Cycle de conférences techniques sur les méthodes formelles de développement, deuxième conférence : ***« La preuve de modèle, preuve de programme »***

Industrial Use of CompCert on a Safety-Critical Software Product

Presented by J.SOUYRIS

(AIRBUS Avionics Software Products)

AIRBUS

SUMMARY

- ***CompCert***
- ***Interest*** for CompCert?
- ***Qualification*** considerations
- ***Conclusion***

SUMMARY

- ***CompCert***
- Interest for CompCert?
- Qualification considerations
- Conclusion

CompCert

CompCert is a ***C compiler*** like Diab C

- Source: a large subset of ISO-C-99/ANSI-C language + several extensions
- Target: machine code for PowerPC, ARM and IA32 architectures

CompCert is a ***formally verified*** compiler

- Machine-assisted mathematical proof (Coq)
  - ➢ *Semantic preservation between source code and compiled code*

CompCert performs ***optimization***

- Simplification of control flow and wise use of data resources
  - ➢ Controlled and non aggressive optimization

CompCert: INRIA Collaboration with Airbus

Airbus / INRIA collaboration (ongoing)

- First meeting on Dec 2008
- At least two meetings per year
- ***Objective: use CompCert in EYY fly-by-wire software development***
- Ricardo Bedin França's "Thèse CIFRE": 2009-2012
- Alexandre Hollocou's "Inside CompCert" (scientific study): 2013
- Airbus's ***feasibility study*** dealing with ***industrial and certification*** aspects: from mid 2012 to Official ***GO by end 2013.***
- ***Extensions of CompCert*** by INRIA since 2009

SUMMARY

- CompCert
- ***Interest for CompCert***?
- Qualification considerations
- Conclusion

Interest for CompCert

Short term ***need of performance*****:** reduction of the WCET

Target: 11% WCET saving

CompCert C compiler

- Suitable for the targeted software product development (PowerPC CPU)

CompCert performs ***optimization***

- Simplification of control flow and wise use of data resources
  - Controlled and non aggressive optimization
- Performance gain objective (WCET) achieved: 12% (so far)
  - ***Addresses the short term application needs***

CompCert is a ***formally verified*** compiler

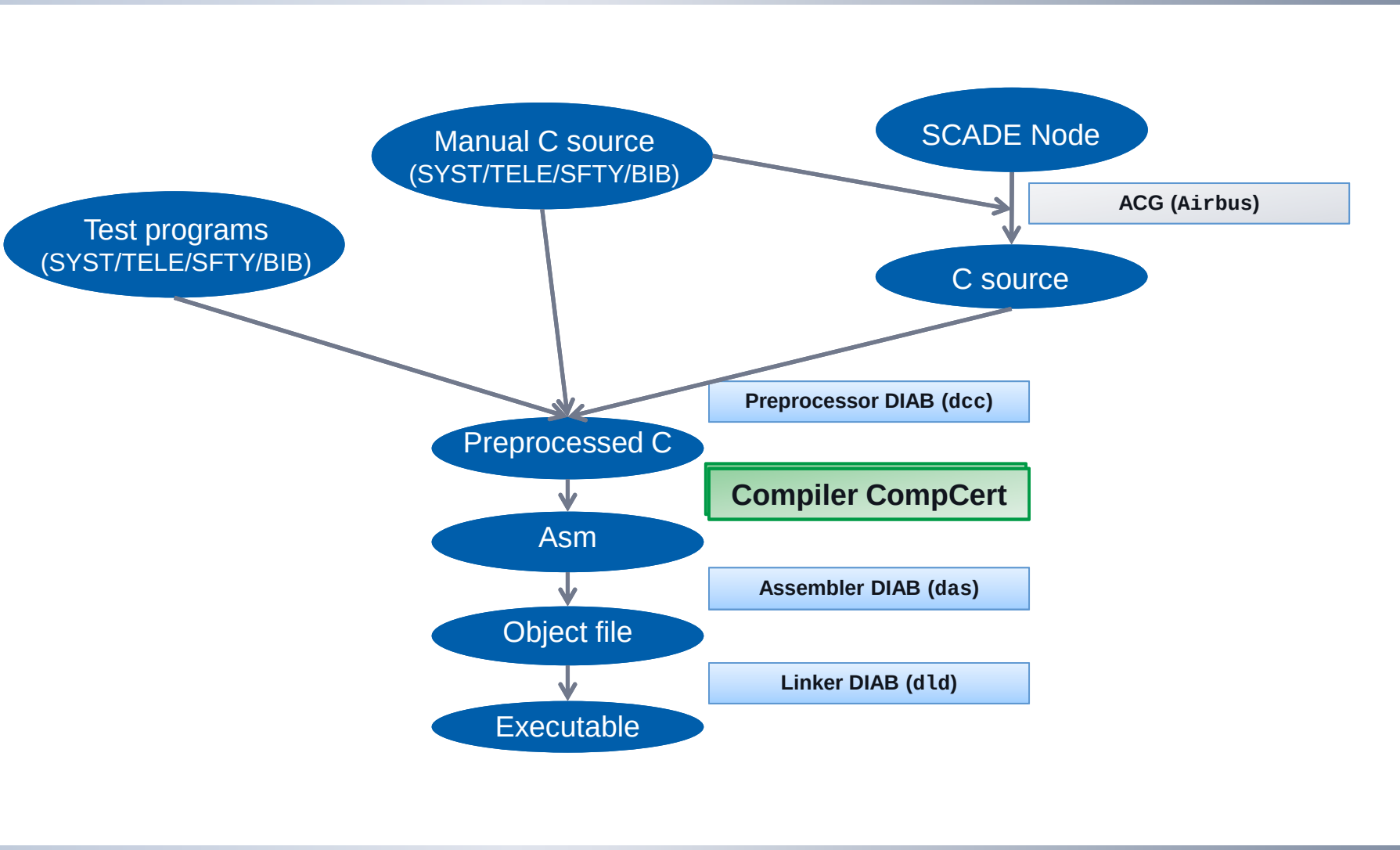
- Machine-assisted mathematical proof (Coq)
  - ***Achieving source code to object code semantics preservation proof.***

