BOEING

Engineering, Operations & Technology
Phantom Works

LANs in Aircraft, including Safety and Security Issues

FAA LAN study Phase 1 result summary
29 Jun 2007

This work was supported by the Federal Aviation Administration, Aircraft Certification Service (AIR-1), 800 Independence Ave., S. W.,

Washington, DC 20591

Eric Fleischman, Randy Smith, Nick Multari
Boeing Phantom Works
Eric.Fleischman@Boeing.com
Randall.E.Smith@Boeing.com
Nicholas.J.Multari@Boeing.com

Disclaimer

The contents of this presentation do not represent the positions of The Boeing Company nor the Federal Aviation Administration. They are only the thoughts of the authors

Presentation Outline

- **Overview**
  - **Trends**
  - **FAA LAN Phase 1 Study**
- **Security and Safety**
- **Initial Acceptance Criteria**
  - **Security Engineering**
    - **Vulnerabilities**
    - **Threats**
    - **Risks**
    - **Countermeasures**
- **Findings and Recommendations**
  - **Findings**
  - **Recommendations**

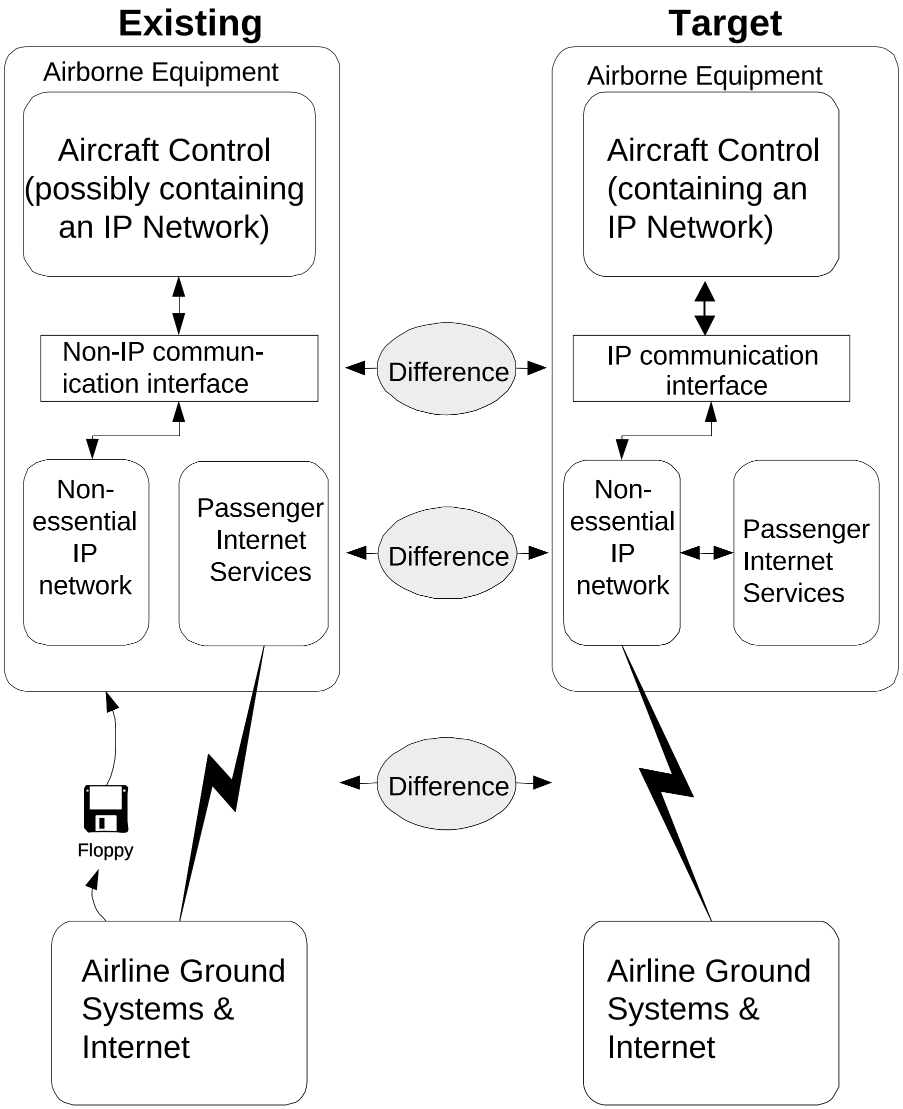
Research Study Motivation

Trend: **Aviation industry is evolving to new, network-based architectures.**

Issue: **Security vulnerabilities introduced by LANs on aircraft could result in unanticipated safety failures.**

Goal: **Develop evaluation criteria that can be used by certification authorities and industry to ensure that onboard networks will not negatively impact aircraft safety.**

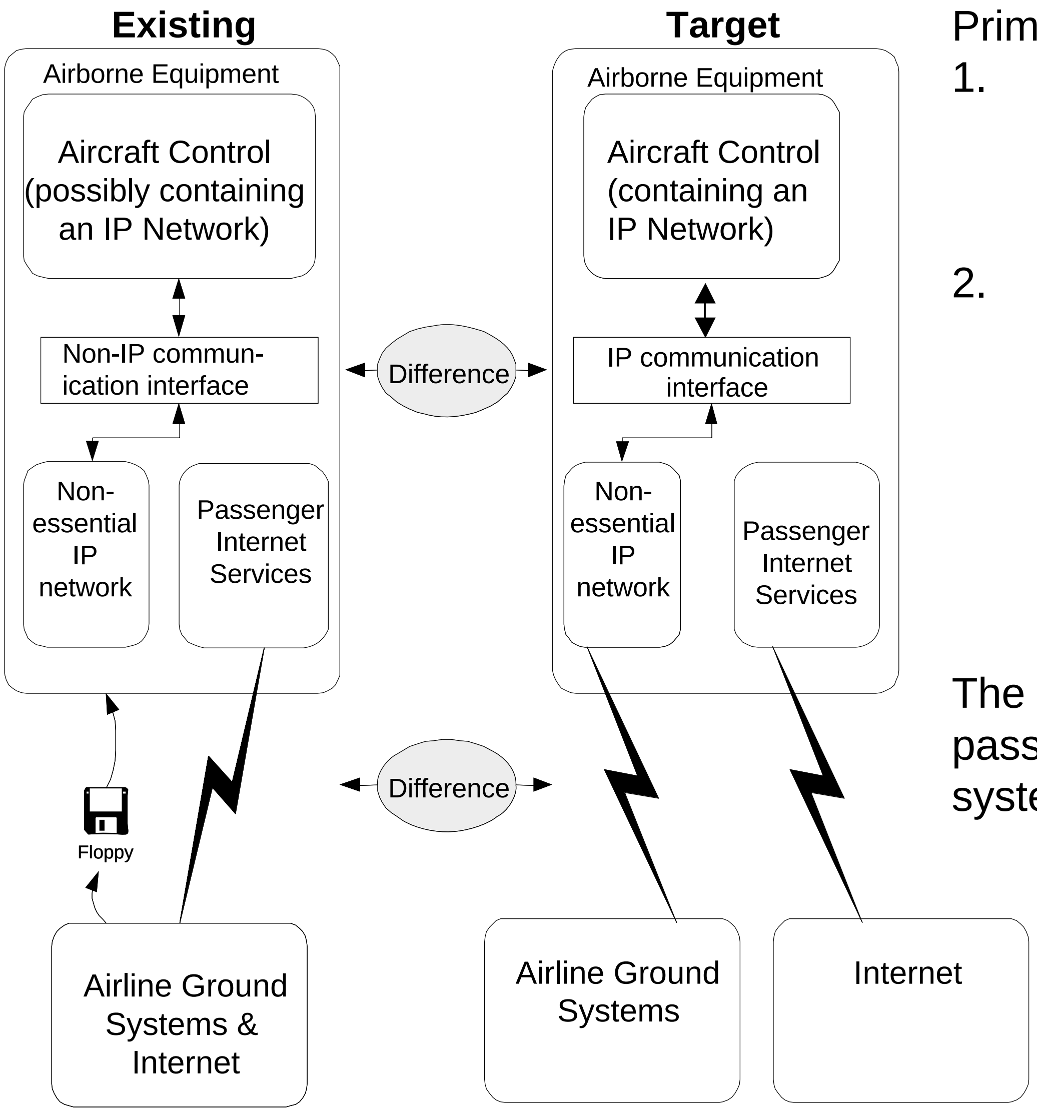
Proposed Target Architecture – Evaluative Domain


