



GEstion Optimisée et sécurisée des DonnEes pour le Système d'Information Embarqué

GEODESIE

Jean Arlat, Yves Deswarte, Youssef Laarouchi, David Powell

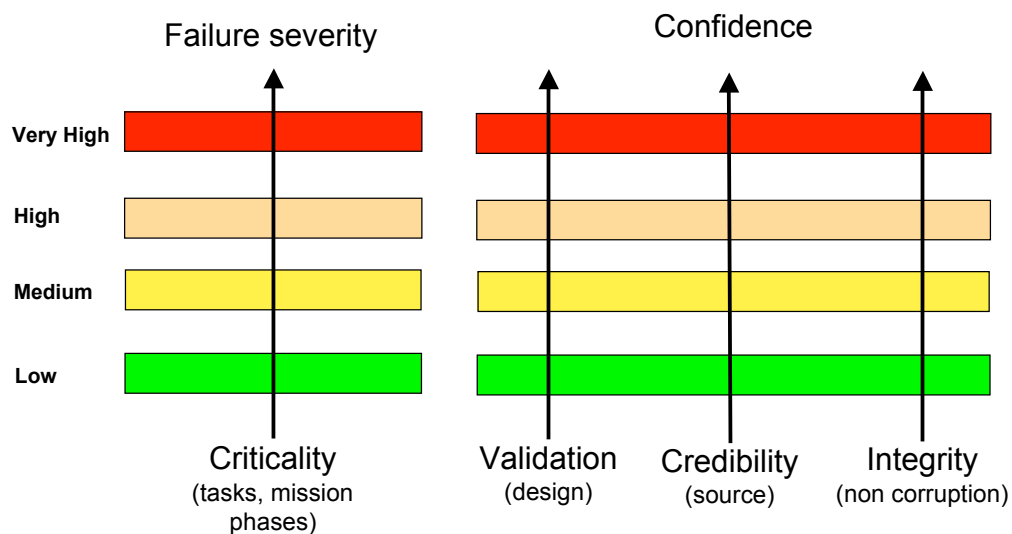
GEODESIE project



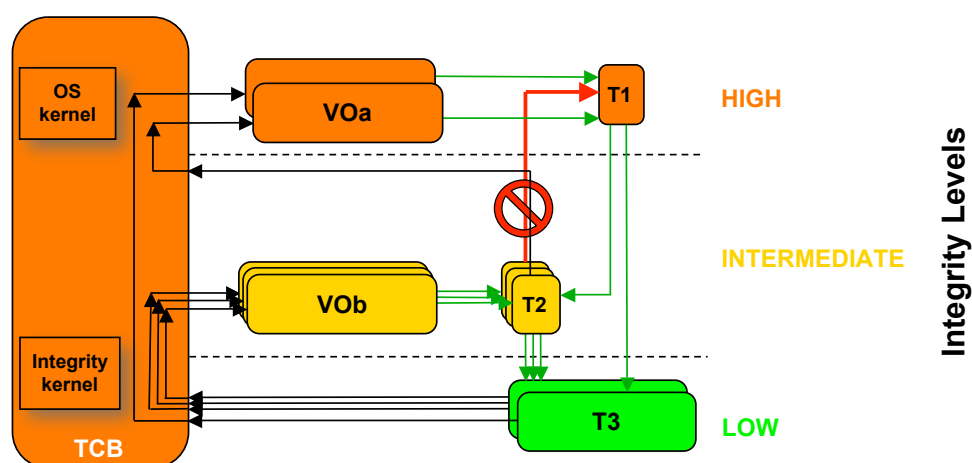
Isolation + Tolerance

- Multiples tasks of various criticalities must interact with each other
- 2 classical solutions:
 - Certify all tasks to the highest level
--> too costly
 - Unidirectional Firewalls
--> too restrictive

