BOEING

Engineering, Operations & Technology
Phantom Works

Safety and Security of Networked LANs in Aircraft

Summary of the FAA LAN Study
June 25, 2008

This work was supported by the Federal Aviation Administration, Aircraft Certification Service (AIR-1),
800 Independence Ave., S. W., Washington, DC 20591

Eric Fleischman
Boeing Phantom Works
Eric.Fleischman@boeing.com

FAA Study Contract High Level Orientation

- **FAA LAN Study: FAA Contract DTFACT-05-C-00003**
- **Two year study project (2005-2006)**
- **Study results are recommendations of the authors**
  - **-- not an official FAA position**
  - **-- not an official Boeing position**
- **Three primary project deliverables:**
  1. Eric Fleischman, Randy Smith, Nick Multari, "Networked Local Area Networks (LANs) in Aircraft: Safety, Security and Certification Issues, and Initial Acceptance Criteria (Phases 1 and 2)," DOT/FAA/AR-xx/xx, December 2006, 185 Pages
  2. Eric Fleischman, "Handbook for Networked Local Area Networks (LANs) in Aircraft", December, 2006, DOT/FAA/AR-xx/xx, 105 Pages
  3. Eric Fleischman, Randall E. Smith, Nick Multari, "Local Area Networks (LANs) in Aircraft, Phase 1 Report, including Safety and Security Issues and Acceptance Criteria", FAA LAN Study Phase 1 Final Report, DOT/FAA/AR-xx/xx, May 10, 2006, 146 Pages
- **Study presumed the use of Internet Protocols (IP) for networking in future NextGen- and SATS-like environments**

Partial Background to the Study

Civilian Aircraft environment is changing

- **Fly-by-wire aircraft (B787, A350, A380) – electrical components and software performing avionics functions that traditionally were done by hydraulics and other analog systems**
  - **E.g., Airbus A380 avionics reportedly comprised of 1400 software modules consisting of over a billion lines of code**

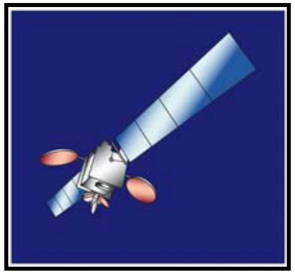
- **Airborne software is increasingly using internal LANs for reduced size, weight, and power (SWAP) footprint**

- **Emerging air-to-air and air-to-ground interactions and algorithms postulate having airborne aircraft systems become connected to the National Airspace System (NAS) ground infrastructure**
  - **NCO operations, e.g., next generation aircraft warning systems combining map and air traffic data, terrain info, weather radar returns, info on man-made obstacles, and imagery on the airport environment**
  - **Algorithm change to decrease aircraft separation in final approach from an average of 4 nautical miles to 3 nautical miles to increase airport capacity 25%**
  - **Automated aircraft maintenance processes and systems**
  - **NASA's Small Aircraft Transportation System (SATS) to enable small aircraft to fly to/from 5400 small airports that are not currently used for public transportation.**

- **NASA's Next Generation Air Transportation System (NextGen) Air Traffic Management (ATM)-Airspace**

Background: NextGen Transformational Framework (2025)

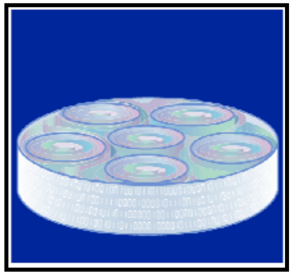
Precision flight anywhere



Enhanced Services

Information Infrastructure

System Wide Information Management



Precision common awareness

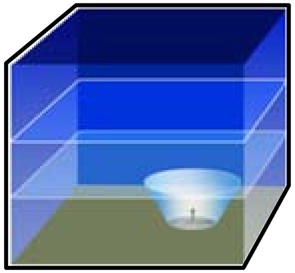
Enables

Capacity, Safety & Efficiency

Enhanced Situational Awareness

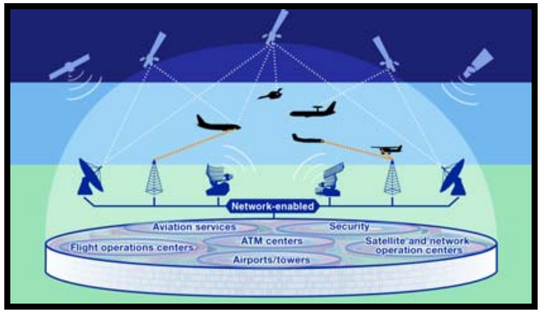
Network Enabled Operations

Dynamic Seamless Airspace



Agility, Security & Economy

Create



Transformed Global Air Traffic System

- ***3X+ airport capacity***
- ***Environmental benefits***
- ***Global interoperability***
- ***Accident reduction***
- ***Threat deterrence***

Background: Today (2008) and NextGen (2025)

Currently	Possible NextGen Future (2025)
Multiple, disjoint air-to-ground communications systems: • **Multiple voice-only links (e.g., VHF, HF, LBand SATCOM)** • **ACARS – teletype-like data only**	**Integrated Air-to-Ground comms supporting both voice and data using a new IPv6 variant of Aeronautical Telecommunications Network (ATN) – Internet Technology**
Today's ATM system is comprised of stand-alone elements that were largely designed in the 1960s	**An integrated ATM system capable of point to point operations to any runway, in any weather, at any time**
Serves Commercial Aviation and (conditionally) Military & Civil Aviation	**Serves Military Aviation, Commercial Aviation, Civil Aviation, and UAVs**
Active Gen Aviation Aircraft: 26,023,000 **Passenger Aircraft: 2,792** **Aircraft using FAA's Air Route Traffic Centers: 48,451,500** **Aircraft Hours flown: 9,862,000**	**Active Gen Av. Aircraft (2020):39,426,000** **Passenger Aircraft (2020): 3,694** **Aircraft using FAA's Air Route Traffic Centers (2020): 65,424,300** **Total Aircraft hours (2020): 19,635,000**

ATM = Air Traffic Management
ACARS = Aircraft Communications Addressing and Reporting System Protocol
Partial source: http://www.faa.gov/data_statistics/aviation/aerospace_forecasts/2007-2020/

Background: Current (or Soon) Data Link Media

	VHF	HF	SATCOM	Broadband SATCOM	Gatelink
Bit Rate	2.4 kbps (ACARS) 31.5 kbps (VDLM2)	1.8 kbps	0.6-10.5 kbps	432 kbps to 10-40 Mbps	384 kbps to 54 Mbps
Coverage	Continental	Continental Oceanic Polar	Continental Oceanic	Continental Oceanic	On ground (airports)

ACARS = Aircraft Communications Addressing and Reporting System
VDLM2 = VHF Digital Link Mode 2

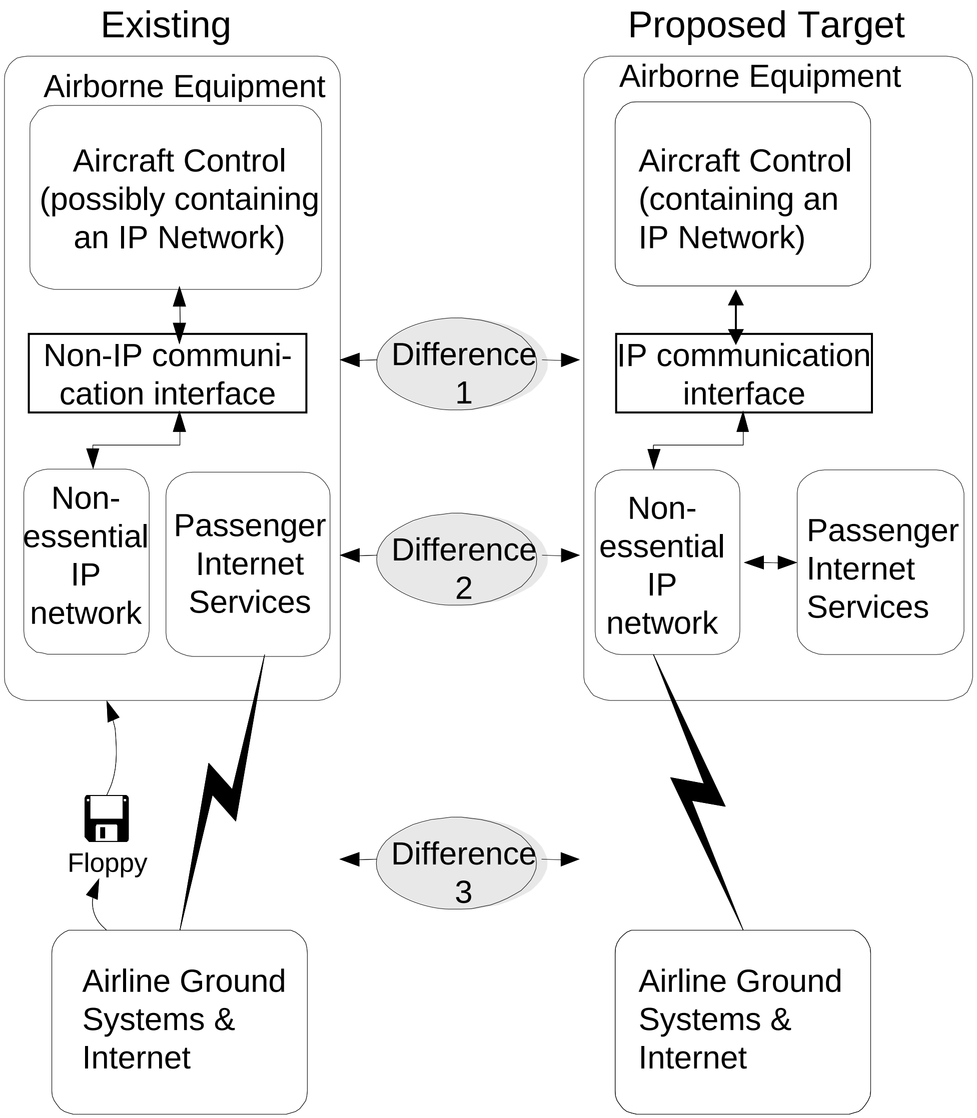
Context: Evaluate aircraft joining the world NCO migration

- **"We're poised to put air-traffic control, banking, military command-and-control, electronic medical records, and other vital systems into the hands of a profoundly insecure, untrustworthy platform cobbled together from complex legacy software components."**

-- Ken Birman, "The Untrustworthy Web Services Revolution,"
IEEE Computer Magazine, February 2006, pages 98 – 100

