Systeme hoher Sicherheit und Qualität

Wintersemester 2013-14

Christoph Lüth
MZH 3100, christoph.lueth@dfki.de, cxl@informatik.uni-bremen.de
Christian Liguda
MZH 3180, christian.liguda@dfki.de

Deutsches Forschungszentrum für Künstliche Intelligenz

Inhalt der Vorlesung

- Organisatorisches
- Überblick über die Veranstaltung
- Was ist Qualität?

ORGANISATORISCHES

Generelles

- Einführungsvorlesung zum Masterprofil **Sicherheit und Qualität**
- 6 ETCS-Punkte
- Vorlesung
  - Montag 12 c.t – 14 Uhr (MZH 1110)
- Übungen:
  - Dienstag 12 c.t. – 14 Uhr (MZH 1450)
- Webseite:

  http://www.informatik.uni-bremen.de/~cxl/lehre/sqs.ws13/

Folien, Übungsblätter, etc.

Folien

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

Übungen

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

Literatur

- Foliensätze als Kernmaterial
- Ausgewählte Fachartikel als Zusatzmaterial
- Es gibt (noch) keine Bücher, die den Vorlesungsinhalt komplett erfassen

  (Wer hat Lust, bei einem Skript mitzuhelfen?)
- Zum weiteren Stöbern
  - Wird im Verlauf der Vorlesung bekannt gegeben

Prüfungen

- Fachgespräch oder Modulprüfung
  - Anmeldefristen beachten!
  - Individuelle Termine nach Absprache Februar / März

- Fachgespräch
  - Notenspiegel:

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
    (aber Bearbeitung dringend angeraten !!!)

OVERVIEW

Objectives

- This is an introductory lecture for the topics

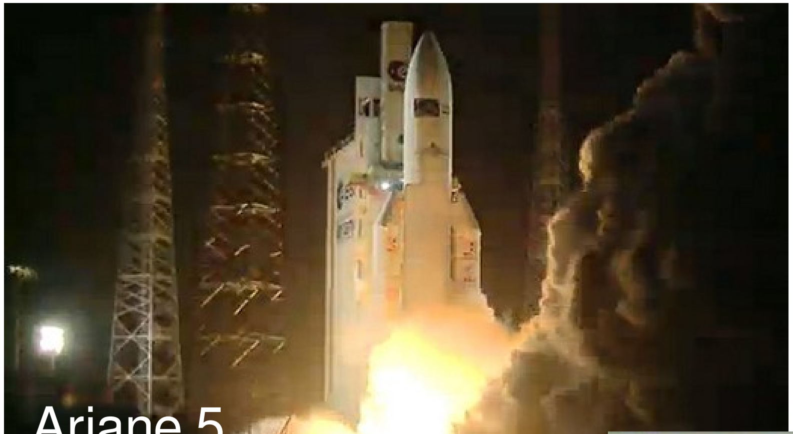
  Quality – Safety – Security

- 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

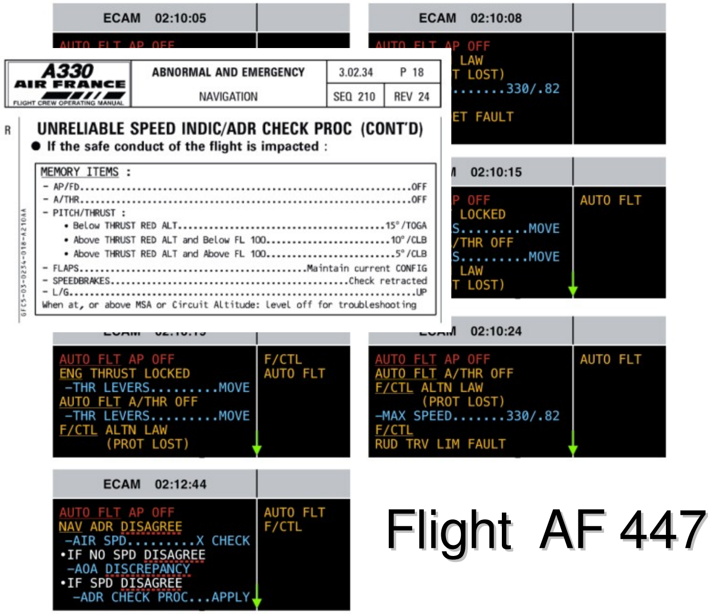
- Recall: the three focal points of computer science research at the FB3 are
  - Digital Media
  - Artificial Intelligence and Cognition
  - Quality, Safety & Security

- Disclaimer
  - “Lecture Eintopf”
  - Choice of material reflects personal preferences

Why Bother with S & Q?


