JOHAN LINÅKER

HASMOSS - Health and Security Management for Open Source Software

Open Source is a building block

- A means to create, share, and distribute reusable and modifiable bricks
- Present in > 90 % of todays software
- But who guarantees their quality and that they are safe to use?

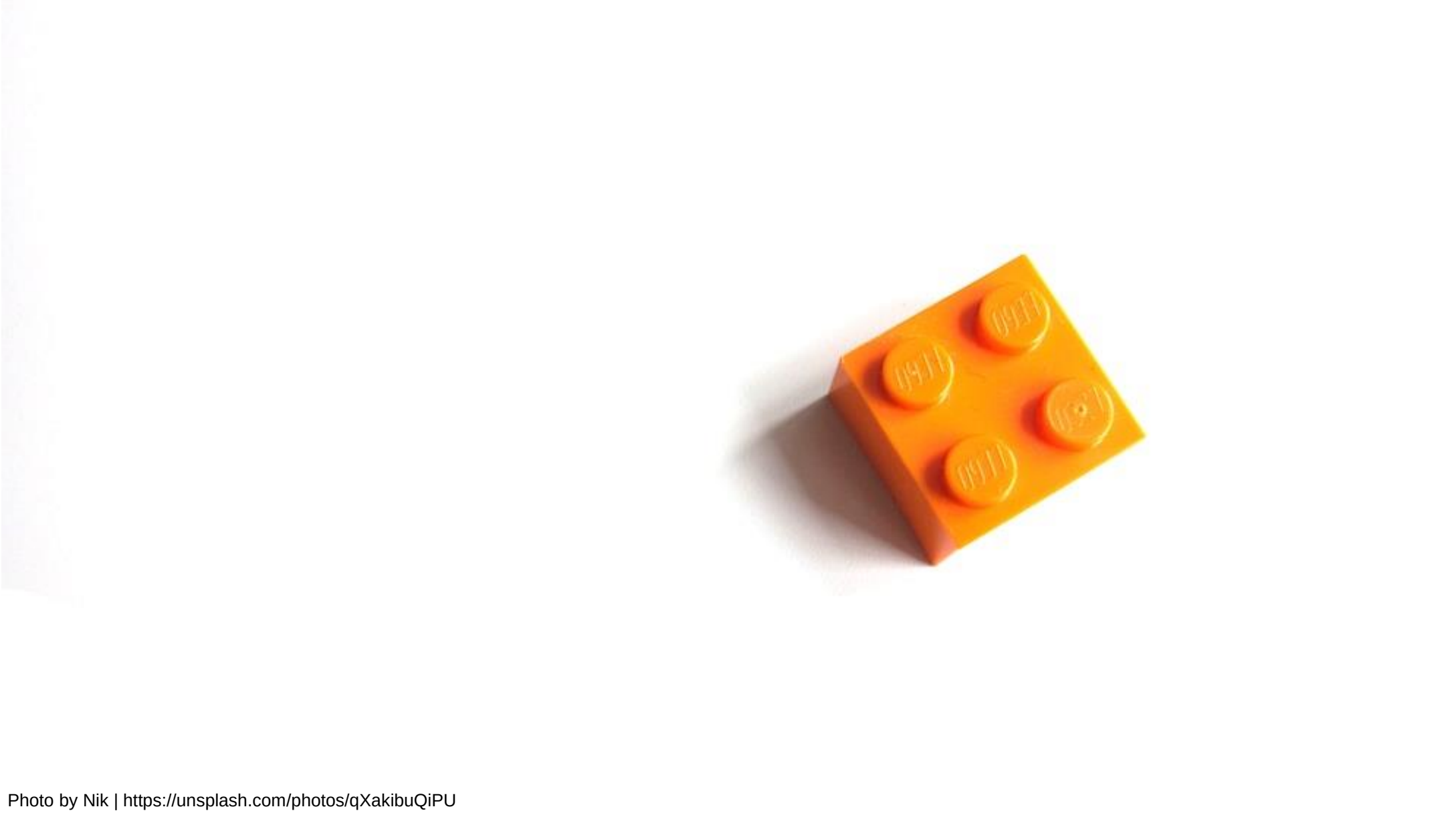


Photo by Nik | https://unsplash.com/photos/qXakibuQiPU