Existing
Target
Airborne Equipment
Aircraft Control (possibly containing an IP Network)
Non-IP communication interface
Non-essential IP network
Passenger Internet Services
Floppy
Airline Ground Systems & Internet
Difference
Difference
Difference
Airborne Equipment
Aircraft Control (containing an IP Network)
IP communication interface
Non-essential IP network
Passenger Internet Services
Airline Ground Systems & Internet

Primary differences:

1. Aircraft shares a common Internet protocol (IP)-based network system.
2. Passenger Services, Aircraft Control, and Airline Information Services share a common network system.
3. Specific Aircraft Control and Airline Information Services processes form distributed network relationships with ground computers.

Alternative Target Architecture



Existing

Airborne Equipment

Aircraft Control (possibly containing an IP Network)

Non-IP communication interface

Non-essential IP network

Passenger Internet Services

Floppy

Airline Ground Systems & Internet

Difference

Difference

Target

Airborne Equipment

Aircraft Control (containing an IP Network)

IP communication interface

Non-essential IP network

Passenger Internet Services

Airline Ground Systems

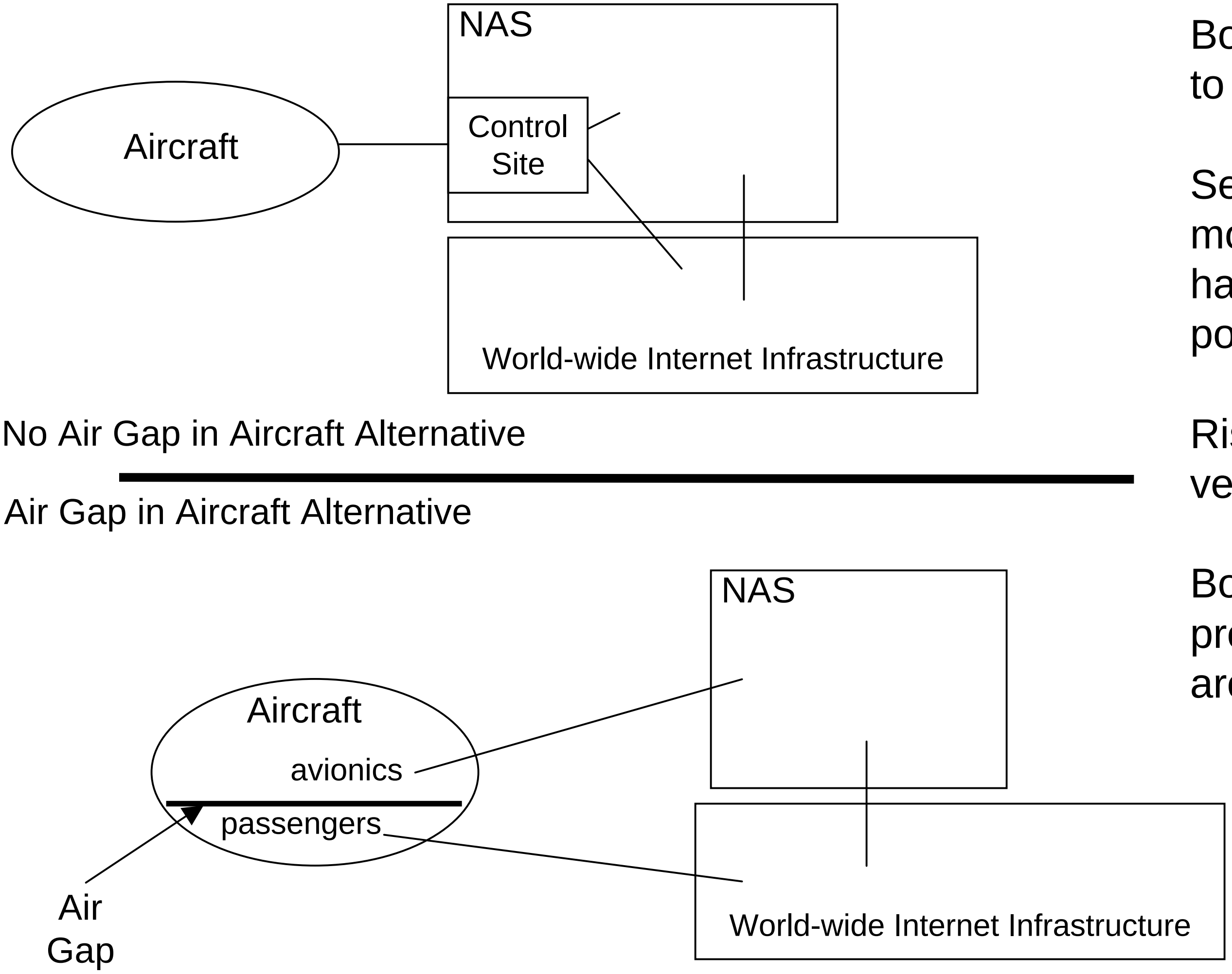
Internet

Primary differences:

1. Aircraft Control, and Airline Information Services share a common network system.
2. Specific Aircraft Control and Airline Information Services processes form distributed network relationships with ground computers by using an IP-based air-to-ground link.