Ariane 5

Chip & PIN


ECAM 02:10:05

ECAM 02:10:08
AUTO FLT AP OFF
LAW
T LOST)
.......330/.82
ET FAULT

A330 AIR FRANCE FLIGHT CREW OPERATING MANUAL | ABNORMAL AND EMERGENCY NAVIGATION | 3.02.34 P 18 SEQ 210 REV 24

R **UNRELIABLE SPEED INDIC/ADR CHECK PROC (CONT'D)**

● If the safe conduct of the flight is impacted :

```
MEMORY ITEMS :
- AP/FD.........................................OFF
- A/THR.........................................OFF
- PITCH/THRUST :
  • Below THRUST RED ALT........................15°/TOGA
  • Above THRUST RED ALT and Below FL 100.......10°/CLB
  • Above THRUST RED ALT and Above FL 100.......5°/CLB
- FLAPS.......................Maintain current CONFIG
- SPEEDBRAKES............................Check retracted
- L/G...........................................UP
When at, or above MSA or Circuit Altitude: level off for troubleshooting
```

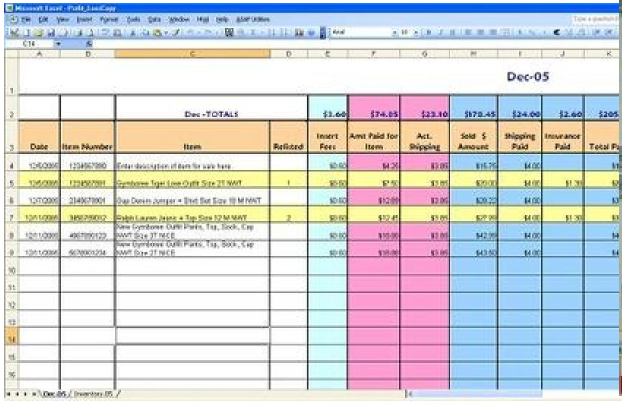
```
02:10:15
P OFF
LOCKED
S.........MOVE
/THR OFF
S.........MOVE
LAW
T LOST)
AUTO FLT
```

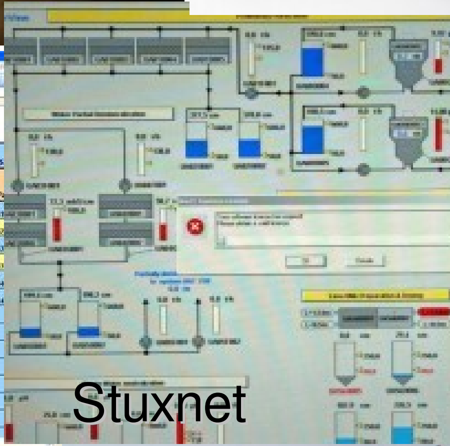
```
AUTO FLT AP OFF            F/CTL
ENG THRUST LOCKED          AUTO FLT
 -THR LEVERS.........MOVE
AUTO FLT A/THR OFF
 -THR LEVERS.........MOVE
F/CTL ALTN LAW
   (PROT LOST)
```

```
ECAM 02:10:24
AUTO FLT AP OFF            AUTO FLT
AUTO FLT A/THR OFF
F/CTL ALTN LAW
   (PROT LOST)
-MAX SPEED.......330/.82
F/CTL
RUD TRV LIM FAULT
```

```
ECAM 02:12:44
AUTO FLT AP OFF            AUTO FLT
NAV ADR DISAGREE           F/CTL
 -AIR SPD.........X CHECK
•IF NO SPD DISAGREE
 -AOA DISCREPANCY
•IF SPD DISAGREE
 -ADR CHECK PROC...APPLY
```

Flight AF 447




Stuxnet

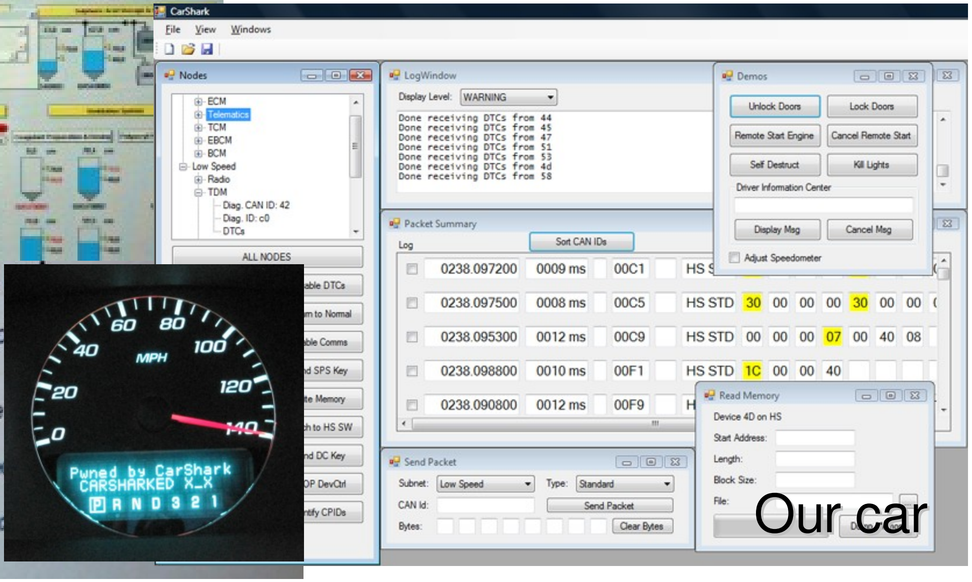
Friday October 7,2011
By Daily Express Reporter

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

The server at www.cia.gov is taking too

- The site could be temporarily unavailable moments.
- If you are unable to load any pages, che connection.
- If your computer or network is protected mitted to access the Web.



