SYM-AM-25-336

Excerpt from the Proceedings

of the

Twenty-Second Annual Acquisition Research Symposium and Innovation Summit

Thursday, May 8, 2025 Sessions
Volume II

Accelerating Satellite Development: A Comparative Simulation of NASA's Waterfall Process and Agile Process Using Innoslate Life Cycle Modeling Language

Published: May 5, 2025

The research presented in this report was supported by the Acquisition Research Program at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School

Accelerating Satellite Development: A Comparative Simulation of NASA's Waterfall Process and Agile Process Using Innoslate Life Cycle Modeling Language

Robin J. Yeman—Senior Director of Engineering, Leidos

Yashwant K. Malaiya—Dept. Computer Science Colorado State University. [malaiya@cs.colostate.edu]

Abstract

Large-scale, safety-critical cyber-physical (LS/SC/CP) systems, such as satellites, face significant challenges in balancing the need for safety, regulatory compliance, and documentation with the demand for faster development cycles. This study examines the impact of applying Agile methodologies to the LS/SC/CP system by modeling the development of a fictional mid-size Low Earth Orbit (LEO) satellite using Innoslate. We created two development models: one following NASA's traditional Waterfall process from Phase A to Phase D, and another using an Agile approach with incremental Minimum Viable Products (MVPs). The models were compared regarding schedule and cost, revealing that the Agile approach delivered the satellite two times faster with reduced costs. However, applying Agile to safety-critical systems introduced several challenges, including regulatory compliance, safety assurance, integration complexity, bi-directional traceability, documentation requirements, and cultural barriers. We applied specific adaptations to the Agile model to address these challenges, including automated compliance checks, integrated hazard analysis, added traceability mechanisms, and streamlined documentation practices. Our findings suggest that these adaptations significantly mitigate the risks associated with Agile adoption in LS/SC/CPS. The study concludes that a tailored Agile approach—augmented with industry-specific adaptations—can improve development speed and flexibility while maintaining compliance, safety, and quality standards, thus providing a viable alternative to traditional Waterfall processes for future satellite development projects.

Keywords: Agile Large-Scale Safety-Critical Cyber-Physical

Introduction

In recent years, product development has increasingly become more volatile, uncertain, complex, and ambiguous (Ciric, 2018). To remain competitive in the marketplace, many businesses building cyber-physical systems are looking at alternatives such as Agile to reduce delivery times. The two most common approaches in product development are Waterfall, a linear stage gate process, and Agile, an iterative incremental approach. This paper focuses specifically on NASA's Waterfall process and scaled Agile approach.

Problem

A fundamental problem exists with traditional development processes. They only work well when requirements and risks are stable and well understood in advance (Heeager & Nielsen, 2018). As systems have become increasingly complex there has been a growing interest in applying Agile methodologies to large-scale, safety-critical cyber-physical (LS/SC/CP) systems across multiple domains due to the need to be able to adapt to changing requirements, increase the speed up delivery cycles, reduce life cycle costs, manage increasing complexity, and increase maintain quality (Yeman & Malaiya, 2023). The space industry struggles with multifaceted requirements, leading to complexity, long project timelines, and stringent safety requirements. Therefore, the application of Agile methods has the potential to impact schedule and cost significantly (Bart, 2024). The challenge is objectively evaluating the impacts of development process implementations in the context of complex systems (SoS) such as a satellite system.

Purpose

This research aims to objectively compare two distinct process implementations regarding cost and schedule when building an LS/SC/CP system, such as a satellite. The first implementation is NASA's life cycle approach to space and ground system development, documented in NASA's Systems Engineering Guidebook (NASA, n.d.). The second implementation is an Agile approach to building the system, utilizing a series of minimum viable products (MVPs).

Research Objectives and Question

Compare Agile and Waterfall approaches for LS/SC/CP system development. Highlight challenges and propose adaptations for Agile in these domains.

- RQ1: How does the application of Agile principles influence the system development process for LS/SC/CP systems compared to NASA's traditional systems engineering approach?
- RQ2: What are the primary challenges in applying Agile to developing safety-critical systems such as satellites?
- RQ3: What adaptations are necessary for Agile methodologies to be effective in LS/SC/CP system development?

Methodology

System Context

The mid-size Low-Earth Orbit (LEO) satellite under development is designed to provide high-resolution Earth imagery and weather monitoring capabilities. With a launch mass of 250 kg, this satellite is equipped with a 1 kW solar array to support its operational power needs. It also features dual band communication via S-band (125 Kbps uplink, 2 Mbps downlink) and X-band (650 Mbps downlink) for efficient data transmission.

The satellite's mission objectives focus on capturing Earth imagery for environmental monitoring, disaster response, and resource management while supporting weather observation and atmospheric data collection. The spacecraft is designed to operate in LEO, optimizing its orbital characteristics for frequent revisit times and continuous global coverage. This satellite aims to deliver critical data to researchers, meteorologists, and government agencies by leveraging advanced sensor payloads and high-speed communication links, contributing to improved forecasting, climate studies, and geospatial intelligence.

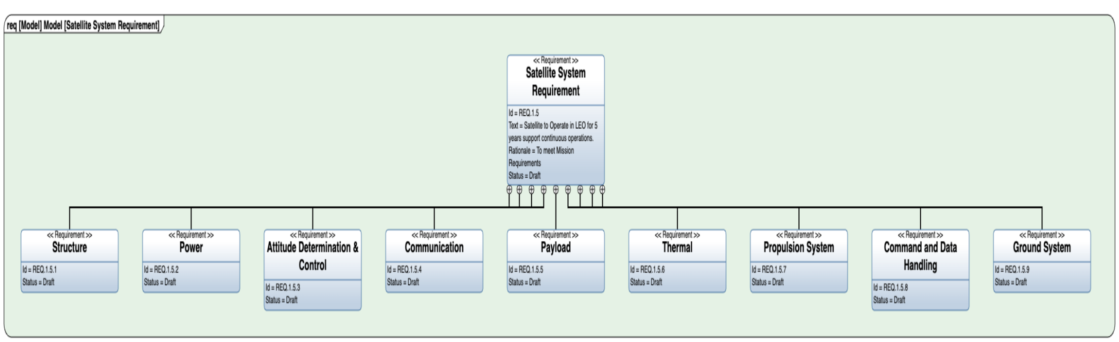

Figure 1. Satellite Requirements Diagram

Each model started with a detailed breakdown of each subsystem's inputs (components, requirements) and outputs (verified functionality). The inputs described in Table 1 were identical for both the Agile and Waterfall models to maintain consistency.

Table 1. Modeled Subsystem

	Subsystem	Inputs	Outputs
1.	Structure	Primary & Secondary Structures	Verified Structural Integrity
2.	Power	Battery, Solar Arrays	Power Distribution Verified
3.	Attitude Determination, Control	Reaction Wheels, Star Trackers, Software	Attitude accuracy verified
4.	Communications	Transmitters, Receivers, Antennae	Reliable communication link established
5.	Payload	Scientific Instruments, Payload Specifications	Data collection and processing operational
6.	Thermal Control	Radiators, Heaters, Insulation, sensors	Thermal Controls Verified
7.	Propulsion	Thrusters, Fuel Thanks, Piping	Basic maneuver capability established
8.	Command & Data handling	Onboard Computer, Software, Sensors	Command/Data Handling Verified

Subsystems

Developing a mid-size LEO satellite requires integrating multiple interdependent subsystems, each critical to mission success. These subsystems work together to provide structural integrity, power generation, attitude control, communication, payload operation, thermal regulation, propulsion, and command and data handling.

Structure

The structural subsystem is the satellite's backbone, providing mechanical support and protection for all internal components. It is designed to withstand the stresses of launch, the space environment, and on-orbit operations. The primary and secondary structures are lightweight yet durable materials, such as aluminum alloys and composite materials, ensuring rigidity and strength while minimizing mass. The structure also houses the payload and ensures proper alignment of sensors and antennas.

Power

The power subsystem generates, stores, and distributes electrical power to all onboard systems. The satellite has a 1 kW solar array, which collects and converts solar energy into electrical power. Lithium-ion batteries store excess energy during eclipse periods when the satellite is not exposed to sunlight. A power distribution unit (PDU) regulates and distributes power efficiently, ensuring uninterrupted operation of critical subsystems.

Attitude

Determination and Control System The Attitude Determination and Control System (ADCS) ensures the satellite's precise orientation and stability to maintain proper pointing for imaging, communication, and orbital maneuvers. The system includes reaction wheels, magnetometers, gyroscopes, and star trackers for attitude sensing and control. Magnetorquers or thrusters may be used for momentum management and stabilization after deployment. The ADCS enables accurate positioning for Earth observation and data transmission, ensuring optimal performance of the payload and antennas.

Communication

The communication subsystem provides command, telemetry, and data transmission capabilities between the satellite and ground stations. It operates in S-band (125 Kbps uplink, 2 Mbps downlink) for telemetry, tracking, and control (TT&C) and X-band (650 Mbps downlink) for high-data-rate payload transmission. The subsystem consists of high-gain and low-gain antennas and software-defined radios (SDRs) for efficient frequency modulation and adaptability to mission requirements.

Payload

The payload subsystem comprises high-resolution imaging sensors and weather monitoring instruments designed for Earth observation. The imaging system captures multispectral and thermal imagery for environmental monitoring, disaster response, and resource management. Weather instruments collect atmospheric data, cloud cover, and temperature variations, contributing to meteorological forecasting and climate studies. The payload is optimized for high spatial and temporal resolution to maximize scientific and operational benefits.

Thermal Control

The thermal control subsystem ensures that all components operate within their required temperature ranges in the extreme space environment. It includes passive thermal elements such as radiators, multi-layer insulation (MLI), coatings, and active thermal management using heaters and heat pipes. The system prevents electronic components from overheating and ensures that the payload, batteries, and communication systems function reliably across day-night temperature cycles in LEO.

Propulsion

The propulsion subsystem provides orbital maneuvering, attitude corrections, and station-keeping capabilities. It consists of thrusters, fuel tanks, piping, and valves for controlled thrust generation. The propulsion system supports collision avoidance maneuvers, deorbiting, and precise station adjustments, extending the satellite's operational lifetime and ensuring compliance with space debris mitigation guidelines.

Command and Data Handling

The command and data handling (C&DH) subsystem acts as the satellite's central processing unit, managing data flow between subsystems and executing mission operations. It includes an onboard computer, data storage units, and fault tolerant software. The system processes telemetry data, executes onboard autonomy algorithms, and ensures real-time decision-making. It also interfaces with the ground control center, executing commands and coordinating data collection, storage, and transmission.

