Systeme hoher Sicherheit und Qualität
Universität Bremen, WS 2017/2018

Lecture 1: Introduction and Notions of Quality

Christoph Lüth, Dieter Hutter, Jan Peleska

Organisatorisches

Generelles

- Einführungsvorlesung zum Masterprofil S & Q
- 6 ETCS-Punkte
- Vorlesung:
  - Montag 12 – 14 Uhr (MZH 1110)
- Übung:
  - Dienstag 12 – 14 Uhr (MZH 1110)
- Material (Folien, Artikel, Übungsblätter) auf der Homepage:

  http://www.informatik.uni-bremen.de/~cxl/lehre/ssq.ws17

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: nächste Woche (24.10.2017)
  - Bearbeitung: während der Übung
  - Abgabe: bis Dienstag 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

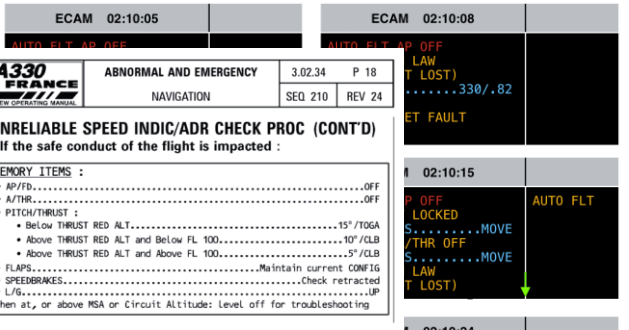
- Bird's eye view of everything relevant related to the development of systems of high quality, high safety or high security.

- 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.

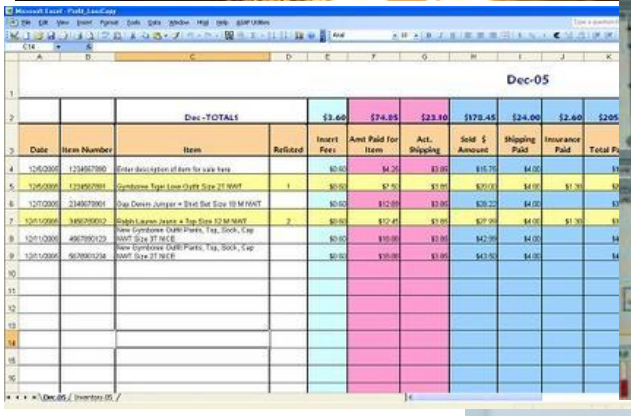
- This lecture is read jointly (and in turns) by Dieter Hutter, Christoph Lüth, and Jan Peleska.

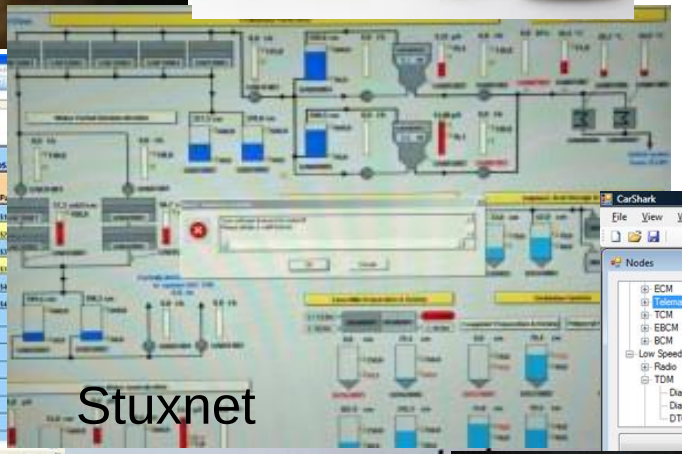
- The choice of material in each semester reflects personal preferences.