Display Level: WARNING

```
Done receiving DTCs from 44
Done receiving DTCs from 45
Done receiving DTCs from 47
Done receiving DTCs from 51
Done receiving DTCs from 53
Done receiving DTCs from 4d
Done receiving DTCs from 58
```

```
0238.097200  0009 ms  00C1  HS S
0238.097500  0008 ms  00C5  HS STD  30 00 00 00 30 00 00
0238.095300  0012 ms  00C9  HS STD  00 00 00 07 00 40 08
0238.098800  0010 ms  00F1  HS STD  1C 00 00 40
0238.090800  0012 ms  00F9  H
```

Device 4D on HS
Start Address:
Length:
Block Size:
File:

Subnet: Low Speed
Type: Standard
CAN Id:
Bytes:

Our car

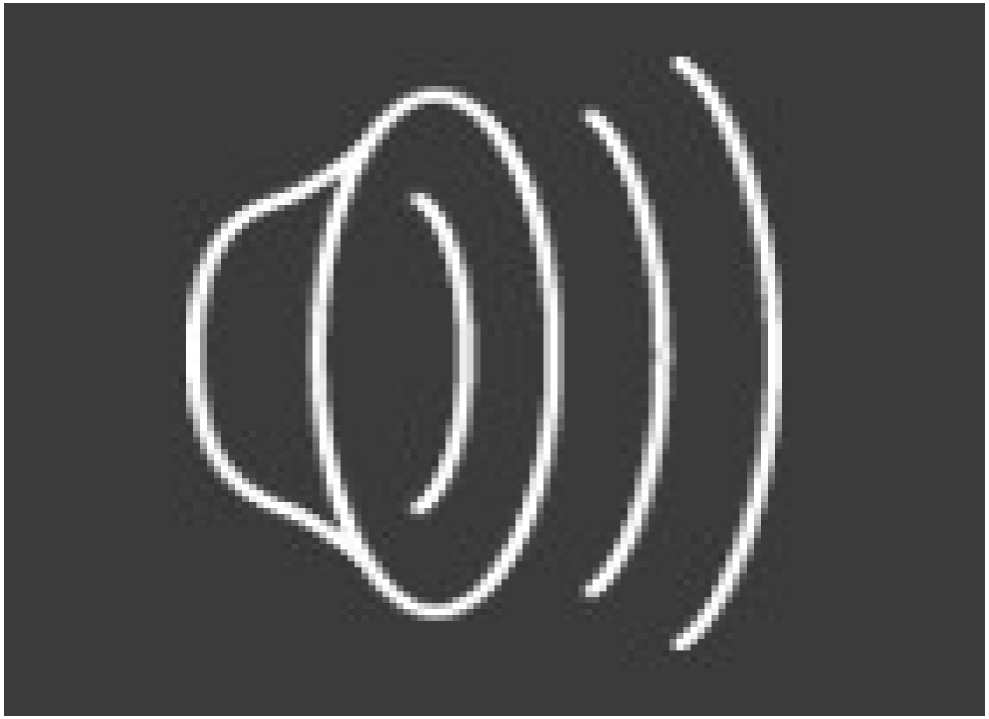
Why did Ariane-5 crash?

- Self-destruction due to instability;
- Instability due to wrong steering movements (rudder);
- On-board computer tried to compensate for (assumed) wrong trajectory;
- Trajectory was calculated wrongly because own position was wrong;
- Own position was wrong because positioning system had crashed;
- Positioning system had crashed because transmission of sensor data to ground control failed with integer overflow;
- Integer overflow occurred because values were too high;
- Values were too high because positioning system was integrated unchanged from predecessor model, Ariane-4;
- This assumption was not documented because it was satisfied tacitly with Ariane-4.

- Positioning system was redundant, but both systems failed (systematic error).
- Transmission of data to ground control also not necessary.