Modeling Environment

Life cycle modeling is a structured approach to visualizing, analyzing, and managing the development, deployment, operation, and retirement of complex systems (Vaneman, 2016). It enables engineers and project managers to model the entire system life cycle using standardized methodologies such as SysML, LML, and UAF, ensuring alignment with industry standards. To effectively compare the Waterfall and Agile life cycles. Life cycle modeling in Innoslate is valuable for our fictional case study because it provides an integrated modeling environment capable of clearly visualizing, simulating, and analyzing differences in these methodologies. LML covers the entire system's life cycle, from conceptual development to disposal. The approach involved creating detailed activity and action diagrams, running simulations, and evaluating outcomes to objectively determine the effectiveness and suitability of Agile versus Waterfall for satellite development. Innoslate is a cloud based and on-premises platform that supports requirements management, modeling and simulation, verification and validation, risk analysis, and collaboration within a single digital environment.

Table 2 summarizes key assumptions underlying the satellite development models using both Waterfall and Agile methodologies. Multiple assumptions were made to simplify the modeling process and effectively compare these two distinct approaches. These assumptions focus on critical aspects such as requirements management, workflow structure, resource availability, integration, testing, compliance, and risk management. Clearly defining these boundaries ensures a consistent and fair comparison of each methodology within the context of satellite development.

Table 2. Modeling Assumptions

Category	**Waterfall Model Assumption**	**Agile Model Assumption**
Workflow	Follows NASA defined approach	Iterative and Incremental with Continuous Assurance Plugin (CAP)
Planning	Complete Integrated Master Schedule is defined before work starts.	Multiple Horizons Roadmap with Years decomposed into Quarterly Increments into 2-week sprints.
Materials/Components	All required materials and components are available from the start and cause no delays.	All required materials and components are available from the start and cause no delays.
Labor / Skill Availability	Skilled workforce available	Skilled Workforce Available
Integration / Test	Access to Test Environments readily available	CI/CD Pipeline
Regulatory Compliance and Safety	Validated at the Phase Gates	Automated and continuously validated at each sprint and Increment.
Material Cost	Fixed 5 million	Fixed 5 million
Labor Cost	$120 per hour	$120 per hour

We leveraged NASA’s Cost Estimating Guide (NASA, 2015) to estimate the satellite build costs under both Waterfall and Agile models. Our approach combined analogy cost estimating with an engineering build-up. We created work breakdown structures for each model for the engineering build-up. After comparing our estimates with subject matter experts and adjusting for their experience, we refined them to a rough order of magnitude.

Development Models

NASA Development Approach

The NASA Systems Engineering Handbook, initially published as SP-6105 in 1995, provided the foundation for the NASA Waterfall life cycle process (Hirshorn et al., 2017). NASA’s process for developing air and ground systems follows a linear approach, segmented into distinct project life cycle phases. The life cycle begins with Pre-Phase A: Concept Studies, where ideas and feasible alternatives are generated and evaluated for cost, technical feasibility, and risk. This leads into Phase A: Concept and Technology Development, which refines mission concepts and validates requirements. Phase B focuses on preliminary design and establishing design-dependent requirements and interfaces, while Phase C finalizes the detailed design and prepares for manufacturing. During Phase D, the system is assembled, integrated, and rigorously tested to ensure operational readiness. In Phase E, the system transitions to operations and sustainment, where performance is maintained and necessary upgrades are made. Finally, Phase F addresses decommissioning, data archival, and disposal. For purposes of this paper, we were interested in phases A–D.

Table 3. NASA Phases

Phase	Purpose	Inputs	Description	Outputs
A	Concept and Technology Development	Mission needs, feasibility studies	Define mission architecture, identify technology gaps	Concept Study Report, preliminary requirements
B	Preliminary Design & Technology Completion	Concept studies, tech develop	Finalize architecture, complete risk analysis, technology	Preliminary Design Review (PDR), risk reduction results
C	Final Design and Fabrication	PDR results, matured requirements	Conduct detailed design, build and test components	Critical Design Review (CDR), manufactured components
D	Assembly, Integration, and Test (AIT) & Launch	CDR results, fabricated components	Integrate subsystems, conduct testing, prepare for launch	Fully integrated system, Launch Readiness Review (LRR)

The NASA Waterfall process was modeled in Innoslate based on NASA's Systems Engineering Handbook (SP-20166105). The model illustrated in Figure 2 adhered to phased development with sequential stages and formal review gates at each phase.

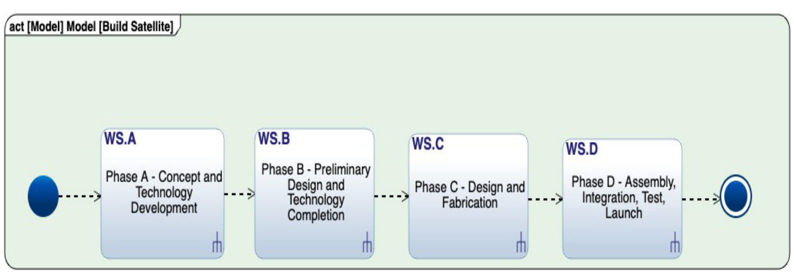

Figure 2. Model, Utilizing NASA Systems Engineering Handbook

Phase A: Concept and Technology Development

Phase A, illustrated in Figure 3, focuses on defining the mission concept, assessing feasibility, and identifying key technologies required for satellite development. The waterfall model, in general, is a sequential design process where progress flows steadily downwards through the phases of conception, initiation, analysis, design, construction, testing, production/implementation, and maintenance. However, at the close of Phase A, the customer will only have a series of documents without working capability. The goal of Phase A is to ensure that the project is technically, operationally, and financially viable before proceeding. However, this approach has not seemed to minimize overrun and schedule delays. The GAO has shown that their program cycle times are increasing by an average of three years from the planned date (GAO, 2024). We decomposed the system using Innoslate into small steps and then estimated using a triangular distribution for each step. For example, updating the Concept of Operations is calculated as a minimum of two weeks, a maximum of six weeks, and four weeks as most likely. The approach allows us to get cost and schedule estimates. The modeled system illustrated in Figure 3 completed in 1.16 years, which aligns with what GAO reports regarding the time SBIRS Phase A took, which is between 12–18 months (GAO, 2024).

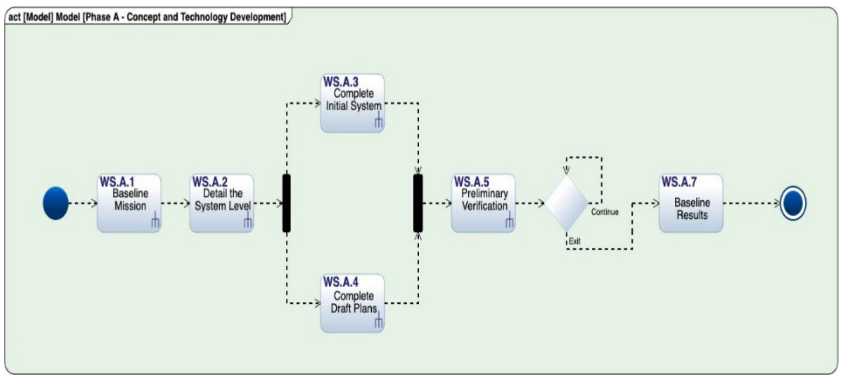

Figure 3. NASA Phase A: Concept and Technology Development

Phase B: Preliminary Design and Technology Completion

Phase 2, illustrated in Figure 4, the Preliminary Design and Technology Completion phase, is paramount to the success of space missions, serving as a critical bridge between the initial concept and final implementation. The mission design is rigorously refined during this phase, and key technologies are matured to minimize technical risks. Key activities include conducting a Preliminary Design Review (PDR) to evaluate the system design and maturing critical technologies like advanced propulsion systems or communication arrays. Further activities involve planning system integration and testing, refining cost and schedule estimates, managing risks, and engaging stakeholders. The goal is to ensure the project is on track for successful implementation, within budget, and on schedule, ultimately paving the way for a successful mission.

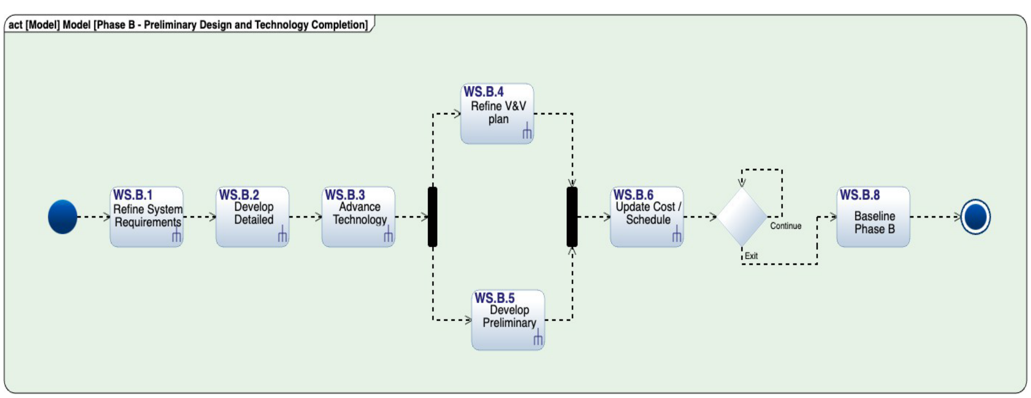

Figure 4. NASA Phase B

Phase C: Final Design and Fabrication

NASA's Phase C, illustrated in Figure 5, known as the Final Design and Fabrication phase, focuses on completing the detailed design of the system, fabricating and assembling components, and preparing for system integration and testing. Key activities include conducting a Critical Design Review (CDR) to ensure the design meets all mission requirements, finalizing detailed engineering drawings and specifications, and beginning the fabrication and assembly of system components. The project team also develops detailed plans for system integration and testing, continues to manage risks, and engages with stakeholders to keep them informed about the project's progress and any changes to the mission design or objectives.