The air gap between the aircraft passengers and the avionics systems remains intact.

Terse commentary on target architecture differences


NAS
Aircraft
Control Site
World-wide Internet Infrastructure
No Air Gap in Aircraft Alternative
Air Gap in Aircraft Alternative
NAS
Aircraft
avionics
passengers
Air Gap
World-wide Internet Infrastructure

Both approaches are exposed to Internet-based threats.

Second approach is somewhat more secure than the first, but has greater size, weight, and power requirements.

Risk mitigation controls are very similar for both targets.

Both targets use the same proposed target network architecture design.

Presentation Outline

- **Overview**
  - **Trends**
  - **FAA LAN Phase 1 Study**
- **Security and Safety**
- **Initial Acceptance Criteria**
  - **Security Engineering**
    - **Vulnerabilities**
    - **Threats**
    - **Risks**
    - **Countermeasures**
- **Findings and Recommendations**
  - **Findings**
  - **Recommendations**

FAA LAN Research Study Approach – two phases

1. **Investigate methodologies for identifying and mitigating potential security risks of onboard networks that could impact safety**
    - **Investigate safety and security issues introduced by using LANs on aircraft**
    - **Investigate the potential security risks of an onboard network that could impact safety**
    - **Identify initial acceptance criteria**

2. **Investigate techniques for mitigating the security risks in the certification environment**
    - **Investigate the means for mitigating the security risks in the certification environment,**
    - **Provide recommendations for assessing safety effects caused by potential security failures, and**
    - **Provide recommendations for certification of local area networks on aircraft.**

Presentation Outline

- **Overview**
  - **Trends**
  - **FAA LAN Phase 1 Study**
- **Security and Safety**
- **Initial Acceptance Criteria**
  - **Security Engineering**
    - **Vulnerabilities**
    - **Threats**
    - **Risks**
    - **Countermeasures**
- **Findings and Recommendations**
  - **Findings**
  - **Recommendations**

Comparing FAA Software and DoD Classification Levels

DO-178B (Safety)	DoD Security (Confidentiality)
Level A (catastrophic condition)	Top Secret (exceptionally grave damage)
Level B (hazardous/severe condition)	Secret (serious damage)
Level C (major condition)	Confidential (damage)
Level D (minor condition)	Sensitive but Unclassified (could adversely affect)
Level E (no-effect condition)	Unclassified (no effect)

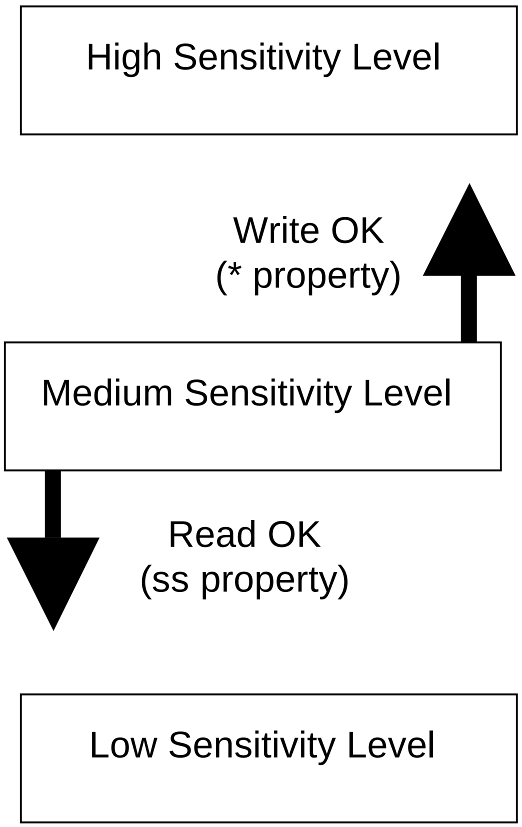
- Both approaches concerned with integrity and availability.
- Both approaches concerned with authentication and authorization in networked environments.
- The DoD Security approach is more concerned with confidentiality and non-repudiation than the safety approach.

Although safety and security have some differences in protection requirements, they also have many similarities.

The levels defining the criticality of the software and data in both domains have parallels. These similarities can potentially help determine where security issues impact the safety of on-board networks.

Security Frameworks for Networked Systems

Bell-LaPadula Confidentiality Model



High Sensitivity Level

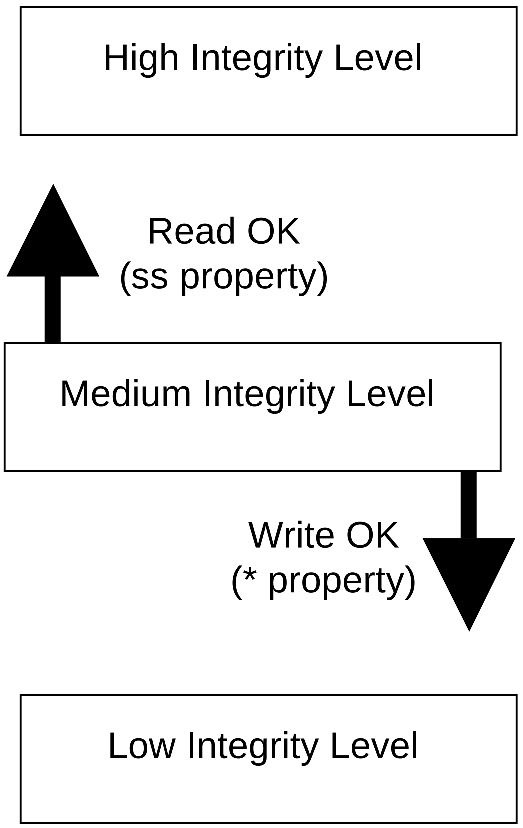
Write OK
(* property)

Medium Sensitivity Level

Read OK
(ss property)

Low Sensitivity Level

Biba Integrity Model



High Integrity Level

Read OK
(ss property)

Medium Integrity Level

Write OK
(* property)

Low Integrity Level

Mapping Classifications to Models

While the Biba Integrity and Bell-LaPadula Confidentiality models are direct analogs of each other, they operate in an inverse fashion to each other.

DoD Security (Confidentiality): Bell LaPadula Model

Top Secret
Secret
Confidential
Sensitive but Unclassified
Unclassified

- Lower level info can be written to (included within) higher level.
- Higher level can see lower level info.