Engineering Sciences

- Mathematical theories
  - Statics
  - Computational models



What is Safety and Security

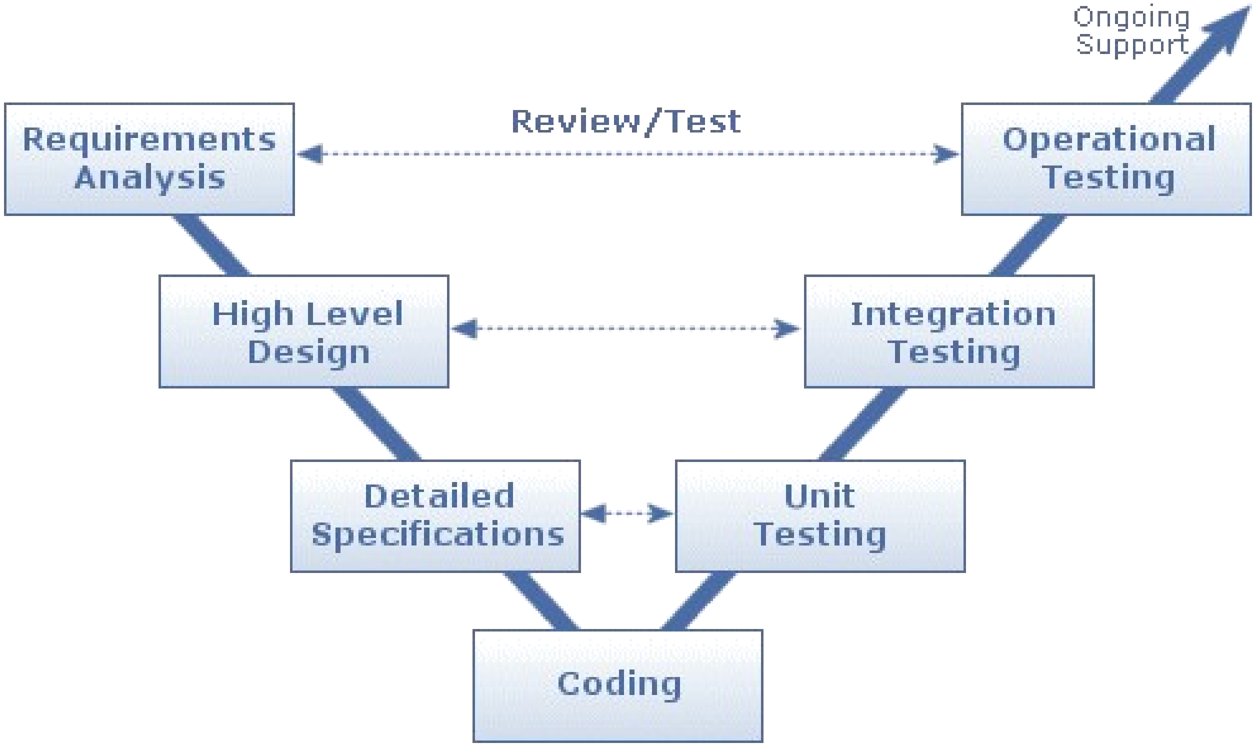
- Safety
  - product achieves acceptable levels of risk or harm to people, business, software, property or the environment in a specified context of use
  - Threats from “inside”
    - Avoid malfunction of a system (e.g. planes, cars, railways…)

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

Software Development

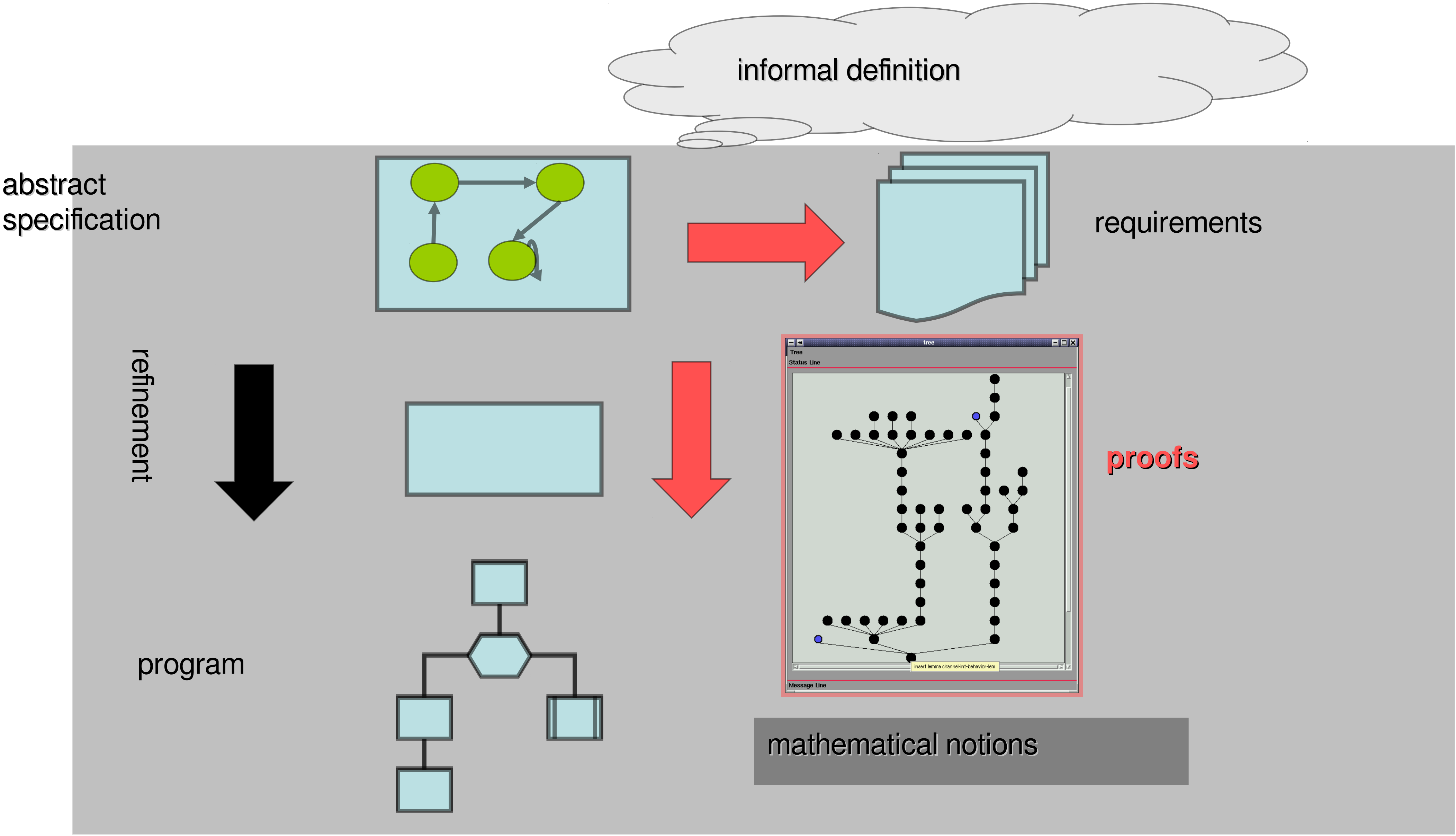
Definition of software engineering processes and documents

