ADVANCE in Smart Grids

Brett Bicknell, Karim Kanso (Critical Software)

Neil Rampton, Daniel McLeod (Selex ES)

ADVANCE Industry Day 2014

SEVENTH FRAMEWORK PROGRAMME

Advance

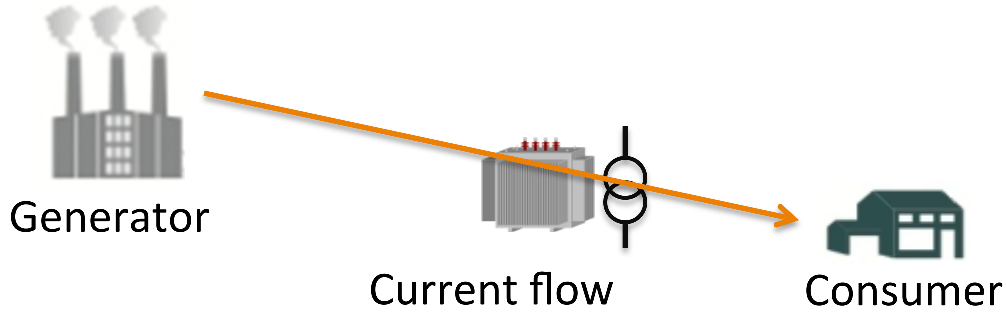
Outline

1. Case Study Background
2. Modelling Strategy
3. Formal Proof
4. Domain Models
5. Co-Simulation
6. Results

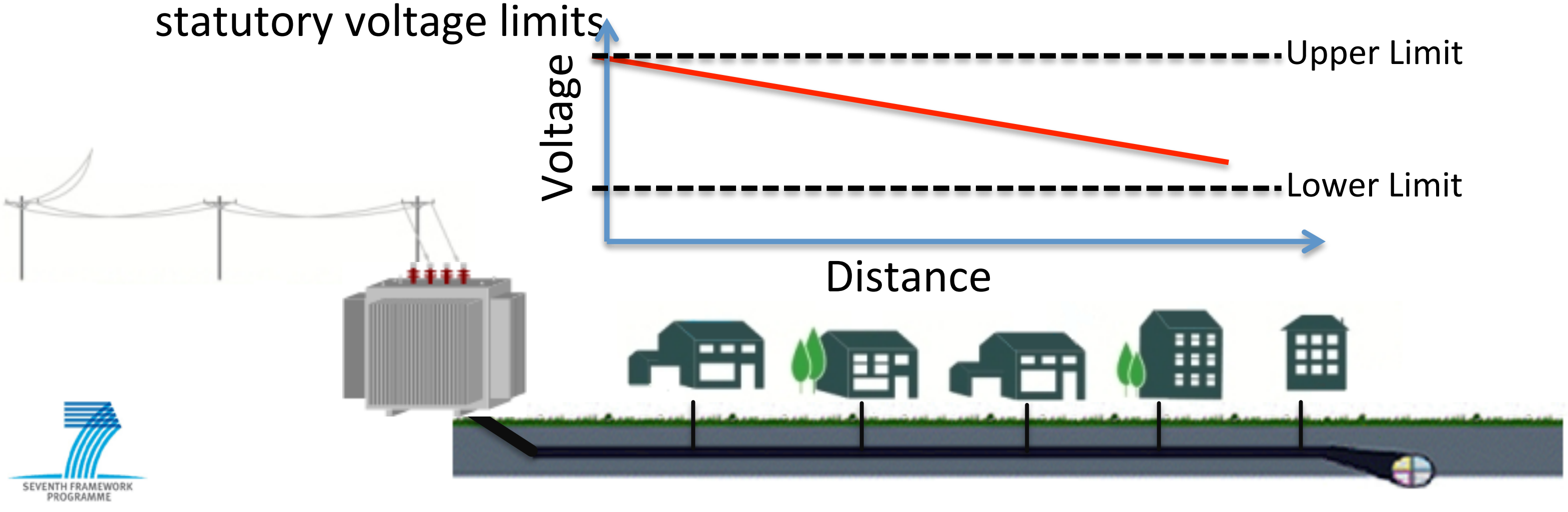
CASE STUDY BACKGROUND

Traditional Network

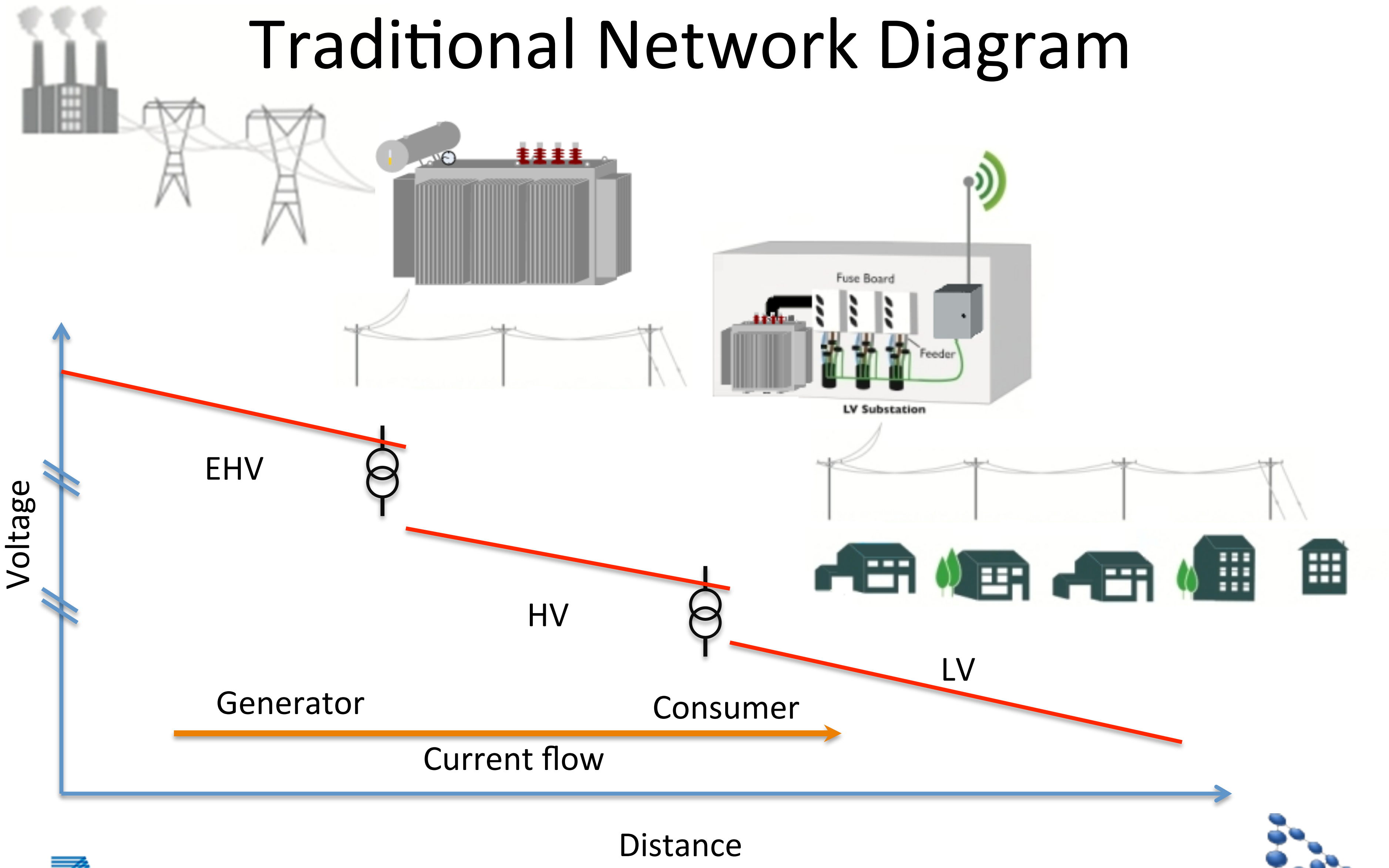
- Power flows from the generator to the consumer



- Voltage drops along cables. Loads are well understood and planned for with sufficient spare ‘head room’ to cope with high demand yet remain well within statutory voltage limits

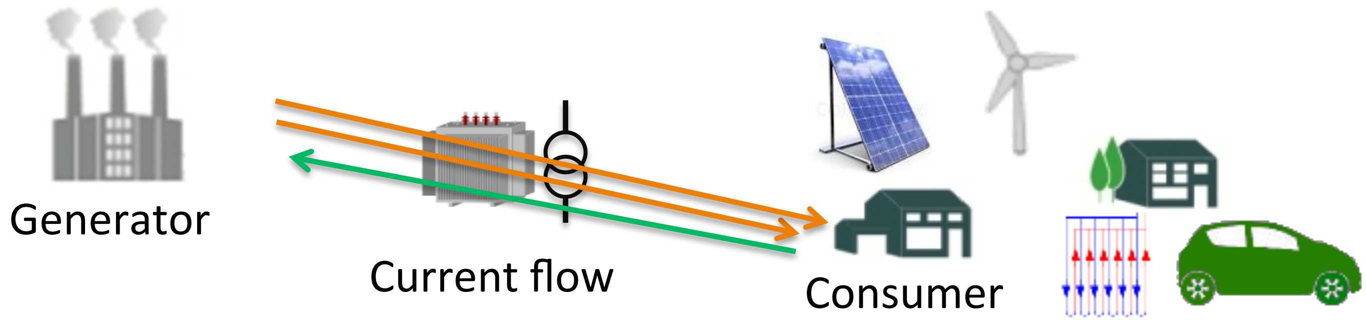


Traditional Network Diagram



Impact of Low Carbon Technologies

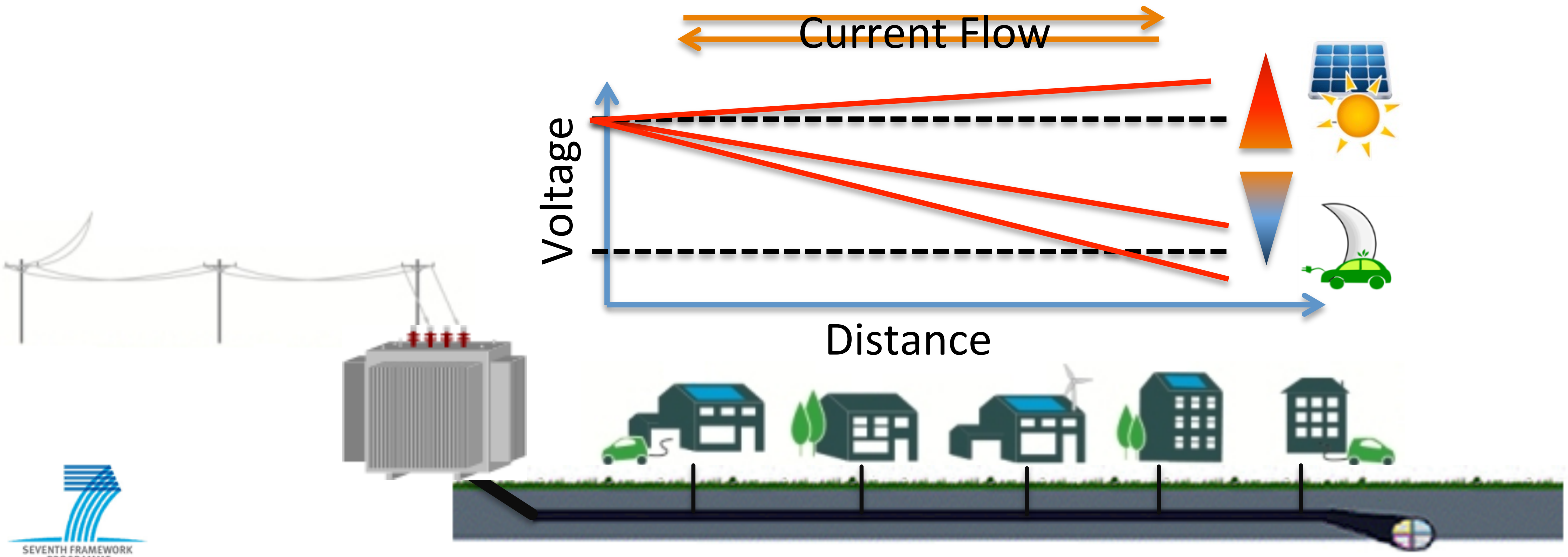
- Traditional grid power flow is changing significantly
- Solar Panel (Photovoltaic) and Wind Power generation are connected throughout the network



