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

**CONTENTS**

1.

INTRODUCTION . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1

مقدمه

Background (1.1–1.9) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1

سابقه

Objective (1.10, 1.11) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

هدف

Scope (1.12–1.15) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

حوزه

Structure (1.16) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

ساختار

2.

KEY CONCEPTS FOR COMPUTER SECURITY OF I&C SYSTEMS (2.1–2.5) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

مفاهیم کلیدی برای امنیت رایانه سیستمهای ابزاردقیق و کنترل

Computer security of I&C systems (2.6–2.14) . . . . . . . . . . . . . . . . . . 6

امنیت رایانه ای سیستم های ابزاردقیق و کنترل

Computer security measures (2.15–2.19) . . . . . . . . . . . . . . . . . . . . . . 8

اقدامات امنیتی رایانه

Application of a graded approach (2.20–2.23) . . . . . . . . . . . . . . . . . . 9

استفاده از رویکرد درجه بندی شده

Computer security levels (2.24–2.27) . . . . . . . . . . . . . . . . . . . . . . . . . 10

سطوح امنیت رایانه

Computer security zones (2.28–2.30) . . . . . . . . . . . . . . . . . . . . . . . . . 10

مناطق امنیتی رایانه

3.

RISK INFORMED APPROACH TO COMPUTER SECURITY FOR I&C SYSTEMS (3.1–3.5) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 12

رویکرد بر مبنای اطلاع از خطردر امنیت رایانه برای سیستم های ابزاردقیق و کنترل

Interface with facility computer security risk management (3.6–3.20) 13

رابط با مدیریت ریسک امنیتی رایانه تسهیلات

Interface with system CSRM (3.21–3.29) . . . . . . . . . . . . . . . . . . . . . 16

Assignment of computer security measures (3.30–3.34) . . . . . . . . . . 18

Safety–security interfaces (3.35–3.41) . . . . . . . . . . . . . . . . . . . . . . . . 18

Safety considerations for computer security measures (3.42–3.52) . . 20

4.

COMPUTER SECURITY IN THE I&C SYSTEM LIFE CYCLE (4.1–4.11) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 22

General guidance for computer security (4.12–4.17) . . . . . . . . . . . . . 25

Aspects of the computer security policy related to I&C systems (4.18–4.20) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 26

Computer security programme (4.21–4.32) . . . . . . . . . . . . . . . . . . . . 27

Secure development environment (4.33–4.40) . . . . . . . . . . . . . . . . . . 28

Contingency plans (4.41–4.45) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 29

I&C vendors, contractors and suppliers (4.46–4.53) . . . . . . . . . . . . . 30

Computer security training (4.54–4.59) . . . . . . . . . . . . . . . . . . . . . . . 31

Common elements of all life cycle phases (4.60) . . . . . . . . . . . . . . . . 32

Management systems (4.61–4.70) . . . . . . . . . . . . . . . . . . . . . . . 32

Computer security reviews and audits (4.71–4.77) . . . . . . . . . . 33

Configuration management for computer security (4.78–4.87) 34

Verification and validation (4.88–4.94) . . . . . . . . . . . . . . . . . . . 36

Computer security assessments (4.95–4.100) . . . . . . . . . . . . . . 37

Documentation (4.101–4.106) . . . . . . . . . . . . . . . . . . . . . . . . . . 38

Design basis (4.107–4.114) . . . . . . . . . . . . . . . . . . . . . . . . . . . . 38

Access control (4.115–4.120) . . . . . . . . . . . . . . . . . . . . . . . . . . 39

Protection of the confidentiality of information (4.121–4.125) 40

Security monitoring (4.126–4.130) . . . . . . . . . . . . . . . . . . . . . . 41

Considerations for the overall defensive computer security architecture (4.131–4.140) . . . . . . . . . . . . . . . . . . . . . . . . . . . 41

Defence in depth against compromise (4.141–4.151) . . . . . . . . 43

Specific life cycle activities . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 44

Computer security requirements specification (4.152–4.155) . 44

Selection of predeveloped items (4.156–4.164) . . . . . . . . . . . . 45

I&C system design and implementation (4.165–4.174) . . . . . . 46

I&C system integration (4.175–4.178) . . . . . . . . . . . . . . . . . . . 47

System validation (4.179–4.185) . . . . . . . . . . . . . . . . . . . . . . . . 48

Installation, overall I&C system integration and commissioning (4.186–4.190) . . . . . . . . . . . . . . . . . . . . . . . . 49

Operations and maintenance (4.191–4.205) . . . . . . . . . . . . . . . 50

Modification of I&C systems (4.206–4.222) . . . . . . . . . . . . . . 52

Decommissioning (4.223–4.226) . . . . . . . . . . . . . . . . . . . . . . . . . . . . 54

REFERENCES . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 57

1. معرفی
2. 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. 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 I&C ترکیب و یکپارچه می شوند. تأسیسات هسته ای جدید و طرح های هسته ای مدرن از سیستم های دیجیتال I&C 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 I&C قبلی دارد. همچنین فن آوری های دیجیتال طی مدرنیزه کردن امکانات موجود به سیستم های I&C وارد می شوند. با این حال ، استفاده از فن آوری های دیجیتال در سیستم های I&C ، 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. 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 I&C 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. حملات سایبری به سیستم های I&C 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 I&C 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 I&C 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. نیاز به حفاظت از سیستم های مبتنی بر رایانه (از جمله سیستم های I&C) 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. 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. 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.

1.6 امنیت رایانه باید در هر مرحله از چرخه سیستم I&C 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 I&C است.

* 1. 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.

1.7 از لحاظ تاریخی ، امنیت رایانه در طراحی سیستم های I&C 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 I&C 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.

1.8 استفاده بیشتر از دستگاه ها و تجهیزات دیجیتال قابل برنامه ریزی، منجر به کاهش تنوع سیستم های I&C 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. اشخاص مجاز ، چه در محل و یا در یک مکان از راه دور ، که دسترسی منطقی یا فیزیکی به سیستم های I&C 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[

1. 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.

1.10 هدف از انتشار این کتاب ارائه راهنمایی برای حفاظت از سیستم های I&C 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.

1.11 این نشریه برای مقامات ذیصلاح ، از جمله نهادهای نظارتی ، و همچنین مدیریت تأسیسات هسته ای ، کارکنان بهره بردار، تعمیر و نگهداری و مهندسین ، فروشندگان I&C ، پیمانکاران و تأمین کنندگان ، طراحان I&C ، 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, security3 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.

1.12 دامنه 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 I&C 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.

1.13 راهنمایی های ارائه شده در این کتاب برای سیستم های I&C در تأسیسات هسته ای جدید (

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

) و سیستم های جدید I&C 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.

1.14 اگرچه 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 سیستمهایI&C به وجود آورد. این خطرات را باید هنگام طراحی و اجرای اقدامات امنیتی رایانه برای سیستم های I&C در یک مرکز به حساب آورد. اقدامات امنیتی رایانه ای برای این سیستم ها ممکن است متفاوت از آنچه در سیستم های I&C 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].

1.15 این کتاب راهنمای جامعی در مورد ملاحظات ایمنی برای سیستم های I&C 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 IAEA و 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.

1.16 پس از این مقدمه ، این کتاب به چهار بخش تفکیک شده است. بخش 2 مروری بر سیستم های I&C 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 I&C ارائه شده است. بخش 4 راهنمایی های امنیتی را که باید در مراحل مختلف چرخه سیستم های I&C ، 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**

2. مفاهیم کلیدی برای امنیت رایانه سیستم های I&C

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

2.1. سیستم های I&C 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 operation5. 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 I&C 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 I&C 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-operation6, such as independence, redundancy, safety defence in depth and diversity7. 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 I&C در تأسیسات هسته ای مفاهیمی را شامل می شود که می توانند اثرات سوء قصد 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.

2.4 اجرای این مفاهیم در معماری کلی I&C 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.

2.5. راهنمایی های موجود در این نشریه برای کلیه سیستم های I&C 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 I&C

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

2.6. بند 2.2 از Ref. [2] بیان می کند:

“The State’s *physical protection regime8* should seek to achieve these objectives through:

1. Prevention of a *malicious act* by means of deterrence and by protection of sensitive information;
2. Management of an attempted *malicious act* or a malicious act by an integrated system of *detection*, delay and response;
3. Mitigation of the consequences of a *malicious act*.”
4. 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. "

* 1. 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.
  2. 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.
  3. 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.

2.7 نمونه هایی از چگونگی استفاده از پیشگیری ، مدیریت و کاهش می تواند در امنیت رایانه ای سیستم های I&C بکار رود ، عبارتند از: پیشگیری: نصب دستگاههای دارای امنیت خراب که ارتباطات داده غیرمجاز را مسدود می کند تا پتانسیل حمله سایبری مبتنی بر شبکه را کاهش دهد که بر سیستم I&C تأثیر منفی بگذارد.

مدیریت ، از جمله تشخیص ، تأخیر و پاسخ: از طریق بازرسی پرونده های ثبت وقایع سیستم ، اپراتور می تواند پیش از شروع یک عمل مخرب که می تواند بر امنیت یا امنیت یک تأسیسات تأثیر بگذارد ، قادر به شناسایی پیش سازها و اقدامات محافظتی باشد.

کاهش و بازیابی: اگر یک سیستم I&C آلوده به بدافزارها شود ، پس از متوقف شدن انتشار بدافزار ، اپراتور تعیین می کند که آیا اقدامات کنترل جبرانی (به عنوان مثال امضاهای ضد ویروس به روز شده ، نصب یا تقویت سیستم های پیشگیری از نفوذ یا تشخیص یا هر دو) وجود دارد. پس از انجام تجزیه و تحلیل ایمنی دقیق و فعالیتهای تأیید صحت سیستم ، در صورت لزوم ، برای جلوگیری از عفونت مجدد ، انجام یک بازسازی سیستم ، تأیید اثربخشی اقدامات کنترل جبرانی ، بازگرداندن سیستم و قرار دادن مجدد آن به خدمت ، لازم است.

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 I&C در برابر سازش ، گاه بر این فرض استوار است که یک اقدام پیشگیرانه تنها ، مانند جداسازی سیستم ها از شبکه های دیگر ، کافی است. با این حال ، چنین پیش فرض به احتمال زیاد منجر به استفاده ناکافی از اقدامات مدیریتی و کاهش می شود تا عدم موفقیت این اقدامات امنیتی رایانه ای منجر به سازش سیستم محافظت شده 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 دستورالعملهای مختلفی برای امنیت رایانه برای سیستمهای اطلاعاتی عمومی ارائه شده است. برخی از این موارد به طور مستقیم برای سیستمهای I&C در تأسیسات هسته ای کاربرد ندارند ، که نیازهای امنیتی رایانه ای خاصی دارند که با سیستم های 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 I&C نمی تواند کاملاً از امنیت رایانه برای سیستم های ICT جدا شود ، اپراتورها و تنظیم کننده ها باید سیاست ها ، الزامات ، اقدامات و شیوه های رایانه ای را که سیستم های I&C و سیستم های فناوری اطلاعات و ارتباطات را به صورت یکپارچه در نظر می گیرد ، توسعه دهند.

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 requirements9 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.

2.11 بسیاری از سیستم های I&C دارای چرخه عمر چندین دهه هستند ، از جمله دوره هایی که در طی آن پشتیبانی از فروشنده برای برآورده کردن الزامات امنیتی رایانه 9 برای این سیستم ها در دسترس نیست یا ناکافی است. این شامل پشتیبانی ارائه شده توسط فروشنده اصلی و توسط 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 های امضا ، محافظت کافی در برابر سوء استفاده از آسیب پذیری در سیستم های I&C 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.

2.12 در اکثر برنامه ها ، سیستم های I&C در زمان واقعی کار می کنند ، و اقدامات سیستم I&C در فواصل زمانی دقیق انجام می شود. نمونه هایی از این قبیل اقدامات سیستم I&C در تاسیسات هسته ای شامل کنترل عملکردهای عادی ، اقدامات محافظتی ، اقدامات محدود کننده و سیگنال زنگ هشدار برای اپراتورها است. اقدامات امنیتی رایانه ای نباید مانع ، مانع یا تأخیر در انجام اقدامات عملیاتی یا ایمنی لازم شود. از اقدامات امنیتی رایانه ای برای سیستم های I&C 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 اقدامات پاسخگو مانع عملکردهای ایمنی معتبر نشده و یا قرار دادن سیستم در خارج از اساس طراحی آن 10

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 امنیتی رایانه ای که به صورت گذشته نگر مورد استفاده قرار گرفته یا ضعیف اجرا شده اند ، ممکن است پیچیدگی دیگری را در طراحی سیستم I&C ایجاد کند ، که ممکن است منجر به افزایش احتمال خرابی سیستم یا سیستم کارآیی 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 عنصر 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 می کند ، ممکن است به دلیل ادغام ویژگی های امنیتی ، از بین بردن عملکردهای غیر ضروری (به عنوان مثال دسترسی از راه دور) یا سخت شدن سیستم ساده و قوی تر باشد. .

COMPUTER SECURITY MEASURES

اقدامات ایمنی رایانه ای

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 اقدامات امنیتی رایانه ای برای جلوگیری ، کشف ، تأخیر و پاسخ به اقدامات مخرب و همچنین برای کاهش پیامدهای چنین اقداماتی استفاده می شود. از اقدامات امنیتی رایانه نیز برای اطمینان از اینكه اقدامات غیرمسئول امنیت را تضعیف نمی كنند و آسیب پذیری سیستم های مبتنی بر رایانه در برابر اقدامات مخرب را افزایش می دهند نیز 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 اقدامات امنیتی رایانه ای که آسیب پذیری های موجود در سیستم را برطرف می کند یا لایه های محافظتی را ارائه می دهد ، می تواند به یکی از سه دسته اختصاص یابد: اقدامات کنترل فنی ، اقدامات کنترل فیزیکی یا اقدامات کنترل اداری. هر سه دسته باید در نظر گرفته شوند و در هنگام توسعه امنیت رایانه ای یکپارچه برای سیستم های I&C ، 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 اقدامات 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 اقدامات کنترلی فنی در ارائه اقدامات محافظتی مداوم و خودکار باید هنگام ارزیابی اثربخشی آنها در مقایسه با اقدامات کنترل فیزیکی یا اداری 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 اقدامات کنترل فیزیکی موانع جسمی است که از ابزارها ، سیستم های مبتنی بر رایانه و حمایت از دارایی در برابر آسیب های جسمی و دسترسی غیرمجاز فیزیکی محافظت می کند. اقدامات کنترل فیزیکی شامل قفل ها ، محاصره های بدنی ، وسایل 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 اقدامات کنترل اداری سیاست ها ، رویه ها و رویه هایی است که برای محافظت از سیستم های رایانه ای با ارائه دستورالعمل برای عملکرد کارمندان و شخص ثالث طراحی شده است. اقدامات کنترل اداری اقدامات مجاز ، لازم و ممنوع کارمندان و شخص ثالث را مشخص می کند. اقدامات کنترل اداری برای تاسیسات هسته ای شامل اقدامات عملیاتی و کنترل مدیریت است.

APPLICATION OF A GRADED APPROACH

کاربرد یک رویکرد درجه

* 1. 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;
  2. The identified and assessed threats to the facility;
  3. The attractiveness of the I&C system to potential adversaries;
  4. The vulnerabilities of the I&C system;
  5. The operating environment;
  6. The potential consequences that could either directly or indirectly result from a compromise of the system.
  7. 2.20 اپراتور باید الزامات امنیتی رایانه را مبتنی بر رویکرد طبقه بندی شده با ریسک آگاهانه اعمال کند که موارد زیر را در نظر می گیرد: اهمیت عملکرد سیستم I&C برای هر دو ایمنی (یعنی طبقه بندی ایمنی) و امنیت.
  8. تهدیدات شناسایی شده و ارزیابی شده برای تأسیسات.
  9. جذابیت سیستم I&C به مخالفان بالقوه.
  10. آسیب پذیری های سیستم I&C؛
  11. محیط عملیاتی؛
  12. عواقب احتمالی که می تواند مستقیم یا غیرمستقیم ناشی از سازش 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 امنیتی رایانه باشد.

* 1. 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.
  2. The function has unexpected behaviours or actions that are observable to the operator.
  3. The function fails.
  4. 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 امنیتی رایانه متناسب با پیامدهای احتمالی یک حمله تعریف می شود. عواقب احتمالی سازش بر عملکرد سیستم I&C به ترتیب بدترین تا بهترین موارد تنظیم شده است: عملکرد نامشخص است. اثرات سازش 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 ناموفق است.

این عملکرد همانطور که انتظار می رود انجام می دهد ، به این معنی که سازش بر عملکرد سیستم تأثیر منفی نمی گذارد (به عنوان مثال تحمل 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 امنیتی رایانه باید مطابق آنچه در این نشریه شرح داده شده است بر روی سیستم های I&C 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 11 در Ref ارائه شده است. [3] در مقابل ، نمونه ای از اجرای یک روش درجه بندی شده برای ایمنی در Ref ارائه شده است. [9]

COMPUTER SECURITY LEVELS

سطح 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 سطح امنیت رایانه و کلاسهای ایمنی مفاهیم مجزا اما مرتبط هستند. طبقه بندی ایمنی موردی که از نظر ایمنی مهم است 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 هر عملکرد سیستم I&C در ارتباط با تأسیسات ، یک سطح امنیت رایانه را نشان می دهد تا میزان حفاظت از امنیت رایانه مورد نیاز را مشخص کند. برای برآورده کردن الزامات مربوط به امنیت رایانه ، هر سطح به مجموعه های مختلفی از اقدامات امنیتی رایانه نیاز دارد. سطح امنیتی اغلب بر اساس اهداف امنیتی سازمان تعریف می شود. مرجع [10] اطلاعات بيشتري در مورد اجراي سطوح و مناطق امنيتي ارائه مي 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 مؤلفه های سیستم های I&C که سوء عملکرد آنها می تواند بر امنیت هسته ای (از جمله کاهش تصادف) تأثیر بگذارد ، امنیت هسته ای و حسابداری و کنترل مواد هسته ای با توجه به سهم آنها در عملکرد سیستم I&C ، در سطوح امنیتی مشخص و به آنها اختصاص داده می شود

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 را به یک سیستم I&C ، زیر سیستم یا مؤلفه ای بر اساس عواقب احتمالی عدم موفقیت یا خراب بودن آن ، از جمله عملکرد نادرست به گونه‌ای که با طراحی یا حالتهای شکست قابل تصور خود که در یک تاسیسات مشخص می شود ، اختصاص می دهد. تجزیه و تحلیل ایمنی. سطح امنیت رایانه اختصاص داده شده به یک سیستم I&C ، زیر سیستم یا مؤلفه مربوط به آن سیستم ، زیر سیستم یا مؤلفه است و مستقل از محیط آن است.

COMPUTER SECURITY ZONES

مناطق ایمنی رایانه ای

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.

2.28 مفهوم منطقه 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 رایانه امنیتی را به اشتراک می گذارند. تمام سیستمهای مستقر در یک منطقه واحد در همان سطح امنیتی محافظت می شوند ، یعنی که به عملکرد سیستم I&C با دقیقترین سطح امنیتی در منطقه اختصاص داده می شود. گروه بندی سیستم های I&C در مناطق امنیتی ممکن است کاربرد و مدیریت اقدامات امنیتی رایانه ای را ساده تر کند.

* 1. 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.
  2. Systems belonging to the same zone form a trusted area for internal communications between those systems (i.e. internal trusted zone area).
  3. 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.
  4. System safety architecture requirements (e.g. redundancy, diversity, geographic and electrical separation, single failure criterion) are maintained.
  5. 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.
  6. 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.
  7. Zones may be partitioned into sub-zones to improve the configuration.

2.29 ملاحظات مربوط به اجرای مناطق امنیتی باید دارای معیارهای زیر باشد: سیستم های متعلق به همان منطقه نیازهای مشابهی برای اقدامات امنیتی رایانه ای دارند.

سیستم های متعلق به همان منطقه یک منطقه قابل اعتماد برای ارتباطات داخلی بین آن سیستم ها (یعنی منطقه منطقه مورد اعتماد داخلی) را تشکیل می دهند.

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

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

اقدامات كنترلی فنی در محدوده منطقه انجام می شود تا جریان داده و ارتباط بین سیستم های واقع در مناطق مختلف (به عنوان مثال از راه دور) محدود شود یا به سطوح مختلف امنیتی اختصاص یابد.

رسانه های قابل جابجایی ، دستگاه های تلفن همراه و سایر تجهیزات موقتی که نیاز به دسترسی منطقی یا فیزیکی به یک سیستم دارند فقط در یک منطقه واحد یا مجموعه مشخصی از مناطق مورد استفاده قرار می گیرند.

برای بهبود پیکربندی ، مناطق ممکن است به زیر مناطق 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 مناطق امنیتی در یک مرکز استفاده می شود ، برخی از سیستم ها یا قطعات I&C می توانند به مناطقی اختصاص داده شوند که سطح امنیتی دقیق تری 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 واگذاری به دلیل امکان استفاده مشکوک از دستگاه برای به خطر انداختن اجزای سیستم محافظ راکتور است که از نظر ایمنی بسیار مهم هستند. علاوه بر این ، استفاده از منطقه امنیتی سیستم حفاظتی راکتور امکان ایجاد منطقه منطقه مورد اعتماد داخلی را فراهم می کند ، در نتیجه اطمینان حاصل می شود که اقدامات اضافی امنیتی رایانه ای 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 اطلاع رسانی شده در معرض خطر نسبت به امنیت رایانه برای سیستم های I&C

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.

3.1 یک رویکرد آگاهانه از خطر در مورد امنیت رایانه برای سیستم های I&C ممکن است از ارزیابی ریسک برای شناسایی آسیب پذیری یک مرکز در برابر حمله سایبری مربوط به این سیستم ها و تعیین عواقب ناشی از بهره برداری موفقیت آمیز از این آسیب پذیری ها استفاده کند. اقدامات امنیتی رایانه سپس بر اساس نتایج ارزیابی ریسک می تواند اختصاص یابد.

