The Next Generation of Safety Standards – Wishful Thinking?

Odd Nordland

Senior Research Scientist

SINTEF ICT

Software Engineering, Safety and Security

odd.nordland@sintef.no

Introduction

- Some myths about using standards
- Standards never come as a surprise
- Standards are inconsistent
- Standards are unclear
- Standards are incomplete
- Room for improvement

Some Myths About Using Standards

1. Following the standards is expensive
   - adequate routines already exist
   - adapting them to a new standard is expensive
2. Most of what the standards require is done anyway
   - reviews, analyses, tests
   - documentation of results
   - justification of design decisions
3. Following a standard does not improve the product
   - same product, different documentation

Standards never come as a surprise

- They are announced and publicly available long before they are adopted
- They are discussed and agreed by the affected industries
- They are a compromise between rivalling interests

- But they are never a surprise!

- So adapting routines and procedures to a future standard can be begun well in advance
  - there’s no excuse for not being ready when a standard is adopted

Standards are inconsistent

- Several standards may apply simultaneously
  - e.g. for computer systems in nuclear power
    - IEC 61508 – Functional safety of E/E/PE safety-related systems
    - IEC 61513 – Nuclear power plants, Instrumentation and control for systems important to safety, General requirements
    - IEC 60880 – Nuclear power plants, Instrumentation and control for systems important to safety, Software aspects...
    - IEEE 7-4.3.2 – IEEE Standard criteria for digital computers...
    - IEEE 1228 – IEEE Standard for software safety plan
  - National regulations and laws can apply in addition, e.g.
    - CE-1001-STD – (Canadian) Standard for Software Engineering of Safety Critical Software
- They have different life cycle models, required activities

Standards are unclear [1]

- IEC 62278 and IEC 62279 have contradicting definitions e.g. verification and validation:
  - IEC 62278 Validation

    Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use have been fulfilled
  - IEC 62278 Verification

    Confirmation by examination and provision of objective evidence that the specified requirements have been fulfilled
  - IEC 62279 Validation

    activity of demonstration, by test and analysis, that the product meets in all respects its specified requirements
  - IEC 62279 Verification

    activity of determination, by analysis or test, that the output of each phase of the life-cycle fulfils the requirements of the previous phase

Standards are unclear [1]

- IEC 62278 and IEC 62279 have contradicting definitions e.g. verification and validation:
  - IEC 62278 Validation

    Confirmation *by examination and provision of objective evidence* that the *particular* requirements for a specific *intended* use have been fulfilled
  - IEC 62278 Verification

    Confirmation *by examination and provision of objective evidence* that the specified requirements have been fulfilled
  - IEC 62279 Validation

    activity of demonstration*, by test and analysis,* that the product meets *in all respects* its specified requirements
  - IEC 62279 Verification

    activity of determination*, by analysis or test,* that the output of each phase *of the life-cycle* fulfils the requirements *of the previous phase*

Standards are unclear [1]

- IEC 62278 and IEC 62279 have contradicting definitions e.g. verification and validation:
  - IEC 62278 Validation

    Confirmation that the requirements for a specific use have been fulfilled
  - IEC 62278 Verification

    Confirmation that the specified requirements have been fulfilled
  - IEC 62279 Validation

    demonstration that the product meets its specified requirements
  - IEC 62279 Verification

    determination that the output of each phase fulfils the requirements

Standards are unclear [2]

- IEC 61508, IEC 62279 and others classify measures as
  - Mandatory
  - Highly Recommended
  - Recommended
  - Not recommended
  - no recommendation
- No explanation of what the difference is supposed to be
  - Mandatory is clear, but:
  - Highly recommended vs. Recommended
    - how high is highly recommended?
  - Not recommended $\neq$ forbidden!
    - so it can be used anyway?

Standards are unclear [3]

- Safety qualification tests: the standards don’t say
  - that these are tests to demonstrate the (theoretically) predicted safety characteristics
    - this means the test object should be tested under genuine safety critical operating conditions
    - which is ‘illegal’, because the safety qualification test is a prerequisite for authorisation to operate!
  - Testing safety characteristics or functions involves generating unsafe conditions
    - Crash tests with cars can be used to test safety functions
    - Crash tests with trains?
    - Crash tests with planes??
    - Nuclear power plants???

Standards are unclear [3]

- Safety qualification tests (continued)
  - Simulations are of limited value
    - simulations are always based on a model
    - so they cannot behave exactly like the real world
      - timing of events
      - extreme conditions
      - physical stress
  - Simulators must be validated
    - this is seldom done explicitly
    - because the standards don't demand it!
  - Alternative and/or supplement to simulation:
    - probationary authorisation for testing purposes field tests under restricted operational conditions
    - but some safety functions might not be tested

Standards are incomplete

- Safety standards address one particular aspect of safety
  - technical properties of safety instrumentation e.g. IEC 62278
  - safety related software e.g. IEC 62279
- Instrumentation and software are not the only means of achieving safety:
  - Administrative procedures
  - Design properties
  - Education and training

Administrative procedures

- Examples
  - Two people required to trigger a nuclear attack
  - Standardised verbal communication protocols in air traffic
  - Speed limits on roads
    - and/or for specific vehicles
  - Load limits for structures
    - tanks or heavy trucks have to cross bridges one at a time
  - Operational directives/regulations
    - forbidden to store explosives in a residential area
    - no smoking at fuel pumps
    - concessions required for certain types of business
- There’s no standard for administrative safety procedures

Design properties ("intrinsic safety")

- Examples
  - Dimensions
    - nuclear radiation has a finite range in concrete, so make the walls thicker than the range
  - Electrical properties
    - fibre optical cables are immune to electromagnetic interference
  - Chemical properties
    - use of stainless steel in (sub)marine applications
    - predefined pairs of materials in space instrumentation
  - Geometry
    - exit doors shall open outwards
    - blunt corners of tables
- There is no standard for "intrinsic safety"

Education and training

- Personnel qualification
    - Which qualification should a safety engineer have?
        - there are no standardised curricula for safety engineering
        - it is up to the individual to decide what he thinks he needs to know
            - e.g. Markov analysis, Petri nets, risk analysis...
    - What is “adequate” experience?
        - a high school degree and how many years learning on the job?
            - several years on the job is no guarantee for quality
    - How should the qualification be documented?
        - high school degrees may not address the right areas
        - CV mentions duration of activities, not quality
- There is no standard for safety education and training

Room for improvement

- In spite of their shortcomings
  - Following standards improves safety
  - Following standards facilitates comparability
  - Following standards is economically sensible
- Standards are to be updated every 5 years
  - Inconsistencies can be removed
  - Clarifications can be made
  - Missing aspects can be included
- The next generation will still be no guarantee for safety
  - But it can come closer!

多谢各位聆聽

Thank you