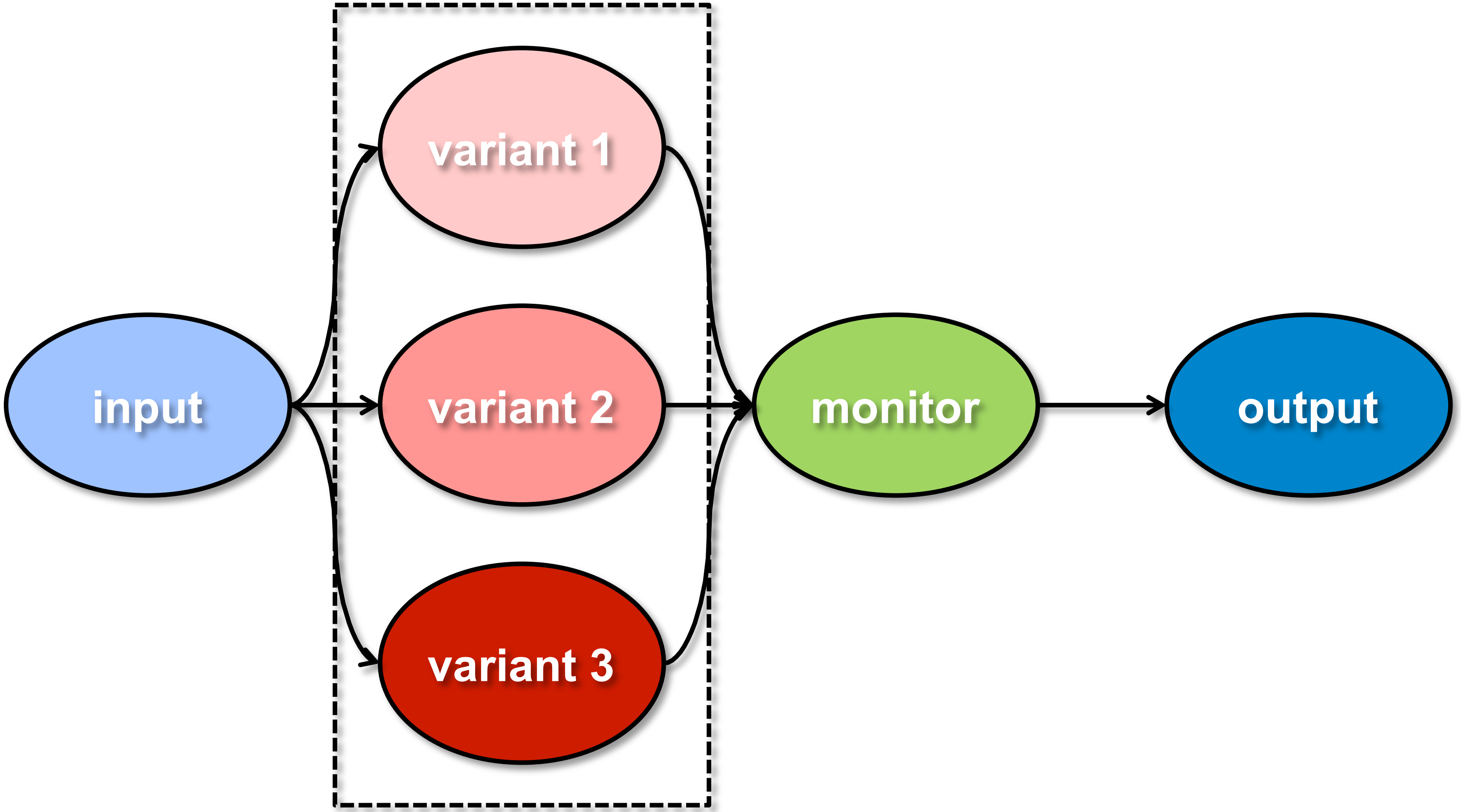
GHUMVEE: Efficient, Effective and Flexible Replication

