-ISO/IEC TR 6114:2023(E)

ISO/IEC TR 6114

ISO/IEC JTC 1/SC 27 N-#:####(X)

~~ISO/IEC TR 6114~~

~~ISO/IEC JTC~~ 1/SC 27/WG 4

Date: 2023-~~01-31~~06-23

Secretariat: DIN

Cybersecurity – Security considerations throughout the product life cycle

Cybersécurité — Considérations relatives à la sécurité tout au long du cycle de vie du produit

Style Definition ...

Formatted: Left: 1.5 cm, Right: 1.3 cm, Top: 1.4 cm, Bottom: 0.5 cm, Gutter: 1 cm, Section start: Odd page, Width: 21 cm, Height: 29.7 cm, Header distance from edge: 1.25 cm, Footer distance from edge: 0 cm, Different first page header

Formatted: Font: 11 pt, Not Bold, English (United Kingdom)

Formatted: zzCover, Left

Formatted ...

Formatted: Font: Not Bold

Formatted: zzCover, Space After: 0 pt, Tab stops: Not at 5.97 cm + 16.51 cm

Formatted: Font: 12 pt

ISO ~~copyright office~~Copyright Office

CP 401 • ~~Ch. de Blandonnet 8~~

CH-1214 Vernier, Geneva

Phone: + 41 22 749 01 11

~~Fax: +41 22 749 09 47~~

~~Email: copyright@iso.org~~

Email: copyright@iso.org

Website: ~~www.iso.org~~www.iso.org

Published in Switzerland.

Formatted: Indent: Left: 0 cm, Right: 0 cm, Space Before: 0 pt, No page break before, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Border: Top: (No border), Left: (No border), Right: (No border)

Formatted: Indent: Left: 0 cm, First line: 0 cm, Right: 0 cm, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Border: Left: (No border), Right: (No border)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: Indent: Left: 0 cm, First line: 0 cm, Right: 0 cm, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Border: Bottom: (No border), Left: (No border), Right: (No border)

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see ~~www.iso.org/directives~~www.iso.org/directives or ~~www.iec.ch/members_experts/refdocs~~www.iec.ch/members_experts/refdocs).

~~Attention is drawn~~ISO and IEC draw attention to the possibility that ~~some of the elements~~implementation of this document may ~~be~~involve the ~~subject~~use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights ~~in~~ in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights. ~~Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).~~

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see ~~www.iso.org/iso/foreword.html~~www.iso.org/iso/foreword.html. In the IEC, see ~~www.iec.ch/understanding-standards~~www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection* ~~OR~~.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at ~~www.iso.org/members.html~~www.iso.org/members.html and ~~www.iec.ch/national-committees~~www.iec.ch/national-committees.

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: Font: 11 pt, Font color: Auto, English (United Kingdom)
Formatted: std_publisher, Font: 11 pt, Font color: Auto, English (United Kingdom)
Formatted: Font: 11 pt, Font color: Auto, English (United Kingdom)
Formatted: std_docNumber, Font: 11 pt, Font color: Auto, English (United Kingdom)
Formatted: std_docNumber, Font: 11 pt, Font color: Auto, English (United Kingdom)
Formatted: Font: 11 pt, Font color: Auto, English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: 11 pt, Font color: Auto, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)

Introduction

The globalization of technology design, development, manufacturing, and distribution has created an environment of complicated supply chains with limited transparency. This presents an incredible challenge for the industry and highlights a growing need to ensure product integrity for all stages of the ~~ICT~~information and communications technology (ICT) product life cycle.

The call for assurance across the supply chain landscape has evolved over several decades. ~~–~~More recently, policy makers around the world have begun to focus on supply chain risks in new ways: from policies considering supply chain security risks for government procurement to various initiatives ~~by~~ adding security considerations ~~throughout the supply chain which spotlight the~~ such as trust and transparency ~~of~~in the supply ~~chains~~chain for ~~information and communications technology~~ICT.

Vendors have been doing their part as well. Over the past several years, ~~Information Communications Technology (~~ICT~~)~~ suppliers have taken important steps towards increasing supply chain transparency~~, including~~. These steps include sourcing conflict-free minerals ~~[1],~~[1] and implementing a set of policies, procedures and tools at factories to improve security consideration throughout the supply chain by validating where and when each component of an ICT product was manufactured.

