MODELLING RELIABILITY OF SMART GRID SERVICES WITH STOCHASTIC REWARD NETS

Stanislav Chren

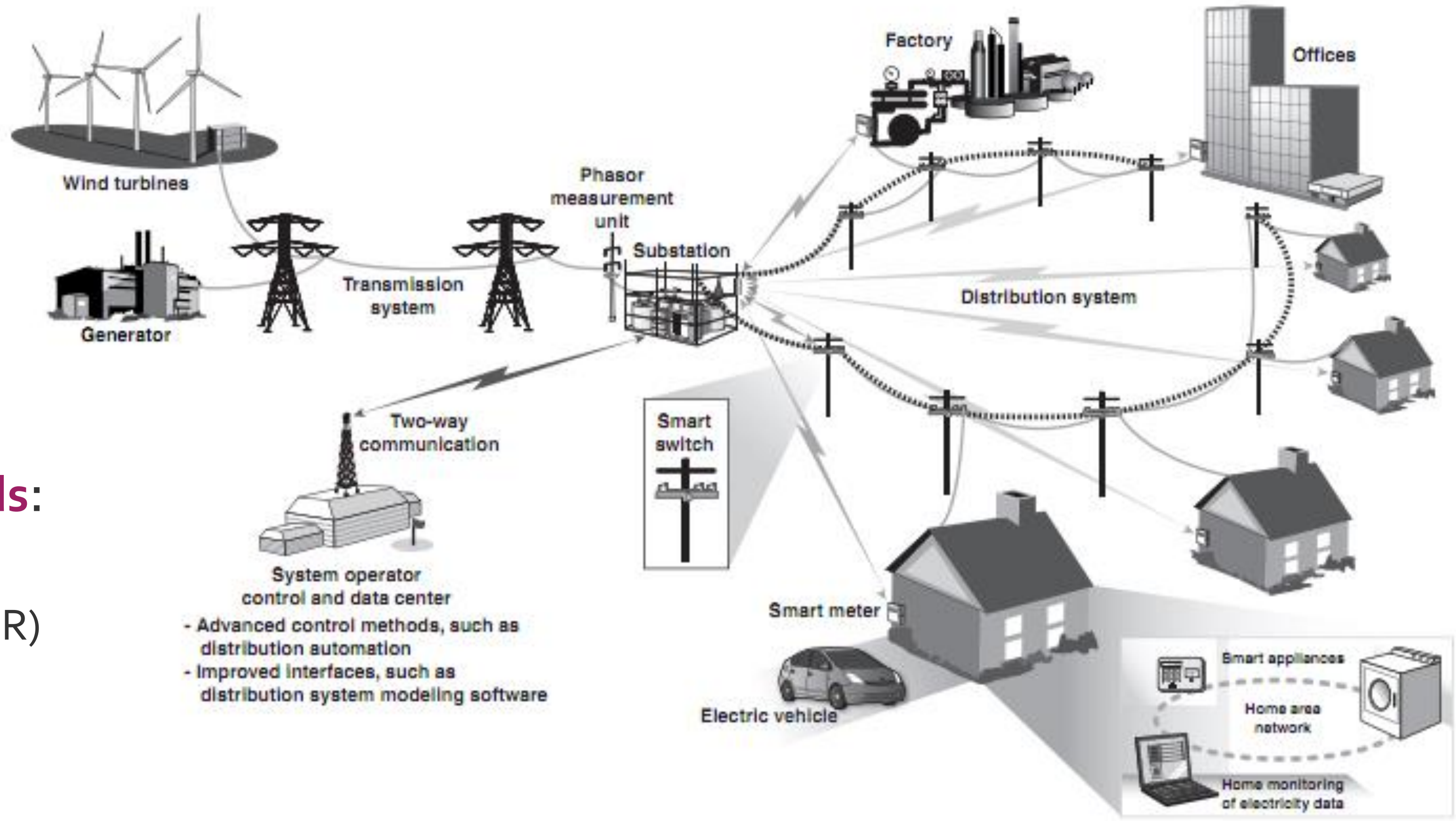
LAB OF SOFTWARE ARCHITECTURES AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY, BRNO

RELIABILITY IN SMART GRIDS

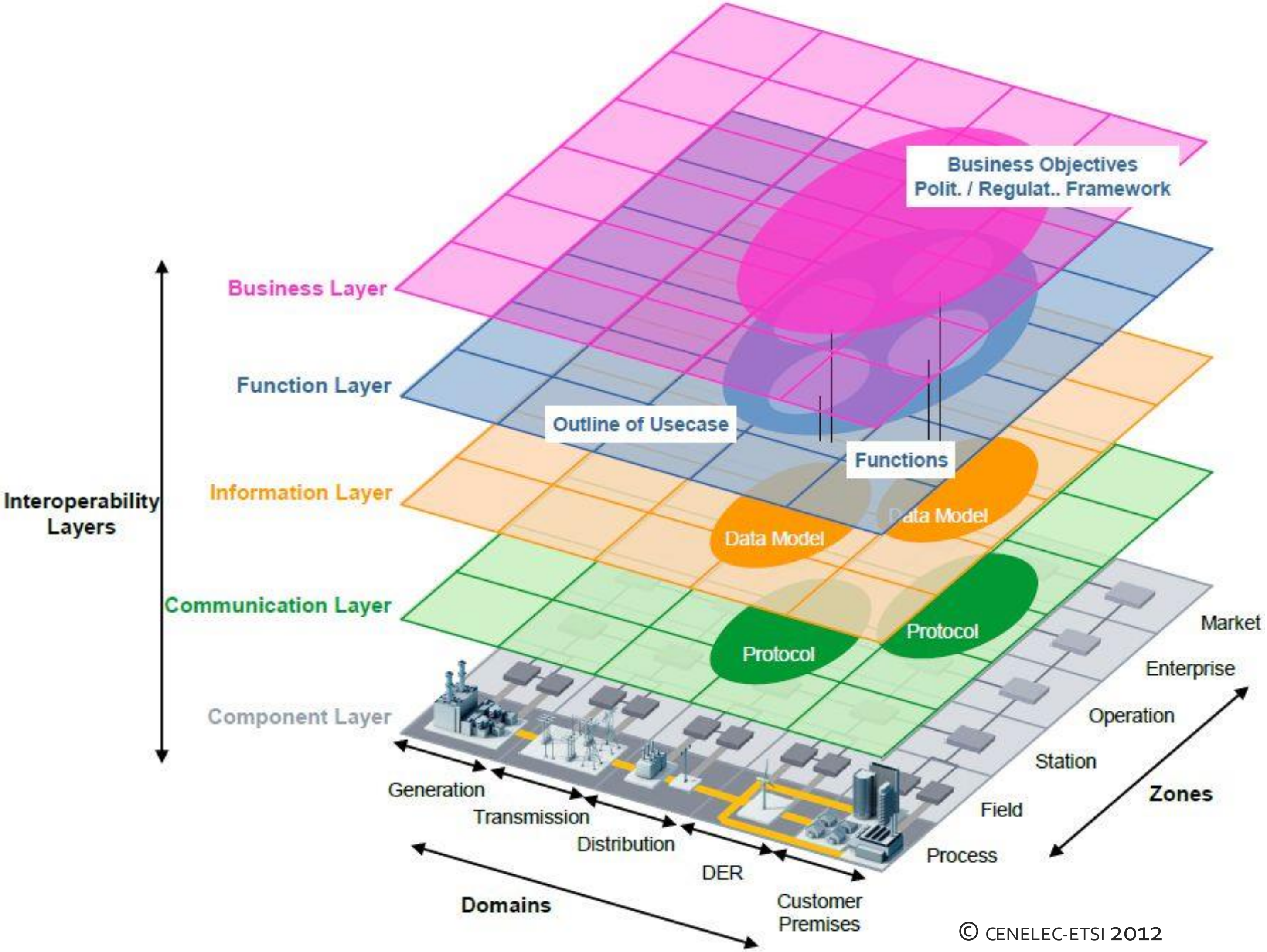
Smart Grid

- **Smart grid** is an electricity network that employs innovative products and services together with intelligent monitoring, control, communication and self-healing technologies.
- Challenges of **legacy power grids**:
  - Uninterrupted power supply
  - Distributed energy resources (DER)
  - Load management
  - New types of electrical devices



lasaris

Smart Grid Reference Architecture



Smart Grid Reliability

- Power (smart) grid is considered a **critical infrastructure**
  - High requirements for reliability
  - Close relation to security, adequacy, availability, survivability and resilience
- Understanding of reliability varies between grid layers
  - **Communication**
    - fraction of time a service is available, fraction of successfully delivered packets, packet delivery latency,…
  - **Distribution**
    - SAIFI, SAIDI, CAIDI, …
- **Loss of load** probability

Existing Approaches for Reliability Analysis

- Reliability engineering
  1. Reducing the likelihood or frequency of the failure.
  2. Identification and correction of the causes of the failures
  3. Dealing with occurred failures
  4. **Estimating the likely reliability of new designs and analysis of reliability data**
- Most of the reliability-related effort focus on
  - Fault-tolerance, fault-prevention and failure-recovery
- Reliability estimation methods for (smart) power grids consider **physical layer only**.
  - Probability of blackouts
  - HW and communication links failures
- **Missing** evaluation of failures in **software components**.

