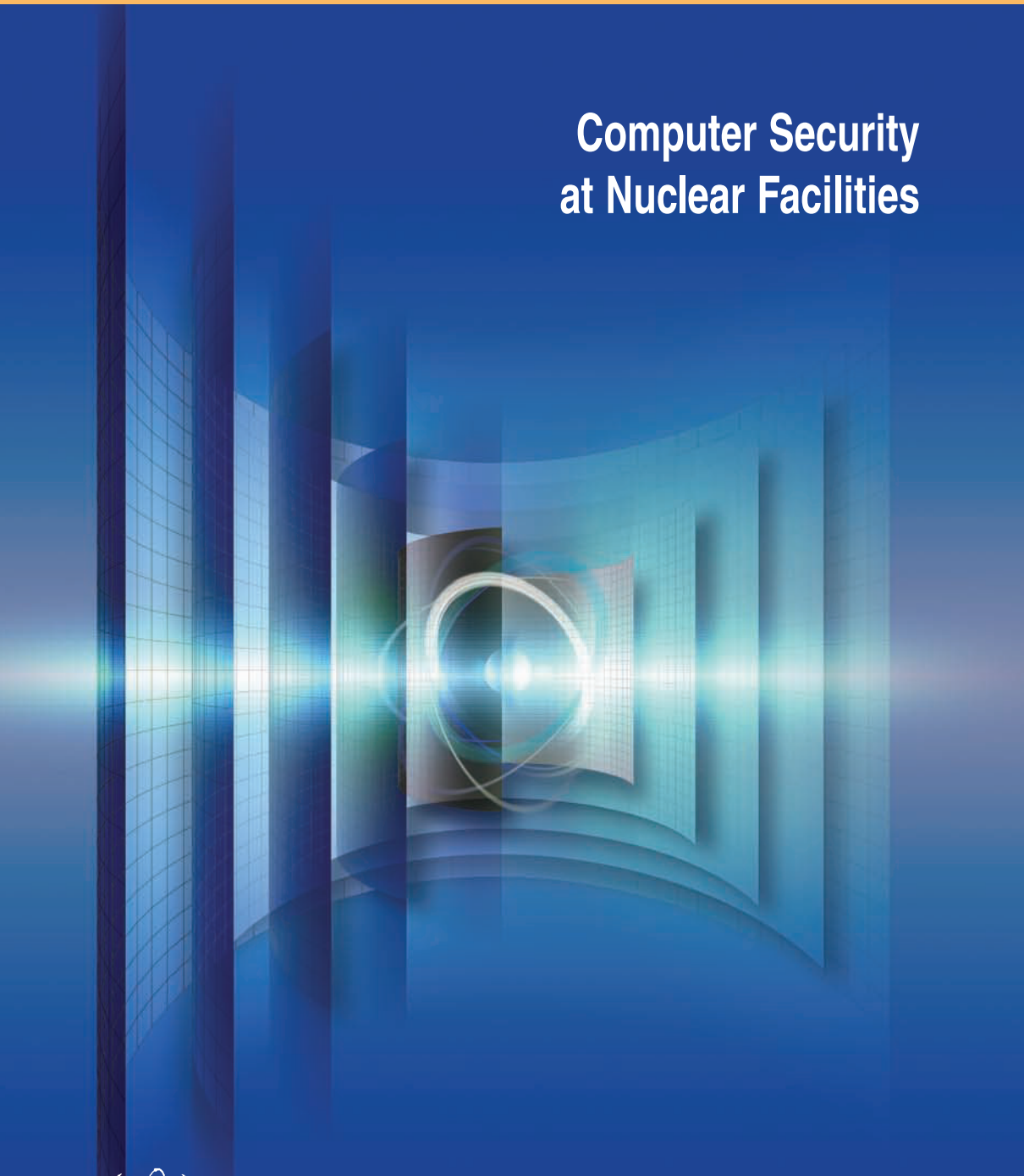
IAEA Nuclear Security Series No. 17

Technical Guidance
Reference Manual

Computer Security at Nuclear Facilities



IAEA
International Atomic Energy Agency

THE IAEA NUCLEAR SECURITY SERIES

Nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities are addressed in the **IAEA Nuclear Security Series** of publications. These publications are consistent with, and complement, international nuclear security instruments, such as the amended Convention on the Physical Protection of Nuclear Material, the Code of Conduct on the Safety and Security of Radioactive Sources, United Nations Security Council Resolutions 1373 and 1540, and the International Convention for the Suppression of Acts of Nuclear Terrorism.

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

Publications in the IAEA Nuclear Security Series are issued in the following categories:

- **Nuclear Security Fundamentals** contain objectives, concepts and principles of nuclear security and provide the basis for security recommendations.
- **Recommendations** present best practices that should be adopted by Member States in the application of the Nuclear Security Fundamentals.
- **Implementing Guides** provide further elaboration of the Recommendations in broad areas and suggest measures for their implementation.
- **Technical Guidance** publications include: **Reference Manuals**, with detailed measures and/or guidance on how to apply the Implementing Guides in specific fields or activities; **Training Guides**, covering the syllabus and/or manuals for IAEA training courses in the area of nuclear security; and **Service Guides**, which provide guidance on the conduct and scope of IAEA nuclear security advisory missions.

DRAFTING AND REVIEW

International experts assist the IAEA Secretariat in drafting these publications. For Nuclear Security Fundamentals, Recommendations and Implementing Guides, open-ended technical meeting(s) are held by the IAEA to provide interested Member States and relevant international organizations with an appropriate opportunity to review the draft text. In addition, to ensure a high level of international review and consensus, the Secretariat submits the draft texts to all Member States for a period of 120 days for formal review. This allows Member States an opportunity to fully express their views before the text is published.

Technical Guidance publications are developed in close consultation with international experts. Technical meetings are not required, but may be conducted, where it is considered necessary, to obtain a broad range of views.

The process for drafting and reviewing publications in the IAEA Nuclear Security Series takes account of confidentiality considerations and recognizes that nuclear security is inseparably linked with general and specific national security concerns. An underlying consideration is that related IAEA safety standards and safeguards activities should be taken into account in the technical content of the publications.

COMPUTER SECURITY AT NUCLEAR FACILITIES

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIETNAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

IAEA NUCLEAR SECURITY SERIES No. 17

TECHNICAL GUIDANCE

COMPUTER SECURITY AT NUCLEAR FACILITIES

REFERENCE MANUAL

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2011

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
December 2011
STI/PUB/1527

IAEA Library Cataloguing in Publication Data

Computer security at nuclear facilities : reference manual : technical guidance. — Vienna : International Atomic Energy Agency, 2011.
p. ; 24 cm. — (IAEA nuclear security series, ISSN 1816–9317 ; no. 17)
STI/PUB/1527
ISBN 978–92–0–120110–2
Includes bibliographical references.

1. Nuclear facilities — Security measures. 2. Computer security. 3. Computer networks — Security measures. I. International Atomic Energy Agency. II. Series.

IAEAL 11–00703

FOREWORD

The possibility that nuclear or other radioactive material could be used for malicious purposes cannot be ruled out in the current global situation. States have responded to this risk by engaging in a collective commitment to strengthen the protection and control of such material and to respond effectively to nuclear security events. States have agreed to strengthen existing instruments and have established new international legal instruments to enhance nuclear security worldwide. Nuclear security is fundamental in the management of nuclear technologies and in applications where nuclear or other radioactive material is used or transported.

Through its Nuclear Security Programme, the IAEA supports States to establish, maintain and sustain an effective nuclear security regime. The IAEA has adopted a comprehensive approach to nuclear security. This recognizes that an effective national nuclear security regime builds on: the implementation of relevant international legal instruments; information protection; physical protection; material accounting and control; detection of and response to trafficking in such material; national response plans; and contingency measures. With its Nuclear Security Series, the IAEA aims to assist States in implementing and sustaining such a regime in a coherent and integrated manner.

The IAEA Nuclear Security Series comprises Nuclear Security Fundamentals, which include objectives and essential elements of a State's nuclear security regime; Recommendations; Implementing Guides; and Technical Guidance.

Each State carries the full responsibility for nuclear security, specifically: to provide for the security of nuclear and other radioactive material and associated facilities and activities; to ensure the security of such material in use, storage or in transport; to combat illicit trafficking and the inadvertent movement of such material; and to be prepared to respond to a nuclear security event.

This publication is in the Technical Guidance category of the IAEA Nuclear Security Series, and deals with computer security at nuclear facilities. It is based on national experience and practices as well as publications in the fields of computer security and nuclear security. The guidance is provided for consideration by States, competent authorities and operators.

The preparation of this publication in the IAEA Nuclear Security Series has been made possible by the contributions of a large number of experts from Member States. An extensive consultation process with all Member States included consultants meetings and open-ended technical meetings. The draft was then circulated to all Member States for 120 days to solicit further comments and suggestions. The comments received from Member States were reviewed and considered in the final version of the publication.

EDITORIAL NOTE

This report does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Attention to computer security has intensified in the last decade as clear and recurring proof of the vulnerabilities of computer systems has come to light. Malicious exploitation of these vulnerabilities has been witnessed with growing frequency and impact. In an increasingly complex threat scenario, the possible occurrences of cyberterrorism as a means of attacking a State's critical infrastructure has prompted a number of national authorities to prepare defences and issue new regulations. Such regulations establish computer security requirements, which affect nuclear facilities at multiple levels and at the various stages of operation. In parallel, information security has itself evolved rapidly, creating a rich set of international best practices and standard documents among which the ISO/IEC 27000 series [1–5] is rapidly achieving prominence.

The IAEA, while recognizing the core validity of the ISO 27000 series and other standards across industries and business, wishes to focus attention on the specific conditions affecting computer security at nuclear facilities. Thus, the need for a publication recognizing and compiling relevant guidance and adequate solutions was identified. This publication brings together the knowledge and experience of specialists who have applied, tested and reviewed computer security guidance and standards within nuclear facilities and other critical infrastructure. It compiles and describes those special provisions, best practices and lessons learned which apply within the nuclear discipline and puts them in the context of a security programme consistent with other IAEA guidance and applicable industrial standards.

1.2. OBJECTIVE

1.2.1. Nuclear security and computer security objectives

Nuclear security involves the prevention of, detection of, and response to, criminal or intentional, unauthorized acts involving or directed at *nuclear material*, *other radioactive material*, *associated facilities*, or *associated activities*, and other intentional acts that could directly or indirectly produce harmful consequences to persons, property, society or to the environment.

Computer security plays an increasingly vital role in ensuring that these objectives are achieved. Thus, this publication will address the establishment and improvement of programmes to protect those computer systems, networks and

other digital systems that are critical for the safe and secure operation of the facility and for preventing theft, sabotage and other malicious acts.

All other systems required for the operation of the facility, or any support or business system whose unauthorized modification or change could compromise the security posture or operability will be covered by extending the provisions in this publication to those systems.

In this context, malicious acts involving computer systems and relevant to nuclear security may be grouped as:

— Information gathering attacks aimed at planning and executing further malicious acts;
— Attacks disabling or compromising the attributes of one or several computers crucial to facility security or safety;
— Compromise of one or several computers combined with other concurrent modes of attack, such as physical intrusion to target locations.

Computer security objectives are commonly defined as protecting the confidentiality, integrity and availability attributes of electronic data or computer systems and processes. By identifying and protecting these attributes in data or systems that can have an adverse impact on the safety and security functions in nuclear facilities, the security objectives can be met.

1.2.2. Scope

The primary aim of this publication is to create awareness of the importance of incorporating computer security as a fundamental part of the overall security plan for nuclear facilities.

The publication further aims to provide guidance specific to nuclear facilities on implementing a computer security programme. This is achieved by presenting some suggested approaches, structures and implementation procedures designed for nuclear facilities. Together, these are crucial for achieving and maintaining the level of protection defined in the site security strategy and conforming to national nuclear security objectives.

This reference manual also aims to provide advice on evaluating existing programmes, assessing critical digital assets and identifying appropriate risk reduction measures.

1.3. CONDITIONS SPECIFIC TO NUCLEAR FACILITIES

The need for guidance addressing computer security at nuclear facilities is supported by the special conditions characterizing the industry. The following list is a sample of these conditions, which will be dealt with in full in this publication:

— Nuclear facilities must abide by requirements set by their national regulatory bodies which may directly or indirectly regulate computer systems or set guidance.
— Nuclear facilities may have to protect against additional threats which are not commonly considered in other industries. Such threats may also be induced by the sensitive nature of the nuclear industry.
— Computer security requirements in nuclear facilities may differ from requirements in other concerns. Typical business operations involve only a limited range of requirements. Nuclear facilities need to take a wider base or an entirely different set of considerations into account than, for example, those affecting e-commerce, banking or even military applications. Section 7 highlights and explains these differences in detail.

