

Title	A Report of the Current Situation on Software Certification in Japan
Author(s)	Mizuguchi, Daichi
Citation	
Issue Date	2006-11-28
Type	Presentation
Text version	publisher
URL	http://hdl.handle.net/10119/8313
Rights	
Description	3rd VERITE : JAIST/TRUST-AIST/CVS joint workshop on VERification TEchnologyでの発表資料, 開催 : 2006年11月27日 ~ 28日, 開催場所 : JAIST 知識科学研究科講義棟・中講義室

A Report of the Current Situation on Software Certification in Japan

Daichi Mizuguchi

CVS-AIST

<http://unit.aist.go.jp/cvs>

Outline

- Talk about
 - the current situation on software certification in Japan
 - our “mock certification” plan
- A “position paper”
 - nothing technical is involved
 - hope to provide seeds for discussion
 - comments and suggestions are welcome

Background

- Software is ubiquitous; an important component of the social infrastructure
 - Its quality must be ensured for a safe and secure life
- International standards on the software quality have been published in succession
 - Certification based on the standards is active in Europe
- Japan is far behind this trend
- CVS-AIST started research on software certification

Situation in Japan

- Three industries are concerned about software certification
 - Safety control equipment industry
 - Automotive industry
 - Measuring instrument industry
- because of the standards to follow

Safety control equipment industry

IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems (1998-2000)

- for computer-controlled safety systems in e.g. chemical plants and product lines in factories
 - emergency stop/shutdown system, interlock system
 - components are intelligent sensors, programmable logic controllers, network equipments, etc.
- Part 3: “Software requirements”
 - on development process, documents, techniques
- recommends techniques and measures according to the safety integrity level (SIL)
 - formal methods are highly recommended for SIL 4

Some opinions

- ✓ As IEC 61508 is getting popular, Japanese manufacturers need to get their products certified, but..
- ✓ How to develop along with IEC 61508?
 - voluminous; hard to understand/interpret
 - how to apply the recommended techniques and measures and to what extent?
 - why formal methods? what is it!?
- ✓ Achieving certification takes a lot of cost!
 - certification business is dominated by German companies
 - judgment criteria are not clear
 - why no Japanese certification body!?

Automotive industry

ISO 26262 – Road vehicles – Functional safety (draft; scheduled 2008)

- adaptation of IEC 61508 to automobile
- for computer-controlled safety related systems in a road vehicle
 - break, steering, powertrain, hybrid control, air bag, etc.
 - “X-by-wire” technology will expand the scope
- Part 6: “Software development”
 - similar requirements to those in IEC 61508
- mainly led by Germany and France
- will possibly be legalized in EU

Some comments

- ✓ The industry is critical to the draft
 - Is this really the best practice?
 - Part 6 says nothing about safety, but only about reliability
 - Does this make a car safer?
 - Technical guideline should be involved
 - Why formal methods?
- ✓ hope not to work as a non-tariff barrier to trade

Measuring instrument industry

MID: Measuring Instruments Directive (2004)

- came into force on October 30, 2006
- for gas and electricity meters, petrol pumps, weighing instruments, taxi meters, etc.
- requirements for correctness and security
 - on data protection, data transmission, software downloading, etc.
- will be promoted to the international standard “OIML D-SW”

Tasks

- ✓ The industry is not so confused, but..
- ✓ AIST is the “notified body” for type approval of measuring instruments in Japan
- ✓ AIST has to set up certification procedure and provide development guideline to manufacturer,
 - which must be practical and agreed with by the industry
- ✓ AIST has to certify measuring instruments according to the procedure

What are the problems?

- Requirements are ambiguous
- Certification criteria are ambiguous
- Requirements are not based on reasonable rationale
- Technical guidelines are insufficient
- All standards are coming from Europe
- Achieving certification costs a lot
- No certification body in Japan
- ...
- CVS-AIST is planning a case-study of software certification in industrial scale

“Mock certification” project

Plan to

- set up a development project
 - of a (prototype) system
 - with industrial partners
- run both the development and a simulation of certification in parallel
- use as much as formal techniques, as long as practicable
- ✓ CVS-AIST has been recruiting partners

Expected results

- knowledge on certification
 - objective certification criteria
 - technical documents
 - evaluation of the techniques and measures in the standards
 - feedback to the standards
 - knowledge for development along with the standard
- the first step for setting up a software certification body in Japan

Concluding remarks

- Talked about
 - the concerned three industries
 - the mock certification project
 - Software certification is such an urgent and practical issue
 - Demands for software certification will expand to other domains
 - Good certification system needs to obtain trust from the industry and the users
 - The mock certification project is meant to contribute to building the trust with formal methods
- ✓ Please contact us if interested