



Flight Software

Matthew Hayden
Software Engineer
NRL
202-404-1602
hayden@nrl.navy.mil



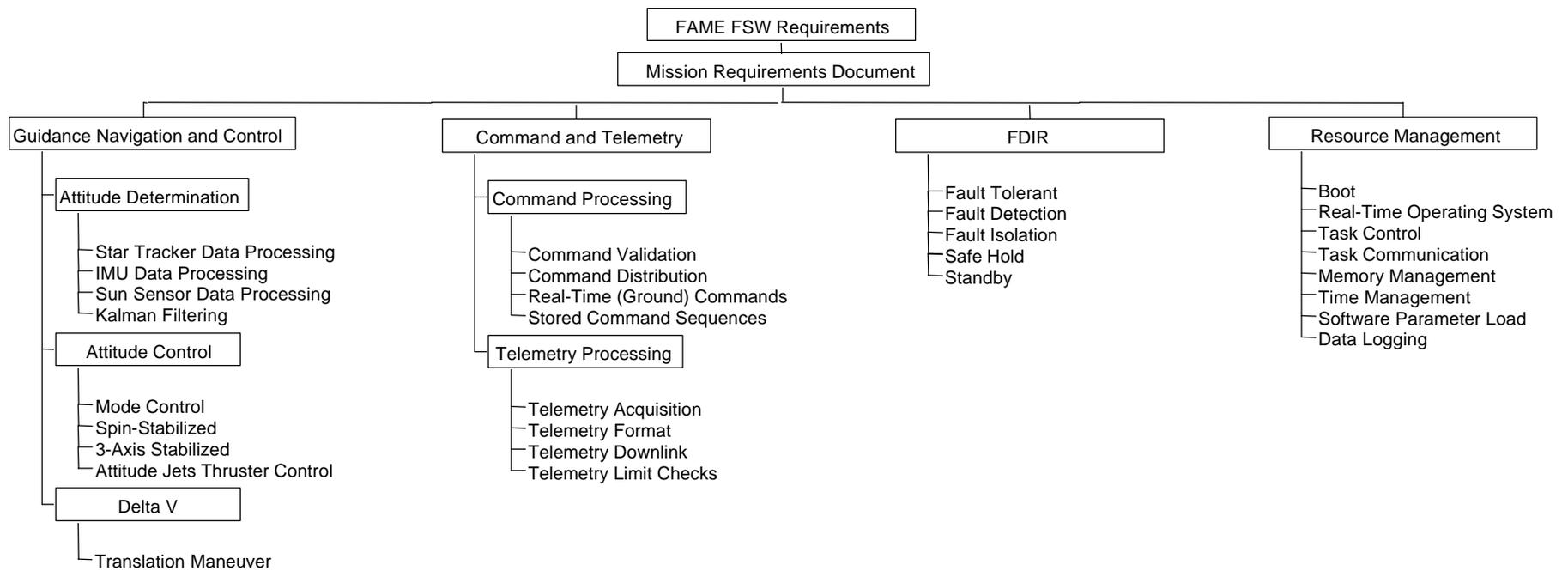
Top Level Requirements



- **Behavioral**
 - **Mission Requirements Document (MRD)**
 - **Concept Study Report (CSR)**
 - **Derived Flight Software Capability Requirements**
- **Procedural**
 - **Software Development Process**
 - **Software Test Process**
 - **Adherence to IVV Guidelines**
- **Administrative**
 - **Software Process Artifacts**
 - **Additional Required Documentation**



Top Level Requirements (Behavioral)





Top Level Requirements (Procedural)



- **To Have a Software Development Process in Place**
 - **Enforces Software Quality Assurance (Sec. D.3.8)**
 - **Guarantee Software End-to-End Test and Verification (Table D-2)**
 - **Implicitly Satisfies Independent Verification and Validation (Derived)**
- **To Document the Software Development Process**
 - **Through Explicitly Called Out Documentation (Sec. 4.3.6.1)**
 - **Software Development Plan**
 - **Through Products of the Process Called Out in the SDP (Derived)**



Top Level Requirements (Administrative)



- **To Document the Software Development Product**
 - **Through Explicitly Called Out Documentation (Sec. 4.3.6.1)**
 - **Software Requirements Spec**
 - **Software Development Plan**
 - **Implicitly Satisfied Through a Self-Documenting Process**
- **To Provide the Software Development Process**
 - **On Budget**
 - **On Schedule**



