Use of STPA In Satellite Hazard Analysis: NASA/JAXA GPM and Payload Safety

Connor Dunn
Masters Candidate
MIT Aero/Astro

Massachusetts Institute of Technology

Outline

- Motivation for Research
- Background: NASA/JAXA GPM
- STPA Case Study: NASA/JAXA GPM with focus on Payload

Motivation for Research

- Provide a template for future space vehicle/satellite STPA analyses
- Examine treatment of modular payloads with STPA
  - Goal: minimize rework required for safety analysis

Global Precipitation Measurement (GPM) Satellite

- Precipitation measurement satellite (TRMM replacement) to serve as the reference data source for a constellation of existing and future precipitation satellites
- NASA satellite bus and operation (GSFC)
- Ball Aerospace GPM Microwave Imager (GMI) (passive)
- JAXA Ka/Ku Dual-Frequency Precipitation Radar (DPR) (active) and H-IIA launch vehicle (TNSC)
- Launch 2014 for 3+ year mission

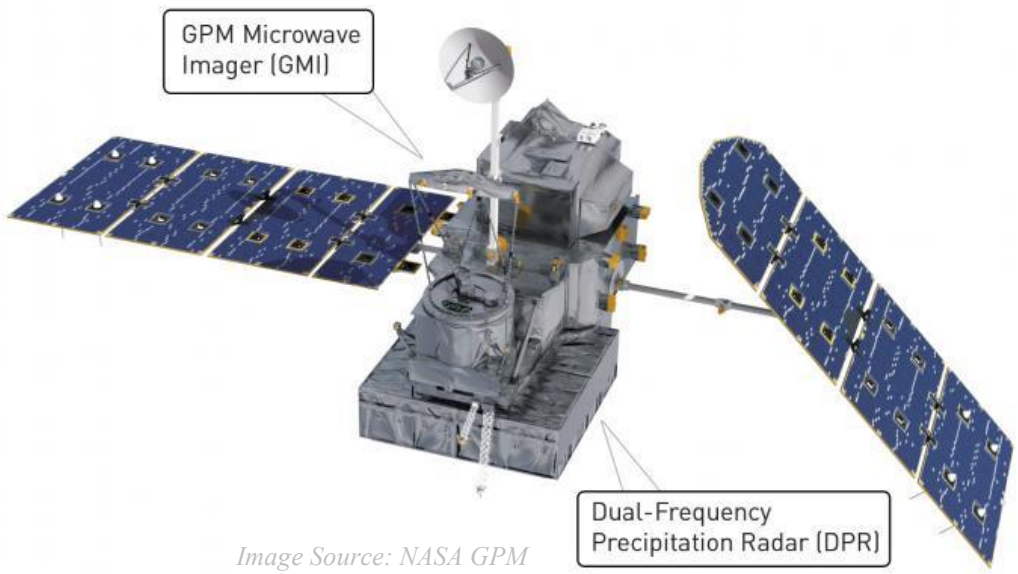


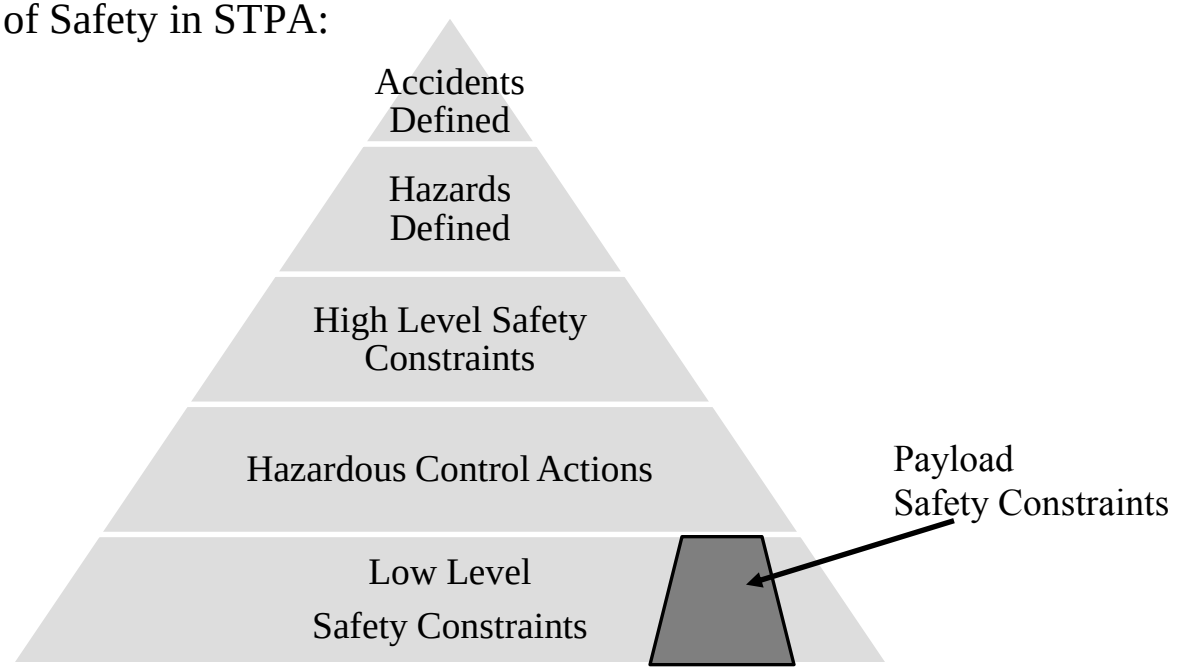
