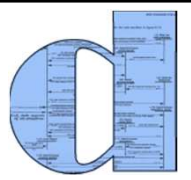


How safe is



your embedded

design, if at all?



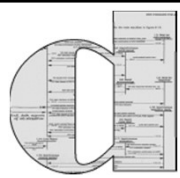
Holger Hermanns

dependable systems and software

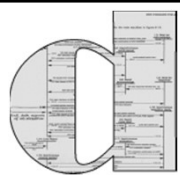
Saarland University

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?

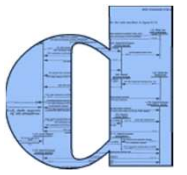


Enforced by various standards:

- 📄 *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*
- 📄 ...

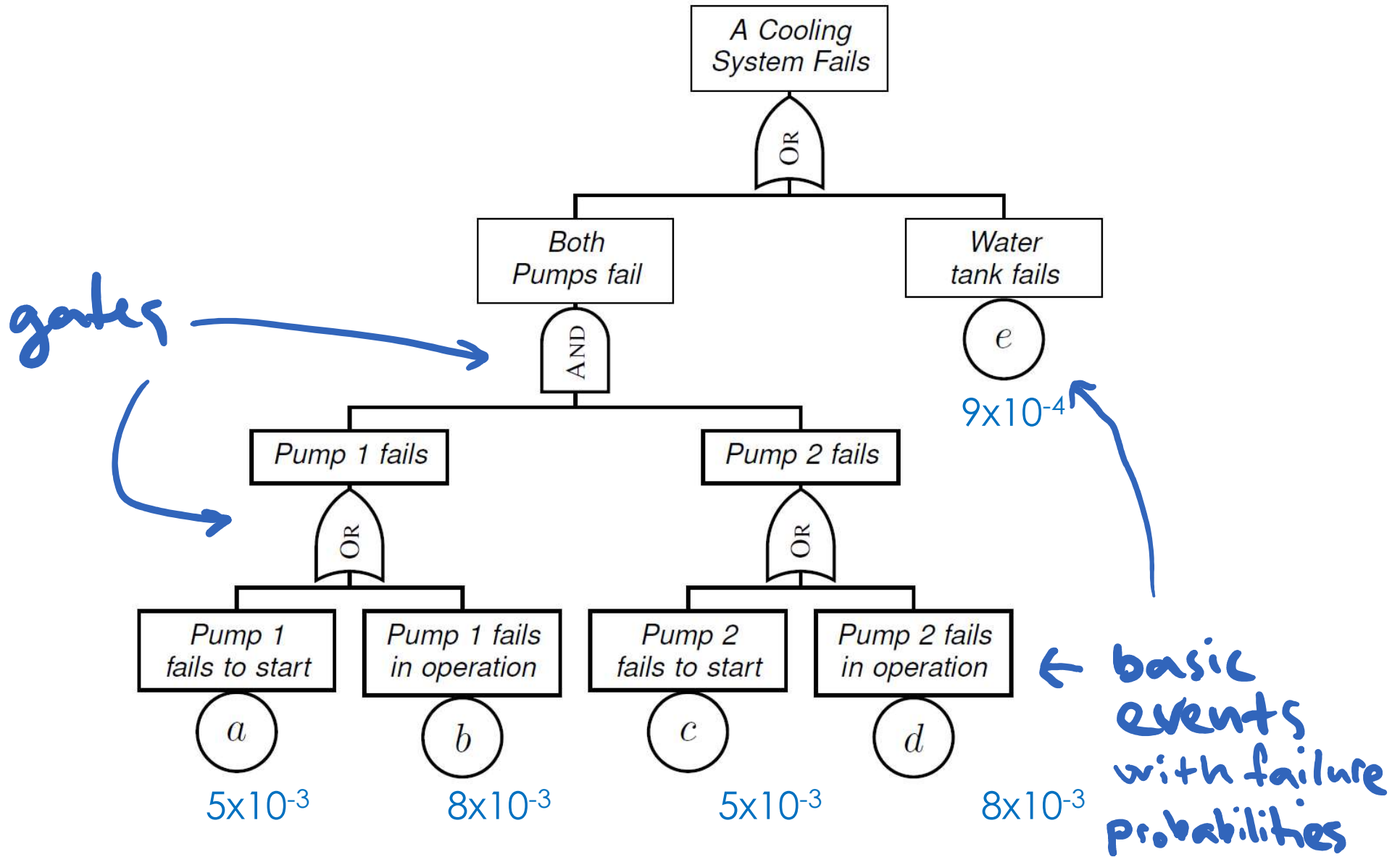
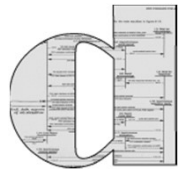
Higher/highest safety levels recommend

Prelude

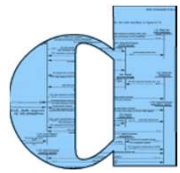


The Static View

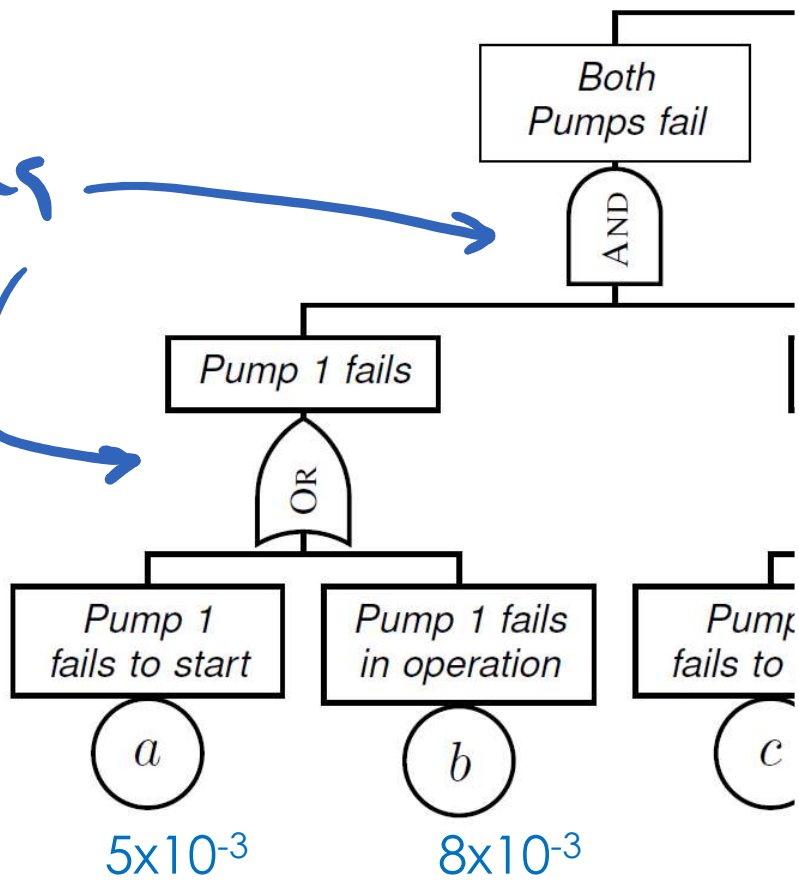
Fault Trees



Fault Trees

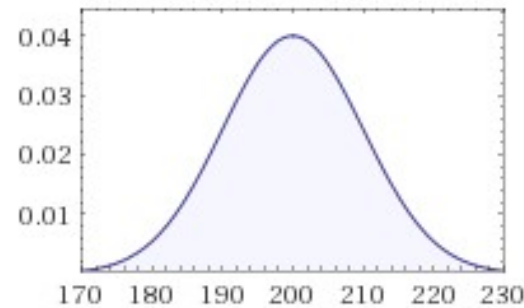


gates



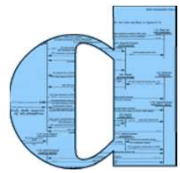
How to obtain the numbers?

- 1) Time-independent failure
- Average number of starts before failure: **200**
⇒ Failure probability **0.005**

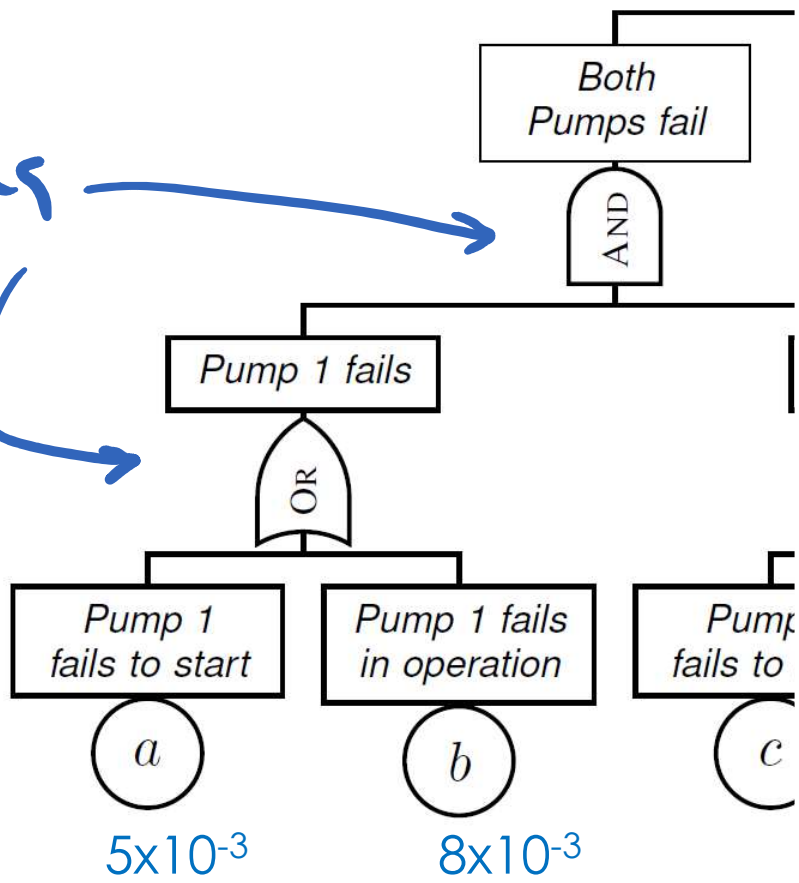


its failure rates

Fault Trees



gates

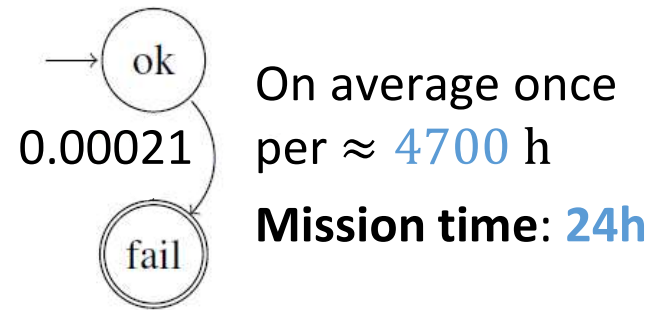


How to obtain the numbers?

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

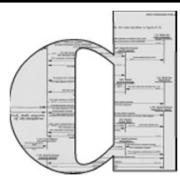
Mission time: 24h

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

... and from further models

its failure rates

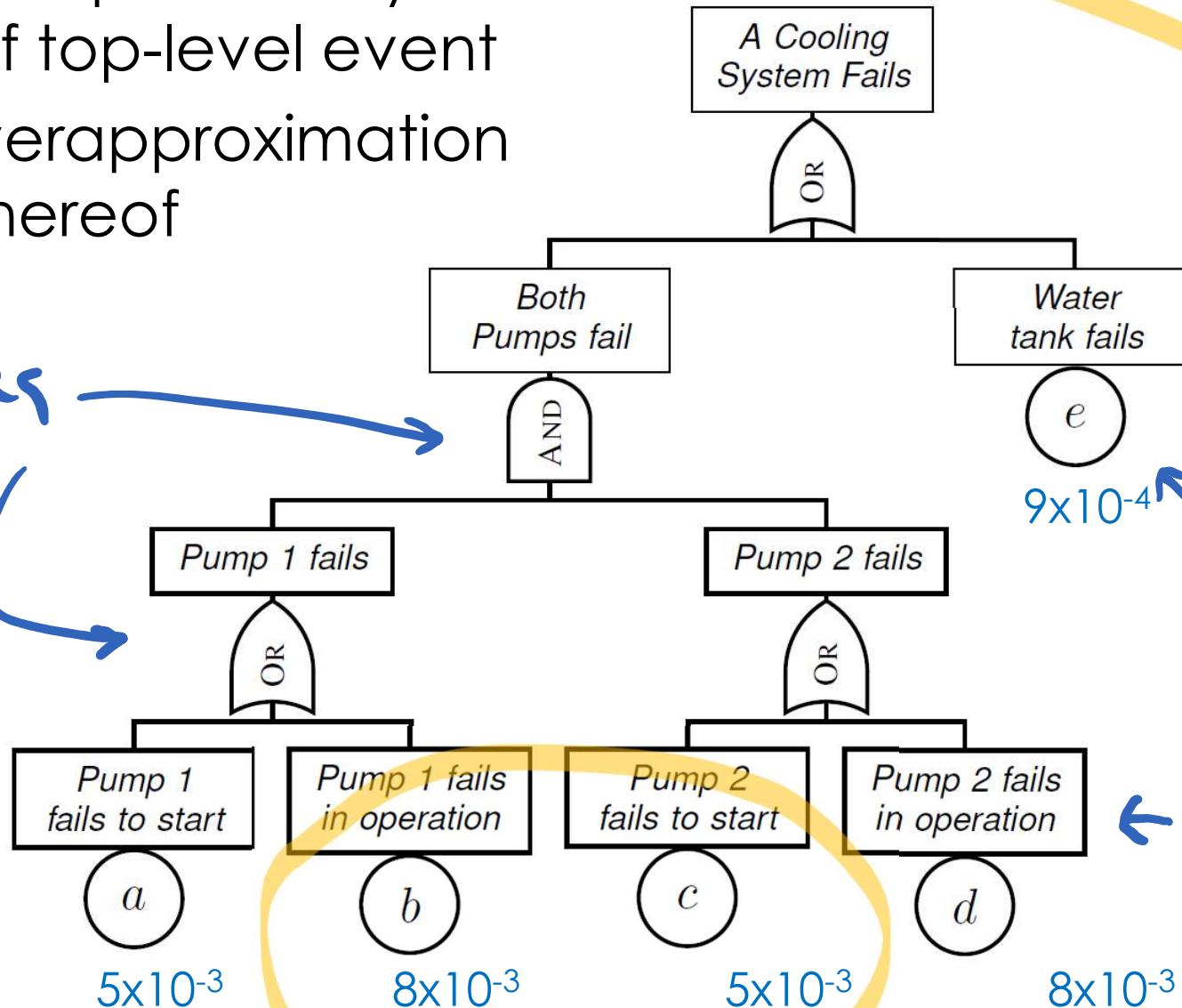
Fault Trees – Analysis Basics



Calculate probability
of top-level event
... or overapproximation
thereof

'Minimal cut set'

gates



9×10^{-4}

5×10^{-3}

8×10^{-3}

5×10^{-3}

8×10^{-3}

basic events with failure probabilities

Fault Trees

- are often very large *50,000+ nodes*

- are very costly to maintain *millions of €*

- are very important

- are stateless

- give imprecise results

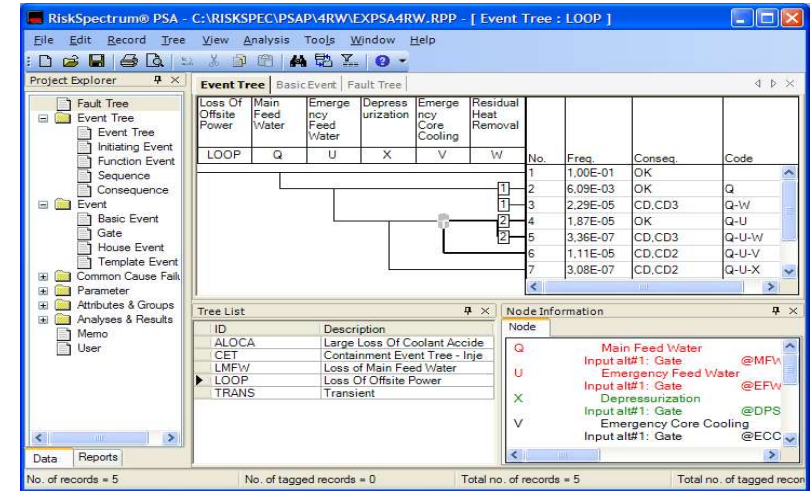
- too pessimistic due to stateless view *e.g. no repair*

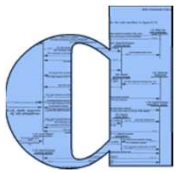
- too optimistic if dependencies *e.g. common cause*

- ...



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





**All models
are wrong,
but some
are useful.**

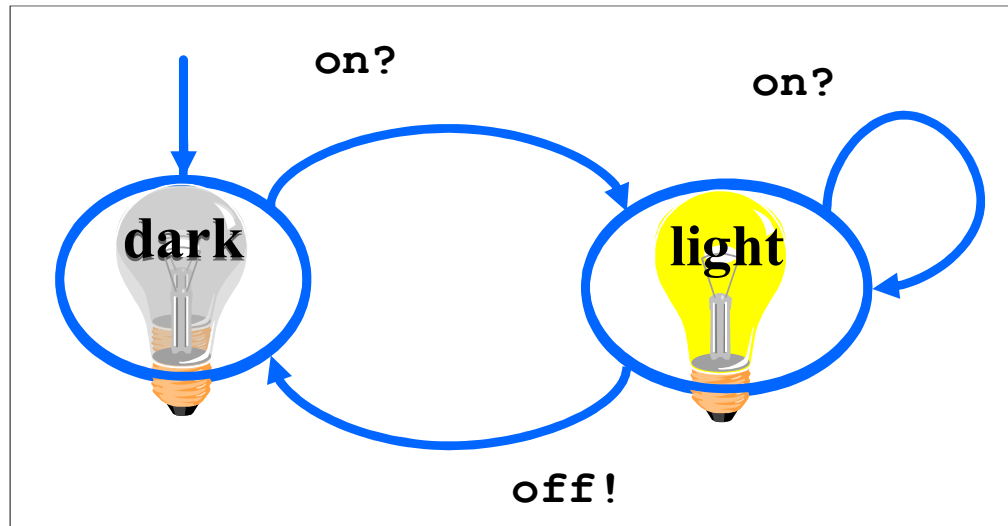


George E. P. Box

Useful Models



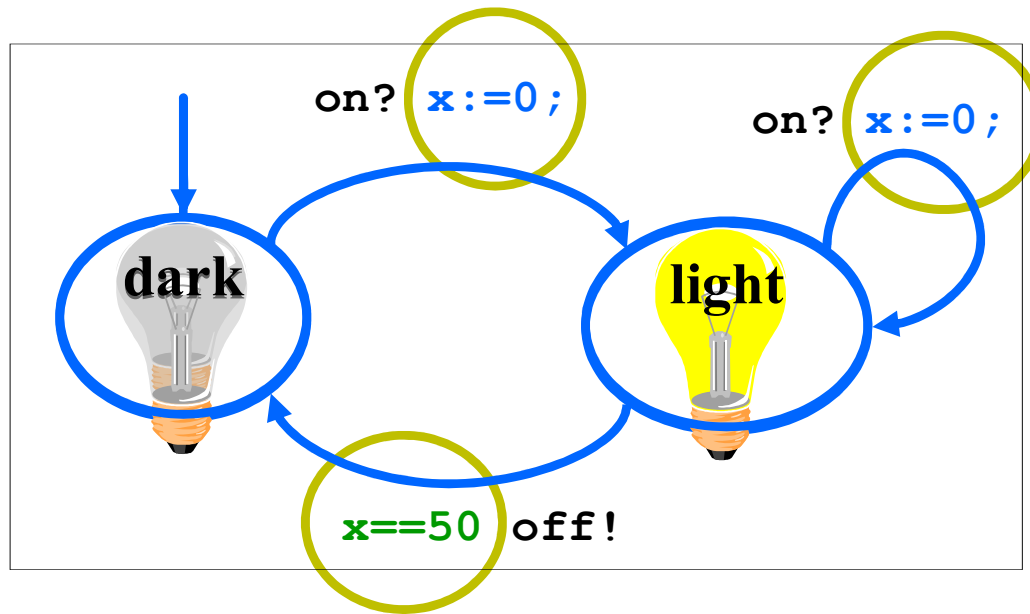
 finite automata



Useful Models

finite automata

with clocks *all running at the same speed*

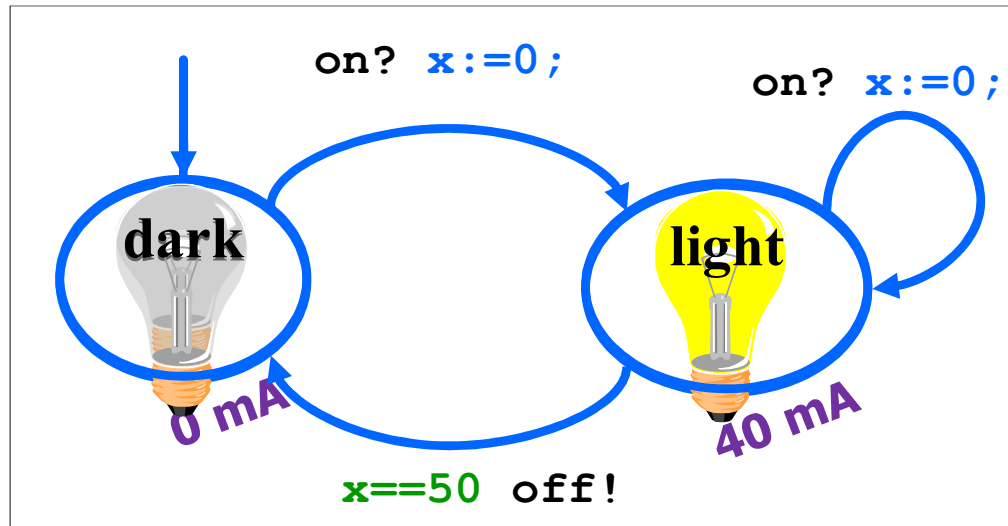


Timed Automata

Useful Models



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

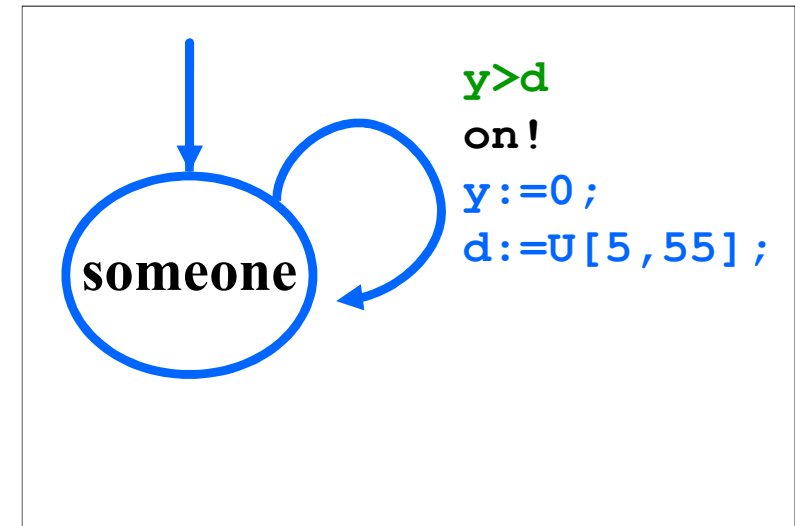
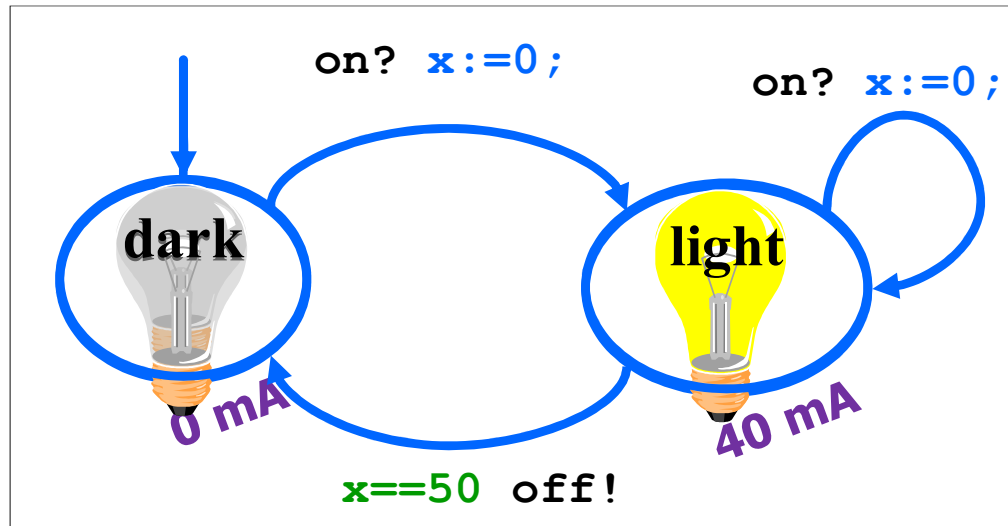


