October 2007

Presented by

Pascal Traverse – EYDS
Claude Cuiller - EYDVA

SYSTEM VALIDATION

Colloque d'Automne du LIX 2007

AIRBUS

System validation – Agenda

0. Consistency of this talk within CAL 07

1. System validation basics (place in aircraft system development process)

2. Companion processes (certification, …)

3. System validation means (test, oracle, …)

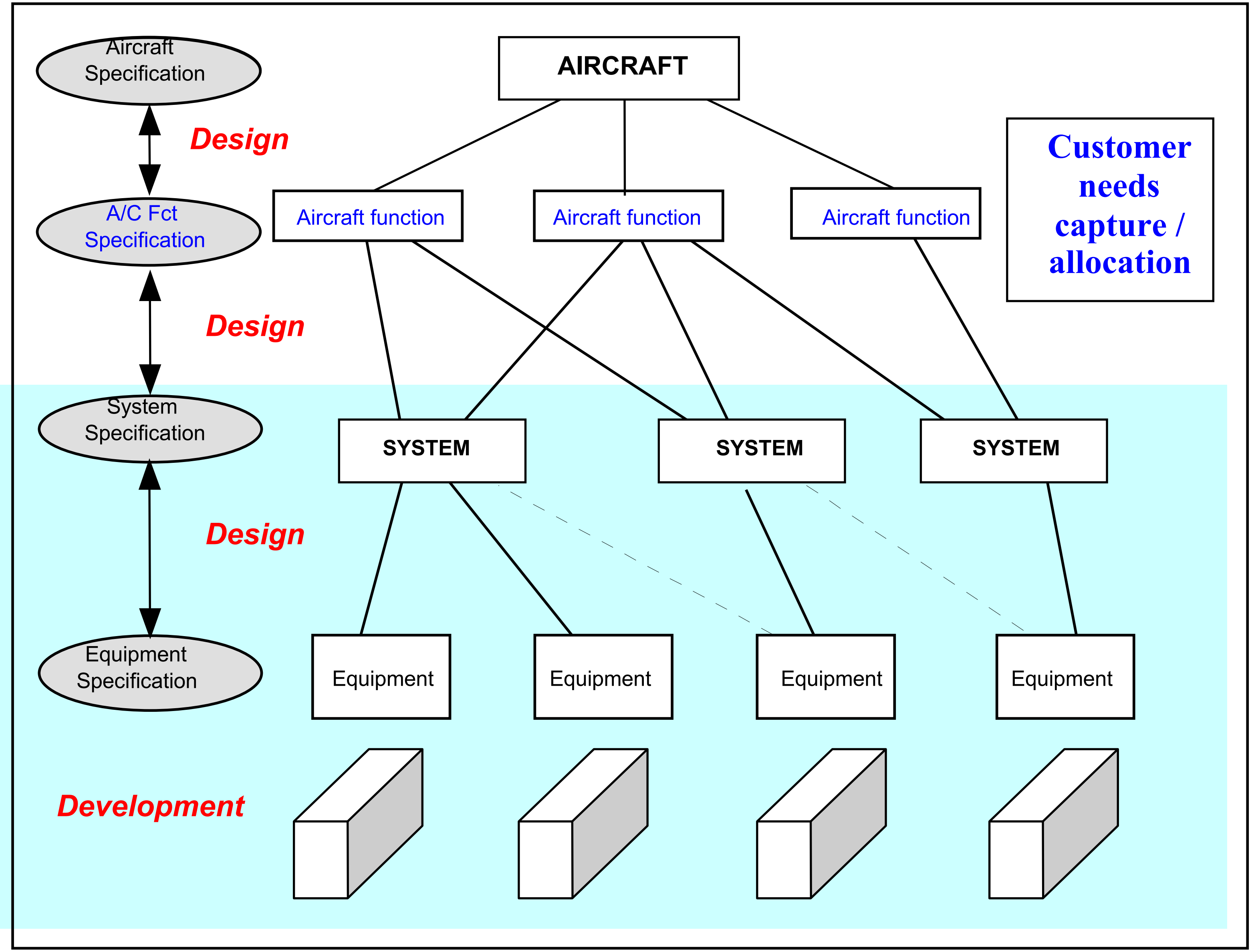
System validation – Consistency within CAL07

