LinuxTesting.org

Predicate Analysis with BLAST 2.7.1

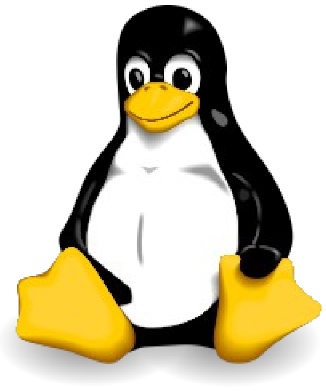
Pavel Shved, Mikhail Mandrykin, and Vadim Mutilin

ISP RAS

Institute for System Programming of the Russian Academy of Sciences

Linux Driver Verification Project Goals

- Provide infrastructure for application of verification tools to Linux device drivers
- Research new verification approaches in the industrial settings
- Improve quality of the Linux device drivers



BLAST 2.5

Berkeley

Lazy

Abstraction

Software Verification

Tool

BLAST is a software model checker for C programs.

It uses counterexample-driven automatic abstraction refinement to construct an abstract model which is model checked for safety properties.

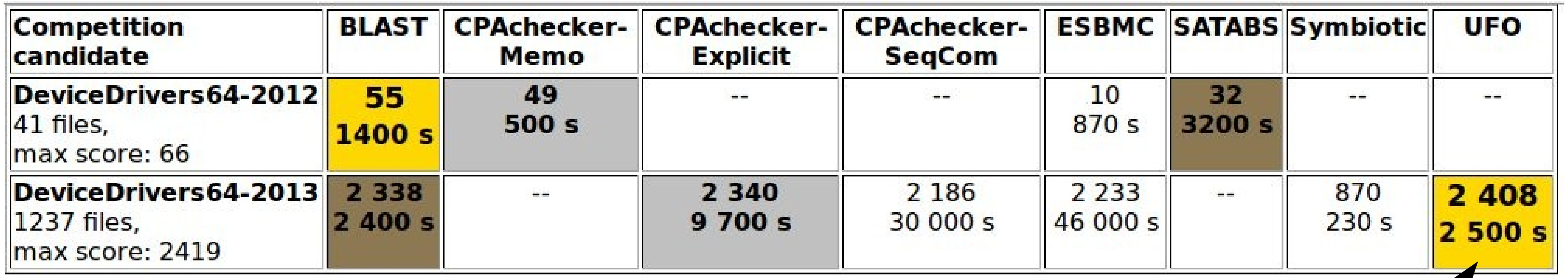
SV-COMP 2012 – BLAST 2.7

- General
- Program Representation
- Counter Example Analysis
- Refinement
- Pointer Analysis
- Configurable Program Analysis

SV-COMP 2013 – BLAST 2.7.1

- Goal of competing:
  To see how far the other tools improved

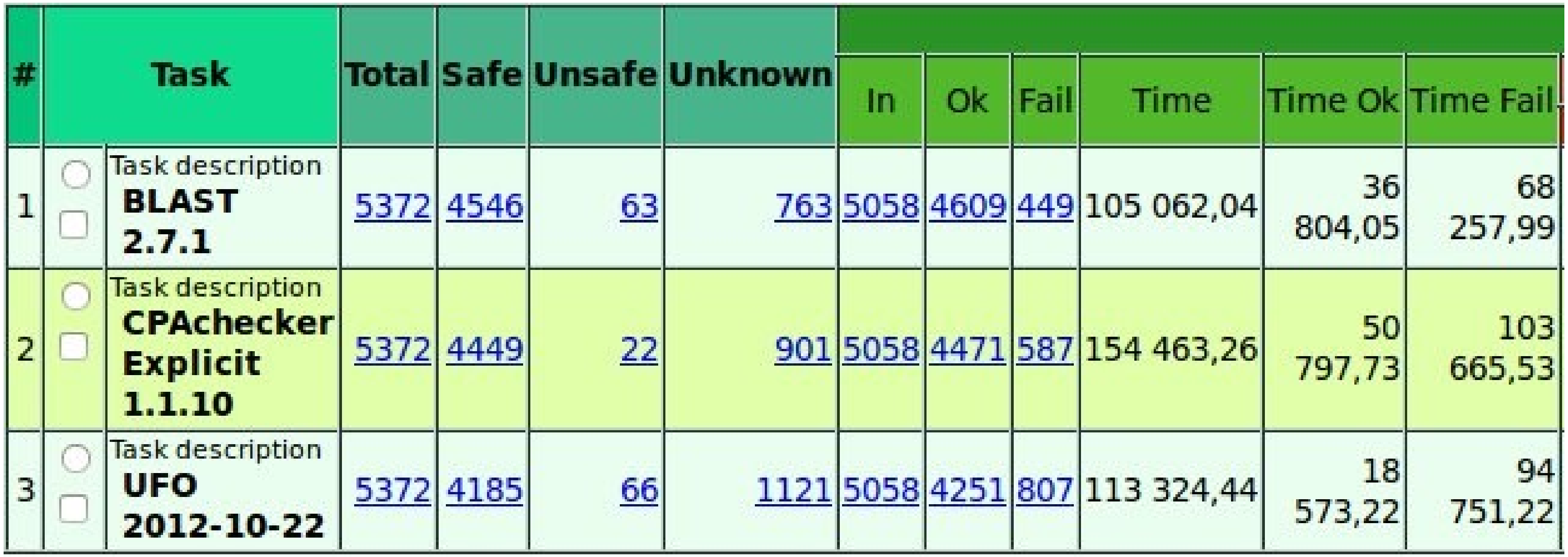
Tool Improvements on DeviceDrivers64 Category



