ATIS Standard:
5G Network Assured Supply Chain

ATIS-I-0000090
June 2022

ABSTRACT

As the deployment of 5G continues to expand in North America and across the globe, it is critical to secure 5G infrastructure. The scale of 5G is rapidly expanding across new vertical markets, broader industry sectors, and a massive number of new devices and applications. This new ATIS standard addresses the 5G supply chain (5G/SC) as a critical function in the design, build, deployment, and operation of 5G assured networks. We define the network to be the interconnecting fabric that enables endpoints (devices and clients) to exchange information with other endpoints or servers. The supply chain aspects associated with the endpoint (devices, clients, and servers) are not within the scope of this document.

This document focuses on the requirements and controls necessary to operationalize a set of agreeable levels of assurance associated with the lifecycle functions of high assurance 5G/SCs. This work is based on a flexible reference model and component flow through the complex 5G/SC to identify specific controls that can mitigate the identified threats and associated attacks. Attack classes are identified by using defined attributes. These attributes represent a defining quality of an asset (hardware component, module, system, software) and consequently reflects the asset's attackable characteristics.

Designating specific system components as "critical" as part of a 5G cybersecurity risk management effort is essential for managing supply chain risks within available or assigned resource constraints. Network operators and enterprises must select, shape, and scale their risk mitigation strategy according to business, operational and security needs. They also must prioritize a subset of "critical components" that warrants "extra attention" in the assurance assessment, testing, and monitoring activities.

The approach taken in this document is to leverage where possible techniques that can link back to a component's source to verify the authenticity and integrity of that component. The use of Software Bill of Materials (SBOM) and Hardware Root of Trust (HRoT) represents two methods that can effectively accomplish this goal. In addition, the application of security best practices helps secure each of the supply chain lifecycle functions identified.

The entity responsible for attesting the level of supply chain assurance for a network can use this specification with suppliers by providing:

- An assurance level that the supplier must comply with.
- A list of the identified critical components that apply to the supplier.
- This document and the set of requirements as listed in Section 8 as part of the purchase agreement, along with any desired exceptions and/or additions.

FORWARD

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global Information and Communications Technology (ICT) companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the all-Internet Protocol (IP) transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle – from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the Third Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [https://www.atis.org/policy/patent-assurances/] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

COPYRIGHT INFORMATION

ATIS-I-0000090

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Table of Contents

1. Introduction

1.1 Scope

This document defines a flexible supply chain flow model and a comprehensive set of requirements that can be applied to any 5G supply chain (5G/SC) ecosystem. These requirements, associated controls, and metrics are applicable to a broad range of network use cases and can be utilized in most risk-management regimes associated with the selection and implementation of controls. The network is defined as the interconnecting fabric that enables endpoints (devices and clients) to exchange information with other endpoints or servers. The supply chain aspects associated with the endpoint (devices, clients, and servers) are not within the scope of this document.

This approach leverages the output of numerous Supply Chain Risk Management (SCRM) best practices, guidelines, and recommendations developed by other collaborative efforts between government and industry, which are referenced throughout this document.

1.2 Purpose

Although other standards venues have explored supply chain requirements, 5G mobile technology introduces an increasingly complex set of challenges due to the diverse application space and 5G's expanding global supply chain model. The goal of this standard is to provide entities operating networks and their suppliers with a flexible approach for assuring a 5G/SC at any level of component integration or product type. By applying these requirements and controls across the 5G/SC, customers can achieve a greater level of assurance that the 5G/SC is secure in light of a constantly changing and evolving threat environment.

1.3 Application

The 5G/SC model and requirements contained in this document have been developed for application in a broad range of high-assurance public and private networks. It is understood that the landscape of 5G/SC needs will continue to evolve with the ever-changing threat environment. Therefore, the approach described in this document is designed to be flexible across a wide range of 5G and beyond applications and solutions and be extensible into the future. Forward-looking use cases that are representative of real-world 5G deployments are selected and applied to the development of requirements in this document and can be translated to an implementable approach for delivering secure, resilient, and trustworthy 5G networks.

2. References

2.1 Normative References

None.

2.2 Other References

The following is a list of reference documents that have been identified as supportive to the requirements and standards contained in this document.

- List of Other References.
  - NIST Special Publication 800-207 - Zero Trust Architecture, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
  - NIST Special Publication 800-53 - Security and Privacy Controls for Information Systems and Organizations
  - NISTIR 7622 - Notional Supply Chain Risk Management Practices for Federal Information Systems, https://csrc.nist.gov/publications/detail/nistir/7622/final
  - NISTIR 8320 - Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases, https://csrc.nist.gov/publications/detail/nistir/8320/final
  - NISTIR 8320A - Hardware-Enabled Security: Container Platform Security Prototype, https://csrc.nist.gov/publications/detail/nistir/8320a/final
  - 3GPP TS 23.501 Technical Specification - System architecture for the 5G System (5GS), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144
  - 3GPP TS 33.501 Technical Specification - 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169
  - SCRM Task Force Year Two Report, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf
  - ICT SCRM Task Force: Vendor Supply Chain Risk Management (SCRM) Template, https://www.cisa.gov/publication/ict-scrm-task-force-vendor-template
  - Mitigating ICT Supply Chain Risks With Qualified Bidder And Manufacturer Lists, https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf

- CISA Threat Scenarios February 2020 Version, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report_0.pdf
- Atlantic Council: Breaking Trust Software Supply Chain Security, https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf
- BSA: Securing 5G Harness Software Innovation, https://www.bsa.org/files/policy-filings/07152020bsa5gsecurityagenda.pdf
- NIST Supply Chain Risk Management Practices for Federal Information Systems and Organizations, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf
- Defending Against Software Supply Chain Attacks, released by CISA and the National Institute of Standards and Technology (NIST), https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
- CSRIC Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks, https://www.fcc.gov/file/14855/download
- CSRIC Report On Recommendations For Identifying Optional Security Features That Can Diminish The Effectiveness Of 5g Security, https://www.fcc.gov/file/20606/download
- Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM), Second Edition, https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf
- The Minimum Elements For a Software Bill of Materials (SBOM), United States Department of Commerce and NTIA, July 12, 2021, https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom
- Trusted Computing Group (TCG) TPM 2.0 (Trusted Platform Module) Resources, https://trustedcomputinggroup.org/resources/
- The Trusted Execution Environment (TEE) Committee, https://globalplatform.org/technical-committees/trusted-execution-environment-tee-committee/
- Security and Privacy Controls for Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final/

3. Definitions, Acronyms, & Abbreviations

3.1 Definitions

The following is a list of terms and definitions contained in this document. For a list of common communications terms and definitions, visit the ATIS Telecom Glossary at https://glossary.atis.org.

Best Practices	Refers to a procedure that research and experience shows can produce optimal results and that is established or proposed as a standard suitable for widespread adoption[1]. Within the scope of this document, current best practices include the NIST Online Informative References Program (OLIR) and other well accepted sources for security-related functions.
Heterogeneous Networks (HetNet)	In network applications, HetNet refers to the use of multiple different access technologies such as the mobile/cellular network, Wireless LAN, and potentially other wireless technologies.
Tier 1 Supplier	Refers to a supplier that delivers components directly to the network operator.

3.2 Acronyms and Abbreviations

3GPP	Third Generation Partnership Project
5G/SC	5G Supply Chain
5GC	5G Core
5GS	5G System
AI	Artificial Intelligence
AI/ML	Artificial Intelligence/Machine Learning
AMF	Access and Mobility Management Function
API	Application Programming Interface
AR	Augmented Reality
ARA	Architectural Risk Analysis
BOM	Bill of Materials
C2	Command-and-Control
CA	Certification Authority
CCA	Client Credential Assertion
CISA	Cybersecurity and Infrastructure Security Agency

[1] https://www.merriam-webster.com/dictionary/best%20practice

COOP	Continuity of Operations
CP/UP	Control Plane/User Plane
CU	Centralized Unit
DN-AAA	Domain Name - Authentication, Authorization, and Accounting
DU	Distributed Unit
E2E	End-to-End
EAP	Extensible Authentication Protocol
EK	Endorsement Key
eMBB	enhanced Mobile Broadband
EO	Executive Order
EO/IR	Electro-Optical/Infrared
EPC	Evolved Packet Core
eSIM	embedded SIM
HetNet	Heterogeneous Network
HRoT	Hardware Root of Trust
HSM	Hardware Security Module
HW	Hardware
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IoT	Internet of Things
IV&V	Integrity, Independent Verification, and Validation
JWT	JSON Web Tokens
MEC	Multi-Access Edge Compute
mMTC	massive Machine-Type Communications
MOCN	Multi-Operator Core Network
MOUT	Military Operations on Urban Terrain
MUD	Manufacturer Usage Description
MVNO	Mobile Virtual Network Operator
NF-C	NF Service Consumer
NF-P	NF Service Producer
NFs	Network Functions
NHN	Neutral Host Network
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
npm	node package manager
NR	New Radio
NRF	Network Repository Function
NS	Network Slice

NSA	Non-Standalone
NTIA	National Telecommunications and Information Administration
NTN	Non-Terrestrial Network
NVD	National Vulnerability Database
OLIR	NIST Online Informative References Program
O-RAN	Open RAN
OS	Operating System
PaaS	Platform as a Service
PCF	Policy Control Function
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
RAN	Radio Access Network
RASP	Runtime Application Self-Protection
RIC	RAN Intelligent Controller
RU	Radio Unit
SA	Standalone
SaaS	Software as a Service
SBA	Service-Based Architecture
SBI	Service Based Interface
SBOM	Software Bill of Materials
SCA	Software Composition Analysis
SCRM	Supply Chain Risk Management
SDE	Software-Defined Everything
SDLC	Software Development Lifecycle
SDN	Software-Defined Networking
SEPP	Security Edge Protection Proxy
SIM	Subscriber Identification Module
SMF	Session Management Function
SPDX®	Software Package Data Exchange®
SW	Software
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communications
V2X	Vehicle to Everything
VNF	Virtual Network Function

4. Overview

The demand for a high-assurance 5G/SC will increase as 5G-enabled technologies are integrated into critical national infrastructures, global e-commerce, and life-critical applications. Assurance reflects the customer's strategic objectives, security policies, risk tolerance, and available resources, all of which will shift as 5G standards, enabling technologies, and associated threats continue to evolve. Therefore, "assured" is not a terminal state. Instead, an assured 5G/SC connotes an agreeable level of transparency across all system components and contributing entities based upon a common set of supply chain assurance requirements. This document is focused on the requirements and controls necessary to operationalize a set of agreeable levels of assurance associated with the lifecycle functions of high assurance 5G/SCs. These assurance levels and the associated controls will naturally intersect with existing cybersecurity risk management aspects that may be in place.

4.1 5G System Overview

The 5G ecosystem is more than an LTE network upgrade. It is a *system of systems* that can be configured in any number of ways to meet specific network operator objectives. With the addition of cloud computing/virtualization, Artificial Intelligence (AI), and Software-Defined Networking (SDN) to the next generation of telecommunications equipment, Network Functions (NFs), and behaviors can be added or modified without human intervention.

The Third Generation Partnership Project (3GPP) defines an overarching structure for this 5G system, or 5GS[2], as the integration of the following subsystems:

- **User Equipment (UE) -** modem-equipped endpoint devices such as smartphones, laptops, and Internet of Things (IoT) sensors/actuators.
- **Radio Access Network (RAN) -** provides cellular connectivity to UEs over a set of 5G frequencies.
- **5G Core (5GC) -** performs essential network and management functions (e.g., subscriber management, charging/billing, authentication & authorization).

5G standards provide network operators with unprecedented flexibility to deploy highly customized network architectures that can satisfy many performance, security, cost, operational or environmental objectives. Consequently, this flexibility may come at a cost, particularly from a supply chain perspective. The following topics highlight 5G-unique scenarios and tradeoffs that have certain supply chain ramifications:

[2] 3GPP TS 23.501, System architecture for the 5G System (5GS), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

- **Public vs. Private -** Corporate and government 5G networks may be deployed over public or private network infrastructure. Hybrid deployments (e.g., a shared ownership model or a mix of commercially available and custom equipment[3]) may complicate the supply chain assurance assessment process.
- **Open, Disaggregated RAN -** Open RAN (O-RAN) refers to the disaggregation of traditional base station functionality into three independent and distributable components: the Radio Unit (RU), the Distributed Unit (DU), and the Centralized Unit (CU). 3GPP disaggregated the DU and CU. O-RAN introduced work that disaggregates the DU and RU. These RAN components are then integrated using standard, open interfaces, and Application Programming Interfaces (API). When combined with virtualization, this deployment strategy allows processing to be sourced from multiple vendors, thus requiring increased emphasis on integration testing, continuous monitoring, and SCRM.
- **Physical vs. Virtual -** 5G networks may be constructed using traditional telecommunications appliances (e.g., base stations, gateways) or virtualized equivalents running on cloud computing infrastructure. As telecom service providers further embrace cloud computing paradigms, disaggregated Virtual Network Functions (VNFs) may be developed as highly scalable microservices and deployed to cloud-native computing platforms.
- **Terrestrial vs. Non-Terrestrial -** Future 5G networks will not be bound to terrestrial deployments. A wide assortment of aerial and space-based assets will form nascent communications capabilities and supply rural and austere locations with robust internet connectivity.
- **Sidelink Communications -** Initially introduced in 3GPP Release 12 for LTE public safety applications, 5G sidelink communications, also referred to as device-to-device communications, enable devices to create ad-hoc networks and connect directly with one another, all without transmitting data over the network. As a result, UEs double as network endpoints and packet-forwarding network routers[4].

4.2 Supply Chain Assessment Methodology

In this document, we define supply chain assurance based on compliance with a set of defined requirements organized into assurance levels as described in Section 8. All other text in this document should be considered informative relative to Section 8 labeled requirements.

[3] Security Guidance For 5G Cloud Infrastructures. https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_IV_508_Compliant.pdf

[4] In general, end-user devices are outside of the scope of this document (as noted in Section 1.1 and Section 5.1.3)

Assuring the 5G/SC for application in a 5G assured network implies that high assurance is achieved across the network 5GS subsystems (RAN and core), as well as the underlying transport network, routing, and all associated operations and management systems. This includes all equipment (hardware), software, computing platforms, support services, and actors engaged in the exchange of information across the 5GS. Moreover, *system assurance* involves more than the integration of assured components. Aspects such as deployment site features and other non-technical (e.g., environmental or policy-related) factors may either enhance or degrade the assurance level for the End-to-End (E2E) solution.

4.2.1 Getting Started

The requirements listed in Section 8 represent a *minimum* set associated with the assurance levels as defined in Section 8. For some organizations, the path to high supply chain assurance will begin by increasing awareness of its growing inventory of networking equipment, software, and contracted services. *Awareness* also includes a thorough understanding of the lifecycle processes used in design, inbound supply, build, distribution, integration, operation, and post-operation functions across the flow of components in the supply chain. Assessments at this phase are limited to simple queries and rule-based processing.

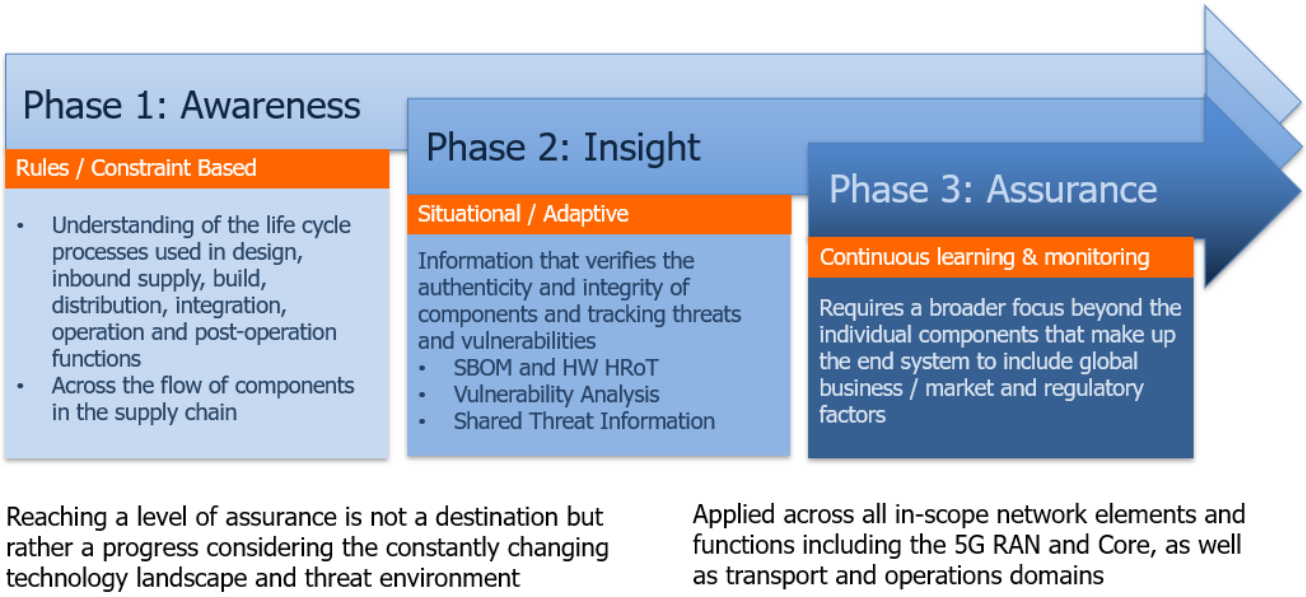


Figure 4.2-1 Evolution to Assured Networks

The next goal is to achieve enhanced insight into the supply chain. *Insight* includes information that verifies the authenticity and integrity of components and tracking novel threats and vulnerabilities. This phase leverages structures such as SBOM, HRoT, and other mechanisms related to component provenance. The National Institute of Standards and

Technology (NIST) defines[5] provenance in the context of supply chain as "the records describing the possession of, and changes to, components, component processes, information, systems, organization, and organizational processes." Assessments at this phase may incorporate situational and deployment environment information to create a more accurate representation of the supply chain and underlying network infrastructure elements. In this document, *provenance* is primarily applicable to component-level requirements.