Priced Timed Automata

Useful Models



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

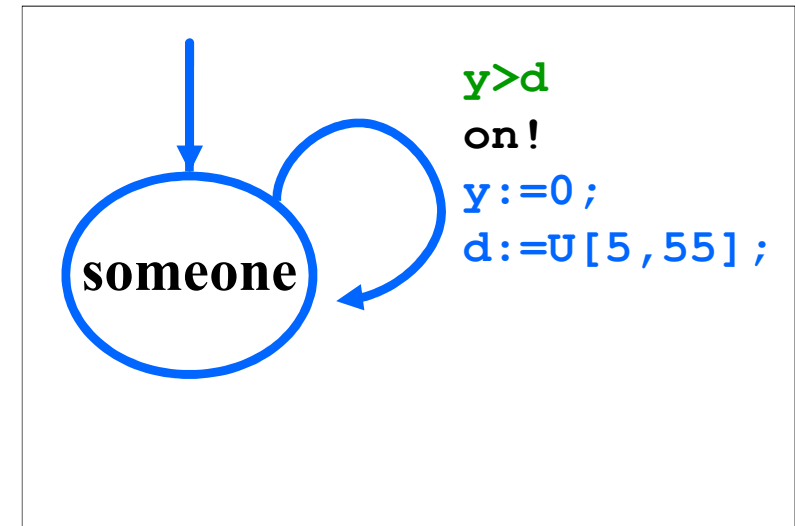
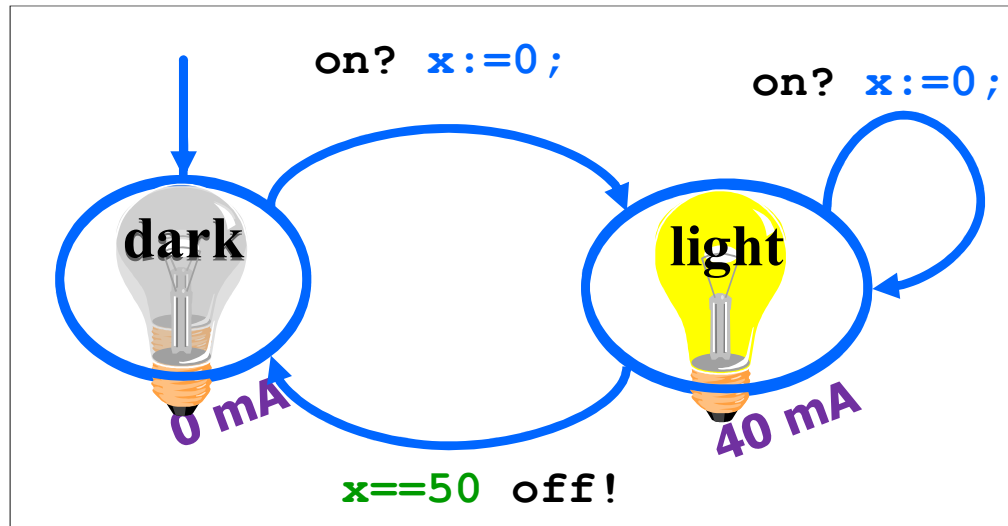
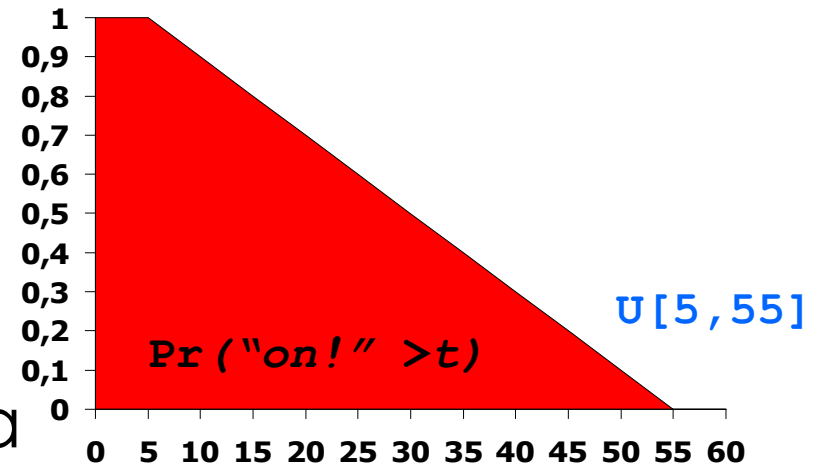


Automata Networks

Useful Models



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



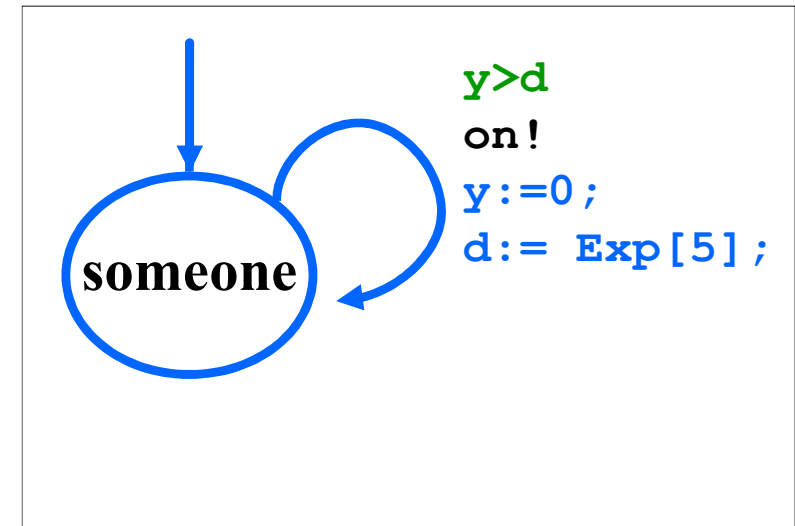
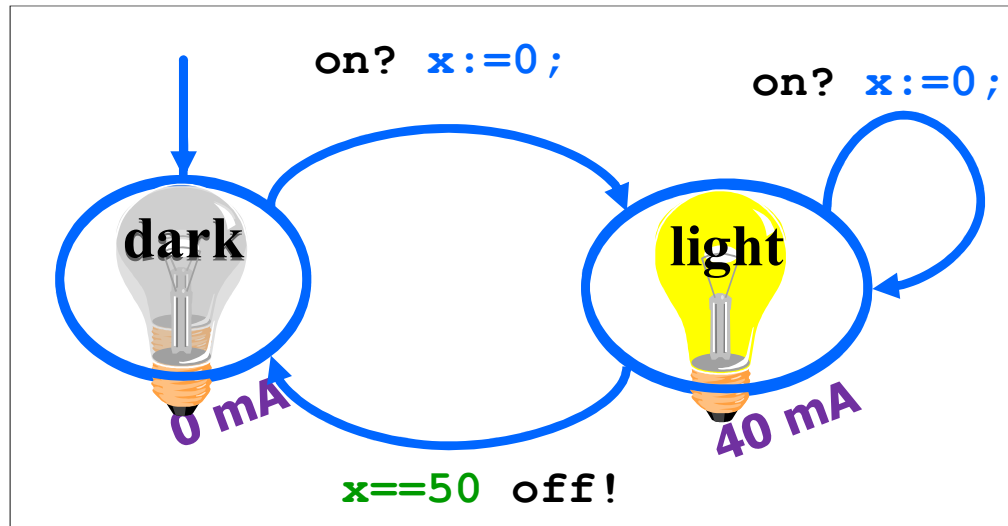
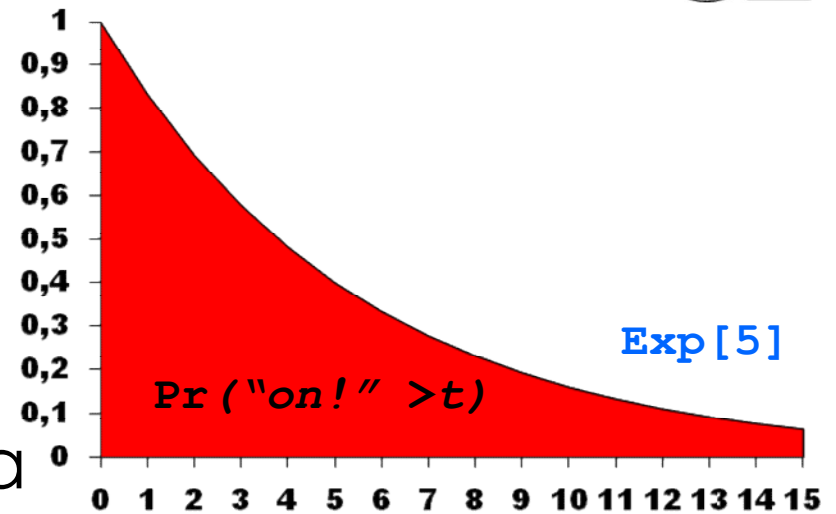
- with probability distributions

Stochastic Timed Automata

Useful Models



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

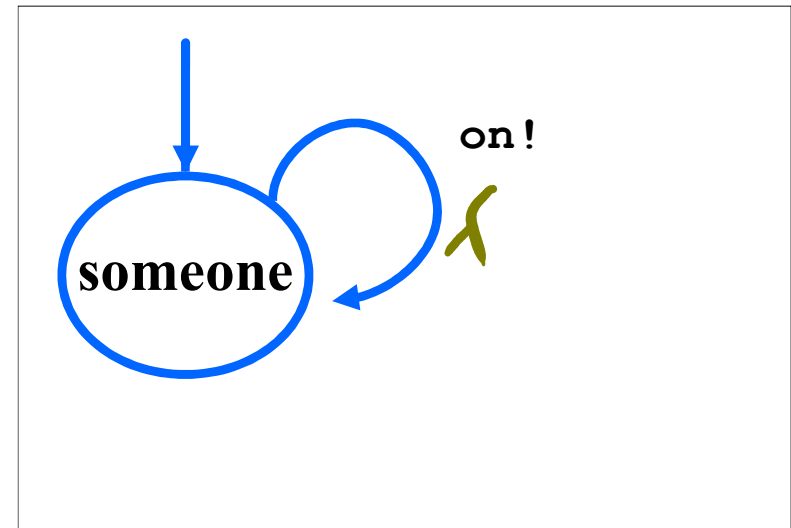
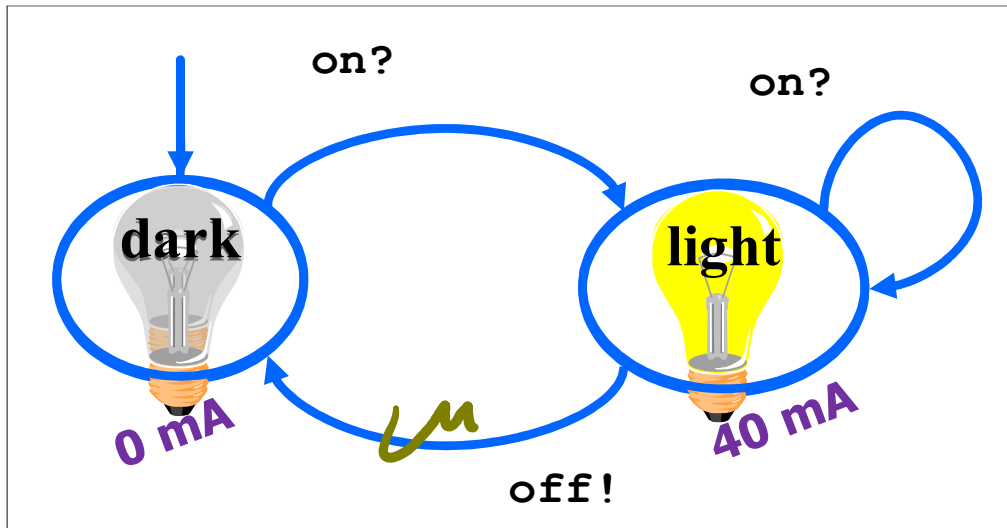
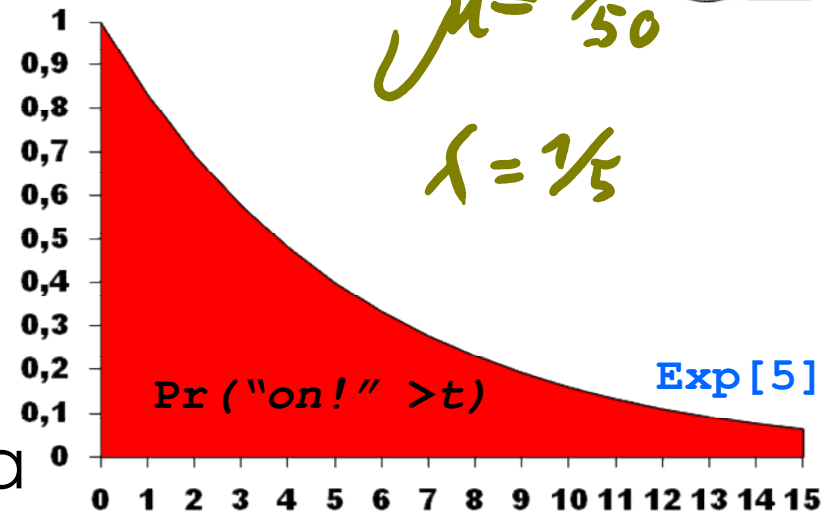


- with probability distributions

Stochastic Timed Automata

Useful Models

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



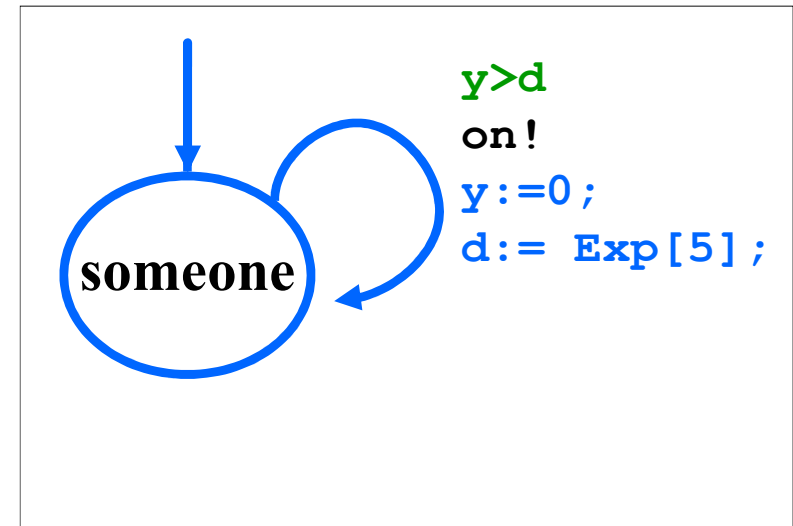
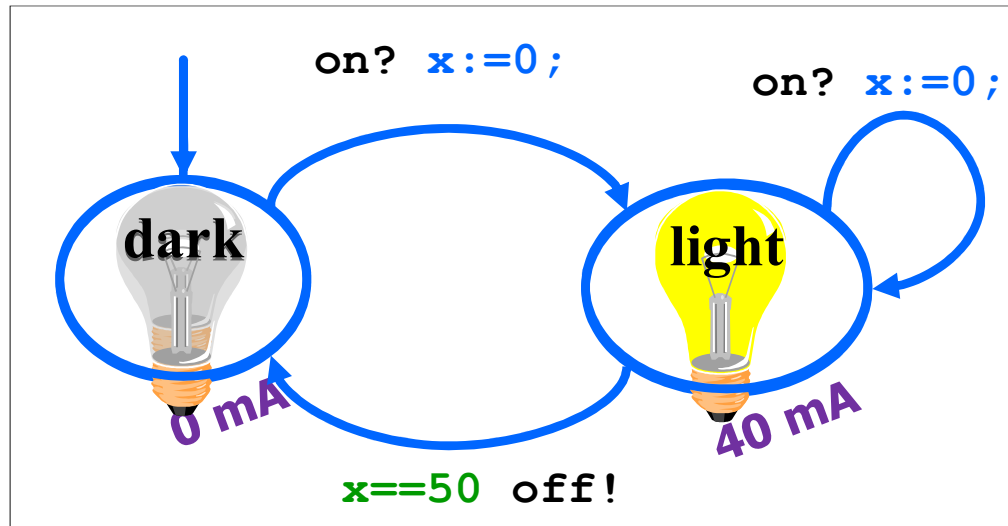
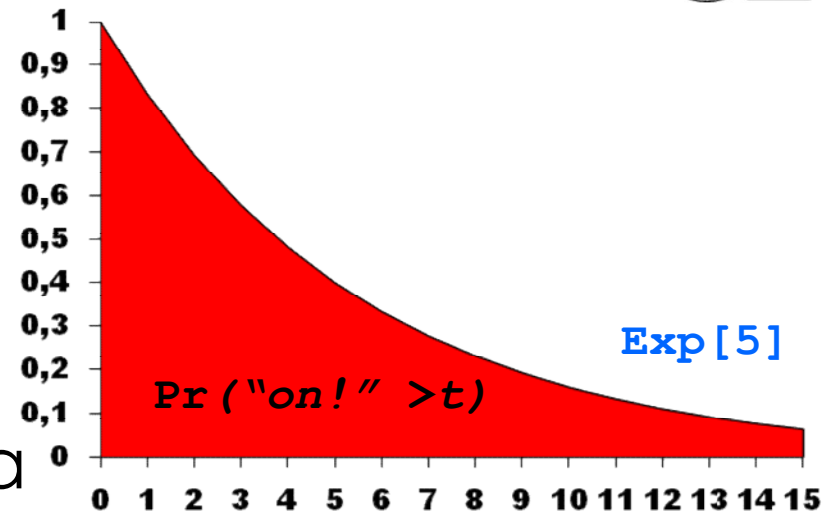
- with probability distributions

Markov Automata

Useful Models



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



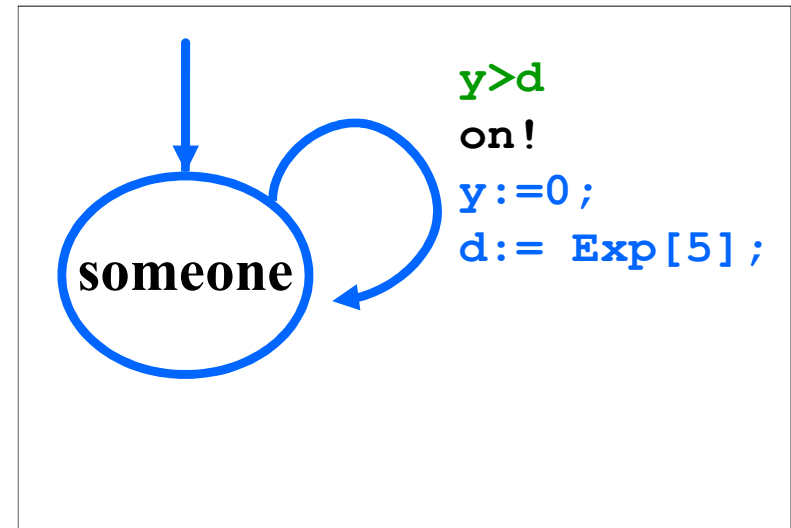
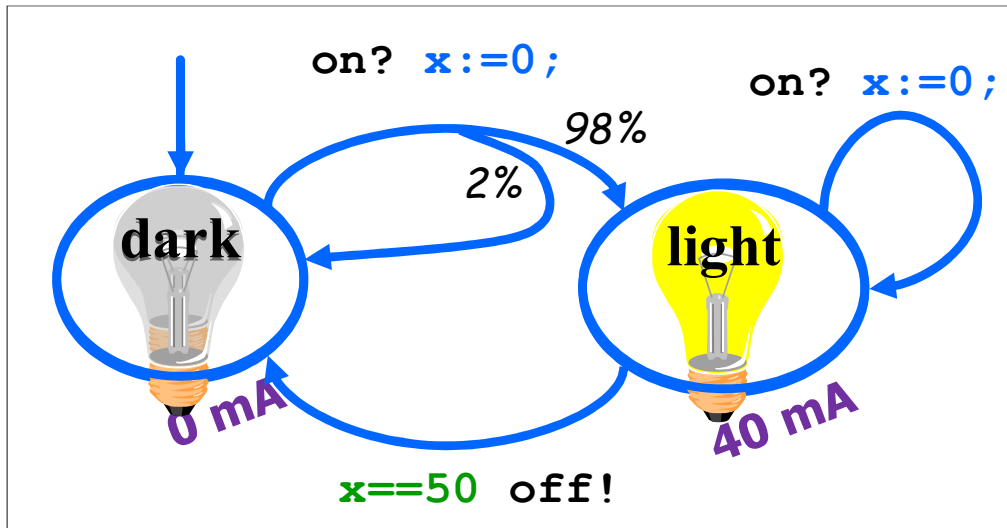
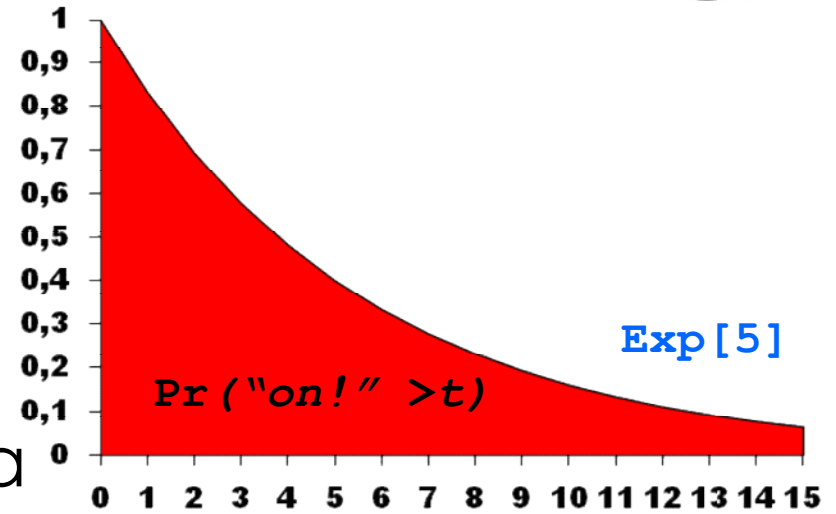
- with probability distributions

Stochastic Timed Automata

Useful Models



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



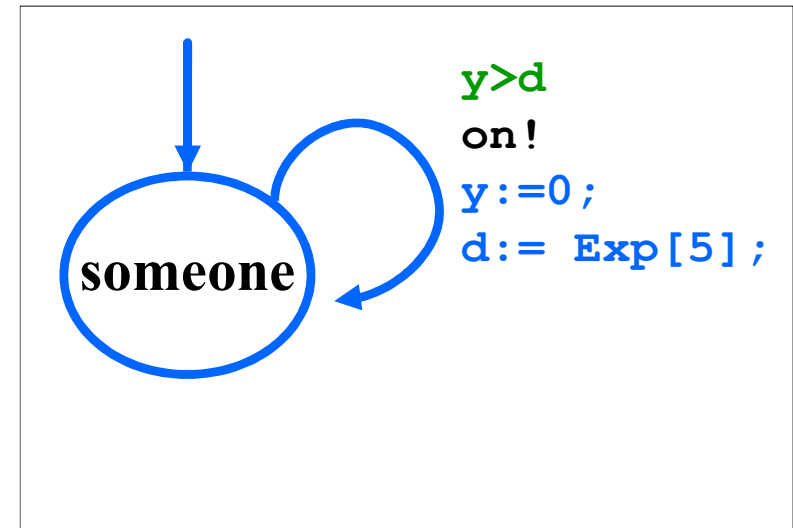
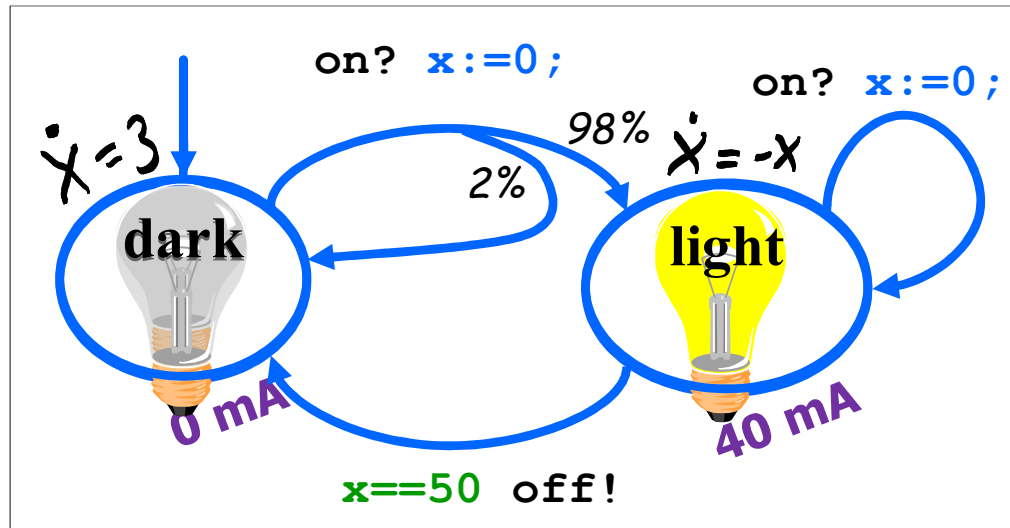
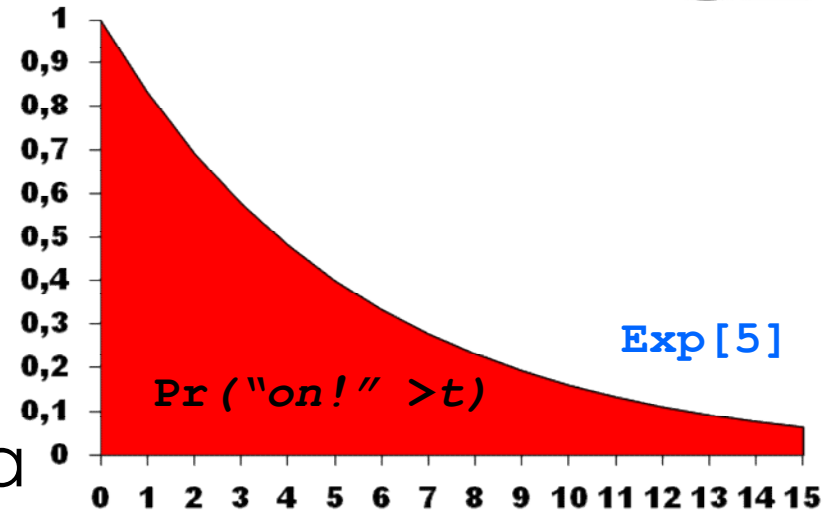
- ☐ with probability distributions

