Newcastle University
UK | Malaysia | Singapore

Model-based SoS Engineering with the COMPASS project

SEVENTH FRAMEWORK PROGRAMME

COMPASS

www.compass-research.eu

Outline

Newcastle University
UK | Malaysia | Singapore

COMPASS

- Systems of systems (SoS)
- The COMPASS Project
  - The COMPASS SoS Engineering Approach
  - Requirements Engineering
  - Architectural Modelling
  - Formal Modelling

Outline

Newcastle University
UK | Malaysia | Singapore

COMPASS

- **Systems of systems (SoS)**
- The COMPASS Project
  - The COMPASS SoS Engineering Approach
  - Requirements Engineering
  - Architectural Modelling
  - Formal Modelling

Defining systems of systems

Newcastle University
UK | Malaysia | Singapore

COMPASS

A system composed of other constituents, each of which is an independent system in its own right

- Operationally & managerially independent constituents
- Geographically distributed
- Continuously evolving
- Exhibiting emergent behaviour

"emergent": global behaviour produced by the whole SoS, can't be produced by a single constituent alone

Systems of systems

Newcastle University
UK | Malaysia | Singapore

COMPASS

Key challenges for modelling SoSs:

- Difficulty of analysing compositions/emergent behaviour
- Wide range of properties to model: functionality, concurrency, communication, inheritance, time, sharing, mobility…
- Lack of full disclosure between constituents: imprecise & uncertain information about “black boxes”
- Heterogeneity – different modelling paradigms in one SoS

Outline

Newcastle University
UK | Malaysia | Singapore

COMPASS

- Systems of systems (SoS)
- **The COMPASS Project**
  - The COMPASS SoS Engineering Approach
  - Requirements Engineering
  - Architectural Modelling
  - Formal Modelling

COMPASS

COMPASS

- Comprehensive Modelling for Advanced Systems of Systems
- EU Framework 7; October 2011 - October 2014

Newcastle University

AARHUS UNIVERSITET

THE UNIVERSITY of York

Universität Bremen

UNIVERSIDADE FEDERAL DE PERNAMBUCO

insiel

BANG & OLUFSEN

atego™

COMPASS case studies

Newcastle University
UK | Malaysia | Singapore

Audio-visual/Home Automation:

- Multiple content sources, DRMs,
- Multiple devices
- Mobile and concurrent systems

Bang & Olufsen (Denmark): Can we ensure consistent "user experience" as devices, content, DRM, etc., change?

Smart Grid:

- Many stakeholders with different needs
- Frequent changes to equipment and stakeholder needs.
- Safety cannot be guaranteed centrally

GridManager (Denmark): Ensure continuity of service & safety in the presence of change & faults?

Traffic Management:

- Wide variety of constituent systems: some legacy, some new
- Harsh physical environment
- Complex integration of new systems and architectures
- Faults & Fault Tolerance

West Consulting (Netherlands): How can we add new/evolved constituent systems, and be sure that they will integrate seamlessly?

Emergency Response:

- Stakeholders (patients to gov't departments)
- Human intervention required for many interactions
- Assurance of global performance and security properties

Insiel (Italy): Can we manage evolution to a decentralised SoS while gaining assurance of global properties?

COMPASS SoS Engineering Challenges

Newcastle University
UK | Malaysia | Singapore

COMPASS

COMPASS focused on three major technical challenges:

- Independence and autonomy of constituent systems
  - Constituent systems evolve at the behest of their owners
  - *Response: Collaborative SoS modelling by contractual (rely, guarantee) interface specification*
- Complexity of confirming/refuting SoS-level properties
  - Verification of emergence
  - *Response: verified refinement for engineering of emergent properties; simulation tools allow exploration for unanticipated behaviours*
- Semantic heterogeneity (integrating models)
  - Wide range of interacting features in models (e.g. location, time, concurrency, data, communication)
  - *Response: extensible semantic basis*

Outline

Newcastle University
UK | Malaysia | Singapore

COMPASS

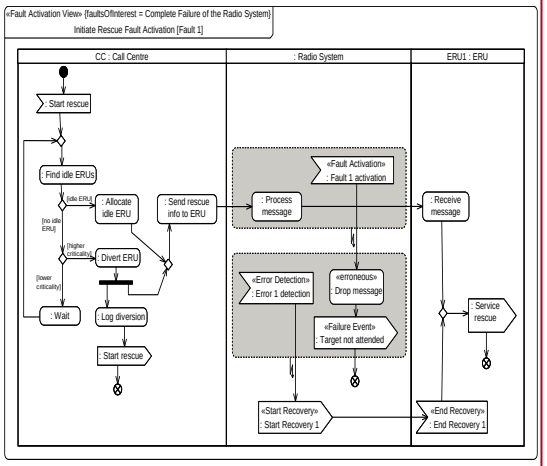
- Systems of systems (SoS)
- **The COMPASS Project**
  - **The COMPASS SoS Engineering Approach**
  - Requirements Engineering
  - Architectural Modelling
  - Formal Modelling

COMPASS Technology

Newcastle University
UK | Malaysia | Singapore

COMPASS

This is what a user of COMPASS technology sees



Semi-formal Modelling

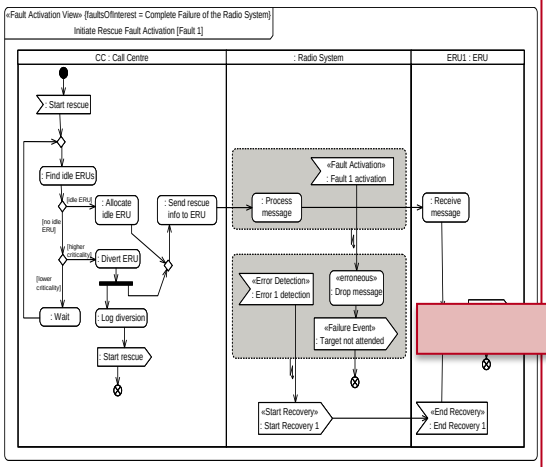
- SysML used for SoS modelling
- Guidelines for Requirements, Architecture, Integration
- SoS modelling profiles
- Architectural patterns and extensible frameworks

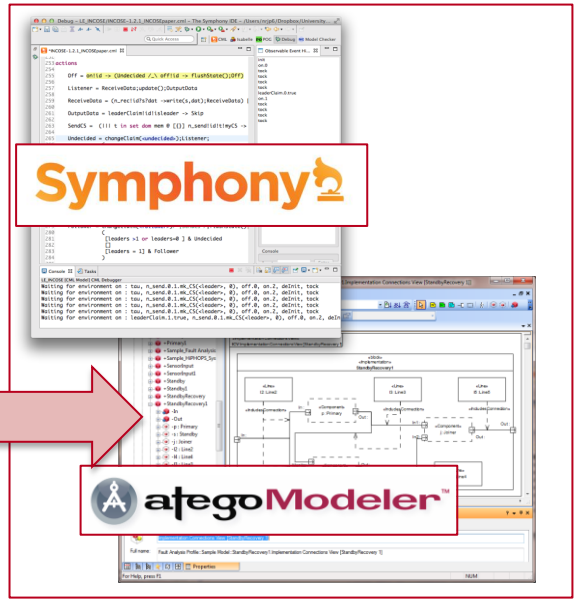
COMPASS Technology

Newcastle University
UK | Malaysia | Singapore

COMPASS

This is what a user of COMPASS technology sees





Semi-formal Modelling

- SysML used for SoS modelling
- Guidelines for Requirements, Architecture, Integration
- SoS modelling profiles
- Architectural patterns and extensible frameworks

Tool-supported Analysis

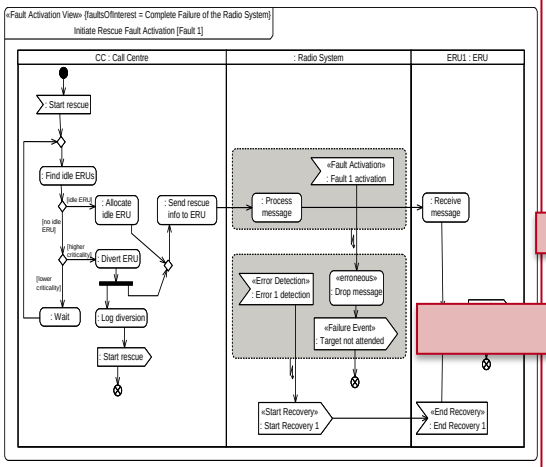
- Model-checker
- Automated proof
- Static Fault Analysis
- Test generation
- Simulation
- Model-in-Loop Test
- Exploration of design space