These are important first steps, however they primarily focus on the production stage, just one stage of the ICT product life cycle. In today's complex environment, hardware platform providers are expected to enable a full range of tools and solutions that improve security consideration across the entire life cycle, from design and sourcing to secure retirement.

Security considerations throughout the product life cycle (SCLC) establishes an end to end framework that can be applied to the multi-year life cycle of ICT product~~[1]~~ to comprehend and address potential risks for improved transparency and higher levels of security assurances. ~~–~~ By enabling transparency and assurances across the ICT product life cycle, supply chain owners can improve platform integrity, resilience and security. ~~-~~The life cycle phases are both iterative and recursive in nature.

~~-~~

~~[1] The main target of the document is ICT hardware products including software such as microcode, firmware, and other software to support the hardware products.~~

Formatted: No page break before, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Pattern: Clear
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Default Paragraph Font, Font color: Auto
Formatted: Font: 11 pt
Formatted: Default Paragraph Font, Font color: Auto
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear

Cybersecurity - Security considerations throughout the product life cycle

1 Scope

This document describes security considerations throughout the product life cycle (SCLC), which is a framework that spans the entire information and communications technology (ICT) product life cycle. The aim of the framework is to align the industry and bring greater transparency to customers at every point on the ICT product life cycle.

This document describes the following items for ~~supplier~~suppliers, end users (~~consumer~~consumers), intermediaries of the ICT supply chain, service ~~provider~~providers, and regulators:

- — definition of phases in the ICT product life cycle from concept to retirement~~,~~;
- — threat vectors possible in each phase of the life cycle~~,~~;
- — potential controls against those threat vectors.

The target audiences of this document are suppliers and consumers of ICT products, including all participants throughout the supply chain such as silicon chip designers, fabricators, product assemblers, logistics providers, service providers, and information security organizations. Clauses 5 to 11 target an organization's strategic and risk management teams. This document provides an end-to-end view of the threats ~~by~~in each phase to help the organization shape their plans, procedures and policies~~.~~

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC/~~IEEE15288~~IEEE 15288:2015, *Systems and software engineering — System life cycle processes*

ISO/IEC/IEEE 24748-1:2018, *Systems and software engineering — Life cycle management — Part 1: Guidelines for life cycle management*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC/IEEE 15288:2015, ISO/IEC/IEEE 24748-1:2018, and the following apply.

ISO and IEC maintain ~~terminological~~terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at ~~https://www.iso.org/obp~~https://www.iso.org/obp

Formatted: Space After: 30 pt
Formatted: Left: 1.5 cm, Right: 1.3 cm, Top: 1.4 cm, Bottom: 0.5 cm, Gutter: 1 cm, Section start: Odd page, Width: 21 cm, Height: 29.7 cm, Header distance from edge: 1.25 cm, Footer distance from edge: 0 cm, Different first page header
Formatted: Left, Space After: 0 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted ...
Formatted ...
Formatted: List Continue 1, No bullets or numbering, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Pattern: Clear
Formatted: Body Text, Indent: Left: 0 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted ...
Formatted: Left, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: std_publisher
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted: English (United States)
Formatted: Body Text, Don't keep with next
Formatted ...
Formatted: English (United States)
Formatted ...
Formatted: Normal, Line spacing: Exactly 12 pt

— IEC Electropedia: available at ~~http://www.electropedia.org/~~https://www.electropedia.org/

3.1
digital signature
data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to verify the source and integrity of the data unit

[SOURCE: ISO/IEC 9798-3:2019, 3.3]

