Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain

IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES AND RELATED PUBLICATIONS

IAEA guidance on nuclear security issues relating to the prevention and detection of, and response to, criminal or intentional unauthorized acts involving, or directed at, nuclear material, other radioactive material, associated facilities or associated activities is provided in the **IAEA Nuclear Security Series**. Publications in this series are consistent with, and complement, international nuclear security instruments, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

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

- **Nuclear Security Fundamentals** specify the objective of a State's nuclear security regime and the essential elements of such a regime. They provide the basis for the Nuclear Security Recommendations.
- **Nuclear Security Recommendations** set out measures that States should take to achieve and maintain an effective national nuclear security regime consistent with the Nuclear Security Fundamentals.
- **Implementing Guides** provide guidance on the means by which States could implement the measures set out in the Nuclear Security Recommendations. As such, they focus on how to meet the recommendations relating to broad areas of nuclear security.
- **Technical Guidance** provides guidance on specific technical subjects to supplement the guidance set out in the Implementing Guides. They focus on details of how to implement the necessary measures.

Other publications on nuclear security, which do not contain IAEA guidance, are issued outside the IAEA Nuclear Security Series.

RELATED PUBLICATIONS

The IAEA also establishes standards of safety for protection of health and minimization of danger to life and property, which are issued in the **IAEA Safety Standards Series**.

The IAEA provides for the application of guidance and standards and makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety and security related publications.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

COMPUTER SECURITY APPROACHES TO REDUCE CYBER RISKS IN THE NUCLEAR SUPPLY CHAIN

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

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

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

COMPUTER SECURITY APPROACHES TO REDUCE CYBER RISKS IN THE NUCLEAR SUPPLY CHAIN

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2022

COPYRIGHT NOTICE

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

For further information on this publication, please contact:

Information Management Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

Printed by the IAEA in Austria
December 2022

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Computer security approaches to reduce cyber risks in the nuclear supply chain / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2022. | Includes bibliographical references.
Identifiers: IAEAL 22-01556 | ISBN 978–92–0–146922–9 (paperback : alk. paper) | ISBN 978–92–0–146822–2 (pdf) ——--
Subjects: LCSH: | Nuclear industry — Computer security. | Nuclear industry — Security measures. | Nuclear industry — Business logistics.
Classification: UDC 621.039:004.056 | IAEA-TDL-011

FOREWORD

The aim of nuclear security is to prevent, detect and respond to malicious acts that involve nuclear and other radioactive material and the associated facilities and operations. Computers, computing systems and digital components play an ever expanding role in the management of sensitive information, nuclear safety, nuclear security, and material accountancy and control at these facilities and operations.

Over the past several decades, there has been a migration to more digital devices, systems, communications and advanced technologies to enhance operational capabilities for more effective and efficient operations in the nuclear sector. With this increased capability in digital technology, there has also been a major increase in threats and computer security incidents across all facets of nuclear security, including the supply chain.

Nuclear security is the responsibility of each individual State. However nuclear security also extends across borders in the supply chain through international suppliers, integrators and support organizations in order to support States in establishing and maintaining effective nuclear security regimes. Nuclear facilities and operations rely on complex networks of suppliers, vendors and integrators with multiple tiers of globally dispersed suppliers throughout the supply chain life cycle. This network also includes shippers, carriers and customs agents. The complexity of these networks provides numerous possibilities for an adversary to inject, substitute or compromise a service or device, or to acquire system information prior to use within a facility or organization within the nuclear security regime.

The purpose of this publication is to assist Member States in raising awareness of cyber risks in the nuclear supply chain. The publication also aims to help identify critical issues and mitigation techniques to reduce the supply chain attack surface by providing information and good practices through the design, hardware and software development, testing, transportation, installation, operation, maintenance and decommissioning of nuclear computer based systems.

The IAEA is grateful to the experts from Canada, Finland, Germany, the Netherlands, Slovenia, the United Arab Emirates, the United Kingdom and the United States of America who contributed to this publication, in particular J. Sladek (Canadian Nuclear Safety Commission), S. Eggers (Idaho National Laboratory) and M. Rowland (Sandia National Laboratory). The IAEA officer responsible for this publication was T. Nelson of the Division of Nuclear Security.

EDITORIAL NOTE

This publication has been prepared from the original material as submitted by the contributors and has not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily represent the views of the IAEA or its Member States.

Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

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

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

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

CONTENTS

1. INTRODUCTION

Nuclear security focuses on the prevention of, detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities [1]. Computers, computing systems and digital components have a continually expanding role in sensitive information management, safety, nuclear security and nuclear material accounting and control (NMAC) at facilities and operations.

Nuclear facilities and operations rely upon complex networks of suppliers, vendors and integrators to provide digital technology, services and support. The term 'supply chain' is commonly used to refer to a network involved in production and distribution of products or services for an end customer and includes the associated entities, resources and information. Supply chains can be viewed as the series of steps involved in producing and delivering a specified product or service to an end customer.

Adversaries are increasingly targeting the supply chain as a means for attacking secure operating environments. Compromise of the supply chain may provide a means to circumvent computer security measures that are in place to protect these secure environments. In a report of the European Union Agency for Cybersecurity [2], it is said:

> "Based on the trends and patterns observed, supply chain attacks increased in number and sophistication in the year 2020 and this trend is continuing in 2021, posing an increasing risk for organizations. It is estimated that there will be four times more supply chain attacks in 2021 than in 2020. With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common non-targeted attacks, and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure" [2].

It is good practice to implement a defence in depth approach that involves people, processes and technology in supply chain risk management. Supply chain risk management could be an integral part of the overall organizational risk management programme or management system. Computer security in the supply chain is an important element of supply chain risk management and the focus of this publication.

In response to the supply chain attack vector, security requirements on the nuclear supply chain have been introduced within nuclear security programmes such as Nuclear Energy Institute (NEI) 08-09 (Rev. 6) [3], and international and national standards such as the International Electrotechnical Commission (IEC) 62645 [4], IEC 63096 [5], and Canadian Standards Association Group (CSA) N290.7 [6]. Computer security of the supply chain is not unique to the nuclear industry, and standards such as ISO/IEC 27036-1 [7] and the Energy Power Research Institute (EPRI) cyber security procurement methodology [8] could also be applied to computer security in the nuclear supply chain.

1.1. BACKGROUND

An important element of supply chain risk management is the protection of assets, information and services within their development, production, provisioning and distribution (i.e. the supply chain). Generally, the challenges for each organization are the identification, analysis and evaluation of the risks associated with the supply chain. The strategy for supply chain risk management involves the reduction and protection of the supply chain attack surface (SCAS) through selection and use of appropriate risk treatment options (e.g. modifying risk by applying

computer security measures, avoiding the activity/supplier or transferring or sharing the risk). Supply chain risk management necessitates an understanding of the procurement life cycle, development of specifications and contracts to appropriately address computer security risk. The complex interrelationships and dependencies of contemporary supply chains increases the difficulty of risk management due to unknown, undisclosed or hidden vulnerabilities among the number of relationships within the supplier community (see Fig. 1).

IAEA Nuclear Security Series (NSS) No. 20, Objective and Essential Elements of a State's Nuclear Security Regime, recommends protection of sensitive information, which it defines as "Information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security" [1]. Supply chain activities to support nuclear security may involve the exchange of sensitive information between customer and supplier relevant entities. The value of information may differ between the customer and the supplier organizations. For example, in situations where the customer classifies the information as sensitive but the supplier does not, the supplier may specify insufficient information security requirements and/or apply ineffective security measures. It is key that both the customer and the supplier organizations understand the value of the information (if compromised) and protect it accordingly.

1.2. OBJECTIVE

The objective of this publication is to provide information on how to manage computer security risk in the supply chain and to assist relevant entities with developing computer security requirements that support the protection of sensitive digital assets throughout the procurement life cycle including design, fabrication, integration, testing, system delivery and system maintenance.

This publication aims to provide information on computer security in the supply chain and is structured to support newcomers to computer security, as well as seasoned organizations in applying computer security requirements and control to reduce risk in the supply chain.

This publication provides examples of international good practices from Member States on implementing computer security defence in depth as a protection against residual risks associated with the supply chain.

1.3. SCOPE

The scope of this publication includes any services, computer based systems and information, if compromised, that are supplied to a customer relevant entity that could adversely affect nuclear security.

This publication is applicable to the procurement of systems, including sensitive digital assets, used for nuclear material, other radioactive material and associated facilities.

The elements of supply chain risk management may apply to a wide range of computer based systems related to nuclear safety, nuclear security, NMAC and supporting functions (i.e. digital assets).

The intended audience for this publication is personnel with responsibilities managing risks in the nuclear supply chain. The intended audience includes customer relevant entities[1], supplier relevant entities, and other organizations.

Customer relevant entities include operators, licensees and nuclear power plant (NPP) integrators, competent authorities, regulatory bodies, individuals responsible for NMAC, export control authorities, and acquirer organizations within a State's nuclear security regime.

Supplier relevant entities include NPP integrators, suppliers (i.e. designers, vendors), technical support organizations and emergency response organizations, transport organizations (i.e. shippers, carriers), and supplier organizations within a State's nuclear security regime.

Other organizations include nuclear facility management, contract management, operations, maintenance and engineering personnel, research laboratories, national organizations for nuclear material accountability, and insurance organizations and think tanks.

1.4. STRUCTURE

This publication is structured to introduce the reader to supply change management approaches, and to assist the reader to understand the complexity of supply chain relationships between customers and suppliers including upstream suppliers' supplier, to understand the threat vectors throughout the supply chain life cycle, and to introduce the four phases within the supply chain (specify, source, use and correct) that can be used to minimize risk. The publication also provides key elements of information and computer security for readers that need to understand the important aspects of computer security to support computer security within the supply chain.

Following this introduction, Section 2 outlines key principles of supply chain management. Section 3 details essentials for information and computer security for the supply chain. Section 4 introduces the supply chain attack surface. Section 5 introduces the procurement process, and Sections 6 through 9 provide detailed information for each of the stages of the procurement process (specify, source, use, and correct). The appendices contain additional information and describe concepts and examples that may assist with the implementation of supply chain risk management. Annex I provides a guide to specific sections of interest based on the reader's background and experience. Annexes II–VIII provide additional perspectives on supply chain attacks, risk transfer, procurement methodologies, certifications, information sharing, communications, and examples of contract terms, conditions, and third party evaluation methods.

[1] Supply chain arrangements can sometimes result in organizations being both a supplier and a customer depending on their position within the supply chain. For example, NPP integrators are a supplier to the NPP operator, but also a customer to original equipment manufacturers (OEMs). See Section 4 for more detail.

2. SUPPLY CHAIN MANAGEMENT

A supply chain management committee is responsible for identifying and addressing emerging and ongoing challenges specifically related to computer security, including procurement challenges. It is a good practice for the committee to meet regularly to promote communication, collaboration, and accountability across functional boundaries within an organization to support computer security within the supply chain, and ensure effective oversight. Such a committee is most effective when all relevant departments within the organization are represented such as risk management, legal, information technology, security, nuclear engineering, internal auditing, and procurement. This group may be supported by a cross-functional team of front-line staff who meet regularly to share information regarding the status of current computer security activities and who can identify significant emergent issues for consideration and disposition by the supply chain management committee.

Section 2.2 of IAEA Nuclear Energy Series No. NP-T-3.21, Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Facilities, states:

> "Supply chain management encompasses the planning and management of all activities involved in sourcing, procurement, conversion and logistics management (according to the Council of Supply Chain Management Professionals). It also includes coordination and collaboration with channel partners, who may be suppliers, intermediaries, third party service providers or customers. Supply chain management integrates supply and demand management within and across companies" [9].

At its most fundamental level, a supply chain is a relationship between an acquirer (i.e. a relevant entity that procures a product or service) and a supplier (i.e. an organization or an individual that enters into an agreement with the acquirer for supply of a product or service) [7]. This single relationship represents one 'link' in a supply chain. This publication provides information about these two distinct groups, namely the acquirers and the suppliers. Each organization typically determines their placement within the supply chain for each relationship to ascertain the applicable guidance (see Appendix I).

The acquirer and supplier designations are context dependent since all organizations are likely to be either a supplier or an acquirer depending on the supply chain relationship. The acquirer and supplier are roles that each stakeholder might fulfil during the supply chain process (i.e. an acquirer will procure products or services from a supplier, and that supplier might need to acquire other products and services to fulfil their agreement).

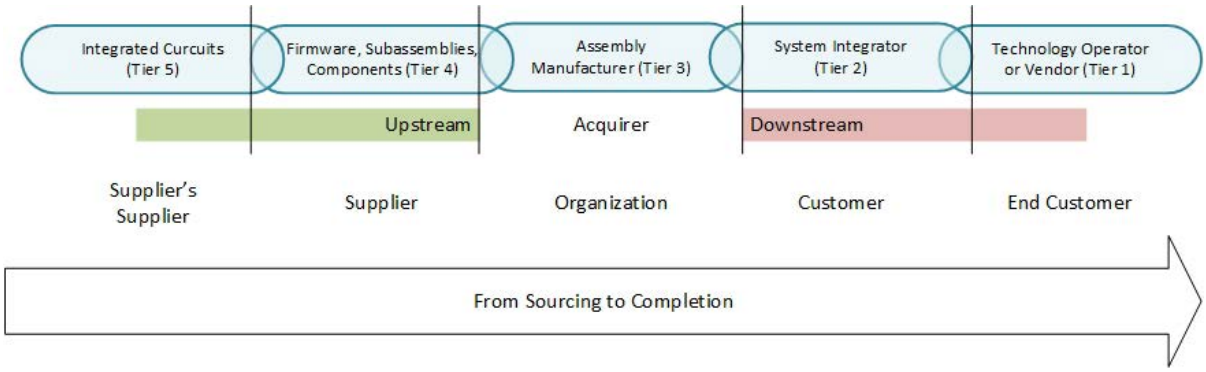

FIG. 1. Supply chain relationships (adapted from Refs [7, 9]).

Context is important in establishing supply chain relationships. For simplicity, the end customer is assumed to be the operator, licensee, or the organization having clear and direct nuclear security responsibilities in the State's nuclear security regime (i.e. compliance with mandatory national requirements or regulations; the organization at Tier 1). Figure 1 shows supply chain relationships. The tiers in Fig. 1 (supplier's supplier, supplier, organization, customer and end customer) align with the supply chain tiers of Ref. [9] (see also Fig. 10 in Appendix I), which are consistent with the relevant entities defined in Section 4. They also align with organizational responsibilities within a nuclear security regime from IAEA NSS No. 42-G, Computer Security for Nuclear Security [10]).

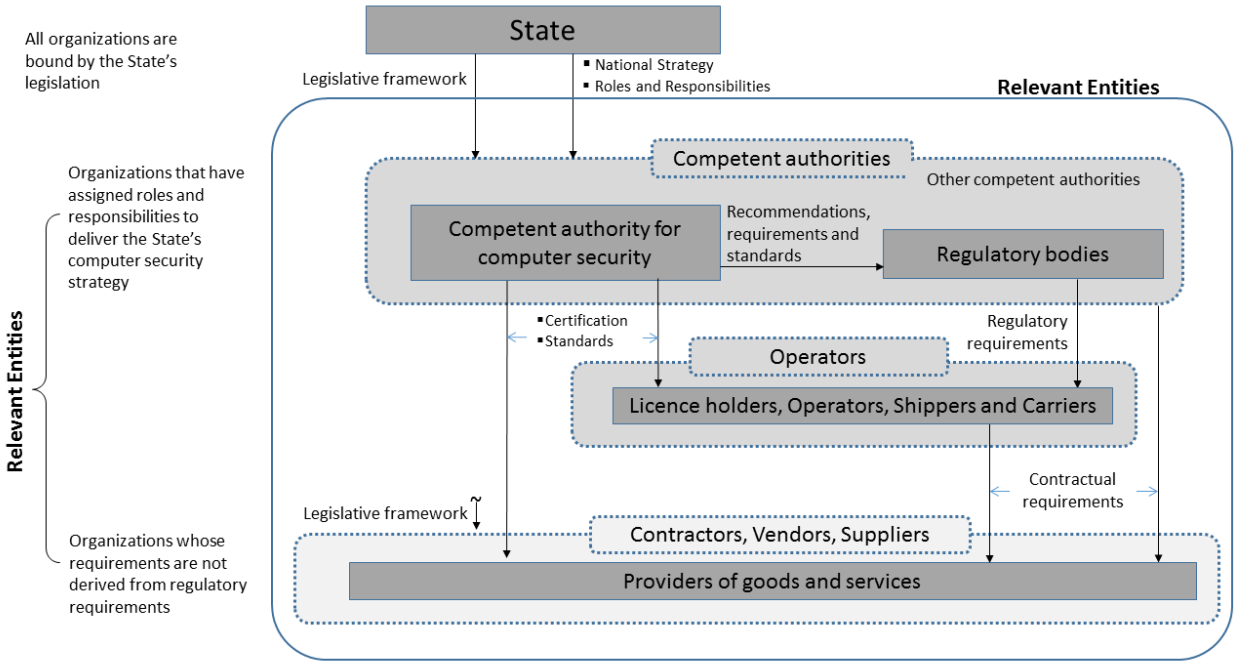

FIG. 2. Organizations having computer security responsibilities within a nuclear security regime figure 5 in Ref. [10].

The State maintains the national strategy and legislative framework with responsibilities to designate a competent authority with the rules, responsibilities, authorities, and accountability to enact regulations for compliance with the national strategy and legislation. The defined regulations are then imposed upon the operators and third party service providers (vendors, contractors, and suppliers) through licensing and contractual requirements for compliance with regulations and national law, which is summarized in Fig. 2.

The term 'relevant entities' refers to organizations having responsibilities for nuclear security within a nuclear security regime [10] including competent authorities; operators and vendors; contractors and suppliers. Since relevant entities are responsible for nuclear security within the supply chain, this publication classifies relevant entities (which can be both customer and supplier depending on the position within the supply chain life cycle) as:

— 'Customer relevant entities' – those that rely upon or operate items or services provided by a supply chain;
— 'Supplier relevant entities' – those that produce, develop, provide or distribute items or services provided by a supply chain.

All relevant entities have suppliers[2] (including vendors and contractors) that deliver goods or services. However, given the complexity of contemporary customer–supplier relationships, the supply chains of organizations have the potential to include a large number of suppliers each having their own complex supply chain relationships. Given the large number of suppliers and the complexity of their relationships, it is a good practice to have a robust supply chain management process.

Historically, safety considerations have been a major driver of supply chain management at nuclear facilities. However, given the growing risk resulting from adversaries with cyber skills targeting the supply chain of relevant entities, greater emphasis on computer security is essential (see Section 3) which will entail changing relationships and corresponding processes with external suppliers.

2.1. SUPPLY RELATIONSHIPS

Relevant entities establish supply chain relationships with vendors, contractors and suppliers for a variety of reasons such as focusing resources on core functions; acquiring capabilities that the relevant entity needs but does not possess; acquiring a utility or basic service that is commonly available; enabling work from remote locations and acquiring new or replacement systems which perform functions related to nuclear safety or security.

Relationships between the supplier and the acquirer exist both within and between relevant entities. Consequently, computer security within the supply chain is necessary in any supplier–acquirer relationship.

2.2. NUCLEAR MATERIAL AND FACILITIES

The supply of a computer based system to a nuclear facility involves both direct supply chain relationships (those organizations that are directly linked with each other through contractual agreements) and indirect relationships (those that affect other relevant entities, but are not directly linked. For example, the hardware original equipment manufacturer (OEM), the software developer, the systems integrator, and the NPP operator all have direct relationships, while the regulatory body and the independent computer security assessor are not in the supply chain line, as illustrated in Fig. 3. Indirect relationships can have a significant impact on supply chain risk management. For example, a compromise of regulatory bodies might result in the disclosure of sensitive information of an NPP operator.

[2] Reference [10] distinguishes contractors from vendors for simplification and to align more strongly with the term ‘supply chain’. In this publication, ‘suppliers’ is equivalent to ‘vendors’, ‘contractors’, and ‘suppliers’ as defined in Ref. [10].

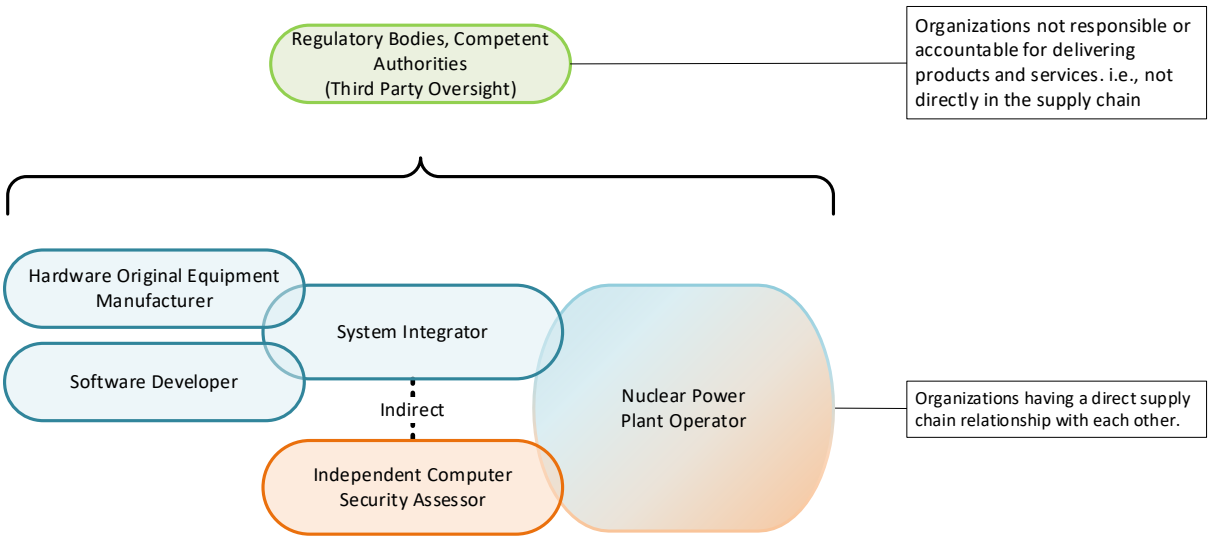

FIG. 3. Example of relevant entities relationships for nuclear facilities.

2.3. OTHER RADIOACTIVE MATERIAL

A radioactive material licensee has several supply chain management lines, including a physical protection system (PPS), sealed source manufacture, and radioactive material carrier, as illustrated in Fig. 4. In this example, there are two supply chains: one for the PPS and the other for the source material. The supply chain for the PPS indicates that there are direct relationships with the physical equipment manufacturer to the shipper and installer that are all linked to the radioactive material licensee. However, there is an indirect relationship between the shipper and the PPS installer.

The supply chain for sealed sources shows a direct relationship between the radioactive material licensee and the sealed source manufacturer and a radioactive material carrier, but there is an indirect relationship between the sealed source manufacturer and the radioactive material carrier. These two supply chains will have distinct sets of identified risks through indirect relationships, including common risks with different levels of consequence.

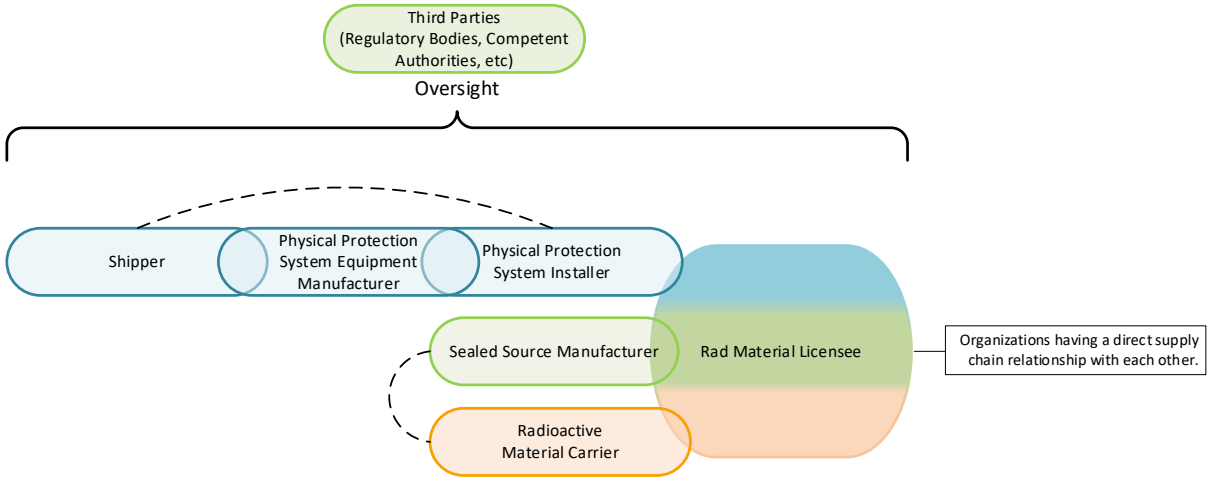

FIG. 4. Example of relevant entities relationships for other radioactive material.

2.4. MATERIAL OUT OF REGULATORY CONTROL

A government organization involved in nuclear security activities involving detection and analysis of material out of regulatory control is illustrated in Fig. 5. In this example, a State's national security operations centre builds an integrated nuclear security network by purchasing detection equipment and telecom services. These systems are turned over to other government organizations (e.g. customs officers, airport security, armed forces) for deployment and provision of physical security of the equipment in the field. Given the need for access of each of the providers and customs border patrol, the risk to the national security operations centre increases due to its exposure to additional organizations and their personnel.

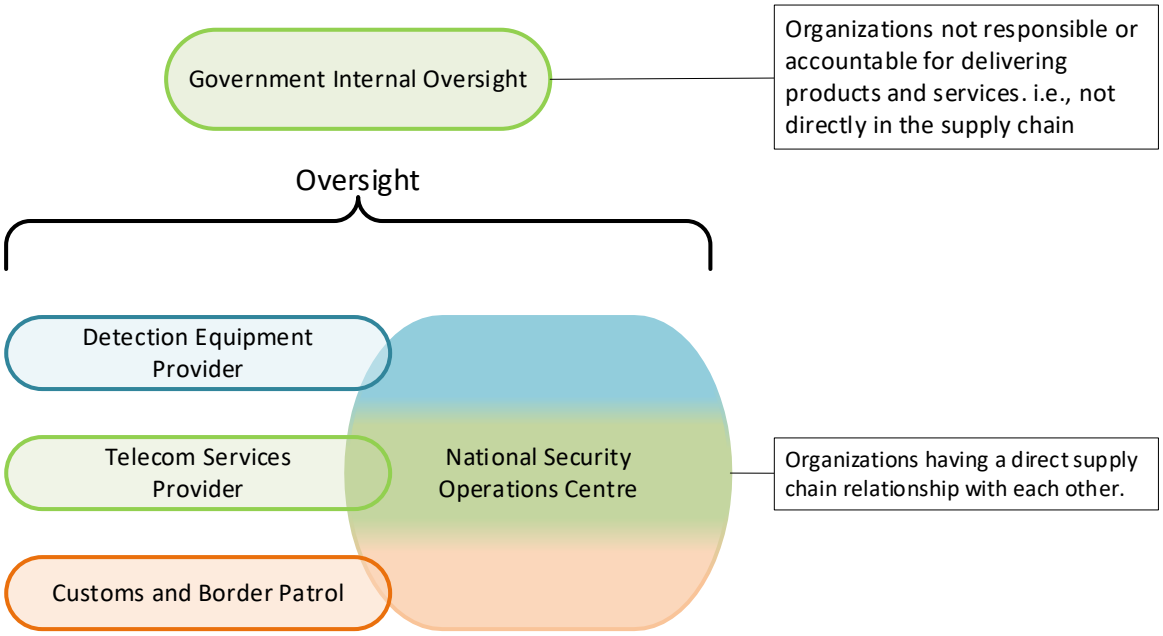

FIG. 5. Example of relevant entities relationships for material out of regulatory control.

2.5. COMPUTER SECURITY REQUIREMENTS BASED ON PRODUCTS AND SERVICES

Gaining a deeper understanding of the types of purchases and associated risks allows for better application of appropriate computer security controls. Computer security requirements could be incorporated into the purchase orders (standard, blanket, planned, contract) and agreements based on the type of purchase (catalogue, simple, complex) to incorporate computer security. See Appendix II for general information about the types of purchase orders, classifications and security levels.

The function[3] of the product or service being procured will have associated computer security requirements that will determine baseline computer security measures which the supplier may need to comply too. The procurement method chosen will likely determine the amount of

[3] A function is a coordinated set of actions, processes, and operations associated with a nuclear facility. Their purpose might include performing functions important or related to nuclear safety, nuclear security, nuclear material accounting and control, or sensitive information management.

influence the acquirer has in order to ensure that the supplier incorporates those measures into the product or service supplied.

Figure 6 illustrates the complexity of supply chain risk and computer security requirements based upon the relationship between purchase order, purchase order type, and computer security requirements. For example, in a standard catalogue purchase, the acquirer cannot impose computer security requirements on the supplier and accepts the risk with limited risk treatment options. Conversely, the acquirer may be able to transfer the risk and impose stringent computer security requirements on the supplier when using contract or planned orders across the types of purchase types to mitigate risk.

FIG. 6. Procurement matrix – increasing level of computer security requirements and complexity based on purchase types, classification and computer security level requirements.

To determine the complexity of procurement, a complexity matrix could be used to determine the type of procurement required (complex, simple, catalogue) and the attributes that contribute to the complexity of the supply chain. Complexity matrices assist in determining the level of resources and computer security requirements that will need to be applied and will also help the supplier achieve alignment with the organization's supply chain strategies. Annex VIII provides an example of a complexity matrix to assist acquirers with understanding the complexity of procurements.

Consideration of computer security of the supply chain typically occurs at the earliest possible stage of any procurement. This involves understanding the type of purchase; the type of product or service; the risk associated with the procurement (see Section 4); the acceptable risk threshold including prioritized risk treatment options (see Section 4) and the supplier tiers where involvement is necessary for the effective management of risk (see Fig. 1, Section 4 and Appendix I).

2.6. RISK TREATMENT OPTIONS

Risk treatment is the process of selecting the appropriate computer security measures to reduce risk. The type and classification of the purchase will constrain the risk treatment options that are available to manage supply chain risk. For example, for a catalogue purchase, risk transfer is limited and there is more reliance upon risk modification (e.g. application of security

measures by the end customer) and risk acceptance. If the end customer can establish strategic relationships with a supplier, there is a greater potential to include security arrangements that leverage this trusted relationship. In contrast, irregular or one-off purchases provide limited opportunity for the acquirer to include specific computer security requirements in the acquired product or service.

There are four options available for risk treatment [11]: risk modification, risk retention, risk avoidance, and risk sharing. These options are further discussed in this section.

Risk modification is an option that aims to reduce (or modify) the level of risk through introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable. System hardening is an example of risk modification by reducing the item's overall attack surface, thereby decreasing susceptibility to cyber-attacks which is correlated with a decreasing likelihood of a successful attack. Risk modification typically needs continual assessment and vulnerability analysis of the item and its associated controls.

Risk retention is an option that is available if and only if the risk level meets acceptance criteria and no further action is required. Catalogue purchases is a type of a purchase that is likely to involve risk retention. For example, commercial software (e.g. an operating system) contains unknown or undisclosed vulnerabilities. The risk is modified via the issue of patches by the supplier and installation of patches by the acquirer. However, the residual risk associated with the unknown or undisclosed vulnerabilities is retained (assuming that evaluated risk is tolerable and therefore no other measures are applied).

Risk avoidance is when the activity or condition associated with an identified risk is not performed or undertaken (i.e. avoided). Air gapping of systems is one example of avoiding identified risks associated with remote network attacks (i.e. attacks targeting systems that connect to authorized always connected, internetwork connections). However, risk is not completely avoided owing to other modes of information transfer (e.g. unauthorized network access points or connections; removable media or portable devices; supply chain) that could still provide attack pathways to adversaries (and therefore risk). Air gapping also eliminates the potential for 'real time' monitoring of security events occurring within the system, although deterministic one-way, fail-secure devices[4] can be used to provide real time monitoring, thereby avoiding this risk.

Risk sharing is an option that is critical for supply chain risk management. This option transfers all or part of the risk (i.e. shares) with another party that can most effectively manage it. Use of an indirect supplier (e.g. supplier's supplier) will necessitate the transfer of risk management to the supplier, as they have the direct relationship and the capability to impose conditions and computer security requirements or measures. Insurance agreements necessitate the transfer of the costs of risks to indirect stakeholders.

Transfer of risks and insurance agreements are not mutually exclusive and can be combined. For example, an acquirer may implement measures to reduce supply chain risk (risk modification) but may also share that risk with contractors or insurers.

Determining the level of risk and the selected risk treatment option typically needs an informed customer. For example, risk sharing can be accomplished through insurance contracts.

[4] In the ideal case, this avoids the risk associated with remote based cyber-attacks through authorized connections. However, certain data diodes may contain vulnerabilities that can be compromised to enable these attacks, thus acting as a risk modifier. Evaluation of security measures for vulnerabilities is typically needed to identify these vulnerabilities, assess their risk and ensure that the correct risk treatment option is identified.

