How safe is your embedded design, if at all?

Holger Hermanns

dependable systems and software

Saarland University

Saarbrücken, Germany

Safety?

Safety by design?

Make sure hazardous situations are unreachable!

Safety by design?

Make sure hazardous situations are unreachable!

Safety by design? Why bother?

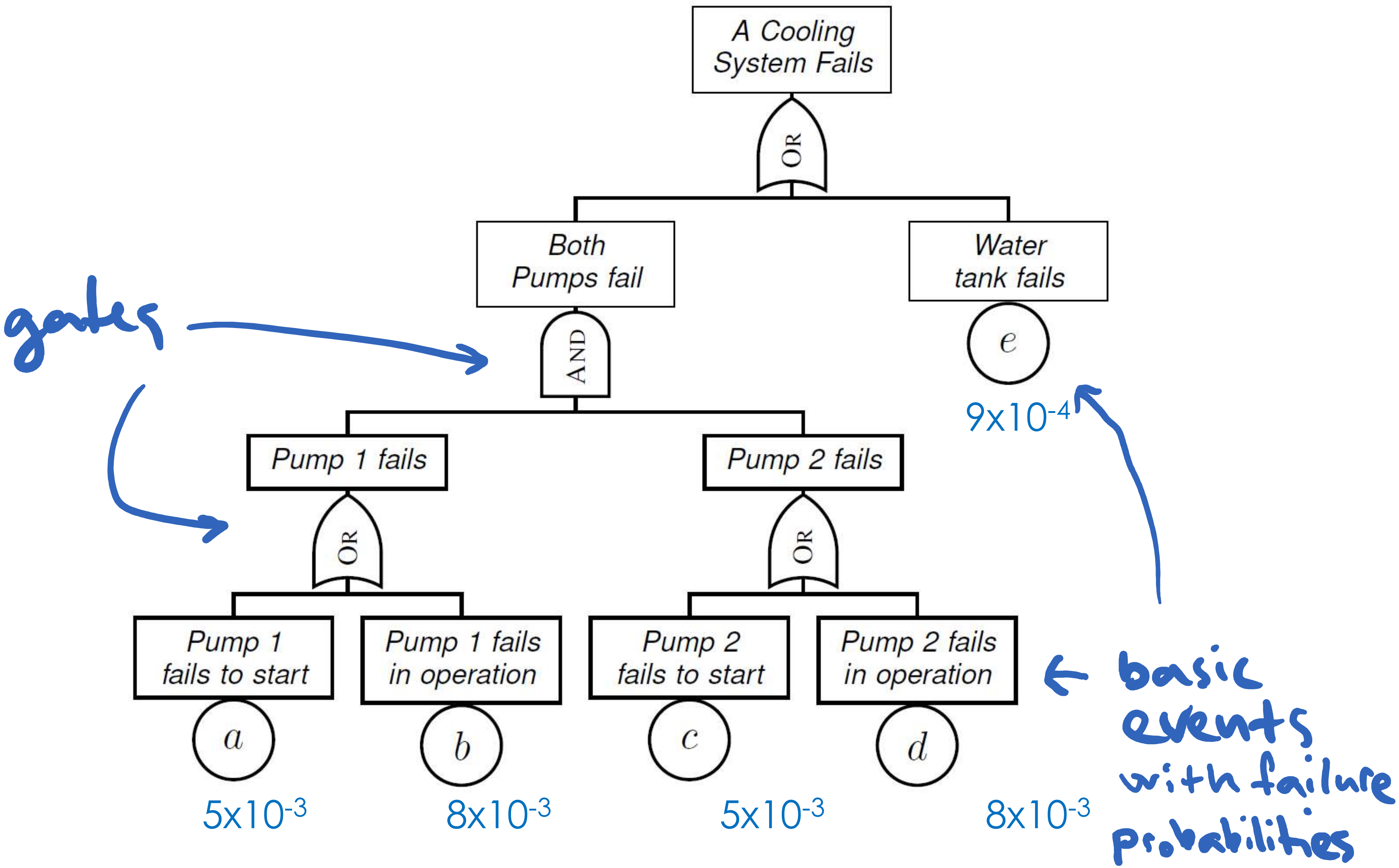
Enforced by various standards:

- *DO-178C/ED-12C for airborne systems* relates to ARP4761
  - Functional Hazard Assessment (FHA)
  - Preliminary System Safety Assessment (PSSA)
  - System Safety Assessment (SSA)
  - Fault Tree Analysis (FTA)
  - Failure Mode and Effects Analysis (FMEA)
  - Failure Modes and Effects Summary (FMES)
  - Common Cause Analysis (CCA)
- *ISO 26262 for automotive systems*
- ...

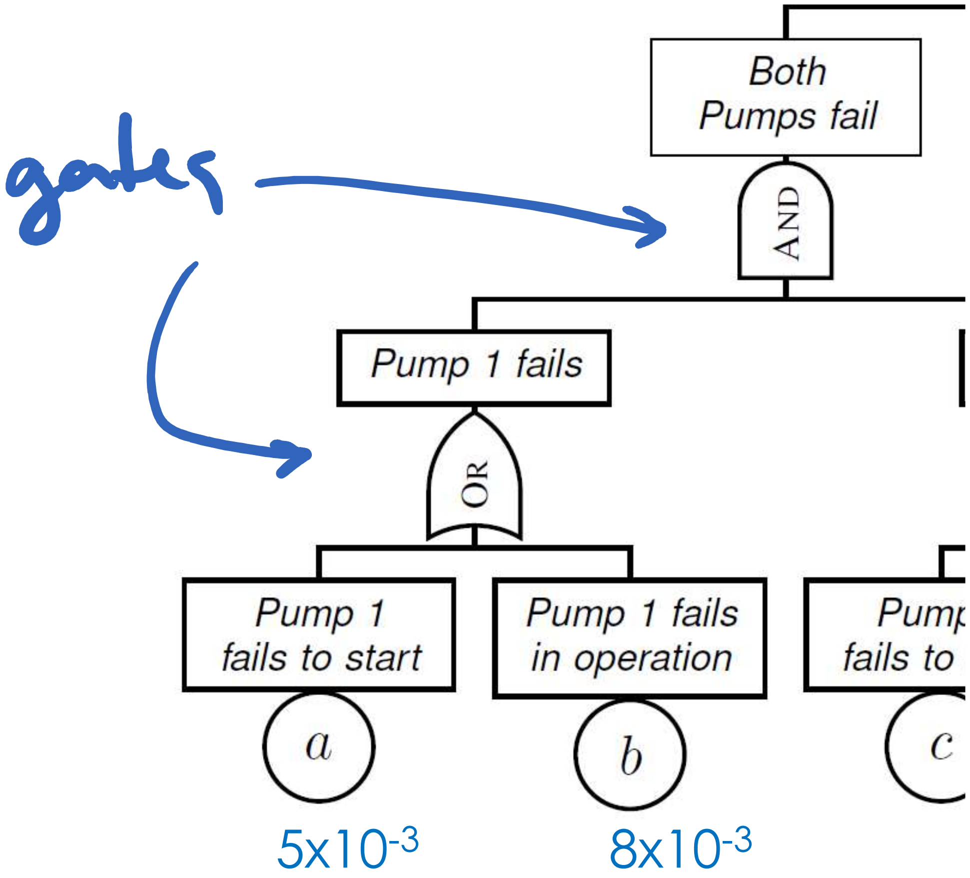
Higher/highest safety levels recommend

The Static View

Fault Trees


A Cooling System Fails
OR
Both Pumps fail
Water tank fails
AND
e
9x10-4
Pump 1 fails
Pump 2 fails
OR
OR
Pump 1 fails to start
Pump 1 fails in operation
Pump 2 fails to start
Pump 2 fails in operation
a
b
c
d
5x10-3
8x10-3
5x10-3
8x10-3
gates
basic events with failure probabilities

Fault Trees

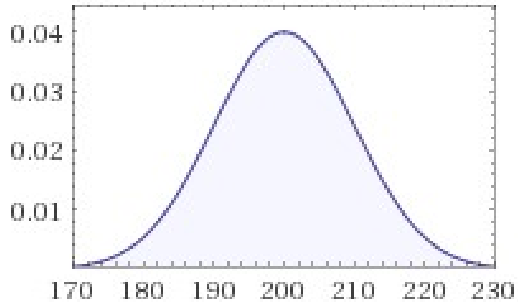


How to obtain the numbers?

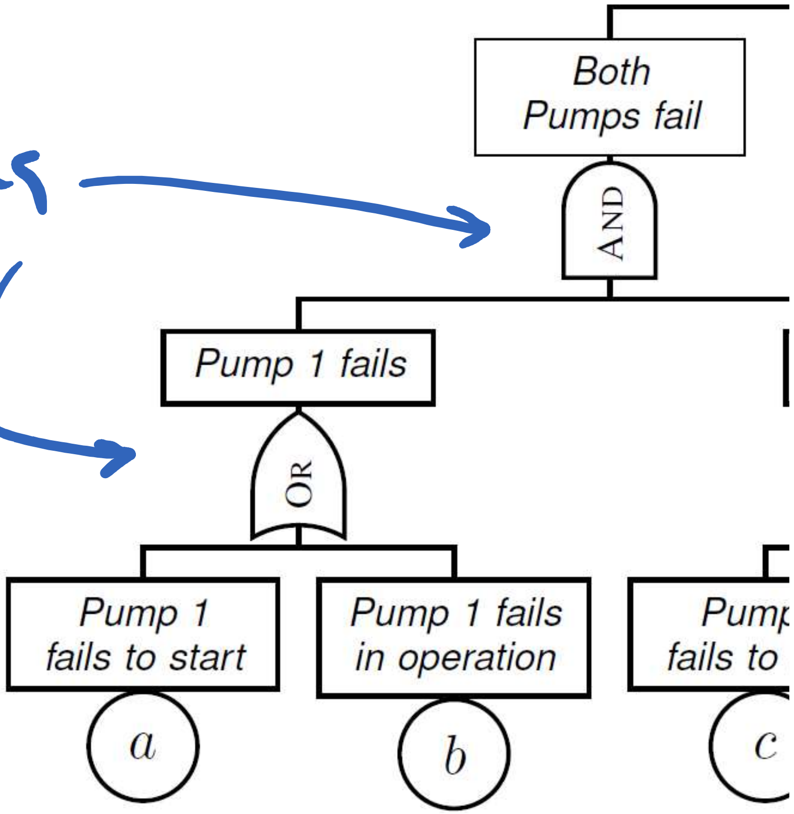
1) Time-independent failure

Average number of starts before failure: 200

⇒ Failure probability 0.005



Fault Trees



5x10^{-3} 8x10^{-3}

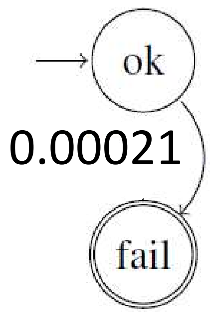
How to obtain the numbers?

1) Time-independent failure

Average number of starts before failure: 200

$\Rightarrow$ Failure probability 0.005

2) Time-dependent failure:



On average once per $\approx$ 4700 h

Mission time: 24h

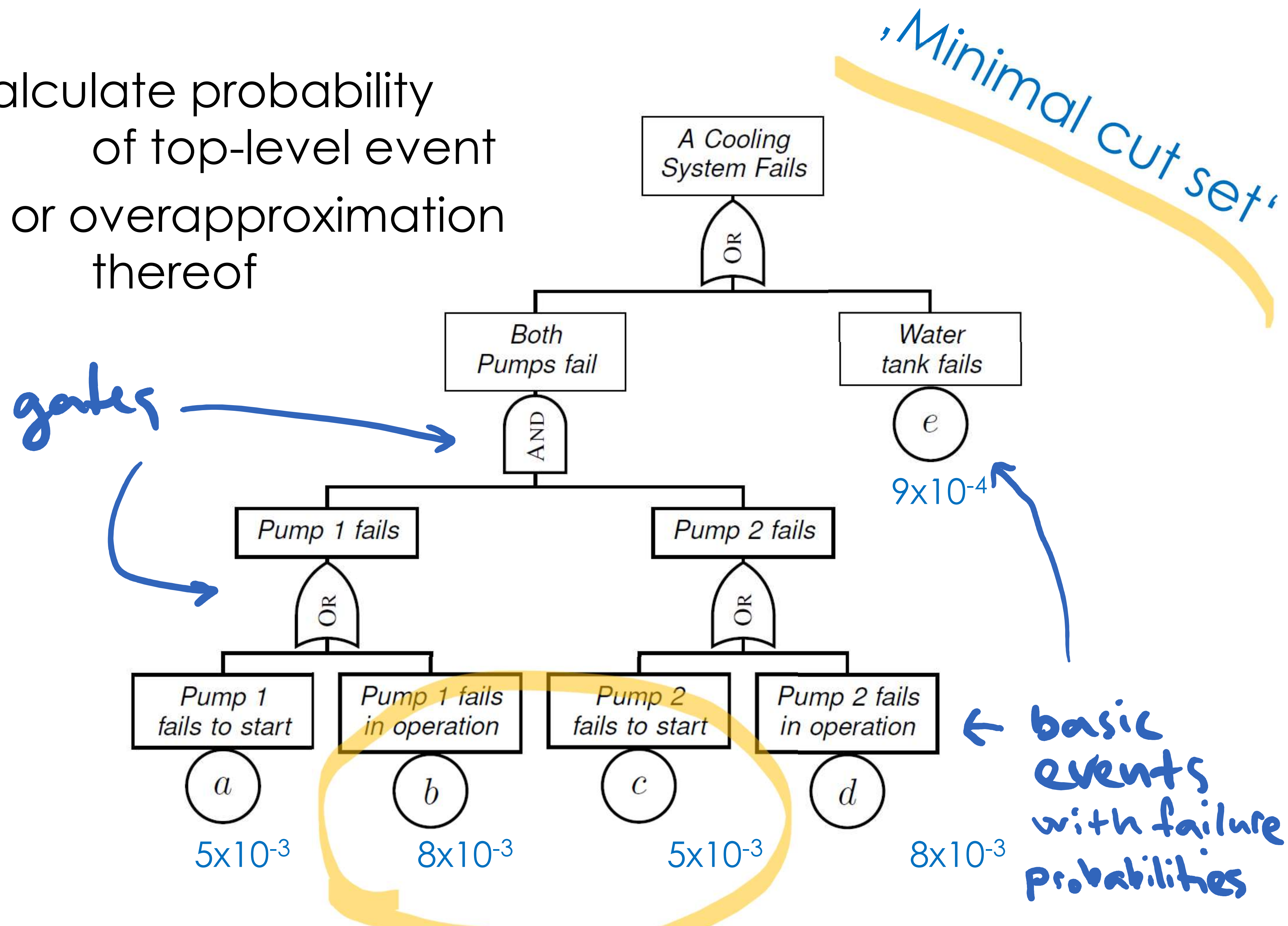
Probability to fail in 24 hours:
$1 - e^{-24 \cdot 0.00021} \approx 0.005$

... and from further models

Fault Trees – Analysis Basics

Calculate probability
of top-level event

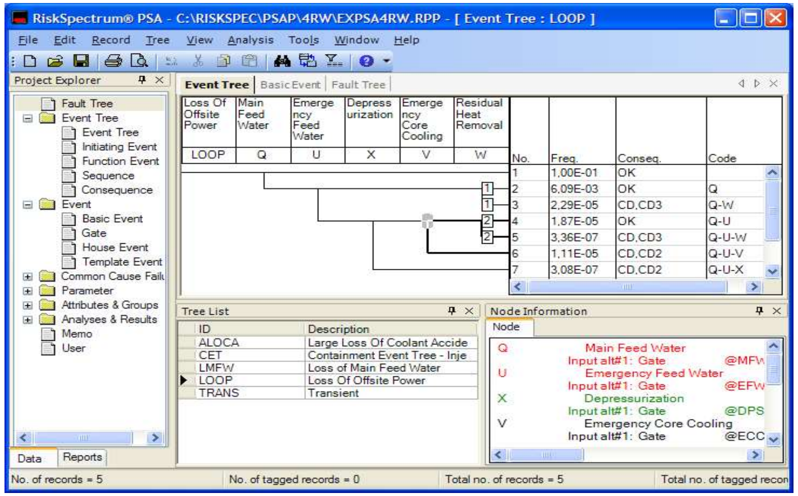
… or overapproximation
thereof



Fault Trees

RISK SPECTRUM licensed at > 55% of nuclear power plants worldwide

- are often very large *50,000+ nodes*
- are very costly to maintain *millions of €*
- are very important
- are stateless
- give imprecise results
  - too pessimistic due to stateless view *e.g. no repair*
  - too optimistic if dependencies *e.g. common cause*
  - ...



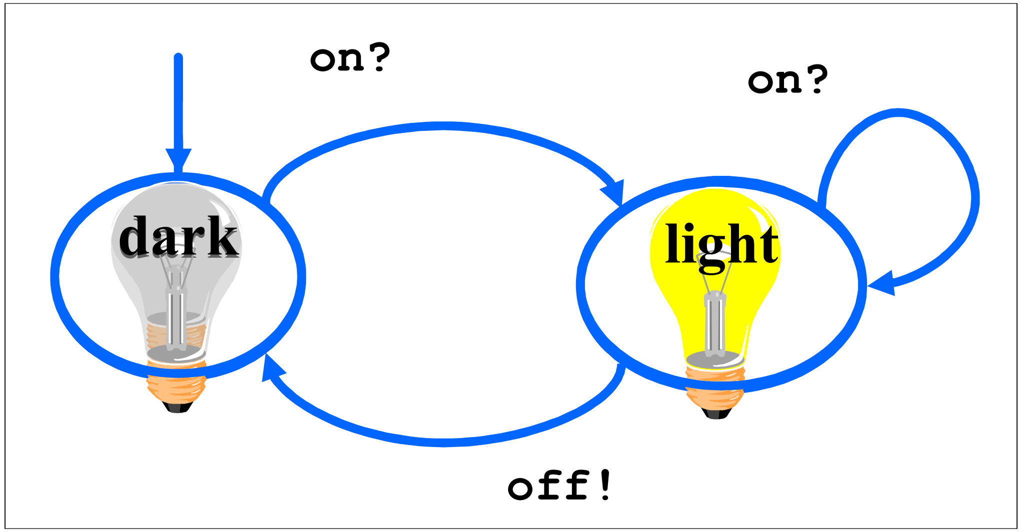
Models for Safety

All models are wrong, but some are useful.

George E. P. Box

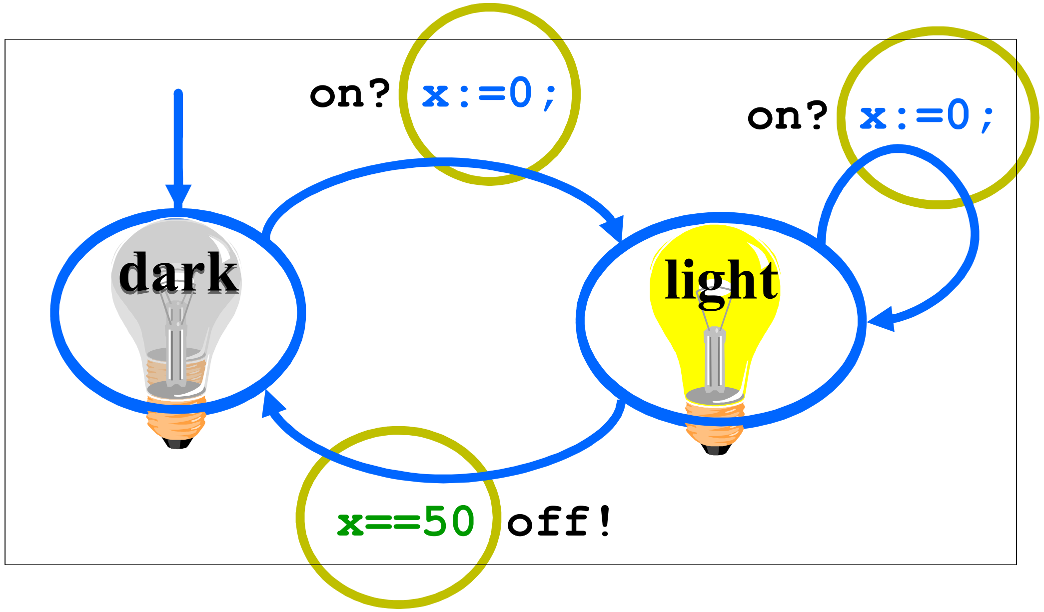
Useful Models

- finite automata



Useful Models

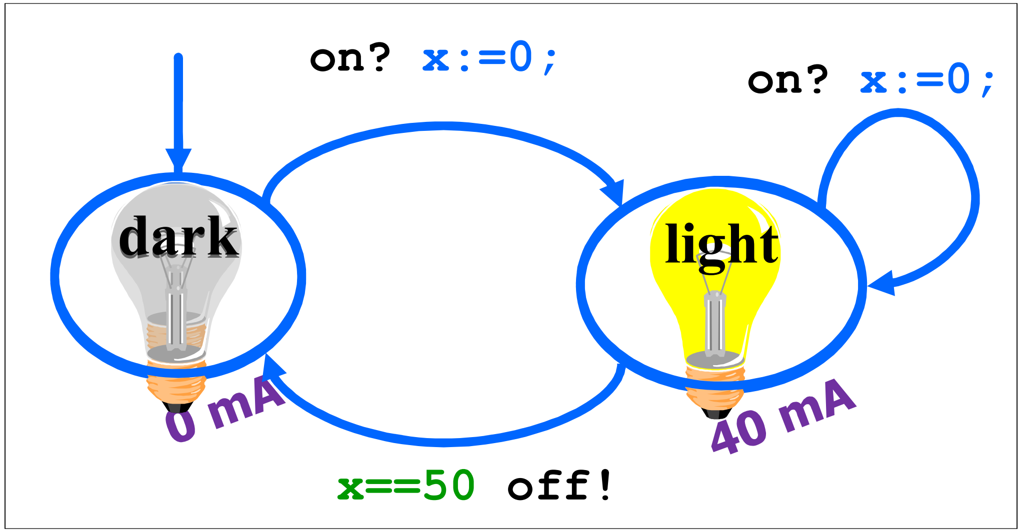
- finite automata
- with clocks *all running at the same speed*



Timed Automata

Useful Models

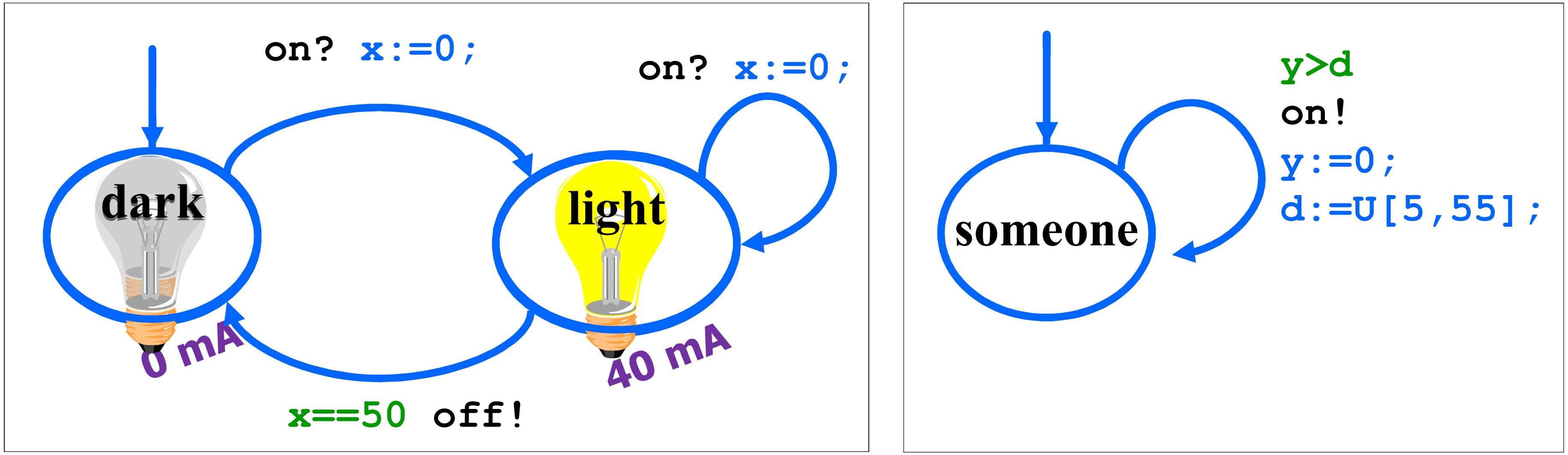
- finite automata
- with clocks
- and with costs *incurred as time advances*



Priced Timed Automata

Useful Models

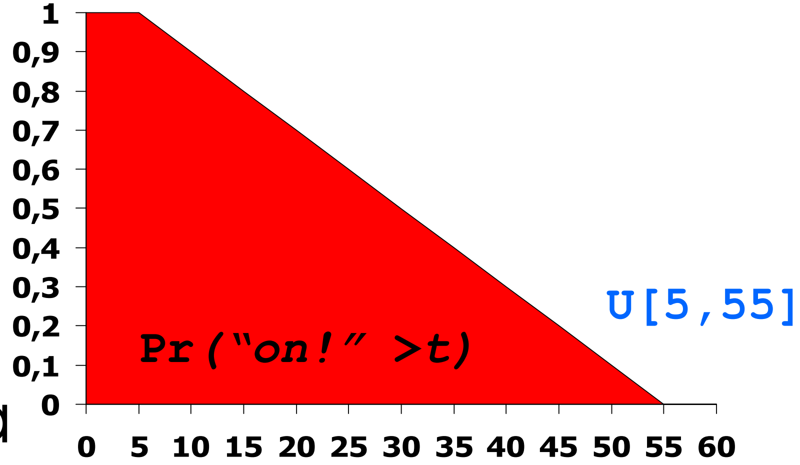
- finite automata
- with clocks
- and with costs
- modular: composition of automata

