Newcastle University
UK | Malaysia | Singapore

Model-based SoS Engineering

Jeremy Bryans and Claire Ingram
Newcastle University

MBSE workshop, Torrance, CA

January 2015

SEVENTH FRAMEWORK PROGRAMME

COMPASS

www.compass-research.eu

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

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

Systems of systems

Newcastle University
UK | Malaysia | Singapore

COMPASS

Defining SoSs:

- Operationally and managerially independent
- Geographically distributed
- Continuously evolving
- Exhibiting emergent behaviour

Degree of central control & CS awareness are often used to "categorise" the SoS

- Directed
- Acknowledged
- Collaborative
- Virtual

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? Vision ...

Newcastle University
UK | Malaysia | Singapore

COMPASS

Methods & Tools for:

- Selecting constituent systems on limited evidence
- Allocating responsibilities
- Managing dependability assumptions
- Providing support for trade-off analysis
- Managing testing of implementations

Challenged by:

- **Managing complexity** of the constituent systems and the SoS;
- **Understanding behaviours and interactions** between constituent systems;
- **Communicating effectively** between diverse stakeholders and constituent systems; and
- **Evidence** on which to base reliance on global end-to-end behaviours.

Model-based SoS Engineering

Newcastle University
UK | Malaysia | Singapore

COMPASS

Potential:

- Effectiveness at addressing complexity e.g. by architectural modelling
- Some industrial support already
- Support for communication between stakeholders & disciplines

Challenged by:

- Operational Independence: black boxes & wrapper derivation
- Managerial Independence: can only *bound* behaviours by contracts
- Evolutionary Development: need basis for re-appraisal
- Emergence: reasoning from compositions

Formally-based SoS Engineering

Newcastle University
UK | Malaysia | Singapore

COMPASS

Potential:

- High level of rigour in analysis
- Wide range of analytic techniques: testing, model-checking, proof
- Cost-effective *if* well supported by tools and applied carefully to important/risky features and *if* integrated

Challenged by:

- SoS need to manage imprecise and uncertain information about constituent systems
  - *We can draw up contracts between constituents (and infrastructure)*
- SoS include functionality, concurrency, communication, inheritance, time, sharing, mobility

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

COMPASS

Newcastle University
UK | Malaysia | Singapore

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

Case studies

Newcastle University
UK | Malaysia | Singapore

A/V/Home Automation:

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

Bang & Olufsen: 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

Service Provider: Can we ensure continuity of service and safety in the presence of change and 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: 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: Can we manage evolution to a decentralised SoS while gaining assurance of global properties?

