IAEA Nuclear Energy Series







IAEA NUCLEAR ENERGY SERIES PUBLICATIONS

STRUCTURE OF THE IAEA NUCLEAR ENERGY SERIES

Under the terms of Articles III.A.3 and VIII.C of its Statute, the IAEA is authorized to "foster the exchange of scientific and technical information on the peaceful uses of atomic energy". The publications in the IAEA Nuclear Energy Series present good practices and advances in technology, as well as practical examples and experience in the areas of nuclear reactors, the nuclear fuel cycle, radioactive waste management and decommissioning, and on general issues relevant to nuclear energy. The IAEA Nuclear Energy Series is structured into four levels:

- (1) The **Nuclear Energy Basic Principles** publication describes the rationale and vision for the peaceful uses of nuclear energy.
- (2) **Nuclear Energy Series Objectives** publications describe what needs to be considered and the specific goals to be achieved in the subject areas at different stages of implementation.
- (3) Nuclear Energy Series Guides and Methodologies provide high level guidance or methods on how to achieve the objectives related to the various topics and areas involving the peaceful uses of nuclear energy.
- (4) Nuclear Energy Series Technical Reports provide additional, more detailed information on activities relating to topics explored in the IAEA Nuclear Energy Series.

The IAEA Nuclear Energy Series publications are coded as follows: NG – nuclear energy general; NR – nuclear reactors (formerly NP – nuclear power); NF – nuclear fuel cycle; NW – radioactive waste management and decommissioning. In addition, the publications are available in English on the IAEA web site:

www.iaea.org/publications

For further information, please contact the IAEA at Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of the IAEA Nuclear Energy Series publications are invited to inform the IAEA of their experience for the purpose of ensuring that they continue to meet user needs. Information may be provided via the IAEA web site, by post, or by email to Official.Mail@iaea.org. COMPUTER SECURITY ASPECTS OF DESIGN FOR INSTRUMENTATION AND CONTROL SYSTEMS AT NUCLEAR POWER PLANTS The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN ALBANIA ALGERIA ANGOLA ANTIGUA AND BARBUDA ARGENTINA ARMENIA AUSTRALIA AUSTRIA AZERBAIJAN BAHAMAS BAHRAIN BANGLADESH BARBADOS BELARUS BELGIUM BELIZE BENIN BOLIVIA, PLURINATIONAL STATE OF BOSNIA AND HERZEGOVINA BOTSWANA BRAZIL BRUNEI DARUSSALAM BULGARIA BURKINA FASO BURUNDI CAMBODIA CAMEROON CANADA CENTRAL AFRICAN REPUBLIC CHAD CHILE CHINA COLOMBIA COMOROS CONGO COSTA RICA CÔTE D'IVOIRE CROATIA CUBA CYPRUS CZECH REPUBLIC DEMOCRATIC REPUBLIC OF THE CONGO DENMARK DJIBOUTI DOMINICA DOMINICAN REPUBLIC ECUADOR EGYPT EL SALVADOR ERITREA **ESTONIA ESWATINI ETHIOPIA** FIJI FINLAND FRANCE GABON

GEORGIA GERMANY GHANA GREECE GRENADA **GUATEMALA** GUYANA 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 NORTH MACEDONIA NORWAY

OMAN PAKISTAN PALAU PANAMA PAPUA NEW GUINEA PARAGUAY PERU PHILIPPINES POLAND PORTUGAL QATAR REPUBLIC OF MOLDOVA ROMANIA RUSSIAN FEDERATION RWANDA SAINT LUCIA SAINT VINCENT AND THE GRENADINES SAN MARINO SAUDI ARABIA SENEGAL SERBIA SEYCHELLES SIERRA LEONE SINGAPORE **SLOVAKIA SLOVENIA** SOUTH AFRICA SPAIN SRI LANKA SUDAN SWEDEN SWITZERLAND SYRIAN ARAB REPUBLIC TAJIKISTAN THAILAND TOGO TRINIDAD AND TOBAGO TUNISIA TURKEY TURKMENISTAN UGANDA UKRAINE UNITED ARAB EMIRATES UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND UNITED REPUBLIC OF TANZANIA UNITED STATES OF AMERICA URUGUAY UZBEKISTAN VANUATU VENEZUELA, BOLIVARIAN REPUBLIC OF VIET NAM 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".

NUCLEAR ENERGY SERIES No. NR-T-3.30

COMPUTER SECURITY ASPECTS OF DESIGN FOR INSTRUMENTATION AND CONTROL SYSTEMS AT NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY VIENNA, 2020

COPYRIGHT NOTICE

All IAEA scientific and technical publications are protected by the terms of the Universal Copyright Convention as adopted in 1952 (Berne) and as revised in 1972 (Paris). The copyright has since been extended by the World Intellectual Property Organization (Geneva) to include electronic and virtual intellectual property. Permission to use whole or parts of texts contained in IAEA publications in printed or electronic form must be obtained and is usually subject to royalty agreements. Proposals for non-commercial reproductions and translations are welcomed and considered on a case-by-case basis. Enquiries should be addressed to the IAEA Publishing Section at:

Marketing and Sales Unit, Publishing Section International Atomic Energy Agency Vienna International Centre PO Box 100 1400 Vienna, Austria fax: +43 1 26007 22529 tel.: +43 1 2600 22417 email: sales.publications@iaea.org www.iaea.org/publications

© IAEA, 2020

Printed by the IAEA in Austria December 2020 STI/PUB/1870

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.

- Title: Computer security aspects of design for instrumentation and control systems at nuclear power plants / International Atomic Energy Agency.
- Description: Vienna : International Atomic Energy Agency, 2020. | Series: IAEA Nuclear Energy Series, ISSN 1995–7807 ; no. NR-T-3.30 | Includes bibliographical references.

Identifiers: IAEAL 20-01325 | ISBN 978-92-0-104919-3 (paperback : alk. paper) 978-92-0-109020-1 (pdf)

Subjects: LCSH: Nuclear power plants — Instruments. | Nuclear reactors — Control. | Computer security.

Classification: UDC 621.039.56 | STI/PUB/1870

FOREWORD

The IAEA's statutory role is to "seek to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world". Among other functions, the IAEA is authorized to "foster the exchange of scientific and technical information on peaceful uses of atomic energy". One way this is achieved is through a range of technical publications including the IAEA Nuclear Energy Series.

The IAEA Nuclear Energy Series comprises publications designed to further the use of nuclear technologies in support of sustainable development, to advance nuclear science and technology, catalyse innovation and build capacity to support the existing and expanded use of nuclear power and nuclear science applications. The publications include information covering all policy, technological and management aspects of the definition and implementation of activities involving the peaceful use of nuclear technology.

The IAEA safety standards establish fundamental principles, requirements and recommendations to ensure nuclear safety and serve as a global reference for protecting people and the environment from harmful effects of ionizing radiation.

When IAEA Nuclear Energy Series publications address safety, it is ensured that the IAEA safety standards are referred to as the current boundary conditions for the application of nuclear technology.

The transition of nuclear power plant instrument and control (I&C) systems to digital technology has changed the nature of these systems by enabling extensive interconnection of reprogrammable, functionally interdependent entities. This development has made computer security a necessary element for consideration in I&C life cycles to ensure that provisions and protections are considered and, where appropriate, established at the appropriate life cycle phase. Computer security vulnerabilities may exist in both the design and implementation process as well as within the design and test environment.

There are many useful publications available from various agencies, regulatory bodies and standards organizations that discuss computer security related to nuclear power plant systems, including I&C systems. One such publication is IAEA Nuclear Security Series No. 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, which focuses on computer security design aspects of an I&C design life cycle. That publication is complemented by the present publication, which focuses on implementation issues related to incorporating computer security measures into an I&C system as well as on providing practical guidance for implementing computer security measures during an I&C life cycle.

This publication was produced by a committee of international experts and advisers from numerous Member States. The IAEA wishes to acknowledge the valuable assistance provided by the contributors and reviewers listed at the end of the report, especially the contribution made by C. Lamb (United States of America) as the Chair of the authoring group. The IAEA officers responsible for this publication were J. Eiler of the Division of Nuclear Power and M. Rowland of the Division of Nuclear Security.

EDITORIAL NOTE

Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.

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.

This publication has been prepared from the original material as submitted by the authors. The views expressed do not necessarily reflect those of the IAEA, the governments of the nominating Member States or the nominating organizations.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this book and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1.	INTR	INTRODUCTION 1					
	1.1.	Background					
	1.2.	Objective					
	1.3.	Scope					
	1.4.	Structure					
2.	KEY	KEY CONCEPTS FOR COMPUTER SECURITY FOR NPP I&C SYSTEMS 2					
	2.1.	Safety concepts in overall I&C architecture					
	2.2.	Safety concepts and DiD 4					
	2.3.	Computer security concepts					
	2.4.	Computer security levels					
	2.5.	Defensive computer security architecture specification					
		2.5.1. Trust models					
		2.5.2. DCSA requirements for computer security DiD					
	2.6.	DCSA implementation					
		2.6.1. Computer security DiD					
		2.6.2. Computer security zones					
	2.7.	Information technology and I&C computer systems					
	2.8.	Types of computer security measures					
	2.9.	Security of design artefacts					
	2.10.	Interface between safety and security					
	2.11.	Opportunities to enhance computer security					
	2.12.	Supply chain considerations 13					
	2.12.						
3.	RISK	RISK INFORMED APPROACH TO COMPUTER SECURITY 14					
	3.1.	Modelling					
		3.1.1. Attack surface modelling					
		3.1.2. Threat modelling					
		3.1.3. Facility and system security modelling 16					
	3.2.	Example scenario analysis					
	3.3.	Common mechanism issues					
	3.4.	Common cause access					
	3.5.	Scenario analysis for common mechanism risk 22					
4.	COMPUTER SECURITY IN THE I&C SYSTEM LIFE CYCLE						
	4.1.	General guidance for computer security					
	4.2.	Secure development environment					
	4.3.	1					
	4.4.	Contingency plans 2' I&C vendors, contractors and suppliers 2'					
	4.4.						
	4. <i>5</i> . 4.6.	Computer security training28Common elements of all life cycle phases28					
	4.0.						
		4.6.1. Management systems 28 4.6.2. Computer coupling and cudits 28					
		4.6.2. Computer security reviews and audits					
		4.6.3. Configuration management for computer security					

	4.6.4.	Verification and validation, testing.	28			
	4.6.5.	Computer security assessments	30			
	4.6.6.	Documentation	30			
	4.6.7.	Design basis	30			
	4.6.8.	Access control	30			
	4.6.9.	Protection of the confidentiality of information.	30			
	4.6.10.	Security monitoring	30			
	4.6.11.	Considerations for the overall DCSA.	31			
	4.6.12.	DiD against compromise	31			
4.7.	Specifi	c life cycle activities.	31			
	4.7.1.		31			
	4.7.2.	Selection of predeveloped items.	31			
	4.7.3.	I&C system design and implementation	31			
	4.7.4.	I&C system integration	32			
	4.7.5.	System validation	32			
	4.7.6.	Installation, overall I&C system integration and commissioning	32			
	4.7.7.	Operations and maintenance	32			
	4.7.8.	Modification of I&C systems	33			
	4.7.9.	Decommissioning.	33			
5. SUM	MARY	AND CONCLUSIONS	33			
APPENDI	X I:	SOFTWARE MODIFICATION VIA REMOVABLE MEDIA	35			
APPENDI	X II:	SEPARATION OF SERVICE SYSTEMS AND EXTERNAL COMMUNICATION				
		FROM CLOSED LOOP OPERATION	39			
APPENDI	X III:	NUCLEAR FUEL DEGRADATION DETECTION SYSTEM	43			
REFEREN	CES		46			
ANNEX I:		DATA COMMUNICATIONS SECURITY	47			
ANNEX II:		RECOMMENDATIONS FOR ESSENTIAL DATA COLLECTION	49			
		S TO DRAFTING AND REVIEW	53 55			
STRUCTURE OF THE IAEA NUCLEAR ENERGY SERIES						

1. INTRODUCTION

1.1. BACKGROUND

Historically, computer security was not given significant consideration in the design of instrumentation and control (I&C) systems at nuclear power plants (NPPs). These systems were traditionally seen as being invulnerable or resilient to cyberattacks due to rigid (i.e. hardwired or analogue) implementation, segregation, independence, redundancy and diversity; isolation from external networks; and a general absence of interactive communications (especially with external networks). However, the transition to digital technology has changed the nature of these systems by enabling extensive interconnection of reprogrammable, functionally interdependent I&C systems. This development has made computer security a necessary element for consideration in I&C system design. Malicious cyberattacks on these systems could have serious effects on plant safety and security, which could have the potential to lead to severe and unacceptable consequences. Also, particularly for countries where nuclear power represents a significant part of electricity production, the availability and performance of NPPs can be of vital economic and societal interest.

Computer security vulnerabilities may be introduced into a system during its design, development, operations or maintenance, and vulnerabilities may be discovered or attacks launched against the system at any time. As a result, computer security needs to be established throughout the I&C system life cycle to prevent computer security incidents that could lead to nuclear security events. The IAEA's Division of Nuclear Security has prepared an IAEA Nuclear Security Series publication, No. 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities [1], which provides guidance on computer security considerations that need to be addressed during the life cycle of I&C systems at nuclear facilities. This publication [1] describes computer security measures that prevent, manage (i.e. detect, delay and respond), mitigate and foster recovery from cyberattacks.

The members of the Technical Working Group on Nuclear Power Plant Instrumentation and Control (TWG-NPPIC) recognized the relevance of the above mentioned issues, and in their 2015 meeting recommended that the IAEA provide specific, detailed guidance on the application of computer security concepts and measures to protect and mitigate I&C systems at NPPs against hazards arising from cyberattacks. This guidance was to ensure that security concepts and measures are applied in a manner that is compatible with the safety and performance objectives of the I&C systems. The TWG-NPPIC concluded that there is benefit in engaging I&C subject matter experts to address the practical aspects of implementing computer security measures aligned with both safety and security requirements.

As a starting point, this publication considers the computer security issues to be addressed during the life cycle of I&C systems at nuclear facilities, as identified in Ref. [1]. This publication complements Ref. [1] and provides practical guidance for and case study examples of the implementation of computer security measures in I&C architectures and systems. The guidance is consistent with the requirements and recommendations addressing safety and ensures that application of computer security does not affect the ability of systems to perform their required safety functions.

1.2. OBJECTIVE

The objective of this publication is to assist Member States in the application of computer security concepts and measures to provide protection from cyberattacks for I&C systems at NPPs; it discusses the benefits and challenges of the various methods. The goal of the publication is to provide an overview of current knowledge, up to date good practices, experience, benefits and challenges. The publication is intended to be used by Member States to support the design, development, implementation, operation, maintenance and modernization of digital I&C systems at NPPs.

1.3. SCOPE

This publication covers relevant aspects of computer security in the engineering and design of digital I&C systems for NPPs. The information is useful in supporting new system designs and the improvement of existing systems in operating NPPs.

This publication is applicable to I&C systems and their development, simulation and maintenance environments. Attacks against these environments could lead to errors in the I&C system and result in the I&C system being outside of its design basis. This publication also provides advice for situations where I&C systems are interconnected with enterprise management systems. These non-I&C systems may need to be included as part of the defence in depth (DiD) approach to securing the I&C systems. Finally, there may be circumstances where, as part of a DiD approach, non-computerized I&C systems and non-computerized equipment important to safety, including support systems, can be used to provide protection and mitigation against hazards arising from cyberattacks at NPPs.

1.4. STRUCTURE

This publication is organized into five major sections, three appendices and two annexes. Section 2 defines the key concepts for computer security for I&C systems at NPPs. Section 3 explains the risk informed approach to computer security. Section 4 describes how computer security measures are applied throughout the I&C system life cycle. Section 5 contains a summary and conclusions. Appendices I to III are case studies. Annex I provides information on data communications security and Annex II suggests data to be collected to support the security of I&C systems.

2. KEY CONCEPTS FOR COMPUTER SECURITY FOR NPP I&C SYSTEMS

Computer security concepts are applied to the design of I&C systems to ensure that safety and security requirements are met, and that the cost of maintaining computer security and the need to retrofit computer security measures in the future are minimized. A key concept is the fundamental conflict between safety and security, which is discussed below. Other key concepts described are computer security levels, security zones and computer security DiD. These are important security concepts that designers have to understand when designing and deploying I&C systems.

2.1. SAFETY CONCEPTS IN OVERALL I&C ARCHITECTURE

Typically, I&C systems are deployed within a layered architecture. For the purposes of this publication, the architecture described in IAEA Nuclear Energy Series No. NP-T-2.11¹ [2] is used. Figure 1 and Table 1 provide an overview of this layered architecture.

In nuclear facilities, layers 0–3 correspond to the I&C systems, the protection of which this publication is primarily concerned with. Systems at layer 4 are typically business systems or information management systems, not I&C systems. These systems focus on enterprise computing rather than system control. Some systems at layer 4 are interconnected with and communicate with I&C systems, and these interconnections create a potential risk to those systems; consequently, the security of these layer 4 systems cannot be managed solely within the information

¹ A similar architectural model is defined in IEC 62264-1:2013, Enterprise-control System Integration — Part 1: Models and Terminology [3].

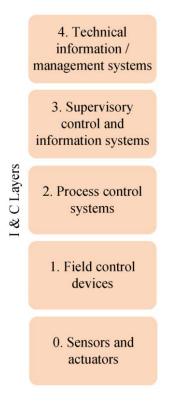


FIG. 1. Concept for I&C layers [2].