lasaris

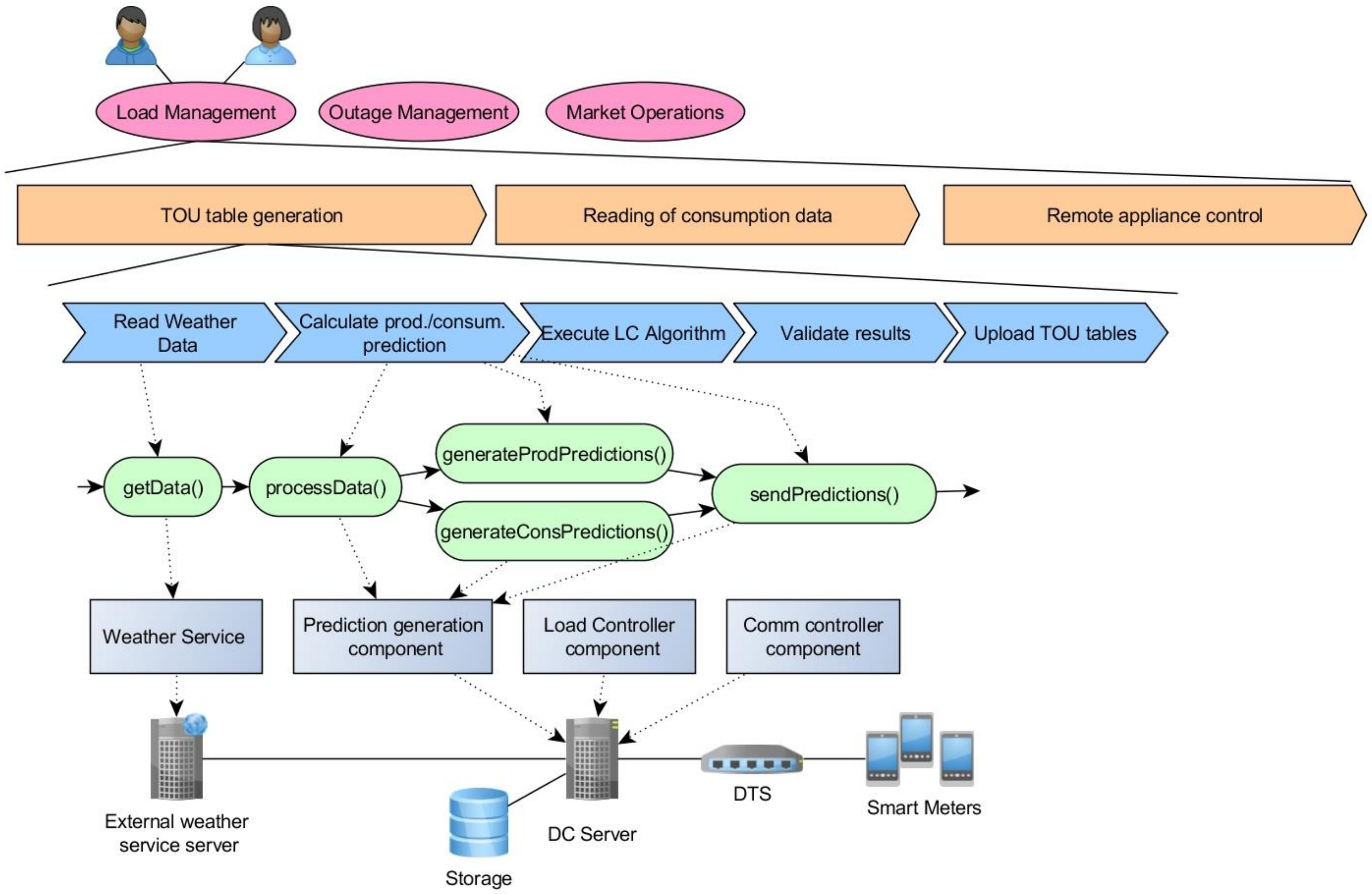
Existing Approaches for Reliability Analysis

- Perception of the reliability in the smart grid systems should expand also to **other layers** and to **additional failure types**
- Not all failures in smart grid must result in blackout
- E.g. a **Billing use case**
  - There might be a failure during the reading of the smart meter
    - Incorrect consumption data => wrongly calculating the price for power consumption.
  - Such failure does not cause a power outage
    - Might have negative impact on the associated stakeholders
    - Possible impact on other use-cases (e.g. load management algorithms).

lasaris

Aims of my research

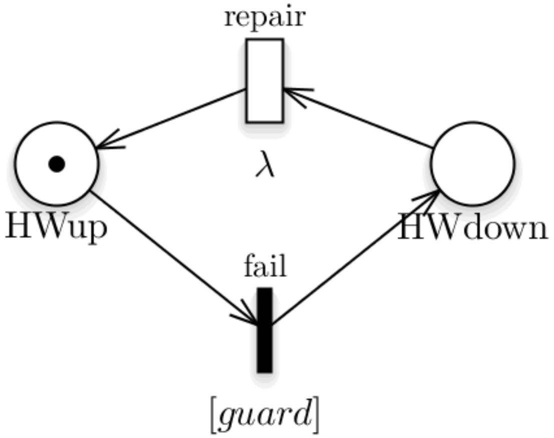
- **Multi-layered** approach for the reliability analysis of a smart grid infrastructure.



PETRI NETS/STOCHASTIC REWARD NETS

Stochastic Reward Nets

- Stochastic Reward Net(SRN) is a special case of PN with several extensions. The most important are
  - **Timed** and **Immediate** transitions
  - Transition **guards**
  - **Reward functions**



- The SRN is transformed into **Markov Reward Model**, which is then solved to provide reliability, availability and performance related measures
- Typical output measures are
  - Pmf of number of tokens at given place
  - Expected number of firings of transitions (throughput)
- Multiple reward functions can be defined for the same net topology

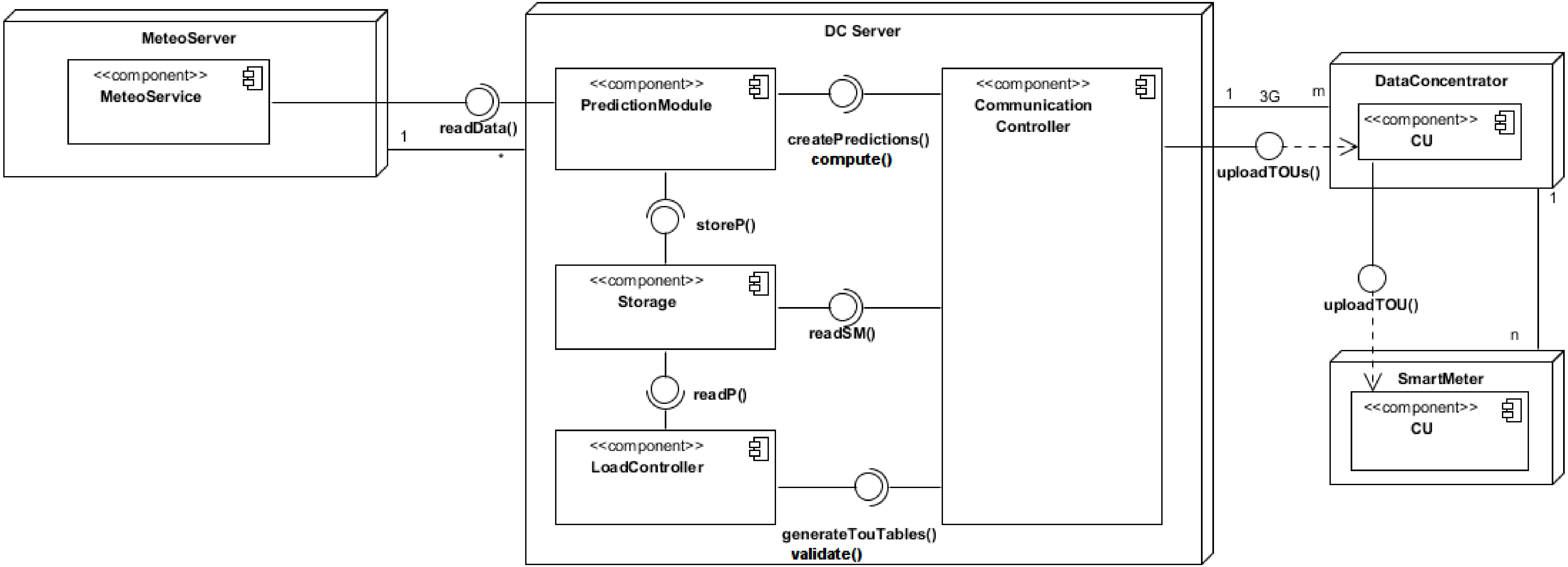
MULTI-LAYERED RELIABILITY MODEL

SRN Model

- Supported layers
  - Physical layer
  - Software/Service layer
  - Communication layer
  - Energy layer
- Will be generated from the annotated UML models (deployment and sequence diagrams)
- Usage/Service layer is hierarchically decomposed into multiple levels
- Connection between levels via guard conditions
- Integration of communication link failures
- Modelling of large number of devices
- Hardware and software failures with dependencies