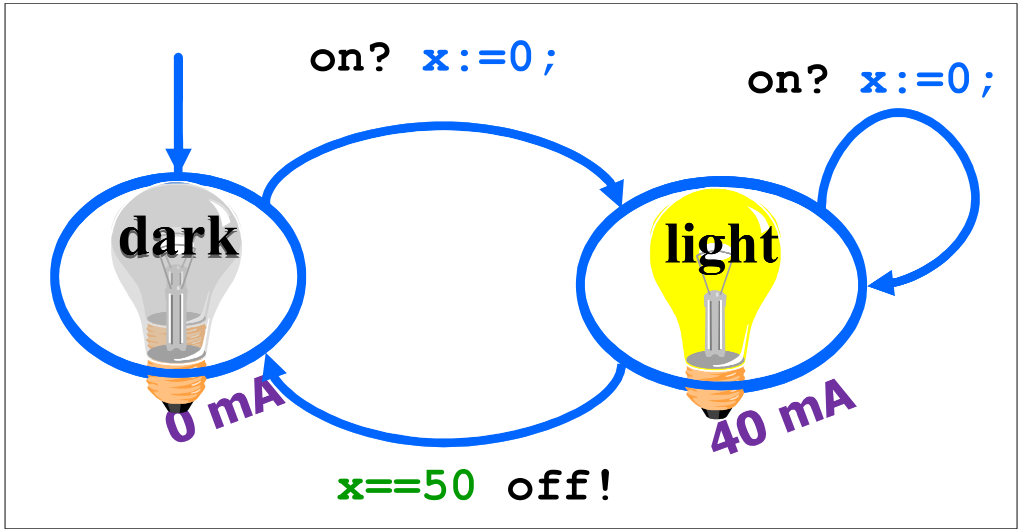


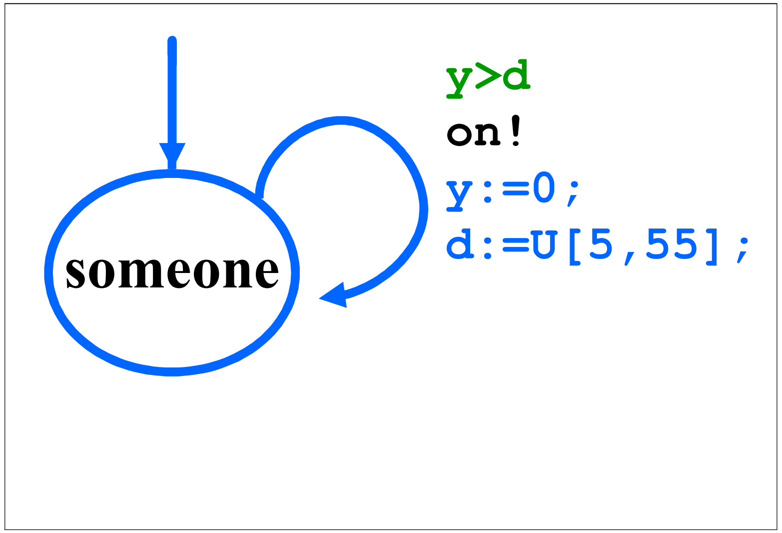
Automata Networks

Useful Models

- finite automata
- with clocks
- and with costs
- modular: composition of automata





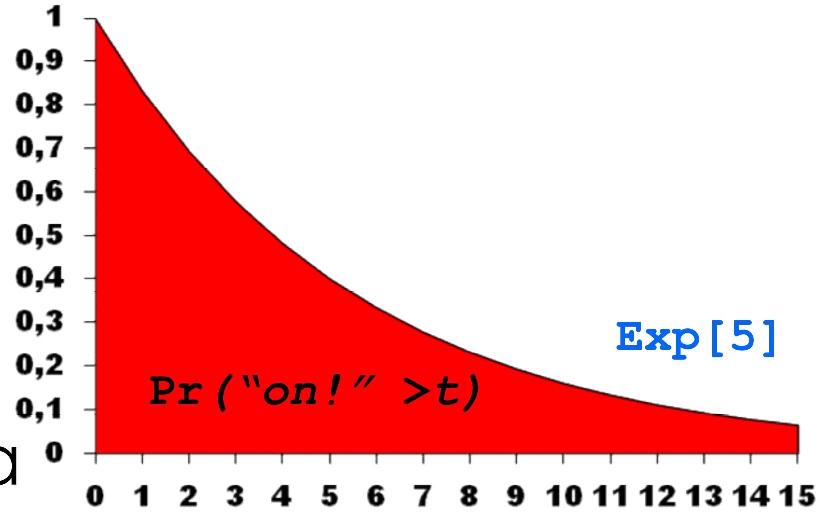


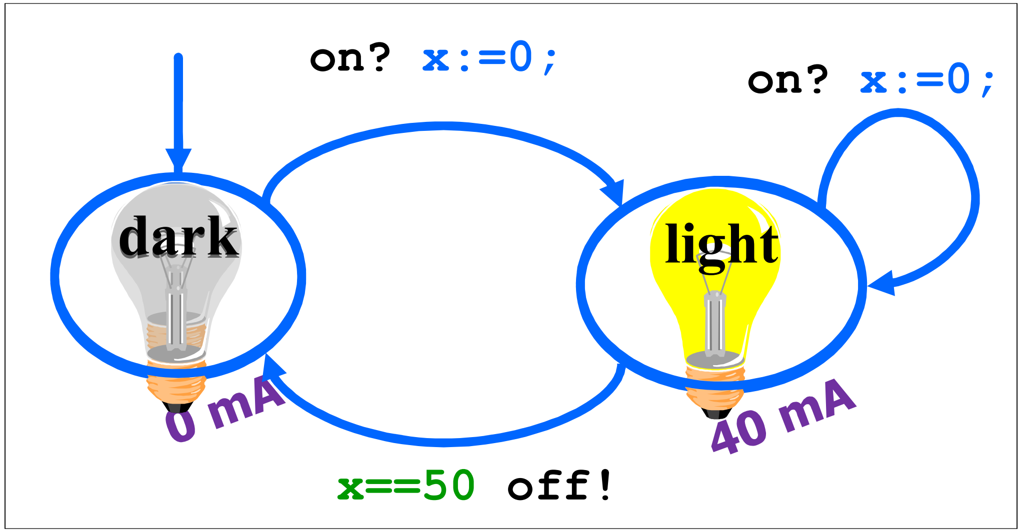
- with probability distributions

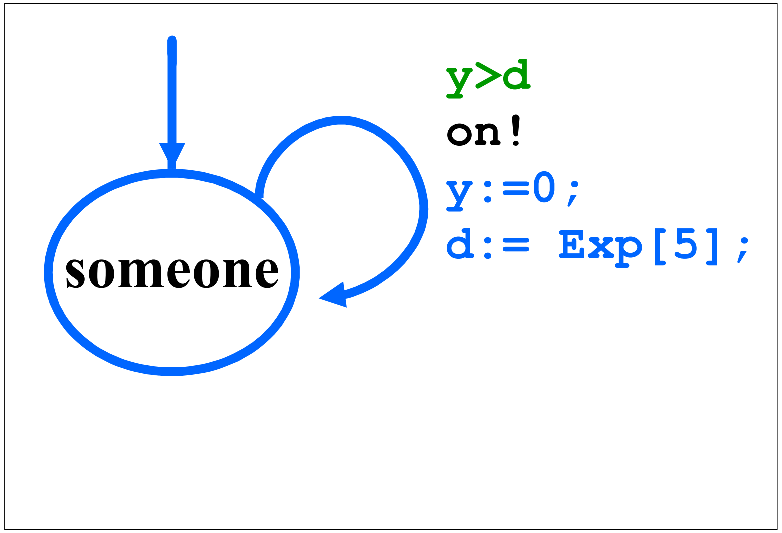
Stochastic Timed Automata

Useful Models

- finite automata
- with clocks
- and with costs
- modular: composition of automata





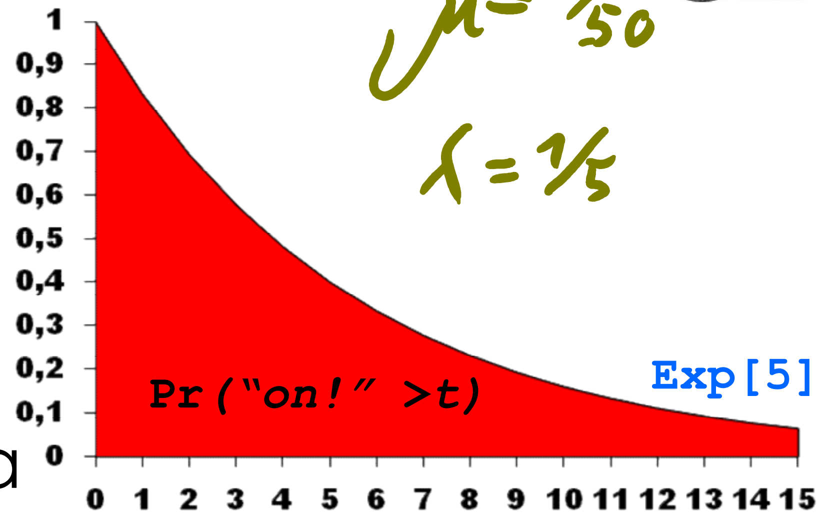


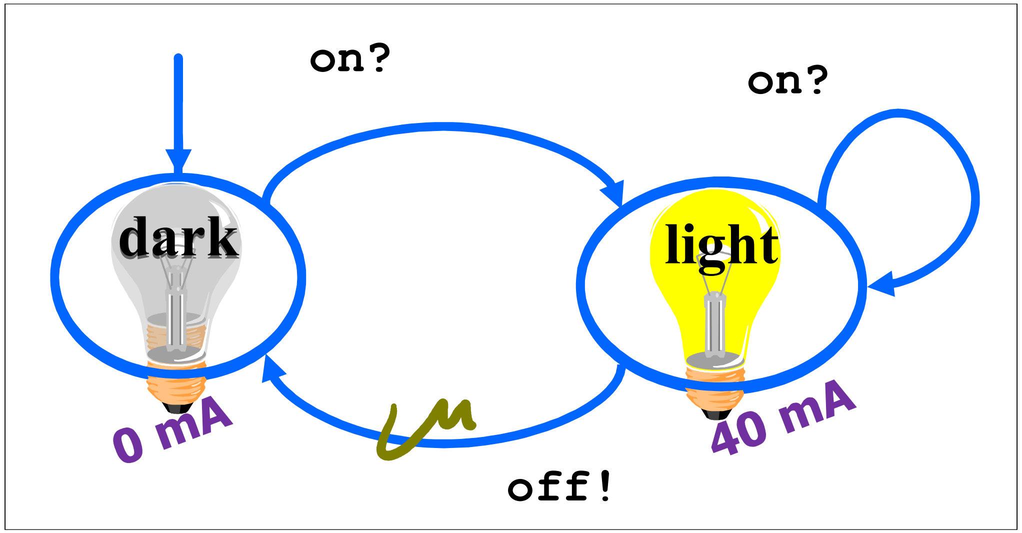
- with probability distributions

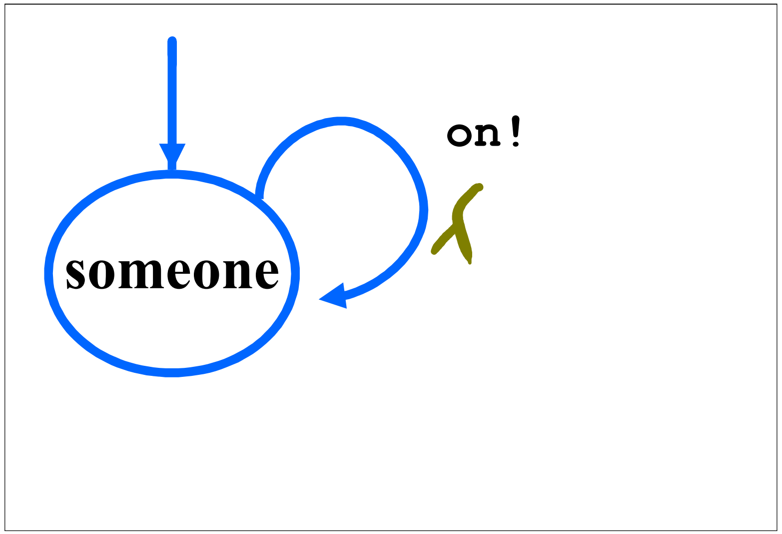
Stochastic Timed Automata

Useful Models

- finite automata
- with ~~clocks~~ memoryless time
- and with costs
- modular: composition of automata





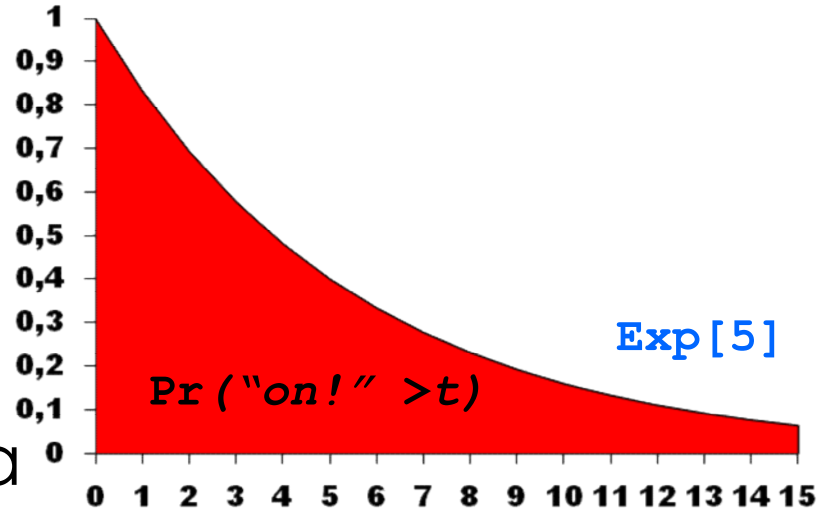


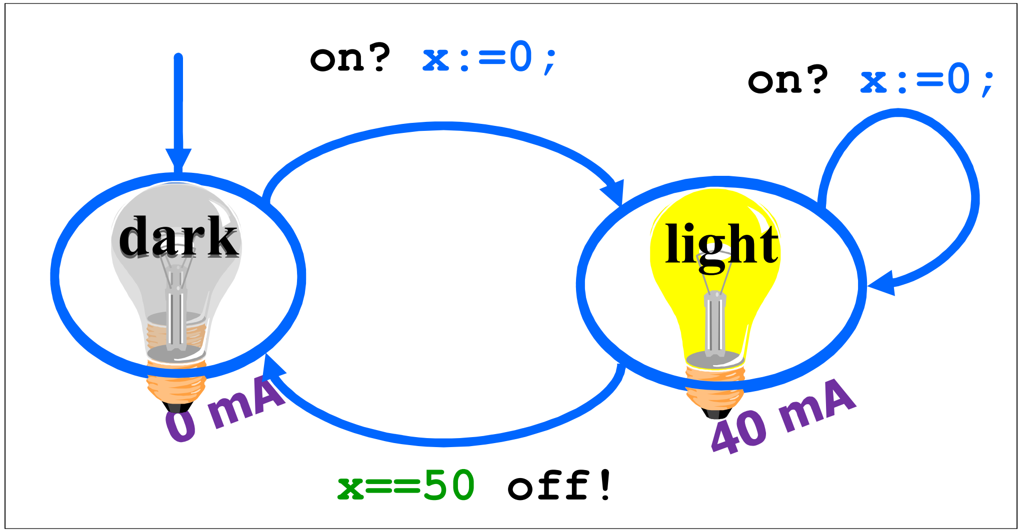
- with probability distributions

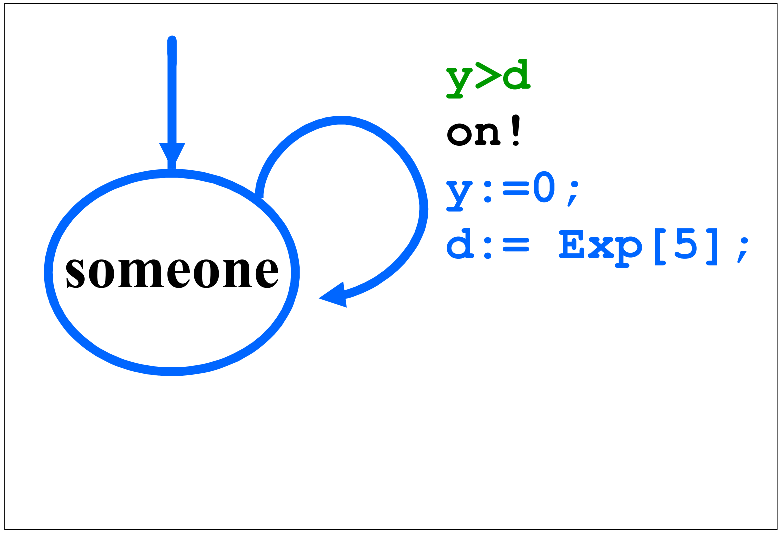
Markov Automata

Useful Models

- finite automata
- with clocks
- and with costs
- modular: composition of automata





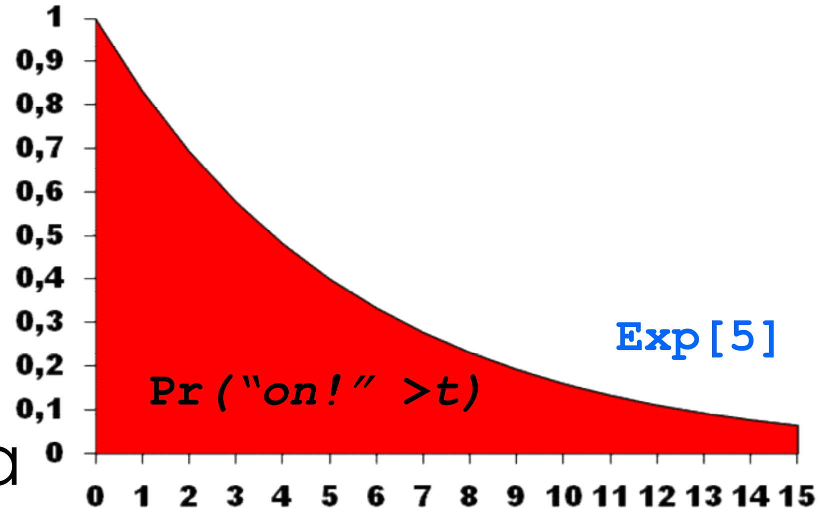


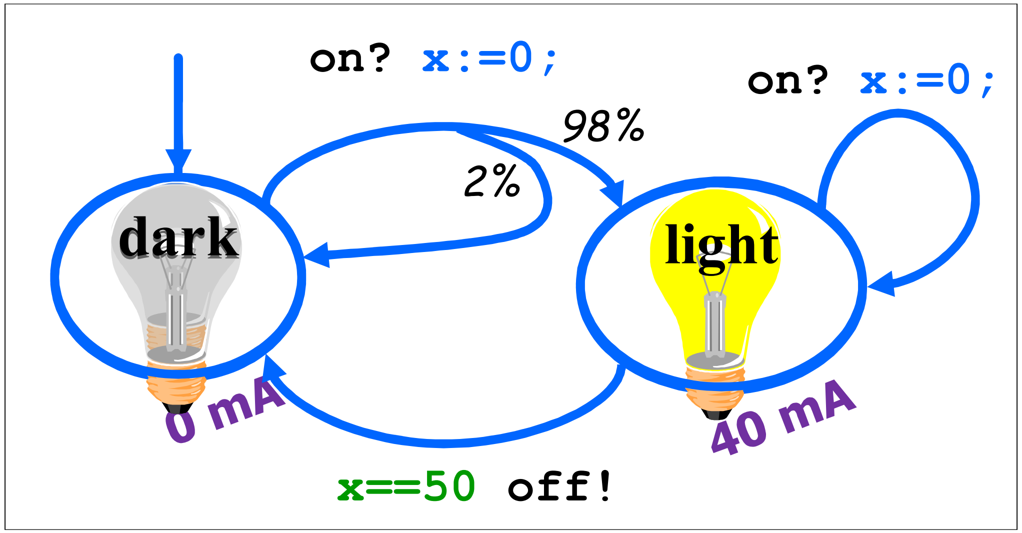
- with probability distributions

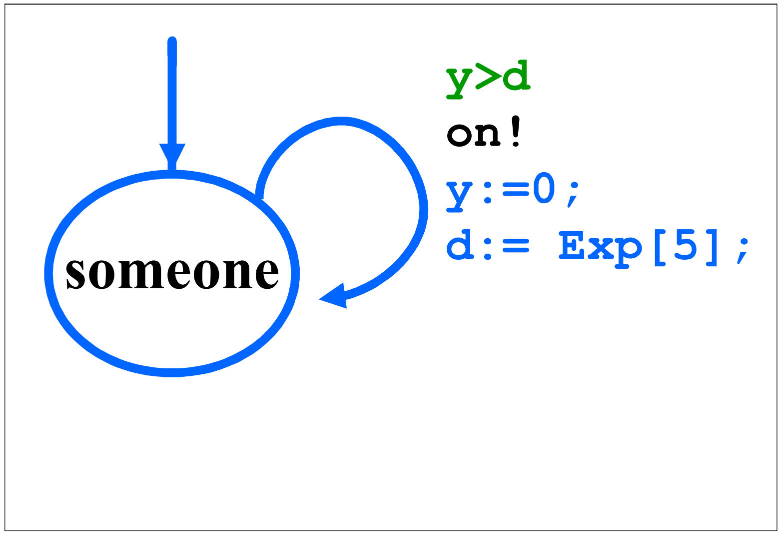
Stochastic Timed Automata

Useful Models

- finite automata
- with clocks
- and with costs
- modular: composition of automata





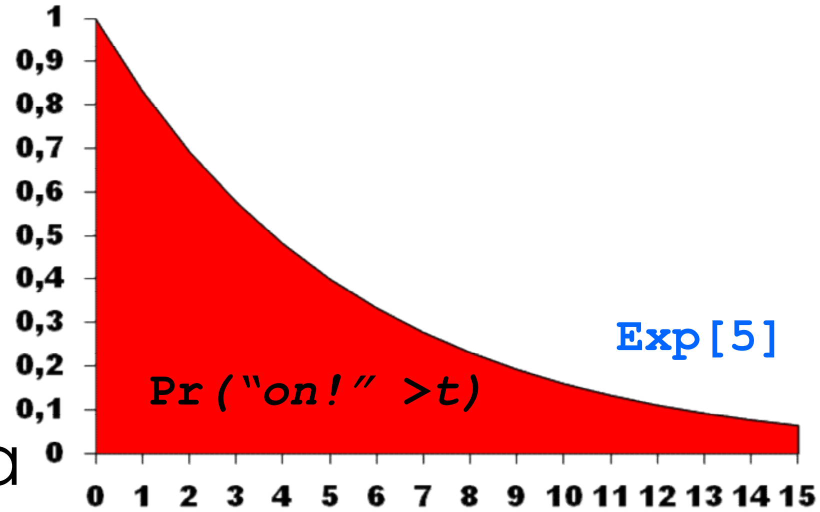


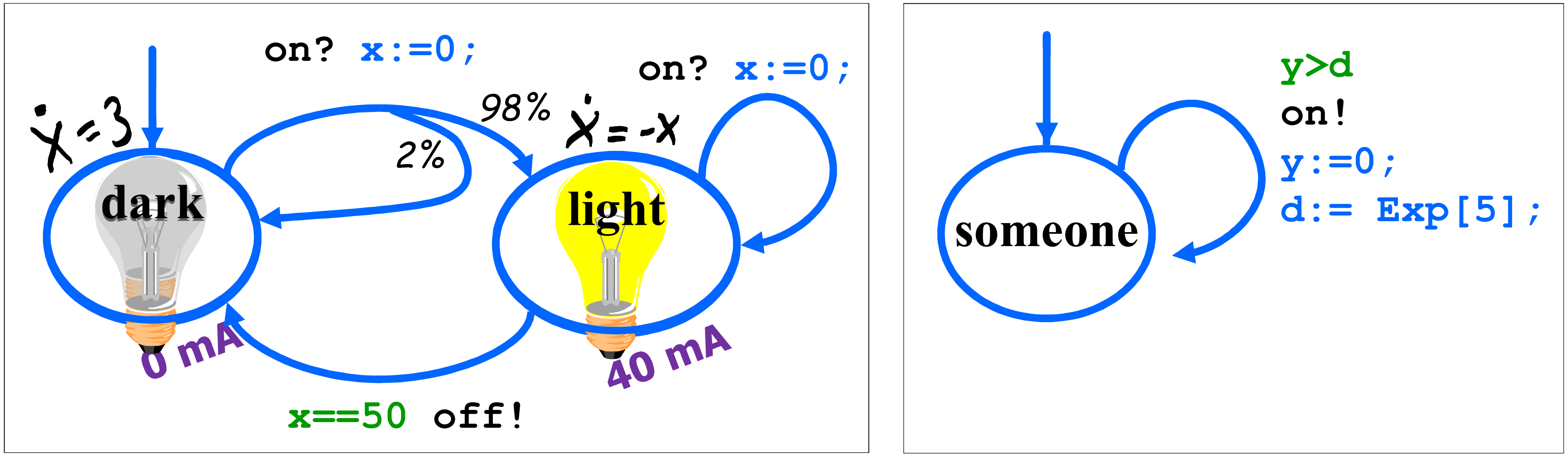
- with probability distributions

Stochastic Timed Automata

Useful Models

- finite automata
- with clocks
- and with costs
- modular: composition of automata





