



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

COTRE as an AADL profile

Pierre GAUFILLET & Patrick FARAIL

AIRBUS FRANCE

pierre.gaufillet@airbus.com / patrick.farail@airbus.com

Tel. : +33 (0)5.61.18.84.85 / +33 (0)5.61.93.66.28



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

COTRE overview 1/2

- Funded by the French research department (total 1.9M€, 230 m.m), from 2002 to 2004
- Goal : Real Time architecture verification (mainly from the behavioral point of view)
- Exploration project aiming to develop a demonstration tool
- Partners : AIRBUS, TNI-Valiosys, IRIT, LAAS, ONERA-DTIM, ENSTB



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

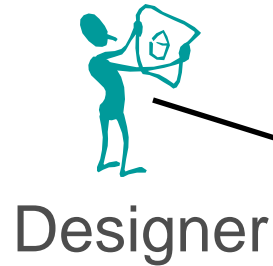
O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

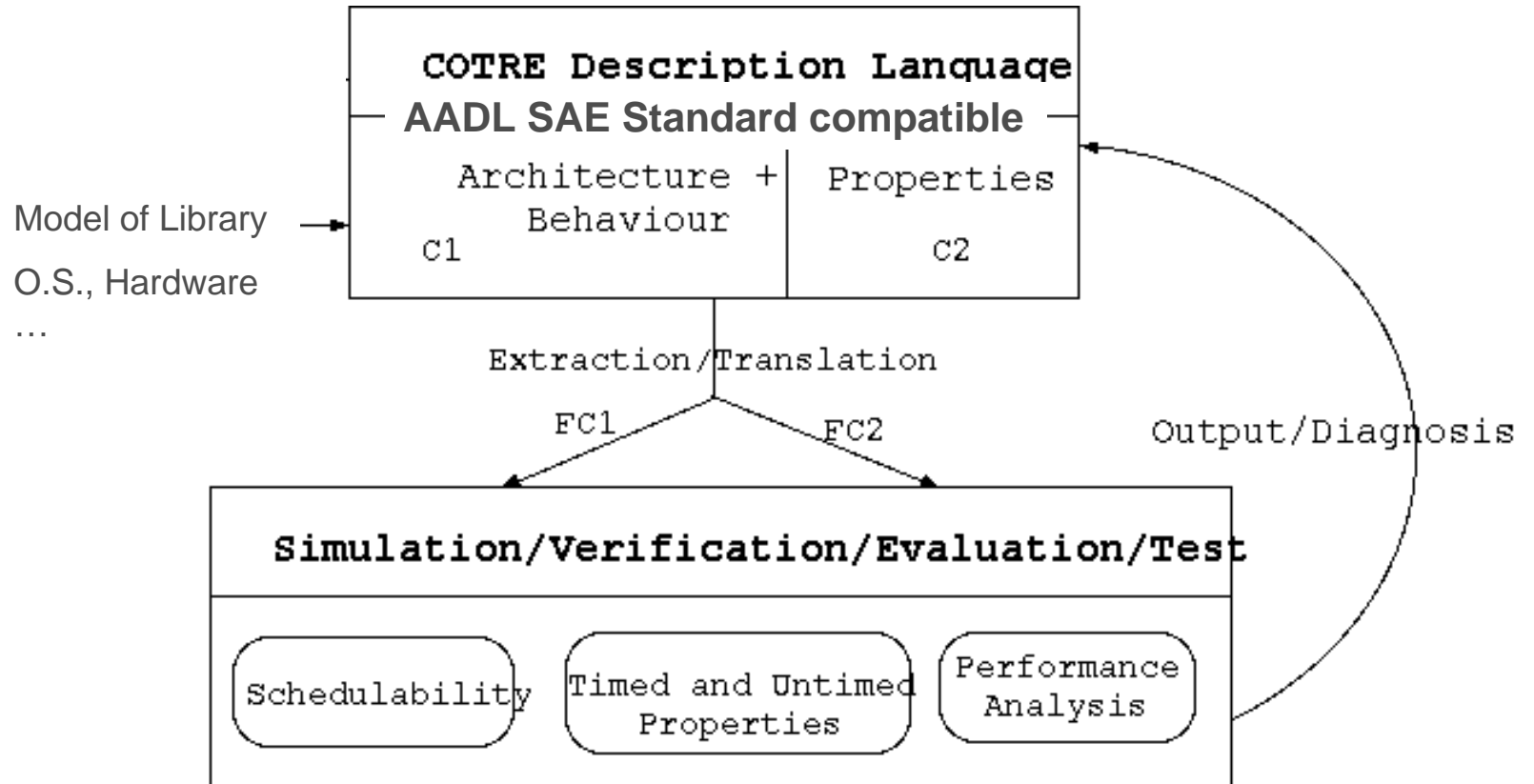
August 27, 2004

copyright ©COTRE
all rights reserved

COTRE overview 2/2



HOOD mapping
UML Mapping





AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

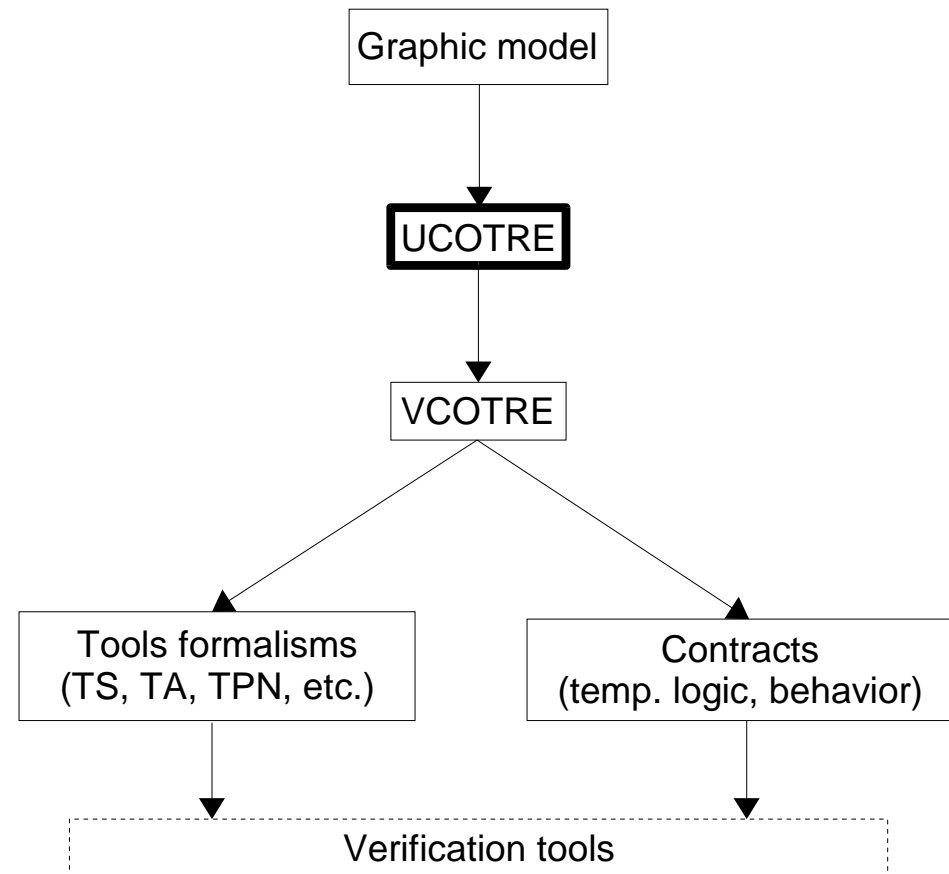
IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

UCOTRE

- User level COTRE language, opposed to VCOTRE, Verification COTRE language. The 2 languages seems mature enough today to be merged.
- Based initially on the HOOD IV and HRT-HOOD concepts, and then on AADL.
- The main restriction to AADL is the lack of ports : every communications are modeled by subprogram calls. Ports should be added for multi-process applications.





AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

AADL extension mechanisms

■ Property sets :

```
PROPERTY SET my_ext IS  
  int    : TYPE INTEGER -32767..32768;  
  duration : TYPE UNITS (s, j => s * 86400,  
                          ms => s * 0.001,  
                          us => s * 0.000001);  
  rate : float => 0.0 APPLIES TO (SUBPROGRAM);  
END my_ext;
```

■ Annexes :

```
ANNEX <name> IS  
  <free syntax>  
END ANNEX <name>;
```



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

Deadlock system

```
SYSTEM deadlock_verification  
END deadlock_verification;
```

```
SYSTEM IMPLEMENTATION deadlock_verification.default
```

```
SUBCOMPONENTS
```

```
dp : PROCESS Partition.A;
```

```
ANNEX cotre.guarantees IS  
IS ALIVE;  
END ANNEX cotre.guarantees;  
END deadlock_verification.default;
```

```
PROCESS Partition  
END Partition;
```

```
PROCESS IMPLEMENTATION Partition.A
```

```
SUBCOMPONENTS
```

```
t_1 : THREAD t.t1(sem1 => sem_1, sem2 => sem_2);  
t_2 : THREAD t.t2(sem1 => sem_2, sem2 => sem_1);  
sem_1 : DATA semaphore.default;  
sem_2 : DATA semaphore.default;
```

```
END Partition.A;
```

```
sys_deadlock_instance: SYSTEM ex_deadlock.default { };
```

COTRE contract annex



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

Contracts

ANNEX cotre.guarantees | cotre.assumes **IS**

((<assertion> | <behavioral equivalence> | <raw formula>);)+

END ANNEX cotre.guarantees | cotre.assumes;

Assertion	Formal description	Comments
potentially reset	AG EF <i>init</i>	From any state, the component may go back to its initial state.
unavoidably reset	AG AF <i>init</i>	From any state, the component must go back to its initial state.
is alive	AG EF EX _c true	Some actions have always to be possible in the future. Applied to a root component, this assertion implies that there is no deadlock.
no livelock	AG AF EX _c true	The component must not stay forever idle.
invariant <exp>	AG <exp>	<exp>has always to be true.
<exp1> leads to <exp2> [within <exp3>]	AG(e1=>AF _{<=d>} e2)	The occurrence of <exp1> always implies the occurrence of <exp2> in less time than <exp3>.
reachable <exp1> [from <exp2>] [within <exp3>]	AG(e1=>EF _{<=d>} e2)	The occurrence of <exp1> may imply the occurrence of <exp2> in less time than <exp3>.
<exp1> after <exp2>	AG(¬EU(¬e2, e1))	<exp2> always occurs after <exp1>.



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

Modeling threads

```
THREAD t  
REQUIRES  
  sem1 : DATA ACCESS semaphore;  
  sem2 : DATA ACCESS semaphore;  
END t;
```

```
THREAD IMPLEMENTATION t.t1  
PROPERTIES  
  Period => 13.96ms;  
  cotre::Priority => 1;  
  cotre::Phase => 0.0ms;  
  Dispatch_Protocol => Periodic;
```

COTRE thread
properties

```
ANNEX cotre.behavior IS  
STATES  
  s0, s1, s2, s3, s4, s5, s6, s7, s8 : STATE;  
  s0 : INITIAL STATE;  
TRANSITIONS  
  s0 -[ ]-> s1 { PERIODIC_WAIT };  
  s1 -[ ]-> s2 { COMPUTATION(1.9ms, 1.9ms) };  
  s2 -[ sem1.wait ! (-1.0ms) ]-> s3;  
  s3 -[ ]-> s4 { COMPUTATION(0.1ms, 0.1ms) };  
  s4 -[ sem2.wait ! (-1.0ms) ]-> s5;  
  s5 -[ ]-> s6 { COMPUTATION(2.5ms, 2.5ms) };  
  s6 -[ sem2.release ! ]-> s7;  
  s7 -[ ]-> s8 { COMPUTATION(1.5ms, 1.5ms) };  
  s8 -[ sem1.release ! ]-> s0;  
END ANNEX cotre.behavior;  
END t.t1;
```

COTRE behavioral annex



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

Behavior 1/3

- Applies to threads and subprograms
- Mealy machines & Timed Transitions Systems

VARs

```
<variable> : <type>;
```

INITs

```
<variable> := <value>;
```

STATES

```
<state name>(, <state name>)* : STATE;
```

```
<state name> : INITIAL STATE;
```

