PRAGMADEV
real time development tools

Verification of model based designs.

Emmanuel Gaudin

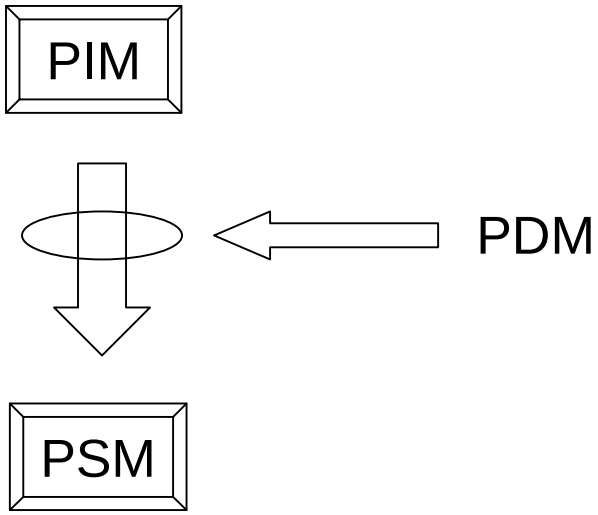
emmanuel.gaudin @ pragmadev.com

PRAGMADEV
real time development tools

Principles

- MDE, MDA et MDD: Model driven approach
  - PIM: Platform Independant Model
  - PDM: Platform Definition Model
  - PSM: Platform Specific Model

Principles



The goal is to transform the abstract model (PIM) to a concrete model (PSM) using the platform definition model (PDM).

PIM

- The abstract model must be platform independant, as its name states.
- The abstract model must be translatable to an implementation platform.
- For that purpose, the abstract model is based on a virtual machine offering:
  - Some basic services
  - A strong enough semantic.

PRAGMADEV
real time development tools

SDL: Specification and Description Language

SDL (Specification and Description Language) is an ITU (International Telecommunication Union) standard under referene Z.100.

- It aims at describing telecommunication protocols in an unambiguous way to ensure inter-operability of equipements,
- It is used by ETSI (European Telecommunications Standards Institute) to describe european telecommunication standards (X25, GSM, UMTS…),
- SDL is updated every four years, the first stable version was published in 1988.

PRAGMADEV
real time development tools

SDL: Specification and Description Language

- SDL models are platform independant,
- SDL defines a strong semantic,
- SDL embeds abstract data types,
- SDL is event driven,
- SDL is graphical,
- SDL is object oriented since 1992 (SDL'92).

PRAGMADEV
real time development tools

SDL: Specification and Description Language

- SDL models can be unformal (an action can be described in natural language)
- SDL models can un complete (operators can be defined outside of the model)
- SDL models can introduce undeterminism (ANY operator)
- SDL models can be formal (complete and non-ambiguous)

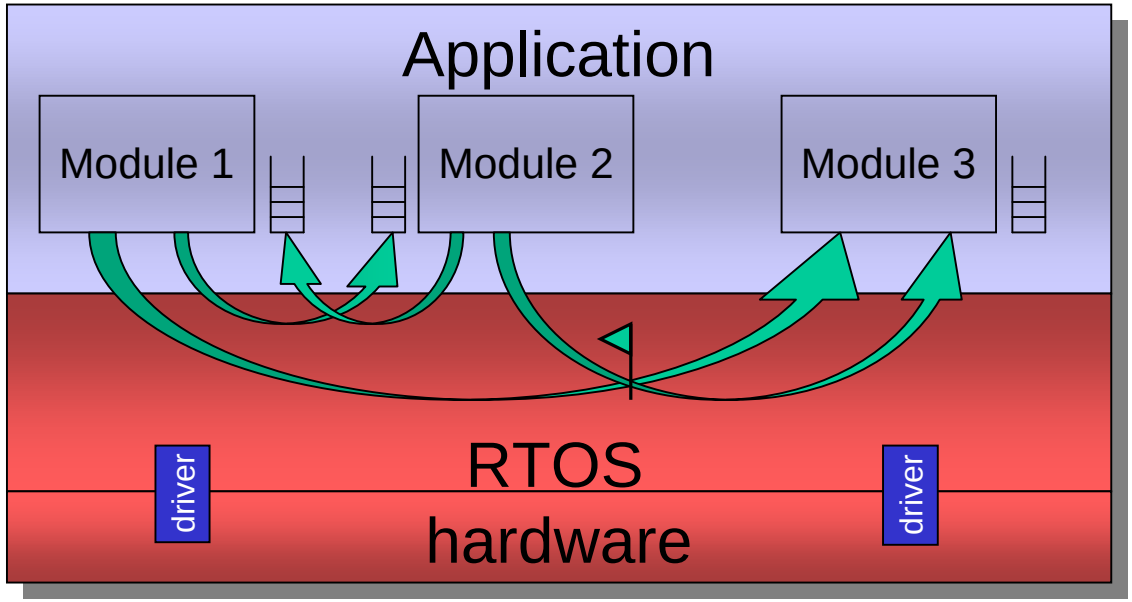
SDL: Specification and Description Language

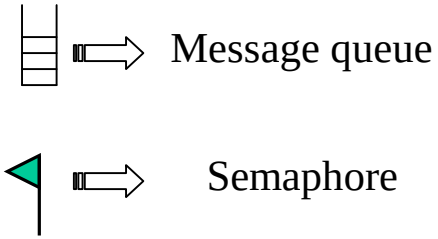
- The semantic and basic services defined in the language define an *SDL virtual machine* with the required characteristics of a Plateform Independant Model (PIM).
- The definition of the operator interfaces and the services implementation define the Plateform Definition Model (PDM),
- It is therefore possible to generate the Plateform Specific Model (PSM) such as for example a combination of an implementation language (C/C++), a Real Time Operating System (RTOS), and drivers on the target (operators).

