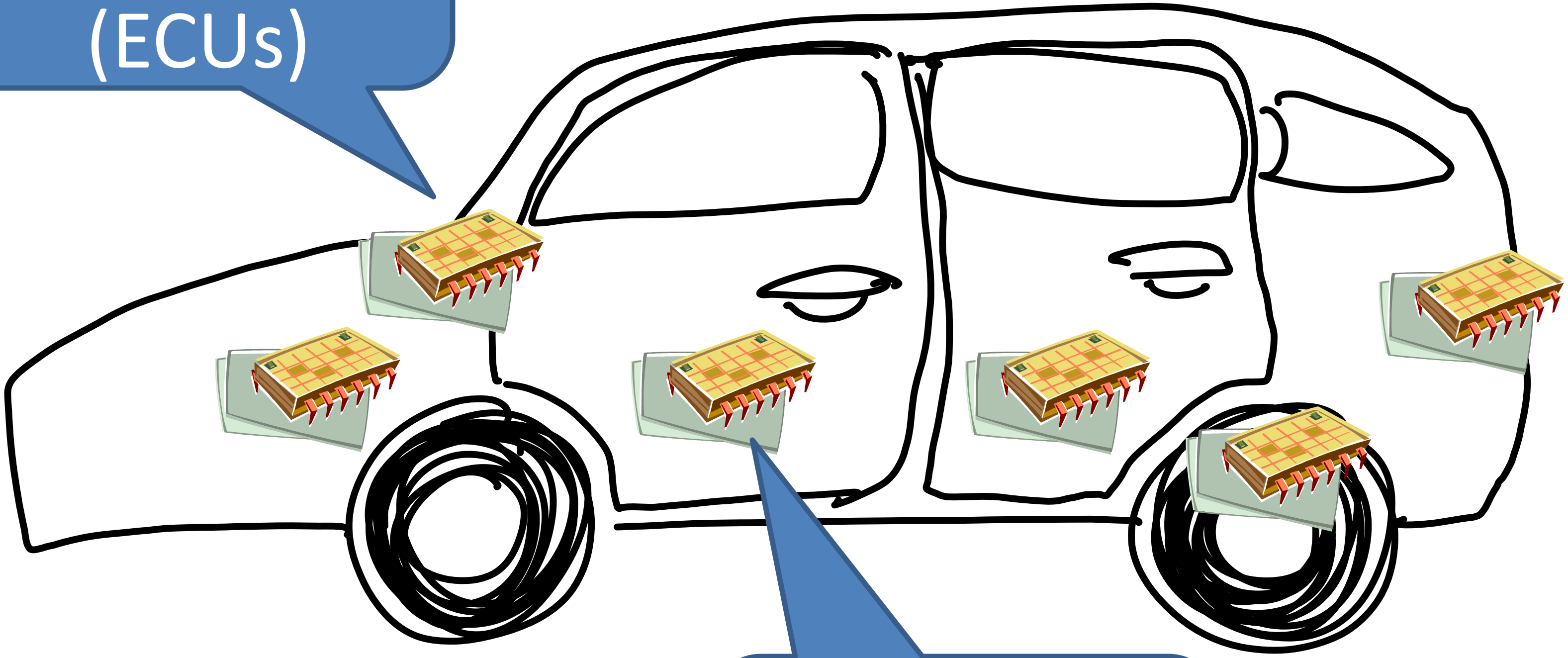
Certifying your car with Erlang

John Hughes

QuviQ

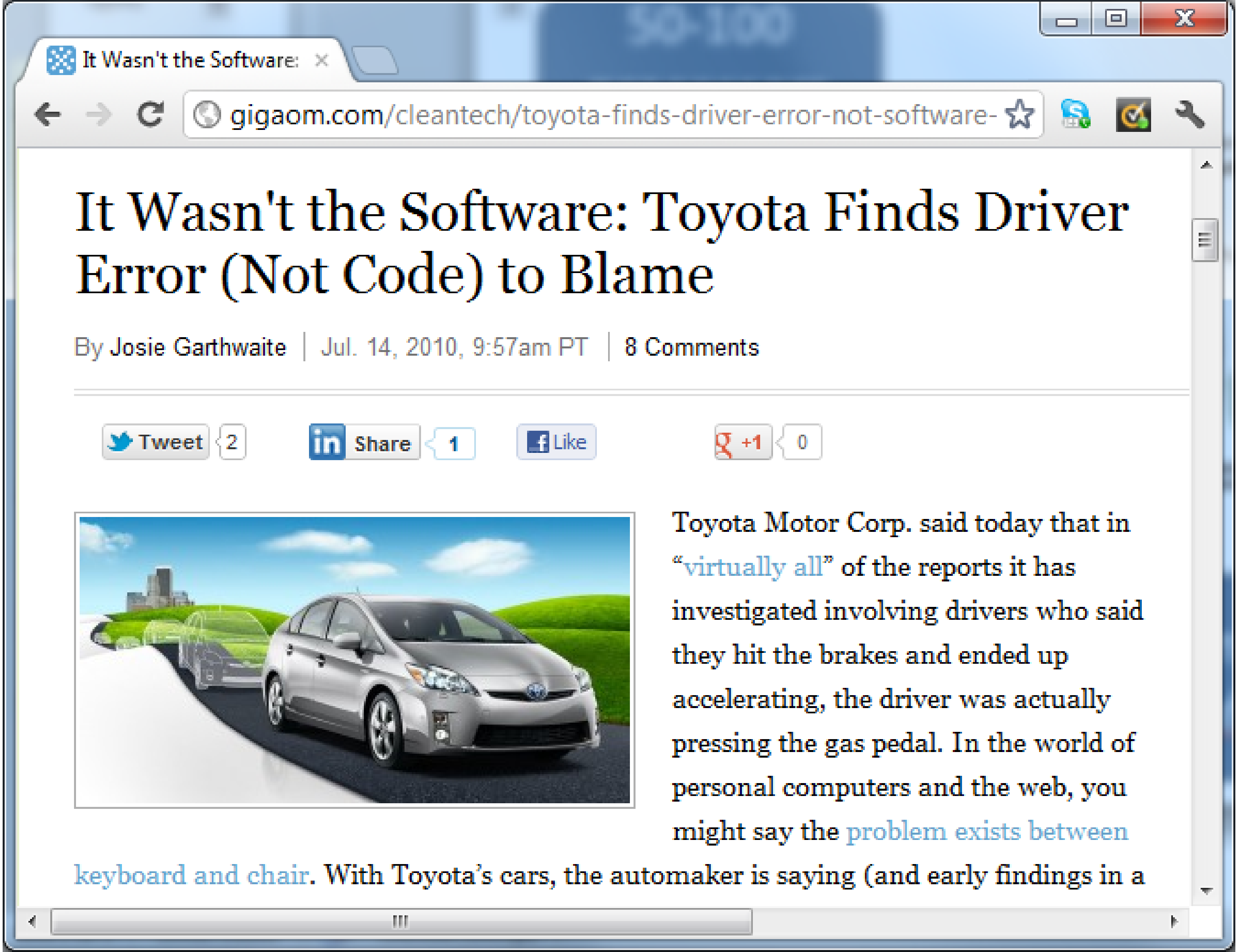
CHALMERS

Here’s your car



50-100 processors (ECUs)

100 million lines of code

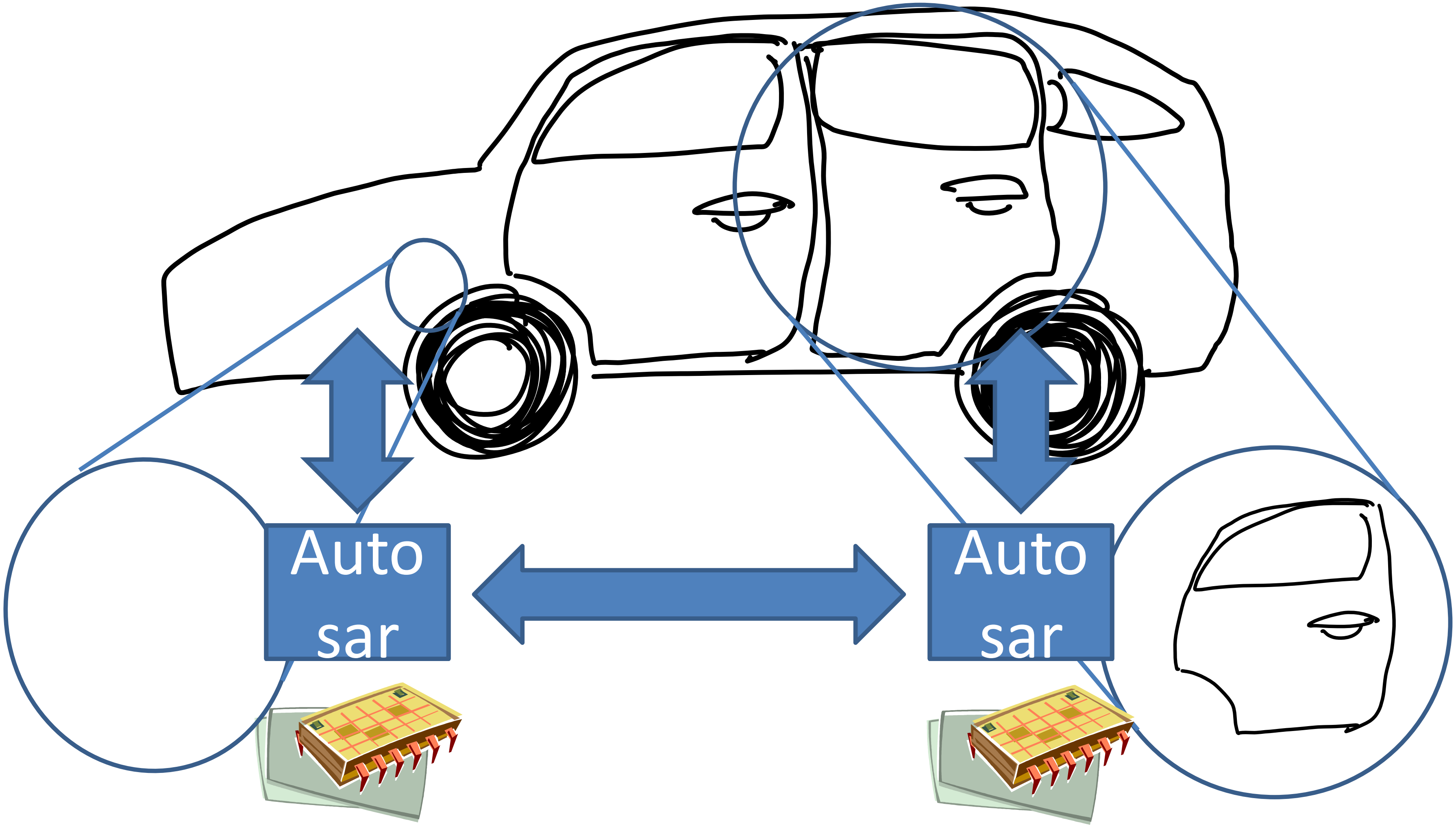

It Wasn't the Software:
gigaom.com/cleantech/toyota-finds-driver-error-not-software-
Tweet 2
in Share 1
Like
+1 0

