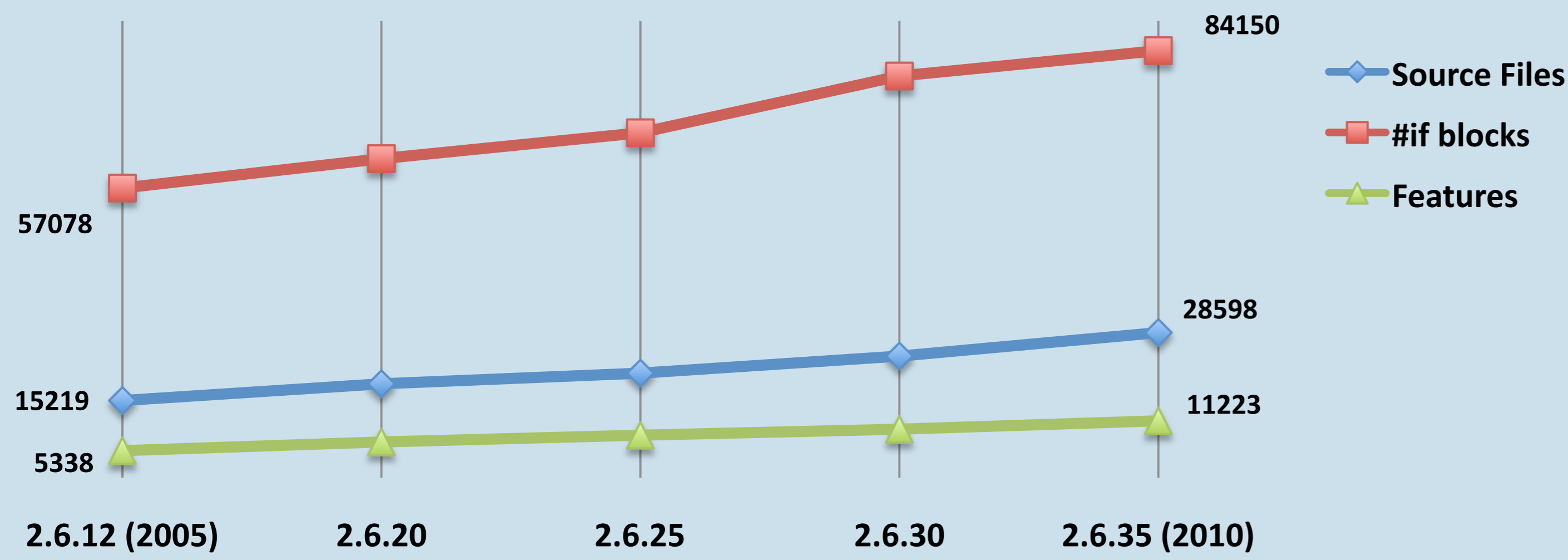


R. Tartler, D. Lohmann, J. Sincero, Ch. Dietrich, Ch. Egger, W. Schröder-Preikschat

## Introduction

- ▶ Much system software is **configurable** at compile-time
- ▶ In fact two worlds: **configuration** ↔ **implementation**  
(in Linux: **10,000** KConfig items ↔ **80,000** #ifdef blocks)
- ▶ This is prone to inconsistencies → **configurability defects** → **bugs**



- ▶ Numbers have **doubled** within the last five years!
- ▶ Existing bug-detection tools are **configurability agnostic**

## Problem Analysis

- ▶ Two flavors of configurability defects:
  1. **Symbolic** defects → integrity violation wrt. feature **identifiers**
  2. **Logic** defects → integrity violation wrt. feature **constraints**
- ▶ Two confirmed examples, found by our tool:

### Symbolic

```
diff --git a/kernel/smp.c b/kernel/smp.c
--- a/kernel/smp.c
+++ b/kernel/smp.c
-#ifdef CONFIG_CPU_HOTPLUG
+#ifdef CONFIG_HOTPLUG_CPU

remained in the kernel
for more than six months!
```

