A STUDY OF THE APPLICABILITY OF ISO/IEC 17799 AND THE GERMAN BASELINE PROTECTION MANUAL TO THE NEEDS OF SAFETY CRITICAL SYSTEMS

EXECUTIVE SUMMARY

March 2003

OF WORK CARRIED OUT FOR JRC ISPRA

UNDER CONTRACT N° 20215 – 2002 - 12 F1EI ISP GB

BY

MEMBERS OF

THE SYSTEMS SECURITY, RAIL AND MEDICAL SUBGROUPS OF THE EUROPEAN WORKSHOP ON INDUSTRIAL COMPUTER SYSTEMS

TECHNICAL COMMITTEE No. 7

Reliability, Safety & Security

EWICS TC7

Edited by

Ian C Smith

Campbell Love Associates

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS REPORT WAS PREPARED BY THE ORGANISATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED BY JRC ISPRA. NEITHER JRC ISPRA OR ANY MEMBER OF JRC ISPRA, THE ORGANISATION(S) NAMED BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM;

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS REPORT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS REPORT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF JRC ISPRA OR ANY JRC ISPRA REPRESENTATIVE, OR THE ORGANISATION(S) NAMED BELOW OR ANY REPRESENTATIVE OF THESE ORGANISATION(S) HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS REPORT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS REPORT.

CAMPBELL LOVE ASSOCIATES

EWICS TC7

Comments or questions to this report may be directed to either

Peter Daniel
Chairman EWICS TC 7 Security Subgroup
Marconi Selenia Secure Systems, Wavertree Technology Park
Liverpool L7 9PE
United Kingdom
e-mail: pete.daniel@marconiselenia.com

or

Udo Voges
Chairman EWICS TC 7
Forschungszentrum Karlsruhe
IAI
Postfach 3640
76021 Karlsruhe
GERMANY
e-mail: udo.voges@iai.fzk.de

© EWICS TC7 2003

CONTENTS

1. TERMS OF REFERENCE FOR THE STUDY

This executive summary presents the highlights of a study carried out by members of EWICS TC7 (the European Workshop on Industrial Computer Systems - Technical Committee 7 Reliability, Safety & Security) of the applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the needs of safety critical systems**.** The work carried out was jointly funded by members' affiliations and by the funding made available under Contract N° 20215 – 2002 - 12 F1EI ISP GB from JRC Ispra.

EWICS TC7 (the European Workshop on Industrial Computer Systems - Technical Committee 7 Reliability, Safety & Security) meets four times per year. Its membership covers representatives from regulators, industrial users, researchers and members of standards committees. It produces guidelines, holds workshops and each Fall runs a specialist conference - SAFECOMP. EWICS TC7 has been an active group since the mid 1970's - there is no restriction to membership - all interested experts are welcome to attend. The Systems Security subgroup was set up over 10 years ago and since 1994 has followed closely and contributed to the evolution of standards in its field.

A previous study[1], similarly sponsored by JRC Ispra and carried out by members of EWICS TC7, examined the extent to which existing standards addressed the security of the information and communications technology (ICT) systems used in safety related applications. This is a matter of increasing concern as public and private networks become more and more interconnected providing the communications for safety critical systems as a part of critical national infrastructures.

The study found that there was currently no code of practice specifically covering the security management aspects of safety critical systems. Such a code of practice would provide a common basis for European safety critical industry to develop, implement and maintain effective security management practice. There is also no standard or guideline that specifically recommends baseline security protection measures for these systems. It would be helpful if there existed a common basis for European industry to determine appropriate

[1] "The Standardisation And Regulatory Environment for the application of worldwide standards relevant to the use of Programmable Electronic Systems in Safety Related and Security Applications - Part II - National Regulatory Requirements" issued in May 2001. Can be accessed at http://www.ewics.org/vanilla/uploads/public/RoadMap/RdMapD22.pdf.

baseline protection measures to counter security threats for safety critical systems. A risk assessment technology could be developed to determine if a higher level of security above the baseline is needed. An infrastructure may be required to certify an organisation's conformance to these standards and guidelines.

In the light of the increasing importance attached to ensuring that safety critical systems can withstand security threats, the study recommended that work should be undertaken to establish a code of practice specifically covering the security management aspects and baseline protection measures for safety critical systems.

