QuickCheck your simulations!

John Hughes
Quviq AB

What is QuickCheck?

- We write *properties:*

```
prop_reverse() ->
  ?FORALL(L,list(int()),
          reverse(reverse(L))==L).
```

- We test them with *random data:*

```
4> eqc:quickcheck(reverse:prop_reverse()).
.....................................
.....................................
..............
OK, passed 100 tests
```

What is QuickCheck?

- Sometimes they are *false:*

```
prop_wrong() ->
  ?FORALL(L,list(int()),
          reverse(L)==L).
```

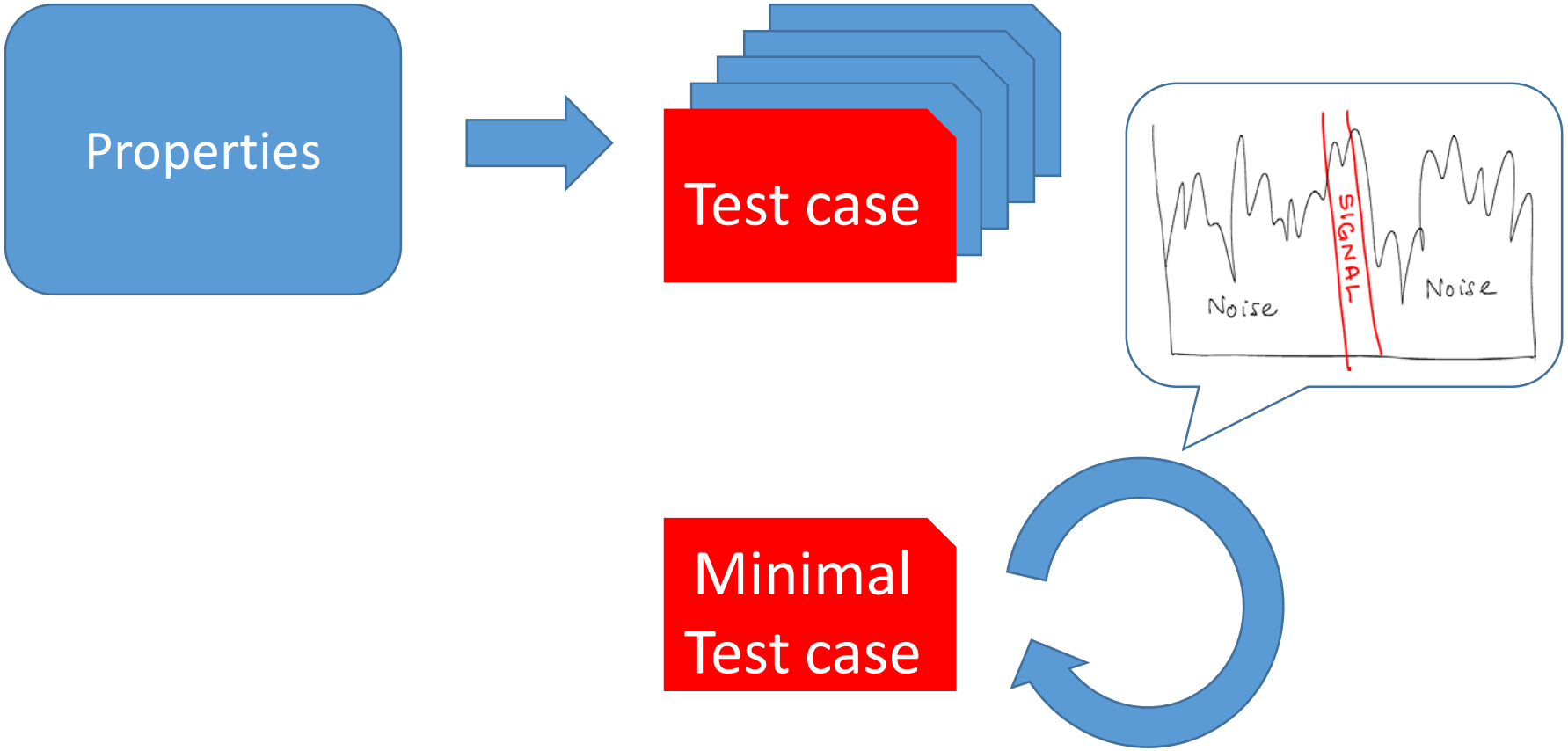
- QuickCheck reports a *minimal counterexample:*

```
5> eqc:quickche                    ong()).
.............Fai                 16 tests.
[4,5,3,7]
Shrinking xxx.x..xx(3 times)
[0,1]
```