The third evolutionary phase is assurance. *Assurance* requires a broader focus beyond the individual components that make up the end system to include global business/market and regulatory factors. Under a full assurance-based approach, assessments require advanced supply chain illumination and threat-modeling tools to facilitate reasoning over an extensive, heterogeneous data set.

4.2.2 System Assurance

A large-scale 5G network deployment is a complex system that may produce behaviors beyond the aggregated functionality of its subordinate components. Details about the deployment environment and other non-technical factors may influence the customer's risk-tolerance level and drive demand for heightened supply chain assurance. In these cases, a mutual, system-level understanding of the target assurance level should be shared between the customer, the network operator, and Tier 1 integrators and suppliers. Indeed, all parties are impacted by the resulting supply chain requirements and, as such, have a stake in determining the appropriate level of assurance needed.

For 5G deployment scenarios that have unique security requirements, additional mitigation measures and reported information may be requested or developed by the customer to attain a desired assurance level for "critical" system components or services. The request will be made via a **private and secured** exchange to protect the interests and sensitivities of all parties[6]. The following examples demonstrate various ways in which a customer may request additional measures and information to enhance their awareness of the supply chain:

- One or more additional levels of component and supplier information.
- Increased reporting frequency (e.g., shift from quarterly to weekly reporting).
- Information on development lifecycle activities, locations, and actors.
- Proof of Integrity, Independent Verification, and Validation (IV&V), or standards compliance.
- Enhanced tracking, inspection, or verification techniques (e.g., waveform fingerprinting).

[5] NISTIR 7622 - Notional Supply Chain Risk Management Practices for Federal Information Systems, https://csrc.nist.gov/publications/detail/nistir/7622/final

[6] The software supplier is responsible for all software it provides. When open source software is part of the supplier's software deliverable, the software supplier is held responsible for the management and integrity of that software.

To achieve and maintain this high level of assurance, the customer will need an active, sustained, bi-directional, and private communication channel with the appropriate entity to expedite responses to supply chain attacks and jointly monitor known vulnerabilities.

4.2.3 Critical Components

Designating specific system components as "critical" as part of a 5G cybersecurity risk management effort is essential for managing supply chain risks within available or assigned resource constraints[7]. It is understood that no supply chain will likely ever be 100% secure, resilient, transparent, and trustworthy. As a result, each customer must select, shape, and scale its risk-mitigation strategy according to business, operational, and security needs. For the enterprise or wide area 5G deployments (e.g., a smart city, military installation, or campus), there are too many hardware and software elements to designate all as critical components. Therefore, the customer will need to prioritize a subset that warrants extra attention in the assurance assessment, testing, and monitoring activities. In most cases, a critical designation will be assigned when a component performs functions that, based on a risk analysis, are more susceptible to high-impact compromise. This designation precipitates additional data requirements and monitoring that are *above-baseline* activities and will require agreement between the customer and impacted vendor(s). Although a general risk-management framework might identify critical components, additional critical components may be identified as a result of deployment and application-specific SCRM assessments.

4.2.4 Equipment (Hardware) Assurance

Assessing the trustworthiness of 5G equipment is a difficult task due to rapid innovations occurring within related technology areas such as microelectronics and cryptography. Hardware assurance can initially be determined from the bill of materials (BOM) data collected from Tier 1 suppliers and confirmed use of a HRoT solution where needed. Under certain circumstances (e.g., critical designation or special circumstances as identified by the customer), additional data elements may be requested from lower-tier suppliers to address data gaps or uncertainties.

Hardware assurance requirements will be presented in Section 8.

4.2.5 Software Assurance

Software assurance presents an even greater challenge as physical inspection and measurement techniques are infeasible due to the volume of source code and use of third-party APIs and libraries that were built from open source codebases that contain significant contributions from virtually unknown, globally distributed software developers. Furthermore,

[7] More details related to the selection of critical components are provided in Section 6.4 and Section 8.

the rampant adoption of cloud computing and virtualization technologies only increases the amount of software comprising the coming generations of networks.

The first step toward software assurance is to enhance awareness of the critical software products within the target system. This inventory step will be achieved using a SBOM. Similar to the hardware assurance process, software products may be designated as critical components, resulting in the application of additional measures and data reporting. For example, such additional measures may be required for automation performed by third-party "xApps" and "rApps," which are AI/ML-based applications that control and optimize network behavior within the RAN[8].

Software assurance requirements will be presented in Section 8.

[8] The supply chain implications for AI/ML implementations remain an area for future study.

5. High-Assurance Use Cases

An example set of high assurance use cases is provided in Appendix D. These use cases highlight a number of key supply chain aspects for consideration in assured networks.

5.1 Use Case Overview

These use cases represent a small sample of applicable 5G use cases but are useful in better understanding how the supply chain impacts and intersects with a 5G network. 5G network deployments may vary greatly in terms of scale, number of components, distribution of processing nodes, and ratio of hardware to software assets. As a result, customers and vendors may need to extend the baseline set of assurance requirements in light of one or more deployment examples presented in this section.

The 5G network is more than just the 5G-specific components in the network. Rather, the 5G network relies on an inherently non-linear combination of multiple intersecting supply chains. These supply chains can be associated with the management layer, the transport layer, and the 5G-specific layer in the network. In addition, each supply chain includes components that are part of other supply chains. These components will also have a lifecycle, which results in a chain of lifecycles. While these complex supplier relationships may be managed independently, the combination directly impacts 5G network assurance. This interplay of components and lifecycle will be incorporated into the 5G/SC model discussed in Section 6.

5.1.1 5G Radio Access Network (RAN)

Compared to the core network and UE, the 5G RAN is viewed as the section of the network where revolutionary innovations can best enhance performance for the user and optimize remote network management, automation, and configuration for the operator. As more data processing, storage, and analysis functions are conducted at the network edge (e.g., via Multi-Access Edge Computing (MEC) in hybrid cloud deployments), greater attention and resources should be applied to achieving and maintaining the desired supply chain assurance level of 5G RAN components and services. Also, depending on the distribution, density, and locations of the entire RAN infrastructure, it is reasonable to expect that ownership and management over RAN-related infrastructure may be a shared responsibility, particularly in RAN-sharing situations. This is where RAN infrastructure is deployed in shared physical environments and when leased facilities are utilized. Contractual agreements may be required to ensure sufficient information sharing channels are established for multiple-customer and/or multiple-operator projects.

RAN Infrastructure Sharing[9]

RAN infrastructure for a single 5G network deployment may consist of several cell sites, which could be owned by a single entity or shared across multiple operators. For Neutral Host Network (NHN) and Multi-Operator Core Network (MOCN) deployments, key structural and functional elements (e.g., power supply, spectrum, towers, or antennas) may be shared assets that are managed by a single party or municipality. Additional agreements may be required to ensure adequate supply chain transparency is achieved and maintained for all utilities and equipment that are integral to the operation of the RAN.

O-RAN

O-RAN refers to the disaggregation of traditional base station functionality into three independent and distributable components: the RU, the DU, and the CU. 3GPP disaggregated the DU and CU. O-RAN introduced work that disaggregates the DU and RU. In addition, the RAN Intelligent Controller (RIC) adds automation and optimization features to the management of the disaggregated RAN functions. The RIC may also comprise third-party apps – "xApps" and "rApps" – that add specialized capabilities such as traffic steering, increased energy efficiency, and multi-vendor network slicing to the standardized set of RAN functions. xApps and rApps have been recognized across industry, including the O-RAN Alliance, to be a supply chain security risk. In addition, AI/ML algorithms and other third-party software components within the ORAN RIC yield *programmable* network behaviors and controls, which may constitute a critical component designation for certain software component suppliers.

Heterogeneous Networks (HetNets) & Brownfield Implementations

Today's 5G networks are often built atop existing 4G network infrastructure. This type of "brownfield" 5G network implementation is referred to as a Non-Standalone (NSA) deployment. For 5G NSA networks, the underlying 4G equipment and services are active and vital to the 5G network operations and should be included in all associated assurance activities.

In a similar fashion, some 5G networks may be deployed as part of a heterogeneous network, or "HetNet" solution. Future networks may aggregate 5G New Radio (NR), 4G LTE, and Wi-Fi into a multi-vendor, multi-network solution running over both licensed and unlicensed spectrum. Depending on the network design and interfaces between the independent networks, assuring the full supply chain of the composite network may be necessary.

Additional agreements may also be required to ensure adequate supply chain transparency is achieved and maintained in situations with shared or HetNet infrastructure.

[9] ATIS-I-0000073: Neutral Host Solutions for 5G Multi-Operator Deployments in Managed Spaces", 2019

5.1.2 5G Core Network

The 5G packet core network is also evolving to meet growing customer and operator demands. One of the notable aspects of the core network's evolution is the increasing virtualization of core NFs and the adoption of cloud-native infrastructure platforms. As more management and processing capabilities are executing at the edges of next-generation mobile networks, the resource burden of assuring the network core's supply chain may lessen with time.

5GC network slicing is a network segmentation technique that establishes multiple, independent logical networks over a shared network infrastructure. The concept of a Network Slice (NS) provides operators with unprecedented flexibility to meet varied service levels and customer requirements by remotely allocating resources and configuring network behaviors. Network slicing is often perceived as a network security feature because of its network segmentation, traffic separation, and network-slice-specific authorization and authentication of attaching devices. However, its value as a mitigator of known and novel supply chain threats and vulnerabilities is limited. Depending upon the details of the vendor implementation, core network slicing – also referred to as E2E network slicing – may reduce the scope of the assurance assessment and the risk exposure for certain vendors.

5.1.3 5G User Equipment (UE)

Handheld mobile devices and other forms of endpoint devices are outside the scope of this specification. However, embedded communications components that are provisioned and managed by network operators (e.g., SIM/eSIM) may be included in supply chain assurance assessments.

5.2 Use Case Summary

The scenarios described above illustrate a number of key aspects that may impact the 5G/SC. For example, 5G deployment scenarios are likely to rely heavily on cloud native and virtualization technologies. These technologies introduce common compute, storage, and networking layers that impact the supply chain by introducing new supply chain risks from software vulnerabilities in infrastructure software and contributions to open source software from untrusted entities. In addition, the introduction of edge computing can create new attack vectors in the 5GS. To help address this issue, 3GPP has added capabilities to better integrate cloud and edge computing in 5G. Cloud capabilities at the edge of the network can effectively deliver real-time performance and reduced latency but can also introduce new supply chain risks.

Although not explicitly shown, each use case can be used in roaming scenarios. To support secure communication between the home and visited Public Land Mobile Networks (PLMN), a new network function called the Security Edge Protection Proxy (SEPP) was introduced in

the 5G architecture. All signaling traffic across operator networks is expected to transit through these security proxies.

Authentication between SEPPs is required, as well as an application layer security solution on the interface between the SEPPs. A supply chain analysis of 5G should include functions such as the SEPP that may not be explicit in the basic architectural description but are essential functions required for network operation.

It is also important to note that in roaming scenarios, both the home and visited networks must be assured 5G networks if an E2E assured network is needed[10].

In addition, 5G specific capabilities such as O-RAN, network slicing, HetNets, and edge computing should be key considerations for supply chain risk analysis.

5G is complex with long supply chains supporting a rich set of applications with combined software/hardware deployments.

[10] This specification addresses supply chain assurance of a specific network segment (as described in Section 8), not the assurance of an E2E connection.

6. Supply Chain Model

6.1 Supply Chain Ecosystem

The ecosystem surrounding 5G/SC is a complex set of stakeholder relationships between acquirers, integrators, and suppliers. In different circumstances, entities can operate at two or more of these levels.

The following diagram provides an E2E view of the 5G/SC ecosystem and its related lifecycle. It is important to note that these stages are not intended as sequential steps, but rather a continuous flow of supply chain functions and processes across the integration and deployment of a 5G assured network, which may include sub-components, components, software, and hardware elements.

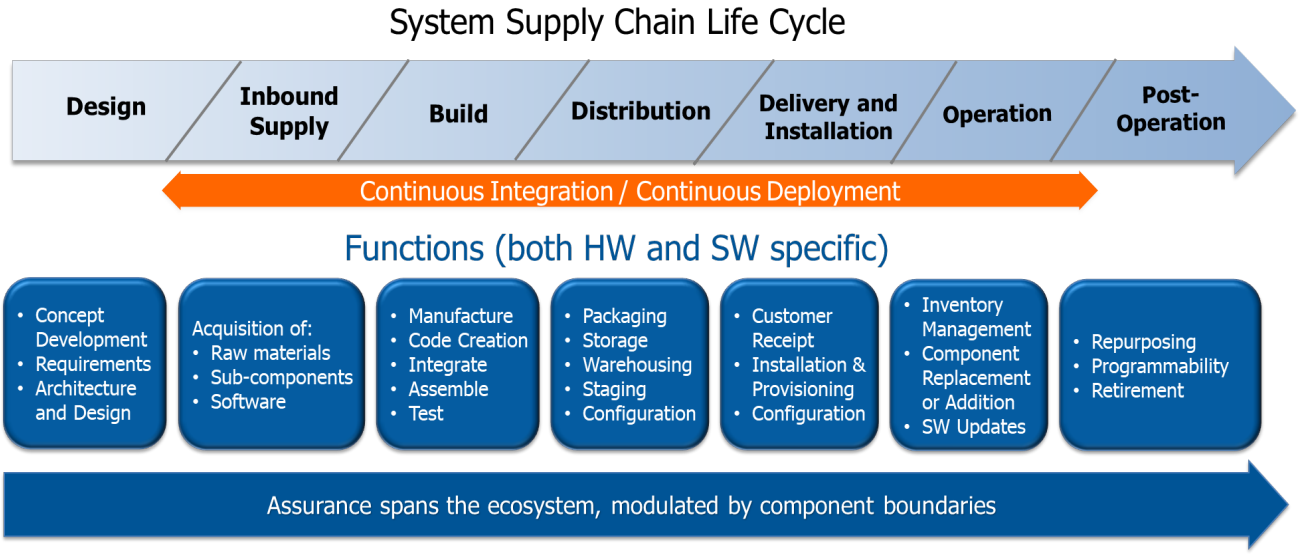


Figure 6.1-1 System Supply Chain Life Cycle Functions

Figure 6.1.1 illustrates the set of functions applicable to both hardware and software components. The identified functions include:

- **Design** includes concept development, requirements, architecture, and high-level functional design activities. The design stage should use robust and secure practices and incorporate security capabilities into the design of the component itself.
- **Inbound supply** includes the acquisition of raw materials, sub-components, and software necessary for the build process. Care must be taken to ensure that the inbound-supply processes source components with known authenticity and integrity. Inbound supply includes the transfer of components from the supplier to build function and as such, includes concerns related to shipping of hardware components, as well as the electronic transfer of data/software related components.

