From Analysis to Code Generation of Protocols and Embedded Software with a UML-Based Formal Environment Named *TURTLE'2005*

Ludovic Apvrille

ludovic.apvrille@enst.fr

Outline

UML at a Glance

- Noting new but a federation of best practices
- A notation, not a methodology
- An international standard at OMG (Object Management Group)
  - *13 diagrams to express complementary point of views*
  - *Semantic variation points*
    - No standardized formal semantics
  - *Profile: the possibility to tailor the UML for your application domain*
- Industry support
  - *Tools (TAU G2, …)*
  - *Lingua franca for software-intensive system designers and developers*
- Research work
  - *Real-time?*
  - *Adding formality to the UML*
  - *A UML model for simulation, verification, code generation, test generation, performance evaluation, …*

UML Profiles for Embedded Systems and Protocols

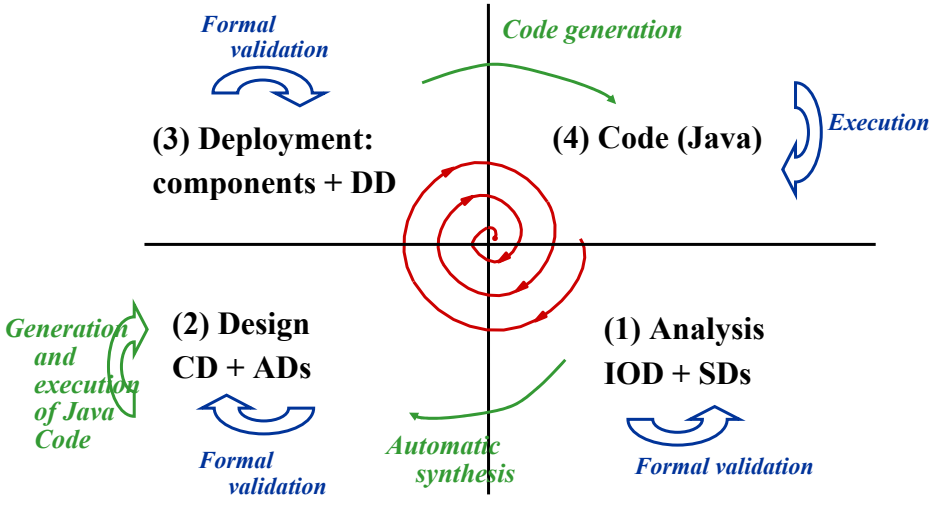
- Profile for Performance, Scheduling and Time
  - *Profile defined at the OMG*
  - *Addresses more specifically real-time systems*
- Rose RT Profile
  - *Toolkit*
    - Capsules
    - Ports
    - Protocols
    - Communication channels
  - *Methodology*
    - RUP
- TAU G2
  - *Toolkit based on UML 2.0 elements issued from SDL*
  - *Methodology*

Propositions

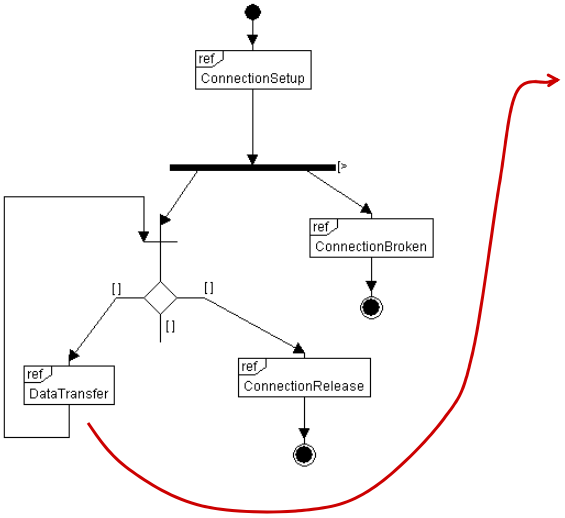
- **Idea: let us enrich UML**
  - *UML operators are informal*
  - *UML lacks advanced temporal operators such as time intervals*
  - *UML has no methodology (no validation)*
- **Proposition: Semi-formal UML-based environment**
  - *Semantics given by mapping to a Formal Description Technique*
- **What formal language?**
  - *Well-defined formal semantics*
  - *Logical and temporal operators*
  - *Tools*

