Why automation matters for security

Thomas Fricke

Partner Endocode AG
Regular changes from Dev to OPS and back
Big Data Architect

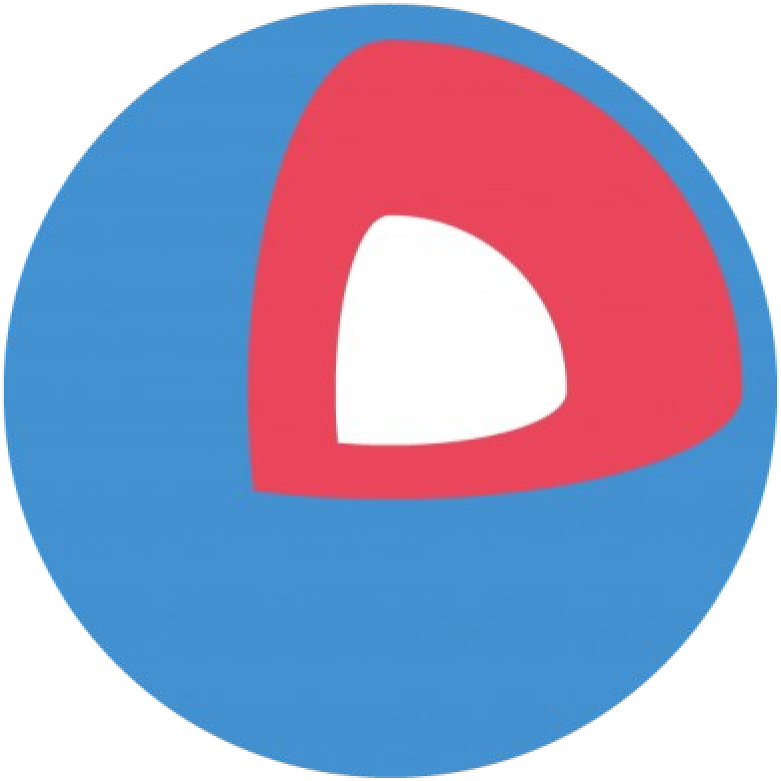
Secure Linux Administration Conference 2015

About Endocode

- Berlin based company: 14 people, 9 Nations
- Open Source Development and Dev Ops Projects
- Customers
  - Startups
    - Scaling
    - Automation
  - Big Customers building Deployment Pipelines
    - Open Invention Network
    - Free Software Foundation Europe
    - Prototype projects
    - Grundgrün
    - Secure Phone based on L4 and Android

Visit us on Github: github.com/endocode

Disclaimer: we work for CoreOs



Endocode does projects with Puppet, Chef, Amazon, Hadoop ...