Application domain

- Apart from telecommunication protocols, SDL concepts are similar to the ones found in embedded and real time applications based on real time operating systems.

- The application is split down in modules (threads) running in parallel,
- Communication is done via:
  - Messages
  - Interrupts
  - Function calls
  - Semaphores





SDL: the figures

Years of experience allows to quantify gains of SDL usage.

- C code: 35 to 50 mistakes per 1000 lines
- SDL code: 8 mistakes per 1000 lines

- Development time is globally reduced by 35%
  - Reduced up to 50% in the left branch of the V cycle
  - Less gain on the right side of the V because of the gap with technical reality

PRAGMADEV
real time development tools

UML: Unified Modeling Language

- **UML** (Unified Modeling Language) standardized by the OMG (Object Management Group).
  - Can be used to represent any type of systems,
  - Graphical,
  - Used at a pretty high level of abstraction,
  - Not formal, e.g. another language is necessary to describe in detail (C, C++, Java, SDL),
  - Very object oriented.

No real time specificity in UML

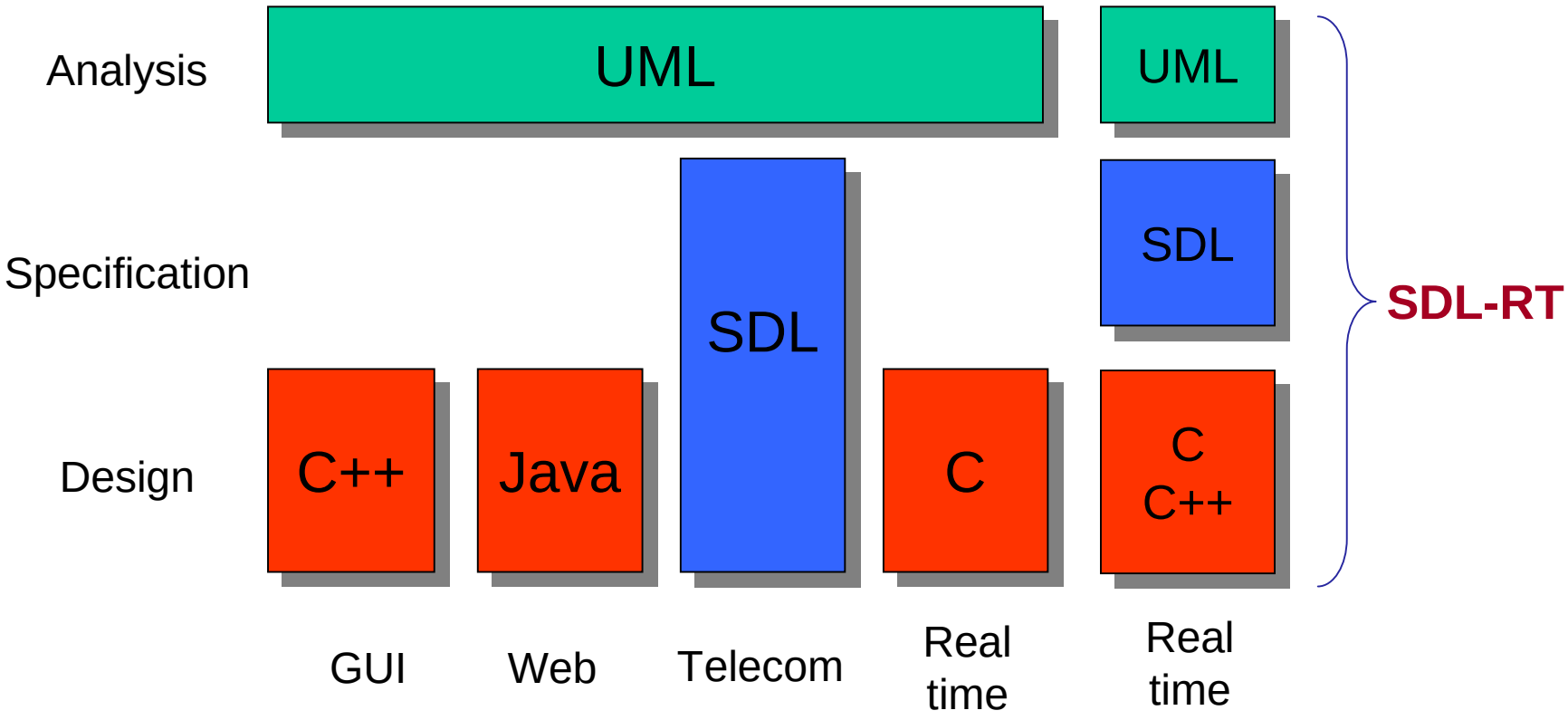
- UML 1 was to generic to be a PIM,
  - UML has no graphical representation for classical real time concepts such as: tasks, semaphores, messages, timers…
  - There is no semantic,
  - There is no data types,
- UML 2 allows to define profiles for each application domain in order to describe a valid PIM.