- V-model



- Model Driven Architectures
- Agile Development

Formal Software Development



informal definition

abstract specification

requirements

refinement

proofs

program

mathematical notions

Verification & Validation

- Verification: have we built the system right (i.e. correct)?
- Validation: have we built the right system (i.e. adequate)?
- Testing
  - Test case generation, black- vs. white box
- Symbolic evaluation
  - Program runs using symbolic values
- Static/dynamic program analysis
  - Dependency graphs, flow analysis
- Model checking
  - Formal verification of finite state problem
- Formal Verification
  - Formal verification of requirements, program properties…

Overview of Lecture Series

- Lecture 01: Concepts of Quality
- Lecture 02: Concepts of Safety, Legal Requirements, Certification
- Lecture 03: A Safety-critical Software Development Process
- Lecture 04: Requirements Analysis
- Lecture 05: High-Level Design & Detailed Specification

- Lecture 06: Testing
- Lecture 07 and 08: Program Analysis
- Lecture 09: Model-Checking
- Lecture 10 and 11: Software Verification (Hoare-Calculus)

- Lecture 12: Concurrency
- Lecture 13: Conclusions

Concepts of Quality

What is Quality

- The 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

- For the development of artifacts quality criteria can be measured with respect to the
  - development process (process quality) *(later in this lecture)*
  - 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)

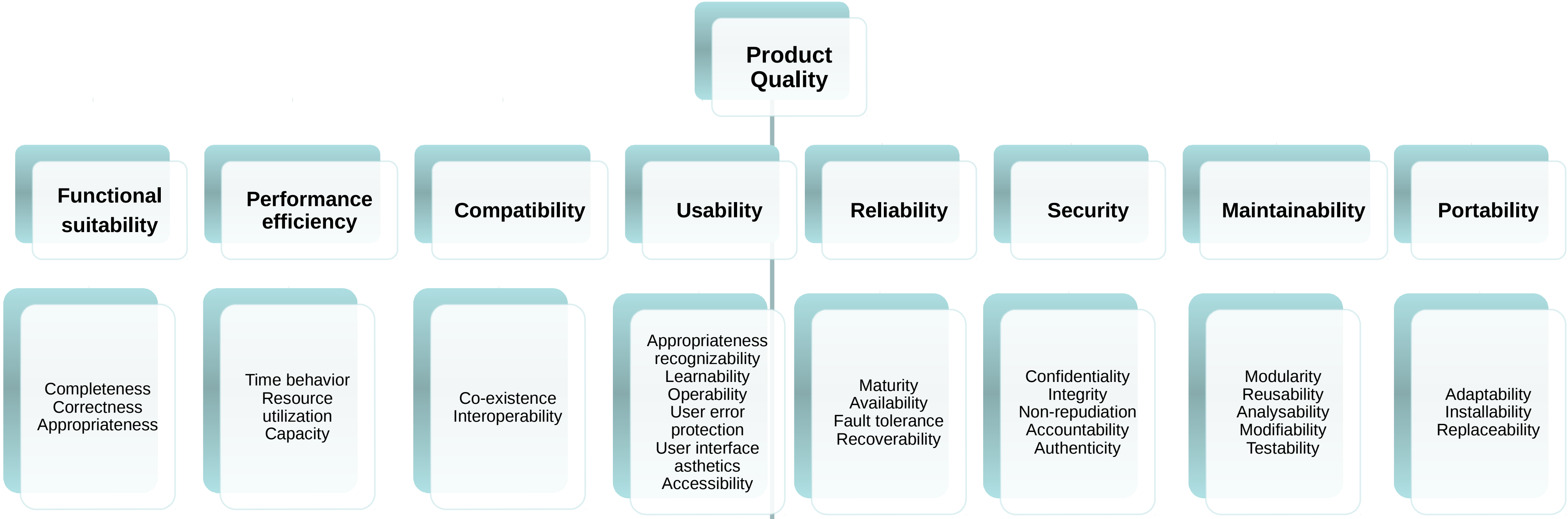
Quality model framework

- 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



Product Quality

Functional suitability

Completeness
Correctness
Appropriateness

Performance efficiency

Time behavior
Resource utilization
Capacity

Compatibility

Co-existence
Interoperability

Usability

Appropriateness recognizability
Learnability
Operability
User error protection
User interface asthetics
Accessibility

Reliability

Maturity
Availability
Fault tolerance
Recoverability

Security

Confidentiality
Integrity
Non-repudiation
Accountability
Authenticity

Maintainability

Modularity
Reusability
Analysability
Modifiability
Testability

Portability

Adaptability
Installability
Replaceability

Source: ISO/IEC FDIS 25010

Functional Suitability

- The capability of the software product to provide functions which meet stated and implied needs when the software is used under specified conditions

