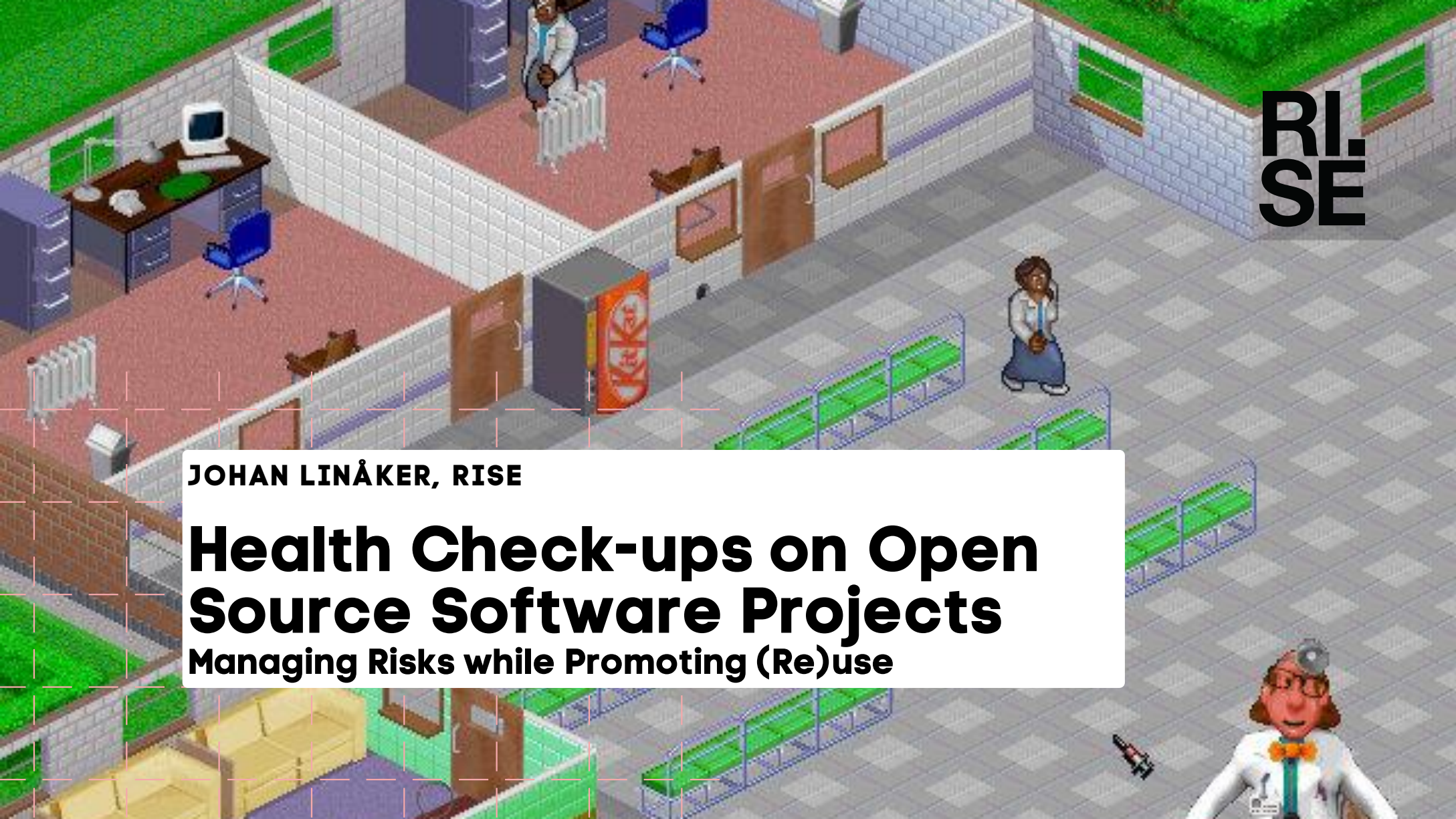


JOHAN LINÅKER, RISE

Health Check-ups on Open Source Software Projects

Managing Risks while Promoting (Re)use

Open Source Software Health

- An Open Source Software project's capability to stay viable and maintained over time without interruption or weakening

