

“Dependability aspects: reliability and safety and their application in Mobile Robotics”

Dr. Roberto A. Valdivia Beuteslpacher

Review by Roberto Hoyos Morales

February the 3rd, 2005

1. Main Ideas

The trend in mobile robotics is to prevent and tolerate faults. A system has to have “dependability”, that is, the trustworthiness of a system, so that it can be accepted by humans and controlled safety.

There are many kinds of faults or errors caused by hardware or software, but most important, operational failures, caused by human intervention, are the vast majority.

There are heuristics followed to obtain dependability on systems, and among them there is the redundancy of components, so that when one fails for any reason, other components can keep the system functioning appropriately. Also, we can react to errors in a static way (hide failures) or dynamically (detecting and repairing errors).

A mistake/error/failure could cause losses, and in the most extreme cases, human lives to be in danger. To avoid this there must be reliability in systems. The way to implement dependability is still a subject of debate, because its three-leveled architecture offers many possibilities.

2. Results and Conclusions by the speaker

Failures are caused by three main actors: hardware (mostly because of design errors, manufacture errors and aging), software (mistakes in the specification), operational (human operators commit mistakes).

Security can be seen in two aspects: the one that has to provide safeguard against intruders; the second, the ability of a system to function without a catastrophic failure.

The cost of creating more secure and dependable systems (redundancy in design, more tests) grows exponentially.

Computers may not be reliable, but humans are the best reliable of them all. If we have that in mind we can acknowledge the dimension of the task to undertake in creating more secure systems.

Investment in reliability will increase till the point when the cost of this exceeds the cost of errors. That's the economical upper bound for this enterprise.

3. Discussion

Two major questions arise from the lecture given, both have to do with humans: If humans are the biggest cause of errors, can we create systems that depend less and less from humans? This seems like a plausible scenario: As our tasks become more and more complex, will we be able to take decisions intelligently? Is not the trend to reduce human intervention?

The second concern is an old debate about the value of life. Failures in systems (especially in mobile robotics) can cause human casualties. So, if investment will not increase beyond the cost of those errors, under which basis do we value human life?

Lastly I will like to debate the statement that says that the cost of investment in preventing errors shall never increase the cost of those errors. This is a tricky question. Personally I think that as long as the systems grow in complexity, errors will just be unacceptable. I think we must perfection the systems no matter the cost; for other applications will be built upon what we have.

4. Conclusions

Human errors are the most frequent and the most costly, and cannot be 'tracked' and 'fixed' like the hardware and software counterparts.

The concern towards failure-proof systems in mobile robotics has a definite support on human safety, not only economical issues.

Investment in these areas will never be costly enough to lessen in human safety. Mobile robotics is not purely software, and every effort must be undertaken to assure dependability.