Stochastic Timed Automata

Useful Models



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

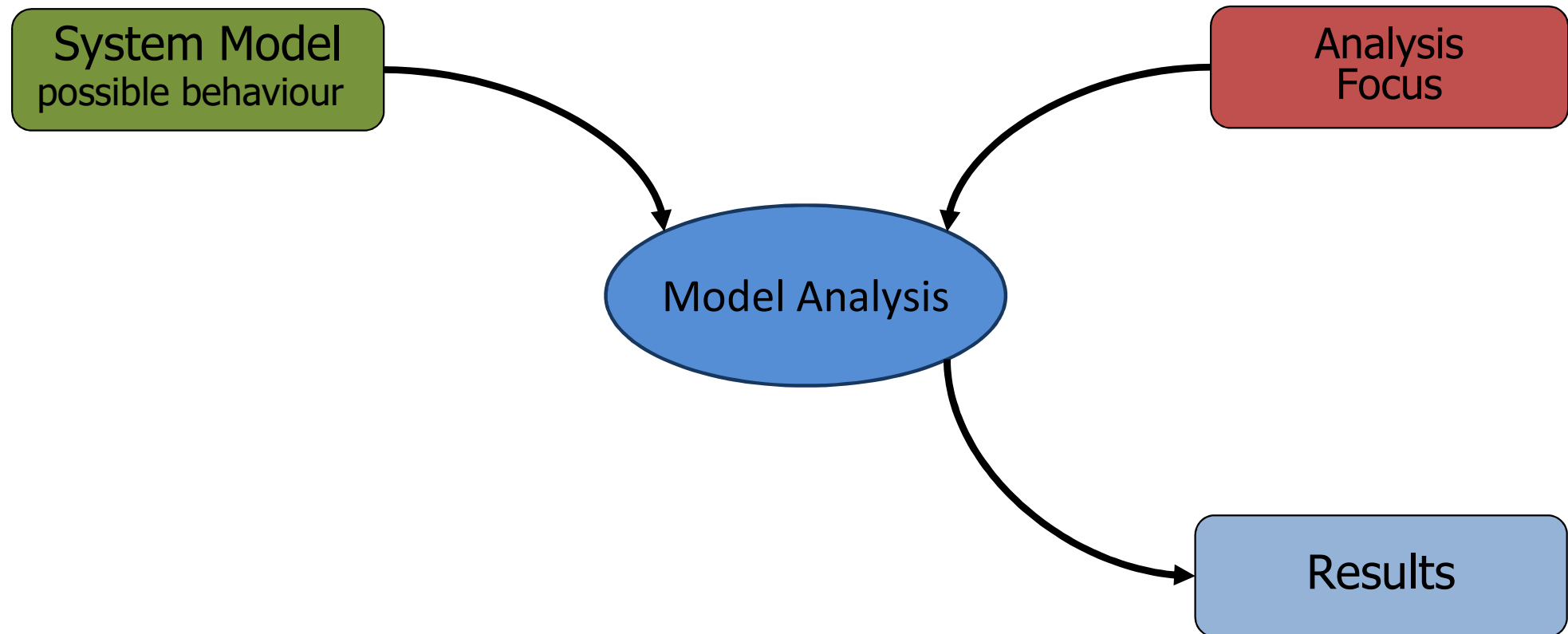


- ☐ with probability distributions
- ☐ and continuous dynamics

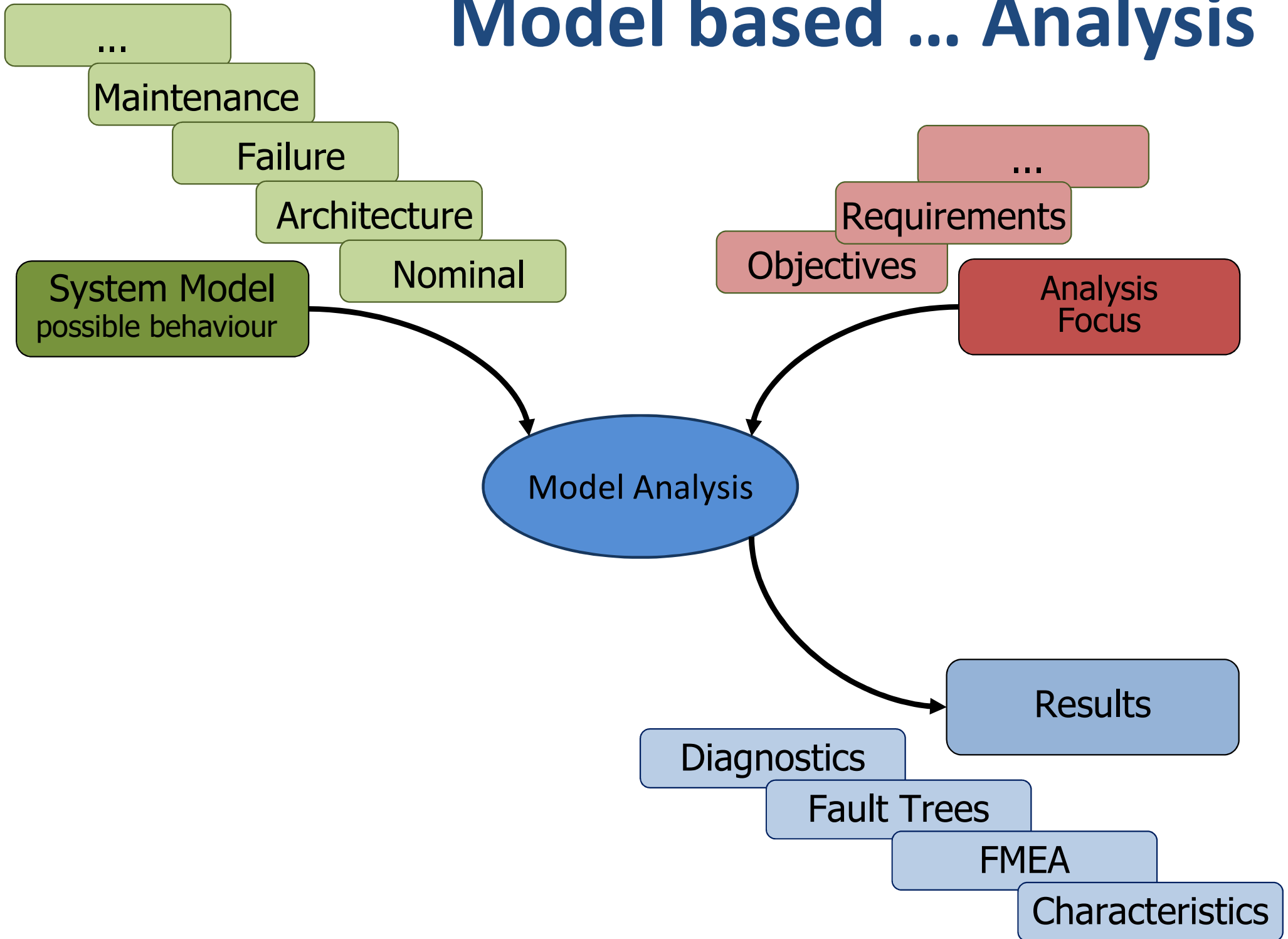
Stochastic Hybrid Automata

**THE
BIGGER
PICTURE**

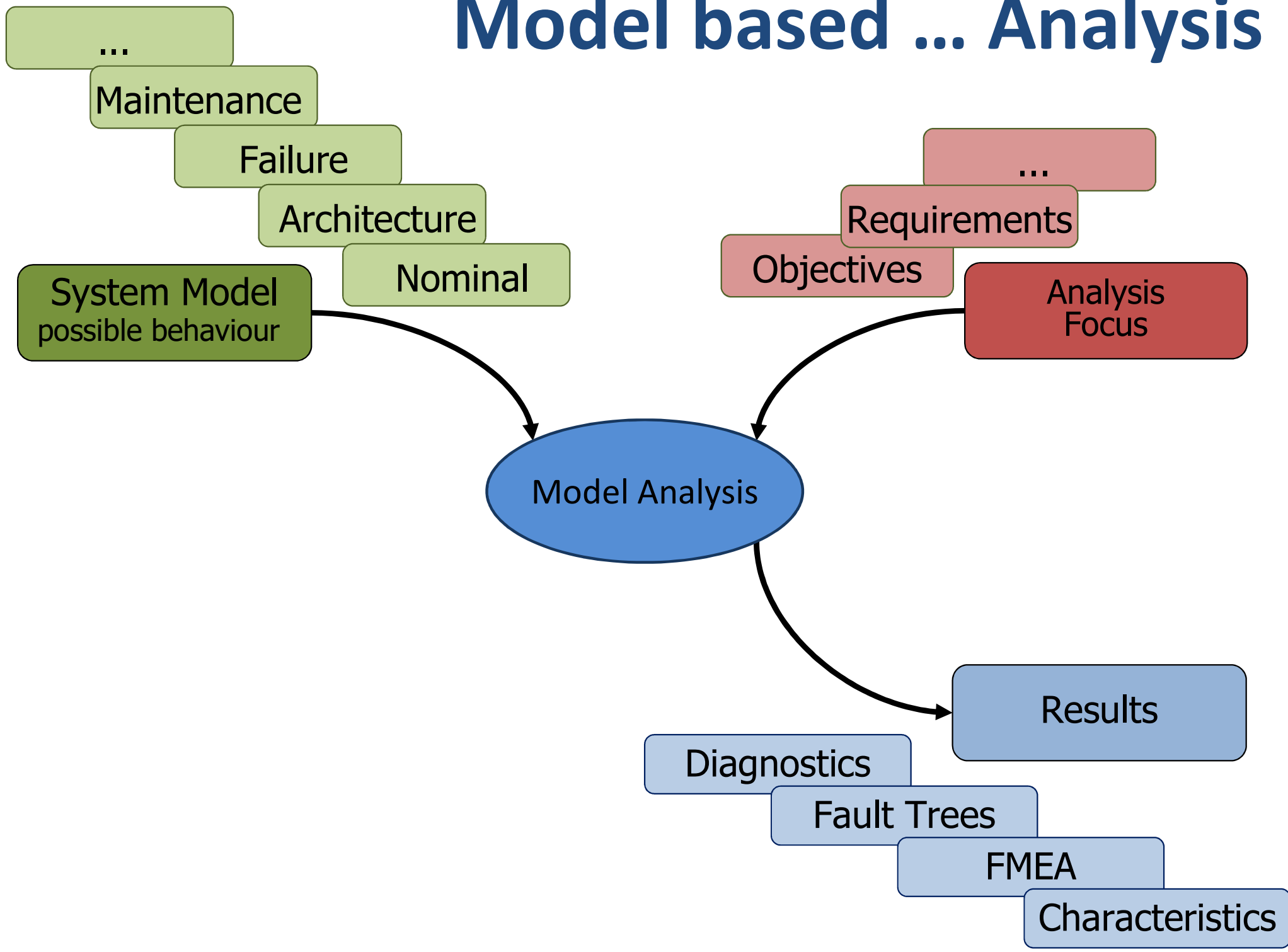
Model based ... Analysis



Model based ... Analysis

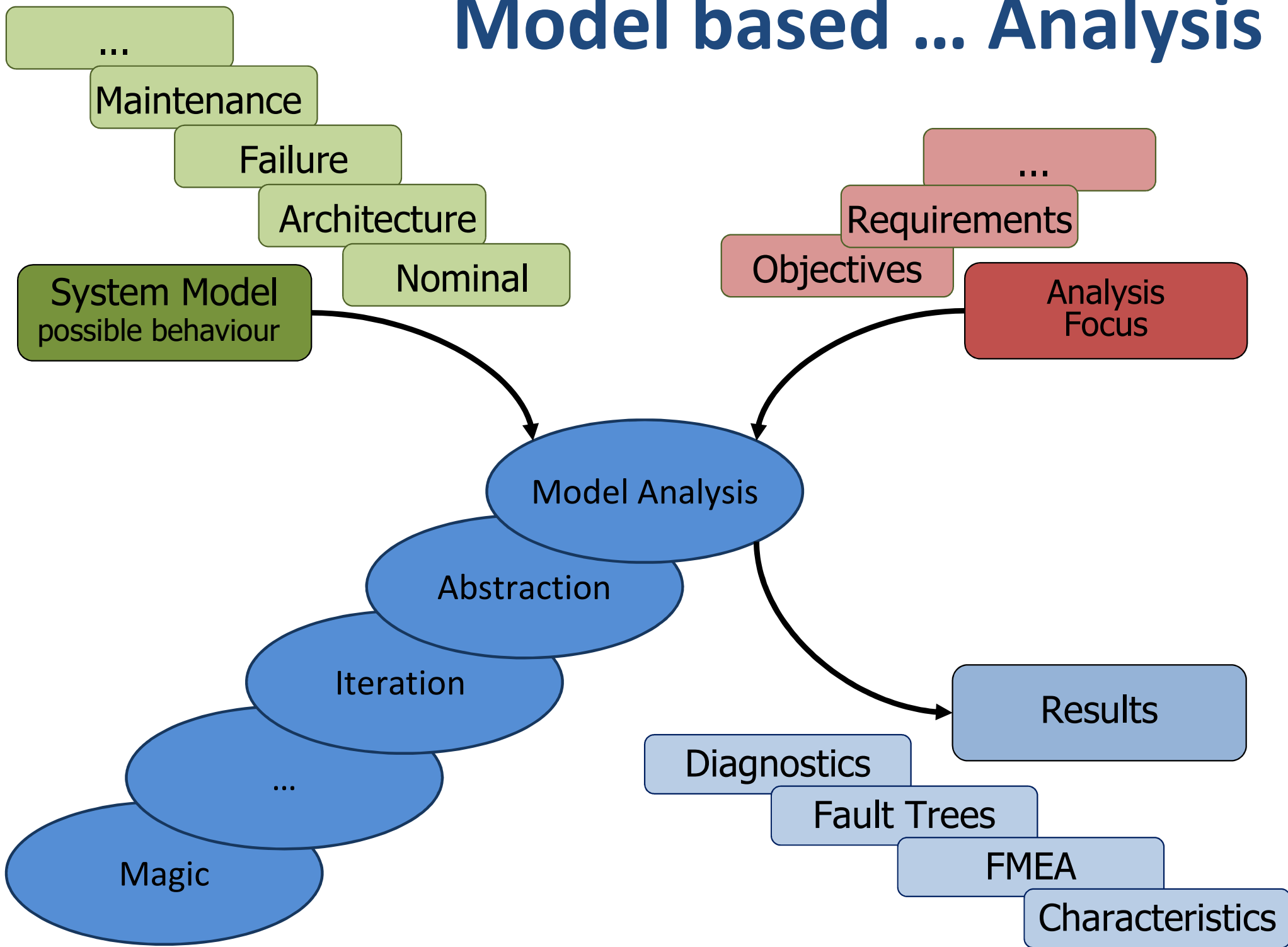


Model based ... Analysis



Model Analysis

Model based ... Analysis



Model based ... Analysis

System Model
possible behaviour

```
mime - brp.modest
File Edit View Model Tools Help
brp.modest [Analysis] brp.modest
bool get_K_seen, a_ok_seen, a_nok_seen, a_dk_seen, a_restart_seen, r_ok_seen, r_ti...
// Invariant (timed) properties (from [BrpOnTime], the TA model)
// "there is at most one message in transit for each channel"
property T_1 = A[] (!did(channel_overflow));
// "there is at most one message in transit in total"
property T_2 = A[] (!inTransitK && !inTransitL);
// Assumption (A1): "no premature timeouts"
property T_A1 = A[] (!did(premature_timeout));
// Assumption (A2): "sender starts new file only after receiver reacted to failure"
// Note that receiver can only notice failure if it received at least one chunk, i
property T_A2 = A[] (!a_restart_seen || !get_K_seen || !r_timeout_seen);
// Probabilistic reachability properties (from [D'AUGLIO], the RAPTURE/FRISK model)
// property A of [D'AUGLIO]: "the maximum probability that eventually the sender r
// a certain unsuccessful transmission but the receiver got the complete file"
property P_A = Pmax(<> a_nok_seen && a_ok_seen);
// property B of [D'AUGLIO]: "the maximum probability that eventually the sender r
// a certain successful transmission but the receiver did not get the complete fil
property P_B = Pmax(<> a_ok_seen && !r_ok_seen);
// property 1 of [D'AUGLIO]: "the maximum probability that eventually the sender
// does not report a successful transmission"
property P_1 = Pmax(<> a_nok_seen || a_dk_seen);
// property 2 of [D'AUGLIO]: "the maximum probability that eventually the sender
// reports an uncertainty on the success of the transmission"
property P_2 = Pmax(<> a_dk_seen);
// property 3 of [D'AUGLIO]: "the maximum probability that eventually the sender
// reports an unsuccessful transmission after more than 8 chunks have been sent su
property P_3 = Pmax(<> a_nok_seen && s > 8);
// property 4 of [D'AUGLIO]: "the maximum probability that eventually the receiver
// does not receive any chunk and the sender tried to send a chunk"
property P_4 = Pmax(<> (s_ok_seen || a_nok_seen || a_dk_seen) && !get_K_seen);
// Probabilistic time-bounded reachability properties
// "the maximum/minimum probability that the sender reports
// a successful transmission within 64 time units"
property Dmax = Pmax(<> a_ok_seen && time <= 64);
property Dmin = Pmin(<> a_ok_seen && time <= 64);
// Expected reachability properties
// "the maximum/minimum expected time until the transfer
// of the first file is finished (successfully or unsuccessfully)"
property Emax = Xmin(time | first_file_done);
property Emin = Xmin(time | first_file_done);
process Sender()
{
  bool bit;
  ...
}
Error List
```

Analysis
Focus

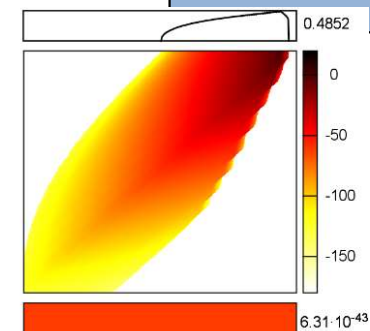
Model Analysis



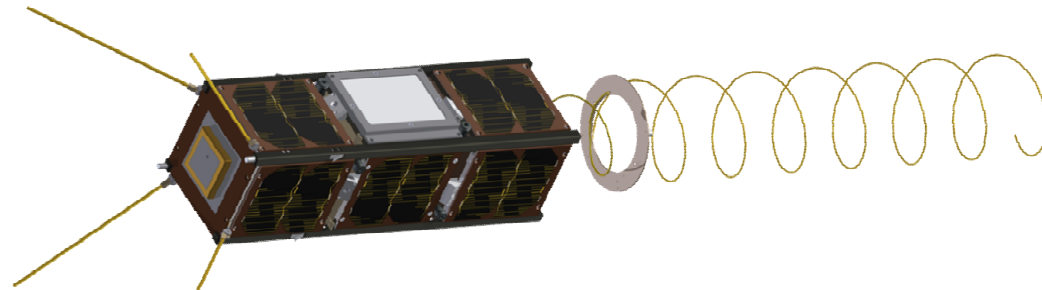
modestchecker.org

UPPAAL CORA

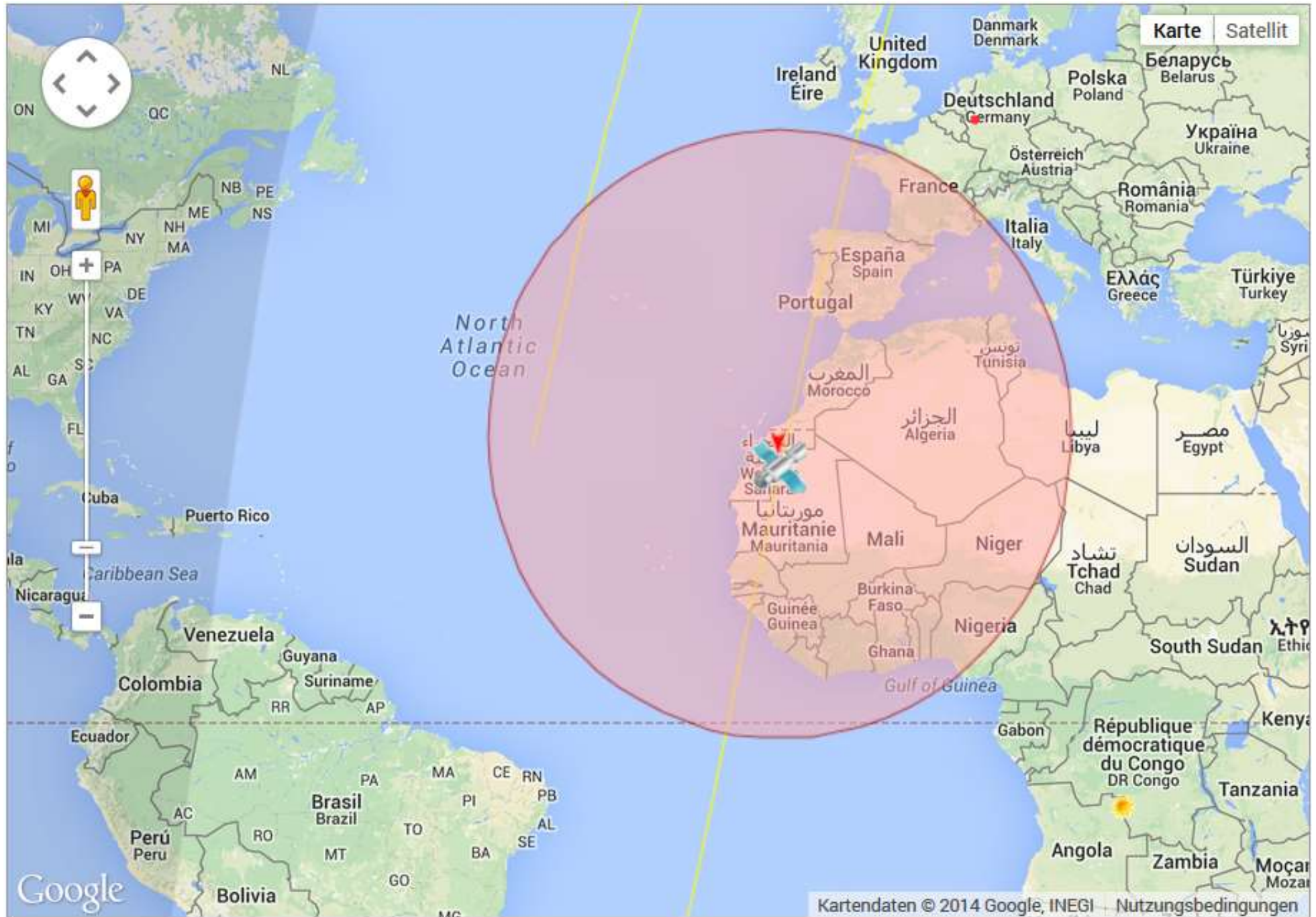
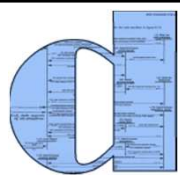
Results



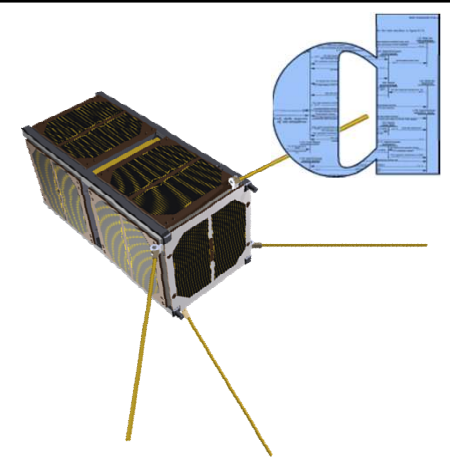
A concrete, mission-critical case



Embedded in Space



GOMSPACE GOMX-1

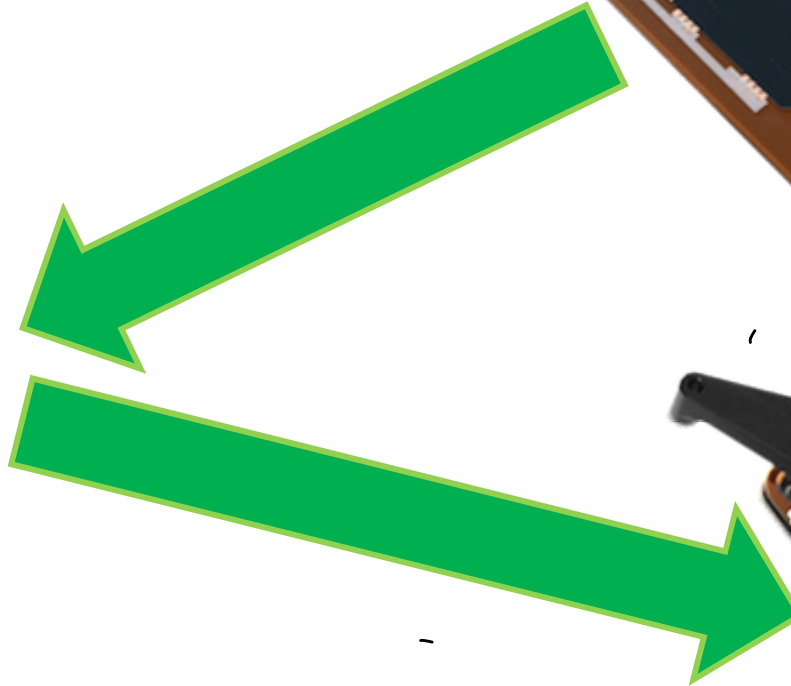
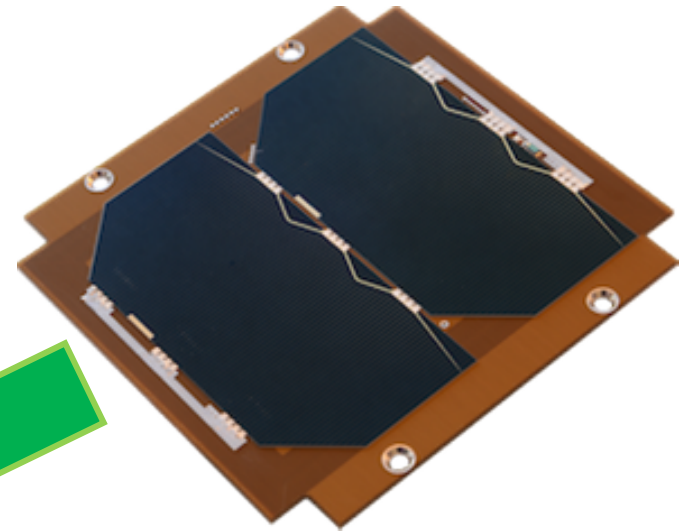
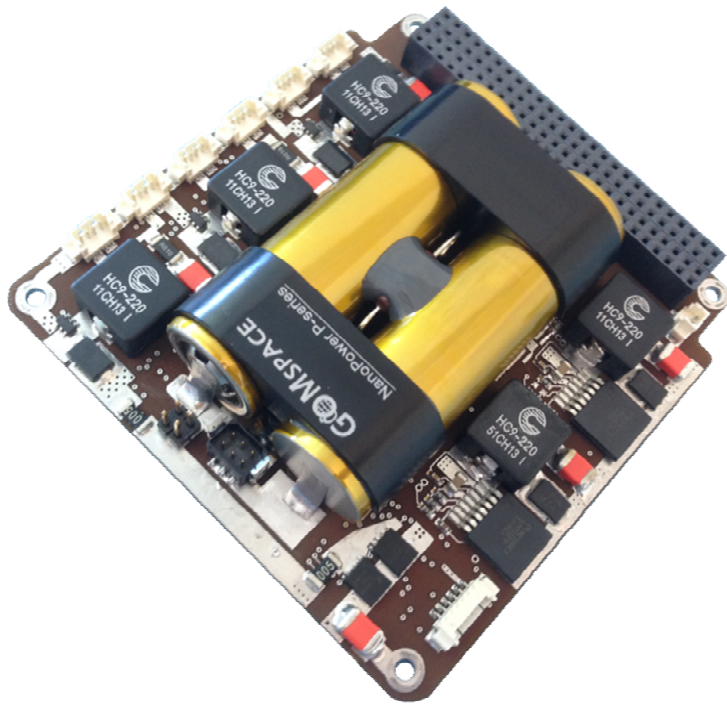
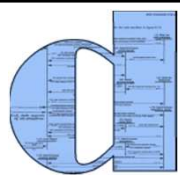


- 2U CubeSat (2 liter)
- Launched in November 2013
- Payloads:
 - software defined receiver for aircraft signals
 - color camera for earth observation
- Telemetry transmitted on amateur radio frequency
- Massive amounts of data collected
 - battery voltage, temperature, solar infeed, ...