PRAGMADEV
real time development tools

UML compatibility

- UML 2.0 did not come with standard profiles for each application domain,
- UML 2.0 profiles are not compatible,
- ITU has standardized a UML2.0 profile based on SDL.

Languages positionning



SDL-RT

specification & description language - real time

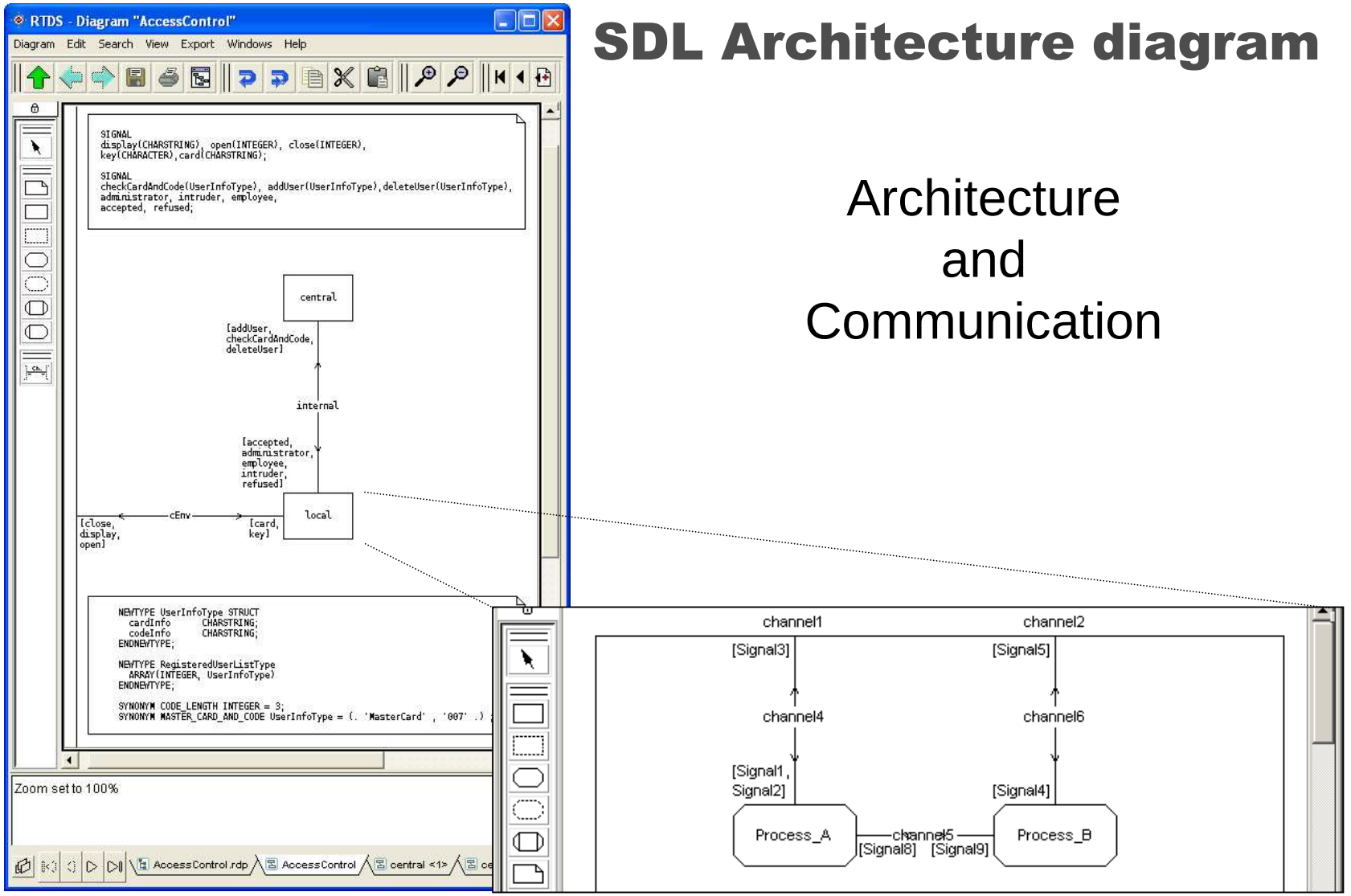
SDL-RT

- Extends SDL usage to all embedded and real time applications based on a RTOS,
- Legible and based on a standard textual storage format (XML),
- Submitted to ITU to be officially integrated in SDL,
- Is a UML profile for real time applications.