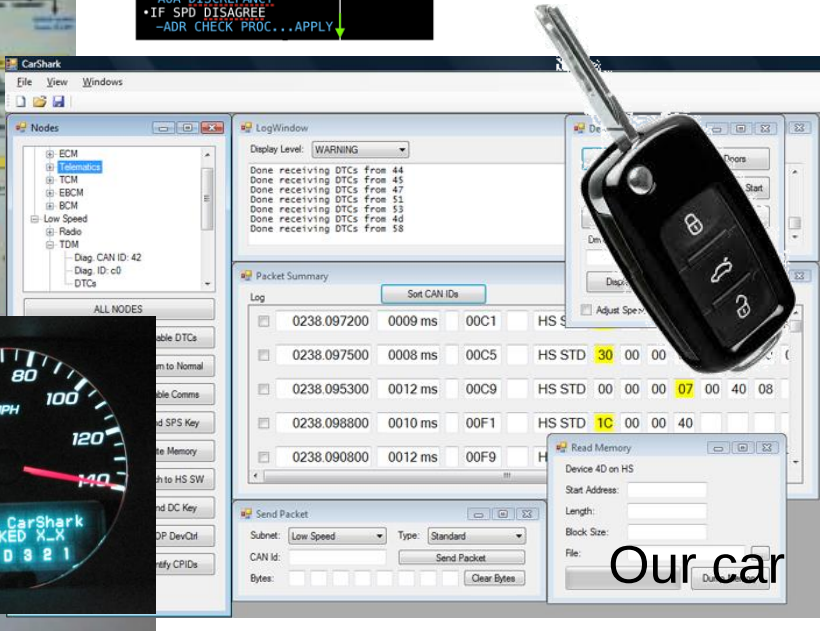
Why bother with Quality, Safety, and Security ?



Flight AF 447

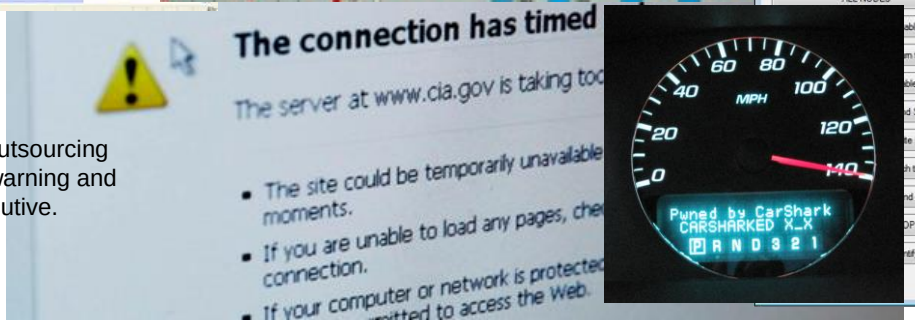






Friday October 7,2011
By Daily Express Reporter

AN accounting error yesterday forced outsourcing specialist Mouchel into a major profits warning and sparked the resignation of its chief executive.



Ariane 5

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

- How could that happen?

