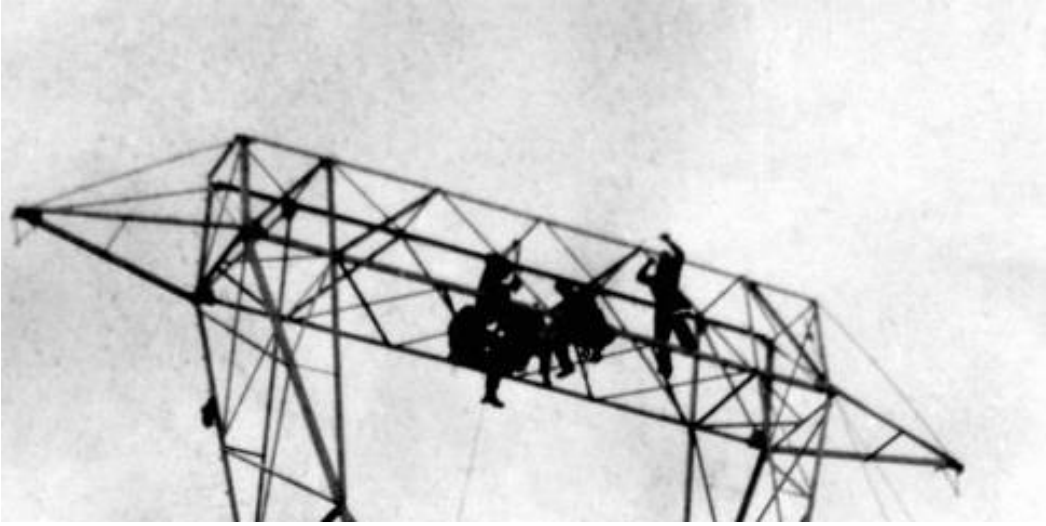


LANDSNET

Comparing Reliability Assessment in Transmission System Operation with the STAMP Model

ESW Conference 2017

Samuel Perkin & Íris Baldursdóttir

samuelp@landsnet.is & iris@landsnet.is

Talk structure

1. Power system reliability
2. The EU FP7 GARPUR project
3. STAMP model of Landsnet
4. Comparing/Combining STAMP and GARPUR
5. Conclusion

Power system reliability

Power systems are:

- Critical infrastructure
- Expected to be approx. 100% reliable
- Complex networks of many machines/components
- Mostly outside and unsupervised
- Becoming harder to control (due to wind, solar, electric vehicles, more automation)

The N-1 philosophy

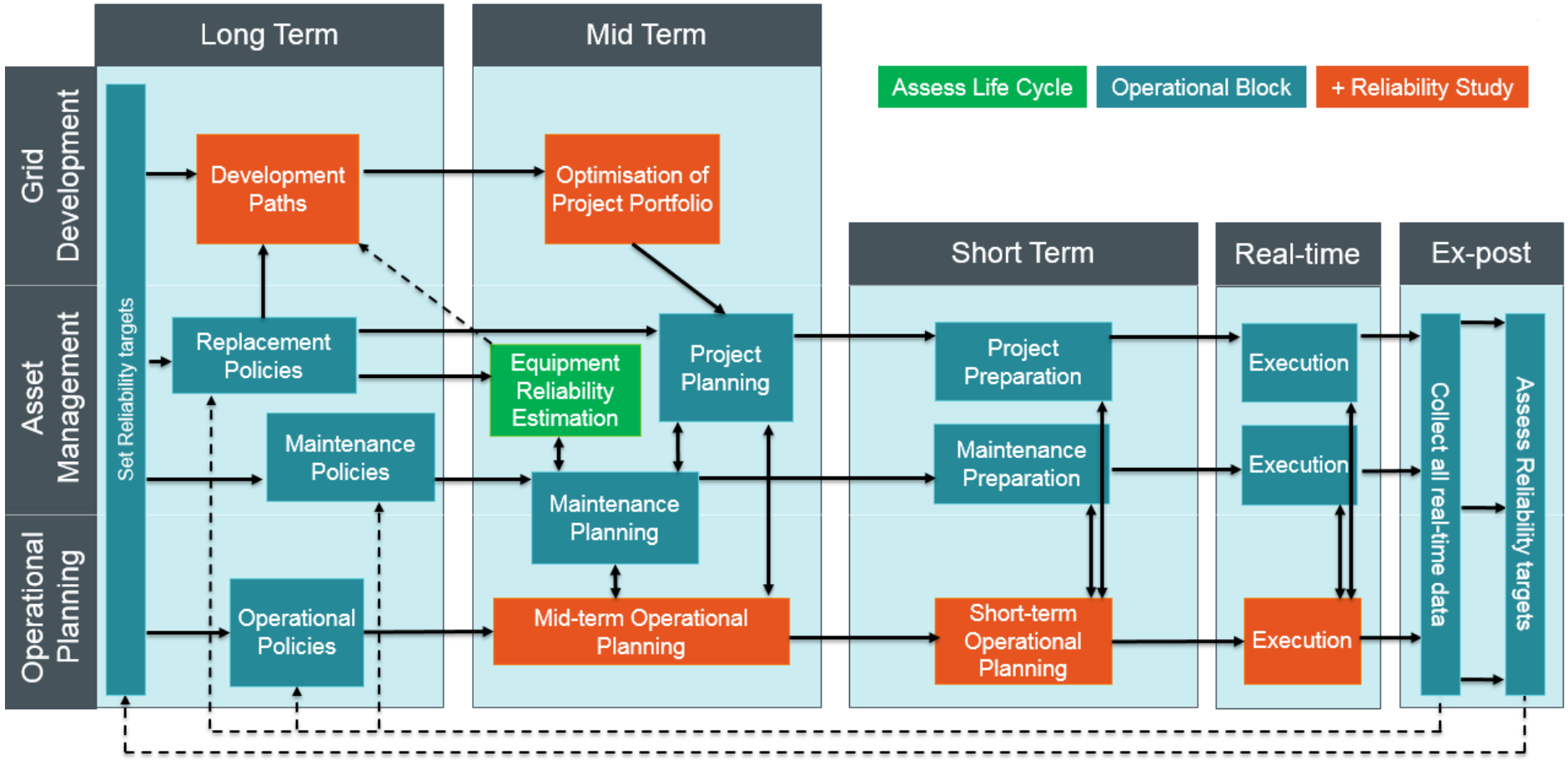
LANDSNET

After the loss of any **single** major grid element, the system must continue to operate without violating Operational Security Limits

VS

See: GARPUR Consortium (2014) *D1.2 Current practices, drivers and barriers for new reliability standards*

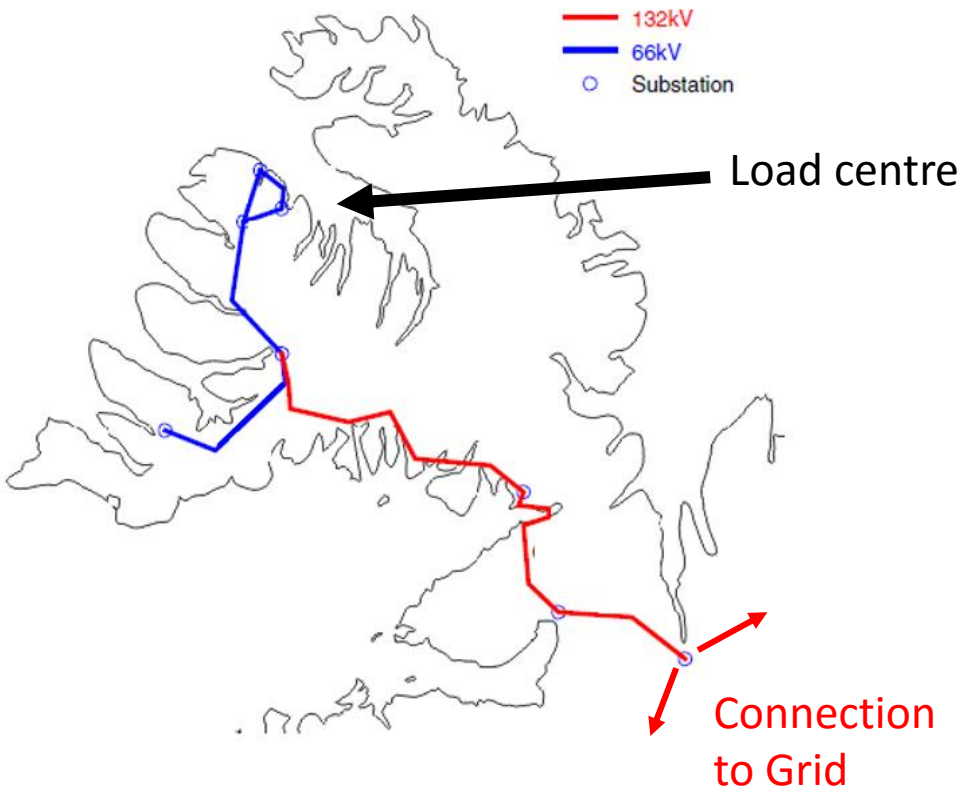
TSOs are complex organisations



TSOs: Transmission System Operators (e.g. Landsnet)

