**International Council on Systems Engineering**
*A better world through a systems approach*

# Integration of Agile and Systems Engineering to Deliver Safety-Critical Cyber-Physical Systems

Dr. Suzette Johnson and Dr. Robin Yeman

# Hello

*On a journey to improve the state of the practice in building large-scale safety-critical cyber-physical systems using Lean, Agile, Systems Thinking, and DevOps*


**Dr. Suzette Johnson**

Fellow, Lean Agile Digital

NORTHROP GRUMMAN



**Dr. Robin Yeman**

Senior Solution Director

leidos

# Agenda

- Large-Scale, Safety-Critical, Cyber-Physical Systems
- Challenges
- Industrial DevOps
- Case Study
- Framework (Continuous Assurance Plug-In)
- Closing / Questions

*The motivation to migrate to modern ways of working is the demand for*

***Faster delivery***

***Managing complexity and risk***

***Responding to uncertainty***

# Large-Scale, Safety-Critical, Cyber-Physical Systems


**Large-Scale**

Organizations with 50 or more people or at least six teams. (Dikert 2016)

**Safety-Critical**

Failures in these systems can lead to severe consequences, including loss of life and significant environmental damage. (Knight 2002)

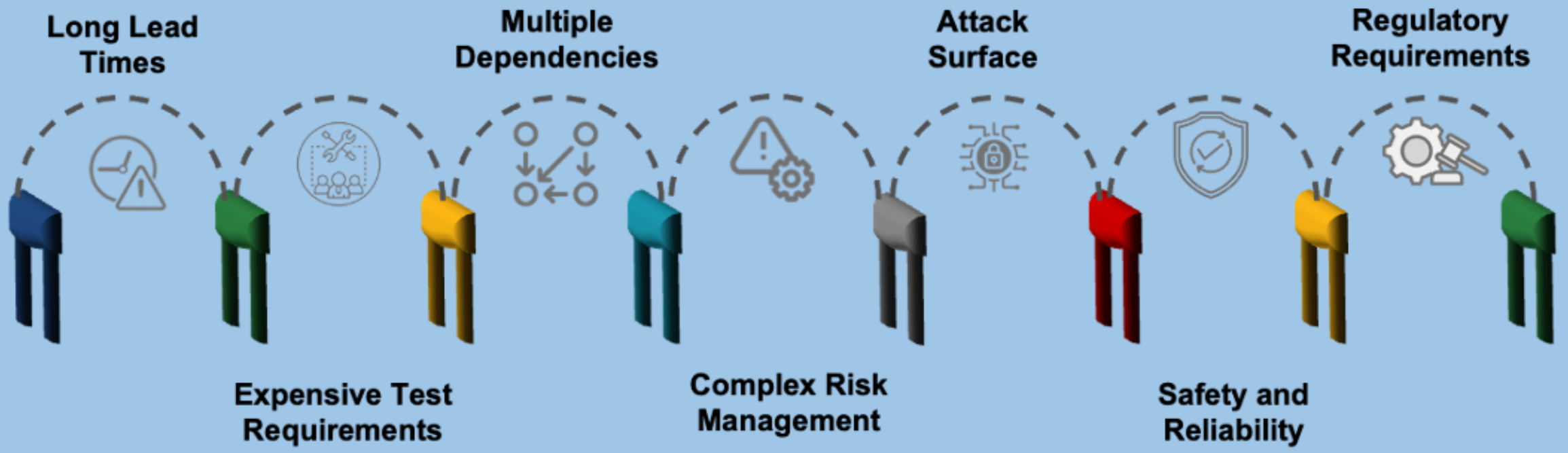
**Cyber-Physical**

Systems that are comprised of computational with physical elements (Lee 2017)

We define **Large-Scale, Safety-Critical, Cyber-Physical (LS/SC/CP) systems** as entities developed by a collective of over fifty people, where failure can result in significant harm, composed of both computational and physical elements.

