n runs professionals

HITBSECCONF2013 MALAYSIA

THE ELEVENTH ANNUAL HITB SECURITY CONFERENCE IN ASIA

Digging Deeper into AVIATION SECURITY

Hugo Teso

Safety IS NOT Security

Agenda

Part I

Previously on...

Part II

Faster, Stronger and Higher

Previously on...

PART I

Attack Review

Discovery

✈ADS-B

Gathering

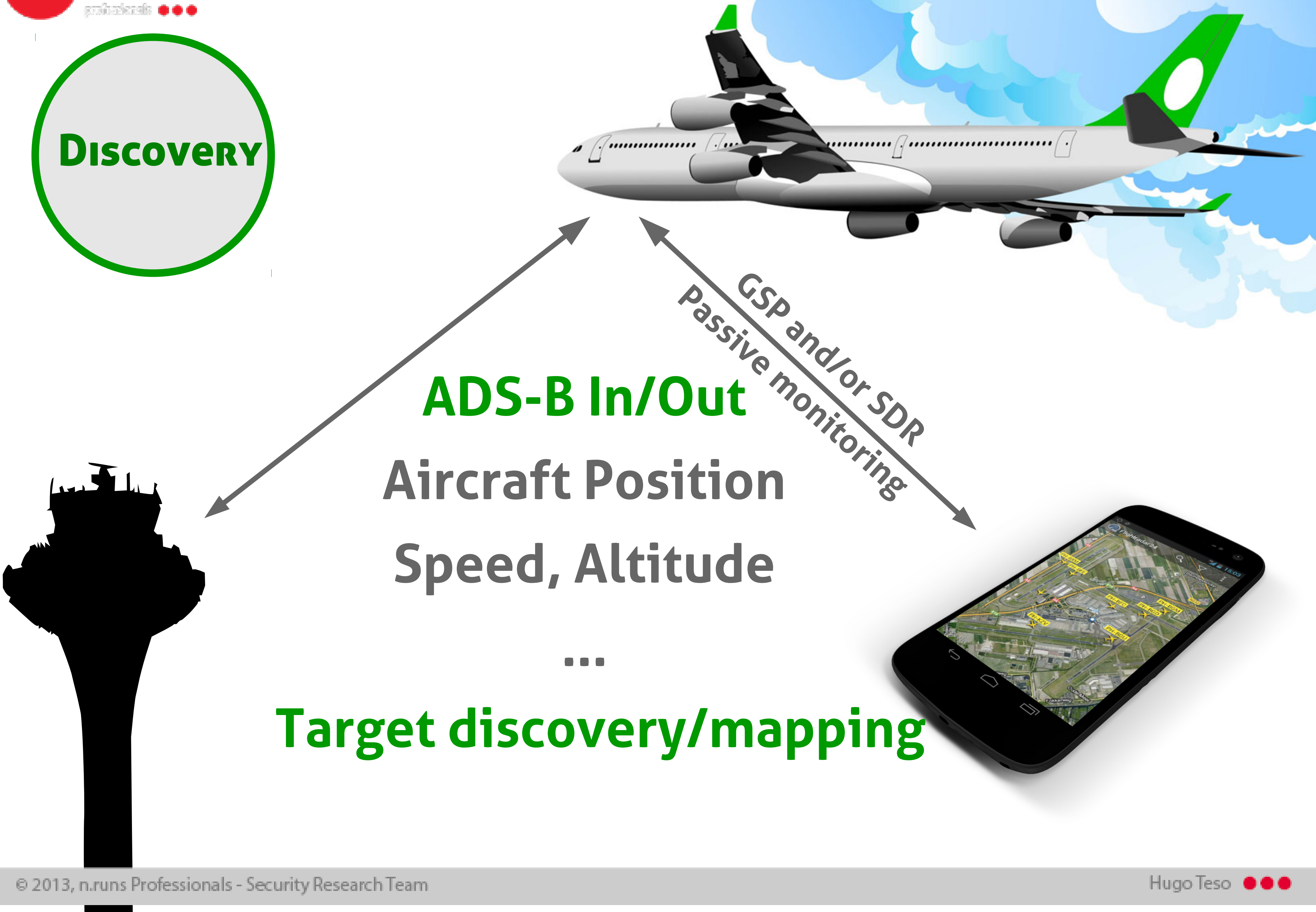
✈ACARS

Exploit

✈SYSTEMS

http://blog.nruns.com/blog/2013/10/14/Aviation-Security-Hugo/

Discovery



ADS-B In/Out

Aircraft Position

Speed, Altitude

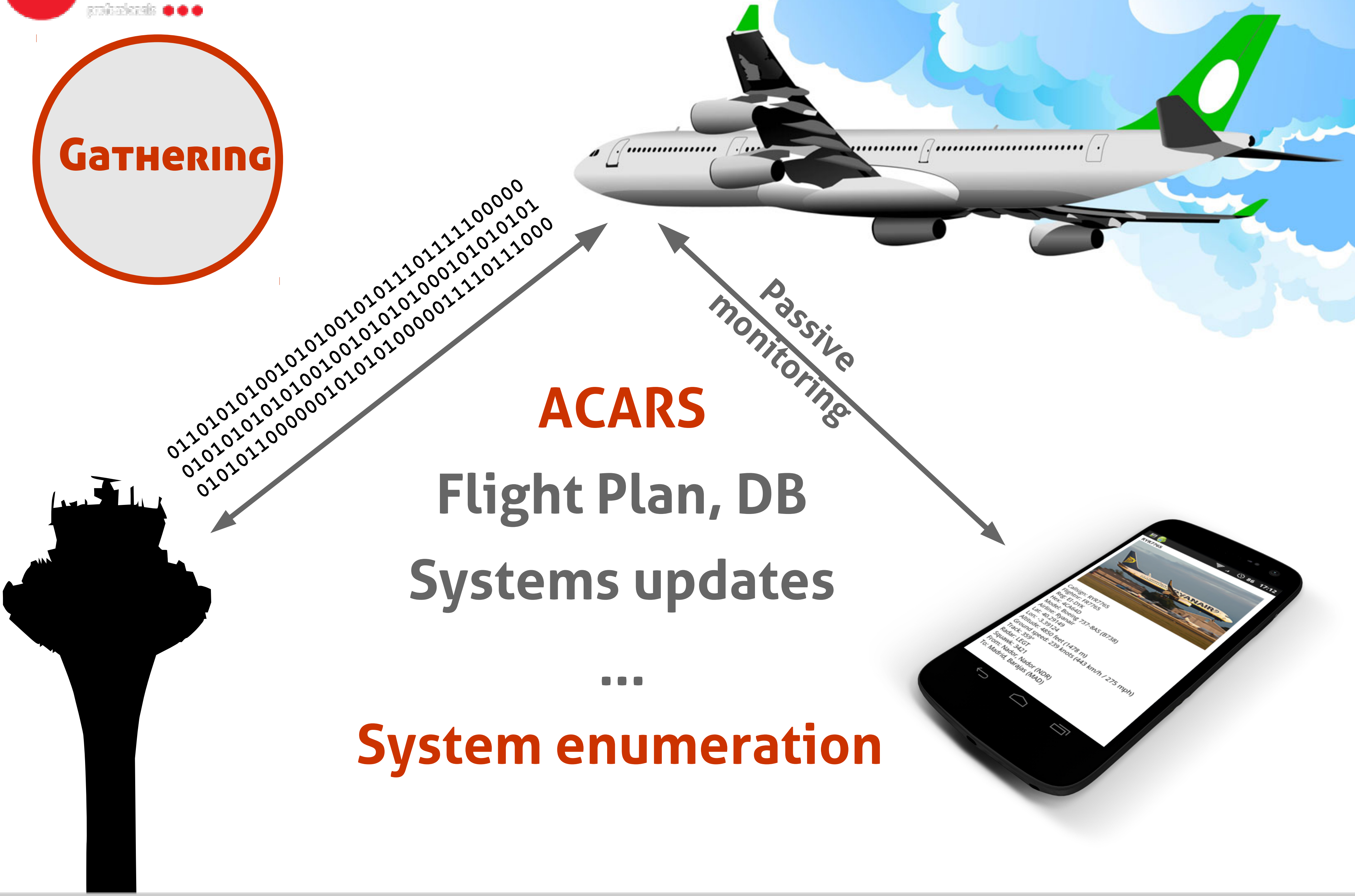
...

Target discovery/mapping

GSP and/or SDR

Passive monitoring

Gathering



RYR7765

Callsign: RYR7765
Flightnr: FR7765
Reg: EI-DYK
Hex: 4CA64D
Model: Boeing 737-8AS (B738)
Airline: Ryanair
Lat: 40.29149
Lon: -3.39124
Altitude: 4850 feet (1478 m)
Ground speed: 239 knots (443 km/h / 275 mph)
Track: 359°
Radar: LEGT
Squawk: 3421
From: Nador, Nador (NDR)
To: Madrid, Barajas (MAD)

ACARS

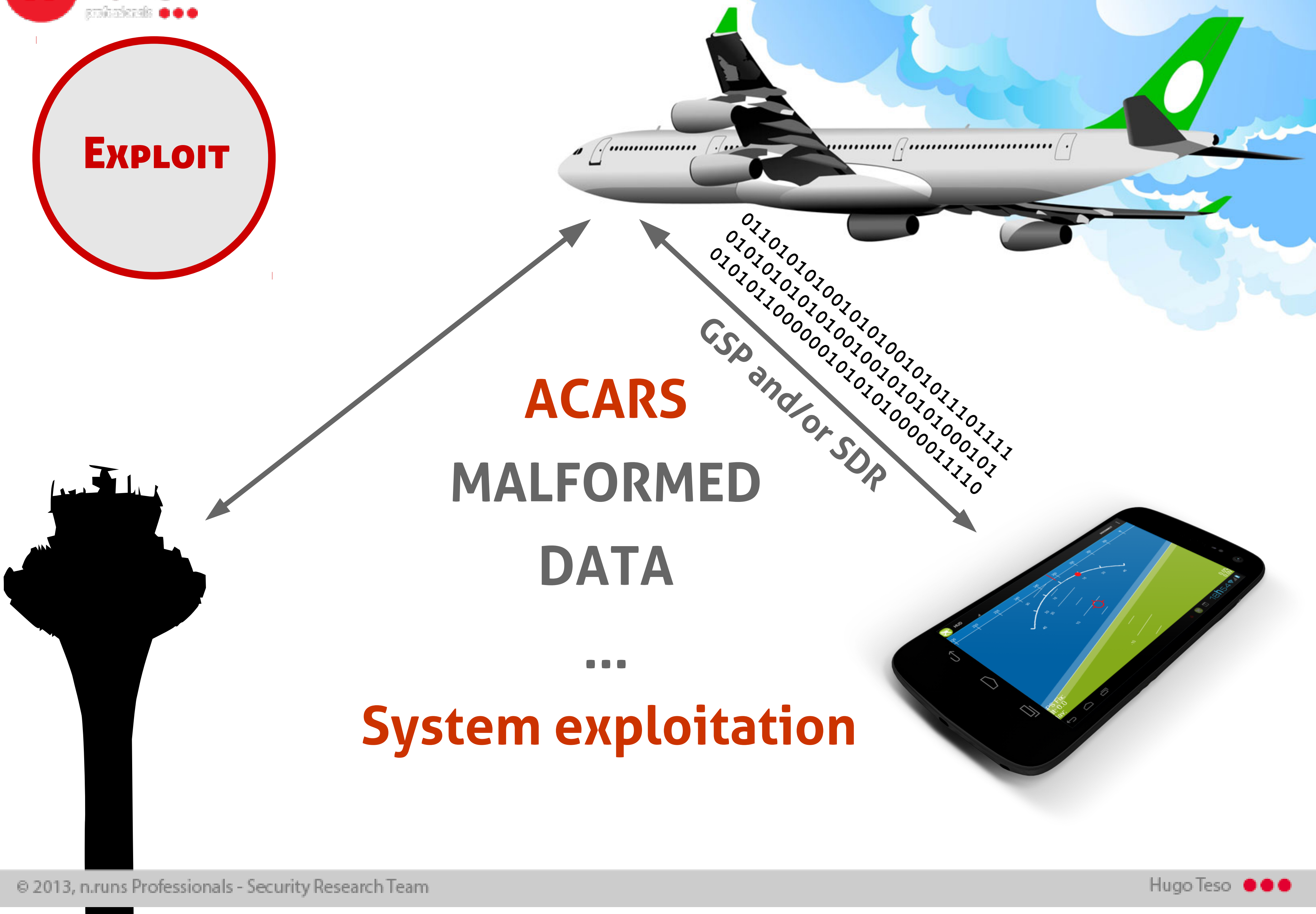
Flight Plan, DB

Systems updates

…

System enumeration

Exploit



ACARS

MALFORMED

DATA

...

