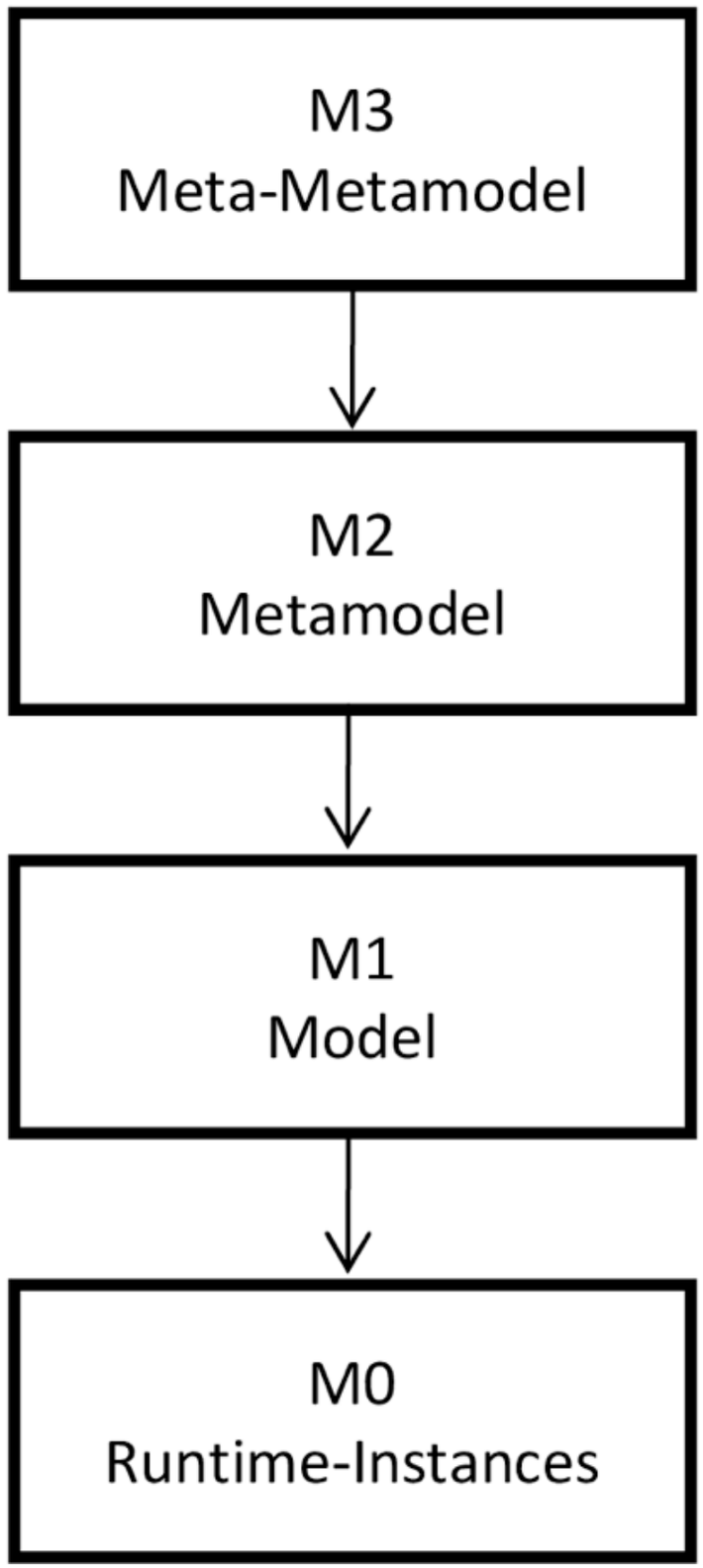
An openETCS DSL Based on GOPPRR

Jan Peleska, Johannes Feuser, and Cécile Braunstein
University of Bremen
2014-04-14

The Approach

How DSL are constructed



Rules for meta-model design

Syntax and static semantics for specific modeling formalism *F*

Concrete model *M* developed using formalism *F*

Executable code generated from *M* and deployed on target hardware

The Approach

An openETCS DSL based on GOPPRR

The GOPPRR meta-metamodel has been elaborated for the purpose of designing graphical domain-specific languages expressed by the "ingredients"

- **G**raphs – where model fragments are presented
- **O**bjects – the individual language element types
- **P**roperties – attributes associated with each type
- **P**orts – connection points "objects ⇿ roles"
- **R**oles – meaning of "relationship ⇿ object" connection
- **R**elationships – between objects on a graph