TABLE 1. I&C ARCHITECTURAL	LAYERS [2]
----------------------------	------------

I&C Layer	Name	Description
0	Sensors and actuators	Devices that interface with the process directly
1	Field control devices	Devices that forward information from the sensors to the process control layer (signal conditioning) or that manage the actuators (priority management and actuator control)
2	Process control systems	Devices required for automation of the process and safety functions
3	Supervisory control and information systems	Subsystems used for operating and controlling the nuclear power unit by staff in the control rooms
4	Technical information/management systems	Systems used for technical management of the plant

technology (IT) management system. Reference [1] provides guidance on implementing computer security at all security levels.

Note that I&C layers are not equivalent to computer security levels or DiD levels, which will be discussed later. These are distinct concepts addressing specific different computer management issues.

2.2. SAFETY CONCEPTS AND DID

DiD from a safety perspective is defined in IAEA Safety Standards Series No. SSR 2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [4]. In its simplest architectural form this can be conceived as different levels of systems, as shown in Fig. 2.

Broadly, these levels prevent accident progression by providing a series of independent systems that perform different functions so that failure of a system at one DiD level does not prevent the systems at other DiD levels from performing their functions. Typically, the functions performed at each safety DiD level are:

- DiD Level 1: Plant control under normal conditions.
- DiD Level 2: Monitoring for abnormal conditions and automatic inhibit functions.
- DiD Level 3: Reactor trip and actuation of engineered safety features (e.g. to remove decay heat).
- DiD Level 4: Monitoring and mitigation of severe accidents.
- DiD Level 5: Monitoring of radioactive releases.

Each of the systems in each DiD level may have dedicated components associated with some or all of the I&C system layers, but it is possible that some DiD levels may not include components at all layers. For example, a very simple manual system might not include an automatic process control element and might simply consist of controls and displays directly connected to field control devices.

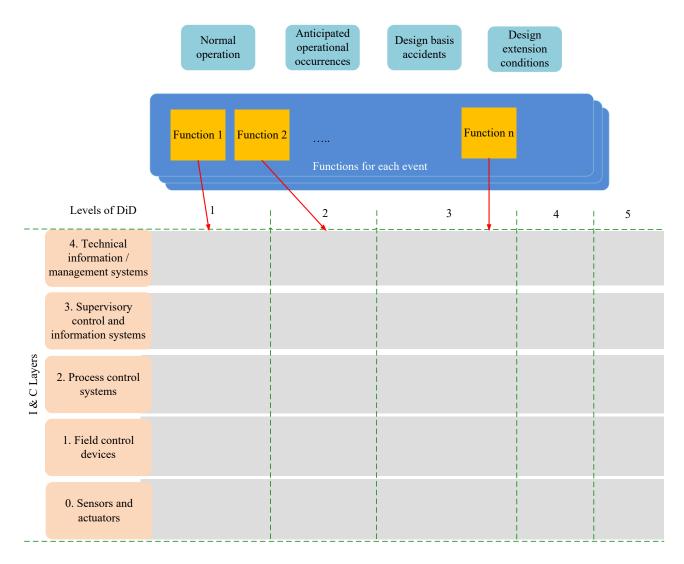


FIG. 2. Generic concept of levels of DiD for safety [2].

It is also possible that there is more than one I&C subsystem for some DiD levels. For example, it is not unusual to see a main protection system at level 3 being backed up by an independent and diverse actuation system to reduce risk further in the event of a protection system failure.

In accordance with the guidance provided in IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [5], DiD within the overall I&C architecture is implemented by means of independent lines of defence so that the failure of one line of defence is compensated for by another one. For a safety system within the overall I&C architecture, this can be achieved by using design principles of physical separation, independence and isolation from other systems (including safety related systems in some cases). These would generally provide adequate segregation between independent parts of the safety system (including pipework and cabling) and also between a safety system and other equipment at the NPP so that in the event of a fault, that fault would not jeopardize the safe working of the safety system(s) within the overall I&C architecture.

Reference [1] notes that the safety analysis alone is not sufficient for managing computer security risk since the malfunctions caused by cyberattacks may place the facility into conditions not considered in the safety analysis. For example, cyberattack has the possibility to cause simultaneous failures of multiple levels of safety DiD. In cases when a cyberattack uses an understood attack technique and known attack goal on a computer based safety system or safety related system, this could be deemed to be another postulated initiating event. There may already be appropriate mitigation in place, but this needs to be confirmed, not assumed. Nevertheless, the increased initiating event frequency needs to be considered. In situations when adversaries use new or unexpected failure goals (e.g. accelerating systems to increase overall system wear), safety impacts are impossible to estimate.

2.3. COMPUTER SECURITY CONCEPTS

Computer security is concerned with three essential attributes: confidentiality, integrity and availability. Different types of computer systems have different levels of requirements for protection of these three attributes. For example, a reactor protective system has stringent requirements for integrity and availability, whereas confidentiality of information contained within the system may be of less importance.

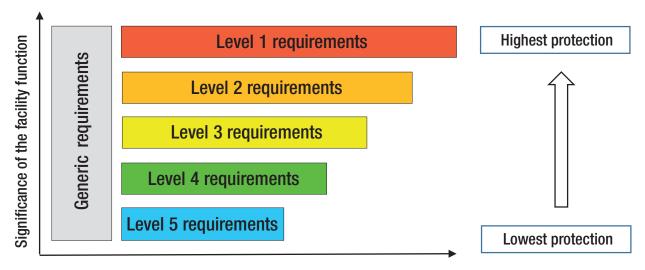
A personnel management system contains sensitive, personal information that must be kept confidential and accurate, but may have less stringent requirements on availability. In this case, the system has high confidentiality and integrity requirements, but limited availability needs. Such a system is an IT system and is not the focus of this publication. The US National Institute of Standards and Technology addresses such systems and the analysis required to categorize their security requirements in their federal information process standards, specifically in Ref. [6].

2.4. COMPUTER SECURITY LEVELS

Reference [1] defines a graded approach in which computer security measures are applied to computer based systems associated with an NPP proportionate to the potential consequences of a cyberattack against the functions that the system performs. Reference [7] provides guidance on the use of a facility computer security risk management process to identify and rank the consequence of compromise of all facility functions. To simplify the application of a graded approach, Ref. [7] proposes that the functions be assigned to a discrete set of security levels and provides an example using five levels. Reference [7] describes criteria for determining the computer security level of an I&C function and describes a typical assignment of I&C systems to computer security levels.

A computer security level consists of a set of computer security requirements or conditions imposed on a computer based system associated with an NPP. In the example of Ref. [7], security levels range between level 5 (least protection needed) and level 1 (most protection needed), as illustrated in Fig. 3. Each level consists of graded computer security requirements, such as restrictions on the communication between systems of different security levels. This graded approach ensures that organizations allocate their limited resources to implement computer security first to those systems performing the most critical functions.

Computer security levels and safety classes are distinct but related concepts. The safety classification, in accordance with Ref. [8], of an I&C system or subsystem is based on the safety category of the safety function that the I&C system performs. The computer security level is assigned to an I&C system, subsystem or component



Security level/strength of requirements

FIG. 3. Illustration of the graded approach using the computer security level concept [7].

based on the potential consequence arising from its failure or maloperation, including operation in a way that differs from the item's design intent or conceivable failure modes.

The potential consequences of a compromise on I&C system function, arranged from worst case to best case, are:

- The function is indeterminate. The effects of the compromise result in an unobserved alteration to system design or function.
- The function has unexpected behaviours or actions that are observable to the operator.
- The function fails.
- The function performs as expected, meaning the compromise does not adversely affect system function (i.e. fault tolerant).

Reference [1] also states that cyberattacks against I&C infrastructure may compromise single I&C systems or multiple I&C systems, and that cyberattacks can be combined with physical elements. Malicious acts have the potential to bypass or cause simultaneous failure of multiple DiD levels. For example, a cyberattack might simultaneously:

- Affect multiple channels of a reactor protective system;
- Affect diverse protective systems;
- Affect a process control system and a protective system.

Such attacks could place the facility in conditions that are not considered by the safety analysis.

The computer security measures required by each security level are not considered to be cumulative, thus computer security measures present in one security level may be repeated in other security levels. This is because a security level (e.g. level 1) does not trust a security level having less stringent requirements (e.g. levels 2, 3, 4, 5) and therefore cannot rely upon computer security activities in these lower levels.

2.5. DEFENSIVE COMPUTER SECURITY ARCHITECTURE SPECIFICATION

Reference [7] provides guidance on developing a defensive computer security architecture (DCSA) specification as part of the facility computer security risk management process. The DCSA specification contains the computer security requirements applicable to the facility's overall I&C architecture.

The DCSA specification uses a graded approach to computer security based on computer security levels and defines architectural requirements that provide a higher degree of protection to functions assigned to higher security levels (i.e. most stringent security level). This includes computer security requirements to restrict and control communications between facility functions and physical security requirements for equipment performing these functions. The DCSA specification ensures that facility functions with the highest significance are assigned to the most stringent security level.

The DCSA specification requirements for communications between facility functions include computer security requirements for controlling data flow between functions assigned to different security levels and for controlling data flow between functions assigned to the same security levels. This could include computer security requirements for the use of secure protocols for communication between functions.

2.5.1. Trust models

The data flow requirements within the DCSA are based on a trust model appropriate for the systems being protected. Different trust models may be used depending upon the objectives for security or integrity. In general, for I&C systems performing critical safety functions, integrity is the overriding security objective. The Biba model is one such trust model, which is intended to provide integrity.

The key properties of the Biba Model are as follows:

- Simple integrity property: A function cannot receive information from a function at a less stringent security level ('read up').
- Star integrity property: A function cannot write data to a function at a more stringent security level ('write down').
- Invocation property: A function at a less stringent security level cannot request access to a more stringent level. It can request access to a function at a less stringent level or one at the same level.

An example of a DCSA that implements the Biba Model is NEI 08-09 [9]. Figure 4 shows a high level representation of the Ref. [9] DCSA requirements on data flows between functions at different security levels.

In the example of Ref. [9], only unidirectional communication is permitted from the most stringent level to the less stringent level below (i.e. NEI 08-09 level 4 to level 3). By requiring unidirectional communication, the star integrity property is strictly enforced by preventing data from being written to the most stringent level (NEI 08-09 level 4) from a less stringent level (i.e. NEI 08-09 level 3). The requirement for unidirectional communication also ensures that the invocation property is strictly enforced by preventing a function at the less stringent level from accessing a function at the most stringent level. The simple integrity property is also met since a function at the less stringent level can receive data from the most stringent level.

In the example of Ref. [9], for communication between the least stringent level (NEI 08-09 level 0) and the more stringent level above it (NEI 08-09 leve 1), the requirements of the Biba Model are less stringently enforced. In the NEI 08-09 model, communications between these levels are permitted to use bidirectional protocols. This allows for the potential for a function at the less stringent level to access a function or to write data to the more

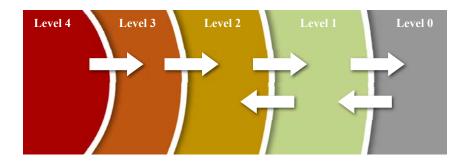


FIG. 4. Arrows here show the NEI 08-09 DCSA requirements on data flows between functions at different security levels. Note that the numbering of security levels in this figure is reversed from those used in IAEA guidance because in NEI 08-09 level 4 is the most stringent level, whereas in IAEA guidance, level 1 is the most stringent level.

stringent level. To ensure that the Biba Model requirements are met, they have to be enforced by the configuration of the boundary control device and the design of the functions themselves.

For example, if a firewall is used as a boundary control device, the firewall configuration could ensure that a function assigned to the more stringent level would be able to initiate transfer to functions assigned to the least stringent level, but that it would block any access attempts in the opposite direction, thereby enforcing the invocation property. However, this single security measure is not sufficient to ensure that this property is strictly met, since once the connection is established, bidirectional communication between functions is permitted. Consequently, the realization of the systems implementing those functions needs to ensure that access and data flow between functions meet the Biba Model requirements (i.e. the simple integrity property and invocation property).

In a cyberattack, adversaries could potentially put systems outside their design basis and exploit permitted communications channels by adding functionality that violated the trust model. Additional measures are required in addition to the firewall to detect and prevent such exploitation of trusted communication between functions that are using bidirectional protocols.

In considering functions at the same level of security, caution needs to be taken in permitting communication between these functions and the requirements for protecting such communication. The designer needs to give careful thought to extending trust between devices and networks at the same level.

Explicit understanding of the trust relationships between functions is vital to making these dependencies clear (see Ref. [10]). The best time to establish, secure and document such relationships is when designing a system, not during implementation. During the design phase, these decisions are easier to make and much less expensive to fix.

It is particularly important that engineers understand the logical interfaces of systems they design, the trust relationships between interfacing devices and how trust is established. Implicit extension of trust to functions outside of the designer's control can undermine the security of critical functions. Mediating measures such as network communication proxies or port mirrors can provide an explicit trust boundary. For example, maintenance or development environments may be completely trusted by production systems. It is important that engineers realize this trust relationship exists, so it can be removed or adequately protected before moving a system into operation. Understanding and explicitly documenting trust relationships, trust constraints and trust controls is vital to ensure secure operation of I&C systems.

2.5.2. DCSA requirements for computer security DiD

Computer security DiD provides protection against the undesirable consequences potentially arising from cyberattack just as safety DiD protects against system failure. While these concepts are similar, there are differences, which are discussed further in Section 2.6.1. DiD is primarily an implementation concern; however, the DCSA specification places requirements upon the application of DiD.

The requirements contained within the DCSA specification include those necessary to provide for computer security DiD using a combination of independent and diverse computer security measures that have to be overcome or circumvented by adversaries to achieve their objectives through a compromise of facility functions. The DCSA specification defines the mixture of technical, physical and administrative control measures that provide adequate protection and ensure that compromise or failure of a single computer security measure does not result in severe or unacceptable consequences. Finally, the DCSA specification provides requirements for independent and diverse computer security measures which prevent an adversary from exploiting a vulnerability common to multiple security levels.

The DCSA requirements for DiD may provide for computer security measures at different system layers to protect against compromise originating within those layers or targeting those layers from adjacent layers (see Ref. [11]).

2.6. DCSA IMPLEMENTATION

Reference [1] recommends the use of DiD in implementing the DCSA requirements, and the DCSA specification will place requirements upon DiD. The primary mechanism recommended for implementing DiD is the computer security zone concept. This concept involves implementing logical and/or physical grouping of systems that share common computer security requirements. DiD is achieved by requiring that each zone assigned

to a specific level be arranged within a DCSA and protected from cyberattacks originating in zones on the same or adjacent levels.

In implementing the I&C system, care needs to be taken to ensure that computer security does not affect the ability of a system to perform its credited safety functions. Computer security zones can be used to establish an area that allows for trusted communications between components that comprise a system implementing a safety function, thereby ensuring that the security measures cannot impact the function. This needs to be considered in the assignment of systems to zones.

2.6.1. Computer security DiD

Reference [1] acknowledges DiD in safety applications and refers to it as 'safety DiD' to differentiate it from DiD as applied to computer security. Reference [1] (para. 4.142) defines DiD against compromise as follows:

"Defence in depth against compromise involves providing multiple defensive layers of computer security measures that must fail or be bypassed for a cyber attack to progress and affect an I&C system. Therefore, defence in depth is achieved not only by implementing multiple defensive layers (e.g. security zones within a defensive computer security architecture), but also by instituting and maintaining a robust programme of computer security measures that assess, prevent, detect, protect from, respond to, mitigate and recover from an attack on an I&C system. For example, if a failure in prevention were to occur (e.g. a violation of policy) or if protection mechanisms were to be bypassed (e.g. by a new virus that is not yet identified as a cyber attack), other mechanisms would still be in place to detect and respond to an unauthorized alteration in an affected I&C system."

Diversity is an important factor to consider for both safety and security DiD. This fundamentally provides additional protection against common cause failure and is an effective and vital measure in both safety and security. When considering diversity in digital systems, it is important to recognize that different manufacturers could be using common third party software and therefore will be subject to both common systematic failures and to cyber vulnerabilities.

2.6.2. Computer security zones

References [1] and [7] use the concept of computer security zones for implementation of the DCSA. Reference [1] discusses the development of security zones and levels for identifying potential security measures. Paragraph 2.28 of Ref. [1] states:

"The security zone concept involves the logical and/or physical grouping of computer based systems that share common computer security requirements, due to inherent properties of the systems or their connections to other systems. All systems located within a single zone are protected at the same security level, namely that assigned to the I&C system function with the most stringent security level within the zone. Grouping of I&C systems into security zones may simplify the application and management of computer security measures."

The use of zoning within a DCSA supports computer security DiD; Ref. [7] states that, in this approach, an adversary may have to traverse multiple zones assigned to different security levels before having the opportunity to compromise a system at security levels 1, 2 or 3. In this way, the measures implemented for zones requiring less stringent levels contribute to the protection of zones requiring more stringent security. For instance, a cyberattack might be detected at level 4 or 5 before the adversary gains access to the most critical systems, thereby allowing a response that prevents the propagation of the attack.

This is only the case if the I&C architecture correctly implements the DCSA requirements. Furthermore, a direct attack against a system performing a security level 1 function could be conducted through direct access to the zone in which the function is implemented (e.g. attaching maintenance equipment to the system without taking required precautions).

DiD between zones assigned to different computer security levels can be maintained by requiring that each zone assigned to a specific level be protected from cyberattacks originating in zones on the same or adjacent levels.

To ensure computer security DiD, the DCSA specification and the computer security plan identify computer security measures assigned to each security level that are implemented within the security zones and at zone boundaries. Cybersecurity staff periodically evaluate the effectiveness of these measures to ensure that sufficient protection is provided for the I&C systems assigned to each security level.

