EWICS TC7 – an insider's tip for safety and security guidance[1]

by Odd Nordland

Introduction

The European Workshop on Industrial Computer Systems (EWICS) was founded in 1974 as the European branch of the International Purdue Workshop on Industrial Computer Systems. Of the original 14 technical committees, only TC7 – on Reliability, Safety and Security – has survived.

The goal of EWICS TC7 is 'to promote the economical and efficient realisation of programmable industrial systems through education, information exchange and the elaboration of standards and guidelines'. To this end, EWICS assesses the state of the art for methods and tools for the development of critical industrial computer systems and produces guidelines and position papers on the development and assessment of safe and secure systems. These guidelines are often inputs to standardisation committees, and EWICS's work was a substantial contribution to IEC 61508.

Membership of EWICS is free; there is no obligation to attend meetings (which are held three to four times a year in various European locations). Much of the work is conducted off-line and coordinated electronically. More information can be found on the EWICS web site (www.ewics.org).

EWICS TC7 subgroups

EWICS TC7 sets up subgroups to work on specific topics. The subgroups determine their own scope of work, their work plan, and the guidelines and position papers that they want to produce. This allows them to act on the needs of the relevant industry and adapt their work to changing contexts. Some subgroups have been dissolved after having completed their work, others emerge as new questions arise and technologies develop. Currently, the following subgroups are active:

- Maintenance of Diverse Systems (MDS);
- Medical Devices (MeD);
- Security of Safety-critical Computer Systems (SEC);
- Education and Training in Dependable Systems Engineering (E&T);
- Object-oriented Software in Safety Systems (OOSS).

Some previous subgroups that have been dissolved are:

- Project Management (PM);
- Safety Aspects of Distributed Systems (SADS);
- Programmable Logic Controllers (PLC);
- Industrial Applications of Formal Methods (FM);
- System Integrity (SI).

The MDS subgroup is a continuation of the former SI subgroup that was concerned with the maintenance of safety-related computer systems. The SI subgroup's guideline was published in [1]. The MDS subgroup is currently working on a guideline on *Specific Requirements for Maintenance and Modification of Redundant and Diverse Safety-critical Systems,* which is planned to become available in 2009. The guideline addresses not only customers, end users, suppliers, developers, designers and maintenance staff, but also assessors, certifiers, licensing authorities and standardisation bodies.

The MeD subgroup focuses currently on the development of safety cases for medical devices, and a generic example for hospital beds is being completed (see also [2]). In

[1] Published in Safety Systems (the Newsletter of the UK's Safety-Critical Systems Club), Vol. 18, No. 2, January 2009. The Newsletter's editor is Felix Redmill, who may be contacted at Felix.Redmill@ncl.ac.uk

addition, work is being done on a guideline for Programmable Electrical/Electronic Medical Systems in cooperation with other TC7 subgroups. The guideline is intended to help stakeholders assess users' needs, identify risks, and specify functional requirements within various operational contexts.

The SEC subgroup's objective is to provide guidance on '*... how to comply with national and international standards, guidelines and legal restrictions ... in protection against security breaches.*' The subgroup has produced briefing papers on 'Information Security Management' [6], 'Information Operations – Targets, Means and Weapons' [7] and a case study on the security of power substations [8]. They are summarised later in this text. It is currently working on a briefing paper on Remote Access.

The E&T subgroup addresses the lack of educational programmes for dependability engineering. The subgroup is working on a position paper that will identify courses, thematic modules, and topics that are relevant to effective design and safe and secure operation of dependable computer systems. It will also propose necessary improvements to current curriculae.

The OOSS subgroup is the newest in EWICS TC7. It was set up in January 2008 to develop guidelines on the use of object oriented software in safety-critical systems, identifying restrictions and limitations and giving guidance for the assessment and certification of safety systems that are based on object oriented software.