COMPASS SoS Engineering Challenges

Newcastle University
UK | Malaysia | Singapore

COMPASS

- 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

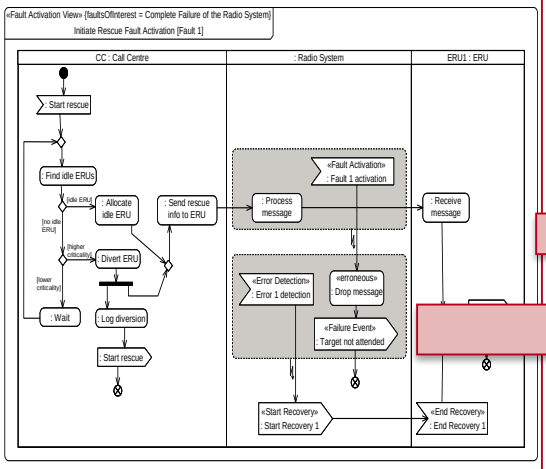
COMPASS

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

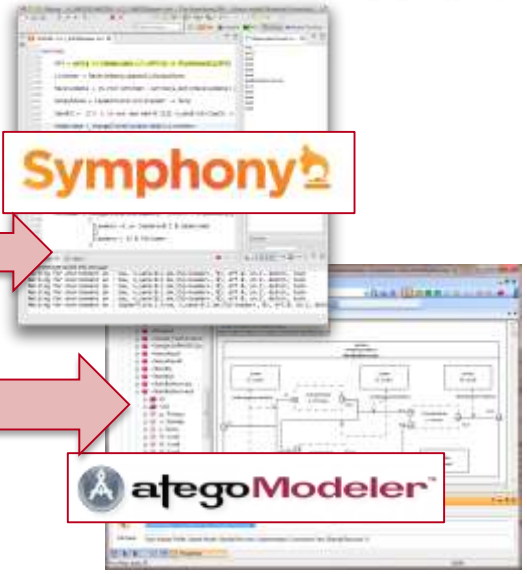
COMPASS Technology

Newcastle University
UK | Malaysia | Singapore

COMPASS




```
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

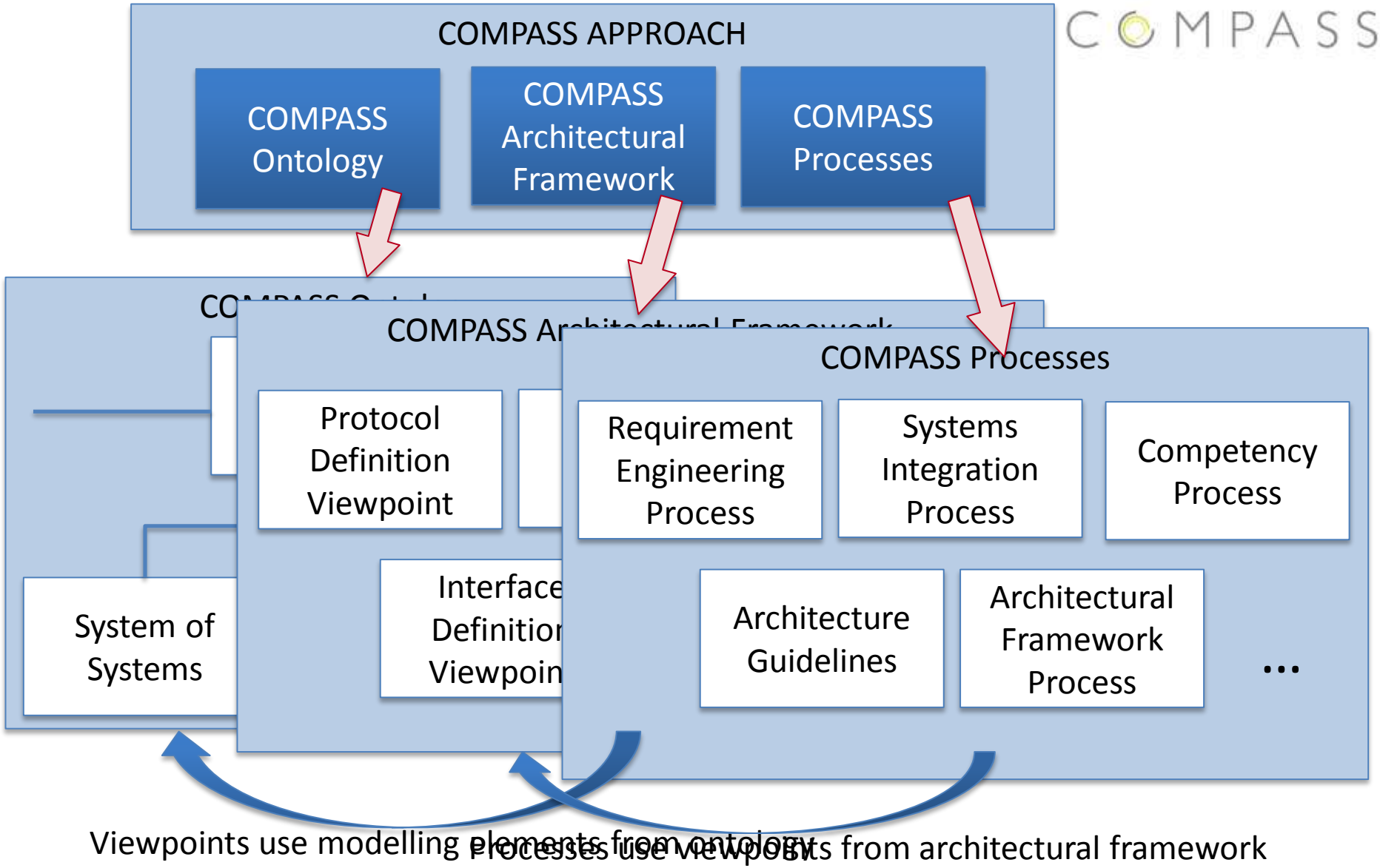
COMPASS SoS Technologies

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 Approach



Outline

Newcastle University
UK | Malaysia | Singapore

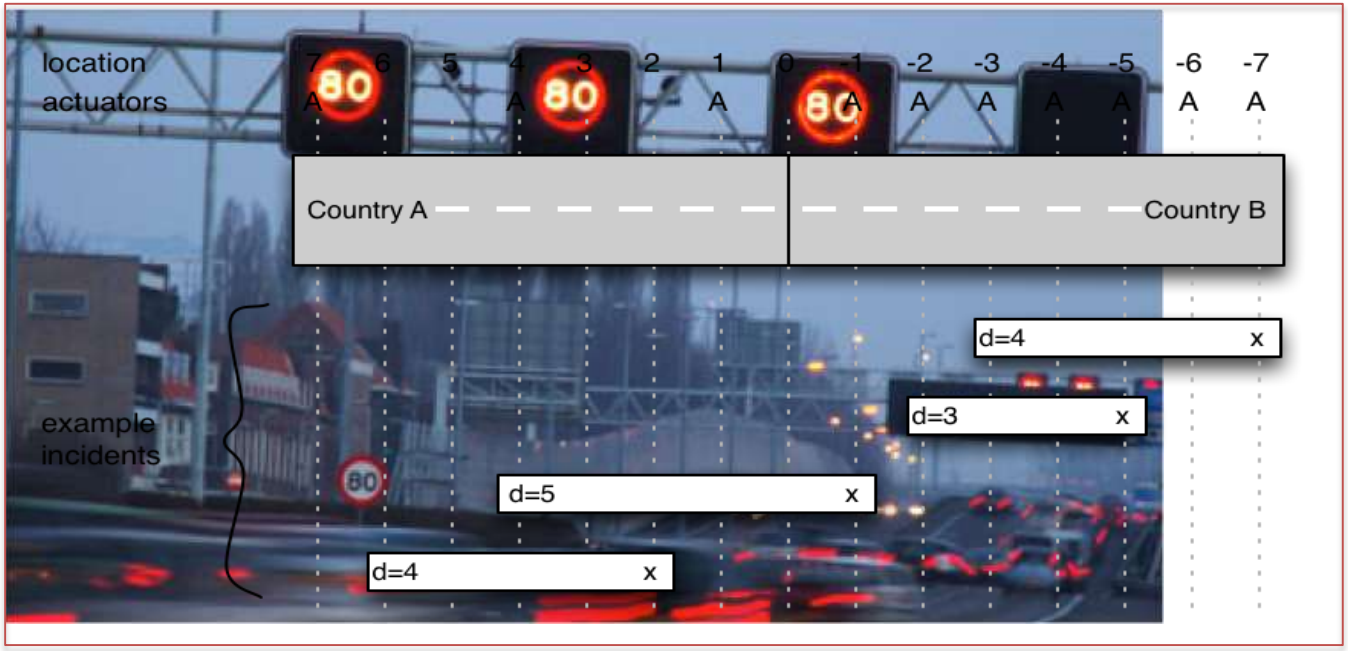
COMPASS

- 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 corridor
- Incident in one country may require corridor across two countries
