

Ada Usage in HMI for Onboard Safety Critical Applications

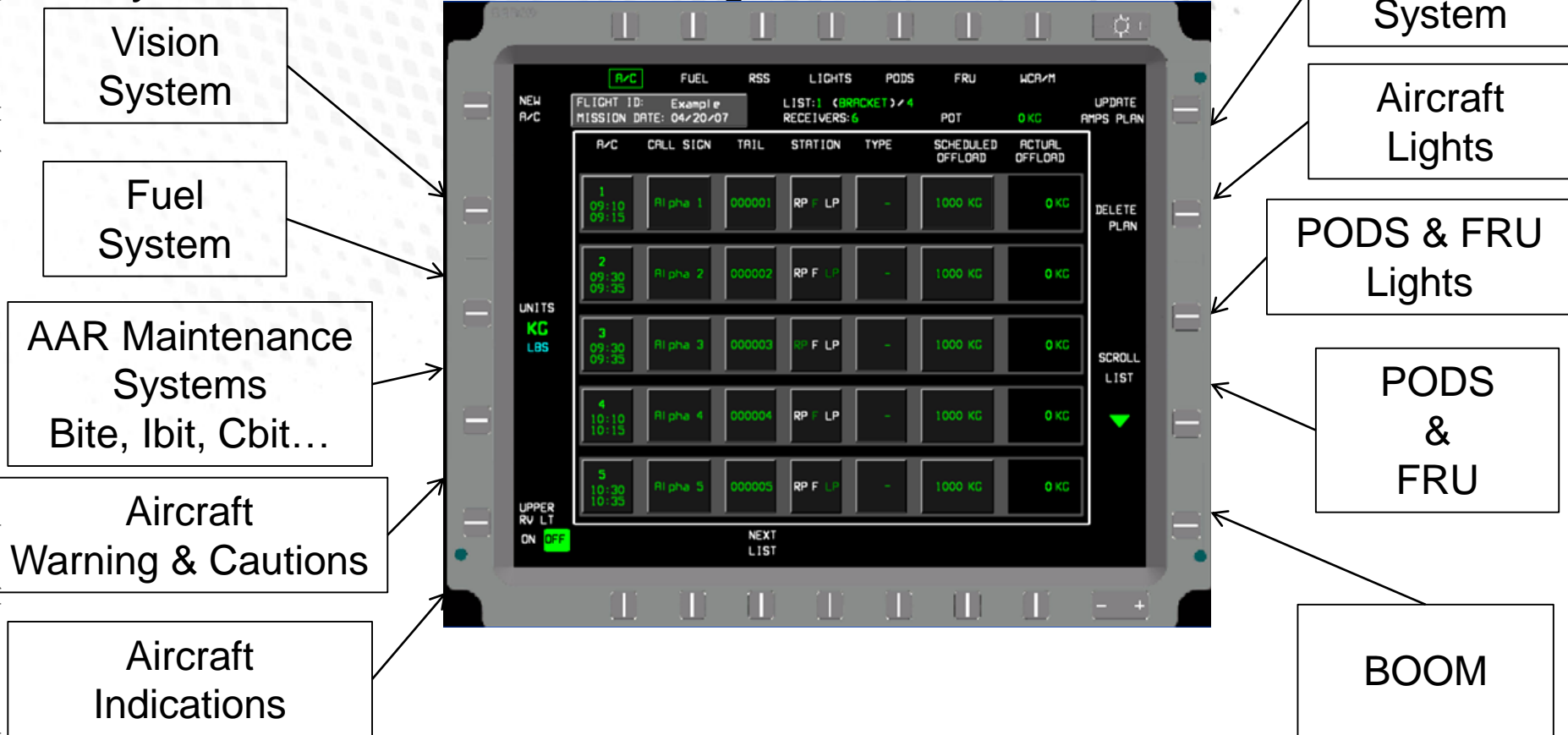


Clara María Arcones Gabriel
Enrique Chicharro López
Ismael Lafoz Pastor

Air Refueling Domain
Mission Systems CoC
AIRBUS DEFENCE & SPACE

MFCD System

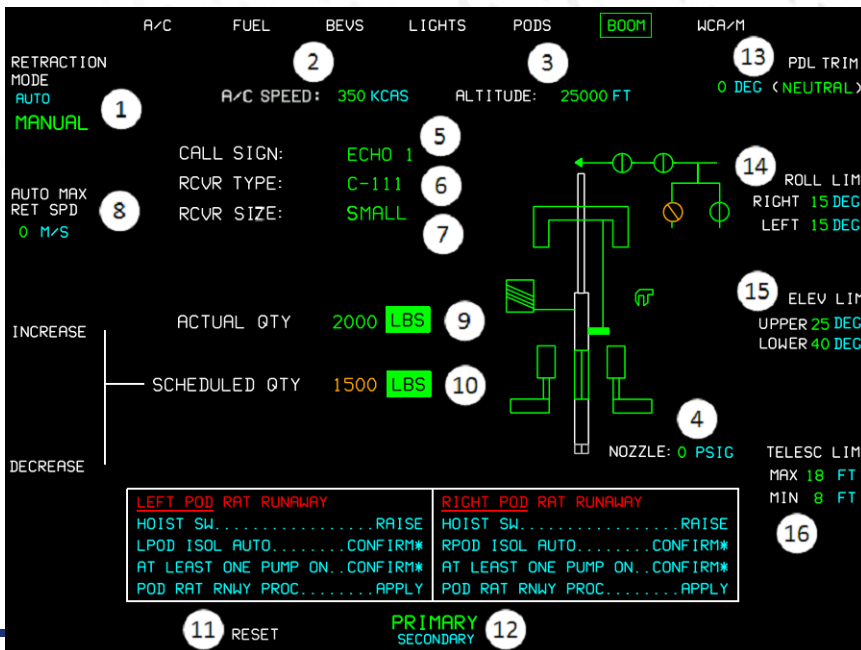
- Multifunction and Control Display (MFCD): interface with refuelling operator to control and display the Air to Air Refuelling (AAR) Systems information, warning and indications



This document and all information contained herein is the sole property of EADS CASA. No intellectual property rights are granted by the delivery of this document or disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of EADS CASA. This document and its content shall not be used for any other purpose than for which it is supplied.

MFCD System

- Multifunction and Control Display (MFCD): interface with refuelling operator to control and display the Air to Air Refuelling (AAR) Systems information, warning and indications.
- MFCD is not just an HMI application but an interface to perform the Refuelling Operation.



- It is a certified application, DO178B, level DAL B, due to it can set values whose failure conditions are considered Harzardous (example BOOM envelope)

MFCD Development

- MFCD HMI developed with VAPS 6.3.1 (Virtual Avionics Prototyping System)
- MFCD SW application developed with Ada 95
- Partitioning-based SW Architecture
- Esterline PU-2000
- Esterline CHDD-268
- VxWorks 653 (2.2.1.1)
- QCG 2.0 / VAPS 6.3.1
 - Generating QCG code is basically a mapping of metafile commands to runtime commands. This runtime commands are code generated as static, constant data structures. This data is interpreted by the runtime library, which also reads the dynamic channel data, to produce the application's runtime behavior.
 - The QCG runtime library was developed using the MISRA C standard. MISRA C is an initiative to define a safe C subset and coding standard for embedded systems.