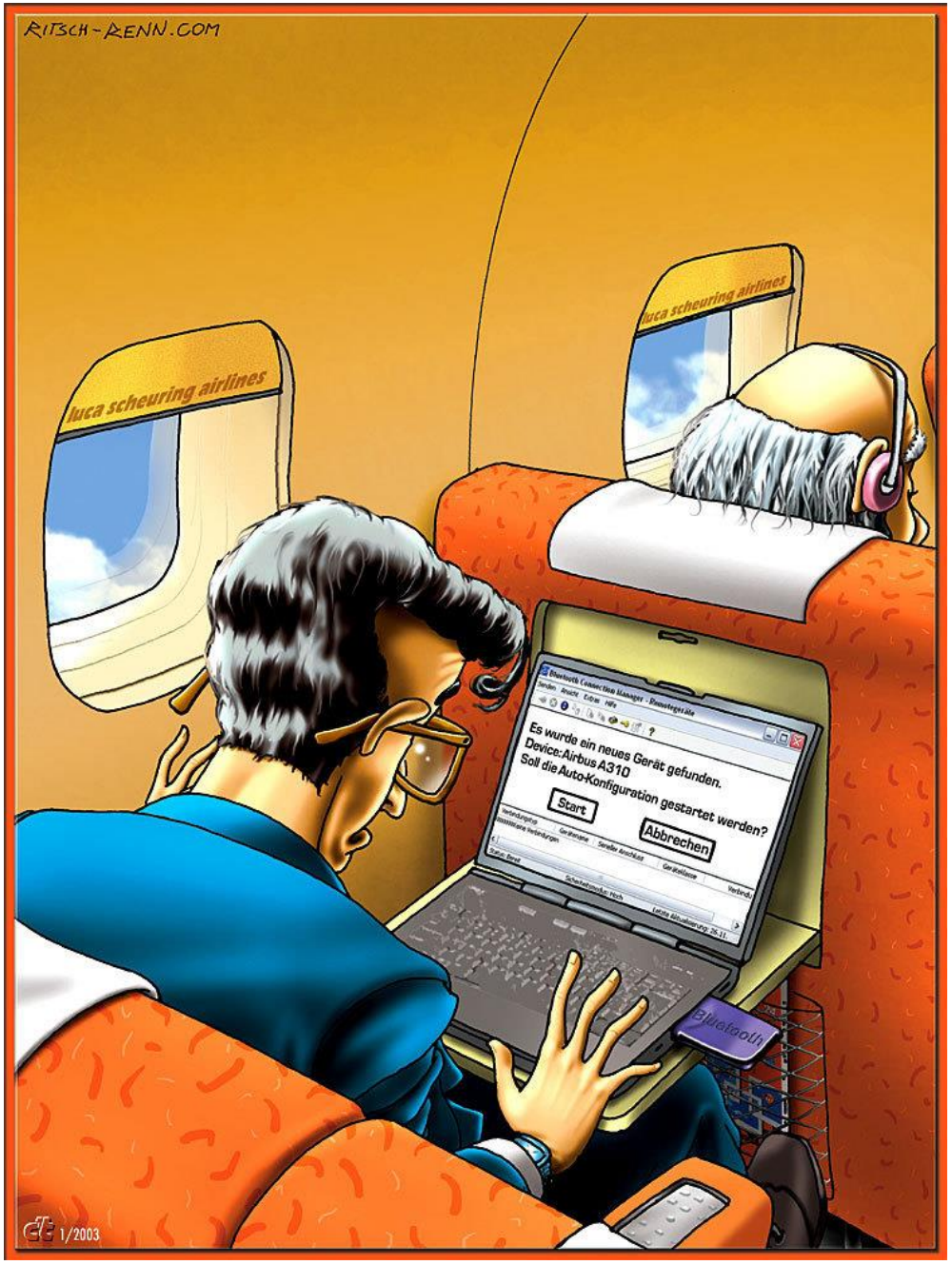
What Went Wrong With Ariane Flight 501?

(1) Self-destruction due to instability;
(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;
(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



from: c't 1/2003 (Heise Verlag)

Mail Online

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money | Vi

Latest Headlines | *Science* | Pictures

Planes are at risk of cyber attack through their Wi-Fi and entertainment systems, says hacker, prompting fears for aircraft security

- **Security researcher Ruben Santamarta says he has figured out how to hack the satellite communications on passenger jets through their WiFi**
- **Communications can also be hacked through inflight entertainment systems**
- **Santamarta is scheduled to lay out the technical details of his research at this week's Black Hat hacking conference in Las Vegas**

By REUTERS

PUBLISHED: 19:44 GMT, 4 August 2014 | **UPDATED:** 10:57 GMT, 5 August 2014

from: Daily Mail Aug. 2014

Frisch auf den Tisch, ein Evergreen zum Thema „Sicherheitslücken in täglich genutzten Protokollen…“

Heise Security, 17.10.2017

What is Safety and Security?