Warning

this talks contains some

- uncomfortable truths
- heretic remarks
- offending pictures
- nerdic jokes

I apologize for possible bad taste and infringements

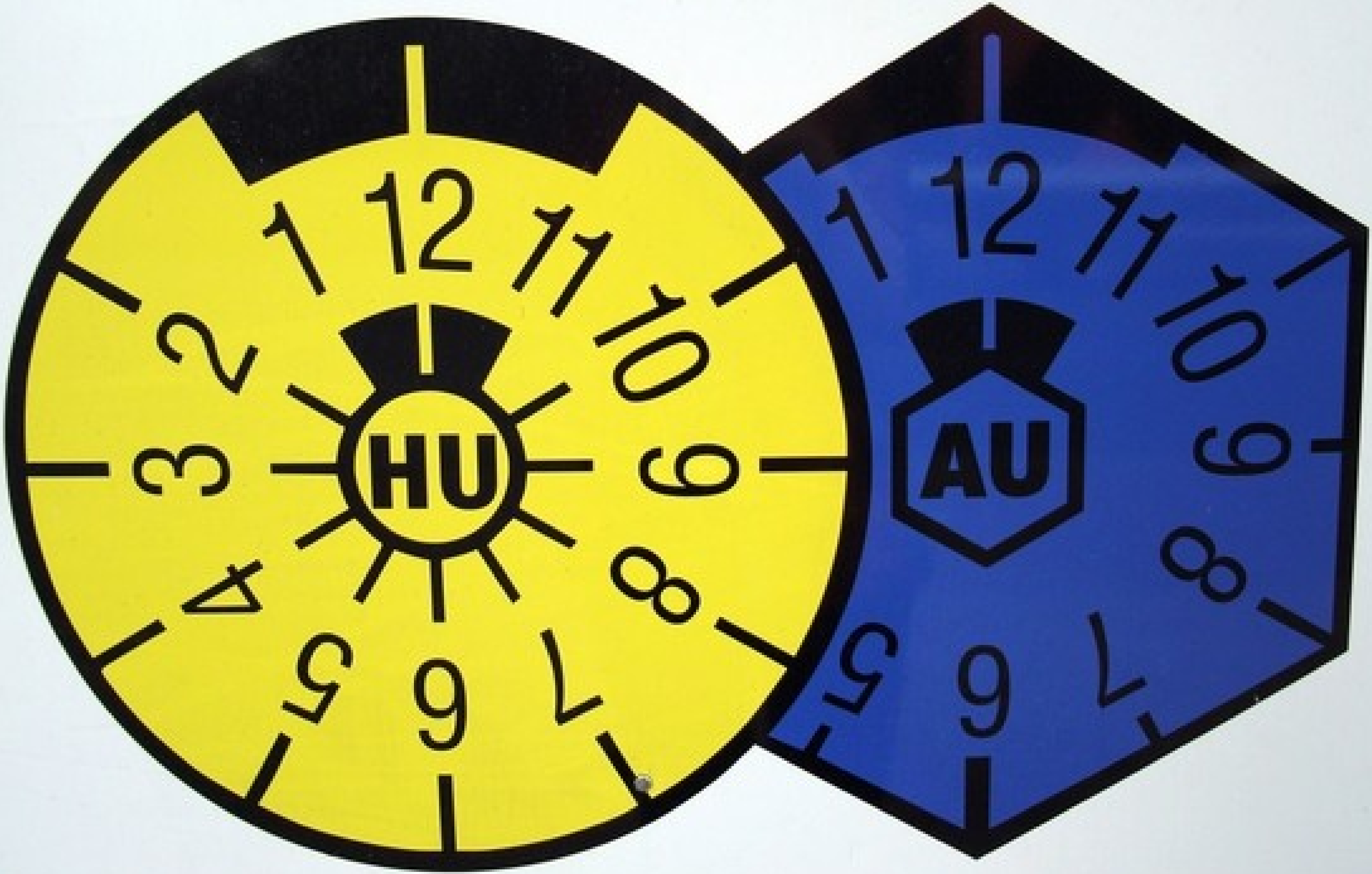
all examples are from real projects

customers have been anonymized to protect the innocent

How to run the whole system secure?

- is this possible?
- failure is not an option?

- How to get there?


HU
1
2
3
4
5
6
7
8
9
10
11
12
AU
1
5
6
7
8
9
10
11
12

Audits

- Highest Reputation?
- What are audits?
- audits check **exactly what is in the contract**
- mixture of usability, security and something
- like checking your car, your insurance and the color of the seats

What does an audit check?

DIP

System Audits

Roles: Auditor and Supporter

- Auditor controls you
- Supporter supports you

Approach corporate style

- good cop, bad cop
- bad cop, good cop

After the Audits

Recommended vendor firmware update
in a **certified** security critical environment:

```
http://linux.dell.com/repo/hardware/latest/bootstrap.cgi
```

proposes

```
Wget -q -O - http://linux.dell.com/repo/firmware/bootstrap.cgi | bash
```

No checking of addresses, certificates etc

Running a complete embedded monitoring systems

- VNC console
- Tomcat (oooold)
- Updated with software from repository

BASF
E·X·T·R·A
5.25"·2S/HD
96 tpi

what else: PCI DSS

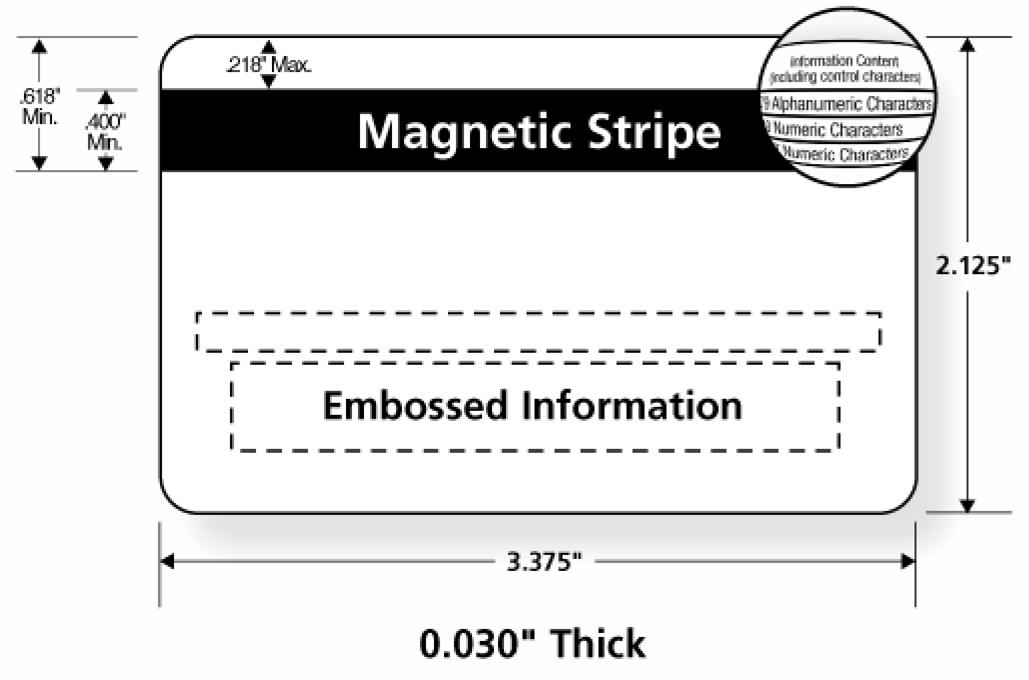
Payment Card Industry Data Security Standard

1) Install and maintain a firewall configuration to protect cardholder data.
2) Do not use vendor-supplied defaults for system passwords and other security parameters.
3) Protect stored cardholder data.
4) Encrypt transmission of cardholder data across open, public networks.
5) Use and regularly update antivirus software.
6) Develop and maintain secure systems and applications.
7) Restrict access to cardholder data by business need-to-know.
8) Assign a unique ID to each person with computer access.
9) Restrict physical access to cardholder data.
10)Track and monitor all access to network resources and cardholder data.
11)Regularly test security systems and processes.
12)Maintain a policy that addresses information security.