Basic VAPS File Types

Frames

- .FRM Contain Graphics Objects and Data Connections.

Metafile

- .VMF ASCII Meta Tagged version of Frame file.
 - QCG code is generated from VAPS metafiles
 - Metafiles are ASCII Human Readable versions of binary Frames.
 - Frames must be converted to Metafiles before they can be built in QCG.

Channels

- .CHA Data Structure Objects, are used to connect data to Graphical objects.

Process

- . C code is imported into Ada 95 with “pragma import”
- Type is created to handle frames and channels:

```
type Channel_Name_T is  
array (Channel_T) of String (1 .. 21);
```

Where Channel_T is a type with all the VAPS Channels.

Two constants were created, one to handle channels and one to handle frames.

- *Frame_Name_1_C : constant Channel_Name_T :=*
- *Channel_Name_C : constant Channel_Name_T :=*

```
Channel_Name_C : constant Channel_Name_T :=  
(Aircraft_Common_Page => "aircraft_cmn_page" & Character'Val(0) & " ",  
Aircraft_List          => "aircraft_list" & Character'Val(0) & " ",  
Aircraft_Main_Page    => "aircraft_main_page" & Character'Val(0) & " ",  
Bevs_Camera_Page      => "bevs_camera_page" & Character'Val(0) & " ",  
Bevs_Image_Page       => "bevs_image_page" & Character'Val(0) & " ",  
Frame_Name_1_C : constant Channel_Name_T :=  
(Aircraft_Common_Page => "Aircraft_Page#1" & Character'Val(0) & " ",  
Aircraft_List         => "Aircraft_Page#1" & Character'Val(0) & " ",  
Aircraft_Main_Page    => "Aircraft_Page#1" & Character'Val(0) & " ",  
Bevs_Camera_Page      => "RSS_Page#1" & Character'Val(0) & " ",  
Bevs_Image_Page       => "RSS_Page#1" & Character'Val(0) & " ",  
Bevs_Lights_Laser_Page => "RSS_Page#1" & Character'Val(0) & " ",  
Bevs_Main_Page        => "RSS_Page#1" & Character'Val(0) & " ",
```

VAPS Channels

VAPS Channel is a data structure that allows information to be sent to, from and between VAPS objects and frames.