- **Build** includes manufacturing (for hardware) and/or coding (for software/firmware) along with the integration, assembly, and test functions. Build processes should follow secure practices.
- **Distribution** includes packaging, storage, warehousing, staging, and initial configuration functions. These functions should follow secure practices. Similar to inbound supply, the distribution function includes the transfer of components from the supplier to the next function in the supply chain lifecycle. As a result, there are concerns related to shipping of hardware components and the electronic transfer of data/software-related components. However, because the subsequent functions lead to operational systems, the components in this lifecycle function tend to be higher-level components, which may include operational systems or products.
- **Delivery and installation** include customer receipt, installation, and associated provisioning and configuration. These functions should follow secure practices and be performed by trusted personnel.
- **Operation,** from a supply chain perspective, includes inventory management, component replacements or additions, and software updates.
- **Post-operation** includes functions that may occur once the component is removed from its initial service environment. This may include repurposing, reprogramming, and retirement activities.

Supply chain threats are present for each of the above lifecycle functions and should be considered for any supply chain mitigation plan.

It is also important to note that components and their associated metadata have a lifecycle.

6.2 5G/SC Attributes

An attribute is a defining quality of an asset (e.g., hardware component, module, system, software) and consequently reflects the asset's attackable characteristics. These attributes are used to help identify a complete set of threats as discussed later in this document. Attributes should exhibit characteristics of completeness and independence. All threats/attacks should map to one or more attributes (e.g., attributes completely cover the attack space). Attribute characteristics should be independent of other attributes by definition as this generally simplifies the model by minimizing redundancy and complication in the analysis.

The following 5G/SC attributes are utilized in this document:

- Integrity
- Authenticity
- Provenance
- Availability

- Confidentiality

Attributes can be characterized in two ways: (1) associated with the components and their flow through the supply chain, and (2) associated with the security of the information (e.g., data, metrics, or information) concerning the components/flow. These are described as follows:

ATTRIBUTE	As Applied to Components	As Applied to Supply Chain Data/Metrics/Information Security
Integrity	Meets stated requirements with no unauthorized modifications or unintended capabilities (e.g., it is what it's supposed to be and nothing else).	Data has not been modified by unauthorized entities.
Authenticity	Created/service performed by known documented entities; touched only by who it was supposed to have been touched by.	Reflecting the property of being verifiably genuine (e.g., associated with the identity of the data and who has access to the data).
Provenance	A historical record of the creation of an object or component, along with tracking information to identify the entities that have integrated or had access to the component as it flows through the supply chain.	A historical record of the creation of the data object.
Availability	The component is available when needed/as planned.	Timely and reliable authorized access to uncompromised data.
Confidentiality	The component can be accessed (e.g., modified, seen, or used) only by authorized, authenticated identities.	Ensuring that data associated with a component is protected from unauthorized use (e.g., read or modify).

As described above, supply chain attributes can be applied at both a component level, within the 5G/SG ecosystem, or at a data security level. The attribute of provenance is primarily applicable to component-level requirements.

The attributes of integrity, authenticity, provenance, availability, and confidentiality will be applied throughout this document to identify the requirements and controls necessary at each stage of the 5G/SC.

6.3 5G/SC Model Architecture

This section provides a high-level architecture covering the scope of supply chain processes contained in this document, the inward/outward flow of objects defined by the architecture, and sub-processes that encompass the 5G/SC architecture. A product/object can either be created natively (e.g., new software module) or integrated from other objects by an entity (e.g., vendor, integrator, or service provider).

The following diagram provides a multi-layered view that can be applied to any 5G/SC component, sub-component, or software analyzing each stage of the flow with respect to the key attributes identified earlier in this document.

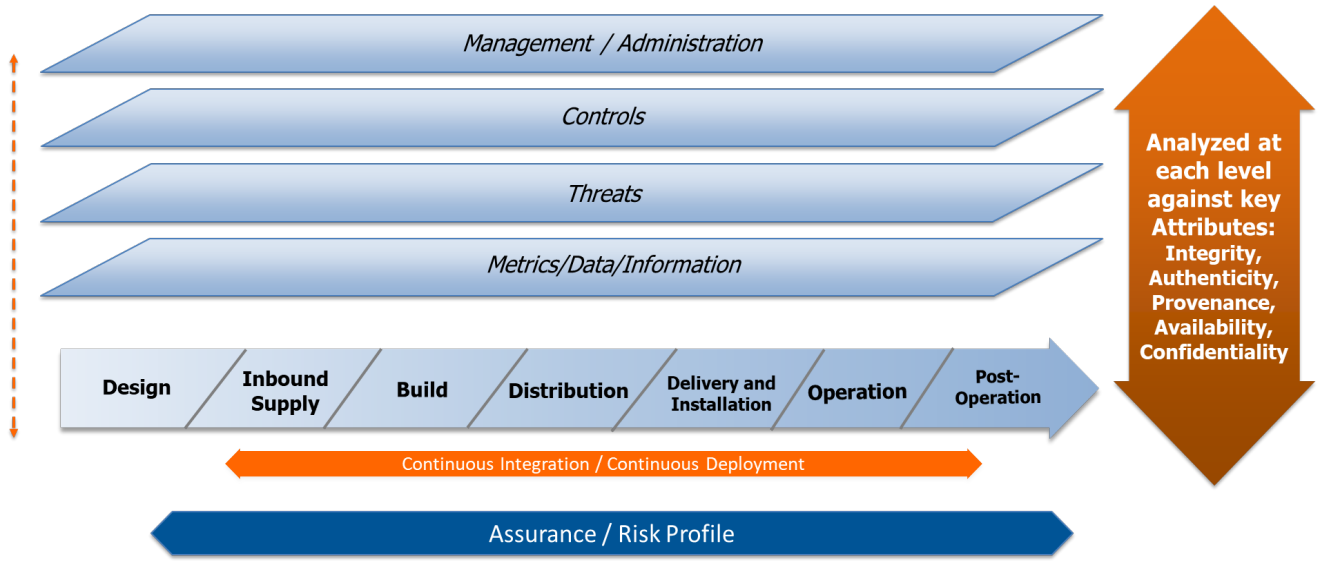


Figure 6.3-1 Supply Chain Model

The goal of the model illustrated above is to determine the common needed controls and management practices and processes to assure the 5G/SC at an acceptable level of risk for a specific application.

Underlying the component sequential flow is the sublayer of assurance and/or risk profile (Bill of Risks) across the supply chain based on the end application. The aggregated Bill of Risks adds up to the overall risk, so that assurance can be evaluated along the entire supply chain.

The *Metrics, Data, and Information* layer is associated with the target component/service/ function used to support the process steps required for assurance. This includes capabilities such as:

- Identity (e.g., signatures, serial numbers, certificates of authenticity).
- Integrity (e.g., using cryptographic hashes and signatures).
- Characteristics (e.g., critical information, programmability level, policy compliance).
- History of activity (e.g., shipping/tracking information, provenance related information).
- Vulnerability tracking (e.g., where the component is deployed and what vulnerabilities exist).

The *Threats* layer contains a list of threats identified and categorized by risk. Controls and management techniques can then be applied to mitigate threats that pose a serious risk of impact based on the end application/service.

For example, threats may include:

- Software vulnerabilities
- Code-signing issues
- Hijacked update processes
- Open source with malware insertion
- Compromised (e.g., embedded) credentials and weak cryptography
- Hardware vulnerabilities
- Tampering/modification
- Programmability vulnerabilities
- Substitution

The *Controls* layer includes the specific tests, verifications, audits, and other functions to provide assurance in mitigating a threat relative to one or more attributes.

For example, typical controls may include:

- Product barcode scans
- Physical security of facilities and packaging (e.g., locks and enclosures)
- Integrity tests of hardware and software via HRoT verification and other means
- Encryption/code signing
- Software scans to identify potential malware
- Inspection
- Tracking with documentation
- Verification of certifications, standards, and compliance requirements

The *Management and Administration* layer includes the supply chain process aspects used to help assure the security of the supply chain.

Common examples of vendor management and contracting include:

- Utilization of preferred vendor lists
- Enforcement of vendor diversity
- Contractual obligations to ensure that vendors meet specific supply chain standards and/or use specific security best practices and processes
- Contractual enforcement provisions (e.g., required audits, liquidated damages)

6.4 Types of Components

The 5G/SC model highlights the progression of components flowing through the supply chain process. A component is generally defined as a part or element of a larger whole. For the purposes of a 5G/SC, the end system is comprised of parts or components, each of which may in turn be comprised of simpler components and so on down the chain. Similarly, a product maybe comprised of a set of component parts, and, in turn, the product may serve as a component in a larger system.

Components have different attackable attributes with different vulnerabilities that may avail different threats. However, components can be sorted into a small set of categories where each category has similar attributes and, as such, similar vulnerabilities with similar associated threats and can be controlled or mitigated using similar techniques. We have identified four such categories of components for our analysis.

1. **Open Source Software** - Software in which the source code is open and can be developed in a collaborative public manner by both trusted and untrusted contributors. Open source software is released under a license in which the copyright holder grants users conditional rights to use, study, change, and distribute the software to anyone and for any purpose.
2. **Proprietary Software** - Software in which the source code is developed/managed by the software publisher and is closed to outside entities. The software's publisher reserves some rights from licensees to use, modify, share modifications, or share the software, sometimes including patent rights.
3. **Software-Controlled Hardware** - A component that includes complex processing/compute capabilities and/or memory/storage, which may be compromised in a way that affects the integrity/behavior of the component while still meeting operational specifications. That is, the component meets requirements but may include new malicious functionality that can be leveraged in attacks.
4. **Other Hardware** - Other hardware has the attribute that compromises generally result in an availability vulnerability. That is, the component has been compromised to greatly reduce its life and thus would fail much sooner or in a coordinated way. Alternatively, the component may no longer meet specifications, resulting in a partial failure.

Note that these components are often integrated into higher-level components, which make up products that would eventually be used to create systems or parts of system. For example, all of the component types listed above are included in a server chassis, router, or other network equipment. These products themselves can be components in a larger configuration such as a network. From a supply chain perspective, these higher-level components can often be treated as a software-controlled hardware component where both software and software-controlled hardware threats and controls are applicable.

A 5G network is comprised of a very large number of hardware and software components. Some of these components are more critical to network operation than others. It will be important to ensure that identified critical components receive more detailed assurance assessment and monitoring.

The criticality of components will depend on many factors, including customer needs relative to the applications and services provided, deployment environment, operator policies and procedures, and the specific operational function being provided. A supply chain risk analysis should be performed on the specific network instance to identify critical components. In most cases, a critical component designation will be assigned when a component performs an operational function that is more susceptible to high-impact compromise. Operational functions implemented by components (e.g., APIs, radio transmission, or security protocols) should be considered in the identification of critical components. In addition, consideration should be given to standard industry definitions of critical software.

A “critical” designation for any component should be assigned by the organization responsible for asserting a level of assurance for the specific network segment as it is deployed. It is important to note that criticality is a factor of use. That is, a specific instance of the use of a hardware or software component is identified as critical when that use is deemed more susceptible to high-impact compromise.

7. Vulnerability Analysis

7.1 Operational Capabilities That Help Mitigate Supply Chain Events

The publication *Defending Against Software Supply Chain Attacks*[11], released by the Cybersecurity and Infrastructure Security Agency (CISA) and NIST, recommends actions to mitigate malicious or vulnerable software that may be inserted via the supply chain. This publication specifically noted security architectural techniques in support of this goal:

> "Using deliberate network segmentation, organizations can mitigate the effects of software vulnerabilities and associated exploits, as well as aid incident response and recovery. Segmentation helps confine a vulnerability or attack to portion of a customer's enterprise. Organizations can also achieve such mitigation by implementing endpoint-based micro-segmentation with host-based firewalls or agents. Micro-segmentation can be part of a 'zero trust' architecture or implemented on its own."

The 5GC network has been designed to incorporate many of these recommendations, specifically those around network segmentation, the use of micro-segmentation, and a variety of capabilities to support zero trust[12] across the 5GC architecture[13].

An overview of many of these capabilities is provide in Appendix E.

Other operational security capabilities can be very helpful in detecting and mitigating supply chain attacks. Runtime Application Self-Protection (RASP)[14] employs runtime instrumentation to attempt to detect and/or block the exploitation of software vulnerabilities by taking advantage of information from the software in execution. Runtime exploit prevention differs from traditional perimeter-based protections, which can only detect and block attacks by using network information without contextual awareness. RASP technology can reduce the susceptibility of software to attacks by monitoring and potentially blocking attacks using runtime logic specific to the context of the runtime code. However, the use of RASP techniques can impact performance and scalability of the application, and the specific details associated with RASP vary by application. As such, the use of RASP must be carefully considered to ensure that performance metrics are maintained, and its use should be agreed between the supplier and the responsible entity.

---

[11] https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

[12] SP 800-207 - Zero Trust Architecture, https://csrc.nist.gov/publications/detail/sp/800-207/final

[13] Zero trust and 5G – Realizing zero trust in networks, https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g

[14] Security and Privacy Controls for Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

RASP is still a nascent technology in its use in large-scale 5G network infrastructure applications. As such, additional experience is needed prior to the creation of specific requirements.

7.2 Vulnerability Management

5G networks are increasingly software driven due to virtualization and include significant proprietary and open source components. Since communication networks are often considered critical infrastructure, dealing with vulnerabilities in a timely and effective way is essential.

Vulnerabilities create threats that contribute to risk. Assurance is the process in which we quantify and manage contextual risks based on threat vectors exposed by vulnerabilities in process and data across the supply chain ecosystem.

Key elements in assuring a secure supply chain include:

- Secure identification of components used within the system and verification of component authenticity.
- Identification of the author/source/provider of the component and verification of their commitment to the security.
- Tracking known vulnerabilities against the identified component to ensure that risk is managed and to enable both reactive and proactive actions.
- Verifying the integrity of the author/source/provider across the entire supply chain lifecycle.
- Verification of integrity should include periodic audits.

These elements can and should be applied to both software and hardware to fully address 5GSs.

The relationship between system software and hardware can be complex and follow a variety of operational models. For example, a 5GS could utilize many different cloud models, including Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and associated public/private/hybrid approaches. These models and approaches present an environment where many third-party providers (e.g., an IaaS or SaaS provider) play a key role in system assurance. Even when these third-party actors follow the necessary supply chain standards, there are likely constraints on what metadata can be shared between parties, which can limit the ability to identify and track vulnerabilities. Ultimately, the party responsible for the specific infrastructure components used (e.g., the platform used in a virtualized/cloud environment) is responsible for supply chain assurance for those components.

The approach taken in this document is to leverage, where possible, techniques that can link back to a component's source to verify the component's authenticity and integrity. The use of SBOM for software and HRoT for hardware and software represent two methods that can effectively accomplish this goal.

7.2.1 Software

SBOM provides a framework to implement vulnerability tracking. An SBOM's primary purpose is to uniquely and unambiguously identify software components and their relationships to one another[15].

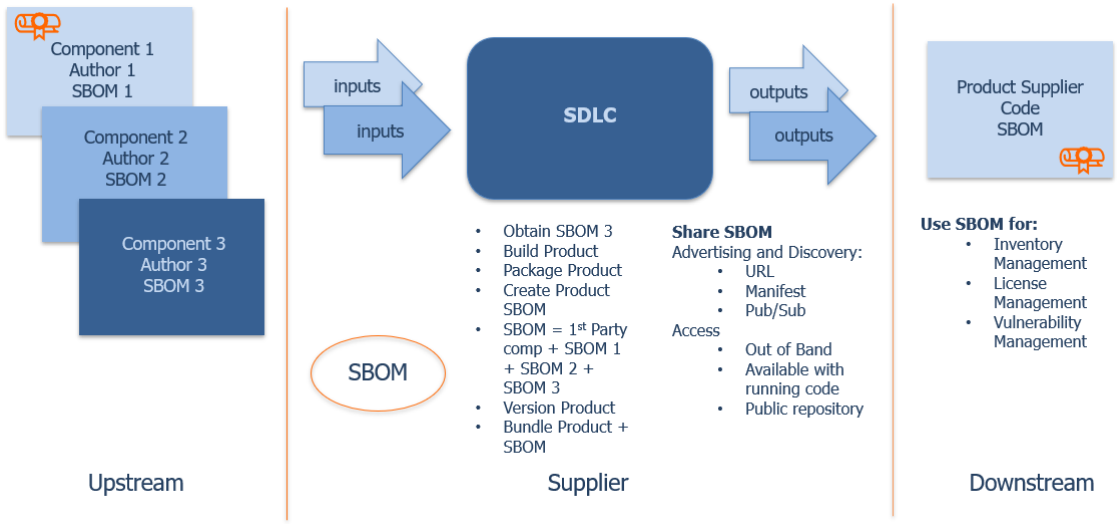


Figure 7.2-1 SBOM and the Software Development Lifecycle

Typically, a software supplier executes a Software Development Lifecycle (SDLC) process. This takes various software components as inputs and builds/packages an output software product, which is then distributed to downstream systems. Each component used or created in this process involves the management of an associated SBOM.

