FV FTW

wldhx

2017-12-29

#Bugs $\propto$ LOC

Every year, about 10 billion embedded devices are produced.

Michael Barr, 2007

Series E65 (2002–04) has over 70 modules on 16 different buses or sub-buses with about 8 modules using the CAN bus protocol.

BMW Vehicle Communication Software Manual (EAZ0025B42B)

In about 1999, BMW introduced EDK, which is a full drive-by-wire system with no mechanical throttle linkage.

BMW Vehicle Communication Software Manual (EAZ0025B42B)

Ford: The new F150 pickup has over 150 million LOC.

CES 2016

- HDDs
- Routers
- Bank cards
- Power banks
- Microwave ovens
- ...
- Internet backbone

SIL LEVELS

SIL 1	10e-5	11 years
SIL 2	10e-6	114 years
SIL 3	10e-7	1141 years
SIL 4	10e-8	11408 years

Only the end product is *tested*

TOYOTA

- 2003-2015
- 90 dead
- "Unintended Acceleration"
- 500 cases settled, >2.2$bn in initial

Michael Barr, Philip Koopman

THERAC-25

To keep a Boeing Dreamliner flying, reboot once every 248 days

https://goo.gl/LlyuRt

To keep Patriot missiles operational, reboot once every 2 days

https://embeddedgurus.com/barr-code/2014/03/lethal-software-defects-patriot-missile-failure/

Chrysler is recalling 1.4 million vehicles that can be remotely hacked over the Internet.

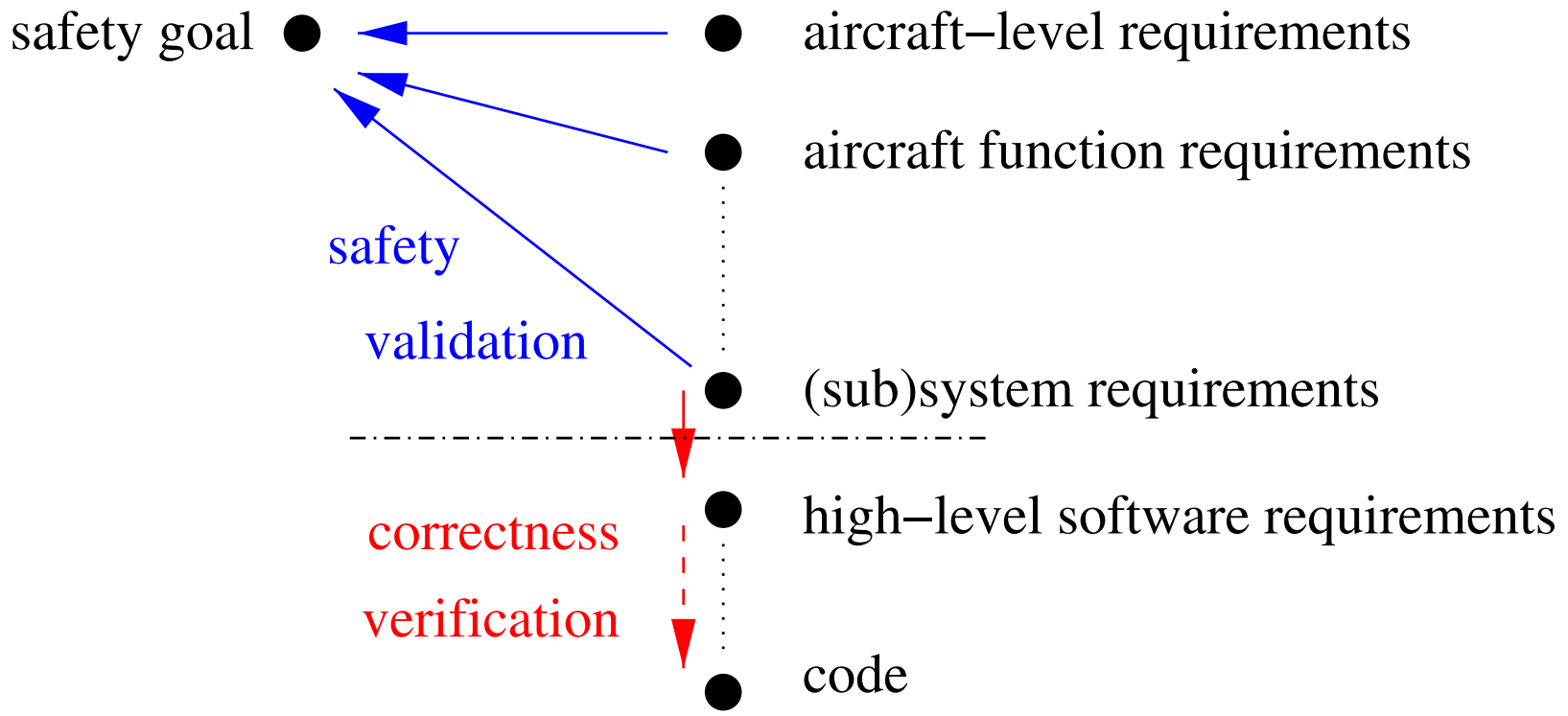
http://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/

