Investigating Model-Based Autonomy for Solar Probe Plus.

Workshop on Spacecraft Flight Software. December, 2013.

Bill Van Besien

Flight Software Engineer

*(Notice: This presentation does **not** contain export controlled information)*

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Contents

Executive Summary

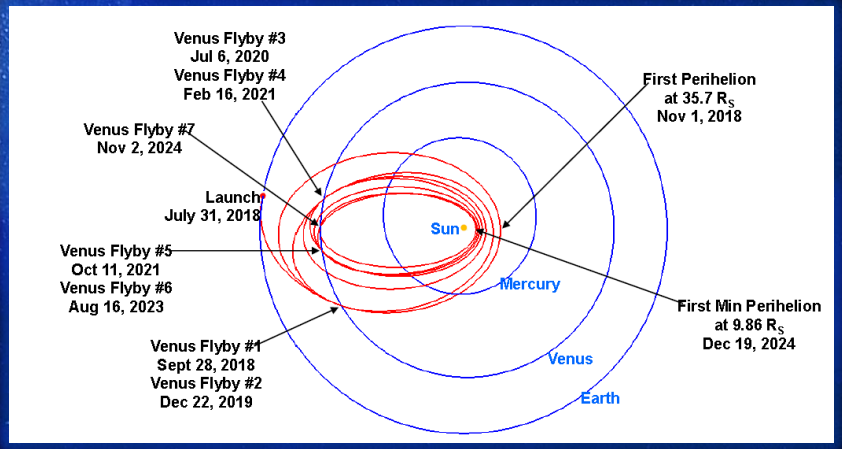
- **Decision to *proceed* with Rule-Based Autonomy system**
  - **Extensive and successful operational history.**
  - **Substantial re-use from previous missions.**
  - **Other program-specific constraints.**
- **Model-Based technology to other applications**
  - **Model-based system planned to be used on other upcoming spacecraft and UAV projects.**
  - **Benefits of this model-based approach to be used in continued development of SPP autonomy engine.**

Mission Profile / Science Objectives

- **Significantly contribute to "*our ability to characterize and forecast the [solar] radiation environment*"**
  - ***Structure and dynamics* of the solar magnetic fields.**
  - **Tracing the *flow of energy* that heats the corona.**
  - **Understanding the mechanisms and flows of energetic particles.**
  - **The "dusty plasma" phenomenon.**

Mission Profile / Spacecraft

- **Trajectory/Mission Plan**
  - **Two dozen orbits, gradually brought in**
- **Propulsion**
  - **3-Axis Stabilized, no deep-space maneuvers**
- **Thermal Protection System (TPS)**
  - **Heat difference of up to 2000 C**
- **Solar Arrays**
  - **Slew deployment, carefully prevent overheating**
- **Instruments**
  - **Magnetometers, particle detectors, imagers, etc…**



Mission Profile / Autonomy Challenges

- **Communication eclipses**
  - **Up to 34 days, cumulatively, throughout orbit**
  - **Very low emergency downlink rate**

- **Primary drivers for on-board Fault Protection**
  - **Maintaining TPS pointing**
  - **Avoiding solar array overheating**

- **Autonomy must recover into operational state during thermal-critical regions**

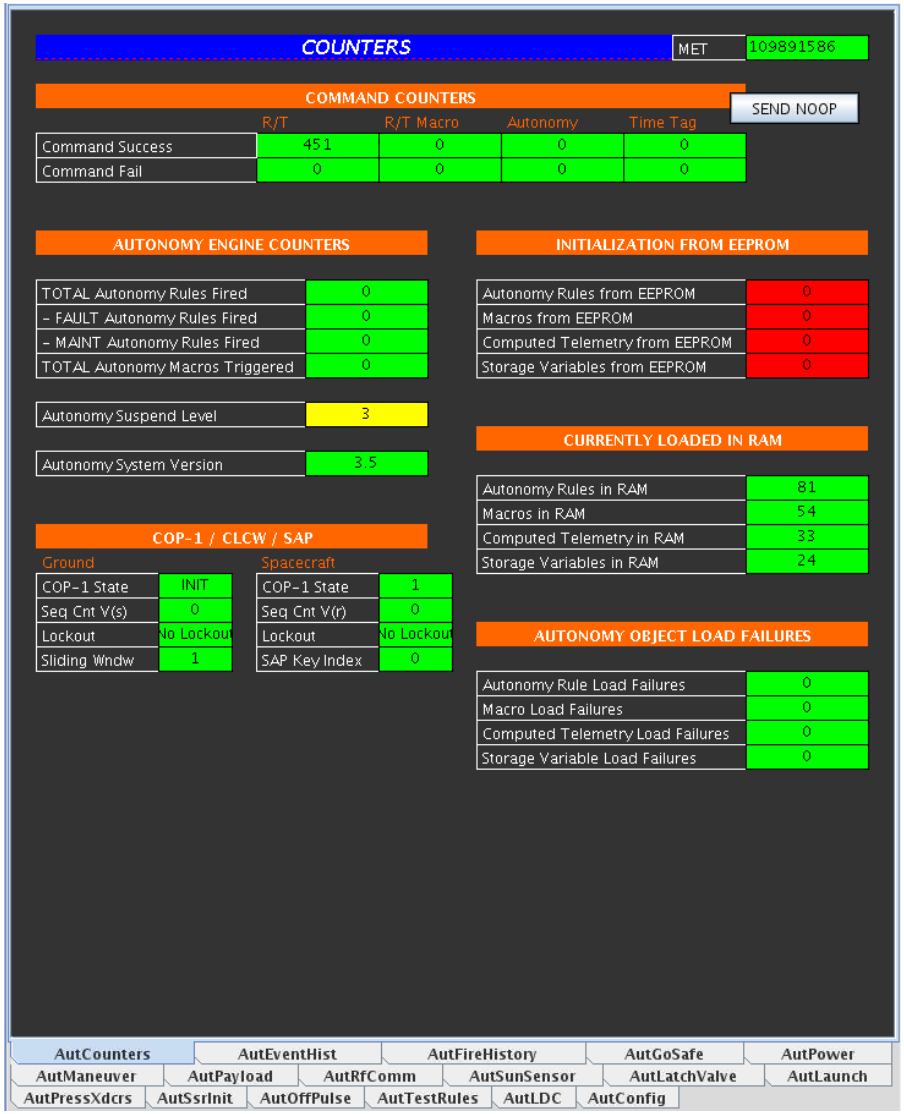
- **Essential Requirements**
  - **Manage design complexity**
  - **Execute predictably and robustly**
  - **Provide high levels of verifiability**