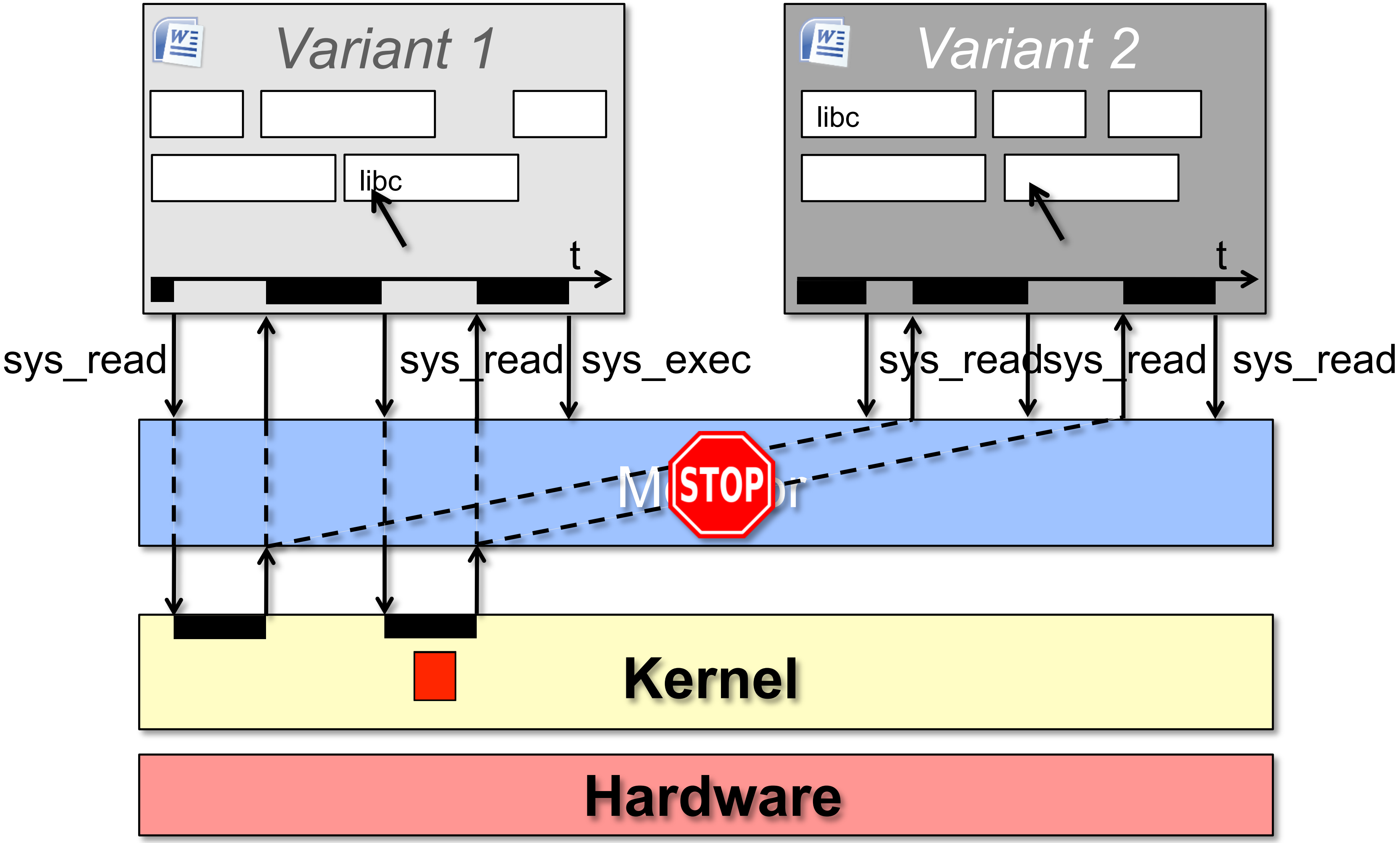
Stijn Volckaert
Computer Systems Lab
Ghent University
Belgium