Randomly generated

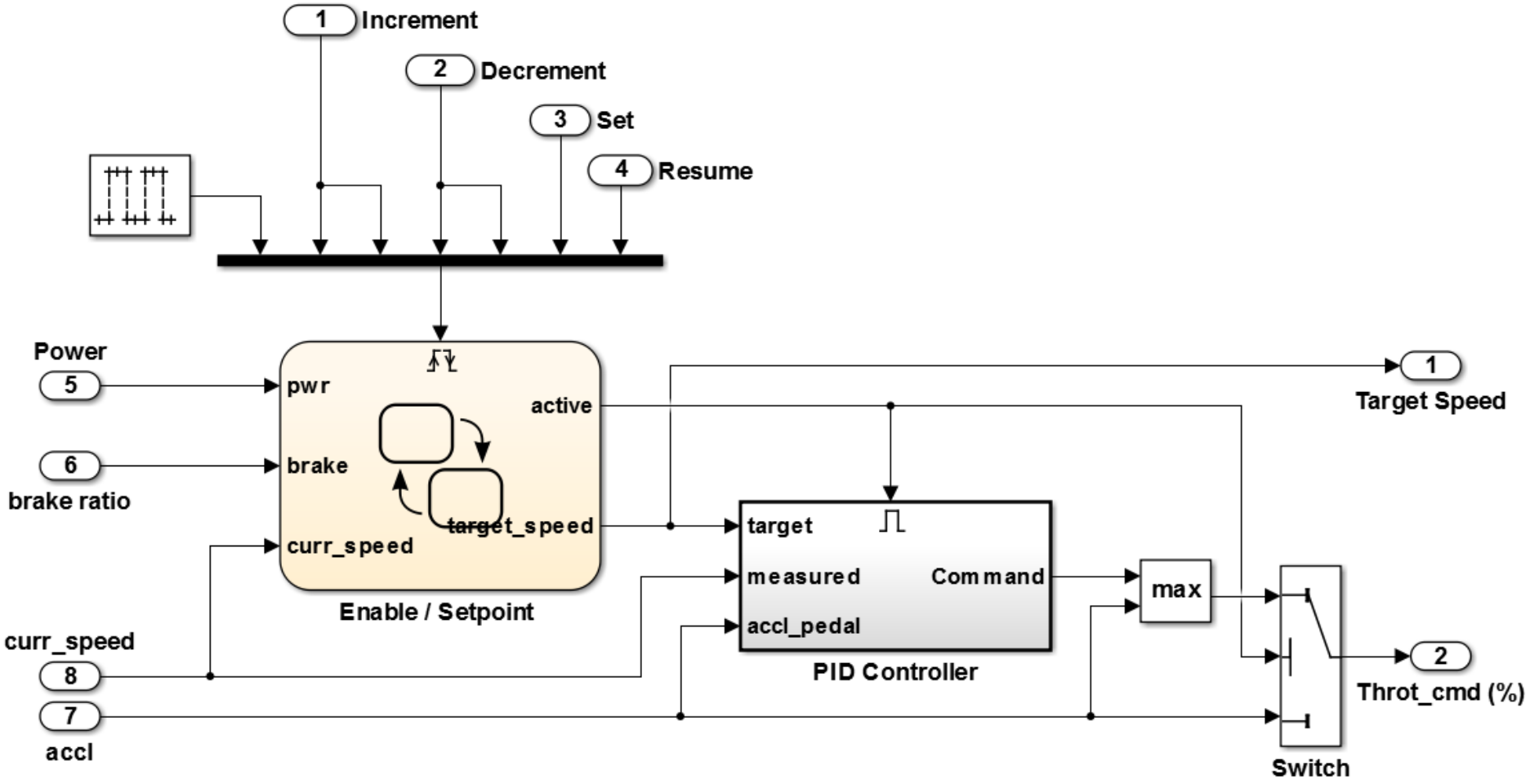
Minimal

QuickCheck in a Nutshell

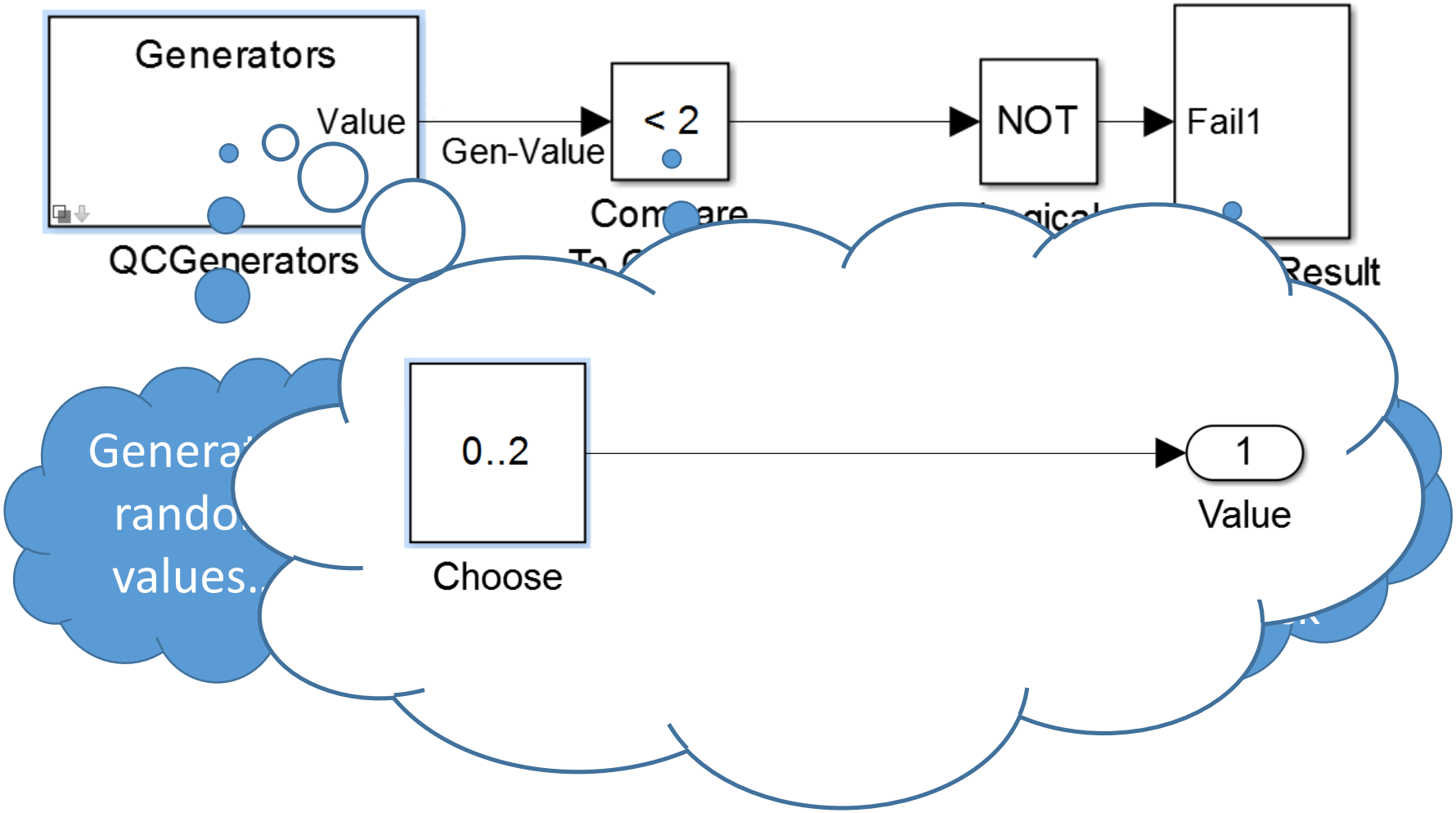



CRUISE
RES
ACCEL
DECEL
SET
CANCEL

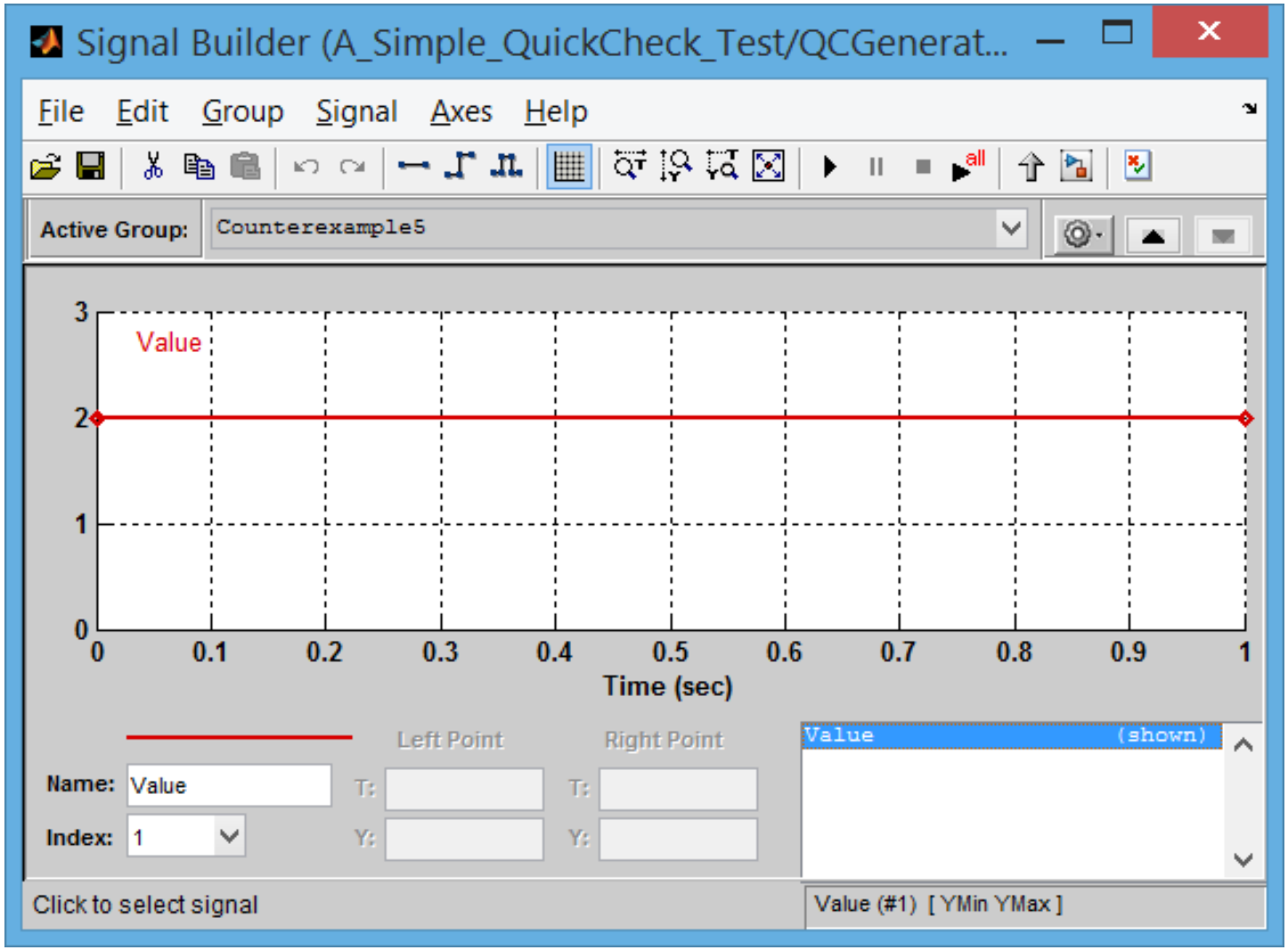
A cruise controller in SIMULINK



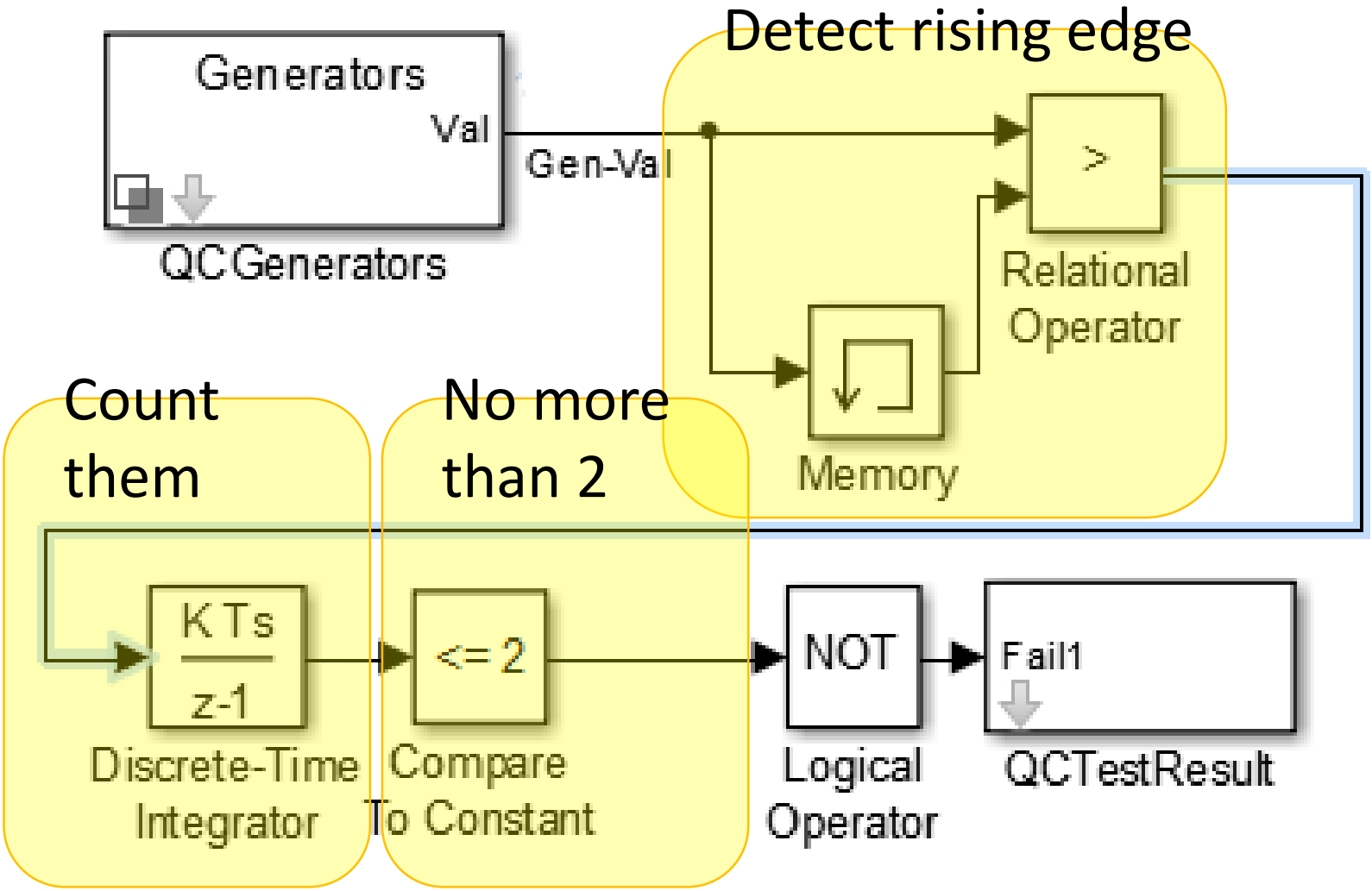
A Simple QuickCheck Test

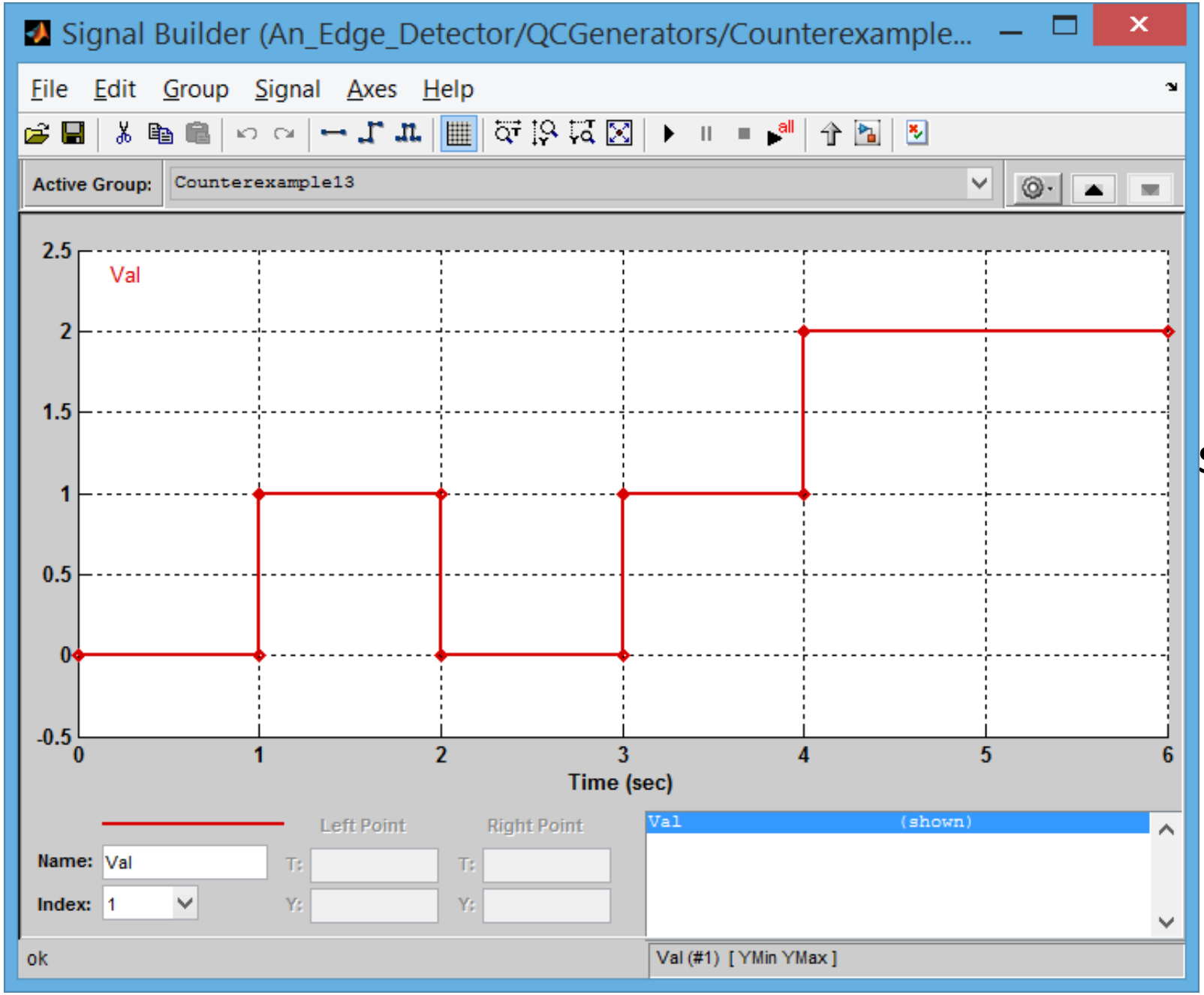


Running the test…



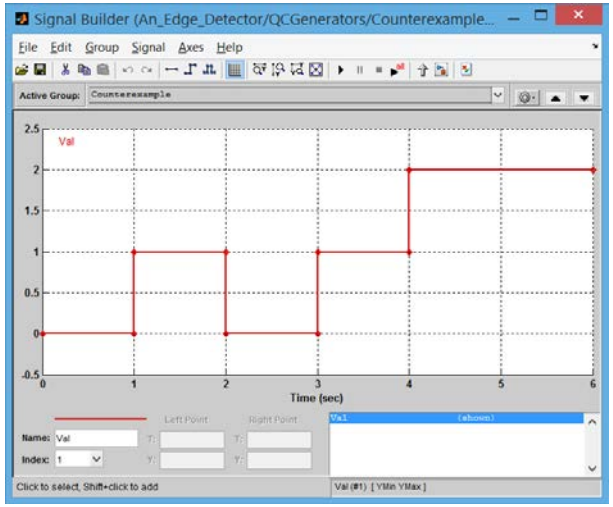
A Simple Edge Detector

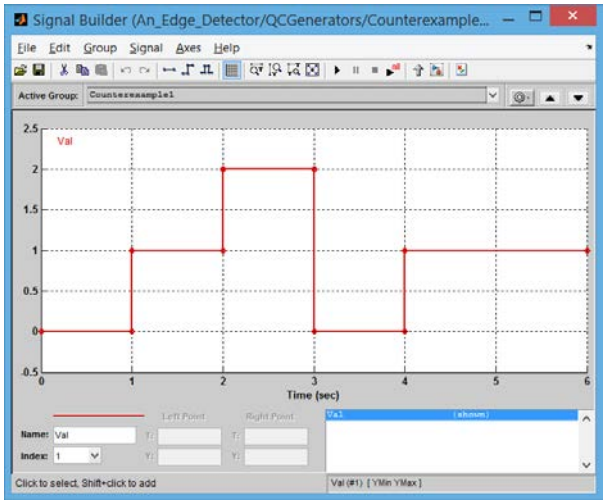