Identifiers

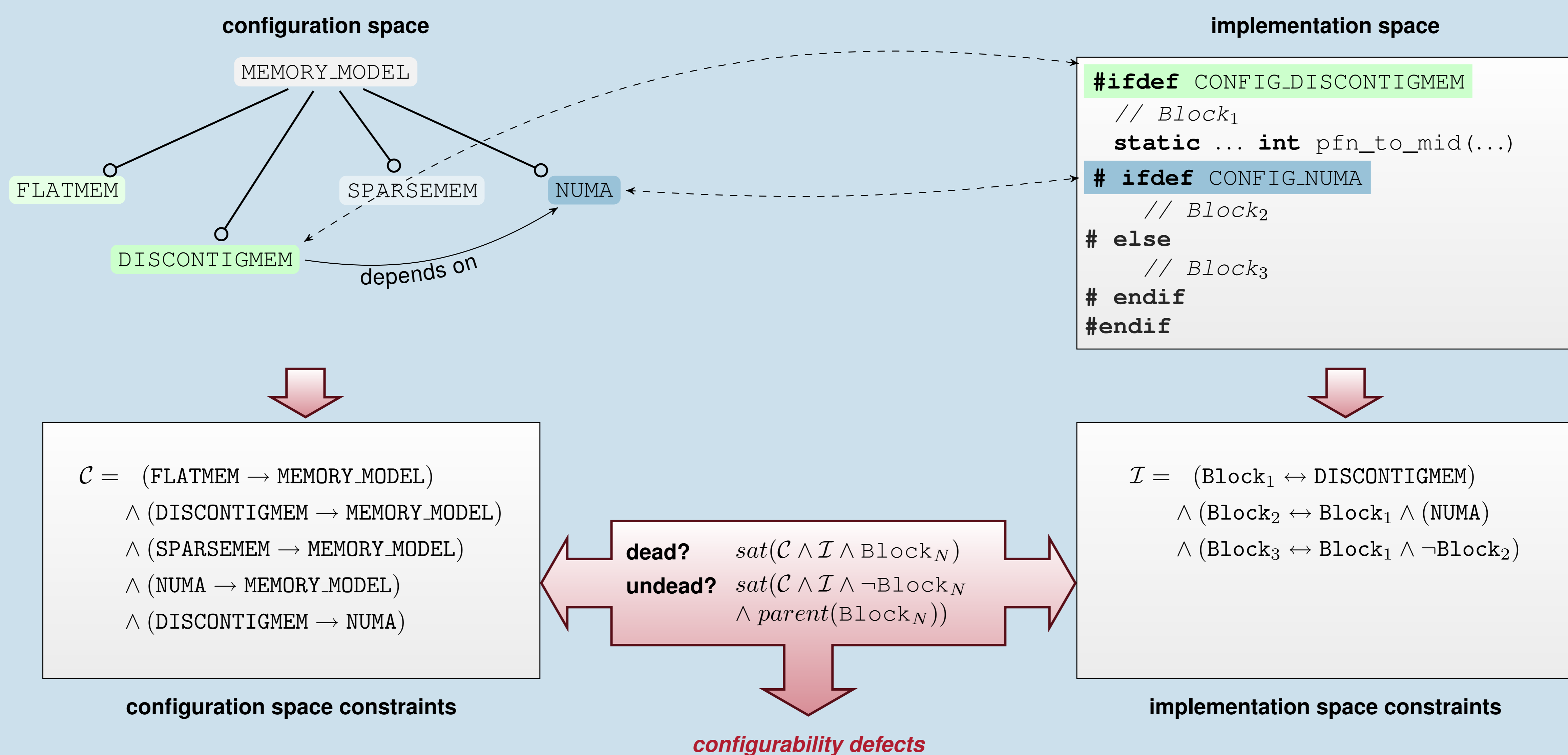
### Logic

```
diff --git a/arch/x86/include/asm/mmzone_32.h
b/arch/x86/include/asm/mmzone_32.h
--- a/arch/x86/include/asm/mmzone_32.h
+++ b/arch/x86/include/asm/mmzone_32.h
@@ -61,11 +61,7 @@ extern s8 physnode_map[];

static inline int pfn_to_nid(unsigned long pfn)
{
-#ifdef CONFIG_NUMA
return((int) physnode_map[(pfn)
/ PAGES_PER_ELEMENT]);
-#else
return 0;
-#endif
}
```