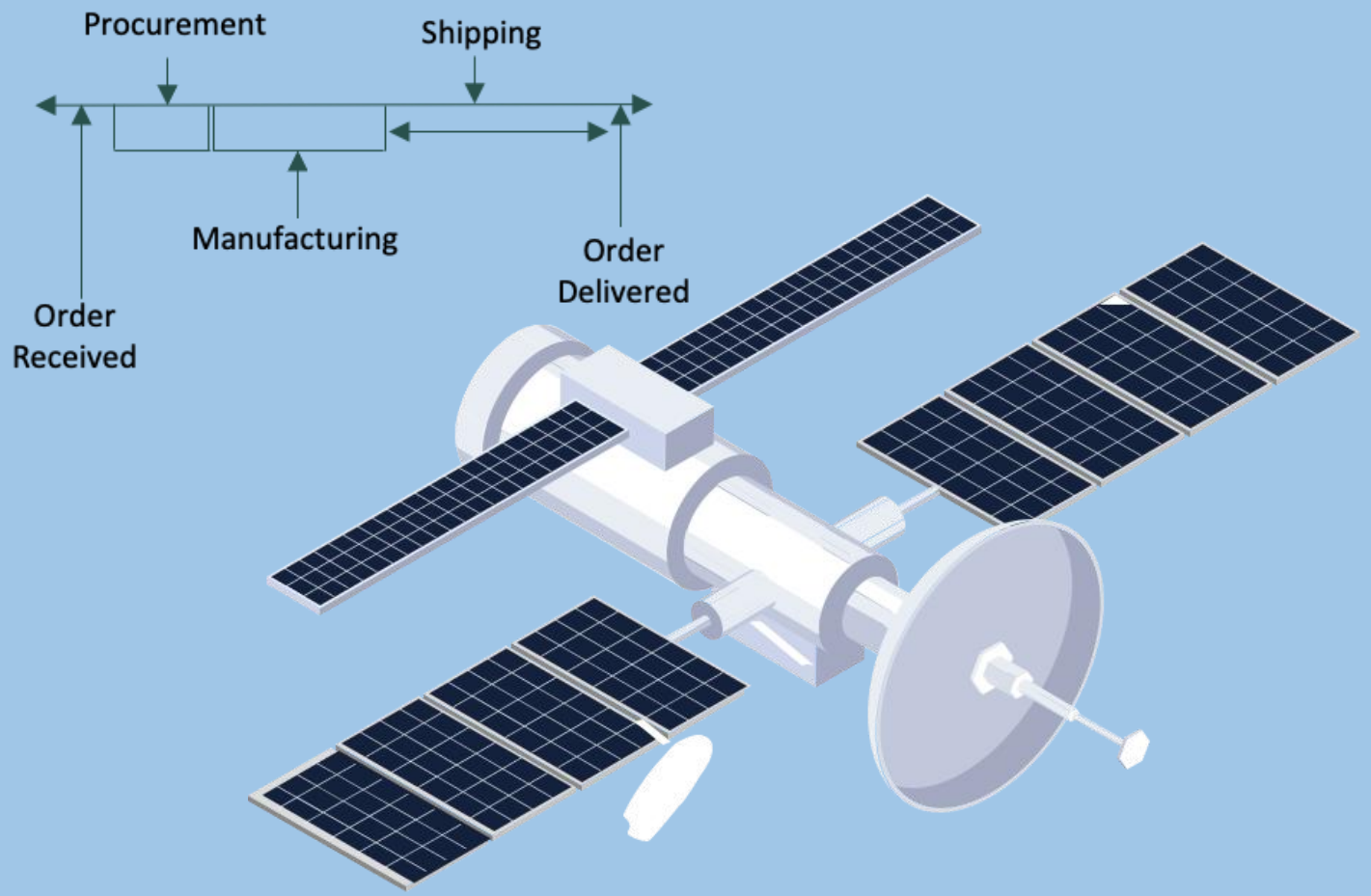
# Examples Cyber-Physical Systems

# Challenges


Long Lead Times
Expensive Test Requirements
Multiple Dependencies
Complex Risk Management
Attack Surface
Safety and Reliability
Regulatory Requirements

# Long lead time

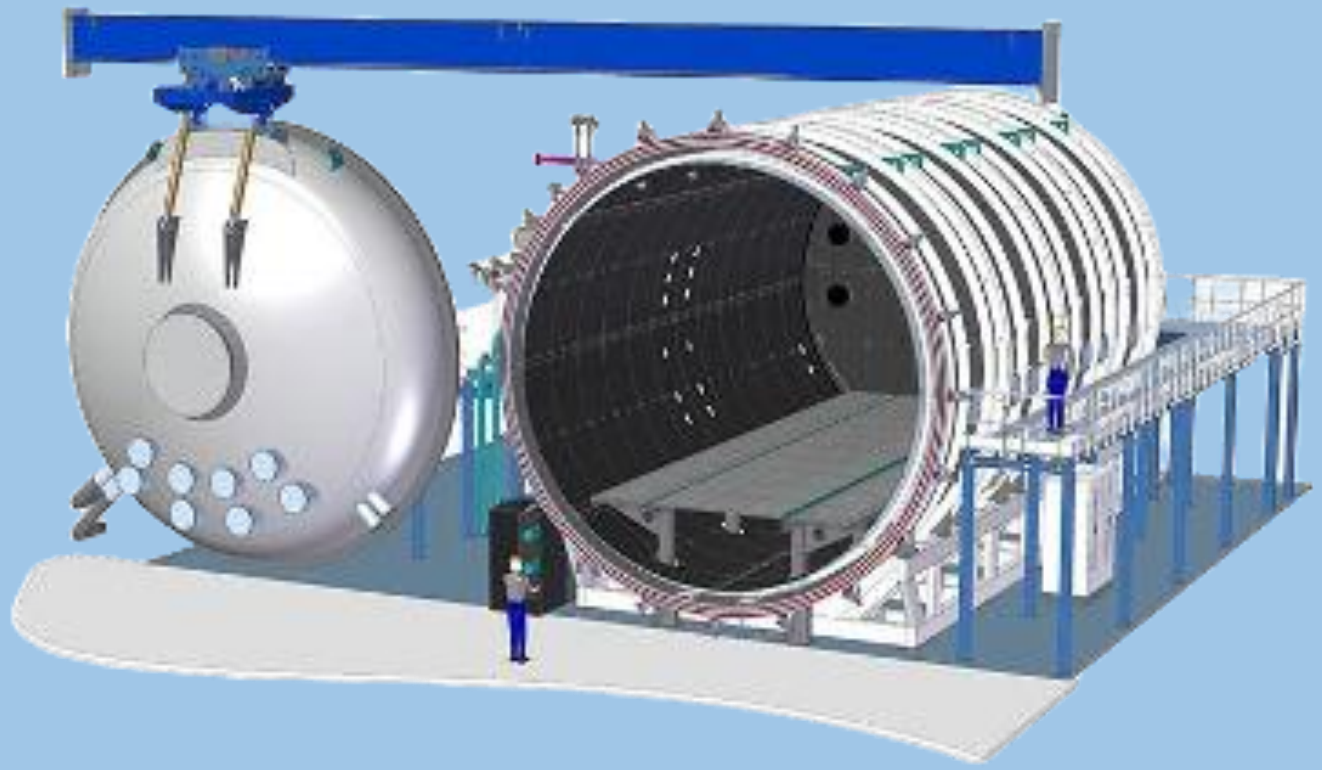
*Typically, cyber-physical systems have components and sub-assemblies from multiple suppliers which delay feedback*



# Expensive integration and test requirements

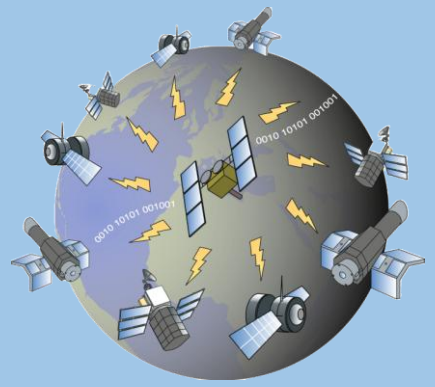
Very large Thermal Vacuum chambers cost millions of dollars and the tests can take months

*Cyber-Physical systems require unique and expensive test equipment*
*Also delaying feedback.*

