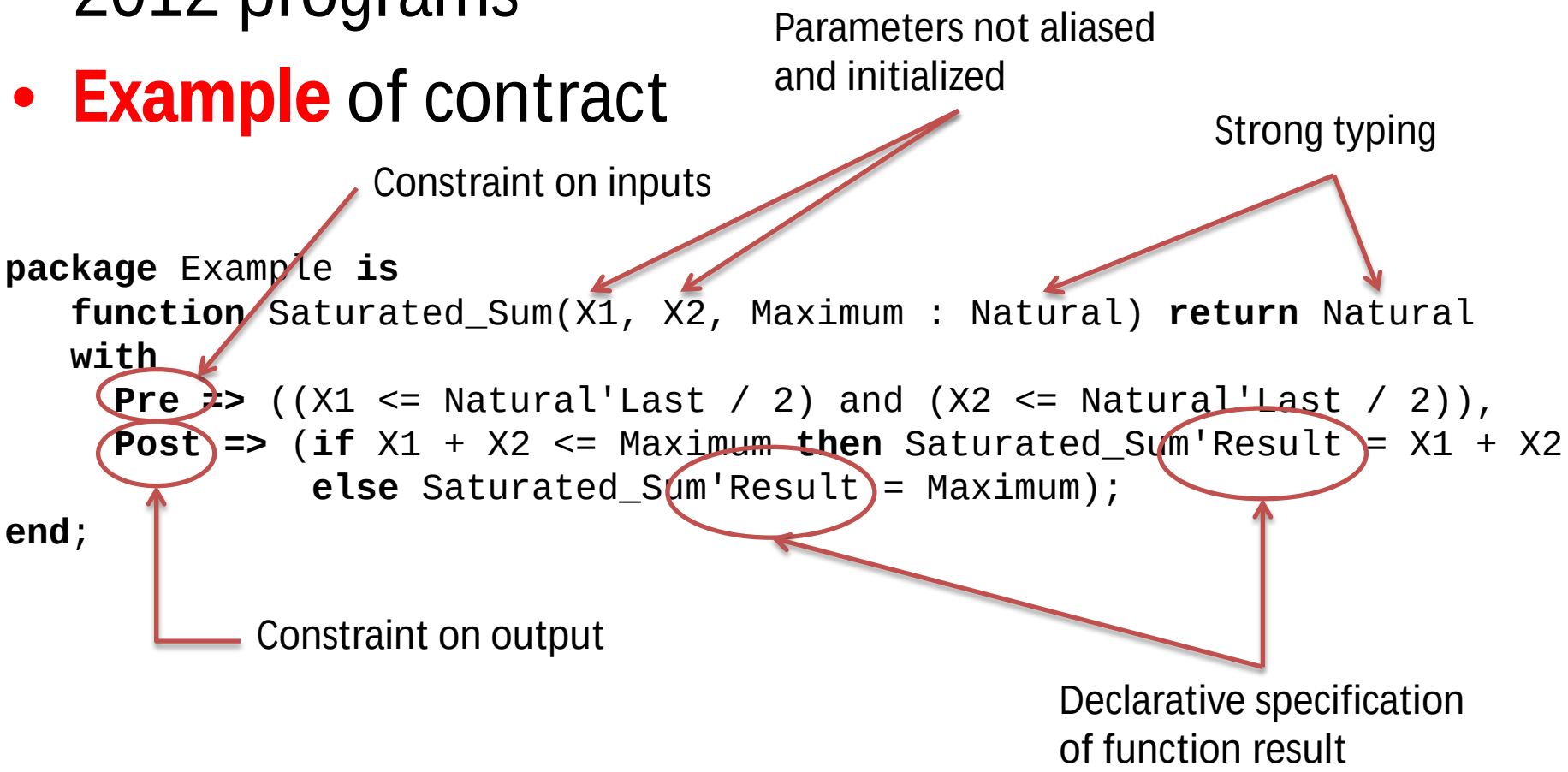
GNATprove ETCS model

David MENTRÉ

2013-04-15

GNATprove: contracts

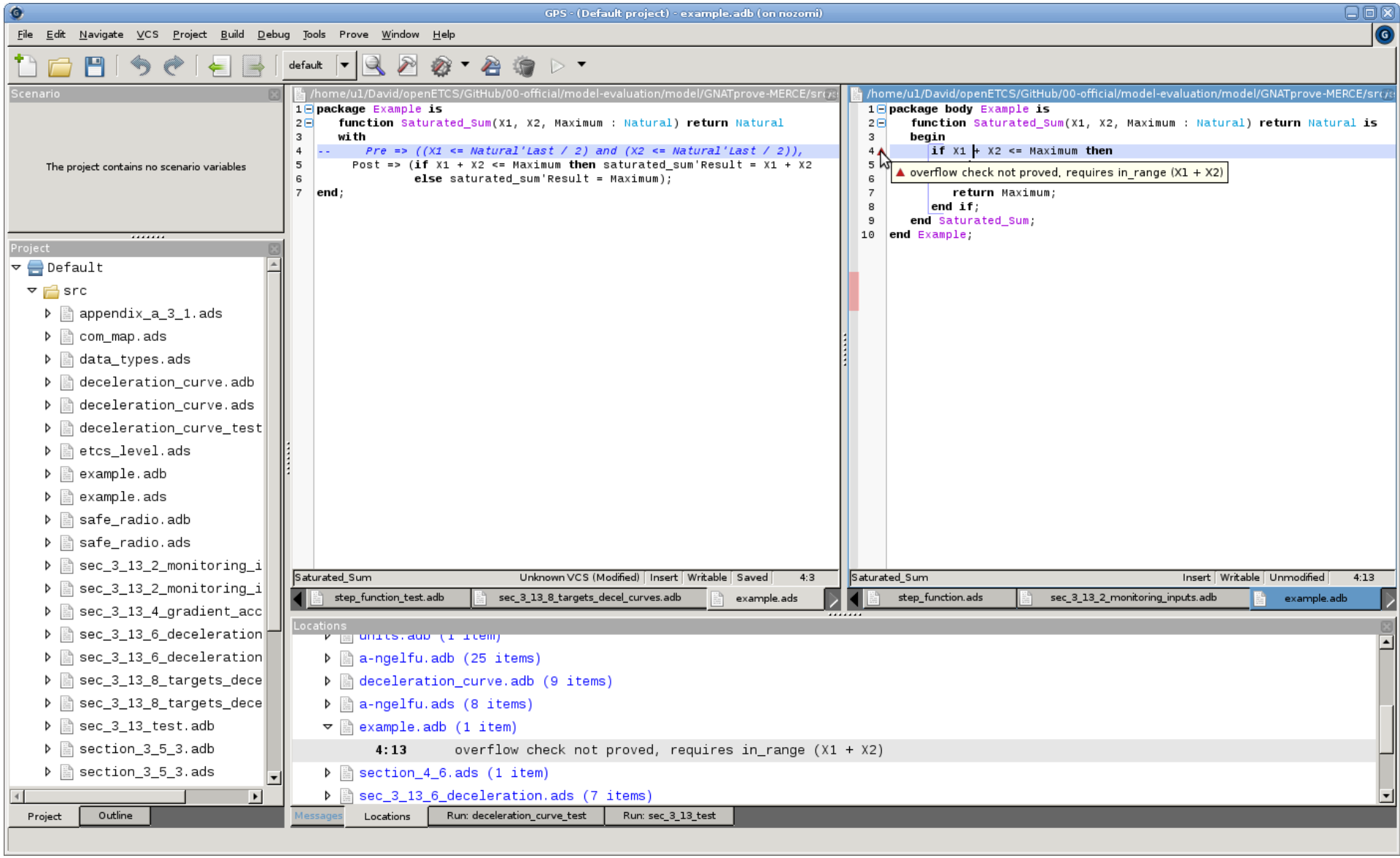
- GNATprove: formal **contract verification** on Ada 2012 programs
- **Example** of contract



GNATprove: verification

- Tool **statically** and **automatically** verifies
  - **Absence of Run Time Errors**: overflow, underflow, out-of-bound access
  - At call point, **Pre-condition is satisfied**
  - **Post-condition is satisfied**, provided Pre-condition is satisfied
    - Need to add specific **annotations**, e.g. for loops
- **Mix test and proof**
  - **Incremental** introduction of formal methods without breaking current development process
  - You can **test** your formal **annotations**!

