Systeme hoher Qualität und Sicherheit
Universität Bremen WS 2015/2016

# Lecture 01 (13-10-2015)

# Introduction and Notions of Quality

Christoph Lüth Jan Peleska Dieter Hutter

# Organisatorisches

# Generelles

- Einführungsvorlesung zum Masterprofil S & Q

- 6 ETCS-Punkte

- Vorlesung:
  - Montag 12 c.t – 14 Uhr (MZH 1110)
- Übungen:
  - Dienstag 12 c.t. – 14 Uhr (MZH 1470)

- Webseite:
  http://www.informatik.uni-bremen.de/~cxl/lehre/ssq.ws15/

# Folien, Übungsblätter, etc.

- Folien
  - ... sind auf Englisch (Notationen!)
  - ... gibt es auf der Homepage
  - ... sind (üblicherweise) nach der Vorlesung verfügbar

- Übungen
  - Übungsblätter gibt es auf dem Web
  - Ausgabe Montag abend/Dienstag morgen
    - Erstes Übungsblatt nächste Woche
  - Abgabe vor der Vorlesung
    - Persönlich hier, oder per Mail bis Montag 12:00

# Literatur

- Foliensätze als **Kernmaterial**
- Ausgewählte Fachartikel als **Zusatzmaterial**
  - Auf der Webseite verfügbar.
- Es gibt (noch) keine Bücher, die den Vorlesungsinhalt komplett erfassen.
- Zum weiteren Stöbern:
  - Wird im Verlauf der Vorlesung bekannt gegeben

# Prüfungen

- **Fachgespräch** oder **Modulprüfung**
  - Anmeldefristen beachten!
- Individuelle Termine nach Absprache Februar / März
- Notenspiegel Übungsblätter:

| Prozent | Note | Prozent | Note | Prozent | Note | Prozent | Note |
|---|---|---|---|---|---|---|---|
| | | 89.5-85 | 1.7 | 74.5-70 | 2.7 | 59.5-55 | 3.7 |
| 100-95 | 1.0 | 84.5-80 | 2.0 | 69.5-64 | 3.0 | 54.5-50 | 4.0 |
| 94.5-90 | 1.3 | 79.5-75 | 2.3 | 64.5-60 | 3.3 | 49.5-0 | N/b |

- Modulprüfung:
  - Keine Abgabe der Übungsblätter nötig
  - Bearbeitung dringend angeraten