N-modular Redundancy



equivalent components

Replication



Replication Goals

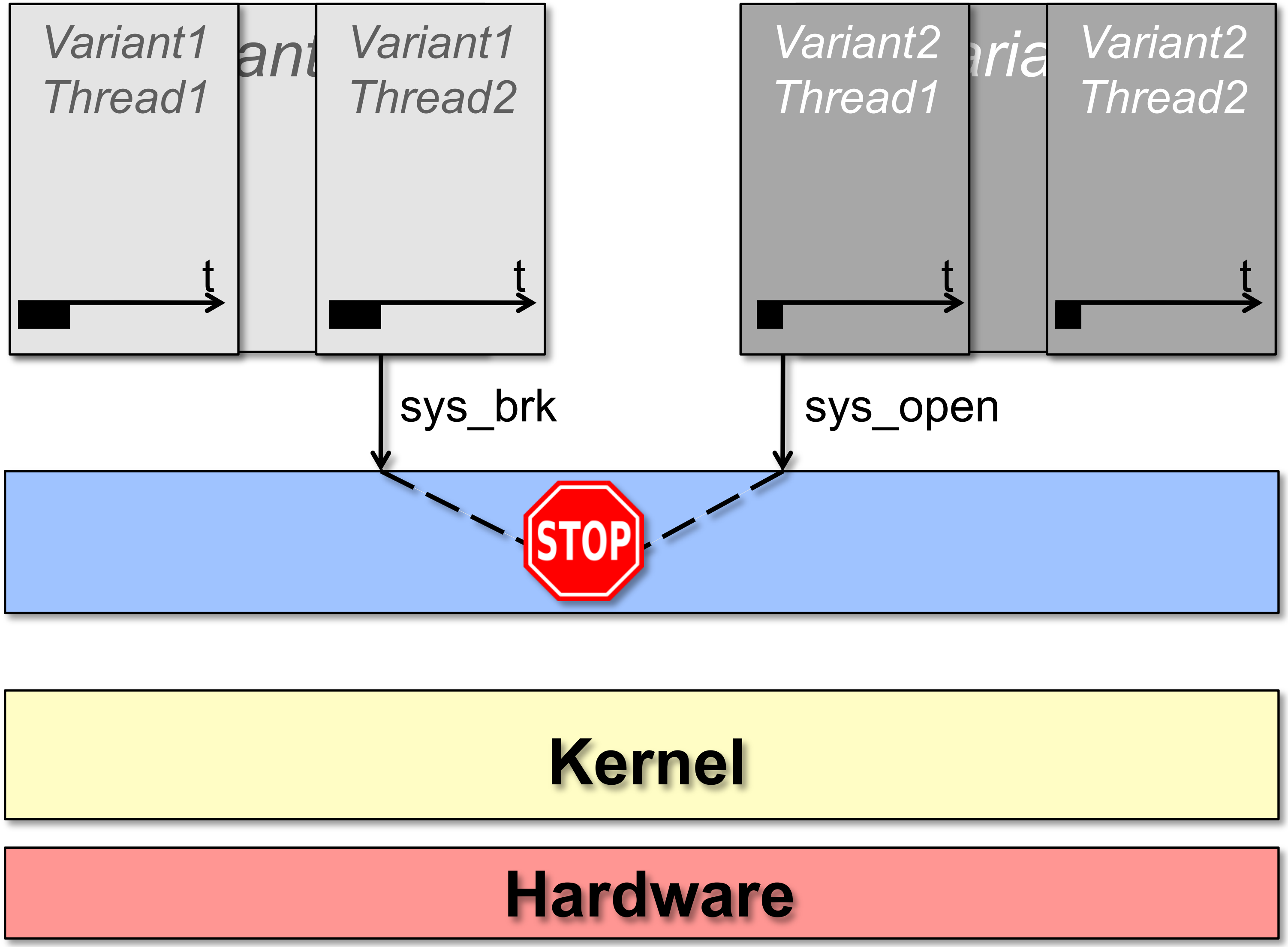
- Run variants in parallel on the same inputs
- Detect inconsistent behavior
- Transparent to user and programmer
- Minimal overhead
- Support wide range of diversity
- Run realistic programs

- Cox, B., Evans, D., et al.: N-variant systems: A secretless framework for security through diversity. In: Proc. USENIX SSYM. (2006) 105-120
- Berger, E., Zorn, B.: DieHard: probabilistic memory safety for unsafe languages. In: Proc. ACM PLDI. (2006) 158-168
- Bruschi, D., Cavallaro, L.: Diversifed Process Replicae for Defeating Memory Error Exploits. In: Proc. IEEE IPCCC. (2007) 434-441
- Salamat, B., Jackson, T., et al.: Orchestra: A User Space Multi-Variant Execution Environment. In: Proc. EuroSys. (2009) 33-46