=> RT-LOTOS / Petri Nets with real-time extensions
=> TURTLE UML profile (Timed UML and RT-LOTOS Environment)

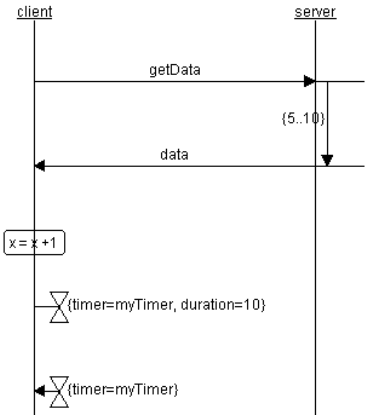
TURTLE: Methodology



TURTLE Analysis

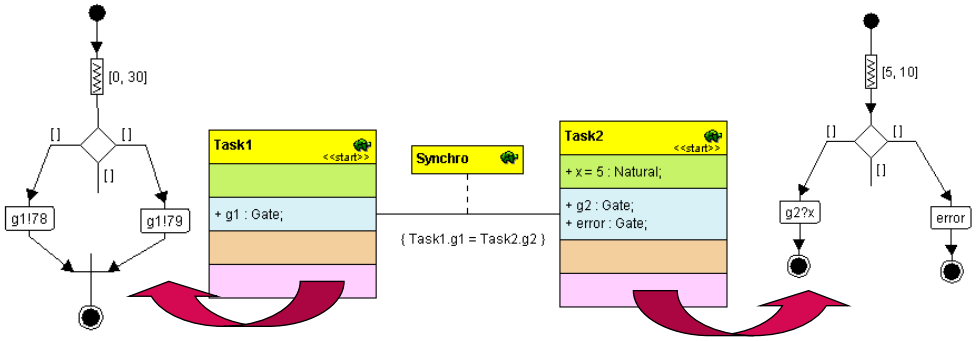


Interaction Overview Diagram



Sequence Diagram

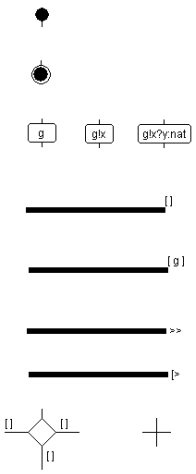
TURTLE Design

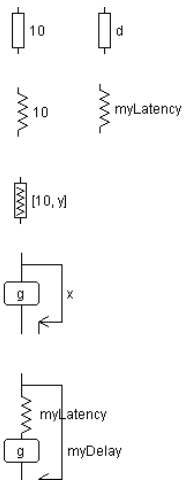


Relations between Tclasses: TURTLE's Composition Operators

- **Default relation**
  - ***Parallel***
- **Communication relations**
  - ***Synchro***
  - ***Invocation***
  - ***Note: Tclasses exchange information exclusively through communication gates***
- **Others**
  - ***Sequence***
  - ***Preemption***
- **There can be only one composition relation between two tclasses**

