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

CONTENTS

نظارت بر امنیت

مراجع

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 ([INFCIRC / 225 / Revision 5) [2] ، 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 acts[2] 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 Ref مشخص 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 new4 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].

2.3طراحی 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 basis[10].

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 levels[11] 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.

3. RISK INFORMED APPROACH TO COMPUTER SECURITY FOR I&C SYSTEMS

3. رویکرد با در نظرگرفتن ریسک در امنیت رایانه برای سیستم های ابزار دقیق و کنترل

3.1. A risk informed approach to computer security for I&C systems may use risk assessments to identify a facility's vulnerabilities to cyber attack related to these systems and determine the consequences that could result from the successful exploitation of these vulnerabilities. Computer security measures can then be assigned based on the results of the risk assessments.

3.1یک رویکرد با در نظر گرفتن ریسک در مورد امنیت رایانه برای سیستم های ابزار دقیق و کنترل، از ارزیابی ریسک برای شناسایی آسیب پذیری یک مرکز در برابر حمله سایبری مربوط به این سیستم ها و تعیین عواقب ناشی از سوء استفاده موفقیت آمیز از این آسیب پذیری ها استفاده می کند. سپس تدابیر امنیت رایانه بر اساس نتایج ارزیابی ریسک مشخص میشوند.

3.2. Because I&C systems are often essential for facility safety, an understanding of nuclear safety can assist in assessing risk, developing computer security measures for the I&C system, assessing potential conflicts between safety and security, and considering how such conflicts could be resolved. For example, adversaries could sabotage a facility through a cyber attack on a facility's I&C systems, resulting in potential safety and security consequences. Such attacks might cause failures of I&C systems or might cause I&C systems to operate in ways that differ from their intended behaviour or their analysed failure modes. Malicious acts may affect a single I&C system or multiple I&C systems. For example, malicious acts have the potential to bypass or cause simultaneous failure of multiple levels of safety defence in depth12. Malicious acts may also combine cyber attacks with physical attack elements.

3.2از آنجا که سیستم های ابزار دقیق و کنترل اغلب برای ایمنی تأسیسات ضروری هستند ، درک ایمنی هسته ای می تواند در ارزیابی ریسک ، تدوین تدابیر امنیت رایانه برای سیستم ابزار دقیق و کنترل ، ارزیابی تعارضات احتمالی بین ایمنی و امنیت و بررسی چگونگی حل اینگونه تعارضات کمک میکند. به عنوان مثال ، افراد متخاصم می توانند از طریق حمله سایبری به سیستم های ابزار دقیق و کنترل یک مرکز ، یک مرکز را خراب کنند و در نتیجه عواقب ایمنی و امنیتی ایجاد کنند. چنین حملاتی ممکن است باعث خرابی سیستم های ابزار دقیق و کنترل شود و یا ممکن است باعث شود سیستم های ابزار دقیق و کنترل به طریقی عمل کنند که با رفتار طبیعی مورد نظر یا حالت های خطای تحلیل شده آنها متفاوت باشد. اقدامات مخرب ممکن است بر یک سیستم منفرد و یا چندین سیستم ابزار دقیق و کنترل اثر بگذارد. به عنوان مثال ، اقدامات مخرب امکان حذف و یا ایجاد خطای

همزمان در سطوح مختلف دفاع ایمن در عمق را دارند. اقدامات مخرب همچنین ممکن است حملات سایبری را با حمله فیزیکی ترکیب کند.

3.3. Inadequate computer security or a compromised I&C system may cause the safety of a facility to be jeopardized. For example, if an I&C system is compromised, an adversary might obtain data that provide the critical information needed to plan an attack or modify data that facilitate sabotage of facility systems or unauthorized removal of nuclear materials. Alternatively, a cyber attack resulting in sabotage might initiate an accident or degrade the performance of a safety function. Such an attack might also lead to a loss of system availability.

3.3امنیت نامناسب رایانه یا سیستم ابزار دقیق و کنترل دستکاری شده ممکن است باعث شود ایمنی یک مرکز به خطر بیفتد. به عنوان مثال ، اگر یک سیستم ابزار دقیق و کنترل دستکاری شود ، ممکن است یک متخاصم داده هایی را بدست آورد که اطلاعات مهم لازم برای برنامه ریزی حمله یا تغییر داده هایی را که باعث کمک به خرابکاری یا برداشت غیرمجاز مواد هسته ای می شود ، فراهم کند. از طرف دیگر ، حمله سایبری که منجر به خرابکاری می شود ممکن است باعث بروز یک حادثه شود یا عملکرد یک سیستم ایمنی را تضعیف کند. چنین حمله ای ممکن است به از دست رفتن در دسترس بودن سیستم نیز منجر شود.

3.4. Cyber attacks on I&C systems might also lead to consequences that enable the unauthorized removal of nuclear material from a facility. I&C systems fulfilling physical protection or nuclear material accounting and control functions may be affected by cyber attacks, which could place a facility in a condition that has not been considered in the site security plan. A malicious act could also combine a cyber attack on these systems with physical attack elements with the objective of the unauthorized removal of nuclear material.

3.4حملات سایبری به سیستم های ابزار دقیق و کنترل همچنین ممکن است منجر به پیامدهایی شود که برداشت غیرمجاز مواد هسته ای از یک مرکز را ممکن می سازد. سیستمهای ابزار دقیق و کنترل که عملکردهای حافظت فیزیکی یا حسابرسی و کنترل مواد هسته ای را انجام می دهند ممکن است تحت تأثیر حملات سایبری قرار بگیرند، که می تواند یک مرکز را در شرایطی قرار دهد که در برنامه امنیتی سایت در نظر گرفته نشده باشد. یک اقدام مخرب همچنین می تواند حمله سایبری به این سیستم ها را با حمله فیزیکی به منظور برداشت غیرمجاز مواد هسته ای ترکیب کند.