Derived Requirements



- **Identify the CSCI Behavioral Requirements**
 - **Attitude Determination**
 - **Attitude Control**
 - **Command Processing**
 - **Telemetry Processing**
 - **Fault Detection, Isolation, and Recovery**
 - **Resource Management**
- **Characterize Them to the Five Main Mission Phases**
 - **Launch Phase (Launch)**
 - **Geosynchronous Transfer Orbit Phase (GTO)**
 - **SuperSynchronous Orbit Phase (SSO)**
 - **Science Operation Phase**
 - **Disposal Phase**



Attitude Determination (1 of 2)



- **Three Attitude Determination Modes**
 - Rate Control Mode (During Star Tracker Acquisition, GTO)
 - 3-Axis Stabilized (During GTO, Science Ops)
 - Spin Stabilized (During AKM Maneuver, SSO)
- **Rate Control Mode**
 - Only IMU Input Required
- **3-Axis Mode**
 - Use of Redundant IMUs, Star Tracker, Sun Sensor and Kalman Filter
 - Open Loop Use of Instrument Data During Science Operation
- **Spin Stabilized**
 - Use of IMUs and Sun Sensor to Update Roll Orientation
 - Kalman Filter
 - Active Nutation Control Enabled



Attitude Determination (2 of 2)



- **Output Time Tagged Attitude Quaternion, Body Rates, and IMU Biases**
- **Output Status, Including Current Mode and Validity**
- **Operate IMUs in Fully Redundant (SSO-AKM), Hot Spare (SSO-Checkout), and Cold Spare (Science Operation) Modes**



Attitude Control (1 of 2)



- **Support of Seven Control Modes**
- **Standby Mode**
 - Monitor Attitude During Science Operation
 - No Thruster Firing
- **Inertial Pointing Mode**
 - Point to Any Inertial Attitude
 - Pointing Tolerances Defined in Command
 - Sub Modes With Control Parameter Variations to Cover Various Spacecraft Configurations and Delta-V Maneuvers
- **Rate Control Mode**
 - Controls Body Rates in Each Axis
- **Safe Hold Mode**
 - Before Solar Array Deployment: Z Axis Perpendicular to Sun; Slow Rotation About Z
 - After Solar Array Deployment: -Z Axis Pointed at Sun; Slow Rotation About Z



Attitude Control (2 of 2)



- **Open Loop Burn Mode**
 - Fire Specified Thrusters for Specified Intervals
 - Used for Coarse Maneuvers
- **Active Nutation Control Mode**
 - Damps Nutation During GTO Spin Stabilized
- **Spin Axis Precession Mode**
 - Precesses Spin Axis During GTO Spin Stabilized
- **Attitude Control Task Cycle Rate May Be Mode Dependent**
- **All Closed-Loop Modes Use Thruster Firing Tables to Convert On/Off Decisions Per Axis to Specific Thrusters**



Command Processing



- **CCSDS Command Format and Protocol Compliant**
- **Command Distribution**
 - **Software Commands**
 - **Spacecraft Subsystem (Hardware) Commands**
 - **Instrument Commands**
- **Parametric Load Support**
- **Memory Load Support**
- **Star Catalog Load Support**
- **Stored Commanding Support**
 - **Command Sequence Load Support**
 - **Sequences Can Be Initiated By Request or Time Released**



Telemetry Processing



- **State of Health (SOH) Telemetry Collection**
 - **Software Telemetry**
 - **Spacecraft Bus Telemetry (Hardware Telemetry)**
 - **Instrument Telemetry**
- **Memory and Parametric Table Downloads**
- **Spacecraft Event Reporting**
- **Telemetry Logging**
- **Summary Status Flags**
- **Telemetry Downlink Is CCSDS Compliant**
- **Commandable Downlink Rates Are 1K, 4K, 8Kbps, ... , 400Kbps**



Fault Detection, Isolation, and Recovery (1 of 3)



