BHDL

Boulanger Jean-Louis

jean-louis.boulanger@utc.fr

UTC/HEUDIASYC

19 Juin 2003

SEE – SIC

Présentation

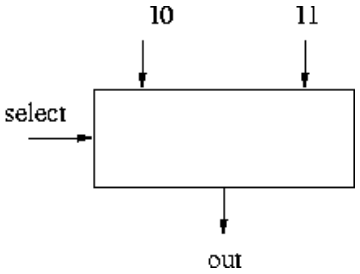
- Pourquoi B-HDL ?
  - Formation
  - Conception
  - Conception sûre
- Conclusions

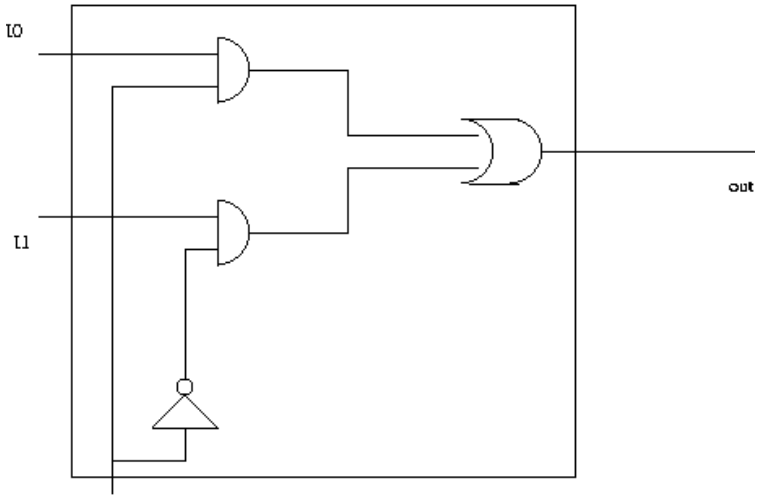
Pourquoi B-HDL ?

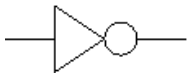
Formation

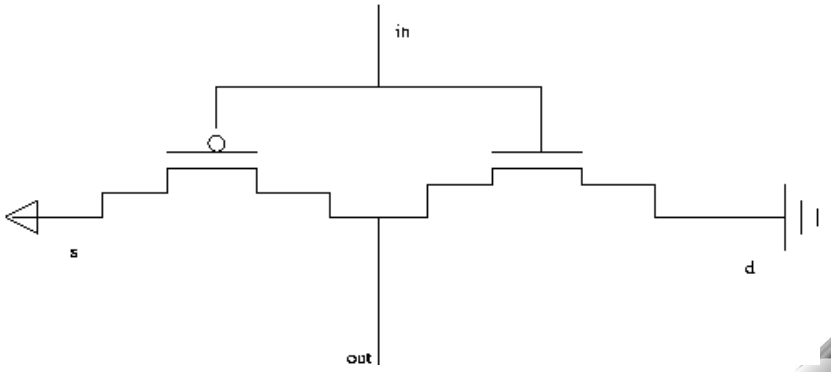
- Objectif :
  - Les circuits numériques sont une source d'exemples simples pour appréhender certains mécanismes (abstraction, modularité et composition) du langage B.
- Délai :
  - Court terme
- Résultats:
  - Une collection d'exemples et un rapport qui peut servir de support de cours.
- Qui :
  - UTC/INRETS

Exemples









B-HDL

- Objectif:
  - Couplage entre les langages de description de circuit numérique (VHDL) et le langage B
  - Profiter de l'expérience du monde VHDL
  - Combiner l'effort de preuve à l'effort de test
- Intérêt :
  - Développer le champ d'application de la méthode B
- Délai :
  - Moyen terme

Moyen humain

- Qui :
  - UTC/LIFL/INRETS
- Aljer Ammar en thèse au LIFL sur le sujet de la complémentarité de VHDL et de B .

Analogy between VHDL and the B method

Circuits synthesis	B Method
Functional Specifications	Abstract machine
Architecture Specification and Behaviour Details	Refinements
Validation “functional to material”	Proof
Hardware Description level	Implementation
Port	Global Variable
Connection	Invariant of relation between variables
Signal Propagation	Operation call (transmission of values)
Modularity and Reusing	Importation and Instanciation and Renaming