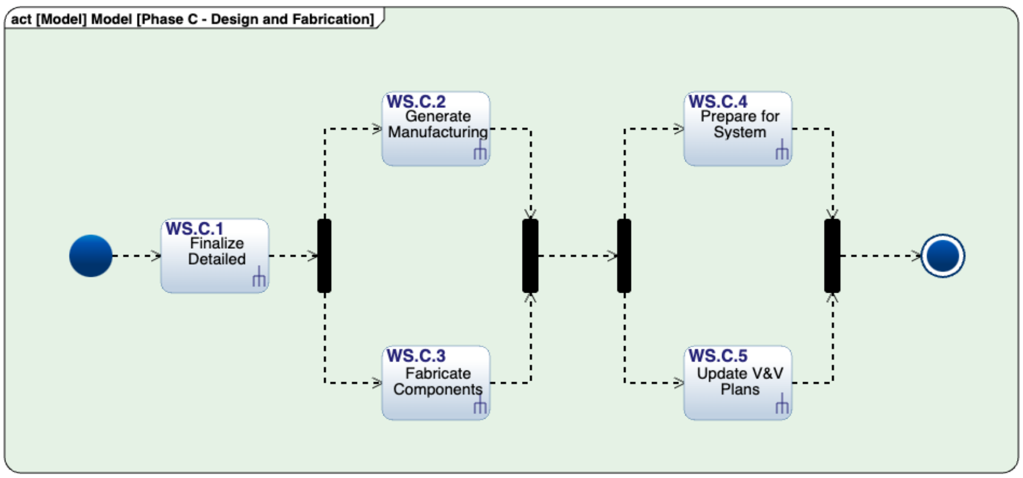

Figure 5. NASA Phase C

Phase D: Assembly, Integration, and Testing

Phase D, shown in Figure 6, known as the Assembly, Integration, and Testing (AIT) phase, focuses on assembling system components, integrating subsystems, and conducting comprehensive testing to ensure the system meets all mission requirements and is ready for deployment. Key activities include system assembly, integration, and extensive testing to verify performance, reliability, and safety. The project team conducts a Test Readiness Review (TRR) to confirm readiness for testing, prepares the system for operational deployment, and continues to manage risks. Ongoing stakeholder engagement ensures that all parties are informed about the project's progress and any changes associated with mission design or objectives.

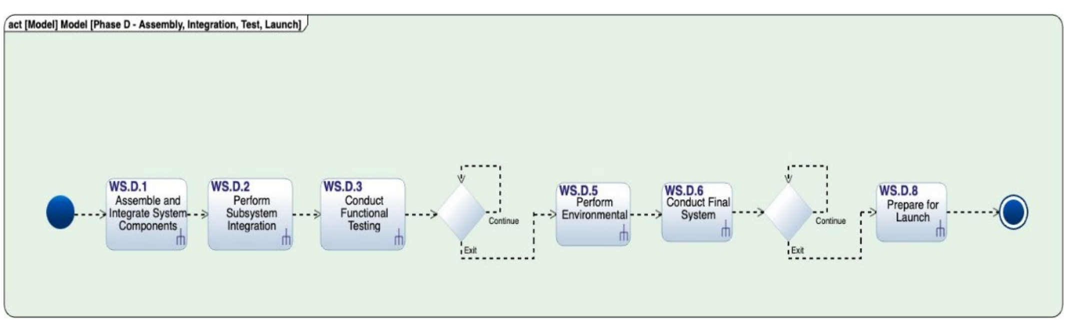

Figure 6. NASA Phase D

Analysis and Results

The Monte Carlo simulation in Innoslate provided key insights into the expected duration and labor cost for building a satellite, considering project timelines and resource expenditures variability. The analysis shown in Figure 7 revealed that the mean duration to build the satellite is 5.89 years, with a standard deviation of 1.53 months. This indicates that the average completion time is relatively stable. This stability is due to the assumption that all materials and resources were readily available. This would exhibit much greater variability if supply chain integration were factored in.

In terms of cost, Labor cost was estimated at $7,858,335.14, representing the primary expenditure tracked in the analysis. We assumed the Agile and Waterfall approaches would yield a similar BoM due to the same hardware and components used in both development methodologies. This assumption allowed for a focused comparison of schedule efficiency and labor expenditures between the two methodologies. The findings highlight the expected resource commitment for satellite development, with potential applications in refining project scheduling and cost allocation strategies for future space missions.

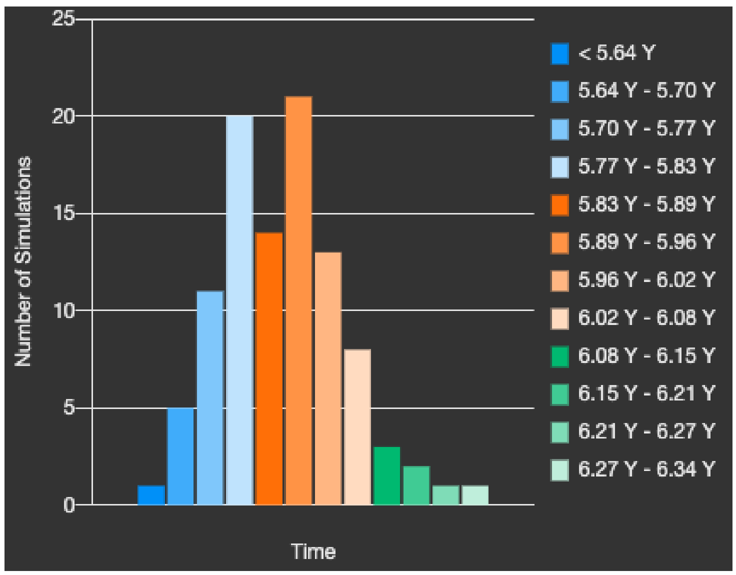

Figure 7. Monte-Carlo Analysis of Waterfall Development Process

Agile Approach

Agile is an iterative and incremental approach to engineering characterized by iterative and incremental development, short feedback loops, continuous integration and verification, and adaptability to change within complex, evolving environments. The traditional Waterfall approach has been the norm for aerospace, but a growing community in Space is transitioning to Agile (Ribeiro et al., 2024). Some of these trailblazers include SpaceX (Peterson & Mocko, 2024), Planet Labs (Donahue et al., 2024), Relativity (Araujo, 2019). For this paper, we took inspiration from organizations such as SpaceX (de Freitas Bart, 2024). We defined a hypothetical approach, the Continuous Assurance Plugin (CAP), that can support Agile Frameworks by adding specific guidance to support regulatory compliance, safety constraints, and integration complexity.

Continuous Assurance Plugin

The CAP illustrated below in Figure 8 begins by leveraging SAFe's core framework. We decomposed the satellite system into MVPs, Epics, Features, and Stories following core principles of decomposition, abstraction, encapsulation, well-defined interfaces, and independence. This resolved some well-documented challenges in Agile for Hardware: products are difficult to decompose into modules, and systems integration efforts are difficult to break down into small tasks (Drutchas & Eppinger, 2022).

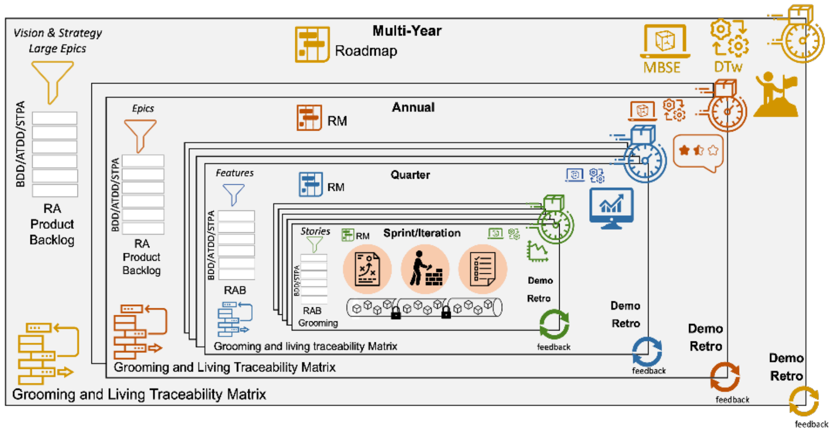

Figure 8. Building LS/SC/CP systems with CAS

An MVP is a concept popularized by Eric Ries. He defined MVP as “a product that allows a team to collect the maximum amount of validated learning about customers with the least effort” (Ries, 2009). We created MVPs associated with each of the satellite subsystems. According to SAFe, Epics are a significant solution initiative that requires an MVP. Due to the size of the fictional case study, our epics and MVPs have a 1 to 1 relationship. Epics decompose into more minor features, which, by definition, need to be less than 12 weeks. Features decompose into stories that need less than a sprint length, typically two weeks. Although our Agile approach forgoes Phase-gated Systems Engineering reviews, we must still meet regulatory compliance and safety assurance requirements through our CAP outlined in Table 4. Therefore, we are implementing a continuous assurance approach, contrasting with the traditional waterfall methodology, where assurance is tightly coupled to phase gates.

Table 4. CAP Features

Feature	Description	Benefit
Modular Architecture	Principles of decomposition with well-defined interfaces	Reduces dependencies across teams and impact of change.
MBSE	Model everything from requirements and design to verification and validation	System Transparency allows communication and reduces integration complexity
Digital Twin	Dynamic interactive model that mirrors the system’s behavior and performance.	Real-time feedback on the impact of system updates. Allowing safe option exploration
Boundary Objects	Artifacts, terms, or concepts that serve as a point of reference	Facilitate communication and understanding between diverse groups.
Enabler Stories	Safety and regulatory tasks in product backlogs (e.g., “As a system, I must comply with MIL-STD-882E for fault tolerance.”)	Ensuring that we are building regulatory compliance, safety, and security into the system.
BDD/STPA Integration	BDD defines system behavior through user stories and scenarios. STPA identifies potential hazards, ensuring safety constraints are met.	Write safety-focused scenarios that prevent hazards, including edge cases.
ATDD	Defining acceptance test criteria for regulatory and safety before development begins.	Ensures capabilities are not accepted until they comply with functional and safety requirements.

Risk-Adjusted Backlog	Prioritized backlog that incorporates risk analysis.	Provides transparency into risk exposure to enable prioritization
Living Traceability Matrix	Every requirement is traced to its corresponding design implementation, and test artifacts,	Provides transparency to support regulatory and safety compliance.
Compliance Test Automation	Automated Safety and Compliance Tests	Compliance validation is integrated into the development process
CI/CD Pipeline	CI/CD pipelines that incorporate HIL and SIL to validate cybersecurity (DO-326A, NIST 800-53) and reliability (ISO 26262)	Integrating SIL and HIL into the CI/CD pipeline, provides continuous/comprehensive validation of the entire system.
Chaos Engineering	CI/CD pipeline that regularly injects failures into the system before they manifest in production,	Enhances the resilience and reliability of systems.
Digital Compliance Checklist	Checklist integrates compliance activities into the Agile workflow.	real-time monitoring, validation, and documentation.
Iterative Reviews	A systematic approach to continuously meet safety and regulatory requirements	Identifies potential issues early, reducing the risk to safety and reliability of the system
Expand the Definition of Done	Define “Done” to include safety and compliance checks.	ensure that these critical aspects are addressed consistently and thoroughly.