System exploitation

GAME OVER

© 2010 WWW.JERSEYIMAGE.CO.UK

ATTACK++

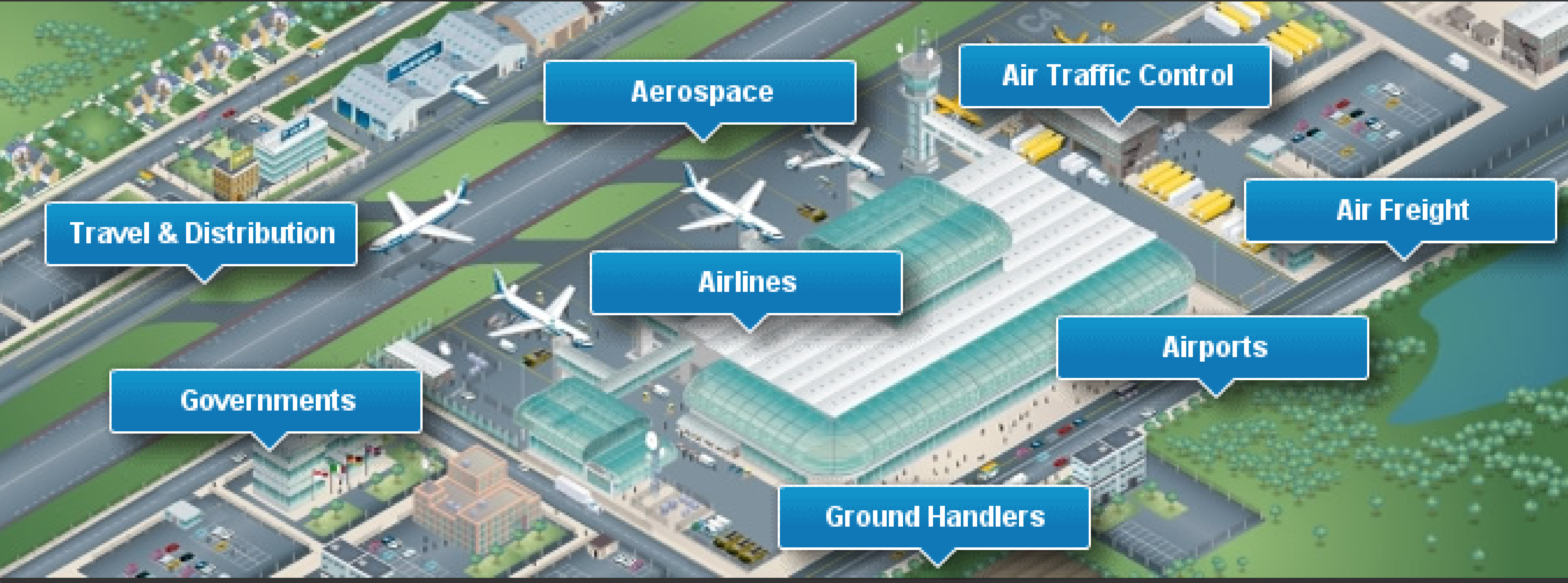
SITA ARINC Honeywell

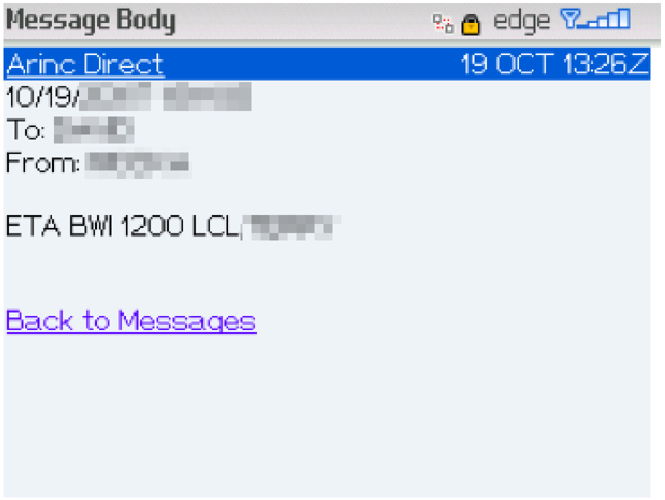
Worldwide targeting

Fewer requirements

Standard technologies

The "glue" of the aviation ecosystem





Message Body edge

Arinc Direct 19 OCT 13:26Z

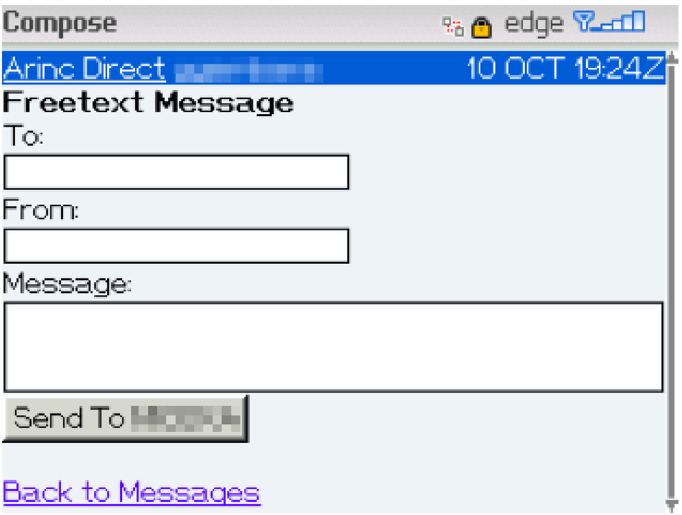
10/19/[redacted]

To: [redacted]

From: [redacted]

ETA BWI 1200 LCL/[redacted]

Back to Messages



Compose edge

Arinc Direct [redacted] 10 OCT 19:24Z

Freetext Message

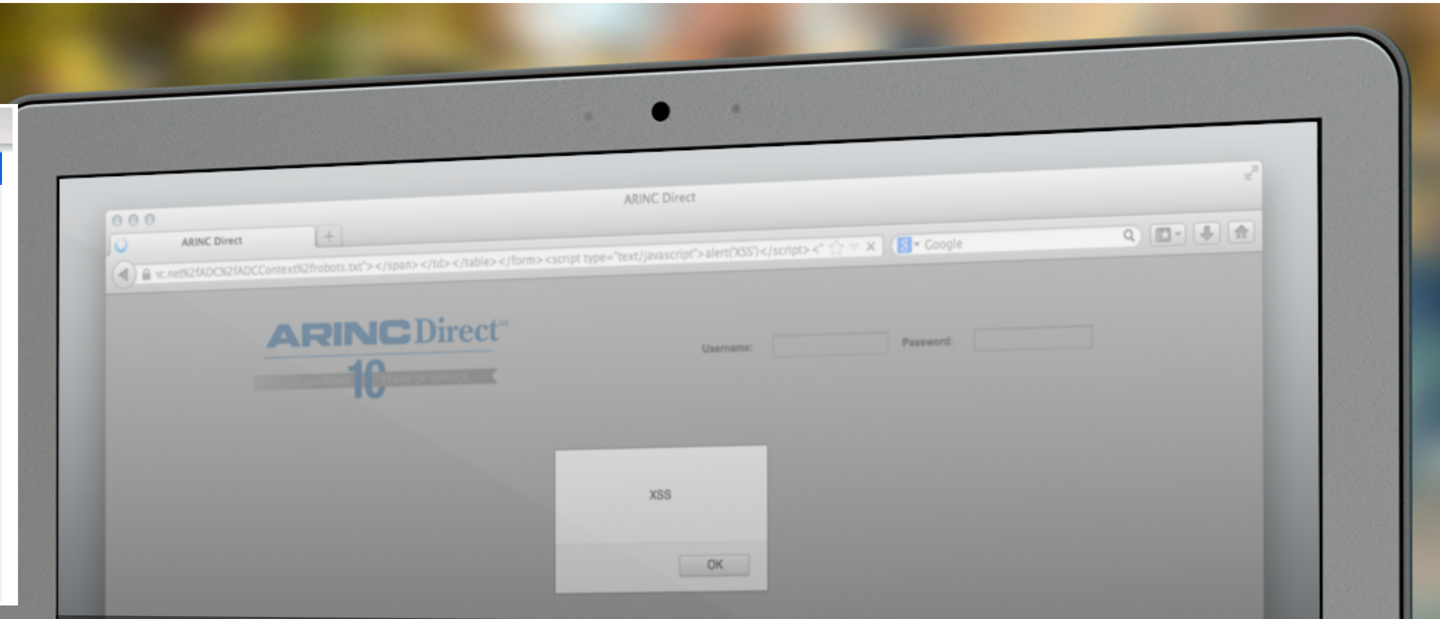
To:

From:

Message:

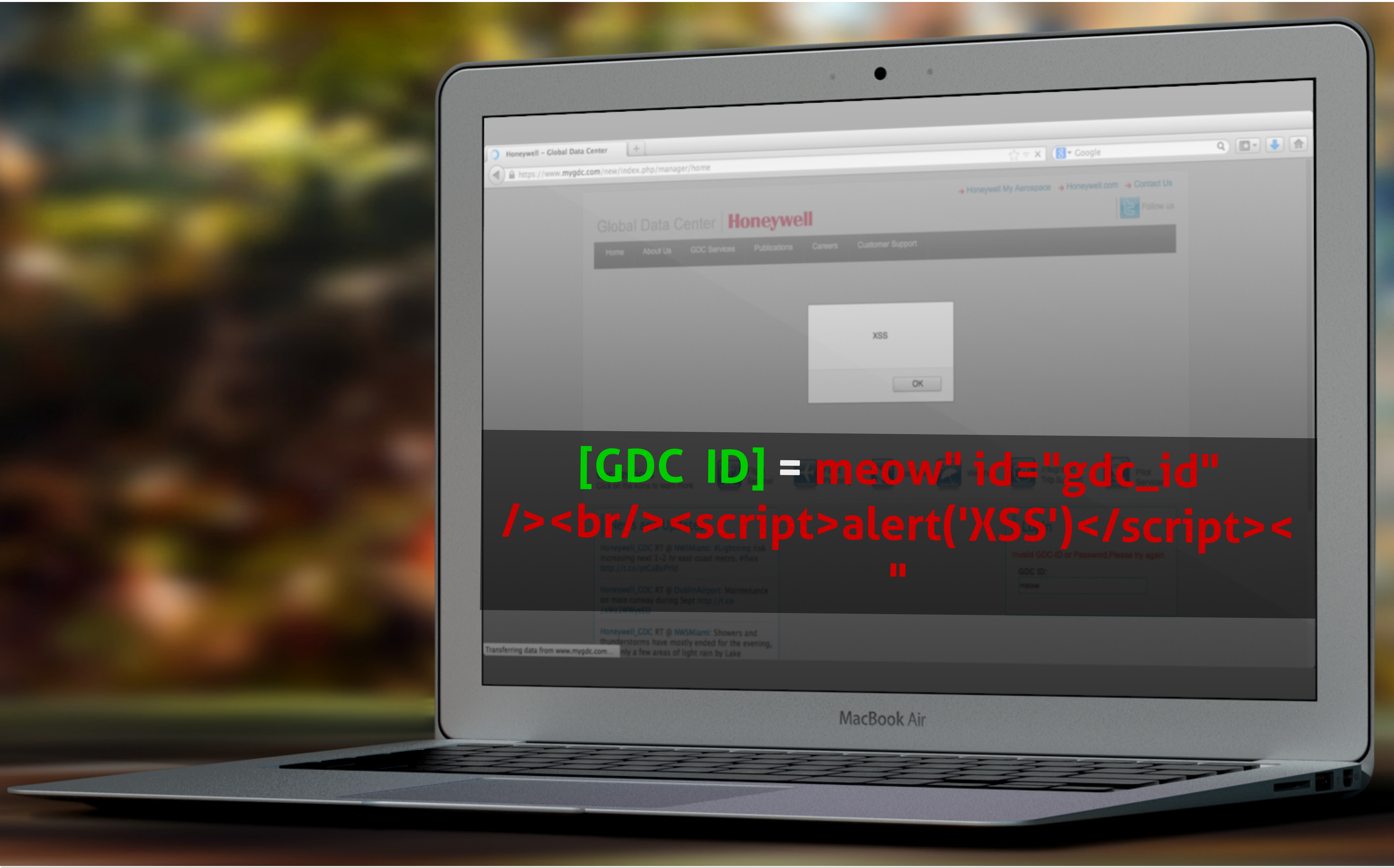
Send To [redacted]