1.4. STRUCTURE

The guidance in this publication is intended for a wide audience that includes policy makers, nuclear security regulators, facility management, staff with security responsibilities, technical staff, vendors and contractors. It applies to all stages of the facility's systems life cycle, including design, development, operations and maintenance.

This publication is divided into two parts:

— Part I (Sections 2–4) is intended to support managers in making balanced judgements and informed decisions concerning policy, design and management of computer security within facilities. It provides guidance on the regulatory and managerial provisions of computer security.
— Part II (Sections 5–7) addresses technical and administrative guidance in the implementation of a comprehensive computer security plan.

1.5. METHODOLOGY

The basic methodology used to implement computer security is similar to methodologies used to ensure nuclear security and safety. This highlights the

need and the advantage of integrating computer security within the overarching facility security plans from the beginning.

Successful protection of computer systems may be achieved by adapting the best practice methods and tools developed within the wider computer security community while taking into account the specificities of the nuclear industry.

The following logical process, described in detail in Section 5, highlights how a nuclear facility can develop, implement, maintain and improve computer security:

— Follow national legal and regulatory requirements;
— Examine relevant IAEA and other international guidance;
— Ensure senior management support and adequate resources;
— Define a computer security perimeter;
— Identify the interactions between computer security and facility operation, nuclear safety and other aspects of site security;
— Create a computer security policy;
— Perform risk assessment;
— Select, design and implement protective computer security measures;
— Integrate computer security within the facility's management system;
— Regularly audit, review and improve the system.

This publication will examine in greater detail those steps in the methodology where specific provisions for nuclear facilities exist. Other stages of computer security methodology may be implemented through direct reference to existing national and international standards (see the references at the end of this publication).

1.6. KEY TERMINOLOGY

As words assume different meanings within different communities of practice, this section clarifies the meaning of certain important terms as used throughout this publication.

In the context of this publication, **computers** and **computer systems** refer to the computation, communication, instrumentation and control devices that make up functional elements of the nuclear facility. This includes not only desktop computers, mainframe systems, servers, network devices, but also lower level components such as embedded systems and PLCs (programmable logic controllers). In essence, this publication is concerned with all components that may be susceptible to electronic compromise.

Throughout this publication the term **computer security** will be used to cover the security of all computers as defined above and all interconnected systems and networks formed by the sum of the elements. The terms **IT security** and **cyber security** are, for the purpose of this publication, considered synonyms of computer security and will not be used in this publication.

Computer security as defined here is a subset of **information security** (as defined, for example in ISO/IEC 27000 [1]) with which it shares many of the goals, methodology and terminology.

Definitions of additional terms used in this publication are provided at the end of this manual.

Part I

MANAGEMENT GUIDE

2. REGULATORY AND MANAGEMENT CONSIDERATIONS

This section highlights the core components of the high level framework for computer security in nuclear facilities. In particular, it addresses issues relevant to the legislative and regulatory bodies as well as to facilities' management and security strategy. Figure 1 shows a simplified visualization of the hierarchy of normative instruments relevant to the establishment and implementation of a computer security programme in a nuclear facility.

2.1. LEGISLATIVE CONSIDERATIONS

A key role of the State is in establishing the legal framework for nuclear security as well as for computer security in general. These should, when

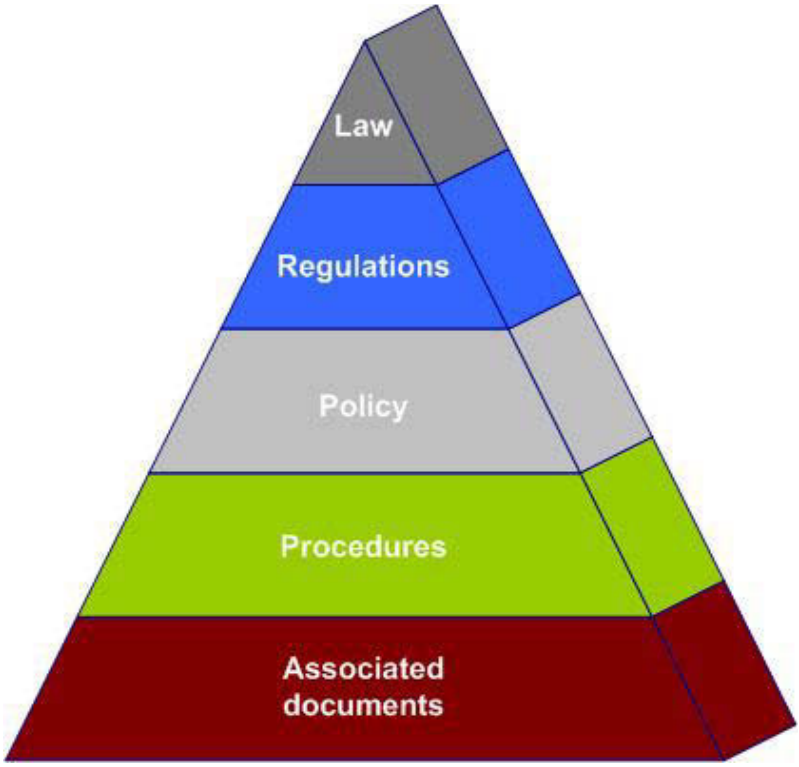


FIG. 1. Relevant normative instruments.

adequately implemented, have a major impact on the safety and security of nuclear facilities. The State legal system should at least provide the legislative and regulatory framework that covers protection of sensitive information and addresses any activity that might precipitate breaches of nuclear security.

Owing to the specificity of its issues, computer security may need special legislative provisions to take into account the unique crimes and modes of operation associated with computer systems. States should carefully consider whether their current legislation adequately covers malicious acts that may be perpetrated with the aid of computers. Among others, important laws that may influence computer security and its implementation include:

— Laws concerning computer offences;
— Laws on terrorism;
— Laws on the protection of critical national infrastructure;
— Laws mandating disclosure of information;
— Laws on privacy and handling of personal information.

It is important that State legislation is continuously reviewed and updated to include provisions for new and emerging criminal activities and other potential threats to computer security.

Given the nature of computer networks, it is possible for adversaries to carry out malicious acts within a State while located outside its physical boundaries and thus potentially out of reach of the State legal system. At the time of formulation of this publication the only international legal instrument of relevance dedicated to regulating international cooperation on computer crimes is the Convention on Cybercrime of the Council of Europe [6].

2.2. REGULATORY CONSIDERATIONS

The regulatory body should take relevant legislation into account in its guidance and make available to operators the tools and the means for correctly interpreting and implementing legal obligations. Regulators could also select or indicate relevant guidance of reference such as ISO standards or IAEA publications.

The activities of regulators in relation to computer security should explicitly recognize the objective of protection against the theft of nuclear material and sabotage resulting in possible radiological release. Therefore, regulations for nuclear security and safety should also be considered when preparing regulations on computer security.

It is advisable that State regulatory bodies (where more than one body is involved) collaborate to achieve harmonized views on necessary requirements to be placed.

The State regulatory bodies could, at a minimum, provide a high level statement of computer security regulatory requirements. More detailed regulatory requirements could also include provisions for:

— Management commitment for computer security (Section 4).
— Computer security programme ownership including designation of the roles of Computer Security Officer(s) and team(s) (Section 4).
— Computer security policy, implementation plan, and enforcement plan (Section 5), including:
  • Computer security perimeter identification;
  • Risk identification;
  • Risk management strategy;
  • Computer security training and awareness programme;
  • Continuity of operations plan.
— Audit and review process, whether internal, external or carried out by the regulators themselves.

Requirements should not prescribe detailed technical solutions, because development may rapidly make such details obsolete. Requirements could instead focus on expected outcomes as these can be written to be less technology dependent.

Facilities may be required to demonstrate conformity to national security requirements through an approved overall site security plan (SSP) or any equivalent or set of documents. **State regulatory bodies should issue requirements for computer security as part of the requirements for the SSP**.

2.3. SITE SECURITY FRAMEWORK

Site security is primarily a management responsibility, specifically of senior management, to ensure that legislative and regulatory requirements are fully met through the implementation of the SSP.

All disciplines of security (including personnel, physical, information and computer) interact and complement each other to establish a facility's security posture as may be defined in the SSP (see Fig. 2). A failure in any of the disciplines of security could impact the other domains and cause extra requirements on the remaining aspects of security. Computer security is a

FIG. 2. Interplay of the different domains of security.

cross-cutting discipline that has interactions with all other areas of security in a nuclear facility.

All provisions in this publication should be implemented with constant regard to the greater framework of the SSP. The SSP should likewise be designed taking into consideration computer security from its inception.

It is also management's responsibility to ensure proper coordination of the various disciplines of security and integration of computer security at the appropriate level.

2.3.1. Computer security policy

Management should be aware that computer technology is being increasingly used for many vital functions at nuclear facilities. This development has brought multiple benefits to operational safety and efficiency. Nonetheless, to ensure the correct functionality of a computer system, they are required to have adequate and balanced security barriers to maximize protection against malicious acts without unnecessarily hampering system operations.

All nuclear facilities should therefore have a computer security policy, which is endorsed and enforced by the site's most senior manager. The policy specifies the overall computer security goals at the facility.

A computer security policy should be part of the overall site security policy and should be negotiated and coordinated with other relevant security responsibilities. When establishing a computer security policy, its impact on legal and human resources should also be considered.

Computer security policy and the associated plan are discussed in greater detail in Section 5.

2.3.2. Computer systems at nuclear facilities

The computer systems and networks supporting nuclear facility operations include many non-standard information technology (IT) computer systems in terms of architecture, configuration, or performance requirements. These systems can include specialized industrial control systems (ICSs), access control systems, alarm and tracking systems, and information systems pertaining to safety and security and emergency response. While ICSs have evolved from strictly proprietary implementations to more mainstream computer architecture, striking differences still exist between ICSs and standard IT systems that must be considered when preparing the site security plan. A full discussion of the uniqueness of computer systems associated with nuclear facilities is located in Section 7.

2.3.3. Defence in depth

Protection requirements should reflect the concept of multiple layers and methods of protection (structural, technical, personnel and organizational) that have to be overcome or circumvented by adversaries in order to achieve their objectives.

The primary means of preventing and mitigating the consequences of security breaches is ‘defence in depth’. Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail or be defeated before a computer system compromise could occur. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. When properly implemented, defence in depth ensures that no single technical, human or organizational failure could lead to computer system compromise, and that the combinations of failures that could give rise to a computer incident are of very low probability. The independent effectiveness of the different levels of defence is a necessary element of defence in depth.

2.4. ASSESSING THE THREAT ENVIRONMENT

The computer security threat environment is a fast changing, evolving scenario. While a good computer security programme will ensure its own

durability, specific controls in place against the most prevalent threats at the present time do not guarantee protection against tomorrow's threats.

The responsible State authority should periodically issue a threat evaluation including threats to the security of computer systems and information on current attack vectors related to the security of computer systems used at nuclear facilities. A typical tool used to determine threat levels and as a basis for developing a security posture is the design basis threat (DBT, see Section 6.3.1).

It is vital that facilities maintain an active and ongoing threat assessment, which is regularly briefed to management and operations.

Section 6 contains a detailed, but non-exhaustive, description of potential sources of attack and associated attack mechanisms relevant to nuclear facilities, and methodologies used to evaluate and identify threats.

3. MANAGEMENT SYSTEMS

A management system is responsible for establishing policies and objectives and enabling the objectives to be achieved in an efficient and effective manner. Management systems are a vital support element to a nuclear security culture. Many activities at nuclear facilities are controlled by management systems. These ideally integrate security, safety, health, environmental, quality and economic elements in a single management tool or a set of integrated and mutually reinforcing systems [7, 8].

Management systems must be reviewed to ensure completeness and compliance with site security policies. More generally, management systems are by nature dynamic and must adapt to changing conditions in the facility and in the environment; they cannot be implemented as a one-off measure but need continuous assessment and improvement. Figure 3 illustrates the life cycle of management processes.

