Property verification on traces

{**emmanuel.gaudin**,eric.brunel}@pragmadev.com

PRAGMADEV

PRESTO

Project consortium

RAPITA SYSTEMS LTD

teletel

THALES ITALY

INRIA

SOFTEAM Think Object

MILTECH HELLAS S.A.

MetaCase

PRAGMADEV real time development tools

VTT

THALES COMMUNICATIONS - FRANCE

PRISMTECH Productivity Tools & Middleware

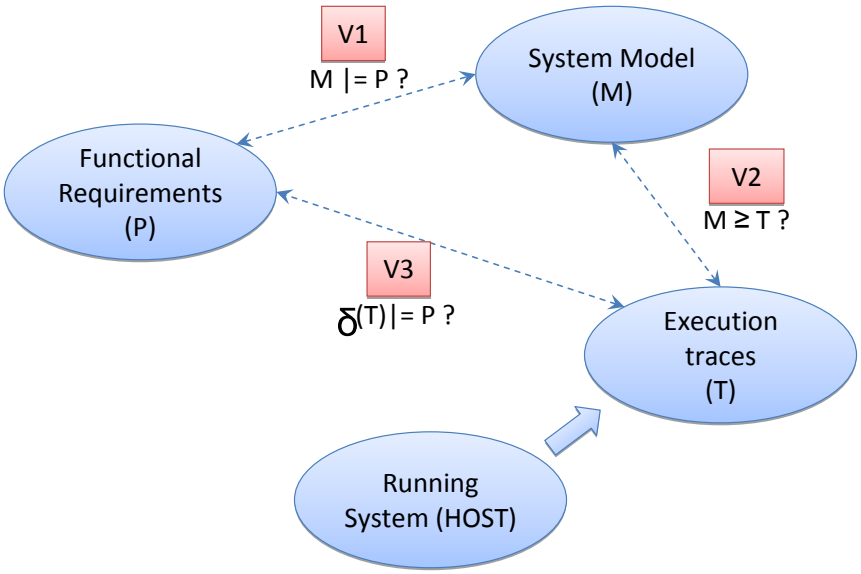
SarokalSolutions

http://www.presto-embedded.eu/

Project objectives

- imProvement of industrial Real time Embedded SysTems development prOcess
- Early verification of functional and non-functional properties

  - V1 – verify that the system model (M) satisfies the properties (P).
  - V2 – verify that the system model (M) contains the traces (T) that have been monitored by observing the running system.
  - **V3 – verify that the execution traces (T) conform to identified properties (P).**



Candidates to express properties

- Temporal logic
  - Ambiguous
  - Complex
- MSC – Message Sequence Chart ITU-T standard
  - Simple
  - Poor to express properties
- Property Sequence Chart
  - Unambiguous
  - Simple (similar to MSC and UML Interactions)
- UML MARTE
  - Activities
  - Interactions (similar to MSC)

Concept

- Use the same type of diagram for:
  - Traces
  - Specification
  - Properties
- In order to easily verify the properties on the traces

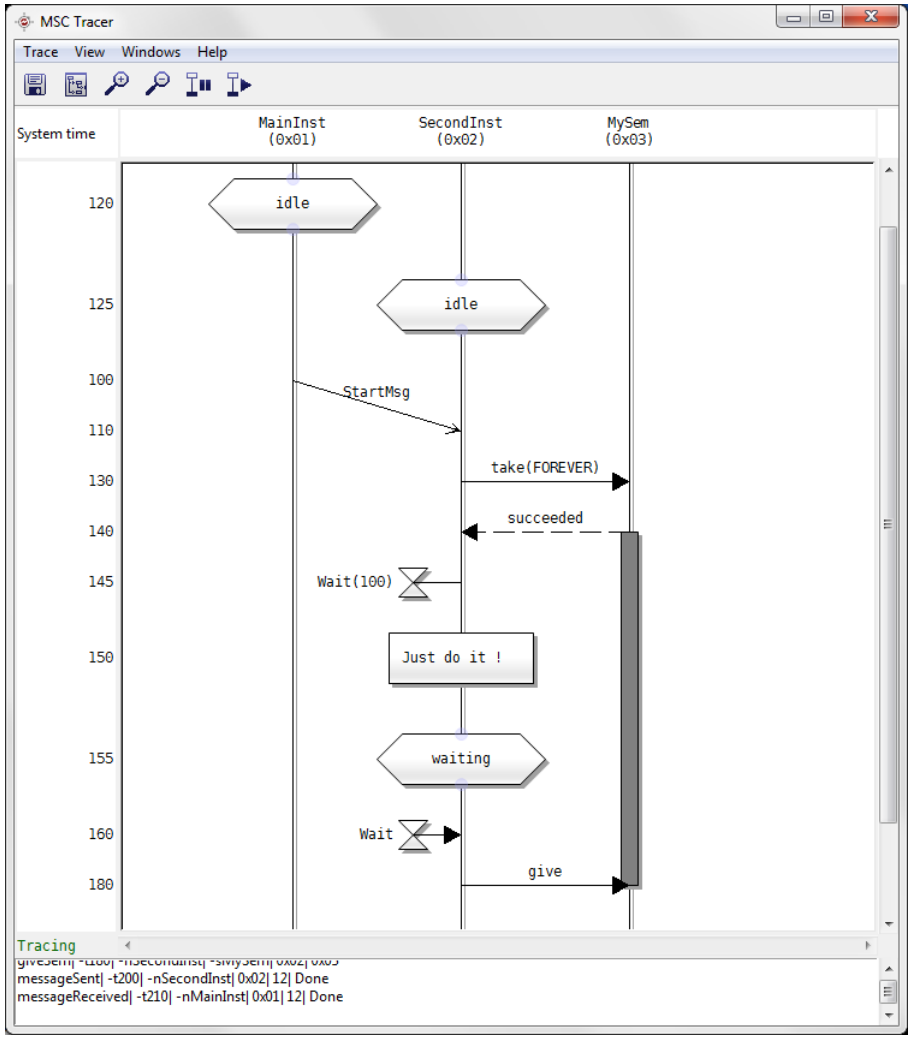
Traces

Message Sequence Chart
MSC
ITU-T Z.120
international standard

Execution traces:

- Instances,
- States,
- Messages,
- Operation calls,
- Semaphores,
- Timers,
- Actions.

