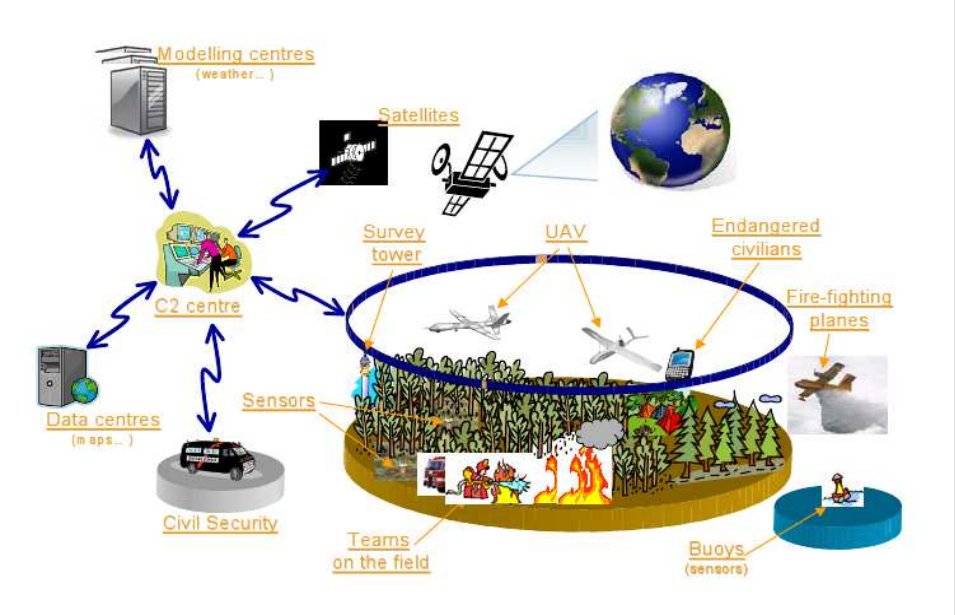
Dependability in dynamic, evolving and heterogeneous systems: the CONNECT approach

*A. Bertolino, F. Di Giandomenico, **P. Masci**, A. Sabetta (ISTI-CNR), V. Issarny, R. Saadi (INRIA), F. Martinelli, I. Matteucci (IIT-CNR), A. Di Marco (UnivAQ)*

