Eclipse Tools Day 2019

# An Eclipse tool to mix DS(M)Ls and formal reasoning

**Akram Idani**

(Univ. Grenoble Alpes – LIG )

# Introduction



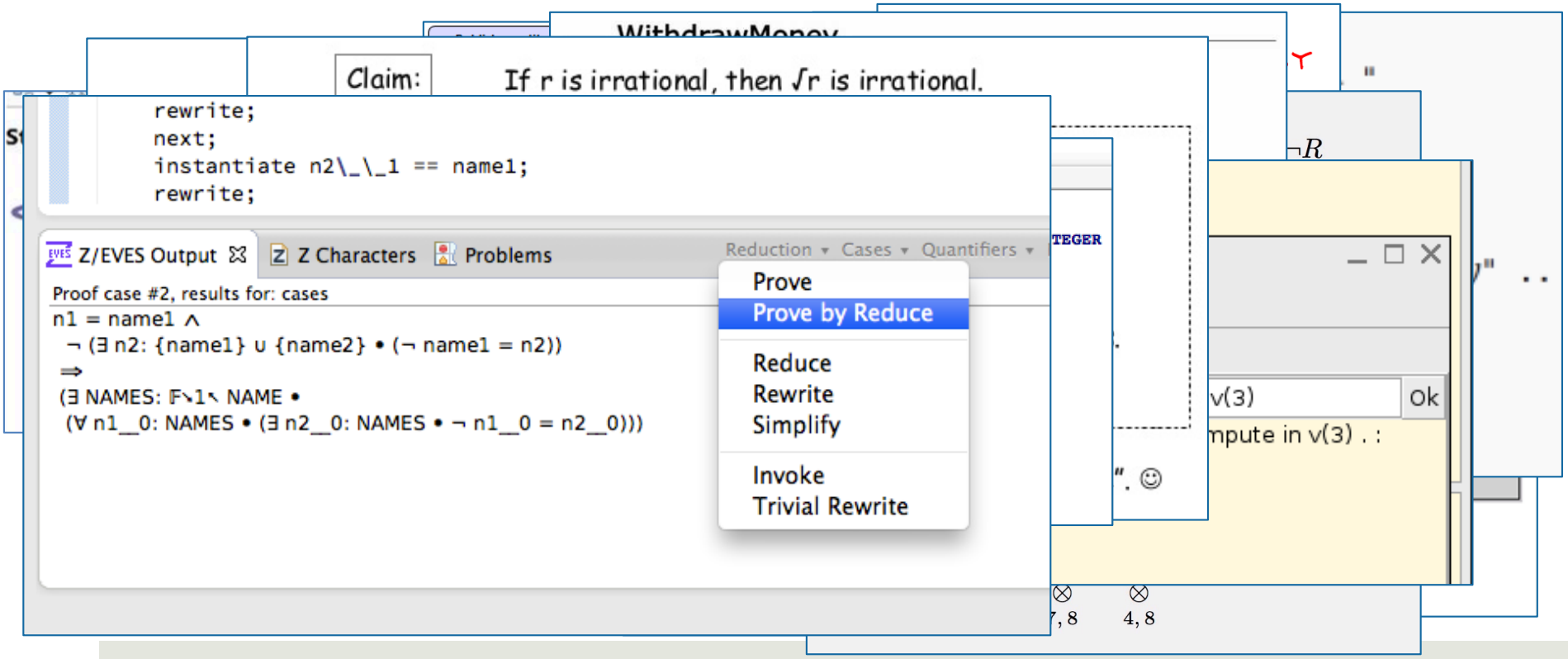
Meeduse

- MDE
  - Communication
  - Standard

Proofs / Refinements

End User needs

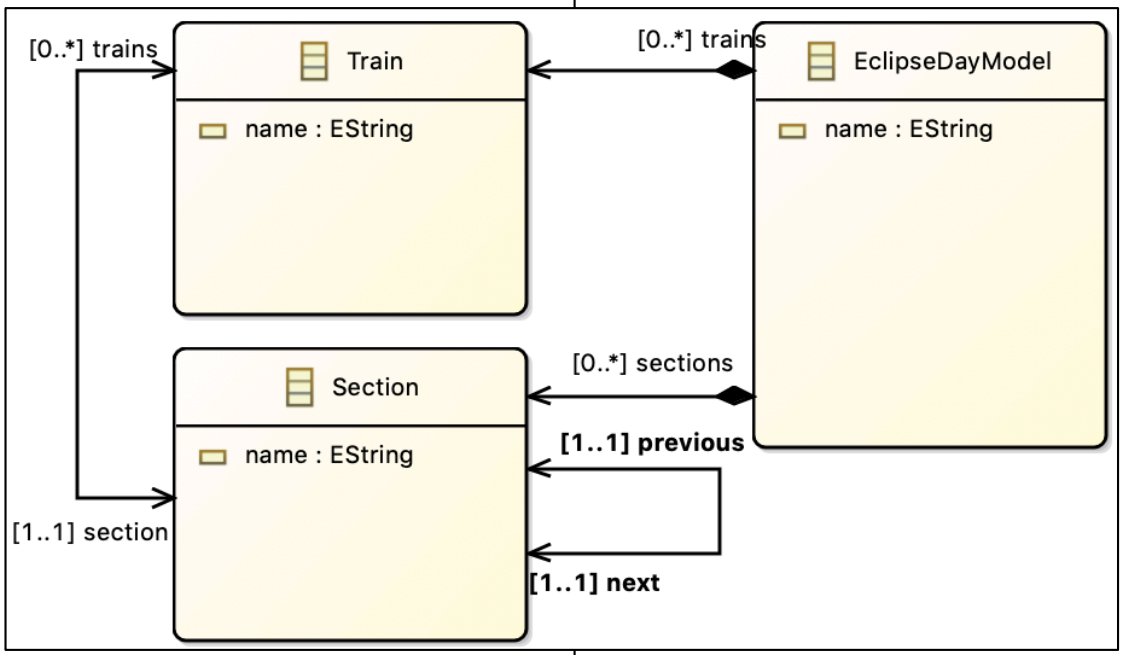
- FM
  - Automated reasoning
  - Safety-critical systems



# A DSL example



```
1  grammar org.xtext.Eclipseday
2      with org.eclipse.xtext.common.Terminals
3  generate eclipseday
4      "http://www.xtext.org/Eclipseday"
5
6  EclipseDayModel:
7      name=ID
8      (sections+=Section)*
9      (trains+=Train)*
10     ;
11
12 Section:
13     name=ID '->'
14     next=[Section] '/'
15     (trains+=[Train])* '-';
16
17 Train : name=ID;
```



# Formal static semantics



- Meeduse automatically extracts a proved formal B specification from the ecore file