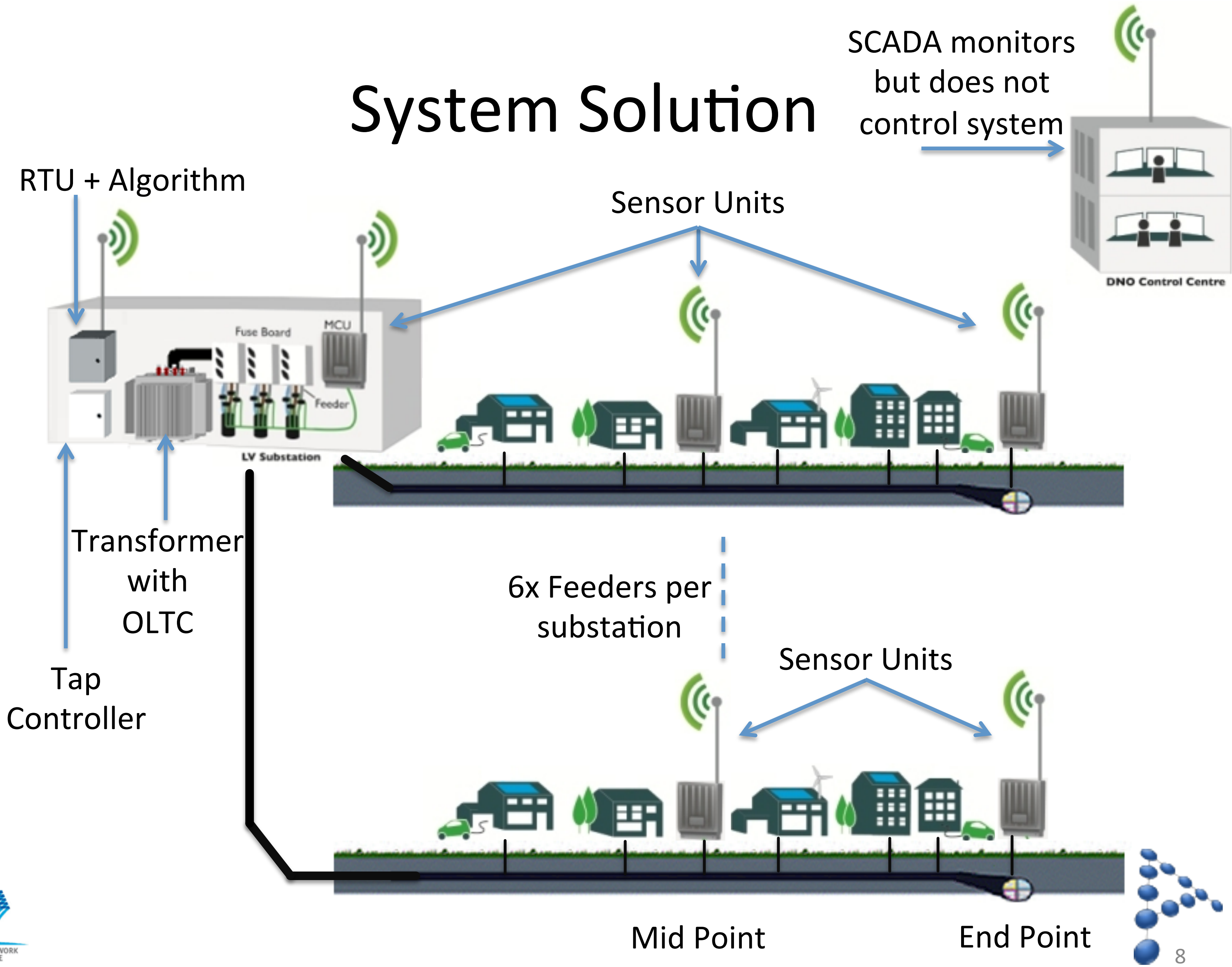
  - Current may flow in the opposite direction
  - Generation varies much more widely over time
- Electric vehicles and Heat pumps increase demand

Voltage Impacts

- In the daytime when demand is typically low, photovoltaics generate the most energy
  - ➔ This increases the voltage towards the end of the feeder
- At night heat pumps and electric vehicles will draw most power
  - ➔ This reduces the voltage towards the end of the feeder
- This situation is much more difficult to plan and manage than traditional static networks



System Solution



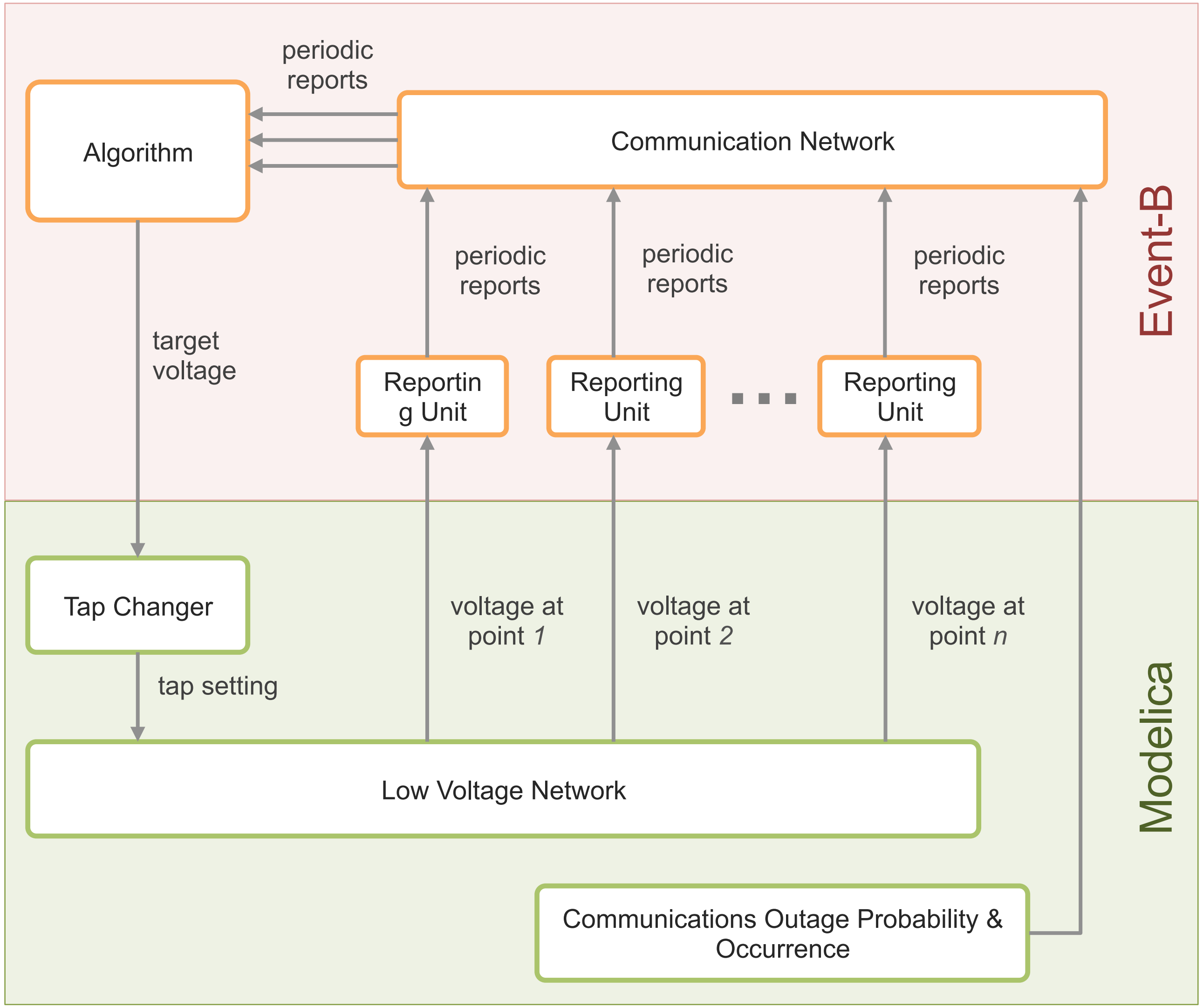
System Requirements/Characteristics

- Measurements of voltage and current provided by 14 sensor units to RTU
- 'Undependable' communications interface between sensors and RTU
- On Load Tap Changer varies network voltage
- Effects of Algorithm acts upon all elements of the system → Feedback
- System shall not exceed statutory voltage limits
- System must act in a safe, consistent and reliable manner
- System must not enter unintended / unwanted states

SEVENTH FRAMEWORK PROGRAMME

MODELLING STRATEGY

Modelling Strategy

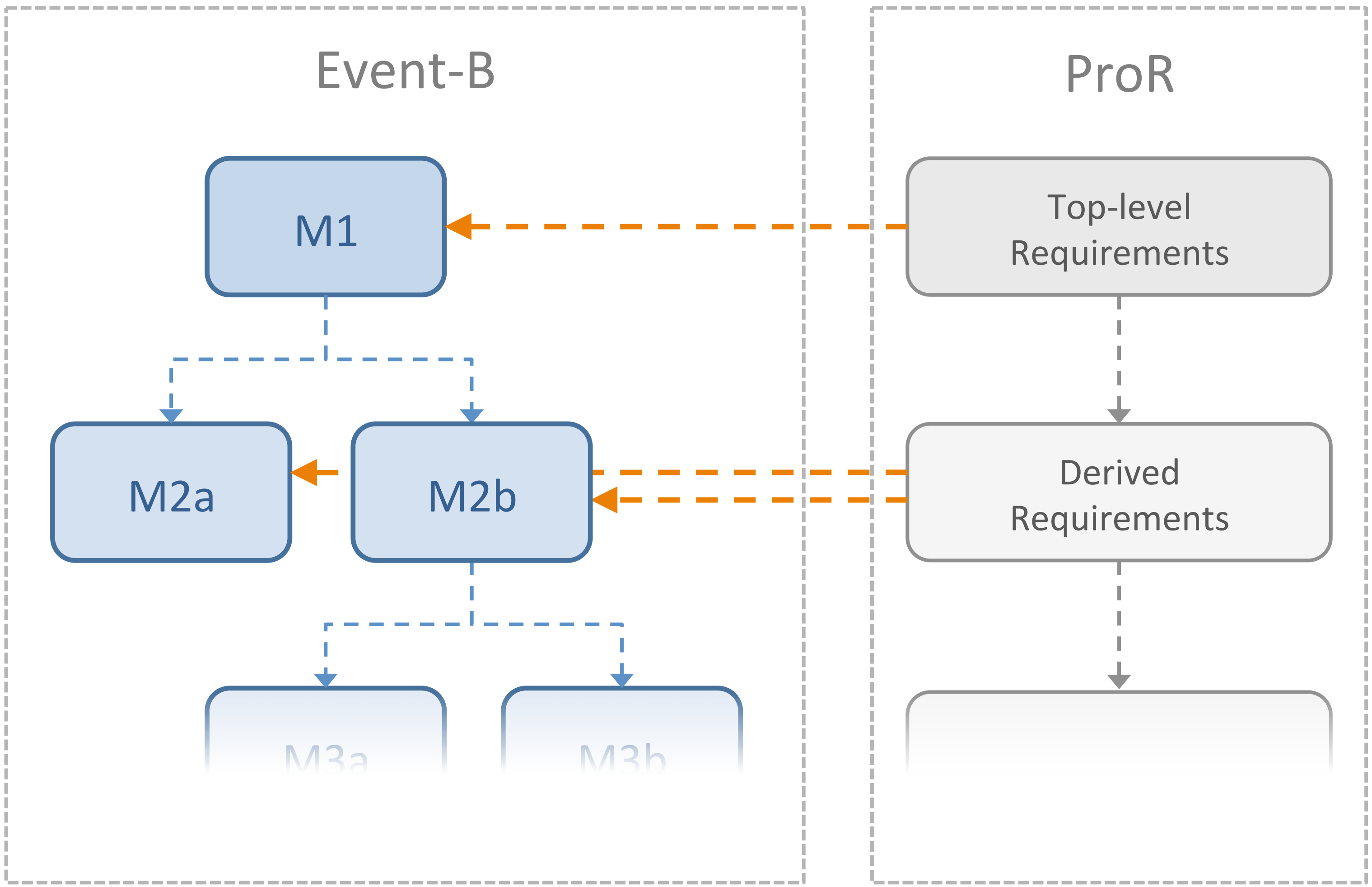


SEVENTH FRAMEWORK PROGRAMME

Decomposition

- Event-B system model developed using decomposition capability within Rodin
  - Separates out complexity - each model can be developed independently
  - Provides clear boundaries between different sub-systems and formalises their interaction
  - Formal process so consistency is maintained
- Models re-composed for simulation