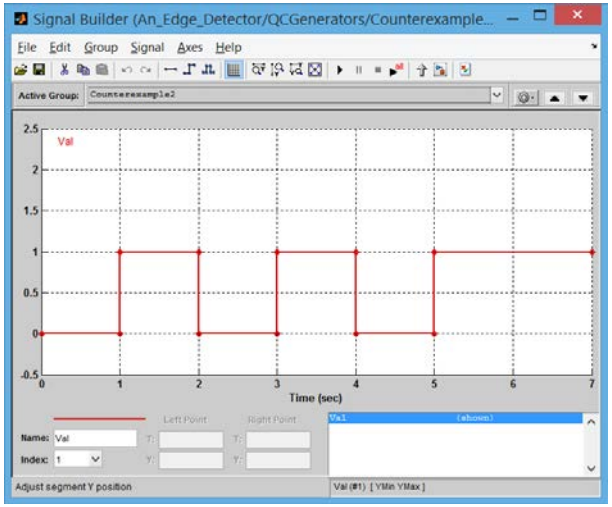

Signal Builder (An_Edge_Detector/QCGenerators/Counterexample...
File Edit Group Signal Axes Help
Active Group: Counterexample13
Val
2.5
2
1.5
1
0.5
0
-0.5
0 1 2 3 4 5 6
Time (sec)
Left Point
Right Point
Name: Val
Index: 1
T:
Y:
Val (shown)
ok
Val (#1) [YMin YMax]

s)

Three minimal counterexamples







Generation and shrinking

- Internally, QuickCheck generated:

[{5,0},{8,1},{10,2},{12,0},{19,2},}]]

- …which shrunk to:

[{1,0},{2,1},{3,2},{4,0},{5,1}]]