Photo by Xavi Cabrera | https://unsplash.com/photos/kn-UmDZQDjM

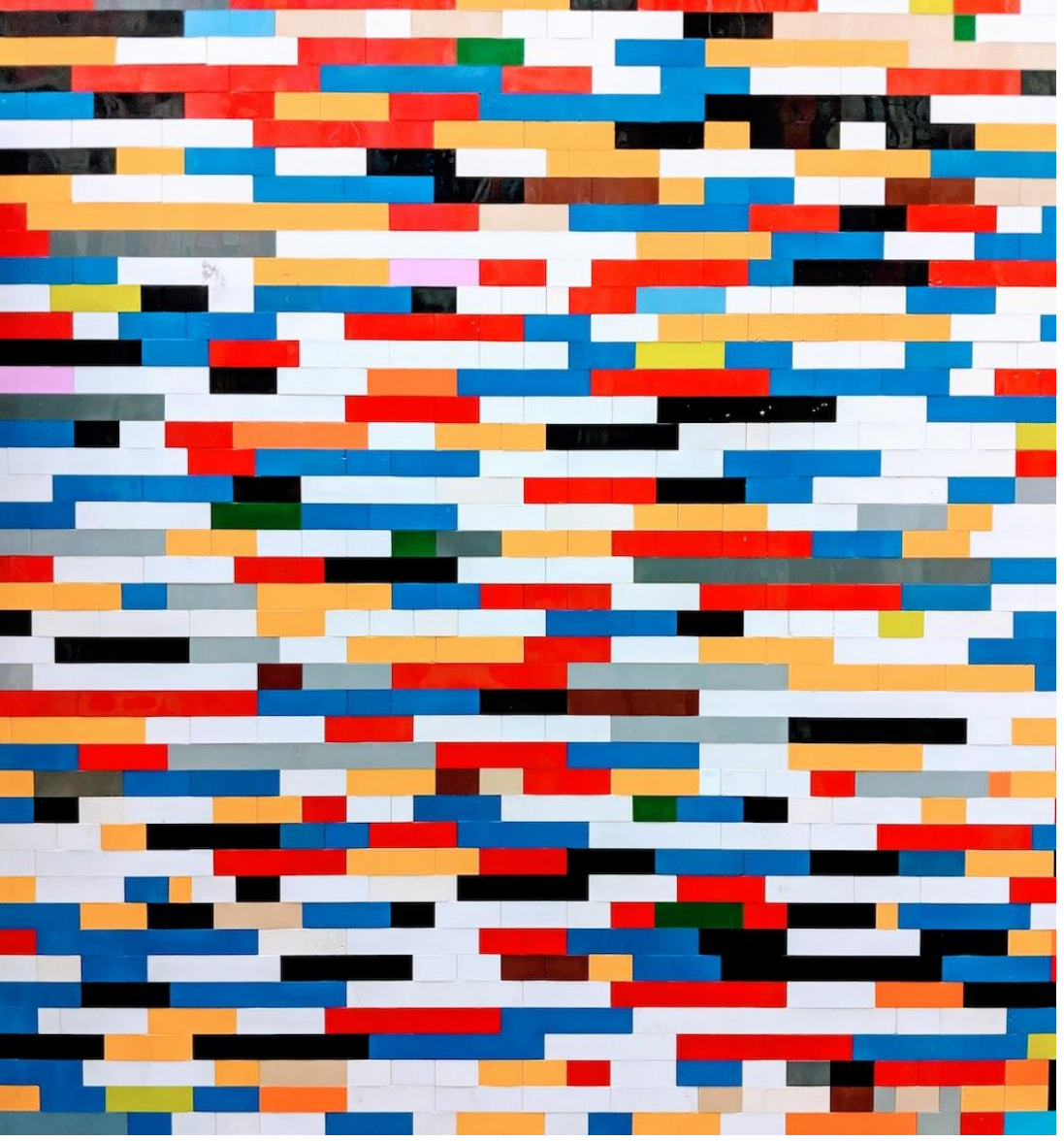


Photo by Omar Flores | https://unsplash.com/photos/lQT_bOWtysE

Open Source Software and our Digital Infrastructure

- Open Source Software makes up a vitale building block in our digital infrastructure
- Needs maintenance as with physical infrastructure to stay secure and robust