- **Attitude Determination**
 - IMU, Star Tracker, Sun Sensor BIT and Sanity Checks
 - On-Board Sensor Cross Checks
 - Hot, Cold Spare of redundant IMU
 - Open Loop Ground Support
- **Attitude Control**
 - **Commanded Mode Transitions Restricted By:**
 - **Current Mode**
 - **Spacecraft Configuration**
 - **Attitude Determination Status**
 - **Autonomous Mode Transitions Restricted to:**
 - **Maneuver Completion (i.e. Open Loop Firing)**
 - **System Failures**
 - **Instrument Protection / Consumables Protection**
 - **Thruster Firing Restricted By:**
 - **Current Mode**
 - **Maximum Duration before Continue Request**



Fault Detection, Isolation, and Recovery (2 of 3)



- **Command Processing**
 - **Commands Shall Be Authenticated**
 - **Command Type, Parameter, and Context Validation Attitude Control**
- **Telemetry Processing**
 - **Diagnostic Telemetry Collection**
 - **Software Diagnostics**
 - **High Rate Hardware Telemetry Collection**
 - **Instrument Diagnostics**
 - **Commandable Downlink Rates**
 - **High Rate Mode for Telemetry Diagnostics Could Be Supported**



Fault Detection, Isolation, and Recovery (3 of 3)



- **Fault Detection**
 - Specified Fault Identification Logic
 - Areas of Concern Include Attitude Sensor Reliability Checks, Undervoltage Detection, Instrument Protection
- **Fault-tolerant - Mission Phase Sensitive**
 - Nominally a Fail-Safe Approach - When Time to Effect Is Short
 - Safe-Hold - When Time to Effect Is Short or After a Ground Response Timeout
 - Inform Ground and Await Instruction
 - Reset Process - Return to Boot/Initial Processor State
- **Fault Containment**
 - Sanity Checks on FSW Inputs (Commands, Parameters, Sensor Inputs)
 - Protection for Consumables and Instrument
 - Protection Against SW/HW Upsets – Processor/Task Watchdog
- **Processor Initialization and Recovery Will Return to a Safe State - Safe State Is Configurable Based on Mission Phase**



Requirements Capture Approach



- **Capture Requirements**
 - Descriptive Text (SRS)
 - Identify System Actors/Users (Use Case)
- **Define Test Requirements**
 - Establish Entry/Exit Criteria (Test Vectors)
 - Identify System (Black-Box) Interfaces (External Event List)
- **Elaborate Complex Behavior**
 - Isolate Interfaces/Interactions (Scenario Diagrams)
 - Identify Time Critical Behaviors (Timing Diagrams)
 - Isolate State Behavior (State Diagrams)
- **Characterize Fault Behavior**
 - Hazard Analysis (Hazard List)
 - Fault Analysis (Fault Trees)



Procedural Requirements



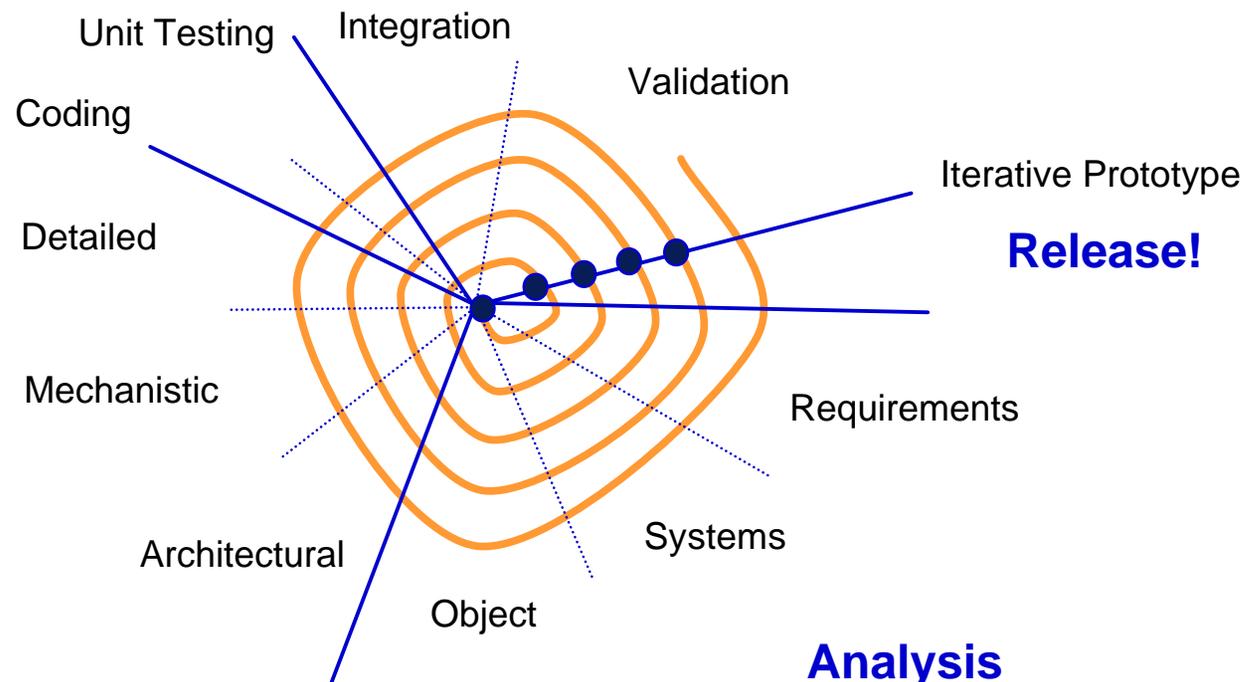
- **Rapid Object-Oriented Process for Embedded Systems (ROPES)**
 - Defines the Process of Development
 - Defines the Process Deliverables (Artifacts)

