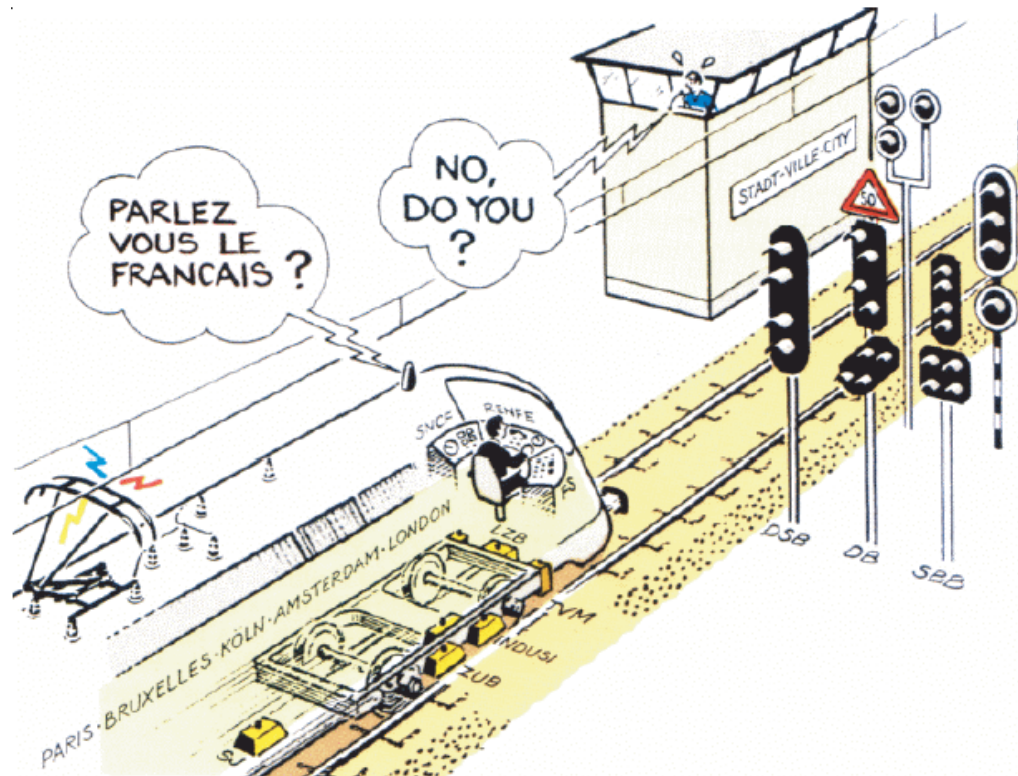
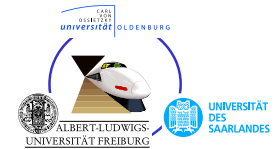


# Projektgruppe «Syspect»

M. Möller, E.-R. Olderog, A. Schäfer

Abteilung **Entwicklung korrekter Systeme**

- SFB AVACS
- Fallstudien zur Sicherheit des Bahnverkehrs



## ► Motivation

Heute  
PG-Ziel  
Angebot

- SFB AVACS
- Fallstudien zur Sicherheit des Bahnverkehrs
- **Formale Spezifikation**  
mit den Aspekten **Kommunikation, Daten und Zeit**



# Bisherige Situation

- CSP-OZ-DC
  - Kommunikation: **CSP**
  - Daten: **Object-Z**
  - Zeit: **Duration Calculus**
- Praxis: **UML**
- Brückenschlag
  - **UML-Profil** für CSP-OZ (Projekt ForMooS)

# Bisherige Situation

*ATM*

method *setup* : [*par?* : *PAR*]

method *insert* : [*id?* : *ID*]

chan *ident* : [*tid!* : {*self*}]

...

*main* = *ident* → *setup* → *LOOP*

*LOOP* = *insert* → *pin* → *auth* →  
(*eject* → *LOOP* □ ...)