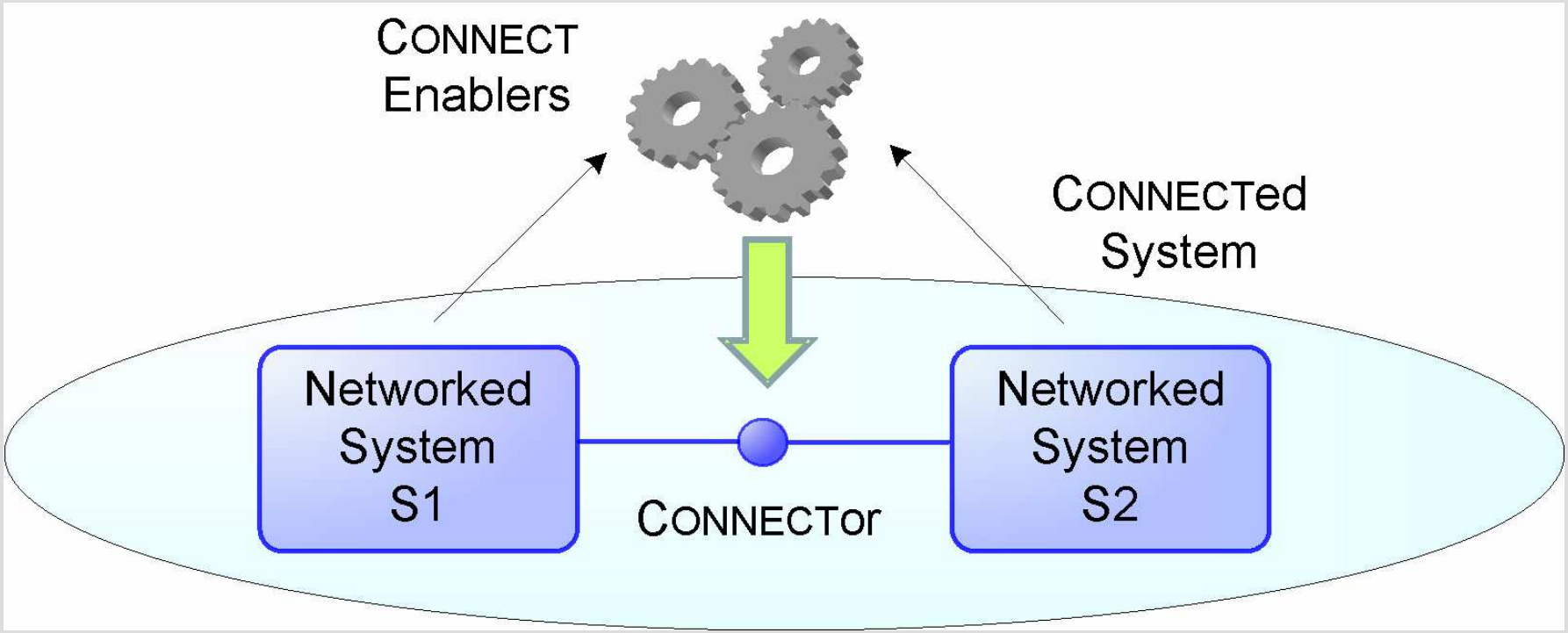
CONNECT

The Interoperability Challenge

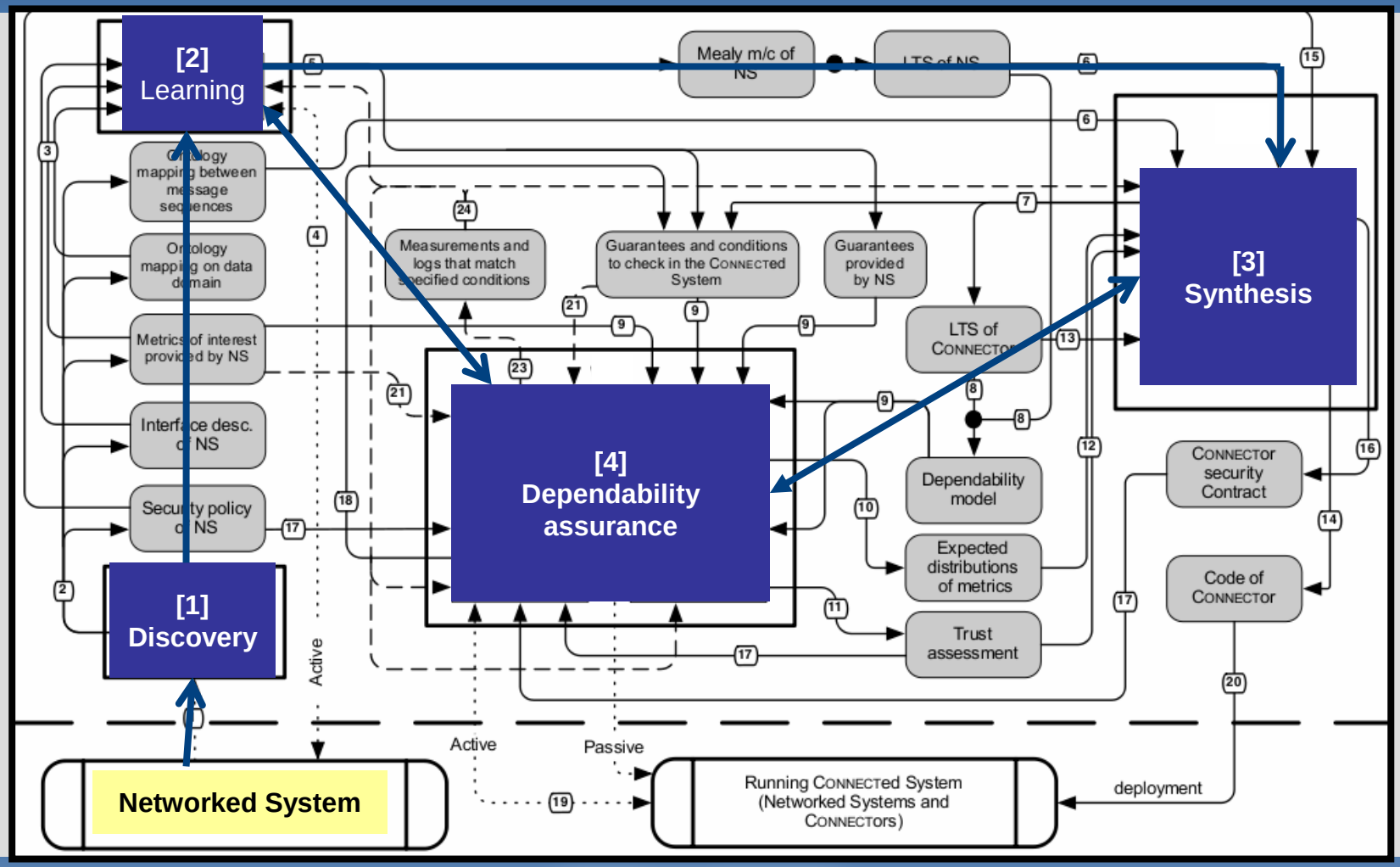
- Interoperability is *"the ability of two or more systems to exchange information, and to use the information"*
  - Heterogeneity
  - Dynamism
  - Evolution
  - …