Image Source: NASA GPM

Safety Analysis

- Current PRA based safety analysis for Risk Informed Decision Making (RIDM) is insufficient
  - Reliability not safety
  - Cannot accommodate system abstraction
  - Must repeat PRA analysis for new payloads
- "Limited PRA" done for GPM

Safety Constraints

- Hierarchy of Safety in STPA:



Modularity

- General subsystem classification:

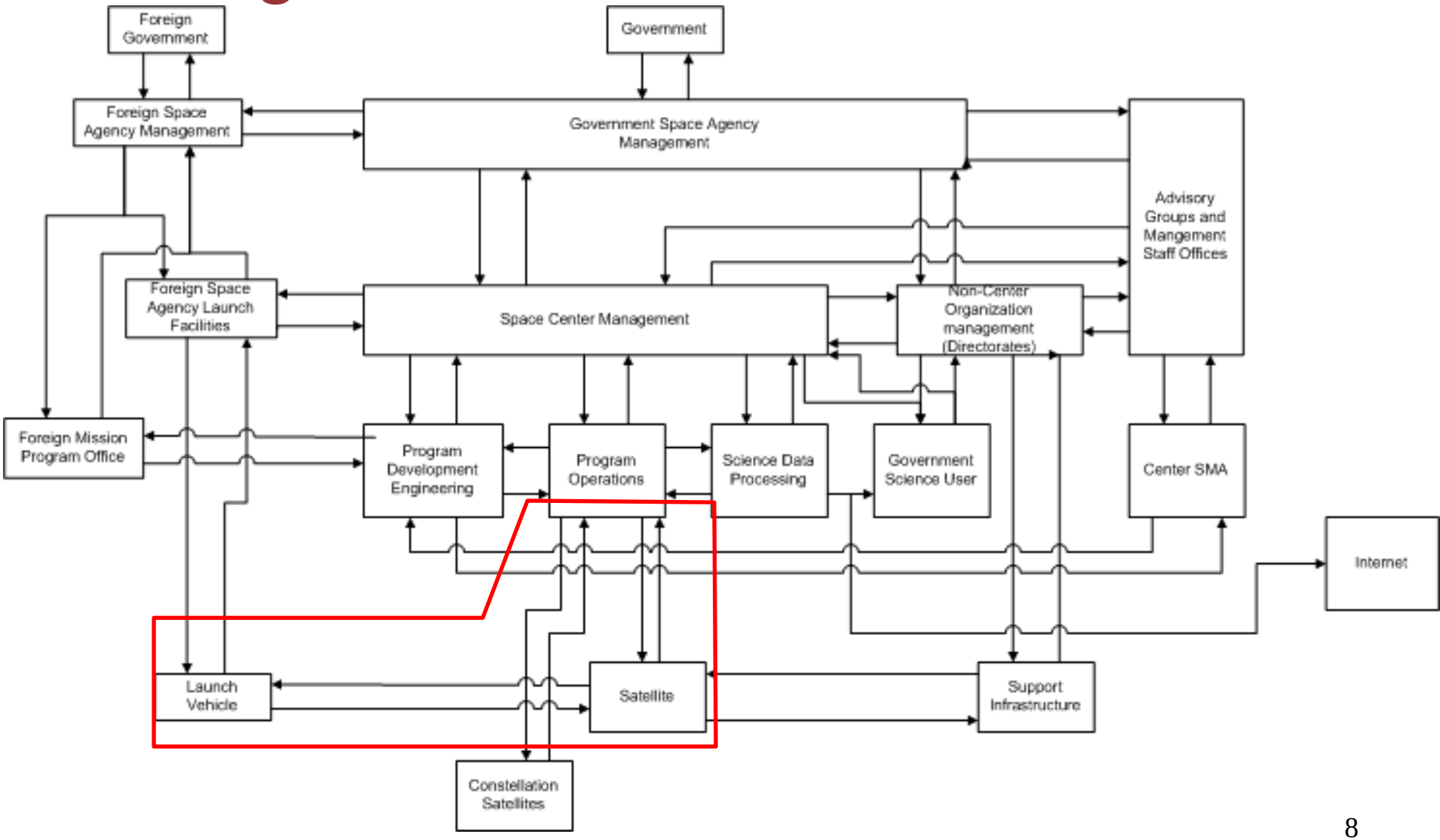
  1) Require no supporting functions, offer supporting functions