Autonomy System Evolution

- **Generation Zero**
  - **Early science missions; No notional separation of Autonomy.**
- **Generation 1**
  - **(ACE) Monitoring of single telemetry points.**
- **Generation 2**
  - **(NEAR, TIMED) More expressive conditions.**
- **Generation 3+**
  - **STEREO, MESSENGER, RBSP/VAP**
  - **More expressiveness; Notions of CT, Storage Vars, etc…**

Rule-Based Autonomy

- **Single-fault tolerant**
- **Allocations for dozens of…**
  - **RPN Expressions**
  - **Computed Telemetry**
  - **Storage Variables**
- **Fine-grained control and manipulation**



Rule-Based HTML X-Reference Doc

Rule Number	1 (Rule DB # = 003)
Title	sLVS in EA
Rule Premise	OBS_MODE == MODE_EA && ((MAIN_BUS_VOLT_EU < 27.0 && PS_MAIN_BUS_VOLT_ST == MUX_AD_OK) || (BATT_PRES1_EU < 600.0 && BATT_PRES1_ST == MUX_AD_OK) || (BATT_PRES2_EU < 600.0 && BATT_PRES2_ST == MUX_AD_OK))

Rule Number	3 (Rule DB # = 023)
Title	sCLT (Not EA)
Rule Premise	OBS_MODE != MODE_EA && SCLT_TIME_OUT_HRS > 60.0

Rule Number	25 (Rule DB # = 032)
Title	Monitor HGA Gimbal Invalid
Rule Premise	OBS_MODE != MODE_EA && GC_HGA_CNTL_ST != HGA_CNTL_DISABLED && GC_HGA_PNTG_AT_EARTH == 0

Rule Number	28 (Rule DB # = 089)
Title	Persistent ST Fault in OBS or STBY
Rule Premise	(OBS_MODE == MODE_STANDBY || OBS_MODE == MODE_OPERATIONAL) && GC_STR_ENA_FOR_USE == 1 && GC_STR_DATA_USED == 0 && GC_HGA_CNTL_ST != HGA_CNTL_DISABLED

Rule Number	37 (Rule DB # = 038)
Title	TWTA to Transmit when Battery OK (Not Ascent)
Rule Premise	OBS_MODE != MODE_ASCENT && TWTA_VOLT_EU > 5.0 && RF_EPC_ST > 0x4A && RF_TWT_ST > 0x4A && ((BATT_PRES1_EU > 650.0 && BATT_PRES1_ST == MUX_AD_OK) || (BATT_PRES2_EU > 650.0 && BATT_PRES2_ST == MUX_AD_OK))

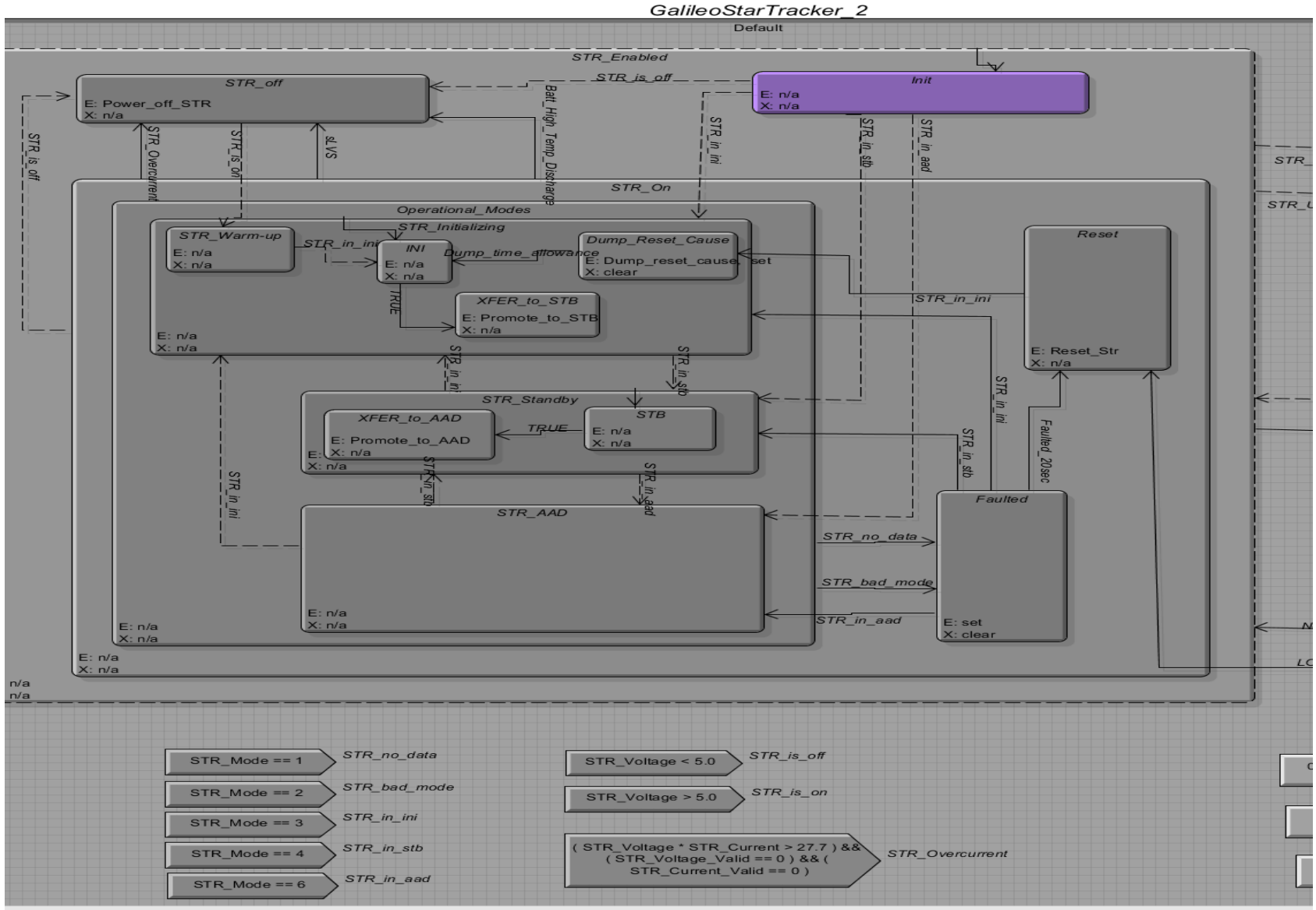
Rule Number	38 (Rule DB # =)
Title	TWTA in Idle Mode (for Launch + Not Ascent)
Rule Premise	OBS_MODE != MODE_ASCENT && TWTA_VOLT_EU > 5.0 && RF_EPC_ST < 0x4A