NCO = Network Centric Operations

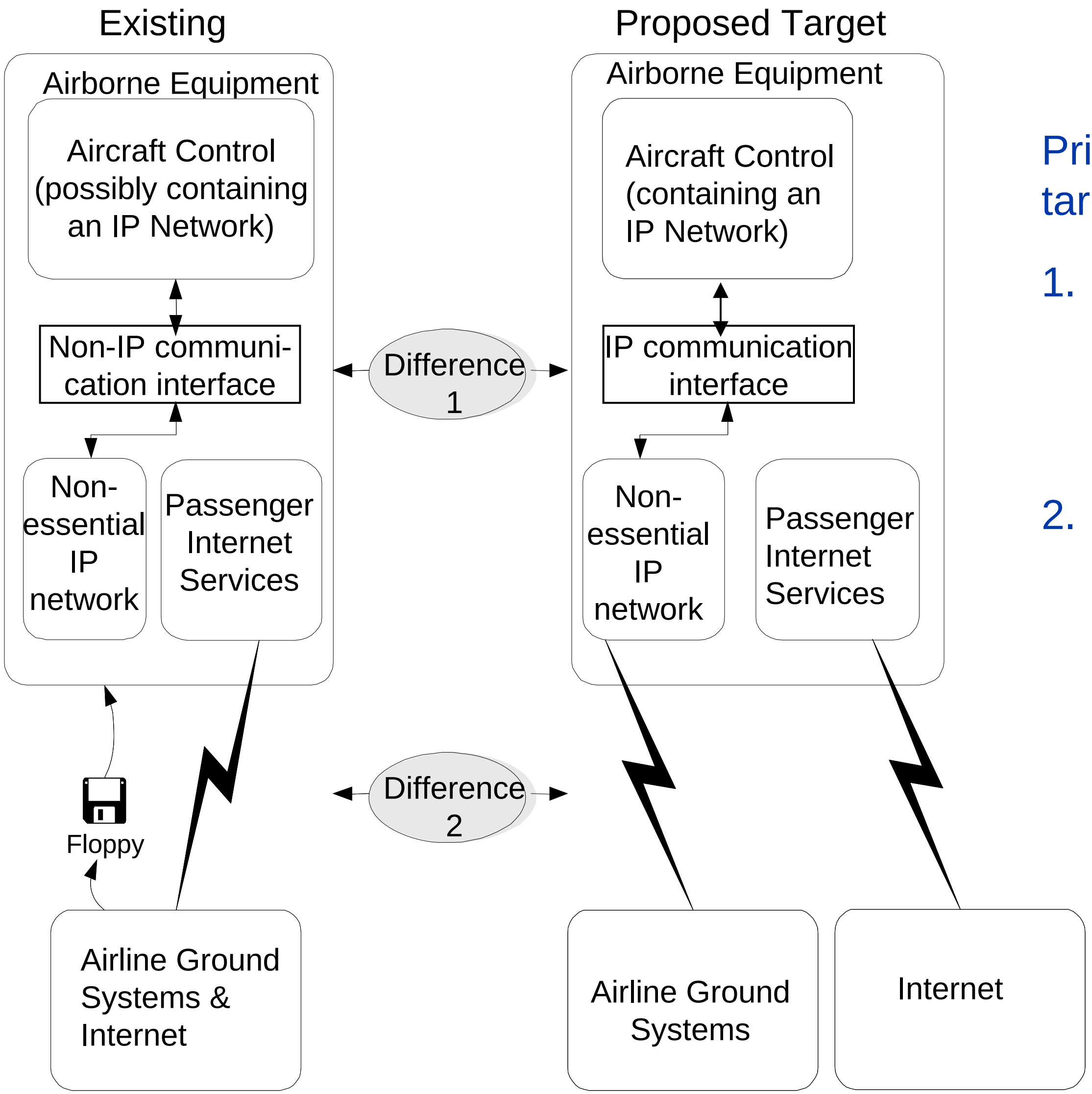
A Proposed Target Architecture – Evaluative Domain


Existing
Proposed Target
Airborne Equipment
Aircraft Control (possibly containing an IP Network)
Non-IP communi-cation interface
Non-essential IP network
Passenger Internet Services
Floppy
Airline Ground Systems & Internet
Difference 1
Difference 2
Difference 3
Airborne Equipment
Aircraft Control (containing an IP Network)
IP communication interface
Non-essential IP network
Passenger Internet Services
Airline Ground Systems & Internet

Primary differences in proposed target environment:

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 NAS ground computers and, potentially, other aircraft.

Alternative Target Architecture


Existing
Airborne Equipment
Aircraft Control (possibly containing an IP Network)
Non-IP communi-cation interface
Non-essential IP network
Passenger Internet Services
Floppy
Airline Ground Systems & Internet
Difference 1
Difference 2
Proposed Target
Airborne Equipment
Aircraft Control (containing an IP Network)
IP communication interface
Non-essential IP network
Passenger Internet Services
Airline Ground Systems
Internet

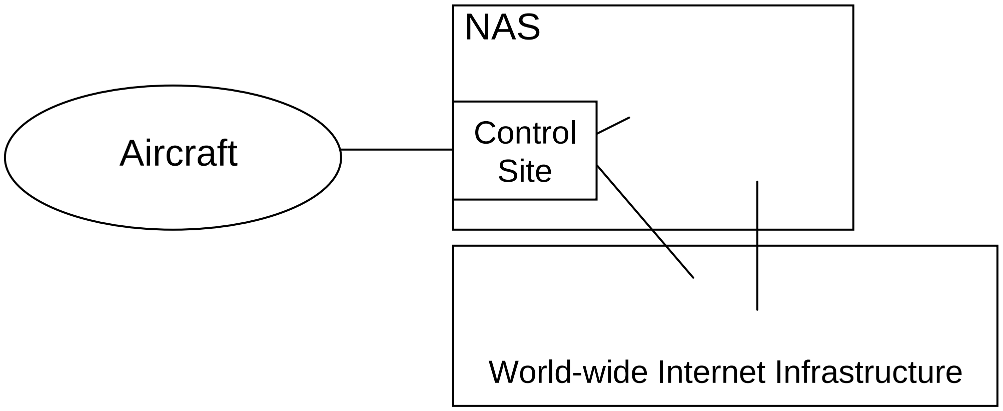
Primary differences in proposed target environment:

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 NAS ground computers by using an IP-based air-to-ground link.

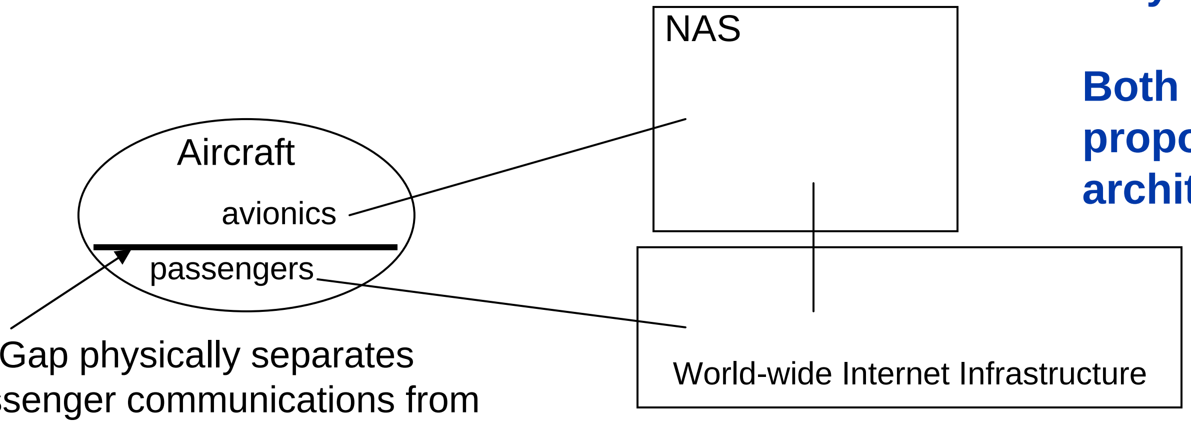
Note: the air gap between the aircraft passengers and the avionics systems remains in tact.

Terse commentary on target architecture differences



No Air Gap in Aircraft Alternative (Proposed Target)

Air Gap in Aircraft Alternative (Alternative Target)



Air Gap physically separates passenger communications from avionics/crew communications

Both target approaches are exposed to Internet-based threats.

Bottom approach is somewhat more secure than the first (i.e., can close the Port 80 (HTTP) overt channel within the firewall), but has greater size, weight, and power (SWAP) requirements.

Risk mitigation controls are very similar for both targets.

Both targets use the same proposed target network architecture design.

NAS = National Airspace System

Background: Regulatory Foundation is Safety Oriented

- **Current FAA safety assurance processes for airborne systems are based on ARP 4754, ARP 4761, and Advisory Circulars (e.g., AC 25.1309-1A, AC 23.1309-1C).**

Airborne Software Assurance Processes:

- **FAA software assurance is based on compliance with RTCA/DO-178B (DO-178B) that guides *software development processes*.**
- **ARP 4754 extends the DO-178B software assurance process to address the additional safety issues that arise when software is embedded into highly integrated or complex airborne system relationships.**
  - **Note: The word "security" does not occur within ARP 4754, which is a partial motivation for this study project.**

ARP 4754: Certification Considerations for Highly-Integrated or Complex Aircraft Systems, 1996

ARP 4761: Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, 1996

AC 25.1309-1A: Equipment, systems and installations, Title 14 (Aeronautics and Space), Chapter I (Federal Aviation Administration), Part 25 (Airworthiness standards: transport category airplanes), Section 1309 (Equipment, systems, and installation), Revised Jan 1, 2006

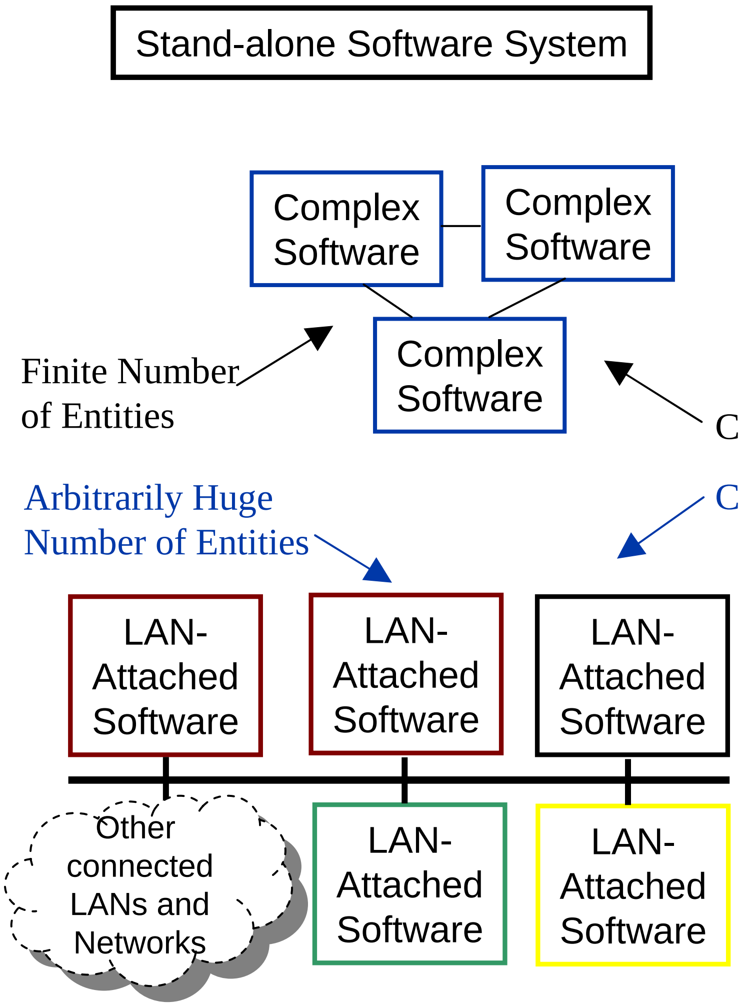
AC 23.1309-1C: Equipment, systems and installations, Title 14 (Aeronautics and Space), Chapter I (Federal Aviation Administration), Part 23 (Airworthiness standards: normal, utility, acrobatic, and commuter category airplanes), Section 1309 (Equipment, systems, and installation), Revised Jan 1, 2006

Background: (Safety-based) Software Level Definitions

DO-178B and other Civil Aviation documents address safety requirements in terms of software level definitions.