Back to Messages



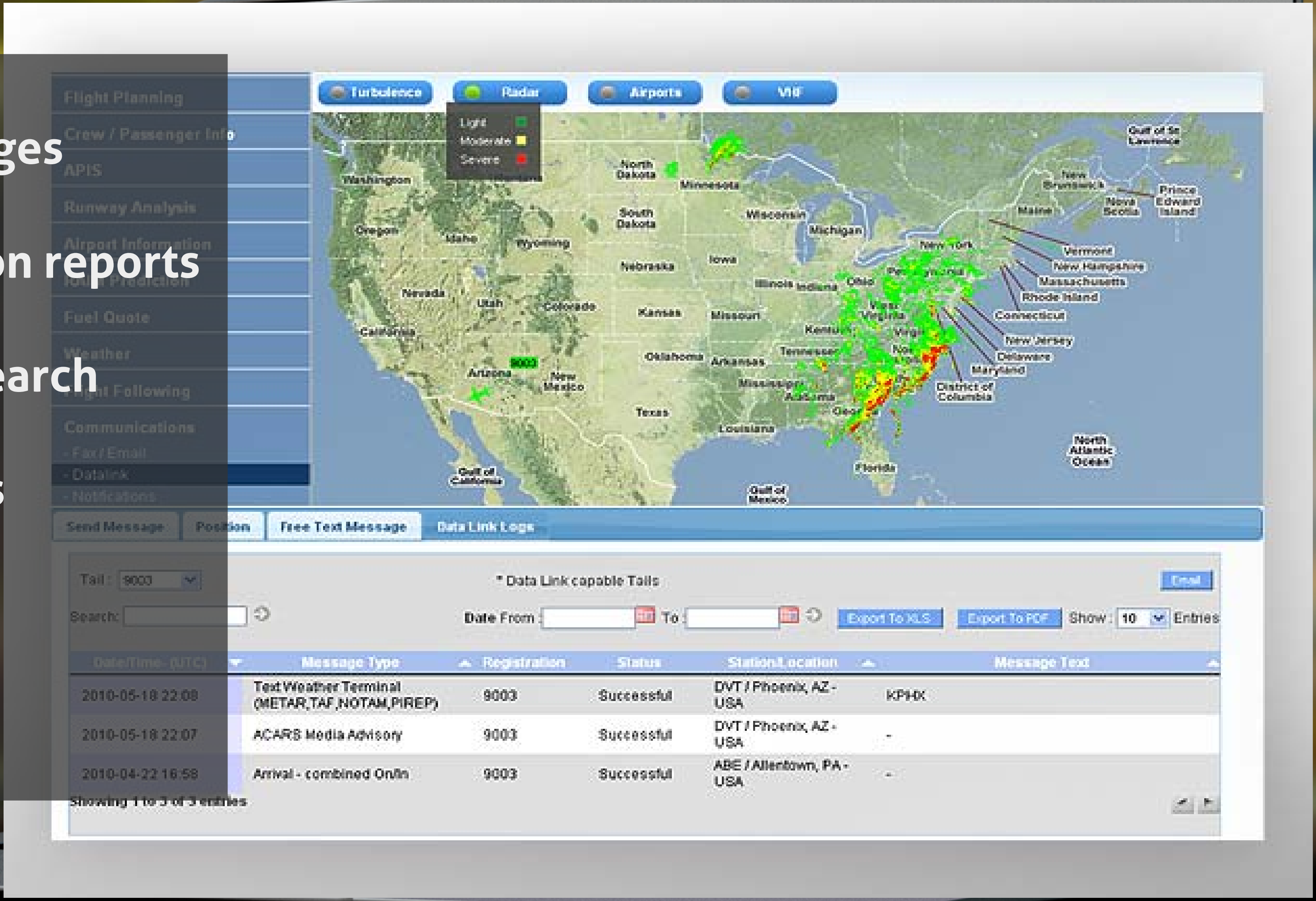
ARINC Direct
ARINC Direct
ıc.net%2fADC%2fADCContext%2frobots.txt"></span></td></table></form><script type="text/javascript">alert('XSS')</script><"
Google
ARINCDirect 10
Username:
Password:
XSS
OK
Read direct.arinc.net
MacBook Air

```
[URL] +
"></span></td></table></form>
<script>alert('XSS')</script><"
```



[GDC ID] = meow" id="gdc_id" /><br/><script>alert('XSS')</script><"

- » Send messages
- » View position reports
- » Advanced search
- » Activity logs
- » Export data
- » ...



Tail : 9003

Search:

* Data Link capable Tails

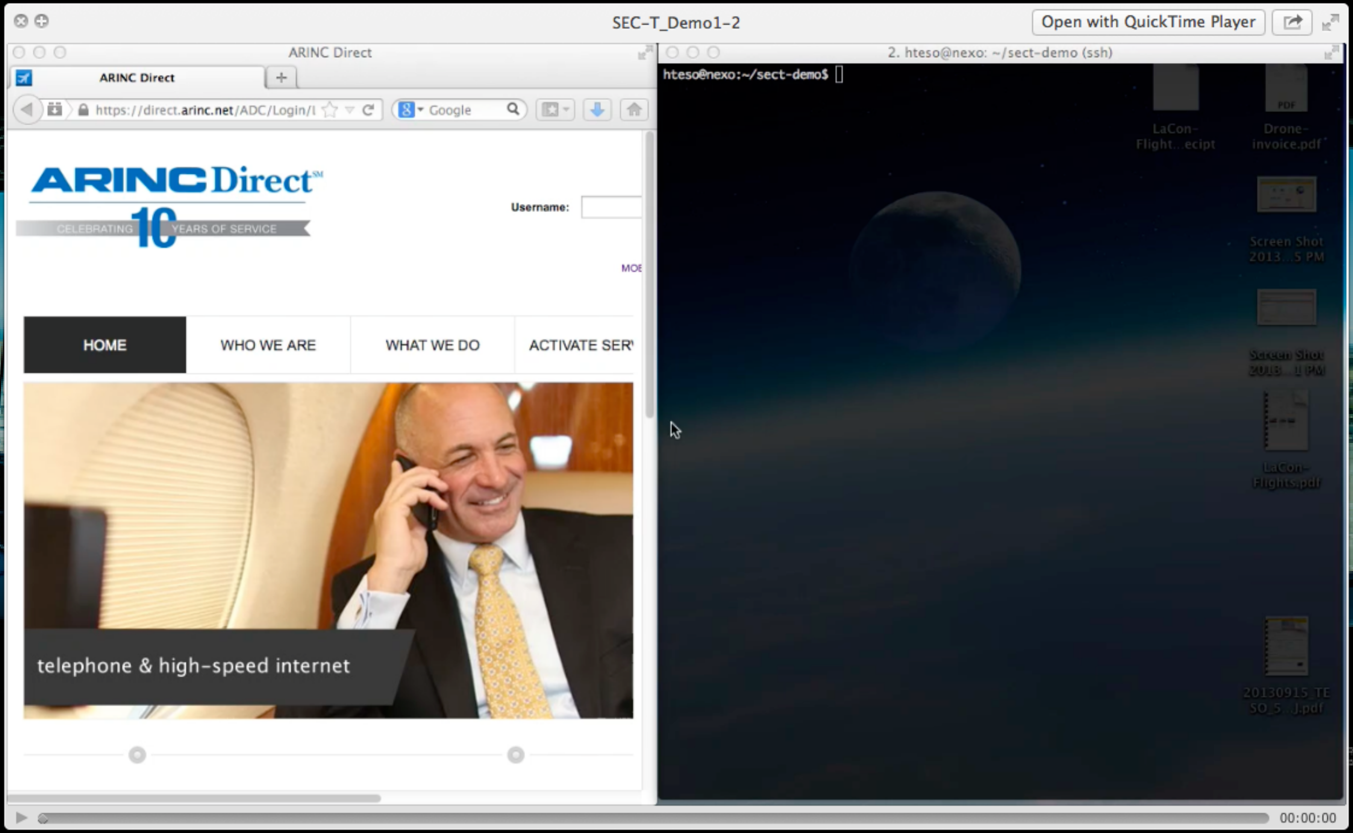
Date From : To :

Show : 10 Entries

Date/Time (UTC)	Message Type	Registration	Status	Station/Location	Message Text
2010-05-18 22:08	Text Weather Terminal (METAR,TAF,NOTAM,PIREP)	9003	Successful	DVT / Phoenix, AZ - USA	KPHX
2010-05-18 22:07	ACARS Media Advisory	9003	Successful	DVT / Phoenix, AZ - USA	-
2010-04-22 16:58	Arrival - combined On/In	9003	Successful	ABE / Allentown, PA - USA	-

Showing 1 to 3 of 3 entries

How Is That Useful?



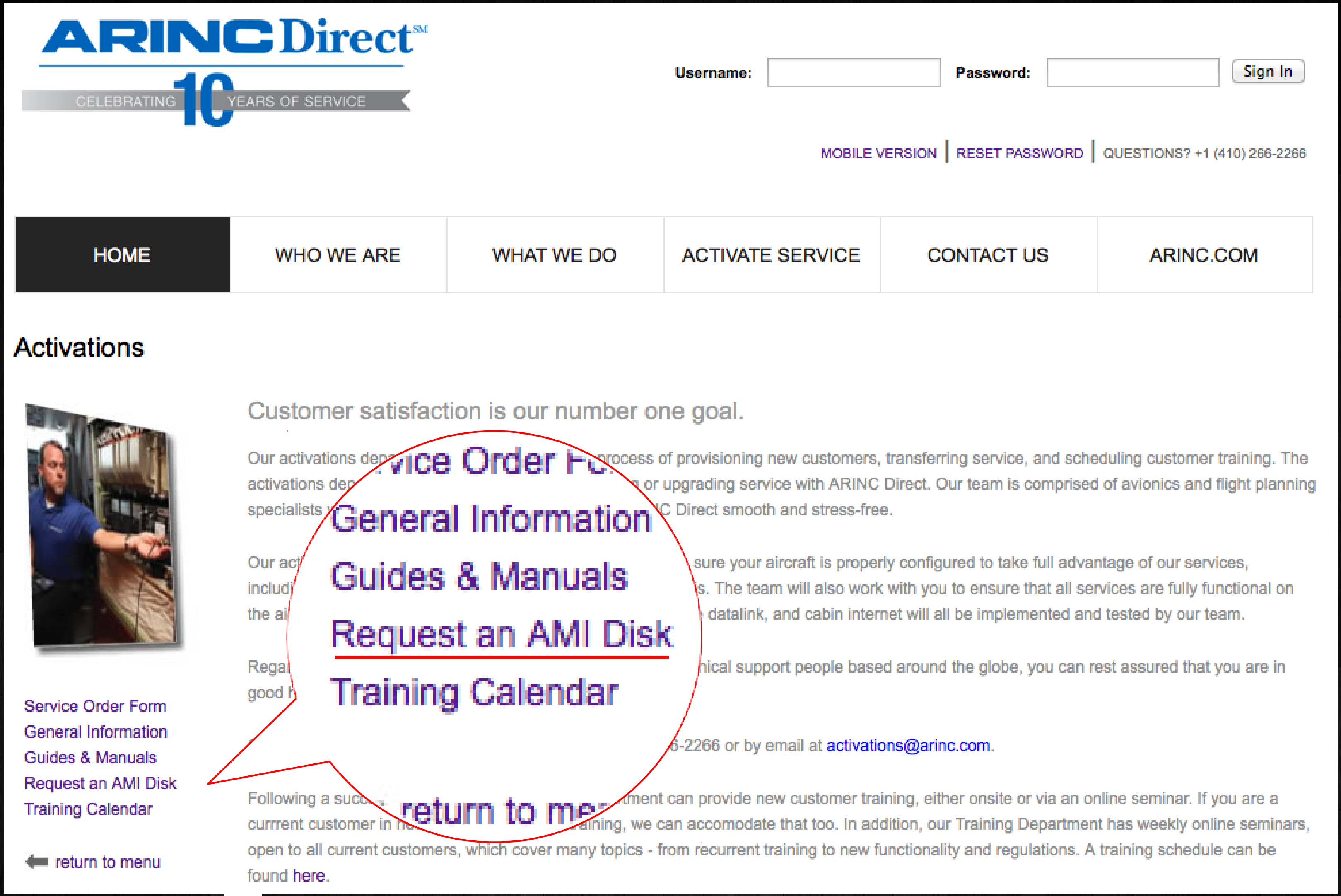
```
hteso@nexo:~/sect-demo$
```

© 2010 WWW.JERSEYIMAGE.CO.UK

DEMO TIME!

Faster Stronger Higher!

PART II



ARINC Direct℠
CELEBRATING 10 YEARS OF SERVICE

Username: ____ Password: ____ Sign In

MOBILE VERSION | RESET PASSWORD | QUESTIONS? +1 (410) 266-2266

HOME | WHO WE ARE | WHAT WE DO | ACTIVATE SERVICE | CONTACT US | ARINC.COM

Activations

Customer satisfaction is our number one goal.