It Wasn't the Software: Toyota Finds Driver Error (Not Code) to Blame

By Josie Garthwaite | Jul. 14, 2010, 9:57am PT | 8 Comments

Toyota Motor Corp. said today that in "virtually all" of the reports it has investigated involving drivers who said they hit the brakes and ended up accelerating, the driver was actually pressing the gas pedal. In the world of personal computers and the web, you might say the problem exists between keyboard and chair. With Toyota's cars, the automaker is saying (and early findings in a

Here’s your car again



BMW GROUP

BMW

MINI

DAIMLER

BOSCH

Ford

AUTOSAR AUTOMOTIVE OPEN SYSTEM ARCHITECTURE

GM

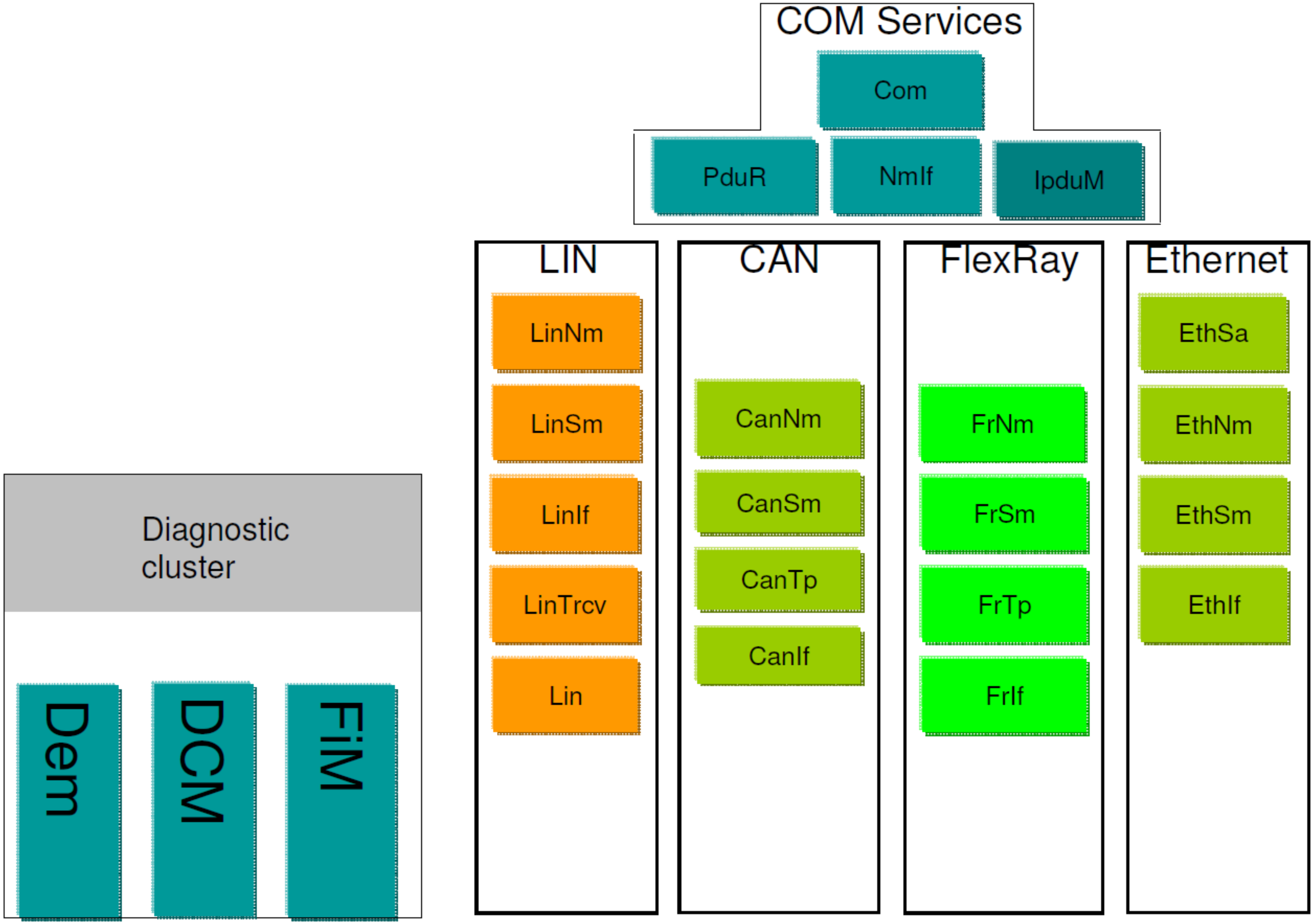
Continental

VOLKSWAGEN
AKTIENGESELLSCHAFT

TOYOTA

PSA PEUGEOT CITROËN

AUTOSAR Basic Software



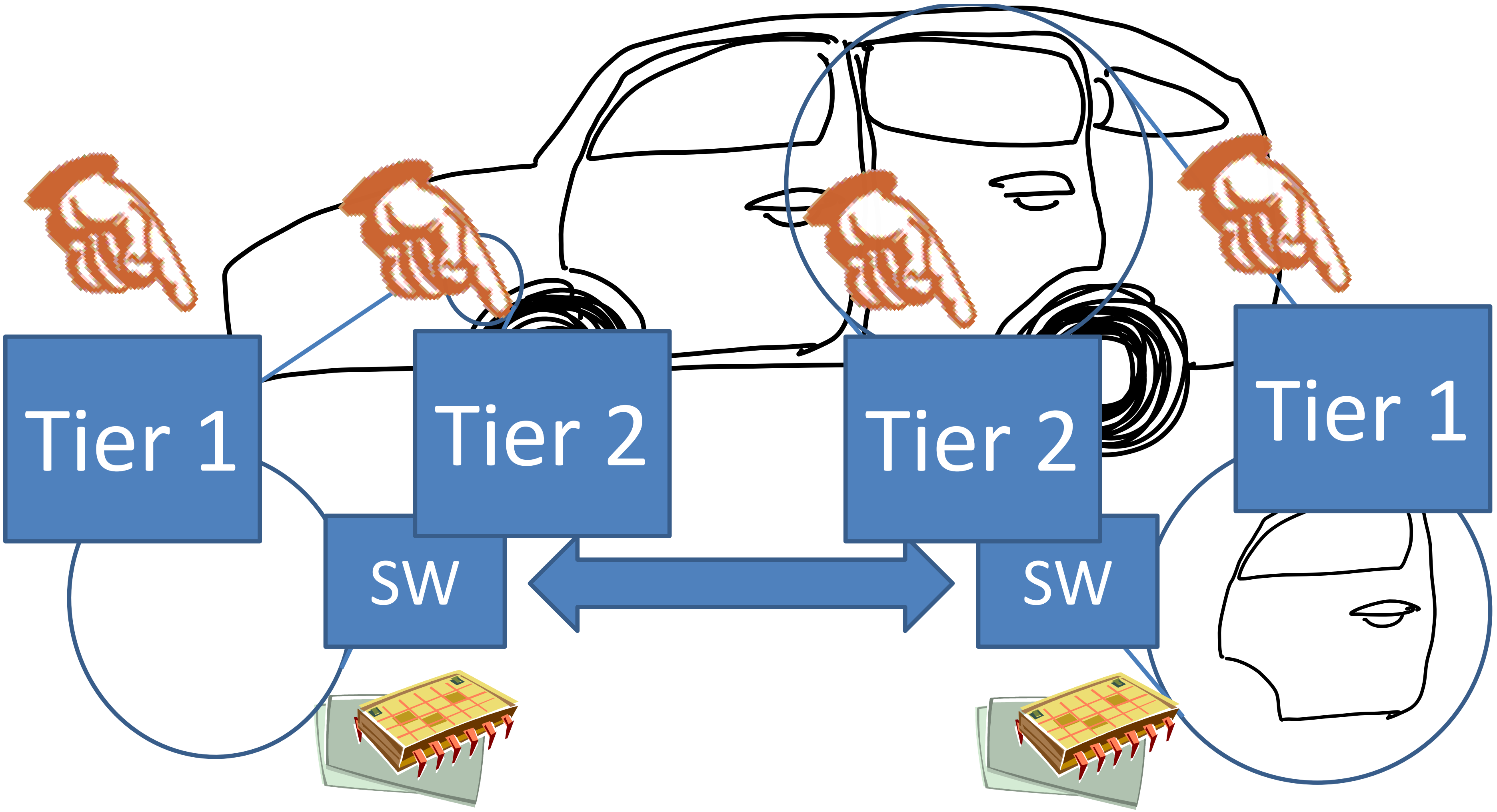
Theory

Car manufacturers should be able to buy code from different providers and have them work seamlessly together