Dynamic Synthesis of Connectors



Dataflow


[2] Learning
Mealy m/c of NS
LTS of NS
Ontology mapping between message sequences
Ontology mapping on data domain
Metrics of interest provided by NS
Interface desc. of NS
Security policy of NS
Measurements and logs that match specified conditions
Guarantees and conditions to check in the CONNECTed System
Guarantees provided by NS
LTS of CONNECTOR
[3] Synthesis
[4] Dependability assurance
Dependability model
Expected distributions of metrics
Trust assessment
CONNECTor security Contract
Code of CONNECTor
[1] Discovery
Networked System
Active
Active
Passive
Running CONNECTed System (Networked Systems and CONNECTors)
deployment

CONNECT Challenges

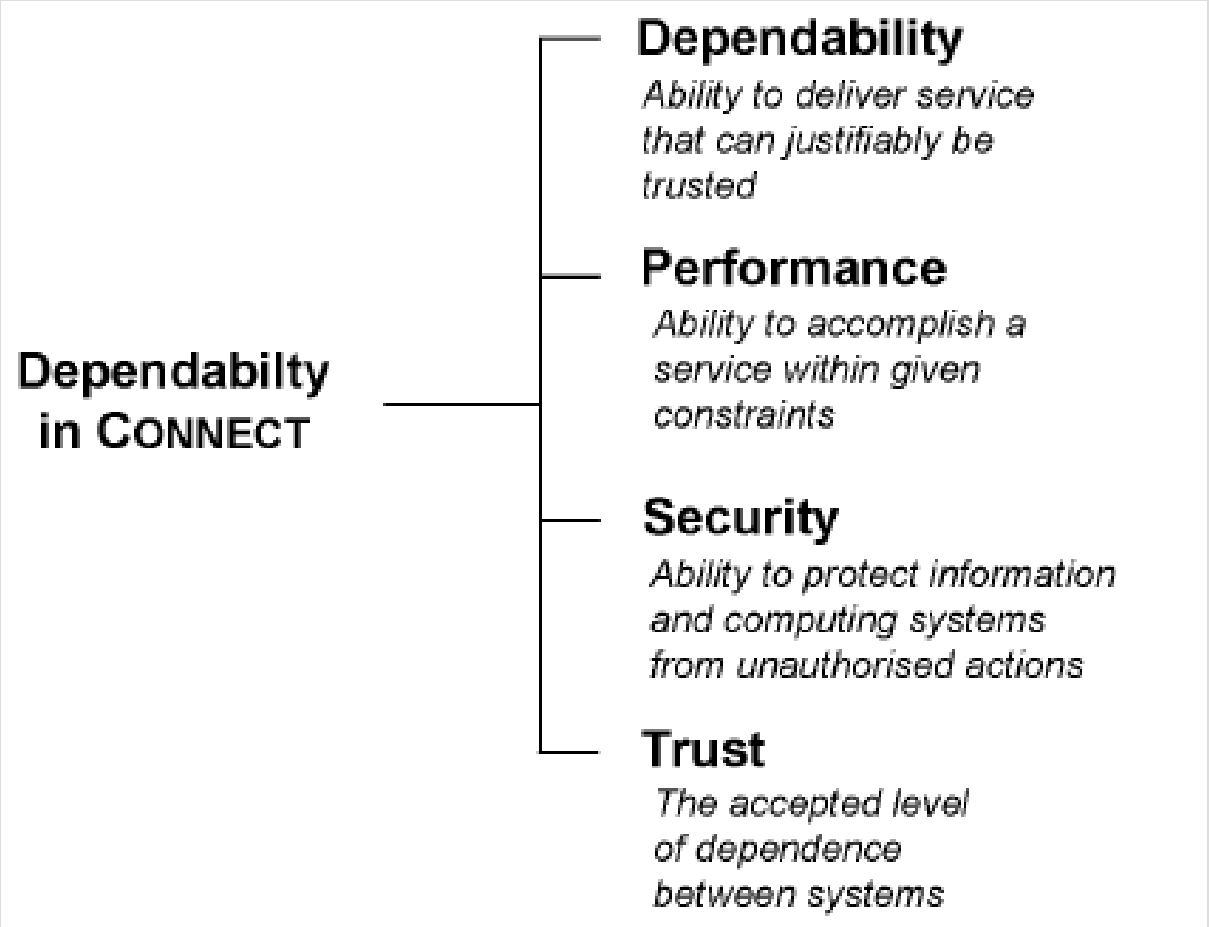
- Modelling and reasoning about peer system functionalities
- Modelling and reasoning about connector behaviors
- Runtime synthesis of connectors
- Learning connector behaviors
- Dependability assurance
- Performant system architecture
- …