1. System validation is NOT **software verification** (see slide 6)

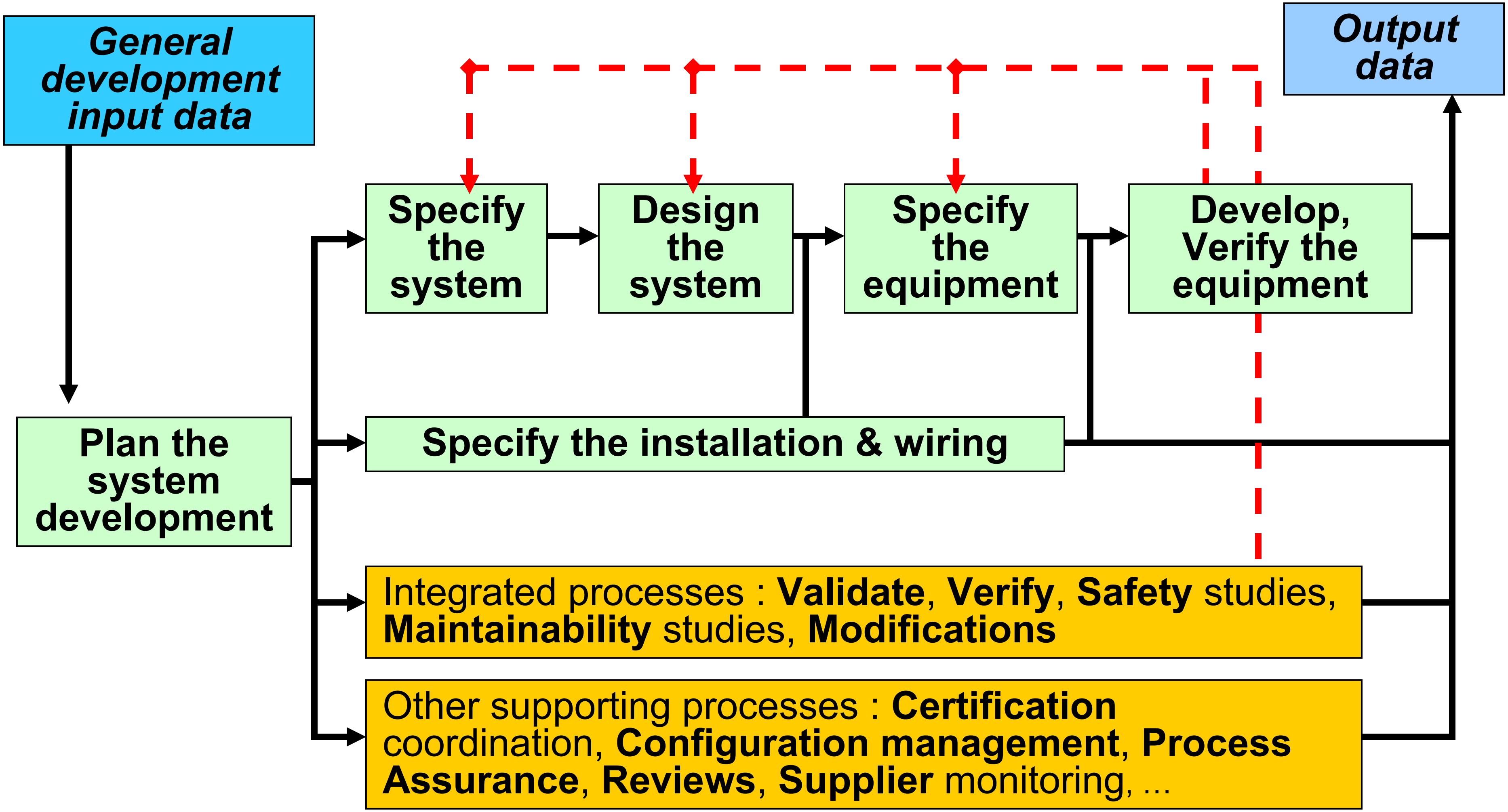
2. System validation relies more and more on **modelling** (see slide 16)

3. System validation is more and more of importance as
   - ➢ **Optimisation** to
     - ✓ Increase safety
     - ✓ Reduce A/C weight and overall cost
   - ➢ Leads to more **complexity**:
     - ✓ New functions (load alleviation, flight envelope protection, …)
     - ✓ Functions integration
     - ✓ Embedded, SW based, systems

