Of Chameleons, Pipelines, Compliance, and Open Source

Sebastian Schürmann, MaibornWolff GmbH

MaibornWolff

The company

- Germany, Ruanda, Spain, Tunisia
- History back to 1989
- 1000 people

THEMEN	IM FOKUS
Apps	Individuelle Softwareentwicklung
Cloud	Individuelle Softwarelösung
Cybersecurity	Softwareentwicklung
Data & AI	Digitalisierung in der Energiewirtschaft
Design & UX	
Embedded & Robotics	
Industrie 4.0	
IoT	
IT-Beratung	
IT-Modernisierung	
Quality Engineering	
VR/AR	
Web	

Department
DevOps & Cloudnative

- 65 Persons in 3 Countries
- Focus on the ‘Cloud Part’ of modern software projects
- Sometimes we touch hardware (IOT and recently more servers)
- ‘We build it, we run it’ as Department

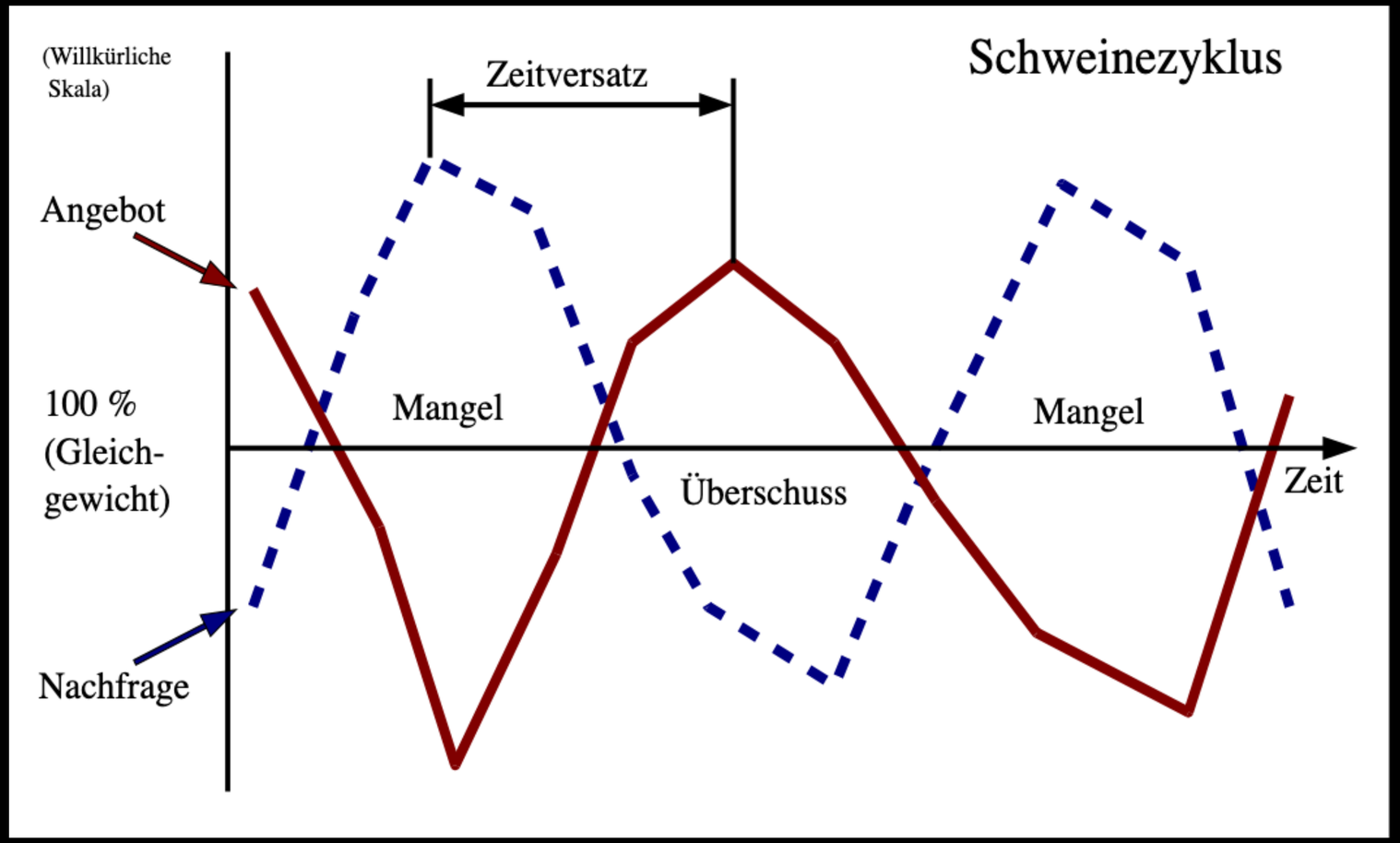
Personal

Sebastian Schürmann

- 49 years. Half of it ‘In IT’
- Role: Principal Architect
- Jobs: Consulting, Org Roles to Development
- Family: Father of a year old
- Private: Synthesizers and a Game.