CONNECT Challenges

- Modelling and reasoning about peer system functionalities
- Modelling and reasoning about connector behaviors
- Runtime synthesis of connectors
- Learning connector behaviors
- Dependability assurance
- Performant system architecture
- …

Dependability Assurance in CONNECT

Dependability in CONNECT

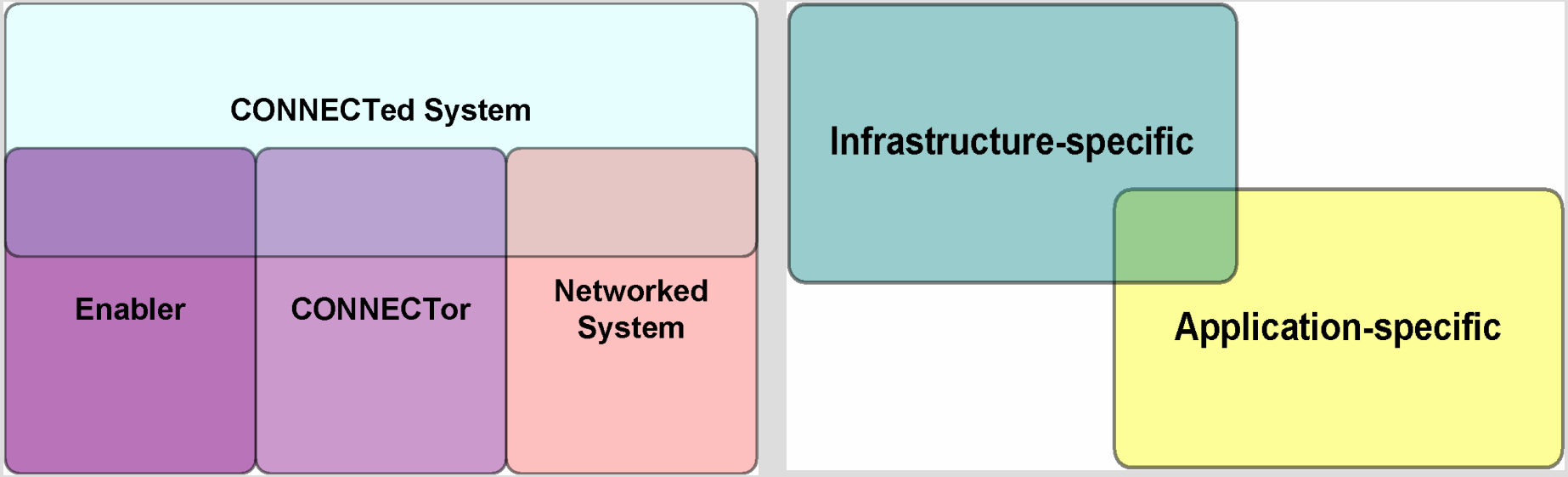


Which entities need to be dependable?