COMPASS Technology

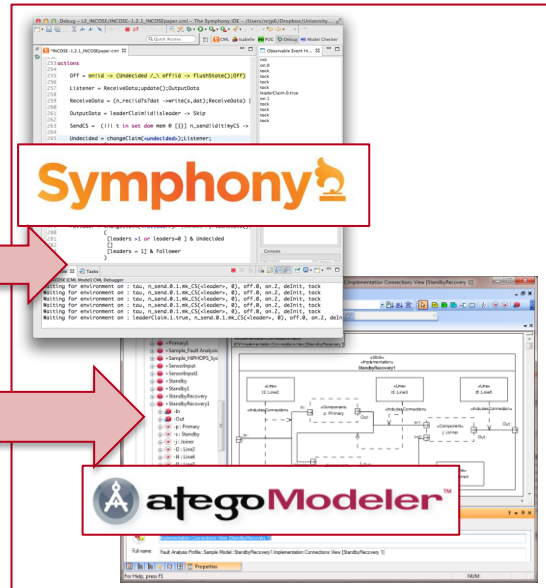
Newcastle University
UK | Malaysia | Singapore

COMPASS

This is what a user of COMPASS technology sees




```
process CallCentreProc = begin
...
actions
 MERGE1(r) =
  (dcl e: set of ERUId @ e := findIdleERUs();
   (do
     e = {} -> DECISION2(r)
     |
     e <> {} ->
      (dcl e1: ERUId @ e1 :=
       allocateIdleERU(e, r); MERGE2(e1, r))

process InitiateRescue = CallCentreProc
          [| SEND_CHANNELS |] RadioSystemProc
          [| RCV_CHANNELS |] ERUsProc
```



Semi-formal Modelling

- SysML used for SoS modelling
- Guidelines for Requirements, Architecture, Integration
- SoS modelling profiles
- Architectural patterns and extensible frameworks

Formal Modelling

- CML allows representation of behavioural semantics of the SoS
- Supports contract specification
- Describes functionality, object-orientation, concurrency, real-time, mobility.
- Can be extended to new paradigms

Tool-supported Analysis

- Model-checker
- Automated proof
- Static Fault Analysis
- Test generation
- Simulation
- Model-in-Loop Test
- Exploration of design space

COMPASS SoS Technologies

Newcastle University
UK | Malaysia | Singapore

Technology	Method /Tool
SoS-ACRE Requirement Eng.	M
COMPASS AF Framework	M
Integration Framework	M
Refinement Framework	M
Interface Pattern	M
Test Pattern	M
Contract Pattern	M
Traceability Pattern	M
Fault Modelling Architectural Framework	M
CML Language	M
Formal Refinement	M
Compositional Analysis	M

Technology	Method /Tool
Compositional Design	M
Specialised Test Strategies	T
Symphony Interpreter	T
Symphony Model Checker	T
Symphony Theorem Prover	T
Symphony RT-Tester	T
Symphony Test Automation	T
Symphony Co-Simulation Engine	T
Symphony Linkage to Executable	T
Fault Analysis Tool	T