Many organizations, including the National Telecommunications and Information Administration (NTIA)[16], have done significant work in defining a common SBOM structure and process by offering a baseline of how software components can be represented and created.

[15] Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM), Second Edition, https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf

[16] The Minimum Elements For a Software Bill of Materials (SBOM), United States Department of Commerce and NTIA, July 12, 2021, https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom

To be effective in vulnerability tracking, a software supplier should provide a complete list of all software in use (via an SBOM), including both proprietary and open source components. The SBOM should include metadata such as supplier name, component name, unique identifier, version string, component hash, relationship, timestamp, and author name (the author's name refers to the author of the SBOM itself). The supplied SBOM file should be digitally signed by the supplier to ensure the file's authenticity and integrity. In addition, the supplier should provide an updated SBOM as part of every code release, each patch, and/or update.

It is important to note that the use of self-signed certificates does not address the question of trust in authenticity attestations. As such, any certificate signature procedure should utilize a signing platform that supports a reasonable level of trust with authenticity checks. "sigstore[17]" is an example of a new standard for signing, verifying, and protecting software. This industry collaborative platform utilizes:

- Automatic key management to generate the key pairs needed to sign and verify artifacts while automating the process as much as possible so there's no risk of losing or leaking them.
- Transparent ledger technology to enable anyone to find and verify signatures, and check whether someone's changed the source code, the build platform, or the artifact repository.

Unfortunately, a single global authoritative source for naming and identifying software components and their corresponding authors does not exist[18]. This absence makes it difficult to map and link software to vulnerabilities recorded in global or national repositories such as the National Vulnerability Database (NVD).

For open source, components are usually managed in complex ecosystems that have their own authoritative systems (e.g., package managers such as a node package manager (npm)). Commercial developers often have an internal software management system or tracking of software branches across builds, but this may not extend outside the organization in a usable fashion. When authoritative upstream SBOMs are unavailable, suppliers may create "best-effort" SBOMs using discovery and scanning tools or obtain upstream component metadata from alternative sources, but this may introduce its own set of risks. On this issue, NTIA published guidelines for software identity on their effort for software component transparency.

[17] A new standard for signing, verifying, and protecting software, https://www.sigstore.dev/
[18] Software Identification Challenges and Guidance, NTIA Multistakeholder Process on Software Component Transparency Framing Working Group, 2021-03-30, https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_software_identity-2021mar30.pdf

Ideally, software suppliers produce, sign, and distribute their first-party components with corresponding SBOMs that get incorporated in downstream products SBOMs using cryptographic linking techniques to maintain integrity and authenticity. The ultimate goal is that entities running software in their environments have a clear inventory of all the components and associated versions. This inventory should also link to the business or network functions dependent on them so they can efficiently and effectively apply remediation actions when vulnerabilities are identified.

By shifting the responsibility of SBOM authorship to the original software supplier, the overall accuracy of metadata across the supply chain increases, which in turn lowers the cost of tracking and inventorying running software. It also improves vulnerability management overall.

Ultimately, suppliers create SBOMs for their first-party components, obtain SBOMs for the upstream components used in their product, and provide assembled SBOMs for their downstream users.

The Software Package Data Exchange® (SPDX®) specification[19] defines a standard data format for communicating the component and metadata information associated with software packages. An SPDX document can be associated with a set of software packages, files, or snippets and contains information about the software in the SPDX format described in this specification. SPDX is recognized internationally for SBOM applications.

SBOMs can be obtained in a variety of ways. For supplier-originated software, contractual terms can be used to ensure that SBOMs are securely delivered and managed with the associated software. There are many possible SBOM delivery mechanisms, including[20]:

- A URL in product literature or packaging, or as part of a Manufacturer Usage Description (MUD) [RFC 8520].
- A manifest in a well-known location in a software repository package.
- A publish/subscribe system where the software consumer would subscribe to a supplier service for updates that would be published.

In addition, Software Composition Analysis (SCA) tools can be used to determine all underlying components of a software system and identify at least the public known (open source) components. Where needed, SCA tools can also be used to generate an SBOM for custom code.

[19] Software Package Data Exchange® (SPDX®) specification, https://www.iso.org/standard/81870.html
[20] Sharing and Exchanging SBOMs, NTIA Multistakeholder Process on Software Component Transparency, https://www.ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf

With an accurate and complete SBOM-based inventory of software for a system, vulnerability management tools can then be used to map vulnerabilities to specific software components to assess risk and manage remediation.

7.2.2 Software-Controlled Hardware

The 5GC packet network infrastructure is well suited to deployment scenarios where server platforms are used to enable software implementations of complex 5G control and management functions.

In the context of a 5G assured network, we define a server platform as a type of software-controlled hardware component where the hardware assembly includes:

- One or more CPUs and associated firmware to provide compute functions.
- Compute-accessible resources such as timers, clocks, and other system controllers.
- Input/output controller(s).
- Network interface controller(s) (optionally).
- Memory and/or storage components (optionally).

A server platform typically operates in conjunction with an Operating System (OS).

Server platforms can be susceptible to a wide variety of vulnerabilities. Specifically, supply chain interception may occur and can result in the physical replacement or modification of firmware or hardware with malicious versions. These malicious modifications may not affect the intended functionality of the server platform. Instead, the modifications may lay dormant in the system until triggered by a cybersecurity attack. These modifications may then facilitate the attack by:

- Enabling a backdoor or other access to the system.
- Compromising built in security functions.
- Enabling persistence of malicious code.
- Supporting privilege escalation of malicious code.
- Supporting defense evasion.
- Enabling credential access and compromise.
- Supporting the lateral movement of malicious code.
- Supporting data collection/theft and exfiltration of the data.
- Enabling system control via the malicious code.

To mitigate these supply chain compromises of server platforms, it is useful to be able to attest to the platform's integrity and authenticity during normal operation. This requires the server platform to have an immutable HRoT upon which a chain of trust can be built.

7.2.3 Other Hardware

A 5G network may be impacted by other hardware components that may not support HRoT but are still critical to the assurance of the 5G/SC. For example, this may include key components such as a Network Interface Card (NIC), a timing reference interface (GPS) or alarm interface.

The threat from the Other Hardware category often manifests as "availability" attribute as described in clause 6.2. Appendix B shows how this category of threat may impact the supply chain lifecycle.

7.3 Metrics and Data Associated with Components

7.3.1 SBOM

SBOM is a formal record containing the details and supply chain relationships of various components used in building software. NTIA has published *Minimum Elements for a Software Bill of Materials*[21] for use in managing the software supply chain.

The minimum elements identified by NTIA comprise three broad, interrelated areas:

- **Data Fields** – Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.
- **Automation Support** – For automatic generation and machine-readability to allow for scaling across the software ecosystem.
- **Practices and Processes** – Define the operations of SBOM requests, generation, and use including Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.

In addition to the baseline data fields noted above, NTIA recommends the use of additional Data Fields, including:

- **Hash of the Component** – When referring to a piece of software, robust identifiers are important for mapping the existence of a component to relevant sources of data, such as vulnerability data sources. A cryptographic hash would provide a foundational element to assist in this mapping, as well as helping in instances of renaming and

[21] https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom.

whitelisting. As such, a hash is a key foundation for using SBOM to have trust in the software supply chain. Nevertheless, there are some situations when a hash may not be possible or convey relatively little value.

- **Lifecycle Phase** – The data about software components can be collected at different stages in the software lifecycle, including from the software source, at build time, or after build through a binary analysis tool. Due to the unique features of each of these stages, the SBOM may have some differences depending on when and where the data was created.
- **Other Component Relationships** – SBOM's minimum elements are connected through a single type of relationship: dependency. That is, X is included in Y. This relationship is implied in the SBOM graph structure. Other types of dependency relationships can be captured, to reflect that, for example, a component is similar to some other known component, but that some changes have been made. It can be useful to track for its shared origins and content.
- **License Information** – SBOMs can convey data about the licenses for each component. This data can also allow the user or purchaser to know if the software can be used as a component of another application without creating legal risk.

It is important to note that not all software will have a complete SBOM to enable robust verification of authenticity, integrity, and to enable vulnerability tracking. In addition, SBOM is not a complete supply chain management security solution, although it plays an important role in the overall supply chain management system.

7.3.2 Hardware Metrics and Data

In general, secure tracking of hardware components can be difficult, if not impossible, because hardware-based labels can often be replicated onto non-authentic components. However, software-controlled hardware can take advantage of software-based cryptographic algorithms working with a Hardware Security Module (HSM) that can be used to attest to the module's authenticity and integrity. The HSM can be used to store measurement data to be attested at a later time.

Server platforms represent a class of software-controlled hardware that can take advantage of various technologies that can be used to create an HRoT to verify authenticity and integrity using a chain of trust rooted in an HRoT. An HRoT must be inherently trusted, and therefore must be secure by design providing a foundation on which all secure operations of a computing system depend. It contains secured and protected keys and cryptographic functions to enable such operations as a secure boot process, secure platform identification (via unique keys verified via the protected cryptographic functions), and software attestation.

NISTIR 8320 – Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases[22] explains hardware-based security techniques and technologies that can improve server platform security and data protection for cloud data centers and edge computing. Hardware-enabled security can provide a stronger foundation than one enabled by software or firmware alone. In addition, HRoT presents a smaller attack surface due to the small codebase. Existing security implementations can be enhanced by providing a base-layer, immutable hardware module that chains software and firmware verifications from the hardware all the way to the application space or specified security control.

Although there are many ways to measure platform integrity, most technologies center around the use of a chain of trust rooted in hardware that is used to store measurement data to be attested at a later point in time.

An HRoT can be implemented using a variety of technologies. NISTIR 8320 uses the term HSM to refer to "a physical computing device that safeguards and manages cryptographic keys and provides cryptographic processing." An HSM typically hosts cryptographic operations such as encryption, decryption, and signature generation/verification. Many implementations provide hardware-accelerated mechanisms for cryptographic operations.

NISTIR 8320 also references the Trusted Platform Module (TPM) as a special type of HSM that can generate cryptographic keys and protect small amounts of sensitive information, such as passwords, cryptographic keys, and cryptographic hash measurements. The TPM can be integrated with server platforms, client devices, and other products.

In addition, many applications utilize a Trusted Execution Environment (TEE) to create an HRoT. A TEE is an isolated execution environment providing security features such as isolated execution to enable higher levels of application integrity and confidentiality

In subsequent text, we will use the term HRoT to refer to any technology that provides the necessary capabilities to create a hardware-rooted chain of trust.

[22] https://csrc.nist.gov/publications/detail/nistir/8320/draft

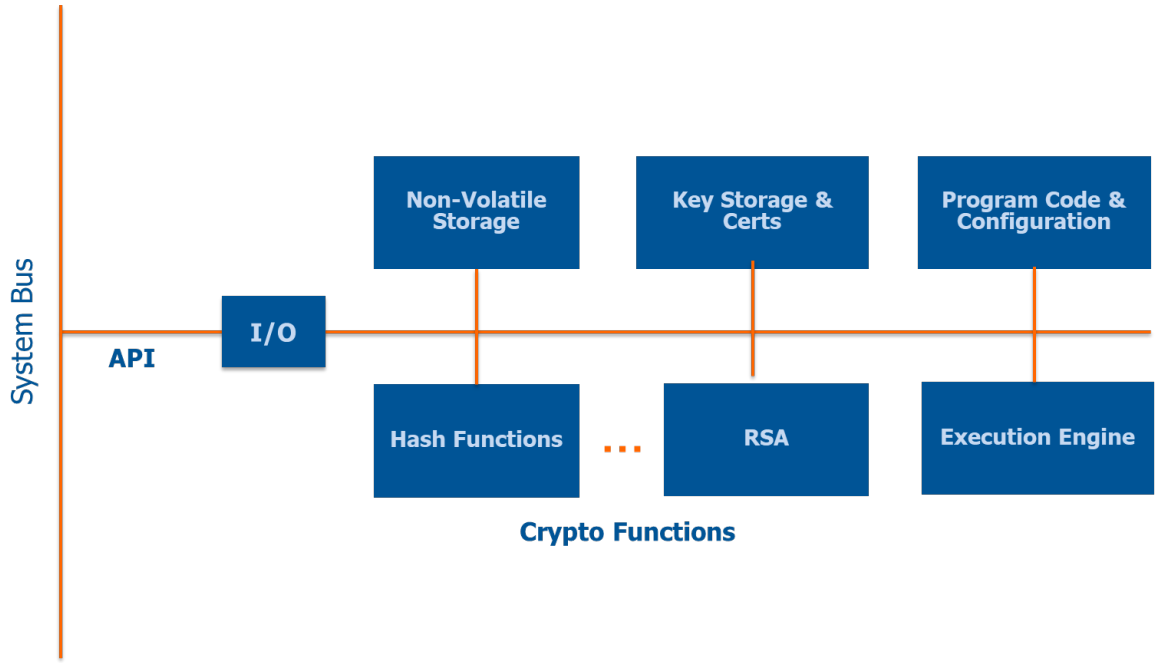


Figure 7.3-1 Generic HRoT Instance

Key storage in an HRoT technology typically includes a public/private key pair built into the hardware (e.g., an Endorsement Key (EK)) that is unique to a specific hardware instance and may be signed by a trusted Certification Authority (CA). The public key can be used as a component identifier, which can then be used to verify the identity and authenticity of at least the embedded HRoT function into the server platform. In some cases, simpler modules may have an identifier and associated shared key for this purpose. The HRoT can also store other key pairs or shared keys used for other functions such as attestation.

The HRoT implementation may also include a measurement function to enable information about the software, hardware, and configuration of a system to be collected and digested. Hash function can be used to fingerprint an executable, an executable plus its input data, or a sequence of such files. An external system then verifies the authenticity of the system by authenticating the embedded HRoT identity credentials. This can be done by verifying the certificate stored in the module as signed by a trusted CA or the identity through a shared key.

Once the server platform embedded HRoT is verified for authenticity and integrity, a chain of trust can be created to verify the entire server platform up to the application software (the appliance).

Figure 7.3-2 Chain of Trust

First, the platform manufacturer permanently builds an HRoT technology onto the server platform, creates the certificates, and binds it to the HRoT keys. A signing service then provides a platform certificate that cryptographically binds the platform to the HRoT. Finally, the system integrator creates an appliance certificate and binds it to the platform certificate.

Remote attestation servers can then be used to periodically verify the chain of certificates to ensure the ongoing integrity of the platform and associated appliance. Further, these certificates can be linked to normal inventory processes to securely track server platforms.

7.3.3 Key Characteristics of Supply Chain Metrics

Although SBOM and HRoT are significantly different mechanisms, they share many of the same cryptographic methods and facilitate the same end goals. The table below compares them relative to the key characteristics of interest in supply chain management.

KEY CHARACTERISTICS	SBOM	HRoT
Authenticity	Public Key Infrastructure (PKI) allows for signing files and packages.	Embedded credentials allows/enables HRoT to be signed.
Integrity	Signed SBOM file(s) allow to verify the integrity of the file.	Resulting chain of trust upward allows elements of the hardware, firmware, and software to be verified for integrity using remote attestation.
Immutability	Using digital hashes of the signed software packages and embedding them in the SBOM allows to link the metadata in	HRoT EKs are immutably stored in a tamper-resistant HSM.

	the SBOM with the executable code.	
Verifiability	Leverage PKI infrastructure provided signing identity can be verified.	Embedded credentials allow verification of the signing identity.
Support for Nested/Hierarchical Structures	SBOM can link to sub structures or files external or embedded to the root component tree.	HRoT chain of trust enables HRoT to support nested/hierarchical layers of hardware and software, particularly with remote attestation.

7.4 Supply Chain Threats

A specific supply chain threat will be dependent on a number of factors such as the category of component and the specific lifecycle function being performed on that component. These factors avail different vulnerabilities, which translate in different threats.

In order to facilitate a robust analysis of threats, the supply chain model is used as a framework. For this analysis, we replace the generic flow of components with the supply chain lifecycle view since components in a supply chain will flow through their lifecycle.

