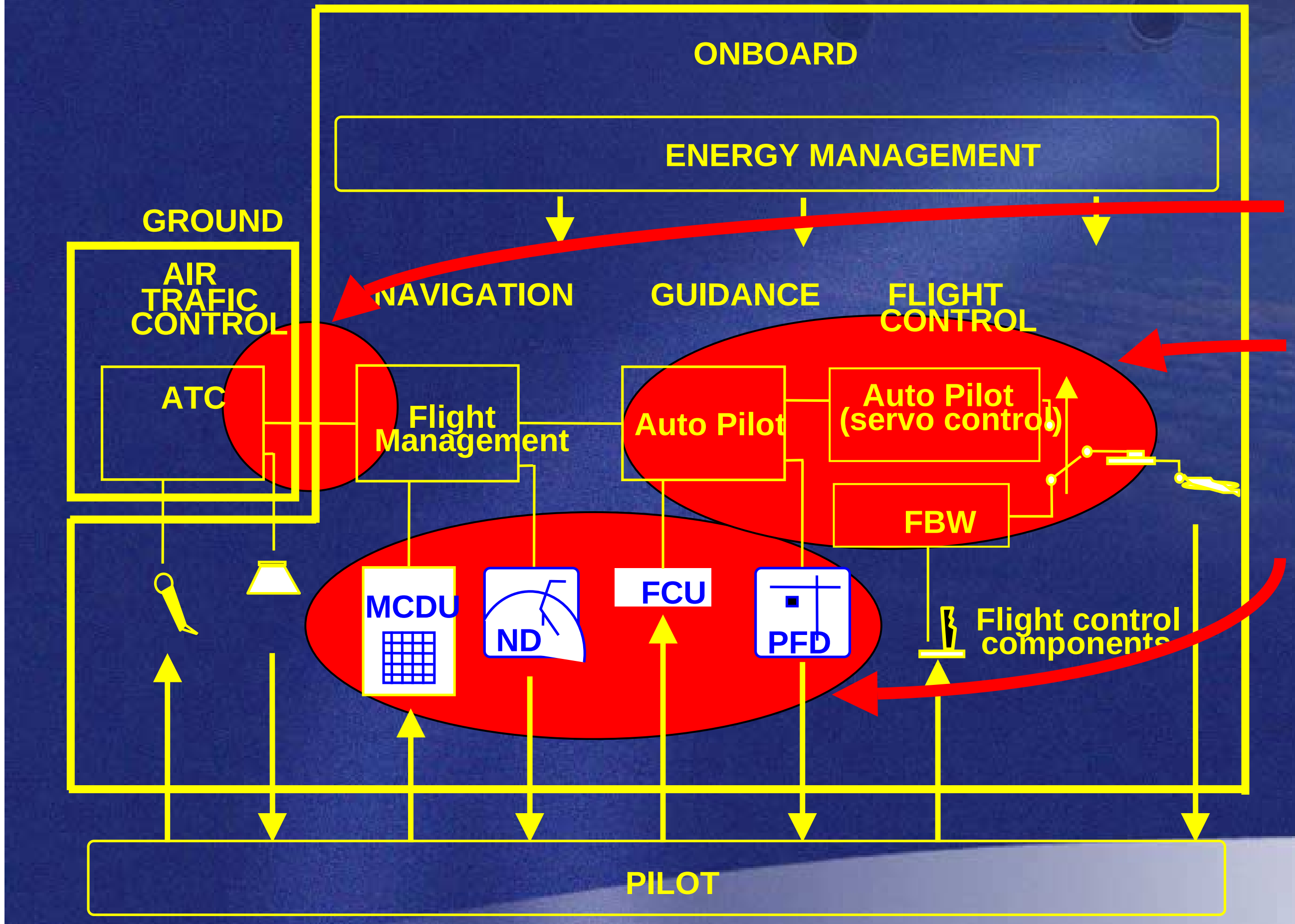
ARE PROOF TECHNIQUES INDUSTRIALY OPERATIONAL ?