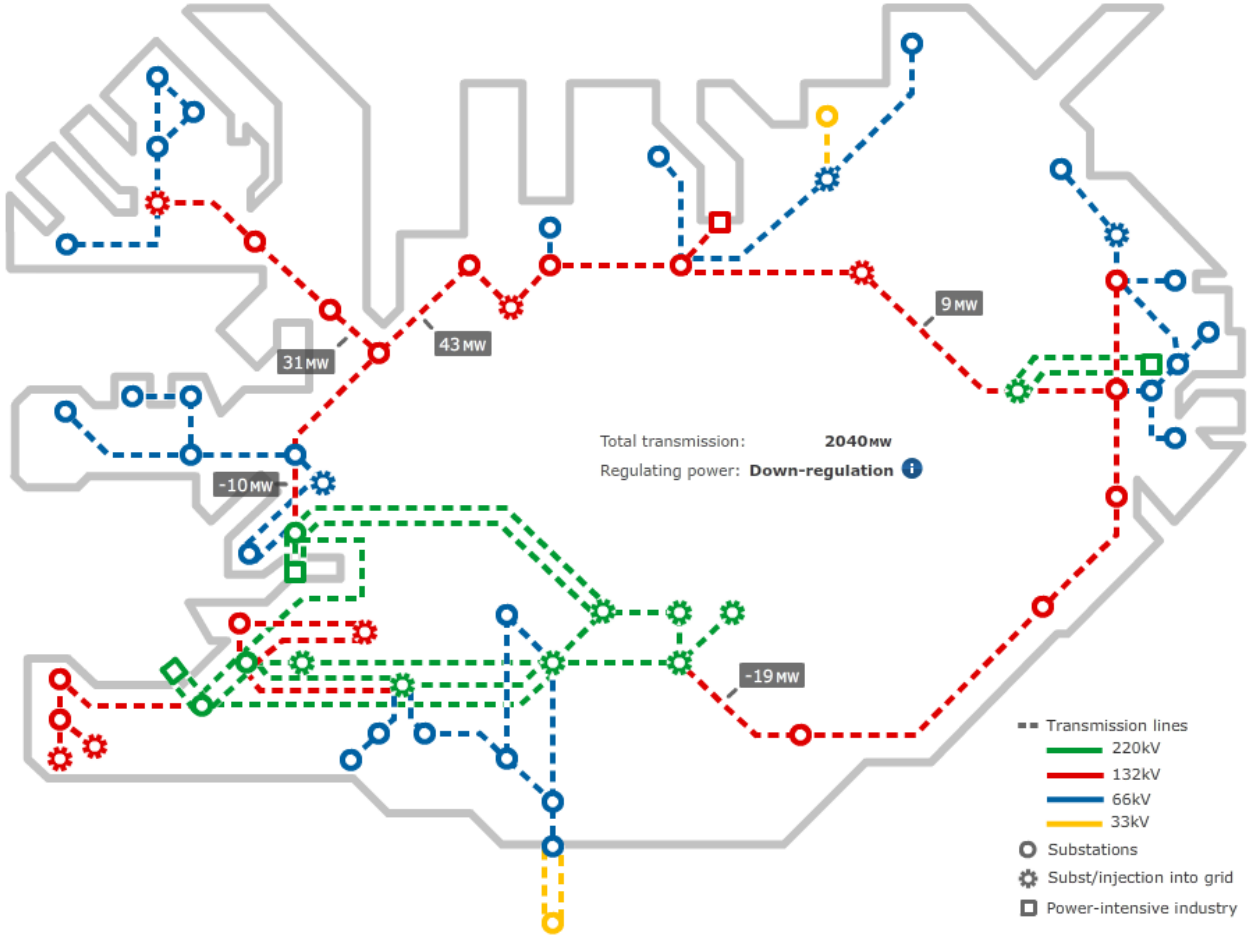
When N-1 isn't enough

- Many radial regions are not N-1 secure
- New lines would fail at the same time as existing lines (large investment for no gain in reliability)
- Installed microgrid system to improve reliability (by reducing outage duration)
- Still not N-1 secure, but more reliable
- **Need new ways to quantify/justify such investments**



Landsnet and GARPUR

- Landsnet operates the Icelandic transmission system
- Part of the GARPUR project on: developing probabilistic reliability management approaches.
- EU FP7 project (funding: 10.9 M€)
- Justification: Growing risk, aging grids
- Why Landsnet?

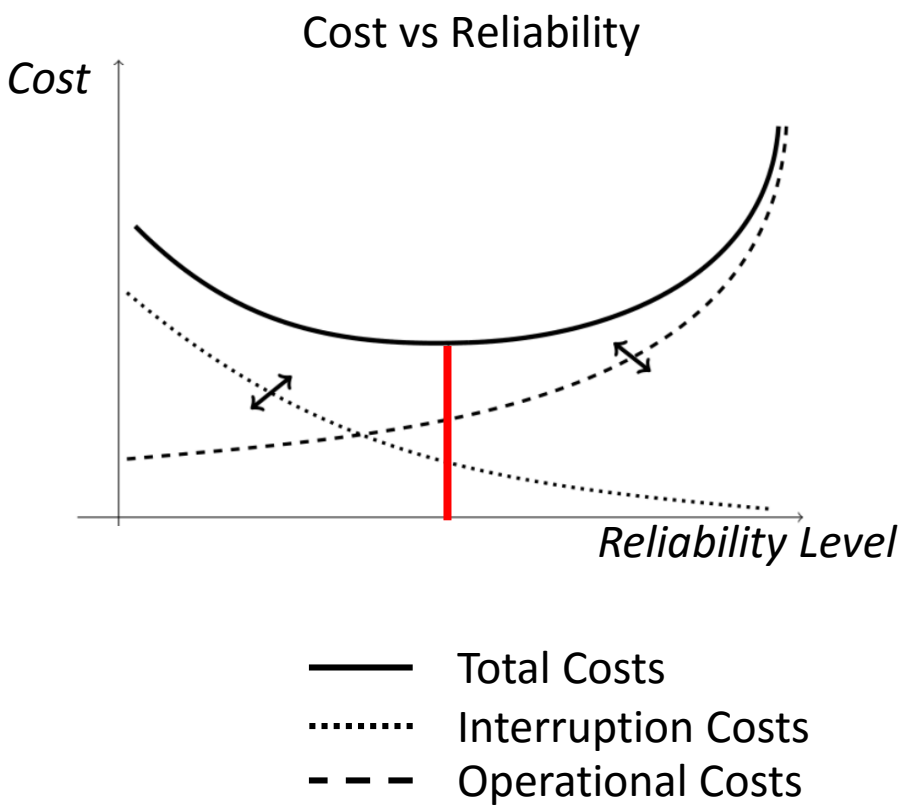


The GARPUR Methodology…

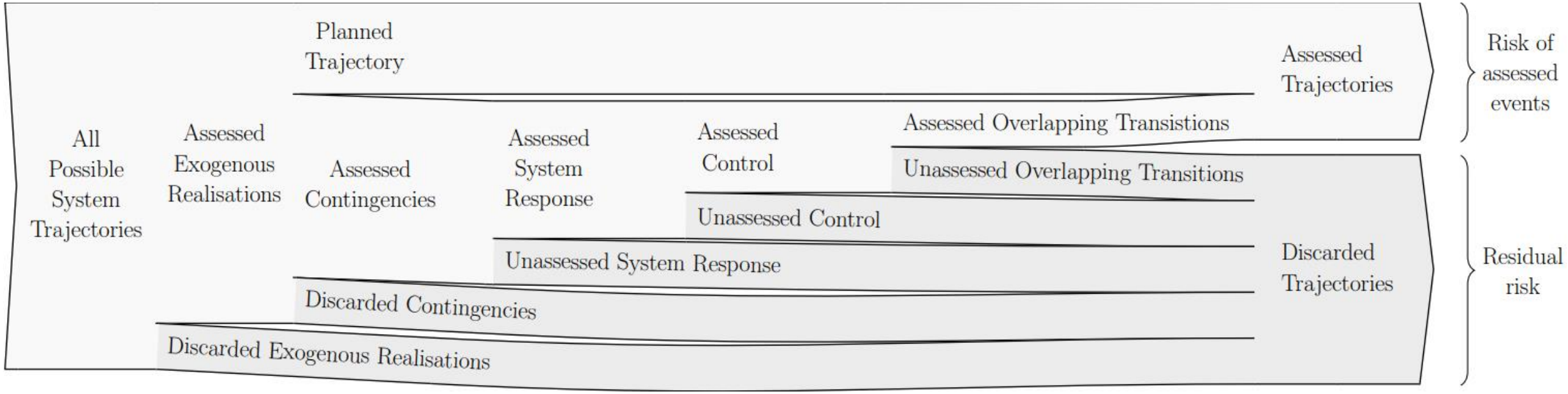
Select and assess a **dynamic** set of contingencies based on their **risk** (*discarding principle*)

Perform **socio-economic impact assessment** for each contingency

Find **decisions** that **maximise social welfare** whilst gauranteeing a high probability of meeting **acceptability constraints**



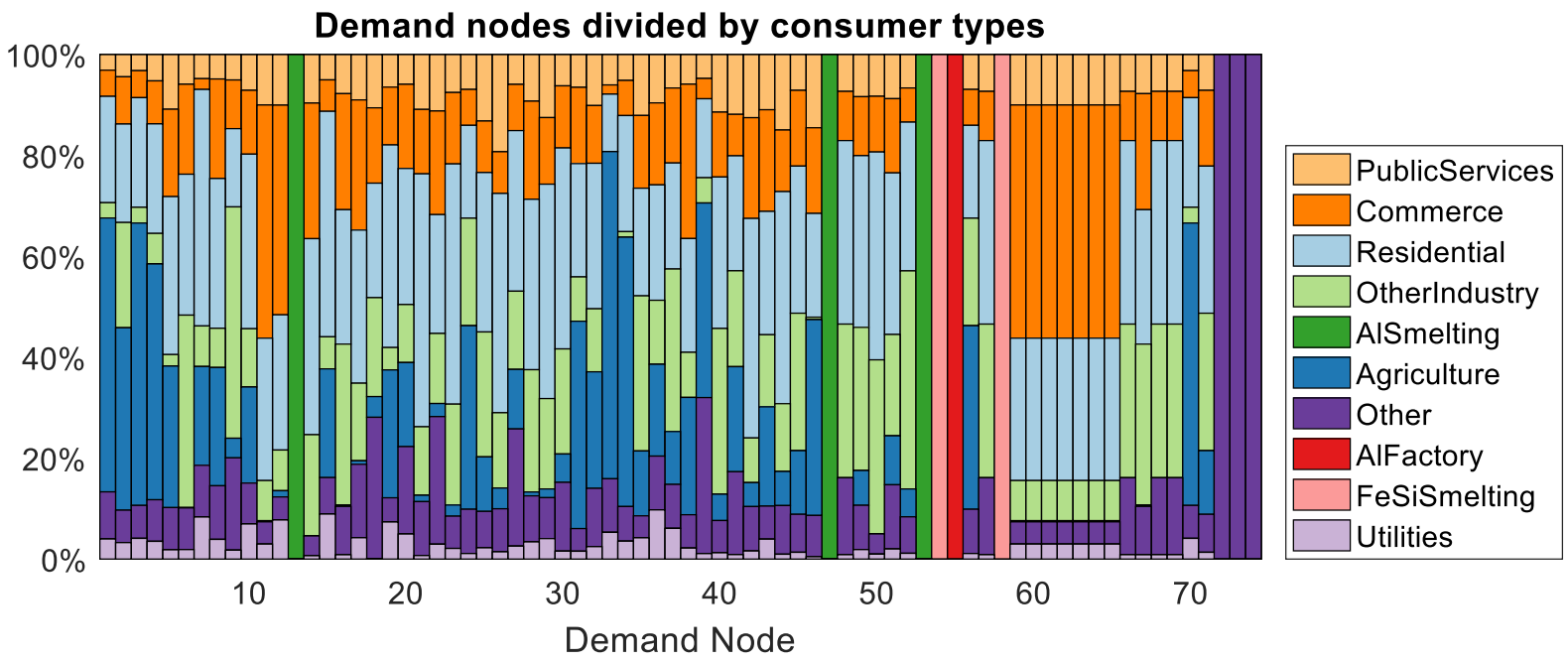
Discarding Principle



Probabilistic accounting of systemic and human control errors
Requires understanding of ‚all that may go wrong‘ to estimate residual risk
– how do we identify out-of-model system trajectories?