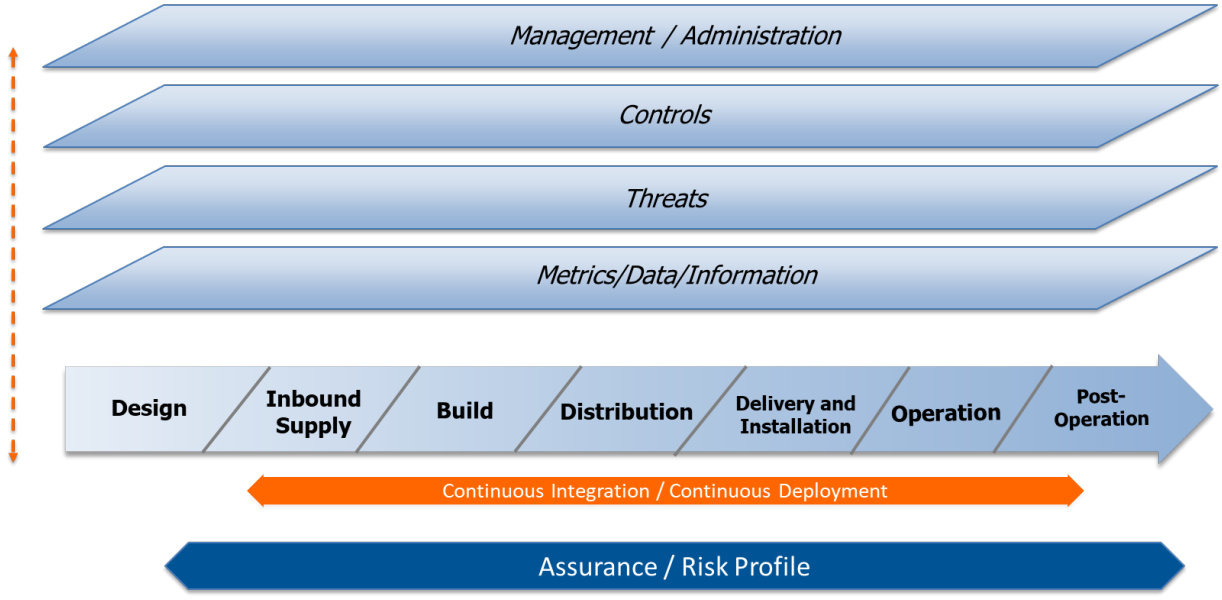


Figure 7.4-1 Supply Chain Model Merged with Lifecycle Functions

This representation of the model (as shown in Figure 7.3-1) allows us to look more closely at each lifecycle function and identify specific threats based on that function for each category of

component. Appendix B lists identified threats for each of the lifecycle functions for each category of component (as described in Section 6.4).

Generally speaking, the threats identified in Appendix B reflect cybersecurity attacks on individual functions within the component lifecycle. In that sense, it is clear that the vendor and integrator level of cybersecurity "hygiene" (e.g., the robustness of cybersecurity controls) plays a major role in mitigating supply chain attacks.

The Management/Administrative layer in the supply chain model (Figure 6.3-1) exposes threats that are not specific to a lifecycle function, but rather spans the breath of the supply chain. Management/Administration-based threats include those associated with supply chain procurement and contracting, social/people-based training and processes, and operational supply chain processes. These threats are also listed in Appendix B.

7.5 Supply Chain Controls

Appendix C mirrors the structure of Appendix B by providing specific controls and mitigations for the threats identified in Appendix B. The identified controls and mitigations are organized into tables for each lifecycle function and for each of the basic component types. In addition, controls and mitigations are listed in the Management and Administration layer of the supply chain model. These controls and mitigations tend to apply across most lifecycle functions.

The controls and mitigations listed in Appendix C will drive many of the many of the requirements provided in Section 8 of this document.

7.6 Summary of Supply Chain Vulnerability Analysis

In this analysis of Supply Chain vulnerabilities, we explored a number of key areas where focused attention can help mitigate the threats associated with these vulnerabilities. As noted in Section 7.1, there are operational cybersecurity controls and architectural constructs that can be used to help mitigate certain supply chain threats.

Vulnerabilities create threats that contribute to risk. Assurance is the process in which we quantify and manage contextual risks based on threat vectors exposed by vulnerabilities in process and data across the supply chain ecosystem.

In Section 7 of this document, we analyzed vulnerabilities and identified four areas in the supply chain where focus can be placed to manage and mitigate the associated threats. Specifically:

1. Methods to verify the identity/authenticity and integrity of software and software-controlled hardware components of an operational system. These methods include the use of SBOM and HRoT and enable vulnerability tracking and component verification

back to the signing source or producer of the component. This provides a top-level verification across the Distribution, Delivery and Installation and Operational phases of the component and system lifecycle.

2. Robust secure Design, Inbound Supply, and Build processes to ensure that the "distribution-ready" component includes necessary cybersecurity mechanisms and is built with integrity.
3. E2E supply chain lifecycle cybersecurity hygiene as deployed by suppliers, vendors, and integrators to help ensure that components have not been tampered or modified with malicious intent.
4. Robust Management and Administrative processes across all lifecycle functions to help ensure procurement and contracting, social/people-based training and processes, and operational supply chain processes are robust against supply chain threats.

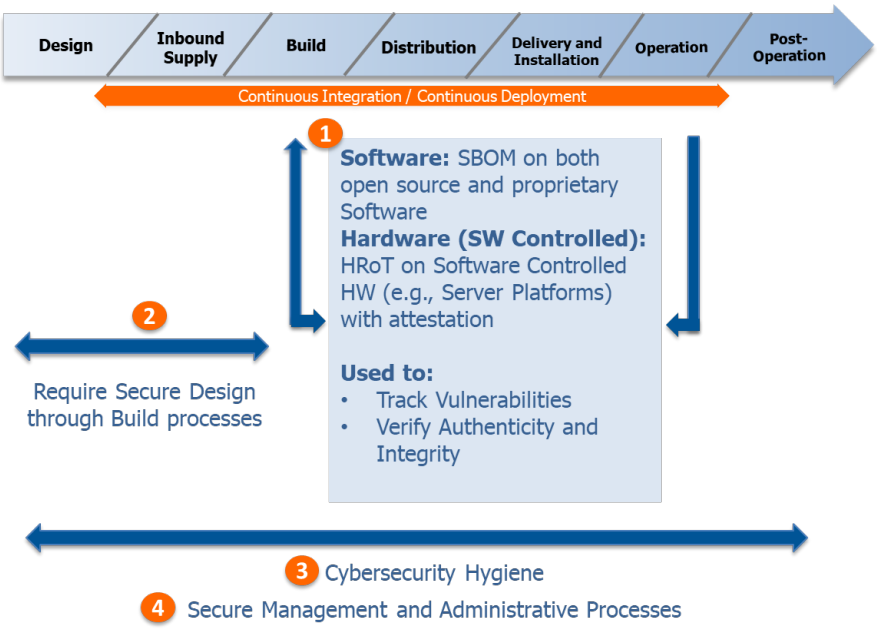


Figure 7.6-1 Supply Chain Vulnerability – Key Areas

The following section of this document will organize supply chain requirements based on these identified key areas.

8. Requirements

Requirements in this section apply to the "5G Supply Chain for Application in 5G Assured Networks." Network-related operational security aspects are not in scope but would generally be required for an assured network.

These requirements are intended for use by a number of different actors within a communication system. These actors include:

- **Users** can include an enterprise, agency (e.g., US Department of Defense), or an individual that has a need to exchange information over a network segment where the supporting supply chain is assured at a defined agreeable level.
- **Network operators** can include traditional network service providers (common for public networks) or an enterprise IT organization (common for private networks). In addition, a network operator can be a virtual network operator, which may lease physical network facilities and features from a facility-based network operator.
- **Suppliers, vendors, and integrators** include the set of organizations that produce, distribute, and/or integrate components used in the target network.

From a user's perspective, an E2E connection likely traverses many different network segments, each of which may be managed by different network operators. A segment would be comprised of the network elements supporting both data and control planes, along with the associated operations systems. High-assurance users would want to ensure that the networks used for high-assurance communication utilize an assured supply chain. To do this, the user of a network service may want the user agreement or contract provided by the network operator to include an assertion about the level of supply chain assurance that is being provided.

The network operator asserting a level of supply chain assurance is referred to as the "responsible entity" in this specification. The responsible entity can be a network service provider (common for public networks), an enterprise IT organization (common for private networks), or the entity offering the service, which may outsource network facilities (e.g., a Mobile Virtual Network Operator (MVNO)). An MVNO offers a service but relies on a network provider to manages/deploy the service.

The responsible entity for a network service would verify that all components needed in the network segment meet supply chain requirements for the advertised level of assurance. The responsible entities would decide first on the specific level of assurance desired. A risk analysis would then be done to identify critical network components appropriate for the desired level of assurance. Components included in this analysis are defined in Section 6.4: Types of Components.

Based on the identification of critical components consistent with an established assurance level, the responsible entity would place requirements on the supply chain of the target network segment and verify these requirements on suppliers, vendors, and integrators, including “internal” development and management functions as needed. The responsible entity attesting to the supply chain of an assured network must have sufficient control over all in-scope components to suitably verify this claim for a specific level of assurance. Explicit requirements are documented in this section of the document. As such, when using this document with suppliers, the responsible entity would:

- Specify an assurance level that the supplier must comply with.
- Specify which identified critical components apply to the supplier.
- Specify this document as part of the purchase agreement, along with any desired exceptions and/or additions.

It is expected that components provided by suppliers, vendors, and integrators are contractually specified for meeting an assurance level. This document does not prescribe the specific method that should be used for enforcing these contractual obligations for measuring compliance with this specification. Nevertheless, it is expected that requirements are met using best practices and standards that address the specific requirements. In addition, it is understood that this specification provides a baseline upon which requirements may be waived or added as indicated in contractual terms and conditions.

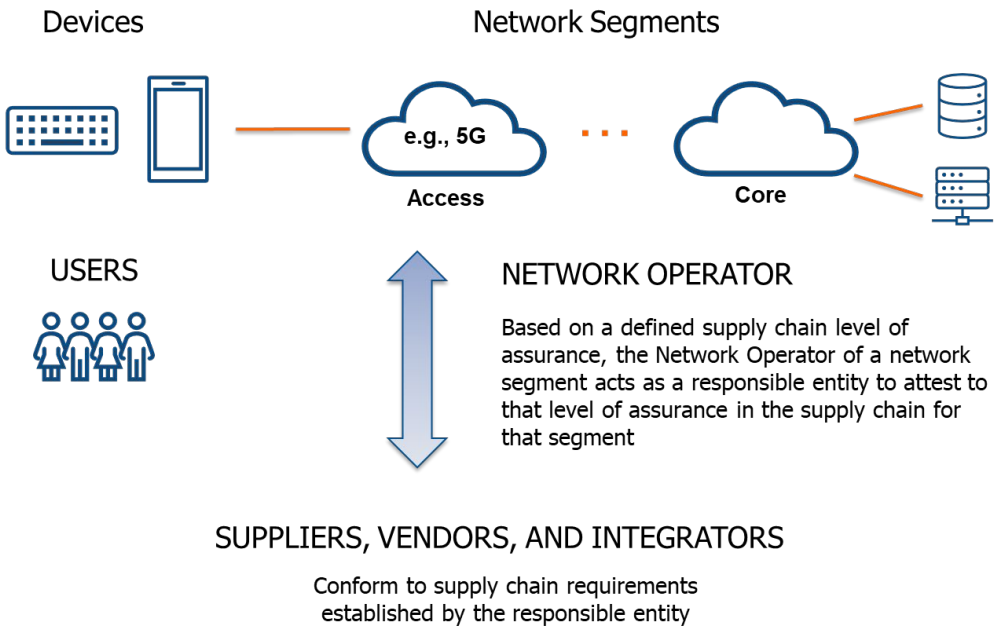


Figure 8.0 – Supply Chain Assurance Actors

This document defines three levels of assurance as follows:

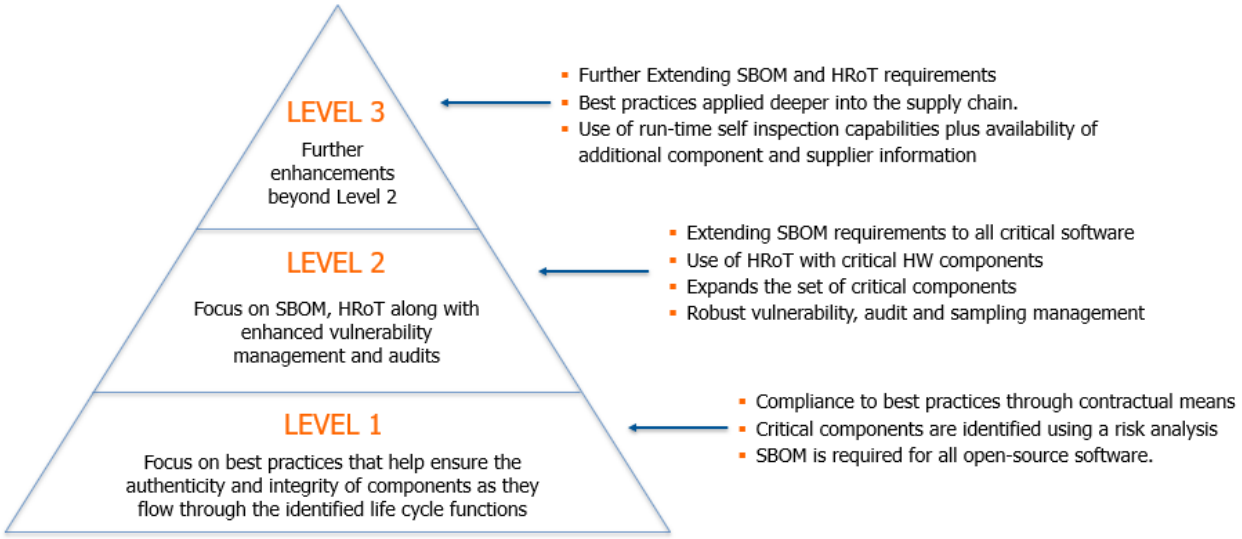
LEVEL 1 –
Level 1 supply chain assurance requirements lay the groundwork for a high assurance supply chain. This level of assurance focuses on implementing best practices that help ensure the authenticity and integrity of components as they flow through the identified lifecycle functions as deployed in the target network segment that would be assured. At this initial level of assurance, it's important to know what is deployed in the network and knowing where its operating. Compliance to best practices is established through contractual terms and conditions which are actively managed on an ongoing basis. Critical components are identified using a risk analysis of the deployed network instance. SBOM is required for all open source software.

LEVEL 2 –
Level 2 expands the breadth of level 1 capabilities by:

- Extending SBOM requirements to all critical software in the network with supplier-authored SBOMs with globally unique identifiers.
- Use of HRoT with critical hardware components (e.g., chipsets).
- Expanding the set of critical components deeper in the supply chain for critical applications.
- Requiring a more formal and complete vulnerability-management process.
- Audits, random sampled inspections, and other operational verification mechanisms may be used to continuously monitor compliance to this level of assurance.

LEVEL 3 –
Level 3 further expands the breadth of level 2 capabilities by:

- Extending SBOM requirements to all software in the network.
- Extending the use of HRoT to software stack attestation.
- Best practices are mandated down multiple layers in the supply chain hierarchy to the producer of all software in use and all critical software-controlled hardware components.
- Use of runtime self-inspection capabilities.
- One or more additional levels of component and supplier information may be required including:
    - Additional HRoT-based metadata.
    - Increased information sharing and reporting frequency, including information about development lifecycle activities, locations, and actors.
    - Proof of IV&V, or standards compliance.
    - Enhanced tracking, inspection, or verification techniques.



Each requirement will be numbered using the form RQ - "subsection number." "requirement number." The subsection number represents the subsection where the requirement is described.

Requirement #	Description	L1	L2	L3
RQ-n.n	Description of the requirement to be met.			

8.1 Software and Software-Controlled Hardware Requirements

Requirement #	Description	L1	L2	L3
RQ-1.1	Critical software and critical software-controlled hardware components are identified based on an overall risk analysis for the target network segment.	√	√	√
RQ-1.2	Component hardware and software composition inventory and component relationships are maintained and accurate with verifiable component provenance and integrity.	√	√	√
RQ-1.3	Vulnerability management processes are in place to continuously identify, evaluate, report, and mitigate security vulnerabilities associated with components.		√	√

Many existing industry-standard risk-analysis frameworks can be used to meet this requirement.

To assist in network architecture security risk assessments, ATIS has developed an Architectural Risk Analysis (ARA) process to identify the security gaps associated with a specific application, system, and network architecture, along with the relative risk, in order to prioritize the deployment of necessary controls and mitigations. The ARA methodology involves defining solution assets and associated attack surfaces, assessing the risk to each asset, and assessing how well the associated threats are mitigated through security controls. Using this analysis, specific assets can be considered for "critical component" designation.

