STRENGTHENING SAFETY IN SOFTWARE ENGINEERING

Dr Leonard Peter Binamungu

Project Principal Investigator

TAIC-2022, 27TH OCTOBER 2022

Ariane 5 Rocket

Launch

37 seconds later

Ariane 5 Rocket

" The failure of Ariane 501 was caused by the complete loss of guidance and attitude information 37 seconds after start of the main engine ignition sequence (30 seconds after lift-off). This loss of information was due to specification and design errors in the software of the inertial reference system. The extensive reviews and tests carried out during the Ariane 5 development programme did not include adequate analysis and testing of the inertial reference system or of the complete flight control system, which could have detected the potential failure."

Board, I. (1996). Ariane 5 Flight 105 Inquiry Board Report. tech. rep., European Space Agency Press.

Boeing 737 Max

Sensor failure which led to disabling of entire control system

Healthcare

1,000 deaths per year in the English NHS are caused by bugs in computer systems

Thomas, M., & Thimbleby, H. (2018). Computer Bugs in Hospitals: An Unnoticed Killer.

3.6 A "Blundering nurse"?

Eighty year old Arsula Samson had a heart attack after she was given an overdose of potassium chloride. The *Daily Mail* paper reported the incident under the headline,

> "Mother-of-four dies after blundering nurse administers TEN times drug overdose." [49]

The nurse pressed the 100 mL per hour button instead of pressing the 10 mL per hour button, so setting the infusion pump to a rate ten times higher than intended. As we showed above, these sorts of error are easy to make and are hard to spot, especially if the infusion pump does nothing to help, such as blocking to wait for the user to confirm such a high dose for a dangerous drug.

The report goes on to say:

> No error was found with the infusion pump and investigators ruled the death was due to "individual, human error."

That "no error" was found with something does not mean it is bug free. It certainly does not mean it has no design problems! How are they sure? (We discussed above the inadequacy of testing; see

Others?

- Self-driving cars
- Robots
- Domain-specific ML software systems
- etc

Problem?

- Engineers lack knowledge and skills on developing safety-critical systems
- Safety-critical systems need specific process and techniques to be followed
- Not given appropriate attention they deserve in UG programs (All of Tanzania!)

Problem?

- The ICTC survey of 2021 identified acute skill gaps in several ICT specializations, including software engineering!

- The skill gaps were attributed to universities' curricula not being able to cope with the ever-changing nature of ICT

Proposed solution

- The project aims to develop a professional course on safety aspects in software systems
- To be delivered to software practitioners in Tanzania, especially those developing safety-critical systems

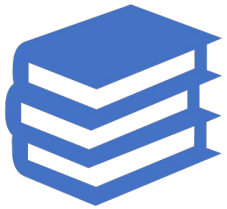
How will the project be conducted?