Socio-economic impact assessment

- Variety of end-users
- All affected differently
- Need to convert ***energy not served*** into ***interruption costs***
- Also need to consider ***environmental costs*** and the ***costs of control actions*** *among others*



See: GARPUR Consortium (2015) D3.2

Acceptability constraints

Technical constraint example:

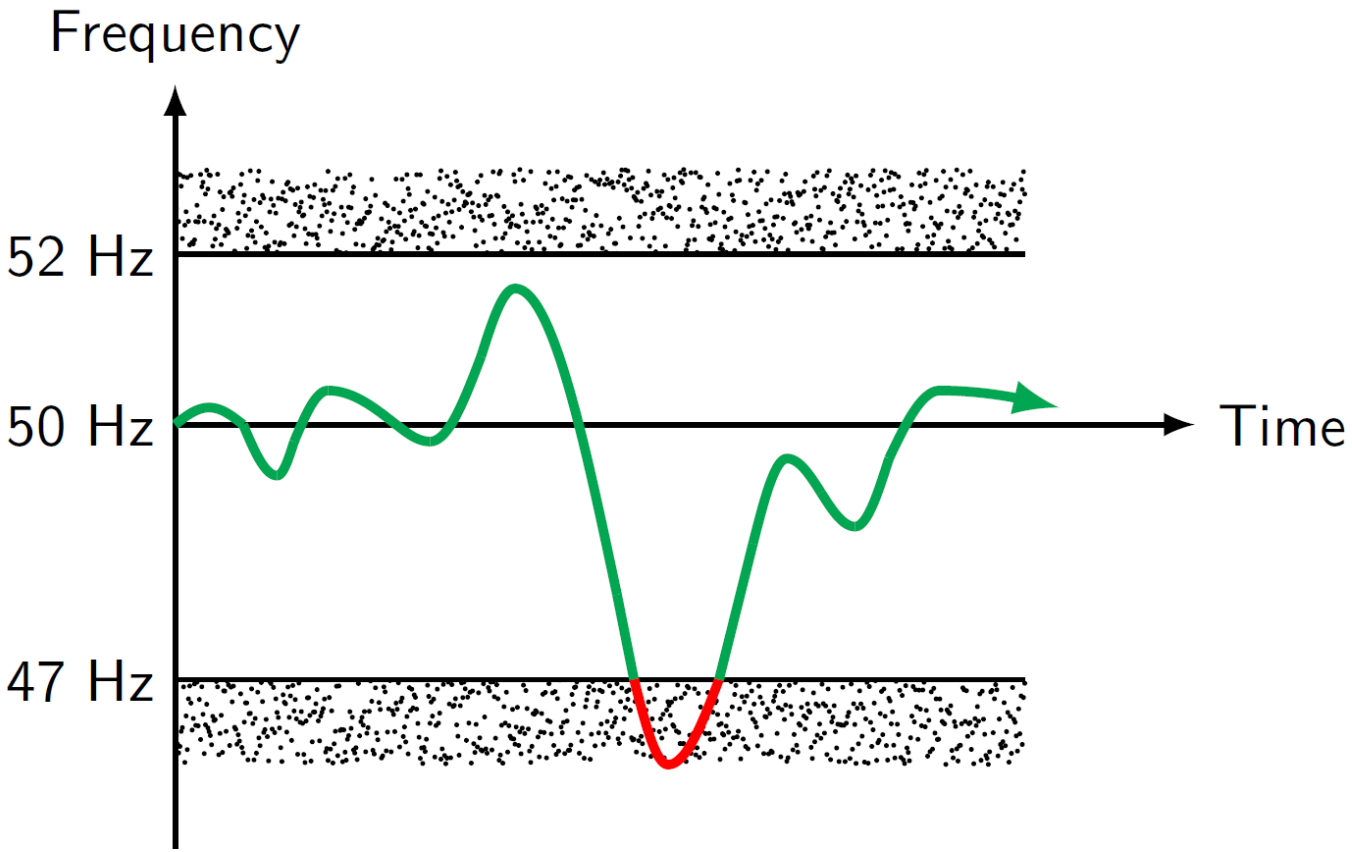
- voltage level constraints
- component loading limits
- Frequency limits

Social constraint examples:

- reliability should be spread equitably
- human safety shouldn‘t be put at risk
- Fair market access for renwables

Others:

- *Constraints resulting from STPA?*

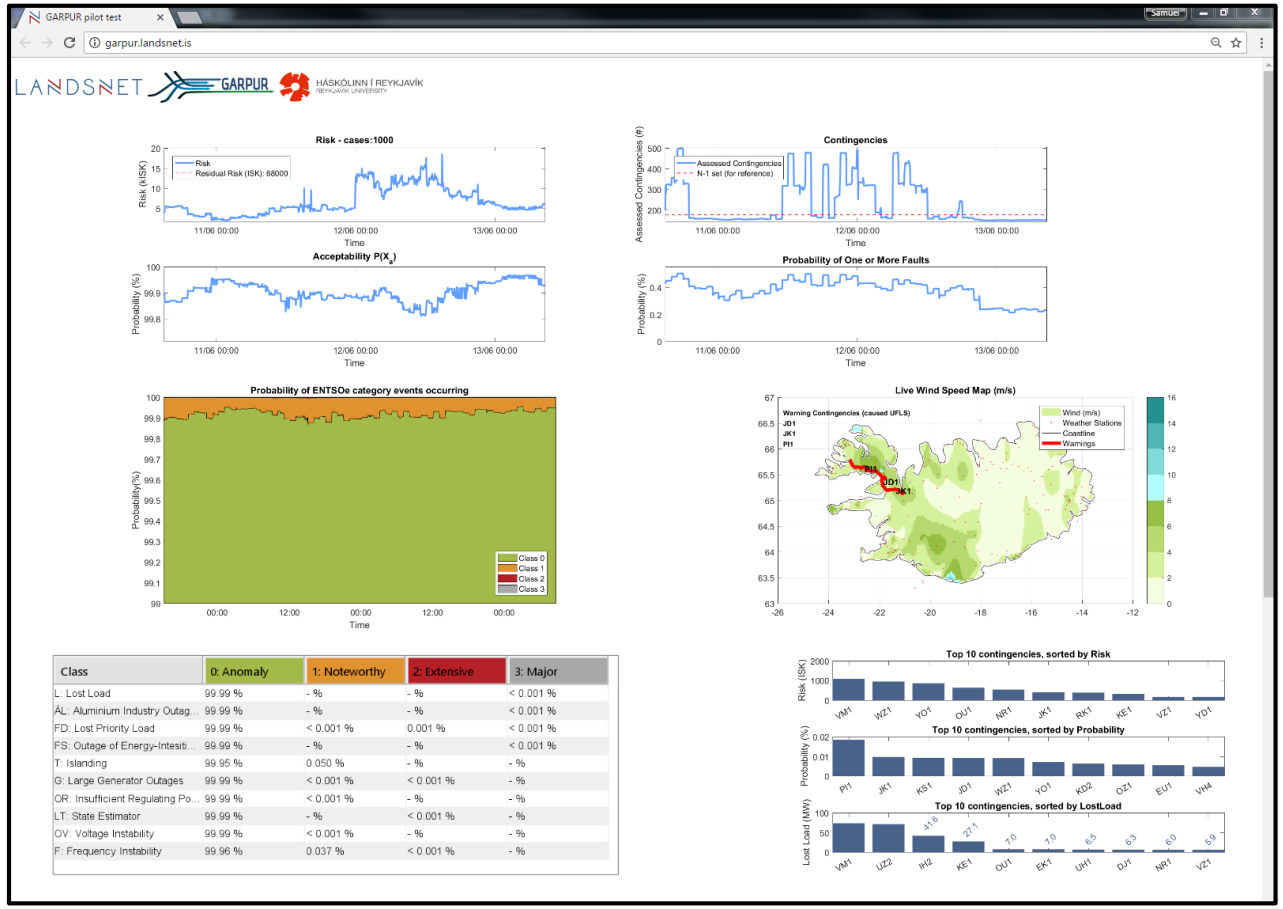


GARPUR at Landsnet

Real-time (minutely) measures on:

- System risk
- Reliability
- Various technical constraints
- Probability of faults
- System response predictions