3.5. Therefore, computer security measures for I&C systems need to address both cyber attacks that directly cause sabotage and those that collect information that could facilitate sabotage of the nuclear facility or unauthorized removal of nuclear material.

3.5.بنابراین ، تدابیر امنیت رایانه برای سیستم های ابزار دقیق و کنترل باید حملات سایبری را که مستقیماً باعث خرابکاری می شوند و کسانی که اطلاعاتی را جمع آوری می کنند که می تواند خرابکاری در تاسیسات هسته ای یا برداشت غیرمجاز مواد هسته ای را تسهیل کند ، را پوشش دهد .

INTERFACE WITH FACILITY COMPUTER SECURITY RISK MANAGEMENT

واسطه با مدیریت ریسک امنیت رایانه موسسه

3.6. The operator should have a facility computer security risk management (CSRM) process to implement computer security to protect the functions performed by I&C systems. This process is used to identify the facility's vulnerabilities[13] to cyber attack and to determine the consequence of successful compromise of one or more functions performed by I&C systems (which may include exploitation of vulnerabilities).

3.6.اپراتور برای اجرای امنیت رایانه برای محافظت از عملکردهای انجام شده توسط سیستمهای ابزار دقیق و کنترل، باید فرآینده مدیریت ریسک امنیت رایانه (computer security risk management CSRM) داشته باشد. این فرایند برای شناسایی آسیب پذیری های تأسیسات در برابر حمله سایبری و تعیین عواقب دستکاری موفقیت آمیز یک یا چند عملکرد انجام شده توسط سیستم های ابزار دقیق و کنترل (که ممکن است شامل سوء استفاده از آسیب پذیری ها باشد) استفاده می شود.

3.7. The outputs of the facility CSRM processes should include an identification of facility functions performed by I&C systems including supporting and complementary systems that, if compromised, could adversely affect safety, security of nuclear material or accident management. The facility safety analysis may be used as an input for the facility CSRM, but the safety analysis alone is not sufficient as it does not address all mal-operations. Mal-operations caused by cyber attacks might place the facility in conditions that have not been considered by the safety analysis.

3.7خروجی فرآیندهای CSRM در تاسیسات باید شامل شناسایی توابع انجام شده توسط سیستم های ابزار دقیق و کنترل از جمله سیستم های پشتیبانی و مکمل باشد که در صورت به خطر افتادن می تواند بر ایمنی ، امنیت مواد هسته ای یا مدیریت حوادث تأثیر منفی بگذارد. تجزیه و تحلیل ایمنی تأسیسات ممکن است به عنوان ورودی برای CSRM تأسیسات مورد استفاده قرار گیرد ، اما تجزیه و تحلیل ایمنی به تنهایی کافی نیست زیرا به کلیه سوء عملکردها نمی پردازد. سوء عملکرد ناشی از حملات سایبری ممکن است موسسه را در شرایطی قرار دهد که با آنالیز ایمنی در نظر گرفته نشده باشد.

3.8. The outputs of the facility CSRM processes should identify the potential consequences related to nuclear safety, nuclear security and nuclear material accounting and control resulting from system compromise due to a cyber attack on the I&C systems. When analysing the consequences of an attack on an I&C system, the possibility should be considered that the attack might be a component of a larger attack affecting multiple I&C systems or a combined cyber and physical attack. This analysis could then be used to assign the appropriate security levels to individual I&C systems and components based upon the potential consequences of their failure or mal-operation.

3.8خروجی فرآیندهای CSRM در تأسیسات باید پیامدهای احتمالی مربوط به ایمنی هسته ای ، امنیت هسته ای و حسابداری مواد هسته ای و کنترل ناشی از دستکاری سیستم به دلیل حمله سایبری به سیستم های ابزار دقیق و کنترل را مشخص کند.
هنگام تجزیه و تحلیل عواقب حمله به سیستم ابزار دقیق و کنترل، باید این احتمال را در نظر گرفت که این حمله می تواند جزئی

از حمله بزرگتر به چندین سیستم و یا یک حمله سایبری و فیزیکی ترکیبی میباشد. سپس این تجزیه و تحلیل می تواند برای اختصاص سطح امنیتی مناسب به سیستم ها و اجزای ابزار دقیق و کنترل بر اساس پیامدهای احتمالی خطا یا سوء عملکرد آنها مورد استفاده قرار گیرد.

3.9. The security levels assigned to the I&C systems may be associated with a hierarchical list of potential safety or security consequences. For example, plant states, sabotage consequences, nuclear material categorization hierarchies or a combination of these might be used, as in the examples in paras 3.10–3.13 and 3.15.

3.9سطح امنیتی اختصاص داده شده به سیستمهای ابزار دقیق و کنترل ممکن است با یک لیست سلسله مراتبی از پیامدهای احتمالی ایمنی یا امنیتی همراه باشد. مثلاً وضعیت نیروگاه ، عواقب خرابکاری ،طبقه بندی مواد هسته ای یا ترکیبی از این موارد ممکن است مورد استفاده قرار گیرد ، همانطور که در مثالهای موجود در بندهای 3.10-3.13 و 3.15 اشاره شده است.

3.10. For reasons of safety, plant states could be used to denote the potential safety consequences of a cyber attack on I&C systems. For example, plant states could be associated with security levels for I&C systems as follows, ordered from the situation with the lowest to the situation with the highest consequence:

(1) Normal operation: A cyber attack on I&C systems cannot cause facility operation outside limits and conditions specified for normal operation.

(2) Anticipated operational occurrence: A cyber attack on I&C systems may cause the plant state to deviate from normal operation in a way that is anticipated to occur, but which in view of appropriate design provisions does not cause any significant damage to items important to safety or lead to accident conditions.

(3) Design basis accident[14]: A cyber attack on I&C systems may cause accident conditions that remain within the facility design basis and for which the damage to the nuclear material (or other radioactive material) and the release of radioactive material are kept within authorized limits.

(4) Design extension conditions: A cyber attack on I&C systems may cause accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions could include severe accident conditions.