  2) Require supporting functions, offer no supporting functions

  3) Require and offer supporting functions

- Satellites are composed of two relatively decoupled functional elements
  - Spacecraft bus (3) - Required for flight and science functions
  - Mission payload (2) - Required for science but not flight functions

High Level Control Structure



Satellite High Level Accidents

Accident	Loss/Accident Description
A1	Humans injured or killed (On earth, in air, in space)
A2	Damage and/or interruption of operations of other systems (Supporting infrastructure, other satellites, all other equipment)
A3	Unplanned damage or disruption of the satellite (LOV)
A4	Mission loss (Unable to perform mission to design standards) (LOM)

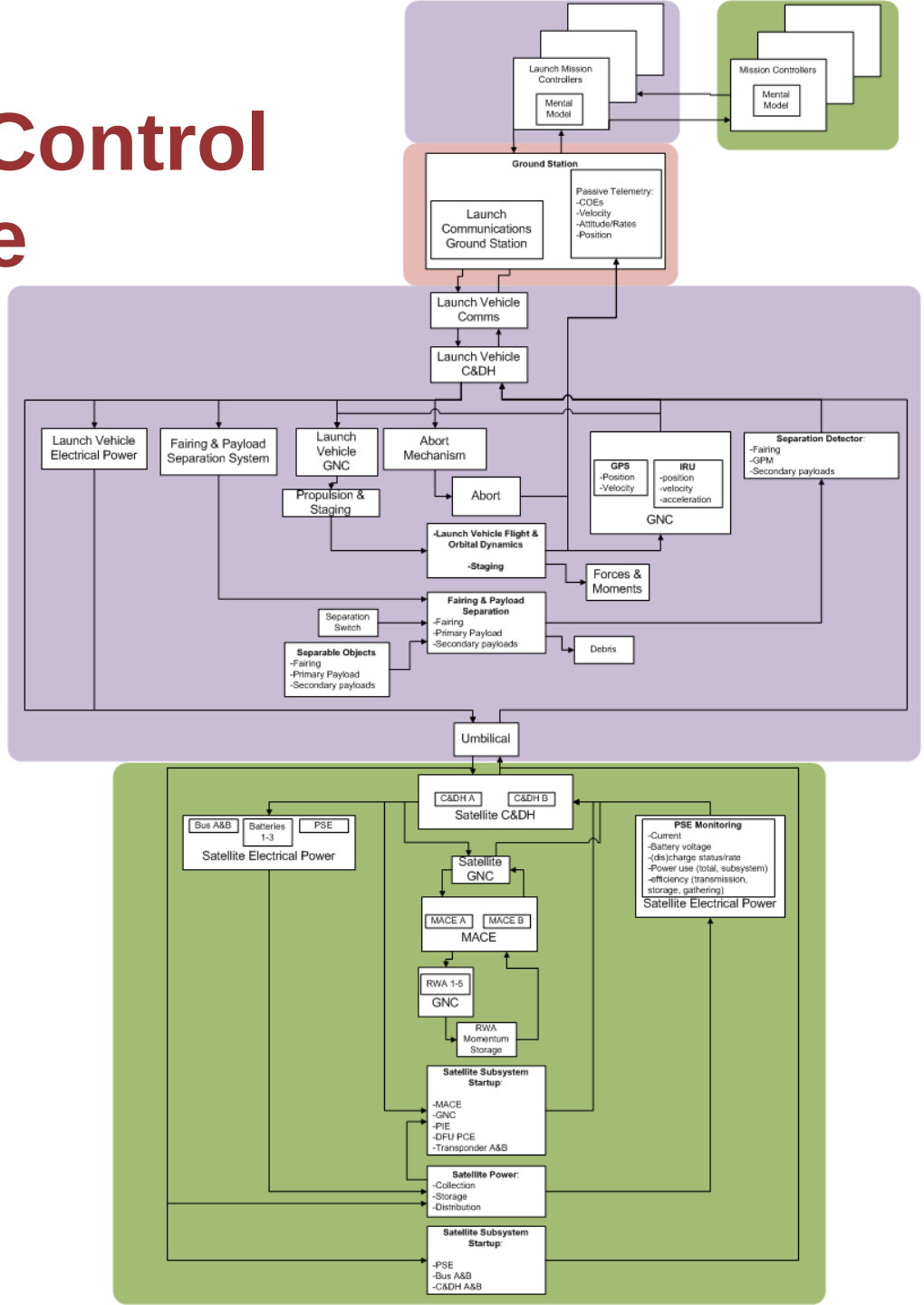
Satellite High Level System Hazards

Hazard	Hazard Description
H1	Humans exposed to radiated energy or to toxic, radioactive, or energetic elements of mission hardware [A1]
H2	Non-human, non-system (the satellite) elements exposed to radiated energy or to toxic, radioactive, or energetic elements of mission hardware [A2]
H3	Satellite hardware exposed to excessive radiation, or caustic or energetic materials [A3]
H4	Satellite enters unsafe environment or orbit/flight path [A3]
H5	Mission science data not gathered, returned, or stored [A4]
H6	Loss of control or communications [A3, A4]