We address safety and regulatory compliance challenges with our CAP that integrates continuous safety and regulatory compliance throughout the MVP development cycle. This approach decouples safety validation from traditional milestone reviews and embeds incremental safety checks, automated compliance verification, and regulatory traceability within Agile workflows.

Table 5. Caption

MVP	Safety / Compliance Actions	Validations
Startup/ Initialization	Incorporate Safety & Compliance into Risk Adjusted Backlog, define incremental safety validation workflow, set up regulatory checklists in Agile tools	System Safety: MIL-STD-882E (DoD, 2012), NASA NPR 8715.3 (NASA, 2020), Cybersecurity: NIST 800-53 (National Institute of Standards and Technology, 2020), ITAR compliance tracking (U.S. Department of State, 2021)
1 Basic Structure & Power System	Perform Continuous structural risk assessments (MBSE for load/stress), Automate material compliance tracking (e.g., REACH)	System Safety: IEC 61508 (Brown, 2000), ISO 26262 (International Organization for Standardization, 2018), Environmental & Health: REACH (European Chemicals Agency, 2022), OSHA (Occupational Safety and Health Administration, 2022), ANSI (American National Standards Institute, 2021) Aerospace: NASA-STD-8719.14 (Wilcutt, 2021)
2 Command & Data Handling (C&DH)	Implement early cyber compliance checks (DO-326A, NIST 800-53), Automate software static analysis	Software & Cybersecurity: DO-178C (Radio Technical Commission for Aeronautics, 2011), DO-326A (Radio Technical Commission for Aeronautics, 2014), NIST 800-53 (National Institute of Standards and Technology, 2020), FedRAMP (GSA, 2021)

3 Attitude Determination & Control	Integrate real-time fault tolerance testing into Agile test pipelines, Validate software/hardware failure modes in digital twin	System Safety: MIL-STD 882E (DoD, 2012), IEC 61508 (Brown, 2000) Cybersecurity: DO 326A (Radio Technical Commission for Aeronautics, 2014), ITAR (U.S. Department of State, 2021)
4 Propulsion System	•Perform continuous hazardous material tracking, Automate ITAR compliance for propulsion components	System Safety: MIL-STD-882E (DoD, 2012), Environmental & Health: EPA (U.S. Environmental Protection Agency, 2022), OSHA (Occupational Safety and Health Administration, 2022), Aerospace: FAA Part 450 (Federal Aviation Administration, 2021)
5 Communication System	Embed EMI/EMC compliance verification within Agile sprints, Automate the regulatory spectrum compliance (FCC, ITU)	Electromagnetic Compliance: MIL-STD-461 (DoD, 2015), FCC (Federal Communications Commission, 2021) regulations, Cybersecurity: NIST 800-53 (National Institute of Standards and Technology, 2020), ITAR (U.S. Department of State, 2021)
6 Thermal System	Integrate thermal risk modeling into MBSE simulations, Automate compliance with NASA-STD-8719.14	System Safety: ISO 26262 (International Organization for Standardization, 2018), IEC 61508 (Brown, 2000), Aerospace: NASA-STD-8719.14 (Wilcutt, 2021)
7 Payload	Ensure payload-specific safety testing in sprint test cases, Continuous FAA payload integration compliance tracking	System Safety: MIL-STD-882E (DoD, 2012), NASA NPR 8715.3 (NASA, 2020), Aerospace FAA Part 450 (Federal Aviation Administration, 2021), ITAR (U.S. Department of State, 2021)
8 Full System Integration	Implement incremental safety audits per increment, Continuous traceability of safety requirements via MBSE	System Safety: MIL-STD-882E (DoD, 2012), IEC 61508 (Brown, 2000), Cybersecurity: DO-178C (Radio Technical Commission for Aeronautics, 2011), DO-326A (Radio Technical Commission for Aeronautics, 2014), NIST 800-53 (National Institute of Standards and Technology, 2020)
9 Launch Ready	Final safety validations automated in DevSecOps pipeline, Incremental FAA Part 450 launch compliance verified continuously	Aerospace & Space: FAA Part 450 (Federal Aviation Administration, 2021), NASA-STD-8719.14 (Wilcutt, 2021), Environmental & Health: OSHA (Occupational Safety and Health Administration, 2022), EPA (U.S. Environmental Protection Agency, 2022), ANSI (American National Standards Institute, 2021)

Model Setup

We began with the SpaceX approach to decomposing the satellite into a modular set of capabilities (de Freitas Bart, 2024). Once we decomposed the system, we outlined a series of MVPs and next viable products (NVPs) to deliver the system. MVP and NVP refer to a concept in product development grounded in the principles of the Lean Startup methodology, which emphasizes rapid iteration, customer feedback, and adaptive planning (Stevenson et al., 2024). We leverage Planet Labs' approach to rapidly create and integrate a prototype and then evolve it with software updates to deliver satellites with relatively short design cycles. Before delivery for launch, the focus is on developing and validating an MVP (Donahue et al., 2024). The top-level model is shown in Figure 9.

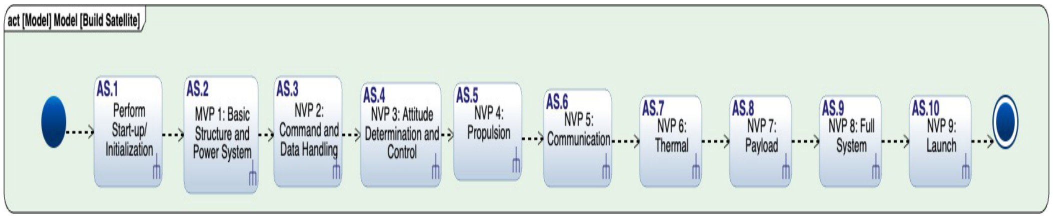

Figure 9. Agile Satellite Approach

Start-up and Initialization

Modeled in Figure 10, our Agile approach's Startup and Initialization timebox focuses on establishing the foundational digital environment, complete with a digital thread that spans the entire development process. This digital-first strategy is gaining traction, as illustrated by Istari's $19 million contract to digitally certify Lockheed Martin's XPlane (Istari Digital, 2024), and the digital system building approaches used in Formula 1 (Mayani et al., 2018). Key inputs include mission and system requirements, regulatory and safety constraints, performance parameters, development tools, and stakeholder involvement. The process begins with analyzing mission objectives and refining system requirements into actionable backlog items. Key performance and compliance factors are reviewed, and initial SysML and 3D modeling help define system structure and behavior. A roadmap outlines incremental MVPs for phased development. Business rhythms are established to ensure synchronization, an Agile performance measurement baseline is defined, and development teams are structured. A product backlog is created, incorporating ATDD acceptance criteria for each feature. Development and test environments, including Continuous Integration/Continuous Delivery (CI/CD) pipelines and automated testing frameworks, are established. Critically, during this increment, we integrate safety and compliance directly into our workflow by incorporating safety and compliance into the risk adjusted backlog, defining an incremental safety validation workflow, and setting up regulatory checklists within our Agile tools. We ensure we meet MIL-STD-882E, NASA NPR 8715.3, NIST 800-53, and ITAR compliance tracking. Outputs of this increment include a risk-adjusted backlog, incorporating quantitative risk analysis (Parente, 2018), an Agile performance measurement baseline covering budget, scope, and schedule (Alleman et al., 2014), a roadmap defining MVPs (Trieflinger et al., 2021), draft management and technical plans, and a finalized organizational structure. The Monte Carlo analysis for this portion of the project had a Mean of 4.05 months with a standard deviation of 11.38 days.

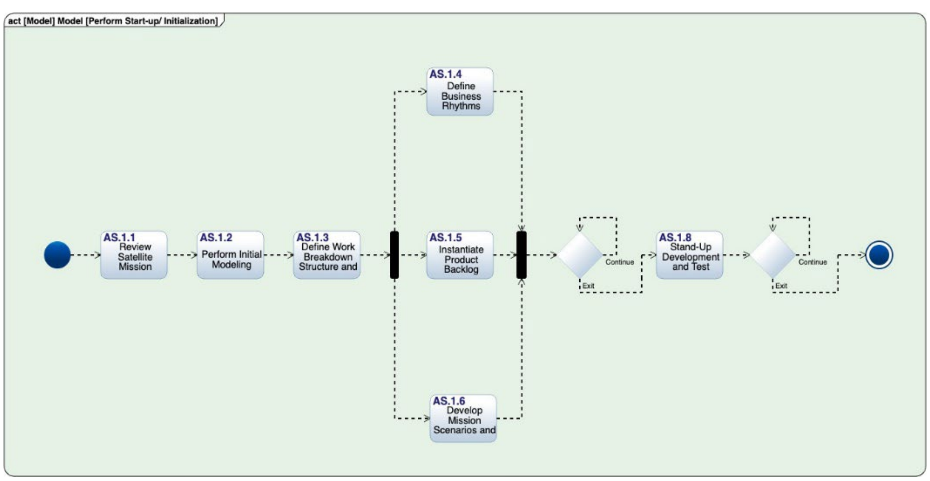

Figure 10. Start-up and Initialization

MVP 1 Basic Structure and Power System

MVP 1, as shown in Figure 11, establishes the foundational framework and power system required for the satellite: basic structure and power. This increment begins with backlog grooming and Program Increment (PI) planning, ensuring that acceptance criteria are well-defined. The roadmap, design specifications, and Interface Control Documents (ICDs) guide the development. Concurrently, teams gather materials, including the primary and secondary structures, solar arrays, batteries, and a PDU. The assembly process involves constructing the satellite's frame, installing solar panels and batteries, and integrating the PDU to regulate power distribution. In parallel with the assembly and testing, we perform continuous structural risk assessments using Model-Based Systems Engineering (MBSE) for load and stress analysis and automate material compliance tracking (e.g., REACH). These actions ensure adherence to critical safety and regulatory standards, including System Safety (IEC 61508, ISO 26262), Environmental & Health (REACH, OSHA, ANSI), and Aerospace (NASA-STD-8719.14). Testing focuses on validating structural integrity, power generation, and energy storage, ensuring all components function as expected before progressing to the next MVP.

Completion of MVP 1 results in a digitally validated structural and power system (Mirabella et al., 2024), with test reports confirming performance and risk-adjusted backlog updates informing the next development iteration. The demonstration showcases the assembled structure, operational solar arrays, and digitally demonstrated functional power distribution. The Monte-Carlo Analysis for this increment showed a Mean of 2.3 months with a standard deviation of 8 days. This would take much longer if we had not assumed we had procured materials.