Activity diagrams: Logical and Temporal Operators



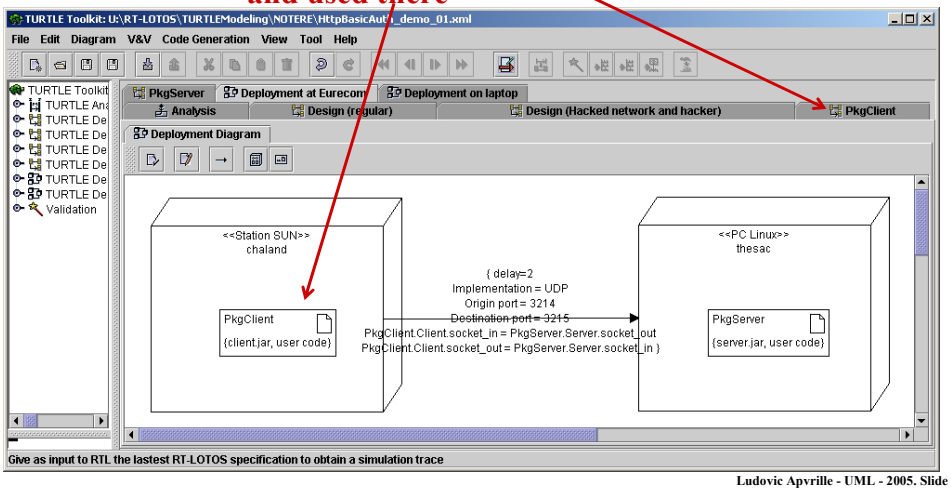


TURTLE Deployment diagrams

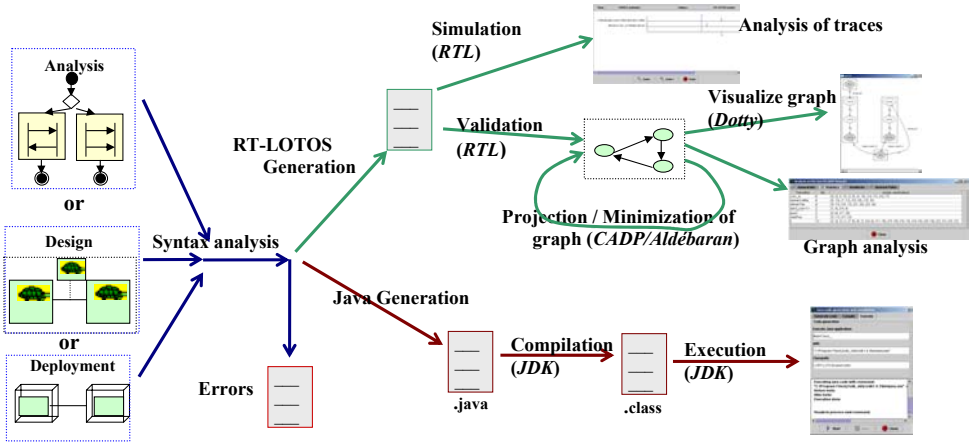
- **TURTLE artifacts**
  - ***Set a classes modeled in a TURTLE designs***
- **TURTLE Deployment diagrams**
  - ***Execution nodes***
    - **May hosts TURTLE artifacts**
  - ***Links between nodes***
    - **Interconnection of Artifacts' gates**
    - **Formal specification**
      - ***Parameter: delay, loss rate***
      - ***Pseudo FIFO***
        - Actions in the same time slot may be reordered
    - **For Java code generation**
      - ***Protocol: UDP, TCP, RMI***
      - ***Ports***

Example of TURTLE Deployment Diagram

Artifact *PkgClient* is defined here, and used there



TTool: an Open-Source Toolkit Developed at ENST - LabSoC



LOTOS

- LOTOS = Language Of Temporal Ordering Specification
  - *Standardized at ISO*
  - *Process algebra*
- Choice, Parallel, Synchro, Sequence, Disrupt
  - *P[a,b, c, d] = P1[a, b] [] P2[c, d]*
  - *P[a,b, c, d] = P1[a, b] ||| P2[c, d]*
  - *P[a, b, c] = P1[a, b] |[b]| P2[b, c]*
  - *P[a, b] = P1[a] >> P2[b]*
  - *P[a, b] = P1[a] [> P2[b]*

RT-LOTOS

- **LOTOS with real-time extensions!**
  - ***Delay***
  - ***Latency***
  - ***Time-limited offer***

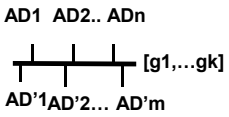
  - ***delay(10) a;***
  - ***latency(15) b;***
  - ***c{12};***

Example of an RT-LOTOS Specification

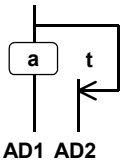
```
specification MEDIUM : noexit :=
(...)
behaviour
    hide iu_s, iu_d in
    let period : nat = 30000 in

    stream_sender[iu_s](0, period)
    |[iu_s]|
    medium[iu_s,iu_d](14000, 20000)

where
    process stream_sender [iu_s] (n : nat, period : nat) : noexit :=
            iu_s0!n; delay(period) stream_sender[iu_s] (n+1, period)
    endproc

    process medium [n_in,m_out] (dmin, dmax : nat) : noexit :=
            m_in?x:nat; delay(dmin,dmax)m_out!x; medium[m_in,m_out](dmin,dmax)
    endproc

endspec
```