RI.
SE

Photo by Modestas Urbonas | https://unsplash.com/photos/vj_9l20fzj0

Open Source Software and our Digital Infrastructure

- Open Source Software makes up a vitale building block in our digital infrastructure
- Needs maintenance as with physical infrastructure to stay secure and robust

RI.
SE

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

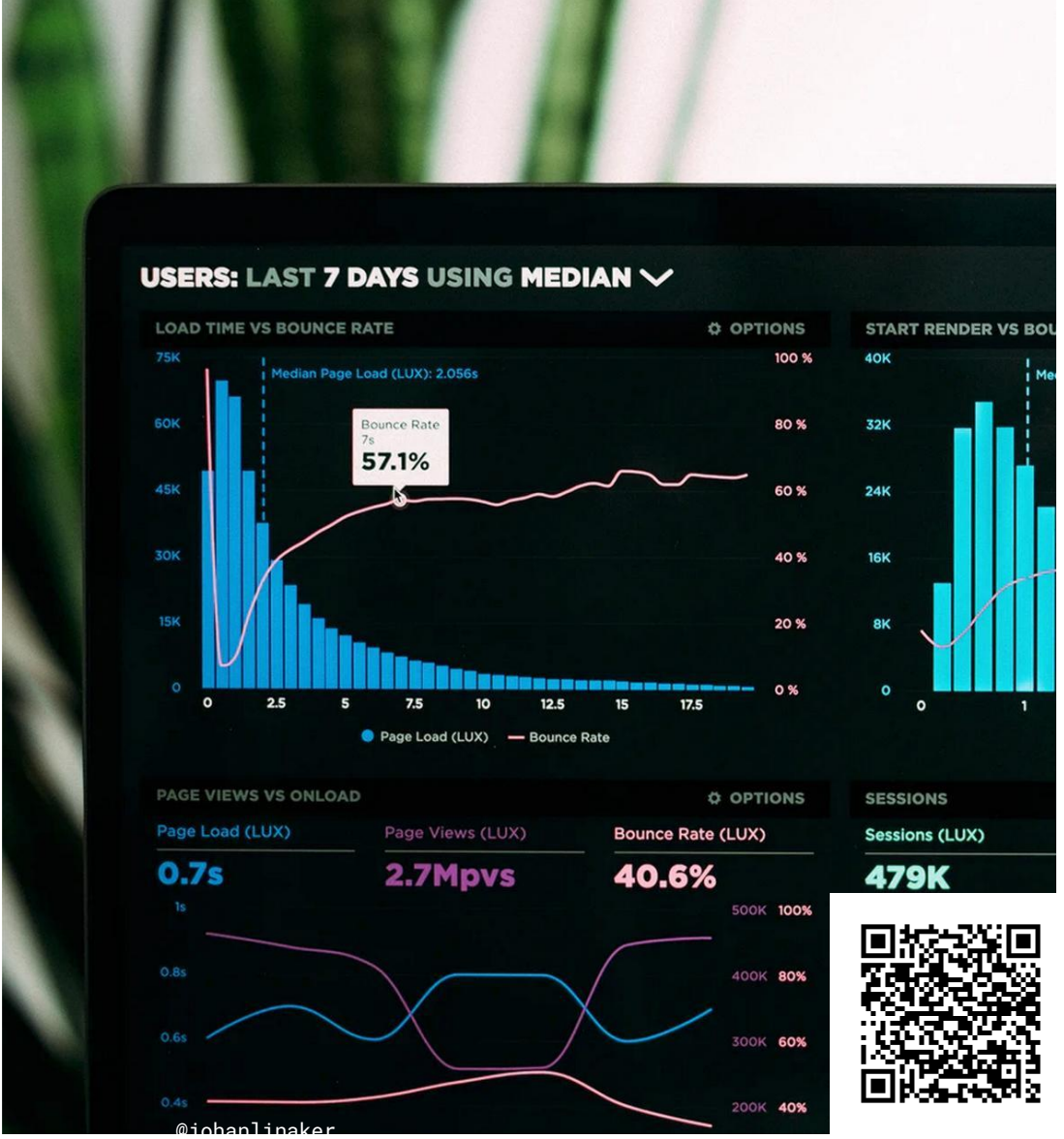
Photo by Markus Frieauff | https://unsplash.com/photos/IJ0KiXl4uys

How can we find the cracks and bumps before they appear?