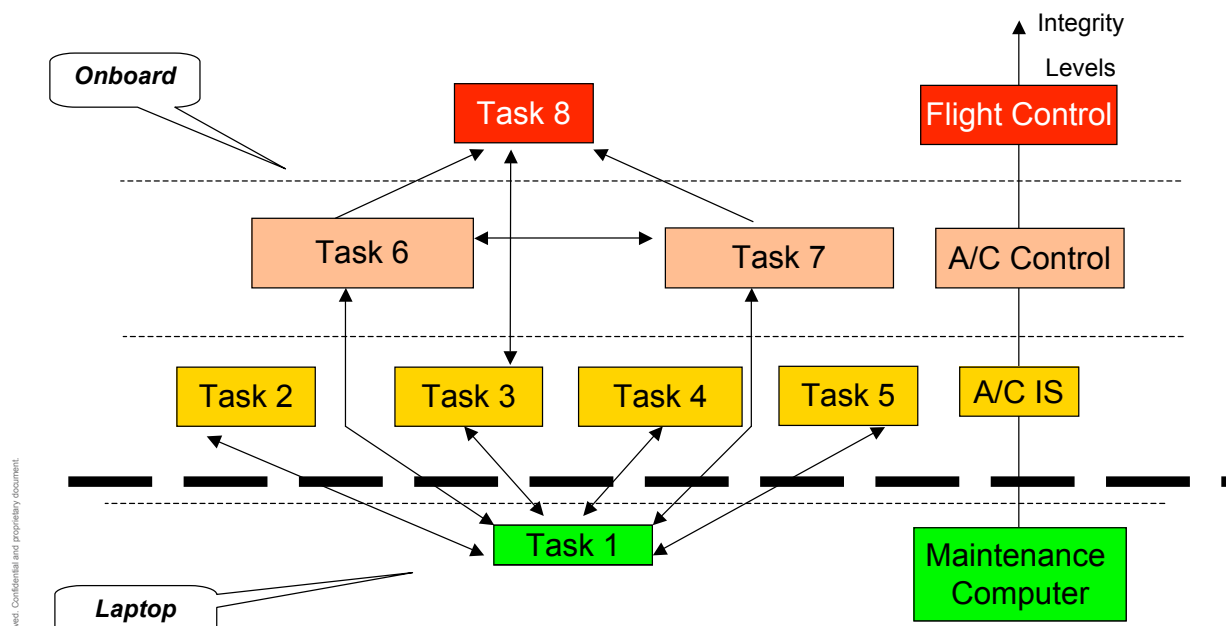
Security/safety multilevel approach



Flow Control Model (Totel 98)