Photo by Jan Piatkowski | https://unsplash.com/photos/eopz9bkwROs

Open Source Software Health

- Productivity: There is an active development of the project
- Robustness: The development is open and spread out on several (independent) individuals
- Openness: Users of the project can influence and contribute to the development of the project

Photo by Markus Frieauff | https://unsplash.com/photos/lJ0KiXl4uys

Linus’ law

- ”Given enough eyeballs, all bugs are shallow”
- Requires that enough eyeballs actually reaches the codebase
- Free-riding, for both good and bad

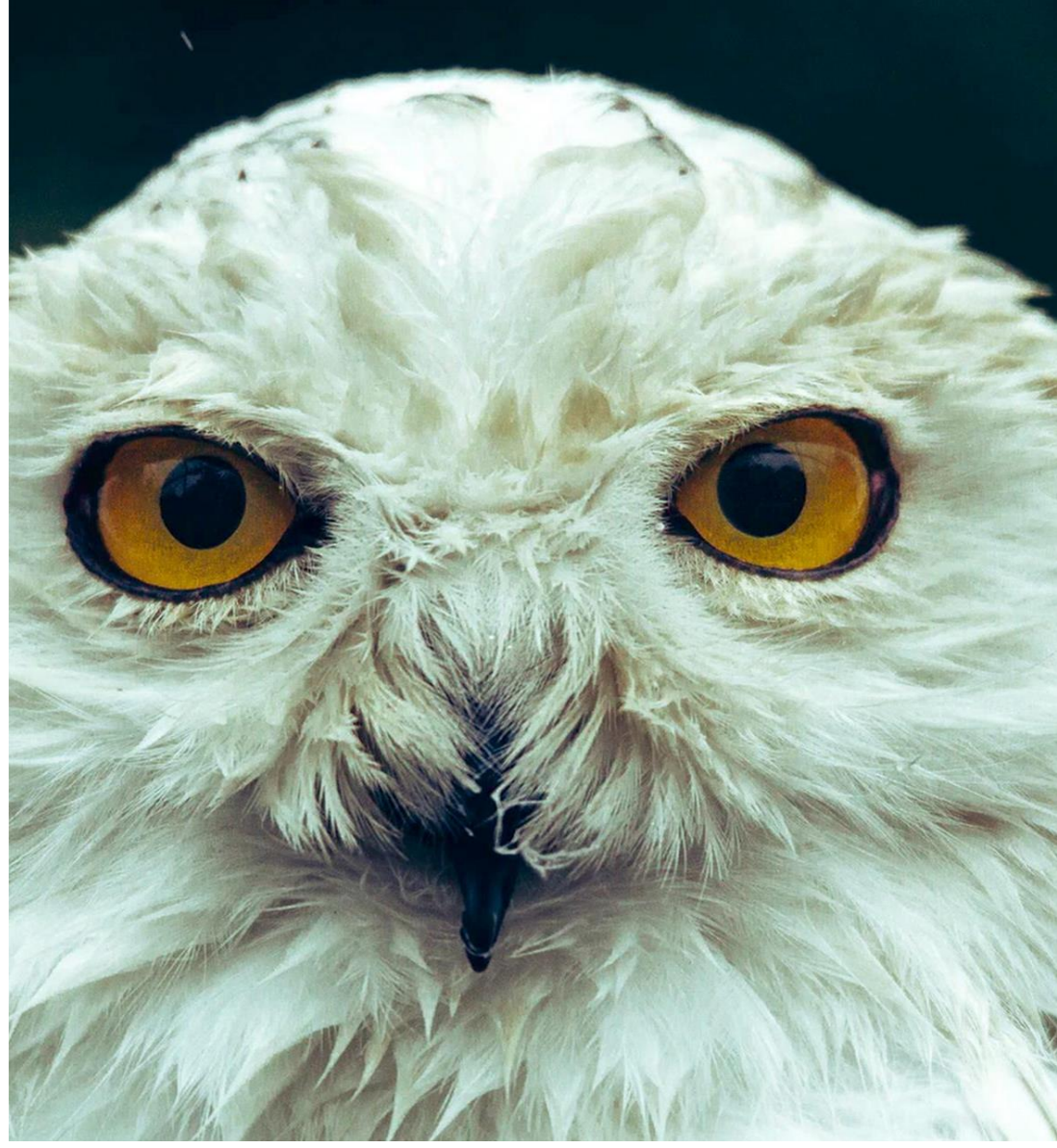


Photo by Frida Bredesen | https://unsplash.com/photos/c1fFv08N7qE

Brain-time as a Common Pool Resource

- “Brain-time” and maintenance effort is subtractable
- Maintainers are humans, not robots
  - Burnout, changed family or working conditions
- Companies must adapt to stay competitive
  - Refactorization, new products, changed business model

Photo by NeONBRAND | https://unsplash.com/photos/KYxXMTpTzek

- An MD asks questions and uses tools at disposal to examine the patient, identify symptoms, arrive at a diagnosis, and prescribe a treatment.

- A developer asks questions and uses tools at disposal to examine the OSS project, identify symptoms, arrive at a sourcing decision, and potential actions for community engagement.

RI.SE

Health and Security Management for OSS (HASMOSS)

- 2021-23 Vinnova-funded R&D-project