# Overview

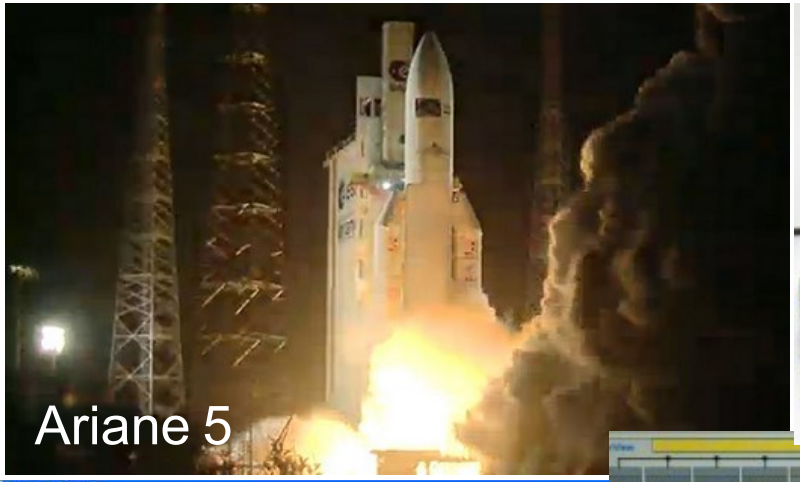
# Objectives

- This is an introductory lecture for the topics

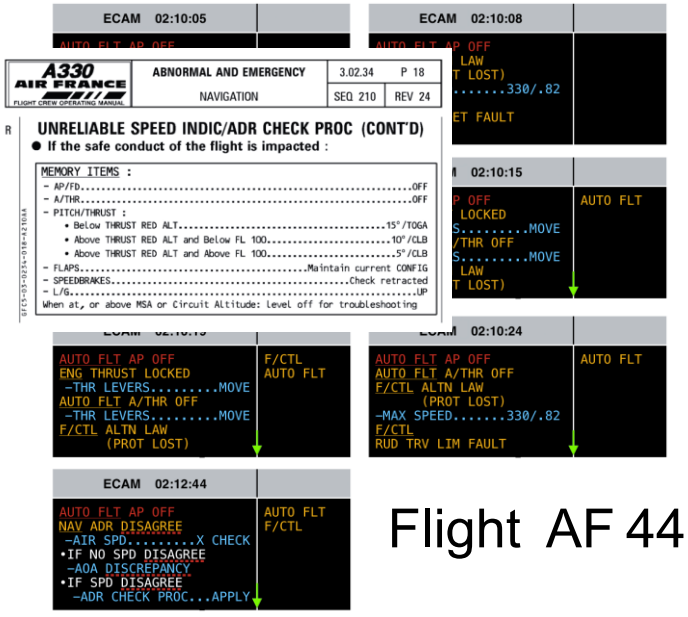
  Quality – Safety – Security

- The aim is **not** an introduction into a particular formal method, or even formal methods in general. Rather, we want to give a bird's eye view of everything relevant in connection with developing 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 elaborated jointly by Dieter Hutter, Christoph Lüth, and Jan Peleska.
- The choice of material in each semester reflects personal preferences.

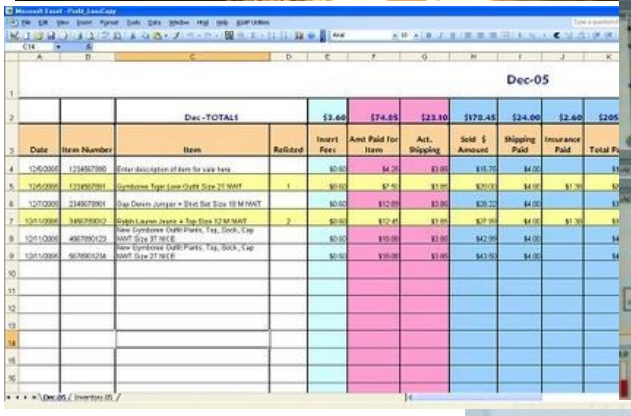
# Why bother with Quality and Safety?

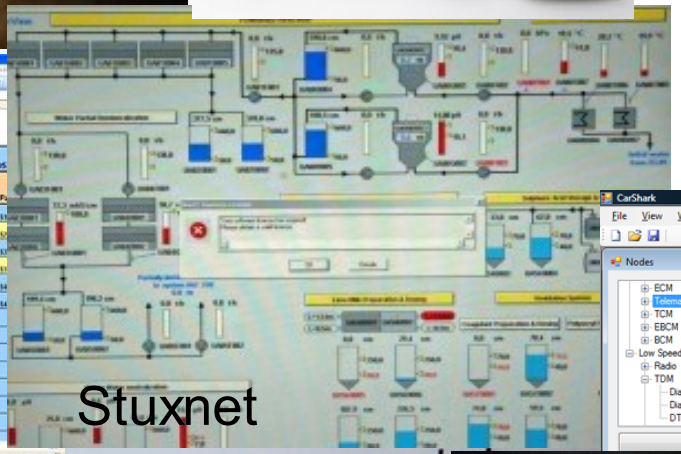






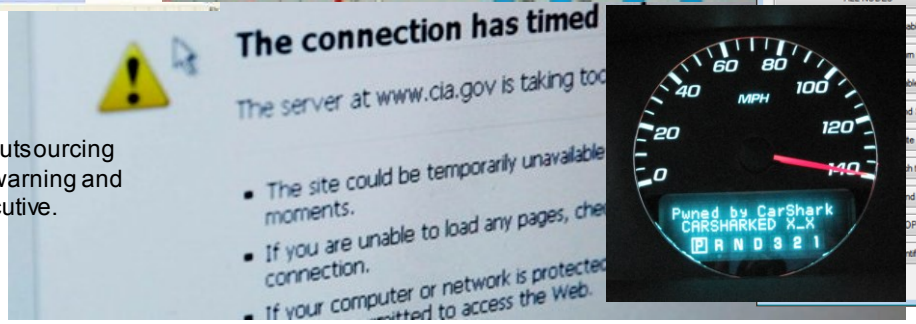

Flight AF 447




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.

