Aircraft Systems and Network Security Mitigation of Cyber Threat Risks

Stephen Sterling

DND / ADM(Materiel)

17 Nov 2016

Acknowledgement

Some material generated and authorized for use by:

Peter Skaves

FAA, Chief Scientific & Technical Advisor for Advanced Avionics

Key Takeaways…

- Aircraft are exposed to cyber threats
- Perfectly secure systems do not exist…no silver bullet
- Requirements, guidance, methodology exist to mitigate risk
- Security is an end-end life cycle requirement…
- Identify, Protect, **Detect, Respond, Recover**
- Adequate, competent resources required

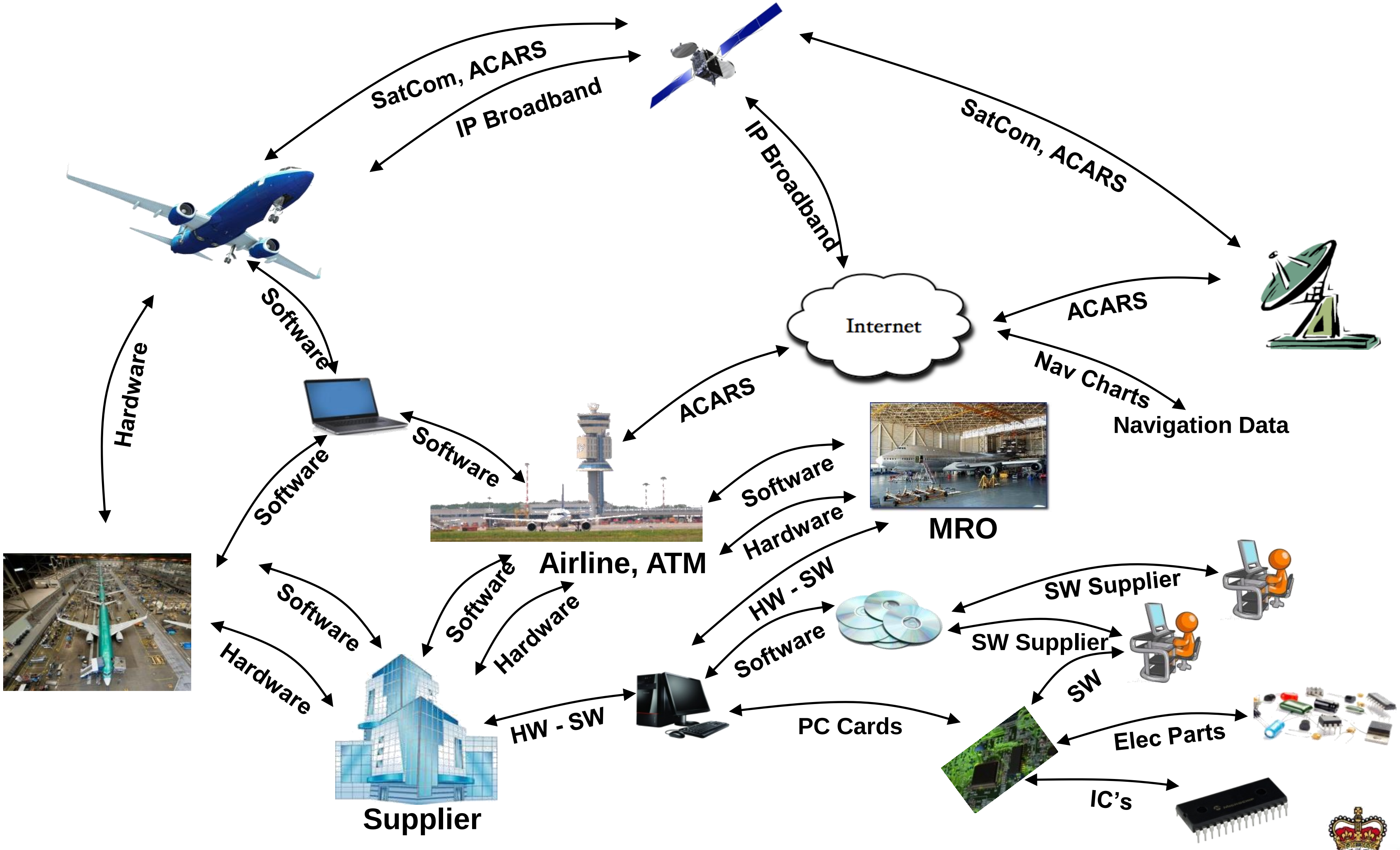
Security Terminology

- Desire to distinguish traditional IT from embedded systems (eg. aircraft systems)

- FAA used several terms for security from electronic attacks on networks and systems: network security, information security, systems security, cyber security…evolving

- FAA are now trying to standardize on the term *Aircraft Systems Information Security Protection* (ASISP)…