Don't be a complete idiot

what else: PCI DSS

- EMV (Europay, MasterCard, and Visa) is standard
- opening a 2nd location without notice
- we have errors, because of this 80 char string being encrypted



Obvious solution:
turn on encryption for the audit,
turn off after the audit

impact on admins

admins are trained for a wrong mindset

- fear
- lies
- fraud
- avoiding truth
- relax folks, we are safe, we have been audited*
- cynism
- burnout
- do you really have to work this way?

Conclusion on audits

- circumvented
- obtained by fraud
- basic policies
- complex systems

- how worse it would be without audits?
- not completely useless
- no warranty

Questions
on audits?

?

Dimension of the problem

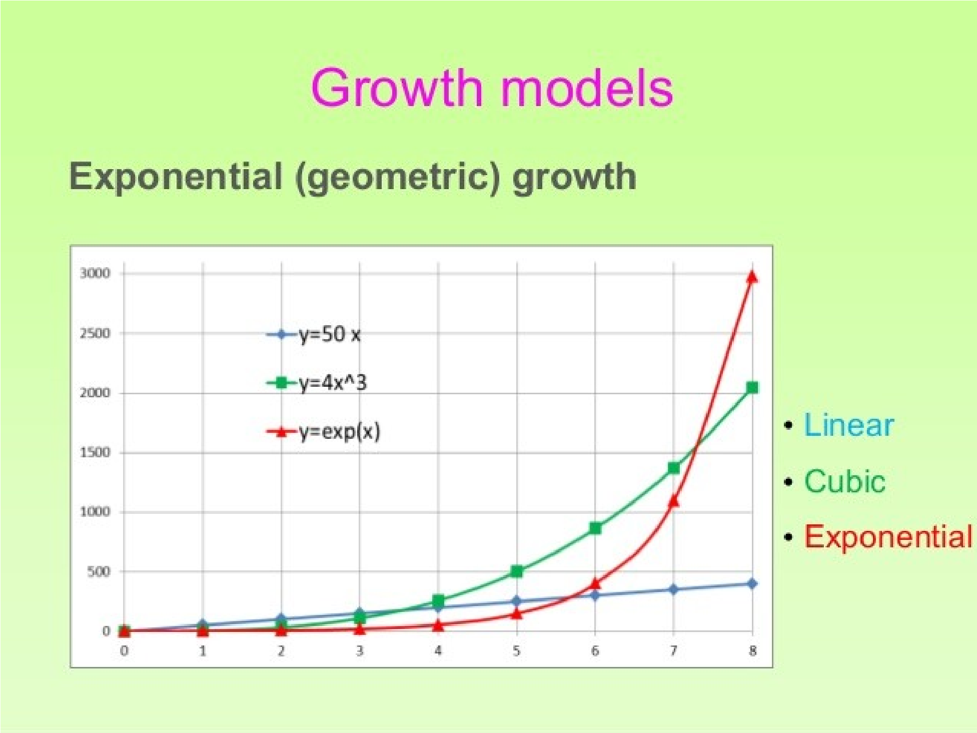
At least three dimensions

- Number of Systems

- Number of Applications

- Number of Updates

cubic growth



Growth models

Exponential (geometric) growth

- Linear
- Cubic
- Exponential

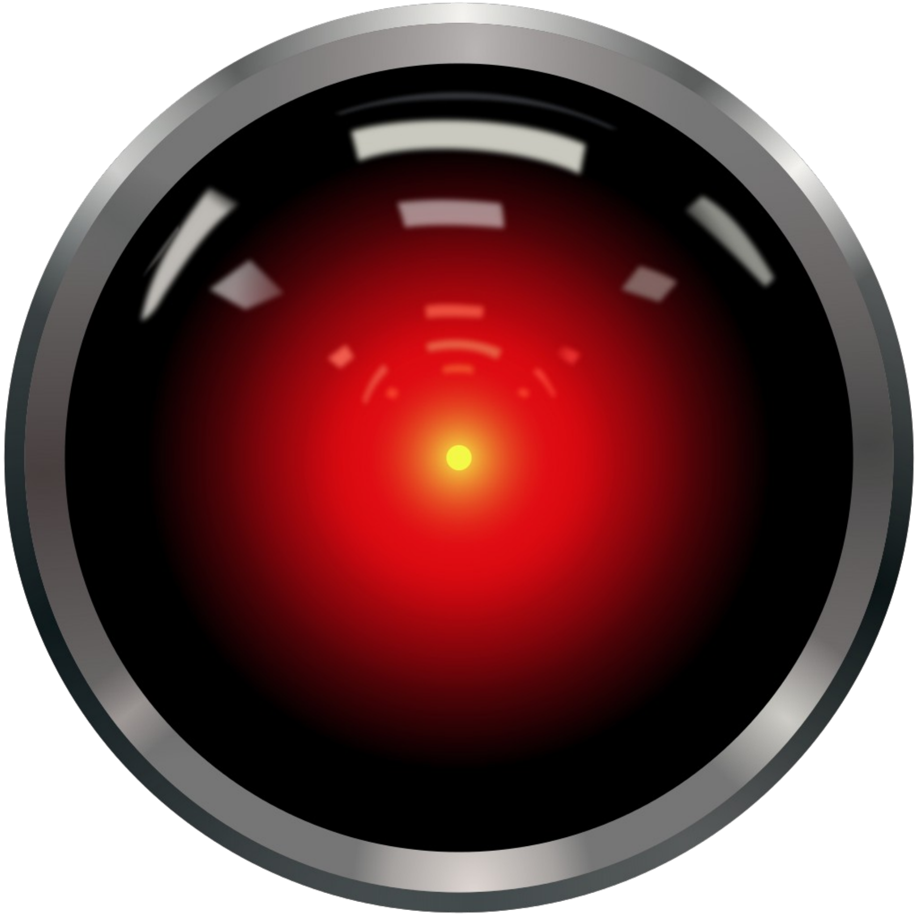
Regain control

- know what you are doing!
- automate
- KISS
- divide et impera
- separation of concerns

complexity of distributed systems

Monitoring

- monitor everything
- part of the deployment
- inversion of control



complexity of distributed systems

Know your complexity

- packages (deb and rpm)
- configuration (Cookbooks, recipes, manifests)
- orchestration (OpenStack, Homegrown)

