امنیت رایانه برای سیستمهای کنترل و ابزار دقیق در تأسیسات هسته ای

CONTENTS

نصب ، یکپارچه سازی و راه اندازی کلی سیستم ابزاردقیق و کنترل

1. معرفی

1.1. زمینه

1.1. Instrumentation and control (I&C) systems play a critical role in ensuring the safe operation of nuclear facilities. As digital technologies continue to evolve and become more capable, they are increasingly being incorporated into and integrated with I&C systems1. New nuclear facilities and modern nuclear facility designs use highly integrated digital I&C systems to efficiently and simultaneously handle vast quantities of process data while requiring less human interaction and intervention than previous I&C systems. Digital technologies are also often introduced into I&C systems during the modernization of existing facilities. However, the application of digital technologies within I&C systems has made these systems vulnerable to cyber attacks.

1.1. سیستم های ابزار دقیق و کنترل (I&C) نقش مهمی در اطمینان از بهره برداری ایمن از تاسیسات هسته ای دارند. از آنجا که فن آوری های دیجیتال همچنان در حال تکامل هستند و توانایی آنها بیشتر میشود ، آنها به طور فزاینده ای با سیستم های ابزار دقیق و کنترل ترکیب و یکپارچه می شوند. تأسیسات هسته ای جدید و طرح های هسته ای مدرن از سیستم های دیجیتال ابزار دقیق و

کنترل کاملاً یکپارچه استفاده می کند تا بتواند مقادیر عظیمی از داده را به طور مؤثر و همزمان پردازش کنند ، در حالی که نیاز به تعامل و مداخله کمتری از انسان در مقایسه با سیستم های ابزار دقیق و کنترل قبلی دارد. همچنین فن آوری های دیجیتال طی مدرنیزه کردن امکانات موجود به سیستم های ابزار دقیق و کنترل وارد می شوند. با این حال ، استفاده از فن آوری های دیجیتال در سیستم های ابزار دقیق و کنترل ، این سیستم ها را در برابر حملات سایبری آسیب پذیر کرده است.

1.2. A cyber attack is a malicious act carried out by individuals or organizations that targets sensitive information or sensitive information assets with the intent of stealing, altering, preventing access to or destroying a specified target through unauthorized access to (or actions within) a susceptible system. Sensitive information assets include control systems, networks, information systems and any other electronic or physical media. Adversaries have launched successful cyber attacks directed at I&C systems, such as the Stuxnet cyber attack, which led to the destruction of equipment at a nuclear facility [1].

1.2. حمله سایبری اقدامی مخرب است که توسط افراد یا سازمانهایی انجام می گیرد که اطلاعات حساس یا تجهیزات اطلاعاتی حساس را با هدف سرقت ، تغییر ، جلوگیری از دسترسی یا از بین بردن یک هدف مشخص از طریق دسترسی غیرمجاز به (یا اقدامات درون) یک سیستم مستعد هدف قرار می دهد. تجهیزات اطلاعاتی حساس شامل سیستم های کنترل ، شبکه ها ، سیستم های اطلاعاتی و سایر رسانه های الکترونیکی یا فیزیکی است. افراد متخاصم حملات سایبری موفقی را به سمت سیستمهای ابزار دقیق و کنترل انجام داده اند ، مانند حمله سایبری استاکس نت ، که منجر به از بین رفتن تجهیزات در تأسیسات هسته ای شد [1].

1.3. Cyber attacks on I&C systems may jeopardize the safety and security of nuclear facilities. They may contribute to sabotage or aid in the unauthorized removal of nuclear material. The effects of cyber attacks on I&C systems related to safety may result in a wide range of consequences, such as a temporary loss of process control or unacceptable radiological consequences. Public awareness of cyber attacks that affect I&C systems may also undermine confidence in the safety and security of nuclear facilities.

1.3. حملات سایبری به سیستم های ابزار دقیق و کنترل ممکن است ایمنی و امنیت تاسیسات هسته ای را به خطر اندازد. آنها ممکن است به خرابکاری یا کمک در برداشت غیرمجاز مواد هسته ای کمک کنند. اثرات حملات سایبری بر روی سیستم های ابزار دقیق و کنترل مربوط به ایمنی ممکن است منجر به طیف گسترده ای از عواقب مانند از دست دادن موقت کنترل فرآیند یا پیامدهای رادیولوژیکی غیرقابل قبول شود. آگاهی عمومی از حملات سایبری که بر سیستم های ابزار دقیق و کنترل تأثیر می گذارد ، ممکن است اعتماد به نفس در ایمنی تأسیسات هسته ای را نیز تضعیف کند.

1.4. The need for the protection of computer based systems (including I&C systems) is established in the Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2], para. 4.10, which states that: "Computer based systems used for physical protection, nuclear safety and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the *threat assessment* or *design basis threat.*"

1.4. نیاز به حفاظت از سیستم های مبتنی بر رایانه (از جمله سیستم های ابزار دقیق و کنترل) در توصیه های امنیت هسته ای در مورد حفاظت فیزیکی از مواد هسته ای و تأسیسات هسته ای ([2] INFCIRC / 225 / Revision 5) ، پاراگراف ارائه شده است. 4.10 که بیان می کند:

"سیستم های مبتنی بر رایانه که برای حافظت فیزیکی ، ایمنی هسته ای و حسابداری و کنترل مواد هسته ای مورد استفاده قرار می گیرند باید در برابر دستکاری محافظت شوند (به عنوان مثال حمله سایبری ، دستکاری یا جعل) سازگار با ارزیابی تهدید یا تهدیدات مبنای طراحی."

1.5. IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities [3], provides guidance specific to nuclear facilities on implementing a computer security programme to support the guidance stated in Ref. [2]. Reference [3] also provides details of key terminology such as 'computer security', 'IT security' and 'cyber security'. The terms 'IT security' and 'cyber security' are, for the purpose of this publication, considered synonyms of computer security and will not be used.

