HITBSECCONF2013 amsterdam

THE FOURTH ANNUAL HITB SECURITY CONFERENCE IN EUROPE

Aircraft Hacking

Practical Aero Series

✈ IT Security

Hugo Teso
(@hteso)

(@48bits)
www.48bits.com
One and a half architecture

✈ Commercial Pilot

Aero Series

www.commandercat.com

Agenda

- Part 1: The $PATH to the exploit
- Part 2: The $PATH to exploit

Disclaimer

- Time constraints
  - Too much to explain
    - Aircrafts != Computers
- Safety reasons
  - Still too much to fix

Part 1

The $PATH to the exploit

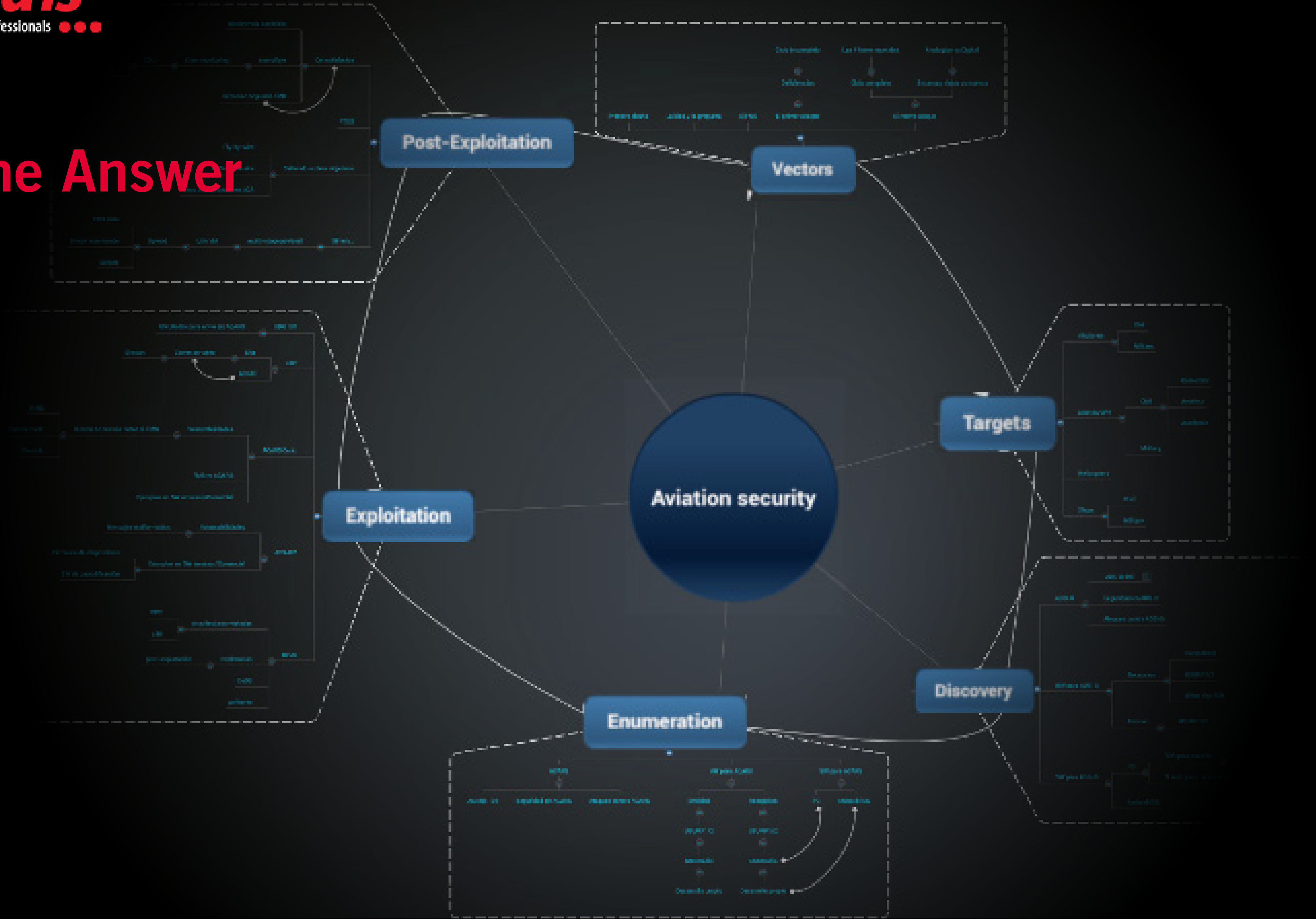
The Target

In the beginning there was “The Question”

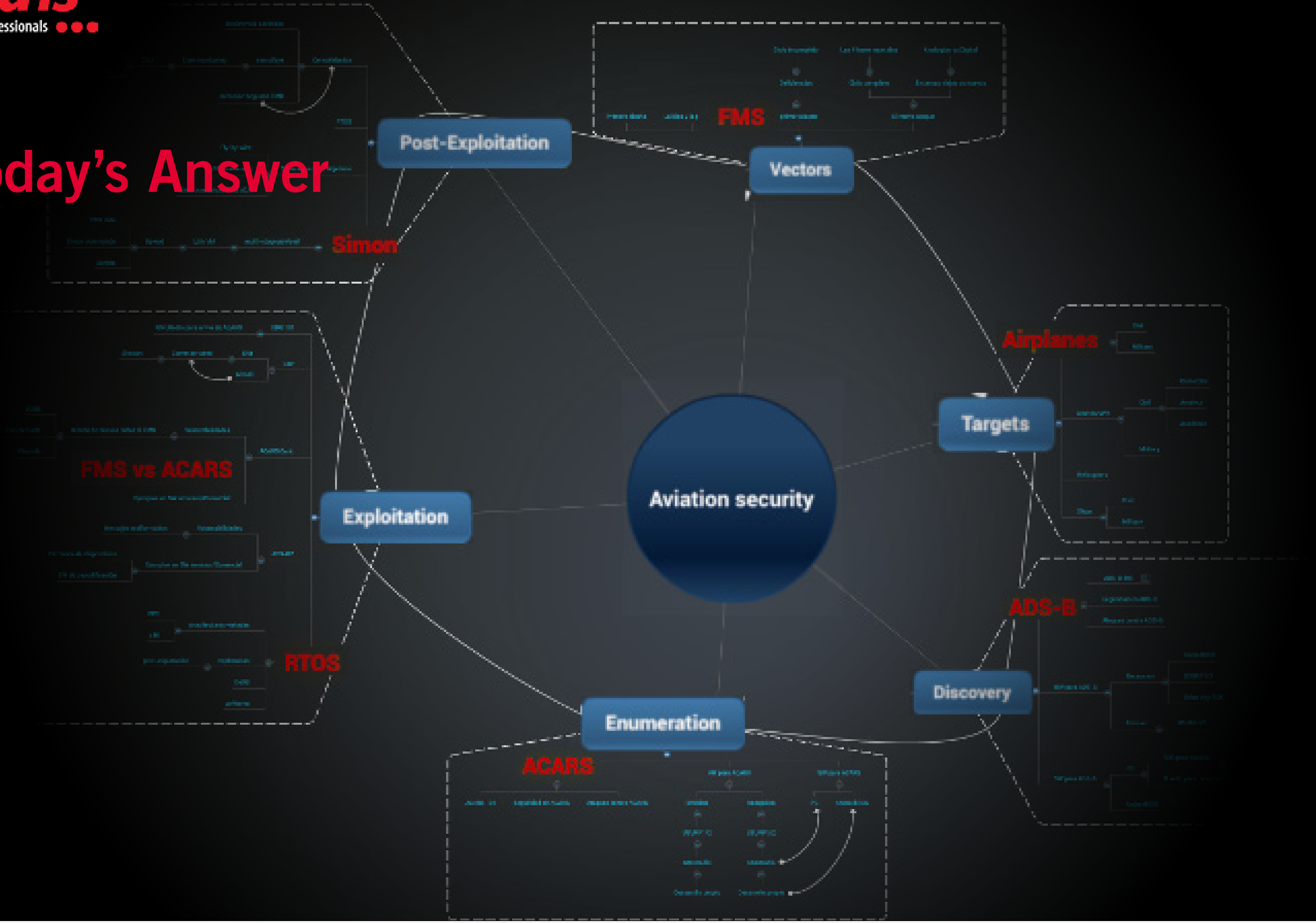
Would I be able to convert THIS...

...into THIS ?

The Answer


Post-Exploitation
Vectors
Targets
Aviation security
Exploitation
Discovery
Enumeration

Today's Answer



Attack Overview

DISCOVERY:
- » ADS-B

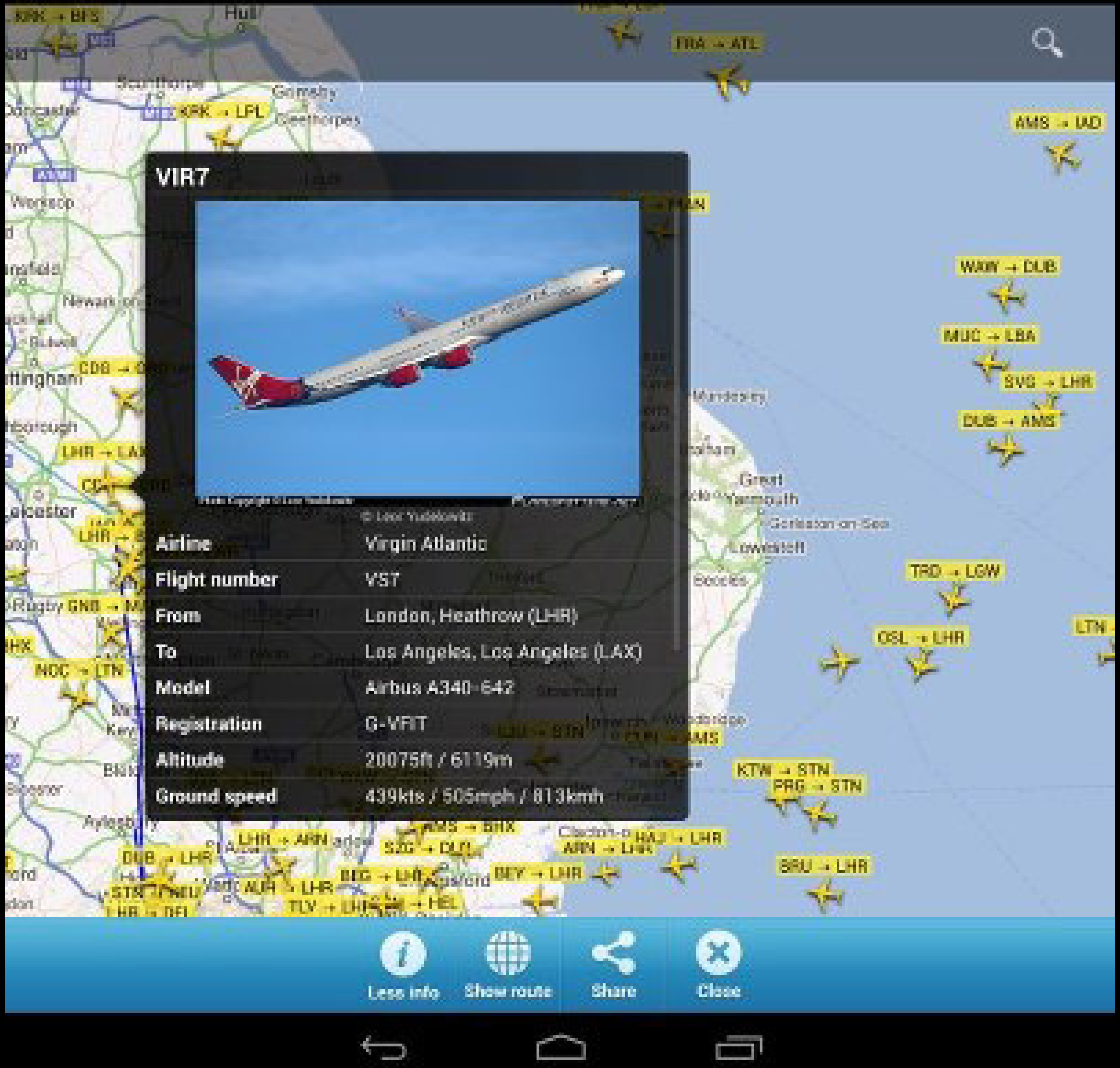
INFO GATHERING:
- » ACARS

EXPLOITATION:
- » Via ACARS
- » Against on-board systems vulns.