Time

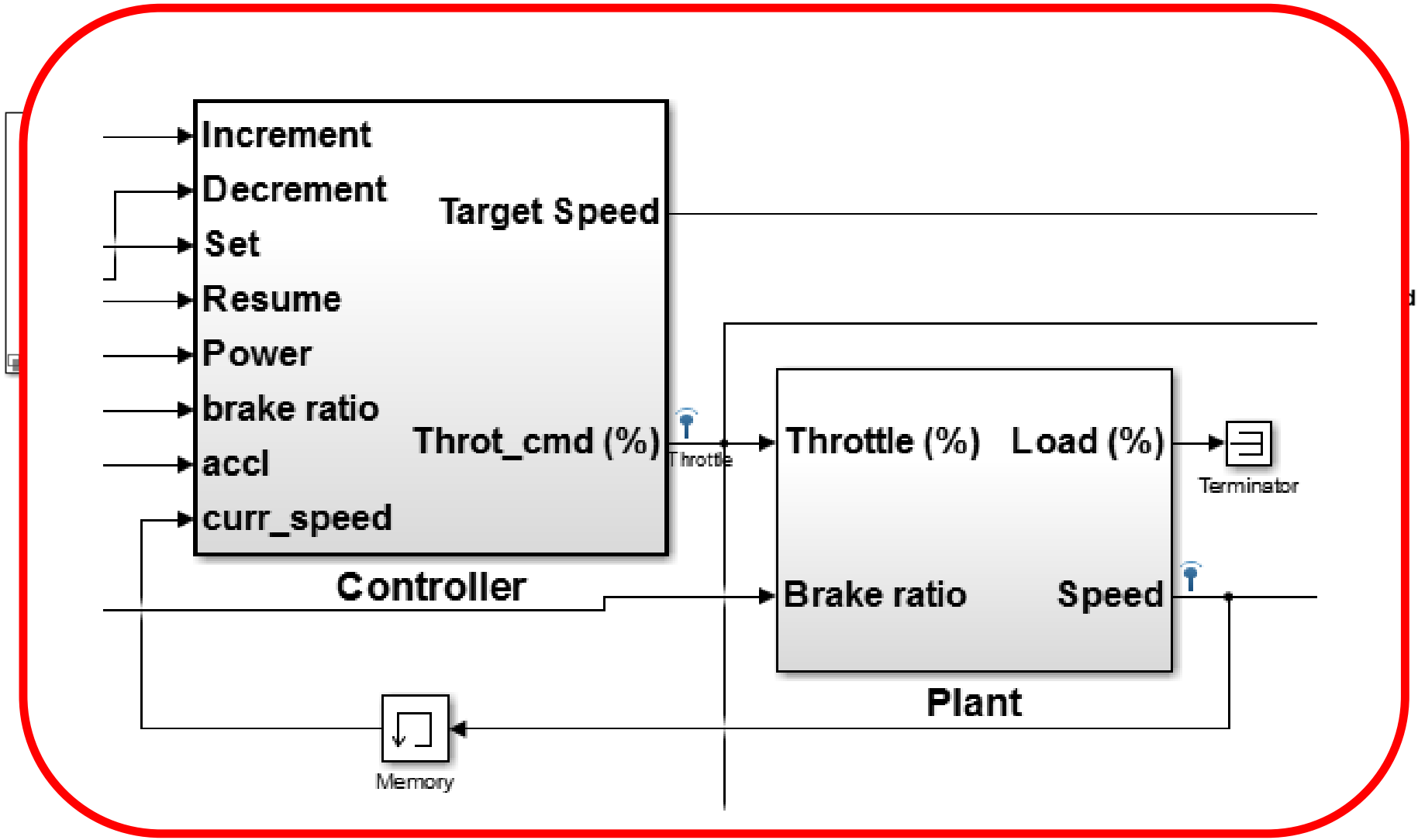
Value

Discard pairs

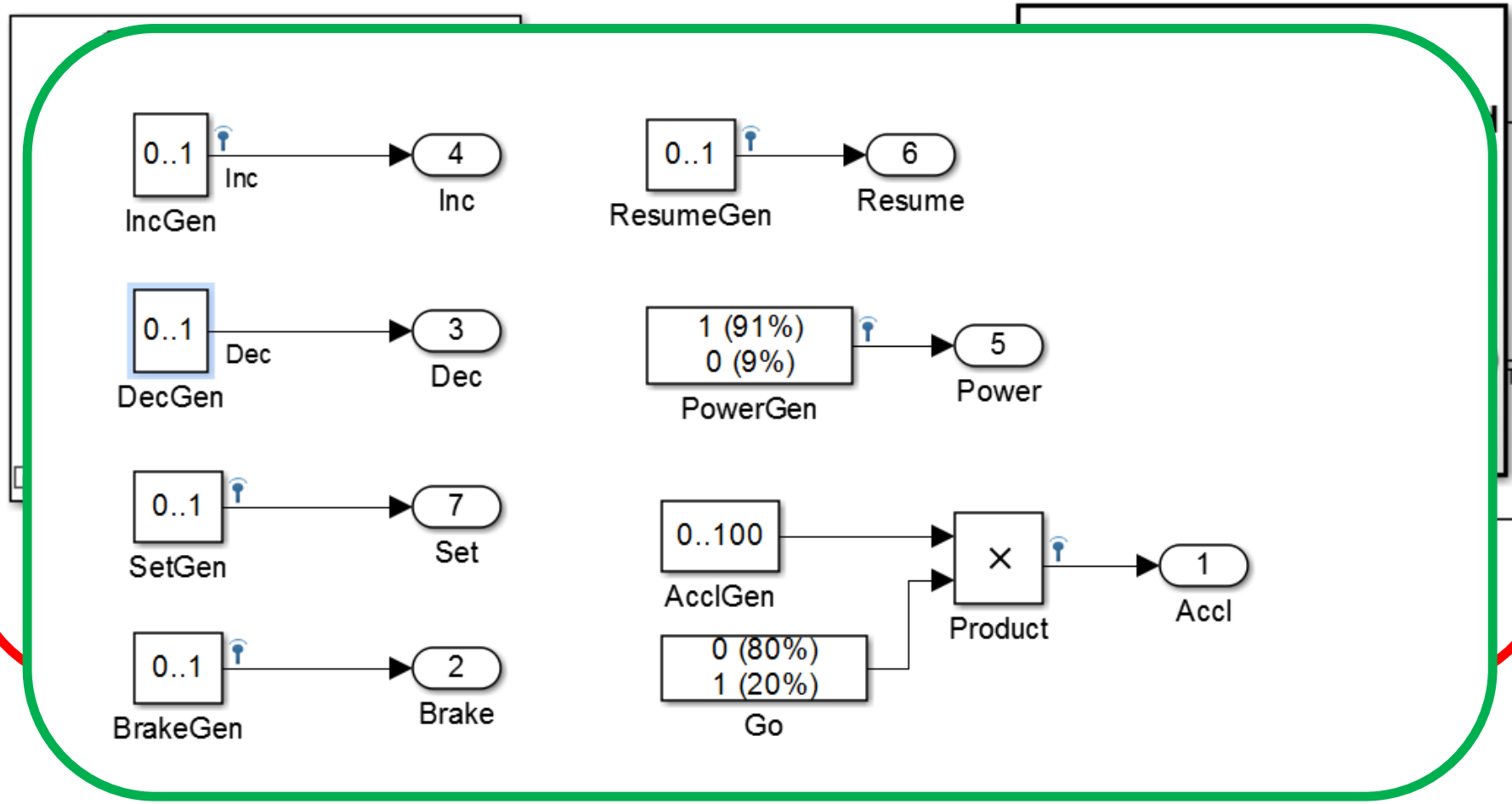
Shrink times

Shrink values

Testing the cruise controller



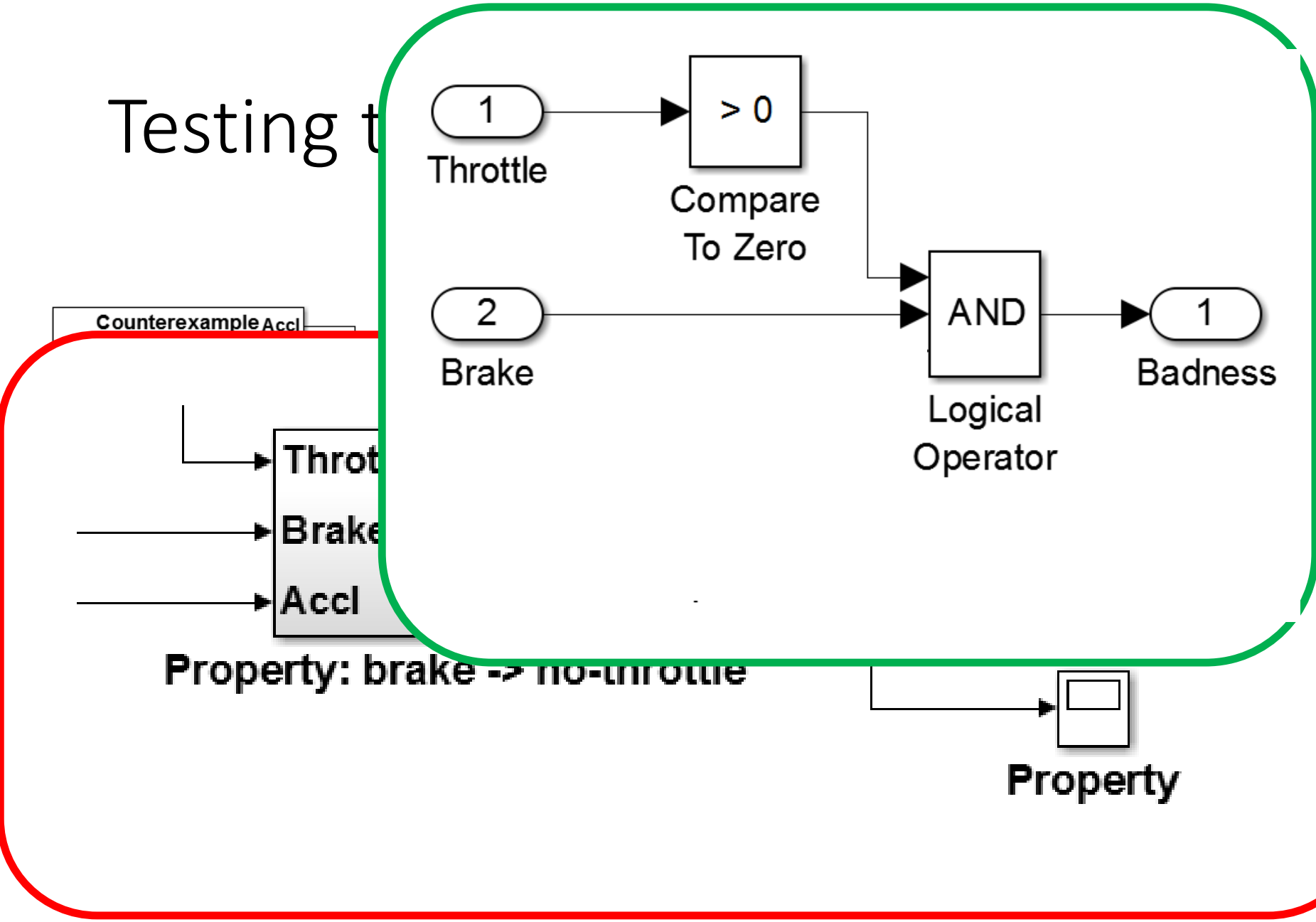
Testing the cruise controller



But what should the property be?

- The controller does nothing when the power is off?
- The actual speed approaches the target speed?
- The controller does not accelerate while the driver is braking?

Testing t


1
Throttle
> 0
Compare
To Zero
2
Brake
AND
1
Badness
Logical
Operator
Counterexample Accl
Throt
Brake
Accl
Property: brake -> no-throttle
Property

Ru

>> q

Con

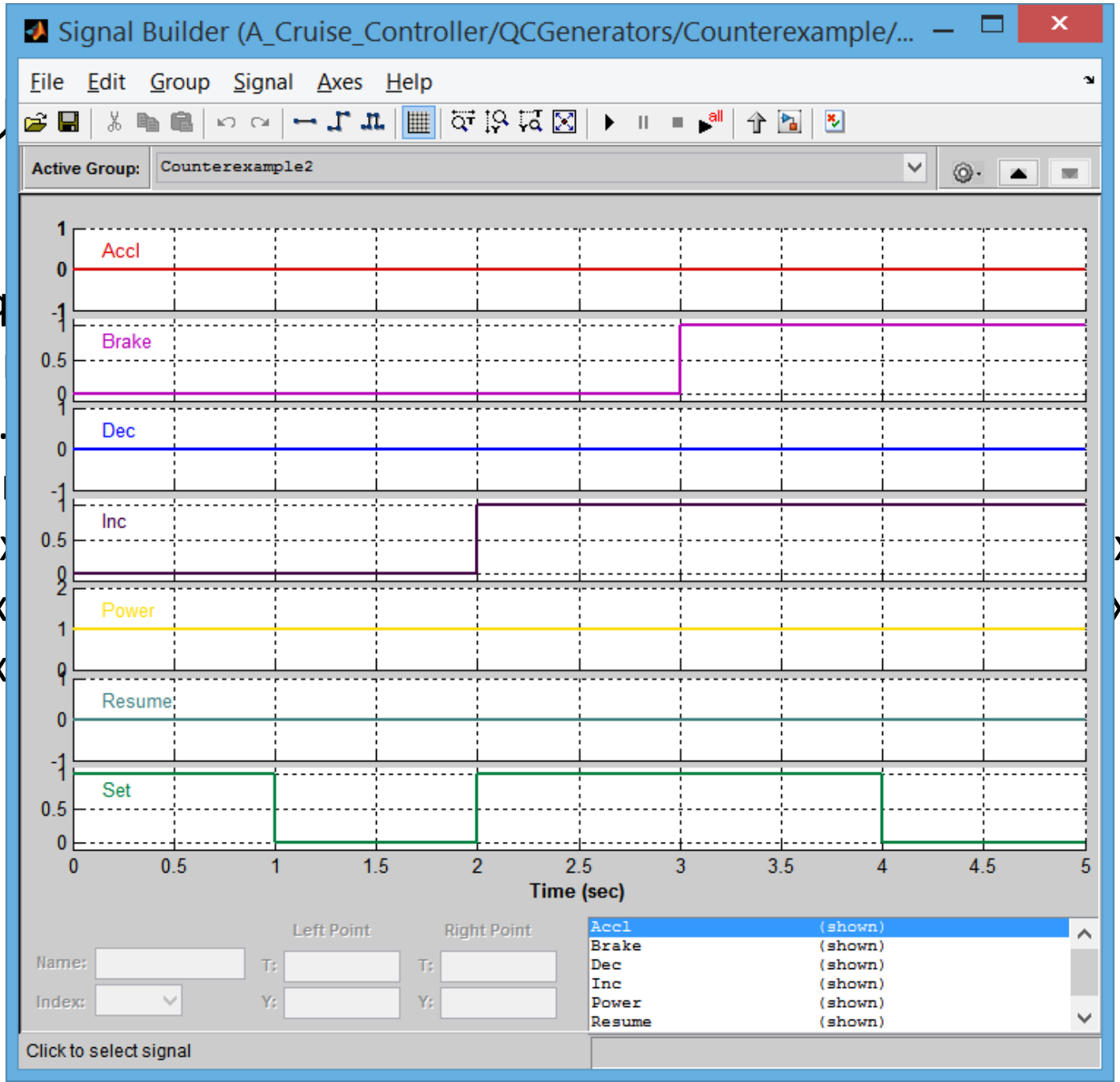
.....