Competition candidate	BLAST	CPAchecker-Memo	CPAchecker-Explicit	CPAchecker-SeqCom	ESBMC	SATABS	Symbiotic	UFO
DeviceDrivers64-2012 41 files, max score: 66	**55** **1400 s**	**49** **500 s**	--	--	10 870 s	**32** **3200 s**	--	--
DeviceDrivers64-2013 1237 files, max score: 2419	**2 338** **2 400 s**	--	**2 340** **9 700 s**	2 186 30 000 s	2 233 46 000 s	--	870 230 s	**2 408** **2 500 s**

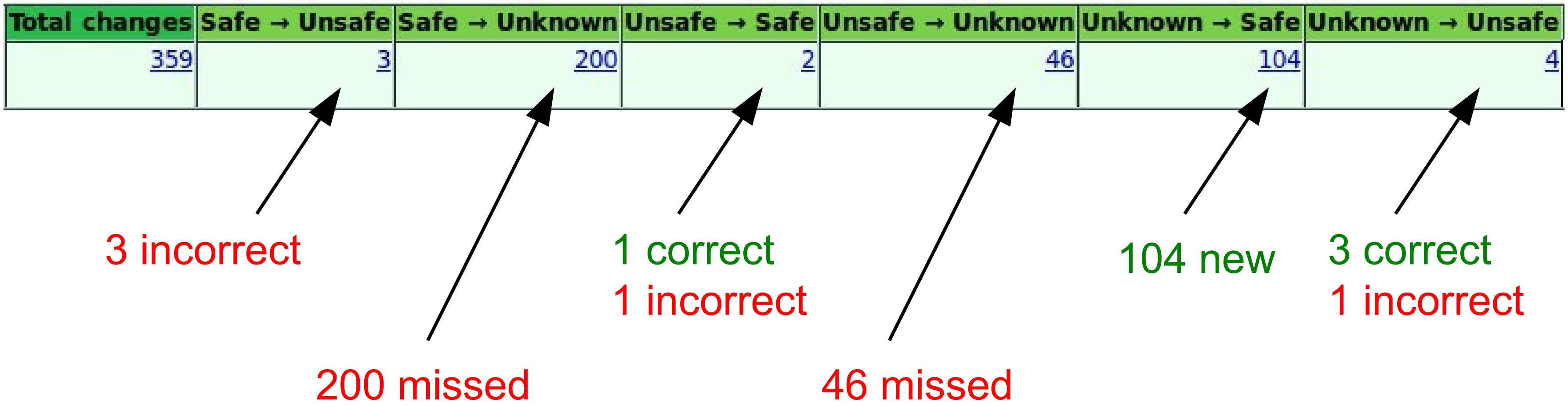
New tool

Verification of Linux-3.8-rc1 Device Drivers



#	Task		Total	Safe	Unsafe	Unknown	In	Ok	Fail	Time	Time Ok	Time Fail
1	○ □	Task description **BLAST 2.7.1**	5372	4546	63	763	5058	4609	449	105 062,04	36 804,05	68 257,99
2	○ □	Task description **CPAchecker Explicit 1.1.10**	5372	4449	22	901	5058	4471	587	154 463,26	50 797,73	103 665,53
3	○ □	Task description **UFO 2012-10-22**	5372	4185	66	1121	5058	4251	807	113 324,44	18 573,22	94 751,22

BLAST → CPAchecker



Total changes	Safe → Unsafe	Safe → Unknown	Unsafe → Safe	Unsafe → Unknown	Unknown → Safe	Unknown → Unsafe
359	3	200	2	46	104	4