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.

3.2 از آنجا که سیستم های I&C اغلب برای ایمنی تأسیسات ضروری هستند ، درک ایمنی هسته ای می تواند در ارزیابی ریسک ، تدوین اقدامات امنیتی رایانه ای برای سیستم I&C ، ارزیابی تعارضات احتمالی بین ایمنی و امنیت و بررسی چگونگی حل اینگونه درگیری ها کمک کند. به عنوان مثال ، مخالفان می توانند از طریق حمله سایبری به سیستم های I&C یک مرکز ، یک مرکز را خراب کنند و در نتیجه عواقب ایمنی و امنیتی بالقوه ایجاد کنند. چنین حملاتی ممکن است باعث خرابی سیستم های I&C شود و یا ممکن است باعث شود سیستم های I&C به طریقی عمل کنند که با رفتار مورد نظر یا حالت های شکست تحلیل شده آنها متفاوت باشد. اقدامات مخرب ممکن است بر یک سیستم منفرد و سیستم عامل منفرد یا چندین سیستم I&C اثر بگذارد. به عنوان مثال ، اقدامات مخرب این امکان وجود دارد که از عمق چندین سطح دفاعی ایمنی در عمق 12 عبور یا باعث خرابی همزمان شود. اقدامات مخرب همچنین ممکن است حملات سایبری را با عناصر 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.

3.3 امنیت نامناسب رایانه یا سیستم I&C به خطر بیافتد ممکن است باعث شود امنیت ایمنی یک مرکز به خطر بیفتد. به عنوان مثال ، اگر یک سیستم I&C به خطر بیفتد ، ممکن است یک مخالف داده اطلاعاتی را بدست آورد که اطلاعات مهم لازم برای برنامه ریزی برای حمله یا تغییر داده هایی را که باعث خرابکاری سیستم های تسهیلاتی یا حذف غیرمجاز مواد هسته ای می شود ، فراهم کند. از طرف دیگر ، حمله سایبری که منجر به خرابکاری می شود ممکن است باعث بروز یک تصادف شود یا عملکرد یک عملکرد ایمنی را تخریب کند. چنین حمله ای نیز ممکن است به از دست رفتن در دسترس بودن سیستم 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.

3.4 حملات سایبری به سیستم های I&C همچنین ممکن است منجر به پیامدهایی شود که حذف غیرمجاز مواد هسته ای از یک مرکز را ممکن می سازد. سیستمهای I&C که عملکردهای محافظت فیزیکی یا حسابداری 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 عناصر حمله فیزیکی با هدف حذف 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 ، اقدامات امنیتی رایانه ای برای سیستم های I&C 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 حذف غیرمجاز مواد هسته ای را تسهیل کند ، برطرف کند.

INTERFACE WITH FACILITY COMPUTER SECURITY RISK MANAGEMENT

رابط با مدیریت خطرات ایمنی رایانه ای

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 vulnerabilities13 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 I&C ، باید یک فرآیند مدیریت ریسک امنیت رایانه (CSRM) داشته باشد. این فرایند برای شناسایی آسیب پذیری های تأسیسات13 در برابر حمله سایبری و تعیین نتیجه موفقیت آمیز یک یا چند عملکرد انجام شده توسط سیستم های I&C (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.

3.7 خروجی فرآیندهای CSRM از تسهیلات باید شامل شناسایی توابع تسهیلات انجام شده توسط سیستم های I&C از جمله سیستم های پشتیبانی و مکمل باشد که در صورت به خطر انداختن می تواند بر امنیت ، 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. عملیات بد ناشی از حملات سایبری ممکن است این مرکز 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.

3.8 خروجی فرآیندهای CSRM در تأسیسات باید پیامدهای احتمالی مربوط به ایمنی هسته ای ، امنیت هسته ای و حسابداری مواد هسته ای و کنترل ناشی از مصالحه سیستم به دلیل حمله سایبری به سیستم های I&C را مشخص کند. هنگام تجزیه و تحلیل عواقب حمله به سیستم I&C ، باید این احتمال را در نظر گرفت که این حمله می تواند جزئی از حمله بزرگتری باشد که بر سیستم های چند و میدانی و یا یک حمله سایبری و فیزیکی ترکیبی تأثیر می گذارد. این تجزیه و تحلیل سپس می تواند مورد استفاده قرار گیرد برای اختصاص سطح امنیتی مناسب به سیستم ها و اجزای I&C فردی بر اساس پیامدهای احتمالی عدم موفقیت یا سوء عملکرد آنها.

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.

3.9 سطح امنیتی اختصاص داده شده به سیستمهای I&C ممکن است با یک لیست سلسله مراتبی از پیامدهای احتمالی ایمنی یا امنیتی همراه باشد. مثلاً گیاه ایالات ، عواقب خرابکاری ، سلسله مراتب 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.

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 accident14: 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 گیاهان گیاه می توان برای عواقب ایمنی بالقوه حمله سایبری به سیستم های I&C استفاده کرد. به عنوان مثال ، حالت های گیاهی می توانند با سطح امنیتی سیستم های I&C به شرح زیر همراه باشند ، که از اوضاع با کمترین تا وضعیت با بالاترین نتیجه سفارش داده شده است:

(1) عملکرد عادی: حمله سایبری به سیستم های I&C نمی تواند باعث ایجاد امکانات 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 I&C ممکن است باعث شود حالت گیاه از عملکرد طبیعی به طریقی که پیش بینی می شود منحرف شود ، اما با توجه به مقررات طراحی مناسب ، خسارت قابل توجهی به موارد مهم وارد نمی کند. ایمنی یا منجر به شرایط تصادف.

(3) طراحی پایه تصادف14: حمله سایبری به سیستم های I&C ممکن است باعث ایجاد شرایط حادثه ای شود که در قالب طرح تأسیسات باقی می ماند و برای آن صدمه به مواد هسته ای (یا سایر مواد رادیواکتیو) و انتشار مواد رادیواکتیو در محدوده مجاز نگهداری می شود. .

(4) شرایط توسعه طراحی: حمله سایبری به سیستم های I&C ممکن است باعث ایجاد شرایط تصادف شود که برای حوادث پایه طراحی در نظر گرفته نشده باشد ، اما در فرآیند طراحی تأسیسات مطابق با بهترین روش تخمین مورد بررسی قرار می گیرد و برای آن انتشار رادیو اکتیو در نظر گرفته می شود. مواد در حد قابل قبول نگه داشته می شوند. شرایط توسعه طراحی می تواند شامل شرایط تصادف 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 I&C همچنین می تواند با سطح امنیتی همراه باشد. چنین رویکردی شامل دولت خواهد بود که آستانه پیامدهای رادیولوژیکی غیرقابل قبول را تعیین کند ، همانطور که در بند توصیه شده است. 3.44 از Ref. [2] تعریف آستانه URC 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) بیان شود. به یک فرد واقع در برخی از نقاط مشخص شده ، معمولاً خارج از محل) یا شرایط تأسیسات (به عنوان مثال خرابکاری که ممکن است منجر به خسارت هسته قابل توجهی در راکتور شود). همانطور که در Ref گفته شده است. [11] ، 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 اشاره شده است ... [در Ref. [2]] به دلیل عواقب رادیولوژیکی بالا.

"بنابراین ، دولت همچنین باید آستانه عواقب رادیولوژیکی بالا را تعیین کند

* 1. 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.
  2. 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.
  3. 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).
  4. Consequence Level A: Sabotage that could give rise to severe deterministic health effects off-site (likely also to be considered high radiological consequences).
  5. 3.12 نمونه ای از لیست سلسله مراتبی از پیامدهای احتمالی خرابکاری در Ref ارائه شده است. [11] و برای توابع سیستم I&C 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 یک سطح مناسب از سطح حفاظت پایین نیاز دارند.
  6. URC را می توان به سه دسته طبقه بندی کرد که از پایین ترین تا بالاترین پیامدها: پیامد سطح C: خرابکاری که منجر به دوز به افراد در محل می شود که اقدامات محافظتی فوری را به حداقل می رساند تا اثرات سلامتی در سایت را به حداقل برساند.
  7. پیامد سطح B: خرابکاری که می تواند منجر به دوز یا آلودگی خارج از سایت شود که اقدامات محافظتی فوری را به حداقل می رساند تا اثرات سلامتی خارج از سایت را به حداقل برساند (ممکن است پیامدهای رادیولوژیکی بالایی نیز در نظر گرفته شود).
  8. پیامد سطح A: خرابکاری که می تواند عوارض جانبی سلامت زیادی را در خارج از کشور ایجاد کند (احتمالاً عواقب رادیولوژیکی بالایی نیز در نظر گرفته شود).

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 همچنین سطح امنیتی می تواند با احتمال حذف غیرمجاز مواد هسته ای همراه باشد. عواقب احتمالی حملات سایبری بر روی سیستم های I&C که دارای حفاظت فیزیکی یا عملکردهای حسابداری و کنترل مواد هسته ای هستند ، می تواند با سطح امنیتی بر اساس طبقه بندی مواد مرتبط باشد که می تواند در معرض حذف 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 حمایت از جسمی 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.

3.14 در 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 حوادث امنیتی هسته ای ناشی از حملات سایبری وجود ندارد. با این حال ، اپراتور یا ایالت 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 شهرت نیز ممکن است هنگام ارزیابی پیامدهای ترکیبی از حمله سایبری به سیستم های I&C تأسیس شود. لیستی از پیامدهای احتمالی را می توان در Ref. [12]

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 مخالف به طور مداوم در حال تغییر است و تأسیسات هسته ای باید یک فرهنگ امنیت هسته ای را تقویت کند که به طور مداوم خطرات امنیتی رایانه را بررسی کرده و امکان سازگاری با برنامه امنیتی رایانه را فراهم می آورد. فرهنگ امنیت هسته ای بیشتر در Ref. [13]

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 I&C که با تجهیزات دیجیتالی تقویت شده اند ، باید مورد تجزیه و تحلیل قرار گیرند تا تغییرات مسیرهای منطقی و فیزیکی شناسایی شوند که می توانند فرصتهایی را فراهم کنند که یک طرف مقابل بتواند از آن سوءاستفاده کند. این فعالیت های مرتبط با سیستم های I&C شامل فعالیت های نگهداری موقت ، فرآیندهای تهیه ، پشتیبانی از فروشندگان ، ارتباط با دستگاه های میدانی و به روزرسانی های نرم افزار دستی 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 Facility 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 باشد. باید یک فرایند پذیرش تعریف شده برای 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 امکانات جدید ، تسهیلات CSRM 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 تسهیلات 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 تسهیلات قبلاً پذیرفته شده باشد.

INTERFACE WITH SYSTEM CSRM

رابط 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 های CSRM (در صورت موجود بودن) از تسهیلات و اسناد مبنای طراحی سیستم های I&C به عنوان ورودی استفاده کند تا خطرات امنیتی ناشی از حملات سایبری به سیستم های فردی یا چندگانه I&C ، زیر سیستم ها یا مؤلفه ها را تعیین کند. ریسک امنیتی رایانه ارزیابی شده برای سیستمهای I&C باید مورد تجزیه و تحلیل قرار گیرد.

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 امنیتی رایانه سیستم I&C باید نقش ها و مسئولیت هایی را در طول چرخه عمر سیستم I&C 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 ایجاد کند مسئولیت مدیریت فرایندها و فعالیتهای امنیتی رایانه و همچنین دریافت مجوزها.

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 موجودی سیستم I&C از جمله نرم افزار ، زیر سیستم ها و مؤلفه ها را حفظ کند ، که در طول چرخه عمر سیستم به روز شده و نگهداری می شود. اپراتور هنگام اجرای سیستم CSRM باید از این موجودی 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 I&C باید بر اساس سیستم CSRM ارزیابی شود و سطح امنیتی مناسبی را اختصاص دهد. برای این مؤلفه ها ، عواقب ایمنی و امنیتی که می تواند ناشی از سوء عملکرد یا سازش باشد ، باید مشخص شود. اگر مناطق امنیتی در داخل تسهیلات اجرا شود ، منطقه امنیتی باید اختصاص داده 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 I&C در نظر بگیرد. اپراتور همچنین باید در ارزیابی ارزیابی کند که حملات سایبری ممکن است بر یک سیستم منفرد یا چندین سیستم اثر بگذارد و می تواند در ترکیب با سایر اشکال اعمال مخرب باعث آسیب جسمی 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 I&C 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 I&C 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 I&C 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 I&C استفاده شود. کاربرد و اثربخشی اقدامات امنیتی رایانه؛ قابلیت های تهدید؛ و سایر اطلاعات مرتبط

* 1. 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:The facility CSRM or facility safety analysis is revised.
  2. System modifications are made.

3.28 سیستم CSRM یک فرایند تکراری و چرخه ای است که ، به طور مشابه با امکانات CSRM ، شامل تجزیه و تحلیل اولیه ، اجرای اقدامات امنیتی رایانه ، بررسی دوره ای و تجزیه و تحلیل به روز است. سیستم CSRM باید هنگام بازبینی یکی از موارد زیر مورد بررسی قرار گیرد: CSRM تسهیلات یا آنالیز ایمنی تأسیسات تجدید نظر می شود.

* 1. اصلاحات سیستم انجام شده است

1. Relevant security events or incidents occur.
2. ——New or changed threats or vulnerabilities are identified.
3. رویدادها یا حوادث امنیتی مربوطه رخ می دهد.
4. threats تهدیدات یا آسیب پذیری های جدید یا تغییر یافته شناسایی شده اند.
5. 3.29. The system CSRM should identify human actions or omissions that might affect security.

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

1. ASSIGNMENT OF COMPUTER SECURITY MEASURES
2. تخصیص اقدامات امنیتی رایانه
3. 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.
4. 3.30 راهنمایی در پاراگراف 3.31-3.34 برای کلیه سیستمهای I&C ، زیر سیستم ها و مؤلفه هایی که ممکن است رویکرد درجه بندی شده مطابق با سطح امنیتی اختصاصی آنها اعمال شود ، اعمال می شود.
5. .
6. 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.
7. 3.31 به هر سیستم ، زیر سیستم یا مؤلفه I&C باید مطابق با عواقب احتمالی عدم موفقیت یا عدم کارایی آن برای امنیت و امنیت ، یک سطح امنیتی اختصاص داده شود.
8. 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.
9. 3.32 استفاده از اقدامات امنیتی رایانه ای برای هر سیستم I&C باید توسط سطح امنیتی اختصاص داده شده یا سطح امنیتی منطقه امنیتی که در آن ساکن است تعیین شود ، هر کدام از اینها دقیق تر باشد
10. 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.
11. 3.33 الزامات امنیتی رایانه باید برای هر سطح امنیتی مشخص و تعریف شود. اثربخشی اقدامات اجرای این الزامات باید مورد ارزیابی قرار گیرد تا اطمینان حاصل شود که از سیستم های I&C که به هر سطح امنیتی اختصاص داده شده ، حفاظت کافی می شود.
12. 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.
13. 3.34 اگر اقدامات امنیتی رایانه ای قادر به محافظت کافی برای سیستم های I&C در هر سطح امنیتی نباشد ، باید اقدامات اضافی یا جایگزینی در نظر گرفته شود ، به عنوان مثال ویژگی های حفاظت فیزیکی در سطح تسهیلات ، 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.
14. SAFETY–SECURITY INTERFACES
15. روابط ایمنی و ایمنی
16. 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 Ref گفته شده است. [8] ، بند 1.2 ،

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

راهنمایی های اضافی در مورد ملاحظات ایمنی برای سیستم های I&C را می توان در Refs [4، 6] 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 معیار امنیتی رایانه ای بستگی به ملاحظات ایمنی ، امنیتی و عملیاتی دارد. برای تعیین اقدامات امنیتی رایانه برای سیستمهای I&C ، از پرسنل ایمنی ، امنیتی و عملیات لازم است. اقدامات امنیتی 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 حسابرسی یا تولید هشدارهای امنیتی) در سیستمهای جداگانه اجرا شود که بتوانند سیستم I&C را نظارت کنند اما بر توانایی سیستم برای انجام وظایف اساسی خود تأثیر منفی نمی گذارد. از طرف دیگر ، عملکرد اسکنهای امنیتی فعال تنها زمانی که سیستم های I&C در خدمت نباشند می توانند ضمن تأثیرگذاری 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 اقدامات امنیتی نامناسب رایانه طراحی شده می تواند حالت های احتمالی خرابی را به سیستم وارد کند ، احتمال انجام عمل جنجالی را افزایش داده و توانایی سیستم را در اجرای قابل اطمینان عملکرد ایمنی خود به چالش بکشد. به عنوان مثال ، اجرای نامناسب طراحی شده ی بدافزار یا سیستم تشخیص ویروس در سیستم I&C می تواند پیچیدگی سیستم I&C را افزایش دهد ، تأخیر سیستم I&C را افزایش داده و منجر به آسیب پذیری سیستم I&C در برابر بهره برداری می شود. با این حال ، یک اندازه گیری کنترل فنی مناسب که تضمین می کند تنها نرم افزار تأیید شده و معتبر مجاز به اجرا در یک سیستم I&C است می تواند توانایی این سیستم را برای اجرای قابل اطمینان عملکرد ایمنی خود ضمن ارائه مزایای امنیتی 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 I&C 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 I&C 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 یک اندازه گیری امنیت رایانه ای مطابق با سطح امنیتی اختصاص یافته سیستم I&C ، به عنوان مثال ، ناشی از درگیری 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 کاملی از اقدامات امنیتی رایانه و سیستم I&C باید با هم کار کنند و از بروز (یا معرفی نکردن) 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 تهیه سیستم های کار برکنار و متنوع است به گونه ای که خرابی های واحد باعث به خطر افتادن عملکردهای مهم نمی شوند. این استراتژی ها منجر به افزایش تعداد زیر سیستم ها در سیستم های I&C می شود که به نوبه خود باعث افزایش تعداد اهداف حمله سایبری می شود. بنابراین ، باید تدابیری اتخاذ شود تا خطر حمله سایبری منجر به از بین رفتن تنوع سیستم یا افزونگی سیستم شود. اقدامات امنیتی رایانه ای نباید آسیب پذیری های جدیدی را ایجاد کند که می تواند منجر به عدم موفقیت بین این سیستم های افزایشی و متنوع شود

SAFETY CONSIDERATIONS FOR COMPUTER SECURITY MEASURES

موارد ایمنی درباره اقدامات ایمنی رایانه ای

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 سیستمهای I&C 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 اقدامات امنیتی رایانه نباید بر عملکردهای اساسی ایمنی و عملکرد سیستم I&C 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 اندازه گیری امنیتی کامپیوتر نباید بر توانایی یک سیستم I&C در عملکرد عملکرد ایمنی آن 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 سیستم تجزیه و تحلیل خطرات سیستم اقدامات امنیتی و چگونگی تأثیر حالت خرابی بر عملکرد سیستم I&C را شناسایی کند ، مستند و در نظر بگیرد.

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 اقدامات امنیتی رایانه ای که از رابط انسان و سیستم محافظت می کند ، نباید بر توانایی اپراتور برای حفظ ایمنی تأثیر تأثیر بگذارد. اپراتور همچنین باید با هدف جلوگیری یا به تأخیر انداختن اپراتور از اجرای یک عملکرد ایمنی (به عنوان مثال سفر دستی) اثرات منفی مانند رهگیری و اصلاح داده های فرآیند ارسال شده به رابط انسان و سیستم (مانند کلاهبرداری) را در نظر بگیرد.

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 اقدامات امنیتی رایانه ای که به طور عملی نمی توانند در سیستم I&C ادغام شوند ، باید جداگانه از سیستم I&C به اجرا درآیند. اقدامات اضافی کنترل اداری ممکن است برای استفاده و نگهداری از این دستگاه های 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 اقدامات امنیتی رایانه ای ادغام شده در سیستم های I&C باید مطابق راهنمایی سیستم های مدیریت در Ref تهیه شود. [14] یا یک سیستم مدیریت جایگزین معادل آن و دارای همان درجه ای است که سیستم امنیتی کامپیوتر در آن ساکن است.

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 تضاد بین ایمنی و امنیت وجود داشته باشد ، باید ملاحظات طراحی شده برای اطمینان از ایمنی حفظ شود به شرطی که اپراتور به دنبال یک راه حل سازگار برای رفع نیازهای امنیتی رایانه باشد. اقدامات امنیتی جبرانی رایانه ای باید انجام شود تا خطر به حد قابل قبولی کاهش یابد و با یک توجیه جامع و تحلیل ریسک امنیتی پشتیبانی شود. اقدامات انجام شده نباید فقط برای یک دوره طولانی فقط به اقدامات کنترل اداری متکی باشد. عدم وجود راه حل 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 مسئولیت اصلی برای طراحی ، انتخاب و اجرای اقدامات امنیتی رایانه باید به طور واضح توسط اپراتور واگذار شود ، اما باید تلاش مشترکی بین پرسنل مسئول فعالیتهای مربوط به طراحی سیستم I&C ، تعمیر و 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 تجزیه و تحلیل طراحی سیستم I&C باید نشان دهد که اقدامات امنیتی رایانه ای ادغام شده در سیستم I&C و مواردی که به عنوان دستگاه های جداگانه اجرا می شوند ، بر عملکردهای ایمنی معتبر سیستم ها و مؤلفه های مهم ایمنی تأثیر منفی نخواهد گذاشت.

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

3.52 حفظ اقدامات امنیتی رایانه نباید بر دسترسی سیستمهای I&C تأثیر منفی بگذارد

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

4. امنیت رایانه در چرخه زندگی I&C SYSTEM

4.1. The design of I&C systems for nuclear facilities should be managed through the facility’s integrated management system15 to ensure that all computer security requirements are considered and implemented in all phases of the I&C system life cycle and that these computer security requirements are met in the final design. Reference [14] establishes the General Safety Requirements for the management systems of nuclear facilities. In addition, Ref. [8], para. 3.12(a) refers to the importance for nuclear security of integrated management systems. Reference [3] provides further discussion of the overall relationship between management systems and computer security.