- Characteristics
  - **Completeness**: degree to which the set of functions cover the specified tasks and objectives
  - **Correctness**: degree to which a system / product provides the correct results within the needed degree of precision
  - **Appropriateness:** degree to which the functions facilitate the accomplishment of specified tasks and objectives

Performance Efficiency

- The capability of the software product to provide appropriate performance, relative to the amount of resources used, when used under specified conditions

- Characteristics
  - **Time behavior:** degree to which the response and processing times and throughput rates of a product meet requirement, when performing its functions
  - **Resource utilization:** degree to which the amounts and types of resources used by a product meet requirements when performing its functions
  - **Capacity:** degree to which the maximum limits of a product parameter meet requirements

Compatibility

- The capability of the software product to exchange information with other products, systems or components, and/or perform its required functions, while sharing the same hardware or software environment

- Characteristics
  - **Co-Existence:** degree to which a product can perform its required functions efficiently while sharing a common environment and resources with other products, without detrimental impact on any other product
  - **Interoperability**: degree to which two or more systems, products or components can exchange information and use the information that has been exchanged

Usability

- The capability of the software product to be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use
- Characteristics
  - **Appropriateness Recognizability**: degree to which users can recognize whether a product is appropriate for their needs
  - **Learnability**: degree to which a product or system can be used by specified users to achieve specified goals of learning to use the product with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use
  - **Operability:** degree to which a product or system has attributes that make it easy to operate and control
  - **User Error Protection:** degree to which a system protects users against making errors
  - **User Interface Aesthetics:** degree to which a user interface enables pleasing and satisfying interaction for the user
  - **Accessibility:** degree to which a product or system can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a specified context of use

Reliability

- The capability of the software product to perform specified functions under specified conditions for a specified period of times

- Characteristics
  - **Maturity**: degree to which a system meets needs for reliability under normal operation
  - **Availability**: degree to which a system, product or component is operational and accessible when required for use
  - **Fault tolerance**: degree to which a system, product or component operates as intended despite the presence of hardware or software faults
  - **Recoverability:** degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system

Security

- The capability of the software product to protect information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization

- Characteristics
  - **Confidentiality:** degree to which a product or system ensures that data are accessible only to those authorized to have access
  - **Integrity:** degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data
  - **Non-Repudiation:** degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later
  - **Accountability:** degree to which the actions of an entity can be traced uniquely to the entity
  - **Authenticity:** degree to which the identity of a subject or resource can be proved to be the one claimed

Maintainability

- The degree of effectiveness and efficiency with which a product or system can be modified by the intended maintainers

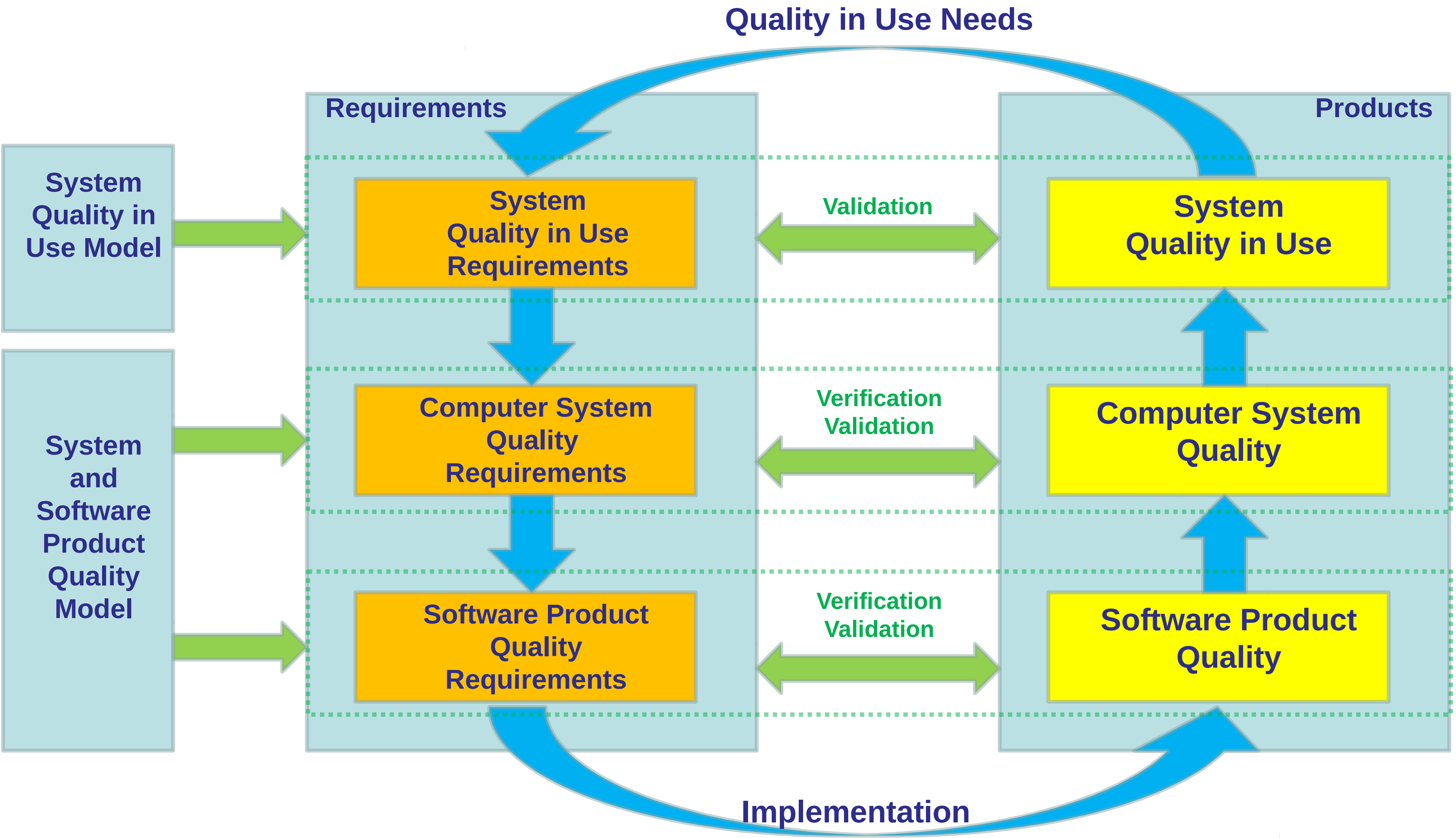
- Characteristics
  - **Modularity:** degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components
  - **Reusability:** degree to which an asset can be used in more than one system, or in building other assets
  - **Analysability:** degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified
  - **Modifiability:** degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality
  - **Testability:** degree of effectiveness and efficiency with which test criteria can be established for a system, product or component and tests can be performed to determine whether those criteria have been met

