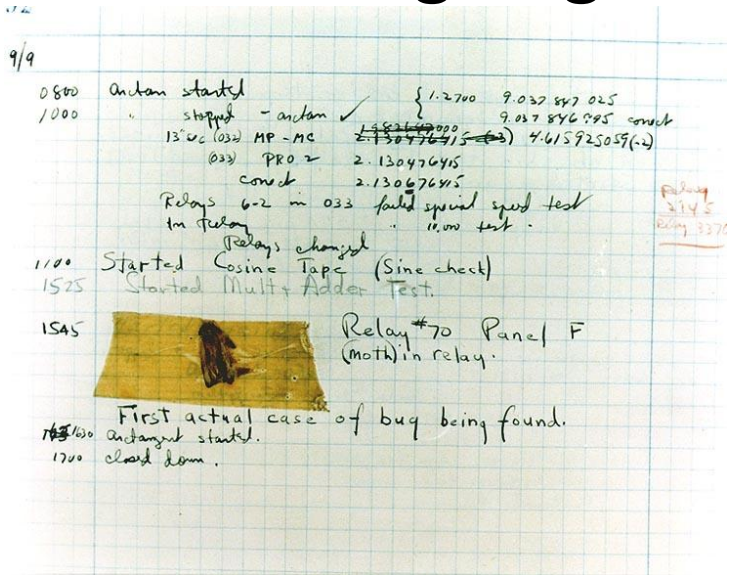
ArduPilot Critical Bug Review 2019-2020

Peter Barker + Andrew Tridgell
ArduPilot Dev Team

Rationale

Why are we talking about solved problems?

- avoid repeating mistakes
- consider hardening against similar problems
- share debugging techniques
- brainstorm new ideas for avoiding bugs



Stack Overflows

ARDUPILOT
Versatile, Trusted, Open

Stack Overflows

- Two instances in last year
  - signing of RC source messages #13619
  - ftp thread stack overflow #13542
- Both first noticed by users
  - easy to reproduce
  - produced watchdog resets
  - quickly diagnosed
  - need to implement stack logging #13896

Buffer Overruns

ARDUPILOT
Versatile, Trusted, Open

Buffer Overruns

- One in last year
  - GPS antenna offset in blending #13802
  - found by Randy in Iris testing
  - not in stable releases
  - took a few hours to diagnose
  - not found by valgrind and other tools
  - research into possible tools to find automatically came up with nothing
  - very difficult to completely avoid in C++

Protocol Timing

ARDUPILOT
Versatile, Trusted, Open

One bug caused by protocol timing

- high CPU load due to RCIN parsing on IOMCU
- led to loss of packets to IOMCU #13410
  - reported by user as motor stutter
  - not noticeable by most users
  - could also cause momentary RC input loss
  - triggered by pulse parsing (for PPM) of SBUS input

Logic Bugs

ARDUPILOT
Versatile, Trusted, Open

Most common bug type

- four serious bugs this year
  - gain restore in AUTOTUNE #13423
  - bootloader update alignment bug #13099
  - CPU overload preventing scheduler tasks #12324
  - 16 bit timer wrap #9284
- Only one (CPU overload) led to crash, but others could have
  - only method to avoid is improving review and testing?

Error Checking

ARDUPILOT
Versatile, Trusted, Open

Lack of error checking gave one serious bug

- lack of check on DMA allocation for sdcard writes #13305
  - showed up as corrupt logs
  - could have been much more serious
  - took two days to track down
  - need to be stricter on error checking in PR review

Hardware Bugs

ARDUPILOT
Versatile, Trusted, Open

We had multiple hardware triggered bugs

- most serious was I2C lockup bugs #16
  - caused watchdog
  - tracked down with noise injection hardware
- Floating CS pin in bootloader #13780
  - caused parameter reset on FRAM
  - very hard to track down (months)
- IMU failover bug #11720
  - triggered by hardware failure on one board type
  - didn’t properly validate previous fix

Future Work

ARDUPILOT
Versatile, Trusted, Open

Ideas for reducing bugs

- funding of bugmaster role (in progress)
- revitalise use of coverity and similar tools
- improve watchdog logging (especially over mavlink) (#13886)
- implement hardware regression suite?