4.1 طراحی سیستم های I&C برای تأسیسات هسته ای باید از طریق سیستم مدیریت یکپارچه تاسیسات15 انجام شود تا اطمینان حاصل شود که کلیه الزامات امنیتی رایانه در کلیه مراحل چرخه عمر سیستم I&C در نظر گرفته شده و اجرا می شود و این الزامات امنیتی رایانه در طراحی نهایی برآورده می شود. مرجع [14] الزامات عمومی ایمنی را برای سیستمهای مدیریت تأسیسات هسته ای تعیین می کند. علاوه بر این ، Ref. [8] ، بند 3.12 (الف) به اهمیت هسته ای سیستم های مدیریت یکپارچه اشاره دارد. مرجع [3] بحث بیشتر در مورد رابطه کلی بین سیستمهای مدیریت و امنیت رایانه را ارائه می دهد.

4.2. Paragraph 2.13 of Ref. [4] states that:

“In digital I&C systems, demonstration that the final product is fit for its purpose depends greatly, but not exclusively, on the use of a high quality development process that provides for disciplined specification and implementation of design requirements.”

Paragraph 2.14 adds that

“in the nuclear power domain as well as in other safety-critical domains such as aerospace, development processes have been applied that are commonly represented as life cycle models, which describe the activities for the development of electronic systems and the relationships between these activities. … Normally, activities relating to a given development step are grouped into the same phase of the life cycle.”

Computer security should be considered in all phases of the I&C system life cycle.

4.2. بند 2.13 از Ref. [4] اظهار داشت:

"در سیستم های دیجیتال I&C ، نشان دادن اینکه محصول نهایی برای اهداف مناسب است ، بستگی زیادی به استفاده از یک فرایند توسعه با کیفیت بالا دارد که مشخصات انضباطی و اجرای الزامات طراحی را فراهم می کند."

بند 2.14 آن را می افزاید

وی گفت: "در حوزه انرژی هسته ای و همچنین سایر حوزه های ایمنی مانند هوافضا ، از فرآیندهای توسعه استفاده شده است که معمولاً به عنوان مدل چرخه زندگی معرفی می شوند ، که فعالیت های مربوط به توسعه سیستم های الکترونیکی و روابط بین این فعالیت ها را توصیف می کند. ... به طور معمول ، فعالیت های مربوط به یک مرحله توسعه مشخص در همان مرحله از چرخه زندگی گروه بندی می شوند. "

امنیت رایانه باید در تمامی مراحل چرخه عمر سیستم I&C در نظر گرفته شود.

4.3. As stated in Ref. [4], para. 2.17,

“Three fundamental levels of life cycles are needed to describe the development of I&C systems:

1. An overall I&C architecture life cycle; [16]
2. One or more individual I&C system life cycles;
3. One or more individual component life cycles: Component life cycles are typically managed in the framework of platform development and independent of the overall architecture level and the individual system level life cycles. Component life cycles for digital systems are typically divided into separate life cycles for the development of hardware and software.”
4. 4.3 همانطور که در Ref گفته شده است. [4] ، بند 2.17 ،
5. "برای توصیف توسعه سیستم های I&C به سه سطح اساسی چرخه زندگی نیاز است:
6. چرخه زندگی معماری I&C؛ [16]
7. یک یا چند چرخه زندگی سیستم I&C فردی.
8. یک یا چند چرخه زندگی مؤلفه های فردی: چرخه های زندگی جزء به طور معمول در چارچوب توسعه پلتفرم و مستقل از سطح معماری کلی و چرخه های زندگی سیستم سطح فردی اداره می شوند. چرخه عمر کامپوننت برای سیستم های دیجیتال به طور معمول برای توسعه سخت افزار و نرم افزار به چرخه زندگی جداگانه تقسیم می شود. "

4.4. The definition of life cycle models and the activities grouped into each life cycle phase are generally determined by a system’s developers and operators, but the definition and implementation should be a multidisciplinary effort involving many other domains, including computer security. Generally the developers have lead responsibility for the I&C systems until the systems are transferred to the operations organization for installation, integration and commissioning.

4.4 تعریف مدل های چرخه زندگی و فعالیت های گروه بندی شده در هر مرحله چرخه زندگی ، عموما توسط توسعه دهندگان و اپراتورهای سیستم مشخص می شود ، اما تعریف و اجرای باید یک تلاش چند رشته ای باشد که شامل بسیاری از حوزه های دیگر از جمله امنیت رایانه است. بطور کلی توسعه دهندگان مسئولیت اصلی سیستم های I&C را دارند تا اینکه سیستم ها برای نصب ، ادغام و راه اندازی به سازمان عملیات منتقل شوند.

4.5. Given that the life cycle I&C systems can span several decades, different organizations may play the role of developers or other roles during the life cycle of a system. For example, it is not uncommon for a vendor to carry out the original development and for the purchaser to develop modifications at a later time, especially if the modifications are minor. The fact that these modifications are developed by different organizations does not eliminate the need to implement computer security measures in all phases in the I&C system life cycle.

4.5 با توجه به اینکه سیستمهای چرخه زندگی I&C می توانند چندین دهه طول بکشد ، سازمانهای مختلف ممکن است در طول چرخه زندگی یک سیستم نقش توسعه دهندگان یا سایر نقش ها را ایفا کنند. به عنوان مثال ، یک فروشنده غیر معمولی نیست که توسعه اولیه را انجام دهد و خریدار بتواند اصلاحاتی را بعداً انجام دهد ، خصوصاً اگر تغییرات جزئی باشد. این واقعیت که این تغییرات توسط سازمانهای مختلف ایجاد شده است ، لزوم اجرای اقدامات امنیتی رایانه را در کلیه مراحل چرخه عمر سیستم I&C از بین نمی برد.

4.6. At the earliest opportunity, computer security should be coherently planned for all I&C architecture, system and component life cycles. This planning should specify the computer security measures to be applied in each phase to protect the I&C architecture, systems and components from cyber attacks that may jeopardize functions important to safety. The possibility that safety functions or computer security measures may change during later phases should be considered.

4.6. در اولین فرصت ، امنیت رایانه باید بطور منسجم برای کلیه معماری I&C ، چرخه عمر سیستم و مؤلفه ها برنامه ریزی شود. این برنامه ریزی باید اقدامات امنیتی رایانه را که در هر مرحله برای محافظت از معماری I&C ، سیستم ها و مؤلفه ها در برابر حملات سایبری که ممکن است عملکردهای مهم برای ایمنی را به خطر اندازد ، مشخص کند. این احتمال که عملکردهای ایمنی یا اقدامات امنیتی رایانه ممکن است در مراحل بعدی تغییر کند باید در نظر گرفته شود.

4.7. The I&C system development process should seek to minimize potential computer security vulnerabilities and weaknesses and identify the residual potential vulnerabilities and weaknesses in each phase of the I&C system life cycle.

4.7 فرایند توسعه سیستم I&C باید به دنبال به حداقل رساندن آسیب پذیری ها و ضعف های امنیتی رایانه ای و شناسایی مانده باقیمانده باشد

آسیب پذیری و ضعف های احتمالی در هر مرحله از چرخه زندگی سیستم I&C.

* 1. 4.8. While life cycle models may be organized in many ways, the following notional life cycle phases are used in this publication as a framework for describing computer security considerations during the I&C life cycle:Process planning;
  2. Design basis;
  3. Overall I&C architecture and functional allocation;
  4. I&C system requirements specification;
  5. Selection of predeveloped items;
  6. Detailed design and implementation;
  7. System integration;
  8. System validation;
  9. Installation, integration and commissioning;
  10. Operation and maintenance;
  11. Modification;
  12. Decommissioning.

1. 4.8 در حالی که الگوهای چرخه زندگی ممکن است از جهات مختلفی سازماندهی شود ، مراحل چرخه عمر مفهومی زیر در این نشریه به عنوان چارچوبی برای توصیف ملاحظات امنیت رایانه در طی چرخه زندگی I&C استفاده می شود: برنامه ریزی فرآیند؛
2. اساس طراحی؛
3. به طور کلی معماری I&C و تخصیص عملکرد
4. مشخصات مورد نیاز سیستم I & C؛
5. انتخاب موارد از پیش توسعه یافته؛
6. طراحی و اجرای دقیق؛
7. ادغام سیستم؛
8. اعتبارسنجی سیستم؛
9. نصب ، ادغام و راه اندازی؛
10. عملیات و نگهداری؛
11. تغییر؛
12. رد کردن
    1. 4.9. In addition to these phases, the I&C system life cycle also involves many activities that are common to all life cycle phases. The common activities that are important to computer security are:Quality assurance;
    2. Configuration management;
    3. Verification and validation17;
    4. Security assessment;
    5. Documentation.
13. 4.9 علاوه بر این مراحل ، چرخه حیات سیستم I&C همچنین فعالیتهای بسیاری را شامل می شود که برای همه مراحل چرخه زندگی مشترک است. فعالیتهای مشترکی که برای امنیت رایانه مهم است عبارتند از: تضمین کیفیت؛
14. مدیریت پیکربندی؛
15. تأیید و اعتبار 17؛
16. ارزیابی امنیتی؛
17. مستندات.

4.10. The computer security requirements and activities for each life cycle phase should be commensurate with the consequences resulting from unauthorized or inappropriate access, use, disclosure, manipulation, disruption or destruction of the I&C system. Consideration should also be given to the compromise of any system, support system or information that might adversely affect safety or security.

1. 4.10 شرایط و فعالیتهای امنیتی رایانه برای هر مرحله از چرخه زندگی باید متناسب با پیامدهای ناشی از دسترسی غیرمجاز یا نامناسب بودن دسترسی ، استفاده ، افشای اطلاعات ، دستکاری ، اختلال یا از بین رفتن سیستم I&C باشد. همچنین باید به سازش مورد توجه قرار گیرد
2. هر سیستم ، سیستم پشتیبانی یا اطلاعاتی که می تواند بر امنیت یا امنیت تأثیر منفی بگذارد.

4.11. The remainder of this section is divided into subsections that discuss general computer security guidance that applies to all life cycle phases, and security guidance that is specific to the individual life cycle phases. In this discussion, the phases are discussed only once but the guidance should be applied to any life cycle in which the phase occurs.

4.11 بخش باقیمانده این بخش به زیربخشهایی تقسیم می شود که در مورد راهنمای کلی امنیت رایانه که در مورد کلیه مراحل چرخه زندگی اعمال می شود ، و راهنمایی های امنیتی ویژه برای مراحل چرخه زندگی فردی بحث می شود. در این بحث ، مراحل فقط یک بار مورد بحث قرار می گیرد ، اما راهنمایی ها باید برای هر چرخه زندگی که در آن مرحله اتفاق می افتد ، اعمال شوند.

.

GENERAL GUIDANCE FOR COMPUTER SECURITY

راهنمای کلی برای امنیت رایانه

4.12. The computer security policy for a nuclear facility specifies the overall computer security objectives for the facility. For facility and system computer security planning, these objectives are specified in the policy in clear, specific and, when possible, measurable terms. The facility objectives are translated into system objectives. Reference [3] provides further guidance on computer security at nuclear facilities.

4.12 سیاست امنیت رایانه برای یک تاسیسات هسته ای اهداف کلی امنیت رایانه را برای این تاسیسات مشخص می کند. برای برنامه ریزی امنیت سیستم و امکانات رایانه ای ، این اهداف در سیاست به صورت واضح ، مشخص و در صورت امکان با اندازه گیری مشخص می شوند. اهداف تسهیلات به اهداف سیستم ترجمه می شوند. مرجع [3] راهنمایی های بیشتری در مورد امنیت رایانه در تأسیسات هسته ای ارائه می دهد.

4.13. The computer security policy should include elements addressing the security of I&C systems and, consequently, the policy should apply to any organization that is responsible for activities in the I&C system life cycle. These organizations include operators, vendors, contractors and suppliers that design, implement and procure I&C systems, software and components.

4.13 سیاست امنیت رایانه باید شامل عناصری باشد که به امنیت سیستم های I&C بپردازند و در نتیجه ، این سیاست باید برای هر سازمانی که مسئولیت فعالیت در چرخه زندگی سیستم I&C را بر عهده دارد ، اعمال شود. این سازمان ها شامل اپراتورها ، فروشندگان ، پیمانکاران و تأمین کنندگان هستند که سیستم ها ، نرم افزارها و اجزای I&C را طراحی ، پیاده سازی و تهیه می کنند.

4.14. Each organization responsible for I&C life cycle activities should identify and document the standards and procedures that conform with the applicable security policies to ensure the hardware, software and firmware minimize undocumented code (e.g. back door coding), malicious code (e.g. intrusions, viruses, worms, Trojan horses and logic bombs) and other unwanted, unnecessary or undocumented functions or applications, with the aim of minimizing the number of possible pathways through which a cyber attack could take place.

4.14 هر سازمان مسئول فعالیتهای چرخه زندگی I&C باید استانداردها و رویه های مطابق با سیاستهای امنیتی قابل اجرا را شناسایی و مستند سازد تا از سخت افزار ، نرم افزار و سیستم عامل کد به حداقل رساندن کد غیر مستند (به عنوان مثال رمزگذاری در پشت درب) ، کد مخرب (به عنوان مثال نفوذ ، ویروس ، کرم) استفاده کند. ، اسب های تروجان و بمب های منطقی) و سایر کارکردها یا برنامه های ناخواسته ، غیر ضروری یا بدون سند ، با هدف به حداقل رساندن تعداد مسیرهای ممکن که از طریق آن می توان حمله سایبری انجام داد

4.15. The computer security policy, programme, associated standards and applicable procedures should address each individual phase of the I&C system life cycle to protect the facility’s I&C systems against compromise.

4.15 سیاست امنیتی رایانه ، برنامه ، استانداردهای مرتبط و رویه های کاربردی باید هر مرحله جداگانه از چرخه عمر سیستم I&C را مورد بررسی قرار دهد تا از سیستم های I&C تأسیسات در برابر سازش محافظت کند.

4.16. Computer security policies, programme, standards and procedures as well as all computer security measures should meet regulatory and computer security requirements.

4.16 سیاست های امنیتی رایانه ، برنامه ، استانداردها و رویه ها و همچنین کلیه اقدامات امنیتی رایانه باید الزامات نظارتی و امنیتی رایانه را برآورده سازند.

4.17. Computer security policies, standards and procedures may be provided in an organization’s I&C security programme or may be incorporated into the I&C system life cycle plans. In practice, a mixed approach is often taken.

ASPECTS OF THE COMPUTER SECURITY POLICY RELATED TO I&C SYSTEMS

4.17 سیاست ها ، استانداردها و رویه های امنیتی رایانه ممکن است در برنامه امنیتی I&C یک سازمان ارائه شده باشد یا ممکن است در برنامه های چرخه زندگی سیستم I&C گنجانیده شود. در عمل ، اغلب یک رویکرد مختلط انجام می شود.

جنبه های سیاست امنیت رایانه مربوط به سیستم های I&C

4.18. The computer security policy for nuclear facilities should describe the application of a graded approach to the implementation of computer security measures for I&C systems. The graded approach should be applied in accordance with the importance for safety and security of each I&C system function (e.g. in accordance with the assigned security level of each system). Management should set and enforce clear computer security policy objectives consistent with overall facility safety and security objectives, and specifically address the security of I&C systems. More detail on general considerations for a computer security policy and programme are identified in Ref. [3].

4.18 سیاست امنیت رایانه برای تأسیسات هسته ای باید از رویکرد تدریجی در اجرای اقدامات امنیتی رایانه برای سیستم های I&C استفاده کند. رویکرد درجه بندی شده باید مطابق با اهمیت برای ایمنی و امنیت هر عملکرد سیستم I&C (به عنوان مثال مطابق با سطح امنیتی اختصاصی هر سیستم) اعمال شود. مدیریت باید اهداف سیاست امنیت رایانهای کاملاً مطابق با اهداف کلی ایمنی و امنیتی را تنظیم و اجرا کند ، و بطور خاص امنیت سیستم های I&C را مورد توجه قرار دهد. جزئیات بیشتر در مورد ملاحظات عمومی برای یک سیاست و برنامه امنیتی رایانه در Ref مشخص شده است. [3]

* 1. 4.19. The computer security policy should include considerations important for I&C systems, such as:Access control, including both physical and logical access control, and use of least privileges.
  2. Configuration and asset management, including password management, patch management, system usage, system hardening, configuration control, restrictions on use of mobile devices and removable media, wireless devices and networks and remote access;
  3. System and component integrity verification activities;
  4. Procurement processes;
  5. Risk and threat management, including processes to gather, analyse, document and share with others who have a need to know and to act upon information about vulnerabilities, weaknesses and threats);
  6. Incident response and recovery;
  7. Auditing and assessments.

1. 4.19 سیاست امنیت رایانه باید ملاحظات مهمی برای سیستمهای I&C باشد ، از جمله: کنترل دسترسی ، از جمله کنترل دسترسی فیزیکی و منطقی ، و استفاده از حداقل امتیازات.
2. پیکربندی و مدیریت دارایی ، از جمله مدیریت رمز عبور ، مدیریت پچ ، استفاده از سیستم ، سخت شدن سیستم ، کنترل پیکربندی ، محدودیت در استفاده از دستگاه های تلفن همراه و رسانه های قابل جابجایی ، دستگاه های بی سیم و شبکه ها و دسترسی از راه دور.
3. فعالیت های تأیید صداقت سیستم و مؤلفه ها؛
4. فرآیندهای تهیه؛
5. مدیریت خطر و تهدید ، از جمله فرایندهای جمع آوری ، تجزیه و تحلیل ، مستند سازی و به اشتراک گذاری با دیگران که نیاز به دانستن و اقدام به اطلاعات در مورد آسیب پذیری ها ، نقاط ضعف و تهدید دارند).
6. پاسخ حادثه و بهبودی؛
7. حسابرسی و ارزیابی.

4.20. The computer security policy should assign roles and responsibilities to organizations or individuals that perform I&C system life cycle activities.

4.20 سیاست امنیت رایانه باید نقشها و مسئولیتها را به سازمانها یا افرادی كه فعالیتهای چرخه عمر سیستم I&C را انجام می دهند اختصاص دهد.

COMPUTER SECURITY PROGRAMME

برنامه امنیت رایانه

4.21. Each organization that has responsibility for implementing I&C system life cycle activities should develop and implement an integrated or separate computer security programme addressing I&C systems.

4.21 هر سازمانی که وظیفه اجرای فعالیتهای چرخه زندگی سیستم I&C را بر عهده دارد ، باید یک برنامه امنیتی رایانه ای یکپارچه یا جداگانه را برای سیستم های I&C تهیه و اجرا کند.

4.22. The computer security programme should define the roles and responsibilities for each phase of the I&C system life cycle for every I&C system.

4.22 برنامه امنیت رایانه باید نقش ها و مسئولیت های مربوط به هر مرحله از چرخه عمر سیستم I&C را برای هر سیستم I&C تعریف کند.

4.23. The computer security programme should specify that responsible organizations apply the concept of defence in depth and identify applicable computer security measures for I&C systems according to their assigned security level.

4.23 برنامه امنیت رایانه باید مشخص كند كه سازمان های مسئول مفهوم دفاع را به طور عمیق به كار می گیرند و اقدامات امنیتی رایانه ای قابل اجرا برای سیستم های I&C را مطابق با سطح امنیتی اختصاص داده شده خود شناسایی می كنند.

4.24. The computer security programme should specify the implementation of computer security measures intended to protect against malicious acts committed by insiders and the manipulation of the I&C system (including its integrity) in each phase of the I&C system life cycle.

4.24 برنامه امنیت رایانه باید اجرای اقدامات امنیتی رایانه را برای محافظت در برابر اقدامات مخرب انجام شده توسط خودی ها و دستکاری در سیستم I&C (از جمله صداقت آن) در هر مرحله از چرخه عمر سیستم I&C مشخص کند.

4.25. The computer security programme should specify that access to I&C systems, components, software, configuration data and tools is controlled during all phases of the I&C system life cycle. Examples of access control practices are the principle of least privilege and need-to-know.

4.25 برنامه امنیتی رایانه باید مشخص کند که دسترسی به سیستم های I&C ، مؤلفه ها ، نرم افزار ، داده های پیکربندی و ابزار در تمام مراحل چرخه عمر سیستم I&C کنترل می شود. نمونه هایی از شیوه های کنترل دسترسی اصل کمترین امتیاز و نیاز به دانستن است

4.26. The computer security programme should address the confidentiality of computer security measures, including the protection of related documentation, consistent with the security level of the I&C systems referred to in the documentation.

4.26 برنامه امنیتی رایانه باید محرمانه بودن اقدامات امنیتی رایانه ، از جمله حفاظت از اسناد مربوطه ، مطابق با سطح امنیتی سیستم های I&C ذکر شده در اسناد را برطرف سازد.

4.27. The computer security programme should address potential computer security vulnerabilities and weaknesses for each phase of the I&C system life cycle.

4.27 برنامه امنیت رایانه باید آسیب پذیری ها و نقاط ضعف امنیتی رایانه ای را برای هر مرحله از چرخه عمر سیستم I&C بررسی کند.

4.28. The computer security programme should identify the process by which I&C system security information, such as details regarding vulnerabilities found in facility I&C systems or the specific defences being used to protect the systems, is classified as sensitive information and compartmentalized18. Reference [8]

defines sensitive information as “Information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security.”

4.28 برنامه امنیت رایانه باید فرایندی را که توسط آن اطلاعات امنیتی سیستم I&C مانند جزئیات مربوط به آسیب پذیری های موجود در سیستم های I&C یا دفاع ویژه ای که برای محافظت از سیستم ها استفاده می شود ، شناسایی کند و به عنوان اطلاعات حساس طبقه بندی و به صورت جزئی تقسیم شود. مرجع [8]

اطلاعات حساس را به عنوان "اطلاعات ، به هر شکلی از جمله نرم افزار ، افشای غیر مجاز ، اصلاح ، تغییر ، تخریب یا انکار استفاده از آنها می تواند امنیت هسته ای را به خطر اندازد."

