Progress and Open Issues in Standards

Udo Voges
Forschungszentrum Karlsruhe
Institut für Angewandte Informatik
udo.voges@kit.edu

Content

- **Existing Standards**
- **Current Projects**
- **Open Issues**

Existing Standards

- **Generic standards**
  - IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems
  - ISO/IEC 20000-1:2005 Information technology – Service management – Part 1: Specification (Part 2: Code of practice)
- **Application areas**

Existing Standards

- **IEC 60601 family**
  - IEC 60601-1:2005 Medical electrical equipment – Part 1: General requirements for basic safety and essential performance
  - IEC 60601-1-6:2006 Medical devices – General requirements for safety and essential performance - Usability
- **ISO 14971:2007 Medical devices – Application of risk management to medical devices**
- **IEC 62304:2007 Medical device software – Software life cycle processes**
- **IEC 62366:2007 Medical devices - Application of usability engineering to medical devices**

Work Programme CEN/TC 251 Health Informatics (1)

- **ENV 12924:1997 Medical informatics – Security categorisation and protection for healthcare information systems**
- **CR 13694:1999 Health informatics – Safety and security related software quality standards for healthcare (SSQS)**
- **ENV 13608-1/2/3:2000 Health informatics – Security for healthcare communication – Part 1 + 2 + 3**

Work Programme CEN/TC 251 Health Informatics (2)

- **ENV 13735:2000 Health informatics – Interoperability of patient connected medical devices**
- **CR 14301:2002 Health informatics – Framework for security protection of healthcare communication**
- **CR 14302:2002 Health informatics – Framework for security requirements for intermittently connected devices**

Work Programme CEN/TC 251 Health Informatics (3)

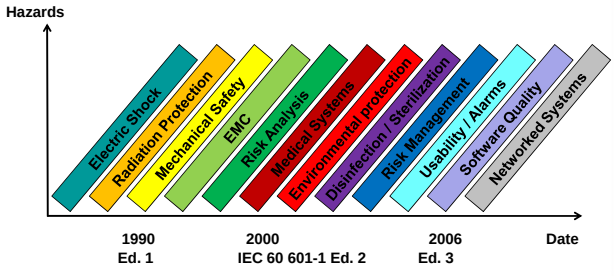
- CEN/TS 15127-1:2005 Health informatics – Testing of physiological measurement software – Part 1: General
- CEN/TR 15299:2006 Health informatics – Safety procedures for identification of patients and related objects
- CEN/TR 15300:2006 Health informatics – Framework for formal modelling of healthcare security policies

Work Programme CEN/TC 251 Health Informatics (4)

- CEN/TS 15260:2006 Health informatics – Classification of safety risks from health information products

IEC 60601 family

Evolution in safety standardization to cover further hazards is going on



© Oliver.christ@prosystem-ag.de

Current Projects

- IEC 80001 Ed. 1: Application of risk management for IT-networks incorporating medical devices
- IEC TR 80002: Medical device software – Guidance on the application of ISO 14971 to medical device software
- ISO TS 29321: Health informatics – Application of clinical risk management to the manufacture of health software

IEC 80001

- Application of risk management for IT-networks incorporating medical devices.
- Current draft: IEC 62A/591/CD 2007-12-07
- Last meeting of the JWG of IEC SC 62A (Common aspects of electrical equipment used in medical practice) and ISO TC 215 (Health informatics): 25-26 Sep 2008 in USA

IEC TR 80002

- Medical device software – Guidance on the application of ISO 14971 to medical device software.
- Current draft: IEC 62A/616/CD 2008-05-09
- Last meeting of JWG 3 (IEC SC 62A + ISO TC 210): 16 Sep 2008 in Germany
  - E.g. in 3.1.1.3 a safety case is recommended
  - "Demonstrate the SAFETY of the system by means of a SAFETY case based on the architecture"

ISO/IEC 27799

- Health informatics – Information security management in health using ISO/IEC 27002
- CEN/TC 251
- Publication before the end of 2008

ISO 14971

- Risk management
- Maintenance cycle
- Update also based on the comments on IEC 60601-1 3rd Edition

IEC/TR 60930 Ed. 2.0

- Guidelines for administrative, medical, and nursing staff concerned with the safe use of medical electrical equipment and medical electrical systems
- CD in 2007

IEC 61258 Ed. 2.0

- Guidelines for the development and use of medical electrical equipment educational materials
- CD in 2007

ISO TS 29321

- Health informatics – Application of clinical risk management to the manufacture of health software
- This project tries to copy ISO 14971 and, with the assumption, that this is mainly HW related, add additional items concerning SW.
- Questionable, whether this project will succeed.
- Current version of 2007-10

ISO/NP TR 29322

- Health informatics – Guidance on risk evaluation and management in the deployment and use of health software (GREMIDUHS)
- Dispatch of TCA draft before 2008-03-27

IEC 62508 Ed. 1.0: Guidance on Human Aspects of Dependability

This International Standard provides guidelines on human aspects of engineering and implementation of systems. It addresses the influence of human aspects on system dependability for life cycle applications. Dependability describes the availability performance of a system which is influenced by its performance characteristics of reliability, maintainability and maintenance support. A system may comprise a combination of interacting hardware, software and the people involved in its operation and maintenance. A dependable system is trustworthy and capable of performing the desirable service upon demand to satisfy user needs. Human oriented design has significant influence on the system enabling it to achieve dependability performance and service quality. By addressing human oriented design early as a part of the systems engineering process, one is able to ensure that total system performance is optimized by addressing human issues in a deliberate and systematic way.