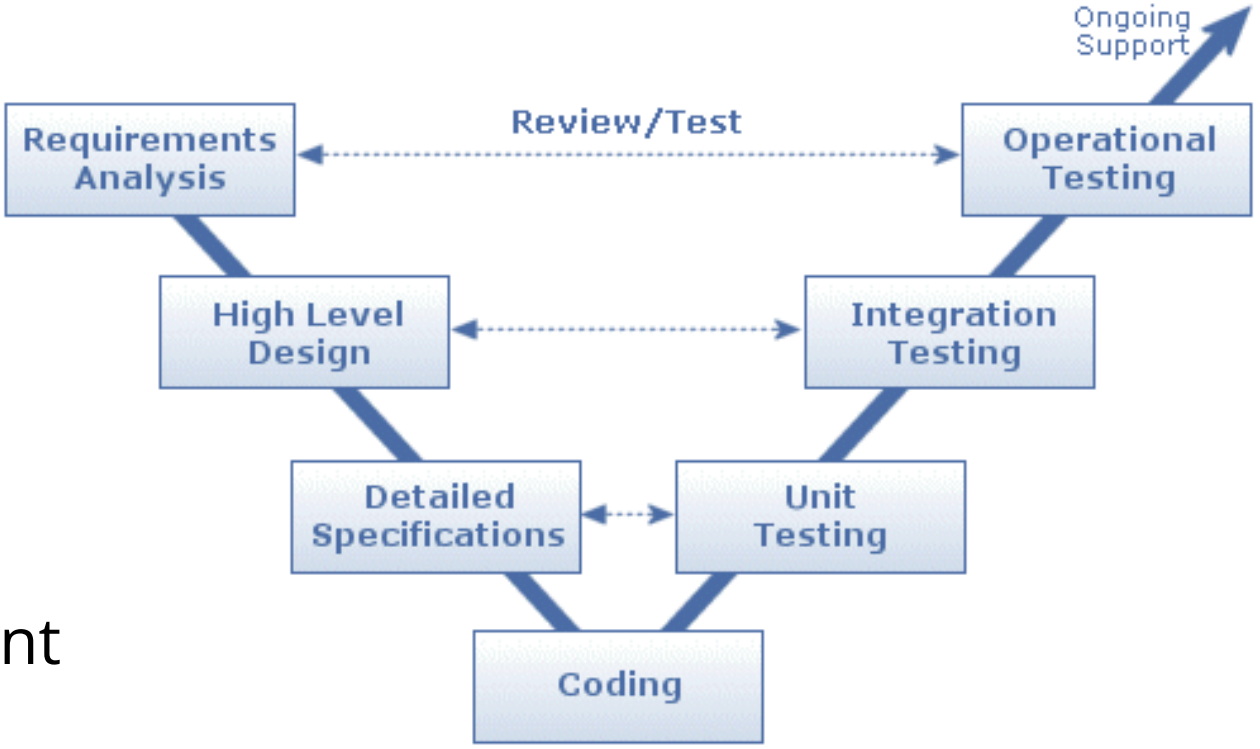
- Safety:
  - product achieves acceptable levels of risk or harm to people, business, software, property or the environment in a specified context of use
  - Threats from “inside”
    - Avoid malfunction of a system (e.g. planes, cars, railways…)

- Security:
  - Product is protected against potential attacks from people, environment etc.
  - Threats from “outside”
    - Analyze and counteract the abilities of an attacker

