Secure Aviation Design

For Defense Suppliers

C3E Symposium/October 2021

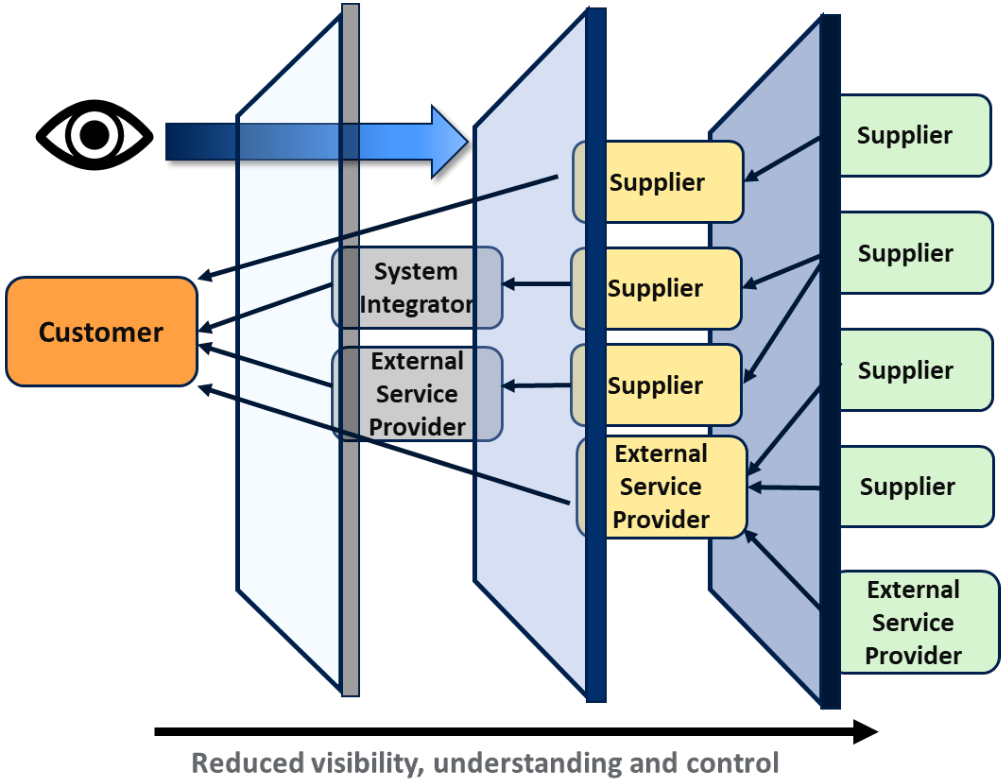
Tim Booher

Vice President, Combat Systems

LOCKHEED MARTIN

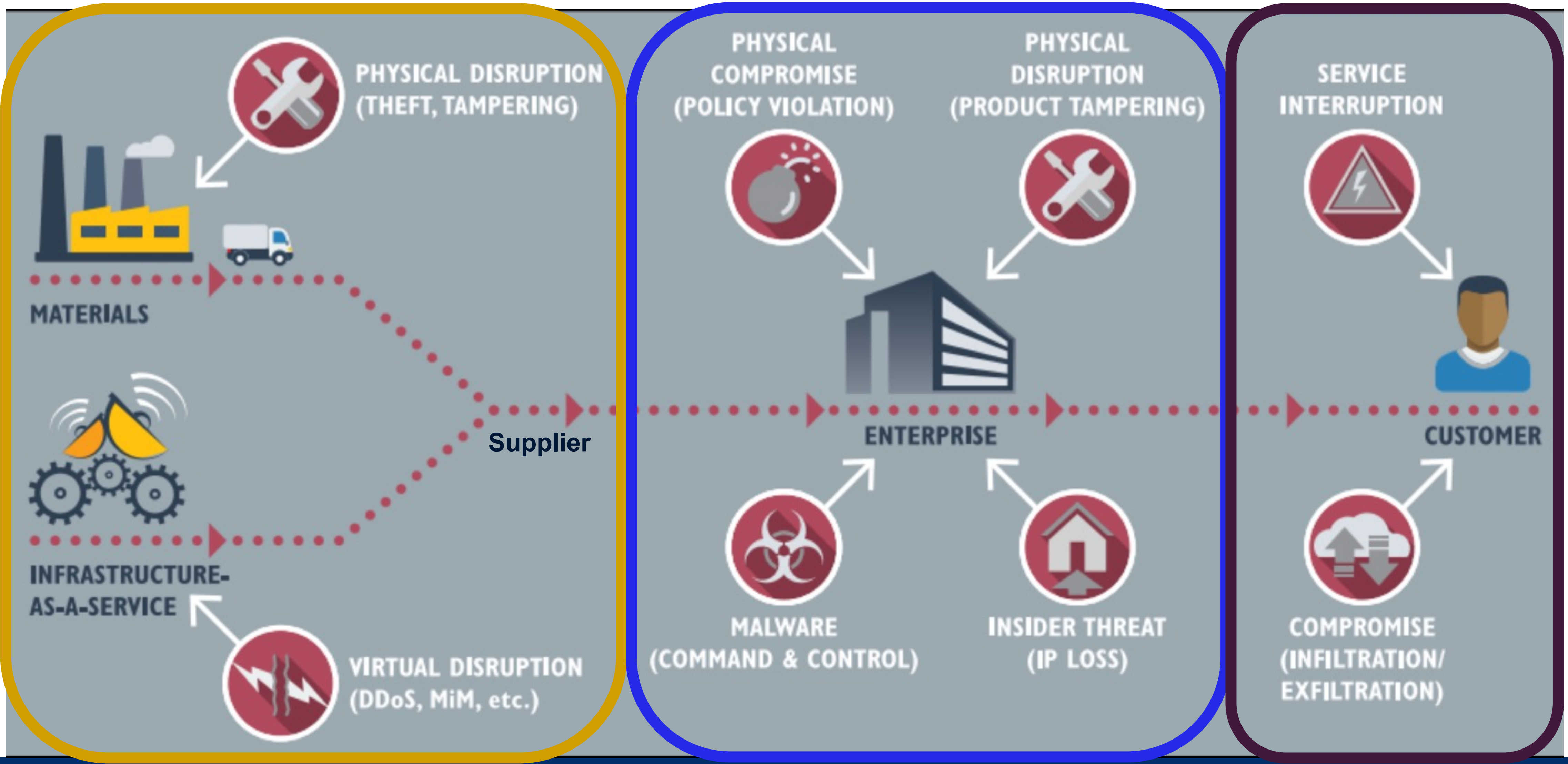
Key Factors Contributing to Defense Industrial Base (DIB) Supply Chain Security Complexity

- Size
- Reduced Visibility
- Globalization
- Increasing Requirements
- Increasing Threats/Awareness


Customer
System Integrator
External Service Provider
Supplier
Supplier
Supplier
External Service Provider
Supplier
Supplier
Supplier
Supplier
External Service Provider
Reduced visibility, understanding and control