1st case : Maintenance Operation



© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

GEODESIE project

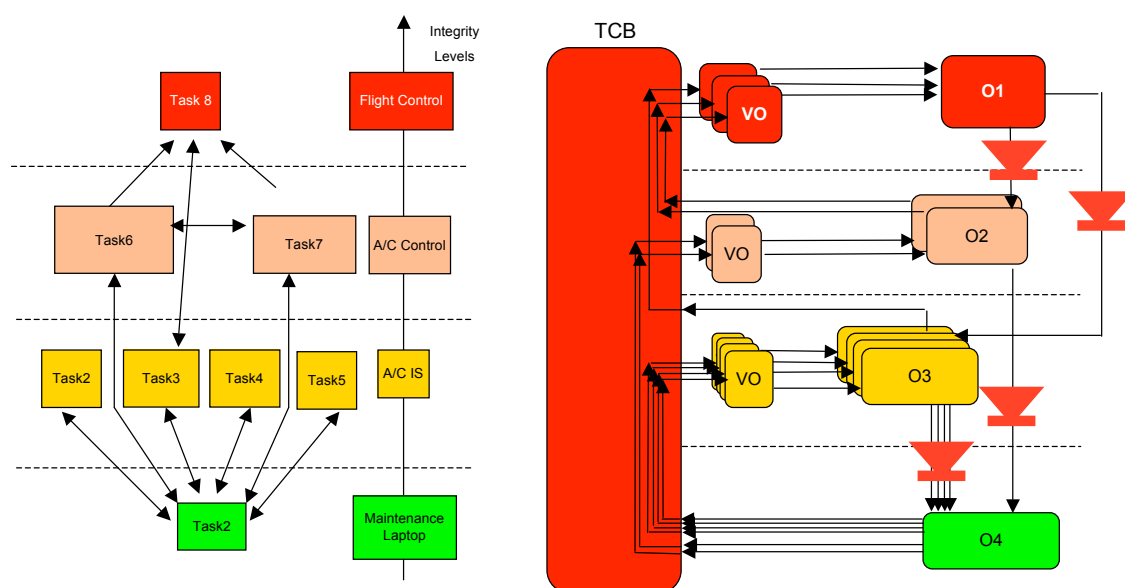


28 novembre 2008

Page 5



Mapping to Totel's model



© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

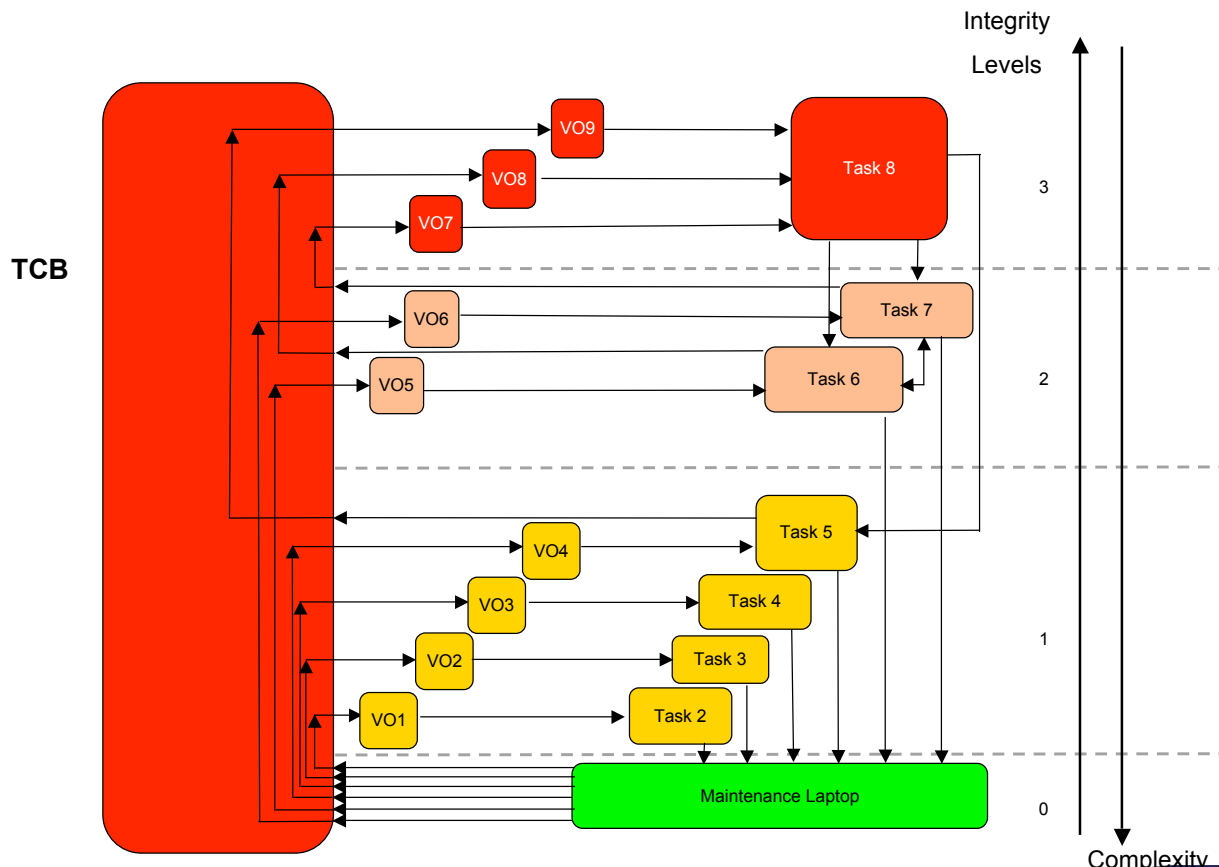
GEODESIE project



28 novembre 2008

Page 6



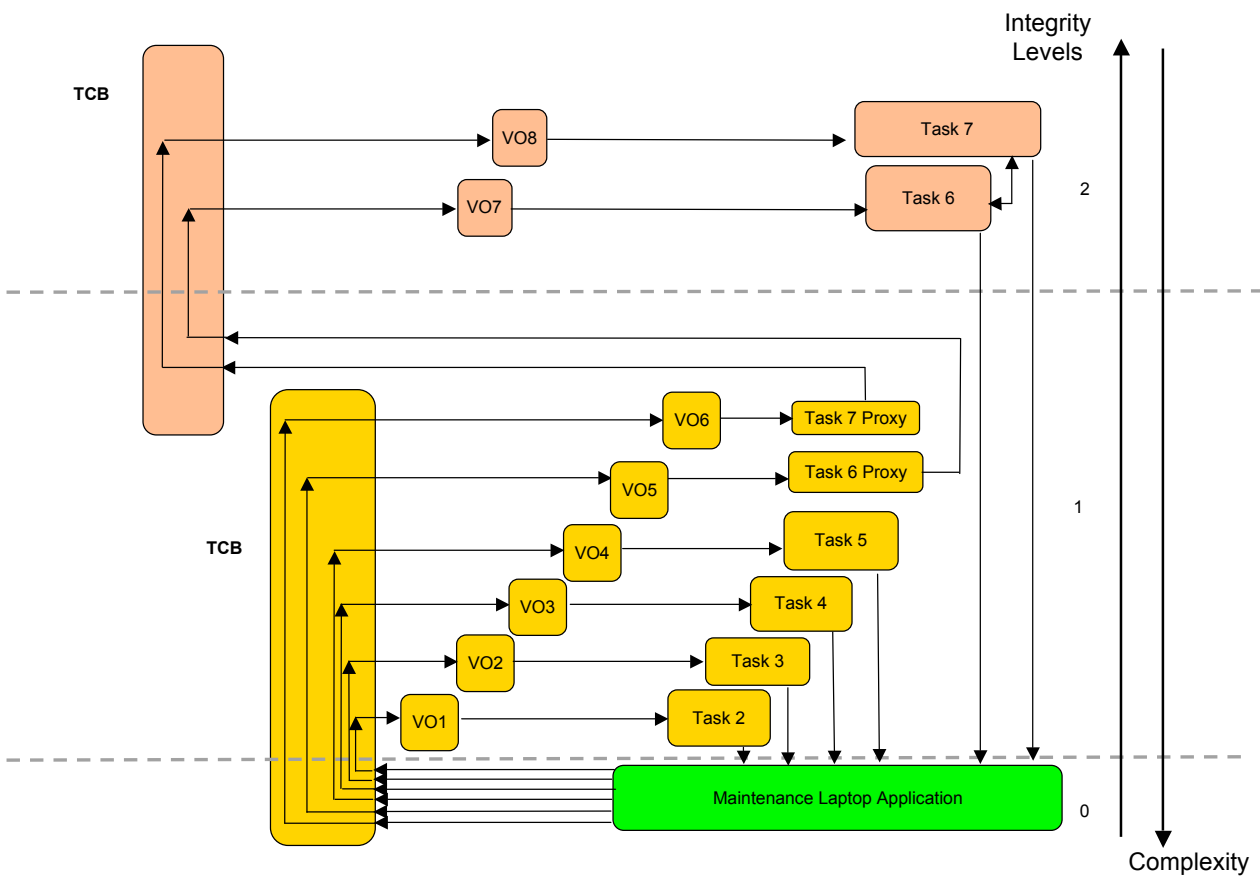
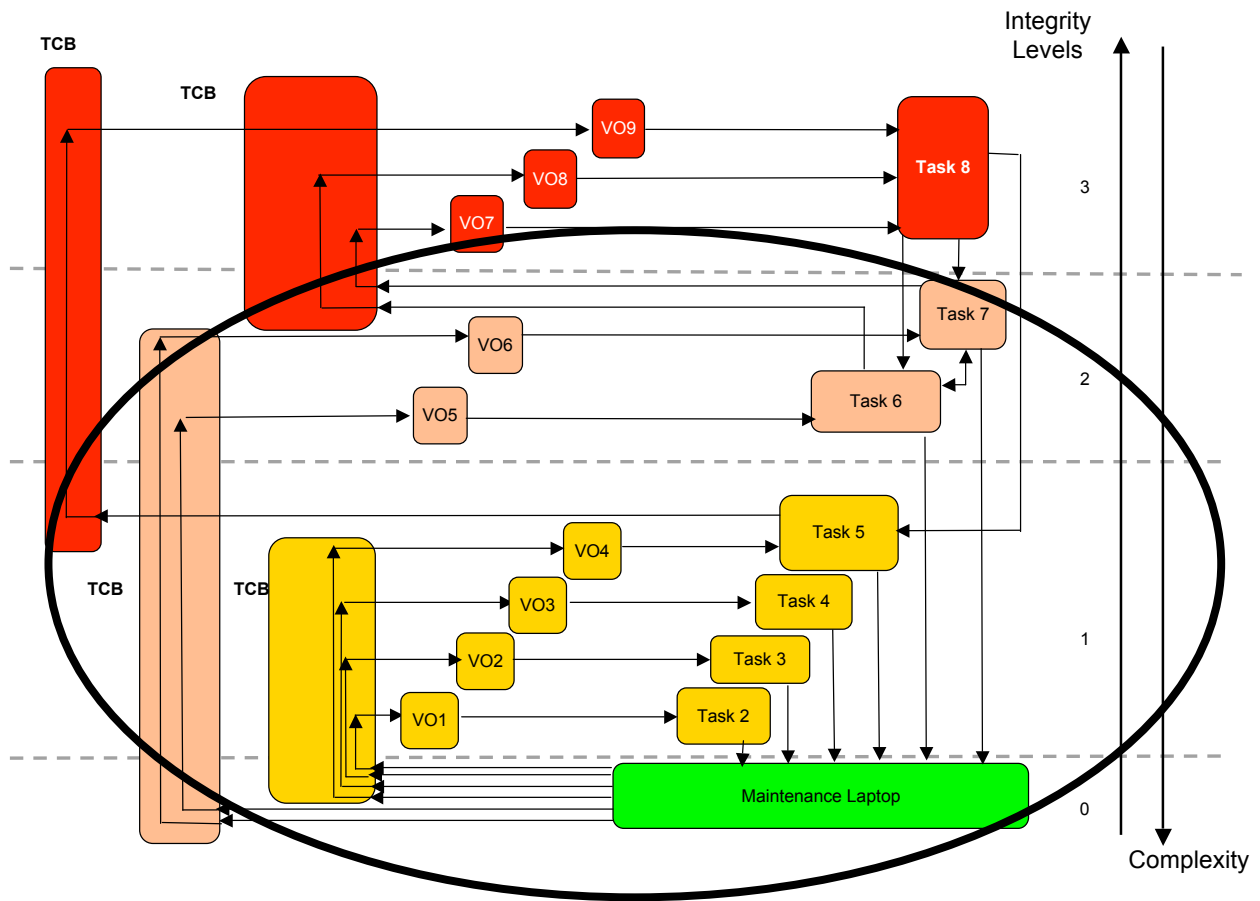