1.5 نشریه امنیت هسته ای شماره 17 آژانس بین المللی انرژی هسته ای ، امنیت رایانه ای در تاسیسات هسته ای [3] ، راهنمایی های ویژه ای را برای تأسیسات هسته ای در مورد اجرای یک برنامه امنیتی رایانه برای پشتیبانی از راهنمایی های اعلام شده در Ref فراهم می کند. [2] مرجع [3] همچنین جزئیات اصطلاحات کلیدی مانند "امنیت رایانه" ، "امنیت IT" و "امنیت سایبر" را ارائه می دهد. اصطلاحات "امنیت فناوری اطلاعات" و "امنیت سایبری" به همین منظور ، مترادف امنیت رایانه در نظر گرفته شده و مورد استفاده قرار نمی گیرند.

1.6. Computer security needs to be explicitly considered in every phase of th I&C system life cycle. The term 'life cycle' (as opposed to lifetime) implies that the system's life is genuinely cyclical (as in the case of recycling or reprocessing), and notably that elements of the old system are used in the new system. Reference [4] contains a list of typical I&C life cycle activities.

1.6امنیت رایانه باید در هر مرحله از چرخه سیستم **ابزار دقیق و کنترل** به صراحت مورد توجه قرار گیرد. اصطلاح چرخه (بر خلاف طول عمر) دلالت بر این دارد که عمر سیستم کاملاً چرخه ای است (مانند مورد بازیافت یا پردازش مجدد) و به ویژه اینکه عناصر سیستم قدیمی در سیستم جدید مورد استفاده قرار می گیرند. مرجع [4] شامل لیستی از فعالیتهای معمول چرخه **ابزار دقیق و کنترل** است.

1.7. Historically, computer security was not given significant consideration in the design of I&C systems at nuclear facilities because hardwired or analogue systems were assumed to be invulnerable to cyber attack owing to their rigid implementation, isolation and system segregation and to a near absence of interactive communications, particularly with external networks or systems. The transition to digital technology has changed the nature of I&C systems at nuclear facilities by enabling the

interconnection of reprogrammable (remotely or locally) and functionally distinct I&C systems.

1.7از لحاظ تاریخی ، امنیت رایانه در طراحی سیستم های ابزار دقیق و کنترل در تأسیسات هسته ای مورد توجه چشمگیری قرار نگرفته است. زیرا فرض بر این است که سیستم های سنتی (مدار فرمان و سیم کشی شده) یا آنالوگ به دلیل اجرای سفت و سخت ، ایزولاسیون و جداسازی سیستم و عدم وجود ارتباطات تعاملی (به خصوص با شبکه ها یا سیستم های خارجی) ، در معرض حمله سایبری قرار نمیگیرند. استفاده از فناوری دیجیتال با فعال کردن امکان اتصال توسط تجهیزات قابل برنامه ریزی (از راه دور یا محلی) ، ماهیت سیستم های ابزار دقیق و کنترل را در تأسیسات هسته ای تغییر داده است.

1.8. The greater use of versatile programmable digital components and devices has resulted in a reduction in the diversity of I&C systems. This includes the use of common elements and approaches across a variety of industrial applications (e.g. communication protocols). Malicious acts2 directed at these common technologies in other industries could also affect a nuclear facility.

1.8استفاده بیشتر از دستگاه ها و تجهیزات دیجیتال قابل برنامه ریزی، منجر به کاهش تنوع سیستم های ابزار دقیق و کنترل شده است. این شامل استفاده از عناصر و رویکردهای رایج در انواع برنامه های صنعتی (به عنوان مثال پروتکل های ارتباطی) است. اقدامات مخرب برروی این فناوریهای رایج در صنایع دیگر نیز می تواند تأسیسات هسته ای را تحت تأثیر قرار دهد.

1.9. Authorized individuals, whether on-site or at a remote location, who have logical or physical access to I&C systems may, as insiders, pose a threat to the safety and security of a nuclear facility. These insiders may be facility employees or personnel employed by vendors, contractors or suppliers who may be able to use their authorized access to perform malicious acts. The need for the protection of computer systems from insider threats is recognized in Ref. [5].

1.9 اشخاص مجاز ، چه در محل و یا در یک مکان از راه دور ، که دسترسی منطقی یا فیزیکی به سیستم های ابزار دقیق و کنترل دارند ، ممکن است به عنوان نفوذی ، ایمنی و امنیت تأسیسات هسته ای را تهدید کنند. این نفوذی ها ممکن است کارمند موسسه و یا پرسنل فروشندگان ، پیمانکاران یا تأمین کنندگان باشند که ممکن است بتوانند از دسترسی مجاز خود برای انجام کارهای مخرب استفاده کنند. نیاز به حفاظت از سیستم های رایانه ای در برابر تهدیدات خودی در Refمشخص شده است. [5]

2. OBJECTIVE

اهداف

1.10. The objective of this publication is to provide guidance for the protection of I&C systems at nuclear facilities on computer security against malicious acts that could prevent such systems from performing their safety and security related functions. While the focus of this publication is

on the secure operation of these systems, application of this guidance may also contribute to improving the safety and operational performance of nuclear facilities.

1.10هدف از انتشار این کتاب ارائه راهنمایی برای حفاظت از سیستم های ابزار دقیق و کنترل در تأسیسات هسته ای در زمینه امنیت رایانه در برابر اقدامات مخرب است. اقداماتی که می تواند مانع از انجام وظایف ایمنی و امنیت این تجهیزات شود. در حالی که تمرکز این کتاب بر امنیت این سیستم ها است ، استفاده از این راهنما همچنین می تواند به بهبود ایمنی و عملکرد عملیاتی تاسیسات هسته ای نیز کمک کند.

1.11. This publication is intended for competent authorities, including regulatory bodies, as well as nuclear facility management, operations, maintenance and engineering personnel, I&C vendors, contractors and suppliers, I&C designers, research laboratories and other organizations concerned with the safety and security of nuclear facilities.