- with probability distributions
- and continuous dynamics

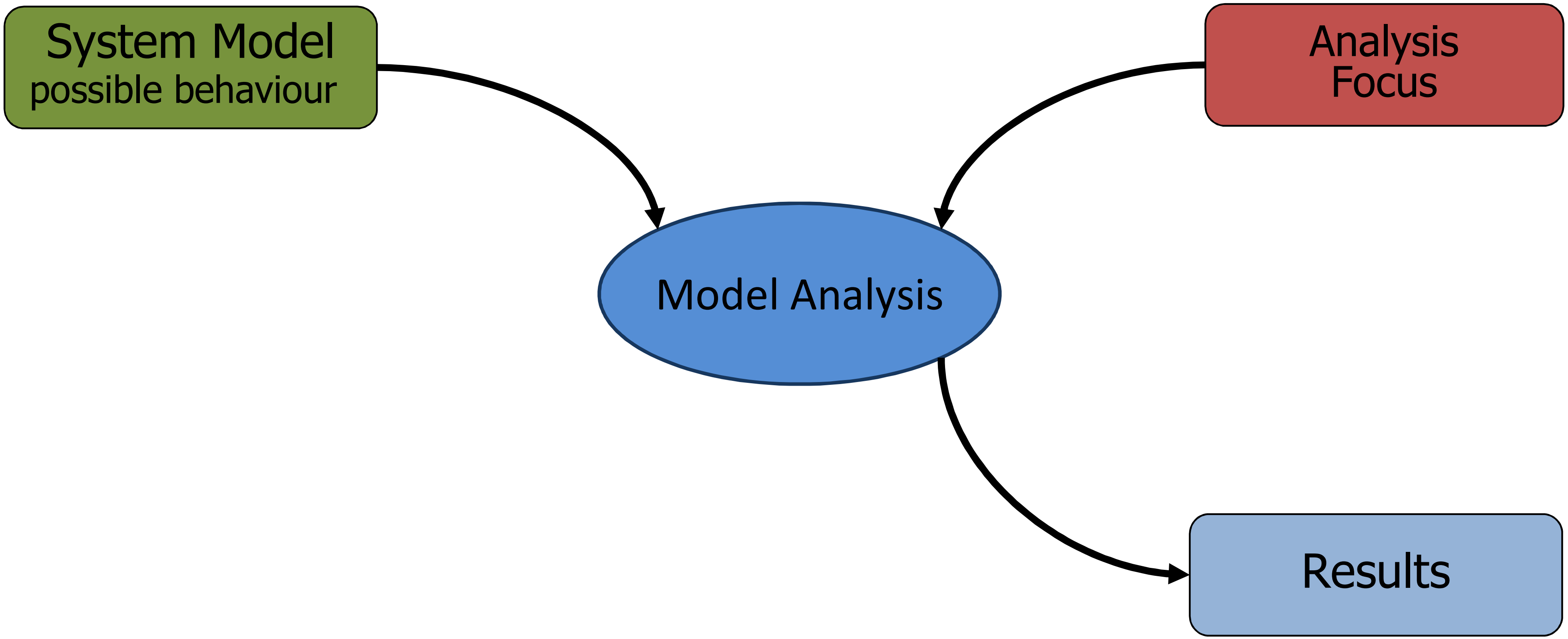
Stochastic Hybrid Automata

THE

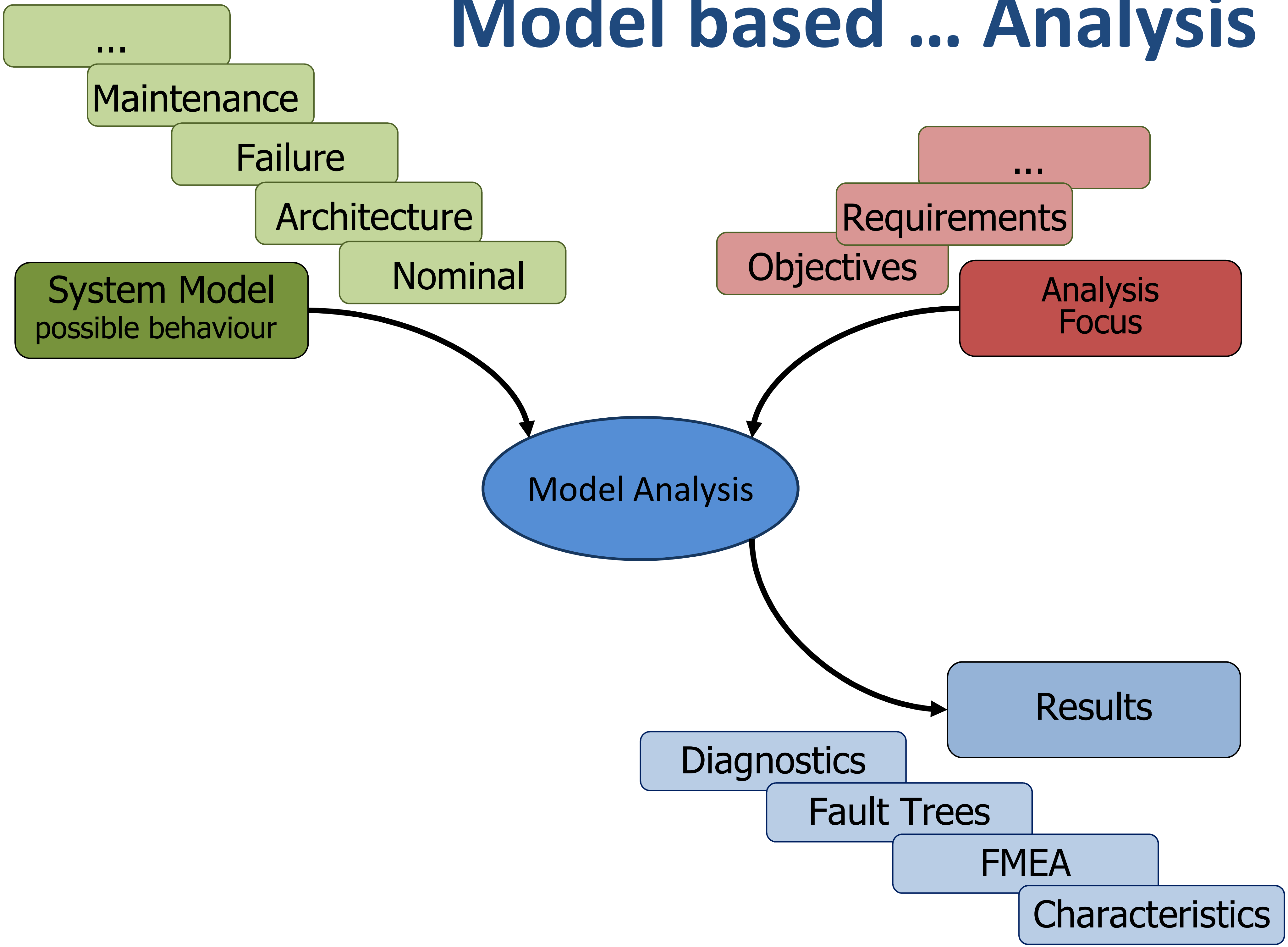
BIGGER

PICTURE

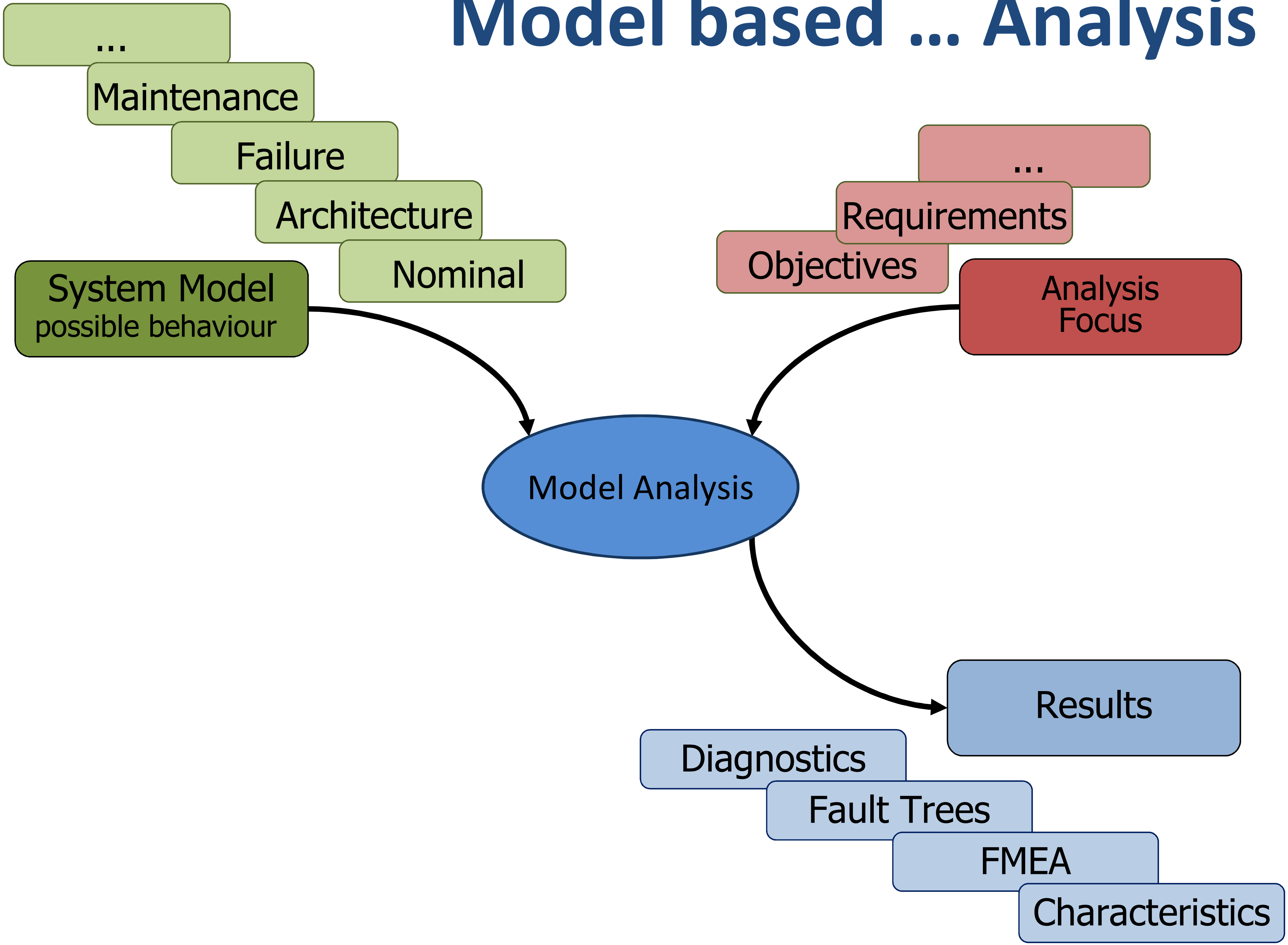
Model based … Analysis



Model based … Analysis



Model based … Analysis



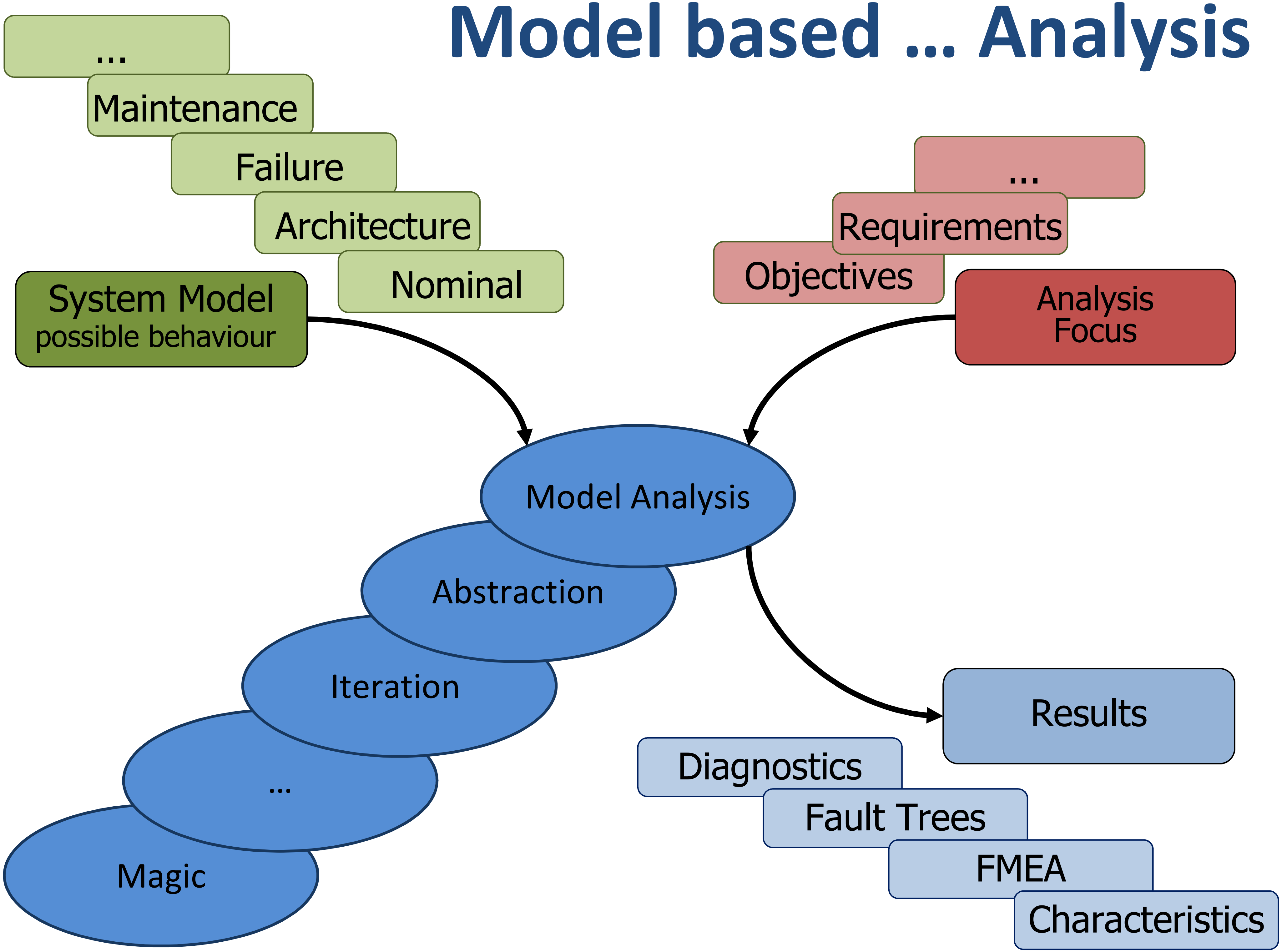
lysis

...

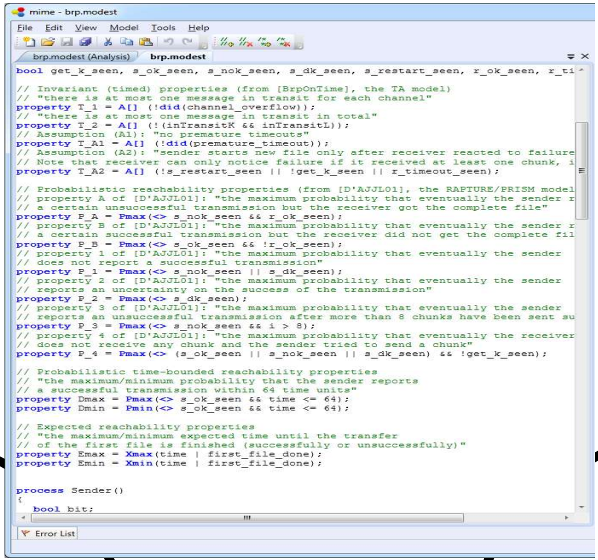
odel Analy

tics

Model based … Analysis



Model based … Analysis



System Model
possible behaviour

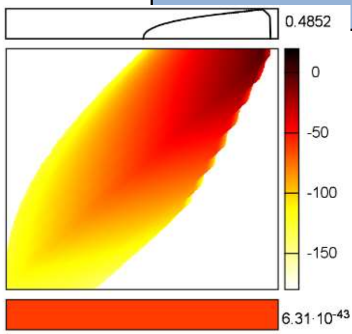
Analysis
Focus

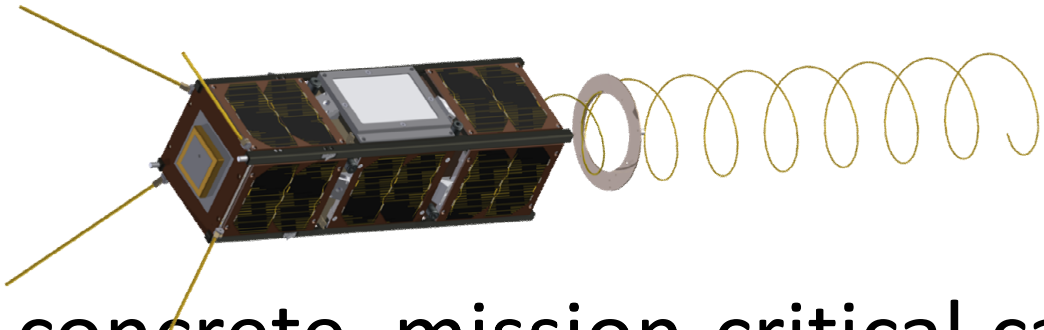
Model Analysis

modestchecker.org

UPPAAL CORA

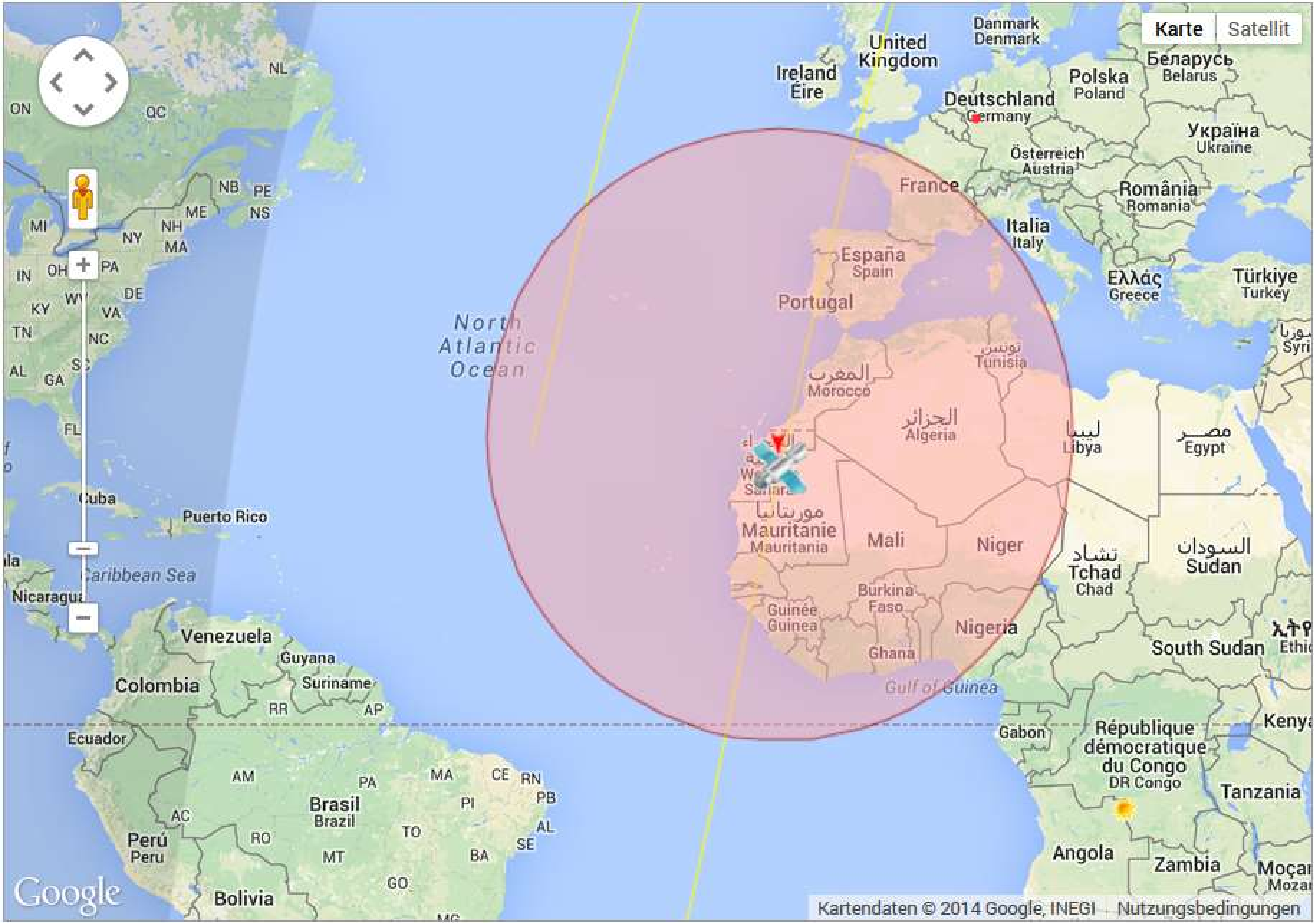
Results





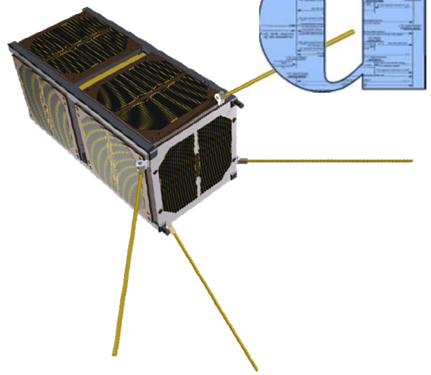
A concrete, mission-critical case

Embedded in Space



GOMSPACE

GOMX-1

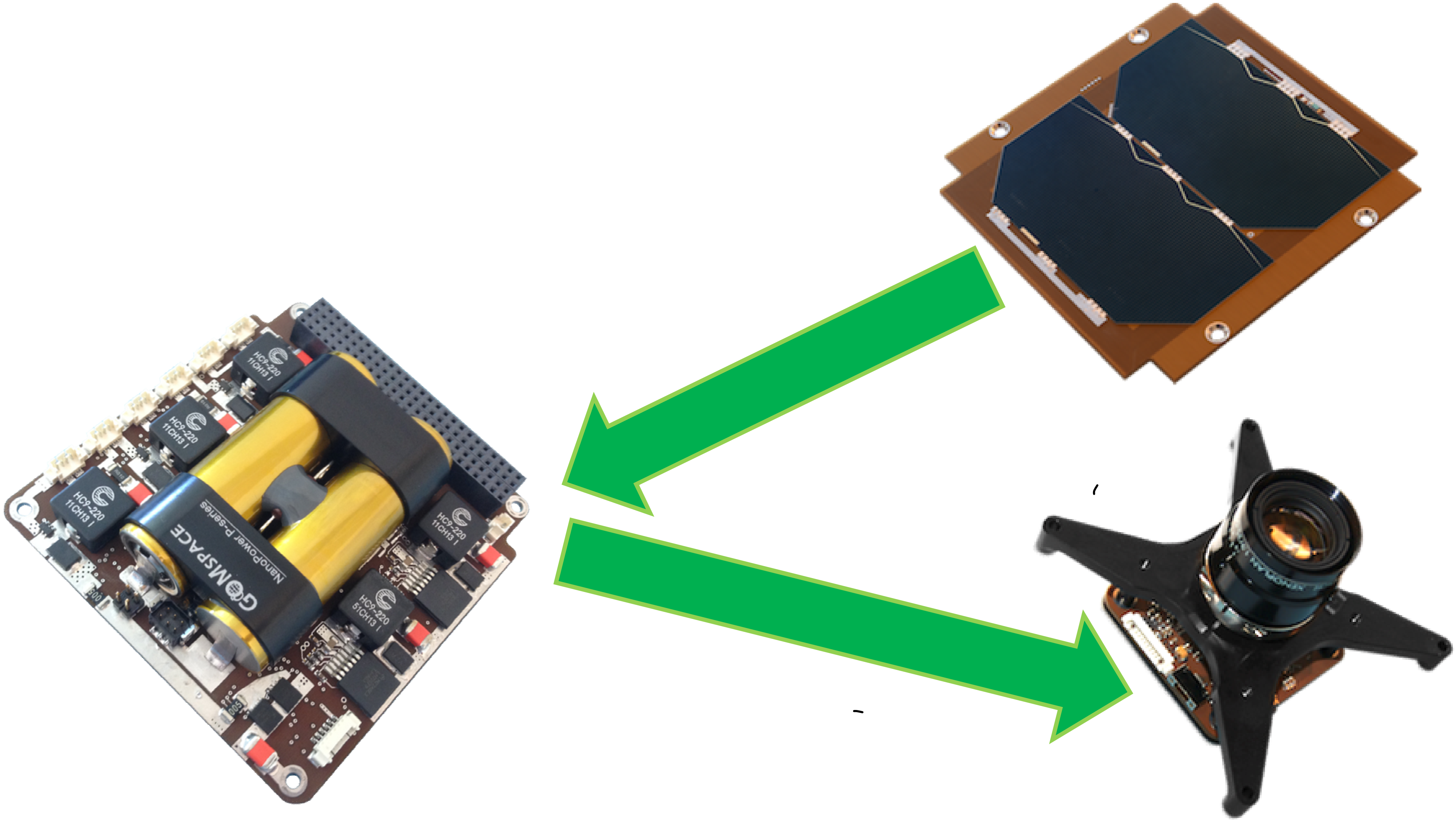


- 2U CubeSat (2 liter)
- Launched in November 2013
- Payloads:
  - software defined receiver for aircraft signals
  - color camera for earth observation
- Telemetry transmitted on amateur radio frequency
- Massive amounts of data collected
  - battery voltage, temperature, solar infeed, …

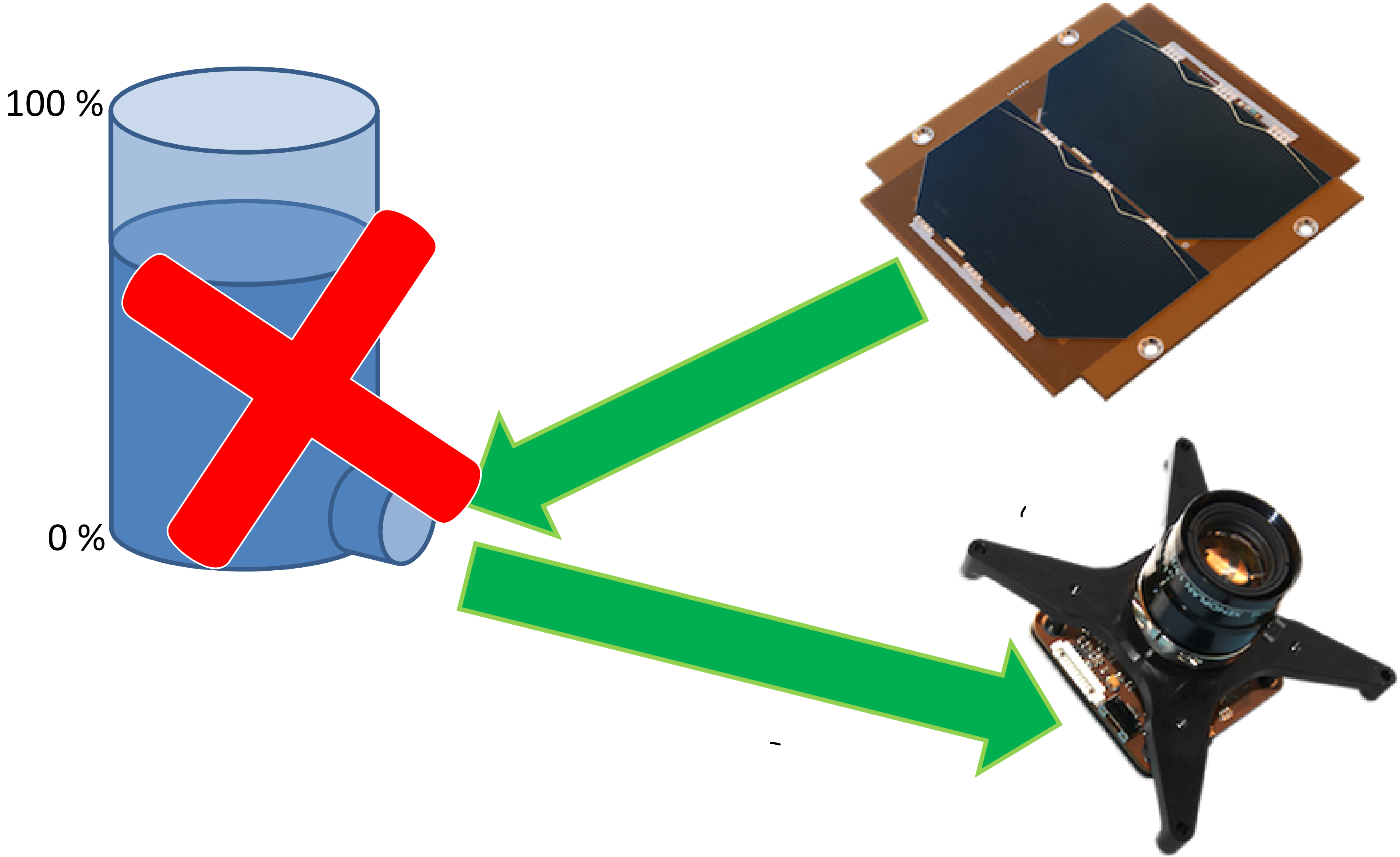
Runs our calibration experiments.