Today's Aircraft Environment



Aircraft Connectivity

- Legacy aircraft have used architectures with limited wired or wireless connectivity

- This is rapidly changing as aircraft are incorporating:
  - ✓ Wi-Fi
  - ✓ Electronic Flight Bags
  - ✓ Wireless Field Loadable Software
  - ✓ Real-time aircraft health monitoring and reporting
  - ✓ Passenger Information and Entertainment Systems connectivity to public networks such as the internet

Attacks are possible (or happened)…

cisco

Incidents

KDFW

Runway Ahead

Entering Runway

Public Demonstration of Aircraft Systems Vulnerabilities

- Hack in The Box (HITB) conference – Amsterdam 2013
  - Hugo Teso presents his research work to hack into the FMS of different aircraft.
  - He shows that he can remotely control an aircraft flight path through a smart phone interface

- Black Hat Las Vegas 2014
  - Hacking aircraft Satcom system
  - Santamarta reveals satcom vulnerabilities that can be exploited using aircraft IFE / Wi-Fi systems

FAA Perspective

- Greatest threat is the exploitation of aircraft electronic access points via public networks
- Focus on connectivity to internal / external aircraft systems, networks
- Published policy statements, special conditions and issue papers to mitigate potential vulnerabilities during type design
- Advisory Circular 119-1: Aircraft Network Security Program for continuing airworthiness
- Aviation Rulemaking Advisory Committee (ARAC) to provide additional recommendations on ASISP (before end 2016)

Aeronautical Systems Security

- Collaborative work between RTCA SC-216 and EUROCAE WG-72 since mid 2007
- Seeking consensus between aircraft OEM, systems designers, CNS/ATM systems designers and operators, airlines maintenance and operations personnel and government