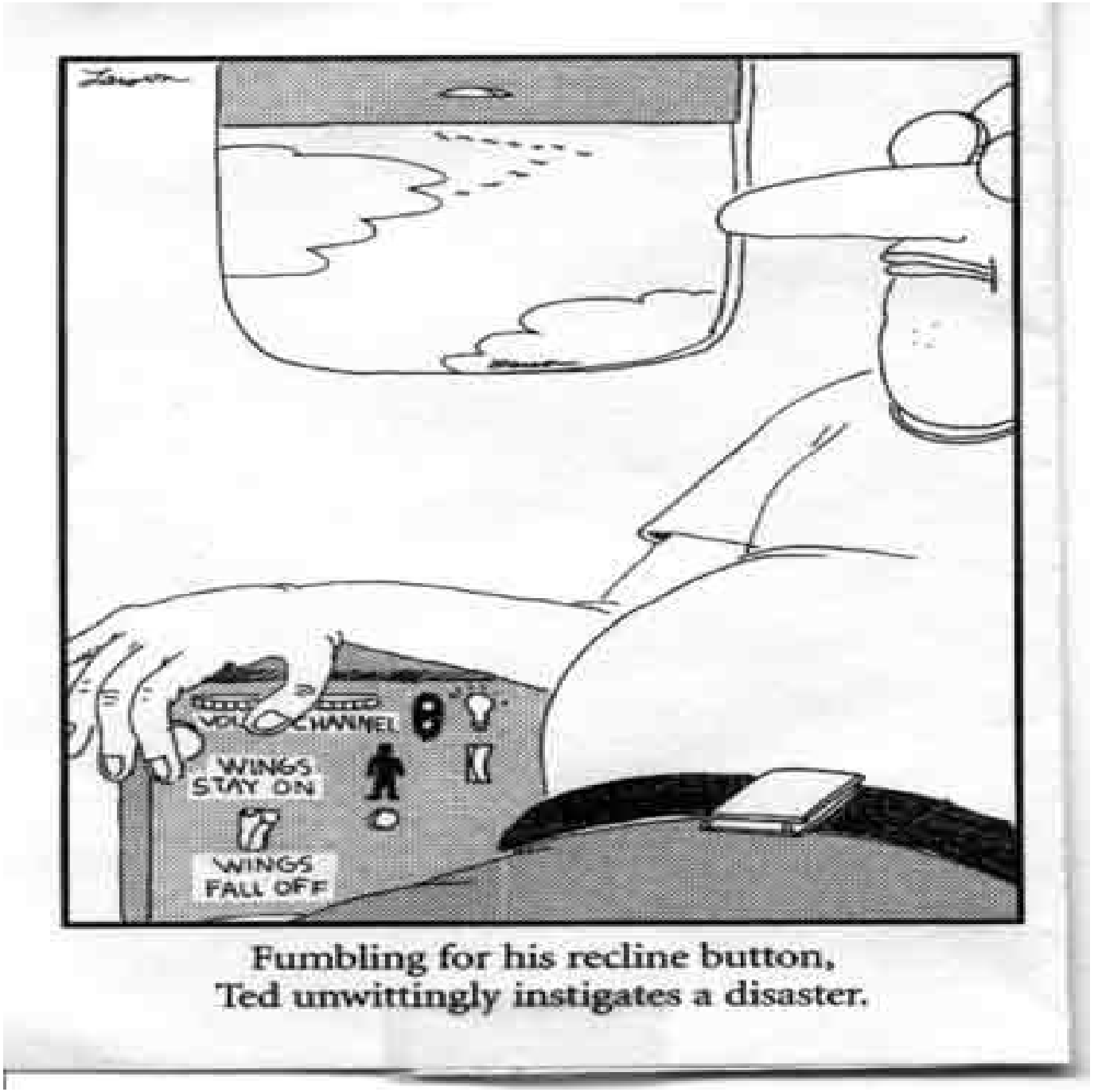
- How could that happen?