SENSATION

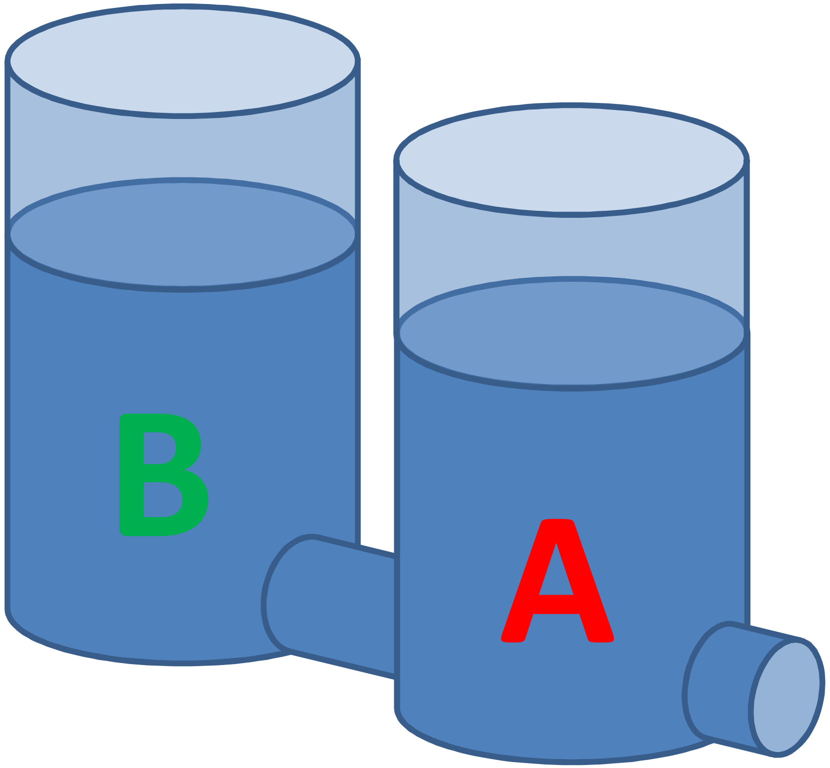
Battery Kinetics

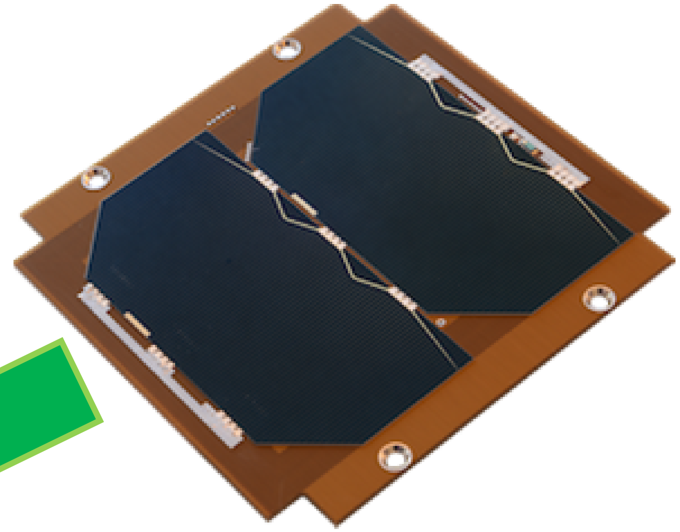


Battery Kinetics



Battery Kinetics





Kinetic Battery Model

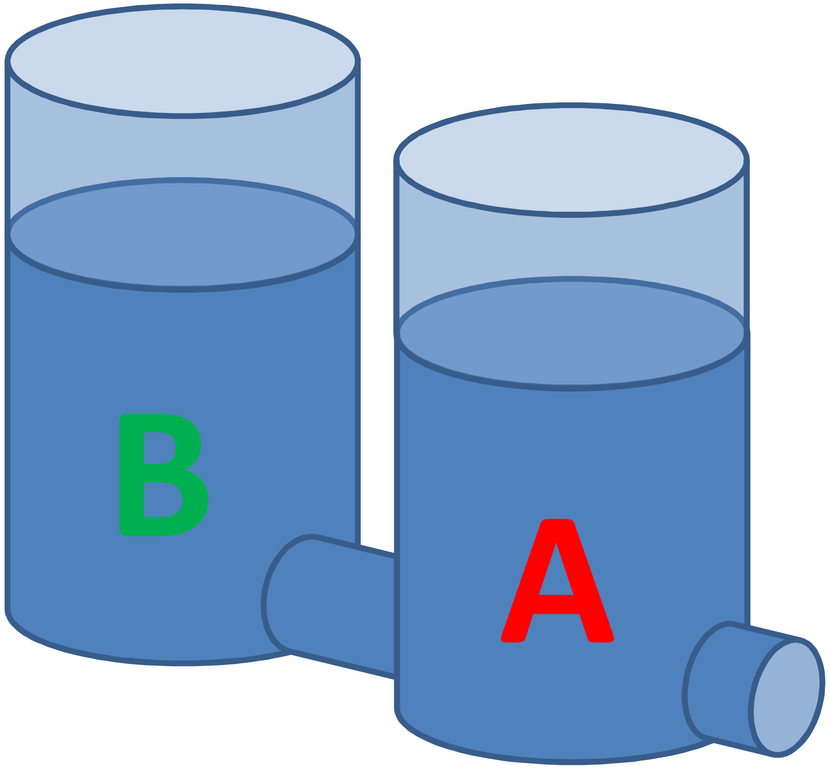
- can represent 'rate-capacity effect'
- can represent 'recovery effect'

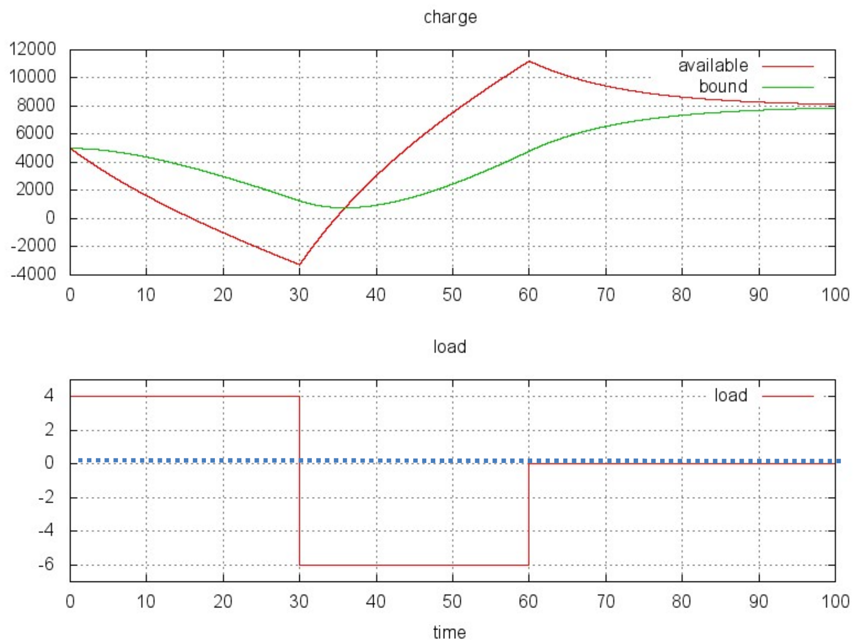
   ➢ *a faithful abstraction of modern battery chemistry*

Battery Kinetics

$$\dot{a}(t) = -I + p\left(\frac{b(t)}{1-c} - \frac{a(t)}{c}\right)$$

$$\dot{b}(t) = p\left(\frac{a(t)}{c} - \frac{b(t)}{1-c}\right)$$





Kinetic Battery Model

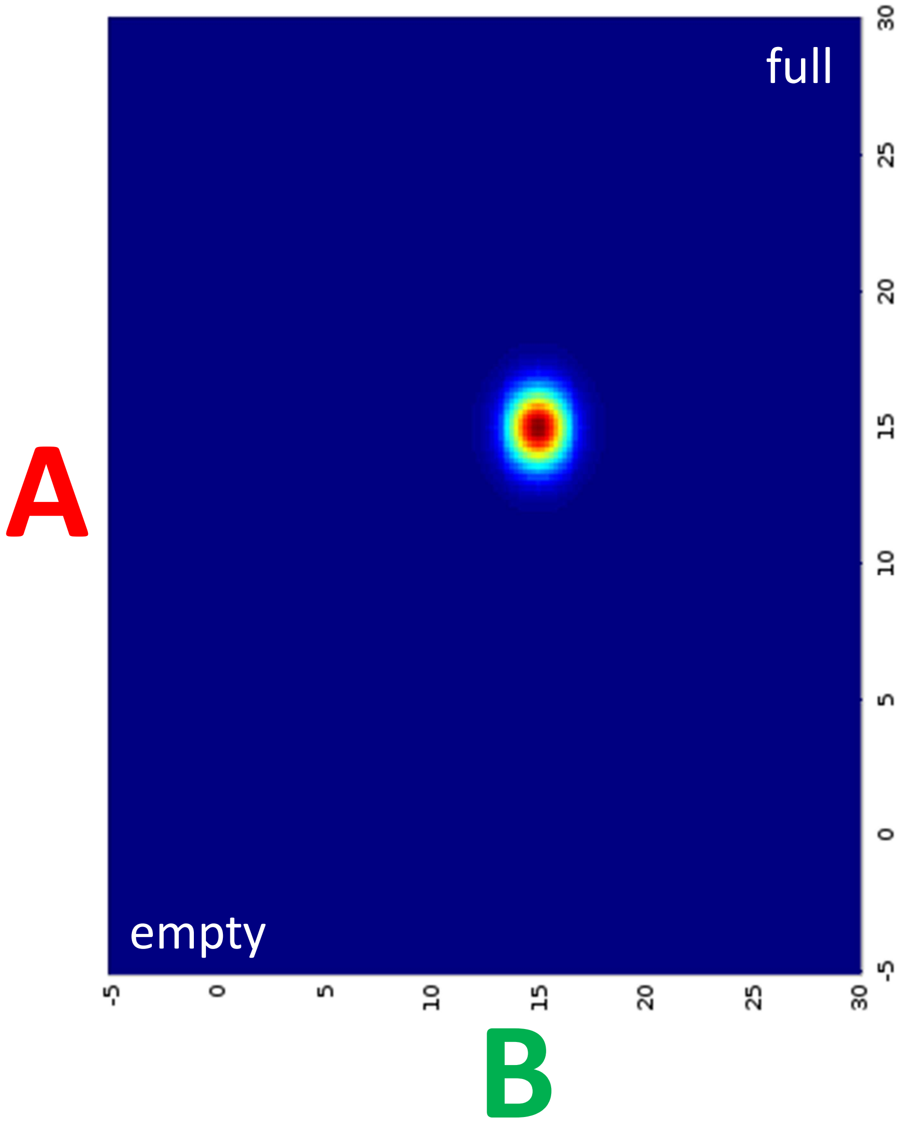
- can represent ‘rate-capacity effect’
- can represent ‘recovery effect’

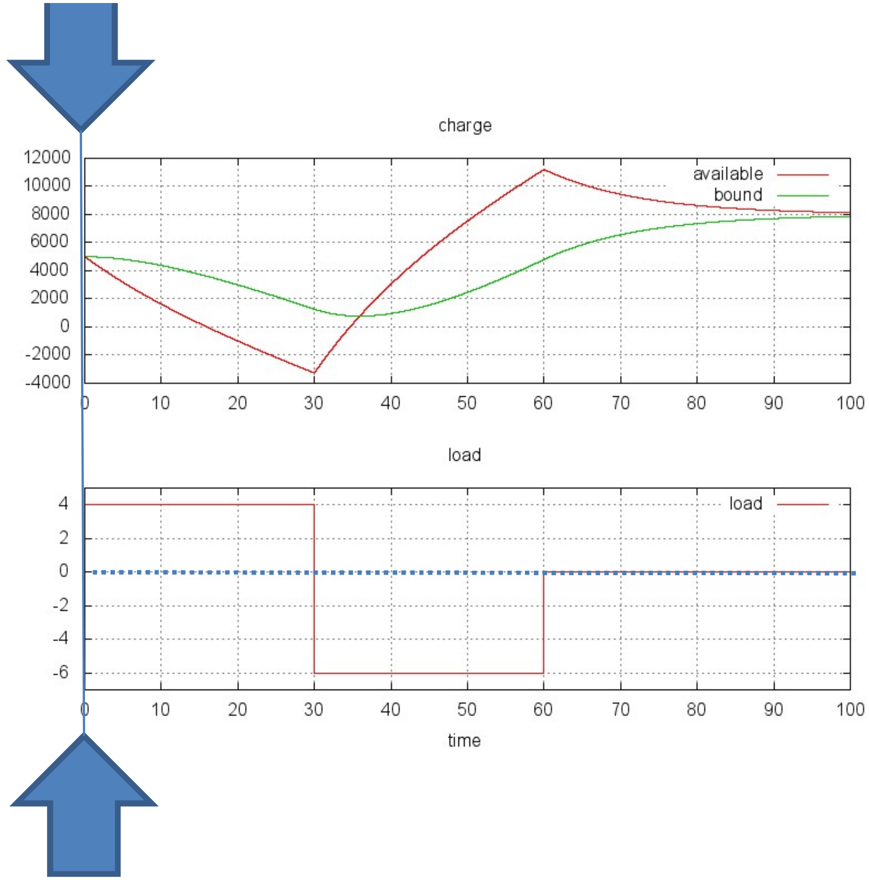
➢ *a faithful abstraction of modern battery chemistry*