RTCA

THE AVIATION GOLD STANDARD SINCE 1935

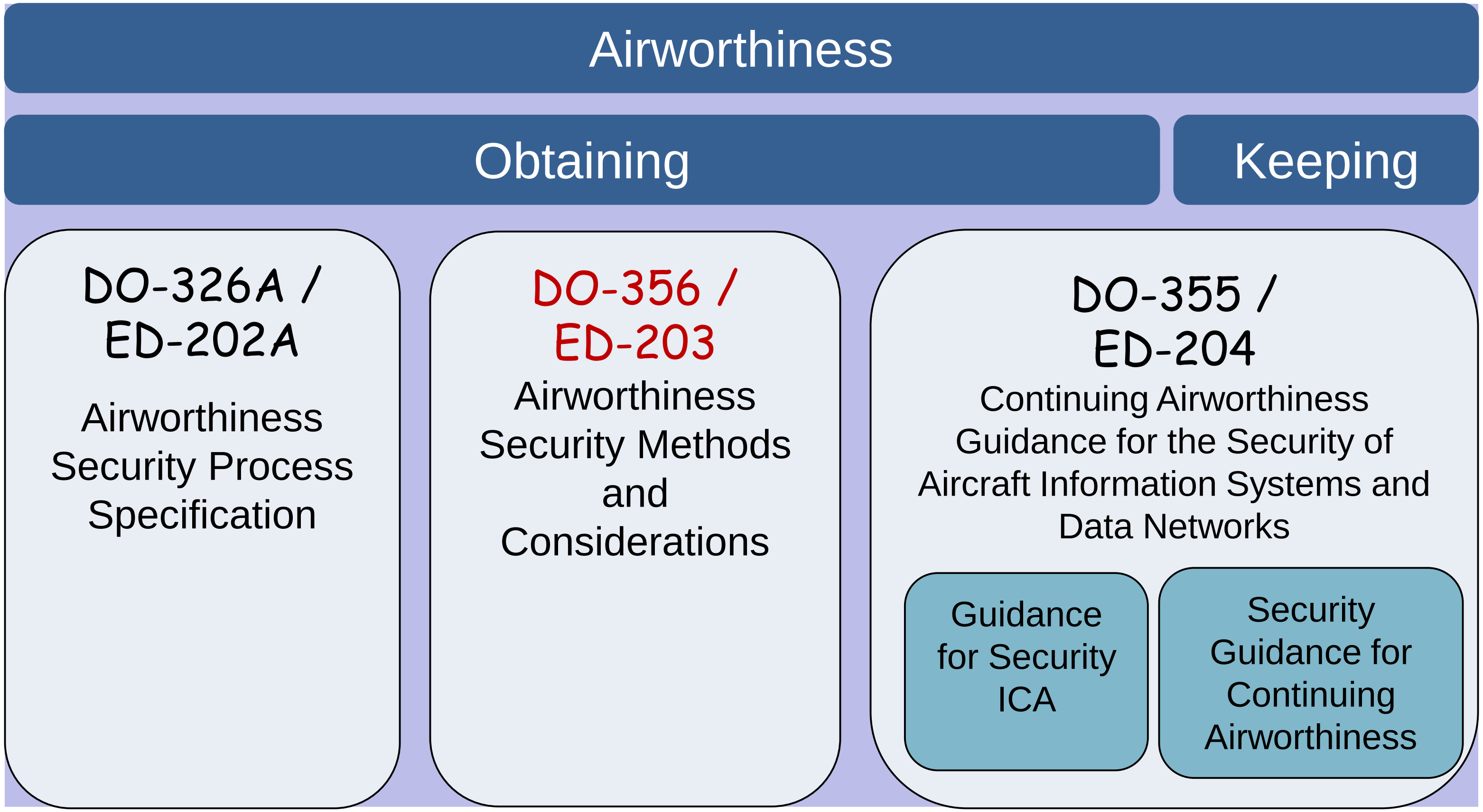
EUROCAE

Outside of scope of SC-216

- Harm from natural events and equipment failure
- Physical security
- Legacy maintenance and physical sabotage
- Business security concerns
- **Design Environment - Suppliers (revisit later…)**
- Security of the deliverables recommended by these standards

NOTE: US NIST / CSEC ITSG cover some gaps for business security and design environment…

SC-216 Deliverables and Respective Roles



Airworthiness

Obtaining

Keeping

DO-326A / ED-202A

Airworthiness Security Process Specification

DO-356 / ED-203

Airworthiness Security Methods and Considerations

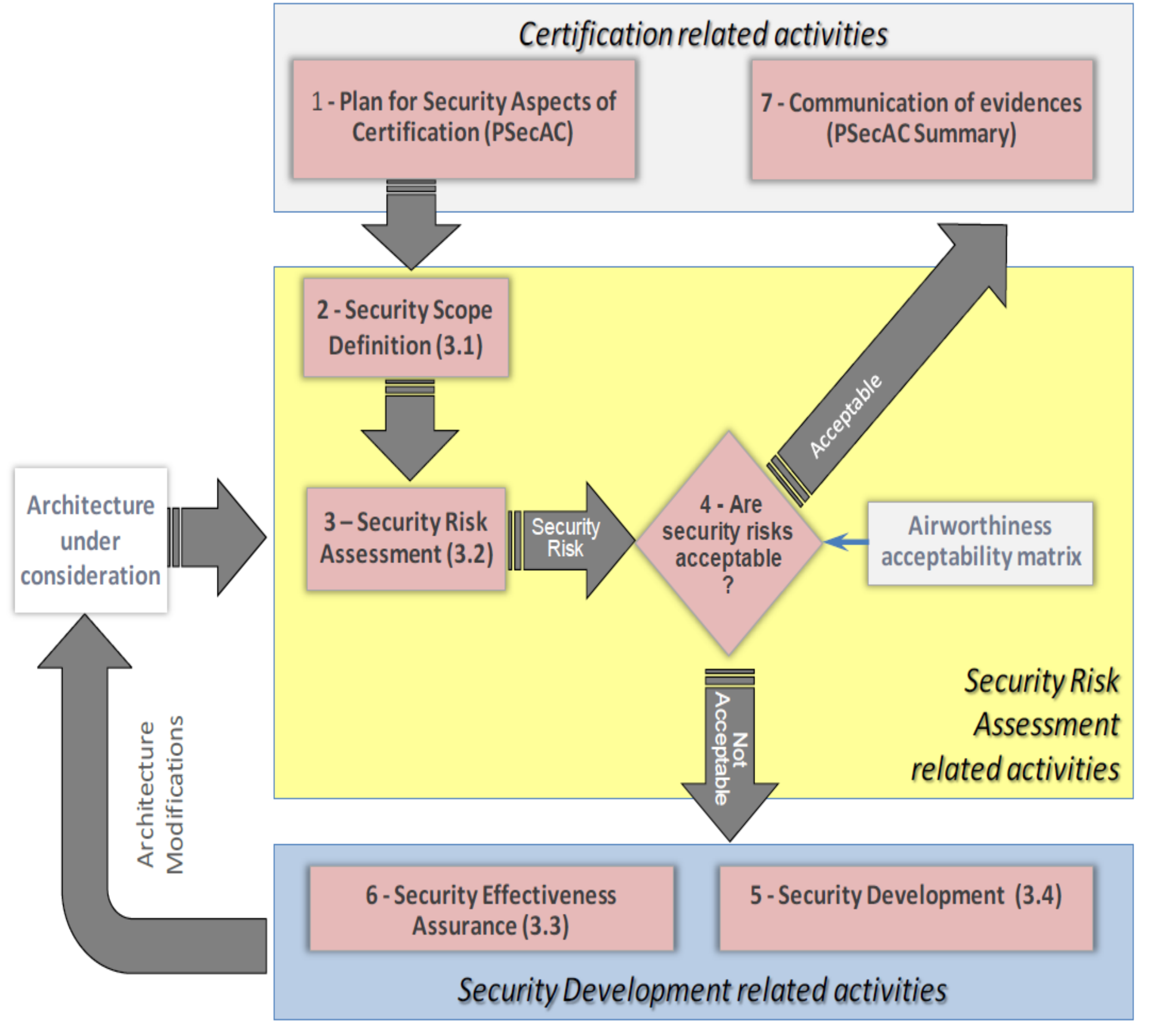
DO-355 / ED-204

Continuing Airworthiness Guidance for the Security of Aircraft Information Systems and Data Networks

