Security Testing with Controller-Pilot Data Link Communications

D Di Marco (ENAV), A Manzo (SICTA), J Hird (EUROCONTROL), M Ivaldi (@mediaservice.net)

SecATM Workshop
ARES 2016
Salzburg, Austria
02/09/2016

Presenter - John Hird

ATM System Assets – What Are We Trying to Protect?

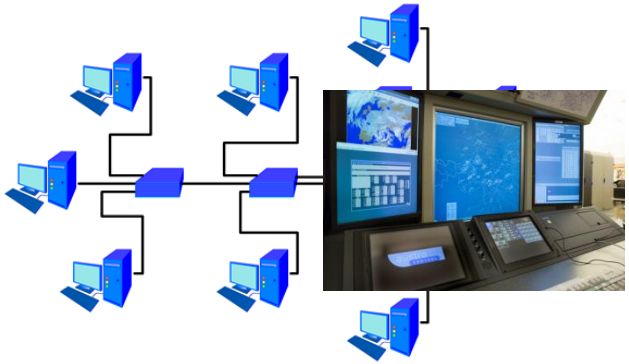
Service Provision

Physical: *e.g. Communications, Navigation, Surveillance (CNS), ATM centres, ...*

Staff: *Operational, Engineering, IT …*

Information: *Operational, Historical*

Organisational: *Financial, Reputation*



Information Systems

Staff

CNS Systems

ANSP Facilities