1.11این نشریه برای مقامات ذیصلاح ، از جمله نهادهای نظارتی ، و همچنین مدیریت تأسیسات هسته ای ، کارکنان بهره بردار، تعمیر و نگهداری و مهندسین ، فروشندگان ابزار دقیق و کنترل ، پیمانکاران و تأمین کنندگان ، طراحان ابزار دقیق و کنترل ، آزمایشگاه های تحقیقاتی و سایر سازمان های مرتبط با ایمنی و امنیت تاسیسات هسته ای در نظر گرفته شده است.

SCOPE

قلمرو

1.12. The scope of this publication is the application of computer security measures to I&C systems that provide safety, security[3] or auxiliary functions at nuclear facilities. These measures are intended to protect I&C systems against malicious acts perpetrated by individuals or organizations. This publication also addresses the application of such measures to the development, simulation and maintenance environments of these systems.

1.12دامنه این کتاب کاربرد امنیت رایانه ای در سیستم های I&C است که وظیفه ایمنی ، امنیت یا کمکی در تاسیسات هسته ای را ارائه می دهند. این اقدامات برای محافظت از سیستم های ابزار دقیق و کنترل در برابر اقدامات مخرب انجام شده توسط افراد یا سازمان ها در نظر گرفته شده است. این کتاب همچنین به کاربرد چنین اقداماتی در محیط های توسعه ، شبیه سازی و تعمیر و نگهداری این سیستم ها می پردازد.

1.13. The guidance given in this publication is applicable to I&C systems at new[4] nuclear facilities and to new I&C systems at existing facilities. The guidance is expected to be implemented to the greatest extent possible for legacy I&C systems at existing facilities, including those that do not use digital technology.

1.13راهنمایی های ارائه شده در این کتاب برای سیستم های ابزار دقیق و کنترل در تأسیسات هسته ای جدید (

A new facility is a facility that has yet to complete the commissioning stage.

) و سیستم های جدید ابزار دقیق و کنترل در تأسیسات موجود قابل استفاده است. انتظار هست که این راهنمایی ها تا حد ممکن برای سیستم های I&C قدیمی موجود در تاسیسات ، از جمله مواردی که از فناوری دیجیتال استفاده نمی کنند ، نیز اجرا شود.

1.14. While not explicitly addressed in this publication, other interfacing systems and information and communications technology (ICT) systems such as work control and communications systems may introduce risks to the I&C system(s). These risks needs to be accounted for when designing and implementing computer security measures for I&C systems in a facility. Computer security measures for these systems may be different from those applied to I&C systems and are to be evaluated and tailored appropriately.

1.14اگرچه در این کتاب به صراحت مورد اشاره قرار نگرفته است ، سایر سیستم های رابط و سیستم های فناوری اطلاعات و ارتباطات (ICT) مانند سیستم های حظور و غیاب و سیستمهای ارتباطی ممکن است خطراتی را برای سیستمهای ابزار دقیق و کنترل به وجود آورد. این خطرات را باید هنگام طراحی و اجرای اقدامات امنیتی رایانه برای سیستم های ابزار دقیق و کنترل در یک مرکز به حساب آورد. اقدامات امنیتی رایانه ای برای این سیستم ها ممکن است متفاوت از آنچه در سیستم های ابزار دقیق و کنترل اعمال می شود باشد و به طور مناسب ارزیابی و تنظیم شوند.

1.15. This publication does not provide comprehensive guidance on safety considerations for I&C systems. Such guidance can be found in Refs [4, 6]. Additionally, this publication does not define or alter the technical terms used in IAEA safety standards and other safety related IAEA publications. These terms are highlighted in this publication, when used, and their definitions can be found in the IAEA Safety Glossary [7].

1.15این کتاب راهنمای جامعی در مورد ملاحظات ایمنی برای سیستم های ابزار دقیق و کنترل ارائه نمی دهد. چنین راهنمایی هایی را می توان در مرجع [4,6] یافت. علاوه بر این ، این نشریه اصطلاحات فنی مورد استفاده در استانداردهای ایمنی IAEAو سایر انتشارات آژانس انرژی هسته ای را تعریف یا تغییر نمی دهد. در هنگام استفاده ، این اصطلاحات برجسته می شوند و تعاریف آنها را می توانید در واژه نامه ایمنی آژانس بین المللی انرژی اتمی یافت [7]

STRUCTURE

ساختار

1.16. Following this introduction, this publication is separated into four sections. Section 2 presents an overview of I&C systems in use at nuclear facilities and the role of computer security

in protecting these systems from cyber attacks. Section 3 presents the relationship between computer security and safety for I&C systems. Section 4 presents computer security guidance to be applied in the various life cycle phases of I&C systems, including during the decommissioning of a facility.

1.16پس از این مقدمه ، این کتاب به چهار بخش تفکیک شده است. بخش 2 مروری بر سیستم های ابزار دقیق و کنترل مورد استفاده در تاسیسات هسته ای و نقش امنیت کامپیوتر در حفاظت از این سیستم ها در برابر حملات سایبری ارائه می دهد. در بخش 3 رابطه بین امنیت و ایمنی سیستمهای ابزار دقیق و کنترل ارائه شده است. بخش 4 راهنمایی های امنیتی را که باید در مراحل مختلف چرخه سیستم های ابزار دقیق و کنترل ، از جمله در مرحله تخریب و جمع کردن یک مرکز استفاده شود ، ارائه می دهد.

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

.2مفاهیم کلیدی برای امنیت رایانه سیستم های ابزار دقیق و کنترل

2.1. The I&C systems in nuclear facilities are used to monitor and control processes and equipment. These systems include:

.2.1سیستم های ابزار دقیق و کنترل در تأسیسات هسته ای برای نظارت و کنترل فرایندها و تجهیزات استفاده می شود. این سیستم ها شامل موارد زیر است:

(a) SCADA (supervisory control and data acquisition) systems;
(b) Distributed control systems;
(c) Centralized digital control systems;
(d) Control systems composed of programmable logic controllers;
(e) Micro-controllers and ‘smart’ devices;
(f) Systems using programmed logic devices (e.g. field programmable gate arrays, complex programmable logic devices and application-specific integrated circuits). Similar systems that control industrial plants are often called ‘industrial control systems’.