GNATprove GNU GPL tools (2012 edition)



GNATprove ETCS model

SRS section	Done	Comment
§5.9 Procedure On-Sight	û	See no particular issue
§3.5.3 Establishing a communication session	ü	
§3.13.4 (Acceleration / Deceleration due to gradients)	~	Support function modeled
§3.13.6.2 Emergency brake	ü	
§3.13.7 Determination of Most Restrictive Speed Profile (MRSP)	~	Support function modeled
§3.13.8.3 Emergency Brake Deceleration curves (EBD)	ü	
§3.13.9.3.3.9 Computation of d_FLOI, using d_SBI2_MREBDT	û	
§3.13.9.4 Release speed supervision limits	û	
§3.13.10.4.2 Calculation of the MRDT	û	
§4.6.2 (Transitions Table) and §4.6.3 (Transitions Condition table)	ü	

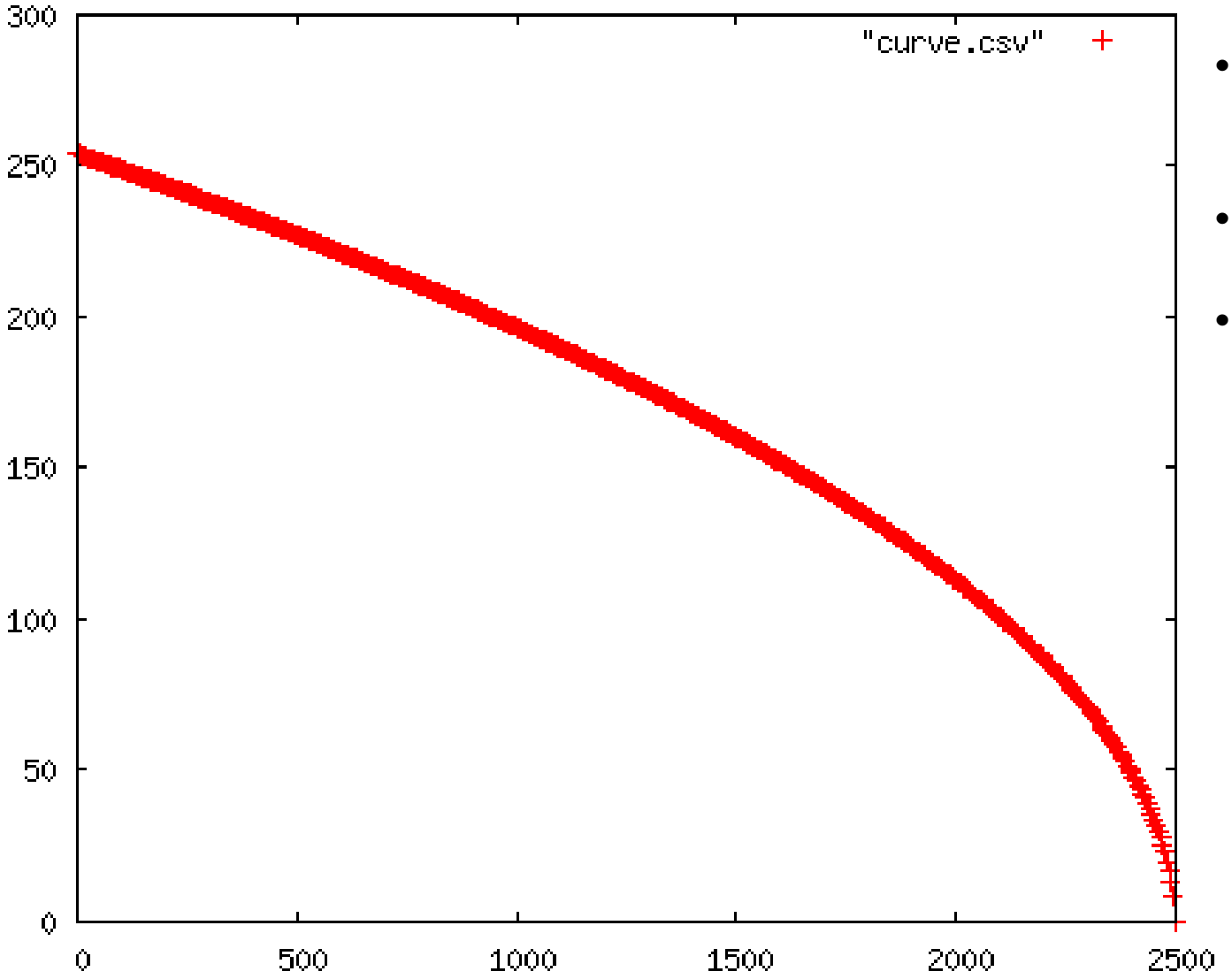
Specification sample

- Excerpt for §3.5.3

```
function Authorize_New_Communication_Session return Boolean is
    ((Start_Of_Mission = True
      and (ertms_etcs_level = 2 or ertms_etcs_level = 3)) -- SUBSET-026-3.5.3.4.a
     and Track_Side_New_Communication_Order = True -- SUBSET-026-3.5.3.4.b
     and (Mode_Change_Report_To_RBC_Not_Considered_As_End_Of_Mission = True
          and (ertms_etcs_level = 2 or ertms_etcs_level = 3)) -- SUBSET-026-3.5.3.4.c
     and (Manual_Level_Change = True
          and (ertms_etcs_level = 2 or ertms_etcs_level = 3)) -- SUBSET-026-3.5.3.4.d
     and Train_Front_Reaches_End_Of_Radio_Hole = True -- SUBSET-026-3.5.3.4.e
     and Previous_Communication_Loss = True -- SUBSET-026-3.5.3.4.f
     and (Start_Of_Mission_Procedure_Completed_Without_Com = True
          and (ertms_etcs_level = 2 or ertms_etcs_level = 3)) -- SUBSET-026-3.5.3.4.g
    );

  -- SUBSET-026-3.5.3.1 and SUBSET-026-3.5.3.2 implicitly fulfilled as we model on-board
  procedure Initiate_Communication_Session(destination : RBC_RIU_ID_t;