Collaborative

Involving stakeholders from

- Industry
- Academia

Expected results and delivery



Curriculum

Development of safety critical systems

A full-fledged professional course

Realistic and contextualized case studies

Hands on practice

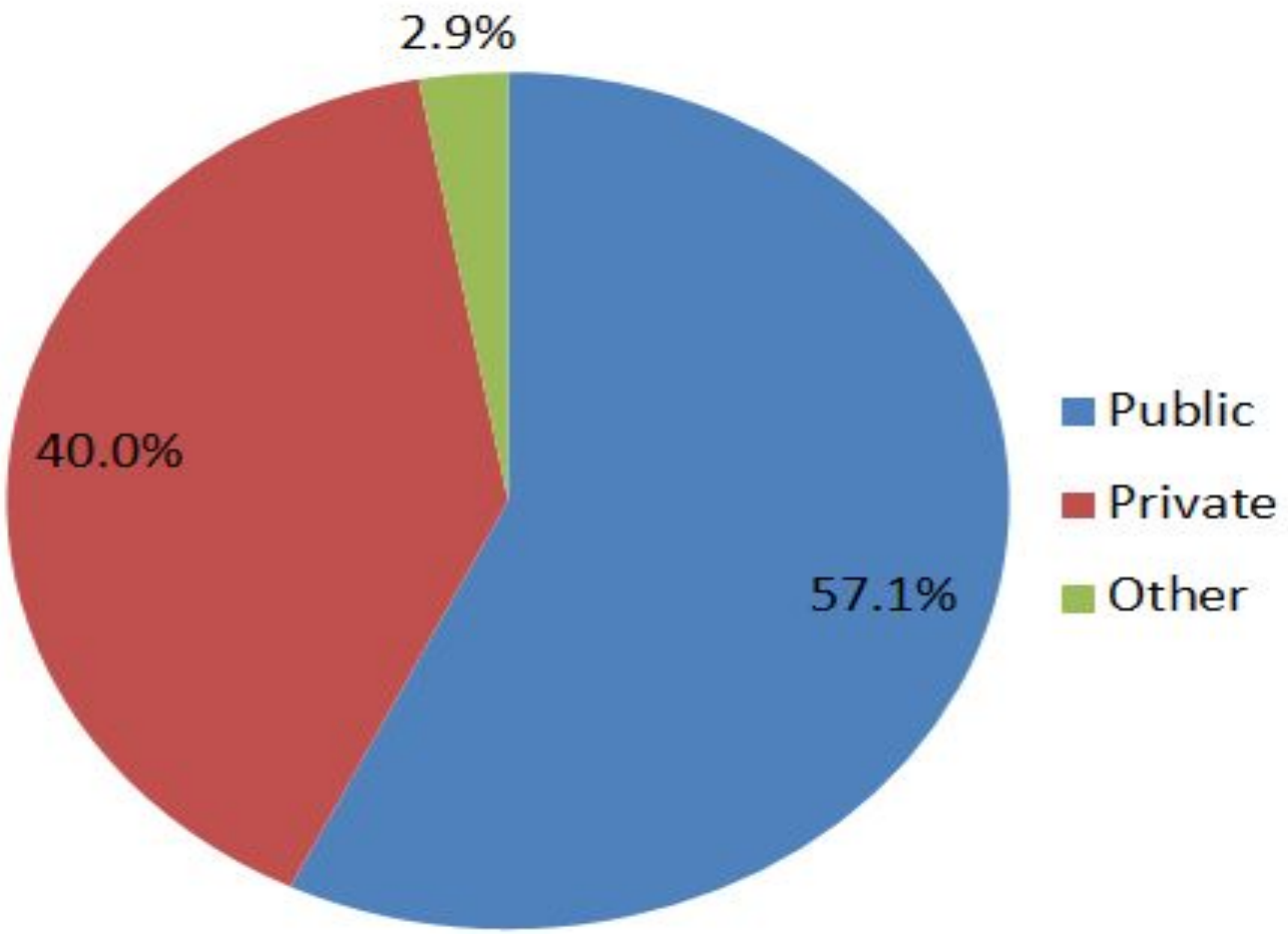
Mode of delivery

Face to face “free” course for 100 participants

Self-paced online course available at a “small” fee

“

How safe are we?



Awareness of software and functional safety

1 = No knowledge/skill

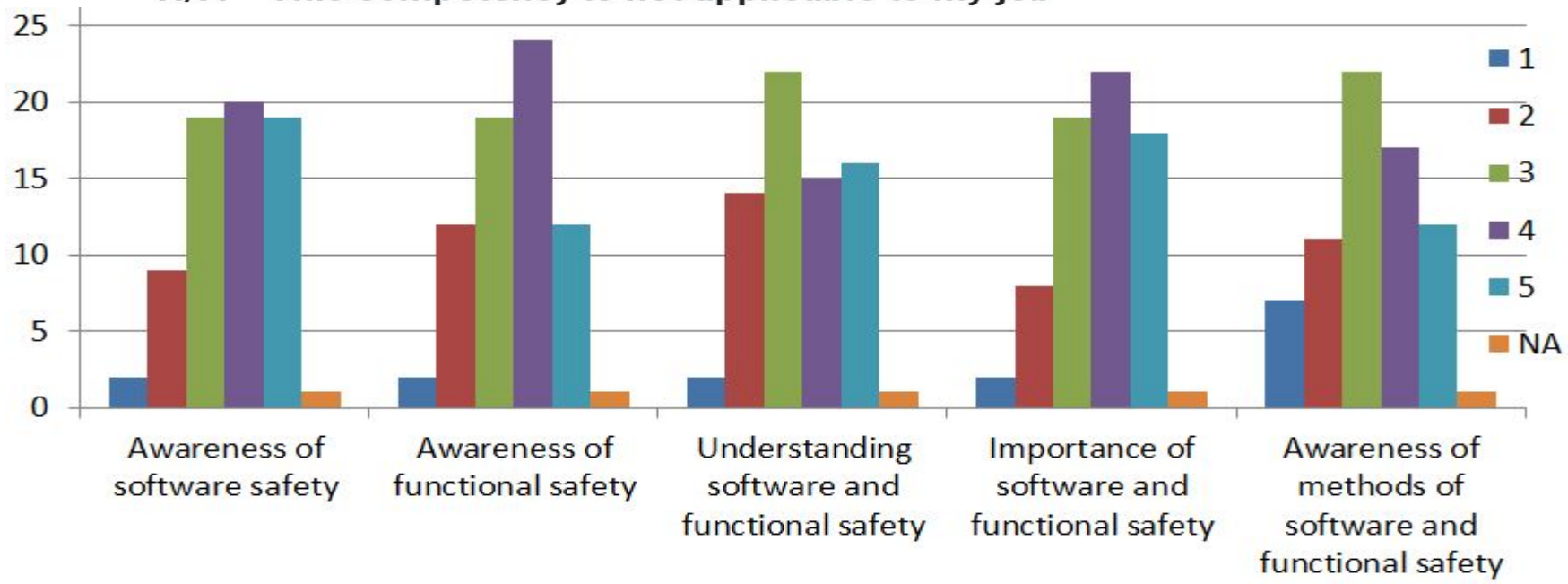
2 = A little knowledge/skill but considerable development required