This section aims to supplement present guidance on management systems with the necessary details for computer security management. The key elements that should be reviewed or added to integrate the necessary provisions for computer security are:

— Information assets identification and classification;
— Formal risk analysis;
— Legislative and regulatory compliance;

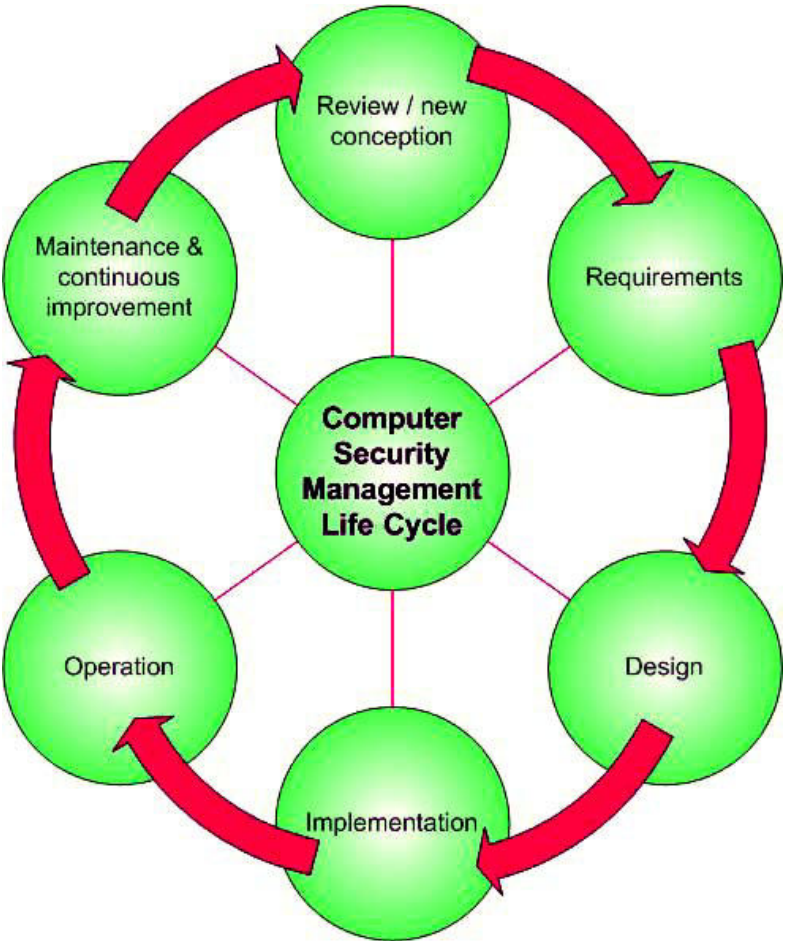


FIG. 3. The security management life cycle.

— Business operational requirements;
— Competency requirements for key persons;
— Business continuity;
— Logical access management;
— System life cycle security;
— Configuration management;
— Amendment and approval of computer security measures;
— Implementation of identified computer security measures;
— Acceptance of implemented computer security measures;
— Compliance with approved computer security measures;

— Immediate analysis of computer security incidents and appropriate reporting;
— Regular reporting on compliance;
— Regular reviews of implemented security measures (audits) by internal and external parties;
— Awareness training;
— New risks and changes to identified risks;
— Changes to legislative and regulatory requirements;
— Medium term plans for information security.

The processes above should be seen as ongoing activities that run through all phases of system life cycles. The specifics of implementation should be detailed in the computer security plan discussed in Section 5.

4. ORGANIZATIONAL ISSUES

4.1. AUTHORITIES AND RESPONSIBILITIES

The sections that follow detail the minimum requirements for management and the specialist staff needed to establish and maintain a computer security programme successfully.

4.1.1. Management

A facility's senior management initiates computer security by establishing an adequate process and support organization. To achieve this, management should:

— Assume overall responsibility for all aspects of computer security;
— Define the facility's security objectives;
— Ensure compliance with laws and regulations;
— Set the risk acceptance level for the facility;
— Assign organizational computer security responsibilities;
— Ensure adequate communication between different aspects of security;
— Ensure an enforceable computer security policy is established;
— Provide adequate resources to implement a viable computer security programme;

— Ensure periodic audits and updates of computer security policy and procedures;
— Ensure support for training and awareness programmes.

Generally, implementation of the permanent computer security process is delegated to specialists within the organization.

4.1.2. Computer Security Officer

Computer security touches almost all facility activities. It is therefore important to assign overarching computer security oversight to one well defined body. In this publication, the title 'Computer Security Officer' (CSO) is used; in other instances this function may be referred to as 'IT Security Officer' or 'Information Security Officer', or may be assigned to multiple roles. Whichever approach is used, this function should be closely coordinated across the facility, should be kept independent of the implementing departments, and should have clear and accessible reporting lines to senior management.

The CSO should have in-depth knowledge of computer security and good knowledge of other aspects of security in nuclear facilities. Further requirements are knowledge of nuclear safety and project management, and the ability to integrate people coming from different disciplines into an efficient team.

The typical responsibilities of a CSO or equivalent include:

— Advising the company's management on computer security.
— Leading the computer security team.
— Coordinating and controlling the development of computer security activities (e.g. implementing security policy, directives, procedures, guidelines, measures).
— Coordinating with physical security and other security and safety disciplines to plan security measures and response to security incidents.
— Identifying systems critical to computer security within a facility (i.e. the computer security baseline). Asset owners should be informed of their equipment's role in computer security.
— Conducting periodic computer security risk assessments.
— Conducting periodic inspections, audits and reviews of the computer security baseline and providing status reports to top management.
— Developing and implementing computer security training and evaluation.
— Developing and leading incident response for relevant computer security emergencies, including coordination with relevant internal and external organizations.

— Investigating computer security incidents and developing post-incident procedures and preventive actions.
— Participating in site security assessment initiatives.
— Participating in requirement analysis in the acquisition/development of new systems.

4.1.3. Computer security team

It is essential for the CSO to have access to adequate interdisciplinary expertise associated with computer security, facility safety, and plant operations as well as physical and personnel security. This may consist of a dedicated computer security team or ad hoc access to specific expertise within the organization. The goal of this team is to support the CSO in fulfilling his/her responsibilities.

4.1.4. Other management responsibilities

The various levels of management within an organization must ensure the appropriate level of computer security within their areas of responsibility. Typical responsibilities include:

— Operating within the guidance of the site computer security plan;
— Providing operational requirements and feedback to the CSO relevant to computer security and resolving potential conflicts between operational, security, and safety requirements;
— Notifying the CSO of any conditions that may lead to changes in the computer security posture, such as personnel changes, equipment changes, or process changes;
— Ensuring that staff are sufficiently trained and briefed on computer security issues relevant to their roles;
— Ensuring that subcontractors and third party vendors working for the contracting unit operate within the context of the site security plan;
— Tracking, monitoring and reporting events of security relevance;
— Enforcing personnel security measures.

4.1.5. Individual responsibilities

Each person within an organization is responsible for carrying out the computer security plan. Specific responsibilities include:

— Knowledge of the baseline computer security procedures;
— Knowledge of job specific computer security procedures;
— Operating within the parameters of the computer security policies;
— Notifying management of any changes that may lead to a reduced computer security posture;
— Notifying management of any incidents or possible incidents involving a compromise of computer security;
— Attending initial and refresher security training on a regular basis.

4.2. COMPUTER SECURITY CULTURE

A robust computer security culture is an essential component of any effective security plan. It is important for management to ensure that computer security awareness is fully integrated into the overall site security culture. The characteristics of nuclear security culture are the beliefs, attitudes, behaviour and management systems, the assembly of which lead to a more effective nuclear security programme. The foundation of nuclear security culture is recognition — by those that have a role to play in regulating, managing or operating nuclear facilities or activities or even those that could be affected by these activities — that a credible threat exists and that nuclear security is important. (For more information on nuclear security culture, see Ref. [9].) Computer security culture is a subset of the overall security culture and is based on an application of the above characteristics to computer security awareness.

Experience has demonstrated that the majority of computer security incidents are human related and the security of any computer system depends largely on the behaviour of all its users. Annex III provides examples of human errors that could lead to security compromise. The computer security culture is developed through a collection of many activities designed to inform personnel and increase computer security awareness (e.g. posters, notices, management discussions, training, tests, etc.). Computer security culture attributes should be periodically measured, reviewed, and continuously improved. The following indicators can be used to evaluate the computer security culture in an organization:

— Computer security requirements are clearly documented and well understood by staff.
— Clear and effective processes and protocols exist for operating computer systems both inside and outside the organization.
— Staff members understand and are aware of the importance of adhering to the controls within the computer security programme.

— Computer systems are maintained to ensure that they are secure and operated in accordance with computer security baseline and procedures.
— Management are fully committed to and supportive of security initiatives.

4.2.1. Computer security training programme

A strong training programme is one of the cornerstones of a computer security culture. It is crucial to educate staff, contractors and third party vendors on the importance of observing security procedures and maintaining a culture of security.

The awareness programme should include the following requirements:

— Successful completion of a computer security training and/or awareness programme should be a precondition for access to computer systems. Training should be commensurate with system security levels and the expected role of users.
— Enhanced training/qualifications should be provided to individuals with key security responsibilities (e.g. CSO, computer security team, project managers, IT administrators).
— Training should be repeated periodically for all staff to include new procedures and emerging threats.
— Staff should be required to acknowledge that they understand their security responsibilities.

The training programme should include metrics to evaluate computer security awareness, training effectiveness, and processes for continuous improvement or retraining.

Part II

IMPLEMENTATION GUIDE

5. IMPLEMENTING COMPUTER SECURITY

This publication does not establish minimum standards of acceptable risk or a specific set of mitigation measures that could be used. Any set of specific standards would be rapidly outdated as digital systems change, new threats emerge, new mitigation tools become available and regulatory requirements change. Part II of the publication focuses on compiling a set of methodological and concrete recommendations to support and guide the implementation of computer security in nuclear facilities.

These recommendations are neither prescriptive nor definitive and should be used as guidance; where appropriate, alternative measures may be adopted to achieve the desired defence in depth and other fundamental nuclear security objectives [10–12].

5.1. COMPUTER SECURITY PLAN AND POLICY

5.1.1. Computer security policy

As introduced in Section 2.3.1, a computer security policy sets the high level computer security goals of an organization. The policy must meet appropriate regulatory requirements. Computer security policy requirements should be factored into lower level documents, which will be used to implement and control policy. Additionally, the policy must be:

— Enforceable;
— Achievable;
— Auditable.

5.1.2. Computer security plan

The computer security plan (CSP) is the implementation of that policy in the form of organizational roles, responsibilities, and procedures. The plan specifies and details the means for achieving the computer security goals at the facility and is a part of (or linked to) the overall SSP.

The plan should contain the primary actions in terms of susceptibility to vulnerabilities, protective measures, consequence analysis and mitigation measures to establish and maintain the nuclear facility's acceptable cyber risk and facilitate recovery to a safe operational state.

5.1.3. CSP components

Based on the established computer security policy, each individual plan component tries to achieve its distinct goals and objectives. The minimum content and itemization of the CSP is suggested in the subsections below:

(a) Organization and responsibilities:
  (1) Organizational charts;
  (2) Responsible persons and reporting responsibilities;
  (3) Periodic review and approval process.

(b) Asset management:
  (1) List of all computer systems;
  (2) List of all computer systems applications;
  (3) Network diagram, including all connections to external computer systems.

(c) Risk, vulnerability, and compliance assessment:
  (1) Security plan review and reassessment periodicity;
  (2) Self-assessment (including penetration testing procedures);
  (3) Audit procedures and deficiency tracking and correction;
  (4) Regulatory and legislative compliance.

(d) System security design and configuration management:
  (1) Fundamental architecture and design principles;
  (2) Requirements related to the different security levels;
  (3) Formalization of computer security requirements for suppliers and vendors;
  (4) Full life cycle security.

(e) Operational security procedures:
  (1) Access control;
  (2) Data security;
  (3) Communication security;
  (4) Platform and application security (e.g. hardening);
  (5) System monitoring;
  (6) Computer security maintenance;
  (7) Incident handling;
  (8) Business continuity;
  (9) System backup.

(f) Personnel management:
  (1) Vetting;
  (2) Training;
  (3) Qualification;
  (4) Termination/transfer.

The above provides a framework for developing a CSP. Many references are available to fill out this framework, the main international references being ISO/IEC 27001 [2] for information security management systems, and ISO/IEC 27002 [3] for implementation recommendations.

While the majority of components listed above are consistent across computer security plans for any business or industry, certain nuances do exist for its implementation within nuclear facilities. These components of the CSP are described in greater detail in Section 7. Risk, vulnerability, and compliance assessment are addressed in Section 6. Asset analysis is further detailed in Section 5.3.

5.2. INTERACTION WITH OTHER DOMAINS OF SECURITY

As stated in Section 2.3, the CSP should be operated and maintained within the framework of the facility's overall protection plan. The facility specific computer security plan should be developed in close consultation with physical protection, safety, operations and IT specialists. The CSP must be regularly reviewed and updated to reflect security events from any domain of security and operational experience from the site security system.

5.2.1. Physical security

The physical security plan and the CSP should complement each other. Computerized assets have physical access control requirements and likewise, electronic compromise can lead to degradation or loss of certain physical protection functions. Attack scenarios may well include the coordination of both electronic and physical attack. The teams in charge of the physical security plan and of the CSP should inform each other and coordinate their efforts to ensure consistency of plans during the development and review process.

5.2.2. Personnel security

Besides awareness and training, other aspects of security — usually handled within the domain of personnel security — are essential for instituting consistent computer security. The necessary provisions for establishing an appropriate level of vetting, confidentiality undertakings, and termination procedures and for defining required job competencies should be coordinated between the computer and personnel security managements. In particular, staff with key security responsibilities (system administrators, security team) may require a higher level of vetting.