- RISE, Scania, Debricked, Addalot
- Goals:
  - Enable health analysis at intake and acquisition of OSS, and ongoing consumption
  - Enable sourcing decisions and proactive health improving measures

RI. SE

Photo by Luke Chesser | https://unsplash.com/photos/JKUTrJ4vK00

Photo by Jaredd Craig | https://unsplash.com/photos/HH4WBGNyltc

What can we find in literature?

- 146 studies
- 107 characteristics (+associated metrics
- Divided over 15 themes
- Supplementary material: https://doi.org/10.6084/m9.figshare.20137175
- Paper: https://www.ri.se/sites/default/files/2022-09/opensym2022-6%20%281%29.pdf

RI.SE

Photo by Austin Distel | https://unsplash.com/photos/smiling-man-reading-book-while-holding-mug-4r72LPFh4Ik

What does experts say?

- 17 interviews with industry and community experts
- 4 areas critical to classify projects, impacting what metrics to prioritize and how tough
- 21 areas of complementary metrics considering
  - Community productivity, and stability
  - Orchestration
  - Production process and outputs

RI.
SE

Project Classifier

- Life-cycle stage
  - 1) inception, 2) growth, 3) stabilization, and 4) decline
- Project Complexity
  - scope, size, and technical complexity of the codebase
- Governance concentration
  - impact on the project's openness to input and external influence on decisions and transparency of discussions
- Strategic Importance
  - importance of the OSS project from a business and technical perspective