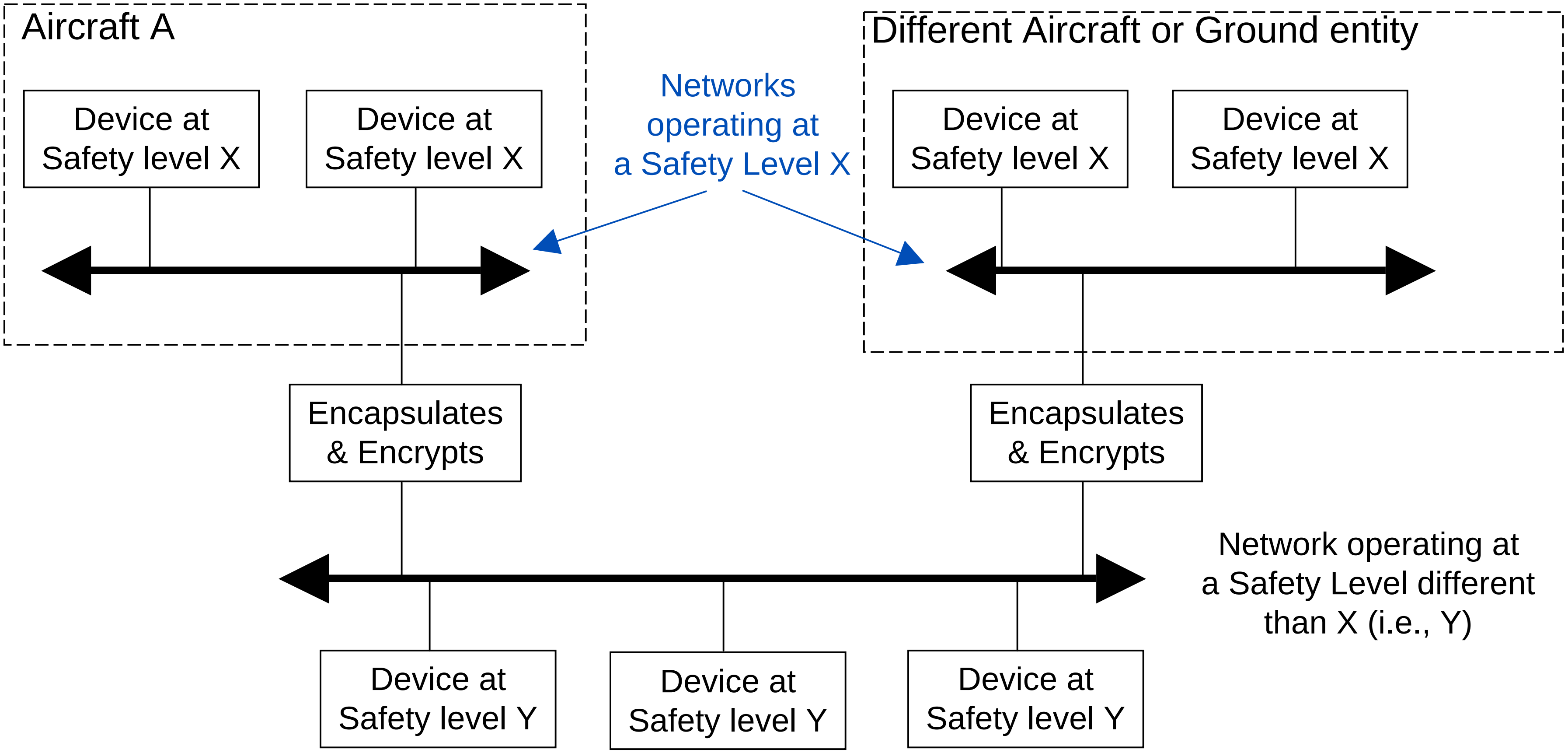
RTCA/DO-178B Safety: Biba Model

Level A
Level B
Level C
Level D
Level E

- Higher level info & processes can be written to (included within) lower level.
- Lower level info can see higher level info.

DO-178B Classifications Extended to Nets. using Biba Model

- Systems grouped into networks each operating at a common safety level
- Common logical networks can be created from physically distributed elements by using virtual private network (VPN) technology.



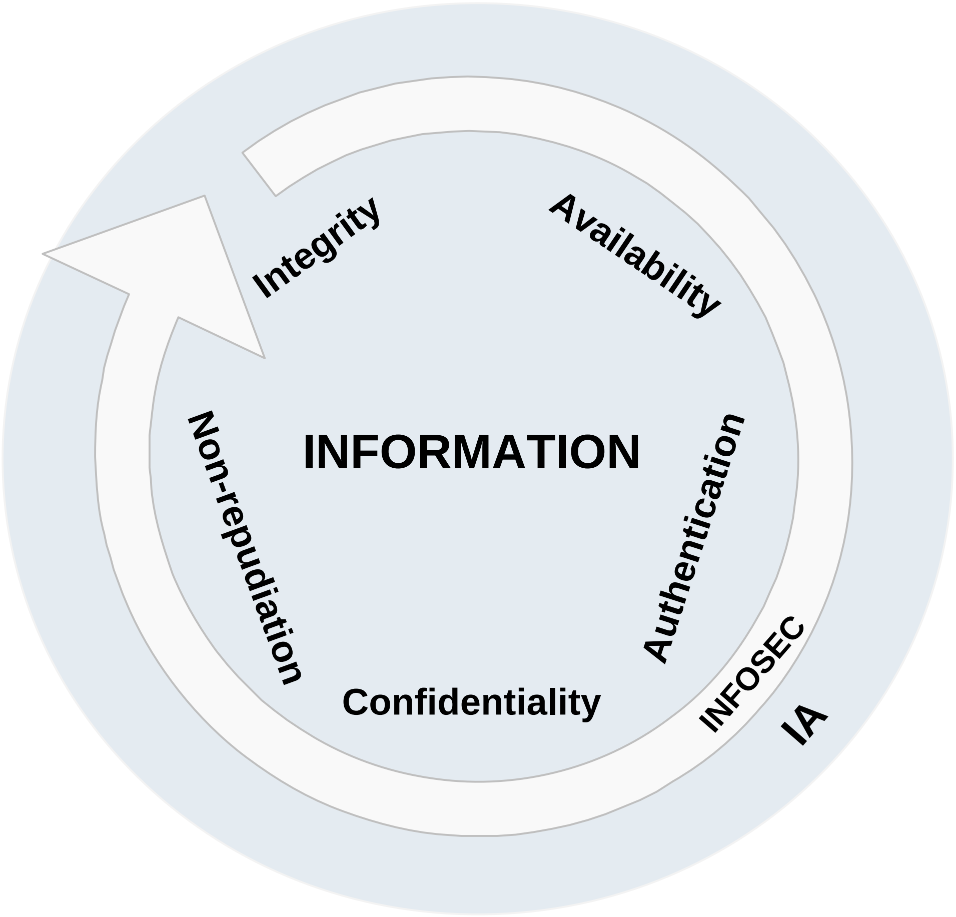
Presentation Outline

- **Overview**
  - **Trends**
  - **FAA LAN Phase 1 Study**
- **Security and Safety**
- **Initial Acceptance Criteria**
  - **Security Engineering** ←
    - **Vulnerabilities**
    - **Threats**
    - **Risks**
    - **Countermeasures**
- **Findings and Recommendations**
  - **Findings**
  - **Recommendations**

What is Information Assurance (IA)?