POST-EXPLOITATION:
- » Party hard!

ADS-B 101

- Automatic Dependent Surveillance-Broadcast
- Radar substitute
- *Position*, *velocity*, *identification*, and other ATC/ATM-related information.
- ADS-B has a data rate of 1 Mbit/sec.
- Used for locating and plotting targets



VIR7

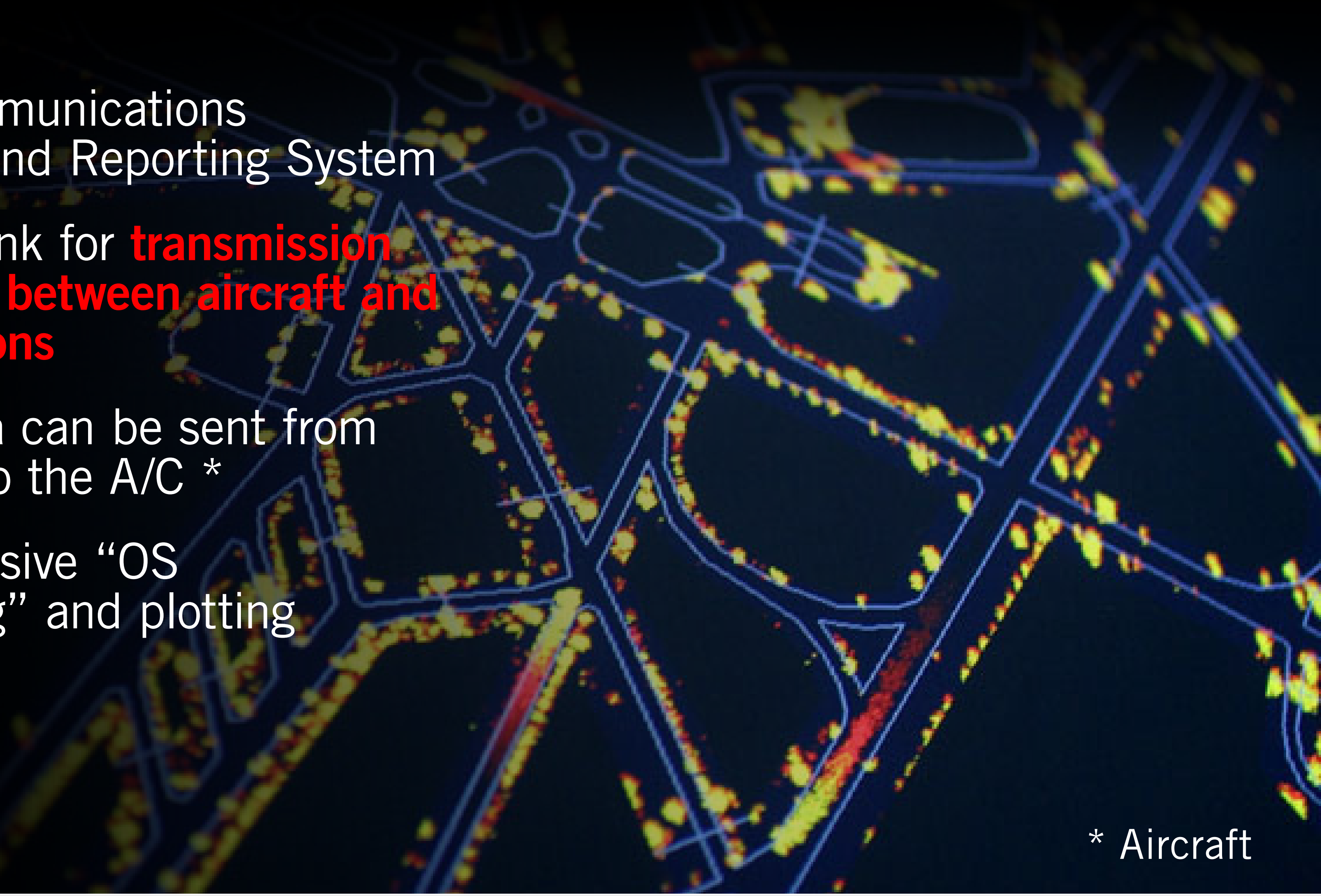
Airline	Virgin Atlantic
Flight number	VS7
From	London, Heathrow (LHR)
To	Los Angeles, Los Angeles (LAX)
Model	Airbus A340-642
Registration	G-VFIT
Altitude	20075ft / 6119m
Ground speed	439kts / 505mph / 813kmh

ADS-B Security

- None at all
- Attacks range from **passive attacks** (eavesdropping) to **active attacks** (message jamming, replaying, injection).
- Target selection
  - » Public Data
  - » Local data (SDR*)
  - » Virtual Aircrafts

* Software Defined Radio

ACARS 101

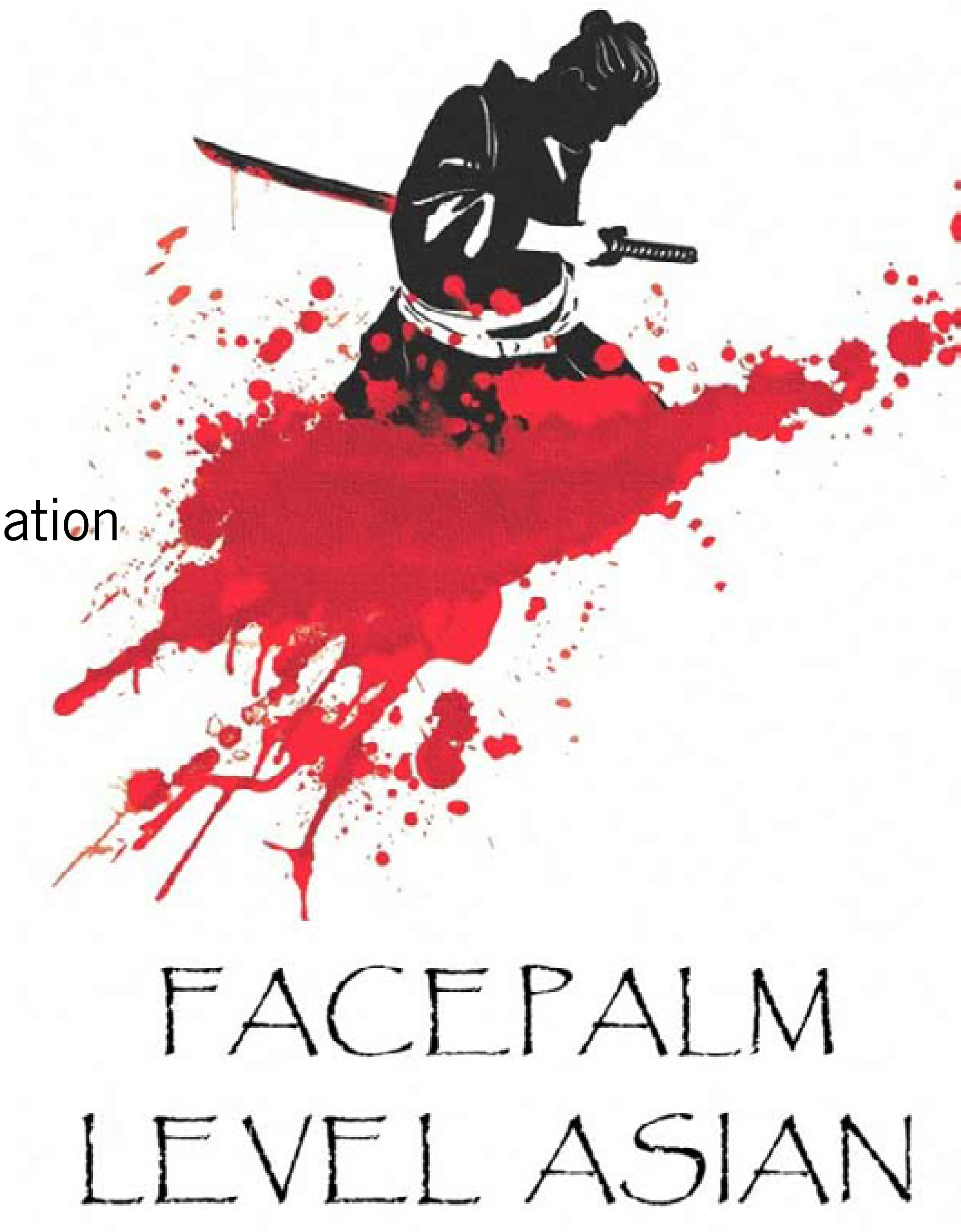


- ✈ Aircraft Communications Addressing and Reporting System
- ✈ Digital datalink for **transmission of messages between aircraft and ground stations**
- ✈ Multiple data can be sent from the ground to the A/C *
- ✈ Used for passive “OS fingerprinting” and plotting targets

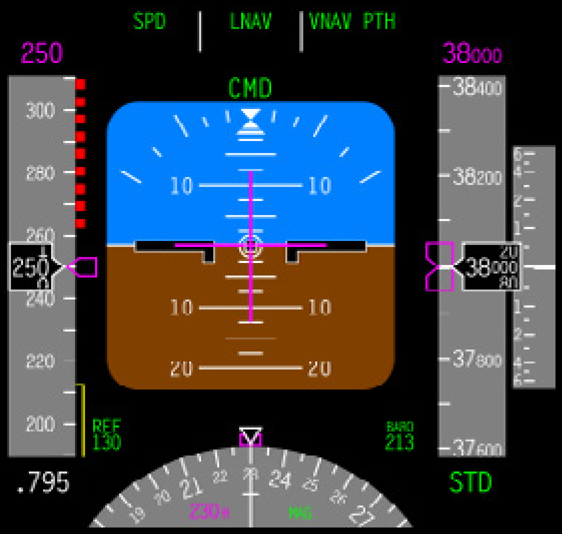
* Aircraft

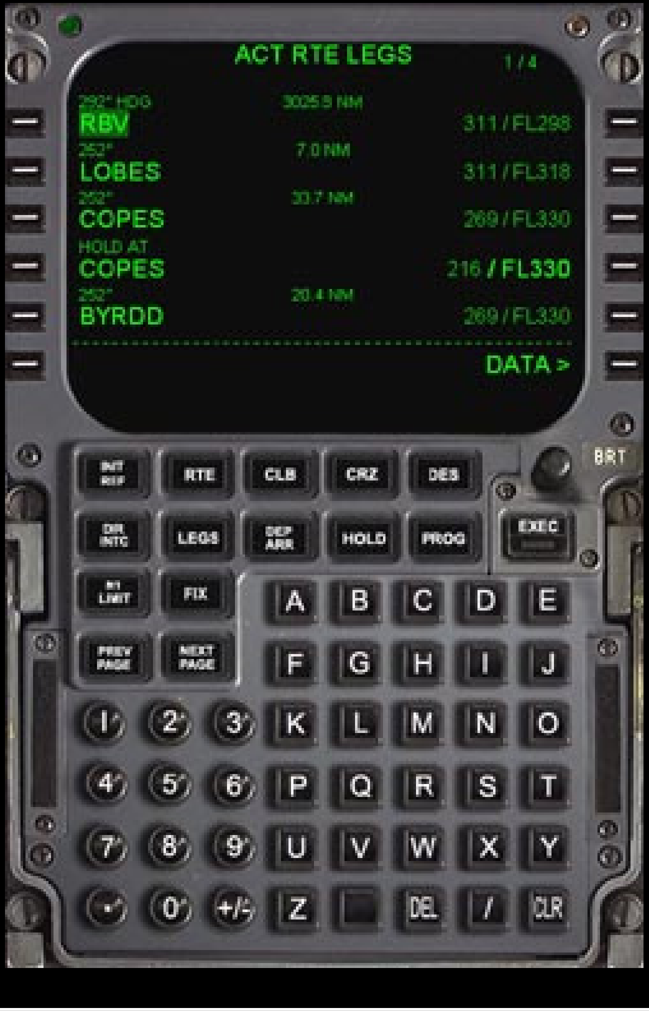
ACARS Security

- ✈ None at all
  - » sometimes monoalphabetic ciphers
- ✈ Detailed flight and Aircraft information
  - » Public DB
  - » Local data (SDR)
  - » Virtual Aircrafts
- ✈ Ground Service Providers
  - » Two main players
  - » Worldwide coverage