Source: NIST SP 800-161
URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf

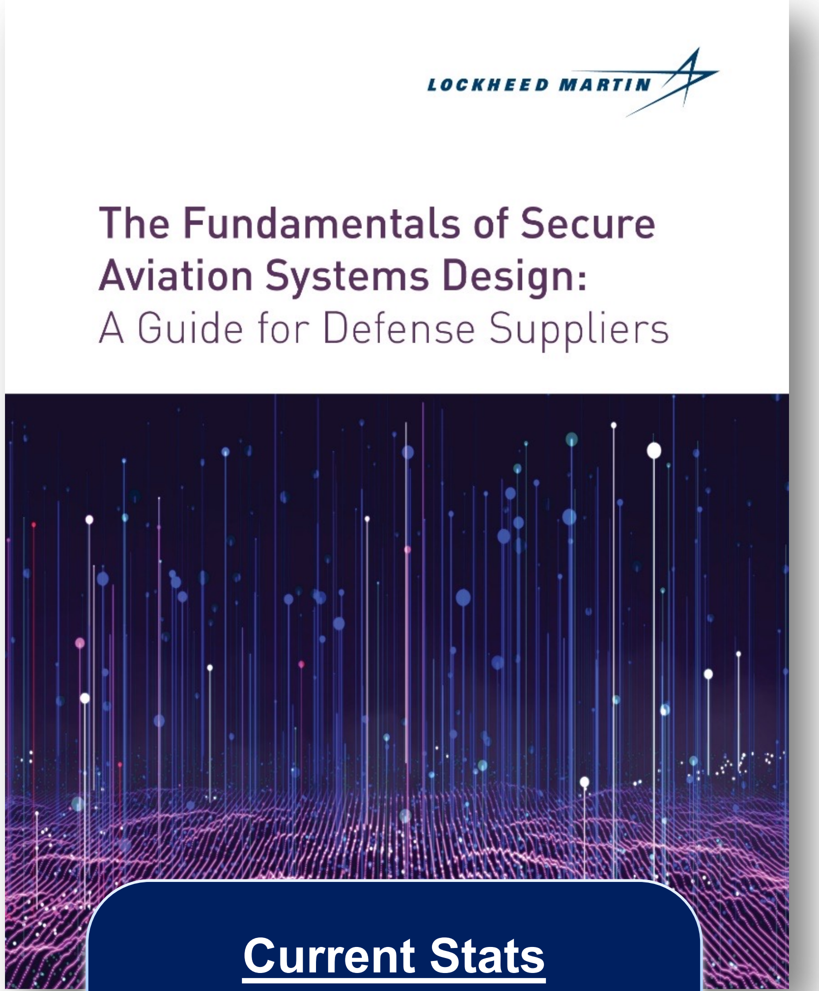
Supply Chain Cyber Vulnerabilities


PHYSICAL DISRUPTION (THEFT, TAMPERING)
MATERIALS
Supplier
INFRASTRUCTURE-AS-A-SERVICE
VIRTUAL DISRUPTION (DDoS, MiM, etc.)
PHYSICAL COMPROMISE (POLICY VIOLATION)
PHYSICAL DISRUPTION (PRODUCT TAMPERING)
ENTERPRISE
MALWARE (COMMAND & CONTROL)
INSIDER THREAT (IP LOSS)
SERVICE INTERRUPTION
CUSTOMER
COMPROMISE (INFILTRATION/ EXFILTRATION)

Source: SANS Institute InfoSec

“Without changing our pattern of thought, we will not be able to solve the problems we created with our current patterns of thought.”