Battery Kinetics

$$\dot{a}(t) = -I + p\left(\frac{b(t)}{1-c} - \frac{a(t)}{c}\right)$$

$$\dot{b}(t) = p\left(\frac{a(t)}{c} - \frac{b(t)}{1-c}\right)$$

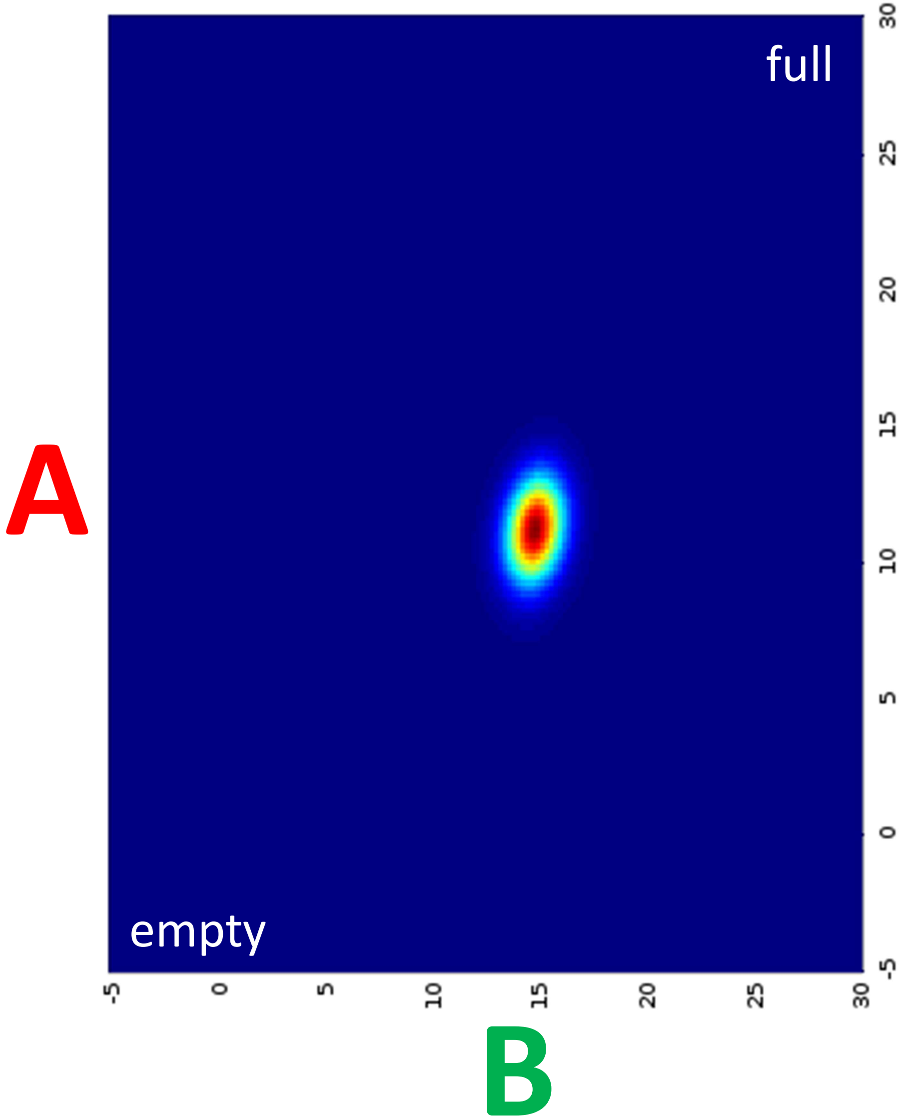


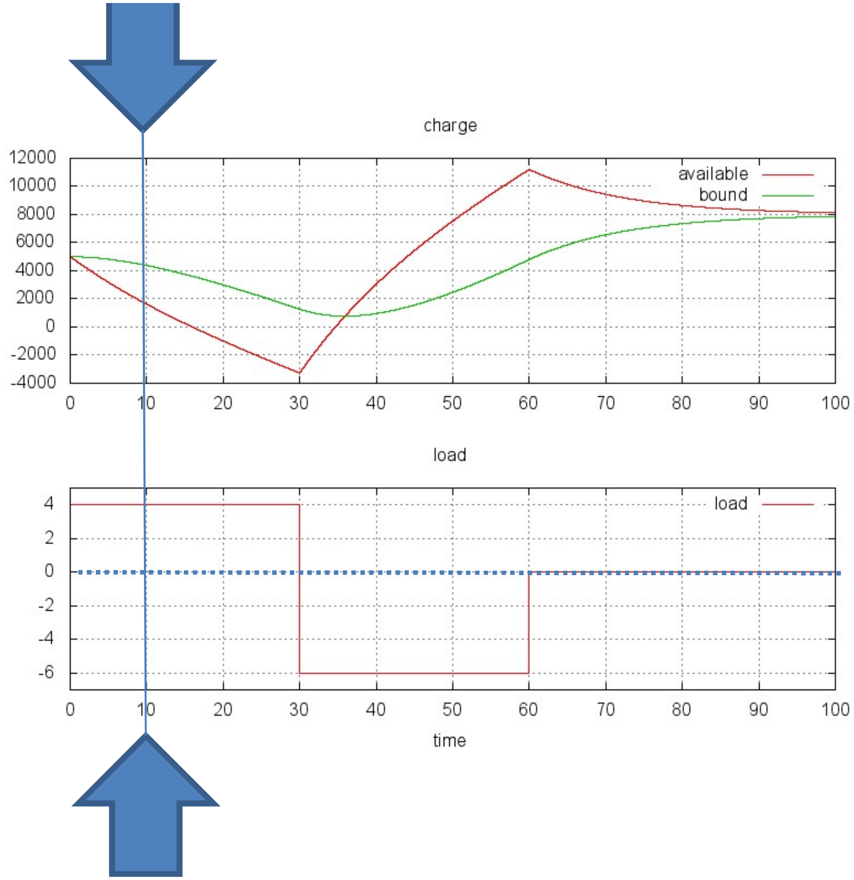


Battery Kinetics

$$\dot{a}(t) = -I + p\left(\frac{b(t)}{1-c} - \frac{a(t)}{c}\right)$$

$$\dot{b}(t) = p\left(\frac{a(t)}{c} - \frac{b(t)}{1-c}\right)$$

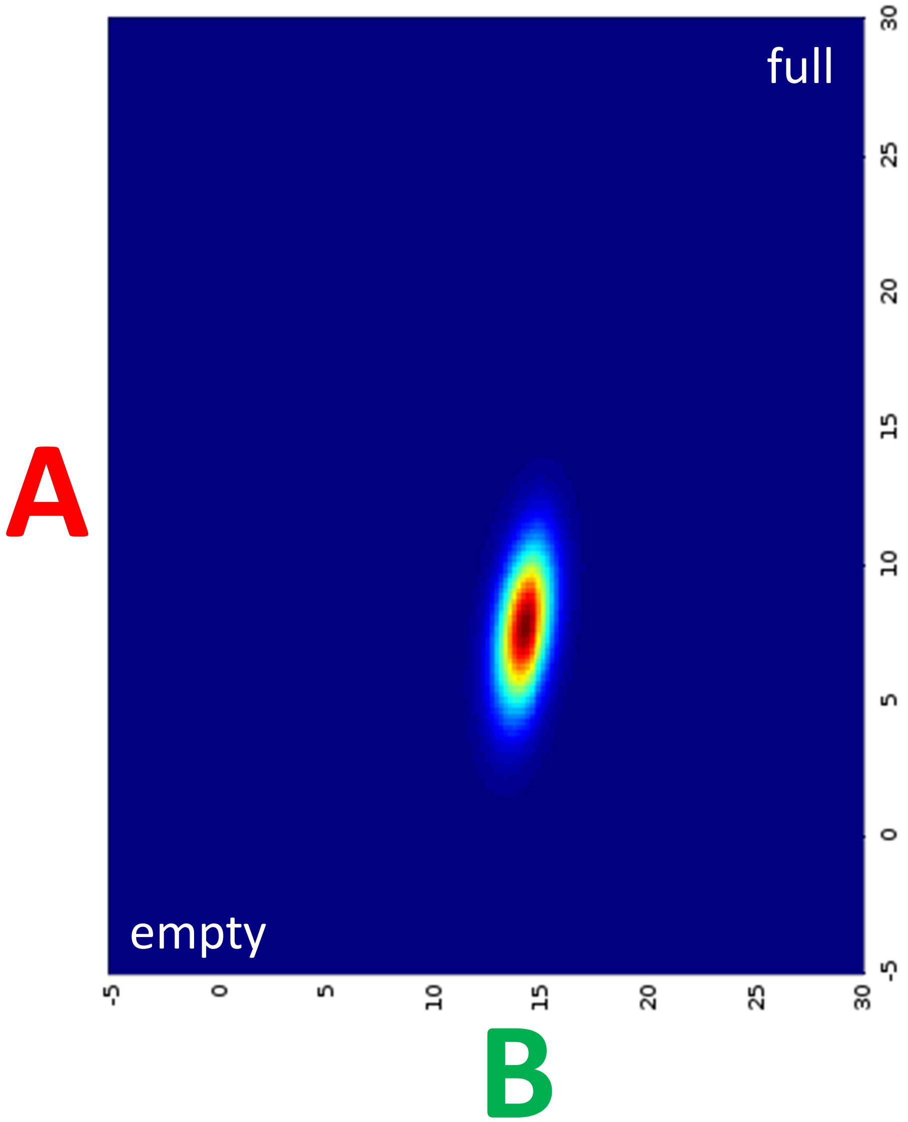


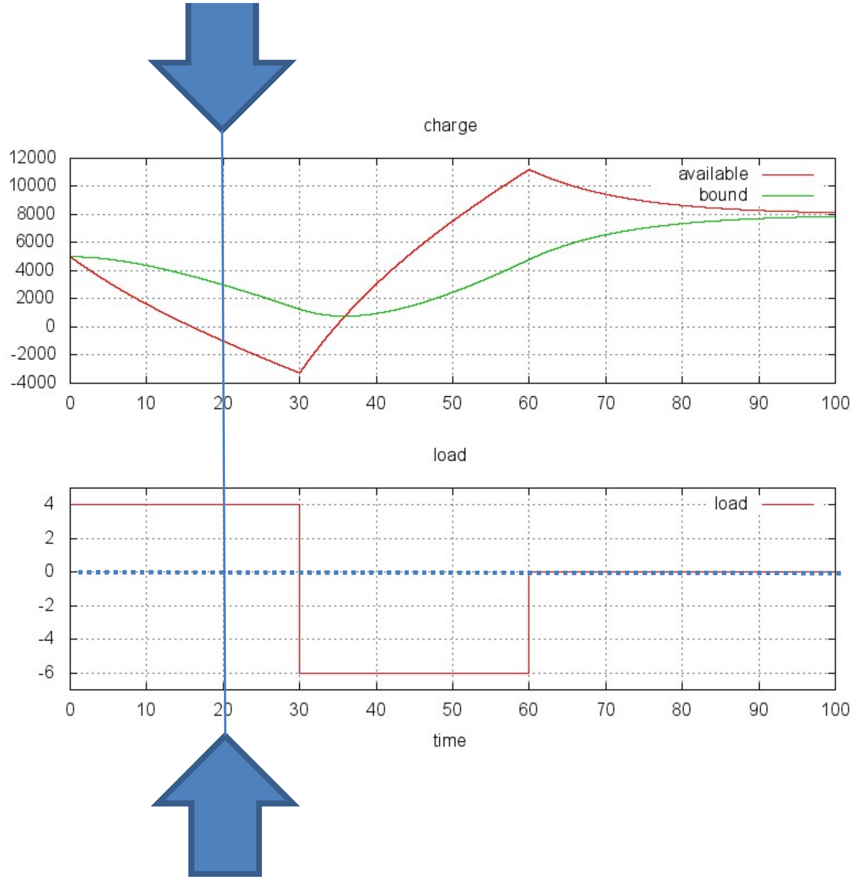


Battery Kinetics

$$\dot{a}(t) = -I + p\left(\frac{b(t)}{1-c} - \frac{a(t)}{c}\right)$$

$$\dot{b}(t) = p\left(\frac{a(t)}{c} - \frac{b(t)}{1-c}\right)$$

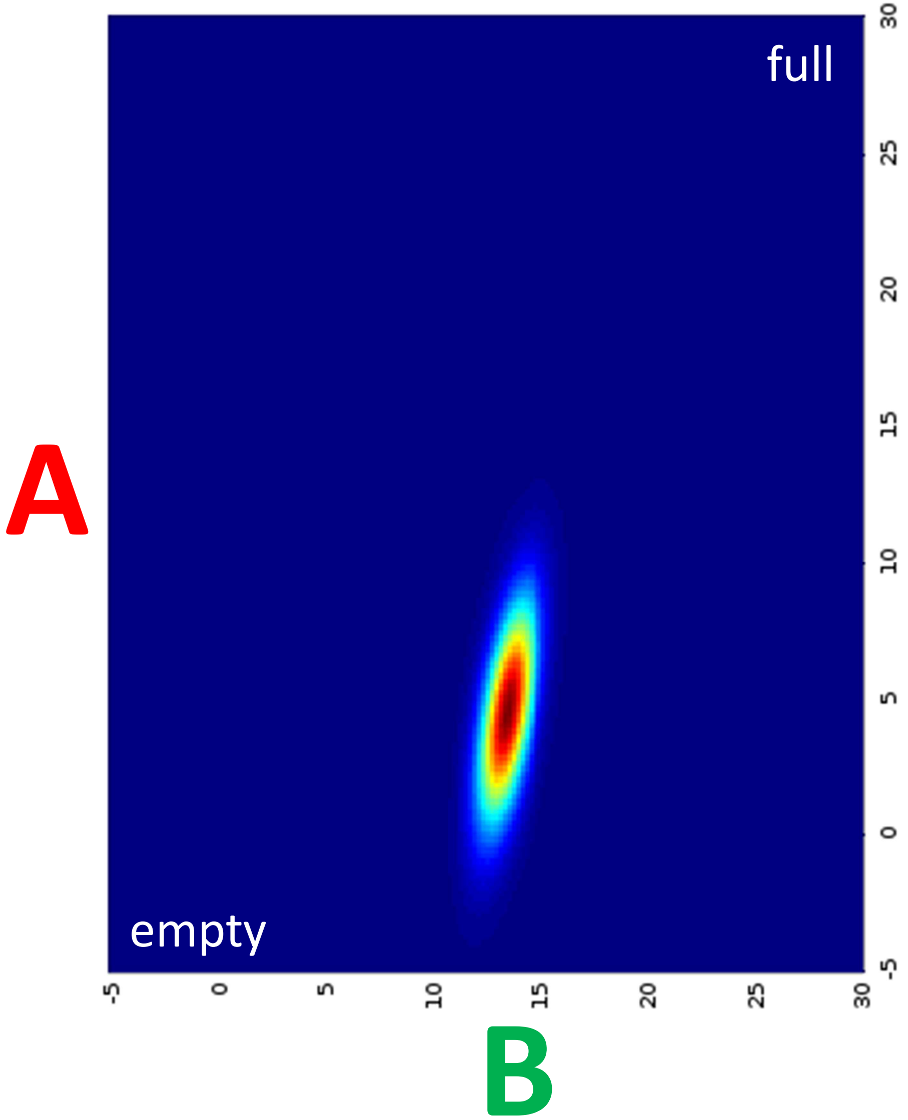


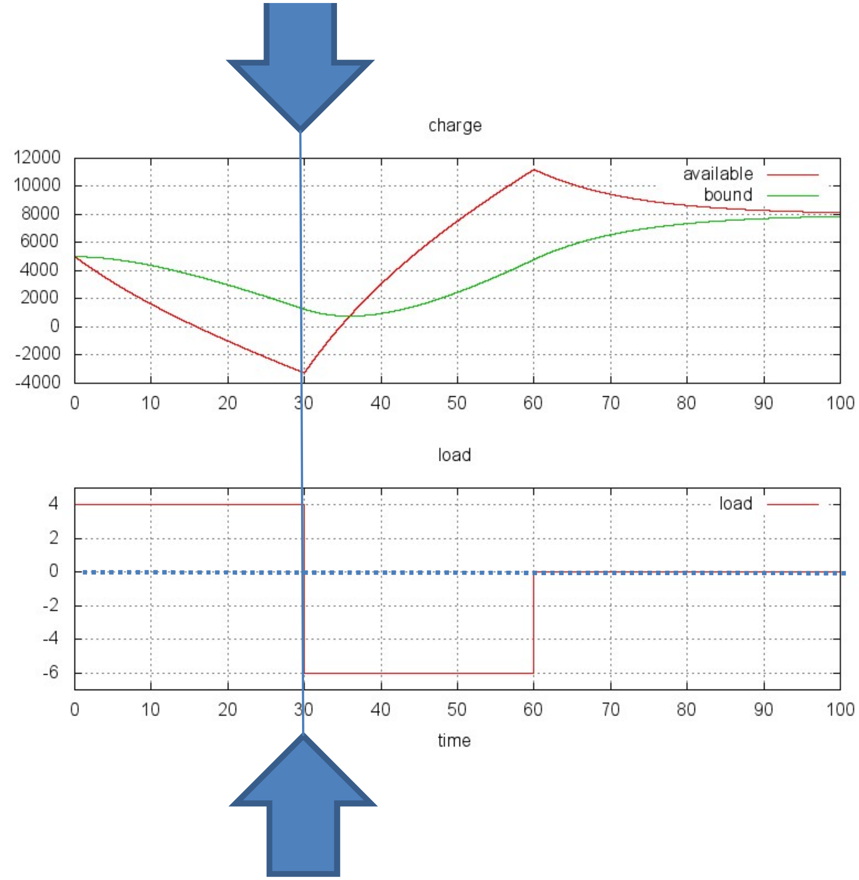


Battery Kinetics

$$\dot{a}(t) = -I + p\left(\frac{b(t)}{1-c} - \frac{a(t)}{c}\right)$$

$$\dot{b}(t) = p\left(\frac{a(t)}{c} - \frac{b(t)}{1-c}\right)$$

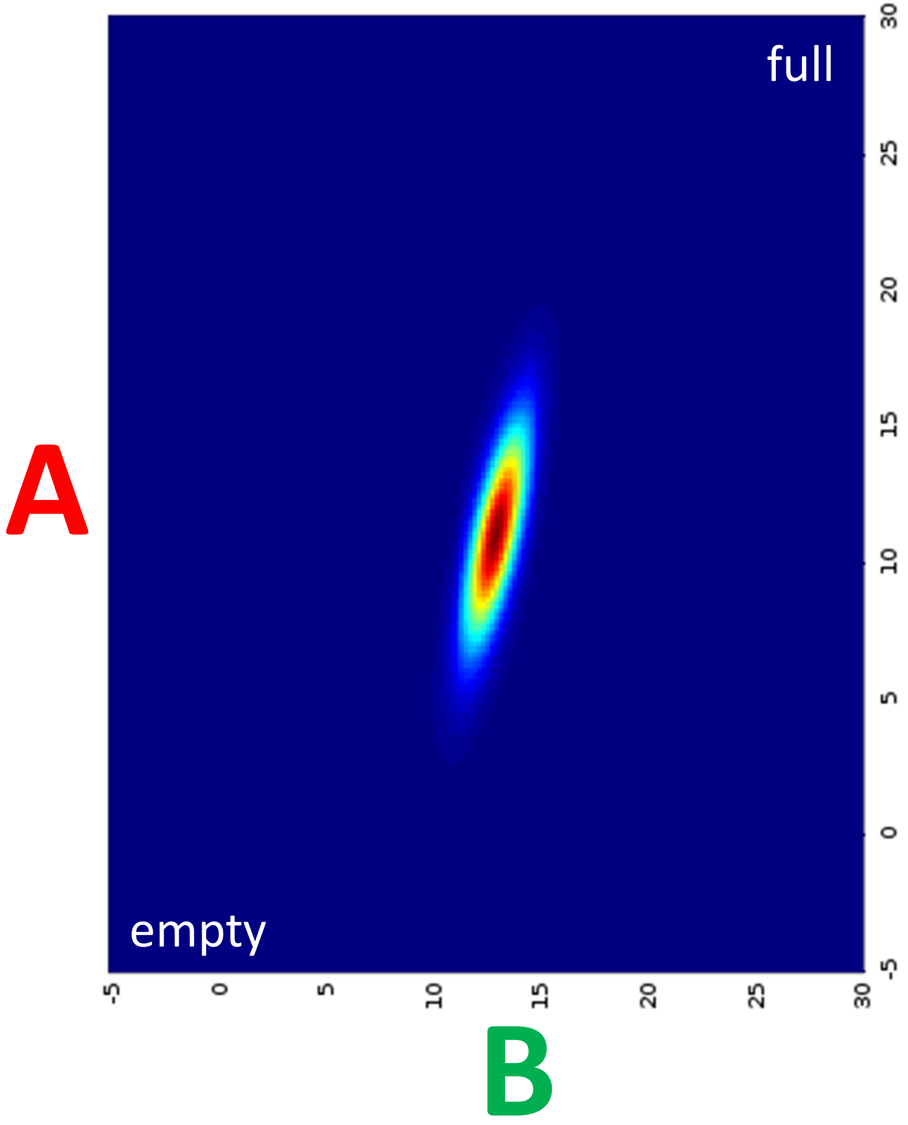


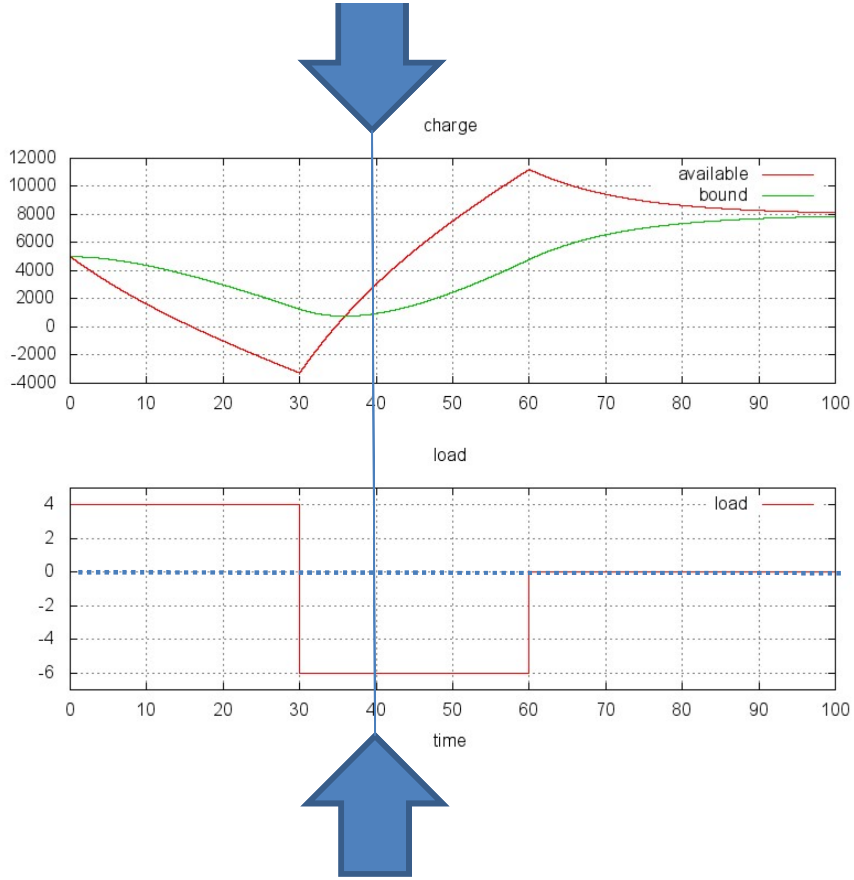


Battery Kinetics

$$\dot{a}(t) = -I + p\left(\frac{b(t)}{1-c} - \frac{a(t)}{c}\right)$$

$$\dot{b}(t) = p\left(\frac{a(t)}{c} - \frac{b(t)}{1-c}\right)$$

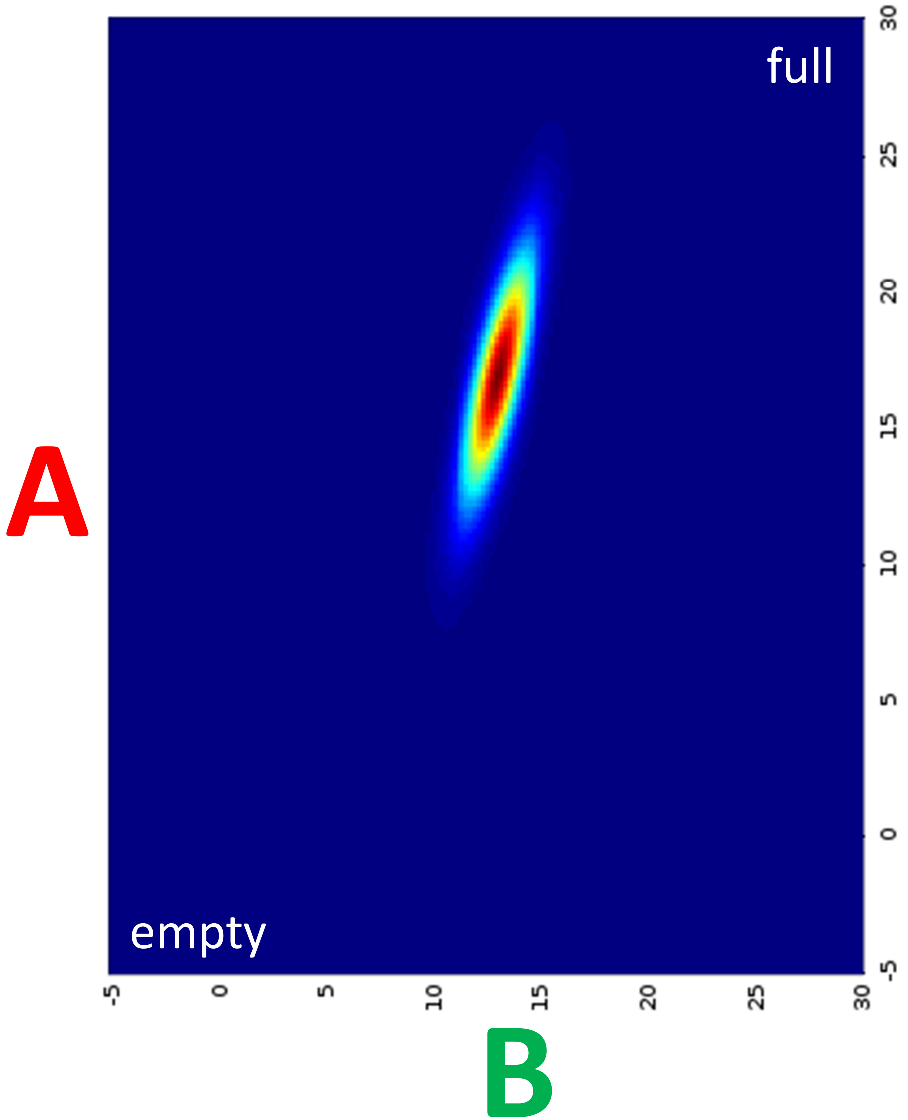


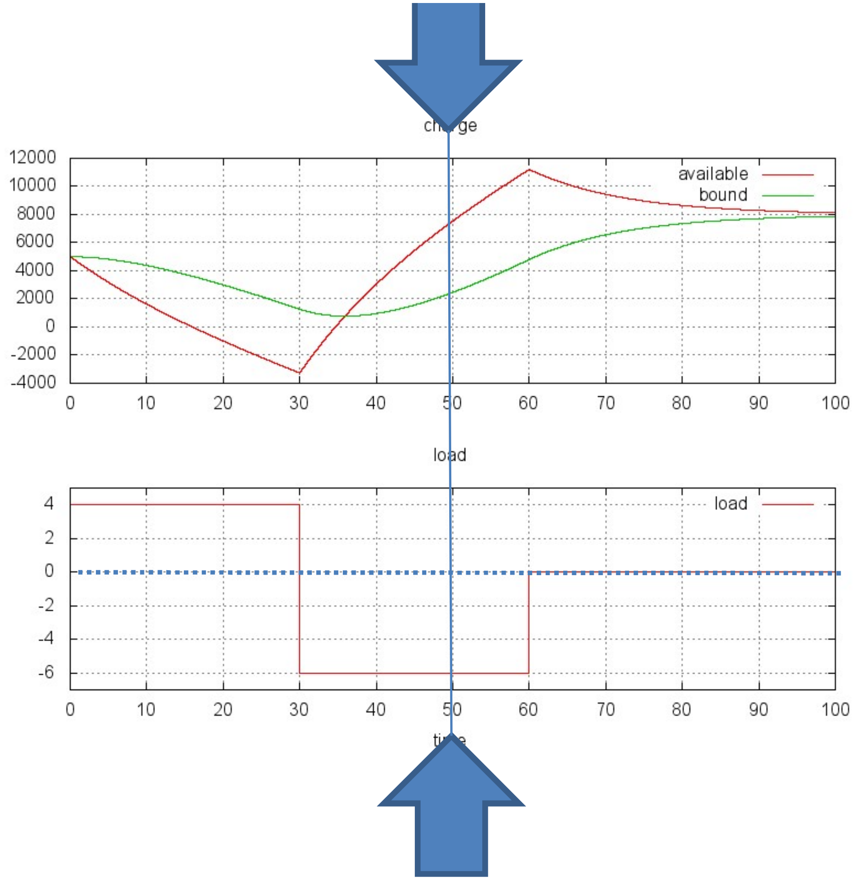


Battery Kinetics

$$\dot{a}(t) = -I + p\left(\frac{b(t)}{1-c} - \frac{a(t)}{c}\right)$$