Failure Condition Categorization	Software Level Definitions
Catastrophic – failure conditions which would prevent continued safe flight and landing	**Level A** – anomalous behavior … contributes to a failure of a system function resulting in a catastrophic failure condition for the aircraft
Hazardous/Severe – Major – Failure conditions … reduce the capability of the aircraft … [resulting in] a large reduction in safety margins	**Level B** – anomalous behavior …results in hazardous/severe failure condition …
Major – Failure conditions …reduce the capability of the aircraft …[resulting in] a significant reduction in safety margins …	**Level C** -- anomalous behavior … results in major failure condition …
Minor – Failure conditions would not significantly reduce aircraft safety…	**Level D** -- anomalous behavior … results in minor failure condition …
No effect – Failure conditions would not affect the operational capability of the aircraft or increase crew workload	**Level E** – failure conditions …do not affect the operational capability …

Three Different Certification Environments

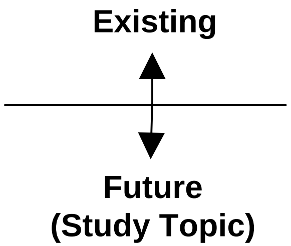


1) Stand alone software system:
Focuses on that software entity (**DO-178B**)

2) Integrated or Complex Systems:
Addresses each software Item (**DO-178B**) as well as the potentially complex affects resulting from their integration together (**ARP 4754**).

Concerned with effective integration techniques

Concerned with fate sharing in a hostile environment



3) Networked Airborne LANs:
A complex system in which every entity in the same network (i.e. the LAN and whatever the LAN directly or indirectly connects to) is inadvertently integrated together, regardless of the functional intent of the system design.

Processes must now also address possible network interactions during (and resulting from) **network attacks**.

Fate sharing: any compromised network entity can theoretically be used to attack other networked entities or their shared network environment.

FAA LAN Study - Identified risks (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
  2. the increased possibility of (human or device) hostile attackers being present within the system.
     - – There are currently more than 1 billion humans connected to the Internet
  - Target NCO networks include both airborne and ground elements.
- Due to the emergence of client-side attacks, the (human) **end users of networked resources are now an integral part of that network's total security defense posture**.
- **Entities** within networks that are directly or **indirectly** connected to the Internet **may be accessible by attackers located elsewhere in the Internet, despite the presence of intervening security firewalls**.
  - Three common vectors for circumventing firewall protections:
    - ➢ Firewall Policy – e.g., Port 80 (HTTP) overt channel through firewalls
    - ➢ Advanced attack techniques (e.g., time based or fragmentation attacks)
    - ➢ Back doors into the network (e.g., modems)

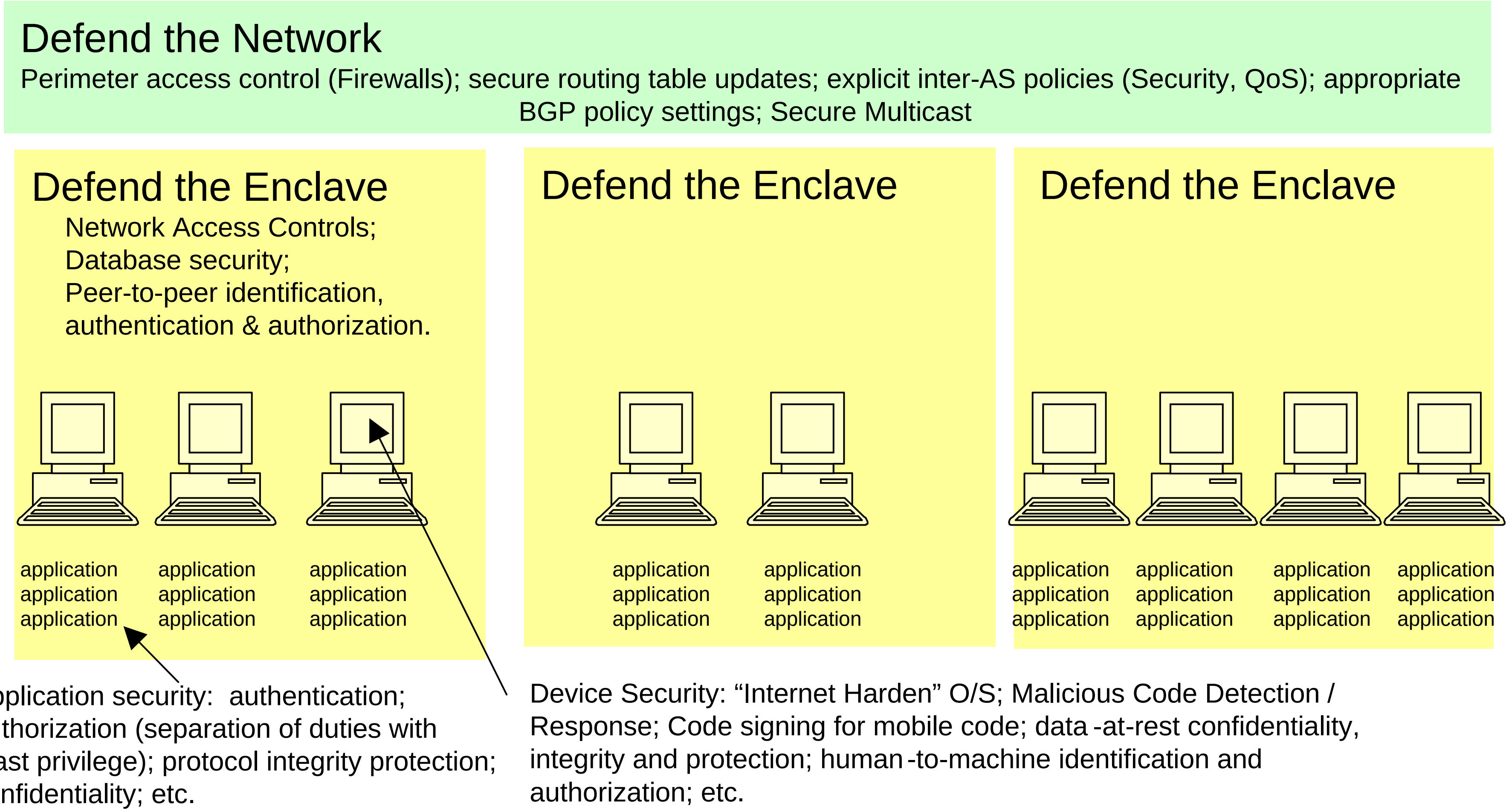
    Therefore, airborne networks need to deploy defense-in-depth network access protections to "back up" firewalls (i.e., VPNs)

FAA LAN Study - Identified risks (2/2)

- Most software systems have an indeterminate number of latent bugs that can be attacked.
- 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.
  - See the NSA's: "The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments" http://www.nsa.gov/selinux/papers/inevit-abs.cfm
- 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 deployed 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.

Address Risks with IA Defense in Depth Provisions

Information Assurance (IA) best common practice is described in “Information Assurance Technical Framework” (IATF), NSA, September 2002
http://www.iatf.net/framework_docs/version-3_1/index.cfm



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.

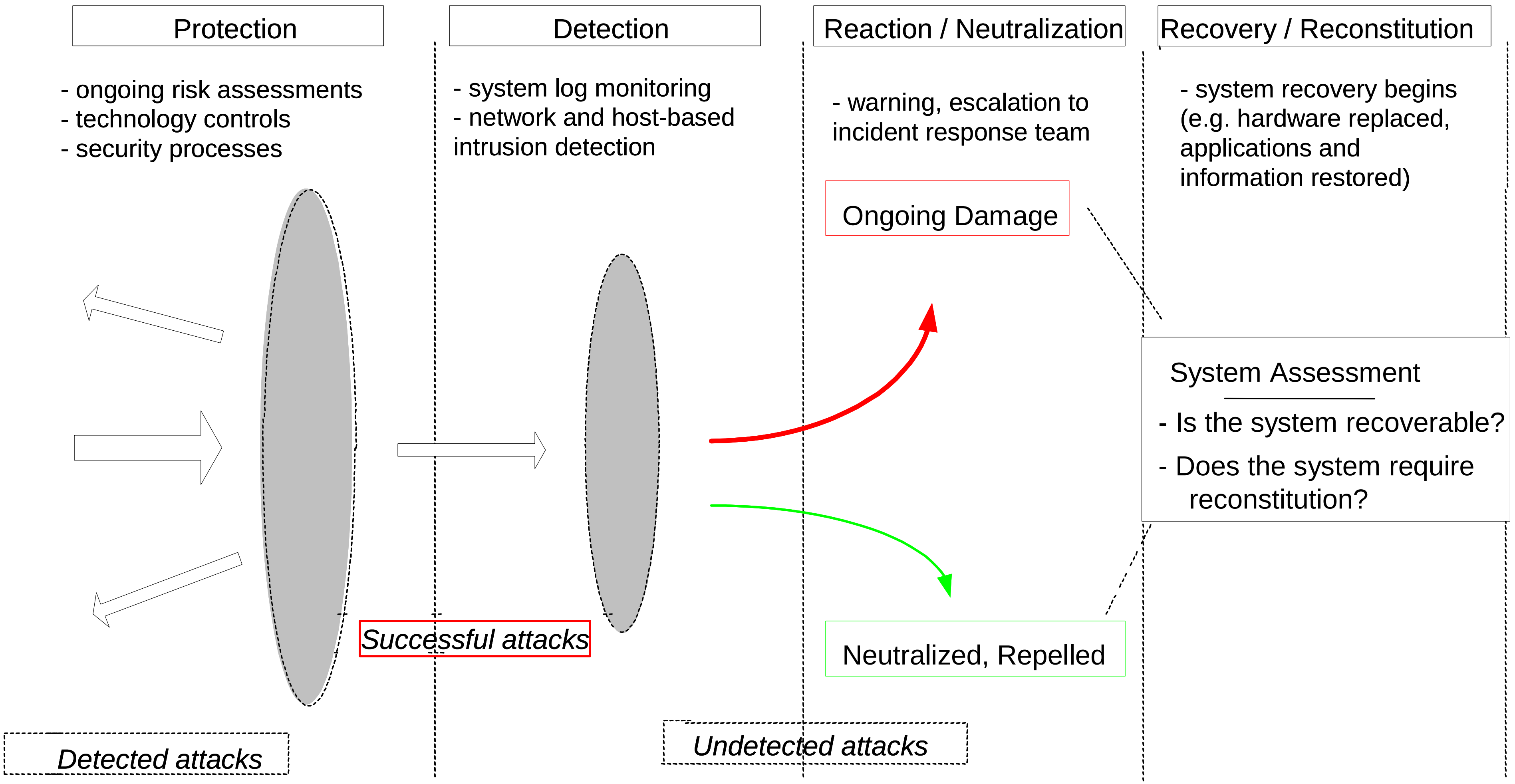
Defend the Enclave

Defend the Enclave

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

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.