3 = Some knowledge/skill, but development required

4 = Good level of knowledge/skill displayed, with a little development required

5 = Fully knowledgeable/skilled – no/very little development required

N/A = This competency is not applicable to my job



Safety competency knowledge/skills

1 = No knowledge/skill

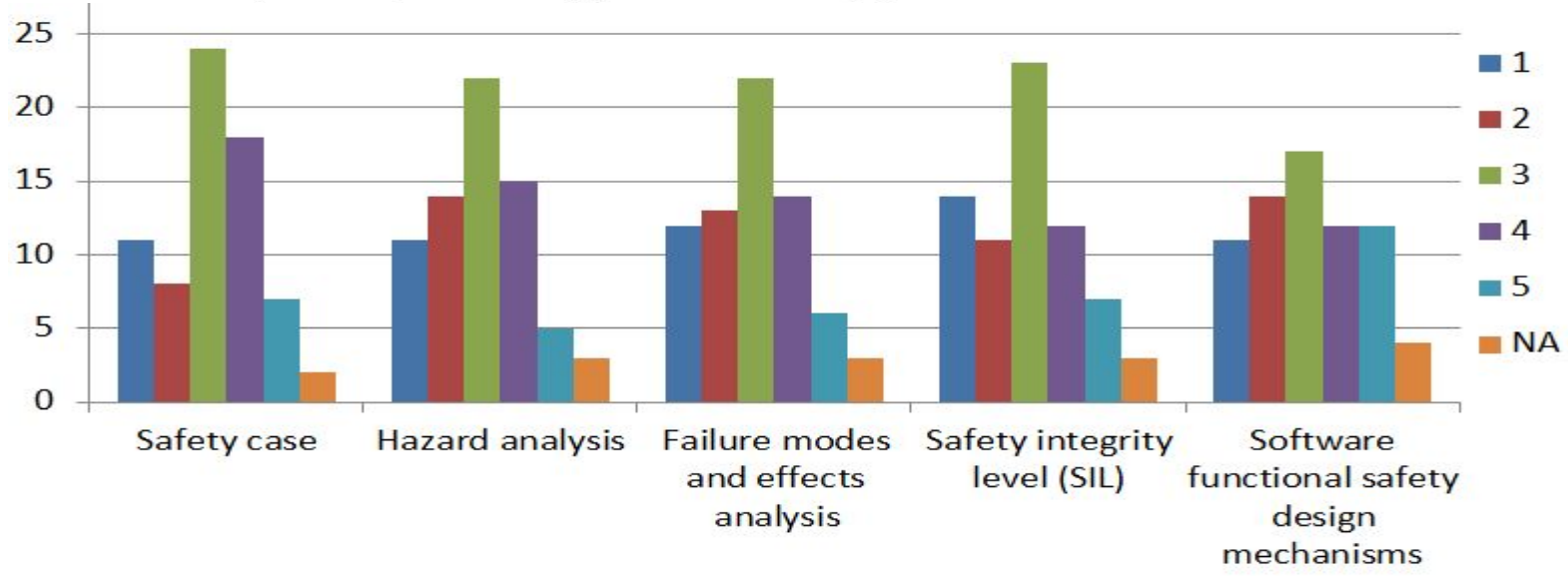
2 = A little knowledge/skill but considerable development required