Photo by Annie Spratt | https://unsplash.com/photos/open-book-page-vpFiAD-WWEs

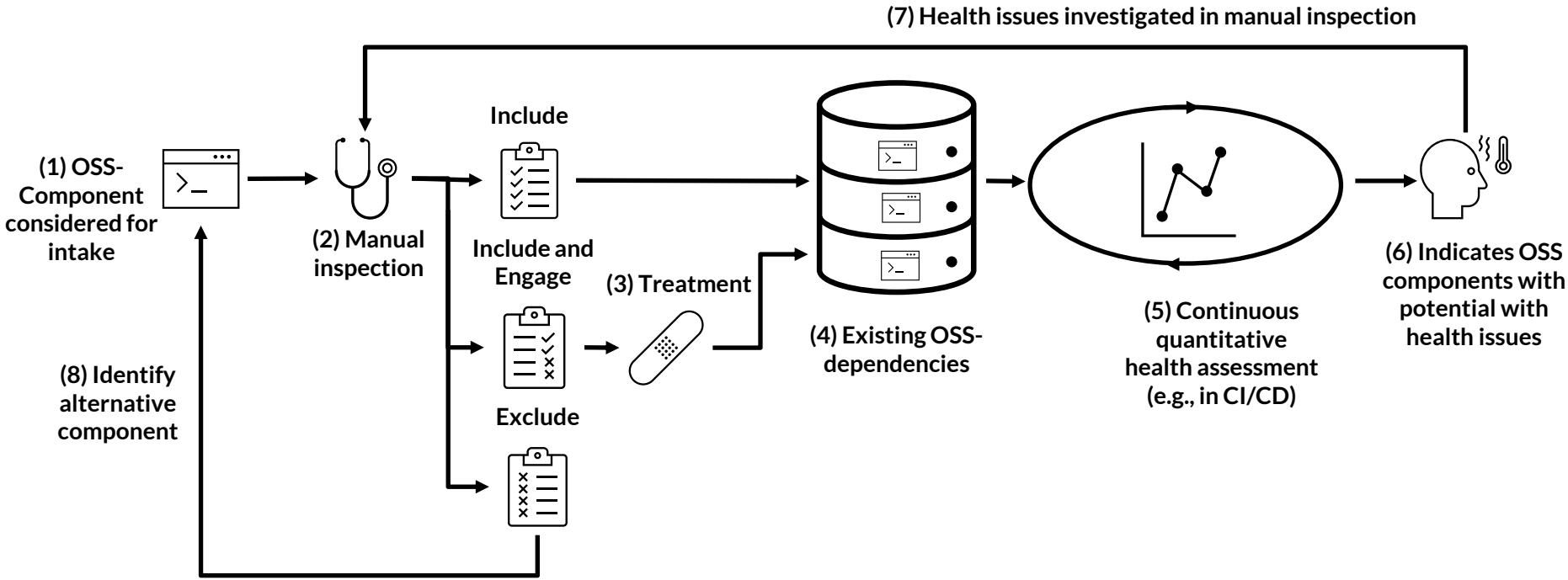
Going from theory to practice

- What:
  - Lower risk of OSS used and considered in the intake process
- How:
  - Set up an intake and screening process for new and existing OSS dependencies
  - Monitor health and make proactive decisions on sourcing options and community engagement
- Key requirements:
  - Decentralized, self-managed process
  - Enable but don't overburden developers
  - Enable follow-up and actionable insights
- Reported in https://ospobook.todogroup.org/06-chapter/ >>

RI. SE

Full paper >>

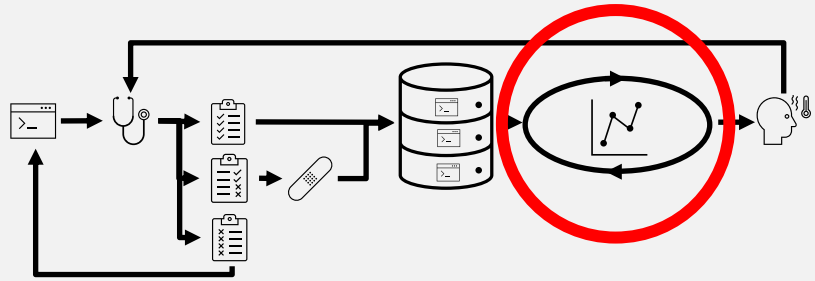
Semi-automating the health-check process



RI. SE

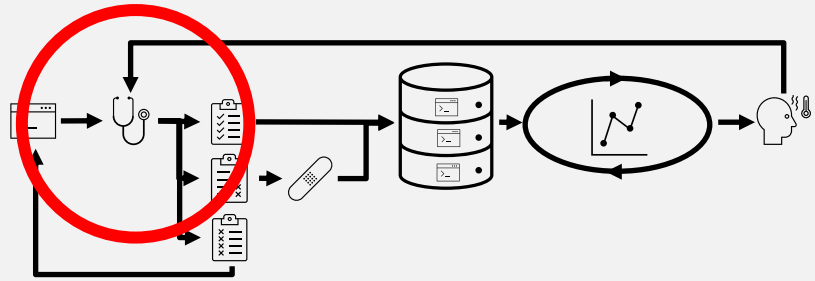
Quantitative screening

- Large amounts of dependencies commonly exist. Manual overview and inspection not applicable
- Tooling needed, intergated in CI/CD pipelines or partial-runs on regular occasions
- Runs high-level tests on dependencies tailored to the type of ecosystem and dependencies
- Flags projects and directs attention where indicators together point towards a potential risk
- Manual inspections follow by developers or analysts
- Custom tooling and/or off-the shelf. See e.g., GrimorieLab and Debricked OSS Intelligence