Semantics of TURTLE Operators

- Translation algorithms



$(\tau(AD1) ||| \tau(AD2) ||| \ldots \tau(ADn)) >>$
$(\tau(AD'1) ||g1, \ldots gk|| \tau(AD'2) ||g1, \ldots gk||$
$\ldots \tau(AD'm))$

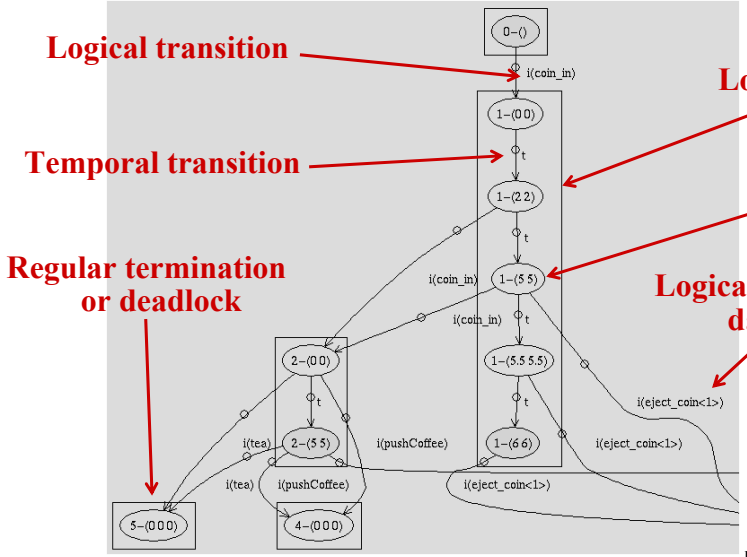


$a\{t, \tau(AD2)\}; \tau(AD1)$

RTL Toolkit (Developed at LAAS-CNRS)

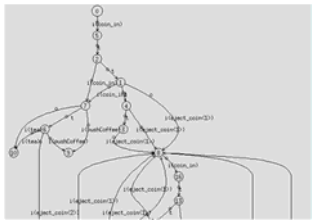
- Simulation
- Generation of DTAs
- Generation of reachability graphs

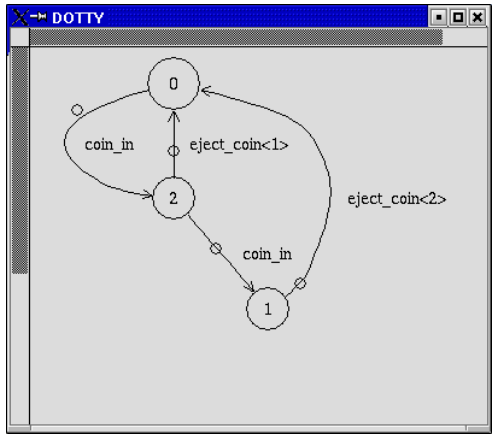
Visualization of Graphs (Cont.)



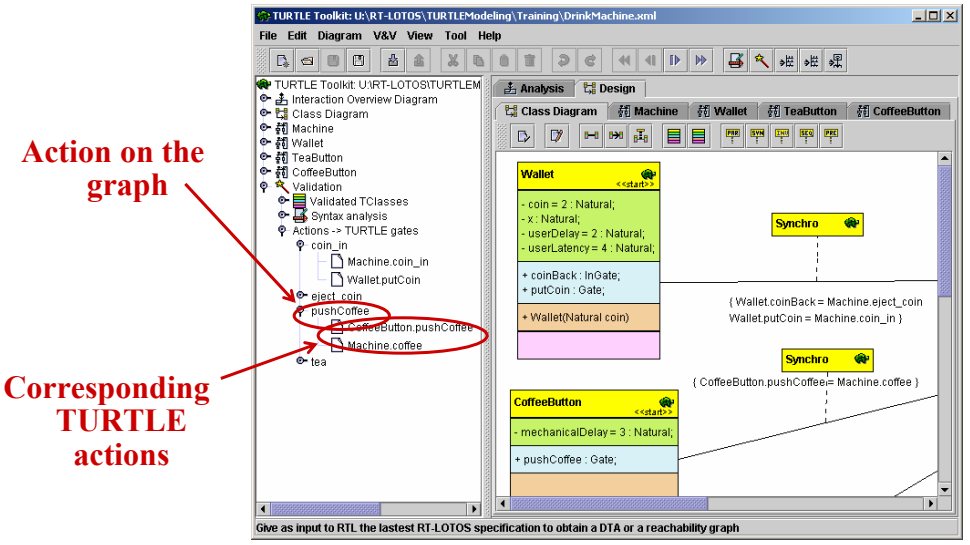
Minimized Graph (Obtained with CADP – INRIA)