                                           phone : Telephone_Number_t)
  with
    Pre => (Authorize_New_Communication_Session -- SUBSET-026-3.5.3.4
            and (not Contains(Connections,destination)) -- SUBSET-026-3.5.3.4.1
            -- FIXME: what should we do for cases f and g?
           ),
    Post => (Contains(Connections, destination));
```

Computed (basic) braking curve



- Target
  - 2500 m
  - speed 0 km/h
- Constant deceleration: -1 m/s²
- Resolution: 5 m

Interesting points on proofs

- Modeling of **step functions**
  - Used throughout SRS
  - Partial **functional proofs** of
    - *Minimum_Until_Point*: minimum of a step function until a given point (e.g. used for acceleration / deceleration due to gradient)
    - *Restrictive_Merge*: merge of two step functions (e.g. MRSP computation)
  - **Full** functional proofs are **possible**
- Modeling of **deceleration curves**
  - Partial proof of **absence of Run Time Errors**
- Modeling of **Mode transition table** §4.6
  - **Impossible** to prove mode **exclusion** without further assumptions (https://github.com/openETCS/model-evaluation/wiki/Open-Question-for-Modeling-Benchmark#section-46)

Conclusion

- **All** SRS objects can be modeled in Ada 2012
  - Strong ability to handle **complex data structures**
  - But one needs to make **support packages**
    - **Generic language + Library** approach
- First **basic** model made
  - A **lot** of possible improvements!
- **Proofs** range from very **easy** to **difficult**
  - Very ***good integer*** support. Poor floating point support
  - **No induction** with automatic prover
    - Fall back to **manual proof**
- **Executable** model or not?
- **Proof of what**? SRS missing underlying safety principles
  - E.g. energy conservation for emergency braking
- Questions?