Practice

VOLVO's experience has been that this is often not the case

VOLVO



Tier 1

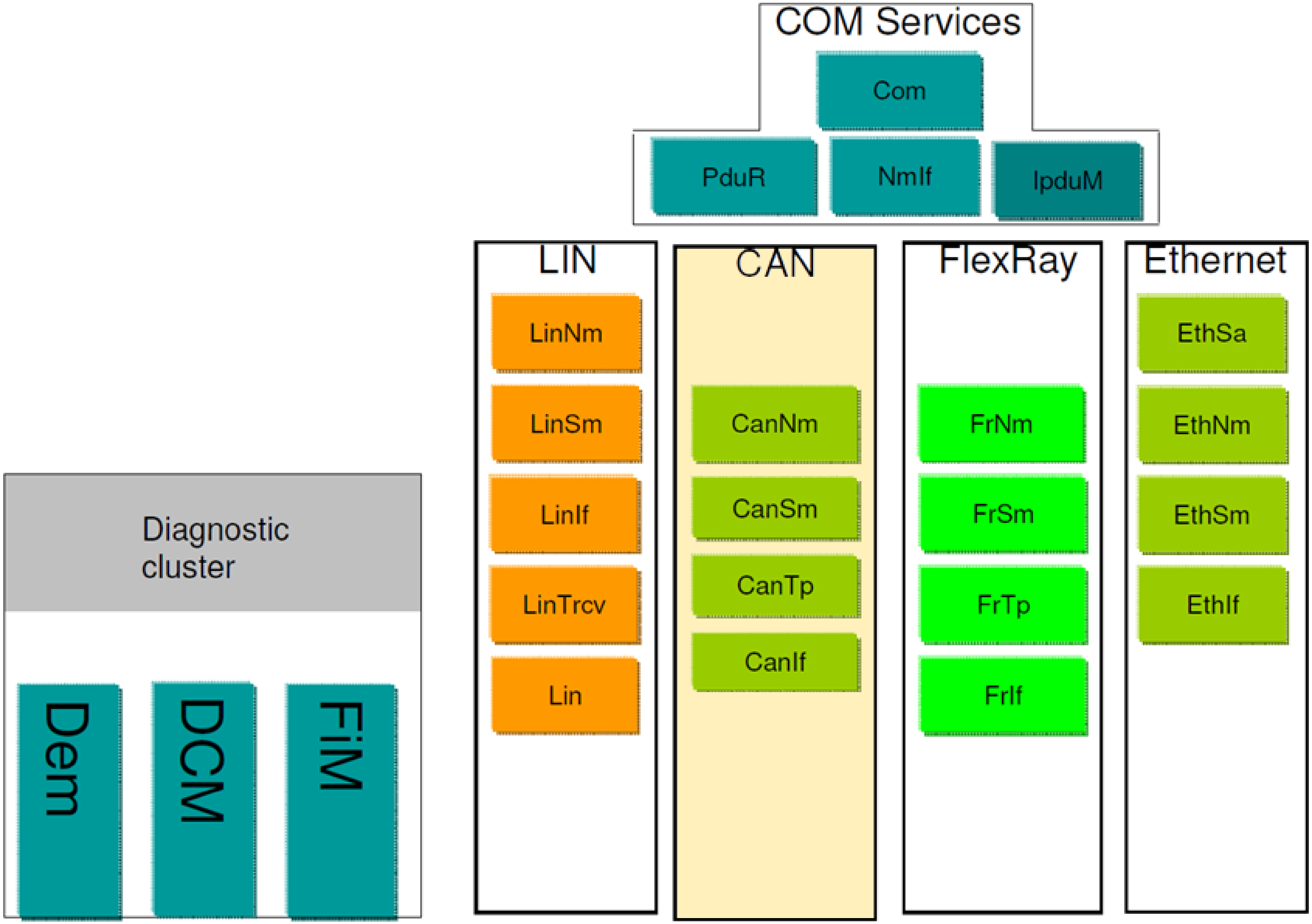
Tier 2

Tier 2

Tier 1

SW

SW



COM Services

Com

PduR

NmIf

IpduM

LIN

LinNm

LinSm

LinIf

LinTrcv

Lin

CAN

CanNm

CanSm

CanTp

CanIf

FlexRay

FrNm

FrSm

FrTp

FrIf

Ethernet

EthSa

EthNm

EthSm

EthIf

Diagnostic cluster

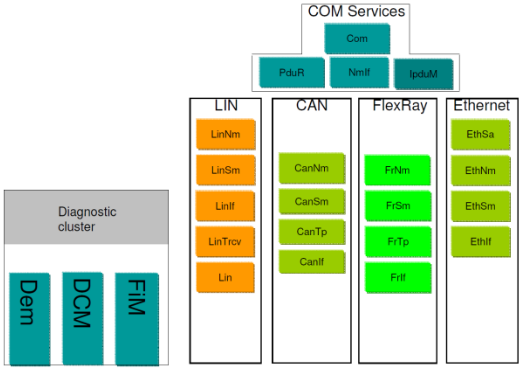
Dem

DCM

FiM

The Plan

VOLVO



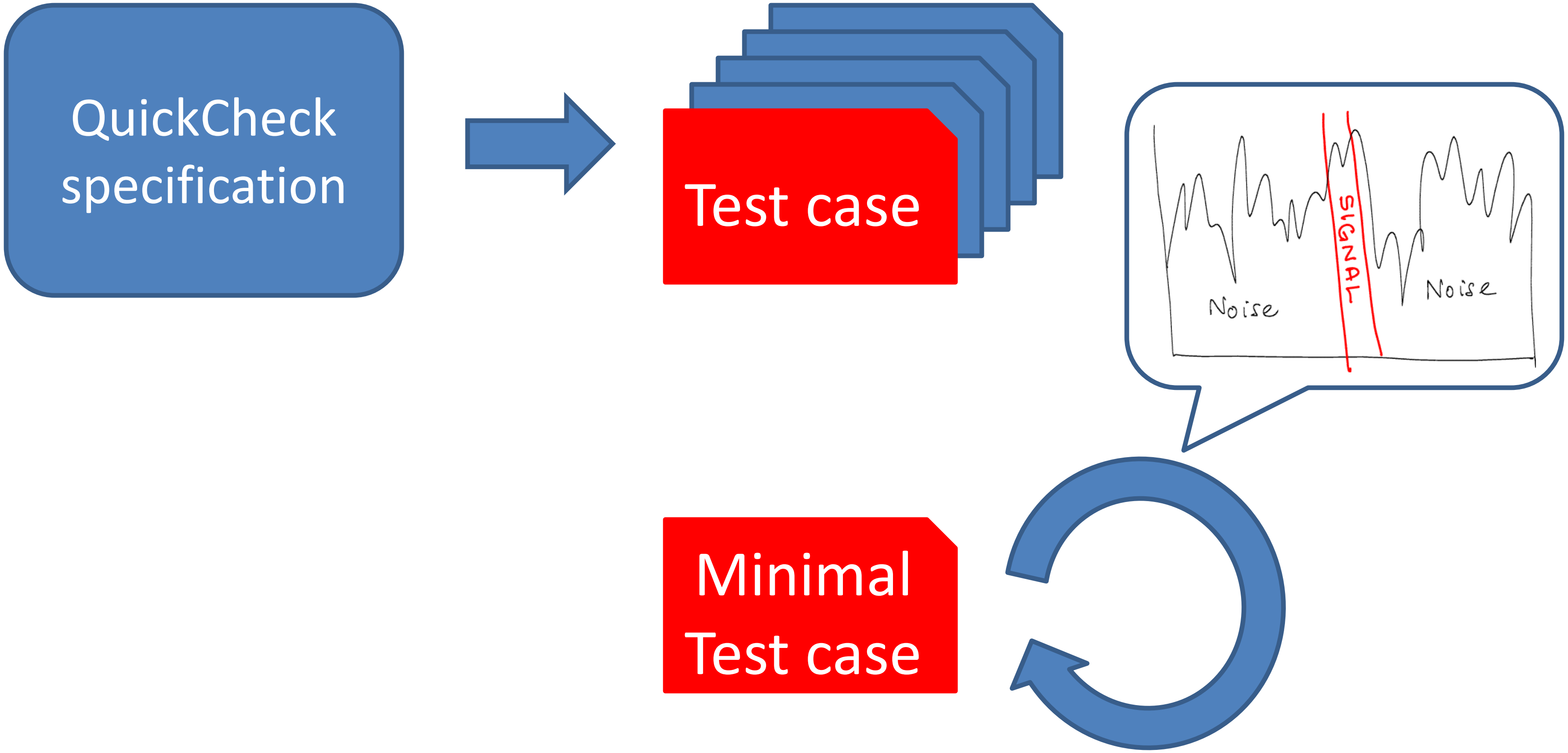
SP

your Science Partner

QuviQ

Demo

QuickCheck in a Nutshell



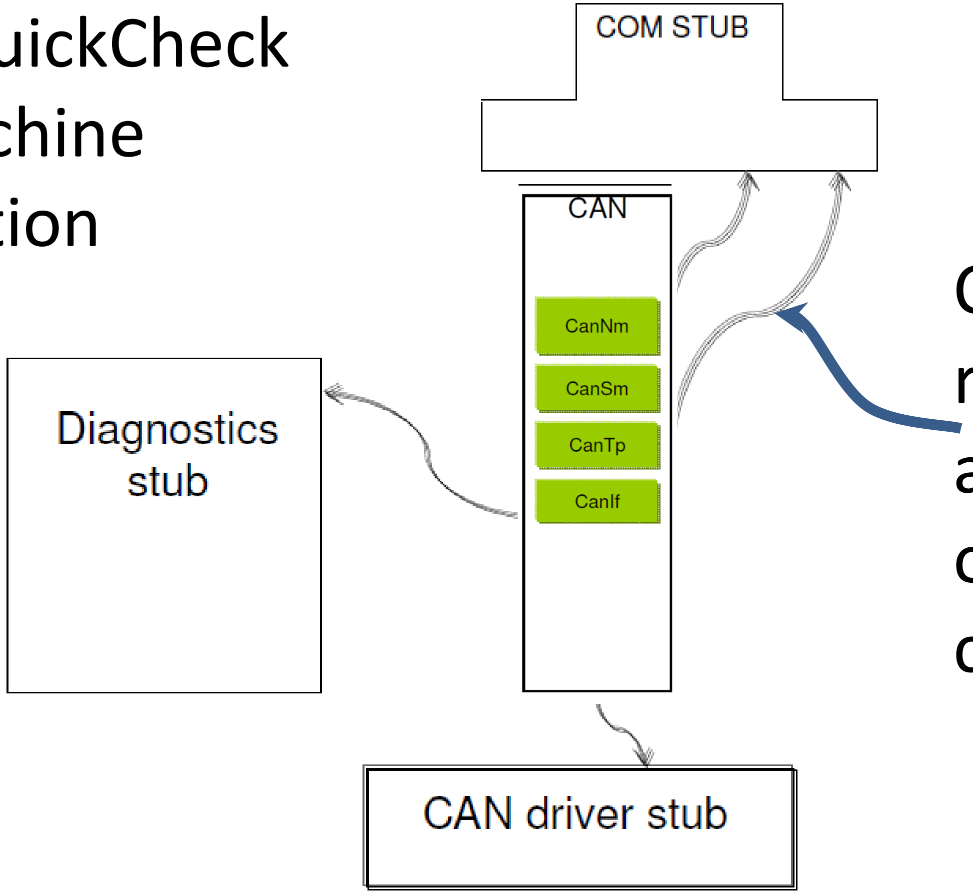
QuickCheck specification

Test case

Minimal Test case

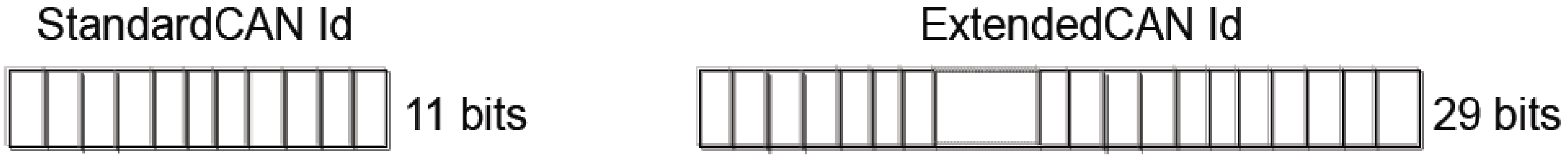
Testing strategy

API calls generated from a QuickCheck state machine specification



Check the right calls are made to other components

Example bug in vendor code



StandardCAN Id

11 bits

ExtendedCAN Id

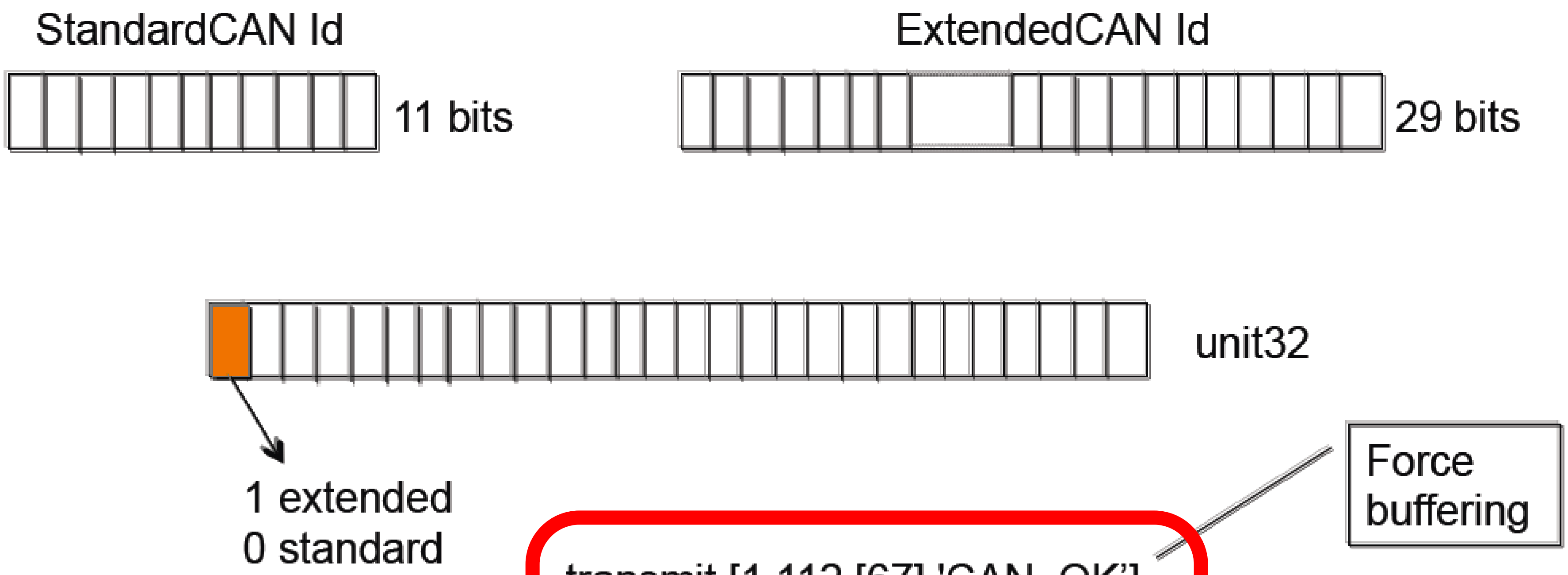
29 bits

Priority: lowest number has highest priority

Example:
Extended Id 113 has higher
priority than standard Id 114

Buffered higher priority