However, an insured organization should prove that they are duly diligent in managing the level of risk outlined to acceptable levels established within the contract.

Once risk treatment options are selected, the procurement plan can identify the specific manner in which computer security risks and liabilities will be managed to include management of the risks within the contract (e.g. modification, retention, sharing); complete transfer of the risk (sharing); provision of good governance (required for insurance) or retention and modification of the risk by the acquirer (e.g. catalogue purchases, no direct or formal contracts, end-user licence agreement).

2.7. INFORMED CUSTOMER

Management systems make use of the concept of informed customer (also referred to as intelligent customer, knowledgeable customer or smart buyer) when planning, implementing and conducting supply chain arrangements. Capabilities typically are established in this area for organizations when using suppliers, vendors, contractors or external expert support [10]. Section 2.3 of Ref. [9] details some of the attributes of the informed customer for nuclear procurement; it states:

> "Some characteristics of an informed customer include (…):
>
> — A full understanding of the need for external expert's services and the context in which [support and/or service] is performed;
> — Knowledge of what is required and how the [support and/or service] will be used;
> — Knowledge of proper specification of objectives, scope and computer security requirements of the [support and/or service] so that the product will meet needs;
> — Knowledge of reasonable time frames for delivery of the [support and/or service] consistent with proper quality;
> — Knowledge and provision of site specific information that could be useful to the external expert;
> — An understanding of expected [support and/or service] outcomes;
> — An ability not to inappropriately influence [support and/or service] outcomes or advice from the external supplier or to allow any other body to do so, in order that the supplier advice reflects its own technical opinion;
> — An ability to oversee the [support and/or service] in accordance with the owner's procedures and management system and to perform technical reviews of the [support and/or service] when necessary;
> — An ability to ensure regular interaction with suppliers and facilitate interaction with other parties relevant to the task if necessary" [9].

For acquirers that have significant nuclear security roles and responsibilities, it is critical that the acquirer develop the necessary capability to perform the informed customer role.

The organizational capabilities of the informed customer could include [12]:

— Implements and sustains a strategy for managing information security risks caused by supply chain vulnerabilities (e.g. SCAS);
— Establishes and maintains baseline security controls to protect the supply chain;
— Establishes and adheres to nuclear supply chain life cycle processes and practices with an aim to protect the supply chain;

— Has a set of baseline computer security requirements that apply to all suppliers and custom (e.g. security levels, SCAS);
— Establishes a repeatable and testable process for establishing computer security requirements for suppliers (e.g. facility computer security risk management, system computer security risk management [13]);
— Establishes change management processes to ensure changes applicable to information or computer security are approved and applied in a timely manner;
— Defines methods for identifying and managing information and/or computer security incidents related to, or caused by, the supply chain.

These capabilities are in addition to those outlined in Refs [10, 12] and the nuclear procurement processes. It is good practice for the acquirer to utilize these capabilities in order to effectively manage computer security risk.

3. INFORMATION AND COMPUTER SECURITY ESSENTIALS FOR THE SUPPLY CHAIN

3.1. POLICY

Organizations typically have an information security policy in place that recognizes that adversaries may target the supply chain in their efforts to identify and plan attacks on susceptible systems. The policy could be integrated into an overall information and computer security policy or a subordinate policy. The policy is complementary to and compatible with safety procedures and practices. The information policy could include the following elements that [22]:

- is appropriate to the purpose of the organization;
- includes information security objectives or provides the framework for setting information security objectives;
- includes a commitment to satisfy applicable requirements related to information security; and
- includes a commitment to continual improvement of the information security management system.

Additional elements specific to supply chain:

- Acknowledge that the challenges of protecting the supply chain are significant (e.g. can impact the integrity, availability and confidentiality of systems important to safety), are diverse (e.g. can impact procurement language, vendor software development practices, maintenance contracts, chain-of-custody practices) and it is difficult to identify all suppliers in the supply chain (e.g. providers of systems, providers of components and subcomponents, parts manufacturers, integrators, transportation providers).
- Establish that a single procurement may cross many organizational boundaries both internal (e.g. engineering, procurement, legal, operations, security, maintenance, end customers) and external (e.g. supplier sales staff, supplier technical staff, supplier legal staff, transport, and system integration among different suppliers).
- Identify the need for strong interfaces between relevant entities to ensure computer security requirements are communicated and satisfied.
- Commit the organization to incorporate information and computer security requirements into systematic and repeatable procurement processes that are performed by appropriately qualified individuals.
- Ensure that computer security requirements are fully integrated into procurement related procedures and practices (e.g. specification preparation, contract language, vendor qualification, security provisions for spare parts storage).

3.2. ESSENTIAL ELEMENTS OF COMPUTER SECURITY

Information and computer security are essential to reduce risk in the supply chain. Awareness of sensitive information, sensitive digital assets, computer security level requirements, zones and a defensive computer security architecture is critical in applying computer security requirements and controls into the supply chain (see Appendix III).

Information security protects the confidentiality (unauthorized access and/or information release), integrity (unauthorized information modification) and availability (unauthorized denial of use) of information within the supply chain.

For example, protection of confidentiality is necessary for supply chain security as suppliers, vendors and contractors of services are likely to require authorized access to acquirer information, and in some cases, access to sensitive information. This authorized access increases the potential for adversaries to acquire this information due to inadequate security at other relevant entities. Addendum 7 to NEI 08-09, Revision 6 [15] identifies cyber threat attack pathways that could provide unauthorized access and disclosure of sensitive information that has the potential to result in increased risk to the acquirer.

Data is of particular importance since it is the bridge between information and computer security. Generally, protection of information is elusive as it can exist in intangible forms, and is therefore supplemented with the protection of data as it exists on computer based systems and associated networks [16]. Data has importance for both services and products. Additionally, data – especially sensitive information – is generally unique and irreplaceable.

Reducing the risk to information and computer based systems that can be compromised via cyber-attack is essential. The significance of the data or system may require computer security requirements for supply of products and managed throughout the entire procurement process. See Appendix III for more information on security levels.

Risk is also dependent on the threat associated with an adversary exploiting vulnerabilities of a digital asset or group of digital assets to commit or facilitate a malicious act. To defend against such acts, relevant entities perform a risk assessment or analysis to determine the inherent risk to their sensitive information, digital asset and computer based system to develop specifications and computer security requirements for products, services, and systems. See Appendix III for more information on computer security risk.

3.3. RISK MANAGEMENT

Traditional supply chain risk management balances objectives of cost minimization, quality and availability against potential disruptions from environmental, geopolitical and financial threats. Supply chain risk management for sensitive digital assets also balances the additional objective of computer security against cyber physical threats.

The information security goals of confidentiality, integrity and availability protection in information security, are similar to the objectives for supply chain risk management for sensitive digital assets that typically includes the protection of confidentiality, integrity and authenticity [17]. Similar to maintaining confidentiality and integrity in an operational environment, maintaining confidentiality in the supply chain ensures that components remain protected with no unauthorized access of data or secrets, while maintaining integrity ensures that components remain trustworthy, untainted and uncompromised. Maintaining authenticity in the supply chain ensures that components are genuine and not substituted or counterfeit. Maintaining exclusivity in the supply chain ensures limited possession, control or use of components by authorized and trusted relevant entities to reduce the number of cyber-attack entry points or touchpoints.

Although it is recognized that computer security objectives and threats are only a subset of the overall supply chain risk management for sensitive digital assets, the remainder of this publication focuses exclusively on the computer security aspects.

3.3.1. A State's nuclear security regime

IAEA NSS No. 42-G [10] and NSS No. 17-T (Rev. 1) [13] provide guidance on risk informed approaches for information and computer security. Reference [10] provides guidance on risk management for computer security within a State's nuclear security regime with roles and responsibilities assigned to organizations that are then provided with the resources to establish and maintain the necessary capabilities to execute their roles and responsibilities. It is therefore critical that a robust security culture is in place to provide the necessary resources and funding to manage supply chain risks[5].

Reference [13] provides guidance for two levels of security risk management: facility computer security risk management and system computer security risk management. These two levels can be considered strategic or tactical, and will produce computer security requirements based on the functions; criticality of the information and/or device; consequences based on threats and levels of required protections that can be incorporated into specifying computer security requirements in the supply chain.

In the case of commodity purchase or international supply of products and services, it is possible the supplier will not be subject to the State's nuclear security regime. In these cases, it is good practice that the security risk is managed by the regulated entity. Computer security requirements could be passed from the regulated entity to the supplier through contractual terms, or the regulated entity could undertake activities to address the risk (e.g. inspection, testing).

3.3.2. Information security management systems

Reference [7] addresses the information security management system and provides examples of risks directly applicable to the supply chain. Examples of supply chain vulnerabilities owing to inadequate security throughout the procurement life cycle include:

— During design and fabrication – an inadequately protected development environment could allow an adversary to access software or hardware and inject malicious code or components;
— During testing – when undetected vulnerabilities (e.g. software buffer overflows, faulty cabinet locks) could create vulnerabilities that could allow an adversary access to the system in the future;
— The system delivery path – could allow an adversary to access software or hardware either logically (e.g. during electronic delivery such as downloading software) or physically (e.g. during transport, at shipping facilities) and inject malicious code or components;
— In system maintenance – when poorly controlled access could allow an adversary (including an insider) to maliciously alter a system's behaviour, whether indirectly through code injection or directly through the system interface.

Important concepts for the information security management system for supply chain risk management include the following (shown alongside relevant IAEA publications and ISO/IEC standards):

[5] IAEA NSS 7 details the attitudes, beliefs, and behaviours that are part of nuclear security culture.

— Risk acceptance criterion: IAEA NSS No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [18], IAEA NSS No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [19], IAEA NSS No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [20], associated Implementing Guides and State Regulatory Framework;
— Context establishment: SCAS (see Section 4); scope definition, facility characterization and threat characterization [13];
— Risk identification: SCAS (see Section 4) and Ref. [7];
— Risk analysis: IAEA NSS No. 23-G, Security of Nuclear Information [21], and Ref. [10] in association with SCAS;
— Risk evaluation: IAEA NSS No. 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities [22], and Ref. [13];
— Risk Treatment: ISO/IEC 27001:2013 [14] (Refs [3, 4] for NPPs); ISO/IEC 27002:2022 [23] (Ref. [5] for NPPs); ISO/IEC 27036-2:2014 [24] and system computer security risk management [13];
— Monitoring and review: assurance activities.

3.4. DIGITAL ASSETS AND SECURITY LEVEL IDENTIFICATION

Attack vectors within the supply chain provide adversaries with increased opportunities to access digital information and systems (e.g. during development, shipment) and to potentially maliciously alter the function[6] (e.g. digital asset). It is possible that compromise of functions while in development are not observable, and there could be increased opportunities for the adversary to use stealth. These opportunities provide tremendous value to potential adversaries.

Wired networks, wireless networks, portable media and mobile devices, physical access and supply chain are attack vectors [13, 14]. These attack vectors exist at the acquirer, the supplier, and throughout the supply chain. It is good practice to recognize that these attack vectors may exist in supplier relationships and that they could have different attributes (e.g. exposure, mode of use, frequency of access) for each organization. The supply chain attack vector may lead to increased uncertainty unless actions are taken to minimize the potential of adversaries to access and/or leverage this access to those attack vectors that exist at the supplier and sub-suppliers.

Supply chain relationships add to risk complexity as suppliers might be relied upon to directly provide the function; provide support for the correct operation of the function (e.g. design services, maintenance, inspection), or provide information upon which critical attributes of function assignment, performance or validation depends. This complexity and the need to transfer risk to the supplier to control access to attack vectors and detect unauthorized access increases uncertainty.

Maintenance services may also be necessary to ensure the correct operation of the computer based systems. However, this may allow for a malicious exchange of data or information (e.g. virus, worm) that results in the maloperation of the system and the non-performance of the function.

[6] A function is a coordinated set of actions, processes and operations associated with a nuclear facility. Their purpose may be, but is not limited to, performing functions that are important or related to nuclear safety, nuclear security, NMAC or sensitive information management.

The concept of attack surface can be defined as a digital asset's full set of actual or potential vulnerabilities. Attack surface is defined as "The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from [that system, system element, or environment] [25]."

The concept of attack surface is of paramount importance for the management of information and computer security associated with supply chain relationships. Understanding and minimizing the attack surface and implementation of a defensive computer security architecture and computer security measures by the acquirer is key to establish effective risk management and defence in depth approach for the protection of both information and digital assets in the supply chain.

Defence in depth involves the use of multiple layers of protection measures, so that protection is provided when one measure fails or is circumvented by an adversary [18]. For example, the failure of boundary protections to mediate and control access would allow the adversary to access digital assets within the zone. Therefore, providing measures in the zone may minimize susceptibility to, and may detect, potential cyber-attacks by an adversary having either direct or indirect access.

4. SUPPLY CHAIN ATTACK SURFACE

A supply chain attack surface (SCAS) is the set of touchpoints (interactions) between the acquirer and supplier organizations that an adversary can use to compromise hardware, firmware, software or system information during supply chain activities, including relevant entity locations, physical or electronic storage locations and transitions between these locations. Touchpoints can be generally understood as any independent relevant entity as well as any exchange (e.g. information, data, product, service) between two relevant entities. These touchpoints are potentially additional areas of compromise to consider in a relevant entity's design basis threat (DBT) and/or risk assessments. A SCAS can be used to establish context for the identification of supply chain risks.

Understanding what the SCAS is for a product or service, and how to apply the concept while identifying supply chain risks, is essential and a critical part of effective computer security risk management for the supply chain.

Supply chain relationships typically involve multiple tiers of globally scattered suppliers throughout the supply chain. This network includes designers, developers, contractors, manufacturers, integrators, solution providers and logistics providers (including shippers, carriers and customs agents). The complexity of these networks provides numerous possibilities for an adversary to compromise a service or device, or to acquire system information prior to use within a facility or organization within the nuclear security regime. The challenge is how to reduce risks associated with compromise (e.g. cyber-attack) of elements within the supply chain [26].

An example of a SCAS is provided in Annex II, Figs II–1 and II–2, which illustrate supply chain attack patterns and identify points of attack at supply chain locations and logistical linkages [27].

Figure 7 (adapted from Ref. [28]) provides an additional example of a SCAS that extends the work of Ref. [27]. The example in Fig. 7 illustrates a typical supply chain life cycle from initiation (system analysis) through development (hardware/software design and integration), up to delivery (testing, installation, and site acceptance testing) and decommissioning. Throughout the supply chain life cycle, relevant entities are identified (relationships) within each stage of the supply chain, including supply chain attacks that can also be used at each touchpoint in the process, identifying potential supply chain cyber risk. By combining relevant entities and supply chain attacks in each phase of the supply chain, threat vectors are identified, which define the SCAS. The stacked boxes also represent multiple components and indirect suppliers that are integrated to make up a supplied item.

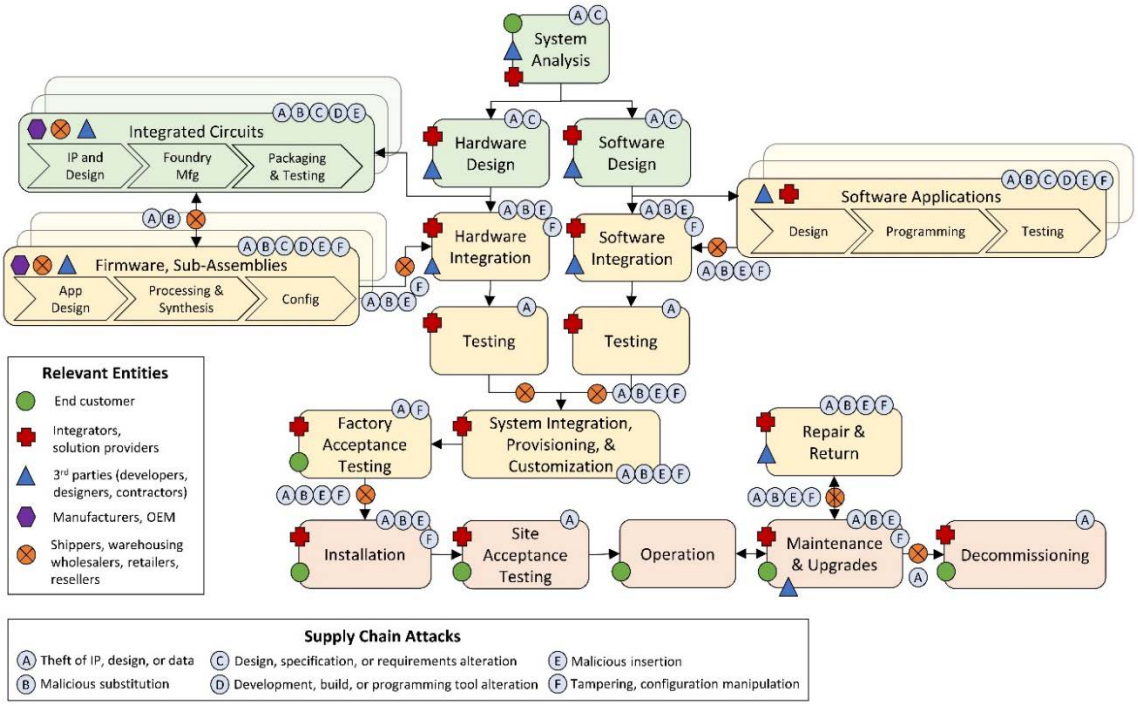

FIG. 7. Notional example of a SCAS (adapted from Ref. [28]).

4.1. SUPPLY CHAIN FLOW PATHS

A SCAS typically includes systems engineering and supply chain activities, including individual flow paths for hardware, firmware and software design and development activities as well as flow paths for final integration, testing, installation, maintenance and decommissioning activities [28].

An analysis of the SCAS can be aligned with the systems engineering life cycle outlined in IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [29], and in IAEA NSS No. 33-T [22]. Controls applicable to equivalent life cycle stages can be applied at the relevant entity locations or touchpoints.

A SCAS and a platform and development life cycle from Ref. [5] are also related. Reference [5] contains recommended controls for instrumentation and control (I&C) systems in NPPs for both the I&C platform development and project engineering phases. Section 4.1 of Ref. [5] provides a mapping of these phases to the life cycle activities.

4.2. RELEVANT ENTITIES

Identification of relevant entities is critical in establishing context for supply chain risk management and analysis of the SCAS. Each relevant entity represents an entry point susceptible to attack by an adversary wishing to harm the acquirer.

A SCAS could include relevant entities, such as:

- End customer (operator–licensee);
- Integrators (tier 1 and tier 2 [9]; vendors, suppliers [10]);
- Third parties (services [9]; contractors, competent authorities, regulators, maintenance and inspection services [10]);
- Manufacturers, OEM (tiers 3 to 5 [9]; vendors, suppliers, contractors [10]);

— Shippers, warehousing, wholesalers, retailers, resellers, customs agents (various [7, 12, 24]; services [7, 9]; shippers, carriers [10]).

An example of supply chain relationships in which arrangement of the above categories forms a single direct supply chain relationship can be found in Fig. 1. The acquirer and supplier designations are context dependent (i.e. an organization in an established supply chain relationship with another organization can be either an acquirer from or a supplier to that organization).

Each group of relevant entities is associated with different sets of risks. Examples of these risks are provided below using a SCAS analysis.

A licensee, such as a hospital, is responsible for managing the identified risks (e.g. via a SCAS analysis) to ensure the security of the radioactive material that is used and stored on its premises. The end customer has a responsibility to have a high level of assurance that a PPS is hardened against cyber-attacks. There is a risk that the end customer may fail to put in place effective procurement specifications that require the supplier to harden the systems and address critical vulnerabilities. Deficiencies in risk management have the potential to increase the susceptibility of a system to cyber-attack.

Integrators are the key supplier of the end customer (especially NPPs). Integrators typically use commercial off the shelf (COTS) or pre-developed items to design, integrate, test, build and sometimes install, commission and maintain nuclear systems, including safety, operational and security systems [29, 30]. Successful attacks against an integrator resulting in information disclosure or compromise of supplied products presents significant risks throughout the entire system's life cycle. Some of these risks are identified in Section 3.3.2.

Third parties that provide maintenance and inspection services to operating equipment will require authorized physical and/or logical access to systems. This may require access to sensitive information associated with the system(s) (e.g. configuration, passwords, security measures) to allow them to proficiently provide the service ('need to know').

It is possible that OEM vendors providing pre-developed software for a specific system have not applied techniques to minimize vulnerabilities (secure coding), have not applied necessary measures to identify and correct these vulnerabilities prior to distribution (e.g. penetration testing and patching), or in the worst case do not have processes in place to handle receipt, reporting and correction of vulnerabilities (e.g. no vulnerability management). These deficiencies lead to downstream relevant entities (e.g. end customer, integrators) inheriting risks from upstream. Reference [7] describes this as a quality risk.

When shippers and warehousing provide a service, typically the risk to the product in transit and storage is considered. If the shipment crosses a border, risks associated with customs and border services are typically considered. For example, a system stored at a shipper's warehouse could be subject to tampering or modification in a manner to evade detection during site acceptance testing. Reference [7] describes 'equipment offsite' or 'access to information and information systems onsite' as an example of information security risks for acquiring services.

The categories of relevant entities in a SCAS analysis may be associated with risks that are typically analysed and evaluated in the specify and source stages (see Sections 5 and 6); typically treated (by the end customer) in the use stage (see Section 7) and typically monitored and reviewed in the correct stage (see Section 8).

The level of effort to identify all relevant entities within a supplier relationship (see Fig. 1) could be dependent upon the following:

— Type of relationship: acquirer, supplier or third party;
— Type of purchase order: standard, blanket, planned or contract;
— Applicable nuclear supply chain tiers;
— Supplied item: products, services or hybrid;
— Type of supplied product: catalogue; simple or complex;
— Computer security requirements (security level);
— Information protection requirements (e.g. top secret, secret, confidential, unclassified but sensitive).

The number of tiers involved in formalized supply chain relationships with the acquirer is dependent on the level of risk associated with the supplied item. Computer security level requirements specify how the tiers of relevant entities involved in the purchase are identified. These computer security requirements may also indicate the nature of the relationship (e.g. direct, delegated, inferred) that is permitted between the acquirer and the supplier tier. For example, the computer security requirements state whether it is acceptable to delegate supplier management to the integrator for lower tiers of a supplied item assigned a specific computer security level.

Systems assigned the most stringent security level (security level 1) [13] are likely to require formalized contracts between the acquirer up to and including tier 5. This will also likely require the use of a contract or planned purchase order since this is a complex product procurement.

Systems assigned the least stringent security level (security level 5) may use an end user licence agreement (EULA, i.e. arrangements that possibly are not known before use or installation[7]) or blanket or standard purchase orders to define the supplier relationship between the supplier (e.g. tier 1) and acquirer.

Relevant entities are a common element between IAEA publications and industry supply chain guidance as detailed in Fig. 7 above [28], Figs II–1 and II–2 in Annex II [27], and these have an impact on Fig. 12 [10]. In Fig. 8, the tiers of relevant entities are reflected by the colours of the boxes. These relevant entity boxes correlate to the ‘supply chain locations’ noted in Ref. [27]. The attack pathways are transformed to less abstract attack types aggregated in Fig. 7. In this manner, Fig. 7 brings together IAEA and industry guidance into a single representation of computer supply chain risk.

4.3. SUPPLY CHAIN TOUCHPOINTS

Touchpoint transitions can be direct (where the relevant entities and relationships are identified) and indirect (where the relevant entities are not identified such as a supplier’s supplier). This publication will consider risks associated with transition touchpoints as including the interval whereby the product or service is at the source touchpoint (after completion of the factory acceptance test), in transition between touchpoints (shipping or information and communication technology (ICT) communication), and at the destination touchpoint (prior to commencement of installation and/or the site acceptance test).

[7] EULAs may involve shrink-wrap or click-wrap licences. The term ‘shrink-wrap licence’ refers colloquially to any software licence agreement which is enclosed within a software package and is inaccessible to the customer until after purchase. The term ‘click-wrap licence’ is a licence that may be presented to the user on-screen during installation.

An example of a direct relationship is a catalogue purchase of a data diode (i.e. unidirectional communications device) from the technology vendor. An indirect relationship exists where the vendor's shipper is used to transport the data diode to the end customer's site.

Another potential indirect relationship for the data diode exists if the vendor's product contains open-source software (e.g. SELinux). Use of open-source software creates an indirect touchpoint with the developer(s) of the software (e.g. SELinux; Red Hat Software and their contributors).

A subset of touchpoints is supply chain linkages as described in Ref. [27]. These supply chain linkages identify the points of attack that are organized based upon two classes: (i) logistics attacks that require physical access to the product; and (ii) ICT attacks that require logical access to the touchpoints (or points in between).

The attack pathways (see Section 3) most applicable to the classes of attack are portable interfaces and physical attacks (logistical attacks), and wired networks and wireless networks (ICT attacks).

The supply chain is another attack pathway. Although an end customer (acquirer) may attribute an attack to the supply chain attack pathway, attack specifics reveal that it is usually one or more of the attack pathways listed above. For example, theft of a vendor's private keys may occur using a wired network (e.g. remote cyber-attack, phishing), physical attack (e.g. infiltration into secure building), or portable interface (e.g. insider with malicious universal serial bus). Nevertheless, these would be considered supply chain attacks from the acquirer's perspective.

It is important to consider touchpoints and their attack pathways during risk identification to ensure that these risks are effectively managed.

4.4. ATTACK TYPES

Adversaries have applied techniques and methods that target the supply chain to compromise functions of, and add new malicious capabilities to, computer based systems. Examples of these techniques and measures include malware or tool implant; device substitution or replacement; unauthorized use of credentials or access; and malicious software updates. Additionally, publicly disclosed supply chain attacks have identified malware that has been designed to perform reconnaissance (gather information) in the supply chain to help better understand the target operating environment [9]. This information may include sensitive information regarding security arrangements, how control systems communicate, and details of the operational environment.

Other supply chain attacks involve the introduction of malicious code via infected removable media, or a portable device used by a person having authorized physical access to the system (e.g. external contractor, unwitting insider[8]). The malware, once introduced, may establish persistence (i.e. techniques adversaries use to keep access to systems) on the affected network and systems. Suppliers of products and services to nuclear facilities represent highly valuable targets to the adversaries to achieve their malicious aims, especially for equipment that contains COTS software components or hardware modules.

[8] An unwitting insider is an insider without the intent and motivation to commit a malicious act who is exploited by an adversary without the unwitting insider's awareness. An unwitting insider could be an employee or authorized subcontractor who has access to systems.

Reference [26] (see Fig. 7) provides examples of six attack types:

Theft of internet protocol address, design or data:

- Unauthorized disclosure of information–confidentiality violation;
- Supplier compromise that enables future attacks on the end target;
- Examples include but are not limited to the theft of design information, operational–configuration data, private key and digital certificates.

Malicious substitution:

- An unauthorized modification or alteration of information (integrity violation) of a supplied item that compromises any end customer of that item (beyond the intended victims);
- Supplier compromise that affects all end customers of compromised service or product;
- Examples include the ASUS ShadowHammer Attack and the Dragonfly Attack.

Design, specification or computer security requirements alteration:

- Unauthorized modification or alteration of information (integrity violation), specifically information provided by the end customer (or standards group) and used by suppliers;
- Compromise in design stages that results in the purposeful inclusion of latent design deficiencies (vulnerabilities) or built-in backdoors;
- An example is the Solorigate backdoor malware (also referred to as SUNBURST) that allowed back door access to an affected device through a supply chain attack of the dynamic link library that was deployed through a vendor product [31].

Development, build or programming tool alteration:

- Unauthorized modification or alteration of information (integrity violation), specifically an intermediary product that is necessary to develop, build or service the end customer product;
- Compromise of a tool to enable future attacks on end customers of the product (e.g. corruption, backdoors).

Malicious insertion:

- An unauthorized modification or alteration of information (integrity violation) of a supplied item that intentionally compromises an end customer or group of customers and not unintended victims;
- Attack is the opposite of substitution attack in that it discriminates between intentional and unintentional victims;
- Typically, involves targeting a specific end customer supplied item that will be exclusively used by the intended victim(s). This attack occurs in SCAS stages in which the end customer is a relevant entity.

Tampering, configuration manipulation:

- Unauthorized disclosure, unauthorized modification or alteration and/or unauthorized denial of use (confidentiality, integrity and availability violations) at any point within a SCAS;
- Associated with touchpoints and not relevant entity locations. Configurations that enable (remote) services or products to be transported;

— Typically, occur between life cycle phases (e.g. after verification and validation or testing activities have completed);
— Tampering specifically denotes logistics attacks, whereas configuration manipulation can apply to either class of attacks (logistics, ICT).

5. TYPICAL PROCUREMENT PROCESS

The typical procurement process is made up of four stages (specify, source, use, and correct) and are described as follows:

- The specify stage is essential in defining computer security requirements and the planning and management of contracts;
- The source stage is essential for quote evaluation, negotiation and contract agreement;
- The use stage is essential for assurance activities (such as factory acceptance testing and site acceptance testing), installation and commission, operation, maintenance and services;
- The correct stage is essential for monitoring and implementing improvements or reducing deficiencies and vulnerabilities, and in extreme case termination of the contract due to repeated non-compliance.

Figure 8 illustrates the four major stages and activities performed during each stage that are directly relevant to nuclear and computer security.

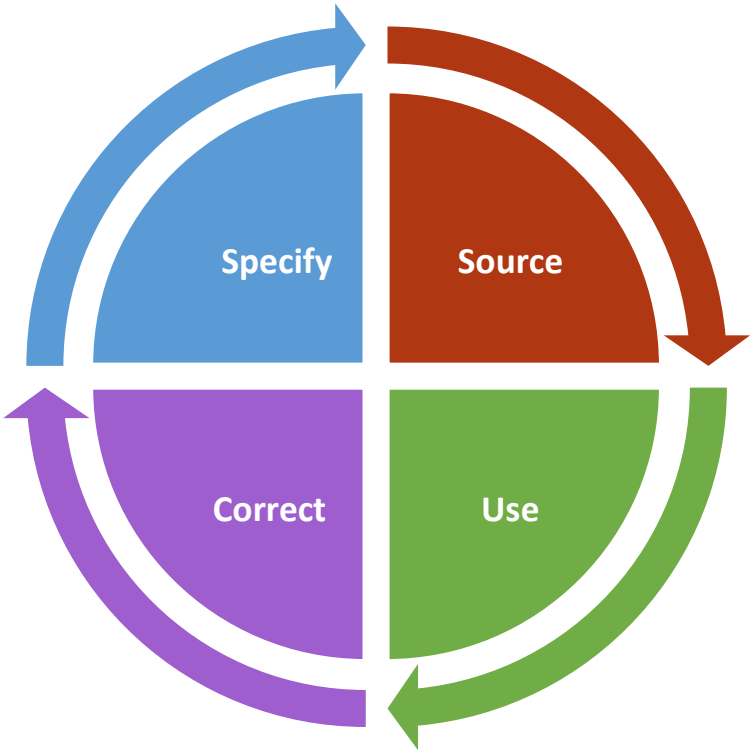

FIG. 8. Nuclear procurement model (adapted from figure 5 in Ref. [9]).

The computer security requirements can be overlaid on this model by an informed customer to ensure that nuclear security is applied appropriately for protection from supply chain compromise.

6. SPECIFY STAGE

The specify stage is the first and most critical stage (as shown in Fig. 8) in the procurement process that requires effective processes for information management and computer security risk management.

The specify stage includes:

6.1. NEEDS IDENTIFICATION

The use of a SCAS analysis (see Fig. 7) can aid in identifying potential and significant risks. This aids in the establishing of both functional and contractual requirements. The functional specifications are based on safety, security and system function or functions performed as well as the computer security level requirements. The contractual requirements establish how the supplier is contractually bound to provide for computer security (risk transfer); the stringency of these computer security requirements is determined by the acceptable risk (risk tolerance of the acquirer), which is informed by the type of purchase order.

6.2. PROCUREMENT PLANNING (MANAGEMENT OF PROCUREMENT STAGES)

This step identifies and outlines the major milestones in the procurement of products or services. It also includes preparation of a procurement plan which includes risk and mitigative actions which could include the prioritization of risk treatment options, defining key supplier relationship processes, procurement scenarios and supplier selection.

The risk treatment options are driven by acceptable risk. Risks that cannot be tolerated are to be avoided or modified (imposition of measures). The supply chain typically involves risk transfer to the supplier by the acquirer.

The supplier relationship engagement process informs how suppliers are engaged, their obligation to provide for computer security and how this security is verified. The supplier relationship management process is how the acquirer imposes milestones and a schedule. The acquirer may gain rights to inspect or assess certain aspects of the supplier's computer security. The supplier relationship termination process is established when the acquirer specifies completion or adverse conditions clauses that provide for a termination of the supply relationship.

Potential procurement scenarios and supplier selection typically considers their ability to provide for computer security and assesses their capability to manage the risks transferred to them. Scenarios are developed to verify the computer security of the supplier or supplied item. For items providing, supporting or relied upon by significant functions (e.g. safety, physical protection), scenarios are based on the identified threat or DBT.