PRAGMADEV
real time development tools

SDL Architecture diagram

Architecture
and
Communication

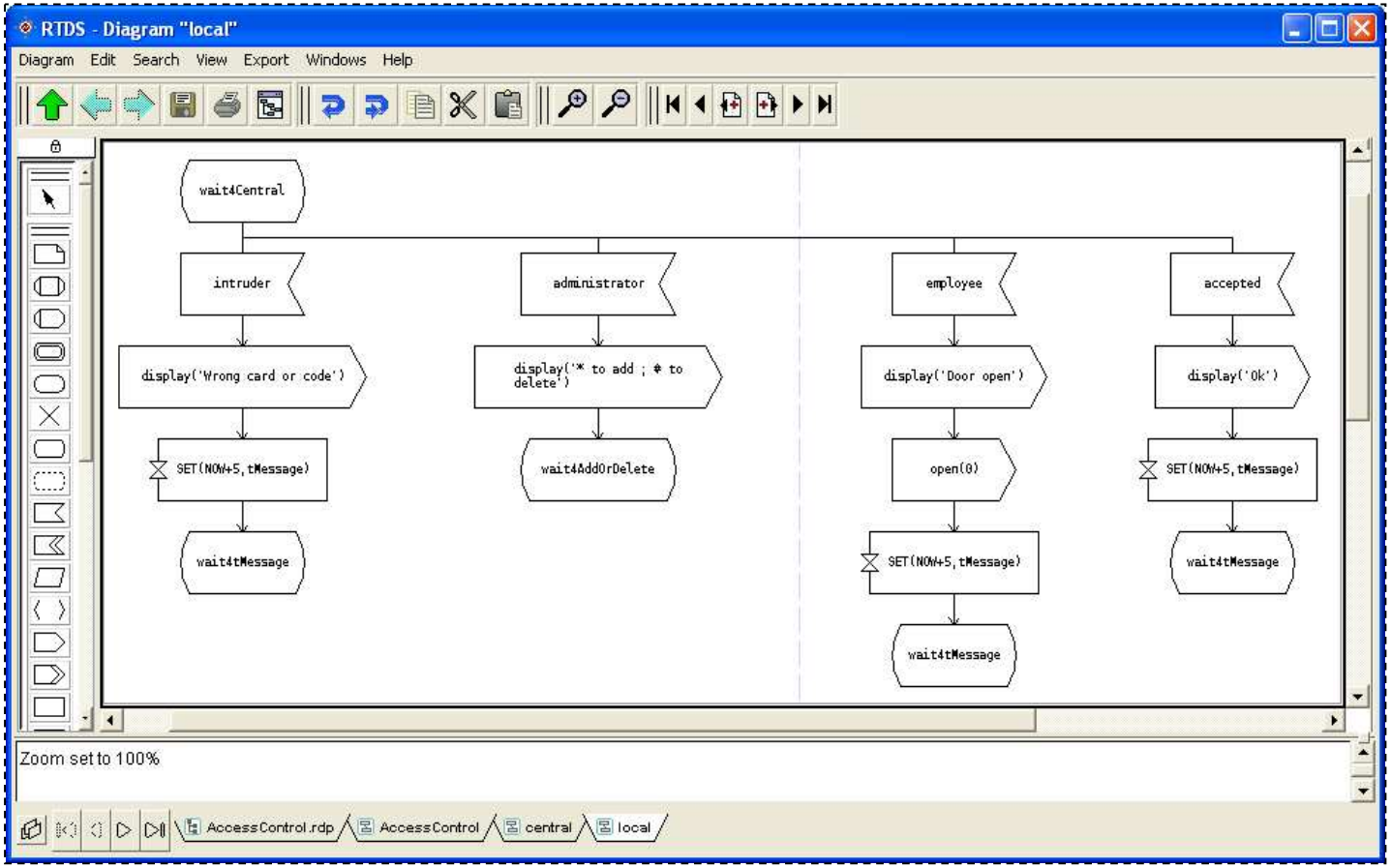


PRAGMADEV
real time development tools

SDL behavioral diagram

Behavior and Data

Process local



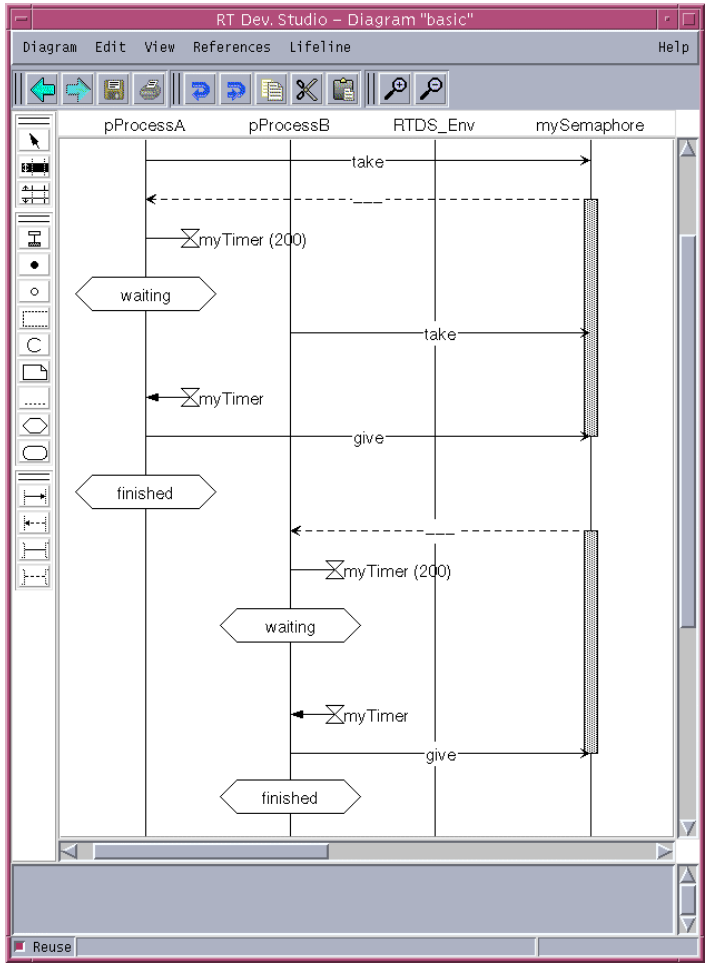
MSC: a dynamic view

Message Sequence Chart

- Vertical lines represent a task, the environment or a *semaphore*,
- Arrows represent message exchanges, a *semaphore manipulation* or timers.