5.3. ASSET ANALYSIS AND MANAGEMENT

Interaction between computer systems in nuclear facilities may affect security in non-obvious ways. It is therefore important that the security plan **identifies all assets** and includes a **more comprehensive inventory of those assets critical to facility security and safety functions**. The inventory could include data, computer systems, their interfaces and their owners.

The following methodology satisfies the above needs:

(a) Relevant information about existing computer systems should be compiled in order to create a complete list of assets;
(b) The interconnection between the identified assets should be mapped out;
(c) The relevance to safety functions and identified safety systems, safety related systems and security systems should be identified and evaluated.

The completeness of each step is a crucial prerequisite for the next steps.

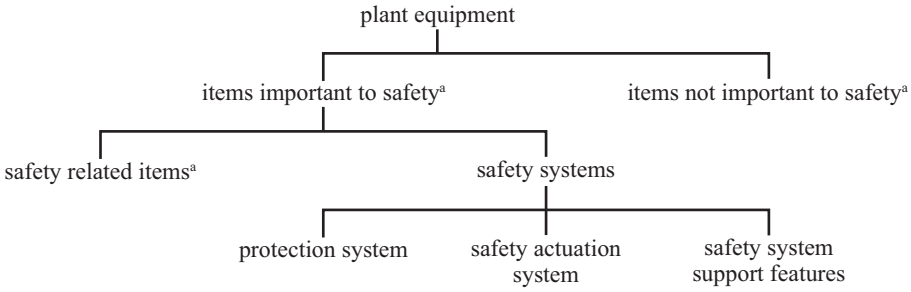
A comprehensive analysis of computer systems in a nuclear facility includes:

— Functions/tasks and operational modes of all existing computerized systems;
— Identification of relevant interconnections, including power supplies;
— Dataflow analysis, to determine what communicates with what, and how and why;
— Procedures that initiate communication, frequency of communication and protocols;
— Computer systems and equipment location;
— Analysis of user groups;
— Ownership (for data and computerized systems);
— Corresponding security level (see Section 5.5, graded approach).

It is assumed that much of the information needed for the analysis would already be available, but it should be collated and organized. Sources of relevant information include system specifications and documentation.

5.4. COMPUTER SYSTEM CLASSIFICATION

As defined in Section 1.6, in the context of this publication, computer and computer systems refer to computation, communication, instrumentation and sensing devices that make up functional elements of the nuclear facility. Computer functions of prime concern are control and data processes associated



[a] In this context, an 'item' is a *structure, system or component.*

FIG. 4. Plant equipment in terms of safety function.

with safety and security. Other computer functions may be a concern in terms of support to these functions, of possible compromise of security through secondary or indirect effects or of overall plant productivity.

Below is a non-exhaustive list of computer systems that can be found at nuclear facilities, and are relevant to the objectives of this guidance. They are separately classified according to their safety importance and security importance. Both of these classifications should be taken into account when defining the appropriate security level to apply (Section 5.5) and in the risk assessment analysis (Section 6.2). Note also that some functions clearly overlap both as safety and security concerns.

5.4.1. Safety importance

IAEA safety standards (e.g. Refs [13–15]) categorize nuclear facility equipment according to their function, as illustrated in Fig. 4.

Plant equipment

— Systems important to safety

• Safety systems

— Protection systems: Instrumentation and control (I&C) systems that are used for automatically initiated reactor and plant protection actions.
— Safety actuation systems: I&C systems that accomplish safety actions, which are initiated by the protection systems and by manual actuations.
— Safety system support features: I&C for emergency power supply systems.

- Safety related systems

  — Process control systems: I&C systems for plant control.
  — Control room I&C including the alarm systems.
  — Process computer systems that collect and prepare information for the control room.
  — Fuel handling and storage I&C systems.
  — Fire protection systems.
  — Access control systems.
  — Voice and data communication infrastructure.

— Systems not important to safety

- Control systems for functions that are not important to safety (e.g. demineralization)

Consideration should also be given to computer systems that are not necessarily within the scope of plant equipment but nevertheless can impact safety.

Non-plant equipment

— Office automation

- Work permit and work order systems: Systems that provide coordination of work activities to provide a sound working environment.
- Engineering and maintenance systems: Systems that handle details of plant operation, maintenance and technical support.
- Configuration management systems: Systems intended to keep track of plant configuration including models, versions and parts installed at the nuclear facility.
- Document management systems: Systems used to store and retrieve plant information, e.g. drawings, minutes of meetings.
- Intranet: System that allows access to all plant documentation — both technical and administrative — on a need to know basis. The access is normally read only.

— External connectivity

- Email: A system that is used to transfer information to external parties.
- Public web site: A system that is used to give Internet users information about the facility.

- Remote access/third party access: Systems that allow strictly controlled access from the outside to certain functions within a site.

5.4.2. Security or security related systems

An established security classification for security systems comparable to the safety classification does not yet exist. Nevertheless, it should be an important part of the asset analysis to compile such a classification for the systems in the facility. The following list may support such classification:

— Physical access control systems: systems used to ensure that only authorized persons enter areas of a site appropriate to the function they perform;
— Voice and data communication infrastructure;
— Security clearance database: used to ensure that persons hold the appropriate security clearance to obtain access to a part of site or information held on the site;
— Security alarm monitoring and control systems: used to monitor all security alarms on the site and assist with assessment of the alarm;
— Computer and network security components;
— Nuclear accountancy and control systems.

5.5. GRADED APPROACH TO COMPUTER SECURITY

The security of computer systems should be based on a graded approach, where security measures are applied proportional to the potential consequences of an attack. One practical implementation of the graded approach is to categorize computer systems into *zones*, where graded protective principles are applied for each zone based on the *level* of security requirement assigned to the zone. The assignment of computer systems to different levels and zones should be based on their relevance to safety and security (see Section 5.4). Nonetheless, **the risk assessment process should be allowed to feed back into and influence the graded approach**.

5.5.1. Security levels

Security levels are an abstraction that defines the degrees of security protection required by various computer systems in a facility. Each level in a graded approach will require different sets of protective measures to satisfy the

security requirements of that level. Some protective measures apply to all computer systems in all levels, while others are specific to certain level(s).

The security level model allows easier assignment of protective measures to various computer systems, based on the categorisation of the system (assigning it to a level) and the definition of the set of protective measures appropriate to that level.

The levels and their associated protective measures should be appropriately documented in the CSP.

5.5.2. Zones

Zones are a logical and physical concept for grouping computer systems for administration, communication and application of protective measures. The zone model allows computers with the same or similar importance concerning safe and secure operation of the plant to be grouped together for administration and application of protective measures.

The application of a zone model should comply with the following guidelines:

— Each zone comprises systems that have the same or comparable importance for the facility's security and safety;
— Systems belonging to one zone have similar demands for protective measures;
— Different computer systems belonging to one zone build a trusted area for internal communication within that zone;
— Zone borders require decoupling mechanisms for data flow built on zone dependent policies;
— Zones can be partitioned into subzones to improve the configuration.

Because zones are comprised of systems with the same or comparable importance for facility safety and security, each zone can have a level assigned, indicating the protective measures to be applied for all computer systems in that zone. However, the relationship between zones and levels is not one-to-one; a level may have multiple zones assigned to it when multiple zones require the same degree of protection. Zones are a logical and physical grouping of computer systems, while levels represent the degree of protection required.

The zone model should be appropriately documented in the CSP, to include an overview of all computer systems, all relevant communication lines, all zone crossings and all external connections.

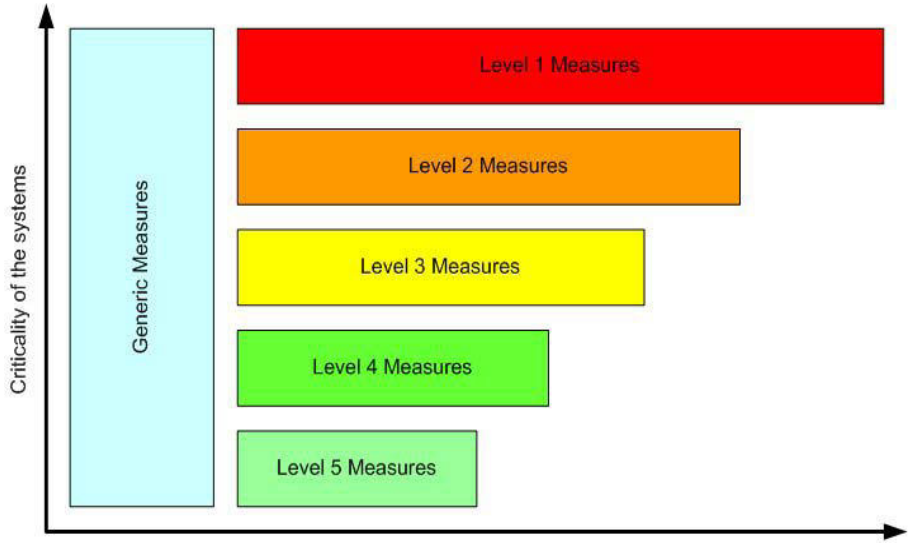


FIG. 5. Level of security/strength of measures.

5.5.3. Example of the application of a security level model

An example of security measures applied at different levels is presented below. This is just one possible implementation of the graded approach; the exact choice of levels and their constitutive security measures should be tailored according to the considered environment, the facility specificities, and the dedicated security risk analysis.

In this implementation:

— Generic level measures should apply to all computer systems.
— Security levels range from level 5 (least protection needed) to level 1 (most protection needed), as illustrated in Fig. 5.
— The measures corresponding to each level are not cumulative (thus, there may be repetitions).

Generic level

For applicable systems and levels, the following generic measures should be applied:

— Policies and practices are defined for each level.
— Security operating procedures are written for and read by all users.

— Staff permitted access to the system must be suitably qualified and experienced and security cleared where necessary.
— Users are given access only to those functions on those systems that they require for carrying out their jobs.
— Appropriate access control and user authentication are in place.
— Anomaly detection systems or procedures are in place.
— Application and system vulnerabilities are monitored, and appropriate measures are taken.
— System vulnerability assessments are undertaken periodically.
— Removable media must be controlled in accordance with security operating procedures.
— Computer and network security components should be strictly maintained.
— Computer and network security components (e.g. security gateways, intrusion detection systems, intrusion prevention systems, virtual private network (VPN)[1] servers) are strictly logged and monitored.
— Appropriate backup/recovery procedures are in place.
— Physical access to components and systems is restricted according to their functions.

Level 1

In addition to the generic measures, level 1 protective measures should be used for systems, e.g. protection systems, which are vital to the facility and require the highest level of security. These measures may include the following:

— No networked data flow of any kind (e.g. acknowledgment, signalization) from systems in weaker security levels should be authorized to enter level 1 systems. Only strictly outward communication should be possible. Note that this kind of strict one-way communication does not ensure reliability and integrity natively (redundancy/error corrections may be considered). Note also that this excludes any sort of 'handshake' protocols (including TCP/IP[2]), even with controlled connection directions. Exceptions are strongly discouraged and may only be considered on a strict case by case basis and if supported by a complete justification and security risk analysis.[3]

[1] A virtual private network (VPN) is a network constructed using public communication means to connect nodes, with encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

[2] Transmission Control Protocol/Internet Protocol — data transmission protocols.

[3] Some Member States feel strongly that exceptions should not be allowed in any case.

— Measures to ensure the integrity and availability of the systems are typically explained as a part of the safety cases.
— No remote maintenance access is allowed.
— Physical access to systems is strictly controlled.
— The number of staff given access to the systems is limited to an absolute minimum.
— The two person rule is applied to any approved modifications made within the computer systems.
— All activities should be logged and monitored.
— Every data entry to the systems is approved and verified on a case by case basis.
— Strict organizational and administrative procedures apply to any modifications, including hardware maintenance, updates and software modifications.

Level 2

In addition to the generic measures, level 2 protective measures should be used for systems, e.g. operational control systems, which require a high level of security. These measures may include the following:

— Only an outward, one way networked flow of data is allowed from level 2 to level 3 systems. Only necessary acknowledgment messages or controlled signal messages can be accepted in the opposite (inward) direction (e.g. for TCP/IP).
— Remote maintenance access may be allowed on a case by case basis, and for a defined working period. When used, it must be protected with strong measures, and users must respect a defined security policy (contractual).
— The number of staff given access to the systems is kept to a minimum, with a precise distinction between users and administrative staff.
— Physical connections to the systems should be strictly controlled.
— All reasonable measures to ensure the integrity and availability of the systems have been taken.
— Vulnerability assessment involving actions on the systems may lead to plant or process instability, and should therefore only be considered using test beds, spare systems, during factory acceptance tests or during long planned outages.