Guidance for Security ICA

Security Guidance for Continuing Airworthiness

Airworthiness Security Process (326A/202) & Methods and Considerations (356, 203)


Certification related activities
1 - Plan for Security Aspects of Certification (PSecAC)
7 - Communication of evidences (PSecAC Summary)
2 - Security Scope Definition (3.1)
Acceptable
Architecture under consideration
3 – Security Risk Assessment (3.2)
Security Risk
4 - Are security risks acceptable ?
Airworthiness acceptability matrix
Not Acceptable
Security Risk Assessment related activities
Architecture Modifications
6 - Security Effectiveness Assurance (3.3)
5 - Security Development (3.4)
Security Development related activities

Security Scope Definition

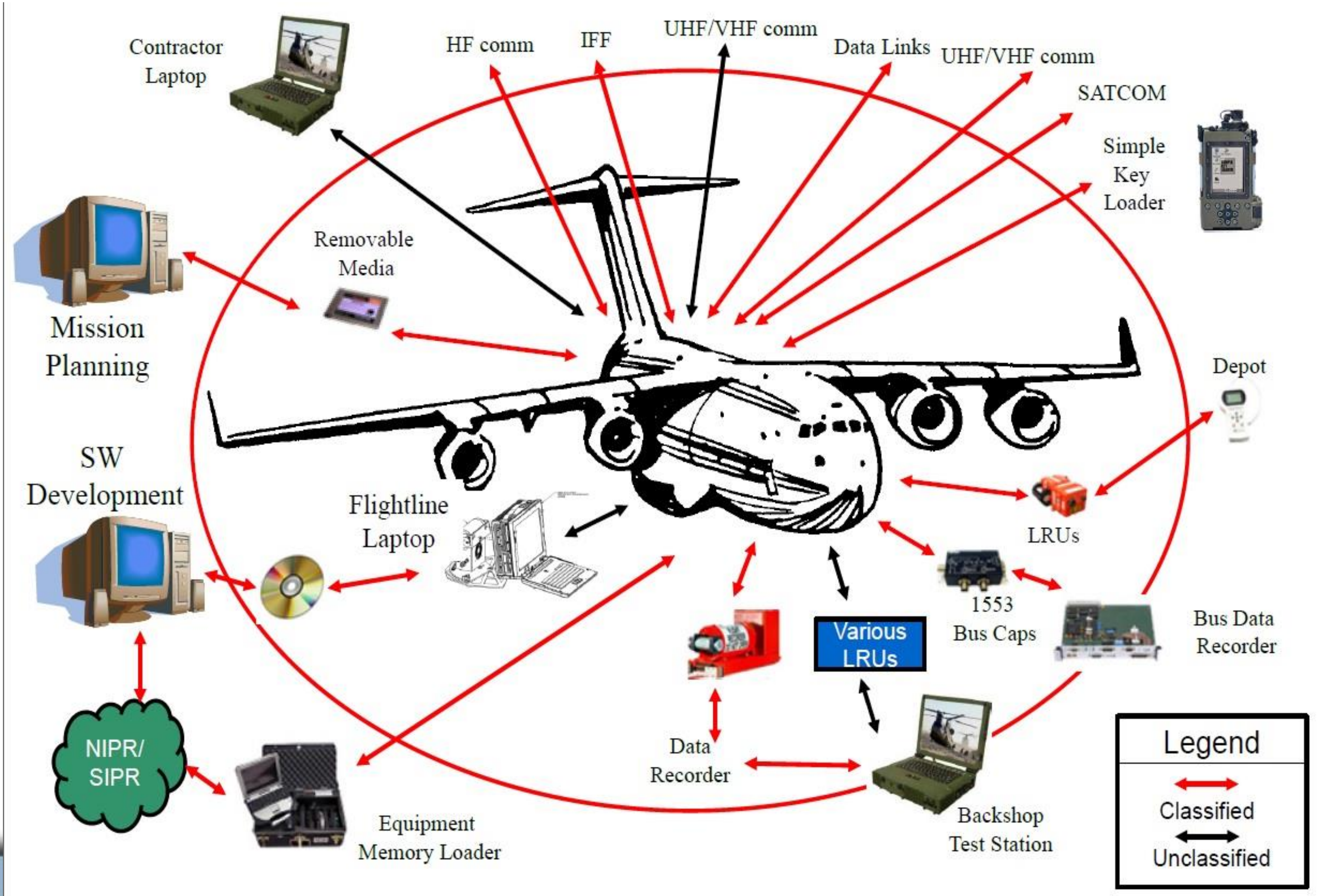
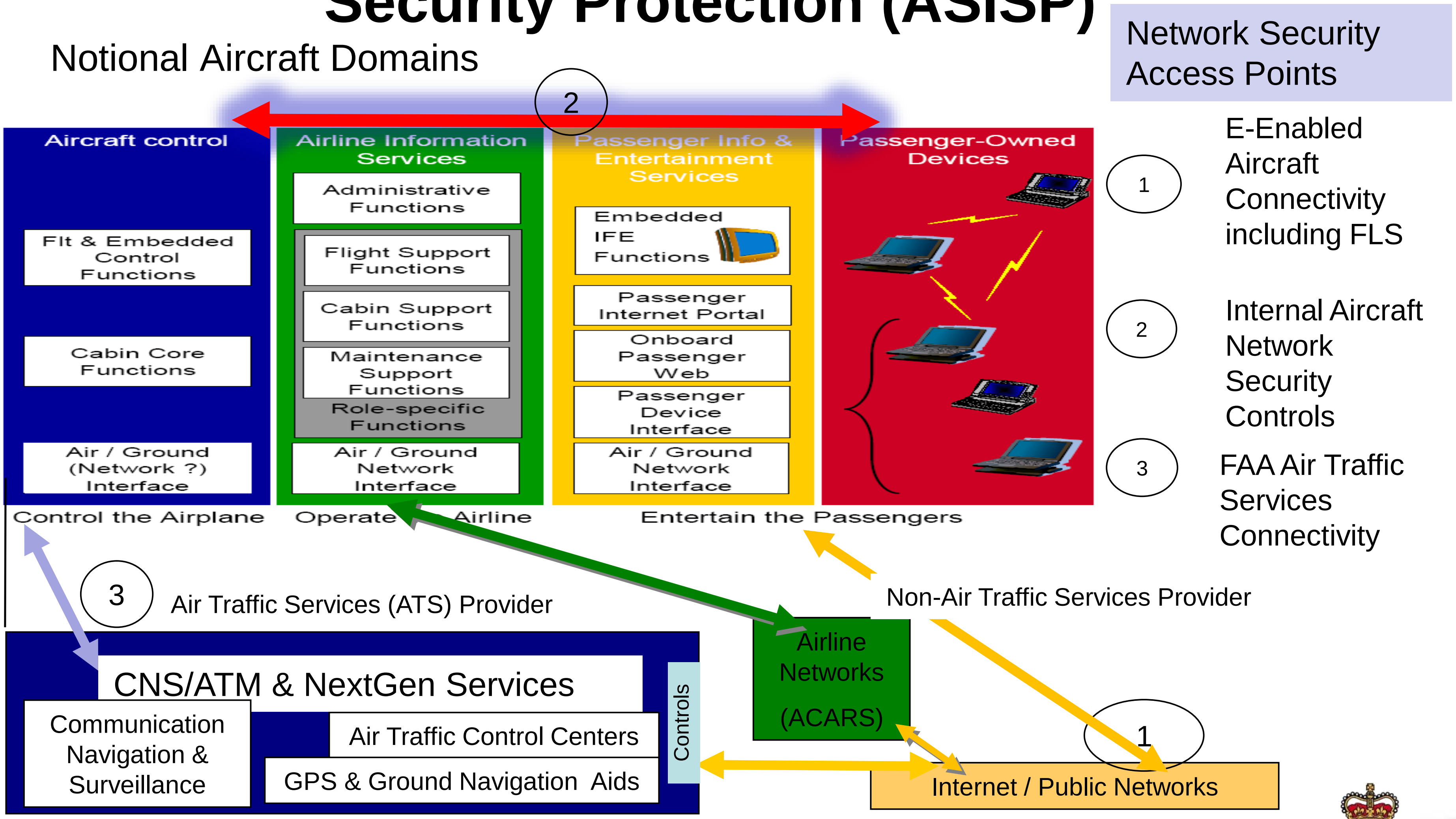


Figure 1 - Aircraft Systems Information Security Protection (ASISP)