Can be used:

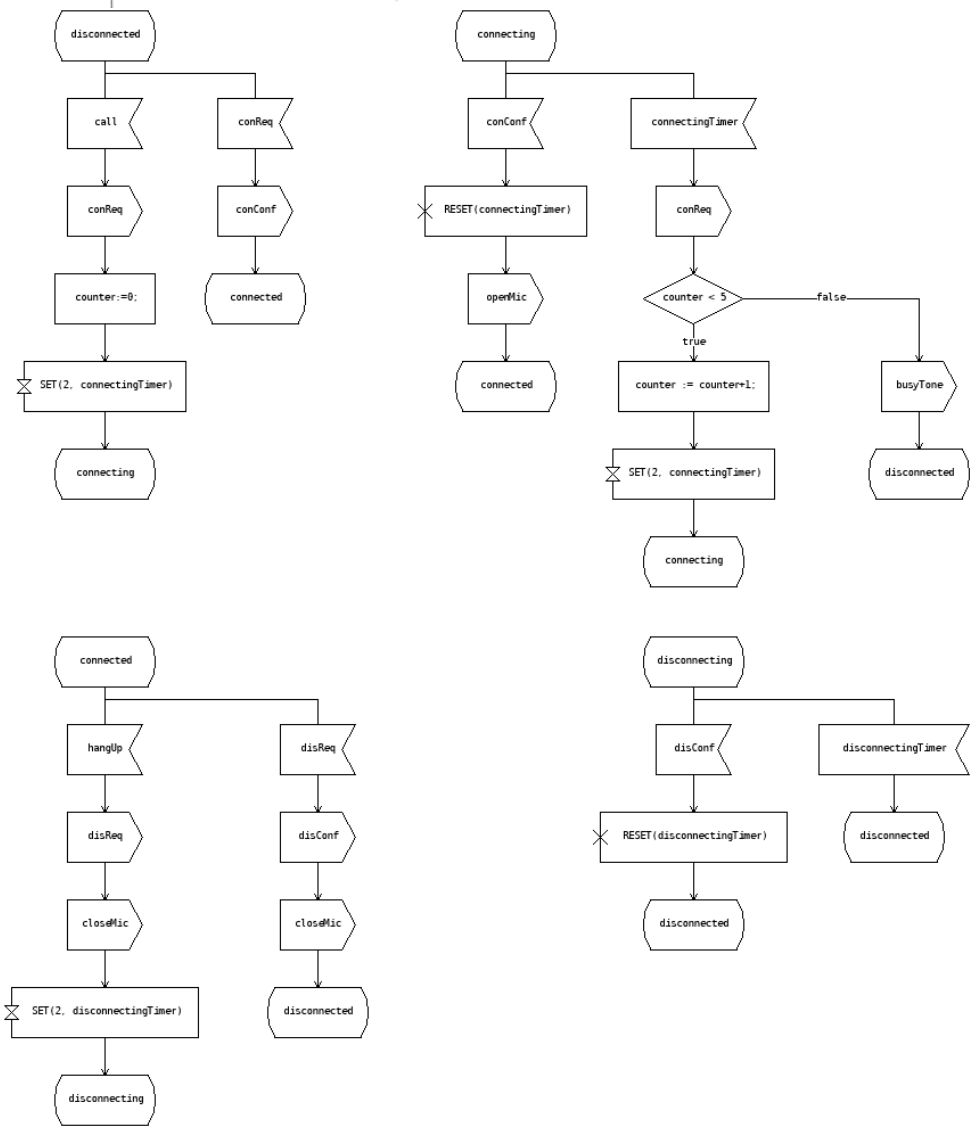
- As specification
- Execution traces



Principles of exhaustive simulation

- The strong semantic on which an abstract model is based allows the model to be interactively simulated.
- Model checking or formal verification requires some properties to be verified in all possible cases.