# 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.

# 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 (eg. 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

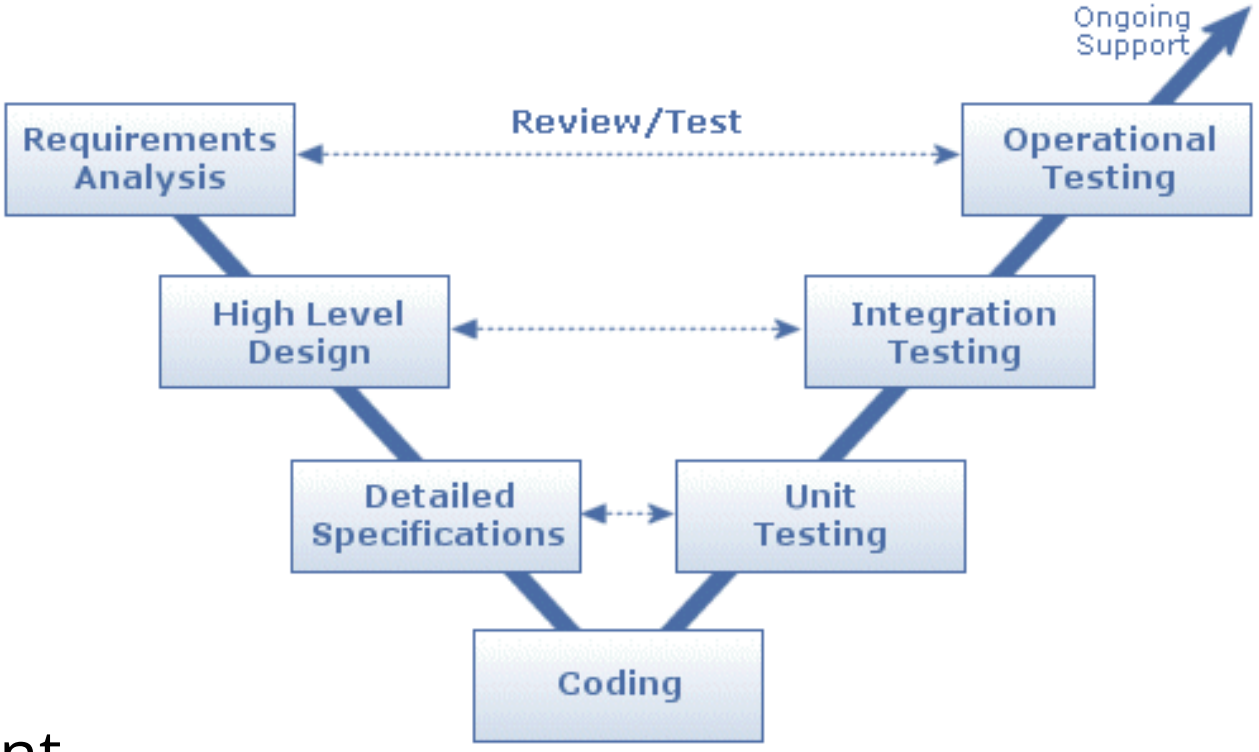



Fumbling for his recline button,
Ted unwittingly instigates a disaster.