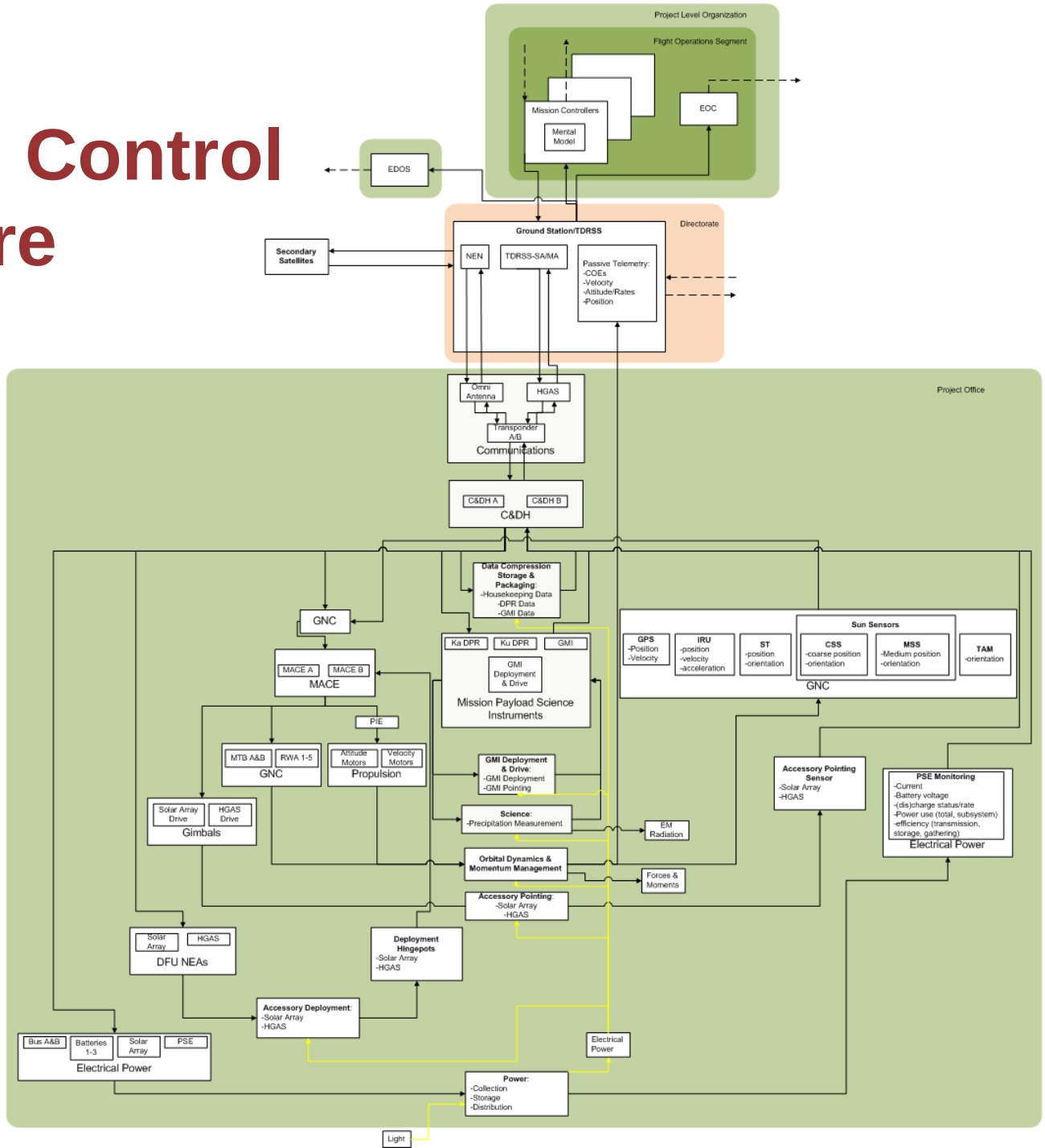
System Safety Requirements/Design Constraints

Requirement	Hazard Description
R1	Radiation and toxic, radioactive, or energetic materials must not be released within range of humans or other systems [H1, H2]
R2	Radioactive, toxic, or energetic materials must be stored away from humans [H1]
R3	Satellite, satellite components, and satellite debris must not impact other systems or debris during launch, on orbit, or during disposal [H1,H2]
R4	Satellite must not radiate energy until on orbit, separated from, and clear of launch vehicle and debris [H2]
R5	Radiated energy frequencies should be selected so as to be different from those used by other systems if possible [H2]
R6	Radiated energy must not be directed at and/or reach other systems using the same frequency if possible. Otherwise, radiation must be at sufficiently low power so as to prevent disruption or damage of other systems [H2]
R7	Satellite must not operate in an environment that poses the risk of excessive radiation or impact from energetic materials [H3]
R8	Satellite must be able to operate for the design life [H4,H5,H6]
R9	Satellite must be able to operate onboard instrumentation [H5]
R10	Satellite must be launched into correct orbit, or means to correct for different orbits must exist [H3,H4]
R11	Data obtained by instrumentation must be stored and/or transmitted to supporting infrastructure [H4,H5,H6]
R12	Satellite must maintain means of transmitting science data to supporting systems [H5]
R13	Satellite must maintain means of communication with supporting systems [H6]
R14	Satellite must maintain means of control [H6]