PRAGMADEV
real time development tools



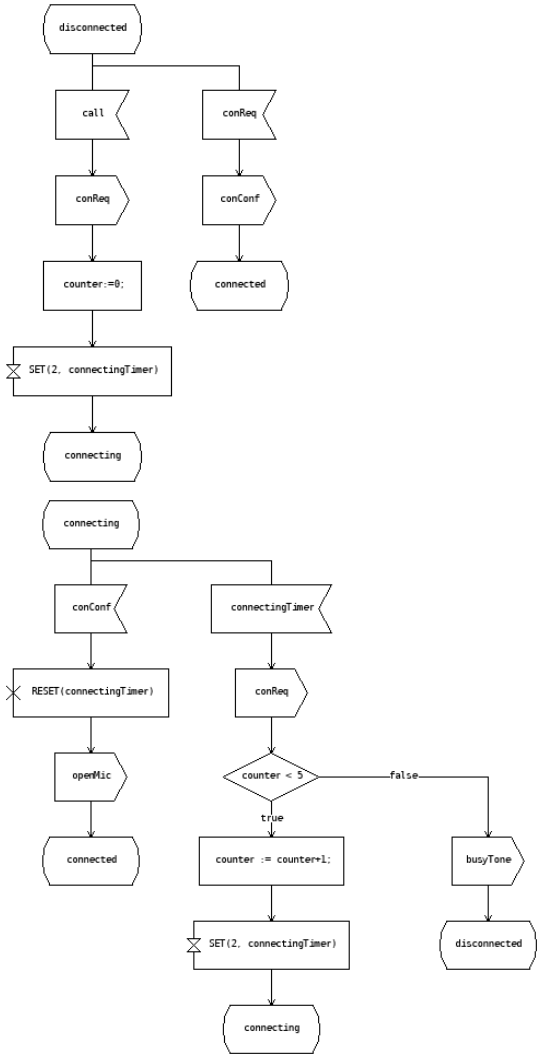
Notion of global system state

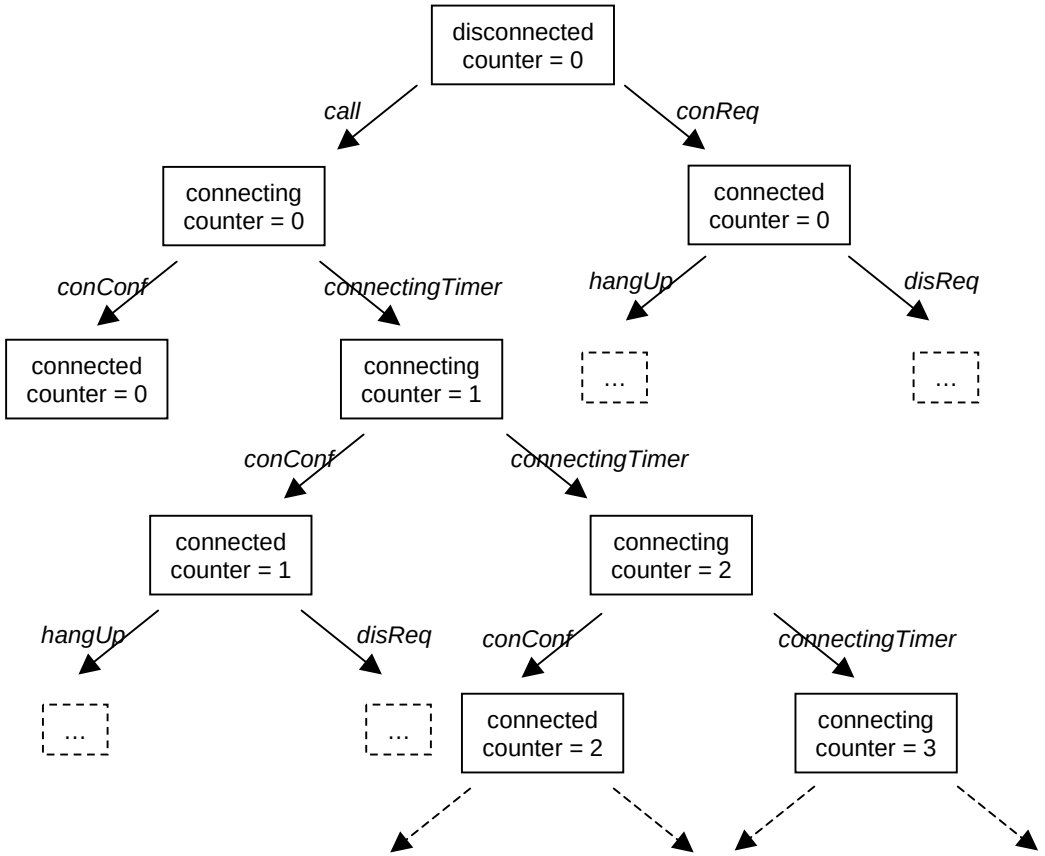
The global **system state** is a photo of the whole system. It includes the combination of the states of all finite state machines and the values of all variables.

In the enclosed example it would be the state of the protocol and the value of the counter.

