TECHNICAL REPORT

ISO/IEC TR 6114

First edition
2023-10

Cybersecurity — Security considerations throughout the product life cycle

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

Reference number
ISO/IEC TR 6114:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights 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.

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. In the IEC, see 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*.

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 and www.iec.ch/national-committees.

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 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 adding security considerations such as trust and transparency in the supply chain for ICT.

Vendors have been doing their part as well. Over the past several years, ICT suppliers have taken important steps towards increasing supply chain transparency. These steps include sourcing conflict-free minerals,[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) establish an end to end framework that can be applied to the multi-year life cycle of ICT products 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.

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 suppliers, end users (consumers), intermediaries of the ICT supply chain, service 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 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/IEEE 15288, *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, ISO/IEC/IEEE 24748-1:2018, and the following apply.

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

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at 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

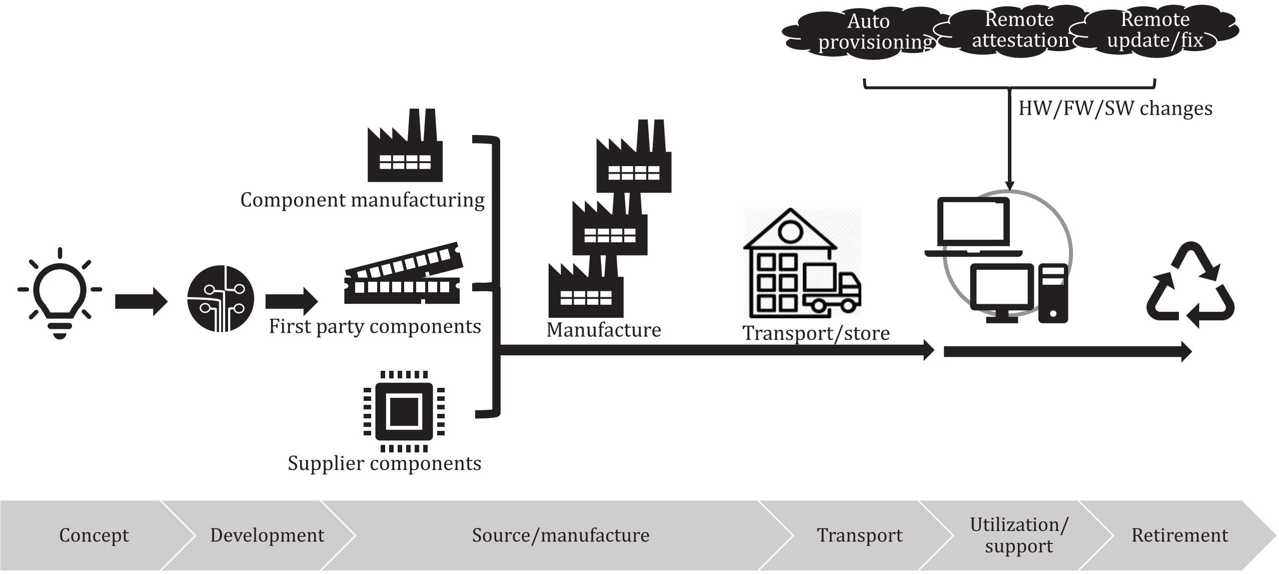
[SOURCE: ISO/IEC 9798-3:2019, 3.3]

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 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 programmable 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



SOURCE ISO/IEC/IEEE 24748-1:2018, reproduced with the permission of the authors.