4.29. Nuclear facilities and associated organizations are strongly encouraged to share other non-sensitive vulnerability information so that facilities will be better prepared in the event that vulnerability information on I&C systems is distributed and shared among potential adversaries. Guidance on the security of nuclear information (including classification) is provided in Ref. [15].

4.29 تأسیسات هسته ای و سازمان های مرتبط به شدت برای تشویق سایر اطلاعات در مورد آسیب پذیری غیر حساس تشویق می شوند تا در صورت تهیه اطلاعات آسیب پذیری در سیستم های I&C بین مخالفان بالقوه ، اطلاعات بهتری تهیه شود. راهنمایی در مورد امنیت اطلاعات هسته ای (از جمله طبقه بندی) در Ref ارائه شده است. [15]

4.30. The computer security programme for I&C systems should specify that periodic computer security reviews and assessments be performed and documented in each life cycle phase.

4.30 برنامه امنیت رایانه برای سیستم های I&C باید مشخص کند که بررسی ها و ارزیابی های دوره ای مربوط به امنیت رایانه در هر مرحله از چرخه زندگی انجام و مستند می شود.

4.31. The computer security programme should specify the computer security measures that provide for a secure environment in which development activities may take place.

4.31 برنامه امنیت رایانه باید اقدامات امنیتی رایانه را مشخص کند که یک محیط امن را فراهم کند که در آن فعالیت های توسعه ای ممکن است انجام شود.

4.32. For legacy I&C systems, there may be more reliance on administrative control measures and isolation than for contemporary systems. The computer security programme should identify and sustain additional compensatory computer security measures that are necessary to ensure computer security for legacy I&C systems.

4.32 برای سیستم های I&C میراث ، نسبت به سیستم های معاصر ممکن است اعتماد به نفس بیشتری نسبت به سیستم های کنترل اداری و انزوا داشته باشد. برنامه امنیت رایانه باید اقدامات امنیتی جبران كننده رایانه دیگری را كه برای اطمینان از امنیت رایانه برای سیستمهای میراث I&C ضروری است ، شناسایی و حفظ كند.

SECURE DEVELOPMENT ENVIRONMENT

محیط امن برای توسعه

4.33. The guidance contained within paras 4.34–4.40 applies to the development of all I&C systems, subsystems and components to which a graded approach to computer security is applied in accordance with their assigned security level.

4.33 راهنمایی های موجود در پاراگراف 4.34-4.40 برای توسعه همه سیستم های I&C ، زیر سیستم ها و مؤلفه هایی که رویکرد درجه بندی شده به امنیت رایانه مطابق با سطح امنیتی اختصاص یافته آنها اعمال می شود ، اعمال می شود.

.

4.34. I&C system development should be conducted in a secure development environment. This applies to both internal and external sites. The assignment of a security level to this environment should consider the security level of the system in the target environment, the security level of other systems developed or stored within the common development environment and the development tools. The environment’s computer security measures should be evaluated to confirm conformance with requirements of the assigned security level.

4.34 توسعه سیستم I&C باید در یک محیط توسعه امن انجام شود. این موضوع در مورد سایتهای داخلی و خارجی صدق می کند. اختصاص سطح امنیتی به این محیط باید سطح امنیتی سیستم را در محیط هدف ، سطح امنیتی سایر سیستمهای توسعه یافته یا ذخیره شده در محیط توسعه مشترک و ابزارهای توسعه در نظر بگیرد. برای تأیید مطابقت با الزامات سطح امنیتی اختصاص یافته ، اقدامات امنیتی رایانه ای محیط باید ارزیابی شود.

4.35. The secure development environment should include administrative control measures, such as configuration control and asset management.

4.35 محیط توسعه امن باید شامل اقدامات كنترل اداری مانند كنترل تنظیمات و مدیریت دارایی باشد

4.36. Physical control measures should be used to control access to secure development environments.

4.36 برای کنترل دسترسی به محیط های توسعه ایمن باید از اقدامات کنترل فیزیکی استفاده شود.

4.37. Test and support equipment used in I&C development environments should be verified to confirm that use of this equipment does not provide pathways for the introduction of malicious code or data into the secure development environment.

4.37 تجهیزات آزمایش و پشتیبانی مورد استفاده در محیط های توسعه I&C باید تأیید شوند تا تأیید شود که استفاده از این تجهیزات مسیر ورود کد یا داده های مخرب را به محیط توسعه امن فراهم نمی کند

4.38. Computer security measures should be in place to control the movement of data and devices for all development phases to ensure that malicious code or data is not introduced into secure development environments and to protect sensitive information associated with I&C systems. These computer security measures should include administrative and technical control measures such as usage restrictions and procedures for the control of removable media and mobile devices. The secure development environment should be recognized as a distinct environment that is both physically and logically separated from the operational and corporate business environments.

4.38 اقدامات امنیتی رایانه باید برای کنترل حرکت داده ها و دستگاه ها در تمام مراحل توسعه صورت گیرد تا اطمینان حاصل شود که کد یا داده های مخرب در محیط های توسعه ایمن وارد نشده اند و از اطلاعات حساس مرتبط با سیستم های I&C محافظت می شود. این اقدامات امنیتی رایانه باید شامل اقدامات کنترل اداری و فنی مانند محدودیت استفاده و رویه هایی برای کنترل رسانه های قابل حمل و دستگاه های تلفن همراه باشد. محیط توسعه امن باید به عنوان یک محیط مشخص شناخته شود که هم از نظر جسمی و هم از نظر منطقی از محیط های عملیاتی و شرکتی جدا باشد.

4.39. Computer security measures should be implemented to protect the integrity of the secure development environment as well as of design inputs and outputs (e.g. data, configuration files, software updates and software patches) during transfers between the secure development environment and the target environment. These measures could include automated asset configuration systems where the security benefit for the secure development and target environments has been confirmed by analysis.

4.39 اقدامات امنیتی رایانه باید برای محافظت از یکپارچگی محیط توسعه امن و همچنین ورودی ها و خروجی های طراحی (به عنوان مثال داده ها ، پرونده های پیکربندی ، به روزرسانی های نرم افزاری و تکه های نرم افزار) در حین انتقال بین محیط توسعه ایمن و محیط هدف انجام شود. این اقدامات می تواند شامل سیستم های پیکربندی دارایی های خودکار باشد که در آن منافع امنیتی برای توسعه امن و محیط های هدف با تجزیه و تحلیل تأیید شده است.

4.40. Third party or vendor tools used for I&C system development should be tested, validated and protected commensurate with the assigned security level of the development environment.

4.40 ابزارهای شخص ثالث یا فروشنده که برای توسعه سیستم I&C مورد استفاده قرار می گیرند باید متناسب با سطح امنیتی اختصاص داده شده در محیط توسعه ، مورد آزمایش ، اعتبار و محافظت قرار گیرند.

CONTINGENCY PLANS

برنامه های احتمالی

4.41. Organizations that implement one or more I&C system life cycle activities should develop contingency plans and procedures to prevent escalation and progression of anomalous behaviour and to recover from computer security incidents. These contingency plans and procedures should be reviewed, periodically exercised and updated when deficiencies are discovered.

4.41 سازمانهایی که یک یا چند فعالیت چرخه حیات سیستم I&C را اجرا می کنند ، باید برنامه ها و مراحل احتمالی را برای جلوگیری از تشدید و پیشرفت رفتار غیر عادی و بهبودی از حوادث امنیتی رایانه تهیه کنند. این برنامه ها و رویه های احتمالی باید هنگام کشف نواقص مورد بازنگری ، ورزش و به روز رسانی قرار گیرند.

4.42. The operator should develop a computer security incident response plan consisting of procedures that define, identify and respond to possible abnormal or suspicious behaviour detected on I&C and associated systems.

4.42 اپراتور باید یک برنامه پاسخگویی به حادثه امنیتی رایانه را تشکیل دهد که شامل رویه هایی است که رفتارهای غیرطبیعی یا مشکوک احتمالی را که در I&C و سیستم های همراه شناسایی شده ، تعریف ، شناسایی و پاسخ می دهد.

4.43. The computer security incident response plan should address information collection and legal requirements for evidence preservation during security events to support investigative analysis.

4.43 برنامه پاسخگویی به حادثه امنیت رایانه باید از مجموعه اطلاعات و الزامات قانونی برای حفظ شواهد در حین وقایع امنیتی ، پشتیبانی کند تا از تحقیقات تحقیقاتی پشتیبانی كند.

4.44. The computer security incident response plan should assign personnel to the facility computer security incident response team. This team should be available at the facility to respond to any identified computer security incident. Assigned personnel may include those having I&C system specific or computer security expertise.

4.44 برنامه پاسخ حادثه امنیت رایانه باید پرسنل را به تیم پاسخگوی حادثه امنیت رایانه اختصاص دهد. این تیم باید برای پاسخ به هرگونه حادثه امنیتی رایانه ای شناسایی شده در این مرکز در دسترس باشد. پرسنل اختصاصی ممکن است شامل افرادی باشند که دارای سیستم خاص I&C یا امنیت امنیتی رایانه هستند.

4.45. I&C system backup and restoration copies important to contingency plans and procedures should include software, essential data and configuration files. These copies should be stored in a physical location separate from the source location to guard against common cause failure. Computer security measures should be used to protect these copies against theft, tampering, and deletion or destruction.

I&C VENDORS, CONTRACTORS AND SUPPLIERS

4.45 نسخه پشتیبان تهیه و ترمیم سیستم I&C مهم برای برنامه ها و مراحل اضطراری باید شامل نرم افزار ، داده های ضروری و پرونده های پیکربندی باشد. این نسخه ها باید در یک مکان فیزیکی جدا از محل منبع ذخیره شوند تا در برابر خرابی علت مشترک محافظت کنند. از اقدامات امنیتی رایانه ای برای محافظت از این نسخه ها در برابر سرقت ، دستکاری و حذف یا تخریب استفاده می شود.

مناقصه های I&C ، پیمانکاران و توزیع کنندگان

4.46. In paras 4.47–4.53, ‘vendors’, ‘contractors’ and ‘suppliers’ are those who supply the nuclear facility with digital equipment, software and services for I&C systems to which a graded approach to computer security is applied in accordance with the assigned security level of the system. The operator should enforce the application of the guidance contained within paras 4.47–4.53 via the execution of a contract with the vendors, contractors or suppliers in question.

4.46 در بندهای 4.47-4.53 ، "فروشندگان" ، "پیمانکاران" و "تأمین کنندگان" کسانی هستند که تأسیسات هسته ای را با تجهیزات دیجیتال ، نرم افزار و خدمات سیستم های I&C تهیه می کنند که رویکرد درجه بندی شده ای برای امنیت رایانه مطابق با امنیت اختصاص یافته اعمال می شود. سطح سیستم. اپراتور باید از طریق اجرای قرارداد با فروشندگان ، پیمانکاران یا تأمین کنندگان مورد نظر ، دستورالعمل موجود در بندهای 4.47-4.53 را اجرا کند.

4.47. Vendor and sub-vendor organizations should have robust and verifiable computer security processes.

4.47 سازمان های فروشنده و فروشندگان فرایندها باید دارای فرایندهای امنیتی رایانه ای قوی و قابل تأیید باشند.

4.48. Vendors, contractors and suppliers should meet all applicable computer security requirements. This includes the application of computer security measures specified by the operator, during support provided on-site or at the vendor, contractor or supplier’s workplace and during any transit or storage of purchased goods.

4.48 فروشندگان ، پیمانکاران و تأمین کنندگان باید کلیه الزامات امنیتی رایانه کاربردی را برآورده کنند. این شامل استفاده از اقدامات امنیتی رایانه ای است که توسط اپراتور ، در حین پشتیبانی ارائه شده در محل یا در محل کار فروشنده ، پیمانکار یا تأمین کننده و در طی هرگونه ترانزیت یا ذخیره کالاهای خریداری شده ارائه شده است.

4.49. The vendor, contractor or supplier should have a computer security management process.

4.49 فروشنده ، پیمانکار یا تأمین کننده باید یک فرایند مدیریت امنیت رایانه داشته باشد.

4.50. The applicable computer security requirements at sites where a vendor, contractor or supplier performs activities with I&C systems should be clearly and contractually specified by the operator based on the assigned security level of the system, subsystem or component.

4.50 الزامات امنیتی رایانه ای قابل اجرا در سایتهایی که فروشنده ، پیمانکار یا تأمین کننده فعالیت هایی را با سیستم های I&C انجام می دهند باید براساس سطح امنیتی اختصاصی سیستم ، زیر سیستم یا مؤلفه توسط اپراتور به طور واضح و قراردادی مشخص شود.

4.51. A process should exist to enable the operator and the vendor, contractor or supplier to report vulnerabilities to one another and to coordinate response and mitigation efforts.

4.51 فرایندی باید وجود داشته باشد تا اپراتور و فروشنده ، پیمانکار یا تأمین کننده بتوانند آسیب پذیری ها را به یکدیگر گزارش دهند و هماهنگی های لازم برای پاسخگویی و کاهش آنها را انجام دهند.

4.52. The vendor, contractor or supplier should demonstrate that it has a credible mechanism for receiving reports of vulnerabilities, assessing them and reporting them to the nuclear facility during the entire period of their contractual service. This consideration may extend beyond any normal warranty period to support the life cycle of the installed equipment. In these cases, the mechanism should be included for the extended period within the contractual obligations agreed upon by the vendors, contractors or suppliers.

4.52 فروشنده ، پیمانکار یا تأمین کننده باید نشان دهد که دارای مکانیزم معتبر برای دریافت گزارش از آسیب پذیری ها ، ارزیابی آنها و گزارش آنها در تأسیسات هسته ای در کل دوره خدمات پیمانکاری خود است. این در نظر گرفتن ممکن است فراتر از هر دوره ضمانت عادی برای پشتیبانی از چرخه عمر تجهیزات نصب شده گسترش یابد. در این موارد ، سازوکار باید برای مدت طولانی در تعهدات قراردادی مورد توافق فروشندگان ، پیمانکاران یا تأمین کنندگان قرار گیرد.

4.53. Audits and assessment of vendors, contractors or suppliers responsible for I&C design, development, integration and maintenance should be conducted and the results reported to the operator.

4.53 حسابرسی و ارزیابی از فروشندگان ، پیمانکاران یا تأمین کنندگان مسئول طراحی I&C ، توسعه ، ادغام و نگهداری باید انجام شود و نتایج به اپراتور گزارش شود.

COMPUTER SECURITY TRAINING

آموزش ایمنی رایانه

4.54. All personnel performing work involving I&C systems, including work involving sensitive information associated with these systems, should receive periodic training on computer security awareness and procedures.

4.54 کلیه پرسنلی که کارهای مربوط به سیستمهای I&C را انجام می دهند ، از جمله کارهایی که شامل اطلاعات حساس مرتبط با این سیستم ها هستند ، باید آموزش دوره ای در مورد آگاهی و روش های امنیتی رایانه دریافت کنند.

4.55. All personnel who have physical or logical access to I&C systems should be qualified consistent with their computer security responsibilities and should receive specialized security training for I&C systems based upon their roles and responsibilities to maintain their qualification.

4.55 کلیه پرسنلی که دسترسی فیزیکی یا منطقی به سیستمهای I&C دارند باید با مسئولیتهای امنیتی رایانه خود مطابقت داشته باشند و برای حفظ صلاحیت خود باید آموزش های ویژه امنیتی را برای سیستمهای I&C دریافت کنند.

4.56. All personnel who have physical or logical access to I&C systems should be trained to a competency level appropriate to their roles to support computer security tasks and recognize potential computer security incidents. These individuals may be informed of the impact of changes made on either the I&C system or its associated computer security measures to which they have access.

4.56 کلیه پرسنلی که دسترسی فیزیکی یا منطقی به سیستمهای I&C دارند باید در سطح صلاحیت متناسب با نقش خود آموزش ببینند تا از وظایف امنیتی رایانه و شناسایی حوادث احتمالی امنیت رایانه ای پشتیبانی کنند. این افراد ممکن است از تأثیر تغییرات ایجاد شده در سیستم I&C یا اقدامات امنیتی رایانه ای مرتبط با آنها که به آنها دسترسی دارند مطلع شوند.

4.57. Personnel identified as computer security incident response team members should receive training on computer security incident identification and response. This may involve the use of an I&C test bed as a component of the I&C security training programme.

4.57 پرسنلی که به عنوان اعضای تیم واکنش حوادث امنیتی رایانه ای شناخته می شوند ، باید آموزش درمورد شناسایی و پاسخ حادثه امنیتی رایانه را دریافت کنند. این ممکن است استفاده از تخت تست I&C به عنوان جزئی از برنامه آموزش امنیتی I&C باشد.

4.58. Engineering, operations and maintenance staff should be trained to maintain both safety and security functions of I&C systems.

4.58 مهندسي ، عمليات و كاركنان نگهداري بايد آموزش داده شوند تا هم سيستم هاي امنيتي و هم امنيت سيستم هاي I&C را حفظ كنند.

4.59. I&C design personnel should receive training on secure design and programming for I&C systems for nuclear facilities (e.g. how to consider security in software design).

4.59 كاركنان طراحي I&C بايد در زمينه طراحي و برنامه ريزي امن براي سيستم هاي I&C براي تأسيسات هسته اي آموزش هاي لازم را بدست آورند (براي مثال ، در نظر گرفتن امنيت در طراحي نرم افزار)

COMMON ELEMENTS OF ALL LIFE CYCLE PHASES

عناصر مشترک کلیه مراحل چرخه زندگی

4.60. In most cases, the Safety Requirements for the management system [14] and the general guidance contained in the associated Safety Guides [16, 17] provide sufficient guidance for management system activities related to computer security in all phases of the I&C system life cycle. There are a few areas, however, where more specific guidance is warranted.

4.60 در اکثر موارد ، الزامات ایمنی برای سیستم مدیریت [14] و راهنمایی های عمومی موجود در راهنماهای ایمنی مرتبط [16 ، 17] راهنمایی کافی برای فعالیت های سیستم مدیریت مربوط به امنیت رایانه در کلیه مراحل چرخه عمر سیستم I&C ارائه می دهند. با این حال ، برخی از زمینه ها وجود دارد که راهنمایی های خاص بیشتری را لازم می داند.

**Management systems**

سیستم های مدیریت

4.61. The guidance contained within paras 4.62–4.70 applies to all organizations that perform one or more life cycle activities relevant to I&C systems to which a graded approach to computer security is applied in accordance with the security level assigned to the system.

4.61 راهنمایی های موجود در پاراگراف 4.62-4.70 برای کلیه سازمانهایی که یک یا چند فعالیت چرخه زندگی مربوط به سیستم های I&C را انجام می دهند ، اعمال می شود.

4.62. The Safety Requirements 6–8 for management systems in Ref. [14], paras 4.8–4.20, should be consulted when drafting regulatory and/or computer security requirements related to management systems.

4.62 الزامات ایمنی 6-8 برای سیستم های مدیریت در Ref. [14] ، پاراگراف 4.8-4.20 ، هنگام تهیه الزامات نظارتی و / یا امنیت رایانه مربوط به سیستم های مدیریت باید با آنها مشورت شود.

4.63. Each organization that is responsible for developing, deploying, operating, maintaining or retiring I&C systems or components should consider computer security for I&C systems in its integrated management system.

4.63 هر سازمانی که وظیفه توسعه ، استقرار ، بهره برداری ، حفظ یا بازنشستگی سیستم ها یا قطعات I&C را بر عهده دارد ، باید امنیت رایانه ای را برای سیستم های I&C در سیستم مدیریت یکپارچه خود در نظر بگیرد.

4.64. The integrated management system of the facility should support computer security processes and procedures.

4.64 سیستم مدیریت یکپارچه تسهیلات باید از فرایندها و رویه های امنیتی رایانه پشتیبانی کند.

4.65. Life cycle activities should be conducted within the framework of a management system providing for adequate arrangements for security of I&C systems and components.

4.65 فعالیت های چرخه زندگی باید در چارچوب یک سیستم مدیریتی انجام شود که مقدمات لازم برای امنیت سیستم ها و مؤلفه های I&C را فراهم کند.

4.66. Auditable processes and procedures should be in place to confirm that I&C systems, subsystems and components that are important for maintaining computer security continue to perform their security functions throughout their operational lives.

4.66 فرایندها و رویه های قابل شنیدن باید تأیید شود که سیستم های I&C ، زیر سیستم ها و مؤلفه هایی که برای حفظ امنیت رایانه مهم هستند ، همچنان عملکردهای امنیتی خود را در طول زندگی عملیاتی خود انجام می دهند.

4.67. Provision should be made for security examinations of I&C systems (e.g. inspections for configuration) throughout the entire I&C system life cycle to demonstrate that security procedures have been followed and the required standard of workmanship has been achieved (e.g. no extra components have been added).

4.67 باید معاینات امنیتی سیستم های I&C (مثلاً بازرسی ها برای پیکربندی) در کل چرخه عمر سیستم I&C فراهم شود تا نشان دهد که رویه های امنیتی رعایت شده اند و استاندارد موردنیاز کار بدست آمده است (به عنوان مثال هیچ مؤلفه دیگری اضافه نشده است).

4.68. Independent19 inspections should be conducted to check that computer security processes and procedures are carried out as described by the operator’s quality assurance plan.

4.68 بازرسی های Independent19 باید انجام شود تا بررسی شود که فرایندها و رویه های امنیتی رایانه مطابق با برنامه تضمین کیفیت اپراتور انجام شده است.

4.69. Detailed records of life cycle activities should be produced and retained in such a way as to allow review of these records and comparison with computer security requirements at any time. These records should include all computer security incidents and the response or contingency actions taken following the incidents.