6.3. DEFINING ACCEPTANCE CRITERIA AND METHODS

Acceptance criteria and methods will define how to verify acceptance of products and services, and by whom (e.g. acquirer, supplier, third party). The definition of acceptance criteria is informed by risk. Therefore, risk management phases below are necessary to ensure that acceptance criteria are coherent with risk tolerance.

Context establishment (State legal and regulatory framework [10, 18–20]):

— An essential part of this is **risk acceptance criteria**. For example, information and computer security risks associated with unacceptable consequences (e.g. unacceptable radiological consequences, unauthorized removal of Category I nuclear material or Category 1 radioactive material) have limited risk treatment options (risk modification or risk avoidance is required).
— A SCAS analysis (or similar) can be used to identify risks associated with both direct suppliers and supplier's suppliers (indirect) to establish internal context (set of organizations most significant to supply chain risks).

The specify stage process is structured as follows:

Risk identification (SCAS (Section 4), facility or threat characterization [13], DBT and Refs [3, 4, 12, 28]):

— Identify risks using a systematic and planned process. The planning of procurements occurs during the specify stage when needs are identified.
— Use a SCAS analysis (or similar) to ensure a comprehensive and complete identification of risks.

Risk analysis (classification of information [21]; computer security levels [13]; supply chain computer security requirements for ICT [24]):

— Determining the nature and level of risk is typically correlated with the sensitivity of information and/or the significance of the function performed by the procured item or service. Based on the consequence of the function, a security level will be associated with a set of requirements (see Section 6.2) that are imposed on the system(s) performing the function.
— Recognize whether the supplier relationship is direct or indirect. Direct supplier relationships involve contracts whereby the acquirer (or end customer) is bound to one or more signing parties subject to a contract. This allows risks to be managed explicitly through compliance with the contract requirements imposed by the acquirer onto the signatory parties (suppliers). However, in the case of indirect supplier relationships where the acquirer has no influence over the supplier's supplier, the risk is effectively transferred completely to the acquirer's direct supplier to manage risks associated with the supplier's supplier depicted in Fig. 10.

Risk evaluation (facility computer security risk management [13], organization computer security risk management [10], Refs [3, 21]):

— Compare the results of the risk analysis to determine whether the level of risk is acceptable or tolerable [11].
— Be aware that risk acceptance criteria determine the level of acceptable or tolerable risk and that this may be different for each of the identified risks. Some risks have associated regulatory or legal requirements, thereby limiting risk treatment options.
— A computer security analysis or risk assessment is typically performed as early as possible (e.g. in the design phase) to identify and assess the computer security requirements. These analyses could consider any vulnerability analysis of the technical, administrative and physical control measures, and specific threat and attack scenario analysis (including the State specific DBT, as applicable). Risk assessments may lead to the improvement of security measures in order to reduce vulnerabilities.

Risk treatment (system computer security risk management [13], Refs [3, 4, 11]). The specify stage mandates the type of risk treatment that is selected.

It is good practice to incorporate effective processes for supply chain risk management into the computer security programme that manages risks related to computer security. It is appropriate for senior managers to prioritize enterprise risk management and integrate good governance into all levels of activities. Demonstration of good organizational governance, including attempts to abide by most current industry practices, will provide evidence of compliance to regulators but also protect the acquirer from potential liability in the event of an incident. Liability can include financial, reputational, civil or criminal.

Management typically reviews its organizational risk appetite periodically, assess its ability to protect and/or ensure against incidents, seeks to obtain contract protections and demonstrate good governance via appropriate risk assessments and risk management (International Standards Organization, 2018).

Typically, the nuclear industry has been hesitant to specify newer technologies despite their potential to provide a higher level of security[9] owing to one or more of the following factors:

— Use is neither widespread or mature resulting in difficulty in meeting or conflicting with safety;
— Security features or functions add complexity that increases the difficulty of deployment and verification and validation testing;
— Fear of increasing attack surface or increasing susceptibility to cyber-attacks.

The specify stage typically identifies security technologies and their associated demands (test equipment, security tools, software, resources and specialized training) to provide a high level of confidence that computer security requirements can be met.

6.4. RISK IDENTIFICATION

Needs identification for computer security of the supply chain requires that the acquirer is an informed customer (see Section 2.7). The acquirer is responsible for the risks associated with how the supplied item (product and/or service) is relied upon to provide or perform significant functions within the nuclear security regime. The acquirer typically identifies all unacceptable risks based on the significance of the function. Section 3.1.1 of NP-T-3.21 states:

> "This [needs identification] step involves an [acquirer] individual or organization identifying that an item or service should be purchased. The information needed is what is required, where that item will be used and for what purpose. The information may be very detailed (e.g. specific make and model of a part to be purchased) or be more in the form of a general requirement or description that might be filled in a variety of ways" [9].

The type of item or service and the type of demand for those items or service are important to identify. The type of item procurement listed from lowest to highest risk are catalogue, simple or complex. The types of demand include, but are not limited to, those associated with major projects; outages; services; spares or reorders; modifications and/or configuration changes; and

[9] Newer products that implement security technologies generally require greater computer security competence to test, configure and use these newer technologies.

emergency replacement or support services. Demands can be both long term and short term (once only), or to support a particular time period or a particular activity, such as an outage.

Use of catalogue purchase orders is typically restricted to the lowest risk since it is unlikely that the acquirer would enter into a direct and formal contract with the supplier requiring some level of risk acceptance or modification. However, complex purchases associated with the highest potential for risk are likely covered through both a direct and formal contract with one or more suppliers and a separate project charter to increase vigilance with respect to risk management [32].

Requirement 11 of IAEA Safety Standards Series No. GSR Part 2, Leadership and Management for Safety, states:

> "The organization shall put in place arrangements with vendors, contractors and suppliers for specifying, monitoring and managing the supply of items, products and services that may influence safety" [33].

As noted in Ref. [9], specifying the requirements for such items, products and services is a key role of procurement documents.

6.5. ESTABLISHING COMPUTER SECURITY REQUIREMENTS

Information and computer security requirements are informed by Refs [10, 13, 20, 21]. Computer security requirements assume that all organizations, products and services are potentially susceptible to cyber-attack. Suppliers could have a computer security programme as well as processes in place to receive and provide solutions (patches, mitigations, workarounds) to vulnerabilities.

The suggested computer security requirements (Sections 6.5.1–6.5.4) can be applied to any relevant entity within a State's nuclear security regime.

General computer security requirements for procurement–supply chain is typically implemented at all end customers within a State's nuclear security regime.

The end customer could establish a graded set of computer security requirements (i.e. information sensitivity or classification levels, security levels) to ensure that risk is appropriately managed in a systematic manner.

These levels are typically based on the severity of the consequences as follows:

- General computer security requirements (baseline (always applied) conditions that also address limited or negligible risks);
- Computer security requirements for supplied items (product and/or service) associated with **moderate** impacts;
- Computer security requirements for supplied items (product and/or service) associated with **high** impacts;
- Computer security requirements for supplied items (product and/or service) associated with **severe** impacts.

6.5.1. Computer security requirements for procurement

All procurement stages (specify, source, use, correct) typically have computer security requirements for information and computer security to ensure that risk is managed to, or below, acceptable or tolerable levels for all types of procurements (catalogue, simple and complex).

Generally, suppliers will have an information and computer security policy that systematically manages risks from information theft or cyber-attacks. Consideration is typically given to those suppliers that are able to demonstrate effective risk management.

Computer security requirements for procurement could consider the following:

- Dependent on the safety or security functions to be performed, the general conditions are likely to have additional specific computer security requirements to address procurements associated with moderate, high or severe impacts.
- Mandatory inclusion of additional computer security requirements when the severity of impact meets or exceeds the moderate level. This includes computer security requirements applicable to sites where a vendor, contractor or supplier performs activities. Additional computer security requirements are clearly and contractually specified by the acquirer based on the assigned security level or classification of information.
- Integration and compatibility with other computer security requirements that are needed for operations, safety, security and physical protection. These may include technical and quality computer security requirements and physical protection regulations.
- Commercial specifications such as commercial contract strategies, commercial conditions of importance and standard commercial terms and conditions.
- Administrative controls necessary to ensure proper management of the supplier as well as ensuring that risk is effectively addressed or sanctions and penalties are able to be imposed.
- The level of rigour of information and computer security processes that need to be implemented at supplier organizations.
- The level of assurance necessary to confirm that suppliers meet all applicable computer security requirements. This includes the application of computer security measures specified by the acquirer, during support provided on-site or at the vendor, contractor or supplier's workplace and during any transit or storage of purchased goods.
- The importance of a mandatory computer security requirement that all suppliers have information and computer security management processes in place.
- Support to extend beyond any normal warranty period to maintain the item. In these cases, the mechanism for the extended period is included within the contractual obligations agreed upon by the vendors, contractors or suppliers. It may be possible for this support to be purchased by third party or after-market suppliers.
- Computer security requirements for audits and assessment of suppliers to be conducted and results provided to the acquirer.
- The importance of establishing a process by where the acquirer and supplier are able to report vulnerabilities to one another and to coordinate response and mitigation efforts.

— For NPPs, information and computer security requirements can be informed by Refs [3, 4, 13] but also could consider safety in IEC 62859 [34]. See Ref. [10] for additional detail on considerations for procurement at NPPs.
— Computer security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships [25]. See clause 6 of Ref. [25] for high level computer security requirements applicable to the management of several supplier relationships and clause 7 of Ref. [25] for computer security requirements applicable to an acquirer and a supplier within a context of a single supplier relationship instance. See chapter 15 of Ref. [4] regarding controls for supplier relationships.
— The computer security requirements for system components to provide capabilities to meet the most demanding security performance as defined in IEC 62443-3-3 [35]. Without inclusion of advanced security features, the appropriate level of protection may be impossible to achieve. The level of security capability of a system or component is determined through application of IEC 62443-4-1 [36].
— The process of system security hardening may eliminate or reduce complexity as it removes or disables unneeded software or services. System security hardening is performed for all systems and the secure configuration is recorded.

6.5.2. Computer security requirements for supplied items associated with moderate impacts

In addition to the general computer security requirements, the list below could provide effective management of risk associated with an item or service that has the potential to result in moderate impacts. These computer security requirements could consider the following:

— The stringency necessary to identify risks, relevant entities and other touchpoints (see Section 4).
— The types of procurement purchase that are allowed. It is expected that catalogue purchases will be limited.
— The need to impose or confirm effectiveness of measures at lower levels within the supply chain (e.g. tiers 2–4 [9]; SCAS (Section 4 and Fig. 7).
— Guidance in determining whether system hardening is to be performed by the vendor, the acquirer or both.
— The necessity of the service or item complying or meeting defensive computer security architecture levels.
— Guidance on mandatory quality assurance processes (e.g. secured development environments, inspections, audits, assessments).
— Guidance on proper configuration management and version control.
— The importance of establishing a process whereby the acquirer and supplier are able to report vulnerabilities to one another and to coordinate response and mitigation efforts.
— Secure means of storage, transport and delivery of products and services.

6.5.3. Computer security requirements for supplied items associated with high impacts

In addition to the general and moderate impacts computer security requirements, the list below could provide effective management of risk associated with an item or service that has the

potential to result in high impacts. These computer security requirements could consider the following:

— The type of procurement purchase that is allowed. It is expected that catalogue purchases will be restricted.
— The number of tiers of suppliers that need to be covered by the procurement contract (see Section 4 and Figs 8 and 11). It is expected that formal and direct contracts (in absence of other types of assurance, standards or certification, or Common Criteria[10] [37]) will be required beyond tier 1 and tier 2.
— The importance of where and when to perform system hardening and by whom.
— The necessity of the service or item to comply with or meet strict defensive computer security architecture levels.
— The importance of establishing a process whereby the supplier provides dedicated support (on-site or remote) during information and/or computer security incidents.
— The mean tolerable outage time for the item or service before the impact is realized (or becomes irreversible).

6.5.4. Computer security requirements for supplied items associated with severe impacts

In addition to the high impacts computer security requirements, the list below could provide effective management of risk associated with an item or service that has the potential to result in severe impacts. These computer security requirements could consider the following:

— All suppliers are identified and controlled via direct and formal contracts.
— All risks are identified (see Section 4) and either modified to acceptable levels or avoided (see Section 2.6).
— The necessity to perform system hardening at all relevant entities, prior to delivery and assurance of hardening by the end customer.
— Stringent computer security requirements may conflict with EULAs or other legal arrangements. For example, a vendor does not permit source code being subjected to a static code analysis where the source code is deemed intellectual property (sensitive to the vendor) and will not be released (or limited to escrow or in trust release upon certain conditions). Therefore, the vendor will need to perform the tests and provide the 'sanitized' results to the customer for acceptance. An alternative would be the use of non-disclosure agreements where results, observation or code review is an absolute necessity.

6.5.5. Quality assurance requirements for computer security

Quality assurance programmes for both the acquirer and the supplier have effective information and computer security processes in place. The purchase computer security requirements

[10] Trusted Computer System Evaluation Criteria (TCSEC) is a United States Department of Defense standard for computer security. It has been replaced by ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation (referred to as Common Criteria) [36].

typically give preference to those suppliers that can demonstrate security aware quality assurance programmes, as well as robust computer security culture.

An analysis of the SCAS could be used to identify key touchpoints that are associated with elevated risk where higher assurance is required.

Quality assurance activities for items typically verify and validate the measures implemented throughout the life cycle and specific touchpoints outlined in the procurement plan. For example, factory acceptance tests and site acceptance tests could be conducted for simple and complex procurements.

Quality assurance for computer security could also consider:

- The timing of the activity;
- Product certification [23, 35, 36] and standards [4, 37], that can be credited in the procurement plan;
- Secure coding and dynamic or static testing;
- Credit for third party assessments.

6.6. PROCUREMENT PLANNING

Section 3.3 of NP-T-3.21 states:

> "Individual projects or major purchases benefit from a formal planning process. (…) individuals [*Acquirers*] requesting items often have unrealistic expectations regarding the ability of the marketplace or the corporate supply chain organization to source an acceptable item within a specific time frame. A procurement planning step allows a market survey to be completed and allows for communication between all involved [*relevant entities*] to ensure expectations regarding timing and other procurement requirements are realistic and that procurement risks are identified and addressed. Such planning also affords the opportunity for the procurement organization to consider consolidation of similar requirements under one contract, or the division of a requirement into several contract packages for economies of scale" [9 – italicized added].

Procurement planning typically addresses the following processes:

(1) Supplier relationship planning process (specify and source stage);
   - Contract options, for example, the type of purchase order(s) appropriate to manage the risk and comply with legal, regulatory and other computer security requirements;
   - Market research, for example, the best practices for computer security[11]. This is a key step in ensuring the acquirer can fulfil the role of an informed customer (see Section 3);
   - Scope of procurement and exclusions, for example, type of procurement, restrictions from computer security level requirements and supplier relationship planning process.

(2) Supplier selection process (specify and source stage);

[11] The Center for Internet Security (CIS) provides a list of 20 individual CIS controls and other resources [38].

— Computer security level requirements for vendors' information security management system;
— Applicable standards and/or certifications.

(3) Supplier relationship agreement process (specify and source stage);
— Interfaces and communication;
— Schedule and planning;
— Roles, responsibilities and resources;
— Identified risks (see Section 4);
— Mitigation or selected risk treatment option.

(4) Supplier relationship management process (specify, source, use and correct stage);
— Request for support;
— Provision of support;
— Oversight, auditing and assessment permissions or privileges (specify and correct stage);
— Penalties for non-compliance.

(5) Supplier relationship termination process;
— Mutual termination (e.g. completion or expiration of contract, change in ownership);
— Unilateral termination due to non-conformance or significant and actionable non-compliance.

Procurement planning allows the acquirer to strategically put in place processes, computer security requirements and detailed procedures to support procurement activities considering the security level of the asset.

Some of these processes are unique for specific procurements (reflecting custom specifications) while others are common and apply to broader computer security requirements (e.g. policy, standard provisions in contracts). It is good practice for the acquirer to review these processes periodically to ensure security is maintained at the appropriate level.

Procurement planning activities typically consider the spare parts list (i.e. inventory and information regarding qualified spares for operational systems). The computer security requirements for qualified spares typically are assigned a similar level to those of the target operational environment (throughout the supply chain). For example, digital assets that can no longer be purchased from the OEM would require that appropriate computer security requirements are imposed upon the commercial grade equipment.

There are numerous variants of procurement methodologies. Annex IV provides an example which specifically addresses computer security in NPPs [8, 39].

6.6.1. Contracts

There are many types of contracts. However, this publication will only address unilateral, implied, and bilateral contracts.

A unilateral contract is a contract where one party makes an offer that requires performance from the other party. Only the party providing the offer is legally bound to provide something. Examples are insurance and shrink wrap EULAs. In both cases, the insured or the user cannot be sued under the terms of the agreement.

An implied contract is a joint agreement that creates obligations and promised intentions among the parties where both are not expressed in writing. For example, contractor staff complying with new information and computer security requirements that are not within their offer letter.

A bilateral contract is where both parties enter into an agreement that binds both parties to implement specific items. This is most likely in simple or complex procurements. A non-disclosure agreement is a bilateral contract.

Direct contracts are contracts where both parties have direct interaction with each other and will mainly be of the implied or bilateral type. Indirect contracts will mainly be of the unilateral type, or instances where no formal relationship exists.

6.6.1.1. General

The nuclear supply chain is a complex global system. It is important for organizations to understand how various contracting parties are affected and treated within and across national legal systems for non-compliance with agreements, non-conformance to good practices and any actual incidents.

A well-managed contracting and insurance approach can help manage, to some extent, supply chain computer security risks.

6.6.1.2. Direct parties

Direct procurement contracts for items and services typically establish the computer security requirements for all tendering companies to meet. These computer security requirements take into account the type of purchase (e.g. item or service) and apply a graded approach (computer security level requirements) accordingly. If required, the contract may have inclusions to allow performance of audits and assessments of the service company or at the service company's locations.

All direct procurement contracts for products could include specifications for secure systems development. Hardware acquisition efforts typically have procedures in place to ensure that equipment received is cyber-secure (or resilient) and not provided in an already compromised state.

Direct procurement contracts may put in place measures to ensure the imposition and maintenance of effective computer and information security arrangements. These arrangements could include:

Integration of all broader computer security requirements;
Inclusion of applicable higher level computer security requirements (i.e. those associated with moderate, high or severe impacts);
Integrate physical, technical and administrative control measures to protect the confidentiality, integrity and availability of sensitive information and sensitive information assets;
Ensure that technology (including equipment and software utilized on nuclear premises) is able to deter, detect and defend against disruptive challenges (such as cyber-attacks);
Contain, defeat or mitigate the effects of, and recover from, malicious acts.

Where possible, direct procurement contracts that are associated with high risk identify the allowed (and denied) information or data flows between the item, service or contracted parties.

6.6.1.3. Indirect contracts (including insurance)

Indirect contracts place greater demand on the acquirer to modify or retain risk (e.g. EULA), or demonstrate good governance (meeting international standards and national regulations) to effectively manage risk that enables risk sharing (e.g. insurance).

In addition, other organizations (indirect parties) that are not contracting parties may be affected by contract terms and performance. This could include the organization's insurers as well as the general public, in the event of an incident. All are bounded by States' international treaties and national legislation.

Assets assigned a stringent security level (e.g. levels 1–3 in Ref. [13]) may have computer security requirements that conflict with EULAs or other legal arrangements. For example, a vendor does not permit source code being subjected to a static code analysis where the source code is deemed intellectual property (sensitive to the vendor) and will not be released (or limited to escrow or in trust release upon certain conditions). Therefore, the vendor performs the tests and provides the sanitized results to the customer for acceptance. An alternative would be the use of non-disclosure agreements (direct contract) where results, observation or code review is an absolute necessity.

Internal guidance on appropriate performance terms typically are included in contracts. These terms carefully consider security risks, including a clear understanding of which potential liabilities and risks that the contracts and insurances do and do not cover. The acquirers typically perform an assessment of their overall governance framework and how it effectively includes computer security related risks.

It is good practice for management to periodically review its organizational risk appetite, assess its ability to insure against incidents, seek to obtain contract protections and demonstrate good governance via appropriate risk assessments and risk management [11].

6.6.2. Cyber insurance for nuclear power plants

Cyber risks could be considered within the nuclear regime's liability and insurance requirements. Although end customers are always strictly liable for their performance, they can pay premiums to other relevant entities who take on some of the financial risks of performance. Although many types of specialty insurance lines are available, the most common types of commercial insurance are property and liability.

The nuclear insurance market is robust and provides alternatives to self-insurance. However, most insurance policies were not initially designed to cover cyber related losses since they did not yet exist. Because these policies were 'silent' on cyber losses, such losses were automatically covered in insurance policies that were not designed to cover these risks. Given the increase in cyber losses, primarily from data breaches and release of personal information, insurers are starting to exclude cyber risks from general and nuclear risk policies (see Annex III). However, the nuclear liability for third party damages from releases of radiation has not been affected by cyber exclusions. The primary goal of civil nuclear liability is to protect the public from nuclear risks and, therefore, it is against public policy to limit coverage for cyber losses.

The Organisation for Economic Co-operation and Development (OECD) lists The Institute Cyber Attack Exclusion Clause, CL380[12], as the most widely used exclusion clause, stating that:

> "in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system" [40].

Acquirers can buy back some of the coverage with some typical clauses on property coverage.

In addition to coverage from nuclear risk insurers, cyber or e-commerce liability insurance can be purchased separately, or endorsed to professional liability or errors and omissions policies that suppliers might carry, with claim limits clearly stated.

Not all suppliers carry cyber coverage. Some suppliers may claim that they are covered by their own errors and omissions policies. However, it is possible that these policies are not comprehensive.

Tailored insurance policies can be crafted to meet an acquirer's needs and reflect its relative risk appetite, but the scope of cyber risks is large and difficult to insure, thus providing limited coverage. In addition to the civil third party liabilities, acquirers face regulatory liability in terms of potential loss of licence and criminal liability including fines and penalties. These cannot be insured. To better defend against potential tort liabilities, acquirers need to not only meet minimum regulatory requirements but also perform to industry norms of good practices in the cyber field.

Acquirers may consult their legal counsel and insurance brokers for specific guidance. Annex III provides an example of insurance for NPPs.

6.7. PROCUREMENT SCENARIOS AND SUPPLIER SELECTION

6.7.1. Supplier selection

Computer security requirements for approved suppliers are typically established and verified before sensitive digital assets or services supporting significant functions are procured. Potential suppliers can be prequalified and listed on an approved supplier list.

Approved supplier list conditions may motivate suppliers to have their services, products and/or processes independently certified to international or national computer security standards. Certified suppliers[13] allow for a greater level of risk transfer (or sharing) to an acquirer than with those suppliers that are not certified.

Where no certified suppliers exist, the acquirer (or a third party) typically performs an assessment of the supplier to determine their capability in managing information and/or computer security risks before a purchase or contract is awarded.

---

[12] Institute clauses are developed by the 'London Market', comprising Lloyd's and the International Underwriting Association.

[13] Certified suppliers have been independently verified to have information and computer security processes in place.

All suppliers on the approved supplier list[14] typically agree to general information and computer security requirements as detailed in the acquirer's terms and conditions and have the capability and resources to comply with these requirements. For example, a formal expectation that suppliers use security benchmarks, where possible, will ensure that good practices with respect to computer security are leveraged. A listing of benchmarks is provided by the National Institute of Standards and Technology (NIST), National Checklist Program Repository [41].

When using approved supplier lists, it is good practice to consider general information and computer security requirements as well as additional requirements imposed for moderate, high or severe impacts.

6.7.2. Scenarios

Both computer security and supply chain risk management have considerable uncertainty. Scenarios reduce uncertainty by developing pragmatic assumptions from previous attacks and using them to help predict more sophisticated attacks.

In this way, scenarios are key for verifying and validating that the information and computer security requirements have been met by the supplier or supplied item.

Scenarios typically include the use of a representative adversary (e.g. design basis threat, national threat statement) or use of publicly disclosed attacks[15]. Alternatively, a supply chain attack catalogue can inform the development of scenarios [28].

Specifications for scenarios are necessary for all supplied items that have the potential to result in moderate to severe harm. These scenarios can be either directly performed on the supplied item or used in design analysis or development of verification and validation testing.

6.8. DEFINING ACCEPTANCE CRITERIA AND METHODS

The acquirer typically establishes processes and detailed procedures to support procurement acceptance activities. These processes and procedures are based on the security level of the item being purchased and are reviewed periodically.

Procurement procedures typically consider the necessity for vendors to support evaluation of the acquired product's computer security. For example, providing configuration options, demonstrating compliance with computer security requirements, allowing the review of development processes, undergoing certification, allowing access to development sites by customer inspectors, providing test results and providing reference site, operations, experience or reputational evaluations.

Computer security requirements are developed in alignment with the risk assessment and the site's security plan [13] as well as appropriate international standards to establish the computer security requirements and responsibilities within the supplier and supplier's supplier.

Computer security requirements for system modifications contain direction for establishing a secure development environment for software and hardware modifications to proceed, so that existing vulnerabilities in the design can be minimized and no new vulnerabilities are

[14] All suppliers where there is a direct bilateral contract, regardless of the security level of the supplied item.
[15] Reference [26] provides an analysis of previously disclosed supply chain attacks.

introduced outside of a controlled environment. These requirements typically are confirmed with an assessment.

During the life cycle of the component, equipment or system, communication pathways typically are evaluated within the system and between the system and all external connections. The connectivity of each pathway is considered for its impact on the overall security, including removable electronic media. If remote reprogramming of electronic devices is possible (or required), compensatory measures typically are put in place to prevent and detect potential exploitation of known device vulnerabilities. Each device within the system or modification scope is periodically evaluated for potential vulnerabilities.

IAEA Nuclear Security Series No. 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities [22], provides an example of acceptance criteria regarding information and control systems at a nuclear facility[16]. Guidance related to supply chain criteria in Ref. [22] includes:

- Interface with facility computer security risk management (paras 3.2—3.29);
- General guidance for computer security (paras 4.12–4.17);
- Aspects of computer security policy related to I&C systems (para. 4.19);
- Secure development environment (paras 4.33–4.40);
- I&C system vendors, contractors and suppliers (paras 4.46–4.53);
- Verification and validation (paras 4.88–4.94);
- Selection of pre-developed items (paras 4.156–4.164);
- I&C system integration (paras 4.175–4.178).

Reference [13] provides guidance in the risk management and stages in the lifetime of a nuclear facility. This will help to inform risk acceptance criteria.

Reference [10] provides guidance around the assignment of roles and responsibilities within a nuclear security regime and the competences and capabilities of organizations. This will help define specifications surrounding the assessment of the capability of organizations to determine whether the counterparty can deliver and comply with the information and computer security requirements.

[16] The technical guidance in Ref. [14] can be applied to both physical protection systems [18, 19] and other systems [21] using the graded approach.

7. SOURCE STAGE

The source stage generally begins following identification of approved suppliers and establishment of the acceptance criteria. This requires that supplier's information and computer security programmes are known, evaluated and have been determined to be effective to supply items or provide services up to the required security level.

Determining the effectiveness of vendor programmes is outlined in Ref. [13]:

- Computer security requirements for information security management system and/or computer security programme (paras 4.54–4.60);
- Computer security requirements for acquirer computer security programme to mandate supply chain protections (para. 6.22);
- Computer security equirements regarding when to use risk transfer to have suppliers carry the risk or implement measures (para. 6.37);
- Contractual computer security requirements (para. 7.20 (c));
- Computer security requirements for vendor–supplier interface (para. 7.28);
- Defensive computer security architecture requirements for remote vendor access (paras 8.10–8.11);
- Authority of engineering staff (paras A.22–A.26); specification (paras A.31, A.34–A.35, A.39); quality assurance (paras A.32, A.36–A.37, A.40); contract execution (para. A.33); touchpoints (paras A.36, A.38); use (paras A.69–A.70).

The source stage consists of the following stages:

- Bidding, evaluation and placement of purchase orders;
- Contract execution, component fabrication, testing, and source surveillance;
- Packing and transport (touchpoints);
- Expediting;
- Acceptance and receipt;
- Storage and warehousing.

The source stage depends upon:

- Specifications (including identification of the associated security level);
- Needs identification (number of tiers (see Fig. 1) for which the supplier or end customer will evaluate information and computer security);
- Terms and conditions (both generic and specific);
- Identified risks (using SCAS (see Section 4), and where known);
- Acceptance criteria (computer security requirements and the level of acceptable risk validation);
- Schedule and milestones;
- Cyber security testing and evaluation (computer security requirements validation);
- Risk treatment, specifically where risk has been transferred to the vendor by requiring vendor implementation of information and computer security measures, for protections with touchpoints including any exchange (e.g. information, data, product, service) between direct or indirect third parties (stakeholders).

7.1. BIDDING, EVALUATION AND PLACEMENT OF PURCHASE ORDERS

It is good practice for the information and computer security requirements, measures and arrangements to be known and accepted by both parties during bidding, evaluation and placement of purchase orders. Furthermore, the supplier typically assures the acquirer that the risk can be managed to an acceptable level.

A formal bid and evaluation process may be necessary when one or more of the following conditions exist:

- Any complex purchase;
- Simple procurements associated with identified risk in information and computer security (see Section 4);
- Any procurement requiring compliance with defensive computer security architecture requirements (e.g. services that demand remote access to sensitive digital assets);
- Any procurement demanding greater assurance of lower tiers (i.e. supplier's suppliers (see Fig. 10)).

Catalogue purchases that are spares replenishment or associated with sufficiently low risk generally will not need a bid invitation.

A list of sample procurement method computer security requirements for an operating organization (e.g. of an NPP) can be found in table 8 of Ref. [9].

Information and computer security requirements could be included in a bid invitation specification or other enquiry document. The number and scope of these computer security requirements will depend on type of contract; size and scope of project; type of service or item purchased; complexity (see Annex VIII); type of contractor and resources available. Some of these computer security requirements may be sensitive and could require secure protocols to be defined and established before sharing them with prospective suppliers.

Information needed from potential bidders could include the following:

- Certified (or verified) to international information and computer security standards or publications (e.g. information security management system [14], computer security programmes [3], Ref. [10]) or equivalent;
- Other certifications or processes supportive of security (e.g. IT service management; information technology infrastructure library, capability maturity model integration for service, control objectives for information and related technologies);
- Secure development practices and environment (if product);
- Public key infrastructure information (e.g. digital signatures, X.509 certificates);
- Cyber security training and awareness programme;
- Cyber security testing and evaluation;
- Corrective action programme;
- Information protection requirements (classified or security sensitive information);
- Performance history on security and information protections (confidentiality and integrity);
- Personnel security programme.

An important aspect of service bids is visits to purchaser sites by prospective suppliers. Prior to site visits, it is necessary to execute a non-disclosure agreement with these suppliers prior to sharing confidential or security sensitive information.

Exceptions to any information and computer security requirements requested by the supplier are typically reviewed and approved by the end customer's computer security point of contact. It is good practice for exceptions regarding defensive computer security architecture requirements or information protection to be stringently guarded against or justified to the satisfaction of the purchaser.

A framework agreement (master contract) typically includes most of the terms contained in future procurements or contracts. These agreements could include trustworthiness checks and performance evaluations needed to determine whether computer security requirements are listed within the master contracts, or in individual contracts for specific purchases. In conducting this evaluation, it is important to consider that computer security requirements can change with increasing adversary capabilities. This may necessitate the need to update master and/or individual contracts to include the most up to date computer security requirements. Where security clauses are in the master contracts, timely updates on imposed computer security requirements could be included in an annex.

7.1.1. Bid evaluation and selection of supplier

Bid evaluation is a key stage in the procurement process which ensures that:

- The purchasing decision is objective (i.e. information and computer security requirements are appropriately weighted with other considerations);
- The decision-making process is fair, transparent and auditable (e.g. both internal and external audits, information sensitivity is typically considered but cannot exempt bids from external assessment and review);
- Bids involving functions important to safety, emergency preparedness, NMAC or other domains involve subject matter experts from those domains as well as security. This will ensure that conflicts between security and other domain specifications are identified and resolved in an effective manner (i.e. security remains integrated into product design);
- The purchaser can demonstrate best value in the tender process (e.g. risks identified as part of SCAS analysis are effectively managed and/or treated).

For formal bids that are associated with significant risks, it is good practice to have personnel with information and computer security expertise for the bid evaluation. These bids are likely to necessitate broad and abstract specifications that require a high degree of information and computer security competencies.

For formal bids associated with items important to safety, it is good practice to have a multi-disciplinary team evaluate supplier bids. This team typically resolves or prioritizes actions taken for security or safety (depending on organizational policy), and ability to provide for compensating measures, if necessary.

For catalogue purchases or those bids associated with low risks, procurement staff might be sufficiently competent to evaluate bids where acceptance criteria are detailed or otherwise a template or checklist is provided. The end customer could consider template bid evaluation checklists that allow for procurement staff to appropriately assess the measures necessary to manage the risks identified by evaluation of their SCAS.