Portability

- The capability of the software product to be from one hardware, software or other operational or usage environment to another

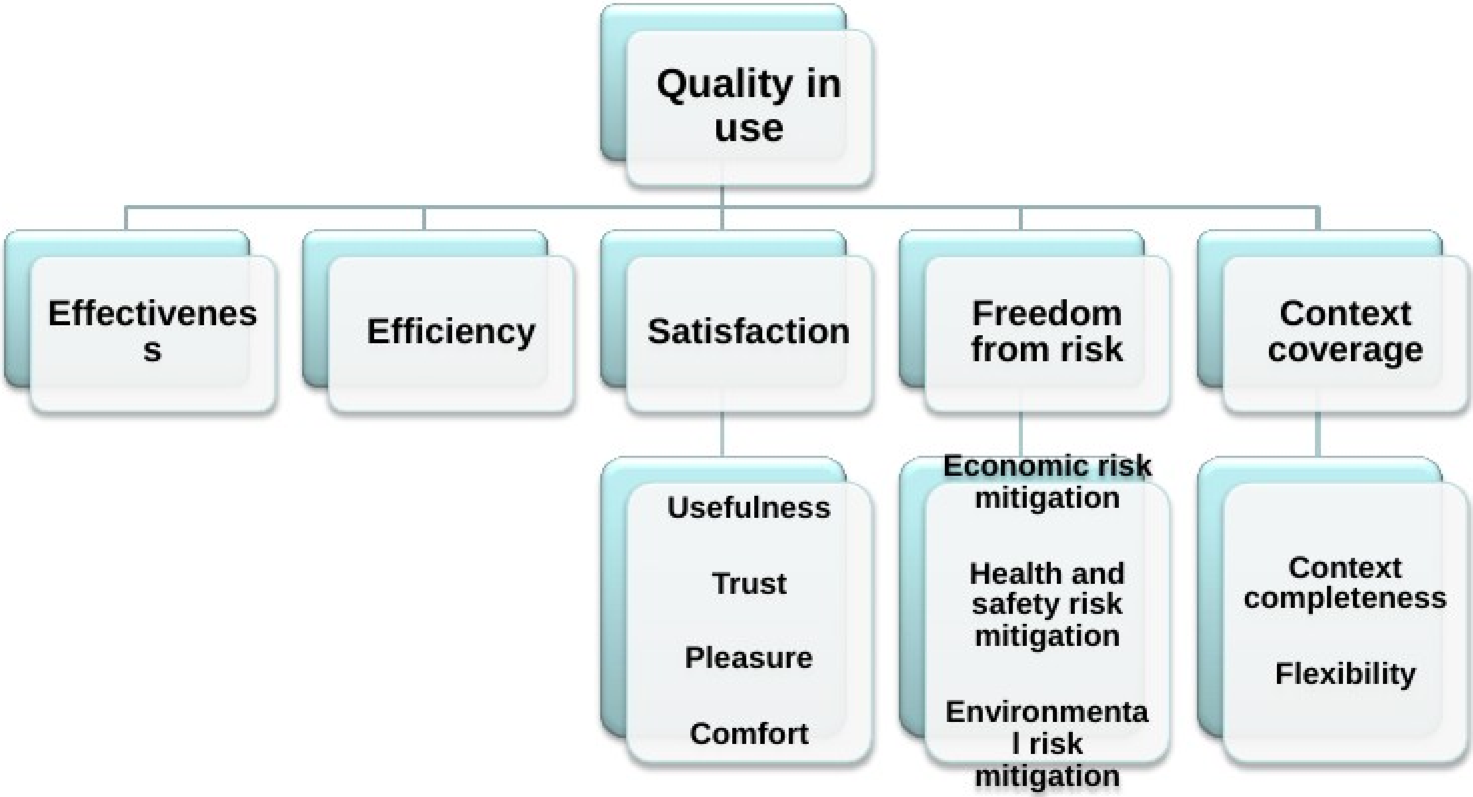
- Characteristics
  - **Adaptability:** degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments
  - **Installability:** degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment
  - **Replaceability:** degree to which a product can be replaced by another specified software product for the same purpose in the same environment