3.2
code scanner
program source code and binary file security analysis tool

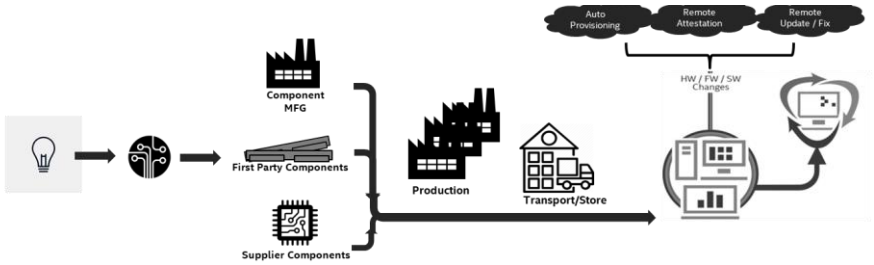
3.3
hardware trojan
malicious program or hardware that masquerades as a benign application

~~4 Acronyms~~

~~ASIC Application specific integrated circuit~~
~~BOM Bill of materials~~
~~CPU Central processing unit~~
~~DRM Digital rights management~~
~~DSP Digital signal processor~~
~~ERP Enterprise resource planning~~
~~FPGA Field programable gate array~~
~~HDL Hardware description language~~
~~IC Integrated circuit~~
~~ICT Information and communication technology~~
~~OEM Original equipment manufacture~~
~~OSAT Outsourced semiconductor assembly and test~~
~~PUF Physically unclonable function~~
~~SaaS Software as a service~~
~~SDL Security Development Life cycle~~
~~SoC System on Chip~~
~~VHDL Very high-speed integrated circuit hardware description language~~

Formatted: English (United States)
Formatted: List Continue 1, Indent: Left: 0 cm, First line: 0 cm, Don't keep with next
Formatted: Font: Times New Roman, No underline, Font color: Auto, English (United States)
Formatted: TermNum, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_year
Formatted: std_section
Formatted: Font: 11 pt
Formatted: Normal, Space Before: 0 pt

Formatted: Right



Stages in ISO/IEC/IEEE 24748-

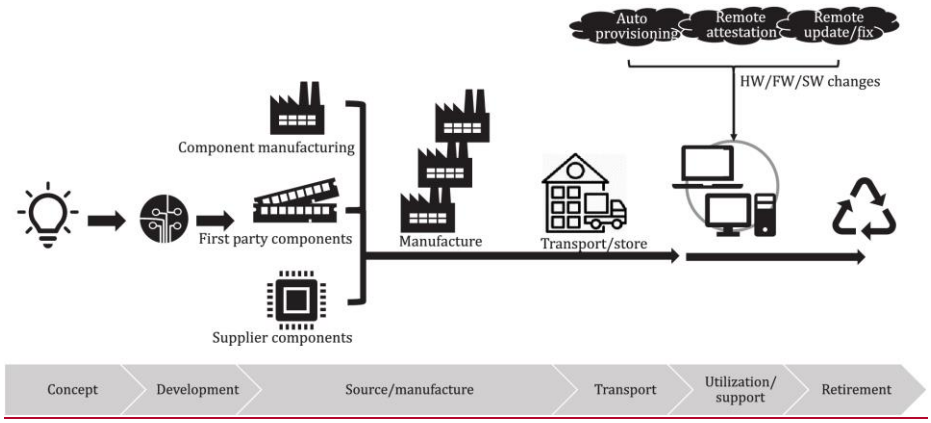
4 ICT system life cycle of ISO/IEC/IEEE 24748-1

Abbreviated terms

ASIC	application specific integrated circuit
BOM	bill of materials
CPU	central processing unit
DRM	digital rights management
DSP	digital signal processor
ERP	enterprise resource planning
FPGA	field programable gate array
FW	firmware
HDL	hardware description language
HW	hardware
IC	integrated circuit
ICT	information and communication technology
ISV	independent software vender
OEM	original equipment manufacture
OSAT	outsourced semiconductor assembly and test
OS	operating system
PUF	physically unclonable function
SaaS	software as a service
SDL	security development life cycle
SoC	system on chip
SW	software
VHDL	very high-speed integrated circuit hardware description language

Formatted: Font: 11 pt

Formatted: Normal, Line spacing: Exactly 12 pt



~~Figure 1 —~~ SOURCE: ISO/IEC/IEEE 24748-1~~:2018]~~ [3], reproduced with the permission of the authors.