Suppliers typically provide proof of certification of their information and computer security programme to a widely accepted international standard (e.g. ISO/IEC 27001 [14], COBIT) or evidence of compliance to international (IEC 62645 [4]) and national standards (NEI 08-09 (Rev. 6) [3], CSA N290.7 [6]). Suppliers providing evidence of information and computer security performance, especially via audits by trusted third parties[17], typically receive greater credit as part of the scoring process. The sharing of this information may be sensitive and is typically protected by the purchaser.

Suppliers typically provide evidence of trustworthiness evaluations of key staff members having key leadership, management or security sensitive responsibilities. For example, any potential security issues or concerns of a personal nature, conflict of interest between the parties or related suppliers and past criminal convictions. The specific steps involved will vary by jurisdiction, but will often include a process for criminal background checks and declarations of any potential conflicts of interest by individuals prior to their involvement in the bidding process.

Bid evaluation could weigh the relative importance of information security, computer security and functional (technical) computer security requirements; initial cost and schedule specifications; and operating costs.

Information and computer security requirements may have a significant impact on cost and schedule. These requirements, if specified correctly, can greatly lower future operating costs or minimize the likelihood of successful cyber-attack on sensitive digital assets. The critical consideration is to ensure that risks identified through use of SCAS analysis have been addressed and provide the assurance necessary for acceptance of residual and acceptable risk.

It is good practice for the acquirer to determine the supplier's capability to manage cyber risk and proceed with technical and economic evaluations only for those bids where the supplier has been deemed capable.

7.1.2. Pre-contract assessment – assessment of the supplier's capability or capacity

Integrators are often a convergence point of a deep and complex supply network. For example, a nuclear computer security integrator will often provide integrated solutions that will need to meet specifications for both physical security and computer security. The integrator will also ensure that nuclear applications work with computer security tools and frameworks to ensure the products and services provided do not degrade the NPP's computer security defensive posture and performance of the safety function.

The acquirer typically considers the supplier's capability including security culture, risk management and governance arrangements. This could include answering questions such as:

- Do senior management set clear directions and expectation with regard to the importance of security throughout the organization, and seek assurance regarding compliance?
- Does the organization have well defined and embedded security risk management processes?
- How does the organization ensure that an effective security culture exists to support the achievement of organization objectives?

[17] For example, third parties that certify ISO/IEC 27001:2013 [14] need themselves to be certified as meeting the computer security requirements for certification bodies as specified in ISO/IEC 27006:2015 [42].

Suppliers that can demonstrate mature security risk management arrangements will provide the acquirer with more confidence that appropriate security measures will be embedded into the product or service provided and may allow for a less prescriptive and more outcome focused approach to be applied.

Acquirers often need to take multiple factors into consideration when making purchases, including supplier specifications, approved supplier list, facility and personnel, receiving, asset isolation, configuration and hardening benchmarks, testing standards, integration of components and systems, and emerging threats.

To ensure supplier pathways do not increase the overall supply chain risk, the following items could be addressed:

- Buying from market platforms without provenance can introduce additional risk, which may need to be addressed in cyber factory acceptance testing.
- During an acquisition when only a single source supplier is available, the acquirer may have no other options than a single choice that is available. In this case, the acquirer maximizes due diligence on cyber acceptance testing before installation. By establishing a good communication channel with the supplier, the acquirer can also exchange information with the supplier regarding any malfunctions, vulnerabilities or malware found during various testing phases so that the supplier can perform corrective actions. In other cases, where the acquirer is purchasing a turnkey system, auditable process artefacts are adequately documented, full scope cyber testing on all assets with test cases traced to performance based specifications are derived, and penetration testing and vulnerability scanning are performed when possible.
- Product certifications, such as IEC 62443-3-3 [35], IEC 62443-4-2 [43], or UL 2900-1 [44], are highly desirable.
- National regulatory requirements from critical infrastructure protection could be considered. It is important that all suppliers demonstrate or ensure that all national regulatory requirements will be met.

7.1.3. Technical bid evaluation

It is good practice to identify computer security supply chain risks (e.g. an analysis of a SCAS) to determine the severity of associated consequences. Once consequences are determined, computer security requirements can be specified (see examples in Section 5). These requirements, along with acceptance criteria (see Section 5), form the basis of the technical bid evaluation.

Other factors with respect to information and computer security that could be considered include:

- The capability of the supplier to deliver in accordance with information and computer security requirements;
- The technical and quality features including commercial grade dedication processes, training and qualifications;
- Warranties (including support lifetimes): mechanism to communicate or provide security updates, workarounds and mitigations;
- EULA software (e.g. determining whether the EULA restricts use of software for nuclear security uses);

— The sourcing (or outsourcing) of key design elements (COTS or pre-developed items). National regulation may demand certain sourcing considerations.

The technical evaluation prioritizes the selection (i.e. higher weighting) of products or services with security features that have been evaluated thoroughly. The weighting considers that these products or services have the potential to incur greater cost and demand higher personnel competence to evaluate the effectiveness of the security feature and resolve conflicts.

7.2. ECONOMIC BID EVALUATION

The technical bid evaluation results are typically combined with an economic evaluation. The following areas are important economic factors for information and computer security:

— Contractual terms and conditions – generic conditions are likely to not increase overall costs. However, for high risk procurements, the terms and conditions to cover information and computer security considerations appropriately will be significant. Furthermore, it is important that the supplier understands the implications and costs associated with meeting these contractual requirements (i.e. informed supplier). However, the end customer is obligated to validate that the vendor is capable and understands the contractual requirements.
— Intellectual property – closed source pre-developed software does not readily provide for certain types of static and dynamic code analysis (especially those using automated tools). For high risk procurements, it is possible that closed source (proprietary) software will not be able to meet specified computer security requirements. If no other economic alternative is possible, compensatory measures may be necessary.
— Ongoing maintenance costs – system patching and/or training of staff to securely configure and maintain necessary technical security measures.

Organizations that prioritize lowest cost bids over security are likely to have a strategic vulnerability to supply chain attacks. For example, lowest cost bidders are likely to have fewer security features and capabilities, placing a greater demand on the acquirer to provide security which could result in greater costs for the acquirer throughout the use stage (see Section 8).

7.2.1. Completing the bid evaluation

Procurement of services and items that are part of a formal bidding process typically weights information and computer security requirements to ensure that they have the appropriate priority. For example, the weighting of information and computer security requirements for security projects will be more significant than those for catalogue purchases on systems that are not sensitive digital assets.

Technical and quality features depend upon a supplier's development processes. For example, a vendor that relies on public vulnerability disclosures (per a fee basis) to support their bug fixes with a patch management approach to software security requires the end customer to patch their systems to maintain security. It is possible this will not be an issue for software that supports or operates within dynamic environments such as corporate computer networks. However, for more static environments such as nuclear reactor control systems, stringent configuration management policies will severely restrict the ability to install patches.

Conversely, specification of a high level of assurance for security (e.g. Common Criteria [37]) will both reduce the functionality of the system and increase the expense to develop and validate this system. This approach would be effective for nuclear reactor control systems but not suitable for corporate computer networks, mostly owing to lack of versatility and excessive security controls and well as user acceptance or expectations.

Nevertheless, all systems will contain vulnerabilities and could require ongoing maintenance either through patching, workarounds or mitigation. It is important for bid evaluations to prioritize vendors that review their systems for security; identify potential weakness, exposures or vulnerabilities; and provide guidance on how to secure their systems.

The bid evaluation considers the exemptions needed by the vendor to comply with the contractual requirements. A key consideration is whether the identified risk requires transfer to the vendor to effectively manage the risk (e.g. computer security testing at a supplier's supplier) or whether the risk can be mitigated by the acquirer (e.g. additional tests during factory acceptance testing or site acceptance testing).

To secure sensitive information from being disclosed during the bidding process, appropriate measures (e.g. advanced encryption standards such as AES 128, 196 and 256; applications such as secure email and secure server) could be used to minimize unauthorized disclosure. The acquirer typically communicates their expected information handling and storage specifications for any sensitive information disclosed during the bid process [21].

To mitigate sensitive information disclosure, formalization of computer security requirements is typically included as part of the contractual negotiation with suppliers. IEC 63096 [5] includes a recommended approach for a nuclear application, including graded computer security requirements. Common Criteria [37] is another possible tool that can be used to formalize such computer security requirements. Another example of a procurement requirement is the US Department of Homeland Security (DHS) Cyber Security Procurement Language for Control Systems [45], which contains guidance and recommendations for defining computer security requirements and specific procurement language for control system acquisitions.

Reference [9] (table 11, sections 3.6.3 and 3.6.4) contains general considerations for negotiation with suppliers, and preparation and placement of purchase orders.

7.3. CONTRACT EXECUTION, COMPONENT FABRICATION AND SOURCE SURVEILLANCE

Identified computer security supply chain risks (e.g. SCAS), the computer security requirements, and the prioritized risk treatment options (specify stage) typically inform the next steps of the procurement process.

For large projects, a 'kick-off' meeting could be used to determine the roles and responsibilities for computer and information security, including which organization's process and computer security requirements will apply to specific stages of the contract. For example, information and computer security requirements are usually assigned by the information owner. In the case where the acquirer is the information owner, equivalent protections are typically provided to the suppliers and any of the supplier's suppliers that need access to the information ('need to know'). This protection is typically assessed, or evidence (e.g. independent certification) provided to the acquirer to determine if the protection meets the acquirer's security standards.

In the case of identified risks that have been determined as requiring transfer to the supplier (e.g. static and dynamic code analysis for closed source software), the acquirer could require

evidence that the supplier is capable of managing transferred risks (i.e. mature processes are in place for computer risk management).

7.3.1. Monitoring contractor performance

During the course of the contract, assurance that security controls are maintained throughout the supplier life cycle of designing, producing, holding and maintaining the asset is typically provided. Assurance could be obtained through regular meetings, completion of self-assessment questionnaires, production of annual reports, or through site visits or assessments. Site visits could be announced or unannounced.

The contract could take into account the nature of the assurance activities, the periodicity with which they will be performed and level of assurance necessary to have confidence that the suppliers are managing identified risks appropriately. This may require onsite access to suppliers' premises to ensure that they have appropriate security controls to adequately secure the asset and any associated sensitive information.

Consideration could also be given to suppliers' self-assessments to determine whether independent assurance is required or accepted.

The necessary assurance is typically commensurate to the computer security requirements assigned to the product or service.

7.3.1.1. Computer security assessment

In addition to the quality of a product and service provided, the supplier's computer security posture may introduce cyber risk to the acquirer. It is important to assess the security posture of the supplier by evaluating their security programmes. The acquirer can request the security framework (security controls, processes, and procedures) of product or service from the supplier to determine if the potential to compromise the acquirer's product or service, and inherent system(s) exists. If the assessment indicates a poor security posture, the acquirer's computer security programme could enact controls on services or access to limit new attack vectors before forming the new supplier relationship.

7.3.1.2. Supplier computer security programme

A supplier's computer security programme is fundamental to effective inclusion of information and computer security into their products or services. The supplier programme could include policies, computer security requirements, processes, evaluations, measurements, monitoring and a corrective action process.

The programme could implement a continual improvement process and provide evidence of both its effectiveness and deficiencies (with corresponding corrective actions).

Supplier security aspects to consider for ongoing monitoring and assessment could include:

- Security governance or computer security programme;
- Manufacturing and operational security;
- Software engineering and architecture;
- Asset management and secure storage of source code repository;
- Incident management;
- Transportation security (incoming and outgoing delivery integrity checks);
- Physical and environmental security;

— Personnel security;
— Information protection;
— Sub-tier partner security (lower tiers, service providers, cloud).

7.3.1.3. Developer security testing

The acquirer could require system developers and integrators of acquired digital asset(s) to create, implement and document a security test and evaluation plan to ensure that the acquired products meet all specified computer security requirements and are free from known, testable vulnerabilities and malicious code. The test and evaluation plan typically identify the following vulnerabilities and other vulnerabilities that may arise from the use of new technology:

— Weak, unproven or nonstandard cryptographic modules;
— Insecure network protocols for sensitive communications;
— Known insecure software components or libraries;
— Known vulnerabilities;
— Insecure configuration files or options that act to control features of the application;
— Inadequate or inappropriate use of access control mechanisms to control access to system resources;
— Inappropriate privileges being granted to users, processes or applications;
— Weak authentication mechanisms;
— Improperly or failing to validate input and output data;
— Insecure or inadequate logging of system errors or security related information;
— Inadequately bounded buffers;
— Format string vulnerabilities;
— Privilege escalation vulnerabilities;
— Unsafe database transactions;
— Unsafe use of native function calls;
— Hidden functions and vulnerable features embedded in the code;
— Use of unsupported or undocumented methods or functions;
— Use of undocumented code or malicious functions that might allow either unauthorized access or use of the system or the system to behave beyond the intended function.

7.3.1.4. Secure development environment

Use of separate and secure development environments by suppliers is typically preferred for product development activities to reduce the risk of malware infection of the digital asset(s).

For secure development environments, the following could apply:

— Internal and external development environments are assessed to determine their security needs. There is a potential that required information flows may differ or even be the reverse of the flows needed during operation. For example, safety systems in operation may rely solely on outward communication flows (i.e. from highest (most stringent) level to lowest) to protect integrity, whereas a development environment may require inward communication flows to protect confidentiality of intellectual property.
— The integrity of the developed software, hardware and firmware are protected by computer security measures (including the configuration management process).

— Distinct environments have isolated or separate networks (e.g. logical) and/or physical locations.
— Anti-malware tools are employed that detect unauthorized software while not restricting necessary development activities.
— Security tools are utilized, such as those that perform static and dynamic software analysis to proactively identify vulnerabilities.
— Access to development environment (or components) is restricted or constrained to authorized and trained personnel. Personnel are competent in the use of secure coding techniques for software development.
— For I&C systems, secure development environments are used with access controls and testing procedures to verify that I&C equipment does not introduce malicious code or activities [22].

7.3.1.5. Additional considerations

Information disclosures are typically evaluated to ensure compliance and reduce the likelihood for information theft or leak.

Training programmes for both suppliers and acquirers could include information on how to establish a secure development environment, including details on how to harden the environment and maintain configuration.

Evaluations of coordination and performance during computer security incidents are typically conducted. This may require joint exercises with the vendor to increase efficiency and raise the capability of responding to events at both the acquirer and vendor.

7.4. TRANSITIONAL TOUCHPOINTS

A SCAS can be used to identify key physical or electronic transitional touchpoints (see Section 4). For identified risks, measures are typically put in place at both ends of the transition.

Transitional touchpoints use the ICT channel to transmit and receive electronic or digital information and uses applications and services such as email, transport layer security, secure shell protocol, virtual private network or file transfer protocol. The ICT channel can be used for remote services, administration or monitoring. The logistics channel is the physical transfer of equipment.

The ICT channel requires protection of integrity and confidentiality that is typically provided by cryptographic mechanisms (e.g. encryption, X.509 certificates, document security systems, media access control, secure hash algorithm (SHA)). The ICT channel also provides a means for entity authentication to ensure that identities of the communicating entities are verified.

Publicly disclosed attacks on the supply chain [26] have targeted the ICT channel. The most common attack on this channel is the abuse of trust based on the theft of a private key with which to sign software. If an adversary can steal the vendor's private key, they can inject malicious software by masquerading as the trusted vendor. It is good practice to include, as a prime requirement, in the acquirer and supplier contract the proper disclosure to ensure that vendors communicate revocation of certificates, incidents that impact trust based mechanism and authorized or signed software that has been validated is reportable.

The logistics channel is vulnerable to attacks such as interdiction and physical tampering. The use of integrity or provenance-tracking tools, such as tamper indicating devices and seals, could be required to ensure that these attacks are detected, even if not prevented.

Additionally, current good practice requires that software and electronic or digital source material is sent via a separate channel (such as the ICT channel) from the equipment (logistics channel). This will ensure that, during the site acceptance test, the object code and the system configuration are installed from known good sources and cannot be affected by tampering or interdiction of the equipment attacked within the logistics channel. This measure also prepares the acquirer for system recovery activities, if necessary, as the software required and instructions for installation would already be available and practiced.

7.5. ACCEPTANCE AND RECEIPT

7.5.1. Accreditation

Computer security certification and accreditation programmes of devices and systems generally involve three steps: (i) an audit of the development process; (ii) computer security stress testing to find vulnerabilities; and (iii) the analysis and testing of security features and capabilities of the product to determine the security level achieved.

Development process audits review the development life cycle from the specification through the design, coding and different phases of testing, as well as support and maintenance activities. An assessment is conducted to determine to what extent security measures are employed in each life cycle phase.

Computer security stress tests include penetration testing, fuzz testing, malformed packet testing and storm testing. The analysis and testing of a product's security features are a review and validation of the security controls available and a determination of the security level achieved. Some States may operate accreditation schemes for certain products, services or organizations. Accredited authorities provide the assurance that a security level of achievement has been obtained based on computer security requirements and standards. The procurement contract specification could detail if such accreditation is a necessary security requirement for the project. However, even if accreditation is not listed as a requirement, it may still be offered by the supplier.

The acquirer typically ensures that the features to which a certification attests meets the security profile desired. It is possible that compliance to a particular security standard does not equate to adequate security for a particular application.

7.5.2. Risk assessment of products

The risk assessment could be revisited at the design stage if the asset to be delivered is a system or system component. The risk assessment will likely be done by the supplier at this stage to help them determine which detailed controls could be built into the product in order to mitigate risk to an acceptable level. Those risk assessments may require regular review as the design for the product matures and could be assessed by the acquirer to ensure that the design and security controls meet their expectations. The purchasing organization may need to bring in expertise to support those reviews, dependent upon their own informed customer capability.

As the product moves into the development stage, where applicable, the purchasing organization could seek assurance that the code used is secure. This is a specialized area and assessment is typically undertaken by specialists independent from the design and build team. The specialists may be suitably qualified personnel within the supplier's organization or independent experts contracted to carry out the work.

Vulnerability management could be incorporated into the development process so that vulnerabilities can be identified and addressed early in the project. Specific software can be used to aid this process.

The contract typically clarifies what support will be provided by the supplier when new vulnerabilities are identified during the lifetime of the asset. This may include frequency of product updates, incident response support and commitment to address new vulnerabilities within agreed and documented timescales.

Consideration is typically given to threat intelligence sources that may help to identify new vulnerabilities as they are discovered or exploited and the responsibility for identifying, analysing and acting upon such intelligence.

Computer security testing and evaluation is a necessary and key component of the factory acceptance test and site acceptance test. Additionally, it is appropriate for acquirers to consider the potential costs to purchase, develop or contract services that have the necessary tools, assets, capability and individual competence to perform the security tests to the required level.

Penetration testing is best conducted during the factory acceptance test since any major vulnerabilities that are identified could require re-design of one or more major elements. For high or severe risk procurements, penetration testing is a fundamental task that is typically conducted.

Owing to the high degree of interdependency with safety and security, a similar level of effort to ensure both safety and security is needed. The evaluation of products may consider IEC 63096 [5] or Common Criteria [37]. Reference [5] is specifically targeted for the nuclear domain and recommended “security controls and baseline requirement” for security degrees S1 (highest), S2, S3 and baseline requirements. Reference [5] also provides guidance on the controls that could be applied during the development phase of products and platforms for the nuclear domain, which can be forwarded to suppliers and sub-suppliers. Beyond meeting the security guidance for product and platform development, it is appropriate to request that suppliers implement the security features that are needed later on during the engineering and integration phase and during the plant operation and maintenance phase. Reference [37] makes use of a protection profile (“packages of security requirements”); “specifications of security target”; “names set of security functional or security assurance requirements” (measures taken during development and evaluation); and evaluation assurance levels (EALs, a numerical rating corresponding to depth and rigour of the evaluation). The increasing grade of levels reflects the increasing rigour of assurance requirements and evaluations for computer security.

The individual EALs, from lowest to highest level of assured security, are as follows [37]:

- EAL1: functionally tested;
- EAL2: structurally tested;
- EAL3: methodically tested and checked;
- EAL4: methodically designed, tested and reviewed;
- EAL5: semi-formally designed and tested;
- EAL6: semi-formally verified design and tested;
- EAL7: formally verified design and tested.

Many COTS and pre-developed items do not meet security specifications above EAL4. Formalized specification of security models and design is a highly specific and time consuming task. Therefore, EAL5 to EAL7 require high-end expertise, and EAL7 requires full source code analysis and as such are typically constrained to military use.

In instances where product certifications are not available, the following security design principles could be encouraged [46]:

- Principle of Economy of Mechanism: the protection mechanism has a simple and small design.
- Principle of Fail-safe Defaults: the protection mechanism denies access by default, and grants access only when explicit permission exists.
- Principle of Complete Mediation: the protection mechanism checks every access to every object.
- Principle of Open Design: the protection mechanism does not depend on attackers being ignorant of its design to succeed. However, it may be based on the attacker's ignorance of specific information such as passwords or cipher keys.
- Principle of Separation of Privilege: the protection mechanism grants access based on more than one piece of information.
- Principle of Least Privilege: the protection mechanism forces every process to operate with the minimum privileges needed to perform its task.
- Principle of Least Common Mechanism: the protection mechanism is shared as little as possible among users.
- Principle of Psychological Acceptability: the protection mechanism is easy to use (at least as easy as not using it).

7.6. STORAGE AND WAREHOUSING

Storage and warehousing are important for information and computer security since the equipment, backup files, physical media, portable devices and maintenance equipment are susceptible to tampering or compromise by insiders with authorized access.

Secure storage areas are established with specific specifications for acquisitions based upon their assigned security level.

Tamper indicating devices, access control to storage and warehouse areas (including the development environment) and trustworthiness evaluations are key measures to minimize the threat posed by the insider.

It may be beneficial to securely store data, software, source files and backups in locations separate from the hardware. For software, data, source files and backups, measures could be implemented to protect integrity and, if applicable, confidentiality of this information.

Secure storage of cryptographic keys is critical to ensure both the integrity and confidentiality of supplied items. This may involve establishing a public key infrastructure to bind public keys with respective identities of relevant entities. X.509 certificates along with authenticated encryption and associated data algorithms or modes fulfil a very important role in ensuring that ICT communication channels are secure.

8. USE STAGE

The use stage generally begins once approved suppliers have completed testing and integration of the product or system. The use stage begins with a factory acceptance test and ends at decommissioning[18]. For product suppliers, the use stage includes the repair and return phase. An important milestone of this stage involves the transfer of risk from the supplier to the acquirer when the acquirer takes ownership of the product.

The risks identified using the SCAS could consider product installation, testing, repair and use, as well as the services required to test, calibrate, monitor and update products.

The phases of the SCAS discussed in this section are:

- Factory acceptance test and site acceptance test;
- Installation (and commissioning);
- Operation;
- Maintenance and upgrades;
- Repair and return;
- Decommissioning;
- End-of-life and end-of-support.

During the use phase and as illustrated in Fig. 7, there are multiple attack paths across the entire supply chain life cycle, which are providing opportunities for targeted supply chain attacks. For example, "[i]n 2014, approximately 23 percent of all cyber breaches were attributed to current service providers or contractors and 45 percent were attributed to previous suppliers" [47].

The use stage may provide the first indication of a conflict between security and safety specifications (see Sections 6 and 7.1.1) or their implementation. While the potential for conflicts are typically considered and addressed within the specify stage, the use stage (e.g. integration and testing phases at the end customer's location) may provide the first indication of conflicts that are the result of unanalysed conditions, implementation elements or dependencies. These conflicts are typically addressed in the 'correct' stage. Paragraph 3.49 of NSS 33-T states: "If there is a conflict between safety and security, then (…) [c]ompensatory computer security measures (…) should not rely solely upon administrative control measures for an extended period" [22].

To overcome these conflicts or difficulties, use formal security models to inform testing. This can include, but is not limited to:

- Common Criteria specifications such as protection profile, security target and security functional specifications [37];
- Applying security models to guide validation and verification processes that integrate security both at the supplier's site and at the acquirer [48];
- Outsourcing testing to certified testing laboratories to verify the computer security requirements have been met [49];
- The capability to provide security via implementation of defensive computer security architecture requirements;
- Effectiveness of existing processes with the end customer to provide security protections to products that are vulnerable.

[18] The upgrade, maintenance and decommissioning phases may include part of the correct stage. This assignment depends upon the impact on the supply chain relationship (see Section 9).

The United States National Nuclear Security Administration, Office of Radiological Security [50], outlines the capabilities that could be considered for products in use:

- Access control;
- Account management;
- Session management;
- Authentication–password policy and management;
- Logging and auditing;
- Communication restrictions;
- Malware detection and protection;
- State of health signals (monitoring);
- Intrusion detection (host based and network based);
- Secured wireless technology security;
- Cryptography for encryption of data, data integrity protections, data origin or entity authentication.

The supplier typically provides documentation on these capabilities, including instructions on how to securely configure and use them.

Additionally, these capabilities require the end customer to have processes in place to securely configure these devices and the boundary protections, including intrusion detection [51].

It is widely accepted that products with security features that have been evaluated or accredited provide assurances of computer security protections. These products have the potential to incur greater cost and need for personnel with higher competence in order to provide confidence that they do not introduce additional security concerns due to improper use or configuration. Furthermore, the greater the degree of evaluation by certified testing organizations or by end customer organizations with proven performance in testing, evaluation and use of these features, the greater the degree of confidence that these capabilities are effectively designed and used.

Products without integrated security capabilities typically need compensating computer security controls (e.g. firewall, physical separation and isolation, anti-malware kiosk). Compensating controls that are implemented at the perimeter provide a single layer of defence. The defensive computer security architecture typically considers the lack of integrated security capabilities within its defence in depth strategy. For example, legacy versions of operating systems were susceptible to buffer overflows (e.g. Conficker worm) which are a particular type of attack that has the potential to allow remote code execution [52]. However, newer versions have implemented security features (e.g. address space layout randomization, data execution prevention, canaries) along with secure coding practices (bounds checking) that have reduced the potential for these types of attacks occurring or remaining undetected.

Another important element as it applies to services (particularly cloud) is the use of single sign-on. Single sign-on authenticates a user using a single identification and password for a set of (or possibly all) services within an organization. Single sign-on has the potential to increase security since passwords do not need to be shared or stored between organizations or departments that use single sign-on.

A secure defensive computer security architecture that supports real time monitoring, detection, protection and recovery will provide computer security protections, but the fear of increasing the attack surface with connected security controls may result in the reliance on physical air-gaps supported by administrative procedures. Reference [51] states: “Physical separation alone

no longer provides a viable business option for managing, utilizing, or securing [industrial control systems]". An additional challenge with air-gapped systems reliant on administrative controls (i.e. processes and procedures) is that non-compliance or adverse conditions that result are likely to require self-reporting, which relies significantly on nuclear and computer security culture.

It is appropriate for the end customer to assess computer security with a continual process improvement approach; otherwise, there is no guarantee that personnel are adhering to policies and procedures. The end customer typically provides the necessary resources (e.g. funding, training, personnel, assets) to develop and sustain this performance (capability).

Holistically, there are four considerations that are typically needed to increase organizational computer security for the end customer: (i) secure integration and configuration of verified security features and capabilities; (ii) continually improved organizational security processes; (iii) establishment of, compliance to and reinforcement of the defensive computer security architecture; and (iv) continual real time monitoring of critical systems.

8.1. TESTING, INSTALLATION AND USE

8.1.1. Overall test planning and preparation

The factory acceptance test, site acceptance test, installation and commissioning testing typically consider when computer security requirements can be evaluated, which tools and configuration will allow for effective evaluation of these computer security requirements and the personnel expertise needed to conduct these tests.

8.1.2. General prerequisites for testing

An analysis of the SCAS can be used to identify risks that are associated with installation, testing and use. These risks could inform procurement planning (see Section 6) as well as inform which tasks and activities could be used to verify and validate security of the procured item.

Computer security testing may require specialized (and qualified) computer security platforms and tools. There are free and publicly available (e.g. open-source, community versions) virtual machine software (e.g. Hyper-V, VirtualBox, VMWare player), network protocol analysers or sniffers (e.g. Wireshark), network scanners–mappers (e.g. NMAP), vulnerability analysers (e.g. OpenVAS), fuzz testers (e.g. Scapy) or penetration testing platforms (e.g. Metasploit Framework). Other commercial and propriety versions of tools (e.g. VMWare Workstation Pro, Nexpose, Metasploit Pro, Defensics) require licences and may require specific hardware to perform.

Other than cost, the difference between open-source and commercial (paid) versions is the level of functionality that is provided. For example, the paid version of penetration testing platform integrates many functions (network discovery, exploitation, automation, remote API) that are not available in the free version. Additionally, the interface is simplified (web versus command-line) to reduce the challenge of not having specialized internal resources (e.g. highly competent penetration testers) available to perform the testing.

From a supply chain perspective, the costs of specialized training and licensing of computer security tools are typically compared to the costs of hiring a penetration testing consultant company to perform the tests. In this comparison, it is important that the organization be an informed customer to define the key success criteria.

The end customer typically identifies whether an EULA or custom contract with their supplier limits the type of testing that can be performed. Performance of testing not allowed by an EULA or contract may void the product warranty.

The end customer could assess the competency of personnel and the performance of their testing procedures in determining whether to directly perform the testing or out-source testing to a certified testing organization [45] that performs inspections according to ISO/IEC 17020:2012 [53].

It is good practice to consider the potentially significant costs necessary to perform the security testing, especially for complex procurements. These costs could include:

- Training of personnel to be highly competent;
- Costs for purchasing specialized security test equipment, software and ongoing licencing costs;
- Establishment, assessment and improving organizational processes required for effective verification and validation of security;
- The need for compensatory measures in cases where necessary security features are not provided to meet security level requirements;
- Ongoing and additional effort to monitor security performance.

Costs may be reduced through procurement of services to perform one or more of the activities listed above. For outsourcing security activities associated with high risk, section 6.4 of Ref. [12] provides information on technical processes that could be in place to "define requirements, transform the requirements into products and services, and address use and sustainment of products and services until disposal" [12].

Additionally, for cloud based ICT services (e.g. data centres, application, platform, infrastructure), section 6.4 of ISO/IEC 27036-4:2016 [54] provides information on these technical processes.

Although no empirical evidence is available at the time of this publication, the expectation is that the use of IEC 62443-2-4:2015+AMD1:2017 CSV [55] may significantly reduce the cost of factory acceptance testing and site acceptance testing of security capabilities provided in the vendor's system. With no vendor certifications, factory and site acceptance testing will have no cost saving and require full testing and validation. With minimum certifications (Bronze – the minimum level of certification) a potentially saves of 40% can be achieved, requiring 60% of the factory and site acceptance testing, and desired certifications (Silver level – desired level of certification) could have a cost saving of 60%, reducing testing to only 40%. Full certifications (Gold –- certification) will only need 25% testing due to the potential saves of 75%. The cost savings are illustrated in Fig. 9.

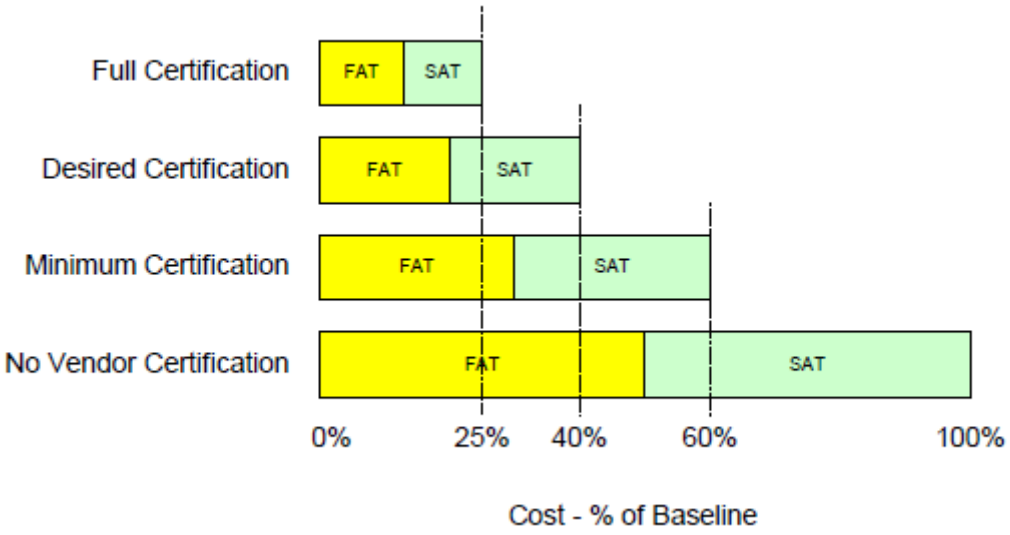

FIG. 9. Postulated effect of IEC 62443-2-4 certification on factory acceptance testing (FAT) and site acceptance testing (SAT) costs [55].

8.1.3. Factory acceptance testing

The factory acceptance test may be performed by the vendor, a third party, end customer or a combination of these. Plans are typically formalized and agreed to by all parties, particularly if exemptions are required to vendor information and computer security policies and practices (e.g. penetration testing platforms, specialized tools) to perform test cases.