Decomposition

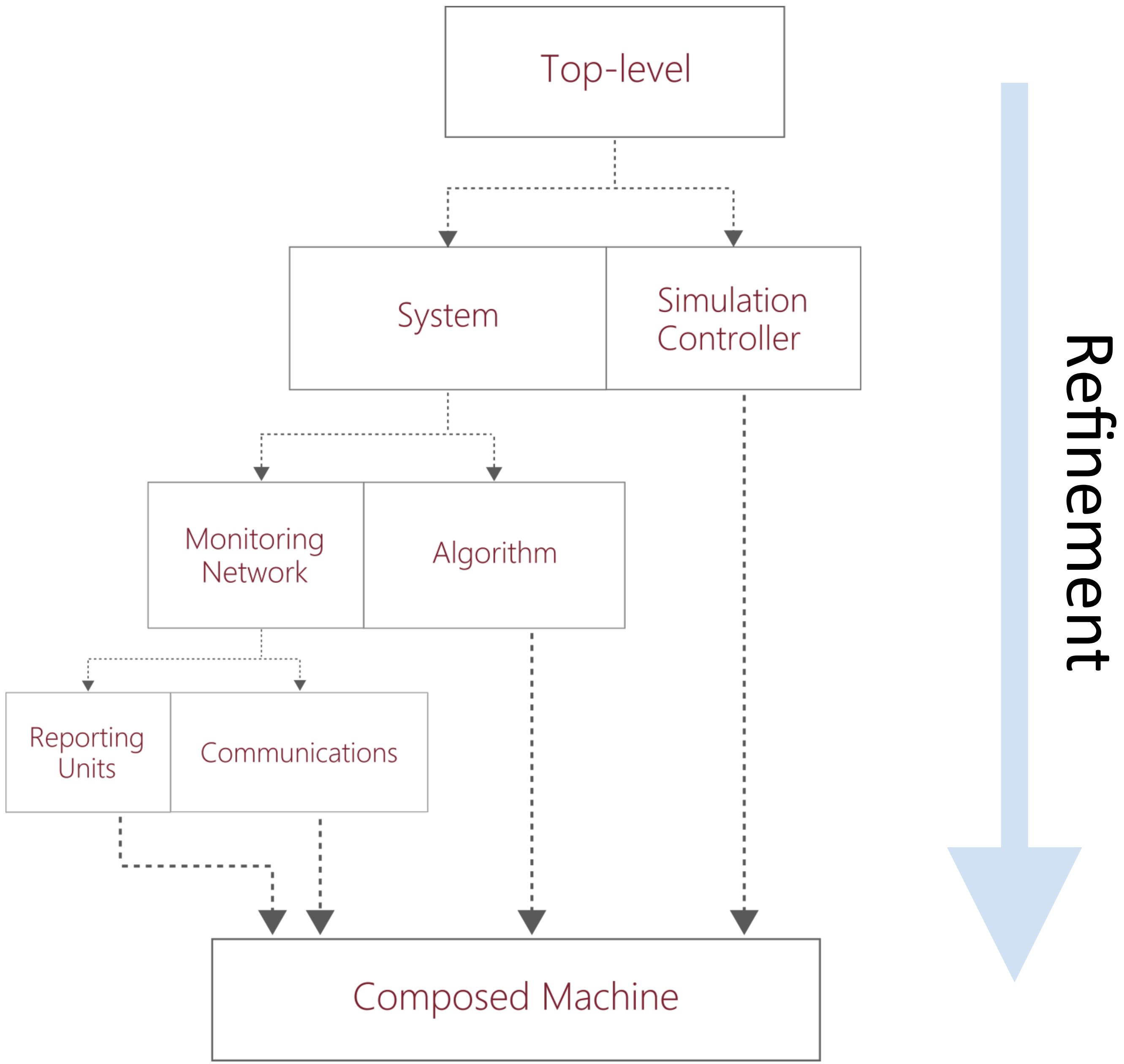


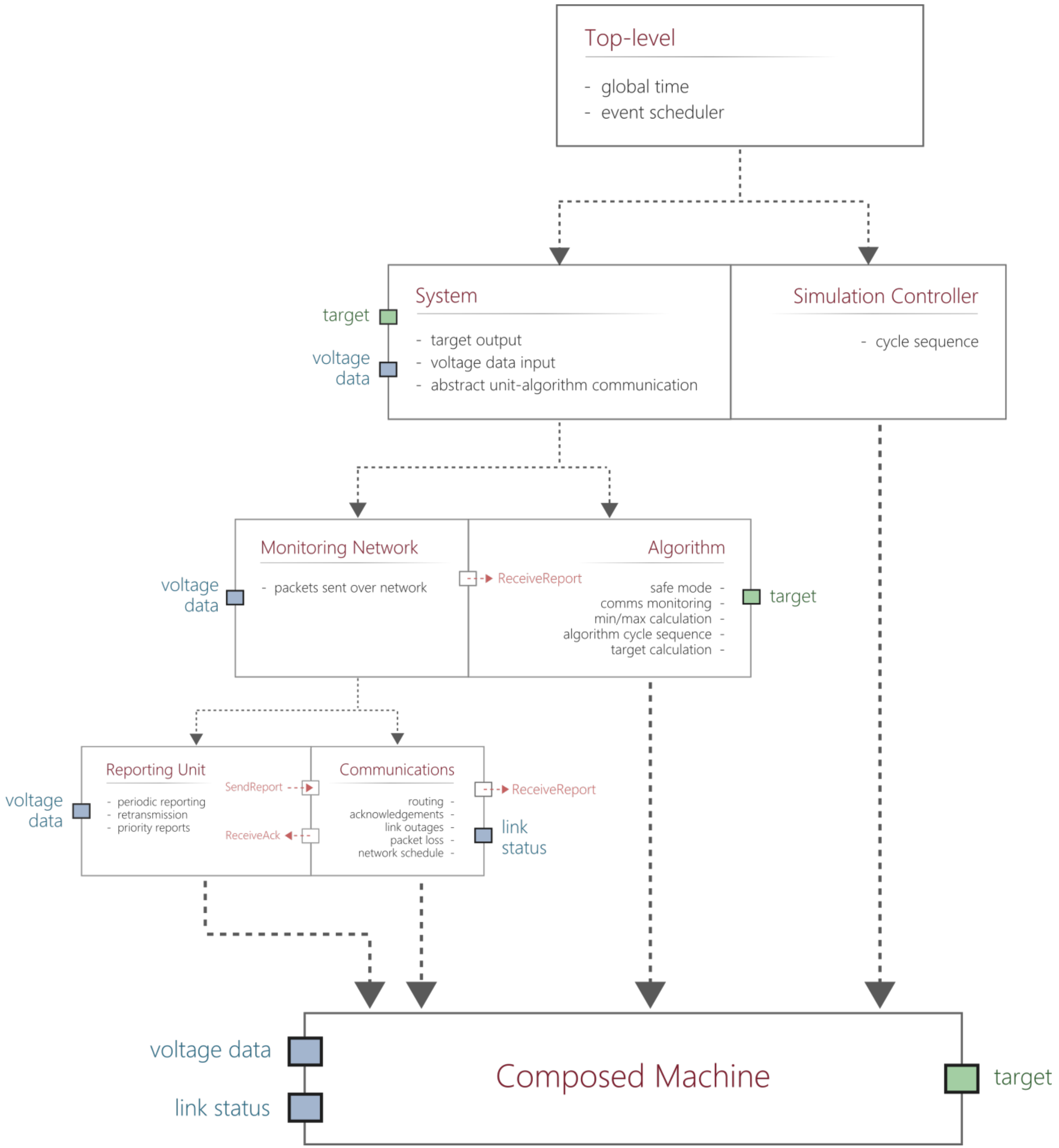
ProR

- Requirements imported into **ProR**
  - Direct link to elements in the Event-B models
  - Changes to requirements or model elements highlighted
  - Traceability between requirement sets also maintained

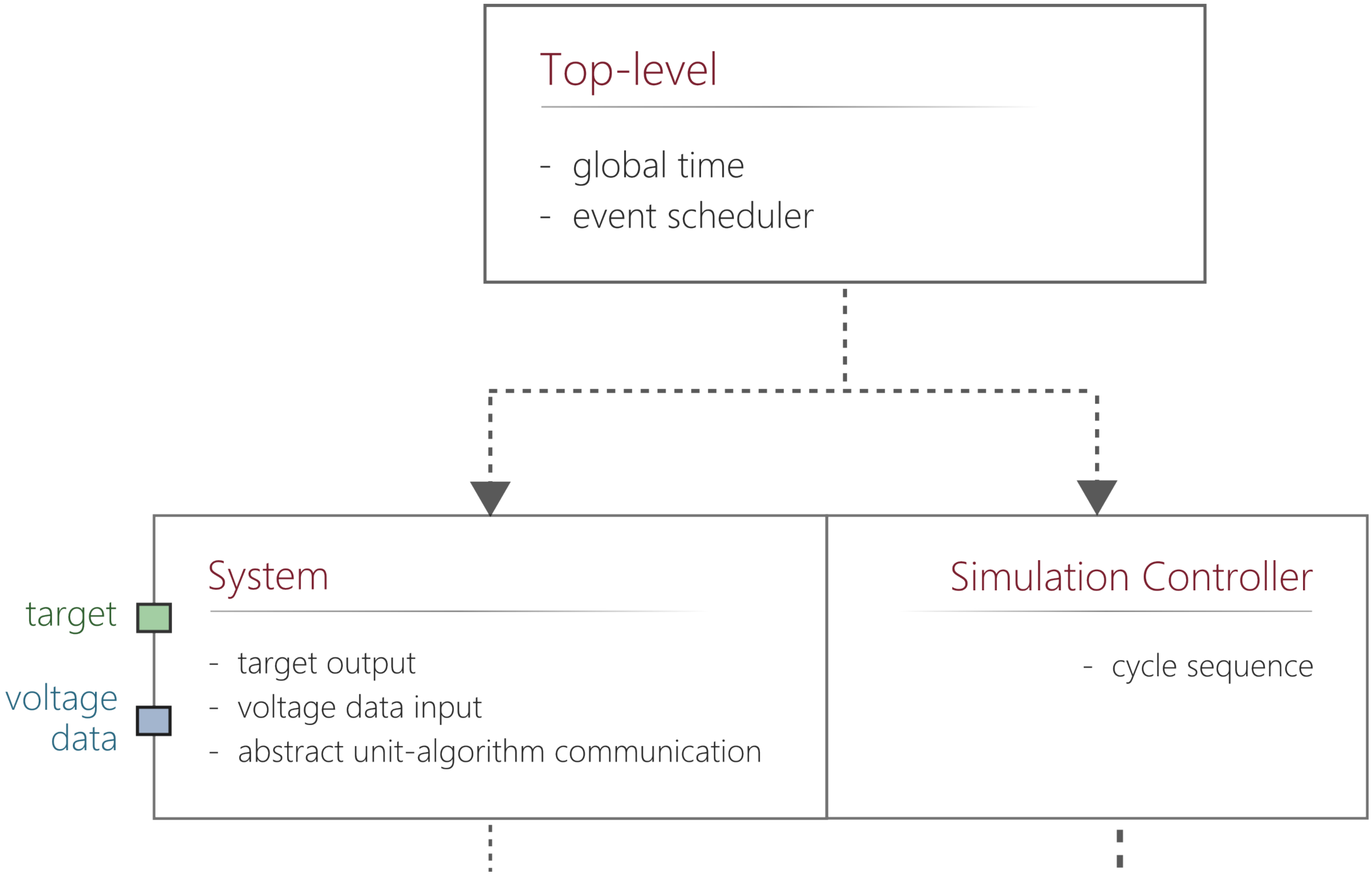
	ID	Description	Source	Target	Link
1	Ⓡ REQ-TL-001	The [algorithm] shall update the [target] on execution			0 ▷ Ⓡ ▷ 1
	▷				SetTarget {act1} (m0)
1.1	Ⓡ REQ-TL-002	If the [maximum] is above 253V and the [minimum] is above 253V then the [target] shall be decreased by 3 voltage [unit]s			0 ▷ Ⓡ ▷ 1
	▷			⚠	inv2 (m0)
1.2	Ⓡ REQ-TL-003	If the [maximum] is below 253V but above 248V and the [minimum] is above 248V then the [target] shall be decreased by 2 voltage [unit]s			0 ▷ Ⓡ ▷ 1
	▷				inv3 (m0)