François PILARSKI
Systems Framework - Systems Department
316 Route de BAYONNE - P.O. Box M0141/6
31060 TOULOUSE Cedex 03 FRANCE

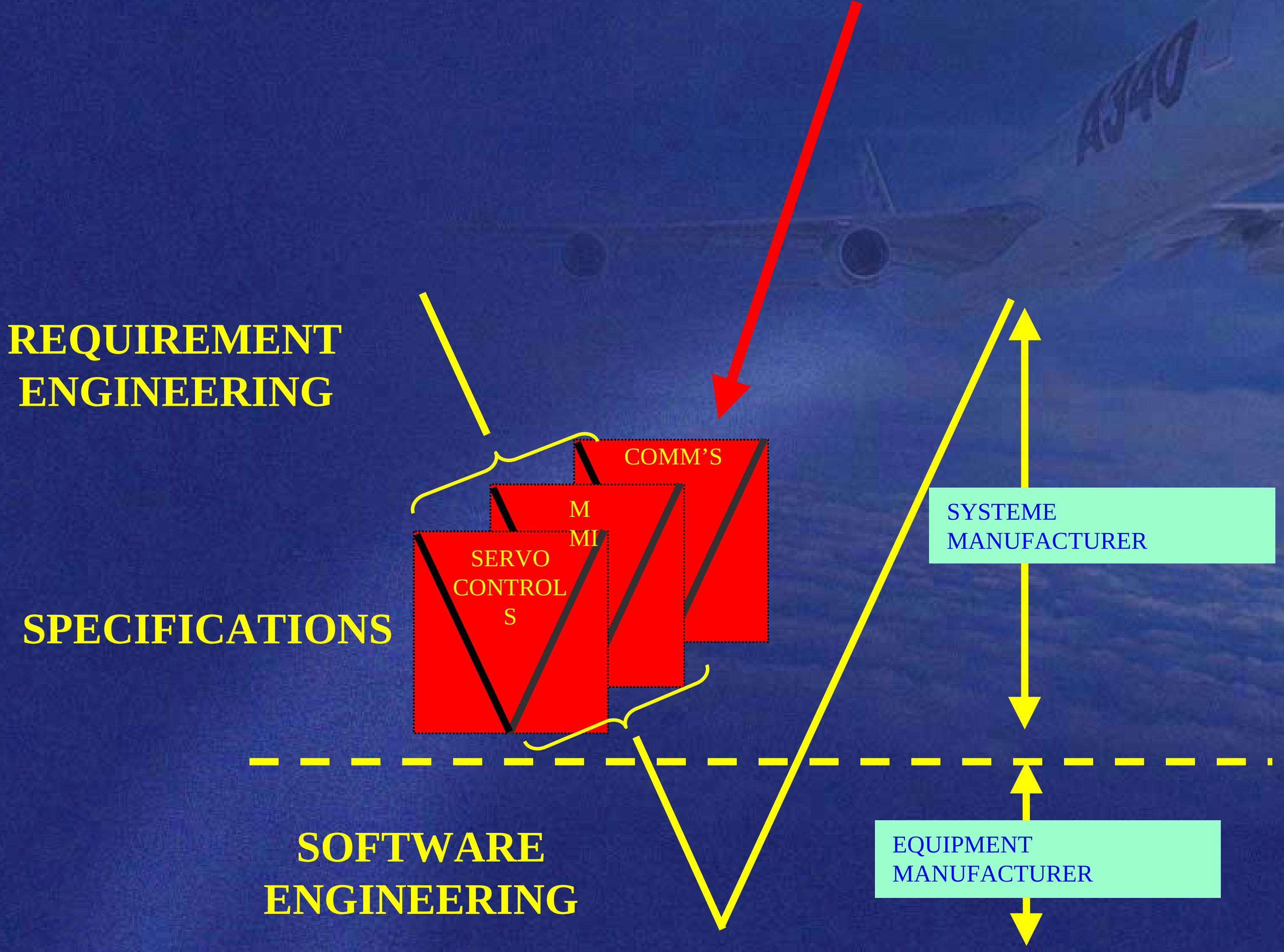
francois.pilarski@airbus.aeromatra.com

TODAY 'S TYPE OF APPLICATIONS
(where proofs techniques could be applicable)