In implementing systems, designers allocate functions to single systems or to multiple systems and can also allocate multiple functions to a system. Facility functions that have similar safety significance may also have similar requirements for security and could be placed in the same zone. Care needs to be taken that allocation of systems to security zones does not create opportunities for an attacker to develop a common cause access based attack against multiple critical functions.

Reference [7] provides further guidance and examples of computer security zones, as shown in Fig. 5.

Computer security zones are intended to prevent or delay attacks since adversaries may need to traverse multiple zones to compromise facility functions. Ideally, computer security measures used in zones at one level are diverse and independent of the computer security measures used in zones at adjacent levels, to mitigate common cause failures of the protection mechanisms. For high consequence facilities, including NPPs, facility functions requiring the highest level of security (i.e. the most stringent security level) are best connected to other facility functions via fail secure, deterministic, unidirectional data communication pathways as per the DCSA specification.

DiD within a specific DCSA level can be encouraged by requiring that each level employ independent and diverse computer security measures within that level. In accordance with the principle of a graded approach, the requirements for independence and diversity are usually greatest for those levels requiring the most stringent protection (i.e. security level 1).

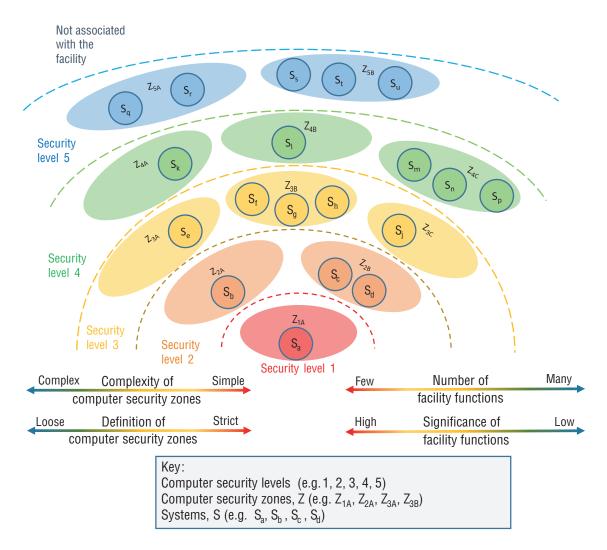


FIG. 5. Conceptual model of computer security levels and zones [7].

The design of the I&C systems takes into account the security requirements in addition to consideration given to monitoring (intrusion detection systems, IDSs) and forensic capture in case a security measure is breached and the system is compromised. Forensic analysis could provide information to assist in identifying vulnerabilities and understanding the severity of a compromise.

Implementation of any computer security measures has always to be mindful of the safety requirements and must not in any way impede the safety system performing its safety function as per the design intent. The IEC Standard 62859, Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Coordinating Safety and Cybersecurity [12], provides further information in this area. It is also discussed in Section 2.10 of this publication.

2.7. INFORMATION TECHNOLOGY AND I&C COMPUTER SYSTEMS

Computer security in I&C systems is typically evaluated against overall availability, integrity and confidentiality requirements, as well as occasionally non-repudiation and authorization/authentication.

I&C systems are different from typical enterprise computer systems and have different security requirements as a result. In general, in I&C systems, confidentiality of plant operational data flowing between system components may be considered of reduced importance in some cases relative to data integrity and availability. Commands transmitted to remote terminal units, if captured, could provide an adversary with insight into normal system operations, allowing for replay or later attack, and credentials can be later reused for system access. Confidentiality is certainly important, though integrity and availability are generally more important operationally. While important from a reconnaissance perspective, this kind of information is also available via the analogue loophole as an adversary may be able to see the effect of a command by observing the physical effect of the command (e.g. closing a valve or activating a switch). Information processed within I&C systems typically has limited value over time and does not have lasting sensitivity when removed from the operational context.

System availability and integrity in I&C systems are much more important than in typical enterprise systems.² In an I&C system, computer security measures that protect integrity are ideally in place to ensure that there is a high guarantee that instructions and interprocess command and control data are not corrupted, whether by accident or intentionally. Similarly, some level of device software integrity is essential to ensure the system operates as expected, as per the system design, implementation and documentation. Failure to ensure device software integrity can put the system outside its design basis. Most I&C systems in NPPs have very stringent availability requirements to ensure that real time performance of these mission critical systems is sustained at all times.

Although non-repudiation is important from an auditing perspective and to enable control system forensics, it may not be as important as other attributes with immediate functional implications. With that in mind, being able to prove that a command message was in fact sent from an authorized system can be a powerful defensive mechanism to ensure the delivery of only appropriately authorized command messages.

These availability and integrity requirements provide a different focus for I&C system computer security compared with enterprise computer deployments. Today, confidentiality of data in enterprise computers is very important to protect against unauthorized access and exposure. On the other hand, I&C systems are more strongly focused on integrity and availability. This has implications for overall system design. Commercial computer security solutions intended for enterprise systems may not be the best fit for nuclear power systems, due to their inability to meet data availability and integrity requirements.

² Authenticity in this publication is considered part of the integrity requirement of the entire I&C system and architecture. Data authentication has two elements: authentication of the transmitting entity (i.e. data source) and validation of the integrity of that data. Annex I provides further details on data communications security.

2.8. TYPES OF COMPUTER SECURITY MEASURES

In general, computer security measures are of three different types: administrative, physical and technical. They all are used to either prevent, detect, and delay or to respond to computer attacks. These types of control measures are distinct and are usually used in groups:

- A *physical* control measure is a physical barrier protecting a sensitive asset. Examples include doors, gates or guards.
- A *technical* control measure uses hardware and/or software (to prevent, detect, mitigate the consequences of and recover from an intrusion or other malicious act). Typical examples include firewalls, IDSs or security event management systems.
- An *administrative* control measure is a policy, procedure or practice to specify certain actions (i.e. permitted, necessary and forbidden ones). It is something that is controlled by the company in some way (such as issuing access passes) and does not technically or physically protect a system or function.

Reference [1] provides additional detail on these kinds of controls.

Two key administrative control measures for I&C systems are the DCSA specification and the computer security programme (CSP). Reference [7] provides guidance on how to define the requirements for the DCSA and elements of the CSP, including the required measures.

The DCSA specification is an administrative control measure that defines the architectural requirements for protection of I&C systems in a graded manner. The DCSA defines requirements for logical and physical protection of I&C systems.

The DCSA specification is not sufficient to reduce the risk of cyberattack to zero and residual risk remains. The CSP (and associated plan and procedures) is an administrative control measure, which ensures that this residual risk is managed to an acceptable level. The CSP plans, controls and records key computer security activities as part of the facility's integrated management system and defines and establishes the interfaces with other facility programmes (e.g. quality management, modifications and emergency response).

2.9. SECURITY OF DESIGN ARTEFACTS

During design, most software and generated design artefacts (e.g. drawings, source code, executable code and configuration files) are best carefully controlled and limited to only authorized access. Product life cycle management software systems provide this kind of functionality and link to other software as well, including requirement management systems, documentation management systems, task management systems, source code management systems, and system maintenance software, as well as systems back in after documentation management scientific, engineering and safety analysis software. Section 4.2 provides additional details on securing the design environment.

All of these systems and their respective documentation can be controlled for data leakage to protect sensitive information from non-authorized users. Information leakage or unauthorized access to any of these systems can lead to potentially serious consequences. For example, software design documentation such as source code or network diagrams can provide adversaries with sufficient information to aid in defeating system access protection mechanisms.

2.10. INTERFACE BETWEEN SAFETY AND SECURITY

Computer security measures and safety measures have to be designed and implemented in an integrated manner so that computer security measures do not compromise safety and safety measures do not compromise computer security. The risk of computer security measures impacting system functions, reliability or overall safety needs to be clearly understood and be subject to ongoing analysis.

Computer security measures, if designed inappropriately, may introduce potential failure modes into the system, increase the potential for a spurious operation and challenge the system's ability to reliably perform its

safety functions. The function or failure of computer security measures must not degrade the safety functions of I&C systems.

Computer security measures must not reduce the effectiveness of the design measures for safety function such as diversity, separation and isolation, redundancy and DiD. However, the absence of a security solution is equally unsuitable.

2.11. OPPORTUNITIES TO ENHANCE COMPUTER SECURITY

NPP I&C designs will vary significantly depending on the NPP's age and position in the upgrade life cycle. This will influence the security issues and opportunities associated with system development that need to be addressed within the life cycle.

The potential for improvement of the plant I&C security architecture as part of an upgrade depends upon the existing architecture and the scope of the upgrade. New systems and equipment or replacements have the potential to allow improvements to the architecture, including possibly centralizing security functions. Overall architectures can be modified to more strongly incorporate computer security services during upgrades as well.

New construction NPPs' I&C architectures typically include a greater level of digitization but can include computer security requirements in their initial system requirements where they can be appropriately balanced between safety, security and operational requirements. This may, however, lead to a higher reliance on digital technologies in every security zone. The ability to have a CSP in place from the beginning of the lifetime of the facility can create a significantly more secure system, provide better system performance and have significant cost savings over adding computer security requirements after the system is designed.

System refurbishment projects provide another opportunity, depending on the breadth of their scope, to improve the overall computer security of the facility. They provide the opportunity to better secure the portion of the system being modernized. New technologies often provide new features to enhance overall computer security, but these new mechanisms need to be understood. These new designs will need to be evaluated according to policies and requirements included in the CSP and DCSA specification.

2.12. SUPPLY CHAIN CONSIDERATIONS

Computer security considerations are mandated on vendors who perform I&C system design, system supply, system storage and system maintenance activities for nuclear facilities. The introduction of system vulnerabilities by an external vendor performing these activities is a risk area, and appropriate measures, procedures and processes are needed to prevent the introduction of system vulnerabilities.

Vendor contracts and agreements define the computer security requirements applicable to the vendor and include terms that stipulate the vendor have a documented CSP, which is reviewed and accepted by the nuclear facility. The vendor's CSP outlines the computer security requirements of any subvendors that are providing materials or services to the vendor. Contract terms can be included that permit the nuclear facility to periodically audit the vendor's CSP. From time to time, the facility will perform these audits to ensure that the vendor's CSP is being appropriately followed.

Computer security measures for vendors designing I&C systems that may be included in the contract terms include:

- Use of computer security design principles and best practices as outlined in this publication, in Ref. [1] and in other applicable standards;
- Requirements for security screening assessments of design and support engineers, as well as any other personnel involved in system development (including subcontract vendors);
- Controlled, secure and restricted access to the vendor's development facility;
- Isolation of development systems and support tools from broader computer networks;
- Allowance for periodic computer security design reviews throughout the design process by knowledgeable representatives from the nuclear facility;

- Contractual clauses that permit the nuclear facility to require that identified computer security concerns are appropriately mitigated or resolved by the vendor prior to completing the system's final design;
- Vulnerability scanning on preliminary designs and implementing appropriate resolutions to identified vulnerabilities;
- Malware scans performed and documented on systems prior to finalizing the software release and prior to system delivery;
- Removal of any unused 'dead code' prior to system software release;
- Disclosure to the nuclear facility of any known system vulnerabilities or common access mechanisms within the final design, whether identified during the design phase or at any point thereafter (including after system delivery);
- Consideration for intrusive assessment testing/penetration testing of the vendor's design by the nuclear facility
 or an agreed upon third party;
- Post-delivery support clauses that require the vendor to provide system support for delivered systems in case there is a subsequent computer security incident involving that system;
- Security requirements that apply during delivery, transit and any storage of systems and/or system components (these can include intrusion and tamper detection tags, requirements on locking of packaging, etc.);
- Disclosure to the nuclear facility of the results of any internal or external audits that the vendor receives on its CSP and/or processes.

For I&C systems that are serviced and/or maintained by an external third party vendor, appropriate computer security clauses are included within the vendor contract terms and agreements. Such clauses may include:

- The requirement that the vendor perform malware scanning using up to date malware definitions, both prior to and after connection of any removable media or portable computing device to an I&C system.
- Ensuring that any maintenance laptops or other portable computing device implement computer security measures, such as having up to date anti-malware software.
- Ensuring that any remote network connections, including wireless connections, are disabled during any maintenance activity on the I&C system.
- The use of dedicated maintenance tools and portable computing devices for each particular instance of an I&C system. Considerations are given to requiring a disk wipe and software reimage of the maintenance tool/ portable computing device prior to connection to the I&C system.
- Requirements for security screening assessments of vendor maintenance personnel.

3. RISK INFORMED APPROACH TO COMPUTER SECURITY

The I&C system computer security risk assessment report uses the facility computer security risk assessment report (if available) and the design basis documents for the I&C systems as inputs to determine the security risk posed by cyberattacks against individual or multiple I&C systems, subsystems or components. This computer security risk assessment is undertaken in accordance with Refs [1] and [13]. The computer security risk assessment is performed by computer security specialists with the involvement of I&C and safety engineers.

To assist in implementing a graded approach, an I&C system, subsystem or component will be assigned to a computer security level and allocated to a computer security zone as described in Section 2.

The level of risk associated with each system is identified as the combination of the likelihood of an adversary initiating an attack, combined with the consequences of such an attack. Modelling provides for a process to quantify the likelihood and consequence. Scenario analysis is performed to raise confidence in the assumptions and the outputs of the model.

3.1. MODELLING

A large variety of modelling techniques can be applied to computer security analysis of NPPs. Some of these, such as attack surface modelling, explicitly address computer security tactics and techniques. Others, such as plant functional modelling, may not explicitly address computer security at all, but can still provide insight into possible consequences of computer attacks.

3.1.1. Attack surface modelling

Attack surface modelling is performed as part of the facility and system modelling and characterization. To understand the means available by which threat actors can potentially gain access to a new system (i.e. the attack vectors), engineers need first to define the system's attack surface. The attack surface describes the set of possible ways an adversary can compromise a system based on the access they may have.

The term attack surface has been defined differently by different organizations. For the purposes of this publication, the definition of attack surface from the EPRI's Cyber Security Technical Assessment Methodology: Vulnerability Identification and Mitigation [14] is used:

"An attack surface is defined by the composition of attack pathways through access points (not to be confused with wireless access points) where an attacker can exploit a vulnerability. Implementation of cyber security control methods mitigates the size of the attack surface by mitigating vulnerabilities and attack pathways."

For a detailed approach on how to identify attack pathways, see Ref. [14]. The security domains outlined in Ref. [13] will assist the assessor with observations and questions to help address these areas. Specifically, the security policy, physical and environmental security and computer system acquisition, development and maintenance domains provide additional focus in these areas.

Part of the attack surface analysis is mapping all data flows required for operation (abnormal and fault operation and severe accident, if appropriate), maintenance and testing. Any setting changes that are permitted without following a formal modification process are also part of the attack surface. From these data flows, the attack vectors are identified. Attack vectors are inherent to the facility or system being modelled and exist irrespective of the capability of an attacker.

The likelihood of exploitation is based on the existence and availability of the vector (system characterization) and the ability of the adversary to access the vector (see Section 3.1.2). The capability of the attacker varies with time (as new techniques are developed) and is difficult to know with certainty since the attackers conduct their activities in secret. Consequently, the existence and availability to the vector is of primary importance to attack surface modelling. Detailed knowledge of the threat is not required to identify the availability of the system. Removal of the attack vector during design reduces the attack surface and can be accomplished without any specific knowledge of the threat.

Accessibility to the vectors identified by Ref. [14] includes the following:

- Wired networks: These communication mechanisms (for example, IEEE 802.1, RS-422) use wires or fibre optic cables to transmit data between computer based systems. To access a wired network, an adversary requires physical access to the network, cabling or a node on that network (including remote nodes).
- Wireless networks (for instance Bluetooth, Zigbee, IEEE 802.11): Radio signals are used to communicate between computer based systems. An adversary needs to have proximity to the network devices to intercept the signal and communicate. For example, for IEEE 802.11 the proximity could be greater than 10 km.
- Physical interfaces: The physical attack vector could allow the adversary to input commands directly into the system, damage or alter the equipment, turn the equipment off or on, or put it into different modes. This requires direct physical access to the equipment, its human-system interfaces (HSIs) or switches and buttons. For example, the adversary could potentially access the HSI to change the function, damage the equipment or alter the equipment in some way. Access requires the attacker to have direct physical contact.
- Portable interfaces: These interfaces are provided to attach portable equipment to computer based systems. Examples of these interfaces are USB ports, serial ports, parallel ports, firewire ports and small computer system interface (SCSI) ports. An adversary requires physical access to these ports to use removable media and

mobile devices to exchange malicious data, attach rogue access points or provide power for other malicious devices. The attacker can directly access the port or compromise media or devices that are to be connected to it.

Supply chain: An adversary's access to the supply chain depends upon the vendor or service provider's security
programmes.

Risk assessments are re-evaluated once new information about the design or threat becomes known, or when computer security measures are implemented or adjusted.

Computer security measures are mapped to the identified attack pathways with focus on high risk pathways. For example, if it is identified that an operator changing trip thresholds is a high risk pathway, then computer security measures that prevent an operator from being able to perform this action when acting alone, along with measures to prevent the operator from becoming compromised by attack (e.g. background check, security culture training, raising awareness of targeted attacks), would both be appropriate. The aim is to balance risks (through appropriate allocation of computer security measures) and eliminate weak spots whereby an attacker can gain access to an attack vector.

A few means of reducing the attack surface that may be identified through attack surface modelling may include isolation of the system from any network, device operating system hardening, and implementing measures to limit physical access to the system.

3.1.2. Threat modelling

Threat modelling is the exercise of enumerating and understanding the overall threat profile of a system. Threat modelling focuses on the attacker and is performed independently of the facility or system characterization. A threat model will address possible adversaries, the motivations of those adversaries, attack vectors that adversaries have used in the past and possible goals of the adversaries.