Notional Aircraft Domains


Network Security Access Points
1
E-Enabled Aircraft Connectivity including FLS
2
Internal Aircraft Network Security Controls
3
FAA Air Traffic Services Connectivity
2
Aircraft control
Flt & Embedded Control Functions
Cabin Core Functions
Air / Ground (Network ?) Interface
Airline Information Services
Administrative Functions
Flight Support Functions
Cabin Support Functions
Maintenance Support Functions
Role-specific Functions
Air / Ground Network Interface
Passenger Info & Entertainment Services
Embedded IFE Functions
Passenger Internet Portal
Onboard Passenger Web
Passenger Device Interface
Air / Ground Network Interface
Passenger-Owned Devices
Control the Airplane
Operate the Airline
Entertain the Passengers
3
Air Traffic Services (ATS) Provider
Non-Air Traffic Services Provider
CNS/ATM & NextGen Services
Communication Navigation & Surveillance
Air Traffic Control Centers
GPS & Ground Navigation Aids
Controls
Airline Networks
(ACARS)
1
Internet / Public Networks

Security in Continuing Airworthiness

DO-355 / ED-204

Provide guidance for information security protection during aircraft operation and maintenance

Security in Continuing Airworthiness

Topics Addressed by DO-355 / ED-204

- Airborne Software
- Aircraft Components
- Aircraft Network Access Points
- Ground Support Equipment
- Ground Support Information Systems
- Digital Certificates
- Aircraft Information Security Incident Management
- Operator Aircraft Information Security Program
- Operator Organization Risk Assessment
- Operator Personnel Roles and Responsibilities
- Operator Personnel Training

DND’s Aerospace Engineering Program Based on…

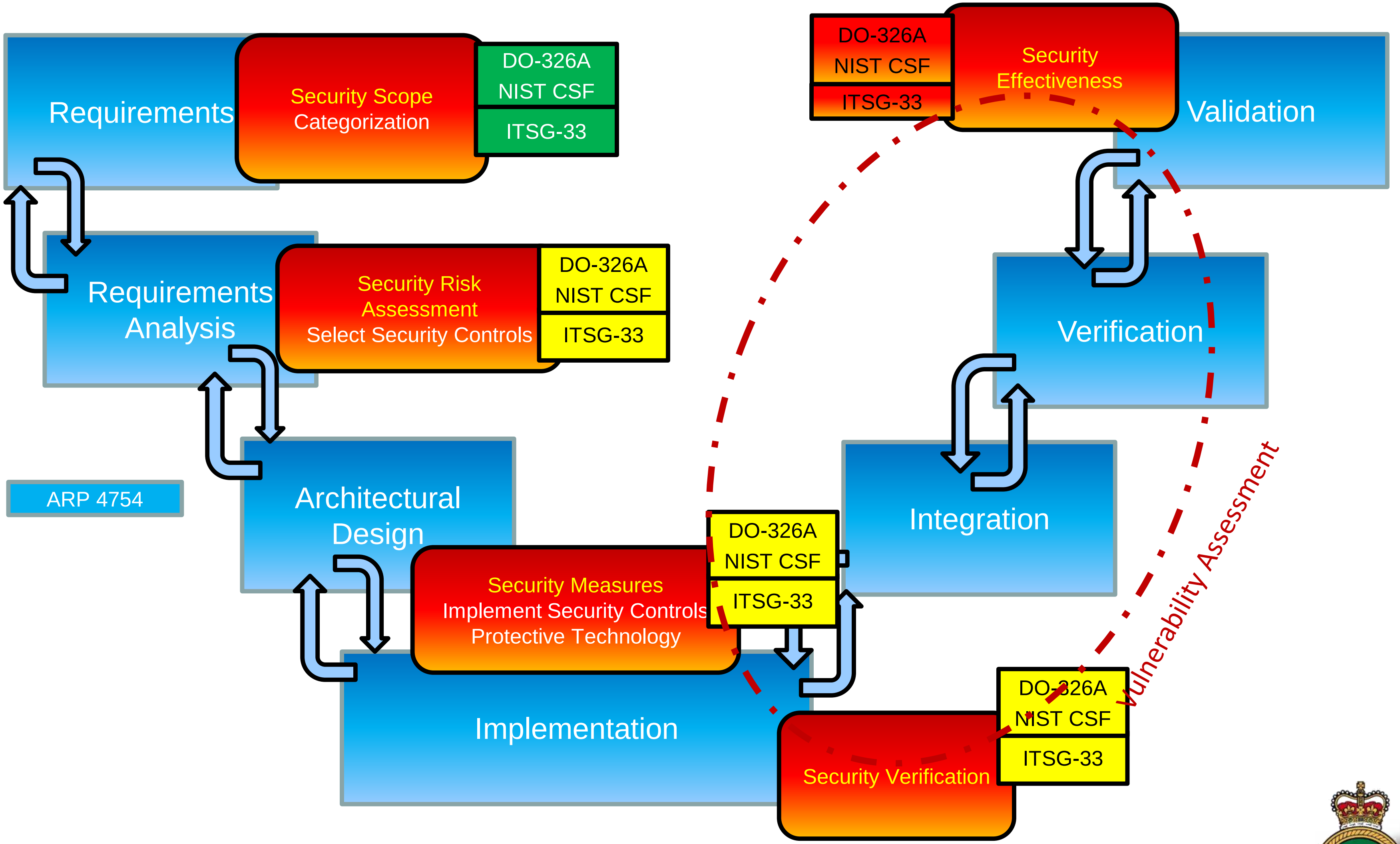
- Airworthiness Requirements (required by Aeronautics Act)
  - Civilian Airworthiness Certification using 3 RTCA/EUROCAE Standards
  - Military Airworthiness Certification (MIL-HDBK-516 / DEF STAN 00-970)