- Need to define contract to which each country adheres
- Driver perceives no difference

Requirements Engineering: SoS-ACRE

Newcastle University
UK | Malaysia | Singapore

COMPASS

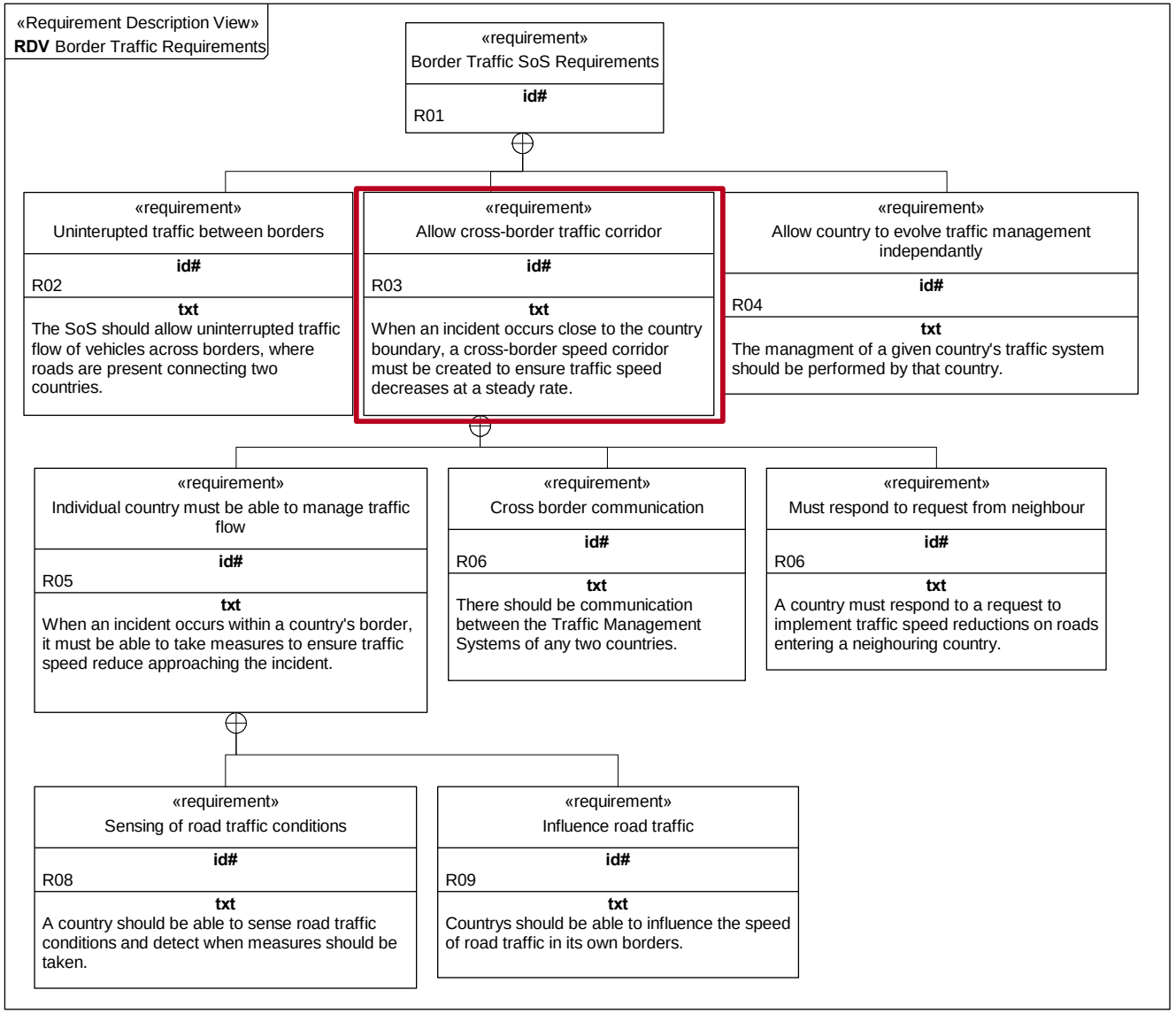
- Guidelines for specification & management of requirements for SoS
  - *Ontology* for model-based reqt. engineering
  - *Framework* containing eight *viewpoints*
  - *Processes* for reqt. engineering and management

- SoS-ACRE requirements engineering process:
  1. Identify source elements of requirements
  2. Identify the constituents and stakeholders of the SoS
  3. Define the SoS requirements
  4. Examine the SoS requirements in context
  5. Identify scenarios for validating the requirements

Requirement Definition

Newcastle University
UK | Malaysia | Singapore

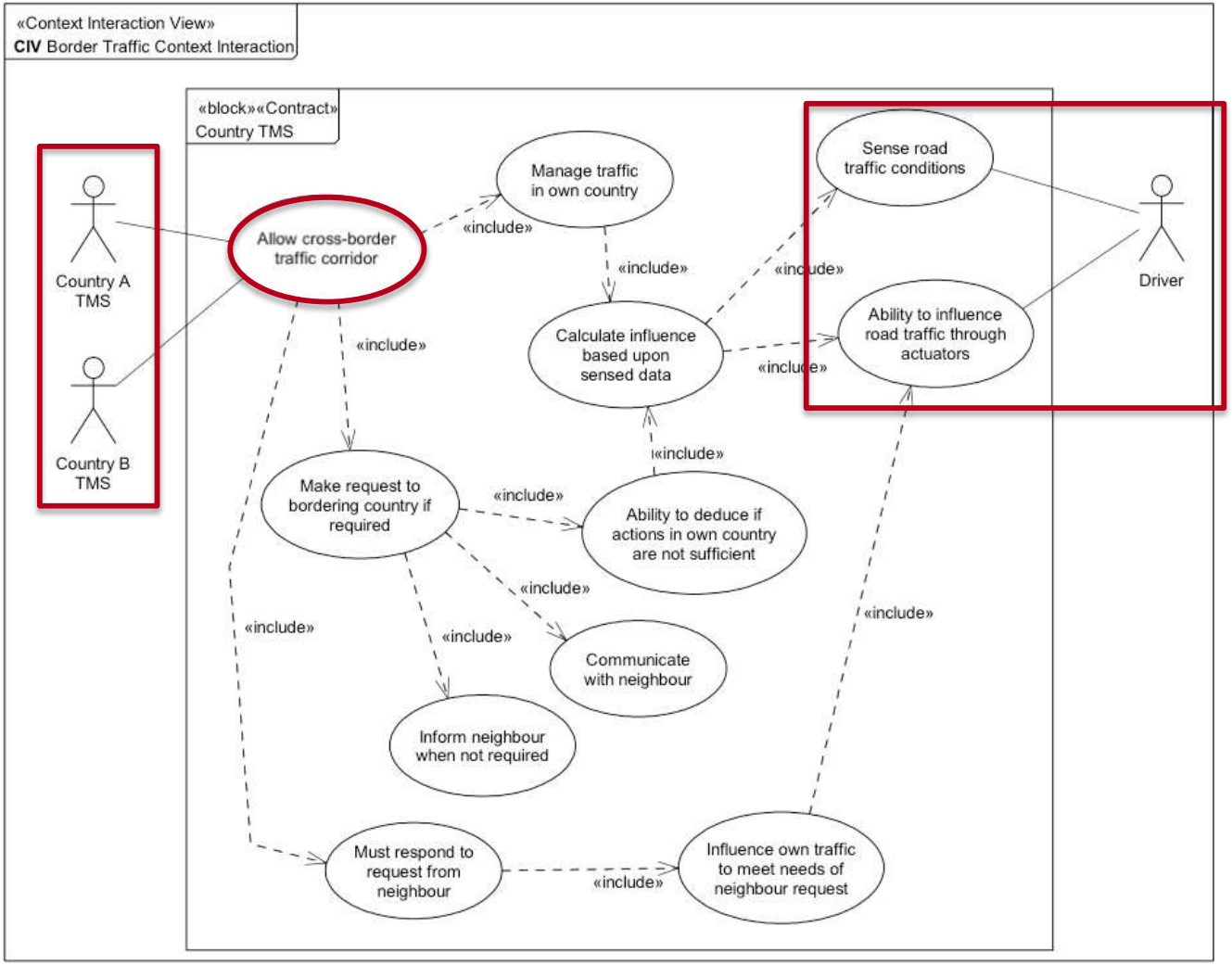