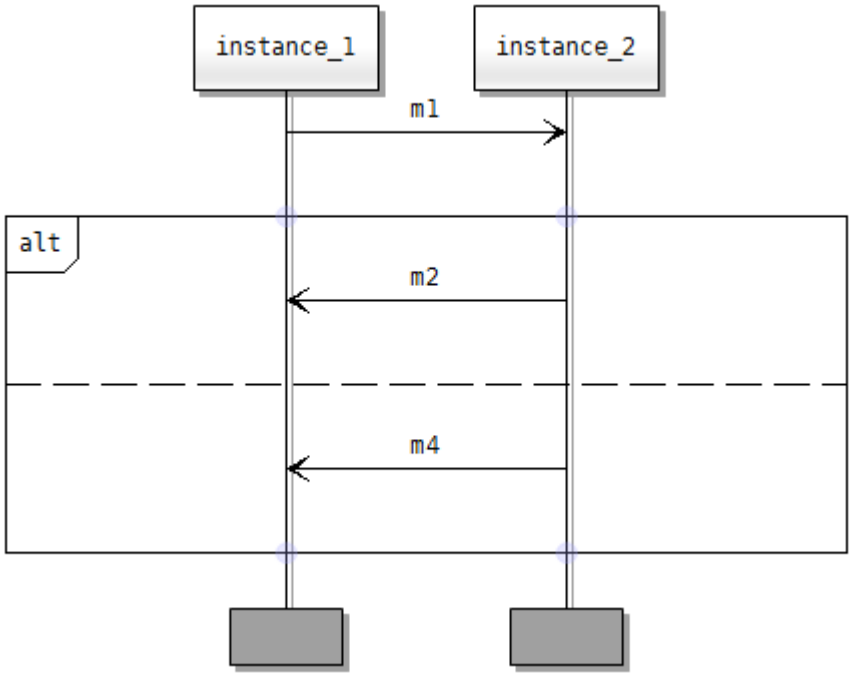
Display of system time



Specification

A specification is an expected behavior for the system.

- Sequence of events
- Alternatives and loops
- Time constraints

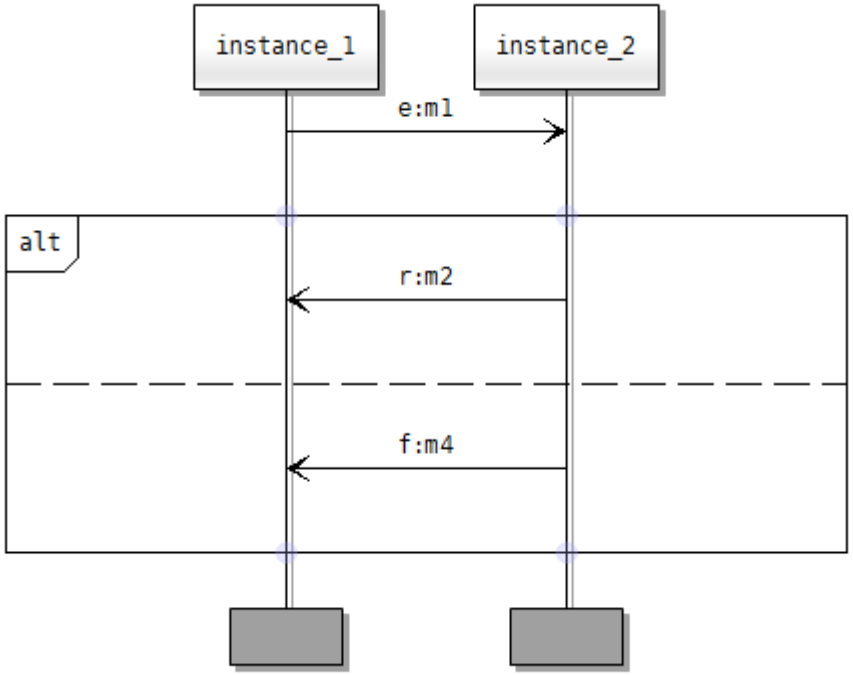


Property

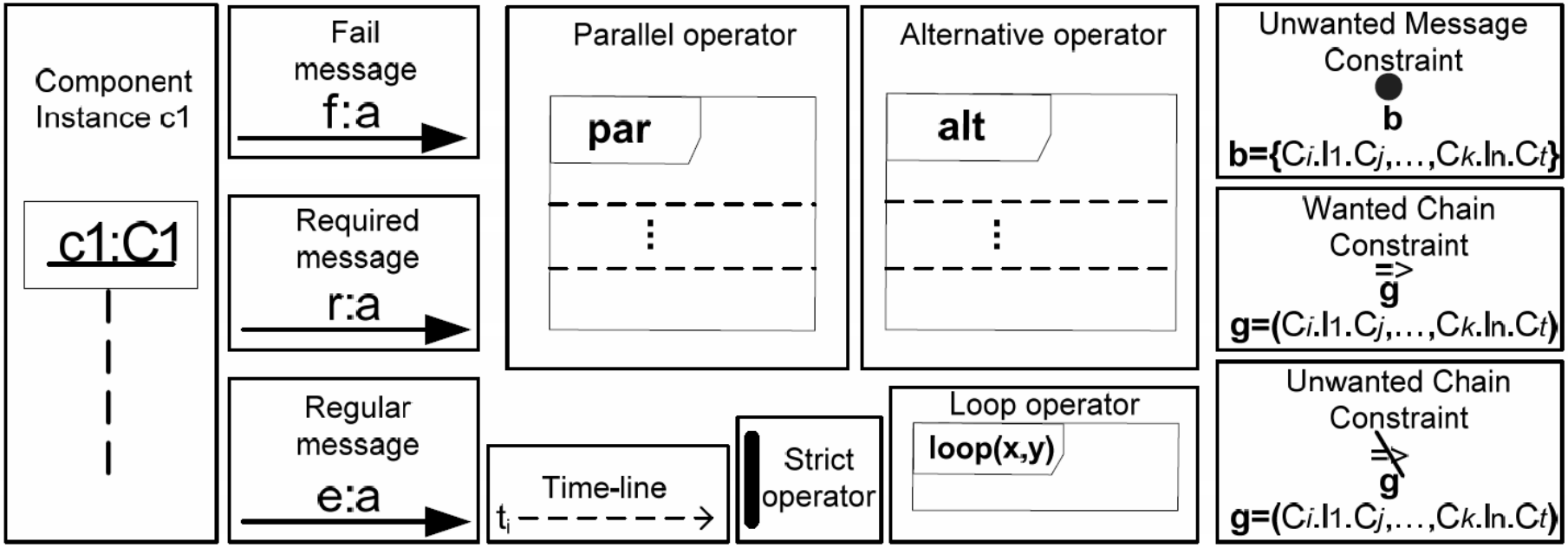
A way to express causality:

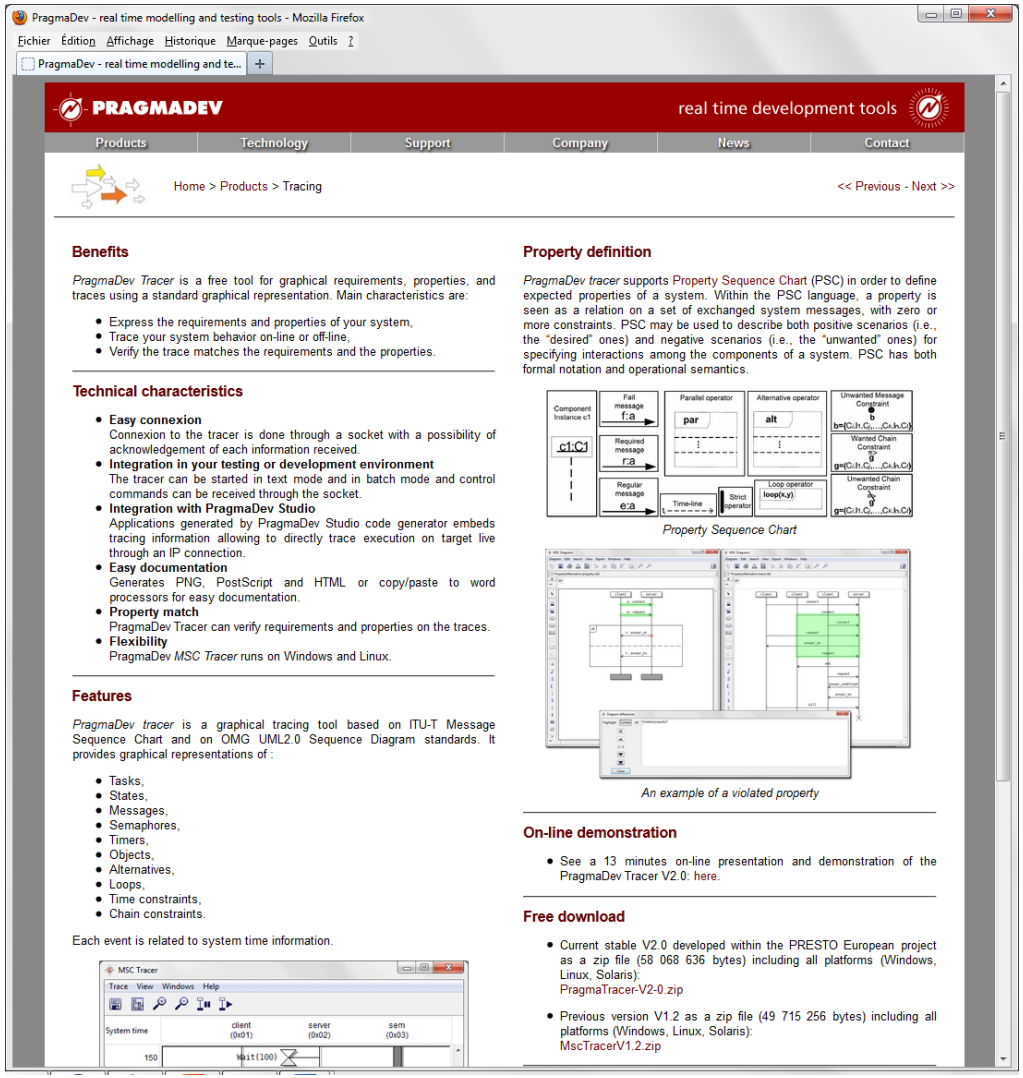
- If *cause* then *effect*
- If *not cause* then *effect*
- If *cause* then *not effect*
- If *not cause* then *not effect*

With simple annotations on the MSC.



Property Sequence Chart

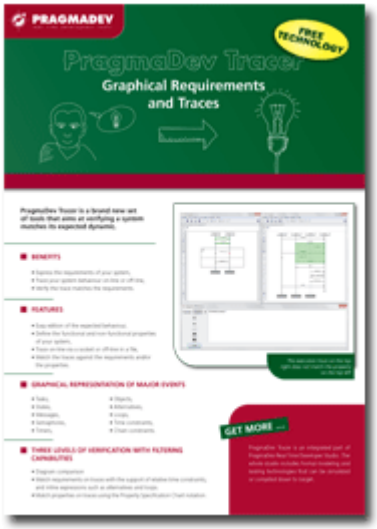




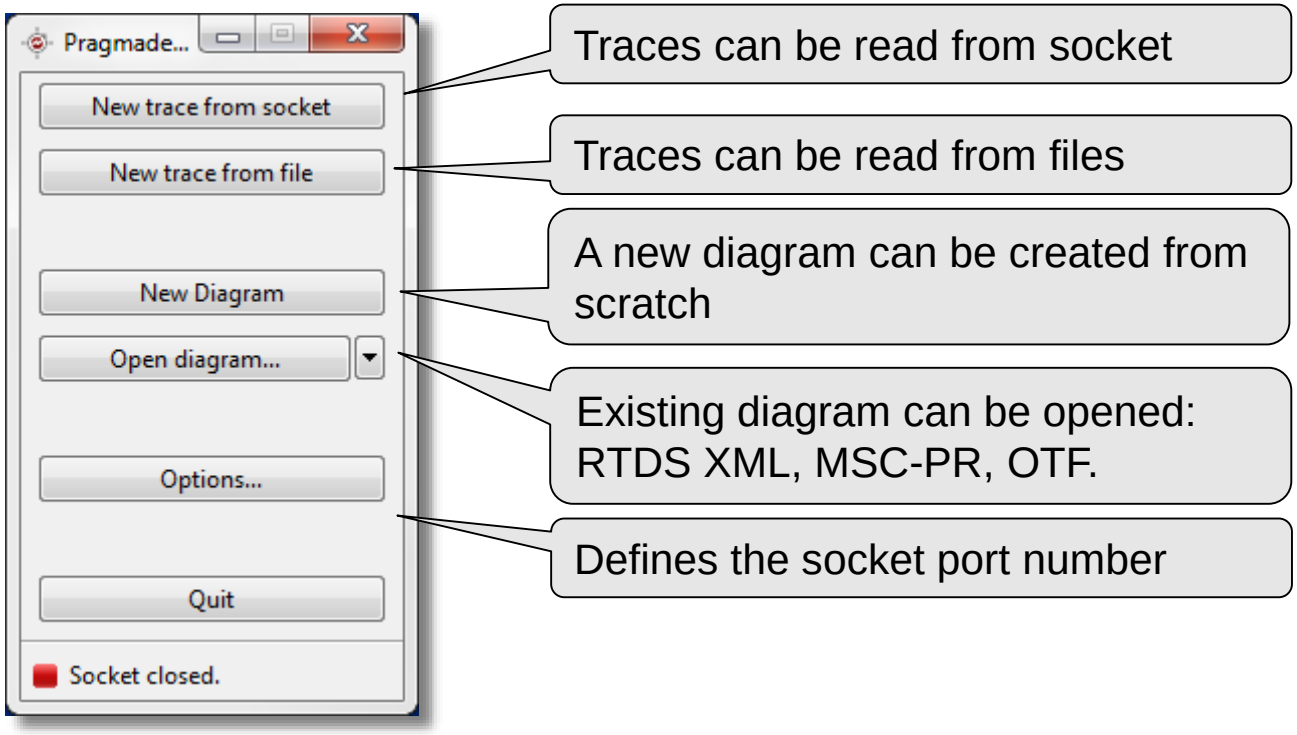
Tool:

PragmaDev Tracer

- Free
- Windows, Solaris, Linux

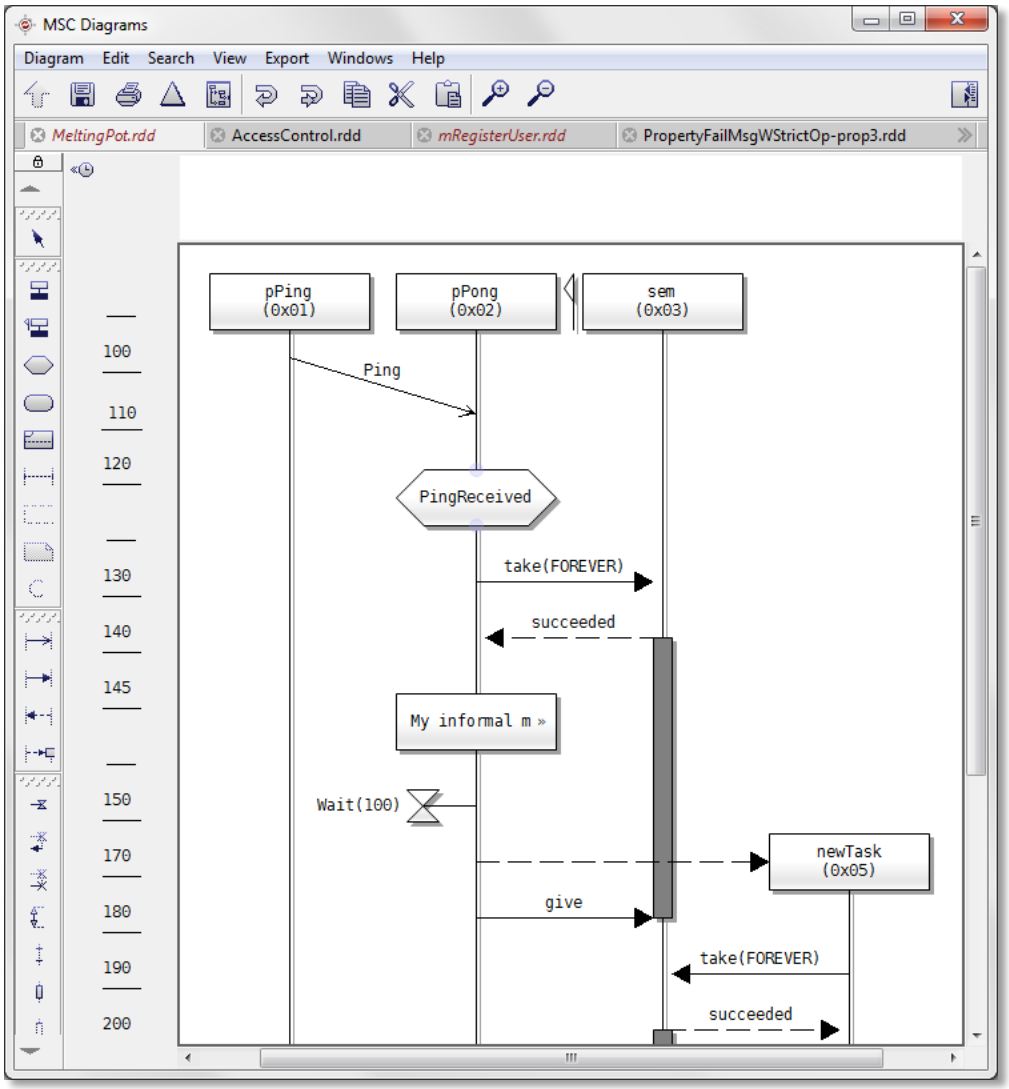


Main window


Pragmade...
New trace from socket
New trace from file
New Diagram
Open diagram...
Options...
Quit
Socket closed.
Traces can be read from socket
Traces can be read from files
A new diagram can be created from scratch
Existing diagram can be opened: RTDS XML, MSC-PR, OTF.
Defines the socket port number

Editor / Tracer

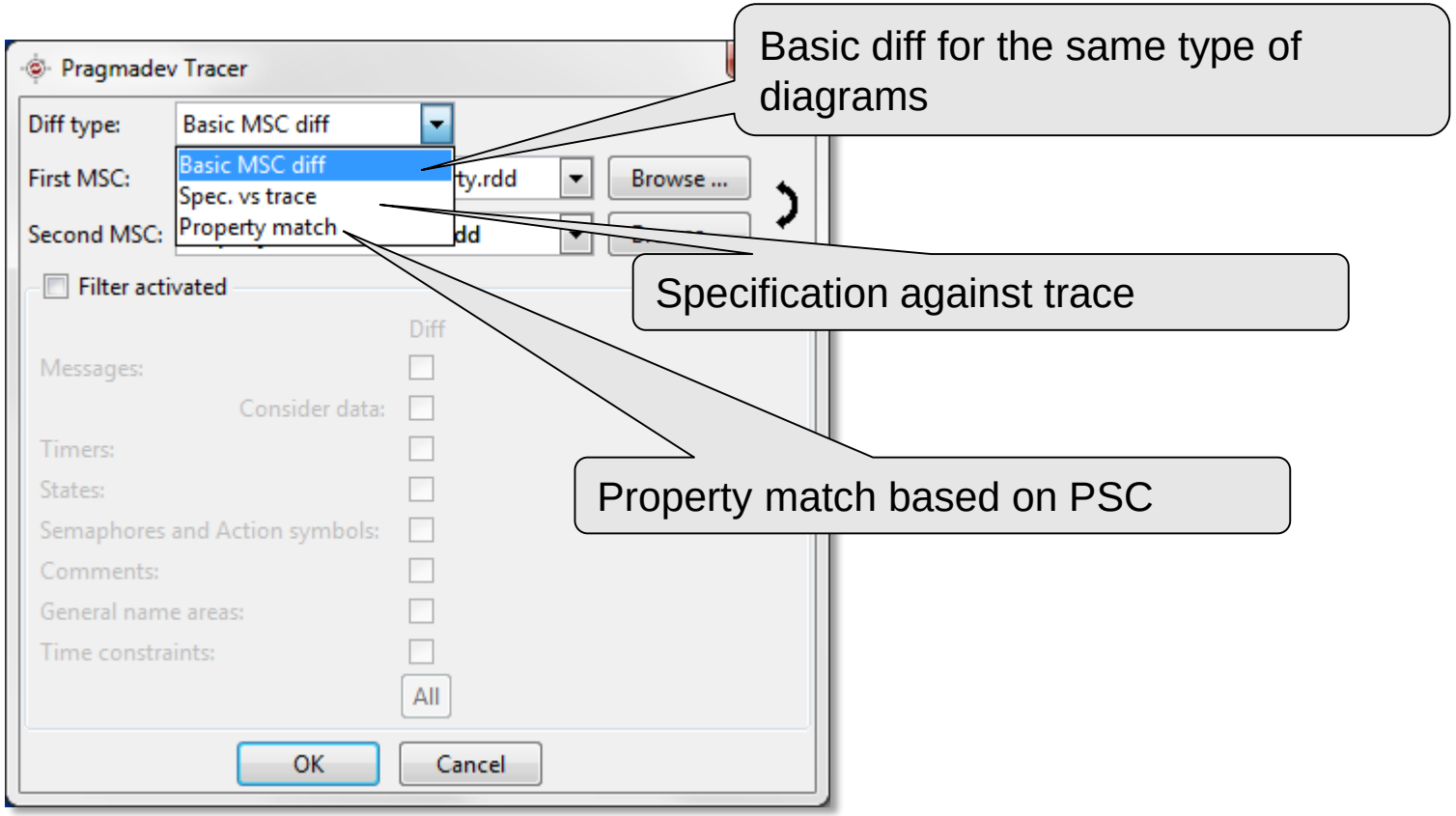
- Preview
- Expand / Collapse
- Filters
- Copy / Paste