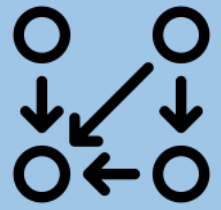


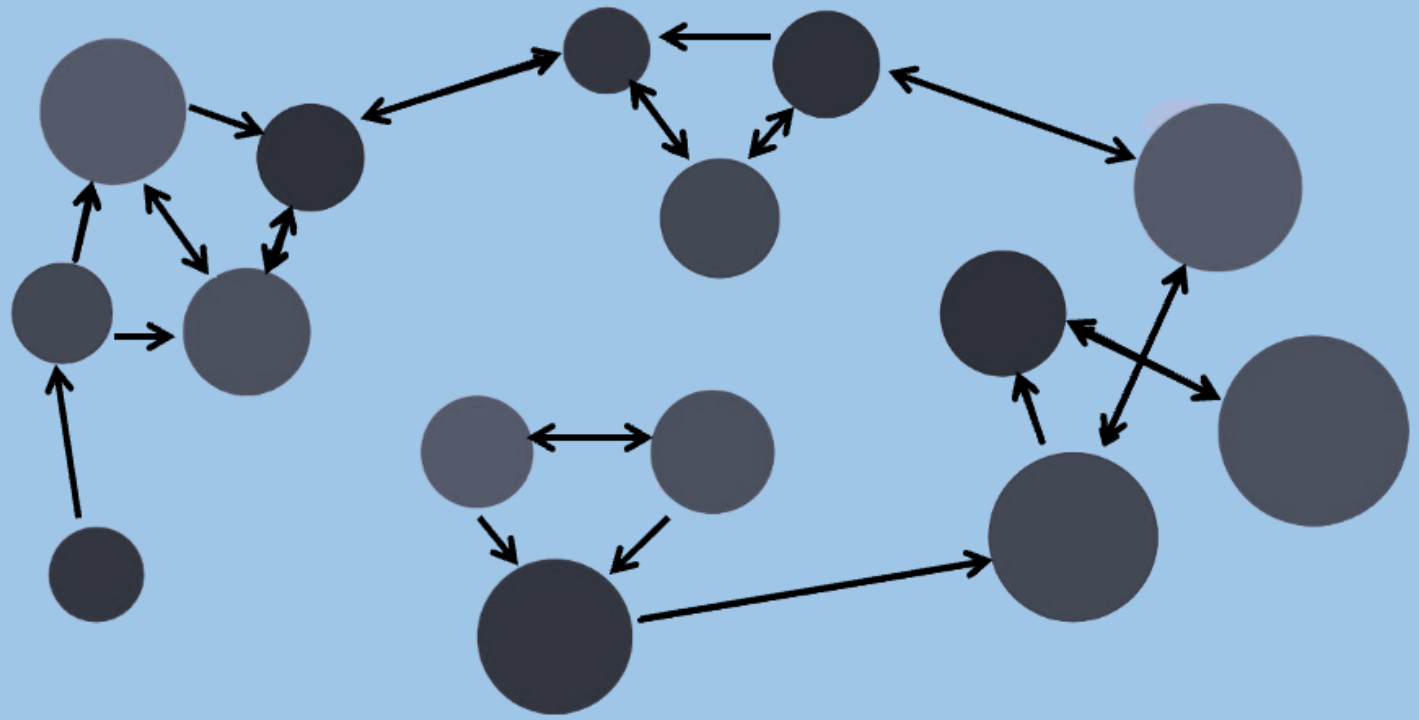
# Multiple dependencies

Cyber-Physical systems have many dependencies
and are often systems of systems magnifying those dependencies.



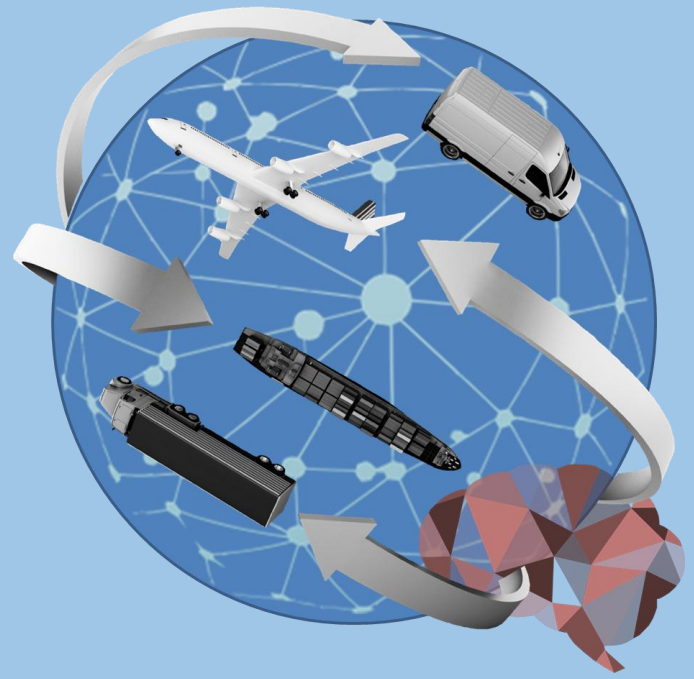
*Can you imagine all the Dependencies in GPS Satellite constellation?*





