SITRAER 2015
AIR TRANSPORTATION SYMPOSIUM
São José dos Campos, SP, Brazil
October 26 - 28, 2015

26/10/2015

Fabio Seiti Aguchiku - Atech
Rafael Leme Costa - Atech
Eric Conrado de Souza - Atech
Newton Maruyama – POLI/USP

THE MODEL-DRIVEN DEVELOPMENT APPROACH & FORMAL SPECIFICATION FOR AIR-TRAFFIC CONTROL SYSTEM OPERATIONS: PRACTICAL COMMENTS AND CASE STUDIES

atech
GRUPO EMBRAER

Agenda

atech
GRUPO EMBRAER

- Motivation
- Introduction - Models
- BridgePoint - xtUML
- Formal Verification – FDR3 & AutoFocus3
- MDD Issues
- Conclusion

Motivation

Corporations want systems that work!

... as fast as possible,

as cheap as possible and

as easy to change as possible...

System development is difficult!

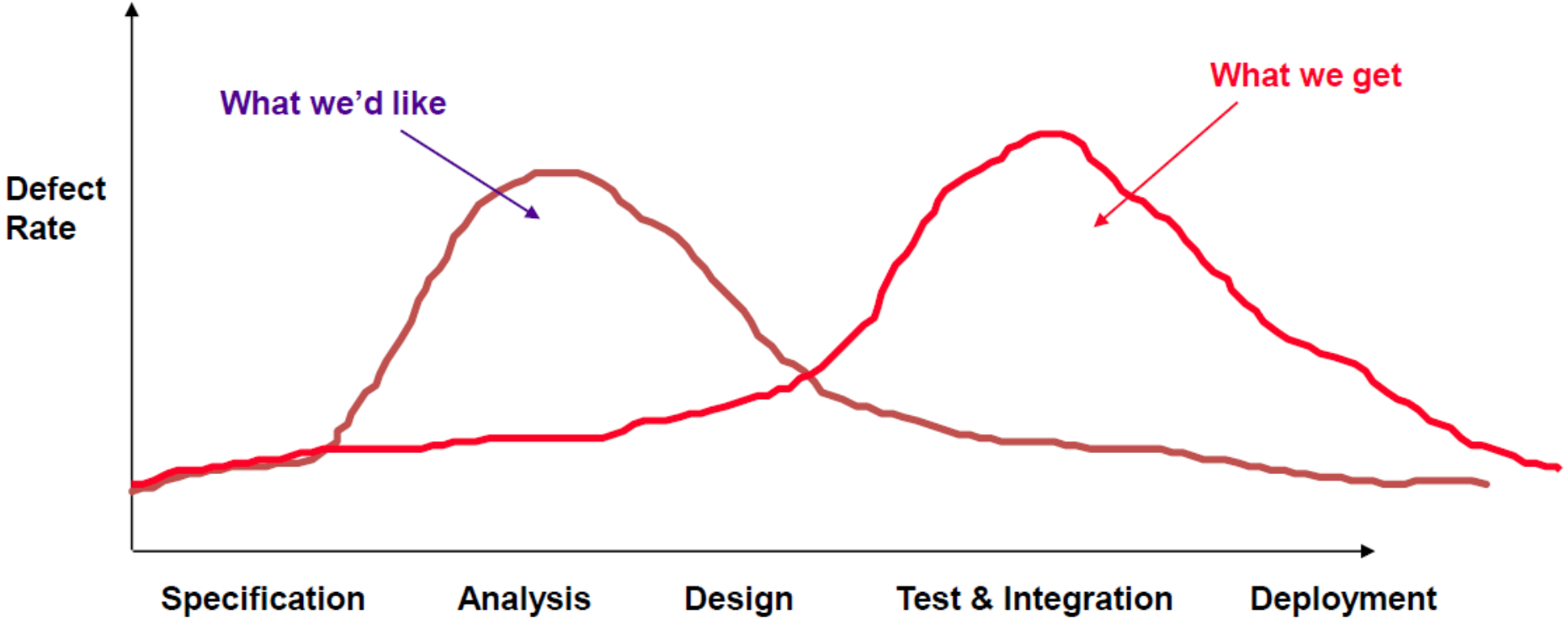
- take overlapping and conflicting requirements
- invention of good abstractions from those requirements
- fabrication of an efficient, cost-effective implementation
- clever solutions
- succesful conclusion at the lowest possible cost in time and money

(Balcer & Mellor, 2002)

Cost of fixing the defect	**Detection of defects**				
Introduction of defects	Requirements	Architecture	Construction	System Test	Post-Release
Requirements	1x	3x	5-10x	10x	10-100x
Architecture	-	1x	10x	15x	25-100x
Construction	-	-	1x	10x	10-25x

(MCCONNELL, 2004) *Code Complete: A Practical Handbook of Software Construction.*

- Systems are difficult to test—and it occurs too late.
  - Wasted effort in constructing wrong code
  - Late discovery of problems and delayed delivery



Motivation

“The lack of an integrated view often forces developers to implement suboptimal solutions.” *– Douglas C. Schmidt (2006)*

“***Model to have a conversation***.” **–** Craig Larman and Bas Vodde

Motivation

"***The sciences do not try to explain, they hardly even try to interpret, they mainly make models***. *... The* ***justification of such a mathematical construct is*** *solely and precisely* ***that it is expected to work***."
— John von Neumann

Motivation

Air Transportation domain:

- **Software** intensive
- Computationally **distributed**
- Great **complexity**
- Represents great potencial for **accidents**

Safety-critical systems

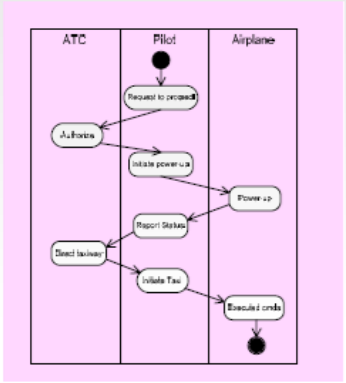
Intro – *From Document-centric to Model-centric*

atech
GRUPO EMBRAER

Past

- Specifications
- Interface requirements
- System design
- Analysis & Trade-off
- Test plans

Future



*"The underlying motivation for MDD is to **improve productivity."** –* Atkinson (2003)

Models

"*Separate those things that change from those things that do not*" – IBM-Rational Software Group (2008)

- Things that change rapidly:

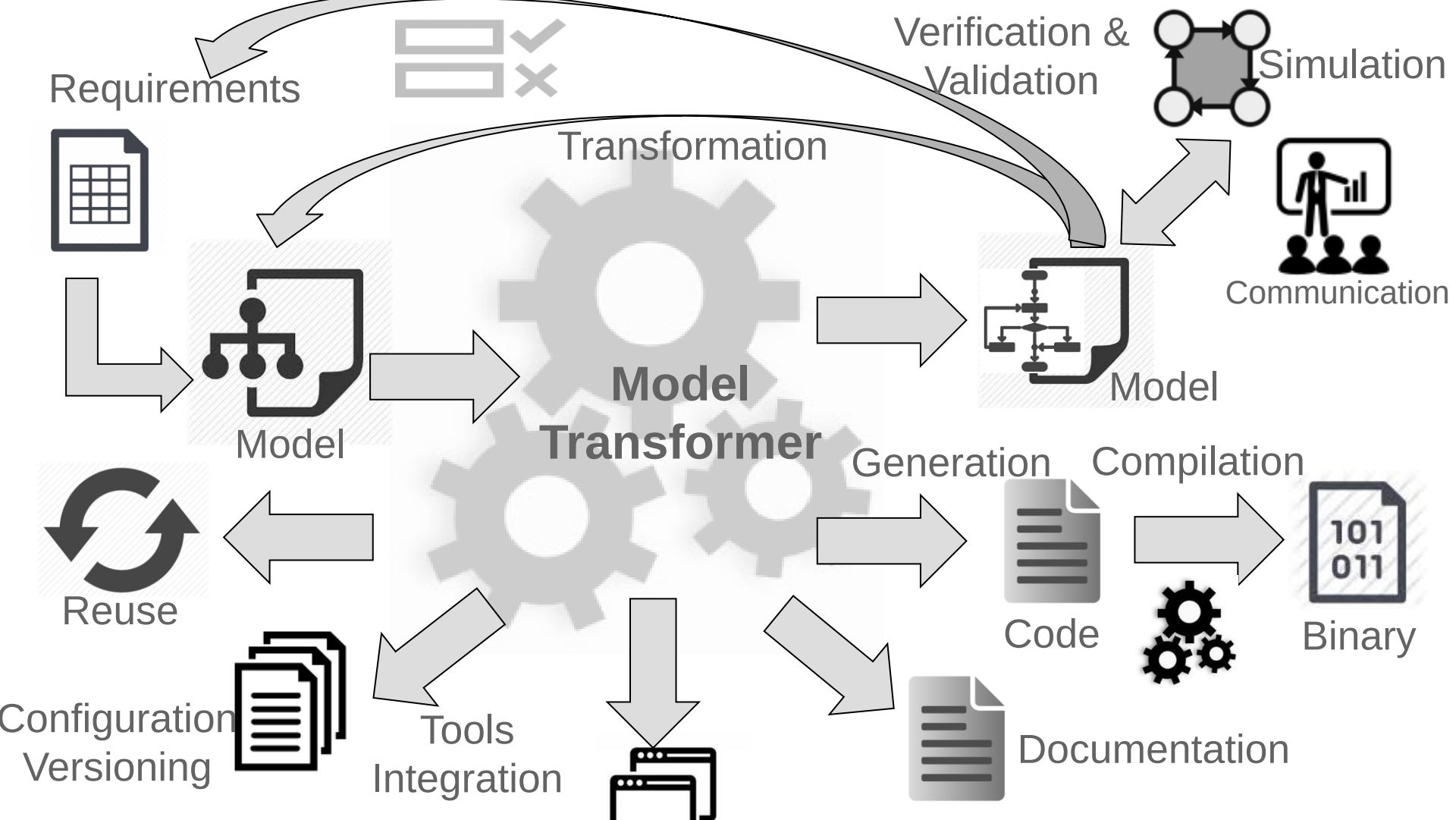
  Technology, Hardware Platforms, Sensor Technology,
  Operating environments, Connectivity

- Things that do not:

  Problem Domain semantics,
  Relations among domain concepts

"Free architecture from implementation details – conceptual architecture and technology decisions are decoupled, making both easier to evolve"

(Volter, 2010)


Requirements
Verification &
Validation
Simulation
Transformation
Communication
Model
Model
Transformer
Model
Generation
Compilation
Reuse
Code
Binary
101
011
Configuration
Versioning
Tools
Integration
Documentation

Mentor Graphic's BridgePoint
(ver.4.1.8Demo)

It is a composition of...

- Open-source UML model editor
  - xtUML Modeling Language (UML profile)
- a verifier (providing simulated execution capability)
  - Model debug
  - Animated features during model execution (simulation)

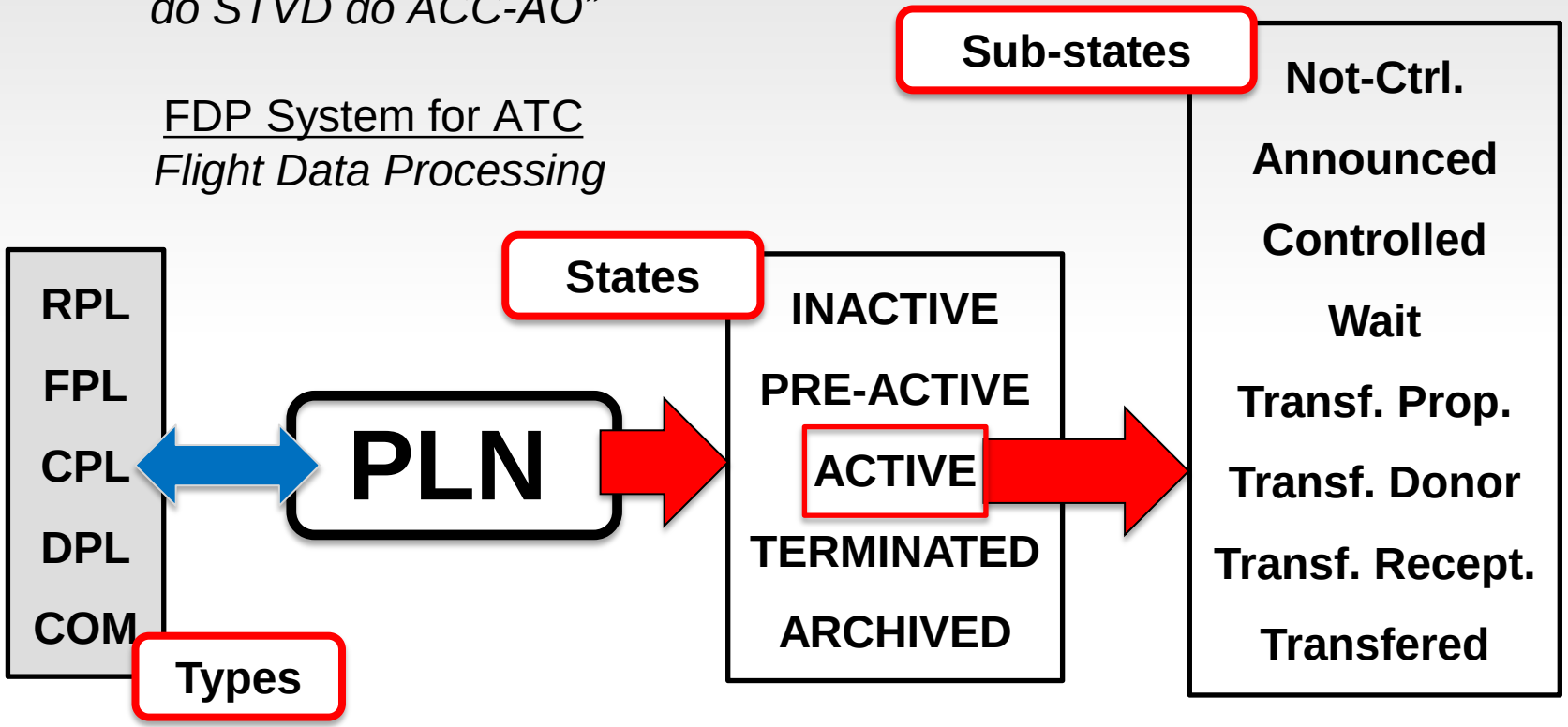
    providing early model verification
  - allows integration with external code
- set of model compilers (providing translation)