As a first step the international standard for information security management ISO/IEC 17799 and the German Baseline Protection Manual should be evaluated as to their applicability to the special needs of safety critical systems. The aim of the evaluation would be to determine whether:

1. the standard and the baseline protection manual adequately address the needs of safety critical systems or;

2. the standard and the baseline protection manual would benefit from an associated guidance document covering the application of the standard and the baseline protection manual to safety critical systems or;

3. a separate standard and the baseline protection manual (or an addendum to the existing standard) specifically addressing the needs of safety critical systems would be beneficial.

This executive summary gives an overview of the work carried out, the approach taken, a summary of the results, the conclusions arrived at and the recommendations made. The work carried out in the study is more fully detailed in the final report[2] published on the study.

[2] "A study of the applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the needs of Safety Critical Systems" – Final Report " issued in March 2003.

2. APPROACH

The method used to evaluate the applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the needs of safety critical systems was as follows:

Individuals who are experts in their field prepared a one-page description of a generic example of a safety critical system in each of four industrial sectors. The sectors chosen are nuclear, rail, medical and power distribution.

The nuclear example described the control system, the protection system and the monitoring system on a generic example of a nuclear power plant.

The rail example described the communication between the train and the traffic control (including GSM-R), the signalling system with associated track circuits, vehicle control, converter (traction) control and brake control.

The medical example described a surgical robot (or telemanipulation system) used to carry out a surgical procedure on the patient under the supervision of the medical doctor (surgeon).

The power distribution example described a generic electrical power distribution system consisting of extra-high voltage (EHV) transmission networks, main load centres, local high-voltage (HV) networks together with associated EHV substations and main HV substations controlled by substation automation systems (SAS).

These experts were asked to assume that they had been tasked with identifying the security requirements for such a system, implementing appropriate protection measures and setting up an appropriate security management system covering all phases of the system lifecycle. They were further asked to assume that their expertise did not cover any security aspects and that they were seeking guidance to enable them to carry out these tasks. They were then asked to evaluate the applicability of the guidance given in ISO/IEC 17799 and the German Baseline Protection Manual, to these tasks for their particular example. They assessed the applicability of each section of the documents as being either:

> Not applicable (NA) – not of particular use for their example system even if applicable to other systems e.g. e-commerce etc. or;
>
> Applicable (A) – of use in their role of ensuring that the safety of their example system is not compromised through any breach of security or;

Very applicable (VA) – virtually essential – a key requirement to ensuring that the safety of their example system is not compromised through any breach of security.

They also commented as to whether the text as written was:

OK - can be interpreted for use for safety critical systems without any additional guidance or;

AG - additional guidance would be beneficial.

Finally for each section of the documents they stated whether in their opinion and in relation to the issues covered by this section, there are any important aspects particular to the security of safety critical systems that have not been adequately addressed – (YES/NO).

NO – there are no important aspects particular to the security of safety critical systems that have not been adequately addressed.

YES – The following important aspect(s) particular to the security of safety critical systems have not been adequately addressed.

3. SUMMARY OF RESULTS

According to IEC 61508, a safety-related system comprises everything (hardware, software and human elements) necessary to carry out one or more safety functions, where failure of the safety function would give rise to a significant increase in the risk to the safety of persons and/or the environment. The consequences of failure could also have serious economic implications. IEC 61508 provides guidance throughout the complete lifecycle for such systems (specification, design, manufacture, operation, etc.).

To each identified safety function is ascribed a safety integrity level. A safety integrity level (SIL) corresponds to a range of target likelihood of failures of a safety function. The higher the SIL level (from 1 to 4), the higher the requirements for the safety function and the lower the required probability of the safety function not being carried out correctly when required to do so. IEC 61508 gives guidance on good practice that should be followed to achieve a required SIL level.

Both the documents studied are strongly focussed on business information assets and its processing and so understandably make no reference to IEC 61508. However, for the designers and users of safety critical systems, how the security life cycle sits alongside the safety life cycle as defined in IEC 61508 is of prime importance. The relationship between the security requirements and the SIL (Safety Integrity Level) of the safety functions to be carried out by safety system is an important issue. As is the relationship between the hazard and operability study or similar safety risk analysis required for safety critical systems as specified in IEC 61508 and the assessment of security risks as specified in both documents. New guidance documents are required to cover these aspects.