- Allied Programs (required by Canada Cyber Security Strategy)
  - DoD Program Protection Plan
  - UK DEF STAN 05-138 Cyber Security for Defence Suppliers
  - Focus of US and UK is security of the Supply Chain (including Cyber Security for Defence Suppliers)

    *** BTI Global Innovation (Bernadette Terry) - Info Assurance for Small and Medium Enterprise, UK Cyber Essentials assistance

- Departmental Policies
  - NDSODs (ITSG-33)

Systems SECURITY Engineering



Requirements

Security Scope Categorization

DO-326A NIST CSF

ITSG-33

Requirements Analysis

Security Risk Assessment Select Security Controls

DO-326A NIST CSF

ITSG-33

ARP 4754

Architectural Design

Security Measures Implement Security Controls Protective Technology

DO-326A NIST CSF

ITSG-33

Implementation

Security Verification

DO-326A NIST CSF

ITSG-33

Integration

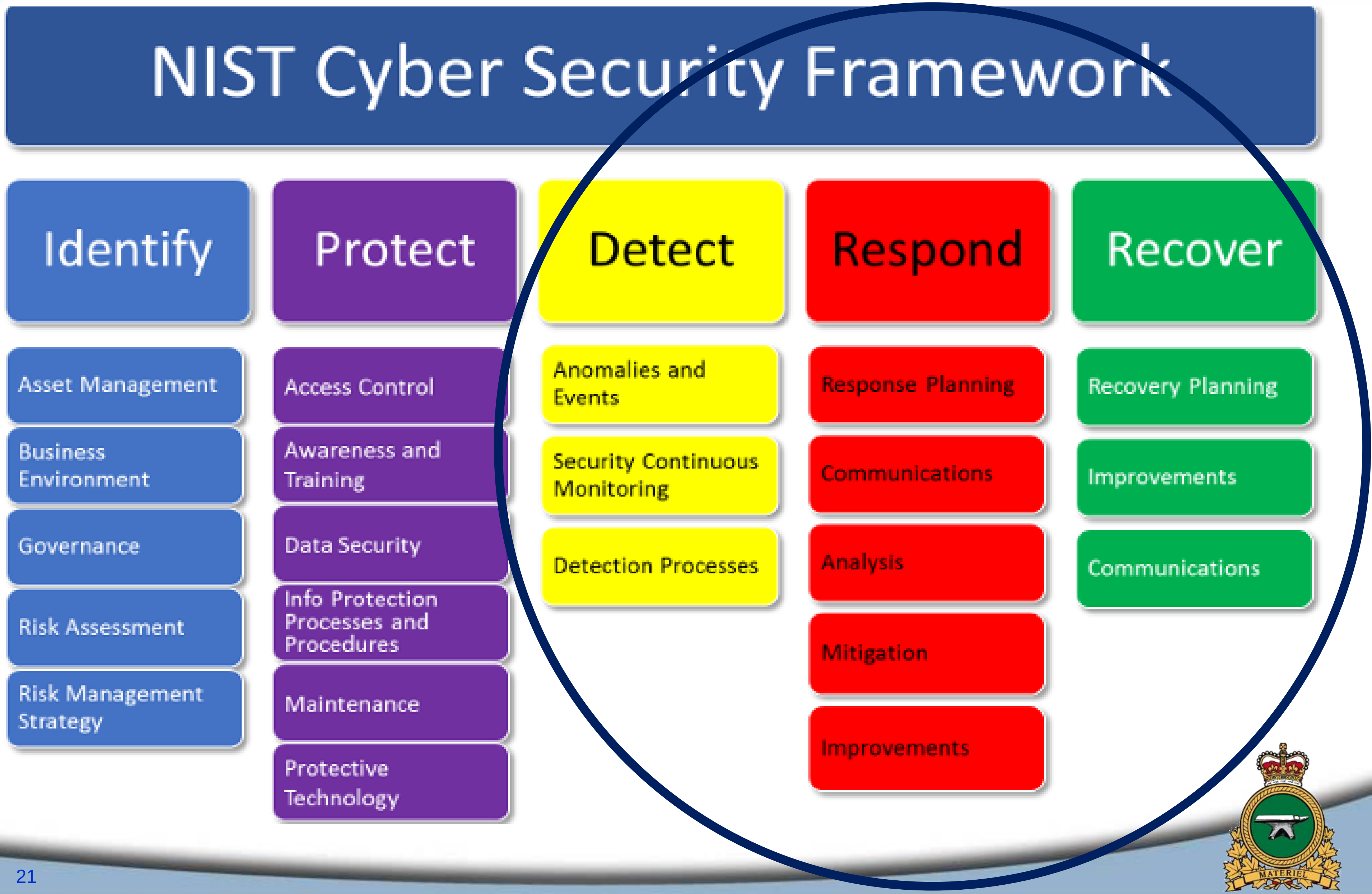
Verification

Validation