الف) سیستم های کنترل نظارتی و جمع آوری داده ها (SCADA)

ب) سیستم های کنترل توزیع شده.

ج) سیستم های کنترل دیجیتال متمرکز؛

د) سیستم های کنترل متشکل از کنترل کننده های منطقی قابل برنامه ریزی (plc).
ه) میکروکنترلرها و دستگاههای "هوشمند"؛
و) سیستم هایی که از دستگاه های منطقی برنامه ریزی شده استفاده می کنند (مثلاً FPGA، CPLD و مدارهای مجتمع اختصاصی یا ACID). سیستمهای مشابهی که تجهیزات صنعتی را کنترل می کنند که غالبا "سیستم های کنترل صنعتی" نامیده می شوند.

2.2. I&C systems are designed to provide for the safe, secure, reliable and deterministic behaviour of the nuclear facility in both normal and abnormal operation[5]. Design considerations and measures intended to improve safety may also provide benefits for security. For example, design measures such as deterministic performance, fault avoidance, fault detection, fault tolerance approaches, configuration management, independent verification and validation, and other advanced testing methods may provide some defence against malicious attempts to alter the behaviour of I&C systems.

2.2. سیستم های ابزار دقیق و کنترل به گونه ای طراحی شده اند که بتوانند رفتار ایمن ، دارای امنیت ، مطمئن و قطعی تاسیسات هسته ای را در هر دو عملکرد عادی و غیر عادی فراهم کنند. ملاحظات و اقدامات در نظر گرفته شده برای بهبود ایمنی نیز می تواند مزایایی برای امنیت ایجاد کند. به عنوان مثال ، اقدامات طراحی مانند عملکرد معین ، اجتناب از خطا ، تشخیص خطا ، رویکردهای تحمل خطا ، مدیریت پیکربندی ، تأیید و اعتبار سنجی مستقل و سایر روشهای پیشرفته آزمایش ممکن است دفاع در برابر تلاشهای مخرب برای تغییر رفتار سیستمهای ابزار دقیق و کنترل را نیز فراهم کند.

2.3. The design of the overall I&C architecture in nuclear facilities incorporates concepts that may contribute to computer security by mitigating the effects of intentional or accidental mal-operation[6], such as independence, redundancy, safety defence in depth and diversity[7]. The term ‘safety defence in depth’ is used in this publication to refer to defence in depth as defined in the IAEA Safety Glossary [7], to distinguish it from the application of the similar, but security-focused concept of ‘defence in depth’ (as defined in the Nuclear Security Fundamentals [8]) in implementing computer security measures, described in Section 4.

[6] The term ‘mal-operation’ is used in this text to refer to situations that have not been previously considered (i.e. are not anticipated operation occurrences), but for which the I&C system does not operate as expected.

[7] Independence, redundancy, safety defence in depth and diversity refer here to specific concepts that are used in the IAEA Safety Glossary [7].

2.3. طراحی کلی ابزار دقیق و کنترل در تأسیسات هسته ای مفاهیمی را شامل می شود که می توانند اثر اقدامات عمدی یا تصادفی را کاهش دهند. مفاهیمی از قبیل استقلال ، سیستم پشتیبان ، دفاع ایمن در عمق و تنوع ، به امنیت رایانه کمک می کنند.

اصطلاح دفاع ایمن در عمق که در این کتاب به کار رفته است ،معادل کلمه استفاده شده در واژه نامه ایمنی آژانس بین المللی انرژی هسته ای تعریف شده است [7] (تا آن را از کاربرد مفهوم مشابه ، اما متمرکز بر امنیت دفاع متمایز کند. (همانطور که در اصول امنیت هسته ای [8] در اجرای اقدامات امنیتی رایانه ، شرح داده شده در بخش 4 تعریف شده است.

2.4. The implementation of these concepts in a facility's overall I&C architecture and other design measures should be assessed to determine their contribution to computer security. For example, diversity of design or technology is likely to reduce common vulnerabilities among key safety or control systems; however, it may add vulnerabilities that are unique to each individual system.

2.4اجرای این مفاهیم در معماری کلی ابزار دقیق و کنترل یک مرکز و سایر اقدامات طراحی باید برای تعیین سهم آنها در امنیت رایانه ارزیابی شود. به عنوان مثال ، تنوع طراحی و فناوری احتمالاً آسیب پذیریهای رایج در بین سیستمهای ایمنی یا کنترل اصلی را کاهش می دهد. با این حال ، ممکن است آسیب پذیری هایی را که منحصر برای هر سیستم هستند اضافه کند.

2.5. Guidance contained in this publication applies to all I&C systems associated with a nuclear facility unless otherwise noted.

.2.5راهنمایی های موجود در این کتاب برای کلیه سیستم های ابزار دقیق و کنترل مرتبط با تأسیسات هسته ای اعمال می شود ، مگر اینکه مواردی دیگر ذکر شده باشد.

COMPUTER SECURITY OF I&C SYSTEMS

امنیت کامپیوتر سیستم های ابزار دقیق و کنترل

2.6. Paragraph 2.2 of Ref. [2] states that:

.2.6بند 2.2 از Ref. [2] بیان می کند:

"The State's *physical protection regime*[8] should seek to achieve these objectives through:

Prevention of a *malicious act* by means of deterrence and by protection of sensitive information;

Management of an attempted *malicious act* or a malicious act by an integrated system of *detection*, delay and response;

Mitigation of the consequences of a *malicious act*."

[8] Historically, the term 'physical protection' has been used to describe what is now known as the nuclear security of nuclear material and nuclear facilities.

"رژیم حفاظت فیزیکی دولت باید به دنبال دستیابی به این اهداف از طریق:

جلوگیری از یک عمل مخرب از طریق بازدارندگی و حفاظت از اطلاعات حساس.

مدیریت یک اقدام مخرب یا یک عمل مخرب توسط یک سیستم یکپارچه تشخیص ، تأخیر و پاسخ.

کاهش عواقب یک عمل مخرب" .

2.7. Examples of how prevention, management and mitigation can be applied to computer security of I&C systems include:Prevention: Installing fail-secure devices that block unauthorized data communications to reduce the potential for a network based cyber attack that would adversely affect the I&C system.