- **Fact 1:** Ultimately, we are interested in establishing a dependable (end-to-end) connection
- **Fact 2:** All CONNECT actors may introduce failures that mine the dependability of the connected system
- **Consequence:** we need to consider (analyse & ensure) dependability attributes for different CONNECT entities
  - Enablers
  - Connectors
  - Networked Systems
  - Connected System

Metrics of interest

Metrics can be obtained by refinement from classical metrics



Refinement Examples

Coverage Probability (generic metric)

- *"Probability for a system to deliver a correct service to a certain percentage of users"*

Derived CONNECT Metrics

- **M1:** *"Probability for the Enabler to successfully synthesise a Connector that delivers a correct service to a certain percentage of users"*
- **M2:** *"Probability to successfully display an alert message on a certain percentage of smartphones brand B"*
- …

Model-based Analysis

- **Quantitative assessment, in terms of probabilities, of the metrics of interest**
- **Offline vs. Online**
  - Estimate expected dependability level
  - Early detect design errors
  - Sensitivity analysis
  - …
- …

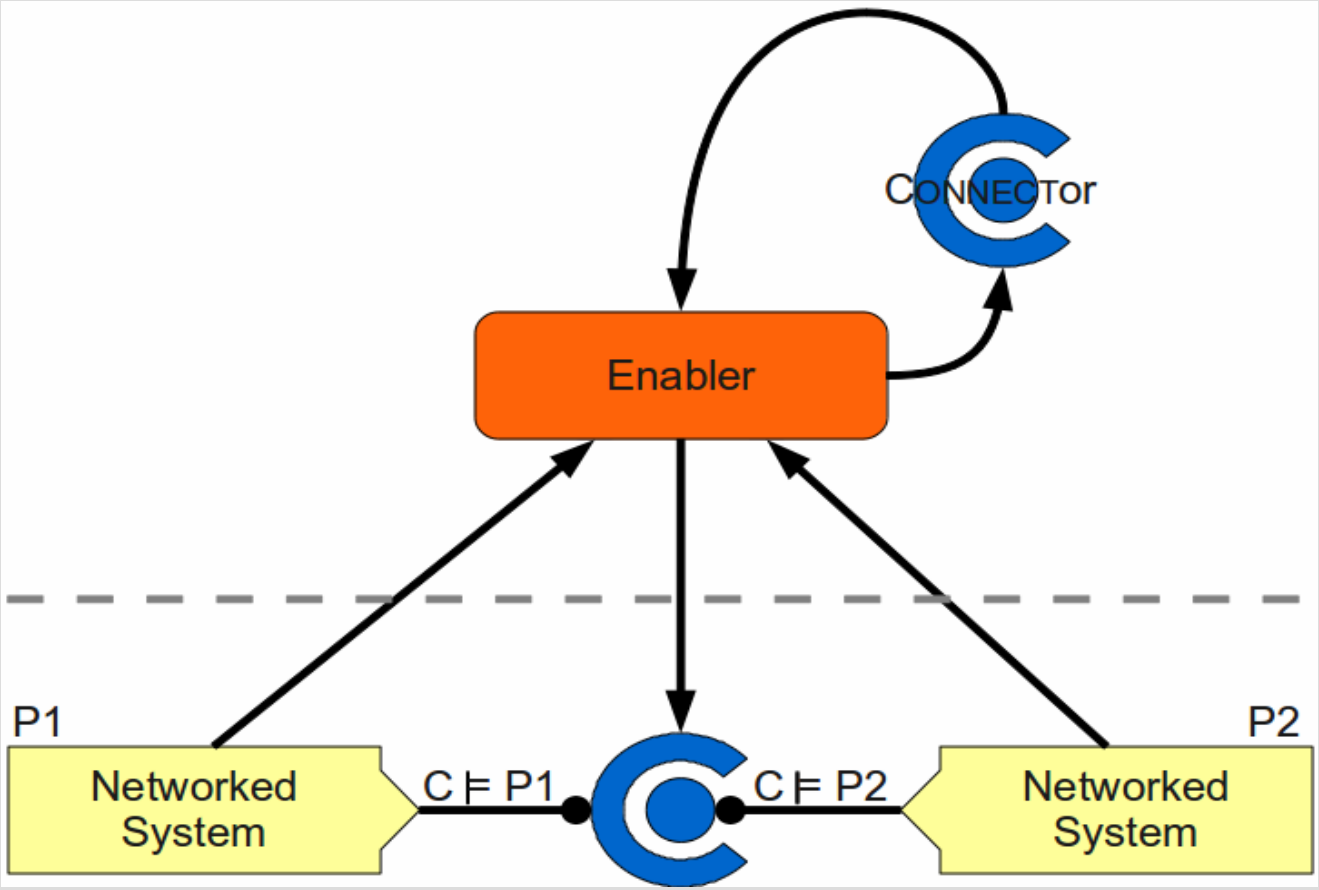
Online vs. Offline Analysis

- **Online**
  - Input parameters from the running system
  - Efficient solution techniques
  - Automated model generation
  - ...
- **Challenges**
  - Progressive model definition
  - Partially Static / Partially Dynamic Methods
  - Integration within CONNECT Enablers
  - …