How can we avoid them?

How can we mitigate them?

RI.
SE



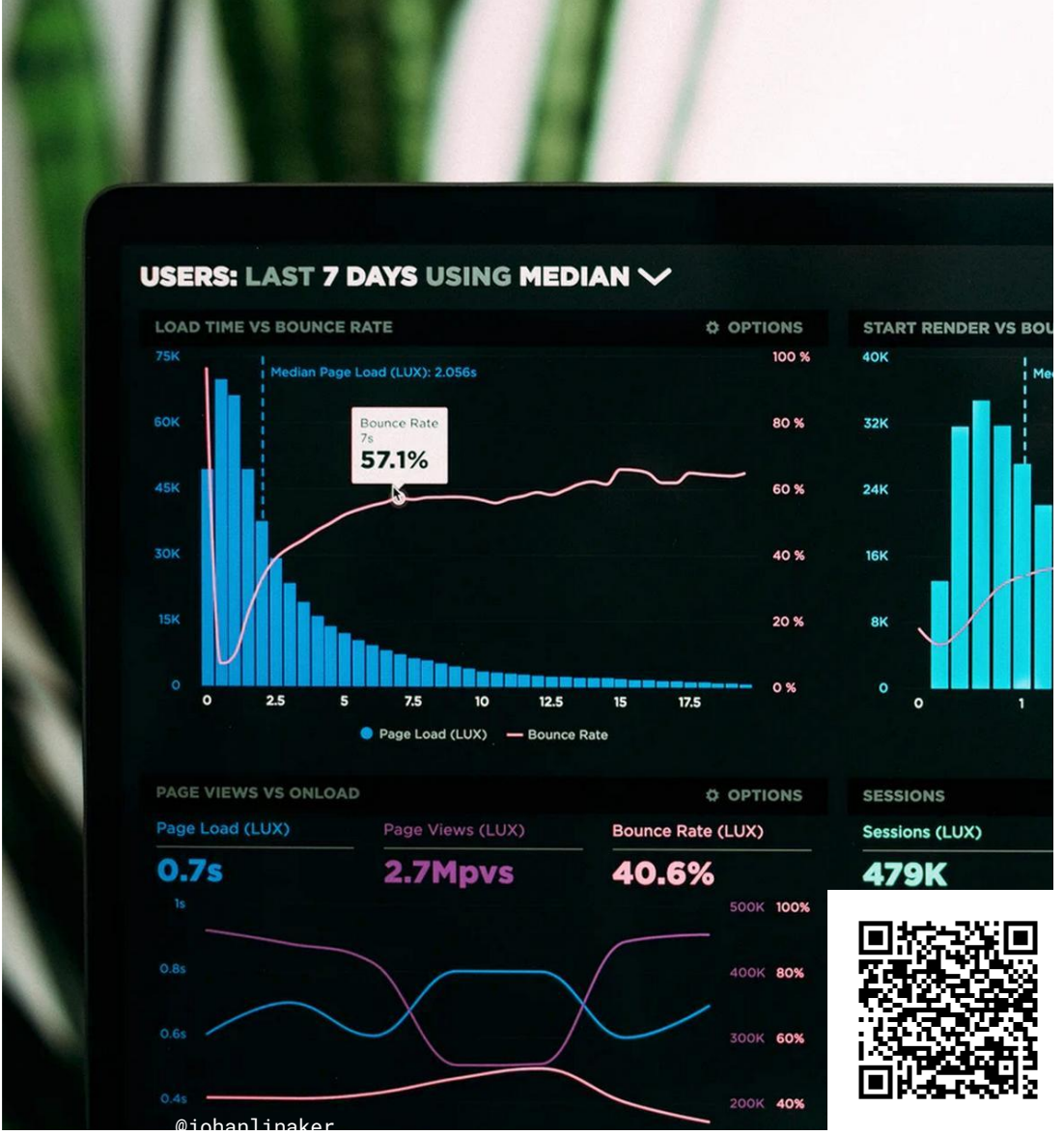
By Considering the Health of Open Source in your Intake Process

