Universität Bremen

Systeme hoher Sicherheit und Qualität

WS 2019/2020

Lecture 1:
Introduction and Notions of Quality

Christoph Lüth, Dieter Hutter, Jan Peleska

Organisatorisches

Generelles

- Einführungsvorlesung zum Masterprofil S & Q
- 6 ETCS-Punkte
- Vorlesung:
  - Dienstag 12 – 14 Uhr (MZH 1110)
- Übung:
  - Donnerstag 16 – 18 Uhr (MZH 4140)
- Veranstalter:
  - Christoph Lüth `<clueth@uni-bremen.de>`, MZH 4186, Tel. 59830
  - Helmar Hutschenreuter `<hutschen@uni-bremen.de>`
- Material (Folien, Artikel, Übungsblätter) auf der Homepage:
  http://www.informatik.uni-bremen.de/~clueth/lehre/ssq.ws19

Vorlesung

- Foliensätze als **Kernmaterial**
  - Sind auf Englisch (Notationen!)
  - Nach der Vorlesung auf der Homepage verfügbar
- Ausgewählte Fachartikel als **Zusatzmaterial**
  - Auf der Homepage verlinkt (ggf. in StudIP)
- Bücher nur für einzelne Teile der Vorlesung verfügbar:
  - Nancy Leveson: Engineering a Safer World
  - Ericson: Hazard Analysis Techniques for System Safety
  - Nilson, Nilson: Principles of Program Analysis
  - Winskel: The Formal Semantics of Programming Languages
- Zum weiteren Stöbern:
  - Wird im Verlauf der Vorlesung bekannt gegeben

Übungen

- Übungsblätter:
  - „Leichtgewichte“ Übungsblätter, die in der Übung bearbeitet und schnell korrigiert werden können.
  - Übungsblätter vertiefen Vorlesungsstoff.
  - Bewertung gibt schnell Feedback.
- Übungsbetrieb:
  - Gruppen bis zu 3 StudentInnen
  - Ausgabe der Übungsblätter Dienstag in der Übung
    - Zeitgleich auf der Homepage
    - Erstes Übungsblatt: diese Woche (17.10.2019)
  - Bearbeitung: während der Übung
  - Abgabe: bis Donnerstag abend

Prüfungsform

- Bewertung der Übungen:
  - A (sehr gut (1.0) – nichts zu meckern, nur wenige Fehler)
  - B (gut (2.0) – kleine Fehler, im großen und ganzen gut)
  - C (befriedigend (3.0) – größere Fehler oder Mängel)
  - Nicht bearbeitet (oder zu viele Fehler)
- Prüfungsleistung:
  - Teilnahme am Übungsbetrieb (20%)
    - Übungen keine Voraussetzung
  - Mündliche Prüfung am Ende des Semesters (80%)
    - Einzelprüfung, ca. 20- 30 Minuten

Ziel der Vorlesung

- Methoden und Techniken zur Entwicklung sicherheitskritischer Systeme
- Überblick über verschiedene Mechanismen
  d.h. auch Überblick über vertiefende Veranstaltungen
  - Theorie reaktiver Systeme
  - Grundlagen der Sicherheitsanalyse und des Designs
  - Formale Methoden der Softwaretechnik
  - Einführung in die Kryptographie
  - Qualitätsorientierter Systementwurf
  - Test von Schaltungen und Systemen
  - Informationssicherheit -- Prozesse und Systeme
- Verschiedene Dimensionen
  - Hardware vs. Software
  - Security vs. Safety
  - Qualität der Garantien