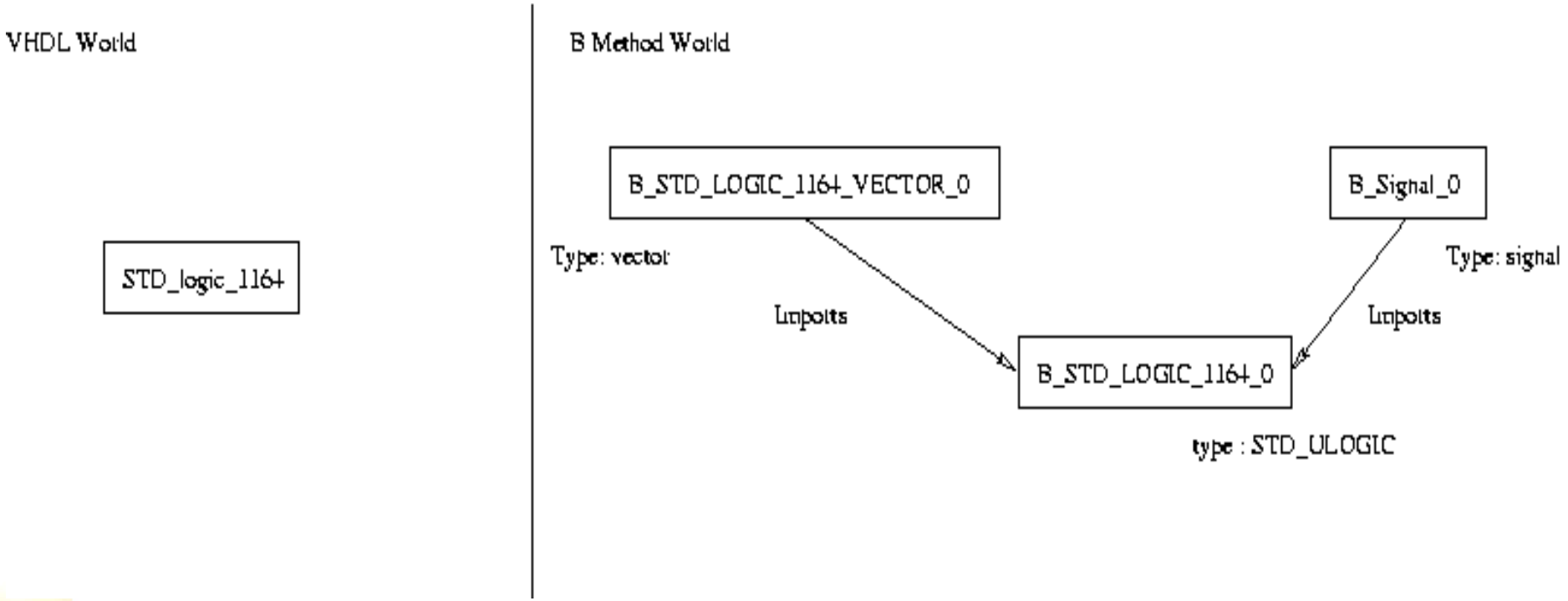
Qui vers qui ?

- Context:
  - Le langage VHDL est bien implanté dans l'industrie,
  - Le langage VHDL est supporté par des outils:
    - Permettant la description graphique de circuit,
    - Permettant la synthèse de circuit,
    - Permettant la simulation,
    - Permettant la gestion des campagnes de test,
    - Permettant la génération de code (C, ...).
  - Il existe des études qui couplent VHDL à des outils de model-checking (vérification de propriété temporelle, ..)

Codesign : deVHDL vers B

- But:
  - Proposer un moyen « complémentaire de vérification »,
  - Ne pas perdre l'expérience des gens
- Tâches:
  - Plonger les bibliothèques de base dans le monde B
    - STD_Logic_1164
  - Définir un sous-ensemble de VHDL qui peut être traduit en B
    - Traduction de plusieurs exemples (Add-4bit, ..)
  - Réalisation d'un traducteur VHDL/B

STD_LOGIC_1164 (1)



La bibliothèque STD_LOGIC_1164

- est une bibliothèque normalisée par l'IEEE,
- est destinée à faciliter la portabilité

STD_LOGIC_1164 (2)

- B_Std_Logic_1164_0
- Définit le type ULOGIC à 9 valeurs et ses sous-types
- Définit une extension des opérateurs booléens
- B_Std_Logic_1164_Vector_0
- Définit la notion de vecteur (taille non bornée) sur les différents types.
- B_Std_Signal_0
- Définit la notion de « signal » (liste chainée d'état);
- Définit les opérateurs « front montant » et « front descendant »

STD_LOGIC_1164 (2)

- Problème rencontrée:
  - VHDL propose la surcharge pas B;
  - Problème de structure (appel locale);
  - Preuve par cas ...
- Validation:
  - Traçabilité du VHDL vers B
  - Définition d'une machine décrivant les propriétés essentielles (identite, nullite, absortion, ..., loi de morgan ...) qui permet de valider la bonne définition du type et des opérations