Shri

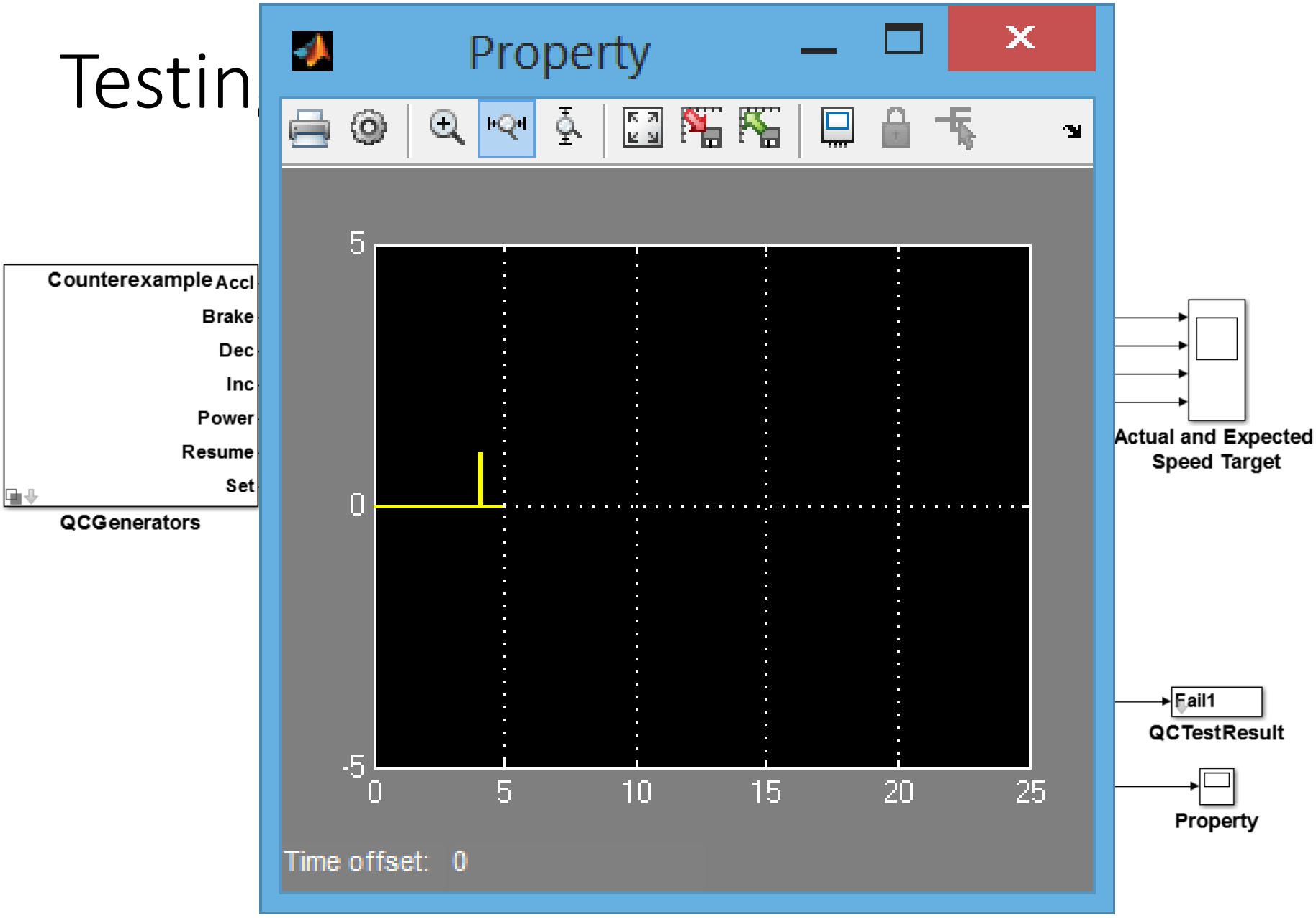
xxx.x xxxxxx

xxxx xxxxxx

xxxx



Testin

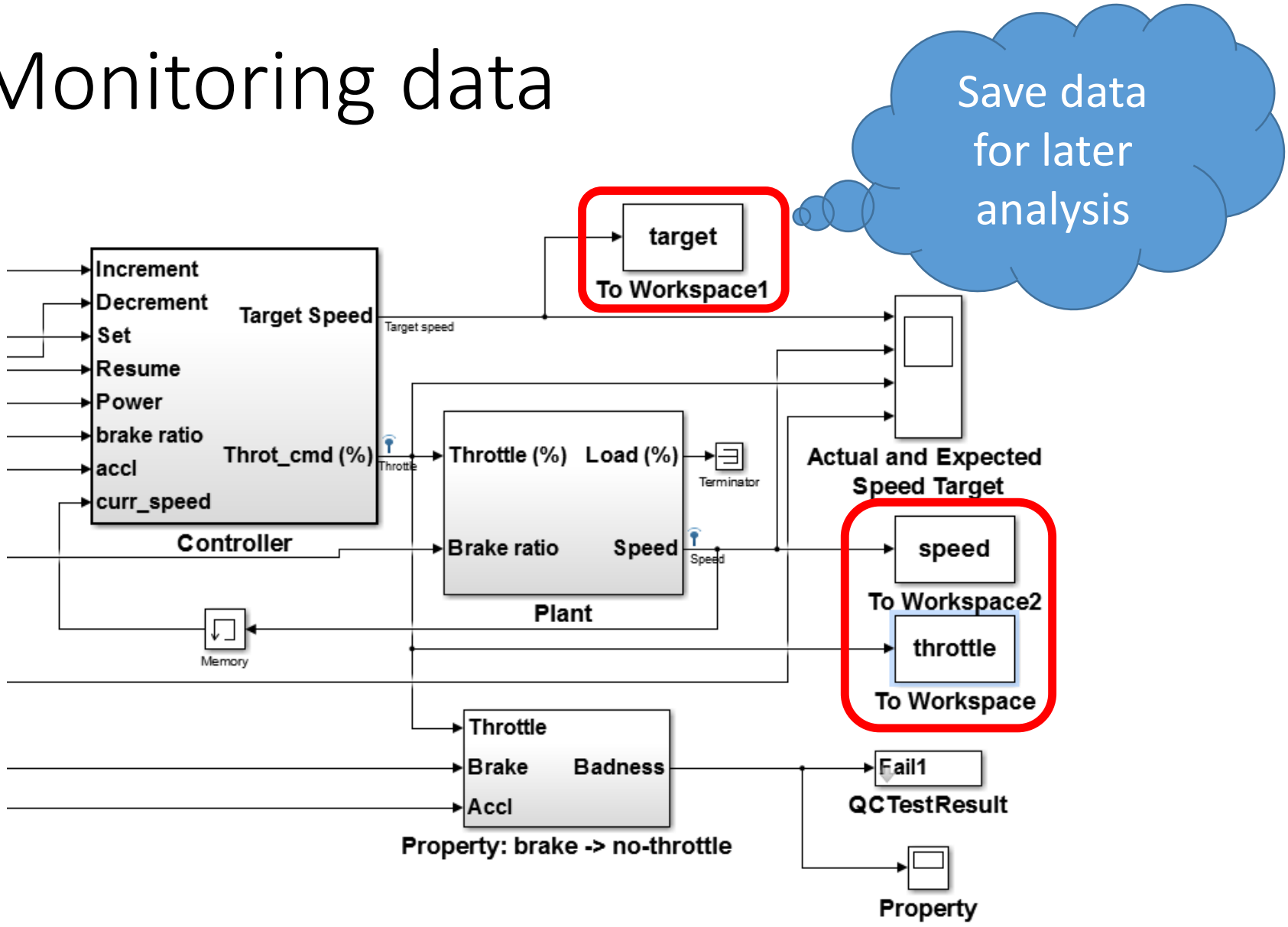

Property
Counterexample
Accl
Brake
Dec
Inc
Power
Resume
Set
QCGenerators
5
0
-5
0
5
10
15
20
25
Time offset: 0
Actual and Expected Speed Target
Fail1
QCTestResult
Property


Figures - Actual and Expected Speed Target
Actual and Expected Speed Target
Target speed
Speed
Throttle
Throttle
Braking
1.5
1
0.5
0
50
0
1
0.5
0
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
5
Time offset: 0

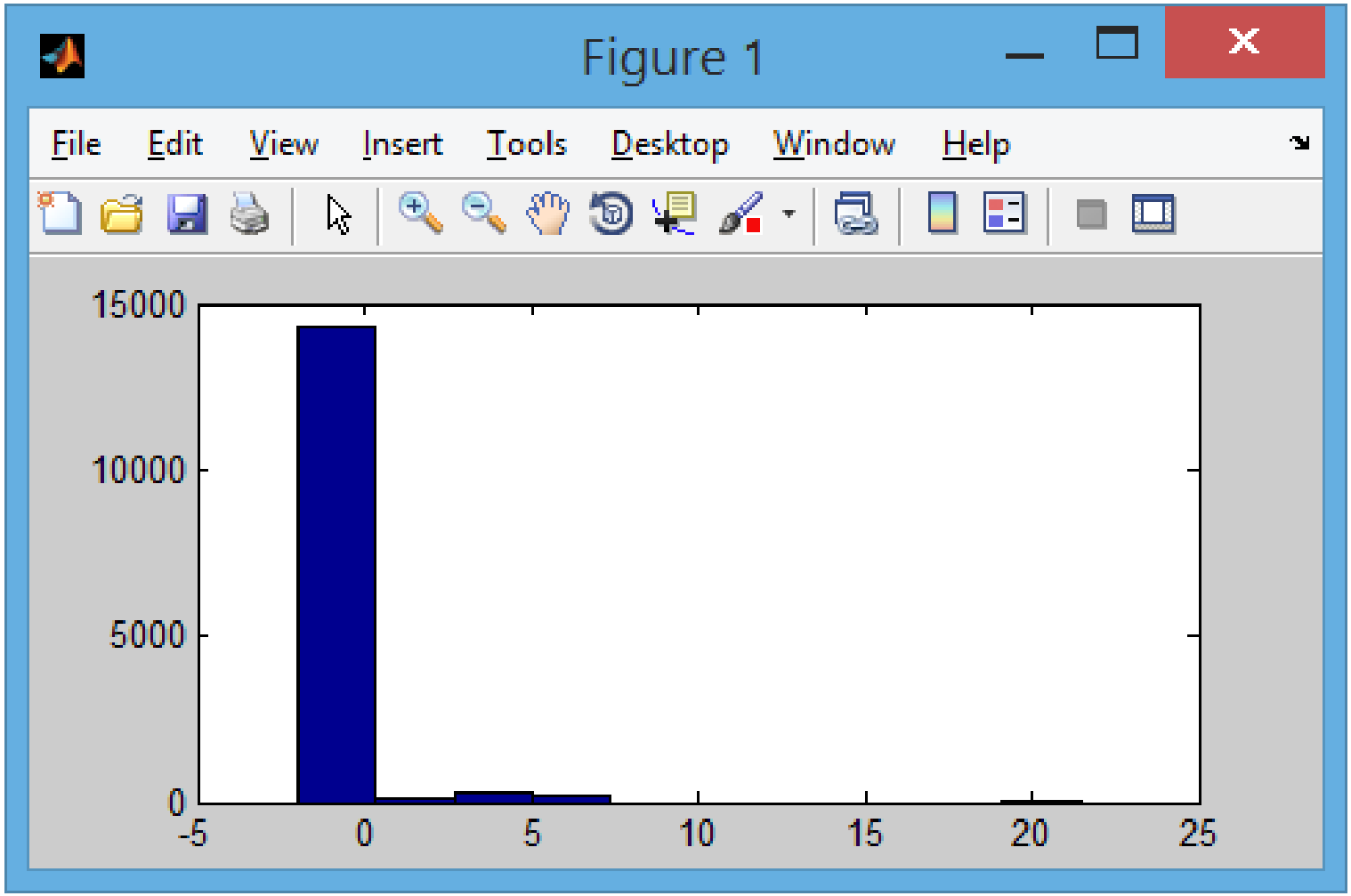
What does this show?

- Unintended acceleration is possible.
- Is it serious?