Code generation functionality into C, C++, System C, Java

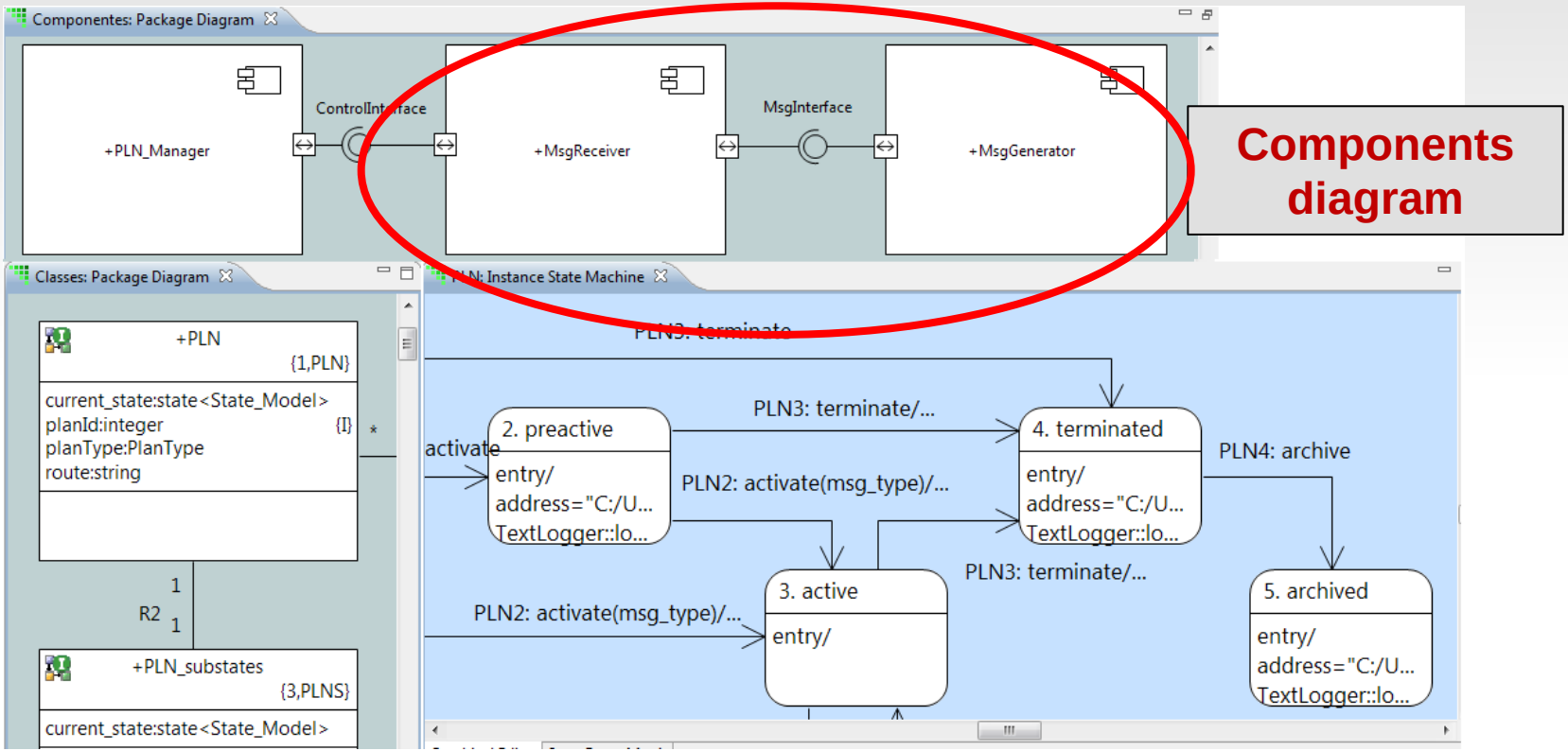
Mentor Graphics®

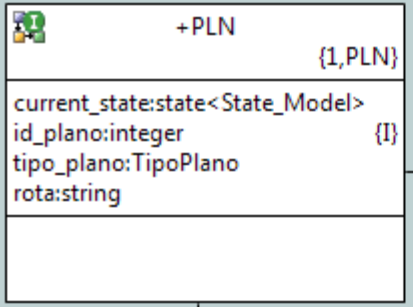
“*Especificação de Requisitos de Sistema do STVD do ACC-AO*”

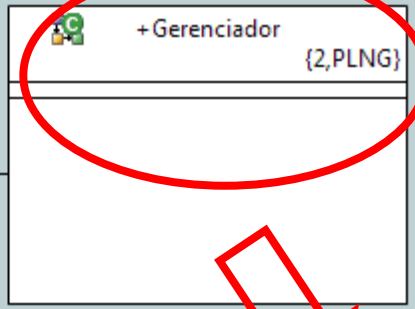
FDP System for ATC
Flight Data Processing