Packages

Everything can be packaged:

configuration
passwords

Sputnik

Immobilienscout24

Packages

- Red Hat, Debian: no support
- repackage everything via deps
- you started packaging your configuration
- and end creating a distro

Configuration Systems

Promise

- no manual configuration
- updates automatically
- runs permanently

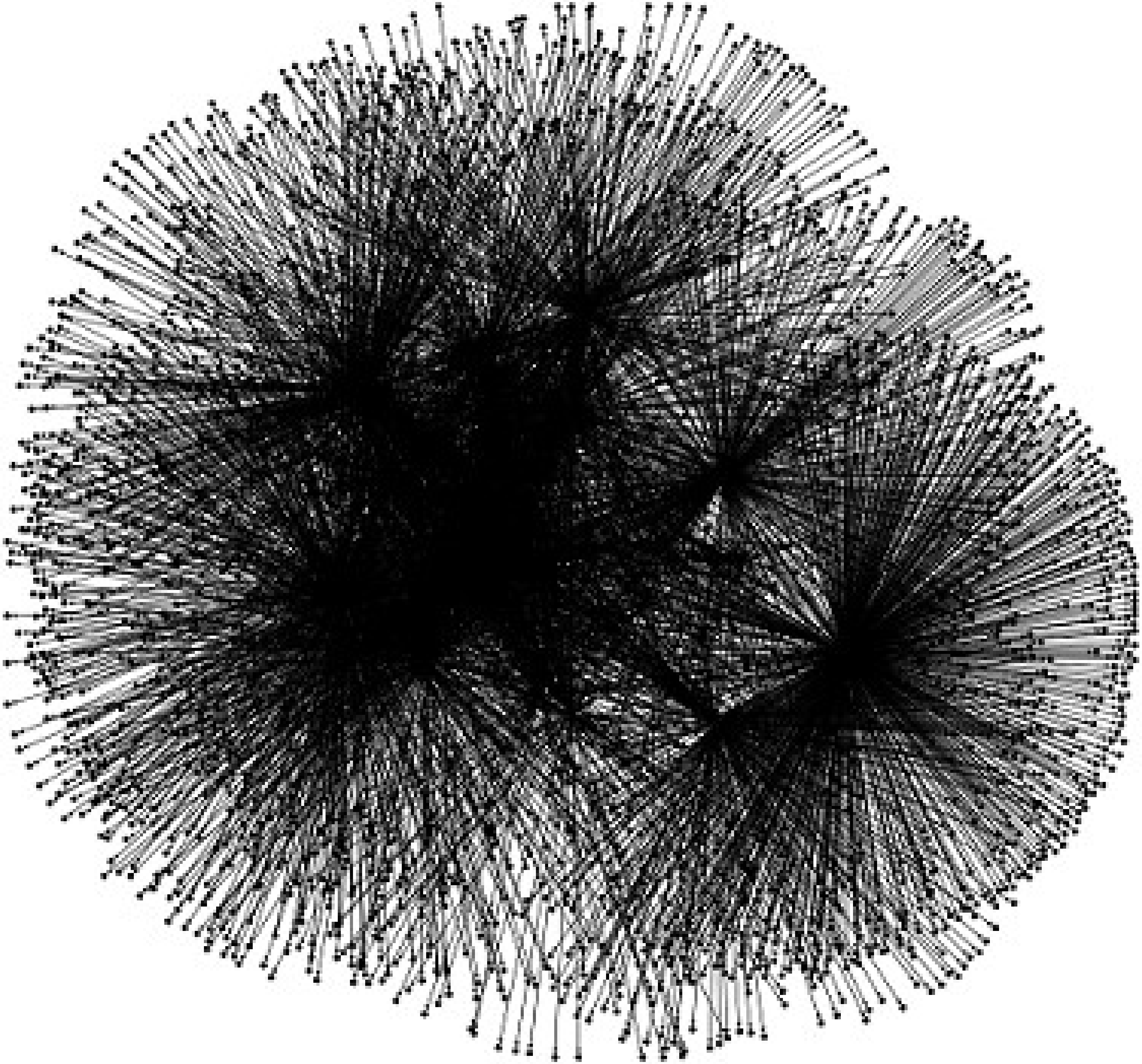
Reality

- Part of the problem
- You need an Architect or an Exorcist
- Predictability
- Updates
- Fear!

