EUROPEAN WORKSHOP ON INDUSTRIAL COMPUTER SYSTEMS TECHNICAL COMMITTEE 7 Reliability, Safety, Security		WP: 5900 – 2.0 Date: 2007-07-10 Status: Released Classification: Public

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

SUBGROUP
SECURITY OF SAFETY CRITICAL COMPUTER SYSTEMS
Briefing paper

1. Introduction
EWICS TC7 (European Workshop on Industrial Computer Systems, Technical Committee 7, Reliability, Safety and Security) is an international workshop of experts in the field of dependability of industrial computer systems regarding reliability, safety and security. In 1988, the Security Subgroup was set up within EWICS TC7.

Before the Security Subgroup was set up, the committee had concentrated on producing guidelines and pre-standards in the field of safety critical industrial computer systems. These guidelines have been published in three books, "Dependability of Critical Computer Systems, Vol. 1-3" by Elsevier. Using this base of experience and inviting other experts involved in security critical applications, the security subgroup started work on the security of industrial computer systems, especially safety critical systems. The work is being undertaken in co-operation with other subgroups of EWICS TC7 such as "Medical Devices" and "Maintenance of Diverse Systems". During this time, security standards have also been evolving at international, European and national levels. These standards are being reviewed by the subgroup and if applicable will be incorporated within the guidelines and briefing papers.

2. Problem Statement
Within Europe, there are different levels of awareness of security of computer systems. In some countries, the government is promoting initiatives on computer security. Legislation is emerging throughout Europe affecting both users and suppliers. The emergence of the IT Security Evaluation Criteria (ITSEC), the Common Criteria (CC), and ISO/IEC 17799 & 27001, the standard for information security management and the certifications based on these standards, have promoted awareness within the IT-community. Also, codes of practice for the management of information security are being produced both internationally and nationally. Within many countries, initiatives are in place for protecting critical national infrastructures, including safety critical systems, such as transportation, utilities and telecommunication systems.

Industrial systems range from small PC based systems to large, geographically separated and complex process control systems. Since security cannot just be a bolt on item, a specialised knowledge in the areas of specification, design and development, operation and maintenance of industrial computer systems is required. An understanding of the safety aspects will also be required to ensure that techniques for both safety and security can be applied in a mutually supportive manner. Security certification of such systems will also require detailed knowledge of these systems, since security will need to be inherent in the total development of the system. Within the industrial computer systems community, security awareness has not been as widespread especially when considering safety critical applications.

The objective of the subgroup is to provide guidance to purchasers and groups responsible for secure operation on what to specify with regard to security and how to undertake the specification process; to suppliers on how to satisfy the security requirements, while maintaining security during the project lifecycle and to users on how to manage and maintain security in their industrial safety critical computer systems.

3. What is Needed

With the emergence of both European security standards and legislation, guidance is required for the application of these standards and the interpretation of this legislation to those involved in industrial computer systems. This guidance should address all the security issues of industrial computer systems from design through to development, operations, maintenance and decommissioning. These guidelines should give a generic overview of the security requirements within the lifecycle phases together with references to the applicable standards and more detailed information. Examples of the implementation of these generic guidelines should be given with a bias to industrial safety critical computer systems. Guidance is needed for both suppliers and persons responsible for operation and purchasing on how to comply with national and international standards, guidelines and legal restrictions, with necessary subsets or supersets of these in the protection against security breaches.

4. Progress to Date

The subgroup, which has over thirty members from twelve European countries as well as the US and Brazil, meets up to four times a year. The members are from industry, government and research institutions. The industrial members have a range of experience in secure systems, access control, surveillance, transportation, process control, atomic energy, telecommunications and standardisation. Government agencies include the regulatory, assessment and testing authorities. Liaisons have been formed with other committees working in the security domain such as International standardisation organisations.

Information from the members' countries, from standardisation organisations and from contacts with their national security organisations has been disseminated through the subgroup and where possible comments have been fed back to the originators. In addition to information from security organisations, members have provided information on security aspects implemented by their own companies, especially in the case of security policies and procedures. This has provided the subgroup with the baseline information to produce generic security guidelines and case studies, in the form of briefing papers. These papers provide guidance to designers, developers, regulators and users of safety-critical computer systems. Briefing papers have been produced on ‘Information Security Management’, ‘Information Operations - Targets, Means and Weapons’ and a power substation security case study.

About every two years, the subgroup holds a symposium on security of safety critical computer systems, and SAFECOMP, the annual EWICS TC7 conference, normally includes a security session. The subgroup was involved in the EWICS TC7 Roadmap project for the European Commission Joint Research Centre. A guideline on navigating through the different standardisation and regulatory environments of countries and their industrial sectors was produced. In 2003, a study on the applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the needs of safety critical systems was completed. Through IEC SC65C/WG13 & WG10, the subgroup is involved in the international standardisation of industrial process monitoring and control security. The subgroup is a stakeholder in a number of European projects involved in critical infrastructure protection.

5. Future Work

Briefing papers are being prepared on Security Activities in the Safety Lifecycle, and Remote Access to Safety Critical Systems. Potential future briefing papers include Digital Signatures, Trusted Third Parties, Safety & Security Analysis, Requirements Definition, Evaluation & Certification and the use of PC based systems. The next symposium on security in safety related computer systems is planned for 2008. Future case studies include security issues in medical and rail applications.

For further information on the Security subgroup visit the website www.ewics.org or contact:

Peter Daniel (Chairman) e-mail: pete.daniel@selex-comms.com	**Odd Nordland** (Vice Chairman) e-mail: odd.nordland@sintef.no