Fuzzy concept -> code

			FV
SIL 1	10e-5	11 years	-
SIL 2	10e-6	114 years	R
SIL 3	10e-7	1141 years	R
SIL 4	10e-8	11408 years	HR

System vs. Software Assurance

- Safety analysis ends at the (sub)system requirements
- Thereafter it's all about correctness: DO-178B



SYSTEM VERIFICATION

TLA+, PlusCal

high-level, concepts, protocols

IMPLEMENTATION VERIFICATION

	static	**dynamic**
simple	type checking	dyn type checking
complex	theorem proving	contract checking

Opposed to exhaustive testing in embedded

SAMPLE: SPARK (FV)

```
procedure Simple (X: in out Integer)
  with Depends => (X => X),
       Pre  => (X < 0),
       Post => (X > 0);
```

SAMPLE: IVORY (FV)

```
make_zero :: (GetAlloc eff ~ Scope s)
          => Ivory eff (Ref s (Stored Sint32))
make_zero = local (ival 0)
```

END-TO-END VERIFICATION

```
Fuzzy concept -> code -> compiler -> hardware
                         ^- Fc       ^- Fc
```

CompCert

AWS

System	Components	Line count (excl. comments)	Benefit
S3	Fault-tolerant low-level network algorithm	804 PlusCal	Found 2 bugs. Found further bugs in proposed optimizations.
	Background redistribution of data	645 PlusCal	Found 1 bug, and found a bug in the first proposed fix.
DynamoDB	Replication & group-membership system	939 TLA+	Found 3 bugs, some requiring traces of 35 steps
EBS	Volume management	102 PlusCal	Found 3 bugs.
Internal distributed lock manager	Lock-free data structure	223 PlusCal	Improved confidence. Failed to find a liveness bug as we did not check liveness.
	Fault tolerant replication and reconfiguration algorithm	318 TLA+	Found 1 bug. Verified an aggressive optimization.

From 2004 on, Astrée analyzed the electric flight control codes for A380 series.

astree.ens.fr (paraphrase)

In April 2008, Astrée was able to prove completely automatically the absence of any RTE in a C version of the automatic docking software of the Jules Vernes Automated Transfer Vehicle (ATV) enabling ESA to transport payloads to the International Space Station.

O. Bouissou et al., Space software validation using Abstract Interpretation

seL4

- Qualcomm baseband
- Apple Secure Enclave (A7+)

Intel and AMD CPU caches

SPARK

- Eurofighter Typhoon
- Ship Self-Defense System
- Rolls-Royce Trent jet engines
- UK NATS iFACTS system
- ...

SpaceX is hiring FV engineers now

- TLA+: Lamport's video course and *Hyperbook*, learntla.com - for everyone
- *Type-Driven Development with Idris* if you have a Haskell background
- Isabelle/HOL or Coq (*Software Foundations*) if you want math