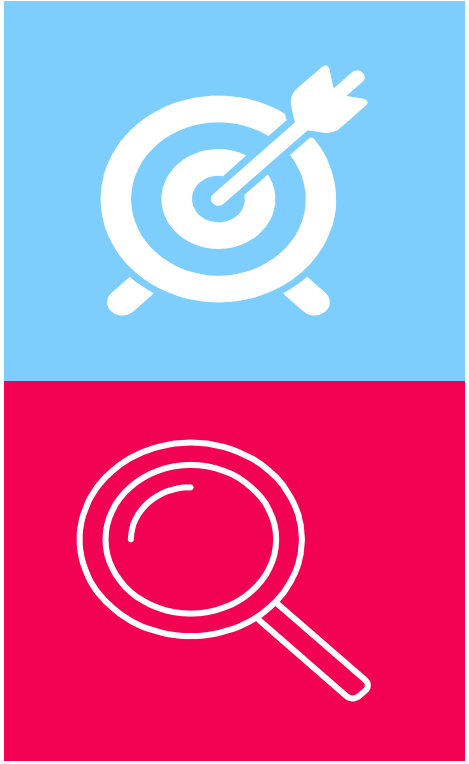
Software verification framework Klever

Ilja Zakharov
ISP RAS
ilja.zakharov@ispras.ru

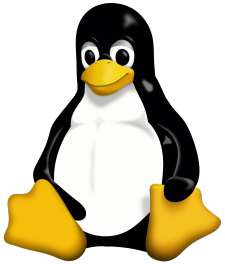


I. Klever

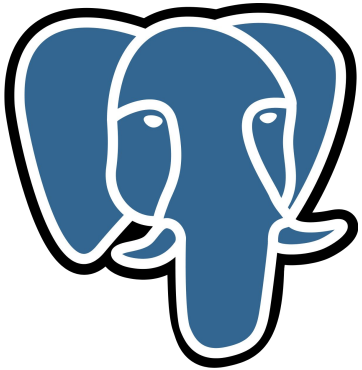
II. CPAchecker in Klever

Klever is a software verification framework for GNU C programs