Our activations dep process of provisioning new customers, transferring service, and scheduling customer training. The activations dep or upgrading service with ARINC Direct. Our team is comprised of avionics and flight planning specialists C Direct smooth and stress-free.

Our act sure your aircraft is properly configured to take full advantage of our services, includi s. The team will also work with you to ensure that all services are fully functional on the ai datalink, and cabin internet will all be implemented and tested by our team.

Rega nical support people based around the globe, you can rest assured that you are in good h

6-2266 or by email at activations@arinc.com.

Following a succ ment can provide new customer training, either onsite or via an online seminar. If you are a currrent customer in ne aining, we can accomodate that too. In addition, our Training Department has weekly online seminars, open to all current customers, which cover many topics - from recurrent training to new functionality and regulations. A training schedule can be found here.

Service Order Form
General Information
Guides & Manuals
Request an AMI Disk
Training Calendar

return to menu

The Internet

No Credit card?

Send me two!

Do you have an aircraft poor lad...?

Erm... I... nop :'(

GAME OVER

Next day on my mailbox...

Thanks ARINC! :D

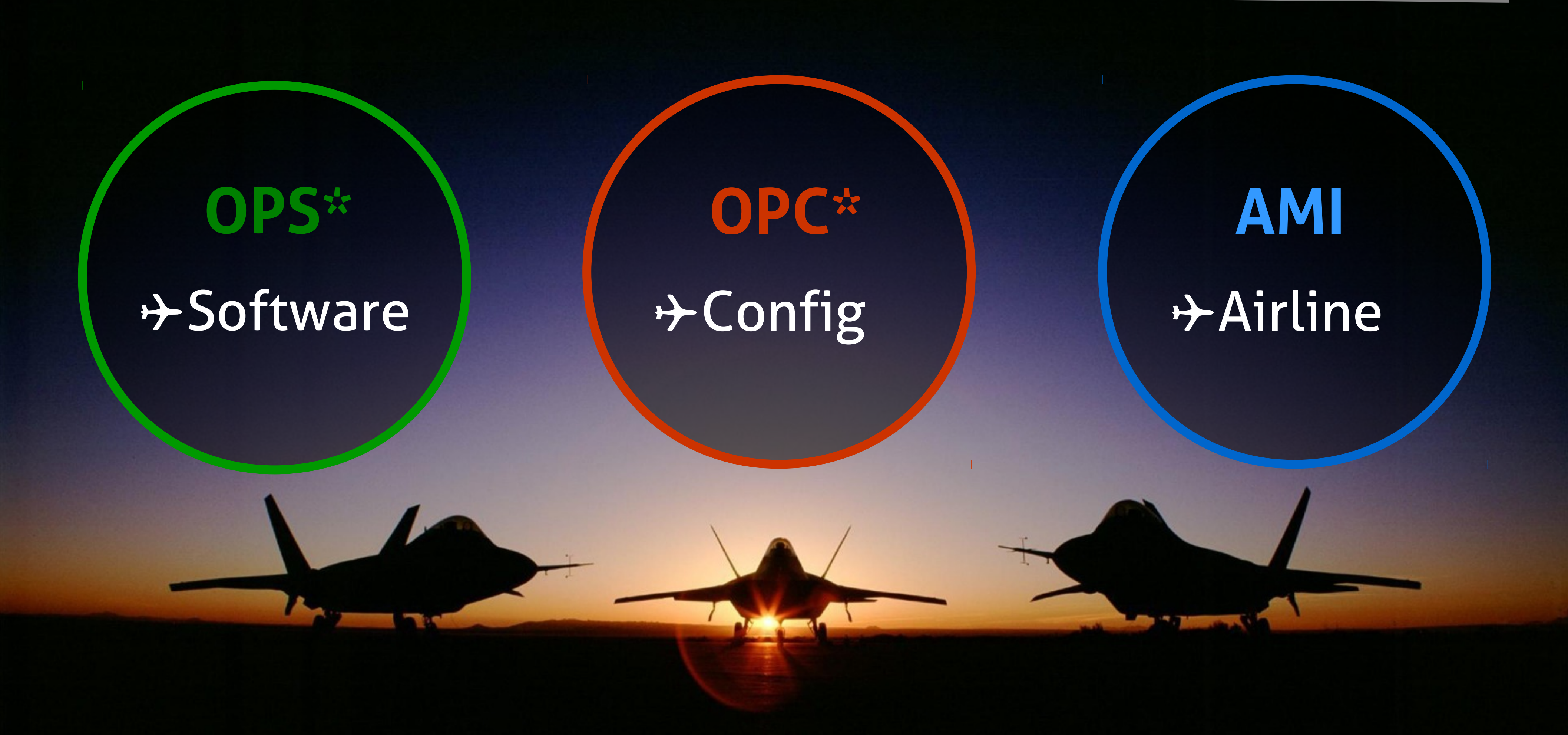
Who cares... ¡It's FREE!

AMI (Airline Modifiable Information)

Modifying system functionality with new software instead of with new hardware…

- All Boeing
- All Airbus
- Etc …

LSP (Loadable Software Parts)



OPS*

✈Software

OPC*

✈Config

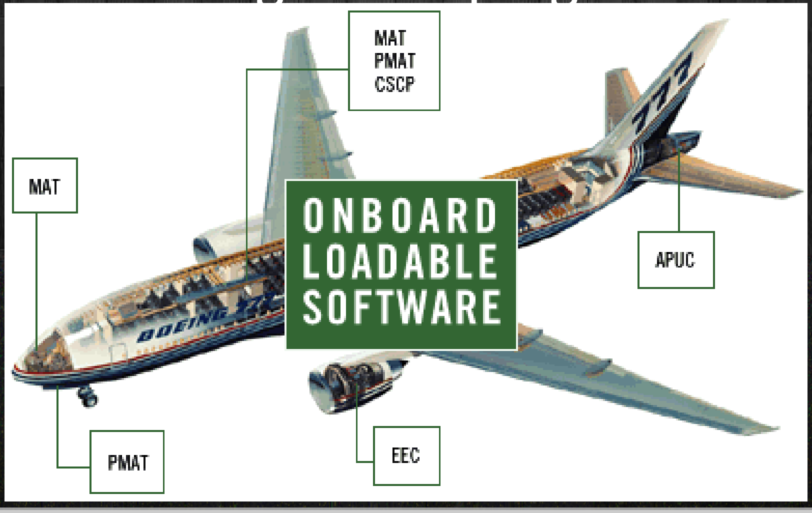
AMI

✈Airline

* Operational program Software/Configuration

LSP (Loadable Software Parts)

- Operational program software (OPS)
  - The operating system of a Line Replaceable Unit (LRU)
- Operational program configuration (OPC)
  - Specialized DB that determines the LRU configuration
- Database
  - FMC NDB, Engine, Performance, takeoffs, ACARS, etc.
- Airline modifiable information (AMI)
  - Supplies information to the OPS
  - Include logic units, which are high-level program code



LSP (Loadable Software Parts)

Attack vector?

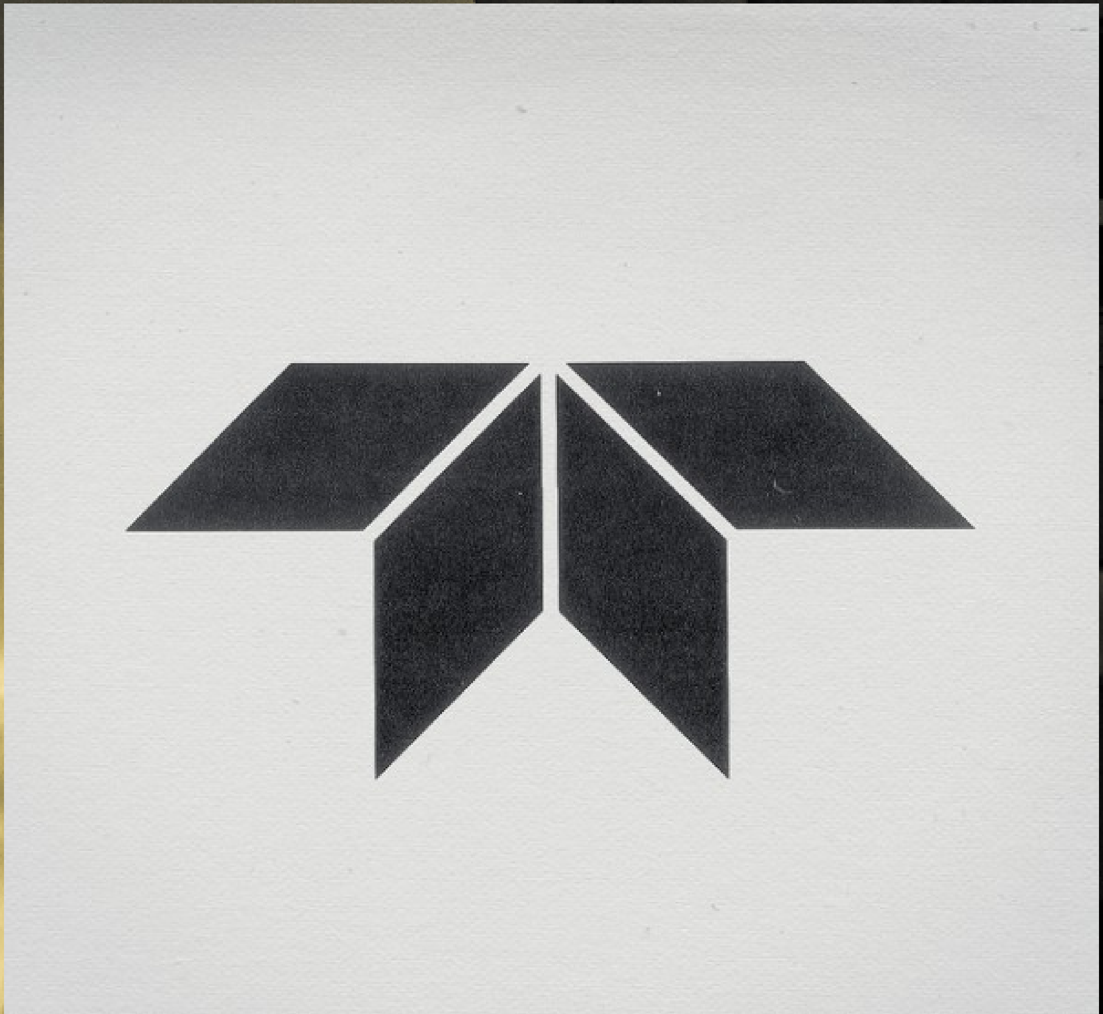
(...) Digital storage media (typically 3.5-in disks)

GAME OVER

Stubborn as I am...

AMI Wireless data loader

TELEDYNE TECHNOLOGIES



TELEDYNE TECHNOLOGIES

Teledyne LoadStar Server Enterprise

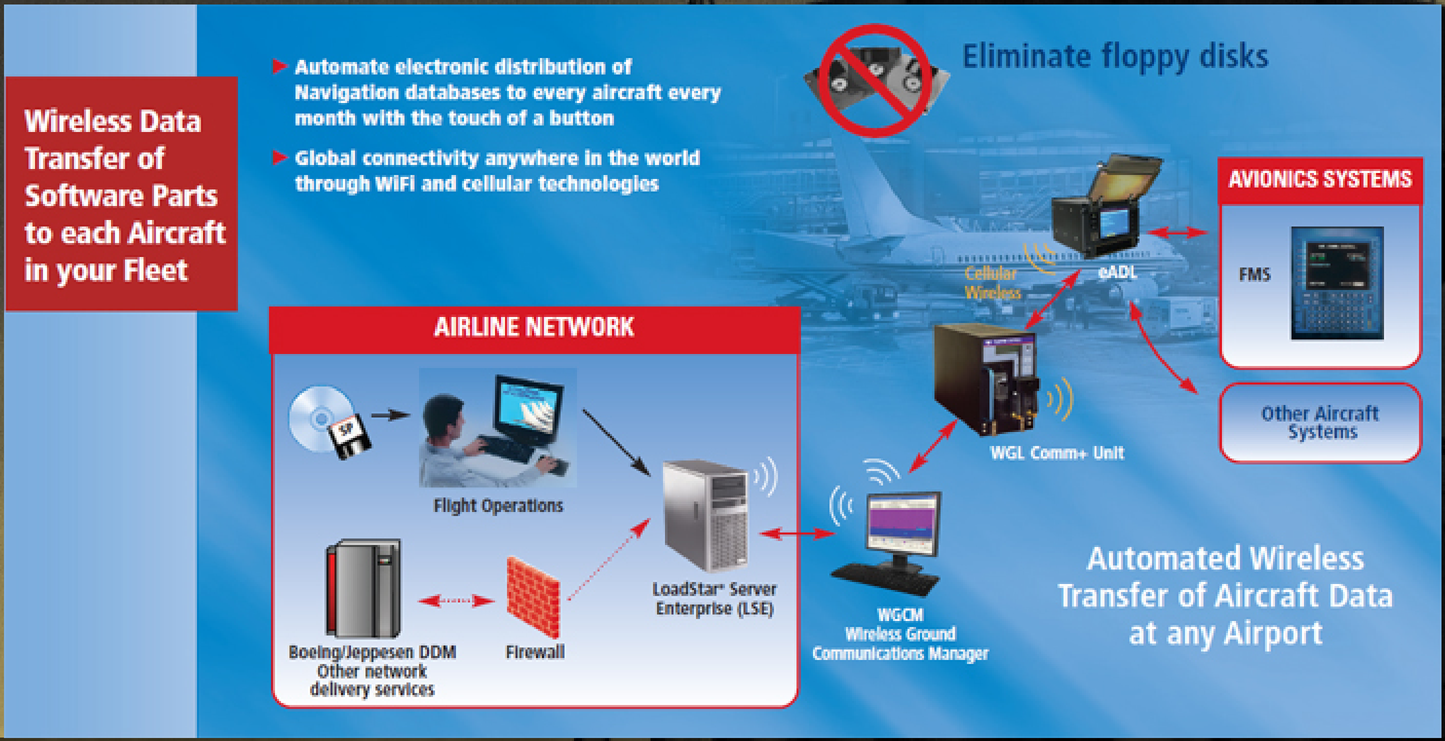
Eliminate media (floppy disks, CDs)