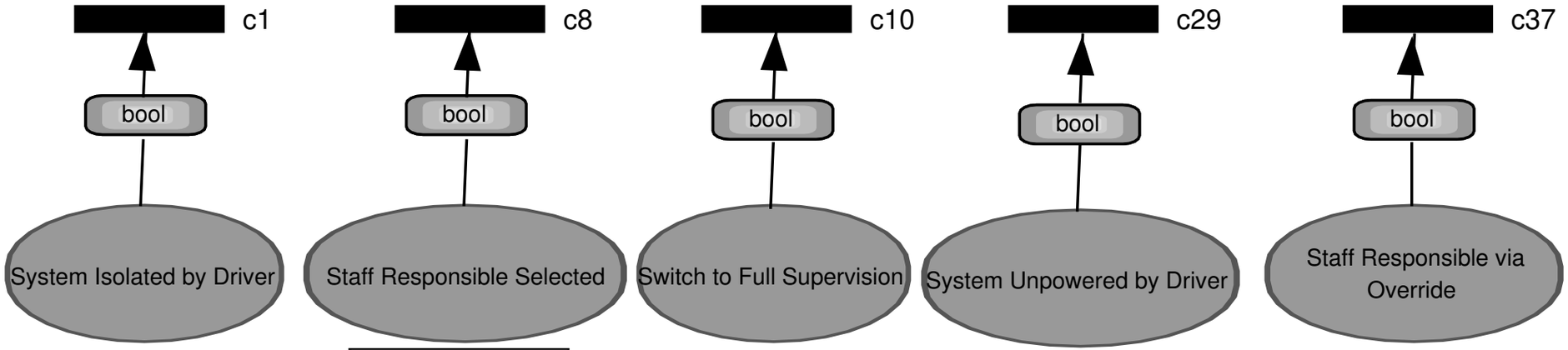
Benchmark Report

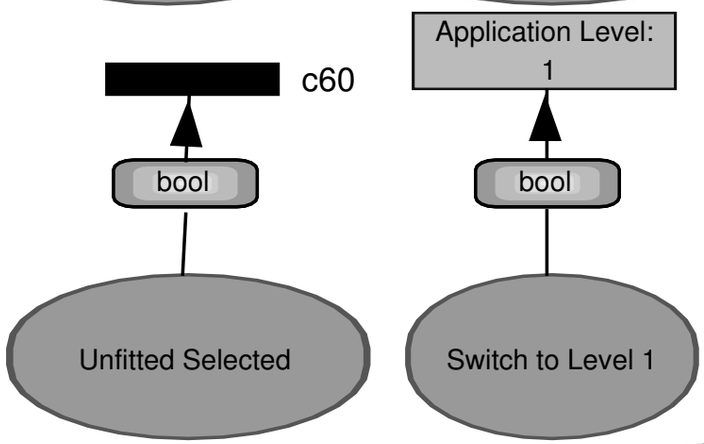
- Formal model of ERTMS Subset 026
  - Levels 0 and 1
  - Modes
    - No Power (NP)
    - Stand By (SB)
    - System Failure (SF)
    - Isolation (IS)
    - Trip (TR)
    - Post Trip (PT)
    - Unfitted (UN)
    - Staff Responsible (SR)
    - Full Supervision (FS)

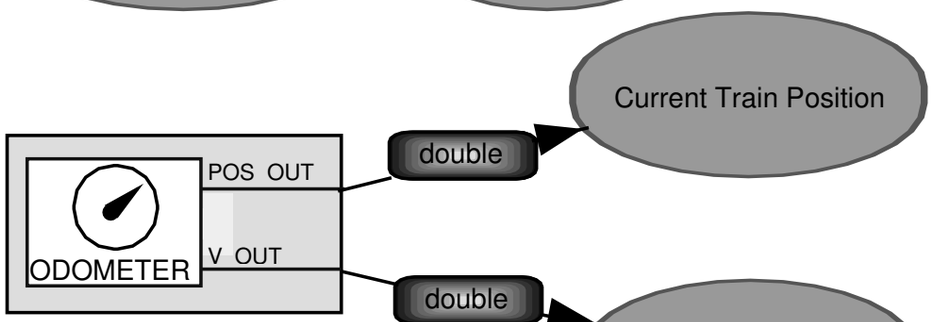
Language Elements (1). Matrix representation for ERTMS modes and transition in-between