# Complex risk management

*Can you imagine all the Dependencies in GPS Satellite constellation?*



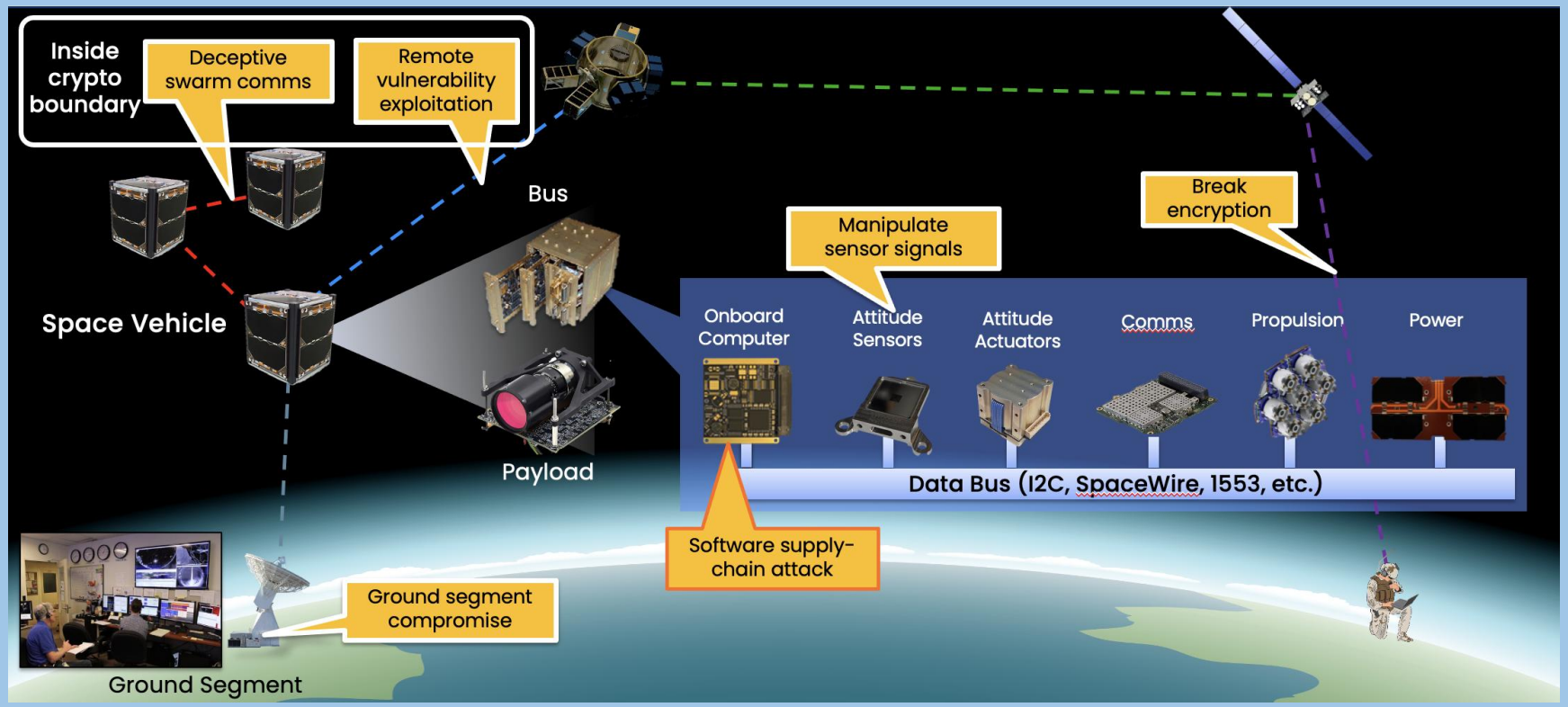
## Example GPS Risks

- Solar Interference
- Frequency Crowing
- Signal Degradation
- Jamming
- Spoofing
- System under attack (Cyber/physical)

# Extensive attack surface

According to Forbes There is a growing global consensus that governments and businesses need to prioritize security when securing the frontier of space systems.

Once we connected everything, they attack surface magnified.



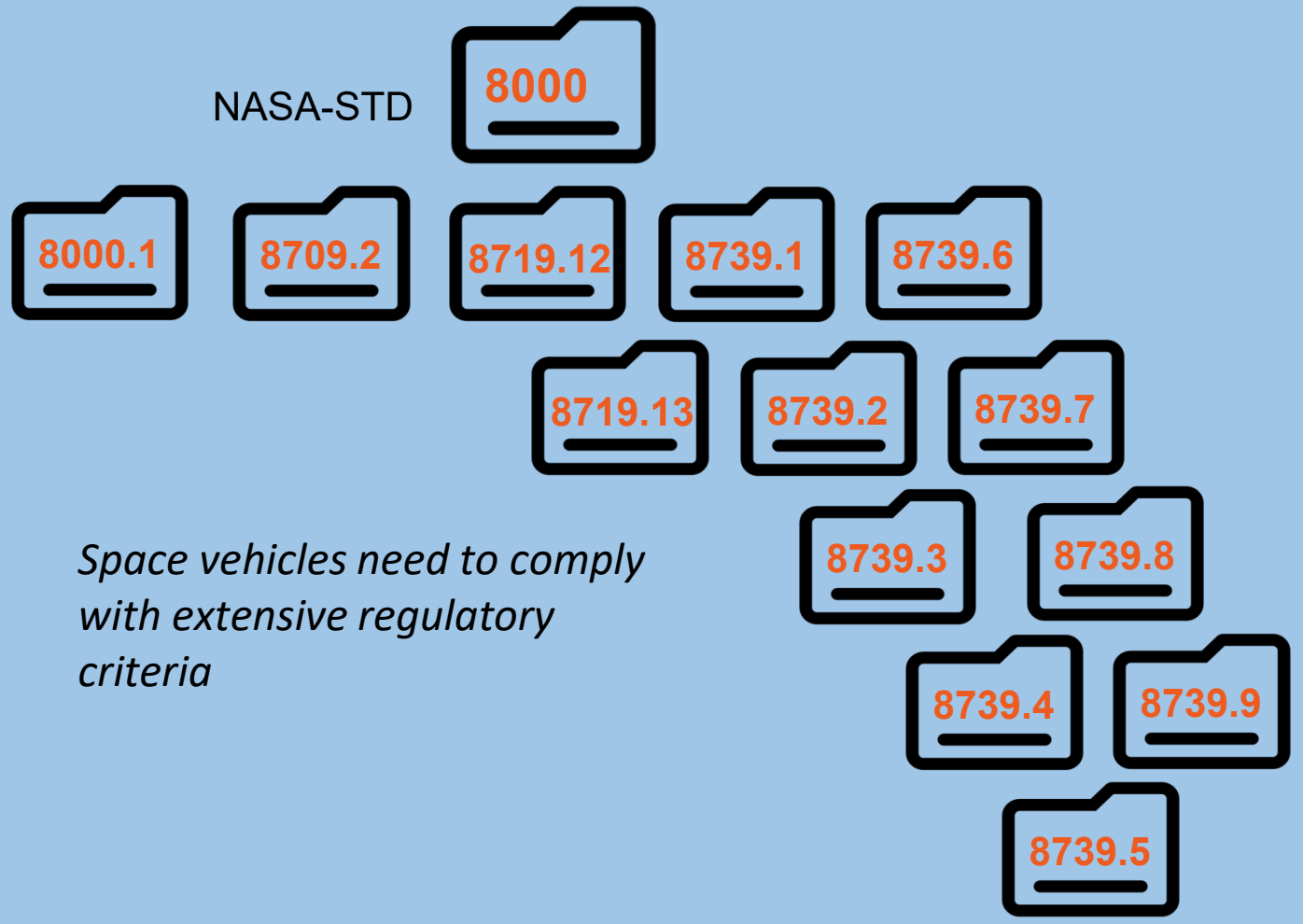


Brooks, C. (2024, April 15). Cyber-securing space systems a growing global concern. Forbes. https://www.forbes.com/sites/chuckbrooks/2024/04/09/cyber-securing-space-systems-a-growing-global-concern/

MIT Lincoln Laboratory. (n.d.). Space systems cyber-resiliency. MIT Lincoln Laboratory. https://www.ll.mit.edu/r-d/projects/space-systems-cyber-resiliency

# High stakes safety and reliability

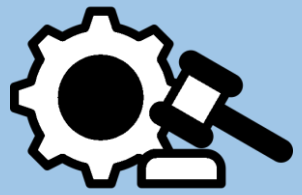
*Space vehicles need to comply with extensive regulatory criteria*