Web-based distribution instantly transfers Software Parts to data loaders and directly to the aircraft via **wireless links**

This integrated solution makes it possible to electronically distribute Software Parts from desktop to data loaders **across the fleet with a single press of a button**

Software Part
Management
Cellular
Wireless
Data
Loading
FMS

TELEDYNE TECHNOLOGIES



Wireless Data Transfer of Software Parts to each Aircraft in your Fleet

- Automate electronic distribution of Navigation databases to every aircraft every month with the touch of a button
- Global connectivity anywhere in the world through WiFi and cellular technologies

Eliminate floppy disks

Automated Wireless Transfer of Aircraft Data at any Airport

AIRLINE NETWORK
Flight Operations
LoadStar® Server Enterprise (LSE)
Boeing/Jeppesen DDM Other network delivery services
Firewall
WGCM Wireless Ground Communications Manager
WGL Comm+ Unit
Cellular Wireless
eADL
AVIONICS SYSTEMS
FMS
Other Aircraft Systems

A reliable and cost effective way to move data on and off the aircraft

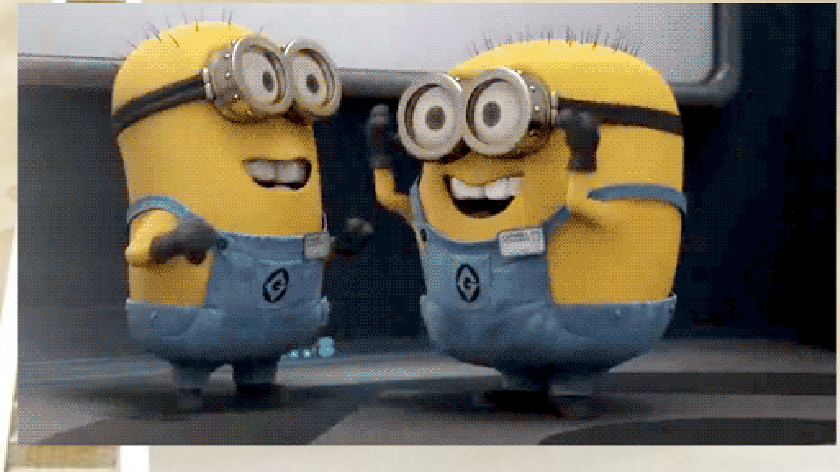
Simultaneous use of 3G/4G cellular radios using enhanced HSPA

Requires a Wireless Access Point in or near the cockpit.

TELEDYNE TECHNOLOGIES

Supported Aircrafts

Boeing 787, 747-8, A380 and A350
Airbus EFB and Boeing EFBs
All legacy aircraft A320, A330, B737, B747, etc.
Boeing 777 and Embraer ERJ 170/190



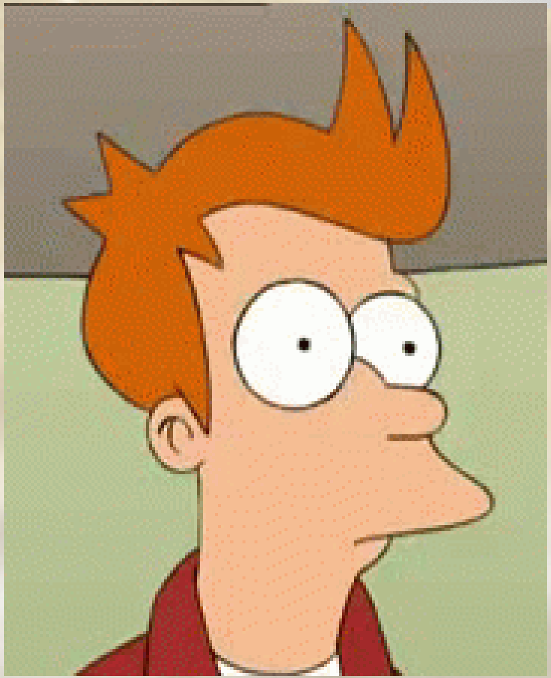
In use at over 40 airlines worldwide

Targets! Targets! Targets!

TELEDYNE TECHNOLOGIES

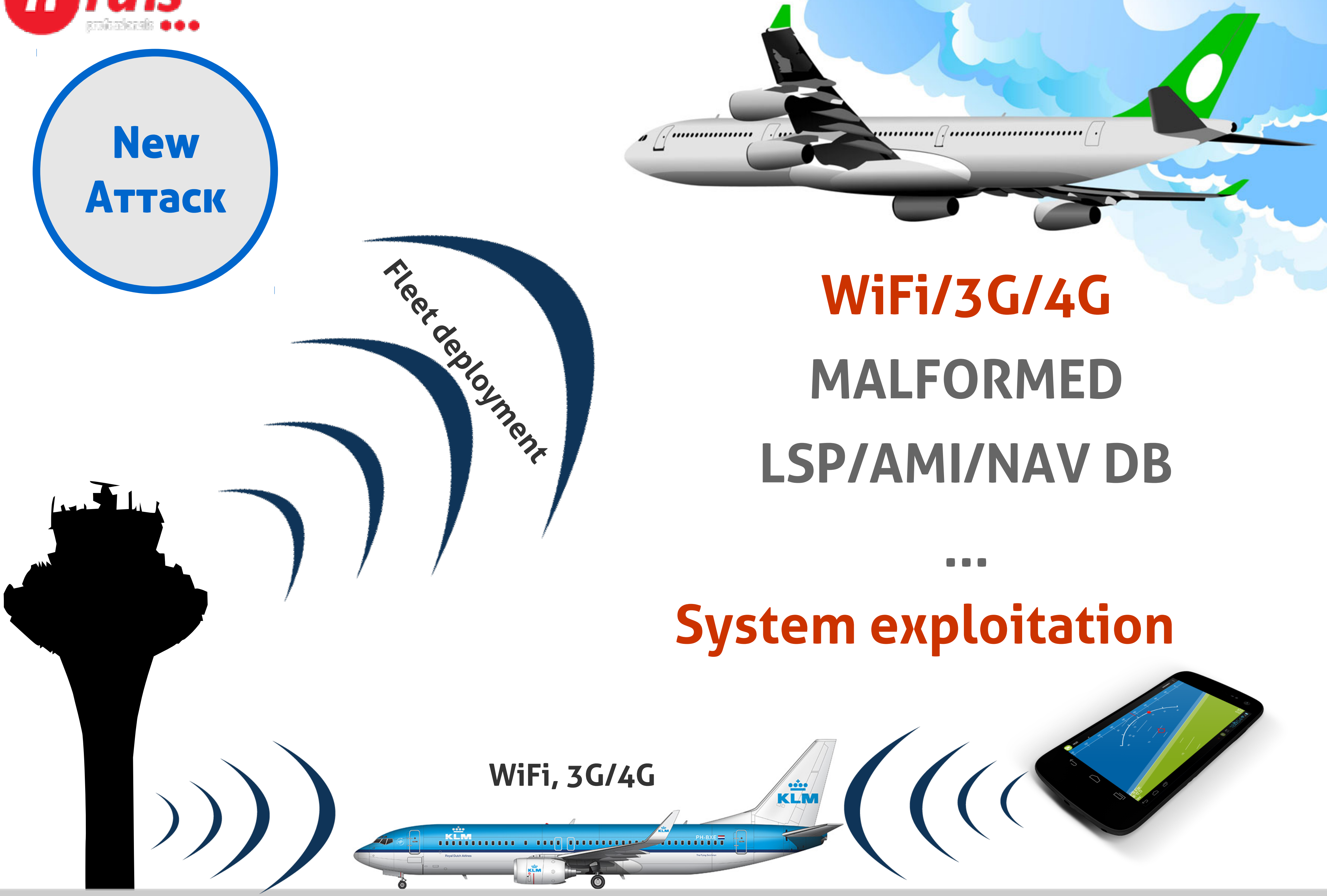
Load Configurations

Fight Management Systems (FMS)
Integrated Display System (IDS)
Aircraft Condition Monitoring System (ACMS)
Advanced Cabin Entertainment and Service System (ACESS)
Central Management System (CMS)
Automatic Flight System (AFS)
Centralized Fault Display System (CFDS)
Aircraft System Controller (ASC)
Flight Management Computer System (FMCS)
Electronic Display System (EDS)
Aircraft Data Acquisition System (ADAS)



FMS: NZ 2000/ Mark III CMU? ✓

CHALLENGE
ACCEPTED



New Attack

WiFi/3G/4G

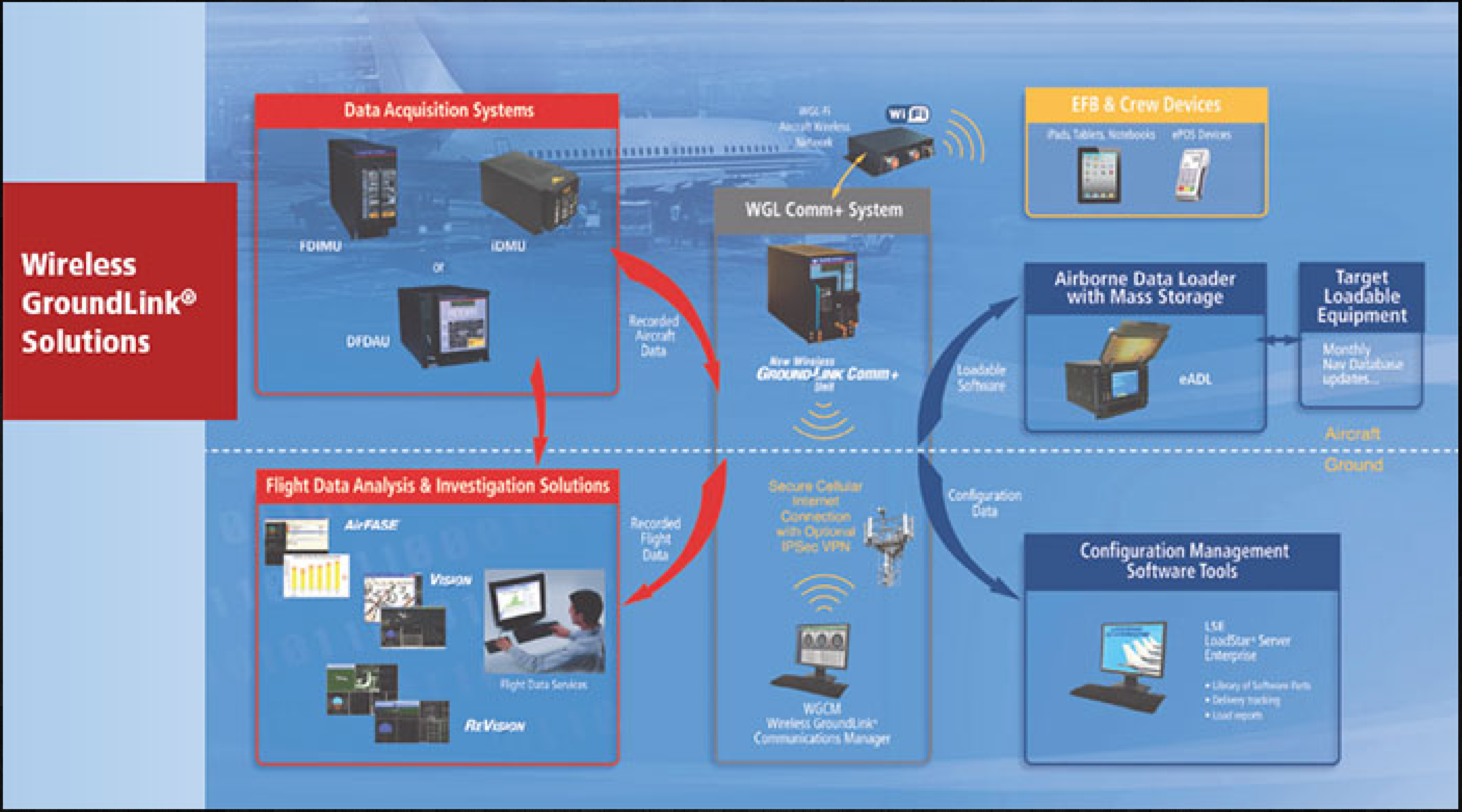
MALFORMED

LSP/AMI/NAV DB

...

