What kind of special training do engineers working on mission-critical software receive? [closed]

I am a software engineer working on iOS apps which is software that is normally quite far from mission-critical industry.

However there have been a number of specific observations I and my colleagues made that made us wonder on what actually makes the practice of a programmer working on mission-critical systems different from what we iOS developers usually do.

Observation #1: "We are not building aircraft here, relax"

Over the years I remember quite a few of my colleagues saying to me "hey, we are not actually building aircraft here, relax" or "no need to test out those edge cases as they will never happen" or even better "no need to write tests we got it covered". Every time I hear that I wonder how the practice of those colleagues would actually change if they were to actually work on something critical.

Observation #2: "Would you fly on a plane if you knew that it is software is 100% Javascript?"

The point is not about safety of particular programming languages but rather about what constitues the skillset and practice of folks working in different programming language communities?

Observation #3: Terrac-25 and Mars Climate Orbiter incidents

https://ru.wikipedia.org/wiki/Therac-25 https://en.wikipedia.org/wiki/Mars_Climate_Orbiter

I wonder what if I would do given I and some of my colleagues from the above were working on these projects.

There are more observations but I'll keep these 3 as most representative.

So here are the questions:

1. What actually makes the difference between and iOS programmer and a programmer working on mission-critical software?
2. Where do the mission-critical software programmers receive their training and what do they study?
3. Any advice on where/how an application programmer (iOS, web) could learn more about the best programming practices used in mission-critical software?

The question has been closed here so I have posted a link to reddit: https://www.reddit.com/r/programming/comments/5iohue/what_kind_of_special_training_do_engineers/.

Similar question on Quora: https://www.quora.com/What-skills-does-a-software-engineer-need-to-work-on-the-safety-critical-mission-critical-software-industry#.

mission-critical

edited Dec 21 '16 at 9:55

asked Dec 16 '16 at 13:00

Stanislav Pankevich
3,370 4 32 74

deleted by High Performance Mark, Dalija Prasnikar, jezrael Jan 9 at 11:30

closed as too broad by Martijn Pieters ♦ Dec 17 '16 at 13:31

There are either too many possible answers, or good answers would be too long for this format. Please add details to narrow the answer set or to isolate an issue that can be answered in a few paragraphs.

If this question can be reworded to fit the rules in the help center, please edit your question.

5 I'm voting to close this question as off-topic because it is not about programming. Nor, before OP asks, is it a good place to ask an off-topic question and ask for recommendations for places where it would be on-topic. – High Performance Mark Dec 16 '16 at 13:02

1 First of all, most of the "mission critical" software is written in C (or, very few, C++). There are standards dictating you what language features to what extent you're allowed to use, for example MISRA-C (en.wikipedia.org/wiki/MISRA_C) (for the automobile industry), the NASA Programming Guidelines (lars-lab.jpl.nasa.gov/JPL_Coding_Standard_C.pdf) or the Cert Securecoding standard (securecoding.cert.org/confluence/display/c/…). Apart from that, testing, testing, testing. Did I already mentioned testing? – Leandros Dec 16 '16 at 15:31

5 Voting to reopen and move it to Software Engineering. – Euphoric Dec 17 '16 at 5:18

1 Martijn Pieters, I saw you put the topic on hold and suggested me to change my question to fit SO format. The point is that I like my question the way it is and don't want to change anything. It does not fit SO and SE, 1500 symbols to long for Quora, not the best choice for reddit. Are you saying that there is no site in SE family where this question could find its place? Where such question can be asked on internet finally?!! – Stanislav Pankevich Dec 17 '16 at 16:33

1 Closing questions like this is what destroys any remaining sense of community in SO. exprienced people would prefer to answer questions like this rather than simple questions like "how do I print to console". Why should experts hang around here when all the interesting questions get closed and there is a flood of basic questions? – Jonathan. Dec 22 '16 at 12:31

|

1 Answer

Where there is software that may impact the safety of humans there is a family of standards for different applications, derived from a parent standard IEC61508 (if you are Eurocentric). There is a history of how these standards emerged, going back to ISA84 and some of the German DIN standards and British EN standards.

Both hardware and software are addressed, as are methodologies and checking, validation, verification, testing and maintenance requirements. There are full life cycle requirements from concept though to decommissioning.

There are many books on the subject and people that specialise in areas such as aero, rail, auto, home appliances or industrial processing plants.

There are specialised qualifications eg Functional Safety Engineers who are formally recognised by organisations such as TUV and Exida after passing of exams.

This is a very brief and general description which only obliquely addresses part of your question, but I have given you enough to begin exploring on your own, it is a broad and complicated subject.

deleted Jan 9 at 11:30

answered Dec 16 '16 at 13:30

Gareth Smith
1 1

Gareth, thanks for the answer. Very interesting. – Stanislav Pankevich Dec 16 '16 at 14:25

1 In the US we have the FAA's DO-178 standard. – M. Dudley Dec 16 '16 at 17:32

1 When and how are those standards enforced? Is there some kind of "periodical" or "random" checks. Or is that all as "it doesn't violate the standard if you don't get caught". Considering the few issues with automotive software, all the involved codebases were one huge violation of all automotive standards. – Euphoric Dec 17 '16 at 5:20