System validation - Basics



System validation - Basics

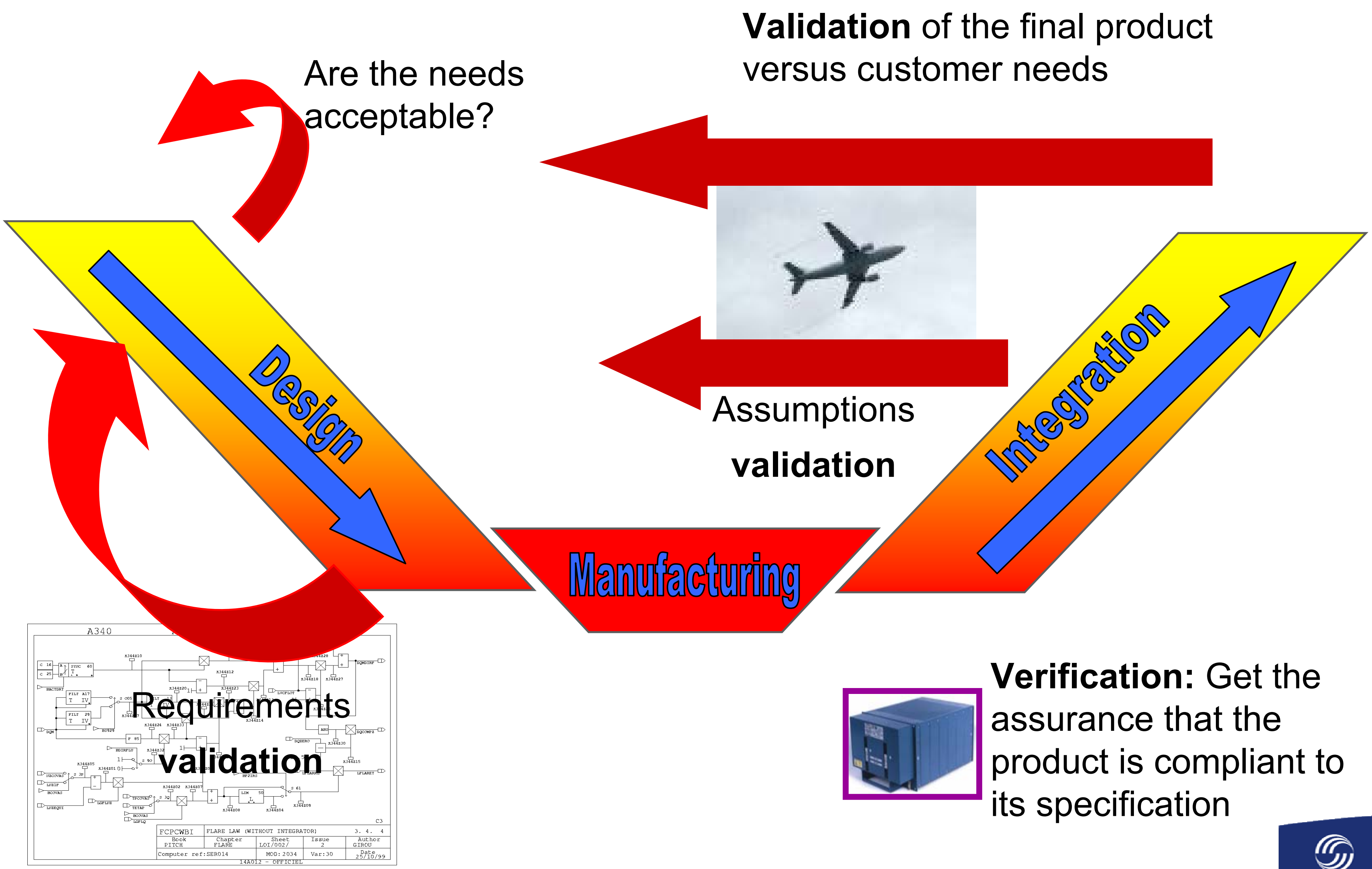


General development input data
Output data
Specify the system
Design the system
Specify the equipment
Develop, Verify the equipment
Plan the system development
Specify the installation & wiring

Integrated processes : **Validate**, **Verify**, **Safety** studies, **Maintainability** studies, **Modifications**

Other supporting processes : **Certification** coordination, **Configuration management**, **Process Assurance**, **Reviews**, **Supplier** monitoring, ...

System validation - Basics



Validation of the final product versus customer needs

Are the needs acceptable?

Assumptions **validation**

Requirements **validation**

Verification: Get the assurance that the product is compliant to its specification

System validation – Companion processes

FAR (US regulations) & **CS** (European regulations) are requirements, part of the A/C specification. Hence V&V shall have to demonstrate A/C compliance to these requirements.