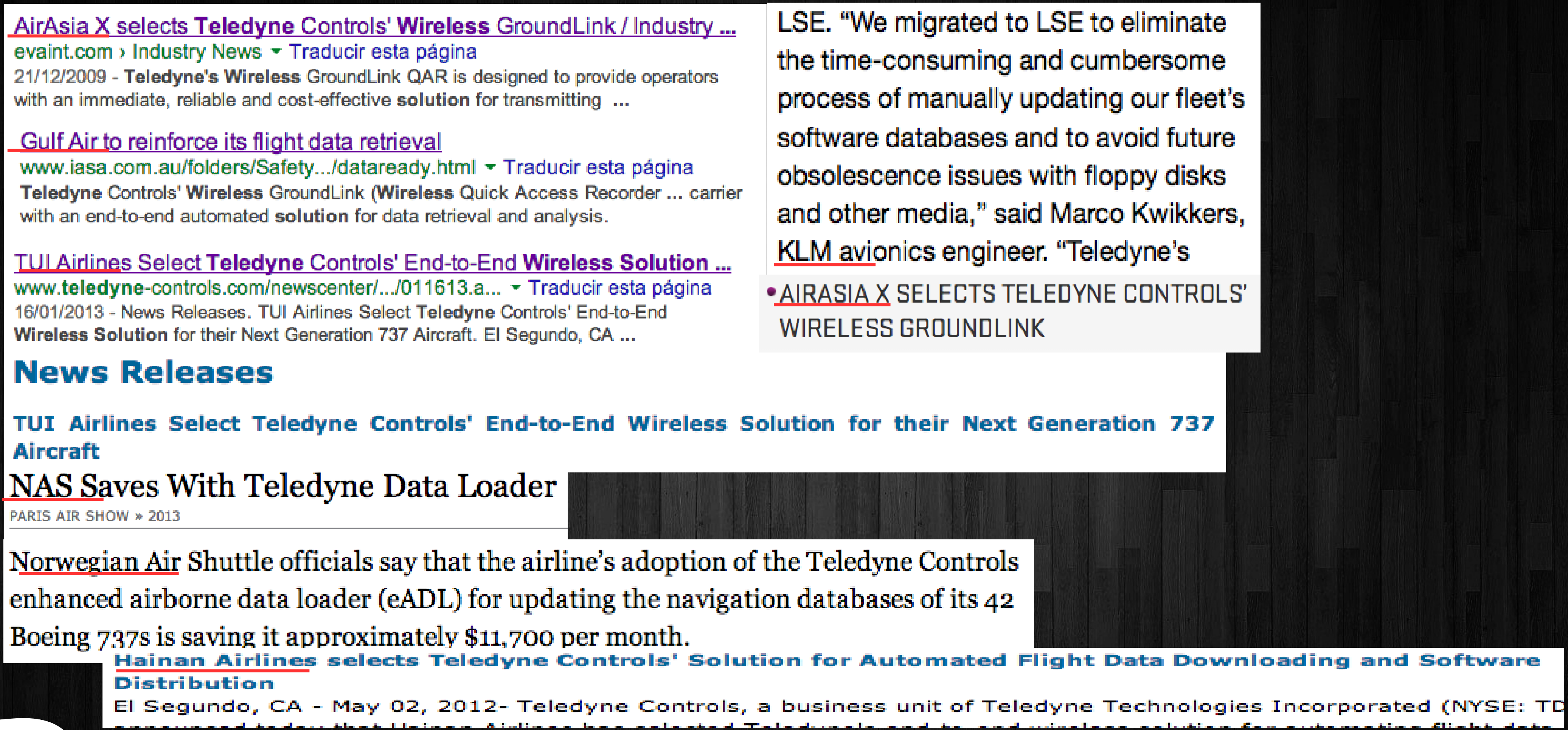
System exploitation

Used by over 100 operators


Wireless GroundLink® Solutions
Data Acquisition Systems
FDIMU
IDMU
or
DFDAU
Recorded Aircraft Data
WGL-Fi Aircraft Wireless Network
Wi Fi
WGL Comm+ System
New Wireless GroundLink Comm+ Unit
EFB & Crew Devices
iPads, Tablets, Notebooks
ePOS Devices
Loadable Software
Airborne Data Loader with Mass Storage
eADL
Target Loadable Equipment
Monthly Nav Database updates...
Aircraft
Ground
Flight Data Analysis & Investigation Solutions
AirFASE
Vision
Flight Data Services
RzVision
Recorded Flight Data
Secure Cellular Internet Connection with Optional IPSec VPN
WGCM
Wireless GroundLink® Communications Manager
Configuration Data
Configuration Management Software Tools
LSE
LoadStar® Server Enterprise
• Library of Software Parts
• Delivery tracking
• Load reports

Delivery

Finding targets... Help me?



AirAsia X selects Teledyne Controls' Wireless GroundLink / Industry ...
evaint.com › Industry News ▾ Traducir esta página
21/12/2009 - Teledyne's Wireless GroundLink QAR is designed to provide operators with an immediate, reliable and cost-effective solution for transmitting ...

Gulf Air to reinforce its flight data retrieval
www.iasa.com.au/folders/Safety.../dataready.html ▾ Traducir esta página
Teledyne Controls' Wireless GroundLink (Wireless Quick Access Recorder ... carrier with an end-to-end automated solution for data retrieval and analysis.

TUI Airlines Select Teledyne Controls' End-to-End Wireless Solution ...
www.teledyne-controls.com/newscenter/.../011613.a... ▾ Traducir esta página
16/01/2013 - News Releases. TUI Airlines Select Teledyne Controls' End-to-End Wireless Solution for their Next Generation 737 Aircraft. El Segundo, CA ...

LSE. "We migrated to LSE to eliminate the time-consuming and cumbersome process of manually updating our fleet's software databases and to avoid future obsolescence issues with floppy disks and other media," said Marco Kwikkers, KLM avionics engineer. "Teledyne's

- AIRASIA X SELECTS TELEDYNE CONTROLS' WIRELESS GROUNDLINK

News Releases

TUI Airlines Select Teledyne Controls' End-to-End Wireless Solution for their Next Generation 737 Aircraft

NAS Saves With Teledyne Data Loader

PARIS AIR SHOW » 2013

Norwegian Air Shuttle officials say that the airline's adoption of the Teledyne Controls enhanced airborne data loader (eADL) for updating the navigation databases of its 42 Boeing 737s is saving it approximately $11,700 per month.

Hainan Airlines selects Teledyne Controls' Solution for Automated Flight Data Downloading and Software Distribution

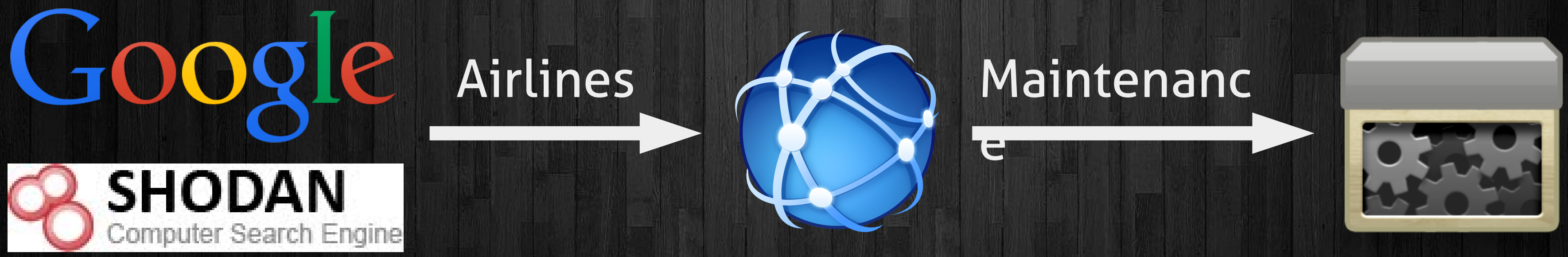
El Segundo, CA - May 02, 2012- Teledyne Controls, a business unit of Teledyne Technologies Incorporated (NYSE: TD

Delivery

How to get the code?

Either…

Or…



Google

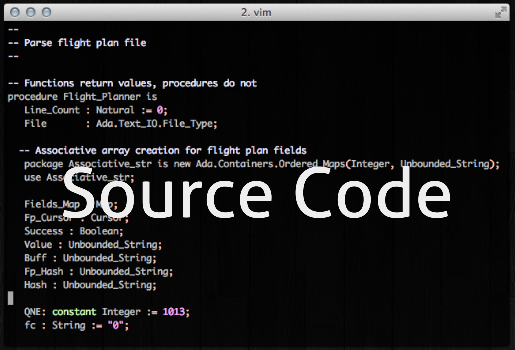
SHODAN Computer Search Engine

Airlines

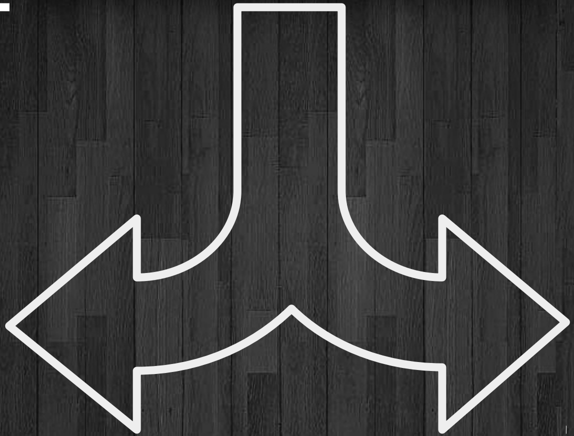
Maintenanc
e

My two cents

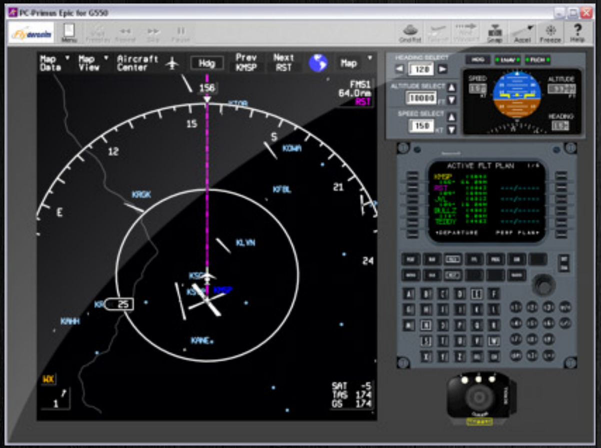
Source Code



```
--
-- Parse flight plan file
--

-- Functions return values, procedures do not
procedure Flight_Planner is
   Line_Count : Natural := 0;
   File       : Ada.Text_IO.File_Type;

  -- Associative array creation for flight plan fields
   package Associative_str is new Ada.Containers.Ordered_Maps(Integer, Unbounded_String);
   use Associative_str;

   Fields_Map : Map;
   Fp_Cursor : Cursor;
   Success : Boolean;
   Value : Unbounded_String;
   Buff : Unbounded_String;
   Fp_Hash : Unbounded_String;
   Hash : Unbounded_String;

   QNE: constant Integer := 1013;
   fc : String := "0";
```