Management, including detection, delay and response: Through the inspection of system event log files, the operator may be able to detect precursors and initiate protective actions prior to the commencement of a malicious act that could adversely affect the safety or security of a facility.

Mitigation and recovery: If an I&C system is discovered to be infected with malware, once the malware's propagation has been stopped, the operator would determine whether compensatory control measures (e.g. updated antivirus signatures, installation or enhancement of intrusion prevention or detection systems or both) are needed to prevent re-infection, conduct a system rebuild, verify the effectiveness of the compensatory control measures, restore the system and place it back into to service, after performing detailed safety analysis and system integrity verification activities, if necessary.

2.7نمونه هایی از چگونگی استفاده از پیشگیری ، مدیریت و کاهش اثرات، می تواند در امنیت رایانه ای سیستم های ابزار دقیق و کنترل بکار رود عبارتند از:

پیشگیری:

نصب دستگاه های دارای امنیت در مقابل خرابی، که ارتباطات غیرمجاز را مسدود می کند تا پتانسیل حمله سایبری مبتنی بر شبکه که میتواند بر سیستم ابزار دقیق و کنترل تأثیر منفی بگذارد را کاهش دهد.

مدیریت ، از جمله تشخیص ، تأخیر و پاسخ: از طریق بازرسی وقایع ثبت شده در سیستم، اپراتور قادر به شناسایی و اقدام محافظتی پیش از شروع یک عمل مخرب که امکان تاثیر بر ایمنی یا امنیت یک تأسیسات را دارد ، میشود.

مهار و بازیابی: اگر مشخص شود یک سیستم ابزار دقیق و کنترل آلوده به بدافزار است، پس از متوقف شدن انتشار بدافزار، اپراتور تعیین می کند که آیا نیاز به اقدامات کنترل جبرانی (به عنوان مثال به روز رسانی ضد ویروس، نصب یا تقویت سیستم های پیشگیری از نفوذ یا تشخیص یا هر دو) برای ممانعت از آلوده شدن مجدد وجود دارد. سپس سیستم را مجددا ساخته و موثر بودن اقدامات جبرانی را بررسی کرده و بعد از آنالیز ایمنی و بررسی یکپارچه بودن سیستم آن را مجددا به خدمت میگیرد.

2.8. Protection of I&C systems against compromise is sometimes based upon the presumption that a single preventive measure is sufficient, such as the isolation of the systems from other networks. However, such a presumption is likely to result in insufficient application of management and mitigation measures so that failure of this single computer security measure might result in the compromise of the protected system.

2.8 محافظت از سیستم های ابزار دقیق و کنترل در برابر دستکاری ، گاه بر این فرض استوار است که یک اقدام پیشگیرانه، مانند جداسازی سیستم ها از شبکه های دیگر ، کافی است. با این حال ، چنین پیش فرضی به احتمال زیاد منجر به استفاده ناکافی از اقدامات مدیریتی و مهاری می شود و در نتیجه عدم موفقیت این تک اقدام امنیت رایانه منجر به دستکاری سیستم محافظت شده می شود.

2.9. Many different approaches, methods, techniques, standards and guidelines for computer security have been developed for general ICT systems. Some of these are not directly applicable to I&C systems at nuclear facilities, which have specific computer security needs that are not shared with ICT systems.

2.9 رویکردها ، روشها ، تکنیکها ، استانداردها و دستورالعمل های مختلفی در امنیت رایانه برای سیستم های اطلاعاتی عمومی ارائه شده است. برخی از این موارد به طور مستقیم برای سیستم های ابزار دقیق و کنترل در تأسیسات هسته ای کاربرد ندارند. تاسیسات هسته ای نیازهای امنیت رایانه خاصی دارند که با سیستم های فناوری اطلاعات و ارتباطات(ICT) مشترک نیستند.

2.10. Nevertheless, since computer security for I&C systems cannot be fully separated from computer security for ICT systems, operators and regulators should develop computer security policies, requirements, measures and practices that consider I&C systems and ICT systems in an integrated way.

2.10 با این وجود ، از آنجا که امنیت رایانه برای سیستم های ابزار دقیق و کنترل نمی تواند کاملاً از امنیت رایانه برای سیستم های فناوری اطلاعات و ارتباطات جدا شود، اپراتورها و تنظیم کننده گان مقررات باید سیاست ها ، الزامات ، اقدامات و شیوه های امنیت رایانه را به گونه ای تنظیم کنند که سیستم های ابزار دقیق و کنترل و سیستم های فناوری اطلاعات و ارتباطات را به صورت یکپارچه در نظر بگیرد.

2.11. Many I&C systems have a life cycle of decades, including periods during which vendor support may be unavailable or inadequate to meet the computer security requirements[9] for the systems. This includes support given by the original vendor and by associated third parties. For example, over time, antivirus programs may not provide sufficient protection against the exploitation of vulnerabilities in I&C systems, owing to loss of hardware or software compatibility or failure to continue providing signature updates.

2.11بسیاری از سیستم های های ابزار دقیق و کنترل دارای چرخه عمر چندین دهه هستند ، از جمله زمانی که در طی آن پشتیبانی فروشنده برای برآورده کردن الزامات امنیت رایانه برای این سیستم ها در دسترس نیست یا ناکافی است. این شامل پشتیبانی ارائه شده توسط فروشنده اصلی و اشخاص ثالث مرتبط است. به عنوان مثال، با گذشت زمان، برنامه های آنتی ویروس ممکن است به دلیل از بین رفتن سخت افزار یا سازگاری نرم افزار یا عدم تداوم ارائه به روزرسانی ها، محافظت کافی در برابر سوء استفاده از آسیب پذیری در سیستم های های ابزار دقیق و کنترل را نداشته باشند.

