Collins Aerospace
An RTX Business

Securing With Constraints: Working With Embedded Systems

Chitra Amzarewale

17/05/2025

Collins Aerospace
An RTX Business

Securing With Constraints: Working With Embedded Systems

Chitra Amzarewale

17/05/2025

Agenda

- Introduction
- Aerospace as a Domain
- Expanding Attack Surfaces in Avionics
- Threats & Risks of Concern
- Security Architectures & Mitigation Strategies
- Zero Trust & Resilient Architectures
- Securing by Processes

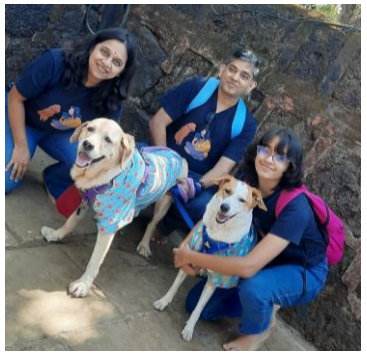
Introduction

Born and Brought up in Gujarat

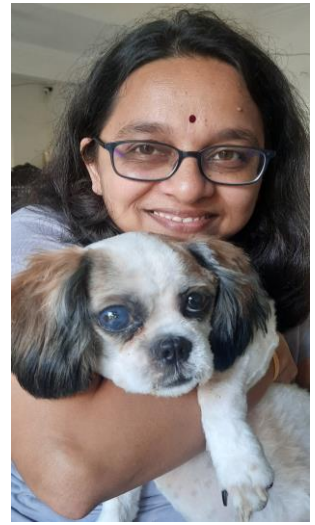
B.Sc (Mathematics)
B.E. (Electronics)
M.E(Control& Robotics)

