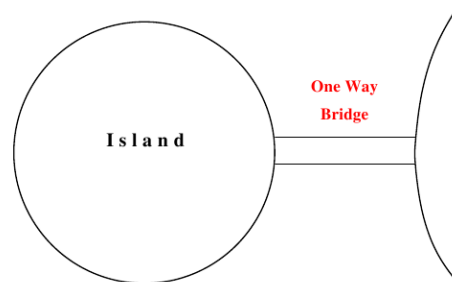


## Formale Entwurf mit Event-B – Die Zugbrücke



In der Vorlesung wurde das formale Entwurfswerkzeug RODIN vorgestellt, mit dem semi-interaktiv Event-B-Modelle bewiesen werden können.

Auf der Vorlesungshomepage finden sich einen Link zu einem Tutorium, in dem ein Modell für eine einspurige Brücke zwischen einer Insel und dem Festland in mehreren Verfeinerungsstufen entworfen wird. Gegenstände der Verfeinerungen sind dabei:

**Ausgangsmodell  $M_0$**  Modellierung von kapazitätsbeschränkter Insel und Festland

**Erste Verfeinerung  $M_1$**  Einführung der Brücke als Einbahnstraße

**Zweite Verfeinerung  $M_2$**  Einführung von Ampeln zur Beschränkung des Verkehrs

**Dritte Verfeinerung  $M_3$**  Einführung von Fahrbahn-Kontakten zur Steuerung der Ampelanlage.

Erarbeiten Sie sich mit Hilfe des Materials auf der Vorlesungshomepage die Event-B-Maschinen  $M_0$  bis  $M_3$  und schließen Sie die auftretenden Beweisverpflichtungen mit Hilfe der verfügbaren Solver.

### Aufgabe „Die Zugbrücke“



In dieser Aufgabe sollen Sie nun selbst ein Verfeinerung einer bestehenden Maschine erstellen und die entsprechenden Beweisverpflichtungen beweisen. Dazu wollen wir das Modell der Brücke, die Insel und Festland verbindet, zu einer Zugbrücke (oder besser “Hebebrücke”, s. Abb.) hin erweitern.

Die Brücke wird dazu mit einer Hebevorrichtung ausgestattet, mit der die Fahrbahn angehoben werden kann, damit Schiffe und Boote mit höheren Aufbauten darunter passieren können.

Die Brücke ist eine Zugbrücke mit zwei dedizierten Zuständen: oben und unten.	EQP-6
---	-------

Offensichtlich sorgt die Hebemechanik dafür, dass die Brücke nicht befahren werden kann, wenn die Fahrbahn gehoben ist. Das ist eine Eigenschaft, die sich aus der Natur der Anlage ergibt.

Solange die Brücke angehoben ist, können keine Autos auf die Brücke auffahren.	EQP-7
--	-------

Die Anlage könnte sich – rein technisch – natürlich heben, auch wenn ein Auto auf der Fahrbahn ist, aber wir wollen als Funktionalitätsanforderung dieses ausschließen.

Die Brücke kann nur angehoben werden, wenn keine Autos auf der Brücke sind.	FUN-4
---	-------

## Einführung der Zugbrücke

Erstellen Sie im bestehenden Projekt “bridge” eine neue Maschine *M1\_ZB1* als Verfeinerung der Maschine *M1*. Am einfachsten geht das, indem Sie mit der rechten Maustaste im Rodin-Explorer auf *M1* klicken und aus dem Kontextmenü *Refine* wählen.

Die damit angelegte Maschine ist als verfeinernde Kopie von *M1* ausgelegt: Sie kopiert alle Ereignisse der abstrakteren Maschine und dupliziert ebenfalls alle Variablen aus der Maschine höherer Abstraktion.

Fügen Sie nun zu diesem Modell eine neue Variable hinzu, die den Zustand der Brücke beschreibt. Fügen Sie außerdem zwei neue Invarianten zu der Maschine hinzu, die die Anforderungen EQP-6, EQP-7 und FUN-4 abbilden.

Ergänzen Sie die bestehenden Ereignisse um die den Anforderungen entsprechenden Vorbedingungen (guards) und evtl. Zuweisungen. Erstellen Sie ebenso zwei neue Ereignisse *BRIDGE\_UP* und *BRIDGE\_DOWN*, die das Heben und Senken der Brücke modellieren.

Beweisen Sie die zur Maschine gehörigen Beweisverpflichtungen.