2.12. In most applications, I&C systems operate in real time, and I&C system actions are performed within strict time intervals. Examples of such I&C system actions at nuclear facilities include control of normal operations, protective actions, limitation actions and alarm signalling to operators. Computer security measures should not impede, prevent or delay the performance of necessary operational or safety actions. Computer security measures for modern I&C systems can be used to prevent, detect, delay and respond to malicious acts and mitigate their

consequences, but care needs to be taken to ensure that the response measures do not impede accredited safety functions or place the system outside of its design basis10.

2.12در اکثر کاربردها ، سیستم های های ابزار دقیق و کنترل در زمان واقعی کار می کنند ، و اقدامات سیستم ابزار دقیق و کنترل در فواصل زمانی دقیق انجام می شود. نمونه هایی از این قبیل اقدامات سیستم ابزار دقیق و کنترل در تاسیسات هسته ای شامل کنترل بهره برداری عادی ، اقدامات محافظتی ، اقدامات محدود کننده و سیگنال هشدار برای اپراتورها است. اقدامات امنیت رایانه نباید بازداری ، مانع یا تأخیر در انجام اقدامات عملیاتی یا ایمنی لازم شود. از اقدامات امنیت رایانه برای سیستم های ابزار دقیق و کنترل مدرن می توان برای جلوگیری، کشف، تأخیر و پاسخ به اقدامات مخرب و کاهش پیامدهای آنها استفاده کرد ، اما باید دقت لازم را انجام داد تا اطمینان حاصل شود که این اقدامات پاسخ، مانع عملکردهای معتبر ایمنی نشده و یا سیستم را خارج از ناحیه طراحی شده قرار ندهد.

2.13. Computer security measures that are retrospectively applied or poorly implemented may introduce additional complexity into the I&C system design, which may result in an increased likelihood of I&C system failure or mal-operation.

2.13 اقدامات امنیت رایانه که به صورت گذشته نگر مورد استفاده قرار گرفته یا ضعیف اجرا شده اند ، ممکن است پیچیدگی دیگری را در طراحی سیستم ابزار دقیق و کنترل ایجاد کند، که ممکن است منجر به افزایش احتمال خطا و خرابی سیستم شود.

2.14. Essential Element 9 of the Nuclear Security Fundamentals [8] identifies the use of risk informed approaches to allocate resources and in the conduct of nuclear security related activities. A design developed using a risk-informed approach to account for security considerations from the beginning of the design process may be simpler and more robust owing to the integration of the security features, the elimination of unnecessary functionality (e.g. remote access) or to system hardening.

2.14 اصل اساسی 9 مبانی امنیت هسته ای [8] استفاده از رویکردهای آگاهانه در مورد ریسک برای تخصیص منابع و انجام فعالیتهای مربوط به امنیت هسته ای را مشخص می کند. طرحی که با استفاده از یک رویکرد آگاهانه از ریسک ایجاد شده است و ملاحظات امنیتی را از ابتدای فرآیند طراحی در نظر میگیرد ، ممکن است به دلیل ادغام ویژگی های امنیتی ، حذف ویژگی های غیر ضروری (به عنوان مثال دسترسی از راه دور) یا سخت شدن سیستم، ساده تر و مقاوم تر باشد.

COMPUTER SECURITY MEASURES

تدابیر امنیت رایانه

2.15. Computer security measures are used to prevent, detect, delay and respond to malicious acts as well as to mitigate the consequences of such acts. Computer security measures are also used to ensure that non-malicious acts do not degrade security and increase the vulnerability of computer based systems to malicious acts.

2.15 از تدابیر امنیت رایانه برای ممانعت، کشف، تأخیر و پاسخ به اقدامات مخرب و همچنین برای کاهش پیامدهای چنین اقداماتی استفاده می شود. همچنین تدابیر امنیت رایانه برای اطمینان از اینکه اقدامات غیرمخرب امنیت را تضعیف نمی کنند و آسیب پذیری سیستم های مبتنی بر رایانه در برابر اقدامات مخرب را کاهش می دهند، استفاده می شود.

2.16. Computer security measures that address vulnerabilities in the system or provide protective layers of defence can be assigned to one of three categories: technical control measures, physical control measures or administrative control measures. All three categories should be considered and an appropriate combination selected when developing integrated computer security for I&C systems.

2.16 تدابیر امنیت رایانه که آسیب پذیری های موجود در سیستم را پاسخ میدهند، و یا لایه های محافظتی دفاعی را ارائه می دهند، می تواند به یکی از این سه دسته تعلق گیرد: تدابیر کنترل فنی ، تدابیر نترل فیزیکی یا تدابیر کنترل مدیریتی. هر سه دسته باید در نظر گرفته شوند و در هنگام توسعه امنیت رایانه یکپارچه برای سیستم های ابزار دقیق و کنترل ، یک ترکیب مناسب انتخاب شود.

2.17. Technical control measures are hardware and/or software used to prevent, detect, mitigate the consequences of and recover from an intrusion or other malicious act. The ability of technical control measures to provide continuous and automatic protective actions should be considered when evaluating their effectiveness compared with physical or administrative control measures.

2.17 تدابیر کنترلی فنی سخت افزاری و/ یا نرم افزاری است که برای جلوگیری ، کشف ، کاهش عواقب و بازیابی از یک نفوذ یا سایر اقدامات مخرب استفاده می شود. توانایی تدابیر کنترلی فنی در ارائه اقدامات محافظتی مداوم و خودکار باید هنگام ارزیابی اثربخشی آنها در مقایسه با اقدامات کنترل فیزیکی یا مدیریتی در نظر گرفته شود.

2.18. Physical control measures are physical barriers that protect instruments, computer based systems and supporting assets from physical damage and unauthorized physical access. Physical control measures include locks, physical encasements, tamper indicating devices, isolation rooms, gates and guards.

2.18 تدابیر کنترل فیزیکی، موانع فیزیکی است که از ابزارها ، سیستم های مبتنی بر رایانه و حمایت از دارایی در برابر آسیب های فیزیکی و دسترسی غیرمجاز فیزیکی محافظت می کند. تدابیر کنترل فیزیکی شامل قفل ها ، محفظه های فیزیکی، تجهیزات نشانگر دستکاری ، اتاق های جداسازی ، دروازه ها و نگهبانان است.