Modeling Tools - BridgePoint

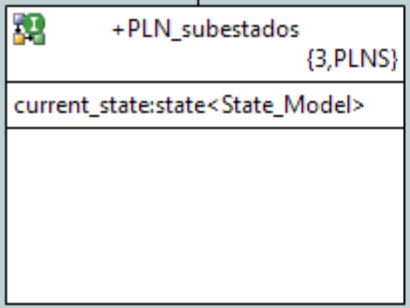




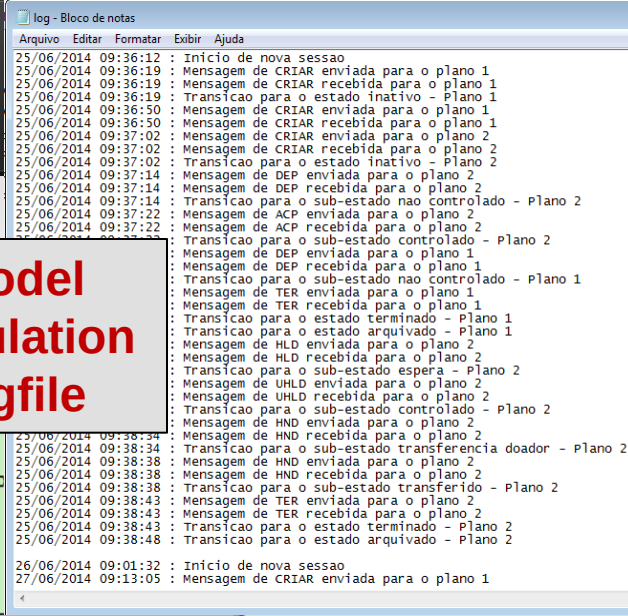


R1 * 1

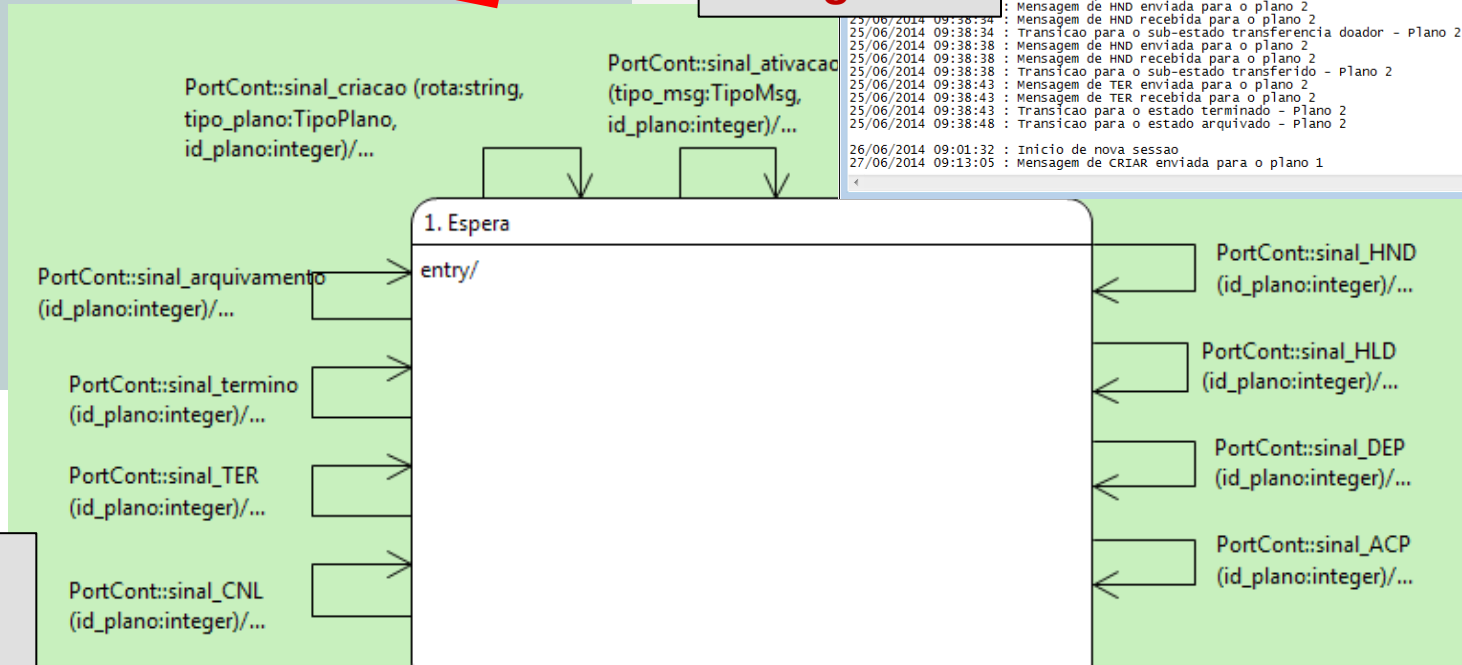
R2 1 1



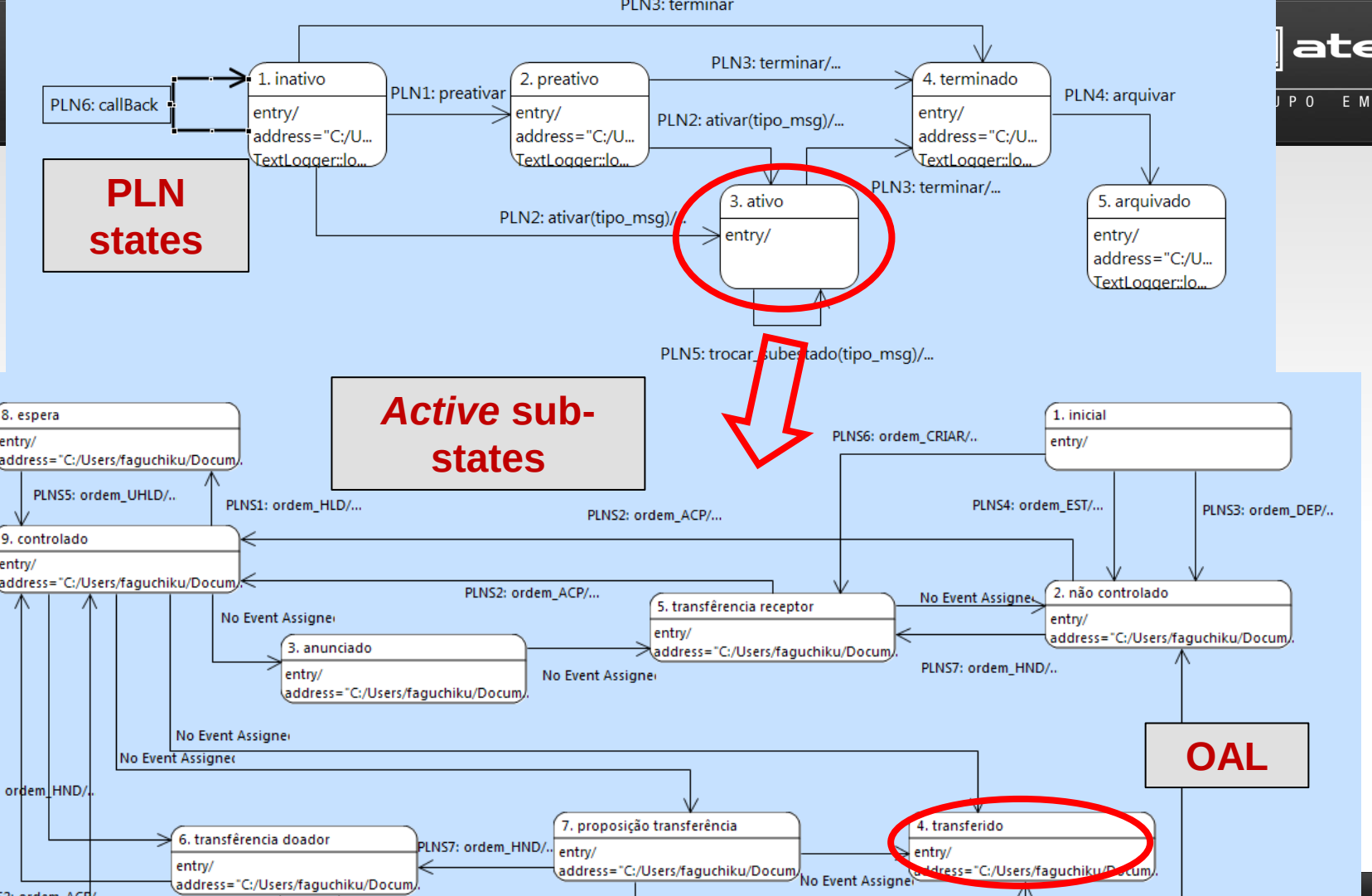
Class diagram



Model simulation logfile



Gerenciador **State-Machine**


PLN3: terminar
PLN6: callBack
1. inativo
entry/
address="C:/U...
TextLogger::lo...
PLN1: preativar
2. preativo
entry/
address="C:/U...
TextLogger::lo...
PLN3: terminar/...
4. terminado
entry/
address="C:/U...
TextLogger::lo...
PLN4: arquivar
PLN2: ativar(tipo_msg)/...
PLN3: terminar/...
PLN2: ativar(tipo_msg)/...
3. ativo
entry/
5. arquivado
entry/
address="C:/U...
TextLogger::lo...
PLN5: trocar_substado(tipo_msg)/...
PLN states
Active sub-states
8. espera
entry/
address="C:/Users/faguchiku/Docum...
PLNS5: ordem_UHLD/..
PLNS1: ordem_HLD/...
PLNS2: ordem_ACP/...
PLNS6: ordem_CRIAR/..
1. inicial
entry/
PLNS4: ordem_EST/...
PLNS3: ordem_DEP/..
9. controlado
entry/
address="C:/Users/faguchiku/Docum...
PLNS2: ordem_ACP/...
No Event Assigne
5. transferência receptor
entry/
address="C:/Users/faguchiku/Docum...
No Event Assigne
2. não controlado
entry/
address="C:/Users/faguchiku/Docum...
3. anunciado
entry/
address="C:/Users/faguchiku/Docum...
No Event Assigne
PLNS7: ordem_HND/..
No Event Assigne