Level 3

In addition to the generic measures, level 3 protective measures should be used for supervision real time systems not required for operations, e.g. process real time supervision systems in a control room, which have a medium severity level for various cyber threats. These protective measures may include the following:

— Access to the Internet from level 3 systems is not allowed.
— Logging and audit trails for key resources are monitored.
— Security gateways are implemented to protect this level from uncontrolled traffic from level 4 systems, and to allow only specific and limited activity.
— Physical connections to systems should be controlled.
— Remote maintenance access is allowed on a case by case basis provided that it is robustly controlled; the remote computer and user must respect a defined security policy, contractually specified.
— System functions available to users are controlled by access control mechanisms, and based on the 'need to know' principle. Any exception to this principle has to be carefully studied and protection should be ensured by other means (e.g. physical access).

Level 4

In addition to the generic measures, level 4 measures should be used for technical data management systems used for maintenance or operation activity management related to components or systems required by the technical specification for operation (e.g. work permit, work order, tag out, documentation management), which have moderate severity level for various cyber threats. Level 4 measures include the following:

— Only approved and qualified users are allowed to make modifications to the systems.
— Access to the Internet from level 4 systems may be given to users provided adequate protective measures are applied.
— Security gateways are implemented to protect this level from uncontrolled traffic from external company or site networks, and to allow specific activities which are controlled.
— Physical connections to systems should be controlled.
— Remote maintenance access is allowed and controlled; the remote computer and user must respect a defined security policy, contractually specified and controlled.

— System functions available to users are controlled by access control mechanisms. Any exception to this principle has to be carefully studied and protection should be ensured by other means.
— Remote external access is allowed for approved users provided that appropriate access control mechanisms are in place.

Level 5

Level 5 measures should be used for systems not directly important to technical control or operational purposes, e.g. office automation systems, which have low severity level for various cyber threats. Level 5 measures include the following:

— Only approved and qualified users are allowed to make modifications to the systems.
— Access to the Internet from level 5 systems is allowed provided adequate protective measures are applied.
— Remote external access is allowed for authorized users provided that appropriate controls are in place.

5.5.4. Decoupling zones

Zone borders require decoupling mechanisms for data flow in order to prevent unauthorized access and also to prevent errors from propagating from a zone with lower protection requirements to a zone with higher ones.

Technical and administrative measures ensuring the decoupling of zones have to be geared to the individual demands of protective levels. A direct connecting passage through several zones should not be allowed.

6. THREATS, VULNERABILITIES AND RISK MANAGEMENT

The section below presents the basic concepts used in risk management for computer systems. Risk management is relevant at all stages of the facility's systems life cycle, including design, development, operations and maintenance. Section 6.2 offers an overview of the steps needed in a comprehensive risk

management methodology. Sections 6.3 and 6.4 focus on stages where the nuclear industry presents specific features.

6.1. BASIC CONCEPTS AND RELATIONSHIPS

Risk in the computer security context is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and the severity of its consequences.

Figure 6 is a flow chart showing the multiple interconnections between the concepts of threat, vulnerability and risk [16].

6.2. RISK ASSESSMENT AND MANAGEMENT

Risk assessment is an important tool for determining the best location to allocate resources and effort in addressing vulnerabilities and the likelihood of their exploitation.

It is a process by which particular combinations of threat, vulnerability and impact are identified and documented, and appropriate protective controls are devised. The threat and vulnerability assessment provides the basis for preparing the countermeasures required to prevent or mitigate the consequences of attacks against computer systems.

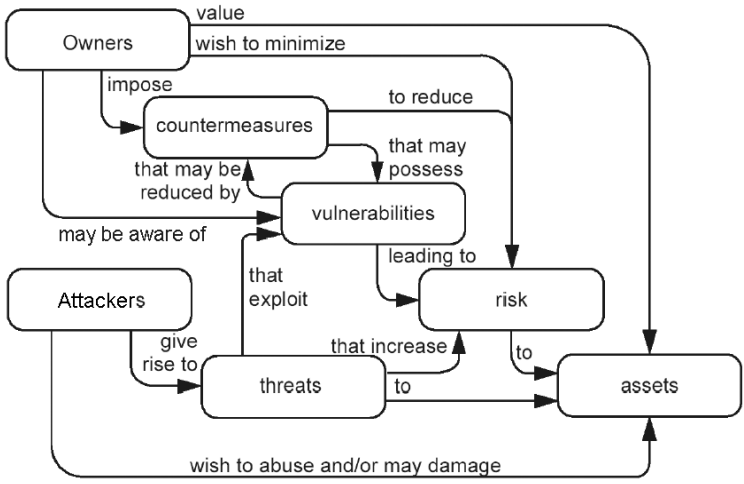


FIG. 6. Security concepts and relationship (adapted from ISO 13335-1 2004 [16]).

The basic steps of a risk assessment and management methodology are:

— Perimeter and context definition;
— Threat identification and characterization;
— Vulnerability assessment;
— Attack scenario elaborations;
— Likelihood of successful exploitation;
— Evaluation of level of risk;
— Countermeasure definition.

In order to implement a systematic and consistent risk analysis and assessment, a well defined process that can comply with the existing standards has to be used. Numerous risk assessment or management methodologies and tools have reached maturity and can structure such a process efficiently, and thus have met with acceptance by a broad audience. Most of them are based on common concepts and logic. The current international standard is ISO/IEC 27005 — Information Security Risk Management [4]. Another specific example of a methodology is given in Annex II. National authorities may require a specific risk assessment methodology or policy to be used and facilities may additionally have their own.

An interesting panorama of risk assessment methods and tools has been undertaken by ENISA (the European Network and Information Security Agency), which devoted a special web page for this survey [17].

The necessity of evaluating systems, the depth of the assessment and the frequency of updating risk analyses depend upon the importance of the system in terms of their safety and security function. Consideration must be given to conducting a new analysis or at least a review when modifications to the system occur. The introduction of new equipment, software, procedures, or a major change in operator skill sets may all fulfil this condition. The number of potential threats and vulnerabilities usually increases as with progress from stand-alone to interconnected systems.

When it is impractical to perform a risk analysis against specific threats, the use of best practices and good engineering principles is recommended.

6.3. THREAT IDENTIFICATION AND CHARACTERIZATION

Figure 7 highlights the continuous trend towards growing attack sophistication and decreasing knowledge required to launch such an attack. Computer security programmes should strive to maintain a level of assessment that covers a very broad range of possible attack scenarios.

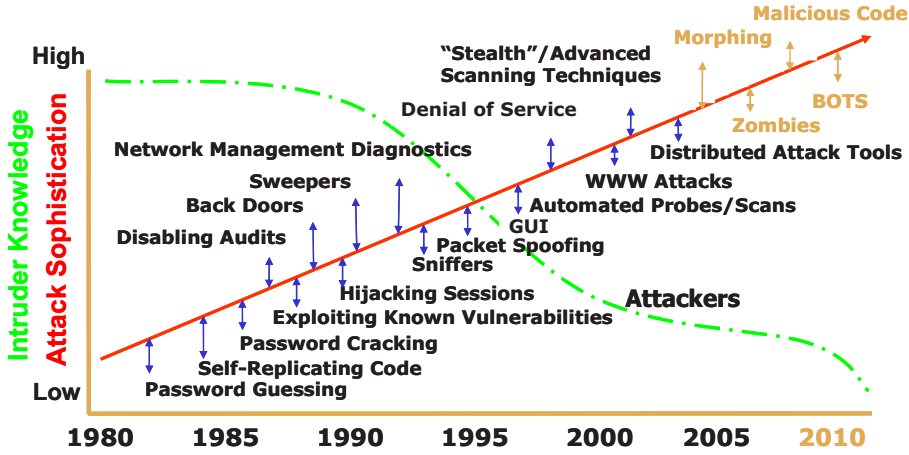


FIG. 7. The increasing complexity of threats as attackers proliferate.[4]

Publications about industrial control system vulnerability are regularly found at major hackers events. Considering that they generally give a delayed picture of the state of the art of real hackers' skills and interests, this should be an additional awareness raising factor. Moreover, ICS software vulnerabilities have recently started to be published by national CERTs (Computer Emergency Response Teams), reinforcing exposure to the public opinion and the computer security community, and focusing interest in such solutions and product weaknesses.

Therefore, after having established adequate support and resources, the initial steps in developing a computer security programme should focus on understanding potential threats based on credible attacker profiles and attack scenarios. A possible first step would be to create an attacker profile matrix listing credible attackers, motivations, and potential objectives. The attacker profile matrix could then be used to build plausible attack scenarios; the following subsections examine this process in greater detail.

6.3.1. Design basis threat

An important tool commonly used to determine threat levels and as a basis for developing a security posture is the design basis threat (DBT). The DBT is a statement about the attributes and characteristics of potential adversaries (internal

[4] LIPSON, H.F., Tracking and Tracing Cyber-Attacks: Technical Challanges and Global Policy Issues, Special Report CMS/SEI-2002-SR-009 (2000) 10.

and/or external). A DBT is derived from credible intelligence information, but is not intended to be a statement about actual prevailing threats. Based on the current threat environment, the DBT represents the largest reasonable threat that a facility should expect to defend against. States use DBTs in their regulatory system to determine appropriate allocation of resources to the protection of nuclear material and nuclear facilities from hostile actions. (For more information on DBT, see Ref. [18].)

Consideration should be given to incorporating into such scenarios threats of either stand-alone attacks using/against computer systems or coordinated attacks including the use of computer systems.

6.3.2. Attacker profiles

Tables 1 and 2 illustrate a possible set of attacker profiles. Table 1 focuses on internal/insider threats (see also Ref. [19] for a discussion of the insider threat), while Table 2 identifies some possible external threats. The tables associate general types of attackers with their resources, the time span of the attack, the tools that are likely to be used and the attacker's motivations. Profiles need to be adapted to the individual facility. Therefore, an adequate process of intelligence gathering is required to ensure the completeness and relevance of each facility's attacker matrix.

6.3.3. Attack scenarios

In creating attack scenarios, one may differentiate between several possibilities. The nuclear facility may be attacked with the purpose of:

— Building up a later coordinated attack intended to sabotage the plant and/or to remove nuclear material;
— Endangering human or environmental safety;
— Launching an attack towards another site;
— Creating confusion and fear;
— Gaining monetary profit for a criminal group of people;
— Creating major market instabilities and gains for selected market players.

Depending on the objectives or aims of the attack, the attacker will try to exploit different system vulnerabilities. Such attacks can lead to:

— Unauthorized access to information (loss of confidentiality);
— Interception and change of information, software, hardware, etc. (loss of integrity);

TABLE 1. INTERNAL THREATS

Attacker	Resources	Time	Tools	Motivation
Covert agent	Facilitated 'social engineering'. System access at some level. System documentation and expertise available.	Varied, but generally cannot devote long hours.	Existing access, knowledge of programming and system architecture: — Possible knowledge of existing passwords; — Possibility to insert specifically crafted backdoors and/or Trojans; — Possible external expertise support.	Theft of business information, technology secrets, personal information. Economic gain (information selling to competitors). Blackmail.
Disgruntled employee/user	Medium/strong resources. System access at some level. System documentation and expertise available on specific business and operations systems.	Varied, but generally cannot devote long hours.	Existing access, knowledge of programming and system architecture. Possible knowledge of existing passwords. Ability to insert 'kiddie' tools or scripts (potentially more elaborate if they have specific computer skills).	Revenge, havoc, chaos. Theft of business information. Embarrass employer/other employee. Degrade public image or confidence.

TABLE 2. EXTERNAL THREATS

Attacker	Resources	Time	Tools	Motivation
Recreational hacker	Varied skills, but generally limited. Little knowledge of the system outside of public information.	Lots of time, not very patient.	Generally available scripts and tools. Some tool development possible.	Fun, status. Target of opportunity. Exploitation of 'low hanging fruits'.
Militant opponent to nuclear power	Limited resources, but may be financially supported through secret channels. Access to tools of the cyber community. Little knowledge of the system outside of public information.	Attacks may be targeted at certain previously known events (e.g. celebrations, elections). Lots of time, patient and motivated.	Computer skills are available. Possible support from the hacker community. 'Social engineering'.	Conviction of saving the world. Sway public opinion on specific issues. Impede business operations.
Disgruntled employee/user no longer employed)	Limited resources if not engaged in a larger group of people. May still possess system documentation. May use unmanaged former access. Possible ties to facility personnel.	Varied and depending on the associated group of people.	Possible knowledge of existing passwords. May use unmanaged former access. May have created system backdoors while still an employee. 'Social engineering'.	Revenge, havoc, chaos. Theft of business information. Embarrass employer/other employee. Degrade public image or confidence.

TABLE 2. EXTERNAL THREATS (cont.)