3.10 به دلایل ایمنی ، از وضعیت نیروگاه می توان برای عواقب ایمنی بالقوه حمله سایبری به سیستم های ابزار دقیق و کنترل استفاده کرد. به عنوان مثال ، حالت های نیروگاه می توانند با سطح امنیتی سیستم های ابزار دقیق و کنترل به شرح زیر همراه باشند ، که از کمترین تا بالاترین عواقب مرتب شده است:

(1)عملکرد عادی: حمله سایبری به سیستم های ابزار دقیق و کنترل نمی تواند باعث ایجاد عملکرد در خارج از محدوده ها و شرایطی باشد که برای عملکرد عادی مشخص شده است.

(2)وقوع عملیاتی پیش بینی شده: حمله سایبری به سیستم های ابزار دقیق و کنترل ممکن است باعث شود وضعیت نیروگاه از عملکرد طبیعی به طریقی که پیش بینی می شود منحرف شود ، اما با توجه به طراحی مناسب ، خسارت قابل توجهی به اجزا مهم از نظر ایمنی وارد نکرده و یا منجر به حادثه نمیشود.

(3) حوادث مبنای طراحی: حمله سایبری به سیستم های ابزار دقیق و کنترل ممکن است باعث ایجاد شرایط حادثه ای شود که در قالب طرحی شده برای تأسیسات باقی می ماند و صدمه به مواد هسته ای (یا سایر مواد رادیواکتیو) و انتشار مواد رادیواکتیو در محدوده مجاز نگهداری می شود.

(4) شرایط بسط طراحی: حمله سایبری به سیستم های ابزار دقیق و کنترل ممکن است باعث ایجاد شرایط حادثه شود که در طراحی در نظر گرفته نشده باشد ، اما در فرآیند طراحی تأسیسات مطابق با بهترین روش تخمین مورد بررسی قرار می گیرد به صورتی که انتشار مواد رادیو اکتیو در حد قابل قبول نگه داشته می شوند. شرایط توسعه طراحی می تواند شامل شرایط حادثه شدید باشد

3.11. The consequences of sabotage of functions performed by I&C systems could also be associated with security levels. Such an approach would involve the State defining the threshold for unacceptable radiological consequences (URC), as recommended in para. 3.44 of Ref. [2]. The definition of a threshold for URC may be based on quantitative or qualitative criteria, which may be expressed in terms of releases of radionuclides (e.g. a release exceeding some identified amount), doses (e.g. a release leading to a radiation dose exceeding some identified value to an individual located at some identified point, usually off-site) or facility conditions (e.g. sabotage that may result in significant core damage in a reactor). As stated in Ref. [11], paras 3.94 and 95: "targets for which sabotage could potentially result in a substantial radiological release significantly affecting the population and environment beyond the boundaries of the nuclear facility need the highest level of protection. Such a severe event is referred to…[in Ref. [2]] as having high radiological consequences.
"Therefore, the State should also define the threshold for high radiological consequences."

3.11 عواقب خرابکاری توابع انجام شده توسط سیستم های ابزار دقیق و کنترل همچنین می تواند با سطوح امنیتی در نظر گرفته شود. در چنین رویکردی دولت باید آستانه پیامدهای رادیولوژیکی غیرقابل قبول را تعیین کند(unacceptable radiological consequences (URC) ، همانطور که در بند 3.44 از Ref. [2] توصیه شده است. تعریف آستانه پیامدهای رادیولوژیکی غیرقابل قبول ممکن است براساس معیارهای کمی یا کیفی باشد ، که ممکن است با توجه به انتشار رادیونوکلئیدها (به عنوان مثال یک انتشار بیش از مقدار مشخص شده) ، دوزها (به عنوان مثال انتشار منجر به دوز تابش بیش از مقداری شناسایی شده به یک فرد واقع در یک نقطه مشخص شده ، معمولاً خارج از محل سایت) و یا شرایط تأسیسات (به عنوان مثال خرابکاری که ممکن است منجر به خسارت هسته قابل توجهی در راکتور شود) بیان میشود. همانطور که در[11]Ref گفته شده است، بندهای 3.94 و 95:
"اهدافی که خرابکاری ها برای آنها به طور بالقوه می تواند منجر به انتشار رادیولوژیکی قابل ملاحظه ای شود که به طور قابل توجهی بر جمعیت و محیط زیست فراتر از مرزهای تأسیسات هسته ای تأثیر می گذارد ، به بالاترین سطح حفاظت نیاز دارند.

چنین واقعه شدیدی در Ref[2] به عنوان عواقب رادیولوژیکی بالا تعریف شده است. "بنابراین ، دولت باید آستانه عواقب رادیولوژیکی بالا را نیز تعیین کند.

3.12. An example of a hierarchical list of potential consequences of sabotage is provided in Ref. [11] and summarized for I&C system functions as follows, ranked from the lowest to the highest consequences:

Radiological consequence below the URC threshold: Targets posing these low consequences need a correspondingly low level of protection.

URC can be graded into three categories ranked from the lowest to the highest consequences:

Consequence Level C: Sabotage that could result in doses to persons on-site that warrant urgent protective action to minimize on-site health effects.

Consequence Level B: Sabotage that could result in doses or contamination off-site that warrant urgent protective action to minimize off-site health effects (may also be considered high radiological consequences).

Consequence Level A: Sabotage that could give rise to severe deterministic health effects off-site (likely also to be considered high radiological consequences).

3.12 نمونه ای از لیست سلسله مراتبی از پیامدهای احتمالی خرابکاری در Ref[11] ارائه شده و برای توابع سیستم ابزار دقیق و کنترل به شرح زیر خلاصه شده است ، از پایین ترین تا بالاترین عواقب رتبه بندی شده است:

پیامد رادیولوژیکی زیر آستانه URC : اهداف ناشی از این پیامدهای کم به سطح حفاظت پایین نیاز دارند.

