CERTIFICATION ISSUES
IN AUTOMOTIVE SOFTWARE

Speaker: Mario Fusani
Systems and Software Evaluation Centre
ISTI – CNR, Pisa, Italy
mario.fusani@isti.cnr.it
CONTENTS

• Certification
  – What is certification?
    • Definitions
    • Objects, actors, schemes
  – Benefits and drawbacks
    • Standards: good things / so&so things
    • Confidence and risks

• Software / Automotive Software certification
  – Reference requirements / standards
  – Comments on some current reference requirements

• Conclusions
WHAT IS CERTIFICATION?

[Optimistic] An activity that provides demonstration that specified requirements relating to an object {product, process, system, person or body} are fulfilled [ISO/IEC 2002]

[Interested] A way to augment the value of a manufactured object [supplier point of view]

[Need oriented] A way to get more confidence (i.e., to know the associated risks) about an object and its associated services [consumer point of view]

[Spoiling] An illusion about an unachievable goal [some scientist’s point of view especially in software]
WHAT CERTIFICATION IS NOT

- **A guarantee** that specified requirements relating to an object are satisfied
- **A snapshot** or measure of a characteristic of an object
- **An assertion of very severe** analyses and tests executed on an object
QUESTIONS ABOUT CERTIFICATION

• What are the **objects** of certification (what is/can be certified)?
• What are the **actors** associated with the certification and how do they behave (duties, opportunities)?
• What is the **chain-of-confidence** around a certified object?
• What is the **added value** of certification?
• Who **benefits** from certification?
ROLE OF STANDARDS IN CERTIFICATION

- **CERTIFICATION BODY**
  - Certifies conformity of object reference model for conformity to a subset of Collection of STDs for object requirements.

- **Collection of STDs for assessing object conformance to requirements and for inspection/surveillance.** They refer to techniques but may not contain techniques.

- **STD for certifying object category**

- **CB rules**

- **OBJECT** (product, process, Q_system or professional skill)

ISTI-CNR

Automotive SPIN - Milano, 11 October 2007
ROLE OF STANDARDS IN CERTIFICATION
(case of product certification)

STD for certifying object category

Collection of STDs for certifying object category

Certifies conformity of CB rules

Collection of STDs for assessing object conformance to requirements and for inspection/surveillance. They refer to techniques but may not contain techniques.

Supplier process

Process monitoring

OBJECT (product)

Conforms to a subset of conformity to a subset of

Collection of STDs for object requirements

Object reference model for

uses

uses

uses

Specialized testing / inspection lab (uses techniques)

Certifies conformity of certification body

accreditation

accreditation
CONTENTS

• Certification
  – What is certification?
    • Definitions
    • Objects, actors, schemes
  – Benefits and drawbacks
    • Standards: good things and not so good ones
    • Confidence and risks

• Software certification
  – Kinds of reference requirements or standards
  – Comments on some current reference requirements

• Conclusions
ABOUT STANDARDS

- Object reqs. stds: public reference, allow comparability
- Cert. Process stds: allow repeatability / reproducibility
- Cost reduction in certification process

- Risk of introducing obsolete techniques (requirement-oriented stds may be exception)
- Risk of protecting corporate business
- With cogent rules, risk to pursue formal compliance and not real qualities (safety)
CONTENTS

• Certification
  – What is certification?
    • Definitions
    • Objects, actors, schemes
  – Benefits and drawbacks
    • Standards: good things and not so good ones
    • Confidence and risks

• Software certification
  – Kinds of reference requirements or standards
  – Comments on some current reference requirements

• Conclusions
WHAT IS THE ADDED VALUE OF CERTIFICATION?

• More confidence on object (based on knowing its associated risks)
• How much would users pay for that?
ADDED VALUE IS BASED ON:

- **Independency** of CB
- Accreditation chain: ability of **transferring confidence** to relevant stakeholders (CB itself is checked !)
- Explicit **certification policy** (liability, certification process, scope, restrictions, duties)
- Good **coverage of the user needs** by the object requirements **standards** (conformance can be assessed and certified against requirements, not against needs)
- **Consensus** and adoption of standards by suppliers and customers
- **Up-to-date techniques** and methods used by CB and/or by n\textsuperscript{th}-party labs
- Stakeholders **investment** (supplier: design for “certifiability”)

ISTI-CNR

Automotive SPIN - Milano, 11 October 2007
WHO BENEFITS FROM CERTIFICATION

• Certification Bodies business
  – induced by suppliers investment / regulations / procurement policies
• Suppliers business
• Intermediate / \textit{end users}
  – they often \textit{can’t judge by themselves} and must trust other parties (1st, 2nd, 3rd, ...), but are the final experimenters (for good or not) of services associated to the objects
KEEP IN MIND