4.69 سوابق تفصیلی از فعالیت های چرخه زندگی باید به گونه ای تهیه و نگهداری شود که امکان بررسی این سوابق و مقایسه آنها با نیازهای رایانه ای در هر زمان فراهم شود. این سوابق باید شامل تمام حوادث امنیتی رایانه و واکنش یا اقدامات احتمالی انجام شده به دنبال حوادث باشد.

4.70. Authorized individuals having privileged logical or physical access to I&C systems should be subject to trustworthiness evaluation, computer security training and behavioural observation consistent with the facility insider mitigation programme or equivalent (see Ref. [5]).

4.70 افراد مجاز با دسترسی منطقی یا بدنی ممتاز به سیستم های I&C باید تحت ارزیابی ارزیابی اعتبار ، آموزش امنیت رایانه و مشاهده رفتار متناسب با برنامه کاهش خودی تسهیلات یا معادل آن باشند (رجوع کنید به مراجعه کنید به [5]).

**Computer security reviews and audits**

بررسیهای امنیتی رایانه و ممیزی ها

4.71. The guidance contained within paras 4.72–4.77 applies to all organizations that perform one or more life cycle activities relevant to I&C systems to which a graded approach to computer security is applied in accordance with its assigned security level.

4.71 راهنمایی های موجود در بندهای 4.72-4.77 برای کلیه سازمان هایی که یک یا چند فعالیت چرخه زندگی مربوط به سیستم های I&C را انجام می دهند ، اعمال می شود.

4.72. Computer security reviews and audits of I&C systems and associated activities should be performed on a regular basis to verify compliance with regulations, computer security policy and good practices for I&C system security.

4.72 بررسیهای امنیتی رایانه و ممیزی سیستمهای I&C و فعالیتهای مرتبط با آن باید بطور منظم انجام شود تا تطابق با مقررات ، سیاست امنیت رایانه و شیوه های خوب برای امنیت سیستم I&C تأیید شود.

4.73. Computer security reviews of I&C systems should be independent and performed by qualified internal and/or external reviewers.

4.73 بررسی های امنیتی رایانه ای سیستم های I&C باید مستقل و توسط داوران داخلی و / یا خارجی واجد شرایط انجام شود.

4.74. Policies and procedures including roles and responsibilities for conducting such reviews should be defined and documented.

4.74 سیاست ها و رویه هایی از جمله نقش ها و مسئولیت های انجام چنین بررسی هایی باید تعریف و مستند شود.

4.75. Computer security reviews of I&C systems should verify the implementation and effectiveness of their associated computer security measures.

4.75 بررسیهای امنیتی رایانه سیستمهای I&C باید عملکرد و اثربخشی اقدامات امنیتی رایانه ای مرتبط با آنها را تأیید کند.

4.76. Intrusive assessment testing should not be conducted against operational I&C systems. Intrusive assessment testing involves attempting to exploit a vulnerability (e.g. as in penetration testing) that may change either the operating conditions or the configuration of the I&C system outside its design basis. The operator should consider using controlled methods to perform payload-free tests while the facility is in a condition in which URC are prevented; for example, if the facility is in a shutdown or defuelled state. Facility policies and procedures should address the conduct and performance of these tests. These tests should be designed specifically for each system. Intrusive assessment tests should involve the computer security incident response team.

4.76 آزمایش ارزیابی مقدماتی نباید علیه سیستم های عملیاتی I&C انجام شود. آزمایش ارزیابی مقدماتی شامل تلاش برای سوءاستفاده از آسیب پذیری است (به عنوان مثال در تست نفوذ) که ممکن است شرایط عملیاتی یا پیکربندی سیستم I&C را خارج از مبنای طراحی آن تغییر دهد. اپراتور باید از روشهای کنترل شده برای انجام آزمایشات بدون بار استفاده کند ، در حالی که تسهیلات در شرایطی است که از URC جلوگیری می شود. به عنوان مثال ، اگر تسهیلات در حالت خاموش یا پیش فرض قرار دارد. خط مشی ها و رویه های تسهیلات باید به عملکرد و عملکرد این تست ها بپردازند. این تست ها باید بطور اختصاصی برای هر سیستم طراحی شوند. تست های ارزیابی جذاب باید تیم پاسخگوی حادثه امنیت رایانه باشد.

4.77. Records of computer security reviews and associated analysis data should be archived, maintained and protected throughout the entire life cycle of the I&C system.

4.77 سوابق بررسی امنیت رایانه و داده های تحلیل همراه باید بایگانی ، نگهداری و محافظت شوند و در کل چرخه زندگی سیستم I&C محافظت شوند.

**Configuration management for computer security**

مدیریت پیکربندی برای امنیت رایانه

4.78. The guidance provided in paras 4.79–4.87 applies to all I&C systems, subsystems and components having an assigned security level.

4.78 راهنمایی های ارائه شده در بندهای 4.79-4.87 در مورد کلیه سیستمهای I&C ، زیر سیستمها و مؤلفههای دارای سطح امنیتی اختصاصی اعمال می شود.

4.79. Software configuration control activities may assist in preventing and detecting computer security incidents, although the primary purpose of these activities is not to address specific nuclear security objectives. The computer security benefit gained by performing these activities should be analysed and confirmed prior to taking credit for such benefits. For example, a computer security incident could be detected through these activities but the timing of the initiation of the response to a detected incident would likely be insufficient to protect the system, compared with the timing of a response in a computer security

system that incorporates layered computer security measures with automatic response elements.

4.79 فعالیت های کنترل پیکربندی نرم افزار ممکن است در جلوگیری و کشف حوادث امنیتی رایانه کمک کند ، اگرچه هدف اصلی این فعالیت ها رسیدگی به اهداف امنیتی هسته ای خاص نیست. منافع امنیت رایانه ای که با انجام این فعالیت ها به دست می آید ، باید قبل از گرفتن اعتبار برای چنین مزایایی ، تجزیه و تحلیل و تأیید شود. به عنوان مثال ، یک حادثه امنیتی رایانه ای می تواند از طریق این فعالیت ها تشخیص داده شود ، اما زمان شروع پاسخ به حادثه شناسایی شده ، در مقایسه با زمان پاسخ در امنیت رایانه ، احتمالاً برای محافظت از سیستم کافی نخواهد بود.

سیستمی که اقدامات امنیتی رایانه ای لایه ای را با عناصر پاسخ خودکار به همراه دارد.

4.80. Unmanaged changes to software configuration are a significant source of new vulnerabilities and unpredictable situations. Typically, the configuration management system used for I&C systems is a generic system that also manages many other types of system. Nevertheless, the configuration management system should be used in a way that incorporates knowledge of both the I&C systems and their computer security measures.

4.80 تغییرات کنترل نشده در پیکربندی نرم افزار منبع قابل توجهی از آسیب پذیری های جدید و شرایط غیرقابل پیش بینی است. به طور معمول ، سیستم مدیریت پیکربندی مورد استفاده برای سیستم های I&C یک سیستم عمومی است که بسیاری از انواع دیگر سیستم را نیز مدیریت می کند. با این وجود ، سیستم مدیریت پیکربندی باید به گونه ای استفاده شود که دانش هر دو سیستم I&C و اقدامات امنیتی رایانه ای آنها را در بر بگیرد.

4.81. Configuration management depends upon change management, which is a process that seeks to ensure that approved design processes and appropriate verification and validation are used when a computer system is changed. It also includes control of documents that support these processes. Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1 [16], para. 5.26, states that:

“The types of document to be controlled should include, but should not be limited to: documents that define the management system; safety requirements; work instructions; assessment reports; drawings; data files; specifications; computer codes; purchase orders and related documents; and supplier documents.”

4.81 مدیریت پیکربندی به مدیریت تغییر بستگی دارد ، این فرایندی است که می خواهد اطمینان حاصل کند که هنگام تغییر سیستم رایانه ای ، از فرآیندهای طراحی تأیید شده و تأیید و اعتبار مناسب استفاده می شود. همچنین شامل کنترل اسنادی است که از این فرایندها پشتیبانی می کند. کاربرد سیستم مدیریت امکانات و فعالیتها ، سری استانداردهای ایمنی آژانس بین المللی انرژی هسته ای شماره GS-G-3.1 [16] ، پاراگراف. 5.26 ، اظهار داشت:

وی می افزاید: "انواع كنترل كننده باید شامل شود ، اما نباید به آنها محدود شود: مداركی كه سیستم مدیریت را تعریف می كنند. الزامات ایمنی؛ دستورالعمل کار؛ گزارش ارزیابی؛ نقشه ها پرونده های داده؛ مشخصات فنی؛ کدهای رایانه ای؛ خرید سفارشات و اسناد مرتبط؛ و اسناد تهیه کننده. "

4.82. Computer security measures for I&C systems using the facility’s configuration management process should be consistent with the facility configuration control requirements applicable to the associated I&C system.

4.82 اقدامات امنیتی رایانه ای برای سیستم های I&C با استفاده از فرایند مدیریت پیکربندی تسهیلات باید مطابق با الزامات کنترل پیکربندی تسهیلات مربوط به سیستم I&C مرتبط باشد.

4.83. Configuration management should be ensured for computer security measures associated with I&C systems throughout the life cycle of I&C systems.

4.83 مدیریت پیکربندی باید برای اقدامات امنیتی رایانه در ارتباط با سیستم های I&C در طول چرخه عمر سیستم های I&C تأمین شود.

4.84. Configuration management for computer security measures associated with I&C systems should include techniques and procedures for analysing the effects of configuration changes, approving configuration changes, ensuring software versions are combined correctly, releasing design documents and software for use, and establishing and maintaining a chronological record of configuration changes (e.g. of which versions of software tools are used at a particular point in design).

4.84 مدیریت پیکربندی برای اقدامات امنیتی رایانه در ارتباط با سیستم های I&C باید شامل تکنیک ها و رویه هایی برای تحلیل اثرات تغییرات پیکربندی ، تأیید تغییرات پیکربندی ، اطمینان از ترکیب صحیح نسخه های نرم افزاری ، انتشار اسناد طراحی و نرم افزارهای طراحی شده برای استفاده و ایجاد و حفظ سابقه زمانی از تغییرات پیکربندی (به عنوان مثال نسخه های ابزارهای نرم افزاری در یک نقطه خاص از طراحی استفاده می شوند).

4.85. Identification, storage and issue for use of I&C components and associated technical control measures should be protected from compromise.

4.85 شناسایی ، ذخیره سازی و انتشار برای استفاده از قطعات I&C و اقدامات کنترل فنی مرتبط باید از مصالحه محافظت شود.

4.86. Configuration documents for computer security measures associated with I&C systems should be maintained and protected from unauthorized access or compromise. This information should be classified as sensitive information and access to this information should be limited to a need-to-know basis.

4.86 اسناد پیکربندی شده برای اقدامات امنیتی رایانه در ارتباط با سیستم های I&C باید از دسترسی یا مصالحه غیرمجاز حفظ و محافظت شوند. این اطلاعات باید به عنوان اطلاعات حساس طبقه بندی شوند و دسترسی به این اطلاعات فقط باید بر اساس نیاز به دانستن محدود شود.

4.87. Technical control measures to limit access and ensure integrity should be applied to software and configuration files during development, transport, installation and operations.

4.87 اقدامات کنترلی فنی برای محدود کردن دسترسی و اطمینان از یکپارچگی باید در نرم افزارها و پرونده های پیکربندی در طول توسعه ، حمل و نقل ، نصب و راه اندازی اعمال شود.

**Verification and validation**

تأیید و اعتبار سنجی

4.88. The guidance provided in paras 4.89–4.94 applies to all I&C systems, subsystems and components having an assigned security level.

4.88 راهنمایی های موجود در پاراگراف 4.89-4.94 برای کلیه سیستم های I&C ، زیر سیستم ها و مؤلفه های دارای سطح امنیتی اختصاصی اعمال می شود.

4.89. Each phase of the I&C system development process uses information from earlier phases and provides results to be used as the input for later phases. Verification should be performed after concluding a phase of the development process and before progressing to the next phase of the development process and should include assessment of the computer security measures.

4.89 هر مرحله از فرآیند توسعه سیستم I&C از اطلاعات مربوط به مراحل قبلی استفاده می کند و نتایج را برای استفاده در مراحل بعدی فراهم می کند. تأیید صحت باید پس از نتیجه گیری از مرحله توسعه و قبل از پیشرفت به مرحله بعدی روند توسعه انجام شود و شامل ارزیابی اقدامات امنیتی رایانه می باشد.

4.90. Prior to the completion of the commissioning phase of the I&C system development process, the validation of the I&C system should be performed with the aim of ensuring that the computer security requirements are met while also continuing to comply with the functional, performance and interface requirements. This is intended to provide a high degree of assurance that the system will perform its function as required. The validation of computer security measures should be carried out by teams, individuals or groups that are independent of the designers and developers. The extent of the independent validation and degree of independence, for example, should be suitable for the security level assigned to the system or component involved whether the validation is performed by vendor, contractor or supplier staff or performed by external experts independent of the vendor, contractor or supplier.

4.90 قبل از اتمام مرحله راه اندازی فرآیند توسعه سیستم I&C ، اعتبارسنجی سیستم I&C با هدف اطمینان از رعایت الزامات امنیتی رایانه و در عین حال ادامه دادن به الزامات عملکردی ، عملکرد و رابط انجام می شود. این درنظرگرفته شده است تا اطمینان بالایی از عملکرد سیستم در صورت نیاز داشته باشد. اعتبار سنجی اقدامات امنیتی رایانه باید توسط تیم ها ، افراد یا گروه هایی انجام شود که مستقل از طراحان و توسعه دهندگان باشند. به عنوان مثال میزان اعتبار سنجی و میزان استقلال مستقل باید برای سطح امنیتی اختصاص یافته به سیستم یا مؤلفه ای درگیر باشد که آیا اعتبار سنجی توسط فروشنده ، پیمانکار یا کارمندان تأمین کننده انجام شده یا توسط کارشناسان خارجی مستقل از فروشنده انجام می شود ، پیمانکار یا تهیه کننده

4.91. Verification and validation activities should demonstrate that the I&C system meets the relevant computer security requirements.

4.91 فعالیتهای تأیید و اعتبار سنجی باید نشان دهند که سیستم I&C الزامات مربوط به امنیت رایانه را برآورده می کند.

4.92. The operator should verify and validate each technical control measure to confirm that it provides the I&C system with the intended protection and does not reduce the reliability of its safety or security functions.

4.92 اپراتور باید هر یک از اقدامات کنترلی فنی را تأیید و تأیید کند تا تأیید کند که سیستم I&C را برای محافظت در نظر گرفته شده است و از قابلیت اطمینان یا عملکردهای امنیتی خود نمی کاهد.

4.93. Computer security measures should be verified and validated using a level of effort commensurate with the security level assigned to the associated I&C system or using a level of effort commensurate with the safety classification of the I&C system, whichever is more stringent.

4.93 اقدامات امنیتی رایانه باید با استفاده از سطح تلاش متناسب با سطح امنیتی اختصاص یافته به سیستم I&C مرتبط یا استفاده از سطح تلاش متناسب با طبقه بندی ایمنی سیستم I&C ، تأیید و تأیید شود.

4.94. Verification and validation activities should identify, record and document detected vulnerabilities, weaknesses or other anomalies and their resolution. Given the size and complexity of most modern computer based systems it may be difficult to ensure that the results of these activities will be comprehensive or successful in uncovering all anomalies. For example, automated tools to perform software code reviews depend on the platform and programming language used, and may only be partially successful. Additionally, it may not be possible to scan certain operating systems, machine code and callable library functions, which may contain vulnerabilities that could be exploited.

4.94 فعالیت های تأیید و اعتبار سنجی باید آسیب پذیری ها ، نقاط ضعف یا سایر ناهنجاری ها و رفع آنها را شناسایی ، ضبط و مستند سازد. با توجه به وسعت و پیچیدگی بیشتر سیستم های مدرن مبتنی بر رایانه ، اطمینان از اینکه نتایج این فعالیت ها در کشف و کشف همه ناهنجاری ها جامع یا موفق باشد ، دشوار خواهد بود. به عنوان مثال ، ابزارهای خودکار برای انجام بررسی کدهای نرم افزاری به بستر و زبان برنامه نویسی مورد استفاده بستگی دارد و فقط ممکن است تا حدی موفقیت آمیز باشد. علاوه بر این ، ممکن است اسکن برخی از سیستم عامل ها ، کد ماشین و توابع کتابخانه قابل تماس ، که ممکن است حاوی آسیب پذیری هایی باشد که امکان سوء استفاده وجود ندارد ، امکان پذیر نباشد.

**Computer security assessments**

ارزیابی امنیت رایانه

4.95. The guidance provided in paras 4.96–4.100 applies to all I&C systems, subsystems and components having an assigned security level.

4.95 راهنمایی های موجود در پاراگراف 4.96-4.100 در مورد کلیه سیستم های I&C ، زیر سیستم ها و مؤلفه های دارای سطح امنیتی اختصاصی اعمال می شود.

4.96. Computer security assessments should be performed for each phase of the I&C system life cycle to identify potential threats as well as vulnerabilities and weaknesses.

4.96 برای شناسایی تهدیدات احتمالی و همچنین آسیب پذیری ها و نقاط ضعف ، ارزیابی امنیت رایانه برای هر مرحله از چرخه زندگی سیستم I&C انجام می شود.

4.97. Public or open source information as well as vendor, contractor or supplier and expert sources should be monitored to promptly identify changes in the threat landscape and new vulnerabilities.

4.97 اطلاعات عمومی یا منبع باز و همچنین فروشنده ، پیمانکار یا تأمین کننده و منابع متخصص باید مورد بررسی قرار گیرند تا به سرعت تغییرات در چشم انداز تهدید و آسیب پذیری های جدید شناسایی شود.

4.98. New or changed threats and vulnerabilities should be assessed to evaluate their potential impact on I&C system computer security. Corrective action (e.g. amended security features) should be taken if these changes could result in potential security violations or unacceptable risks for the facility.

4.98 تهدیدات و آسیب پذیری های جدید یا تغییر یافته باید ارزیابی شود تا تأثیر احتمالی آنها بر امنیت رایانه سیستم I&C ارزیابی شود. اگر این تغییرات منجر به نقض امنیتی احتمالی یا خطرات غیرقابل قبول برای تأسیسات شود ، باید اقدامات اصلاحی (به عنوان مثال ویژگیهای امنیتی اصلاح شده) انجام شود.

4.99. Each organization that is responsible for developing, deploying, operating, maintaining or decommissioning I&C systems or components should perform periodic computer security assessments and audits.

4.99 هر سازمانی که وظیفه توسعه ، استقرار ، بهره برداری ، حفظ و یا رفع سیستم های I&C یا اجزای سازنده را بر عهده دارد ، باید ارزیابی و ممیزی امنیتی دوره ای رایانه را انجام دهد.

4.100. The results of the computer security assessments should be used to update the system CSRM.

4.100 برای به روزرسانی CSRM سیستم باید از نتایج ارزیابی های امنیت رایانه استفاده شود.

**Documentation**

مستندات

4.101. The guidance provided in paras 4.102–4.106 applies to all I&C systems, subsystems and components having an assigned security level.

4.101 راهنمایی ارائه شده در بندهای 4.102-4.106 برای کلیه سیستمهای I&C ، زیر سیستمها و مؤلفههای دارای سطح امنیتی اختصاصی اعمال می شود.

4.102. Documentation for I&C system computer security helps in avoiding ambiguities and facilitates correct and error-free operation, surveillance, troubleshooting, maintenance, future modification and modernization of the system and training of facility and technical support staff.

4.102 مستندات مربوط به امنیت رایانه ای سیستم I&C در جلوگیری از ابهامات و تسهیل عملکرد صحیح و بدون خطا ، نظارت ، عیب یابی ، نگهداری ، اصلاح و اصلاح در آینده و نوسازی سیستم و آموزش کارکنان تسهیلات و پشتیبانی فنی کمک می کند.

4.103. Documentation should be generated to record sufficient information related to the computer security of I&C systems to demonstrate that computer security measures are designed, implemented and maintained in a way that meets the required level of protection consistent with the assigned security level.

4.103 مستندات باید برای ضبط اطلاعات کافی مربوط به امنیت رایانه سیستمهای I&C ایجاد شود تا نشان دهد اقدامات امنیتی رایانه به گونه ای طراحی شده ، پیاده سازی و نگهداری می شود که مطابق با سطح امنیتی اختصاصی باشد.

4.104. Computer security input documents and output documents should be defined for the activities of each phase of the I&C system life cycle.

4.104 اسناد ورودی امنیت رایانه و اسناد خروجی باید برای فعالیتهای هر مرحله از چرخه عمر سیستم I&C تعریف شوند.

4.105. Documentation should ensure the traceability of the computer security requirements across all activities of the I&C system life cycle. The addition, modification and removal of computer security measures for I&C systems should be recorded.

4.105 مستندات باید قابلیت ردیابی الزامات امنیتی رایانه را در کلیه فعالیتهای چرخه عمر سیستم I&C تضمین کند. علاوه بر این ، اصلاح و حذف اقدامات امنیتی رایانه برای سیستم های I&C باید ثبت شود.

4.106. Documentation should be protected against unauthorized disclosure, tampering and deletion, and destruction commensurate with the assigned security level of the associated I&C system.

4.106 مستندات باید در برابر افشای غیرمجاز ، دستکاری و حذف و نابودی متناسب با سطح امنیتی اختصاص یافته سیستم I&C مرتبط محافظت شود.

**Design basis**

اساس طراحی

4.107. The guidance contained within paras 4.108–4.114 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.107 راهنمایی های موجود در پاراگراف 4.108-4.114 برای کلیه سیستم های I&C ، زیر سیستم ها و مؤلفه هایی که ممکن است رویکرد درجه بندی شده مطابق با سطح امنیتی اختصاص یافته آنها اعمال شود ، اعمال می شود.