AIRBUS

SUMMARY

- CompCert
- Interest for CompCert?
- ***Qualification considerations***
- Conclusion

CompCert in the Compilation chain



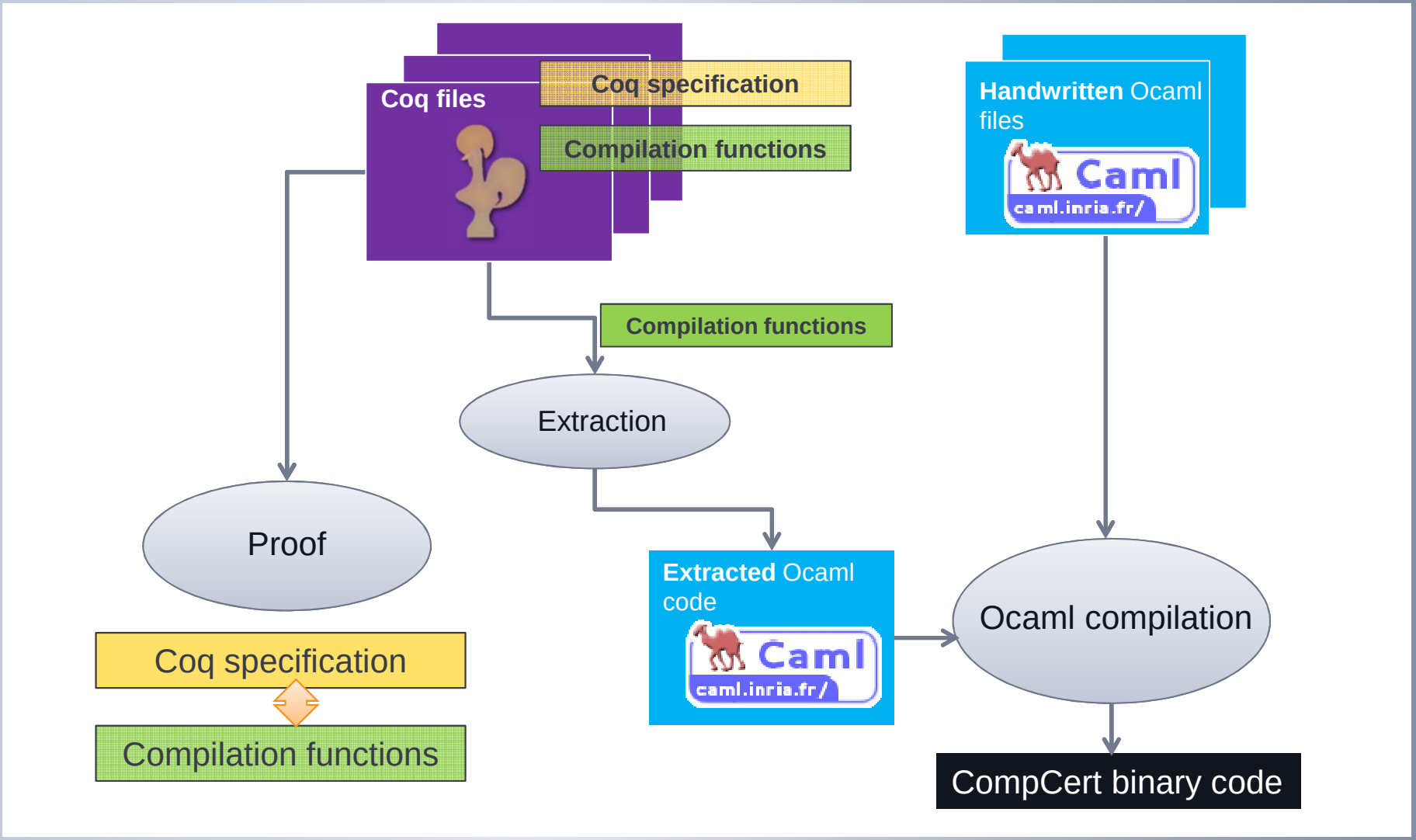
Answer to DO-178[BC]