- COMUNICATIONS
- SERVO LOOPS
- MAN MACHINE INTERFACE

TARGETED PART OF THE LIFE CYCLE



REQUIREMENT ENGINEERING

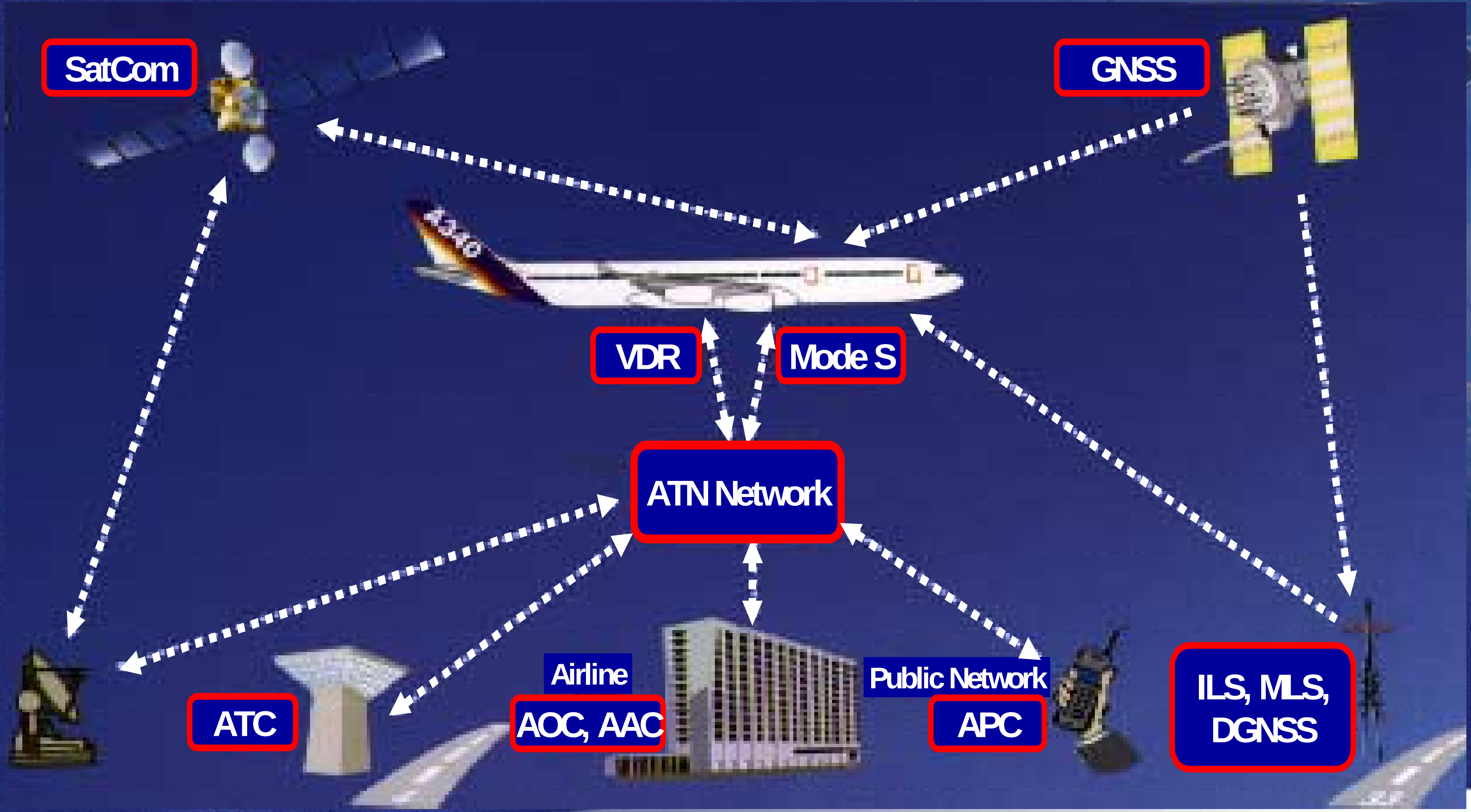
SPECIFICATIONS

SOFTWARE ENGINEERING

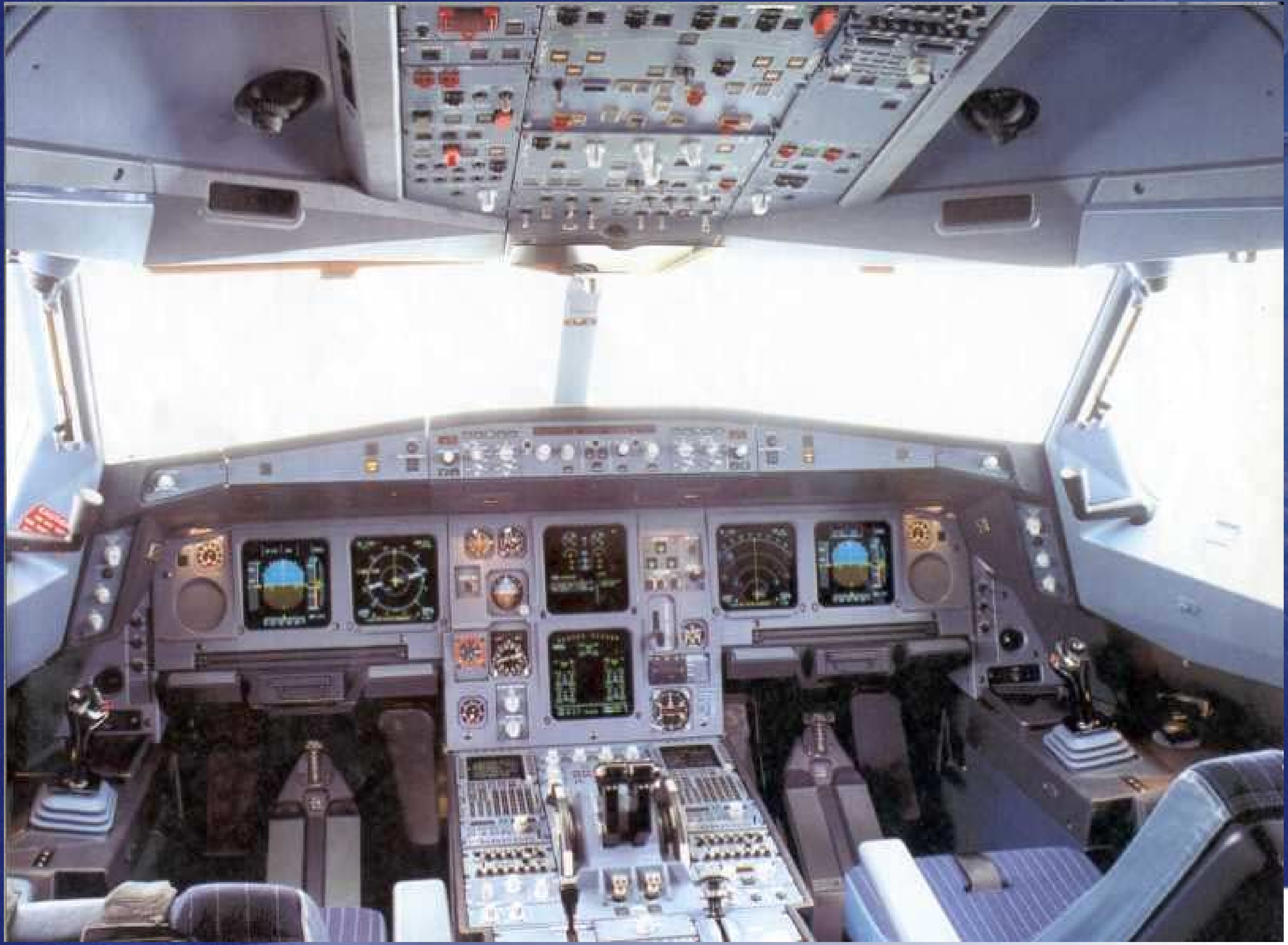
SYSTEME MANUFACTURER

EQUIPMENT MANUFACTURER

COMMUNICATIONS

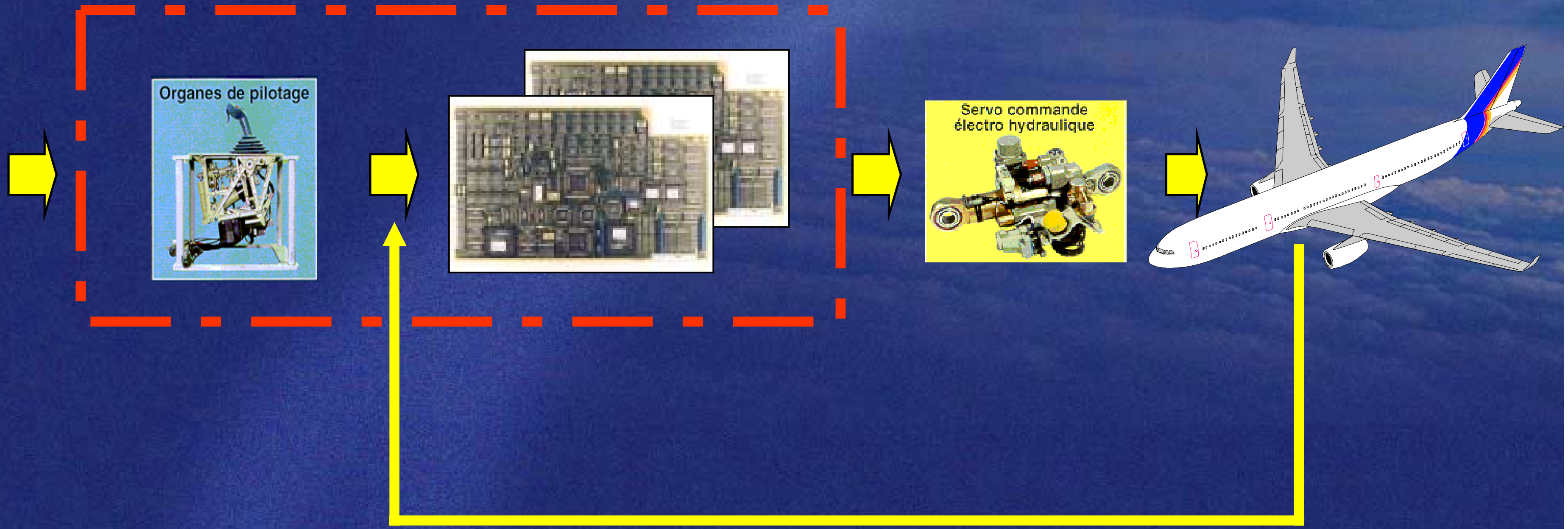


MAN MACHINE INTERFACE

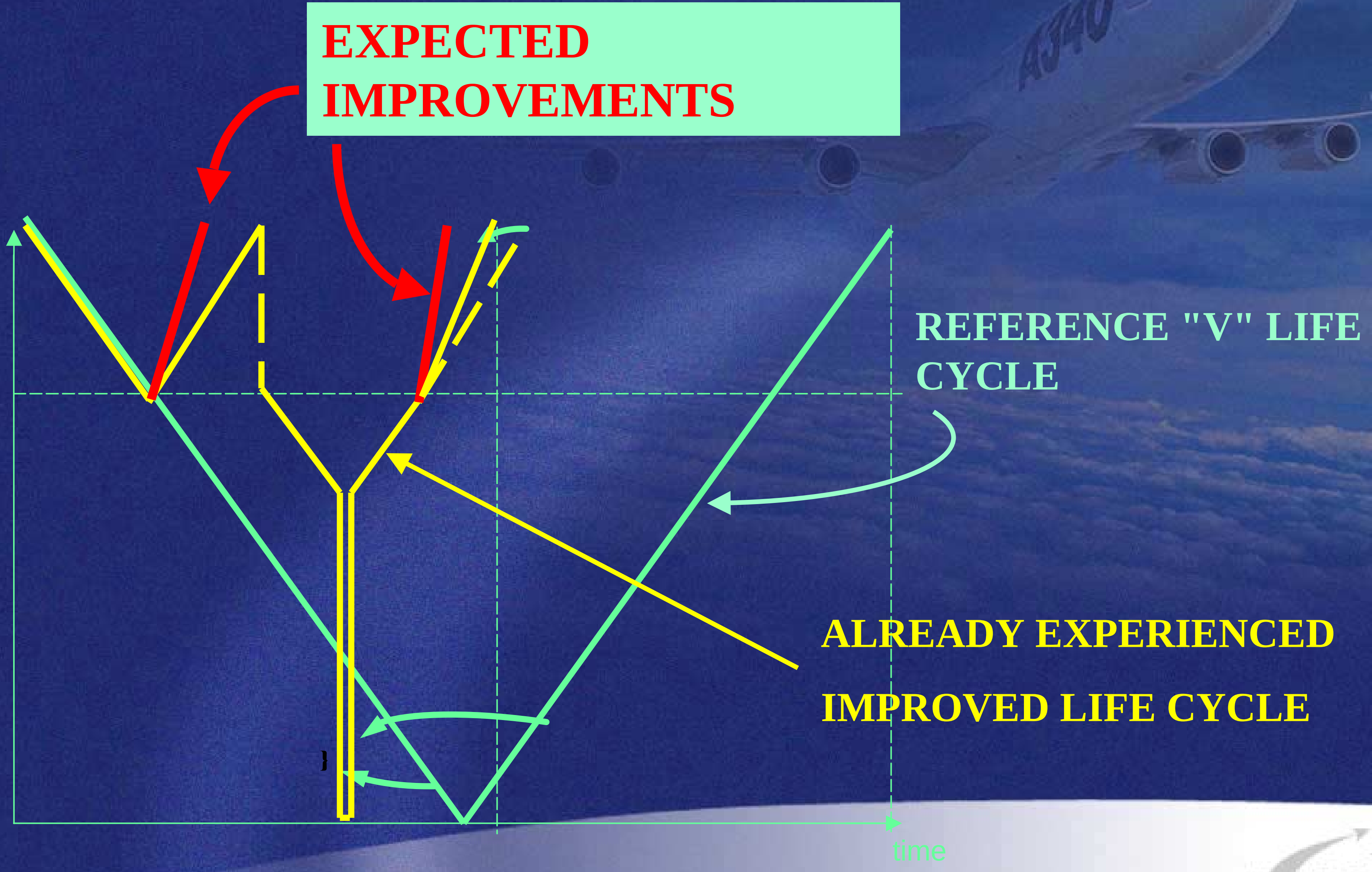


SERVO LOOPS

CONTROL LAWS



EXPECTATIONS



SOME EXPERIENCES

- MEANS (Languages)
  - LOTOS, ESTELLE, …
  - B
  - SDL
  - LUSTRE

- PILOT STUDIES
  - FLIGTH WARNING SYSTEM
  - MMI part of the FMS
  - FLIGHT CONTROL SYSTEM
  - ELECTRICAL POWER MANAGEMENT

RESULTS
LOTOS / ESTELLE / B (Early 90 ’s)

- **DIFFICULTIES**
  - **TOO MATHEMATICAL APPROACH**