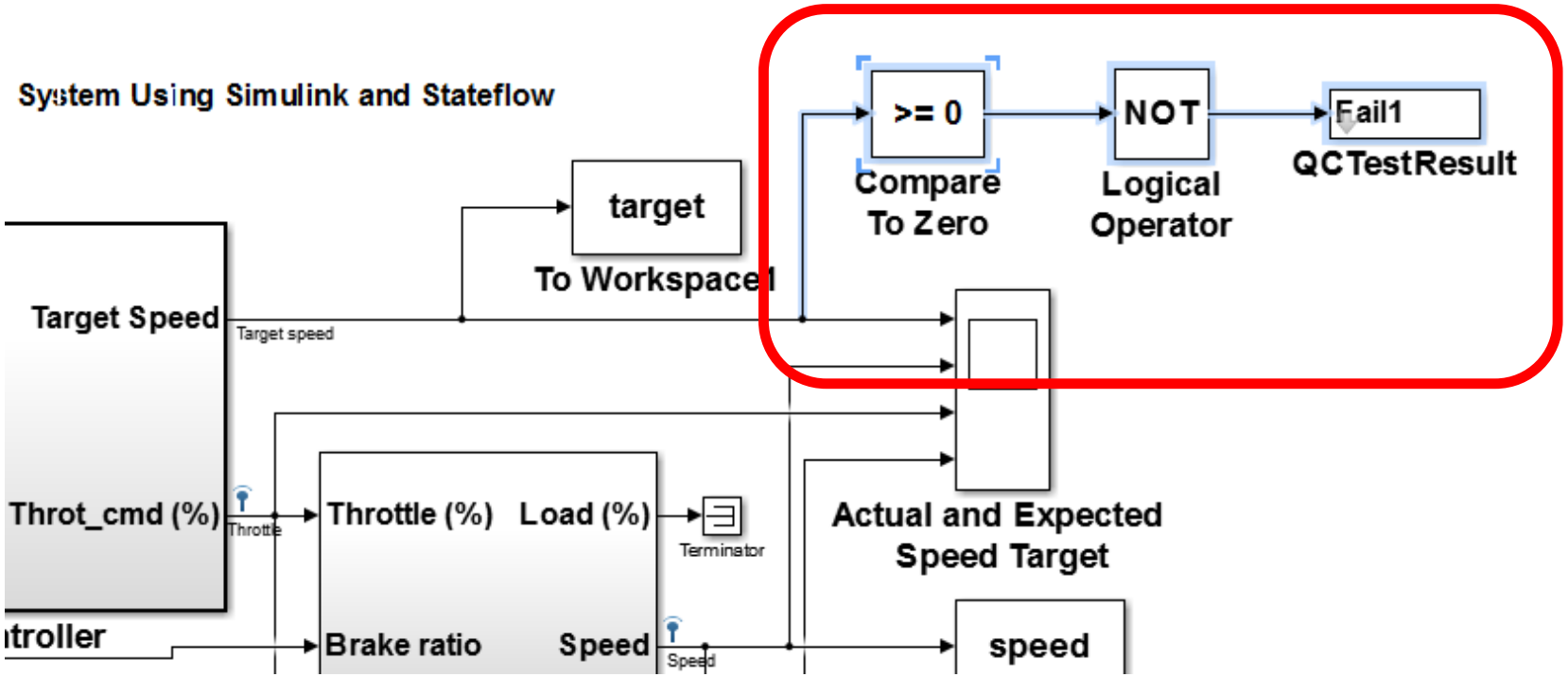
Monitoring data

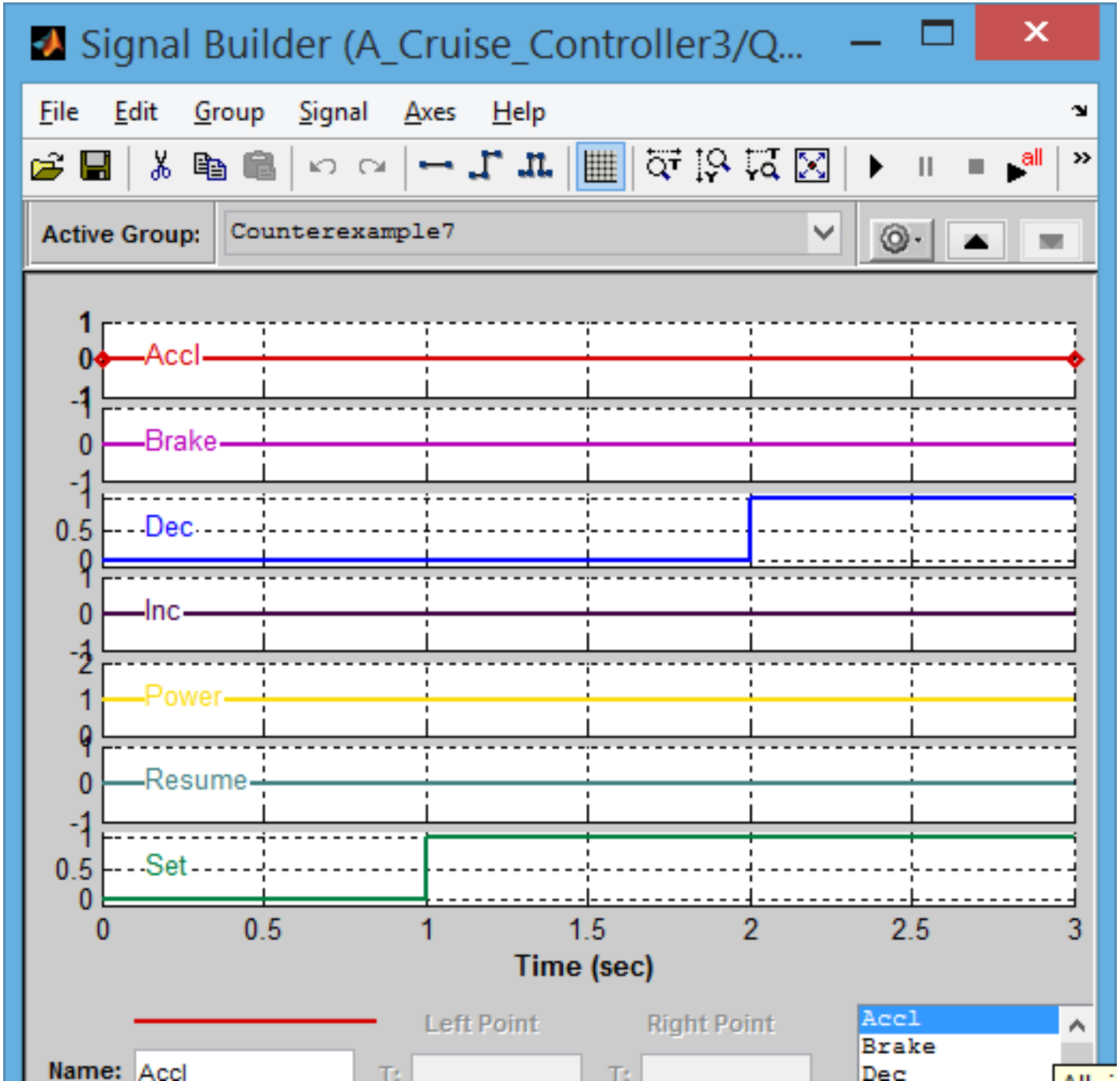


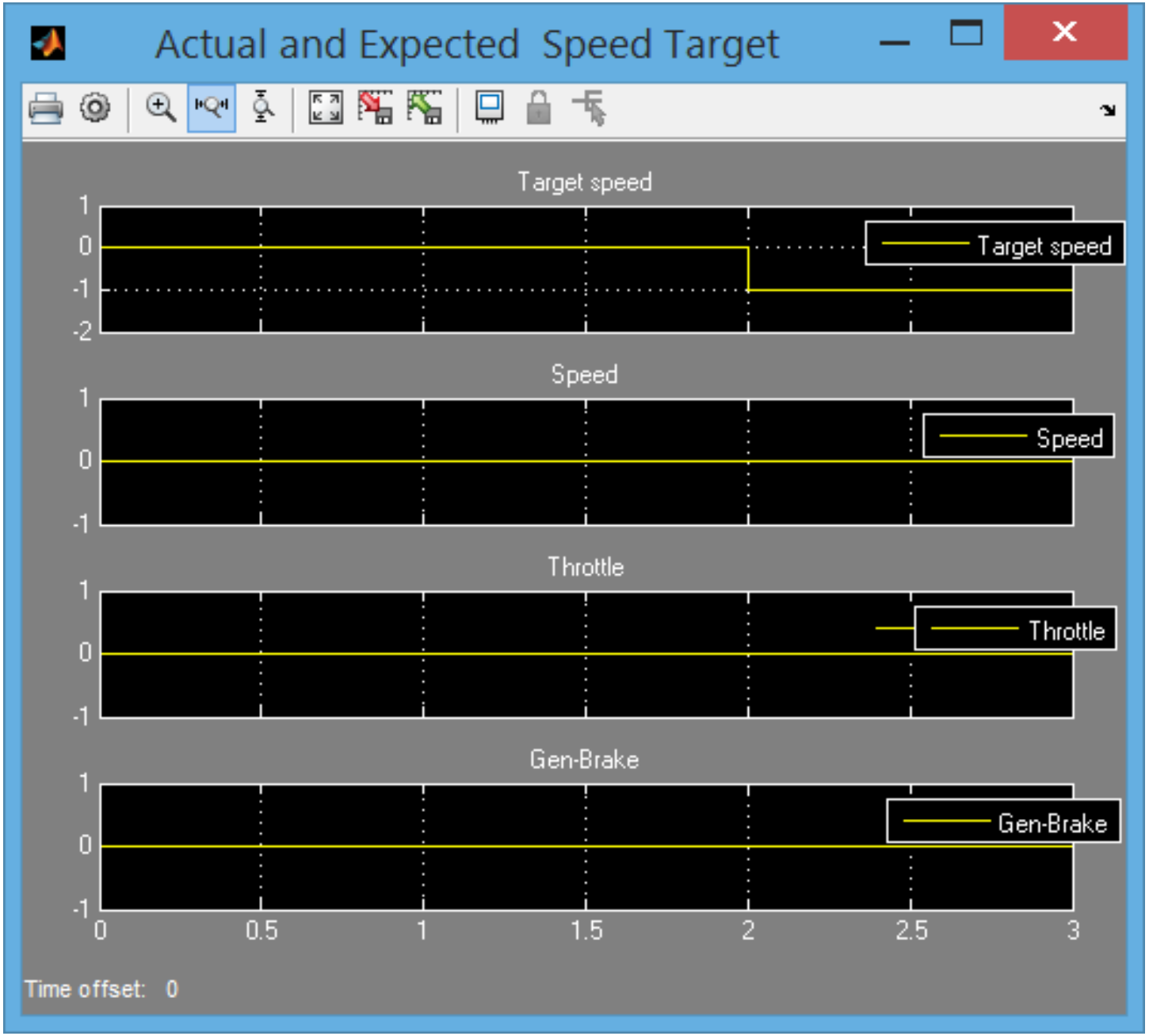
>> histogram('target')



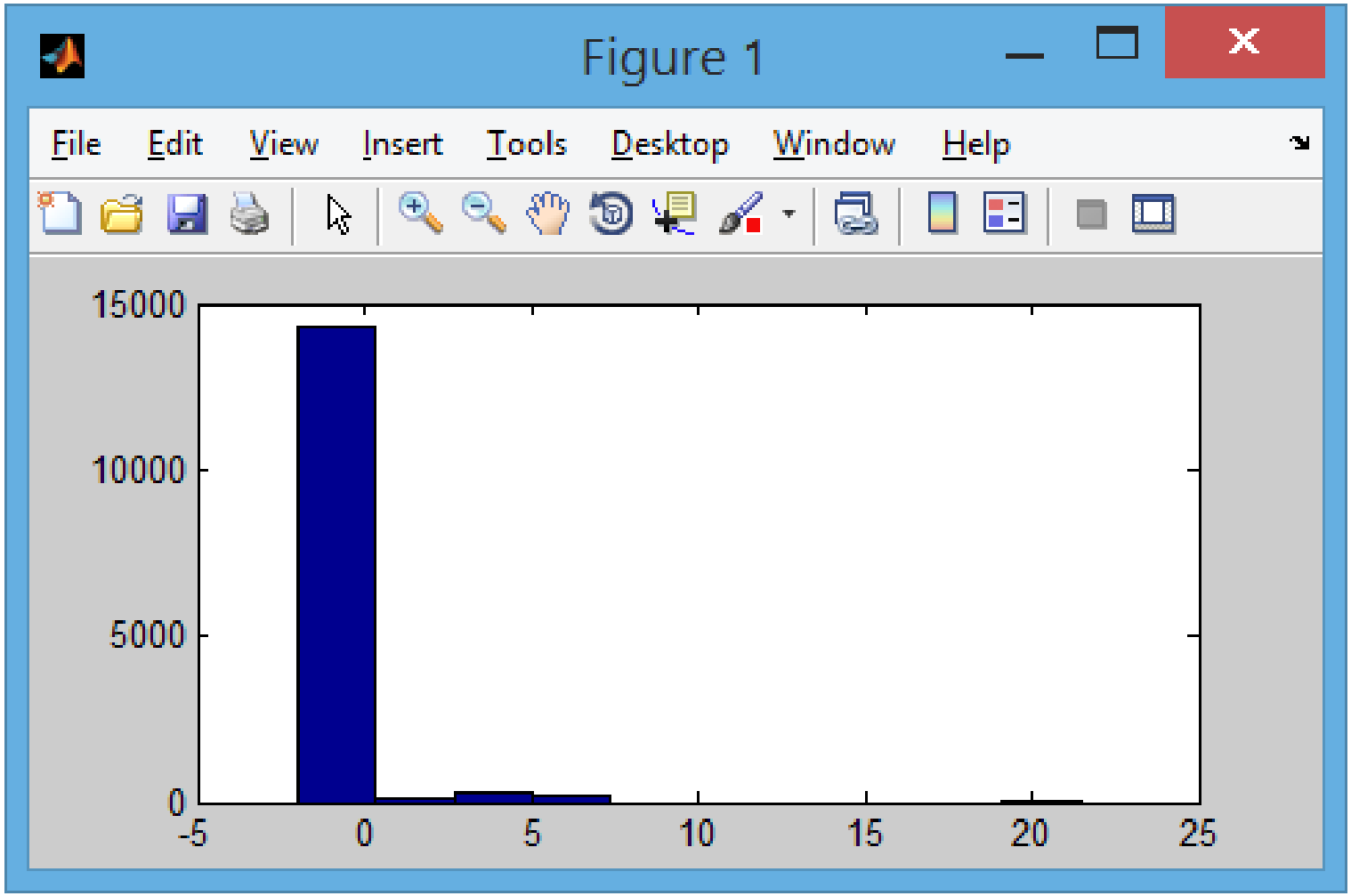
How can that happen?