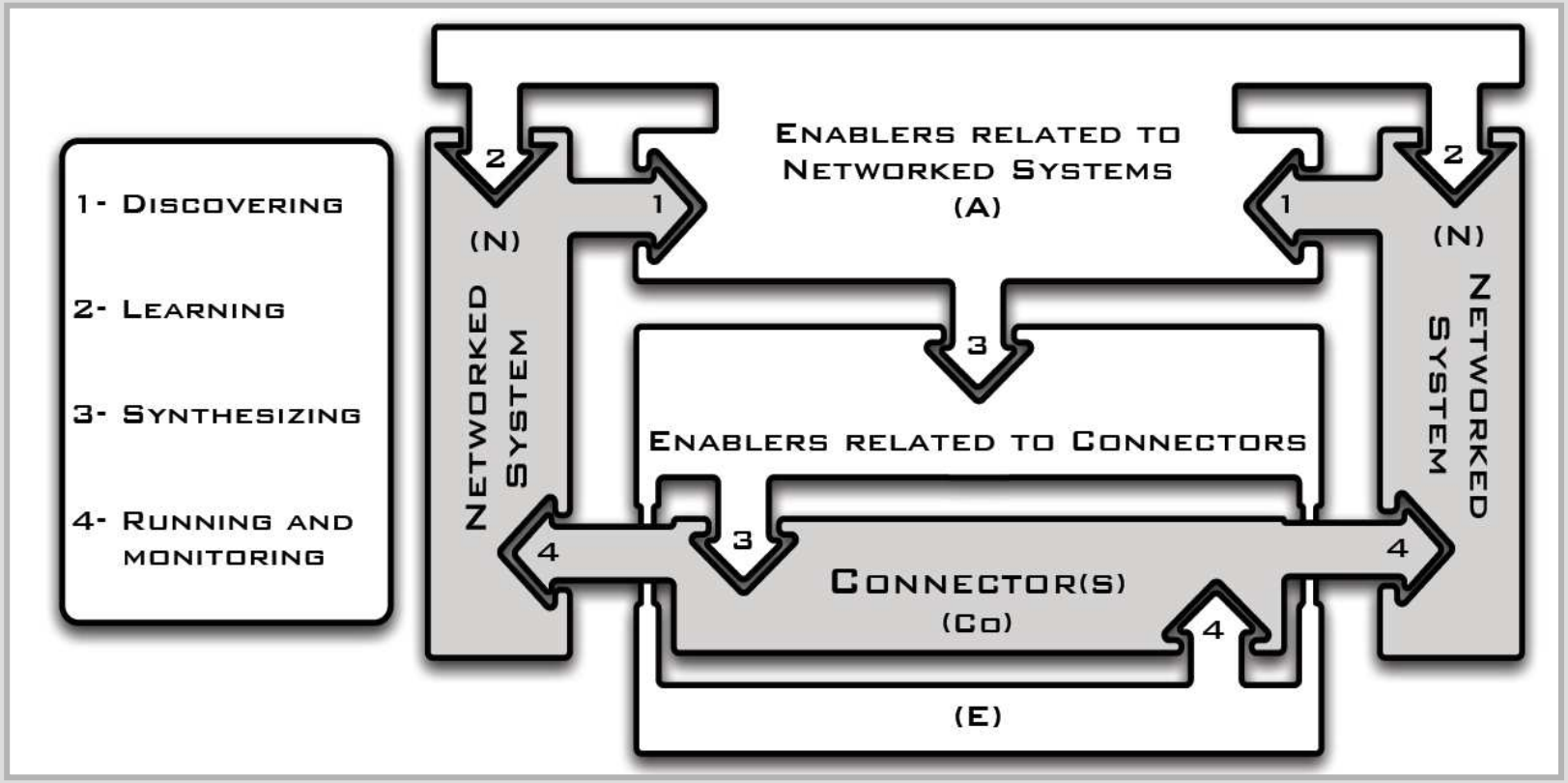
Towards Dependability Assurance

- **Embed dependability mechanisms**
  - Enablers
  - Connectors
- **Embed monitoring mechanisms**
  - Feedback
  - Enforcement
- **...**