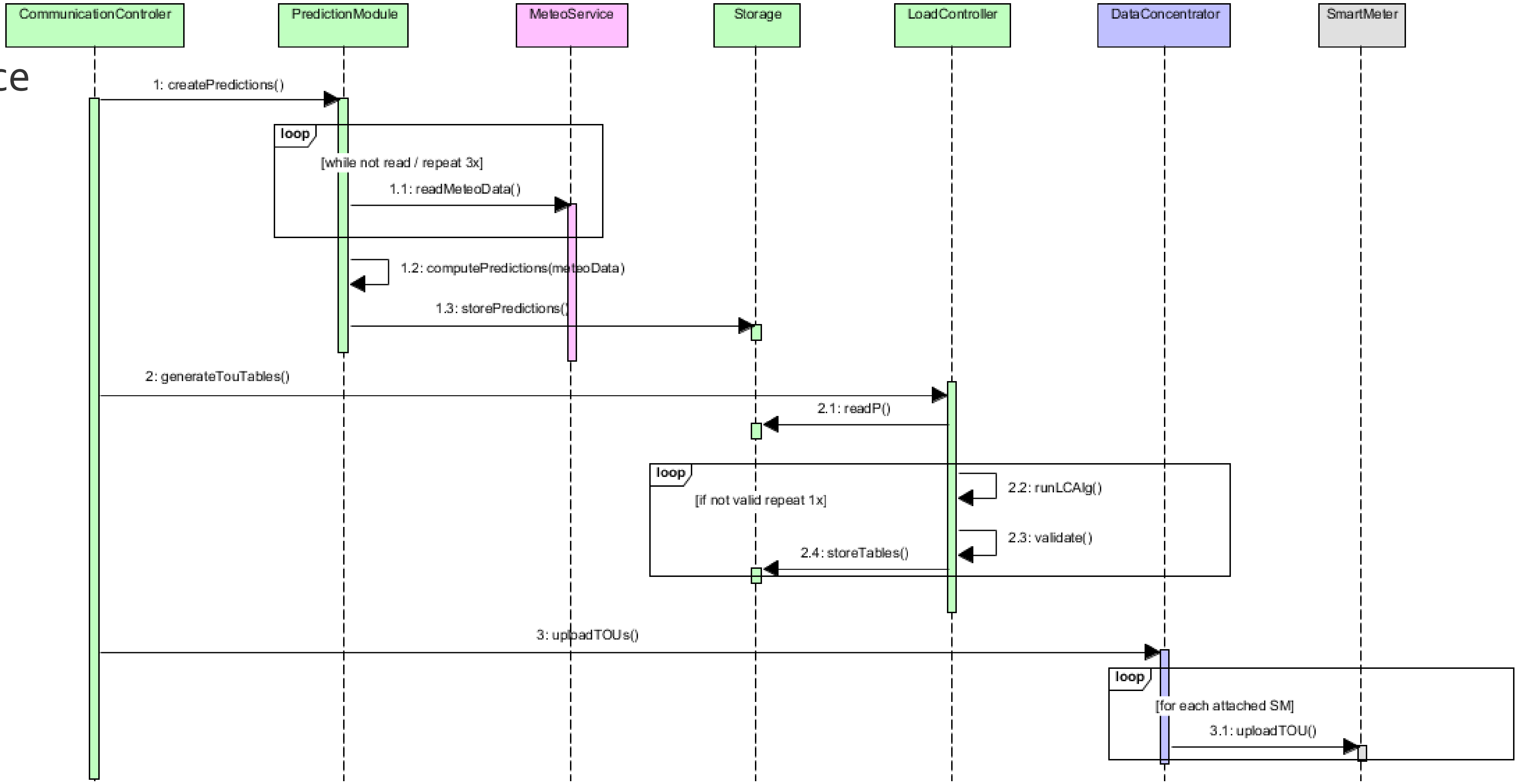
TOU Table Generation and Upload Scenario

- Deployment diagram



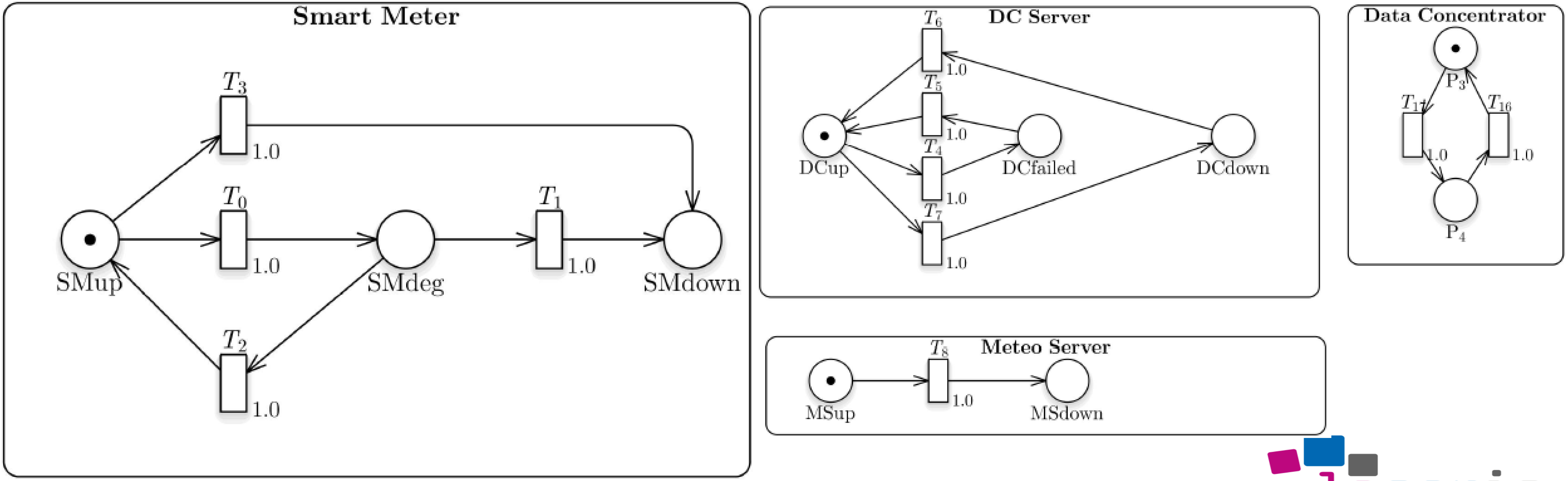
TOU Table Generation and Upload Scenario

- Sequence diagram



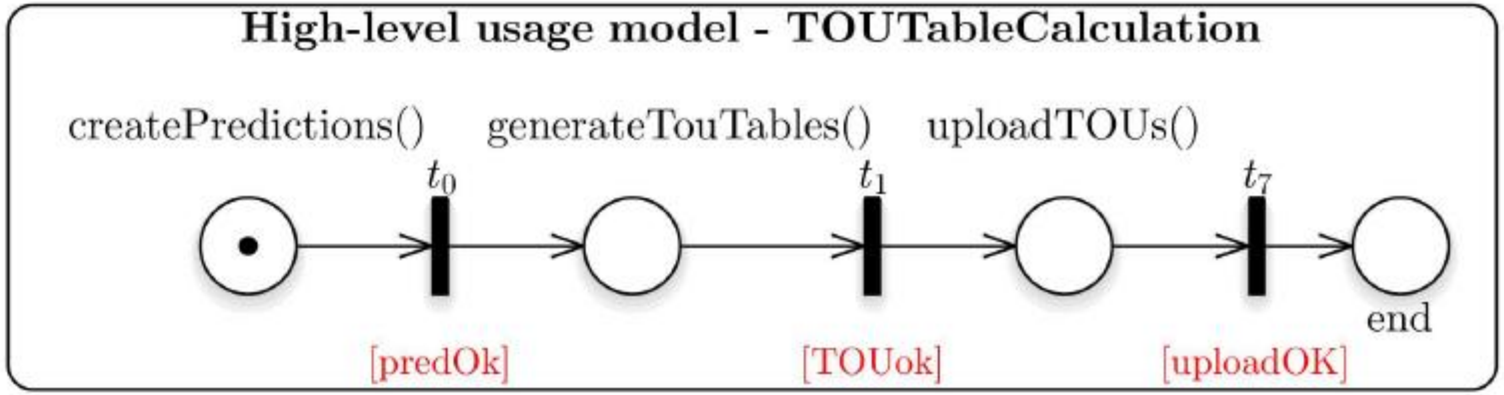
Hardware/system model

- Support for failure and degraded service states.
- Connected to service models through guards