No Event Assigne
OAL
PLNS7: ordem_HND/..
6. transferência doador
entry/
address="C:/Users/faguchiku/Docum...
PLNS7: ordem_HND/..
7. proposição transferência
entry/
address="C:/Users/faguchiku/Docum...
4. transferido
entry/
No Event Assigne

BridgePoint – *The benchmark problem*

atech
GRUPO EMBRAER

Achievements:

- Data structure was devised to emulate many instances of flights
- Verifier functionality tested (*Model Debbuger*)
- Testing: automatic and man-in-the-loop
- Logging Interface (Java *External Entities*)
- User Interface (Java *Realized Component*)
- Code Generation (compiled & tested)

Formal Specification

Specification of a system properties, using a language defined by mathematical logic

- Improve system reliability
- Based on:
  - process algebra,
  - first order logic,
  - temporal logic,
  - set theory...
- Each language represents a view of the system – languages are complementary
- Formal Verification

Formal Verification

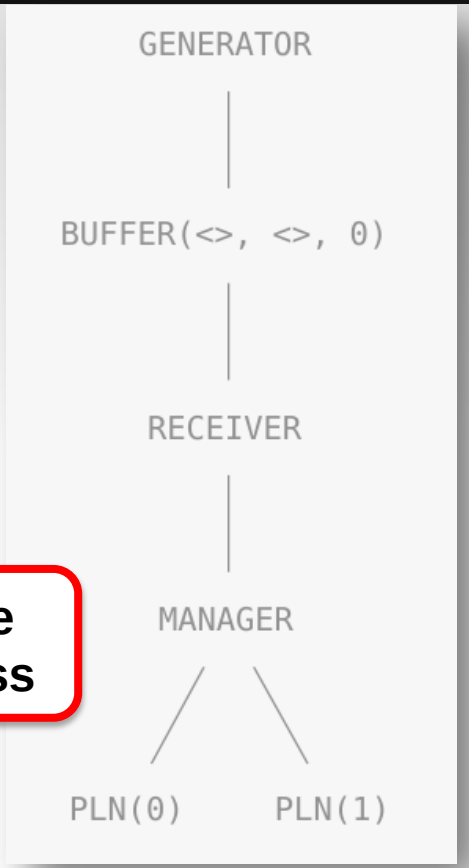
Communicating Sequential Process (CSP) – process algebra:
Description of programs or processes that communicate events, from a set, within an environment

FDR3 - Failures Divergence Refinement (a refinement checker)

Constructing equivalent refinement checks (models)
- traces
- failures
- failures-divergences