Half_adder (1)

```
entity Half_adder is
  port (X, Y: in Bit;
        Sum, Carry: out Bit);
  end Half_adder;

architecture HA_Behavior of Half_adder is
  begin
    process
     begin
      Sum <= X XOR Y after 5 Ns;
      Carry <= X AND Y after 5 Ns;
      wait on X, Y ;
  end process;
end HA_Behavior;
```

```
MACHINE
        Half_adder
DEFINITIONS
        Compute_(xx,yy,sum,carru)== ...
SEES
        STD_LOGIC_1164
VARIABLES
        xx,yy,sum,carry
INVARIANTS
        xx,yy,sum, carry : BIT*BIT*BIT*BIT
        & Compute_(xx,yy,sum,carry)
INITILISATION
        ...
OPERATION
        xx_in =
        ....
```

Half_adder (2)

```
entity Half_adder is
  port (X, Y: in Bit;
        Sum, Carry: out Bit);
  end Half_adder;

architecture HA_Behavior of Half_adder is
  begin
    process
     begin
      Sum <= X XOR Y after 5 Ns;
      Carry <= X AND Y after 5 Ns;
      wait on X, Y ;
  end process;
end HA_Behavior;
```

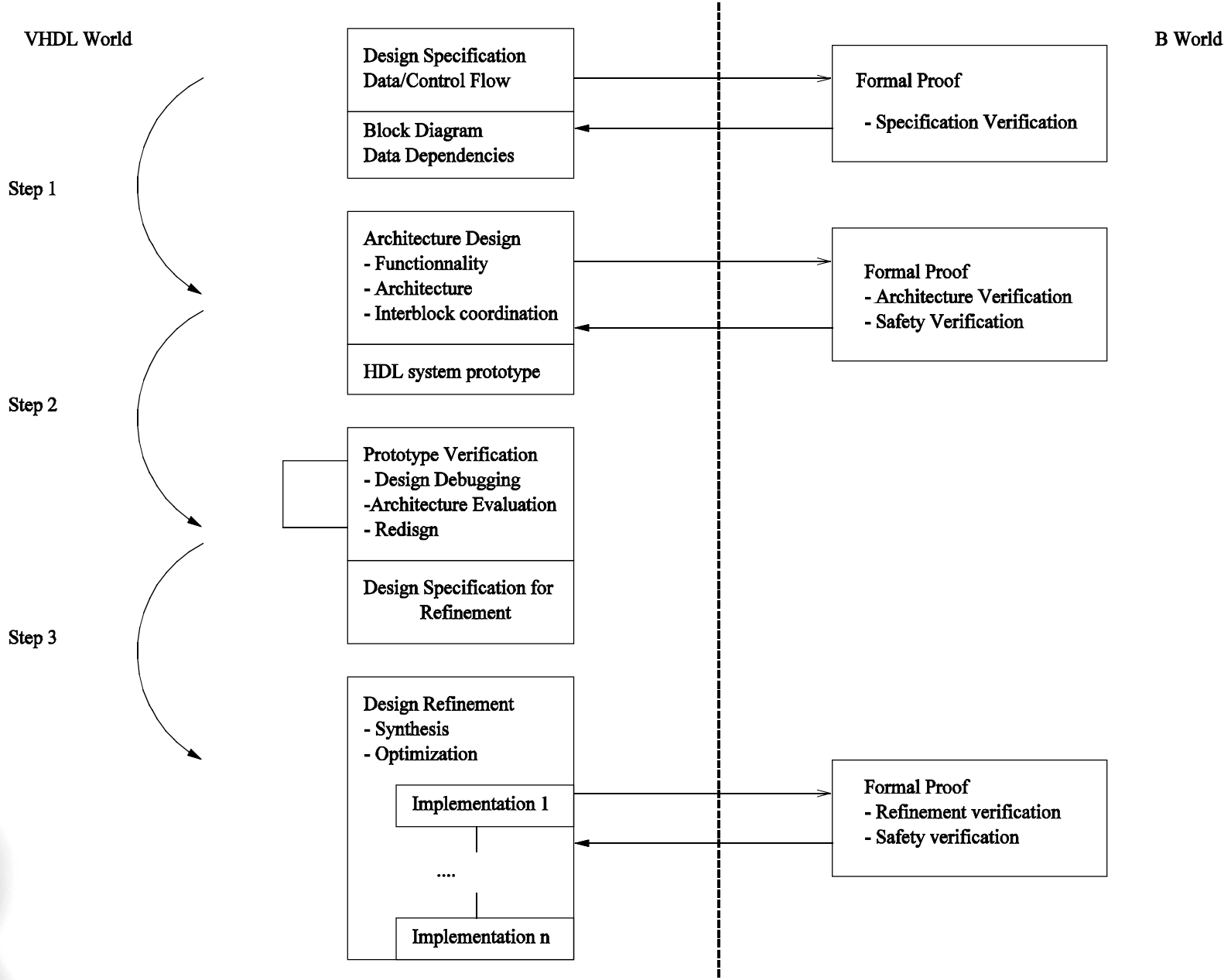
```
IMPLEMENTATION
        Half_adder_i
REFINES
        Half_adder
SEES
        STD_LOGIC_1164
IMPORTS
        AND, XOR
INVARIANTS
        AND.in1=xx & AND.in2=yy &
        AND.out = sum &
        XOR.in1=xx & XOR.in2=yy &
        XOR.out = carry
```