Full 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

Security Controls Needed for Network Airborne Safety

Protocols and Entities (e.g., Software Items)

- **Integrity of communications protocols**
- **Integrity and Availability of the physical network (e.g., LAN, router)**
- **Integrity and Availability of applications supporting airborne operations**
- **Integrity and Availability of security controls that are used for defense-in-depth protections (e.g., firewall, packet filter)**
- **Authentication within communications protocols to discern spoofed versus real communications**
- **Applications shall ensure that their users (both processes and humans) are Authenticated**

Management & Administration

- **Authentication, Authorization, and Non-repudiation of all administrative & management actions upon networked devices and systems**
- **Integrity and Non-repudiation of airborne software**

Key Observations of the Study (1 of 2)

- **The primary issue impacting the safety of airborne networks is how to extend existing ARP 4754, ARP 4761, DO-178B, and DO-254 assurance processes into networked systems in a mathematically viable manner (i.e., must not be *ad hoc*)**
- **Recommend that current FAA orders, guidance, and processes ("safety policies") be mapped into the Biba Integrity Model framework to create a safety-oriented security system.**
  - **Parallel to the US Federal security system (e.g., US DoD), which is created by mapping Federal information classification law and policies into the Bell-LaPadula confidentiality model framework.**
  - **Both the Bell-LaPadula and Biba models are security models.**
  - **"A security model maps the abstract goals of the policy into information system terms by specifying explicit data structures and techniques necessary to enforce the security policy. A security model is usually represented in mathematics and analytical ideas …"**

--All in One CISSP Certification Exam Guide by Shon Harris page 240

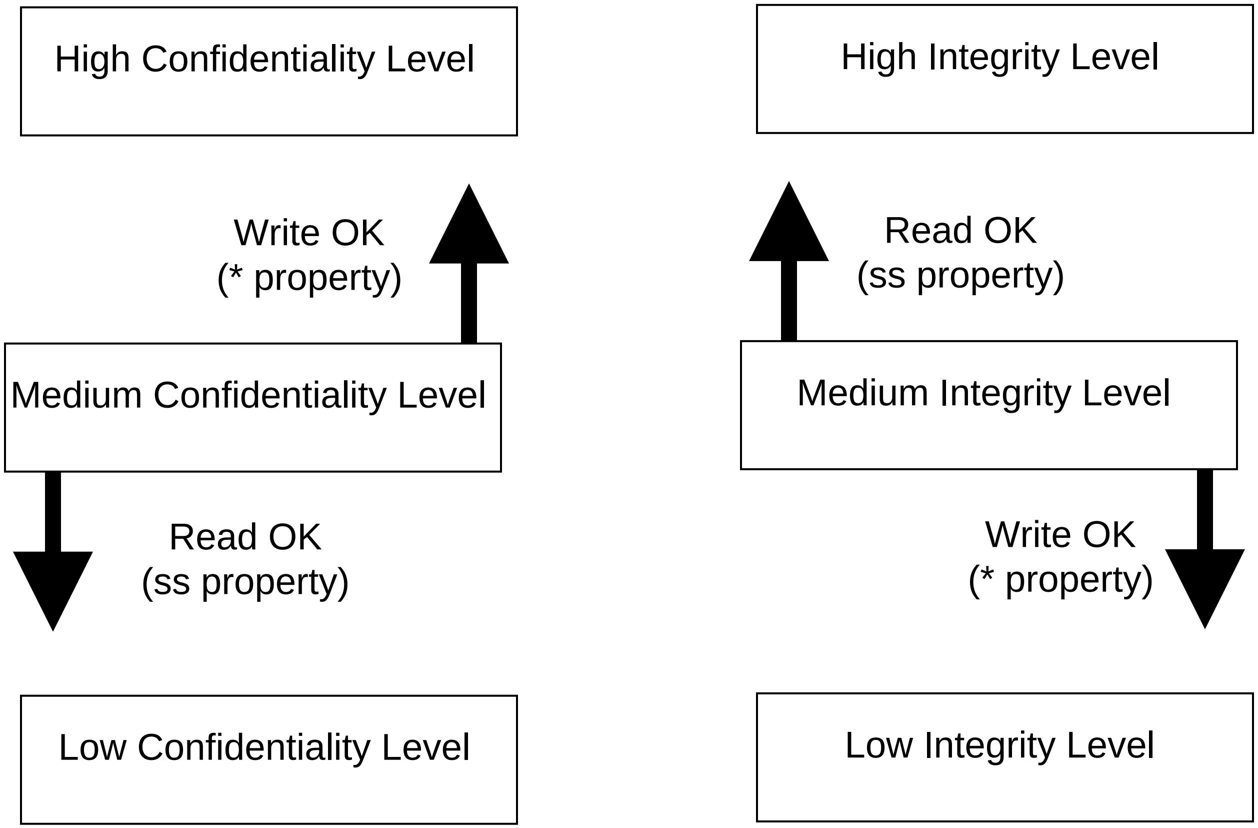
Background: Bell-LaPadula and Biba Models

Bell-LaPadula and Biba Models are both informational flow models enabling multilevel security systems.

Bell-LaPadula model addresses confidentiality; Biba model addresses integrity.

Bell-LaPadula Confidentiality Model

Biba Integrity Model



High Confidentiality Level

Write OK
(* property)

Medium Confidentiality Level

Read OK
(ss property)

Low Confidentiality Level

High Integrity Level

Read OK
(ss property)

Medium Integrity Level

Write OK
(* property)

Low Integrity Level

Background: Models that Establish Network System Assurance Levels

Theoretical Models exist to determine the assurance level of networks.

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

DoD Security (Confidentiality): Bell LaPadula Model

Used by the DoD

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.

Appropriate for Safety

DO-178B Safety: Biba Integrity Model (proposed)

Theoretical model recommended for the FAA by this study.

Level A
Level B
Level C
Level D
Level E

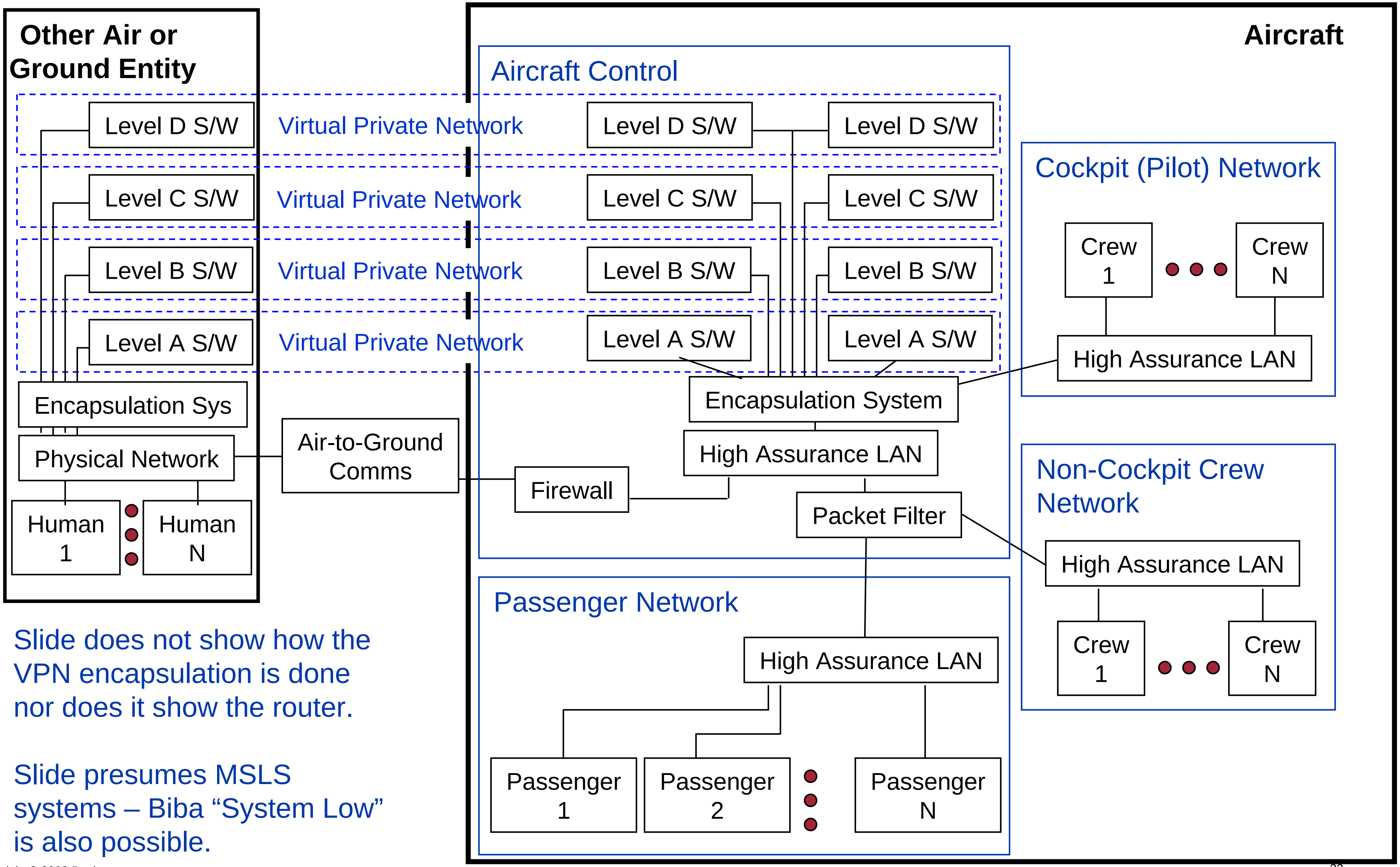
- Higher level info & processes can be written to (included within) lower level.
- Lower level info can see higher level info.

Key Observations of the Study (2 of 2)

- **This study defined an exemplar airborne network architecture by identifying a minimal set of security controls necessary to generically implement FAA software "safety policies" in terms of the Biba model framework.**
- **Mechanism used to derive Exemplar Architecture:**
  1. **Map current DO-178B and ARP 4754 processes into the Biba Integrity Model Framework**
  2. **Mapping done by using well-established System Security Engineering (SSE) processes to define a set of derived airborne safety requirements (see slide after next).**
  3. **Apply best current Information Assurance processes (e.g., NSA's IATF) upon those derived airborne safety requirements to define a generic exemplar airborne network architecture (see next slide).**

Note: The SSE process (see http://www.software.org) assumes the requirements are for a specific deployment. By contrast, our requirements are the derived airborne safety requirements. Therefore, our results indicate a minimum set of the generic security controls needed to satisfy the FAA software "safety policies". Our results are not a specific deployment architecture. Deployments may have additional requirements (and additional controls) to our generic Exemplar Architecture.

Exemplar Airborne Network (Safety-oriented) Architecture



Slide does not show how the VPN encapsulation is done nor does it show the router.

Slide presumes MSLS systems – Biba “System Low” is also possible.