MPASS



Requirements in Context

Newcastle University
UK | Malaysia | Singapore

COMPASS



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

Architectural Modelling

Newcastle University
UK | Malaysia | Singapore

COMPASS

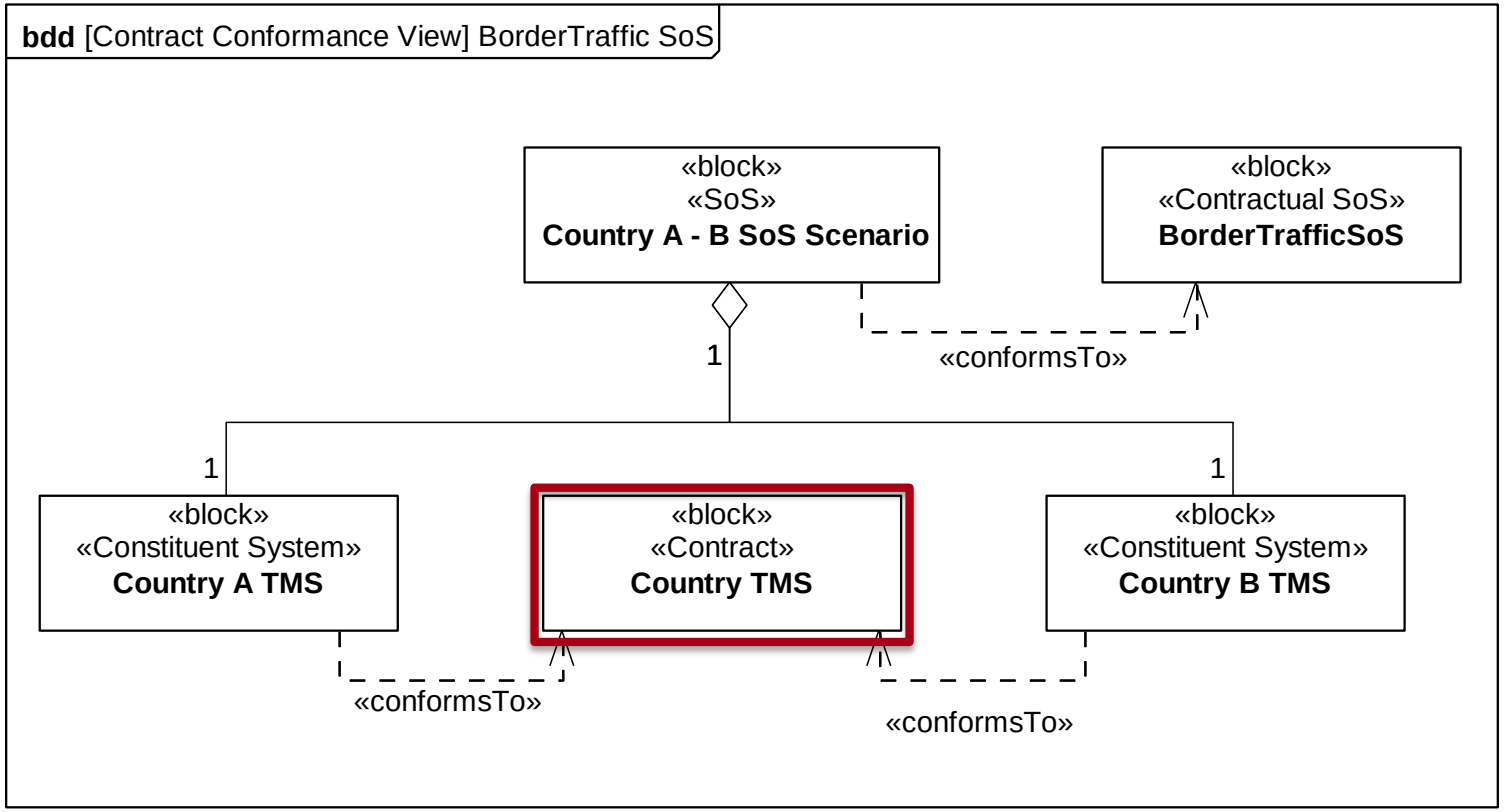
- When defining a SoS architecture, follow COMPASS architectural approach
  - patterns and guidelines
- Use collections of *modelling patterns* to define SoS structure and behaviour
- COMPASS architectural modelling approach also includes *guidelines* for SoS integration and development lifecycles
-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

Architectural Modelling

Newcastle University
UK | Malaysia | Singapore

COMPASS

- Identifying contract conformance

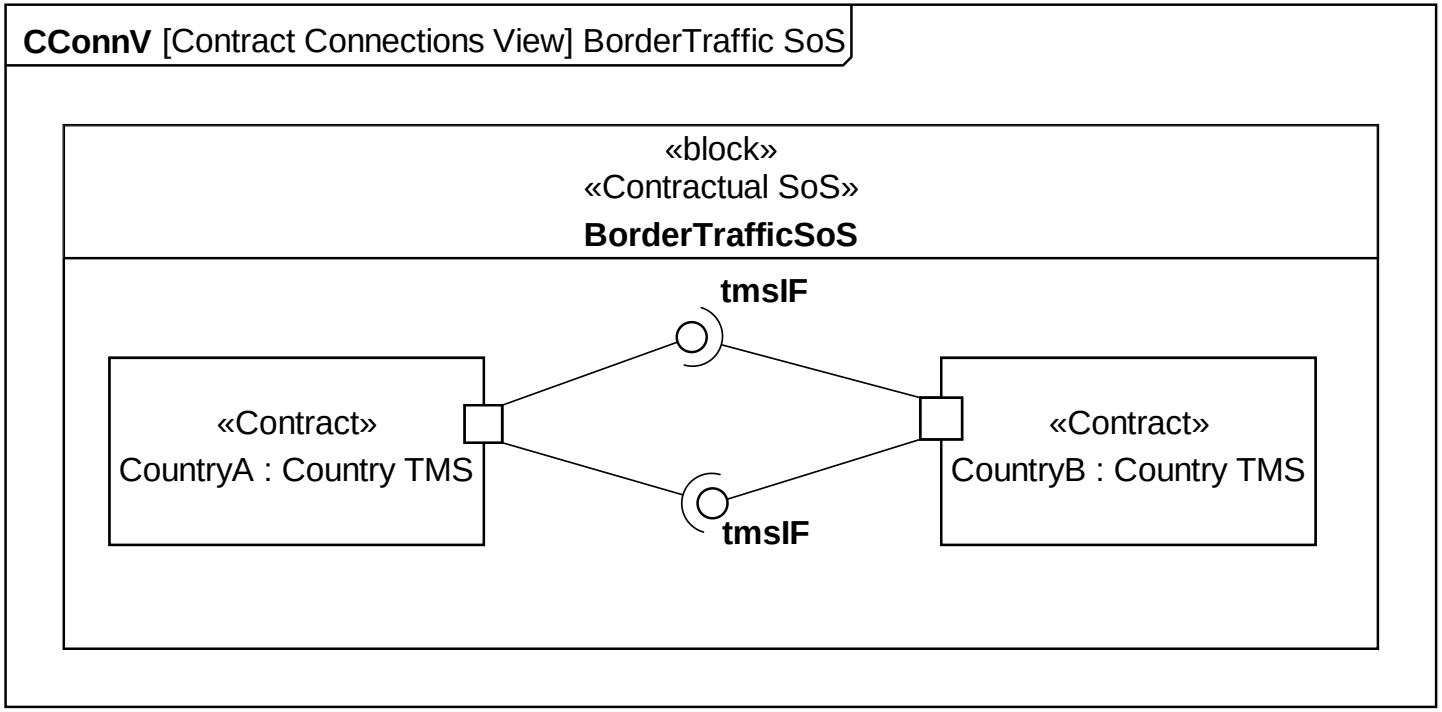


Architectural Modelling