$$\dot{b}(t) = p\left(\frac{a(t)}{c} - \frac{b(t)}{1-c}\right)$$

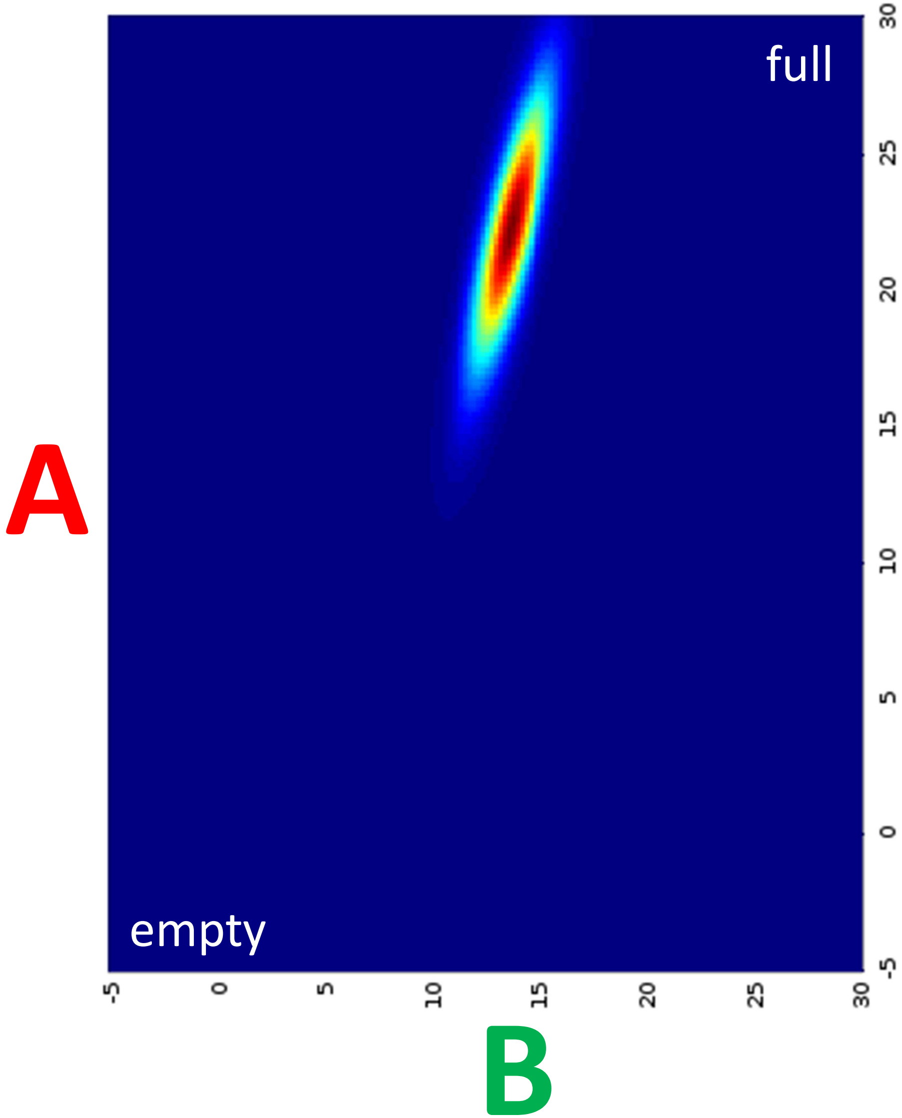


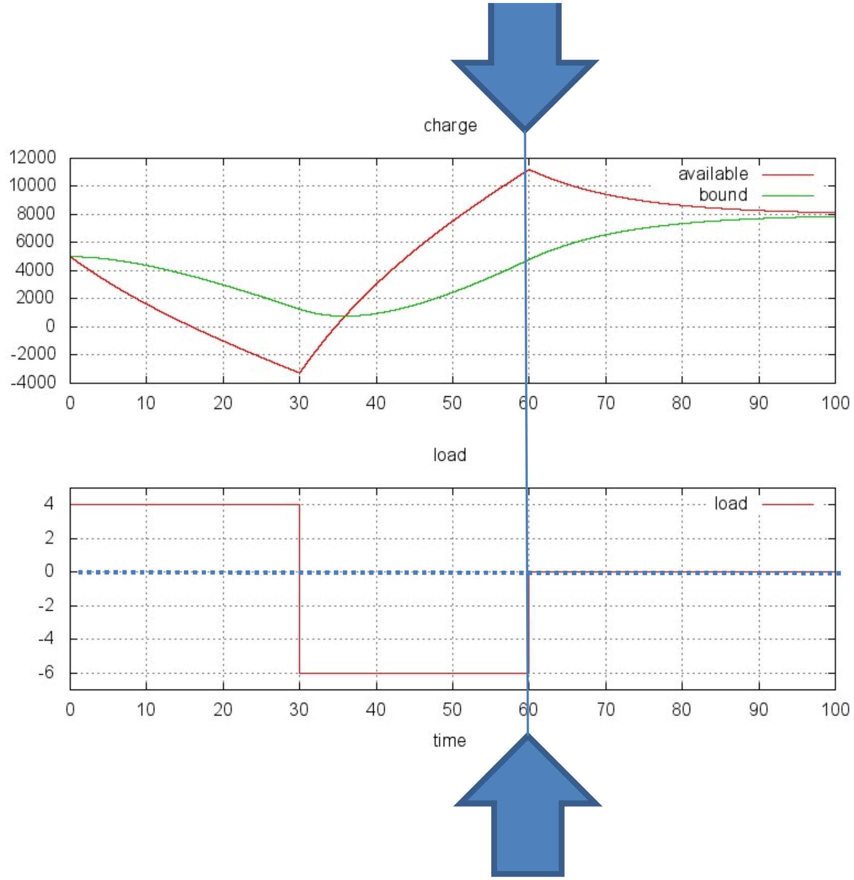


Battery Kinetics

$$\dot{a}(t) = -I + p\left(\frac{b(t)}{1-c} - \frac{a(t)}{c}\right)$$

$$\dot{b}(t) = p\left(\frac{a(t)}{c} - \frac{b(t)}{1-c}\right)$$

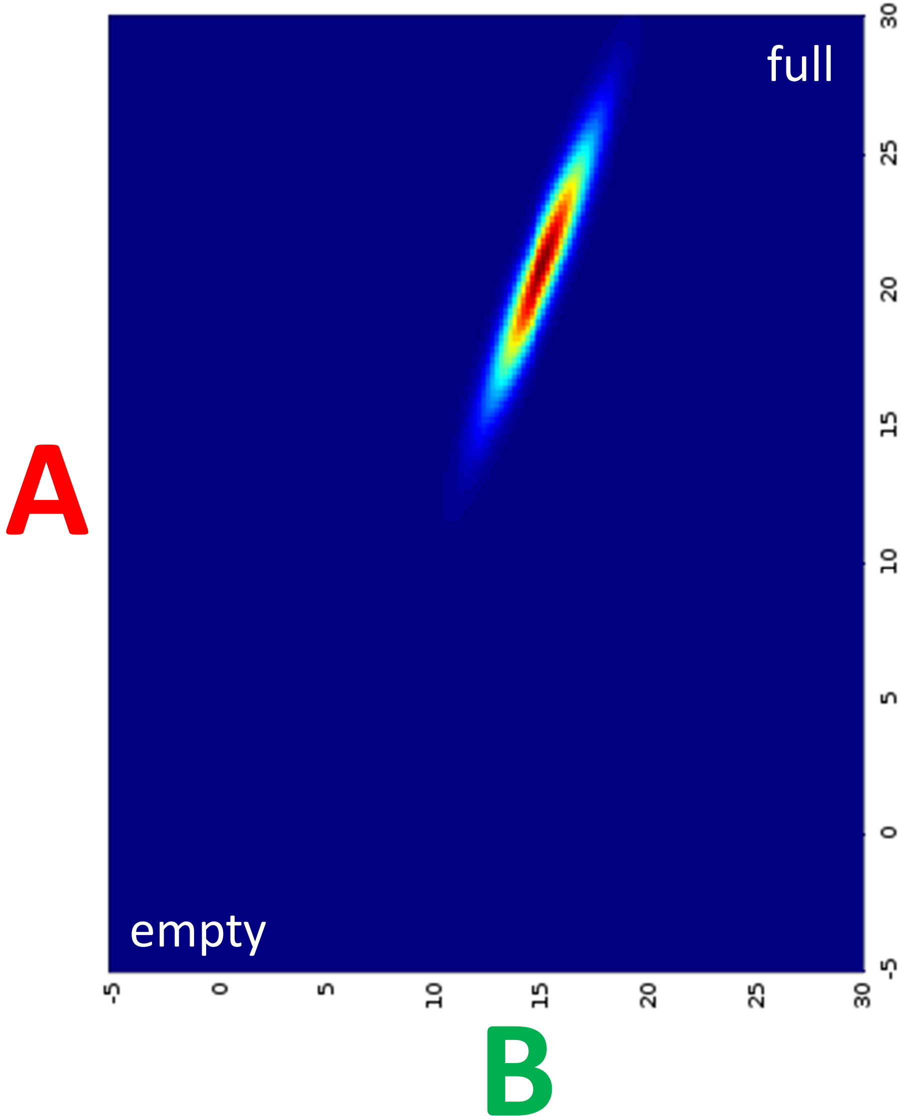


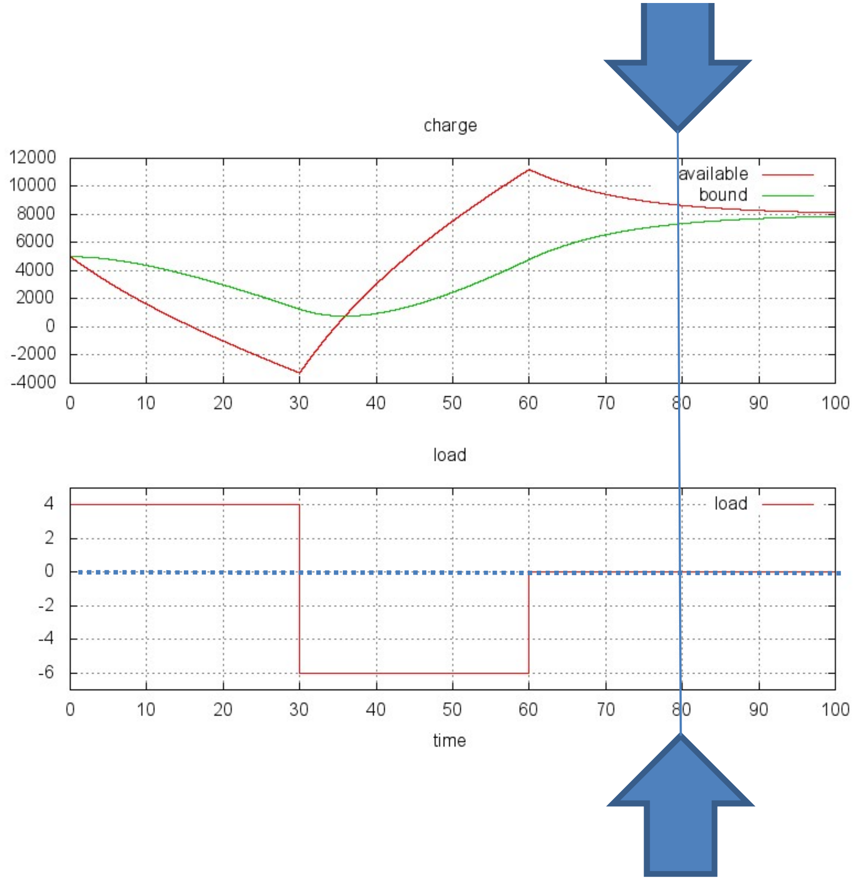


Battery Kinetics

$$\dot{a}(t) = -I + p\left(\frac{b(t)}{1-c} - \frac{a(t)}{c}\right)$$

$$\dot{b}(t) = p\left(\frac{a(t)}{c} - \frac{b(t)}{1-c}\right)$$

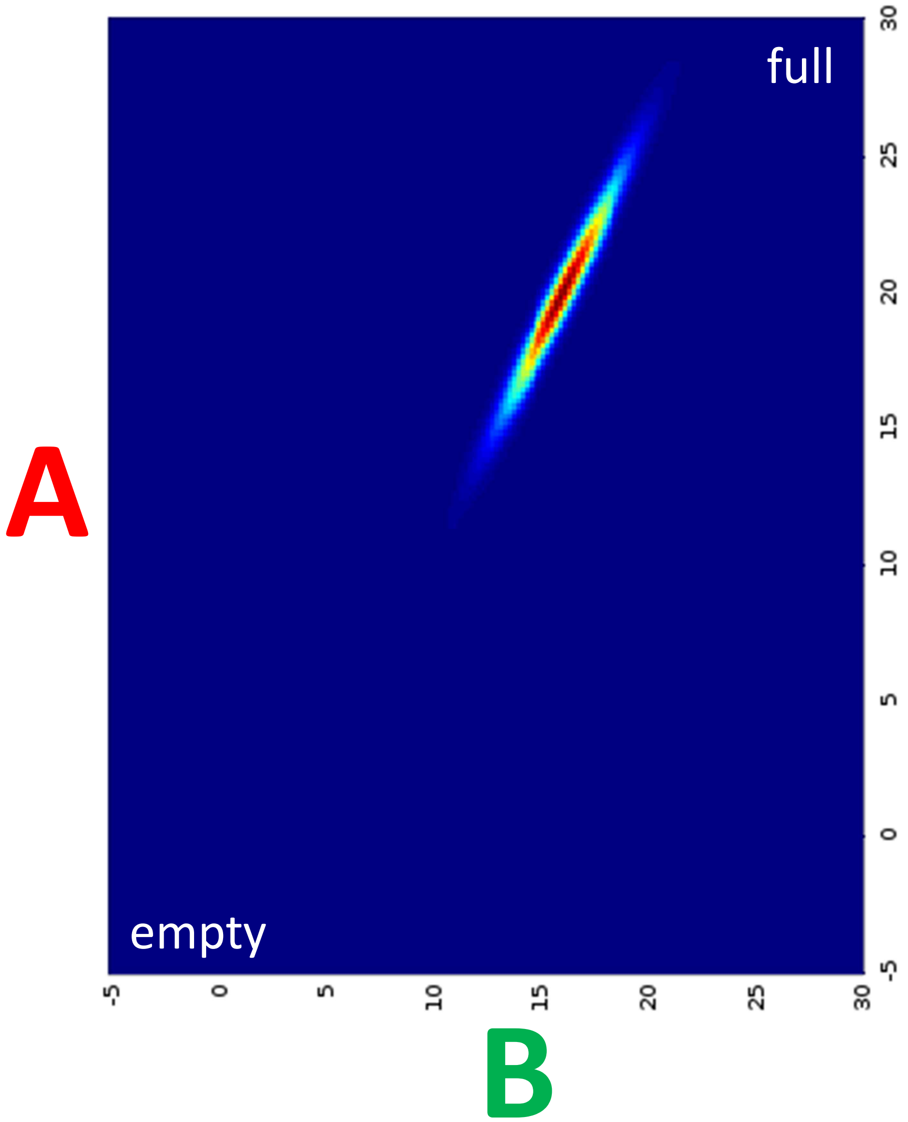


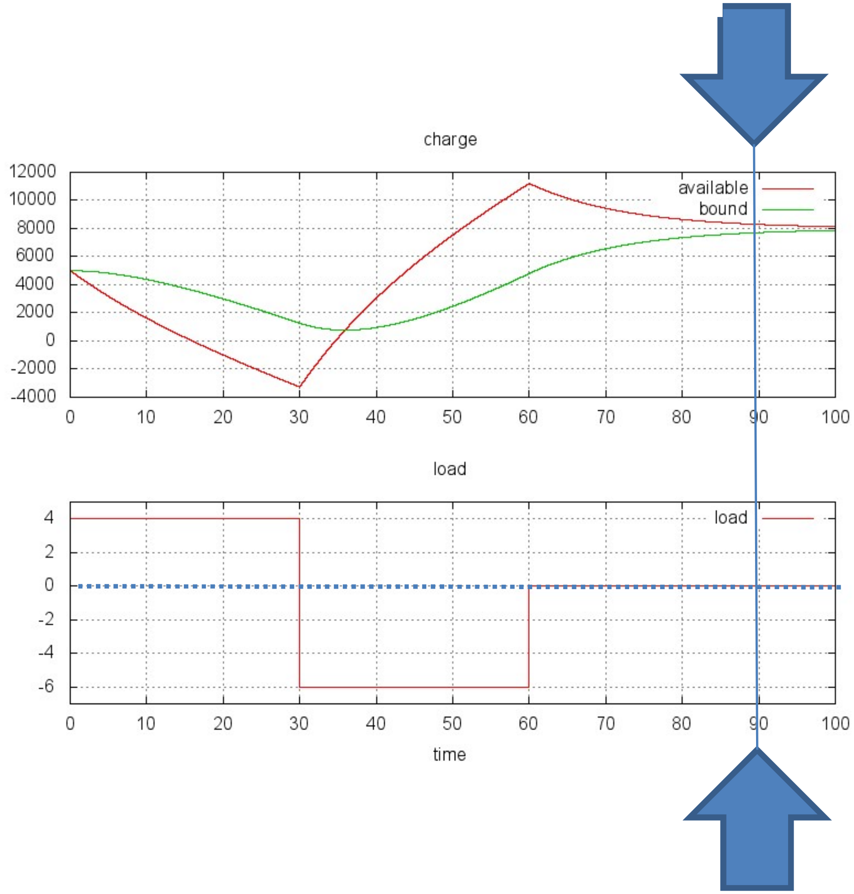


Battery Kinetics

$$\dot{a}(t) = -I + p\left(\frac{b(t)}{1-c} - \frac{a(t)}{c}\right)$$

$$\dot{b}(t) = p\left(\frac{a(t)}{c} - \frac{b(t)}{1-c}\right)$$

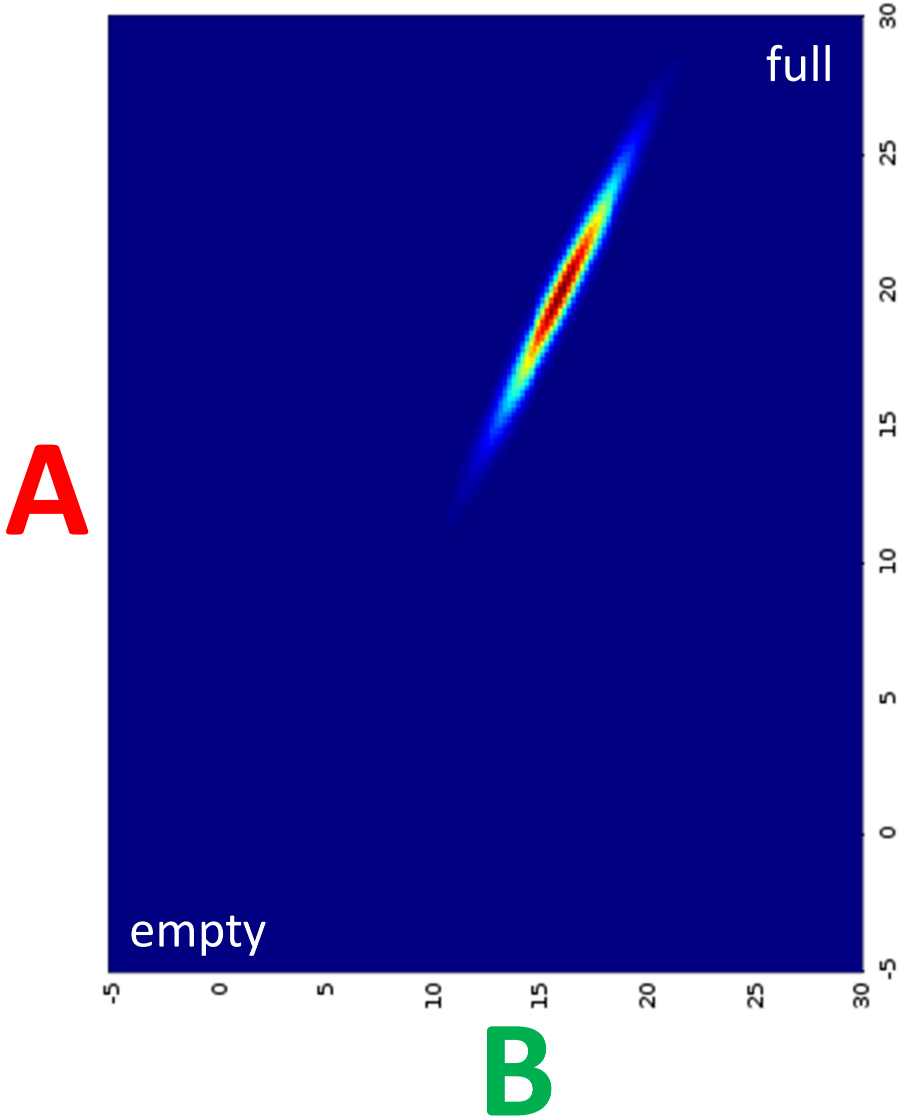


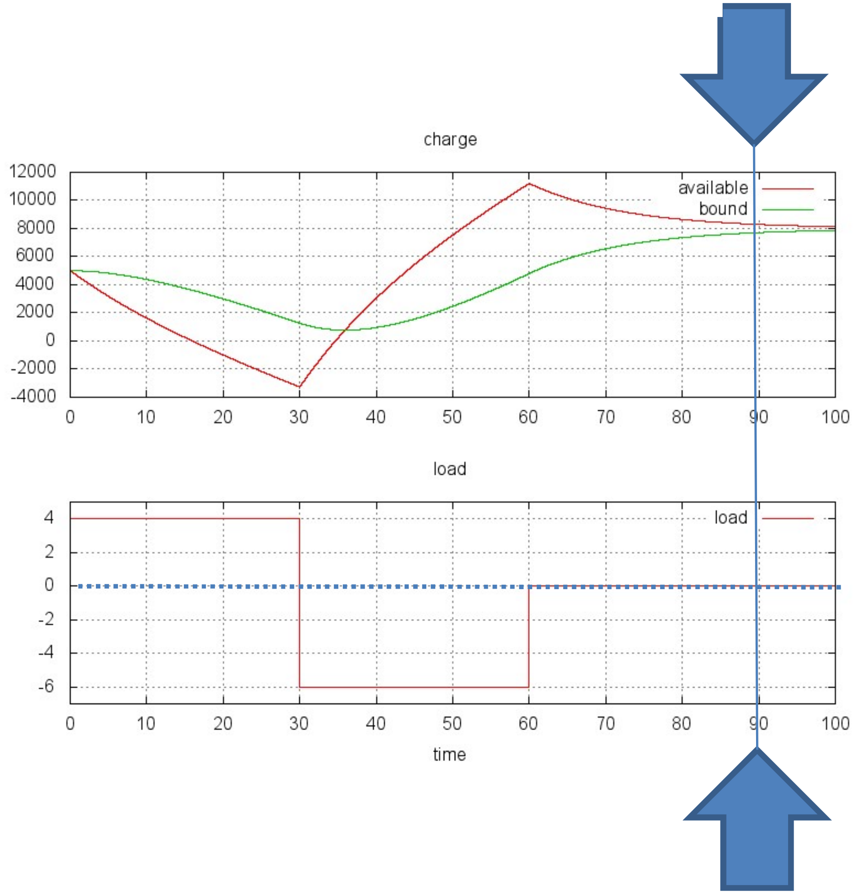


Battery Kinetics

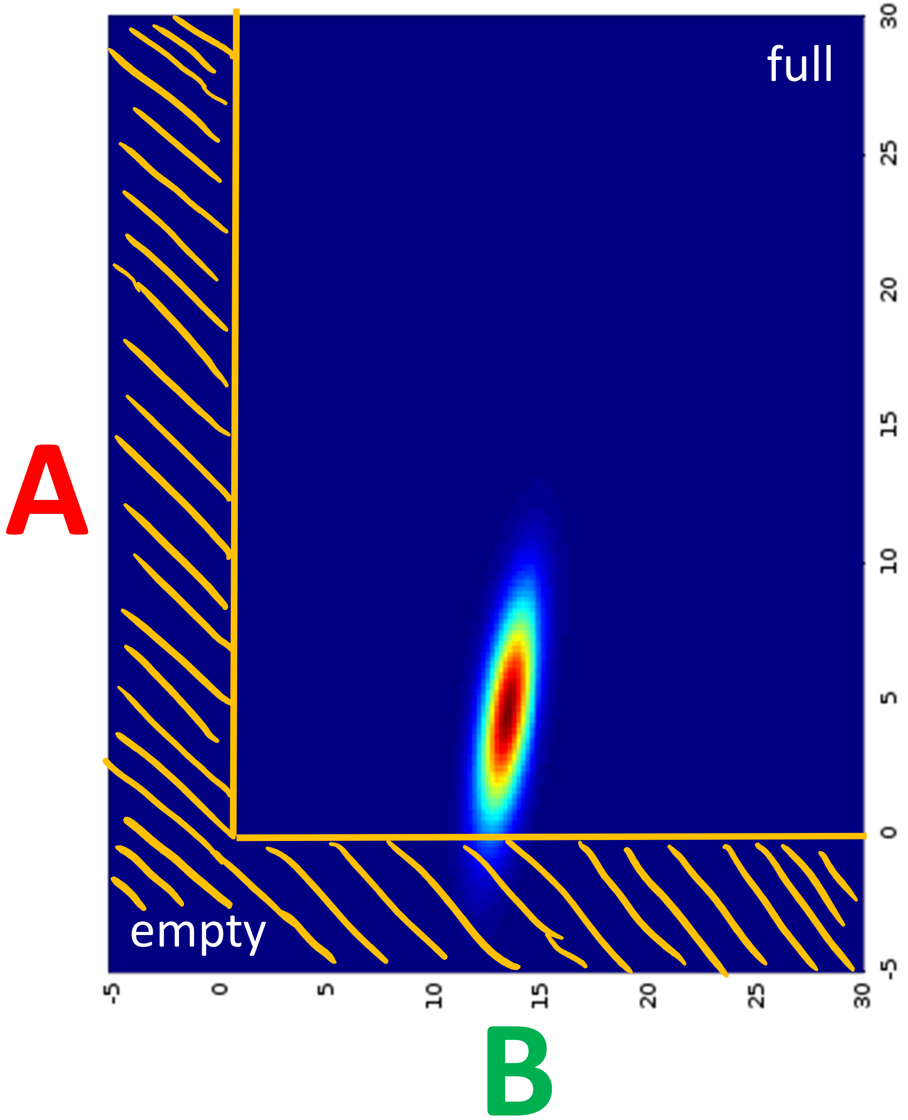
$$\dot{a}(t) = -I + p\left(\frac{b(t)}{1-c} - \frac{a(t)}{c}\right)$$

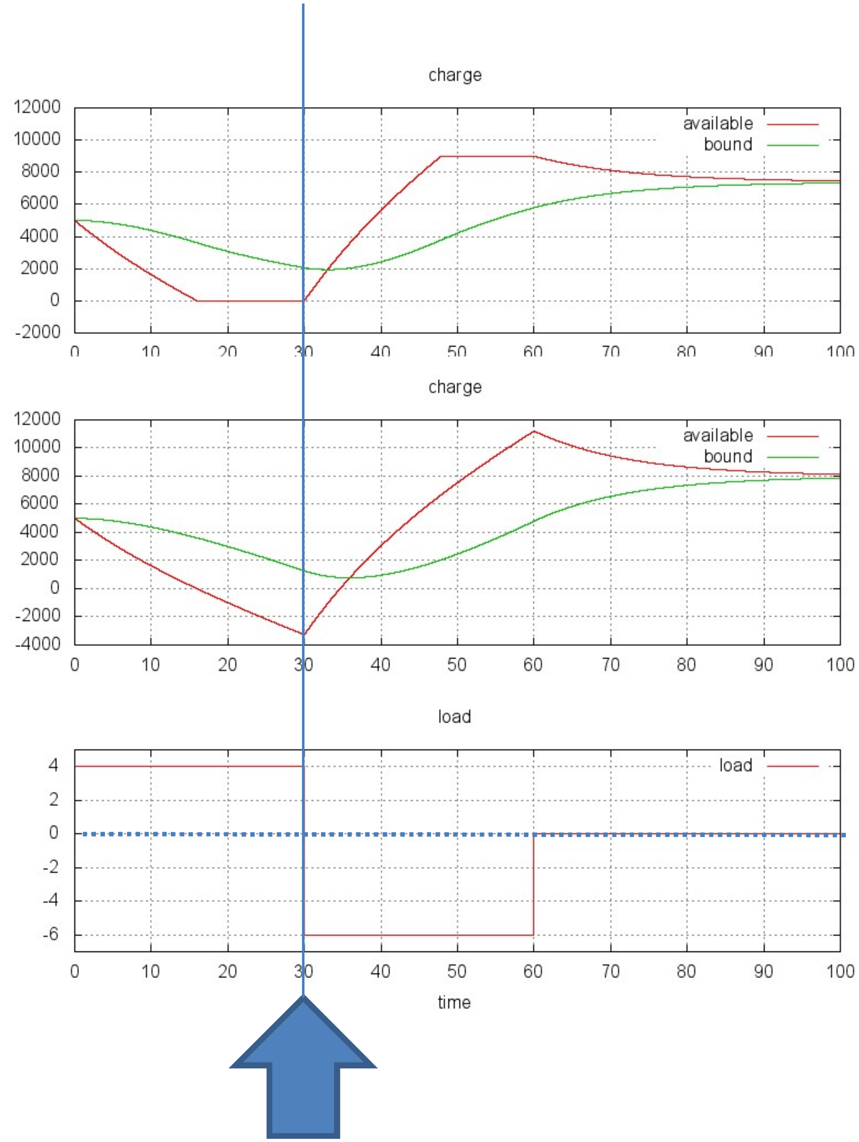
$$\dot{b}(t) = p\left(\frac{a(t)}{c} - \frac{b(t)}{1-c}\right)$$





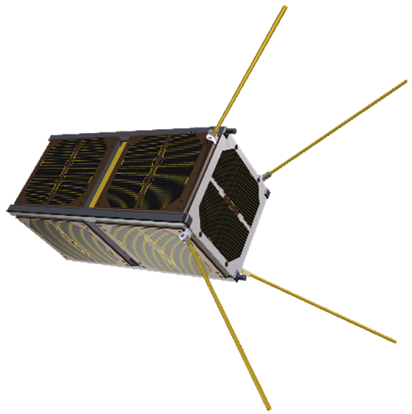
Battery Kinetics

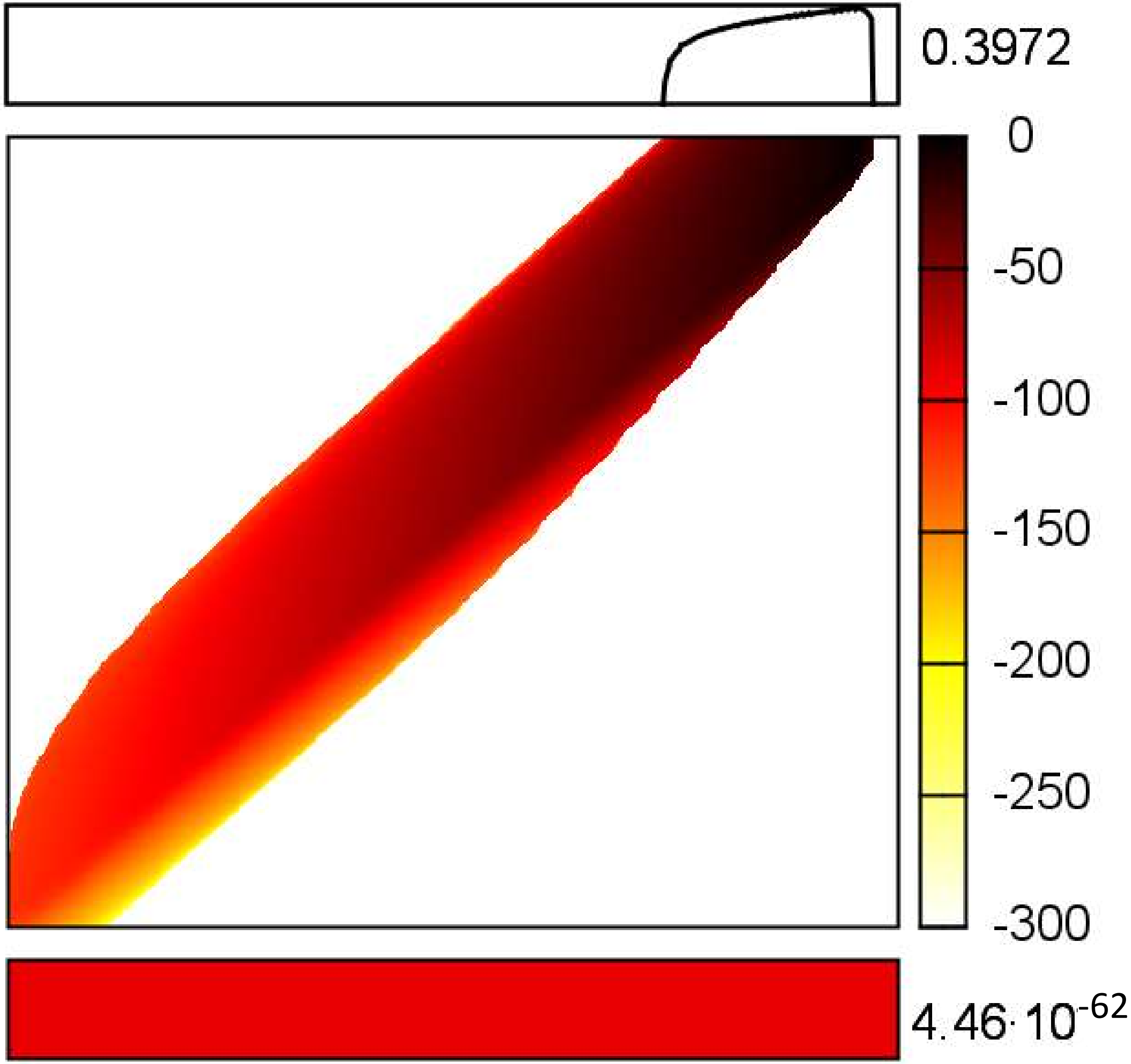




Concretely.