A safety-critical design flaw – invented by Gary Larson

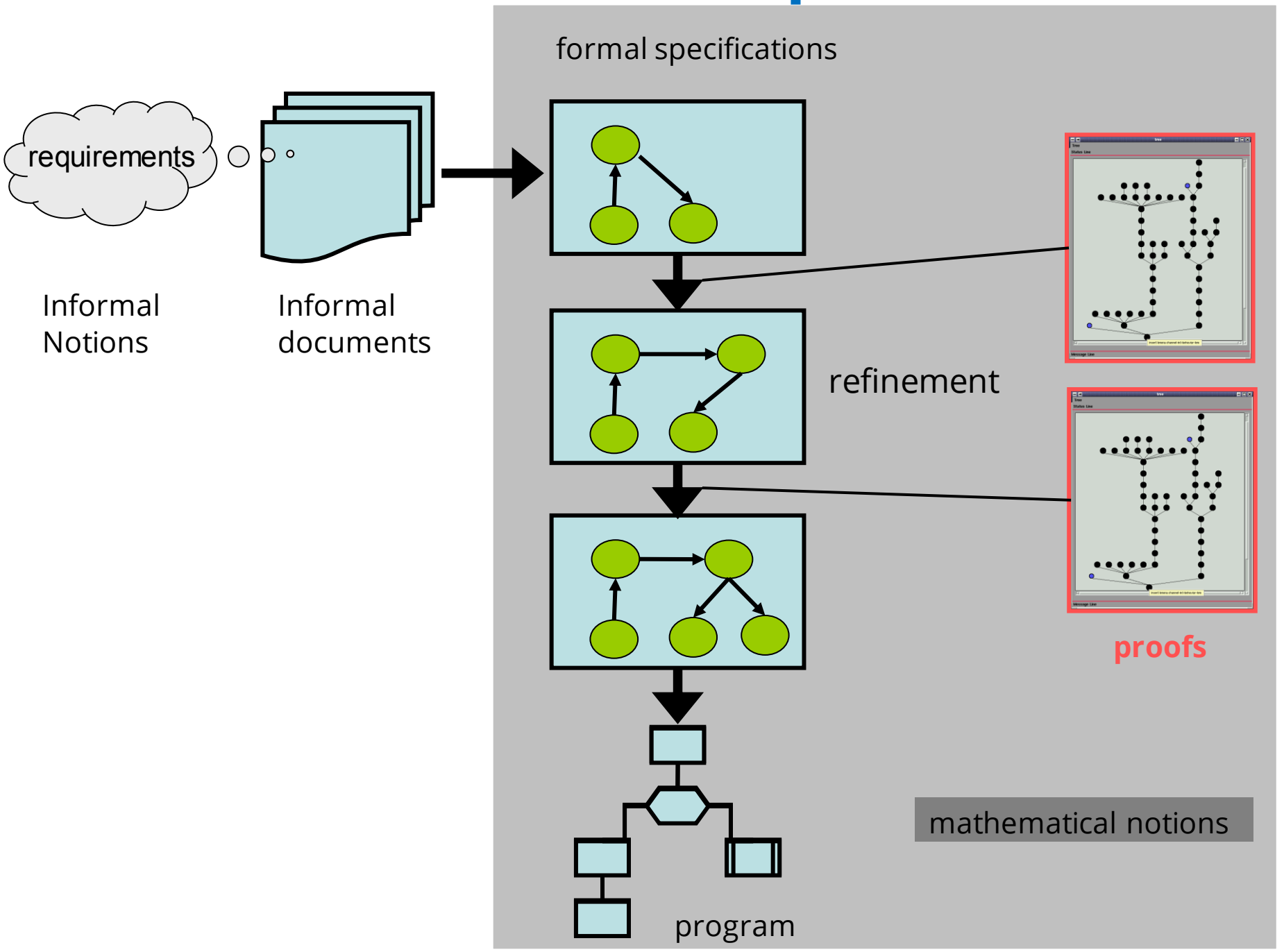
# Software Development Models

- 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

# Overview of Lecture Series

- 01: Concepts of Quality
- 02: Concepts of Safety, Legal Requirements, Certification
- 03: A Safety-critical Software Development Process
- 04: Requirements Analysis
- 05: High-Level Design & Detailed Specification with SysML
- 06: Testing
- 07 and 08: Program Analysis
- 09: Model-Checking
- 10 and 11: Software Verification (Hoare-Calculus)
- 12: Concurrency
- 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.

# 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

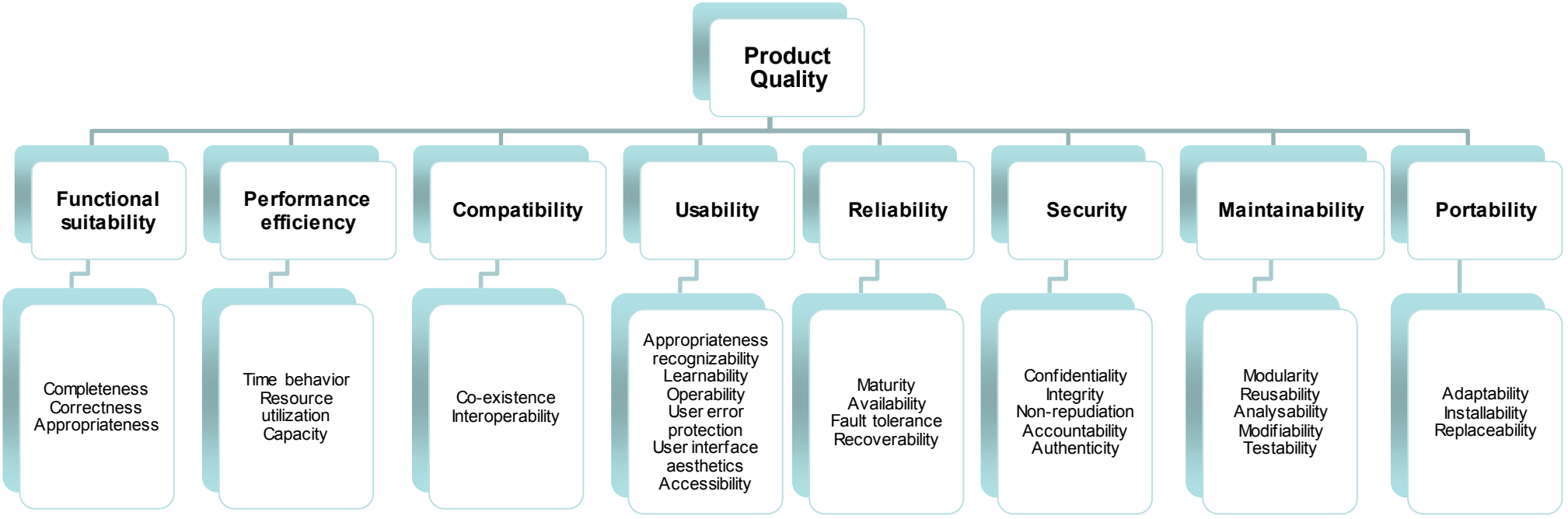
# Quality Criteria (cont.)