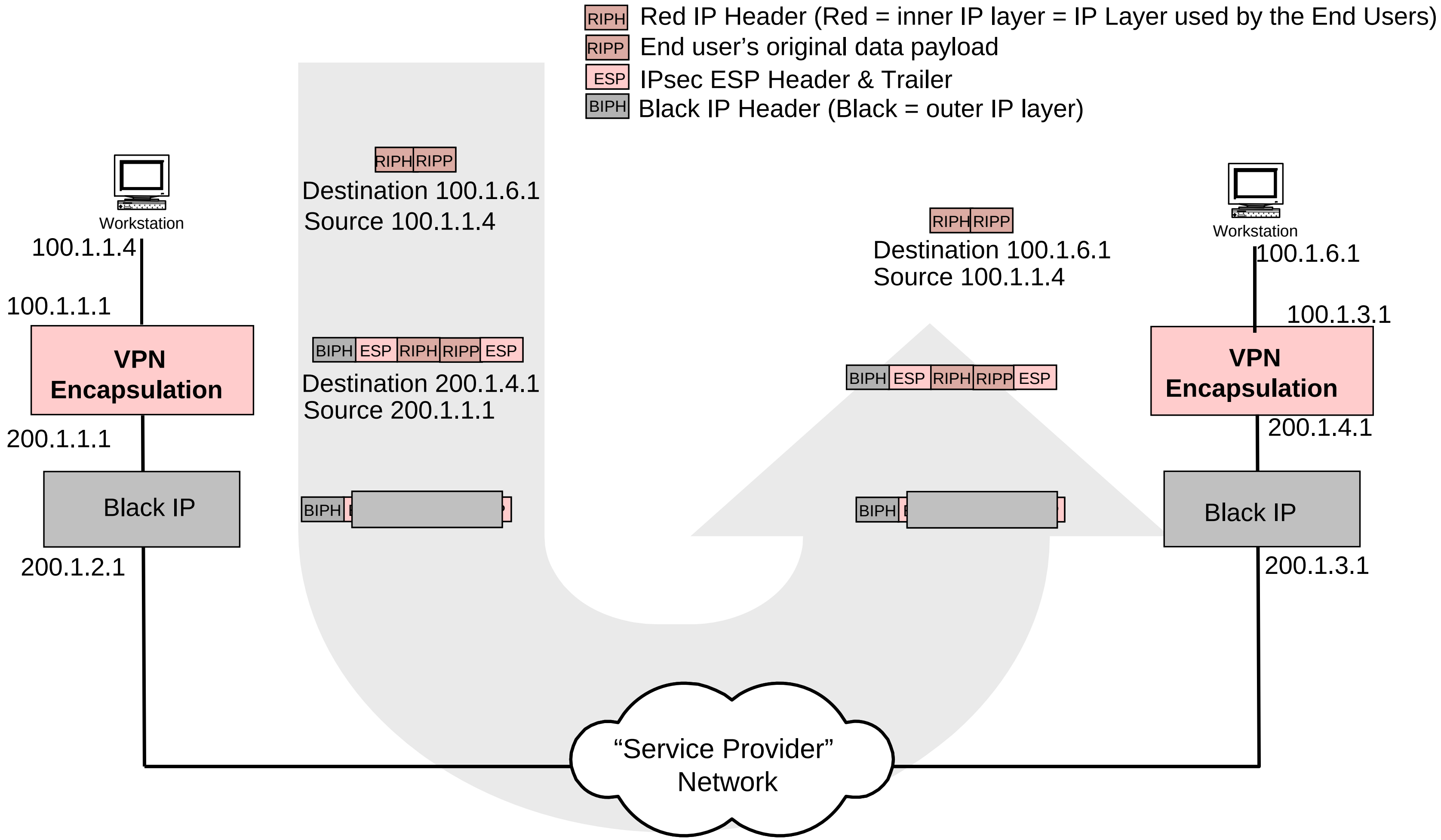
Derived Airborne Safety Requirements

1. **Network systems and software entities are classified at specific safety levels. Those with safety affects are partitioned via VPNs (see next slide).**
2. **Entities without safety affects (Level E) need not be partitioned by VPNs.**
3. **Physical network media and devices must be assured at the same assurance level as the highest software level entity they support.**
4. **Entities that are located outside of the aircraft that directly or indirectly communicate with aircraft entities are similarly treated in accordance with Rules 1 and 2.**
5. **The physical network system elements that connect aircraft to other aircraft or ground systems must comply with Rule 3.**
6. **If software systems exclusively communicate in a tight relationship within a select group, then that community can form a “system low” network that includes multiple safety levels (e.g., equivalent to DoD “system high” concept; e.g., some Integrated Modular Avionics (IMA) systems)**
7. **Entities having real-time, latency-sensitive, or high availability requirements may need to receive dedicated physical links**
8. **Apply Biba high assurance guards (HAGs) to handle exceptions to any of the above rules.**

Background: Mechanism for ARP 4754 Partitions within Networks

- Virtual Private Networks (VPNs) are a widely used technique to partition (in accordance with ARP 4754 Section 5.4.1.1) networked systems.
  - VPNs enable the creation of a networked system having partitions that can operate at specific assurance levels. Each partitioned "enclave" can operate at a potentially different assurance level than either the underlying physical network itself (e.g., the LAN) or the other VPNs (including their Items) also supported by that physical network.
  - Examples of a VPN-partitioned network:
    - DoD's Global Information Grid (GIG) network architecture
    - Internet Service Provider (ISP)-provided VPN services (IETF L3VPN; e.g., see http://www.ietf.org/html.charters/l3vpn-charter.html)

IPv4 Example of VPN Encapsulation Protocol Behavior



RIPH Red IP Header (Red = inner IP layer = IP Layer used by the End Users)

RIPP End user's original data payload

ESP IPsec ESP Header & Trailer

BIPH Black IP Header (Black = outer IP layer)

Workstation

100.1.1.4

100.1.1.1

VPN Encapsulation

200.1.1.1

Black IP

200.1.2.1

RIPH RIPP

Destination 100.1.6.1
Source 100.1.1.4

BIPH ESP RIPH RIPP ESP

Destination 200.1.4.1
Source 200.1.1.1

BIPH

"Service Provider" Network

BIPH

BIPH ESP RIPH RIPP ESP

RIPH RIPP

Destination 100.1.6.1
Source 100.1.1.4

Workstation

100.1.6.1

100.1.3.1

VPN Encapsulation

200.1.4.1

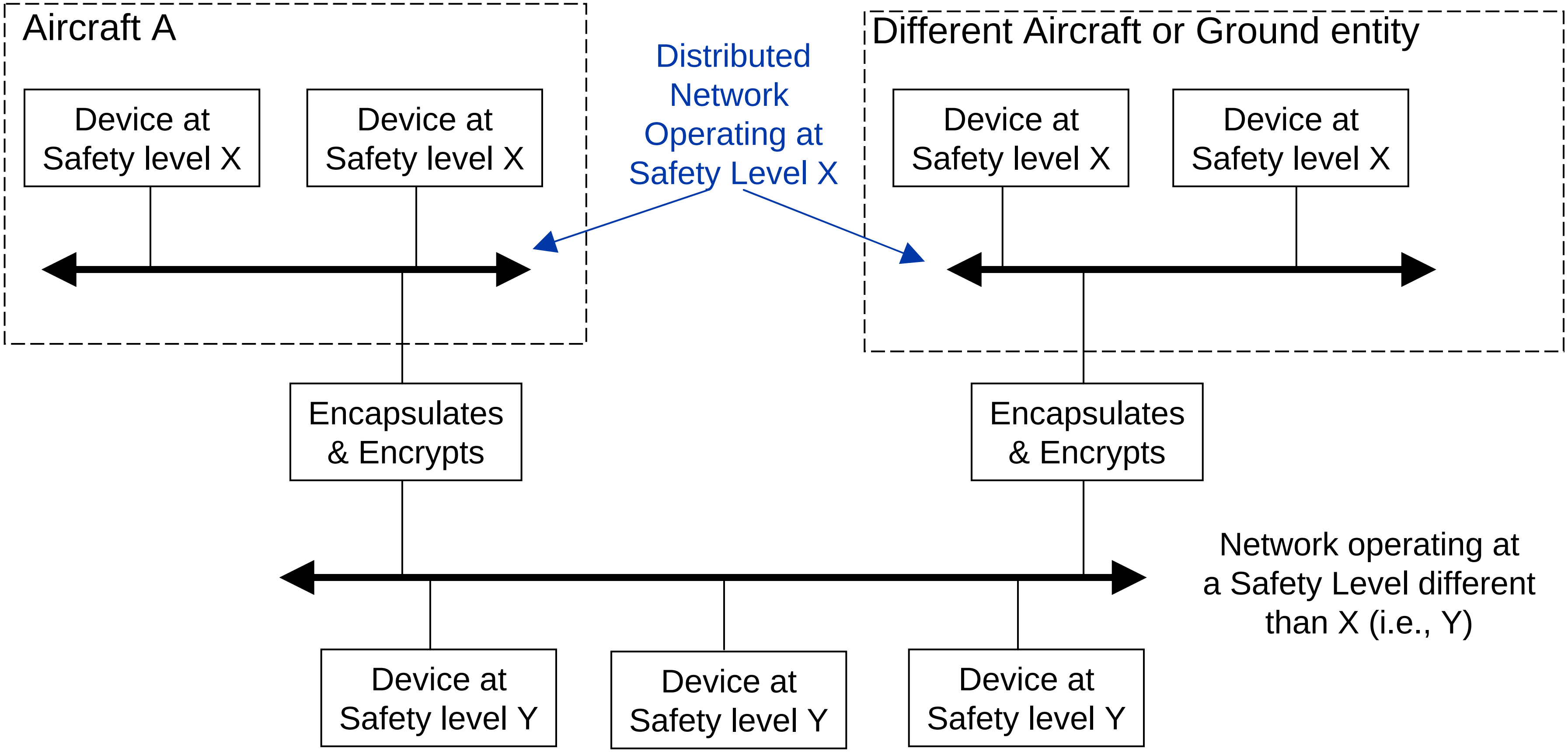
Black IP

200.1.3.1

Examples: Internet Service Providers (ISPs); IETF's IPsec's ESP in tunnel mode; IETF's L3VPN