Rule Number	39 (Rule DB # =)
Title	TWTA in Off Mode (for Launch + Not Ascent)
Rule Premise	OBS_MODE != MODE_ASCENT && TWTA_VOLT_EU < 5.0

Rule Number	41 (Rule DB # = 040)
Title	High Temp Batt Discharge (Not EA)
Rule Premise	OBS_MODE != MODE_EA && BATT_CURR1_EU < 0.0 && BATT_CURR1_ST == MUX_AD_OK && (BATT_TEMP1_EU > 18.0 || BATT_TEMP2_EU > 18.0 || BATT_TEMP3_EU > 18.0)

Rule Number	118 (Rule DB # = 201)
Title	Monitor HGARA Temperature
Rule Premise	OBS_MODE != MODE_EA && HGARA_TMP_EU > 55.0 && TRIO_B2_ACK_ST == 0

Roughly Equivalent Model-Based View



Principles of Autonomy System Design

- **Understandability**
  - **Necessary for reviews.**
  - **Essential for future modifications.**
- **Flexibility**
  - **Speeds development and testing.**
  - **Eases the burden on ops staff.**
- **Verifiability**
  - **Prevent crunch in I&T testing.**
  - **Ensure risk level.**

Model-Based Motivations – Testing

- **2008 NASA Fault Management Workshop findings**
- **Finding #1 – The "Downstream" Testing Crunch**
  - **Late testbed availability led to rapid spending growth during I&T.**
- **Finding #4 – FM Representation and Design Guidelines**
  - **Lack of sufficient formalization in FM design and documentation.**
  - **Recommendation: Identify representation techniques to improve FM system design and review.**

Motivation: Design-as-Implementation

- **Understandability**
  - ***The design is the implementation*.**
  - **Design not subject to interpretation.**
  - **Intuitive understanding of the autonomy system behavior.**

- **Flexibility**
  - **Ability to manipulate, alter autonomy model behavior on-the-fly.**

- **Verifiability**
  - **Ability to test early *without* testbed integration.**
  - **Graph-based foundation amenable to formal verification methods.**

“ExecSpec” Background

- **Core concepts developed FY 06 – FY 09 PI George Cancro**
- **Based upon Bell Labs Virtual Finite State Machine (VFSM)**
- **ExecSpec Software Suite**
  - **Design Tool (ESD)**
    Intuitive visual programming for state model logic through diagrams
  - **Interpreter (ESI)**
    Interprets and executes diagrams
  - **Visualizer (ESV)**
    Monitoring tool to provide situational awareness

Why not Model-Based Auto-coders?

- **Similar COTS offerings exist, why not use them?**

"[COTS alternatives] do not provide the end-to-end flexibility and operations monitoring capability necessary for next generation autonomy development systems"