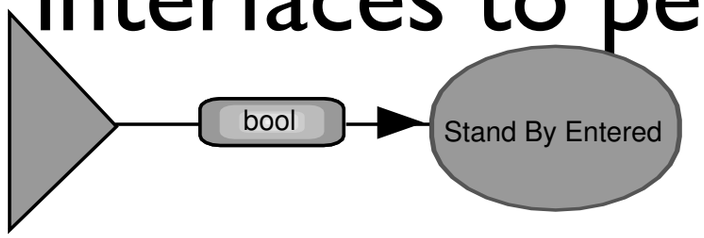
	No Power (INITIAL)	Stand By	Full Supervision	Staff Responsible	Unfitted	Trip
No Power (INITIAL)		c4-p2				
Stand By	c29-p2		c10-p7	c37-p7, c8-p7	c60-p7	
Full Supervision	c29-p2	c28-p5		c37-p6	c21-p6	c12-p4, c16-p4, c1
Staff Responsible	c29-p2	c28-p5	c31-p6, c32-p6		c21-p6	c18-p4, c20-p4, c3
Unfitted	c29-p2	c28-p6	c25-p7	c44-p4		c39-p5, c67-p5
Trip	c29-p2				c62-p3	
Post Trip	c29-p2		c31-p4	c37-p4, c8-p4		
System Failure	c29-p2					
Isolation						

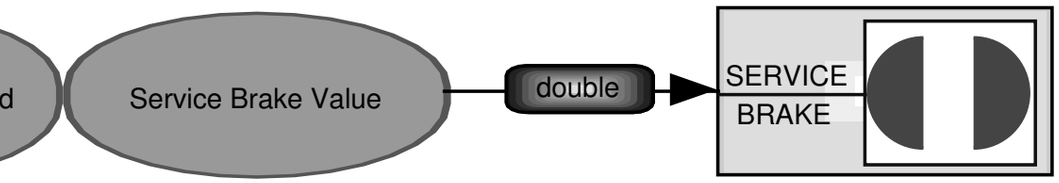
Language Elements (2). Data flow language, guards for mode transitions, pre-defined interfaces to peripherals