URC را می توان به سه دسته طبقه بندی کرد از پایین ترین تا بالاترین پیامدها:

پیامد سطح c: خرابکاری که منجر به دوز به افراد در محل می شود و نیاز به استفاده از اقدامات حافظتی فوری به منظور به حداقل رساندن اثرات سوء بر سلامتی افراد.

پیامد سطح b: خرابکاری که می تواند منجر به دوز یا آلودگی خارج از سایت شود و نیاز به استفاده از اقدامات حافظتی فوری به منظور به حداقل رساندن اثرات سوء بر سلامتی افراد خارج از سایت (ممکن است به عنوان پیامدهای رادیولوژیکی سطح بالا در نظر گرفته شود)

پیامد سطح a: خرابکاری که می تواند عوارض سلامتی شدید در خارج از سایت ایجاد کند (احتمالاً به عنوان پیامدهای رادیولوژیکی سطح بالا در نظر گرفته میشود)

3.13. Security levels could also be associated with the possibility of the unauthorized removal of nuclear material. The potential consequences of cyber attacks on I&C systems performing physical protection or nuclear material accounting and control functions could be associated with security levels on the basis of the category of material that could be subject to unauthorized removal. Table I of Ref. [2] provides the criteria for the categorization of nuclear material and further identifies recommendations for physical protection based on this categorization.

3.13 سطوح امنیتی می تواند با احتمال برداشت غیرمجاز مواد هسته ای تعریف شود. عواقب احتمالی حملات سایبری بر روی سیستم های ابزار دقیق و کنترل که وظیفه حفاظت فیزیکی یا عملکردهای حسابرسی و کنترل مواد هسته ای را انجام میدهند ، می تواند با سطوح امنیتی بر اساس طبقه بندی مواد مرتبط باشد که می تواند در معرض برداشت غیرمجاز باشد. جدول اول Ref.

[2]معیارهای طبقه بندی مواد هسته ای را ارائه می دهد و بر اساس این طبقه بندی ، توصیه هایی را برای حفاظت فیزیکی بر مبنای طبقه بندی مشخص می کند.

3.14. There is currently no international consensus on a model for a completely integrated hierarchy of all safety and security consequences arising from accidents and nuclear security events resulting from cyber attacks. However, the operator or State should develop such a hierarchy at a national level.

3.14در حال حاضر هیچ اجماع بین المللی در مورد الگویی برای یک سلسله مراتب کاملاً یکپارچه از کلیه پیامدهای ایمنی و امنیتی ناشی از حوادث و وقایع امنیتی هسته ای ناشی از حملات سایبری وجود ندارد. با این حال ، اپراتور یا حکومت باید چنین سلسله مراتبی را در سطح ملی توسعه دهد.

3.15. Other consequences, such as loss of reputation, may also be considered when evaluating the combined consequences of a cyber attack on facility I&C systems. A listing of possible consequences can be found in Ref. [12].

3.15 عواقب دیگری مانند از دست دادن اعتبار نیز ممکن است هنگام ارزیابی پیامدهای حمله سایبری به سیستم های ابزار دقیق و کنترل در نظر گرفته شود. لیستی از پیامدهای احتمالی را می توان در[12] .Ref یافت.

3.16. Adversary tactics and techniques are constantly changing and nuclear facilities should foster a nuclear security culture that continually reviews computer security risks and allows for the adaptability of the facility computer security programme. Nuclear security culture is further explained in Ref. [13].

3.16 تاکتیک ها و تکنیک های متخاصمین به طور مداوم در حال تغییر است و تأسیسات هسته ای باید فرهنگ امنیت هسته ای را به کار گیرند و به طور مداوم خطرات امنیت رایانه را بررسی کرده و امکان سازگاری با برنامه امنیت رایانه را فراهم آورند. فرهنگ امنیت هسته ای در[13] .Ref معرفی شده است.

3.17. System configuration and activities associated with I&C systems enhanced with digital equipment should be analysed to identify changes to logical and physical pathways that could provide opportunities that an adversary could exploit. These activities associated with the I&C systems include temporary maintenance activities, procurement processes, vendor support, communication with field devices and manual software updates.

3.17 پیکربندی سیستم و فعالیتهای مرتبط با سیستمهای ابزار دقیق و کنترل که با تجهیزات دیجیتالی تقویت شده اند، باید مورد تجزیه و تحلیل قرار گیرند تا تغییرات مسیرهای منطقی و فیزیکی که می توانند فرصتهایی برای دشمن فراهم کنند را شناسایی کنند. این فعالیت های مرتبط با سیستم های ابزار دقیق و کنترل شامل فعالیت های نگهداری موقت، فرآیندهای تامین تجهیزات ، پشتیبانی ، ارتباط با دستگاه های میدانی و به روزرسانی های نرم افزار است.

3.18. Facility CSRM is an iterative and cyclical process that could include an initial analysis, threat identification and assessment, definition of security levels, periodic review and updated analysis. There should be a defined acceptance process to review and verify the results of new or updated analyses.

3.18 در یک موسسه CSRM یک فرایند تکرار شونده و چرخه ای است که می تواند شامل تجزیه و تحلیل اولیه ، شناسایی و ارزیابی تهدید ، تعریف سطوح امنیتی ، بررسی دوره ای و تجزیه و تحلیل به روز شده باشد. باید یک فرایند مشخص برای پذیرش بررسی و تأیید نتایج تحلیل های جدید یا به روز وجود داشته باشد.

3.19. For new facilities, the facility CSRM should be performed as part of the design process and accepted before completion of the initial commissioning phase.

3.19 برای تاسیسات جدید ، CSRM موسسه باید به عنوان بخشی از فرایند طراحی انجام شود و قبل از اتمام مرحله راه اندازی اولیه پذیرفته شود.

3.20. For existing facilities, inputs to the new or updated facility CSRM may include safety analysis, details of safety and process architecture and previously accepted facility CSRM outputs.