Giving Back To Society

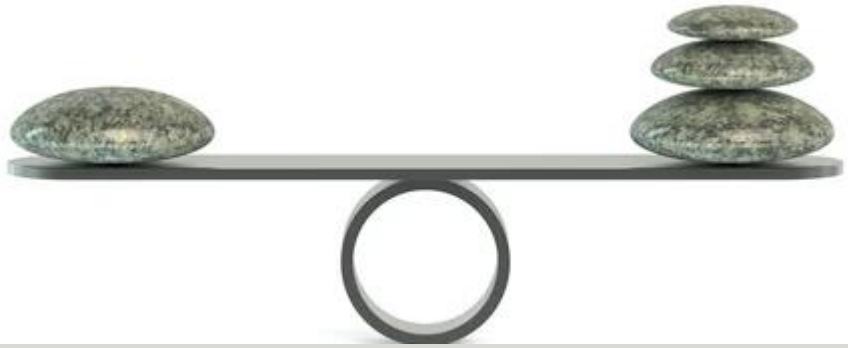
Fascinating world of Aerospace



Our Small World

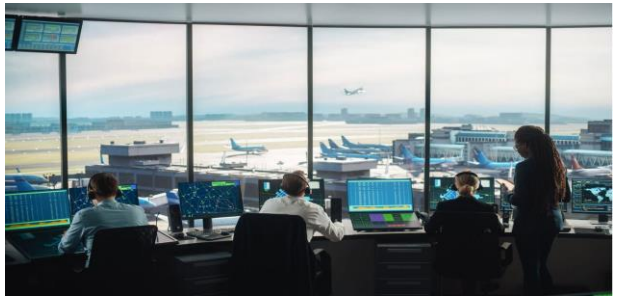


Rescue & Rehab
Founder @TheWagSocial



Work Life Balance is a Myth

Get to Know Collins Aerospace



Air Traffic Management

Military & Defense

Commercial Aviation

Airports

Helicopters

Business Aviation

Space

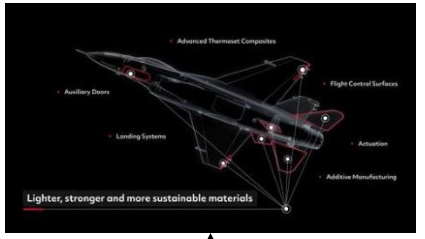
Collins Aerospace
An RTX Business

Collins Aerospace Initiatives

Autonomous Operations

Electrified Aircraft

Integrated Solutions



Advanced Structures

Connected Ecosystem

Cabin Experience

Connected Battlespace

Redefining Aerospace

Aerospace Domain: Background Concept & Design

Conceptualizing the product

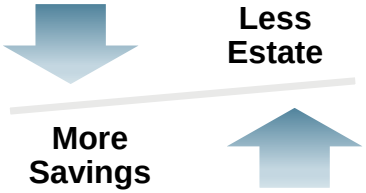
Life Span of the Product

Development Cycle

Obsolescence Management

?

Serviceability of the Product



Cost and Real Estate

Emerging Technological Trends

Design that Sustains Generations

Increased Attack Surfaces

- Rapid growth of IoT
- Extensive usage of Cloud
- Reliance on Digital Systems
- Digital transformation
- Sophistication of Threat Actors
- Increase in WFH or more connectivity facilities
- Aging technology and outdated hardware/software/firmware
- Insider Threats

One's loss
Other's gain:

Is Avionics Remains Secure?

Growing Threats & Risks: Embedded Systems

- Targeted Ransom Attacks
- Phishing Attacks
- Fileless Attacks
- Malware
- DDOs Attack
- Insider Threats
- Crypto Jacking
- Supply Chain Attacks

- Intellectual Property Compromise
- Code Integrity
- Data Confidentiality & Integrity
- Communication Channel Authentication & Authorization

Steady Growth in Attacks on Engineering

Generic Security Measures

- Robust Security Controls

  Patch Management, Multi-Factor Authentication (MFA), Firewalls and Intrusion Detection Systems (IDS), Encryption, Antivirus and Anti-Malware Software, Network Segmentation, Zero – Trust Architecture
- Regular Risk Assessments and Audits
- Awareness and Training

  Every person in organization must speak security
- Incident Response

  Plan, Monitor and Respond
- Compliance to Standards and Guidelines
- Technology Based Measures

  Monitor network traffic using edge technologies, Physical Measures and access control, BioMetrics, Encryption
- Collaborate

  Join other organization to defend the cyber threats, the rate at which cyber is growing, collaboration is the key

We Are Stronger Together

What do you all think?

- Do you think aviation is not secure anymore?

  Yes/No
- Are the listed measures enough?

  Yes/No
- Can all commercial electronics products be secured with these measures?

  Yes/No
- Can all avionics products be secured with all these measures?

  Yes/No
- Do you think any different measure/approach is needed?

  Yes/No

One Solution For All?

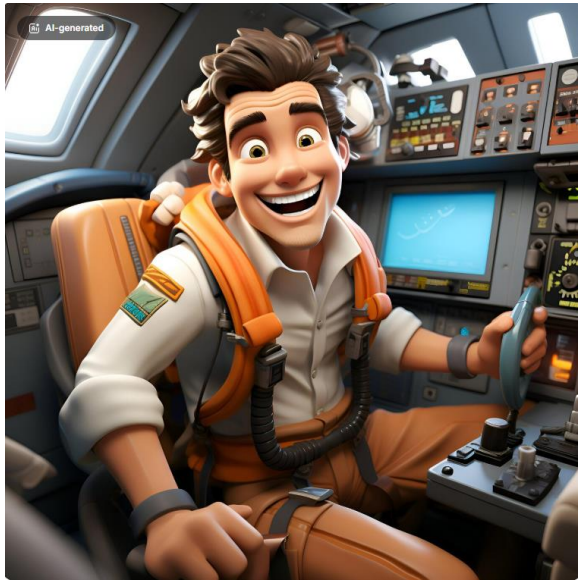
Approach: Securing Embedded Systems

- Legacy, Modified, New
- Airborne, On – Ground
- Embedded, Web Application, Mobile Application
- Connected, Not – Connected, Partially – Connected
- SDLC Phases: Development, Production, Maintenance, Operation, Disposal