The ARA process is documented in a variety of ATIS reports:

- An overview presentation of the application of the ARA to a network scenario is provided at https://access.atis.org/apps/group_public/download.php/55928/cybersec-2020-00066R000.pdf.
- An Architectural Risk Analysis for Internet of Things (IoT) Services https://access.atis.org/apps/group_public/download.php/46163/ATIS-I-0000072.pdf.
- Cybersecurity Architectural Risk Analysis Process https://access.atis.org/apps/group_public/download.php/35401/ATIS-I-0000057.zip.

The end goal of the following component related requirements is to create an operating environment where:

- Component hardware and software composition inventory is accurate.
- Component provenance is verifiable and trusted.
- Integrity is verifiable.

8.1.1 Software

This section will address methods to verify the identity/authenticity and integrity of software components of an operational system (the top of the primary supply chain of interest). These methods enable vulnerability tracking and component verification of integrity and authenticity back to the source or creator of the software component. This information provides a top-level verification across the Distribution, Delivery and Installation, and Operational phases of the component and system lifecycle.

Within the industry, the May 12, 2021, Executive Order[23] on Improving the Nation's Cybersecurity (EO) directed the Secretary of Commerce, acting through the Director of NIST, to issue guidance identifying practices that enhance the security of the software supply chain.

[23] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

The EO specifically requires that, for federal systems, a supplier will provide to the purchaser an SBOM for each product directly or by publishing it on a public website. The EO further specifies the development of minimum requirements that an SBOM shall meet in order to enable vulnerability tracking and component verification of integrity and authenticity back to the software component's producer.

Consistent with U.S. governmental guidance, this section identifies applicable SBOM requirements within the scope of this document.

For open source software, components are usually managed in complex ecosystems that have their own authoritative systems (e.g., package managers such as npm). Commercial developers often have an internal software management system or tracking of software branches across builds, but this may not extend outside the organization in a usable fashion.

We understand that when authoritative upstream SBOMs are not available, suppliers may create "best-effort" SBOMs using discovery and scanning tools or obtain upstream component metadata from alternative sources. However, this may introduce its own set of risks and may involve some amount of manual configuration. The long-term goal is for all software to have an associated SBOM where the supplier is also the author of the SBOM and where the creation and signing of the SBOM can be done using automated tools, minimizing cost and impact to the development processes.

Requirement #	Description	L1	L2	L3
RQ-1.4	An SBOM list of software in use is provided by the software supplier for all open source software.	√	√	√
RQ-1.5	For proprietary software, the vendor maintains the software composition of its products consistent with SBOM requirements and has processes in place to traverse the lineage when a vulnerability is identified, report vulnerabilities to the users of the product, and verify software integrity.	√	√	√
RQ-1.6	An SBOM list of software in use is provided by the software supplier for all software (e.g., proprietary and open source) associated with an identified critical component.		√	√
RQ-1.7	An SBOM list of software in use is provided by the software supplier for all software.			√

The term “software in use” means the software of interest that exists in the system as part of the executable code. Software that has been licensed to an entity but never loaded into executable memory is not “in use.”

In RQ-1.4, this requires the software supplier integrating open source software to generate an SBOM for open source software that does not have a supplier-authored SBOM.

SBOM Attributes:

Requirement #	Description	L1	L2	L3
RQ-1.8	The supplied SBOM is provided using a standard format that is both machine and human readable and that can be easily parsed (e.g., XML, JSON).	√	√	√
RQ-1.9	The supplier in the associated SBOM data object is the author of the SBOM.		√	√
RQ-1.10	The supplied SBOM file is digitally signed by the supplier to ensure the integrity and authenticity of the SBOM data object.	√	√	√

One common method for digitally signing a data object is through the use of a standard cryptographic certificate (e.g., X.509 digital certificate). Certificates can be generated and signed by a CA for better level of trust but can be self-signed for localized self-assertion of trust requirements.

“sigstore” is an example of a new standard for signing, verifying, and protecting software. This industry collaborative platform utilizes automatic key management and transparent ledger technology to enable anyone to find and verify signatures, and to check whether someone has changed the source code, the build platform, or the artifact repository.

SBOM Lifecycle

Requirement #	Description	L1	L2	L3
RQ-1.11	For provided SBOMs, the supplier also provides an updated SBOM as part of every code release, each patch, and/or update.	√	√	√
RQ-1.12	The supplied SBOM metadata is immutably linked to the delivered software.	√	√	√

SBOM Required Information Parameters

Requirement #	Description	L1	L2	L3
RQ-1.13	The supplied SBOM metadata includes the following: • Author Name • Timestamp • Supplier Name • Component Name • Version String • Component Hash • Unique Identifier • Relationship	√	√	√
RQ-1.14	The identity of the SBOM author, supplier, and associated software product is globally unique.		√	√

8.1.2 Software-Controlled Hardware Requirements

This section will address methods to verify the identity/authenticity and integrity of software-controlled hardware components of an operational product (the top of the primary supply chain of interest). These methods generally utilize hardware-centric tamper-resistant techniques to enable isolated API-based access to cryptographic, compute, and storage functions to enable protected cryptographic processing and key storage (commonly referred to as an HSM or TEE). This technology can be used as an HRoT. By storing unique keys and associated cryptographic functions in an HRoT, hardware identity/authenticity can be verified back to the signing source of the component. This provides a top-level verification across the Distribution, Delivery and Installation and Operational phases of the component and system lifecycle. In addition, embedded firmware and software in a software-controlled hardware component that utilizes a HRoT can be used to securely attest firmware and software up through the software stack running on the specific software-controlled hardware component.

Because this document addresses assured 5G networks, an operational product refers to network functions, transport products, and associated operations systems needed to manage these functions and products.

Requirement #	Description	L1	L2	L3
RQ-1.15	Critical software-controlled hardware products utilize a hardware-centric tamper-resistant technology to enable isolated API-based access to cryptographic, compute, and storage functions to enable protected cryptographic processing and key storage creating an HRoT.		√	√
RQ-1.16	Critical software-controlled hardware products utilize its HRoT to assert a unique cryptographically verifiable identity.		√	√

It is not sufficient for a software-controlled hardware product to simply have a unique identifier securely stored in hardware. To prevent replication attacks, the identifier should be cryptographically verifiable, too. For example, the unique identifier might be a public key that can be verified against the associated private key stored in the component's HRoT.

A specific software-controlled product such as a "blade" or circuit pack may include a TEE and multiple HSMs because this product may have multiple hardware-controlled software components. For example, each CPU and software-controlled "controller"/chipset may have its own integrated HSM or TEE for use in attesting to the authenticity and integrity of that component. In addition, the product may have a non-integrated HSM or TEE that may be used in attesting to the authenticity and integrity of the product itself. Any of these could be used for higher-level software attestation based on security considerations.

Requirement #	Description	L1	L2	L3
RQ-1.17	Critical software-controlled hardware products utilize an HRoT integrated into the product to create a chain of trust to enable remote attestation of the product's software up to the OS level in the software stack.			√
RQ-1.18	Critical software-controlled hardware products provide the following metadata immutably linked to the product's cryptographically verifiable identifier: • Component name • Component version string • Component supplier • Manufacturing and integration site(s) • Metadata author • Metadata timestamp			√

8.2 Secure Design Through Build

This section will address methods to ensure the integrity of components from the design phase to the build phase of the development process.

Requirement #	Description	L1	L2	L3
RQ-2.1	Software is developed using fundamental, sound, and secure software development practices based on an established security framework.	√	√	√

For example, the NIST Special Publication (SP) 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities,* along with its listed references, can provide a basis for secure software development.

8.2.1 Design Phase Requirements

Design-based requirements include those associated with concept development, requirements, component architecture, and the design phases of the lifecycle.

Requirement #	Description	L1	L2	L3
RQ-2.2	Hardware and software utilizes design and security best practices and processes in component and product design.	√	√	√
RQ-2.3	A security strategy and risk assessment is performed in the component and product design phase.	√	√	√
RQ-2.4	Components and products are designed where possible to support architectural constructs that mitigate supply chain attacks (e.g., network segregation and zero-trust mechanisms between assets/functions and resources).	√	√	√

8.2.2 Inbound Supply Requirements

Inbound supply-based requirements include those associated with acquisition of the various types of components, including open source and proprietary software, software-controlled hardware, and other types of hardware in support of a build process that creates a new component or product.

Requirement #	Description	L1	L2	L3
RQ-2.5	Data objects input into the build process utilize information security techniques to ensure both the integrity and authenticity of these data objects as the build process acquires them.	√	√	√
RQ-2.6	Software data objects input into the design process are subject to scans to identify potential malware prior to use in the build process.	√	√	√
RQ-2.7	Secure software distribution mechanisms are used to distribute software objects.	√	√	√
RQ-2.8	All physical components are tracked during shipping and use verified shippers.	√	√	√
RQ-2.9	All identified critical hardware components have assigned identifiers physically displayed on the components (e.g., barcodes) that are used to verify the identity of the component prior to use in a subsequent build process.	√	√	√
RQ-2.10	All identified critical hardware components are subject to inspection and sampled “stress tests” against component specifications.	√	√	√

8.2.3 Build Requirements

Build requirements include those associated with manufacturing, code creation, integration of subcomponents, assembly, and test.

Requirement #	Description	L1	L2	L3
RQ-2.11	Both software and hardware development environment tools are up to date and subject to audits/scans to ensure the integrity of build tools.	√	√	√
RQ-2.12	Hardware-based manufacturing tools are subject to regular calibration to ensure their operational integrity.	√	√	√
RQ-2.13	The build physical environment is secured.	√	√	√
RQ-2.14	The build environment utilizes secure process and product management processes.	√	√	√

RQ-2.15	The build environment utilizes secure data management systems and processes.	√	√	√

8.3 Cybersecurity Hygiene in Post Build Supply Chain Lifecycle Functions

8.3.1 Distribution Requirements

Distribution-based controls and mitigations include those associated with packaging, storage, warehousing, staging, and configuration of products for use in an assured network.

Requirement #	Description	L1	L2	L3
RQ-3.1	Storage and distribution of data objects utilize information security techniques to ensure both the integrity and authenticity of these data objects.	√	√	√
RQ-3.2	Secure software distribution mechanisms are used to distribute software objects.	√	√	√
RQ-3.3	All physical components are tracked during shipping and use verified shippers.	√	√	√
RQ-3.4	All identified critical hardware components have assigned identifiers physically displayed on the components (e.g., barcodes) that are used to verify the identity of the component prior to use in a subsequent build process.	√	√	√
RQ-3.5	All identified critical hardware components are subject to inspection and sampled “stress tests” against component specifications.	√	√	√

8.3.2 Delivery and Installation Requirements

Delivery and installation-based requirements include those associated with customer receipt, installation, provisioning, and configuration of a product in support of an assured network.

Requirement #	Description	L1	L2	L3
RQ-3.6	Installation processes include security-based integration and system tests.	√	√	√

RQ-3.7	Installation and integration procedures are reviewed to ensure both product and process security mechanisms are in place.	√	√	√
RQ-3.8	All identified critical hardware components are subject to random sampled inspection against component specifications based on manual or technology-assisted methods.		√	√

8.3.3 Operations Requirements

Operations-based requirements include those associated with operations, maintenance and repair, and software updates in an operational network.

Requirement #	Description	L1	L2	L3
RQ-3.9	Software in the operational network utilizes secure update processes with secure procedures and capabilities.	√	√	√
RQ-3.10	Software asset management in the network (both operational and corporate) uses available SBOM information to monitor for reported vulnerabilities.		√	√
RQ-3.11	Critical software-controlled hardware products in the operational network utilizes its HRoT to create a chain of trust to enable remote attestation of the product's software up to the OS level in the software stack.		√	√
RQ-3.12	Network product architectures in the operational network utilize security capabilities known to mitigate supply chain and other security attacks (e.g., network segregation and use of zero-trust mechanisms between critical internal functions).		√	√

8.3.4 Post-Operations Requirements

Post-operation-based requirements include those associated with repurposing, programmability for reuse, and retirement of components previously used in an operational network.

Requirement #	Description	L1	L2	L3
RQ-3.13	Operational software-controlled hardware components are subject to data-clearing processes to protect embedded proprietary information and capabilities.	√	√	√

8.4 Management and Administrative Requirements

Management/administration-based requirements include those associated with supply chain procurement and contracting, social/people-based training and processes, and operational supply chain processes.

8.4.1 Procurement and Contracting

Requirement #	Description	L1	L2	L3
RQ-4.1	Component procurement utilizes qualified vendors on preferred vendor lists.	√	√	√
RQ-4.2	Vendors and integrators providing software and hardware-controlled software directly to the network operator (Tier 1 suppliers) asserting a level of supply chain assurance comply with requirements in this specification as enforced through contractual terms and conditions.	√	√	√
RQ-4.3	Software suppliers to Tier 1 suppliers meet secure software requirement RQ-2.1 and build requirements in 8.2.3.			√

Specifically, policies, and processes should be in place to ensure that no supplier or third-party components are restricted for use by applicable laws or regulations. In addition, procurement can include other companies on such a list as determined by company policies. Generally speaking, hardware components included in the product offering should be acquired from original equipment manufacturers or licensed resellers.

Vendors and integrators that source products and services directly to the network operator asserting a level of supply chain assurance must meet the requirements as documented in this specification. We have defined this set of suppliers as Tier 1 suppliers (see Section 3.2). These Tier 1 suppliers can acquire components from other upstream suppliers in the production of Tier 1 products. These suppliers conform to requirements as applicable related to the creation of SBOM, HRoT, and inbound-supply-related requirements.

Requirement #	Description	L1	L2	L3
RQ-4.4	Component procurement processes use supplier diversity to avoid single sources where possible.	√	√	√
RQ-4.5	Vendor contracts for component procurement have terms and conditions requiring the vendor to: • Meet specific supply chain standards. • Use best practices and processes in supply chain operations (including development processes with security objectives/strategy). • Provide access to specific supply chain data artifacts as needed (e.g., the information object for components, provenance). • Provide notification of security-related vulnerabilities and events affecting components. • Include contract terms related to vendor company mergers/acquisitions and dissolvement relative to the disposition of intellectual property rights. • Provide contractual enforcement provisions (e.g., required audits, liquidated damages). • Provide ongoing vendor and contract management (and associated processes).	√	√	√

8.4.2 Social/People Training and Processes

Requirement #	Description	L1	L2	L3
RQ-4.6	Organizations utilize hiring processes that include specific hiring criteria and background checks for direct employees, contractors, and interns.	√	√	√
RQ-4.7	Organizations provide security-related onboarding, offboarding, and awareness training for direct employees, contractors and interns that includes: • Security-related policies for use of company and personal equipment/devices (in personal and business settings). • Security-related polices for access and use of company proprietary information.	√	√	√

	• Security-related policies dealing with information sharing in personal interactions with both employees and non-employees.			

8.4.3 Practices and Processes

For the following requirements, supply chain lifecycle functions include:

- Design
- Inbound
- Build
- Delivery and Installation
- Operation
- Post-Operation

These functions are defined in Section 6.1 of this document.

Critical components are as identified in RQ-1.1.

Requirement #	Description	L1	L2	L3
RQ-4.8	Organizations ensure that robust, documented processes are in place for all supply chain lifecycle functions to provide: • Information security (including data access, storage, and transport). • Quality management (e.g., application of a Quality Management System (QMS)). • Organization-wide analysis and strategy for managing E2E supply chain risks. • Audit, accountability, and planning (process and program management). • Certification, accreditation, and security assessments as required. • Physical facility security and admittance policies. • Contingency planning for emergency response, backup operations, and post-disaster recovery.	√	√	√
RQ-4.9	Organizations report the status of the processes listed in RQ-4.7 to their customers on an as-needed basis.			√

RQ-4.10	Organizations provide for the maintenance and management of information systems (e.g., servers and software tools) and production (e.g., build) equipment, systems (e.g., servers), and software tools to ensure that both hardware and software are up to date relative to security.	√	√	√

Appendix A – Future Areas of Supply Chain Development

This section identifies future considerations beyond the current scope of this document. These may include aspects not covered in this document and identification of needs or gaps that define extension to future work. For example, elements such as recommended design attributes for 5G assured networks.

It serves as a means to warehouse issues and application areas that are outside the direct scope of the 5G/SC standard.

Appendix B – Threat Tables

Design-Based Threats

Design-based threats include threats associated with concept development, requirements, architecture, and the design phases of the lifecycle.