Orchestration

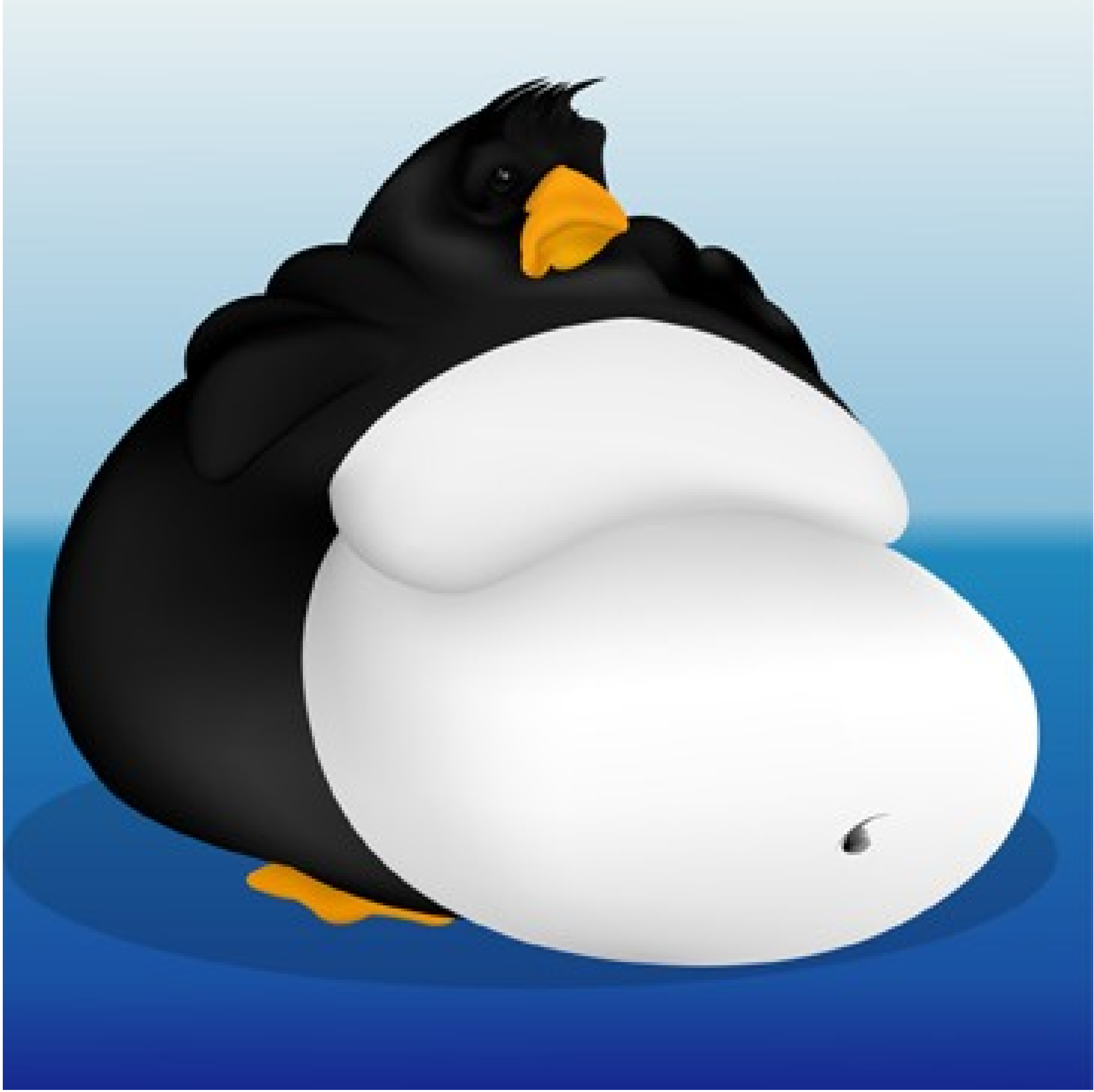
Not yet ready??!!

OpenStack?



Tux must get lean again

!