Implementation

Testing

Design

Analysis





Issues



- **Clean Integration of Object Oriented Design Approach With Current Functional Decomposition Products (i.e. Code Reuse)**
- **Definition of ACS/RCS Controller (ARC) Capability and Subsequent Flight Software Complexity**
 - **Thruster Sanity Checks**
- **Level of Autonomy in Instrument Protection**
- **Time Tagging Design**



Major Trade Studies



- **Software Development Software**
 - Rhapsody, Rational Rose for the OO CASE Tool
 - Visual Programming Environment Versus Development Tool
 - Clearcase for Configuration Management
 - Integrated Defect Tracking (DDTS/ClearQuest)
 - Tornado/VxWorks as the Development Suite
 - Sparc Solaris/Windows Hosting
- **Legacy Software Integration**
 - SCL Version 2.6 or 3.0 (C vs. C++, Single- vs Multi-Threaded)
- **FPGA Versus Low Level Processor/Software Implementations**



Backup



FSW Reuse (1 of 3)



- ***Clementine*, Interim Control Module (ICM) and Naval Earth Map Observer (NEMO) FSW Systems Are Available for Design and Code Reuse**
- ***Clementine***
 - 1750 and R-3000 Based Processors
 - 1750 Utilized ADA Kernel, ADA Code and C Code
 - R-3081 Utilized VxWorks
 - Supported IMU and Star Tracker Attitude Sensors
 - Potential Area of Design/Code Re-Use Is the Attitude Determination and Control Function
 - ***Clementine* Utilized Both Spin and 3-Axis Stable Control Modes**



FSW Reuse (2 of 3)



- **Interim Control Module**
 - **R-3000 Based Processor (Harris RHC-3001)**
 - **VxWorks Based**
 - **Supported IMU and Star Tracker Attitude Sensors**
 - **Supported 1553 Interface**
 - **Potential Areas of Design/Code Re-Use - Processor Independent:**
 - **Resource Management Functions - Software Support**
 - **Command Distribution and Logging**
 - **Stored Command Sequence Execution**
 - **Telemetry Collection and Logging**
 - **Attitude Determination and Control**
 - **Memory and Parametric Load/Dump**
 - **Math Libraries**
 - **Potential Areas of Design/Code Re-Use - Processor Dependent:**
 - **Resource Management Functions - Processor Support**
 - **Boot**



FSW Reuse (3 of 3)



