Developing of a safety-critical standard for the Swiss railways (SBB) with xUML and UTP

Markus Schacher, KnowBody

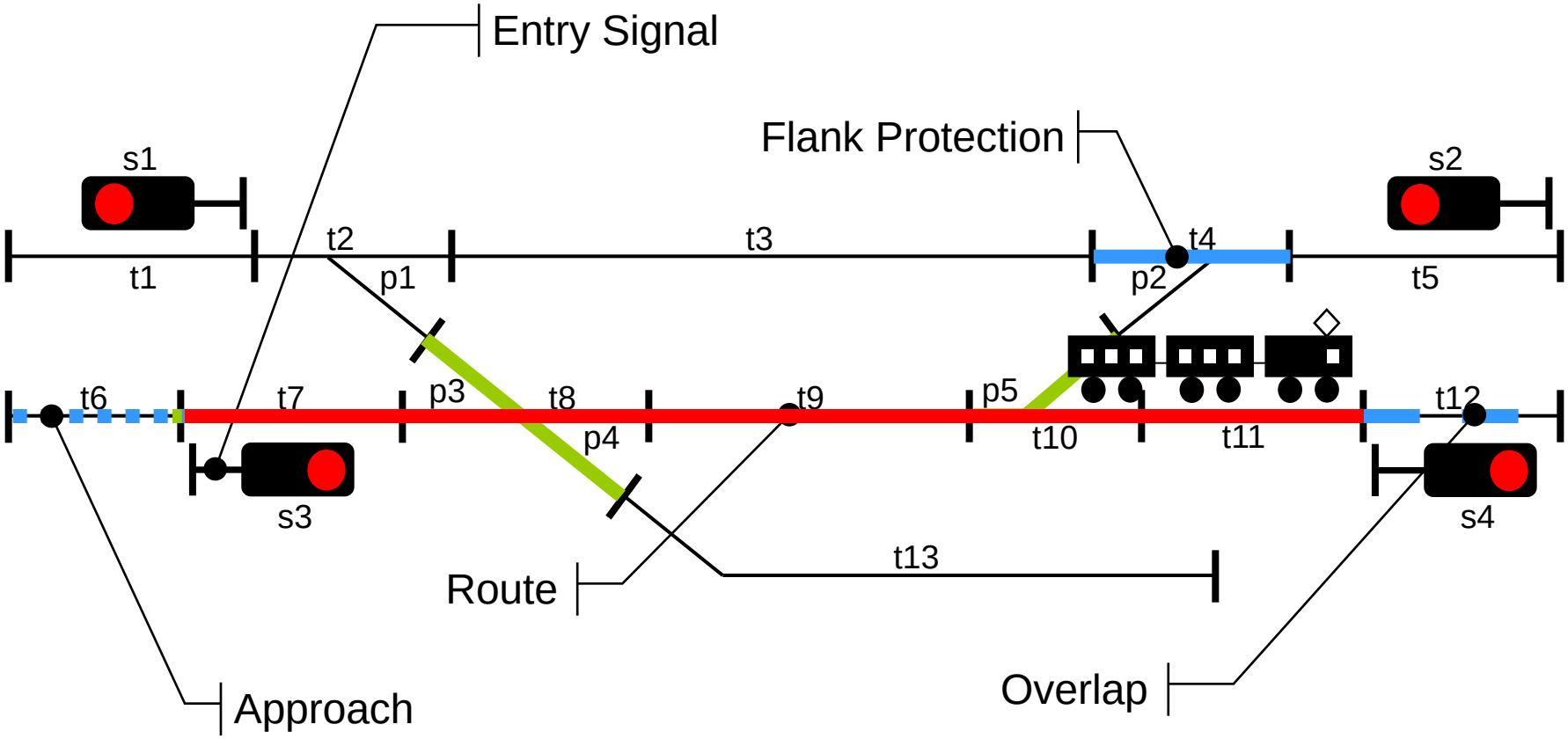
Hohlstrasse 534, 8048 Zürich, Switzerland
www.knowgravity.com

The Project SwISS

SwISS

Stellwerk Interface Standard SBB

What is an Interlocking (IL)?



