


<p>EUROPEAN WORKSHOP ON INDUSTRIAL COMPUTER SYSTEMS TECHNICAL COMMITTEE 7 Reliability, Safety, Security</p>		<p>WP: 8900 – 2.1 Date: 2008-09-16 Status: Released Classification: Public</p>
<p style="text-align: center;">DISCLAIMER: If the status of this page is "Proposed" or "Draft", it is not yet endorsed and may not be quoted or referenced in publications. If its classification is NOT "Public", it may not be quoted or referenced in publications without the prior consent of the author.</p> <p style="text-align: center;">ACKNOWLEDGEMENTS: This work was funded by the members' affiliations.</p>		

SUBGROUP MEDICAL DEVICES (MeD)

Briefing Paper

1. Introduction

EWICS TC7 (European Workshop on Industrial Computer Systems, Technical Committee 7, Safety, Reliability, and Security) is an international workshop of experts in the field of dependability of industrial computer systems with respect to safety, reliability, and security. TC7 represents a broad coverage of industry, manufacturers and users, as well as universities, research centres, standardisation committees and licensing authorities.

The Medical Devices (MeD) Subgroup has been initiated at the TC7 spring meeting of 1997. Now, the subgroup has about 30 members from 9 European countries, the USA and Japan. MeD subgroup members also participate in standardisation bodies such as IEC TC 62, ISO TC 210, AAMI SW, BSI CH 62, BSI CH 210, DKE GK 914, and DKE UK 811.3.

2. Problem Statement

Active medical devices are more and more dependent on and controlled by programmable electrical/electronic (PE) systems. Standards on Medical Devices address only some aspects of PE-related topics. The application domain of PE-controlled systems which are critical for the health and safety of patients include:

- Patient life supporting functions (e.g. ICU, pacemaker)
- Therapy treatment (including surgical robots)
- Diagnostic equipment
- Laboratory equipment like analysers (blood, urine, etc.) and compounders
- Critical data communications (measurement data, device status, remote control, incl. the 'medical information bus')

A medical system can become a real threat to a patient, even from a remote location and even though it is not necessarily connected to this patient. Patients and medical professionals have to rely on proper functioning of such devices. These systems need to be operated safely and not induce user errors. Design implications regard also the human/machine interaction and the user training. Electromagnetic interference and compatibility problems are huge, especially regarding those devices that are PE-controlled. Interference issues are the more relevant as 'foreign', i.e. non-medical systems come into the hospitals in an uncontrolled way.

3. Activities and Progress to Date

The main activities focus on the development of safety cases for medical devices. A generic example for hospital beds will be completed in 2008. A paper on this topic has been presented on Safecomp 2007. The Roadmap Project has finished. Ongoing work regards the Programmable Electrical/Electronic Medical Systems (PEMS) Guideline. The development of a position paper on risk analysis regarding medical systems (see below) gave rise to submit review comments concerning the standard ISO/IEC 14971 on risk management and the standard on software life cycle

processes, IEC 62304. Other subgroup work includes review of papers and other sources of possibly relevant information and contributing to the standards development by commenting on international draft standards.

4. PEMS Guideline

In co-operation with other TC7 subgroups, the Medical Devices Subgroup targets at a guideline in which the different categories of stakeholders may get guidance on effective and robust development, market approval, purchase and use of software systems for use in medical applications for effective control of device-related risks. The guideline will help different stakeholders in the medical domain to assess user needs, identify context-specific risks, and specify functional requirements for PEMS within a variety of operational contexts.

The safety life cycle is the core for guidance given to users, manufacturers and certifying bodies regarding the specification and evaluation of DOs and DON'Ts for and approval of PEMS. The guideline is restricted to safety- or availability-critical PEMS.

5. Roadmap Project

The Roadmap Project is focussed on issues relating to the use of computer-based systems in safety related applications. The aim of the project is to create a guideline document, which will assist users and suppliers and other interested parties in navigating through the different standardisation and regulatory environments that currently exist between countries and industrial sectors. In part 1 of the project a description of the standardisation and regulatory environments is presented for a total of 17 examples selected from 8 countries and 6 sectors. The MeD Subgroup took care of the medical sector. In part 2 of the Roadmap Project a description of the regulatory requirements is presented for a total of 17 examples selected from 10 countries and 6 sectors. In 2002, the medical sector has been covered in part 3 of the Roadmap Project about the applicability of the international standard for information security management ISO/IEC 17799 and the German Baseline Protection Manual to the special needs of safety critical systems. These documents are available from the EWICS website (www.ewics.org).

6. Position Paper on Risk Analysis Regarding Medical Systems

The topic of assessment of System Integrity Levels (SILs) for PEMS requires special consideration with regard to the weighing of expected benefits of therapeutic or diagnostic functions against iatrogenic risks for patients in different classes of initial health condition. The translation of risk concepts from the industrial towards the medical sector deserves thorough reflection. Therefore, a position paper on this topic is envisaged.

7. Work Plan

EWICS TC7 has produced guidelines on relevant aspects of PE-controlled critical systems. Relationships will be made explicit between the specific topic of the PEMS guideline, other TC7 guidelines, and existing standards. The development of an example safety case for networked medical systems has been initiated in 2008 together with the Security Subgroup. Also, a third medical devices workshop with industry, regulators, users, etc., has been organised in conjunction with Safecomp 2008 in Newcastle (UK).

8. Contacts and Membership

The Medical Devices Subgroup welcomes new members to participate in the development of the guidelines, to review the work as it matures and to provide information on particular problems and practices related with medical devices. Additional liaisons are being sought with industry, licensing bodies and other committees working in the domain of medical devices. For information about the Medical Devices Subgroup or EWICS TC7 in general please visit the website www.ewics.org or contact the subgroup chair:

- **Floor Koornneef** (Chairman), Delft University of Technology, TPM – Safety Science Group, Jaffalaan 5, 2628 BX Delft, The Netherlands, tel: ++31 15 2786437, fax: ++31 15 2787155, e-mail: f.koornneef@tudelft.nl, www.vk.tbm.tudelft.nl
- **Udo Voges** (Vice-Chairman), Forschungszentrum Karlsruhe, IAI - Institute for Applied Computer Science, Postfach 3640, 76021 Karlsruhe, Germany, tel: ++49 7247 825725, fax: ++49 7247 825786, e-mail: voges@iai.fzk.de