TCB implementation and validation

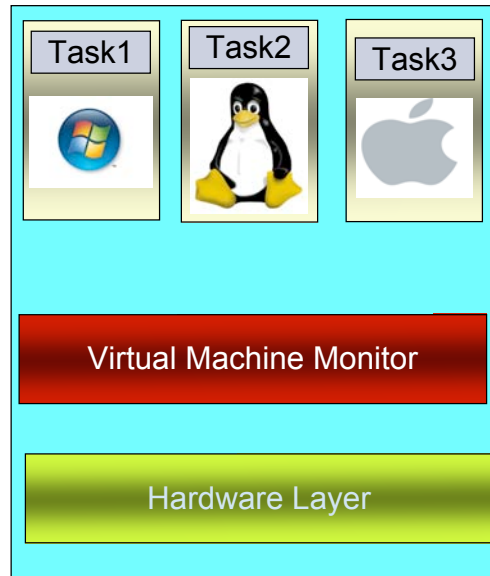
- The TCB manages all integrity levels:

- **Criticality** of the highest level
- **Complexity** of the lowest level

→ **TCB Validation ?**



Diversification by Virtualization



© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

GEODESIE project

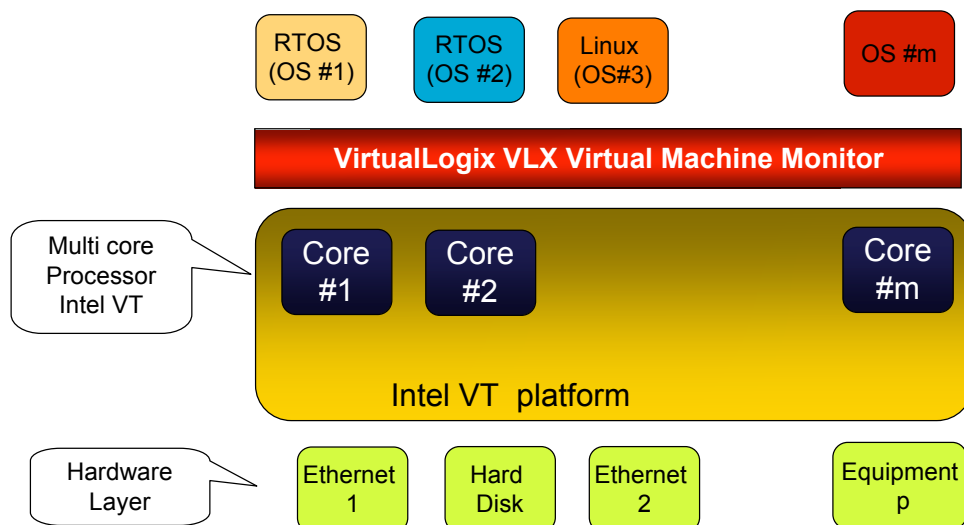


28 novembre 2008

Page 11



VLX Monitor



© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

GEODESIE project

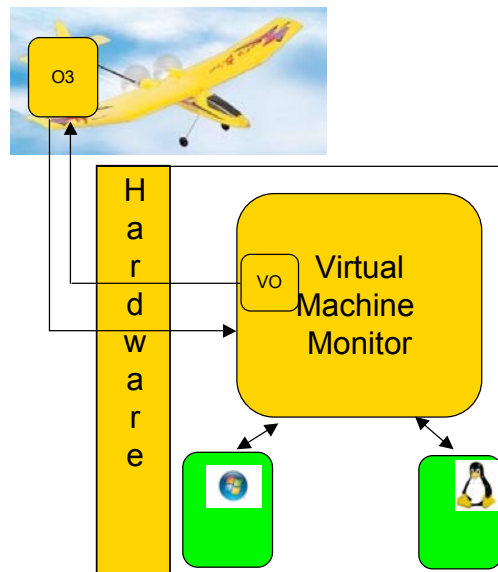
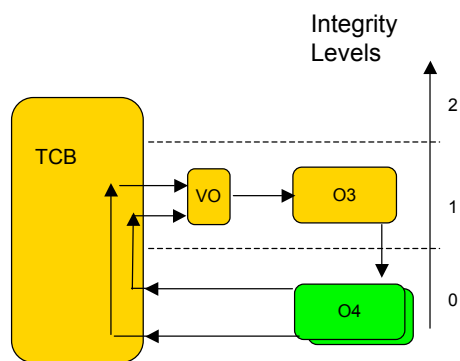