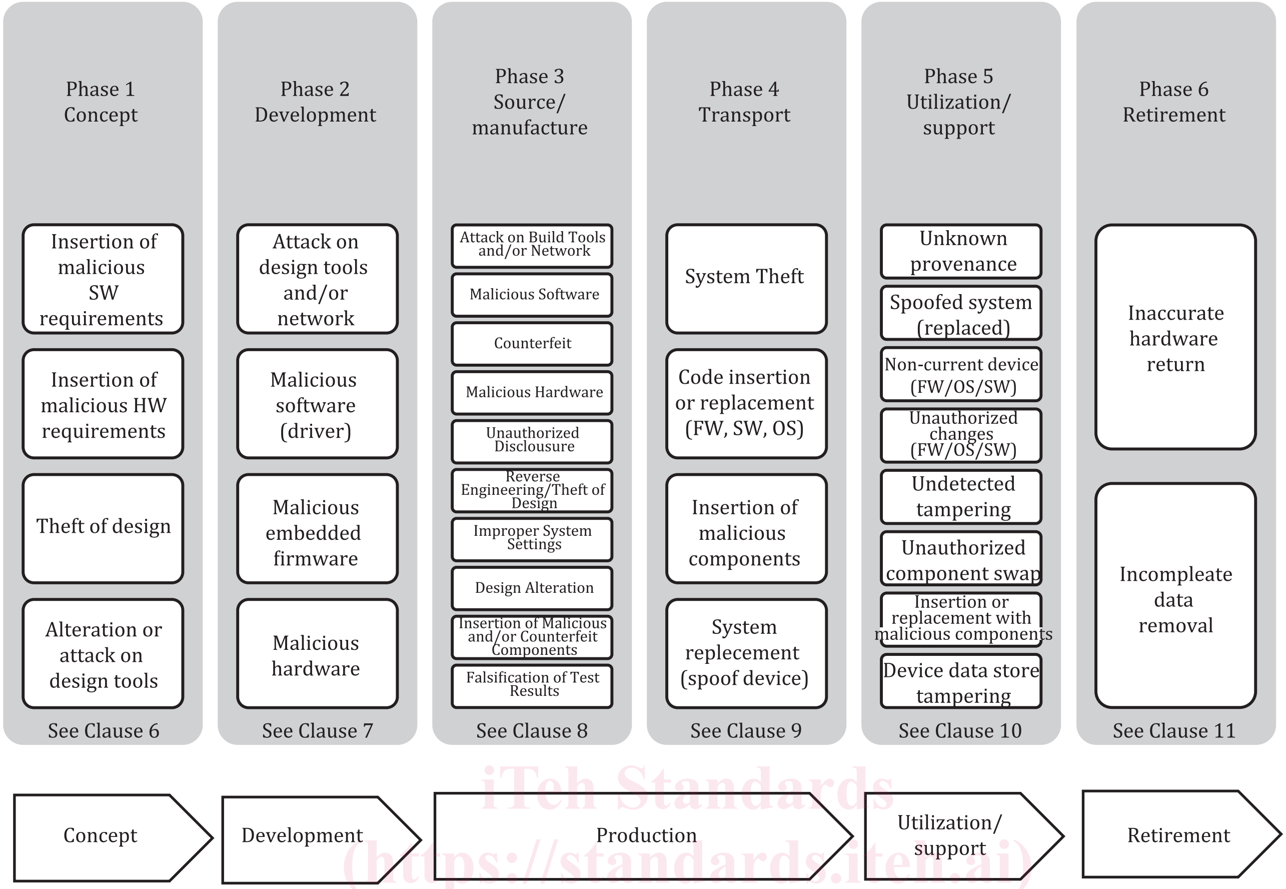
Figure 1 — ICT system life cycle

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 names of the phases are derived from ISO/IEC/IEEE 24748-1 and 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 (e.g. integrated circuits go through wafer fabrication, sorting, assembly and final test. Those facilities, if separate, introduce multiple build/transfer phases).

