EUROPEAN WORKSHOP ON INDUSTRIAL COMPUTER SYSTEMS TECHNICAL COMMITTEE 7 Reliability, Safety, Security		WP: 1900 – 1.2 Date: 2007-09-05 Status: Released Classification: Public

ACKNOWLEDGEMENTS:
This work was funded by the members' affiliations.

SUBGROUP
MAINTENANCE OF DIVERSE SYSTEMS (MDS)

Briefing Paper

Specific Requirements for Maintenance and Modification of Redundant and Diverse Safety Critical Systems

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 "Maintenance of Diverse Systems (MDS)" subgroup carries on the work of the former "System Integrity (SI)" subgroup, whose concern was the maintenance of safety related computer systems. The SI subgroup has already published a guideline, and now the MDS subgroup has started a new work item titled "Specific Requirements for Maintenance and Modification of Redundant and Diverse Safety Critical Systems".

To stimulate new input and further progress, a half-day workshop was organized in April 2003 during the EWICS Spring meeting in Rotterdam, and a panel session on "Dependable Embedded Systems: Roadmap and Challenges from Requirements to Maintenance" was held at SAFECOMP 2003 in Edinburgh. In January 2005, a "Workshop on Diversity" took place at the EWICS winter meeting in London.

2. Problem Statement

The "Guidelines on the Maintenance and Modification of Safety Related Computer Systems" of the System Integrity-Subgroup, published in book 2 of the series "Dependability of Critical Computer Systems" (Elsevier Applied Science), takes a very rigorous view of the procedures to be applied in the maintenance and modification of critical computer systems. But it does not address the specific problems of maintaining diverse and redundant systems.

"Diversity", i.e. the application of different methods in a redundant manner to perform the same task, is used in avionics, spacecraft, nuclear power plants, telecommunications, access and security control systems, railway interlocking and process control, in hardware as well as in software. Diversity is mainly used to cope with design faults of a system and specific risks and hazards implied by the environment of the system. Several standards and guidelines recommend diversity in hardware, software or both for the highest safety levels. Especially when dealing with software, the problem of common mode failures is reduced by applying diverse software paths, since all software faults are logical faults (mainly specification or design faults).

The aim of the new work item is to provide guidance on handling maintenance and modification of redundant and diverse systems.

The guideline will:

- Provide (according to the safety integrity levels 1-4 as defined in IEC 61508) guidance on all aspects related to maintenance and modification of diverse and redundant systems to preserve the desired integrity level.
- Support the documentation of the maintenance process, to guarantee the compliance of the diversity/redundancy requirements as implied by the safety integrity levels and system requirements.
- Complement the existing guidelines of EWICS TC7 for maintenance and modification. The guideline concentrates on the problem of keeping or adapting the required diversity/redundancy level to guarantee the expected safety level.

3. Progress to Date

The MDS-subgroup began by examining the basic concepts underlying the use of redundancy and diversity (Part II of the draft guideline: Redundant/Diverse System Architectures and Concepts, thus providing additionally some basic guidance on redundancy and diversity). Human – machine diversity was identified as a new issue important in complex systems having very high interactions with their real-world environment. Further levels of diversity will be investigated including diverse security strategies and use of dissimilar degrees of formalism. In order to structure the discussion a classification of different redundancy/diversity levels is required. The MDS-subgroup will develop a classification scheme and identify a system of metrics for redundancy/diversity in order to be able to evaluate the redundancy/diversity level of a system (Annex of the draft guideline).

The main work of the subgroup will be devoted to the task of providing guidance on management of maintenance of redundant/diverse systems (Part III of the draft guideline). This is done by looking at the safety implications of system architectures and concepts in general and especially on the maintenance life cycle. Management of redundancy and diversity during the maintenance life cycle includes definition of preconditions, identification of activities and strategies, execution of planned activities, safety impact assessment, revalidation, re-integration, documentation and human factors in the broad sense. Part IV is intended to provide a comprehensive set of examples from different application areas.

Another important point is the role of the ”Safety Case”, the arguments of which shall not be violated by maintenance and enhancement activities.

The intended audience of the guideline will include customers, suppliers, developers/designers, assessors/certification organisations, authorities, maintenance staff, safety managers, safety and standardisation bodies.

4. Contacts and Membership

The MDS subgroup welcomes new members willing to contribute to the development of the guideline, to review the work as it matures and to provide information on particular methods and tools. For information about the MDS subgroup or EWICS TC7 in general please visit the website www.ewics.org or contact:

Erwin Schoitsch (Chairperson)
Austrian Research Centers - ARC
Smart Systems Division
Tech Gate Vienna,
Donau-City-Straße 1
A-1220 Vienna, Austria
tel: ++43 50550 4117, fax: ++43 50550 4250
E-mail: erwin.schoitsch@arcs.ac.at

Francesca Saglietti (Vice-Chairperson)
Department of Software Engineering
University of Erlangen-Nuremberg
Martensstrasse 3
91058 Erlangen, Germany
tel: ++49 9131 85 -27870 / -27877
fax: ++49 9131 85 28746
E-mail: saglietti@informatik.uni-erlangen.de