Properties
- **deadlock-freedom**
- livelock-freedom
- Determinism

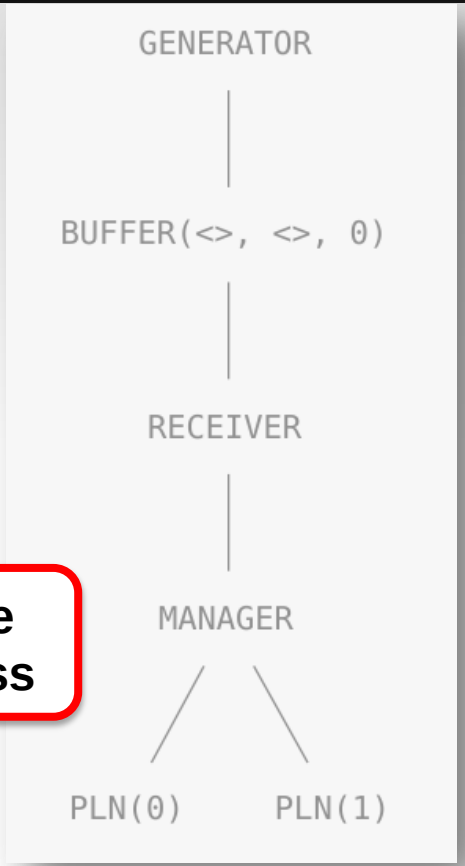
Single Process



Formal Verification

State Explosion Problem:

- Two Flight Plan processes;
- Three Buffer messages;



Single Process

Formal Verification

AutoFocus3

Funcionality:

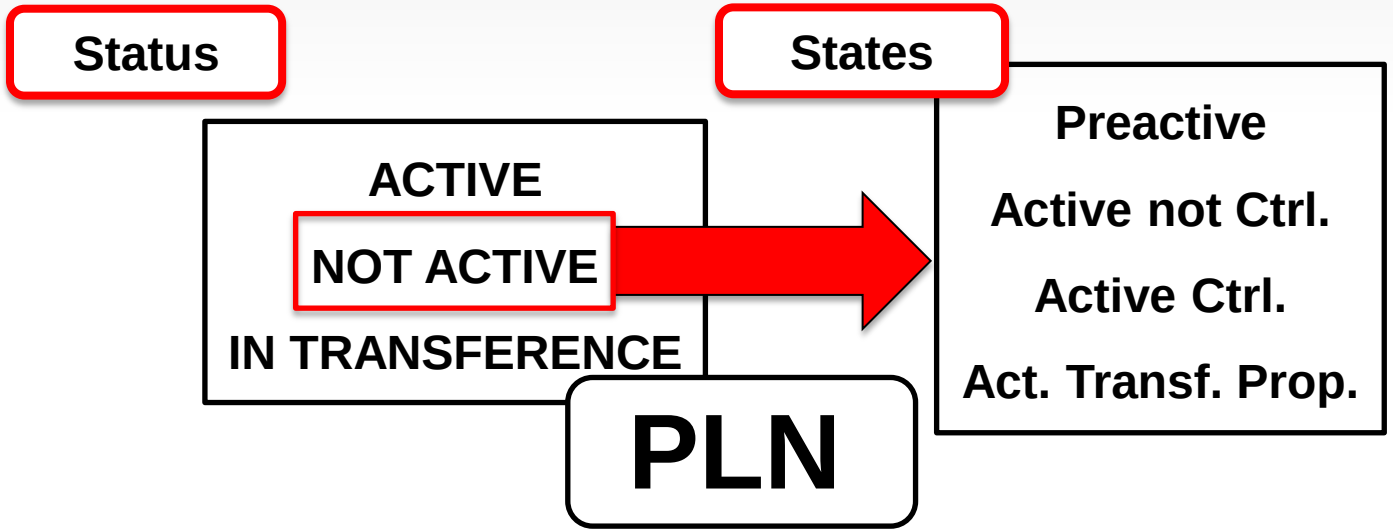
- Requirements Engineering
- Modeling and Simulation
- Code Generation
- Deployment
- Testing
- Formal Verification – NuSMV
    - Model Checking CTL/LTL property