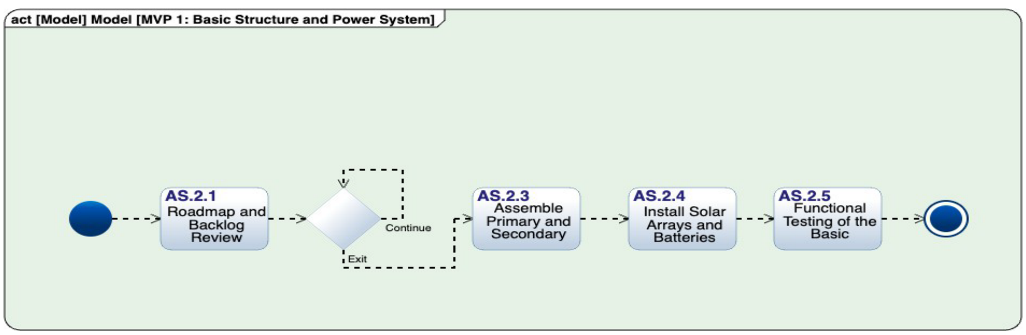

Figure 11. Structure and Basic Power

NVP 2 Command and Data Handling

C&DH, modeled in Figure 12, focuses on integrating the satellite's central processing and data management system, ensuring it can receive, process, and execute commands while handling telemetry and onboard data storage. This increment of development includes critical safety and compliance actions: implementing early cyber compliance checks (DO-326A, NIST 800-53) and automating software static analysis. The development starts with backlog grooming, PI planning, and refining acceptance criteria. The key components include the Onboard Computer (OBC), Data Storage Unit, Telemetry Interface, and redundant processing modules, all integrated and tested within our NASA-verified digital environment (Hill et al., 2024). The process involves assembling and connecting the OBC, configuring data storage, linking telemetry interfaces, and deploying the initial software stack to validate system functionality. Testing ensures command execution, data processing, and real-time system health monitoring, confirming that the C&DH system meets mission requirements before progressing to the next MVP. This work is conducted to meet the following standards: DO-178C, DO-326A, NIST 800-53, and FedRAMP.

The successful completion of NVP 2 results in an integrated and validated C&DH

system, providing a functional command execution and data handling framework. This system is foundational for controlling all subsequent subsystems, including Attitude Determination and Control (ADC), Propulsion, and Communication, ensuring the satellite can effectively manage operations and respond to mission commands. The output includes a risk-adjusted backlog, an operational OBC, verified telemetry reporting, and test reports confirming system reliability by following an iterative Agile approach similar to Liubimov's approach for CubeSat (Liubimov et al., 2023). Monte Carlo Analysis for this increment had a mean of 2.22 months with a standard deviation of 8 days.

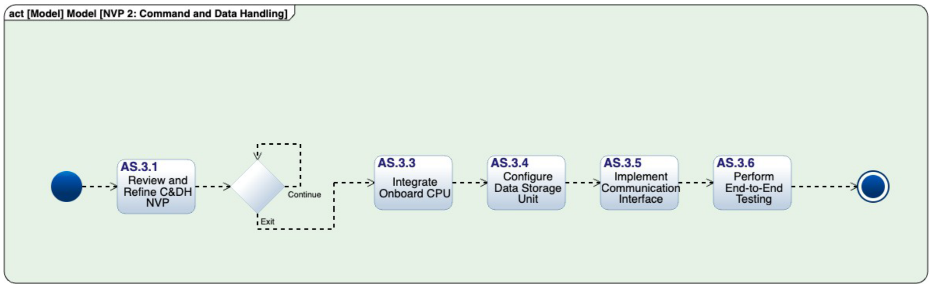

Figure 12. Command and Data Handling

NVP 3 Attitude Determination and Control

As illustrated in Figure 13, the ADCS enables the satellite to determine and adjust its orientation in Space. This increment begins with backlog grooming and PI planning. Key steps include integrating and configuring ADCS sensors, implementing attitude determination algorithms, and testing system responsiveness under Hardware-in-the-Loop (HIL) and Software-in-the-Loop (SIL) simulations. Testing ensures the system accurately determines orientation, executes attitude corrections, and maintains stability under simulated mission conditions.

In parallel with the ADCS integration and testing, we integrate real-time fault tolerance testing into Agile test pipelines and validate software/hardware failure modes in the digital twin. These actions ensure adherence to critical safety and regulatory standards, including System Safety (MIL-STD882E, IEC 61508) and Cybersecurity (DO-326A, ITAR).

Successful completion of NVP 3 results in a fully operational ADCS, with validated attitude accuracy, control responsiveness, and integration with the OBC. Key outputs include calibration reports, Reaction Control System (RCS) performance logs, end-to-end integration test reports, and updated ICDs. The RCS is a system of thrusters used to control the attitude and position of the satellite. These validations ensure the ADCS can support precision pointing for payload operations, stable communication alignment, and controlled maneuvers in future MVPs. MVP 3 sets the foundation for integrating propulsion, communications, and mission-specific payload operations by establishing a stable and autonomous orientation control system. The Monte Carlo analysis shows a Mean of 2.81 months with a standard deviation of 9 days.

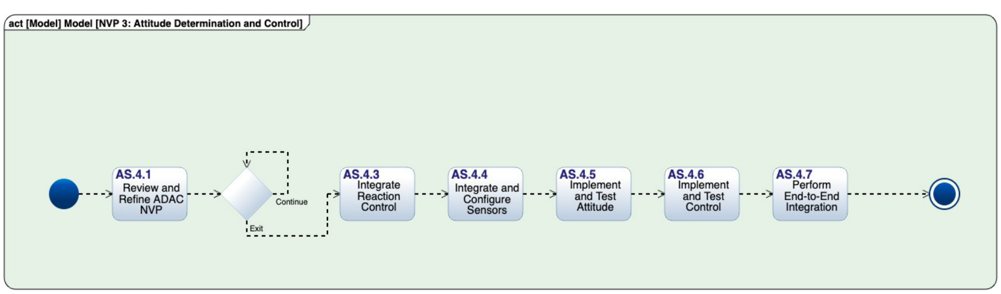

Figure 13. Attitude Determination and Control

NVP 4 Propulsion System

The process begins with backlog grooming and PI planning, ensuring alignment with previous NVPs such as ADCS and C&DH. The integration phase includes installing the propulsion unit, fuel tanks, valves, and sensors, and implementing thruster control algorithms to regulate fuel flow and thrust activation. Testing employs HIL and SIL simulations, assessing system responsiveness under simulated orbital conditions to validate fuel system functionality, thruster performance, and maneuver execution before final integration. (HIL simulations test the hardware and software together, while SIL simulations focus on testing software components.) Monte Carlo analysis for this MVP indicated a mean completion time of 3.28 months with a standard deviation of 11 days. This work is conducted to meet the following standards: System Safety: MIL-STD-882E; Environmental & Health: EPA, OSHA; and Aerospace: FAA Part 450.

The successful completion of NVP 4 ensures validated thruster performance, fuel flow control, and essential maneuvering capability, enabling the satellite to conduct orbital corrections and maintain stability. Key outputs confirm propulsion functionality within expected mission parameters, including integration and test reports, updated ICDs, and end-to-end system validation results. This increment lays the foundation for higher-level operations, such as payload positioning, communication adjustments, and station-keeping, while resolving anomalies and refining system parameters for future NVPs.

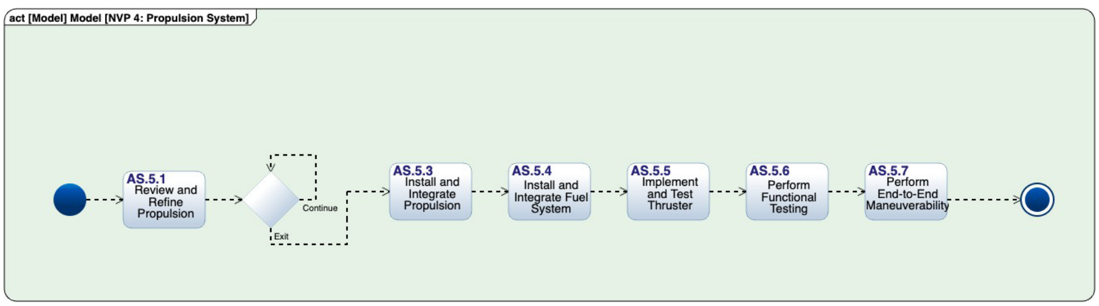

Figure 14. Propulsion

NVP 5 Communication System

The communication subsystem, illustrated in Figure 15, focuses on integrating and validating the satellite's ability to transmit and receive data reliably, a critical function for maintaining mission control and data integrity. This increment includes vital safety and regulatory actions: embedding EMI/EMC compliance verification within Agile sprints and automating regulatory spectrum compliance (FCC, ITU). This increment involves installing and testing transmitters, receivers, amplifiers, and high/low-gain antennas, ensuring seamless integration with the C&DH system. The system's communication control algorithms are deployed and validated through HIL and SIL setups, simulating real-world orbital conditions. (HIL simulations test the hardware and software together, while SIL simulations focus on testing software components.) Functional testing ensures data transmission rates, telemetry downlink, and ground station communication operate within expected parameters before full system integration. RF performance metrics are vital to ensure the signal strength and quality are within acceptable ranges for reliable communication. Monte Carlo analysis for this MVP indicated a mean completion time of 2.8 months with a standard deviation of 9 days. This work is conducted to meet the following standards: Electromagnetic Compliance: MIL-STD-461, FCC regulations; Cybersecurity: NIST 800-53, ITAR.

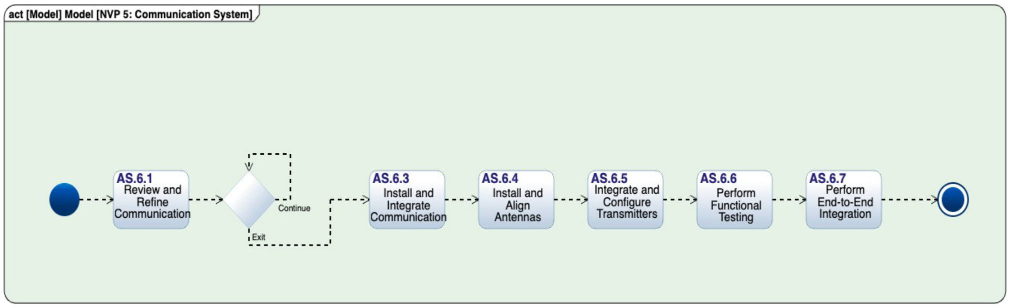

Figure 15. Communication

The successful completion of MVP 5 results in a validated communication system, enabling secure and efficient data exchange between the satellite and the ground station. Output includes integration test reports, RF performance metrics, updated ICDs, and resolved anomaly logs. This MVP ensures that telemetry, remote command execution, and payload data transmission function as required, laying the groundwork for full operational deployment. With a robust and tested communication link, the satellite is prepared for advanced mission operations, including real-time system monitoring and data collection, supporting the final integration and launch readiness phases.