TRANSITIONS

```
...
```

EXCEPTIONS

```
...
```



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

Behavior 2/3

■ Transitions

(<label>:)* <origin state> -[<clearing condition>]-> <arrival state>
{<actions>};

■ Exceptions

<sensibility cond.> -[<clearing cond.> **BEFORE**
<end of sensibility cond.>]-> <final state> { <actions> };

■ Conditions

WHEN <boolean condition> => <synchronization event>

Synchronization events	Comments
<subprogram name> ! [(<parameters>)]	Calls the named subprogram with the required parameters. The subprogram is identified by using the dotted notation <object>.<subprogram>. Parameters are separated by commas.
CALLED ?	The subprogram being described is called.
RESUME [(<parameters>)]	Give back the control to the caller (but the subprogram being described can go on running).



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

Behavior 3/3

■ Actions

Actions	Comments
COMPUTATION (<max_duration or range>)	Consumes a CPU time smaller then <max_duration> or bounded by <range>.
DELAY (<max_duration or range >)	The execution is deferred for a time smaller than <max_duration> or bounded by <range>.
PERIODIC_WAIT	Delays the execution of a periodic thread until the beginning of its next period. For an aperiodic thread, it is equivalent to SKIP .
SKIP	Does nothing.
<l_exp> := <exp>	Modifies the value of the variable <l_exp>.



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

Modeling semaphore

DATA semaphore

PROVIDES

wait: **SUBPROGRAM**;

release: **SUBPROGRAM**;

PROPERTIES

cotre::Protected => TRUE;

END semaphore;

DATA IMPLEMENTATION semaphore.default

PROPERTIES

sem_p::Max_tokens => 1;

ANNEX cotre.guarantees **IS**

INVARIANT tokens < Max_tokens;

INVARIANT tokens >= 0;

END ANNEX cotre.guarantees;

ANNEX cotre.behavior **IS**

VAR

tokens : **INTEGER** 0..+infinity;

INITS

tokens := sem_p::Max_tokens;

SUBPROGRAM wait

STATES

s0, s1 : **STATE**;

s0 : **INITIAL STATE**;

TRANSITIONS

s0 -[**WHEN** tokens > 0 => **CALLED ?**]->

s1 { tokens := tokens - 1 };

s1 -[**RESUME**]-> s0;

...

END ANNEX cotre.behavior;

END semaphore.default;



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

Types

- Basic types : AADL data, Boolean, integer, real, ranges, with or without units.
- Data definition is required for behavioral verification.

DATA IMPLEMENTATION <name>

ANNEX cotre.type **IS**

<field 1> : **<type 1>**;

...

<field n> : **<type n>**;

END ANNEX cotre.type;

END <name>;

- Or :

DATA IMPLEMENTATION <name>

ANNEX cotre.type **IS**

<type>;

END ANNEX cotre.type;

END <name>;



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

COTRE Property Set

Name	Type	Applies to	Default value	Comments
cotre::Ceiling_priority	integer	DATA	-	For data protected using PCP.
cotre::Description	string	any component and subcomponent	-	Informal comments, traceability informations, ...
cotre::Min_Time	time	THREAD	-	Minimum time between 2 sporadic thread activations.
cotre::Phase	time	THREAD	0.0s	Offset from the beginning of the period for periodic threads.
cotre::Priority	integer	THREAD	-	Base priority of the thread (semantic is scheduling policy dependent).
cotre::Protected	boolean	SUBPROGRAM	false	true if the subprograms of the component are executed exclusively.
cotre::Reentrant	boolean	SUBPROGRAM	false	true if the subprogram is reentrant.



AIRBUS France

TNI-Valiosys

E.N.S.T. Bretagne

I.R.I.T.

L.A.A.S.

O.N.E.R.A. - D.T.I.M.

IFIP WCC
Toulouse

August 27, 2004

copyright ©COTRE
all rights reserved

Conclusion

- Main differences with AADL are :
 - The lack of ports
 - Behaviors
 - Types
 - Contracts
- The AADL core used have to be upgraded.
- Support for multi-application models has to be added (using ports).
- UCOTRE/VCOTRE merge still to be done.
- Some tuning to do at the property set level and for variables (using data instead).
- A partial implementation of the method exists. An industrial-strength open source tool supporting COTRE is planned in the forthcoming TOPCASED project.