Will the battery survive a one-year mission?

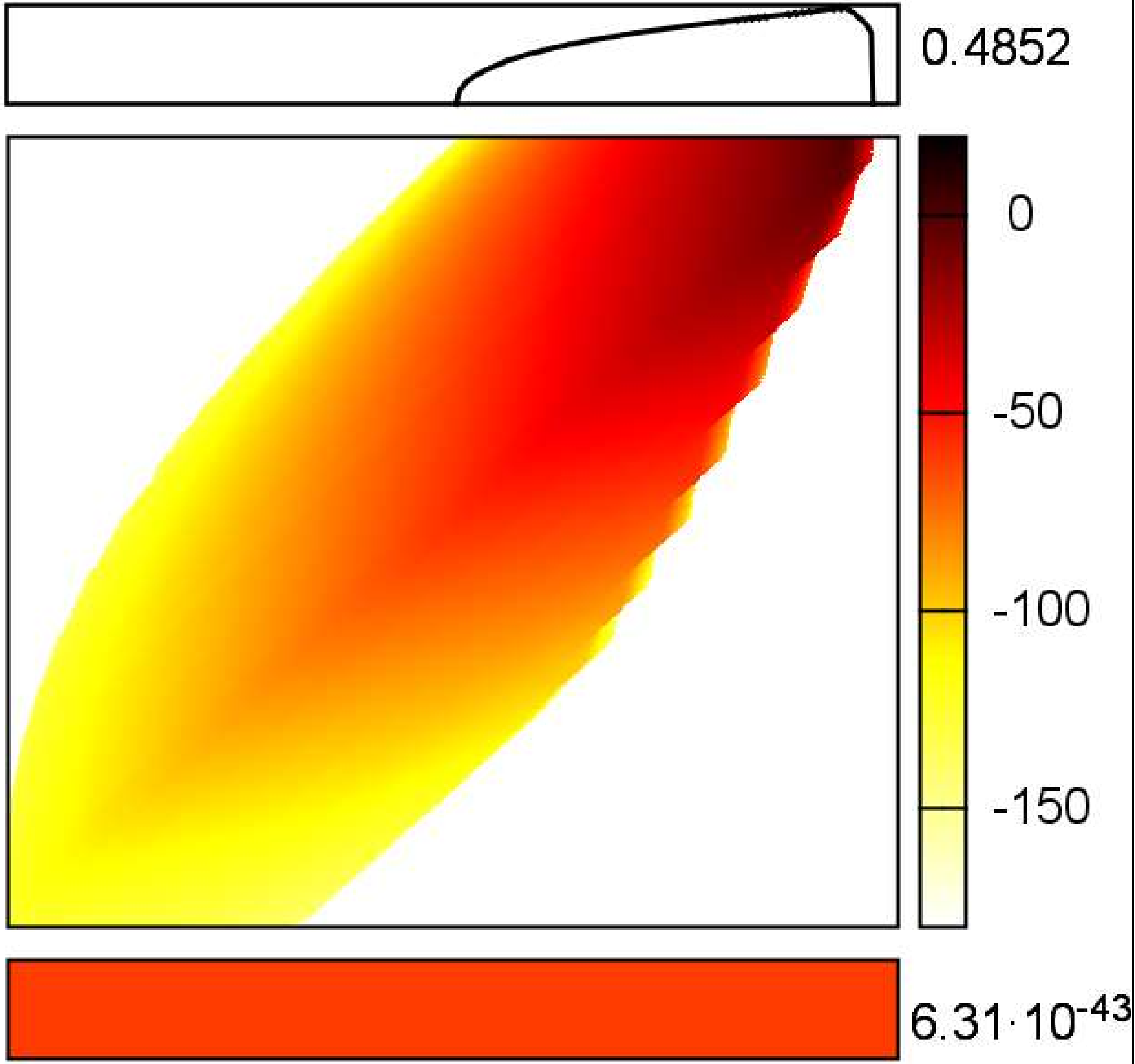


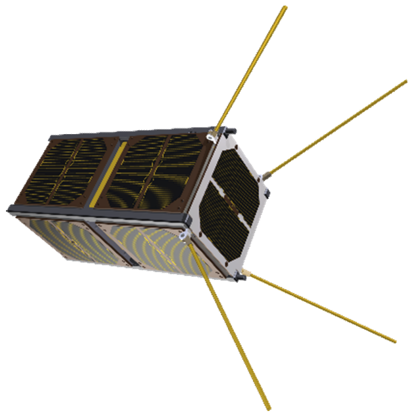


with 5000 mAh

Concretely.

Will the battery survive a one-year mission?



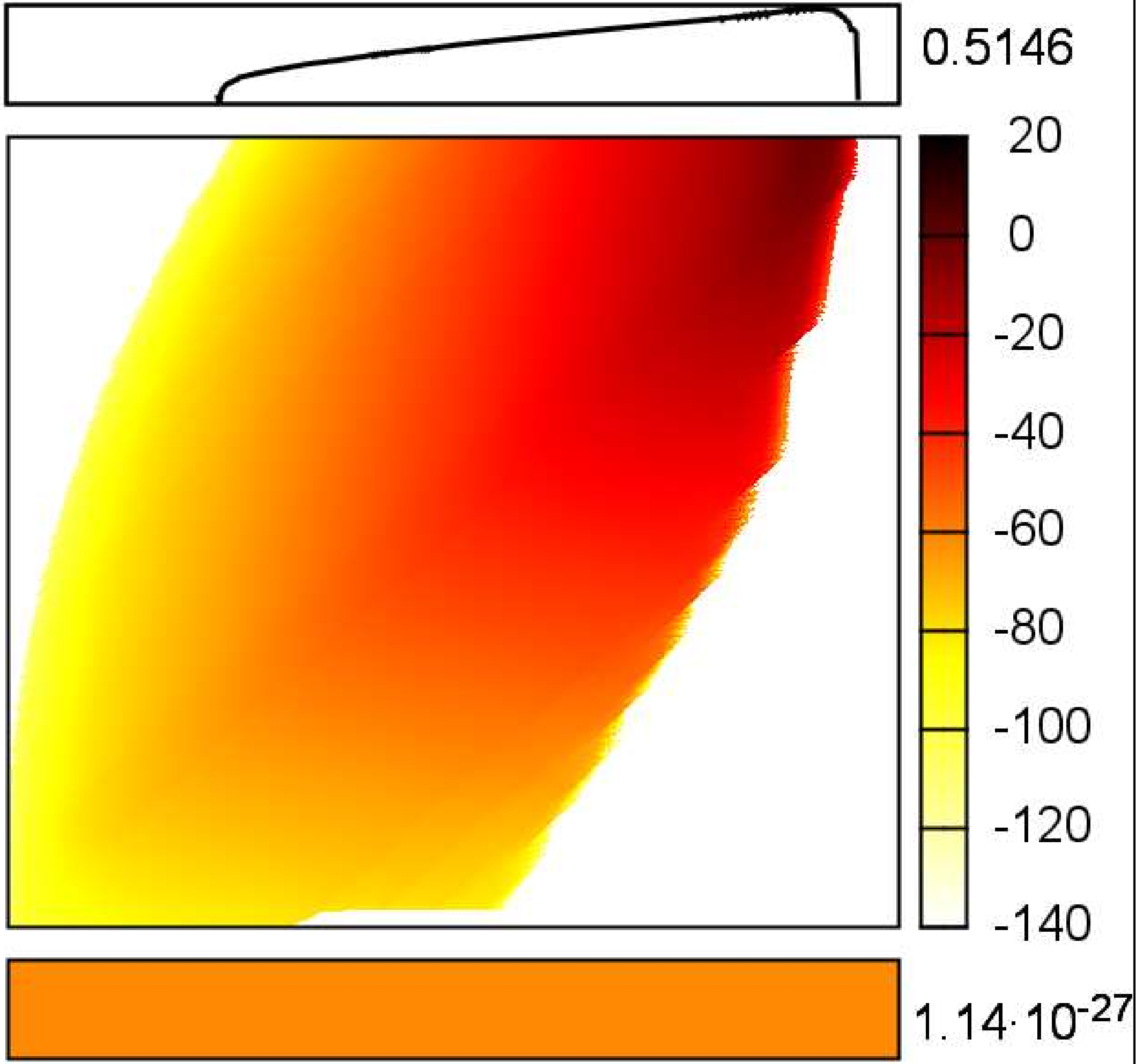


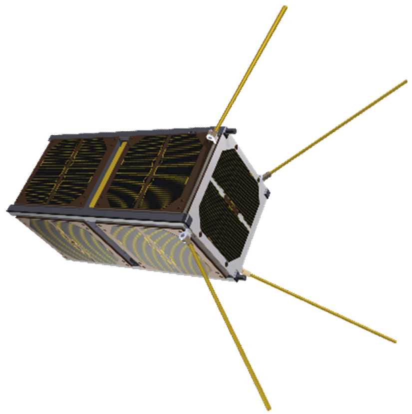
With half the capacity?

2500 mAh

Concretely.

Will the battery survive a one-year mission?



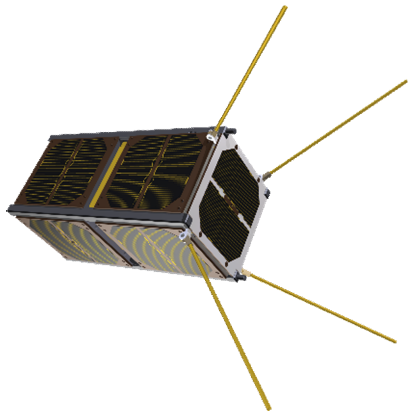


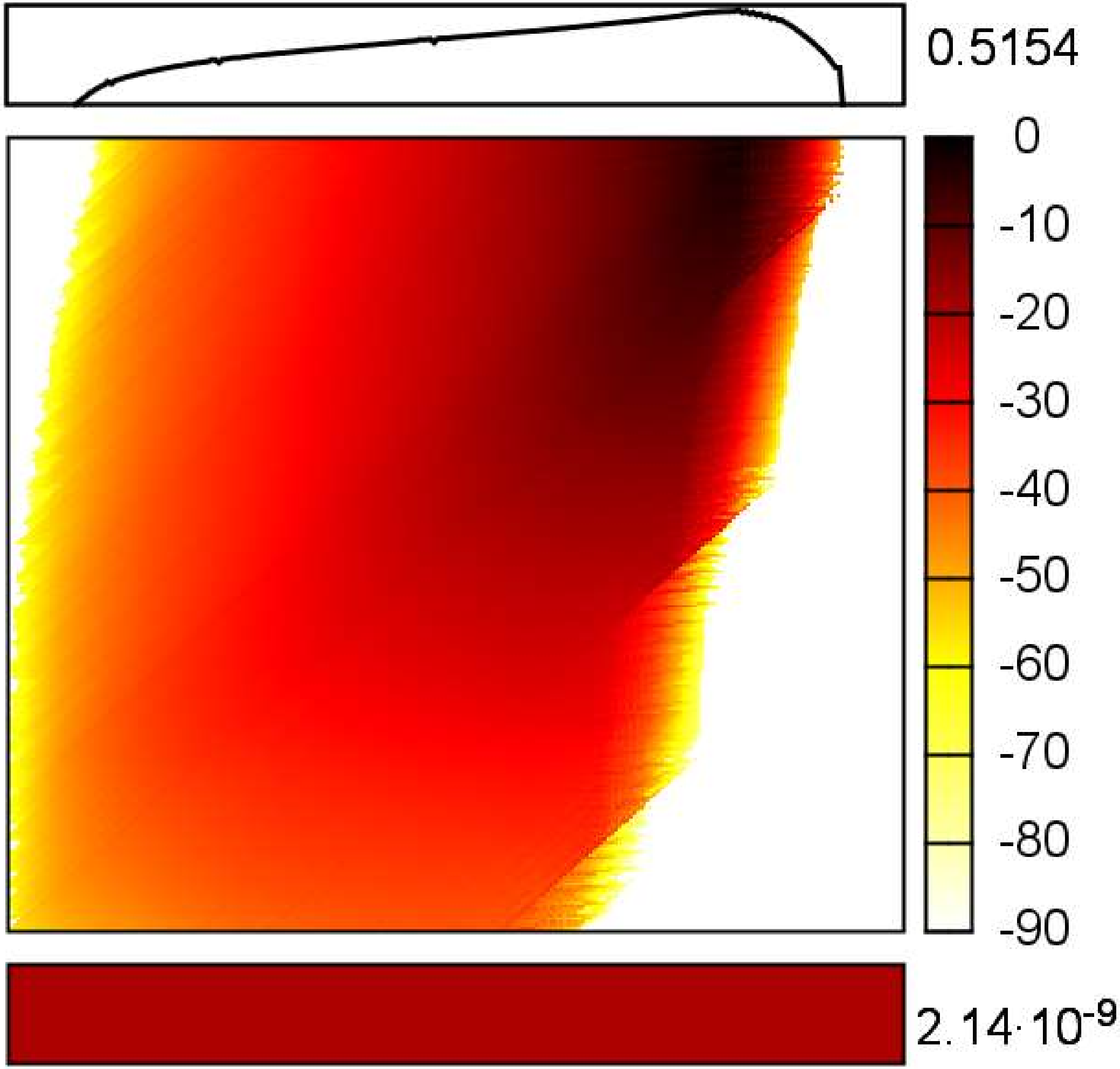
With a quarter of the capacity?

1250 mAh

Concretely.

Will the battery survive a one-year mission?



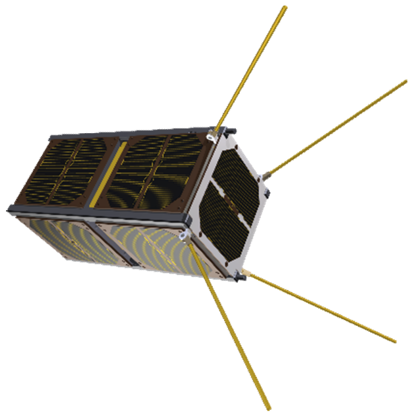


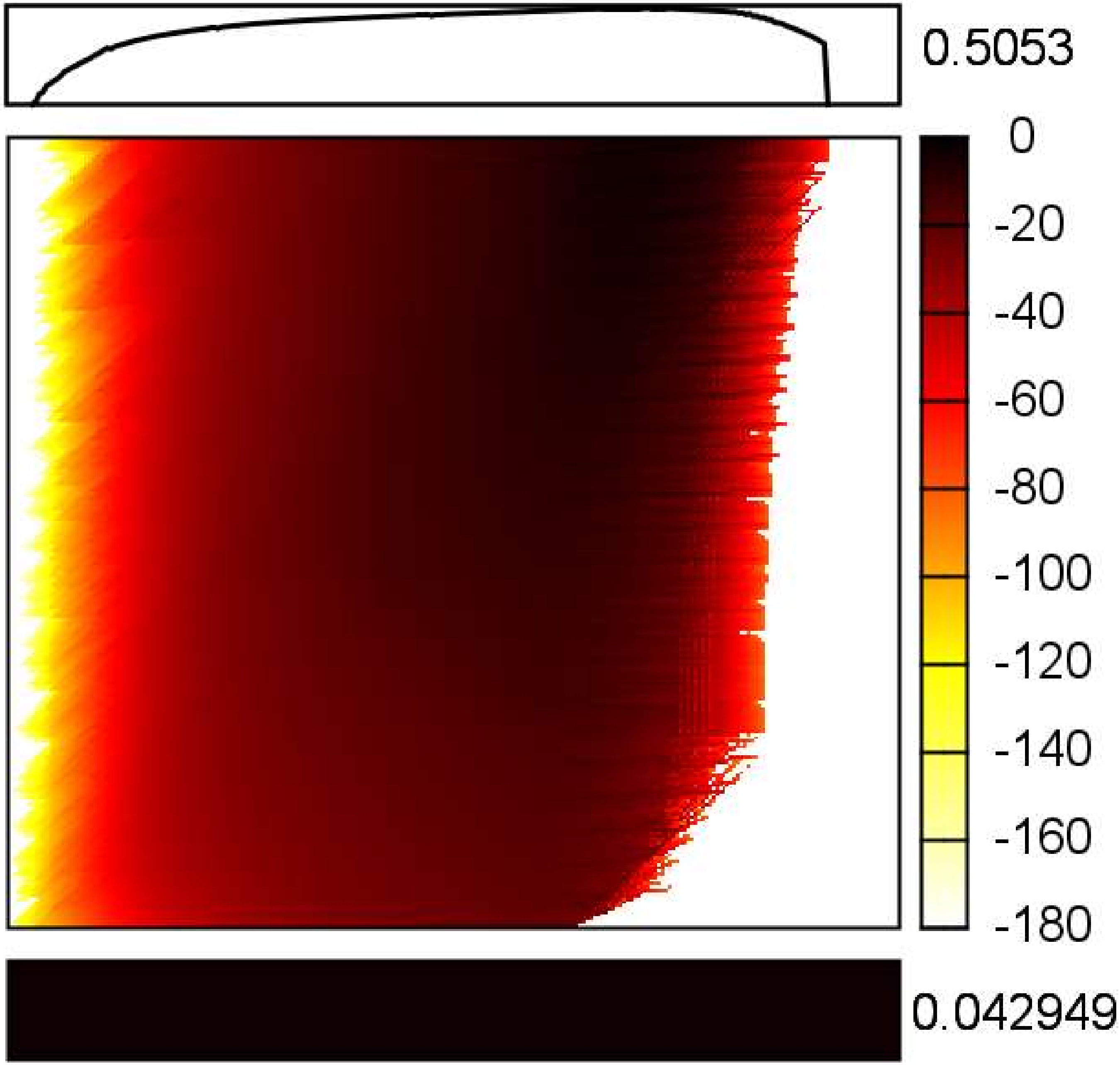
With an eighth of the capacity ?

625 mAh

Concretely.

Will the battery survive a one-year mission?





With a sixteenth of the capacity ?

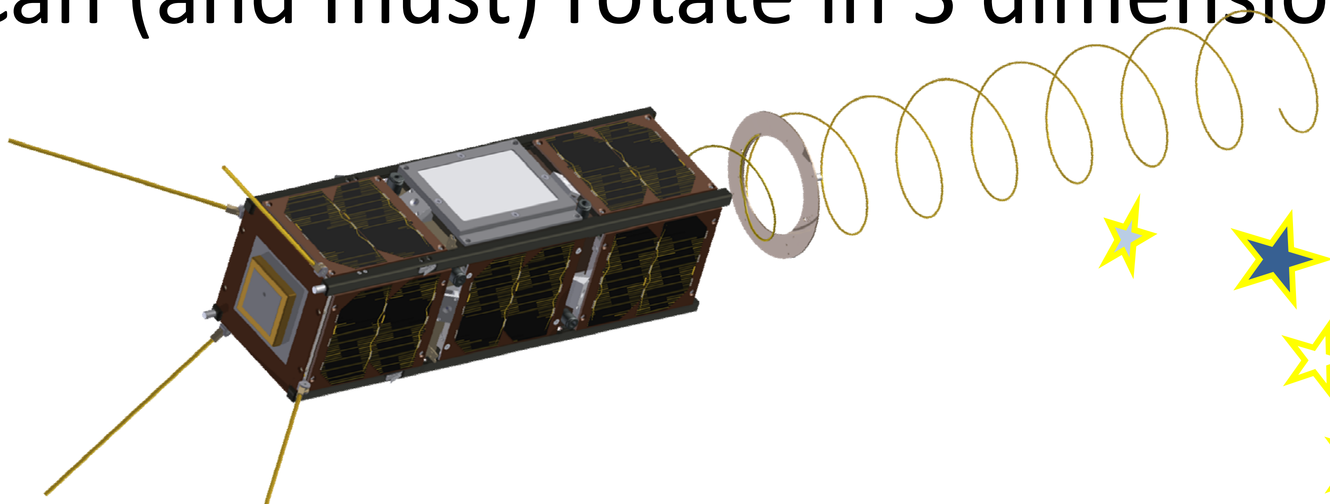
312.5 mAh

GOMX-2

- 2U CubeSat (2 liter)
- Shipped in October 2014 with Cygnus CRS-3 towards ISS
- Payloads:
  - Optical communication experiments from NUS
  - Highspeed UHF and SDR receiver
- Shipping failed after liftoff
- Satellite was recovered from wreckage and returned to GomSpace

GOMX-3

- 3U CubeSat (3 liter)
- Launched from ISS in October 2015
- Payloads:
  - L-band communication to geostationary satellit
  - X-band transmitter for CNES
  - Highspeed UHF and SDR receiver
- Can (and must) rotate in 3 dimensions



GOMSPACE GOMX-4

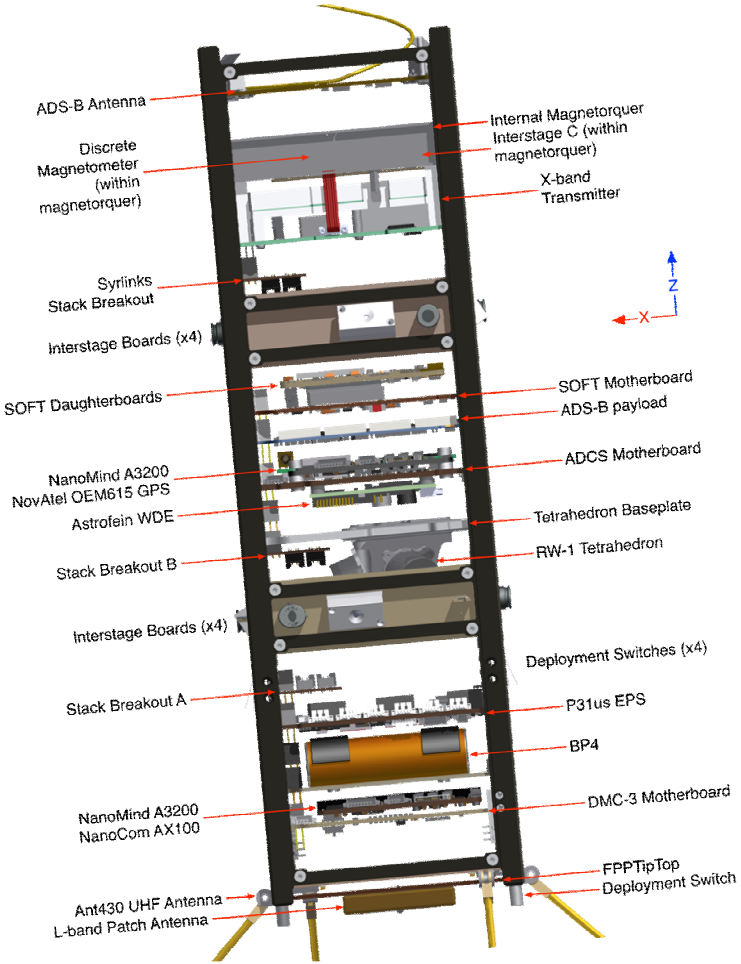
- Two 6U CubeSats (6 liter)
- Launch expected in 2016
- Initial design in the making
- Focus on support for flexible payload model

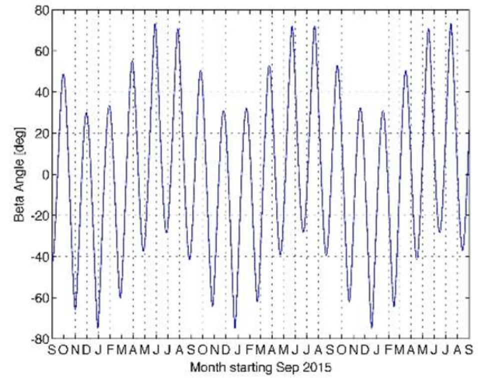
"Satellite-as-a-Service"

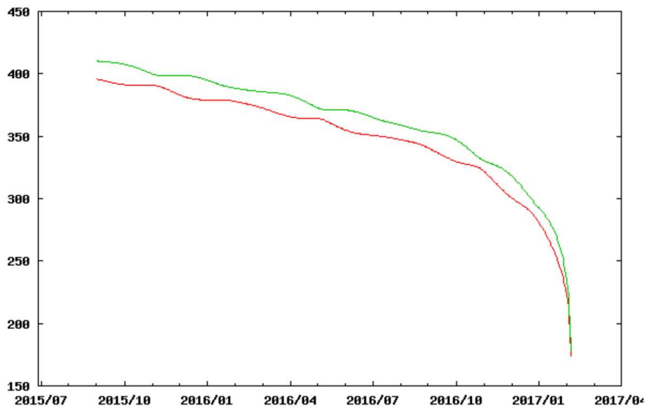
- Needs strong support for dynamic load scheduling
- Battery states are critical