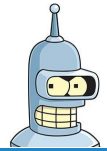
Variety of Software Projects



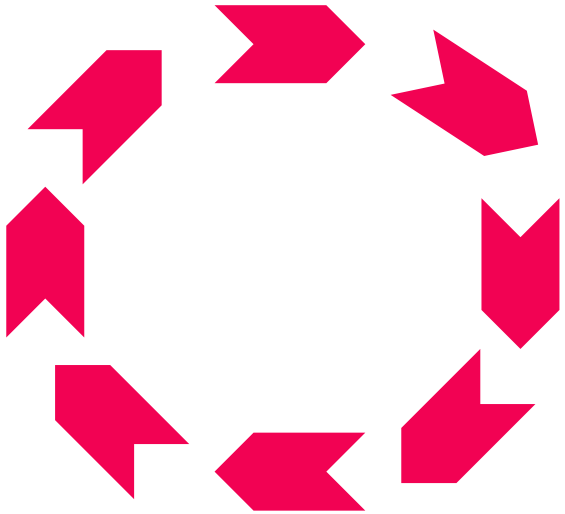
TM



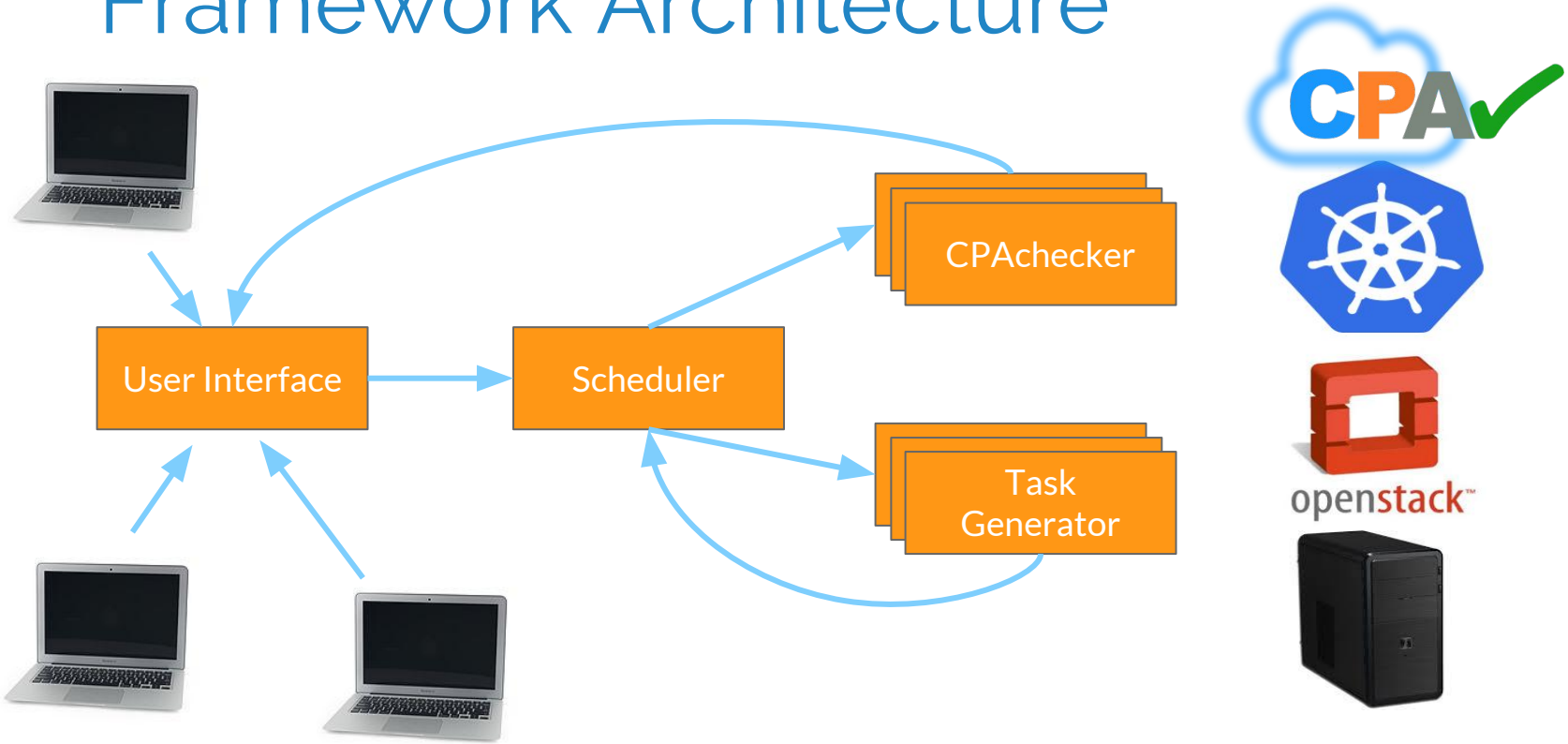
OpenSSL



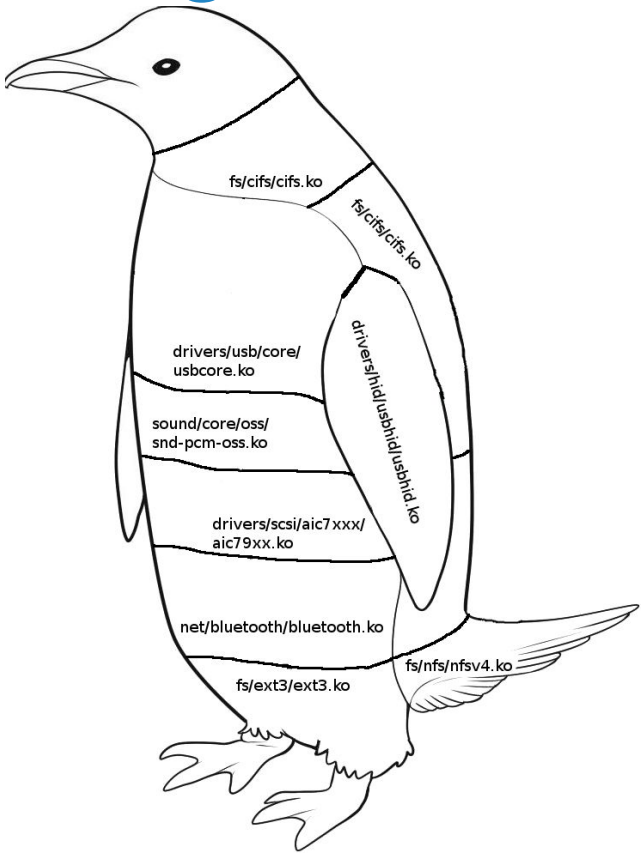
Verification Workflow



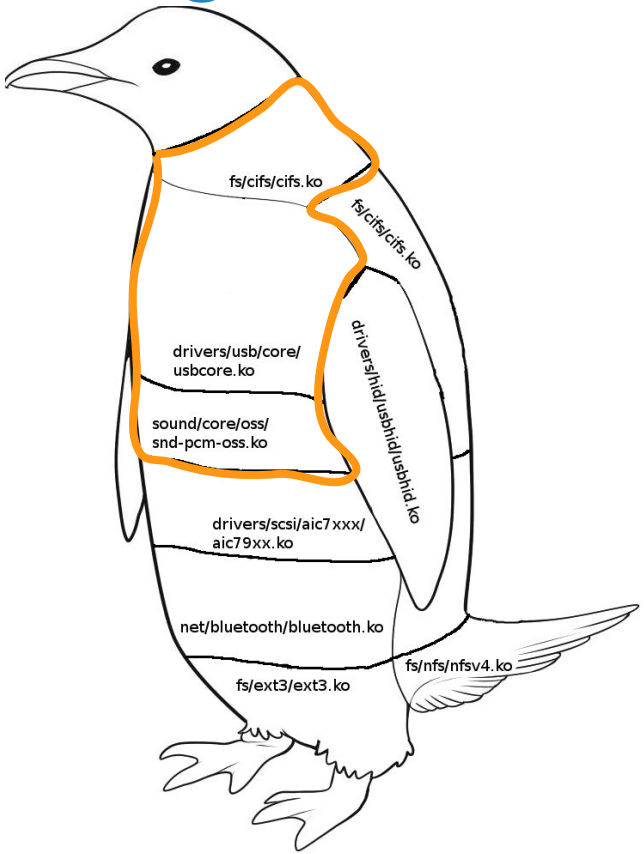
Framework Architecture

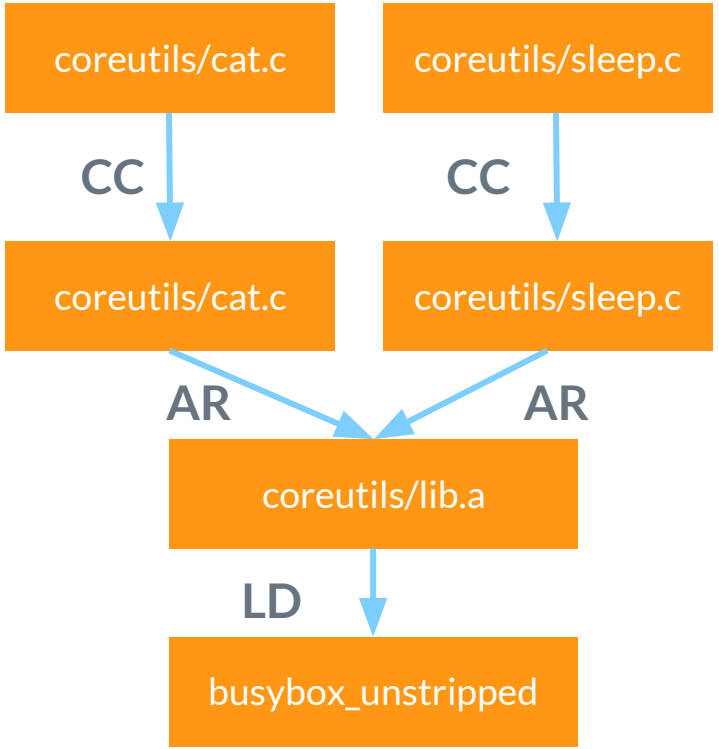