Half_adder (3)

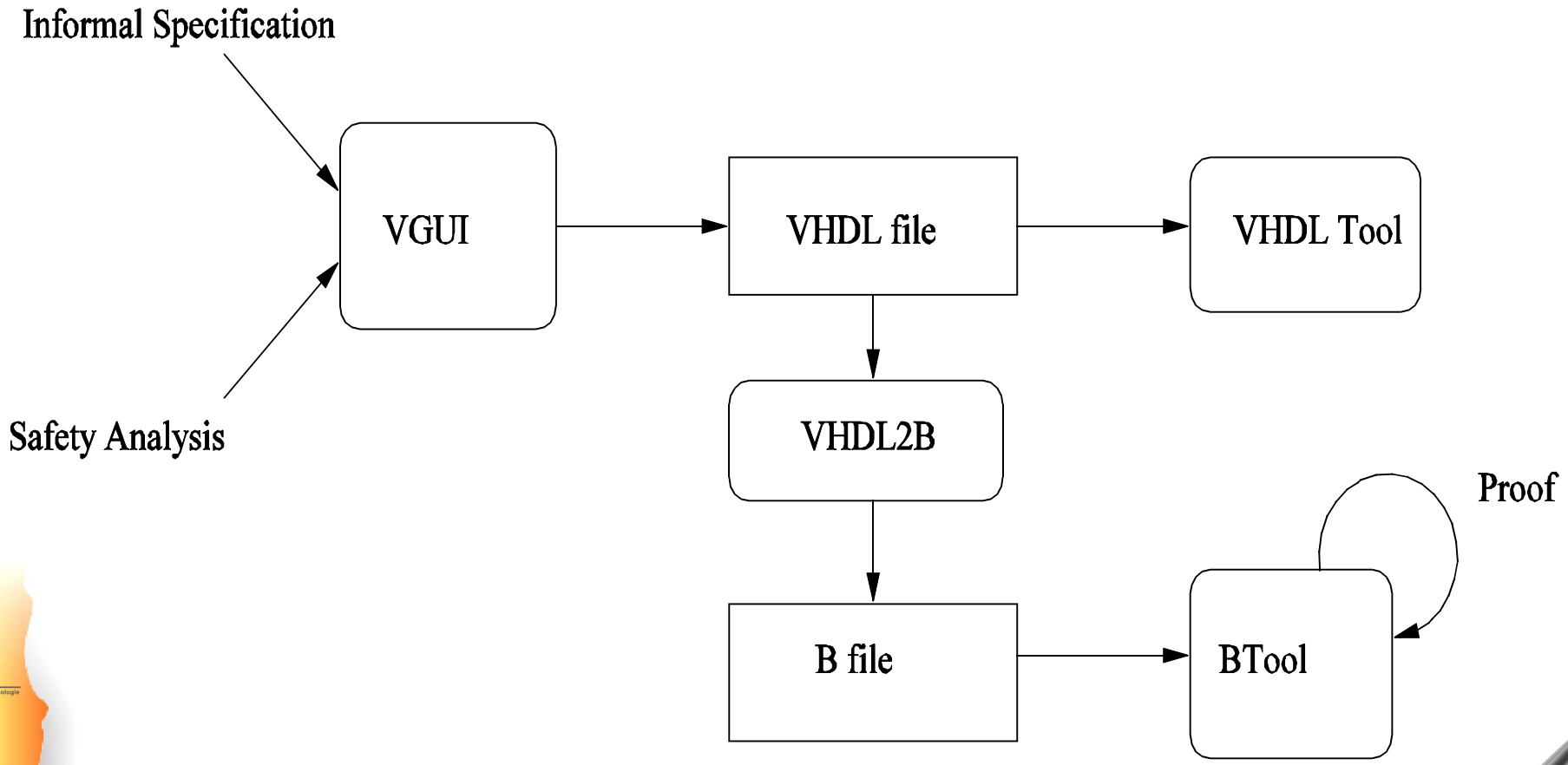
```
entity Half_adder is
  port (X, Y: in Bit;
        Sum, Carry: out Bit);
  end Half_adder;

architecture HA_Behavior of Half_adder is
  begin
    process
     begin
      Sum <= X XOR Y after 5 Ns;
      Carry <= X AND Y after 5 Ns;
      wait on X, Y ;
  end process;
end HA_Behavior;
```