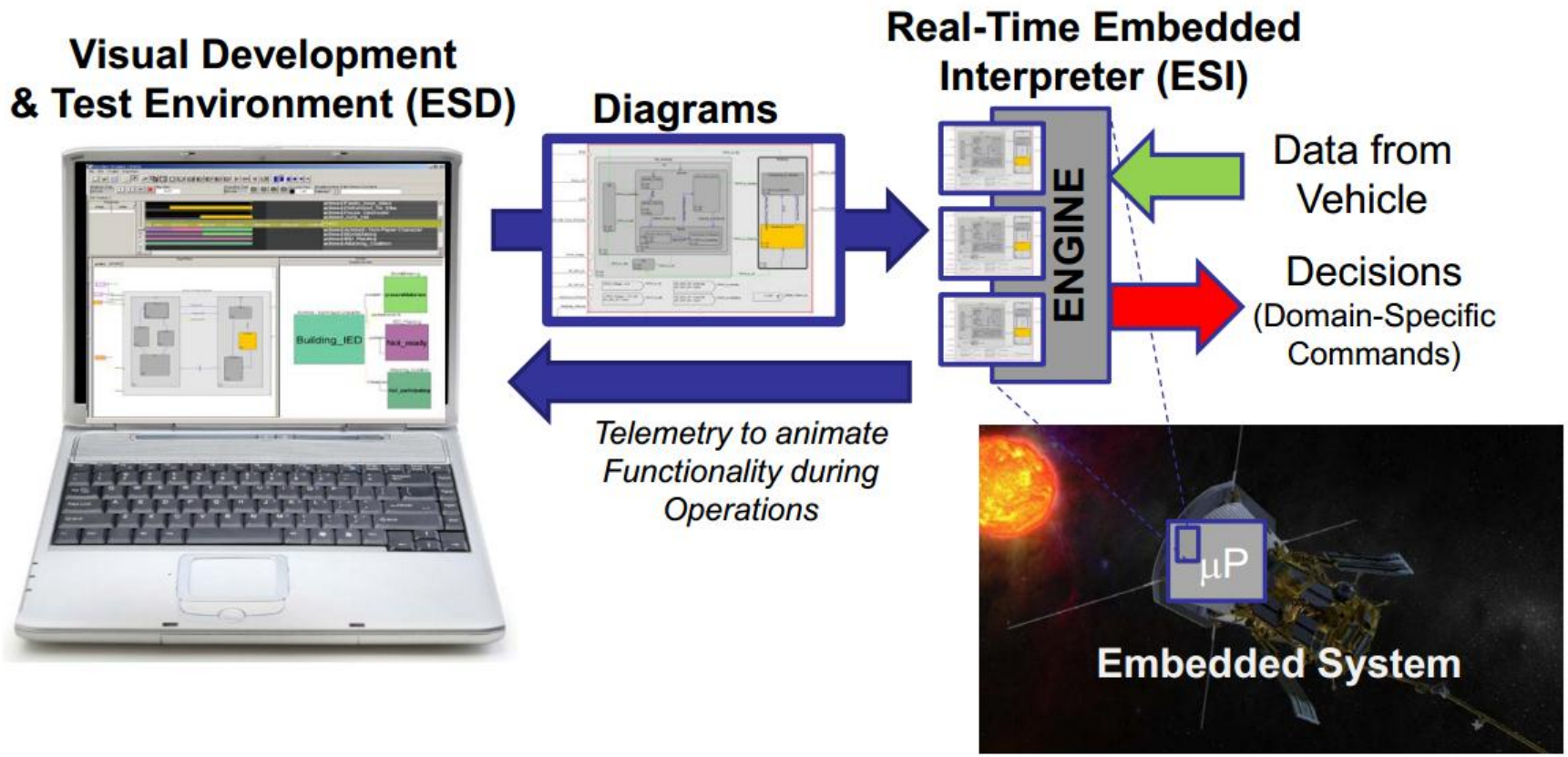
- **Desire to separate "interpreter"/engine from autonomy model**
  - **Simpler to alter or upload new models.**

- **Surveyed alternatives can not support CONOPS**
  - **MOPS, command and telemetry infrastructure.**
  - **Run-time manipulation of models, inputs.**
  - **No separate designer, visualizer, interpreter.**