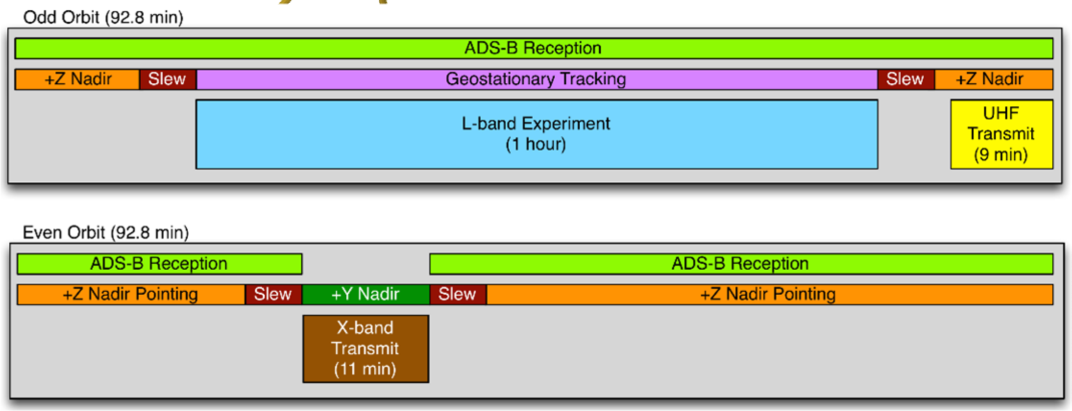
SENSATION

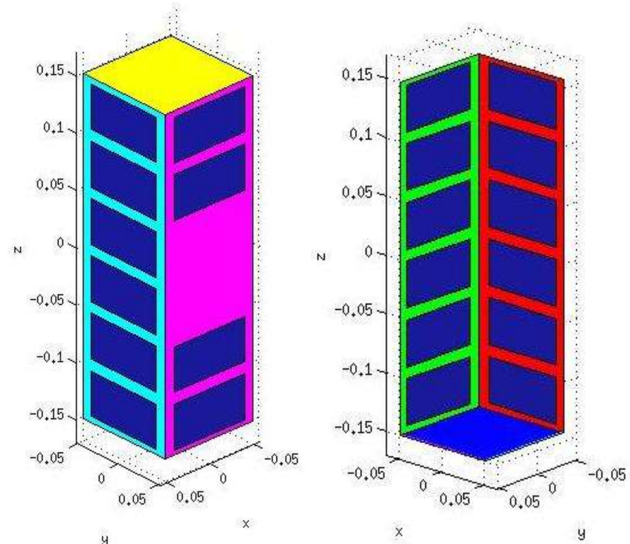
GOMX-3 mission details



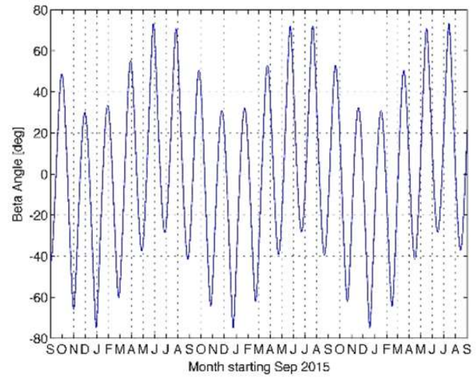




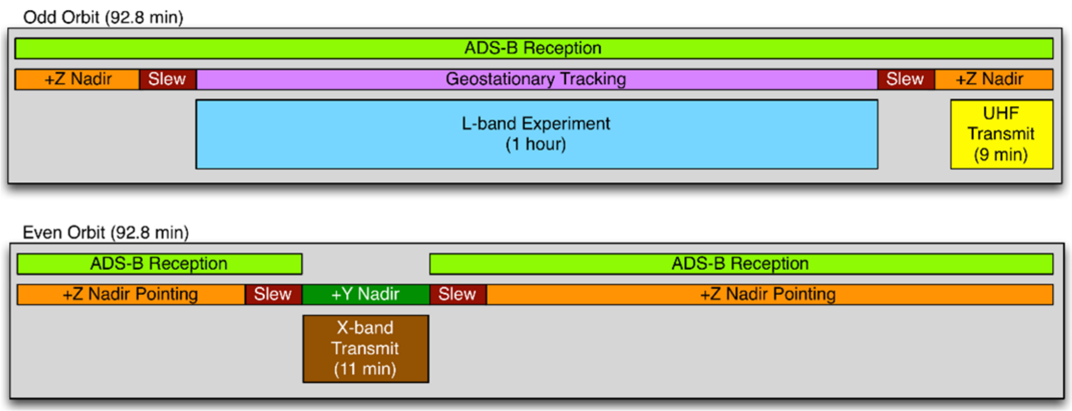




GOMX-3 mission planning



- Very tight power budget
- Needs dynamic and battery aware scheduling
- What we do:
  - Priced Timed Automata modelling
  - Generate optimal schedules for 1 week or day horizon
  - Evaluate schedules on random KiBaM for robustness
  - Send to orbit, observe behaviour, update model



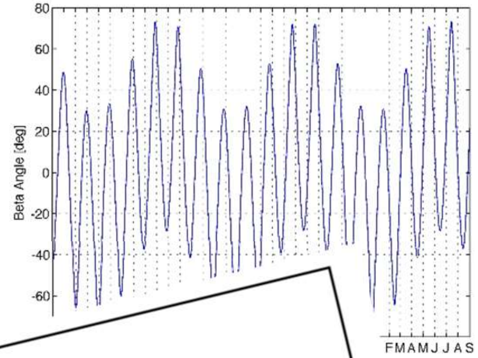
SENSATION

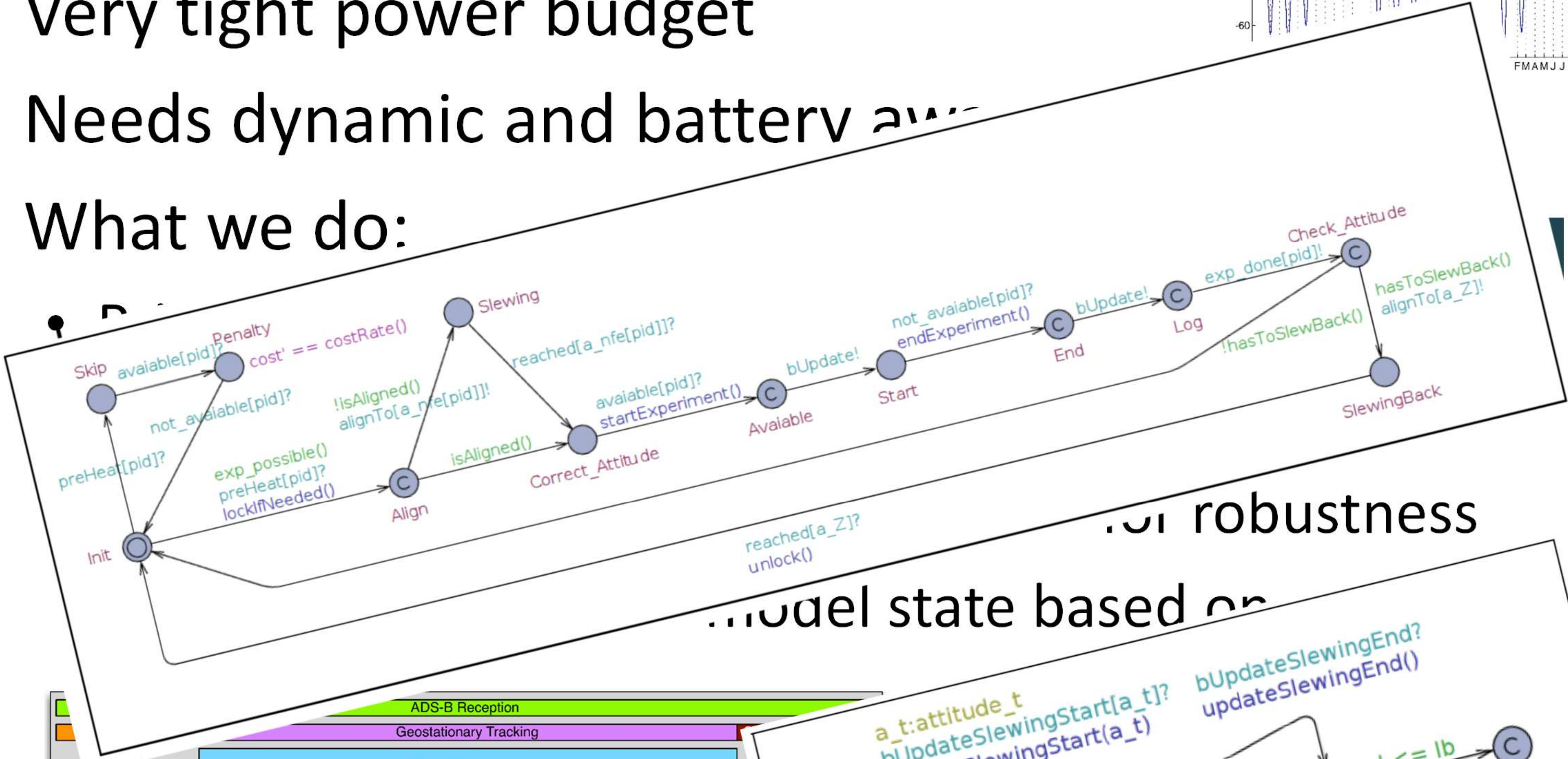
GOMX-3 mission planning

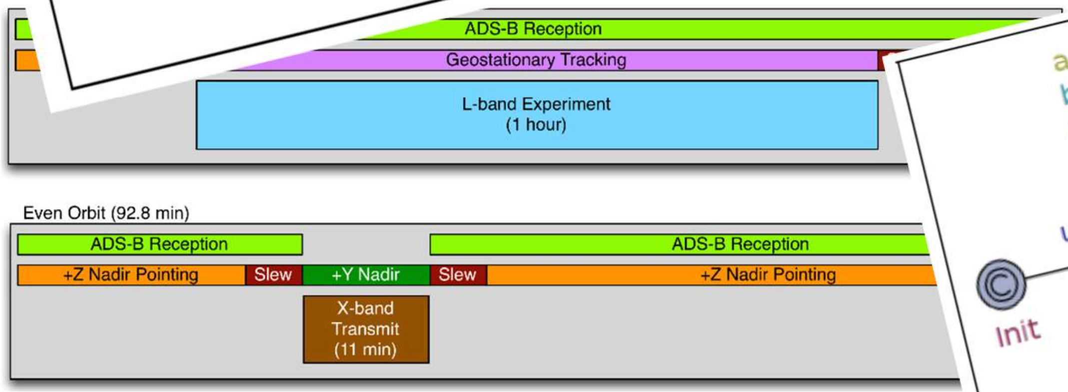
- Very tight power budget
- Needs dynamic and battery aw
- What we do:

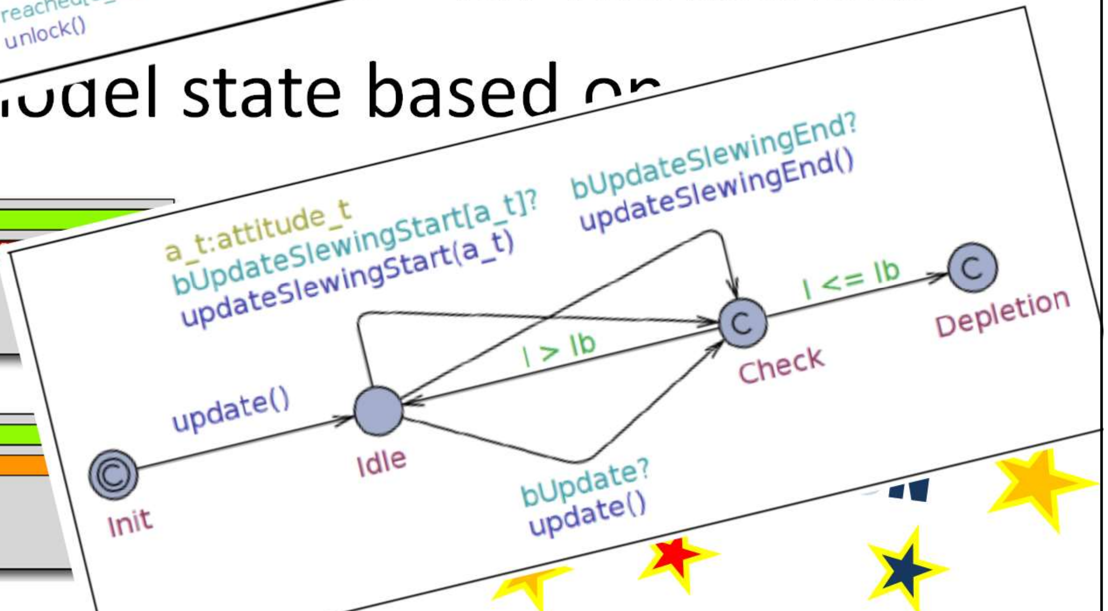
for robustness

model state based on

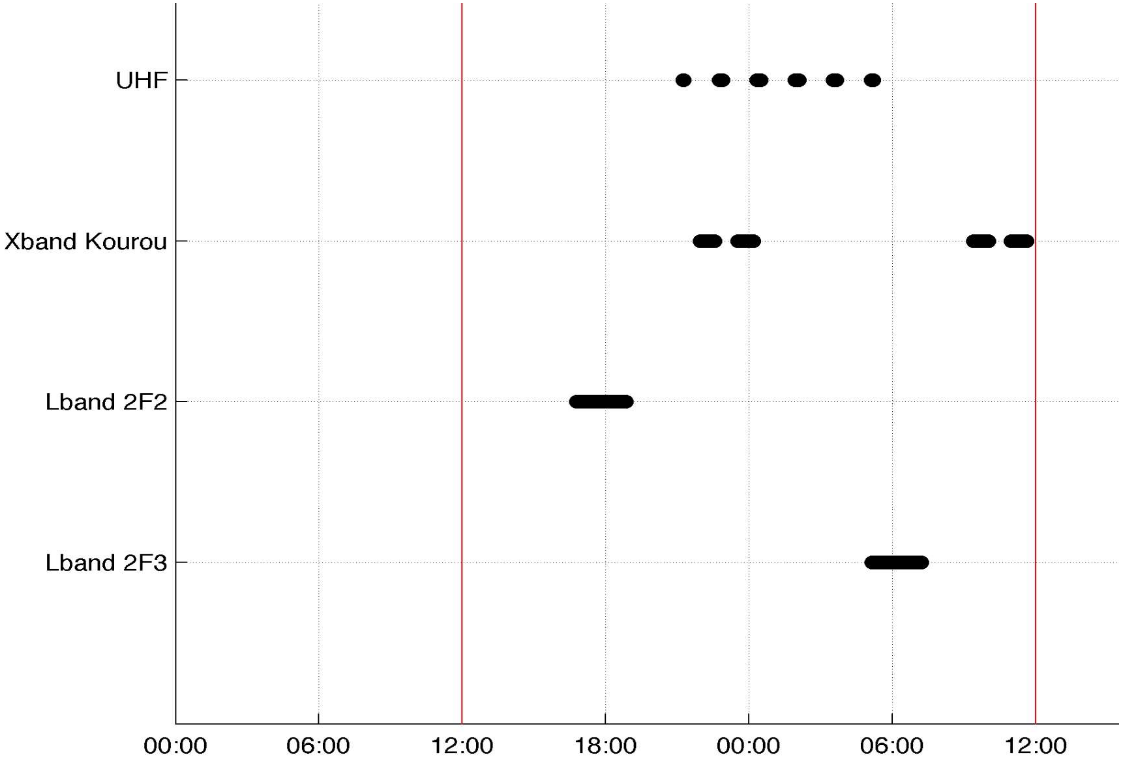


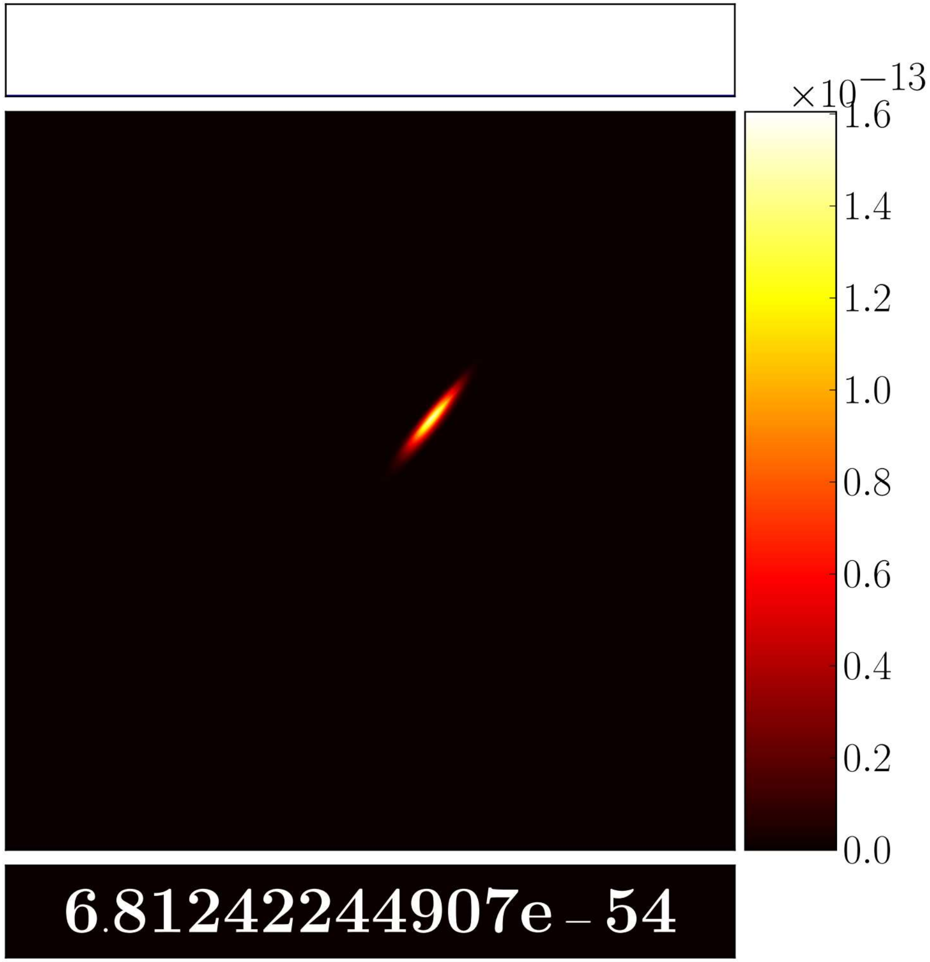






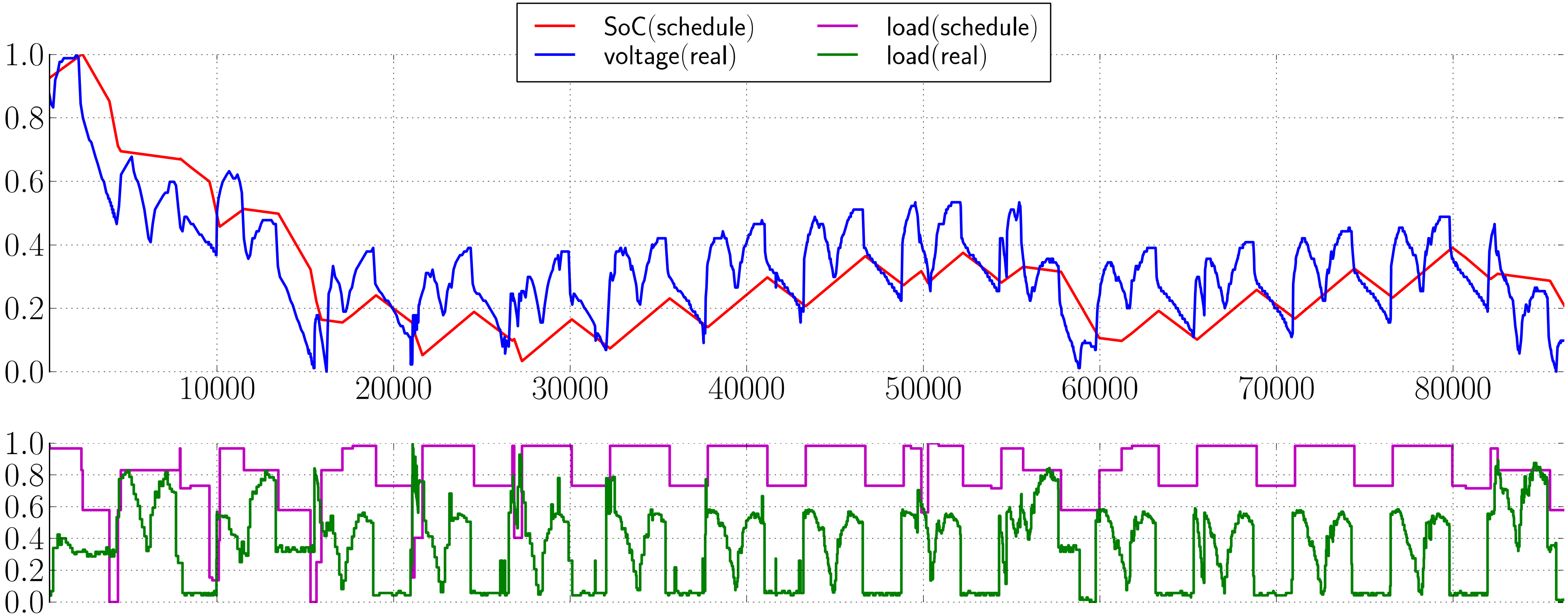
A one-day schedule (for yesterday)



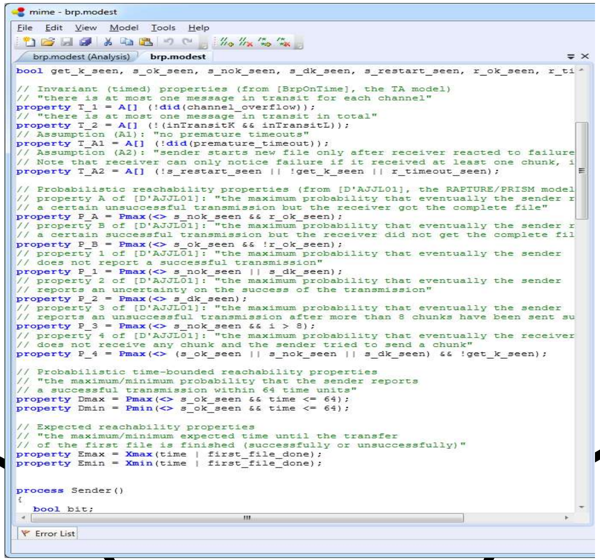


and its depletion risk

Meeting Reality, safely



You saw: Model based … Analysis



System Model
possible behaviour

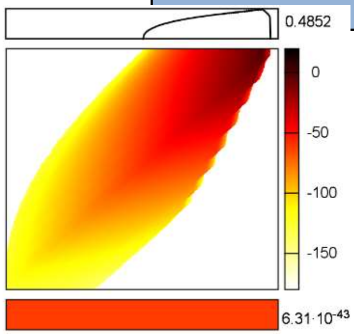
Analysis
Focus

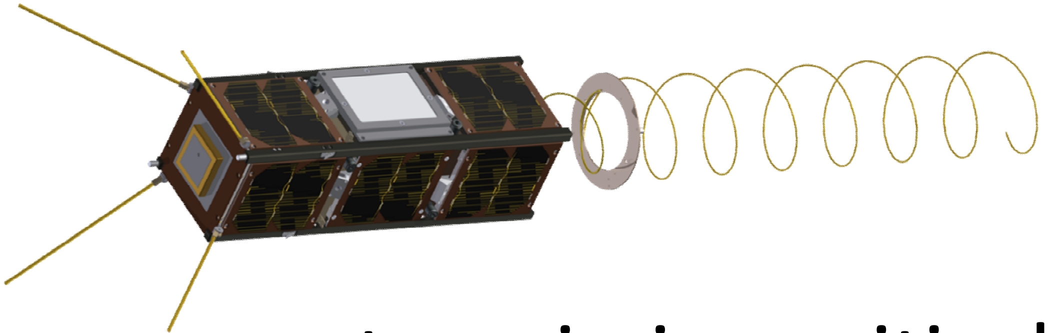
Model Analysis

modestchecker.org

UPPAAL CORA

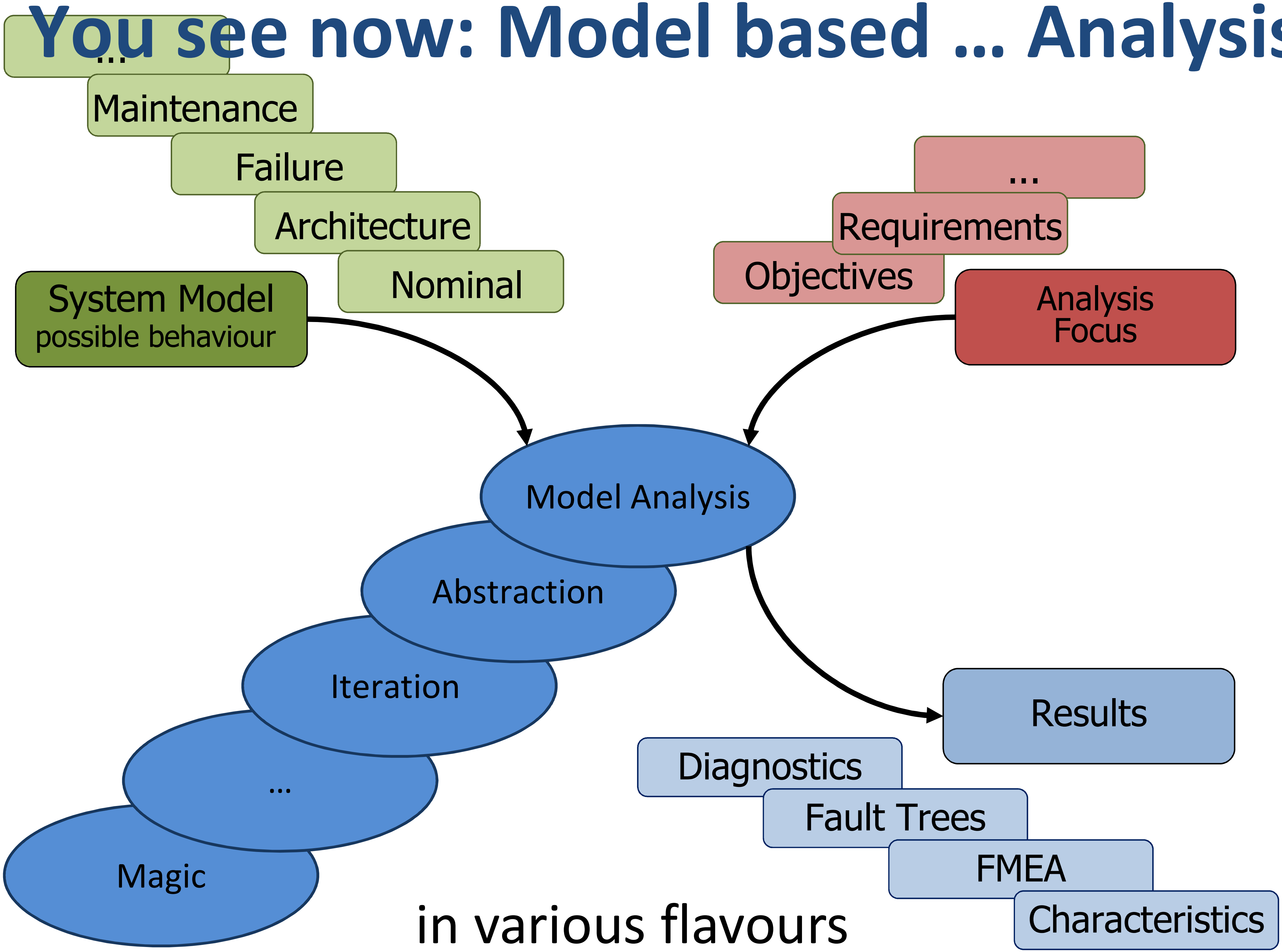
Results





on a concrete, mission-critical case

You see now: Model based … Analysis



in various flavours

Safety by Design?

Some incidents you cannot avoid.
For everything else there are … **formal methods!**