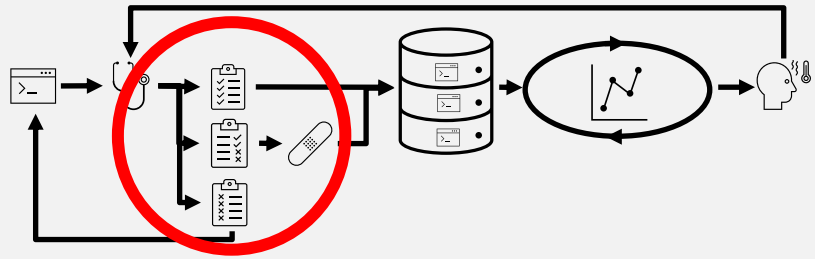
Manual inspections

- Analysis on single projects, either identified in screening, or as input to sourcing decision (intake process)
- Use of standardized checklist with automated tool support as needed
  - Trade-off between rigor and efficiency
  - Interview and map up main concerns from internal stakeholders
  - Consider types of projects used and need for tailoring
  - Needs simple answers (Yes/No) or clear categories (1-5, 6-10…)
- Lightweight documentation process, persisting and indexing analysis for future follow-up



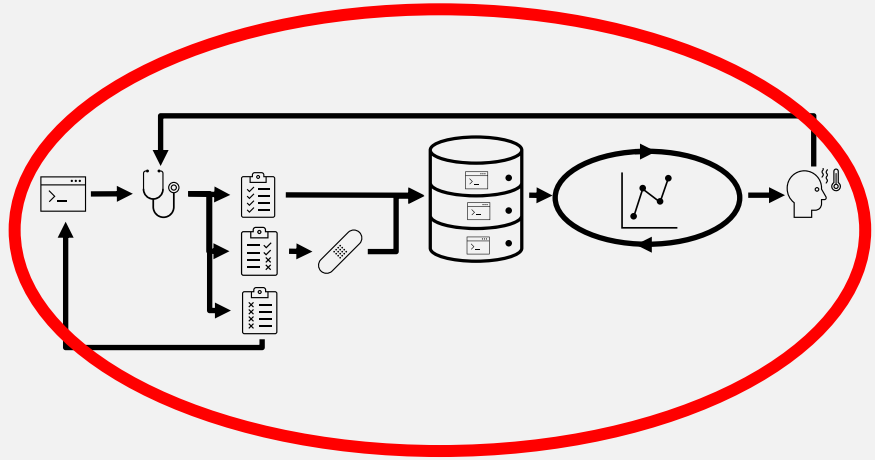
What to check for?

- Need to define the goals the analysis and the questions you want to answer
  - Main concerns and risks
  - types of OSS projects, in what domains, etc.
- Literature and practice have provided a knowledge base use together with existing initiatives, e.g., CHAOSS, OpenSSF
- Requires work up-front
- Evaluation at Scania
  - Focus group + user observations
  - Condensed into checklist of 14 health attributes



Training and follow-up needed

- Workshops for introducing checklists and analysis process
- Integrate as standard practice in development and Q&A
- Recurrent feedback session for presenting analysis of OSS projects
  - Encourage discussion, knowledge-sharing, and critical mindset
  - Contrast between types of projects, relevant questions to ask, and application/interpretation of metrics