- “Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.”
- A holistic approach to all facets of Information Protection
- Required for all Government Information Systems (contracts)
- Critical for Certification and Accreditation

Scope of Information Assurance

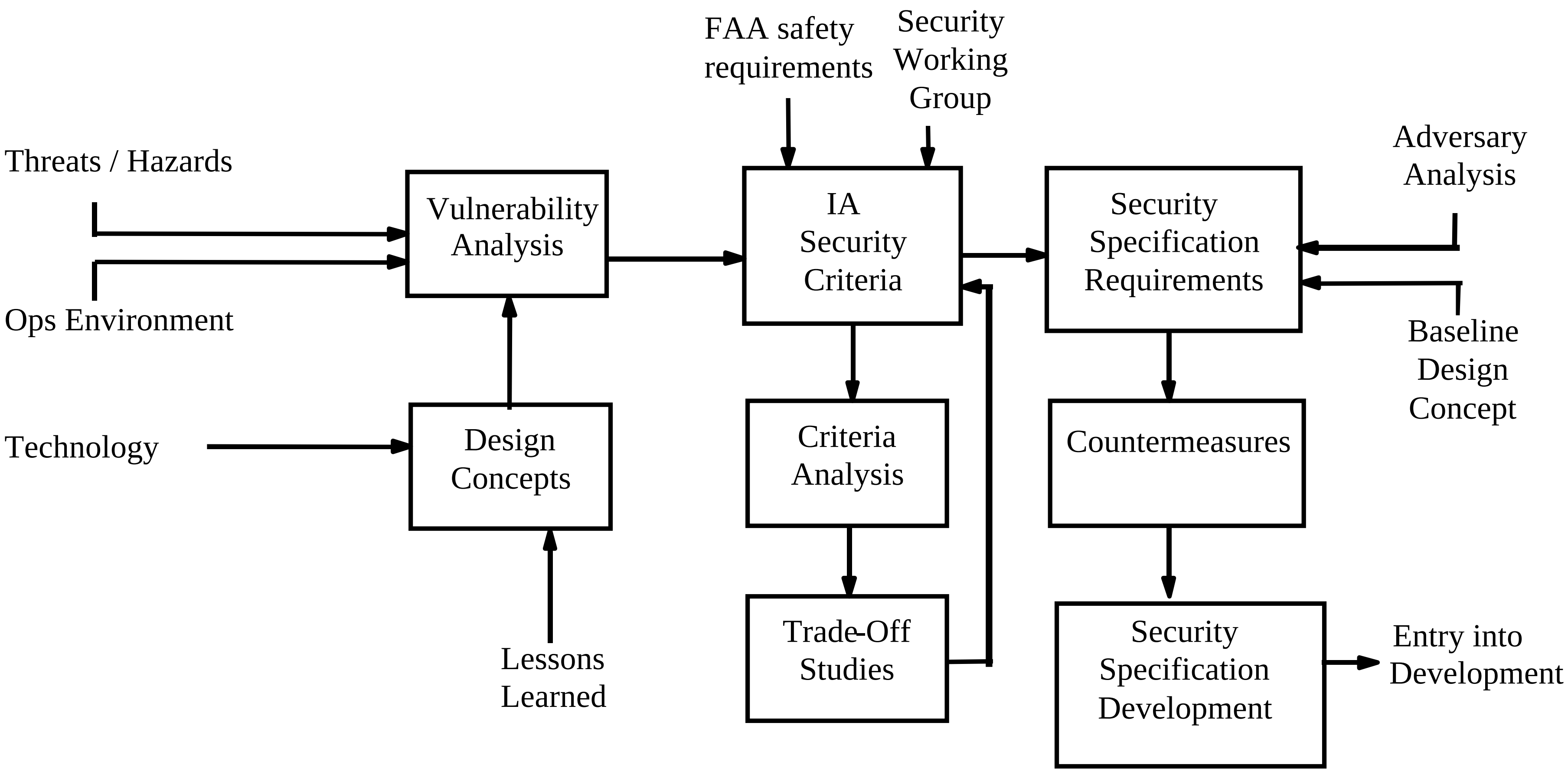


Information Assurance encompasses the INFOSEC role.

System Security Engineering (SSE)

- **Identify the threats to the system**
- **Determine component/system vulnerabilities**
- **Establish effective protection measures**
- **Apply analyses, trade studies, design to cost**
- **Quantify residual risk and formalize a process of risk acceptance and system certification.**