In most cases, a designer needs to have access to a threat model developed by NPP computer security personnel. This can be used in tandem with the attack surface model developed by the designer when designing the control system to better understand risks associated with possible attack vectors.

The capabilities of the adversary are constantly changing and, as a result, the threat model needs to be periodically updated. If the adversary develops new or greater capabilities, this may provide the adversary with greater opportunity to compromise facility functions in a manner that was not previously considered. If the threat model identifies changes in adversary capabilities, it is important to reassess the adequacy of the I&C system design and the computer security measures to ensure that the risk remains acceptable. New computer security measures or changes to existing ones may be required to address the change in risk.

Threat modelling has many uses that are not limited to the incorporation of computer security measures to counter the threat. Threat modelling is important in the development of credible scenarios used for scenario analysis (see Section 3.2). This requires the threat model be updated over time to ensure that security measures are adequate. However, changes to the threat model do not identify new vulnerabilities or attack vectors, since these are associated with the facility or system, not with the threat.

3.1.3. Facility and system security modelling

Typically, the overall facility risk assessment is performed regarding nuclear safety and does not consider nuclear security. The use of models and simulators concentrates on the physical properties and processes of NPPs involved in preventing the release of radioactive material and maintaining reactor cooling. In these models, the focus is on the changes in the plant's state, based on anticipated transients such as control rod movements, design base conditions and accidents.

The security risk is addressed through the security risk analysis plan, which considers physical sabotage of the I&C systems and which protects these systems through the application of a site security plan.

The safety and physical security analyses may not adequately account for security against attackers with cyber capabilities, and specific computer security modelling is needed. It will benefit from the inclusion of system models for I&C systems (including their attack surfaces) and simulation specific details. It will represent an additional risk assessment layer that needs to be considered in an integrated and comprehensive manner. It will be performed as

part of an overall I&C computer security risk assessment at the facility level. The need for modelling is also due to the increasing complexity of I&C systems and the dependencies between the functions that they perform.

Comprehensive security modelling depends upon asset identification, role assignment, location of I&C systems (as part of facility management/building technology), access control and other objects. The level of detail depends upon the purpose of a specific security model and the security level assigned to the system(s) being modelled. Typically, a security model will allow for several layers of abstraction such as for risk assessments at the I&C architecture level, for network risk assessments, for physical access control related assessments (e.g. to sites, buildings, rooms and cabinets) or for the assessment of a single I&C system (including its maintenance equipment, etc.).

It is important to note that the actual attacks cannot be modelled because the first order effects of compromise are to alter the I&C system function in a manner that differs from natural system failures. However, the benefit of security modelling is the explicit indication of the security measures that are applied to the I&C system. This allows for systematic and, in some cases, tool supported analyses on the role of the measures in mitigating the impact of the actions of a given adversary. Security modelling will also facilitate the update of previous risk assessments after changes of the I&C infrastructure.

The adversary may also be modelled, with properties such as the initial physical location, the current set of security relevant roles, a set of capabilities including IT and I&C, and the level of security knowledge.

If computer security modelling is in place, it can support further security related activities, including the prioritization of security tests, the generation of documentation needed for certifications or the documentation needed for security training.

3.2. EXAMPLE SCENARIO ANALYSIS

Figure 6 shows a hypothetical operational system consisting of a programmable logic controller (PLC) isolated from any business or general purpose computer network, an engineering workstation (EWS) used to program PLCs, and a group of pumps and valves controlled by the PLC. This configuration, in fact, is similar to the configuration taken advantage of by the Stuxnet campaign in 2010 [15]. In this example, assume that the controlled plant is a single pipe with valves on both ends of the pipe with the pump in the centre. The left side valve controls the rate of liquid input to the pump and the other valve the rate of liquid from the pump.

In this example, the PLC does not have Internet access, and neither does the EWS. The EWS is attached to systems that do have Internet access, however, for system updates and file transfer only. The EWS can access the PLC and alter its control logic. The PLC is wired to the valve actuators and the pump motor. The PLC communicates with the actuators via Modbus over user datagram protocol.

The PLC is programmed with three simple rules:

- (1) The pump can never run with the upstream valve closed.
- (2) The pump can never run with the downstream valve closed.
- (3) The upstream valve must always be opened less than the downstream valve.

A more detailed illustration of this system, showing the network devices and interconnection, is in Fig. 7. For this simplified example, assume that the attack surface was identified as physical or logical access to:

- The EWS;
- The PLC;
- The sensors and actuators;
- The network switch connecting the sensors, actuators and the PLC;
- Assets on the corporate network (which can communicate with the above devices);
- The vendor web site (from which updated software is obtained).

This attack surface is illustrated in Fig. 8. Note that this is only a partial description of the attack surface for the purposes of this example.

The vendor is external to the facility and consequently the attack surface of the vendor is difficult to define with certainty. It is assumed that the attacker would maliciously modify the vendor's software updates in some way (e.g. by attacking the vendor's development environment or the web server used to distribute the updates).

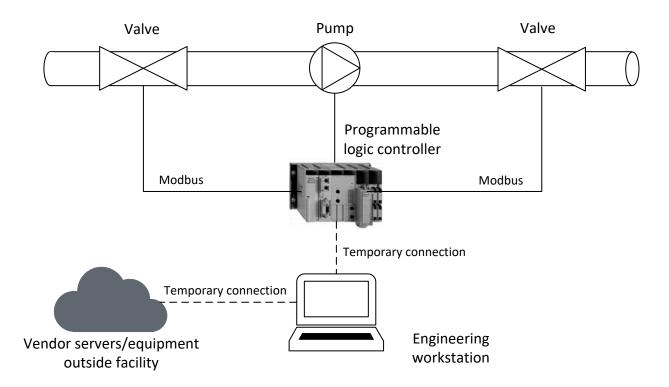
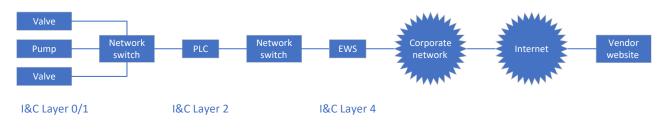
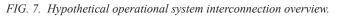


FIG. 6. Hypothetical operational system overview.





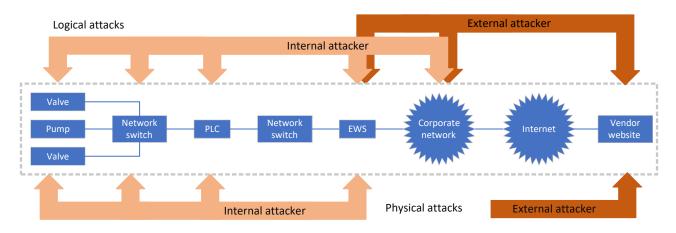


FIG. 8. Hypothetical operational system attack surface.

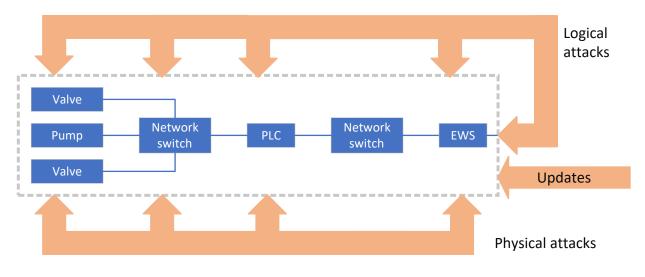


FIG. 9. Hypothetical operational system simplified attack surface.

To simplify the attack surface definition, the vendor attack surface is defined as the software update package itself since this is the means by which the adversary accesses the facility.

The corporate network is a large network, which is outside the responsibility of I&C designers and is typically the responsibility of IT. The I&C network is very dynamic and has many devices that can be potentially used to logically access the I&C system. To simplify the attack surface analysis, the interconnections between the I&C system and the corporate network are considered to be the means by which the adversary accesses the I&C system from the corporate network.

By using these two simplifications, the attack surface can be simplified. This is shown in Fig. 9.

The attack vectors are identified for this attack surface. (In this example, the attack surface has only been partially identified, so this list of attack vectors is incomplete and is intended to be illustrative rather than exhaustive.) The attack vectors accessible to an external adversary are the updates received from the vendor and the

network interface on the I&C systems accessible from the corporate network.

The attack vectors accessible to an internal adversary include all access vectors available to the external adversary. In addition, the insider has physical access vectors consisting of the programming ports and HSIs (e.g. keyboards, mice, pushbuttons, displays), which can be used to modify the configuration and programming of the sensors, actuators, PLC, network switch and EWS. Finally, the attack vectors include any logical communication with the above devices.

In assessing risk, Section 3.1.1 notes that EPRI considers network access vectors to be the most exploitable and that physical access vectors are considered to be the least exploitable if the physical protection is adequate. Finally, supply chain security is highly dependent upon the vendor security programme.

To address the risk from access to physical attack vectors, the physical security of the I&C system and EWS is increased. This includes removing physical interfaces (where possible) or blocking access to them, locating the equipment in a locked cabinet and providing alarms to site security personnel when the equipment is accessed. The stringency of the physical protection is graded consistent with the consequence of compromise.

To address the risk from compromised security patches, the way by which security updates are obtained from the vendor and loaded onto the EWS is changed. The updates are not downloaded directly from the vendor web site to the EWS. Instead, they are downloaded from the vendor web site to a corporate computer and burned onto a DVD. The DVDs are scanned for malware prior to transferring the files from the DVD to the EWS. Appendix I provides a case study on the secure use of removable media.

To address the risk of logical access via network access vectors, the risk may be reduced by controlling or eliminating logical access to the EWS and I&C systems. Again, the stringency of protection is graded based on the consequence of exploitation of the functions performed by the system. Some possible options include the following:

- Establishing a secure network zone for the EWS and I&C system using a combination of boundary protection measures such as firewalls, network IDSs and network intrusion prevention systems (IPSs; see Fig. 10). This

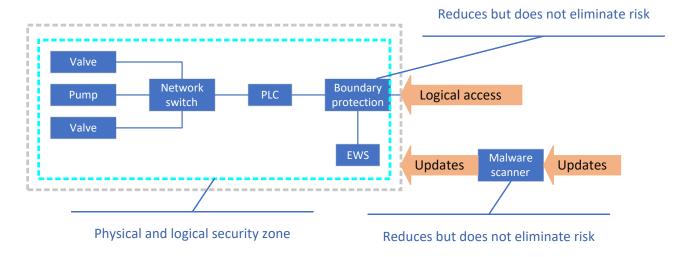


FIG. 10. Establishing a secure network using boundary protection.

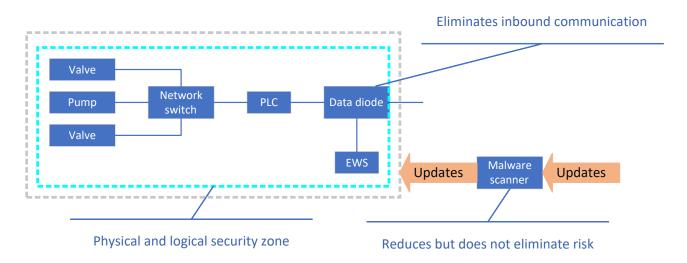


FIG. 11. Establishing a secure network using data diode.

does not eliminate the risk of compromise but reduces it by making it more difficult for the adversary to access the attack vector.

- Establishing a secure network zone for the EWS and I&C system using a data diode to allow only outbound communication from the secure zone (see Fig. 11).
- Establishing a secure network using isolation (see Fig. 12).

Other options could be considered to reduce the risk. For instance, risk reduction could also be applied to system support tools used to maintain and manage the system, such as engineering support software, maintenance computers and system software. This would be considered in a more complete analysis.

This example highlights some of the considerations one would expect to extract from threat modelling and attack surface analysis, leading to the implementation of computer security measures to reduce the overall vulnerability of the system based on an analysis of system risk. This example did not follow any particular attack surface or threat modelling process but did highlight the outcomes and value of threat modelling.

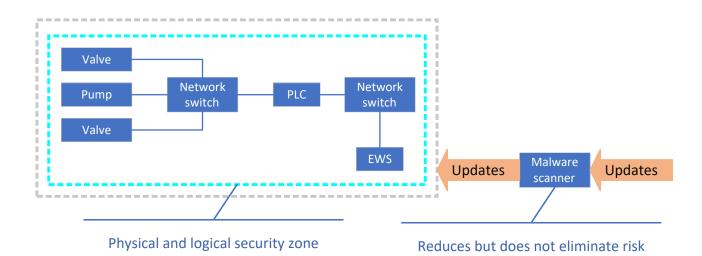


FIG. 12. Establishing a secure network using isolation.

3.3. COMMON MECHANISM ISSUES

One key trait of safety systems in NPPs is protection from common cause failures. Design and engineering of I&C systems are required through various standards to be resilient against failures with particular emphasis on common cause failures [4]. The IAEA Safety Glossary [16] defines common cause failure as a failure "of two or more *structures, systems or components* due to a single specific *event* or cause", and includes failure through human induced events. Systems are designed with a variety of strategies to support this, ranging from forced heterogeneity to complete redundancy to various fault tolerance schemes. One of the key techniques is limiting common mechanism [17].

Limiting common mechanism specifically refers to limiting the number of monolithic components or subsystems upon which a system depends. It is very common to find single, high availability and high cost components in key positions in modern systems. Ranging from proprietary back end database systems to hardware proxies as well as encryption appliances, incorporating components that are single points of dependence by the system is a common problem. This also includes common support resources such as programming workstations, artefact repositories and other common tools.

From a security perspective, compromising single points of dependence can serve to compromise an entire system. For example, if several systems are connected to and communicate through a single network switch, compromising that switch may cause several systems to stop working properly. Limiting common mechanism as much as realistically possible helps support stronger computer security. Limiting common components reduces exposure to system components if a system is compromised.

Appendix II provides a case study of separation of communications within a multichannel safety system. Appendix III provides a case study showing how risk analysis leads to the development of the computer security zones and the requirements for protection of communication.

3.4. COMMON CAUSE ACCESS

Common cause access refers to cyberattacks in which the adversary only needs to compromise a single access point or exploit a single attack vector in order to create a plant safety or security significant event. An example of common cause access would refer to a single compromised access point within an I&C system, in which an adversary would be capable of executing an attack or a series of attacks that would impact the system accessed as well as other systems that are in communication with or otherwise have an interface with the accessed system.

A common cause access attack vector might entail compromising a specific device's software release in a software configuration management system, such as a PLC's operating system or a common EWS. If a software release is installed on the same model of device in multiple plant systems or process channels, a single exploit could cause an event or series of events necessary to cause a safety significant event. Alternately, if a single system,

such as a plant data historian, has bidirectional communication with multiple I&C systems, a single compromise of the plant data historian may become a common cause access attack vector. An adversary with access to the plant data historian may use the communication links to the plant I&C process systems to insert software into plant process systems.

In a potential scenario where there are adversaries whose goal is to create core damage, the adversaries might need to manipulate a system into an undesired state as well as confuse the operators on the state of that system or the overall plant in order to achieve their objective. This might require the adversaries to create multiple attacks: one to manipulate the system and another to manipulate the overall plant displays, including responses from other systems. This potential scenario becomes much easier if the adversaries only need to gain access at a single access point.

In order to understand the impact of common cause access vulnerabilities, it is necessary to understand the role of the I&C systems in ensuring nuclear safety under all plant conditions. Facility event trees and fault trees can be used to identify digital components that play a key role in the nuclear safety of the facility.

Furthermore, Ref. [1] (para. 4.90) states:

"Prior to the completion of the commissioning phase of the I&C system development process, the validation of the I&C system should be performed with the aim of ensuring that the computer security requirements are met while also continuing to comply with the functional, performance and interface requirements. This is intended to provide a high degree of assurance that the system will perform its function as required."

A risk assessment based on adversarial tactics, techniques and capabilities can be used as one component of this computer security requirement validation. For instance, attack scenarios can be developed based on this vector and used to test the adequacy of the security measures.

3.5. SCENARIO ANALYSIS FOR COMMON MECHANISM RISK

The example hypothetical system consists of six sensors (S1A, S1B, S1C, S2A, S2B, S2C) communicating via Modbus transmission control protocol/Internet protocol (TCP/IP). These sensors monitor the same physical process, and the readings from the sensors are used in a Byzantine fault tolerance scheme to determine the conditions in the physical system.

Sensors S1A, S1B and S1C are provided to Accumulator 1, which emits a final calculated value (out1) to a PLC. Sensors S2A, S2B and S2C are provided to Accumulator 2, which sends a final calculated value (out2) to the same PLC. If the readings from Accumulator 1 (out1) or Accumulator 2 (out2) exceed a set point, the PLC will perform a protective action.

The accumulators communicate with the sensors via a single proxy (P1). This arrangement is shown in Fig. 13.

If an adversary can compromise the single proxy, that adversary can compromise the system measurement data from all six sensors, thereby affecting the calculation performed by the PLC and undermining the entire Byzantine fault tolerance scheme.

To rectify this vulnerability, designers determine that they need to remove the common dependency on proxy (P1) and the common network used by the six sensors. Usually designers will choose one of two possible solutions (shown in Fig. 14) to this particular problem:

- (1) Using different instances of the same logical proxy along the different paths;
- (2) Implementing different proxies along each of the possible communication paths.

In selecting the same proxies (type P1) on each communication path, the designer did not change the risk of an attacker exploiting all six sensors since the same attack that successfully exploits sensors S1A, S1B and S1C can also be used against S2A, S2B and S2C. Where two diverse proxies are used (types P1 and P2), the attack is more difficult since different attacks may be required to compromise both proxies.