Channels has:

- SCOPE:
 - Local
 - Session
- TYPE:
 - Fast
 - Queued
- One or more “members”
 - Scalar (1element)
 - 1,2,3 dimensional array of elements

There is one to one mapping relationship between VAPS channels and MFCD Ada code, so in both files the channels members has to be written in the same order.

SCOPE	LOCAL		
TYPE	FAST		
Aircraft_Speed_State	1	S	
Aircraft_Speed_Variant	1	S	
Aircraft_Speed_Value	1	L	
Altitude_State	1	S	
Altitude_Variant	1	S	
Altitude_Value	1	L	
LP_Amber_Signal_Light_State	1	S	
LP_Amber_Signal_Light_Variant	1	S	
LP_Amber_Signal_Light_Value	1	L	

```
type Channel_T is
record
  Aircraft_Speed : GC.Display_Channel_T (GC.Integer_Data);
  Altitude : GC.Display_Channel_T (GC.Integer_Data);
  Left_Pod_Amber_Signal_Light : GC.Display_Channel_T (GC.Enumeration_Data);
  Left_Pod_Box : GC.Display_Channel_T (GC.Enumeration_Data);
  Left_Pod_Green_Signal_Light : GC.Display_Channel_T (GC.Enumeration_Data);
  Left_Pod_Hose_Length : GC.Display_Channel_T (GC.Integer_Data);
```

herein is the sole property of EADS CASA. No intellectual property rights are granted by the delivery of this document or disclosure of its content. This document shall not be used for any other purpose than for which it is supplied.

Additional Uses

This application SW has been reused to develop other useful tools:

- Simulator
 - To evaluate HMI aspects and behaviour quick and easy in a desktop computer.
 - Debugger.
- Offline Refuelling Operation Simulator (OROS)
 - Replay air refuelling mission on ground including operator actions.

Simulator

VAPS Code Generators

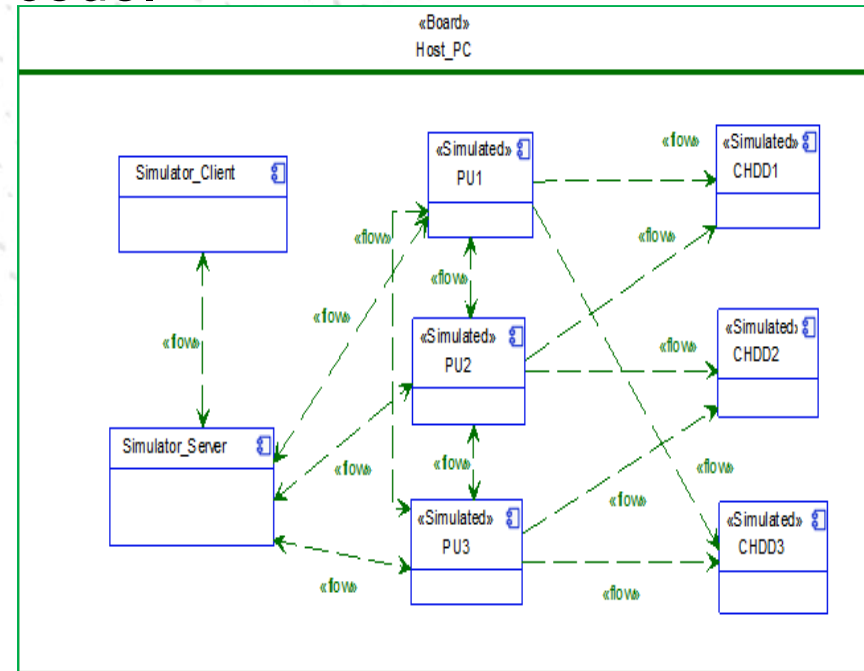
- CCG Lite 3.1 → **C Code Generator** (Host – Windows)
 - Allows users to create executables or libraries (dll) based on VAPS. Output is ANSI-standard C code.
- QCG 2.0 → **Qualified C Generator** (Target)

- Conformance to DO-178B level A. Application

- Client, Server, running on a PC:

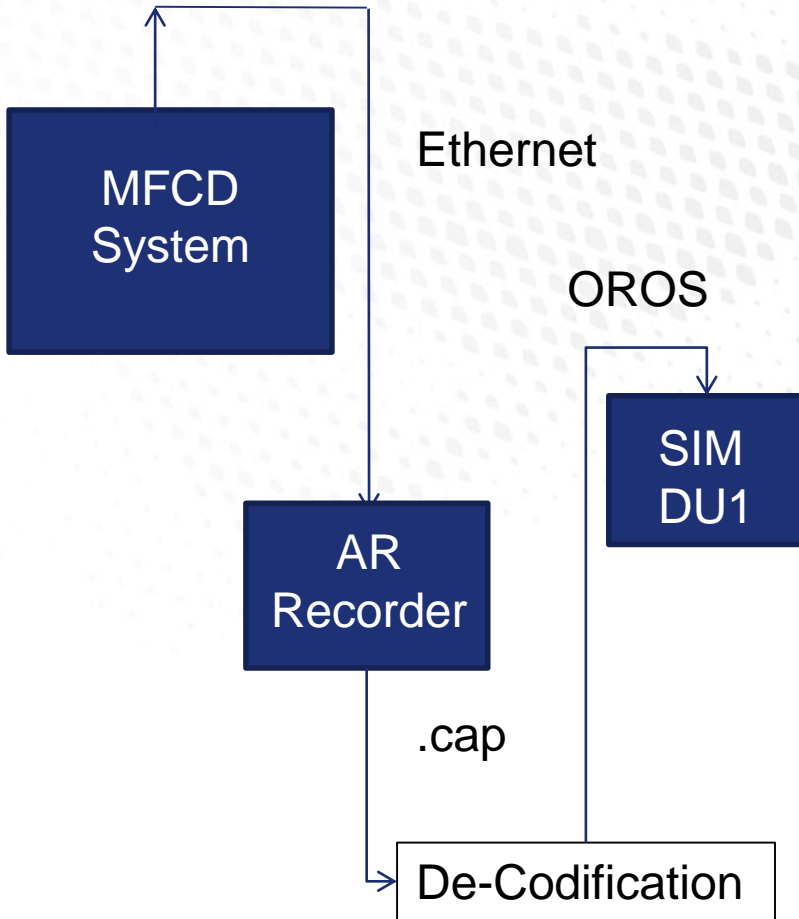
- Simulated PUs and Displays running on desktop or
- Real PUs and Displays

- All buses simulated through Ethernet sockets
- Deployment possible on multiple computers



Offline Refuelling Operation Simulator (OROS)