Newcastle University
UK | Malaysia | Singapore

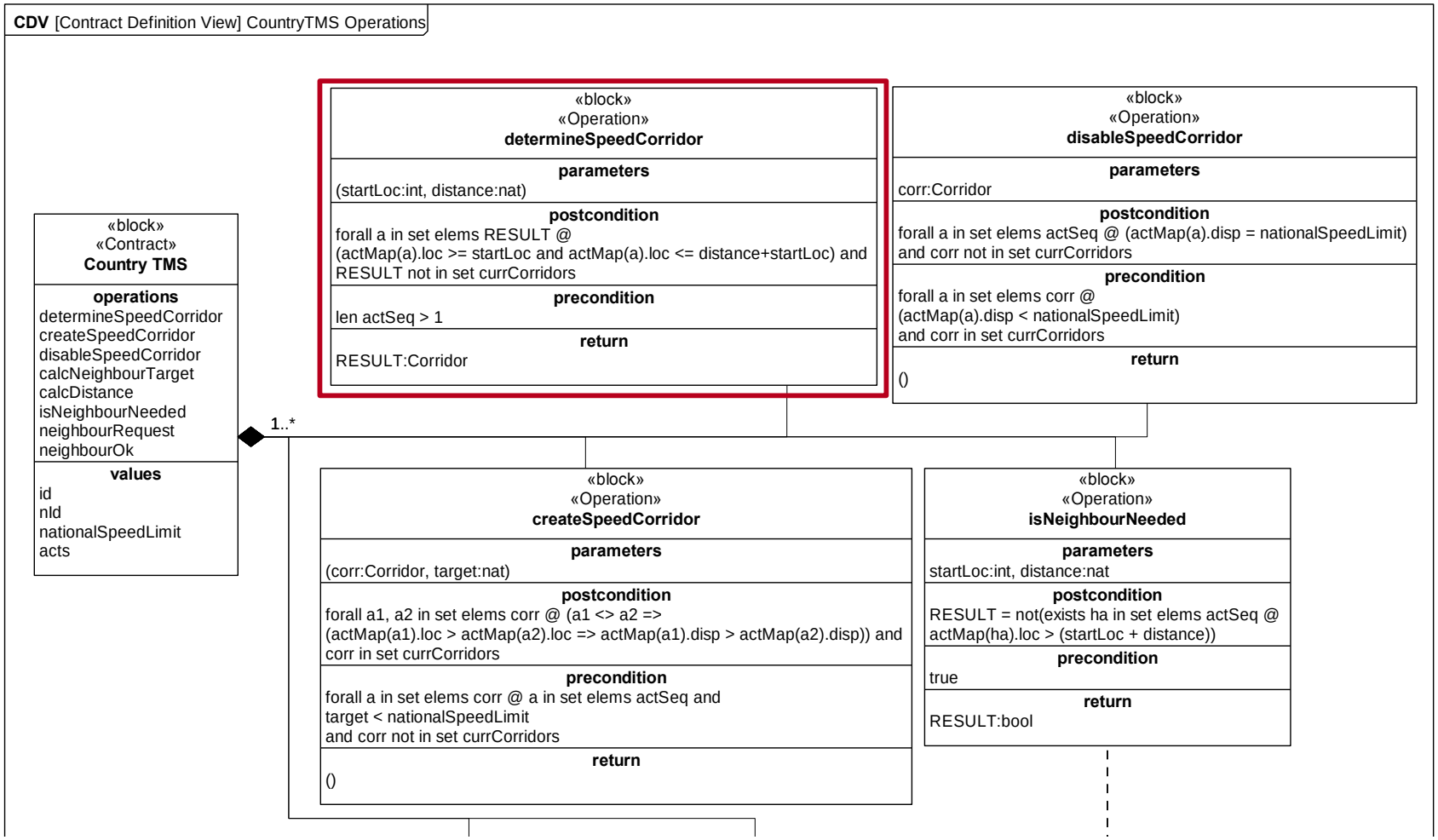
COMPASS

- Defining connections and interfaces between systems



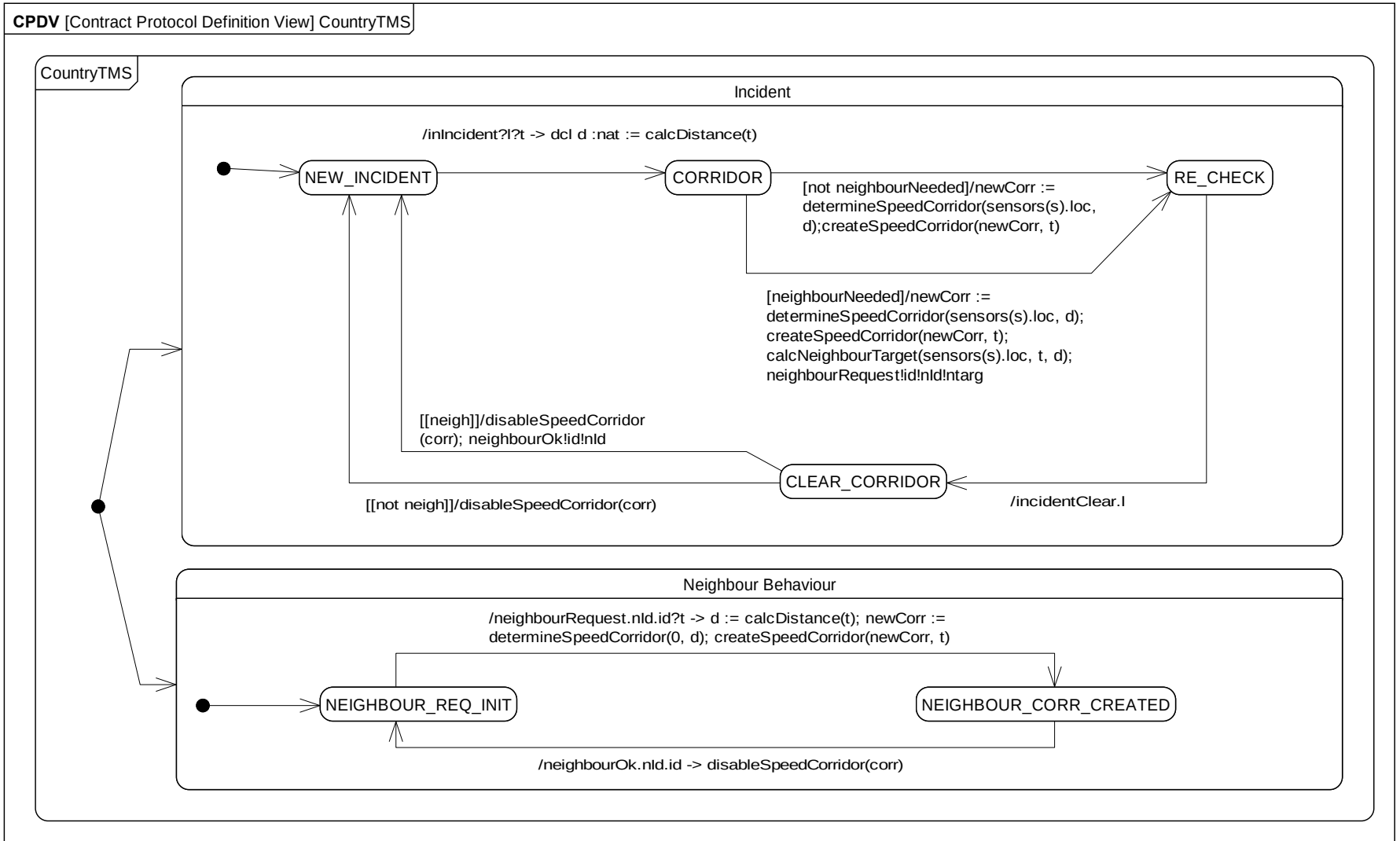
Architectural Modelling

- Defining the functionality of the contract



Architectural Modelling

- Defining behaviour and ordering



Patterns and Frameworks

Newcastle University
UK | Malaysia | Singapore

COMPASS

- Modelling patterns for SoS
  - Architectural patterns: centralised, service-oriented, reconfiguration control, supply chain, …
  - Enabling patterns: interface definition, interface contracts, testing, …
- Architectural frameworks
  - Domain-specific: music streaming (B&O)
  - Specific modelling activities: Fault Modelling AF
- Use COMPASS AF Framework to define patterns and AFs