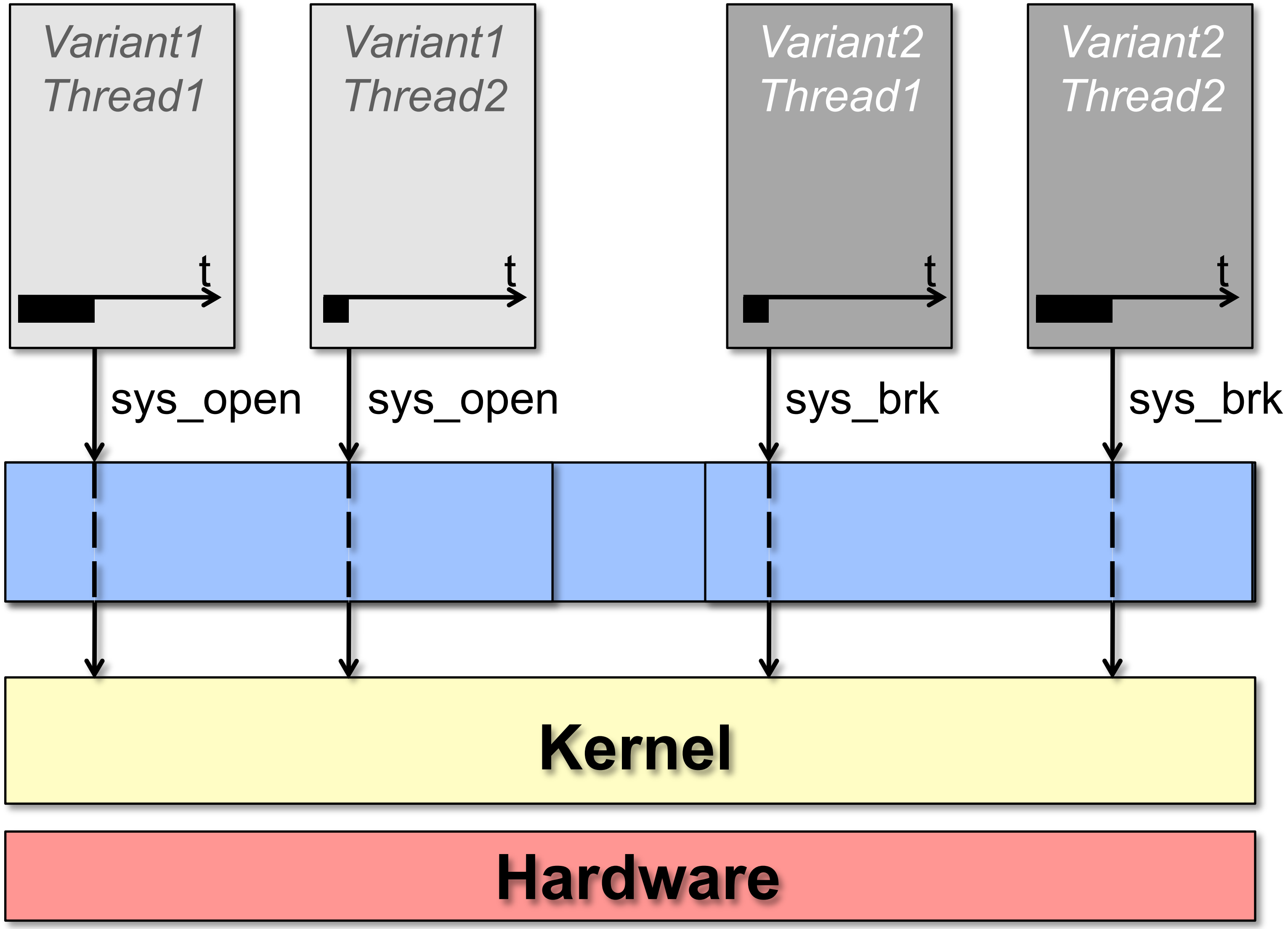
Overview

- **Introduction**
  - Replication
  - GHUMVEE Overview
- **Implementation challenges**
  - Multithreading & synchronization
  - Address-sensitive behavior
- **Evaluation**
- **Conclusions**

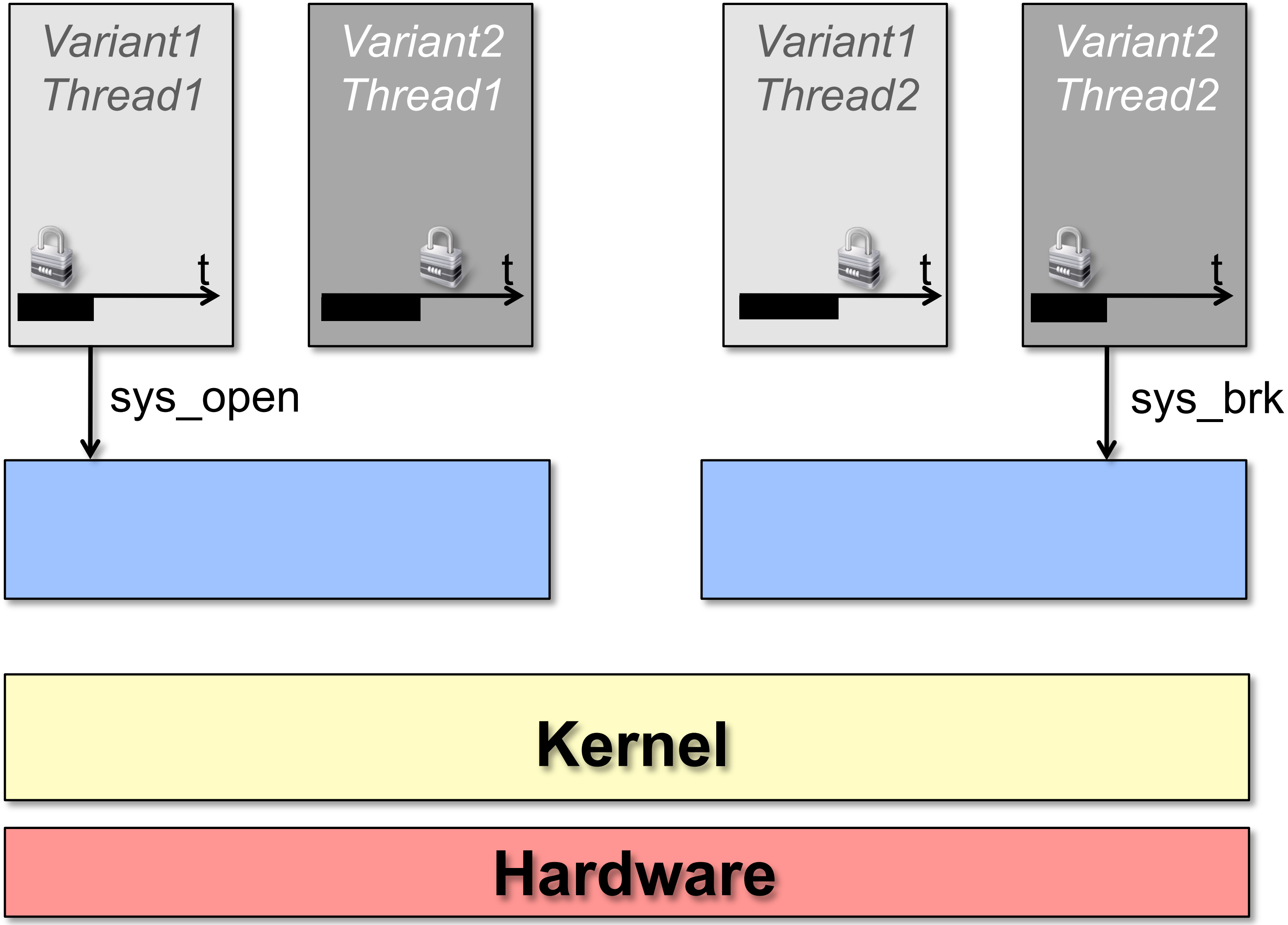
Multithreading (1)