Codification



events_12.log: Bloc de notas

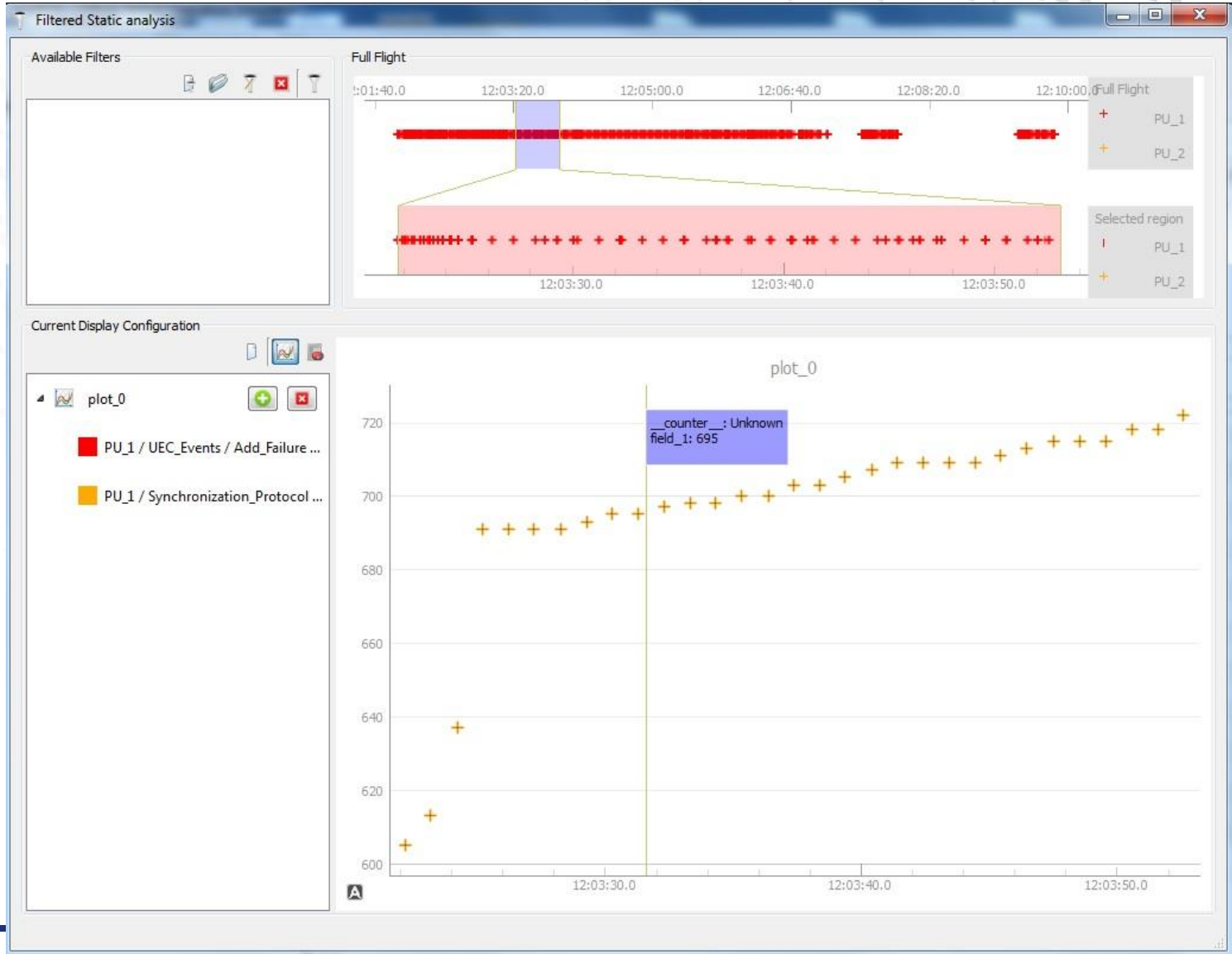
Archivo	Edición	Formato	Ver	Ayuda
0.840214130	MFD 1	: Default	:	238
0.840214130	MFD 1	: XLInk_Protocol_Default	:	239
0.840214130	MFD 1	: XLInk_Protocol_Default	:	240
0.840214130	MFD 1	: Bevs_Traffic_Default	:	241
0.840214130	MFD 1	: Default	:	242
0.840214130	MFD 1	: Printer_Traffic_Default	:	243
0.840214130	MFD 1	: XLInk_Protocol_Default	:	244
0.840214130	MFD 1	: Bevs_Traffic_Default	:	245
0.840214130	MFD 1	: Printer_Traffic_Default	:	246
0.840214130	MFD 1	: Default	:	247
0.840214130	MFD 1	: XLInk_Protocol_Default	:	248
0.840214130	MFD 1	: XLInk_Protocol_Default	:	249
0.840214130	MFD 1	: Default	:	250
0.840214130	MFD 1	: HWI_Events	:	251
0.840214130	MFD 1	: HWI_Events	:	252
2.070894495	MFD 1	: HWI_Events	:	253
2.070894495	MFD 1	: HWI_Events	:	254
2.070894495	MFD 1	: HWI_Events	:	255
2.070894495	MFD 1	: HWI_Events	:	256
2.070894495	MFD 1	: Printer_Traffic_Default	:	257
2.070894495	MFD 1	: XLInk_Protocol_Default	:	258
2.070894495	MFD 1	: XLInk_Protocol_Default	:	259
2.070894495	MFD 1	: XLInk_Protocol_Default	:	260
2.070894495	MFD 1	: Printer_Traffic_Default	:	261
2.070894495	MFD 1	: Default	:	262
2.070894495	MFD 1	: XLInk_Protocol_Default	:	263
2.070894495	MFD 1	: Printer_Traffic_Default	:	264
2.070894495	MFD 1	: Miibus_Rx_Traffic	:	265
2.070894495	MFD 1	: Miibus_Rx_Traffic	:	266
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	267
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	268
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	269
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	270
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	271
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	272
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	273
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	274
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	275
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	276
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	277
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	278
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	279
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	280
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	281
2.070900268	MFD 1	: Miibus_Rx_Traffic	:	282

```

24863527 System time is 12:00:30
25045309 XL_ERROR Synchronisation Timed out
25045317 XL_ERROR MFD 2 has failed to respond
25354470 Starting test on PU1
25364057 Bevs_Protocol_State changed state from Inactive
25435164 PART2 :Timeout in state Waiting_To_Send_SAL
25547276 XL_ERROR Synchronisation Timed out
25711279 Failed test 2
25722820 PART2 :Received status Init
25732382 Bevs_Protocol_State changed state from Performing_Pbi
25753036 XL_ERROR Synchronisation Timed out
25753043 XL_ERROR MFD 2 has failed to respond
25844651 System time is 12:00:31
25844983 Touchscreen_Handler changed state from Released
25844990 Touchscreen_Handler changed to Touch_Pending KDU
25926950 Touchscreen_Handler changed state from Touch_Pending
26090518 Touchscreen_Handler changed state from Touched
26090525 Touchscreen_Handler changed to Release_Pending KDU
26171707 Touchscreen_Handler changed state from Release_Pending
26252193 PART2 :Timeout in state Waiting_To_Send_SAL
26261228 XL_ERROR Synchronisation Timed out
26464062 XL_ERROR Synchronisation Timed out
26464071 XL_ERROR MFD 2 has failed to respond
26740034 PART2 :Received status Init
26861877 System time is 12:00:32
26973150 XL_ERROR Synchronisation Timed out
27064201 PART2 :Timeout in state Waiting_To_Send_SAL
27145481 Received sa 012000 FC18 0000 0000 0000 0000 0140 0000 000E 0000 0001 0000
27145497 Received sa 022000 FC18 0000 0000 0000 0000 0140 0000 000E 0000 0001 0000
27145510 Received sa 032000 FC18 0000 0000 0000 0000 0140 0000 000E 0000 0001 0000
27145516 Received sa 050000
27145527 Received sa 070000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
27145543 Received sa 091249 2491 2492 0481 0555 0000 0000 4155
27145638 Received sa 100000 0000 0000 0000 0000 4000 0001 0000 0000 0000 0000 0000 0000
27145659 Received sa 110000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
27145665 Received sa 150000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
27145671 Received sa 160000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
27145678 Received sa 170000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
27145712 Received sa 240000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
27145745 Received sa 250000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
27145774 Received sa 260000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
27145782 Received sa 180000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
27145790 Received sa 190000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
27145797 Received sa 200000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
27145803 Received sa 210000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
    
```