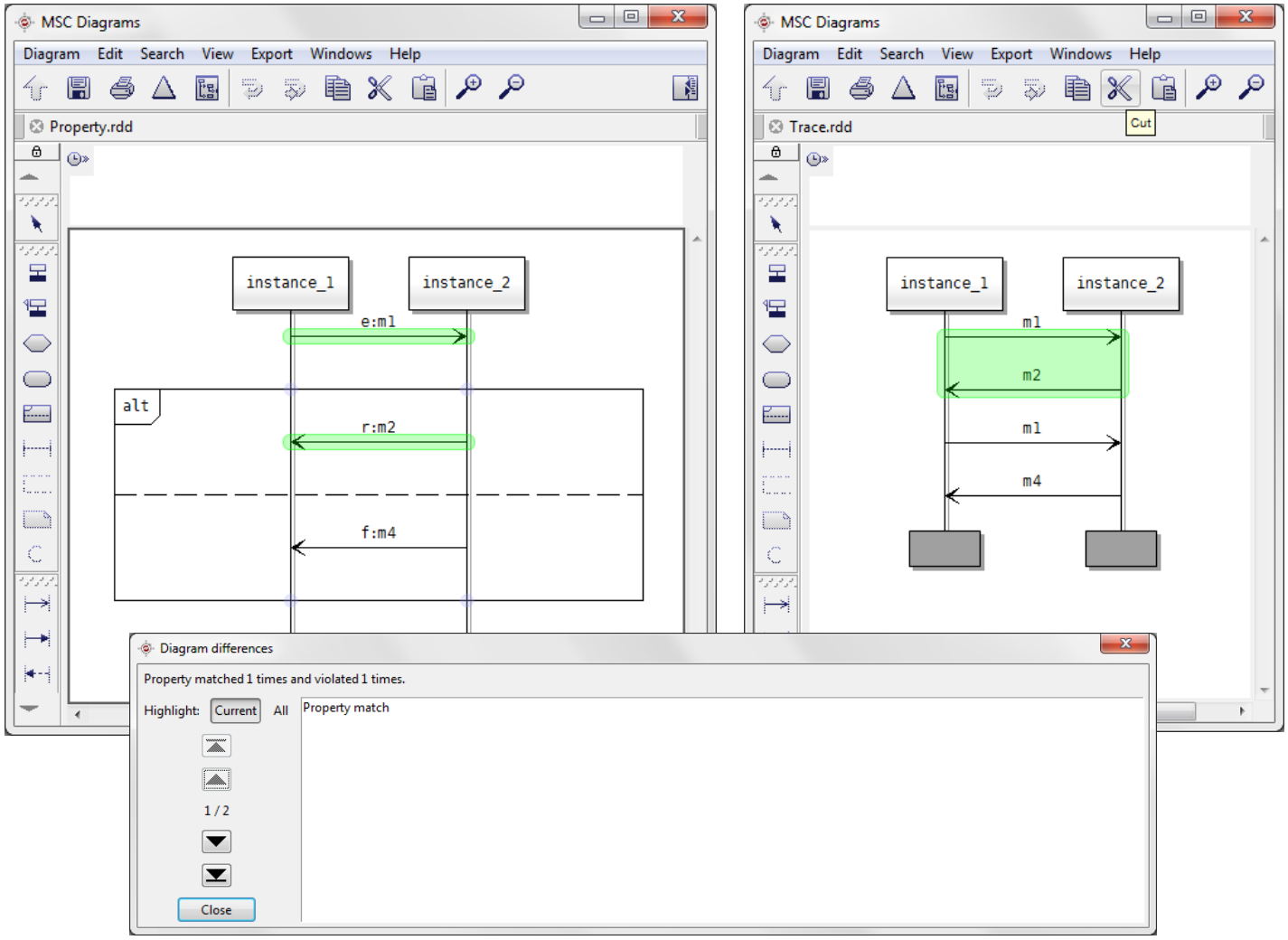


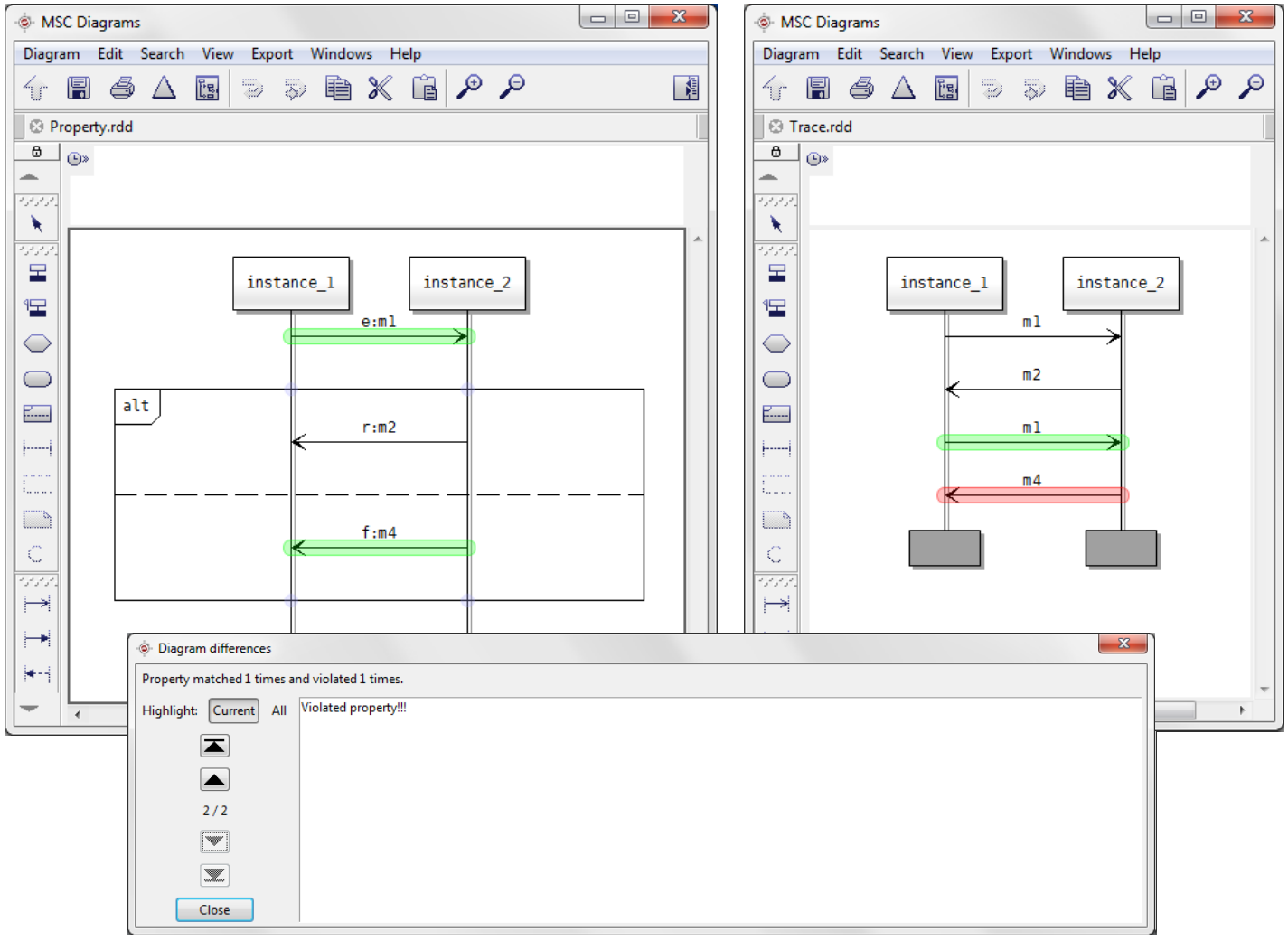
How to generate traces

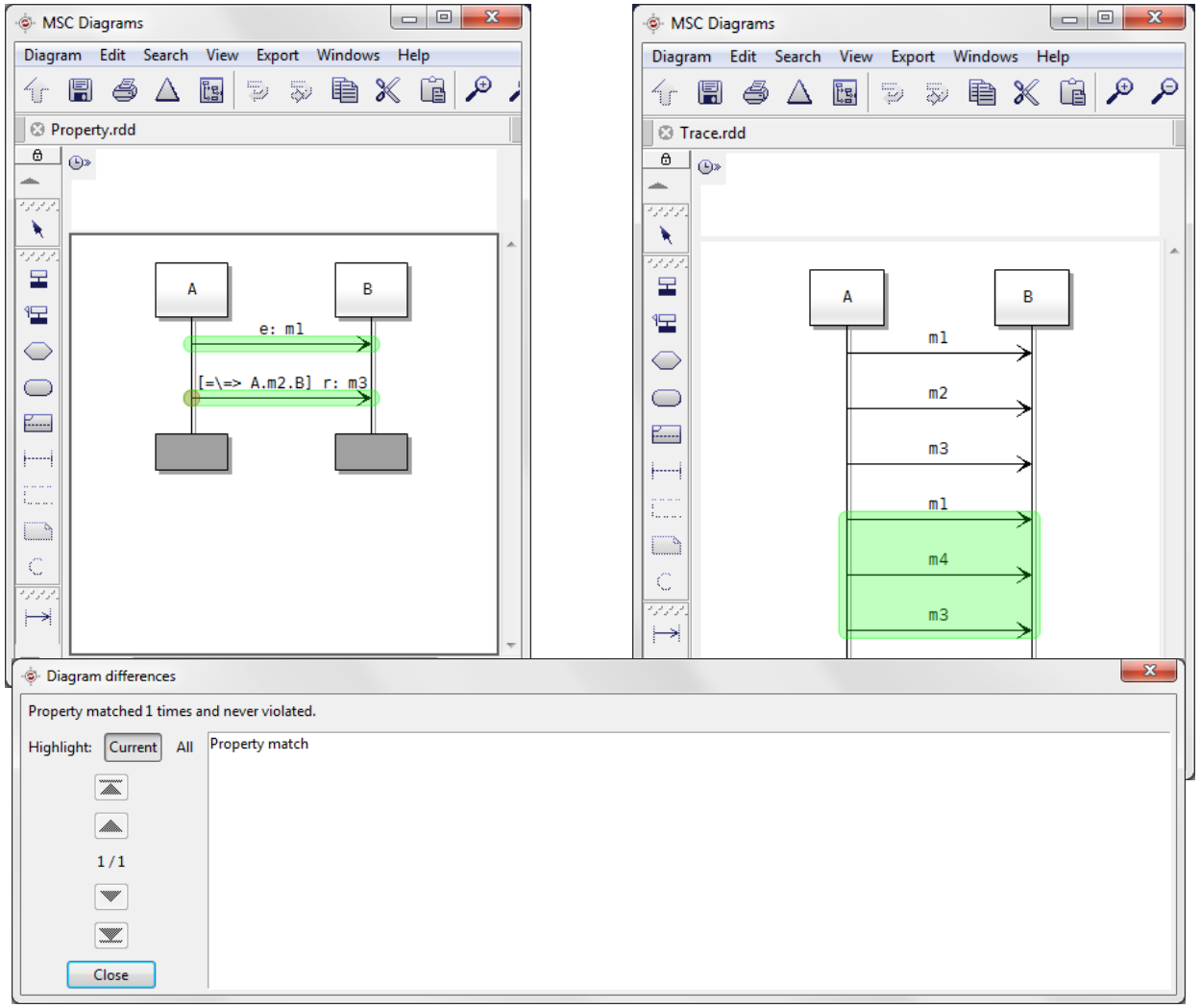
- Model simulation (requires an executable model such as an SDL model)
- C macros for legacy code
  - Easy to insert in existing code
  - Easy to generate from a modeling tool
  - Write in a file or in a socket
  - File or socket can be read by the tracer
- MSC-PR, OTF, TTCN-3