Attacker	Resources	Time	Tools	Motivation
Organized crime	Strong resources. Employment of cyber expertise.	Varied, but mostly short term.	Scripts, home grown tools. May employ 'hacker for hire'. May employ former/current employee. 'Social engineering'.	Blackmail. Theft of nuclear material. Extortion (financial gain). Play upon financial and perception fears of business. Information for sale (technical, business or personal).
Nation State	Strong resources and expertise. Intelligence gathering activities. Possible training/operating experience on the system.	Varied.	Teams of trained cyber experts. Sophisticated tools. May employ former/current employee. 'Social engineering'.	Intelligence collection. Building access points for later actions. Technology theft.
Terrorist	Varied skills. Possible training/operating experience on the system.	Lots of time, very patient.	Scripts, home grown tools. May employ hacker for hire. May employ former/current employee. 'Social engineering'.	Intelligence collection. Building access points for later actions. Chaos. Revenge. Impact public opinion (fear).

— Blockage of data transmission lines and/or shutdown of systems (loss of availability);
— Unauthorized intrusion into data communication systems or computers (loss of reliability).

All these aspects can have major consequences and impacts on the functionality of computer systems, which may, directly or indirectly, compromise the safety and security of the facility. When building up attack scenarios, the technological trends and ease of access to attack technologies should be considered. Some scenarios illustrating fictional, but realistic, attacks at a nuclear facility are developed in Annex I.

6.4. SIMPLIFIED OUTCOMES OF RISK ASSESSMENT

Table 3 provides, for illustrative purposes only, examples of systems that may be found at a nuclear facility. It identifies potential impacts of successful attacks on the considered systems, the corresponding impacts on the facility and generic examples of appropriate countermeasures.

The notion of likelihood, fundamental for risk evaluation, is not considered in this table. The likelihood of successful attacks, and also potential consequences, depends on the context and the facility considered. In addition, a more thorough assessment of the confidentiality, integrity and availability requirements should be done for each system considered in the risk assessment.

7. SPECIAL CONSIDERATIONS FOR NUCLEAR FACILITIES

Given the unique nature of the nuclear industry, computer security for nuclear facilities must address concerns additional to those for computer security for business IT networks or even comparable process control systems outside the nuclear industry. The following sections describe some of these nuclear industry related concerns.

TABLE 3. TYPICAL SYSTEMS IN NUCLEAR FACILITIES

System	Impacts on computer security	Potential impacts on facility	Suggested counter measures
Reactor protection system	Loss of integrity of safety critical software/data. Loss of function availability.	CRITICAL Plant safety compromised, radiological release.	Security Level 1 measures
Process control system	Loss of integrity of control software/data. Loss of function availability.	HIGH Plant operation compromised.	Security Level 2 measures
Work permit and work order system	Loss of integrity of data and availability of the system.	MEDIUM Wrong actions on components. Disruption of normal operation and maintenance.	Security Level 4 measures
Physical access control system	Loss of availability and integrity of site access systems. Loss of confidentiality of site access data.	HIGH Access given to unauthorized persons. Authorized persons prevented from gaining access to areas they are required to access.	Security Level 2 measures
Document management system	Loss of confidentiality, availability, and integrity of data.	MEDIUM Information used to plan more severe attacks.	Security Level 4 measures
Email	Loss of confidentiality, integrity and availability.	LOW Administrative burdens. Daily operations made more difficult.	Security Level 5 measures

7.1. FACILITY LIFETIME PHASES AND MODES OF OPERATION

Nuclear facilities have a wide variety of designs and operational characteristics. They have multiple lifetime phases and modes of operation, which include:

— Design, construction and commissioning.
— Operations:
  • Power operations;
  • Plant startup;
  • Hot shutdown;
  • Cold shutdown;
  • Refuelling and maintenance.
— Decommissioning.

These multiple lifetime phases and modes of operation may involve different systems and likewise different operational environments. For example, maintenance intense periods often involve equipment replacement, modification, and testing, or may require extra staff and third party/contractor access. This diversity should be taken into account in the CSP. In particular, different lifetime phases might imply strong revisions of the CSP.

7.2. DIFFERENCES BETWEEN IT SYSTEMS AND INDUSTRIAL CONTROL SYSTEMS

Computer systems and network architectures supporting nuclear plant operations are not standard computer systems in terms of architecture, configuration, or performance requirements. These systems can be classified as specialized industrial control systems (ICSs). While ICSs have evolved from strictly proprietary implementations to more mainstream computer architectures, striking differences still exist between ICSs and standard IT systems that must be considered in any CSP.

Table 4, based on material from NIST [20], presents the main differences between ICSs and classical IT systems.

TABLE 4. DIFFERENCES BETWEEN IT AND ICSs [20]

Category	Information technology system	Industrial control system
Performance requirements	Non-real-time Response must be consistent High throughput is demanded High delay and jitter may be acceptable	Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is a serious concern
Availability requirements	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated, depending on the system's operational requirements	Responses such as rebooting may not be acceptable because of process availability requirements Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing
Risk management requirements	Data confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations	Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime is not acceptable Major risk impact is regulatory non-compliance, loss of life, equipment, or production
Architecture security focus	Primary focus is protecting the IT assets, and the information stored on or transmitted among these assets. Central server may require more protection	Primary goal is to protect edge clients (e.g., field devices such as process controllers) Protection of central server is still important
Unintended consequences	Security solutions are designed around typical IT systems	Security tools must be tested to ensure that they do not compromise normal ICS operation
Time critical interaction	Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary	Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, yet not hamper human-machine interaction
System operation	Systems are designed for use with typical operating systems Upgrades are straightforward with the availability of automated deployment tools	Differing and custom operating systems often without security capabilities Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Resource constraints	Systems are specified with enough resources to support the addition of third-party applications such as security solutions	Systems are designed to support the intended industrial process, with minimal memory and computing resources to support the addition of security technology
Communications	Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices	Many proprietary and standard communication protocols Several types of communications media used including dedicated wire and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers
Change management	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance
Managed support	Allow for diversified support styles	Service support is usually via a single vendor
Component lifetime	Lifetime on the order of 3-5 years	Lifetime on the order of 15-20 years
Access to components	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to them

7.3. DEMAND FOR ADDITIONAL CONNECTIVITY AND RELATED CONSEQUENCES

A growing area of concern for ICSs is the growing desire for interconnectivity between business and engineering systems to the operational systems. Driven by a desire from corporate headquarters, planners, and engineers to access real time plant data, bridges are being established between the tightly bounded control networks running the plant and the unbounded data networks used for corporate access. This bridge can present a gateway for network intrusion.

Another unique architectural characteristic is the existence of emergency remote operating centres. These emergency operating centres offer a remote location for plant monitoring and emergency operation in case an incident makes the primary station unusable. The requirements for monitoring/maintaining some elements of plant control create the need for data flow over some communications medium. This medium offers a potential path for compromise and entry into the main system. Additionally, the requirements for duplicate function create the need for maintaining consistent security requirements across two systems. The failure to maintain one system could create a path for intrusion and exploit injections.

The need for remote analysis, maintenance or updates can also introduce similar vulnerabilities. Before agreeing on such additional connectivity, a thorough risk analysis has to be performed.

7.4. CONSIDERATIONS ON SOFTWARE UPDATES

Many of the current regulations concerning validation or certification of nuclear plant equipment have been developed with analog equipment in mind. This does not become quickly outdated. On the other hand, IT security plans and best practices imply regular updates and patches of software and digital components as these components become obsolete much faster.

It is therefore important to consider the challenge posed by software patches and updates into digital nuclear control or monitoring systems. In the worst case scenario, each software modification or revision could be considered as a system change and may lead to a specific system validation or even recertification for some critical systems. Since such an approach is cumbersome, the result may be a backlog in patch implementation or a conscious decision to delay software upgrade. To limit these effects, distinction should be made between normal maintenance, avoiding such processes, and system modifications requiring retest or even recertification for critical systems. In all cases, any

modifications to safety or safety related systems and to security systems have to be carried out according to agreed procedures.

7.5. SECURE DESIGN AND SPECIFICATIONS FOR COMPUTER SYSTEMS

During the original design and development of many of the existing process control and industrial control systems and instrumentation, computer security was not a major consideration. The recent drive for system and interprocess connectivity, the integration of commercial off the shelf computer systems, and the rise in malicious computer activity (i.e. hacking) has driven the need to consider computer security as a core requirement in the procurement of new equipment.

As a consequence, a formalization of security requirements should be done as a part of the contractual negotiation with suppliers. The ISO document Common Criteria (ISO 15408) [21] is a possible tool to formalize such security requirements. Another example can be found in the attempt to define a Procurement Language for Control Systems [22] by the US Department of Homeland Security, which has published guidance and recommendations on defining cyber security requirements and specific procurement language for control system acquisition.

7.6. THIRD PARTY/VENDOR ACCESS CONTROL PROCEDURE

It is essential that the level of security of any third party and vendors is taken into account. It is paramount that the security department works closely with the contracts department to ensure that the security provisions are incorporated in each contract.

Contracts are often awarded to external entities by organizations in the nuclear industry; some of these contracts will entail the contracting companies holding protectively marked information or assets on their own premises. Unless the award of such a contract and its subsequent management follow stringent rules, the protectively marked information and assets associated with the contract could risk compromise or unauthorized disclosure.

In view of the above factors, it is important that the responsible management of each site/organization in the nuclear industry maintain a close working relationship with the contracting company in order to ensure that essential security aspects are addressed throughout the development and implementation of the contract, and during final handover.

When considered necessary, checks and audits should be made to ensure that the contracting organization's management system adequately addresses security issues, and that the organization's practices and measures are in compliance with the system.

REFERENCES

[1] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary, ISO/IEC 27000:2009, ISO, Geneva (2009).

[2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Information Security Management Systems — Requirements, ISO/IEC 27001:2005, ISO, Geneva (2005).

[3] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Code of Practice for Information Security Management, ISO/IEC 27002:2005, ISO, Geneva (2005).

[4] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:2008, ISO, Geneva (2008).

[5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, ISO/IEC 27006:2007, ISO, Geneva (2007).

[6] COUNCIL OF EUROPE, Convention on Cybercrime, ETS No. 185, COE, Strasbourg (2001).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2002).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection Objectives and Fundamental Principles, Resolution GOV/2001/41, IAEA, Vienna (2001).

[11] The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4 (Corrected), IAEA, Vienna (1999).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance and Considerations for the Implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities, IAEA-TECDOC-967 (Rev.1), IAEA, Vienna (2000).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.3, IAEA, Vienna (2002).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection — 2007 Edition, IAEA, Vienna (2007).

[16] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Management of Information and Communications Technology Security — Part 1: Concepts and Models for Information and Communications Technology Security Management, ISO/IEC 13335-1:2004, ISO, Geneva (2004).

[17] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, Inventory of Risk Management/Risk Assessment Methods and Tools, http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-ra-tools.

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[20] STOUFFER, K.A., FALCO, J.A., SCARFONE, K., Guide to Industrial Control Systems (ICS) Security — Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), Rep. NIST SP-800-82, National Institute of Standards and Technology, Chicago (2011).

[21] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Evaluation Criteria for IT Security, ISO/IEC 15408:2008, ISO, Geneva (2008).

[22] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Cyber Security Procurement Language for Control Systems, September (2009), http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf

[23] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Risk Management — Vocabulary, ISO/IEC Guide 73:2009, ISO/IEC, Geneva (2009).

BIBLIOGRAPHY

AMERICAN NATIONAL STANDARDS INSTITUTE, INTERNATIONAL SOCIETY FOR AUTOMATION, Security Technologies for Industrial Automation and Control System, ANSI/ISA-TR99.00.01-2007, ANSI, Washington DC, (2007).

FEDERAL MINISTRY OF THE INTERIOR, National Plan for Information Infrastructure Protection, BMI, Berlin (2005).

INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection Objectives and Fundamental Principles, Resolution GOV/2001/41, IAEA, Vienna (2001).

INTERNATIONAL SOCIETY FOR AUTOMATION, Integrating Electronic Security into the Manufacturing and Control Systems Environment, Instrumentation, Systems and Automation Society, ISA-TR99.00.02-2004, ISA, Research Triangle Park, NC (2004).

KOREA INSTITUTE OF NUCLEAR SAFETY, Cyber Security of Digital Instrumentation and Control Systems in Nuclear Facilities, KINS/GT-N09-DR, KINS, Seoul (2007).

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE, Good Practice Guide: Process Control and SCADA Security, Version 2.0, NISCC, November (2006).

NUCLEAR ENERGY INSTITUTE, Cyber Security Plan for Nuclear Power Reactors, NEI 08-09 (Rev. 5), NEI, Washington DC (2010).

NUCLEAR REGULATORY COMMISSION, Cyber Security Programs for Nuclear Facilities, Regulatory Guide 5.71, NRC, Rockville, MD (2010).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD, Paris (2002).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks-Towards a Culture of Security, DSTI/ICCP/REG (2003) 5/REV1, OECD, Paris (2003).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, DSTI/ICCP/REG (2005) 1/FINAL, OECD, Paris (2005).