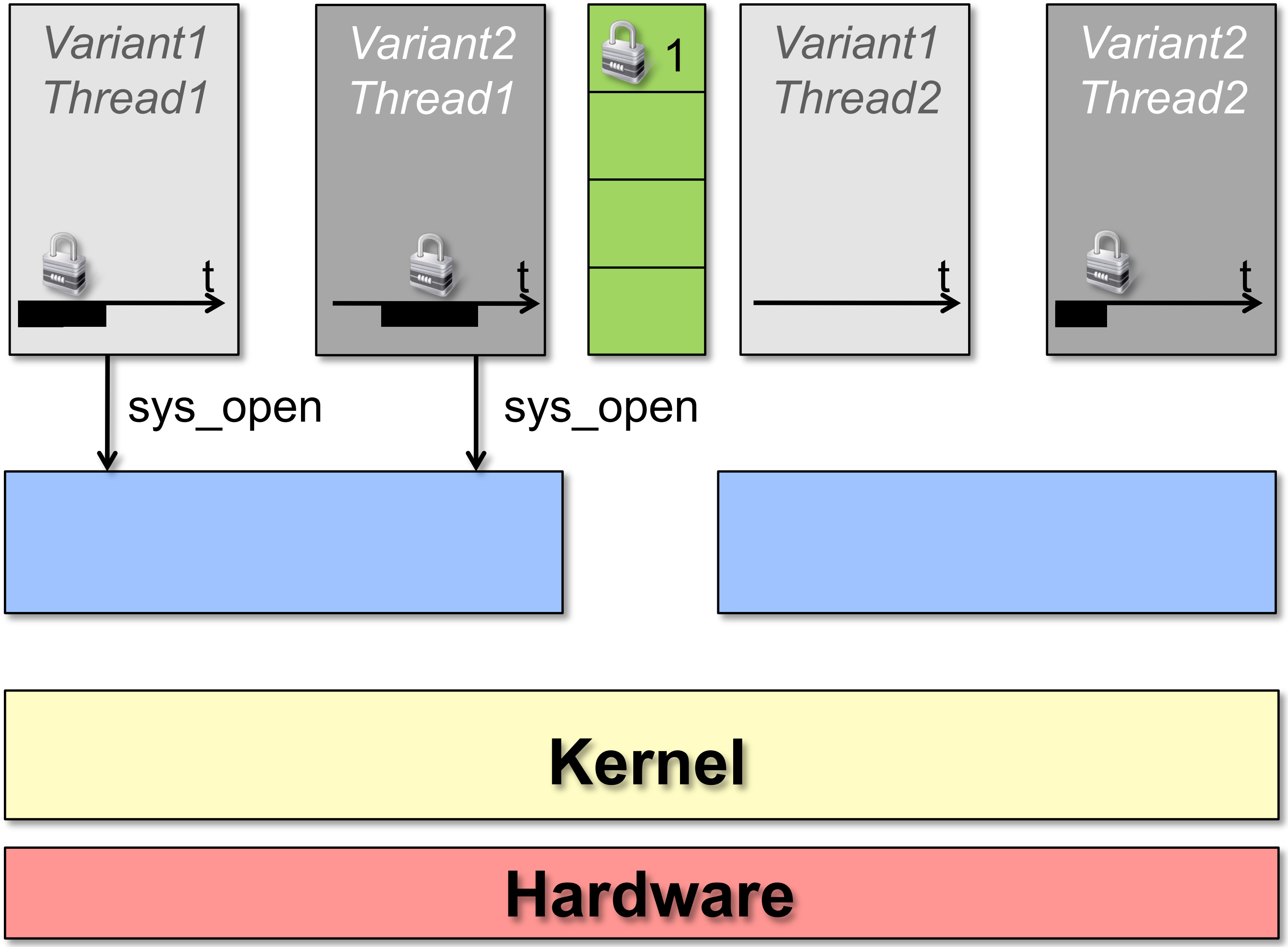
Multithreading (2)