messages should be sent first

Example bug in vendor code



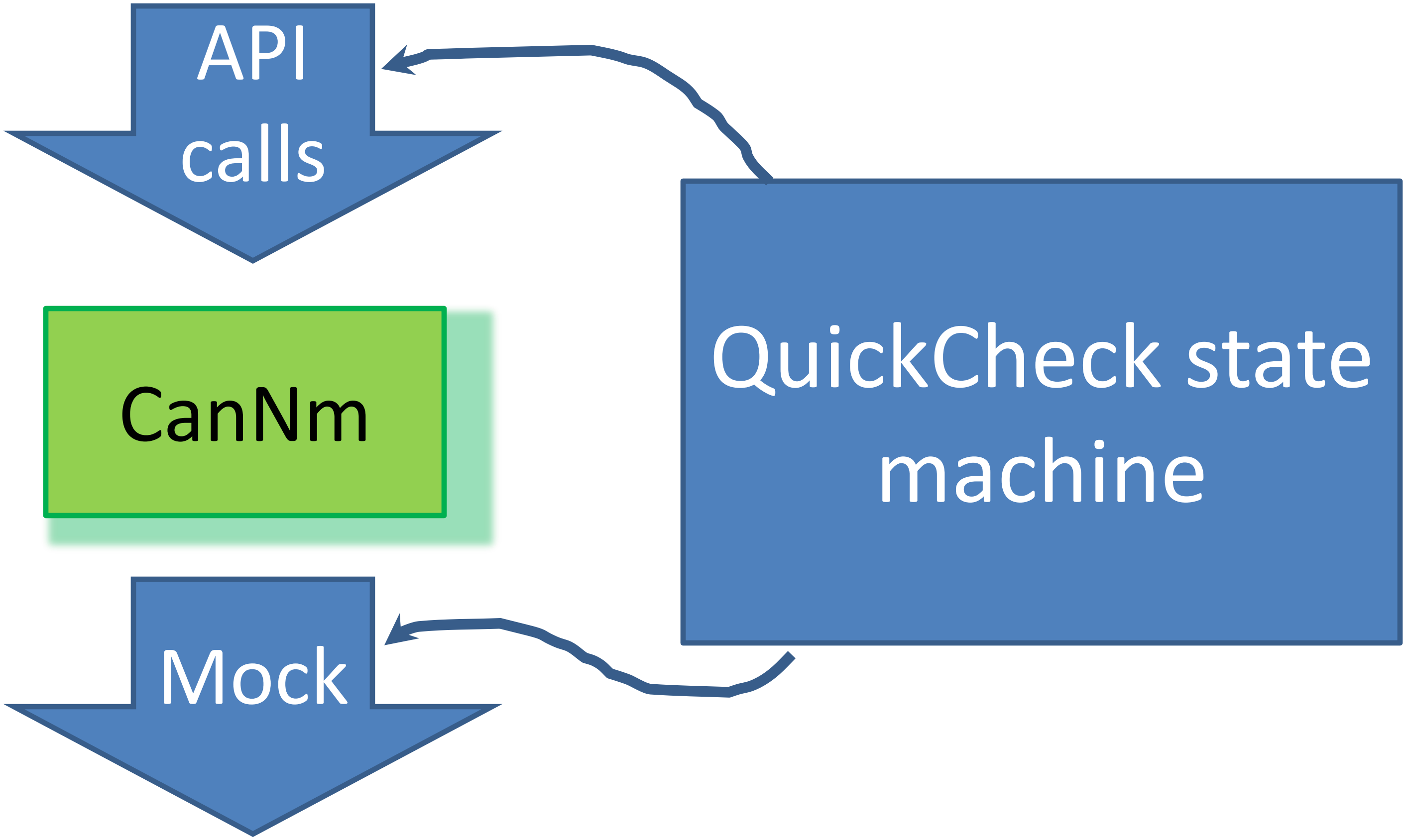
```
transmit,[1,112,[67],'CAN_OK’],
transmit,[2,113,[0],'CAN_BUSY’],
transmit,[3,114,[0],'CAN_BUSY’],
tx_confirmation,[1,112,[67]]
```

Force buffering

Trigger sending

Check callouts: 112, 114 sent, why?

Testing Components



eqc_component

```
% halt_communication

halt_communication(CtrlIdx) ->
    c_call:'FrIf_HaltCommunication'(CtrlIdx).
```

Uses QuickCheck's link to C

```
halt_communication_pre(S,[Ctrl]) ->
    synchronized(S,Ctrl) andalso
        S#frif_state.initialized.
```

Precondition

```
halt_communication_next(S,_V,[Ctrl],_Callouts) ->
    on_controller_state(S,Ctrl,
        fun (_) -> 'FR_POCSTATE_HALT' end).
```

State transition

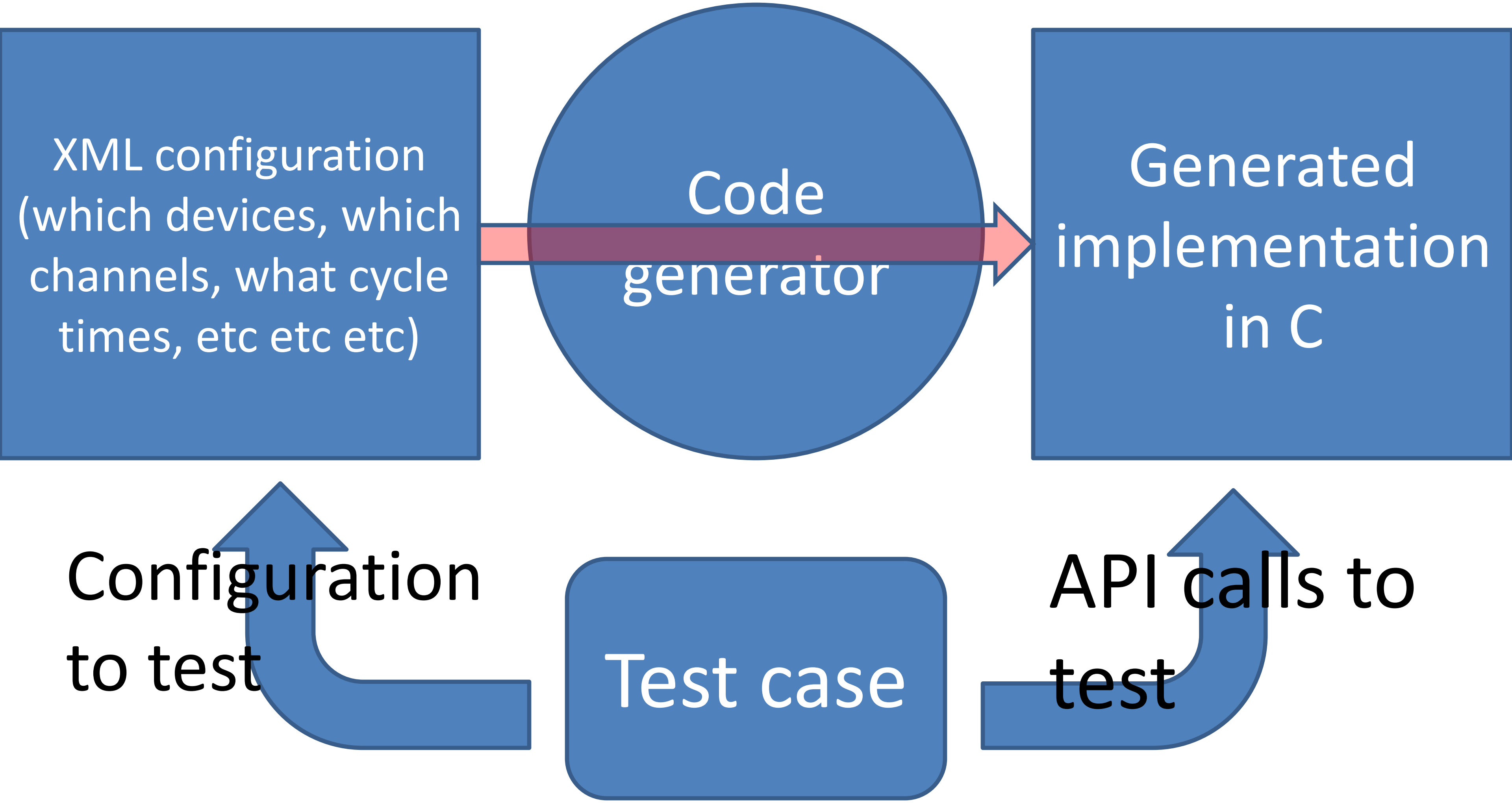
```
halt_communication_callouts(_S,[Ctrl]) ->
    [{{callout, c_call,?HaltCommunication,
        [translate_ctrl(Ctrl)]},ok}].
```

Expected callouts

”For every sequence of API calls satisfying the preconditions, all postconditions hold and the callouts are as specified.”