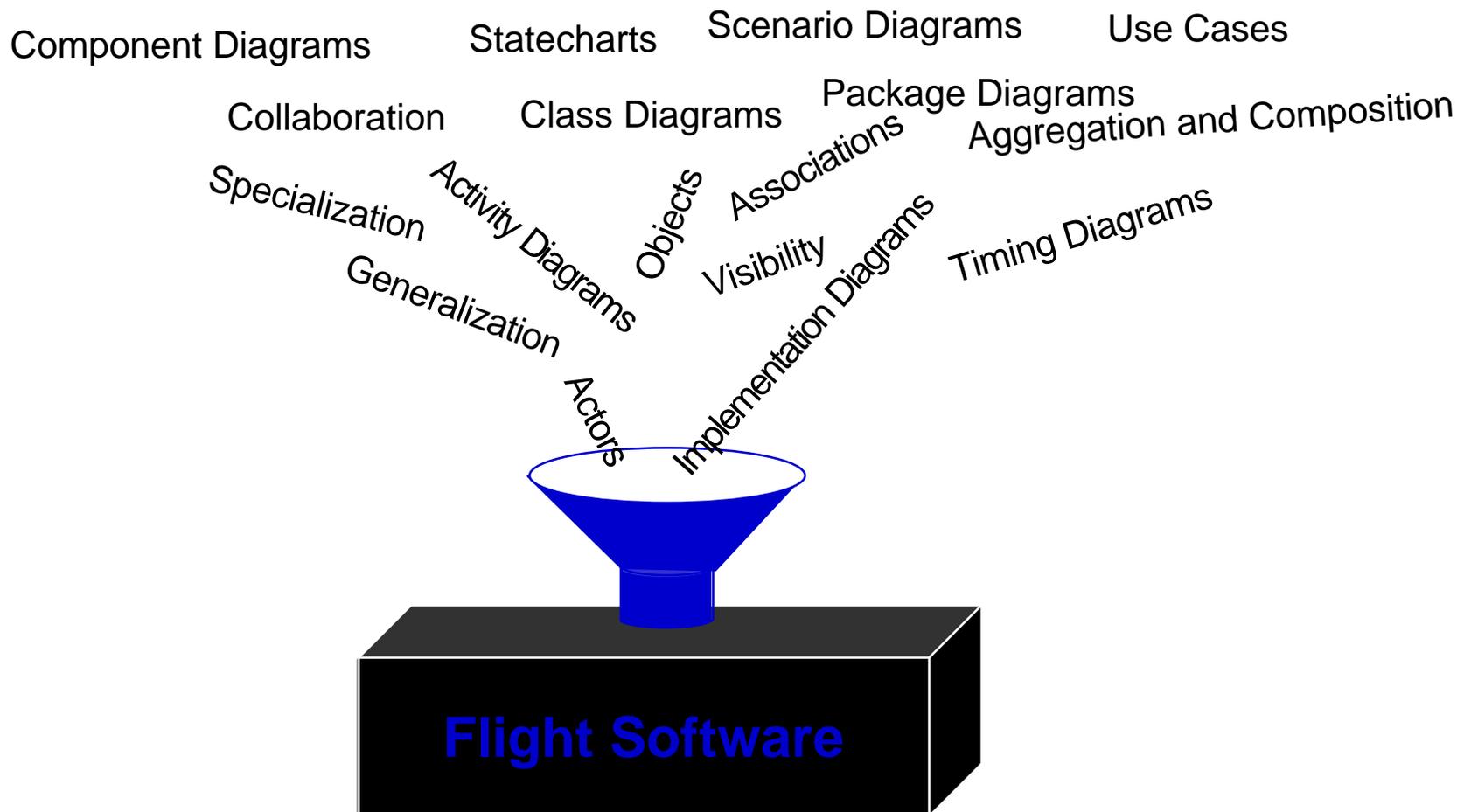
- **Naval Earth Map Observer**
 - **Power PC Based Processor (Payload Controller)**
 - **VxWorks Based**
 - **Potential Areas of Design/Code Re-Use**
 - **CCSDS Compliant Command and Telemetry Support**



Unified Modeling Language (UML)



- Defines a Common Notation for Capturing System Behavior
- Defines Terms, Usages, and Relationships





Top Level Requirements (ROPES Artifacts)