3.20 برای تاسیسات موجود ، ورودی های جدید برای CSRM یا به روزرسانی شده ممکن است شامل تجزیه و تحلیل ایمنی ، جزئیات ایمنی و معماری فرآیند و خروجی های CSRM قبلاً پذیرفته شده موسسه باشد.

INTERFACE WITH SYSTEM CSRM

واسطه با سیستم CSRM

3.21. The system CSRM should use the facility CSRM outputs (if available) and the design basis documents of the I&C systems as inputs to determine the security risk posed by cyber attacks on individual or multiple I&C systems, subsystems or components. The assessed computer security risk to the I&C systems should be analysed and documented.

3.21 سیستم CSRM باید از خروجی هایCSRM موسسه (در صورت موجود بودن) و اسناد مبنای طراحی سیستم های ابزار دقیق و کنترل به عنوان ورودی استفاده کند تا خطرات امنیتی ناشی از حملات سایبری به سیستم های فردی یا چندگانه ابزار دقیق و کنترل ، زیر سیستم ها یا اجزاء را تعیین کند. ریسک امنیت رایانه ارزیابی شده برای سیستمهای ابزار دقیق و کنترل باید مورد تجزیه و تحلیل قرار گرفته وثبت شود.

3.22. The operator should assign roles and responsibilities throughout the I&C system life cycle for the assessment and management of the I&C system computer security risks. Computer security needs focused efforts by multidisciplinary organizations and teams. For example, the

operator may establish working groups responsible for managing the computer security processes and activities as well as for obtaining authorizations.

3.22 اپراتور برای ارزیابی و مدیریت خطرات امنیت رایانه سیستم ابزار دقیق و کنترل باید پستها و مسئولیت هایی را در طول چرخه عمر سیستم ابزار دقیق و کنترل اختصاص دهد. امنیت رایانه نیاز به تلاشهای متمرکز توسط سازمانها و تیمهای چند رشته ای دارد. به عنوان مثال، اپراتور ممکن است گروه های کاری برای مدیریت فرایندها و فعالیتهای امنیت رایانه و همچنین دریافت مجوزها ایجاد کند.

3.23. The operator should keep an inventory of the I&C system, including software, subsystems and components, which is updated and maintained throughout the life cycle of the system. The operator should use this inventory when performing the system CSRM.

3.23 اپراتور باید فهرست سیستم ابزار دقیق و کنترل از جمله نرم افزار ، زیر سیستم ها و مؤلفه ها را نگهداری کند، که در طول چرخه عمر سیستم به روز شده و نگهداری می شود. اپراتور هنگام اجرای سیستم CSRM باید از این فهرست استفاده کند.

3.24. I&C system components should be assessed and assigned the appropriate security level based on the system CSRM. For these components, the safety and security consequences that could result from mal-operation or compromise should be identified. If security zones are implemented within the facility, the security zone should be assigned and identified.

3.24 اجزای سیستم ابزار دقیق و کنترل باید بر اساس سیستم CSRM ارزیابی شوند و سطح امنیتی مناسبی به آنها اختصاص یابد. برای این اجزا ، عواقب ایمنی و امنیتی که می تواند ناشی از سوء عملکرد یا دستکاری باشد، باید مشخص شود. اگر نواحی امنیتی در داخل موسسه اجرا شود ، منطقه امنیتی باید مشخص و شناسایی شود.

3.25. When performing the system CSRM, the operator should consider the possibility of cyber attack at each phase of the I&C system life cycle. The operator should also consider in the assessment that cyber attacks may affect an individual system or multiple systems and could be used in combination with other forms of malicious acts causing physical damage. Malicious actions that could change process signals, equipment configuration data or software should also be considered in the system CSRM.

3.25 هنگام اجرای سیستم CSRM ، اپراتور باید احتمال حمله سایبری را در هر مرحله از چرخه عمر سیستم ابزار دقیق و کنترل در نظر بگیرد. اپراتور همچنین باید در نظر بگیرد که حملات سایبری ممکن است بر یک سیستم منفرد یا چندین سیستم اثر بگذارد و می تواند در ترکیب با سایر اشکال اعمال مخرب میتواند باعث آسیب فیزیکی شود. اقدامات مخرب که می توانند سیگنال های فرآیند ، داده های پیکربندی تجهیزات یا نرم افزار را تغییر دهند نیز باید در CSRM سیستم در نظر گرفته شوند.

3.26. In addition, all attack vectors that could be used to inject malicious code or data into the I&C system should be considered in the system CSRM. For example, malicious code could be introduced into the I&C system via communication connections, supplied products and services or portable devices that are temporarily connected to target equipment.

3.26 علاوه بر این ، تمام بردارهای حمله ای که می توانند برای تزریق کد یا داده های مخرب به سیستم ابزار دقیق و کنترل استفاده شوند باید در سیستم CSRM در نظر گرفته شوند. به عنوان مثال، کد های مخرب می توانند از طریق اتصالات ارتباطی ، محصولات و خدمات و یا دستگاههای قابل حمل که به طور موقت به تجهیزات مورد نظر وصل می شوند ، وارد سیستم ابزار دقیق و کنترل شوند.

3.27. The system CSRM should determine the likelihood of each potential consequence associated with the I&C system occuring, using as inputs the following: the availability of specific attack vectors that could be used to inject malicious code or data into the I&C system; application and effectiveness of computer security measures; threat capabilities; and other associated information.

3.27 سیستم CSRM باید احتمال بروز هر پیامد احتمالی مرتبط با سیستم ابزار دقیق و کنترل را با استفاده از ورودی های زیر تعیین کند:

در دسترس بودن بردارهای حمله خاص که می تواند برای تزریق کد یا داده های مخرب به سیستم ابزار دقیق و کنترل استفاده شود.