Projection and Minimization





From Graphs to TURTLE Actions



Other Useful Features

- **Generation of executable Java code**
  - ***From design: monolithic application***
  - ***From deployment: network-aware code***
    - **UDP, TCP, RMI**
- **Libraries of TURTLE elements**
- **Design**
  - ***Observer***
    - **Reduce combinatory explosion**
  - ***TObjects***
    - **Instances of TURTLE classes**
  - ***TDatas***
    - **Definition of complex types**

Other Useful Features

- **TTool is released with a CeCILL License**
  - ***GPL-like***
  - ***Sources may be quite easily extended to***
    - **Support other diagrams**
    - **Provide other semantics to diagrams**
    - **Implement other code generators**

Use of TURTLE / TTool

- **Modeling of embedded software**
  - ***Alcatel Space (proofs of dynamic reconfiguration)***
- **Modeling of protocols**
  - ***TéSA laboratory (DIPCAST Project)***
  - ***UDCast (Maestro project)***
- **Modeling of security constraints**
  - ***LAAS-CNRS (Safecast project)***
- **Others**
  - ***Link between Telelogic TAU G2 / TTool***
  - ***Generator of documentation***
  - ***Use in lab sessions***
  - ***…***

Any questions?

- **TURTLE's website:**
  - *http://labsoc.comelec.enst.fr/turtle*
- **TTool's website:**
  - ***http://****labsoc.comelec.enst.fr/turtle/ttoolindex.html*

References

- **Definition of the profile**
  - *L. Apvrille, P. de Saqui-Sannes, A. Apvrille, "Une méthodologie de conception des systèmes distribués basée sur UML", Actes de la 5ème conférence sur les nouvelles technologies de la répartition (NOTERE'05), p 217-214, Gatineau, QC, Canada, 29 aout - 1er septembre 2005.*
  - *L. Apvrille, P. de Saqui-Sannes, F. Khendek, "Synthèse d'une conception UML temps-réel à partir de diagrammes de séquences", Actes du Colloque Francophone sur l'Ingénierie des Protocoles (CFIP'05), Bordeaux, France, 29 mars - 1er avril 2005 (in French).*
  - *L. Apvrille, J.-P. Courtiat, C. Lohr, P de Saqui-Sannes , "TURTLE: A Real-Time UML Profile Supported by a Formal Validation Toolkit", IEEE Transactions on Software Engineering, Vol. 30, No. 7, pp. 473-487, July 2004*
  - *C. LOHR , L. APVRILLE, P DE SAQUI-SANNES, J.-P. COURTIAT, "New Operators for the TURTLE Profile", 6th IFIP International Conference on Formal Methods for Open Object-based Distributed Systems (FMOODS'03), LNCS, Springer, Paris, France, November 2003.*
  - *P. DE SAQUI-SANNES, L. APVRILLE, C. LOHR, P. SÉNAC, J.-P. COURTIAT, "UML and RT-LOTOS: An Integration for Real-Time System Validation", European Journal of Automation (JESA), Vol. 36, p. 1029-1042, Ed. Hermès, 2002.*
  - *L. APVRILLE, P. DE SAQUI-SANNES, C. LOHR, P. SÉNAC, J.-P. COURTIAT, "A New UML Profile for Real-time System Formal Design and Validation", Proceedings of the Fourth International Conference on the Unified Modeling Language (UML'2001), Toronto, Canada, October 2001.*
- **Use of the profile**
  - *L. APVRILLE, P DE SAQUI-SANNES, P. SENAC, C. LOHR, "Verifying Service Continuity in a Satellite Reconfiguration Procedure", Journal of Automated Software, Engineering, Kluver , issue 11:2, 2004.*
  - *L. APVRILLE, P. DE SAQUI-SANNES, P. SÉNAC, C. LOHR, "Reconfiguration dynamique de protocoles embarqués à bord de satellites", Actes du Colloque Francophone sur l'Ingénierie des Protocoles (CFIP'2002), Montréal, mai 2002.*