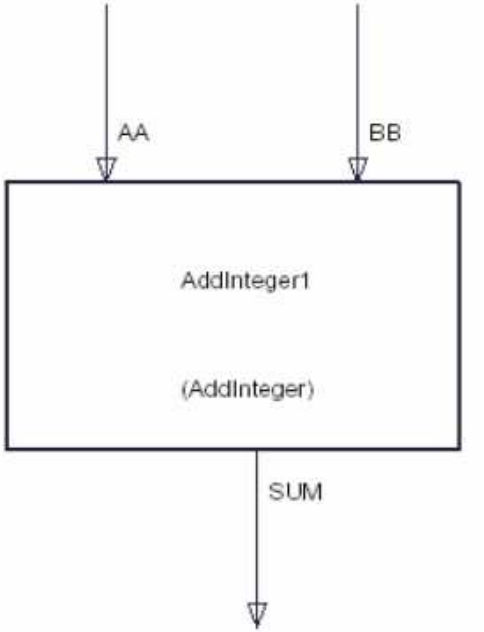
```
INITILISATION
        AND.in1:= II;
        AND.in2:= II;
        XOR.in1:= II;
        XOR.in2:= II
OPERATIONS
in1 (xx) =
PRE xx : BIT THEN
        AND.in1:=xx ;
        AND.out := sum ;
        XOR.in1:=xx ;
        XOR.out = carry
END
....
```


VHDL World
B World
Step 1
Step 2
Step 3
Design Specification
Data/Control Flow
Block Diagram
Data Dependencies
Formal Proof
- Specification Verification
Architecture Design
- Functionnality
- Architecture
- Interblock coordination
HDL system prototype
Formal Proof
- Architecture Verification
- Safety Verification
Prototype Verification
- Design Debugging
-Architecture Evaluation
- Redisgn
Design Specification for
Refinement
Design Refinement
- Synthesis
- Optimization
Implementation 1
....
Implementation n
Formal Proof
- Refinement verification
- Safety verification

Codesign


Informal Specification
Safety Analysis
VGUI
VHDL file
VHDL Tool
VHDL2B
B file
BTool
Proof