NVP 6 Thermal

The Thermal Control System, modeled in Figure 16, ensures that the satellite can maintain stable operating temperatures in extreme orbital conditions, a critical function for preserving the integrity and performance of all onboard systems. This MVP includes vital safety and regulatory actions: integrating thermal risk modeling into MBSE simulations and automating compliance with NASA-STD8719.14. This subsystem integrates radiators, heaters, MLI, and temperature sensors, ensuring thermal regulation across all subsystems. The process begins with PI planning and backlog refinement, followed by the installation of thermal hardware and validation through thermal vacuum (TVAC) chamber testing and simulations. (TVAC testing simulates Space's vacuum and extreme temperature conditions to ensure the thermal system can perform as expected.) The thermal control algorithms are implemented and tested under simulated operational scenarios to verify heat dissipation, insulation efficiency, and active temperature regulation. Functional and end-to-end integration tests confirm that radiators manage excess heat, heaters prevent cold-related failures, and MLI stabilizes subsystem temperatures, ensuring compliance with mission requirements. MLI is vital to minimize heat transfer through radiation, the primary form of heat transfer in Space. Monte Carlo analysis for this MVP indicated a mean completion time of 2.7 months with a standard deviation of 9 days. This work is conducted to meet the following standards: System Safety: ISO 26262, IEC 61508; Aerospace: NASA-STD-8719.14.

The successful completion of NVP 6 results in a validated thermal system, with test reports confirming temperature stability, heater responsiveness, and subsystem integration with the power and structural systems. Key output includes updated ICDs, integration test reports, and an adjusted backlog reflecting lessons learned. This MVP establishes a reliable thermal management framework, protecting critical satellite components and enabling sustained operation in Space. A robust and tested thermal system prepares the satellite for mission operations and long-duration performance in extreme environments.

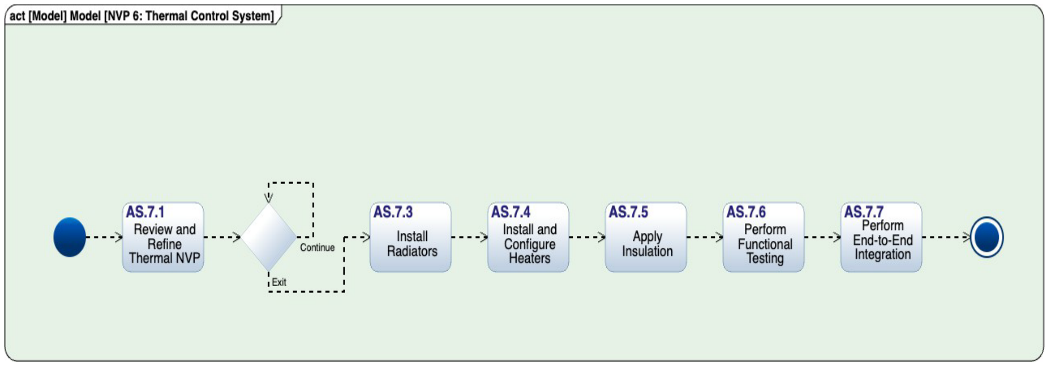

Figure 16. Thermal

NVP 7 Payload System

The Payload System, illustrated in Figure 17, focuses on integrating and validating the scientific instruments and data processing capabilities essential for the satellite's mission. This increment includes critical safety and regulatory compliance activities: ensuring payload-specific safety testing in sprint test cases and continuous FAA payload integration compliance tracking. This increment ensures seamless integration with the C&DH, Power, and Communication Systems, enabling efficient data collection, processing, and transmission. The process begins with planning for the PI, refining backlog priorities, and defining key milestones. The scientific instruments, power and data harnesses, and payload control software are installed and tested using HIL setups, functional test benches, and simulated operational scenarios. (HIL setups allow for testing hardware and software components in a simulated environment, ensuring they function together as expected.) Functional testing validates instrument accuracy, data acquisition, and real-time processing, ensuring stable payload operations before full system integration. The Monte Carlo analysis for this MVP indicated a mean completion time of 2.83 months with a standard deviation of 9 days. This work is conducted to meet the following standards: System Safety: MIL-STD-882E, NASA NPR 8715.3; Aerospace: FAA Part 450, ITAR.

The successful completion of NVP 7 results in a validated payload system with proven data collection, processing, and communication capabilities. Key output includes integration test reports, updated ICDs, and functional verification results, confirming power efficiency, OBC integration, and ground station connectivity. This NVP ensures the satellite is fully equipped for its mission by establishing a robust payload management and data transmission framework. With all payload components successfully tested and integrated, the satellite is prepared for final system validation and launch preparation in the next phase.

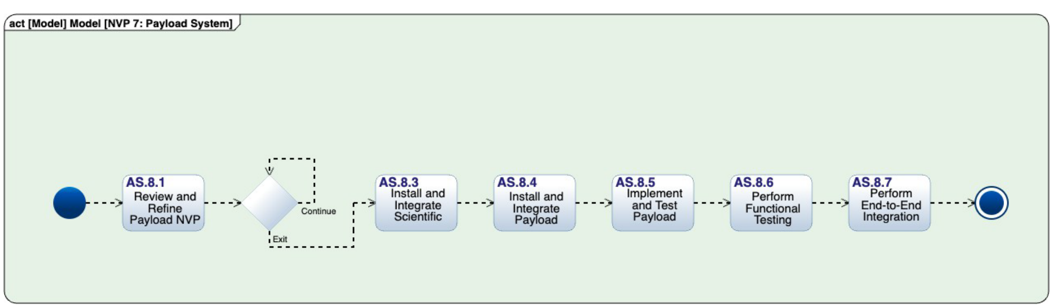

Figure 17. Payload

NVP 8 Full System Integration

The Full System Integration step, illustrated in Figure 18, ensures that all previously developed subsystems—including structure, power, C&DH, ADCS, propulsion, communication, thermal, and payload—are successfully assembled into a fully functional satellite, a pivotal achievement for mission success. This NVP includes critical safety and regulatory actions, such as implementing incremental safety audits per increment and continuous traceability of safety requirements via MBSE and digital twin. This increment begins with PI planning, refining integration steps, and validating that all ICDs, mission objectives, and testing procedures are in place. The integration process involves assembling mechanical, electrical, and data systems, ensuring seamless subsystem interaction. The payload control software is deployed and tested to verify command execution, telemetry monitoring, and data processing, while power and data harnesses are connected to ensure full operational capability.

The final integration test reports updated ICDs, and mission validation reports comprehensively assess system performance. These ICDs are vital for documenting and controlling the interfaces between the many subsystems of the satellite. Comprehensive functional and environmental testing is conducted to validate the satellite's performance under real-world conditions. TVAC tests simulate space conditions, ensuring the thermal control system functions as expected. Vibration and acoustic tests ensure structural integrity for launch, verifying that the satellite can withstand the stresses of liftoff. HIL and SIL setups are used for mission simulations, verifying end-to-end mission execution from launch to operational scenarios. (HIL tests combine hardware and software components, while SIL tests focus on software components.) A ground station emulator validates the satellite's ability to receive and execute ground commands, perform orbital maneuvers, and process payload data. Monte Carlo analysis for this MVP indicated a mean completion time of 3.1 months with a standard deviation of 8 days. This work is conducted to meet the following standards: System Safety: MIL-STD-882E, IEC 61508; Cybersecurity: DO-178C, DO326A, NIST 800-53.

With full-system functionality verified, this MVP confirms that the satellite is mission-ready and compliant with all regulatory requirements. The successful integration and testing of all components ensure the satellite can withstand launch stresses, operate reliably in orbit, and achieve mission objectives. This milestone prepares the satellite for final launch readiness assessments, marking the transition from development to deployment.

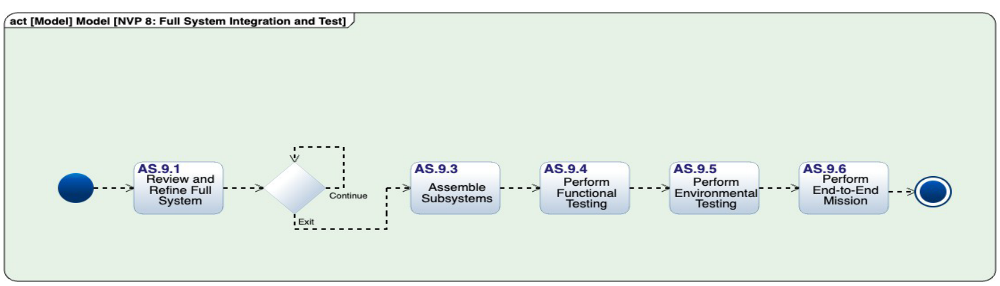

Figure 18. Full System Integration

NVP 9 Launch

The final MVP, shown in Figure 19, Launch Readiness ensures the satellite is fully prepared for launch, validating mechanical, electrical, and software integration with the launch vehicle and ground control systems, a crucial step for mission success. This NVP includes critical safety and regulatory actions: final safety validations are automated in the DevSecOps pipeline, and incremental FAA Part 450 launch compliance is verified continuously. This increment involves final pre-launch inspections, system validation, and compliance certification, ensuring the satellite can withstand launch conditions and establish a stable connection with ground control. The Launch Readiness Checklist, mission software, and telemetry systems are tested in a simulated launch control environment, verifying that the satellite can receive and execute commands post-deployment. (Simulating a launch control environment allows for verification of all procedures and software in a controlled setting.) The ground control interface is validated, ensuring seamless data transmission between the satellite and ground stations. Monte Carlo analysis for this NVP indicated a mean completion time of 2.8 months with a standard deviation of 9 days. This work is conducted to meet the following standards: Aerospace & Space: FAA Part 450, NASA-STD-8719.14; Environmental & Health: OSHA [126], EPA, ANSI.