Security Effectiveness

DO-326A NIST CSF

ITSG-33



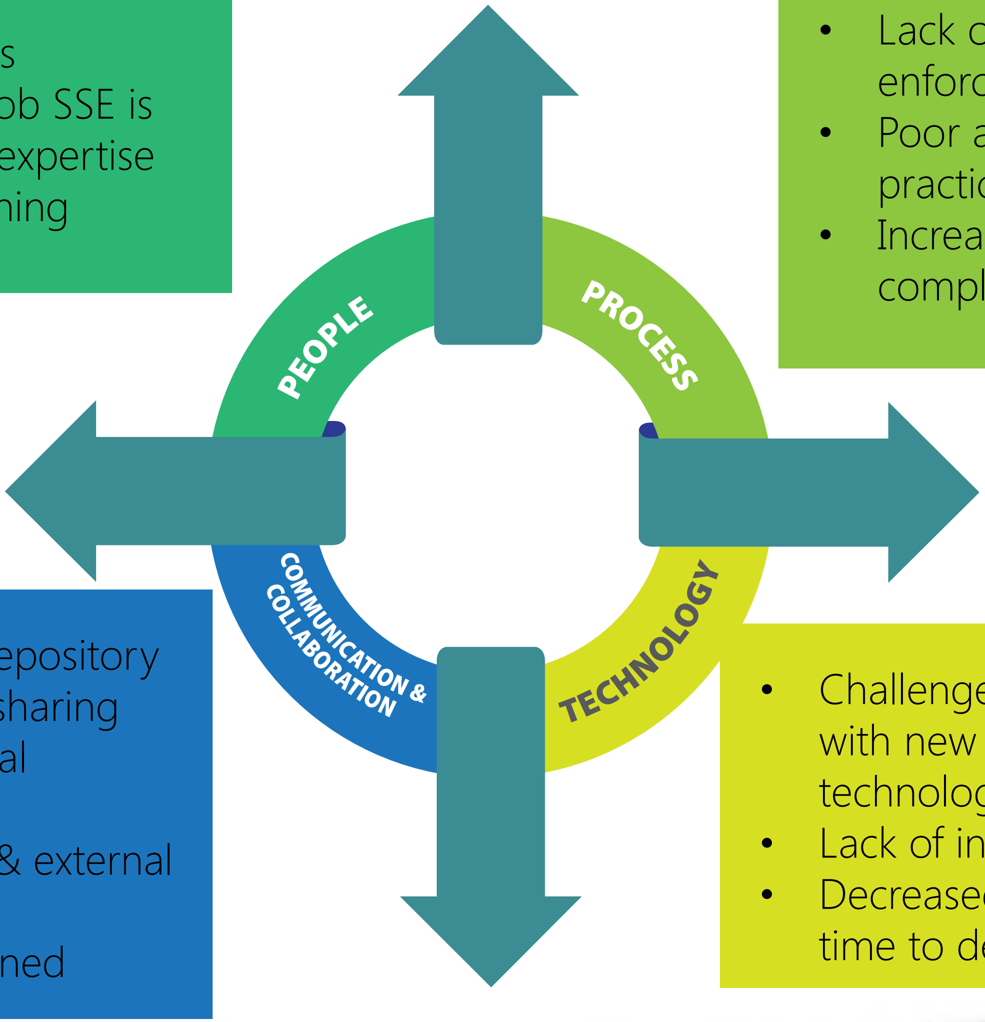
NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Acquisition Lifecycle Development Challenges

- Lack of SSE skills
- Lack of resources
- Unclear whose job SSE is
- Lack of domain expertise
- Lack of SSE training

- Non-agile development
- Lack of regulations & process enforcement
- Poor adoption of SSE best practices
- Increasing SoS – SSE design complexity of large system



- Lack of central repository for information sharing
- Lack of situational awareness
- Lack of internal & external collaboration
- Few lessons learned

- Challenge keeping up with new & changing technology
- Lack of interoperability
- Decreased development time to deployment

Questions?

Stephen Sterling
Team Leader – Aircraft System Security Engineering
Directorate Technical Airworthiness and Engineering Support
Stephen.sterling@forces.gc.ca
819-939-4741