Challenges

Configurations



XML configuration (which devices, which channels, what cycle times, etc etc etc)

Code generator

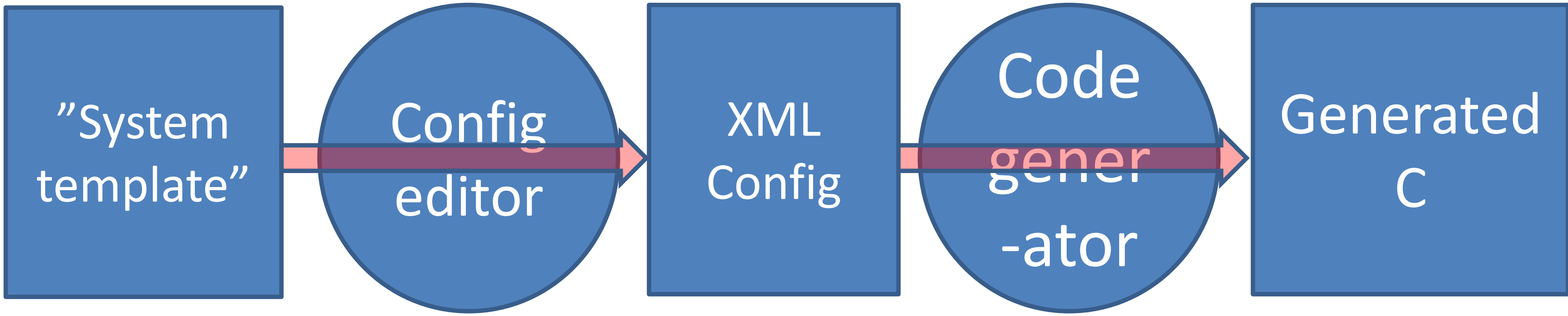
Generated implementation in C

Configuration to test

Test case

API calls to test

Configurations in reality



”System template”