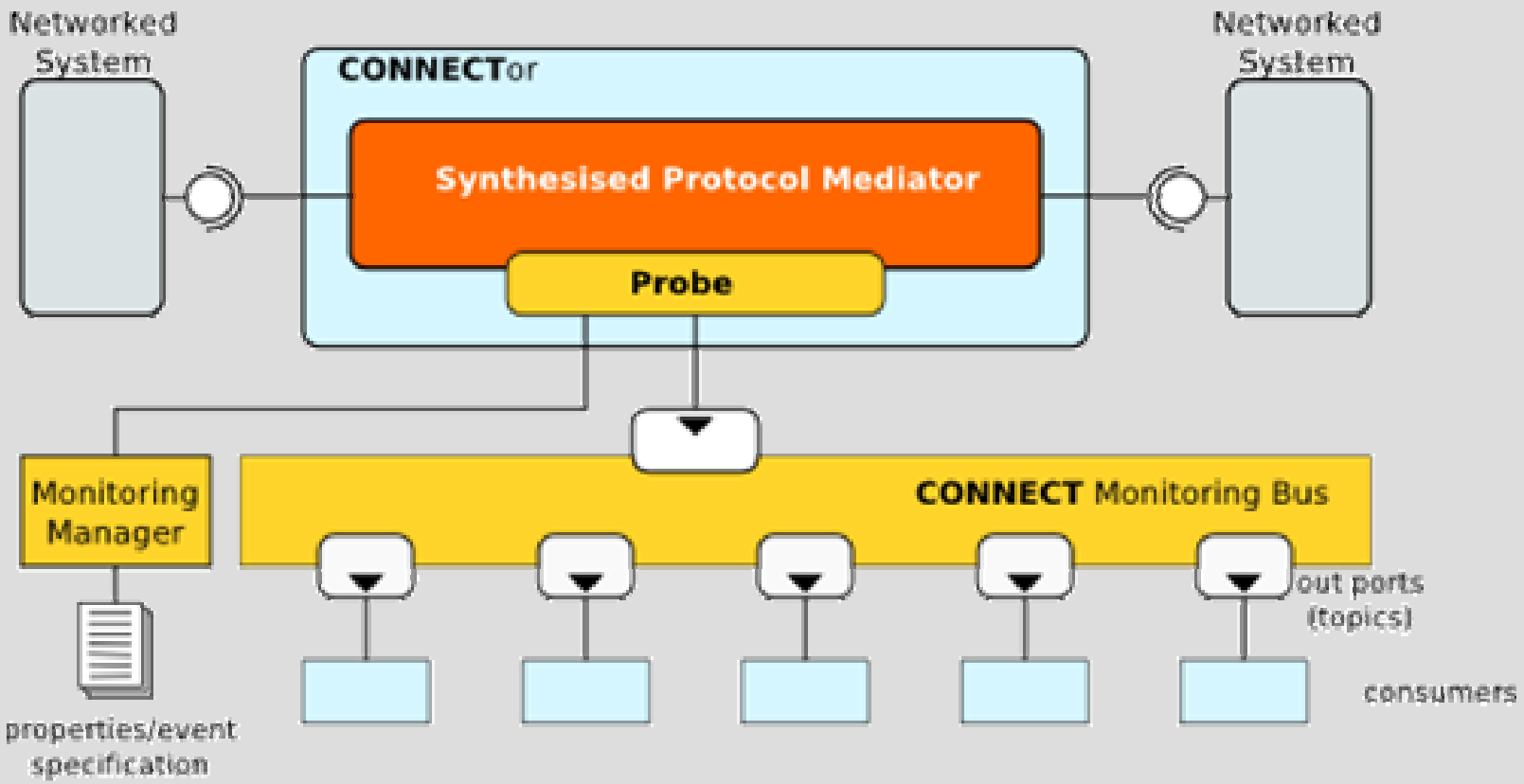
Security and Privacy



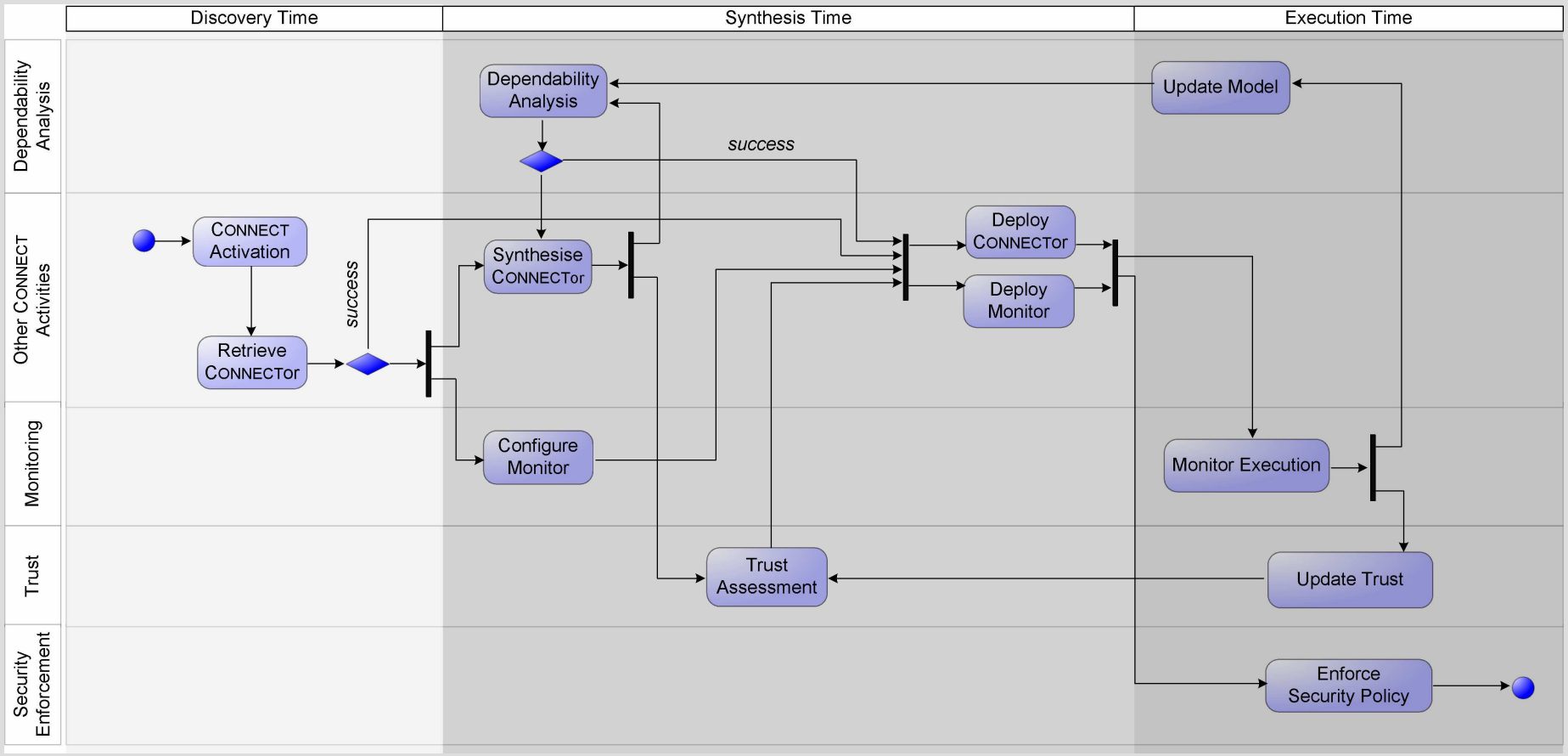
Trust


1- Discovering
2- Learning
3- Synthesizing
4- Running and monitoring
Enablers related to Networked Systems (A)
Networked System (N)
Networked System (N)
Enablers related to Connectors
Connector(s) (Co)
(E)
1
2
3
4

Monitoring


Networked System
CONNECTor
Networked System
Synthesised Protocol Mediator
Probe
Monitoring Manager
CONNECT Monitoring Bus
out ports (topics)
consumers
properties/event specification

Overall Workflow Process View



Concluding Remarks

- Dependability Challenges in CONNECT
  - Definition of CONNECT Dependability Metrics
  - Offline and Online Quantitative Analysis
  - Security Model based on Security-by-Contract
  - Trust Model and Trust Management
  - Monitoring Framework