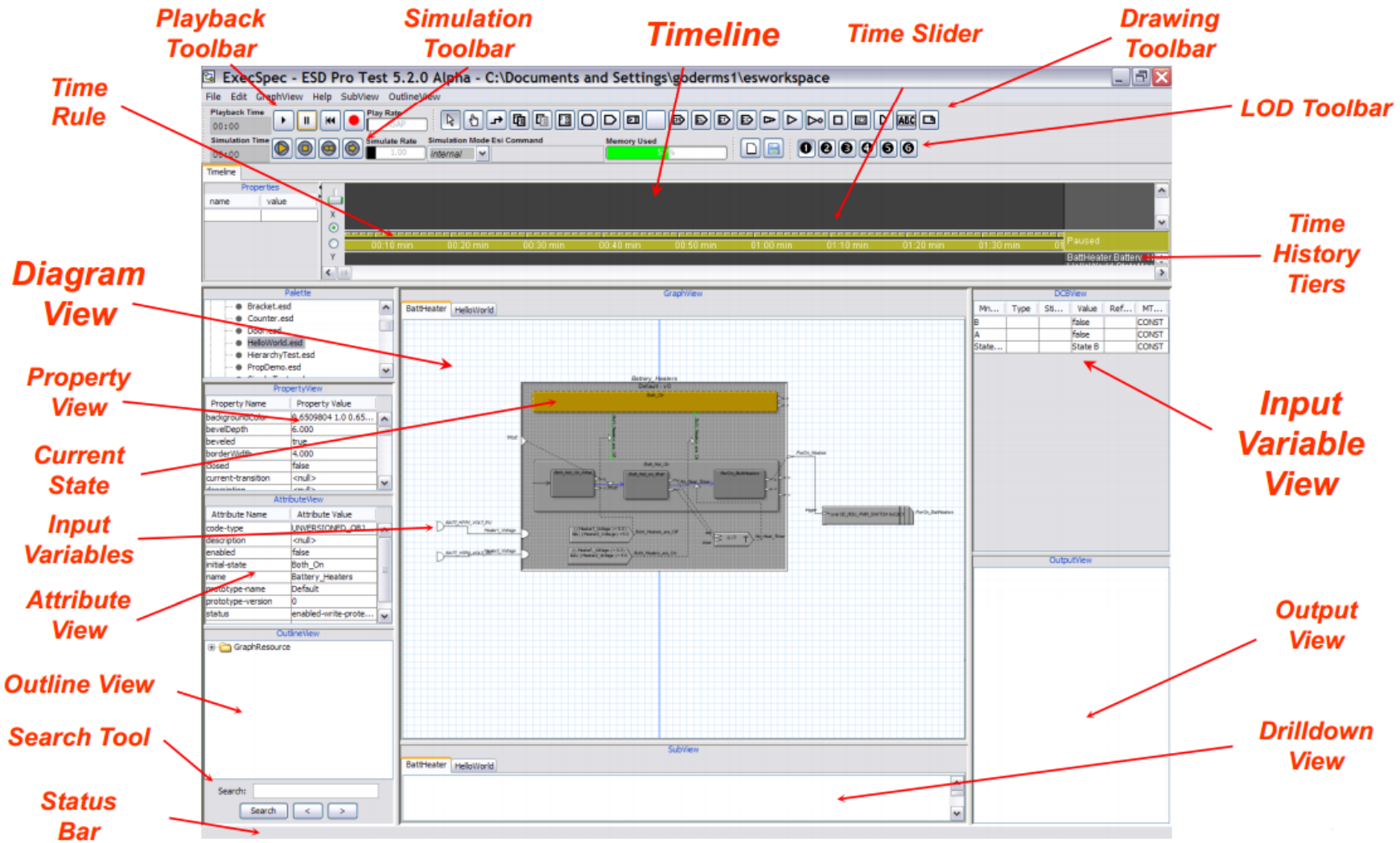
Investigating Suitability for SPP

- **Early Technology Development**
  - **Concept-development IRADs on STEREO**
- **SPP Suitability Investigation**
  - **SPP FSW integration prototype**
  - **Tech readiness demo on UAV**
  - **Formal verification IRAD**
  - **Trade study**