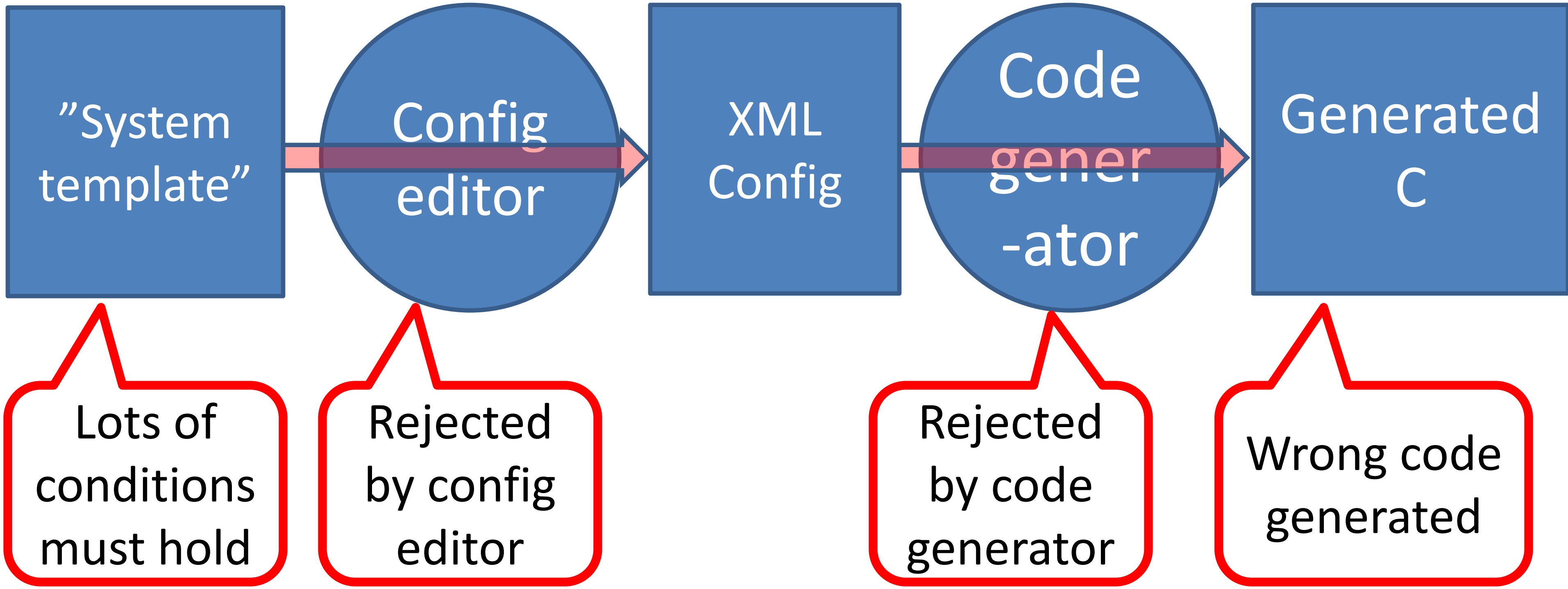
Config editor

XML Config

Code gener -ator

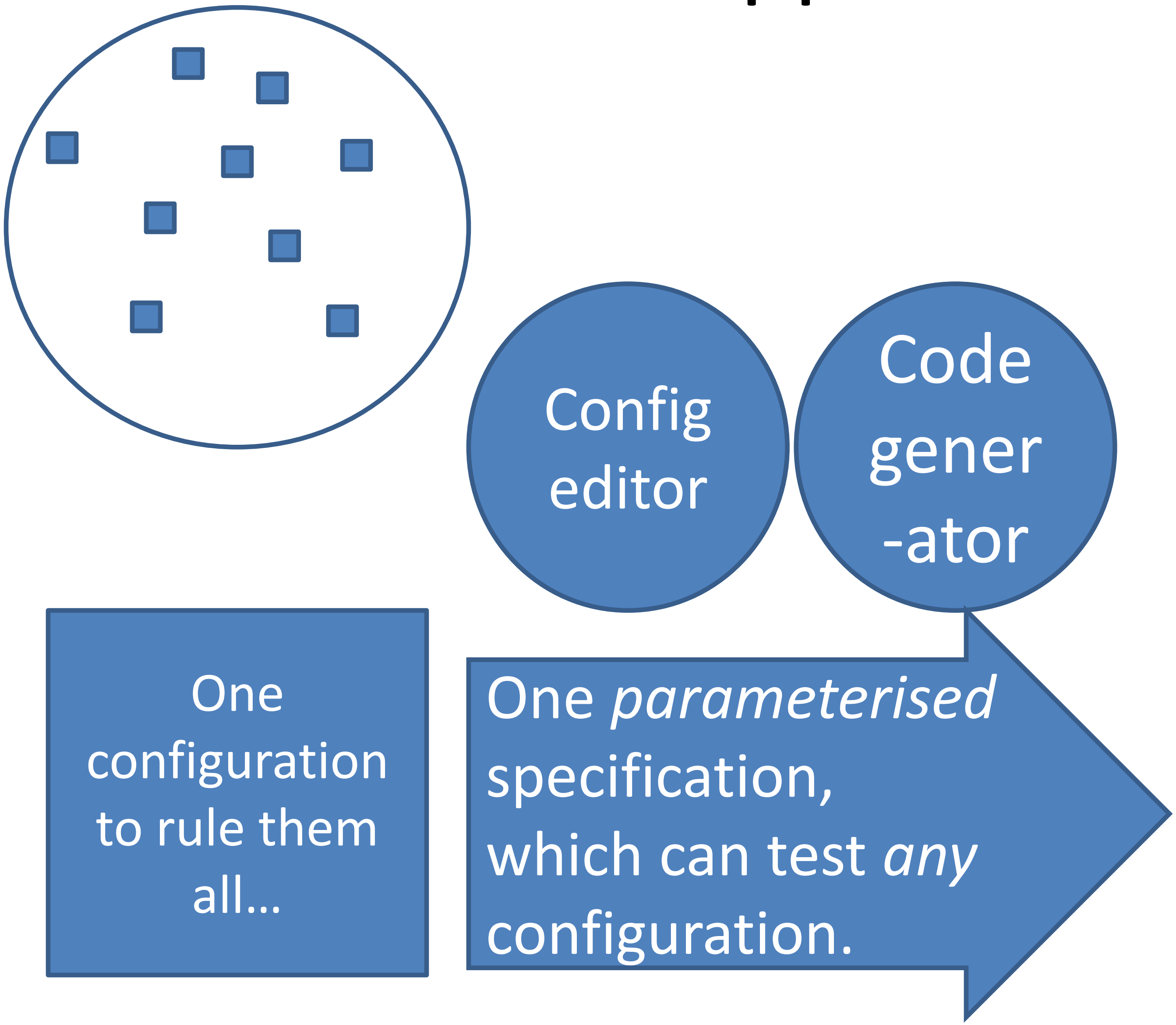
Generated C

Configuration errors



- Sometimes a genuine error, sometimes just ”not supported” by the vendor

Our Approach



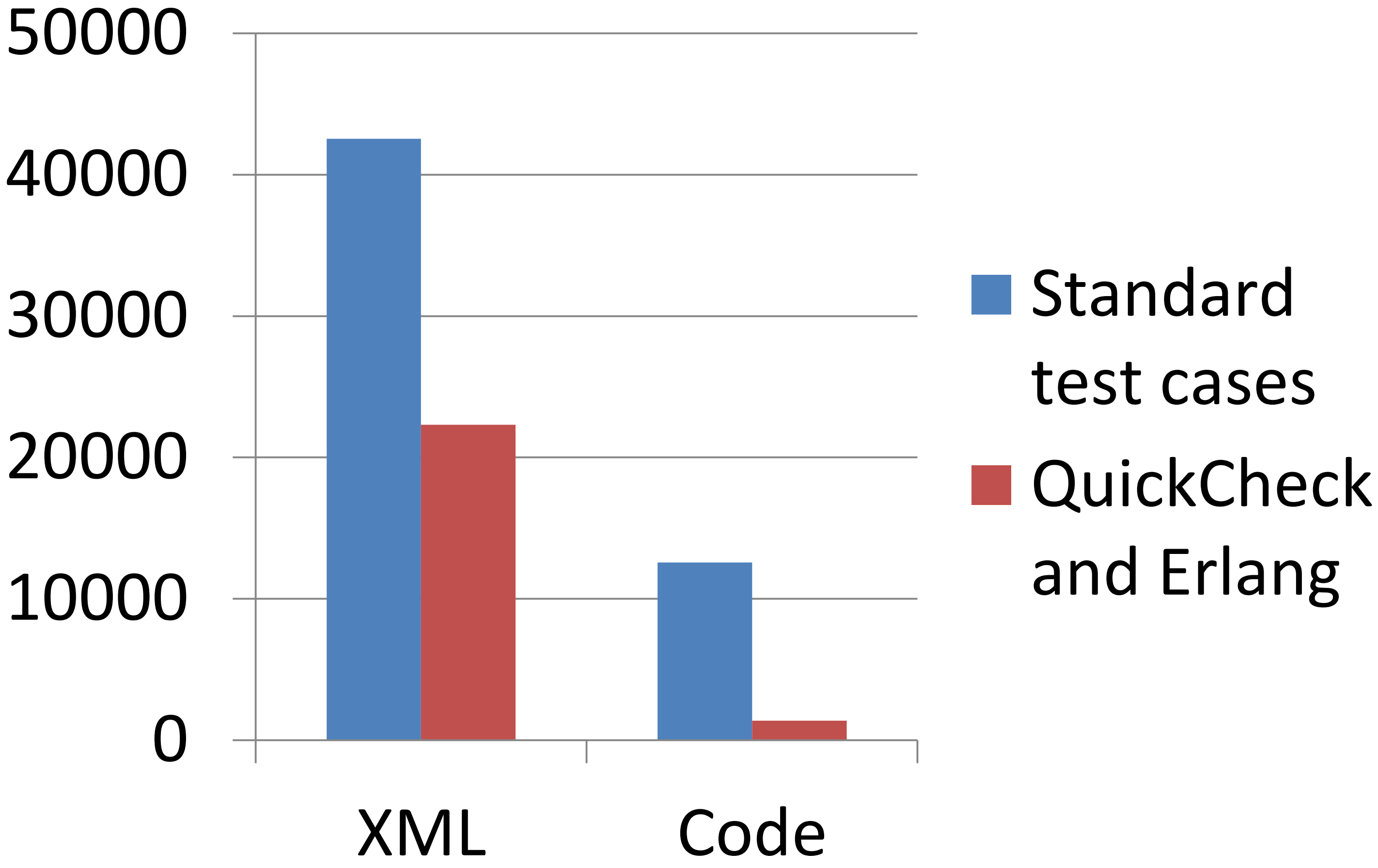
Config editor

Code gener-ator

One configuration to rule them all…

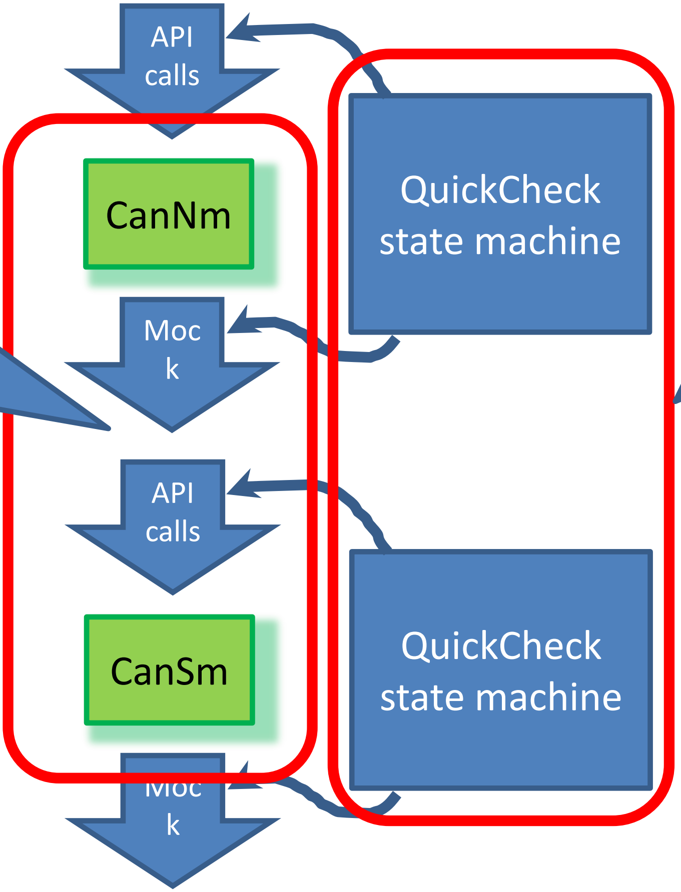
One *parameterised* specification, which can test *any* configuration.

Test code for Flexray Interface



- The code is 16x smaller!

Challenge: Clusters

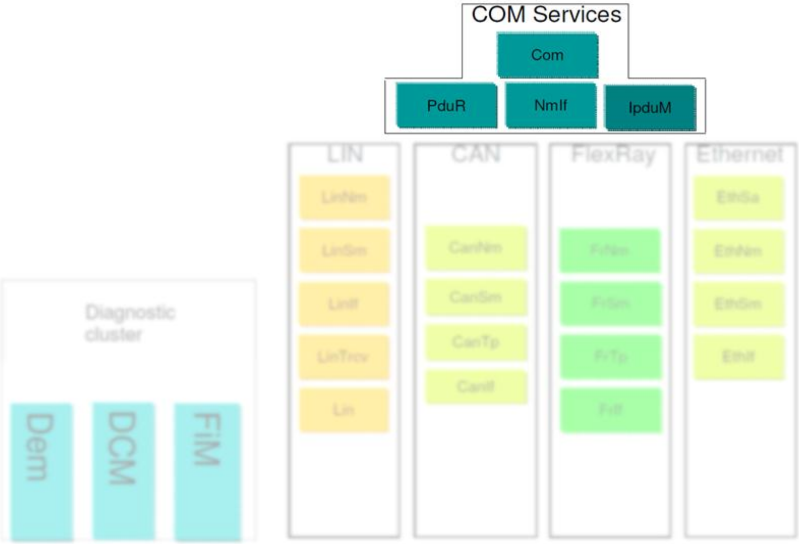


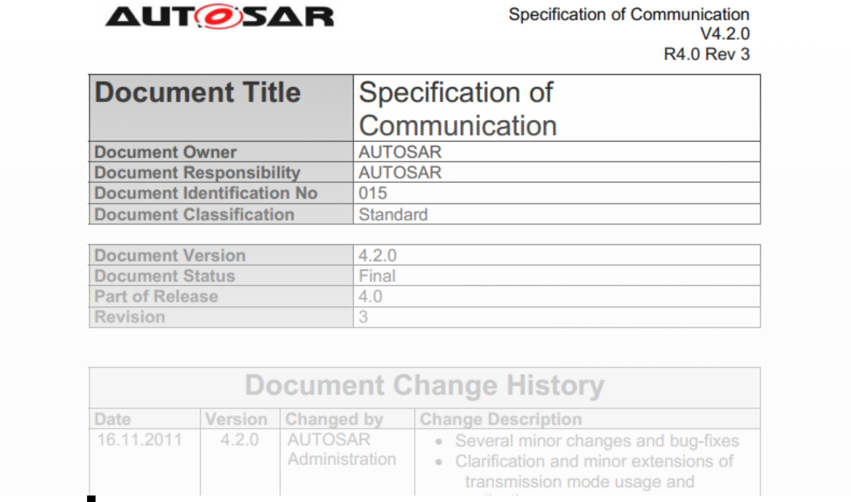
This interface need not exist!

Composable specifications

Important for writing *modular* specifications

Challenges





AUTOSAR

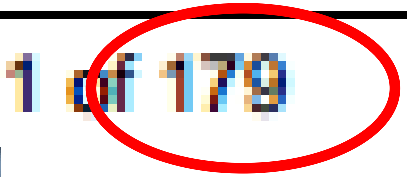
Specification of Communication
V4.2.0
R4.0 Rev 3

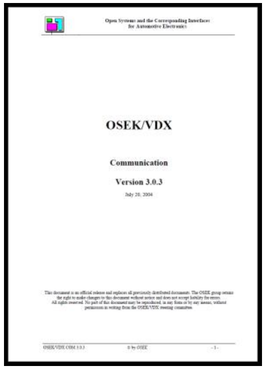
Document Title	Specification of Communication
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	015
Document Classification	Standard

Document Version	4.2.0
Document Status	Final
Part of Release	4.0
Revision	3

Document Change History

Date	Version	Changed by	Change Description
16.11.2011	4.2.0	AUTOSAR Administration	• Several minor changes and bug-fixes • Clarification and minor extensions of transmission mode usage and





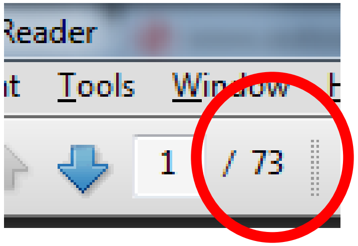
Open Systems and the Corresponding Interfaces for Automotive Electronics