  - **NEED THE USERS TO BE TRAINED (Language is not natural)**
  - **…**
- **TOOLS NOT MATURE YET**
  - **NO MEANINGFULL RESULTS**
- **METHODOLOGICAL CONCERNS**

  (B mainly)

==> CANNOT BE ADOPTED

RESULTS (Cont ’d)
SDL (mid 90 ’s)

- **APPLICATION : part of the Ground / Onboard Comm ’s**
- **SIGNIFICANT RESULTS :**

  Proofs were considered as a real help to debug the spec
- **MAIN CONCERN WAS TO ABSTRACT TREATMENTS :**
  - **MODEL CHECKING NEED TO FOCUS ON STATES (and transitions)**
  - **DATA TRANSFORMATIONS ARE NOT TO BE CONSIDERED**

==> NEED TO MANAGE AN ABSTRACT MODEL OF THE SPEC
(for model checking purposes)
AND THE COMPLETE SPEC AT THE SAME TIME

RESULTS (Cont 'd)
LUSTRE

- THREE DIFFERENT APPLICATIONS
  - MMI part of the FMS
  - FLIGHT CONTROL SYSTEM
  - ELECTRICAL POWER CONTROL (ELMU)
- MMI :
  - Example was not self-standing ==> no significant results
- FCS & ELMU :
  - Use of LESAR as well as NP_TOOLS
  - Convincing results
  - Tools to be improved / integrated
  - Main difficulty is to identify properties to be proven

SEEMS TO BE ON A GOOD WAY

RECOMMENDATIONS

(for proofs) TO BE ACCEPTED

- USERS SHOULD BE DESIGNERS

  (the ones who validate systems now)

- (Property) LANGUAGE SHOULD BE AS NATURAL AS POSSIBLE

  ==> to be adopted by users

- PROOF TECHNIQUES SHOULD APPLY ON ACTUAL SPECIFICATIONS ==>
  - no specific design language for proofs
  - no modification and/or adaptation and/or abstraction of the spec
  - seamlessness design process

RECOMMENDATIONS

(for proofs) TO BE EFFICIENT

- **PROOF TECHNIQUES NEED TO BE EXPLAINED**
  - **no "miracle"**
  - **part of the validation set of means**

- **PROOF TECHNIQUES NEED TO BE LEARNED**
  - **heuristics to formulate properties to be provided**
  - **overall process to be defined (where and when and how)**

==> NEED SIGNIFICANT TRAINING

CONCLUSION

- TOOLS ARE NEARLY " INDUSTRIALY OPERATIONAL "
  - EXPECTED IMPROVEMENTS ARE :
    - user friendly interface
    - user oriented language (to express properties)
    - need no spec transformation (abstraction)
  - SIGNIFICANT RESULTS CAN BE OBSERVED
    - effectiveness stil to be assessed wrt "classical techniques"

- TECHIQUES NOT YET UNDERSTOOD

==> STRONG NEED TO TRAIN FUTURE "DESIGNERS-PROVERS"