2.19. Administrative control measures are policies, procedures and practices designed to protect computer based systems by providing instructions for actions of employees and third party personnel. Administrative control measures specify permitted, necessary and forbidden actions

by employees and third party personnel. Administrative control measures for nuclear facilities include operational and management control measures.

2.19 تدابیرکنترل مدیریتی سیاست ها ، رویه ها و روش هایی است که برای محافظت از سیستم های رایانه ای با ارائه دستورالعمل برای عملکرد کارمندان واشخاص ثالث طراحی شده است. اقدامات کنترل مدیریتی اقدامات مجاز، لازم و ممنوع کارمندان و اشخاص ثالث را مشخص می کند. تدابیر کنترل مدیریتی برای تاسیسات هسته ای شامل تدابیر عملیاتی و تدابیرکنترلی مدیریت است.

APPLICATION OF A GRADED APPROACH

استفاده از رویکرد درجه بندی شده

2.20. The operator should impose computer security requirements based on a risk informed graded approach that takes into account the following:The importance of I&C system functions for both safety (i.e. safety classification) and security;

The identified and assessed threats to the facility;

The attractiveness of the I&C system to potential adversaries;

The vulnerabilities of the I&C system;

The operating environment;

The potential consequences that could either directly or indirectly result from a compromise of the system.

2.20اپراتور باید الزامات امنیت رایانه را مبتنی بر رویکرد درجه بندی شده با آگاهی از ریسک اعمال کند و موارد زیر را در نظر گیرد: اهمیت عملکرد سیستم ابزار دقیق و کنترل در ایمنی (یعنی طبقه بندی ایمنی) و امنیت.

تهدیدات شناسایی شده و ارزیابی شده برای تأسیسات.

جذابیت سیستم ابزار دقیق و کنترل برای متخاصمان بالقوه.

آسیب پذیری های سیستم ابزار دقیق و کنترل ؛

محیط عملیاتی؛

عواقب احتمالی که می تواند مستقیم یا غیرمستقیم ناشی از دستکاری سیستم باشد.

Such an approach could be based on the results of a computer security risk assessment.

چنین رویکردی می تواند مبتنی بر نتایج ارزیابی ریسک امنیت رایانه باشد.

2.21. In a graded approach, computer security requirements are defined proportionately to the potential consequences of an attack. The potential consequences of a compromise on I&C system function are, arranged in the order of worst to best cases:

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. it is fault tolerant).

2.21.در یک رویکرد درجه بندی شده ، الزامات امنیت رایانه متناسب با پیامدهای احتمالی یک حمله تعریف می شود. عواقب احتمالی دستکاری بر عملکرد سیستم ابزار دقیق و کنترل به ترتیب از بدترین تا بهترین به صورت زیر است:

عملکرد نامشخص است. اثرات دستکاری منجر به تغییر غیرقابل نظارت در طراحی یا عملکرد سیستم می شود.

عملکرد دارای رفتارهای غیر منتظره ای است یا عملکردهایی که برای اپراتور قابل مشاهده است.

عملکرد عمل نمیکند

عملکرد همان است که انتظار می رود، به این معنی که دستکاری بر عملکرد سیستم تأثیر منفی نمی گذارد (به عنوان مثال سیستم مقاوم در برابر خطا است)

2.22. Computer security levels should be applied as described in this publication to I&C systems to allow for the implementation of a graded approach to computer security.

2.22 سطوح امنیت رایانه باید مطابق آنچه در این کتاب شرح داده شده است بر روی سیستم های ابزار دقیق و کنترل اعمال شود تا امکان استفاده از رویکرد درجه بندی شده برای امنیت رایانه فراهم شود.

2.23. An example of an implementation of a graded approach using security levels11 is provided in Ref. [3]. Conversely, an example of an implementation of a graded approach for safety is provided in Ref. [9].

2.23 نمونه ای از اجرای یک روش درجه بندی شده با استفاده از سطوح امنیتی در[3]Ref ارائه شده است. در مقابل ،نمونه ای از اجرای یک روش درجه بندی شده برای ایمنی در[9]Ref ارائه شده است.

COMPUTER SECURITY LEVELS

سطوح امنیت رایانه

2.24. Computer security levels and safety classes are distinct but related concepts. The safety classification of an item important to safety is based upon the relevance to safety of its function as well as the potential consequences of its failure.

2.24 سطوح امنیت رایانه و کلاسهای ایمنی مفاهیم مجزا اما مرتبط هستند. طبقه بندی ایمنی یک وسیله از نظر ایمنی مهم است و بر اساس ارتباط با ایمنی عملکرد آن و همچنین پیامدهای احتمالی عدم موفقیت آن استوار است.

2.25. Each I&C system function associated with a facility is generally assigned a computer security level to indicate the degree of computer security protection it needs. Each level will need different sets of computer security measures to satisfy relevant computer security requirements. The security levels are often defined based on an organization’s security objectives.
Reference [10] provides further information on the implementation of security levels and zones.

2.25 به طور کلی به هر عملکرد سیستم ابزار دقیق و کنترل در تأسیسات ، یک سطح امنیت رایانه تعلق میگیرد تا میزان امنیت رایانه مورد نیاز را مشخص کند. برای برآورده کردن الزامات مربوط به امنیت رایانه ، هر سطح به مجموعه های مختلفی از تدابیر امنیت رایانه نیاز دارد. سطح امنیتی اغلب بر اساس اهداف امنیتی سازمان تعریف می شود. مرجع [10] اطلاعات بیشتری در مورد اجرای سطوح و مناطق امنیتی ارائه می دهد.

2.26. The subsystems and components of I&C systems whose mal-operation could affect nuclear safety (including accident mitigation), nuclear security and nuclear material accounting and control are identified and assigned to security levels according to their contribution to I&C system function.

2.26 زیر سیستم ها و اجزاء سیستم های ابزار دقیق و کنترل که سوء عملکرد آنها می تواند بر ایمنی هسته ای (از جمله مهار حادثه) ، امنیت هسته ای و حسابداری و کنترل مواد هسته ای تأثیر بگذارد، با توجه به سهم آنها در عملکرد سیستم ابزار دقیق و کنترل، سطوح امنیتی مشخص قرار میگیرند.