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

Formal Modelling

Newcastle University
UK | Malaysia | Singapore

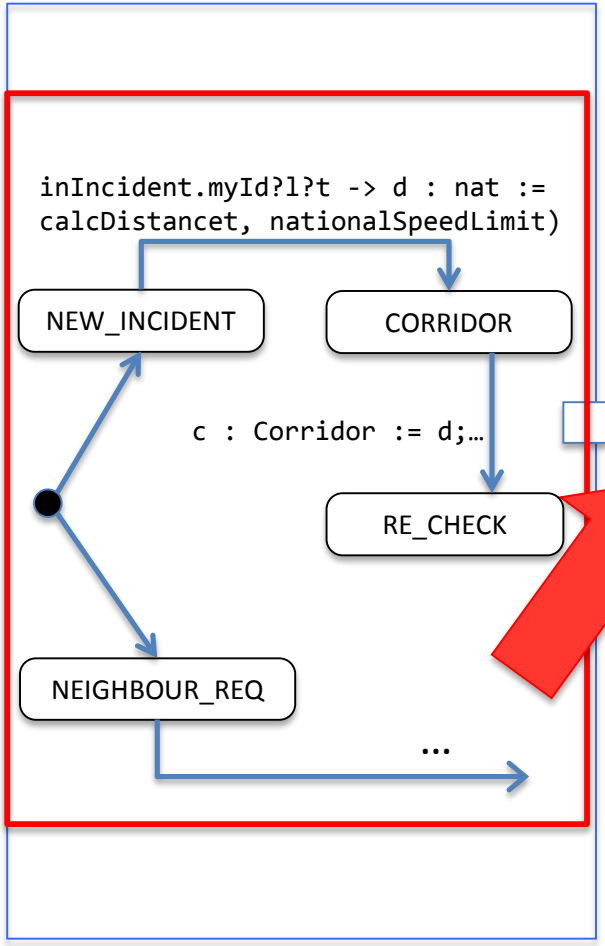
COMPASS

- 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 translation from SysML to CML

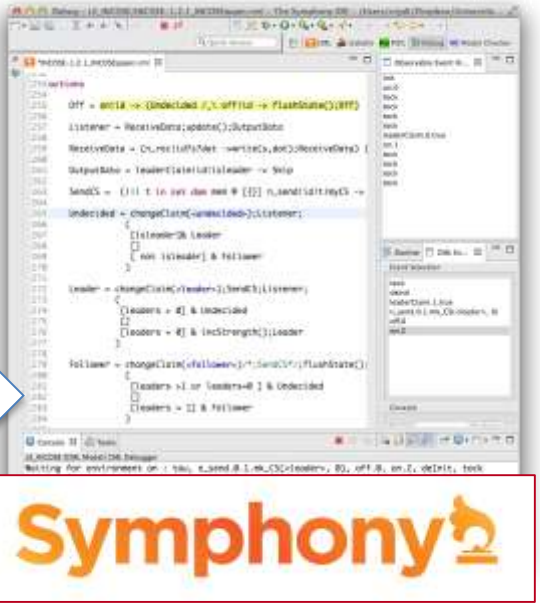
Analysing the Model

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

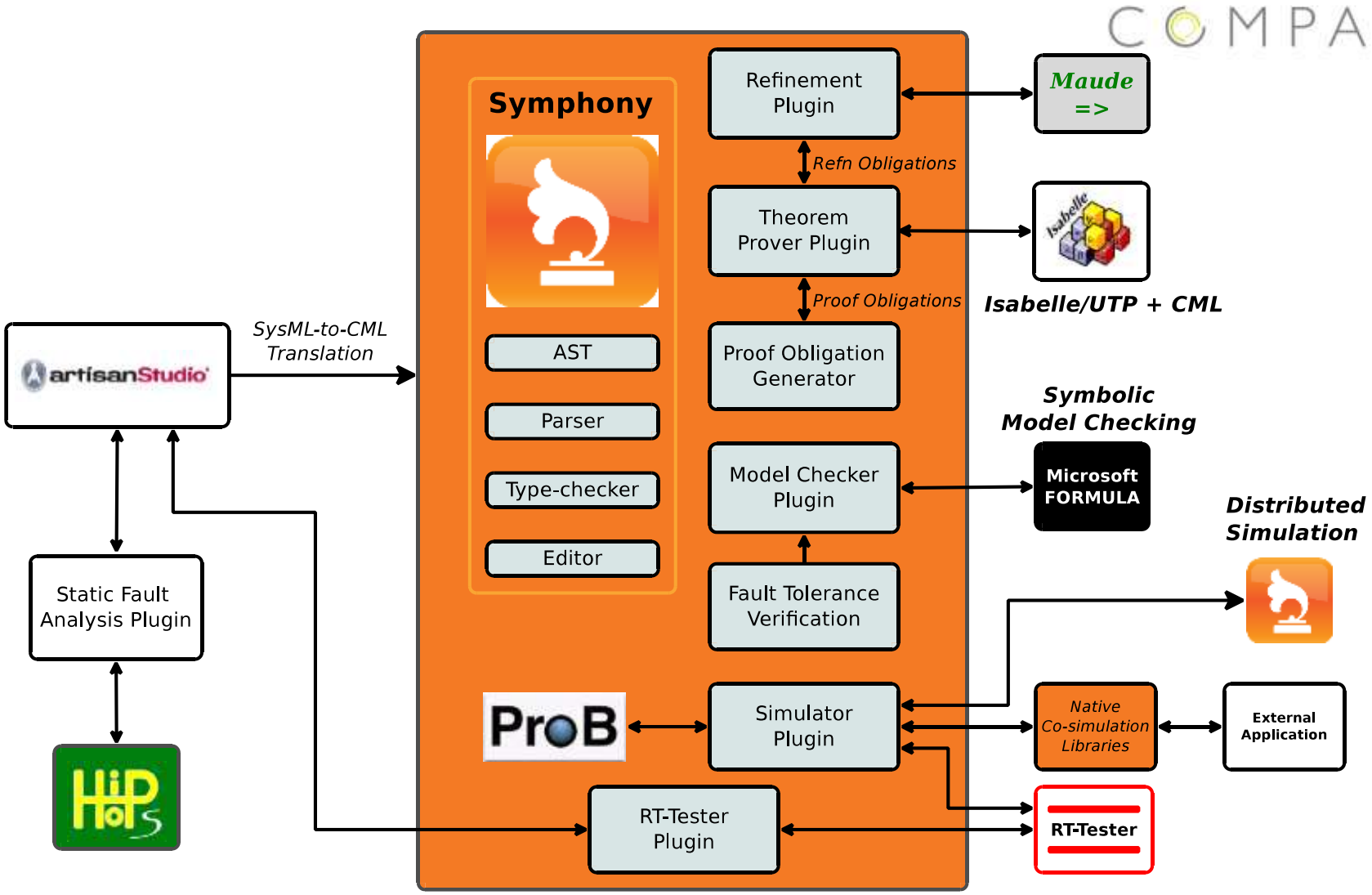
Outline

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

The Symphony Tool Platform

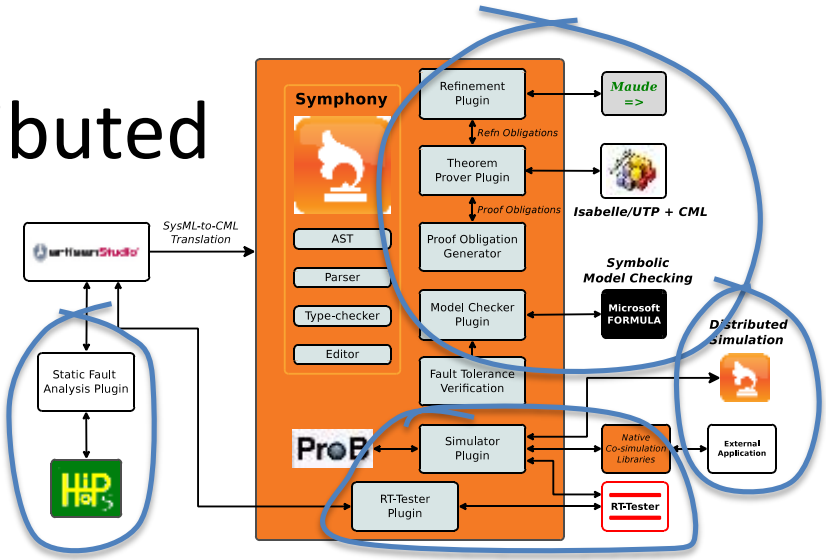


Model-based Validation and Verification

Newcastle University
UK | Malaysia | Singapore

COMPASS

- Interpreter and RT-Tester used for *requirement validation*
- Theorem prover and model checker used for *property verification*
- Static fault analysis allows *FMEA* and *fault tree analysis*