GUI of the Landsnet pilot test of GARPUR



Class	0: Anomaly	1: Noteworthy	2: Extensive	3: Major
L: Lost Load	99.99 %	- %	- %	< 0.001 %
AL: Aluminium Industry Outag...	99.99 %	- %	- %	< 0.001 %
FD: Lost Priority Load	99.99 %	< 0.001 %	0.001 %	< 0.001 %
FS: Outage of Energy-Intesiti...	99.99 %	- %	- %	< 0.001 %
T: Islanding	99.95 %	0.050 %	- %	- %
G: Large Generator Outages	99.99 %	< 0.001 %	< 0.001 %	- %
OR: Insufficient Regulating Po...	99.99 %	< 0.001 %	- %	- %
LT: State Estimator	99.99 %	- %	< 0.001 %	- %
OV: Voltage Instability	99.99 %	< 0.001 %	- %	- %
F: Frequency Instability	99.96 %	0.037 %	< 0.001 %	- %

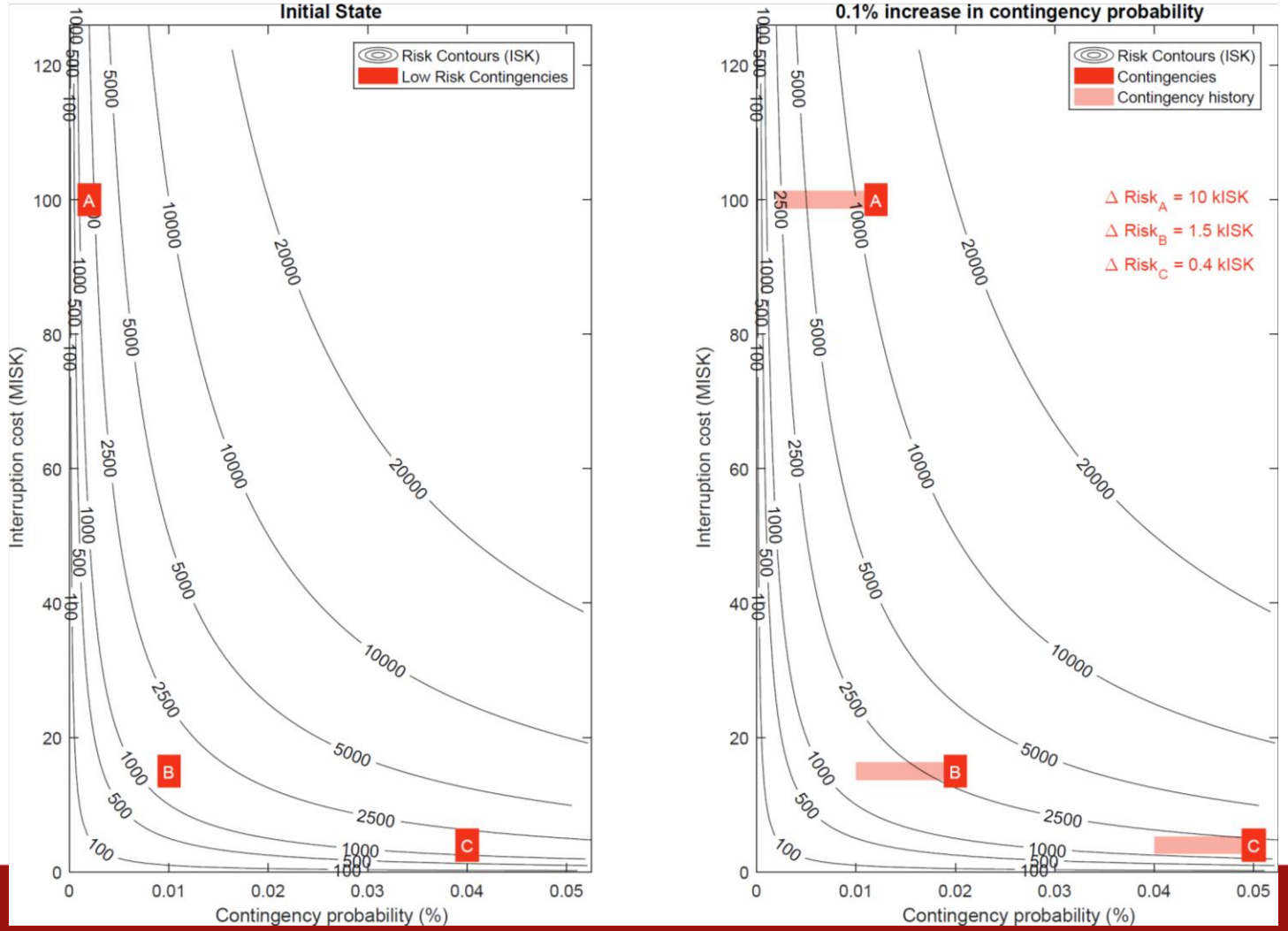
Probabilistic methods in practice

Risk map: differentiate between high-risk faults.

probability estimation errors greatly impact risk estimates of **HILP** events (A)

Probability estimates depend upon models of threats/hazards

Difficult to validate probability estimates - especially when conditional on many factors!



STAMP model of Landsnet

- Main features of the Landsnet model
- Applications/purpose
- Main accident/loss = service outages and their implications
- Insights (multiple hazards in one context may have an underlying cause in another)
- Aim to diagnose hazards as processes, rather than as events. Define operational constraints to prevent hazards.

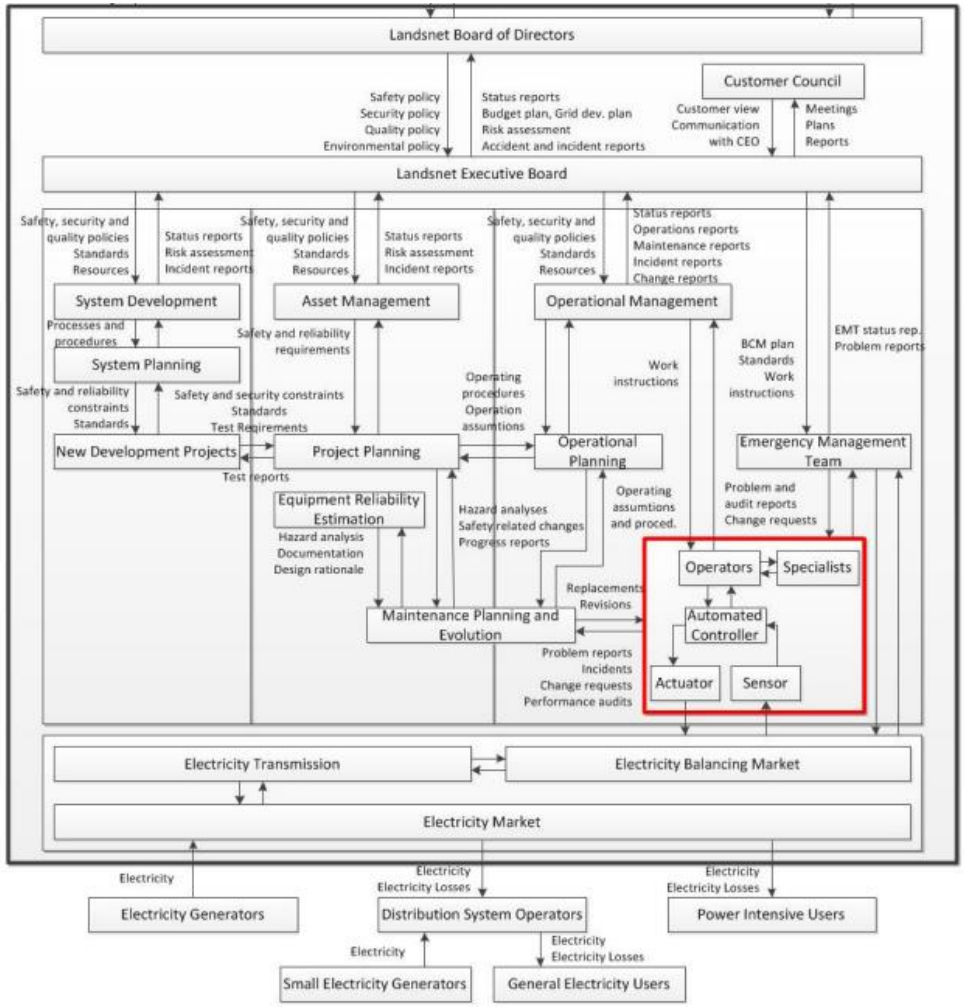


Figure Source:
Björnsdóttir, S.H. (2015) *Comparison of Risk Analysis Methodologies in an Electrical Grid,* European STAMP Workshop, Amsterdam

STAMP model of control room operator

LANDSNET

- Captures relationship between human, exogenous, cyber and physical systems.
- Aim of system operation is to achieve socio-economic optimal levels of reliability.
- **Prior decisions (investment, maintenance, planning) are equivalent to process inputs from RT perspective**
- Imperfection in physical and cyber systems are learned by operators (experience + intuition).
- Systems and models are highly complex, difficult to define/estimate reliability