*id* : *ID*

*pin* : *PIN*

*amount* :  $\mathbb{Z}$

*retcard* :  $\mathbb{B}$

*Init*

$\neg$ *retcard*

...

```
\begin{class}{ATM}
  \method\ setup : \lsch par? : PAR \rsch
  \method\ insert : \lsch id? : ID \rsch
  \chan\ ident : \lsch tid! : {\self}
```

...

```
\begin{array}{rcl}
  \main & = & \& ident \to setup \to LOOP
  LOOP & = & \& insert \to pin \to auth \to
  & \& \big( eject \to LOOP \text{extchoice
```

```
\end{array} \\
\begin{state}
```

```
  id : ID \\
```

```
  pin : PIN \\
```

```
  amount : \integer \\
```

```
  retcard : \bool
```

```
\end{state} \\
\begin{init}
```

```
  \neg retcard
```

```
\end{init} \\
...
```

```
\end{class}
```

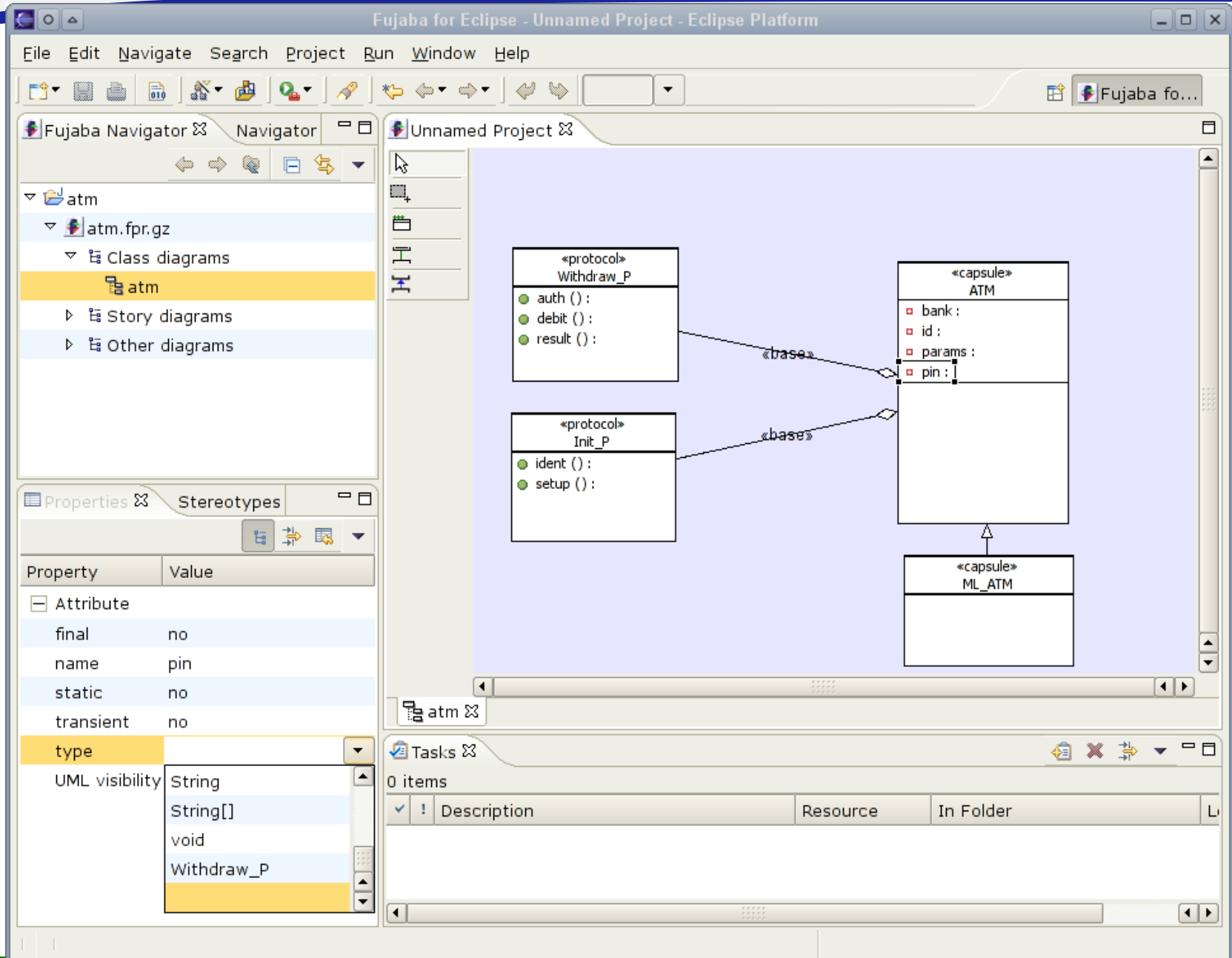
```
%
```

# Ziel der PG «Syspect»

## «Syspect» – **Sy**stem **Spec**ification **T**ool

- Eine **grafische Entwicklungsumgebung** für eine **formale UML-Teilsprache**
- UML-Profil für CSP-OZ-DC
- Visuelle Eingabe (insbesondere Object-Z)
- Integration existierender **Verifikationstools**