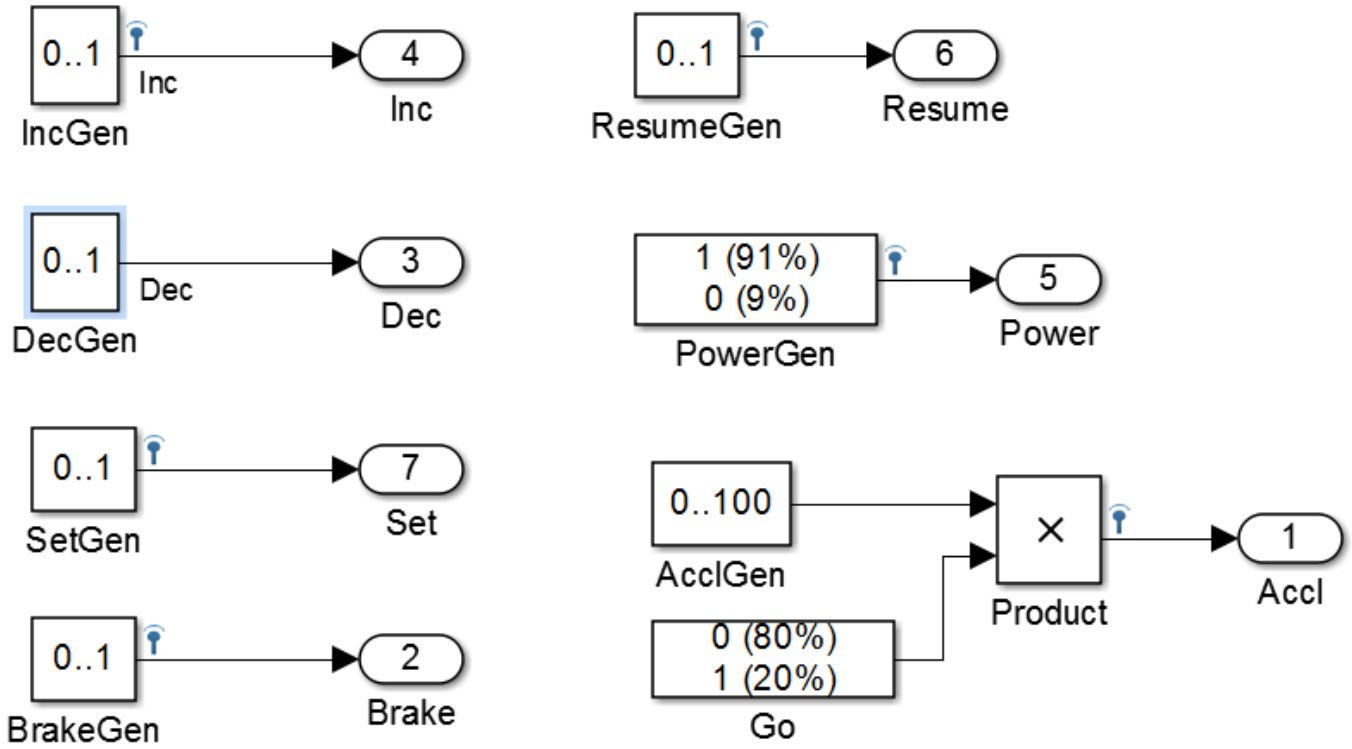

Signal Builder (A_Cruise_Controller3/Q...
File
Edit
Group
Signal
Axes
Help
Active Group:
Counterexample7
Accl
Brake
Dec
Inc
Power
Resume
Set
1
0
-1
0.5
2
0
0.5
1
1.5
2
2.5
3
Time (sec)
Left Point
Right Point
Name:
Accl
Brake
Dec


Actual and Expected Speed Target
Target speed
Target speed
1
0
-1
-2
Speed
Speed
1
0
-1
Throttle
Throttle
1
0
-1
Gen-Brake
Gen-Brake
1
0
-1
0
0.5
1
1.5
2
2.5
3
Time offset: 0

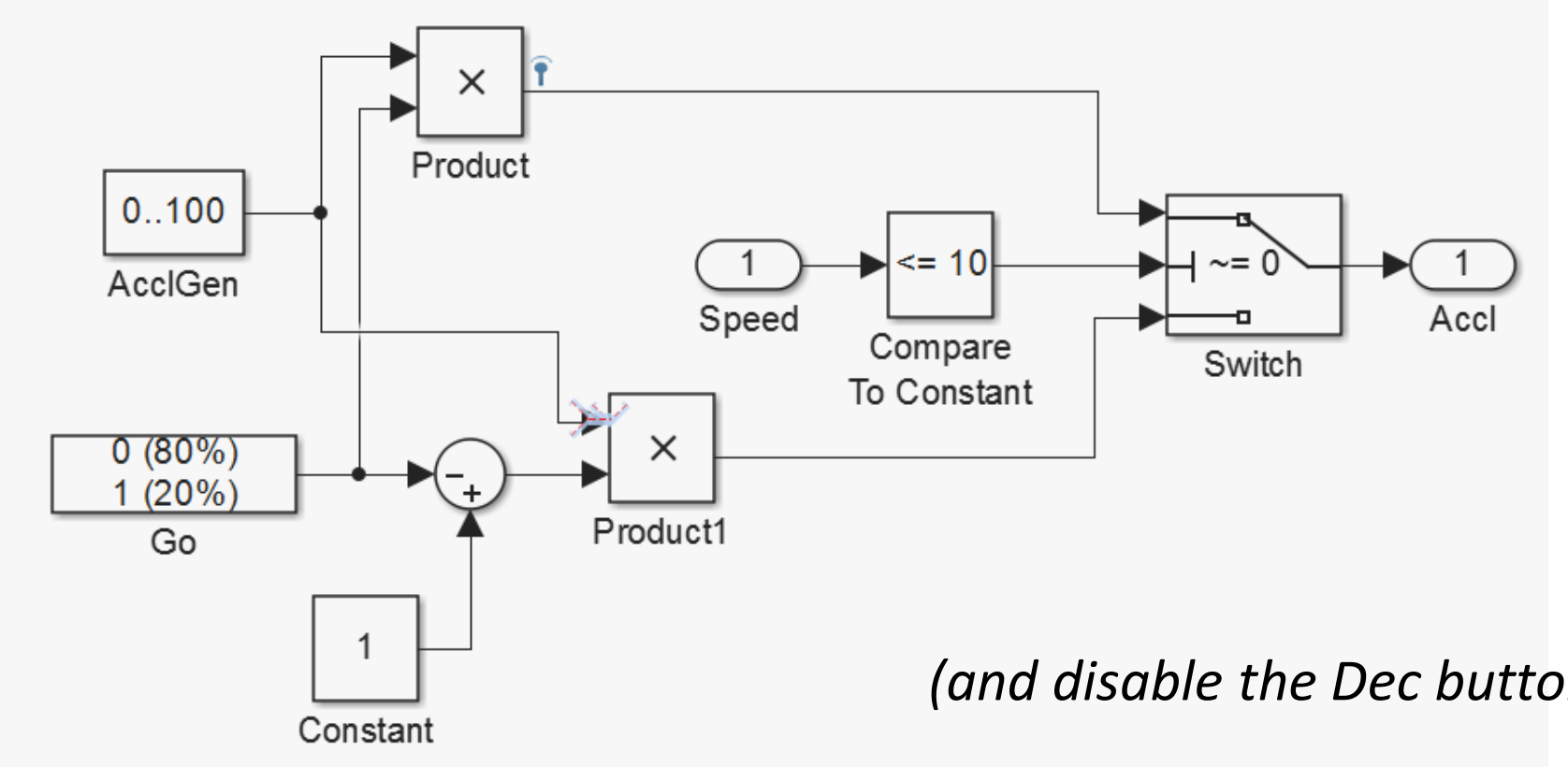
>> histogram('target')



Recall the generators…



Accelerate more often *at low speed*…



(and disable the Dec button)

Better (a bit)

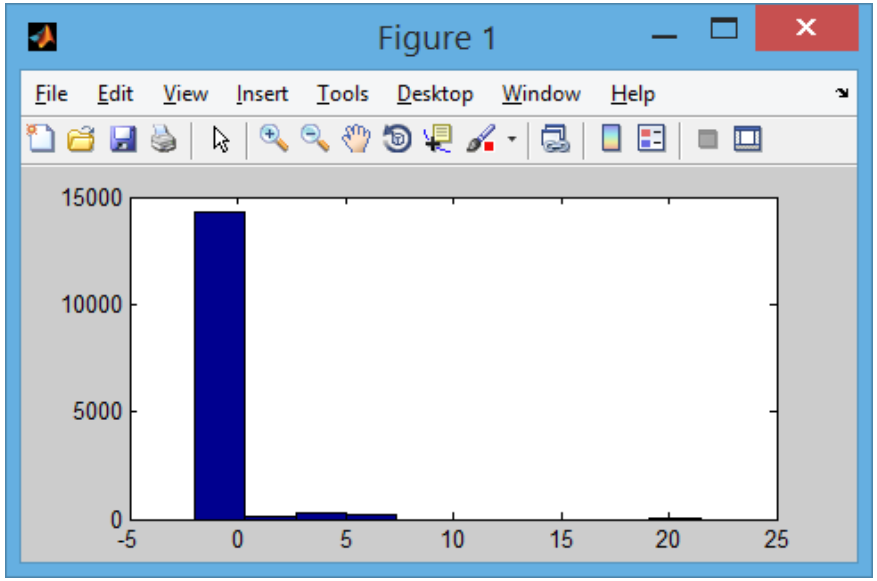


Figure 1
File Edit View Insert Tools Desktop Window Help
15000
10000
5000
0
-5 0 5 10 15 20 25