Program Decomposition

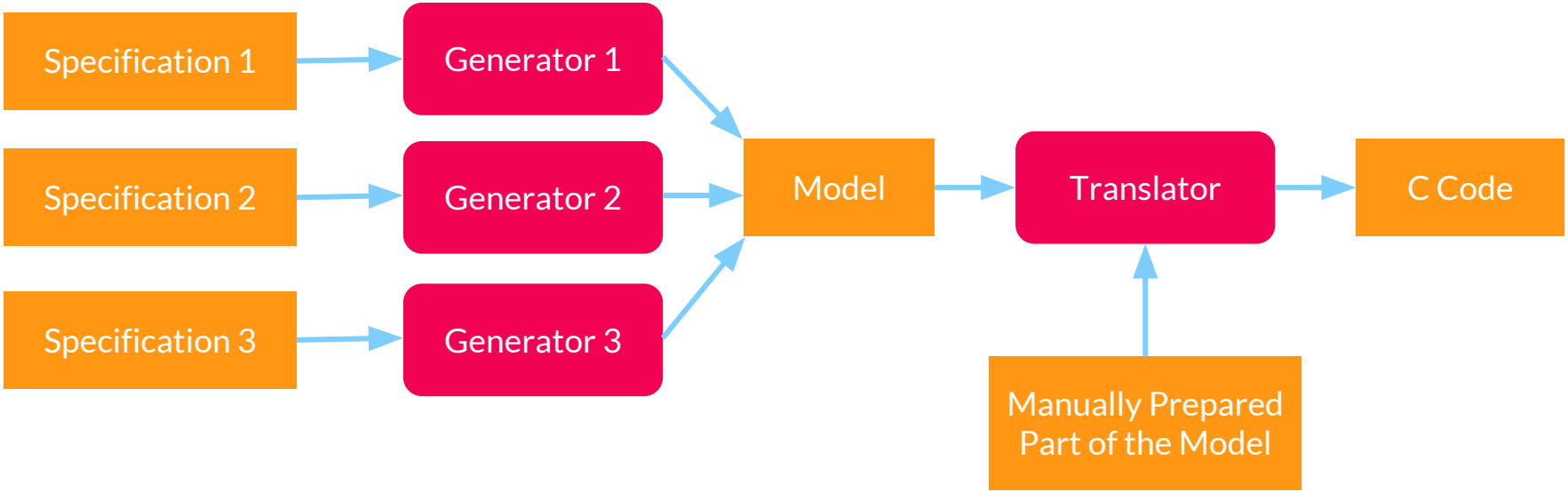


Program Decomposition



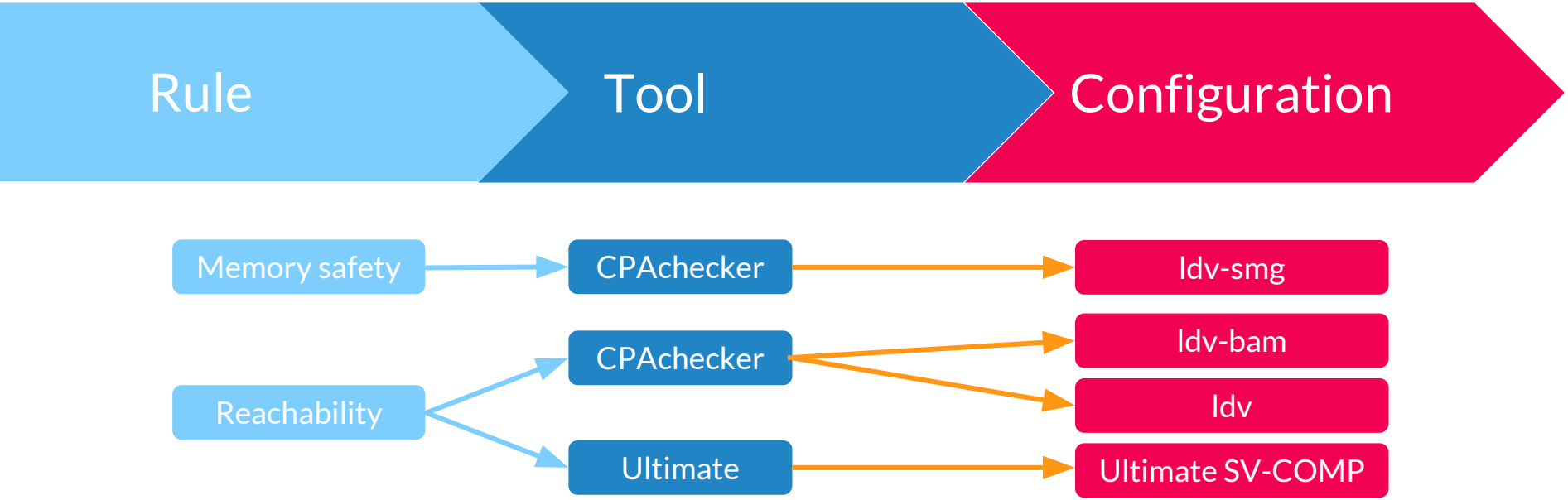


Environment modeling



Tools Configuring

Tools Configuring



Results Analysis

Witnesses visualization

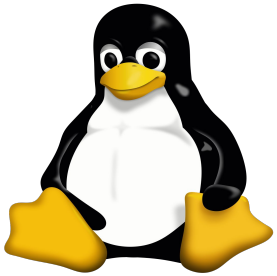
Coverage visualization