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/IEEE 15288 and this document. Another systems approach to security is the NIST SP 800-160V1 that aligns with this approach.[3]


Phase 1
Concept
Insertion of malicious SW requirements
Insertion of malicious HW requirements
Theft of design
Alteration or attack on design tools
See Clause 6
Phase 2
Development
Attack on design tools and/or network
Malicious software (driver)
Malicious embedded firmware
Malicious hardware
See Clause 7
Phase 3
Source/ manufacture
Attack on Build Tools and/or Network
Malicious Software
Counterfeit
Malicious Hardware
Unauthorized Disclousure
Reverse Engineering/Theft of Design
Improper System Settings
Design Alteration
Insertion of Malicious and/or Counterfeit Components
Falsification of Test Results
See Clause 8
Phase 4
Transport
System Theft
Code insertion or replacement (FW, SW, OS)
Insertion of malicious components
System replecement (spoof device)
See Clause 9
Phase 5
Utilization/ support
Unknown provenance
Spoofed system (replaced)
Non-current device (FW/OS/SW)
Unauthorized changes (FW/OS/SW)
Undetected tampering
Unauthorized component swap
Insertion or replacement with malicious components
Device data store tampering
See Clause 10
Phase 6
Retirement
Inaccurate hardware return
Incompleate data removal
See Clause 11
Concept
Development
Production
Utilization/ support
Retirement

SOURCE ISO/IEC/IEEE 24748-1:2018, reproduced with the permission of the authors.

Figure 2 — ICT Product life cycle and threat vectors

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

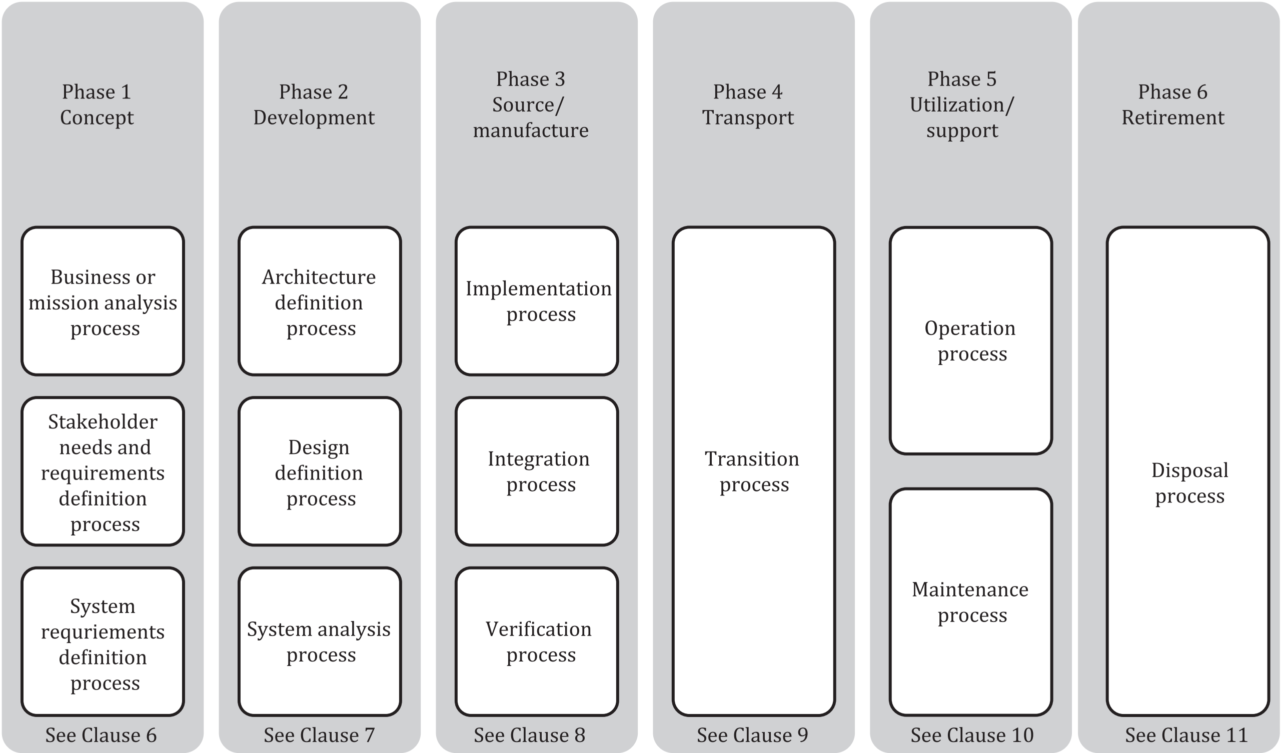


Figure 3 — Mapping technical processes of ISO/IEC/IEEE 15288 and SCLC life cycle phases

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.[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.