As a consequence, **certification** may be considered as a sub-process of the V&V process...
... With a bit more of formalism (certification sheets, reviews, ...)
... And a particular point of view (safety oriented)

Certification is encompassing process, not only product.
Guidance provided (SAE ARP 4754 – EUROCAE ED79 “certification considerations for highly-integrated or complex systems”)

System validation – Companion processes

<u>Level of V&V effort</u> and demonstration for certification (including Authorities attend to the activities) are depending on

- system/function criticality (DAL A B C D E)
- expected maturity
- risks & novelties
  (ex.: A380 size, new technologies like AFDX communication network on A380)

System validation – Companion processes

V & V ⇒ **<u>Maturity</u>** = as expected by the customer

⇨ *<u>detect implicit needs</u>*:

- early detection by meetings, task forces, …before beginning of development

- before entry into service or before fleet wide extension by:
  - route proving
  - early long flight
  - in flight evaluation

⇨ *<u>sufficient coverage</u>* of the V&V activities to ensure that the final product corresponds to what expects the customer

System validation – Companion processes

<u>Design to validate</u>:

- inclusion of specific tools into system/equipment at the stage of design for validation purposes
  - gauges
  - data observer embedded in real time computer configuration modifications
  - flight control computer modification in order to generate calibrated surface movements for aeroelasticity analysis
- design complexity should be limited: if validation is difficult to perform, then design is not adequate

System validation – Means

Human means, based on

- skills of the teams,
- critical minded judgments,
- inquisitiveness (capability to think/investigate beyond the test program)

From the simplest methods:

- reviews & readings
- specification guides
- analysis (examples: monitoring thresholds justification, braking performance, electrical consumption)

To the more sophisticated ones:

- SSA
- Human Factor demonstration
- … and test

System validation – Means

System Safety Assessment

- at a Failure Condition is associated a safety requirement (FHA)

  “ probability of control loss of one elevator shall be less than 10^{-5}/FH”

- these safety requirements are validated

  “10^{-5}/FH because A/C consequence is not more than Major”

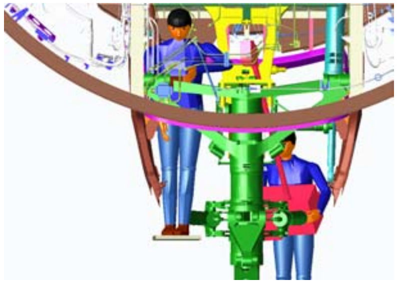
- this validation is documented according to Flight Test, Lab test, report or engineering judgment

- compliance to safety requirements is verified by failure diagrams (Fault Tree analysis) using FMEA/FMES plus common-mode assessment (independence between redundant components vs design, installation, particular risks, ..)

System validation – Means

Human Factor Assessment

- Human factors are taken into account in design
  - early in the development (brainstorming with pilots, human factor tools to develop the design)
  - in cockpit interface definition.
    Validation on A/C –1 and on flight test A/C
  - for maintenance activities
  - in safety analysis (impact of an human error in SSA consideration).
    All procedures are reviewed to be adequate against the safety classification of failure conditions



System validation – Means

The world of tests / input

- testing is not exhaustive

- test cases are defined, based on
  - functional requirements “black box”
  - equivalence classes of test cases

- completeness of these test cases is assessed
  - generally by engineering judgement, supported by check-lists, past experience, cross-ref to requirements
  - sometimes based on the structure of the tested entity “white box”

System validation – Means

The world of tests / output

- “oracle” problem: how to decide that a test result is good?
  - generally by engineering judgement, based on upper-level requirements
    - by comparison with expected test results
    - by examination of test results
  - by comparison to global standards (acceptable level of vibration, of altitude loss, ...)
  - by comparison between the entity-under-test and a “golden” one (comparison between previous version of a software and a new version to detect potential regressions)

System validation – Means

Simulations:

- A/C level: aerodynamic, handling qualities, engines, weight and CG, loads, hinge moments

- System level: flight controls, fuel, hydraulic, electrical power, …

- Environment: atmosphere, wind and turbulence, visual feedback, sound feedback, cabin movement

⇨ Flight tests to identify the A/C and to readjust its models (validation of assumptions)

System validation – Means

System validation – Means

System validation - Trends

- Emphasis on functions

- Earlier validation: shift of activities & model based

- Increase formalism

- Some very preliminary applications of formal proof techniques

Les déclarations faites dans ce document ne constituent pas une offre commerciale. Elles sont basées sur les postulats indiqués et sont exprimées de bonne foi. Si les motifs de ces déclarations n'étaient pas démontrés, AIRBUS FRANCE S.A.S serait prêt à en expliquer les fondements.

AIRBUS

AN EADS COMPANY