Overview

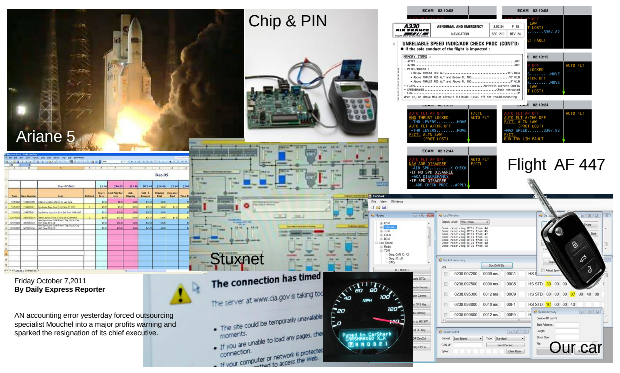
Objectives

- This is an introductory lecture for the topics

  Quality – Safety – Security

- Bird's eye view of everything relevant related to the development of systems of high quality, high safety or high security.
- The lecture reflects the fundamentals of the research focus quality, safety & security at the department of Mathematics and Computer Science (FB3) at the University of Bremen. This is one of the three focal points of computer science at FB3, the other two being Digital Media and Artificial Intelligence, Robotics & Cognition.
- This lecture is read jointly (and in turns) by Dieter Hutter, Christoph Lüth, and Jan Peleska.
- The choice of material in each semester reflects personal preferences.

Why bother with Quality, Safety, and Security ?


Ariane 5
Chip & PIN
Flight AF 447
Stuxnet
Friday October 7,2011
By Daily Express Reporter
AN accounting error yesterday forced outsourcing specialist Mouchel into a major profits warning and sparked the resignation of its chief executive.
The connection has timed
Our car

Ariane 5

- Ariane 5 exploded on its virgin flight (Ariane Flight 501) on 4.6.1996.

- How could that happen?

What Went Wrong With Ariane Flight 501?

(1) Self-destruction due to instability; — The Accident
(2) Instability due to wrong steering movements (rudder);
(3) On-board computer tried to compensate for (assumed) wrong trajectory;
(4) Trajectory was calculated wrongly because own position was wrong;
(5) Own position was wrong because positioning system had crashed;
(6) Positioning system had crashed because transmission of sensor data to ground control failed with integer overflow; — The root cause
(7) Integer overflow occurred because values were too high;
(8) Values were too high because positioning system was integrated unchanged from predecessor model, Ariane-4;
(9) This assumption was not documented because it was satisfied tacitly with Ariane-4.
(10) Positioning system was redundant, but both systems failed (systematic error).
(11) Transmission of data to ground control also not necessary.

Railway Accident in Bad Aibling 2016

- Two trains collided on a single-track line close to Bad Aibling

- Human error ?
  - cf. Nancy Leveson: Engineering a Safer World

Recent Crashes of Boeing 737 MAX

- Lion Air flight JT 610 29.10.2018 06:33 near Jakarta
- Ethopian Airlines flight ET 302 10.03.2019 08:44 near Addis Ababa
- Accidents:
  - New planes in perfect weather fly into the ground.
- Causes:
  - Manoeuvring Characteristics Augmentation System (MCAS) automatically pushes down nose of aircrafts in risk of stall.
  - What happens when sensor readings are faulty?
  - MCAS can be switched off, but not permanently – warning lights and permanent switch off are premium features.
  - Pilots not trained with MCAS.
  - See here: https://www.bbc.com/news/world-africa-47553174
  - MCAS introduced for cost reasons.
- Accidents caused by push for low costs, poor user interface and sloppy certification process.
- See also: Air France flight AF 447

What is Safety and Security?

Safety:

- product achieves acceptable levels of risk or harm to people, business, software, property or the environment in a specified context of use
- Threats from "inside"
  - Avoid malfunction of a system
  - E.g. planes, cars, railways
- Threats from "outside"
  - Protect product against force majeure ("acts of god")
  - E.g. Lightening, storm, floods, earthquake, fatigue of material, loss of power

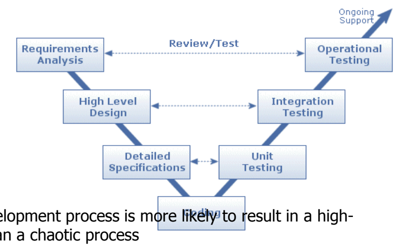
What is Safety and Security?