COMPONENT CATEGORY	Design Threats

Open Source SW	• Insertion of design aspects that weaken component or system security including:
	  ○ Flawed cryptography
	  ○ Default and/or hard-coded passwords/keys
	  ○ Enable backdoor or non-authenticated access
	  ○ Compromise isolation of a cloud platform
	  ○ Create “persistence” capabilities for real-time attacks
	  ○ Exfiltration via direct access to malicious server
	  ○ Split tunneling to direct data flows to malicious server

Proprietary SW	• Insertion of design aspects that weaken component or system security • Design theft • Flawed cryptography • Default and/or hard-coded passwords/keys • Enable backdoor or non-authenticated access • Compromise isolation of a cloud platform • Create persistence capabilities for real-time attacks • Exfiltration via direct access to malicious server • Split tunneling to direct data flows to malicious server
SW-Controlled HW	• Insertion of design aspects that weaken component or system security • Design theft • Flawed cryptography • Default and/or hard-coded passwords/keys • Firmware editing
Other HW	• Materials that do not support specifications • Design manipulation

Inbound Supply-Based Threats

Inbound supply-based threats include those associated with acquisition of the various types of components, including open source and proprietary software, software-controlled hardware, and other types of hardware.

COMPONENT CATEGORY	Inbound-Supply Threats
Open Source SW	• Manipulation of source code repositories • Manipulation of source code in open source dependencies
Proprietary SW	• Compromised/infected system images (e.g., multiple cases of removable media infected at the factory) • Replacement of legitimate software with modified versions • Sales of modified/counterfeit products to legitimate distributors
SW-Controlled HW	• Sales of modified/counterfeit products to legitimate distributors
Other HW	• Sales of modified/counterfeit products to legitimate distributors

Build Environment Threats

Build environment threats include those associated with manufacturing, code creation, integration, assembly, and test.

COMPONENT CATEGORY	Build Environment Threats
Open Source SW	• Manipulation of development tools • Manipulation of development environment • Code insertion or modification to insert/enable vulnerabilities • Compromised information system security, (e.g., obscure tracking of compromised components (provenance) and credentials theft)
Proprietary SW	• Manipulation of development tools • For closed networks, insider threat: Manipulation of development environment • Code insertion or modification to insert/enable vulnerabilities • Compromised information system security, (e.g., obscure tracking of compromised components (provenance) and credentials theft)
SW-Controlled HW	• Manipulation of development tools • Manipulation of development environment • Insertion of non-authentic components • HW insertion or modification to insert/enable vulnerabilities • Compromised information system security, (e.g., obscure tracking of compromised components (provenance) and credentials theft)
Other HW	• Manipulation of development tools

	• Manipulation of development environment • Compromised information system security, (e.g., obscure tracking of compromised components (provenance) and credentials theft)

Distribution Threats

Distribution-based threats include those associated with packaging, storage, warehousing, staging, and configuration.

COMPONENT CATEGORY	Distribution Threats
Open Source SW	• Shipment interdiction • Substitution of non-authentic software • Insertion of non-secure or malicious code/configuration • Theft of SW
Proprietary SW	• Shipment interdiction • Substitution of non-authentic software • Insertion of non-secure or malicious code/configuration • Theft of SW
SW-Controlled HW	• Shipment interdiction • Substitution of non-authentic hardware • Insertion of malicious hardware function • Damage to HW • Theft of HW
Other HW	• Shipment interdiction • Substitution of non-authentic hardware • Damage to HW • Theft of HW

Delivery and Installation Threats

Delivery and installation-based threats include those associated with customer receipt, installation, provisioning, and configuration.

COMPONENT CATEGORY	Delivery and Installation Threats
Open Source SW	• Provisioning and/or configuration that compromises product security
Proprietary SW	• Provisioning and/or configuration that compromises product security
SW-Controlled HW	Delivery: • HW modification or substitution during transit

	• Insufficient transit product protection capabilities • Compromised tracking capabilities Installation: • HW modification, substitution, or insertion during installation • Improper installation techniques that may compromise availability later
Other HW	Delivery: • HW modification or substitution during transit • Insufficient transit product protection capabilities • Compromised tracking capabilities Installation: • HW modification, substitution, or insertion during installation • Improper installation techniques that may compromise availability later

Operational Threats

Operations-based threats include those associated with operations, maintenance and repair, and SW updates.

COMPONENT CATEGORY	Operational Threats
Open Source SW	• Compromised software update process (availability) • Insertion of vulnerabilities into planned updates
Proprietary SW	• Compromised software update process (availability) • Insertion of vulnerabilities into planned updates
SW-Controlled HW	• Compromised HW update process with insertion of non-authentic components or new exploitable HW functions
Other HW	• Compromised hardware update process with insertion of non-authentic components

Post-Operation Threats

Post-operation-based threats include those associated with repurposing, programmability for reuse, and retirement.

COMPONENT CATEGORY	Post-Operation Threats
Open Source SW	• Exposure of embedded proprietary information and/or capabilities • Reuse of compromised software
Proprietary SW	• Exposure of embedded proprietary information and/or capabilities

	• Reuse of compromised software
SW-Controlled HW	• Exposure of embedded proprietary information and/or capabilities • Reuse of compromised hardware
Other HW	• Reuse of compromised hardware

Management/Administration Threats

Management/administration-based threats include those associated with supply chain procurement and contracting, social/people-based training and processes, and operational supply chain processes.

COMPONENT CATEGORY	Management/Administration Threats
Procurement and Contracting	• Use of vendors not on approved vendor lists • Use of vendor products that have poor cybersecurity practices • Fraudulent claims by vendors • Inability of vendor to provide ongoing support • Lack of vendor diversity (e.g., multi-sourcing)
Social/People Training and Processes	• Insider sabotage
Supply Chain Processes	• Compromise of physical facilities: break-in with component replacement or modification • Compromise of data-tracking capabilities • Security breaches in any of the lifecycle processes

Appendix C – Controls and Mitigations Tables

Design-Based Controls and Mitigations

Design-based controls and mitigations include those associated with concept development, requirements, component architecture, and the design phases of the lifecycle.

COMPONENT CATEGORY	Design Controls and Mitigations
Open Source SW	• Application of best-in-class design and security practices and processes on product design • Creation and use of a security strategy and risk assessment, both component and architectural • Design using architectural constructs that mitigate supply chain attacks (e.g., network segregation and zero-trust mechanisms between internal resources/functions)
Proprietary SW	• Application of best-in-class design and security practices and processes on product design • Creation and use of a security strategy and risk assessment, both component and architectural • Design using architectural constructs that mitigate supply chain attacks (e.g., network segregation and zero-trust mechanisms between internal resources/functions)
SW-Controlled HW	• Application of best-in-class design and security practices and processes on product design • Creation and use of a security strategy and risk assessment, both component and architectural • Design using architectural constructs that mitigate supply chain attacks (e.g., network segregation and zero-trust mechanisms between internal resources/functions)
Other HW	• Application of best-in-class design and security practices and processes on product design • Creation and use of a security strategy and risk assessment, both components and products

Inbound Supply-Based Controls and Mitigations

Inbound supply-based controls and mitigations include those associated with acquisition of the various types of components, including open source and proprietary software, software-controlled hardware, and other types of hardware. To the extent that some components may be modules or other products that are composed of multiple basic components, the controls and mitigations noted for these components could include multiple rows in the table below.

COMPONENT CATEGORY	Inbound Supply Controls and Mitigations
Open Source SW	• Encryption/code signing (e.g., robust SBOM requirements) • Software scans to identify potential malware • Secure software and SBOM distribution mechanisms
Proprietary SW	• Encryption/code signing (e.g., robust SBOM requirements) • Software scans to identify potential malware • Secure software and SBOM distribution mechanisms
SW-Controlled HW	• Integrity tests of HW/SW via HRoT verification and other means • Product barcode scans – identity verification • Sampled stress tests against specifications • Inspection
Other HW	• Product barcode scans – identity verification • Sampled stress tests against specifications • Inspection

Build Environment Controls and Mitigations

Build environment controls and mitigations include those associated with manufacturing, code creation, integration, assembly, and test.

COMPONENT CATEGORY	Build Environment Controls and Mitigations
Open Source SW	• Software Development Environment (SDE) audits/scans and signature checks (verification of the SDE) • Secure physical environment along with robust product management processes • Secure development processes • Secure data management systems and processes
Proprietary SW	• SDE audits/scans and signature checks (verification of the SDE) • Secure physical environment along with robust product management processes • Secure development processes • Secure data management systems and processes
SW-Controlled HW	• Periodic calibration and operational integrity tests (on manufacturing tools) • Secure physical environment along with robust product management processes • Secure development processes • Secure data management systems and processes

Other HW	• Periodic calibration and operational integrity tests (on manufacturing tools) • Secure physical environment along with robust product management processes • Secure development processes • Secure data management systems and processes

Distribution Controls and Mitigations

Distribution-based controls and mitigations include those associated with packaging, storage, warehousing, staging, and configuration. To the extent that some components may be modules or other products that are composed of multiple basic components, the controls and mitigations noted for these components could include multiple rows in the table below.

COMPONENT CATEGORY	Distribution Controls and Mitigations
Open Source SW	• Secure software and SBOM distribution mechanisms • Secure storage (data management) capabilities (e.g., authentication, encryption) • Security-specific scans
Proprietary SW	• Secure software and SBOM distribution mechanisms • Secure storage (data management) capabilities (e.g., authentication, encryption) • Security-specific scans
SW-Controlled HW	• Robust tracking capabilities • Robust and secure packaging and storage processes • Inspection • Software and hardware verification tests
Other HW	• Robust tracking capabilities • Robust and secure packaging and storage processes • Inspection

Delivery and Installation Controls and Mitigations

Delivery and installation-based controls and mitigations include those associated with customer receipt, installation, provisioning, and configuration.

COMPONENT CATEGORY	Delivery and Installation Controls and Mitigations
Open Source SW	• Secure infosec capabilities (e.g., authentication, encryption) • System security-specific software/configuration scans • Security-based integration and system tests • Robust integration documentation and practices

Proprietary SW	• Secure infosec capabilities (e.g., authentication, encryption) • System security-specific software/configuration scans • Security-based integration and system tests • Robust integration documentation and practices
SW-Controlled HW	• Robust tracking capabilities • Robust transit processes • Inspection • Security-based software and hardware integration and system tests • Robust integration documentation and practices
Other HW	• Robust tracking capabilities • Robust transit processes • Inspection • Security-based integration and system tests • Robust integration documentation and practices

Operational Controls and Mitigations

Operations-based controls and mitigations include those associated with operations, maintenance and repair, and SW updates.

COMPONENT CATEGORY	Operational Controls and Mitigations
Open Source SW	• Robust update processes with secure procedures and capabilities. • Use of security capabilities known to mitigate supply chain and other security attacks (e.g., network segregation, use of zero -trust mechanisms between internal functions, etc.) • Attestation based on SBOM information on operational systems
Proprietary SW	• Robust update processes with secure procedures and capabilities. • Use of security capabilities known to mitigate supply chain and other security attacks (e.g., network segregation, use of zero-trust mechanisms between internal functions, etc.) • Attestation based on SBOM information on operational systems
SW-Controlled HW	• Robust update processes with secure procedures and capabilities. • Use of security capabilities known to mitigate supply chain and other security attacks (e.g., network segregation, use of zero-trust mechanisms between internal functions, etc.) • Attestation based on HRoT information on operational systems
Other HW	• Robust update processes with secure procedures and capabilities.

Post-Operation Controls and Mitigations

Post-operation-based controls and mitigations include those associated with repurposing, programmability for reuse, and retirement.

COMPONENT CATEGORY	Post Operation Controls and Mitigations
Open Source SW	• Processes to protect embedded proprietary information and capabilities (e.g., data-clearing operations)
Proprietary SW	• Processes to protect embedded proprietary information and capabilities (e.g., data-clearing operations)
SW-Controlled HW	• Processes to protect embedded proprietary information and capabilities, e.g., (data-clearing operations)
Other HW	• NA

Management/Administration Controls and Mitigations

Management/administration-based controls and mitigations include those associated with supply chain procurement and contracting, social/people-based training and processes, and operational supply chain processes.

CATEGORY	Management/Administration Controls and Mitigations

Procurement and Contracting	• Utilization of preferred vendor lists
	• Contractual obligations to ensure that vendors:
	  ○ Meet specific supply chain standards
	  ○ Use specific best practices and processes in supply chain operations (including development processes with security objectives/strategy)
	  ○ Provide access to specific supply chain data artifacts as needed (e.g., the information object for components, provenance)
	  ○ Notification of security related events affecting components
	  ○ Intellectual property considerations – contract terms related to vendor company mergers/acquisitions and dissolvement
	• Contractual enforcement provisions (e.g., required audits, liquidated damages)
	• Ongoing contract management (and associated processes)
	• Ongoing vendor management (and associated processes)

Social/People Training and Processes	Personnel-Centric Processes: • Hiring criteria and background checks • Awareness and training related to security

	Policies: • Security-related policies for use of company equipment/devices (e.g., in personal and business settings) • Security-related policies for use of personal equipment/devices in company spaces or for business use

Supply Chain Practices and Processes	• Ensure robust processes in place for all supply chain functions noted in the model
	• Audit, accountability, and planning (process and program Management)
	• Certification, accreditation, and security assessments
	• Physical facility security and admittance policies
	• Contingency planning for emergency response, backup operations, and post-disaster recovery
	• Incident response
	• Vulnerability management and reporting
	• Maintenance and management of:
	  ○ Information systems (e.g., servers and software tools)
	  ○ Production (e.g., build) equipment, systems (e.g., servers) and software tools

Appendix D – Example 5G Use Cases

This appendix identifies three forward-looking use cases for 5G/SCs and provides a description and a template of use case parameters, actors, threat environment, and process flows.

Note that actors in this context are stakeholders that include suppliers, acquirers, and integrators. NISTIR 7622, "Notional Supply Chain Risk Management Practices for Federal Information Systems," defines these terms as:

> *Acquirers* are stakeholders that acquire or procure a product or service.
>
> *Integrators* are an organization that customizes (e.g., combines, adds, optimizes) elements, processes, and systems. The integrator function can be performed by acquirer, integrator, or supplier.
>
> *Suppliers* are an organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain.

AR-Enabled 5G

The AR-enabled 5G use case provides a realistic distributed training platform with interoperable equipment and systems that can be rapidly integrated and deployed into ongoing training operations. The use case assumes that all equipment and software are procured via approved channels and comply with mandated security controls.

This use case features 3GPP 5G SA deployments in private network configurations in a secure indoor or outdoor setting, as well as public 5G network access.

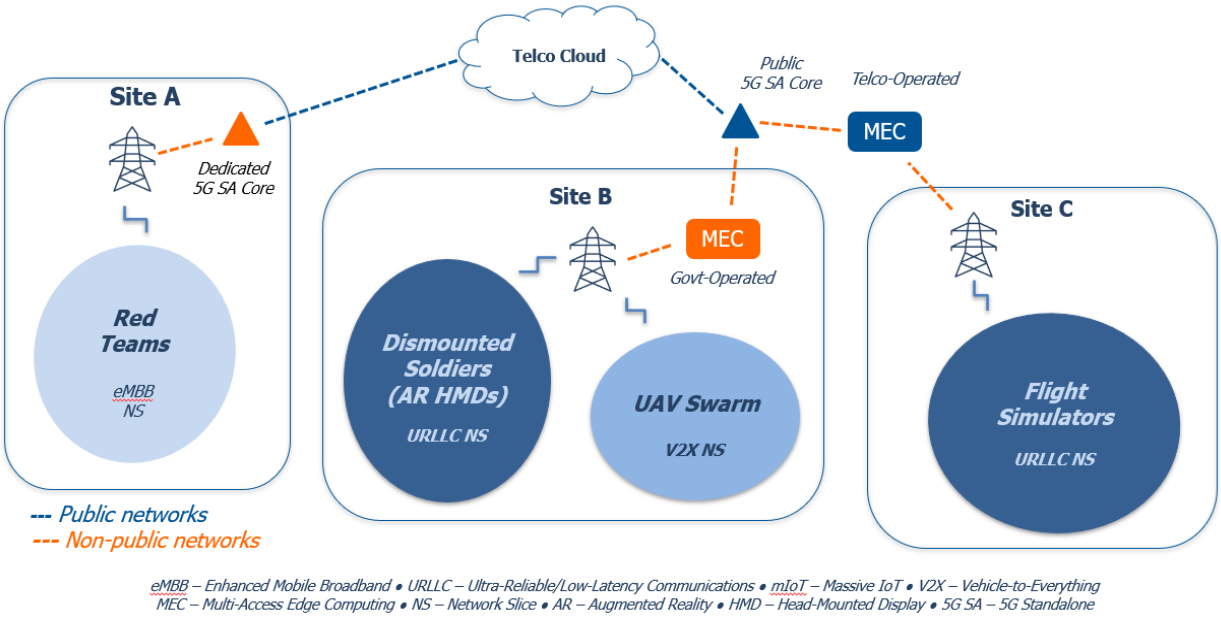


Figure D-1 AR-Enabled 5G Use Case

Description/Objective

This use case provides distributed live, virtual, and constructive simulation-based training capabilities for joint warfighting and peacekeeping scenarios conducted in real, digitally enhanced, or fully virtual environments. Separate NSs are used to securely deliver Ultra-Reliable Low Latency Communication (URLLC) for airborne assets, Vehicle to Everything (V2X) for ground-based vehicles, massive Machine-Type Communication (mMTC) for smart Electro-Optical/Infrared (EO/IR) sensors, and enhanced Mobile Broadband (eMBB) for dismounted soldiers. MEC is employed at sites with high-throughput and/or low-latency demands.