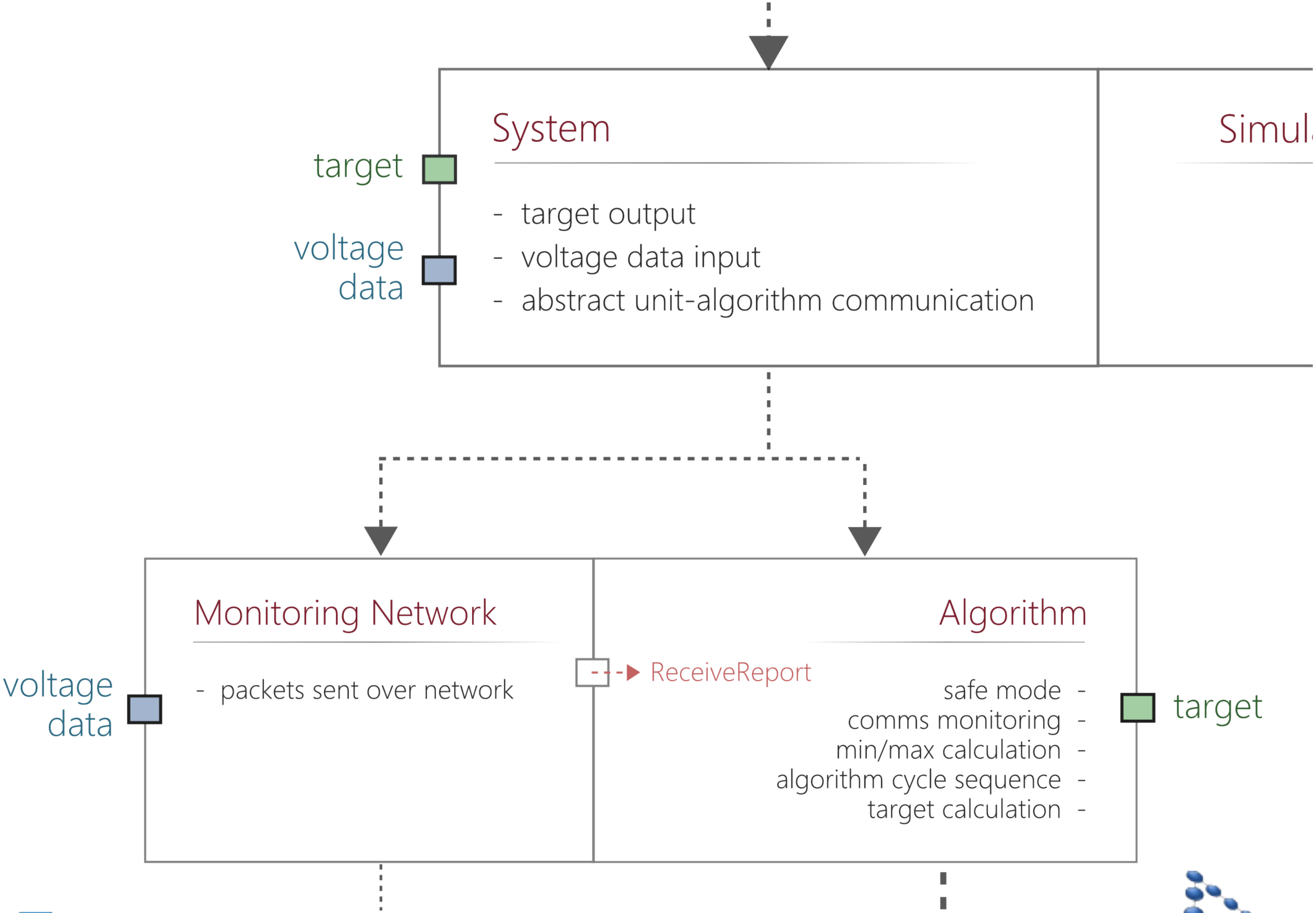
SEVENTH FRAMEWORK PROGRAMME

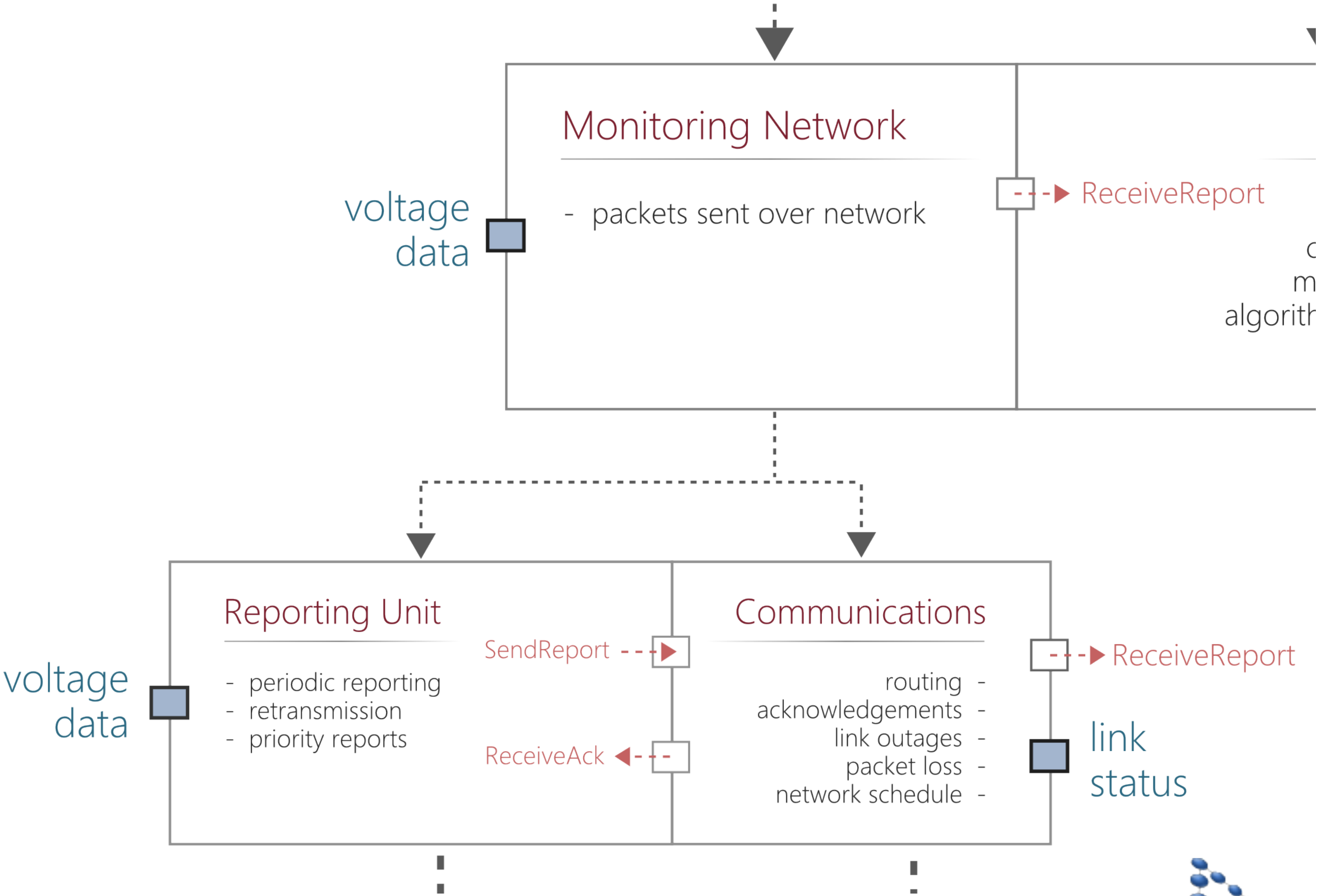

Top-level
System
Simulation Controller
Monitoring Network
Algorithm
Reporting Units
Communications
Composed Machine
Refinement

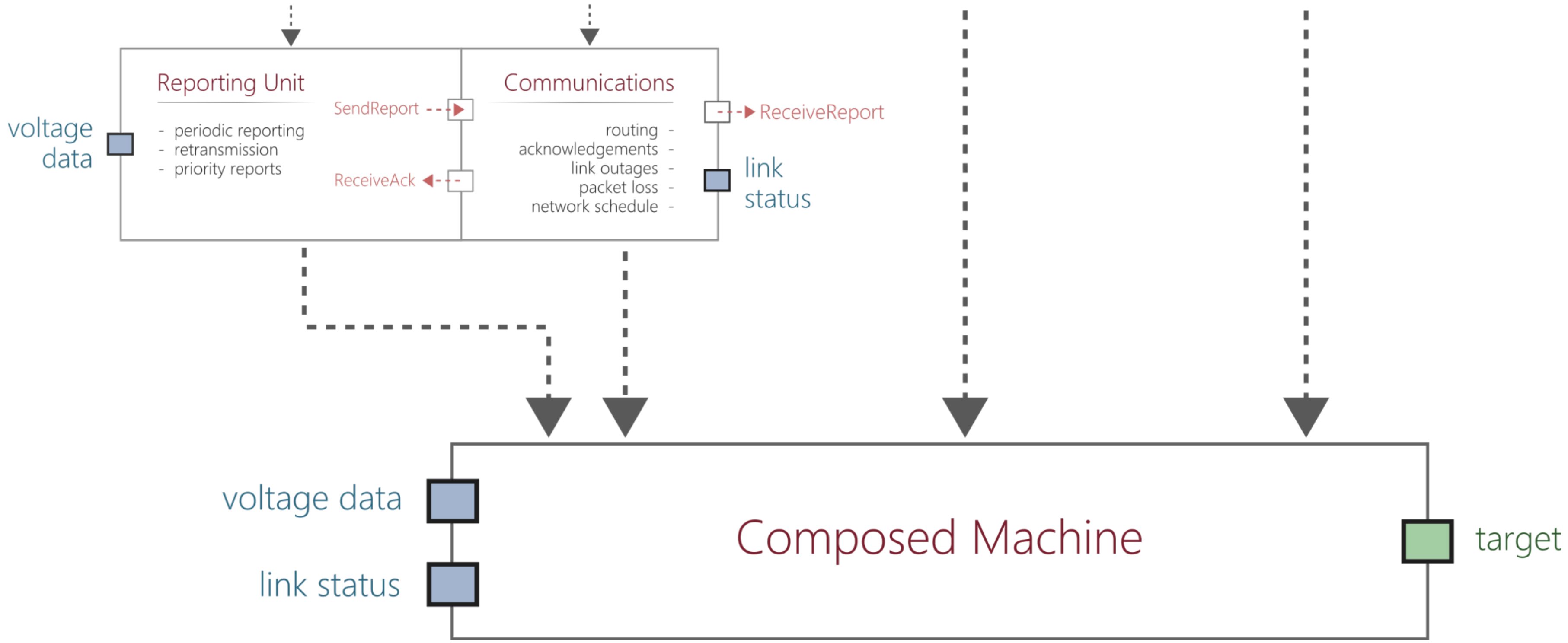


Top-level
- global time
- event scheduler
target
voltage data
System
- target output
- voltage data input
- abstract unit-algorithm communication
Simulation Controller
- cycle sequence
voltage data
Monitoring Network
- packets sent over network
ReceiveReport
Algorithm
safe mode -
comms monitoring -
min/max calculation -
algorithm cycle sequence -
target calculation -
target
voltage data
Reporting Unit
- periodic reporting
- retransmission
- priority reports
SendReport
ReceiveAck
Communications
routing -
acknowledgements -
link outages -
packet loss -
network schedule -
ReceiveReport
link status
voltage data
link status
Composed Machine
target


Top-level
- global time
- event scheduler
System
- target output
- voltage data input
- abstract unit-algorithm communication
Simulation Controller
- cycle sequence
target
voltage data