Distributed Networks using the Biba Model

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

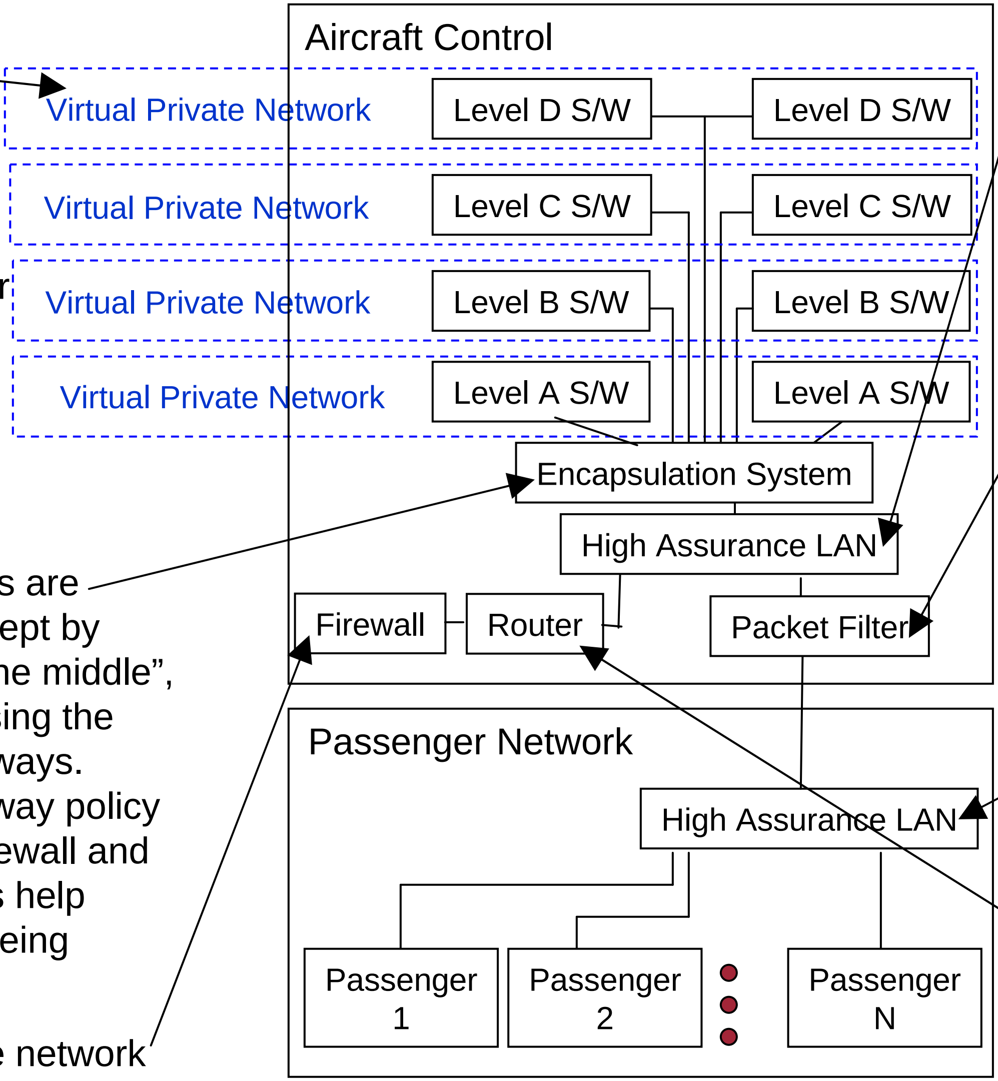


Threats and their mitigation

Securely Limits Threat Environment: Controls population that can access this Network to that VPN population only. Other VPNs have different address and name spaces. Each VPN securely partitions the network.

VPNs and their Items are difficult to attack except by inserting a “man in the middle”, including compromising the Encapsulation Gateways. Encapsulating Gateway policy together with the Firewall and Packet Filter policies help protect VPNs from being vulnerable to attack.

Provides Airplane network perimeter defense.



Ideally needs virtual link capability to provide physical layer connectivity that duplicates the VPN Connectivity limitations for Defense in Depth protection.

QoS and network assurance that passengers can’t DoS Aircraft LAN nor can they address or access any aircraft control element.

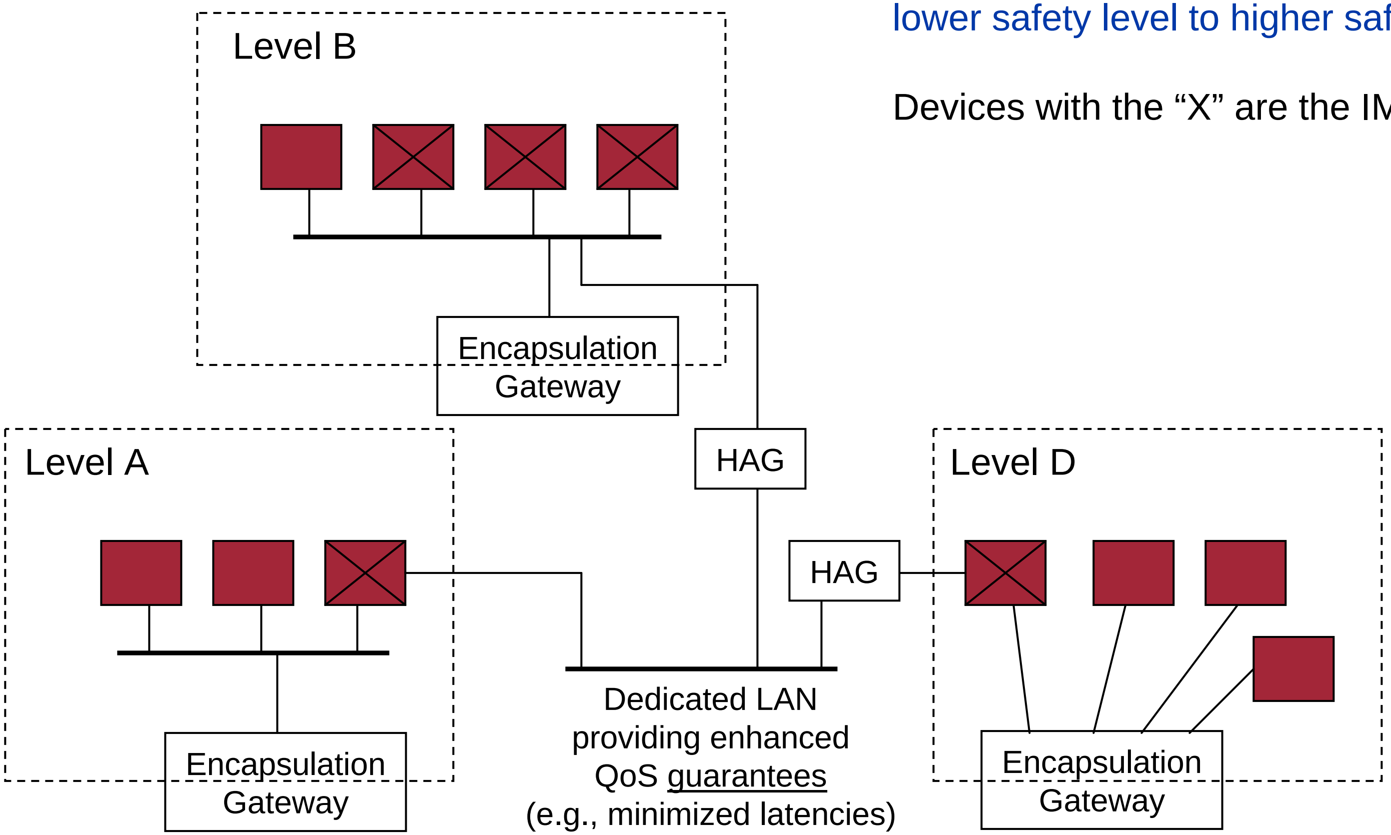
Separate LAN for passengers so can’t bypass the packet filter.

Configured so that only network management or IDS devices can send packets having the router as the IP destination address.

Threats and their mitigation -- continued

Larger the network, the larger the number of threats -- Indirect Internet connectivity means 1B+ potential users	**• VPN for network partitioning • Firewall for network perimeter defense • IPsec required for protocol security**
End users are now part of Security framework	**• VPN for network partitioning • Packet filter keeps passengers from accessing inappropriate Items and LANs**
Availability of Airborne LAN	**• Firewall and Packet Filter to control access • QoS policies ensure support for VPN traffic**
Integrity of Computers, Networks, Applications, and Data	**• VPN for network partitioning • Firewall and Packet filter for LAN defense • IPsec for secure protocol interactions • Assurance: DO-178B, ARP 4754, DO-254, CC**
COTS device security questionable (e.g., routers, PCs) and subject to compromise	**• IATF Defense in Depth Security Controls • Increase CC Assurance when relied upon • Only attached to VPN via HAG**
Complex Internet Protocol Family Security	**Use available IETF protocols' security alternatives and IPsec whenever possible**
SNMPv3 security issues	**• Always use IPsec with SNMPv3 • Once secure SNMPv3 (i.e., ISMS) alternative available, preferentially use it.**

Example: An Integrated Modular Avionics (IMA) Implementation



High Assurance Guards (HAGs) are uni-directional: Only needed from lower safety level to higher safety level.

Devices with the "X" are the IMA devices.

Implications of FAA LAN Study upon Avionics Software

- **Need non-reputable mechanism for establishing the identity of each network-attached entity – both onboard and on the ground**
- **Need a reliable mechanism for quickly verifying the integrity of each LAN-attached entity (during flight and on the ground)**
  - **e.g., Tripwire-like mechanisms (http://sourceforge.net/projects/tripwire/)**
- **Need an effective mechanism for system reconstitution should the integrity of major systems become damaged (during flight??)**
- **Need a reliable software management system that includes software integrity protection from software creation or update through secure storage through secure distribution within the aircraft**
  - **Leverage the Federal Digital Signature Standard (FIPS Publication 186) for authentication and integrity provisions throughout software life-cycle**
- **Need security controls and security partitioning (defense in depth)**
- **Security designs need to anticipate and address (and mitigate) evolving systems interactions stemming from Network Centric Operation changes within the national airspace system that may result in future air-to-air and air-to-ground interactions.**
- **Need to address how aircraft will survive worst case scenarios (e.g., a country destroys important communications satellites and initiates conventional and electronic warfare against all assets of another country, including its civil aircraft).**

High Assurance Software Certification Dilemma

- **High assurance software is trusted to behave in the same manner before, during, and after attacks.**
- **Current security theory has no viable mechanism for ensuring that software does not have latent bugs that cannot be exploited by attackers.**
  - **Certification processes increasingly seek to address this problem by subjecting software to test suites. Unfortunately, testing cannot provide assurance guarantees.**
    - Tests can only identify problems examined by the test suite and not the absence of untested problems.
    - A vast and unknown number of possible problems can theoretically exist – cannot test for them all.
  - **Higher assurance software processes also rely on formal methods and a line-by-line code inspection.**
    - **Detailed code inspections are only trustworthy for small code bases**

Issue: Safety Assurance Level for Security Controls

- **Need a mechanism to establish the integrity of security controls so that they can be evaluated in terms of our proposed Safety System.**
  - **The Exemplar Network Architecture relies upon Security Controls (e.g., Firewall, Packet Filter, Router, (VPN) Encapsulation Gateway, High Assurance Guards) to provide security protections to the networked system.**
  - **Study proposes that airborne networks operate at specific Biba integrity levels established in terms of (DO-178B) Safety Levels. Therefore, the integrity assurance of a security control needs to become correlated with an appropriate DO-178B safety level.**
- **Carol Taylor, Jim Alves-Foss and Bob Rinker of the University of Idaho have studied the issue of dual software certification: certifying software in terms of Common Criteria (CC) properties for security and DO-178B properties for Safety.**
  - **One of their articles suggests that security functionality certified at EAL5 can be compared with DO-178B.**
    - **U of Idaho didn't state the level. We thought they implied Level A.**
    - **Others: it should be Level C – not Level A.**
  - **Our study recommends that the basis for equivalency between the Integrity of Security Controls and DO-178B safety levels needs to be more fully studied.**

Study’s Conclusions and Recommendations (1 of 2)

- **LAN deployments are inherently complex integrated systems. Every entity in a network is potentially “integrated together” via fate sharing**
- **In networked environments, certification must now address network attacks.**
  - **Security controls (primarily for integrity and availability) are an integral safety element in networked environments**
    - **Recommend that the FAA requires that security controls (Firewall, Packet Filter, Router, Encapsulation Gateway, HAG) be certified at Common Criteria EAL5 or higher**
  - **DO-178 software development processes need to be extended to mitigate network attack vulnerabilities**
    - **Recommend the introduction of specific tests into the development and certification processes**
      - Process maturity models, formally verify protocols, software fault injection, model checkers, buffer overflow tests, “dead code” tests, Fuzz testing
    - **Unless a solution to the current security theory limitation can be found, high assurance (Level A or B) software will require line-by-line software code inspection for fault identification as a constituent part of the certification process**
  - **ARP 4754 integration processes need to be extended to recognize that LANs and networks are a complex integrated system with several unique attributes**
    - **ARP 4754 needs to recognize that humans are a constituent element within airborne networked systems**