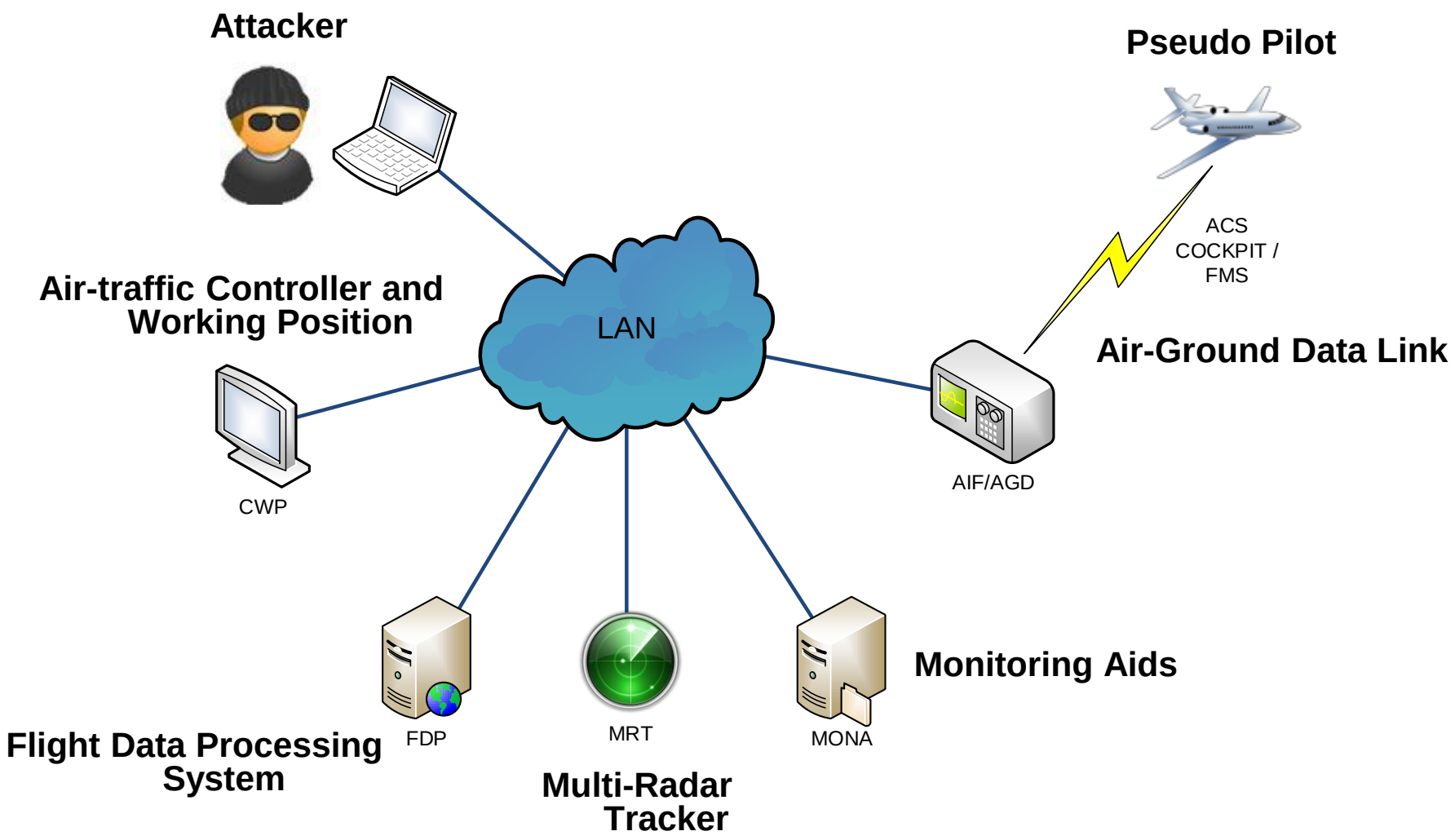
Service Provision

Potential Consequences of an Attack – Impact Areas

Personnel	Stress, minor injury, …, fatality
Capacity	Reduction, loss
Performance	Reduction, loss
Economic	Financial loss
Branding	Reputation
Regulatory	Breach of requirement
Environment	Impact on environment

Cyber Attack Simulation

Security Test - Simplified Network Architecture



Approach Taken

Security risk Assessment :

- Use the SESAR SecRAM methodology to identify potential threats applicable to CPDLC

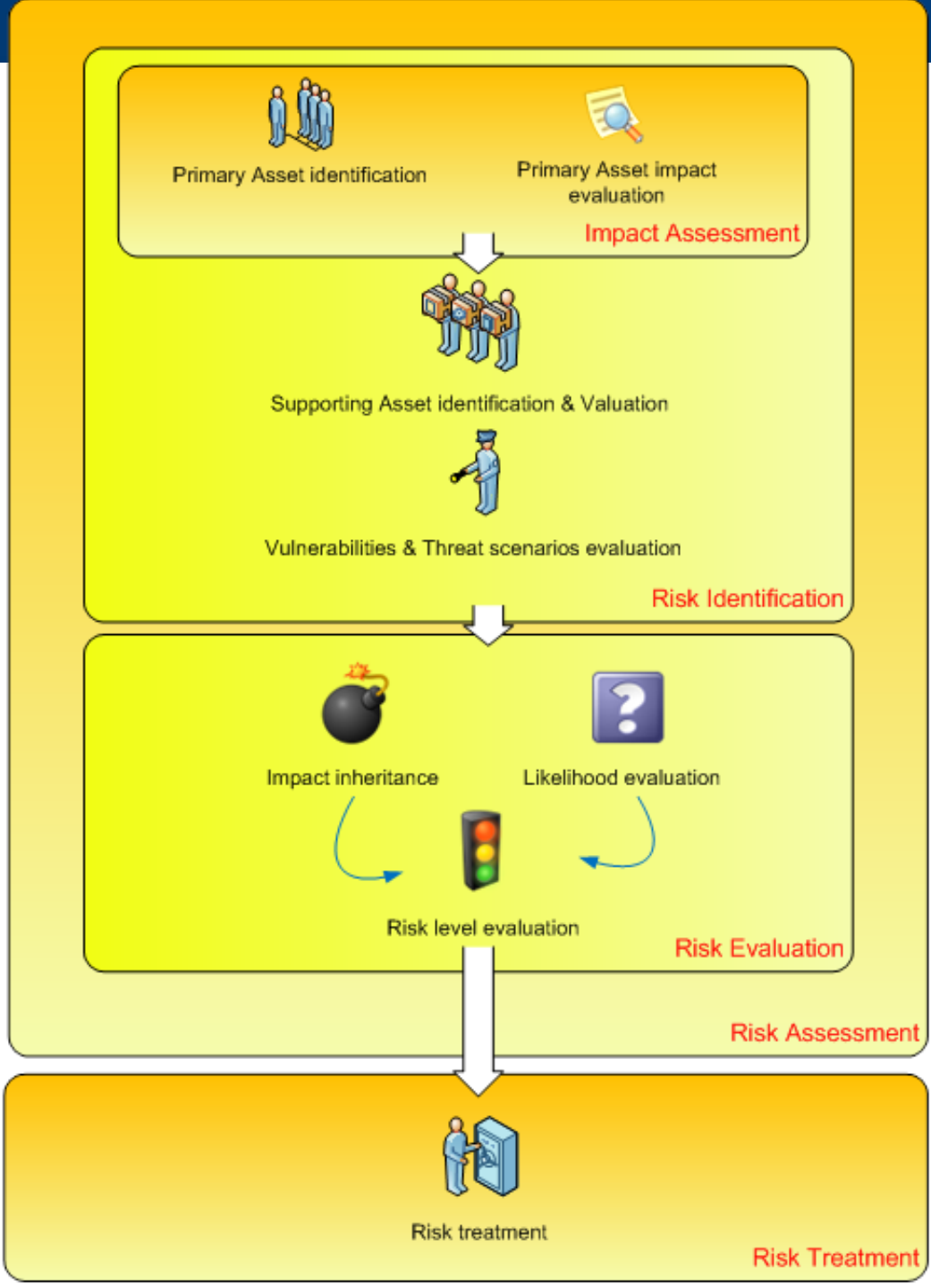
Security testing sessions:

- Select and Perform a Cyber attack on a specific technical and operational scenario

The Security Risk Assessment Methodology

Identify :

- Assets
- Impacts on CIA
- Risks
- Controls



Primary & Supporting Assets

Primary Assets:

intangible entities

- processed/used information
- services executed/provided

Supporting Assets:

tangible entities that enable the primary assets e.g.:

- Systems
- Network
- People

	Primary Assets				
Supporting Assets	PA#1	PA#2	PA#3	PA#4	PA#5
	Flight data Management for i4D (CTA)	Arrival Management	Controller working position ASPA services	Surveillance Management	ASPA S&M Messages management
Flight Data Processor (FDP)	X				X
FMS	X				X
Controller Working Position			X		
Surveillance				X	
Monitoring AIDS				X	
Air Ground Data Link	X	X			X
LAN (in RTS)	X	X	X	X	X
AGDL network (only in live trial)*		X		X	X
Executive controller	X		X	X	X
Planner controller		X	X	X	
Pilot	X				X

Threats to Supporting Assets

Supporting Assets	Type	Reference	Threat	Likelihood
Air Ground Data Link	Compromise of functions	Th_C_Fun02	Denial of Service	3
	Unauthorized action	Th_C_Act01	Corruption of data	2
	Unauthorized action	Th_C_Act02	Cyber intrusion	2
LAN (in RTS)	Compromise of functions	Th_C_Fun02	Denial of service	3
	Compromise of functions	Th_C_Inf02	Network eavesdropping	3
	Unauthorized action	Th_C_Act01	Corruption of data	2
Executive controller Planner controller	Attack through Internal perpetrators	Th_P_Int01	Internal perpetrator	1
	Abuse of rights	Th_P_Abu01	illicit use of equipment or personal access rights	2
	Compromise of information	Th_C_Inf01	Disclosure of confidential information via electronic means	1
Pilot	Attack through Internal perpetrators	Th_P_Int01	Internal perpetrator	1
	Abuse of rights	Th_P_Abu01	illicit use of equipment or personal access rights	1

