hifrog - Bug #7276

crash on busybox categories; Ideally we should return UNSUPPORTED!

07/05/2018 11:52 - Sepideh Asadi

Status:	Resolved	**Start date:**	07/05/2018
Priority:	Normal	**Due date:**	
Assignee:	Martin Blicha	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

File is:
/home/asadis/hi-bench/challenge-bench/sv-comp17/c/busybox-1.22.0/touch_false-unreach-call_true-no-overflow_true-valid-memsafety.c

```
Verification was not successful, here is the last few lines: ...
```

Total number of claims in program...(1).
; Warning: disabling SATElite preprocessing to track proof
Use QF_UF logic.

```
---------checking claim # 1 ---------
```

; Warning: disabling SATElite preprocessing to track proof
hifrog: /home/asadis/new-hifrog/hifrog/trunk/cprover/src/funfrog/symex_assertion_sum.cpp:1695: ssa_exprt symex_assertion_sumt::get_next_version(const symbolt&): Assertion `state.level2.current_names.find(ssa_l1_identifier) != state.level2.current_names.end()' failed.

- INLINING function: __CPROVER_initialize
- INLINING function: main
  Processing a deferred function: __CPROVER_initialize
  Processing a deferred function: main
  Command terminated by signal 6
  real 4.12

Note: Busybox is full of pointer, heap manipulation,...as sated in the svcomp webpage this category aims to represent verification tasks from real software systems.

Note2: This crash happens in 9 benchmarks out of 40.

History

#1 - 07/05/2018 12:43 - Karine Even Mendoza

- Assignee set to Martin Blicha

- Priority changed from Low to Normal

It is a bug in the creation of the SSA symbols. Somehow a symbol in modified_globals container isn't in the cprover's tables.
It is a program variable, not a fabricated one.

#2 - 10/05/2018 09:27 - Martin Blicha

- Status changed from New to Resolved

Previously we were expecting to see a declaration of all symbols, but there are symbols that do not have declarations, like extern variables.
Now, we let the state before symex know about such variables before-hand. See git commit f8cc89bc