





Modelling a Safe Interlocking Using the Event-B Theory Plug-in

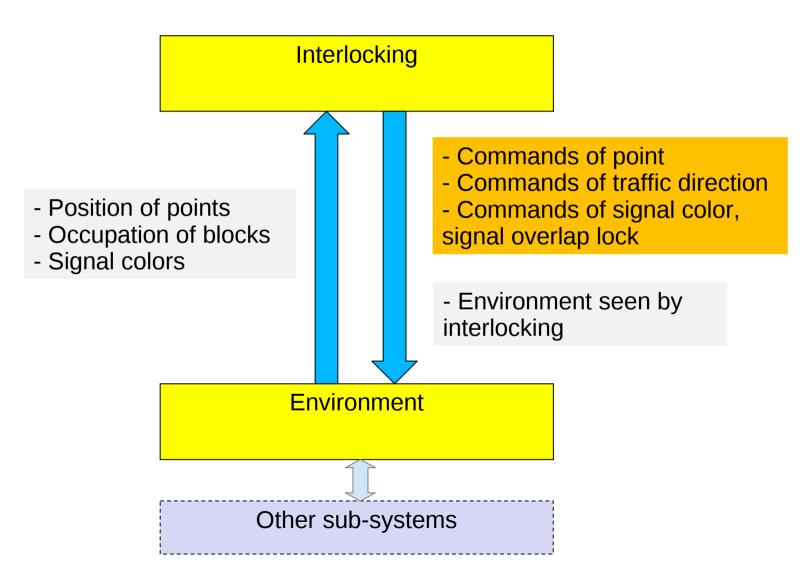
Rodin Workshop 2014 Toulouse, France

Laurent VOISIN Systerel

Minh-Thang KHUU Systerel

Fernando MEJIA Alstom TIS

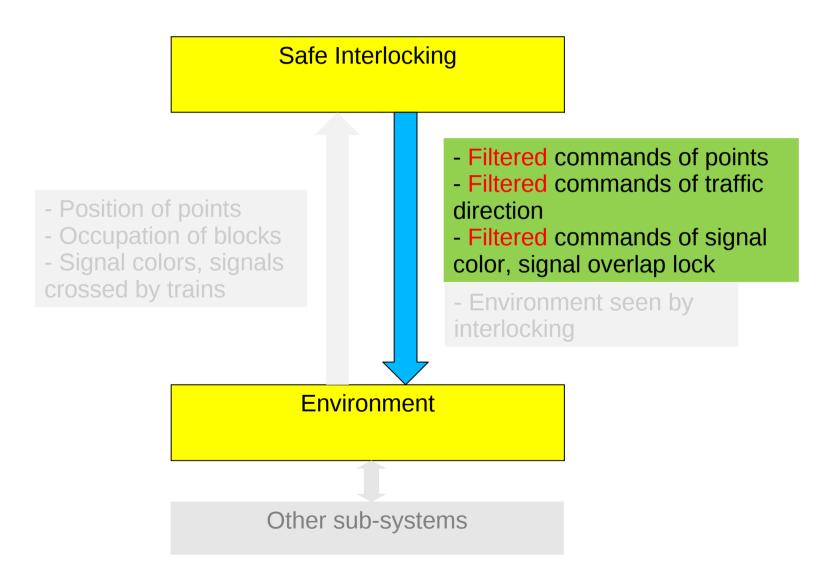
Interlocking sub-system



Interlocking sub-system Trains collision? Train derailment? **Interlocking** - Commands of points - Commands of traffic direction - Position of points - Commands of signal color, - Occupation of blocks signal overlap lock - Signal colors, signals crossed by trains - Environment seen by interlocking **Environment**

Other sub-systems

Interlocking sub-system

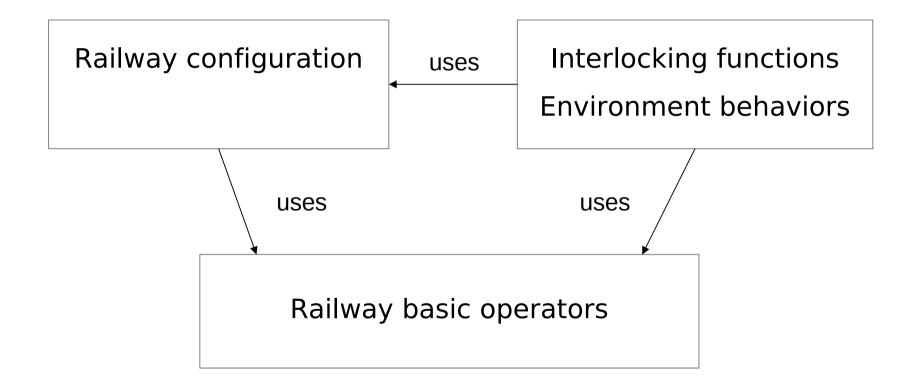


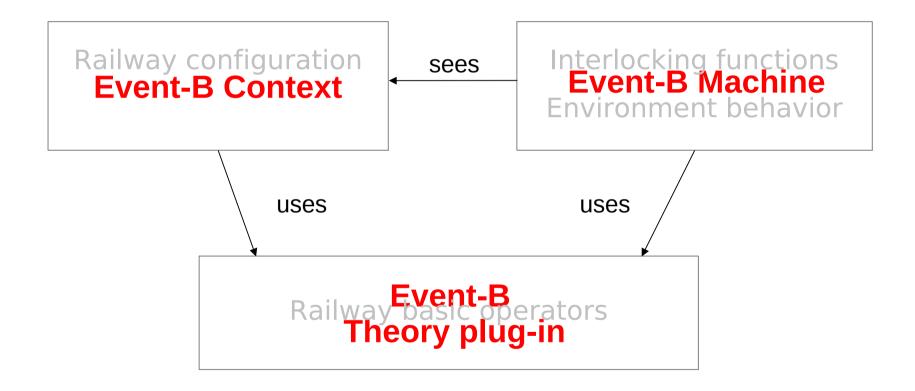
No derailment

Block chaining based on point positions

Track occupation/liberation sequence

No collision





The event-B model in developping

Conclusion and Future work

Conclusion

- Clarify domain terms
- Domain terms defined in *Theory* can be reused
 - **→** Enhance model maintainability
 - → Reduce proving effort

Conclusion and Future work

Conclusion

- Clarify domain terms
- Domain terms defined in *Theory* can be reused
 - **→** Enhance model maintainability
 - → Reduce proving effort

On working

- > A more visual animation of the model (BMotion Studio)
- Decomposition of the model :
 - Environment
 - Interlocking
 - Communication buffer

Conclusion and Future work