2.27. The operator assigns a security level to an I&C system, subsystem or component based on the potential consequences of its failure or mal-operation, including mal-operation in a way that differs from its design or conceivable failure modes that would be identified in a facility safety analysis. The computer security level assigned to an I&C system, subsystem or component is specific to that system, subsystem or component, and is independent of its environment.

2.27 اپراتور سطح امنیتی به یک سیستم ابزار دقیق و کنترل ، زیر سیستم یا اجزاء آن را بر اساس عواقب احتمالی عدم عملکرد موفق یا خراب بودن آن ، از جمله عملکرد نادرست به گونه‌ای که با طراحی یا حالتهای خطا که از قبل در تجزیه و تحلیل ایمنی متصور بوده متفاوت است، تخصیص میدهد. سطح امنیت رایانه اختصاص داده شده به یک سیستم ابزار دقیق و کنترل، زیر سیستم یا اجزاء آن، مختص خودش است و از محیط آن مستقل است.

COMPUTER SECURITY ZONES

نواحی امنیت رایانه

2.28. 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.

2.28مفهوم نواحی امنیتی شامل گروه بندی منطقی و یا فیزیکی سیستم های مبتنی بر رایانه است که به دلیل ویژگی های ذاتی سیستم ها یا اتصال آنها به سیستم های دیگر ، نیازهای مشترک امنیت رایانه دارند. تمام سیستمهای مستقر در یک منطقه واحد در همان سطح امنیتی محافظت می شوند ، یعنی که به عملکرد سیستم ابزار دقیق و کنترل با بالاترین سطح امنیتی در ناحیه اختصاص داده می شود. گروه بندی سیستم های ابزار دقیق و کنترل در نواحی امنیتی ممکن است کاربرد و مدیریت تدابیر امنیت رایانه ای را ساده تر کند.

2.29. Considerations for implementation of security zones should fulfil the following criteria:

Systems belonging to the same zone have similar needs for computer security measures.

Systems belonging to the same zone form a trusted area for internal communications between those systems (i.e. internal trusted zone area).

Each zone comprises systems that have the same or comparable importance for the security and safety of the facility, or belong to an internal trusted zone area.

System safety architecture requirements (e.g. redundancy, diversity, geographic and electrical separation, single failure criterion) are maintained.

Technical control measures are implemented at zone boundaries to restrict data flow and communication between systems located within different zones (e.g. remote location) or assigned to different security levels.

Removable media, mobile devices and other temporary equipment that needs logical or physical access to a system are used only within a single zone or a specified set of zones.

Zones may be partitioned into sub-zones to improve the configuration.

2.29ملاحظات مربوط به اجرای نواحی امنیتی باید دارای معیارهای زیر باشد:

سیستم های متعلق به هر ناحیه نیازهای مشابهی برای تدابیر امنیت رایانه ای دارند.

سیستم های متعلق به هر ناحیه یک محیط قابل اعتماد برای ارتباطات داخلی بین آن سیستم ها (یعنی ناحیه مورد اعتماد داخلی) تشکیل می دهند.

هر ناحیه شامل سیستمهایی است که برای امنیت و ایمنی تأسیسات از اهمیت یکسانی برخوردار هستند یا به یک ناحیه قابل اعتماد داخلی تعلق دارند.

الزامات معماری ایمنی سیستم (به عنوان مثال افزونگی ، تنوع ، جدایی جغرافیایی و الکتریکی ، معیار خرابی منفرد) حفظ می شوند.

تدابیر کنترلی فنی در مرزهای ناحیه انجام می شود تا جریان داده و ارتباط بین سیستم های واقع در نواحی مختلف (برای مثال سایر مکانها) محدود شود یا به سطوح مختلف امنیتی اختصاص یابد.

رسانه های جدا شونده ، دستگاه های قابل حمل و سایر تجهیزات موقتی که نیاز به دسترسی منطقی یا فیزیکی به یک سیستم دارند فقط در یک ناحیه واحد یا مجموعه مشخصی از نواحی مورد استفاده قرار می گیرند.

برای بهبود پیکربندی ، نواحی ممکن است به زیر ناحیه تقسیم شوند.

2.30. When security zones are used in a facility, some I&C systems or components could be assigned to a zone assigned a more stringent security level than their own inherent security level. For example, a communication device that performs only lower level safety or security functions may be assigned the same security level as the reactor protective system, if it is located within the reactor protective system security zone. This assignment is due to the potential for malicious use of the device to compromise the reactor protective system components, which are highly important for safety. Furthermore, the use of the reactor protective system security zone allows for the creation of an internal trusted zone area, thereby ensuring that additional computer security measures will not need to be implemented between the reactor protective system components and the communication device.

2.30 هنگامی که از نواحی امنیتی در یک موسسه استفاده می شود ، برخی از سیستم های ابزار دقیق و کنترل یا اجزاء می توانند به مناطقی اختصاص داده شوند که سطح امنیتی بالاتری نسبت به سطح امنیتی ذاتی خود داشته باشند. به عنوان مثال ، یک وسیله ارتباطی که فقط عملکردهای ایمنی یا امنیتی سطح پایین تری را انجام می دهد ، ممکن است در صورتی که در منطقه امنیتی سیستم محافظ راکتور قرار داشته باشد ، همان سطح امنیتی مانند سیستم محافظ راکتور را اختصاص دهد. این اختصاص به دلیل امکان استفاده مخرب از دستگاه برای به خطر انداختن اجزای سیستم محافظ راکتور است که از نظر ایمنی بسیار مهم هستند. علاوه بر این ، استفاده از ناحیه امنیتی سیستم حفاظتی راکتور امکان ایجاد ناحیه مورد اعتماد داخلی را فراهم می کند ، در نتیجه اطمینان حاصل می شود که تدابیر اضافی امنیت رایانه نیازی به اجرای بین اجزای سیستم محافظ راکتور و وسیله ارتباطی نخواهد داشت.