VGUI : VHDL Graphical User Interface



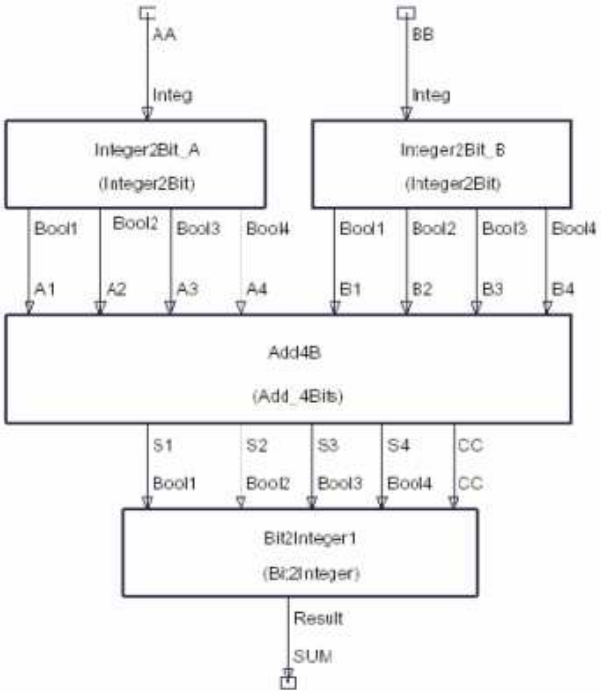
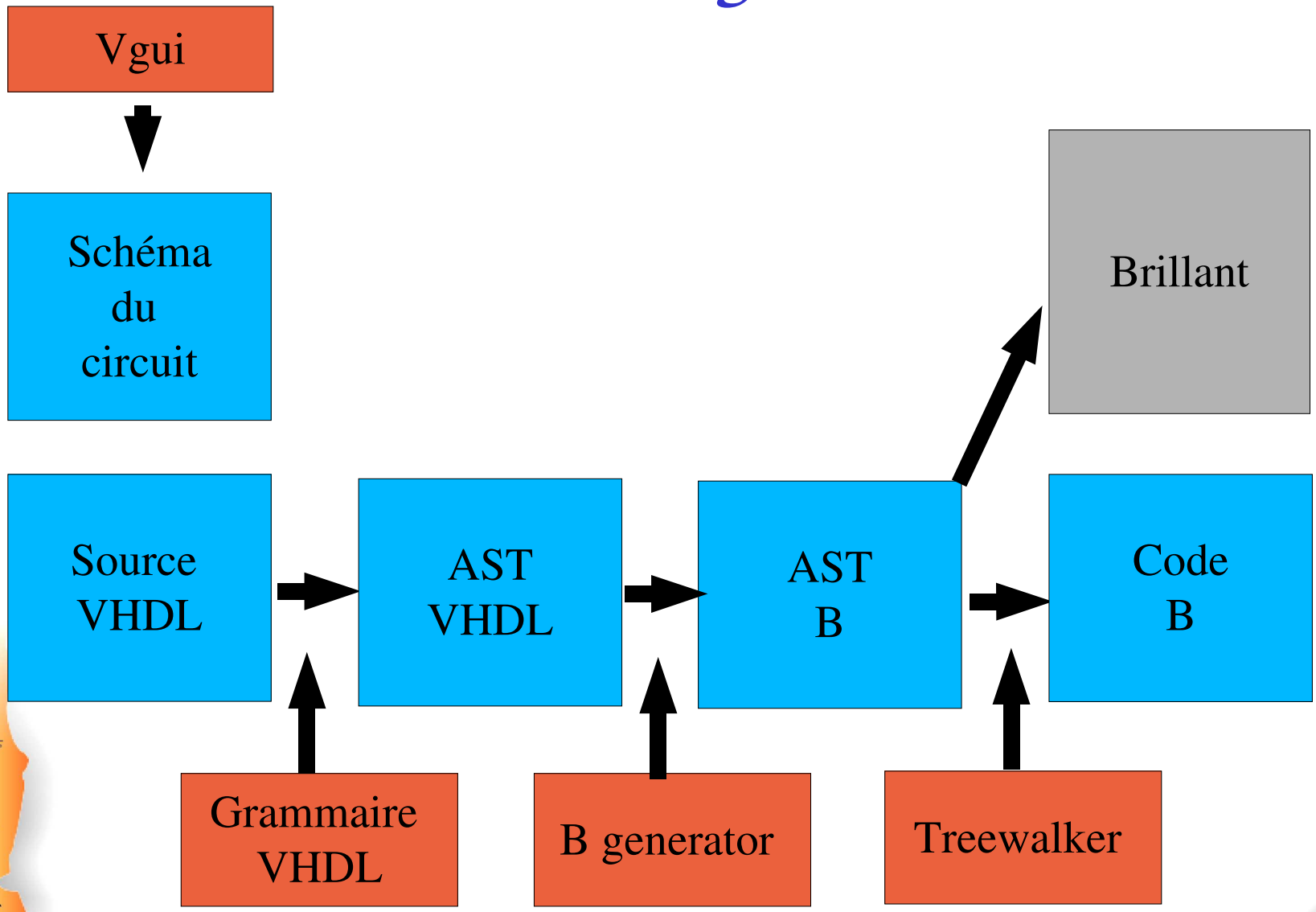


Schéma général



Circuit numérique sûr de fonctionnement

- Objectif:
  - Spécifier des circuits sûrs de fonctionnement (self-testing, failsafe, ..)
- Intérêt:
  - Démontrer la prise en compte de contrainte de sécurité dès la conception du circuit.
  - Démontrer que certains circuits vérifient des propriétés complexes.
- Délai:
  - Long terme.
- Qui :
  - UTC/INRETS

Safety, reliability and availability

- Circuit Failsafe
  - Lorsque le circuit est en fonctionnement toutes les anomalies amènent dans un état de sécurité
- Technologie dédiée
  - Circuits auto-testables et circuits failsafe
- Etat de l'art :
  - Dans le cadre de ses travaux le groupement INRETS-TIMA a étudié l'aspect simulation mais pas l'aspect preuve formelle.

Hardware Failures

- Stuck value
  - Boolean variable becomes a constant (0 or 1)
- Stuck-Open
  - Unwanted memory state
  - Combinatorial circuit --> Séquential circuit
- Others
  - Short circuits, stuck-on