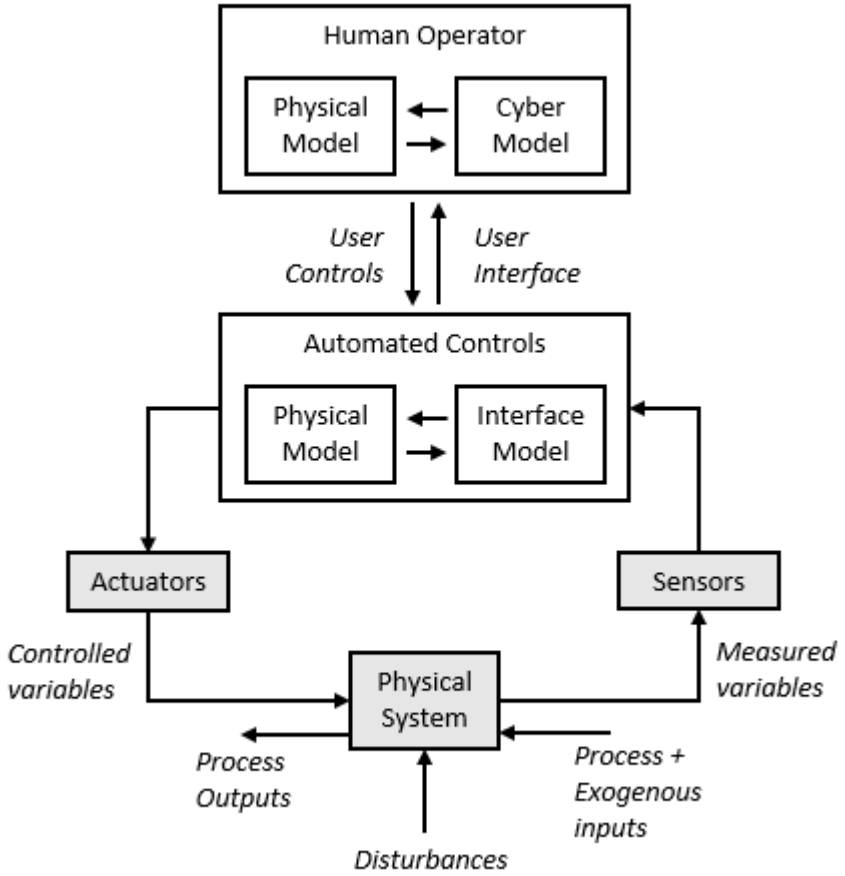
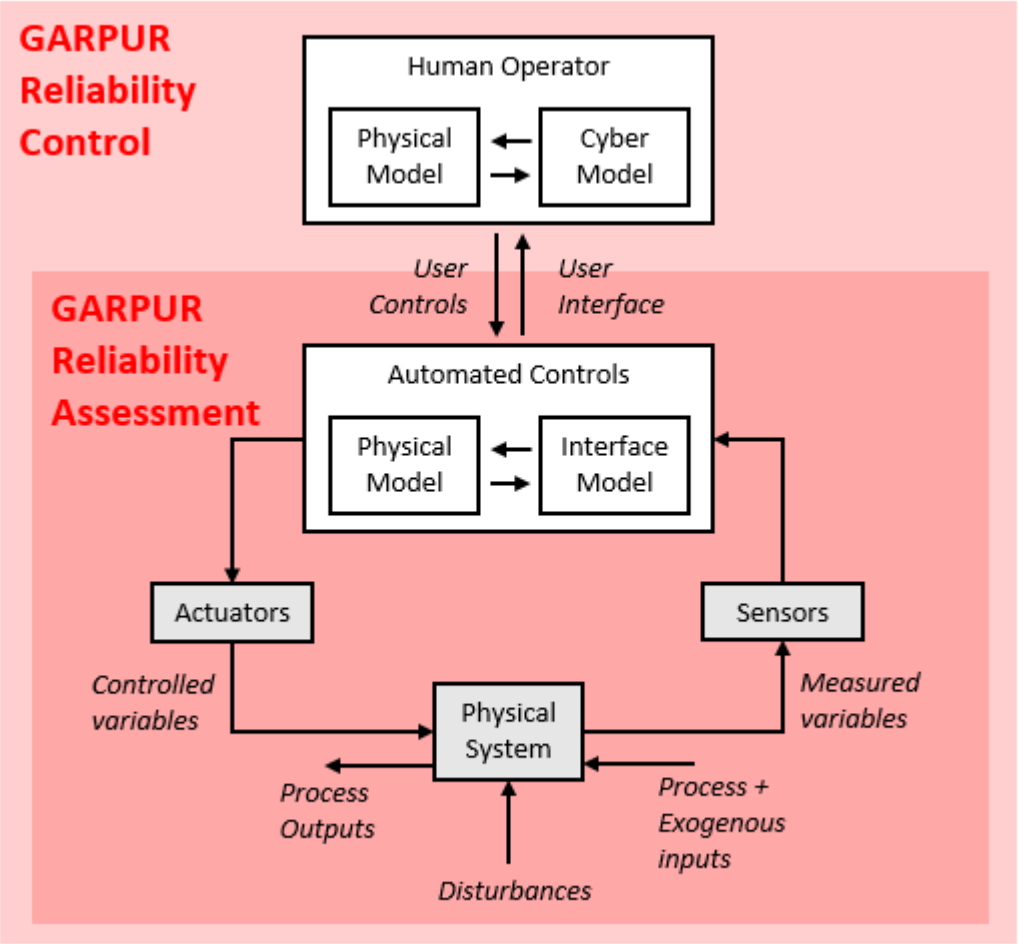


Figure adapted from: Leveson, N. (2004), *A new accident model for engineering safer systems*. Safety science, 42(4), 237-270.

Linking STAMP to GARPUR

- Reliability assessment:
  - Is the present system state acceptable?
- Reliability control:
  - Can we improve the present state?
- Need to capture control failure in probabilistic models
- GARPUR relies on the physical model, and its usefulness depends on the design of its interface (making meaningful risk visualisations)



See appendix for high-level STAMP diagrams of short-term operational planning and control processes

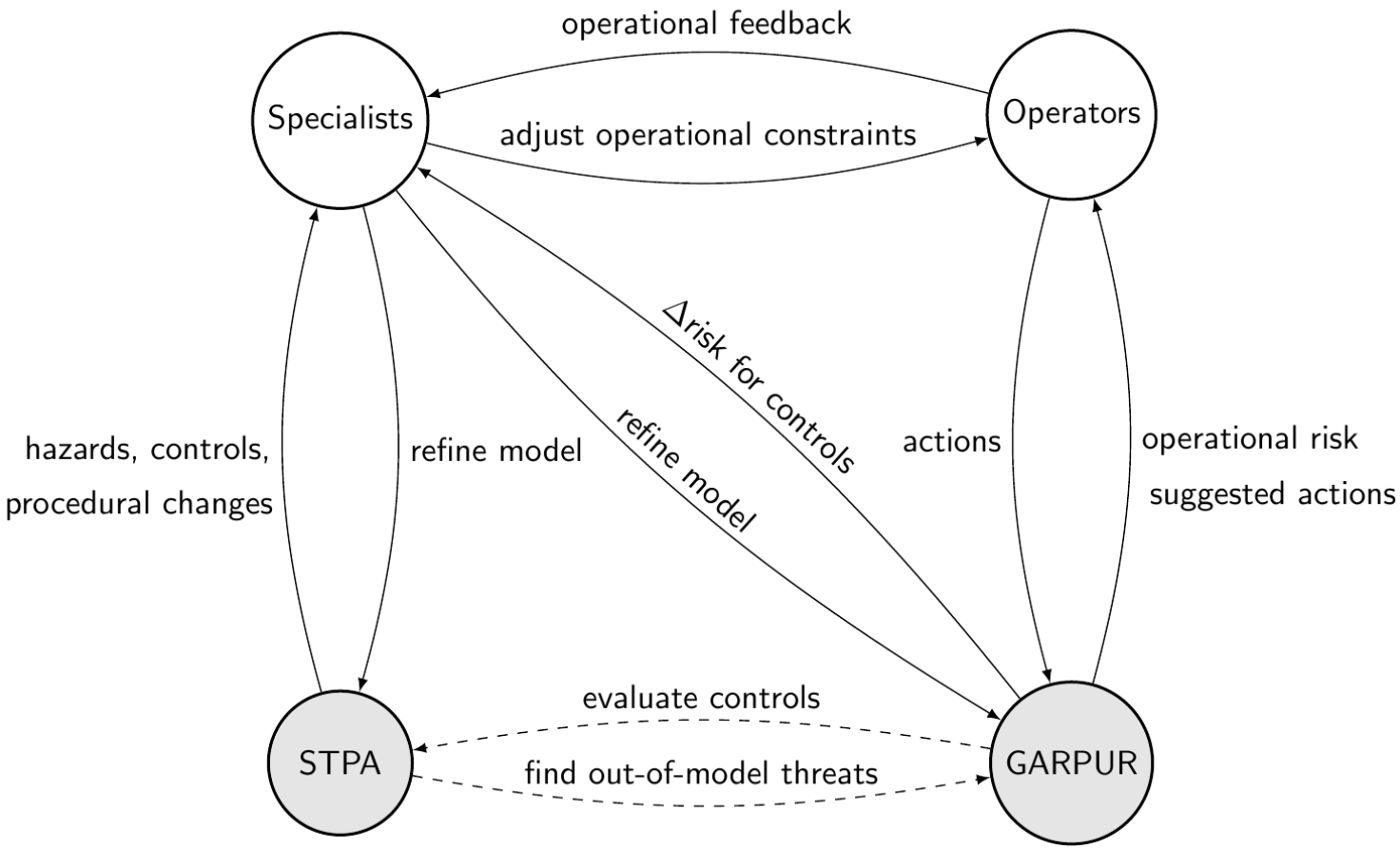
Comparing STAMP and GARPUR

LANDSNET

STAMP/STPA	GARPUR at Landsnet
Qualitative	Quantitative
Process-driven	Event-driven
Expert informed	Data informed
“How can we avoid hazardous states?”	“How can we improve reliability?”
Creates boundaries for operation (safety constraints)	Assesses performance within boundaries
Capable of assessing/controlling HILP events	Highly sensitive to HILP events
Used in anticipation of operation	Used by operators