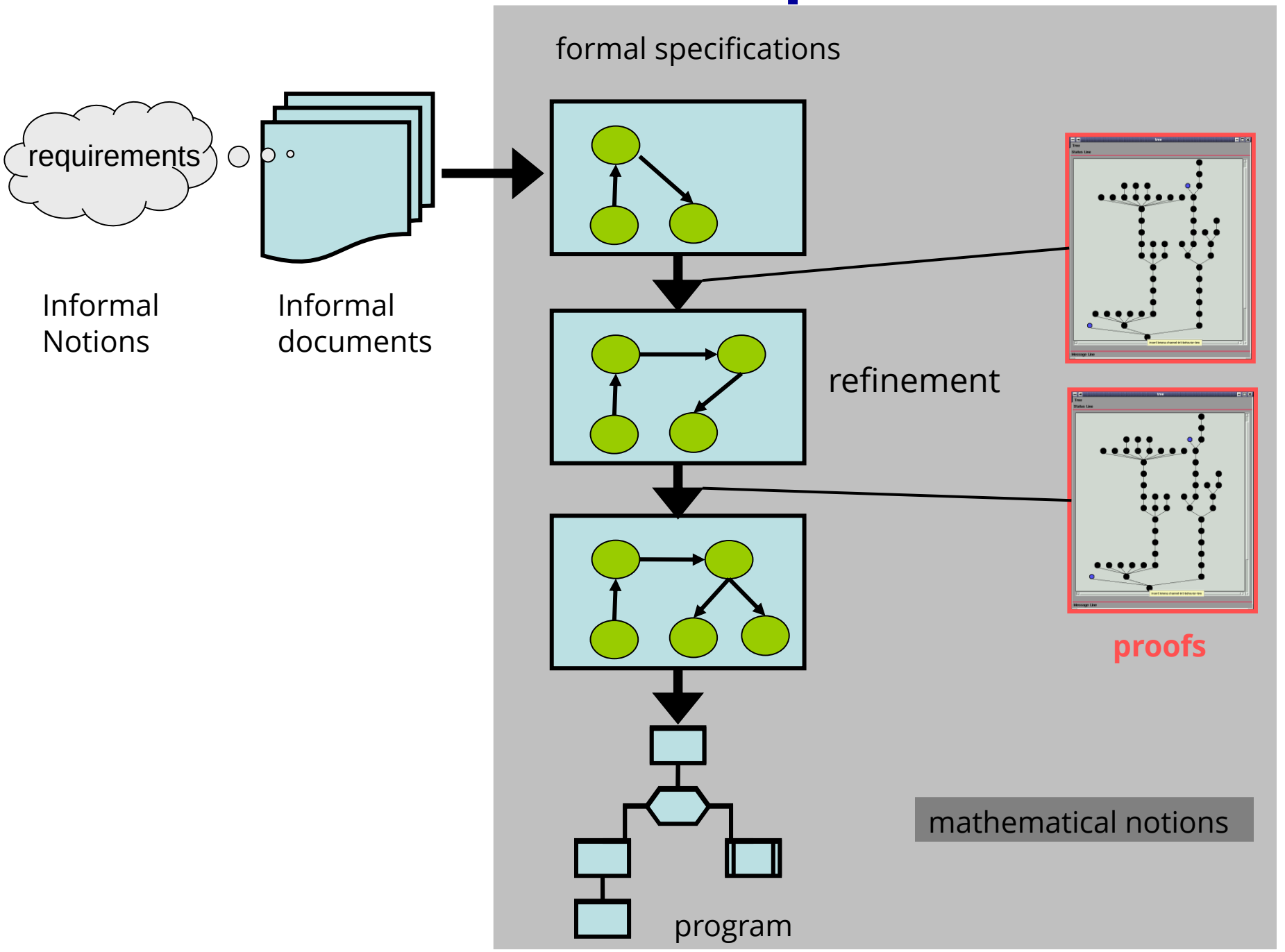
Software Development Models

- Definition of software development process and documents

- Examples:
  - Waterfall Model
  - V-Model
  - Model-Driven Architectures
  - Agile Development



Formal Software Development



Verification and Validation

- **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. adequate for its intended operation?

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?

- 01: Concepts of Quality
- 02: Legal Requirements: Norms and Standards
- 03: The Software Development Process
- 04: Hazard Analysis
- 05: High-Level Design with SysML
- 06: Formal Modelling with OCL
- 07: Testing
- 08: Static Program Analysis
- 09-10: Software Verification
- 11-12: Model Checking
- 13: Conclusions

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.

