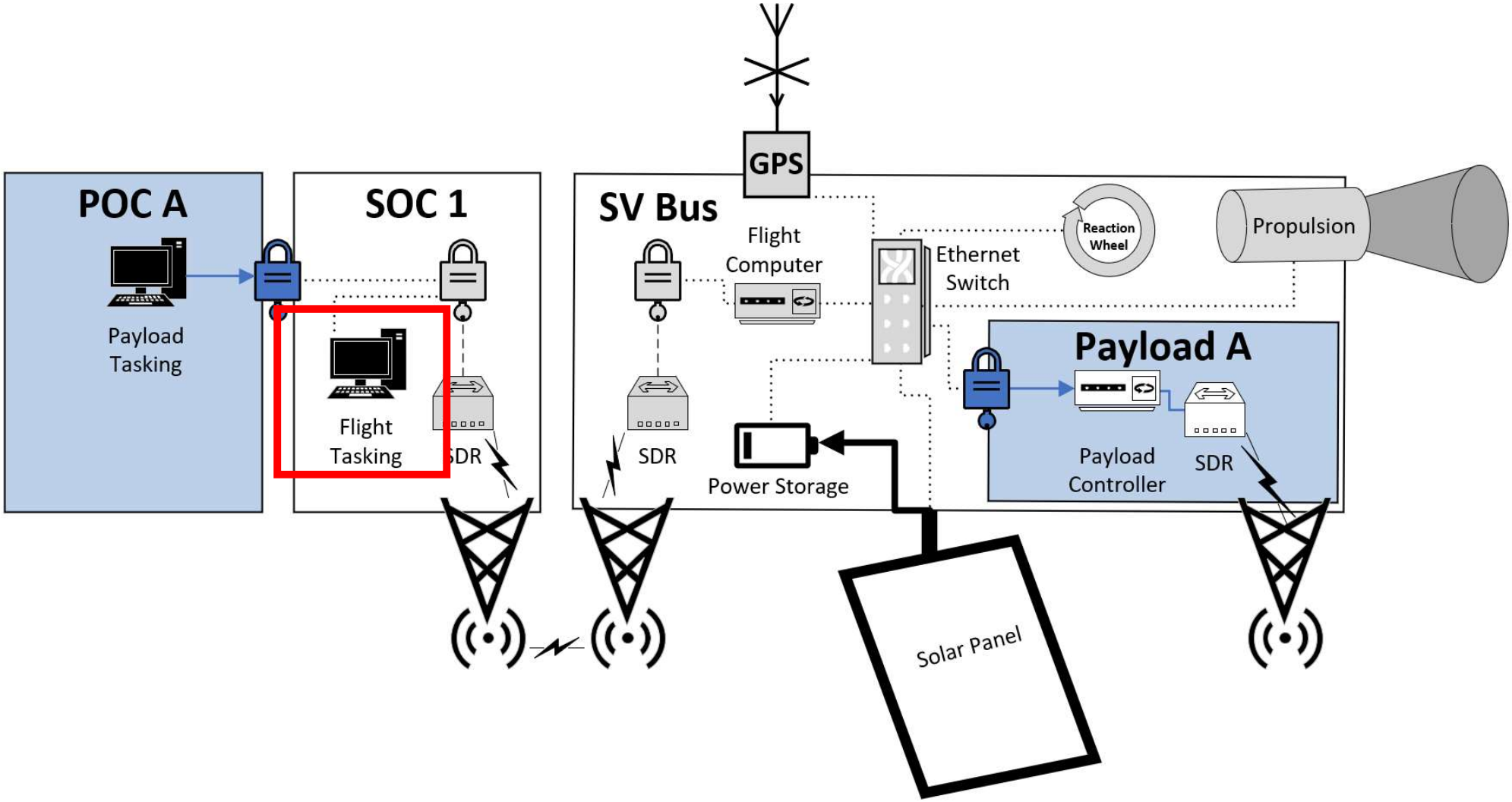
# Safeguards

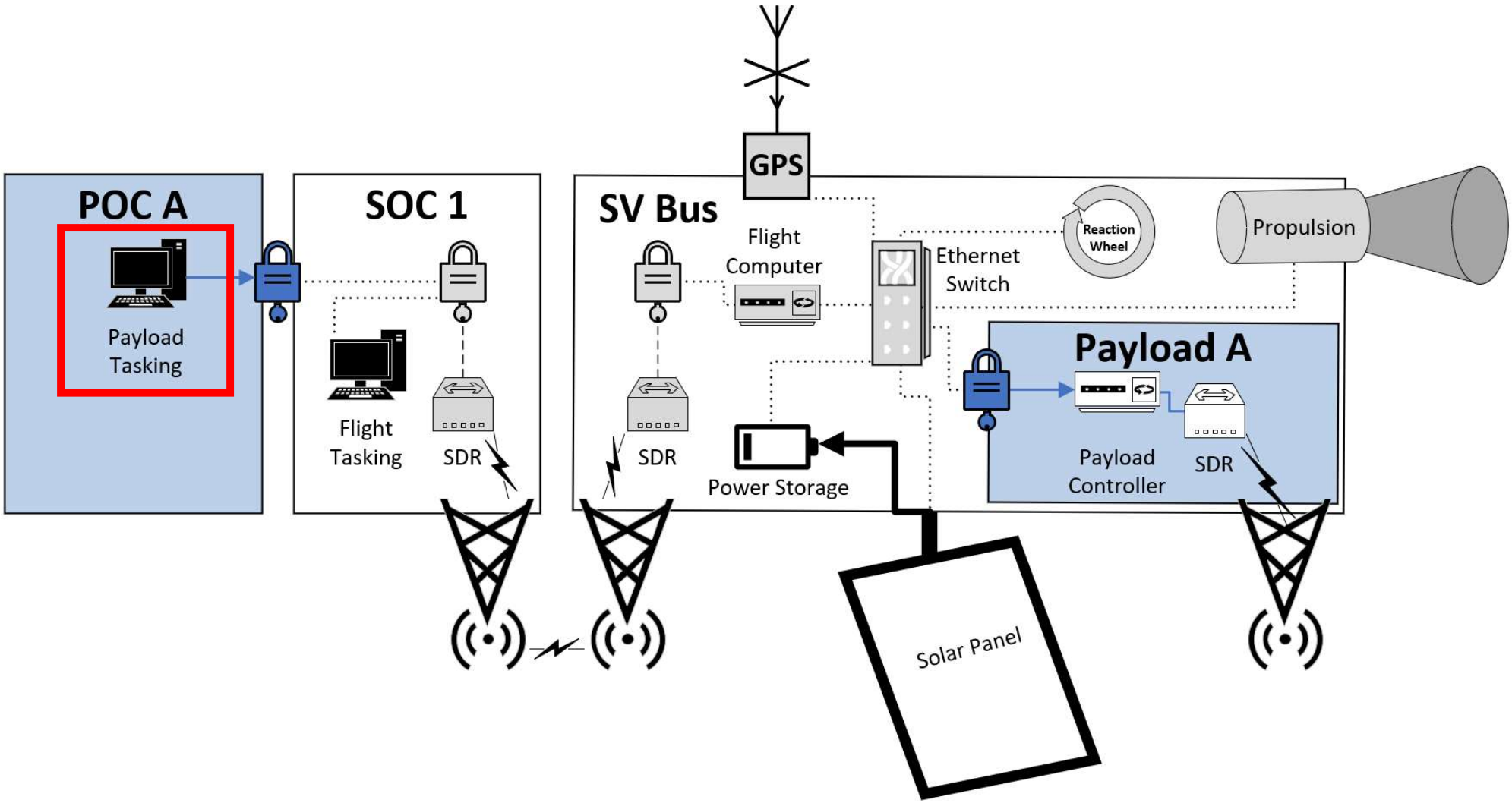

- Back-ups
- Gold images
- Watchdogs
- Fall-back communications / encryption settings
- Resource limiters