Case Study

FDP System for ATC

Flight Data Processing

- Transferal of a flight plan from one ATC to another

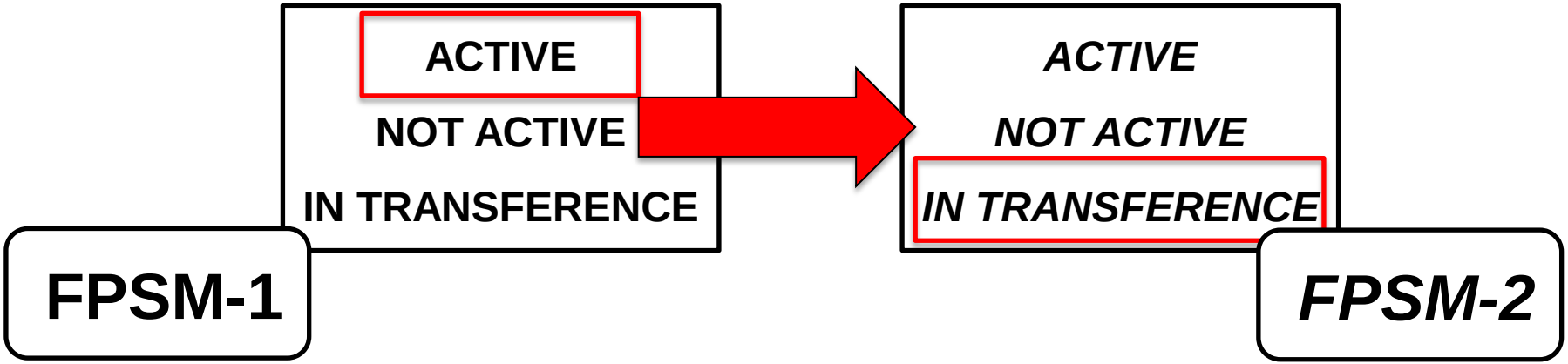


Case Study

FDP System for ATC

Flight Data Processing

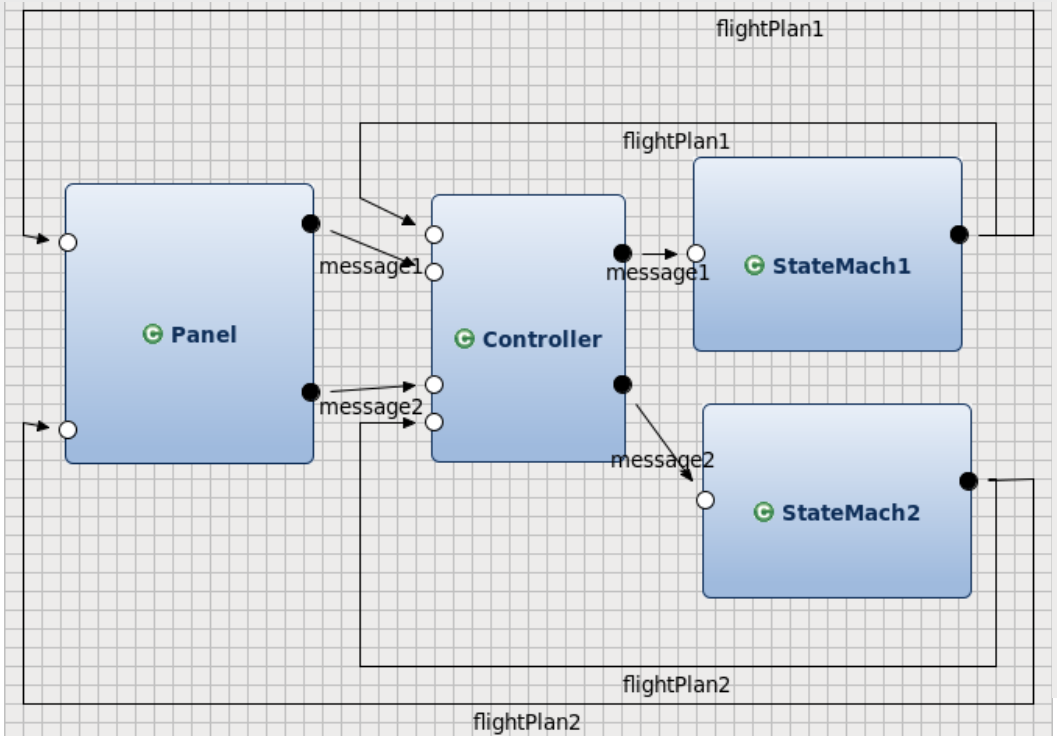
- Safety properties:
  - Active x *Active*
  - Active - *In Transference* to Not Active – *Active*