Many safety critical systems form part of and/or have a high reliance on critical national infrastructures. The protection of critical information infrastructures has become a key action in most information age countries. Critical information infrastructure protection programmes have been set up providing information on threats and vulnerabilities.

The threat to an individual computer based safety critical system from potential breaches of security is that its ability to carry out its designated safety functions when it is required to do so is impaired. Since the system is computer based, preserving the integrity of relevant information and ensuring that it continues to be correctly processed is of prime importance. However security breaches affecting other aspects e.g. hardware, human factors, etc. could also potentially degrade the safety functionality of the

system. New guidance documents should address the security of the whole safety system and its associated safety functions rather than just of the information within the safety system and its processing.

The following aspects particular to the security of safety critical systems were found to be not adequately addressed in the two documents studied:

- the role of and interaction with regulatory bodies
- cross-references to IEC 61508
- the relationship between the security lifecycle and the safety life cycle
- the relationship between the risk analysis carried out to determine safety requirements and the risk assessment mentioned in the documents to determine security requirements
- detailed guidance on a standard risk assessment methodology for the security of computer based safety related systems
- the potential impact of technical measures applied for ensuring security of real-time systems on their real-time properties as well as their availability, reliability or other attributes
- the relationship between levels of security required and the safety integrity level (SIL) required by a safety function
- the coverage of the vulnerability of a safety system during access for maintenance is not detailed enough – both on-line and off-line maintenance should be addressed.
- there is no detailed reference to a "permit to work" procedure. Such a procedure is not normally focussed on defending against intentional acts of sabotage but is generally focussed on:
    - the safety of maintenance staff by ensuring that the equipment under maintenance is electrically isolated
    - preserving sufficient acceptable though possibly degraded functionality while carrying out on-line maintenance
    - ensuring that the full functionality of the safety system has been restored following maintenance
- while event reporting is covered no mention is made of mandatory requirements on reporting laid down by regulatory bodies for safety systems.

- there is no discussion on how a security management system relates to a quality management system (ISO 9000 series), an environmental management system (ISO 14000 series) or a safety management system (IEC 61508). Is there a need for a separate, independent chain of command up to the highest management levels for each of these systems or is some combination acceptable?

- Distributed control and protection systems are not adequately covered.

New guidance documents should address these aspects.

In new documents providing guidance on the security of computer based safety systems it might be reasonable to consider separately the threats, vulnerabilities and counter-measures for each of the following classes of system:

- Protection system
- Control system
- Monitoring system
- Associated non-safety related systems

And as subclasses:

- Operating system software/firmware/hardware
- Application programmes software/firmware/hardware
- Communication software/firmware/hardware
- Human factors

Together with associated information sub-classes:

- Data for control settings
- Data for protection settings
- Data for monitoring leading to safety related human actions
- Data for monitoring system health for maintenance purposes
- Data which is not directly or immediately safety–related but which could be security sensitive

While there are a large number of aspects which have both a safety and a security implication there may be aspects that have either a security implication without having a direct safety implication or a safety implication without having a direct security implication. New guidance documents should cover this aspect.

Hardware/software/firmware maintenance and periodic testing to preserve the integrity of hardware components provides the possibility of detecting sabotage. New guidance documents should discuss the extent to which periodic testing can be used to reveal the occurrence of intentional sabotage.

Currently security requirements for information and information processing systems used in connection with the following:

- Design and development
- Specifications
- Safety requirements
- Hazard and operability analysis
- Choice of suppliers
- The supply chain
- Maintenance and operational procedures
- Work instructions

Are put in place primarily to;

- Preserve commercial confidentiality
- Protect intellectual property rights
- Assure quality

And not primarily to defend against intentional sabotage attacks. New documents should cover the additional requirements to counter potential threats to security.

The extent to which redundancy and diversity that is already used to improve reliability and safety can also counter security threats should be addressed.

The use of COTS (commercial-off-the-shelf) software and SOUP (software of uncertain pedigree/provenance) should also be re-examined. Arguably

widely used software could be more readily the subject of a sabotage attack than bespoke software subject to tight security measures.