The factory acceptance test is a key milestone that confirms that all computer security requirements of the product have been met. There may be some computer security requirements that cannot be evaluated at the vendor's site (factory) and these tests could be deferred to later in the life cycle (i.e. conducted during the site acceptance test or during installation and commissioning). The deferred tests are typically identified and agreed upon with the supplier.

Paragraph 4.184 of NSS 33-T states:

> "The validation of I&C system computer security measures should include an assessment of system configuration (including all external connectivity), software qualification testing, [hardware] 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" [22].

The factory acceptance test typically includes computer security requirements for integrity protection of source and configuration files; qualified security test tools and equipment; the level of earlier security tests that can be accredited (e.g. subsystem or integration tests); the level of access to be provided to the end customer to observe or conduct the security test and, if applicable, any third parties that will be contracted to conduct the factory acceptance test in whole or in part.

The protection of the integrity of source code, configuration files and installation files using secure hash algorithm (e.g. SHA-2 or SHA-3) is fundamental to ensure protection of the validated files during transfer to the end customer at the completion of a successful factory

acceptance test. Secure hash functions are typically chosen based upon recommendations for use by international or national bodies (e.g. NIST).

All factory test equipment, software and files that are needed for the factory acceptance test are typically evaluated and assessed to ensure they do not introduce the potential for an unwanted or undetected compromise of the item, product or system by an adversary.

The supplier typically provides installation and configuration procedures that will be executed and tested during the factory acceptance test. It is important that the supplier provide instructions on how to securely configure the product or item and how to leverage important security features.

The factory acceptance test typically performs the system build procedure (developed during the design phase) and confirms that the system is hardened to the greatest degree possible. System hardening may increase or decrease depending on the type and size of the procurement.

The end customer typically documents and puts in place compensating measures to minimize risk (e.g. strict access control at the factory acceptance test and end customer site, additional procedures, tamper indicating devices during transport and storage) in cases where system hardening cannot be performed prior to the factory acceptance test owing to the need for accessing certain functions and features to support testing, contract constraints or features that are needed for testing at the end customer's location.

For complex procurements, the factory acceptance test and site acceptance test typically have a documented standard build procedure that establishes the known good configuration and secure environment prior to verification and validation of system security.

Additionally, the factory acceptance test may include penetration tests that have the potential to modify the system from a secure configuration. If these types of tests are performed, the build procedure could be re-executed prior to the site acceptance test to ensure that any artefacts of the successful or attempted exploitation are removed.

The factory acceptance test typically considers mandatory inclusion of security test cases that identify whether publicly known vulnerabilities exist on the system (e.g. National Vulnerability Database – common vulnerabilities and exposures [52]) or types of software and hardware weaknesses. Identified common vulnerabilities and exposures or common weakness enumerations are typically assessed for their risk, and treated (e.g. patch update, system hardening, compensatory measures) to the greatest extent possible.

The factory acceptance test typically includes assessment of the supplier's security certificates (e.g. X.509) to establish a mechanism by which the end customer can verify the authenticity of the private key used to sign electronic communications between the supplier and the end customer.

If possible, the factory acceptance test typically includes provision of the public key of the end customer to ensure that encrypted communications from the supplier are only accessible to the end customer.

As the final procedure, the factory acceptance test typically includes the manner to securely transport and store the item, product or system between the factory and the end customer site, including use of tamper indicating devices or seals. This will increase the likelihood that unauthorized access or alteration to the system will be detected.

Electronic files (software) and hardware are typically delivered via separate channels to reduce the potential for undetected alteration to software resident within the system.

The end customer typically accepts the factory acceptance test report prior to preparing the system for transport to the site. The report typically contains at a minimum:

- Pass–fail results of security tests;
- Security exemptions required to perform the security tests;
- Security functions or features tested (or deferred to site acceptance testing);
- Secure hash checksum of all significant electronic files (based on security level);
- Installation status of tamper indicating devices.

8.1.4. Site acceptance testing

The site acceptance test is a major milestone usually involving significant risk transfer from the supplier to the acquirer, which confirms the delivered product, item or system meets the acquirer's computer security requirements through security testing. In the SCAS example illustrated in Fig. 8, the site acceptance test occurs after the product or system is installed in the target operational environment as part of the installation and commissioning phase identified in figure 1 of Ref. [29]. However, in other cases, the site acceptance test occurs prior to installation and commissioning during the system validation phase [29].

While it may be necessary to repeat performance of the factory acceptance test procedures (e.g. the build procedure) during site acceptance testing, it is good practice to have some degree of independence and diversity in testing, especially for complex procurements.

The site acceptance test typically includes, to the greatest degree possible, all end customer measures, systems and architectural features that are required in the end-state configuration (i.e. in-service state). In cases where this configuration cannot be suitably re-created or established, these security tests could be identified and performed during installation and commissioning.

All site test equipment, software and files that are needed for the site acceptance test are typically evaluated and assessed to ensure they do not introduce the potential for an unwanted or undetected compromise of the item, product or system by an adversary.

The site acceptance test is likely the final opportunity to safely perform penetration (or active) testing that could potentially result in modification or alteration of the item, product or system. These tests are typically chosen carefully to ensure that the factory acceptance test system configuration can be re-established.

The site typically provides a secure environment (physical access control, network access control, portable device or removable media restrictions) in which to conduct these security tests as well as areas for secure storage of equipment, files and test tools.

It is appropriate to indicate that the security test equipment, software and applications may require policy exemptions (e.g. password crackers, exploits) or require access to sites that are restricted by the end customer's internet proxy or firewall. Exemptions and/or access typically are carefully considered and justified.

The site acceptance test could include a vulnerability assessment to identify necessary compensatory measures that are to be validated during installation and commissioning.

Modification to the configuration or application of the patches after the site acceptance test is often difficult, if not impossible, owing to configuration management controls.

Upon completion of the site acceptance test, the system is typically stored in a secure storage location. The time constraints (outage, project, work groups) will make it increasingly unlikely that the item, product or service can be rebuilt from source files (i.e. the verified system upon the completion of site acceptance test is directly installed). This increases the importance on provision of access control and intrusion detection to the verified system.

8.1.5. Installation and commissioning

The end customer typically provides a secure installation and commissioning workspace for the item, product or system.

Generally, installation and commissioning are performed by work groups that are not involved in the earlier stages of the life cycle. Typically, these groups are identified, the personnel vetted and their access controlled.

Installation and commissioning may represent the only opportunity to test critical security features. For example, compatibility of host based and network based agents with the site's security operation centre . The factory acceptance test and site acceptance test may use internet protocol addresses, hostnames or dedicated networks that do not accurately represent the actual conditions within the site.

Installation and commissioning typically need the organizational procedures to be effective in securely configuring the device, integrating the device within the site's defensive computer security architecture and securely configuring the boundary devices.

Installation and commissioning could be viewed as the last potential opportunity to discover, characterize and mitigate vulnerabilities within the system and the defensive computer security architecture as well as evaluate the effectiveness of compensatory controls.

The completion of installation and commissioning typically verifies that the system is in a secure configuration, is compatible and compliant with the defensive computer security architecture and that access to attack pathways have either been eliminated or minimized and are controlled.

8.1.6. Operation

Upon completion of the installation and commissioning, the end customer typically provides for an enhanced monitoring period to confirm system performance of critical functions, baseline of its performance, as well as analysis to propose potential anomalous behaviour that may indicate compromise during the start of the operation phase.

Systems associated with high risk may require continuous access and configuration control, and security monitoring with the aim of detecting potential unauthorized access to attack pathways. In some cases, such as emergency preparedness systems, devices located in public areas such as airports and hospitals or for devices used at major public events, it may be impossible to exclude adversary access to all pathways. If this is the case, specific compensatory measures could be implemented, focusing on detection of malicious access to these pathways.

It is also likely that the operation phase will have the longest duration of any phase within the supply chain. Therefore, it could be necessary to consider:

— The longevity of controls (i.e. the control will remain effective or conversely, will have the potential to introduce critical vulnerabilities). For example, it is possible that vendors of ICT consumer firewalls will not provide support (approximately 3 to 5 years) that matches with the lifetime of the system (more than 10 years);
— Cryptography; key management concerns (e.g. steps to take if the keys are stolen or disclosed) and novel attack techniques that result in deprecation of an algorithm (e.g. data encryption standard);
— Service contracts that are inflexible or do not scale;
— Increasing demand for remote connectivity and real time process information;
— Compatibility of system software with information technology applications. For example, file formats that support unsupported or legacy applications;
— The potential for operating states or environment to change (e.g. lifetime of a facility);
— The increased reliance on virtualization and/or cloud services;
— The adoption of wireless or emerging technologies for other applications either supporting or having proximity to systems performing nuclear security functions;
— The increasing capability of the adversary during the lifetime of the system.

Enterprise solution providers may provide upgrade paths when systems go out of support and provide sufficient notice that a product is going out of support. The end customer typically establishes a process to monitor supplier updates to allow for sufficient time to procure the replacement, especially for long lead items (e.g. engineered item or complex procurements).

A key consideration is the application of configuration management. Where possible, the risks associated with delay of security patches, updates to configurable files and other improvements to security could be weighed against safety and/or reliability computer security requirements.

Security updates are often necessary to ensure the continued level of protection. The adversary capabilities will increase over time and while for a short period these might be mitigated by administrative control measures or other external compensating controls, these are not durable (long-lasting) enough to sufficiently reduce risk for extended lifetimes. For example, the WannaCry attack on 12 May 2017 impacted all versions of server message block (SMB) and particularly impacted systems running Windows XP. Windows XP was out of support at the time which left its versions of SMB vulnerable to CVE-2017-0144 [52] which was patched on supported versions of Windows in March 2017 (MS17-010) [56]. However, owing to the widespread damage caused by the attack, Microsoft issued a special release patch for Windows XP on 13 May 2017.

In the case of WannaCry, it was fortunate that the vendor still existed, had capability with the out of support software and was able to freely and publicly provide an effective patch on the day after the attack. While this did not provide protection to those compromised on 12 May 2017, it would have been effective if the patch was installed immediately.

Follow on attacks in 2017 (NotPetya and BadRabbit) were the costliest cyber-attacks ever perpetrated resulting in billions of dollars in damage. This had major impact on the shipping company, Maersk [57]. This demonstrates the need to continually assess risk and vulnerabilities and prioritize critical updates or other risk mitigation activities.

Unfortunately, at the end of 2018, millions of systems were still vulnerable to EternalBlue, which indicates that configuration management controls or organizational processes are ineffective in assessing and prioritizing security patch updates [57].

It is important to understand that when a system (or key part of the system) goes out of support, any security responsibilities that were provided by the supplier may no longer be readily available. This may require extended service contracts with the supplier or third party. Otherwise, the end customer may be responsible for these capabilities (e.g. hardening, vulnerability assessment, patching, workarounds, mitigating controls). This may have very significant training and resource implications the longer out of support systems (or components) are relied upon.

Furthermore, in some cases end customer capability to provide for sufficient information and computer security protection for systems relying on out of support components may be impossible. For example, it is possible that source code will not be available for the product to allow for effective self-support of legacy products (e.g. Windows XP), and software licences may restrict or prevent reverse engineering of the product. As an immediate measure (but not permanent) the end customer can perform system hardening and apply all outstanding security patches from the original supplier for these out of support systems (or components). Periodic and robust vulnerability assessments and real time monitoring may be required to provide the minimum level of protection.

Out of support software may require significant effort due to the decreasing availability of compatible tools (vulnerability scanners), hardware (trusted platform module), software (e.g. anti-virus, whitelisting) and market availability of expertise and platforms that support these assessments.

In cases where the parts of the system or components will end support (i.e. out of support) before the lifetime of the system, patches may no longer be readily available through their normal mechanisms (e.g. update channels) or through other trusted supplier channels. In these cases, the end customer could have a process to obtain and securely archive all available patches while they are readily available with the expectation that sometime after the end of support, the patches will be installed. This key step may provide extended time for which information and computer security risks can be treated as near baseline (i.e. fewer vulnerabilities that need to be addressed via compensatory controls).

Where risks are high, assessments are typically performed by external, certified organizations that have the capability and competence required for the system, platform or environment being assessed.

Anti-malware scanning applications are also typically assessed to determine whether they provide protection for the legacy or out of support software. As mentioned earlier, protections implemented in current operating systems and development practices have greatly reduced exploitation of buffer overflows. This may lead to anti-malware application suppliers not providing signatures for ‘older’ buffer overflow attacks leading to unmitigated risk to legacy systems.

For systems having longer lifetimes (more than 10 years), it is possible that commercial or market viability of security services will not be available for the entire lifetime. Having a training programme in place to develop and sustain competence as well as continually improving organizational processes may deliver the necessary capabilities.

It is possible that a service contract is put in place for a supplier to provide the necessary competences and capabilities, but this is likely economical only in instances where a wide distribution of similar systems exists.

National export control, laws and regulations may pose restrictions to the level of service provided by an international partner.

8.2. REPAIR, REFURBISH AND RETURN TO STOCK

Repair, refurbishment and return to stock may represent a transfer of custody of equipment or software. This introduces touchpoint risks at both relevant entity and transition locations.

These activities typically are assessed for risk. Those that are associated with information and computer security risks may require additional computer security requirements.

The tasks and activities for repair and refurbishment could include:

- Location of the activities (site or vendor);
- Availability of hot or cold spares;
- Independent and/or concurrent (e.g. two person rule) verification process;
- Certification of the vendor's information security management system or computer security programme (process capability, trustworthiness evaluations);
- Competence of vendor staff;
- Temporary modifications to allow for the repair or refurbishment (remote connection, disabling or removal of measures, non-standard configuration);
- End customer site condition (e.g. outage);
- Computer security requirements for secure maintenance environment.

When managed, these risks will likely require similar measures put in place as those for factory acceptance testing, site acceptance testing and installation and commissioning. It is good practice to ensure that the services do not introduce malware or maliciously implanted devices (e.g. hardware). For this reason, it is less likely that penetration testing is done during repair of the items.

Unplanned repairs on high risk items, products or systems typically have approved procedures prior to the use stage to account for expected operational failures. These procedures are typically reviewed and validated to ensure the continued provision of the required information and computer security protections.

Return to stock, especially of inspection or maintenance equipment stored at the supplier location, could include tamper indicating devices or seals; full disk encryption (i.e. password is required to decrypt non-volatile media); use of secure storage locations that provide the necessary monitoring and detection of accesses; unique identifiers for equipment; logs and records and security procedures (check system start up times, logs, inspection, malware scans, integrity checks, vulnerability scanning) to check in and check out items, products or equipment from stock.

Processes typically are put in place to restore computer security measures that are required by the system (e.g. disabled controls to allow for maintenance or repair procedures).

8.3. DISPOSAL OF UNUSED MATERIAL

Decommissioned or removed items, products or systems typically are sanitized prior to disposal to remove sensitive information.

Guides such as NSA/CSS Policy Manual 9–12 [58] may be used to inform storage device sanitization procedures.

It is appropriate to ensure that all data is removed or erased (e.g. no data remanence) especially with media that allows for recovery of deleted or overwritten data. Further potential solutions are encryption or media destruction as well as degaussing for magnetic media.

9. CORRECT STAGE

The correct stage has greater importance for information and computer security than for other considerations such as safety or quality assurance because it could be significantly impacted by external considerations (e.g. adversary). Coupled with the inherent ambiguity on the exact computer security requirements, the uncertainty involved with information and computer security risks is considerable and will only increase over time. The quantification of this uncertainty is even more challenging given the complexity of contemporary supply chain arrangements.

The correct stage includes non-conformance control and supplier management activities such as contract close out. This stage is particularly important for ensuring continued compliance to meeting computer security requirements.

Whereas the use stage is concerned with establishing the security baseline (i.e. factory acceptance testing, site acceptance testing, installation and commissioning, operation, maintenance and decommissioning), the correct stage is concerned with taking significant action to update security due to external events such as new classes of malware, increased adversary capability or disruptive advances in tactics, techniques and procedures.

Significant corrective actions are typically needed for the following events:

- Major changes or updates to national regulations or computer security requirements;
- Update or changes to end customer policies or processes;
- Issue of a new DBT or threat statement by national authorities;
- Change in status of product (e.g. out of support, obsolete, ICT technology (Frame Relay, 2G, 3G) unavailable);
- Change in status of vendor (e.g. merger, bankruptcy, ownership, spin-off);
- Deprecation of standard (e.g. DES, MD5, SSL);
- Other changes as per ISO/IEC 27036-2:2014 section 7.4.3 (e) [24].

Examples of corrective actions could include:

- Re-negotiation of the contract with the supplier to provide additional support or a decrease in capability to support the end customer;
- Close out of the contract and negotiation of a new contract with a third party supplier;
- Coordination in exercises to ensure effective response and recovery during an attack performed by the hypothetically most capable adversary for which the end customer is responsible to provide protection (as described in DBT);
- Update of systems or services to meet current computer security requirements.

It is good practice for the end customer to consider risks to the long term effectiveness of security for the supplied item, product, system or service. The contracts are typically flexible to allow for necessary corrective actions to be performed without the need to re-negotiate or re-tender contracts.

9.1. CHANGES TO NATIONAL REGULATIONS OR LAWS

A significant change to national regulations or laws may involve one or more of the following:

— Nuclear or operational technology standard. For example, computer security requirements to provide real time monitoring and an increased application of security features to provide services (i.e. identification, authentication, authorization, accountability, auditing). These changes may force the update to newer technology that can provide the necessary features to verify compliance.
— National legal requirements for information protection (e.g. personally identifiable information). For example, the General Data Protection Regulation (GDPR) of the European Union (EU) [59] went into effect on 25 May 2018. This strengthened individuals' fundamental rights to data protection to provide natural persons with more control over their personal data and increased obligations on businesses and organizations that collect, store or process such data. Most importantly, the GDPR applies to organizations outside of Europe when they collect, store or process data belonging to EU citizens and residents. Obligations to comply with the GDPR may be a significant consideration for international companies and particularly for those that employ EU citizens and residents.

Given the increasing importance of information and computer security, governments and international bodies may demand greater effort to provide appropriate protection to information and items, products and services that support significant nuclear security functions. Therefore, it is important that contracts with suppliers consider that significant updates or changes to applicable laws and regulations may occur at some point during medium to long term contracts (more than five years).

9.2. ADVERSARY CAPABILITY

Information and computer security are an ever-changing domain of nuclear security. This can be driven by the increasing pace of adoption of new technologies by businesses and consumers and the increasing ability of adversaries to identify and exploit vulnerabilities in adopted technologies.

Supplier relationships and contracts typically take into account significant revision to adversary capabilities, tactics, techniques and procedures particularly as they pertain to increasing advancement, use and/or adoption of cyber-attack skills. Specific drivers could be malware platform development that reduces the competence required to deploy and manage sophisticated cyber-attacks (e.g. Ransomware as a service, Botnet command and control); circumvent advanced capabilities (e.g. techniques to jump the air-gap) or vulnerability information (e.g. EternalBlue) that enable increasingly impactful and consequential attacks and increasing integration and adoption of always on, always connected technology (e.g. industrial internet of things).

The end customer typically establishes good computer security culture to ensure that necessary corrective actions are considered based upon conservative estimations (i.e. exceed the level) of adversary capability advancement.

It is no longer satisfactory to maintain a static level of security since an adversary could learn to overcome today's protections at some point in the future. Supplier relationships typically consider this dynamic attribute to continually improve upon security for items, products and systems as well as organizations and suppliers.

Considerations for cryptographic protocols in long term contracts can be significant. For example, the transport layer security (TLS) cryptographic protocol TLS v.1.2 was issued in

August 2008 and replaced by TLS v.1.3 in August 2018 to address new adversary tactics, techniques and procedures that reduced the security of v.1.2 (see Annex VI). For systems having long lifetimes, it is essential that the current standards are used for both items and products as well as services (e.g. remote maintenance or monitoring).

Contracts typically allow for an update and correction mechanism or a process that allows for the best security practices to be applied in the most effective and efficient manner possible.

It is generally unacceptable to operate using deprecated protocols, algorithms, software, libraries or other standards owing to restrictive contracts that do not consider the ever-changing needs of information and computer security. During the transition to upgrade from deprecated protocols, compensating security controls are typically put in place (e.g. in line with the 'legacy' security controls sections of IEC 63096 [5]).

9.3. CONTROL OF NON-CONFORMANCES

Supplier non-conformance to computer security requirements set by the customer could result in undesirable outcomes such as:

- Significant vulnerabilities that are disclosed to the supplier are not communicated to the end customer, resulting in the end customer being unable to reduce or eliminate the risk. It is good practice to have a metric that reflects the acquirer's risk to determine significance of vulnerabilities (i.e. the supplier typically does not determine what is significant to the acquirer since it is possible that the supplier will not know the function of the sensitive digital assets affected by the vulnerability).
- Security patches and updates are not communicated and provided to the end customer, resulting in the end customer being unable to eliminate the risk through patching.
- Cyber-attacks that result in supplier compromise (or the compromise of the supplier's supplier) are not reported to the end customer, resulting in delivery of a compromised item to the end customer. This is particularly important for supplier's that are providing continued services, items, products or systems to the end customer, or the attack compromises key technical details of operational systems.
- Revocation of supplier security certificates (X.509) or expiration of certificates. Certificates are a key aspect of trust. Compromised or revoked certificates can have major security impacts especially on ensuring authentication and integrity of signed digital messages (e.g. SolarWinds supply chain code compromise [31, 60]).
- Discovery of common weakness enumerations (e.g. back doors, poor coding practices) that existed during development stages but were not corrected prior to the factory acceptance test.

The risk of these non-conformances can be lowered by:

- Establishment of robust security culture for both the acquirer and supplier;
- Training of personnel at both the acquirer and supplier;
- Contract clauses that include identifying and reporting processes regarding changes and incidents that have information or computer security impacts;
- Effective monitoring and enforcement by the acquirer with support provided by the supplier.

Typically, a timescale (e.g. days, months, years) is indicated for which the non-conformance needs to be corrected.

9.4. SUPPLIER MANAGEMENT

Supplier management typically involves the following considerations to ensure the continued compliance with information and computer security requirements:

- Supplier relationship process: this involves the strategy, such as determining if vendor support will be available for the entire lifetime use of the system or service. If not, the acquirer could consider developing internal capability or identify and select a third party to provide the necessary capability.
- Supplier maintaining computer security certification: this involves the certifications, expected performance and standards that are obligated for the supplier to maintain over the duration of the contract. For example, IEC 62443-2-4 [55] maintenance of Gold certification may require the supplier to update their security programmes. Additional considerations, especially for risk transfer, involve the necessary reporting by the supplier to the acquirer based upon changes, incidents or periodic reviews.
- Supplier relationship agreement process: this involves clauses and processes to allow for the efficient and timely update or modification to the agreement based upon changing information and computer security challenges.
- Supplier relationship management process: this involves key time scales for certain activities that are postulated to occur during the lifetime of the contract. Specific events may be cyber-attack on the acquirer, supplier or supplier's supplier; routine exercises that involve one or more contracted organizations and end of support or lifetime of a service or product; or other changes such as those listed in section 7.4.3 of Ref. [24]. This is likely the longest duration of any acquirer–supplier relationship, and care is typically taken when listing the postulated tasks, activities, incidents and events that may occur during this time.
- Supplier relationship termination process: contracts may be terminated owing to successful completion of the contract; changes to the business or system of the acquirer or supplier; establishment of a contract with a competitor making the original contract redundant; or resulting from non-compliances that require punitive action. Care is typically taken when terminating contracts as it may result in periods for which information and computer security requirements are not ensured nor attained. Generally, termination also includes return, retention or destruction of specific sensitive information by the acquirer or supplier based upon the contractual requirements of the information owner.

APPENDIX I. THE NUCLEAR SUPPLY CHAIN

I.1. NUCLEAR POWER

Section 2.2 of IAEA Nuclear Energy Series No. NP-T-3.21 [9] states:

> "Typical nuclear supply chain tiers are shown in [Fig. 10]. New build projects are typically concerned with how tier 1 technology vendors set up and manage their supply chains, while operating plants typically deal directly with tier 3 and below for spare parts associated with operation and maintenance activities. The two activities are invariably linked, as decisions and procurement choices made by the technology vendor (e.g. choice and location of key suppliers) will have implications for the supply chain throughout a plant's life" [9].

Figure 10 outlines the supply chain tiers from tier 1 to tier 6. OEMs in the SCAS align with both tier 3 and tier 4.

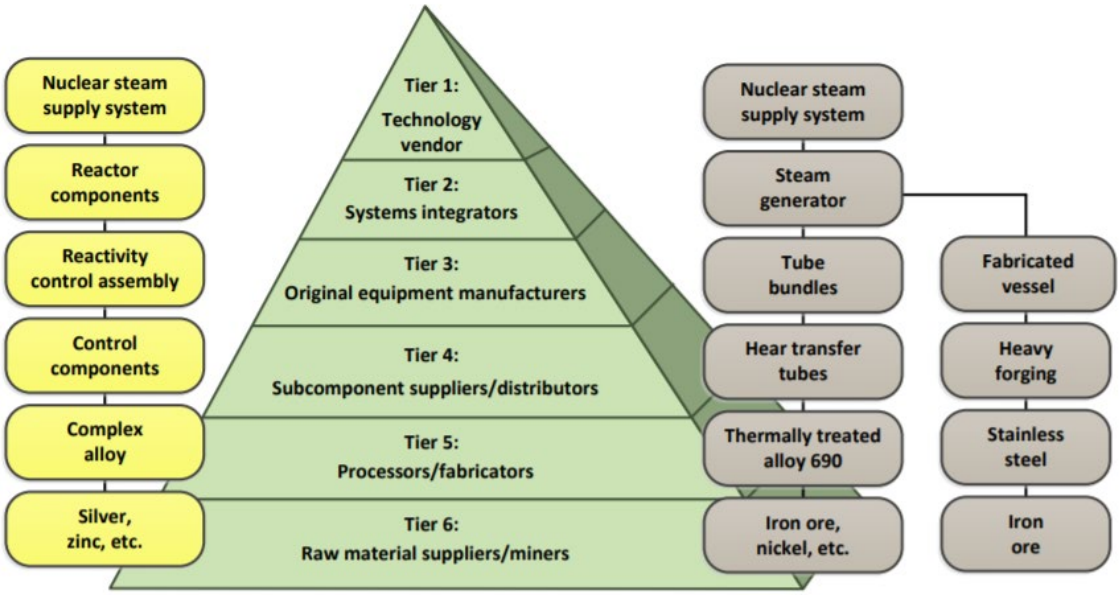

FIG. 10. Typical nuclear supply chain tiers figure 2 from Ref. [9].

Reference [9] contains references to national standards that contain limited guidance on computer security. However, the process of specify, source, use, and correct stages along with the tiers are key concepts upon which this publication is structured.

For computer security, the concerns are pervasive throughout all tiers of the supply chain (tiers 1 through 6). The scarce resources for protection generally require pragmatic decisions and, most importantly, the application of the graded approach to be limited to those tiers that have unacceptable risks associated with compromising suppliers.

Generally, direct relationships between the acquirer and the supplier fall into tiers 1 through 3[19]. General computer security requirements apply to tiers where there exists a direct contract. However, the transfer of risk to indirect relationships typically need these considerations to be

[19] Tier 3 –OEMs are the exception rather than the rule. The OEM would likely be direct, in the case of large projects that involve complex procurements.

detailed within direct contracts. This implies that tier 2 or tier 3 suppliers (integrators, OEM) will manage or modify the risk and provide assurance that risk has been effectively managed at lower tiers (tiers 4 through 6, OEM subcomponent suppliers and distributors, manufacturers, processors and fabricators).

It is good practice to use the SCAS (see Section 4) to identify risks and evaluate the severity of the associated risk to ensure sufficient protection of the supply chain.

I.2. INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN

Paragraph 5.23 of Ref. [7] states:

> "An ICT supply chain is a set of organizations with a linked set of resources and processes that form successive supplier relationships of ICT products and services. (…) As depicted in Figure 1 [Fig. 11], an organization in an ICT supply chain is an acquirer in relation to the upstream organization, and a supplier in relation with downstream organization" [7].

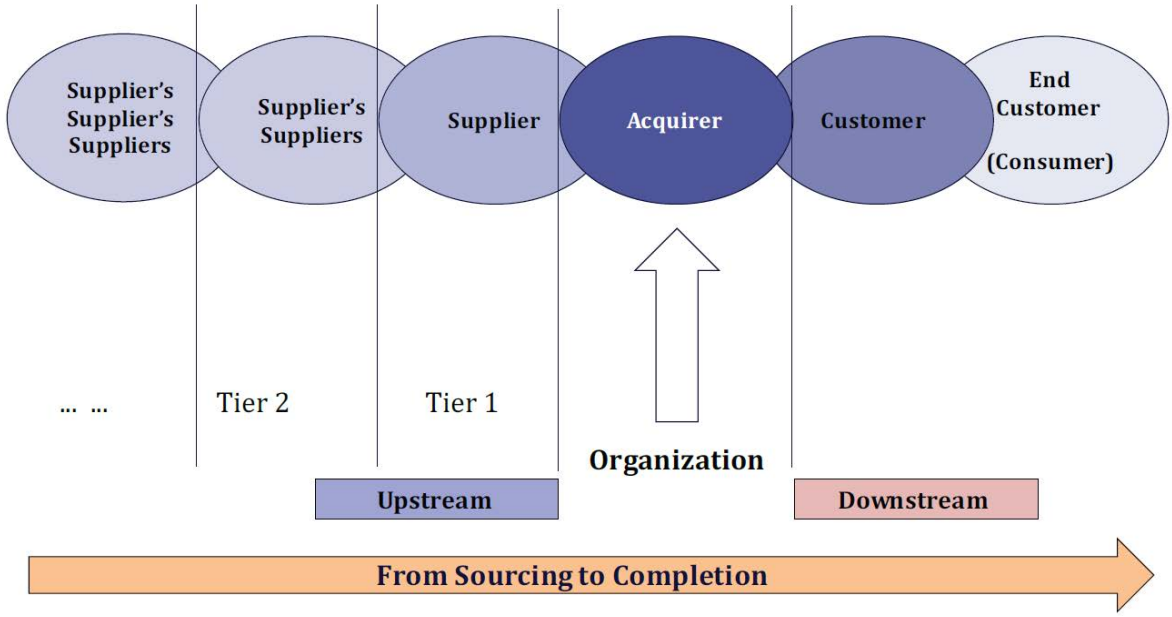

FIG. 11. Typical nuclear supply chain tiers figure 1 from Ref. [7].

The designation as a customer or supplier depends on the placement of the organizations within the supply chain. As depicted in Fig. 11, the supplier to the acquirer is also an acquirer of the supplier's supplier services or products. This is also true of the acquirer which is a supplier to the customer and end customer.

The tiers in Fig. 10 do not align with how the tiers are used in this publication or in Ref. [9]. Reference [14] discusses supply chain security for an information security management system. The wide acceptance and adoption of the ISO/IEC 27001 series could be critical to ensuring a common framework and vocabulary for global supply chain computer security.

ISO/IEC 27001 [14] certification for organizations provides the acquirer with confidence that the supplier considers information and computer security important to their mission. ISO/IEC 27001 [14] certification requires independent assessment by qualified auditors.

Other similar certifications, such as ITIL and COBIT, are well recognized international norms and standards.

I.3. CLOUD SERVICES

Reference [54] states: “Typically, cloud services are purchased “as is”; a cloud service customer has no ability to specify or request changes to the cloud service being purchased. However, in certain cases, the customer has the ability to specify the service and the detail of that service, including the information security arrangements required of the supplier” [54].

Three potential cloud deployment options are identified in Ref. [54]: public cloud, hybrid cloud and private cloud. The public cloud is the option where the service does not consider the risk to the acquirer, whereas for the private (and less so hybrid cloud), the supplier agrees to fulfil the acquirer’s information computer security requirements (i.e. risk transfer).

The following three cloud capability types are identified in Ref. [61]:

- Application capabilities type: the cloud service customer can use the cloud service provider’s applications. ‘Software as a service’ is the cloud service that offers application capabilities.
- Infrastructure capabilities type: the cloud service customer can provision and use processing, storage or networking resources. ‘Infrastructure as a service’ is the cloud service that offers infrastructure capabilities.
- Platform capabilities type: the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider. ‘Platform as a service’ is the cloud service that offers platform capabilities.

APPENDIX II. TYPES OF PURCHASES, PRODUCTS AND SERVICES

Computer security requirements could be incorporated into the purchase orders and agreements based on the type of purchase (i.e. standard, blanket, planned blanket, contract) and the classification of the purchase (i.e. catalogue, simple, complex). Based on these factors, the level of risk will inform the acquirer of the level of computer security requirements and security controls that are typically implemented to minimize the associated risks.

II.1. PURCHASE ORDERS

Purchase orders can be divided into four types: standard, planned, blanket and contract purchases.