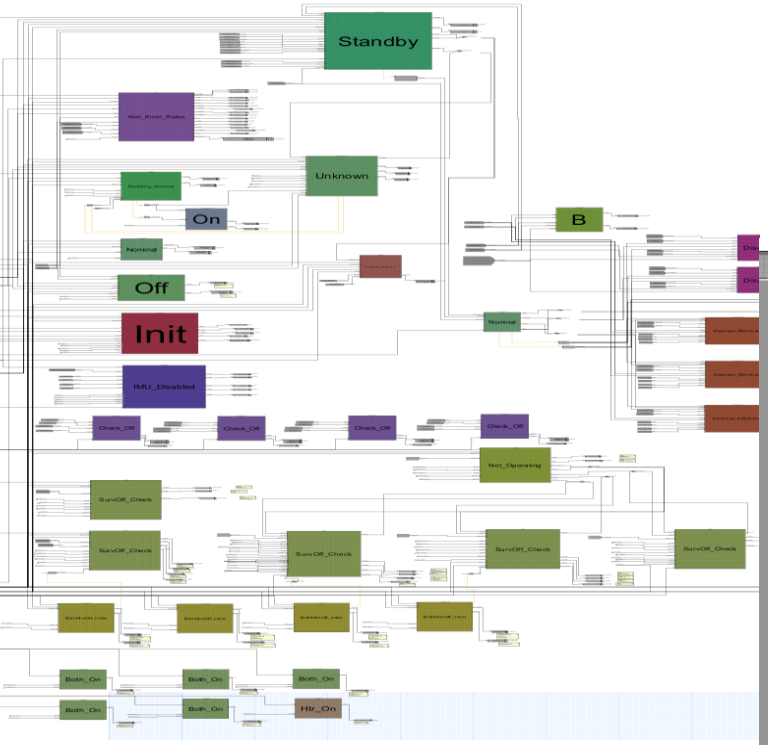
1 – ExecSpec Concept of Operations

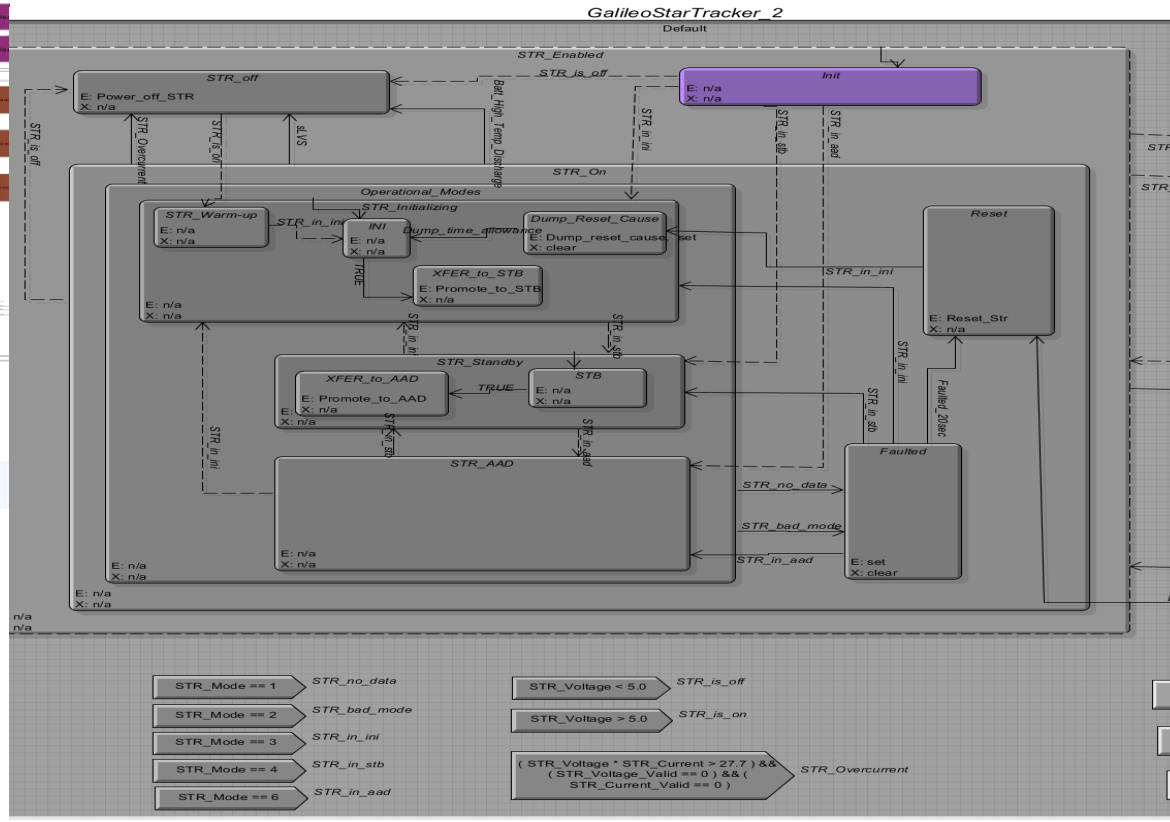


2 – ExecSpec Designer Overview



Modeling STEREO

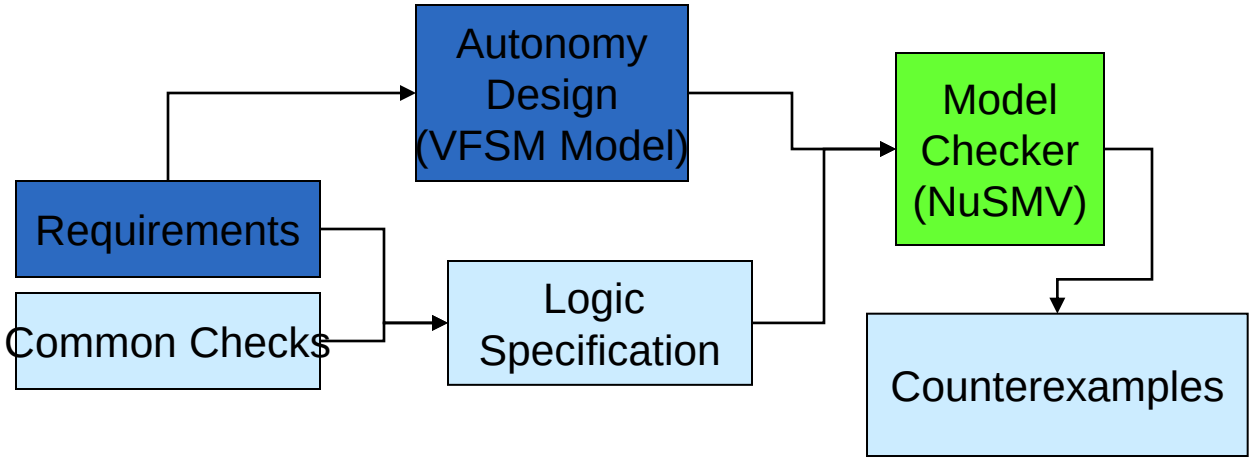




3 – Early Work on STEREO Testbed

- **STEREO autonomy system *translated* into 43 state machines.**
- **ExecSpec interpreter inserted into STEREO flight software.**
- **ExecSpec visualizer/designer inserted into ground system.**
- **Demonstrated in hardware testbed our model-based software handing *most* STEREO fault management requirements.**

4 – Formal Verification Concept

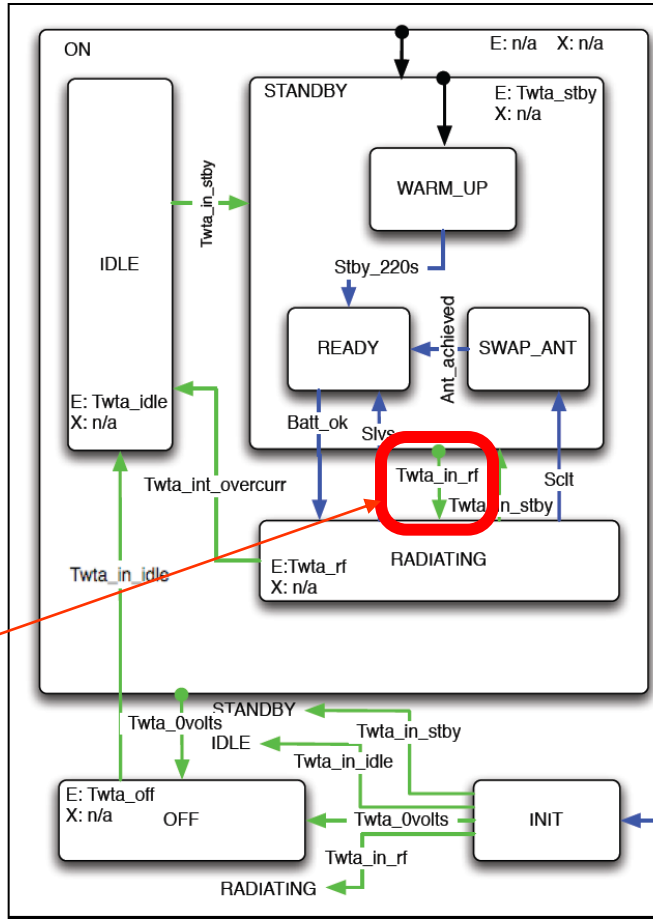


Requirement:

***Safety*: "Never radiate while swapping antennas"**

AG !(twta=radiating & ant=swapping)