FMS 101





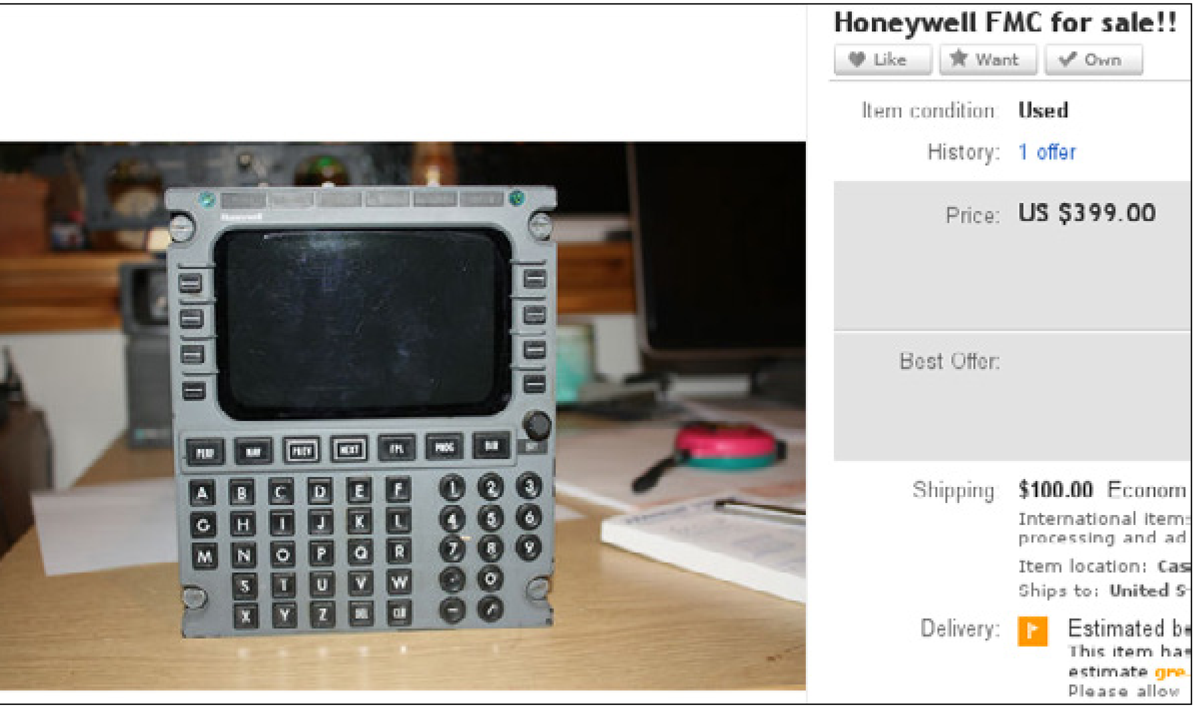
- ✈ Flight Management System typically consists of two units:
  - » A computer unit
  - » A control display unit
- ✈ Control Display Unit (CDU or MCDU) provides the primary human/machine interface for data entry and information display.
- ✈ FMS provides:
  - » Navigation
  - » Flight planning
  - » Trajectory prediction
  - » Performance computations
  - » Guidance

FMS

- Goal: Exploit the FMS
  - Using ACARS to upload FMS data
  - Many different data types available
- Upload options:
  - Software Defined Radio
  - Ground Service Providers
- The path to the exploit:
  - Audit aircraft code searching for vulnerabilities
- We use a lab with virtual airplanes
  - but real aircraft code and HW

Aircraft Hardware and Software

- The good old…
  - eBay!!
- Russian scrapings
  - You name it
- Loving salesman
  - Value-added products
- Third party vendors
  - /wp-admin… Sigh
- Resentful users or former employees



Honeywell FMC for sale!!

Item condition: **Used**

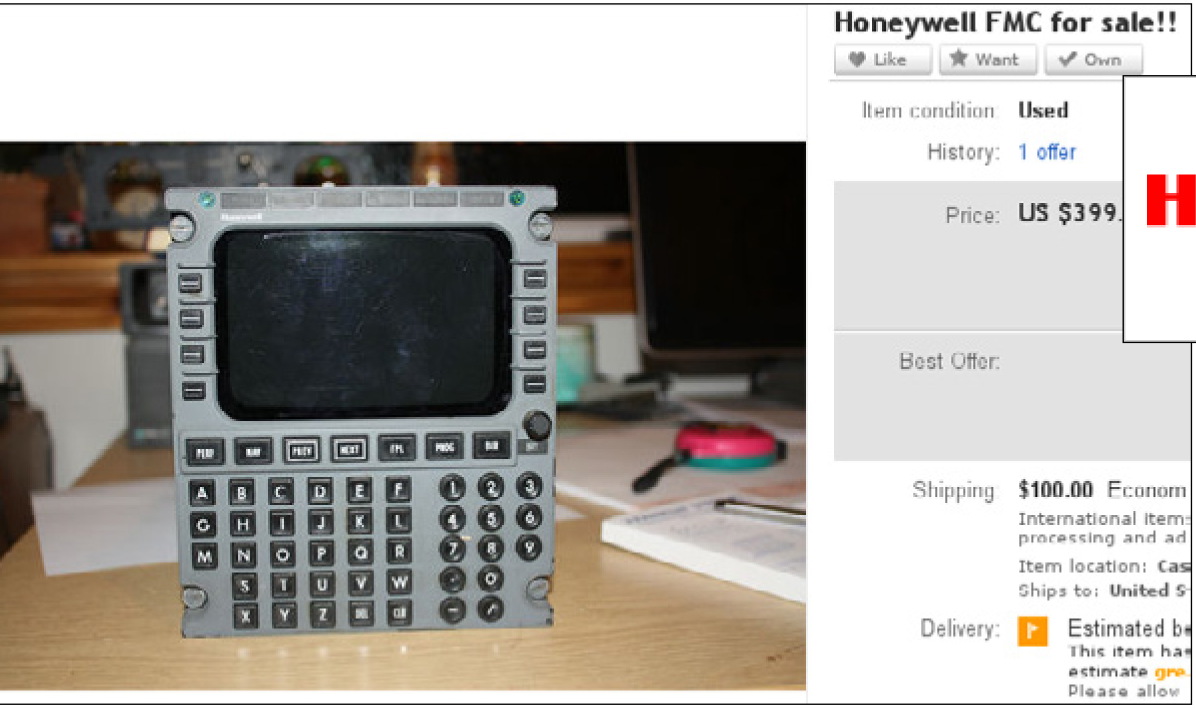
History: 1 offer

Price: **US $399.00**

Best Offer:

Shipping: **$100.00** Econom
International items
processing and ad
Item location: **Cas**
Ships to: **United S**

Delivery: Estimated b
This item has
estimate gre
Please allow



Honeywell FMC for sale!!

Item condition: Used

History: 1 offer

Price: US $399.

Best Offer:

Shipping: $100.00 Econom

International item:
processing and ad

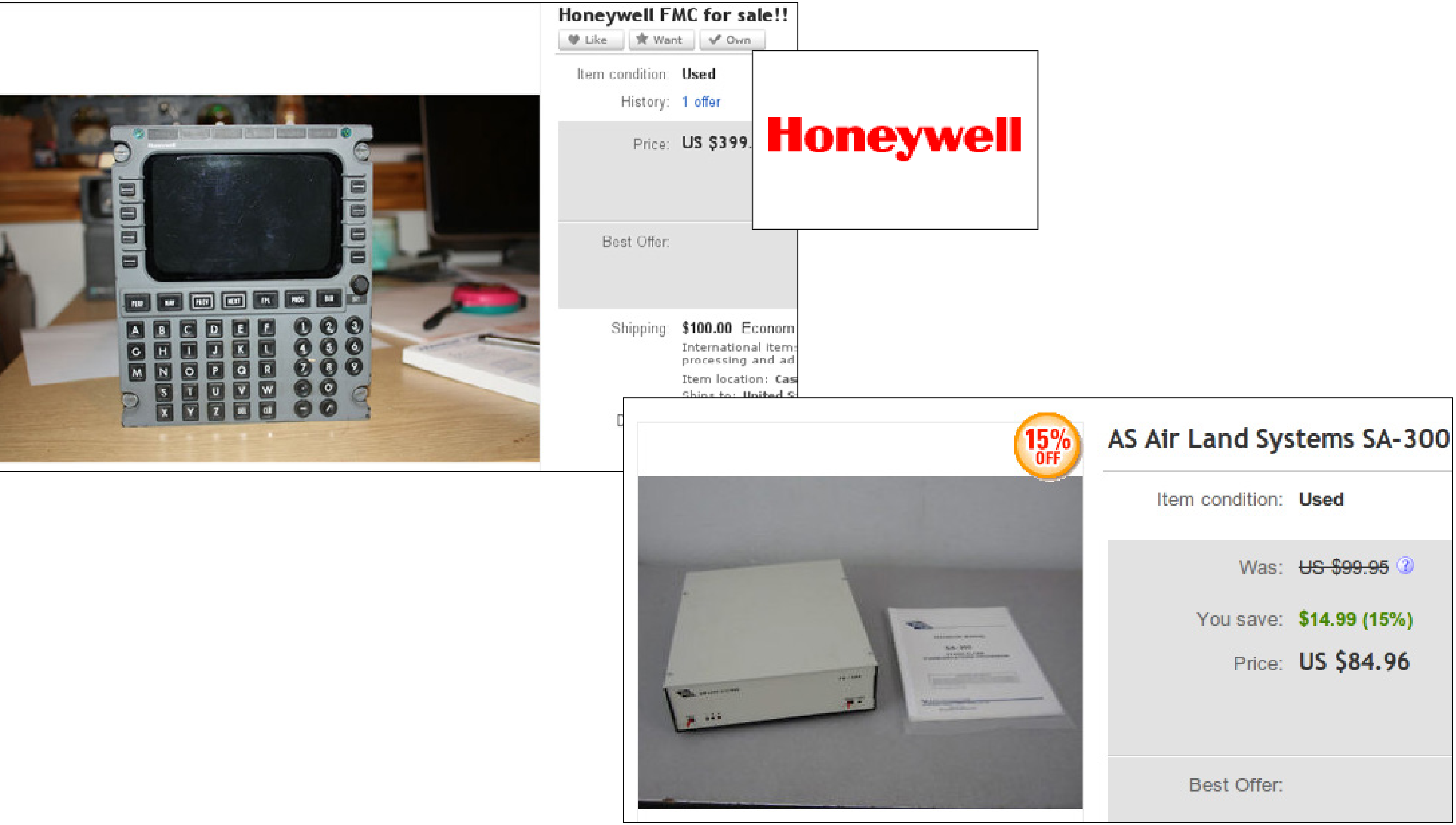
Item location: Cas

Ships to: United S

Delivery: Estimated b

This item has
estimate gre
Please allow

Honeywell



Honeywell FMC for sale!!