System
- target output
- voltage data input
- abstract unit-algorithm communication
Simul
target
voltage data
Monitoring Network
- packets sent over network
voltage data
ReceiveReport
Algorithm
safe mode -
comms monitoring -
min/max calculation -
algorithm cycle sequence -
target calculation -
target


Monitoring Network
- packets sent over network
voltage data
ReceiveReport
Reporting Unit
- periodic reporting
- retransmission
- priority reports
SendReport
ReceiveAck
voltage data
Communications
routing -
acknowledgements -
link outages -
packet loss -
network schedule -
ReceiveReport
link status

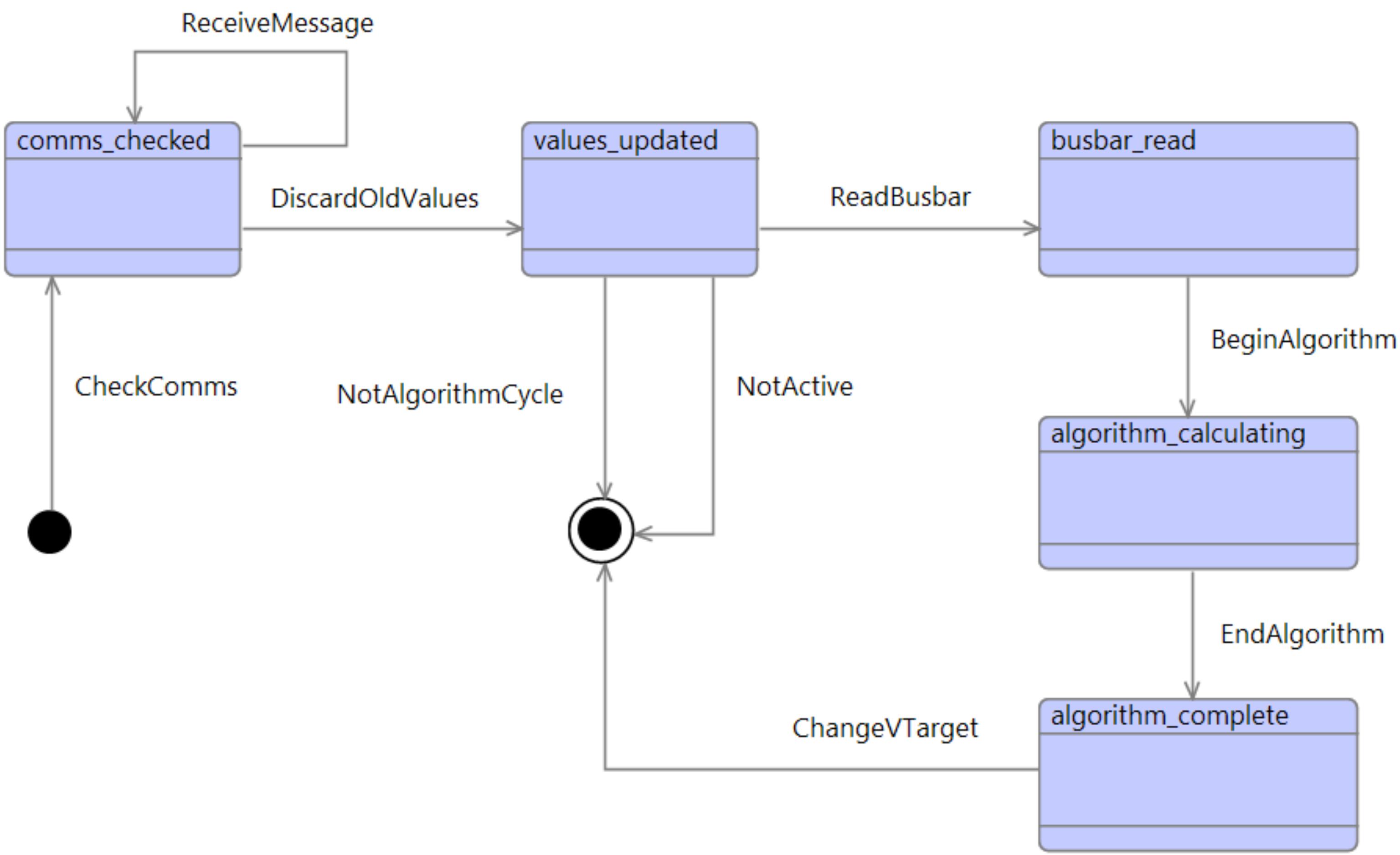

Reporting Unit
- periodic reporting
- retransmission
- priority reports
SendReport
ReceiveAck
Communications
routing -
acknowledgements -
link outages -
packet loss -
network schedule -
ReceiveReport
voltage data
link status
voltage data
link status
Composed Machine
target

UML-B

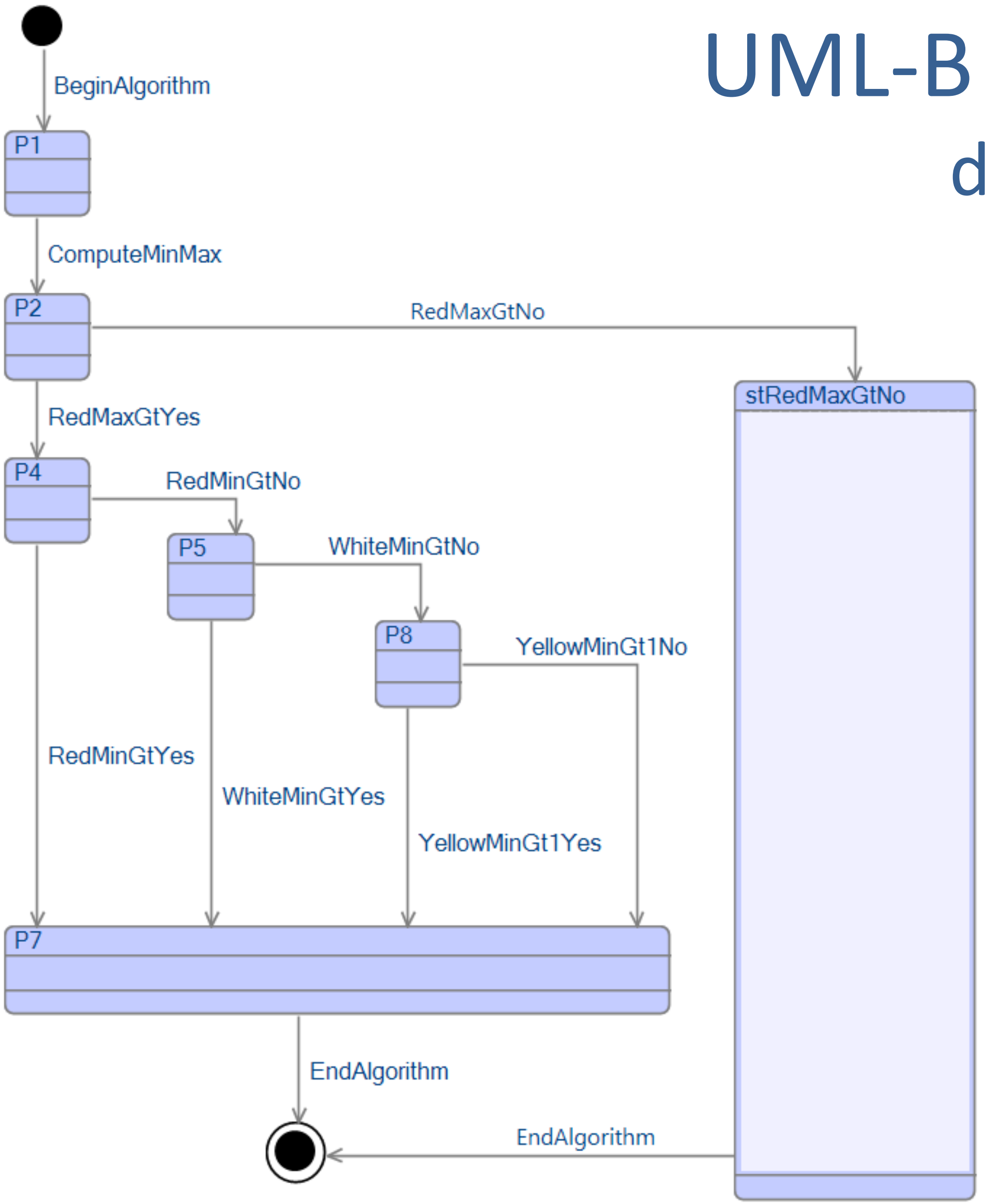
UML-B

- UML-B plugin used to generate state machines
  – Automated translation to Event-B
  – Various behaviour modelled:
    - Abstract system states
    - Algorithm cycle sequence
    - Algorithm decision flow

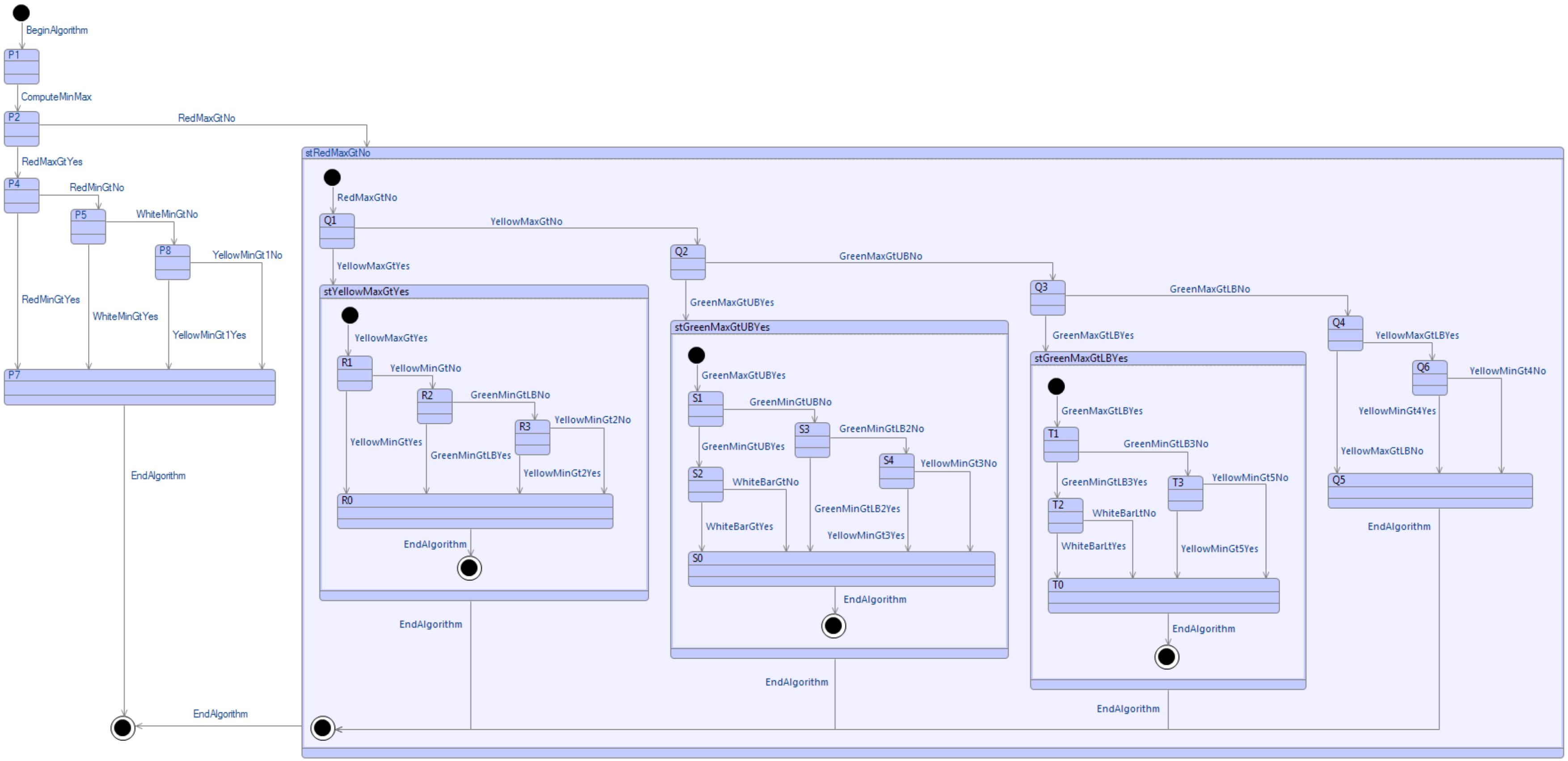
UML-B – algorithm cycle behavior



UML-B – algorithm decision flow



UML-B – algorithm decision flow



SEVENTH FRAMEWORK PROGRAMME

FORMAL PROOF

Formal Proof

- Proof used to analyse **correctness** and **consistency** of algorithm design
  - Effort: ≈ 1 Man Week
- Several issues found as a result and reported back to Selex ES
  - All issues agreed to be valid
  - Some subtle behaviour was previously unknown