Risk Assessment Conclusions

Top Risks

- Impact of Integrity on Flight data Management for i4D → High
- Impact of Integrity on Arrival Management → High
- Impact of Integrity on **ASPA S&M message** management → High

Medium Risk

- Impact of Availability on all PAs → Medium (due to LAN and AG data link network)

	Reviewed Impact				
Likelihood	1	2	3	4	5
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

Acronyms

ASAS – Airborne Separation Assurance System

ASPA S&M – Airborne Separation Assistance Spacing & Merging

Selected Attack Scenario

Threat Description

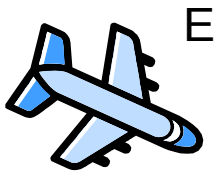
- CPDLC traffic is neither authenticated nor encrypted.
- Consequently, the data is vulnerable to breach of confidentiality (eavesdropping)
- The data is also vulnerable to intentional modification (breach of integrity)
- An attacker with access to CPDLC traffic (either on the local network or potentially over radio communication) might be able to exploit the lack of integrity and authentication in order to perform packet injection and manipulation.

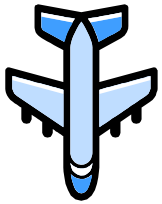
Packet Injection and Manipulation

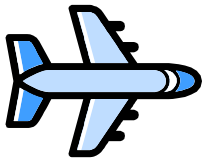
- Aimed at impacting the services in scope, resulting in, for example, the loss of integrity of aircraft trajectories (e.g. i4D, AMAN), or CWP messages.
- Operational consequences include a potential impact on Safety, Capacity, and Performance.

→ Vulnerability tests concentrated on this specific misuse case, in order to demonstrate the weaknesses of communication protocols against threats affecting Integrity.

Sequencing & Merging (1/2)