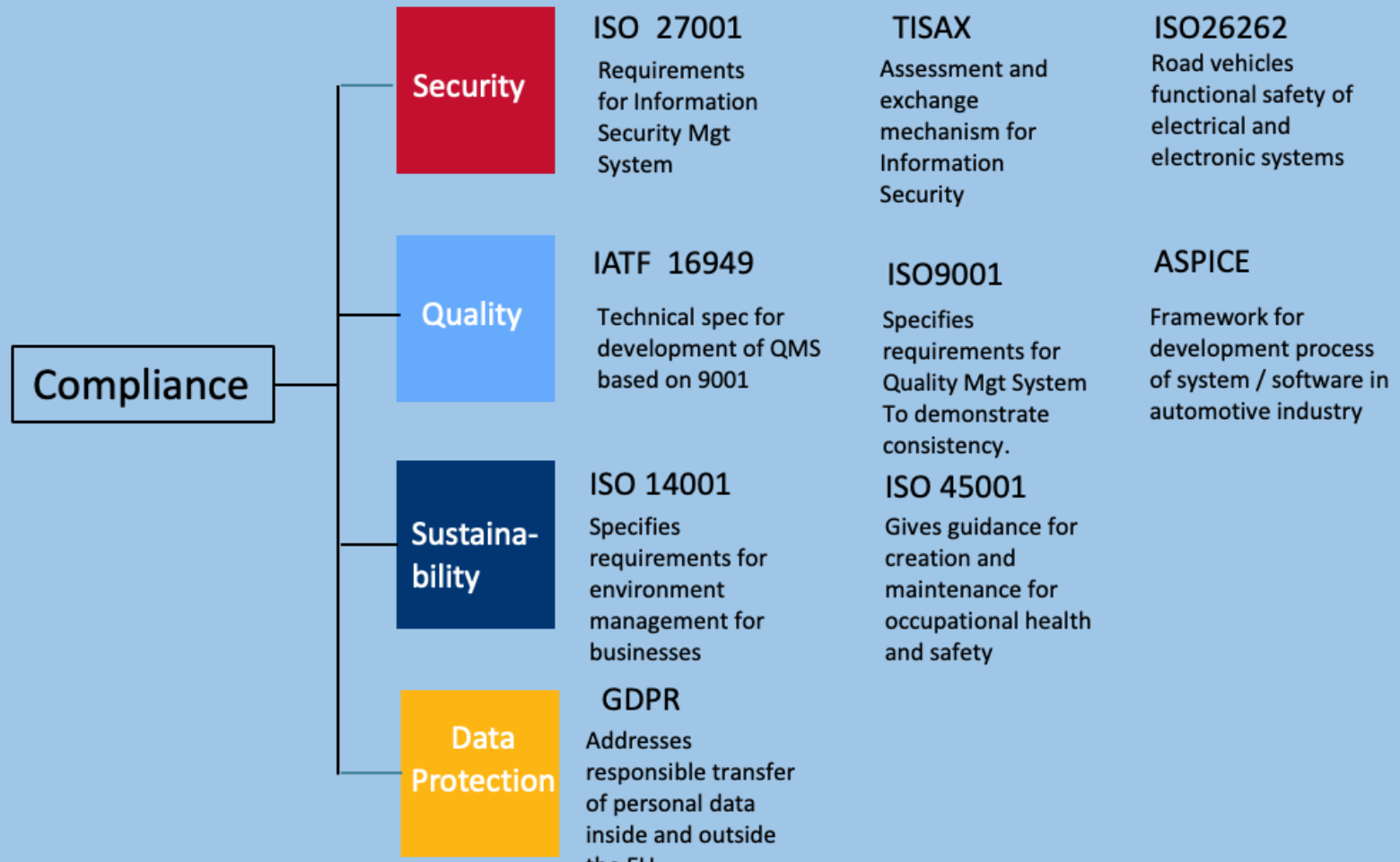



*Space vehicles need to comply with extensive regulatory criteria*

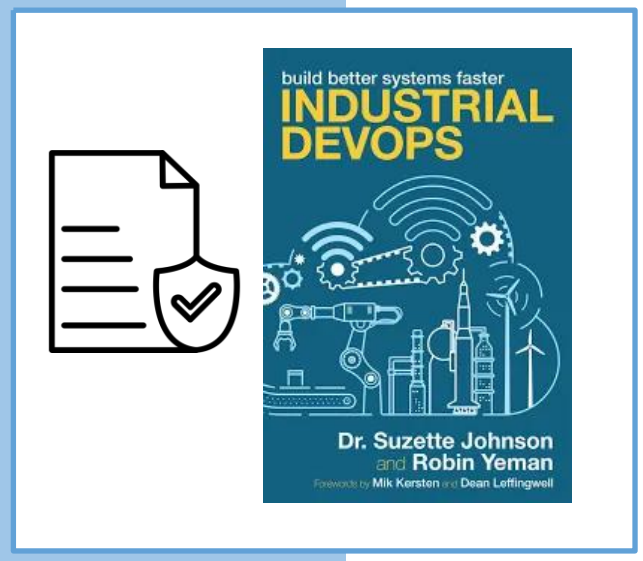
# Regulatory Compliance

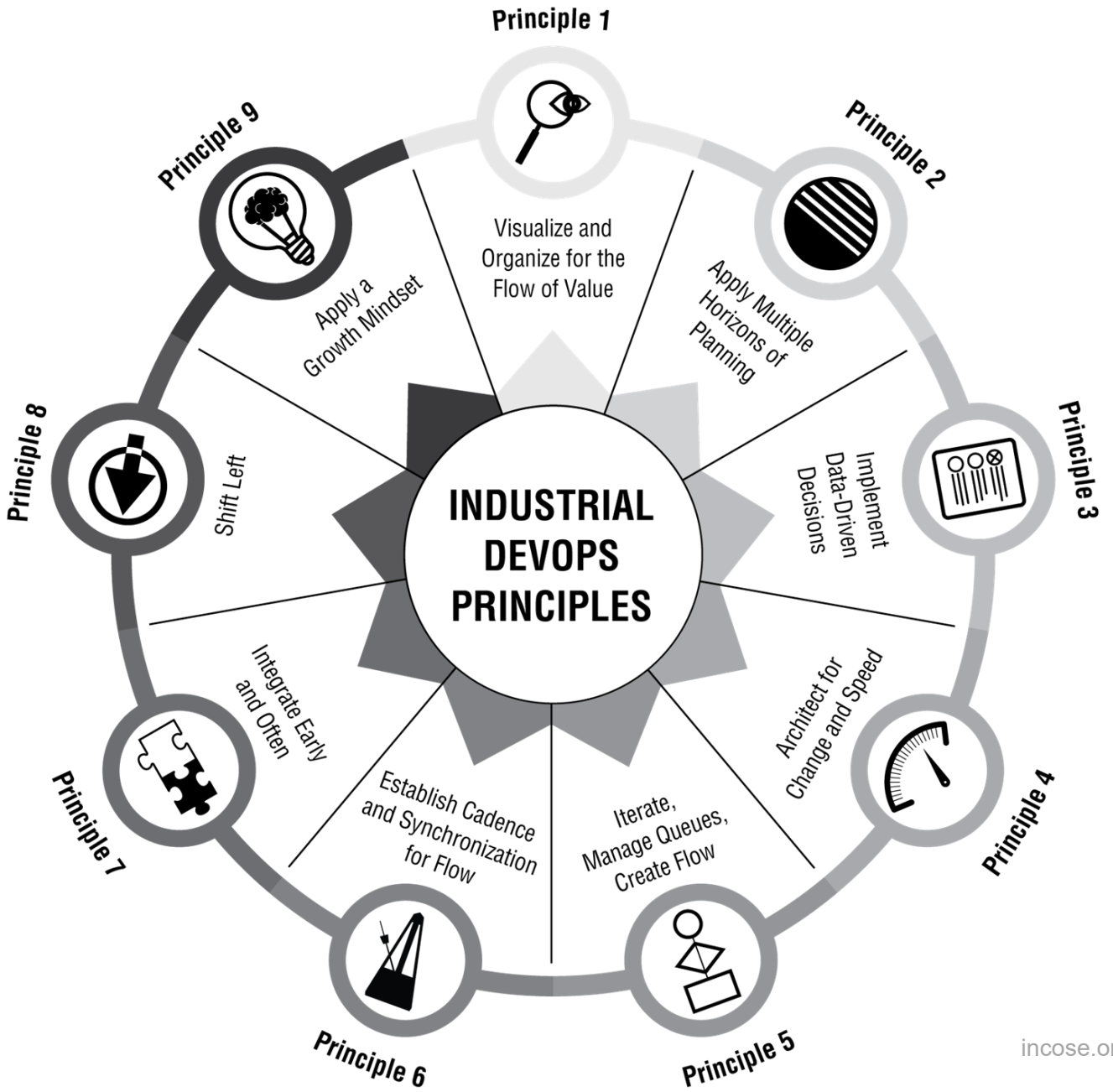
*Cyber-physical* ***systems*** *are subject to multiple regulatory standards.*





***Industrial DevOps*** *applies the principles of Lean, Agile, DevOps to planning development, manufacturing, deployment, and serviceability to significant cyber-physical systems.*



# Satellite Case Study (Waterfall vs Agile)

**Identified Existing Satellite and defined Specifications**

Used Nebula from Terran Orbital as a starting Point

**Created Mission Requirements Model (Why)**

Highest level Objectives (Earth Observation)

**Created Requirements Model (How)**

Decomposed satellite into subsystems using MOSA Principles

**Developed Assumptions**

Assumed procurement was complete

**Developed Waterfall Model**

NASA SE Manual

NASA SP-2016-6105 Rev2