-Albert Einstein



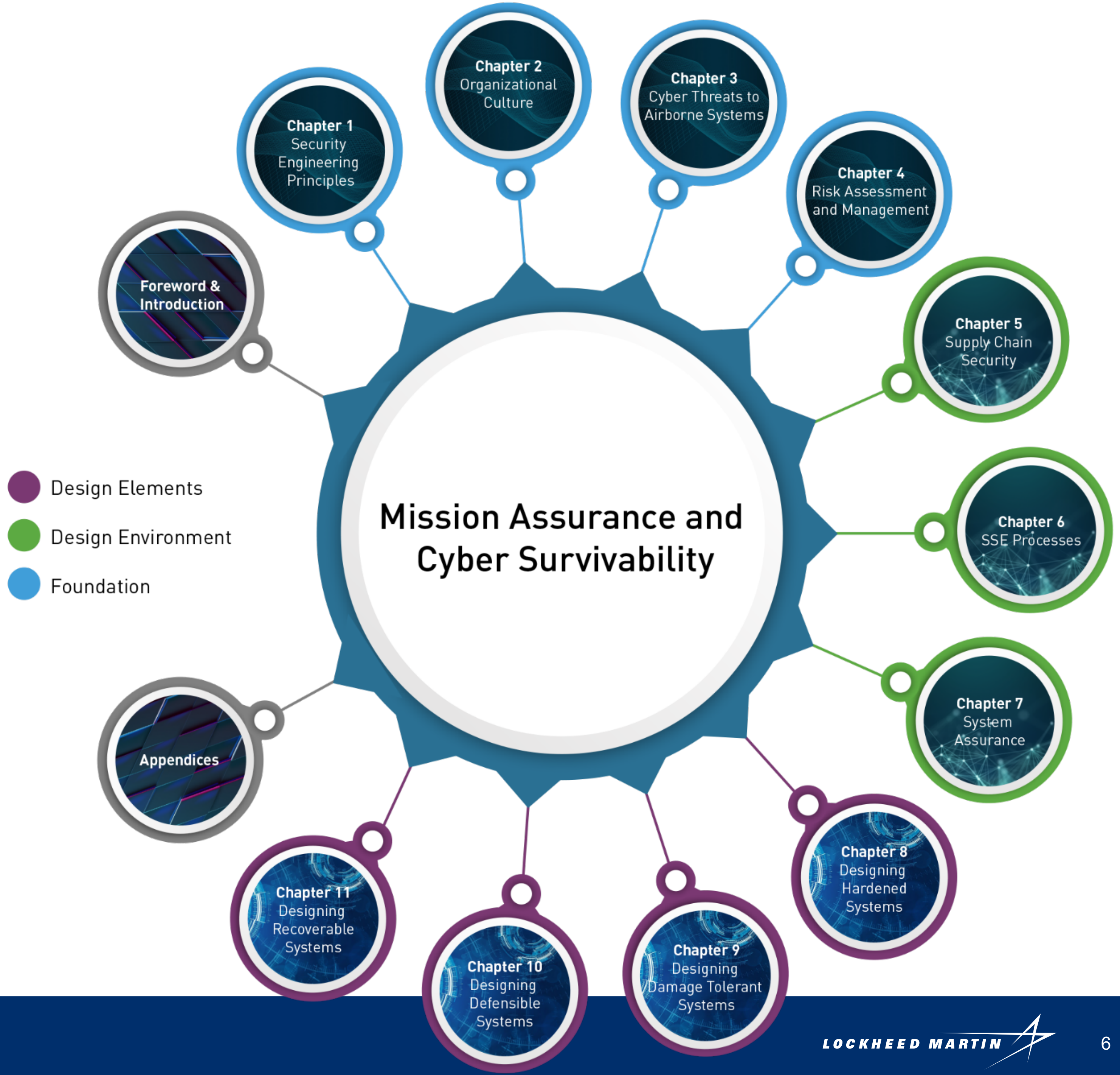
LOCKHEED MARTIN

The Fundamentals of Secure Aviation Systems Design:

A Guide for Defense Suppliers

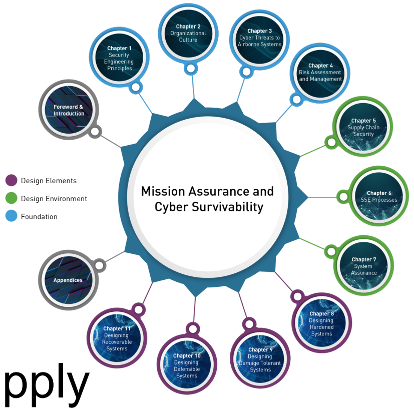
Current Stats

- 21 Sections
- >200 pages
- 15 Authors
- >20 Expert Reviewers



Mission Assurance and Cyber Survivability
Design Elements
Design Environment
Foundation
Foreword & Introduction
Chapter 1 Security Engineering Principles
Chapter 2 Organizational Culture
Chapter 3 Cyber Threats to Airborne Systems
Chapter 4 Risk Assessment and Management
Chapter 5 Supply Chain Security
Chapter 6 SSE Processes
Chapter 7 System Assurance
Chapter 8 Designing Hardened Systems
Chapter 9 Designing Damage Tolerant Systems
Chapter 10 Designing Defensible Systems
Chapter 11 Designing Recoverable Systems
Appendices

Foundational Elements


Chapter 1 Security Engineering Principles
Chapter 2 Organizational Culture
Chapter 3 Cyber Threats to Airborne Systems
Chapter 4 Risk Assessment and Management
Foreword & Introduction
Design Elements
Design Environment
Foundation
Mission Assurance and Cyber Survivability
Chapter 5 Supply Chain Security
Chapter 6 SSE Processes
Chapter 7 System Assurance
Appendices
Chapter 11 Designing Recoverable Systems
Chapter 10 Designing Defensible Systems
Chapter 9 Designing Damage Tolerant Systems
Chapter 8 Designing Hardened Systems

Understand The Fundamentals

Engineers involved in design need to be familiar with the security engineering principles that apply to securely designing ICT/OT systems

Cultivate the Culture

Even though some engineers specialize in systems security engineering, all engineers need to understand its basic concepts and security attributes as they emerge from the system. Unless an organization understands and values product security, it will always regard it as an area that increases cost, but provides no functional value. With that perspective, organizations tend to trade off product security in favor of other priorities.