System Security Engineering (SSE) Process



Presentation Outline

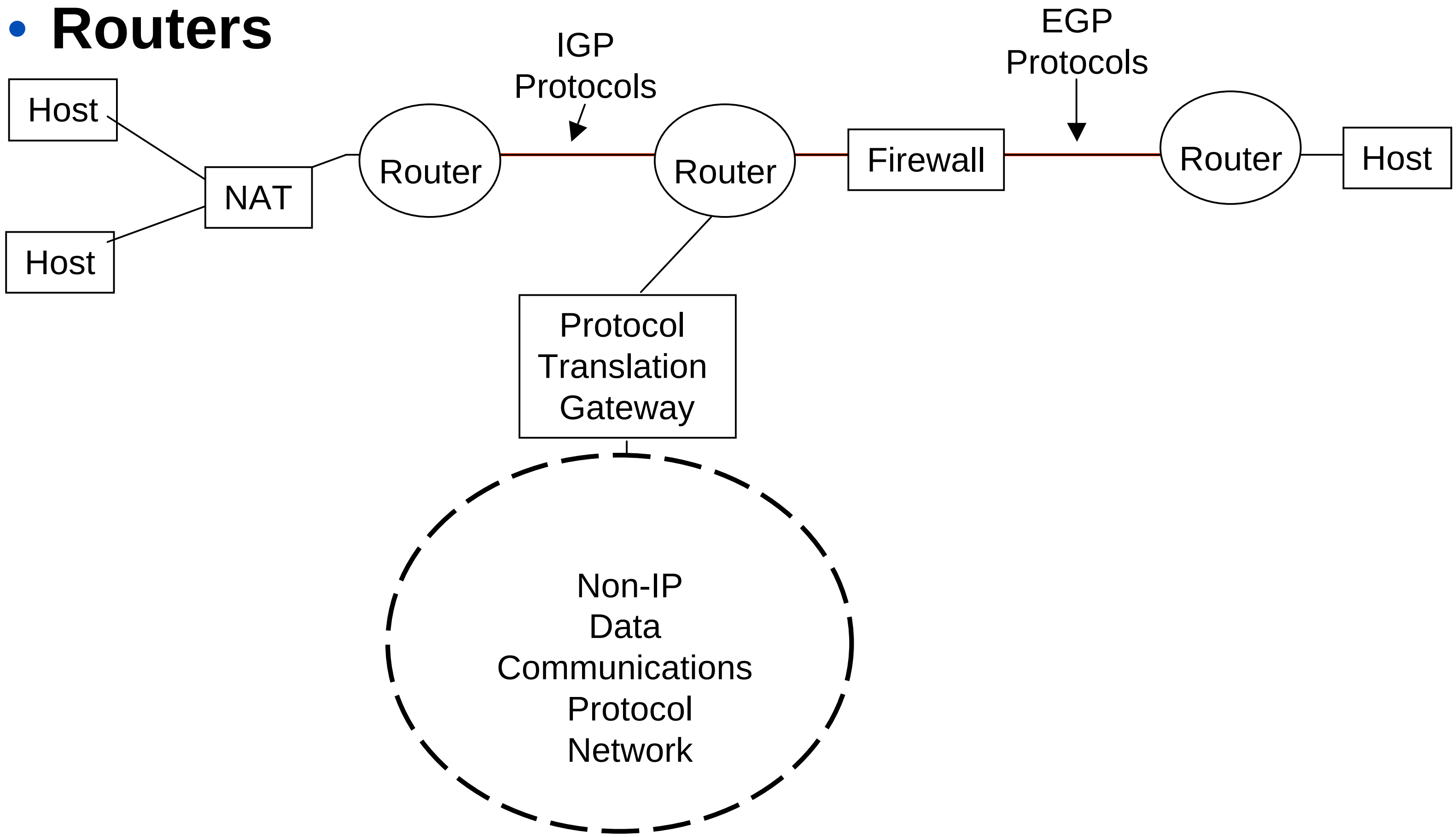
- **Overview**
  - **Trends**
  - **FAA LAN Phase 1 Study**
- **Security and Safety**
- **Initial Acceptance Criteria**
  - **Security Engineering**
    - **Vulnerabilities**
    - **Threats**
    - **Risks**
    - **Countermeasures**
- **Findings and Recommendations**
  - **Findings**
  - **Recommendations**

Safety and Security Intertwined in Network Environments

- **The latent security vulnerabilities of COTS devices, when combined with increased exposure of networked systems, results in potential security problems that can have direct safety implications. E.g.,:**
  - **Protecting authentic aviation software from being modified or replaced by a variant introduced by an attacker.**
  - **Protecting network system elements from attacks that either hinder correct software operation or else modify the reported results of correct software operation.**

Entities Potentially Subject to Attack

- **Hosts (including their applications and data)**
- **Middleboxes**
- **Network protocols and links**
- **Routers**


IGP Protocols
EGP Protocols
Host
Host
NAT
Router
Router
Firewall
Router
Host
Protocol Translation Gateway
Non-IP Data Communications Protocol Network

Presentation Outline

- **Overview**
  - **Trends**
  - **FAA LAN Phase 1 Study**
- **Security and Safety**
- **Initial Acceptance Criteria**
  - **Security Engineering**
    - **Vulnerabilities**
    - **Threats**
    - **Risks**
    - **Countermeasures**
- **Findings and Recommendations**
  - **Findings**
  - **Recommendations**

Threat Agents

- **Corrupted or Careless Insider**
  - Are authorized to access the network
  - NAS personnel, aircraft personnel, aircraft passengers
- **Hostile Outsider**
  - Are not authorized to access the network
  - Located on “the Internet”
- **Client-side Attacks**
  - Malicious software lurking in “neutral” environments (e.g., email, web sites, other)
  - The historic distinction between “data” and “code” is vanishing
  - NAS personnel, aircraft personnel, and aircraft passengers may be duped into inadvertently executing, and thereby introducing, malicious software into the network
  - Network users therefore have become an integral element of a network’s security defenses

Presentation Outline

- **Overview**
  - **Trends**
  - **FAA LAN Phase 1 Study**
- **Security and Safety**
- **Initial Acceptance Criteria**
  - **Security Engineering**
    - **Vulnerabilities**
    - **Threats**
    - **Risks**
    - **Countermeasures**
- **Findings and Recommendations**
  - **Findings**
  - **Recommendations**

The proposed target environments have risk (1/2)

- The larger the networked community, the larger the potential number of threats to the entities within those networks due to (1) direct or indirect relationships between the networked entities themselves and (2) the increased possibility of hostile attackers being present within the system.
- Due to the emergence of client-side attacks and other threats, the (human) end users of networked resources are now an important part of that network’s total security defense posture. Aircraft have limited control over the computer and network behavior of their Internet-connected passengers.
- Entities within networks that are directly or indirectly connected to the Internet may possibly be accessible by attackers located elsewhere in the Internet, despite the presence of intervening security firewalls.
- The Internet has experienced many well-documented instances of hostile attacks affecting the integrity of computers, networked systems, and the data and services they support.
- COTS computer systems have an indeterminate number of latent bugs that can be attacked.

The proposed target environments have risk (2/2)

- **COTS computer systems cannot be adequately secured within large network environments in the general case because their security controls cannot be trusted to perform as intended when attacked.**
- **The security viability of current networked systems is partially a direct function of the configuration and management expertise of its administrative personnel.**
- **The protocols of the Internet Protocol family can be secured but their cumulative underlying key management system is *ad hoc* and complex – with direct configuration and management implications.**
- **The SNMPv3 management protocol has questionable security viability when used in network environments that have large numbers of devices built by many different vendors.**
- **Whenever different security administrations or technologies are joined together in a cooperative manner (e.g., aircraft and ground systems), it is important and challenging to define interfaces between the systems in such a way that a diminished security posture for the total system as a whole doesn't result.**

Presentation Outline

- **Overview**
  - **Trends**
  - **FAA LAN Phase 1 Study**
- **Security and Safety**
- **Initial Acceptance Criteria**
  - **Security Engineering**
    - **Vulnerabilities**
    - **Threats**
    - **Risks**
    - **Countermeasures**
- **Findings and Recommendations**
  - **Findings**
  - **Recommendations**