• Certification gives confidence on **compliance** to **standards** and not to implicit/explicit needs

• The latter is good-standardization job!
  – Need-capturing ability of STDs
CONTENTS

• Certification
  – What is certification?
    • Definitions
    • Objects, actors, schemes
  – Benefits and drawbacks
    • Standards: good things and not so good ones
    • Confidence and risks

• Software certification
  – Kinds of reference requirements or standards
  – Comments on some current reference requirements

• Conclusions
SOFTWARE CERTIFICATION

• Rather oriented to **system properties**
  – Difficult system/software properties separation
  – Security
  – Other sectored functional standards
  – Safety (search for system SW-independent safe states!)

• Very **high cost** for 3rd-party bodies
  – are the most expensive techniques the most effective ones?
  – “Certifiability”

• Lack of product requirement reference standards
  – Product standards (lack quality, little domain coverage)
  – Process standards (CMMI, SPICE, ISO/IEC 90003, …)
CONTENTS

• Certification
  – What is certification?
    • Definitions
    • Objects, actors, schemes
  – Benefits and drawbacks
    • Standards: good things and not so good ones
    • Confidence and risks

• Software certification
  – Kinds of reference requirements or standards
  – Comments on some current reference requirements

• Conclusions
REFERENCE STANDARDS IN CERTIFICATION

• requirements standards for software products

• requirements standards for software processes

• standards enabling a certification body to **assess conformance** (typically, of properties of products/processes to requirements)

• standards usable as **internal rules by certification bodies**
SUITABILITY CRITERIA FOR STANDARDS
(both for object requirements and for certification process)

• Easy to understand and use
• Grounded on scientific bases
• Support evolving techniques
• Cost effective
• Ability to capture stakeholders (users?) needs
CONTENTS

• Certification
  – What is certification?
    • Definitions
    • Objects, actors, schemes
  – Benefits and drawbacks
    • Standards: good things and not so good ones
    • Confidence and risks

• Software certification
  – Kinds of reference requirements or standards
  – Comments on some current reference requirements

• Conclusions
REQUIREMENTS STANDARDS FOR SOFTWARE PRODUCTS

• Functional standards
  – general case (customer reqs): hardly unsuitable for **product** certification
  – compilers, protocols, graphic&sound, special domains: suitable but no market
• Quality standards
  – ISO/IEC 9126, SQUARE, IEEE, ...
    • partially suitable (standard makers claim), no policy available
  – Security (ITSEC, CC)
    • suitable enough (schemes exist), claimed by certification bodies (mostly UK CBs), good market, no policy available
  – Safety (MIL, IEC 61508, WD 26262 … , corporate)
    • Avionics: suitable enough
    • On-rail vehicles: mostly mentioned
    • automotive: scarcely suitable, need process so far
OBJECT REQUIREMENTS STANDARDS FOR SOFTWARE PROCESS

• CMM, CMMI
  – suitable for process certification (scarce certification policy availability)

• ISO/IEC 15504 (12207)
  – suitable for certification, but purpose disclaimed (projects exist for certification policy)

• IEEE, IEC 61508, WD 26262
  – partially suitable (document based, phased-project based, scarce technique assessment)
STANDARDS FOR CERTIFICATION PROCESS

• CMM, CMMI
  – suitable in a certification scheme (not well distinguished from process reference stds)

• ISO/IEC 15504
  – suitable enough but purpose disclaimed (well separated from process reference stds.)

• SQUARE (ISO/IEC 14598)
  – not yet suitable
STANDARD FOR CERTIFICATION BODIES

• ISO Guides
  and
• EN 45000, ISO/IEC 17000 family
  – naturally suited: purposely written for certification schemes, explicitly recommend certification policy associated with certificate
CONCLUSIONS

• Common understanding needed about certification and software certification (also in Automotive)

• No guarantee, no ultra-severity, but higher confidence on STD compliance and hopefully on object-associated services (also in Automotive)

• Build added value of certificate crucial as market drive (especially in Automotive)

• What can be certified is not the outcomes of service associated, but conformance to standards (warning for Automotive safety)

• Successful software product certification still a challenge (especially in Automotive)

• High variability of product certification scenarios (application domain, scope, purpose, …) (also in Automotive)

• Costs are a problem (cost reduction by supplier support, certifiability, user support, …) (also in Automotive)