Item condition:	Used
History:	1 offer
Price:	US $399.
Best Offer:	
Shipping:	$100.00 Econom International item: processing and ad Item location: Cas Ships to: United S

Honeywell

AS Air Land Systems SA-300

Item condition:	Used
Was:	~~US $99.95~~
You save:	$14.99 (15%)
Price:	US $84.96
Best Offer:	

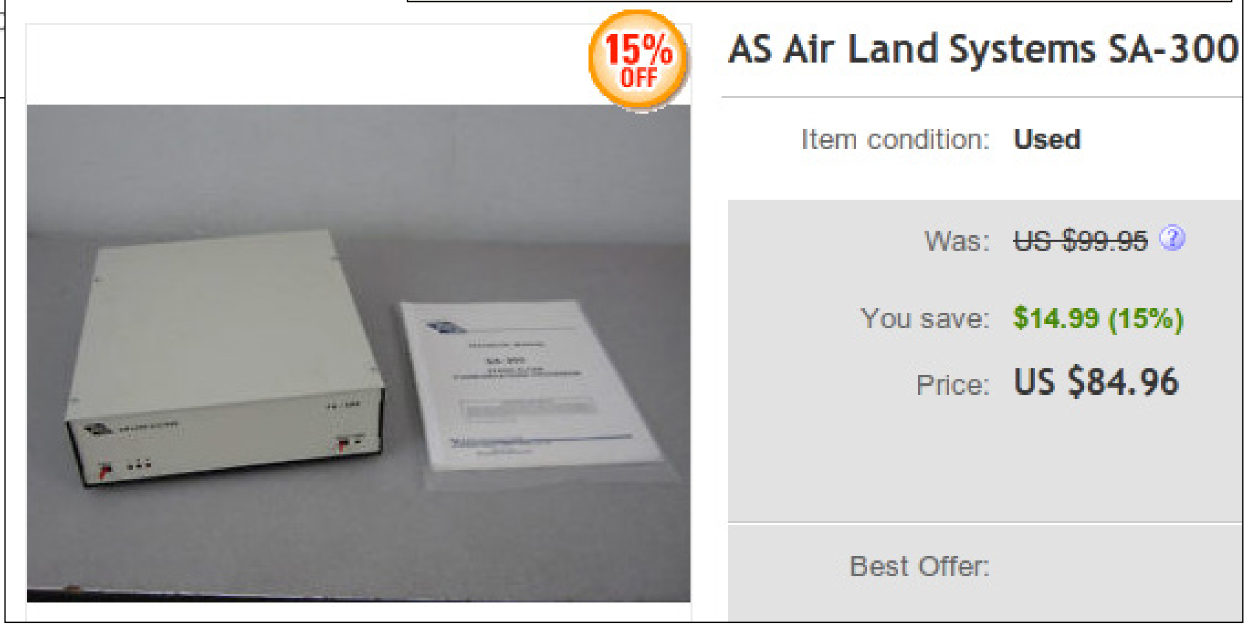
Honeywell FMC for sale!!

♥ Like ★ Want ✓ Own

Item condition:	Used
History:	1 offer
Price:	US $399.
Best Offer:	
Shipping:	$100.00 Econom International item processing and ad Item location: Cas Ships to: United S

Honeywell

A truly effective solution is the Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.



15% OFF

AS Air Land Systems SA-300

Item condition:	Used
Was:	~~US $99.95~~
You save:	$14.99 (15%)
Price:	US $84.96
Best Offer:	

Honeywell FMC for sale!!

Like Want Own

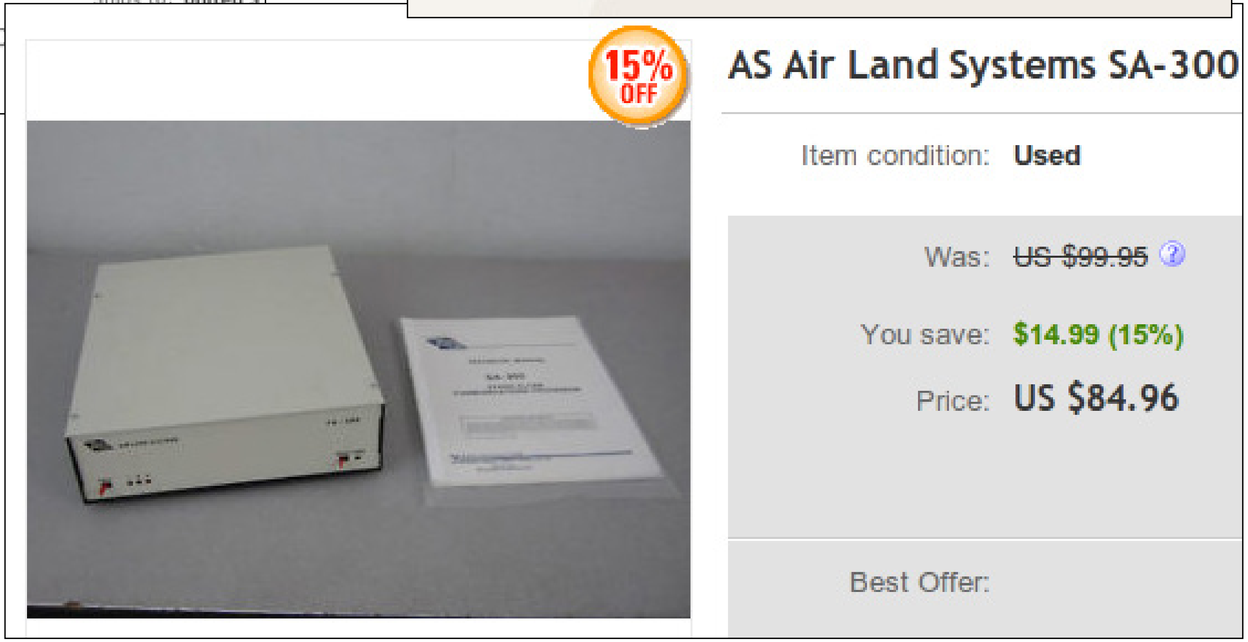
Item condition:	Used
History:	1 offer
Price:	US $399.
Best Offer:	
Shipping:	$100.00 Econom International items processing and ad Item location: Cas Ships to: United S

Honeywell

Key advantages

The PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.

A truly effecti Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.



AS Air Land Systems SA-300

Item condition:	Used
Was:	~~US $99.95~~
You save:	$14.99 (15%)
Price:	US $84.96
Best Offer:	

Key advantages

he PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.

THALES

Honeywell

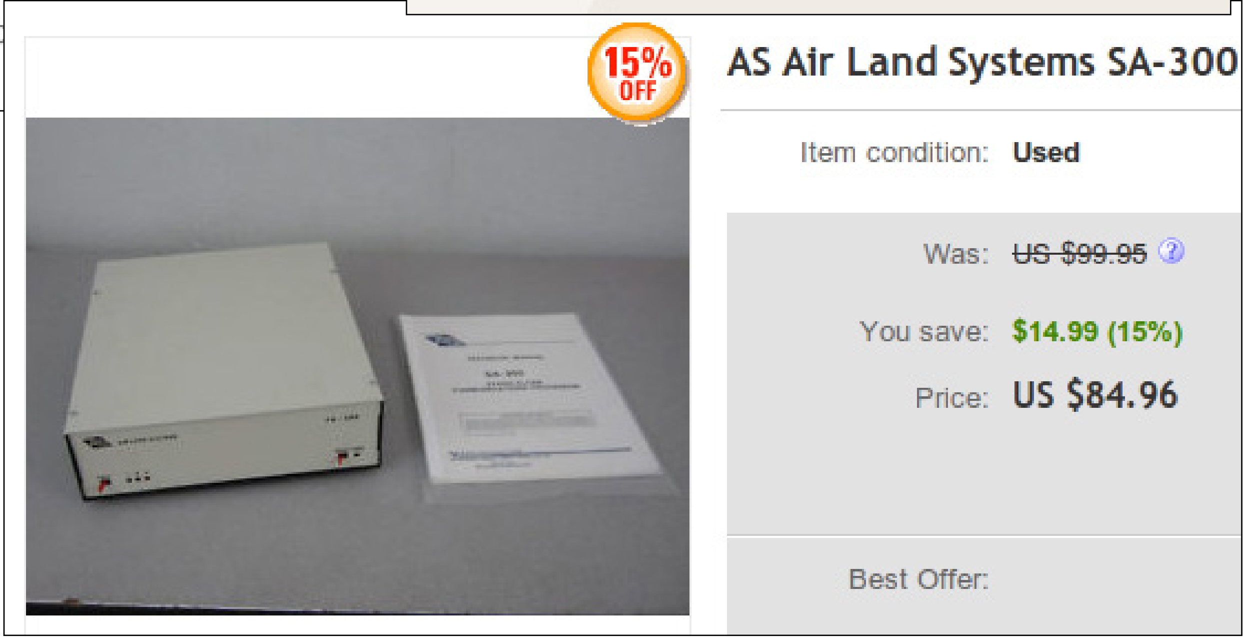
A truly effecti

Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.

Honeywell FMC for

♥ Like ★ Want ✓ Own

Item condition:	Used
History:	1 offer
Price:	US $399.
Best Offer:	
Shipping:	$100.00 Econom International items processing and ad Item location: Cas Ships to: United S

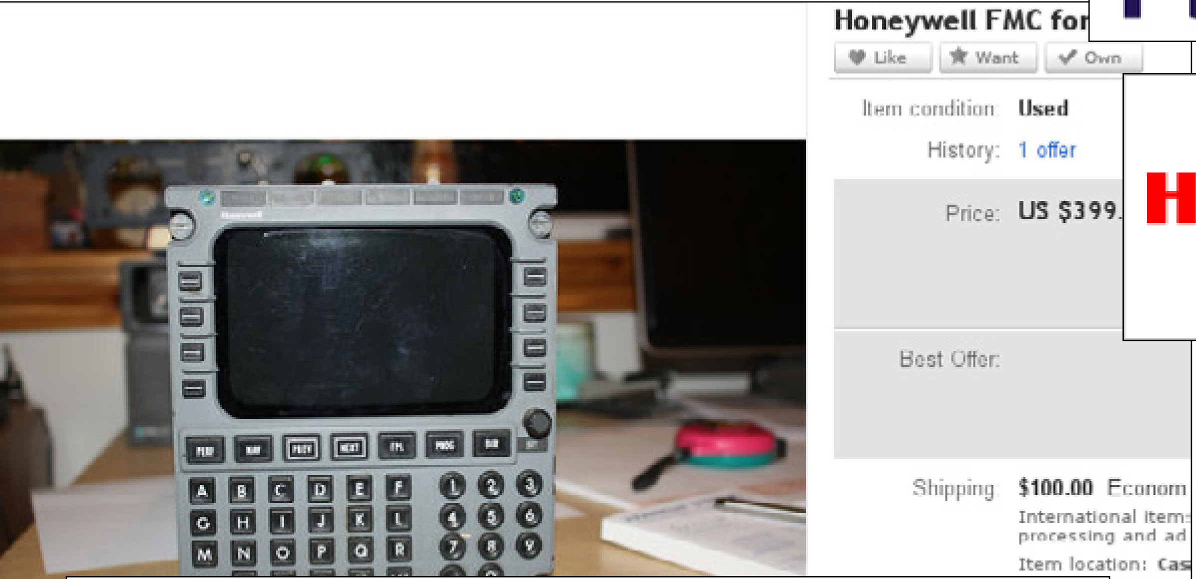


AS Air Land Systems SA-300

Item condition:	Used
Was:	~~US $99.95~~
You save:	$14.99 (15%)
Price:	US $84.96
Best Offer:	

THALES

Honeywell



Honeywell FMC for

♥ Like ★ Want ✓ Own

Item condition: Used

History: 1 offer

Price: US $399.

Best Offer:

Shipping: $100.00 Econom

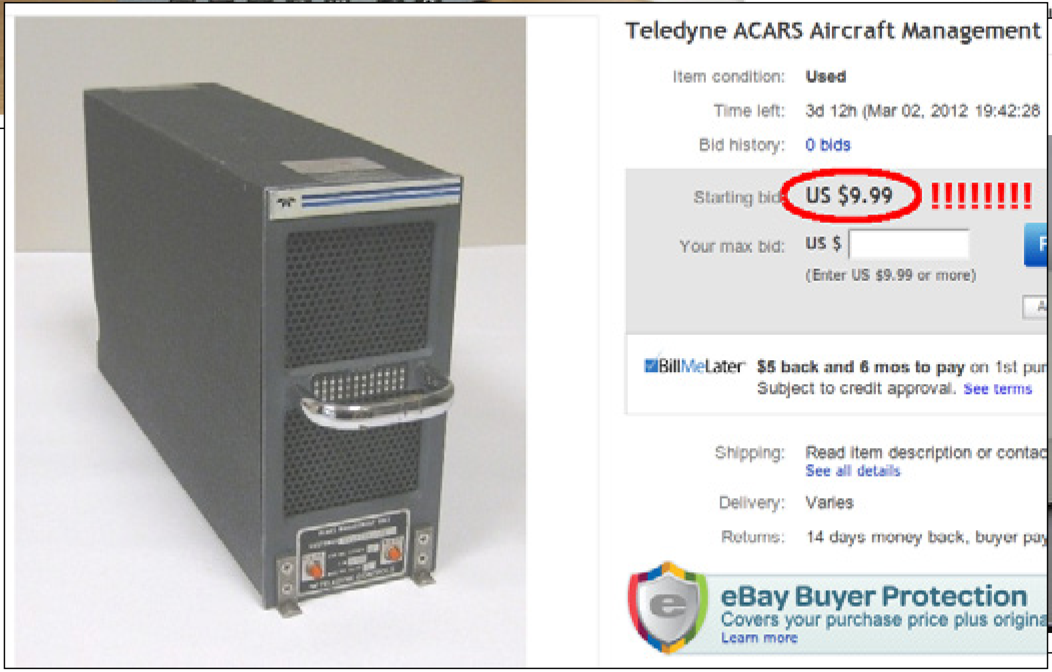
International item:
processing and ad

Item location: Cas
United S

Key advantages

The PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.