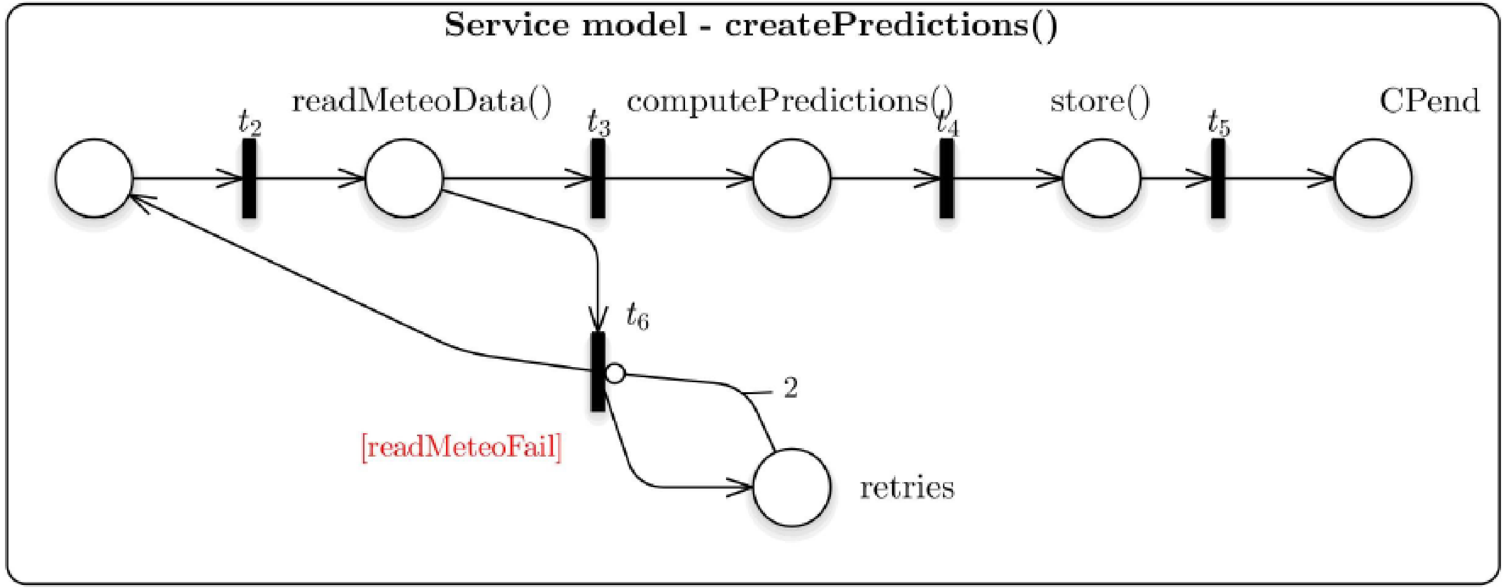
High-level usage model

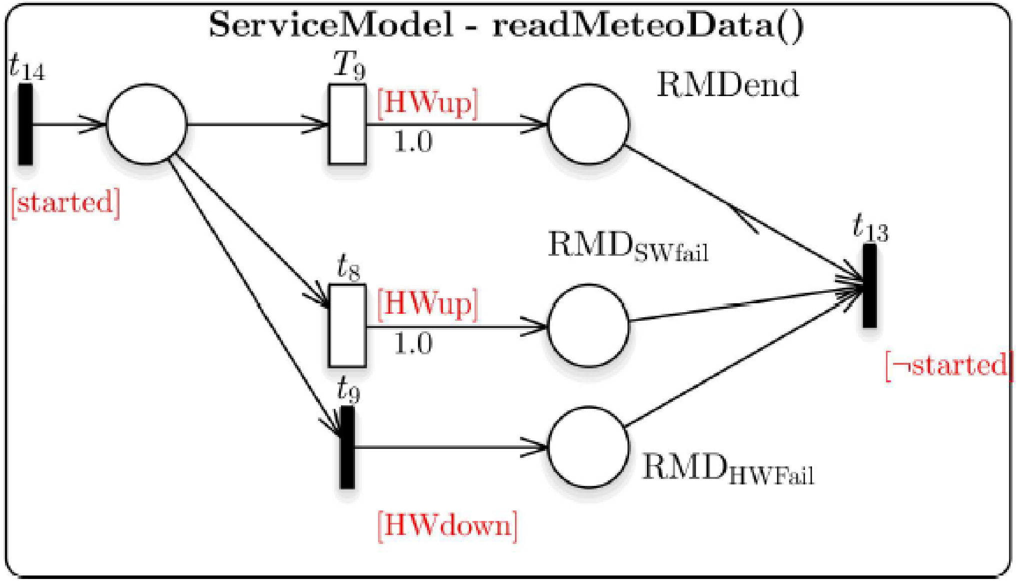
- Contains methods/service calls from the actor
- The immediate transitions are enabled by successful completion of the previous operation



Usage model - service level

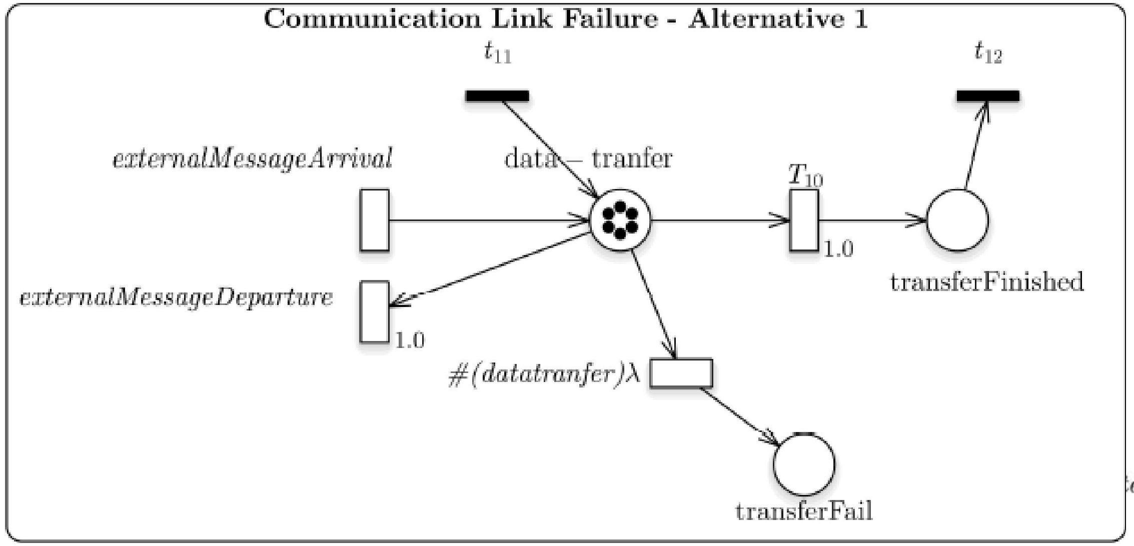
- Represents behaviour of the service/method calls
- Can contain other service/method calls or internal processing actions
- The internal actions depend on the availability of the required HW resources
- Can model different types of failures (hw, sw) and recovery mechanisms.