- 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)

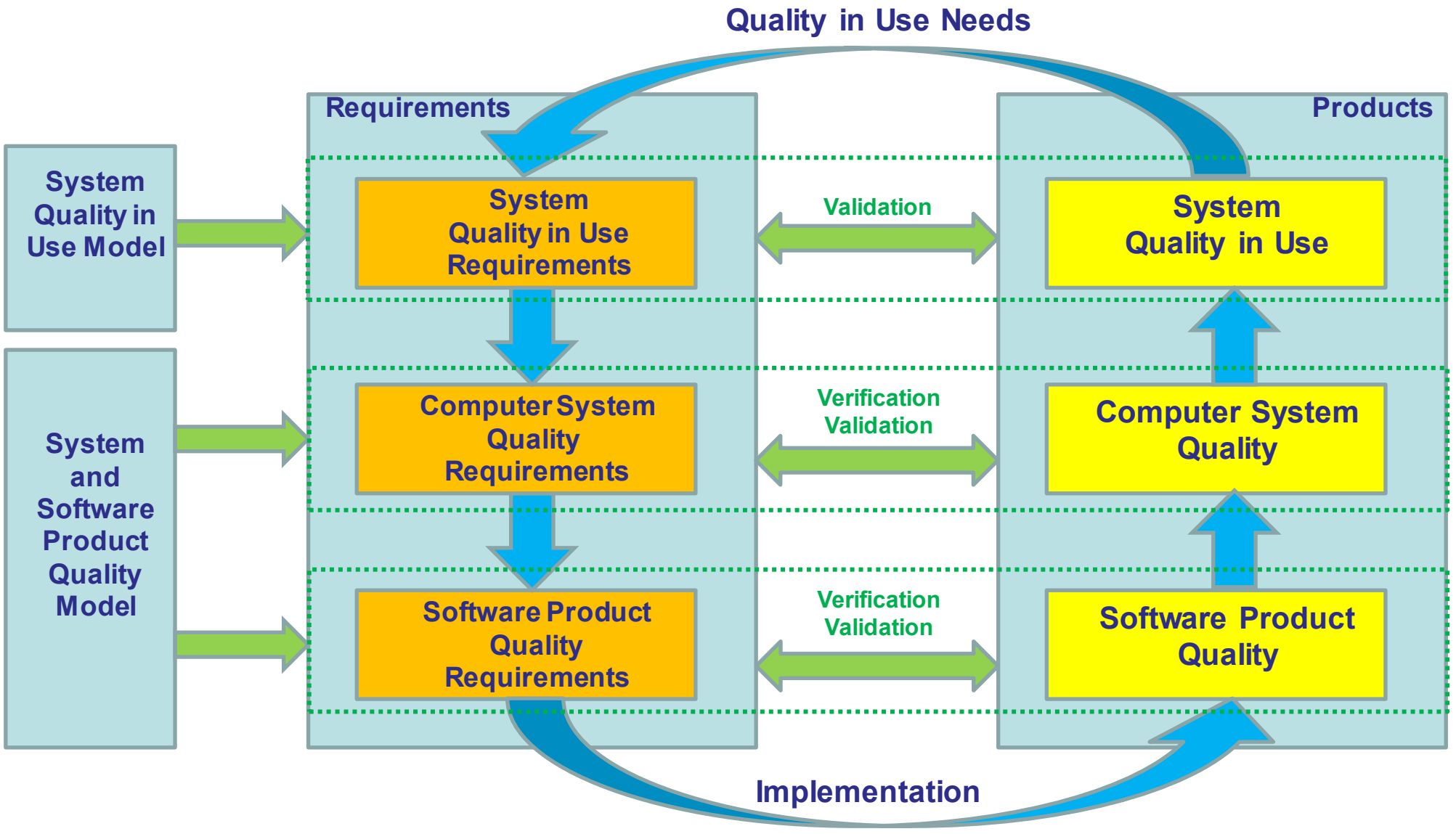
- "Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models"
  - Quality model framework (replaces the older ISO/IEC 9126)
- Product quality model
  - Categorizes system/software product quality properties
- Quality in use 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