A truly effecti
Rockwell Collins FMS desktop trainer (DTT).
Our solution uses the same software that
is used by the actual Rockwell Collins FMS
and display avionics software.



Teledyne ACARS Aircraft Management

Item condition: Used

Time left: 3d 12h (Mar 02, 2012 19:42:28

Bid history: 0 bids

Starting bid: US $9.99 !!!!!!!!!

Your max bid: US $

(Enter US $9.99 or more)

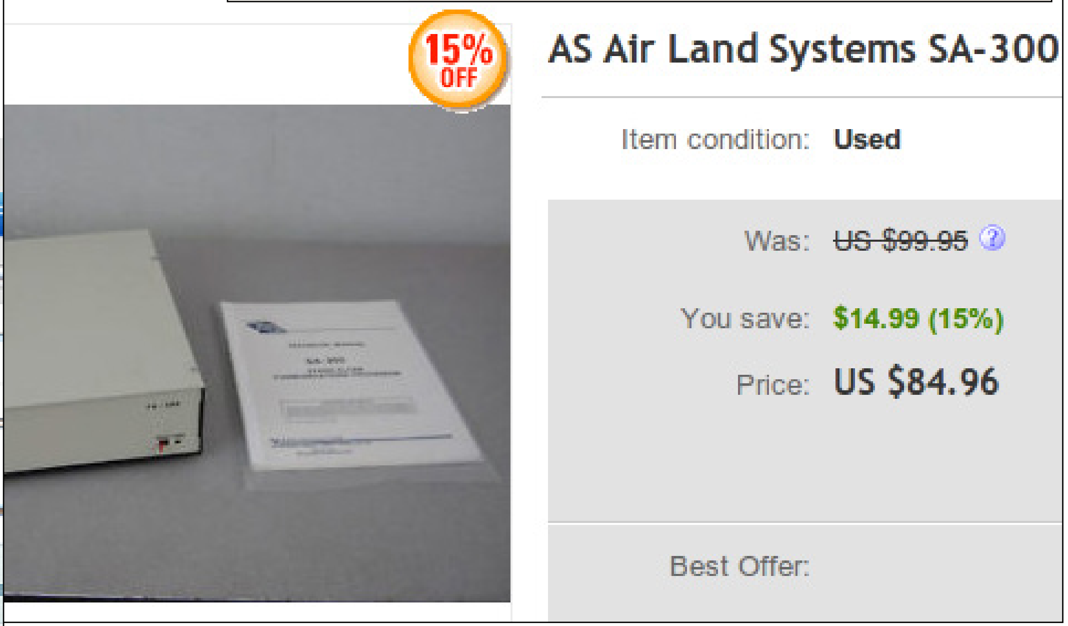
☑BillMeLater $5 back and 6 mos to pay on 1st pur
Subject to credit approval. See terms

Shipping: Read item description or contac
See all details

Delivery: Varies

Returns: 14 days money back, buyer pay

eBay Buyer Protection
Covers your purchase price plus origina
Learn more



AS Air Land Systems SA-300

15% OFF

Item condition: Used

Was: ~~US $99.95~~

You save: $14.99 (15%)

Price: US $84.96

Best Offer:

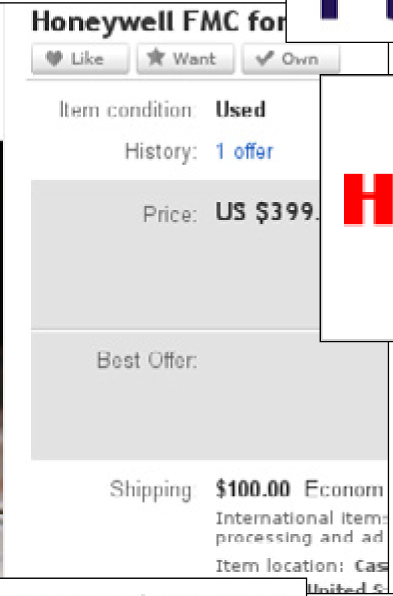
THALES

Honeywell

Key advantages

The PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.

A truly effecti
Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.



Honeywell FMC for

♥ Like ★ Want ✓ Own

Item condition: Used

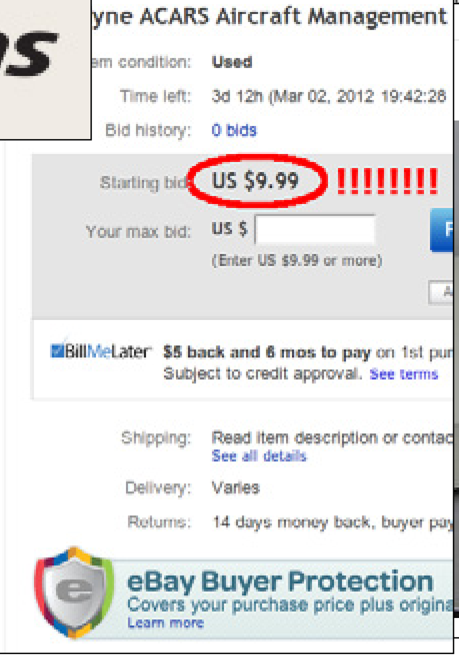
History: 1 offer

Price: US $399.

Best Offer:

Shipping: $100.00 Econom
International item:
processing and ad
Item location: Cas
United S

Rockwell Collins
Building trust every day



yne ACARS Aircraft Management

em condition: Used

Time left: 3d 12h (Mar 02, 2012 19:42:28

Bid history: 0 bids

Starting bid: US $9.99 !!!!!!!!

Your max bid: US $

(Enter US $9.99 or more)

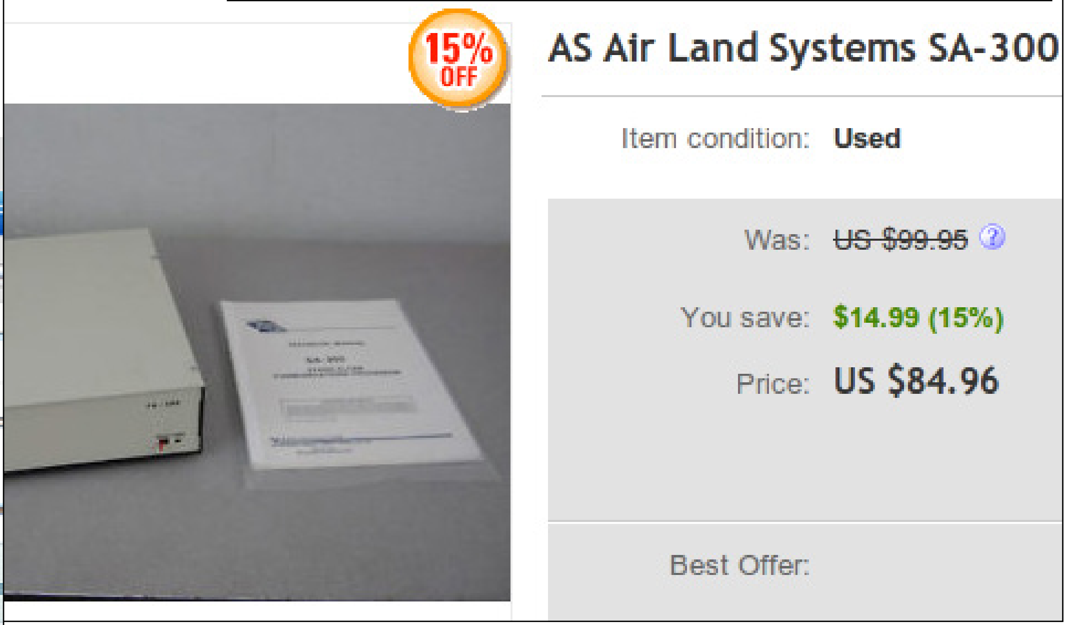
BillMeLater $5 back and 6 mos to pay on 1st pur
Subject to credit approval. See terms

Shipping: Read item description or contac
See all details

Delivery: Varies

Returns: 14 days money back, buyer pay

eBay Buyer Protection
Covers your purchase price plus origina
Learn more



15% OFF

AS Air Land Systems SA-300

Item condition: Used

Was: ~~US $99.95~~

You save: $14.99 (15%)

Price: US $84.96

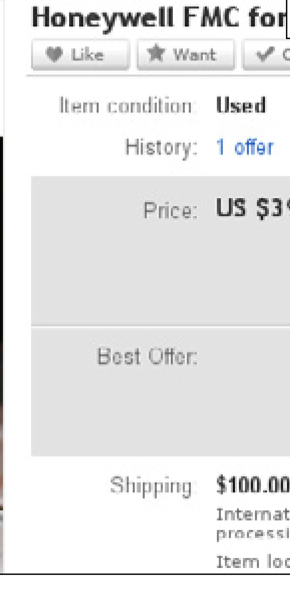
Best Offer:

THALES

Honeywell

Key advantages

he PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.


Honeywell FMC for

Like | Want | Own

Item condition: Used

History: 1 offer

Price: US $399.

Best Offer:

Shipping: $100.00 Econom

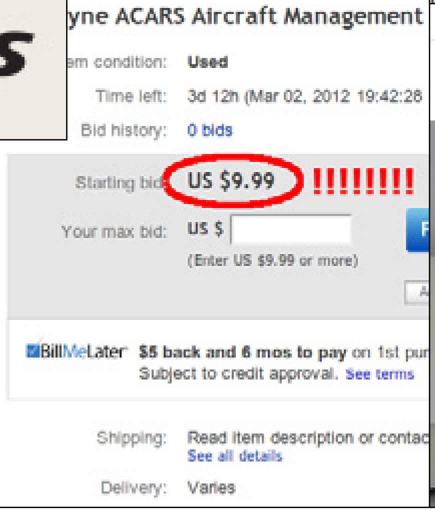
International items processing and ad

Item location: Cas United S

A truly effecti Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.

Rockwell Collins

Building trust every day


yne ACARS Aircraft Management

em condition: Used

Time left: 3d 12h (Mar 02, 2012 19:42:28

Bid history: 0 bids

Starting bid: US $9.99 !!!!!!!!