Embedded System Is Not A Commercial Electronics

Security Measures: Web or Mobile

- Access Controls
- Bio Metrics
- MFA Authentication
- Real Time OTP/notifications
- End to End Encryption
- On Device Authentication
- AI/ML implementation for analysis
- PCIDSS Compliance for in air payment

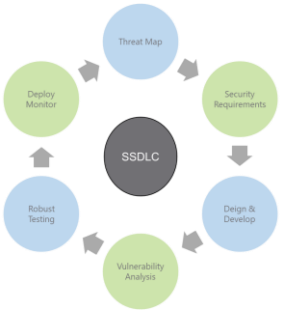


Security Measures: Product Evolution

Solution Fit for all? Products are diverse in terms hardware, software capabilities which prohibits us from arriving at a common solution however it could still enable us to propose a common solution for a subset of the products.

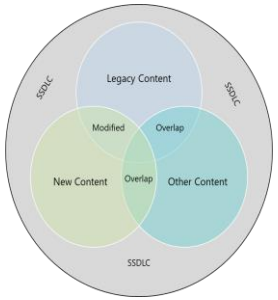
New Products

- Recommend Trusted Hardware Package based architecture
- Governed by Secure Software Development Process (SSDLC)
- Threat model guiding security requirements and robust testing
- Vulnerability Analysis at appropriate stage
- Secure Infrastructure etc.



Modified Products

- Governed by Secure Software Development Process (SSDLC) for the modified portion
- Most process for “Modified Portion” remains same as “New Products”
- Code reuse is enabled based on Threat Map & vulnerabilities
- Vulnerabilities are categorized based on risk & need mitigation



Legacy Products

- Perform product assessment for threat and vulnerability analysis
- Document risks based on inputs
- Product team to provide mitigation based on risk score or justification
- Prioritize fixes based on the modification plan

Security Measures: Bare Minimum

- ✓ Secure Development Lifecycle
- ✓ Risk Assessments
- ✓ Impact Analysis for the vulnerabilities
- ✓ Static Code Analysis or Dynamic in certain cases
- ✓ Digital Signature authentication
- ✓ Pen Testing and Vulnerability Identification
- ✓ Software Bill of Materials with patch update agreement
- ✓ Compliance and Cert

Protect any or all systems

Security Measures: Product Evolution

Enable Systems to Protect Itself

Securing Perimeter

- Inbuilt Crypto
- Secure Ground Support Equipment
- Secure Debug/Test Interface
- Secure Inputs
- Boot Securely

Tampering

- Secure Loading
- Encrypted Loads
- Encrypted Storage
- Secure Architecture
- Privileged Maintenance Access

Field Threats

- Encrypted Logs
- Secure Communications
- Secure Identify
- Reporting
- AI Solutions for faults/reports

Aim is Zero Trust

Zero Trust Architecture → Resilient Architecture

Verify Everything Every time

- Based on continuous validation and monitoring
- Strict controlled access privileges
- Assume compromise is reality
- Identify each user and access levels
- Compliance to Connected devices
- Clear distinction between assets