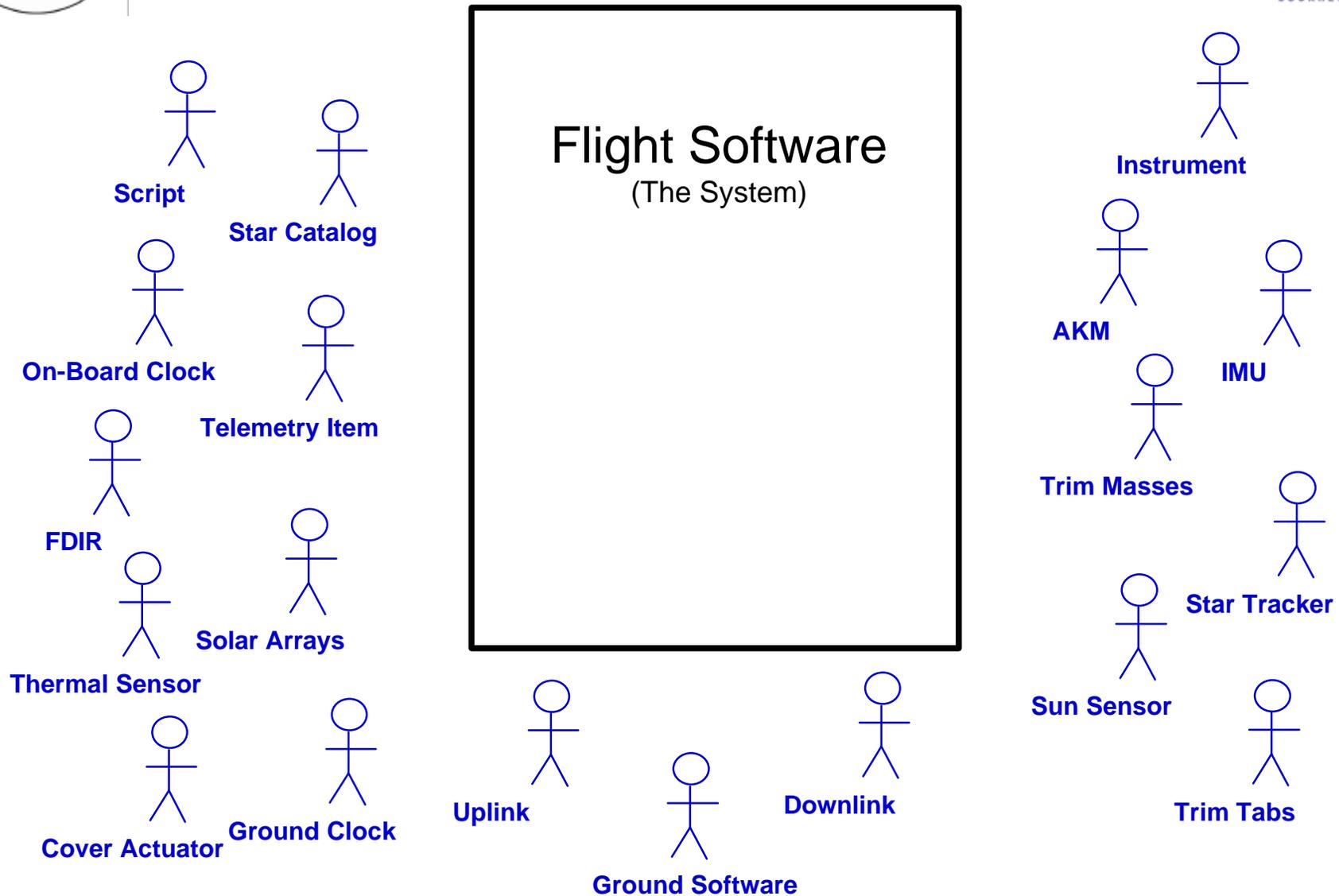


At the completion of Requirements Analysis:

- **Software Lifecycle Schedule**
- **Optional Textual Requirements Document (SRS)**
- **Context Diagram**
- **Use Cases**
 - **Use Case Diagrams**
 - **Statecharts**
 - **External Event List**
- **Use Case Scenarios**
 - **Sequence Diagrams**
 - **Timing Diagrams**
- **Hazard Analysis**
- **Test Vectors**