کاربرد و اثربخشی اقدامات امنیت رایانه؛

قابلیت های تهدید؛ و سایر اطلاعات مرتبط

3.28. The system CSRM is an iterative and cyclical process that, similarly to the facility CSRM, involves an initial analysis, implementation of computer security measures, periodic review and updated analysis. The system CSRM should be considered for review when one of the following occurs: 3.28 سیستم CSRM یک فرایند تکراری و چرخه ای است که ، به طور مشابه با CSRM موسسه ، شامل تجزیه و تحلیل اولیه ، اجرای تدابیر امنیت رایانه ، بررسی دوره ای و تجزیه و تحلیل به روز است. سیستم CSRM باید هنگام بروز موارد زیر مورد بازبینی قرار گیرد.

The facility CSRM or facility safety analysis is revised.
System modifications are made.
Relevant security events or incidents occur.
New or changed threats or vulnerabilities are identified.

تجدید نظر CSRM موسسه یا آنالیز ایمنی تأسیسات

اصلاحات سیستم انجام شده است
رویدادها یا حوادث امنیتی مربوطه رخ می دهد.
تهدیدات یا آسیب پذیری های جدید یا تغییر یافته شناسایی شده اند.

3.29. The system CSRM should identify human actions or omissions that might affect security.

3.29 سیستم CSRM باید اقدامات انسانی یا عدم انجام کار را که ممکن است بر امنیت تأثیر بگذارد ، شناسایی کند.

ASSIGNMENT OF COMPUTER SECURITY MEASURES

تخصیص تدابیر امنیت رایانه

3.30. The guidance in paras 3.31–3.34 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

3.30 راهنمایی در پاراگراف 3.31-3.34 برای کلیه سیستم های ابزار دقیق و کنترل، زیر سیستم ها و اجزایی که رویکرد درجه بندی شده در آنها به کار گرفته میشود و مطابق با سطح امنیتی تعیین شده آنها، اعمال می شود.

.

3.31. Each I&C system, subsystem or component should be assigned a security level in accordance with the potential consequences of its failure or mal-operation for both safety and security.

3.31 به هر سیستم ، زیر سیستم یا اجزاء ابزار دقیق و کنترل باید مطابق با عواقب احتمالی خرابی یا سوء عملکرد آن برای ایمنی و امنیت ، یک سطح امنیتی اختصاص داده شود.

3.32. The application of computer security measures to each I&C system should be determined by its assigned security level or the security level of the security zone in which it resides, whichever is more stringent.

3.32استفاده از تدابیر امنیت رایانه برای هر سیستم ابزار دقیق و کنترل باید توسط سطح امنیتی اختصاص داده شده یا سطح امنیتی منطقه امنیتی که در آن قرار دارد تعیین شود ، هر کدام از اینها سختگیرانه تر باشد.

3.33. Computer security requirements should be identified and defined for each security level. The effectiveness of measures implementing these requirements should be evaluated to ensure that sufficient protection is provided for the I&C systems assigned to each security level.

3.33 الزامات امنیت رایانه باید برای هر سطح امنیتی مشخص و تعریف شود. اثربخشی اجرای این الزامات باید مورد ارزیابی قرار گیرد تا اطمینان حاصل شود که از سیستم های ابزار دقیق و کنترل که به هر سطح امنیتی اختصاص داده شده اند، حفاظت کافی می شود.

3.34. If computer security measures are not able to provide sufficient protection for I&C systems at each security level, additional or alternative measures should be considered, e.g. facility level physical protection features, independent electronic functions, system redesign or administrative measures that eliminate specific vulnerabilities or reduce the consequences of mal-operation.

3.34اگر تدابیر امنیت رایانه قادر به محافظت کافی برای سیستم های ابزار دقیق و کنترل در هر سطح امنیتی نباشد، باید تدابیر اضافی یا جایگزینی در نظر گرفته شود، به عنوان مثال ویژگی های حفاظت فیزیکی در سطح موسسه ، کارکردهای الکترونیکی مستقل ، طراحی مجدد سیستم یا اقدامات اداری که آسیب پذیری های خاص را از بین می برد یا عواقب سوء عملکرد را کاهش می دهد.

SAFETY–SECURITY INTERFACES

واسطه های ایمنی - امنیتی

3.35. As stated in Ref. [8], para. 1.2,

“Nuclear security and nuclear safety have in common the aim of protecting persons, property, society and the environment. Security measures and safety measures have to be designed and implemented in an integrated manner to develop synergy between these two areas and also in a way thatsecurity measures do not compromise safety and safety measures do not compromise security.”

Additional guidance on safety considerations for I&C systems can be found in Refs [4, 6].

3.35 همانطور که در[8]Ref بند 1.2 گفته شده است:

" هدف مشترک امنیت هسته ای و ایمنی هسته ای حفاظت از افراد ، دارایی ها ، جامعه و محیط زیست است. تدابیر امنیتی و تدابیر ایمنی باید بصورت یکپارچه طراحی و اجرا شود تا هم افزایی بین این دو حوزه ایجاد شود و همچنین به گونه ای که تدابیر امنیتی، ایمنی را به خطر نمی اندازد و تدابیر ایمنی، امنیت را به خطر نمی اندازد" .

راهنمایی های اضافی در مورد ملاحظات ایمنی برای سیستم های ابزار دقیق و کنترل را می توان در[4,6]Ref یافت.

3.36. The appropriateness of a given computer security measure will depend on safety, security and operational considerations. Input from safety, security and operations personnel is needed to assign computer security measures for I&C systems. Computer security measures cannot exist in isolation from safety concerns, and safety features cannot exist in isolation from security concerns. For example, for safety reasons, certain security functions (e.g. collection of audit records or generation of security alarms) might need to be implemented in separate systems that can monitor the I&C system but do not adversely affect the system’s ability to perform its essential functions. Alternatively, performance of active security scans only when I&C systems are not in service could meet security goals while limiting the impact on the operational systems.