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

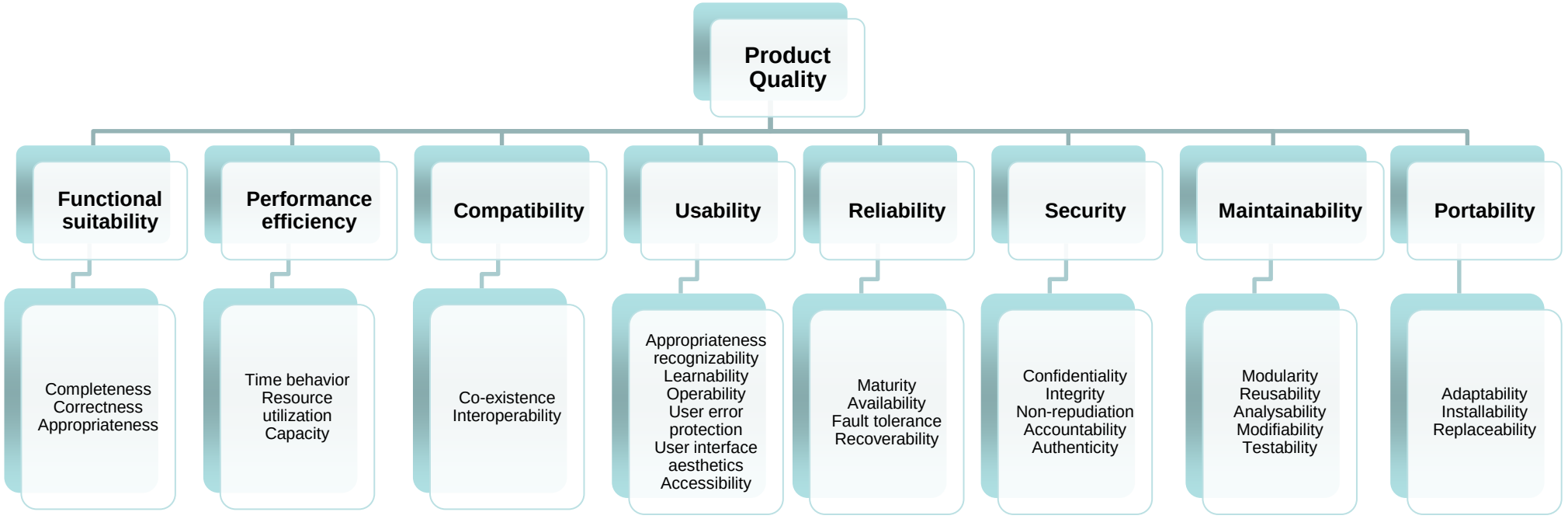
Quality Criteria (cont.)

- 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)