3 incorrect

200 missed

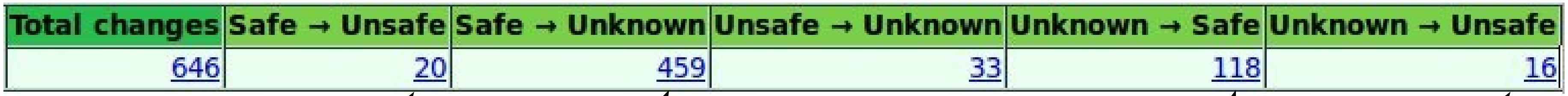
1 correct
1 incorrect

46 missed

104 new

3 correct
1 incorrect

BLAST → UFO



Total changes	Safe → Unsafe	Safe → Unknown	Unsafe → Unknown	Unknown → Safe	Unknown → Unsafe
646	20	459	33	118	16

Incorrect ???

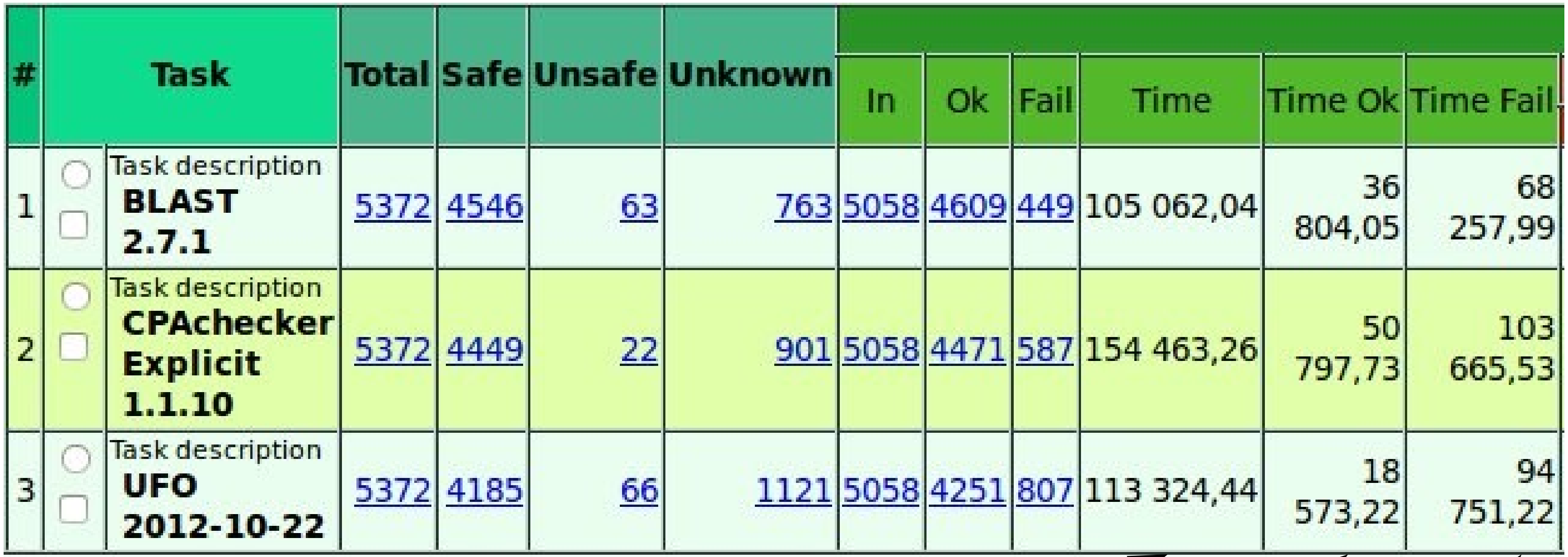
459 missed

33 missed

118 new

Incorrect ???

Verification of Linux-3.8-rc1



#	Task		Total	Safe	Unsafe	Unknown						
							In	Ok	Fail	Time	Time Ok	Time Fail
1	○ □	Task description **BLAST 2.7.1**	5372	4546	63	763	5058	4609	449	105 062,04	36 804,05	68 257,99
2	○ □	Task description **CPAchecker Explicit 1.1.10**	5372	4449	22	901	5058	4471	587	154 463,26	50 797,73	103 665,53
3	○ □	Task description **UFO 2012-10-22**	5372	4185	66	1121	5058	4251	807	113 324,44	18 573,22	94 751,22

Time of waiting for the results

SV-COMP time

Time for UNKNOWN verdicts

Suggestions

- Require to produce readable verification trace (preferably in a common format)
- Compare verification times together with time for UNKNOWN verdicts

LinuxTesting.org

Thank you!

- Vadim Mutilin
mutilin@ispras.ru
http://linuxtesting.org/project/ldv

ISP RAS

Institute for System Programming of the Russian Academy of Sciences