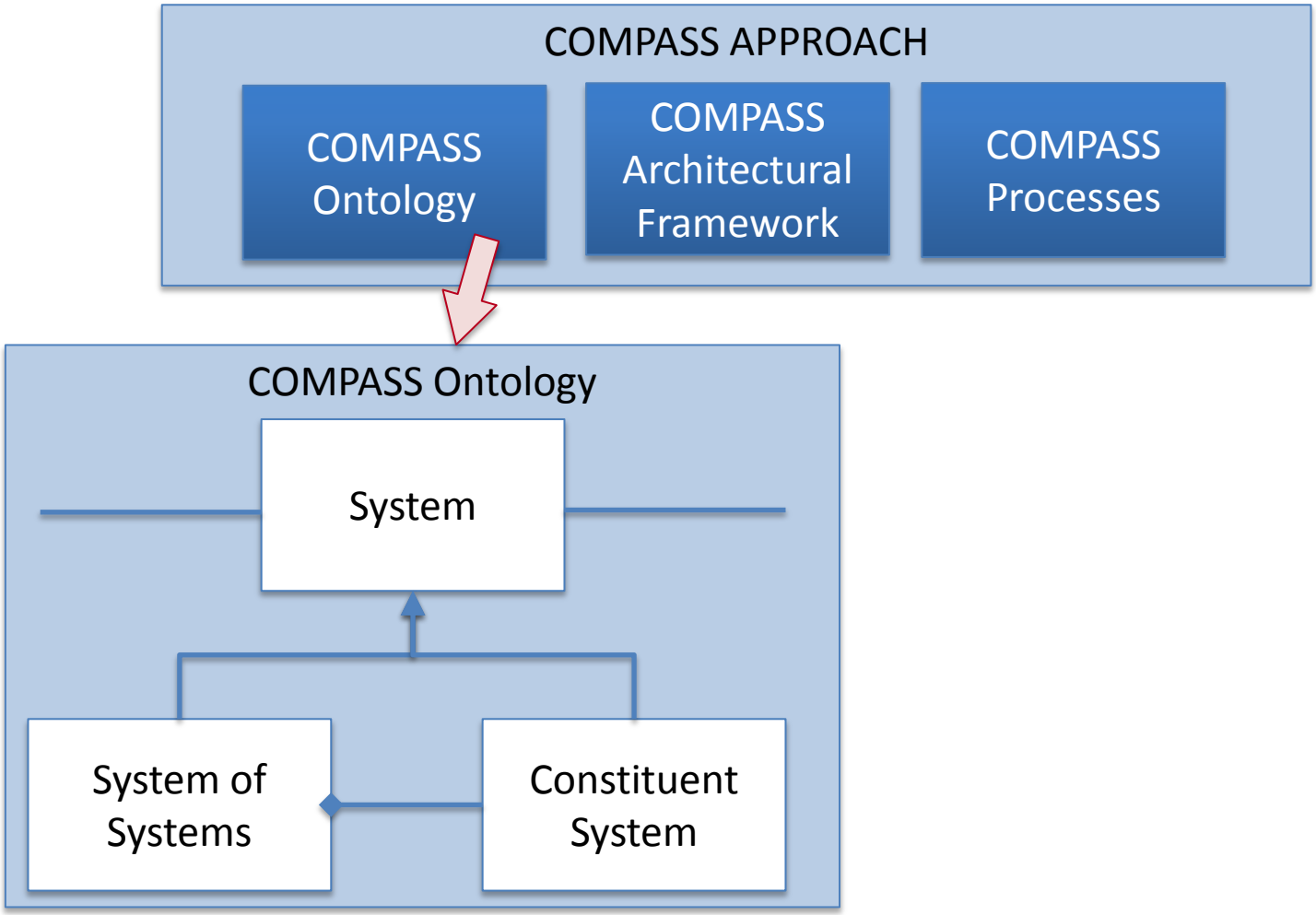
COMPASS SoS Technologies

Newcastle University
UK | Malaysia | Singapore

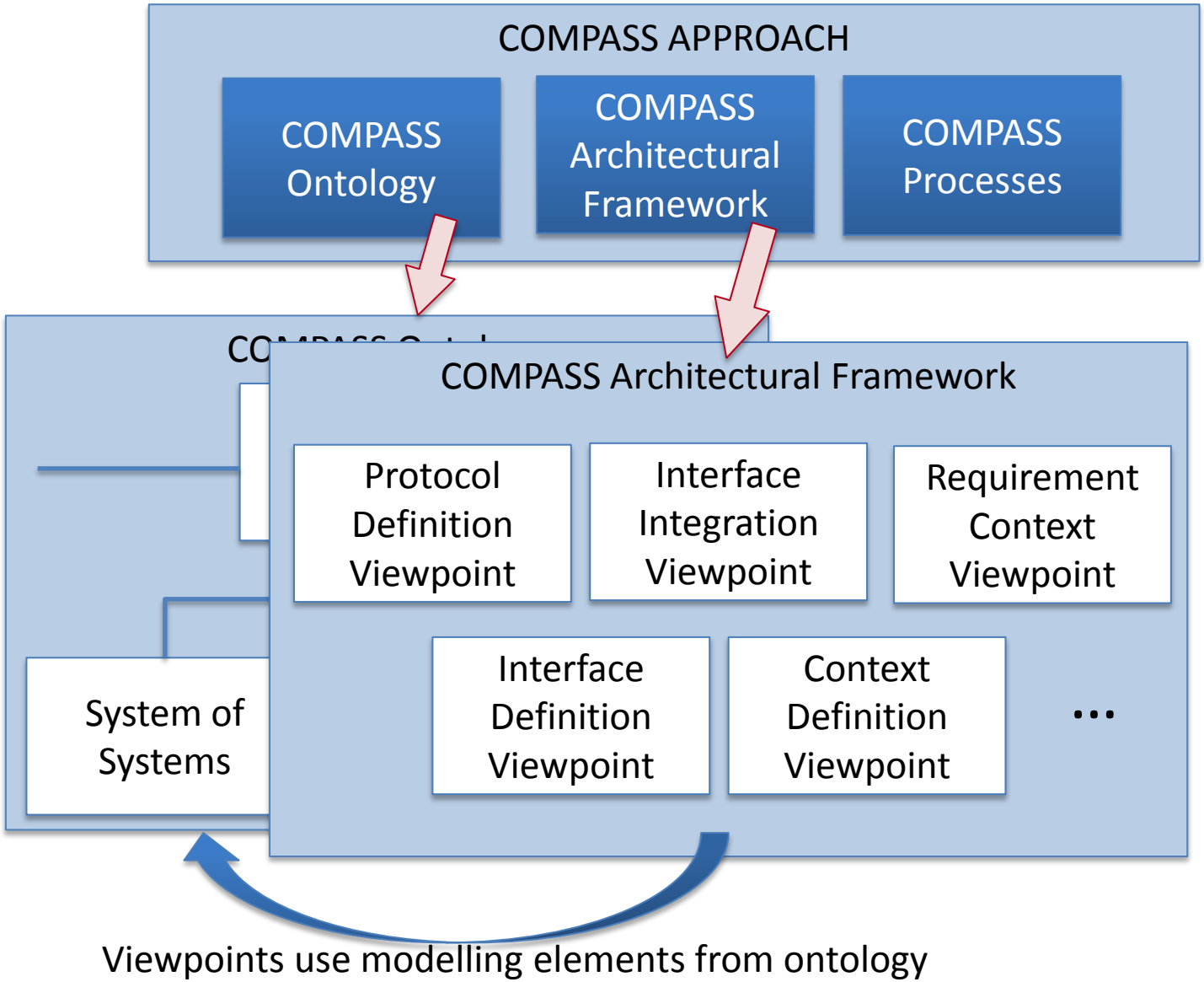
Technology	Method /Tool
SoS-ACRE Requirement Eng.	**M**
COMPASS AF Framework	**M**
Integration Framework	M
Refinement Framework	M
Interface Pattern	M
Test Pattern	M
Contract Pattern	**M**
Traceability Pattern	M
Fault Modelling Architectural Framework	**M**
CML Language	**M**
Formal Refinement	M
Compositional Analysis	M

Technology	Method /Tool
Compositional Design	M
Specialised Test Strategies	T
Symphony Interpreter	T
Symphony Model Checker	T
Symphony Theorem Prover	T
Symphony RT-Tester	T
Symphony Test Automation	T
Symphony Co-Simulation Engine	T
Symphony Linkage to Executable	T
Fault Analysis Tool	T

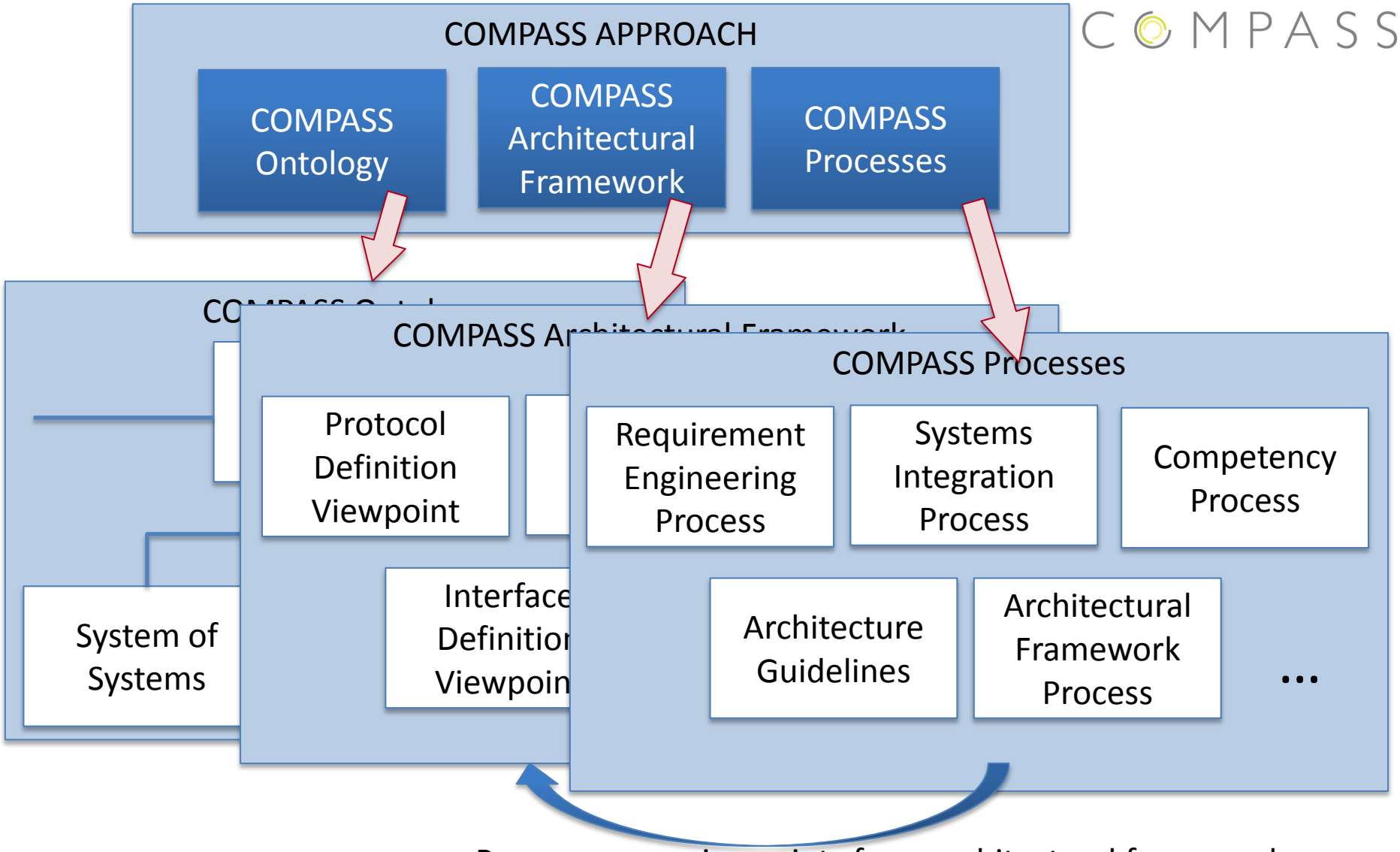
COMPASS Approach



COMPASS Approach



COMPASS Approach



Processes use viewpoints from architectural framework

Outline

Newcastle University
UK | Malaysia | Singapore

COMPASS

- Systems of systems (SoS)
- Model-based SoS Engineering
- **The COMPASS Project**
  - The COMPASS SoS Engineering Approach
  - **Requirements Engineering**
  - Architectural Modelling
  - Formal Modelling
  - Verification and Analysis
  - Fault Modelling