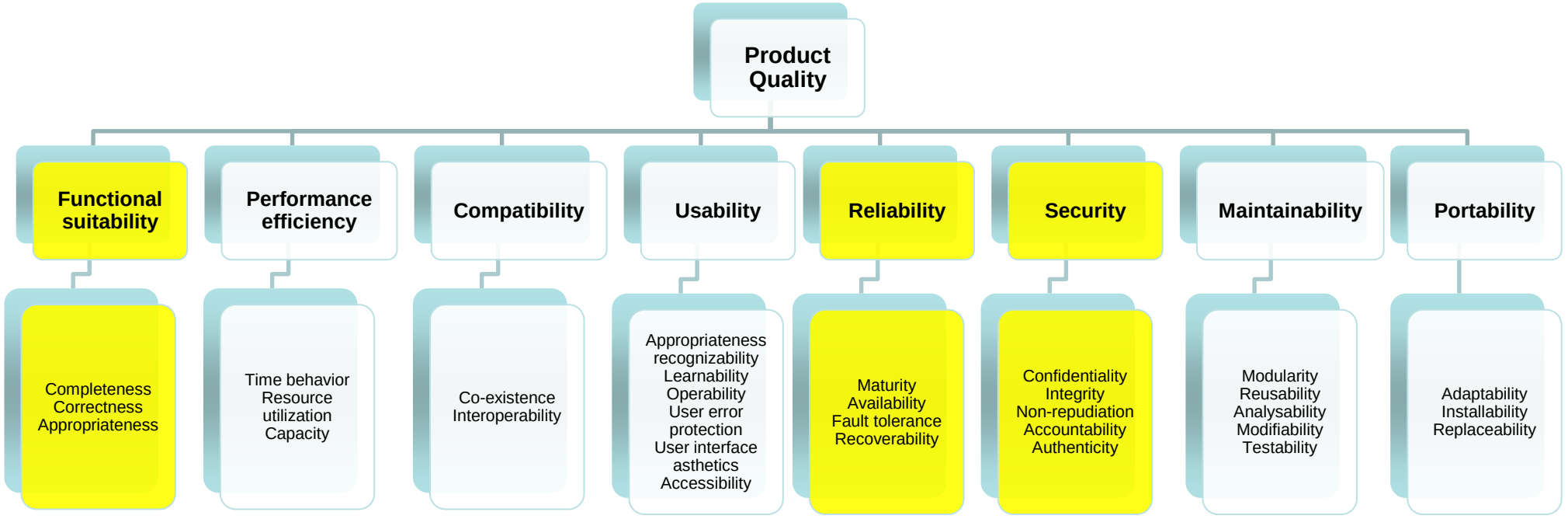
- "Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models"
  - Quality model framework (replaces the older ISO/IEC 9126)
- Product quality model
  - Categorizes system/software product quality properties
- Quality in use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