Study's Conclusions and Recommendations (2 of 2)

- **ARP 4754 needs to be extended to address the integrity and availability of the system and its items**
  - Require assured software download process using FIPS 186
  - Require a deployed airborne Item integrity verification system – consider using technologies such as Tripwire
- **ARP 4754 needs to be extended to address Attack Prevention and Mitigation by using IATF-defined defense in depth concepts**
- **Recommend that ARP 4754 explicitly leverage the <u>Biba Integrity Model</u> to define Network safety assurance concepts**
- **Recommend that VPNs be recognized as viable network partitions in accordance to ARP 4754 Section 5.4.1.1**
- **Recommend that ARP 4754 processes be extended to test the Integrated LAN and network system previous to deployment**
  - Network mapping, vulnerability scanning, penetration testing, password cracking, Item log reviews (including Security Controls) from the "red team" penetration tests, integrity and confirmation checking

Topics needing further study

1. **Civil Aviation policies and trust models (e.g., rogue nations)**
2. **Common solutions for identity, IP addressing, naming, routing, authentication, and network management.**
3. **Seek to find a better mechanism to address the problem of removing latent software bugs that can be attacked in networked environments. Testing is currently necessary but demonstrably inadequate, resulting in potential safety risks. Testing needs to be supplemented with rigorous code inspection for high assurance certification.**
4. **Study and articulate the controls needed within Biba High Assurance Guards (HAGs). Distinguish the differences (if any) between Biba HAG technology and the US DoD Bell-LaPadula HAG technology.**
5. **Further mature mechanism to map the integrity of Security Controls to DO-178B Safety Levels (e.g., build upon the University of Idaho work).**
6. **Study potentially integrating DoD and FAA certification processes and procedures. Alternatives include:**
   - **Implications of joint certification solely in terms of the loose Safety – Security mappings suggested by the University of Idaho results**
   - **Implications of joint certification should tighter Safety – Security mappings be created, for example via leveraging the mission assurance category (MAC) levels identified by DoDI 8500.2 to define the security needs of safety environments or by more explicitly relating DO-178B with the Common Criteria**

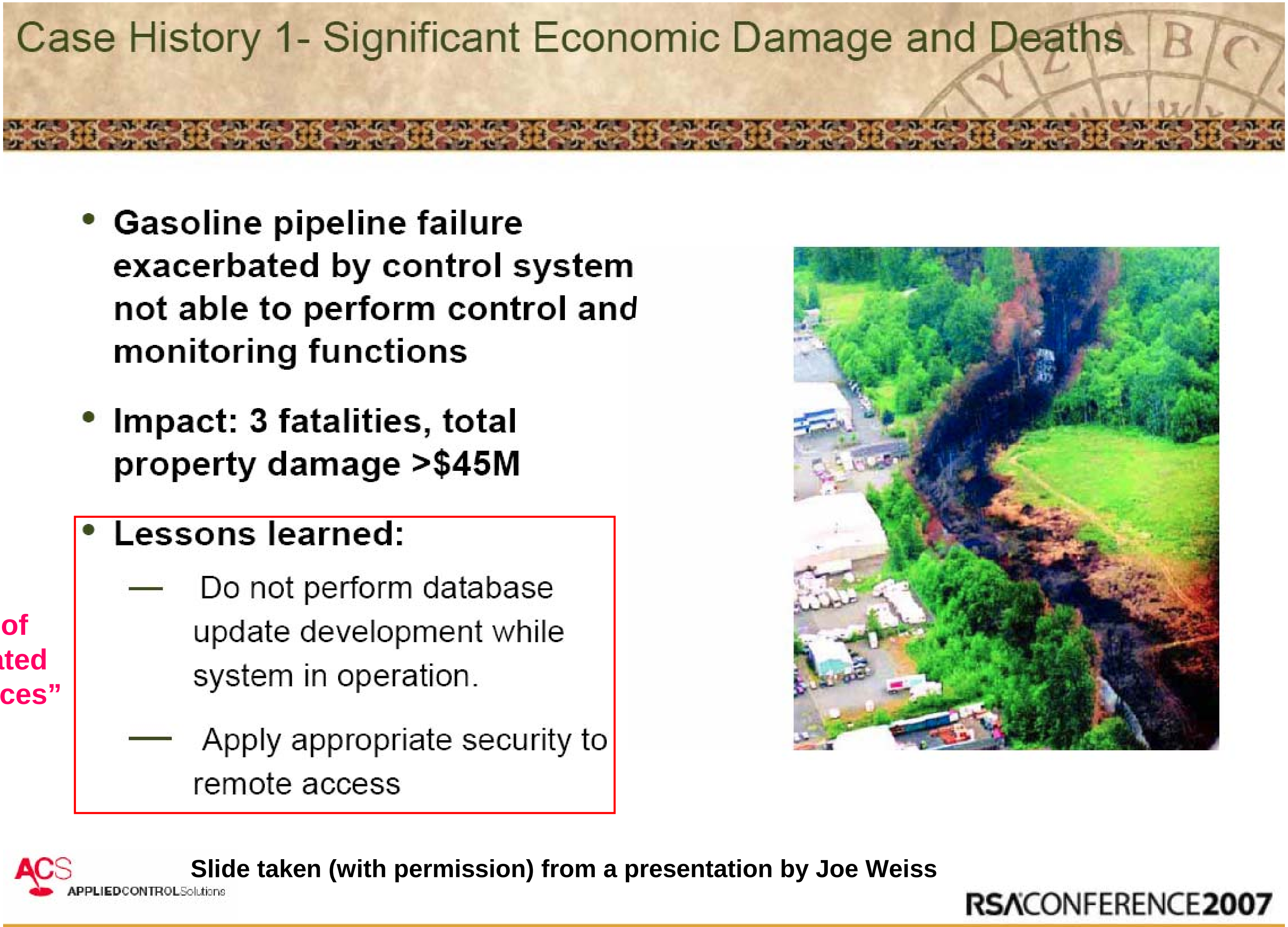
Backup Slides

Backup Slides now follow

Connecting any Network to the Internet has Risks

- By the end of 2000, the life expectancy of a default installation of Red Hat 6 was less than 72 hours.
- One of the fastest times a honeypot was compromised [in 2002] was 15 minutes. This means that within 15 minutes of being connected to the Internet, the system was found, probed, attacked, and successfully exploited by an attacker. The record for capturing a worm was under 90 seconds.
- The BBC reported in 2006: “When we put our honeypot online the fastest an attack struck was mere seconds and it was never longer than 15 minutes before the honeypot logged an attempt to subvert it.” <Article also described Botnets>
- In the beginning of 2002, the average home network was scanned on average by 31 different systems a day.
- The most virulent computer virus to date infected several million machines in about 20 minutes.
- IronPort published a report in 2006 showing that Trojan horses and system monitors – two of the most serious types of malware – infect one out of every 14 corporate PCs.
- “The number of new [COTS] software security vulnerabilities identified by security experts, hackers and others during the first eight months [of 2006] has already exceeded the total recorded for all of 2005, according to Internet Security Systems. … Of the 5,300 [new] vulnerabilities recorded for 2006 so far, 0.4 percent were deemed critical (could be used to form a prolific automated worm); 16.6 percent were deemed high (could be exploited to gain control of the host running software); 63 percent were medium (could be used to access files or escalate privileges); and 20 percent were low (vulnerabilities that leak information or would allow a denial of service attack).” -- Computerworld

Example from the Control Systems Industry (1 of 3)



Case History 1- Significant Economic Damage and Deaths

- **Gasoline pipeline failure exacerbated by control system not able to perform control and monitoring functions**
- **Impact: 3 fatalities, total property damage >$45M**
- **Lessons learned:**
  - Do not perform database update development while system in operation.
  - Apply appropriate security to remote access

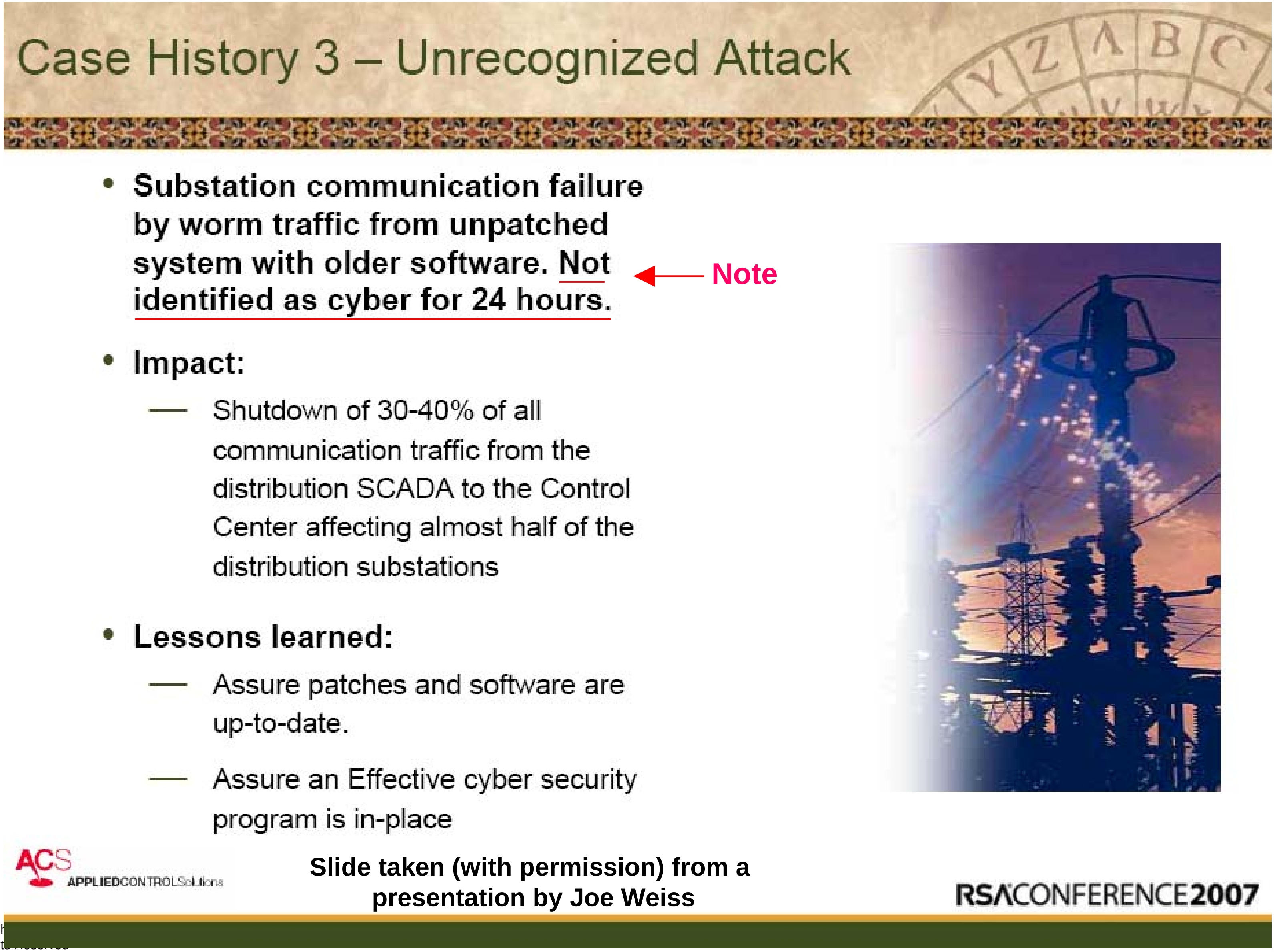
Point: “Beware of Unanticipated Consequences”