> "A standard purchase orders is typically used for irregular, infrequent or one-off procurements. (…) It contains a complete specification of the purchase, setting out the price, quantity and timeframes for payment and delivery.
>
> Planned purchase orders is relatively comprehensive. A planned purchase requires full details of the goods and services to be purchased and their costs. Dates for payment and delivery are also included in a planned purchase, but these are treated as tentative dates. Issuing a release against the planned purchase places individual orders.
>
> A blanket purchase orders involve an acquirer agreeing to purchase particular goods or services from a specific vendor, but not at any specific quantity. Pricing may or may not be confirmed in a blanket purchase order. This type of order is typically used for repetitive procurement of a specific set of items from a supplier such as basic materials and supplies.
>
> A contract purchase orders set out the vendor's details and potentially also payment and delivery terms. The products to be purchased are not specified. A contract purchase order is used to create an agreement and terms of supply between a purchaser and vendor as the basis for an ongoing commercial relationship. To order a product, the purchaser may refer to the contract purchase when raising a standard purchase" [62].

The type of purchase is typically informed by both the risk and resources. Design, implementation and verification of security requires resources (funds, time, personnel) that typically are accommodated in the purchase planning. Selecting an appropriate type of purchase will allow for the efficient use of resources for the inclusion of computer security requirements and controls for nuclear security.

II.2. TYPES OF PURCHASES, PRODUCTS AND SERVICES

The ability of the customer relevant entities to secure the supply chain is related to the type of purchases. Purchases can either be for products, services or both (i.e. hybrid). The more substantial the relationship that exists between the acquirer and supplier, the greater the potential to include or inform necessary security arrangements that leverage this trusted and continual relationship. For example, irregular or one-off purchases provide limited opportunity for the acquirer to include specific computer security requirements in the acquired product or service.

Consideration of computer security of the supply chain typically occurs at the earliest possible stage of any procurement. This involves understanding the type of purchase; the type of product or service; the risk associated with the procurement (see Section 4); the acceptable risk threshold including prioritized risk treatment options (see Section 4) and the supplier tiers that need involvement for the effective management of risk (see Fig. 1, Section 4 and Appendix I).

II.2.1. Products

The type of product purchase can further be classified as catalogue, simple or complex. The following three types of purchases for products could be considered for the application of computer security measures:

- Catalogue purchase: the acquirer takes on the responsibility for computer security requirements. Typically, this involves purchase of a COTS item (or product) that may undergo commercial grade inspection along with additional tests as required by the acquirer. Generally, the acquirer interfaces only with tier 1 of the nuclear supply chain (see Fig. 1), but the supplier likely involves the other tiers that are unknown to the acquirer.
- Simple procurement: the acquirer can impose a limited number of computer security requirements on the supplier via a formal contractual relationship to customize the design of a product for which the nuclear security function is known. Typically, this involves a pre-developed item that is modified to meet nuclear computer security requirements. This is a hybrid between catalogue purchase and complex procurement. Generally, the acquirer interfaces with tiers 1 and 2, and potentially tier 3 of the nuclear supply chain (see Fig. 1).
- Complex procurement: the acquirer can impose all computer security requirements that are necessary to meet all regulatory requirements. Typically, this involves the acquirer specifying computer security requirements and evaluating the systems that implement these computer security requirements. The acquirer potentially interfaces with all tiers of the supply chain for critical elements of the system.

II.2.2. Services

Nuclear security may require support and maintenance that requires access for support from a variety of services and service providers. These can include contracts for physical protection personnel; computer security specialists; maintenance of sensitive digital assets; independent assessments or audits of security activities; and technical or administrative support, which would be considered complex procurements.

Purchases of services are typically executed via contract. The scope of contracting can be small, task or deliverable focused activities, larger in the case of major projects or lifetime activities or a complete outsourcing of specific functions. Typically, many end customers within a nuclear security regime either partially or completely outsource both physical and computer security functions.

Current outsourcing trends in information computer technology services are leading to the adoption of cloud based services. In Ref. [63], cloud computing is defined as “[p]aradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.” The explanatory note accompanying this definition adds: “Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.” [63].

The different types of cloud service (e.g. infrastructure as a service, platform as a service, software as a service) typically determine the level of responsibility of the acquirer in managing risk. The nuclear security risk is always retained by the acquirer unless risk has been transferred via contract agreement. For example, acquirers purchasing infrastructure as a service will have the greatest share of risk responsibility with respect to the cloud service. For software as a service, the supplier will have the greatest risk with the responsibility in ensuring the protection of the application or software. The use of cloud services also requires special consideration. For example, if a supplier uses them to produce products or to perform engineering for equipment that is shipped to the plant operator [54].

II.2.3. Hybrid

An example of a purchase that involves both types is an engineer procure construct (i.e. turnkey) contract where the supplier(s) provide both a system and the services. The engineer procure construct contractor coordinates all design, procurement and construction work, and ensures that the entire project is completed as required and on time.

APPENDIX III. INFORMATION AND COMPUTER SECURITY CONCEPTS

The Information security in a multi-user computer environment, Advances in Computers article by J.P. Anderson states:

> "One aspect of information security is the protection of information, which can be both tangible and intangible. There are three specific types of security compromise: unauthorized information release; unauthorized information modification and unauthorized denial of use" [64].

Protection against these violations is critical to ensure nuclear security, and protection of sensitive information is a fundamental element of nuclear security [8]. Information security measures are typically implemented for the protection of sensitive information [22]. Additionally, sensitive digital assets need to be protected [8] by implementation of computer security measures.

III.1. RISK

Risk, in the computer security context, is the risk associated with an adversary exploiting vulnerabilities of a digital asset or group of digital assets to commit or facilitate a malicious act. It is expressed in terms of a combination of the likelihood of a successful attack and its consequences if it occurs [13].

Figure 12 provides an illustration of increasing impact (consequences) for different types of nuclear security events across the domains of nuclear security. Figure 12 also makes note that the scales used in Refs [18–20] are considered independently.

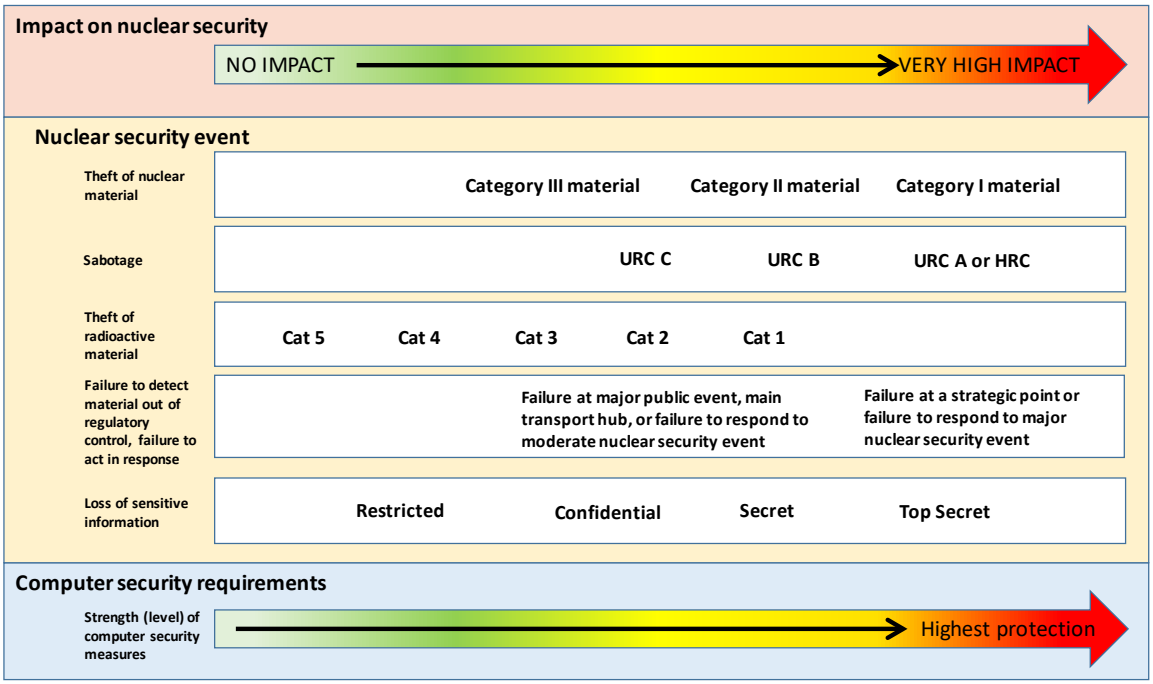

FIG. 12. Illustration of varying severity of consequence for different types of nuclear security event figure 7 from Ref. [10]. HRC — high radiological consequences, URC — unacceptable radiological consequences.

Risk is defined as the effect of uncertainty on objectives [65]. It is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

Likelihood is considered as a combination of the following [22]:

- The identified and assessed threats to the facility;
- The attractiveness of the digital asset to potential adversaries;
- The vulnerabilities of the digital asset[20];
- The operating environment.

The challenge with likelihood (exploit difficulty) determinations is the lack of comprehensive data sets, based upon operational experience, which can be used to accurately quantify likelihood. Publicly disclosed attacks against nuclear security are too limited to provide the necessary information upon which to quantify likelihood. Paragraph 4.18 of NSS 17-T (Rev. 1) states:

> "For facility functions important or related to nuclear security, a classification scheme based on consequences for nuclear security, such as that outlined in [figure 7 of Ref. [10]], should be used to determine the significance of the function" [13].

Reference [13] applies to nuclear facilities, and this pragmatic assumption is necessary owing to the difficulty in accurately determining likelihood of a successful attack, and therefore the general determination of significance (and by inference, risk evaluation) relies almost exclusively on consequence severity.

The significance of the function will inform computer security level requirements based upon the potential severity of the consequence that may result from compromise of the system. These requirements are typically considered and managed throughout the entire procurement process.

Information and computer security risk management is an ongoing process that requires continuous improvement. This could include:

- Planned risk assessment updates;
- Continual improvement to conform to updated industry practices;
- Periodic assessment of security culture and how it affects conformance to policies and procedures;
- Attention to changing legislation for coverage under treaties or statutes and subsequent financial liability and increasing insurance needs;
- Noting that insurance markets are maturing in their approaches to cyber risks and policies, with new coverage opportunities or restrictions;
- Training in computer security and acquisition or contracting practices across the organization;

References [10, 13] are well-aligned with the risk management processes standardized in Ref. [14] and further expanded upon in Ref. [11]. Figure 13 illustrates the risk management processes of Ref. [11]. Additional information on risk assessments for automation systems to meet graded computer security requirements can also be found in Ref. [35].

According to Ref. [65], an information security management system

> "consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting

[20] Vulnerabilities are weaknesses or flaws in systems and/or the security measures that protect them, that have the potential to be exploited by an adversary.

its information assets. An [information security management system] is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks" [65].

The steps of an information security management system risk assessment are [14]:

— Establish risk acceptance – criteria to determine risk treatment options for identified risks;
— Risk identification – identify risks associated with loss of confidentiality, integrity and availability;
— Risk analysis – determine likelihood and severity of consequence;
— Risk evaluation – compare results against risk acceptance criteria and prioritize risk treatment.

Information security management system risk treatment consists of selecting the correct option; comparing and determining necessary controls; producing a statement of applicability and formulating a risk treatment plan [14].

The overall flow of risk management is illustrated in Fig. 13.

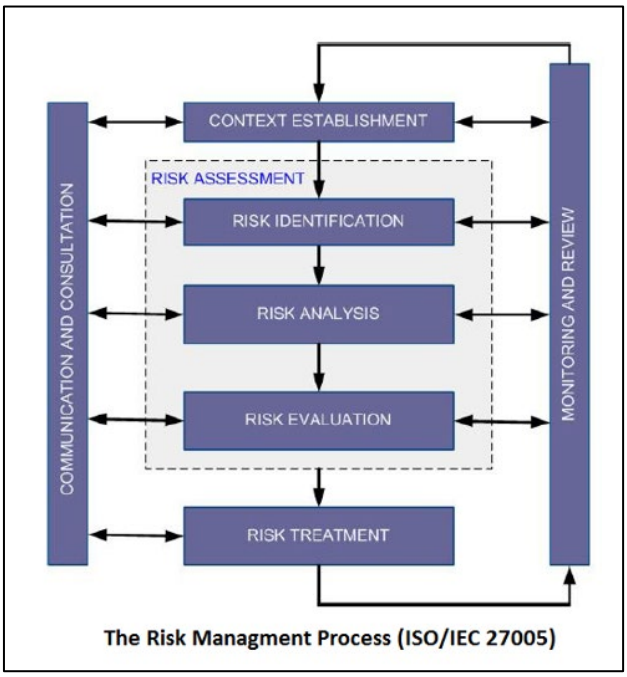

FIG.13. Risk management processes in Ref. [11]

Table 1 is a cross-reference of the eight risk management elements in Ref. [11] with the State's corresponding activities international standards and guidance (IAEA, ISO/IEC).

TABLE 1. RISK MANAGEMENT CROSS REFERENCE

Risk Management Element (ISO/IEC 27005)	**State**	**ISO/IEC**	**IAEA General**	**IAEA Specific (Information and Computer Security)**	**This Publication**
Context Establishment (External)	State Legal and Regulatory Framework	ISO/IEC 27036 IEC 62645	Risk Acceptance Criterion NSS Nos 13,14,15 and associated Implementing Guides	NSS No. 42-G National Policy	Section 4 Appendix III Annex IV
Context Establishment (Internal)		ISO/IEC 27036		NSS No. 23-G NSS No. 17-T, Rev.1 (Definition, Facility Characterization) NSS No. 33-T	Section 4
Communication and Consultation	National Legislation Regulatory Requirements	ISO/IEC 27036	NSS No. 10	NSS 42-G (Coordinating Mechanism) NSS No. 17-T, Rev. 1 (Facility SSP, SAR, Policy, Computer Security Plan, SS Threat Statement. Information Protection	Section 6
Risk Identification	DBT or Threat Statement	ISO/IEC 27036 IEC 62645		NSS No. 17-T, Rev. 1 (Facility Characterization, Threat Characterization)	Section 4
Risk Analysis		ISO/IEC 27036 IEC 62443-3-2	NSS Nos 23-G, 33-T, 42-G, 17-T, Rev. 1	NSS No. 23-G (Classification of Information). NSS No. 17-T, Rev. 1 (Facility Characterization, Threat Characterization)	Section 4 Section 6
Risk Evaluation		ISO/IEC 27036, 15408	NSS Nos 33-T, 17-T, Rev. 1	NSS No. 17-T, Rev. 1 (CSR Specifications)	Section 6 Section 7
Risk Treatment		ISO/IEC 27001, 27002, 27036 IEC 63096, 62645	NSS No. 17-T, Rev. 1	NSS No. 17-T, Rev. 1 (System CSRM, DEFENSIVE COMPUTER SECURITY ARCHITECTURE)	Sections 6–8
Monitoring and Review	Inspections	ISO/IEC 27036		NSS No. 17-T, Rev. 1 (Assurance Activities)	Section 9

III.2. SENSITIVE INFORMATION AND SENSITIVE DIGITAL ASSETS

Sensitive information and sensitive digital assets are important subgroups of nuclear information and digital assets, respectively. The distinction between non-sensitive and sensitive has considerable importance for nuclear supply chain as new supplier relationships introduce new computer based systems and information into a State's nuclear security regime. It may be necessary to have additional analysis, application of measures, and regression testing to determine the risk associated with the establishment of these new relationships.

The type of relationship (service, product), the sensitivity of information [21], or the significance of the function are important considerations in establishing criterion for managing risk to within or below acceptable levels.

The type of asset (information object, computer based system) generally informs the selection and feasibility of protective measures.

Sensitive information is defined as "[i]nformation, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security" [13].

Sensitive information assets are defined as "[a]ny equipment or components that are used to store, process, control or transmit sensitive information. For example, sensitive information assets include control systems, networks, information systems, and any other electronic or physical media" [13].

Computer based systems are defined as "[t]echnologies that create, provide access to, process, compute, communicate or store digital information or that perform, provide or control services involving such information. These technologies may be physical or virtual" [13]. According to para. 2.31 of Ref. [13], "[c]omputer based systems make use of, depend on or are supported by digital technologies" [13]. They include those that are not within the nuclear security regime (i.e. cover the entire world and applications of computers and their derivatives).

Sensitive digital assets are defined as "[s]ensitive information assets that are (or are parts of) computer based systems" [13]. Digital assets include sensitive digital assets and other computer based systems that are not sensitive but are part of the nuclear security regime.

A graded approach for computer security requirements and the prioritization of risk treatment options to provide defence in depth can be achieved by the identification and classification of sensitive information and sensitive digital assets that perform or support significant functions.

III.3. FUNCTIONS

Functions may be considered to be objectives that typically are achieved to ensure nuclear security (including safety). When functions are performed by, depend upon or are supported by sensitive digital assets, there is a potential that cyber-attack can compromise functions resulting in unacceptable consequences.

Functions rely upon products and services that are provided through the supply chain. Consequently, it is good practice to have computer security within the supply chain to ensure the correct performance of functions.

The supply chain provides adversaries with increased opportunities to access digital information and systems (e.g. during development or shipment) and to potentially maliciously

alter the function (e.g. create a logic bomb[21]). It is possible that compromise of functions while in development will not be observable, and there could be increased opportunities for the adversary to use stealth. These factors provide tremendous value to potential adversaries.

There can be nuclear security consequences to a facility if functions are not performed correctly. Footnote 23 in NSS 17-T (Rev. 1) states:

> "The significance of the function to nuclear security can often be associated with the consequences of the function's not being performed correctly. For nuclear facilities, the consequences that are considered most significant are unauthorized removal of nuclear material and sabotage resulting in unacceptable radiological consequences. Other consequences, such as unauthorized disclosure of sensitive information, might be considered. Other possible consequences might be associated with other organizational objectives, for example maintaining reputation or remaining compliant with other environmental regulations. A list of possible consequences can be found in ISO 27005:2018 [15]" [13].

Cloud services such as 'infrastructure as a service' or 'platform as a service' may directly provide a significant function. In this case, it is critical that the customer accurately specify the computer security requirements to ensure that the security provided by the cloud service provider is appropriate and sufficient.

This uncertainty can be grouped into four potential results of compromise of a system function. Paragraph 2.21 of NSS 33-T states:

> "The potential consequences of a compromise on I&C system function are, arranged in the order of worst to best cases:
>
> — The function is indeterminate. The effects of the compromise result in an unobserved alteration to system design or function.
> — The function has unexpected behaviours or actions that are observable to the [acquirer].
> — The function fails.
> — The function performs as expected, meaning the compromise does not adversely affect system function (i.e. it is fault tolerant)" [22].

Therefore, compromised functions are strongly correlated with nuclear security consequences by the significance of the function and the effects of compromise on system function.

III.4. SECURITY LEVELS

Computer security levels and computer security zones are a standard approach to protect systems. Paragraph 2.8 of NSS 17-T (Rev. 1) states:

> "A computer security level is a designation that indicates the degree of security protection required for a facility function and consequently for the system that performs that function. Each computer security level is associated with a set of requirements imposed by the [acquirer] to ensure that the appropriate level of

[21] A logic bomb is a malicious program that is triggered when a specific logical condition is met, for example after a certain number of transactions have been processed, when starting execution of an infected code, when deleting a specific data set from a system, or on a specific date and time (also called a time bomb).

protection is provided to digital assets assigned to that level based on a graded approach. Each computer security level will need different sets of computer security measures to satisfy the computer security requirements for that level" [13].

Critical functions are important to and support nuclear security. Current IAEA guidance provides defined levels for nuclear facilities (e.g. NPPs – 1 to 5) and other radioactive material and associated activities (A to C). Figure 12 provides an illustrative example of information and computer security consequences for nuclear security domains, but does not apply a deterministic approach.

Table 2 simplifies the relation of the different domains of nuclear security to their computer security level requirements for supply chain relationships in other domains.

TABLE 2. NUCLEAR DOMAINS AND SECURITY LEVEL CROSS REFERENCE

Nuclear domain security impact	NSS 13 Security level	NSS 14 Security level	NSS 15 Assets or function	Classified info NSS 23-G
Severe	1 – Reactor protection system	No equivalent	Prevention and detection	Top secret
High	2 – Physical protection system (PPS)	A/B (e.g. PPS) (Cat 1, 2 source)	Prevention and detection	Secret
Moderate	3	C (PPS) (e.g. Cat 3 source) (demilitarized zone)	Detection	Confidential
Limited	4	No equivalent	Detection	Restricted
Negligible	5	Corporate environment	Under regulation	Unclassified

For simplicity, this publication will use the security levels associated with Ref. [13] to represent the specific computer security level requirements applicable to other security levels or assets found in other nuclear security series domains.

III.5. SECURITY ZONES (AND MEASURES)

Zones contain assets that share computer security requirements due to inherent properties and need for communication. Computer security zones are a means of grouping digital assets to simplify the administration and application of computer security measures.

Computer security requirements and security zones are the essential building blocks of a defensive computer security architecture. Furthermore, defensive computer security architectures are an important concept necessary for implementing computer security defence in depth for sensitive digital assets. Implementing defensive computer security architectures are typically part of the 'security by design', and typically considered during the specify (design) stage.

Reference [13] provides an example of a defensive computer security architecture for an NPP. However, this defensive computer security architecture cannot be directly copied and applied to development or supply chain activities. It is appropriate that the needed communications,

information transfers and access be analysed to develop a defensive computer security architecture specification that will allow for monitoring and mitigation of risk associated with necessary supply chain activities. For example, a software vendor that is developing a custom application may require privileged access (both physical and logical) to the software development environment as well as the target system. The vendor may also need to install or add additional software or code to allow for debugging or verification activities. It is good practice that security allow for these authorized actions but at the same time monitors them to ensure that they have not been leveraged to attack the application and/or target system. Capturing, forwarding, evaluating and monitoring related activities at the operator site, but also for the suppliers of sensitive digital assets can be supported by forensic readiness preparations and security information and event management.

It may often be necessary that the development defensive computer security architecture and the operations defensive computer security architecture for a system differ widely owing to differences in necessary activities, environments, national considerations (including regulations) and logistical constraints.

III.6. ATTACK PATHWAYS ARE MITIGATED USING SECURITY CONTROLS

In order to mitigate attack pathways, the defensive computer security architecture "should be designed to eliminate or limit the possible routes for cyber-attack (as identified in the threat characterization) that an adversary could exploit to compromise systems performing facility functions", as stated in para. 4.69 of NSS 17-T (Rev. 1) [13].

Therefore, the defensive computer security architecture may reduce or eliminate an attacker's ability to access attack pathways. However, given that attack pathways exist for each of the supplier relationships, consideration is typically given to computer security measures that are informed by the risks associated with the activities performed by the supplier. It is good practice for the procurements associated with significant functions (and risk) to require the establishment of a defensive computer security architecture by the supplier, where applicable, that will allow for necessary activities to occur, but limit their exposure to the adversary.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2] EUROPEAN UNION AGENCY FOR CYBERSECURITY, ENISA Threat Landscape for Supply Chain Attacks, ENISA, Athens (2021). Available online at https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

[3] NUCLEAR ENERGY INSTITUTE, Cyber Security Plan for Nuclear Power Reactors, NEI 08-09 (Rev. 6), NEI, Washington, DC (2010). Available online at https://www.nrc.gov/docs/ML1011/ML101180437.pdf

[4] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity Requirements, IEC 62645:2019, IEC, Geneva (2019).

[5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Security Controls, IEC 63096:2020, IEC, Geneva (2020).

[6] CANADIAN STANDARDS ASSOCIATION GROUP, Cyber Security for Nuclear Facilities, CSA N290.7-21, CSA Group, Toronto (2021).

[7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Cybersecurity — Supplier Relationships — Part 1: Overview and Concepts, ISO/IEC 27036-1:2021, ISO, Geneva (2021).

[8] ENERGY POWER RESEARCH INSTITUTE, Cyber Security in the Supply Chain: Cyber Security Procurement Methodology, Rev. 2, EPRI Technical Report 3002012753, EPRI, Palo Alto, CA (2018).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Facilities, Nuclear Energy Series No. NP-T-3.21, IAEA, Vienna (2016).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

[11] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Security Techniques – Information Security Risk Management, ISO/IEC 27005:2018, ISO, Geneva (2018).

[12] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Part 3: Guidelines for Information and Communication Technology Supply Chain Security, ISO/IEC 27036-3:2013, ISO, Geneva (2013).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021).

[14] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Security Techniques – Information Security Management Systems, ISO/IEC 27001:2013, ISO, Geneva (2013).

[15] NUCLEAR ENERGY INSTITUTE, Addendum 7 to NEI 08-09, Revision 6 Dated December 2018: Evaluating and Documenting Use of Alternative Cyber Security Controls/Countermeasures, NEI, Washington, DC (2018). Available online at https://www.nrc.gov/docs/ML1834/ML18348B211.pdf

[16] GOLLMANN, D., Computer Security, 3rd edn, John Wiley & Sons, Ltd, Chichester, UK (2011). pp 495.

[17] WINDELBERG, M., Objectives for managing cyber supply chain risk, International Journal of Critical Infrastructure Protection **12** (2016) 4–11. Available online at https://www.sciencedirect.com/science/article/pii/S1874548215000785

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[20] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[23] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Security

– Cybersecurity and Privacy Protection – Information Security Controls, ISO/IEC 27002:2022, ISO, Geneva (2022).

[24] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Security Techniques – Information Security for Supplier Relationships – Part 2: Requirements, ISO/IEC 27036-2:2014, ISO, Geneva (2014).

[25] NATIONAL INSTITUTES OF STANDARDS AND TECHNOLOGY, Developing Cyber Resilient Systems: A Systems Security Engineering Approach, NIST Special Publication 800-160 Vol. 2 Revision 1, NIST, Gaithersburg, MD (2021).

[26] EGGERS, S., ROWLAND, M., "Deconstructing the nuclear supply chain cyber-attack surface", Proc. 61st Annual Meeting of the Institute of Nuclear Materials Management (INMM 2020), Baltimore, 12–16 July (2020), Volume 1, 371–380.

[27] MILLER, J., Supply Chain Attack Framework and Attack Patterns, MITRE Technical Report MTR140021, MITRE Corporation, McLean, VA (2013).

[28] EGGERS, S., A novel approach for analyzing the nuclear supply chain cyber-attack surface, Nuclear Engineering and Technology **53** (2021) 879–887. Available online at https://doi.org/10.1016/j.net.2020.08.021

[29] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[30] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, IAEA, Vienna (2019).

[31] CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations, Alert (AA20-352A) (2021). Available online at https://us-cert.cisa.gov/ncas/alerts/aa20-352a

[32] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Risk Management – Guidelines, ISO 31000:2018, ISO, Geneva (2018).

[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).

[34] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Coordinating Safety and Cybersecurity, IEC 62859 Edition 1.1, IEC, Geneva (2019).

[35] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Industrial Communication Networks – Network and System Security – Part 3-3: System Security Requirements and Security Levels, IEC 62443-3-3, IEC, Geneva (2019).

[36] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Security for Industrial Automation and Control Systems – Part 4-1: Secure Product Development Lifecycle Requirements, IEC 62443-4-1, IEC, Geneva (2018).

[37] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, ISO, Geneva (2005). Available online at https://www.commoncriteriaportal.org/cc/

[38] CENTER FOR INTERNET SECURITY, CIS Controls V.7.1, CIS, Albany, (2019). Available online at https://www.cisecurity.org/controls/

[39] ENERGY POWER RESEARCH INSTITUTE, Cyber Security Technical Assessment. Methodology, Risk Informed Exploit Sequence Identification and Mitigation, Rev. 1, EPRI Technical Report 3002012752, EPRI, Palo Alto, CA (2018).

[40] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris (2017).

[41] NATIONAL INSTITUTES OF STANDARDS AND TECHNOLOGY, National Checklist Program. Available online at https://ncp.nist.gov

[42] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, ISO/IEC 27006:2015, ISO, Geneva (2015).

[43] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Security for Industrial Automation and Control Systems – Part 4-2: Technical Security Requirements for IACS Components, IEC 62443-4-3, IEC, Geneva (2019).

[44] UNDERWRITERS LABORATORIES, Standard for Software Cybersecurity for Network – Connectable Products, Part 1: General Requirements, UL 2900-1, UL, Chicago (2017).

[45] DEPARTMENT OF HOMELAND SECURITY, Department of Homeland Security: Cyber Security Procurement Language for Control Systems, DHS, Washington, DC (2009).

[46] SALTZER, J.H., SCHROEDER, M.D., The protection of information in computer systems, Communications of the Association for Computing Machinery **17** (1974). Available online at https://www.cs.virginia.edu/~evans/cs551/saltzer/

[47] LAWSON-JENKINS, K., DE PERALTA, F., "Consideration of cybersecurity risks with the use of emerging technologies", Proc. 61st Annual Meeting of the Institute of Nuclear Materials Management (INMM 2020), Baltimore, 12–16 July (2020), Volume 1, 343–352.

[48] DENNING, D.E., A lattice model of secure information flow, Communications of the Association for Computing Machinery **19** (1976) 236–243. Available online at https://courses.cs.washington.edu/courses/cse590s/02sp/secure-information-flow.pdf

[49] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, General Requirements for the Competence of Testing and Calibration Laboratories, ISO/IEC 17025:2017, ISO, Geneva (2017).

[50] NATIONAL NUCLEAR SECURITY ADMINISTRATION, OFFICE OF RADIOLOGICAL SECURITY, Cybersecurity Procurement Requirements for ORS-Provided Security Systems, ORS, Washington, DC (2018).

[51] DEPARTMENT OF HOMELAND SECURITY, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies – Industrial Control Systems Cyber Emergency Response Team, DHS, Washington, DC (2016). Available online at https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[52] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, National Vulnerability Database: NIST, Gaithersburg, MD. Available online at https://nvd.nist.gov/

[53] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Conformity Assessment – Requirements for the Operation of Various Types of Bodies Performing Inspection, ISO/IEC 17020:2012, ISO, Geneva (2012).

[54] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Security Techniques – Information Security for Supplier Relationships – Part 4: Guidelines for Security of Cloud Services, ISO/IEC 27036-4:2016, ISO, Geneva (2016).

[55] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Security for Industrial Automation and Control Systems Part 2–4: Security Program Requirements for IACS Service Providers, IEC 62443-2-4:2015+AMD1:2017 CSV Consolidated Version, IEC, Geneva (2017).

[56] MICROSOFT CORPORATION. Microsoft Security Bulletin MS17-010 – Critical, Security Update for Microsoft Windows SMB Server (4013389), Version 1.0 (2017). Available online at https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

[57] GREENBERG, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired.com (2018). Available online at https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[58] UNITED STATES NATIONAL SECURITY AGENCY, Storage Device Sanitization and Destruction Manual, NSA/CSS Policy Manual 9–12, NSA, Fort Meade, MD (2017).

[59] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on The Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union No. L 119, Publications Office of the European Union, Luxembourg (2016).

[60] MICROSOFT CORPORATION, Deep Dive into the Solorigate Second-stage Activation: From SUNBURST to TEARDROP and Raindrop (2021). Available online at https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop

[61] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Cloud Computing – Overview and Vocabulary, ISO/IEC 17788:2014, ISO, Geneva (2014).

[62] UNLEASHED, The four main types of purchase orders (2019). Available online at https://www.unleashedsoftware.com/blog/managing-procurement-purchase-orders

[63] INTERNATIONAL TELECOMMUNICATION UNION, Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks – Cloud Computing, ITU-T Y.3500, ITU, Geneva (2014).

[64] ANDERSON, J.P., Information security in a multi-user computer environment, Advances in Computers **12** (1972) 1–36. Available online at https://www.sciencedirect.com/science/article/abs/pii/S0065245808605069

[65] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary, ISO/IEC 27000:2018, ISO, Geneva (2018).

ANNEX I. SUPPLY CHAIN READER'S GUIDE

Table I–1 provides a guide to specific sections of interest in this publication, based on the reader's background and experience.

TABLE I–1. SUPPLY CHAIN READING REFERENCE

Section	Computer Security Specialist	Supply Chain Specialist	Other Readers
Section 2, Supply Chain Management, defines a robust supply chain management approach to understand the complexity of supply chain relationships between customer and supplier including upstream suppliers' supplier through a procurement process; and introduces the four phases of procurement.	X		X
Section 3, Information and Computer Security Essentials for the Supply Chain, provides awareness and understanding of information and computer security concepts. It describes the need to protect sensitive information and critical digital assets and elements of nuclear security through the establishment of procurement computer security requirements within the supply chain.		X	X
Section 4, Supply Chain Attack Surface, introduces SCAS. The SCAS includes the attack vectors (touchpoints) that adversaries can use to compromise stakeholders during supply chain activities. This section explains how a SCAS can be used to identify computer security requirements that protect supply chain activities throughout the entire supply chain.	X	X	X
Section 5, Typical Procurement Process, provides an overview of the procurement process that is used as the basis of this document. This process is based upon four phases: specify, source, use and correct.	X	X	X
Section 6, Specify Stage, is considered the most critical stage and is where computer security requirements are implemented for security processes, procedures, contracts and controls to reduce risk through risk identification, analysis, evaluation and treatment.	X	X	X
Section 7, Source Stage, supports the identification, approvals and acceptance criteria of suppliers including computer security requirements, terms and conditions, risk identification, acceptance and testing.	X	X	X
Section 8, Use Stage, begins at factory acceptance testing and integration, during use, and ends at the decommissioning phase. Elements of supply chain consideration are in continued testing, maintenance and repair and support services including third party support contracts.	X	X	X
Section 9, Correct Stage, focuses on supplier management activities and continued compliance to meet computer security regulations and monitoring of external events including changes and updates to national regulation, operational policies or procedure changes and the evolving threat.	X	X	X
Appendix I, The Nuclear Supply Chain, provides additional information on the supply chain from international standards and guidance.	X		X

Section	Computer Security Specialist	Supply Chain Specialist	Other Readers
Appendix II, Type of Purchases, Products and Services, provides details on the types of purchases (standard, planned, blanket and contract) and their classification (catalogue, simple and complex), which constrain the computer security requirements that can be applied within a particular supply chain.	X		X
Appendix III, Information and Computer Security Concepts, provides an overview of IAEA guidance for defining and managing computer security risk.		X	X

ANNEX II. SUPPLY CHAIN ATTACKS, LOCATIONS AND LINKAGES

Figure II–1 details the points and types of attacks that can be directed against products and services at supply chain locations.