Figure 1 — ICT system life cycle

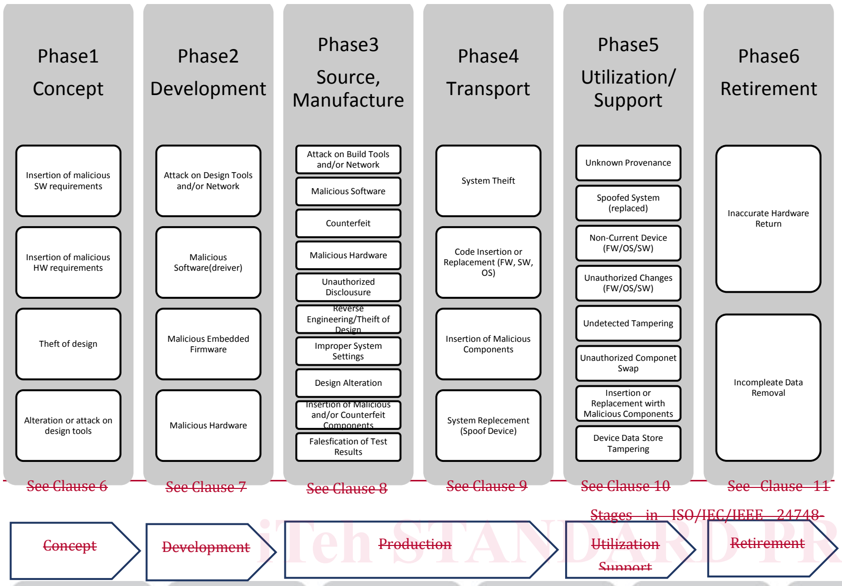
5 Security considerations throughout the product life cycle

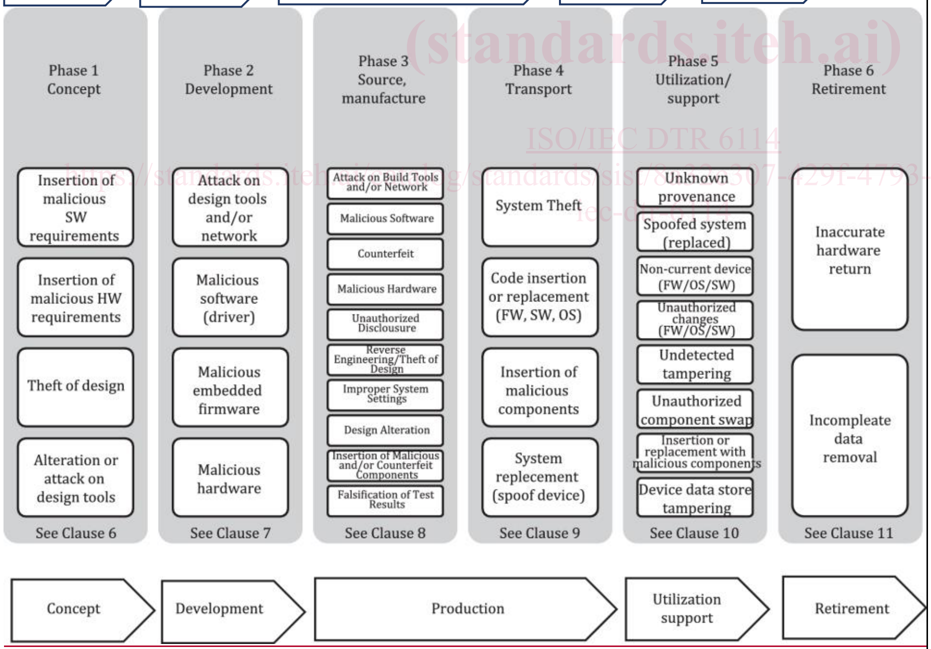
5.1 Security considerations throughout the product life cycle overview

Security considerations throughout the product life cycle (SCLC) is a framework to describe the ICT products life cycle from security assurance and manufacturing perspectives~~(~~ (see Figure 1). The concept of SCLC can be applied to hardware products and software such as microcode, firmware, and other software to support the hardware. SCLC consists of six common product life cycle phases which are shown in Figure 2 with typical threat vectors. The ~~name~~names of the phases ~~is mapped~~are derived from ISO/IEC/IEEE 24748-1~~:2018 [3]~~ and ~~added SCLC unique~~ processes unique to SCLC have been added. It is important to note that each phase exists for individual components, sub-systems and end products. It is both possible and highly likely that some of the phases are executed more than once for an individual component (~~for example, Integrated~~e.g. integrated circuits go through wafer fabrication, sorting, assembly and final test~~ and those~~. Those facilities, if separate~~ will~~, introduce multiple build/transfer phases).