ACS APPLIEDCONTROLSolutions

Slide taken (with permission) from a presentation by Joe Weiss

RSACONFERENCE2007

Example from the Control Systems Industry (2 of 3)



Case History 3 – Unrecognized Attack

- **Substation communication failure by worm traffic from unpatched system with older software. Not identified as cyber for 24 hours.**

Note

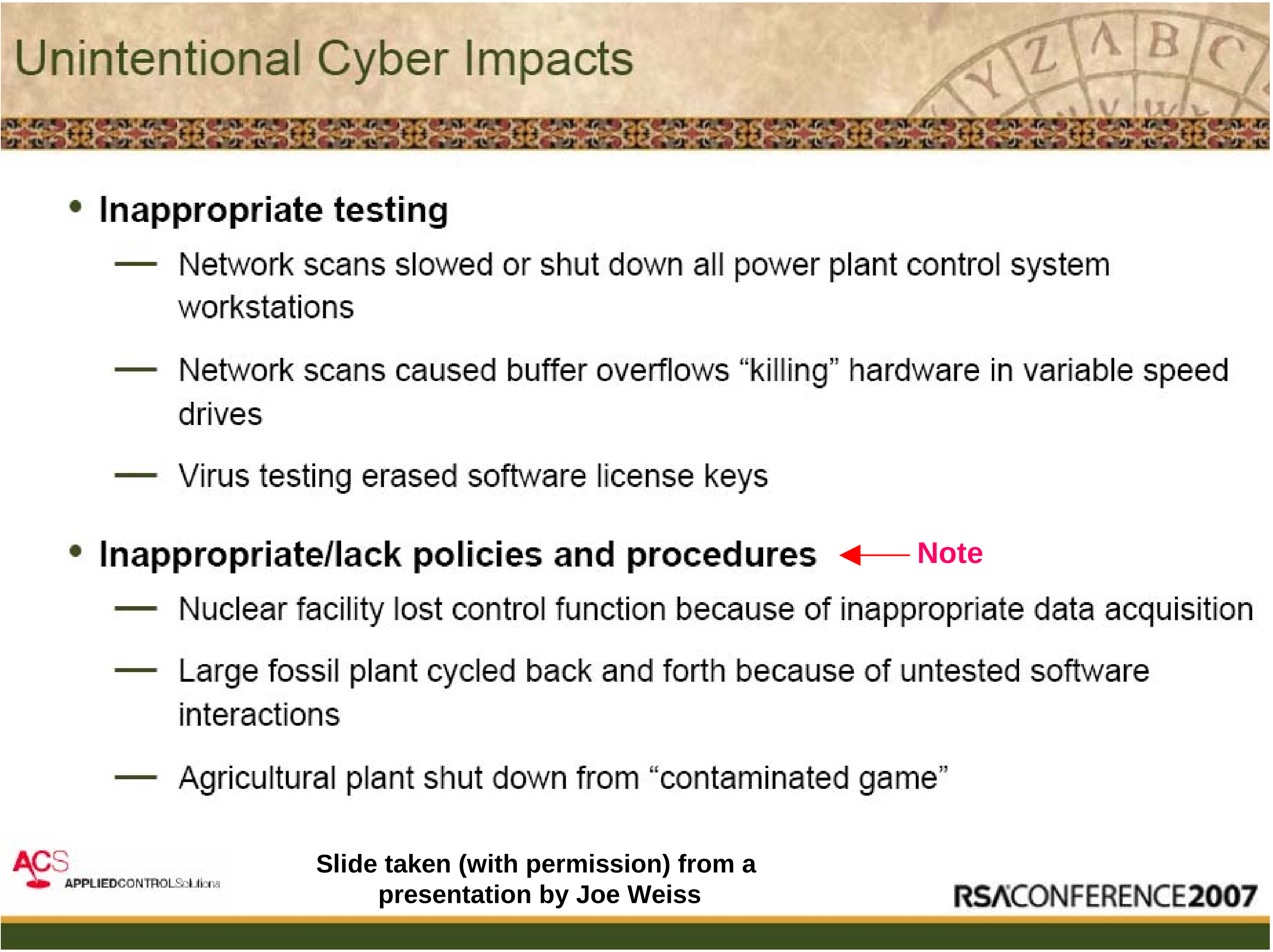
- **Impact:**
  - Shutdown of 30-40% of all communication traffic from the distribution SCADA to the Control Center affecting almost half of the distribution substations
- **Lessons learned:**
  - Assure patches and software are up-to-date.
  - Assure an Effective cyber security program is in-place

ACS APPLIEDCONTROLSolutions

Slide taken (with permission) from a presentation by Joe Weiss

RSA CONFERENCE2007

Example from the Control Systems Industry (3 of 3)



Unintentional Cyber Impacts

- **Inappropriate testing**
  - — Network scans slowed or shut down all power plant control system workstations
  - — Network scans caused buffer overflows "killing" hardware in variable speed drives
  - — Virus testing erased software license keys
- **Inappropriate/lack policies and procedures** ← **Note**
  - — Nuclear facility lost control function because of inappropriate data acquisition ← **OOPS!!**
  - — Large fossil plant cycled back and forth because of untested software interactions
  - — Agricultural plant shut down from "contaminated game"

Slide taken (with permission) from a presentation by Joe Weiss

Threat Agents

- **Corrupted or Careless Insider**
  - Are authorized to access the network
  - E.g., NAS personnel, aircraft personnel, passengers, local systems
- **Hostile Outsider**
  - Are not authorized to access the network
  - Attackers are located on “the Internet”
    - – Random “cracker”
    - – Malicious criminal syndicates (currently a multi-billion dollar “industry”)
    - – Hostile governments (electronic warfare)
- **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

Security Controls in the Exemplar Airborne Arch (1/3)

- **Physical Security**
  - **“Aircraft Control” and “Cockpit (Pilot) Network” networks and their devices should not be physically accessible by aircraft passengers. HAGs similarly should not be accessible. The “Non-Cockpit Crew Network” may be accessible to unattended passengers.**
- **Encapsulation Gateways**
  - **Should be configured so that all communications to the gateways must be dropped unless they use IPsec’s ESP in transport mode and all communications to their supported enclave must use ESP in tunnel mode.**
- **Packet Filter**
  - **Packet Filter should be configured so that:**
    - **No device within the passenger network can access either the Non-Cockpit Crew network or the Cockpit Crew Network.**
    - **No device within either the Non-Cockpit Crew Network or the Passenger network can send packets to any encapsulation gateway.**
    - **Attack fingerprinting activities (see Section 3.3.1) are blocked without harming normal ICMP traffic.**
  - **The packet filter, or a device closely associated with it, should also rate limit communications from the passenger network to a threshold rate. This is to ensure that passengers cannot cause denial of service (DoS) to the aircraft LAN.**

Security Controls in the Exemplar Airborne Arch (2/3)

- **Firewall**
  - **The firewall should be configured to operate in as exclusive a manner as possible. It is desirable that pilot and crew not use HTTP so that HTTP use (port 80 and 443) can be restricted to passengers only, thereby reducing the HTTP overt channel through the firewall.**
  - **The firewall should be configured so that:**
    - **All fingerprinting (see Section 3.3.1) activity will fail (i.e., packets dropped). Needs to ensure that normal ICMP packet behavior is not obstructed.**
    - **All communications to encapsulating gateways from outside of the airplane are blocked unless they use IPsec's ESP.**
    - **All packets originating from outside of the airplane to IP destination addresses that are not in use within the airplane should be dropped.**
  - **It is desirable that the firewall have Network Intrusion Detection capabilities.**
- **AS Boundary Router (ASBR)**
  - **ASBR should be configured such that all packets that are sent to it (i.e., the ASBR as the destination IP address) are dropped unless they come from the network management or Intrusion Detection System that is local to that airplane.**

Security Controls in the Exemplar Airborne Arch (3/3)

- **High Assurance LAN**
  - **Should comply with the *Safety and Certification Approaches for Ethernet-based Aviation Databuses* document.**
    - **E.g., Avionics Full Duplex Switched (AFDX) deterministic Ethernet**
  - **Should be configured to provide physical layer connectivity that duplicates the virtual private network enclave configurations as a defense in depth provision.**
  - **The passenger network's LAN should be a distinct physical LAN, solely used by the passengers alone. That LAN must be solely connected to other aircraft LAN(s) by means of the packet filter.**
- **QoS**
  - **It is desirable that links implement QoS rate control semantics so that the safety enclaves are ensured that they have the physical LAN capacity required to perform their function. If the traffic exceeds the LANs capacity, then the difference needs to come from dropping passenger packets.**
- **Air-to-Ground and Air-to-Air Communications**
  - **Wireless signals in space should be encrypted**
  - **FAA should consider the appropriateness of deploying anti-jamming (AJ) or low probability of intercept / low probability of detection (LPI/LPD) waveforms.**

Background: CC's Evaluation Assurance Levels (EAL)

- **The Common Criteria (CC) has provided seven predefined security assurance packages, on a rising scale of assurance, known as Evaluation Assurance Levels (EALs). These provide groupings of assurance components that are intended to be generally applicable. The seven EALs are as follows:**

1. **EAL 1 – Functionally Tested**
2. **EAL 2 – Structurally Tested**
3. **EAL 3 – Methodically Tested and Checked**
4. **EAL 4 – Methodically Designed, Tested, and Reviewed**
5. **EAL 5 – Semi-formally Designed and Tested**
6. **EAL 6 – Semi-formally Verified Design and Tested**
7. **EAL 7 – Formally Verified Design and Tested**

EAL1 - EAL4 are expected to be generic commercial products.
EAL5 - EAL7 are high assurance products.

Possible Joint FAA and DoD Certification Processes

- **The only correlation between safety and security required by the Biba model is to map the integrity of the airborne security controls to specific DO-178B safety assurance levels.**
- **However, the FAA and DoD may be able to create complementary certification systems due to the fact that**
  - ➢ **The Biba and Bell-LaPadula Models are direct analogs of each other**
  - ➢ **Our Recommended Exemplar Airborne Architecture is remarkably similar to the DoD's Global Information Grid (GIG) architecture**
  - ➢ **Coincidence: DoD Confidentiality Levels can be directly compared with the DO-178B Safety Levels**
- **Recommend: Investigate DoDI 8500.2 Enclosure 4 Mission Assurance Category (MAC) as a possible avenue for FAA-DoD certification synergy**
  - **MAC is defined in terms of integrity and availability – Key safety req.**
  - **Confidentiality mappings may be required for DoD but not FAA**
- **The DoD also has Safety standards that are articulated by MIL-STD 882D.**
  - **MIL-STD 882D shares many similarities with existing FAA processes (e.g., ARP 4754, DO-178B) including a remarkably similar safety severity classification system.**