Counter Example

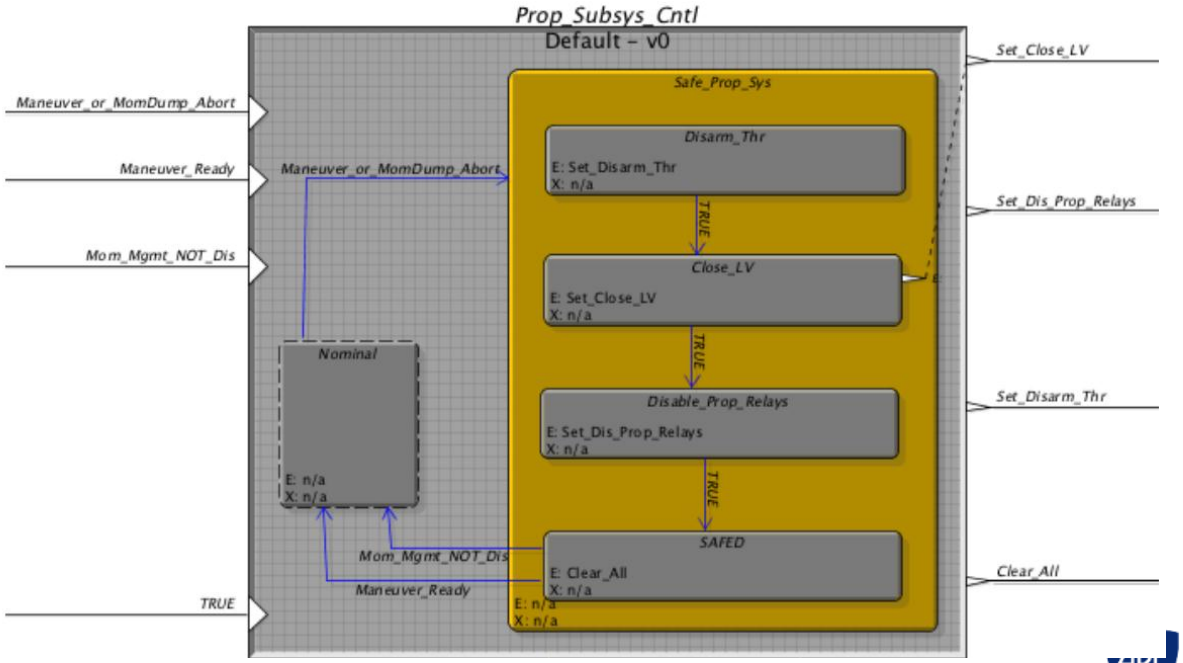


Formal Verification Study

- **"Translated" STEREO autonomy system into a model-based conception**

- **Developed *ExecSpec-to-NuSMV* compiler**
  - **Assumptions → Plant Models**
  - **Significant interactions across system**

- **Proved critical safety constraints**
  - **Introduced faults, confirmed detection**
  - **Order of seconds**



5 – UAV Flight Demonstration

- **Objective: Demonstrate performing critical in-flight fault management in challenging environment for UAV platform.**

- **Approach**
  - **Develop FM design**
  - **Integrate in UAV FSW environment**
  - **Establish and demo CONOPS**

- **Flight tests**
  - **Override in-flight autopilot under anomalous conditions.**

- **Successful Demonstrations**
  - **First - “Unicorn” UAV in MD.**
  - **Second – Commercial UAV on West Coast.**

5 – Trade Study

- **Formal, comparative analysis of both approaches**
- **"Null Hypothesis" – H_0: *Rule-Based autonomy suitable for SPP.***
- **Question – Does model-based scheme provide a *substantially compelling* case to overrule H_0 ?**
- **Concerns – Risk Management**
  - **Limit additional new technology on SPP**
  - **Leverage software re-use**
- **Approach**
  - **Several dozen metrics to compare schemes**
  - **Each with "suitability score"**

Comparative Metrics (1)

- **Re-initialization speed**
  - **Frequent processor rotation is expected**
- **Managing subsystem interdependencies**
  - **Complex system with many interactions**
- **Intuitive, visual system for reviewing designs**
  - **Model-Based on top for “design”**
  - **No clear benefit for either for mission ops**
- **Designing sequences of several decision points**
  - **Complex responses requiring checks of telemetry while in progress**

Comparative Metrics (2)

- **Path dependent responses**
  - **When path to fault is as important as fault itself.**
  - **Finer "granularity" to responses.**

- **Similarity of design to implementation**
  - **Reduces cost and risk; Review of design becomes review of implementation**

- **Facilitation of formal verification**
  - **Important, but not expected to replace testing, so will add additional setup cost**
  - **Model-Based, but potential for rule based**

- **Efficiency of implementation**
  - **Speed of rule evaluation, time budget, non-volatile footprint**

Comparative Metrics (3)

- **Parallel development**
  - **Well established process in RB approach**
  - **Merging process not clear in MB approach**