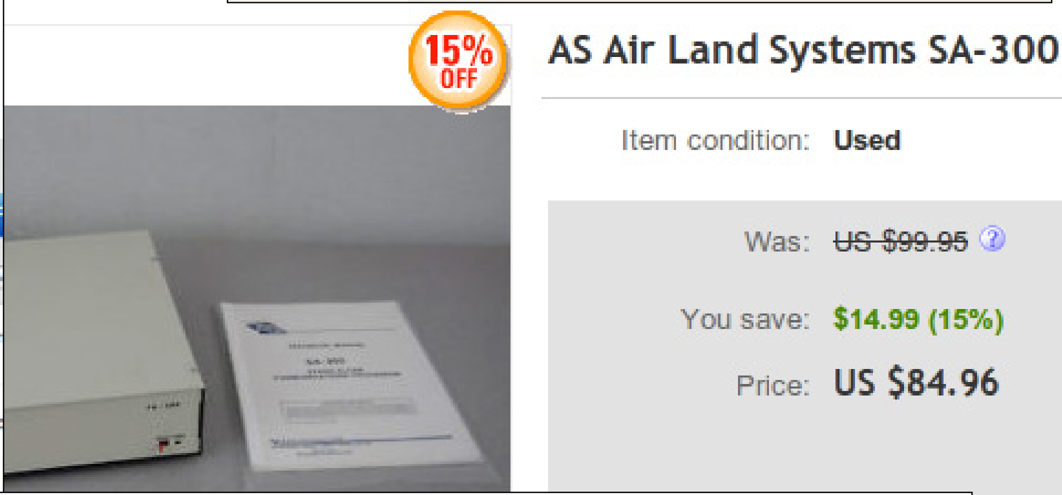
Your max bid: US $

(Enter US $9.99 or more)

BillMeLater $5 back and 6 mos to pay on 1st pur Subject to credit approval. See terms

Shipping: Read item description or contac See all details

Delivery: Varies


15% OFF

AS Air Land Systems SA-300

Item condition: Used

Was: ~~US $99.95~~

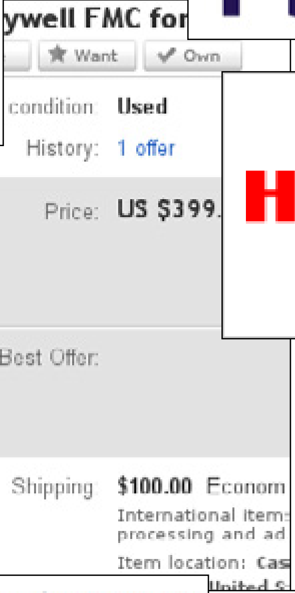
You save: $14.99 (15%)

Price: US $84.96

Honeywell's CMUs and ATSU AOC products are supported by a ground based tool called Airsim. The Airsim tool is a PC-based program that is designed to simulate a datalink system. The Airsim incorporates over 95% of the actual CMU and ATSU AOC software. This allows it

Honeywell offers tools using actual aircraft FMS code…for your genuine training experience

Honeywell's PC-FMS™ free play software provides simulation based on actual flight code software.



ywell FMC for

★ Want ✓ Own

condition: Used

History: 1 offer

Price: US $399.

Best Offer:

Shipping: $100.00 Econom

International item

processing and ad

Item location: Cas

United S

THALES

Honeywell

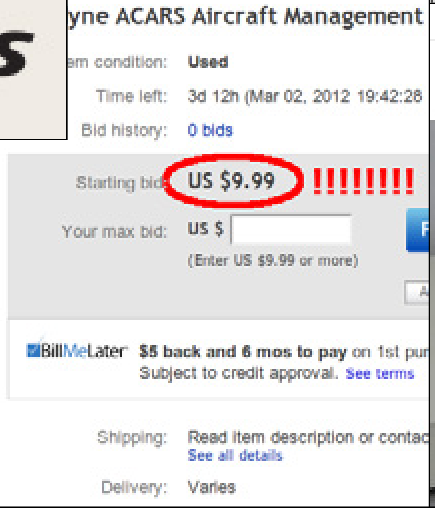
Key advantages

The PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.

A truly effecti
Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.

Rockwell Collins

Building trust every day



yne ACARS Aircraft Management

em condition: Used

Time left: 3d 12h (Mar 02, 2012 19:42:28

Bid history: 0 bids

Starting bid: US $9.99 !!!!!!!!

Your max bid: US $

(Enter US $9.99 or more)

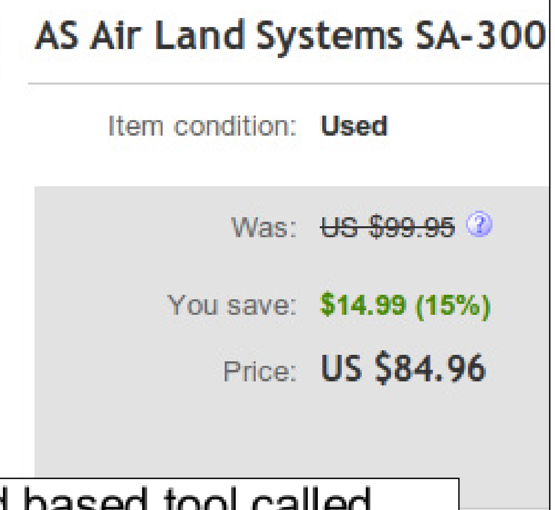
BillMeLater $5 back and 6 mos to pay on 1st pur

Subject to credit approval. See terms

Shipping: Read item description or contac

See all details

Delivery: Varies



AS Air Land Systems SA-300

Item condition: Used

Was: ~~US $99.95~~

You save: $14.99 (15%)

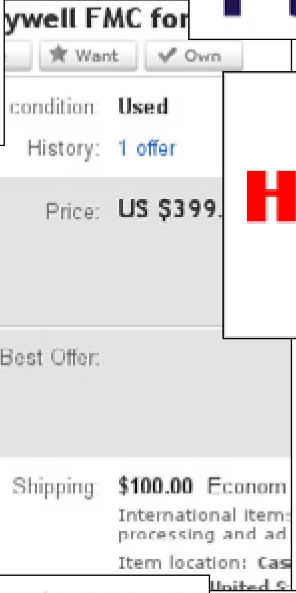
Price: US $84.96

Honeywell's CMUs and ATSU AOC products are supported by a ground based tool called Airsim. The Airsim tool is a PC-based program that is designed to simulate a datalink system. The Airsim incorporates over 95% of the actual CMU and ATSU AOC software. This allows it

n runs professionals

Honeywell offers tools using actual aircraft FMS code…for your genuine training experience

Honeywell's PC-FMS™ free play software provides simulation based on actual flight code software.



ywell FMC for

★ Want ✓ Own

condition: **Used**

History: 1 offer

Price: **US $399.**

Best Offer:

Shipping: **$100.00** Econom

International item processing and ad

Item location: Cas United S

THALES

Honeywell

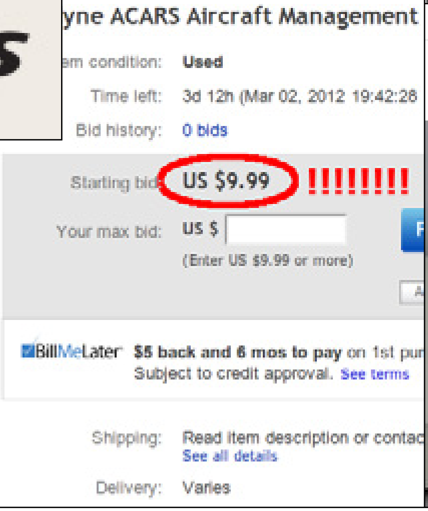
Key advantages

he PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.

A truly effecti Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.

Rockwell Collins

Building trust every day



yne ACARS Aircraft Management

em condition: **Used**

Time left: 3d 12h (Mar 02, 2012 19:42:28

Bid history: 0 bids

Starting bid: **US $9.99** !!!!!!!!

Your max bid: US $

(Enter US $9.99 or more)

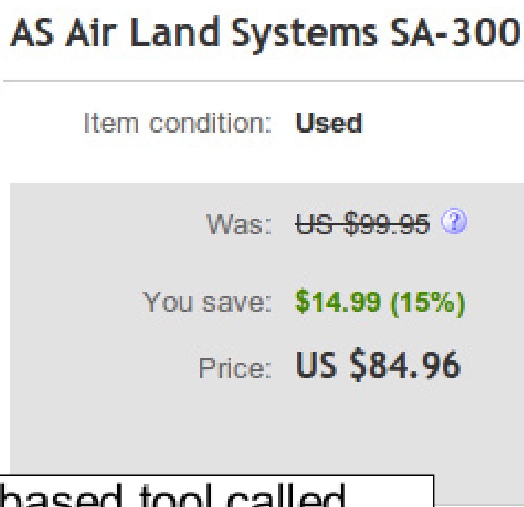
BillMeLater **$5 back and 6 mos to pay** on 1st pur

Subject to credit approval. See terms

Shipping: Read item description or contac

See all details

Delivery: Varies



AS Air Land Systems SA-300

Item condition: **Used**

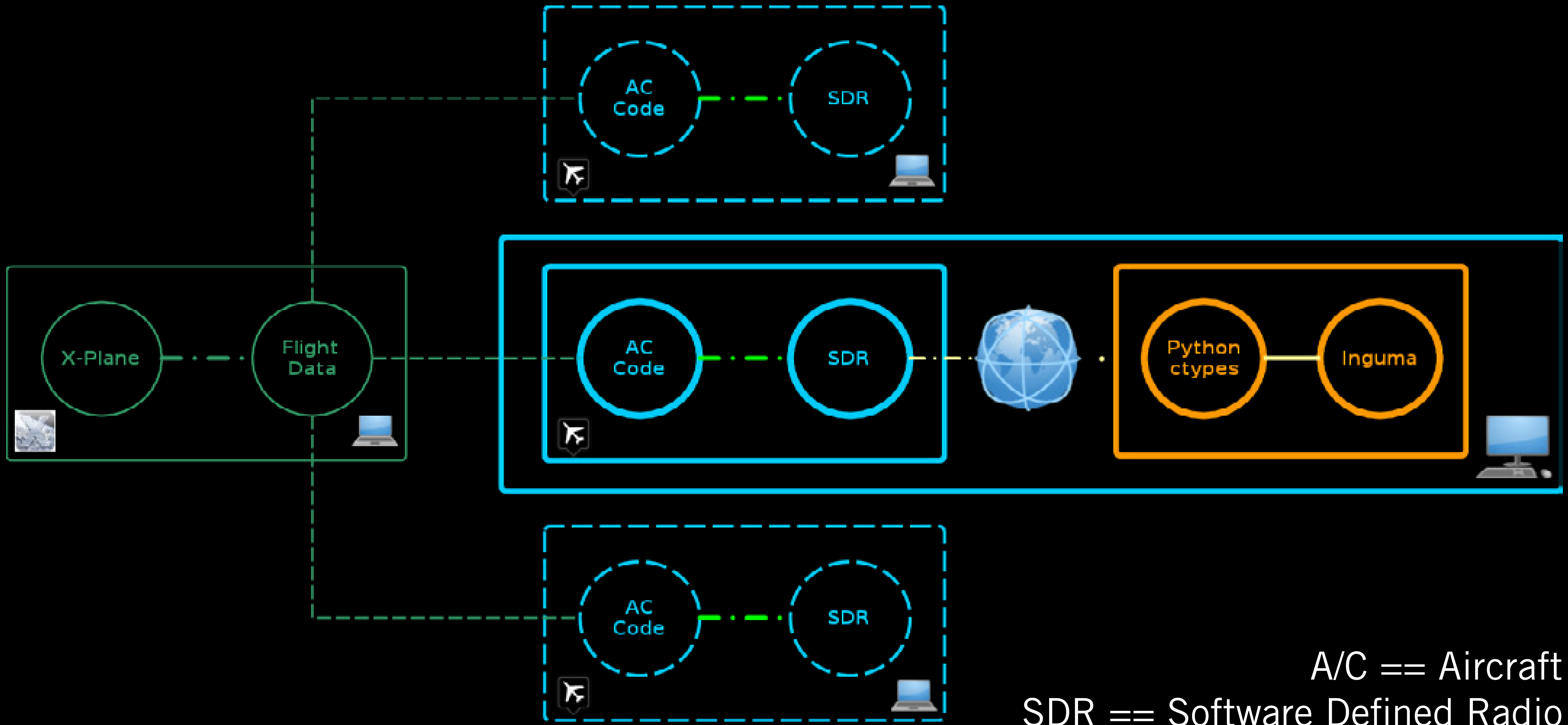
Was: ~~US $99.95~~

You save: **$14.99 (15%)**

Price: **US $84.96**

Honeywell's CMUs and ATSU AOC products are supported by a ground based tool called Airsim. The Airsim tool is a PC-based program that is designed to simulate a datalink system. The Airsim incorporates over 95% of the actual CMU and ATSU AOC software. This allows it