```
MACHINE
        eclipseday

SETS
        ECLIPSEDAYMODEL;
        SECTION;
        TRAIN

ABSTRACT_VARIABLES
        EclipseDayModel,
        Section,
        Train,
        connection,
        position,
        A_trains_eclipseDayModel,
        A_sections_eclipseDayModel

INVARIANT
        EclipseDayModel : FIN(ECLIPSEDAYMODEL) &
        Section : FIN(SECTION) &
        Train : FIN(TRAIN) &
        connection : Section >->> Section &
        position : Train --> Section &
        A_trains_eclipseDayModel : Train +-> EclipseDayModel &
        A_sections_eclipseDayModel : Section +-> EclipseDayModel
```

# Formal dynamic semantics



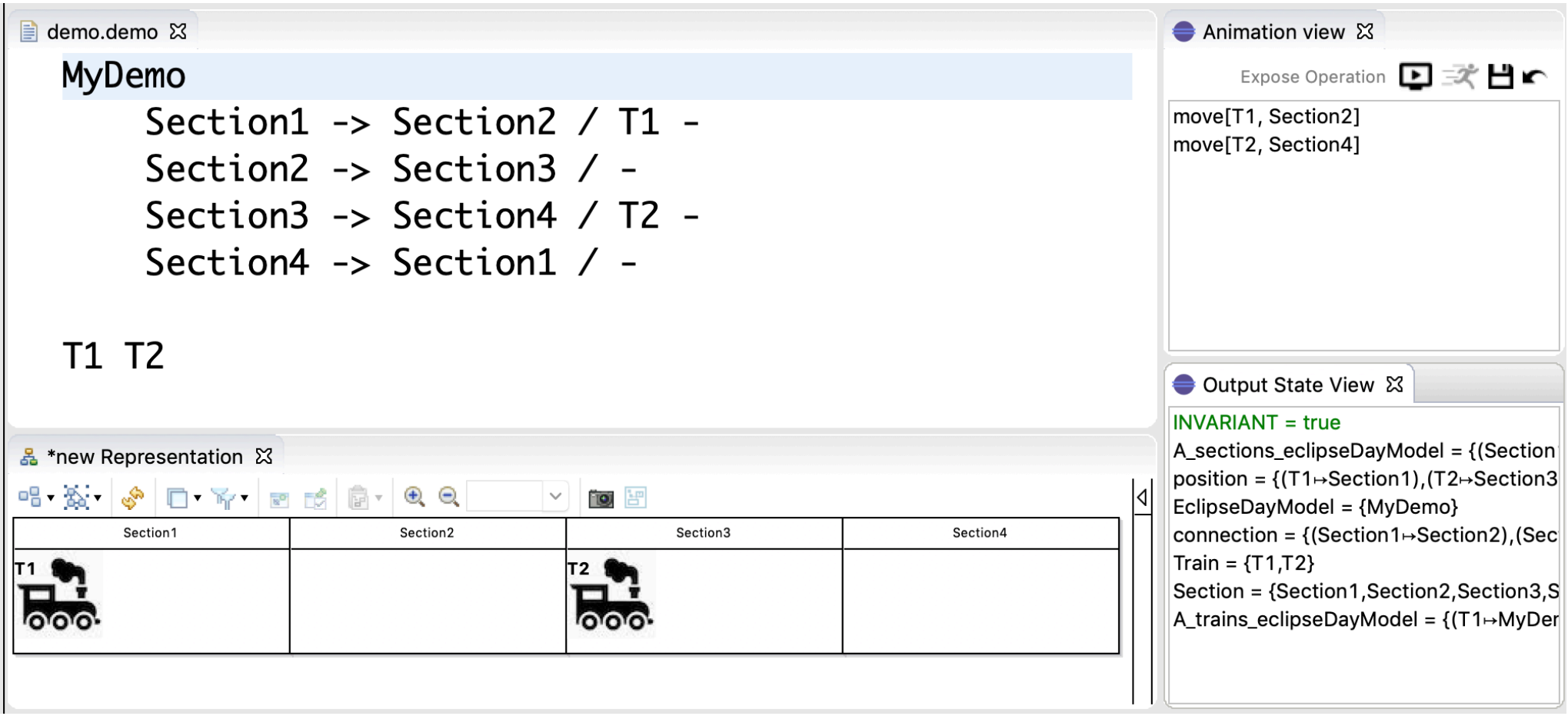
- Meeduse allows to integrate within the EMF package dynamic specification written in the B language