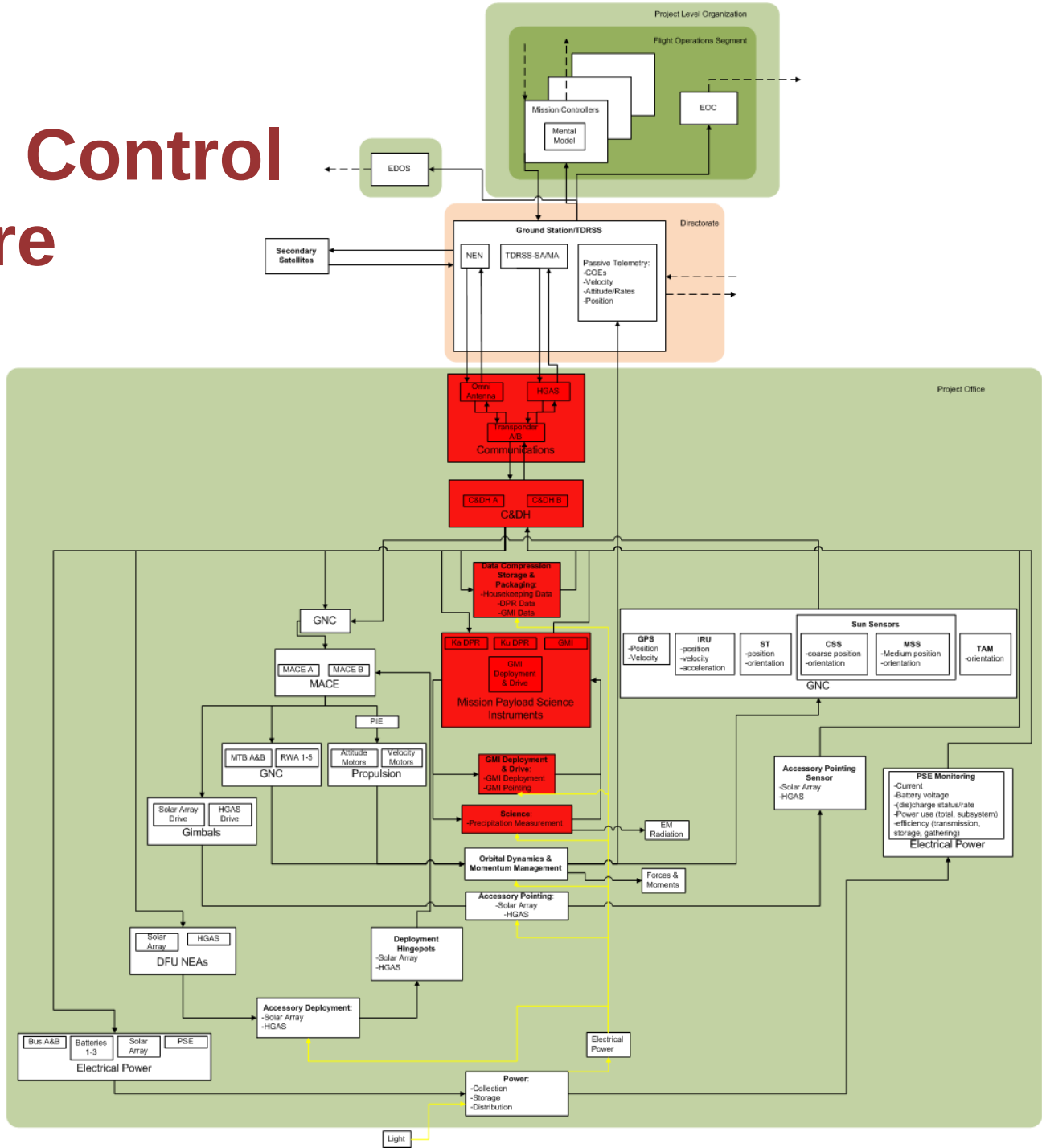
Launch Control Structure



Mission Control Structure



Mission Control Structure



Control Actions

- 82 Control Actions: Launch and Mission Phases
- 250+ Hazardous control actions
  - 31 GMI/DPR specific safety constraints (many are grouped)