Commercially available EWICS TC7 position papers and guidelines

EWICS TC7 has published position papers on:

- The Development of Safety Related Software;
- The Hardware of Safe Computer Systems;
- The Verification and Validation of Safety Related Computer Systems;
- The Documentation of Safety Related Computer Systems;
- Techniques for the Verification and Validation of Safety Related Software;
- System Requirements Specification for Safety Related Systems;
- Maintenance and Modification of Safety Related Computer Systems;
- Safety Related Measures to be Used and Software Quality Assurance;
- The Design of Computer Systems for Safety;
- The Assessment of the Safety and Reliability of High Integrity Industrial Computer Systems.

These are all included in [1].

In addition, '*Safety Assessment and Design of Industrial Computer Systems – Techniques Directory*' is published in [3].

Both [1] and [3] are available from Springer by Printing on Demand.

EWICS TC7 guidelines available from the Instrumentation Society of America (www.isa.org)

Two guidelines were produced in collaboration with members of this Society.

Guidelines on Achieving Safety in Distributed Systems

'The objective of this document is to provide guidance on achieving safety in industrial computer-based distributed systems over the system life-cycle ... It is not intended that this guideline be self-contained. It should be used in conjunction with other guidance, standards and lifecycles relating to the development of safety-related systems.

'This guideline focuses exclusively on those aspects of distributed systems which influence the safety of the system.'

Guidelines for the Use of Programmable Logic Controllers in Safety Related Applications

'This document provides a guideline defining the proper use of Programmable Logic Controllers in Safety-related Systems according to Safety Integrity Levels 1-3 (typically in demand mode, de-energized to trip) as defined in IEC 61508 or according to requirements classes 1-6 as defined in DIN V 19250, in a way that:

- utilises existing and developing practices, guidelines and standards;
- considers users', procurers', developers', engineering, and certifiers'/assessors' needs;
- allows a path forward to guideline development for other programmable electronic controllers (e.g. DCSC = distributed control system controller, SLC = single loop control etc.);
- allows guideline users to implement computer technology to improve safety in their plants.

'Higher safety integrity levels such as SIL 4 (IEC 61508) or requirements classes 7/8 (DIN V 19250) typically require additional design considerations that are not provided in this guideline.'

The latter is also downloadable from the EWICS TC7 web site (www.ewics.org).

Guidelines that are available from the EWICS TC7 web site

The above mentioned guidelines and briefing papers are commercially available; in addition, EWICS TC7 has a number of papers available for free on its web site.

Guidance on the use of Formal Methods in the Development and Assurance of High Integrity Industrial Computer Systems

This document ([4] and [5]) is intended as a companion to standards that require or recommend the use of formal methods. It provides an appraisal of formal methods and an introduction to their use. It is intended for project managers, developers and users, as well as assessors. It is divided into three parts:

- Part 1 describes how to use the guideline;
- Part 2 contains the actual guidance;
- Part 3 is a directory of formal methods.

Briefing Paper in Information Security Management

This document ([6]) reviews work that is being done on standards and guidelines for the management of information security. Information contained in the paper can be used for implementing security in safety systems.

Information Operations – Targets, Means and Weapons

This article ([7]) describes terms such as Information Warfare, Information Operations, Information Assurance, and Cyberwar, and provides technical descriptions of important concepts. It considers both national and supranational aspects and provides recommendations for an information defence programme.

Electric Power Systems Cyber Security: Power Substation Case Study

This case study ([8]) presents the physical and organisational structure of an electric power system and describes the basics of electric power control. Hazards in connection with the use of computer-based systems are described, emphasising the differences between the safety of an electric power system as compared to process control systems. The current state of the art is presented and a security analysis of a software interlocking system based on an extra-high voltage subsystem case study is provided as an example.