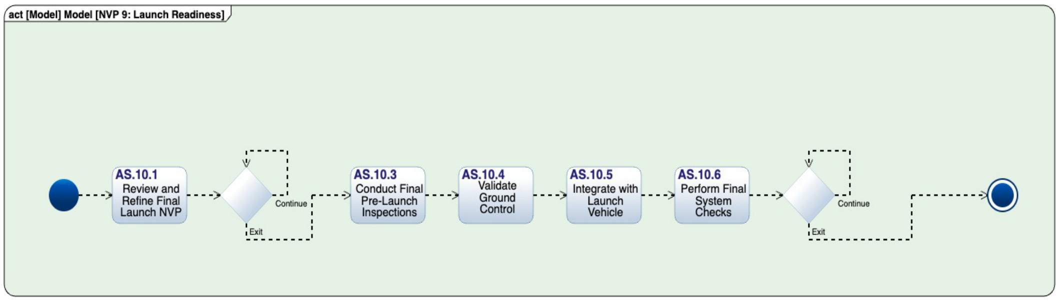

Figure 19. Launch

With successful final system checks, integration with the launch vehicle, and regulatory approval, this MVP confirms that the satellite is flight-ready and has no unresolved technical issues. Key outputs include final inspection reports, launch readiness certification, and validated telemetry systems. These telemetry systems are essential for monitoring the satellite's health after launch. This milestone marks the transition from development to operational deployment, ensuring the satellite is cleared for launch and prepared for its mission in orbit.

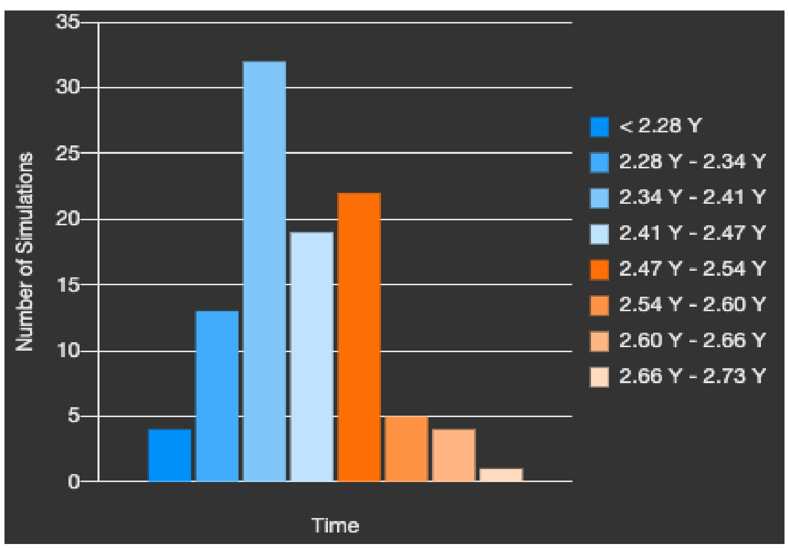

Figure 20. Monte-Carlo Analysis of Agile Development Cycle

Analysis and Results

The Monte Carlo simulation illustrated in Figure 20 for the Agile satellite development approach yielded a mean duration of 2.4 years with a standard deviation of 1 month. In terms of labor cost, we calculated $2,636,244.12. This result indicates a highly predictable development timeline, with Agile allowing for faster delivery compared to the Waterfall approach's mean duration of 5.89 years. The relatively low standard deviation further reinforces that Agile's incremental development cycles, iterative feedback loops, and continuous integration practices help maintain schedule stability, even in complex system builds.

Importantly, this analysis assumed full availability of materials and resources, meaning that delays related to procurement, supply chain disruptions, or resource shortages were not factored into the simulation. This assumption contributed to the high predictability of Agile's results, minimizing variability in the projected timeline. In real-world conditions, Agile's adaptability to changing requirements and resource fluctuations may provide an advantage over Waterfall, which tends to experience more schedule slips when unexpected constraints arise. The findings demonstrate that, under optimal conditions, Agile can deliver a satellite in less than half the time of a traditional approach while maintaining low schedule uncertainty, making it a viable methodology for accelerating space system development.

Discussion

This study compares Agile and Waterfall methodologies for satellite system development, evaluating their impact on timeline efficiency, risk mitigation, and regulatory compliance. The Monte Carlo analysis demonstrated that Agile significantly reduces development time, with a mean duration of 2.4 years compared to Waterfall's 5.89 years, while maintaining a lower standard deviation. These findings suggest that Agile's iterative cycles, continuous integration, and incremental validation contribute to a more predictable and efficient development process. Our results align with the results Ciric found in their paper regarding Agile Project Management (APM; Ciric et al., 2019).

Agile's Impact on Development Efficiency

With its iterative approach, Agile development significantly shortens development timelines by fostering early and frequent testing, thereby minimizing late-stage rework—a clear advantage over the Waterfall model's delayed validation. We implemented a CAP to bolster agility in safety critical and regulated domains, seamlessly integrating people, process, and technology. This framework prioritizes the inclusion of regulatory compliance and safety expertise within development teams, early engagement of auditors for automated test development, and continuous collaboration with subject matter experts during reviews. Process enhancements include embedding compliance and safety user stories into the risk-adjusted product backlog, which is constantly managed to address emerging risks proactively, conducting hazard analysis via STPA, and employing continuous validation checklists (Vieira et al., 2020; Zahedi et al., 2023). Technology is leveraged through advanced verification and validation using MBSE, digital twin simulations, robust automated testing, and integrated toolsets. We emphasize quantifiable metrics, such as reduced compliance defects and improved safety rates, and cultivate a culture of shared responsibility and continuous improvement. By integrating a risk adjusted product backlog, we ensure that risk management is a dynamic and integral part of the development process, allowing teams to respond swiftly to potential issues and maintain project agility while upholding stringent safety and compliance standards.

Challenges in Applying Agile to Safety-Critical Systems

Despite its advantages, Agile's implementation in a safety critical domain such as regulatory compliance, safety assurance, integration complexity, traceability and documentation, and organizational communication barriers.

Regulatory Compliance

Space systems must comply with stringent industry standards, including MIL-STD-461, NASASTD-8719.14, FAA Part 450, NIST 800-53, and ITAR regulations. Traditional Waterfall models inherently align with these compliance requirements through predefined verification stages. Conversely, Agile's iterative approach requires decoupling regulatory compliance checks from stage gates and moving to right-size documentation (Rodrigues et al., 2022), performing incremental compliance checks with checklists (Zaydi et al., 2024). In addition, we can model compliance using MBSE, simulating the impact using a digital twin (Bouhali et al., 2024). For instance, digital twin simulations can assess compliance impact by virtually testing system responses to various regulatory scenarios. Compliance with these regulations is crucial for ensuring the space systems.

Safety Assurance

Failures in safety-critical systems necessitate rigorous methodologies that ensure consistent safety evaluations across design and operational stages. The integration of a CAP that employs Behavior Driven Development (BDD) and Acceptance Test Driven Development (ATDD) can complement the Systems-Theoretic Process Analysis (STPA) framework to enhance safety verification. STPA is particularly effective in identifying potential failure modes, as it views safety violations as a result of unsafe interactions among components rather than merely from component failures (Kim et al., 2021). In addition to STPA, implementing MBSE systematically organizes safety system designs within agile frameworks. MBSE enhances the iterative development approach by documenting safety requirements, facilitating clear communication among stakeholders, and integrating safety checks into the user story definition of done (Ahlbrecht et al., 2022). We utilize the risk-adjusted product backlog to prioritize safety concerns continuously. In conclusion, the CAP that integrates BDD, ATDD, and STPA, enhanced by MBSE, and managed in a risk-adjusted backlog presents a robust approach for managing safety in complex systems.

Integration Complexity

Our CAP supports the challenge of integration complexity by supporting Agile with MBSE and digital twins. This synergistic approach fosters early integration and validation, which are pivotal in managing the inherent complexities associated with these systems. MBSE provides a structured and formalized method for capturing CPS's requirements, architecture, and design, thus establishing a well-documented framework that supports iterative development. The integration of MBSE and digital twins to support Agile was demonstrated by Vodyaho with the Smart City case study, which managed transport and flows in St. Petersburg (Russia; Vodyaho et al., 2022). Digital twins complement MBSE by creating real-time virtual representations of physical systems, allowing continuous integration and validation throughout development. They enable hardware-software co-simulation, predictive analytics, and real-world scenario testing without waiting for full system deployment. Integrating Agile, MBSE, and digital twins reduces delivery times and lowers risk exposure (Honcak & Wooley, 2024).

Traceability and Documentation

MBSE within our CAP enhances traceability and documentation processes. A common perception is that Agile teams often neglect documentation, presenting a barrier to effective traceability. However, integrating Agile methodologies with MBSE can address these challenges while ensuring the documentation is appropriately scaled and valuable. MBSE leverages models to facilitate various systems engineering activities, including requirements capture, system functionalities identification, and verification tasks, significantly improving traceability (updating requirements as changes occur) compared to traditional document based methods (Boggero et al., 2021; Huss et al., 2023). For Agile teams, embracing these methods allows for a more adaptable documentation process that aligns with rapid development cycles while maintaining compliance with traceability requirements.

Organizational Culture Barriers

The fictional case study did not demonstrate unique considerations regarding overcoming organizational and cultural barriers. This contrast between industry mindsets creates inherent challenges when introducing agile methodologies. Safety-critical industries prioritize risk minimization and predictability, often adopting a “fail-safe” rather than “fail-fast” mentality. In contrast, Agile methodologies emphasize cross-functional, self-organizing teams. However, traditional structures in safety-critical sectors typically separate engineering, safety, regulatory compliance, and testing into separate silos. Furthermore, the heterogeneous teams familiar with cyber-physical systems tend to increase resistance to change. Heterogeneity, defined in this context as the diversity of team backgrounds and perspectives, significantly impacts communication, collaboration, and overall teamwork dynamics, as noted by Grotto and Andreassi (2022). These implications highlight the challenges of integrating agile practices into environments where rigid, siloed structures have historically prevailed. Socio-technical systems (STS) theory may effectively resolve the difficulties of incorporating agile methodologies into safety-critical industries. STS theory emphasizes the interplay between social and technical factors in organizational systems, recognizing that both aspects must be considered for optimal performance. Therefore, by utilizing STS theory, safety-critical industries can better integrate agile methodologies.”

Conclusion

This study demonstrates that Agile can significantly reduce satellite development time while maintaining predictable scheduling and adherence to regulatory requirements. However, its application in safety-critical space systems requires specific adaptations, including incremental safety audits, continuous compliance tracking, and advanced risk modeling. While Agile’s benefits are evident, its limitations in full-system integration and long-term mission assurance highlight the potential value of a hybrid development model. Future research should investigate Agile’s impact on mission reliability, cost, and scalability in real-world space system deployments.

References

Ahlbrecht, A., Zaeske, W., & Durak, U. (2022). Model-based STPA: Towards agile safety-guided design with formalization. In Proceedings of the 2022 IEEE International Symposium on Systems Engineering (ISSE), 1–8.