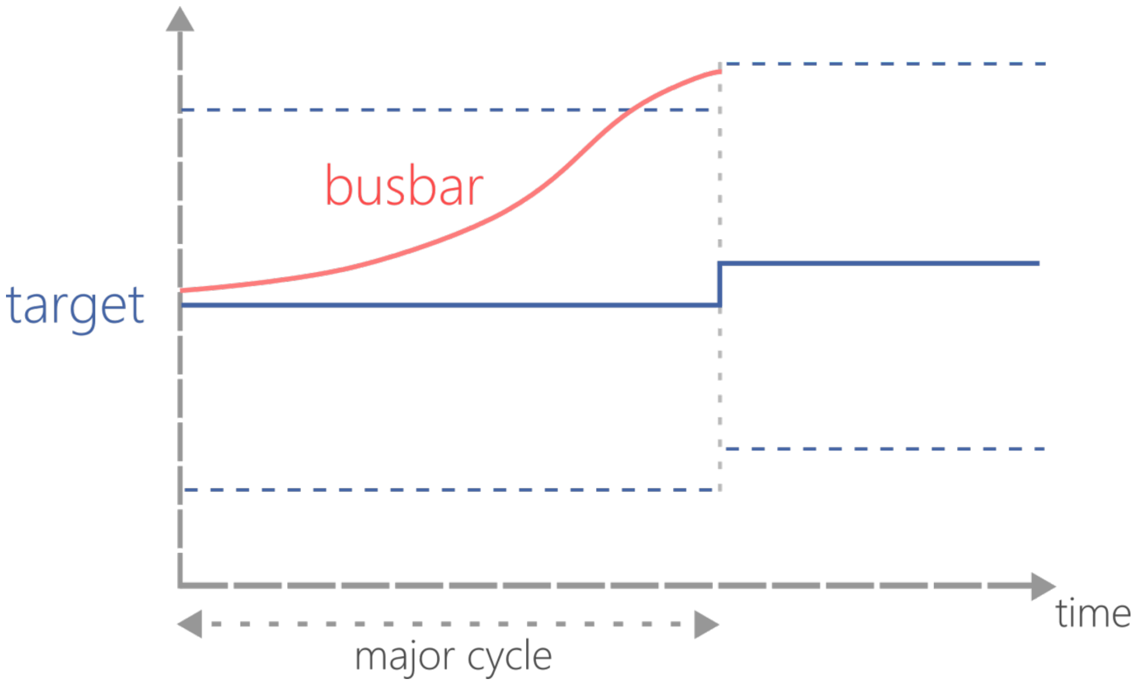
Algorithm Issues

- Violation of busbar voltage bounds
  - No limitations within the formal algorithm design
  - Target voltage could be set outside valid bounds at the transformer
- Simultaneous minimum and maximum voltages
  - No well defined behaviour in this case

SEVENTH FRAMEWORK PROGRAMME

Algorithm Issues

- Potentially unexpected behaviour when busbar voltage is close to the allowed bandwidth
  - New target calculation based on busbar voltage, not current target



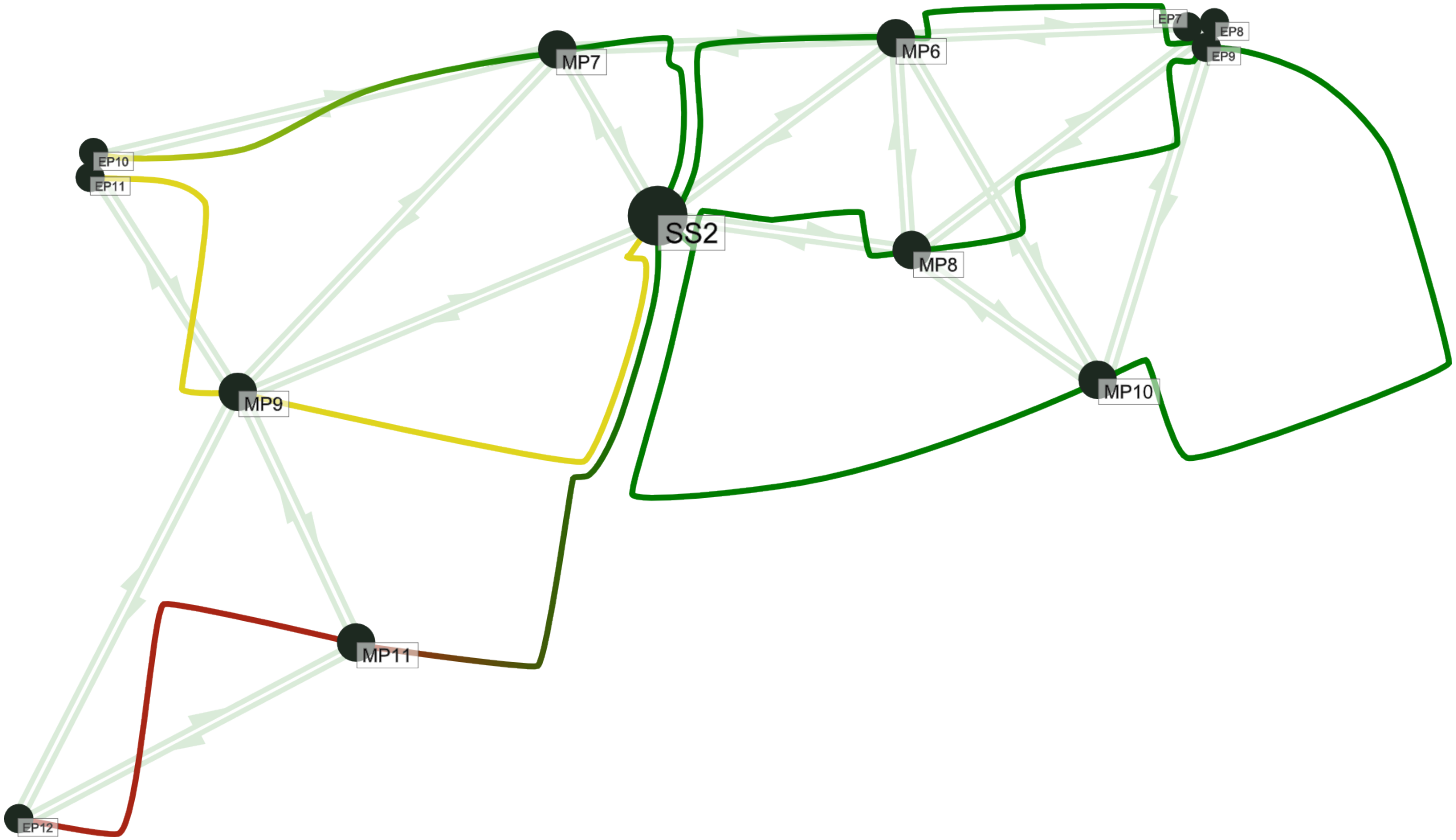
COMMUNICATION MODEL

SEVENTH FRAMEWORK PROGRAMME

Communications Model

- The sensors are connected to the algorithm via a mesh network
- Communication through each node is provided by a SilverSprings module, and decides how to route packets based on link characteristics
- The behaviour of the nodes is modelled using Event-B, and the status of each communication link is modelled using Modelica
- When links are down, nodes store packets. This behaviour is explored during the verification and simulation.

Mesh Network



DOMAIN MODELS

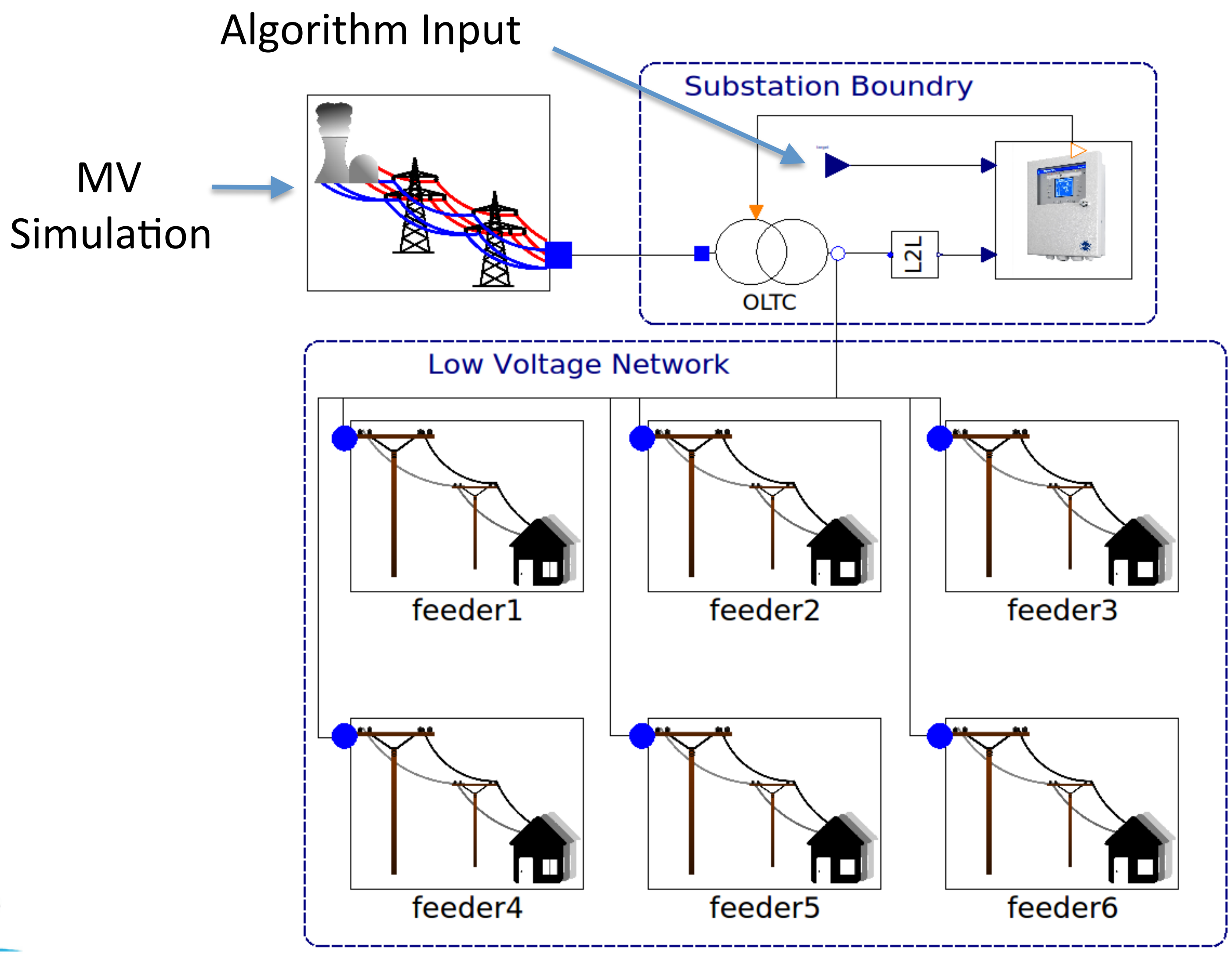
SEVENTH FRAMEWORK PROGRAMME

Domain Models

- Represents **physical aspects** of the system.
  - Low Voltage network.
  - Consumer demand and generation.
  - Communications outages.
- Uses **graphical** modelling language: Modelica.
- Validates solution by **Model-In-the-Loop** testing.