Project Chameleon

Changing how we teach each other



INSERT CRISIS HERE

Internal Training in times of uncertainty

- Vendor certifications are qualification as well as education - but with a limited scope on education
- Diverse education needs and interests in our diverse (skill, gender, nationality) team
- Surprisingly: We gained time! A lot or maybe not?????
- Challenge: Uncertainty is not a great motivator - without Buttons to press

Solution

- Deliberate Practice - Build new things. Create the ability to fail.
- Create ‘Larger than Life’ projects
- Huge scopes
- Something no one built before and something we can not build ‘from the top of our head’
- Provide a ‘home’ for people without projects
- Upskill Opportunities

Project Cars

- Phase 1: Serverless Data Processing Pipeline of EV Car Data
- Phase 2: MLOps Pipeline + Build a Model
- Phase 3: Inference on Edge - In a car (Goal: Make it possible to win ADAC E-Competition)

Challenges

Obvious and not so Obvious

- Minimal Automotive Experience in the team: We should have started on a track for ‘frame of reference’
- Model Inference on the Edge: With the ability to replace the model on track
- Machine telling driver how to drive: UX- and Liability-Challenge

Results
Project Cars

- We really ‘stepped up’ to the challenge
- People filled roles they never had before
- We built 60% of the feature set planned
- We learned a lot from each other
- We created ‘sense of community’

Extra Curriculum Activity

- Contributing to vendor OS projects
- Implementing Ephemeral Environments for ‘fun and profit’

Left to be desired

Project Cars

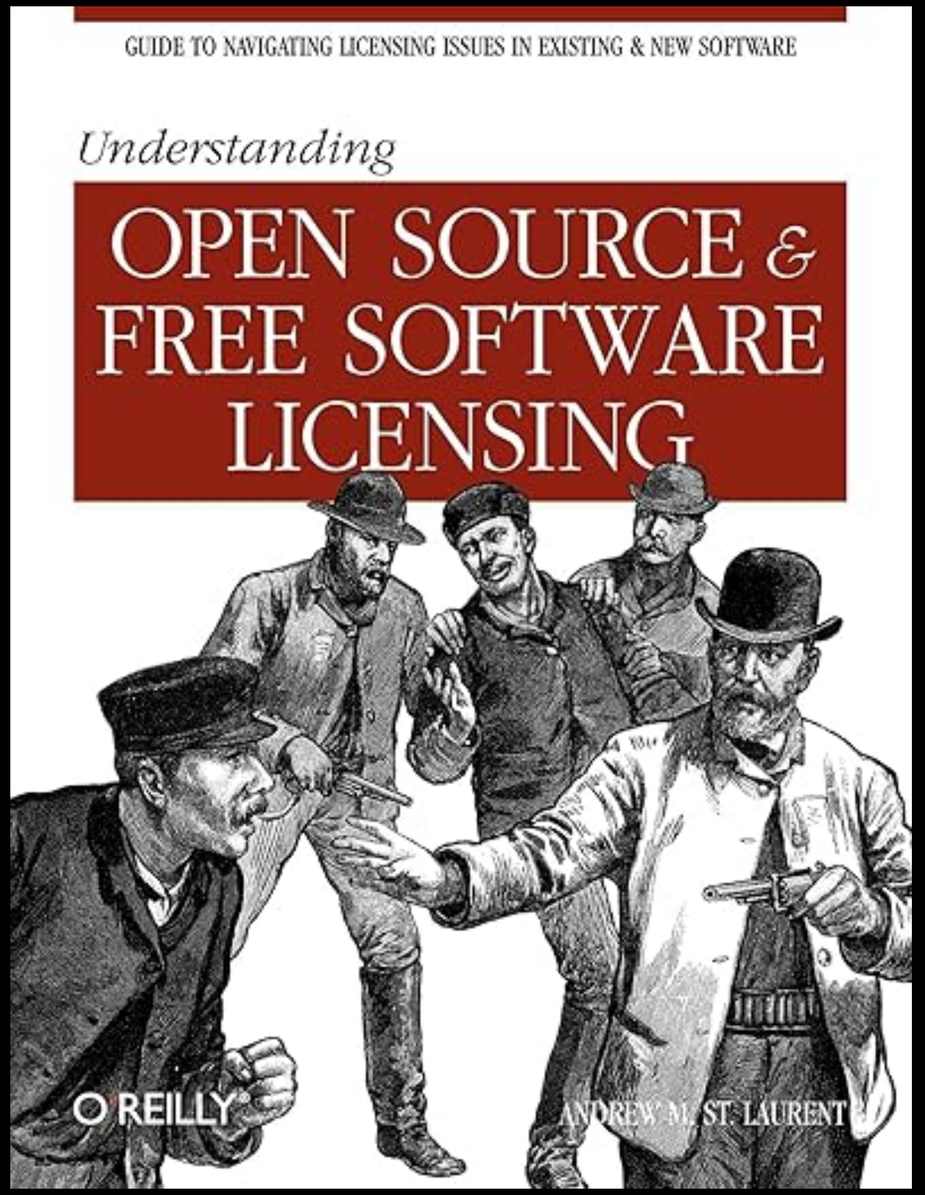
- The public side of the project was hard to sell - going racing was a tad visionary to far for many.
- We should have bought hardware and do live testing much earlier
- Compared to the overall project cost we could have easily jumped into a car and actually raced