and traced activities to requirements to model

**Developed Agile Model**

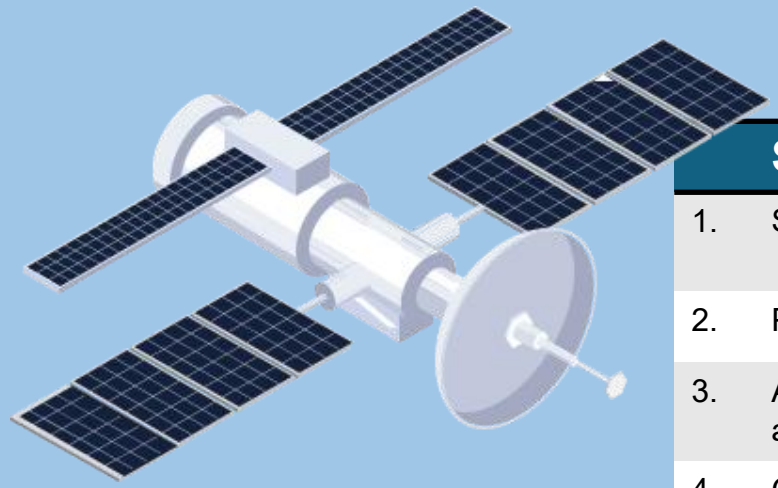
Developed a series of MVPs based on Modular Architecture and traced activities to requirements to model

**Monte Carlo Analysis**

Innoslate performs Monte-Carlo Simulation)

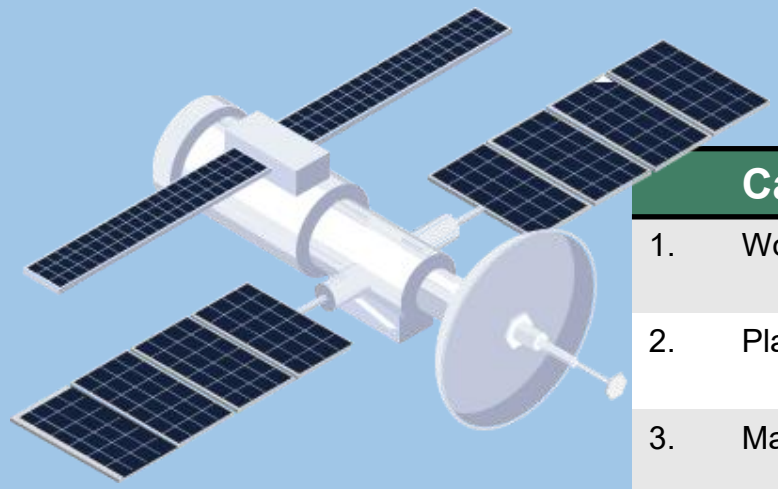
***Estimates were expert judgement and comparisons of similar activities***

# System Requirements



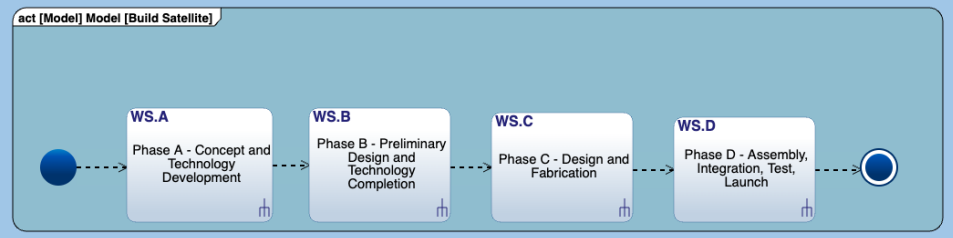
| | Subsystem | Inputs | Outputs |
|---|---|---|---|
| 1. | Structure | Primary & Secondary Structures | Verified structural integrity |
| 2. | Power | Battery, Solar Arrays | Power distribution verified |
| 3. | Attitude Determination and Control | Reaction Wheels, Star Trackers, Software | Attitude accuracy verified |
| 4. | Communication | 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 and Data Handling | Onboard Computer, Software, Sensors | Command & Data handling verified |