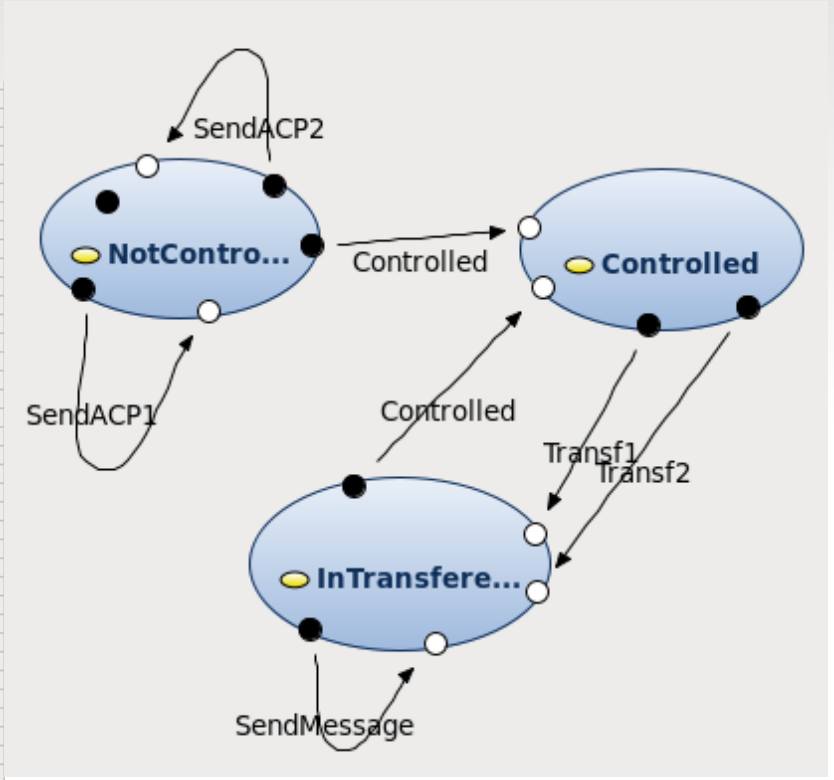


Formal Verification

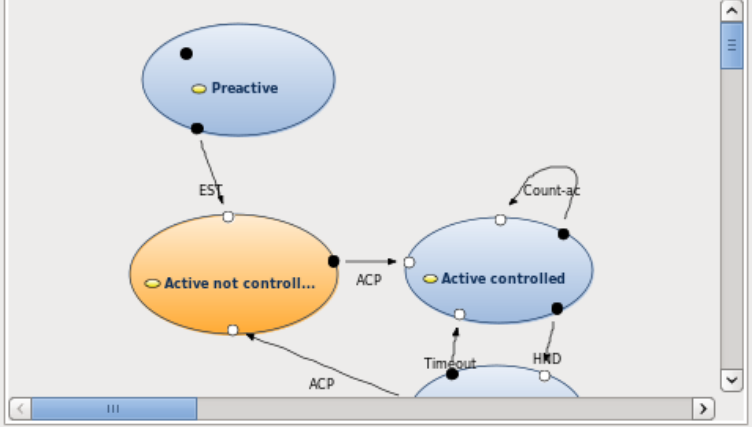
atech
GRUPO EMBRAER

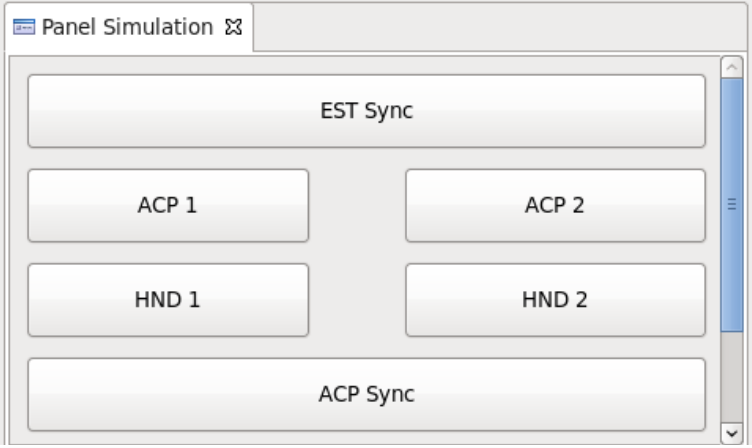
AutoFocus3

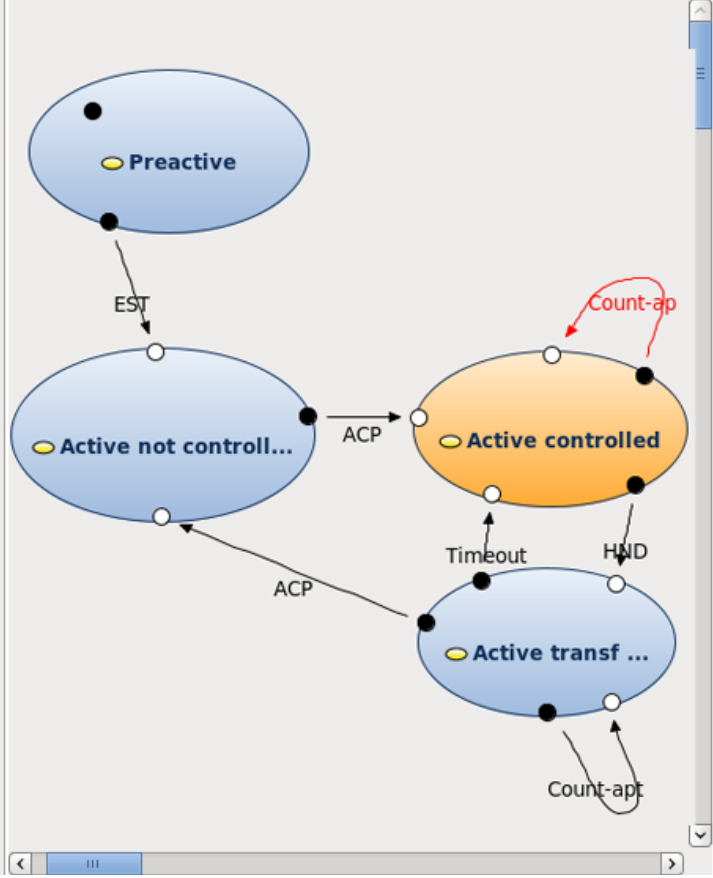




AutoFocus3
– NuSMV







Specification Atom	Verification c	Last check date	Last check result
Property 'flightPlanIn1 == Controlled( ) && flightPlar	Arch_v1	Wed Aug 26 11:25	SUCCESS
If '((flightPlanIn1 == Controlled( ) && flightPlanIn2 =	Arch_v1	Wed Aug 26 11:26	SUCCESS

MDD Issues

atech
GRUPO EMBRAER

"Some companies have reported great success with it, whereas others have failed horribly"
(Whittle, Hutchinson, Rouncefield 2014)

Issues related to MDD:

- UML – Abstraction level
- UML 2.0 – low acceptance
- Code generation

"*8 Reasons Why Model-Driven Approaches (will) Fail*" (DenHaan, 2008; 2009)

"*Model Driven Development Misperceptions and Challenges*" (Portier, Ackerman, 2009)

Conclusion

Gain from MDD:

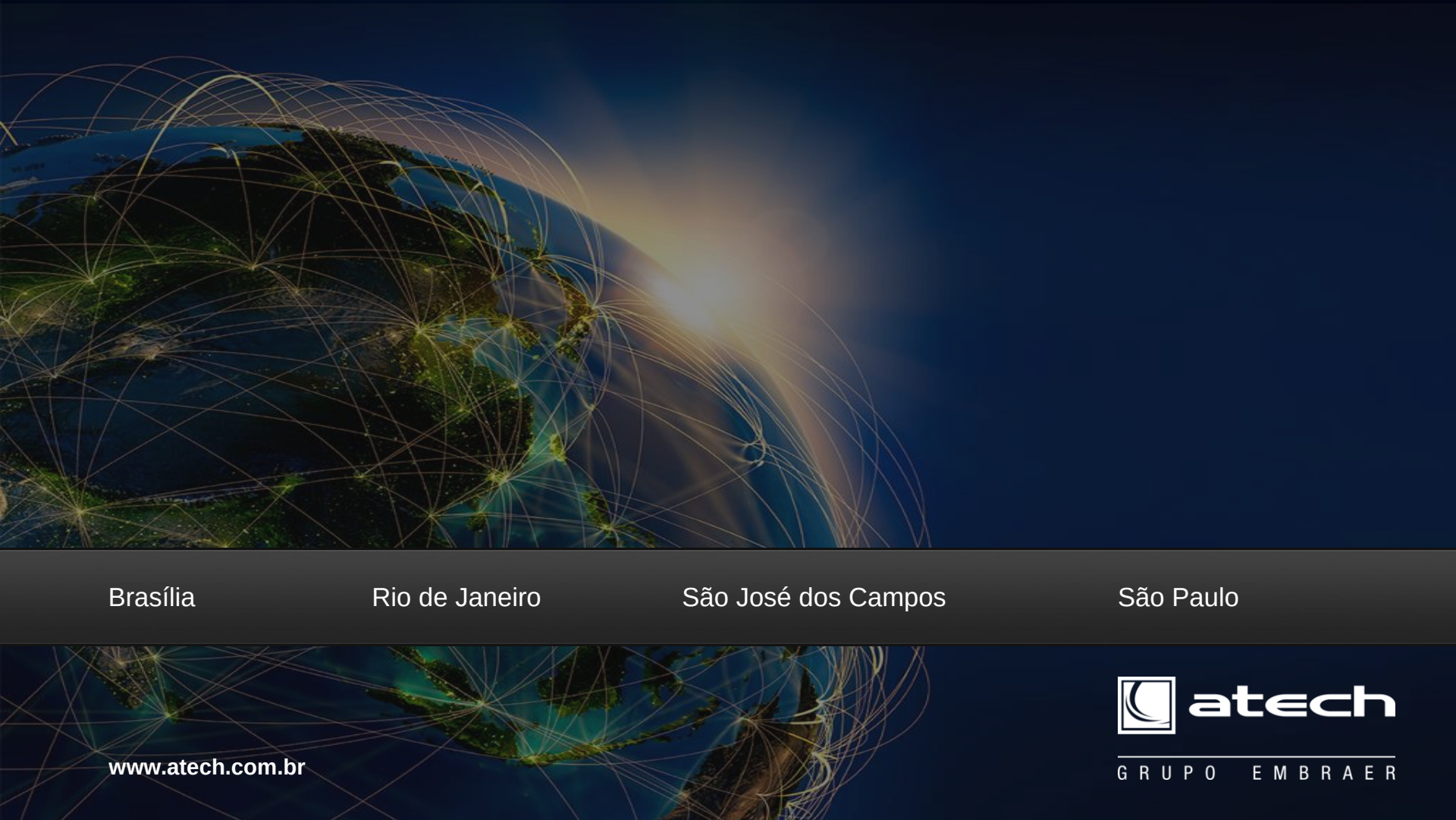
- Reuse
- Documentation
- Maintenance

Verification:

- Mapping of methods, modeling tools
- Model execution (simulation, debugging)
- Formal verification – model checking
  - Model refinement

“However, used in moderation and where appropriate, UML and MDA code generators are useful tools, although not the panaceas that some would have us believe”

(Thomas, 2004)



Brasília Rio de Janeiro São José dos Campos São Paulo

www.atech.com.br

atech

GRUPO EMBRAER