# Ziel der PG «Syspect»

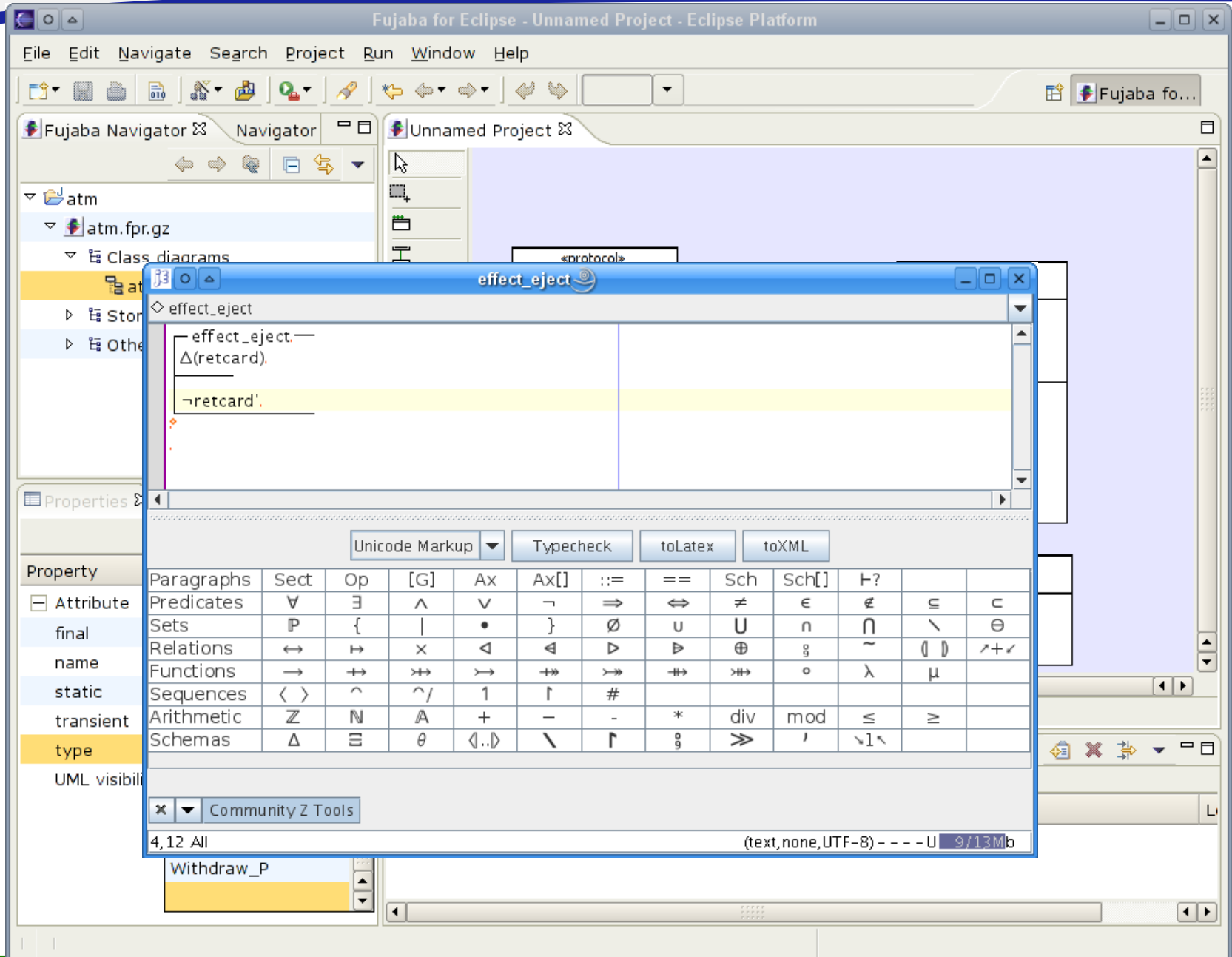


The screenshot shows the Fujaba IDE interface with the following components:

- Navigator:** Shows a project structure with 'atm.fpr.gz' containing 'Class diagrams' and 'atm'.
- Properties - Stereotypes:** A table showing properties for the selected element:
 