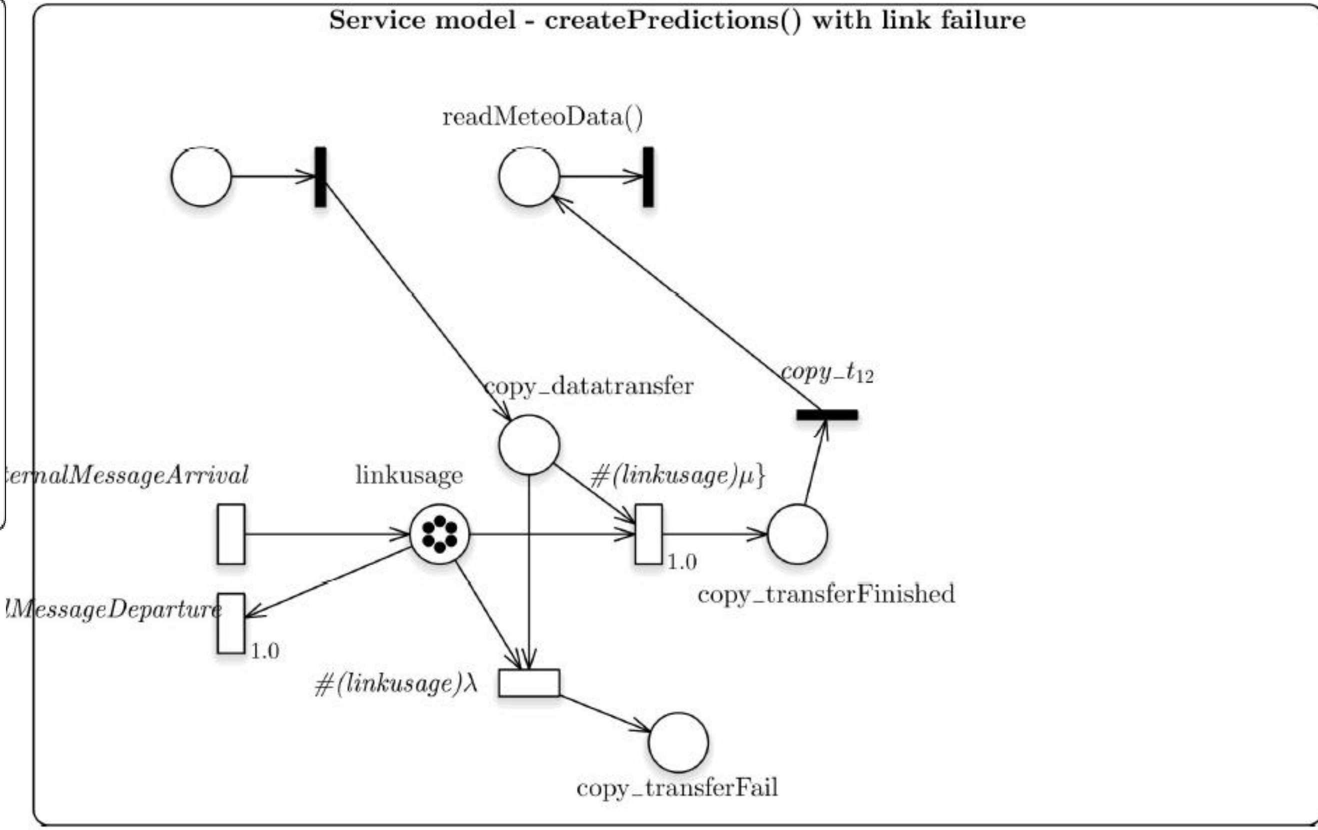




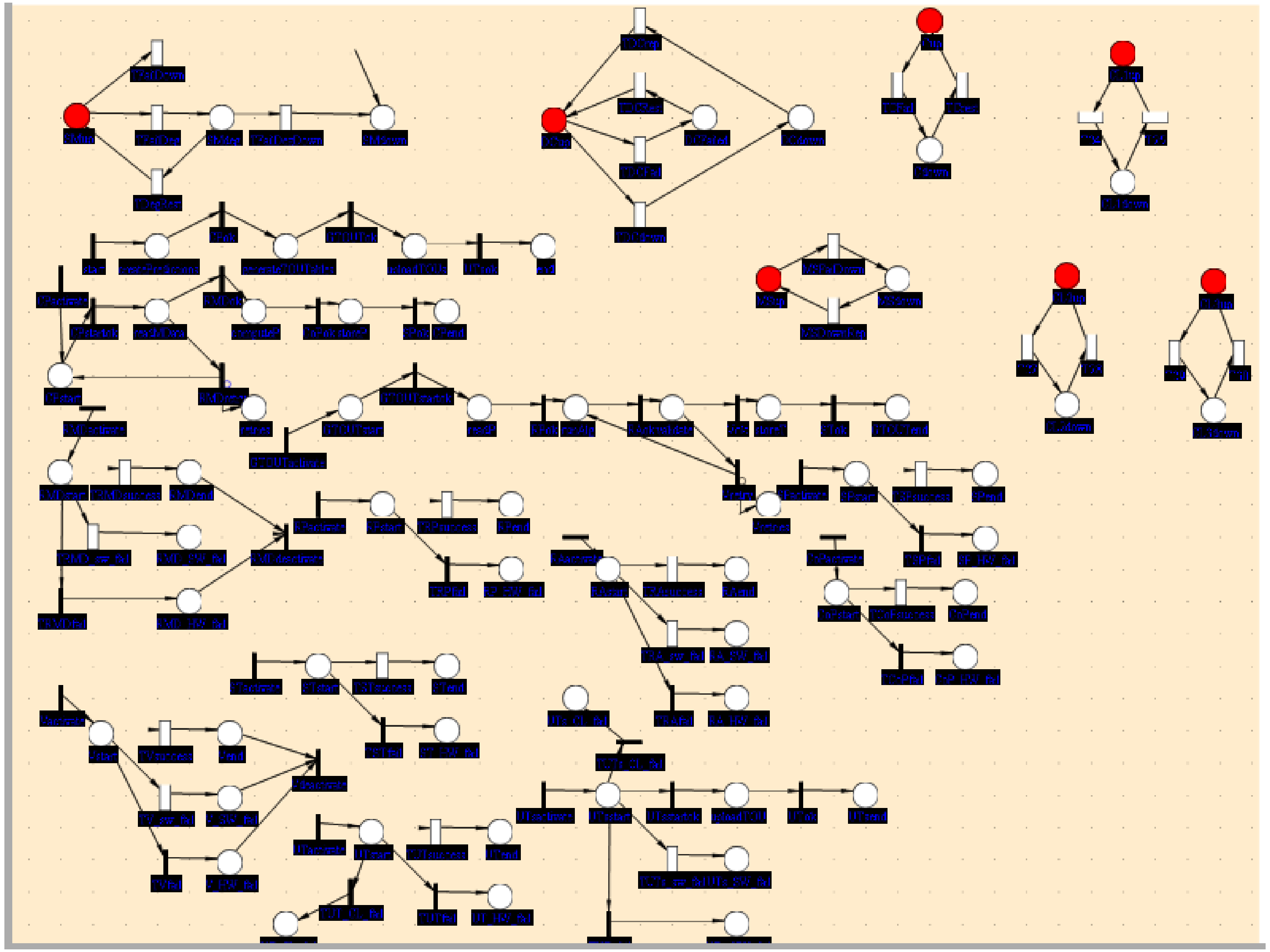
Communication link failures

- Inserting communication segment into a service model





Scenario – SPNP implementation

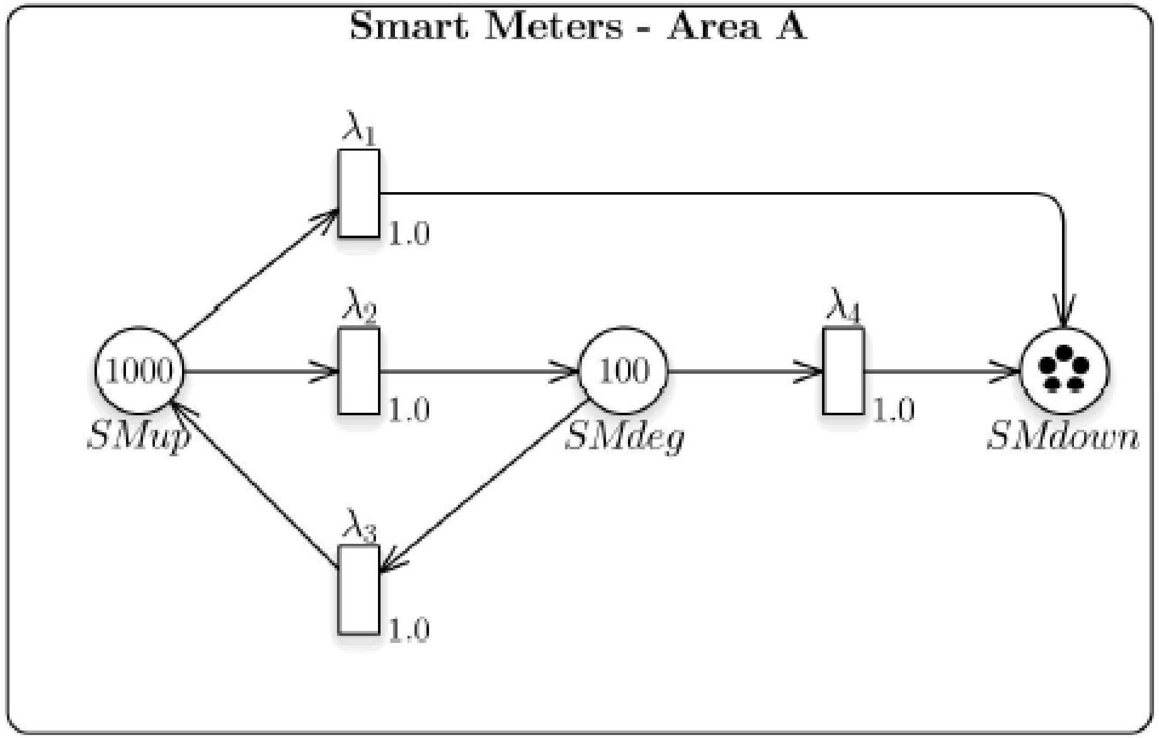


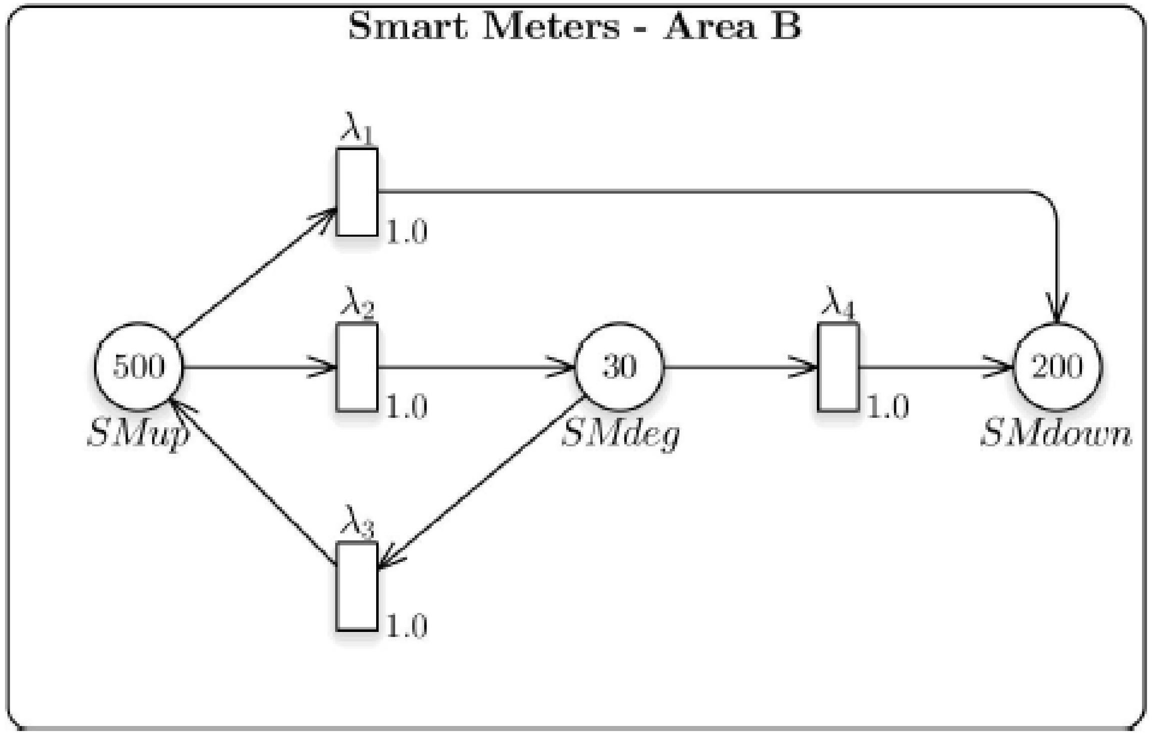
- SRN
  - 67 places
  - 41 immediate transitions
  - 30 timed transitions
  - Guards on most transitions
- Reachability graph/CTMC
  - 17 760 markings
  - 140 177 transitions
  - Analysis time – 3s