OSEK/VDX

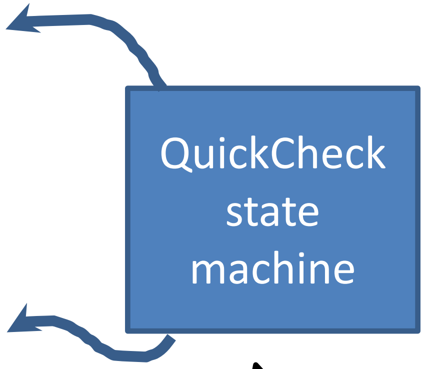
Communication

Version 3.0.3

July 29, 2004

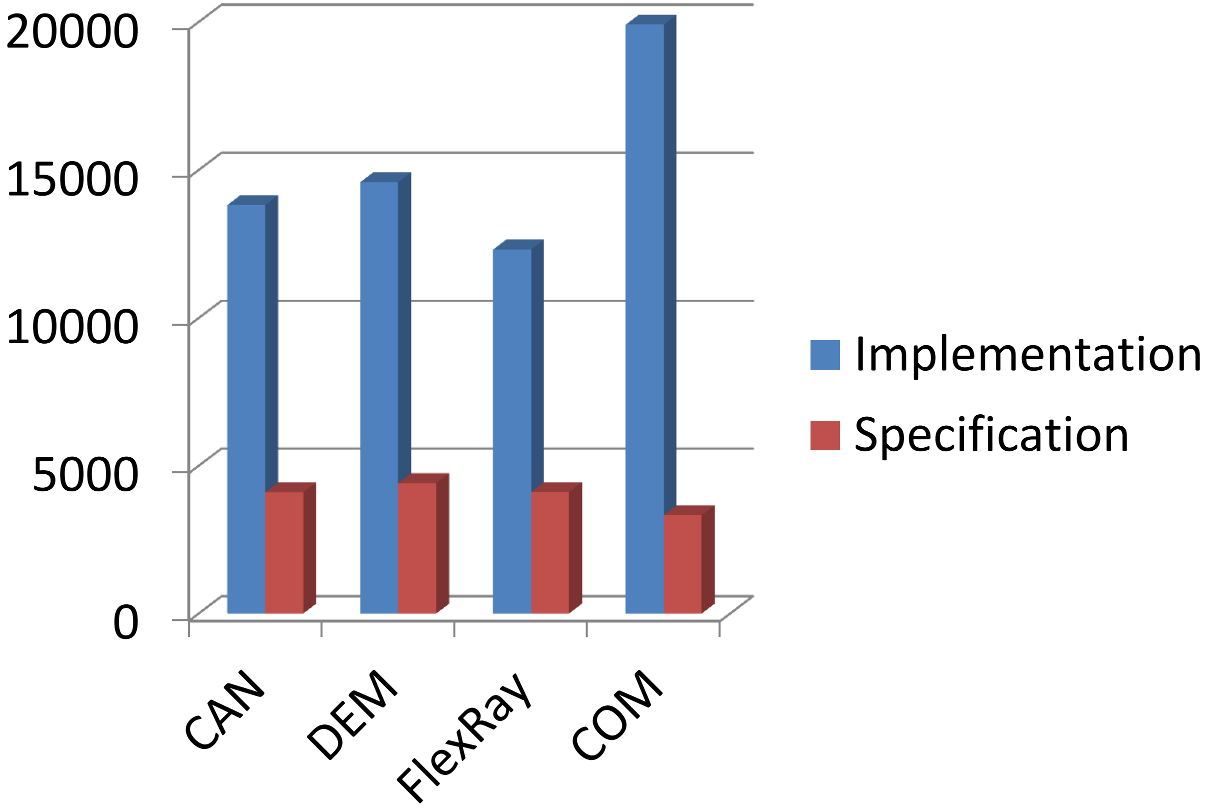


The Problem of Scale

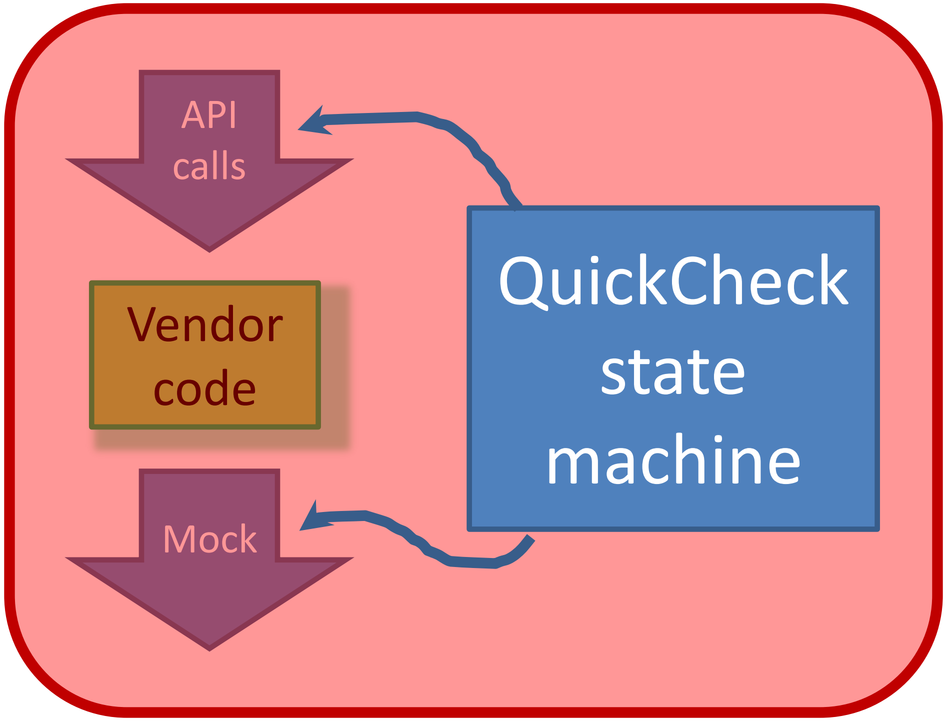


QuickCheck state machine

Essentially an implementation of AUTOSAR in Erlang!



How do we know our code is right?



- QuickCheck tests vendor code
- Vendor code tests our models

Who is right?

- Read the standard
- Ask Volvo!

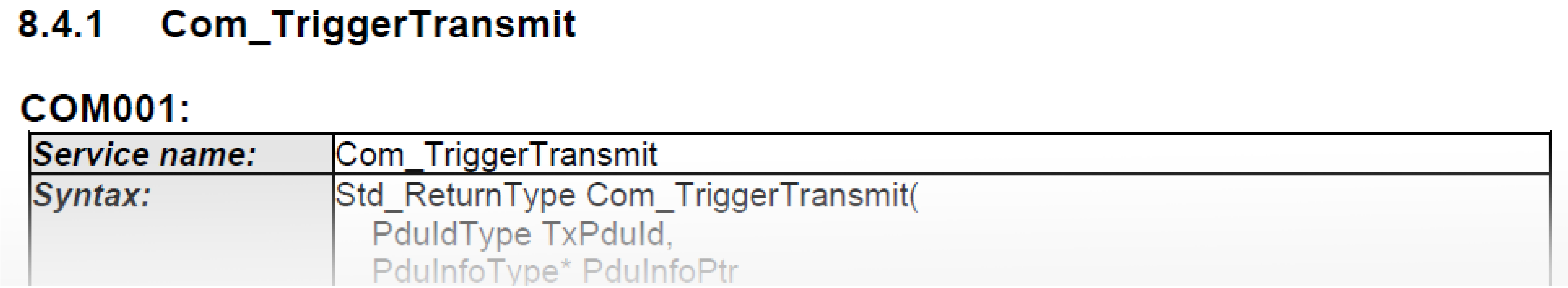
Read the Standard

> CANNM066: When the NM Message Tx Timeout Timer expires, the CanNm Module shall optionally call the function Nm_TxTimeoutException once.

- Once every…
  - Power-on?
  - Reinitialization?
  - Timer expiry?

- Optionally?

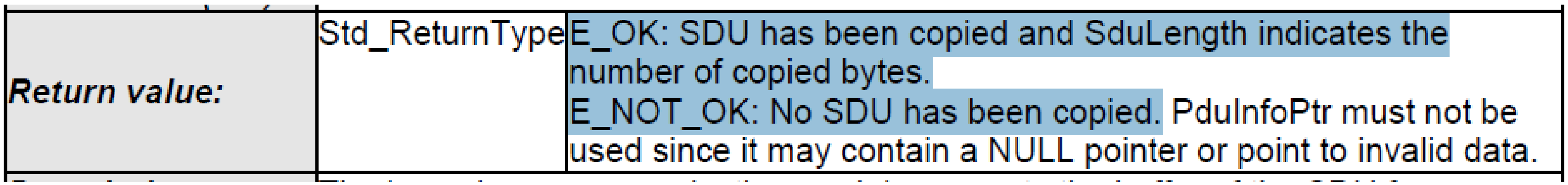
Read the Standard



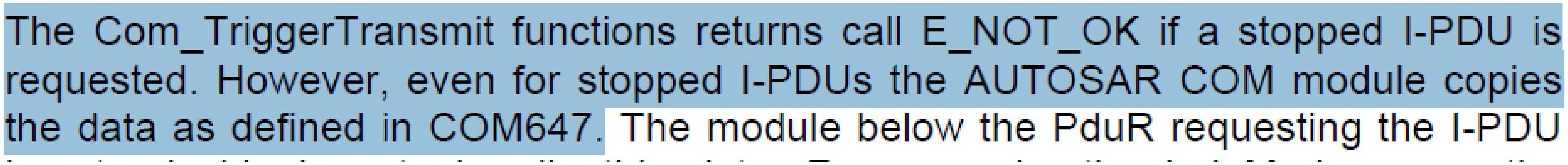
8.4.1 Com_TriggerTransmit

COM001:

Service name:	Com_TriggerTransmit
Syntax:	Std_ReturnType Com_TriggerTransmit(PduIdType TxPduId, PduInfoType* PduInfoPtr



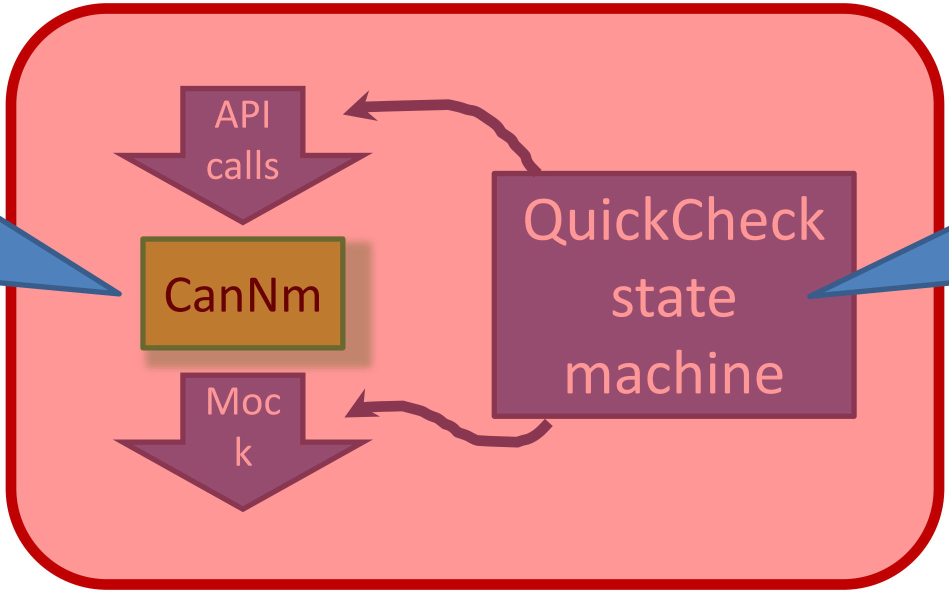
Return value:	Std_ReturnType	E_OK: SDU has been copied and SduLength indicates the number of copied bytes. E_NOT_OK: No SDU has been copied. PduInfoPtr must not be used since it may contain a NULL pointer or point to invalid data.



The Com_TriggerTransmit functions returns call E_NOT_OK if a stopped I-PDU is requested. However, even for stopped I-PDUs the AUTOSAR COM module copies the data as defined in COM647. The module below the PduR requesting the I-PDU

Challenge: the Most Probable Bug

Fix the bug?



API calls

CanNm

Mock

QuickCheck state machine

…or *unfix* the spec!

Almost always the same!