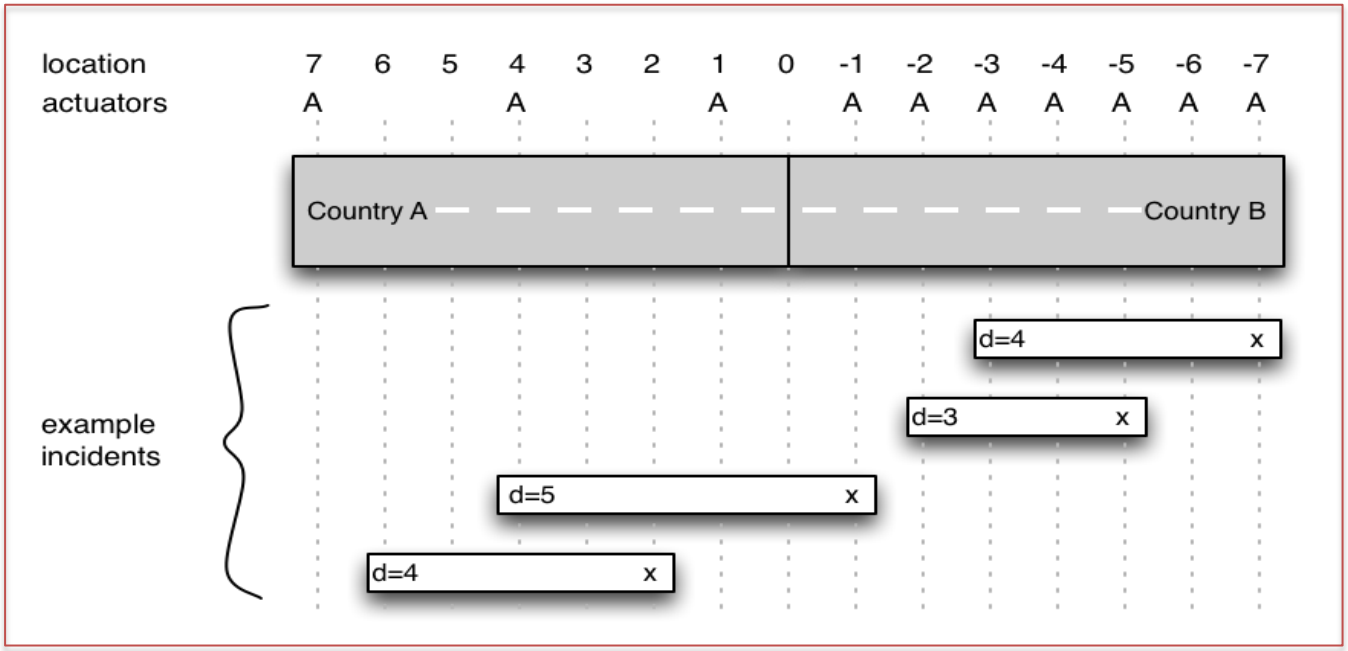
SoS Engineering Example

Newcastle University
UK | Malaysia | Singapore

COMPASS

- Cross-border traffic control
- Incident in one country may require “corridor” with temporary traffic controls to be established across an international border, in a co-ordinated way
- Need to define contract to which each country adheres
- Driver perceives no difference from one country to another

SoS Engineering Example



- Cross-border traffic control
- Incident in one country may require “corridor” with temporary traffic controls to be established across an international border, in a co-ordinated way
- Need to define contract to which each country adheres
- Driver perceives no difference from one country to another

SoS-ACRE Viewpoints

Newcastle University
UK | Malaysia | Singapore

COMPASS

COMPASS developed SoS-ACRE, a requirements process for SoSs, with the following viewpoints

Viewpoint	Description
Source Element	Identifies requirements source information
Requirement Description	Contains a structured description of each requirement
Context Definition	Identifies the points of view (contexts) which will be explored in the RCVs
Requirement Context	Describes the requirements defined on the RDV in context
Context Interaction	Overview of relationships between the contexts of various CSs; combines the RCVs for each CS
Validation	Provides the basis for demonstrating that requirements can be validated
Validation Interaction	A combined view of the scenarios for related use cases in the SoS; combines the VVs of the use cases

SoS-ACRE Viewpoints

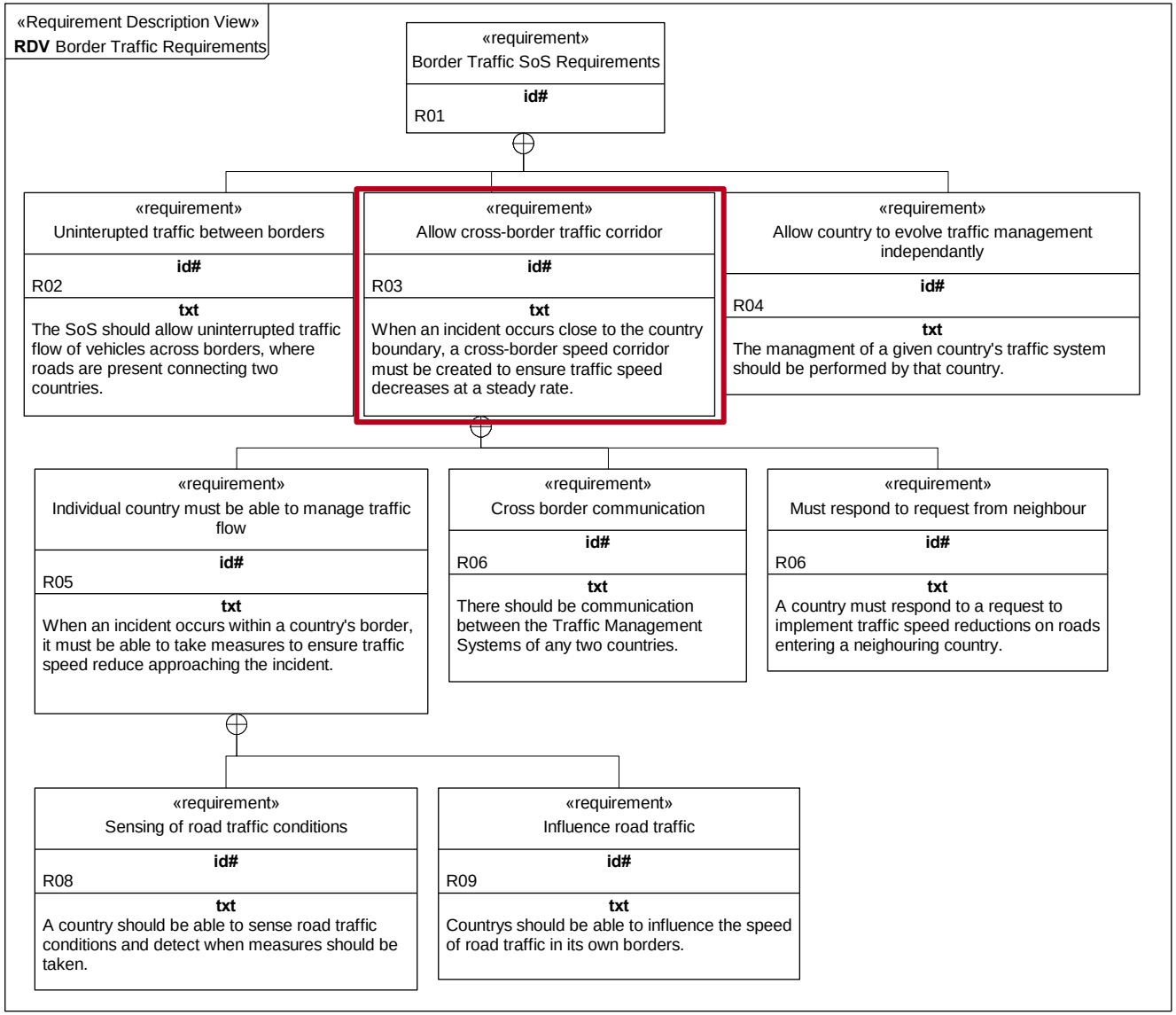
Newcastle University
UK | Malaysia | Singapore