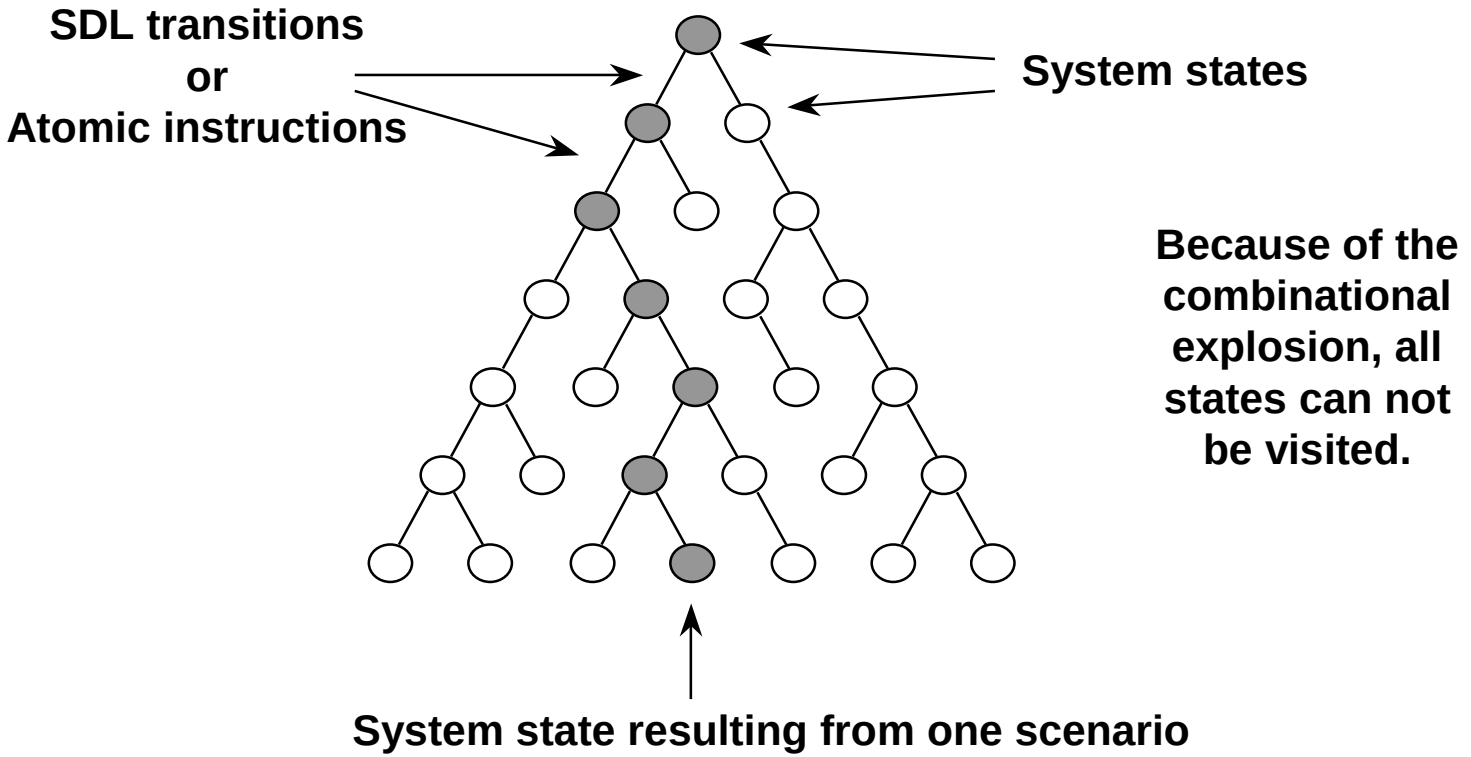
PRAGMADEV
real time development tools

Behavioral tree reachability graph





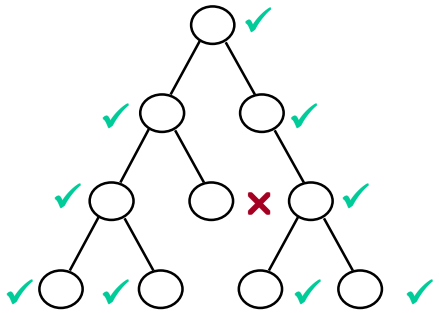
Behavioral tree or reachability graph



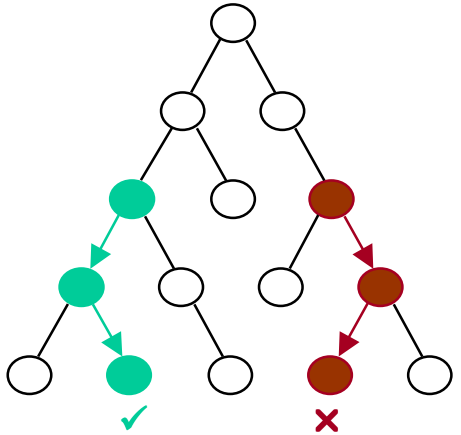
Rules

For each system state, some verifications are to be made:

- Static rules defined by axioms
- Dynamic rules defined by observers



Static rules verification



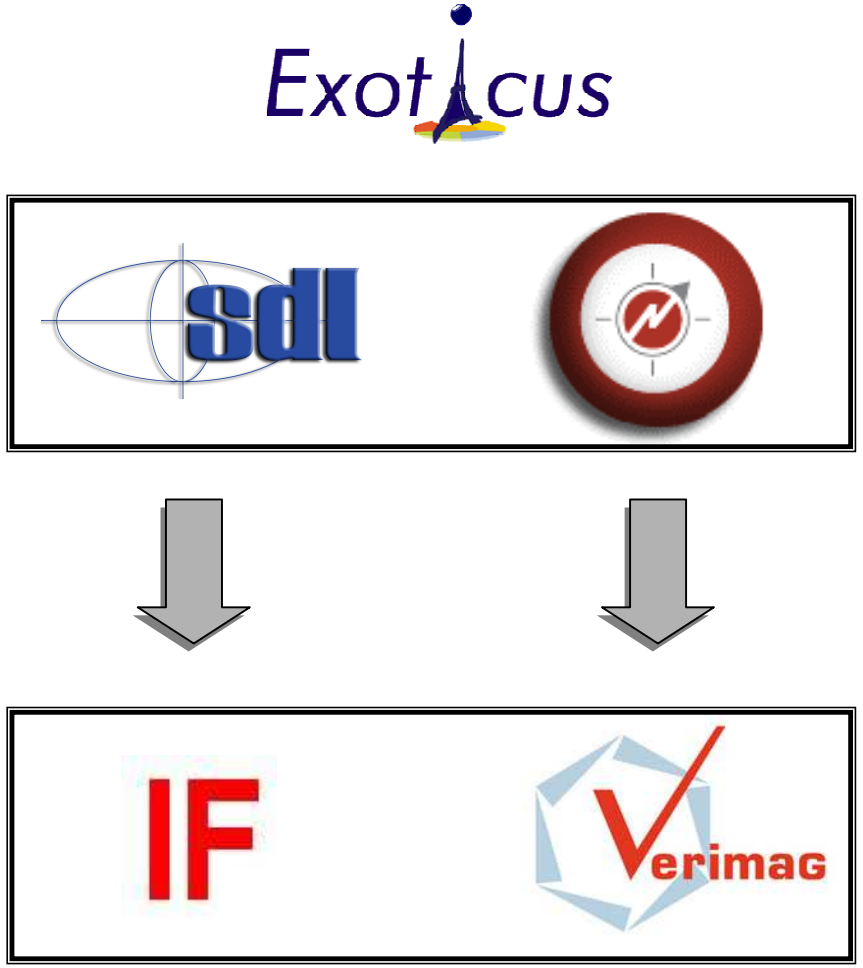
Dynamic rules verification

The same technic used to verify properties can be used to generate tests.

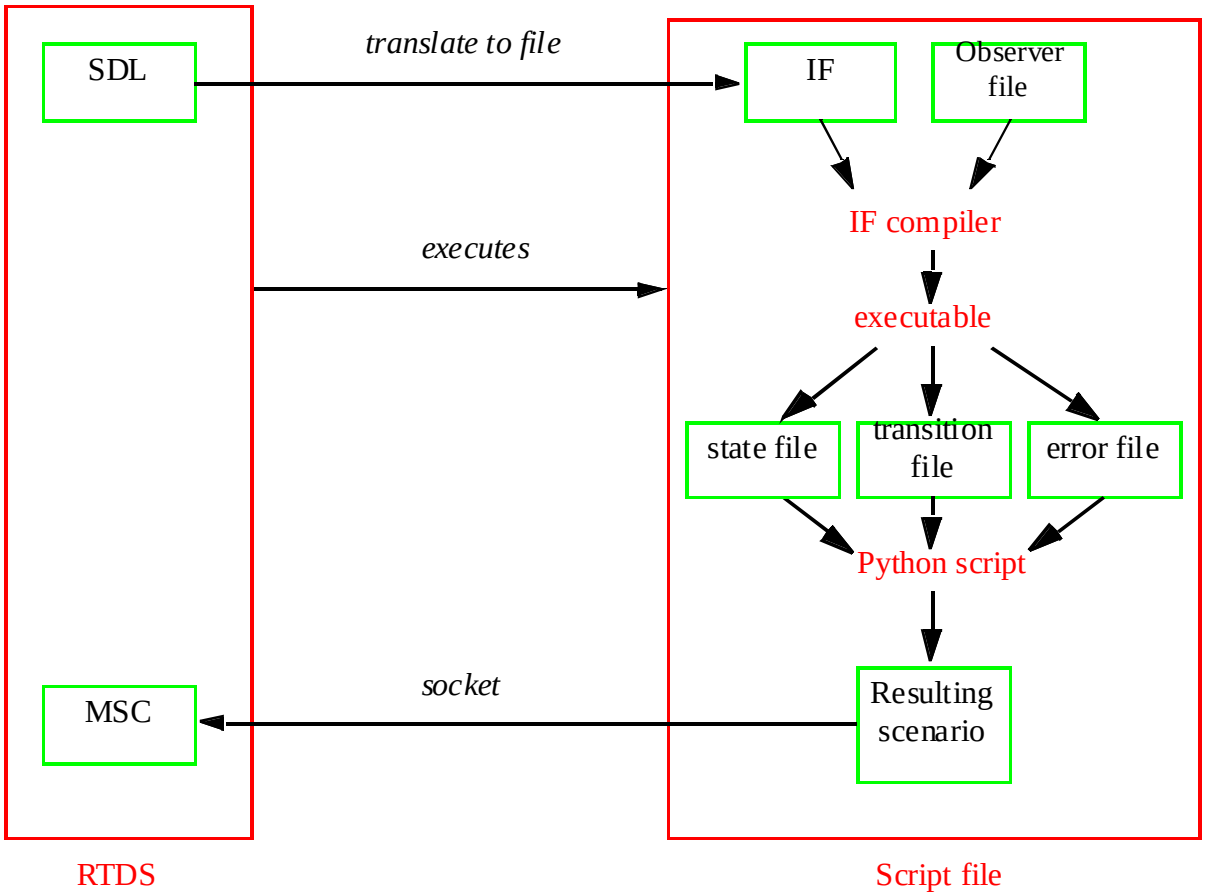
SDL model verification

Within the French national *competitiveness cluster* ExoTICus:

- Partnership with Verimag a national French lab on IF technology.
  - Exhaustive simulation,
  - Observers,
  - Test generation.
- Tool functionality
  - IF export,
  - Runs a script,
  - Generates an MSC trace.



Implementation



Conclusion

- SDL technology allows model based design for more than 20 years in the telecommunication domain
- ITU has defined a standard UML 2.0 profile based on SDL
- SDL-RT has extended SDL usage to all embedded an real time applications based on a RTOS
- SDL formalism allows interactive and exhaustive simulation
- Verification of static or dynamic rules allows to check the model or generate test suites