This document and all information contained herein is the sole property of EADS CASA. No intellectual property rights are granted by the delivery of this document or disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of EADS CASA. This document and its content shall not be used for any other purpose than for which it is supplied.

Offline Refuelling Operation Simulator (OROS)



This document and all information contained herein is the sole property of EADS CASA. No intellectual property rights are granted by the delivery of this document or disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of EADS CASA. This document and its content shall not be used for any other purpose than for which it is supplied.

Offline Refuelling Operation Simulator (OROS)

OROS Events Player: Events timeline

TimeLine for Events

UTC: 12h 2m 6s TIMESTAMP:

PU 1

SYNCHRO_HANDLER
Master
SYSTEM_STATE
Master

PU 2

SYNCHRO_HANDLER
Slave
SYSTEM_STATE
Slave

PUs / CHDDs Control

HMI Events for CHDD 1

HMI Events for CHDD 2

This document and all information contained herein is the sole property of EADS CASA. No intellectual property rights are granted by the delivery of this document or disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of EADS CASA. This document and its content shall not be used for any other purpose than for which it is supplied.

Offline Refuelling Operation Simulator (OROS)

Dialog
?

Monitors

12:02:25
R_PAN 00:00

DOPR

0 kg/min

12:02:25
CTR_PAN 00:00

0 kg/min

12:02:25
00:00 L_PAN

0 kg/min

12:02:25
CTR_PAN 00:00

0 kg/min

ARO VIEW

DUAL INSP L INSP

R INSP 3D

MS CTR_PAN

Panoramic Cameras

Inspection Cameras

Right IR Laser Light

Left IR Laser Light

UEC List

	Timestamp	System	UEC Number
1	12:02:03	MFC	CHDD1 - G25_F06 - TS FRAME DRIVER
2	12:02:03	MFC	CHDD1 - G25_F07 - TS FAILED BEAMES
3	12:02:03	MFC	CHDD1 - G13_F26 - LED SENSOR
4	12:02:02	MFC	MFC-PU1 VMU COMMUNICATION FAILED
5	12:02:03	MFC	CHDD2 - G13_F04 - LCD HEATER
6	12:02:03	MFC	CHDD2 - G25_F06 - TS FRAME DRIVER
7	12:02:03	MFC	CHDD2 - G25_F07 - TS FAILED BEAMES
8	12:02:03	MFC	CHDD2 - G13_F26 - LED SENSOR
9	12:02:07	MFC	MFC-PU2 VMU COMMUNICATION FAILED
10	12:02:03	MFC	CHDD1 - G13_F04 - LCD HEATER
11	10:48:06	MFC	CHDD2 - DV12 FAULT
12	10:48:18	CNI_Comms...	NO COMMUNICATION RMS1 WITH MFC1
13	10:48:18	CNI_Comms...	NO COMMUNICATION RMS2 WITH MFC1