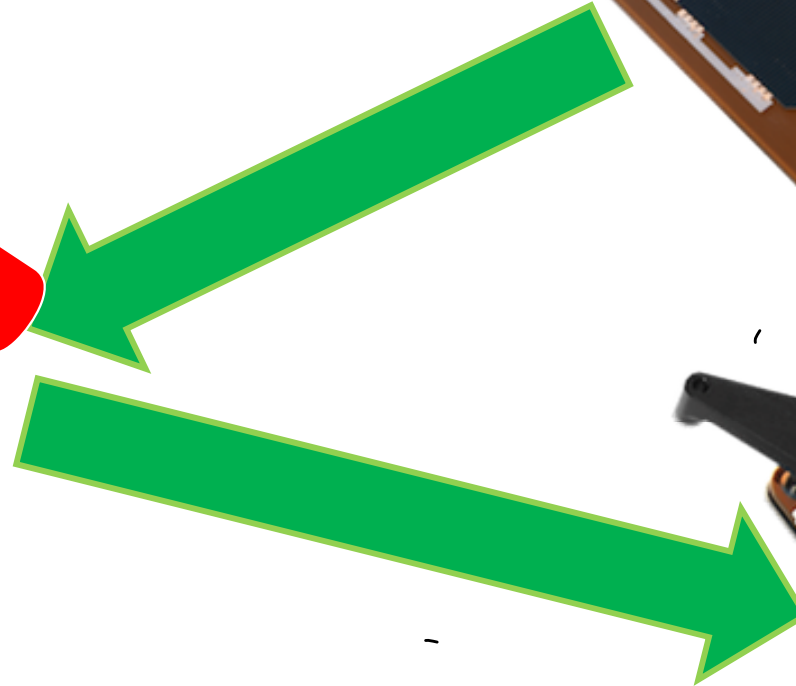
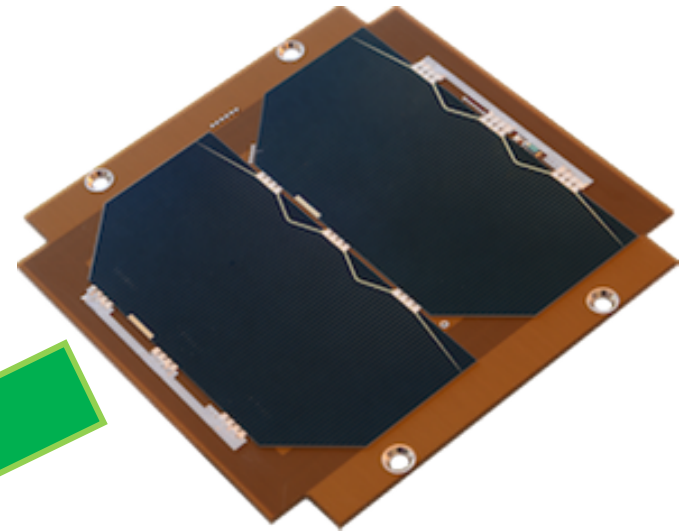
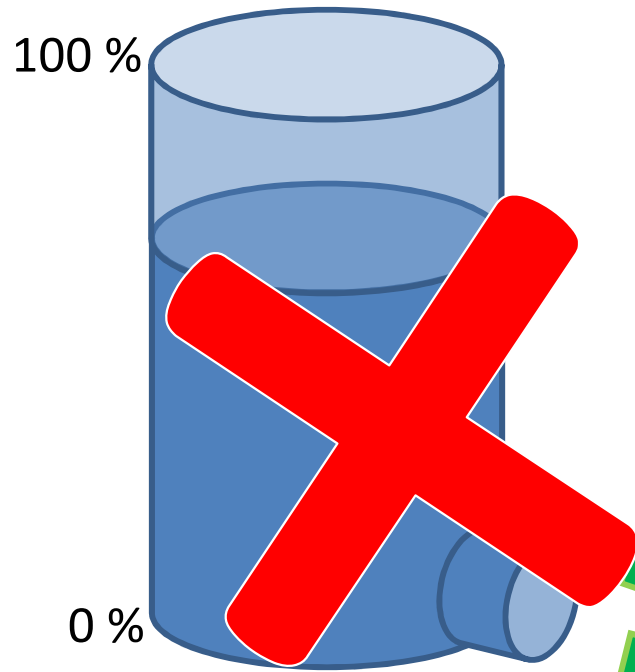
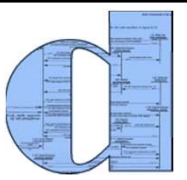
Runs our calibration experiments.



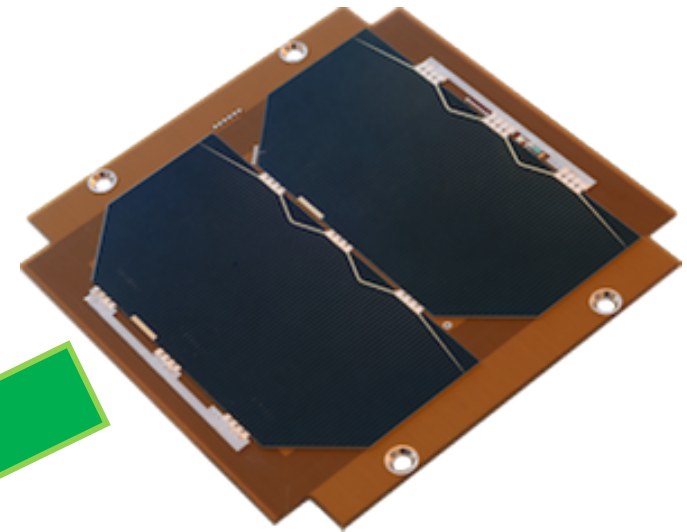
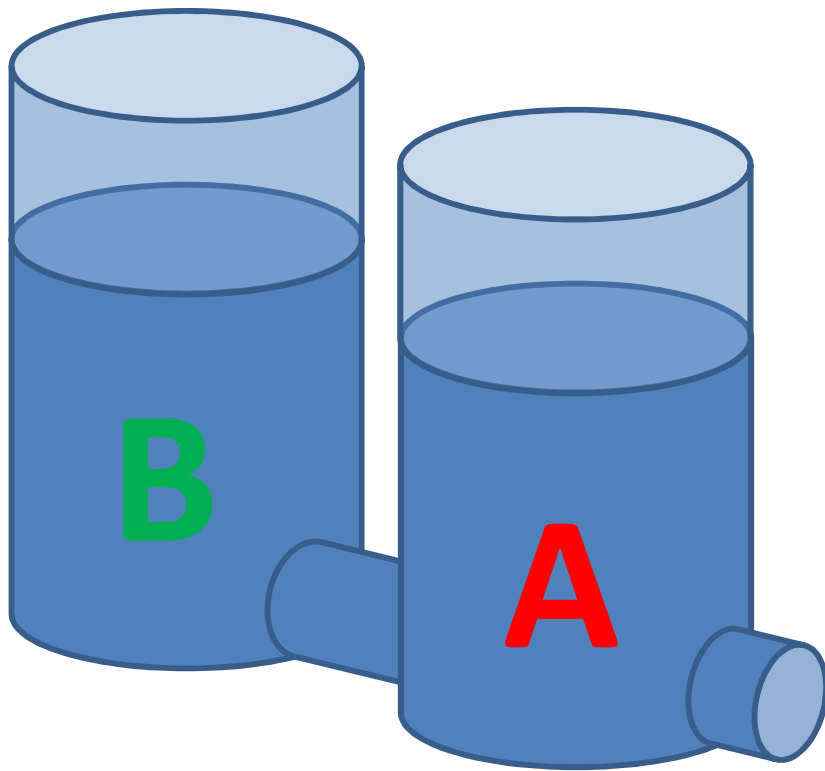
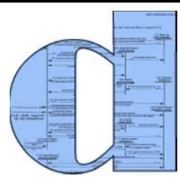
Battery Kinetics



Battery Kinetics



Battery Kinetics

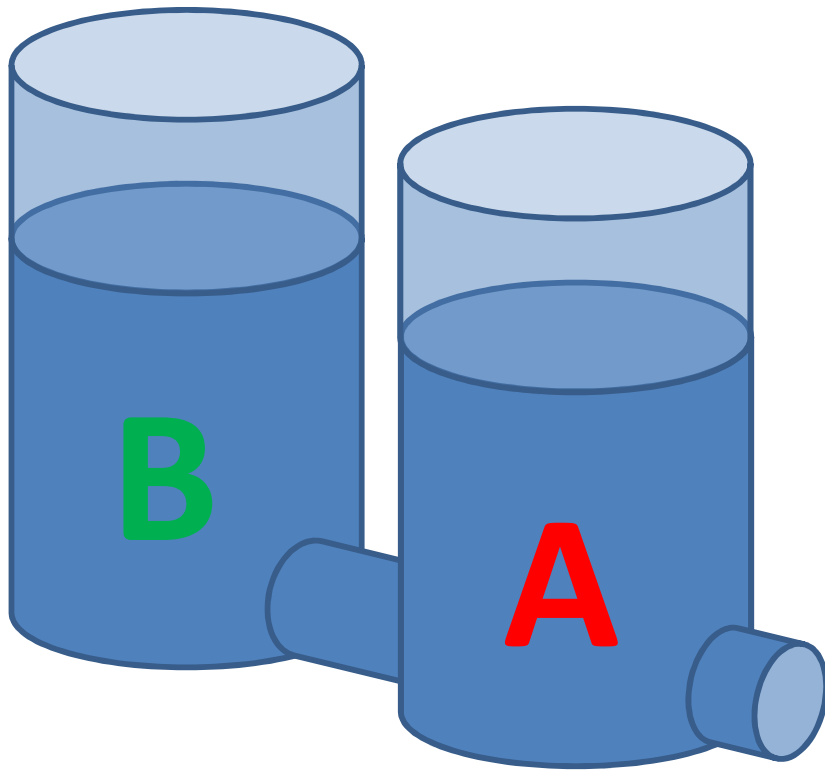
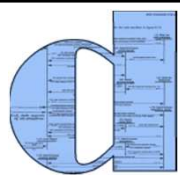


Kinetic Battery Model

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

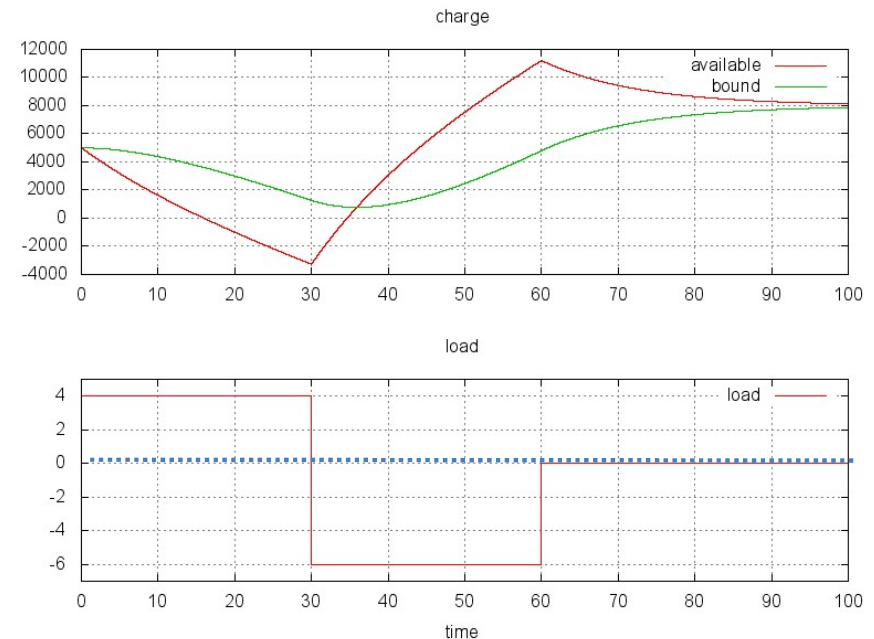
➤ *a faithful abstraction of modern battery chemistry*

Battery Kinetics



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

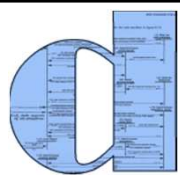
$$\dot{b}(t) = p \left(\frac{a(t)}{c} - \frac{b(t)}{1-c} \right)$$



Kinetic Battery Model

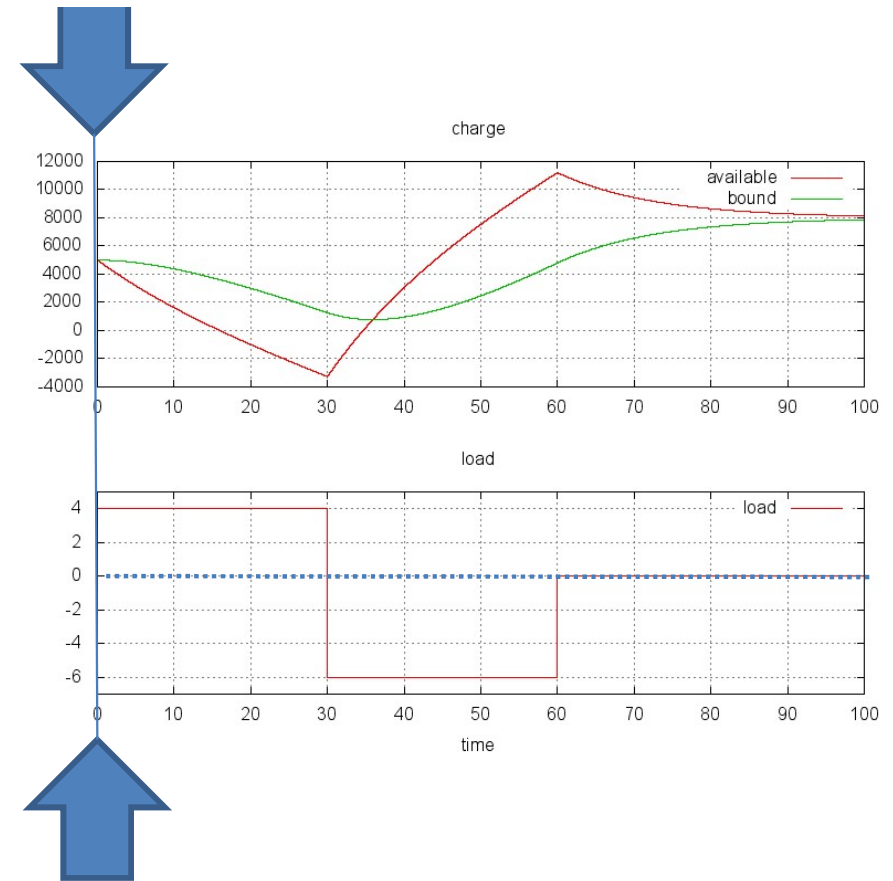
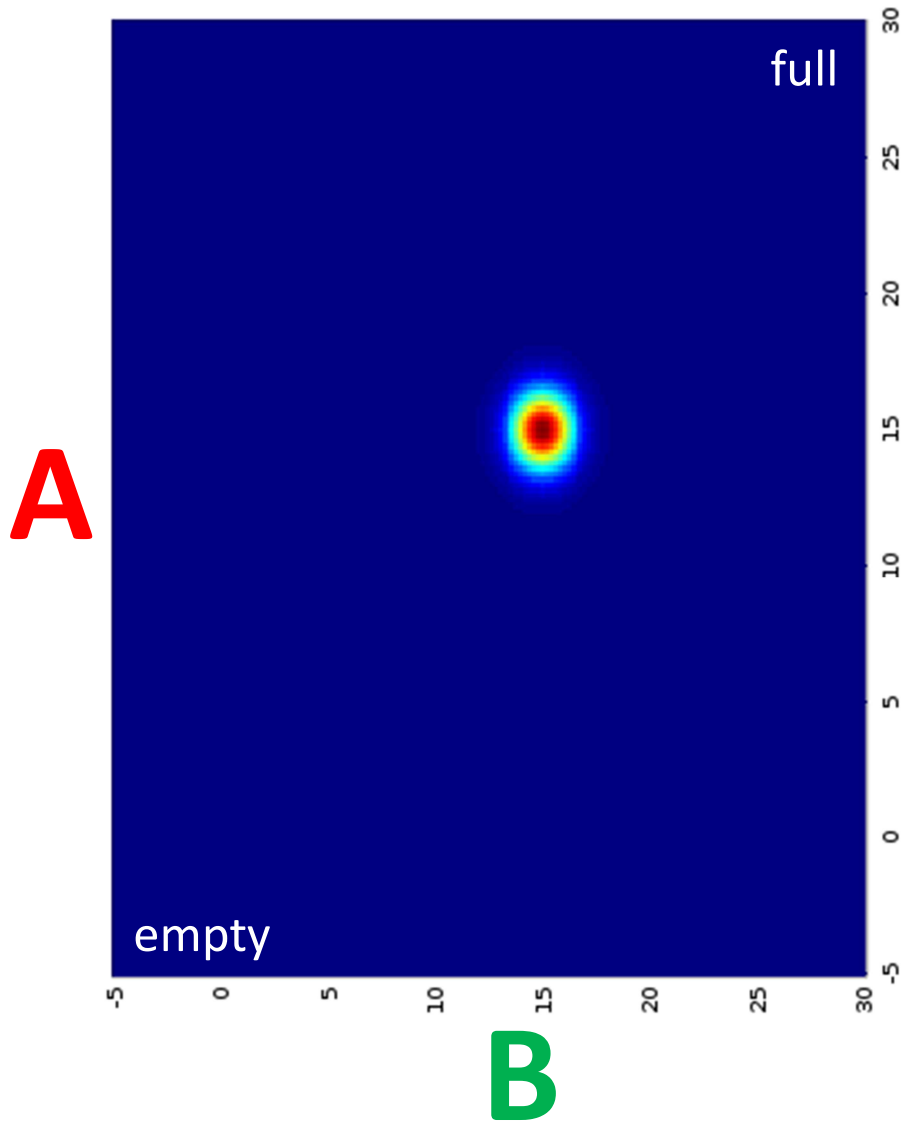
- can represent 'rate-capacity effect'
- can represent 'recovery effect'
- *a faithful abstraction of modern battery chemistry*

Battery Kinetics

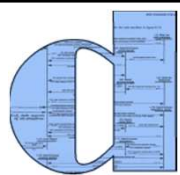


$$\dot{a}(t) = -I + p \left(\frac{b(t)}{1-c} - \frac{a(t)}{c} \right)$$

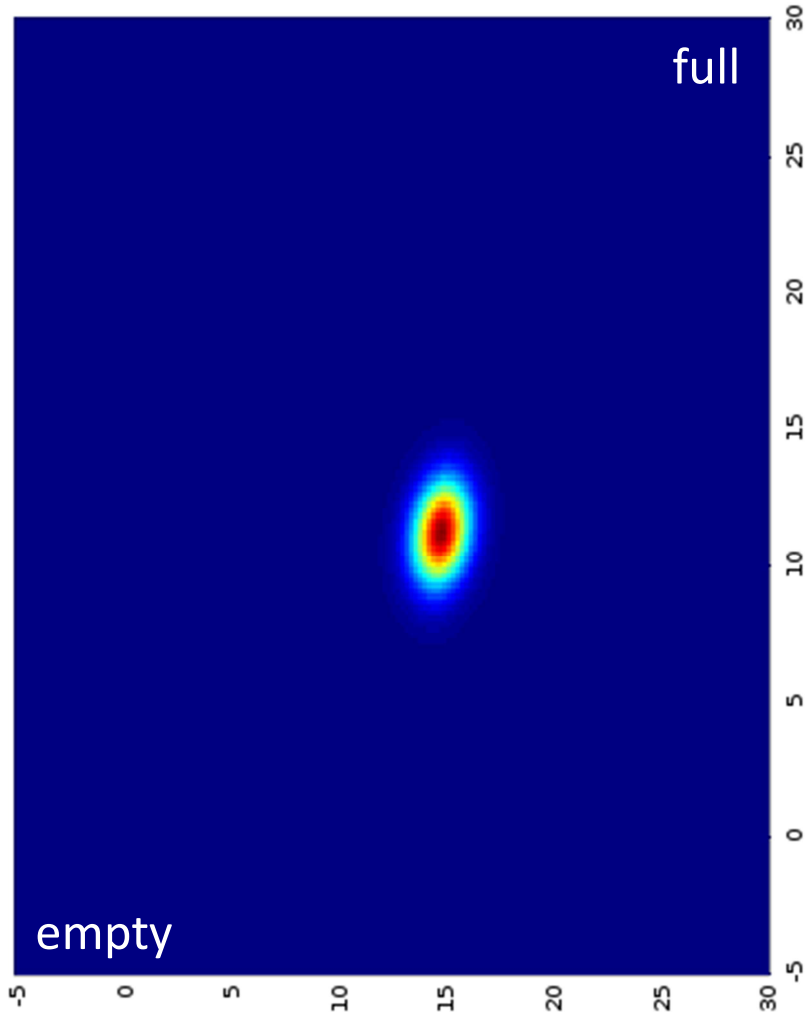
$$\dot{b}(t) = p \left(\frac{a(t)}{c} - \frac{b(t)}{1-c} \right)$$



