|  |  |  |
| --- | --- | --- |
|  | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2022-2024 | SG17-C639 |
| STUDY GROUP 17  |
| Original: English |
| **Question(s):** | 1/17  | Geneva, 20 February – 1 March 2024  |
| **CONTRIBUTION** |
| **Source:** | India |
| **Title:** | Proposal for new work item TR.cs-sc: Collection of Security Concerns for extracting the Security Requirements for Cyber Security Reference Architecture |
| **Contact:** | Pushpendra Kumar SinghMinistry of Communications India | Tel: +91 94120 00042Email: pushpendraks.its@gov.in |
| **Contact:** | Preetika SinghMinistry of Communications India | Tel: +91 9868137608Email: preetika.singh87@gov.in |
| **Contact:**  | N. Kishor NarangNarnix Technolabs Pvt. Ltd.India  | Tel: +91 98101 63990E-mail: kishor@narnix.com |

|  |  |
| --- | --- |
| **Abstract:** | This document proposes to develop a new work item proposal as envisaged in the WP-4 SG17-[TD1401R1](https://www.itu.int/md/T22-SG17-230829-TD-PLEN-1401/en) to supplement the work of X.cs-ra, titled “ Technical Report on Collection of Security Concerns of Digital Systems, Digital Infrastructures and Networks for extracting the Security Requirements to help develop a comprehensive and Granular Cyber Security Reference Architecture. This document is focussing on the Security concerns vis a vis the various use cases as envisaged in the WP-4 of the annex-B of SG17-[TD1401R1](https://www.itu.int/md/T22-SG17-230829-TD-PLEN-1401/en).  This document focusses on the security concerns in the IMT-2020 Telecommunications services network comprising of the Radio Access Network(RAN) , Packet Core(PaCo) and User Equipment (UE) as the Operational Technology (OT) Part of the IMT-2020 and the CRM/Billing, SIEM etc. as Information Technology (IT) part of the network under the overall Service Provider’s network.   |

1. **Background**

The Draft Recommendation X.cs-ra is aimed at providing the Reference Architecture for Cyber Security including views, models, and guidelines to demonstrate that cyber security and related characteristics are adequately addressed in the architecture of an entity of interest.

Mobile communications provide a means for people to communicate with one another over long distance. Throughout the years, ever since it was introduced, mobile technology has been constantly evolving from the First Generation (1G) analogue based technology, to the Fifth Generation (5G) technology or commonly known as International Mobile Telecommunications-2020 (IMT-2020) with the development work on 6G or IMT-2030 having started under the aegis of Standards development Organisations including ITU. The current state of the art mobile communication technology being the IMT-2020 is capable of supporting even higher speed than the other previous telecommunication technologies, in addition to capability of supporting ultra reliable & low latency services, enhanced broadband service and massive machine number of devices connected to the network. With capability to support a wide range of services, it is crucial for the IMT-2020 network and devices to be secured from external attacks and threats, as they can compromise the confidentiality, availability and integrity of the network. Mitigation controls for these threats and attacks should be in place to ensure that the network is available all the time, in addition to preventing espionages and sensitive data breach.

The adoption of the TCP/IP technology into the telecommunication technology has revolutionised the telecom service spectrum. The internet connectivity through the telecom networks and its adoption for facilitating various types of voice, video & data-based services has extended the use of regular ICT equipment like computers and mobile phones, much beyond what they designed for. This in turn is fuelling the development of cyber-physical or ‘smart’ systems. This coverage comprising of the virtual and real expanse has enlarged the attack surface with threat of remote exploitation of Operational Technology (OT) networks and systems, such as Telecom Switching system, power grids, air traffic control systems, port operation systems, railway signalling systems, industrial plants etc.

Based on the past experiences and the current best practices, there is an urgent need to strengthen the cyber resilience of critical functions, business and industrial processes, underlying ICT infrastructure and systems. With ever-increasing interconnectivity, there has been a huge expansion of the attack landscape for cybercriminals to exploit the vulnerabilities and deploy malware with malicious intent. This expansion is further driven by the explosive growth of mobile, IoT devices and Industry 4.0. Traditional approaches of cybersecurity, such as perimeter security and cyber protection of a few devices, are no longer sufficient for the defence of an enterprise or the nation’s ICT infrastructure. The attack landscape now also includes threats via interconnected systems. Poor cyber hygiene and non-compliance to basic precautions in the cyberspace expose the systems and infrastructure to cyber threats. Many cyber-attacks are not necessarily sophisticated, but are often the result of exploited vulnerabilities, which could have been easily patched by the individual or the organisation.