Property	Value
final	no
name	pin
static	no
transient	no
type	Withdraw_P
UML visibility	String
- UML Class Diagram:**
  - Withdraw\_P** (protocol): Methods: auth(), debit(), result().
  - Init\_P** (protocol): Methods: ident(), setup().
  - ATM** (capsule): Attributes: bank, id, params, pin.
  - ML\_ATM** (capsule): Inherits from ATM.
  - Relationships: Withdraw\_P and Init\_P are shown as base protocols for ATM (indicated by dashed arrows with open arrowheads and the stereotype «base»).
- Tasks:** Shows 0 items in a table with columns: Description, Resource, In Folder.

# Ziel der PG «Syspect»



The screenshot shows the Eclipse IDE interface. The Fujaba Navigator on the left displays a project structure with folders like 'atm', 'atm.fpr.gz', 'Class diagrams', 'Storage', and 'Other'. The main editor shows a code snippet for 'effect\_eject' with the following content:

```

effect_eject
Δ(retcard)
- retcard!

```

Below the code editor is a Properties window with a table of symbols. The table has columns for various symbols and their corresponding mathematical or logical notations. The 'type' property is highlighted in the Properties window.

Property	Paragraphs	Sect	Op	[G]	Ax	Ax[]	::=	==	Sch	Sch[]	F?		
Attribute	Predicates	$\forall$	$\exists$	$\wedge$	$\vee$	$\neg$	$\Rightarrow$	$\Leftrightarrow$	$\neq$	$\in$	$\notin$	$\subseteq$	$\supseteq$
final	Sets	$\mathbb{P}$	$\{$	$ $	$\cdot$	$\}$	$\emptyset$	$\cup$	$\cap$	$\setminus$	$\ominus$	$\oplus$	$\otimes$
name	Relations	$\leftrightarrow$	$\rightarrow$	$\times$	$\triangleleft$	$\triangleleft$	$\triangleright$	$\triangleright$	$\oplus$	$\otimes$	$\sim$	$( )$	$\wedge$
static	Functions	$\rightarrow$	$\leftrightarrow$	$\leftrightarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\lambda$	$\mathbb{F}$	$\mathbb{F}$
transient	Sequences	$\langle \rangle$	$\wedge$	$\wedge$	$1$	$\uparrow$	$\#$						
type	Arithmetic	$\mathbb{Z}$	$\mathbb{N}$	$\mathbb{A}$	$+$	$-$	$-$	$*$	div	mod	$\leq$	$\geq$	
UML visible	Schemas	$\Delta$	$\exists$	$\theta$	$\langle \dots \rangle$	$\setminus$	$\uparrow$	$\otimes$	$\Rightarrow$	$'$	$\setminus$	$\setminus$	

At the bottom of the Properties window, there is a 'Community Z Tools' section with a list of tools including 'Withdraw\_P'.

# ...was wir bieten

- ▣➔ Speziell bei «**Syspect**»
  - ▣➔ Erfahrungen im Umgang mit **UML**
  - ▣➔ **Formale Spezifikationen**  
(mit Kommunikation, Daten und Zeit)
  - ▣➔ Einblick in **aktuelle Forschung** (SFB AVACS)
  - ▣➔ Fallstudien zu Realzeitsystemen
  - ▣➔ Themengebiete für Diplomarbeiten oder individuelle Projekte

# ...was wir bieten

- Speziell bei «**Syspect**»
  - Erfahrungen im Umgang mit **UML**
  - **Formale Spezifikationen**  
(mit Kommunikation, Daten und Zeit)
  - Einblick in **aktuelle Forschung** (SFB AVACS)
  - ...
- Allgemein in PGs
  - Softwareentwicklung im Team  
(Versionsverwaltung, Absprachen, ...)
  - Wiederverwendung vorhandener Komponenten
  - „kundenorientierte“ Entwicklung (hier: AVACS R1)

# ...was wir bieten

- ▶▶▶ Speziell bei «**Syspect**»
  - ▶▶ Erfahrungen im Umgang mit **UML**
  - ▶▶ **Formale Spezifikationen**  
(mit Kommunikation, Daten und Zeit)
  - ▶▶ Einblick in **aktuelle Forschung** (SFB AVACS)
  - ▶▶ ...
- ▶▶▶ Allgemein in PGs ...

Alle Informationen und weitere Details:

<http://syspect.informatik.uni-oldenburg.de/>