COMPASS

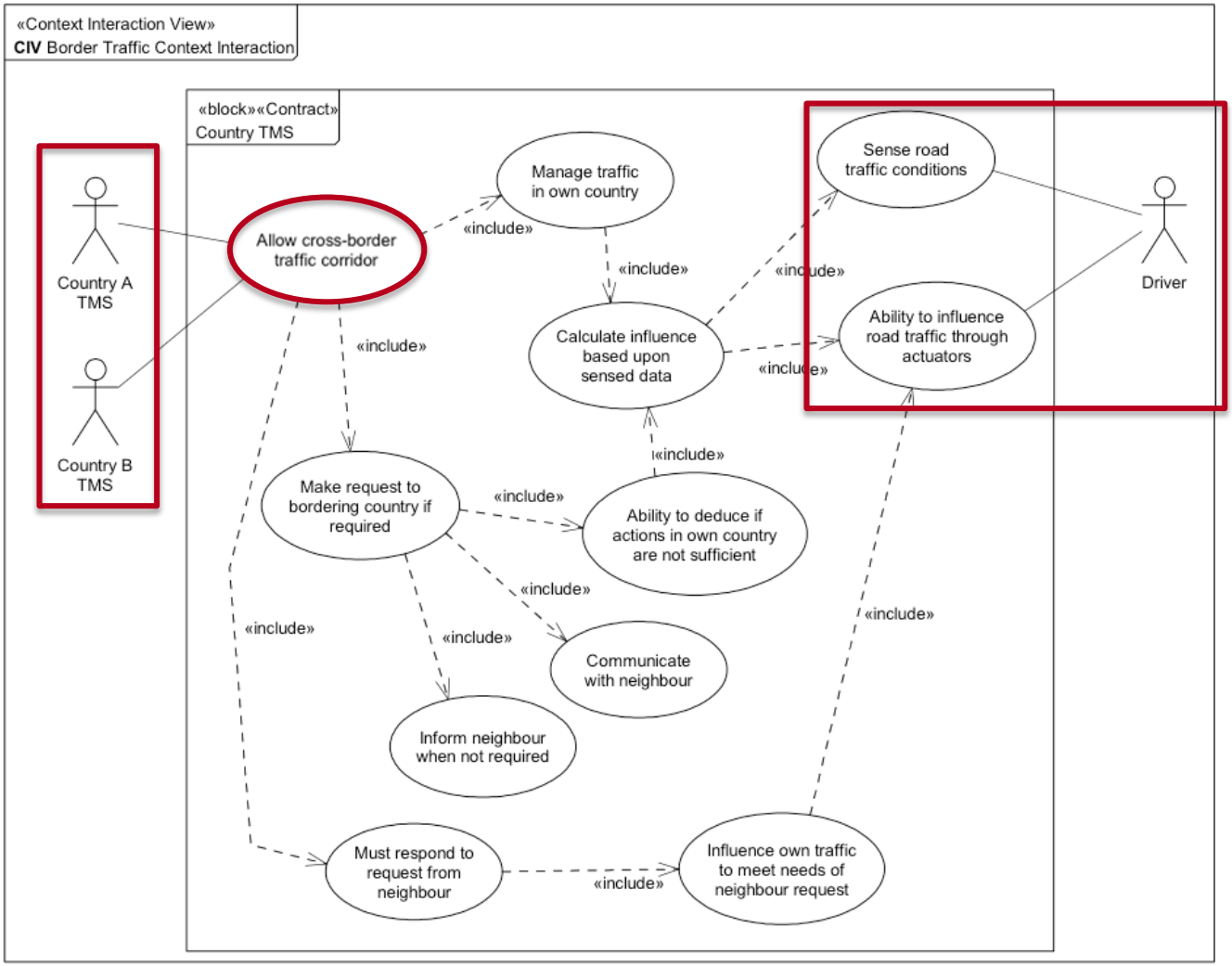
COMPASS developed SoS-ACRE, a requirements process for SoSs, with the following viewpoints

Viewpoint	Description
Source Element	Identifies requirements source information
Requirement Description	**Contains a structured description of each requirement**
Context Definition	Identifies the points of view (contexts) which will be explored in the RCVs
Requirement Context	Describes the requirements defined on the RDV in context
Context Interaction	**Overview of relationships between the contexts of various CSs; combines the RCVs for each CS**
Validation	Provides the basis for demonstrating that requirements can be validated
Validation Interaction	A combined view of the scenarios for related use cases in the SoS; combines the VVs of the use cases

Requirement Definition



Requirements in Context



Outline

Newcastle University
UK | Malaysia | Singapore

COMPASS

- Systems of systems (SoS)
- Model-based SoS Engineering
- **The COMPASS Project**
  - The COMPASS SoS Engineering Approach
  - Requirements Engineering
  - **Architectural Modelling**
  - Formal Modelling

Architectural Modelling

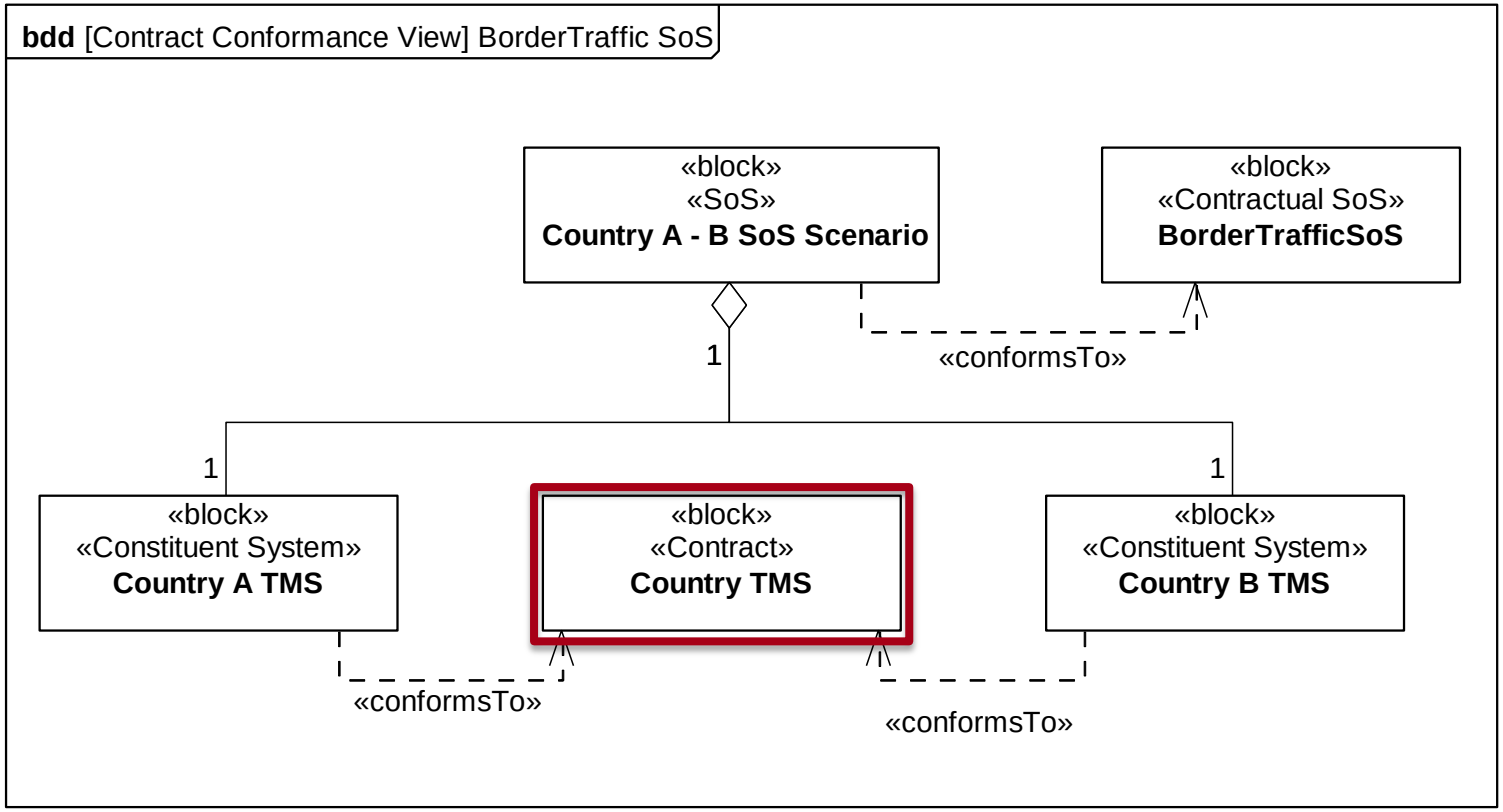
Newcastle University
UK | Malaysia | Singapore