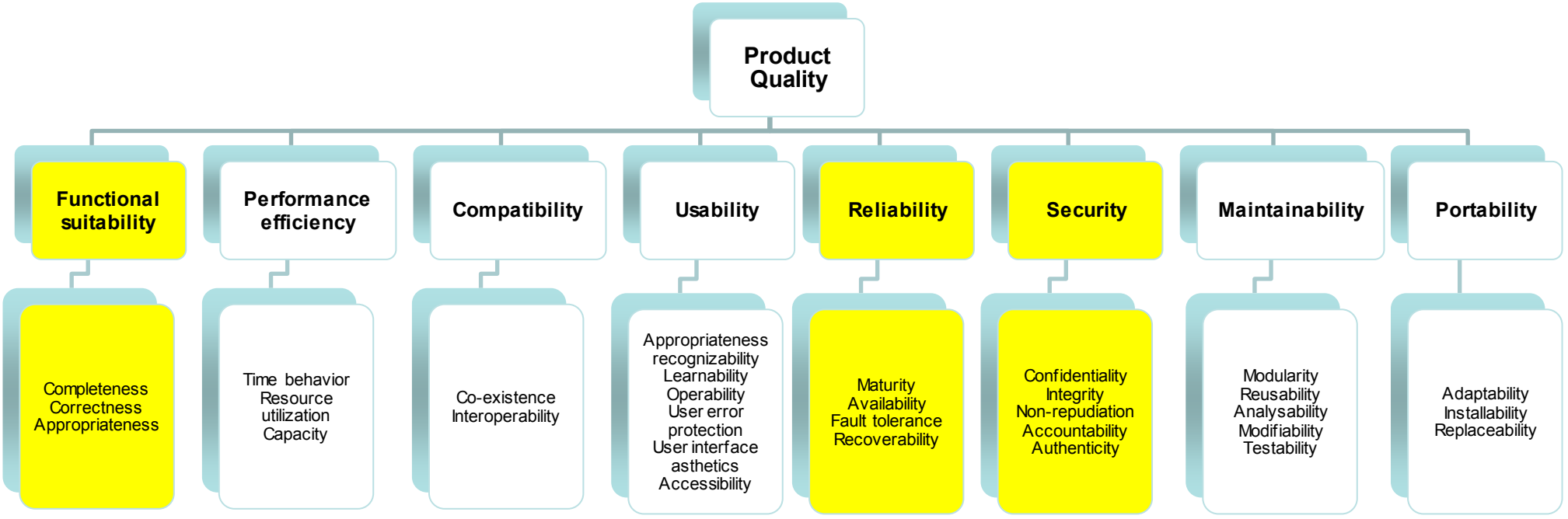
# System Quality Life Cycle Model




Source: ISO/IEC FDIS 25010

# Quality in Use Model

# Our Focus of Interest




How can we „guarantee“ safety and security ?

Source: ISO/IEC FDIS 25010

# 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
  - Standardises maturity of development process
  - Level 1 (initial): Ad-hoc
  - Level 2 (repeatable): process dependent on individuals
  - Level 3 (defined): process defined & institutionalised
  - Level 4 (managed): measured process
  - Level 5 (optimizing): improvement fed back into process

# Today's 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