# System Assumptions

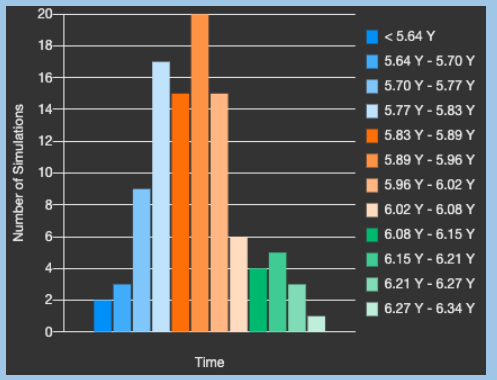


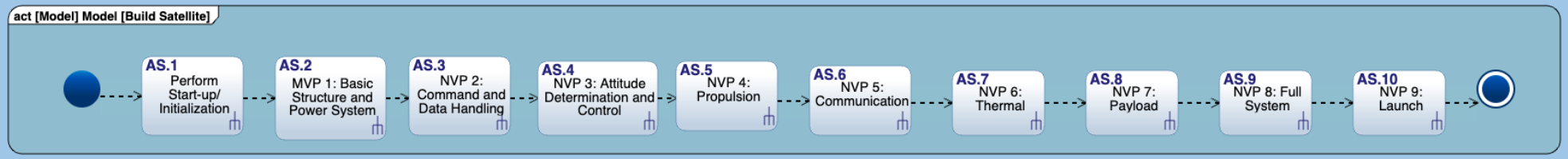
| | Category | Waterfall Assumption | Agile Assumption |
|---|---|---|---|
| 1. | Workflow | NASA Defined approach (NASA SP-2016-6105 Rev2) | Iterative and Incremental with Continuous Assurance Toolkit Plugin |
| 2. | Planning | Complete Integrated Master Schedule defined before work starts. | Roadmap and Planning approach defined |
| 3. | Materials / Components | All required resources are available from the start and cause no delays. | All required resources are available from the start and cause no delays. |
| 4. | Labor / Skill Availability | Functionally Organized Workforce | Cross-Functional Workforce with T-Shaped skills. |
| 5. | Integration and Test | Test equipment and Infrastructure available immediately. | Test equipment and Infrastructure available immediately. |
| 6. | Regulatory Compliance and Safety | Validated at the Phase Gates | Automated and continuously validated at each sprint and Increment (Quarter) |
| 7. | Material Cost | Fixed Material Cost | Fixed Material Cost |
| 8. | Labor Cost | $120 Per Hour | $120 Per Hour |

# Model Results

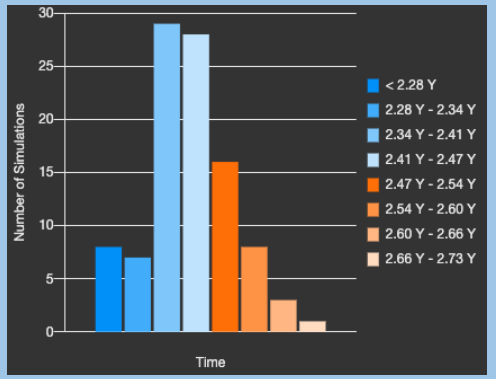



Mean: 5.92 Year / SD 2.7 M

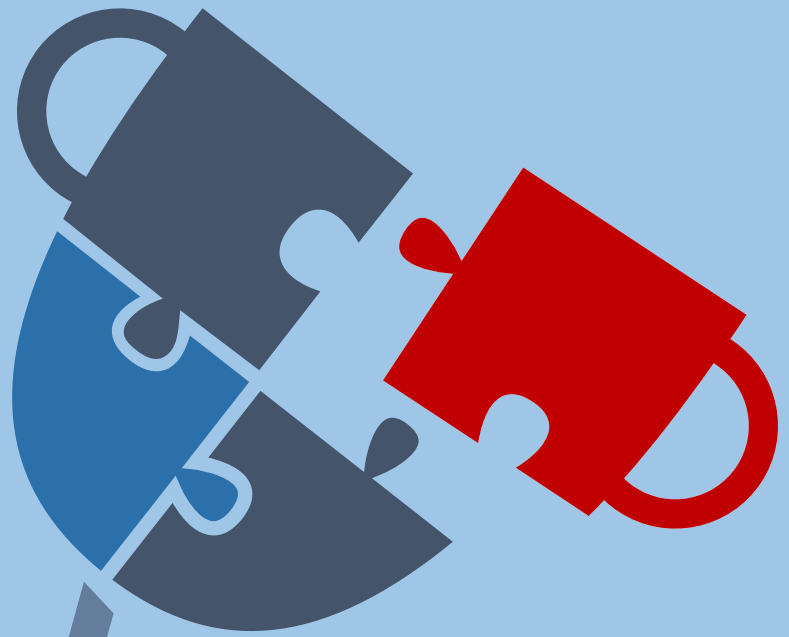



Mean: 2.43 Year / SD 1.09 M



# Proposed Framework (Continuous Assurance Plugin)




## People

Safety, Regulatory compliance expertise; Extreme Ownership

## Process

Risk Management, Hazard Analysis, Fault Injection, Intent Driven Development.