4.108. Reference [4], para. 3.11, states that “The design basis identifies functions, conditions and requirements for the overall I&C and each individual I&C system.” This information is then used to assign computer security requirements to each I&C system and to supporting security systems. The design basis is also used to establish design, implementation, construction, testing and performance specifications for computer security measures.

4.108 مرجع [4] ، بند 3.11 ، اظهار داشت كه "مبناي طراحي ، توابع ، شرايط و الزامات مربوط به كل I&C و هر سيستم I&C فرد را مشخص مي كند." این اطلاعات سپس برای اختصاص نیازهای امنیتی رایانه به هر سیستم I&C و پشتیبانی سیستم های امنیتی استفاده می شود. همچنین از مبنای طراحی برای تعیین مشخصات طراحی ، اجرای ، ساخت ، آزمایش و مشخصات عملکرد برای اقدامات امنیتی رایانه استفاده می شود.

4.109. The design basis for the overall I&C architecture and each I&C system should be used to inform the design of computer security measures to be implemented to meet regulatory computer security requirements (including design basis threat or threat assessment). Further guidance on design basis threat (including threat assessments and alternative threat statements) is provided in Ref. [18].

4.109 مبنای طراحی برای معماری کلی I&C و هر سیستم I&C باید برای آگاهی از طراحی اقدامات امنیتی رایانه مورد استفاده جهت تأمین نیازهای امنیتی نظارتی رایانه (از جمله تهدید مبانی طراحی یا ارزیابی تهدید) مورد استفاده قرار گیرد. راهنمایی های بیشتر در مورد تهدید مبانی طراحی (از جمله ارزیابی تهدید و اظهارات تهدید جایگزین) در Ref ارائه شده است. [18]

4.110. Computer security design considerations and assumptions for the I&C systems and the supporting security systems should be identified in the design basis.

4.110 ملاحظات و فرضیات طراحی امنیت رایانه برای سیستم های I&C و سیستم های امنیتی پشتیبانی باید در مبنای طراحی مشخص شود.

4.111. The level of protection to be applied to each I&C system should be defined in the design basis, consistent with the assigned security level identified in the facility and system CSRM

4.111 سطح حفاظتی که برای هر سیستم I&C اعمال می شود باید بر اساس طراحی ، مطابق با سطح امنیتی اختصاص یافته مشخص شده در تسهیلات و سیستم CSRM تعریف شود.

4.112. The design basis should specify requirements for computer security measures, including technical, physical and administrative control measures.

4.112 مبنای طراحی باید الزامات اقدامات امنیتی رایانه ، از جمله اقدامات کنترل فنی ، فیزیکی و اداری را مشخص کند.

4.113. The design basis should specify safety requirements that allow for effective validation activities, with the aim of preventing computer security measures from adversely affecting the safety performance of I&C systems.

4.113 مبنای طراحی باید با هدف جلوگیری از اقدامات امنیتی رایانه ای که بر عملکرد ایمنی سیستم های I&C تأثیر منفی می گذارد ، الزامات ایمنی را برای فعالیتهای تأیید مؤثر مشخص کند.

4.114. The design basis should be maintained and periodically updated to reflect changes to regulatory computer security requirements or risks.

4.114 مبنای طراحی باید حفظ و به صورت دوره ای به روز شود تا منعکس کننده تغییرات در الزامات امنیتی یا خطرات امنیتی رایانه ای باشد.

**Access control**

کنترل دسترسی

4.115. The guidance contained within paras 4.116–4.120 applies to all I&C systems, subsystems and components to which a graded approach to computer security is applied in accordance with their assigned security level.

4.115 راهنمایی های موجود در پاراگراف 4.116-4.120 در مورد کلیه سیستم های I&C ، زیر سیستم ها و مؤلفه هایی که رویکرد درجه بندی شده به امنیت رایانه مطابق با سطح امنیتی اختصاص داده شده آنها اعمال می شود ، اعمال می شود.

4.116. Physical and logical access to I&C systems should be controlled with the aim of preventing unauthorized access. Privileged access to I&C systems should be strictly controlled such that only authorized personnel have access to or are able to make changes to the existing configuration, software and hardware. This access may be restricted according to the work function of the authorized personnel, both in terms of duration and the numbers of systems that are able to be accessed.

4.116 دسترسی فیزیکی و منطقی به سیستم های I&C باید با هدف جلوگیری از دسترسی غیرمجاز کنترل شود. دسترسی ممتاز به سیستمهای I&C باید به طور دقیق کنترل شود که فقط پرسنل مجاز به آن دسترسی داشته یا قادر به ایجاد تغییراتی در پیکربندی ، نرم افزار و سخت افزار موجود باشند. این دسترسی ممکن است با توجه به عملکرد کارمندان مجاز ، از نظر مدت زمان و تعداد سیستمهایی که امکان دسترسی دارند محدود شود.

4.117. The number of access points to networks and devices should be reduced to as few as possible to minimize the number of potential attack vectors.

4.117 تعداد نقاط دسترسی به شبکه ها و دستگاه ها باید تا حد ممکن کاهش یابد تا تعداد بردارهای حمله بالقوه به حداقل برسد.

4.118. Digital communication should be restricted to authorized uses and monitored for abnormal activity. Appropriate actions should be taken when abnormal activity is detected.

4.118 ارتباطات دیجیتال باید محدود به کاربردهای مجاز باشد و برای فعالیت غیر طبیعی کنترل شود. هنگام تشخیص فعالیت غیر طبیعی باید اقدامات مناسب انجام شود.

4.119. For I&C systems assigned the most stringent security level, multifactor authentication methods should be considered where such methods are compatible with time dependent interactions between facility personnel and the I&C system.

4.119 برای سیستم های I&C که دقیق ترین سطح امنیتی اختصاص داده شده است ، باید روش های تأیید اعتبار چند فاکتور را در نظر گرفت که چنین روش هایی با تعامل وابسته به زمان بین پرسنل تسهیلات و سیستم I&C سازگار باشد.

4.120. Procedures for managing and assigning roles and access rights for system and user accounts should be developed and updated periodically. The procedures should take into account the principle of least privilege. This process may be referenced or integrated into the facility computer security programme and the facility integrated management system.

4.120 مراحل مدیریت و تعیین نقش ها و حقوق دسترسی برای سیستم و حساب های کاربری باید بصورت دوره ای تدوین و به روز شود. رویه ها باید اصل حداقل امتیاز را در نظر بگیرند. این فرآیند ممکن است در برنامه امنیت رایانه تسهیلات و سیستم مدیریت یکپارچه تسهیلات ارجاع یا ادغام شود.

**Protection of the confidentiality of information**

محافظت از محرمانه بودن اطلاعات

4.121. The guidance contained within paras 4.122–4.125 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.121 راهنمایی های موجود در پاراگراف 4.122-4.125 برای کلیه سیستم های I&C ، زیر سیستم ها و مؤلفه هایی که ممکن است رویکرد درجه بندی شده مطابق با سطح امنیتی اختصاص یافته آنها اعمال شود ، اعمال می شود.

4.122. When insufficient physical protection and computer security measures for protecting the confidentiality of information are applied, it is possible for an unauthorized disclosure of information to occur that could lead to a compromise of the physical protection or computer security of the system or facility. IAEA Nuclear Security Series 23-G [15] states that:

“Information is knowledge, irrespective of its form of existence or expression. It includes ideas, concepts, events, processes, thoughts, facts and patterns. Information can be recorded on material such as paper, film, magnetic or optical media, or held in electronic systems.”

4.122 در صورت عدم استفاده از حفاظت جسمی کافی و اقدامات امنیتی رایانه ای برای محافظت از محرمانه بودن اطلاعات ، امکان افشای غیرمجاز از اطلاعات وجود دارد که می تواند منجر به سازش حفاظت فیزیکی یا امنیت رایانه ای سیستم یا تأسیس شود. سری امنیت هسته ای آژانس بین المللی انرژی هسته ای 23-G [15] اظهار داشت:

"اطلاعات ، دانش است ، صرف نظر از نوع وجود یا بیان آن. این شامل ایده ها ، مفاهیم ، وقایع ، فرایندها ، افکار ، حقایق و الگوهای است. اطلاعات را می توان در موادی مانند کاغذ ، فیلم ، رسانه مغناطیسی یا نوری ضبط کرد یا در سیستمهای الکترونیکی نگهداری کرد. "

4.123. Information related to I&C systems should be identified (e.g. associated databases, files and documentation; change components; simulators), and, where appropriate, classified as sensitive information and secured with appropriate measures. References [12, 15] provide additional information on recommendations for protecting sensitive information.

4.123 اطلاعات مربوط به سیستم های I&C باید شناسایی شوند (به عنوان مثال پایگاه داده های مرتبط ، پرونده ها و مستندات ؛ تغییر مؤلفه ها ، شبیه سازها) ، و در صورت لزوم ، به عنوان اطلاعات حساس طبقه بندی شوند و با اقدامات مناسب تهیه شوند. منابع [12 ، 15] اطلاعات اضافی در مورد توصیه های محافظت از اطلاعات حساس ارائه می دهند.

4.124. Computer security measures should be used to protect the confidentiality of information associated with I&C systems, which may include information about the design, manufacturing, installation and operations of I&C systems and associated equipment.

4.124 اقدامات امنیتی رایانه باید برای محافظت از محرمانه بودن اطلاعات مرتبط با سیستم های I&C ، که ممکن است شامل اطلاعات مربوط به طراحی ، ساخت ، نصب و راه اندازی سیستم های I&C و تجهیزات مرتبط باشد ، استفاده شود.

4.125. The operator should apply technical, physical and administrative control measures for the prevention, detection and response to unauthorized disclosure or exfiltration of sensitive information related to I&C systems.

4.125 اپراتور باید از اقدامات كنترلی فنی ، فیزیكی و اداری برای پیشگیری ، تشخیص و پاسخ به افشای غیرمجاز یا استخراج اطلاعات حساس مربوط به سیستم های I&C استفاده كند.

**Security monitoring**

نظارت بر امنیت

4.126. The guidance contained within paras 4.127–4.130 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.126 راهنمایی های موجود در پاراگراف 4.127-4.130 برای کلیه سیستم های I&C ، زیر سیستم ها و مؤلفه هایی که ممکن است رویکرد درجه بندی شده مطابق با سطح امنیتی اختصاص یافته آنها اعمال شود ، اعمال می شود.

4.127. Computer security requirements for the security monitoring of I&C systems should be specified consistent with the systems’ assigned security levels.

4.127 الزامات امنیتی رایانه برای نظارت بر امنیت سیستمهای I&C باید مطابق با سطح امنیتی اختصاص یافته سیستم باشد.

4.128. Monitoring of I&C systems requiring the highest or a high level of security should employ independence20 or diversity in the computer security measures deployed to detect compromise or mal-operations. User interfaces for security monitoring, compromise indications, recording instrumentation and alarms should be provided at appropriate locations and should be suitable and sufficient to support effective monitoring of computer security in all plant states.

4.128 نظارت بر سیستم های I&C که به بالاترین و بالاترین سطح امنیتی نیاز دارند ، باید از استقلال 20 یا تنوع در اقدامات امنیتی رایانه ای که برای شناسایی سازش یا سوء عملکرد استفاده می شود ، استفاده کند. رابط های کاربر برای نظارت بر امنیت ، نشانه های سازش ، ابزار ضبط و آلارم باید در مکان های مناسب تهیه شده و برای پشتیبانی از نظارت مؤثر بر امنیت رایانه در کلیه ایالات گیاهی مناسب و کافی باشد.

4.129. Requirements for monitoring the status of technical or physical control measures should be established to facilitate the taking of any necessary safety and security actions.

4.129 برای تسهیل در انجام اقدامات ایمنی و امنیتی لازم باید شرایط لازم برای نظارت بر وضعیت اقدامات فنی و کنترل فیزیکی ایجاد شود.

4.130. I&C systems and their associated computer security measures should be continuously monitored and logged. Analysis should identify unauthorized access or changes. The integrity of these records should be protected.

4.130 سیستم های I&C و اقدامات امنیتی رایانه ای مربوط به آنها باید به طور مداوم مورد نظارت و ثبت قرار گیرند. تجزیه و تحلیل باید دسترسی یا تغییرات غیرمجاز را شناسایی کند. از تمامیت این سوابق باید محافظت شود.

**Considerations for the overall defensive computer security architecture**

ملاحظاتی در مورد معماری کلی امنیت دفاعی رایانه

4.131. The guidance provided in paras 4.132–4.140 applies to all I&C systems, subsystems and components having an assigned security level.

4.131 راهنمایی های ارائه شده در بندهای 4.132-4.140 برای کلیه سیستمهای I&C ، زیر سیستمها و مؤلفههای دارای سطح امنیتی اختصاصی اعمال می شود.

4.132. The operator should specify an overall defensive architecture for the computer security of I&C systems in which all I&C systems are assigned a security level and protected according to the applicable requirements.

4.132 اپراتور باید یک معماری دفاعی کلی برای امنیت رایانه سیستمهای I&C باشد که در آن به کلیه سیستمهای I&C یک سطح امنیتی اختصاص داده شده و مطابق با الزامات قابل اجرا محافظت می شود.

4.133. Defensive architecture should be used to facilitate and maintain the capability for I&C systems to prevent, detect, delay, mitigate and recover from cyber attacks. Defensive architecture includes, but is not limited to, formal logical or physical boundaries such as the security zones in which defensive measures are deployed.21 When implementing such architecture, operators should consider limiting the dynamic elements of both the composite networks and their individual systems to increase the determinacy of their behaviour. This increase in determinacy may assist the implementation of effective computer security measures for the detection of potential computer security incidents.

4.133 از معماری دفاعی برای تسهیل و حفظ توانایی سیستمهای I&C برای جلوگیری ، شناسایی ، تأخیر ، کاهش و بهبود حملات سایبری استفاده می شود. معماری دفاعی شامل مرزهای منطقی یا جسمی رسمی مانند محدوده های امنیتی که در آن اقدامات دفاعی مستقر شده اند ، را شامل می شود ، اما محدود به آن نیست. تعیین کننده رفتار آنها را افزایش می دهد. این افزایش در تعیین ممکن است به اجرای اقدامات مؤثر امنیتی رایانه برای تشخیص حوادث احتمالی امنیت رایانه کمک کند.

4.134. Computer security boundaries should be implemented between I&C systems, subsystems and components that have different security levels and are protected using different computer security measures. Computer security boundaries are the logical and physical boundaries of a system or a set of systems at the same security level, and may therefore be secured by the application of common defensive measures (e.g. computer security zones).

4.134 مرزهای امنیتی رایانه باید بین سیستم های I&C ، زیر سیستم ها و مؤلفه هایی که دارای سطح امنیتی مختلف هستند و با استفاده از اقدامات امنیتی رایانه ای مختلف محافظت می شود ، اجرا شود. مرزهای امنیتی رایانه ، مرزهای منطقی و فیزیکی یک سیستم یا مجموعه ای از سیستم ها در همان سطح امنیتی هستند و بنابراین ممکن است با استفاده از اقدامات دفاعی رایج (به عنوان مثال مناطق امنیتی رایانه) امن شوند.

4.135. Data flow should be controlled between security zones assigned to different security levels and between individual I&C systems on the same security level based on a risk informed approach to ensure that the defensive architecture remains effective.

4.135 جریان داده باید بین مناطق امنیتی اختصاص داده شده به سطوح مختلف امنیتی و بین سیستمهای I&C فردی در همان سطح امنیتی براساس یک رویکرد آگاهانه در معرض خطر کنترل شود تا از اثربخشی معماری دفاعی اطمینان حاصل شود.

4.136. I&C systems requiring the highest level of security (i.e. the most stringent security level) should only be connected to systems requiring lower levels of security (i.e. weaker security levels) via fail-secure, deterministic, unidirectional data communication pathways.22 The direction of these data pathways should be limited to the transmission of data from devices requiring the most stringent security level to the devices assigned to weaker security levels. Exceptions are strongly discouraged and may only be considered on a strict case by case basis and if supported by a complete justification and security risk analysis.23

4.136 سیستم های I&C که به بالاترین سطح امنیتی نیاز دارند (یعنی دقیق ترین سطح امنیتی) فقط باید به سیستم هایی که سطح امنیتی پایین تری دارند (یعنی سطح امنیتی ضعیف تر) وصل شوند از طریق مسیرهای ارتباطی با داده های ایمن ، قطعی ، یک طرفه. مسیرهای داده باید محدود به انتقال داده ها از دستگاه هایی باشد که نیاز به دقیق ترین سطح امنیتی به دستگاه های اختصاص داده شده برای سطح ضعیف تر امنیتی دارند. استثنائات به شدت دلسرد می شوند و فقط در موارد سخت و جدی مورد بررسی قرار می گیرند و در صورت توجیه کامل و تحلیل ریسک امنیتی پشتیبانی می شوند.

4.137. Digital devices or communications networks used for monitoring, maintenance and recovery activities should not bypass technical control measures used to protect communication pathways between devices having different security levels.

4.137 دستگاه های دیجیتالی یا شبکه های ارتباطی که برای نظارت ، نگهداری و فعالیتهای بازیابی مورد استفاده قرار می گیرند ، نباید از اقدامات کنترلی فنی که برای محافظت از مسیرهای ارتباطی بین دستگاههای دارای سطح امنیتی مختلف استفاده می شود ، عبور کنند.

4.138. Systems assigned to the most stringent security level should be placed within the most secure zone boundaries. Wireless communications functions are problematic when implemented in I&C systems that are assigned to the most stringent security level as it is difficult to provide a secure boundary for such communications.

4.138 سیستم های اختصاص یافته به دقیق ترین سطح امنیتی باید در امن ترین مرزهای منطقه قرار بگیرند. عملکردهای ارتباطات بی سیم هنگام اجرای در سیستمهای I&C که به دقیق ترین سطح امنیتی اختصاص یافته اند مشکل پذیر هستند ، زیرا تهیه یک مرز امن برای چنین ارتباطات دشوار است.

4.139. Data communications between facility I&C systems and the emergency centre (either on-site or off-site) should be protected and controlled by computer security measures.

4.139 ارتباطات داده ها بین سیستم های I&C تأسیسات و مرکز اضطراری (چه در محل و چه خارج از سایت) باید با اقدامات امنیتی رایانه محافظت و کنترل شود.

4.140. Technical control measures implemented within each security zone or at the security zone boundary should employ different technologies from those implemented in adjacent security levels or boundaries. This will ensure the use of diverse technologies to protect the I&C systems.

4.140 اقدامات كنترلی فنی كه در هر منطقه امنیتی یا در محدوده منطقه امنیتی اجرا می شوند باید از فن آوری های مختلفی كه در سطوح امنیتی یا مرزهای امنیتی مجاور استفاده می شود ، استفاده كنند. این کار با استفاده از فن آوری های متنوع برای محافظت از سیستم های I&C تضمین می کند.

**Defence in depth against compromise**

عمق دفاع در برابر سازش

4.141. The guidance contained within paras 4.142–4.151 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.141 راهنمایی های موجود در پاراگراف 4.142-4.151 برای کلیه سیستم های I&C ، زیر سیستم ها و مؤلفه هایی که ممکن است رویکرد درجه بندی شده مطابق با سطح امنیتی اختصاص یافته آنها اعمال شود ، اعمال می شود.

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

4.142 عمق دفاع در برابر سازش شامل ارائه چندین لایه دفاعی از اقدامات امنیتی رایانه ای است که برای پیشرفت و تأثیرگذاری بر سیستم I&C می توانند در حمله سایبری از بین بروند یا از آن دور شوند. بنابراین ، عمق دفاع نه تنها با اجرای چندین لایه دفاعی (به عنوان مثال مناطق امنیتی در یک معماری امنیتی رایانه ای دفاعی) بلکه با ایجاد و حفظ یک برنامه قوی از اقدامات امنیتی رایانه ای که ارزیابی ، جلوگیری ، شناسایی ، محافظت از ، پاسخ ، انجام می شود ، حاصل می شود. برای کاهش ، بهبود و بازیابی از حمله به سیستم I&C. به عنوان مثال ، در صورت بروز عدم موفقیت در پیشگیری (به عنوان مثال نقض خط مشی) یا اگر می بایست از مکانیسم های حفاظتی عبور کرد (به عنوان مثال توسط ویروس جدیدی که هنوز به عنوان حمله سایبری شناخته نشده است) ، مکانیسم های دیگر هنوز هم وجود دارند. برای شناسایی و پاسخ به یک تغییر غیرمجاز در یک سیستم I&C مبتلا.

4.143. No single failure within or across the defensive layers should render the overall computer security of the I&C systems invalid or ineffective. For example, the exploitation of a critical vulnerability within a common network protection device used at two logically linked but physically separated locations would have the potential to facilitate an attack bypassing multiple layers of computer security measures.

4.143 هیچ خرابی واحدی در لایه های دفاعی یا در سراسر آن نباید باعث شود امنیت رایانه ای سیستم های I&C نامعتبر یا ناکارآمد شود. به عنوان مثال ، بهره برداری از یک آسیب پذیری مهم در یک دستگاه حفاظت از شبکه مشترک که در دو مکان منطقی به هم پیوسته اما از نظر جسمی جدا از هم استفاده می شود ، این امکان را برای تسهیل حمله با دور زدن چندین لایه از اقدامات امنیتی رایانه دارد.

4.144. I&C systems and related digital components should be designed and operated in accordance with the concept of defence in depth against compromise.

4.144 سیستم های I&C و مؤلفه های دیجیتال مرتبط باید مطابق با مفهوم دفاع در عمق در برابر سازش طراحی و عملیاتی شوند.

4.145. Personnel should be assigned to perform security actions that complement technical control measures. The balance between human activity and technical control measures should be analysed and justified.

4.145 پرسنل باید برای انجام اقدامات امنیتی که مکمل اقدامات کنترل فنی هستند ، اختصاص یابد. تعادل بین فعالیتهای انسانی و اقدامات کنترل فنی باید تحلیل و توجیه شود.

4.146. A systematic approach should be taken to identify and document human actions that can adversely affect I&C security in each phase of the I&C system life cycle.