Both approaches in harmony

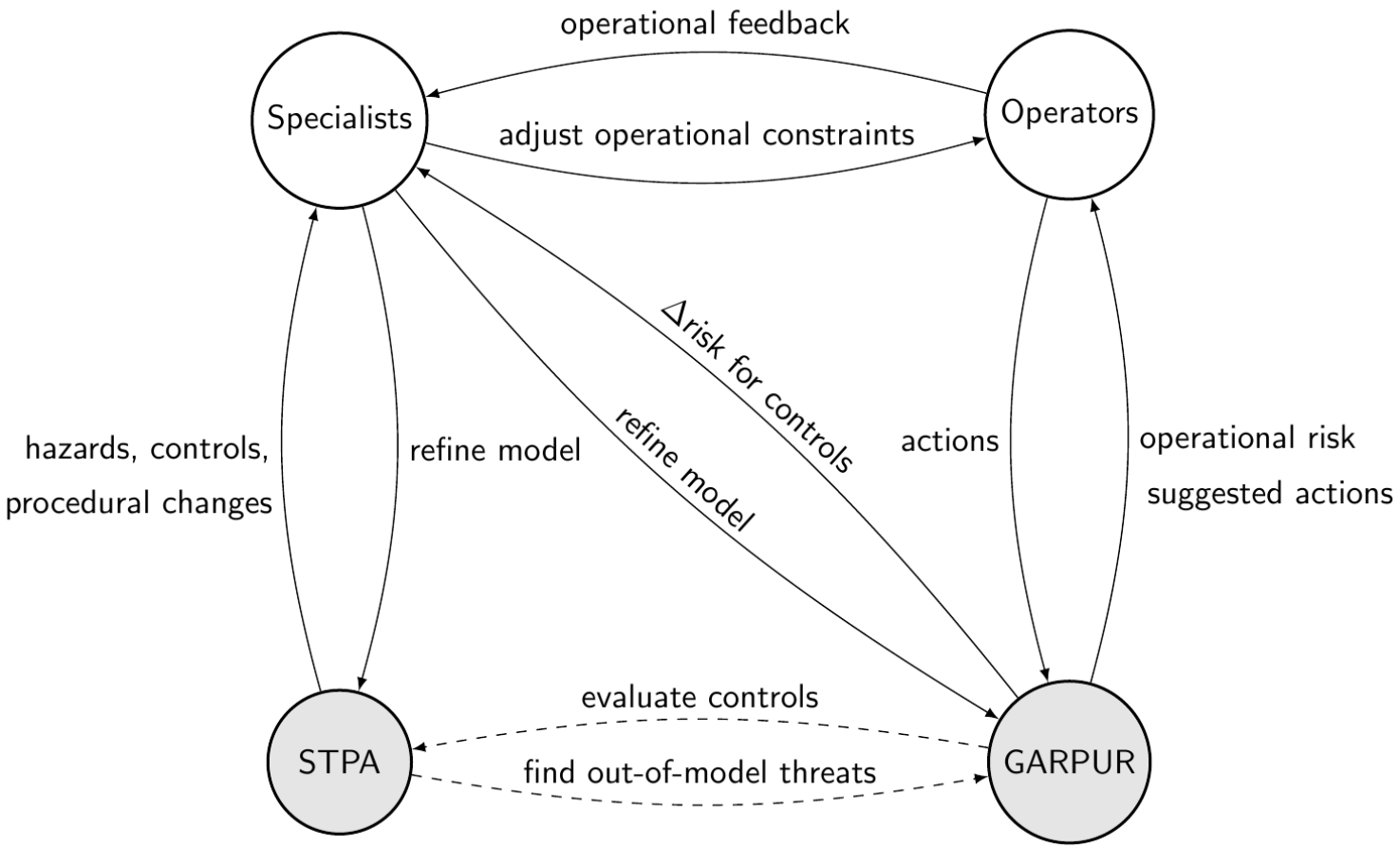
- Both methods provide different approaches to assessing and managing system risk
- STAMP/STPA can **identify new hazards** that may be missed by GARPUR
- GARPUR can **evaluate controls and constraints** proposed by STAMP/STPA
- GARPUR may provide a bridge between STAMP/STPA and real-time operators



Note: 'STPA' and 'GARPUR' in the diagram can be substituted for any top-down and bottom-up approaches, respectively

On acceptability constraints

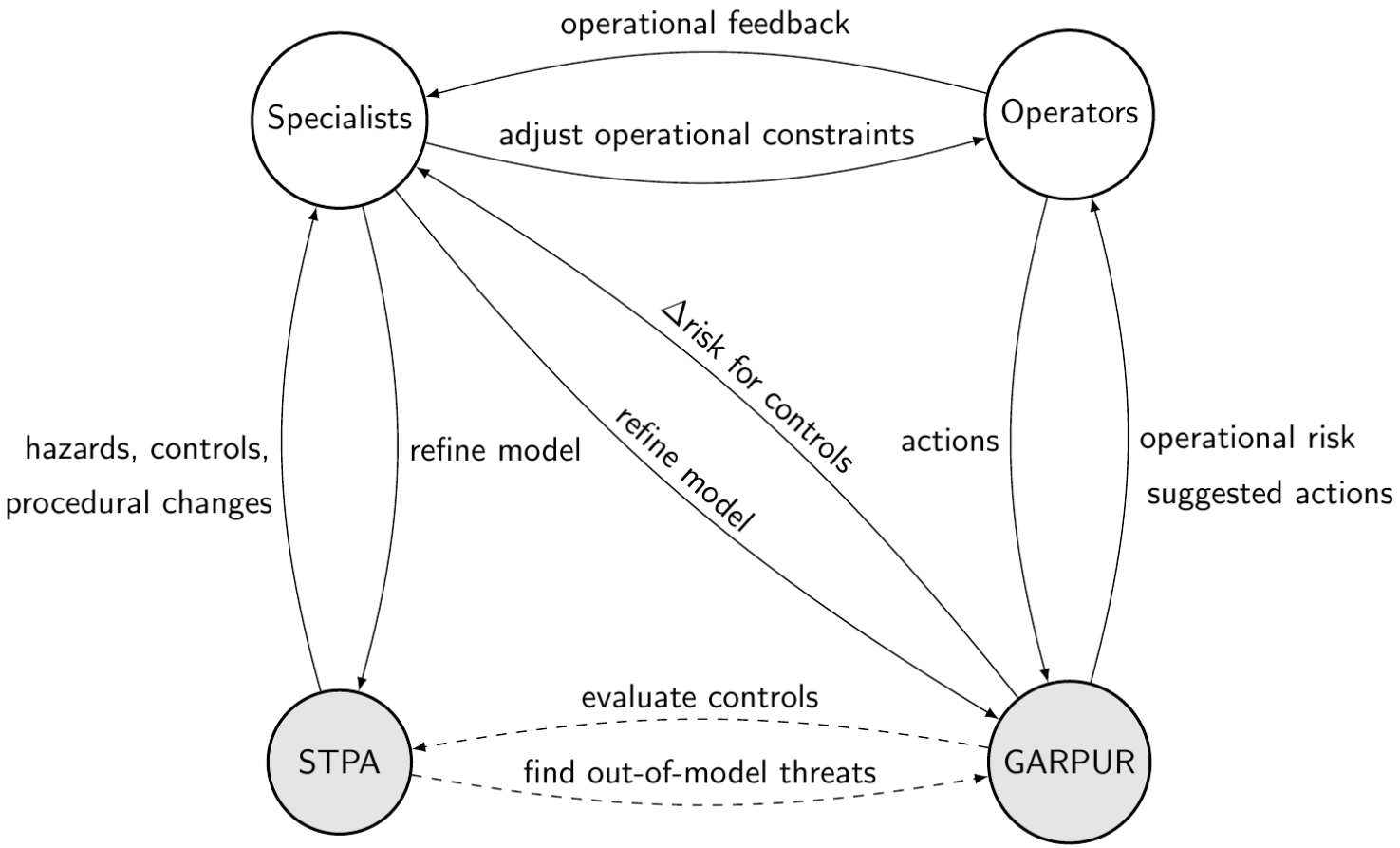
- STAMP/STPA provides controls (constraints) to manage hazards
- Some may be formulated as acceptability constraints (particularly for HILP events)
- Can measure impact of controls on overall system risk
- Can provide real-time feedback to Operators/Specialists on compliance



Note: 'STPA' and 'GARPUR' in the diagram can be substituted for any top-down and bottom-up approaches, respectively

On other TSO processes

- Prior decisions = process inputs
- GARPUR approaches may be able to assess impact of improving process inputs
- For example: reducing forecast errors through timing of tasks (changing organisational structure)
- May provide feedback to upstream processes about **Value of Information**, hence value of organisational change



Note: 'STPA' and 'GARPUR' in the diagram can be substituted for any top-down and bottom-up approaches, respectively

Conclusion

- Power system reliability is a complex topic
- New probabilistic approaches aim to quantify risk
- STAMP/STPA style approaches are important to ensure we don‘t get surprised

2nd GARPUR Webinar (2nd Oct):
Registration

Final Conference (17th & 18th Oct):
Info Programme Registration

Project info and deliverables at: http://www.garpur-project.eu/

+ STAMP

Today

LANDSNET

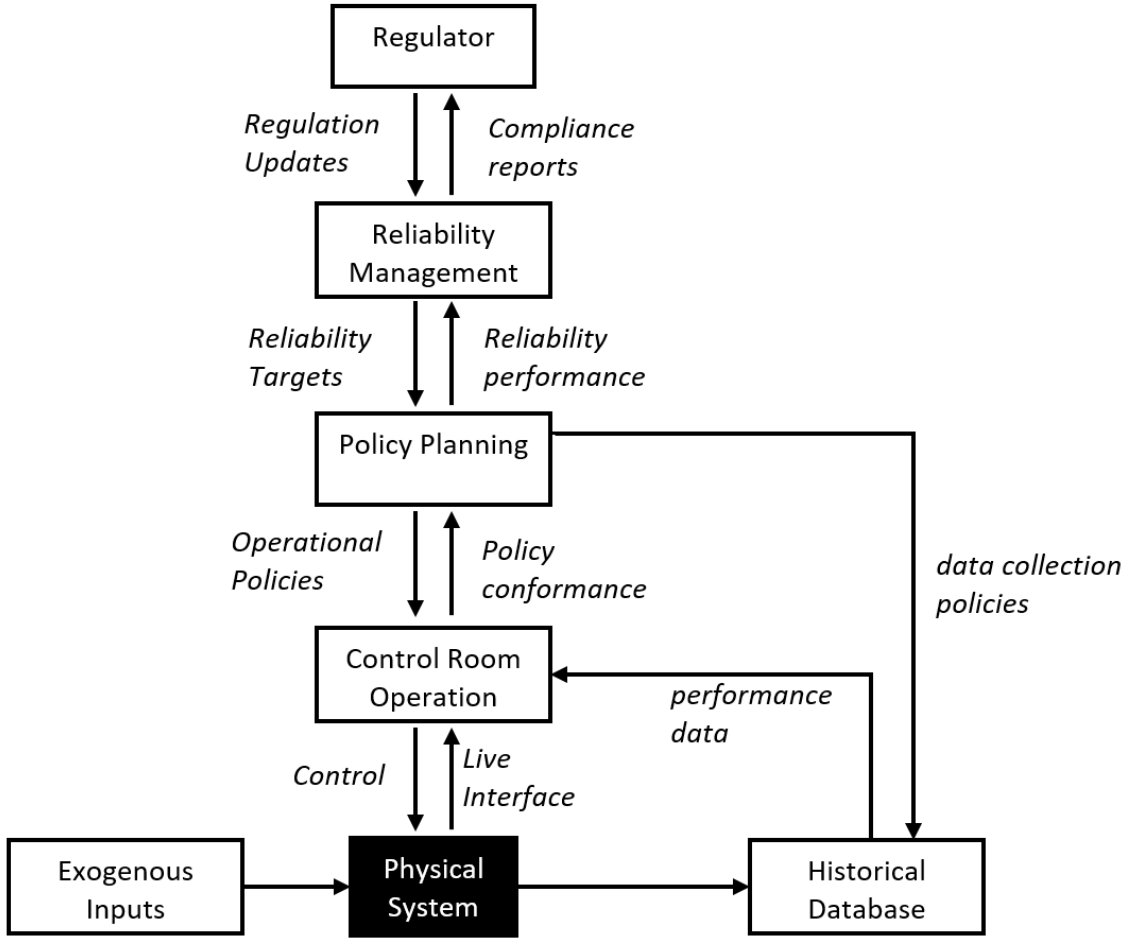
Appendix:

Basic STAMP diagrams of short-term TSO workflows

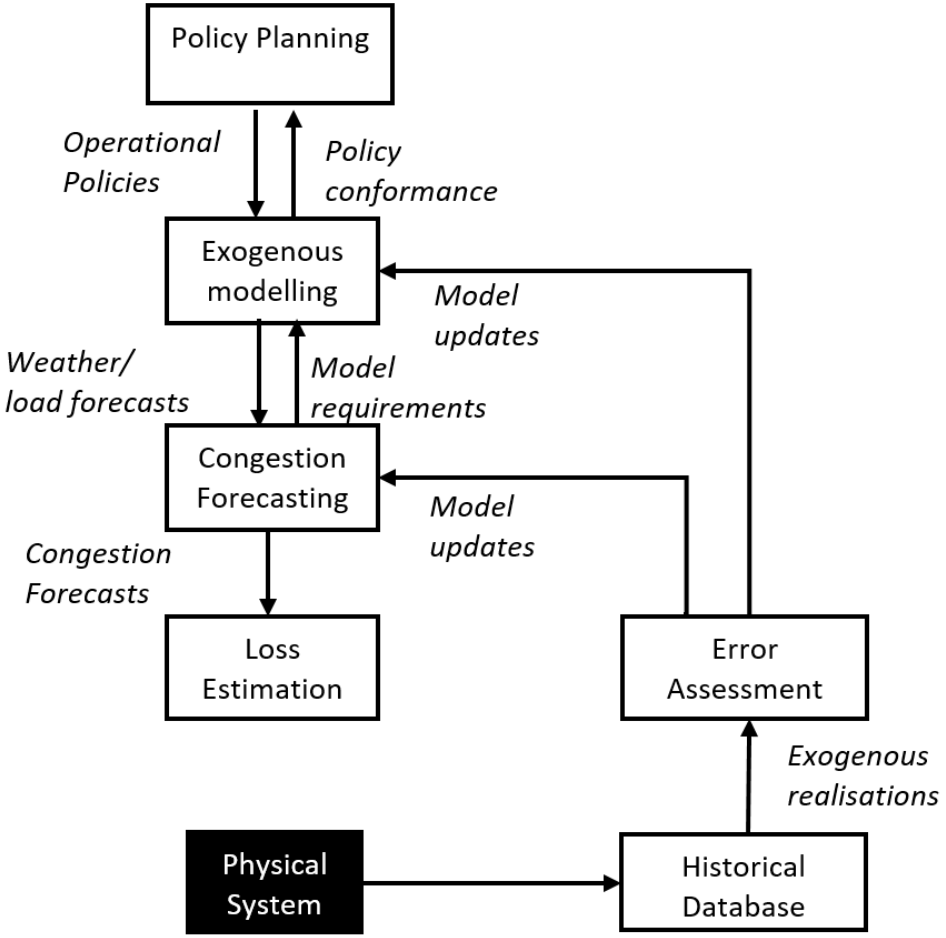
All figures in this appendix are adaptations of the workflow diagrams in:
GARPUR Consortium, *D6.1 Functional analysis of System Operation processes*, 7th framework programme, EU Commission grant agreement 608540, 2015. Available at: http://www.garpur-project.eu/deliverables

Please refer to the above report for some definitions of the terms used.