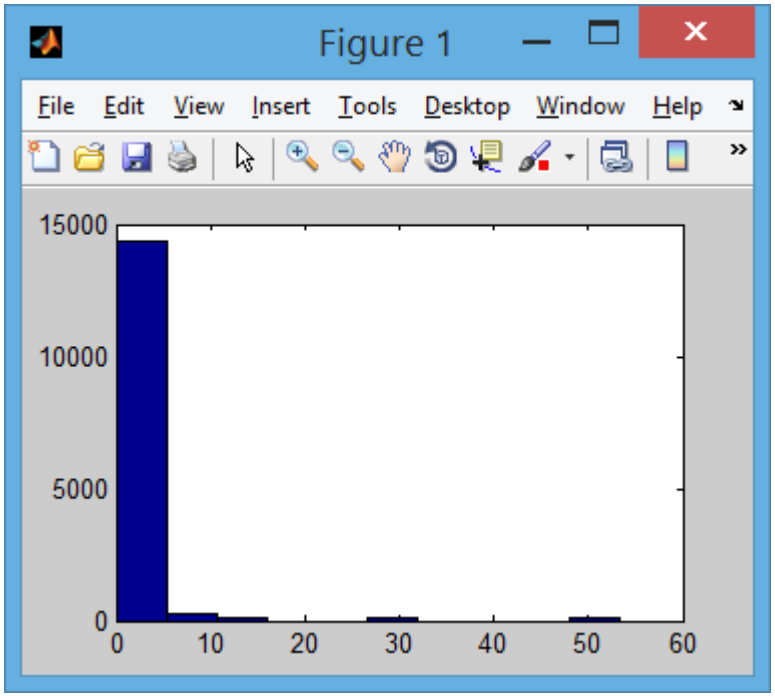
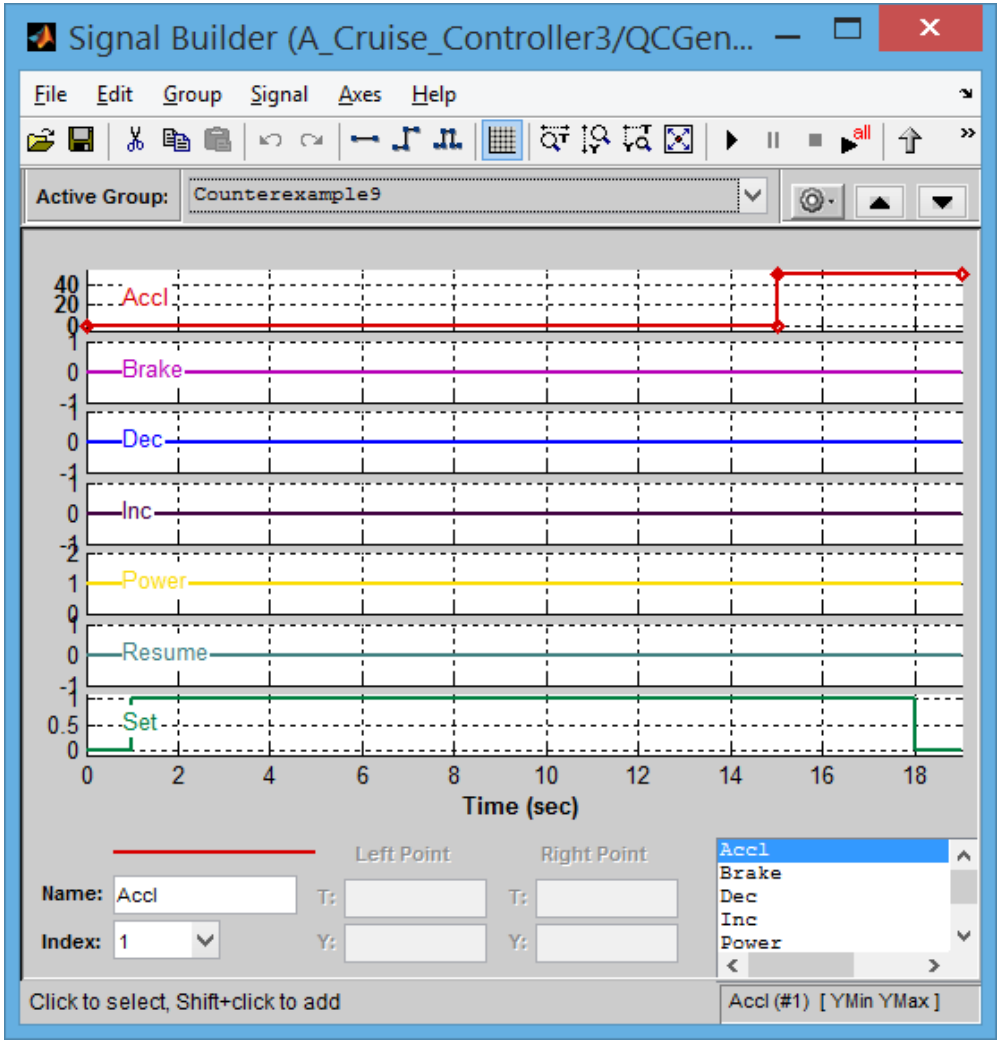
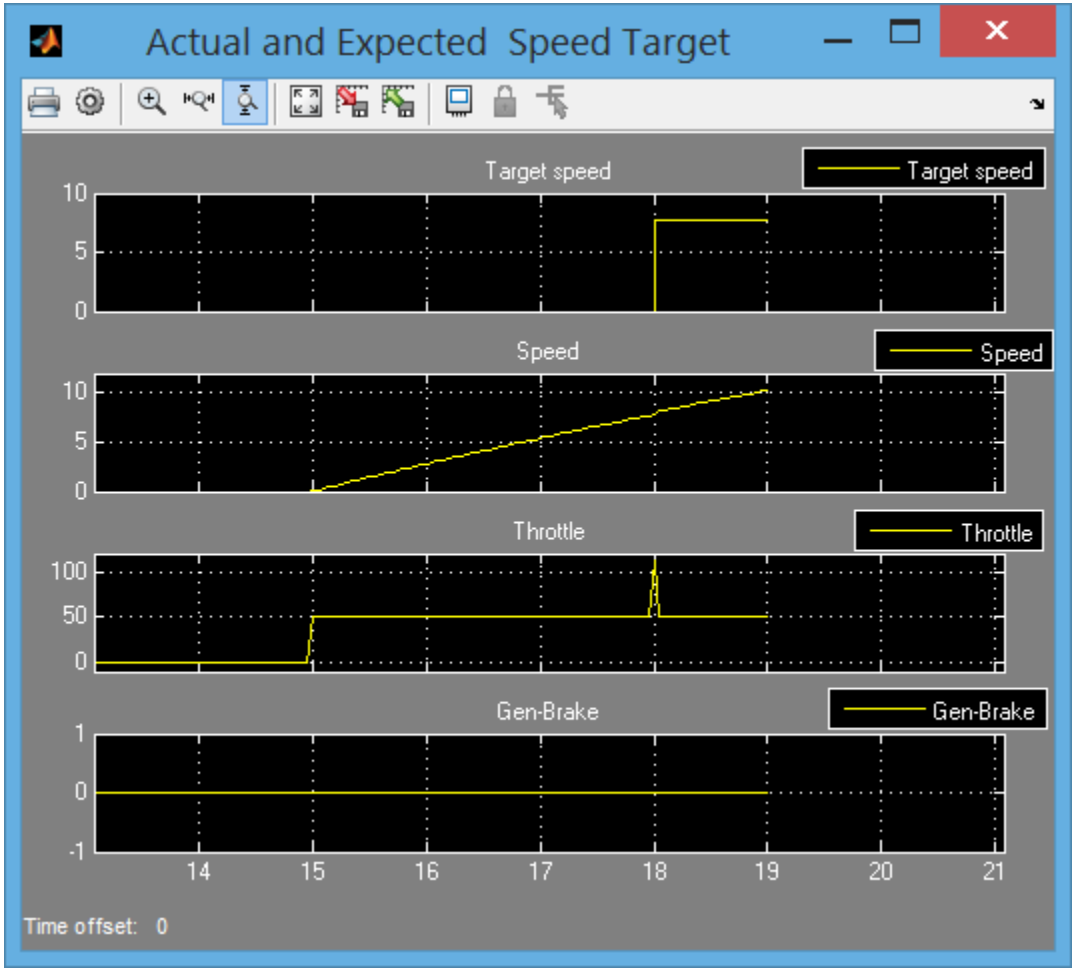


Figure 1
File Edit View Insert Tools Desktop Window Help
15000
10000
5000
0
0 10 20 30 40 50 60

One more example

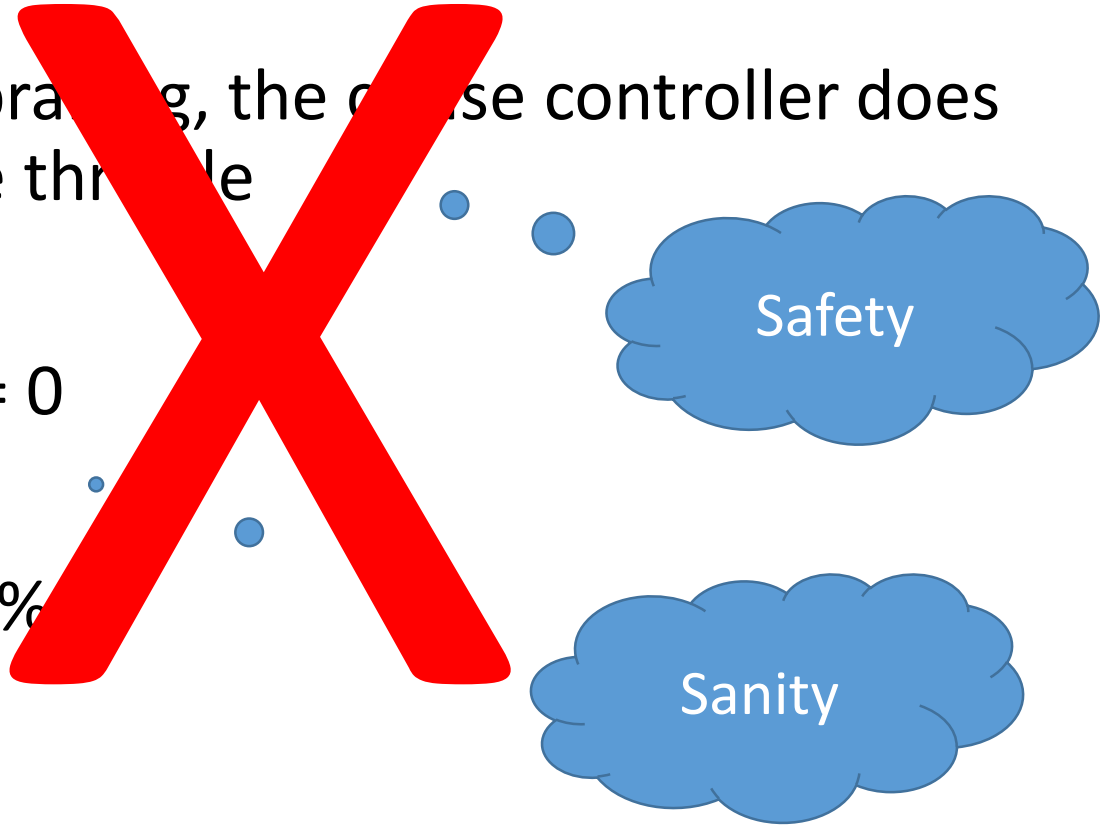


What can go wrong?



Three nice properties

- If the driver is bra g, the c se controller does not operate the thr le
- Target speed >= 0
- Throttle <= 100%



A more realistic cruise controller

- With an option to maintain (desired-speed – speed-limit)

- Rounding of desired speed leads to

  Desired speed < speed limit ➔ desired speed > speed limit

- Turning ”follow speed limit” mode off and on either side of a speed limit change leads to a sudden jump in desired speed

Work in progress

- Only a few generators implemented so far; slower than it should be
- Generators and properties can be implemented in a way familiar to SIMULINK developers
- Signals can be generated and shrunk to find interesting examples for a small cruise controller