COMPASS

- When defining a SoS architecture, follow COMPASS architectural approach
  - patterns and guidelines
- Use collections of *modelling patterns* to define SoS structure and behaviour
- In border traffic example, we define the behaviour required by each country's TMS – using the *interface contract* pattern

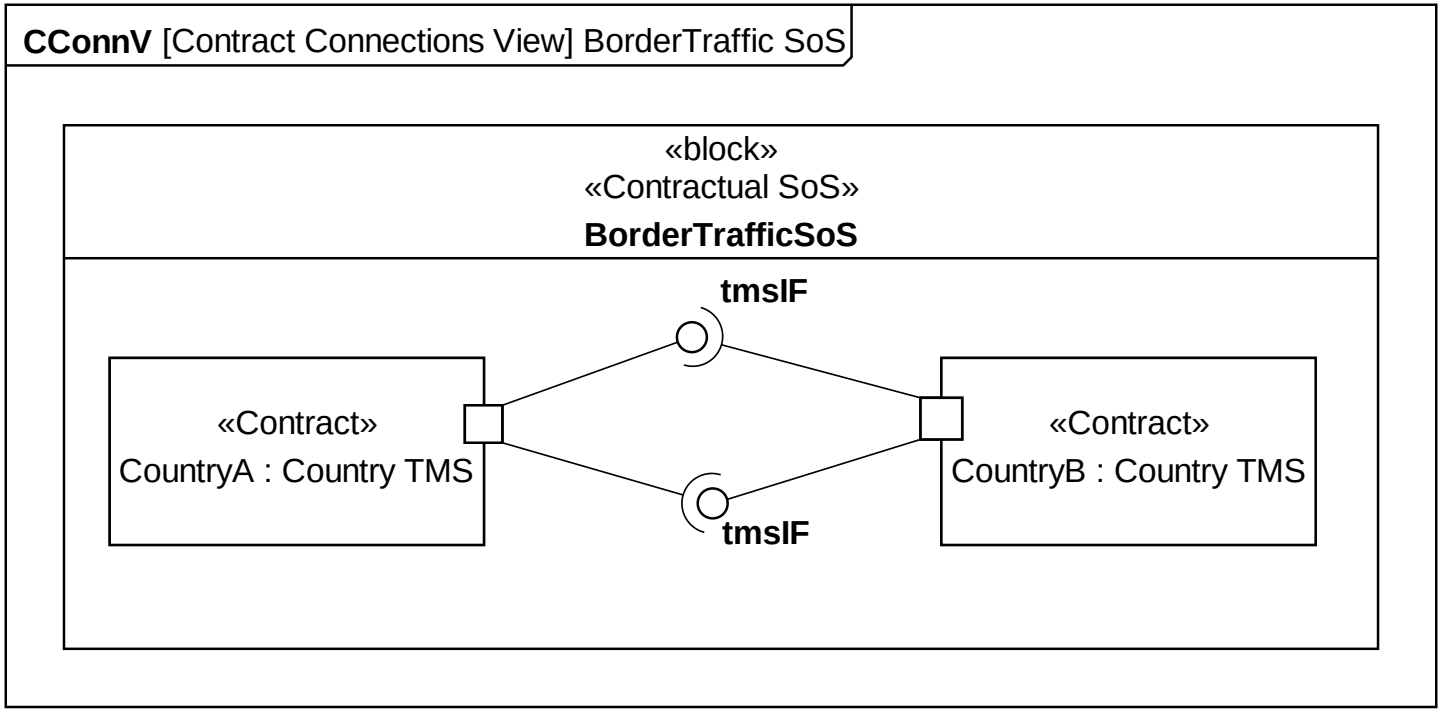
Architectural Modelling

- Identifying contract conformance



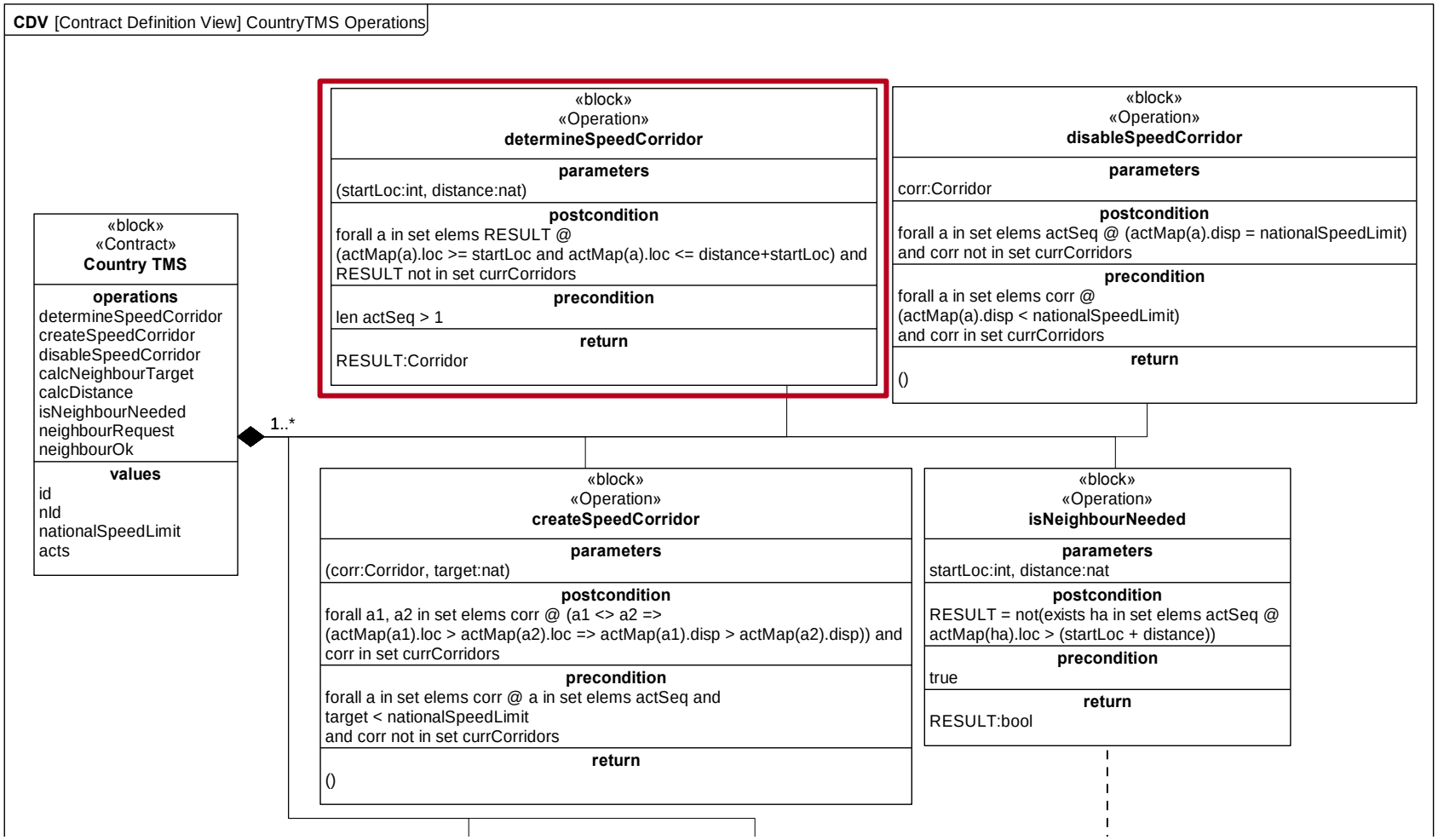
Architectural Modelling

- Defining connections and interfaces between systems



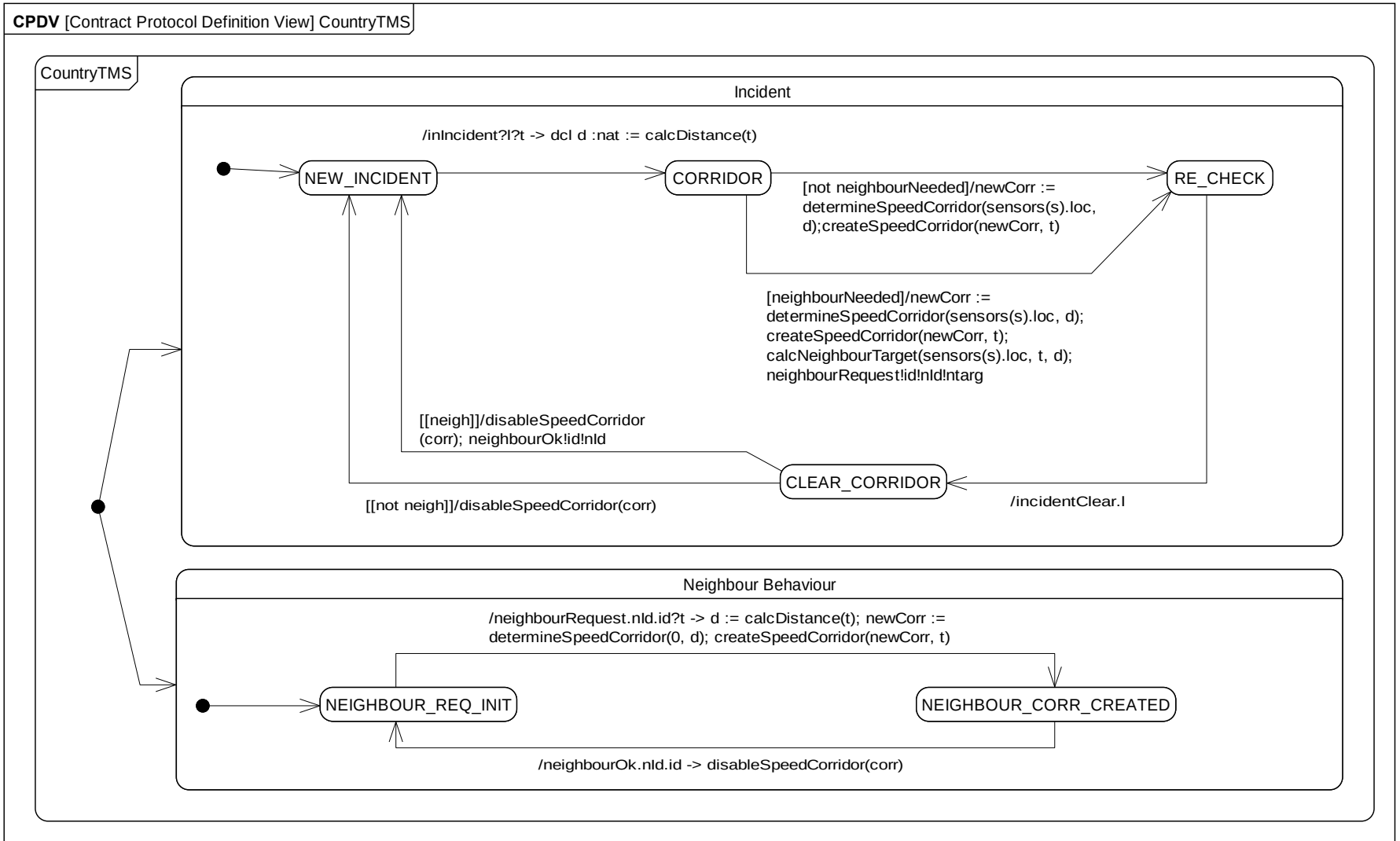
Architectural Modelling

- Defining the functionality of the contract



Architectural Modelling