Alleman, G. B., Coonce, T. J. & Price, R. A. (2014). Building a credible performance measurement baseline. The Measurable News, 1(4), 15–18.

American National Standards Institute. (2021). ANSI safety standards. https://www.ansi.org

Araujo, B. (2019). How relativity space is able to 3D print a rocket in 60 days? Agile is the answer. LinkedIn. https://www.linkedin.com/pulse/ how-relativity-space-able-3d-print-rocket-60days-agile-araujo/

Bart, R. d. F. (2024). Is hardware agile worth it? Analyzing the SpaceX development process. In AIAA SCITECH 2024 Forum.

Boggero, L., Ciampa, P. D., & Nagel, B. (2021). An MBSE architectural framework for the agile definition of system stakeholders, needs and requirements. In Proceedings of the AIAA Aviation 2021 Forum, 3076. doi:10.2514/6.2021-3076

Bouhali, I., Idasiak, V., Martinez, J., Mhenni, F., Choley, J.-Y., Palladino, L., & Kratz, F. (2024). A collaboration framework using digital twin for dynamic simulation and requirements verification based on MBSE and the MIC concept. In Proceedings of the 2024 IEEE International Systems Conference (SysCon), 1–8. doi:10.1109/SysCon61195.2024.10553495

Brown, S. (2000). Overview of IEC 61508: Design of electrical/electronic/programmable electronic safety-related systems. Computing and Control Engineering, 11, 6–12.

Ciric, D., Lalic, B., Gracanin, D., Palcic, I., & Zivlak, N. (2018). Agile project management in new product development and innovation processes: Challenges and benefits beyond software domain. In 2018 IEEE International Symposium on Innovation and Entrepreneurship (TEMS-ISIE), 1–9. doi: 10.1109/TEMSISIE.2018.8478461

Ciric, D., Lalic, B., Gracanin, D., Tasic, N., Delic, M., & Medic, N. (2019). Agile vs. traditional approach in project management: Strategies, challenges and reasons to introduce agile. Procedia Manufacturing, 39, 1407–1414.

de Freitas Bart, R. (2024). Is hardware Agile worth it? Analyzing the SpaceX development process. In Proceedings of the AIAA SCITECH 2024 Forum, 2054. doi:10.2514/6.2024-2054

DoD. (2012). MIL-STD-882E: Standard practice for system safety.

DoD. (2015). MIL-STD-461G: Requirements for the control of electromagnetic interference characteristics of subsystems and equipment.

Donahue, K., Devaraj, K., Mason, J., & Ozturk, M. (2024). Planet's Agile software development for spacecraft. In Proceedings of the Small Satellite Conference.

Drutchas, J., & Eppinger, S. (2022). Guidance on application of agile in combined hardware and software development projects. In Proceedings of the Design Society, 2, 151–160.

European Chemicals Agency. (2022). Registration, evaluation, authorisation and restriction of chemicals (REACH). European Union. https://echa.europa.eu/regulations/reach

Federal Aviation Administration. (2021). 14 CFR part 450: Launch and reentry licensing requirements. https://www.ecfr.gov/current/title-14/chapter-III/part-450

Federal Communications Commission. (2021). FCC regulations on electromagnetic compatibility. https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization

GAO. (2024). Next generation overhead persistent infrared: Cost and schedule challenges (GAO-24-106831). https://www.gao.gov/products/gao-24-106831

Grotto, A. R., & Andreassi, J. K. (2022). Mix it up? The influence of team composition on employee perceptions of stressors in a post-merger environment. The Journal of Applied Behavioral Science, 58(3), 442–476. doi:10.1177/0021886320923370

GSA. (2021). Federal risk and authorization management program (FedRAMP). U.S. Government. https://www.fedramp.gov

Heeager, L. T., & Nielsen, P. A. (2018). A conceptual model of agile software development in a safety-critical context: A systematic literature review. Information and Software Technology, 103, 22–39. doi: 10.1016/j.infsof.2018.06.004

Hill, T. R., Nicoli, P., Pierce, G. J., Woodham, K., & Gati, F. (2024). Digital transformation of the NASA engineering domain. In Proceedings of the 2024 IEEE Aerospace Conference, 1–15. doi:10.1109/AERO58975.2024.10521274

Hirshorn, S. R., Voss, L., D., & Bromley, L. K. (2017). NASA systems engineering handbook, NASA.

Honcak, R., & Wooley, A. (2024). An MBSE approach for virtual verification & validation of systems with digital twins. In Proceedings of the ACM/IEEE 27th International Conference on Model Driven Engineering Languages and Systems, 390–400. doi:10.1145/3652620.3688252

Huss, M., Herber, D. R., & Borky, J. M. (2023). An Agile model-based software engineering approach illustrated through the development of a health technology system. Software, 2(2), 234–257. doi:10.3390/software2020011

International Organization for Standardization. (2018). ISO 26262: Road vehicles—functional safety. https://www.iso.org/standard/68383.html

Istari Digital. (2024, August 19). Istari Digital unveils X-Plane to become world's first digitally-certified aircraft. https://www.istaridigital.com/press-releases/

istari-digital-unveils-x-plane-to-become-worlds-first-digitally-certified-aircraft.

Kim, H., Lundteigen, M. A., Hafver, A. & Pedersen, F. B. (2021). Utilization of risk priority number to systems-theoretic process analysis: A practical solution to manage a large number of unsafe control actions and loss scenarios. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 235(1), 92–107.

Liubimov, O., Turkin, I., Pavlikov, V., & Volobuyeva, L. (2023). Agile software development lifecycle and containerization technology for CubeSat command and data handling module implementation. Computation, 11(9), 182. doi:10.3390/computation11090182

Mayani, M. G., Svendsen, M., & Oedegaard, S. I. (2018). Drilling digital twin success stories the last 10 years. In Proceedings of the SPE Norway Subsurface Conference, D011S007R001. MS

Mirabella, C., Tuccillo, M., & Della Vecchia, P. (2024). A model-based systems engineering digital certification framework for general aviation aircraft. Aerotecnica Missili & Spazio, 1–16. doi:10.1007/s42496-024-00241-5

NASA. (n.d.). 3.0 NASA program/project life cycle. NASA Reference Guide. https://www.nasa.gov/reference/3-0-nasa-program-project-life-cycle/

NASA. (2015). NASA cost estimating handbook version 4.0, appendix C: Cost estimating methodologies. https://www3.nasa.gov/sites/default/files/files/CEH AppC.pdf

NASA. (2020). NPR 8715.3: NASA general safety program requirements. https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=8715&s=3

National Institute of Standards and Technology. (2020). NIST special publication 800-53: Security and privacy controls for federal information systems and organizations. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Occupational Safety and Health Administration. (2022). OSHA standards and regulations. U.S. Department of Labor. https://www. osha.gov/laws-regs.

Parente, S. (2018). Agile quantitative risk analysis. PM World Journal 7.

Peterson, M. & Mocko, G. (2024). Case study in Agile for hardware: Aerospace systems. In Proceedings of the ASME 2024 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, 88407, V006T06A004. 146431.

Radio Technical Commission for Aeronautics. (2011). DO-178C: Software considerations in airborne systems and equipment certification. https://www.rtca.org/content/publications

Radio Technical Commission for Aeronautics. (2014). DO-326A: Airworthiness security process specification. https://www.rtca.org/content/publications

Ribeiro, J. E. F., Silva, J. G., & Aguiar, A. (2024). Weaving agility in safetycritical software development for aerospace: From concerns to opportunities. IEEE Access. doi:10.1109/ACCESS.2024.3387730

Ries, E. (2009). Minimum viable product: A guide. Startup Lessons Learned 3(1).

Rodrigues, J. M. S. C., Ribeiro, J. E. F.. & Aguiar, A. (2022). Improving documentation agility in safety-critical software systems development for aerospace. In Proceedings of the 2022 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 222–229. doi:10.1109/ISSREW55968.2022.00071

Stevenson, R., Burnell, D., & Fisher, G. (2024). The minimum viable product (MVP): Theory and practice. Journal of Management, 50(8), 3202–3231. doi:10.1177/01492063241227154

Trieflinger, S., Mu¨nch, J., Schneider, J., Bogazko¨y, E., Eißler, P., Roling, B., & Lang, D. (2021). Product roadmapping processes for an uncertain market environment: A grey literature review. In Lean and Agile Software Development: 5th International Conference, LASD 2021, Virtual Event, January 23, 2021, Proceedings, 5, 111–129. doi:10.1007/978-3-030-67084-9 7

U.S. Department of State. (2021). International traffic in arms regulations (ITAR). Bureau of Political-Military Affairs. https://www.pmddtc.state.gov

U.S. Environmental Protection Agency. (2022). Environmental regulations and compliance standards. https://www.epa.gov/regulations

Vaneman, W. K. (2016). Enhancing model-based systems engineering with the lifecycle modeling language. In Proceedings of the 2016 Annual IEEE Systems Conference (SysCon), 1–7. doi:10.1109/SYSCON.2016.7490581

Vieira, M., Hauck, J. C. R., & Matalonga, S. (2020). How explicit risk management is being integrated into agile methods: Results from a systematic literature mapping. In Proceedings of the XIX Brazilian Symposium on Software Quality, 1–10. doi:10.1145/3439961.3439976

Vodyaho, A., Zhukova, N., Subbotin, A., & Anaam, F. (2022). Towards dynamic model-based agile architecting of cyber-physical systems. Sensors, 22(8), 3078. doi:10.3390/s22083078

Wilcutt, T. W. (2021). Process for limiting orbital debris (NASA-STD-8719.14A). NASA.

Yeman, R. J., & Malaiya, Y. K. (2023). Comparison of agile scaling frameworks. In Proceedings of the 2023 6th International Conference on Information Science and Systems.

Yeman, R. J. & Malaiya, Y. K. (2024). A systematic literature review of the application of agile applied to large-scale, safety-critical, cyber-physical systems. In 2024 IEEE International Conference on Data and Software Engineering (ICoDSE). IEEE, pp. 13–18.

Zahedi, M. H., Kashanaki, A. R., & Farahani, E. (2023). Risk management framework in Agile software development methodology. International Journal of Electrical & Computer Engineering, 13(4). doi:10.11591/ijece.v13i4.pp4379-4387

Zaydi, M., Maleh, Y., Zaydi, H., Khourdifi, Y., Nassereddine, B., & Bakouri, Z. (2024). Agile security and compliance integration. In Agile Security in the Digital Era: Challenges and Cybersecurity Trends, p. 68. CRC Press

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net