## Tools

Traceability Matrix, automate safety and compliance, expand scope of CI/CD and Stories

***A plugin is a software component that extends the functionality of an existing software system, we expand this metaphor to upgrade or delivery model.***

# Continuous Assurance Plugin Details

| | Feature | Description | Benefit |
|---|---|---|---|
| **People**   | **Dedicated Safety Engineers** | Safety engineers are embedded within Agile teams to collaborate on risk identification, mitigation strategies, and verification activities. | Real-time identification and management of hazards as the system evolves, preventing safety issues from being discovered too late in development. |
| | **Regulatory Compliance Experts** | Compliance experts ensure that evolving features and system changes align with standards (e.g., DO-178C, ISO 26262, NASA NPR 8715.3, ITAR) | Reduces the risk of non-compliance and costly delays by aligning features and decisions to standards continuously. |
| **Process**  | **BDD/STPA Integration** | BDD focuses on defining system behavior through user stories and scenarios. At the same time, STPA is a safety analysis technique that identifies potential hazards and ensures that safety constraints are met. | Write safety focused scenarios that prevent hazards, including edge cases. |
| | **ATDD** | Defining acceptance criteria and tests for regulatory and safety before development begins. | Ensures capabilities are not accepted unless they comply with functional and safety requirements. |
| | **Risk Adjust Backlog** | Prioritized backlog that incorporates risk analysis. | Provides transparency into risk exposure in dollars allowing a prioritization of value and safety. |
| | **Chaos Engineering** | CI/CD pipeline regularly injects failures into the system before they manifest in production. | Enhances the resilience and reliability of systems by intentionally introducing failures and learning from the system's response. |
| | **Iterative Reviews** | A systematic approach to ensuring that safety and regulatory requirements are continuously met throughout the lifecycle. | Teams can identify and address potential issues early, reducing the risk of the overall safety and reliability of the system. |

# Continuous Assurance Plugin Details

| | Feature | Description | Benefit |
|---|---|---|---|
| **Tools**  | **Living Traceability Matrix** | Ensures that every requirement is traced to its corresponding design, implementation, and testing artifacts. | Provides transparency that improves change management, supports regulatory compliance, ensures quality assurance and simplifies audits and reviews. |
| | **Digital Compliance Checklist** | Checklist integrates compliance / safety activities found in the SETRs into the Agile workflow. | Provides real-time monitoring, validation, and documentation |
| | **Automate Safety / Compliance** | Place automated tests to continuously verify compliance and safety. | Compliance activities are consistently and integrated into the development process, reducing the risk of human error and improving overall system quality. |
| | **Expanded CI/CD Pipeline** | Incorporate HIL and SIL to validate cybersecurity (DO-326A, NIST 800-53) and hardware reliability (ISO 26262) | Integrating SIL and HIL into the CI/CD pipeline, teams can<br>ensure comprehensive testing and validation of the entire system. |
| | **Expanded Stories** | Track safety and regulatory tasks in product backlogs (e.g., "As a system, I must comply with<br>MIL-STD-882E for fault tolerance") | Ensuring that we are building regulatory compliance, safety, and security into the system. |
| | **Expanded Definition of Done** | Define "Done" criteria to include safety verification and compliance checks for each timebox. | Teams ensure that these critical aspects are addressed consistently and thoroughly throughout the development process. |

# Practical Application

## Planet Labs

American private company with a mission to image all the Earth daily to identify temporal global changes. The imaging data allows them the ability to analyze agricultural, energy, forestry, maritime, and sustainability events and impacts.

Optimizing spacecraft design using success patterns of **modularity, standardized interfaces, and open architecture along with Agile and DevOps practices.**

Results: Faster time to delivery; ability to continuously optimize designs.

## Joby Aviation

American aerospace company developing an electric vertical takeoff and landing aircraft for urban air mobility with plans to launch an air-taxi service.

Joby uses a **modular architecture with standardized interfaces and a delivery pipeline that enables them to rapidly iterate on changes** to the vehicle.

They use agile practices and test-driven development of the entire vehicle to ensure quality is built in.

## Automotive - Tesla

Architect for Change and Speed.
The automotive industry leverages modular design in electronic vehicle development to increase the speed of innovation and adoption of new technology.
Tesla is an extreme example where they go to the extent of having modular reconfigurable manufacturing allowing A/B testing on new ideas all the time.
Key benefits are the speed of innovation delivered to the market.




INCOSE International Symposium 2025 | Ottawa, Canada

# Getting Started

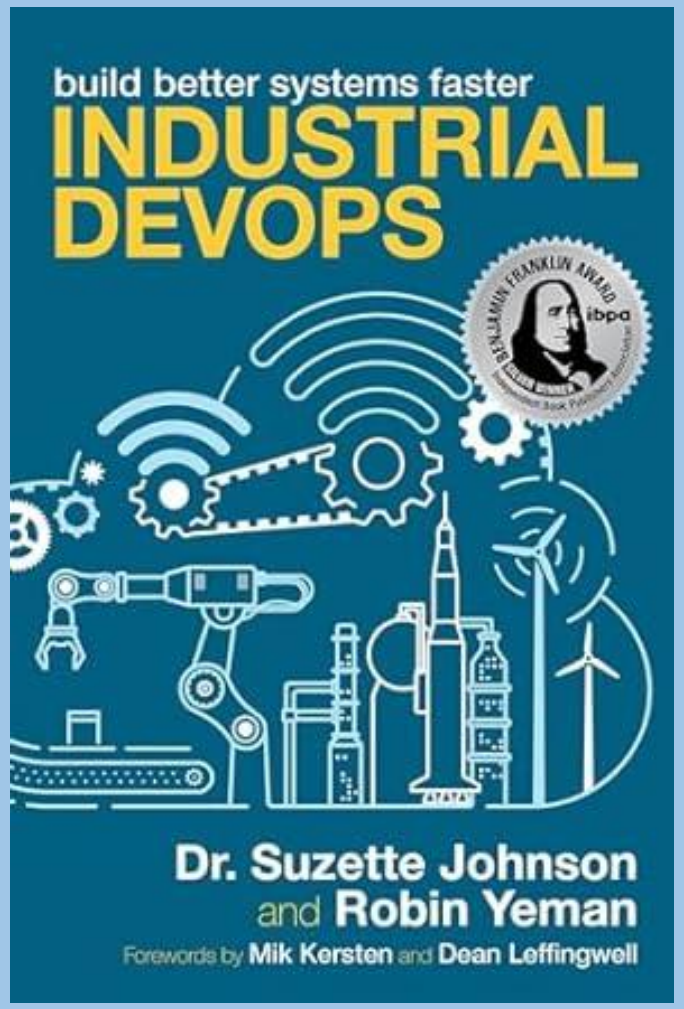
*Recommendations for getting started as you continue to shape your technology roadmap.*

- Define Mission Needs
- Assess Current State: Infrastructure, Simulation/Modeling Tools, Visualization Tools, Data Sources/Tools, Platforms, Domain Specific (Space) Situational Awareness tools, Human Capital
- Determine Planning Horizons
- Define Road Map and MVP/NVP
- Build: Infrastructure, Data Sources, Models, Simulation environments
- Integrate with Operations
- Inspect and Adapt
- Scale and Adjust your operating model for greater ROI
- Embrace a continuous learning and improvement mindset





*Reference: Johnson and Yeman. The Application of Industrial DevOps using Digital Twins. 2024. IT Revolution.*





INCOSE International Symposium 2025 | Ottawa, Canada

# Questions


INCOSE