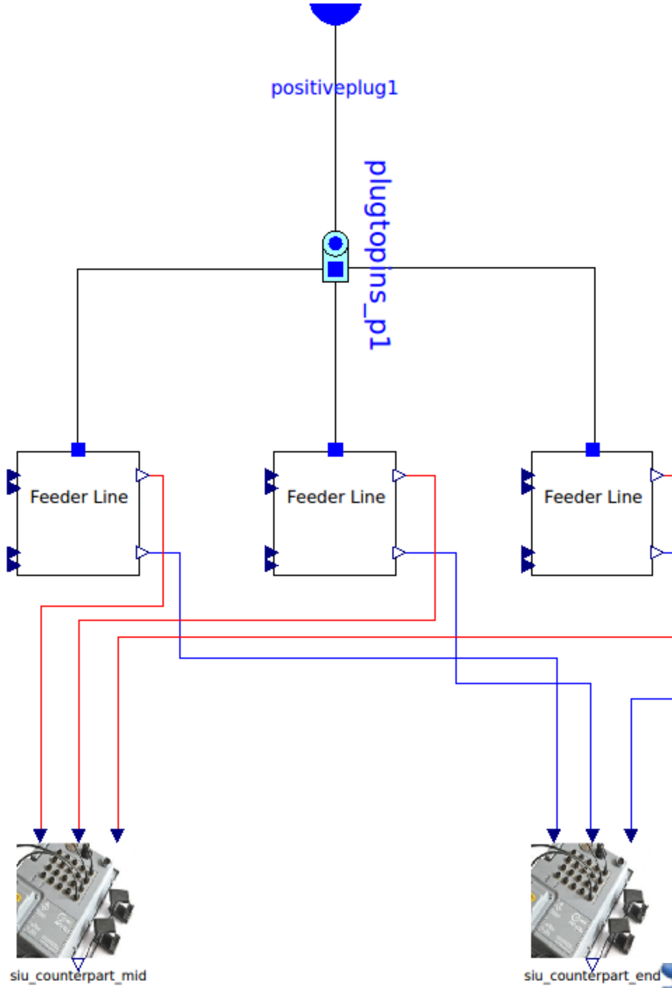
SEVENTH FRAMEWORK PROGRAMME

Network Model

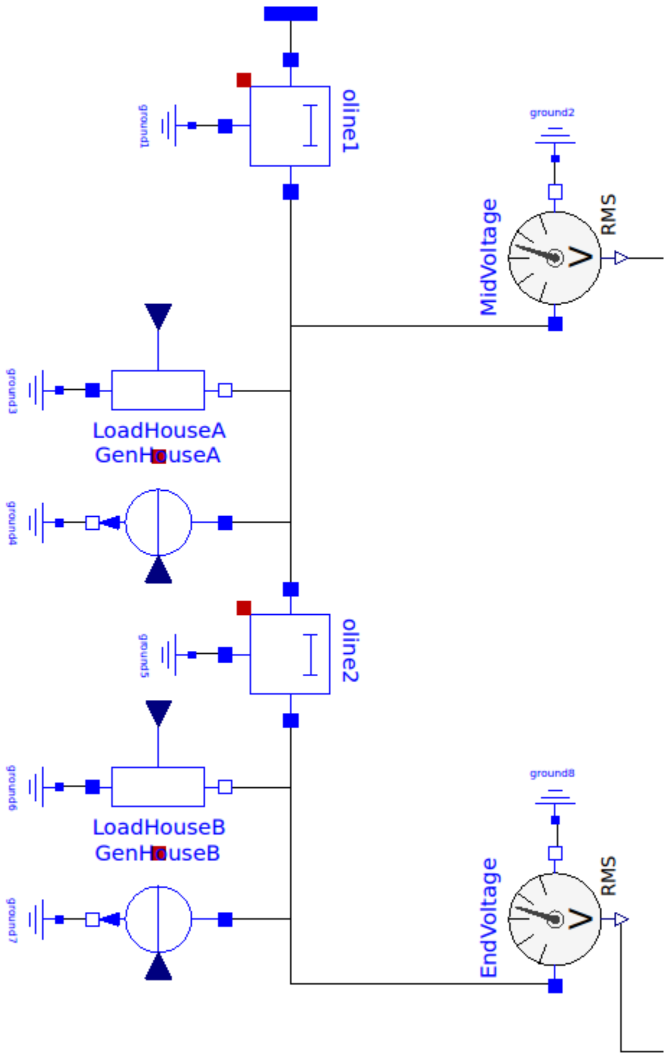


3 Phase Feeder

- Represents 3 phase feeder with two MCU units.
- Splits 3 phase line into 3 single phase lines.

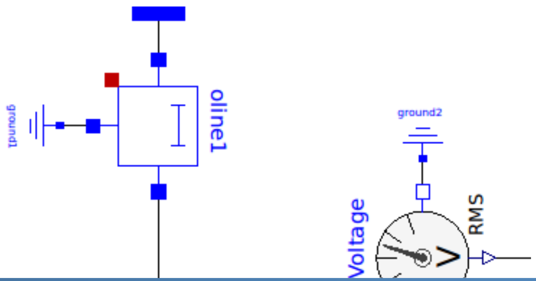


Single Phase Line

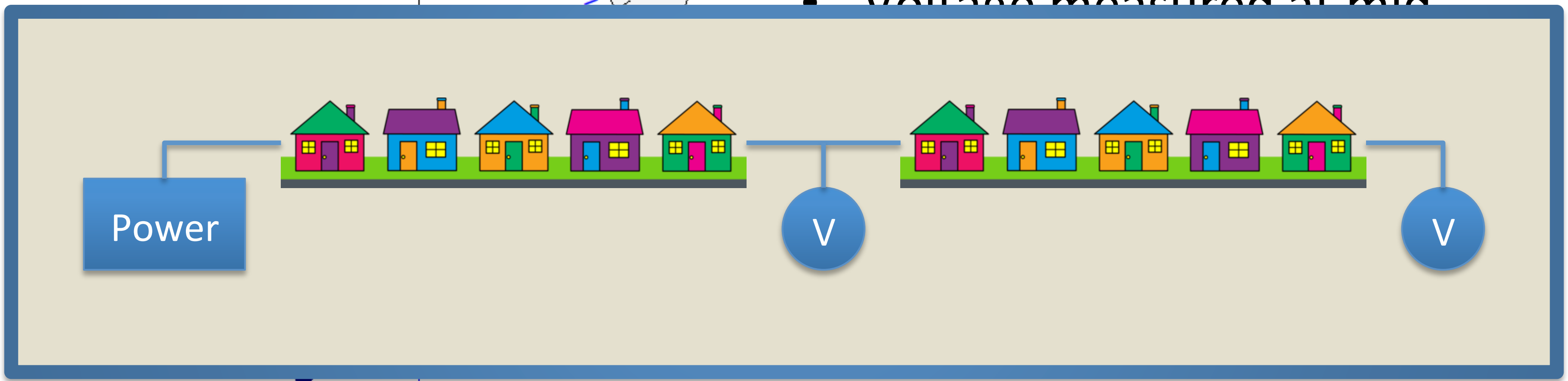


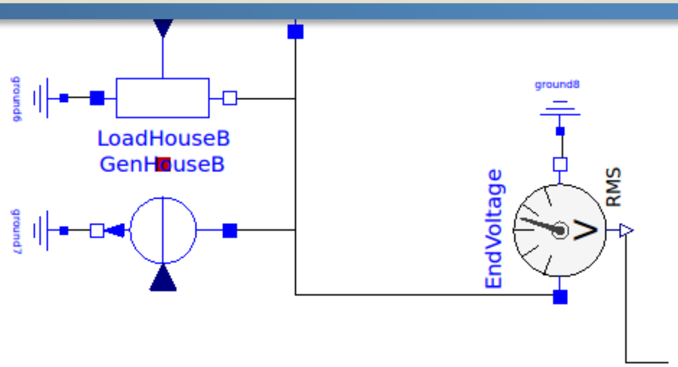
- Represents two blocks of houses with photovoltaics
- Voltage measured at mid and end points
- Photovoltaic simulations are provided by stochastic model

Single Phase Line



- Represents two blocks of houses with photovoltaics
- Voltage measured at mid





End-User Simulation (1)

- Used pre-built consumer model.
  - Demand and Generation.
  - Based on actual statistics.

- Parameterised by:

Appliances in house	Number of occupants
Weekday / Weekend	Day of year
PV panel size	

SEVENTH FRAMEWORK PROGRAMME

End-User Simulation (2)

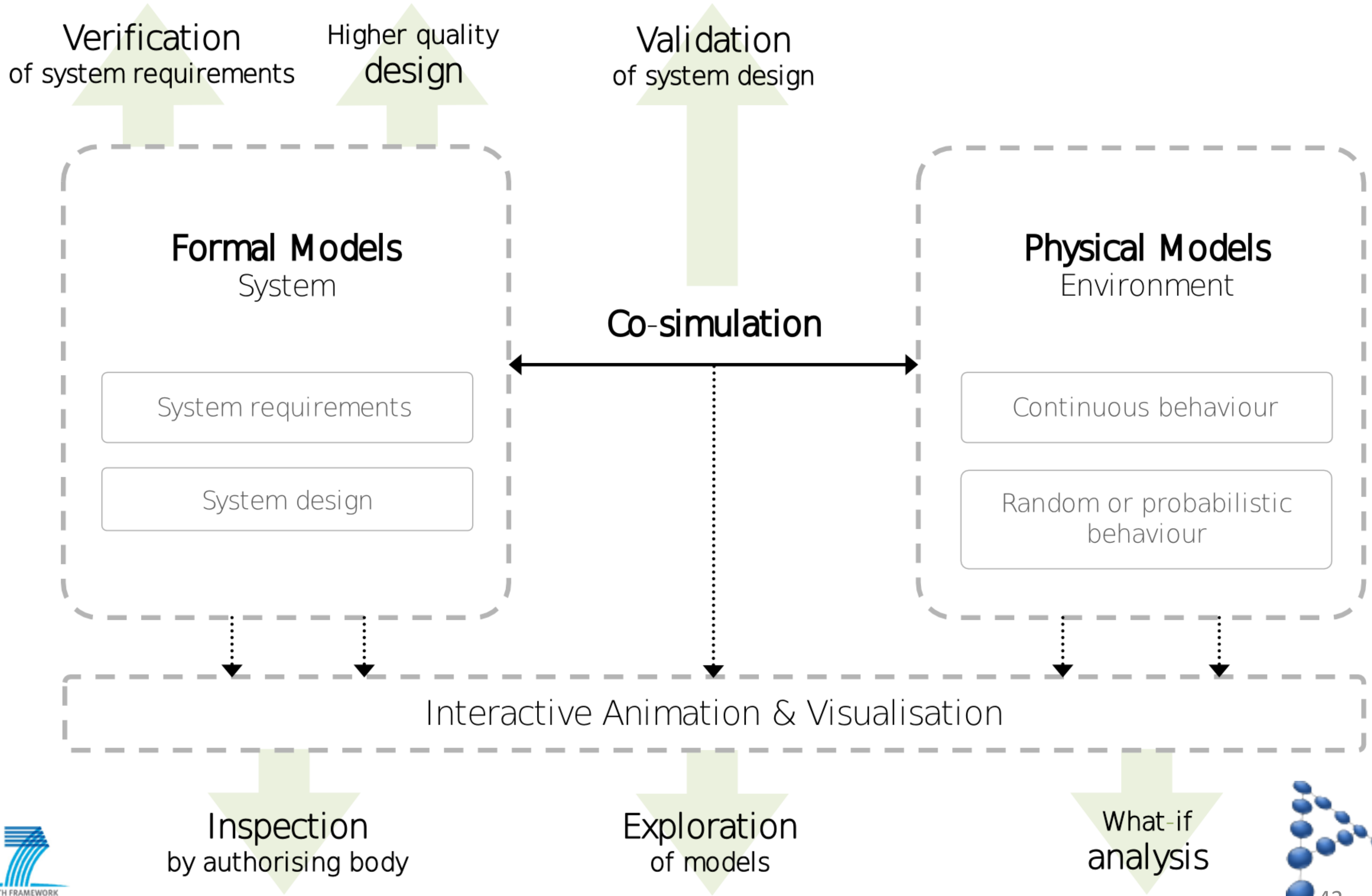
- Gathered statistics from Government sources.
  - Probability of house having PV = Number of PV installations/Number of dwellings.
  - Average generating size of PV panel.
  - Probability of number of occupants being 1,2,3,4,5+.

- Used real data from install site to determine number of on each feeder.