Project Background

Situation in 2010

- There are **multiple suppliers for interlockings** (in Switzerland mainly Siemens and Thales) as well as different types and generations
- There are **no standards** for the communication between interlockings
- Today, interlockings are coupled via **expensive individual solutions**
- There are **many projects** to couple interlockings **in the pipeline**
- **Suppliers agreed to cooperate** on a standardization
- **DB** and **ÖBB** face **similar problems**

SBB's call for tender 2010

- **Development of an interface standard** between interlockings
- **Preliminary study and concept** for standardizing interfaces between interlockings and peripherials
- Coordination with DB

Project Vision and Deliverables

Vision: Due to a common interface standard, the Swiss Railways SBB may freely choose between suppliers in every interlocking and/or peripherial project.

Primary Deliverables:

- SwISS Vocabulary
- Specification SwISS Communication Layer
- Specification SwISS Application Layer ILn
- Executable version of the functional specification
- Test specification with test reports
- Preliminary study and technical concept for peripherial interface standard for peripherials

No software – no code

Secondary Deliverables:

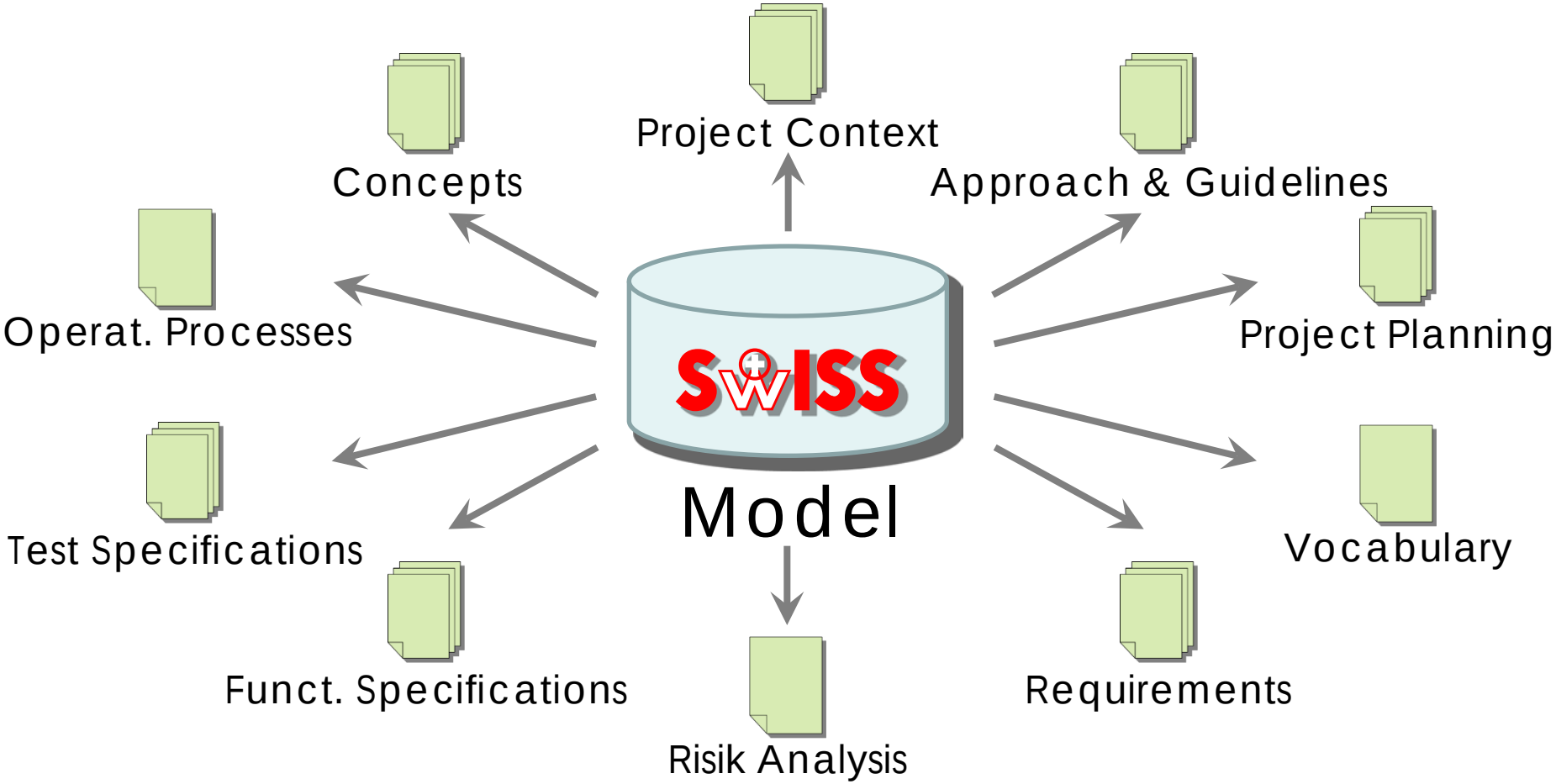
Project context, methodical approach, requirements catalogues, operational processes