From Clause 6 to Clause 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 that targets unintentional vulnerability, such as ICT product security vulnerability in the manufacturing process or in the physical storage and transportation processes. The second type is an intentional attack 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

Clauses 6 to 11 give an overview of each phase, threats, and controls. Additionally, Annexes A, B, C and D provide specific best practice procedures and controls for practitioners that they can implement within their operation to mitigate against potential threats.

6 Phase 1: Concept

6.1 General

In the concept phase, user needs are identified, and system concepts are described and evaluated. In addition to the 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 combine internal design, third party design and open source design to deliver a single component on a system that can comprise hundreds of components. For example, the system on a chip (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 that are incorporated into the end product, possibly creating a vulnerability that can be attacked. For this reason, the product flows 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 life cycle (SDL) process that conforms to ISO/IEC 27034-1. 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 engineers, designers and architects that work on how to best maintain a secure system, thereby increasing the security of the product.

SCLC in the concept phase addresses the questions:

- What is in the products function?
- Does the product contain anything additional that can be used against the owner/operator of the ICT product?

In 6.2, possible threat vectors and mitigations in this phase are described.

6.2 Summary of concept threats and controls

6.2.1 Workflow toolchain tampering

Management of the software tools used in support of the concept phase is critical to mitigating attacks to the tool that can alter the design or allow feature requirements to be stolen. These tools often support integration with third-party plugins, such as those from outside tool vendors or even from the original tool provider. If the plugins are not properly verified/certified, they can contain malicious elements. Additionally, installation of these modules can be subject to man-in-the-middle (MITM) attacks during transit over the network or in the build of the tool software by the software provider. The modules require sufficient verification before installation into the concept toolchain. It is essential to implement a practice for managing design tools and keeping them up to date and secure. Best practice ensures these plugins have been digitally signed and licensed by a reputable producer, are regularly scanned by source code scanners (static and dynamic) and have an internal team responsible for securing the design tools. Moving to a SaaS workflow toolchain vendor properly skilled in secure life cycle practices and verified by an independent third party can also be an effective way to improve controls on the toolchain. However, this comes with risks, as the SaaS providers are a likely target of attack due to the multitude of customers in one spot. The ICT product developer is responsible for securing their workflow toolchain and for assessing their own internal security controls against that of a SaaS provider to determine the best way to implement their workflow toolchain.

In cases where the network used in the concept phase is not a closed network, attacks can be launched against these networks from external adversaries in the hopes of obtaining or modifying sensitive design files. Such attacks can be supported by an insider threat that installs malware or a virus on critical security systems, allowing for easier access and attacks against target platforms. Refer to ISO/IEC 27032 for guidance on building and maintaining secure networks, as this issue is the same for any ICT entity that runs a private network.

6.2.2 Unauthorized operations

The unauthorized invocation of data operations for creating, reading, updating/modifying or deleting data in the concept phase can impact the development of the product, its components or sub systems. For example, a security feature developed in concept phase, but which has been deleted/rejected or changed and which influences the product design and build to not include a security feature necessary to protect the product in operation or add a backdoor into the product for future attacks once in operation.

6.2.3 Integrity faults

The integrity faults can occur by unintentional modification or destruction of data due to technical or operational errors, faults or failures occurring within a product, or related to supporting the product's concept phase. Like unauthorized operations, this can lead to a manipulation or exclusion of requirements for the development phase, thereby altering the function of the ICT product. These faults can get caught in development if the appropriate test cases are in place to validate the correct requirements. However, if they are not caught, or caught too late in the life cycle, additional costs are incurred as the product is looped back into the development phase to remove the vulnerability.

6.2.4 Theft or loss

The absence, removal or destruction of a data asset, or unauthorized data access due to actions taken by a malicious actor, or by environmental hazards can occur within the concept phase.