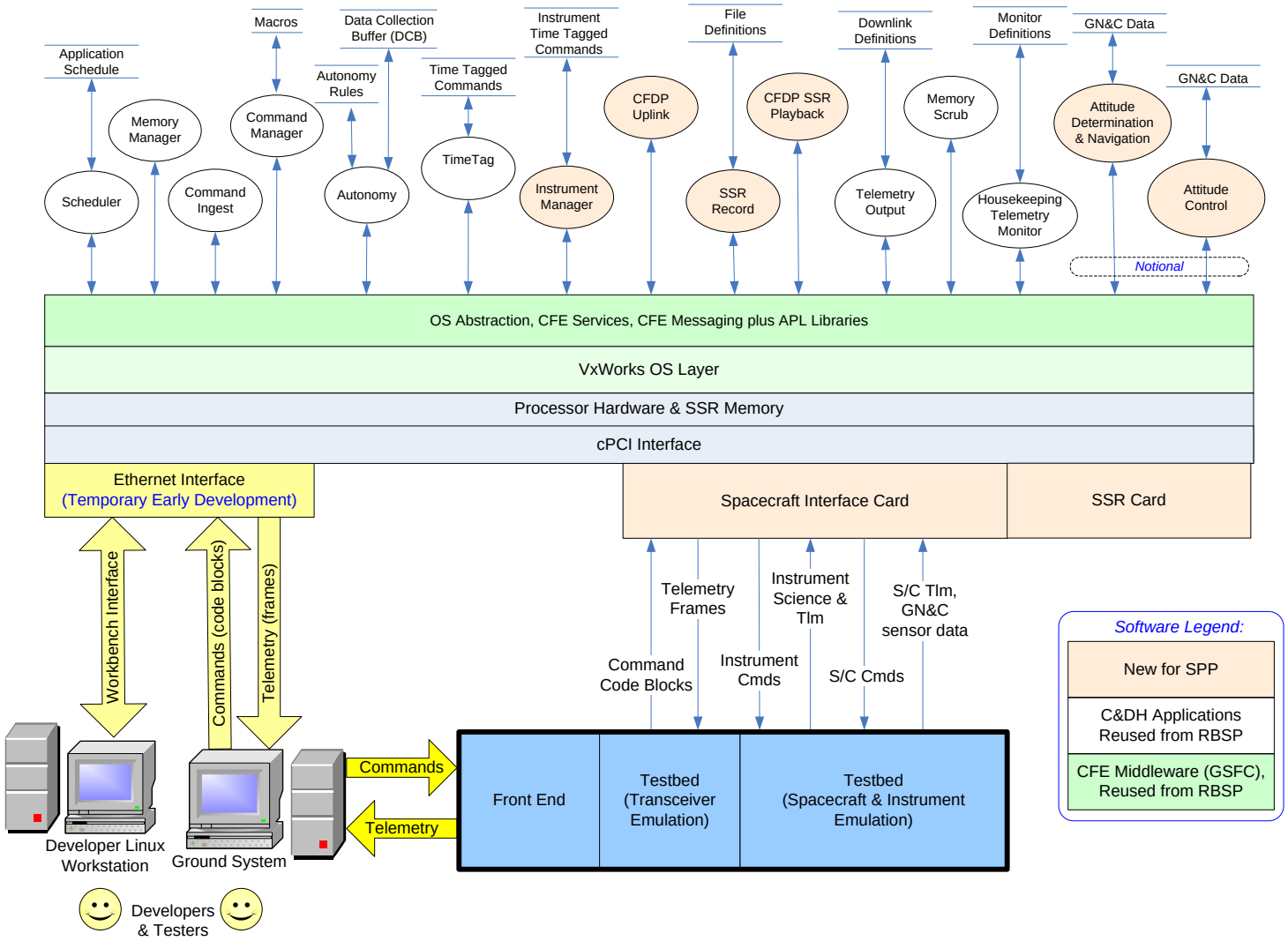
- **Starting point for testing and implementing logic**
  - **Can start preliminary testing and implementation sooner**

- **Past Mission Experience**
  - **Previous successful expertise valuable during all mission phases**
  - **FM Working Group finding – switching autonomy paradigms can be problem-prone**

Evaluative Conclusions

- **Model-based, rule-based systems *equivalent expressiveness***
- **By formal metrics, marginal benefit for MB approach for SPP**
  - **However, not sufficiently compelling to overcome motivations to remain with RB approach**
- **Post-investigation plans**
  - **Proceed with Rule-Based autonomy system**
  - **Elements of MB software to be leveraged for rule-based system**

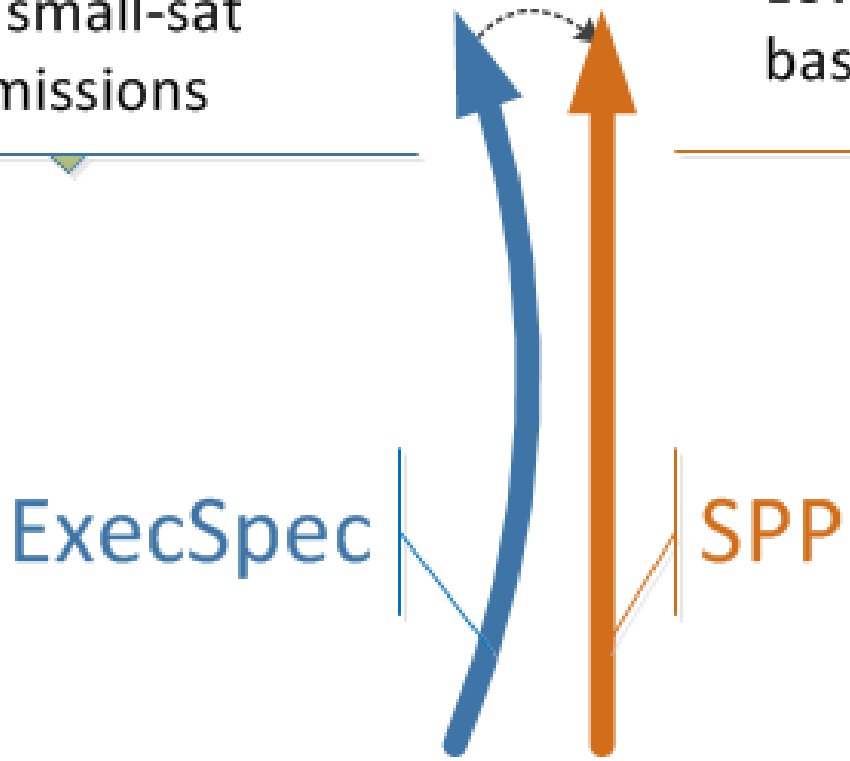
Reusable FSW Architecture in Context



Future Developments

- UAV Systems
- Cyber security
- Future small-sat space missions

- Rule-Based System
- Maximize tech and s/w reuse
- Leverage some model-based benefits



Sources, References, and Further Reading

- ***This presentation is an overview of the contributions made by:***

  Justin Thomas, George Cancro, Russell Turner, Paul Rosendall, Eli Kahn, Eric Melin, Mike Pekala, among others. Thank you!

- **Autonomy System Trade Study - Internal Publication, 2013.**
- **Thomas, Justin. "Infusing Next Generation Fault Management Software on Solar Probe Plus". Workshop on Spacecraft Flight Software. 2012.**
- **Cancro, George. "APL Spacecraft Autonomy: Then, now, and tomorrow". APL Technical Digest. 2010.**
- **R. Turner, S. Hooda, J. Gersh, G. Canco. "ExecSpec: Visually Designing and Operating a Finite State Machine-based Autonomy System". 9th International Symposium on Artificial Intelligence, Robotics and Automation for Space. Pasadena, CA. 2008.**