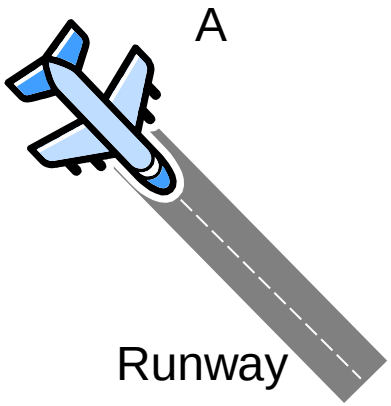




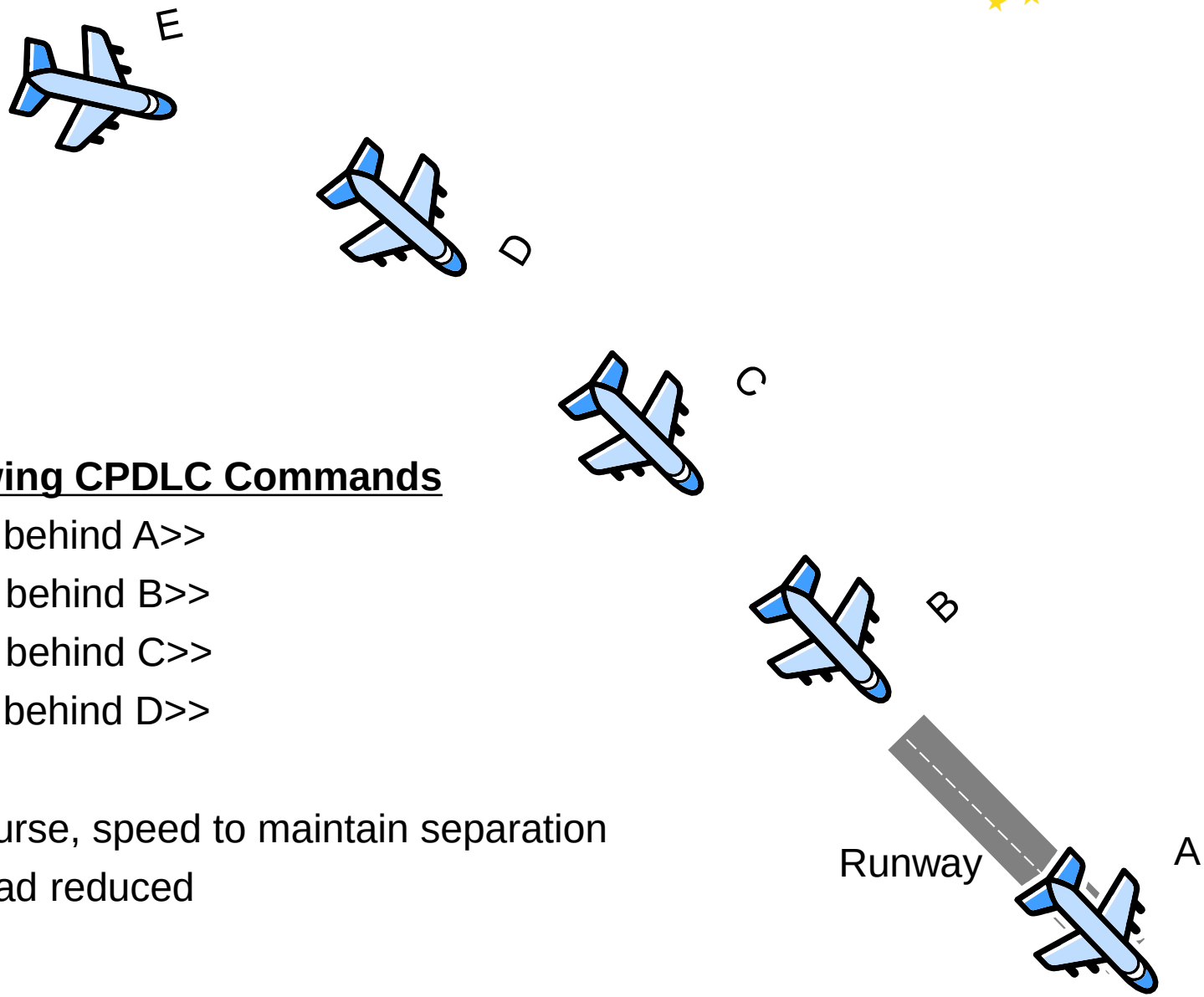


Possible CPDLC Commands from Controller to pilots

- To B : <<Remain behind A>>
- To C : <<Remain behind B>>
- To D : <<Remain behind C>>
- To E : <<Remain behind D>>



Sequencing & Merging (2/2)