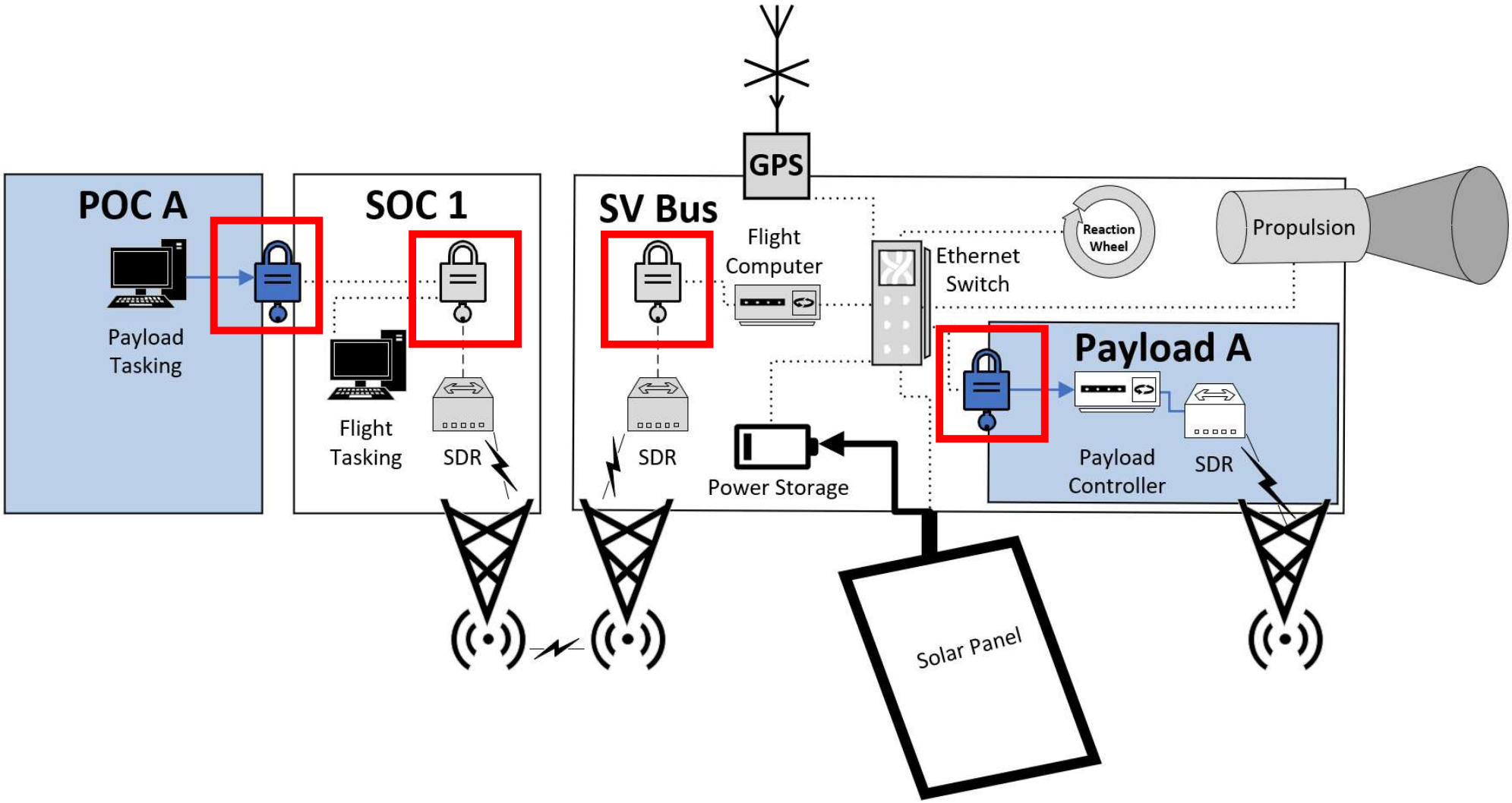
***These are redundancy focused***

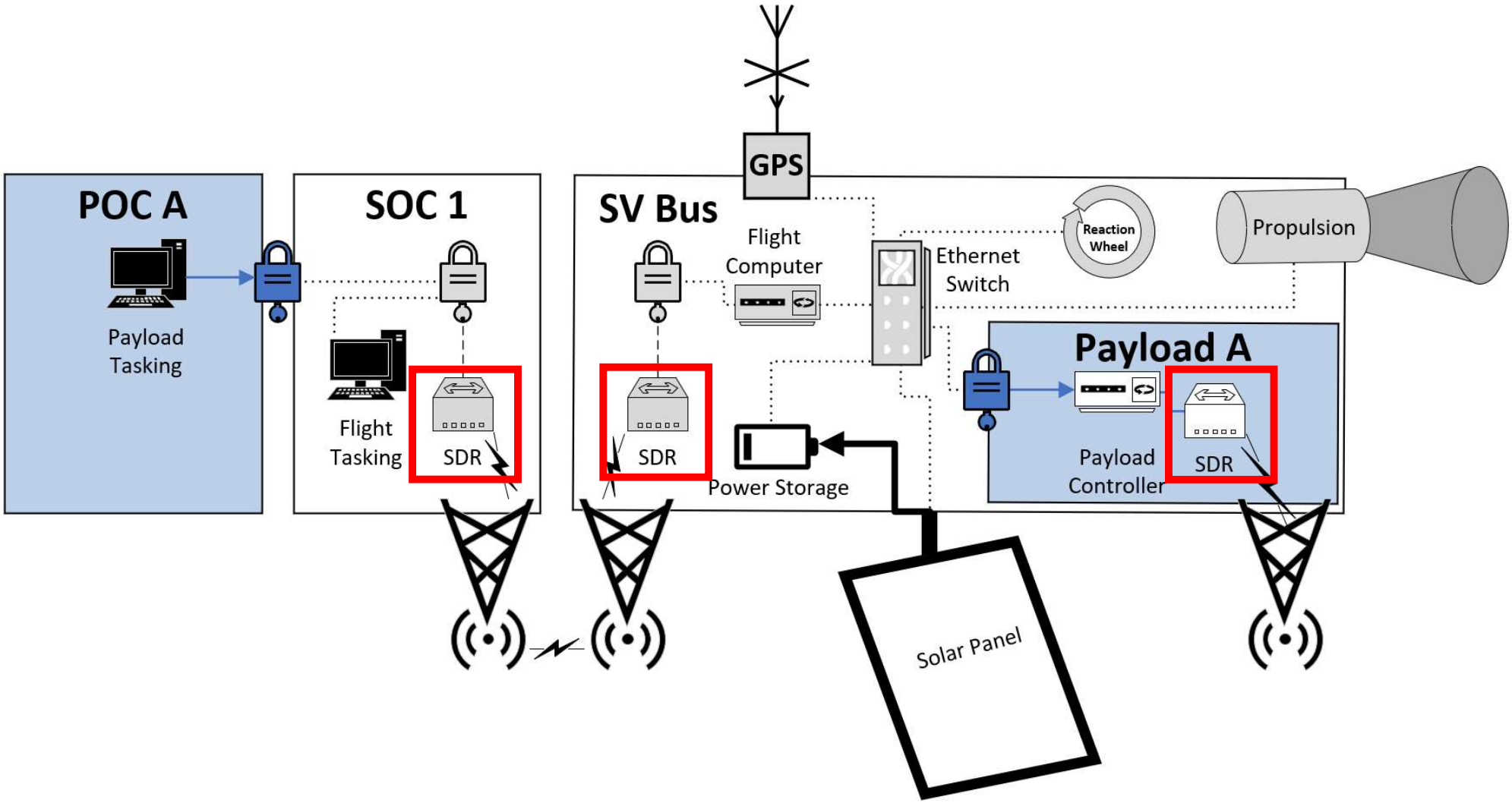
# What’s in the Box?

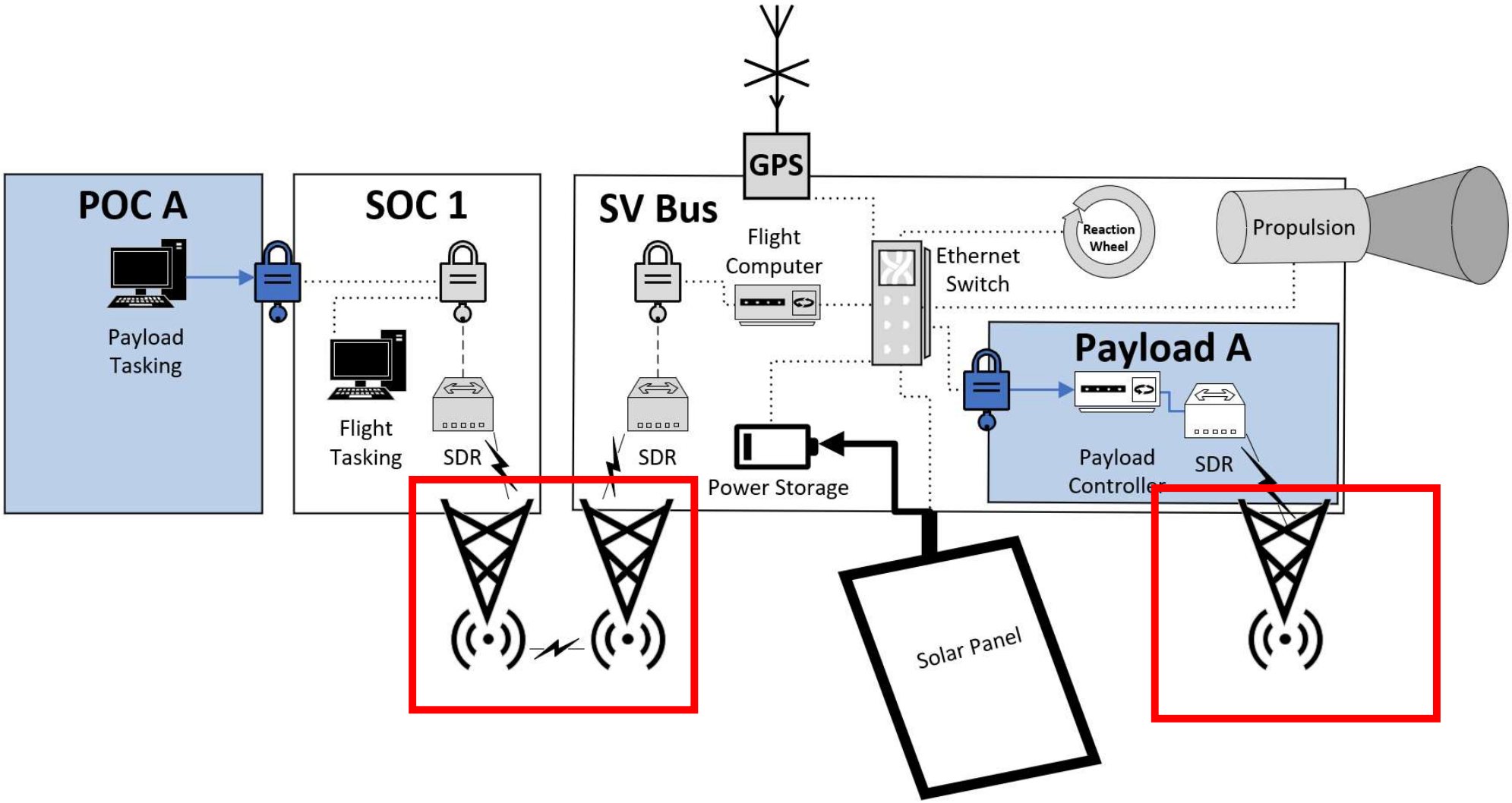

EARTH
SPACE
POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
GPS
SV Bus
Flight
Computer
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
SDR
Power Storage
Solar Panel

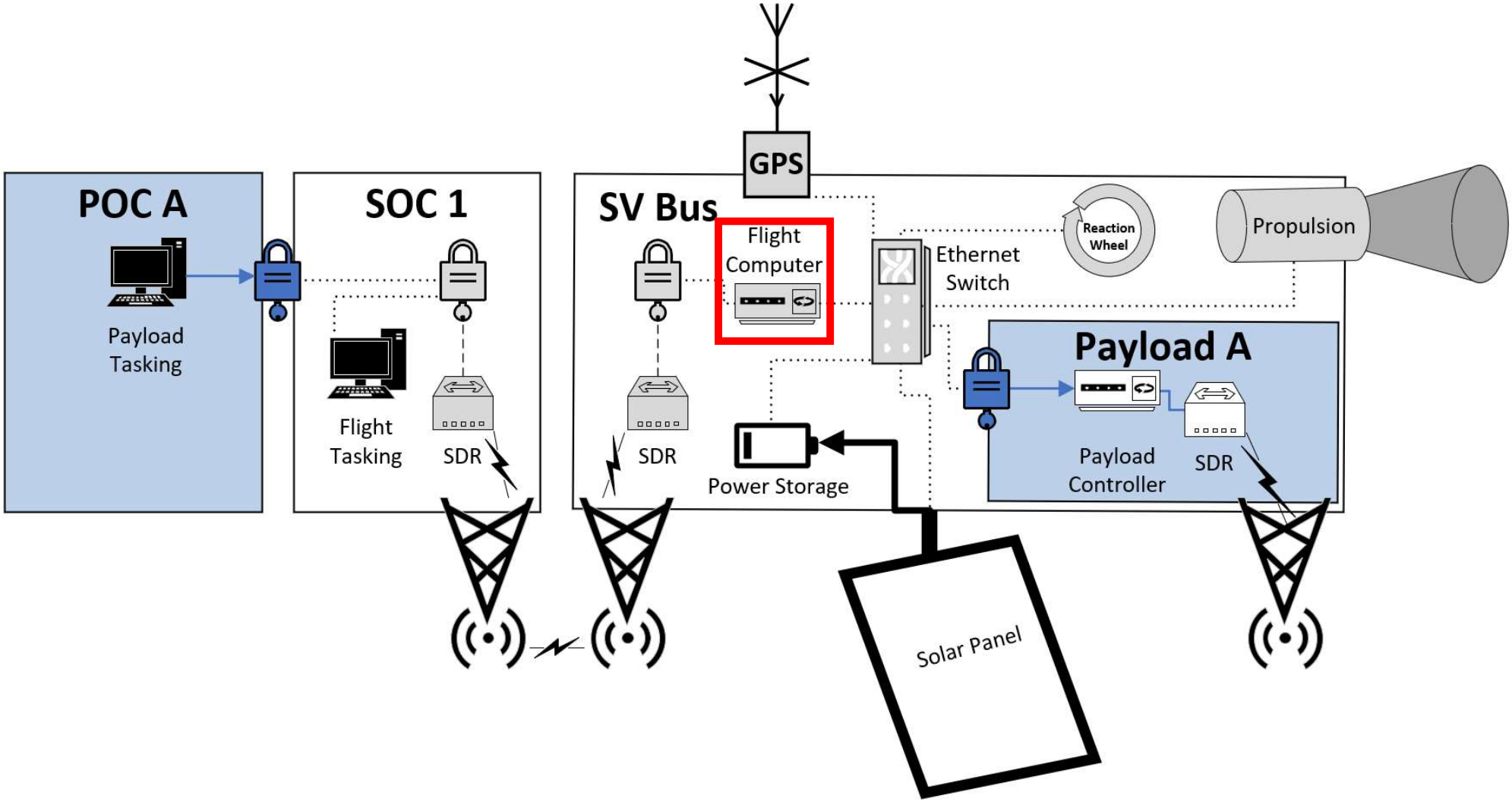

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
GPS
SV Bus
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel

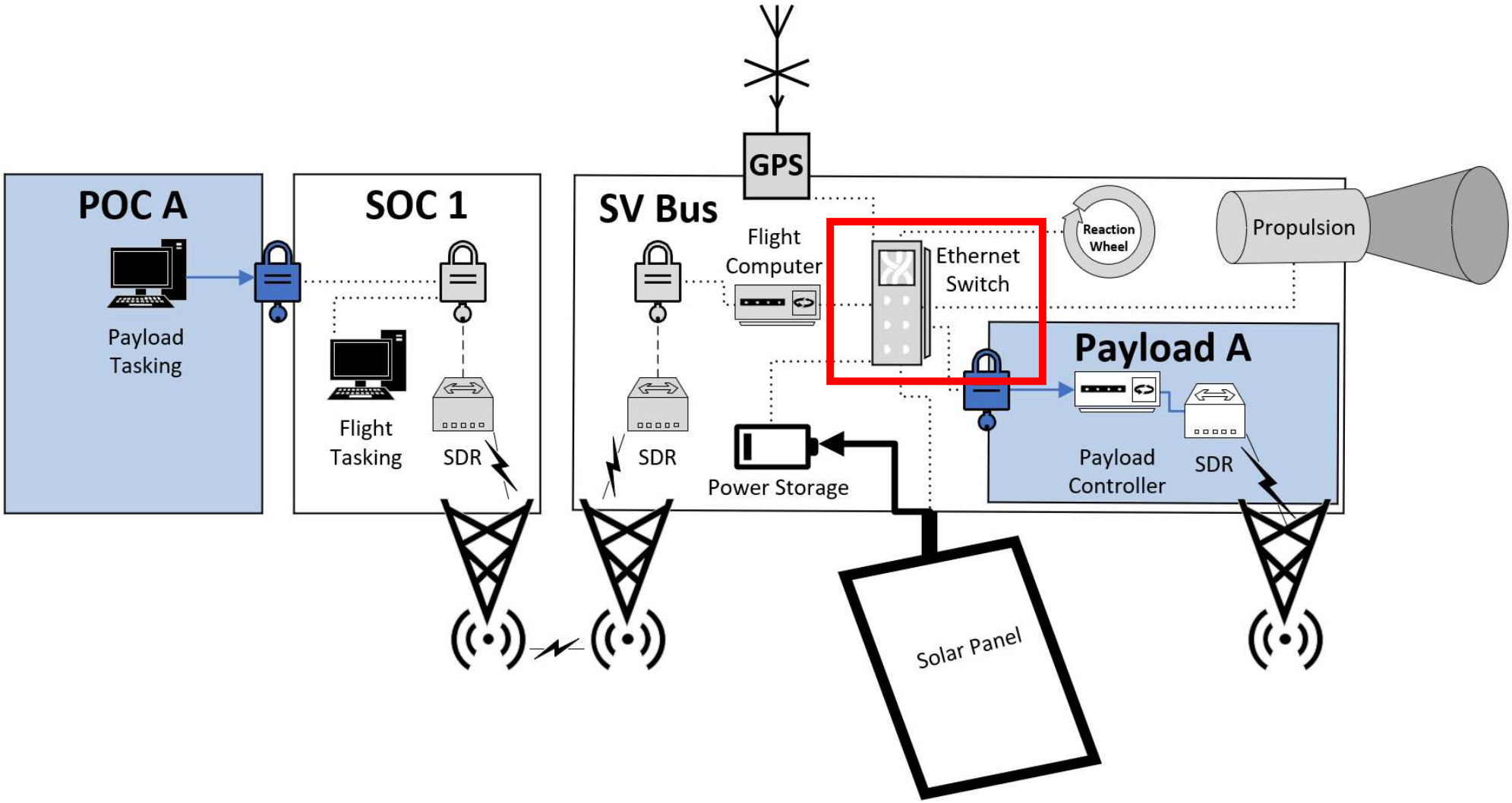

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
GPS
SV Bus
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel

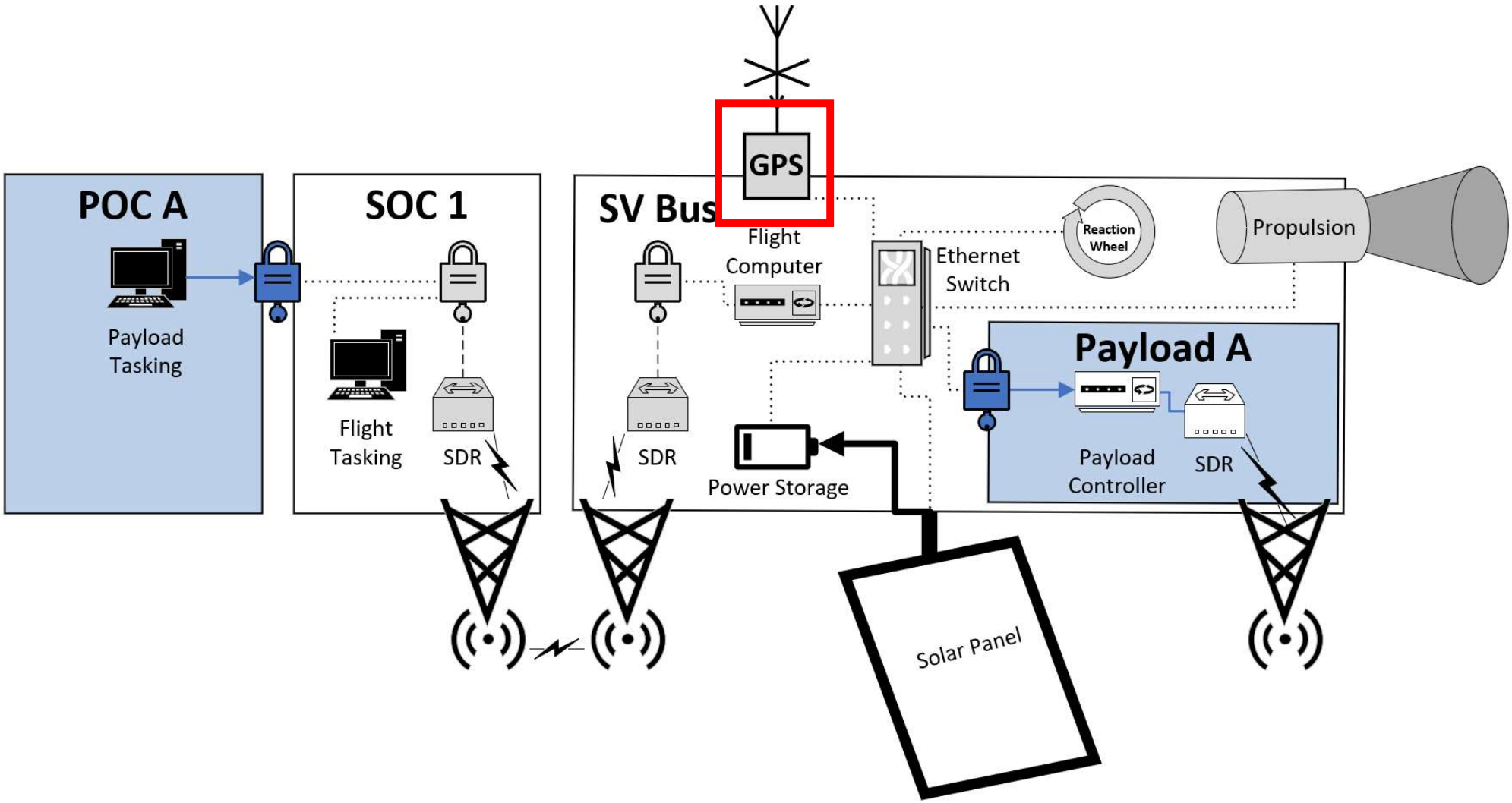

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
SDR
GPS
Flight
Computer
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Power Storage
Solar Panel