28 novembre 2008

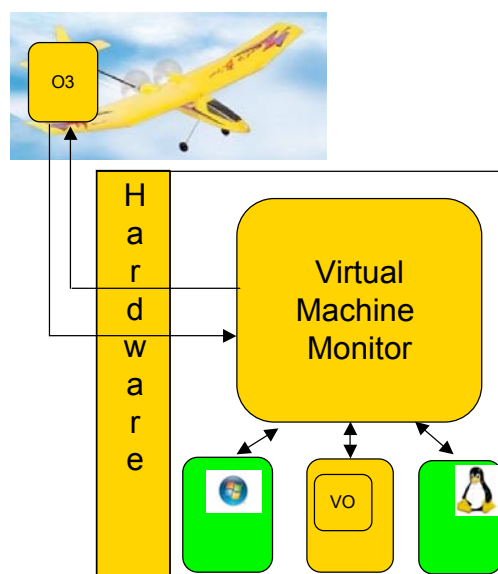
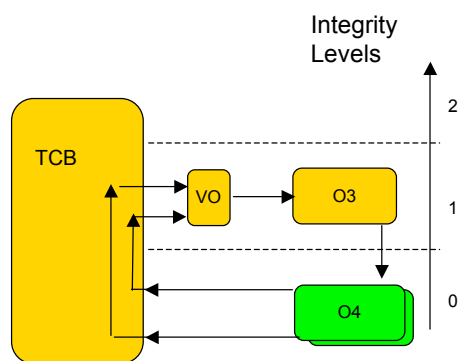
Page 12