Methodical Approach

"Total Modeling" – Everything is a Model

Principle 1: The Model is the Project

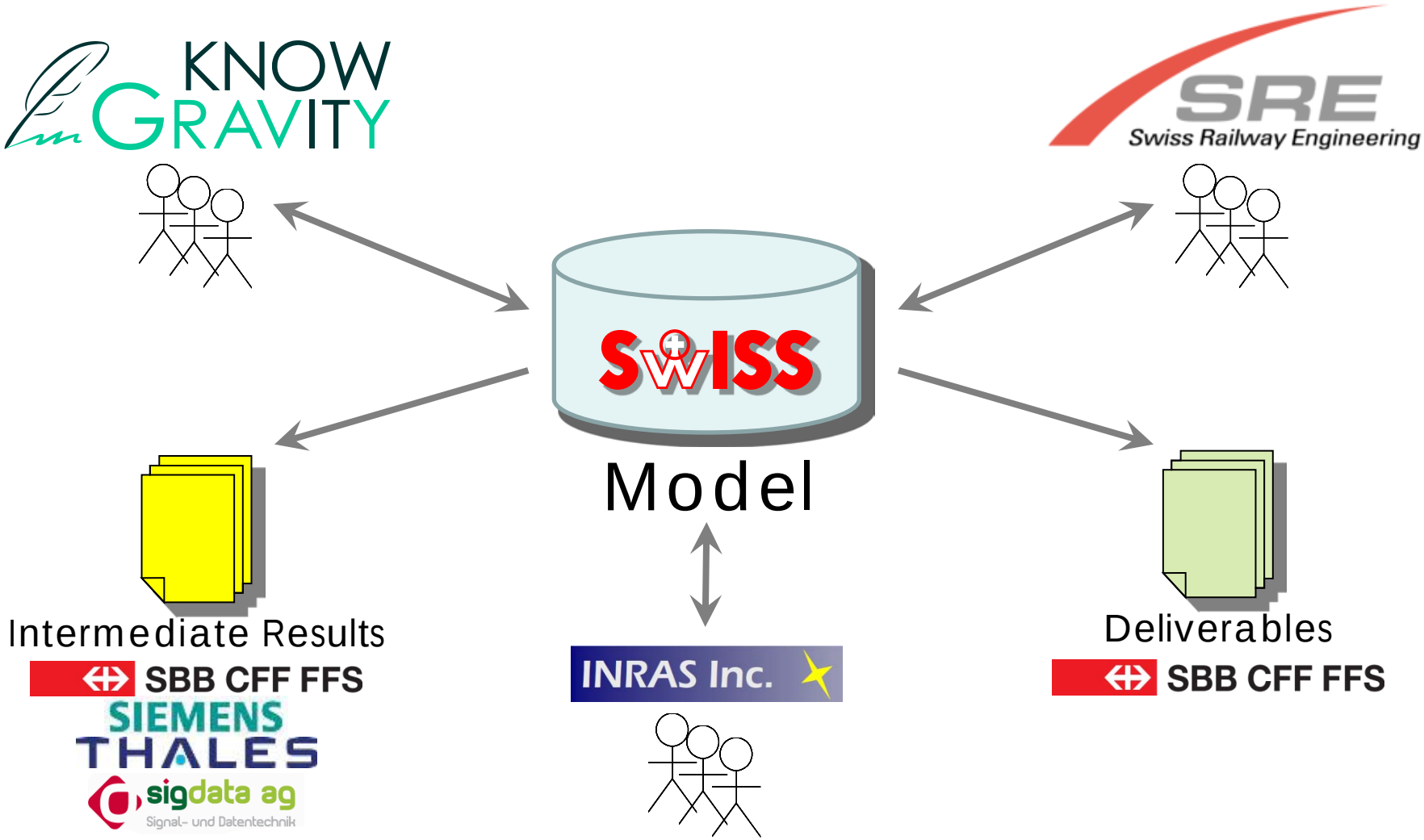
<u>One</u> model as central repository of all project information