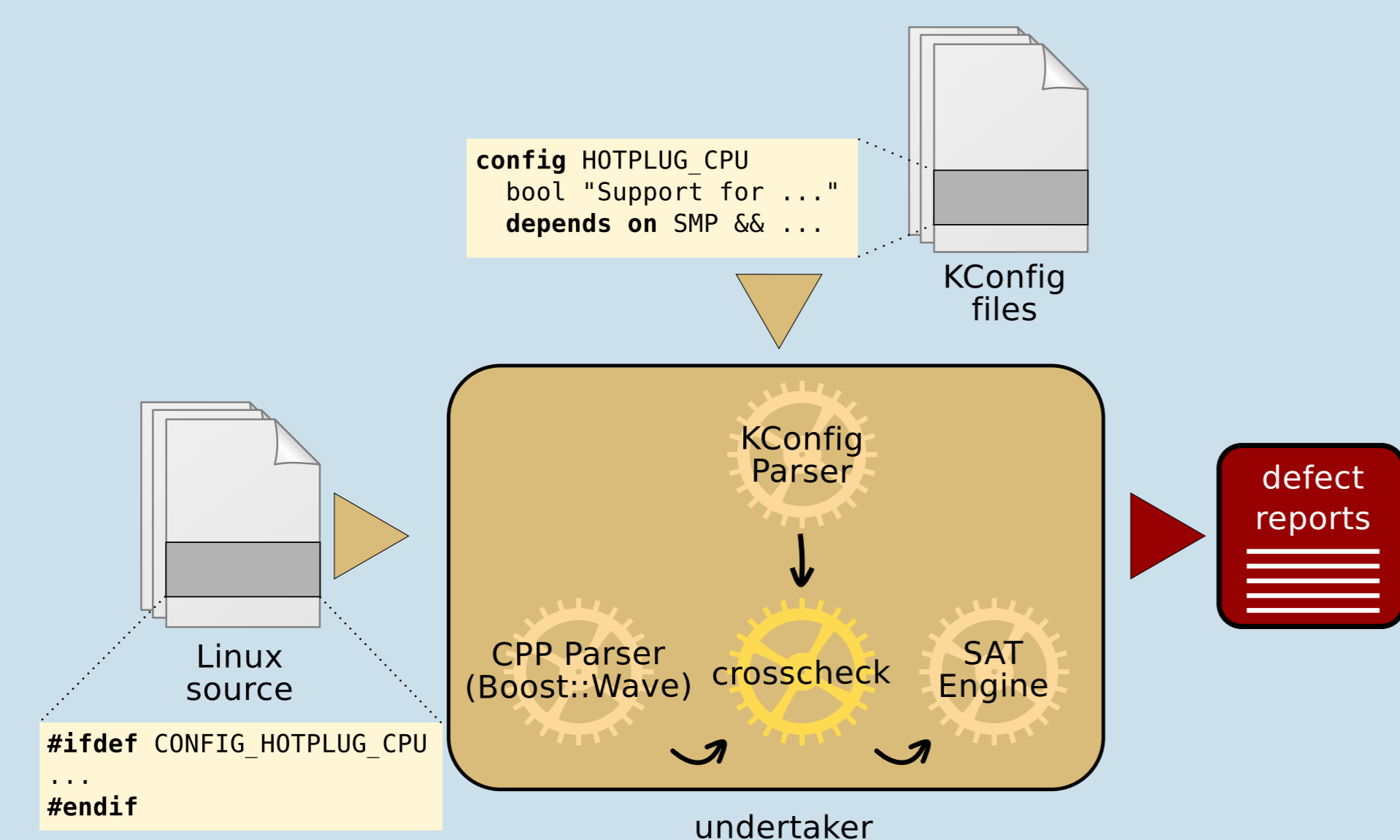
Constraints

## Our Approach



## Realization: The undertaker Tool

**Mission:** The undertaker finds dead and undead feature code (in order to bury it, eventually!)



- ▶ Finds **1776** defects in Linux 2.6.35; on this basis we have
  - ▶ proposed a fix for **364**, among them **23** bugs (**22** new)
  - ▶ removed **5129** lines of **superfluous #ifdef cruft** from the source
- ▶ So far **123** patches submitted (**15** acked, **49** merged, **36** pending)

## Results and Conclusion

subsystem	#ifdefs	logic	symbolic	$\Sigma$
arch/	33757	345	581	926
drivers/	32695	88	648	736
fs/	3000	4	13	17
include/	7241	6	11	17
kernel/	1412	7	2	9
mm/	555	0	1	1
net/	2731	1	49	50
sound/	3246	5	10	15
virt/	53	0	0	0
other subsystems	601	4	1	5
$\Sigma$	85291	460	1316	1776
fix proposed		150 (1)	214 (22)	364 (23)
confirmed defect		38 (1)	116 (20)	154 (21)
confirmed rule-violation		88 (0)	21 (2)	109 (2)
pending		24 (0)	77 (0)	101 (0)

**Conclusion:** Configurability is a **significant** (and underestimated) **source of bugs** in system software!