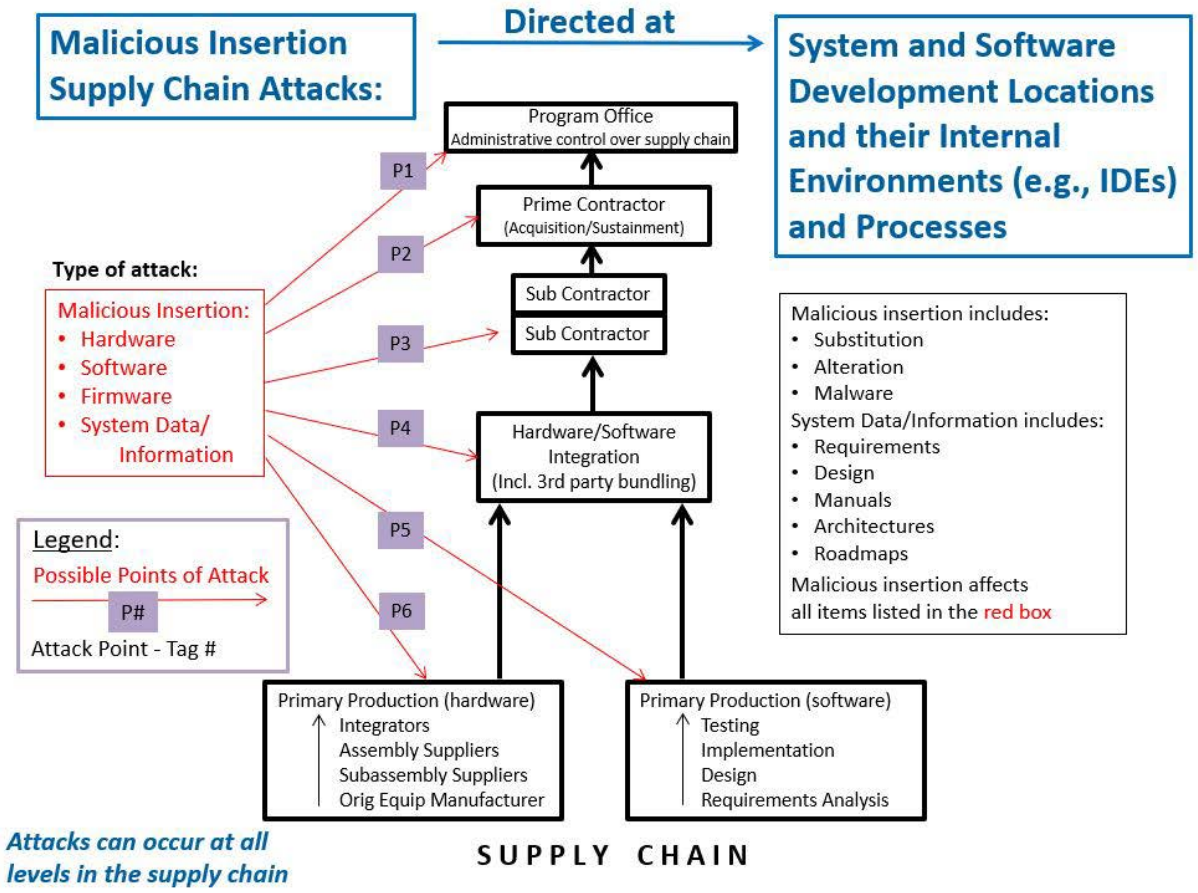

FIG. II–1. Points of attack – supply chain locations figure 1 from Ref. [II–1]. IDE — integrity and data encryption.

Supply chain locations identified in Ref. [II–1] form the basis for the stakeholders and locations detailed in the SCAS (see Section 4). The SCAS consolidates the 41 types of attacks listed in Ref. [II–1] into six basic attack types that also involve the logistical attack in Fig. II–2 below.

The SCAS provides all of the necessary information that is found in Ref. [II–1], with an intuitive dashboard to identify and assess risks. As shown in Fig. II–1, malicious insertion (including substitution, alteration and malware) can occur at any supplier location.

Figure II–2 details the points and types of attacks that can be directed against products, data and remote services over supply chain linkages (either via physical–logistics or ICT communication channels).

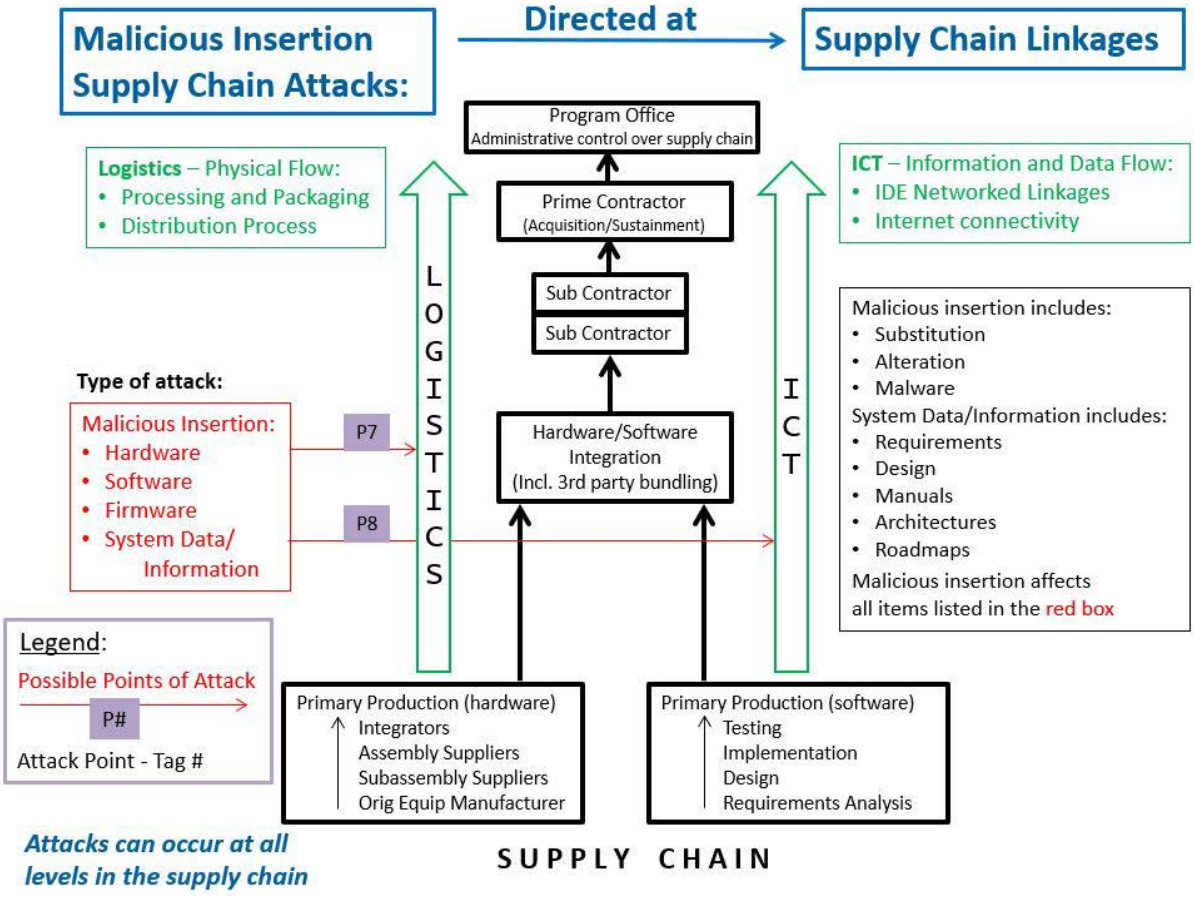

FIG. II–2. Points of attack – supply chain linkages figure 2 from Ref. [II–1].

Risks associated with linkages are fundamentally different than those associated with locations. They can be considered similar to nuclear material or other radioactive material that is in long term storage or in transport. While the material is more exposed during transport, its time in transport is a fraction of the time it will spend in long term storage. The strategy and techniques to secure material in transport or in storage are different. These differences also apply to computer security.

Figure II-1 and II-2 are from Supply Chain Attack Framework and Attack Patterns, MITRE Technical Report MTR140021 with permission from NITRE.

REFERENCES TO ANNEX II

[II–1] MILLER, J., Supply Chain Attack Framework and Attack Patterns, MITRE Technical Report MTR140021, MITRE Corporation, McLean, VA (2013).

ANNEX III. INSURANCE FOR NUCLEAR POWER PLANTS

The nuclear supply chain is a complex global system. It is important for organizations to understand how various contracting parties are affected and treated within and across national legal systems for non-compliance with agreements, non-conformance to good practices and any actual incidents. In addition, other organizations (indirect parties) that are not contracting parties may be affected by contract terms and performance. This could include the organization's insurers as well as the general public, in the event of an incident. All are bounded by States' international treaties and national legislation.

Good practices for computer security in the supply chain include a management commitment to a culture of overall good safety and security. The Convention on the Physical Protection of Nuclear Materials and its Amendment [III–1, III–2] calls on all involved organizations, including licence holders, to establish an effective security culture as well as quality policies and programmes to ensure effective physical protections. To ensure such physical protection in the current dynamic threat environment, it is good practice for computer supply chain security to be well managed with continual attention to the evolving threat environment.

Good computer security risk management is an ongoing process that requires continuous improvement. This could include:

- Planned risk assessment updates;
- Continual improvement to conform to updated industry practices;
- Periodic assessment of security culture and how it affects conformance to policies and procedures;
- Attention to changing legislation for coverage under treaties or statutes and subsequent financial liability and insurance needs increasing;
- Noting that insurance markets are maturing in their approaches to cyber risks and policies, with new coverage opportunities or restrictions;
- Training in good computer security and acquisition or contracting practices across the organization.

The following sections in this annex outline some examples of ways to manage computer security risks and liabilities effectively. These include transferring the risk, reducing the risks via contract language, and ensuring good organizational governance.

III-1. EXAMPLE – TRANSFERRING CYBER RISKS TO INSURERS

Cyber risks are typically considered within the context of overall risks within the nuclear liability regime and insurances. Although owners and operators are always strictly liable for their performance, they can pay premiums to other entities who take on some of the financial risks of performance. Although many types of specialty insurance lines are available, the most common types of commercial insurance are property and liability insurance.

Property insurance covers a licensee's own equipment and business continuity. In addition to standard property coverage (e.g. fire, theft), nuclear property insurance covers the licensee's obligation to stabilize and decontaminate its own site. The acquirer typically decides how much insurance to contract, although a State may require a minimum level as a condition of licensing. The United States of America is the only State which requires facilities to carry property insurance through regulation; 10 CFR 50.54 (Code of Federal Regulation) requires each facility

to procure US $1.06 billion in property insurance as a license requirement for each operational NPP site.[1]

Liability insurance covers third party damages from an incident. This is typically a licensing requirement with a State defining minimum levels of operator financial assurance for liability. Special nuclear liability coverage (e.g. for broader decontamination costs) is required prior to the arrival of nuclear fuel on site. About half of the NPPs worldwide are located in States that are party to international nuclear liability conventions that require certain minimum levels of financial assurance, with operators typically using insurance to demonstrate financial capacity to pay third parties in case of an incident (for details, see chapter 5 of Ref. [III–3]).

In addition to gaining standard coverage from the commercial insurers, who cover the non-nuclear risks, operating organizations obtain insurance from special nuclear insurers for damages caused by the harmful effects of ionizing radiation. The nuclear insurers traditionally have been local entities that enter into pooling arrangements or mutuals.

Nuclear insurance pools are created when domestic insurers form a specialty nuclear insurance entity to provide local insurance to domestic licensees and then enter into a pooling arrangement internationally. Insurance companies from around the world have joined forces by forming nuclear insurance pools to share the large risks. Furthermore, pools are formed because the consequences of the hazards concerned are unknown, the number of insured risks is low, and the development of specific know-how at individual insurance companies to evaluate the risks would be too costly. In such cases, it makes sense to pool the knowledge needed to estimate the insurance exposure and share the exposure. Nuclear insurance pools have been established in practically all States that operate NPPs. The financial capacity of nuclear insurance pools throughout the world supplements the statutory liability and helps to spread the risk. Such principles have introduced a total transparency of insurance exposure to nuclear risk and enabled individual insurance companies to cover operators with the highest possible financial commitment. Pools reinsure each other, providing a global nuclear pooling capacity.

Another insurance system is known as the mutual. Some owners or operators of nuclear facilities have established mutual insurance. Mutuals are captive to the acquirers who have ownership stake in the mutual, which encourages social responsibility. Examples of mutual insurance are the European Mutual Association for Nuclear Insurance (EMANI) and Nuclear Electric Insurance Limited (NEIL) in property and business continuity insurance, and European Liability Insurance for the Nuclear Industry (ELINI) and American Nuclear Insurance (ANI) in liability insurance.

New commercial capacity, including via new mechanisms such as insurance linked securities, looks to expand the market. Most insurance underwriters of all types subscribe to reinsurance from major commercial reinsurers to further share risks.

III-2. EXAMPLE – MANAGING CYBER RISKS WITHIN THE CONTRACTING PROCESS

Owners and operators may be able to transfer some risks through contracting and receive some recompense from those deemed accountable for incidents.

[1] NUCLEAR REGULATORY COMMISSION, Conditions of Licenses, 10 CFR 50.54, US Government Printing Office, Washington, DC (1983).

Many parties may be responsible for an incident related to computer or technology systems, explicitly or negligently, for example:

— Manufacturers and suppliers of cyber systems and components, for failure of systems or components to operate as contracted and/or to prevent failure or attack;
— Design authorities for flaw in integration of technology into the design;
— Construction consortia for flaw in installation of technology.

Operators and their employees may also be directly responsible for flawed operation or maintenance of computer or technology systems, with potential also for employee or third parties causing deliberate or reckless damage. It is good practice for all computer security practices of engaged parties to be addressed.

Operators have rights of recourse against a company or an individual acting or omitting to act with intent to cause damage and where such recourse is expressly provided by contract, which is why contracting is so critical. Suppliers, vendors and other third party contractors have potential liabilities for non-nuclear claims and for liability from radiation releases in some cases, such as in States that are not parties to the nuclear liability regime. These can be allocated by contract.[2]

State legal and regulatory requirements may dictate some contract elements and may affect technology suppliers as follows:

— Information security: requirement to maintain the security of sensitive nuclear information, software and equipment; computer security requirements for secure communications including with regulators and safeguard inspectors.
— Anti-terrorism and official secrets: prohibition on disclosure of information which could prejudice national security, prohibition on making records or communicating information for purposes prejudicial to the safety or interests of the State (or knowingly allowing others to do so); information security requirements to classify documents in accordance with the national regime.
— Import and export controls: compliance declaration and/or licences required for trade in technology, compliance with embargoes on trade with specific States and persons.
— Physical security, including of technology: requirement for transport of equipment by approved carriers in accordance with approved nuclear security transport plans; appropriate access authorizations.

It is appropriate for procurement managers to be aware of all the legal, regulatory, and information and computer security requirements as they manage risks across the procurement process life cycle.

[2] Some States such as India will also allow owners/operators limited recourse to suppliers for radiation releases (subject to some limitations).

REFERENCES TO ANNEX III

[III–1] The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1, IAEA, Vienna (1980).

[III–2] Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1/Mod. 1 (Corrected), IAEA, Vienna (2021).

[III–3] OECD NUCLEAR ENERGY AGENCY, Principles and Practice of International Nuclear Law, NEA No. 7599, OECD, Paris (2022).

ANNEX IV. ELECTRIC POWER RESEARCH INSTITUTE COMPUTER SECURITY PROCUREMENT METHODOLOGY

The supply chain represents a significant cyber-attack pathway for digital assets and systems at both existing and new nuclear generating stations. The buyers[1] and suppliers of digital components are faced with several key issues owing to threats posed by this pathway such as software and hardware provenance, regulatory uncertainty and the lack of visibility into lower tier suppliers and processes. As a result, the Electric Power Research Institute (EPRI) researched this issue while maintaining awareness of the computer security risks associated with the supply chain and incorporating new research and guidance surrounding digital engineering processes. The EPRI cyber security procurement methodology [IV–1] was developed from this research. The methodology described in Ref. [IV–1] presents a model establishing a common understanding among all parties within the supply chain and integrates the EPRI cyber security technical assessment methodology [IV–2] to assist in the development of computer security requirements, which can support the overall digital design process as described in the EPRI digital engineering guide [IV-3].

The EPRI supply chain model illustrated in Fig. IV–1 uses a series of segments and transitions for describing computer security across the supply chain. As the digital asset being procured, known as the target asset, traverses each segment and transition, its attack surface is analysed, and the computer security requirements needed to ensure its security are well defined. The use of the technical assessment methodology provides the technical approach for determining the attack surface and for identifying the appropriate mitigations. The model also accounts for the differences between the computer security features and functions provided by the target asset and maintaining the integrity of the asset when traversing the segments and transitions. The digital assets used in a supplier's development environment, known as development assets, present a pathway that an adversary can leverage to gain unauthorized access to the target asset. Since the expectation is that the custodian during a specific segment is responsible for the integrity of the target asset, the methodology provides an approach for identifying the computer security requirements that ensures a secured development, integration and delivery environment while the target asset is being developed.

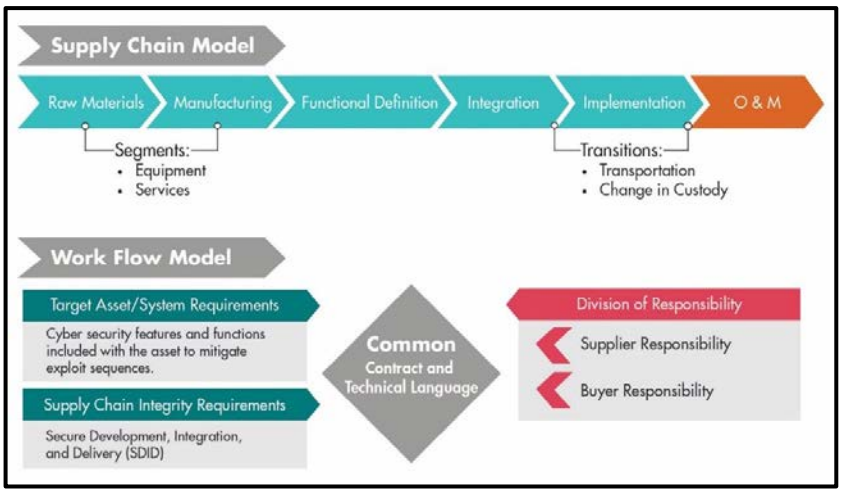

FIG. IV–1. EPRI supply chain model.

[1] Buyer is equivalent to acquirer in this publication.

The methodology recognizes that it is good practice to consider a graded approach to imposing computer security due to the range of procurement types presented by the supply chain. Three procurement types are presented in Fig. IV–2: catalogue procurement, engineered component procurement, and custom or integrated procurement. The buyer typically recognizes which type of procurement is to be pursued in order to ensure that a supplier responds to a computer security specification. For example, when obtaining a mass-produced commodity item, such as a network switch, imposing stringent integrity specifications upon a supplier's development environment would more than likely result in an exception. By identifying this prior to submittal, the buyer can identify which computer security gaps will likely result and take the appropriate mitigating actions to establish the integrity of the target asset upon its receipt.

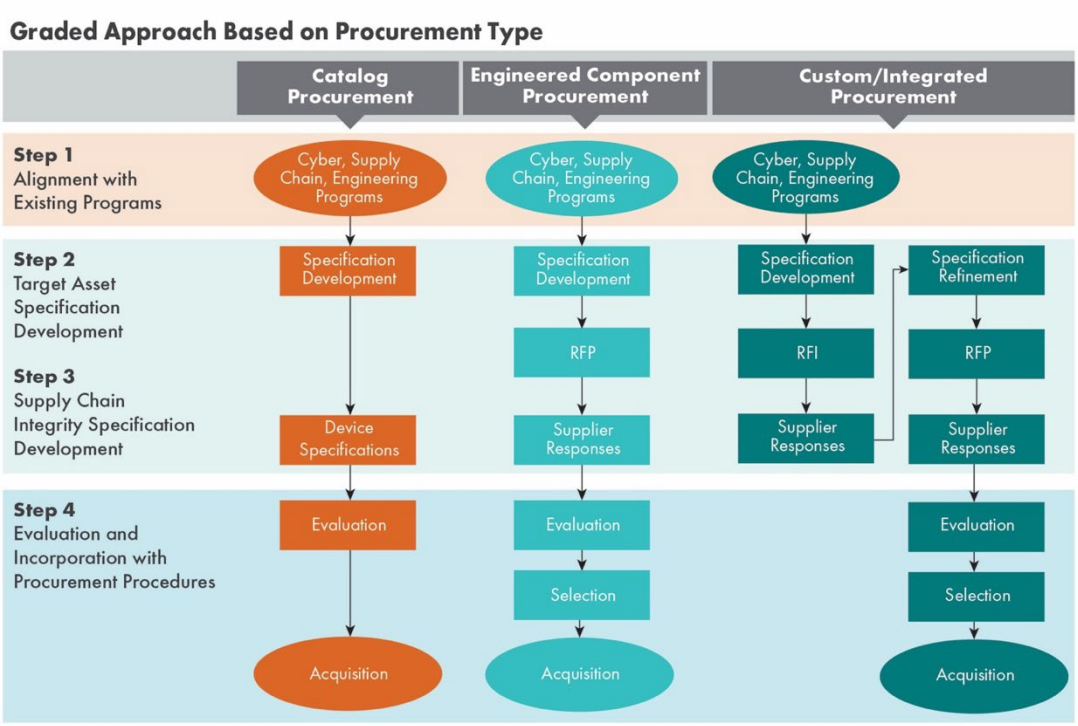

FIG. IV–2. Graded approach based on procurement type.

A significant issue for computer security that has commonly presented is risk transference deadlock. This typically occurs due to how the specification are written, implying that the supplier will assume most of the responsibility for computer security risk. The result is either the supplier passing on the opportunity or significant negotiations that result in additional costs to the target asset. The methodology guides the users in developing specification language that provides for computer security capabilities that a supplier can implement, allowing the buyer to determine how to utilize the capabilities at their station.

Integrated throughout the procurement methodology is the use of the EPRI technical assessment methodology [IV–2]. A risk informed engineering process, the technical assessment methodology provides an efficient and repeatable approach to characterize the attack surface of a target asset and to determine which computer security features and functions are to be incorporated within the asset. This assists with determining the division of responsibility as shown in Fig. IV–3. The use of this methodology also allows the buyer to identify what control methods are needed external of the asset to achieve a specific computer security risk acceptance level.

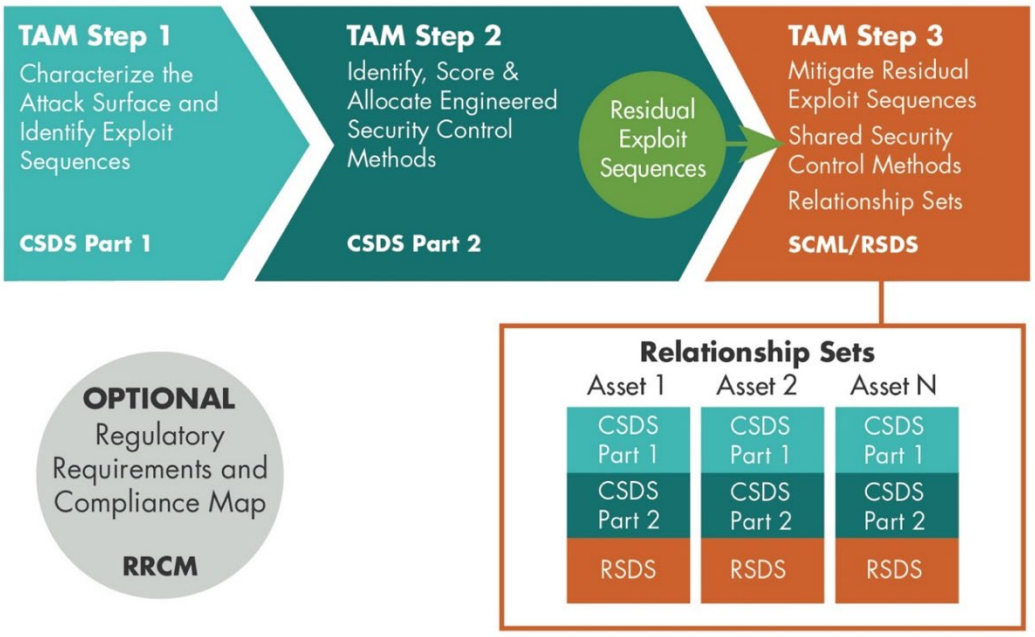

FIG. IV–3. EPRI computer security technical assessment methodology overview.

By using the technical assessment methodology, a buyer is able to understand the target assets, analyse the actual weaknesses of the target assets and identify the control methods that can mitigate the weaknesses. This is achieved by identifying the attack surface of the device and understanding its relationships to surrounding systems and components. The buyer can accomplish this by analysing the expected installed configuration and data flow of the target asset. Using this information, the attack pathways are identified along with the mechanisms used to achieve specific adversarial goals along those pathways, which are known as exploit sequences. Each exploit sequence is assigned a risk based target level using an analysis from a separate hazards and consequence assessment methodology. In addition, the features, functions and capabilities that can be leveraged as computer security control methods are identified and evaluated for security effectiveness. These methods are then available to be allocated to the individual exploit sequence where appropriate until the target level is met. However, at this point, it is expected that this would not be achieved resulting in a residual exploit sequence. This allows the buyer to identify security control methods that are available from other systems and components based upon their relationship to the target asset. The end result is that the buyer has identified the computer security capabilities of the target asset, developed the appropriate computer security requirements for the specification, and determined the additional mitigation techniques that will be required to achieve a computer security risk acceptance for the station.

Suppliers can also use the technical assessment methodology to understand the attack surface of their development assets in preparation of becoming the custodian of a target asset for their given supply chain segment. The goal here is to ensure the integrity of their development environment. This is achieved in fully understanding the data flows for each development asset to determine the exploit sequences that an adversary can use. The supplier can then identify, score and allocate security control methods to provide mitigation until their risk acceptance level is achieved. The results of this analysis can be provided when a buyer requests information prior to acquisition or can be used as evidence to support the results of an audit.

The EPRI cyber security procurement methodology [IV–1] provides a consistent and common model for the supply chain that both buyers and suppliers can understand. It is optimized by

leveraging the engineering analysis with the procurement process that results in concise and appropriate specification language for computer security requirements with a clear division of responsibility among the parties. Overall, supply chain integrity is maintained owing to its consistent technical approach, allowing all affected parties in the supply chain to have a common technical foundation.

REFERENCES TO ANNEX IV

[IV–1] ENERGY POWER RESEARCH INSTITUTE, Cyber Security in the Supply Chain: Cyber Security Procurement Methodology, Rev. 2, EPRI Technical Report 3002012753, EPRI, Palo Alto, CA (2018).

[IV–2] ENERGY POWER RESEARCH INSTITUTE, Cyber Security Technical Assessment. Methodology, Risk Informed Exploit Sequence Identification and Mitigation, Rev. 1, EPRI Technical Report 3002012752, EPRI, Palo Alto, CA (2018).

[IV–3] ENERGY POWER RESEARCH INSTITUTE, Digital Engineering Guide: Decision Making Using Systems Engineering, EPRI Technical Report 3002011816, EPRI, Palo Alto, CA (2021).

ANNEX V. PRODUCT CERTIFICATIONS

Certification is a third party attestation that is performed against a set of requirements based on a recognized standard. Certifications are available in the computer security domain and can assist the procurement effort for an acquirer. For example, the following are applicable to devices:

- A certified device will have built-in or native security features that can facilitate implementation of security solutions.
- It is easier to specify that a device has a particular certification, rather than to specify the individual computer security requirements required of a device.
- A certified device will have already undergone validation testing of its security features, which could reduce the testing effort during factory or site acceptance testing.
- A certified device will be characterized as having a particular level of security achievement, which could facilitate assessment of suitability for particular security applications.
- Owing to the repeatable and traceable certification steps, a certified device is inherently more secure than an equivalent product that has not been subjected to certification steps.
- A vendor that has undergone a certification effort is generally a vendor that may have stronger security maturity compared to those vendors who have not. A vendor with stronger security maturity can be a more effective partner in developing security solutions.

The following are benefits of certifying products from a supplier's perspective:

- It is an exercise that can be performed on one device for the benefit of a product line of identical devices.
- A certification is a formal recognition of quality assurance efforts that are otherwise difficult to quantify.

The availability of certification programmes is contributing to the movement by manufacturers to incorporate computer security defence mechanisms in their products.

Certification can also apply to individuals as an attestation of an individual's knowledge, skills and capabilities in computer security. Certifications can also apply to an organization and/or software development processes within an organization as a measure of the organization's computer security maturity.

V-1. GOOD PRACTICES

Evidence of compliance by an independent and accredited authority to recognized computer security standards is typically used to provide assurance that a level of achievement has been attained in meeting a prescribed set of computer security requirements.

Certifications are typically used as an evidentiary mechanism of compliance to procurement specifications when procuring goods or services.

It is good practice for organizations performing the certification to be accredited to perform such assessments. A certification is typically from a reputable accrediting organization.

Third party certification and approvals usually come with an assessment report. It is good practice for the effectiveness of the methods and tools used for the certification to be justified. The assessment report is obtained and reviewed to understand the security capabilities of the item and obligations with regard to mitigations and processes necessary to be addressed by the asset owner.

Certifications that are more 'closed' and lacking transparency with regard to the tests performed warrant greater scrutiny as to the extent they can be accredited, if at all.

Some certification schemes include a required surveillance audit where the independent and accredited authority re-audits periodically.

It is good practice for vendors to be able to demonstrate that a certification is current and applies to the version of the product being supplied. For example, does the actual product supplied meet the certification specifications in terms of version of hardware and/or firmware for all components or modules supplied, and is the vendor guaranteeing the version shipped fully meets the original certification? Has the product design been 'frozen' by the vendor or has the design changed since the certification was issued? What is the impact of the change?

In the context of development processes, certification provides evidence that a vendor's product development site incorporates security considerations throughout the development life cycle including the maintenance and support phases. It may be the case that a certification only applies to a particular part of an organization; the scope of a certification is typically checked to confirm that it is applicable to the item of interest.

In the context of devices and systems, a successful certification does not necessarily mean that the device is free from vulnerabilities. A certification contributes confidence that the item is robust against network attacks and free from known vulnerabilities. Evidence of certification is a management control that contributes to the arguments used to demonstrate that there is adequate security for the level of risk to the particular application where the device or service is being deployed.

Cyber security certifications may have an expiry date, which is a reflection that new vulnerabilities can be discovered and apply to a previously certified item. Certifications that include an audit of the security development life cycle will assess a vendor's response to the discovery of new vulnerabilities after the initial certification is complete.

Devices or systems having safety related certifications will have engineering processes and features that may be leveraged as computer security control methods. For example, higher level safety integrity level certifications require robust software development practices that may also be credited towards meeting the computer security requirements for a secure development environment.

Cyber security certification programmes of devices and systems generally involve three steps:

(1) An audit of the development process;
(2) Cyber security stress testing to find vulnerabilities;
(3) The analysis and testing of security features and capabilities of the product to determine security level achieved.

Development process audits review the development life cycle from the specification of computer security requirements, design, coding, different phases of testing through support and

maintenance activities. An assessment is conducted to determine to what extent security measures are employed in each life cycle phase.

Cyber security stress tests include penetration testing, fuzz testing, malformed packet testing and storm testing. The analysis and testing of a product's security features are a review and validation of the security controls available and a determination of the security level achieved.

V-2. EXAMPLE – IEC 63096

Suppliers and integrators that specifically target the nuclear domain could select and apply the security controls of IEC 63096 [V–1] based on a risk informed approach. Similar to the dedicated software development (i.e. according to IEC 60880 [V–2]), the suppliers and integrators could also perform security tests to verify and validate the effectiveness of the security controls selected and documented according to IEC 63096 [V–1]. When meeting computer security requirements, coverage of security objectives, appropriate selection and configuration and use of state-of-the art security controls can be independently verified by a certified testing organization (i.e. certified according to ISO/IEC 17025 [V–3]).