Security:

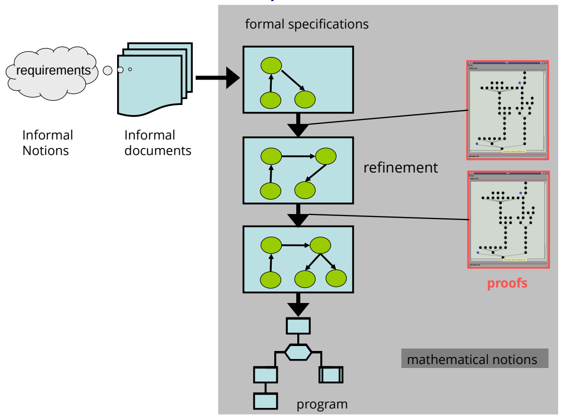
- Product is protected against potential attacks from people, environment etc.
- Threats from "outside"
  - Analyze and counteract the abilities of an attacker
- Threats from "inside"
  - Monitor activities of own personnel:
  - Selling of sensitive company data
  - Insertion of Trojans during HW/SW design
- In this context: "cybersecurity" (not physical security)

Software Development Models

- Definition of software development process and documents
- Examples:
  - Waterfall Model
  - V-Model
  - Model-Driven Architectures
  - Agile Development
- Motivation:
  - A well-defined development process is more likely to result in a high-quality product than a chaotic process
  - "Process quality ensures product quality"



Formal Software Development



Verification and Validation (V&V)

- **Verification**: have we built the system right?
  - i.e. correct with respect to a reference artefact
    - specification document
    - reference system
    - model
- **Validation**: have we built the right system?
  - i.e. effective (or adequate) for its intended operation?

Korrektheit

Wirksamkeit

V&V Methods

- **Testing**
  - Test case generation, black- vs. white box
  - Hardware-in-the-loop testing: integrated HW/SW system is tested
  - Software-in-the-loop testing: only software is tested
  - Program runs using symbolic values
- **Simulation**
  - An executable model is tested with respect to specific properties
  - This is also called Model-in-the-Loop Test
- Static/dynamic **program analysis**
  - Dependency graphs, flow analysis
  - Symbolic evaluation
- **Model checking**
  - Automatic proof by reduction to finite state problem
- **Formal Verification**
  - Symbolic proof of program properties

Where are we?

Concepts of Quality

What is Quality?

- Quality is the collection of its characteristic properties
- Quality model: decomposes the high-level definition by associating attributes (also called characteristics, factors, or **criteria**) to the quality conception
- Quality **indicators** associate **metric values** with **quality criteria**, expressing "how well" the criteria have been fulfilled by the process or product.
  - The idea is that to **measure** quality, with the aim of continuously **improving** it.
  - Leads to **quality management** (TQM, Kaizen)

Quality Criteria: Different „Dimensions" of Quality

- For the development of artifacts quality criteria can be measured with respect to the
  - development process (**process quality**)
  - final product (**product quality**)
- Another dimension for structuring quality conceptions is
  - **Correctness**: the consistency with the product and its associated requirements specifications
  - **Effectiveness**: the suitability of the product for its intended purpose

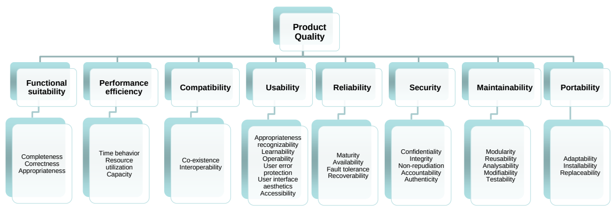
Quality Criteria (cont.)