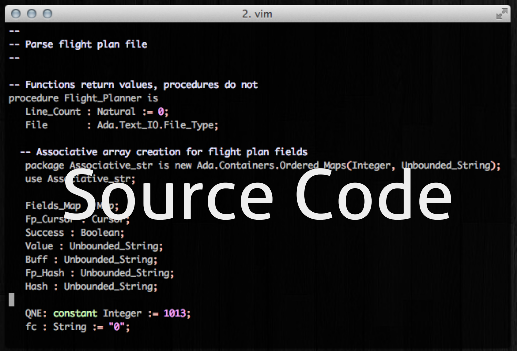


Training SW



System SW

WIND RIVER



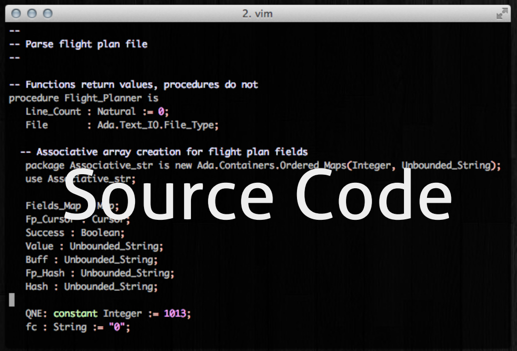
```
--
-- Parse flight plan file
--

-- Functions return values, procedures do not
procedure Flight_Planner is
   Line_Count : Natural := 0;
   File       : Ada.Text_IO.File_Type;

  -- Associative array creation for flight plan fields
   package Associative_str is new Ada.Containers.Ordered_Maps(Integer, Unbounded_String);
   use Associative_str;

   Fields_Map : Map;
   Fp_Cursor : Cursor;
   Success : Boolean;
   Value : Unbounded_String;
   Buff : Unbounded_String;
   Fp_Hash : Unbounded_String;
   Hash : Unbounded_String;

   QNE: constant Integer := 1013;
   fc : String := "0";
```

Source Code

Compile

Training SW

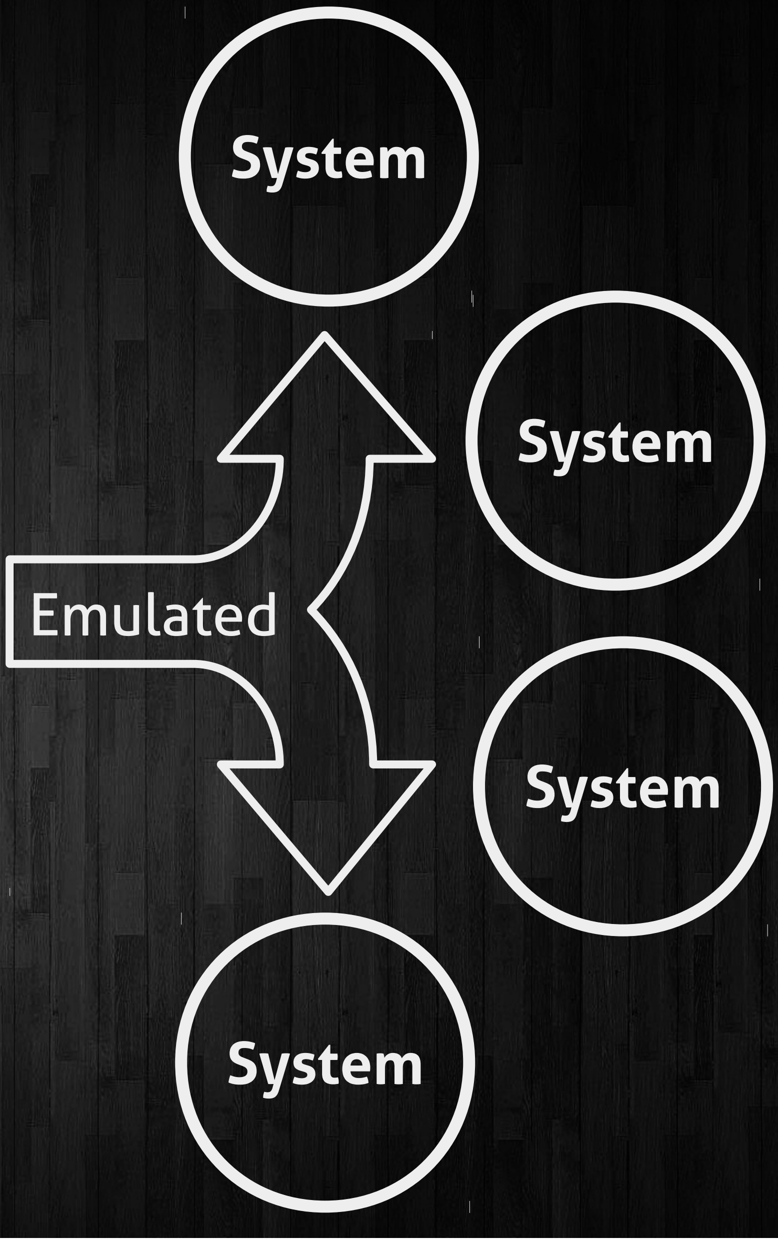
Training SW

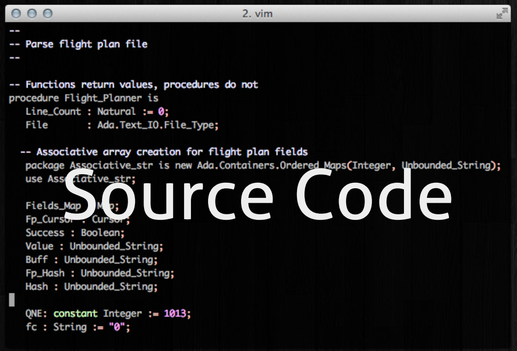


```
--
-- Parse flight plan file
--

-- Functions return values, procedures do not
procedure Flight_Planner is
   Line_Count : Natural := 0;
   File       : Ada.Text_IO.File_Type;

  -- Associative array creation for flight plan fields
   package Associative_str is new Ada.Containers.Ordered_Maps(Integer, Unbounded_String);
   use Associative_str;

   Fields_Map : Map;
   Fp_Cursor : Cursor;
   Success : Boolean;
   Value : Unbounded_String;
   Buff : Unbounded_String;
   Fp_Hash : Unbounded_String;
   Hash : Unbounded_String;

   QNE: constant Integer := 1013;
   fc : String := "0";
```

Source Code

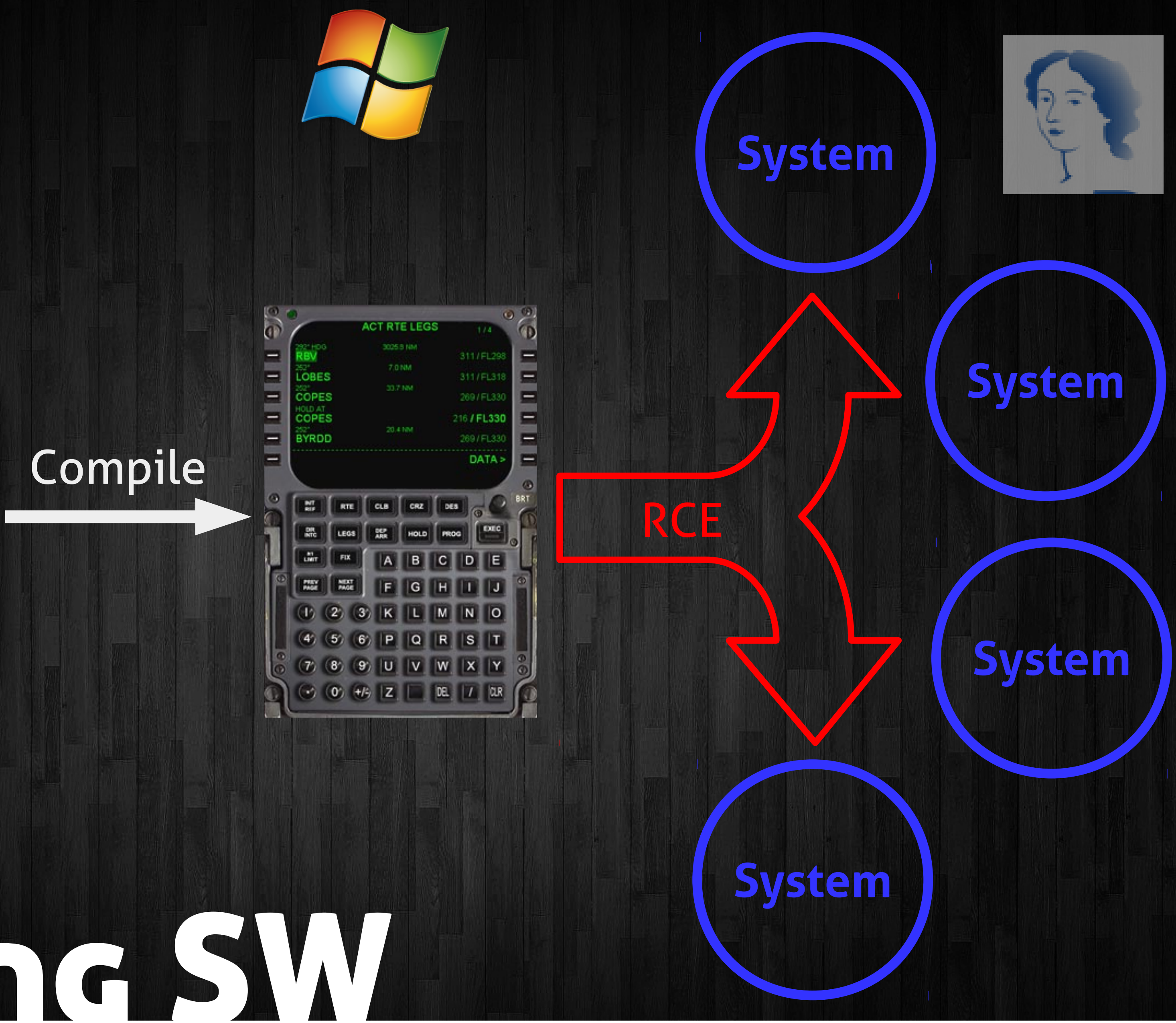
Compile





```
--
-- Parse flight plan file
--

-- Functions return values, procedures do not
procedure Flight_Planner is
   Line_Count : Natural := 0;
   File       : Ada.Text_IO.File_Type;

  -- Associative array creation for flight plan fields
   package Associative_str is new Ada.Containers.Ordered_Maps(Integer, Unbounded_String);
   use Associative_str;

   Fields_Map : Map;
   Fp_Cursor : Cursor;
   Success : Boolean;
   Value : Unbounded_String;
   Buff : Unbounded_String;
   Fp_Hash : Unbounded_String;
   Hash : Unbounded_String;

   QNE: constant Integer := 1013;
   fc : String := "0";
```

Source Code



Compile

RCE

System

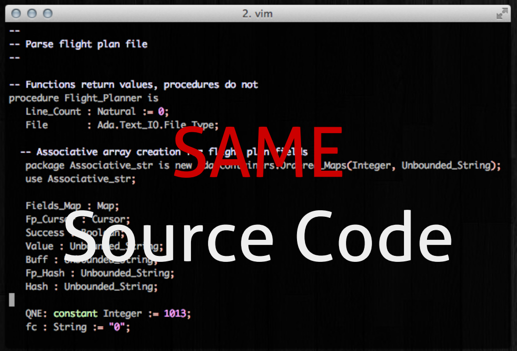
System

System

System

Training SW

WIND RIVER



```
--
-- Parse flight plan file
--

-- Functions return values, procedures do not
procedure Flight_Planner is
   Line_Count : Natural := 0;
   File       : Ada.Text_IO.File_Type;

  -- Associative array creation for flight plan fields
   package Associative_str is new Ada.Containers.Ordered_Maps(Integer, Unbounded_String);
   use Associative_str;

   Fields_Map : Map;
   Fp_Cursor : Cursor;
   Success : Boolean;
   Value : Unbounded_String;
   Buff : Unbounded_String;
   Fp_Hash : Unbounded_String;
   Hash : Unbounded_String;

   QNE: constant Integer := 1013;
   fc : String := "0";
```