7 Phase 2: Development

7.1 General

This is the second phase of the ICT product life cycle, where engineering design and development are conducted. Example processes are prototype design and evaluation, engineering sample development and manufacturing, threat analysis, manufacturing tool development and production operation planning.

7.2 Summary of development threats and controls

7.2.1 Attacks on development tools and/or network

The same security threats and prevention mechanisms described in 6.2.1 can be applied to this phase.

7.2.2 Malicious embedded firmware

Hardware that has any intelligence requires firmware, so the hardware knows how to operate. Firmware typically sits in non-volatile memory and is not authenticated prior to execution making it vulnerable to attack through alterations. This characteristic of firmware makes firmware susceptible to attack at many stages in the SCLC. This subclause deals with malicious firmware during the design and creation of firmware by the original designer. It is important to note that manufacturers of ICT products can take the firmware from the hardware manufacturer and change it for their unique need or ignore it all together and replace it with their own firmware or that of another third party.

Due to the fluidity of firmware from the original product designer throughout the supply chain, it is important for firmware to be maintained and tracked with good source code management tools and version control processes. Firmware not only changes within the supply chain, prior to provisioning, but it is not uncommon for it to change throughout phase 5 and even into phase 6. Firmware changes in the utilization phase typically occur to address performance and security updates in the hardware that were not discovered in validation.

In design, all firmware can include a process for adding a digital signature to the firmware prior to distribution so the ICT process can verify the signature and only load the firmware if the signature is valid. The signature ensures the firmware has not been tampered with in phase 2. Combining this process with the security design life cycle practices can improve confidence in the validity of the firmware.

7.2.3 Malicious hardware

Malicious hardware (HW) can be introduced by an internal or external source adding additional circuitry into a design that performs a function other than what was specified in the product requirements. Best practices to mitigate the implementation of malicious HW are the implementation of peer code reviews and the utilization of code scanners. Additionally, characterizing the normal behaviour of the HW enables the implementation of test cases that test for abnormal behaviours.

Malicious HW results in additional circuitry added to the design. The hardware performs all the functionality to meet the design requirements but has additional circuitry that can activate only after a specific condition exists (number of executions, amount of time since power on, etc.). It is almost statistically impossible to exhaustively test with every possible input vector. The types of hardware trojans are broad, but it is technically possible to send data back to an unauthorized party. Another hardware trojan can invoke a destructive action or prevent any action during the operation of the product.

7.2.4 Malicious software (driver)

Software drivers and firmware typically come from the hardware supplier, but there are instances where these are provided by a third party. This can be done when a single software driver is controlling components from multiple hardware manufacturers, and it requires the integration of multiple sets of software into a single signed software module. This software is susceptible to the same design threats for software implemented internally, like the insertion of hidden functionality. To mitigate this threat, when selecting suppliers it is important to consider the SDL and supply chain controls followed by the supplier. Additionally, validation results can be made available as part of the product delivery to ensure that there can be independent verification of code scans results and test results and to ensure no abnormal behaviour. Requiring only signed software as a standard practice enables software traceability directly back to the signing organization and possible verification that no manipulation has occurred. Performing static code scans of each version of software provided will give an additional internally verifiable result to the state of the software provided.

Malicious software can also occur from software tampering. Some common types of software tampering mechanisms are described in Annex F.

7.2.5 Counterfeit

Counterfeit components can appear to operate within the requirements established by stakeholders, but can suffer from substandard materials and insufficient quality controls and validation, leading to unpredictable life. This can lead to higher failure rates, inoperability within the required environment (heat, moisture, vibration, etc.) and the inability to hold the product manufacturer accountable.

One best practice which can be implemented in the supply chain is to buy only from distributors that are authorized (by the manufacturer of the component). Another best practice is to perform routine audits of the suppliers on their security practices to prevent counterfeit parts from entering their supply chain. Audits can include observation of supply chain practices, destructive tests on components and verification of validation results.