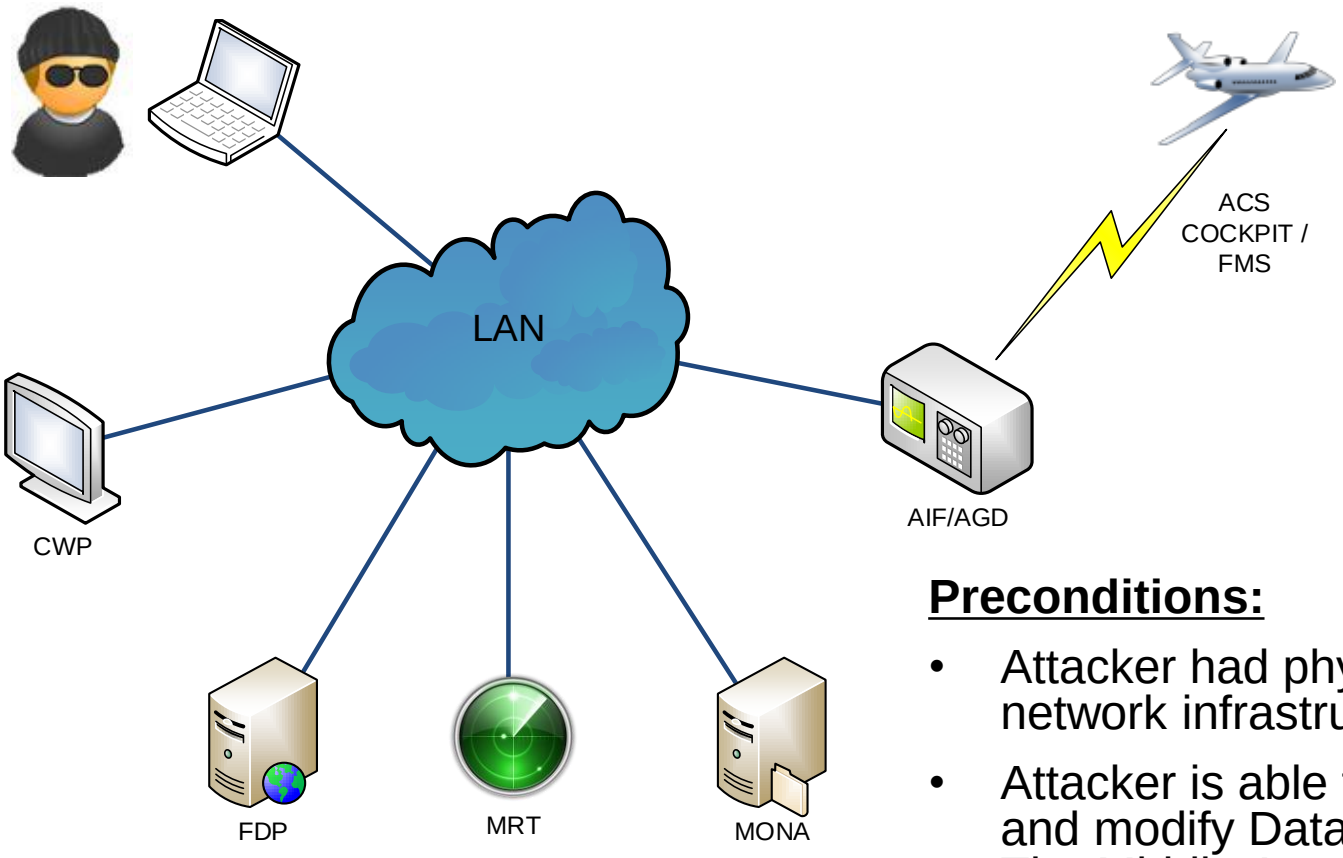


Result of the following CPDLC Commands

- To B : <<Remain behind A>>
- To C : <<Remain behind B>>
- To D : <<Remain behind C>>
- To E : <<Remain behind D>>

- Aircraft adjust course, speed to maintain separation
- Controller workload reduced

Cyber Attack Simulation



EXE-805 Simplified Network Architecture

Preconditions:

- Attacker had physical access to the network infrastructure(→low likelihood)
- Attacker is able to act as the controller and modify Datalink messages (Man in The Middle Attack)

Note:

- Controllers and Pilots in the exercise were not aware of the details of the test.

Scenario Description (1/5)

CONTROLLER

The controller sends an order to VLG5192 to select as target the flight EZY47HC (ASAS «SELECT TARGET» message)

ATTACKER

Via a Man in The Middle (MITM) attack, the Datalink message is modified by replacing the EZY47HC flight with another nearby flight, DLH2025 (see picture)

PILOT

Even if the pseudo-pilot recognizes that something unusual is happening, he accepts the Datalink command (select the DLH2025 flight as target)