3.36 مناسب بودن تدابیر امنیت رایانه بستگی به ملاحظات ایمنی، امنیتی و عملیاتی دارد. دریافت اطلاعات از پرسنل ایمنی، امنیتی و بهره بردار برای تعیین تدابیر امنیت رایانه برای سیستمهای ابزار دقیق و کنترل لازم است. تدابیر امنیت رایانه نمی تواند جدا از نگرانی های ایمنی باشد ، و ویژگی های ایمنی در انزوا از نگرانی های امنیتی نمی توانند وجود داشته باشند. به عنوان مثال، به دلایل ایمنی ، ممکن است کارکردهای امنیتی خاصی (مثلاً جمع آوری سوابق ممیزی یا تولید هشدارهای امنیتی) در سیستم های جداگانه اجرا شود که بتوانند سیستم ابزار دقیق و کنترل را مانیتور کنند اما بر توانایی سیستم برای انجام وظایف اساسی خود تأثیر منفی نمی گذارد. از طرف دیگر، اجرای اسکنهای امنیتی فعال تنها زمانی که سیستم های ابزار دقیق در بهره برداری نباشند می توانند ضمن تأثیرگذاری محدود بر سیستم های عملیاتی ، اهداف امنیتی را برآورده سازند.

3.37. Inappropriately designed computer security measures could introduce potential failure modes into the system, increase the likelihood of spurious operation and challenge the system's ability to reliably perform its safety function. For example, an inappropriately designed implementation of a malware or virus detection system within the I&C system could increase I&C system complexity, increase I&C system latency and result in the I&C system being vulnerable to exploitation. However, an appropriately designed technical control measure that ensures that only verified and validated software is allowed to run on an I&C system could improve this system's ability to reliably perform its safety function while providing significant security benefits.

3.37 تدابیر طراحی شده نامناسب امنیت رایانه می تواند حالت های احتمالی خرابی را برای سیستم به عمل آورند ، احتمال انجام عمل جعلی را افزایش داده و توانایی سیستم را در اجرای مطمئن عملکرد ایمنی خود به چالش بکشد. به عنوان مثال، طراحی و اجرای نامناسب سیستم تشخیص ویروس یا بدافزار در سیستم ابزار دقیق و کنترل می تواند پیچیدگی سیستم ابزار دقیق و کنترل را افزایش دهد ، تأخیر سیستم ابزار دقیق و کنترل را افزایش داده و منجر به آسیب پذیری سیستم ابزار دقیق و کنترل در برابر بهره برداری می شود. با این حال ، تدابیر طراحی شده فنی مناسب که تضمین می کند تنها نرم افزار تأیید شده و معتبر مجاز به اجرا در یک سیستم ابزار دقیق و کنترل است می تواند توانایی این سیستم را برای اجرای مطمئن عملکرد ایمنی خود ضمن ارائه مزایای امنیتی را به طرز قابل توجهی بهبود بخشد.

3.38. Many functions that are designed into I&C systems for safety reasons may also have security benefits. One example is the checking of received data for validity, authenticity and integrity before it is used in an I&C system function.

3.38 بسیاری از کارکردهایی که به دلایل ایمنی در سیستم های ابزار دقیق و کنترل طراحی شده اند نیز ممکن است دارای مزایای امنیتی باشند. یک مثال، بررسی داده های دریافتی برای اعتبار، صحت و صداقت قبل از استفاده در یک عملکرد سیستم ابزار دقیق و کنترل است.

3.39. There may be situations where a computer security measure cannot be implemented in accordance with an I&C system's assigned security level, for example, owing to conflicts with essential safety functions, but these exceptions should be thoroughly analysed and justified.

3.39 ممکن است موقعیت هایی وجود داشته باشد که نتوان یک تدبیر امنیت رایانه را مطابق با سطح امنیتی اختصاص یافته سیستم ابزار دقیق و کنترل اجرا کرد، به عنوان مثال، به دلیل تضاد جدی با کارکردهای اساسی ایمنی قابل اجرا نباشد ، اما این استثنائات باید کاملاً مورد تجزیه و تحلیل و توجیه قرار گیرد.

3.40. The full set of I&C system computer security measures should work together and prevent (or not introduce) single points of failure.

3.40 مجموعه کامل تدابیر امنیت رایانه و سیستم ابزار دقیق و کنترل باید با هم کار کنند و از بروز (یا عدم معرفی) نقاط ضعف جلوگیری کنند.

3.41. Safety strategy may have the potential to adversely affect security. For example, design for safety often involves the allocation of functions to different subsystems (or processors) in order to isolate the effects of failure, and the provision of redundant and diverse systems so that single failures will not compromise important functions. These strategies result in an increase in the number of subsystems in the I&C systems, which in turn increases the number of targets for cyber attack. Therefore, measures should be taken to reduce the risk that a cyber attack would result in a loss of system diversity or redundancy. Computer security measures should not introduce new vulnerabilities that could result in common cause failures between these redundant and diverse systems.

3.41 استراتژی ایمنی ممکن است این پتانسیل را داشته باشد که بر امنیت تأثیر منفی بگذارد. به عنوان مثال، طراحی برای ایمنی اغلب شامل اختصاص توابع به زیر سیستم های مختلف (یا پردازنده ها) به منظور جداسازی اثرات خرابی، و به کار گیری سیستم های پشتیبان و متنوع است به گونه ای که خرابی های یک واحد باعث به خطر افتادن عملکردهای مهم نمی شوند. این استراتژی ها منجر به افزایش تعداد زیر سیستم ها در سیستم های ابزار دقیق و کنترل می شود که به نوبه خود باعث افزایش تعداد اهداف حمله سایبری می شود. بنابراین، باید تدابیری اتخاذ شود تا حمله سایبری منجر به از بین رفتن تنوع سیستم یا افزونگی سیستم نشود. تدابیر امنیت رایانه نباید آسیب پذیری های جدیدی را ایجاد کند که منجر به عدم عملکرد مشترک بین این سیستم های پشتیبان و متنوع شود.