4.146 برای شناسایی و مستندسازی اقدامات انسانی که می تواند تأثیر منفی بر امنیت I&C در هر مرحله از چرخه زندگی سیستم I&C بگذارد ، باید رویکردی منظم انجام شود.

4.147. A risk informed approach should be used to determine the appropriate provision of security for I&C systems, including the implementation of technical control measures and defence in depth against compromise. The layers of computer security measures used to implement defence in depth against compromise should be implemented in accordance with the facility and system CSRM.

4.147 برای تعیین تأمین امنیت مناسب برای سیستمهای I&C ، از جمله اجرای اقدامات کنترل فنی و عمق دفاع در برابر سازش ، باید از رویکرد آگاهانه در مورد ریسک استفاده شود. لایه های اقدامات امنیتی رایانه ای که برای اجرای عمق دفاع در برابر سازش مورد استفاده قرار می گیرد ، باید مطابق با تسهیلات و سیستم CSRM اجرا شوند.

4.148. Each defensive layer should be protected from cyber attacks originating in adjacent layers.

4.148 هر لایه دفاعی باید از حملات سایبری ناشی از لایه های مجاور محافظت شود.

4.149. Protection mechanisms used for isolation between defensive layers should mitigate common cause failures.

4.149 مکانیسم های محافظتی که برای جداسازی بین لایه های دفاعی مورد استفاده قرار می گیرند ، باید شکست های عادی را کاهش دهند.

4.150. Defensive layers and associated countermeasures should prevent or delay the advancement of attacks.

4.150 لایه های دفاعی و اقدامات متقابل مرتبط باید از پیشگیری یا به تاخیر انداختن پیشرفت حملات جلوگیری کنند.

4.151. Defensive layers should be effective throughout the I&C system life cycle and should be considered in the design, configuration, modification and parameter assignment of the components of the system.

SPECIFIC LIFE CYCLE ACTIVITIES

4.151 لایه های دفاعی باید در طول چرخه عمر سیستم I&C مؤثر باشند و باید در طراحی ، پیکربندی ، اصلاح و تعیین پارامترهای مؤلفه های سیستم در نظر گرفته شوند.

فعالیت های چرخه زندگی خاص

**Computer security requirements specification**

مشخصات مورد نیاز امنیت رایانه

4.152. The computer security requirements for the defensive architecture and for individual I&C systems and components should be established and documented. These requirements for the defensive architecture should be derived from the I&C design basis.

4.152 الزامات امنیتی رایانه برای معماری دفاعی و سیستم ها و مؤلفه های I&C فردی باید تنظیم و مستند شود. این الزامات برای معماری دفاعی باید از مبنای طراحی I&C باشد.

4.153. The computer security requirements for I&C systems, subsystems and components should consider functional and performance requirements, system configuration, qualification, human factors engineering, data definitions and communication, documentation, installation and commissioning, operation, and maintenance.

4.153 الزامات امنیتی رایانه برای سیستم های I&C ، زیر سیستم ها و قطعات باید الزامات عملکردی و عملکرد ، پیکربندی سیستم ، صلاحیت ، مهندسی عوامل انسانی ، تعریف داده ها و ارتباطات ، اسناد ، نصب و راه اندازی ، بهره برداری و نگهداری را در نظر بگیرد.

4.154. The development of computer security requirements for I&C systems should take into account the facility and system CSRM. The computer security requirements should be reviewed and updated based upon changes to the outputs for the facility and system CSRM.

4.154 توسعه الزامات امنیت رایانه برای سیستمهای I&C باید امکانات و سیستم CSRM را در نظر بگیرد. الزامات امنیتی رایانه باید بر اساس تغییر در خروجی ها برای تسهیلات و سیستم CSRM بررسی و به روز شود.

4.155. The combination of the computer security requirements for defensive architecture and individual I&C systems should fulfil the design basis established for the overall I&C architecture.

4.155 ترکیب الزامات امنیت رایانه برای معماری دفاعی و سیستم های I&C منفرد باید پایه طراحی را برای معماری کلی I&C برقرار کند.

**Selection of predeveloped items**

انتخاب موارد از پیش توسعه یافته

4.156. The guidance contained within paras 4.157–4.164 applies to all I&C systems, subsystems and components to which a graded approach may be applied.

4.156 راهنمایی موجود در پاراگراف 4.157-4.164 برای کلیه سیستمهای I&C ، زیر سیستم ها و مؤلفه هایی که ممکن است رویکرد درجه بندی شده اعمال شود ، اعمال می شود.

4.157. Predeveloped items might include electronic devices, predeveloped software (PDS), commercial off-the-shelf (COTS) products, digital devices composed of hardware and software (including firmware), hardware devices configured using hardware description language or predeveloped functional blocks.

4.157 موارد پیش بینی شده ممکن است شامل دستگاههای الکترونیکی ، نرم افزارهای پیشرفته توسعه یافته (PDS) ، محصولات خارج از قفسه تجاری (COTS) ، دستگاههای دیجیتالی متشکل از سخت افزار و نرم افزار (از جمله سیستم عامل) ، دستگاههای سخت افزاری است که با استفاده از زبان توصیف سخت افزار یا بلوکهای کاربردی از پیش توسعه یافته تنظیم شده اند.

4.158. Predeveloped items could include predeveloped hardware and software (including firmware) from organizations that do not have an appropriate computer security programme or who are not willing to share the details of their computer security programme. In such cases, it is necessary to analyse the computer security characteristics of the items and to justify their use within either I&C systems or auxiliary systems.

4.158 موارد پیش فرض می تواند شامل سخت افزار و نرم افزار از پیش توسعه یافته (از جمله سیستم عامل) از طرف سازمان هایی باشد که برنامه امنیتی رایانه ای مناسبی ندارند یا مایل به اشتراک گذاری جزئیات برنامه امنیتی رایانه خود نیستند. در چنین مواردی ، نیاز به تجزیه و تحلیل ویژگی های امنیتی رایانه ها و توجیه استفاده آنها در سیستم های I&C یا سیستم های کمکی است.

4.159. PDS and COTS products are likely to be proprietary and generally their source code is unavailable for extensive verification activities. Consequently, it is likely that there is no reliable method for the operator to comprehensively determine security vulnerabilities for these products. In such cases, compensatory computer security measures will be needed unless these products are modified by the application developer.

4.159 محصولات PDS و COTS احتمالاً اختصاصی هستند و به طور کلی کد منبع آنها برای فعالیتهای تأیید گسترده گسترده در دسترس نیست. در نتیجه ، این احتمال وجود دارد که هیچ روش قابل اطمینان برای اپراتور وجود نداشته باشد تا آسیب پذیری های امنیتی را برای این محصولات بطور جامع مشخص کند. در چنین مواردی ، اقدامات امنیتی جبرانی رایانه مورد نیاز خواهد بود مگر اینکه این محصولات توسط برنامه نویس برنامه اصلاح شوند.

4.160. Computer security measures should be applied to ensure that PDS and COTS product features are not able to cause the I&C systems to fail to meet their computer security requirements. For example, guidance may be available to reduce the amount of code running, to prevent entry points from being available to unauthorized users and to eliminate unnecessary functionality, thereby minimizing the attack surface (i.e. system hardening). However, only limited protection can be obtained by the application of these computer security measures, and the operator should apply additional compensatory computer security measures.

4.160 اقدامات امنیتی رایانه باید به کار گرفته شود تا اطمینان حاصل شود که ویژگی های محصول PDS و COTS قادر به ایجاد سیستم های I&C در عدم رعایت الزامات امنیتی رایانه خود نیستند. به عنوان مثال ، ممکن است راهنمایی برای کاهش میزان کد در حال اجرا ، برای جلوگیری از در دسترس بودن نقاط ورود برای کاربران غیرمجاز و از بین بردن عملکردهای غیرضروری ، در نتیجه سطح حمله (حداقل سخت شدن سیستم) به حداقل برسد. با این وجود ، فقط با اعمال این اقدامات امنیتی رایانه ای ، می توان حفاظت محدودی را بدست آورد و اپراتور باید اقدامات امنیتی جبرانی رایانه ای دیگری را اعمال کند.

4.161. Predeveloped components or software should be selected and configured using a security qualification process commensurate with the security level of the I&C system.

4.161 کامپوننت ها یا نرم افزارهای توسعه یافته باید با استفاده از یک فرآیند صلاحیت امنیتی متناسب با سطح امنیتی سیستم I&C انتخاب و پیکربندی شوند.

4.162. The use of PDS and COTS products should be verified to ensure these products meet I&C system computer security requirements.

4.162 استفاده از محصولات PDS و COTS باید تأیید شود تا اطمینان حاصل شود که این محصولات الزامات امنیتی رایانه سیستم I&C را برآورده می کنند.

4.163. The operator should determine the documentation required to qualify PDS products. Technical control measures that cannot be verified as effective should not be relied upon.

4.163 اپراتور باید مستندات مورد نیاز برای واجد شرایط بودن محصولات PDS را تعیین کند. اقدامات کنترلی فنی که قابل اثبات نیستند که اثربخش باشد نباید به آنها اعتماد کرد.

4.164. Unneeded functions or services in a configurable PDS or COTS product should be removed.

4.164 توابع یا خدمات غیر ضروری در یک محصول PDS یا COTS قابل تنظیم باید حذف شود.

**I&C system design and implementation**

طراحی و اجرای سیستم I&C

4.165. The guidance contained within paras 4.166–4.174 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.165 راهنمایی های موجود در پاراگراف 4.166-4.174 شامل کلیه سیستم های I&C ، زیر سیستم ها و مؤلفه هایی است که ممکن است رویکرد درجه بندی شده ای مطابق با سطح امنیتی اختصاصی آنها اعمال شود.

4.166. In the I&C system (integrated hardware and software) implementation phase, the system design is transformed into code, database structures and related machine executable representations. Implementation addresses hardware configuration and set-up, software coding and testing, and communication configuration and set-up (including, where decided, the incorporation of reused software and COTS products).

4.166 در مرحله اجرای سیستم I&C (سخت افزار و نرم افزار یکپارچه) ، طراحی سیستم به کد ، ساختارهای پایگاه داده و نمایندگی های اجرایی دستگاه مربوطه تبدیل می شود. پیاده سازی به پیکربندی و راه اندازی سخت افزار ، برنامه نویسی و تست نرم افزار ، و پیکربندی ارتباط و تنظیم (شامل ، در صورت تصمیم ، ترکیب نرم افزار استفاده مجدد و محصولات COTS) می پردازد.

4.167. In the design and implementation phases of the I&C system life cycle, computer security requirements for the I&C systems should be identified and their implementation verified.

4.167 در مراحل طراحی و اجرای چرخه عمر سیستم I&C ، الزامات امنیتی رایانه برای سیستم های I&C باید شناسایی و اجرای آنها تأیید شود.

4.168. Requirements identified in the I&C system specification should be translated into specific design items in the system design description. These specific design items should include provisions to be implemented within the I&C system design or by computer security measures implemented externally to the I&C system.

4.168 الزامات مشخص شده در مشخصات سیستم I&C باید در توضیحات طراحی سیستم به موارد طراحی خاص تبدیل شود. این موارد طراحی خاص باید شامل مواردی باشد که باید در طراحی سیستم I&C یا اقدامات امنیتی رایانه ای که به صورت بیرونی برای سیستم I&C اجرا می شود ، اجرا شود.

4.169. The I&C system computer security design items should address control over physical and logical access to the system functions, use of I&C system services and data communication with other systems.

4.169 آیتم های طراحی امنیت رایانه و سیستم I&C باید کنترل دسترسی فیزیکی و منطقی به عملکرد سیستم ، استفاده از خدمات سیستم I&C و ارتباط داده با سایر سیستم ها را کنترل کنند.

4.170. Physical and logical access to an I&C system should be controlled based on the assigned security level of the I&C system. For example, systems assigned to the most stringent security level will need to have computer security requirements for multifactor access control, such as access control requiring a combination of knowledge (e.g. password), property (e.g. key, smart card) and personal features (e.g. fingerprints).

4.170 دسترسی فیزیکی و منطقی به سیستم I&C باید بر اساس سطح امنیتی اختصاصی سیستم I&C کنترل شود. به عنوان مثال ، سیستم های اختصاص داده شده به دقیق ترین سطح امنیتی برای کنترل دسترسی چند فاکتور ، مانند کنترل دسترسی نیاز به ترکیبی از دانش (به عنوان مثال رمز عبور) ، خاصیت (به عنوان مثال کلید ، کارت هوشمند) و ویژگی های شخصی (به عنوان مثال اثر انگشت).

4.171. I&C systems should be designed to include features to provide resistance to or protection against compromise.

4.171 سیستم های I&C باید به گونه ای طراحی شوند که مقاومت در برابر یا محافظت در برابر سازش را ارائه دهند.

4.172. Design measures should provide adequate confidence that the security of a system assigned to a given security level is not reduced by connections to systems assigned to weaker security levels.

4.172 اقدامات طراحی باید اطمینان کافی را به وجود آورد که امنیت سیستم اختصاص داده شده به سطح امنیتی معین با اتصال به سیستم های اختصاص یافته به سطح ضعیف تر امنیتی کاهش نمی یابد.

4.173. Appropriate combinations of administrative control measures (e.g. a computer security programme) and physical control measures should be designed to reduce the susceptibility of an I&C system to cyber attack.

4.173 ترکیب های مناسب از اقدامات کنترل اداری (به عنوان مثال یک برنامه امنیتی رایانه ای) و اقدامات کنترل فیزیکی باید به منظور کاهش حساسیت سیستم I&C در برابر حمله سایبری طراحی شود.

4.174. I&C system components should be allocated and installed in facility locations that physically secure the equipment and its network communications with other systems, for example, the placing of all data connections for systems and components within secure enclosures.

**I&C system integration**

4.174 اجزای سیستم I&C باید در مکانهای تأسیساتی که از لحاظ جسمی تجهیزات و ارتباطات شبکه آن را با سایر سیستمها ایمن می کنند ، اختصاص داده و نصب شوند ، به عنوان مثال ، قرار دادن کلیه اتصالات داده ها برای سیستم ها و مؤلفه ها در محفظه های امن.

ادغام سیستم من و سی

4.175. The guidance provided in paras 4.176–4.178 applies to all I&C systems, subsystems and components.

4.175 راهنمایی ارائه شده در پاراگراف 4.176-4.178 در مورد کلیه سیستمهای I&C ، زیر سیستم ها و مؤلفه ها اعمال می شود.

4.176. I&C system integration is the process of combining I&C system hardware and software (including firmware) into a single system. Often, vendors, contractors or suppliers will perform integration testing of each individual system

4.176 ادغام سیستم I&C فرایند ترکیب سخت افزار و نرم افزار سیستم I&C (از جمله سیستم عامل) به یک سیستم واحد است. اغلب ، فروشندگان ، پیمانکاران یا تهیه کنندگان آزمایش یکپارچه سازی سیستم های مختلف را انجام می دهند

که آنها تولید می کنند و همچنین ترکیبی از سیستم ها در محدوده آنها قبل از حمل و نقل به سایت تسهیلات است. این آزمایش عملکرد صحیح اجزای نرم افزار و رابط مناسب بین اجزاء موجود در سیستم I&C را تأیید می کند.

4.177. During the system integration phase of the I&C system life cycle, the integrated technical control measures should be in place and configured according to specifications prior to testing.

4.177 در طی مرحله ادغام سیستم چرخه عمر سیستم I&C ، اقدامات کنترل فنی فنی یکپارچه باید براساس مشخصات قبل از آزمایش تنظیم و اجرا شوند.

4.178. During integration testing, the vendor, contractor or supplier should confirm that the integrated computer security measures perform as specified and do not adversely affect the I&C systems’ ability to perform their essential functions.

4.178 در حین آزمایش یکپارچه سازی ، فروشنده ، پیمانکار یا تأمین کننده باید تأیید کند که اقدامات امنیتی یکپارچه رایانه مطابق مقرر انجام می شود و بر توانایی سیستم های I&C در انجام وظایف اساسی خود تأثیر منفی نمی گذارد.

**System validation**

اعتبارسنجی سیستم

4.179. The guidance provided in paras 4.180–4.185 applies to all I&C systems, subsystems and components having an assigned security level.

4.179 راهنمایی های ارائه شده در پاراگراف 4.180-4.185 برای کلیه سیستم های I&C ، زیر سیستم ها و مؤلفه های دارای سطح امنیتی اختصاصی اعمال می شود

4.180. System validation activities normally occur in parallel with other life cycle phases. After system integration has been completed, partial system validation is typically performed, for example, by using simulated inputs. Validation activities usually continue as part of the installation, I&C integration and commissioning phases. Validation is considered complete when a system is turned over for normal facility operations.

4.180 فعالیت های اعتبار سنجی سیستم به طور معمول به موازات سایر مراحل چرخه زندگی اتفاق می افتد. پس از اتمام ادغام سیستم ، اعتبار بخشی جزئی سیستم به طور معمول با استفاده از ورودی های شبیه سازی شده انجام می شود. فعالیت های اعتبار سنجی معمولاً به عنوان بخشی از مراحل نصب ، ادغام I&C و مراحل راه اندازی ادامه می یابد. وقتی سیستم برای عملیات تأسیسات عادی روشن شود ، اعتبارسنجی کامل است.

4.181. During the validation of each I&C system, subsystem and component, the implementation of computer security requirements and configuration items should be demonstrated. The objective of testing security functions is to ensure that the computer security requirements for the I&C systems are validated by the execution of integration, system and acceptance tests where practical and necessary.

4.181 در طول اعتبارسنجی هر سیستم I&C ، زیر سیستم و مؤلفه ، اجرای الزامات امنیتی رایانه و موارد پیکربندی باید نشان داده شود. هدف از آزمایش عملکردهای امنیتی اطمینان از تأمین اعتبار سیستمهای I&C با اجرای آزمونهای ادغام ، سیستم و پذیرش در موارد عملی و ضروری است.

4.182. System validation activities should confirm the effectiveness of the computer security measures and check for potential impacts, direct or indirect, on safety functions.

4.182 فعالیت های اعتبار سنجی سیستم باید تأثیر اقدامات امنیتی رایانه را تأیید کرده و تأثیرات احتمالی ، مستقیم یا غیرمستقیم بر عملکردهای ایمنی را بررسی کند.

4.183. Each technical control measure that is implemented in the I&C system should be demonstrated to perform in the intended manner and not to increase the risk of security vulnerabilities or reduce the reliability of safety functions.

4.183 هر یک از اقدامات کنترلی فنی که در سیستم I&C به اجرا در می آید ، باید نشان داده شود که به روش مورد نظر انجام شود و خطر آسیب پذیری های امنیتی را افزایش ندهد یا قابلیت اطمینان عملکردهای ایمنی را کاهش دهد.

4.184. The validation of I&C system computer security measures should include an assessment of system configuration (including all external connectivity), software qualification testing, system qualification testing and system factory acceptance testing. The validation of these computer security measures may be supported by I&C system tests that identify potential vulnerabilities or characterize unexpected behaviours or actions.

4.184 اعتبارسنجی اقدامات امنیتی رایانه ای سیستم I&C باید شامل ارزیابی پیکربندی سیستم (از جمله کلیه اتصالات خارجی) ، تست صلاحیت نرم افزار ، تست صلاحیت سیستم و آزمایش پذیرش کارخانه سیستم باشد. اعتبار این اقدامات امنیتی رایانه ممکن است توسط آزمایشات سیستم I&C انجام شود که آسیب پذیری های احتمالی را شناسایی کرده یا رفتارها یا اقدامات غیرمنتظره را مشخص می کند.

4.185. System validation testing should be conducted within a secure environment. For example, testing devices such as simulators or emulators should be secured by computer security measures. The stringency of computer security measures should be commensurate with the security level assigned to the I&C system.

4.185 آزمایش اعتبار سنجی سیستم باید در یک محیط امن انجام شود. به عنوان مثال ، دستگاههای آزمایش مانند شبیه سازها یا شبیه سازها باید با اقدامات امنیتی رایانه ایمن شوند. سخت گیری اقدامات امنیتی رایانه باید متناسب با سطح امنیتی اختصاص یافته به سیستم I&C باشد.

that they produce as well as a combination of systems within their scope prior to shipping to the facility site. This testing verifies the proper execution of software components and proper interfacing between components within the I&C system.

**Installation, overall I&C system integration and commissioning**

نصب ، یکپارچه سازی و راه اندازی کلی سیستم I&C

4.186. During installation and commissioning, the operator should perform an acceptance review of the correctness of the physical and technical control measures in the target environment while taking into account the overall I&C system integration24.

4.186 در حین نصب و راه اندازی ، اپراتور باید ضمن در نظر گرفتن یکپارچه سازی کلی سیستم I&C ، بررسی درستی از اقدامات کنترل فیزیکی و فنی در محیط هدف را انجام دهد.

4.187. I&C system installation, overall I&C system integration and commissioning should be conducted in a secure environment. The assignment of a security level to this environment should consider the security level of the system in the target environment and the security level of tools used in installation and commissioning.

4.187 نصب سیستم I&C ، یکپارچه سازی و راه اندازی کلی سیستم I&C باید در یک محیط امن انجام شود. اختصاص سطح امنیتی به این محیط باید سطح امنیتی سیستم را در محیط هدف و سطح امنیتی ابزارهای مورد استفاده در نصب و راه اندازی در نظر بگیرد.

4.188. The secure environment should be protected using computer security measures commensurate with the security level assigned to the I&C system and the security processes being undertaken to achieve installation and commissioning. In some cases, compensatory administrative and physical control measures should be provided to control access to the secure environment as well as associated equipment and data sources.

4.188 با استفاده از اقدامات امنیتی رایانه متناسب با سطح امنیتی اختصاص یافته به سیستم I&C و فرآیندهای امنیتی که برای دستیابی به نصب و راه اندازی انجام می شود ، باید از محیط ایمن محافظت شود. در بعضی موارد ، اقدامات كنترل اداری و جسمی برای كنترل دسترسی به محیط امن و همچنین تجهیزات و منابع داده همراه باید انجام شود.