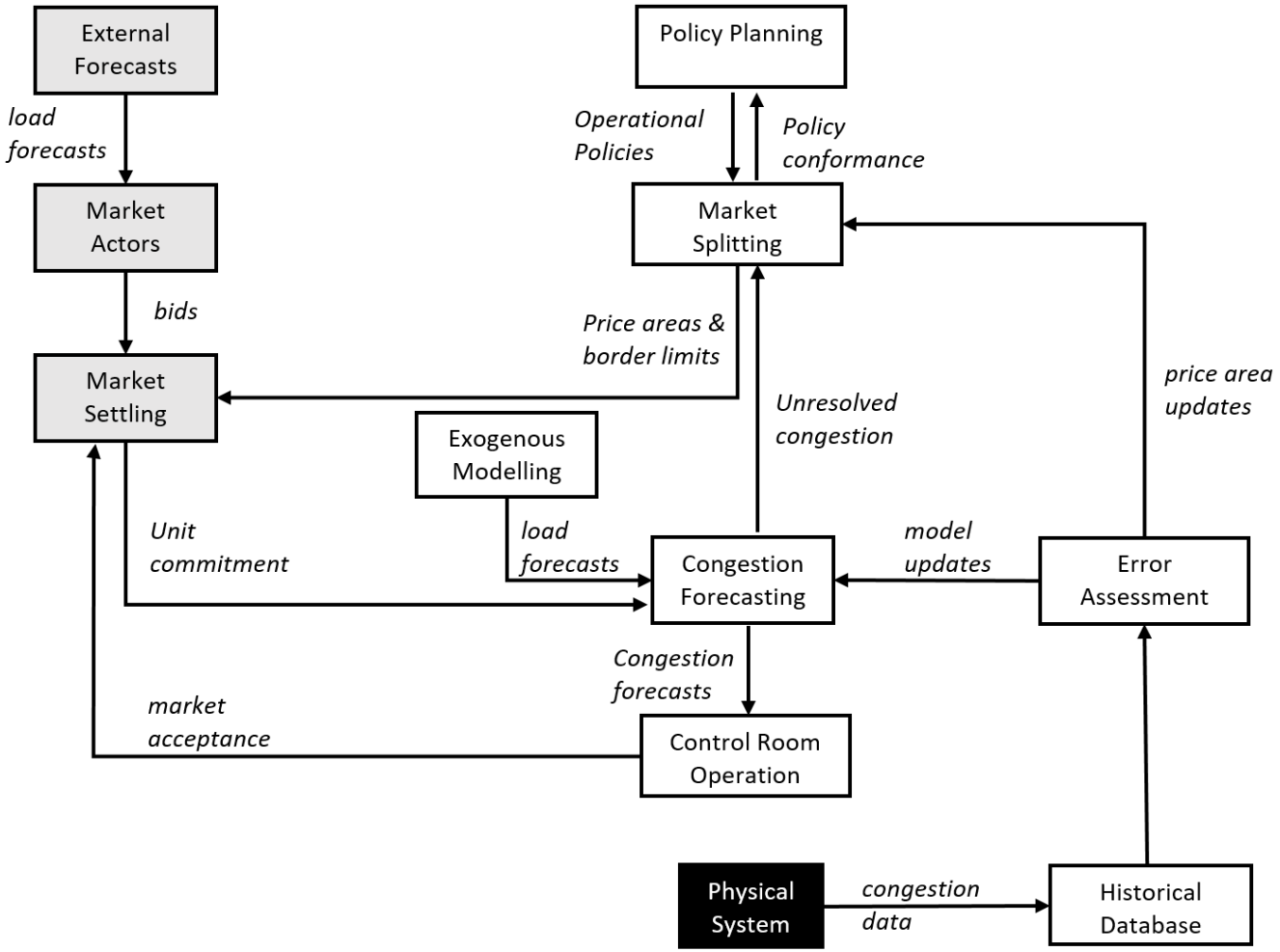
Operational Policies



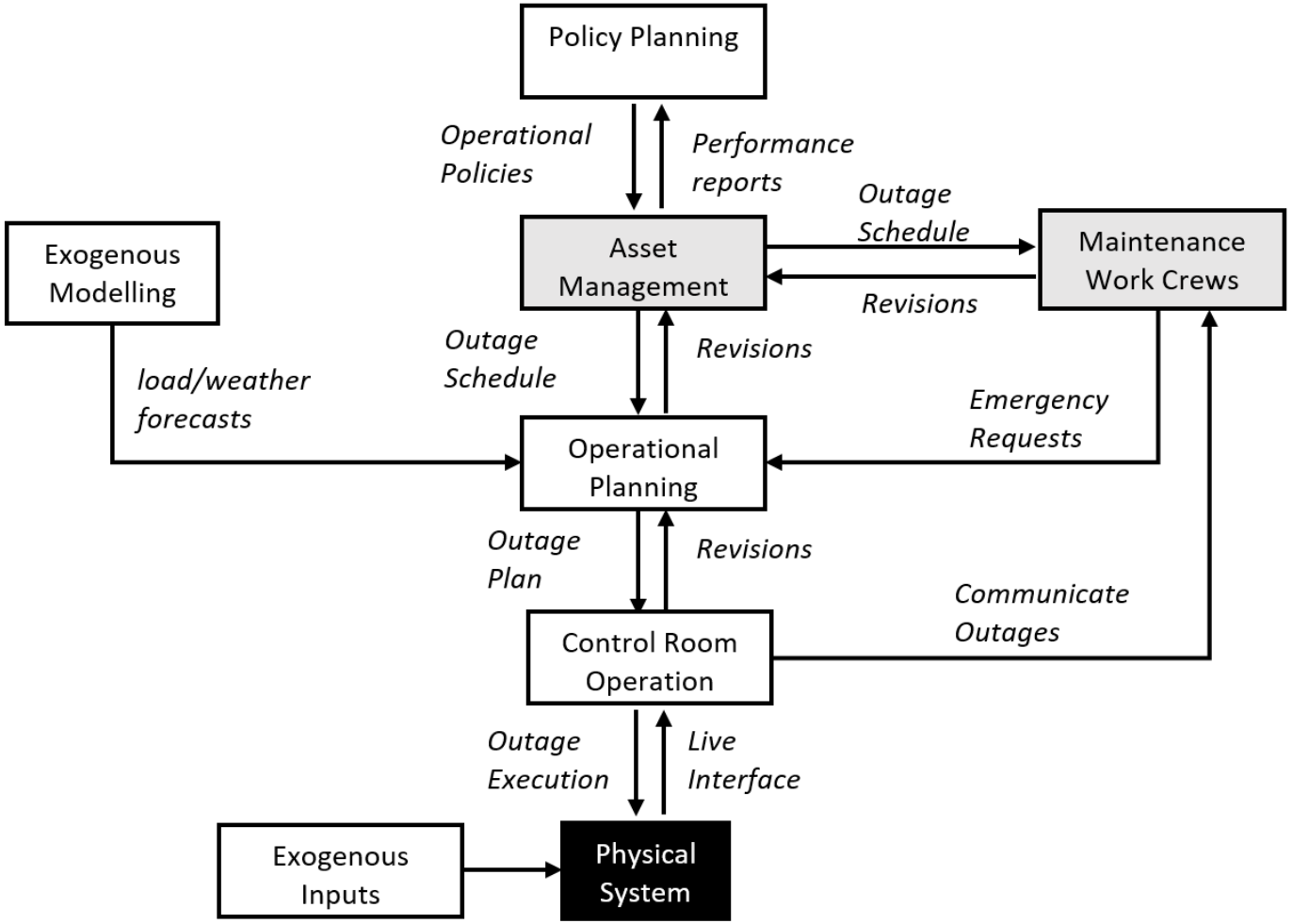
Forecasting



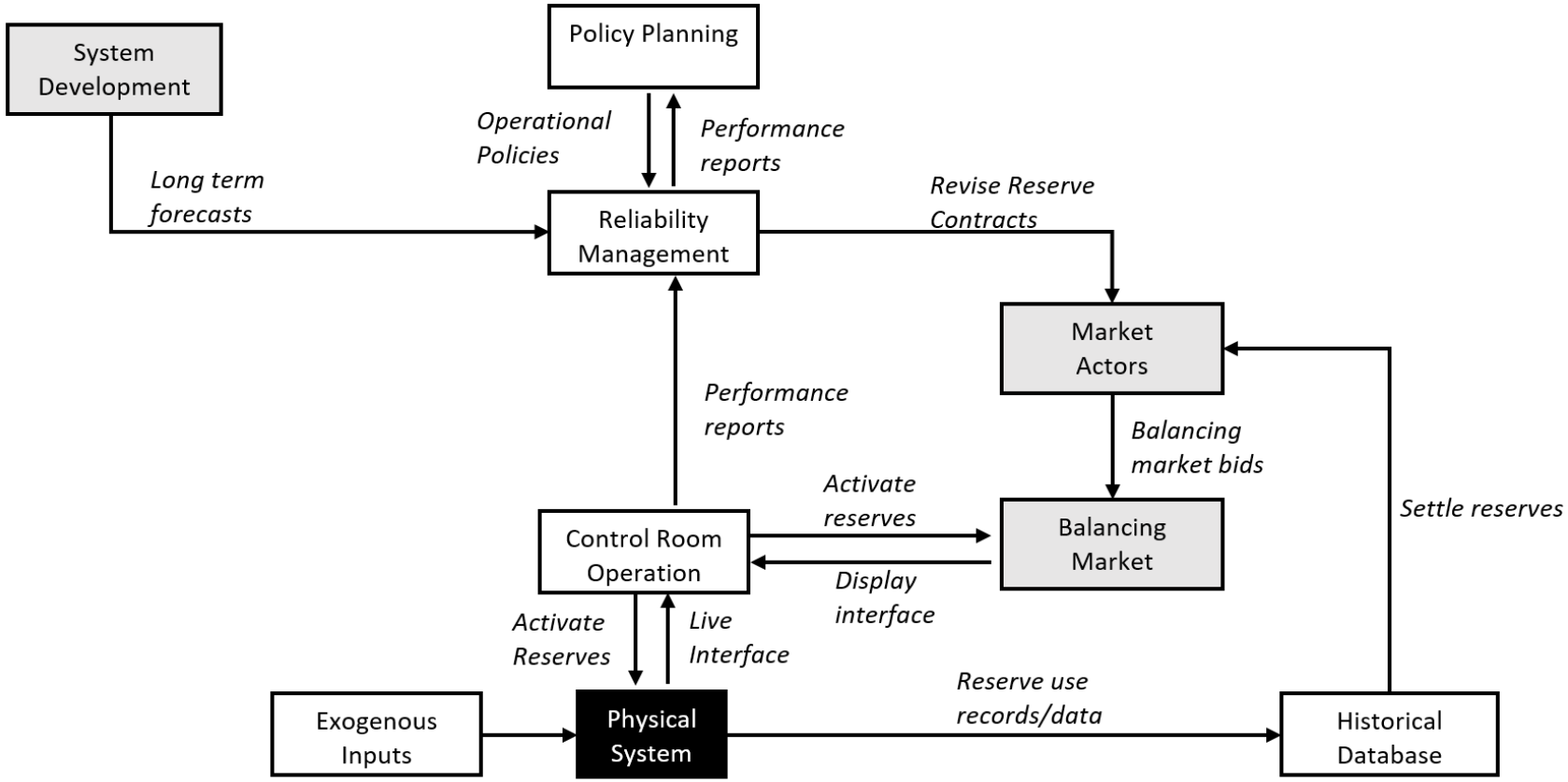
Network Capacities



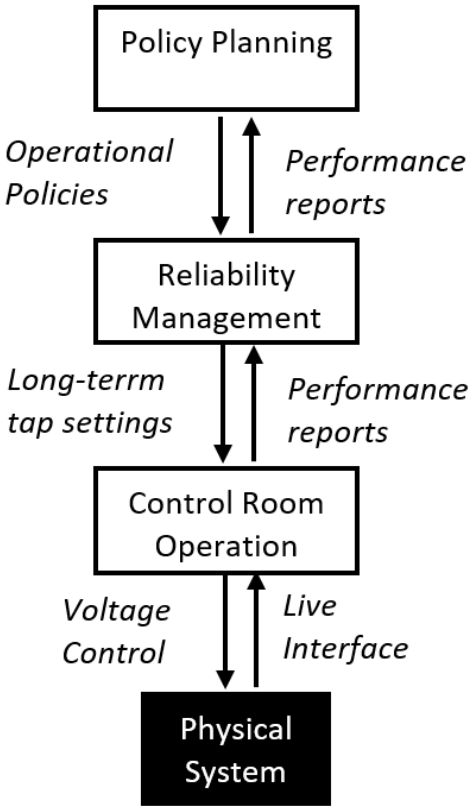
Outage Execution



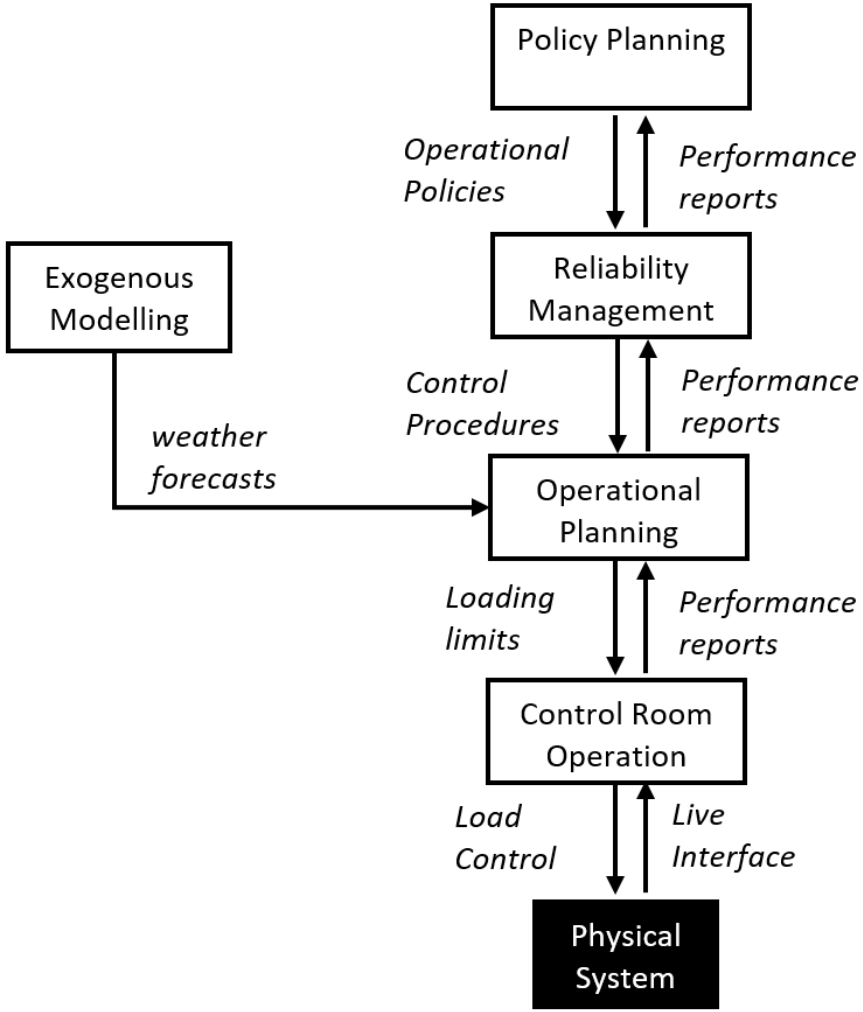
Reserve Management



Voltage Control



Component Load Control



System Protection