Three levels of verification



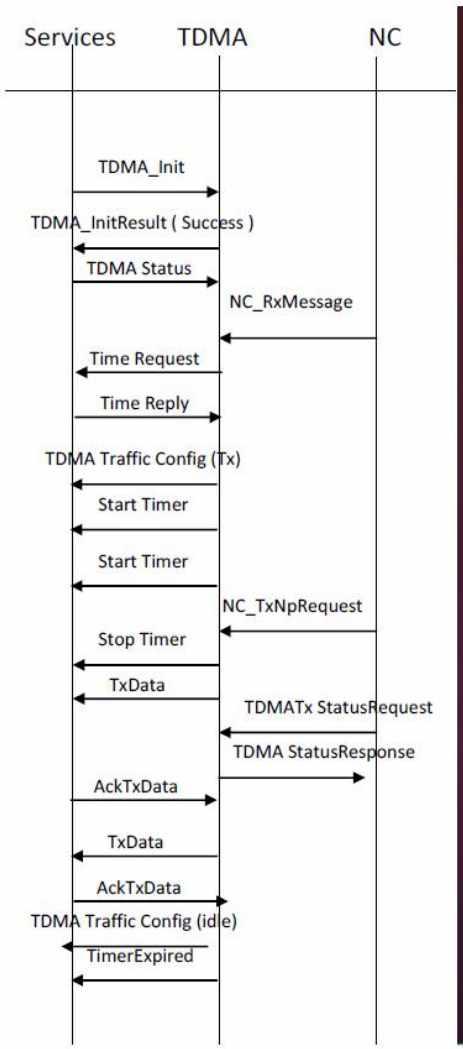

MSC Diagrams
Diagram Edit Search View Export Windows Help
Property.rdd
instance_1
instance_2
e:m1
alt
r:m2
f:m4
MSC Diagrams
Diagram Edit Search View Export Windows Help
Trace.rdd
Cut
instance_1
instance_2
m1
m2
m1
m4
Diagram differences
Property matched 1 times and violated 1 times.
Highlight: Current All
Property match
1 / 2
Close

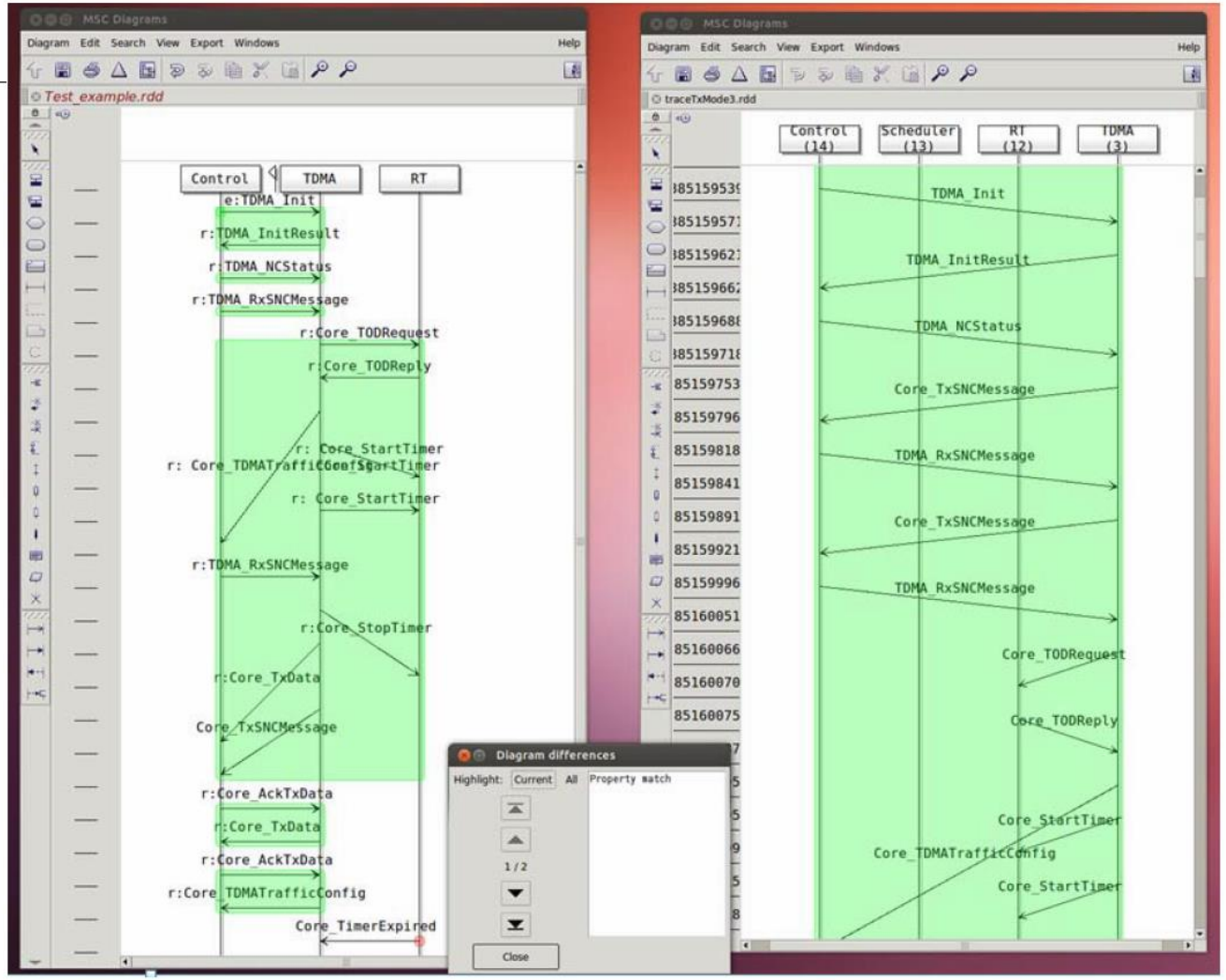

MSC Diagrams
Diagram Edit Search View Export Windows Help
Property.rdd
instance_1
instance_2
e:m1
alt
r:m2
f:m4
MSC Diagrams
Diagram Edit Search View Export Windows Help
Trace.rdd
instance_1
instance_2
m1
m2
m1
m4
Diagram differences
Property matched 1 times and violated 1 times.
Highlight: Current All
Violated property!!!
2 / 2
Close