The Lab

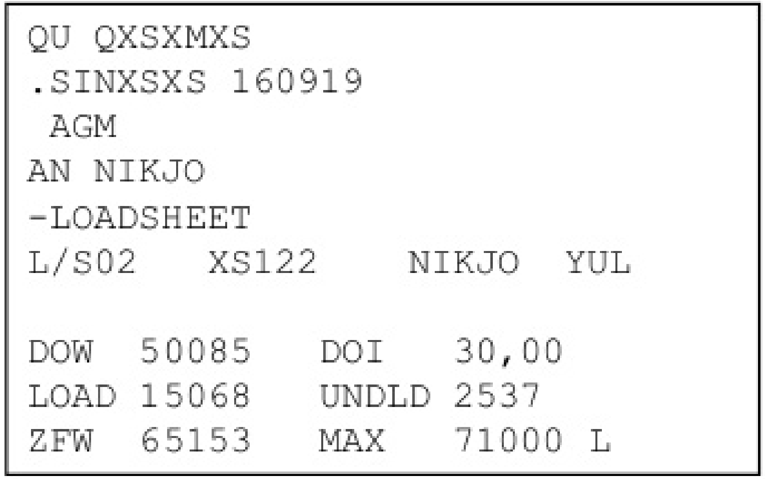


A/C == Aircraft
SDR == Software Defined Radio

The Lab

FMS vulnerabilities

- Many different data types to upload
- Many FMS manufacturers, models and versions.
- Architectures: PPC (Lab x86)
- Language: mostly ADA (old ones)
- SO – RTOS realm:
  - DeOS
  - VxWorks
- ACARS:
  - ACARS datalink allows real time (avg of 11s delay) data transmission
  - Size: Max 220 chars * 16 blocks :S

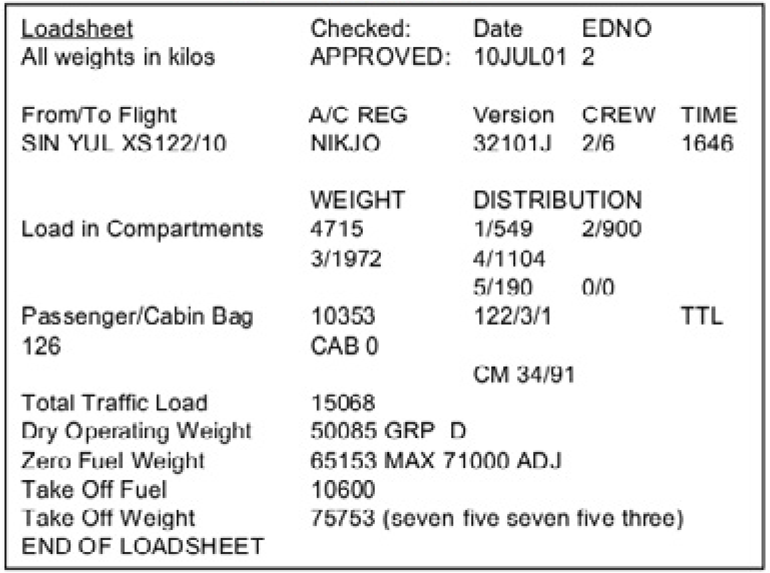


```
QU QXSXMXS
.SINXSXS 160919
 AGM
AN NIKJO
-LOADSHEET
L/S02   XS122    NIKJO  YUL

DOW  50085   DOI   30,00
LOAD 15068   UNDLD 2537
ZFW  65153   MAX   71000 L
```

ACARS encoded message

EDP* Loadsheet



Loadsheet	Checked:	Date	EDNO	
All weights in kilos	APPROVED:	10JUL01	2	
From/To Flight	A/C REG	Version	CREW	TIME
SIN YUL XS122/10	NIKJO	32101J	2/6	1646
	WEIGHT	DISTRIBUTION		
Load in Compartments	4715	1/549	2/900	
	3/1972	4/1104		
		5/190	0/0	
Passenger/Cabin Bag	10353	122/3/1		TTL
126	CAB 0			
		CM 34/91		
Total Traffic Load	15068			
Dry Operating Weight	50085 GRP D			
Zero Fuel Weight	65153 MAX 71000 ADJ			
Take Off Fuel	10600			
Take Off Weight	75753 (seven five seven five three)			
END OF LOADSHEET				

ACARS Messages during flight

Dispatch, Operations, Maintenance, Engineering, Catering, Customer Service

Taxi	Take-Off	Departure	En Route	Approach	Land	Taxi
From A/C OUT Link Test Clock Update Delay Reports To A/C PDC, and ATIS Weight and Balance Airport Analysis V-Speeds Flight-Plan, Loaf FMC	From A/C OFF	From A/C Engine Data To A/C Flight Plan Update Weather Reports	From A/C Position Reports Weather Reports Delay Info/ETA Voice Request Engine Information Maintenance Reports To A/C ATC Oceanic Clearance Weather Reports Reclearance Ground Voice Request	From A/C Catering Requests Gate Requests ETA Special Requests Engine Information Maintenance Reports To A/C Gate Assignment Connecting Gates Pax and Crew ATIS	From A/C ON	From A/C IN Fuel Information Crew Information Fault Data from CMC

http://www.sita.aero/file/3744/Aircom Ekaterinburg - Oct 09 ENG.pdf

HITBSECCONF2013 amsterdam

THE FOURTH ANNUAL HITB SECURITY CONFERENCE IN EUROPE

Demo

HITBSECCONF2013 amsterdam

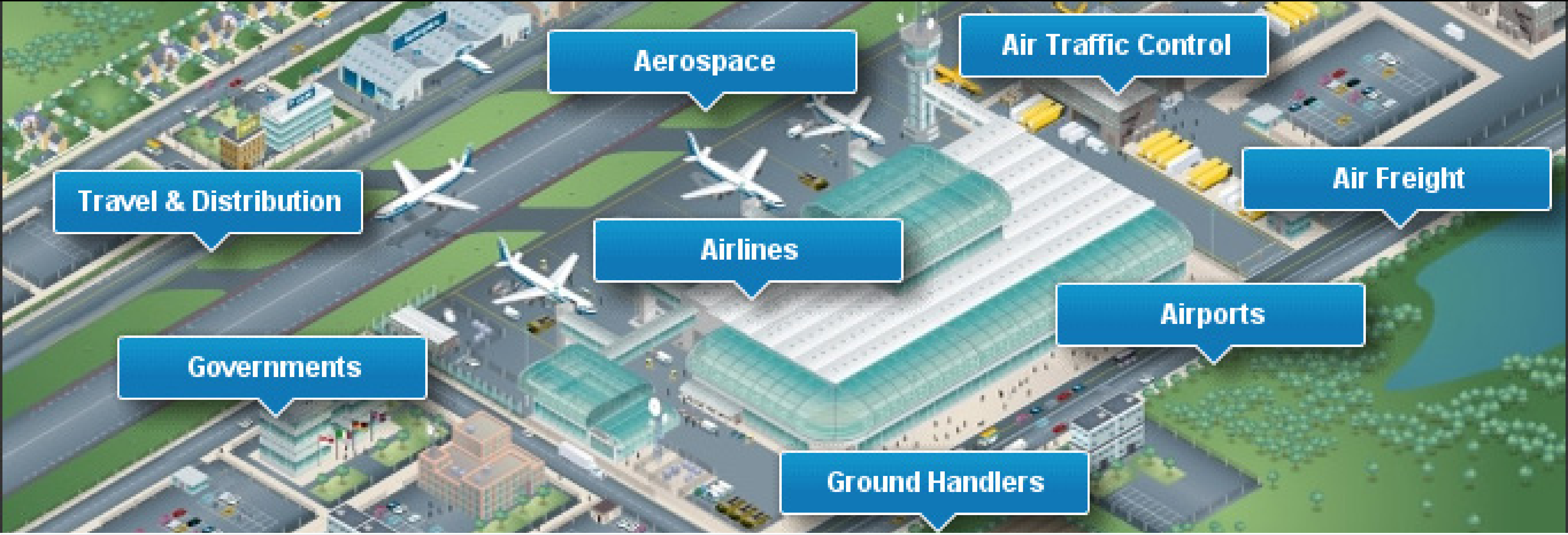
THE FOURTH ANNUAL HITB SECURITY CONFERENCE IN EUROPE

Part II

The $PATH to exploit

SITA/ARINC

- ✈ Société Internationale de Télécommunications Aéronautiques (SITA)
  - » IT and telecommunication services to the air transport industry.
  - » 90% of the world's airline business.
- ✈ Aeronautical Radio, Incorporated (ARINC)
  - » Major provider of transport communications and systems solutions:
  - » Aviation, airports, defense, government, healthcare, networks, security, and transportation.



Access methods:

- ✈ E-Mail Clients
  - » SMTP / POP3
  - » Lotus Notes
- ✈ Desktop Apps, connection over:
  - » X.25
  - » TCP
  - » MQ Series (IBM WebSphere)
  - » MSMQ (Microsoft queues)
  - » MS SQL Database
  - » ORACLE Database
- ✈ Web App
- ✈ Mobility
  - » Mobile App
  - » Pager/SMS
  - » Printer
  - » SDK
  - » Stations

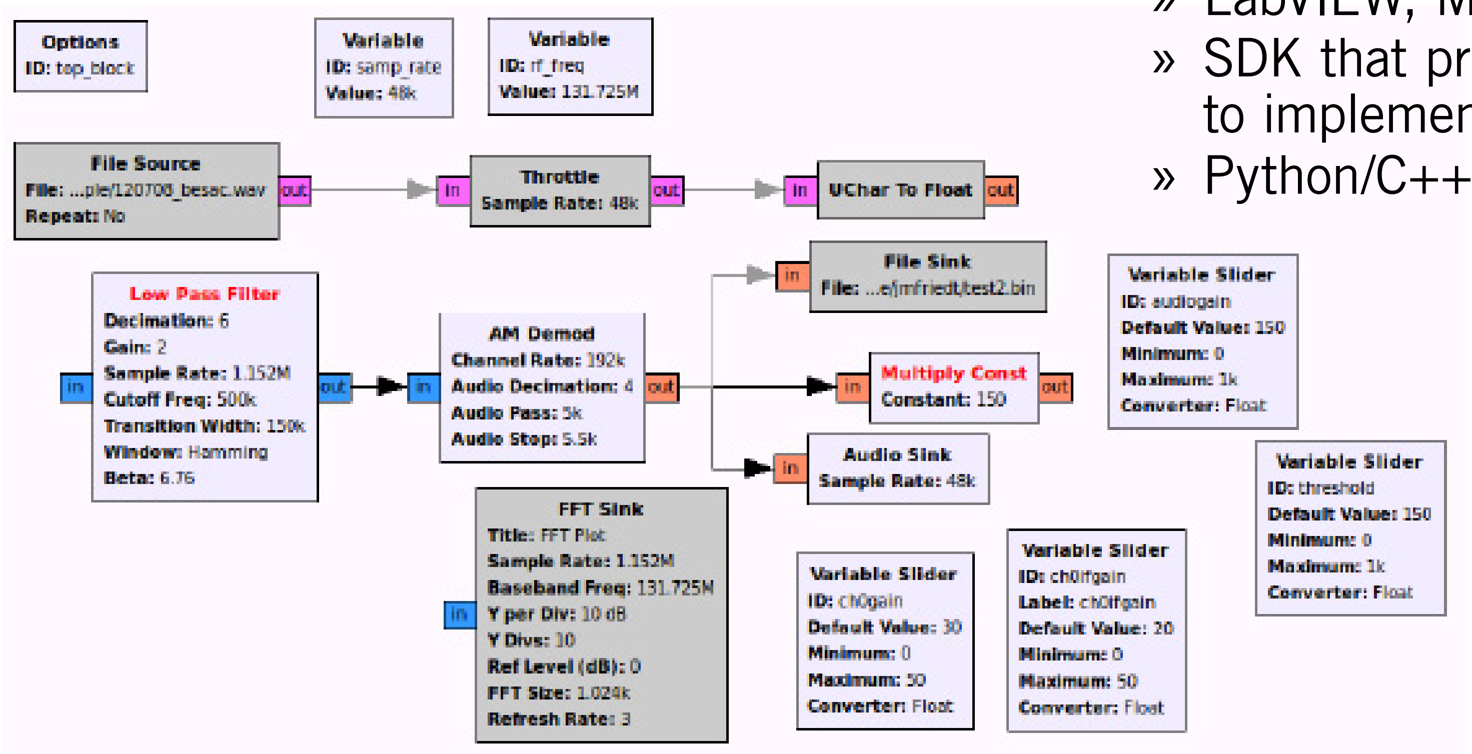
Be my guest...