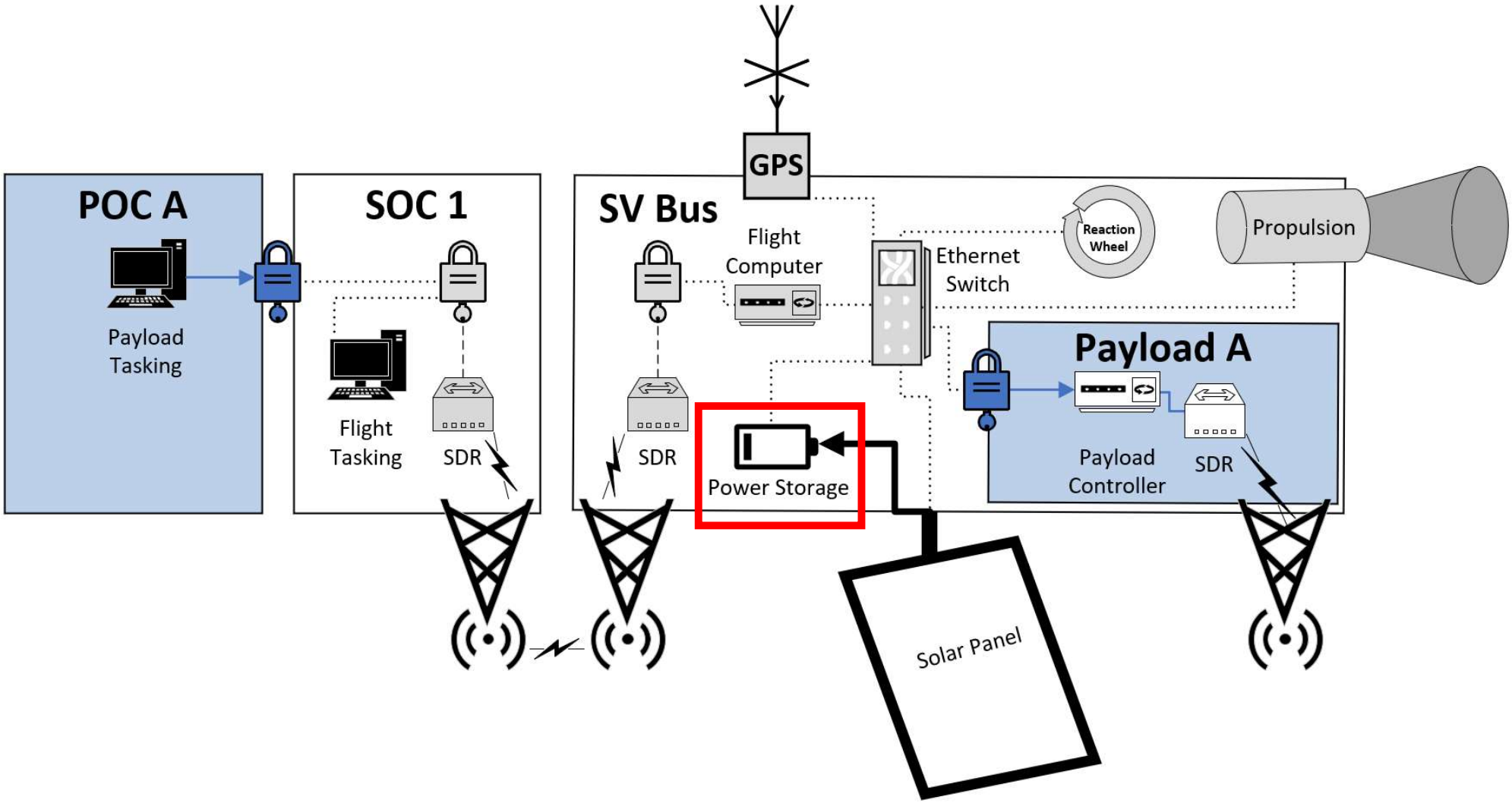

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel

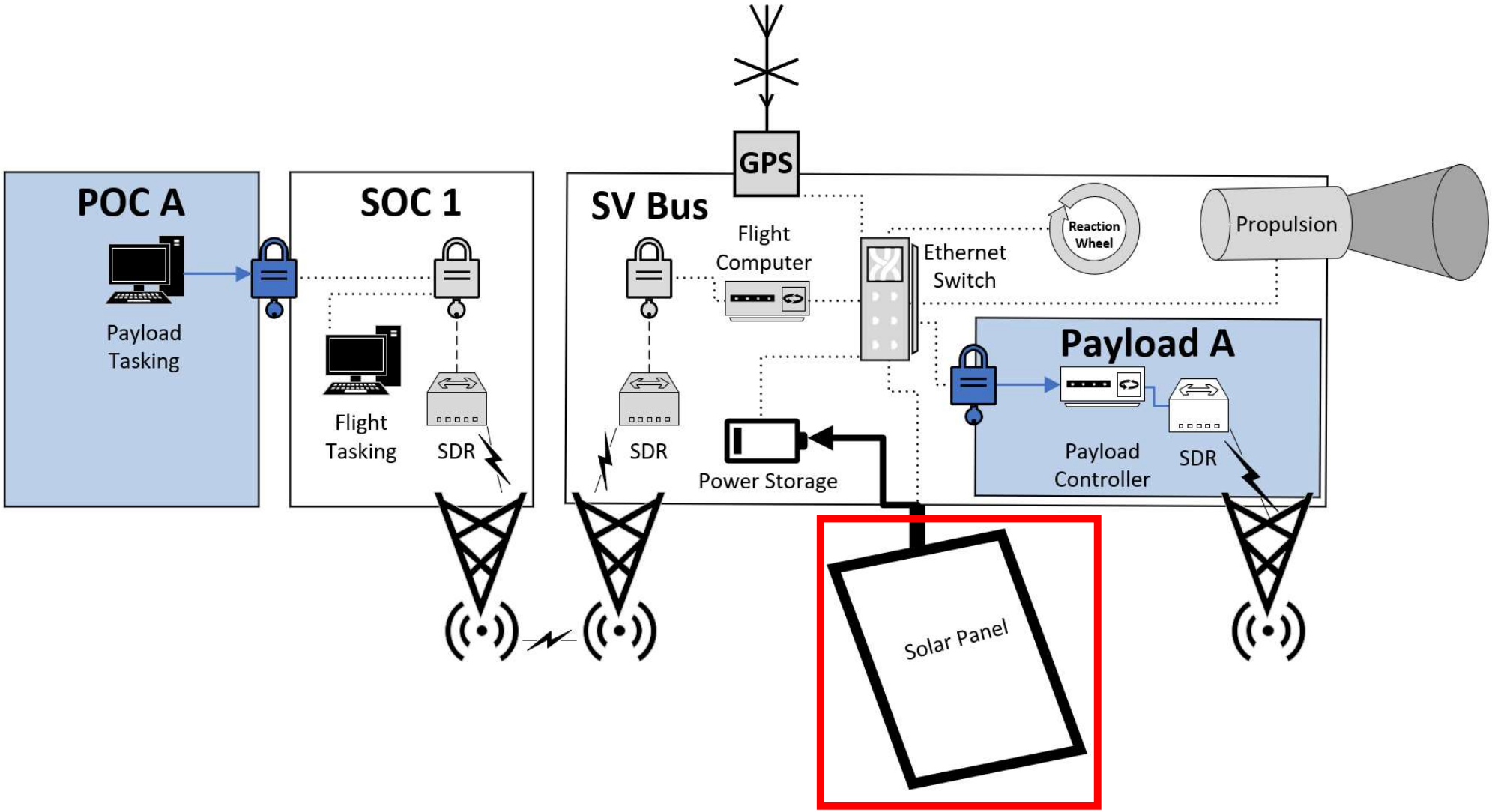

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel

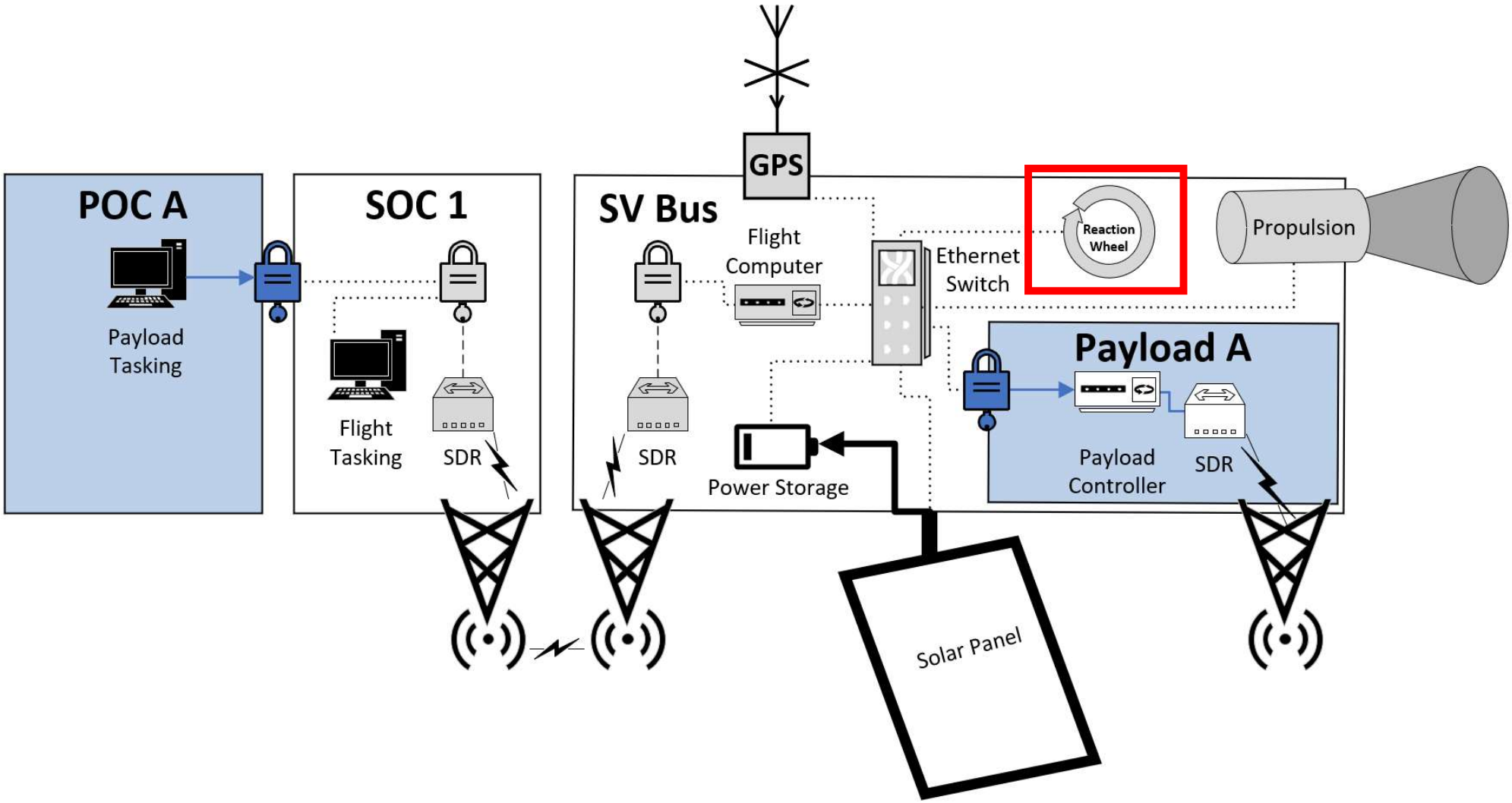

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel

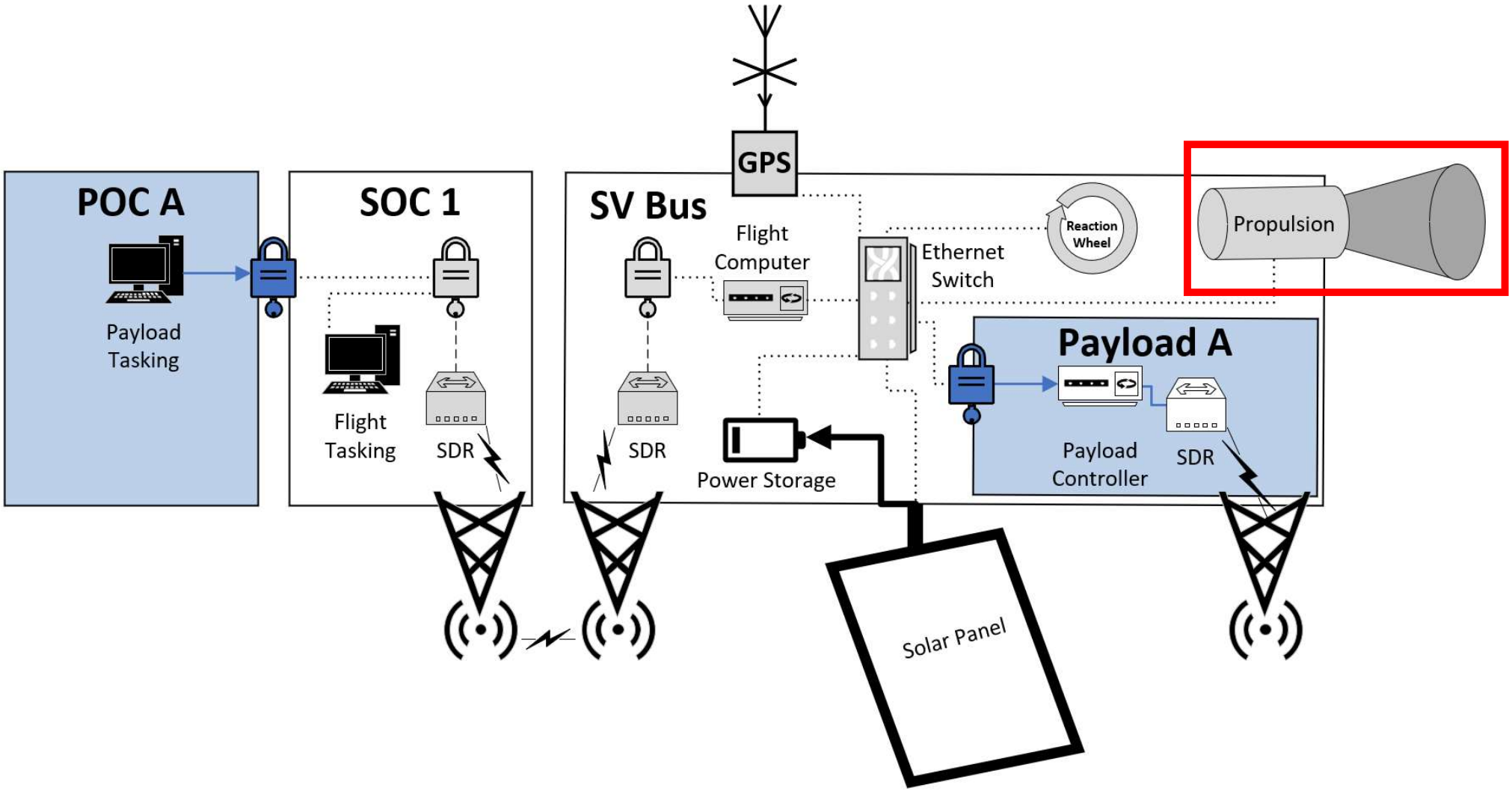

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
Ethernet
Switch
Reaction
Wheel
Propulsion
SDR
Power Storage
Payload A
Payload
Controller
SDR
Solar Panel

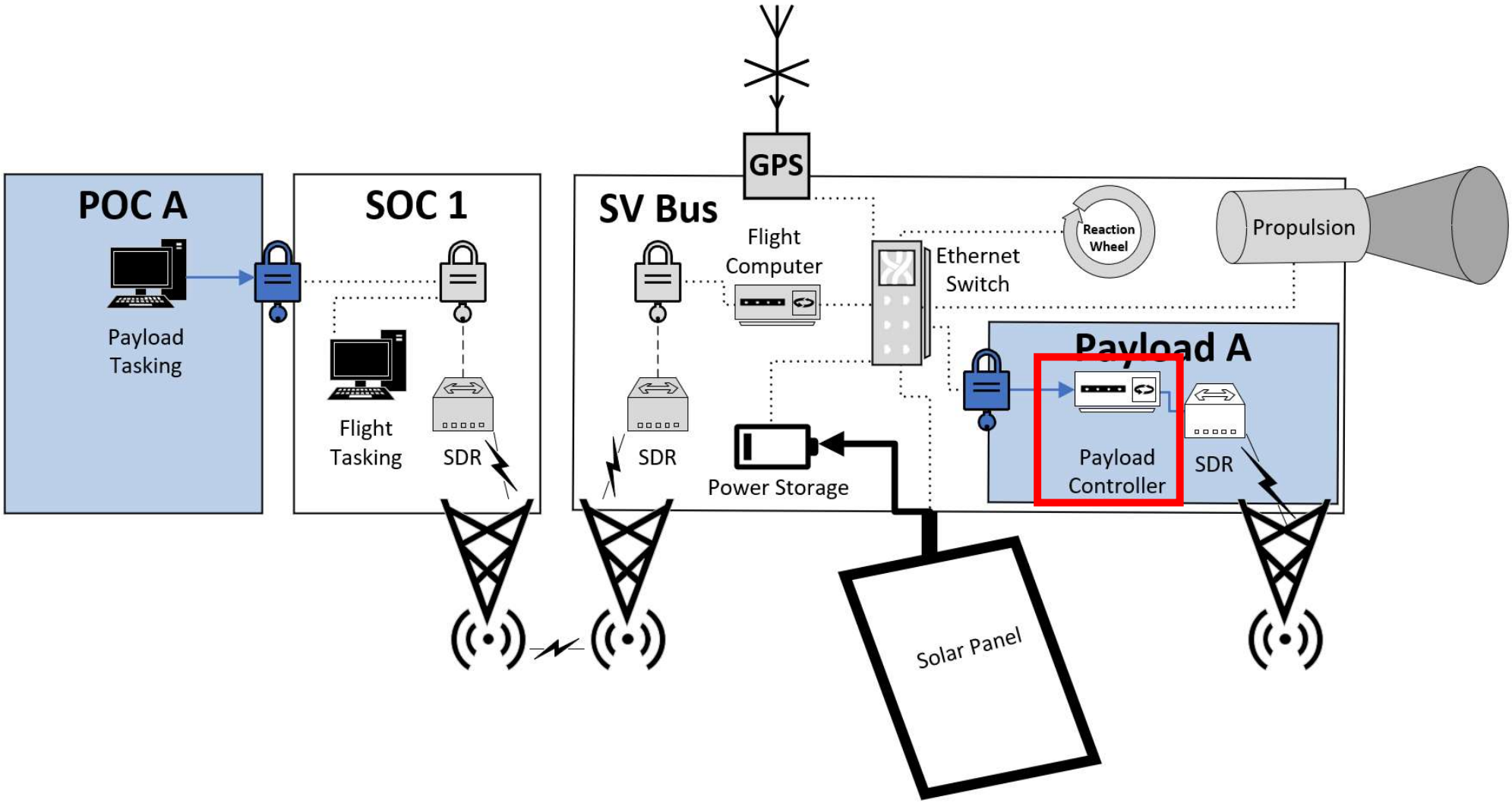

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel


POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
GPS
SV Bus
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel


POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel


POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel

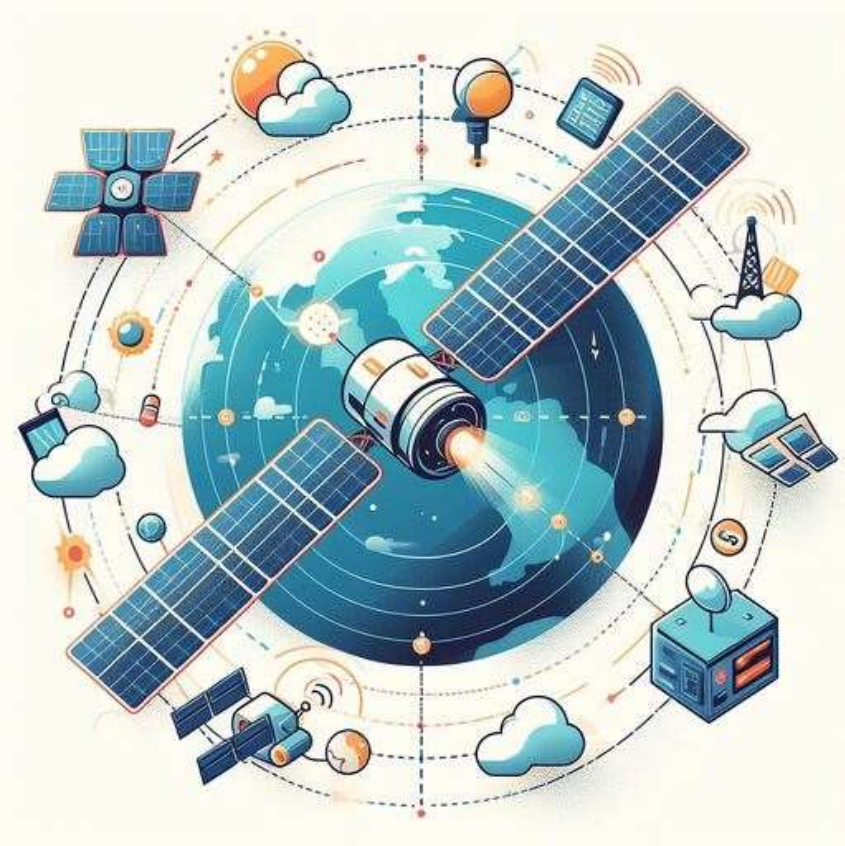

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
Ethernet
Switch
Reaction
Wheel
Propulsion
SDR
Power Storage
Payload A
Payload
Controller
SDR
Solar Panel

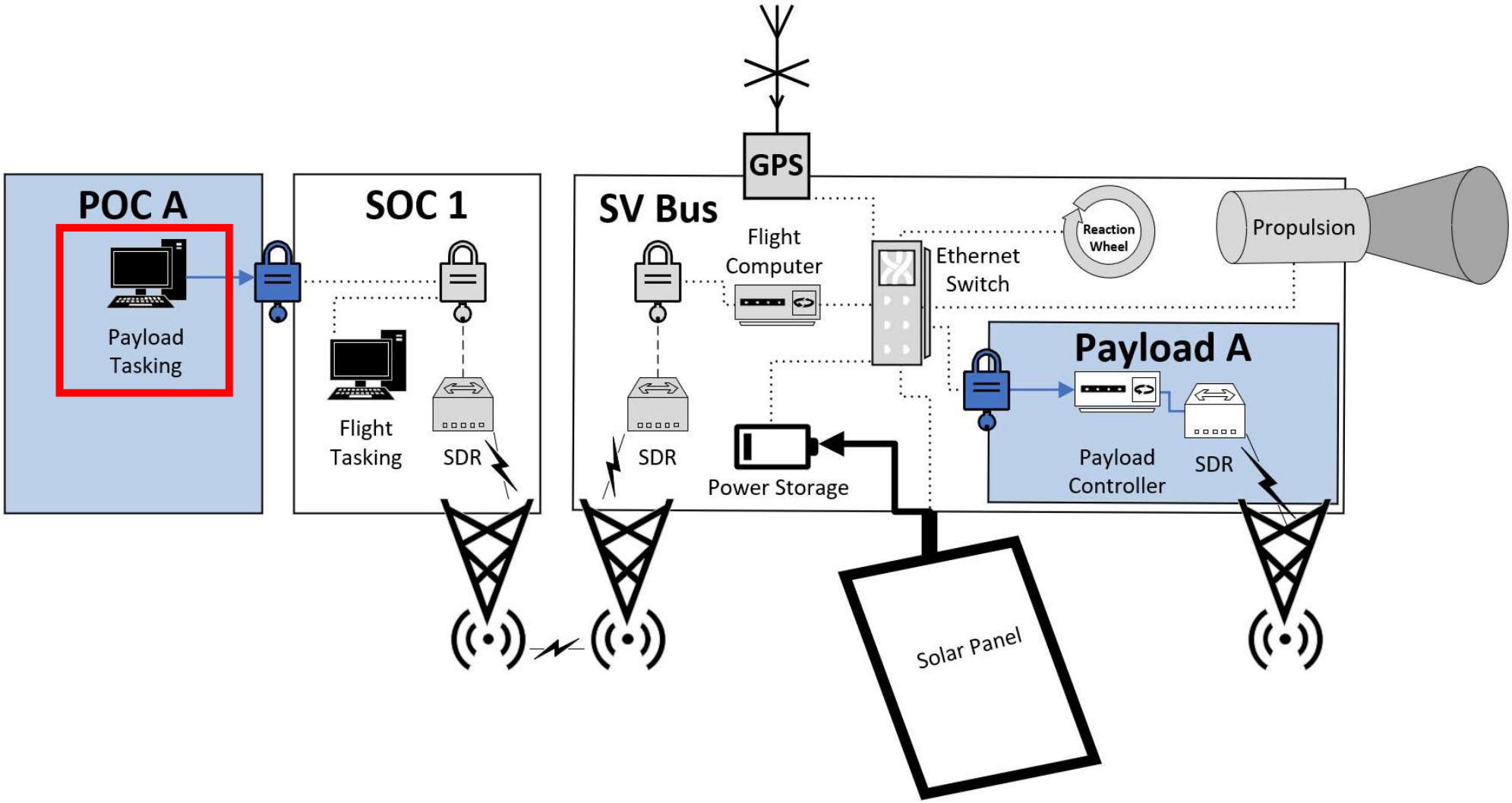

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
Ethernet
Switch
Reaction
Wheel
Propulsion
SDR
Power Storage
Payload A
Payload
Controller
SDR
Solar Panel