All documents are automatically generated – no manual authoring!

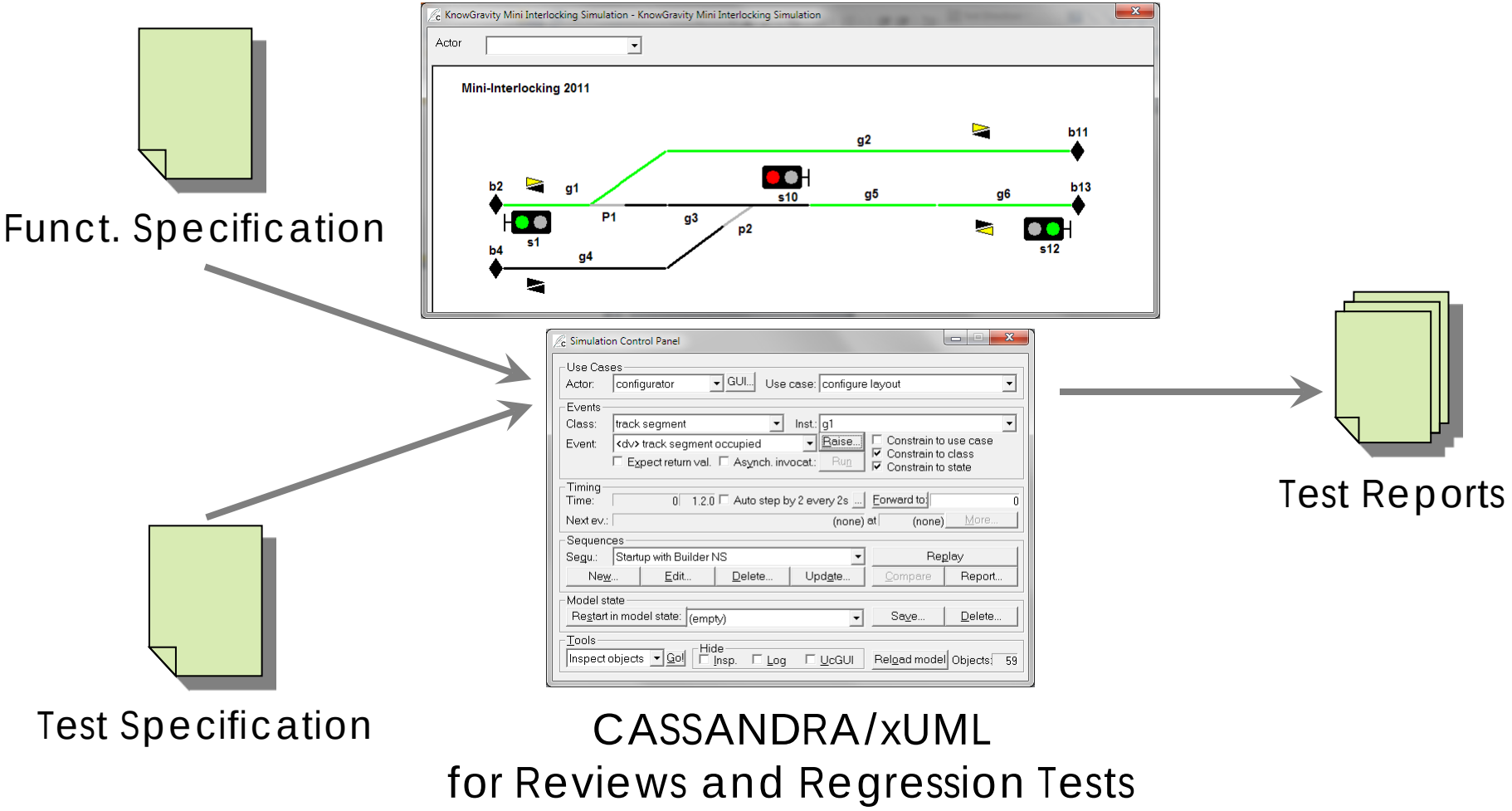
Prinziple 2: Parallel Modelling

<u>One</u> model – decentral and parallel elaboration by 3 companies



Prinziple 3: Testable Specifications

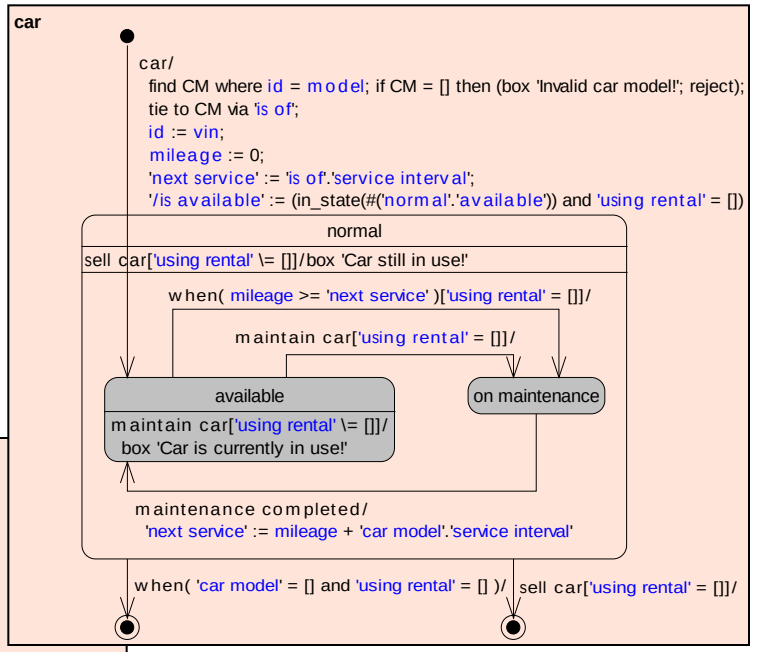
Executable and testable specification of interface standard



xUML: Raising the level of abstraction

Abstraction: *Any technique to generalize by ignoring or hiding details in order to identify commonalities among different pieces and to get a grip on the complexity of a designed system such as a software system.*

3rd Generation



2nd Generation

```
class AnimationFrame extends JFrame {
  private Label mStatusLabel;
  private NumberFormat mFormat;

  public AnimationFrame(TextBouncer ac) {
    super();
    setLayout(new BorderLayout());
    add(ac, BorderLayout.CENTER);
    add(mStatusLabel = new Label(), BorderLayout.SOUTH);
    // Create a number formatter.
    mFormat = NumberFormat.getInstance();
    mFormat.setMaximumFractionDigits(1);
    // Listen for the frame rate changes.
    ac.setRateListener(this);
    // Kick off the animation.
    Thread t = new Thread(ac);
    t.start();
  }

  public void rateChanged(double frameRate) {
    mStatusLabel.setText(mFormat.format(frameRate)+" fps");
  }
}
```