The certified independent testing organization performs inspections according to ISO/IEC 17020 [IV–4]. For example, as part of the inspections, the supplier submitting a product or platform component for certification may be requested to provide additional documentation or to extend the submitted security test suite, to provide additional test result details or to consider additional use cases that are within the certification scope.

Additionally, to the comprehensive security tests developed and maintained by the supplier that applied for certification, the certified independent testing organization may perform additional tests by their own certified security experts, depending on the specifically addressed topics (e.g. network security, source code level security).

Beyond the security assessments of components that were specifically developed for use in the nuclear domain, the supplier and the certified independent testing organization may include the security testing of comprehensive system hardening and secure configuration of COTS components (e.g. an operating system running on a gateway).

The security certification scope may include specific configurations (similar to a demilitarized firewall) that can be implemented as security defence in depth measures with the products and platform components.

As a result of the ISO/IEC 17020 [V–4] conform inspection, the ISO/IEC 17025 [V–3] certified testing organization may issue appropriate certificates.

Each issued certificate lists the input documents of the product; platform component or representative system; the supplier provided security test documentation with test results and a reference to the approach and complementing security tests performed by the certified independent testing organization.

The independent testing organization's test report accompanying the certificate describes the overall approach; all input documents; all considered standards; justification with regard to the state-of-the art; and security testing methodologies and tools that were used.

Typically, the security test certificates are forwarded to the plant integrator and plant owner. The security test certificates clearly indicate the maximum security capability degree (e.g.

security degree SD2) that can be achieved by the respective product without additional compensating measures.

The test report accompanying the certificates is usually available only to the supplier and on request to regulatory bodies in charge of inspecting the NPPs.

This approach is expected to be comprehensive and effective, as IEC 63096 [V–1] is specifically targeted for the nuclear domain and explicitly recommends security controls for the security degrees S1 (highest), S2, S3 and baseline requirements. IEC 63096 [V–1] also provides guidance on the security controls that could be applied during the development phase of products and platforms for the nuclear domain, which can be forwarded to suppliers and sub-suppliers. Beyond meeting the security guidance for product and platform development, the independent testing organization typically verifies whether security features that are needed later during the engineering and integration phase and during the plant operation and maintenance phase have been implemented by the products submitted for certification.

A certification based on IEC 63096 [V–1] will implicitly consider IEC 62645 [V–5] as a top level nuclear IEC security standard. However, the need for certification or demonstration of compliance with IEC 63096 [V–1] for the systems under consideration may be decided on the basis of the intended deployment of sensitive digital assets (i.e. S1, S2 and S3 but not for baseline requirements).

V-3. EXAMPLE – COMMON CRITERIA

Common Criteria is based on ISO/IEC 15408 [V–6] and is used to specify and evaluate the security properties of IT products. It defines a framework for the oversight of evaluations, syntax for specifying the computer security requirements to be met in a particular device and a methodology for evaluating those computer security requirements. It is designed to ensure that IT products achieve an agreed standard for security deployment by government agencies and critical infrastructure, and is often specified as a pre-requisite to procurement.

Common Criteria provides an extensive catalogue of security functions to support the specification of functional specifications. It also provides an extensive catalogue of assurance requirements so that, depending on the application in which the device is being deployed, the user can have flexibility in choosing the degree of assurance rigour required (e.g. it may only be warranted to check a device for vulnerabilities as opposed to also auditing the development process). Using the Common Criteria framework, a vendor can have a product certified by an independent body to an EAL ranging from EAL1 (the least stringent) to EAL7 (the most stringent). The increasing grade of levels reflects the increasing rigour of assurance requirement. Alternatively, a custom set of assurance components can be specified.

While Common Criteria is currently an IT standard, the global infrastructure is in place in the form of technical community groups to support discussion with regard to the application to industrial devices and networks. Such discussions among relevant entities are necessary in order to identify the desired security features of products used in this industrial environment, and how they are typically tested.

Lessons learned include[1]:

— When evaluating network devices, significant attention is paid to the management plan of the device.
— There is great value in having technical community groups, such as a nuclear industrial control system community group, developing protection profiles – to ensure products are developed to consistently high standards and that reasonable, comparable, reproducible and cost-effective evaluation results can be achieved. In this way, technical community groups can influence the quality of products available on the market.
— Threat intelligence could be shared by organizations participating within a trust community in order to leverage the experience others have acquired defending against attacks in their own networks, which might influence procurement decisions.

REFERENCES TO ANNEX V

[V–1] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Security Controls, IEC 63096:2020, IEC, Geneva (2020).

[V–2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions, IEC 60880:2006, IEC, Geneva (2006).

[V–3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, General Requirements for the Competence of Testing and Calibration Laboratories, ISO/IEC 17025:2017, ISO, Geneva (2017).

[V–4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Conformity Assessment – Requirements for the Operation of Various Types of Bodies Performing Inspection, ISO/IEC 17020:2012, ISO, Geneva (2012).

[V–5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity Requirements, IEC 62645:2019, IEC, Geneva (2019).

[V–6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, ISO, Geneva (2005). https://www.commoncriteria portal.org/cc/

[1] Lachlan Turner, Lightship Security, from presentation made at IAEA Technical Meeting on Reducing Cyber Risks in the Supply Chain, Vienna, Austria, 25–29 June 2018.

ANNEX VI. WIRELESS AND INTERNET TECHNOLOGIES

Wired and wireless data communication technologies have historically been found to be susceptible to cyber-attacks due to weaknesses in their design and implementation. Industry has addressed through the improvements in the design of security features, and over time, less secure technologies are replaced with more secure ones.

As systems with improved functionality, performance and security are developed, national authorities may reuse or re-assignment of wireless frequency spectrum to allow for their adoption. For example, in 2008, the government of the United States of America auctioned the 700 MHz band, previously used by analogue television broadcasts, to allow for the implementation of 4G long term evolution cellular wireless communications. Many States and mobile carriers have phased out their 2G general packet radio service cellular communications which could lead to interruption of service if suppliers and acquirers are unable to support newer technologies.

It is increasingly important to note that the security of cellular communications has been significantly improved with migrations to newer generations.

Cryptographic protocols that secure sensitive internet communications (e.g. online banking) and implementations of the current version of transport layer security (i.e. TLS v.1.3) conform to request for comment (RFC) 8446 [VI–2]. This RFC made RFCs 5077 (session resumption without server-side state), 5246 (TLS v.1.2), and 6961 (multiple certificate status request extension) obsolete and updated RFCs 5705 (keying material exporters for TLS) and 6066 (TLS extensions: extension definitions).

The updates in RFC 8446 [VI–2] include:

— Deprecation of symmetric algorithms that are not authenticated encryption and associated data algorithms.
— Removal of all static Rivest, Shamir, and Adelman (RSA) and Diffie-Hellman cipher suites.
— Redesign of key derivation functions.
— Reduction in the number for round trips required to set up a secure channel. This includes the encryption of all handshake messages after the ‘ServerHello’ message.
— Support for only three basic key exchange modes: Diffie Hellman exchange (either finite fields or elliptic curves); pre-shared key only or pre-shared key with Diffie Hellman exchange.
— Removal of compression.

The rationale for all of these changes to TLS were the disclosure or publication of attacks that could be launched against implementations of TLS v.1.2. These attacks included [VI–3]:

— Padding oracle on downgraded legacy encryption (POODLE, CVE-2014-3566 [VI–4]), which is based on a man-in-the-middle attack that is able to impersonate the server until the client agrees to downgrade the connection to secure socket layer (SSL) v.3.0. The vulnerability in some OpenSSL versions uses non-deterministic cipher block chain padding, which allows the attacker to obtain cleartext data via altering padding and observing the server response.

— Compression ratio info-leak made easy (CRIME, CVE-2012-4929 [VI–4]), which results from encryption compressed data without properly obfuscating the length of the unencrypted data. This may allow for the man-in-the-middle attacker to obtain plaintext HTTP headers by observing length differences during a series of guesses. The attacker could reconstruct sensitive items such as cookie values using the feedback they get from the server.

An important attribute of the above is the scoring of CVE-2014-3566 [VI–4] and CVE-2012-4929 [VI–4] under the common vulnerability scoring system (CVSS) v.2.0 are 'medium' (i.e. 4.3 out of 10) and 'low' (i.e. 2.6 out of 10), respectively. These and other attacks resulted in a significant revision of TLS and the obsolescence of older versions.

However, at the time of publication, the adoption of the newest secure implementation of TLS (v.1.3) is lagging. Figure VI–1 illustrates the support for internet cryptographic protocols.

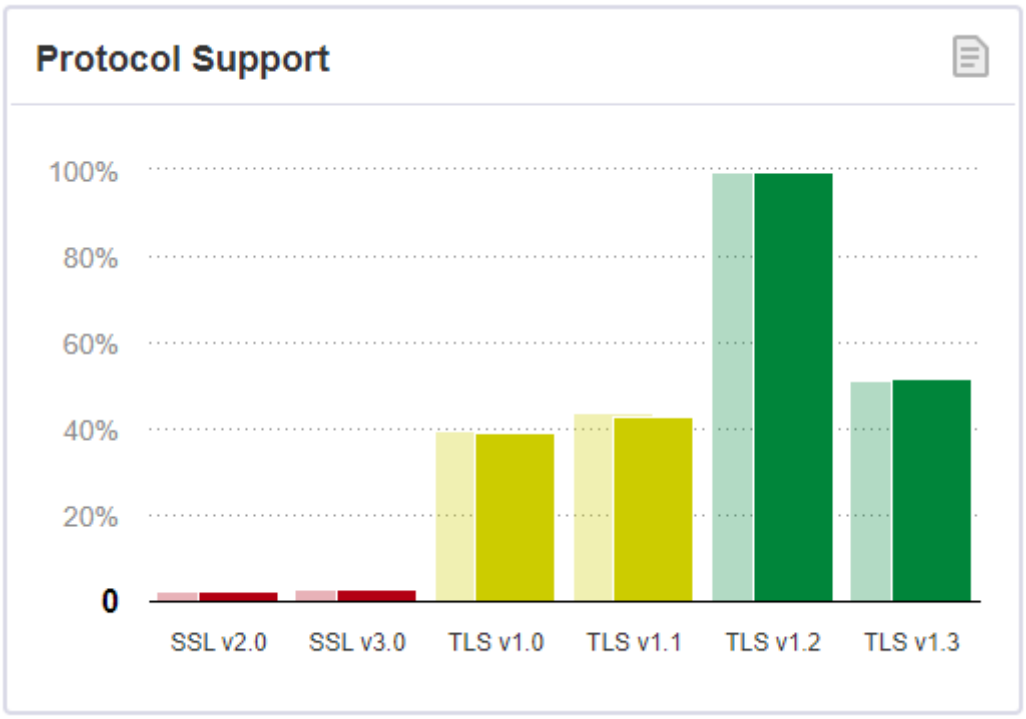

FIG. VI–1. Support for internet cryptographic protocols (January 2022) [VI–5].

Wireless encryption standards change frequently and generally follow technology generations. 3G networks used A5/1 and A5/2 encryption algorithms, with A5/2 withdrawal taking four years for all GSM (UMTS) acquirers to fix their networks [VI–6]. Current 3G algorithm is KASUMI (i.e. A5/3); however, this may be vulnerable to related key attacks [VI–7]. 4G (LTMS) adopted the SNOW 3G algorithm; however, there has been some indication that it also may be vulnerable to related key attacks.

REFERENCES TO ANNEX VI

[VI–1] 3G4G WIRELESS RESOURCE CENTRE, Security in Mobile Cellular Networks, https://www.3g4g.co.uk

[VI–2] INTERNET ENGINEERING TASK FORCE, The Transport Layer Security (TLS) Protocol Version 1.3 (2018), https://datatracker.ietf.org/doc/html/rfc8446

[VI–3] ACUNETIX, TLS Security 6: Examples of TLS Vulnerabilities and Attacks (2019), https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/

[VI–4] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, National Vulnerability Database: CVE-2014-3566, CVE-2012-4929, NIST, Gaithersburg, MD (2008). https://nvd.nist.gov/vuln/search

[VI–5] QUALYS, SSL Pulse (2021), https://www.ssllabs.com/ssl-pulse/

[VI–6] OPEN SOURCE MOBILE COMMUNICATIONS, Withdrawal of A5/2 Algorithm Support, https://osmocom.org/projects/security/wiki/a52_withdrawal/

[VI–7] DUNKELMAN, O., KELLER, N., SHAMIR, A., A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony, International Association for Cryptologic Research, Berkeley (2010).

ANNEX VII. SAMPLE CONTRACT TERMS AND CONDITIONS

Supply chain relationships for procurement of products or services are managed by contracts that include terms and conditions that should be met to maintain and address computer security risks. Table VII-1 provides sample contractual terms and conditions.

TABLE VII–1. SAMPLE CONTRACT TERMS AND CONDITIONS

Contract Terms	Related Considerations
Prevention Responsibilities	
Prioritize confidentiality and performance certifications, include limited access to hardware, systems and data, e.g. in the plant solely to perform service, 'need to know' personnel.	Conduct due diligence via site visits to supplier, review supplier policies and procedures, request information on prior incidents, develop a security questionnaire for potential supplier to complete, check all licenses and certifications.
Include clauses which require disclosure and pre-approval of subcontractors or suppliers, with prime contractor responsible for the performance of the sub-contractor, including its compliance with authorities' contractual requirements. Include in contract documentation the maintenance of any mandatory accreditations or equivalent alternative certification meeting the same contractual requirements for and scope of accreditation.	Consider compromise of computer hardware and software at the vendor, while in storage, in transit and at installation. Perform similar due diligence on outsourced functions and sub-contractors and/or seek certifications and/or written assurances from prime contractor.
Data protection, require compliance with customer policies, use of secure databases and encryption, no data sent offshore for access or storage without customer consent.	Comply with all applicable laws and regulations, including for transmission of encrypted data which is limited in some States.
Specify background checks and export controls, such as criminal background checks and identity verification, representation and warranties (certification) to not involving a non-State entity or person to be involved with the project – with quarterly certifications.	Background checks most important when supplier personnel are dedicated to the customer account, are performing on customer premises, and/or have access to sensitive information. Some States limit or prohibit certain background checks or screening; if so, require a representation that no personnel have been convicted of a felony (or local equivalent), crime of dishonesty or fraud.
Disaster Recovery and Business Continuity Plans (DR/BCP)	

Contract Terms	Related Considerations
For cloud–SaaS[1] offerings: have institutional and DR/BCP in place. For managed services, a tailored plan to align with customer-specific contractual requirements. Require customer approval for changes to DR/BCP. Establish service level or performance standards, e.g. recovery time objective or recovery point objective. Require suppliers to conduct annual testing and reporting, with customer right to participate.	Conduct due diligence, as above, and consider geographic diversity of facilities, geo-political climate, personnel and information access.
Audit and Incident Reporting	
Include a comprehensive audit and reporting regime in the contract arrangements, including customer independent audit rights. Seek no-notice audit rights. Include key performance indicators to measure performance and hold suppliers accountable, including penalty clauses for poor levels of performance or compliance. For cloud–SaaS, require annual security audits (all systems) and notification of 'security incidents' impacting the customer. For managed services, require additional independent customer audit rights including of provider systems.	Suppliers are sensitive to (and protective of) access to systems. Depending on the type of service and the system or platform, suppliers may segregate auditable versus non-auditable systems. Suppliers typically require non-disclosure agreements or confidentiality agreements with third party auditors.
Seek additional protections, such as: Pursue audits in compliance with standards, e.g. Statement on Standards for Attestation Engagement (SSAE) No. 16 [VII–1]. Ask for reporting on "all" security incidents" (not limited to incidents	SSAE 16 can be expensive – cost is negotiable. At customer's cost. Shared cost up to $X. At supplier's cost.

[1] SaaS refers to software as a service, a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.

Contract Terms	Related Considerations
directly impacting customer operations or data). Seek notification (and potentially approval) of remediation.	Notification of endemic issues or vulnerabilities is important even if no immediate impact to customer.
Cyber Indemnities (in favour of the acquirer)[2]	
For third party claims arising out of breaches of supplier's obligation under confidentiality and data protection provisions, the supplier could pay the cost of remediation, restoration or recovery of data and any government fines or penalties. Seek the acquirers' right to [control] [participate in] any formal proceedings. Require acquirer consent for any settlement.	Indemnities are heavily negotiated clauses as they cover which party will have to bear the cost of defending a legal claim typically for professional errors by the supplier, contractor or its subcontractors. These are contested by cloud providers. Suppliers seek carve outs, e.g. for data restoration, notifications, call centre operations (e.g. if required by regulators, states). Suppliers also seek monetary caps.
Liability Limits and Exclusions	
Define liabilities for which the supplier is responsible. Define as 'direct' damages the costs the acquirer wants covered.	Suppliers may accept direct damages only, whereas the acquirer prefers to include consequential or incidental damages, such as cost of remediation, recovery, restoration or notification. Defining what is 'direct' avoids judicial interpretation.
Negotiate the supplier's monetary exposure. Seek a 'no cap' or large 'super-cap' equal to a high multiple of the supplier's fees or as a set monetary amount.	Suppliers want these limited and capped at a measure of supplier fees, e.g. 12 months. Contracts have a wide range of monetary 'super-cap' measures (low 2X to as high as 5X annual fees or flat multi-million $ amount).
Agreement on Post-Project Arrangements	
Consider computer security requirements and the period of performance over the life cycle of the system. Make sure the system being procured is secure and future proofed – technology changes rapidly. Ongoing support – hardware and software. Ongoing vulnerability notifications.	Computer hardware and software change faster than acquirers may be able to accommodate changes. It is possible that providers are not providing updates to some older systems. Good documentation helps system administrators and new service providers

[2] Note that if the operator contracted with a supplier for indemnification of damages, while the operator will still be liable for damages, the operator might be able to reclaim limited damages from the supplier.

Contract Terms	Related Considerations
Require project and programme documentation, including detailed programming updates.	adapt, update or replace appropriately the older systems.
Plan for inadequate project or contract close-down procedures, including for the return or destruction of classified information or assets and for ending access to acquirer's systems.	

VII-1. ADDITIONAL CONTRACT CONSIDERATIONS

A new element that has entered contracting with certain suppliers in the United States of America is the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act, enacted in 2002, which eliminates or minimizes tort liability for sellers of certain US Department of Homeland Security-approved 'technologies' if lawsuits arise after a (physical or cyber) attack. A SAFETY Act designation can be applied to services, products or policies, including self-deployed programmes. The designation allows for dismissal of claims against acquirers using related SAFETY Act-designated systems. Contracts can call for suppliers to certify that they have obtained or will seek to obtain SAFETY Act certifications or designations. Tying the SAFETY Act to cyber insurance can result in reduced premiums. Other States might pursue a similar approach of providing liability limitations to those using approved good practices.

Additional guidance on contracting in this area is available from the IAEA [VII–2] and from other entities. The United Kingdom's Energy Networks Association has guidance, which also notes some of the challenges, such as that IT standards are not necessarily appropriate or sufficient for the operational environment and that industrial control system standards are evolving, making any standards hard to apply to suppliers [VII–3]. Cybersecurity controls catalogue could also be a reference for computer security controls that could be applied to instrumentation and control systems at nuclear power plants [VII-4]. Compliance with the International Electrotechnical Commission standard on industrial control systems development life cycle for nuclear power plants may be required of full-service providers as defined in IEC 62443 [VII–5]. Some high-level guidance is available from the US Department of Energy [VII–6], the US Department of Commerce National Institute of Standards and Technology [VII–7], and the US Department of Homeland Security [VII–8]. The North American Electric Reliability Corporation addresses supply chain standards [VII–9].

REFERENCES TO ANNEX VII

[VII–1] SSAE16, An Internet Resource Fully Dedicated to the SSAE No. 16 Standard and Service Organization Reporting. Available online at http://ssae16.com/index.html

[VII–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Procurement Engineering and Supply Chain Guidelines in Support and Operation and Maintenance of Nuclear Facilities, Nuclear Energy Series No. NP-T-3.21, IAEA, Vienna (2016).

[VII–3] ENERGY NETWORKS ASSOCIATION, Energy Delivery Systems – Cyber Security Procurement Guidance. Available online at https://www.energynetworks.org/assets/images/Resource%20library/BEIS%20ENA%20Cyber%20Security%20Procurement%20Language%20Guidance%20(final).pdf

[VII–4] BOCHTLER, J., QUINN, E.L., BAJRAMOVIC, E.L., "Development of a new IEC Standard on Cybersecurity Controls for I&C in Nuclear Power Plants – IEC 63096", Proc. 10th International Embedded Topical Meeting on Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies (NPIC & HMIT 2017), San Francisco, CA, 11–15 June (2017), Volume 1, 423–433. Available online at http://npic-hmit2017.org/wp-content/data/pdfs/158-20165.pdf

[VII–5] INTERNATIONAL SOCIETY OF AUTOMATION, InTech, New ISA/IEC 62443 standard specifies security capabilities for control system components (2018). Available online at https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

[VII–6] UNITED STATES DEPARTMENT OF ENERGY, Electricity Subsector Cybersecurity Capability Maturity Model (ES–C2M2) (2014). Available online at https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

[VII–7] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Computer Security Resource Center, Cyber Supply Chain Risk Management C-SCRM. Available online at https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/publications

[VII–8] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, QSMO Services – Supply Chain Risk Management. Available online at https://www.cisa.gov/qsmo-services-supply-chain-risk-management

[VII–9] NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION, Cyber Security Supply Chain Risks. Available online at https://www.nerc.com/pa/Stand/Pages/Project2019-03CyberSecuritySupplyChain-Risks.aspx

ANNEX VIII. COMPLEXITY MATRICES

Understanding the sources of complexity is a key factor in developing an effective cost reduction programme across supply chain management. It helps alignment with organization segmented supply chain strategy with suppliers. It also will guide organization computer security related investment and process rationalization via an understanding of the attributes that contribute to organization supply chains complexity.

Each attribute of a supply chain is typically weighted and then scored. A weight is a measure of relative importance within the overall supply chain. Setting the weights is an important factor. Through analysis and end customer experience with a specific statement of work, the end customer may have a perception of which drivers are more important than others. After weighting the attributes, the end customer typically scores those that are applicable.

Figure VIII–1 provides an example of results that would provide a range of attributes that affects the complexity of the organization supply chain. Depending on organization business strategy, the end customer will be able to make computer security decisions about how to manage the supply chain.

How Complex Is Your Supply Chain?						
		How Complex Is Your Supply Chain?	Developing Your Supply Chain Complexity Score			
Attribute	Attribute Type	Attribute Description	Comments	Score (1–5) 1=Low, 3=Medium 5=Complex	Weight	Total
1	Stock-keeping units	Number of items by location (items x locations = stock-keeping units)	Greater than 1 million, score = 5; From 1 million to 200,000, score = 3; Less than 100,000, score = 1	5	0.10	0.50
2	Constraints	Number and/or types of constraints modelled simultaneously in analysis (optimization)	Greater than 5, score = 5; From 5 to 2, score = 3; Less than 2, score = 1	1	0.10	0.10
3	Constraints	Number of independent tiers of the supply chain network	Greater than 4, score = 5; Either 4 or 3, score = 3; Less than 3, score = 1	5	0.10	0.50
4	Time phasing	Is time phasing of data modelled required (planning data, constraints)?	If 'yes', then score = 5; If 'no,' then score = 1	3	0.07	0.21
5	Demand types	On average, is more than 40% of the demand 'on promotion'?	If 'yes', then score = 5; If 'no', then score = 1	1	0.06	0.06
6	Product portfolio	On average, do new product introductions represent 20% of the item file per year?	If 'yes', then score = 5; If "no," then score = 1	3	0.06	0.18
7	Product portfolio	Average product life cycle (short or long-life cycle)	Less than 12 months, score = 1; From 12 to five months, score = 3; Less than five months, score = 5	1	0.06	0.06
8	Product portfolio	When demand is excessively seasonal	No seasonality, score = 1; 80% or more of annual demand sold in less than three months, score = 5	3	0.05	0.15
9	Product portfolio	Ratio of longest lead-time item to shortest lead-time item; the greater the ratio, the less efficiency can be realized	Greater than 10, score = 5; From 10 to 2, score = 3; Less than 2, score = 1	3	0.02	0.06
10	Management	Timeliness of supply chain evaluation (re-planning)	Daily or less, score = 5; From one day to one week, score = 3; Greater than one week, score = 1	1	0.02	0.02
11	Management	Number of segmented supply chain designs (vendor-managed inventory, consignments, returns, make-to-order and make-to-stock)	Greater than 3, score = 5; If equal to 3, then score = 3; If less than 3, then score = 1	5	0.10	0.50
12	Management	Number of trading partners sharing business process control (for example, multi enterprise business process fusion)	Greater than 3, score = 5; Either 3 or 2, score = 3; Less than 2, score = 1	3	0.03	0.09
13	Management	Number of departments sharing in business process control (for example, business process fusion)	Greater than 3, then score = 5; Either 3 or 2, then score = 3; Less than 2, score = 1	1	0.02	0.02
14	Supply chain	Amount of non-bulk transportation	Greater than $75 million per attribute, score = 5; Less than $75 million per attribute, score = 1	1	0.05	0.05
15	Customers	Average number of customer-ordered line items per day (including returns as a separate line item count)	Greater than 25,000, score = 5; From 25,000 to 5,000, score = 3; Less than 5,000, score = 1	5	0.03	0.15
16	Manufacturing	The more complex the bill of materials, the more complex the supply chain generally is	Greater than 5 levels in bill of materials, score = 5; From 5 to 3 levels in bill of materials, score 3; Less than 3 levels in bill of materials, score = 1	5	0.04	0.20
17	Warehousing	For warehousing, the number of simultaneous order lines and items, or unique configurations or constraints (no staging area)	Greater than 10,000 lines per day per facility, score = 5; From 9,999 to 5,000, score = 3; Less than 5,000, score = 1	3	0.02	0.06
18	Transportation	Support for the multiple factors (multiple carriers, number of modes, number of locations, number of businesses and geography)	If 'yes', then score = 5; If 'no', then score = 1	3	0.01	0.03
19	Supply chain	Globalization of the supply chain	Greater than 2 tax–duty trading zone, then score = 5; If 2 tax–duty trading zone, then score = 3; If less than 2 tax–duty trading zone, then score = 1	3	0.01	0.03
20	Procurement	Primary form of sourcing relationships (most typical, most likely)	Relationship-based, score = 5; Transaction-based, score = 1	3	0.02	0.06
21	Supply chain	Simultaneous attributes (example: refrigerated versus non; hazardous versus non)	Greater than 4, score = 5; From 4 to 2, score = 3; Less than 2, score = 1	3	0.03	0.09
22	Computer Security	Supplier has an established information and computer security programme (information protection)	If 'yes', then score = 1; If 'no', then score = 5	1	0.05	0.05
23	Computer Security	Does the supplier has a computer security posture with secure coding procedures?	If 'no', then score = 5; If 'yes', then score = 1	1	0.03	0.03
24	Computer Security	What security level assignment is required (information sensitivity/classification level/security level)?	Security level 1-2, score = 5; Security level 3, score = 3; Security level 4-5, score = 1;	5	0.05	0.25
25	Computer Security	Does the supplier have a testing/vulnerability management program?	If 'no', then score = 5; If 'yes', then score = 1	1	0.04	0.04
				Supply Chain Complexity Score	1.17 must = 1.0	3.49
		Scores and Ratings Greater than 3.5 = Your supply chain is 'complex' From 3.0 to 3.5 = Your supply chain is medium complexity 'simple' Less than 3.0 = Your supply chain is of low complexity 'catalogue'				

FIG. VIII–1. Range of attributes that affect the complexity of the supply chain.

Figure VIII–2 illustrates how to score each attribute and categorize the complexity of the supply chain. Generally, a score of less than 3.0 implies a low complexity supply chain with perhaps one or two stressful characteristics, but on the whole, the end customer supply chain is 'not complex'. A score between 3.0 and 3.5 implies that the end customer supply chain may suffer

from some limited stressful condition that lead to ‘moderate complexity’. A score of more than 3.5 implies that the end customer supply chain is ‘complex’, either from combined stresses of a wide range of characteristics, or through a large number of extremely stressful characteristics. The higher the score above 3.5, the more likely that the supply chain is complex and highly stressed.

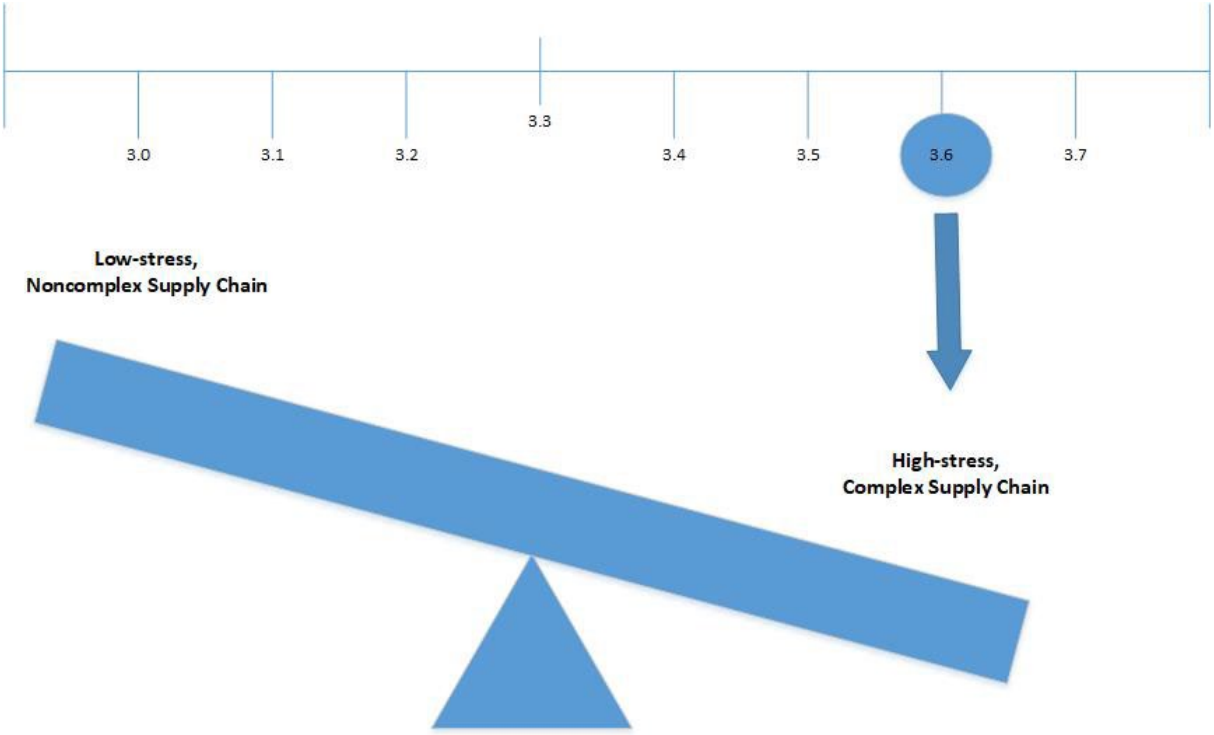

FIG. VIII–2. Complexity of the supply chain scores.

GLOSSARY

The following definitions of terms apply for the purposes of this publication only.

Customer relevant entities. Operators, licensees and nuclear power plant integrators, competent authorities, regulatory bodies, and acquirer organizations within a State's nuclear security regime.

Function. A coordinated set of actions, processes, and operations associated with a nuclear facility. Their purpose might include performing functions important or related to nuclear safety, nuclear security, nuclear material accounting and control, or sensitive information management.

Risk treatment. The process of selecting the appropriate computer security measures (risk modification, risk retention, risk avoidance, and risk sharing) to reduce risk.

Supplier relevant entities. Suppliers (designers, vendors), technical support organizations, emergency response organizations, transport organizations (shippers, carriers), and supplier organizations within a State's nuclear security regime.

Supply chain attack surface. The set of touchpoints between the acquirer and supplier organizations an adversary can use to compromise hardware, firmware, software or system information during supply chain activities, including relevant entity locations, physical or electronic storage locations and transitions between these locations.

Supply chain touchpoints. Exchanges of information (e.g. information, data, product, service) between two relevant entities.

ABBREVIATIONS

DBT	design basis threat
COTS	commercial off the shelf
EAL	evaluation assurance level
EULA	end user licence agreement
I&C	instrumentation and control
ICT	information and communication technology
NMAC	nuclear material accounting and control
NPP	nuclear power plant
OEM	original equipment manufacturer
PPS	physical protection system
SCAS	supply chain attack surface

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

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

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

NORTH AMERICA

Bernan / Rowman & Littlefield

15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550

Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

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

Eurospan Group

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

Trade orders and enquiries:

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

Individual orders:

www.eurospanbookstore.com/iaea

For further information:

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

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

International Atomic Energy Agency
Vienna