Battery Kinetics



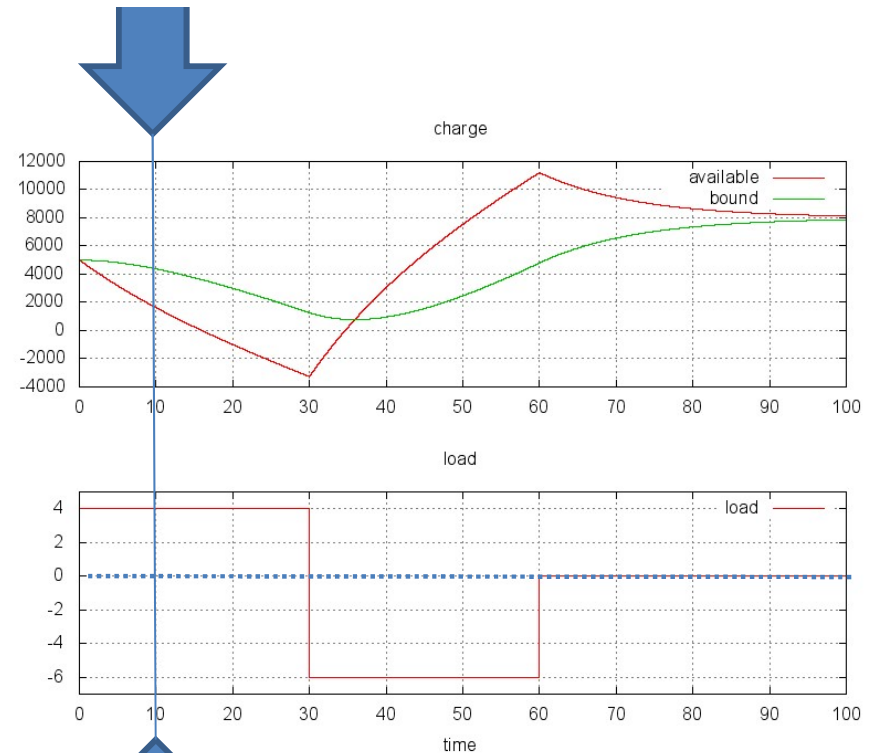
A



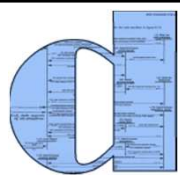
B

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

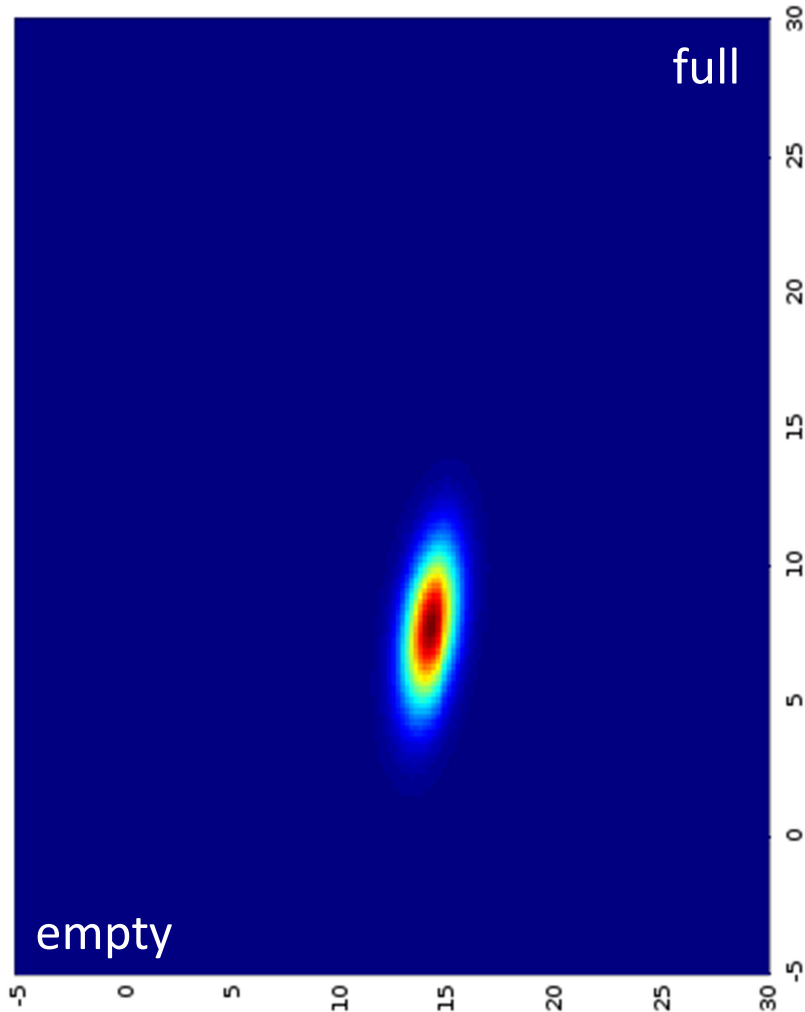
$$\dot{b}(t) = p \left(\frac{a(t)}{c} - \frac{b(t)}{1-c} \right)$$



Battery Kinetics



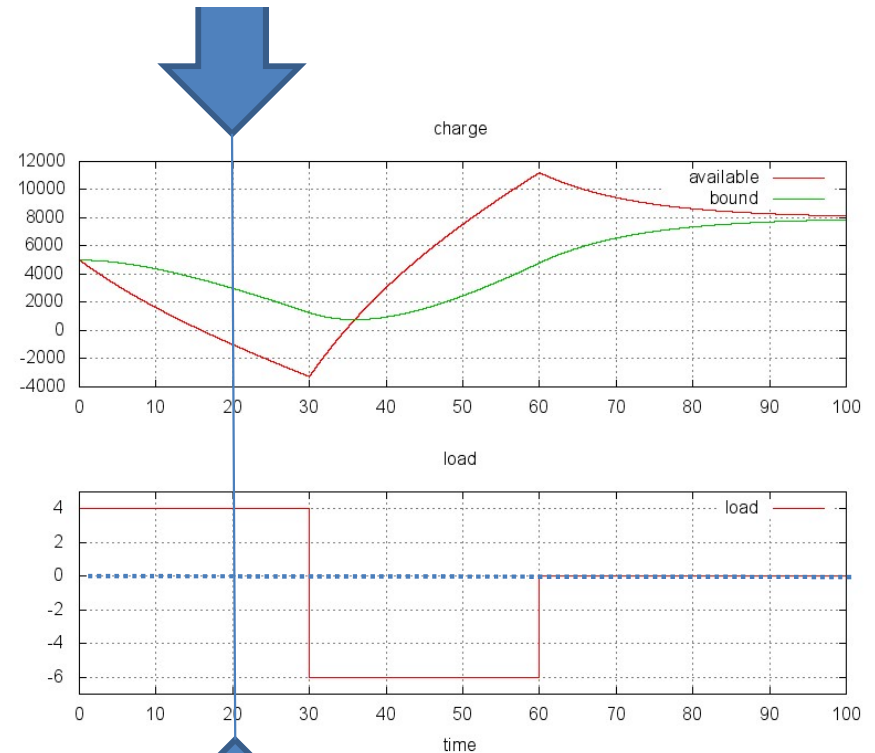
A



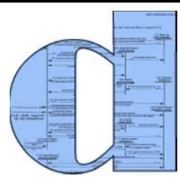
B

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

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



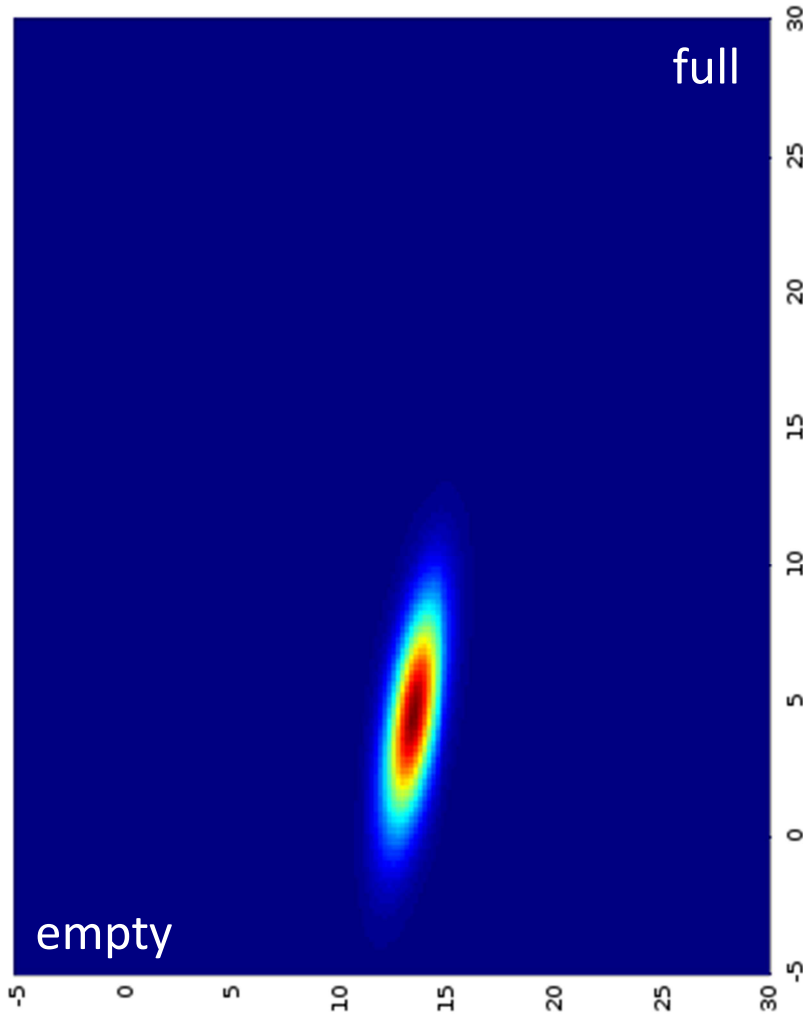
Battery Kinetics



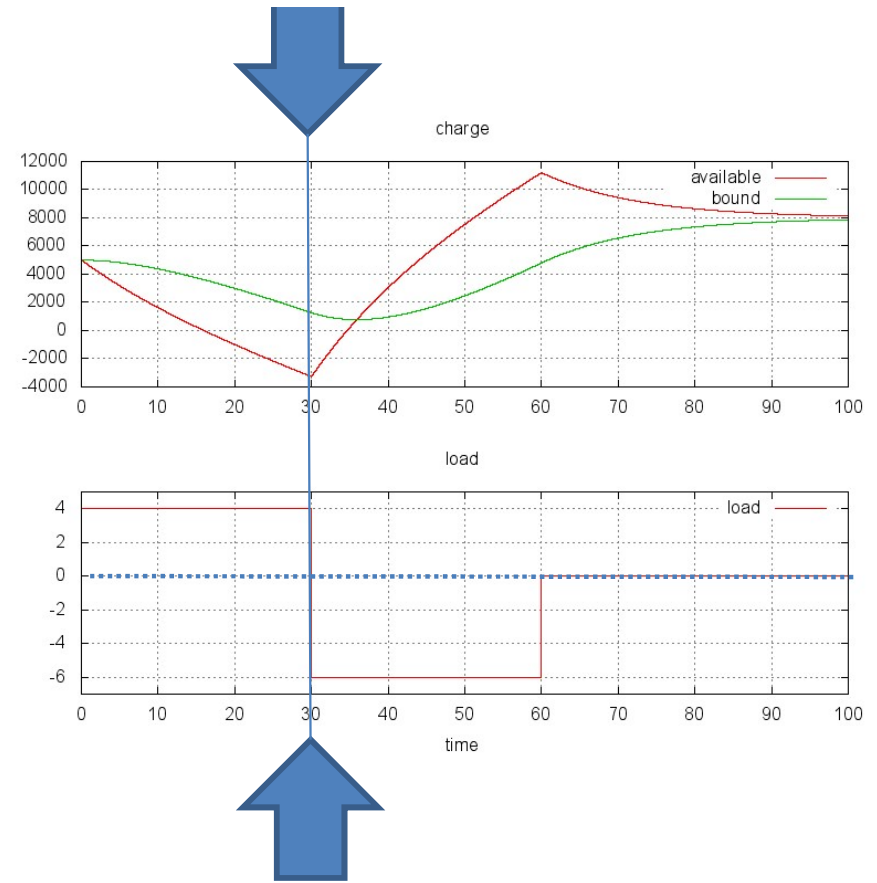
$$\dot{a}(t) = -I + p \left(\frac{b(t)}{1-c} - \frac{a(t)}{c} \right)$$

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

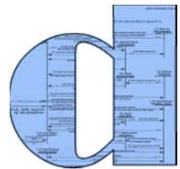
A



B



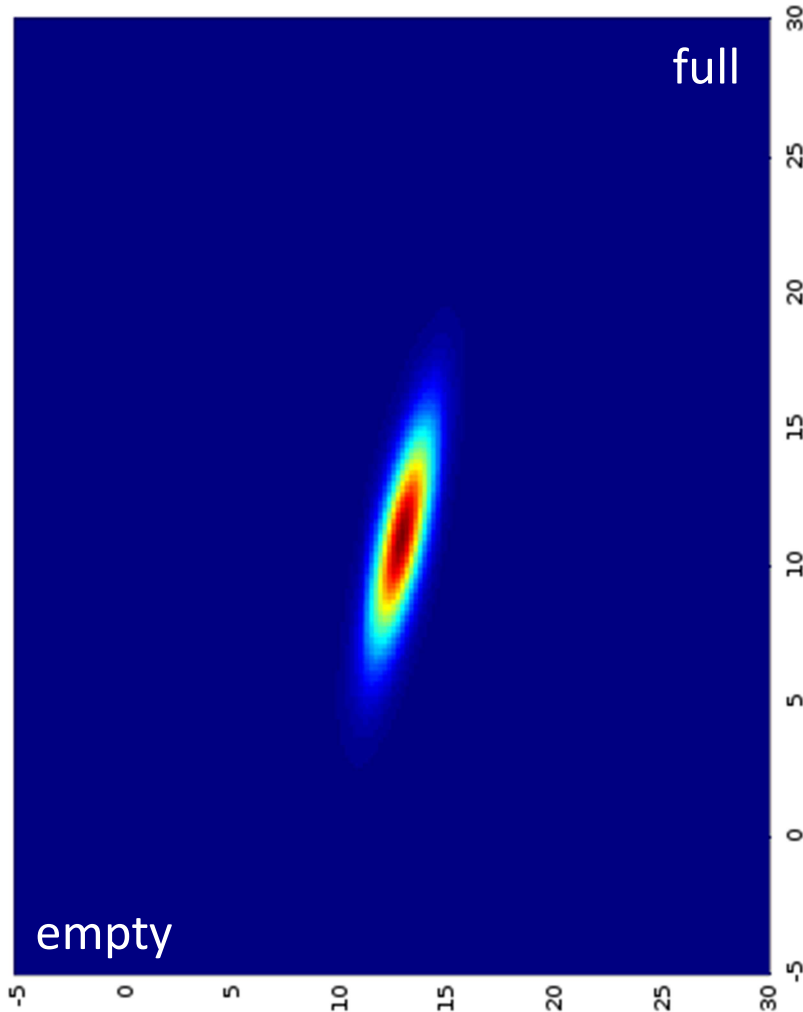
Battery Kinetics



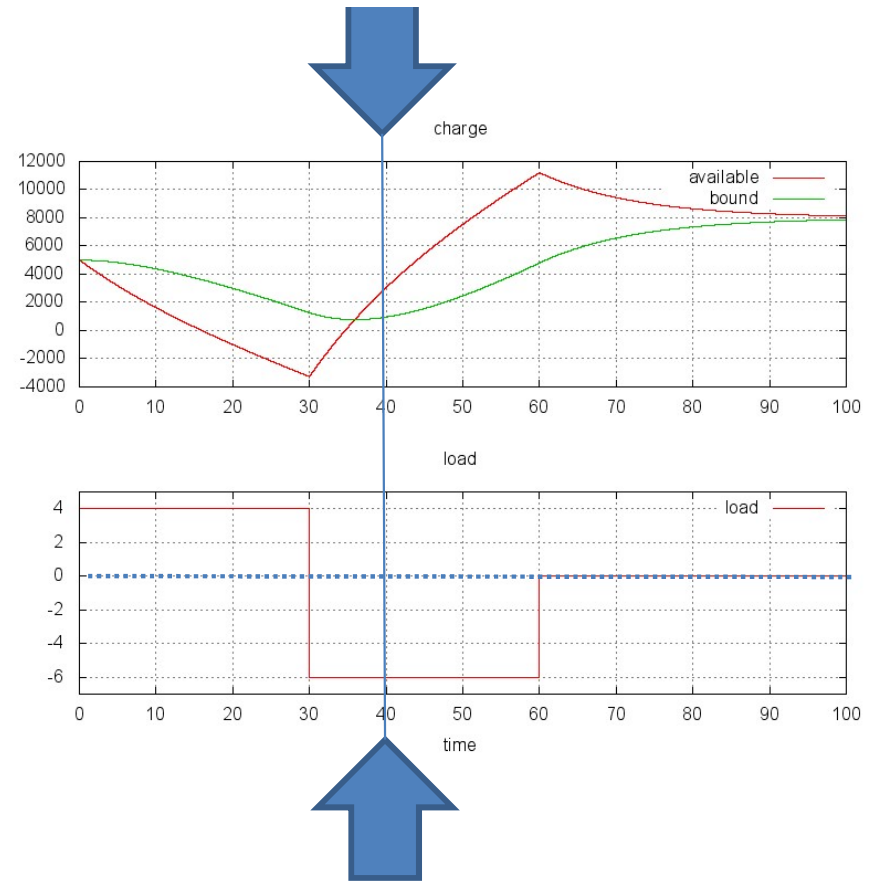
$$\dot{a}(t) = -I + p \left(\frac{b(t)}{1-c} - \frac{a(t)}{c} \right)$$

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

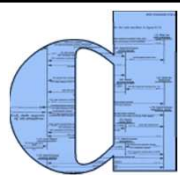
A



B



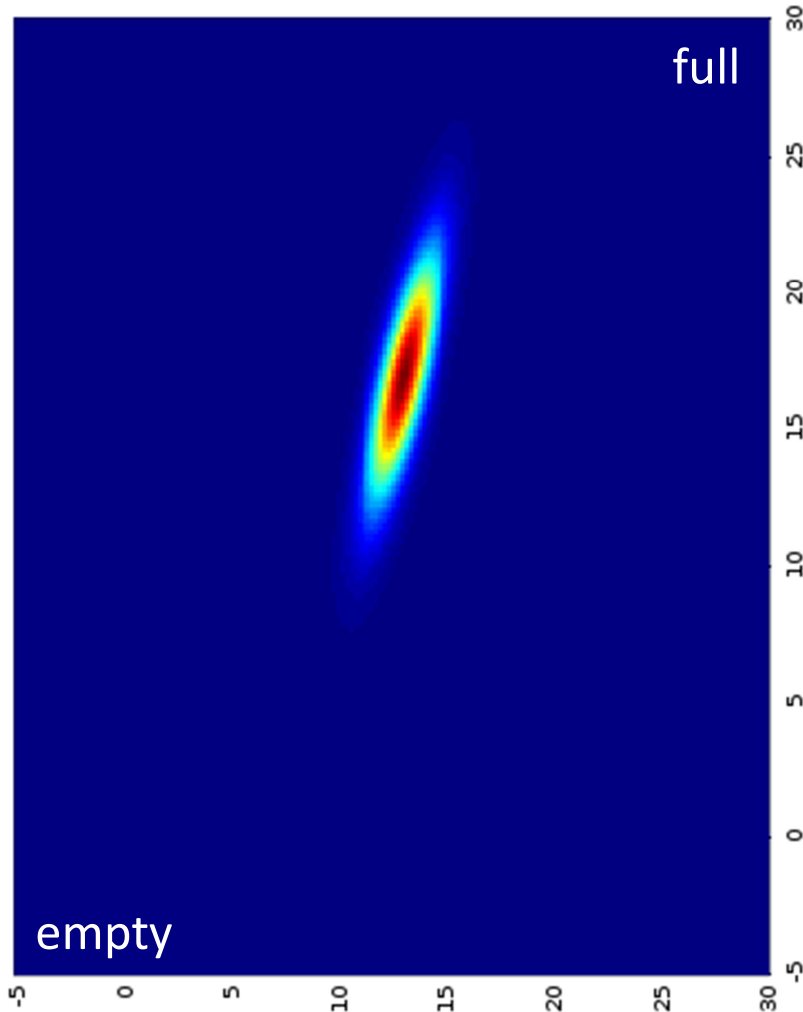
Battery Kinetics



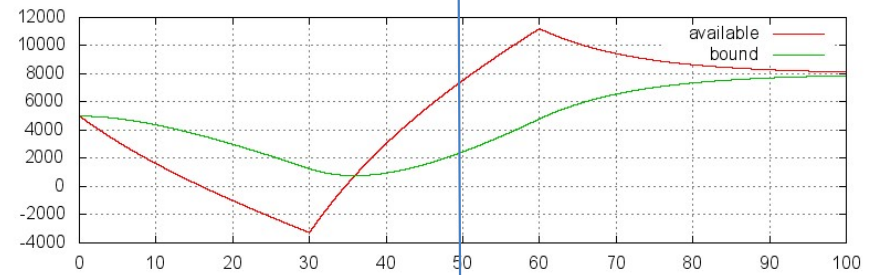
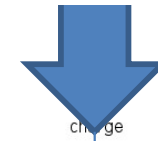
$$\dot{a}(t) = -I + p \left(\frac{b(t)}{1-c} - \frac{a(t)}{c} \right)$$

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

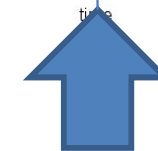
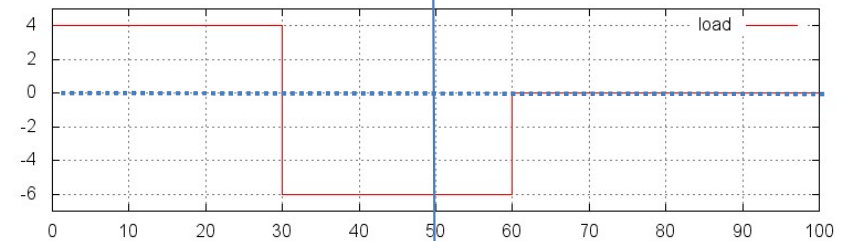
A



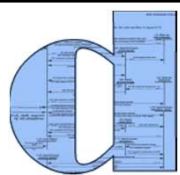
B



load



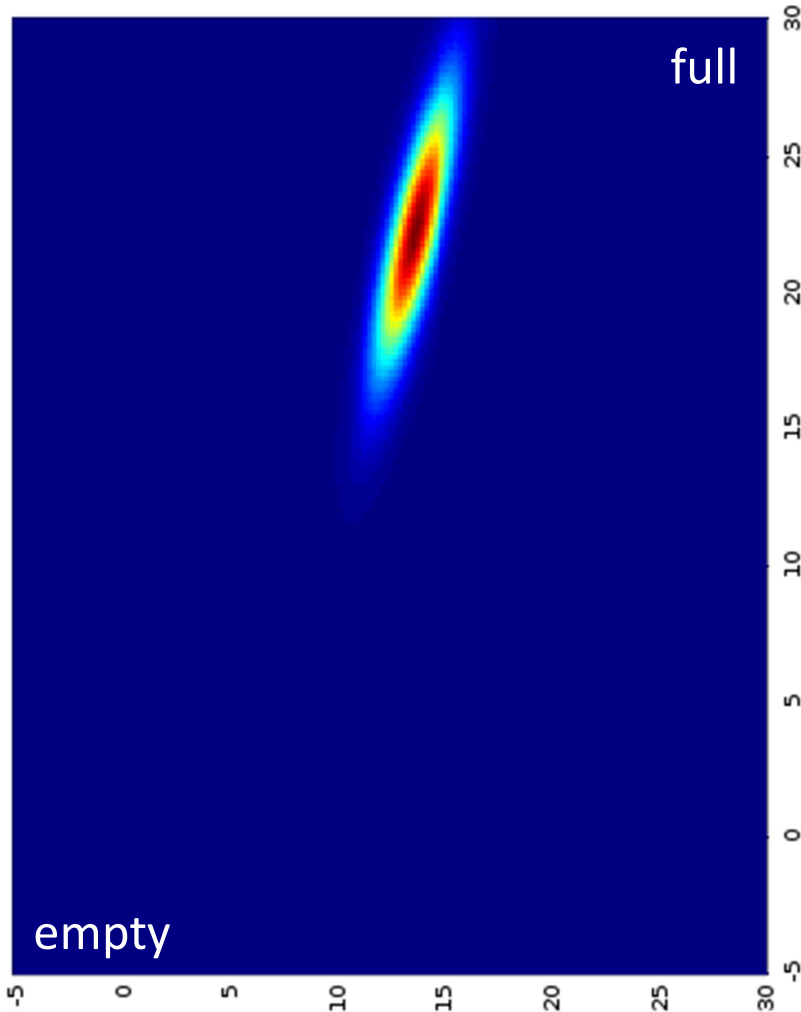
Battery Kinetics



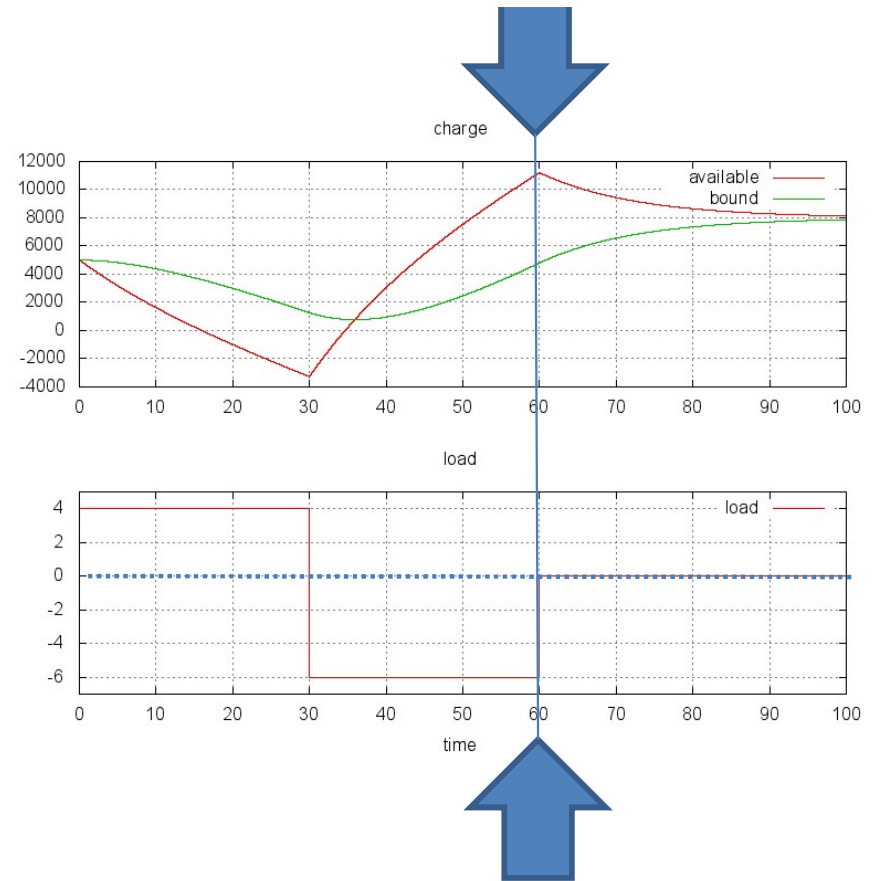
$$\dot{a}(t) = -I + p \left(\frac{b(t)}{1-c} - \frac{a(t)}{c} \right)$$