When these new design options are reviewed, the designers notice that there is still a common attack possible against the accumulators, since they are on the same network and are of the same model. The designers note that compromise of both accumulators will affect the values provided to the PLC (out1, out2), thereby undermining the

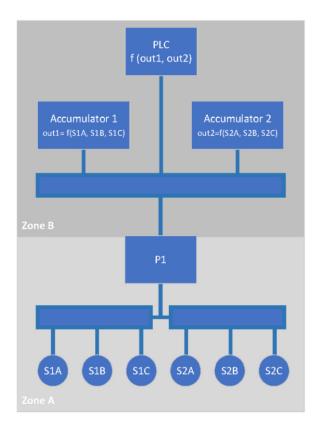


FIG. 13. A Byzantine fault tolerance scheme with a single proxy.

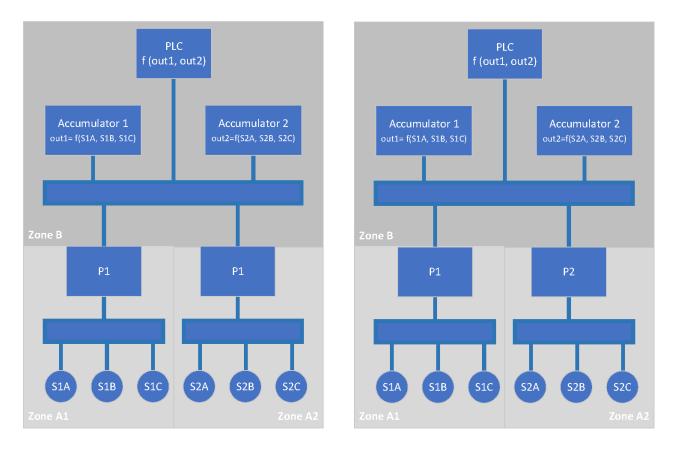


FIG. 14. Example of multiple proxies of same and diverse types.

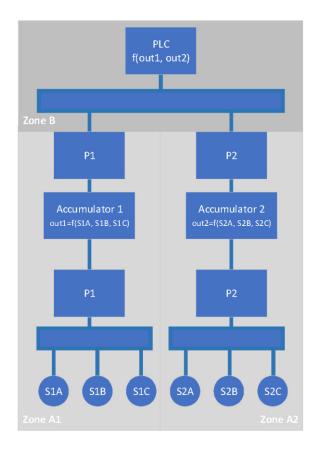


FIG. 15. Introducing proxies between the accumulators and the PLC protects the accumulators from a common attack.

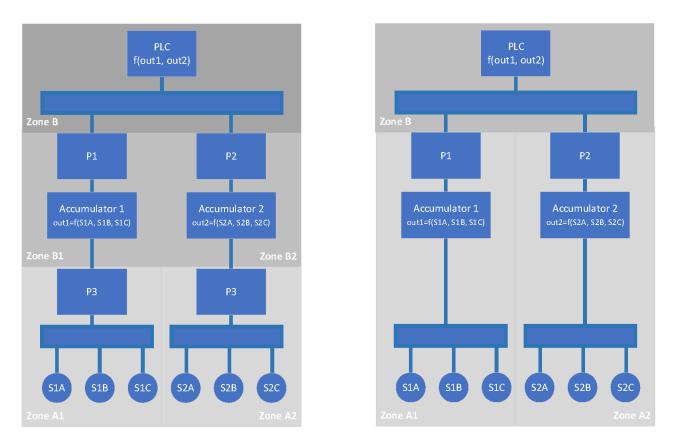


FIG. 16. Example of protecting each accumulator with a single diverse proxy.

function performed by the PLC. The designers modify the design to introduce proxies between the accumulators and the PLC, as shown in Fig. 15.

In reviewing this design, the designers note that the complexity of the design has increased significantly with the introduction of the new proxies. Also, an attacker who could compromise P1 could access Accumulator 1, S1A, S1B and S1C. Similarly, an attacker who could compromise P2 could access Accumulator 2, S2A, S2B and S2C. The designers consider two options shown in Fig. 16:

- (1) Replacing the proxies protecting the sensors with a new proxy (P3);
- (2) Removing the proxies protecting the sensors.

The designers determine that the introduction of proxy P3 decreases the possibility of attacks against the sensors since to compromise them the attacker will have to:

- Compromise P1 and P3 to access S1A, S1B and S1C;
- Compromise P2 and P3 to compromise S2A, S2B and S2C.

The designers also determine that the attacker still only requires attacks against P1 and P2 to compromise Accumulator 1 and Accumulator 2, which is no better than the design shown in Fig. 15. The designers also note that this option also suffers from increased costs associated with management of three different types of proxy. There is also a common failure mode introduced, whereby failure of P3 could result in the loss of all six sensor signals.

The designers settle on a less complex option shown on the right side of Fig. 16, whereby P1 is used to protect Accumulator 1 and sensors S1A, S1B and S1C, and P2 is used to protect Accumulator 2 and sensors S2A, S2B and S2C. In doing so, the level of attacker effort becomes the same as in Fig. 15.

In this example, the single physical common mechanism is separated by creating additional proxies and relocating them. This particular strategy is only effective when the separate instances are not accessible via a common access pathway. If these proxy components are accessible via a single point of compromise, then the multiple proxy design is no more secure than a single common mechanism design as a malicious actor can easily attack multiple accessible instances via the same vulnerability.

Another strategy could be segmentation and separation, where the equipment used to calculate one input to the PLC (i.e. Accumulator 1, S1A, S1B and S1C) is located on physically separated networks from the equipment used to calculate the second input to the PLC (i.e. Accumulator 2, S2A, S2B and S2C).

These approaches help limit the consequence of an attack by limiting the privilege and authority an adversary can acquire via a single exploit as well as the resources available to a malicious user from any single location in a network. For instance, an attacker who had direct access to the network containing the PLC, P1 and P2 could potentially compromise the PLC directly.

Limiting single common mechanisms can be difficult, particularly in heavily virtualized systems. A common issue in virtualized architectures is maintaining physical separation of the systems hosting the virtual machines. Systems may be designed with a high level of service redundancy, but if those redundant services are hosted on the same physical platform, the system becomes vulnerable to a single host failure. The design needs to explicitly address this vulnerability so that virtual images are not migrated to or instantiated on inappropriate hosts.

4. COMPUTER SECURITY IN THE I&C SYSTEM LIFE CYCLE

Development of new and replacement I&C systems and modifications to existing I&C systems follow a life cycle that is managed within the facility's integrated management system. Computer security activities for I&C systems are conducted throughout the lifetime of the facility and throughout the life cycle of each I&C system. Paragraphs 4.1 to 4.11 of Ref. [1] discuss the requirements for using the facility's integrated management system to provide computer security throughout the I&C system life cycle.

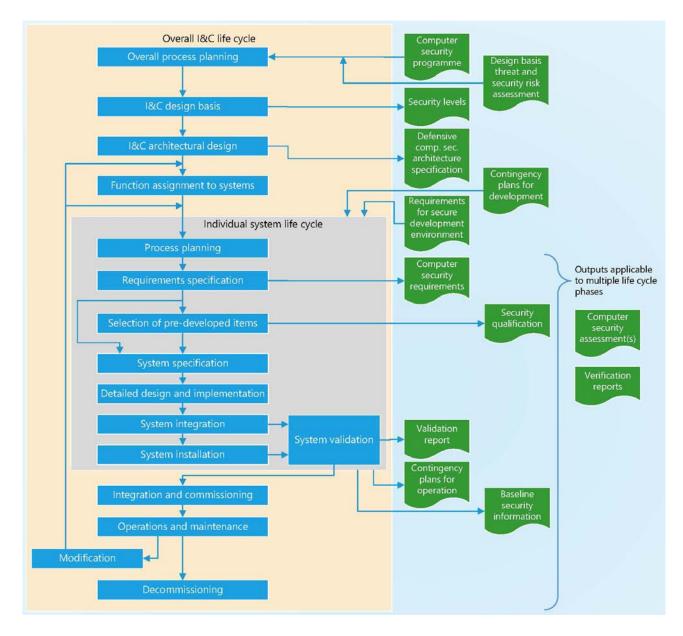


FIG. 17. System life cycle (left) and associated artefacts (right). (Adapted from SSG-39 [5].)

The life cycle used in this publication is based on SSG-39 [5] and is shown in Fig. 17. The life cycle phases are shown on the left, starting at the top of the figure and moving through the individual system life cycles. The artefacts are shown on the right and are linked to the specific life cycle phases in which they are developed or used. Annex II provides a detailed list of artefacts that might be collected during the I&C system life cycle.

Security activities are conducted during each life cycle phase and are not treated as separate activities. For instance, a system has one set of requirements, including the computer security requirements, which are contained in the I&C system requirements specification. The activities conducted during the I&C life cycle ensure the development of an I&C system that complies with these requirements.

Although the life cycle is shown as once through, the process is usually iterative, particularly during the design and development phases, with potential architectures and system designs being developed and refined over successive iterations. Reference [1] lists the issues to be considered throughout the life cycle and during specific life cycle phases. Different groups of people are involved at different phases of the life cycle.

Artefacts collected during the life cycle demonstrate the implementation of appropriate computer security measures aligned with an overall security plan.

The facility's computer security risk management process provides guidance on how to define the requirements for a DCSA, assign facility functions to computer security levels and define the computer security requirements

for each security level. To design a system, the designer needs to identify the functions performed by the I&C system so that the system can be assigned to a computer security level. The computer security level determines the defensive computer security architectural requirements and the requirements for computer security measures.

4.1. GENERAL GUIDANCE FOR COMPUTER SECURITY

Paragraphs 4.12 to 4.32 of Ref. [1] provide general guidance for the computer security policy and programmes that ensure the security of I&C systems throughout their life cycles.

4.2. SECURE DEVELOPMENT ENVIRONMENT

Paragraphs 4.33 to 4.40 of Ref. [1] define the requirements for the use of secure development environments within the I&C system life cycle. Secure development environments may be used for development and testing of I&C systems. The secure development environment includes protection of both physical and logical access to I&C systems and systems used to support development to protect the integrity and confidentiality of their data.

Activities performed in the development environment will be substantially different from the operating environment; I&C designers need to take this into consideration in order to define the security controls that ensure the required level of security. For example, whitelisting rules will need to be relaxed in the development environment to allow for loading of new code, whereas in the operation phase, they will be restrictive to prevent the execution of new code. Similarly, penetration testing tools may be used in the development environment, but not permitted in the operational environment.

The secure development environment is assessed or inspected to ensure that the computer security measures are adequate. For example, an inspection may find that systems of different security levels are co-located, which may not be acceptable. For commercial off the shelf products, assessment or inspection of the secure development environment may not be possible. Third party tools used for I&C system development and testing are tested, validated and protected commensurate with the assigned security level of the development and testing environment.

4.3. CONTINGENCY PLANS

Paragraphs 4.41 to 4.45 of Ref. [1] provide requirements for contingency planning during the I&C system life cycle.

Contingency plans include restoration plans that are used to restore I&C systems to their design basis after a cyberattack. These plans typically require the use of restoration media and restoration procedures. Execution of these procedures using the restoration media ensures that they are complete and accurate. Such testing could be executed during the factory acceptance test (FAT).

At any point in the I&C system life cycle, vulnerabilities may be identified within I&C systems. The risk arising from these vulnerabilities is assessed and may be avoided by installing a vendor patch or reduced by applying mitigating measures that reduce the risk to an acceptable level. Patching or applying mitigating measures involves design changes to the system. Effective contingency plans for addressing vulnerabilities require the establishment of processes that enable the operator and the vendor, contractor or supplier to report vulnerabilities to one another and to coordinate response and mitigation efforts. Contingency plans may also be developed for restoring the secure development environment in case it has become compromised.

4.4. I&C VENDORS, CONTRACTORS AND SUPPLIERS

Paragraphs 4.46 to 4.53 of Ref. [1] provide recommendations applicable to I&C vendors. The designer is typically involved in writing procurement specification and needs to ensure that the specification includes the appropriate computer security requirements applicable to the vendor. The designer also needs to be satisfied

that the computer security requirements have been met. This can be done by ensuring that the computer security requirements are verified and validated and that any design reviews consider computer security.

When identifying the required design outputs in the procurement specification, the designer considers that these outputs will be used to support other activities during the operation and maintenance phases and during future modifications. Examples of such activities include conducting computer security risk assessments, configuring monitoring tools and determining if a system is exhibiting unexpected behaviour (e.g. during incident response). The designer identifies design outputs that can support these activities. Examples include logical data flow diagrams and baseline information such as lists of running processes and network ports and protocols.

4.5. COMPUTER SECURITY TRAINING

Paragraphs 4.54 to 4.59 of Ref. [1] provide requirements for computer security training for personnel performing work involving I&C systems.

4.6. COMMON ELEMENTS OF ALL LIFE CYCLE PHASES

Paragraph 4.60 of Ref. [1] notes that specific guidance on computer security is warranted in some I&C life cycle phases.

4.6.1. Management systems

Paragraphs 4.61 to 4.70 of Ref. [1] provide requirements for the management system to ensure that computer security of I&C systems is addressed within the facility management system.

4.6.2. Computer security reviews and audits

Paragraphs 4.71 to 4.77 of Ref. [1] provide requirements for the conduct of computer security reviews and audits within the I&C system life cycle.

4.6.3. Configuration management for computer security

Paragraphs 4.78 to 4.87 of Ref. [1] provide requirements for configuration management for computer security within the I&C system life cycle.

Configuration management for security is handled in the same way as safety and general system configuration management. Technical control measures to ensure integrity of software and configuration files could include cryptographic hash verification. The information produced in the design process is classified and protected in accordance with the facility information protection programme. Confidentiality controls include labels, marking, seals and encryption.

4.6.4. Verification and validation, testing

Paragraphs 4.88 to 4.94 of Ref. [1] provide requirements for verification and validation.

During design, it is necessary to verify and validate computer security measures for compliance with the CSP, the computer security requirements for the I&C system, and DCSA requirements. Systems need to be able to support detection and recovery from attacks as well as prevention.

During verification and validation, it is important that designers account for the time required to test system security, the specialized security tools and software needed, the training required in order to perform these tests and any additional cost incurred by acquiring these tools and software. Tools need to be approved by computer security specialists. These kinds of tests may very well be destructive, and so they need to be performed before FAT. Appropriate mitigations need to be put in place to account for any potential damage incurred. Finally, computer

security measures are in place with safety measures and other controls during validation and verification to ensure that the different sets of functions do not interfere with one another.

During these tests, the tester tries different methods of attack, regardless of the expected outcomes. Penetration testing is similar to vulnerability assessment, but penetration testing has an emphasis on gaining as much access to a given system as possible, while vulnerability assessment (with the use of scanners) only identifies the possible vulnerabilities. 'Red team' assessments are conducted from the perspective of an adversary and use adversarial techniques to identify vulnerabilities and weaknesses in computer security. Red teaming, penetration testing and vulnerability assessment can be guided by the overall threat model but do not necessarily need to be.

The aim of computer security testing is to verify the fulfilment of computer security requirements while confirming that real time function and performance of the I&C system under test are not impacted. The requirements are defined in the computer security plan and/or in other security policy documents of the organization.

Computer security testing is performed at different phases of the I&C systems' life cycle. The FAT is the first opportunity to check whether the system fulfils all computer security requirements. The goal of these tests is to investigate that all computer security measures that are developed in advance and detailed in the CSP are in place. Tests in this phase give an opportunity to collect missing computer security related data and/or check the completeness of already collected data. At this stage, the system can still be rebuilt to prevent operational consequences. While it is important to validate system security at this point, it is equally important to not neglect security during earlier phases of the development cycle.

During site acceptance testing, the goal of testing differs. Computer security testing is performed to check that no computer security related changes have happened in I&C systems since the FAT. Testing is intended to ensure that no new factors that lower the expected level of security are introduced into the system. Since it is possible that any of the components may have changed, testing makes it possible to check that the modified system still maps to the requirements. Further data can be collected in this phase.

After the system has been upgraded or modernized, new security testing is performed. These tests are intended to check that the new configuration of the I&C system or a given part of the I&C system still fulfils the requirements that were set for the previous state of the system or the requirements that were set for the refurbished system. The range of tests varies and depends on the extent of the changes. During test development, it has to be kept in mind that if the system was partially modified, the impact of potential side effects needs to be considered. The tests are divided into the following two parts:

- (a) Tests done on the system before integration;
- (b) Tests done on the system after integration.

The former tests ensure that all security requirements are addressed and that the new assets are not going to lower the desired security level after integration. The latter tests ensure that no other negative side effects were introduced into the system after integration.

Audits, covering and reviewing available tests, are performed on a regular basis to check that no security related change has been made on the system during operation. With the aid of testing, the deviations from a baseline state or configuration of a given system can be detected. These deviations may have negative impacts on computer security; testing helps detect and eliminate the computer security risks that may emerge from them.

The information on the baseline state or configuration is stored in a database, which contains all software and hardware assets and all computer security related information. These data are needed as inputs to test results. The definition of the scope of testing and the elaboration of test methods are based on this collection of information. Parts of the asset management and configuration management databases may be filled during design and during the FAT phase.

Tests are also performed when security events occur. The main indicators of these tests include a computer security incident, a new vulnerability announcement that affects the applied I&C system, any changes in security requirements or any changes in the configuration of the I&C system. In any of these cases, an action plan is developed after testing. The action plan describes the necessary actions when a discrepancy is found.

After a computer security incident, the first step is to restore the integrity of the system, if possible. The traces of the incident are preserved for forensic analysis; all logs, files and system states are collected. The aim of the test (maybe as part of forensic activities) is to find the factors that make a successful attack possible. After the factors are revealed, the necessary actions that eliminate the possibilities for further successful attacks can be identified.