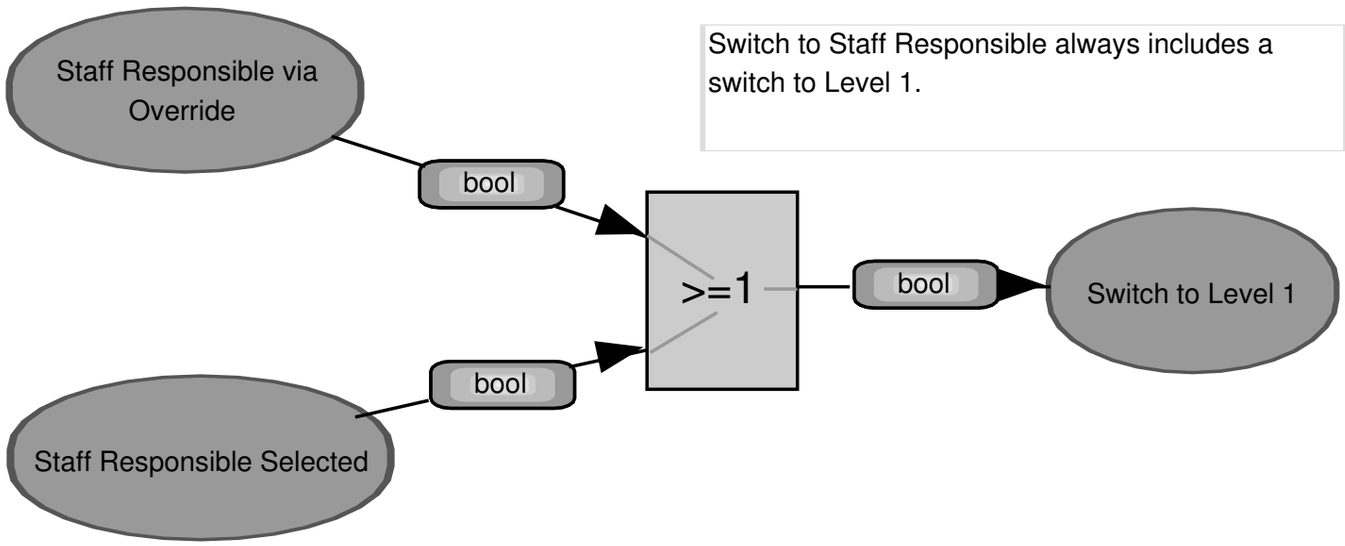












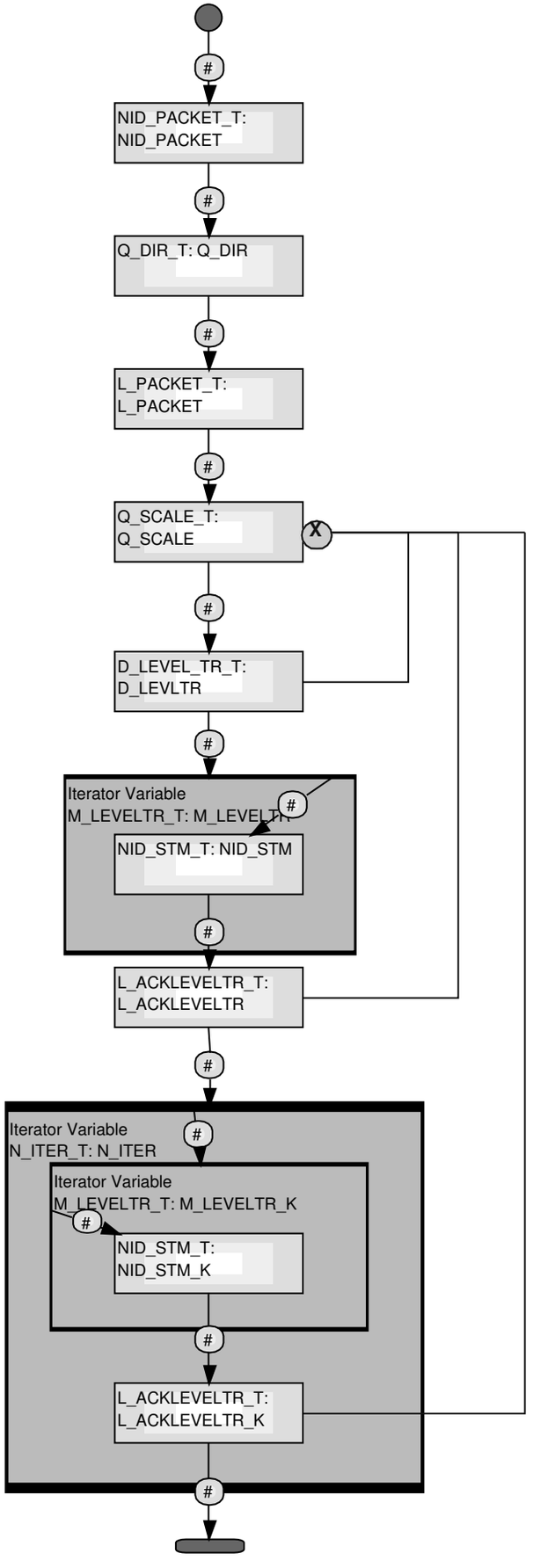
Switch to Staff Responsible always includes a switch to Level 1.

Sub-Function:
DMI Stand By

Sub-Function:
Stand Still Supervision

Sub-Function:
Start Of Mission in Stand By

Language Elements (3). Graphical sub-language for telegram representation



Benchmark Report (cont.)

Details in

1. **Jan Peleska, Johannes Feuser, and Anne E. Haxthausen.** *The Model-Driven openETCS Paradigm for Secure, Safe and Certifiable Train Control Systems.* **In Flammini, Francesco (ed.).** *Railway Safety, Reliability, and Security: Technologies and Systems Engineering.* **IGI Global, 2012. pp. 22-52. Web. 4 Jun. 2012. doi:10.4018/978-1-4666-1643-1**

2. **Johannes Feuser.** *Open Source Software for Train Control Applications and its Architectural Implications.* **Dissertation, University of Bremen, February 2013. Available under http://elib.suub.uni-bremen.de/edocs/00103095-1.pdf**

Results of Benchmark

- **Pros**
  - Formal model – yet quite intuitive for ERTMS domain experts
  - Full tool chain support possible – prototype tool chain already available
    - Code generator
    - Unit tester with assertion checker for static semantics
    - Simulator
    - Model-based testing with RT-Tester

Results of Benchmark

- **Cons**
  - Unanimous adoption of DSL in such a large project as openETCS seems very unlikely
  - Benefits of DSL will only be fully appreciated when using it over several versions of the ERTMS standard
  - SysML with a light-weight profile will do the modelling job just as well
  - Requirements tracing from ERTMS standard to model is better in SysML than in GOPPRR DSL

Missing Elements, Ongoing Work

- University of Bremen currently favours SysML-based approach
- All benefits of DSL approach will be transferred to SysML-based approach
- This includes the complete tool chain