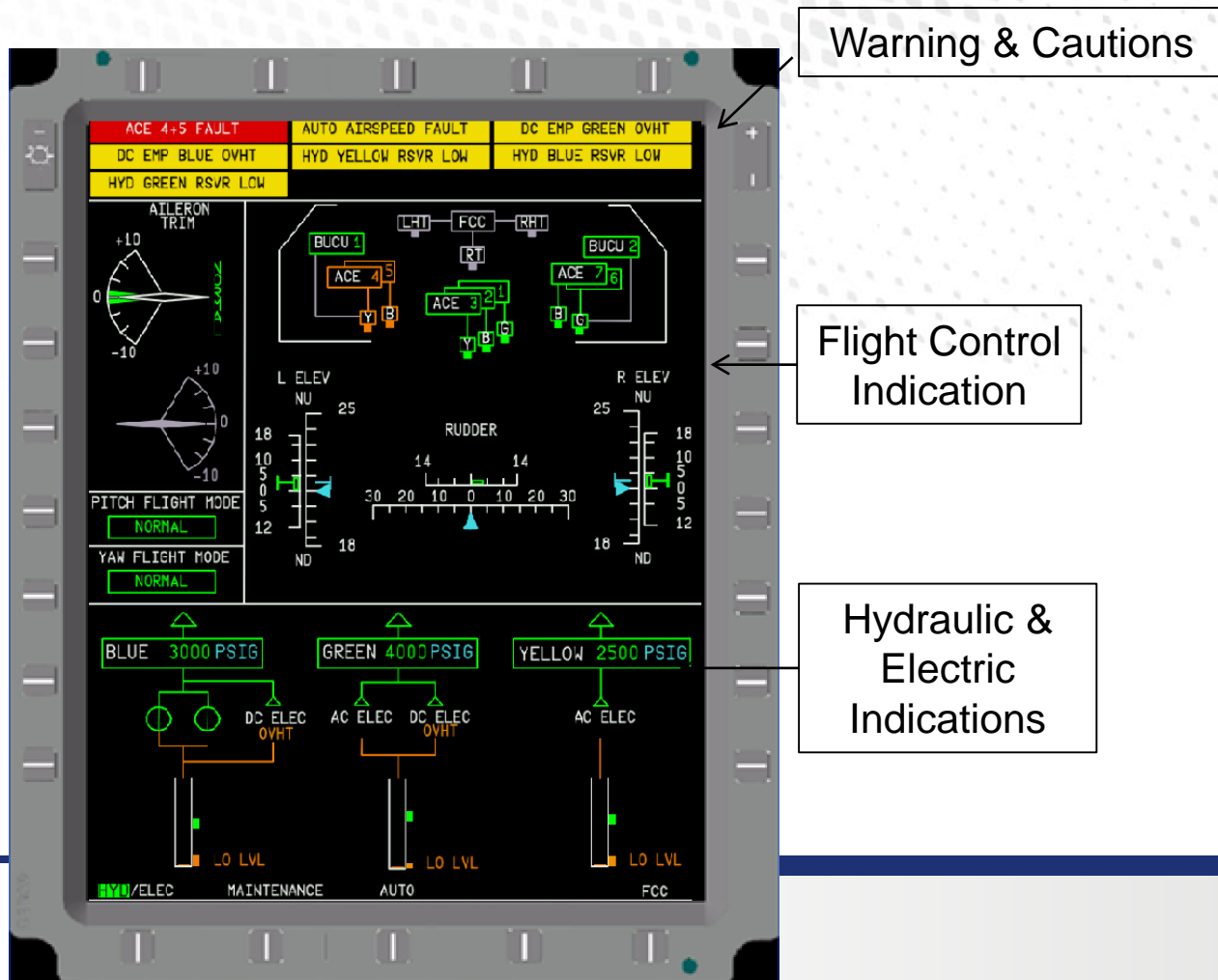
Tailcone IR Laser light 1

Tailcone IR Laser light 2

This document and all information contained herein is the sole property of EADS CASA. No intellectual property rights are granted by the delivery of this document or disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of EADS CASA. This document and its content shall not be used for any other purpose than for which it is supplied.

D2CU System

- Two D2CU (Data Display Control Unit) are installed in the cockpit to provide Information to the pilots about the C295 Aircraft Data for this Fly By Wire Prototype under ClearSky2 project.



Warning & Cautions

Flight Control Indication

Hydraulic & Electric Indications

D2CU Development

• HW

- Esterline PU-2000 & CHDD-268

• SW

- Partitioning-based SW Architecture (4 partitions)
- VxWorks 653 (2.2.1.1)
- D2CU developed with SCADE, HMI (Display) + Behaviour (Suite)
 - KCG6.6 - Qualifiable as DO-330 TQL-1 tool under DO-178C or DO-178B
- IO & Moding partitions developed with Ada 95

Process (Lessons Learnt)

• First Prototype

- All Manual Code in Ada95. Link with C code via pragma import.
- Each new model integration took several weeks. Mapping Ada Types and C-structs generated by KCG are complex.
- SCADE Display KCG has been qualified as development tool for DO-178B up to level A