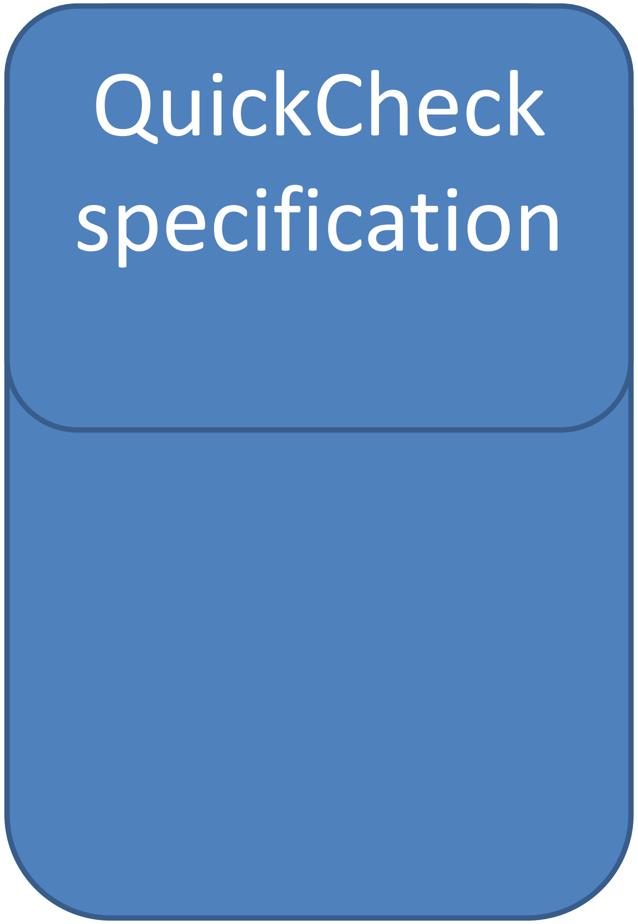
The *minimal failing test case*

”Bug specifications”

```
initial_send_timer(#tm_periodic{delay = T}) ->
  Ticks = com_cfg:ticks(T,tx),
  case ?com_bug_014 of
      true  -> Ticks;
      false -> Ticks + 1    % we decrement before test
  end;
```

```
deinit_next(S, _V, [], []) ->
    case ?com_bug_027 of
       true ->  S#state{comstate = 'COM_UNINIT'};
       false ->
         (initial_state_data())#state{comstate = 'COM_UNINIT'}
    end.
```

Delousing the Specification



QuickCheck specification

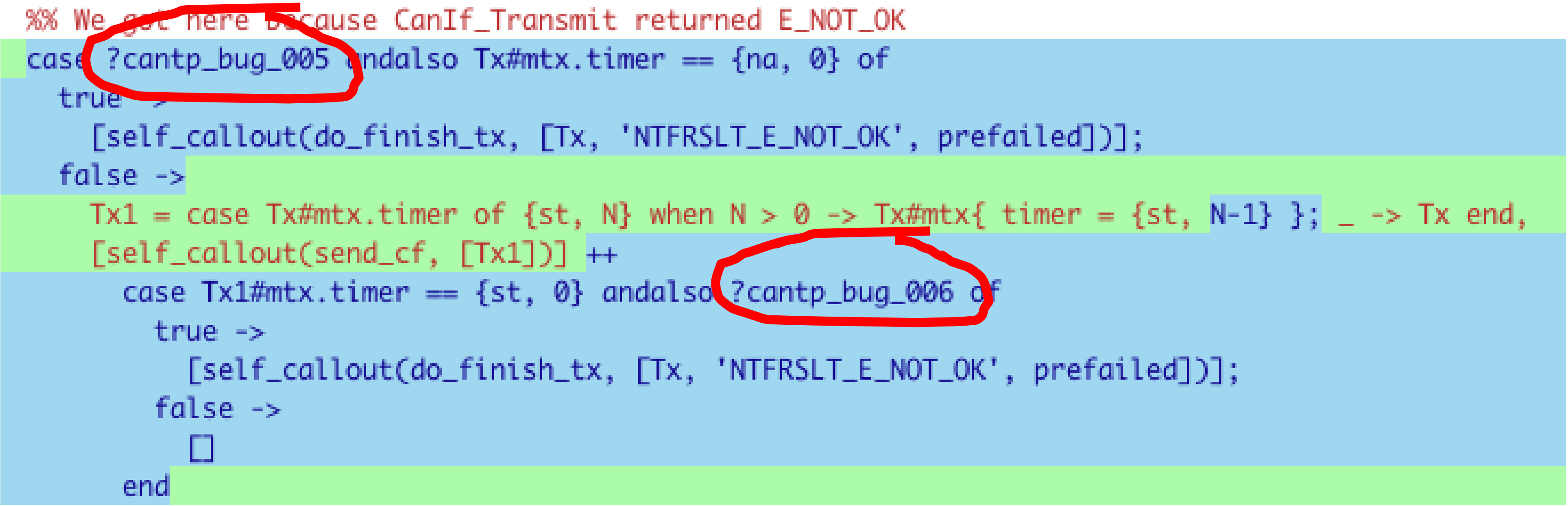
VOLVO

Enter: Wrangler!

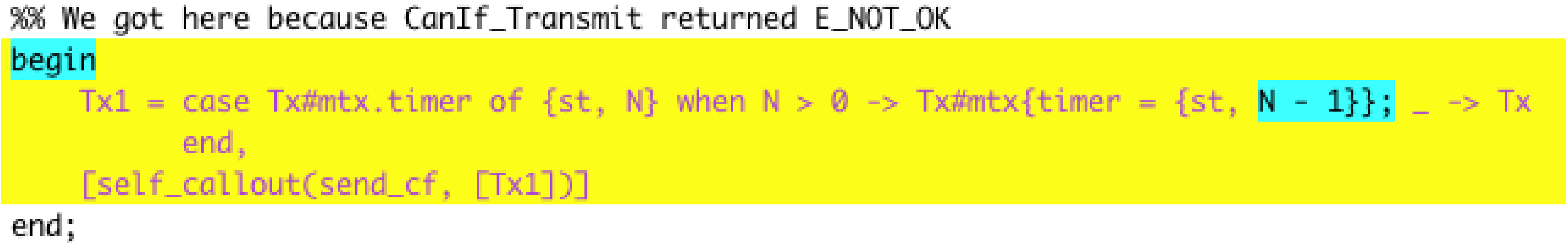
- A *scriptable* refactoring tool for Erlang

- Delousing
  - ?xxx_bug_ddd ➔ false
  - Boolean simplification
  - Remove clauses with false guards
  - Simplify case true/false of …
  - Simplify list comprehensions

Wrangling



```
%% We got here because CanIf_Transmit returned E_NOT_OK
case ?cantp_bug_005 andalso Tx#mtx.timer == {na, 0} of
  true ->
    [self_callout(do_finish_tx, [Tx, 'NTFRSLT_E_NOT_OK', prefailed])];
  false ->
    Tx1 = case Tx#mtx.timer of {st, N} when N > 0 -> Tx#mtx{ timer = {st, N-1} }; _ -> Tx end,
    [self_callout(send_cf, [Tx1])] ++
      case Tx1#mtx.timer == {st, 0} andalso ?cantp_bug_006 of
        true ->
          [self_callout(do_finish_tx, [Tx, 'NTFRSLT_E_NOT_OK', prefailed])];
        false ->
          []
      end
```



```
%% We got here because CanIf_Transmit returned E_NOT_OK
begin
    Tx1 = case Tx#mtx.timer of {st, N} when N > 0 -> Tx#mtx{timer = {st, N - 1}}; _ -> Tx
          end,
    [self_callout(send_cf, [Tx1])]
end;
```

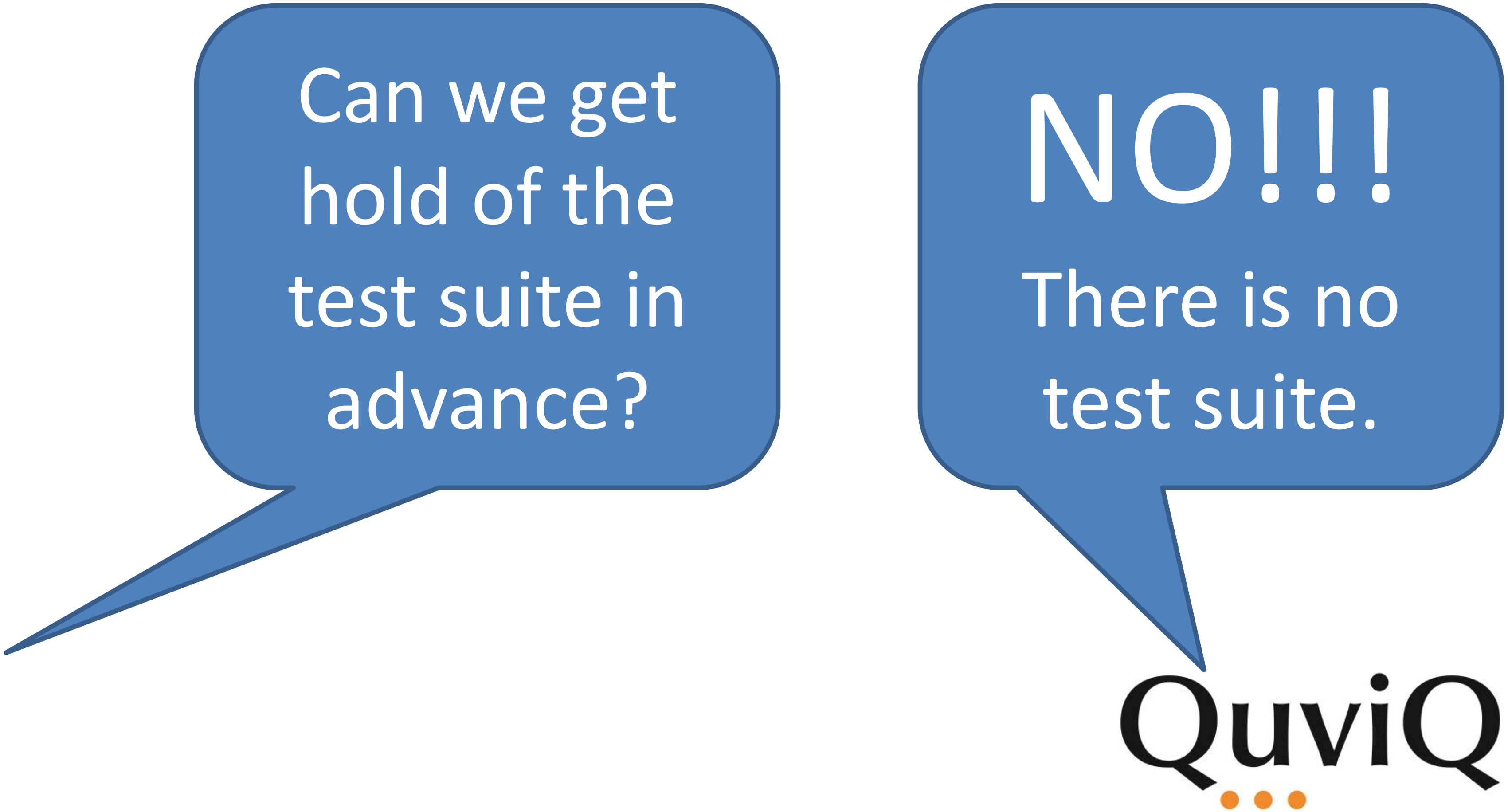
Results so far…

- Testing code from 6 suppliers

- **100+ issues identified already**
- **30+ bugs identified in the standard**

- On target to certify code later this year

Culture Shock



Can we get hold of the test suite in advance?

NO!!!

There is no test suite.

QuviQ

APPROVED

QuickCheck Automotive