System Quality Life Cycle Model



Source: ISO/IEC FDIS 25010

Quality in Use Model



Effectiveness

- The accuracy and completeness with which users achieve specified goals

- No further characteristics

Efficiency

- The resources expended in relation to the accuracy and completeness with which users achieve goals

- No further characteristics

Satisfaction

- The degree to which user needs are satisfied when a product or system is used in a specified context of use

- Characteristics
  - **Usefulness:** degree to which a user is satisfied with their perceived achievement of pragmatic goals, including the results of use and the consequences of use
  - **Trust:** degree to which a user or other stakeholder has confidence that a product or system will behave as intended
  - **Pleasure:** degree to which a user obtains pleasure from fulfilling their personal needs
  - **Comfort:** degree to which the user is satisfied with physical comfort

Freedom From Risk (Safety)

- The capability of the software product to mitigate the potential risk to economic status, human life, health, or the environment

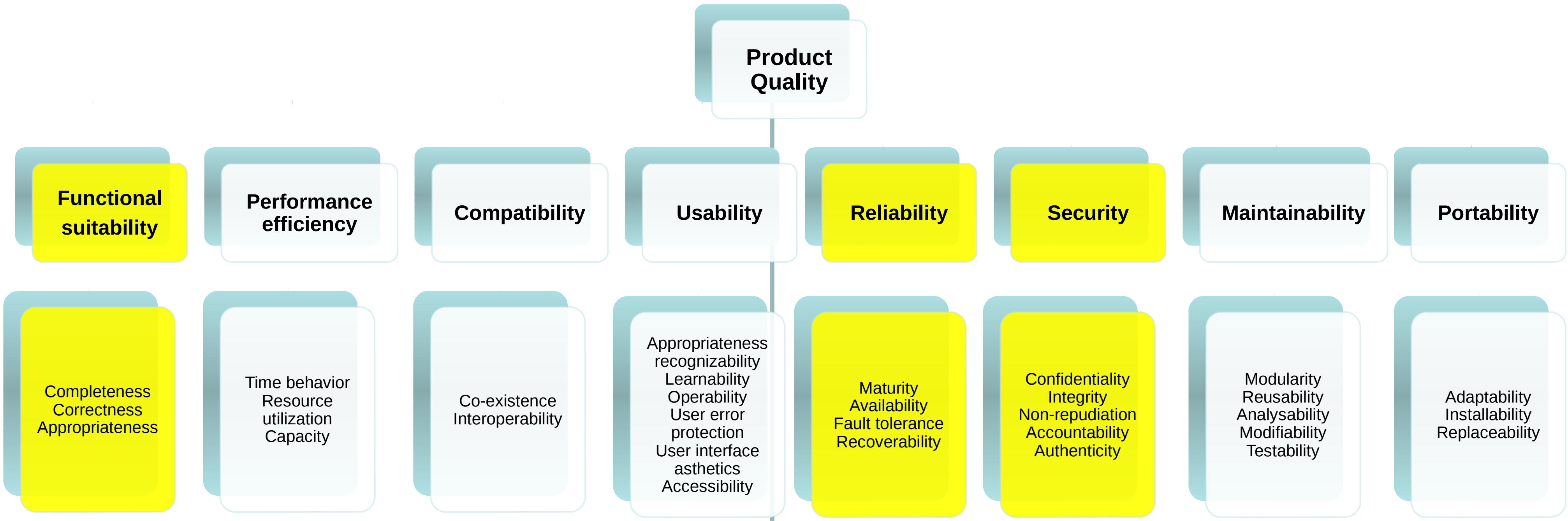
- Characteristics
  - **Economic risk mitigation:** degree to which a product or system mitigates the potential risk to financial status, efficient operation, commercial property, reputation or other resources in the intended contexts of use
  - **Health and safety risk mitigation:** degree to which a product or system mitigates the potential risk to people in the intended contexts of use
  - **Environmental risk mitigation:** degree to which a product or system mitigates the potential risk to property or the environment in the intended contexts of use

Context Coverage

- The capability of the software product to be used with effectiveness, efficiency, freedom from risk and satisfaction in both specified contexts of use and in contexts beyond those initially explicitly identified

- Characteristics
  - **Context completeness:** degree to which a product or system can be used with effectiveness, efficiency, freedom from risk and satisfaction in all the specified contexts of use
  - **Flexibility:** degree to which a product or system can be used with effectiveness, efficiency, freedom from risk and satisfaction in contexts beyond those initially specified in the requirements

Focus of Interest



Product Quality

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

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 & institionalized
    - Level 4 (Managed): measured process
    - Level 5 (optimizing): improvement fed back into process

Summary

- Quality:
  - collection of characteristic properties
  - quality **indicators** measuring quality **criteria**

- Relevant **aspects** of quality here:
  - Functional suitability
  - Reliability
  - Security