lasaris

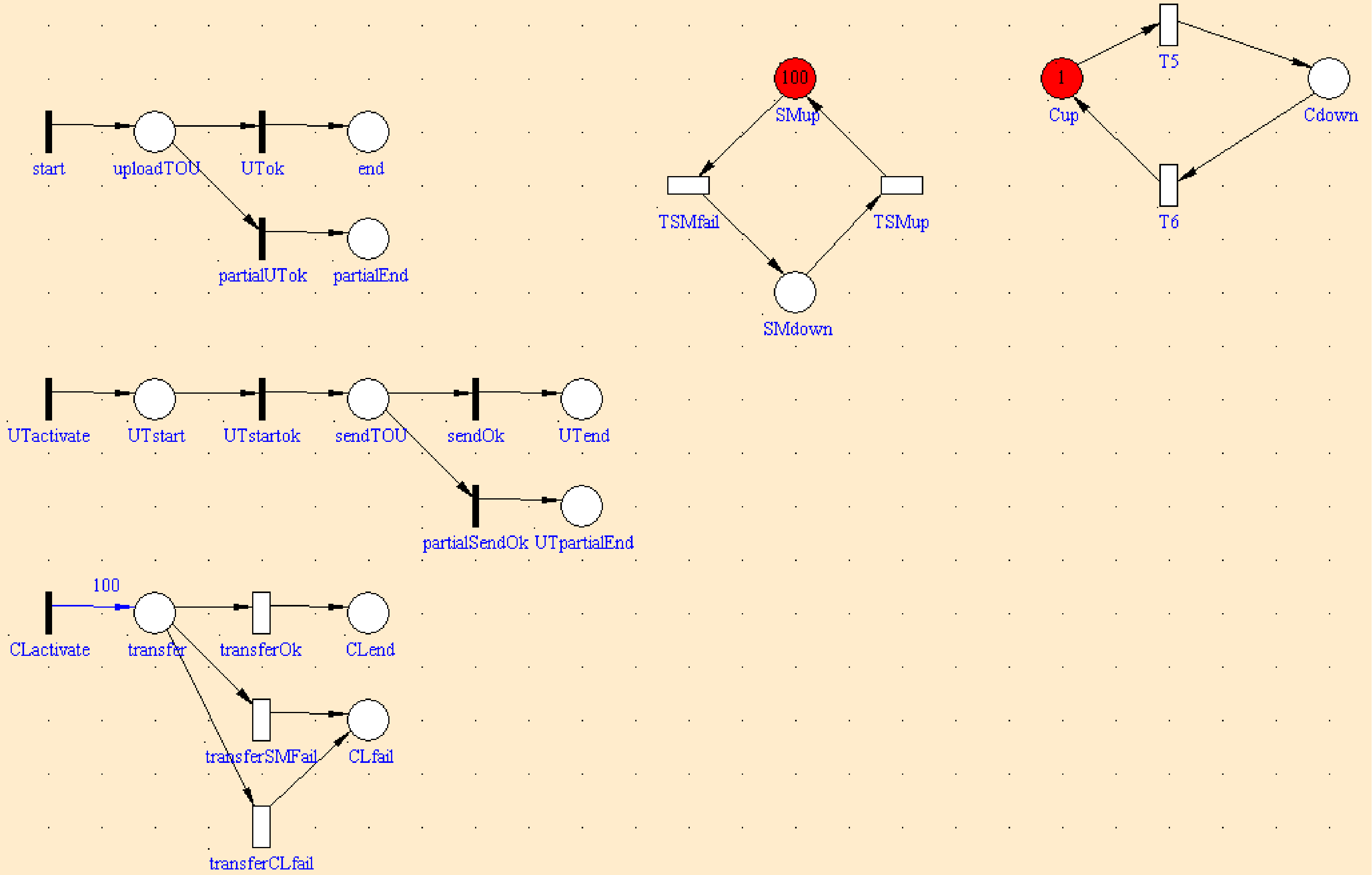
Large number of devices

- The devices are represented by tokens instead of nets.



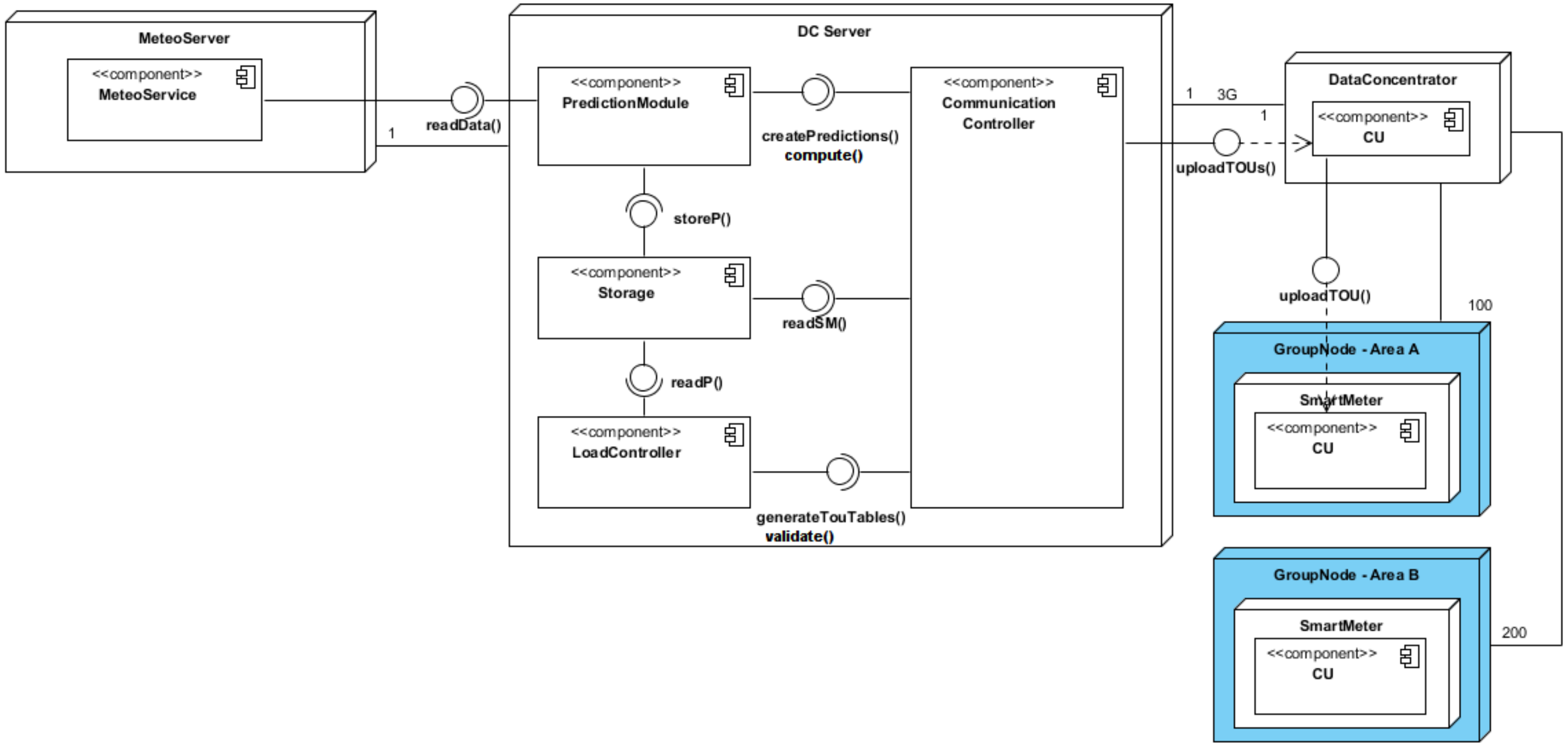


Large number of devices - SPNP



- 100 tokens for messages and 100 tokens for SM
- G_transferOk = [#transfer<=#SMup]
- Reachability Graph/CTMC
  - 1 040 502 markings
  - 4 797 703 transitions
  - ~ 10min computation