What could possibly go WRONG?

http://www.sita.aero/file/3744/Aircom Ekaterinburg - Oct 09 ENG.pdf

Software Defined Radio 101

- ✈ A radio communication system where components that have been typically implemented in hardware are instead implemented by means of software.
- ✈ HW: USRP1/USRP2
  - » Universal Software Radio Peripheral
  - » USB or Gigabit Ethernet link
- ✈ SW: GNU Radio
  - » LabVIEW, MATLAB and Simulink
  - » SDK that provides signal processing blocks to implement software radios.
  - » Python/C++



Options
ID: top_block

Variable
ID: samp_rate
Value: 48k

Variable
ID: rf_freq
Value: 131.725M

File Source
File: ...ple/120708_besac.wav
Repeat: No

Throttle
Sample Rate: 48k

UChar To Float

Low Pass Filter
Decimation: 6
Gain: 2
Sample Rate: 1.152M
Cutoff Freq: 500k
Transition Width: 150k
Window: Hamming
Beta: 6.76

AM Demod
Channel Rate: 192k
Audio Decimation: 4
Audio Pass: 5k
Audio Stop: 5.5k

File Sink
File: ...e/jmfriedt/test2.bin

Multiply Const
Constant: 150

Audio Sink
Sample Rate: 48k

FFT Sink
Title: FFT Plot
Sample Rate: 1.152M
Baseband Freq: 131.725M
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
FFT Size: 1.024k
Refresh Rate: 3

Variable Slider
ID: audiogain
Default Value: 150
Minimum: 0
Maximum: 1k
Converter: Float

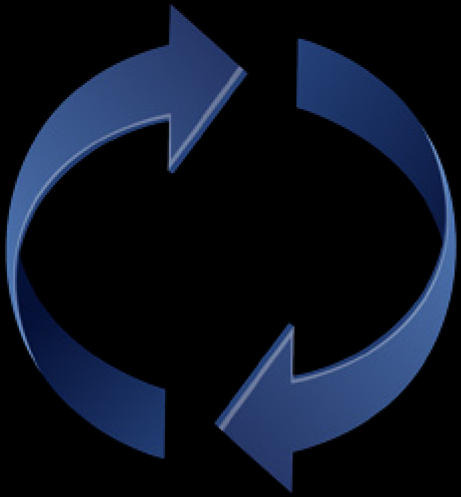
Variable Slider
ID: threshold
Default Value: 150
Minimum: 0
Maximum: 1k
Converter: Float

Variable Slider
ID: ch0gain
Default Value: 30
Minimum: 0
Maximum: 50
Converter: Float

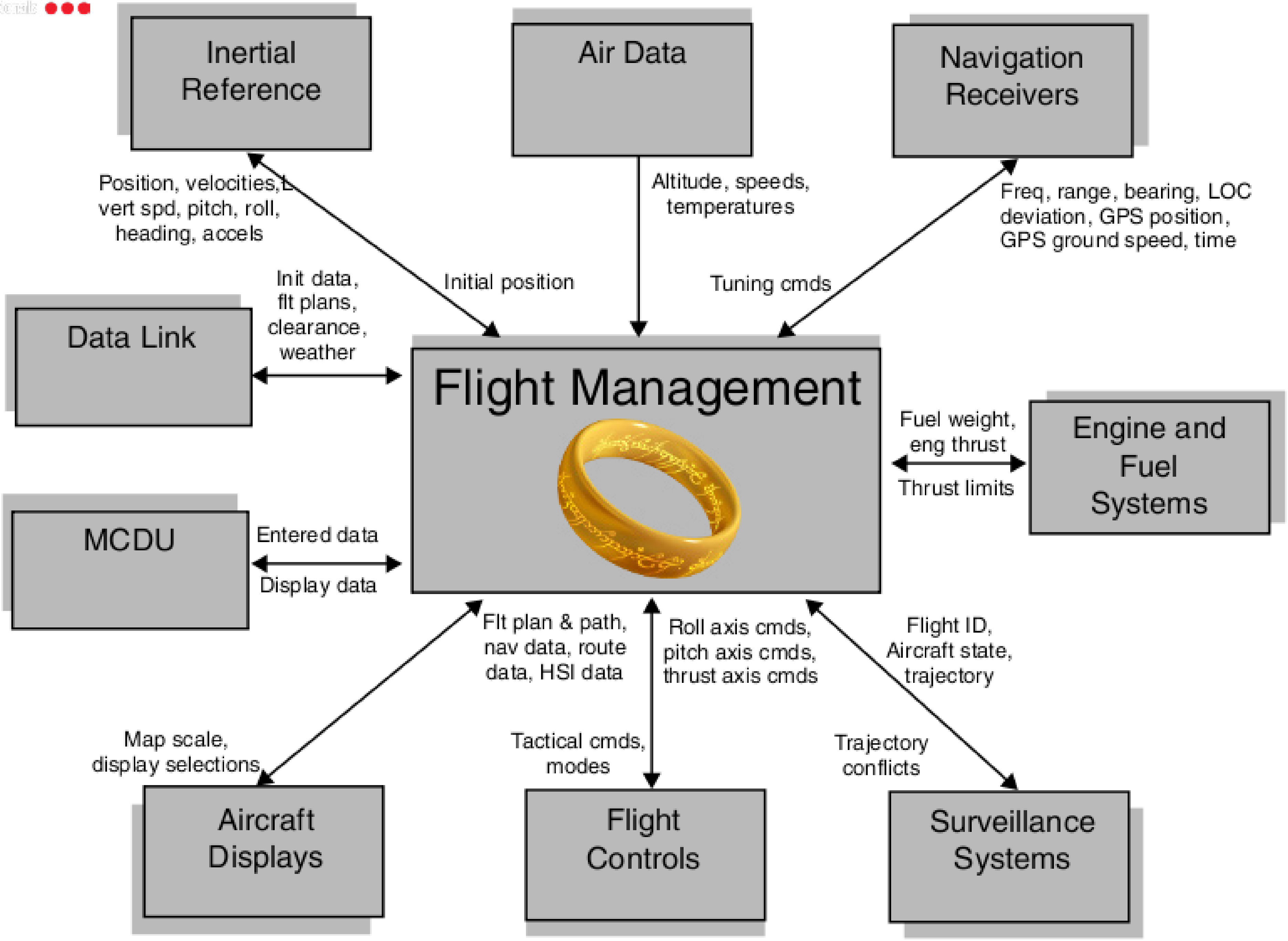
Variable Slider
ID: ch0ifgain
Label: ch0ifgain
Default Value: 20
Minimum: 0
Maximum: 50
Converter: Float

Post-Exploitation

- ✈ Consolidation
  - » Protection & Monitoring
- ✈ Communication
  - » Two way communication
- ✈ Expansion
  - » Other systems
  - » Back to Discovery



"Smiths Aerospace chose Wind River Systems' VxWorks 653 RTOS for the B787's common core system (CCS), a cabinet that will host ***80 to 100 applications****, including Honeywell's* ***FMS*** *and* ***health management software*** *and Collins'* ***crew alerting and display management software****"*



Inertial Reference

Air Data

Navigation Receivers

Position, velocities, vert spd, pitch, roll, heading, accels

Initial position

Altitude, speeds, temperatures

Freq, range, bearing, LOC deviation, GPS position, GPS ground speed, time

Tuning cmds

Data Link

Init data, flt plans, clearance, weather

Flight Management

Fuel weight, eng thrust

Thrust limits

Engine and Fuel Systems

MCDU

Entered data

Display data

Flt plan & path, nav data, route data, HSI data

Roll axis cmds, pitch axis cmds, thrust axis cmds

Flight ID, Aircraft state, trajectory

Map scale, display selections

Tactical cmds, modes

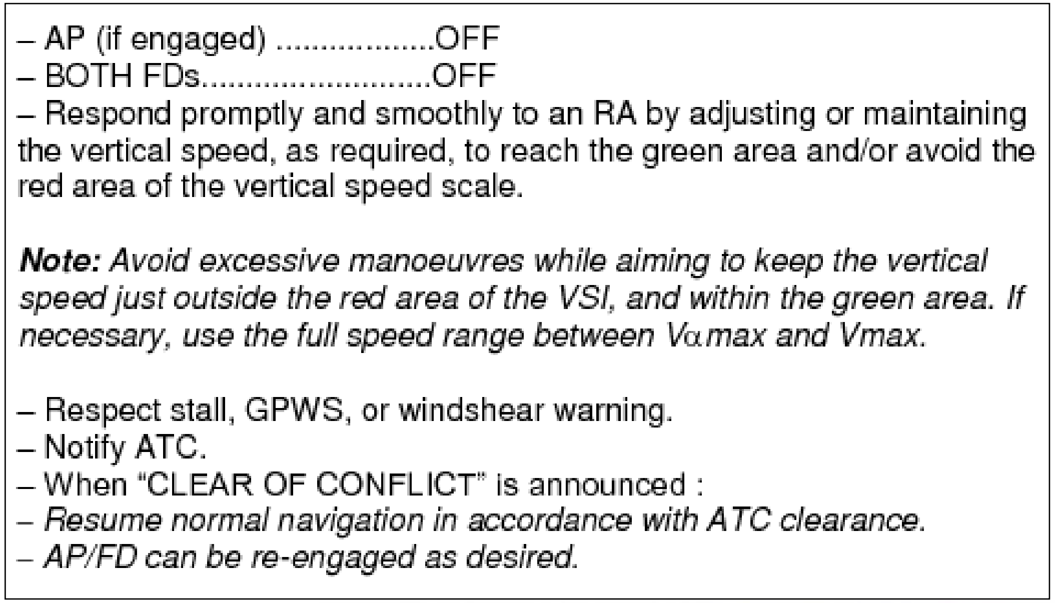
Trajectory conflicts

Aircraft Displays

Flight Controls

Surveillance Systems

Aircraft Post-Exploitation



– AP (if engaged) ....OFF
– BOTH FDs.........................OFF
– Respond promptly and smoothly to an RA by adjusting or maintaining the vertical speed, as required, to reach the green area and/or avoid the red area of the vertical speed scale.

***Note:** Avoid excessive manoeuvres while aiming to keep the vertical speed just outside the red area of the VSI, and within the green area. If necessary, use the full speed range between Vαmax and Vmax.*

– Respect stall, GPWS, or windshear warning.
– Notify ATC.
– When "CLEAR OF CONFLICT" is announced :
– *Resume normal navigation in accordance with ATC clearance.*
– *AP/FD can be re-engaged as desired.*

- ✈ Aircraft and Pilots
  - » Predictables
  - » Checklists and procedures
- ✈ Exploiting other comm and nav systems or protocols
- ✈ Planning and timing!
- ✈ C&C
  - » Two way communication
  - » Actions
  - » Limitations

SIMON

- ✈ Why SIMON?
- ✈ Multi-stage payload
- ✈ Control ADS-B/ACARS
  - » Upload via ADS-B/ACARS
- ✈ Persistence
- ✈ Stealthness (No Rootkit)
- ✈ Accept and inject:
  - » FP/DB
  - » Payloads (scripts)
  - » Plugins (code)
  - » Commands
  - » Two way comm

Demo

Conclusions

Remediation
Safety != Security

- Where to start from?
  - NextGen Security
  - On-board systems security audit
- Who is affected?
  - Manufacturers
  - Ground Service Providers
  - Airlines
- We are working with EASA to improve the situation

References

- Aviation 101
  - » http://en.wikipedia.org/wiki/Portal:Aviation
- ADS-B
  - » http://en.wikipedia.org/wiki/Automatic_dependent_surveillance-broadcast
  - » https://www.blackhat.com/html/bh-us-12/bh-us-12-briefings.html#Costin
- ACARS
  - » http://en.wikipedia.org/wiki/Aircraft_Communications_Addressing_and_Reporting_System
  - » http://spench.net/
- FMS
  - » http://en.wikipedia.org/wiki/Flight_management_system
  - » http://www.b737.org.uk/fmc.htm
- SDR
  - » http://en.wikipedia.org/wiki/Software-defined_radio
  - » http://gnuradio.org

THANKS TO:

- ✈ @d0tslash
- ✈ @vierito5
- ✈ @searchio
- ✈ @48bits
- ✈ @kuasar
- ✈ Many others

Hugo Teso

hugo.teso@nruns.com

http://conference.hitb.org/hitbsecconf2013ams/materials/