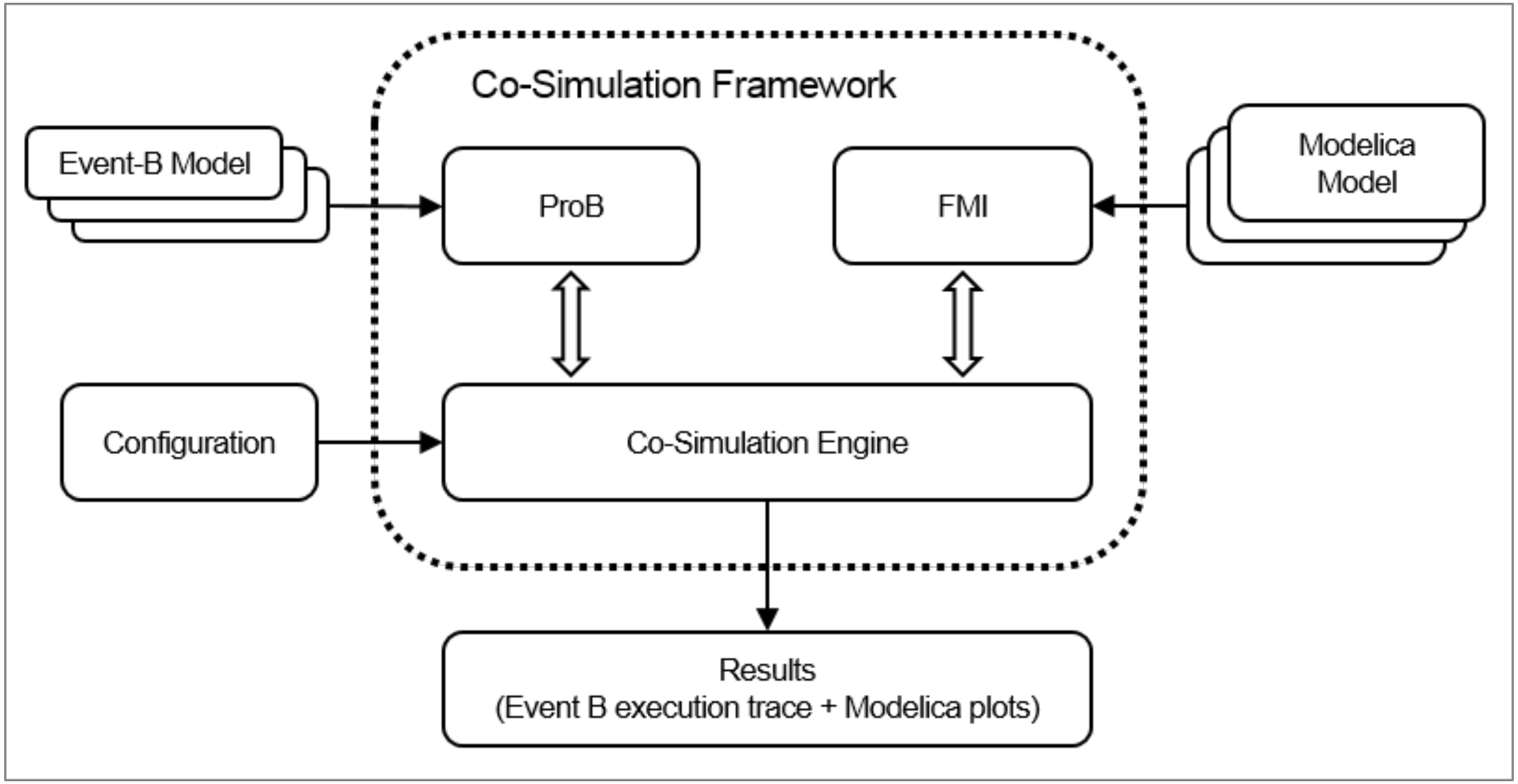
SEVENTH FRAMEWORK PROGRAMME

CO-SIMULATION

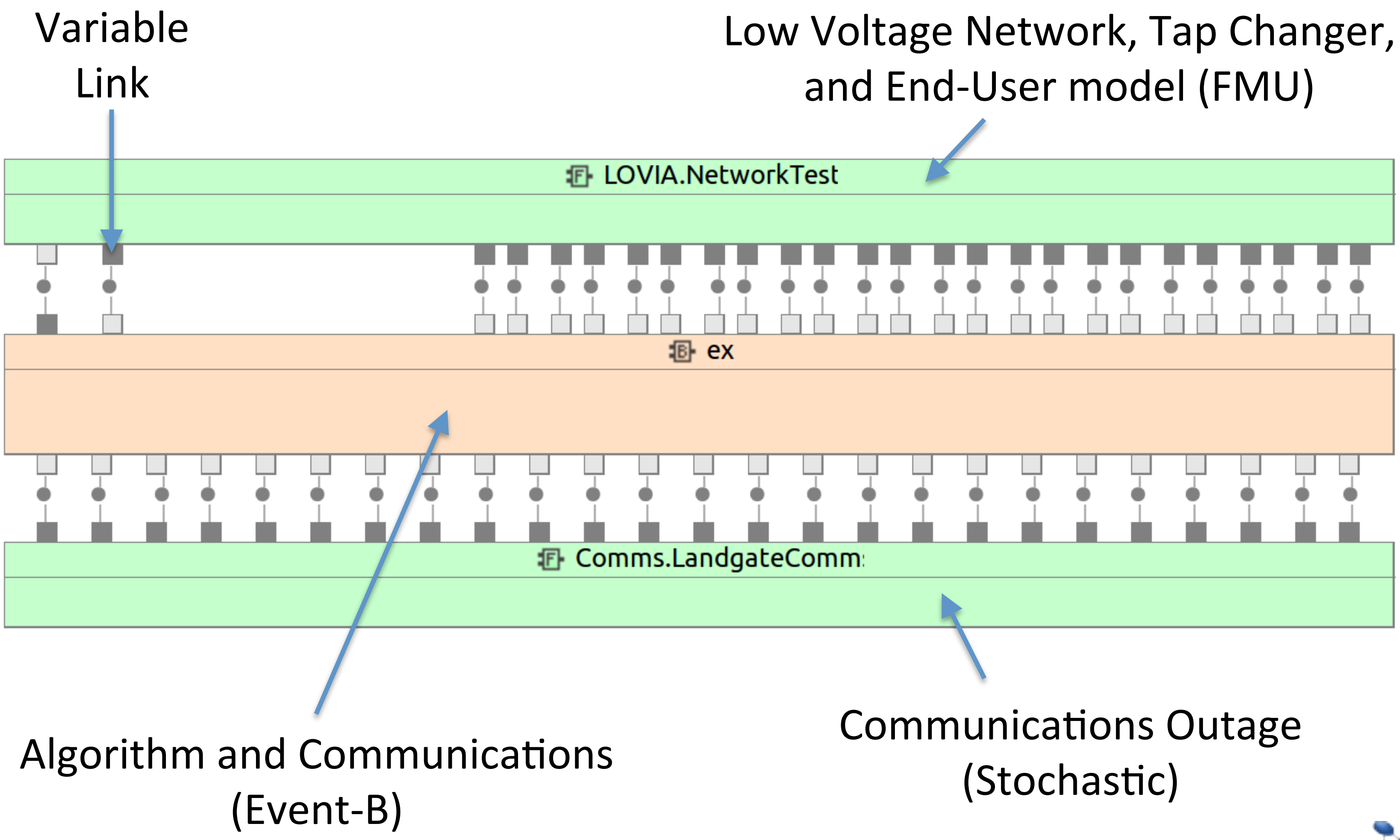
Co-Simulation



Simulation Architecture

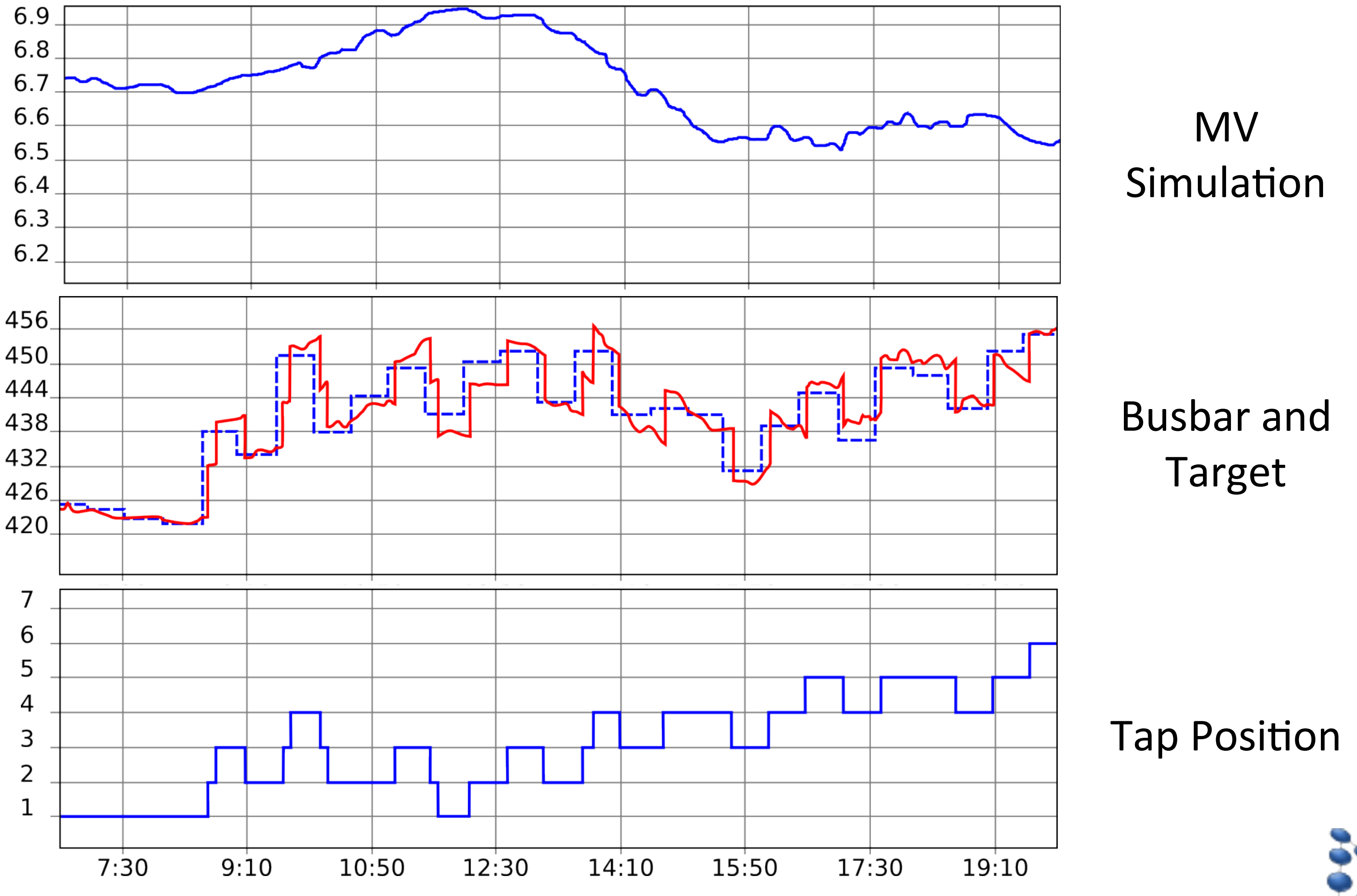


Co-simulation Component View



RESULTS

Inputs and Outputs of Algorithm



Visualisation

Visualisation

SEVENTH FRAMEWORK PROGRAMME

CONCLUSIONS

SEVENTH FRAMEWORK PROGRAMME

Conclusions

- Smart Grid application was to challenge ADVANCE toolset on complex systems.
  - Demonstrated: applying formal proof to large systems is feasible.
  - Application outside traditional formal methods domain.
- Some issues found with **scalability** of approach.
  - Performance issues due to size and complexity of models.
  - Tool improvements implemented as a result.
- Toolset still requires specialist support when adopting into industry.
  - Visualisations and graphical tools (UML-B) help mitigate this.
  - Automated proof removes burden from engineer, but still require a good understanding of the underlying formalism.

SEVENTH FRAMEWORK PROGRAMME

Conclusions

- Combined **simulation**, **animation** and **formal proof**.
  - Identifies erroneous designs faster, with higher assurances.
  - Allows 'what-if' analysis

- The composition of both methods is complementary:
  - **Simulation** helps the **validation**,
  - **Formal methods** helps the **verification**.

SEVENTH FRAMEWORK PROGRAMME