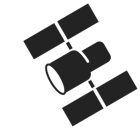
Lesson 2

Software specifications. Formal methods

In this lesson we will talk about:
Software specifications, Formal methods,
Software verification and validation

”Todays software has grown by evolution, not by intelligent design”

— *Leslie Lamport*



Space Instruments
Hubble Telescope

Military drones, Mars Curiosity Rover

Modern airplanes
Boeing Dreamliner

F35 Lightning II

Computer Software
Windows, Debian, Office

Apple macOS

Automotive
BMW, Mercedes, Tesla

Our software is getting more and more **complex**, **buggy** and **difficult** to maintain.


GLOBAL OUTAGE
2024 CrowdStrike
2
4
Clear Channel


:(
Your PC ran into a problem and needs to restart. We're jus
some error info, and then we'll restart for you.
100% complete
For more information about this issue and possible fixes, visit https://www.windows.com/st
Women
Gates B62 to B81
Men
Family
B63
Gate

2024 CrowdStrike-related IT outages

Article Talk

From Wikipedia, the free encyclopedia

On 19 July 2024, American cybersecurity company CrowdStrike distributed a faulty update to its Falcon Sensor security software that caused widespread problems with Microsoft Windows computers running the software. As a result, roughly 8.5 million systems crashed and were unable to properly restart[1] in what has been called the largest outage in the history of information technology[2] and "historic in scale".[3]

The outage disrupted daily life, businesses, and governments around the world. Many industries were affected—airlines, airports, banks, hotels, hospitals, manufacturing, stock markets, broadcasting, gas stations, retail stores, and more—as were governmental services, such as emergency services and websites.[4][5] The worldwide financial damage has been estimated to be at least US$10 billion.[6]

What can we do about it?

Start with a **smart design** at the specification level

Software Specifications

What is a computer specification?

A **specification** often refers to a set of documented requirements to be satisfied by a material, design, product, or service.[1] A specification is often a type of technical standard.

There are different types of technical or engineering specifications (specs), and the term is used differently in different technical contexts. They often refer to particular documents, and/or particular information within them. The word *specification* is broadly defined as "to state explicitly or in detail" or "to be specific".

A **requirement specification** is a documented requirement, or set of documented requirements, to be satisfied by a given material, design, product, service, etc.[1] It is a common early part of engineering design and product development processes in many fields.

A **functional specification** is a kind of requirement specification, and may show functional block diagrams. [*citation needed*]

What is a software specification?

A **Software Specification** is a written description of what a system is supposed to do.

Software specification

helps us understand our software. Its a good idea to understand a system before building it, so its a good idea to write a specification of a program before implementing it.

But how can we write the specification?

- English? Finnish? Chinese? Words or sentences
- Graphical diagrams? Drawing?
- Programmable? Coding?

But all these are imprecise. How can we be precise? What does it mean to be precise?

Imprecision can lead to **ERRORS!**

Precise specifications

Its hard to be precise using English or other language. Thats why in science and engineering fields precise specifications have adopted basic maths to describe the specifications.