User-space locking operations (1)



User-space locking operations (2)



Variant1 Thread1

Variant2 Thread1

1

Variant1 Thread2

Variant2 Thread2

t

t

t

t

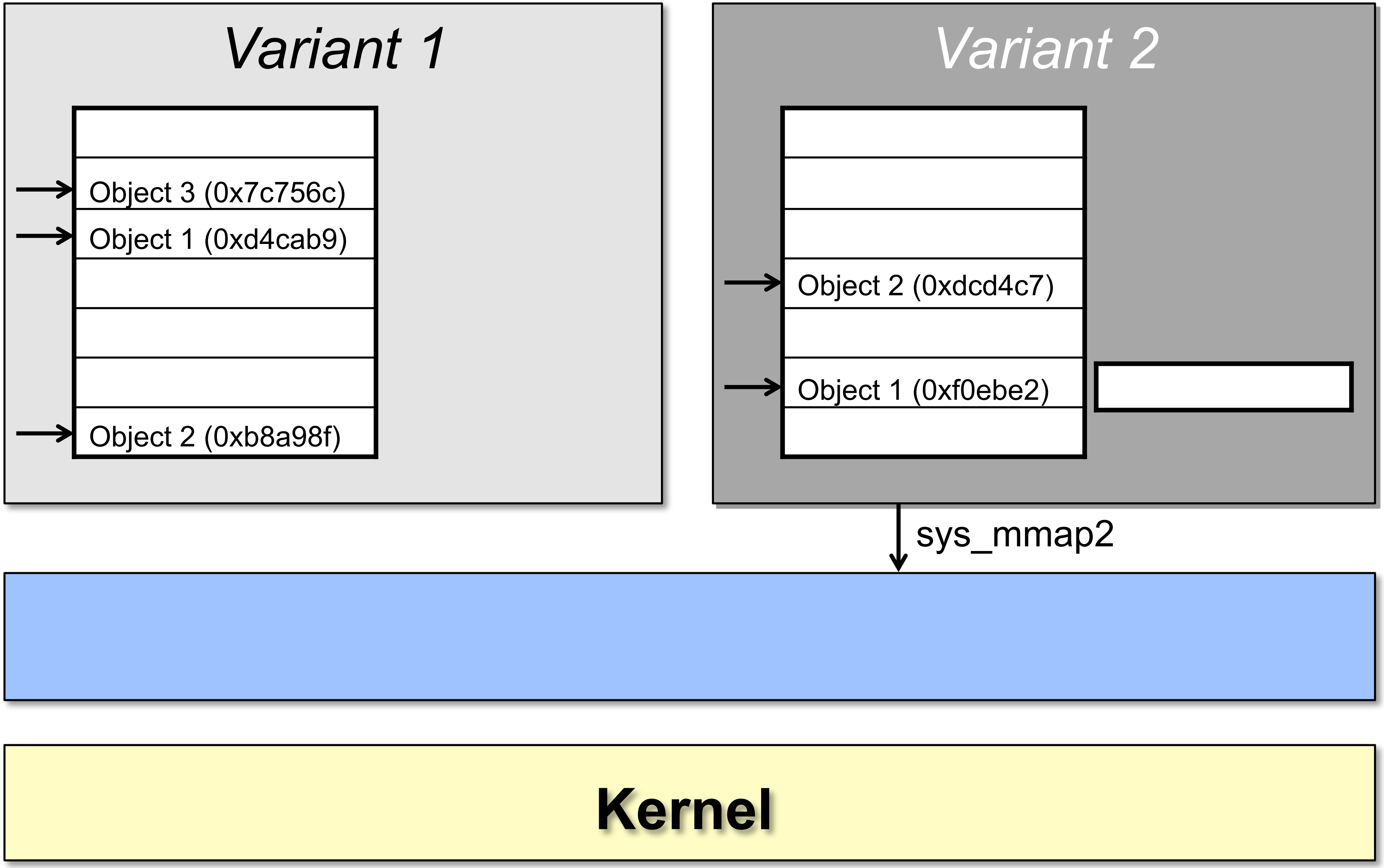
sys_open

sys_open

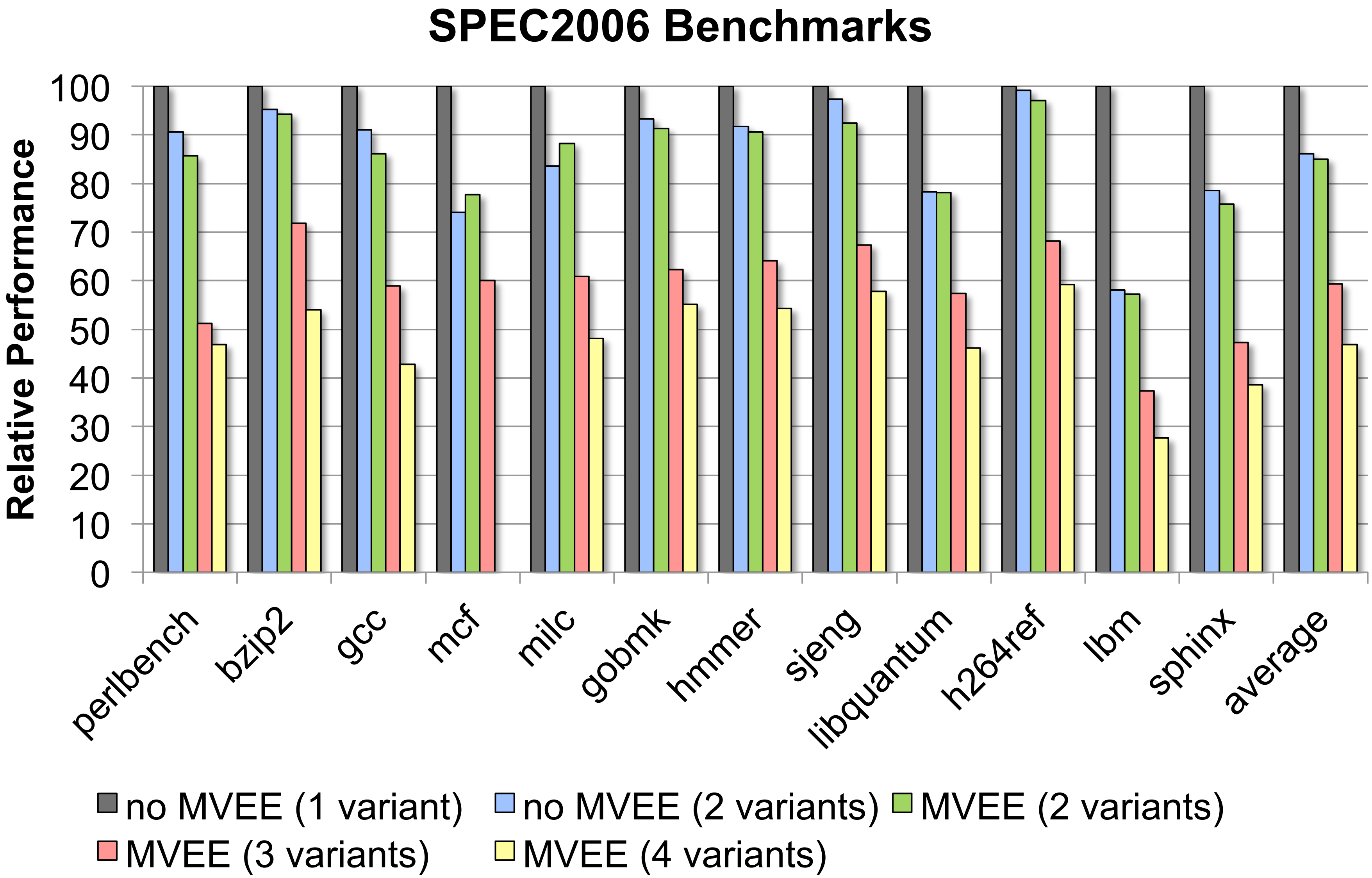
Kernel

Hardware

Address-Sensitive Behavior

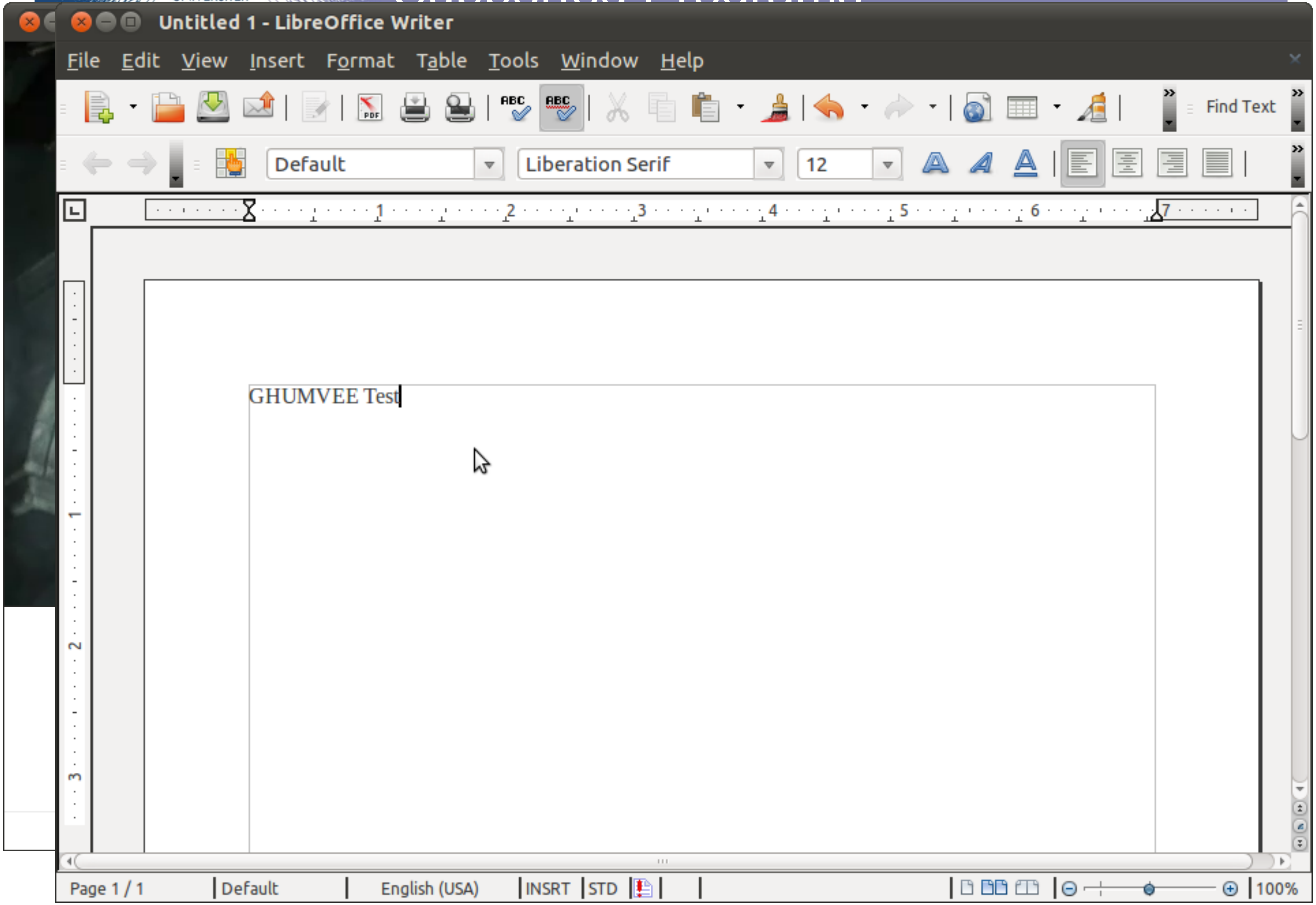


Benchmarks



Measured on a core i7-870 quad core system

Supported Programs



Untitled 1 - LibreOffice Writer
File Edit View Insert Format Table Tools Window Help
Find Text
Default
Liberation Serif
12
Page 1 / 1
Default
English (USA)
INSRT
STD
100%

GHUMVEE Test

Problematic features

	Multi-threaded	Custom Sync	Address Sensitive	Shared Mem	Mem-mapped I/O	Time-Aware (rdtsc)	Self-aware (/proc)
Glibc	✓	✓				✓	✓
Glib (GNOME)	✓		✓	✓			
kcalc	✓			✓	✓		
firefox	✓	✓	✓	✓	✓		✓
LibreOffice	✓	✓	✓	✓	✓		
MPlayer	✓				✓		

Transparency

- **For the user:**
  - Startup overhead
- **For the programmers:**
  - Indicate names of functions that need interception
  - Don’t inline these functions

standard library	interposer library (header files)	libc	pthread	interposer base lib	total
lines of C code	260	654	766	829	2509

application library	glib	gtk	orbit	pango	libreoffice	total
lines of C code	105	54	78	54	183	474

Conclusions

- Realistic programs
- Limited performance overhead (~15%)
- Limitations for programmers