Large number of devices – Group nodes

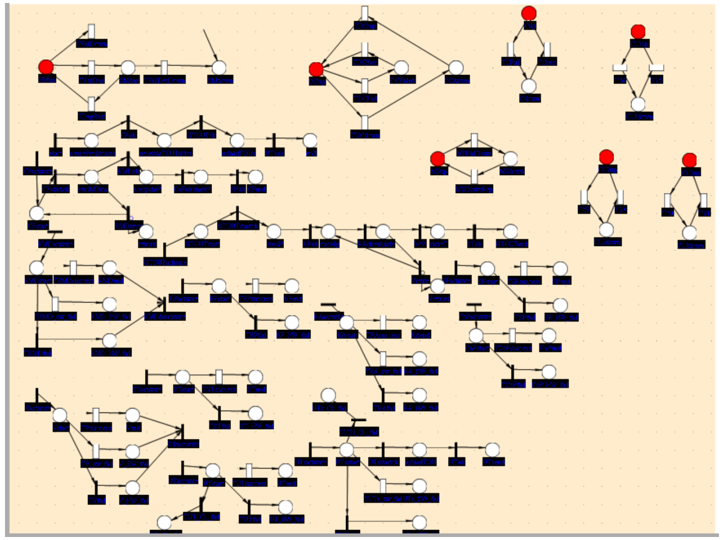


- Group nodes (GNs) represent large number of HW nodes
  - Group nodes for different locations, technologies, etc. with different parameters
- Alternatively, GNs could contain sub-nodes for different classed of devices.

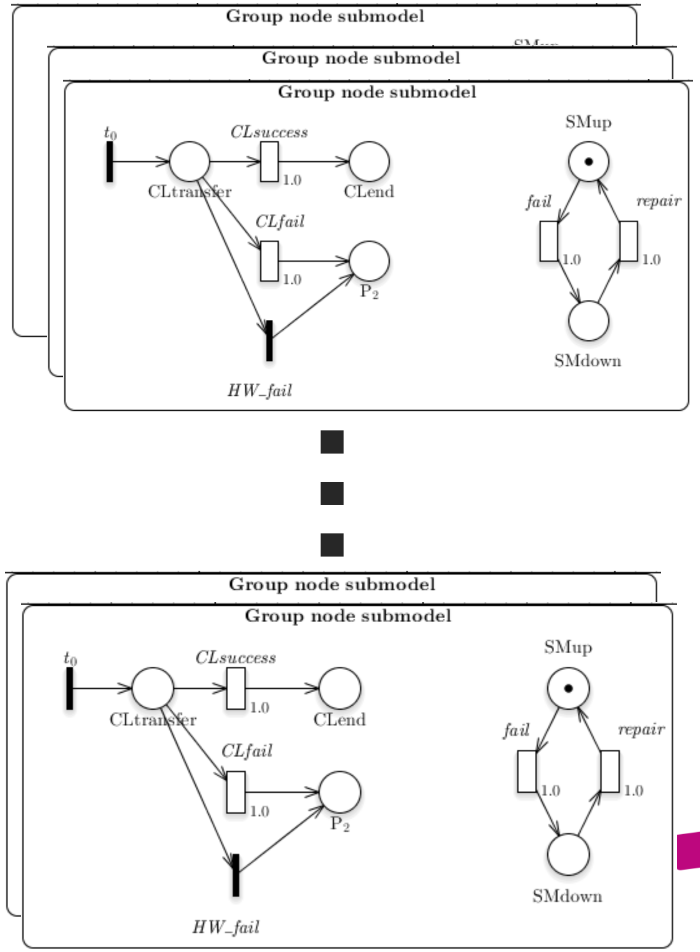
Large number of devices – Group nodes II

- GN submodel is solved first and serves as input for Service/HW model

Service/HW model



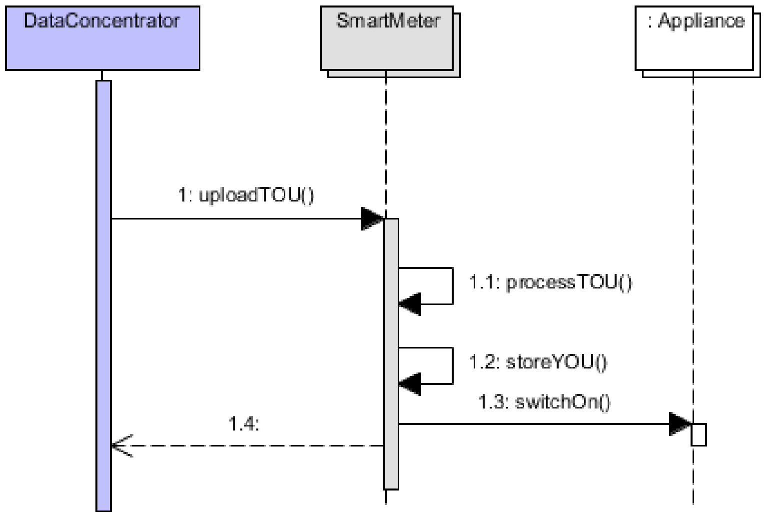
Failure/success rates, number of successes

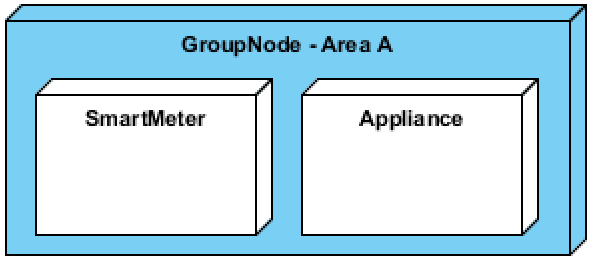


lasaris

Large number of devices – Possible enhancements

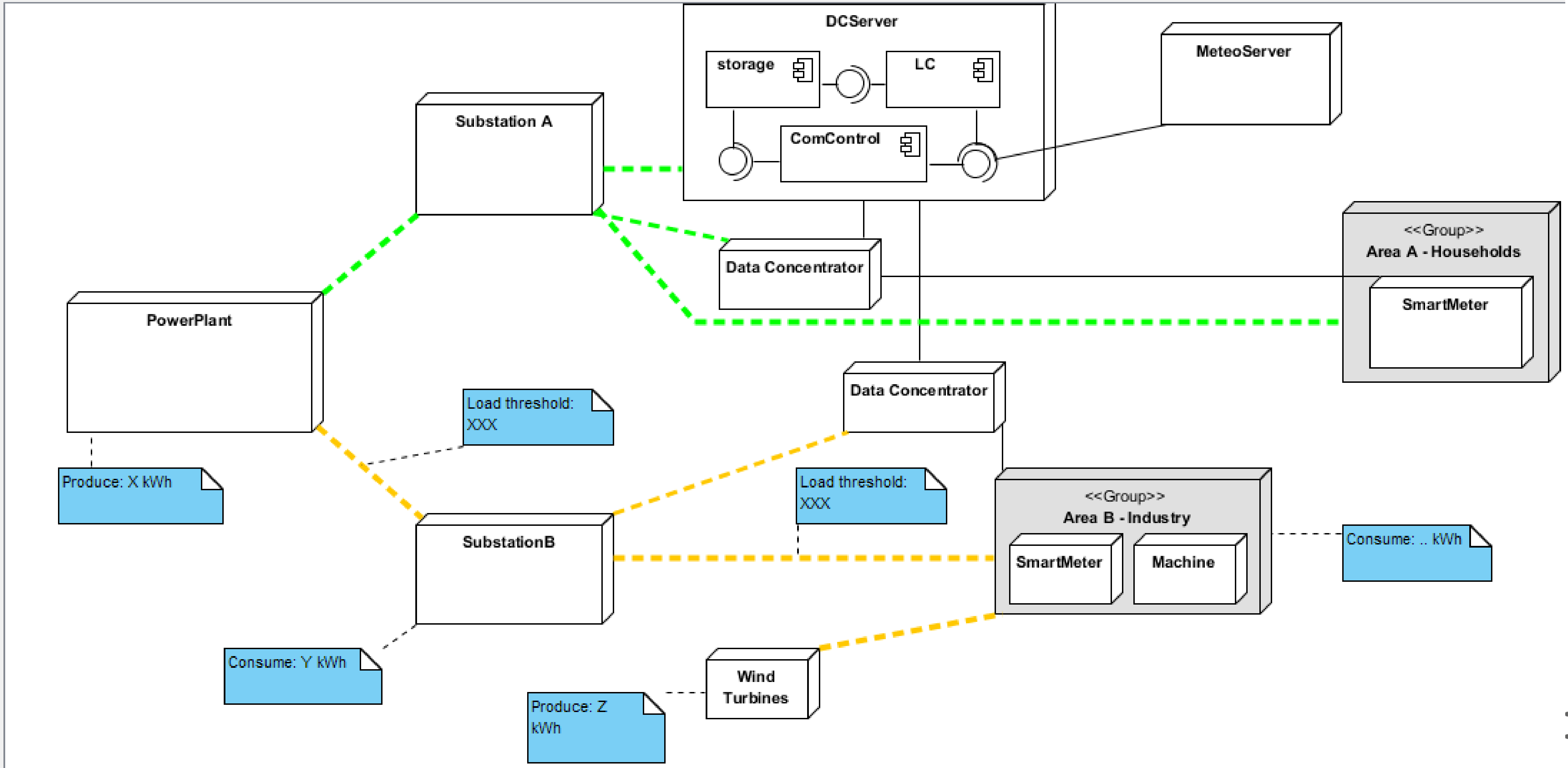
- Modelling of more complex services in the group nodes
  - Each of the device in the group node can have some internal behaviour or it can communicate with other devices
  - The submodels might be fully specified service/HW models
    - The output for the main model can be computed at the point of the return message.