Roadmap Reports

The ROADMAP project was carried out for the Joint Research Centre ISPRA (www.jrc.ec.europa.eu). The following reports are downloadable:

- *The collection and categorisation of worldwide standards relevant to the use of programmable electronic systems in safety-related applications [9];*

- *The standardisation and regulatory environment relating to the use of programmable electronic systems in safety-related applications [10];*
- *The standardisation and regulatory environment for the application of worldwide standards relevant to the use of programmable electronic systems in safety-related applications [11];*
- *A study of the applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the needs of safety-critical systems [12].*

Conclusion

EWICS TC7 has produced, and is producing, a variety of guidelines and briefing papers that can be of assistance to practitioners involved with the safety and/or security of industrial computer systems. The guidelines are produced by experts in the respective fields, coming from industry, academia, and governmental and regulatory organisations, and are made readily available to the safety and security communities. There are further guidelines in production, and experts are invited to participate in EWICS TC7 work in order to assure the quality and usability of the guidelines.

EWICS TC7 is also the organiser of the SAFECOMP conferences (see also www.safecomp.org) and informs delegates at SAFECOMP about the ongoing work. Nevertheless, there is still a low level of awareness that expert guidance is constantly available through EWICS TC7. Feedback and – more important – participation in our work will be greatly appreciated.

Acknowledgements

Much of the above text is derived from the EWICS papers themselves and the author does not claim to be the originator. Since EWICS is a dynamic organisation, membership varies over time and it is not always possible to identify the names of the persons responsible for particular wording. Credit belongs therefore to all members of EWICS TC7, both past and present.

References:

[1] F Redmill (editor). *Dependability of Critical Computer Systems – Vol. 1 and 2.* Springer Verlag, ISBN 1 85166-389-1

[2] M-A Sujan, F. Koornneef, U Voges. Goal-Based Safety Cases for Medical Devices: Opportunities and Challenges. in *Lecture Notes on Computer Science 4680.* Springer Verlag, ISBN 3-540-75100-9

[3] P Bishop (editor). *Dependability of Critical Computer Systems – Vol. 3.* Springer Verlag, ISBN 1 85166-544-7

[4] S O Anderson, R E Bloomfield, G L Cleland (editors). *Guidance on the use of Formal Methods in the Development and Assurance of High Integrity Industrial Computer Systems Parts I and II.* Working paper 4001. http://www.ewics.org/attachments/formal-methods-subgroup/wp4001v10_fm_guide_parts1and2.pdf

[5] S O Anderson, R E Bloomfield, G L Cleland (editors). *Guidance on the use of Formal Methods in the Development and Assurance of High Integrity Industrial Computer Systems Part III.* Working paper 4002. http://www.ewics.org/attachments/formal-methods-subgroup/wp4002v10_fm_guide_part3.pdf

[6] P Daniel (editor). *Briefing paper in Information Security Management.* Working paper 5016. http://www.ewics.org/attachments/security-subgroup-bps/Information+Security+Management+V1.pdf

[7] P Daniel, E Luiijf (editors). *Information Operations – Targets, Means and Weapons.* Working paper 5017. http://www.ewics.org/attachments/security-subgroup-bps/Information+Operations+V1.pdf

[8] Z Zurakowski (editor). *Electric Power Systems Cyber Security: Power Substation Case Study.* Working paper 5086. http://www.ewics.org/attachments/security-subgroup-bps/Electric+Power+Systems+Cyber+Security++WP+5086+V1_1.pdf

[9] M v d Meulen, I C Smith (editors). *The Collection and Categorisation of Worldwide Standards Relevant to the Use of Programmable Electronic Systems in Safety Related Applications.* http://www.ewics.org/attachments/roadmap-project/RdMapD10.pdf

[10] I C Smith (editor). *The Standardisation and Regulatory Environment Relating to the Use of Programmable Electronic Systems in Safety Related Applications.* http://www.ewics.org/attachments/roadmap-project/RdMapD21.pdf

[11] I C Smith (editor). *The Standardisation and Regulatory Environment for the Application of Worldwide Standards Relevant to the Use of Programmable Electronic Systems in Safety Related Applications.* http://www.ewics.org/attachments/roadmap-project/RdMapD22.pdf

[12] I C Smith (editor). *A Study of the Applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the Needs of Safety Critical Systems.* http://www.ewics.org/attachments/roadmap-project/RdMapD31.pdf

Odd Nordland is at SINTEF ICT in Trondheim, Norway. He may be contacted at Odd.Nordland@sintef.no