Answering to DO-178[BC] sections 4.4.2 “Language and compiler considerations” and 6.4.4.2 “Structural coverage analysis”:

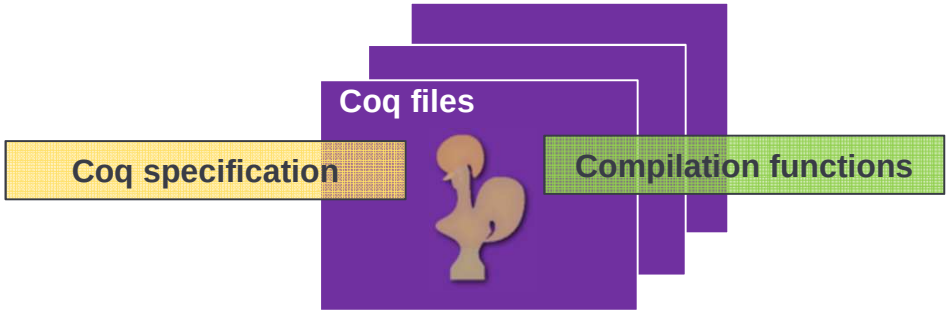
- Requires us to continue ***testing compiled code*** (DO-178[BC] section 6 Software Verification Process), and

- Requires confidence in the ***soundness of the optimisations***
  - This confidence is based on the proof of ***semantic preservation*****.**

CompCert development



CompCert development



- Coq specification
  - Specification of the C source language and of the ASM PPC target language
  - Specification of the compilation process (semantics preservation)

- Compilation functions (as Diab C compiler)

```
Theorem transf_c_program_preservation:
  forall p tp beh,
  transf_c_program p = OK tp ->
  program_behaves (Asm.semantics tp) beh ->
  exists beh', program_behaves (Csem.semantics p) beh' /\ behavior_improves beh'
beh.
Proof.
```

Qualification considerations

Establishing the ***confidence in CompCert*** will be mainly based on:

- Informal ***user's requirements*** and their validation
- The demonstration of ***compliance*** of both formal and informal ***tool requirements*** to the ***user's requirements*** (most of them being formal)
- ***CompCert's formal proof*** as the main demonstration of the soundness of the optimizations
- The ***verification and validation*** of CompCert's informally developed parts.

AIRBUS

Conclusion

- CompCert is an example of ***formally developed software product***
- This gives it a ***high correctness level***
- ***Confidence*** in CompCert's correctness must be established in the frame of a ***DO-178[BC] compliant*** development process.

QUESTIONS?