Actors

Primary actors include:

- Network service providers providing public 5G services and transport services.
- Private IT (e.g., governmental or outsourced but controlled by governmental entities) providing private 5G equipment, services, and transport.

Secondary actors include:

- Trainees (live dismounted soldiers with head-mounted displays, live pilots in flight simulators, constructive sailor entities), cyber red team.
- Command-and-Control (C2) entities, trainers/exercise operators, cloud/edge service providers.

Assumptions/Pre-conditions

The communications environment is comprised of 3GPP 5G SA deployments in private network configurations in a secure indoor or outdoor setting, as well as public 5G services.

Trainees participate in a joint training exercise. Physical attributes (e.g., RF emanation, IR imagery) and communications of all primary actors are susceptible to detection, infiltration, and attack by red team participants.

Environment

Both indoor and outdoor environments are leveraged with training centers (indoors), Military Operations on Urban Terrain (MOUT) sites (outdoors).

User Process Flow

Trainees can interact with the environment and, when applicable, receive visual/haptic feedback within "normal" delay parameters. Vehicles, munitions, and other equipment conform to expected levels of performance, mobility, lethality, power consumption, etc.

Outcome/Post Conditions

Operational training objectives aside, the technology demonstration will showcase 5G's flexibility and security features, along with cross-MEC, cross-NS handovers as actors, entities traverse the simulation environment.

Non-Terrestrial 5G for Continuity of Operations (COOP) Backhaul

The Non-Terrestrial COOP 5G use case illustrates how commercial 5G services can be delivered via an integrated 5G satellite-terrestrial network using both direct access and commercial satellite gateways.

This use case provides efficient multicast/broadcast delivery to network edges for content such as live broadcasts, group communications, MEC, and system update distribution. This deployment scenario also enables connectivity to underserved areas in tandem with terrestrial wireless and wireline networks.

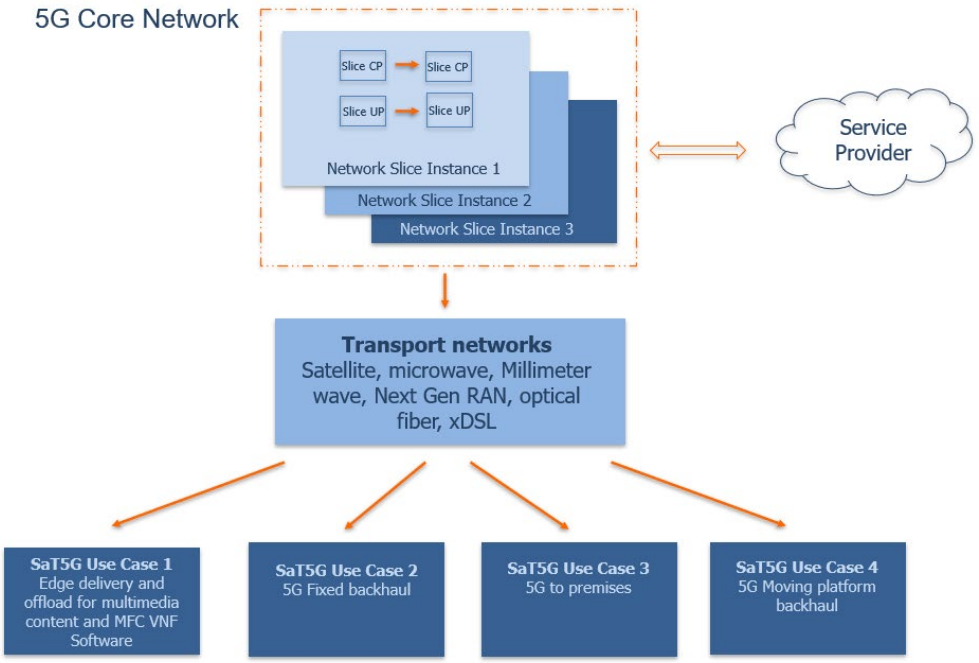


Figure D-2 Non-Terrestrial 5G for Continuity of Operations (COOP) Backhaul

Description/Objective

This use case provides commercial 5G services delivered via an integrated 5G satellite-terrestrial network using both direct access and commercial satellite gateways. This deployment scenario enables connectivity to underserved areas in tandem with terrestrial wireless and wireline networks.

Actors

Primary actors include:

- The commercial satellite service providers
- Wireless network operators
- Rural/austere-area mobile users

Secondary actors include:

- Cloud service provider(s)
- Non-3GPP network operators

Assumptions/Pre-conditions

This use case assumes integration of cross-band and licensed/unlicensed spectrum networks operated and managed by different service providers and municipal authorities.

Environment

This use case is well suited to rural or austere locations with unreliable backhaul being a single point of failure.

Process Flow

Bi-directional network traffic seamlessly hands over between terrestrial 5GSs to Non-Terrestrial Network (NTN) backup when certain extreme conditions persist. Multi-hop NTN relays may be necessary to propagate high-band signal to specific zones.

Outcome/Post-conditions

This use case highlights 5G's flexibility and the likely deployment in heterogeneous network architectures and spectrum bands with various equipment types.

5G Smart Warehouse

The 5G smart warehouse use case demonstrates how 5G networking can play a key role in a warehouse (or industrial) environment. In this case, the network is used to identify, test, and confirm warehouse and support logistics improvements to enhance the efficiency, accuracy, security, and safety of material and supply handling, management, storage, and distribution.

The specific instance illustrated describes a semi-automated warehouse where robots work alongside people. Basic tasks such as scanning barcodes and moving packages are performed by IoT devices on the network. Both stationary and mobile robots (e.g., aerial and ground-based) are used.

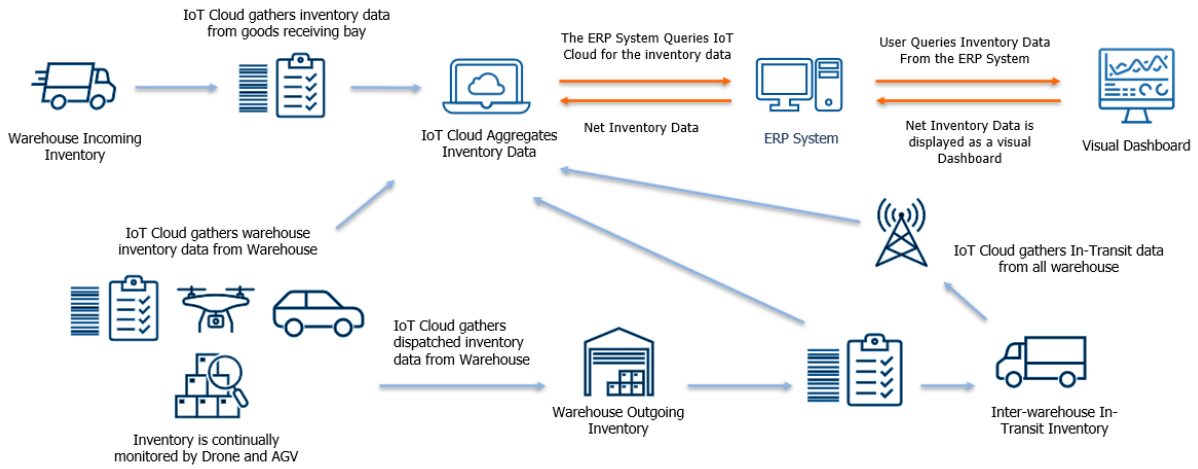


Figure D-3 5G Smart Warehouse Use Case

Description/Objective

Commercial 5G services to interconnect, control, and task up to hundreds of IoT devices (e.g., mostly single-function, intelligent autonomous robots) to efficiently perform warehousing tasks.

Actors

Primary actors include:

- Network operators
- Local IT operations that own and maintain the private 5G network in the smart warehouse
- Human warehouse managers, workers

Secondary actors include:

- Cloud/edge service provider(s)
- Non-3GPP network operators

Assumptions/Pre-conditions

This use case assumes massive deployment of IoT devices within a smart warehouse that are connected to private and commercial networks to track the movement of components, parts, devices, and systems.

Environment

This use case is well suited to smart warehouses applications deployed (e.g., across military sites) and connected to other smart warehouse locations.

Process Flow

Inventory data is centrally managed from receipt of product through dispatch from the warehouse. The IoT cloud becomes the aggregator of data, with the ability to provide dashboarding of such data to approved personnel.

Outcome/Post-conditions

This use case demonstrates the ability to maintain supply chain assurance across a large number of IoT devices and systems managed within a private network and one or more commercial networks.

Appendix E: Overview of 5GC Supply Chain Mitigation Capabilities

The 5GC is based on functional interconnections through a "common bus" approach that permits functional elements to communicate based on service definition.

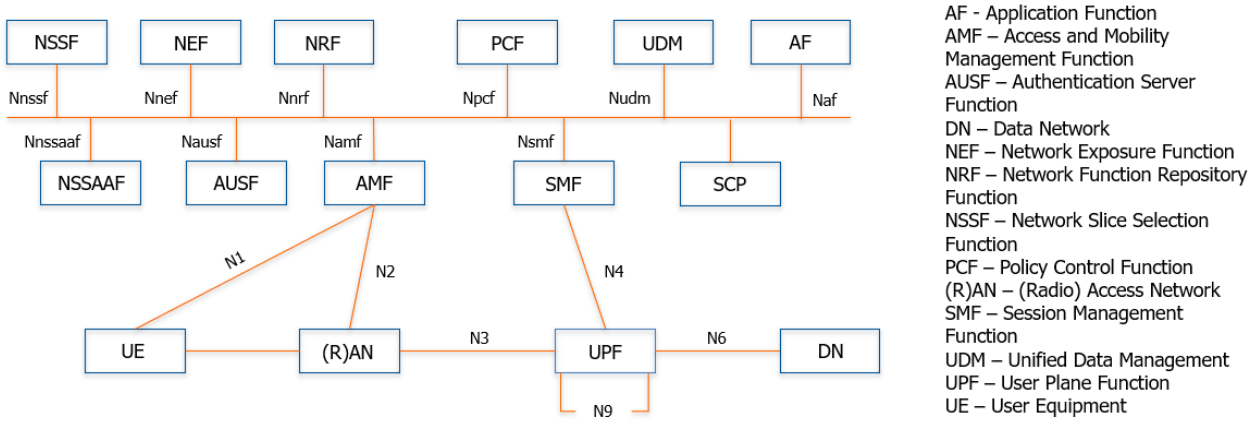


Figure E-1 5GC Service-Based Architecture

The architecture is called a service-based architecture (SBA), where key differentiators include:

- **Control Plane/User Plane (CP/UP) Split** - 5G standards require the separation of the control and user planes (traffic paths within the 5G architecture) within the network. The separation is driven by the notion that user plane and control plane functionalities are quite different given the performance characteristics of exchanging signaling messages between network control functions and the needs of a transport network that carries user/application traffic.
- **Network Slicing** - Network slicing is a fundamental new capability of 5GC that provides flexibility when deploying diverse network services and applications. A logical E2E network slice has pre-determined service capabilities, traffic characteristics, and service level agreements. It also includes the virtualized resources required to service the needs of a group of subscribers, including a dedicated User Plane Function (UPF), Session Management Function (SMF) and Policy Control Function (PCF). Key capabilities include:
    - Slice-specific authentication and authorization
    - Improvements in slice interworking with Evolved Packet Core (EPC)

The network segmentation and traffic separation provided by the above capabilities plays an important role in mitigating supply chain attacks. Network-based segregation inhibits the lateral movement of compromised function while also preventing direct system access to the internet where it is not needed. One important class of supply chain compromise is when a backdoor is inserted into the code within the supply chain. However, to activate the backdoor,

the malicious code must first contact a command-and-control server someplace on the internet. As such, preventing internet access when not functionally necessary, or by providing API gateway functionality when internet access may be necessary, can prevent compromised software from "activating," thus providing a level of protection in the system. In addition, typical 5GC deployments also protect the user plane using firewall and intrusion detection logic in the N6 LAN (formerly known as the SGi-LAN in LTE/4G) area of the network.

Other 5GC architectural and security enhancements can play a role in supply chain security. Many of these capabilities provide micro-segmentation using various zero-trust techniques to provide authentication, integrity, and confidentiality protection between functions of the system to further limit lateral movement of compromised software. Here are a few examples:

- Unified Authentication Framework enables more consistent use of zero-trust techniques between endpoints:
    - Access-agnostic authentication. Use of the same authentication methods for both 3GPP and non-3GPP access networks.
    - Native support of EAP (allows for ability to plug in new authentication methods in future without impacting the serving networks).
- Increased home network control for authentication enables better UE/network segmentation in roaming scenarios:
    - Ability for the home network to verify that the UE is actually present and requesting service from the serving network. This may be useful in certain roaming scenarios (e.g., a roaming operator claims that the UE is roaming into their network when in fact it is not).
- Authentication and authorization between NFs over a Service Based Interface (SBI) enables zero-trust capabilities within the 5GC:
    - Mutual authentication between NFs shall be based on client-side and server-side certificates by means of either Transport Layer Security (TLS) 1.2 or TLS 1.3 when transport layer protection is used. In indirect communication scenarios, where an SCP is used as intermediate proxy, the NF Service Consumer (NF-C) and NF Service Producer (NF-P) shall use implicit authentication by relying on authentication between NF-C and SCP, and between SCP and NF-P. If additional authentication of the NF-C is required based on operator policy, a client credential assertion (CCA) may be used. The NF-C generates the CCA using its private key for access token request to the Network Repository Function (NRF). Additionally, the NF-P may authenticate the NF-C at the application layer using the CCA.
    - If the PLMN uses token-based authorization, then the authorization framework relies on the OAuth 2.0 framework as specified in RFC 6749. The grants provided shall be of the type client credential grant, as described in clause 4.4 of RFC 6749 and the access tokens shall be JSON Web Tokens (JWT) as described in RFC 7519. The JWT shall be secured with digital signatures or

message authenticate codes based on JSON Web Signature (JWS) as described in RFC 7515. If token-based authorization is used, then the network shall use protection at the transport layer by means of TLS.

- Secondary authentication to enable zero trust between the UE and access services:
  - As an implementation option, the 5GC provides capabilities to perform secondary authentication (e.g., a second authentication level occurring after successful primary mutual authentication of the UE and network), to support enhanced security and verification when user devices access services provided by external networks.
  - Secondary authentication is based on EAP protocols using a method that is determined and controlled by the external network, where an external DN-AAA acts as the authentication server. The credentials used for secondary authentication are different from the ones used for primary authentication and are controlled by the external network.
- Backhaul IPsec providing micro-segmentation between the RAN and the 5GC:
  - N2 is the reference point (as shown in Figure 7.1.1) between the AMF (5GC) and the RAN. It is used to carry network-associated signaling traffic between the UE and the 5GC for 3GPP and non-3GPP accesses. N3 is the reference point between the RAN and UPF (in the 5GC). It is used to carry user plane data from the UE to the UPF. Both N2 and N3 are carried over a backhaul network transport and often use untrusted network facilities. To address this potential issue, 3GPP TS 33.501 (security mechanisms for the N2 interface, section 9.2), has specified that both N2 and N3 reference points shall be integrity, confidentiality, and replay-protected using IPsec ESP and IKEv2 certificate-based authentication. This feature limits the impact of supply chain vulnerabilities in untrusted backhaul networks by mitigating “man-in-the-middle” attacks. These reference points would still be subject to availability (DoS) attacks.
  - It is important to note that 3GPP also states that if interfaces are trusted (e.g., physically protected), it is up to the PLMN operator to decide whether to use cryptographic protection.