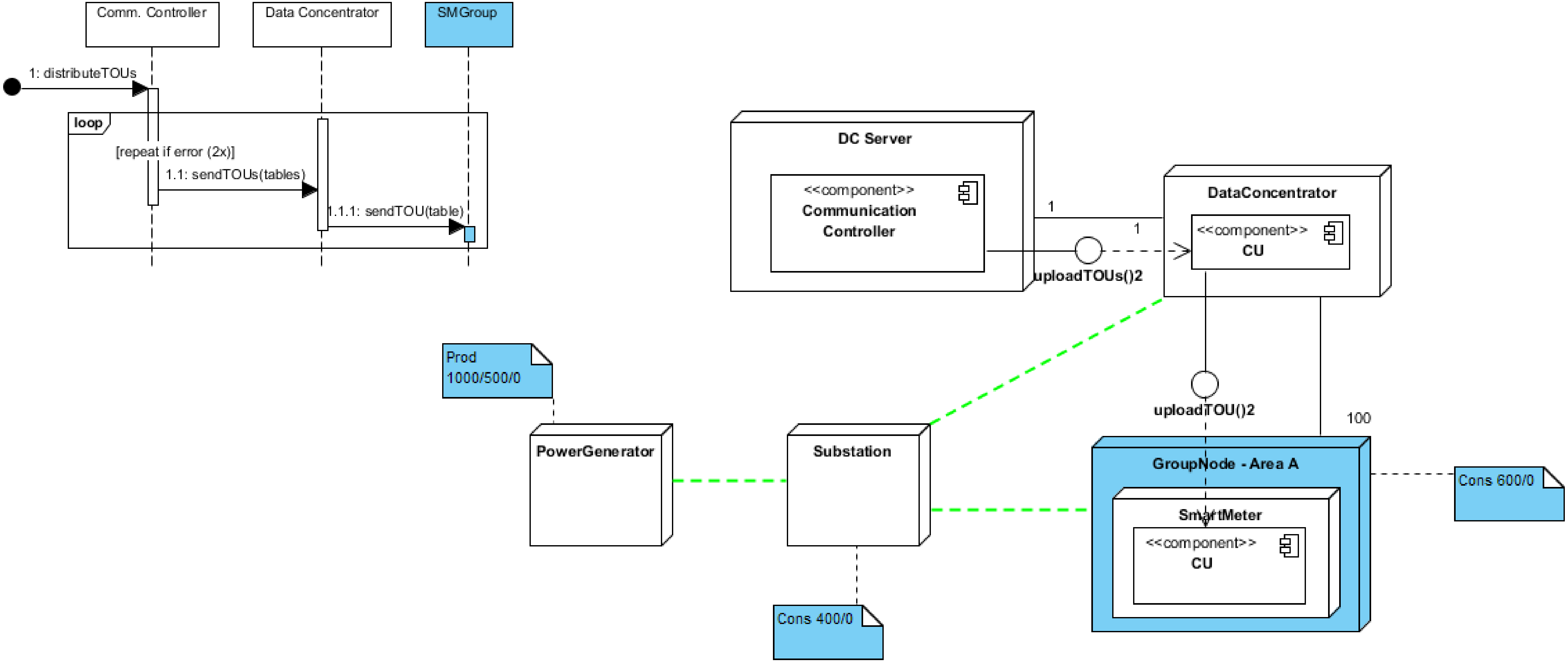
lasaris

Resource management – Energy requirements

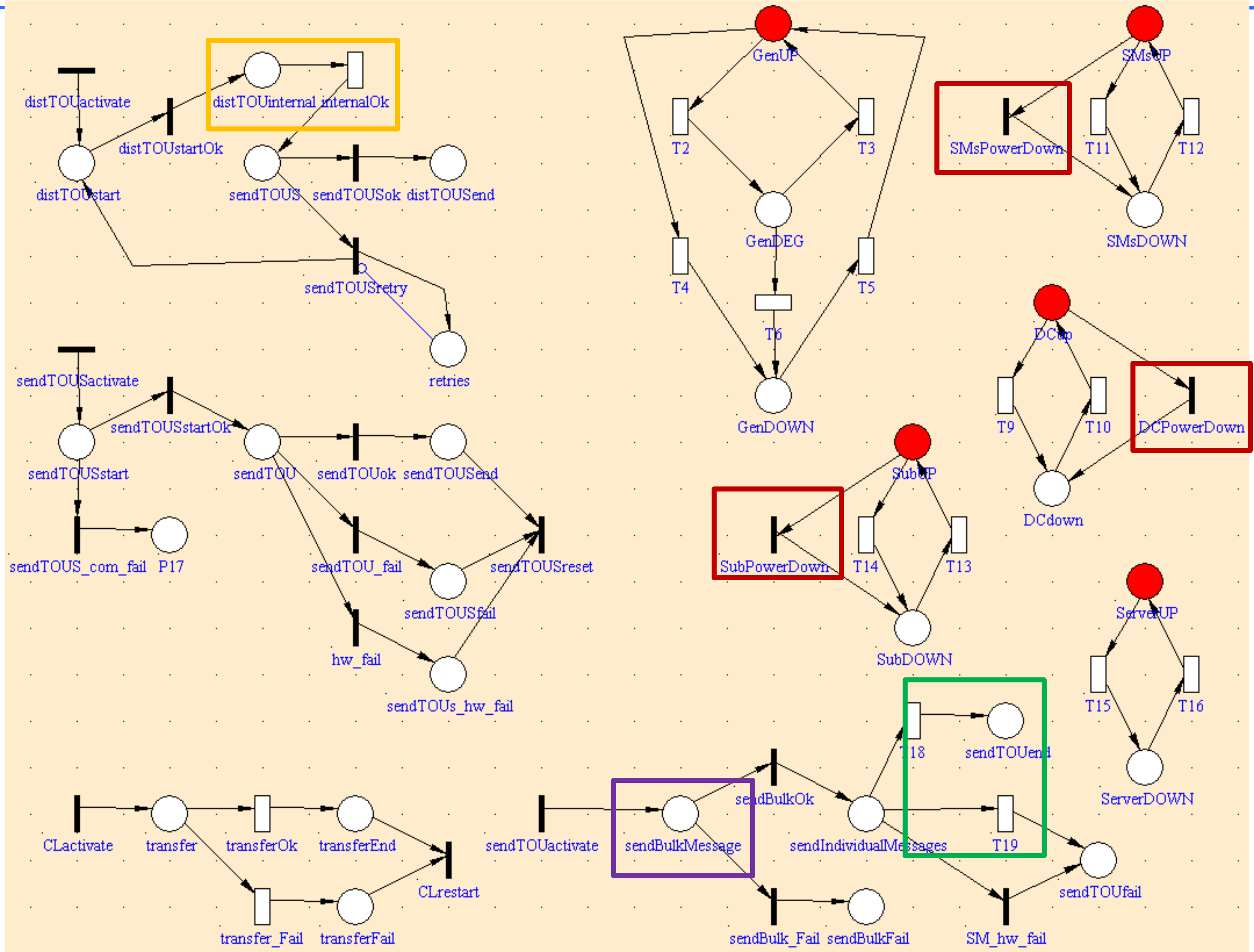


is

Scenario – Sending TOU tables



Scenario – Sending TOU tables



- PN
  - 30 places
  - 20 trans.
- RG
  - 174 markings
  - 752 trans.

Input Data

- Operational data
  - Operations/methods being executed
  - Duration of individual operations
  - Sources
    - Application logs
    - Event logs
- Failure data
  - Possible failure types
  - Frequency of failure occurrence
  - Sources
    - Application & event logs
    - Crash logs
    - Documentation
- Communication data
  - Message sizes, link reliability, communication duration
  - Sources
    - Communication logs
    - Network monitoring

lasaris

Related Projects

- C4E - Simulation and prediction analysis of critical infrastructures
  - Extension to other types of infrastructures
  - Adding support for other qualitative attributes – availability, performance
  - Case studies
- Hardware-Software Fault Analysis for Cyber-Physical Systems of Systems
  - General Failure, Error and Fault (FEF) classification, taxonomy and ontology
  - Catalogue of FEF
  - Preparing proposal for H2020

lasaris

Next Steps

- Validation
  - Validation of the **abstraction**
  - Validation of input **parameter assumptions**
  - Evaluation of the **largeness** and **stiffness** problems
  - Comparison of **analytical** and **simulation** results (in the SPNP tool)
  - **Cross-validation** through implementation in different simulator, e.g. GridMind
- Tool for model generation from annotated UML diagrams
- Future research
  - Extension of the model with additional measures – availability, performance, survivability, …
  - Application of the model to different domains – smart cities, software systems, automotive…
  - Optimization of the state-space, improvement of the abstraction