- External links allow distributed SoS engineering



Outline

Newcastle University
UK | Malaysia | Singapore

COMPASS

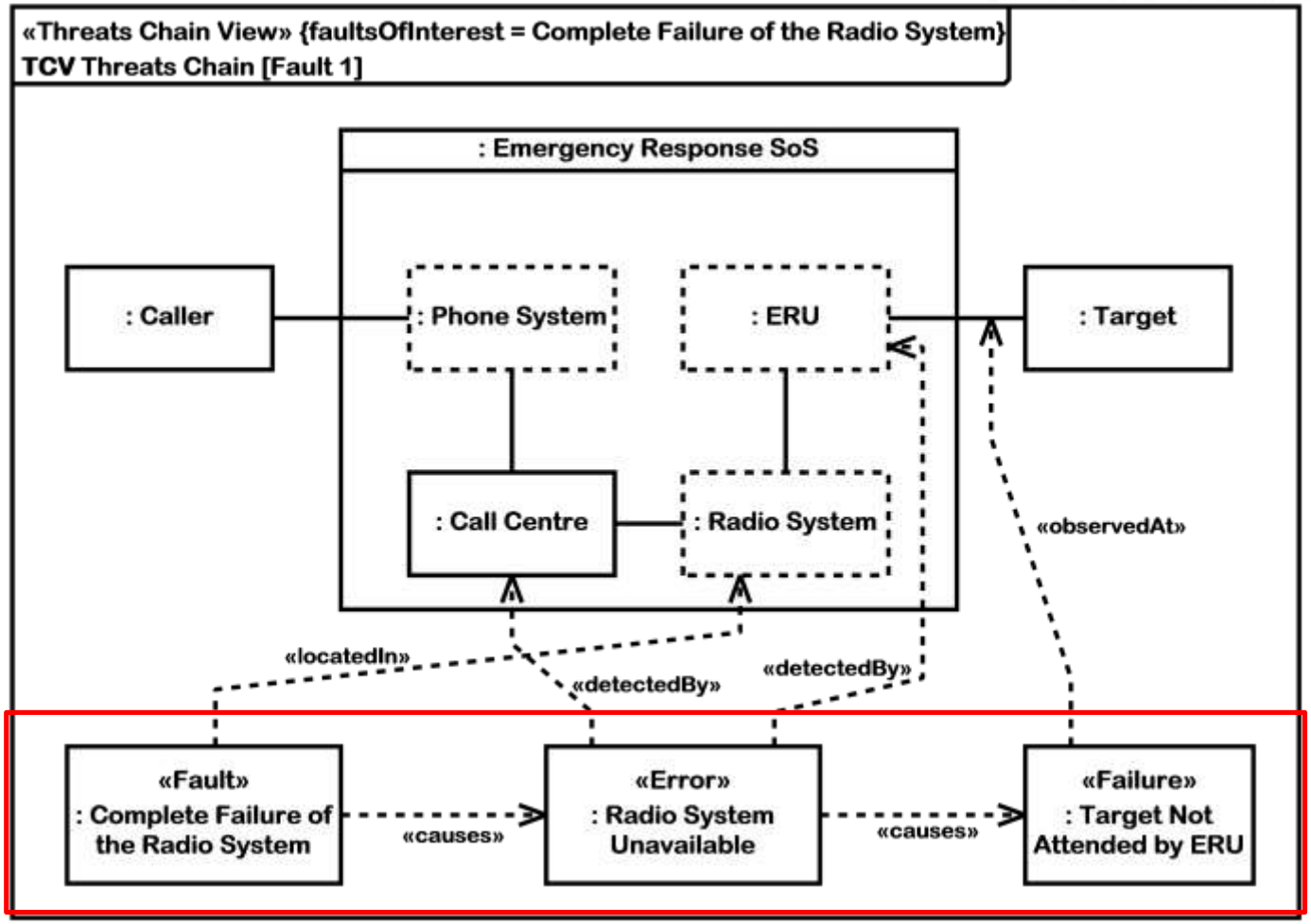
- Systems of systems (SoS)
- Model-based SoS Engineering
- **The COMPASS Project**
  - The COMPASS SoS Engineering Approach
  - Requirements Engineering
  - Architectural Modelling
  - Formal Modelling
  - Verification and Analysis
  - **Fault Modelling**

Fault Modelling

Newcastle University
UK | Malaysia | Singapore

COMPASS

- Applying Fault Modelling Architectural Framework
- Shows the fault, error, failure chain and how these affect the SoS
- Blocks, dependencies and diagrams stereotyped as part of a SysML fault modelling profile

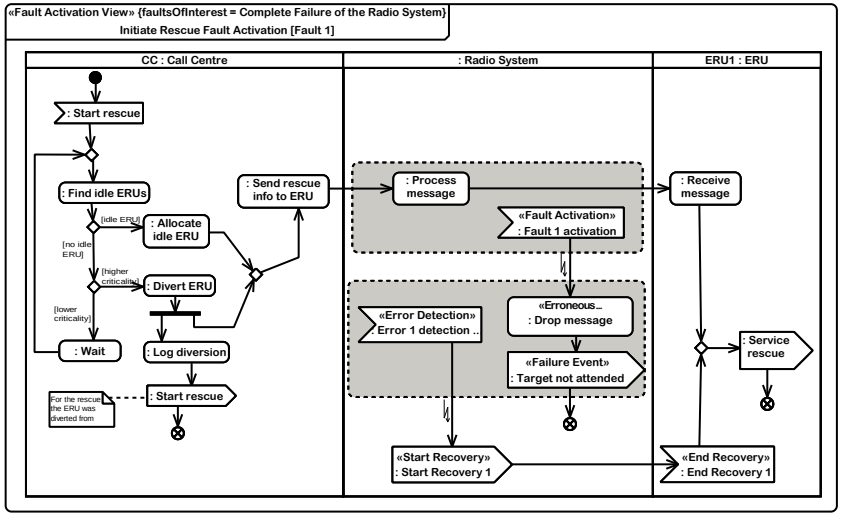


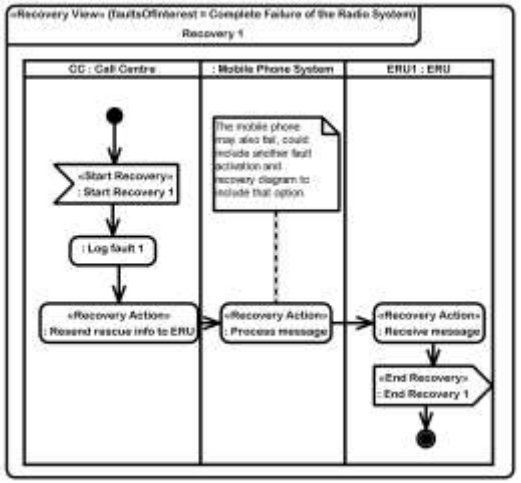
Fault Modelling

Newcastle University
UK | Malaysia | Singapore

COMPASS

- FMAF also includes views for:
  - Fault activation
  - Erroneous behaviour processes and scenarios
  - Fault tolerance structures
  - Recovery procedures





Conclusions

Newcastle University
UK | Malaysia | Singapore

COMPASS

- Large set of usable outputs
- Based on an extensible approach
- Gain large benefits from both semi-formal and formal modelling
  - Significant progress in this area
- A unified model-based approach promotes consistency, rigour, traceability, validation and verification

- Join thecompassclub.org !

Newcastle University
UK | Malaysia | Singapore

claire.ingram@ncl.ac.uk @_Claire_Ingram
jeremy.bryans@ncl.ac.uk @JWBryans

COMPASS

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

thecompassclub.org

www.compass-research.eu