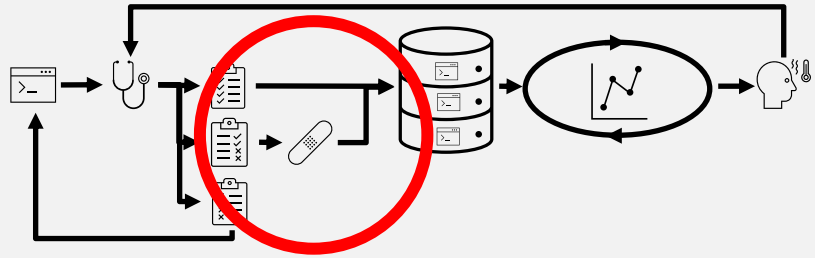
Sourcing and acquisition

- Pre-trial at large Swedish national agency
- Workshop format with internal stakeholders
- Goal was to evaluate health of to OSS e-archival solutions
- Questionnaire developed through iterations based on CHAOSS metrics
- Enable comparison between open and closed alternatives in an acquisition
- Evaluation needs to be thorough and detailed

RI.
SE

Prescribing the necessary treatments

- Secure and enable the need human resources needed for a sustainable maintenance
- Originates either from the maintainers, or the community
- Requires investments and support of a human infrastructure in the projects



Full paper >>

Human Infrastructrue in support of a sustainable maintenance

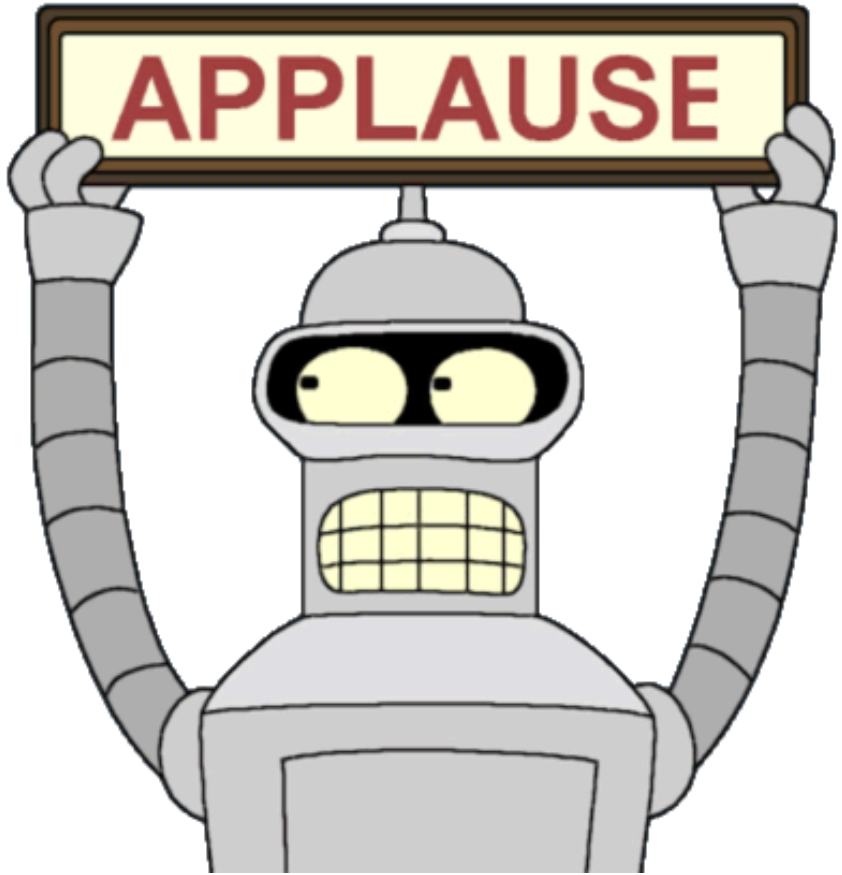
- Maintainer resources
  - Managing social expectations and peer-pressure
  - Balancing of workload with capacity
  - Finding time through funding
  - Work-life balance and prioritization
- Community resources
  - Embracing the episodic contributors
  - Mitigating toxicity
  - Promoting inclusiveness
  - Managing impact of project characteristics
  - Low-cost contributor support
  - Marketing and outreach
  - Distributing knowledge

RI. SE

Resource funding

- Full-time employment dedicated to projects
- Partially-dedicated employment
- Entrepreneurship, a common but risky endeavor
- Sponsorship, a diverse and limited source of income

Photo by Anne Nygård | https://unsplash.com/photos/brown-and-white-paper-bag-OtqaCE_SEMI


APPLAUSE