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

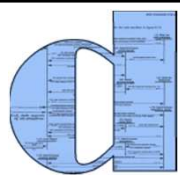
A



B



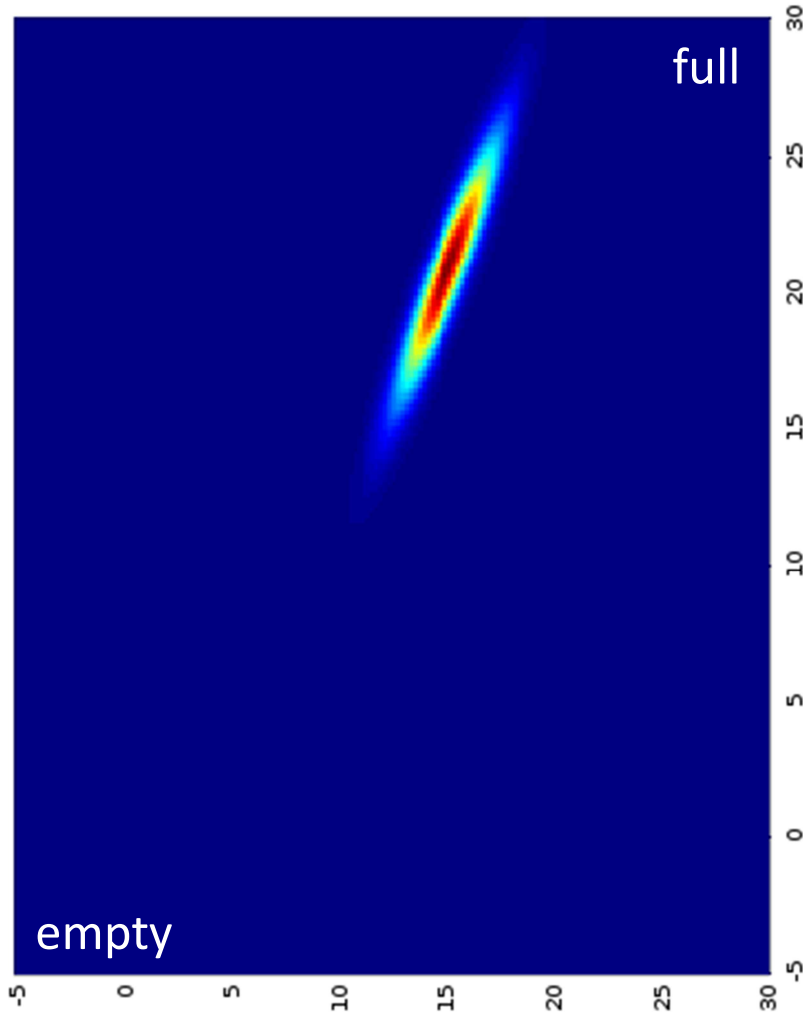
Battery Kinetics



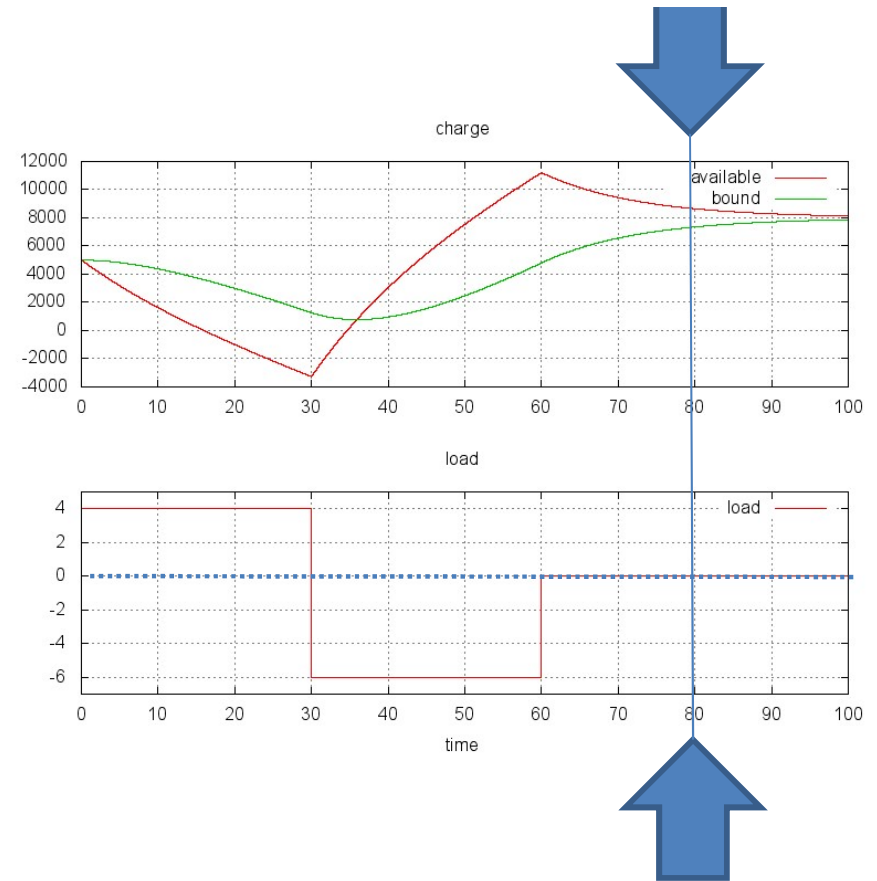
$$\dot{a}(t) = -I + p \left(\frac{b(t)}{1-c} - \frac{a(t)}{c} \right)$$

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

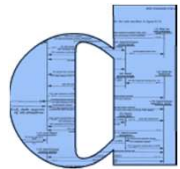
A



B



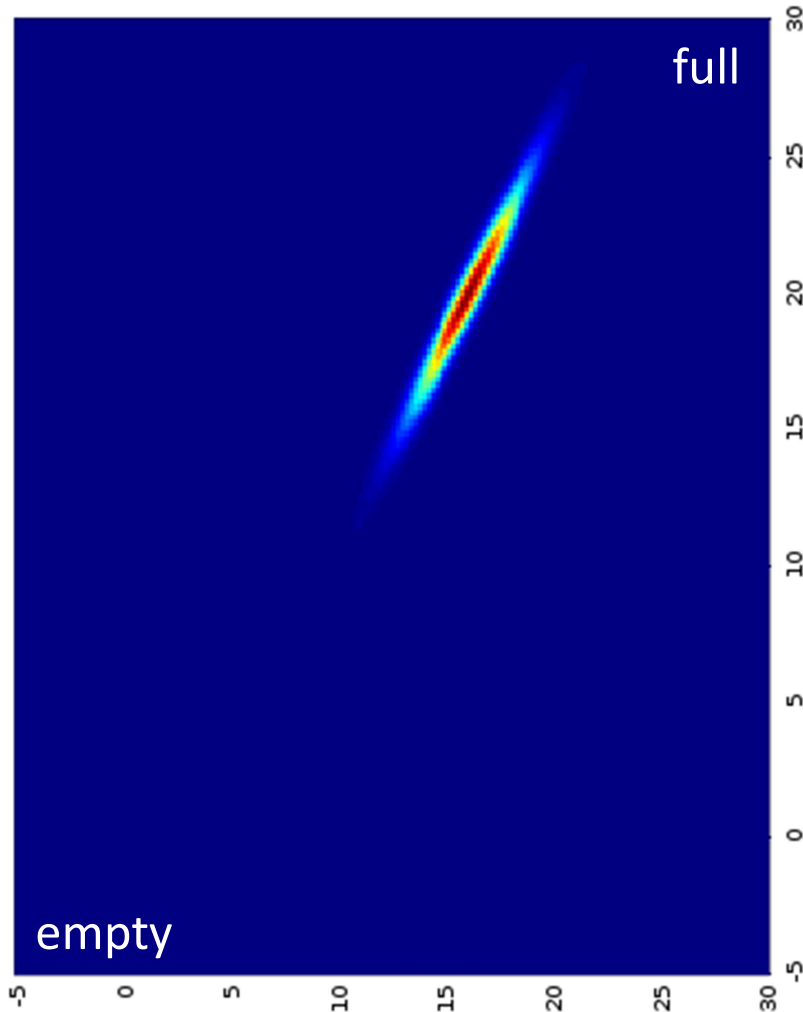
Battery Kinetics



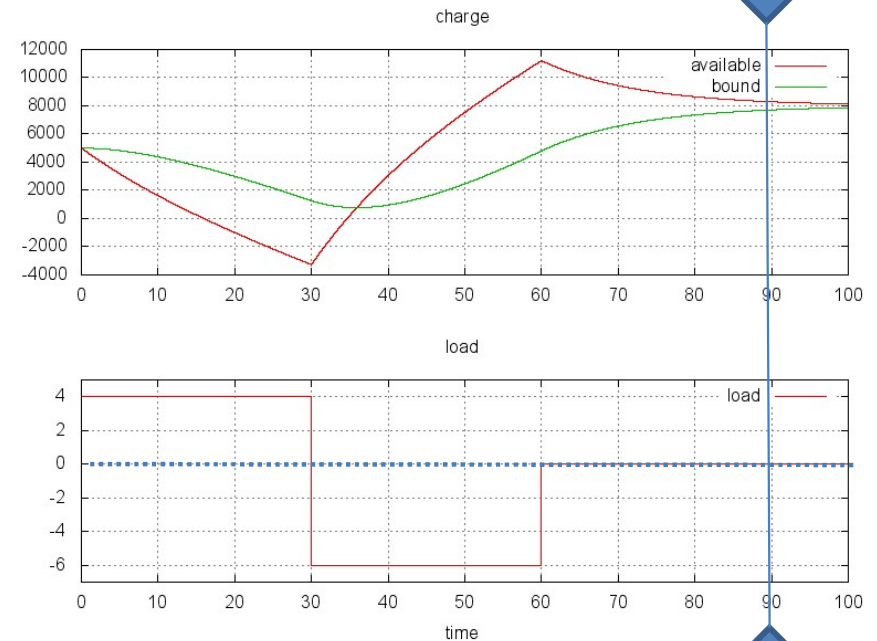
$$\dot{a}(t) = -I + p \left(\frac{b(t)}{1-c} - \frac{a(t)}{c} \right)$$

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

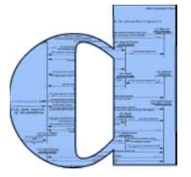
A



B



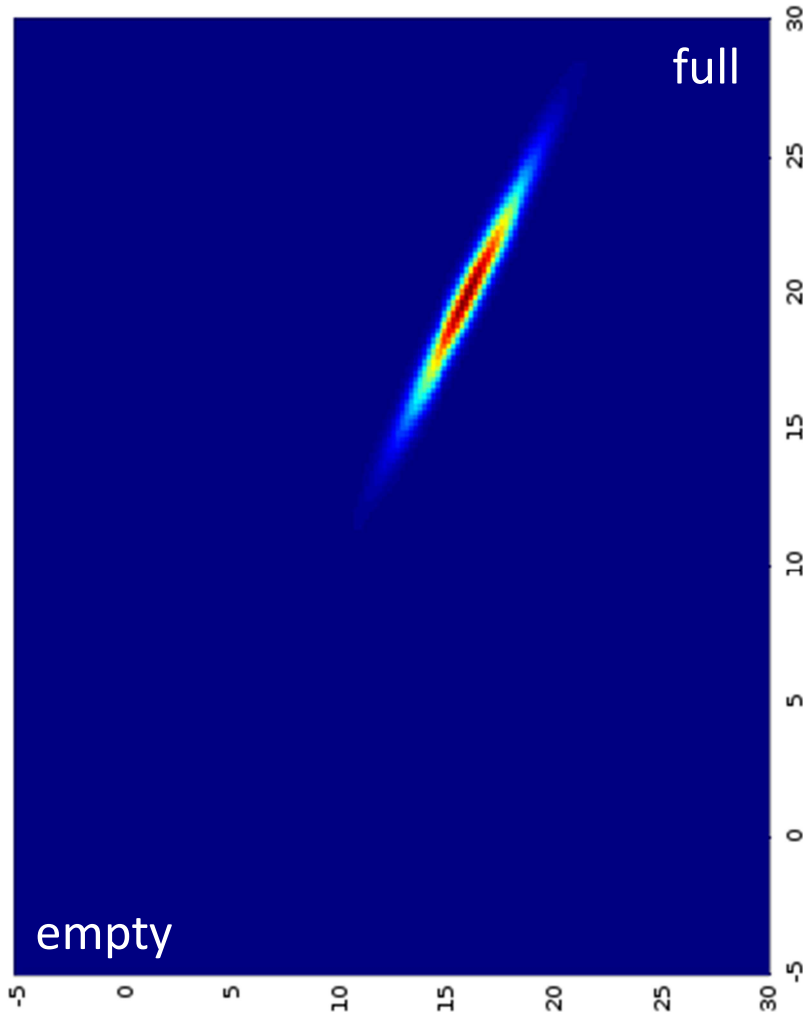
Battery Kinetics



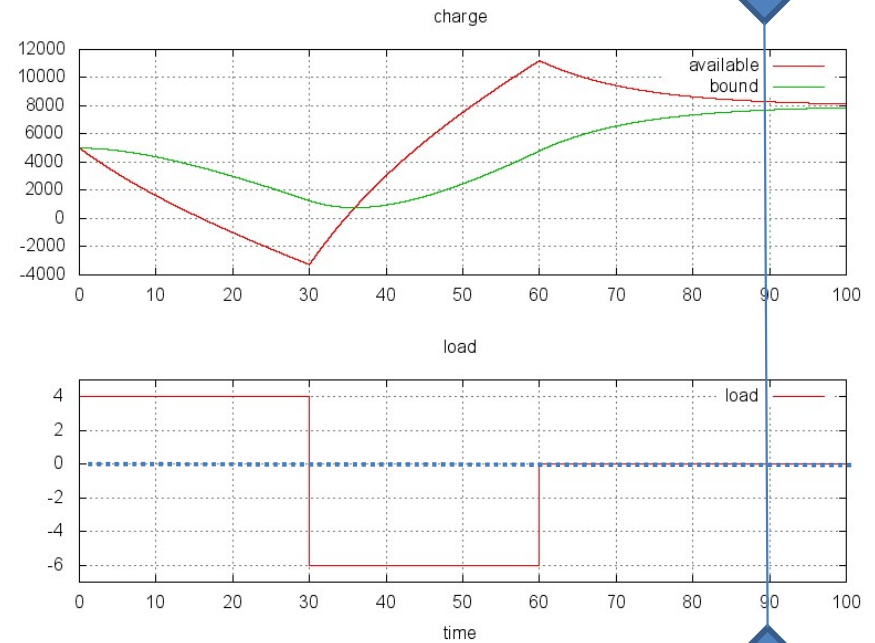
$$\dot{a}(t) = -I + p \left(\frac{b(t)}{1-c} - \frac{a(t)}{c} \right)$$

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

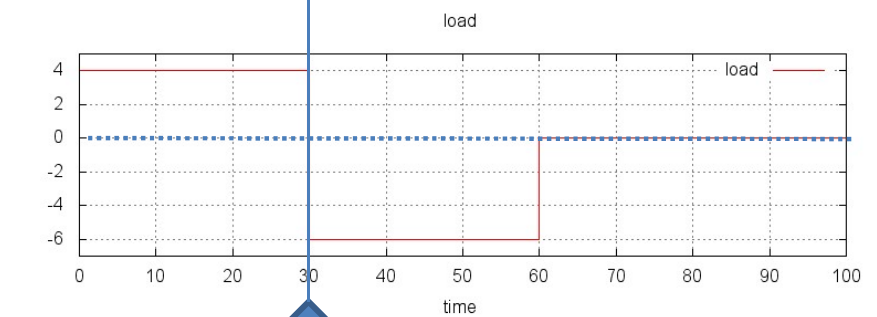
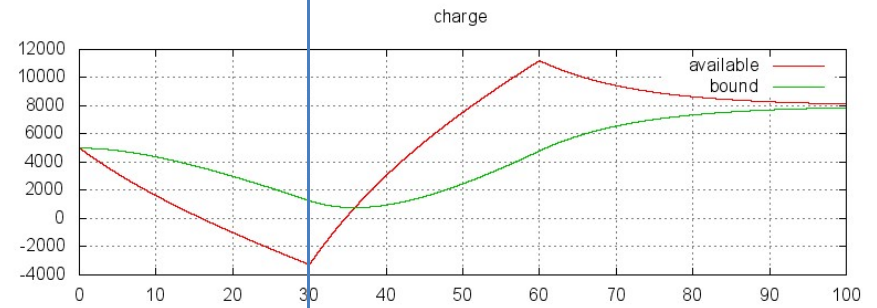
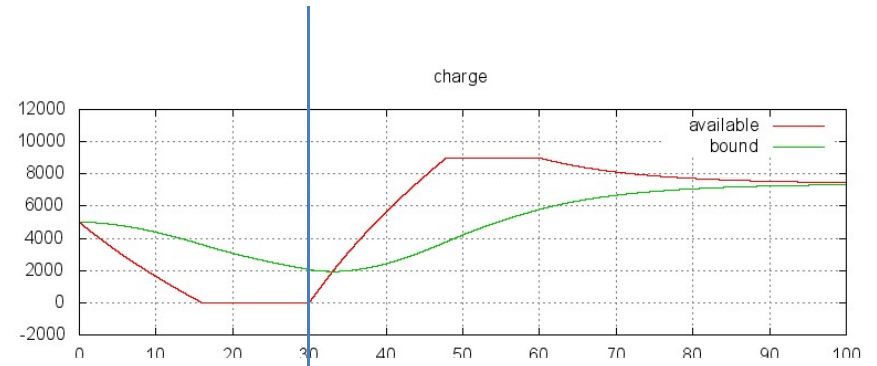
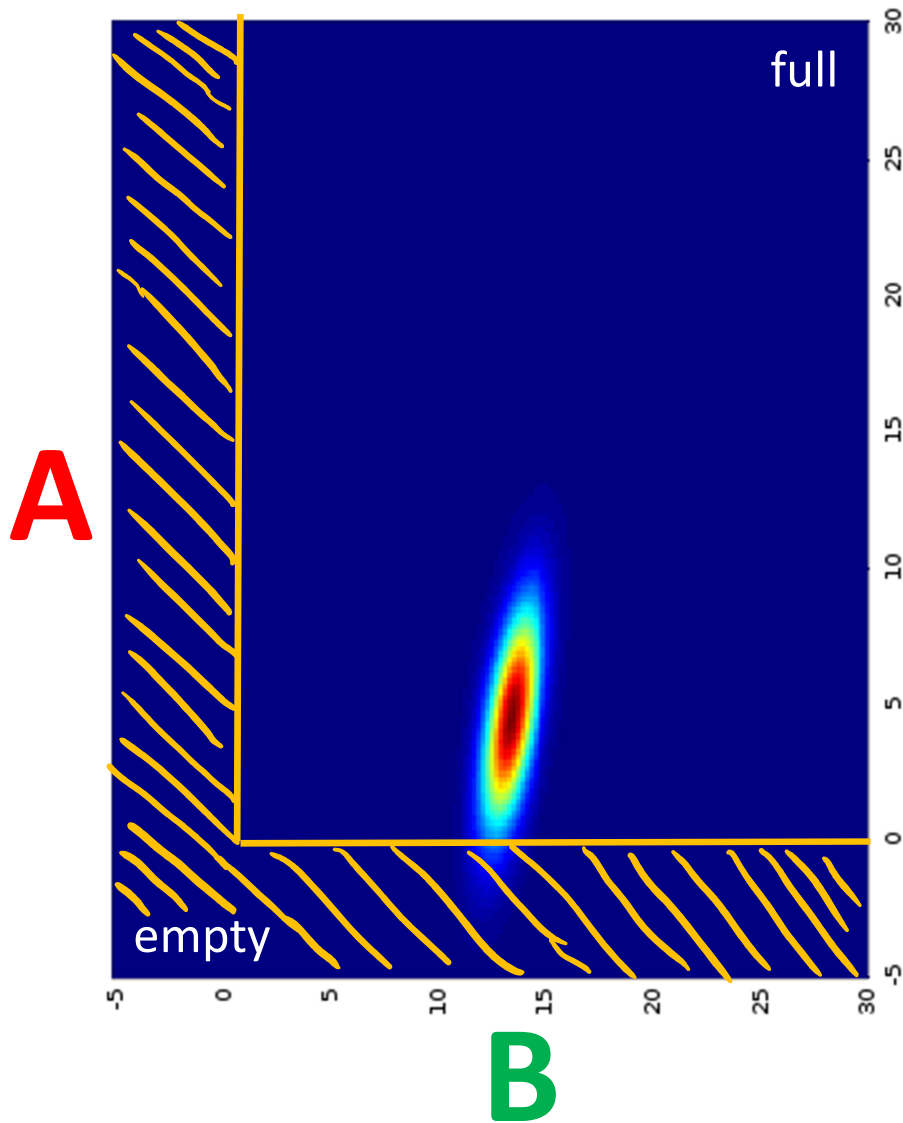
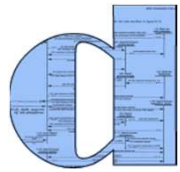
A



B

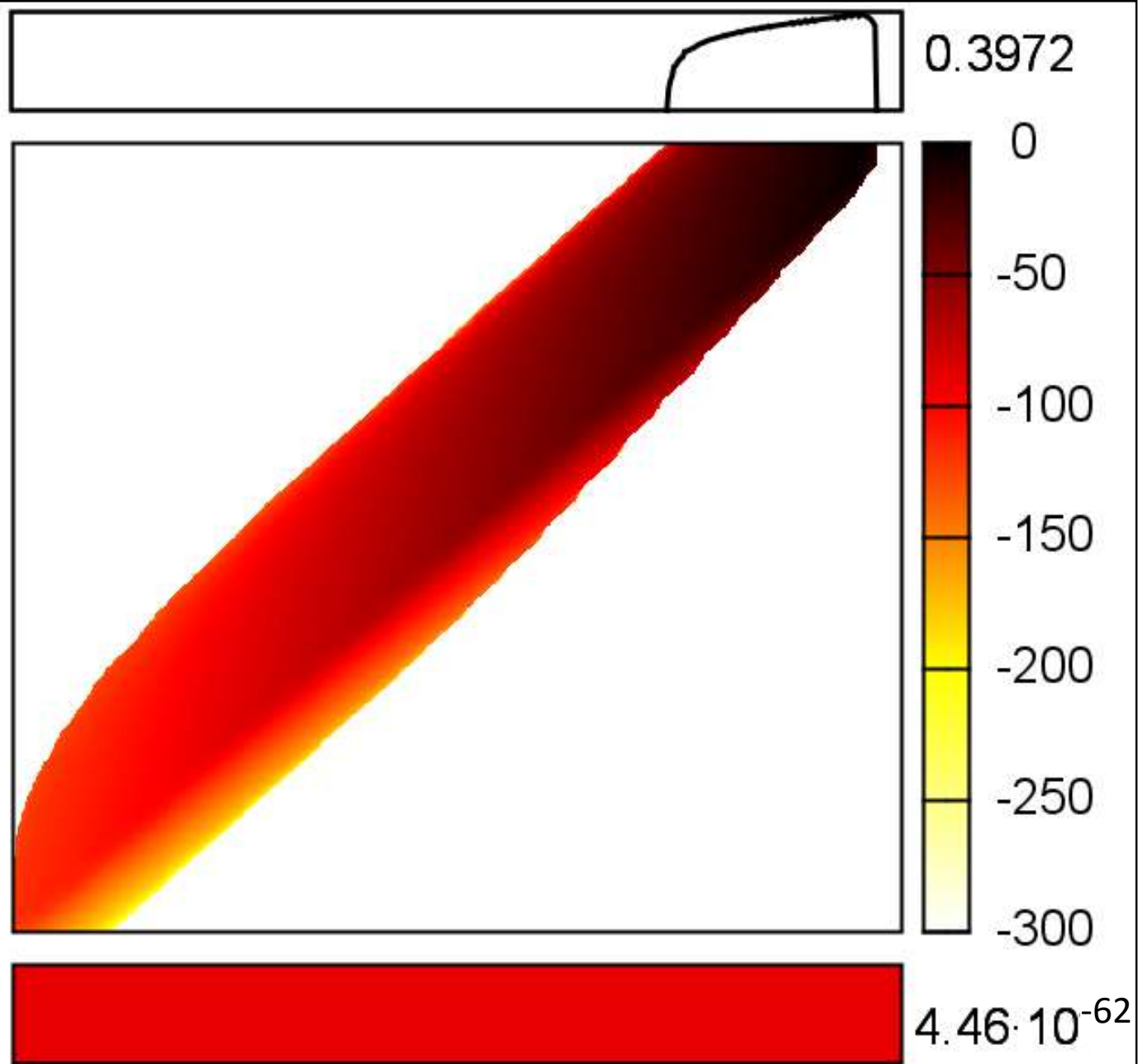
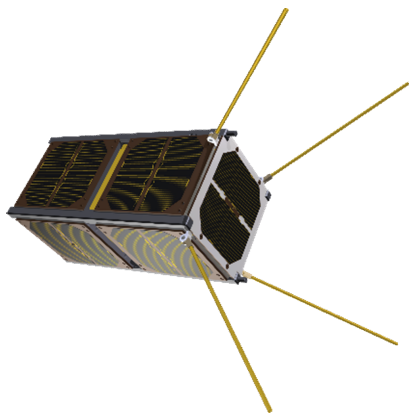


Battery Kinetics



Concretely.