The new guidance documents should include in the text examples and concepts familiar to the designers, users and owners of safety critical systems.

Although not covered in IEC 61508, a guideline on the security of safety systems should arguably include a section dealing with sensors and actuators.

It should be noted that ISO/IEC 17799 gives only sub-optimal guidance on implementing security. It merely lists 127 controls. The Information Security Management System to build a quality system (based on the well-known PDCA (Plan-Do-Check-Act) model) for those controls is described in detail in British Standard BS 7799 Part 2:2002. That standard was recently aligned with ISO 9001, ISO 14001 and the OECD security guidelines.

Security evaluation criteria are the 'standards' against which the correctness and effectiveness of security countermeasures are evaluated. They define several degrees of rigour for the testing and the levels of assurance that each confers. They also define the formal requirements needed for a product or system to meet each Assurance level. ISO 15408, the Evaluation Criteria for IT Security, better known as the Common Criteria, represents the outcome of international efforts to align and develop existing European and North American criteria. The Common Criteria (CC) is used as the basis for evaluation of the security properties of IT products and systems. The CC permits comparability among the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and the assurance measures applied to them during a security evaluation. The applicability of the CC to the needs of safety critical systems should be studied. This would include an exploration of the relationship between the Safety Integrity Levels (SILs) defined in IEC 61508 and the Evaluation Assurance Levels (EALs) defined in the Common Criteria.

4. CONCLUSIONS AND RECOMMENDATIONS

4.1 CONCLUSIONS

Because both the documents studied are strongly focussed on business information assets and its processing and make no reference to IEC 61508, the standard and the baseline protection manual do not adequately address the needs of safety critical systems. The standard and the baseline protection manual would benefit from an associated guidance document covering the application of the standard and the baseline protection manual to safety critical systems. However because of the significant number of aspects particular to safety systems which are not covered in the two documents a separate standard and baseline protection manual (or an addendum to the existing standard and baseline protection manual) specifically addressing the needs of safety critical systems is needed. The two documents studied provide an excellent source of material and provide guidance on the structure and content for the new documents. Other source material should include the ISO/IEC TR 13335[3] series of technical reports and British Standard BS 7799 Part 2:2002.

An approach for evaluating the correctness and effectiveness of security countermeasures for safety critical systems should be developed. As a first step, the applicability of the ISO 15408 (Common Criteria) to the needs of safety critical systems should be studied. This would include an exploration of the relationship between the Safety Integrity Levels (SILs) defined in IEC 61508 and the Evaluation Assurance Levels (EALs) defined in ISO 15408.

4.2 RECOMMENDATIONS

It is recommended that:

1. A management model like that in BS7799 Part 2:2002 should also be evaluated for its adequacy as a source for a standard for the security management of computer based safety related systems.

2. A document giving a code of practice for security management for computer based safety related systems should be produced.

[3] ISO/IEC TR 13335 Series - The Guidelines for the Management of IT Security (GMITS) series of Technical Reports

3. A document giving guidance on the security of computer based safety related systems should be produced.

4. Research should be undertaken to determine the extent to which redundancy and diversity, already used to improve the reliability and safety can also act as a countermeasure to security threats.

5. A document should be produced which cross-references existing standards and guidelines for controls for safety and security critical environments, to ISO/IEC 17799 and the German baseline protection manual.

6. A standard risk assessment methodology for the security of computer based safety related systems should be developed – possibly based on an extension of HAZOP or other established safety risk analysis techniques.

7. A study is made on the need for an infrastructure to certify an organisation's conformance to any guidelines produced.

8. Research should be undertaken to determine the extent to which technical measures applied for ensuring security of real-time systems can impact their real-time properties as well as their availability, reliability or other attributes of real-time safety related systems.

9. An approach for evaluating the correctness and effectiveness of security countermeasures for safety critical systems should be developed. As a first step, the applicability of ISO 15408 (Common Criteria) to the needs of safety critical systems should be studied. This would include an exploration of the relationship between the Safety Integrity Levels (SILs) defined in IEC 61508 and the Evaluation Assurance Levels (EALs) defined in ISO 15408.