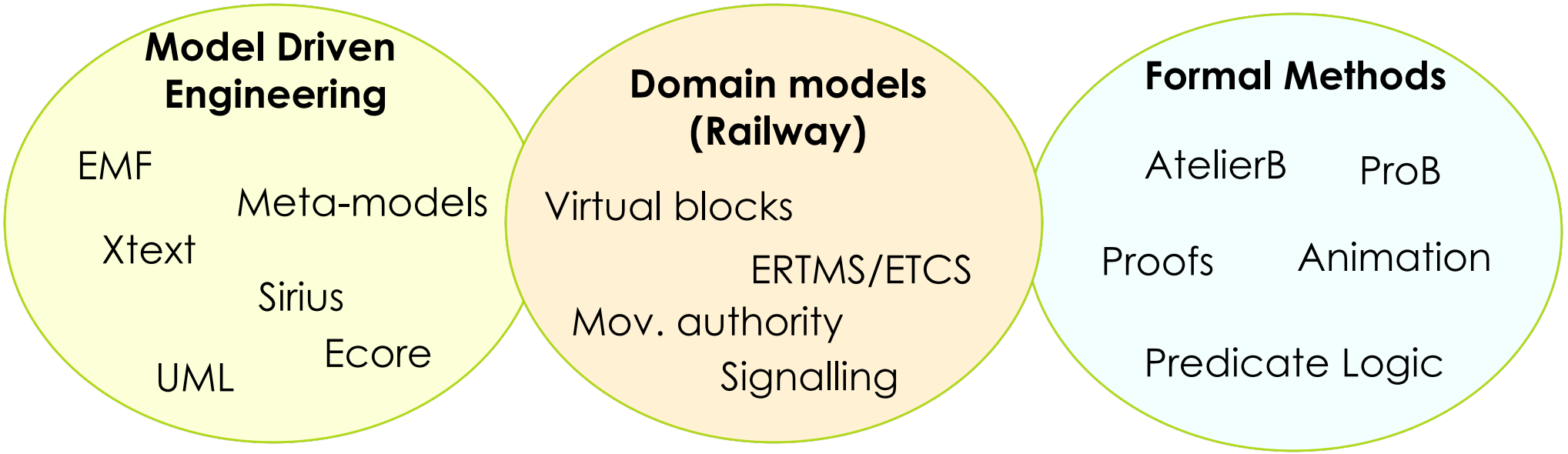
```
MACHINE
        eclipsedaymain
INCLUDES
        eclipseday
INVARIANT
        position : Train >-> Section
OPERATIONS
move(tt,ss) =
        PRE
                tt : Train &
                ss : Section &
                connection(position(tt)) = ss &
                {(tt |-> ss)} /<: position &
                ss /: ran(position)
        THEN
                Train_SetSection(tt,ss)
        END
END
```

# DSL Animation



- Given a model (written in EMF-based tools, like Xtext) Meeduse allows to animate its dynamic semantics.






- Meedsue for MDE
  - Award for **best verification**, and Third audience award in the 12th Transformation tool contest (TTC'19)
- Meeduse for Railway
  - Akram Idani, et al., Towards a Tool-Based Domain Specific Approach for Railway Systems Modeling and Validation. 3rd International conference on Reliability, Safety, and Security of Railway Systems. **RSSRail 2019**.
- Meeduse for FM
  - Akram Idani, et al., Incremental Development of a Safety Critical System Combining formal Methods and DSMLs - Application to a Railway System. 24th International Conference on Formal Methods for Industrial Critical Systems. **FMICS 2019.**