PAUL NICKLE

What we really want

Unikernels

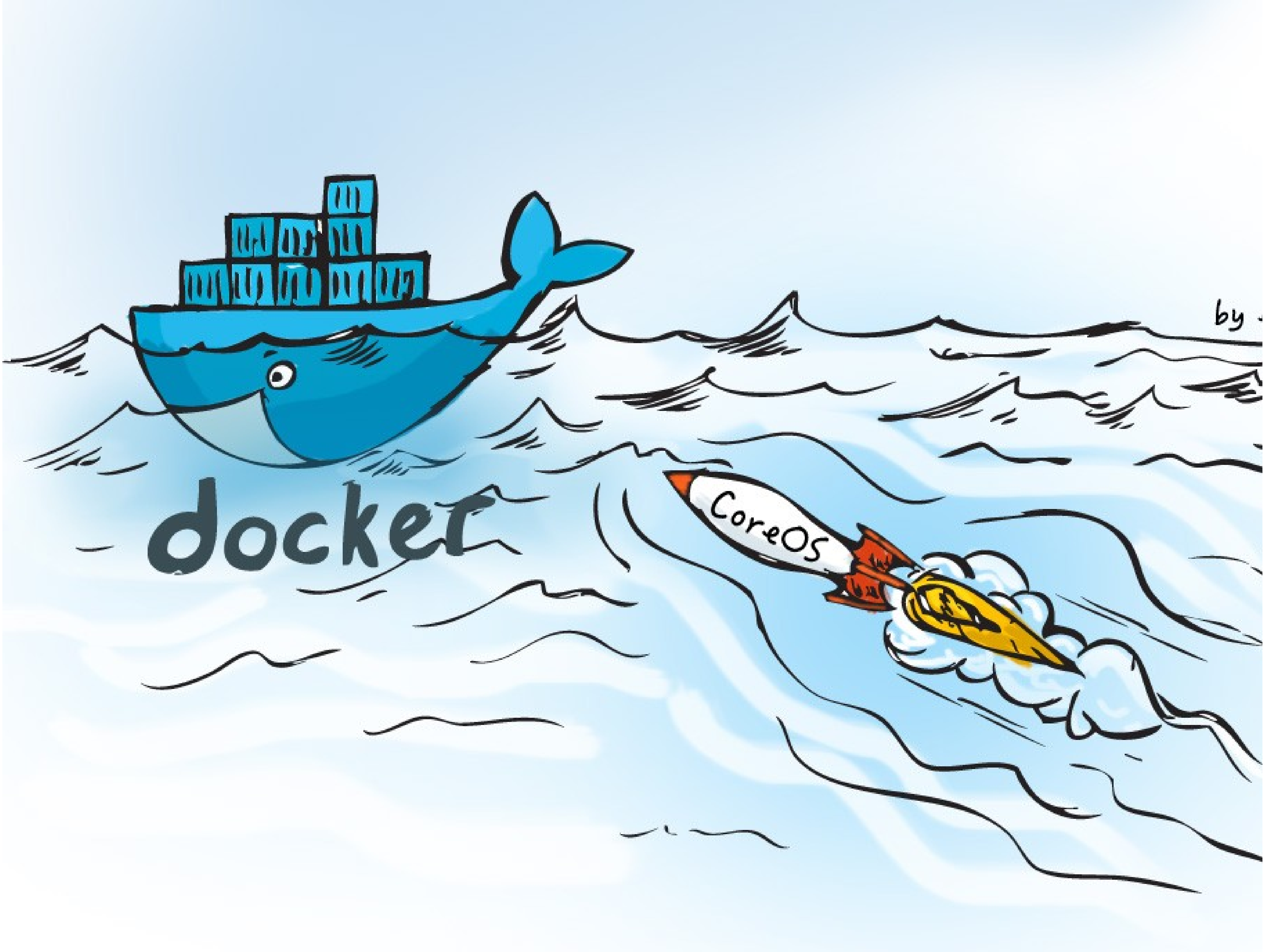
- MirageOS
- OCaml
- rewrite everything

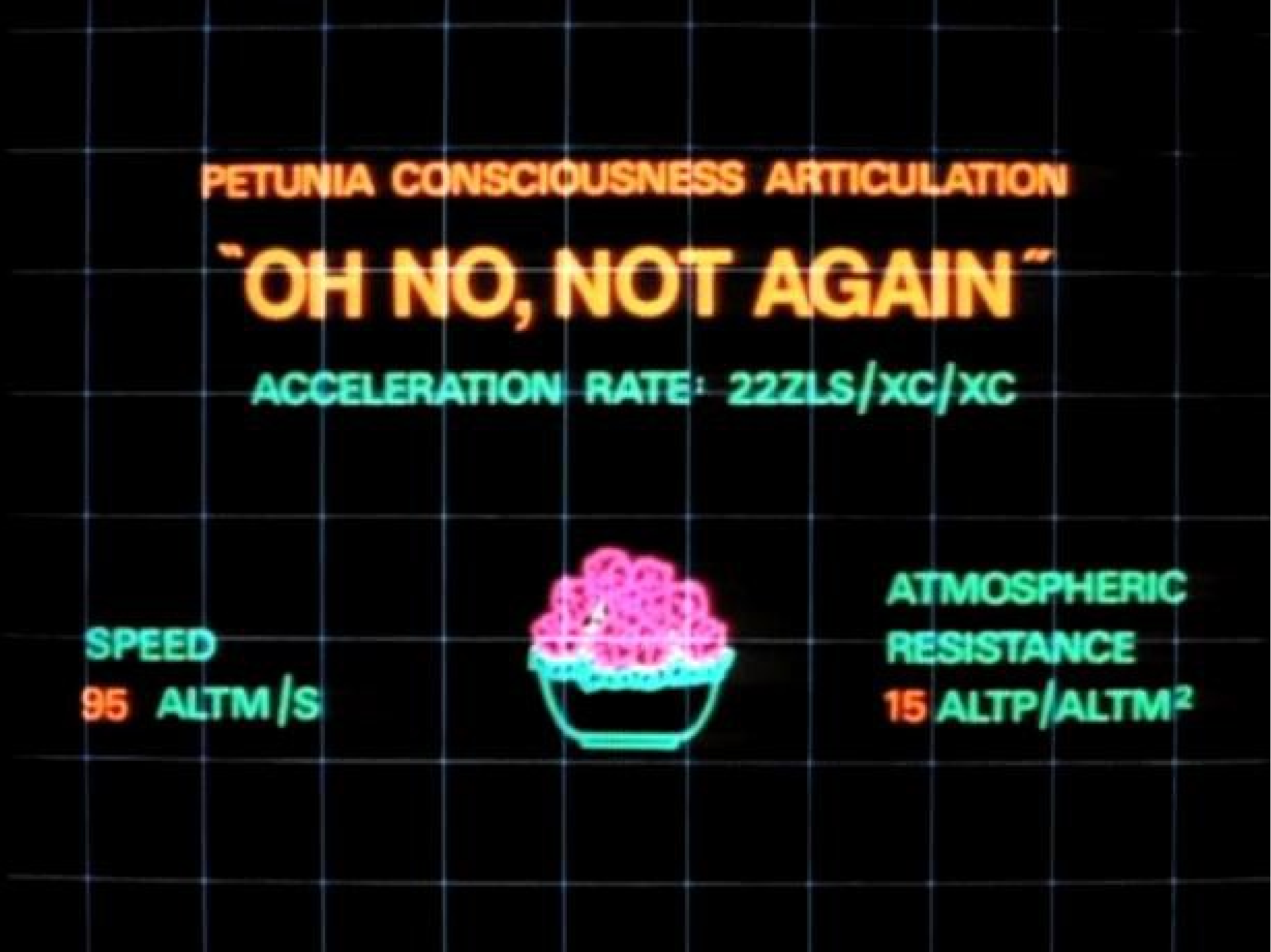
Microservices

- containers
- immutable
- shrinked

CoreOS

- immutable
- runs containers
- tin cans


docker
CoreOS
by



PETUNIA CONSCIOUSNESS ARTICULATION

“OH NO, NOT AGAIN”