• Actual Status

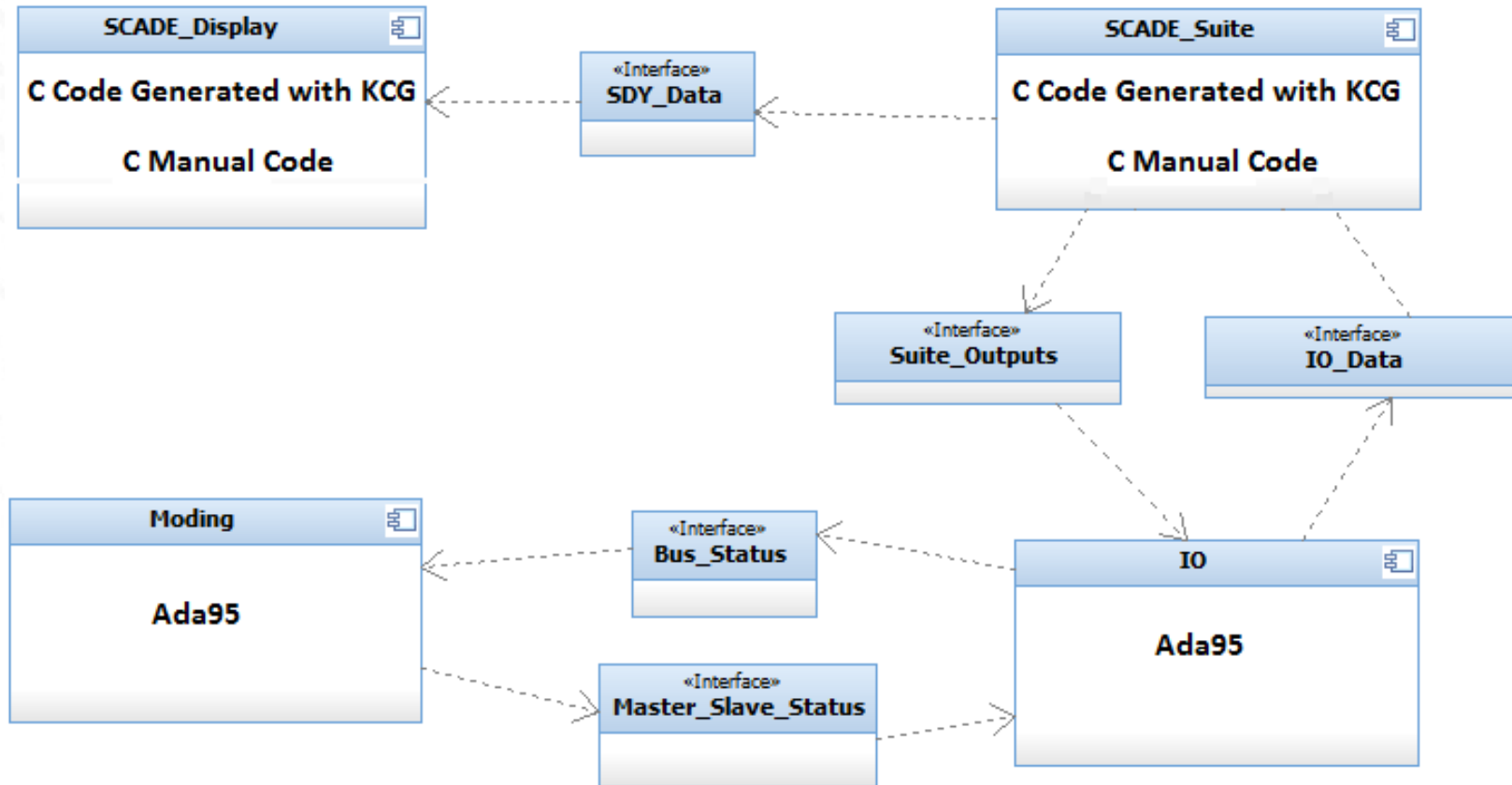
- Separate C/Ada Partitions communicating data through Apex Ports.
- Data Interface between partitions defined in Doors.
- Several model integration done in one day.
- Types range protection included in partition communication to avoid abnormal situations.

• Future

- AESA Flight Permit for first flight expected by end 2016.

D2CU Architecture

• Current D2CU Partition Architecture



This document and all information contained herein is the sole property of EADS CASA. No intellectual property rights are granted by the delivery of this document or disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of EADS CASA. This document and its content shall not be used for any other purpose than for which it is supplied.

D2CU & SCADE Tools

- SCADE Display

An easy environment to create HMI specification. It includes some simulation capabilities allowing the user to test in a computer before loading the sw into the target. Reducing time/costs.

- SCADE Suite

- Simple logic for activating some indications.
- Complex logics (Master/slave selection and other) remain in Ada95

- Requirements Gateway

This tools allows an easy way to trace DOORS requirements to any object in the specification/model.

- SCADE Test

- Automatic test tool including HMI (currently being evaluated).

Questions?