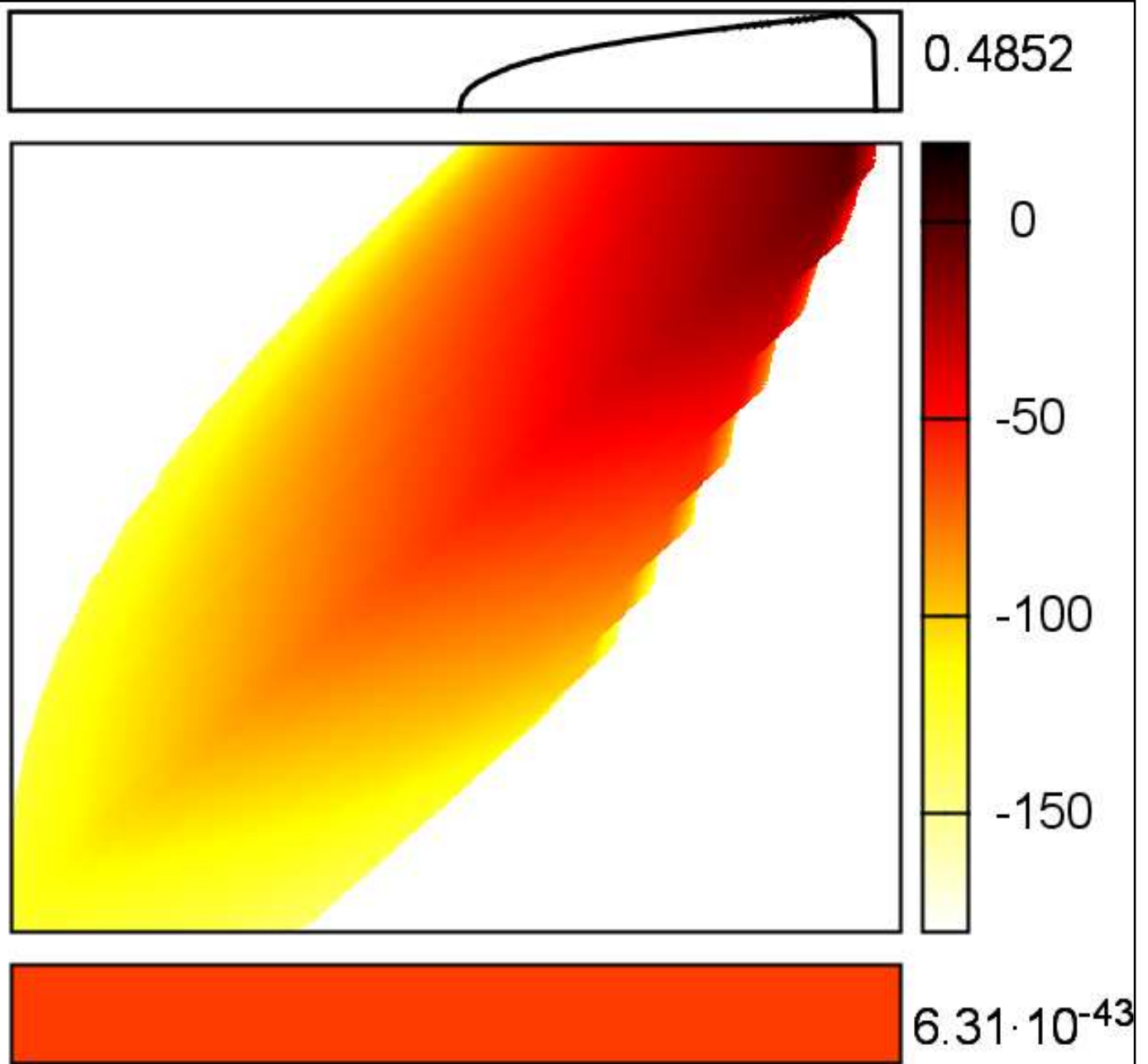
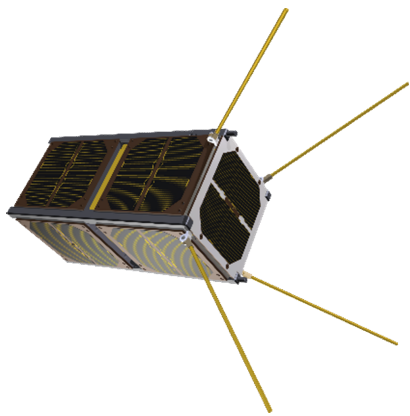
Will the battery survive a one-year mission?



with 5000 mAh

Concretely.

Will the battery survive a one-year mission?

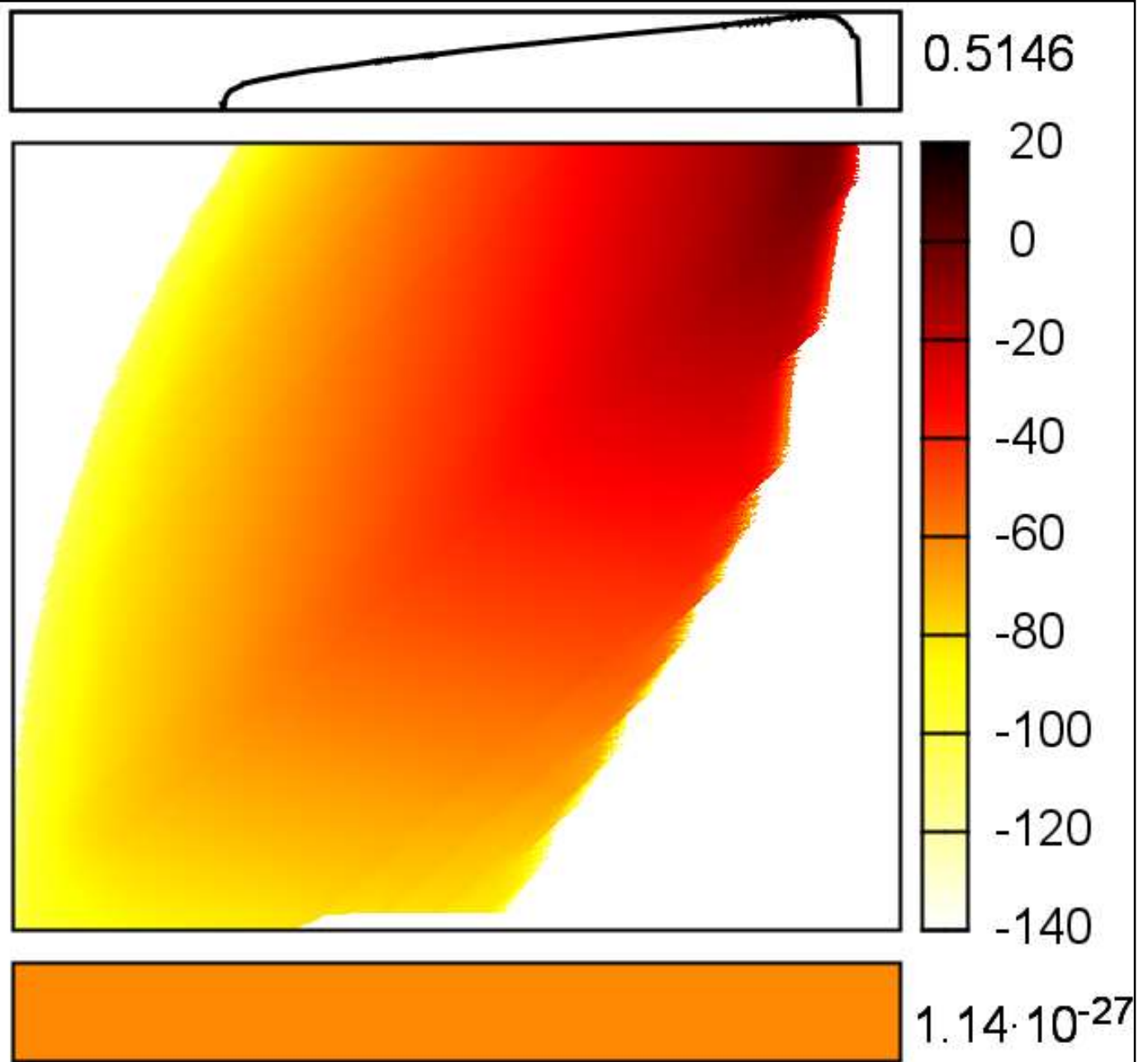
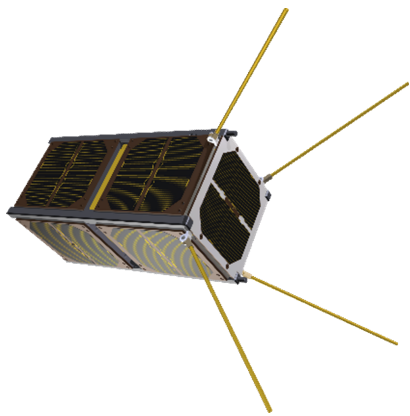


With half the capacity?

2500 mAh

Concretely.

Will the battery survive a one-year mission?

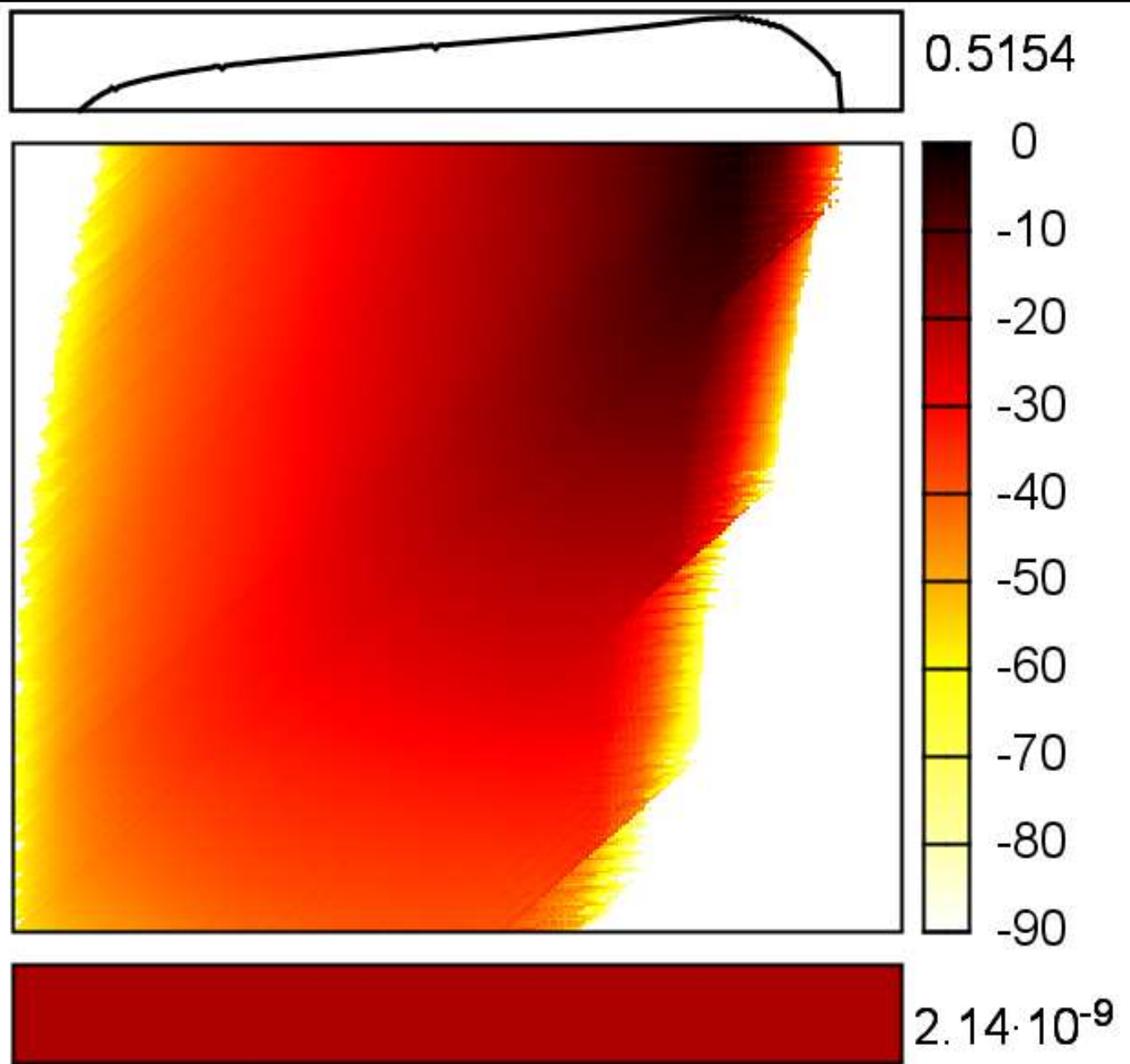
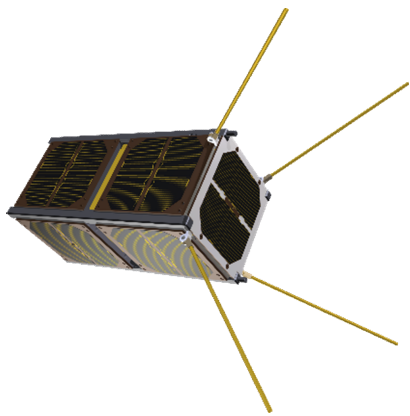


With a quarter of the capacity?

1250 mAh

Concretely.

Will the battery survive a one-year mission?

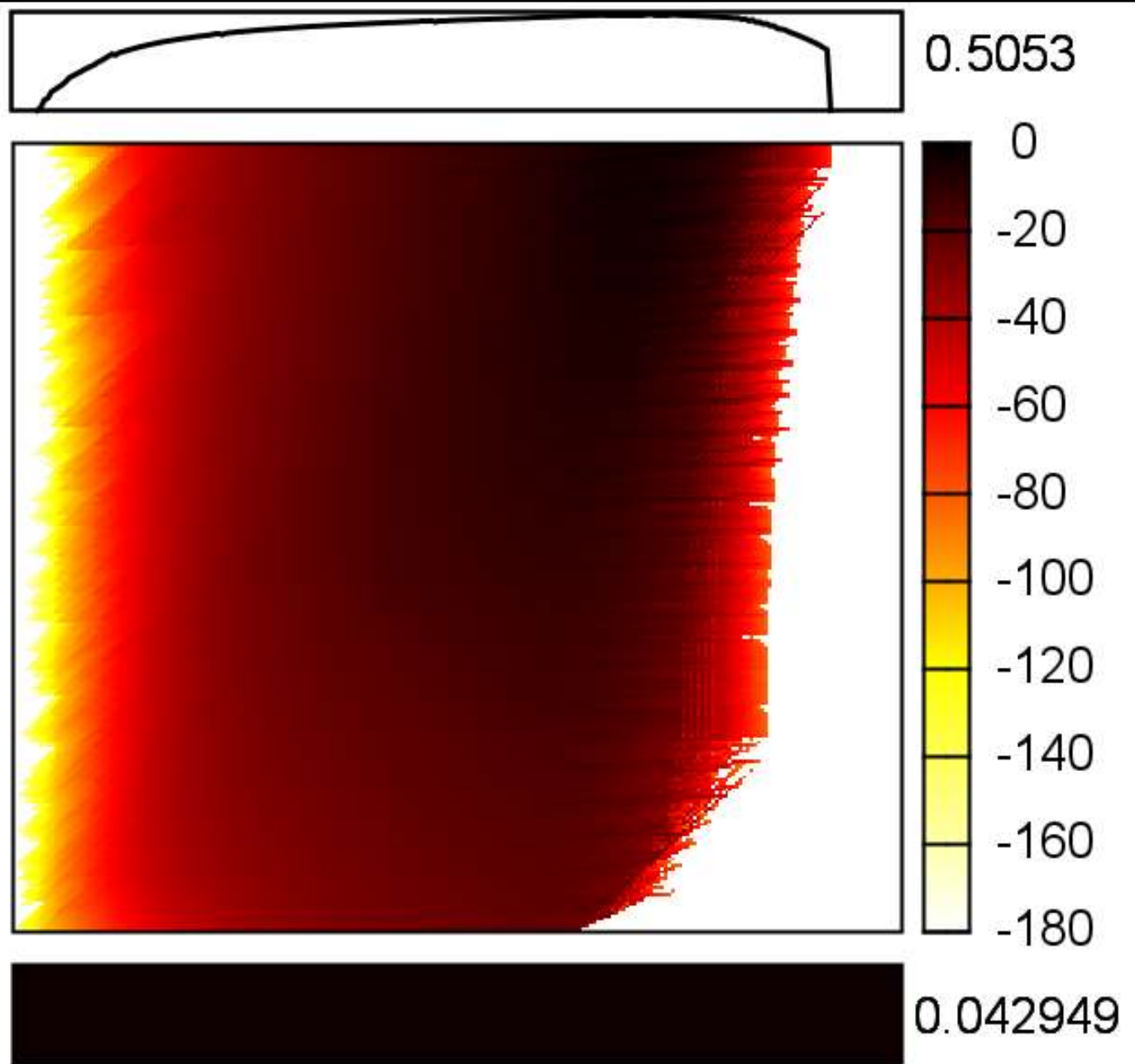
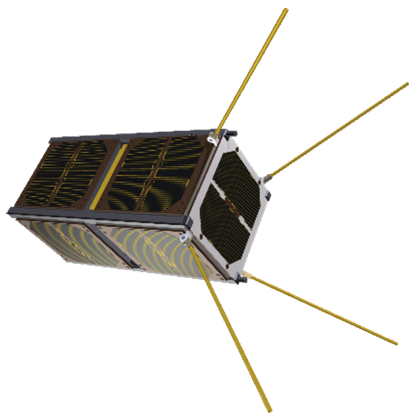


With an eighth of the capacity ?

625 mAh

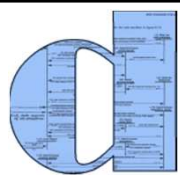
Concretely.

**Will the
battery
survive a
one-year
mission?**



With a sixteenth of the capacity ?

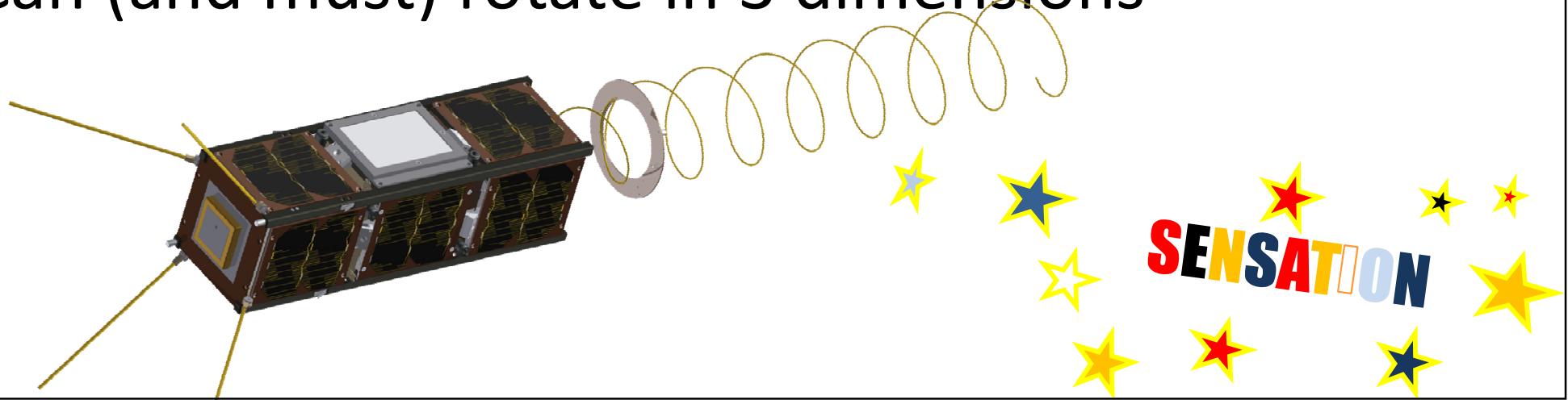
312.5 mAh

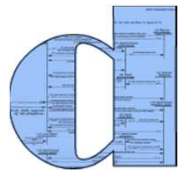


- 2U CubeSat (2 liter)
- Shipped in October 2014
with Cygnus CRS-3 towards ISS
- Payloads:
 - Optical communication experiments from NUS
 - Highspeed UHF and SDR receiver
- Shipping failed after liftoff
- Satellite was recovered from wreckage and returned to GomSpace



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





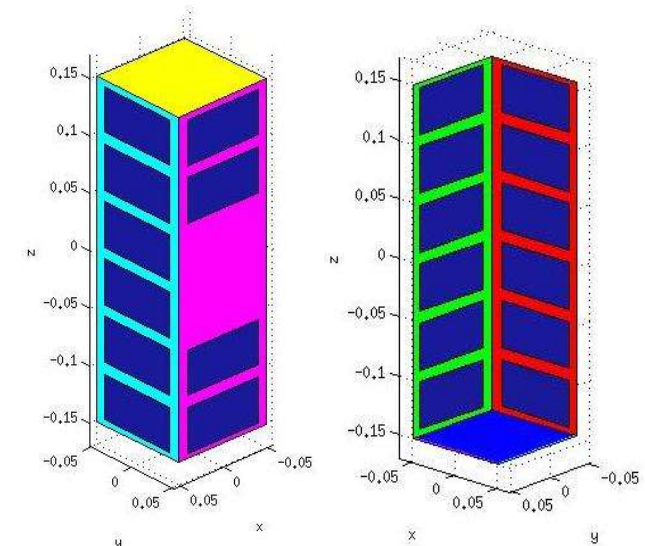
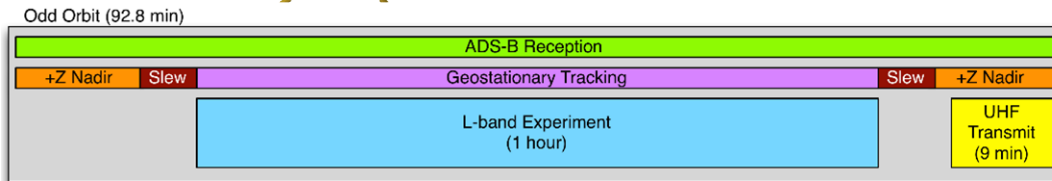
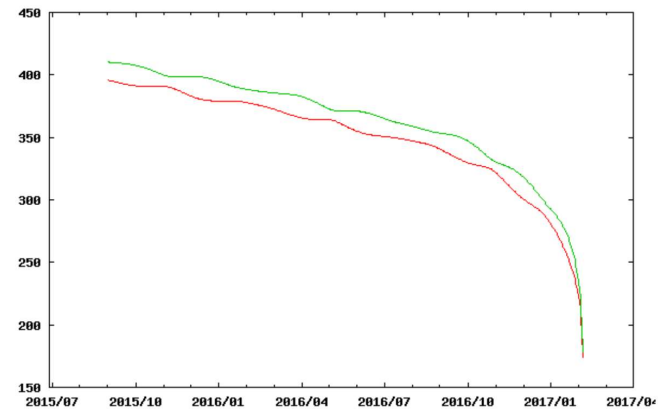
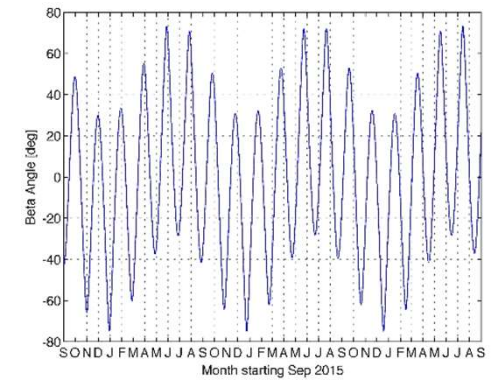
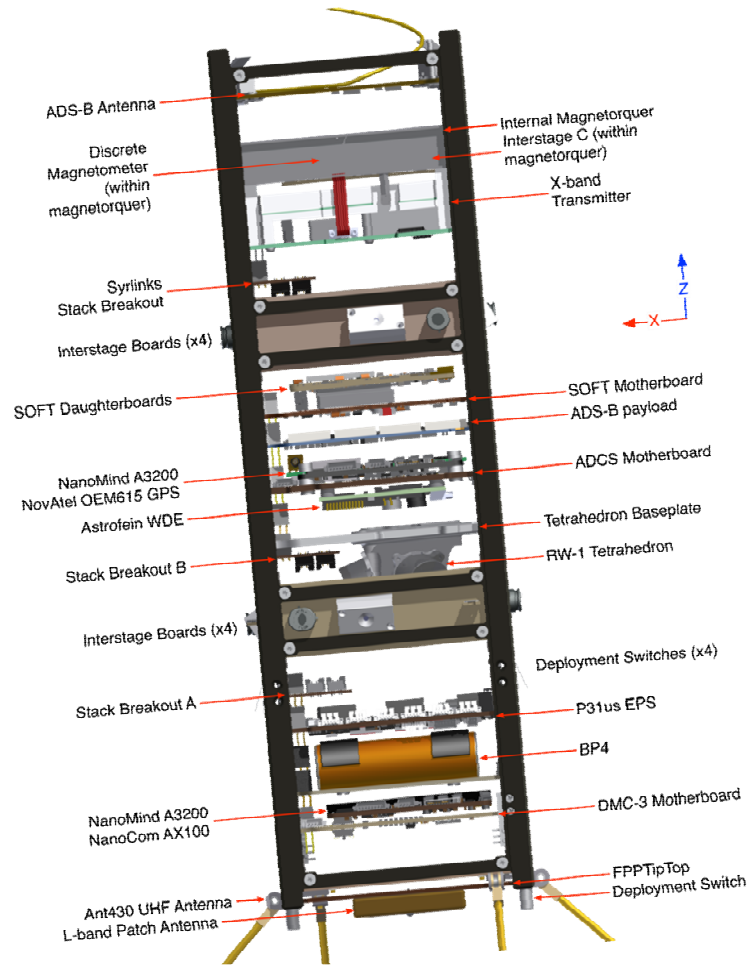
- Two 6U CubeSats (6 liter)
- Launch expected in 2016
- Initial design in the making
- Focus on support for flexible payload model