When a new vulnerability is publicly announced, the first step is to determine if there are any assets that are affected by the given vulnerability. After all such assets are found, the risk arising from the vulnerability is determined. If the risk is unacceptable, an action plan is developed, which defines the necessary actions to reduce the risk to an acceptable level (e.g. install the patch or implement other measures to reduce vulnerability). The action plan is executed and its effectiveness is confirmed, typically by testing, which shows that the vulnerability no longer exists or is no longer exploitable.

When a security requirement has changed or the configuration of an I&C system has been modified, the test demonstrates that the new requirements are met and that the new configuration fulfils all computer security requirements without introducing unintended changes.

The configuration may change during maintenance with a replacement of an asset or when a functionally identical, but technically different asset needs to be installed. In the latter case, preinstall testing is performed on the asset to ensure that it can be safely installed into the infrastructure and that all security requirements are still met.

4.6.5. Computer security assessments

Paragraphs 4.95 to 4.100 of Ref. [1] provide requirements for the performance of computer security assessments. The computer security assessments will generally require knowledge about the plant process, interconnection to other systems and computer security measures. This may require the use of multidisciplinary teams in many cases, though smaller projects may be able to proceed with single individuals. The outputs of the assessments are requirements and are tracked in the same way as other system requirements. These new requirements can lead to new security measures to mitigate identified risks.

4.6.6. Documentation

Paragraphs 4.101 to 4.106 of Ref. [1] provide requirements for documentation. The issue of confidentiality is handled in Section 4.6.9 of this publication.

4.6.7. Design basis

Paragraphs 4.107 to 4.114 of Ref. [1] provide requirements for design basis. They are generally achieved by ensuring that the design basis threat or risk assessment informs the DCSA and resultant requirements for the NPP. See Appendix III of this publication for an illustration of how these requirements may flow down to an individual I&C system.

4.6.8. Access control

Paragraphs 4.115 to 4.120 of Ref. [1] provide requirements to establish proper access control. In the development phase, the secure development environment addresses access control. In the operational phase, the CSP sets requirements for access control. For transportation and storage, measures such as chain of custody processes, secure storage and tamper evident seals provide protection.

4.6.9. Protection of the confidentiality of information

Paragraphs 4.121 to 4.125 of Ref. [1] provide requirements to protect the confidentiality of information. Designers need to follow the facility's information protection procedures and policies. The information classification of design artefacts has to be determined and the requisite security measures established before initiating system design.

4.6.10. Security monitoring

Paragraphs 4.126 to 4.130 of Ref. [1] provide requirements for security monitoring. It is important to monitor the effectiveness of protective security measures. Designers need to provide the ability to monitor system functions and computer security measures. Collected network traffic and system logs need to be accessible by analysis

systems such as security information and event management systems, generally housed in a security operations centre. As much as possible, these capabilities need to be able to provide continuous monitoring and alerting over the control system state. Designers need to engage computer security staff early in the design process in order to understand specific facility and DCSA requirements with respect to system monitoring.

Where it is not possible to implement continuous monitoring, such as in the cases of small isolated networks, stand-alone computers, smart devices or legacy systems, other means to provide assurance of the protective security measures may include the following:

- Checking/verifying software and configuration settings routinely;
- Manually inspecting logs, locally or after export by removable media routinely;
- Running bootable anti-malware tools during routine maintenance (if other boot media are allowed on the device);
- Auditing key issue and return;
- Inspecting tamper evident seals.

4.6.11. Considerations for the overall DCSA

Paragraphs 4.131 to 4.140 of Ref. [1] provide requirements for overall DCSA. Additional information is provided in Section 2 of this publication.

4.6.12. DiD against compromise

Paragraphs 4.141 to 4.151 of Ref. [1] provide requirements for a DiD approach against compromise. Additional details are provided in Section 2 of this publication.

4.7. SPECIFIC LIFE CYCLE ACTIVITIES

4.7.1. Computer security requirements specification

Paragraphs 4.152 to 4.155 of Ref. [1] contain guidance on computer security requirements specifications.

4.7.2. Selection of predeveloped items

Paragraphs 4.156 to 4.164 of Ref. [1] address predeveloped item management. In cases where integrity cannot be established, using compensatory measures such as running the software in secure virtual environments (sandboxes), dynamic analysis, static analysis or continuous monitoring of impacted systems can help minimize overall risk.

4.7.3. I&C system design and implementation

Paragraphs 4.165 to 4.174 of Ref. [1] and this publication address system design and implementation computer security concerns.

Ideally, the designer would implement all of the security measures recommended for the high consequence system. However, for I&C systems, some security measures cannot be supported by the system or may not be acceptable to implement. For instance, if a specific computer security measure is proven or known to negatively impact a required safety function of the I&C system or if it prevents operators from responding to an emergency in a timely manner, then it cannot be implemented. In these cases, alternative measures need to be found to mitigate the attack vectors or vulnerabilities that were left unaddressed by the security measures that could not be implemented. For example, if the system cannot support logging of user access, physical access may be restricted, and an administrative process used as an alternative method to log user access. Ultimately, the best selection of controls is determined through consultation with the system stakeholders, I&C safety engineers, computer security specialists, maintenance and operations staff.

It is common practice to use an iterative design process to evaluate the security measures needed for the system. For example, a computer security assessment could be performed at the 10%, 50% and 90% completion milestones in the design process. The idea of performing a computer security assessment on a system that does not exist yet may seem strange, but the designer can walk through and assess the vulnerabilities and attack vectors for the conceptual system based on the required physical and logical characteristics, functions, communications, location and users. The designer can then assess the security measures needed to mitigate the identified vulnerabilities and attack vectors during a 10% assessment. The designer would revisit and adjust as necessary the proposed security controls during the 50% assessment once the actual system devices have been selected, the capabilities and limitations are understood and the security measures have been incorporated into the design. Finally, the designer would revisit the security assessment at the 90% milestone of the design process once the design is nearly complete and no longer changing to make sure that the selected security measures are properly incorporated into the final design.

4.7.4. I&C system integration

Paragraphs 4.175 to 4.178 of Ref. [1] provide requirements for computer security during system integration. Integration testing is addressed in Section 4.6.4 of this publication.

4.7.5. System validation

Paragraphs 4.179 to 4.185 of Ref. [1] provide guidance on the computer security measures in place or in a test environment that are confirmed to be the same as the installed configuration for the I&C system.

4.7.6. Installation, overall I&C system integration and commissioning

Paragraphs 4.186 to 4.190 of Ref. [1] provide guidance on installation, overall I&C system integration and commissioning. The facility security procedures need to be followed during installation, integration and commissioning for secure environments.

4.7.7. Operations and maintenance

Paragraphs 4.191 to 4.205 of Ref. [1] provide guidance on all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level. Operations and maintenance activities continue throughout the I&C life cycle and have already been discussed above in sections dealing with process planning and activities common to all life cycle phases. The operating organization assumes full responsibility for computer security for the ongoing performance of operation and maintenance activities when entering the operations and maintenance phase for a system. As a result, computer security measures and systems need to be designed to accommodate risk assessment, monitoring and continuous improvement. Adversaries and vulnerabilities change over time, and systems need to be able to change to meet them.

One important example is forensic readiness. To monitor and detect computer security related manipulations during plant operation, appropriate forensic security controls such as auditing, traffic monitoring and security event management need to be in place. If set points of an I&C device can be changed without any logging (either automatic or via administrative measures), additional steps will be needed to subsequently detect an unauthorized change of a set point. This will also have an impact on the time that elapses between the malicious change of a set point and the subsequent detection of the manipulation. During the I&C platform design phase, appropriate release and permission granting functionality (preventive computer security measures) are supported. Otherwise, additional administrative control measures will be needed to compensate for missing release and permission granting functionality at the I&C platform level. Forensic analysis is dependent on baseline technical behaviours defined during initial design phases and early system monitoring, as described in Section 4.6 of this publication.

Typically, the entry point for malware into these systems is via removable media or portable programming and maintenance laptops. These systems need to be managed as a key part of control systems they attach to and need to have the same level of computer security measures applied. See Appendix I of this publication for more information.

4.7.8. Modification of I&C systems

Paragraphs 4.206 to 4.222 of Ref. [1] provide requirements for modification of legacy I&C systems.

The modified system or component is assessed to determine if new or changed functionality, capabilities or connectivity can enhance security or introduce new vulnerabilities that need to be addressed or that could compromise existing security measures for connected or associated systems. If changes are needed to computer security measures, they are included as part of the modification process.

During the modification process, computer security measures remain in place for the system being modified and care is taken to ensure that the new system is secure during the development and installation process by applying computer security measures consistent with the computer security level assigned and consistent with those described under secure development environments.

Security measures are also applicable to the removable media and connected tools or computers used for configuration and programming from development through to commissioning. Temporary data residing on removable media and tools are treated at the same security level as the component on which they are used. When no longer needed, these data are deleted consistent with the CSP to prevent disclosure to unauthorized persons.

Any replacement with a non-identical component is a modification. New components may have new features (e.g. syslog capability, digital firmware signing, encryption), interfaces and vulnerabilities that may impact or invalidate the original system risk assessment and thus require re-evaluation. Although these new features may increase the security of the new component, they might also degrade the overall security posture of the system.

4.7.9. Decommissioning

Paragraphs 4.223 to 4.226 of Ref. [1] provide computer security requirements specific to the decommissioning phase of the I&C system life cycle.

I&C systems and components will need to be replaced during the life cycle of the NPP, which will involve decommissioning the old system or component and replacing it with new equipment. Decommissioning and retirement of I&C systems and components can pose a security risk and need to be addressed properly. Data from retired systems and components, including development systems, workstations, support tools, and data historian, as well as design, maintenance and operational documentation are useful to an adversary when crafting an attack. This includes both electronic and printed information. Decommissioned systems and components are sanitized before disposal consistent with the facility information protection programme.

5. SUMMARY AND CONCLUSIONS

The overarching objective of this publication is to highlight an approach to producing more secure I&C system designs for NPPs. In doing so, contributing topics, including system life cycles, trust models and system partitioning became specific focus areas. By focusing on these areas, the goal of this report is to highlight these contributing topics, identify specific design requirements, describe life cycle considerations and their impacts on computer security, and then to use these concepts in a tractable example to show designers how they can use these ideas to design more secure control systems.

This publication first covers general computer security topics and describes how they apply to digital I&C systems. The goal of this section is to expose engineers and designers to specific computer security concepts that directly influence the security of I&C designs. Some of the specific topics addressed include network security layering, threat modelling, communications security and trust modelling. This report also discusses common cause access and mechanism issues and key computer security concepts such as the confidentiality, integrity and availability triad, DiD and the graded approach.

Next, the publication delves into specific computer security design requirements for NPP I&C systems, based on current practices and standards. Specific topics covered include the concepts of security levels and how they contribute to the design of security zones in an I&C architecture. Those zones are defined and then associated with common I&C layers where appropriate. This publication also highlights how these concepts can be brought together into a unified DCSA. This publication also touches on the use of modelling, how to appropriately build and implement a security testing capability and how to handle sensitive data when plants are decommissioned or retired.

These concepts, ideas and models come together with life cycle considerations in NPPs. Of particular concern is the application of these concepts to legacy systems as well as new designs. After all, in new designs, engineers have much more flexibility with respect to security controls and their integration into larger scale control systems than they tend to have in legacy systems.

This publication includes three case studies showing how these concepts have been applied in operational NPPs today as well as two annexes that describe various approaches to protecting computer communications and baseline data of possible interest to control system designers.

Overall, the report addresses computer security in I&C systems via introducing the relevant concepts and going into details where appropriate. Specific attention is paid to relevant security standards in place for NPPs, and how these plants differ from typical computer systems with respect to computer security. After covering these basic ideas, the report applies them in specific sample cases, showing how designers can incorporate these ideas into more secure and securable designs.

Appendix I

SOFTWARE MODIFICATION VIA REMOVABLE MEDIA

I.1. SUMMARY

Removable media controls allow for the assignment of devices to levels and for the authorization of devices to be used in specific security levels and zones. Devices will be sanitized and scanned before and after use to check for malware and unauthorized digital content. Removable media assigned to a specific level are not allowed to be used on other levels or zones other than those authorized. The removable media computer security measures also include storage of the devices between use at the security level commensurate with the highest level at which they may be used. The removable media programme includes periodic auditing of the programme to ensure that the process is being followed. There are also provisions for use of removable media that originate outside the set of controlled devices, such as those that are required by site software licences or original equipment manufacturer requirements. These devices can be temporarily authorized and assigned to the system and controlled in accordance with the process. After use, these devices will be properly sanitized and unauthorized from the system to be returned to the vendor or destroyed as appropriate.

I.2. PROBLEM

A software modification required on a level 2 sensitive digital asset (SDA) requires the use of a removable media device with software received at the vendor at level 5. Network access to transfer the files is prohibited from level 5 to level 2 as per security architecture requirements. Software needs to be moved from a less secure to a more secure system.

I.3. LIFE CYCLE PHASES

The process for removable media use described below applies to the operations, maintenance and modification life cycle phases as described in section 2 of SSG-39 [5]. Table 2 here provides an overview of the tasks, roles and responsibilities involved in this process.

I.4. CASE STUDY

Facility processes and procedures are in place for secure handling of removable media and installation of software modifications. Facility procedure requires removable media to be designated to the system or level and only used within that system or level. Removable media for SDAs are tagged with a permanent tag that is colour coded by level to assist spot checks by operations or security staff. Before storage, level 2 removable media have to be sanitized as per facility procedures and stored in tamper evident packaging and locked into a secure storage area. The level 2 removable media are issued to the technician with a paper form that is signed by both the issuer and the user to be used for tracking and auditing purposes. The form will document the system and security level and zone, if applicable, that the level 2 removable media are authorized for use in, along with the work order used to complete the task. This form has to accompany the removable media and has to be available for spot checks by security forces or operations. The media have to be in the direct control of the person listed on the issuing form; there are provisions for transferring the control to another authorized individual by signing the transfer portion of the issuing form. Transfer is accomplished by two persons' signatures.

Before the software is loaded onto the removable media device, SHA256 hash verification is required to validate the integrity of the file provided by the vendor. Once the hash is verified, the file can be loaded onto the level 2 removable media. The files will be transferred from the level 5 removable media to the level 2 removable

Item	Task	Е	Т	LOS	CS	RMI	Comments
1	Software modification required on level 2 SDA.	Х					Software is delivered from the vendor via electronic transfer from level 5. The electronic delivery includes instructions, and SHA256 hash values are provided out of band by the vendor.
2	Verify software from the vendor.	(X)	Х				Use software to determine the SHA256 hash of the software and compare with vendor provided SHA256 hash and copy to level 5 removable media.
3	Complete security test plan on software.				Х		Static and dynamic analysis is completed on the software to identify any vulnerabilities or malware. Software composition analysis, sandbox analysis and fuzz testing are used to test the software.
4	Complete security risk assessment and approve software.				Х		Complete a security risk assessment from the computer security test plan. All risks identified are required to be accepted or mitigated by an appropriate level of management before security approval.
5	Complete regression testing in engineering development environment and approve software.	Х					Regression and functional testing of the software modification is completed in a development environment as per facility procedures. Software approval is granted as per facility procedures.
6	Complete request form for level 2 removable media.	(X)	Х				Complete a removable media release form identifying the work authorization number, security level, security zone and system.
7	Issue level 2 removable media and forms.	(X)	Х			Х	Collect level 2 media from secure storage and verify the tamper proof packing has not been tampered with. Issue colour coded removable media from secure storage for level 2 to the authorized individual.
8	Transfer verified software files with level specific appliance.	(X)	Х				Use the level 2 file transfer appliance to move files from the level 5 removable media to the level 2 removable media. The transfer appliance performs additional security checks before transfer.
9	Scan removable media at level 2 virus kiosk.	(X)	Х				Level 2 removable media is taken to a level 2 kiosk for multiengine malware scanning.
10	Retrieve cabinet and port blocker keys from LOS.	(X)	Х	Х			Bring forms and work authorization to LOS to allow for release of the keys from the lockboxes.
11	Unlock cabinets and remove port blockers.	(X)	Х				Cabinets unlocked and port blockers removed. Extra care required on port blocker storage so as to not introduce a foreign material if dropped.
12	Install software modification.	(X)	Х				Software modification is installed on the system following commissioning steps.

TABLE 2. REMOVABLE MEDIA — TASKS, ROLES AND RESPONSIBILITIES

Item	Task	Е	Т	LOS	CS	RMI	Comments
13	Functional testing after software installation.	(X)	Х				Functionality of the system is confirmed as per facility procedures after the software modification has been applied.
14	Restore port blockers and lock cabinet.	(X)	Х				Port blockers are reinstalled into the system and the cabinet is locked.
15	Return keys to LOS.	(X)	Х	Х			The port blocker and cabinet keys are returned to LOS and logs are signed off with the return.
16	Scan removable media at level 2 kiosk.	(X)	Х			(X)	Level 2 removable media are scanned at the level 2 kiosk to test that no malware infected the removable media while inserted into the level 2 system.
17	Return removable media to RMI.	(X)	Х			Х	Level 2 removable media are returned to the RMI. Logs and forms are signed off and stored for audit and incident response.
18	Sanitize removable media and return to secure storage.					Х	RMI scans and sanitizes level 2 removable media to facility procedure requirements. Level 2 media is put in tamper evident packaging and returned to secure storage.

TABLE 2. REMOVABLE MEDIA — TASKS, ROLES AND RESPONSIBILITIES (cont.)

Note: E — engineer; T — technician; LOS — licensed operations staff; CS — computer security specialist; RMI — removable media issuer; X — task, role or responsibility of the given person; (X) — potentially, dependent on the facility process and procedures.

media via the secure transfer appliance. After the files are loaded onto the removable media, a malware scan is required at the level 2 antivirus kiosk before connecting it to the SDA. The software will undergo security and regression testing before being loaded onto the SDA.