This international standard provides guidance to facilitate incorporation of human centred design issues and requirements in system design, development, operation and maintenance. It permits practical human oriented design applications and design trade-offs with other key system hardware and software elements for cost-effective implementation. Technical approaches and human centred design methods are adopted from industry best practices suitable for systems engineering applications.

IEC 61131-6: Programmable controllers - Part 6: Functional safety

This Part of IEC 61131 addresses the functional safety requirements of the FS-PLC ae related to potential functional safety requirements of the ultimate application/interface of the FS-PLC with the overall E/E/PE safety-related system. The functional safety requirements of the overall safety-related system and the functional safety requirements of the ultimate application of the safety-related system are outside the scope of this Part. For the latter, the reader is referred to application specific standards such as IEC 61511, IEC 62061, and ISO 13849. The object of this Part is;

- to establish and describe the life-cycle elements identified in IEC 61508-1, -2 and -3 that are applicable to FS-PLCs.
- to establish and describe the requirements for FS-PLC HW and SW.
- to establish evaluation methods for a FS-PLC to this Part for the following parameters/criteria;
  - a Safety Integrity Level (SIL) claim for which the FS-PLC is capable,
  - a Probability of Failure on Demand (PFD) value,
  - a Probability of Failure per Hour (PFH) value,
  - a value for the safe failure fraction (SFF),
  - a diagnostic coverage (DC) value,
  - a verification that the specified FS-PLC manufacturer's safety lifecycle processes are in place,
  - Proof test interval,
  - Safe state,
  - the measures and techniques for the prevention and control of systematic faults, and
  - for each credible failure mode, the functional behaviour in the failed state.
- to establish the definitions and identify the principal characteristics relevant to the selection and application of FS-PLCs and their associated peripherals.

This Part is primarily intended for FS-PLC manufacturers. It also includes the critical role of FS-PLC users through the user documentation requirements. Some user guidelines for FS-PLCs may be found in Part 4.

Not Approved Projects

ISO/IEC NWIP:

Medical devices and medical systems — Basic safety and essential performance of the patient-centric integrated clinical environment (ICE)

— Part 1: General requirements for network control

Open Issues

- **Will the recommended safety case remain in IEC 80002**
- **80002 is only a TR, therefore no obligation for use**
- **Security issues are barely dealt with in 80001**
- **Use of classification or levels in discussion**
- **Object oriented software**
- **COTS / SOUP**
- **Use of generic safety standard IEC 61508**

Maintenance Cycle IEC SC62A

Publication no.	Date of Publ.	Review date	Maint. result date	Responsibility (Team)
IEC/TR 60513, Ed.2	1994-01	Preparatory work	2007	62A
IEC 60601-1, Ed. 3	2005-12	2007-12	2010	62A
IEC 60601-1-1, Ed. 2	2000-12	2010-01	2010	62A WG 11
IEC 60601-1-2, Ed. 3	2007-03	Work in progress	2009	62A MT 23
IEC 60601-1-4/A1, Ed. 1	1999-10	2010-01	2010	62A WG 22
IEC 60601-1-6, Ed. 2	2006-12	2007-12	2009	62A WG 5
IEC 60601-1-8, Ed. 2	2006-09	2009-09	2011	ISO/TC 121/SC 3 – IEC/SC 62A JWG 02
IEC 60601-1-9, Ed. 1	2007-07	2010-05	2012	62A WG 20
IEC 60601-1-10, Ed. 1	2007-11	2011-01	2013	ISO/TC 121/SC 3 – IEC/SC 62A JWG 05
IEC/TR 60878, Ed. 2	2003-07	Preparatory work	2007	62A WG 5
IEC/TR 60930, Ed. 1	1988-08	Work in progress	2008	62A MT 24
IEC/TR 61258, Ed. 1	1994-02	Work in progress	2009	62A MT 24
IEC/TR 62296, Ed.1	2003-03	Work in progress	2007	62A WG 14
IEC 62304, Ed. 1	2006-05	2009-01	2011	IEC/TC 210 – IEC/SC 62A JWG 03
IEC/TR 62348, Ed. 1	2006-05	2010-05	2011	62A
IEC 62353, Ed. 1	2007-05	2010-05	2012	62A WG 14
IEC/TR 62354, Ed. 1	2005-12	Work in progress	2010	62A WG 14
IEC 62366, Ed. 1	2007-10	2010-10	2012	ISO/TC 210 – IEC/SC 62A JWG 04
ISO 14971, Ed. 2	2007-03	2012-03	2014	ISO/TC 210 – IEC 62A JWG 01