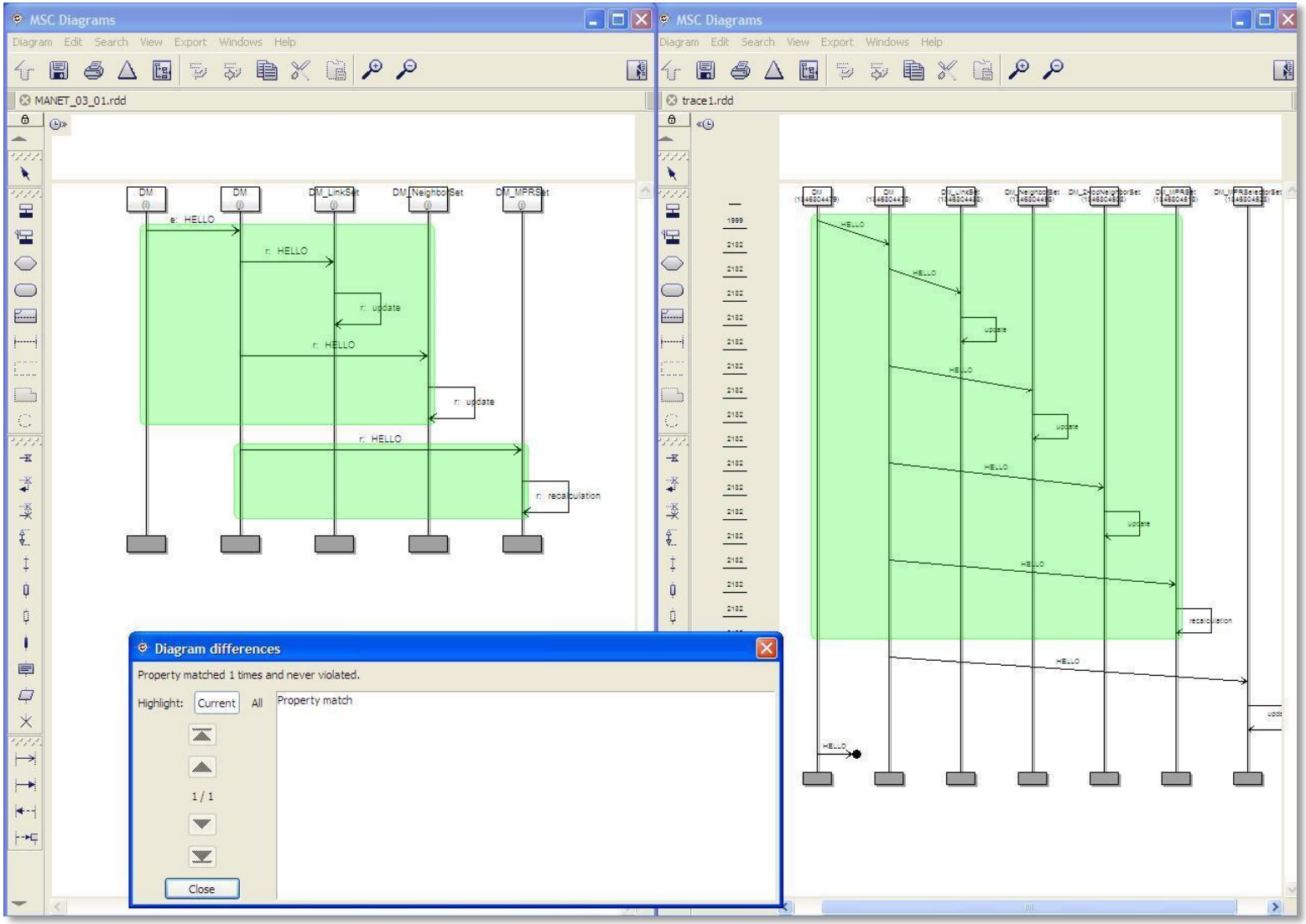

MSC Diagrams
Diagram Edit Search View Export Windows Help
Property.rdd
A
B
e: m1
[=\=> A.m2.B] r: m3
MSC Diagrams
Diagram Edit Search View Export Windows Help
Trace.rdd
A
B
m1
m2
m3
m1
m4
m3
Diagram differences
Property matched 1 times and never violated.
Highlight: Current All
Property match
1 / 1
Close

Use cases

- Thales Communications & Security - France
  - Software Defined Radio (SDR) system
  - TDMA MAC layer
- Thales - Italy
  - Mobile Ad Hoc Network (MANET) in support of the Ultra-Wide Band (UWB) positioning system
  - Selected component: OLSR (Optimized Link State Routing) level-3 network protocol


Services
TDMA
NC
TDMA_Init
TDMA_InitResult (Success)
TDMA Status
NC_RxMessage
Time Request
Time Reply
TDMA Traffic Config (Tx)
Start Timer
Start Timer
NC_TxNpRequest
Stop Timer
TxData
TDMATx StatusRequest
TDMA StatusResponse
AckTxData
TxData
AckTxData
TDMA Traffic Config (idle)
TimerExpired


MSC Diagrams
Diagram Edit Search View Export Windows Help
Test_example.rdd
Control
TDMA
RT
e:TDMA_Init
r:TDMA_InitResult
r:TDMA_NCStatus
r:TDMA_RxSNCMessage
r:Core_TODRequest
r:Core_TODReply
r: Core_StartTimer
r: Core_TDMATrafficConfig
r: Core_StartTimer
r:TDMA_RxSNCMessage
r:Core_StopTimer
r:Core_TxData
Core_TxSNCMessage
r:Core_AckTxData
r:Core_TxData
r:Core_AckTxData
r:Core_TDMATrafficConfig
Core_TimerExpired
Diagram differences
Highlight: Current All
Property match
1/2
Close
MSC Diagrams
Diagram Edit Search View Export Windows Help
traceTxMode3.rdd
Control (14)
Scheduler (13)
RT (12)
TDMA (3)
TDMA_Init
TDMA_InitResult
TDMA_NCStatus
Core_TxSNCMessage
TDMA_RxSNCMessage
Core_TxSNCMessage
TDMA_RxSNCMessage
Core_TODRequest
Core_TODReply
Core_StartTimer
Core_TDMATrafficConfig
Core_StartTimer


MSC Diagrams
Diagram Edit Search View Export Windows Help
MANET_03_01.rdd
DM
DM_LinkSet
DM_NeighborSet
DM_MPRSet
s: HELLO
r: HELLO
r: update
r: HELLO
r: update
r: HELLO
r: recalculation
Diagram differences
Property matched 1 times and never violated.
Highlight: Current All
Property match
1 / 1
Close
MSC Diagrams
Diagram Edit Search View Export Windows Help
trace1.rdd
HELLO
update
recalculation