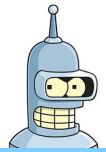
Expert analysis

Results comparison and statistics visualization

Application results

- Linux Device Drivers
- Linux kernel subsystems
- BusyBox applets
- Apache http server (initial)





Results

Project	Modules	Line coverage	Function coverage	False positives	Bugs	
Drivers (3.14)	3821	48%	36%	70%	30%	ldv-bam
Subsystems (3.9-3.19)	3 (86)	79%	70%	57%	43%	ldv-bam SMG
BusyBox	185	93%	86%	93%	7%	SMG

Status of Development

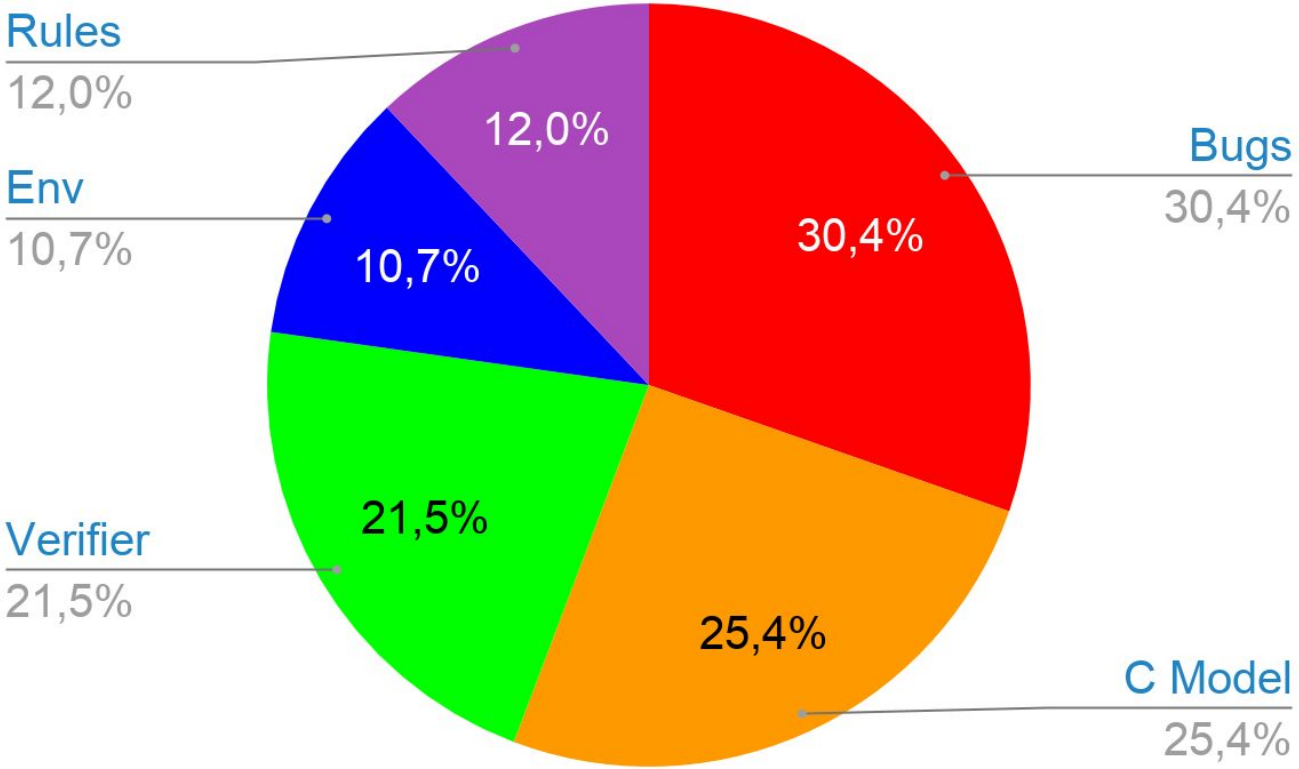
Klever 1.1	Klever 2.0	Klever 2.1
Stable framework	Userspace	Optimizations
Tests & CI	Busybox	Extended witnesses
Drivers support	Kernel subsystems	Models library