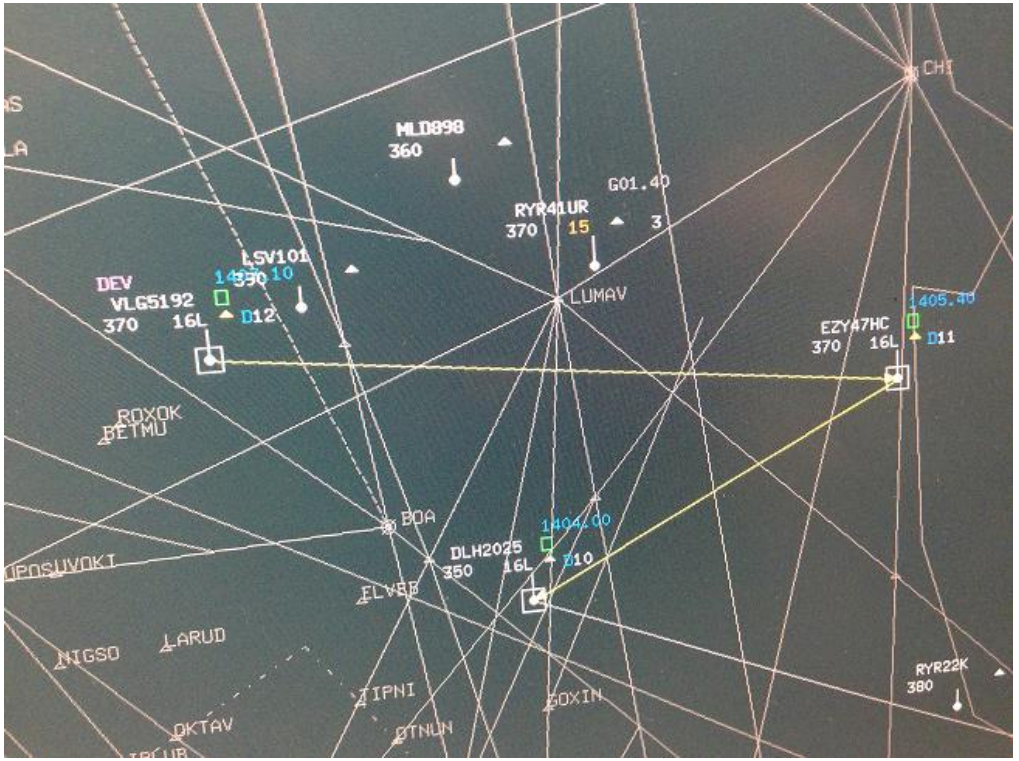
Message Modified via MITM

Scenario Description (2/5)

CONTROLLER

The controller visualizes the ASAS command as he inserted it into the tool (Target EZY47HC)

Note that in this phase, the controller has no visibility of the actual message received by the pilot



Controller's View

Scenario Description (3/5)

CONTROLLER

After a few minutes, at arrival phase, the controller sends the flight VLG5192 a «remain behind EZY47HC» message.

ATTACKER

The MITM attack is still active: the Datalink message related to the remain behind is modified as the previous one and the target is replaced with DLH2025

PILOT

The pseudo-pilot accepts the «remain behind» with the DLH2025 and consequently increases the speed to reach the target