Recommended Response to Risks

1. **Extend the DO-178B safety framework into networked environments (see next section)**
2. **Ensure security protections for all deployed networked systems**
   - **Follow the Information Assurance Technical Framework (IATF) best practices, including its defense in depth provisions.**
   - **Provide full control life-cycle protections for the defense in depth control elements.**

Sample Defense in Depth Systems

Defend the Network

Perimeter access control (Firewalls); secure routing table updates; explicit inter-AS policies (Security, QoS); appropriate BGP policy settings; Secure Multicast

Defend the Enclave

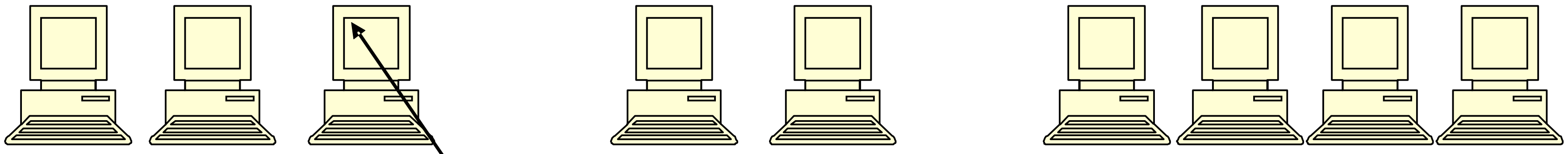
Network Access Controls;
Database security;
Peer-to-peer identification,
authentication & authorization.

Defend the Enclave

Network Access Controls;
Database security;
Peer-to-peer identification,
authentication & authorization.

Defend the Enclave

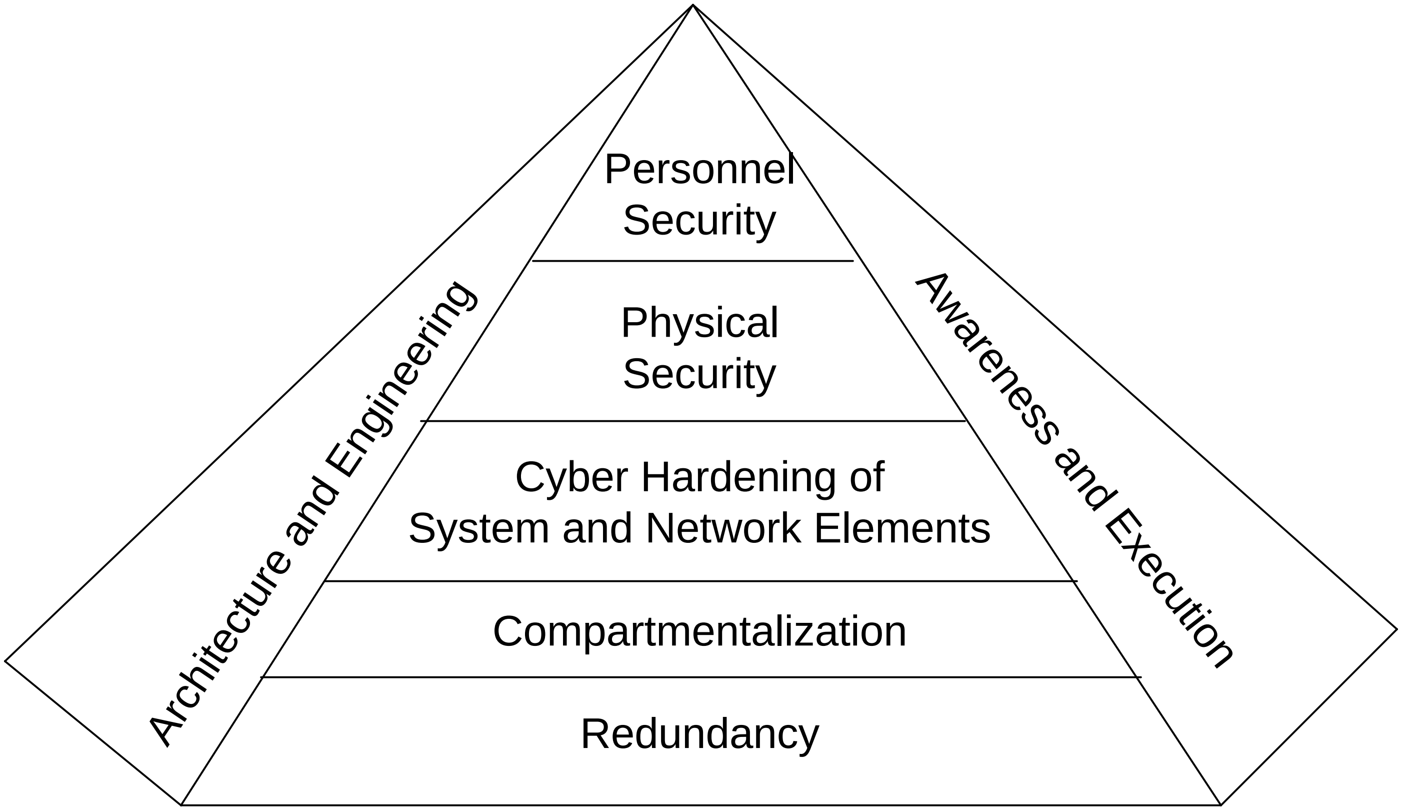
Network Access Controls;
Database security;
Peer-to-peer identification,
authentication & authorization.