- A third dimension structures quality according to product properties:
  - **Functional properties**: the specified services to be delivered to the users
  - **Structural properties**: architecture, interfaces, deployment, control structures
  - **Non-functional properties**: usability, safety, reliability, availability, security, maintainability, guaranteed worst-case execution time (WCET), costs, absence of run-time errors, …

Quality (ISO/IEC 25010/12)

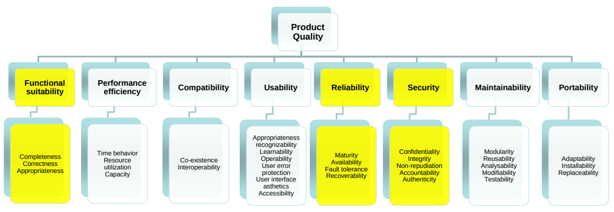
- "Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models"
  - Quality model framework (replaces the older ISO/IEC 9126)
- Product quality model
  - Categorizes system/software product quality properties
- Quality in use model
  - Defines characteristics related to outcomes of interaction with a system
  - Also known as „end user experience" („UX")
- Quality of data model
  - Categorizes data quality attributes

Product Quality Model


Product Quality
Functional suitability
Performance efficiency
Compatibility
Usability
Reliability
Security
Maintainability
Portability
Completeness Correctness Appropriateness
Time behavior Resource utilization Capacity
Co-existence Interoperability
Appropriateness recognizability Learnability Operability User error protection User interface aesthetics Accessibility
Maturity Availability Fault tolerance Recoverability
Confidentiality Integrity Non-repudiation Accountability Authenticity
Modularity Reusability Analysability Modifiability Testability
Adaptability Installability Replaceability

Source: ISO/IEC FDIS 25010

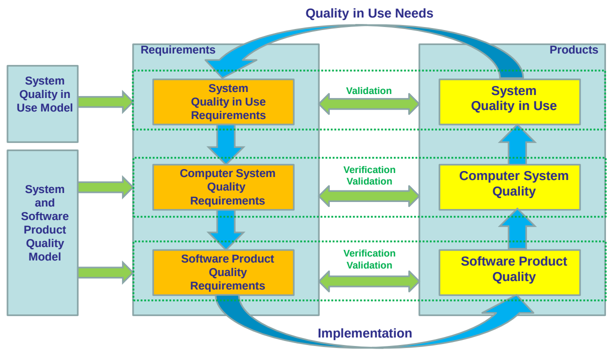
Our Focus of Interest


Product Quality
Functional suitability
Performance efficiency
Compatibility
Usability
Reliability
Security
Maintainability
Portability
Completeness Correctness Appropriateness
Time behavior Resource utilization Capacity
Co-existence Interoperability
Appropriateness recognizability Learnability Operability User error protection User interface asthetics Accessibility
Maturity Availability Fault tolerance Recoverability
Confidentiality Integrity Non-repudiation Accountability Authenticity
Modularity Reusability Analysability Modifiability Testability
Adaptability Installability Replaceability

How can we „guarantee" safety and security ?

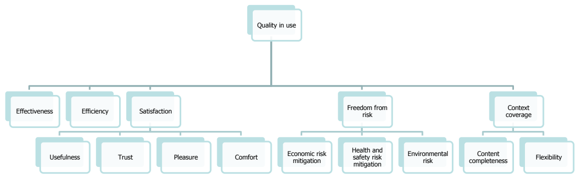
Source: ISO/IEC FDIS 25010

System Quality Life Cycle Model



Source: ISO/IEC FDIS 25010

Quality in Use Model



Other Norms and Standards

- ISO 9001 (DIN ISO 9000-4):
  - Standardizes definition and supporting principles necessary for a quality system to ensure products meet requirements
  - "Meta-Standard"
- CMM (Capability Maturity Model), Spice (ISO 15504)
  - Standardizes maturity of development process
  - Level 1 (initial): Ad-hoc
  - Level 2 (repeatable): process dependent on individuals
  - Level 3 (defined): process defined & institutionalized
  - Level 4 (managed): measured process
  - Level 5 (optimizing): improvement feed back into process

Summary

- Quality
  - collection of characteristic properties
  - quality indicators measuring quality criteria
- Relevant aspects of quality here
  - Functional suitability
  - Reliability
  - Security
- Next week
  - Concepts of Safety, Legal Requirements, Certification