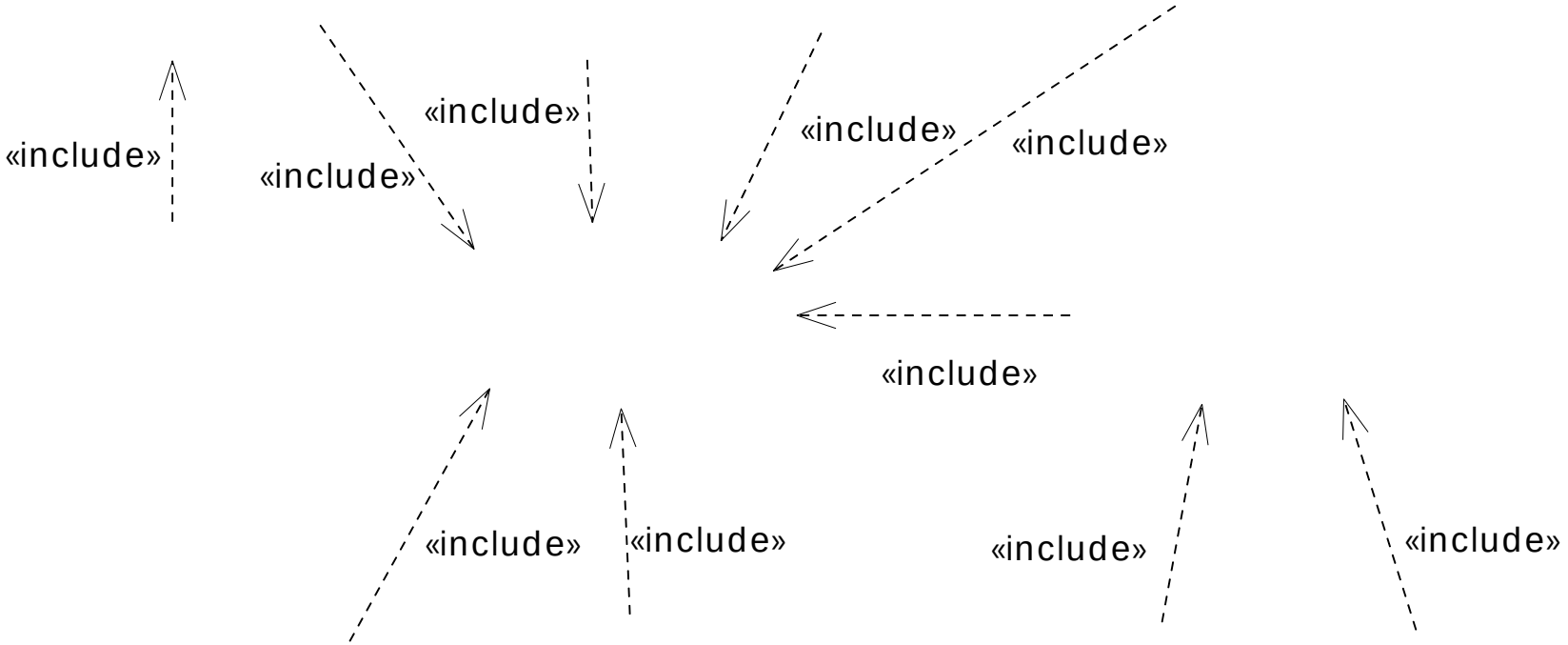
1st Generation

```
   .begin
   .org 2048
 a_start .equ 3000
2048   ld length,%
2064   be done
2068   addcc %r1,-4,%r1
2072   addcc %r1,%r2,%r4
2076   ld %r4,%r5
2080   ba loop
2084   addcc %r3,%r5,%r3
2088 done: jmpl %r15+4,%r0
2092 length: 20
2096 address: a_start
   .org a_start
3000 a:
```

Examples from the Project

Application of xUML and UTP in a safety-critical environment

Test Map (not yet part of UTP)