- Goals:
  - Enable health analysis at intake and acquisition of OSS, and ongoing consumption
  - Enable sourcing decisions and proactive health improving measures

* https://bit.ly/3AM5NR8

RI.SE

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



HASMOSS – Health and Security Management for Open Source Software

Partners

Observers

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 John Schnobrich | https://unsplash.com/photos/FlPc9_VocJ4

What does practice say?

- Interview survey + case study at Scania
- Validates but narrows down characteristics to smaller groups
- Need for automation
- Need to consider
  - Size & complexity
  - Strategic importance
  - Life-cycle stage
  - Governance and ownership
- Study ongoing

RI.SE

Framework structure

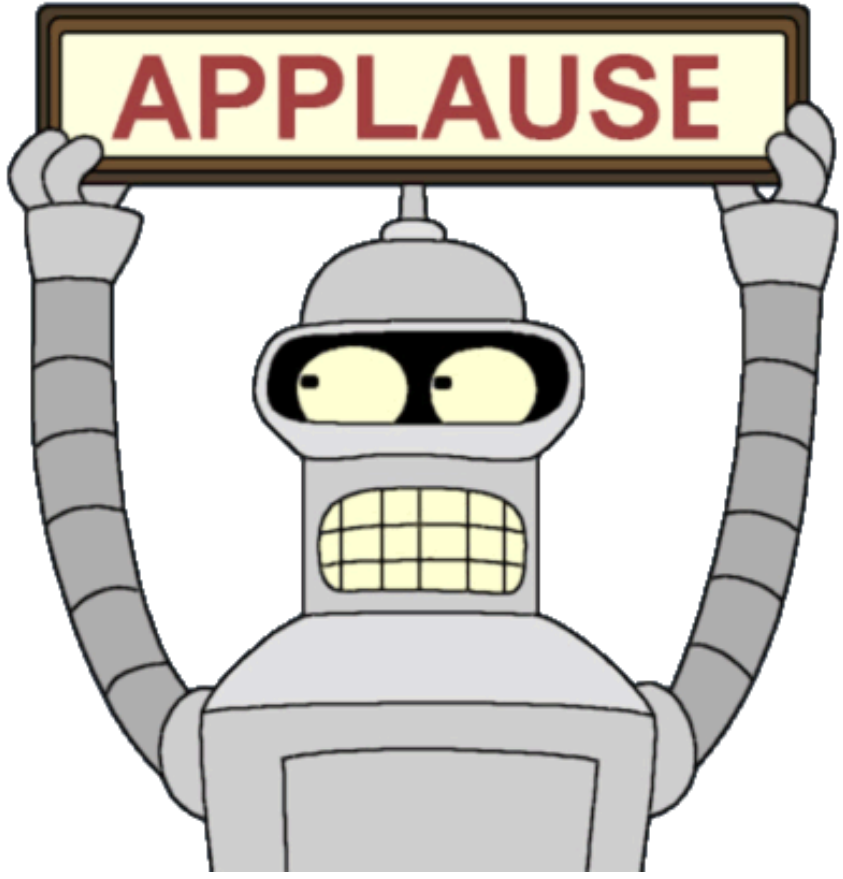
- Level of abstraction
  - Network-level
    Characteristics related to the Overarching software ecosystem or network that the OSS project is part
  - Project-level
- Socio-technical dimension
  - Actors
    Human and Community-related characteristics
  - Software
    Technical and project-related characteristics
  - Orchestration
    Governance-related characteristics

RI.SE

Future work

- Gather metrics and data sources from practitioners through observations, and contrast to what we've found in literature
- Investigate applicability and possibility to automate and quantify characteristics with industry partner (ongoing)

Photo by Tomasz Frankowski | https://unsplash.com/photos/kBUfvkbFIoE



RI.
SE