~~ISO/IEC/IEEE15288 [2] is a technical standard which~~ISO/IEC/IEEE 15288 defines the life cycle of a system by four process groups which are 1) agreement process, 2) organizational project-enabling process, 3) technical management process and 4) technical process. Since this document describes the life cycle from a different perspective that is, the "product life cycle", there is no conflict or inconsistency between ISO/IEC/~~IEEE15288~~IEEE 15288 and this document. Another systems approach to security is the NIST SP 800-160V1 that aligns with this approach~~. [5]~~.[3]

Formatted: Default Paragraph Font
Formatted: Figure note
Formatted: Left, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: cite_fig
Formatted: cite_fig
Formatted: cite_fig
Formatted: cite_fig
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_publisher
Formatted: std_publisher
Formatted: std_documentType
Formatted: std_docNumber
Formatted: Font: 11 pt
Formatted: Normal, Space Before: 0 pt





SOURCE: ISO/IEC/IEEE 24748-1, reproduced with the permission of the authors.

© ISO/IEC 2023 – All rights reserved 5

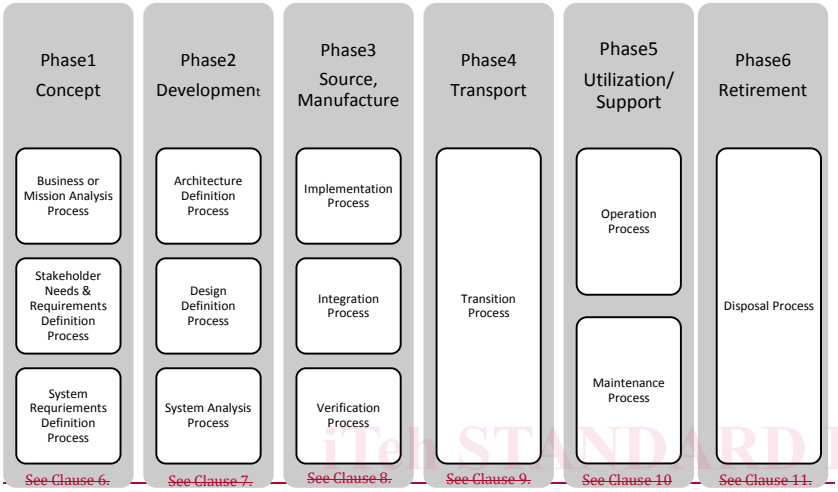
Formatted: Right

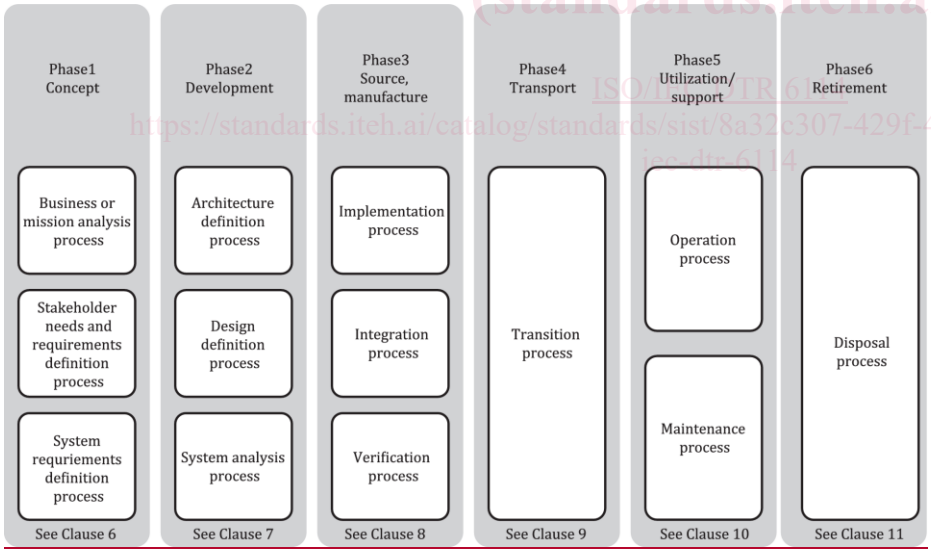
Formatted: Font: 11 pt

Formatted: Normal, Line spacing: Exactly 12 pt

~~Figure 2~~ **Figure 2 — ICT Product life cycle and threat vectors**

Figure 3 shows a relationship of technical processes in ISO/IEC/IEEE 15288 ~~[2]~~ and SCLC phases.





~~Figure 3 —~~ **Figure 3 — Mapping ~~ISO/IEC/IEEE 15288 [2]~~ technical processes of ISO/IEC/IEEE 15288 and SCLC life cycle phases**

Formatted: Font: Bold
Formatted: Figure title, Level 1, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: cite_fig
Formatted: std_docNumber
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: cite_fig
Formatted: std_publisher
Formatted: Figure title, Level 1, Line spacing: Multiple 1.08 li, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Font: 11 pt
Formatted: Normal, Space Before: 0 pt

5.2 Information and communication technology threat model

Security threats against ICT products exist not only in the utilization/support phase but in all six phases shown in Figure 2 [6]. 2.[4] Each phase has different threat vectors, but some vectors such as theft occur in multiple phases. This means responsible parties are expected to apply proper measures in each phase for each threat vector applicable to the phase. .

From Clause 6 6 to Clause 11, 11. the key characteristics of each ICT product's life cycle phase and typical threat vectors are described.

5.3 Classes of threats