Interlude: Why BOM Matters now

Why is OS Licensing getting spotlight now?

Legal issues!

- The nuts and bolts of OS Licensing have not changed over the last 20 years
- CRE just makes everyone create SBOM
- Result: The issue of OS licensing can not be as easily ignored anymore



Why is OS Licensing getting spotlight now?

Technology!

- More customers build solutions that put devices in the hands of users (edge computing)
- Sovereign Cloud Operations en vogue
- Hyperscaler ‘Opensource’ = Vendor Lock in. There will be lots of new tooling to replace this

Why is OS Licensing getting spotlight now?

Gaps

- Skill gap - Practical experience with in depth reporting and software lifecycle integration tooling is rare
- Knowledge GAP - Neither SBOM nor Software Licensing are in any of the curriculums we point our Staff to
- Tooling not Ubiquitous - Many specific solutions


What now?

Obvious Solution

‘Learning’ from ‘AI HYPE 2025’

- Create Demo
- Spam Social Media
- Find Customer for ‘Prototype’ Project
- Build the Business from there
- Sell “10K Euro PDF” repeatedly
- **This is not how we will do it!**


Don't count your chickens before they hatch
What about?

Our Solution

Bottom Up approach

- Educate developers and management by **building** the tools we need
- Provide this tooling to teams and customers for feedback
- Get to the bottom of DEV-X Problems

Project: Compliant Pipelines

Let’s do Software License Compliance Right

What?

Team works it out

- Check dependencies of a Project against a defined ruleset for license compliance
- purl-patrol + config.json =
- Integrates into 2 Major pipeline providers
- Uses established OS Solutions if possible

Who?

Self-Organize

- Find motivated volunteers in 3 departments
- Across all Experience Levels: Junior to Department Lead
- With a diverse set of goals

How?

- MVRS (Minimum viable ruleset): Daily Standup & Pair Programming
- 1 long form text to define the goals
- Pull Principle
- Assume good intentions and negotiate differing ideas

Why?

On a Personal, Department and Company Level

- Start spreading the ‘Gospel of SBOM’
- Educate ourselves about licensing in OS Projects
- Run a OS Project with a ‘Net Profit’
- Normalise: Solving Wicked Problems and ‘Disagree and Commit’

Sources of truth

Where to obtain license information

- Package Registry
- Sourcecode
- 3rdParty Databases
  - e.g. https://ecosyste.ms

Multitude of Challenges

Technical

- Moving target: Multiple CI Platforms
- Evaluate everything: Many tools to do the job
- Production deploy without ‘calling a friend’ - aka external web service or git repos
- Lots of dependencies

Process

- Multi Platform releases
- Open Source release procedures
- Internal Siloing
-

Personal

- Team composition constantly changed
- Personal Skill of Limited use when working many platforms and many languages
- The scope of the project lends to politics - Multiple Departments etc.

Results

Results

- https://github.com/maibornwolff/purl-patrol
- checks your SBOM against a policy file
- 2 platforms (github actions, azure) - 2 languages (Java, Python)

Extras!

- Started to develop a own scraper and (meta-)database for license data
- Project members have a deeper understanding of the “Cyber Resilience Act” and the adjacent SBOM Topic

Next UP

Future

- Make it a living breathing open source project
- Lift the “Bus Factor”
- Solve the DevX Questions around SBOMS and open source licenses
- Make running the project feasible

Questions?

sebastian.schuermann@maibornwolff.de