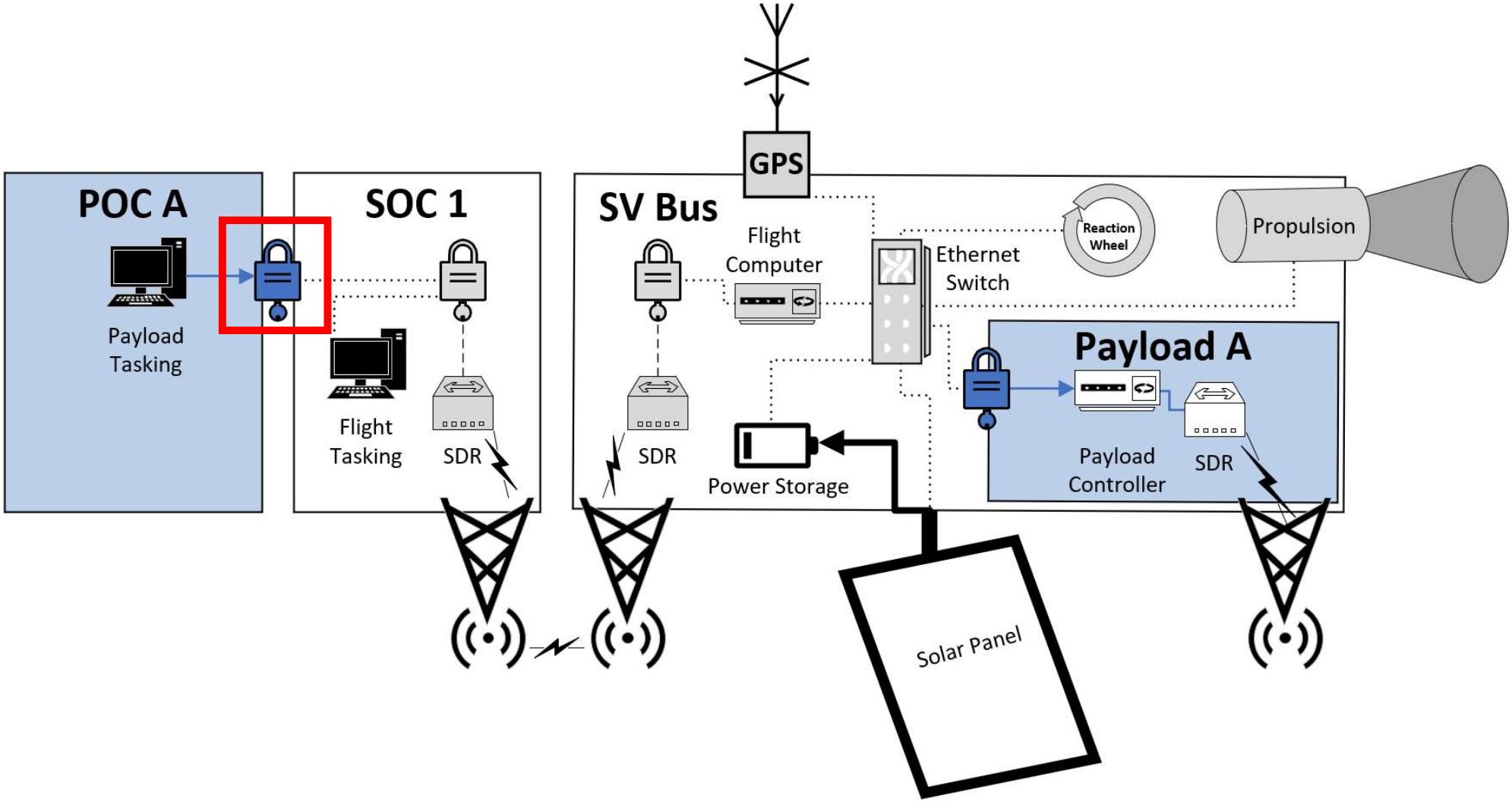
# Components

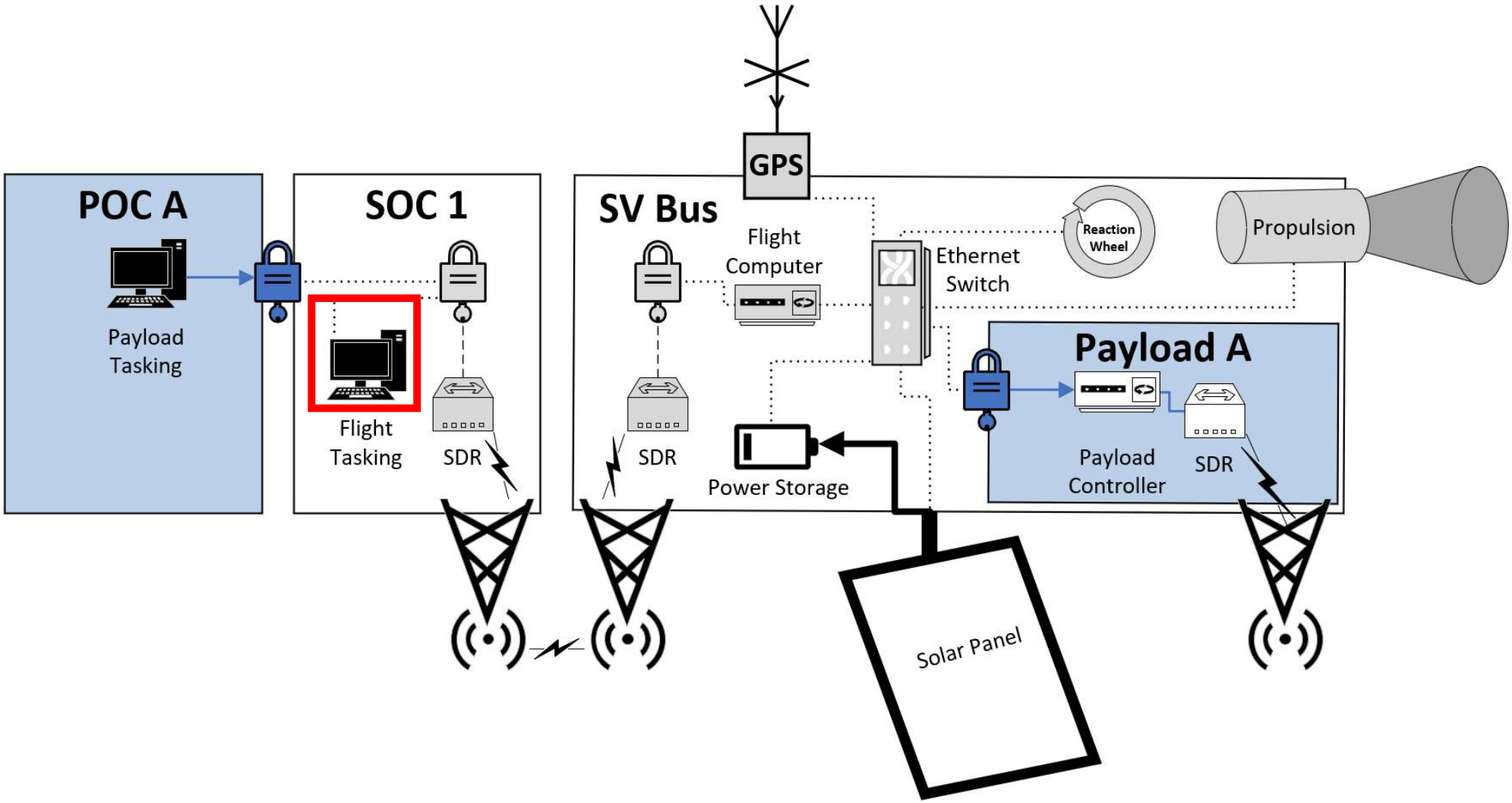
- Logic Bearing
  - SDRS
  - Flight computer
  - Encryption devices
- ‘Dumb’
  - Reaction Wheels
  - Propulsion
  - Antennae
  - Solar panels

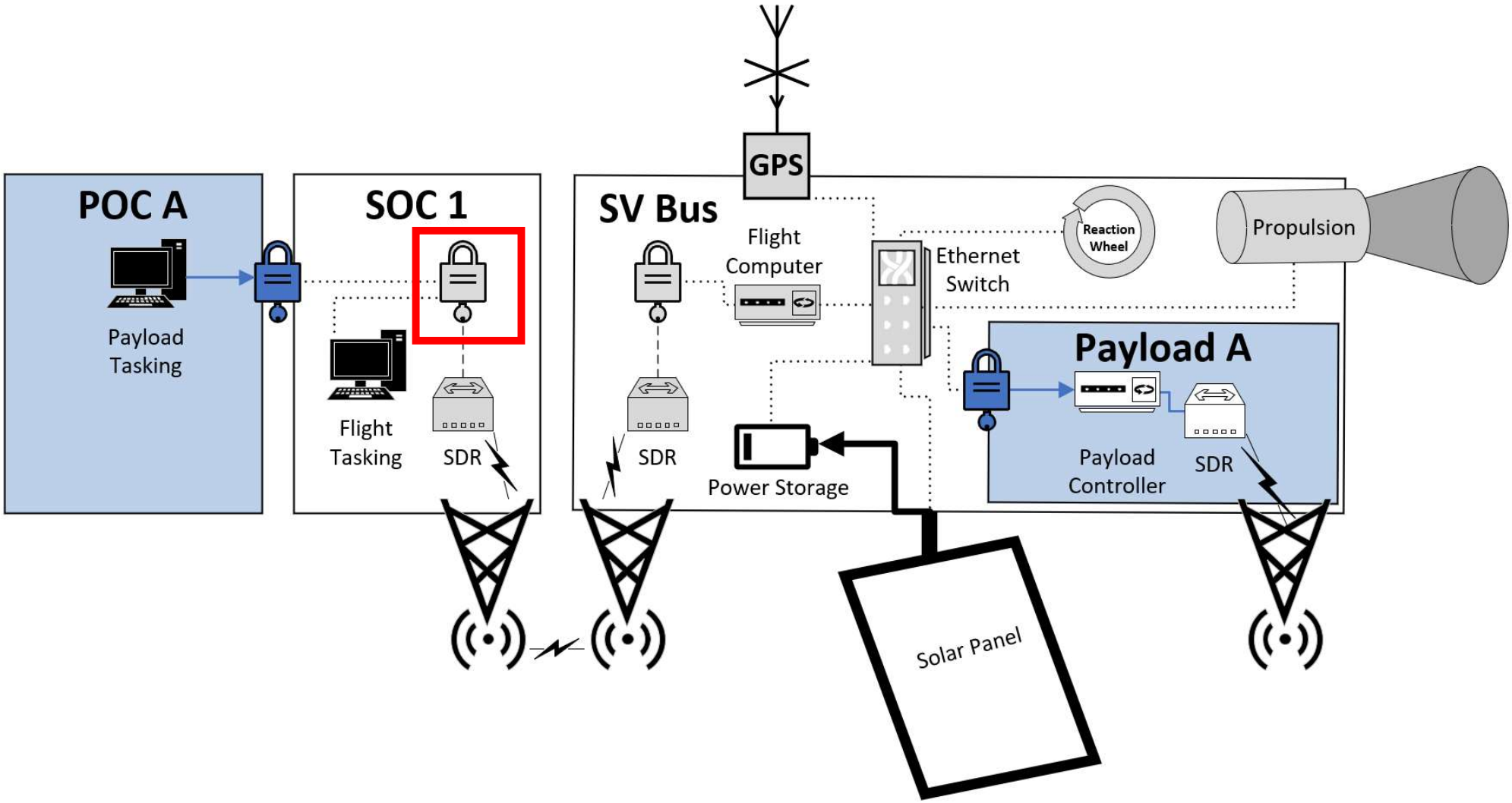
# CONOPS

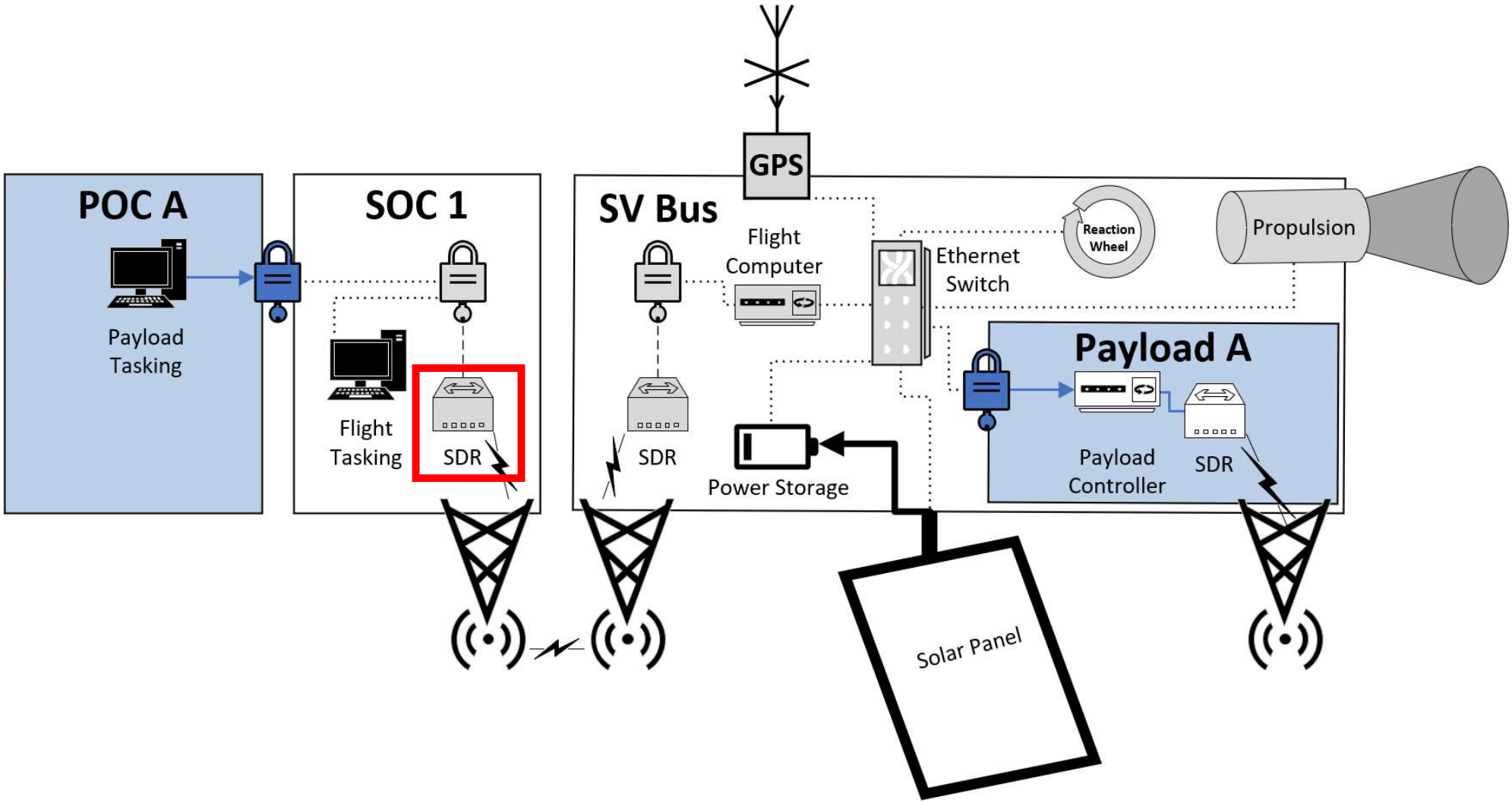


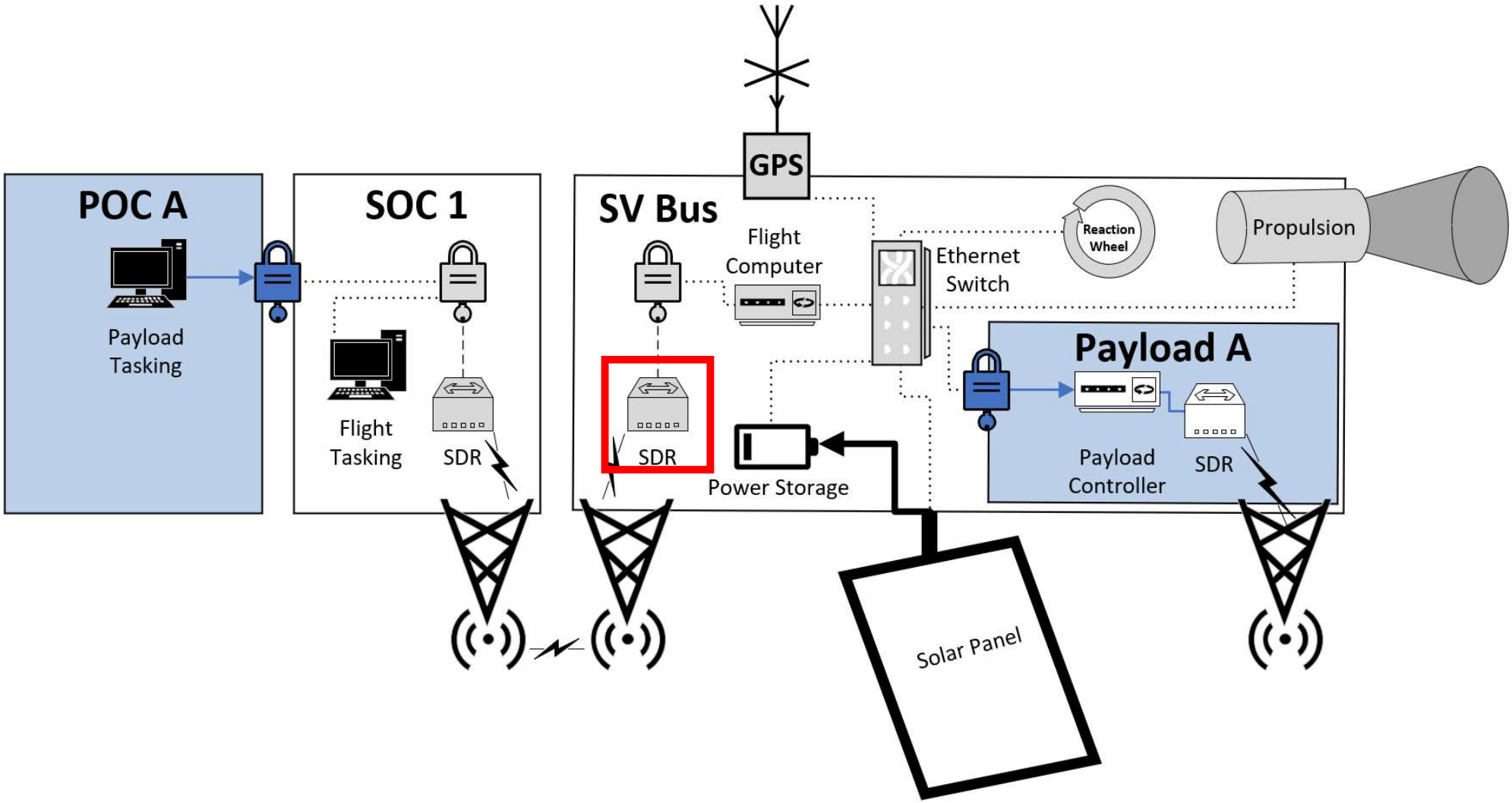

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
GPS
SV Bus
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel

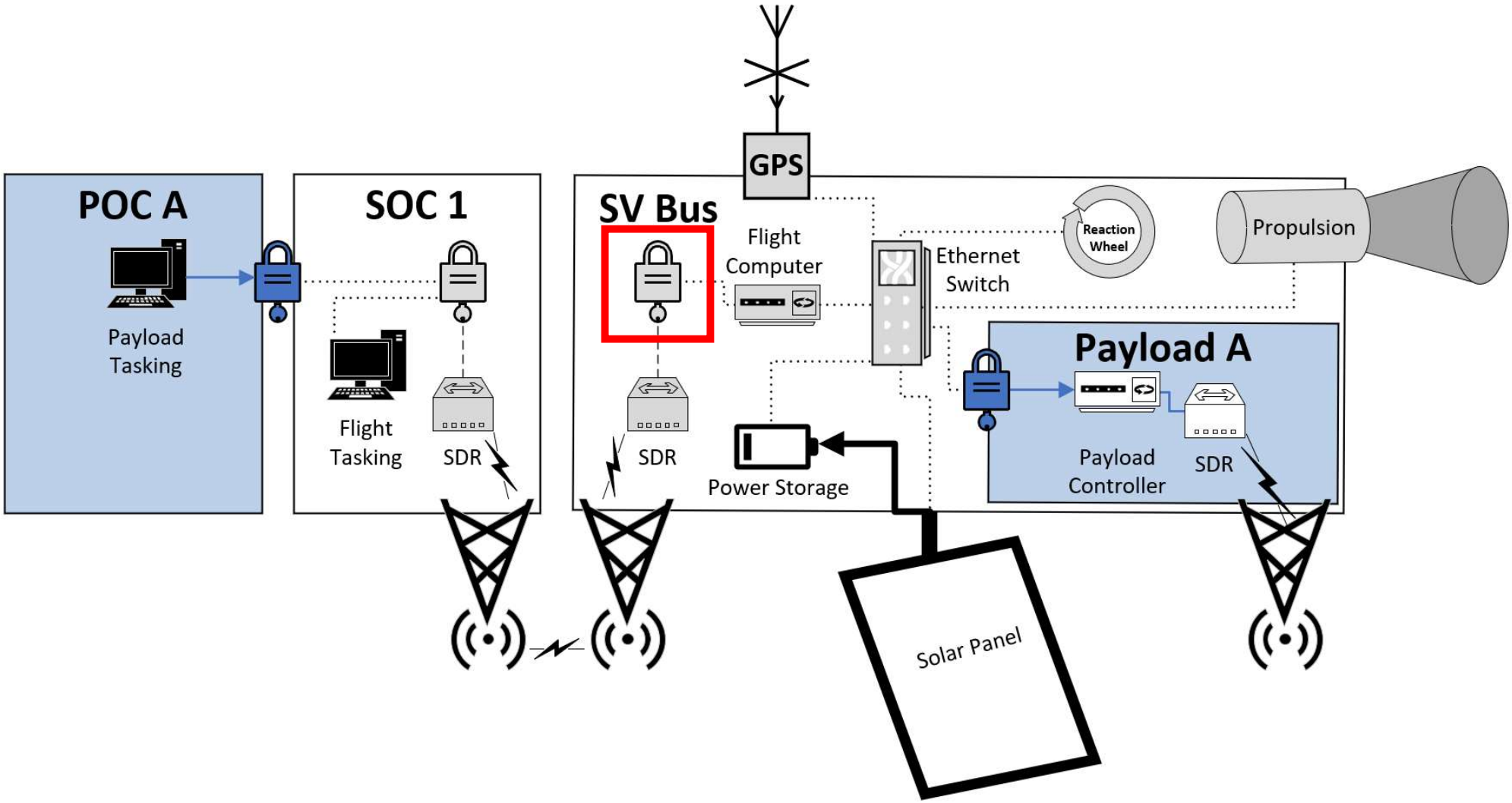

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
Ethernet
Switch
Reaction
Wheel
Propulsion
SDR
Power Storage
Payload A
Payload
Controller
SDR
Solar Panel

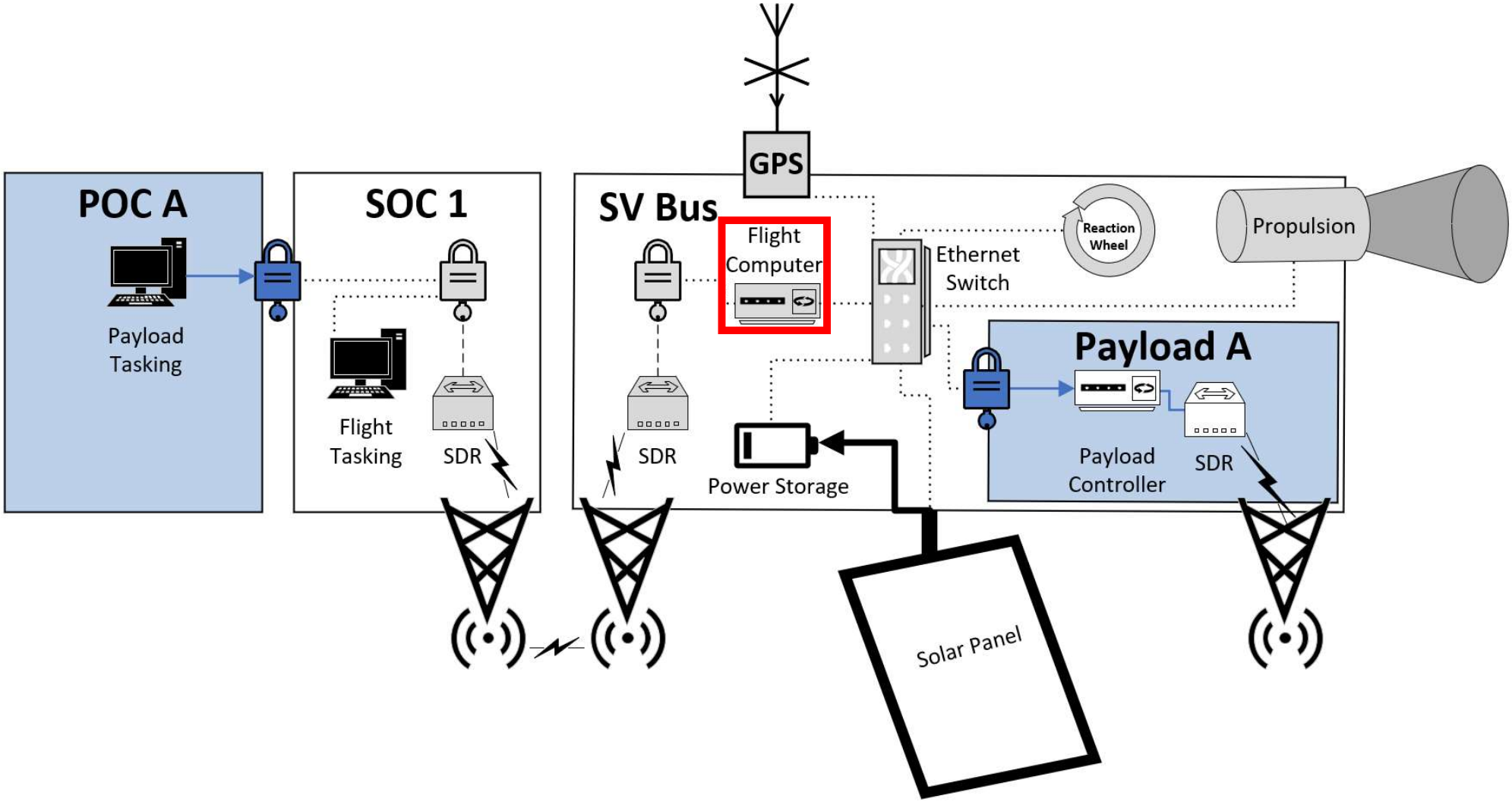

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
Ethernet
Switch
Reaction
Wheel
Propulsion
SDR
Power Storage
Payload A
Payload
Controller
SDR
Solar Panel

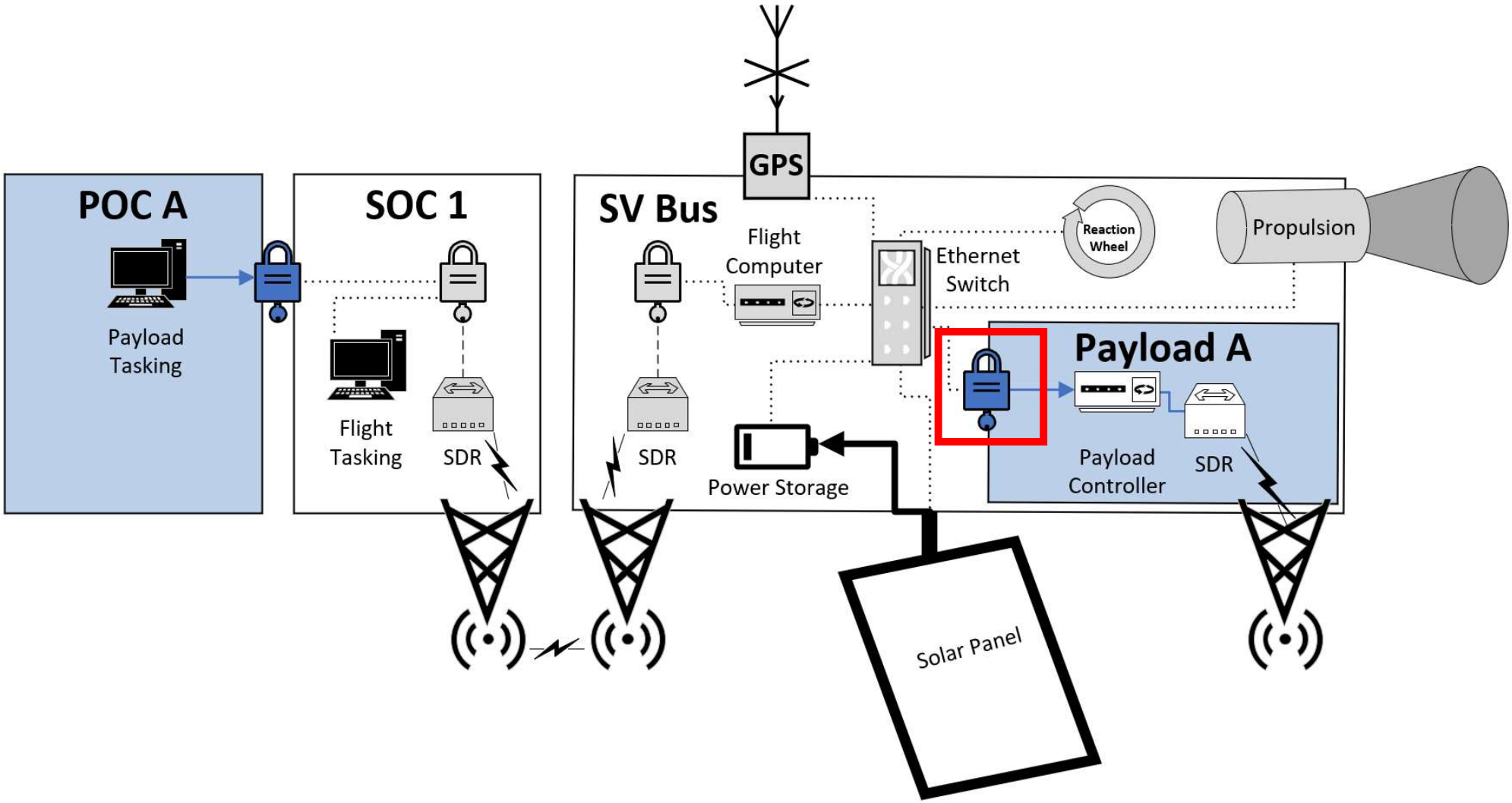

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
GPS
SV Bus
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel

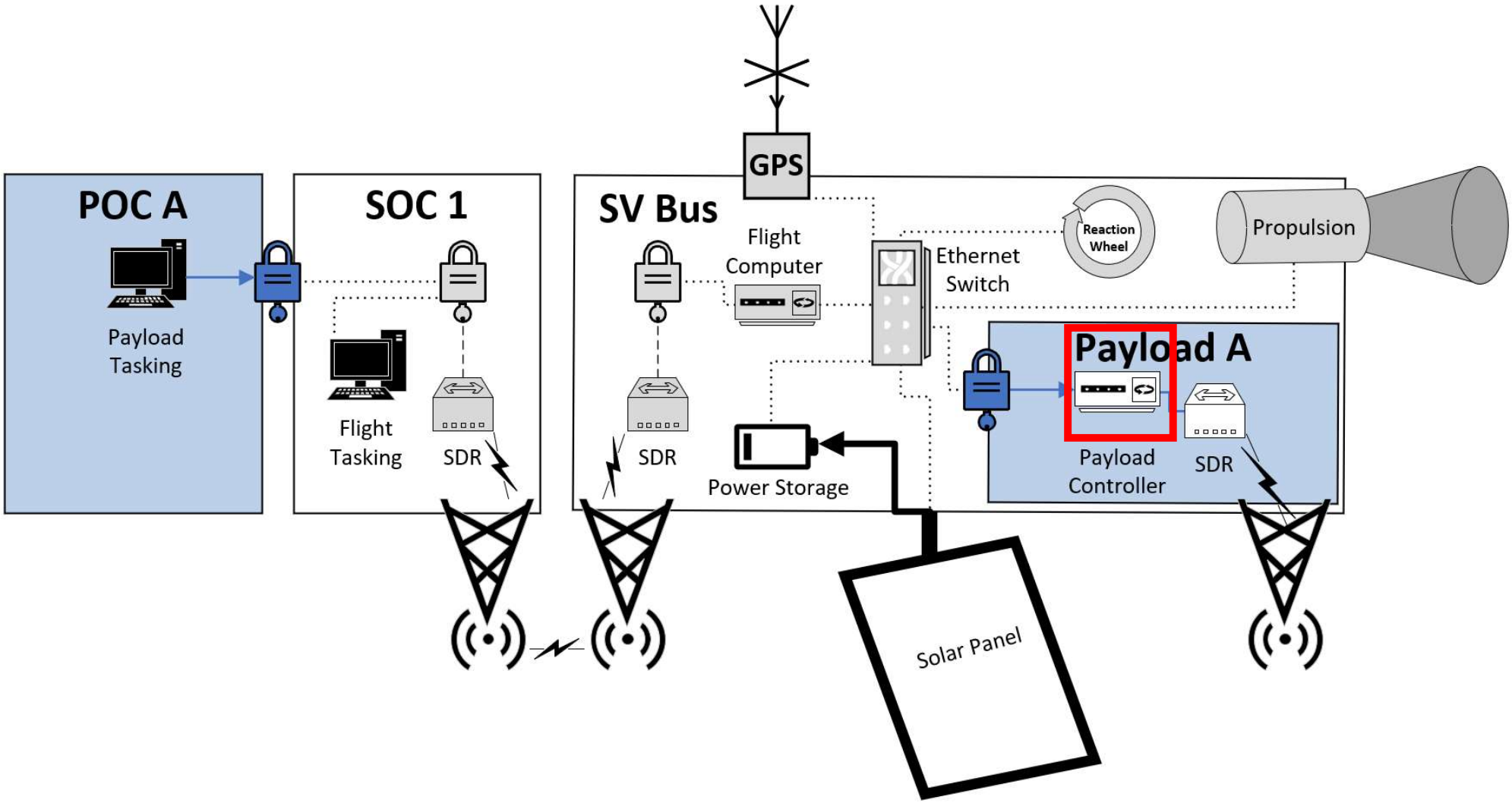

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
GPS
SV Bus
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel

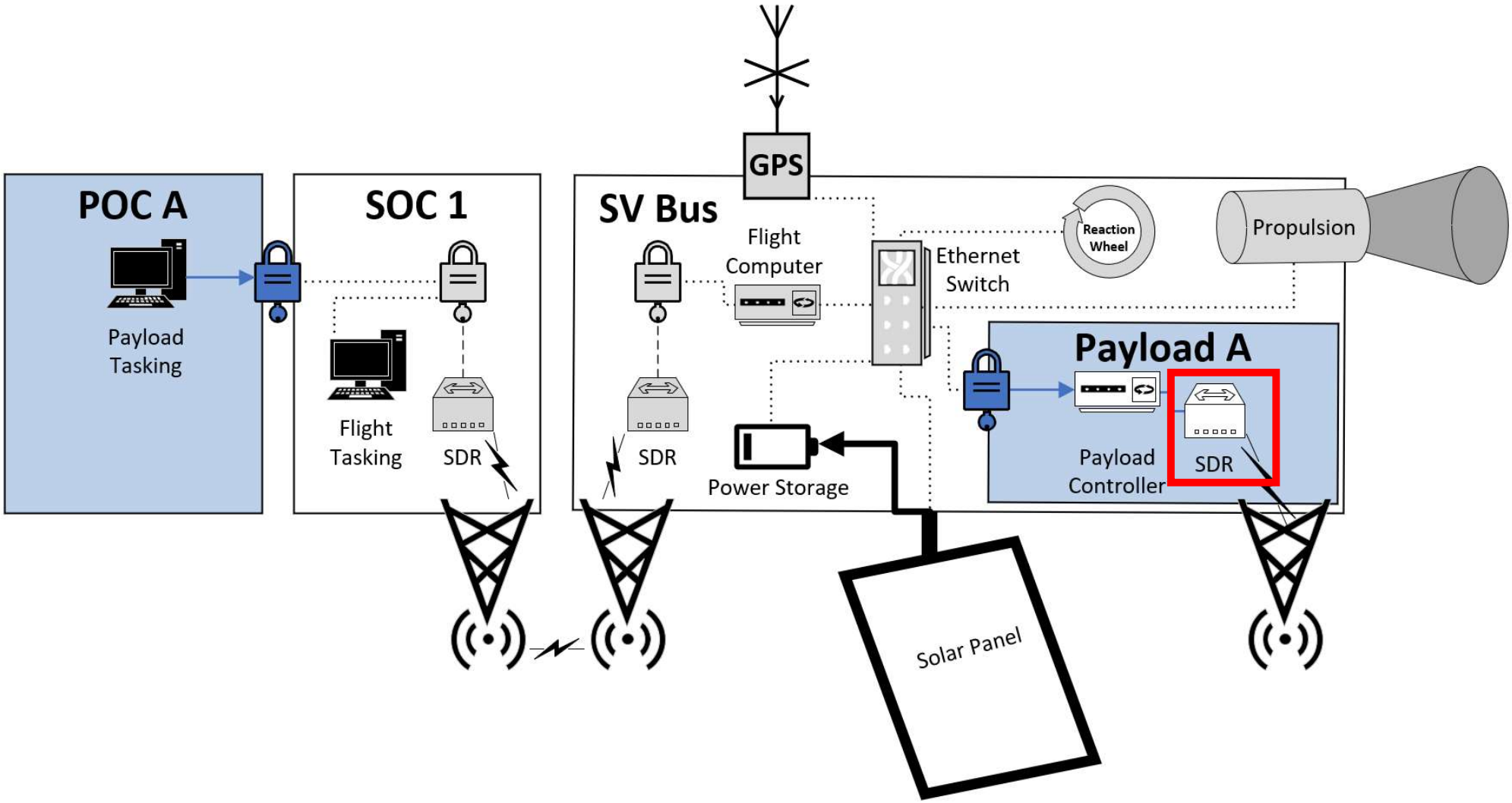

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel


POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
SDR
GPS
Flight
Computer
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel

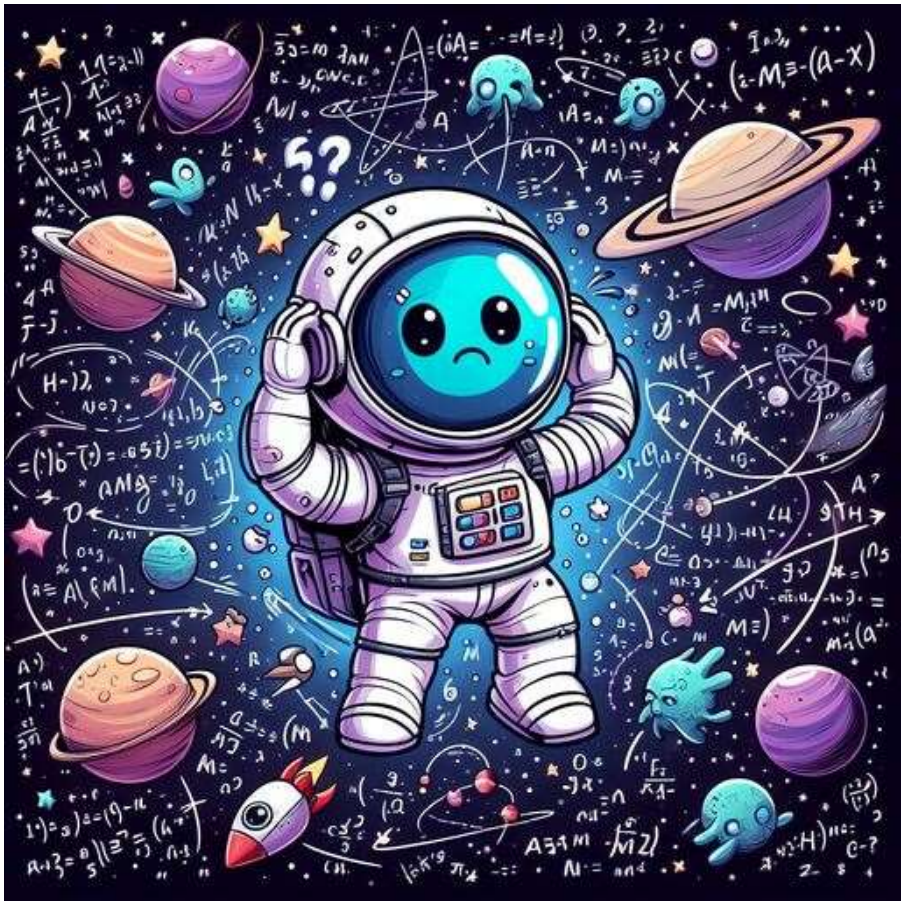

POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel


POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
GPS
SV Bus
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel


POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel


POC A
Payload
Tasking
SOC 1
Flight
Tasking
SDR
SV Bus
GPS
Flight
Computer
SDR
Power Storage
Ethernet
Switch
Reaction
Wheel
Propulsion
Payload A
Payload
Controller
SDR
Solar Panel

# Space Is Like…Really Hard…



# Hayabusa

- May 9th, 2003, Japan launches the satellite that will eventually be renamed to Hayabusa with the intention of sampling surface material from a small asteroid and bringing it back to Earth. Something that had never been done before.

# Hayabusa

- In late 2003, a large solar flare significantly damaged its solar panels, delaying its intended 2005 arrival at the asteroid by several months.

# Hayabusa

- In July 2005 one of three reaction wheels (the x-axis controller) used to adjust the satellite's attitude, fails.
- In October 2005 another reaction wheel fails (the y-axis controller), forcing it to use the one remaining reaction wheel and some of its thrust to fly and steer.

# Hayabusa

- On November 12, 2005, the satellite's small lander vehicle was launched at an incorrect altitude and flew off into space.
- November 19, 2005, the satellite itself tried at landing on the asteroid, but bounced and lost contact. Eventually contact was restored and it left the asteroid surface after 30 minutes.

# Hayabusa

- November 25, 2005, the satellite made its second landing, attempting to fire its two sampling bullets, which both failed.
- December 2005, a thruster leak alters the direction of the antennae and connection is lost for three months.
- Use of Backup antenna results in 1000x slower communications, protocol re-engineering made bandwidth usable

# Hayabusa

- Hayabusa limped back to Earth with:
  - 10-100x slower communications due to damaged primary antenna
  - No chemical fuel
  - A small portion of its solar panels powering a limited thrust ion thruster,
  - Only 1 out of 3 reaction wheels still functioning
  - 4 of the 11 batteries on board not functioning.