“Satellite-as-a-Service”

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

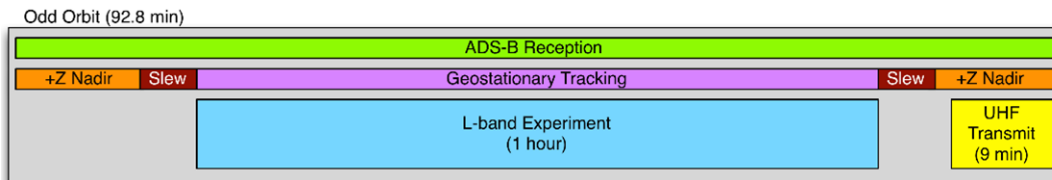
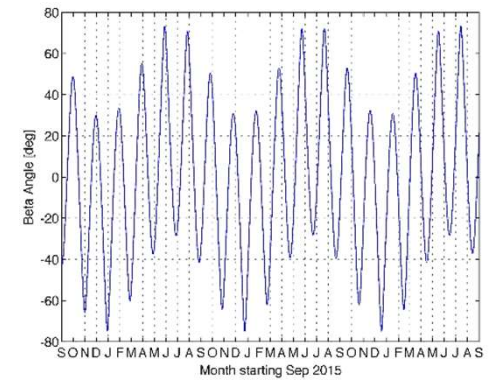


GOMX-3 mission details



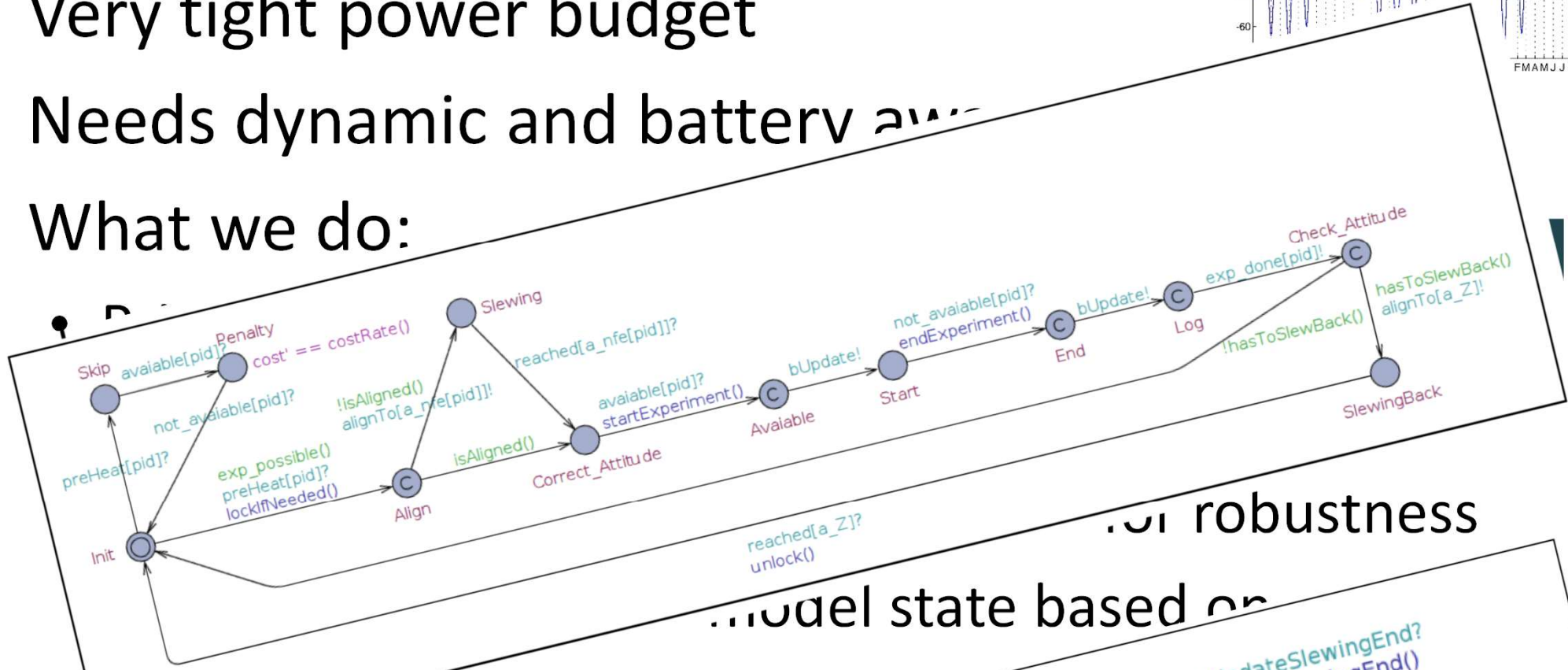
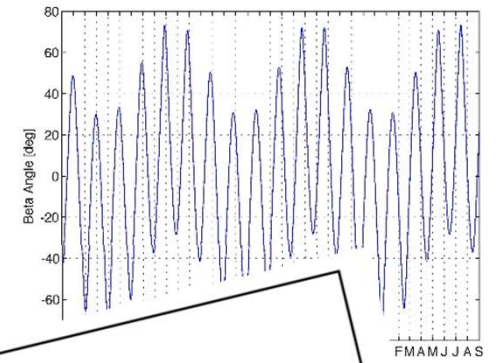
GOMX-3 mission planning

- 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

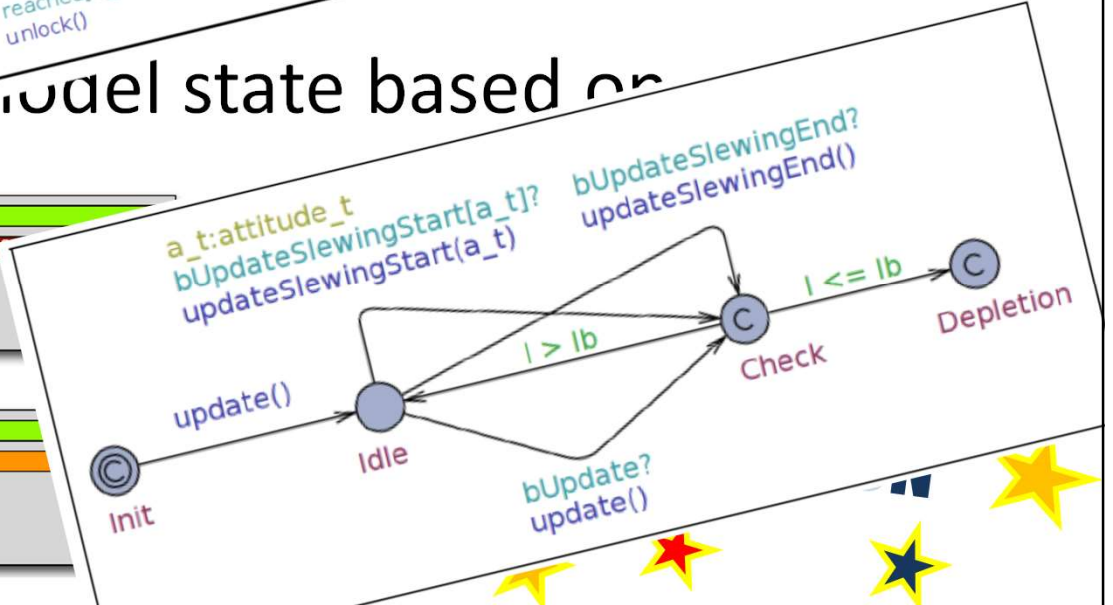
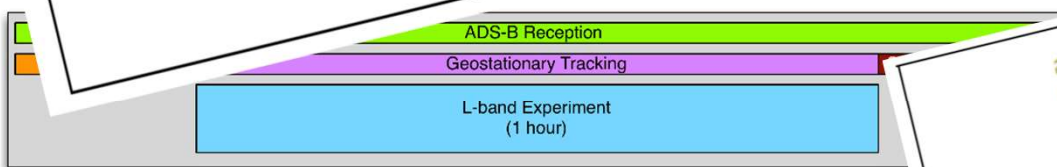


GOMX-3 mission planning

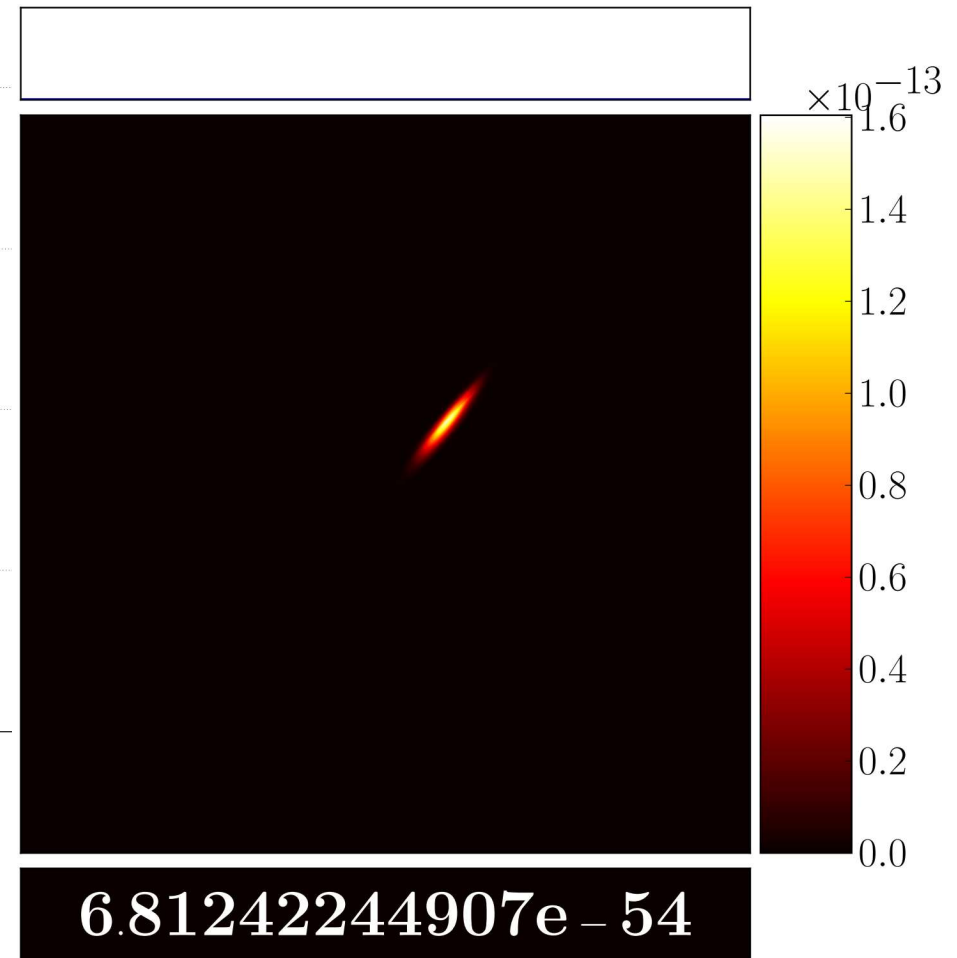
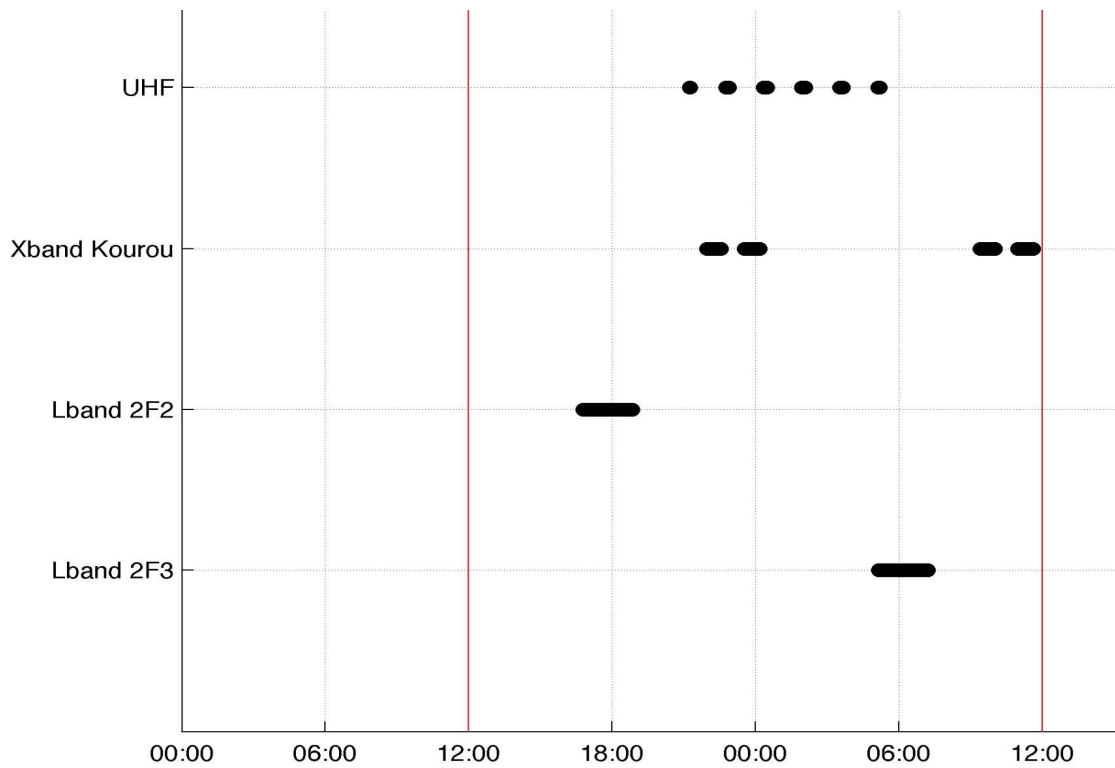
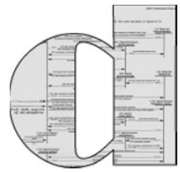
- Very tight power budget
- Needs dynamic and battery aware
- What we do:



model state based on robustness



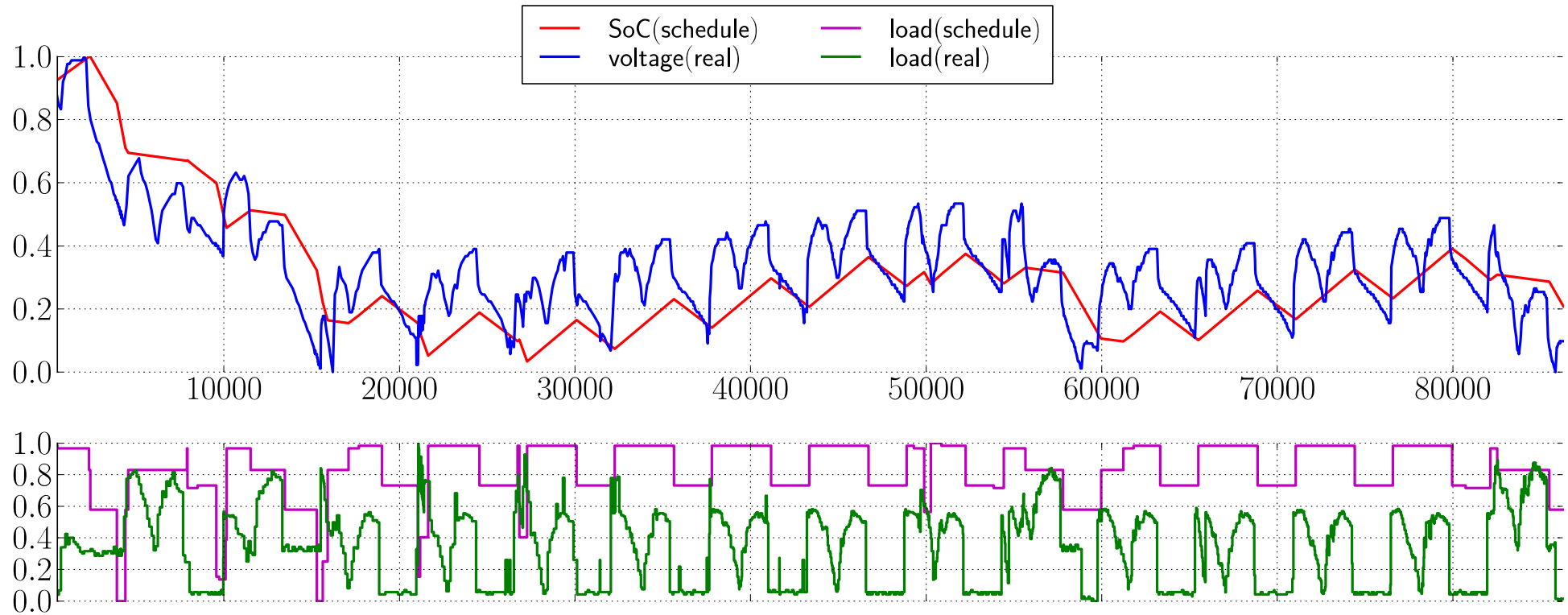
A one-day schedule (for yesterday)



and its depletion risk



Meeting Reality, safely



You saw: Model based ... Analysis

System Model
possible behaviour

```
mime - brp.modest  
File Edit View Model Tools Help  
brp.modest [Analysis] brp.modest  
bool get_K_seen, a_ok_seen, a_nok_seen, a_dk_seen, a_restart_seen, r_ok_seen, r_t...  
// Invariant (timed) properties (from [BrpOnTime], the TA model)  
// "there is at most one message in transit for each channel"  
property T_1 = A[] (!did(channel_overflow));  
// "there is at most one message in transit in total"  
property T_2 = A[] (!inTransitL && !inTransitR);  
// Assumption (A1): "no premature timeouts"  
property T_A1 = A[] (!did(premature_timeout));  
// Assumption (A2): "sender starts new file only after receiver reacted to failure"  
// Note that receiver can only notice failure if it received at least one chunk, i...  
property T_A2 = A[] (!a_restart_seen || !get_K_seen || !T_timeout_seen);  
// Probabilistic reachability properties (from [D'AJJL01], the RAPTURE/FRISK model)  
// property A of [D'AJJL01]: "the maximum probability that eventually the sender r...  
// a certain unsuccessful transmission but the receiver got the complete fil...  
property P_A = Pmax(<> a_nok_seen && a_ok_seen);  
// property B of [D'AJJL01]: "the maximum probability that eventually the sender r...  
// a certain successful transmission but the receiver did not get the complete fil...  
property P_B = Pmax(<> a_ok_seen && !r_ok_seen);  
// property 1 of [D'AJJL01]: "the maximum probability that eventually the sender...  
// does not report a successful transmission"  
property P_1 = Pmax(<> a_nok_seen || a_dk_seen);  
// property 2 of [D'AJJL01]: "the maximum probability that eventually the sender...  
// reports an uncertainty on the success of the transmission"  
property P_2 = Pmax(<> a_dk_seen);  
// property 3 of [D'AJJL01]: "the maximum probability that eventually the sender...  
// reports an unsuccessful transmission after more than 8 chunks have been sent su...  
property P_3 = Pmax(<> a_nok_seen && s > 8);  
// property 4 of [D'AJJL01]: "the maximum probability that eventually the receiver...  
// does not receive any chunk and the sender tried to send a chunk"  
property P_4 = Pmax(<> (s_ok_seen || a_nok_seen || a_dk_seen) && !get_K_seen);  
// Probabilistic time-bounded reachability properties  
// "the maximum/minimum probability that the sender reports...  
// a successful transmission within 64 time units"  
property Dmax = Pmax(<> a_ok_seen && time <= 64);  
property Dmin = Pmin(<> a_ok_seen && time <= 64);  
// Expected reachability properties  
// "the maximum/minimum expected time until the transfer...  
// of the first file is finished (successfully or unsuccessfully)"  
property Emax = Xmin(time | first_file_done);  
property Emin = Xmin(time | first_file_done);  
process Sender()  
{  
  bool bit;  
  ...  
}
```

Analysis
Focus

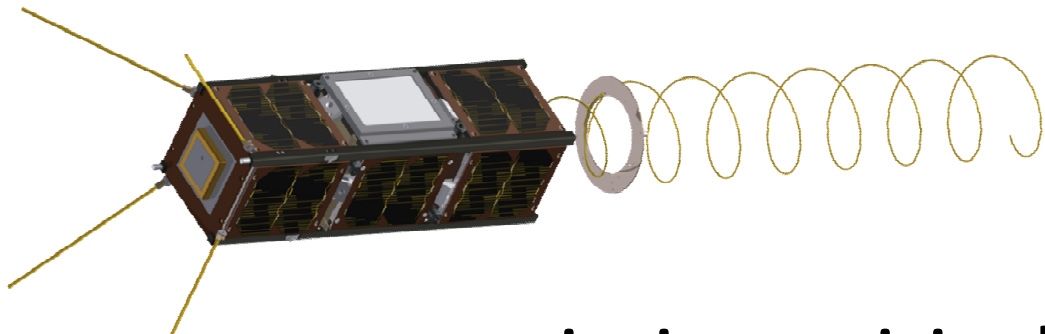
Model Analysis

Results

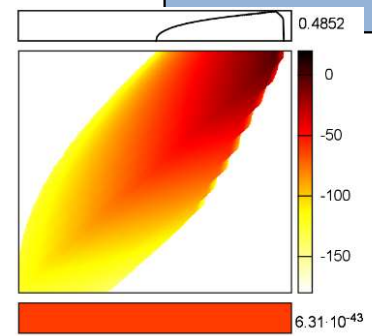


modestchecker.org

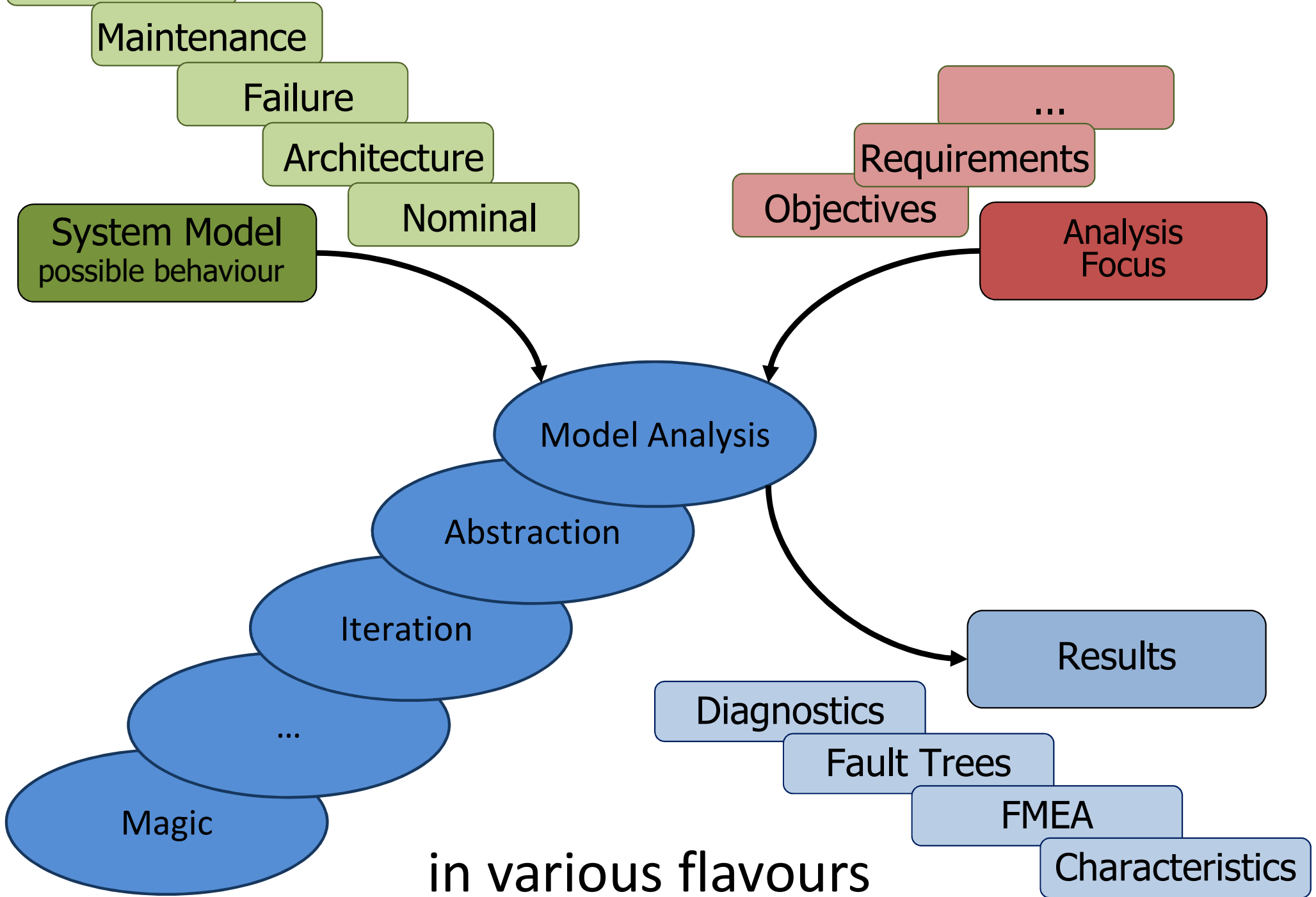
UPPAAL CORA



on a concrete, mission-critical case



You see now: Model based ... Analysis



Safety by Design?



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