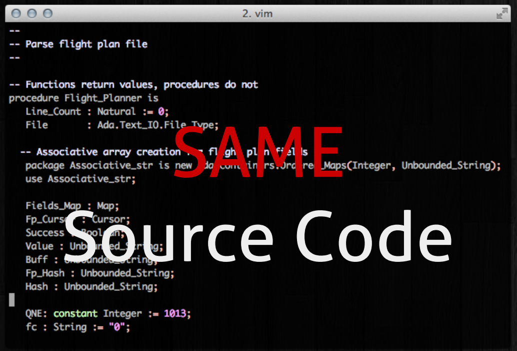
SAME

Source Code

Compile

Real SW

WIND RIVER

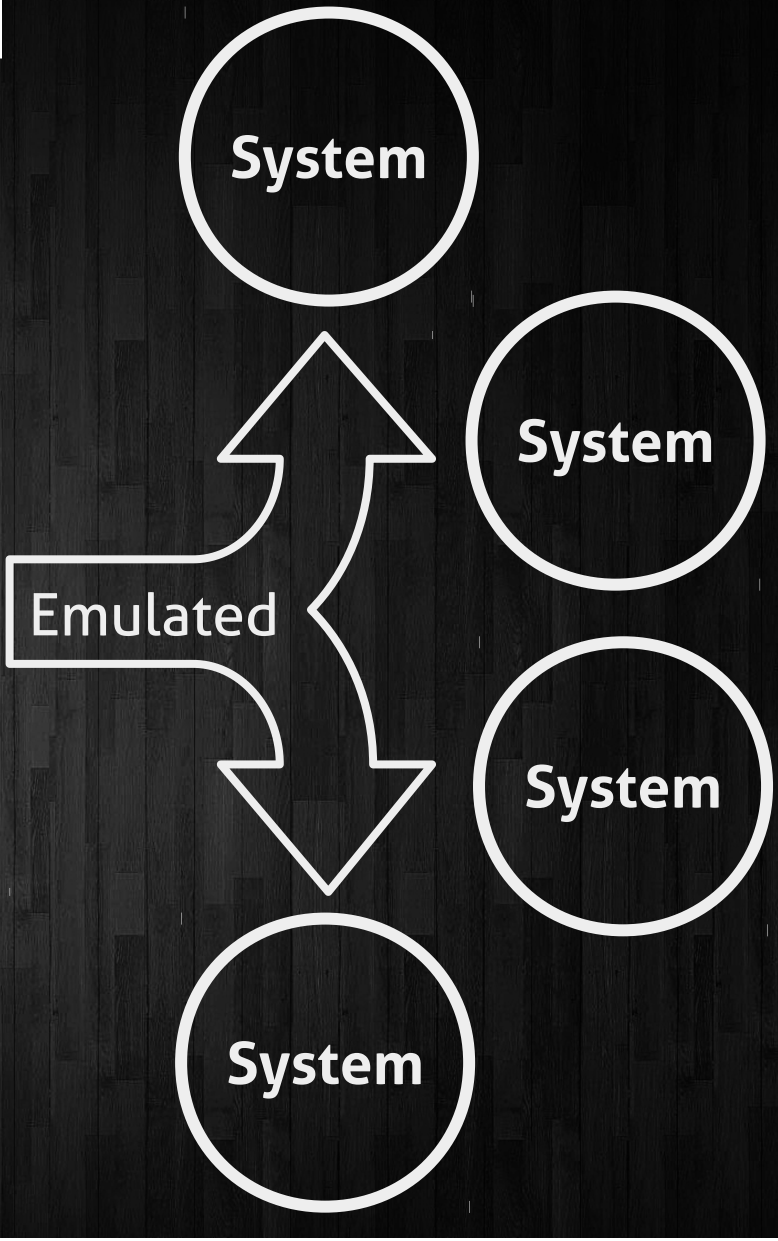


```
--
-- Parse flight plan file
--

-- Functions return values, procedures do not
procedure Flight_Planner is
   Line_Count : Natural := 0;
   File       : Ada.Text_IO.File_Type;

  -- Associative array creation for flight plan fields
   package Associative_str is new Ada.Containers.Ordered_Maps(Integer, Unbounded_String);
   use Associative_str;

   Fields_Map : Map;
   Fp_Cursor : Cursor;
   Success : Boolean;
   Value : Unbounded_String;
   Buff : Unbounded_String;
   Fp_Hash : Unbounded_String;
   Hash : Unbounded_String;

   QNE: constant Integer := 1013;
   fc : String := "0";
```

SAME

Source Code

Compile



Real SW

VxWorks

An embedded, RTOS developed by Wind River Systems

- Multitasking kernel
  - Preemptive and round-robin scheduling
  - Fast interrupt response
- User-mode applications ("Real-Time Processes", or RTP)
  - Isolated from other user-mode applications as well as the kernel via memory protection mechanisms.
- SMP and AMP support
- Error handling framework
- Binary, counting, and mutual exclusion semaphores with priority inheritance
- Local and distributed message queues
- POSIX certified

VxWorks

Really...?

- All "applications" run as kernel threads
- Little memory protection between apps
- Everything runs with the highest privileges
- ...but not necessarily the highest priority.

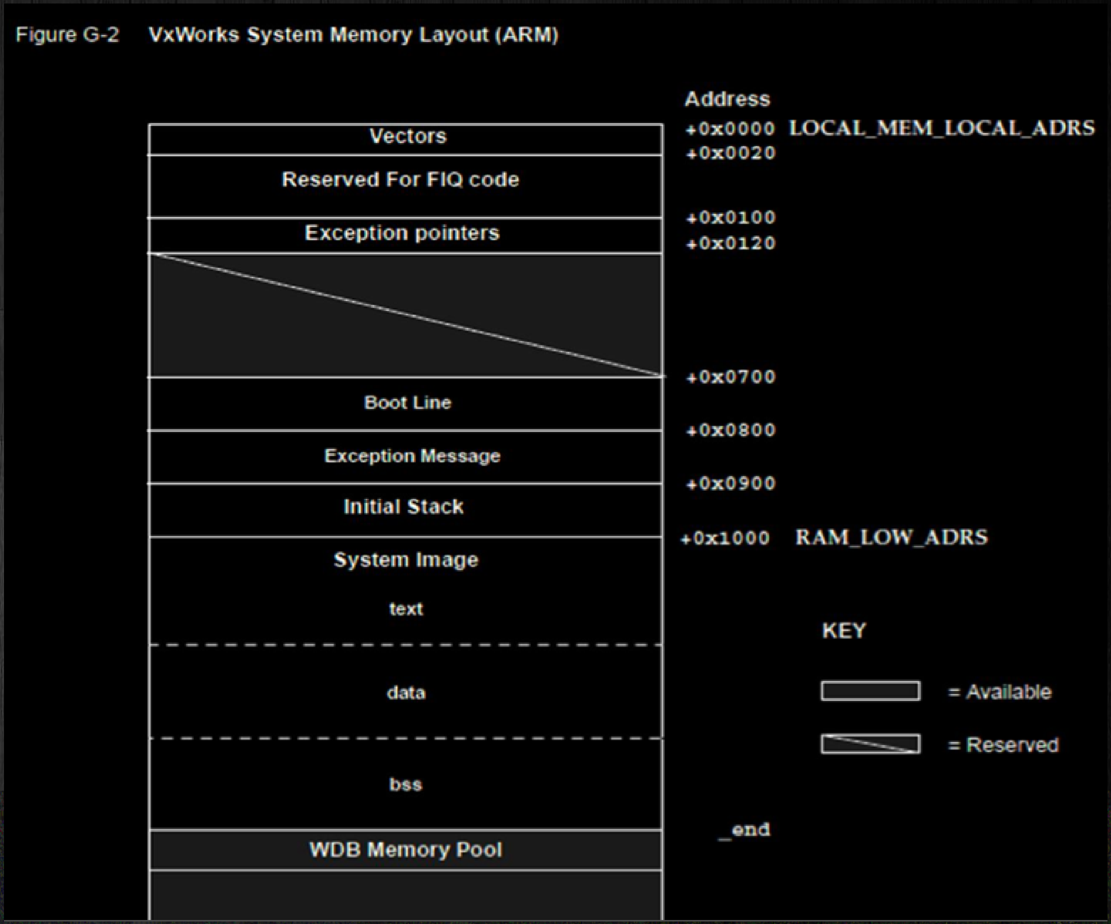
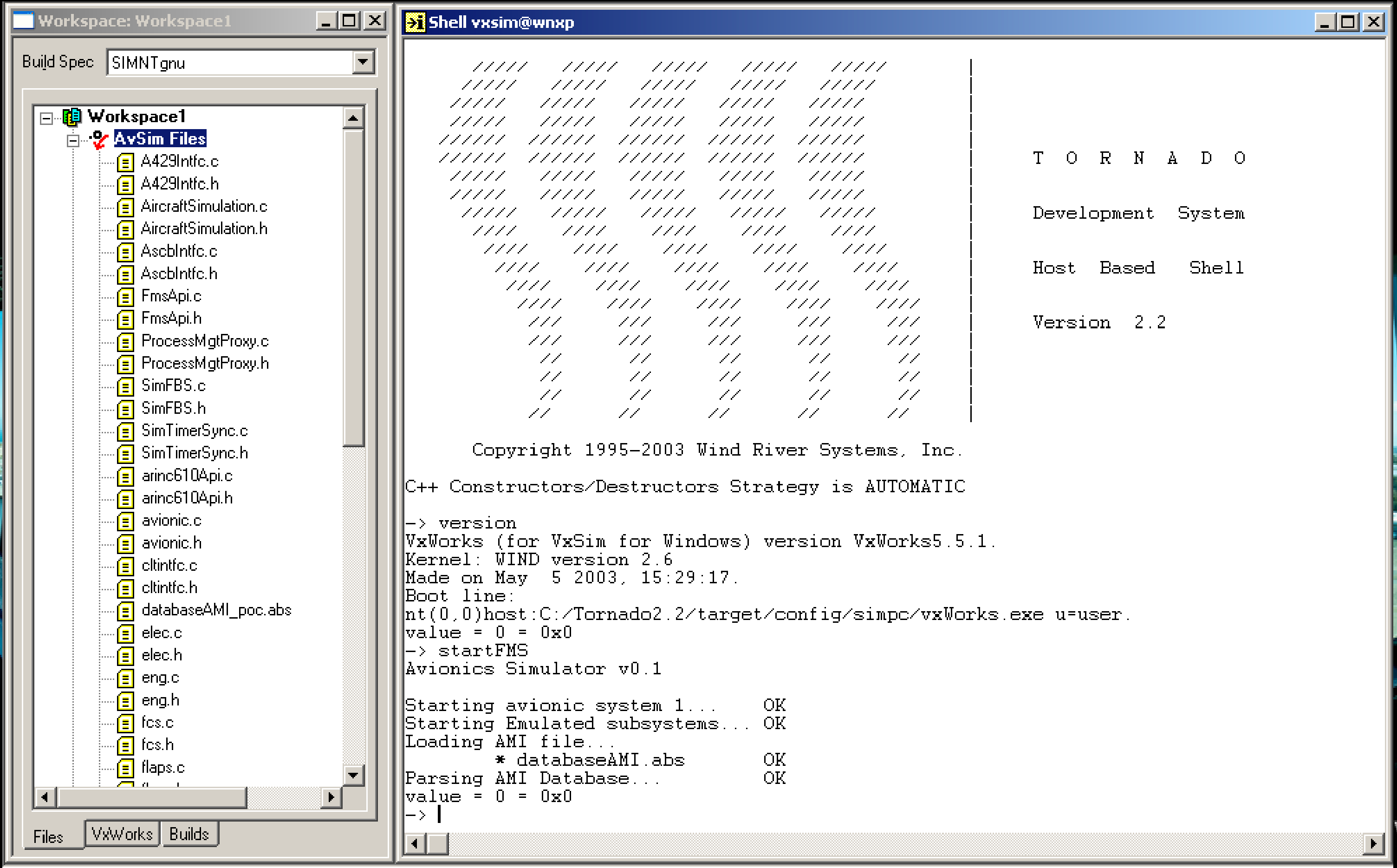


Figure G-2 VxWorks System Memory Layout (ARM)

Fun with VxWorks (H D Moore)



```
      /////   /////   /////   /////   /////       |
     /////   /////   /////   /////   /////        |
    /////   /////   /////   /////   /////         |
    /////   /////   /////   /////   /////         |
   //////  //////  //////  //////  //////         |
   //////  //////  //////  //////  //////         |     T  O  R  N  A  D  O
    /////   /////   /////   /////   /////         |
    /////   /////   /////   /////   /////         |
     /////   /////   /////   /////   /////        |     Development  System
      ////    ////    ////    ////    ////        |
       ////    ////    ////    ////    ////       |
        ////    ////    ////    ////    ////      |     Host  Based   Shell
         ////    ////    ////    ////    ////     |
          ////    ////    ////    ////    ////    |
           ///     ///     ///     ///     ///    |     Version  2.2
           ///     ///     ///     ///     ///    |
            //      //      //      //      //    |
            //      //      //      //      //    |
            //      //      //      //      //    |
           //      //      //      //      //     |

      Copyright 1995-2003 Wind River Systems, Inc.

C++ Constructors/Destructors Strategy is AUTOMATIC

-> version
VxWorks (for VxSim for Windows) version VxWorks5.5.1.
Kernel: WIND version 2.6
Made on May  5 2003, 15:29:17.
Boot line:
nt(0,0)host:C:/Tornado2.2/target/config/simpc/vxWorks.exe u=user.
value = 0 = 0x0
-> startFMS
Avionics Simulator v0.1

Starting avionic system 1...    OK
Starting Emulated subsystems... OK
Loading AMI file...
        * databaseAMI.abs       OK
Parsing AMI Database...         OK
value = 0 = 0x0
->
```

WWW.JERSEYIMAGE.CO.UK

DEMO TIME!

GAME OVER

HITBSECCONF2013 MALAYSIA

THE ELEVENTH ANNUAL HITB SECURITY CONFERENCE IN ASIA

Hacking Aircrafts since 2009

@hteso
http://www.commandercat.com
http://blog.nruns.com

hugo.teso@nruns.com