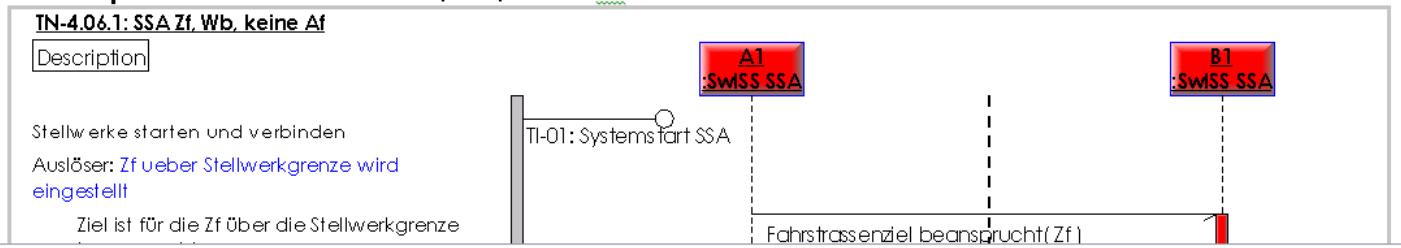
Test Case (1)

SBB CFF FFS nur für internen Gebrauch SwISS

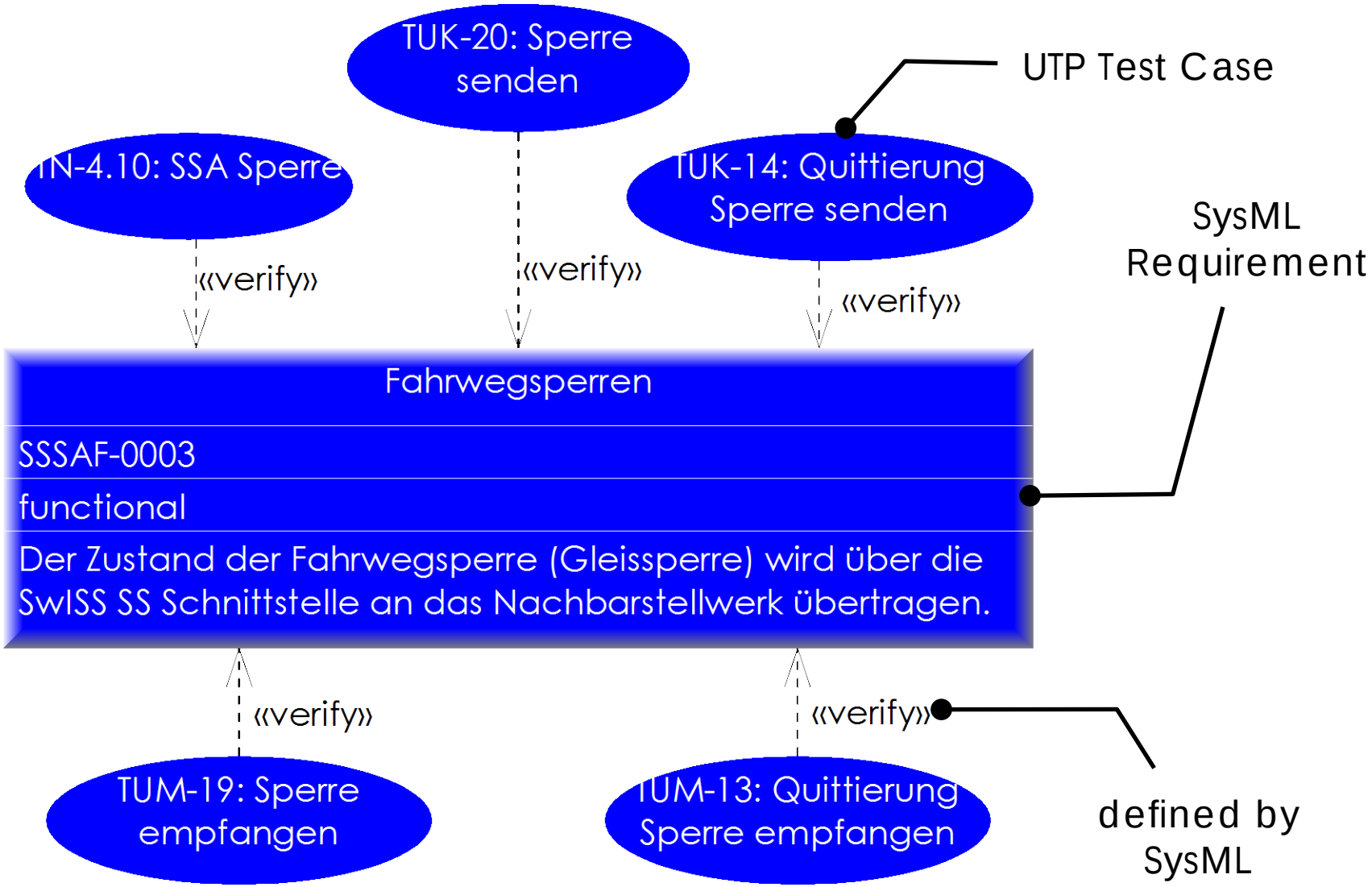
4.2.1.1.2 Test Case "TN-4.06.1: SSA Zf, Wb, keine Af"