There are multiple classes of security threats. The first type is an attack which targets unintentional vulnerability, such as ICT product security vulnerability in the manufacturing process or in the physical storage and transportation processes. The second type of security threats areis an intentional attacksattack by insider personnel who can access the process and change or replace tools, products, or components. The focus of this document is to identify and protect ICT products from the first type of threats. However, the methods described in this document can also be used to mitigate the risks of the second type of threats. In many cases, additional protection measures are necessary, such as employee/personnel management and access control in all phases for all stakeholders who participate in the product life cycle.

5.4 Structure of the report

From clause Clauses 6 to 11, give an overview of each phase, threats, and controls are described. Additionally, annexes [see Annex Annexes A, B, C and D] are included for practitioners on provide specific best practice procedures and controls for practitioners that they can be implementedimplement within their operation to mitigate against potential threats.

6 Phase 1: Concept

6.1 General

This is the first phase of the ICT product life cycle. In the concept phase, user needs are identified, and system concepts are described and evaluated. In addition to the users'user needs, companies are expected to consider regulatory controls and security objectives to establish a comprehensive set of requirements to be met in development.

Given the complexity of ICT products, many companies will combine internal design, 3rdthird party design and open source design to deliver a single component on a system where a system which can be comprised ofcomprise hundreds of components. For example, the Systemsystem on a Chipchip (SOC) component can contain hardware blocks sourced from many third parties, as well as blocks designed by the product manufacturer. This complexity introduces additional risks as unneeded features from external components which are incorporated into the end product, possibly creating a vulnerability that can be attacked. For this reason, the product flowflows back through the concept phase to add additional security control requirements based upon decisions made in development.

It is best practice for ICT product organizations to adopt a Security Development Lifesecurity development life cycle (SDL) process that conforms with ISO/IEC 27034-1:2011 [7]. . This process ensures the identification of unique threats at the start of the concept phase and turns those into a set of requirements to be met during the development phase. Additionally, SDL requires the training of the

Formatted: Right
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: cite_fig
Formatted: cite_sec
Formatted: cite_sec
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left
Formatted: Font: 12 pt
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: cite_sec
Formatted: Pattern: Clear
Formatted: cite_app, Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Left, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: Font: 11 pt
Formatted: Normal, Line spacing: Exactly 12 pt