- Defining behaviour and ordering



Outline

Newcastle University
UK | Malaysia | Singapore

COMPASS

- Systems of systems (SoS)
- Model-based SoS Engineering
- **The COMPASS Project**
  - The COMPASS SoS Engineering Approach
  - Requirements Engineering
  - Architectural Modelling
  - **Formal Modelling**

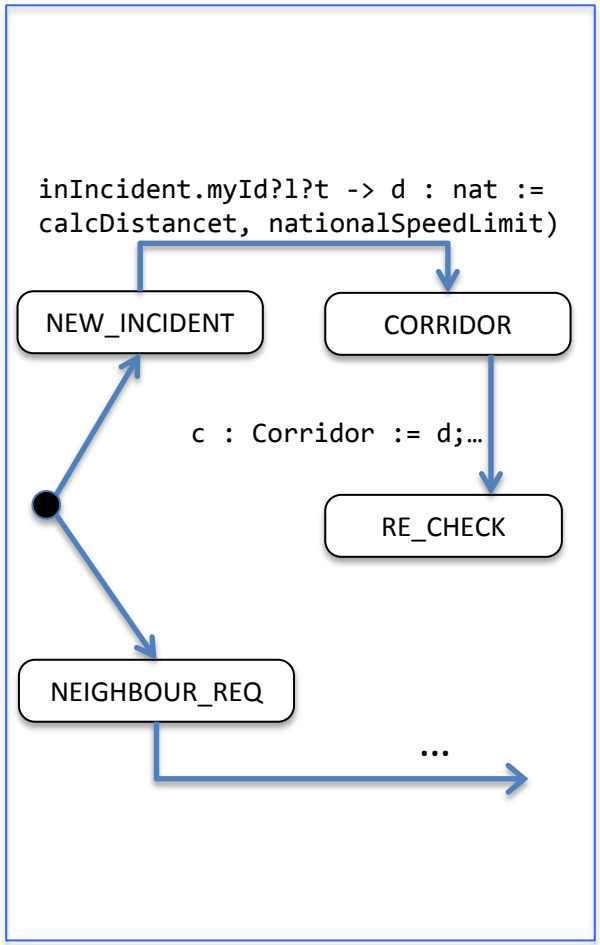
Formal Modelling

Newcastle University
UK | Malaysia | Singapore

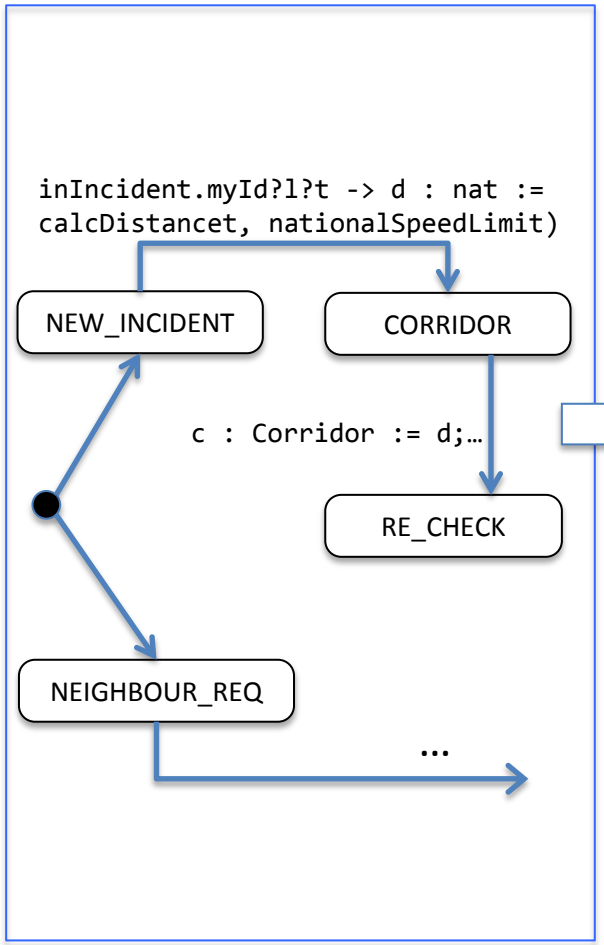
COMPASS

- CML – COMPASS Modelling Language – developed for modelling SoS
- Can model data, functionality, event ordering and communication
  - extensible
- Range of formal analysis techniques
- Tools developed for translating models from SysML into CML