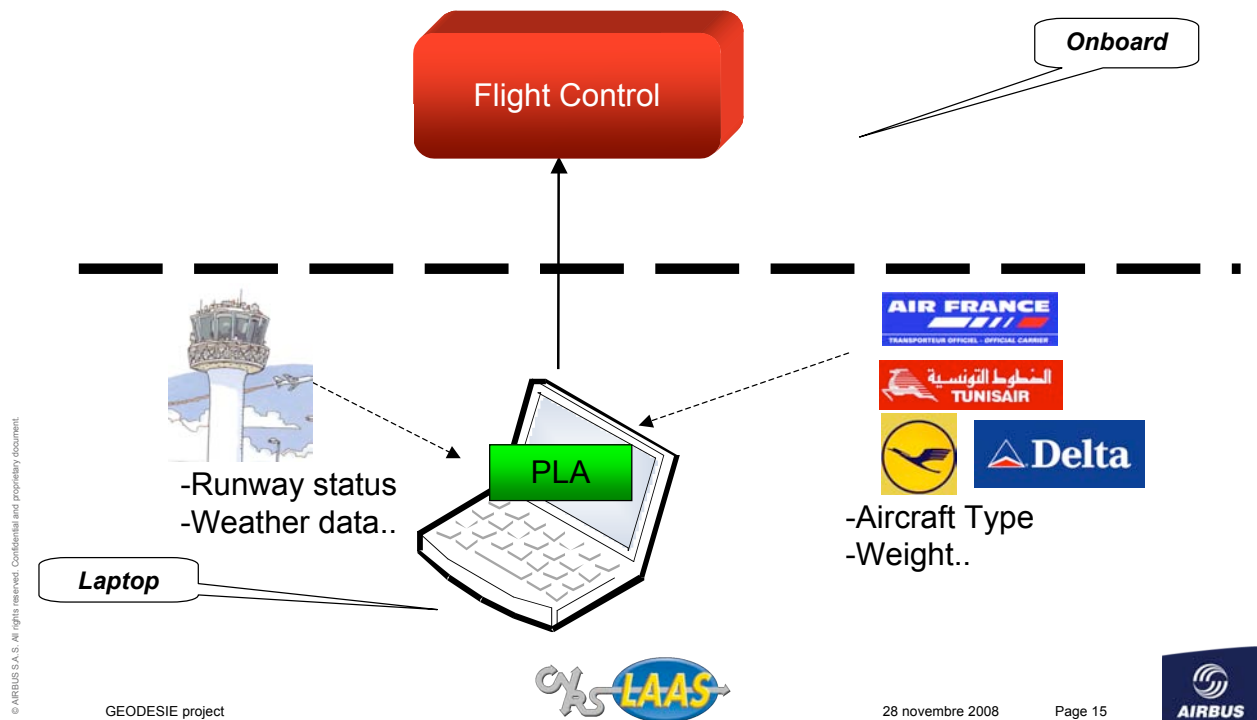
Virtualization and Totel's model



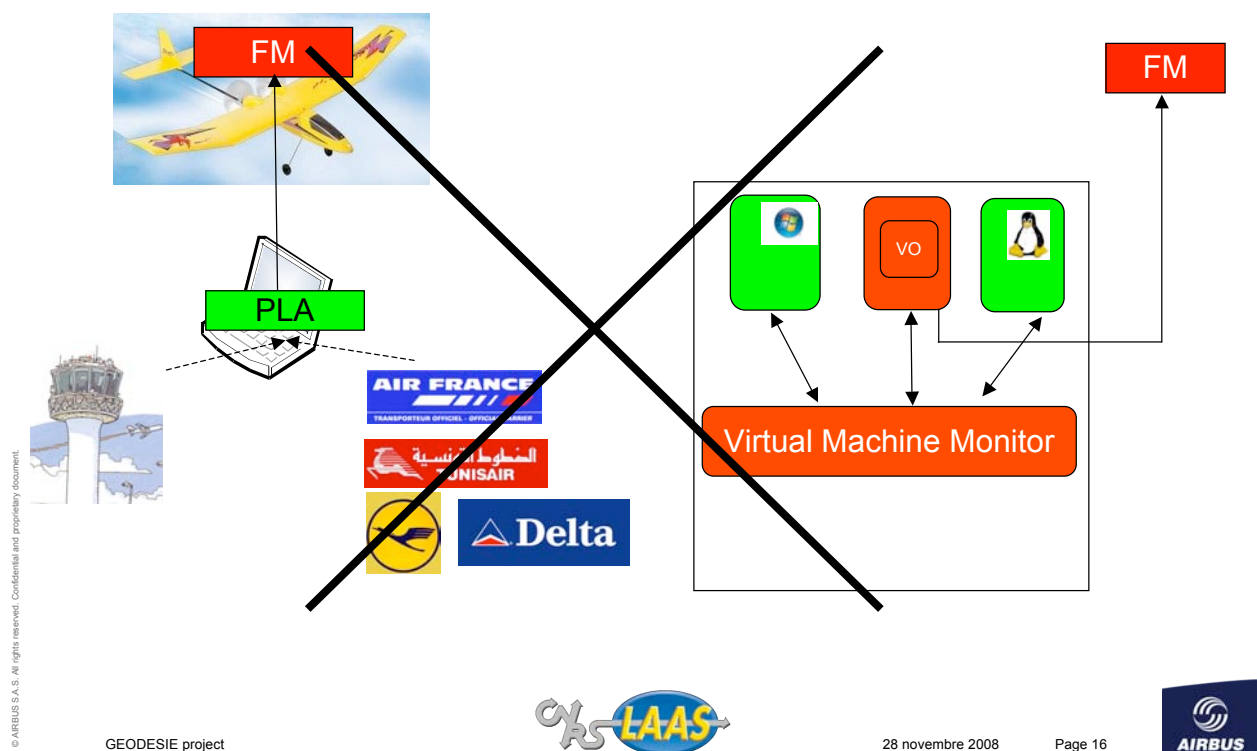
Virtualization and Totel's model



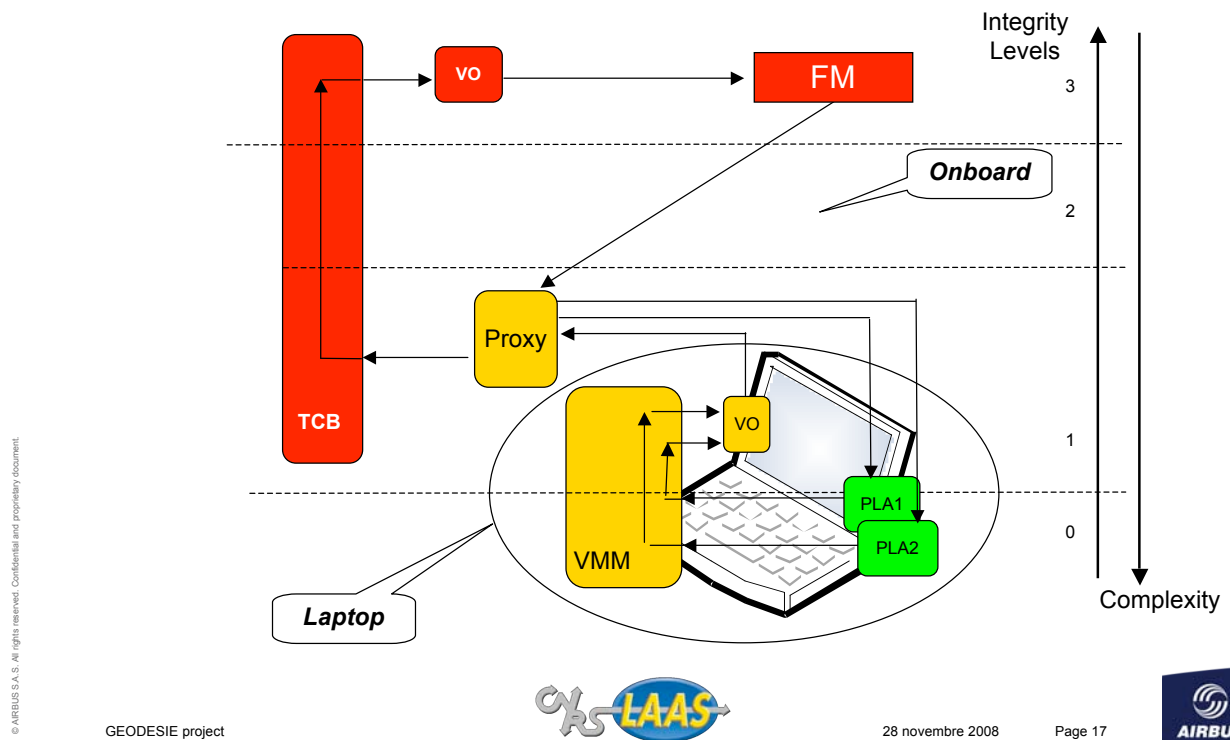
2nd case : Pilot Laptop Application



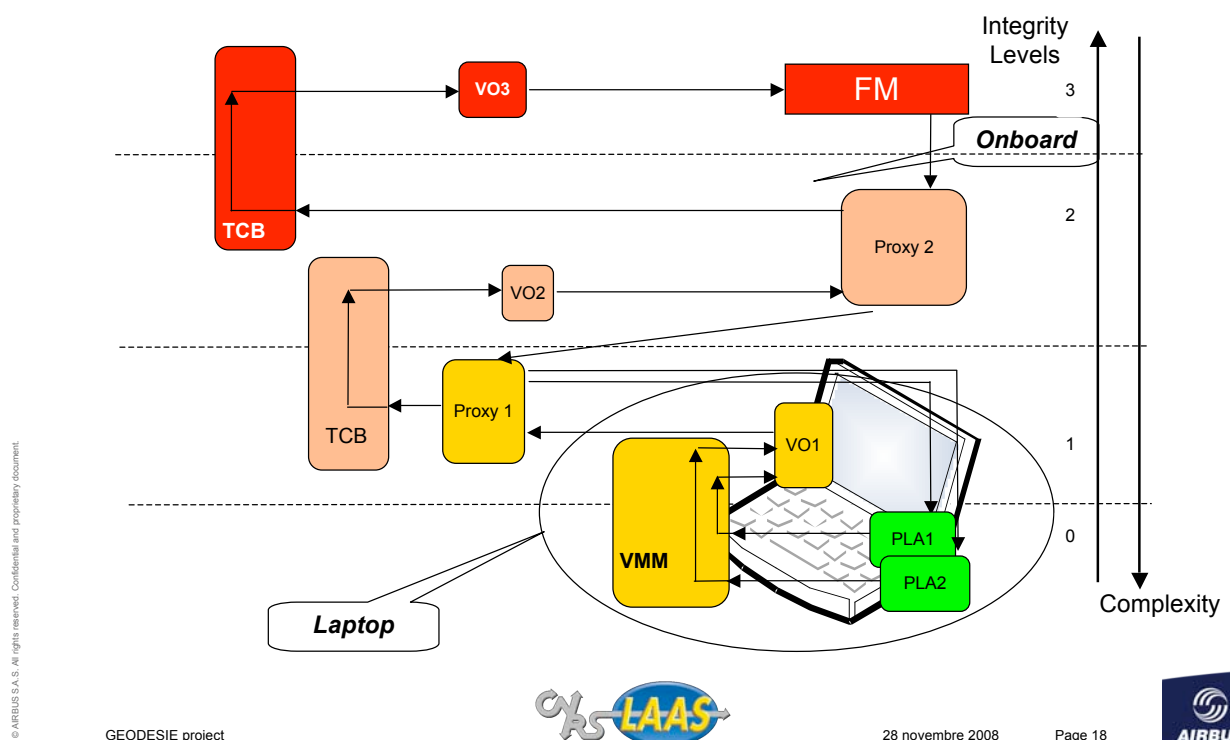
Application to the 2nd case study



Application to the 2nd case study



Application to the 2nd case study



ArSec Project (Airbus-LAAS)

- Fault tolerance mechanisms to be implemented into [Validation Objects](#)
- Flow control mechanisms:
 - Applications
 - Network gateways
 - Middleware
 - OS
 - Hypervisor