Imposed Safety Constraints (Payload Specific)

Constraint	Description
SC1	GMI must not be deployed until separated and clear from the launch vehicle, obstacles, and orbital debris
SC2	GMI must not be deployed until rates are within tolerable structural limits
SC3	GMI must be deployed
SC4	Do not power on GMI or DPR sufficient electrical power has been stored
SC5	GMI and DPR must be powered on
SC6	DPR must not radiate energy before sufficient electrical power has been stored
SC7	DPR must not radiate energy until separated and clear from the launch vehicle, orbital debris, and radiation vulnerable obstacles
SC8	GMI and DPR shall be functionality checked on orbit
SC9	GMI must not be activated or functionality checked (Rx) before deployed and detector field clear of obstacles
SC10	GMI must not be activated or functionality checked during excessive in-band radiation (ie during DPR pulse)
SC11	DPR must not radiate such as to drain the battery below flight critical limits (*must trump all others)
SC12	DPR must be activated (Tx/Rx).
SC13	DPR must be activated (Tx/Rx) within sufficient time as to cover the science target region
SC14	DPR must not be deactivated before covering the science target region
SC15	GMI must be activated (Rx)
SC16	GMI must not operate such as to drain the batteries below flight critical limits (*must trump all others)

Imposed Safety Constraints (Payload Specific) Ctd.

Constraint	Description
SC17	GMI must be activated (Rx) within sufficient time as to cover the science target region
SC18	GMI must not be deactivated before covering the science target region
SC19	DPR and GMI must be calibrated on orbit before performing science mission
SC20	DPR and GMI on orbit calibration must be performed correctly (for sufficient duration, on the correct refence target, while sufficiently stable)
SC21	GNC must be in mission mode (correct pointing and sufficient stability) before DPR and GMI performing science mission
SC22	DPR and GMI must not produce heat outside tolerable limits
SC23	Science data must be stored onboard until transmission opportunity
SC24	Science data must not exceed storage capacity
SC25	Science data must be transmitted before exceeding storage capacity
SC26	Gathered science data rate must not exceed compression, storage, packaging and transmission rate capabilities
SC27	Data must be transmitted in TDRSS-SA/MA compatible formats
SC28	Science data must be archieved in ground support systems
SC29	Science data memory must be cleared
SC30	Science data memory must not be cleared until storage confirmed by ground
SC31	Safe Hold must indefinitely terminate science mission (*must trump all others)

Safety Constraints

- Safety constraints define requirements to operate the payload without creating higher level hazards
- Safe* alternative payloads :
  - May require fewer supporting controlled processes, but not more
  - May remove unnecessary control actions, but not introduce new control actions
- Other modifications to the satellite and mission architectures require new STPA analysis

*Without modification of existing STPA analysis

Questions

My contact information :

Connor Dunn

ncdunn@mit.edu

References

- Griswald, Britt. *GPM Core Observatory Diagram*. 2011. Photograph. *GPM Core Observatory Diagram*. By Jacob Reed. NASA Goddard Space Flight Center, 5 May 2011. Web. 18 Mar. 2013. <http://pmm.nasa.gov/image-gallery/gpm-core-observatory-diagram>.
- Leveson, Nancy. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA: MIT, 2011. Print.
- Reed, Jacob. "PRECIPITATION MEASUREMENT MISSIONS." *Precipitation Measurement Missions*. N.p., n.d. Web. 18 Mar. 2013. <http://pmm.nasa.gov/>