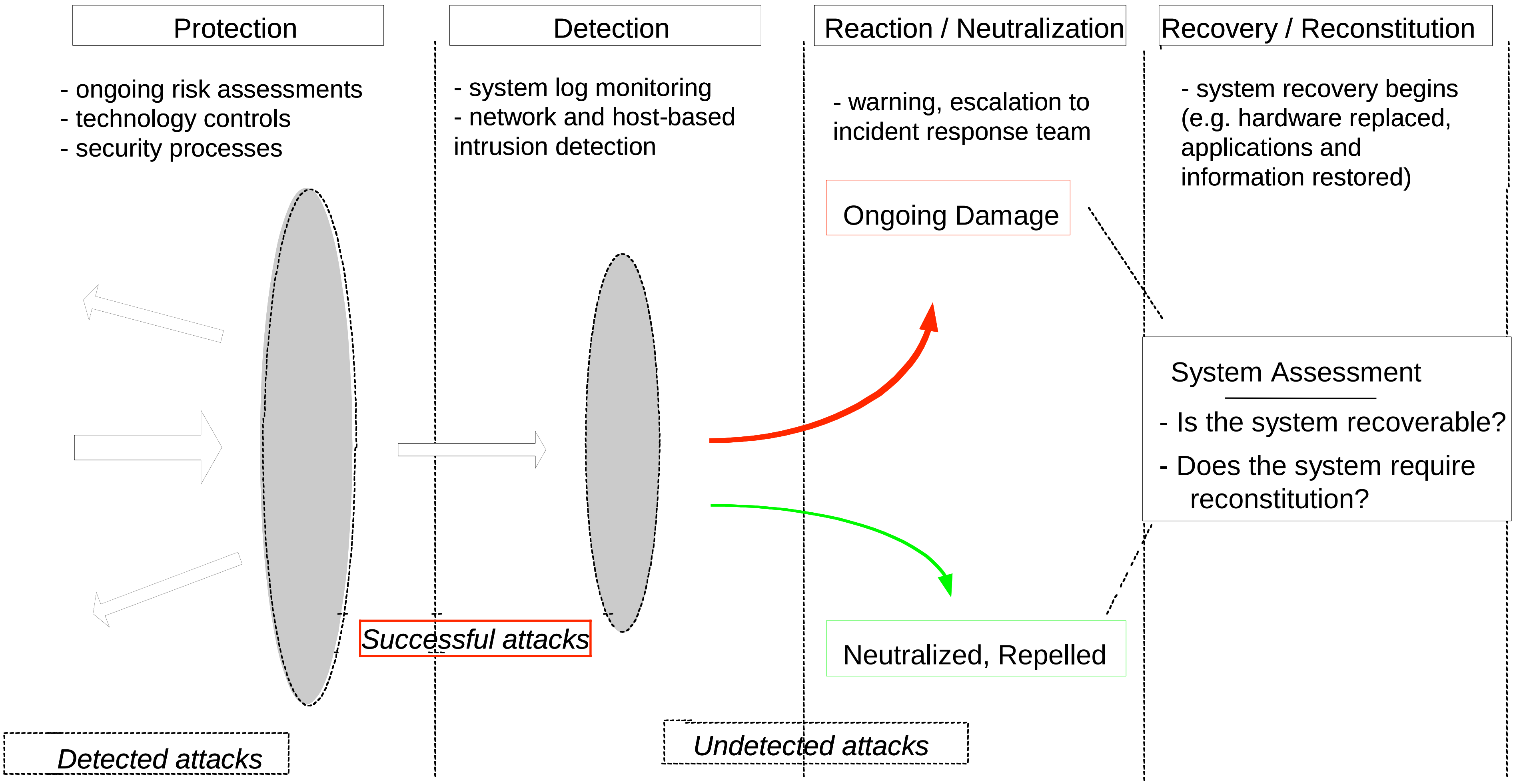
Device Security: "Internet Harden" O/S; Malicious Code Detection / Response; Code signing for mobile code; data-at-rest confidentiality, integrity and protection; human-to-machine identification and authorization; etc.

Application security: authentication; authorization (separation of duties with least privilege); protocol integrity protection; confidentiality; etc.

FAA’s Five Layers of System Protection



Control Life-Cycle



Protection

- ongoing risk assessments
- technology controls
- security processes

Detection

- system log monitoring
- network and host-based intrusion detection

Reaction / Neutralization

- warning, escalation to incident response team

Recovery / Reconstitution

- system recovery begins (e.g. hardware replaced, applications and information restored)

Ongoing Damage

System Assessment

- Is the system recoverable?
- Does the system require reconstitution?

Neutralized, Repelled

Successful attacks

Detected attacks

Undetected attacks

Presentation Outline

- **Overview**
  - **Trends**
  - **FAA LAN Phase 1 Study**
- **Security and Safety**
- **Initial Acceptance Criteria**
  - **Security Engineering**
    - **Vulnerabilities**
    - **Threats**
    - **Risks**
    - **Countermeasures**
- **Findings and Recommendations**
  - **Findings**
  - **Recommendations**

Phase 1 Findings (1/2)

1. **Safety and security are intertwined concepts in airborne networked environments.**
2. **Security models exist that are directly applicable for creating safe and secure networked systems. These models identify how elements that are classified at a given assurance level can interoperate together in specifically restricted and prescribed ways in order to create network systems that also function at a known classification level.**
3. **The DoD has based their security foundation and processes on the Bell LaPadula Confidentiality Model. We identify a similar model, the Biba Integrity Model, for airborne network safety and security.**
   - **The fact that DoD (confidentiality) classifications and FAA (safety) classification levels can be mapped and that the Bell-LaPadula and Biba models are analogs of each other, theoretically results in the DoD and FAA potentially sharing very similar processes, security engineering methodologies, deployment architecture approaches, and certification systems.**

Phase 1 Findings (2/2)

4. **Entities that are assured at a certain safety classification for stand alone system deployments should be re-certified for deployment into networked environments.**
5. **Software entities comprised of large numbers of lines of code necessarily pose certification challenges. Attempts to strengthen existing system security engineering (SSE) processes for network environments remain demonstrably inadequate for large software code bases. Therefore, assurance results for large software code base entities that are targeted for deployment within large network environments (e.g., networks that are directly or indirectly connected to the Internet) should not be trusted at this time.**
6. **COTS computer systems cannot be adequately secured within large network environments in the general case because their security controls cannot be trusted to perform as intended when attacked. These devices should not be deployed in higher DO-178B software level networks except via high assurance guards (HAGs).**
7. **Only devices that cannot be mis-configured or mismanaged should be certified at higher DO-178B software levels.**

Presentation Outline

- **Overview**
  - **Trends**
  - **FAA LAN Phase 1 Study**
- **Security and Safety**
- **Initial Acceptance Criteria**
  - **Security Engineering**
    - **Vulnerabilities**
    - **Threats**
    - **Risks**
    - **Countermeasures**
- **Findings and Recommendations**
  - **Findings**
  - **Recommendations**

Phase 1 Study Recommendations

1. **Devices operating at specific safety levels should be organized into specific logical network (i.e., virtual private network (VPN)) enclaves in a manner parallel to current DoD practice.**
2. **Network communications between devices within each safety enclave should use IPsec ESP in transport mode whenever performance requirements permit.**
3. **On-board aircraft network LAN implementations should deploy physical network protections to implement integrity enclave separation to physically isolate devices into networked enclaves on a need-to-communicate basis (e.g., AFDX deterministic Ethernet).**
4. **Airborne networked entities should be protected by defense in a depth security protection system that is operative within each network safety level enclave.**
5. **NAS and airborne network architecture should follow the NSA's IATF recommended best-practices. Airborne and NAS entities should also use compatible authentication systems.**
6. **NAS and airborne elements should be appropriately certified by means of established Common Criteria and DO-178B practices enhanced to address networked threats.**