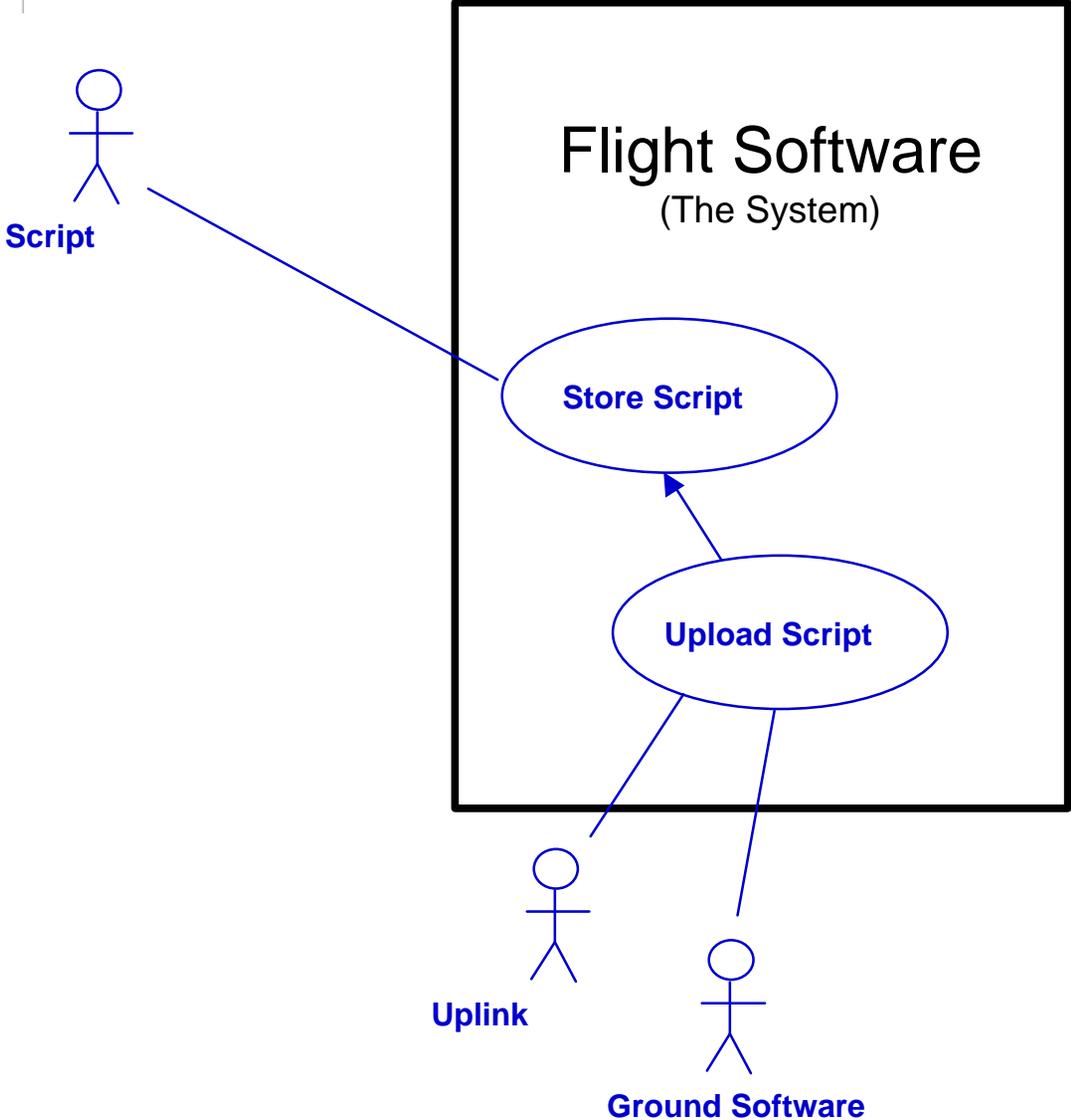


Context Diagram





Use Case Diagrams





External Event List



Event	Description	Direction	Arrival Pattern	Response Performance
Third Stage Separation	Indicator of Third Stage Sep	SCIO to System	Asynchronous	Must Set Timer w/in 10s
Ten Minute Timer	Indicator of Safe to Activate	Clock to System	Asynchronous	Must Start S/C w/in 5s
Trim Mass Location	Telemetry of Mass Displacement	Trim Mass to System	Periodic (100ms)	Update Telemetry w/in Xms
Ordnance Control	Telemetry of Safed/Armed	OC to System	Episodic	Update Telemetry w/in Xms
Open Instrument Sensor Cover	Command to Open Cover	System to Mechanisms	Asynchronous	None Required
Set D/L Rate	Command to Set D/L Bitrate	System to Downlink	Asynchronous	None Required