ACCELERATION RATE: 22ZLS/XC/XC

SPEED
95 ALTM/S

ATMOSPHERIC
RESISTANCE
15 ALTP/ALTM^2

www.opencontainers.org

Containers?

needs some orchestration

- Fleet: systemd configuration
- Flannel: networking
- Etcd: configuration registry
- kubernetes: orchestration

systemd

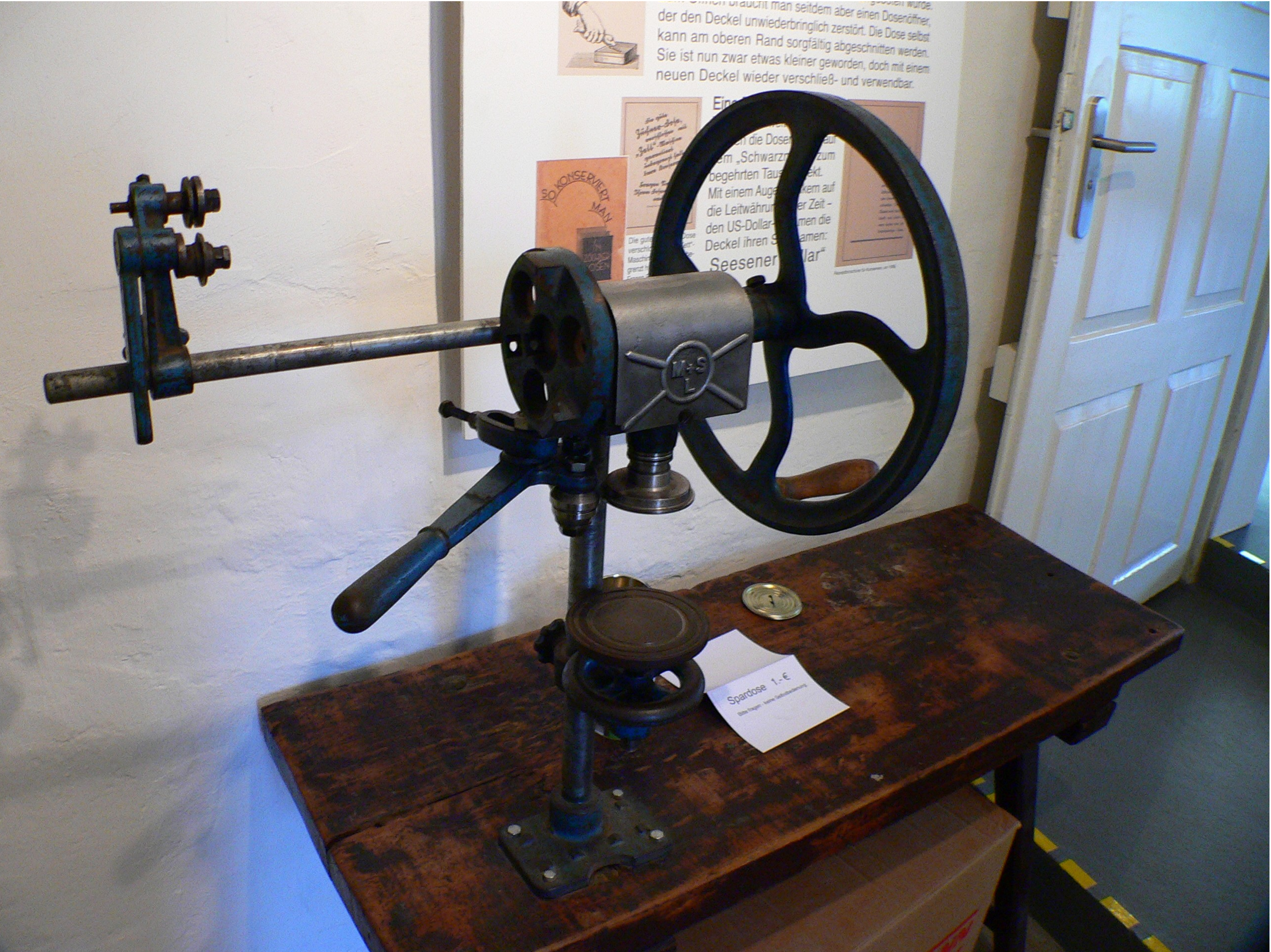
- Systemd: inside and outside rkt containers
- requires access to external resources: disks, inter
- network
- storage