Pilot's View

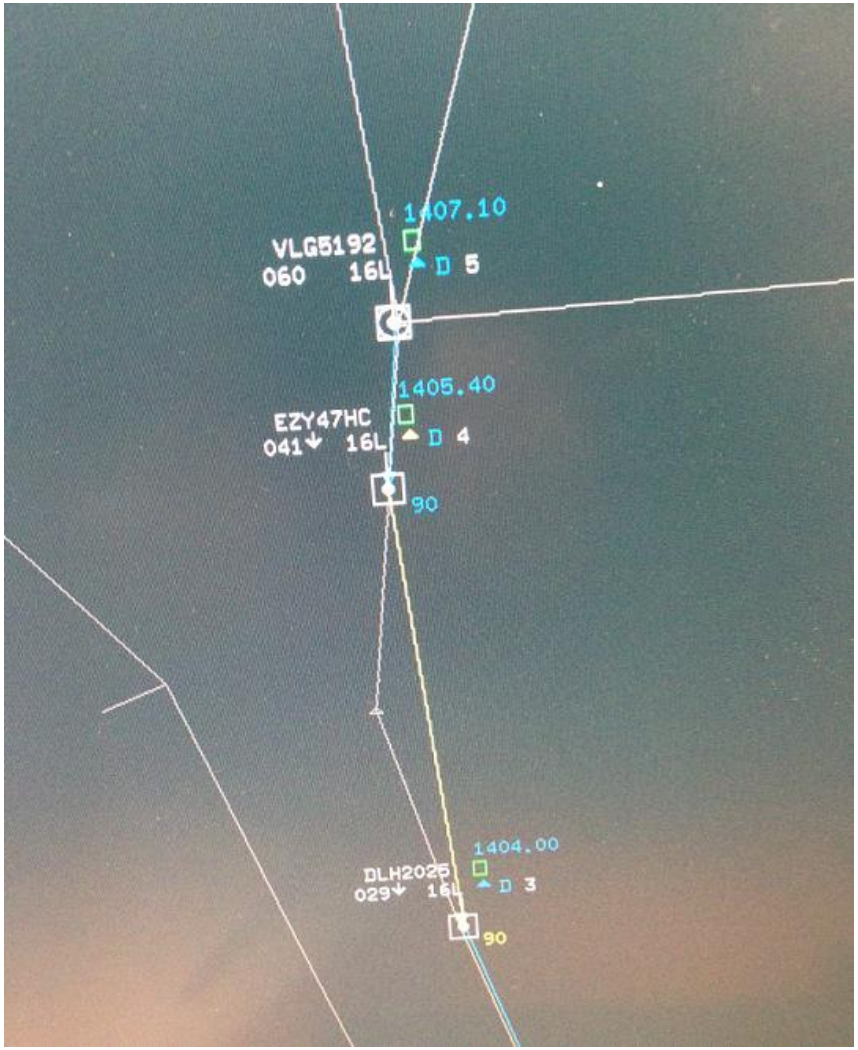
Scenario Description (4/5)

CONTROLLER

À few seconds after the command has been sent, the controller observes unusual (and potentially dangerous) behaviour of flight VLG5192:

- an unexpected increase in velocity, and
- a reduction in longitudinal separation with flight EZY47HC

Note: no separation infringement is observed due to the different flight level - "vertical separation"



Controller's View

Scenario Description (5/5)

CONTROLLER

Due to the unexpected maneouvre by the pseudo-pilot caused by the “remain behind” command :

- the controller cancels the ASAS maneuver via radio

The approach controller’s comment was:

“Due to a sudden and unexpected speed increase during an ASPA maneouvre between EXY47HC and VLG5152, the maneouvre was interrupted and flight VLG5152 was positioned in sequence”

Controller’s View

Test outcome

Exercise Run

- From a Safety point of view, no incidents have occurred, because the controller noticed the anomaly in time and re-established standard procedures.
- Nevertheless, a loss of confidence has developed and before the controller recognized the anomaly, two flights had reduced their longitudinal separation (although they were still separated vertically).

General comments

- The CPDLC protocol is vulnerable to threats affecting data integrity because of weaknesses in the authentication mechanisms (authentication of the control center that sends the data is not supported natively by the protocol).
- Without a radio confirmation, a generic cyber attack on a generic Datalink scenario is potentially very risky.

Summary

Security risk Assessment:

- SESAR SecRAM methodology to identify potential threats applicable to EXE-805 concepts and systems

Main result:

- Threats on integrity and availability of Datalink messages are applicable to the test scenario

Security testing sessions:

- Cyber attack on technical and operational scenario :
  - Intentional Modification of ASPA messages

Main result:

- Modification of Datalink messages is possible
- Cyber attacks can result in operational consequences

Conclusions

- The intentional modification of ASPA messages may impact Key Performance Areas, including:
  - **Safety**
  - **Capacity**
  - **Performance**
- This attack demonstrates some weaknesses of communications protocols against threats affecting Integrity.
- Security tests may highlight weaknesses and provide guidance for security controls to be taken into account.

Recommendation

→ Apply all security recommendations as described in SESAR 16.06.02 Security Reference Material from the initial phases of the Software Development Life Cycle (SDLC).


Thank you!