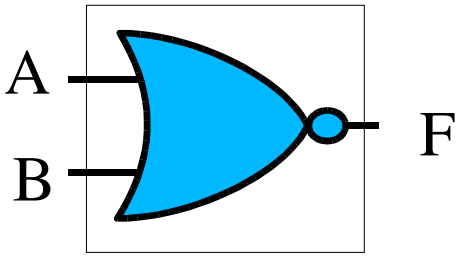
Propriétés fondamentales

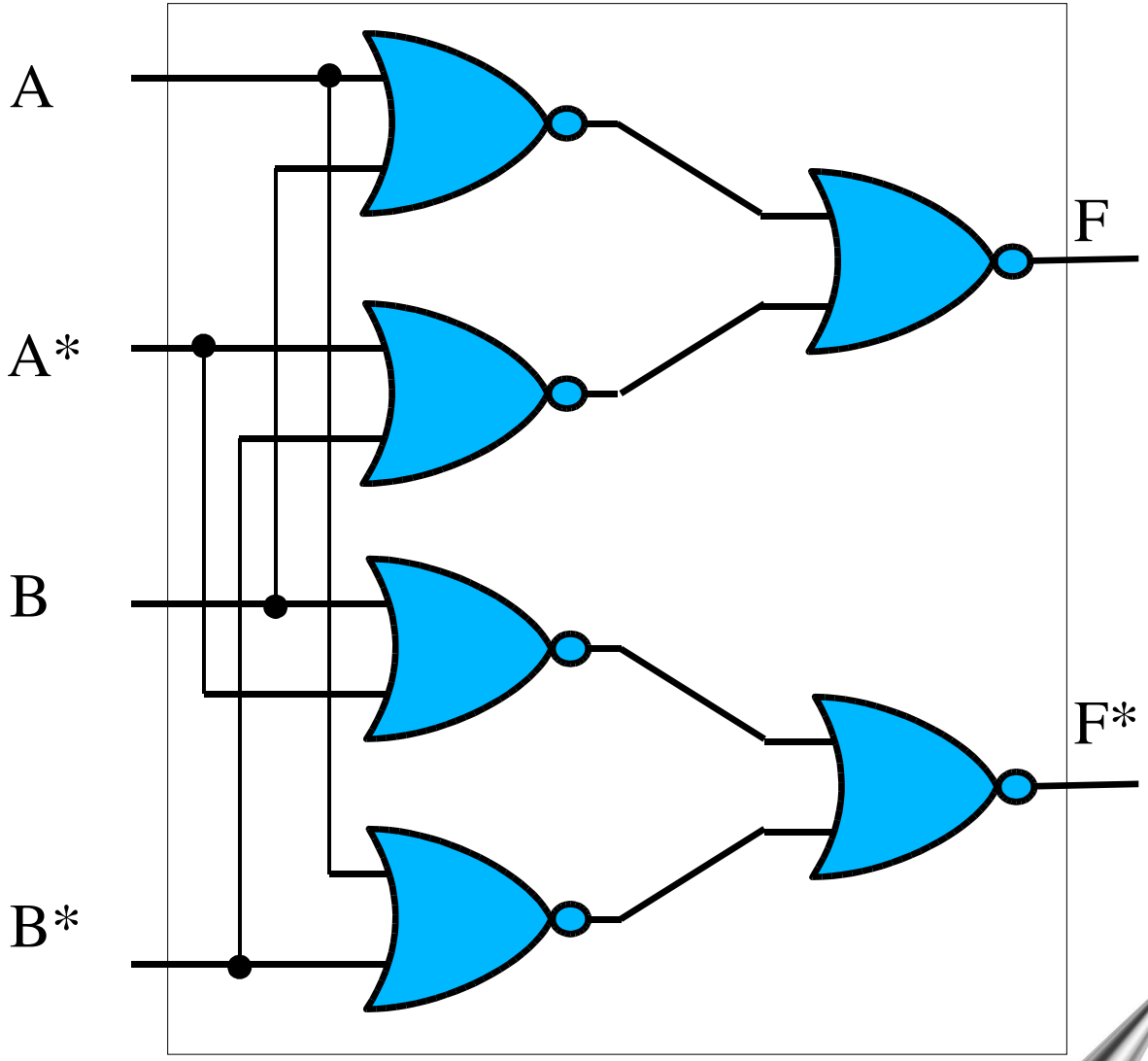
- Concepts de base
  - F, ensemble des anomalies connues
  - X, ensemble des vecteurs d'entrées
  - G, la fonction à réaliser
  - Les valeurs calculées sont codées (Code)
- Self-testing