Benefits for you

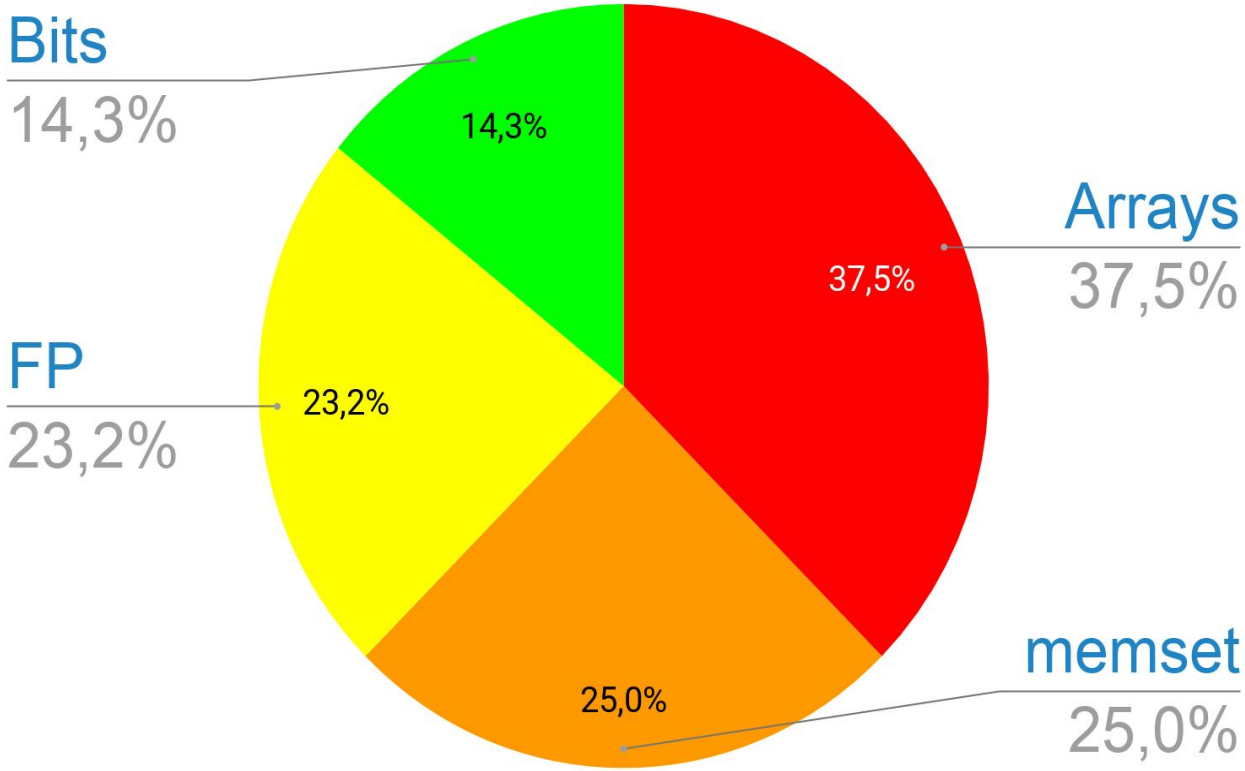
- ✓ Verification tasks from Klever
- ✓ Real bugs
- ✓ Revealed problems and restrictions
- ✓ Education

CPAchecker in Klever: statistics & feature requests

Violations for drivers



Accuracy problems (ldv-bam)



Features Wanted (CPAchecker)

Extended Witnesses

CPAchecker without CIL/with a slicer

Timeouts debug

Highlight assumptions and unsupported statements

Generic rules checking (integer overflows, deadlocks)

Features Wanted (BenchExec)

Verification mode

Benchmarking mode

Questions?

https://github.com/ldv-klever/klever
https://forge.ispras.ru/projects/klever