Annex I

ATTACK SCENARIOS AGAINST SYSTEMS IN NUCLEAR FACILITIES

As described in Section 6.3, the nature and form of computer based attacks, all of which must be guarded against, can vary significantly. While the attacks may be of different types, the consequences at a high level include:

— Unauthorized access to or interception of information (loss of confidentiality);
— Unauthorized modification of information, software, hardware, etc. (loss of integrity);
— Block of data transmission lines and/or shutdown of systems (loss of availability).

In developing preventive measures against computer attacks, it is very important to understand the nature of attacks and the potential venues that an attack or attackers may use to gain relevant information and access to target computer systems. **The following are only examples meant to encourage readers — once they have gained a greater understanding of threats — to reflect upon their own organization/system and, if needed, correct the security posture accordingly.** While the depicted attacks are fictional, they relate to plausible scenarios built upon similar attacks seen in other industries. Thinking through such scenarios is a good way to ensure that the security plan addresses the dynamics of the changing threat environment.

A well orchestrated computer attack consists of multiple phases. These phases include:

— Target identification;
— Reconnaissance;
— System access/compromise;
— Attack execution;
— Covering of tracks to maintain deniability.

The following subsections list three fictional computer attack scenarios. The first scenario, having information gathering as one of the goals, could be applicable, as a prelude, to the following two scenarios.

Scenario I — Gathering information to support a malicious act

Goal of the attack — to gain physical access to controlled (limited access) areas of the facility to support subsequent attack.

The target of interest is the person that manages access cards and assigns access privileges. Gaining physical access to restricted areas would include both compromise of the card manager's computer and compromise of the access code system. The attacker chooses to pose as a subcontractor delivering equipment parts.

Possible targets of information collection to support the attack include:

— Personnel information for possible extortion or 'social engineering';
— Design documentation for the access control system;
— Policy and engineering plans of the security systems or other relevant areas of the plant;
— Operational schedules — plant schedule, daily routine, who is working, when they are working, who is on vacation, when certain changes are occurring;
— List of suppliers and when they are working on equipment;
— Equipment and parts inventory;
— Password and access control measures;
— Access control administrative and technical measures;
— Software developer and current project information;
— Network architecture;
— Telecommunication architecture.

Potential methods to gather this information include:

— 'Social engineering';
— Web searches for public information;
— Dumpster diving;
— War dialling, war driving;
— Email attacks — 'phishing'[1] to gain network access, key loggers;
— Installation of software or devices on host machines —via disk, memory stick or CD;
— Eavesdropping on password entry or access code entry (manual, audio or video surveillance).

[1] 'Phishing' refers to attempts to fraudulently acquire sensitive information, such as user names, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

Components of the attack may include:

— Obtaining access card (swipe card) and code;
— Theft/duplication of existing access card;
— Access to card machine to create new card;
— Creation of new employee entry;
— Assuming identity of recently terminated employee;
— Granting desired level of access.

Once card and codes are obtained, the attacker uses the acquired information for organizational activity to enter the facility inconspicuously as a person delivering equipment parts.

Scenario II — Attack disabling or compromising one or several computer systems

Goal of the attack — to sabotage a nuclear power plant and prevent the immediate restart of the plant.

In this example, during a shutdown period a subcontractor is conducting tests on the feedwater control system. The contractor installs a remote access point for monitoring and testing the system from his office. After the contractor completes work the access point remains mistakenly in place.

The attacker has collected plant information that identifies the subcontractor as a prior worker at the plant and a prime target for information regarding the plant. The attacker conducts an email 'phishing' attack against the subcontractor's office and implants a root kit in the system, which gives administrative controls. The attacker thus gains access to the contractors' computer network and discovers the test plans from the plant and also the remote access port which has not been disabled by the plant.

With this information, the attacker is able to conduct a denial of service (DoS)[2] attack on the feedwater control system by flooding the network with traffic causing system failure. The system was designed to process only minimal traffic load.

Once the attacker has gained access, mapped the network and identified the communications protocol, he conducts the attack. The attack results in the loss of response on the feedwater control system that causes manual scramming of the

[2] Denial of service (DoS) is the prevention of authorized access to a system resource or the delaying of system operations and functions.

plant. The reason for the feedwater control system malfunction cannot be immediately determined and the plant remains shut down for investigation.

Scenario III — Computer system compromise as a tool of coordinated attack

Goal of the attack — theft of nuclear material while in transit between storage facilities. A computer attack is to be used to modify the inventory and tracking system to hide the loss of the stolen material.

Reconnaissance and intelligence gathering identifies the process for tagging and tracking radioactive material shipments between storage facilities. This includes RFID[3] tags on the individual items describing the component and listing the content.

The plan of attack includes insider assistance for removal of the material en route. The phases of the attack include:

— Interception of the transport en route;
— Removal of a small quantity of the radioactive material being shipped;
— Reprogramming of the RFID chip to reflect the actual quantity remaining;
— Modification of the inventory tracking system to reflect the new amount as being shipped with the stolen quantity still residing in storage at the home facility.

The computer attack focuses on gaining network access to the inventory database and modifying the inventory and transition log.

[3] Radio frequency identification: A technology used for identification and tracking using radio waves.

Annex II

A METHODOLOGY FOR IDENTIFYING COMPUTER SECURITY REQUIREMENTS

The process of identifying, controlling, eliminating or minimizing threats that may affect computer security at a nuclear facility should be implemented in a systematic and consistent way in compliance with existing standards. This annex offers a more in-depth view of a specific methodology. The choice of this methodology over the many available does not imply its endorsement by the IAEA and should be seen as a detailed example only. For a generic introduction to risk assessment, please refer to Section 6.1.

Generally speaking, to understand the threats and vulnerabilities of a particular computerized system, it is first necessary to analyse the system, functionally and technically, and identify the relevant dependability factors that need to be maintained. Next, risks associated with these factors need to be identified and analysed.

The following paragraphs give an overview of EBIOS. 'EBIOS' is a French acronym standing for *expression of needs and identification of security objectives* (expression des besoins et identification des objectifs de sécurité). It has been designed by the French Information Security Central Office (DCSSI — Direction Centrale de la Sécurité des Systèmes d'Information).[1]

EBIOS provides a formalized approach for assessing and treating risks within the field of information systems security, including support tools for contracting authorities, drafting documents, and raising awareness.

Only the basic principles of the approach are given here, adapted from the documentation available on DCSSI's support web site.

Principles of the EBIOS method

Context study and perimeter definition

The first step is to outline the technical, business and regulatory context of the study. In particular, an information system is based on **essential elements**, functions and information that constitute the added value of the information system for the organization.

[1] Methods to achieve information systems security: http://www.ssi.gouv.fr/site_rubrique113.html

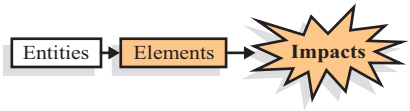
For example, a system monitoring a power plant cooling system relies on various items of information such as measures, parameters and computation results, and on various functions allowing this computation to be carried out.

The essential elements are linked to a set of **entities** of various types: hardware, software, networks, organizations, human resources and sites.

Take the example of a parameter used to trigger a specific pump activation of the cooling system. It is linked to the monitoring computers, processing software, operators, the cold sources state, the plant state, applicable regulations, etc.

Output: Target of the study (Context + elements + entities).

Expression of sensitivities



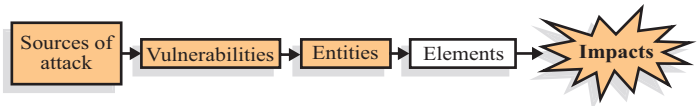
To guarantee that the business operates correctly, the **sensitivity** of each essential element must be expressed.

This expression is based on various **security criteria** such as availability, integrity and confidentiality. If this sensitivity is not covered, there will be an **impact** on the organization, which may take various forms, such as breaches of nuclear security, impaired safety, impaired operation of the activities, loss of customer confidence or financial losses.

Returning to the example of the pump activation parameter for the power plant cooling system, the availability and integrity requirement for this information should be high to avoid any detrimental impact on material, environment or personnel, but also for plant availability.

Output: Sensitivities.

Threat study



Every organization is exposed to various threat agents through its natural environment, culture, image, field of activity, etc. A threat agent can be

characterized by its type (natural, human or environmental) and by its cause (accidental or deliberate).

The threat agent can use various **attack methods** that therefore need to be identified. An attack method is characterized by the security attributes (e.g. availability, integrity, confidentiality) that it can violate and by the likely threat agents.

Returning to the example, a nuclear power plant must take into account a large number of threat agents, as developed in Section 6.3:

— Espionage/technology thieves;
— Disgruntled employee/user (internal or external);
— Recreational hacker;
— Cyber activist;
— Organized crime;
— Nation State;
— Terrorist.

And also attack methods:

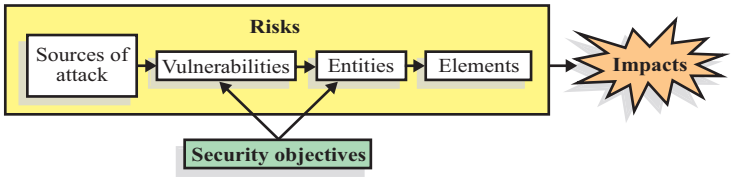
— Eavesdropping;
— Flooding/denial of service;
— Software entrapment/backdoor;
— Login/password attacks (brute force, dictionary, etc.).

Each entity has **vulnerabilities** that can be exploited by threat agents using the relevant attack methods. We can therefore highlight several vulnerabilities linked to the NPP cooling system:

— The possible existence of hidden functions introduced during the design and development phase (software);
— Use of non-assessed equipment (hardware);
— The possibility of creating or modifying system commands online (networks);
— The network, which can be used to tamper with system resource software (networks);
— The ease of intruding into the site through indirect access routes (premises);
— Operators' failure to comply with instructions (personnel);
— The absence of security measures during the design, installation and operation phases (organization).

Output: Threat formalization (including scenarios).

Expression of security objectives



Now determine how the essential elements can be affected by the threat agents and their attack methods: this is the **risk**.

The risk represents possible damage. It arises from the fact that a threat agent can affect the essential elements by using a given attack method to exploit the vulnerabilities of the entities on which these elements depend.

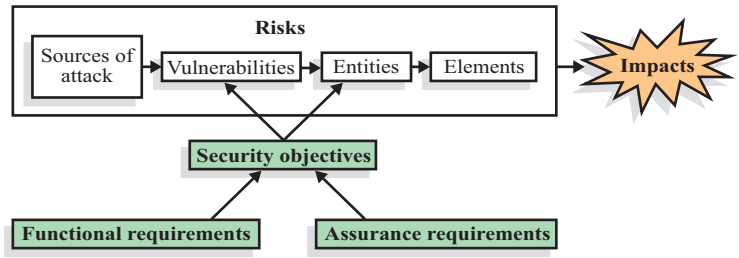
In the example, there is a risk of sensitive information being compromised by software entrapment arising from the possibility of creating or modifying system commands linked to the network, which could have an impact on material, environment, personnel safety, plant availability and public confidence.

The **security objectives** consist mainly in covering the vulnerabilities of the entities representing all the retained risks. Clearly, there is no point in protecting what is not exposed. However, as the risk potential increases, the strength of the security objectives must also increase. These objectives therefore constitute a perfectly adapted set of specifications.

One of the security objectives for the nuclear power plant in the example is to protect the creation and modification of system commands linked to the network for the cooling system.

Output: Security objectives.

Determining security requirements



The team in charge of implementing the approach must then produce exact specifications of the required security functions. After this, it must demonstrate

that the security objectives are perfectly covered by these **functional requirements**.

In the example, functional requirements for protecting the creation and modification of system commands linked to the network could include:

— A series of self-tests run by the system at regular intervals during normal operation to demonstrate that it is operating correctly;
— Physical and logical access control.

Finally, the team in charge must specify the **assurance requirements** allowing the required level of confidence to be attained and then demonstrated.

One of the assurance requirements could be that the developer must carry out a resistance analysis of the system security functions at the required level of resistance.

Output: Functional and assurance requirements.

Annex III

THE ROLE OF HUMAN ERROR IN COMPUTER SECURITY

This annex examines human performance issues associated with computer security; specifically it looks at how human performance can affect an organization's ability to resist attack, recognize attack, recover essential data/service, and adapt against emerging threats. Research continues to push for the development of technical solutions such as security monitoring software, intrusion detection/prevention programmes, stronger authentication systems, and more resistant encryption methods, but very often the human element is ignored as both a cause and as a preventive measure in computer security.

Multiple reports have identified human error as the main cause of computer security breaches. Recent estimates place the number of human error related breaches at 60–80%. Most of these errors could have been prevented with greater investment in awareness and greater diligence in operation and oversight.

System/operational survivability is one of the goals of a computer security programme. The elements of system survivability are:

— System resistance to attack;
— Recognition of attack and damage assessment;
— Essential service and full service recovery;
— System adaptation and evolution as a defence against future attacks.

Table III–1 illustrates these focus areas with an attempt to categorize common types of human errors in processes and applications. Human errors are captured for both system administrators and system users. This list in not intended to be exhaustive, but is meant to illustrate the level of human interaction associated with the implementation of these systems and processes.