SAFETY CONSIDERATIONS FOR COMPUTER SECURITY MEASURES

ملاحظات ایمنی درباره تدابیر امنیت رایانه

3.42. The guidance contained in paras 3.43–3.52 applies to all I&C systems important to safety.

3.42 راهنمایی موجود در پاراگراف 3.43-3.52 در مورد کلیه سیستم های ابزار دقیق و کنترل که برای ایمنی مهم هستند اعمال می شود.

3.43. The implementation of computer security measures should not adversely affect the essential safety functions and performance of the I&C system.

3.43 اجرای تدابیر امنیت رایانه نباید بر عملکردهای اساسی ایمنی و عملکرد سیستم ابزار دقیق و کنترل تأثیر منفی بگذارد.

3.44. Neither the normal nor the abnormal operation of any computer security measure should adversely affect the ability of an I&C system to perform its safety function.

3.44 نه عملکرد طبیعی و نه عملکرد غیر طبیعی هیچ تدبیر امنیت رایانه نباید بر توانایی عملکرد ایمنی یک سیستم ابزار دقیق و کنترل تأثیر منفی بگذارد.

3.45. The operator should identify, document and consider in the system hazard analyses the failure modes of the computer security measures and how the failure modes would affect I&C system functions.

3.45 اپراتور باید در تحلیل خطر سیستم , حالت‌های شکست اقدامات امنیت رایانه و چگونگی تاثیر حالت‌های شکست بر عملکرد سیستم ابزار دقیق و کنترل را شناسایی کند .

3.46. Computer security measures that protect the human–system interface should not adversely affect the operator's ability to maintain the safety of the facility. The operator should also consider adverse effects such as the interception and modification of process data sent to the human–system interface (e.g. spoofing) with the aim of preventing or delaying the operator from actuating a safety function (e.g. manual trip).

3.46 تدابیر امنیت رایانه که از رابط سیستم انسانی حفاظت می‌کنند نباید تاثیر منفی بر توانایی اپراتور در حفظ ایمنی تاسیسات داشته باشند. اپراتور باید اثرات نامطلوب مانند رهگیری و اصلاح داده‌های فرآیند ارسال‌شده به رابط سیستم - انسان (برای مثال فریب) را با هدف جلوگیری یا به تاخیر انداختن اپراتور از تحریک یک تابع ایمنی در نظر بگیرد (برای مثال قطع دستی) .

3.47. Computer security measures that cannot be practically integrated into the I&C system should be implemented separately from the I&C system. Additional administrative control measures may be necessary to use and maintain these separate devices.

3.47 معیارهای امنیت رایانه که نمی‌تواند عملاً در سیستم ابزار دقیق و کنترل ادغام شود ، باید بطور جداگانه از سیستم ابزار دقیق و کنترل اجرا شود. اقدامات اضافی کنترل اجرایی ممکن است برای استفاده و نگهداری از این دستگاه‌های جداگانه لازم باشد .

3.48. Computer security measures integrated into I&C systems should be developed according to the management systems guidance in Ref. [14] or an equivalent alternative management system and qualified to the same level as the system in which the computer security measures reside.

3.48 معیارهای امنیت رایانه یکپارچه در سیستم‌های ابزار دقیق و کنترل باید مطابق با راهنمای سیستم‌های مدیریت در Ref[14] توسعه یابند . یک سیستم مدیریت جایگزین معادل و واجد شرایط مشابه سیستمی است که در آن معیارهای امنیت رایانه قرار می‌گیرند .

3.49. If there is a conflict between safety and security, then design considerations taken to ensure safety should be maintained provided that the operator seeks a compatible solution to meet computer security requirements. Compensatory computer security measures should be implemented to reduce the risk to an acceptable level and be supported by a comprehensive

justification and security risk analysis. The implemented measures should not rely solely upon administrative control measures for an extended period. The absence of a security solution should never be accepted.

3.49 اگر یک تعارض بین ایمنی و امنیت وجود داشته باشد , باید ملاحظات طراحی در نظر گرفته شود تا اطمینان حاصل شود که اپراتور به دنبال یک راه‌حل سازگار برای تامین نیازمندی‌های امنیت رایانه است . اقدامات امنیتی جبرانی برای کاهش خطر به سطح قابل‌قبول باید اجرا شوند و توسط یک توجیه جامع و تحلیل ریسک امنیت پشتیبانی شوند . اقدامات اجرایی نباید صرفاً متکی بر معیارهای کنترل اجرایی برای یک دوره طولانی باشند . عدم وجود یک راه‌حل امنیتی هرگز نباید پذیرفته شود

3.50. The primary responsibility for design, selection and implementation of computer security measures should be clearly assigned by the operator, but should be a collaborative effort between personnel responsible for activities involving I&C system design, maintenance, safety and security.

3.50 مسیولیت اولیه طراحی ، انتخاب و اجرای معیارهای امنیت رایانه باید به وضوح توسط اپراتور تعیین شود ، اما باید یک تلاش مشترک بین پرسنل مسیول فعالیت‌های مربوط به طراحی سیستم ابزار دقیق و کنترل ، نگهداری ، ایمنی و امنیت باشد.

3.51. I&C system design analysis should demonstrate that computer security measures integrated into the I&C system and those implemented as separate devices will not adversely affect the accredited safety functions of systems and components important to safety.

3.51 تحلیل طراحی سیستم ابزار دقیق و کنترل باید نشان دهد که معیارهای امنیت رایانه یکپارچه در سیستم ابزار دقیق و کنترل ادغام می‌شوند و آن‌هایی که به عنوان وسائل مجزا پیاده‌سازی می‌شوند, تاثیر منفی بر عملکرد ایمن سیستم‌ها و اجزای مهم امنیت ندارند .

3.52. The maintenance of computer security measures should not adversely affect the availability of I&C systems.

3.52 حفظ معیارهای امنیت رایانه نباید تاثیری منفی بر قابلیت استفاده از سیستم‌های ابزار دقیق و کنترل داشته باشد.