TN-4.06.1: SSA Zf, Wb, keine Af	
Description	Dieser Testcase prüft folgendes Szenario: • Der Stw-Übergang wird durch eine Zugfahrstrasse beansprucht • Die ankommende Seite ist vom Typ Wirkbereich • Es ist keine Anschlussfahrstrasse Eingestellt • Die Beanspruchung wird wieder aufgelöst
precondition	U-Projektierung von A1: Empfang Weggeschwindigkeit: true U-Projektierung von B1: Typ der Zf-Stellwerkgrenze ankommend: Wirkbereich Ausgabe Weggeschwindigkeit: true Stw Uebergang ist im Grundzustand
postcondition	Stw Uebergang ist im Grundzustand

Test Sequence 'TN-4.06.1: SSA Zf, Wb, keine Af'



Traceability (1)



Traceabilty (2)

SBB CFF FFS nur für internen Gebrauch SwISS

Fahrwegsperren	
Beschreibung	Der Zustand der Fahrwegsperre (Gleissperre) wird über die SwISS SS Schnittstelle an das Nachbarstellwerk übertragen.
Anforderungs-Id	SSSAF-0003
Anforderungstyp	functional
Priorität	muss
Bemerkungen	Anforderungen und Informationen SBB [PHFAP2010]: Die Schnittstelle verfügt in der Regel über Fahrwegsperren. Diese Sperren sind in jedem der beiden Stellwerke als normale Befahrbarkeitssperren ausgeführt. Der Zustand der Sperre wird an das Nachbarstellwerk übertragen und neben der eigenen Sperre dargestellt. Beide Sperren werden für Fahrstrassen über diesen Gleisabschnitt berücksichtigt. Bedienbar ist nur die jeweils eigene Sperre.
Status	in Vernehmlassung
Quelle	[PHFAP2010], Abschnitt 2.3, Seite 10, Absatz 5
Verifiziert durch	TUM-19: Sperre empfangen, TUM-13: Quittierung Sperre empfangen, TUK-20: Sperre senden, TUK-14: Quittierung Sperre senden, TN-4.10: SSA Sperre

Summary

Testing in the Requirements Engineering Phase

Summary and Key Figures

Summary

- SwISS is a **standard for interlocking interfaces**
- An **executable functional specification** based on xUML has been developed
- **UTP** has been applied in a **pragmatic way** to model test cases to verify the functional specification
- **Regression tests** have been carried-out using CASSANDRA/xUML

Key Figures

- Issues found while developing the funct. specification: ~400
- Size of the functional specification IL-IL: ~100 pages
- Size of the test specification IL-IL: ~150 pages
- Number of test cases in test specification IL-IL: ~110
- Ø runtime of a test case in regression test: ~30 sec.