While the table focuses on the negative aspects of human performance, the positive impact of human performance must also be noted. While sometimes the weakest link in the chain, the human operator or employee can be a stop-gate that prevents system failure or compromise. Technology will never be a complete solution. Employees are one of the layers of a defence in depth strategy for ensuring system security/survivability. Surveys regularly find that the foremost security issue is inadequate computer security awareness and training.

TABLE III–1. COMMON HUMAN ERRORS

Process/application	Common human errors
Resistance to attack	
Access restriction (System administration)	— File permissions inadequate. — Unnecessary services left on. — Vulnerable ports left open. — Physical access granted. — Failure to use screen savers with password. — Failure to install system patches. — Failure to understand the implication of installing a patch. — Downloading/installing malicious/corrupted software.
Password generation/use	— Passwords written down. — Weak passwords. — Use of default passwords. — Disclosure of password. — Not using a password. — Using the same password on both secure and non-secure systems.
Recognition of attack and damage	
Intrusion detection systems	— Improper configuration (rule set). — Failure to do system updates. — Lack of vigilance in log review.
Log auditing	— Failure to diligently review logs. — Failure to notice trends over multiple log periods.
System recovery	
Backup and restoration	— Failure to make backups. — Failure to make backups in a timely manner. — Improper configuration. — Causing physical damage to the backup media. — Accidental data deletion. — Storage of backup media in an unsecured/unprotected location. — Using defective media. — Mislabelling media. — Physical destruction of media. — Failure to test restoration procedures. — Failure to have multiple copies of critical system information. — Failure to store backup media in an off-site location.

TABLE III–1. COMMON HUMAN ERRORS (cont.)

Process/application	Common human errors
Adaptation to new threats	
Company procedures	— Failure to know company policy. — Violation of company policy. — Lack of a company recovery policy. — Use of an outdated policy. — Failure to verify the policy/procedure work. — Failure to enforce policy.

For employees to be fully utilized as an asset in computer security and system survivability, they need:

— A strong understanding of the importance of their role in the overall computer security plan;
— The computer security knowledge and skills necessary to cover their responsibilities;
— The understanding that an effective security culture starts with them.

DEFINITIONS

For the purposes of this publication, the following terms are used with the meanings given here. These definitions may differ from usage in other disciplines. When available, definitions are taken from existing IAEA publications, though a few terms are used here in the specific context of computer security. Other definitions come from international standards (e.g. Refs [1, 15, 23] of this publication).

access control. Means to ensure that access to assets is authorized and restricted based on business and security requirements (ISO).

attack. An attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset (ISO).

authentication. The provision of assurance that a claimed characteristic of an entity is correct (ISO).

availability. The property of being accessible and usable upon demand by an authorized entity (ISO).

computer security. A particular aspect of information security that is concerned with computer based systems, networks and digital systems.

computer security incident. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a computer based, networked or digital information system or the information that the system processes, stores, or transmits or that constitutes a violation or imminent risk of violation of security policies, security procedures, or acceptable use policies.

computer security perimeter. The logical border around a network to which critical assets are connected and to which access is controlled.

computer security policy. Aggregate of directives, regulations, rules and practices that prescribes how an organization manages and protects computers and computer systems.

confidentiality. The property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO).

countermeasure. An action taken to counteract a threat, or to eliminate or reduce vulnerabilities.

defence in depth. The combination of successive layers of systems and measures for the protection of targets from nuclear security threats.

information security. The preservation of the confidentiality, integrity and availability of information.
Note: In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved (ISO).

integrity. The property of protecting the accuracy and completeness of assets (ISO).

need to know. A principle under which users, processes and systems are granted access to only the information, capabilities and assets which are necessary for execution of their authorized functions.

nuclear facility. A facility (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored or disposed of and for which an authorization or license is required.

risk. The potential that a given threat will exploit the vulnerabilities of an asset, or group of assets, and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and the severity of its consequences.

risk assessment. Overall process of systematically identifying, estimating, analysing and evaluating risk

social engineering. A non-technical form of information gathering or attack that relies on human interaction to manipulate people into inadvertently breaking security procedures, for example disclosing information or performing other actions with a security impact.

threat. Potential cause of an unwanted incident, which may result in harm to a system or organization (ISO).

Note: In other IAEA Nuclear Security Series publications, 'threat' is typically defined as 'a person or group of persons with motivation, intention and capability to commit a malicious act'. However, this publication uses the term in the computer security context, where a threat is not necessarily a person or persons.

vulnerability. Weakness of an asset or control that can be exploited by a threat (ISO).

No. 22

IAEA
International Atomic Energy Agency

Where to order IAEA publications

In the following countries IAEA publications may be purchased from the sources listed below, or from major local booksellers. Payment may be made in local currency or with UNESCO coupons.

AUSTRALIA
DA Information Services, 648 Whitehorse Road, MITCHAM 3132
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

BELGIUM
Jean de Lannoy, avenue du Roi 202, B-1190 Brussels
Telephone: +32 2 538 43 08 • Fax: +32 2 538 08 41
Email: jean.de.lannoy@infoboard.be • Web site: http://www.jean-de-lannoy.be

CANADA
Bernan Associates, 4501 Forbes Blvd, Suite 200, Lanham, MD 20706-4346, USA
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: customercare@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Telephone: +613 745 2665 • Fax: +613 745 7660
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

CHINA
IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing

CZECH REPUBLIC
Suweco CZ, S.R.O., Klecakova 347, 180 21 Praha 9
Telephone: +420 26603 5364 • Fax: +420 28482 1646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FINLAND
Akateeminen Kirjakauppa, PO BOX 128 (Keskuskatu 1), FIN-00101 Helsinki
Telephone: +358 9 121 41 • Fax: +358 9 121 4450
Email: akatilaus@akateeminen.com • Web site: http://www.akateeminen.com

FRANCE
Form-Edit, 5, rue Janssen, P.O. Box 25, F-75921 Paris Cedex 19
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: formedit@formedit.fr • Web site: http://www. formedit.fr

Lavoisier SAS, 145 rue de Provigny, 94236 Cachan Cedex
Telephone: + 33 1 47 40 67 02 • Fax +33 1 47 40 67 02
Email: romuald.verrier@lavoisier.fr • Web site: http://www.lavoisier.fr

GERMANY
UNO-Verlag, Vertriebs- und Verlags GmbH, Am Hofgarten 10, D-53113 Bonn
Telephone: + 49 228 94 90 20 • Fax: +49 228 94 90 20 or +49 228 94 90 222
Email: bestellung@uno-verlag.de • Web site: http://www.uno-verlag.de

HUNGARY
Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
Telephone: +36 1 257 7777 • Fax: +36 1 257 7472 • Email: books@librotrade.hu

INDIA
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001,
Telephone: +91 22 22617926/27 • Fax: +91 22 22617928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell, 2/72, Nirankari Colony, Delhi 110009
Telephone: +91 11 23268786, +91 11 23257264 • Fax: +91 11 23281315
Email: bookwell@vsnl.net

ITALY
Libreria Scientifica Dott. Lucio di Biasio “AEIOU”, Via Coronelli 6, I-20146 Milan
Telephone: +39 02 48 95 45 52 or 48 95 45 62 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Website: www.libreriaaeiou.eu

JAPAN
Maruzen Company, Ltd., 13-6 Nihonbashi, 3 chome, Chuo-ku, Tokyo 103-0027
Telephone: +81 3 3275 8582 • Fax: +81 3 3275 9072
Email: journal@maruzen.co.jp • Web site: http://www.maruzen.co.jp

REPUBLIC OF KOREA
KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seoul 137-130
Telephone: +02 589 1740 • Fax: +02 589 1746 • Web site: http://www.kins.re.kr

NETHERLANDS
De Lindeboom Internationale Publicaties B.V., M.A. de Ruyterstraat 20A, NL-7482 BZ Haaksbergen
Telephone: +31 (0) 53 5740004 • Fax: +31 (0) 53 5729296
Email: books@delindeboom.com • Web site: http://www.delindeboom.com

Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Telephone: +31 793 684 400 • Fax: +31 793 615 698
Email: info@nijhoff.nl • Web site: http://www.nijhoff.nl

Swets and Zeitlinger b.v., P.O. Box 830, 2160 SZ Lisse
Telephone: +31 252 435 111 • Fax: +31 252 415 888
Email: infoho@swets.nl • Web site: http://www.swets.nl

NEW ZEALAND
DA Information Services, 648 Whitehorse Road, MITCHAM 3132, Australia
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

SLOVENIA
Cankarjeva Zalozba d.d., Kopitarjeva 2, SI-1512 Ljubljana
Telephone: +386 1 432 31 44 • Fax: +386 1 230 14 35
Email: import.books@cankarjeva-z.si • Web site: http://www.cankarjeva-z.si/uvoz

SPAIN
Díaz de Santos, S.A., c/ Juan Bravo, 3A, E-28006 Madrid
Telephone: +34 91 781 94 80 • Fax: +34 91 575 55 63
Email: compras@diazdesantos.es, carmela@diazdesantos.es, barcelona@diazdesantos.es, julio@diazdesantos.es
Web site: http://www.diazdesantos.es

UNITED KINGDOM
The Stationery Office Ltd, International Sales Agency, PO Box 29, Norwich, NR3 1 GN
Telephone (orders): +44 870 600 5552 • (enquiries): +44 207 873 8372 • Fax: +44 207 873 8203
Email (orders): book.orders@tso.co.uk • (enquiries): book.enquiries@tso.co.uk • Web site: http://www.tso.co.uk

On-line orders
DELTA Int. Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Email: info@profbooks.com • Web site: http://www.profbooks.com

Books on the Environment
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Telephone: +44 1438748111 • Fax: +44 1438748844
Email: orders@earthprint.com • Web site: http://www.earthprint.com

UNITED NATIONS
Dept. I004, Room DC2-0853, First Avenue at 46th Street, New York, N.Y. 10017, USA
(UN) Telephone: +800 253-9646 or +212 963-8302 • Fax: +212 963-3489
Email: publications@un.org • Web site: http://www.un.org

UNITED STATES OF AMERICA
Bernan Associates, 4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4346
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: customercare@bernan.com · Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Telephone: +888 551 7470 (toll-free) • Fax: +888 568 8546 (toll-free)
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

Orders and requests for information may also be addressed directly to:

Marketing and Sales Unit, International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 (or 22530) • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

11-34841

NUCLEAR SECURITY RECOMMENDATIONS ON PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (INFCIRC/225/REVISION 5)
IAEA Nuclear Security Series No. 13
STI/PUB/1481 (62 pp.; 2011)
ISBN 978–92–0–111110–4 Price: €28.00

DEVELOPMENT, USE AND MAINTENANCE OF THE DESIGN BASIS THREAT
IAEA Nuclear Security Series No. 10
STI/PUB/1386 (30 pp.; 2009)
ISBN 978–92–0–102509–8 Price: €18.00

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS
IAEA Nuclear Security Series No.8
STI/PUB/1359 (25 pp.; 2008)
ISBN 978–92–0–109908–2 Price: €20.00

NUCLEAR SECURITY CULTURE
IAEA Nuclear Security Series No. 7
STI/PUB/1347 (37 pp.; 2008)
ISBN 978–92–0–107808–7 Price: €30.00

INTERNATIONAL LEGAL FRAMEWORK FOR NUCLEAR SECURITY
IAEA International Law Series No. 4
STI/PUB/1486 (30 pp.; 2011)
ISBN 978–92–0–111810–3 Price: €26.00

THE MANAGEMENT SYSTEM FOR FACILITIES AND ACTIVITIES
IAEA Safety Standards Series No. GS-R-3
STI/PUB/1252 (27 pp.; 2006)
ISBN 92–0–106506–X Price: €25.00

APPLICATION OF THE MANAGEMENT SYSTEM FOR FACILITIES AND ACTIVITIES
IAEA Safety Standards Series No. GS-G-3.1
STI/PUB/1253 (123 pp.; 2006)
ISBN 92–0–106606–6 Price: €31.00

INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY IN NUCLEAR POWER PLANTS
IAEA Safety Standards Series No. NS-G-1.3
STI/PUB/1116 (91 pp.; 2002)
ISBN 92–0–110802–8 Price: €14.50

SOFTWARE FOR COMPUTER BASED SYSTEMS IMPORTANT TO SAFETY IN NUCLEAR POWER PLANTS
IAEA Safety Standards Series No. NS-G-1.1
STI/PUB/1095 (89 pp.; 2000)
ISBN 92–0–101800–2 Price: €14.50

This publication seeks to create awareness of the importance of incorporating computer security as a fundamental part of the overall security plan for nuclear facilities. It further aims to provide guidance to nuclear facilities on implementing a computer security programme, and provide advice on evaluating existing programmes, assessing critical digital assets and identifying appropriate risk reduction measures.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–120110–2
ISSN 1816–9317