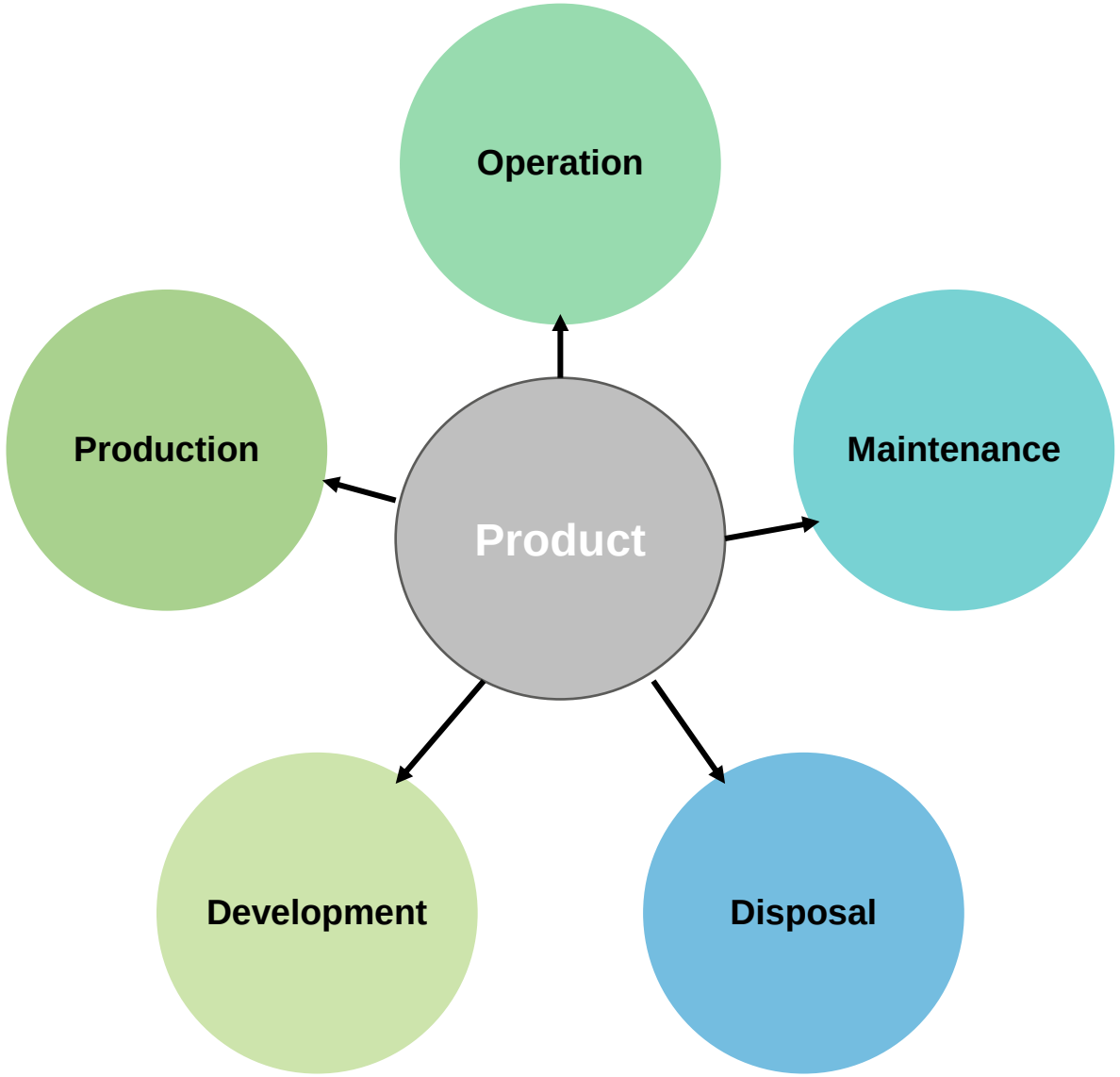
Ability to withstand Failures and Interruptions

- Failure is reality but the essence is recovery
- Monitoring and Adapting
- Uninterrupted Operation
- Proactive Anomaly Detection
- Dissimilar Redundant Backup
- Scalable

No fixed requirement for Zero Trust based Resilient Architecture, it depends what needs to be secured or resilient and from which threat?

Zero Trust & Resilient Architecture Is The Future

Security Measures: Secure By Process



- Maintenance at Airports and at Airlines owned facilities
- To tackle and protect IP there needs to be clear agreement between supplier and customer
- Access privileges help but the strategic agreements like field loading, repairs in own facilities are key
- Disposal of the retired unit is another challenge if not done appropriately
- The cases in which aircraft is not in service but not yet dismantled are tricky

Thank You

Q & A

Collins Aerospace
An RTX Business