$\exists f \in F, \forall x \in X, G(x,f) \neq Code$

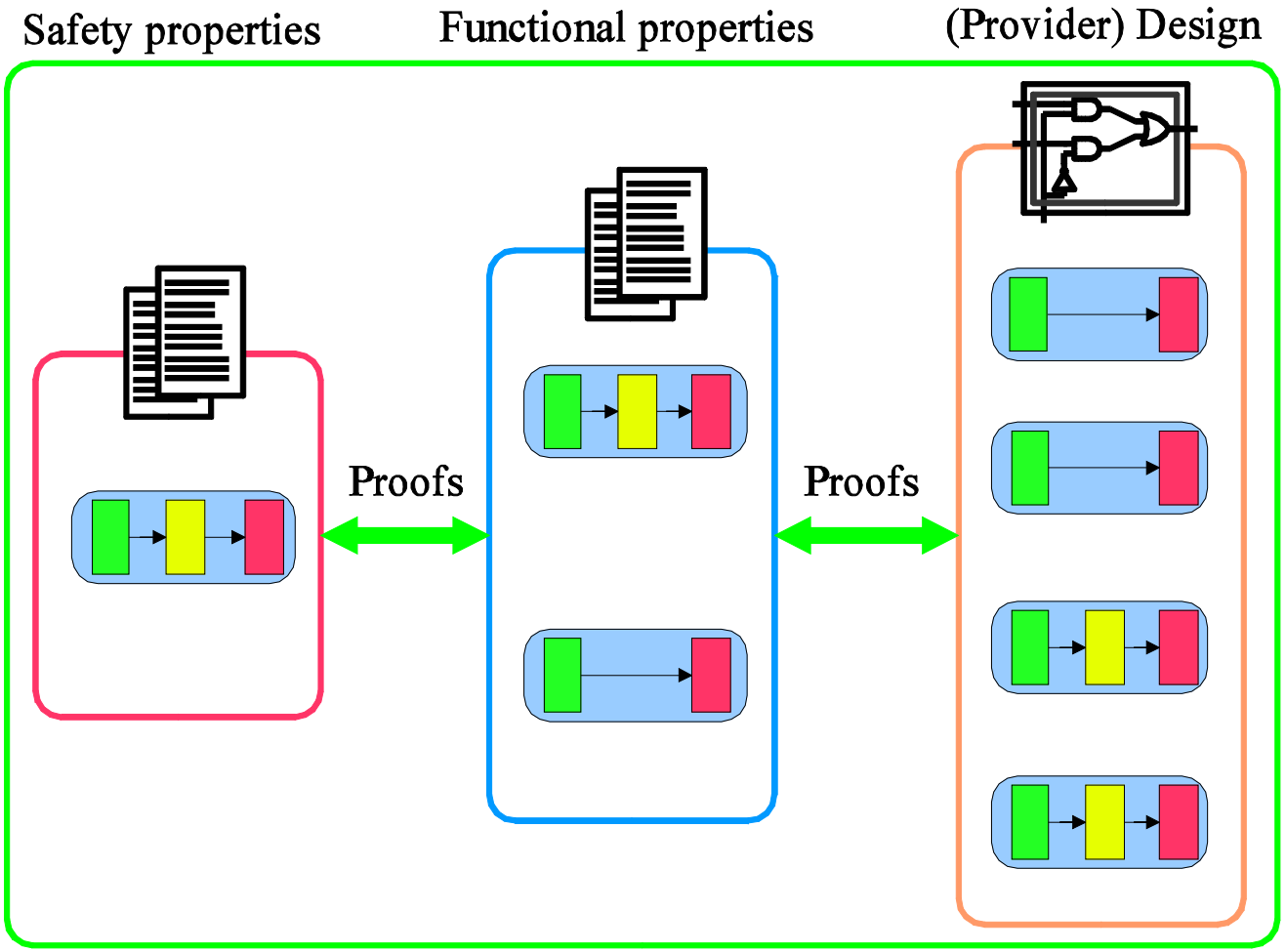
- Fail-safe (0/1)

$\exists x \in X, \forall f \in F, G(x,f) = G(x,\bar{f}) \text{ or } G(x,f)=0$


A
B
F


A
A*
B
B*
F
F*

Aspect Méthodologique



Conclusions
Limites
Perspectives

Résultats

1. Une image de la bibliothèque VHDL *STD_LOGIC_1164* est implantée en B,
2. Plusieurs circuits de base (AND,..,Multiplexor, 4bit-Add, ..) définissent notre bibliothèque standard.
3. Nous avons défini un processus de traduction d'un sous-ensemble de VHDL vers le langage B
4. Un traducteur automatique de code VHDL vers B est en cours de développement.

Limites

- Aspect temporel:
  - Introduction d'une extension de B au calcul des durées (Thèse INRETS).
- Aspect sous ensemble VHDL:
  - Nous savons parser correctement tout le langage VHDL;
  - Il faut déterminer le périmètre final;
  - Passer d'un prototype à un outil.

Perspectives

- Propriétés de haut niveau:
  - Mise en place d'une thèse pour étudier:
    - Le domaine des circuits sûrs de fonctionnement,
    - Le domaine des circuits vérifiant des propriétés complexes.
- Utilisation grandeur nature:
  - Définitions de circuits de taille plus importante,
  - Un contact industriel est intéressé par l'approche.

Publications

- ICSSEA01 lien entre VHDL et B
- COMPRAIL02 VHDL dans B
- EDCC4 2002 aspect outils
- ESREL2003 aspect méthode ADD-4bit
- ASCD03 aspect outils
- ELECTROCOMP03 aspect méthode

- Pour en savoir plus:
  - www.hds.utc.fr/bhdl