Product Quality Model



Source: ISO/IEC FDIS 25010

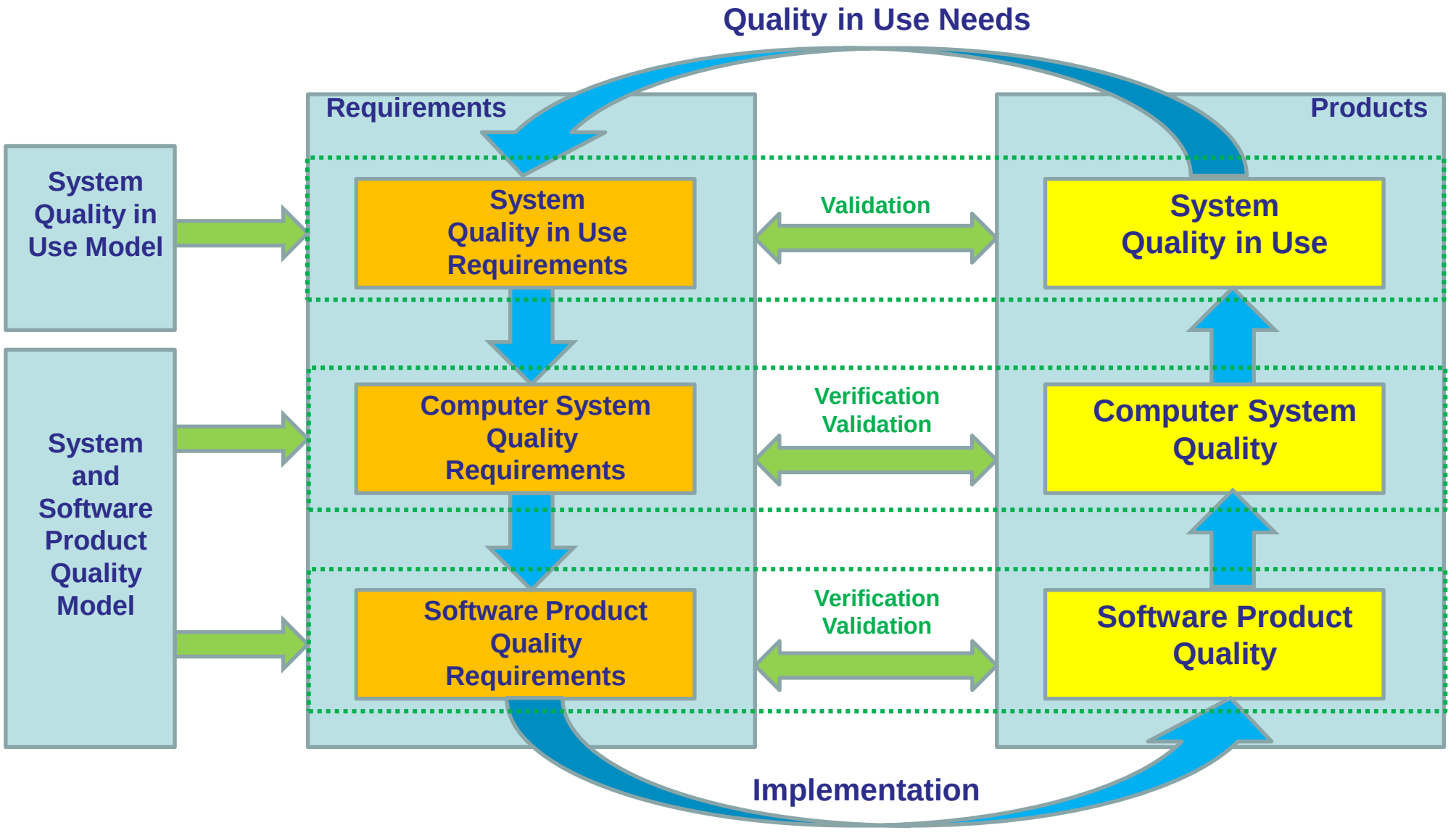
Our Focus of Interest



How can we „guarantee“ safety and security ?

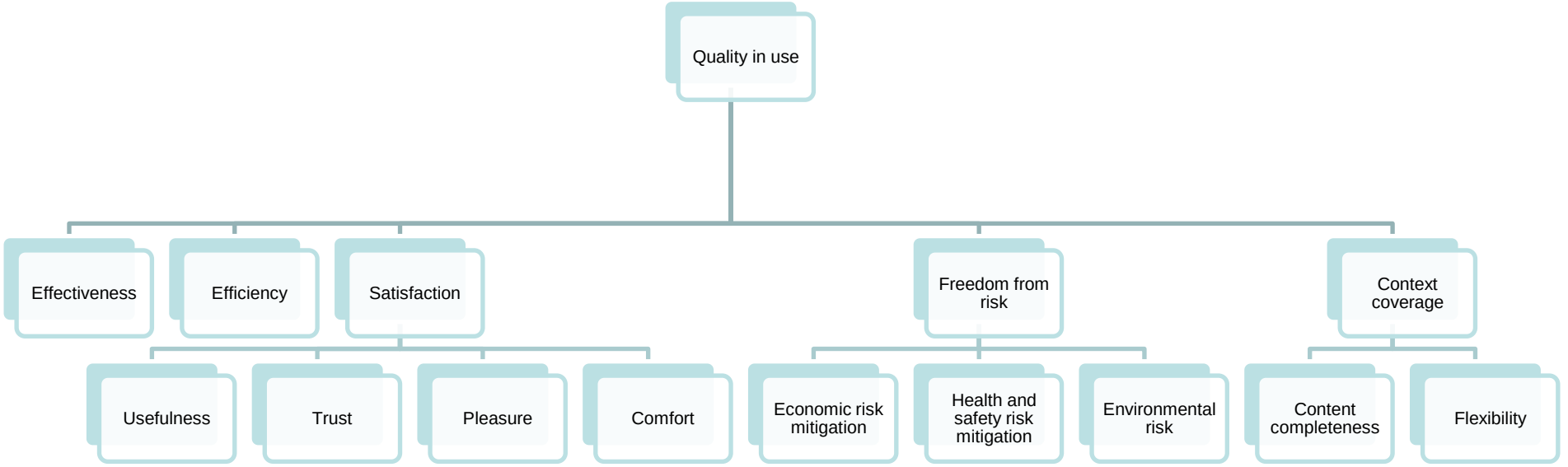
Source: ISO/IEC FDIS 25010

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