Optimized Containers

- stripped down to the bare necessities
- mostly stateless
- orchestration by Kubernetes

see

Jason Wilders Squashing Docker Images
http://jasonwilder.com/blog/2014/08/19/squashing-docker-images/



der den Deckel unwiederbringlich zerstört. Die Dose selbst
kann am oberen Rand sorgfältig abgeschnitten werden.
Sie ist nun zwar etwas kleiner geworden, doch mit einem
neuen Deckel wieder verschließ- und verwendbar.
Ein
die Dose
em „Schwarzm
zum
begehrten Taus
ekt.
Mit einem Auge
kem auf
die Leitwähru
er Zeit -
den US-Dollar-
men die
Deckel ihren S
amen:
Seesener
llar"
SO KONSERVIERT MAN
M+S L
Spardose 1.-€
Bitte fragen - keine Selbstbedienung

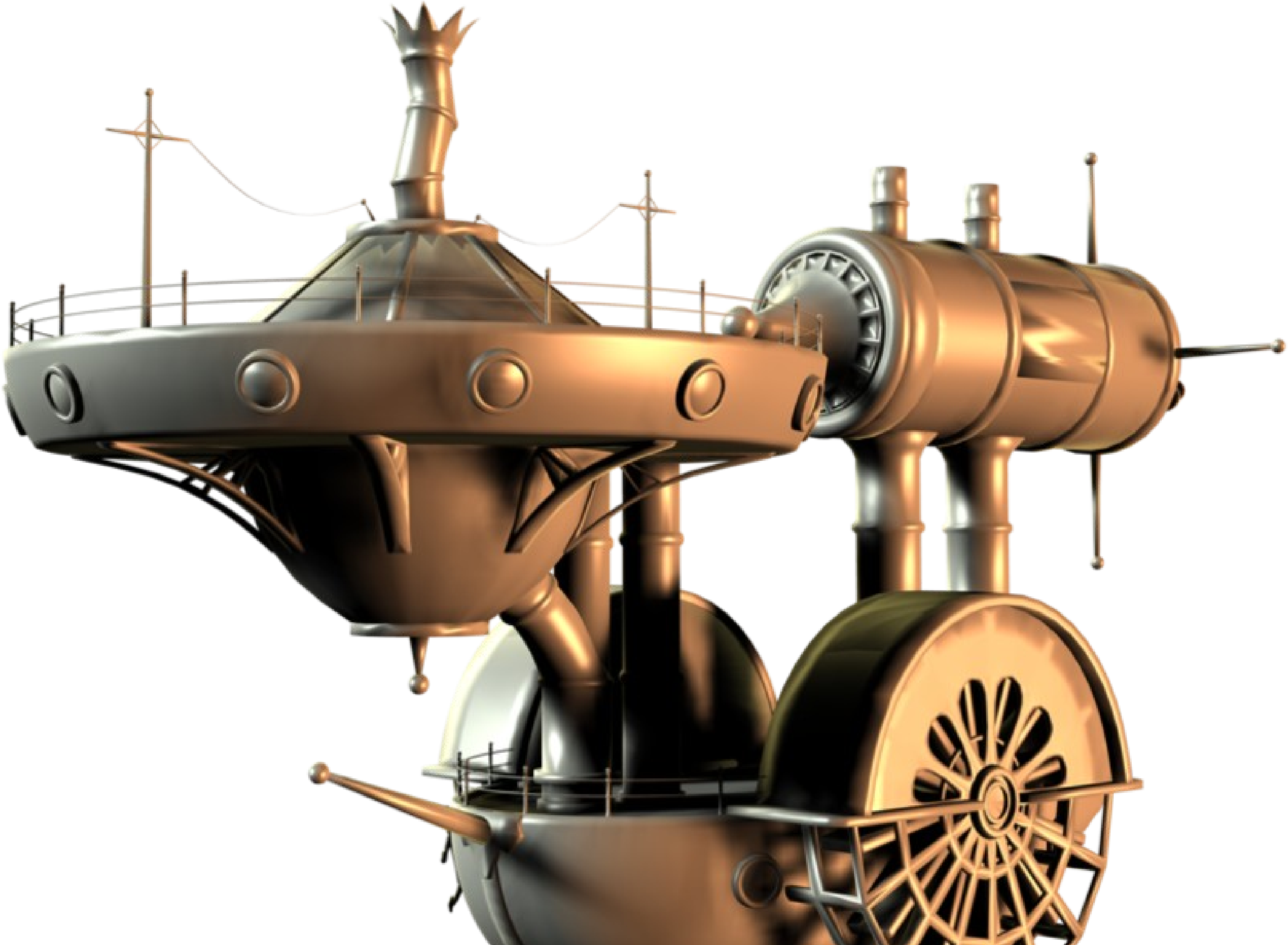
Heinz
CHILI CON CARNE
Bonduelle
Campofino
0.89
0.59
1.59
1.59
1.19
2.19
2.99
1.99
ja!
Dörffler
Ragout fin
Erasco
Graupen Topf
Westfälischer Linsen-Eintopf
Erbsen-Eintopf
Kartoffel Topf
1.89
2.99
2.19
2.19
2.19
2.19
2.99
2.19
1.99
4 KÖNIGSBERGER KLOPSE
Reistopf
Linsen Eintopf
Grüne Bohnen Eintopf
2.99
2.19
2.19
2.19
2.59
2.79
2.99
2.79
2.19
2.19
2.19
1.99
Mark-Klößchen
im Doppelbeutel
1.29
1.29
1.29
1.49
0.99
1.15
Texas-Pfanne
0.89
0.79
0.89
0.89
0.75
0.75
1.29
1.59
2.19
2.19
2.69
2.99

If you do not want it

Fight!

- containers
- systemd
- CoreOS

Our
current
Starship



Thank you!
Questions!

?