4.189. Equipment used in the secure environment should be verified to confirm that its use does not provide pathways for the introduction of malicious code or data into the environment or I&C system components.

4.189 تجهیزات مورد استفاده در محیط ایمن باید تأیید شوند تا تأیید شود که استفاده از آن مسیری را برای ورود کد یا داده های مخرب به محیط یا اجزای سیستم I&C فراهم نمی کند.

4.190. Computer security measures should be in place to control and monitor the movement of data and digital assets into and out of the secure environment.

4.190 اقدامات امنیتی رایانه باید برای کنترل و نظارت بر حرکت داده ها و دارایی های دیجیتال به داخل و خارج از محیط امن انجام شود.

**Operations and maintenance**

عملیات و نگهداری

4.191. The guidance contained within paras 4.192–4.205 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.191 راهنمایی های موجود در پاراگراف 4.192-4.205 برای کلیه سیستم های I&C ، زیر سیستم ها و مؤلفه هایی که رویکرد درجه بندی شده مطابق با سطح امنیتی اختصاص یافته آنها اعمال می شود ، اعمال می شود.

4.192. Operations and maintenance activities continue throughout the I&C life cycle and have already been discussed in the above sections dealing with process planning and activities common to all life cycle phases. The operating organization should assume full responsibility for computer security for the ongoing performance of operations and maintenance activities when entering the operations and maintenance phase for a system.

4.192 فعالیتها و فعالیتهای نگهداری در طول چرخه زندگی I&C ادامه دارد و قبلاً در بخشهای فوق در مورد برنامه ریزی فرآیند و فعالیتهای مشترک در تمام مراحل چرخه زندگی بحث شده است. سازمان عامل باید مسئولیت کامل امنیت رایانه را برای عملکرد مداوم عملیات و فعالیتهای نگهداری در هنگام ورود به مرحله عملیات و مرحله نگهداری از سیستم ، به عهده بگیرد.

* 1. 4.193. Maintenance activities are activities required by the operator to maintain systems or components in good operating condition. These maintenance activities should be extended to the technical and physical control measures providing computer security to I&C systems and may include:Periodic preventive maintenance or testing;
  2. Actions to detect, preclude or mitigate degradation of components;
  3. Actions to diagnose, repair, overhaul or replace failed components with identical components.

4.193 فعالیت های تعمیر و نگهداری فعالیت هایی است که اپراتور برای نگهداری سیستم ها یا مؤلفه ها در شرایط عملیاتی مورد نیاز دارد. این فعالیتهای نگهداری باید به اقدامات کنترل فنی و فیزیکی که امنیت رایانه را به سیستمهای I&C ارائه می دهند ، گسترش یابد و شامل موارد زیر می باشد: تعمیر و نگهداری دوره ای یا آزمایش پیشگیرانه دوره ای.

اقدامات برای شناسایی ، جلوگیری یا کاهش تخریب اجزاء.

اقدامات برای تشخیص ، ترمیم ، تعمیرات اساسی و یا جایگزینی اجزای ناموفق با اجزای یکسان.

4.194. Computer security measures should be applied to operations and maintenance activities to ensure components and systems are not compromised.

4.194 اقدامات امنیتی رایانه باید در عملیات و فعالیتهای نگهداری اعمال شود تا اطمینان حاصل شود که اجزا و سیستم ها به خطر نمی افتند.

* 1. 4.195. The operations phase involves the use of the I&C system by the operator in its intended operational environment. During the operations phase, the operator should:Check that the I&C system security is intact through techniques such as periodic testing and monitoring, review of system logs and real time monitoring, where possible;
  2. Evaluate the impact of I&C system changes in the operating environment on I&C system security;
  3. Assess the effect on I&C system security of any proposed changes;
  4. Evaluate operating procedures for compliance with the intended use;
  5. Analyse security risks affecting the operator and the system;
  6. Evaluate new security constraints in the system;
  7. Evaluate operating procedures for correctness and usability;
  8. Perform periodic computer system security self-assessments and audits, which are key components of a good security programme;
  9. Assess the available incident reports about new threats and vulnerabilities.

4.195 مرحله عملیات شامل استفاده از سیستم I&C توسط اپراتور در محیط عملیاتی مورد نظر خود است. در طی مرحله بهره برداری ، اپراتور باید: بررسی کند که امنیت سیستم I&C از طریق تکنیک هایی مانند آزمایش و نظارت دوره ای ، بررسی سوابق سیستم و نظارت بر زمان واقعی ، در صورت امکان ، دست نخورده است.

تأثیر تغییرات سیستم I&C در محیط عملیاتی بر امنیت سیستم I&C را ارزیابی کنید.

ارزیابی تأثیر امنیت سیستم I&C از هرگونه تغییر پیشنهادی.

روشهای عملیاتی را برای انطباق با استفاده در نظر گرفته شده ارزیابی کنید.

خطرات امنیتی را که بر اپراتور و سیستم تأثیر می گذارد ، تحلیل کنید

محدودیتهای امنیتی جدید را در سیستم ارزیابی کنید.

روش های عملیاتی را برای صحت و قابلیت استفاده ارزیابی کنید.

انجام ارزیابی های خودکار و ممیزی های مربوط به امنیت سیستم رایانه ای ، که اجزای اصلی یک برنامه امنیتی خوب هستند ، انجام می دهند.

گزارش وقایع موجود در مورد تهدیدات و آسیب پذیری های جدید را ارزیابی کنید.

4.196. Operations and maintenance activities should be analysed to ensure that computer security measures are implemented to prevent the introduction of malicious software to the I&C system.

4.196 برای اطمینان از اجرای اقدامات امنیتی رایانه جهت جلوگیری از ورود نرم افزارهای مخرب به سیستم I&C ، باید عملیات و فعالیتهای نگهداری آنالیز شود.

4.197. Maintenance activities should conform to existing I&C system computer security requirements unless those requirements are to be changed as part of the maintenance activity. In some cases, computer security measures may need to be temporarily removed or disabled to permit execution of the required maintenance tasks. During the period for which the computer security measures are unavailable, the system is at greater risk and compensatory measures should be implemented.

4.197 فعالیتهای تعمیر و نگهداری باید مطابق با الزامات امنیتی رایانه ای سیستم I&C باشند ، مگر اینکه این الزامات به عنوان بخشی از فعالیت تعمیر و نگهداری تغییر یابد. در برخی موارد ، اقدامات امنیتی رایانه ممکن است نیاز باشد که به طور موقت از بین بروند یا غیرفعال شوند تا بتوانند کارهای لازم برای نگهداری را انجام دهند. در دوره ای که اقدامات امنیتی رایانه در دسترس نیست ، سیستم در معرض خطر بیشتری قرار دارد و باید اقدامات جبرانی اجرا شود.

* 1. 4.198. Calibration, testing and maintenance activities might involve the use of removable media and mobile devices that are temporarily connected to digital I&C systems and components. Computer security measures for these activities should consider:The implementation of effective administrative and technical control measures in the safe and secure handling of the digital devices;
  2. The verification of the integrity of all control set points with the aim to prevent and protect them from undesired changes;
  3. The use of qualified personnel (including third parties) that have received training in the performance of these activities based on computer security requirements.

4.198 فعالیت های کالیبراسیون ، آزمایش و نگهداری ممکن است شامل استفاده از رسانه های قابل جابجایی و دستگاه های تلفن همراه است که به طور موقت به سیستم ها و اجزای دیجیتال I&C متصل هستند. اقدامات امنیتی رایانه ای برای این فعالیت ها باید در نظر داشته باشد: اجرای اقدامات کنترل اداری و فنی مؤثر در استفاده ایمن و ایمن از دستگاه های دیجیتالی؛

تأیید صحت تمام نقاط کنترل شده با هدف جلوگیری و محافظت از آنها در برابر تغییرات ناخواسته.

استفاده از پرسنل واجد شرایط (از جمله اشخاص ثالث) که براساس الزامات امنیتی رایانه در اجرای این فعالیت ها آموزش دیده اند.

4.199. Interfaces should be disabled or access restricted when not required or not in use (e.g. connection of maintenance and development computers).

4.199 رابط ها باید در صورت عدم استفاده یا عدم استفاده (مثلاً اتصال رایانه های نگهداری و توسعه) غیرفعال شوند یا دسترسی محدود شوند.

4.200. Computer security measures should be in place to prevent unnecessary or unauthorized access.

4.200 اقدامات امنیتی رایانه برای جلوگیری از دسترسی غیرضروری یا غیرمجاز باید انجام شود.

4.201. Monitoring processes or applications should be in place to verify the current software configuration against known configurations.

4.201 فرآیندهای نظارت یا برنامه های کاربردی باید به منظور تأیید پیکربندی نرم افزار فعلی در برابر پیکربندی های شناخته شده موجود باشد.

4.202. Remote access should be restricted to the greatest extent possible. When remote access is needed, the risk of such connections should be considered, and additional computer security measures need to be implemented. Such connectivity should be maintained for only as long as needed for its specific purpose.

4.202 دسترسی از راه دور باید تا حد ممکن محدود شود. در صورت نیاز به دسترسی از راه دور ، باید خطر چنین ارتباطاتی در نظر گرفته شود و اقدامات امنیتی اضافی رایانه ای نیز به مرحله اجرا برسد. چنین اتصال باید فقط تا زمانی که برای هدف خاص خود لازم باشد ، حفظ شود.

4.203. Operation and maintenance activities should be carefully controlled through formal work order processes and maintenance procedures. For example, checks and balances, such as the two person rule, should be considered for tasks such as performing configuration changes on operational I&C systems.

4.203 فعالیت های عملیاتی و نگهداری باید با دقت در فرایندهای رسمی سفارش کار و روشهای نگهداری کنترل شوند. به عنوان مثال ، بررسی ها و توازن ها ، مانند قانون دو نفر ، باید برای کارهایی مانند انجام تغییرات پیکربندی در سیستم های عملیاتی I&C در نظر گرفته شود.

4.204. Operation activities should not require changes to the I&C system computer security measures.

4.204 فعالیتهای عملیاتی نباید به اقدامات امنیتی رایانه ای سیستم I&C نیاز داشته باشند.

4.205. System operational and maintenance tools that may be used to compromise the I&C system should be protected commensurate with the security level of the associated I&C system. For example, tools used on a system assigned to a more stringent security level should not be used on a system assigned to a weaker security level.

4.205 ابزارهای عملیاتی و نگهداری سیستم که ممکن است برای به خطر انداختن سیستم I&C استفاده شود باید متناسب با سطح امنیتی سیستم I&C مرتبط باشد. به عنوان مثال ، ابزارهای بکار رفته در سیستمی که به سطح امنیتی دقیق تری اختصاص داده شده است ، نباید در سیستم اختصاص داده شده به سطح امنیتی ضعیف تر استفاده شوند.

**Modification of I&C systems**

اصلاح سیستم های I&C

* 1. 4.206. The application of computer security measures to legacy I&C systems at an existing nuclear facility is not always straightforward. For example, the following difficulties may arise:Alteration of the legacy I&C architecture may not be possible without affecting the deterministic behaviour of the legacy I&C systems.
  2. Existing technologies used for program or data storage, interfaces, or communication may not support modification.
  3. Existing facility structures and layout may not allow for sufficient physical protection measures.
  4. Contemporary technical control measures that provide security monitoring functions may not be compatible with the technologies implemented within legacy I&C systems.

4.206 استفاده از اقدامات امنیتی رایانه ای برای میراث I&C در میراث هسته ای موجود ، همیشه ساده نیست. به عنوان مثال ، ممکن است مشکلات زیر بوجود آید: تغییر در میراث I&C میراث ممکن است بدون تاثیرگذاری بر رفتار تعیین کننده سیستم های میراث I&C امکان پذیر نباشد.

فن آوری های موجود مورد استفاده برای برنامه یا ذخیره داده ها ، رابط ها یا ارتباطات ممکن است از اصلاح پشتیبانی نکند.

ساختار و امکانات موجود موجود نمی تواند اقدامات محافظت جسمی کافی را انجام دهد.

اقدامات کنترلی کنترل فنی معاصر که عملکردهای نظارت بر امنیت را ارائه می دهند ممکن است با فن آوری های اجرا شده در سیستم های I&C میراث سازگار نباشد.

4.207. During the modernization of a nuclear facility that involves the replacement of legacy I&C systems with modern I&C systems, the operator should consider the possibility that legacy interfaces with the original facility systems and other systems may need to be maintained and that new vulnerabilities and weaknesses may be introduced owing to the new technology or design.

4.207 در طی مدرنیزه کردن یک تاسیسات هسته ای که شامل جایگزینی سیستم های I&C میراث با سیستم های I&C مدرن است ، اپراتور باید این احتمال را در نظر بگیرد که رابط های میراث با سیستم های تأسیسات اصلی و سایر سیستم ها نیاز به حفظ داشته باشد و ممکن است آسیب پذیری ها و ضعف های جدیدی باشد. با توجه به فناوری جدید یا طراحی جدید معرفی شده است.

* 1. 4.208. Modifications of I&C systems change the system or its documentation. These changes may be categorized as follows:Changes or enhancements (corrective or adaptive);
  2. Migration (i.e. the movement of a system to a new operational environment);
  3. Replacement (i.e. the withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system).

4.208 تغییرات در سیستم های I&C باعث تغییر سیستم یا مستندات آن می شود. این تغییرات ممکن است به شرح زیر طبقه بندی شوند: تغییرات یا پیشرفت ها (اصلاحی یا تطبیقی).

مهاجرت (یعنی حرکت یک سیستم به یک محیط عملیاتی جدید).

جایگزینی (یعنی برداشتن پشتیبانی فعال توسط سازمان عملیات و نگهداری ، تعویض جزئی یا کل توسط یک سیستم جدید یا نصب سیستم به روز شده).

4.209. I&C system modifications may be derived from requirements or specified to correct errors (corrective), to adapt to a changed operating environment (adaptive), or to respond to additional operator requests or enhancements.

4.209 تغییرات سیستم I&C ممکن است از الزامات یا مشخص شده برای اصلاح خطاها (اصلاحی) ، سازگاری با محیط عملیاتی تغییر یافته (تطبیقی) یا پاسخگویی به درخواست ها یا پیشرفتهای اپراتور اضافی باشد.

4.210. When modifications to an I&C system are made, an assessment of the security of the modified I&C system should be included, for example, by updating the system CSRM.

4.210 وقتی تغییراتی در سیستم I&C ایجاد می شود ، ارزیابی امنیت سیستم اصلاح شده I&C باید به عنوان مثال با به روزرسانی CSRM سیستم درج شود.

4.211. Computer security should be considered as part of the change management process. This includes changes to software and hardware for I&C systems.

4.211 امنیت رایانه باید به عنوان بخشی از فرایند مدیریت تغییر در نظر گرفته شود. این شامل تغییراتی در نرم افزار و سخت افزار برای سیستمهای I&C است.

4.212. To ensure that vulnerabilities have not been introduced into the facility environment by modifications, the operator should assess proposed I&C system changes including their impact on the computer security programme and existing I&C system security, evaluate anomalies that are discovered during operation, assess migration needs and assess modifications made, including validation and verification activities.

4.212 برای اطمینان از عدم آسیب پذیری ها با تغییراتی در محیط تأسیسات وارد نشده است ، اپراتور باید تغییرات سیستم پیشنهادی I&C از جمله تأثیر آن بر برنامه امنیتی رایانه و امنیت سیستم I&C موجود را ارزیابی کند ، ناهنجاری هایی را که در حین کار کشف شده اند ارزیابی کند ، نیازهای مهاجرت را ارزیابی کرده و ارزیابی کند. اصلاحات انجام شده ، از جمله فعالیت های تأیید صحت و تأیید.

4.213. Computer security measures should be assessed as described in paras 4.206–4.212 above, and should be revised to reflect computer security requirements derived from the modification process, as appropriate.

4.213 اقدامات امنیتی رایانه باید مطابق با بند 4.206-4.212 در بالا ارزیابی شود ، و باید مورد بازبینی قرار گیرد تا در صورت لزوم ، منعکس کننده امنیت سیستم رایانه ای حاصل از فرآیند اصلاح باشد.

4.214. During modification, existing I&C system computer security requirements should remain in force unless those requirements are to be changed as part of the modification activity.

4.214 در حین اصلاح ، الزامات امنیتی رایانه سیستم I&C موجود باید در قوت خود باقی بماند مگر اینکه این الزامات به عنوان بخشی از فعالیت اصلاح تغییر یابد.

4.215. Configuration management for computer security measures should be in place to prevent the introduction of unauthorized software to I&C systems.

4.215 مدیریت پیکربندی برای اقدامات امنیتی رایانه باید انجام شود تا از ورود نرم افزارهای غیرمجاز به سیستمهای I&C جلوگیری شود.

4.216. When migrating systems, the operator should verify that the migrated systems meet the computer security requirements for the I&C system.

4.216 هنگام مهاجرت سیستم ها ، اپراتور باید تأیید کند که سیستم های مهاجرت مورد نیاز امنیت رایانه برای سیستم I&C را برآورده می کنند.

4.217. Artefacts from development, installation and testing should be removed from the system and its configuration files prior to placing in service for operation.

4.217 آثار باقیمانده از توسعه ، نصب و آزمایش باید قبل از قرار دادن در سرویس برای بهره برداری از سیستم و پرونده های پیکربندی آن حذف شوند.

4.218. Modifications to I&C systems should be treated as development processes and should be verified and validated.

4.218 تغییرات در سیستم های I&C باید به عنوان فرآیندهای توسعه تلقی شوند و باید تأیید و اعتبار سنجی شوند.

4.219. All modifications to the I&C system and its components, including software, hardware and system configurations, should account for potential security vulnerabilities and threats that may occur not only during the execution of these activities but also as a result of the modifications.

4.219 کلیه تغییرات در سیستم I&C و مؤلفه های آن ، از جمله نرم افزار ، سخت افزار و تنظیمات سیستم ، باید آسیب پذیری و تهدیدهای امنیتی احتمالی باشد که ممکن است نه تنها هنگام اجرای این فعالیت ها بلکه در نتیجه تغییرات ایجاد شود.

4.220. Many digital assets and associated components, including removable storage media, have the ability to retain digital data when removed from a system. This digital data may include preprogrammed logic or residual system data such as sensor readings, control signals, analytical data and network traffic. These data may be extractable from the discarded components.

4.220 بسیاری از دارایی های دیجیتال و مؤلفه های مرتبط ، از جمله رسانه ذخیره سازی قابل جابجایی ، توانایی حفظ داده های دیجیتالی را در هنگام حذف از یک سیستم دارند. این داده های دیجیتال ممکن است شامل منطق از پیش برنامه ریزی شده یا داده های سیستم باقیمانده مانند خوانش سنسور ، سیگنال های کنترل ، داده های تحلیلی و ترافیک شبکه باشد. این داده ها ممکن است از اجزای دور ریخته شده استخراج شود.

4.221. Administrative and technical control measures should be in place to ensure that remnant data on discarded components cannot be used to support the development of a computer exploit. The components should be destroyed or the data should be securely removed, unless residual data on components to be discarded have been evaluated to show that the data do not pose a risk of security compromise.

4.221 اقدامات كنترلی اداری و فنی باید انجام شود تا اطمینان حاصل شود كه داده های باقیمانده در مورد اجزای دور ریخته شده نمی توانند برای حمایت از توسعه یك بهره برداری از رایانه استفاده شوند. اجزای سازنده باید از بین بروند یا داده ها به طور ایمن از بین بروند ، مگر اینکه داده های باقیمانده در مورد اجزای مورد استفاده قرار گیرد که مورد استفاده قرار نگیرند.

4.222. For modifications involving the replacement of I&C systems, the operator should conduct activities such as data cleansing, disk destruction or complete overwrite to ensure data cannot be recovered from the replaced I&C system upon removal from service.

DECOMMISSIONING

4.222 برای تغییرات مربوط به جایگزینی سیستم های I&C ، اپراتور باید فعالیت هایی مانند پاکسازی داده ها ، تخریب دیسک یا بازنویسی کامل را انجام دهد تا اطمینان حاصل شود که پس از حذف خدمات ، داده ها از سیستم جایگزین I&C قابل بازیابی نخواهند بود.

تصدیق

4.223. In the decommissioning phase, before nuclear materials, other radioactive material and sensitive information assets have been removed from the facility, the operator should assess the effect of replacing or removing the existing I&C system security functions from the operating environment.

4.223 در مرحله تخریب ، قبل از حذف مواد هسته ای ، سایر مواد رادیواکتیو و دارایی های حساس اطلاعات از تسهیلات ، اپراتور باید اثر جایگزینی یا حذف عملکردهای امنیتی سیستم I&C موجود از محیط عملیاتی را ارزیابی کند.

4.224. The operator should include in the scope of this assessment the effect on safety and non-safety system interfaces of removing the system security functions.

4.224 اپراتور باید در دامنه این ارزیابی اثر در رابط های ایمنی و غیر ایمنی از بین بردن عملکردهای امنیتی سیستم را درج کند.

4.225. The operator should document the methods by which a change in the I&C system security functions will be mitigated (e.g. replacement of the security functions, isolation from other safety systems and operator interactions or decommissioning of the I&C system interfacing functions).

4.225 اپراتور باید روشهایی را که با استفاده از آنها می توان تغییر در عملکردهای سیستم I&C را کاهش داد (به عنوان مثال جایگزینی عملکردهای امنیتی ، جداسازی سایر سیستمهای ایمنی و تعامل اپراتور و یا رفع توابع واسط سیستم I&C) مستندسازی کند.

4.226. Until decommissioning of a facility has been completed, the security procedures should retain elements that ensure the cleansing of hardware and data.

4.226 تا زمانيكه ركودكشي تسهيلات به اتمام نرسد ، رويه هاي امنيتي بايد عناصري را حفظ كنند كه از پاكسازي سخت افزار و داده ها را تضمين مي كند.