Analysing Hierarchical Control Software application to CERN’s detector control systems
Jeroen Keiren
MDD Days Eindhoven, April 25, 2013
Background

LHC

source: CERN
Background

LHC

source: CERN
Control software

source: CERN
Control software
Global structure
Control software
Local structure

Wheel subsystem

Wheel (2)

Sector (3)

Chamber (5)

Sector (4)

Chamber (6)

Chamber (7)

Chamber (8)
Problem
Unresponsive subsystems
Methodology

1. Understand/define semantics SML
2. Identify desirable properties
3. Verify properties
4. Automate verification
5. Develop dedicated tooling
6. Integrate tooling into IDE
Example (SML)

class: $FWPART$_$TOP$RPC_Chamber_CLASS
  state: OFF
    when (($ANY$FwCHILDREN in_state ERROR) or
         ($ANY$FwCHILDREN in_state TRIPPED))
      move_to ERROR
...

action: STANDBY
  do STANDBY $ALL$RPC_HV
  do ON $ALL$RPC_LV
Processing in a state machine

When phase

- receive state-update
- all guards false
- evaluating when clauses
- command queue empty

Action phase

- waiting for command or state-update
- received command
- executing statements
- executed last statement
- emptying command queue
Stabilisation
Liveloocks

state: ANALOG_ON_RED
...
when ( $ANY$TkPowerGroup not_in_state DIGITAL_ON_RED )
move_to LVMIXED
...
state: LVMIXED
...
when ( $ANY$TkPowerGroup in_state {ON, HVMIXED} )
move_to HVMIXED
when ( $ALL$FwCaenChannelCtrl in_state ON and
      $ALL$TkPowerGroup in_state ANALOG_ON_RED )
move_to ANALOG_ON_RED
...

Stabilisation

TkControlGroup

TkPowerGroup
(ANALOG_ON_RED)

FwCaenChannelCtrl
(ON)
state: ANALOG_ON_RED
...
when ( $ANY$TkPowerGroup not_in_state DIGITAL_ON_RED )
move_to LVMIXED
...
state: LVMIXED

...  
when ( $ALL$FwCaenChannelCtrl in_state ON and  
  $ALL$TkPowerGroup in_state ANALOG_ON_RED )  
move_to ANALOG_ON_RED  
...
state: ANALOG_ON_RED
...
when ( $ANY$TkPowerGroup not_in_state DIGITAL_ON_RED )
    move_to LVMIXED
...
state: LVMIXED
...
when ( $ALL$FwCaenChannelCtrl in_state ON and
    $ALL$TkPowerGroup in_state ANALOG_ON_RED )
move_to ANALOG_ON_RED
...

Unreachable states

- Error
- Standby
- On
- Busy
- Off

Diagram shows transitions between states.
Results
Livelocks

- Full system checking in 79 seconds
- 1302 FSMs have looping potential
- Most not observed/short lived
- Outages of control system traced back to detected problems:

  ...  
  ...  
  ...
Results
Reachability

- Full system checked in 18 minutes
- 903 FSMs have reachability issues
- Partly due to clever programmer tricks
- Real problems typically due to copy/paste
Implementation

- Full automated translation to mCRL2
- Dedicated translations to SMT for described problems
- Integration of dedicated tools in IDE
Conclusions

- CERN: eager to improve software
- Generic solutions
- Huge system, yet effective verification
- Real-life problems detected
- Diagnostics ensure quick fixing

“We should have had these tools at the start of the LHC project” — CMS engineer
Future work

- Scale model checking techniques
- Verify larger subsystems
- Continue developing dedicated tooling
- Integrate additional tooling in IDE
- Verify standard SCADA systems
Thank you

source: http://xkcd.com/401