Analysing the Model



Analysing the Model

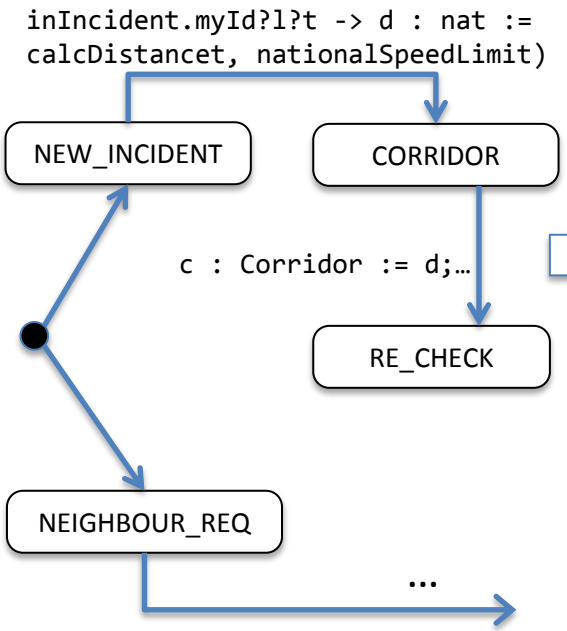



```
process CountryTMS =
begin
  …
  actions
  BEHAVIOUR= NEW_INCIDENT
             []
             NEIGHBOUR_REQ

   NEW_INCIDENT = inIncident.myId?l?t ->
        (dcl d : nat := calcDistance
        (t, nationalSpeedLimit) @
                    CORRIDOR(l, t, d))

   CORRIDOR = l : int, t: nat, d:nat
      @ ACT_STATUS;c:Corridor :=det; …
…
   @ BEHAVIOUR
End

process CountryA = CountryTMS(theAId,
             theBId, limitA, actCorrA)
process CountryB = CountryTMS(theBId,
             theAId, limitB, actCorrB)

process BorderTrafficSoS =
              CountryA [|interface|]
              CountryB
```

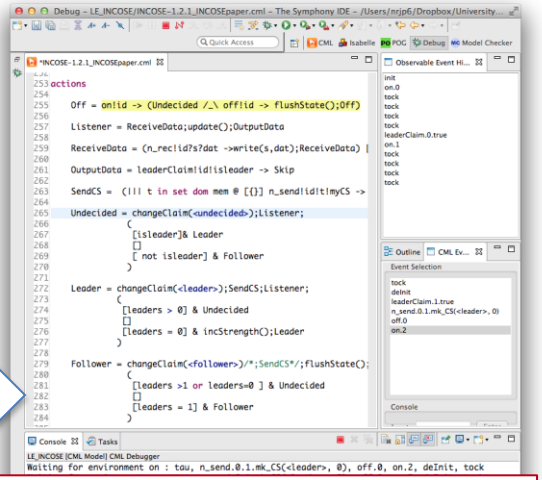
Analysing the Model

Newcastle University
UK | Malaysia | Singapore

COMPASS




```
process CountryTMS =
begin
  …
  actions
  BEHAVIOUR= NEW_INCIDENT
             []
             NEIGHBOUR_REQ

   NEW_INCIDENT = inIncident.myId?l?t ->
        (dcl d : nat := calcDistance
        (t, nationalSpeedLimit) @
                    CORRIDOR(l, t, d))

   CORRIDOR = l : int, t: nat, d:nat
      @ ACT_STATUS;c:Corridor :=det; …
…
   @ BEHAVIOUR
End

process CountryA = CountryTMS(theAId,
            theBId, limitA, actCorrA)
process CountryB = CountryTMS(theBId,
            theAId, limitB, actCorrB)

process BorderTrafficSoS =
             CountryA [|interface|]
             CountryB
```



Symphony

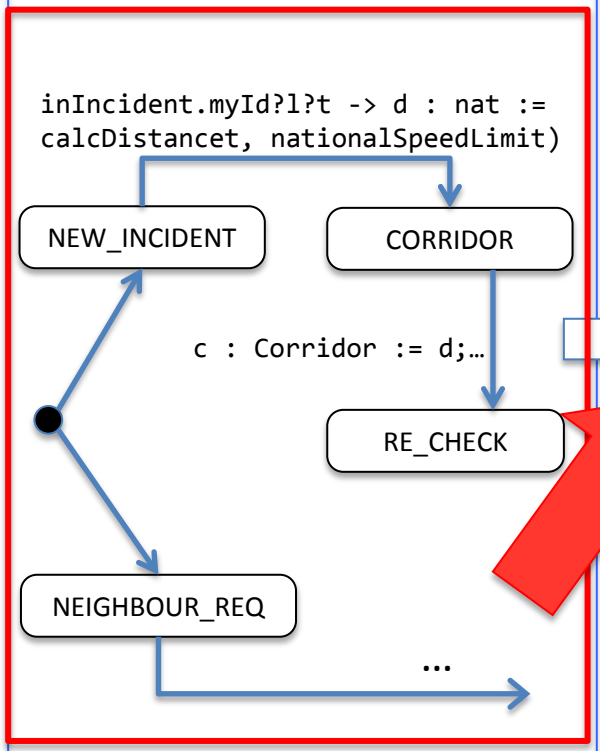
Symphony Tool Platform

- Analyse cross border emergent behaviour
- Simulate execution of model
- Proof obligations generated
- Theorem proving

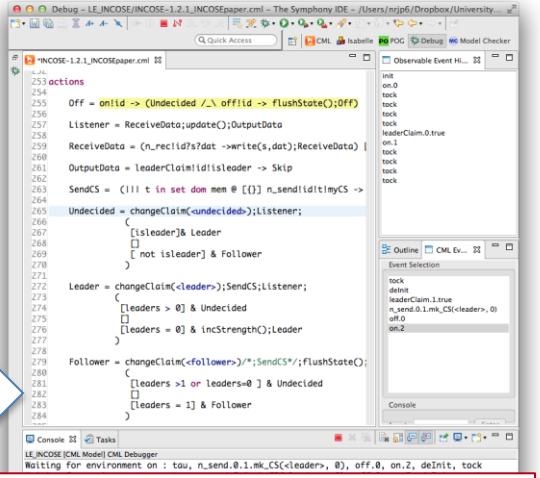
Analysing the Model

Newcastle University
UK | Malaysia | Singapore

COMPASS




```
process CountryTMS =
begin
  …
  actions
  BEHAVIOUR= NEW_INCIDENT
             []
             NEIGHBOUR_REQ

   NEW_INCIDENT = inIncident.myId?l?t ->
        (dcl d : nat := calcDistance
        (t, nationalSpeedLimit) @
                    CORRIDOR(l, t, d))

   CORRIDOR = l : int, t: nat, d:nat
      @ ACT_STATUS;c:Corridor :=det; …

   @ BEHAVIOUR
End

process CountryA = CountryTMS(theAId,
             theBId, limitA, actCorrA)
process CountryB = CountryTMS(theBId,
             theAId, limitB, actCorrB)

process BorderTrafficSoS =
             CountryA [|interface|]
             CountryB
```



Symphony

Symphony Tool Platform

- Analyse cross border emergent behaviour
- Simulate execution of model
- Proof obligations generated
- Theorem proving

Conclusions

Newcastle University
UK | Malaysia | Singapore

COMPASS

- COMPASS has produced a large set of outputs, including methods, tools and guidelines
  - Based on an extensible approach
  - Benefits integrating both semi-formal and formal modelling
  - A unified model-based approach promotes consistency, rigour, traceability, validation and verification

- Join thecompassclub.org !

Newcastle University
UK | Malaysia | Singapore

COMPASS

Research into model-based techniques for developing, analysing and maintaining SoSs

thecompassclub.org

www.compass-research.eu