Security testing of the software is conducted to determine if vulnerabilities exist in the software and that the software is malware free. Composition analysis of the software is completed, which catalogues all the libraries and software licences used. Any vulnerabilities in the national vulnerability database are identified and listed along with remediation details. Information leakage is also identified through network calls and noting if any private keys exist in the software.

Sandbox analysis is conducted on the software to test for malicious indicators. If any outbound network connections are detected, they are reviewed against operating documentation. Any deviations from the documentation require additional testing to determine if they are part of normal operations or if they are potentially malicious. All system calls that are detected in the sandbox are reviewed to identify any malicious changes to files or system registries. During the sandbox analysis, YARA³ rules that are maintained by the facility are also used to look for indicators of compromise from open and closed source intelligence.

If possible, fuzzing is completed against the development system to identify any adverse conditions while the software is running. If an adverse condition is detected, the system is reset and the test cases that caused the condition are run again. If the condition persists, a report is generated and provided to the vendor for remediation. A risk assessment is completed to determine whether the system can be put into production with the condition and if there are any computer security measures that can be applied to mitigate the vulnerability. Once the security test plan is completed and risks are mitigated or accepted, security approval is granted for the software installation.

³ YARA is an open source tool supported by VirusTotal for string and binary matching via predefined rule files to identify malware.

The software installation is accomplished within the plant work control processes and will require physical access to the SDA. The SDA has physical port blockers installed and is located in a locked cabinet. All individuals who require access to SDAs are required to have a qualification that is granted after completing computer based training. Work authorization and qualifications are checked before unlocking the cabinet and releasing port blocker keys by LOS. Release of the cabinet and port blocker keys are logged with the work authorization number and employee number by the LOS.

Work control process after installation requires applicable regression testing on the system to confirm that the system works as expected after the update. Prior regression testing is completed in a development system to ensure that the patch will have no adverse impact on system function and exhibits no unusual behaviours; this will be confirmed as part of the post-installation test. After the software is loaded onto the SDA and the SDA is functionally tested, port blockers are reinserted into the SDA, the system is returned to operation and the cabinet is locked. The cabinet and port blocker keys are returned to the LOS and the audit log is signed off with the time the cabinet and port blocker keys were returned. If the keys have not been returned within the time window of the work authorization, the employee's supervisor is notified.

The level 2 removable media have to be returned at the end of the shift if not transferred to another individual. The level 2 removable media will be turned in with the form and signed back in to the issuer where they will be scanned at the antivirus kiosk. If malware is detected on the removable media device, the computer security incident response process is initiated and the forms are used to identify where the removable device was used. If system backups are needed, these will be copied onto another removable media device via the secure file transfer appliance and transferred to secure backup storage. The level 2 removable media will be sanitized as per facility procedures before returning the device for reuse or destruction.

Appendix II

SEPARATION OF SERVICE SYSTEMS AND EXTERNAL COMMUNICATION FROM CLOSED LOOP OPERATION

II.1. SUMMARY

This case study addresses the need to pass selected real time control data from a low level security zone to higher security zones. This example describes the kind of hardware used, the controls needed, and data security mechanisms put in place to ensure that sensitive data are not transmitted out from dedicated high security zones.

II.2. PROBLEM

The closed loop control functions of a safety I&C system need to send data to other systems that are less trusted, including maintenance and engineering systems.

II.3. LIFE CYCLE PHASES

This study applies mostly to the following life cycle phases from SSG-39 [5]:

- I&C design basis (section 3).
- I&C architectural design (section 4).
- Detailed design and implementation from individual system life cycle implementation:
 - Software design (section 9);
 - Hardware design (sections 2, 6 and 7).

II.4. CASE STUDY

TELEPERM XS (TXS) is an I&C platform used to implement safety functions. It has a modular structure and includes data acquisition, calculation, voting, control output and information output functions.

These functions are handled within the automation computer, which includes input/output modules, processing modules, voting modules and communication modules. This automation computer can be built in a redundant configuration or duplicated with more redundancy channels and two out of three or two out of four voting logic.

The service unit is the engineering station for the whole system.

All communication outside the automation computers is handled by the monitoring and service interface (MSI). This includes communication to the service unit and the gateway, which correspondingly have no direct access to automation computer modules. In this way, the MSI can be seen as an additional boundary device to give a better DiD. Today, the MSI barrier is a mandatory interface to the automation computers.

The TXS gateway is mandatory when exchanging data with external I&C systems and acts as a boundary device.

Figure 18 shows a simplified structure in a redundant configuration that uses only one train.

The exact number of MSI barriers and TXS gateways will be determined during the detailed design and implementation phase by also considering the desired redundancy degree, overall system availability, required functional independence and other criteria. That said, typically each redundancy train will have its own MSI barrier and TXS gateway.

Table 3 shows all communications required by TXS. With this communication structure, the MSI with the gateway and the service unit are positioned in a dedicated zone model. In this model it is possible to bundle and check the communication outside the closed loop control. All communication within or in between automation

computers has no boundary device because of fast data transmission requirements that in effect require all automation computers to be in the same zone.

The engineering data from and to the service unit are not needed in real time and can therefore support a boundary based security mechanism. In this system, this is the role of the MSI, which extracts needed data from the protocol used by the service unit to pass specific data to less secure systems. The MSI is located in the same security zone as the automation computer since a boundary control mechanism has always to be protected as a member of the highest supported security zone. The service unit will also mostly be in the same zone as the automation computer, since the service unit contains the software and engineering data for the automation computer, and most regulations require the same security level for the service unit as for the automation computer. As a result, keeping the service unit and the automation computer in the same zone eases the cost and difficulty of applying computer security measures. Command and signalling messages from the service unit to the automation computer need special measures according to the system computer security risk analyses. A key switch, as one example, can protect the transfer of new set points from service unit via MSI to the automation computer.

The data for visualization and archiving are going to a less trusted system, so a boundary protection mechanism between zones is needed. In this case there are two different boundary protection devices, the MSI and the gateway, which perform data interception and protocol translation services.

Figure 19 shows a possible security zone arrangement before a dedicated facility and system computer security risk analysis.

The communication mechanisms within TXS play an essential role in the I&C design to meet the security requirements. There are separate, dedicated and isolated networks within the inner security zone as well as limited and monitored separate networks to outer security zone(s). These networks use TXS ethernet protocols. The networks that connect the input/output modules, processing modules, communication modules and voting modules within the automation computers and between the different channels of the automation computer are implemented with the TXS Profibus network protocol. The TXS ethernet network protocol is also used for communication between MSI, service unit and gateway.

For both standard TXS network protocols, the following applies:

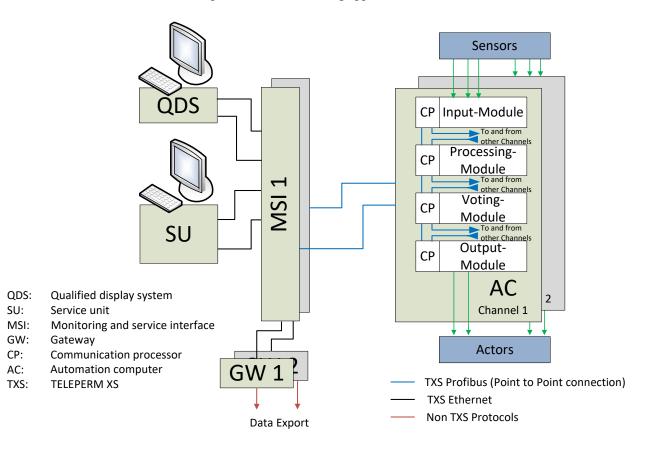
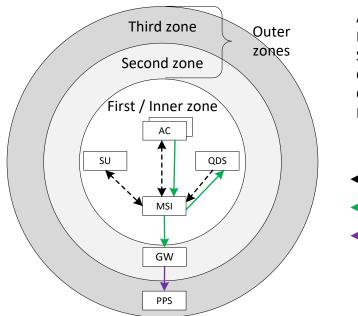


FIG. 18. Simplified structure of single train TXS in a redundant configuration.

Path	Why communication	Boundary device	Boundary security measures	Protocols used
Within automation computer	Connecting subsystems for closed loop control	No boundary device needed	N/A	TXS Profibus as point to point connection
Between automation computers	Connecting subsystems from different channels for 2 out of 3 or similar	No boundary device needed	N/A	TXS Profibus as point to point connection
From service unit to automation computer via MSI	Sending configuration data to the automation computer, read parameters from the automation computer (both for engineering purposes)	Boundary device needed MSI used for that purpose	MSI breaks protocol and inspects sent messages	TXS Profibus as point to point to MSI TXS ethernet from MSI to service unit
From automation computer to other I&C via MSI and gateway	Sending data to other plant systems for visualization	Boundary device needed MSI and gateway used for that purpose	MSI breaks protocol and inspects sent messages Gateway breaks protocol and checks on allowed functionality	TXS Profibus as point to point to MSITXS ethernet from MSI to gatewayOther protocol from gateway to outside I&C system

TABLE 3. COMMUNICATION PATHS WITHIN TXS



AC MSI SU QDS GW PPS	Automation computer Monitoring and service interface Service unit Qualified display system Gateway Plant process computer or Operational I&C
	Command and signaling messages Data messages Plant specific messages (non TXS)

FIG. 19. Possible security zones design for a typical TXS system architecture.

- Only the two lowest ISO layers (layer 1 and layer 2) and the application layer (layer 7) are used.
- Only fixed message sizes are used (configured by the code generators).
- Cyclic redundancy checks are performed at the application layer.

For communication via TXS ethernet, a layer 2 protocol (in accordance with IEEE 802.2 technology) without network services is used. A protocol framework in accordance with IEEE 802.3 (ethernet) is used for media access. All communication telegrams work with the fixed maximum application data length that is defined during the specification of the networking relevant hardware with the TXS editor. Buffer overflow is thereby avoided since the fixed message sizes result in static data structures generated by the TXS code generators.

This protocol framework and its length are fixed and can thus be analysed by the communication processor hardware in TXS for correctness. The controller's method of operation for checking the protocol framework cannot be modified.

The design of all processing modules, communication modules and input/output boards ensures that no cross communication between different ports (e.g. serial port for administration to TXS ethernet) can be performed (i.e. there is no protocol for forwarding low level service commands). This is realized by specially chosen hardware. Also, the MSI can be configured so that it cannot receive data from the gateways.

The separation of equipment for different tasks via separation of duties ensures that all external messages are evaluated by the MSI, which performs any needed protocol translation according to a specific set of rules.

No functionality for changing the communication configuration settings is provided, except by shutting down and loading new software. The detailed version information of all loaded software components (runtime environment, function block libraries, real time operating system kernel, networking software, etc.) can be downloaded at any time. The integrity of the embedded software can be verified based on outputs of cryptographic hash functions or algorithms (e.g. SHA-2, SHA-3, BLAKE2, Whirlpool) and by completely downloading the binary of the embedded application software and system software.

Appendix III

NUCLEAR FUEL DEGRADATION DETECTION SYSTEM

III.1. SUMMARY

This case study, of the replacement of a single I&C system within an operating NPP, illustrates that recognized industry standards (in this case, IEC standards) may be used to achieve compliance with IAEA guidance. In this study:

- A DCSA model for the NPP had been predetermined, including the definition of zones suitable for defined security levels.
- The safety function of the system is determined according to Ref. [8], which leads directly to the assignment of security levels and the creation of security zones. This allows system components to be allocated to zones.
- A system specific security risk assessment is done at an early/high level design phase and is used to determine the required security control measures in detail, using, for example, ISO/IEC 27000 series standards [18].
- I&C security requirements are then tracked though the verification and validation process in the same way as
 other project requirements are.

All work is put out to bid and performed by a third party contractor.

III.2. PROBLEM

The nuclear fuel degradation detection system of an NPP needs replacement due to obsolescence, in order to support safe electricity generation to the projected end of life of the NPP. Fuel degradation is detected by monitoring the levels of radionuclides within the primary coolant. Although simple radiation detection equipment is available, the use of more sensitive detectors and computerized signal processing techniques allows more detailed information to be obtained: this can improve safety margins by detecting more minor fuel degradation earlier. Furthermore, a requirement has been identified to pass measurement data to the company's IT network.

III.3. LIFE CYCLE PHASES

This case study addresses all system life cycle phases as described in SSG-39 [5].

III.4. CASE STUDY

Prevention or mitigation of nuclear fuel degradation outside the limits and conditions of normal operation is a Category B safety function in accordance with Ref. [8]. At this NPP, the Category B function is implemented by two diverse and independent systems, each assigned Class 3 in accordance with Ref. [19]. The equipment to be replaced is one such Class 3 system.

The NPP operator's policy for implementing a graded approach to I&C security is that the I&C security level is determined by the safety function category outlined in Ref. [8].

Information security attributes may be summarized as:

- Confidentiality is low (no specific confidentiality requirements apply);
- Integrity is high (primary coolant activity measurement data are used to support the safety case);
- Availability is medium (time limited operation of the reactor is permissible with only one of two diverse detection systems).

The NPP had a DCSA model and associated security control measures that were developed as part of a proprietary security risk assessment methodology. A concept analogous to security zones is inherent in the methodology, which accounts for pre-existing physical security measures at various locations within the NPP.

The procurement specification made clear that security control measures to ISO/IEC 27000 series standards [18], and support for a security risk assessment, would be required.

After the selection of a preferred bid, which included selection of a preferred high level concept design and major predeveloped components, a security risk assessment was done early in the design process, in order to precipitate more detailed and specific security requirements.

The high level concept design included the following components, organized here according to Ref. [3] I&C architecture levels:

- Level 0 (physical process) reactor primary coolant fluid.
- Level 1 (sensing and manipulating the physical process) detector and signal processing equipment.
- Level 2 (monitoring and controlling the physical process) HSIs and control room alarms and indications.
- Level 3 (workflow activities) data storage and off-line analysis.
- Level 4 (business related activities) data sharing via the company IT network provides business benefits.

The overall use of Refs [3] and [8], the IEC 27000 series [18], Ref. [19] and the proprietary risk management framework led to the creation of specific security levels that were then implemented within dedicated, segmented, physical security zones. This combination of standards led first to the grouping of systems into individual system functions, which were then assigned a specific security level. These functions were then implemented within specific systems, and those systems were housed in distinct security zones that provided an environment compatible with defined security levels. This decomposition of systems to functions, assignment of security levels to functions and instantiation of functions as system components housed in specific security zones is essentially compliant with IAEA computer security guidance.

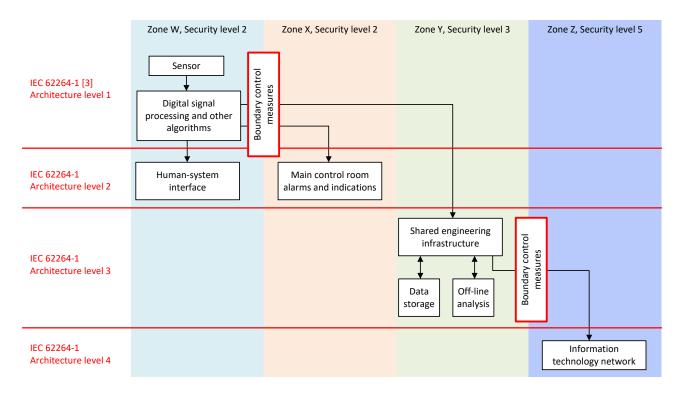


FIG. 20. Nuclear fuel degradation detection system design.

The identified security requirements were tracked in the same way as other requirements throughout the (V model) verification and validation process Ref. [1]. Both company standard and system specific security control measures were implemented.

Figure 20 shows the overall system design. The overall system has four distinct security zones and three different security levels. Zone W and Zone X are at the same security level, but at different physical locations within the NPP.

Zone W contains sensing and processing equipment, as well as HSI systems to provide overall system management and control. These functions are grouped into three systems: sensor systems, digital signal processing equipment, and dedicated HSI equipment. All these functions are associated with security level 2.

Zone X, also at level 2, is located in a different area of the plant. Zone X is the plant main control room, and boundary control measures are in place to protect data transmitted from Zone W to Zone X. Both zones are at the same security level, but the connected network is not protected at that level, nor are the data transmitted between the zones considered that sensitive. As a result, the internal zone networks are protected via boundary protection measures to support their higher security levels.

Zone Y is associated with security level 3. Boundary control mechanisms are in place to protect Zone W from Zone Y as they are at different security levels. Zone Y equipment stores specific data for later analysis on a dedicated, secured engineering network.

Finally, data are moved from Zone Y into Zone Z, at security level 5, for further review and archiving.

Overall, this system design supports IAEA computer security guidance, even though it was designed with a combination of standards from other standards organizations (such as the International Electrotechnical Commission) and private entities (the overall risk management plan). Furthermore, data generated in a highly secure area are moved in a secure way through the zoned infrastructure from very secure environments to relatively less secure areas.

REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-2.11, IAEA, Vienna (2018).
- [3] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Enterprise-control System Integration Part 1: Models and Terminology, IEC Standard 62264-1, IEC, Geneva (2013).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).
- [6] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Standards for Security Categorization of Federal Information and Information Systems, Report No. 199, NIST, Gaithersburg, MD (2004).
- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (in preparation).
- [8] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants Instrumentation and Control Systems Important to Safety — Classification of Instrumentation and Control Functions, IEC Standard 61226, 3rd edn, IEC, Geneva (2009).
- [9] NUCLEAR ENERGY INSTITUTE, Cyber Security Plan for Nuclear Power Reactors, NEI 08-09, Rev. 6, NEI, Washington, DC (2010).
- [10] SALTZER, J.H., KAASHOEK, M.F., Principles of Computer System Design: An Introduction, Morgan Kaufmann, Burlington, MA (2009).
- [11] SMITH, R.E., Elementary Information Security, Jones & Bartlett Learning, Burlington, MA (2015).
- [12] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants Instrumentation and Control Systems — Requirements for Coordinating Safety and Cybersecurity, IEC Standard 62859, IEC, Geneva (2016).
- [13] INTERNATIONAL ATOMIC ENERGY AGENCY, Conducting Computer Security Assessments at Nuclear Facilities, IAEA-TDL-006, IAEA, Vienna (2016).
- [14] ELECTRIC POWER RESEARCH INSTITUTE, Cyber Security Technical Assessment Methodology: Vulnerability Identification and Mitigation, EPRI Technical Report 3002008023, EPRI, Palo Alto, CA (2016).
- [15] SYMANTEC, W32.Stuxnet Dossier, Version 1.4, Symantec Corporation, Cupertino, CA (2011).
- [16] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, IAEA, Vienna (2018).
- [17] SALTZER, J.H., SCHROEDER, M.D., The Protection of Information in Computer Systems, Proc. IEEE 63 9 (1975) 1278–1308.
- [18] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Security Management Systems, ISO/IEC Standard 27000 series, ISO/IEC, Geneva (2013).
- [19] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants Instrumentation and Control Important to Safety — General Requirements for Systems, IEC Standard 61513, IEC, Geneva (2011).

Annex I

DATA COMMUNICATIONS SECURITY

Data communications are protected by following computer and communications security measures as defined in the facility computer security programme (CSP) and defensive computer security architecture (DCSA).

I-1. DESIGN MEASURES

Network topology design, access control, event logging and configuration management using hardware, software and procedural solutions have to be assessed for use in providing computer network security for instrumentation and control (I&C) systems. Similarly, access to physical network components and network configuration parameters have to be appropriately restricted, controlled and logged. Measures have to be implemented to allow only authorized individuals to implement approved changes to a network.

Hardware devices (e.g. firewalls, data diodes, trusted hardware or cryptographic solutions) or software solutions (e.g. software based network management and monitoring systems, intrusion detection systems (IDSs)) may be used in network design to improve the security of control system networks [I–1].

I-2. NETWORK SEGMENTATION/SEGREGATION

A common solution for the I&C system network protection of nuclear power plants (NPPs) is full network isolation from other networks (i.e. air gapping). Air gapped systems have still to implement some kind of internal monitoring through which data can be exported to analysis systems. Where air gapping is not feasible, networks need to be decomposed into security zones and need to be segregated strongly via both administrative and technical controls in compliance with the NPP's computer security requirements (i.e. level assigned to zone/system) and DCSA specification. For example, data diodes can be used to enforce unidirectional network based information flows, while hardened firewalls can help control and monitor bidirectional communications. Network traffic needs to be controlled and monitored to ensure that only expected devices communicate with one another, and that any unexpected network traffic or devices attempting to communicate on a network are appropriately detected as potential adverse events. Unused ports need to be physically detached or disabled.

I–3. I&C SYSTEM NETWORK DEFENCES

Most of these kinds of solutions today are focused on common computer networking protocols and have been extended to support certain industrial protocols. Industrial network defences do support a variety of industrial protocols, but they do not support all protocols in all environments. Furthermore, some areas of a system may not be able to be actively monitored due to safety requirements. In these cases, system designers have to apply compensating controls to help minimize computer security risk overall.

I-3.1. Mirroring networks

To monitor network traffic, the network infrastructure has to support and implement port mirroring or aggregating taps. This will allow engineers to inspect and archive traffic from network segments in real time, without impacting the overall network quality of service. The taps or mirrors may also contain vulnerabilities and therefore need to be unidirectional so as to not provide an attack vector. Additionally, span traffic aggregation needs to consider the potential for electrical faults to propagate between independent systems via network monitoring hardware (i.e. electrical isolation/protection). Network data can then be collected for either security

analysis or traffic profiling. The access of this mirror has to be controlled in order to prevent unauthorized access to network data.

I-3.2. Intrusion detection and prevention systems

IDSs observe whether a system being monitored is operating as expected. This is implemented through a system or device monitoring mechanism that connects directly to an I&C device and monitors for anomalies in internal device behaviour. For example, during routine operation of a device, a firmware or other software logic update would not be expected. An IDS may monitor a device for such abnormal behaviour and may provide an alarm if and when this abnormal behaviour is observed. IDSs can be host based or network based. Network based IDSs can be configured to use a mirror port to collect data. Host based IDSs will be part of a system design.

Intrusion prevention systems (IPSs) are active hardware/software solutions that receive and evaluate data sent over a network and can generate a predetermined response. Any responses have to be evaluated to ensure that no critical communications or functions are disabled inadvertently by those responses. They can detect attacks early on, generate alarms that notify monitoring staff of attacks and implement predetermined actions. Possible predetermined actions in response to adverse network traffic may include blocking specific network traffic (i.e. between particular devices), blocking the source of the adverse traffic or blocking entire network segments. An IPS operates in real time and includes IDS modules. These IDS modules may include sensing subsystems that are designed to collect events related to the security of the protected network. The modules may also include system and subsystem analysis designed to detect network attacks and suspicious activity.

When IPSs are implemented in I&C systems, care needs to be taken to ensure the IPS in no way adversely affects or stops (through its protective action) the ability of the system to meet its performance, safety or any other requirements.

I-3.3. Wireless

Wireless technologies introduce an attack vector for an adversary. It is impossible to implement a defined secure boundary for wireless signals. Thus, the use of wireless technologies in I&C systems has always to be in compliance with an established DCSA.

I-4. REMOTE ACCESS

Components of I&C systems that provide remote access have to be maximally isolated from the industrial network by means of data diodes and firewalls and have to comply with NPP computer security requirements and DCSA specification. Appropriate authentication, authorization, logging and other security controls need to be placed at points of remote access as well. In some cases, systems have to be accessed remotely. When this is the case, these systems have to have compensating security controls in place to minimize the risk of intrusion and be designed in strict accordance with the facility CSP and DCSA.

REFERENCE TO ANNEX I

[I-1] HURD, C.M., McCARTY, M.V., A Survey of Security Tools for the Industrial Control System Environment, Idaho National Laboratory, Idaho Falls, ID (2017).

Annex II

RECOMMENDATIONS FOR ESSENTIAL DATA COLLECTION

Category	Asset type
Hardware assets	 Programmable/intelligent assets of I&C systems (intelligent sensors and actuators, HSI, DCS, FPGA, etc.); Servers and workstations; Peripheral devices, such as printers, storage devices, etc.; Active elements of a network (switches, routers, firewalls, data diodes, etc.).
Software assets	 Software that operates a programmable/intelligent hardware asset of an I&C system (e.g. platform software, firmware without possibilities for human interaction); Operating systems; Software installed over an operating system (they are presented in a list of installed programs); Software that is not installed but runs on an operating system (they are not presented in a list of installed programs); Software that runs in the background as a service; Firmware that offers human interaction (e.g. BIOS of a workstation or a server or HSI of a printer).
Configuration files/static databases of a hardware/software asset	 Configuration files that have effects on operation of an asset; Databases that work the same way as configuration files mentioned above; Other databases such as malware databases; Access lists, firewall rules.
User accounts for the assets	 Users of the operating systems; Users of software and services; Users of firmware with human interaction possibilities; User groups.
Communication pathways	 Firewall configurations; System white lists; Application white lists; Router and switch configurations; Proxy configurations.
Security policies applied on hardware/software assets	- Documents describing computer security policies and CSP.

TABLE II-1. POSSIBLE BASELINE INFORMATION

Note: BIOS — basic input/output system; CSP — computer security programme; DCS — distributed control system; FPGA — field programmable gate array; HSI — human–system interface; I&C — instrumentation and control.

TABLE II-2. SUGGESTED DATA TO BE COLLECTED BY CATEGORY

Category	Data to be collected
Hardware assets	 System ID; Hardware ID; Hardware version; Hardware type (server, workstation, peripheral device (printer, storage device, etc.), network device (switch, router, etc.), I&C device (DCS, FPGA, etc.) or other); Virtualization status (e.g. is it virtualized?); List of its physical ports; Hardware location; Access permissions needed; Key, key card, etc. needed for physical access; Responsible authority.
Software assets	 Software ID; Software name; Software version and/or patch level; Type (operating system, firmware, installed software or not, service); Realized data communication ports; Remote control/access capabilities; Licences (expiration date, number of users/nodes/CPUs); Responsible authority.
Configuration files/static databases of a hardware/software asset	 File ID; File name; File type; File size; File version; Asset the file belongs to; Where the file is stored (locally, on a remote server, on removable media); Where the backup of the file is stored; Responsible person to update and upload the configuration file; Last modification.
User accounts	 Account ID; Account type (operating system, software, firmware); ID of the asset this account belongs to; User name; Full name; Description of user; User type (normal user, administrator, technical user (who runs services?)); Account status (active, disabled); Group membership; Where the user account is stored/located/handled (locally, in a domain or in an access control system); User rights and permissions; Expiration date and time.

TABLE II-2. SUGGESTED DATA TO BE COLLECTED BY CATEGORY (cont.)

Category	Data to be collected			
Communication pathways	 Description and purpose of the given data communication pathway, distinguishing data flow in and data flow out. What systems the given channel connects to. Whether the communication is bidirectional or unidirectional (in the unidirectional case: which system is the source, and which is the destination). Protocol (Modbus, Profibus, Fieldbus, HART, TCP, UDP, etc.). Local address. Local port. Remote address. Remote port. ID of the software/hardware asset that realizes the channel (and what mode it communicates: server and/or client). Documentation for physical and logical network diagrams for all cyber assets showing the assets within each zone and the security level assigned to each asset and each zone. These diagrams also show computer security components. Complementary physical and logical network diagrams: Physical diagrams show room location of physical equipment, including passive devices such as switches that may not appear on a logical diagram, as well as the physical protective measures that may be present. Logical diagrams show components and the communication paths between components and whether security boundaries are being traversed. The logical diagram also depicts segregated connections within a device, such as a 'virtual local area network', that would not be visible on physical network diagrams. Both types of diagrams are necessary in order to capture and analyse the security posture of a system. 			
Security policies applied on hardware/software assets	 Documented source; Version of the document/policies; Assets these policies apply to. 			

Note: CPU — central processing unit; DCS — distributed control system; FPGA — field programmable gate array; HART — highway addressable remote transducer; I&C — instrumentation and control; TCP — transmission control protocol; UDP — user datagram protocol.

TABLE II-3. SUGGESTED DATA TO BE COLLECTED ON USER GROUPS

Category	Data to be collected	
User groups	 Group type; Group name; Group description; Rights and permissions; IDs of member users. 	

TABLE II-4. SUGGESTEI	D SECURITY ACTIONS BY CATEGORY

Category	Action
Hardware assets	 Check that all non-necessary input/output ports (network, USB, serial, etc.) are disabled in the firmware settings or in the operating system. If a port cannot be disabled via firmware, physical protection on those ports has to be stated in the physical protection plan. Check that configuration of the hardware is only possible via an authenticated account in the firmware. Check that all default passwords are changed.
Software assets	 Uninstall any unnecessary software. Update to the latest versions of necessary software. Check and store information of the known vulnerabilities of the given version.
Configuration files/static databases of a hardware/software asset	 — Give an ID to the file. — Make a backup copy of the file.
User accounts	 Delete unnecessary accounts. Disable temporary accounts that are not in use. Make sure that all accounts have an appropriate password (which conforms to the given password policy). Check the rights of the enabled accounts. Check that no real user account runs any services in the background. Check that all technical users have appropriate passwords. Check that no technical user is able to log in interactively.
Communication pathways	 Disable unnecessary pathways by removing the software asset that realizes it and/or by blocking its data communication via firewalls. Check that unidirectional pathways can communicate only in the allowed direction. Check the presence of any unnecessary open communication ports and disable them as described above. Check that the pathway only transfers data that it is intended to.
Security policies applied on hardware/software assets	— Check that all security policy settings are set correctly.

TABLE II–5. SUGGESTED SECURITY ACTIONS FOR USER GROUPS

Category	Action
User groups	 Check permissions of a given user group. Check the members of the group. Delete unnecessary user groups.

ABBREVIATIONS

CSP	computer security programme
DCSA	defensive computer security architecture
DiD	defence in depth
EWS	engineering workstation
FAT	factory acceptance testing
HSI	human-system interface
I&C	instrumentation and control
IDS	intrusion detection system
IPS	intrusion prevention system
MSI	monitoring and service interface
NPP	nuclear power plant
PLC	programmable logic controller
SDA	sensitive digital asset
TXS	TELEPERM XS

CONTRIBUTORS TO DRAFTING AND REVIEW

Bajramovic, E.	Framatome, Germany
Batson, S.	Deloitte and Touche LLP, United States of America
Cary, A.	EDF Energy, United Kingdom
Chernyaev, A.	Rusatom Automation and Control Systems, Russian Federation
Collier, T.	Ontario Power Generation, Canada
Dickinson, J.	Sellafield Ltd, United Kingdom
Dyer, P.	Office for Nuclear Regulation, United Kingdom
Eiler, J.	International Atomic Energy Agency
Ellis, A.	Indigo Consulting, United Kingdom
Estes, M.	Deloitte and Touche LLP, United States of America
Franzén, P.	Westinghouse Electric Sweden AB, Sweden
Herb, R.	Southern Nuclear, United States of America
Holappa, J.	Nixu, Finland
Jung, C.H.	Canadian Nuclear Safety Commission, Canada
Lamb, C.	Sandia National Laboratories, United States of America
Lawson-Jenkins, K.	Nuclear Regulatory Commission, United States of America
Lee, C.K.	Korea Atomic Energy Research Institute, Republic of Korea
McCrory, F.	Sandia National Laboratories, United States of America
MacDonald, M.	Canadian Nuclear Laboratories, Canada
Podolniy, V.	Rusatom Automation and Control Systems, Russian Federation
Posch, A.	Paks II. Ltd., Hungary
Robinson, S.	EDF Energy, United Kingdom
Rowland, M.	International Atomic Energy Agency
Russomanno, S.	SunPort S.A., Canada
Sakharov, K.	Rusatom Automation and Control Systems, Russian Federation
Sladek, J.	Lofty Perch Inc., Canada
Thompson, J.	Bruce Power, Canada
Turi, T.	Paks II. Ltd., Hungary
Waedt, K.	Framatome, Germany

Technical Meeting

Gloucester, United Kingdom: 8-12 May 2017

Consultants Meetings

Vienna, Austria: 4–8 April 2016, 28 November–2 December 2016, 10–14 July 2017, 2–6 July 2018

and Decommissioning Objectives NW-O 2. Decommissioning of Nuclear Facilities NW-G-2.# NW-T-2.# Radioactive Waste Management 1. Radioactive Waste Management NW-G-1.# NW-T-1.# (*) as of 1 January 2020 (**) Formerly 'Nuclear Power' (NP) 3. Environmental Remediation NW-G-3.# Nuclear Reactors (NR)*, Technical Report (T), Research Reactors (topic 5), #4 Nuclear Fuel (NF), Technical Report (T), Spent Fuel Management (topic 3), #6 Radioactive Waste Management and Decommissioning (NW), Guides NW-T-3.# and Methodologies (G), Radioactive Waste Management (topic 1) #1 Nuclear Energy General (NG), Guides and Methodologies (G), Nuclear Infrastructure and Planning (topic 3), #1 2. Fuel Engineering and Performance NF-G-2.# Nuclear Fuel Cycle Objectives 1. Exploration and Production of Raw Materials for Nuclear Energy NF-G-1.# 5. Nuclear Fuel Cycle Facilities NF-G-5.# NF-T-5.# 3. Spent Fuel Management NF-G-3.# NF-T-3.# Structure of the IAEA Nuclear Energy Series* 4. Fuel Cycle Options NF-G-4.# NF-T-4.# NF-T-2.# NF-T-1.# NF-O Nuclear Energy Basic Principles NE-BP Commissioning of Nuclear Power Plants NR-G-2.# NR-T-2.# NW-G-1.1: NG-G-3.1: 3. Operation of Nuclear Power Plants NR-G-3.# NR-T-3.# Examples NR-T-5.4: NF-T-3.6: 4. Non Electrical Applications NR-G-4.# NR-T-4.# Nuclear Reactor** Objectives 1. Technology Development NR-G-1.# NR-T-1.# 2. Design, Construction and 5. Research Reactors NR-G-5.# NR-T-5.# NR-O Guides and Methodologies 4. Economics and Energy System Analysis NG-G-4# NG-T-4# Topic designations Guide or Report number Nuclear Energy General Objectives 3. Nuclear Infrastructure and Planning NG-G-3.# NG-T-3.# 1. Management Systems NG-G-1.# NG-T-1.# 6. Knowledge Management 5. Stakeholder Involvement Technical Reports 2. Human Resources **Basic Principles** NG-G-6.# NG-T-6.# NG-G-2.# NG-T-2.# NG-G-5.# NG-T-5.# Objectives NG-O Nos 1–6: #: ₩ 6 0 0 1 7 6 0 1

57



ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

NORTH AMERICA

Bernan / Rowman & Littlefield

15250 NBN Way, Blue Ridge Summit, PA 17214, USA Telephone: +1 800 462 6420 • Fax: +1 800 338 4550 Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group

Gray's Inn House 127 Clerkenwell Road London EC1R 5DB United Kingdom

Trade orders and enquiries:

Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640 Email: eurospan@turpin-distribution.com

Individual orders: www.eurospanbookstore.com/iaea

For further information:

Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609 Email: info@eurospangroup.com • Web site: www.eurospangroup.com

Orders for both priced and unpriced publications may 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 26007 22529 Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

INTERNATIONAL ATOMIC ENERGY AGENCY VIENNA