Knows the threats and Know your risks

Designers and builders also need both an awareness of threats and an understanding of how to assess and manage risks to systems. Without an understanding of the types of cyber threats and how they operate, designers will simply be guessing as they develop their systems.

Design Environment – Trending Design Philosophies

Design Elements
Design Environment
Foundation
Mission Assurance and Cyber Survivability
Foreword & Introduction
Chapter 1 Security Engineering Principles
Chapter 2 Organizational Culture
Chapter 3 Cyber Threats to Airborne Systems
Chapter 4 Risk Assessment and Management
Chapter 5 Supply Chain Security
Chapter 6 SSE Processes
Chapter 7 System Assurance
Chapter 8
Appendices

Model-Based Systems Engineering (MBSE)

- Evidence-based assessments of vulnerabilities of supplier-provided components
- Early discovery of system vulnerabilities which would save program cost/schedule, and improve quality
- Reduction in cost/schedule associated with production of documentation
- Timely impact assessments for shifting design decisions or requirements

DevSecOps

- Facilitates rapid delivery of capability in increments for early security assessment
- Proactive security equates to early vulnerability detection that saves the cost/time of addressing downstream issues
- More secure product and prevention of breaches early in product lifecycle
- Reduced insider threat via SPEs
- CI/CD pipeline fosters culture of continuous improvement
- Quantifiable risk metrics

Zero-Trust Architecture (ZTA)

- Protection from both internal and external threats
- Embeds security throughout the architecture to prevent unauthorized access to critical assets
- Provide zones of visibility
- Reduces the attack surface and risk
- Damage is contained if compromise occurs

Design Elements

Mission Assurance and Cyber Survivability
Foreword & Introduction
Chapter 1 Security Engineering Principles
Chapter 2 Organizational Culture
Chapter 3 Cyber Threats to Airborne Systems
Chapter 4 Risk Assessment and Management
Chapter 5 Supply Chain Security
Chapter 6 SSE Processes
Chapter 7 System Assurance
Chapter 8 Designing Hardened Systems
Chapter 9 Designing Damage Tolerant Systems
Chapter 10 Designing Defensible Systems
Chapter 11 Designing Recoverable Systems
Appendices
Design Elements
Design Environment
Foundation

	Hardening	Damage Tolerance	Defensibility	Recover
Security Pillars for a Medieval Castle	• Walls • Moat • Drawbridge	• Built of damage resistant materials • Multiple water sources • Multiple storage areas	• Rampart to walk on and observe the enemy • Towers • Holes in the walls to shoot from	• Building materials to rebuild walls • Skilled masons, carpenters and blacksmiths

	Cyber Hardening	Cyber Damage Tolerance	Cyber Defensibility	Cyber Recover
Security Pillars for a Notional Future Fighter	• Attack-surface minimization • Access control • Encryption • Segmentation • Data security	• Distributed, diversified and redundant avionics • Partitioning • Out-of-band backup systems and fail-safes	• Monitoring and logging tools built into the baseline • Intrusion detection and prevention systems • Data strategy facilitating defense	• Forensics capability • War reserve modes • Rapid software development and loading capabilities

Parting Thoughts

- For Lockheed to succeed with our customers, our supply chain must be able to defend itself, and provide secure defendable components.

- The threat is real, both theft of Intellectual Property, and to the mission assurance of a delivered product.

- Lockheed is spending internal funds to assist the supply chain.

- We hope this guidebook provides key information that the supply chain, from the smallest shop to the majors, can use.

“Knowledge without practice is useless.
Practice without knowledge is dangerous.”

-Confucius

LOCKHEED MARTIN