3 = Some knowledge/skill, but development required

4 = Good level of knowledge/skill displayed, with a little development required

5 = Fully knowledgeable/skilled – no/very little development required

N/A = This competency is not applicable to my job



Awareness of safety standards

1 = No knowledge/skill

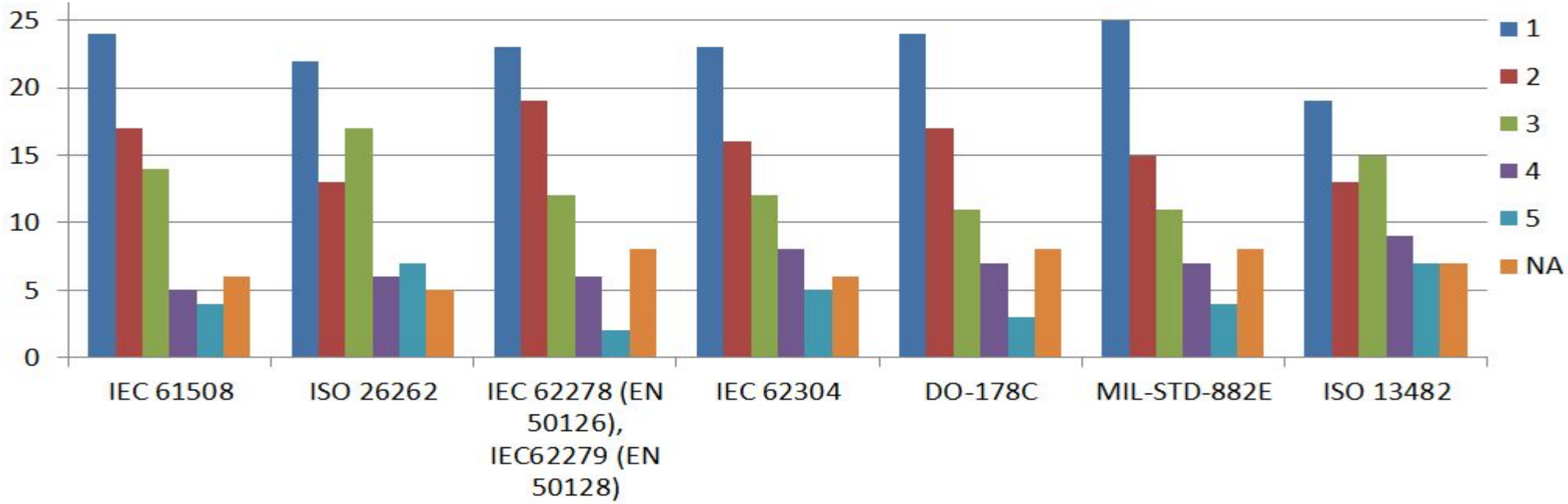
2 = A little knowledge/skill but considerable development required

3 = Some knowledge/skill, but development required

4 = Good level of knowledge/skill displayed, with a little development required

5 = Fully knowledgeable/skilled – no/very little development required

N/A = This competency is not applicable to my job



On s/w safety practices in Tz

*On behalf of the YY [organisation with interest in safety], we are really appreciated for the wonderful initiative on software safety. We will be more than glad if we are also involved in this research
*Software safety is rarely practiced, most developers base on functional implementation of the software and they don't care of safety
*More and more systems are being implemented with direct impact to human safety. Although not to a high degree, we should preempt systems that could be critical to human safety
*Tanzania is moving fast in terms of technology adaptation, software safety practice become crucial now and then. I think we as tech/software engineers need to consider this practice while developing software.
*It is still new concept in most organization. Most organization have been focusing on security of software rather than safety it is high time to bring on board this knowledge to organisations developers implementors
*Seem a good concept to include in IT courses even in engineering to promote awareness. In a length engagement on Dev works 20 years I have never come across such a concept
*Software safety and other practices have to be looked at practically not theoretically. There is a big gap between what academic theory and the practical part of things

Need for software safety training in Tz

*I believe this is a very ignored aspect in software development and to most developers and its a good movement and practice to initiate Software Safety training in Tanzania
*By priotizing safety training to Tanzanians, We may be able to identify, estimate and by so be able to prevent hazards
*The Government academic High level institutions should consider incorporate into curriculum
*Whenever the systems concern the safety of the users or equipment or environment, I suggest , the safety should be prioritized, and this is is possible if the systems development practitioners are trained well to identify safety issues and develop safety procedures to handle and improve the system safety
*There should be regular education about this issue to promote greater understanding among developers
*Seem a good concept to include in IT courses even no engineering to promote awareness. In a length engagement on Dev works 20 years I have never come across such a concept
*I strongly agree that there is a need of safety training in Tanzania.
*I don't recognise most of the terms used it might lead to wrong information
*I am not recommending teaching people about software security while they even don't know coding well. Let's *choose the good choice... otherwise we are teaching them fearing


Thank You
Merci
Obrigado
Dyakuyu
Arigato
Salamat
Spasibo
Juspaxar
Dank Je
Kiitos
Grazie
Asante
Vinaka
Dankon
Mochchakkeram
Multumesc
Maake
Mamana
Terma Kasih
Kia Ora
Chokrane
Nirringrazzjak
Cam on ban
Raibh Maith Agat
Matur Nuwun
Welalin
Ua Tsaug Rau Koj
Matondo

Discussion