1. **Introduction:**

The pace of digitalisation has been very rapid over the past few years. The adoption of the TCP/IP technology for all activities has converted/transformed the digital Systems & Digital Infrastructures and Networks into a interconnection of Operations Technology(OT) part of the network and information Technology (IT) Part of the network. Security risks and concerns are managed differently in IT and OT networks. Security in IT is primarily focused on protecting data confidentiality, ensuring that sensitive information is accessible only to authorized users. OT security, however, prioritizes the safety and availability of industrial systems and processes. The integrity and continuous operation of physical equipment are paramount in OT, given that a failure can result in significant safety and financial implications.

The wireless connectivity, or wireline connectivity, the authentication of the customers/subscriber, the actual routing/switching of the communication signals etc. is facilitated through the Operations Technology based network. The subscriber acquisition, charge/subscription management, deletion etc. are facilitated through IT part of the service provider’s network. The Security concerns of the OT part and the IT part are to be taken together so as to devise a strategy & Mitigation measure toward building a secure and resilient digital Service Provider’s network. The Security concerns or threats are interchangeably used but have slightly different connotations and contexts to the OT part and IT part of the Service provider’s network , hence need not necessarily be the same. A Collection of the same for both with the context shall help in identifying the security requirements, and the stakeholders to be addressed through the Cyber Security Reference Architecture as proposed in X.cs-ra.

1. **Gap Analysis:**

**Security Concerns :** Security Concern is **a novel security metric introduced to assess the security of business processes in the context of relevant threat scenarios**. It is a function of threat and vulnerability. It quantitatively measures the "concern" due to various attributes of the security of a business process, considering the threat scenario and asset sensitivity whereas the Security Threat refers to **any type of malicious activity or attack that could potentially cause harm or damage to an organization, its data or its personnel**. Security threats may refer to physical threats, such as theft or vandalism, as well as digital threats, such as malware or ransomware. In many a literature the two terms are interchangeably used however as brought out above the two may not be same.

The Collection of the Security concerns will play a major role in applying them as an important pillar for developing any Reference Architecture, because the comprehensive and granular understanding of diverse applications and their respective security concerns which are planned to be addressed through the reference architecture, can only be achieved by knowing all the security concerns s in all the relevant Use Cases and analysing them with structured approach to extract the security requirements and collate them in a proper manner.

ITU-T SG 17, other ITU study groups and even other global, regional & national SDOs have developed many a Standards on different aspects of Cyber Security. However, if any stakeholder wants to embed/design-in comprehensive Cyber Security & Resilience in any Digital System or Digital Infrastructure, there are NO guiding collaterals to help them identify and map all the relevant Standards with diverse security concerns from different perspectives, as most of the standards are Point Solutions to Point Problems. There is no comprehensive guidance/documentation on diverse security concerns from different perspectives and viewpoints, more so all of them being mapped to the appropriate standards to ensure that with help of that Standards ToolBox, the stakeholders could architect/design a comprehensively cyber secure and resilient digital system.

The Annex B of X.cs-ra in [TD 1401R1](https://www.itu.int/md/T22-SG17-230829-TD-PLEN-1401/en) outlines a very crucial step by step approach to develop Cyber Security Reference Architecture and demystifying the complex paradigm of Cyber Security in a comprehensive manner, as under:

*Along with developing a Granular Cyber Security Reference Architecture with multiple views and interdependence matrix of stakeholders, their respective concerns and technologies, standards (also Policies & Regulatory interventions) and governance required to address them in a wholistic manner, a few more initiatives could be undertaken by ITU-T SG 17 as smaller Packages and developed in structured phases like:*

* *Work Package 1: A Technical Report undertaking the required groundwork of collecting detailed information on different aspects of the Security paradigm including but not limited to the domains, context, nuances, attributes, stakeholders, applications, and use cases etc. etc.*
* *Work Package 2: Collections of Use Cases*
* *Work package 3: Stakeholders Identification, Classifications, expectations, and Concerns…*
* *Work Package 4: Collection of Security Concerns…*
* *Work Package 5: Analysing the collected information to extract the requirements, relationships, interdependence, views, models etc. amongst various aspects that can help develop a comprehensive Reference Architecture of Cyber Security. 🡺 Cyber Security Reference Architecture Development*
* *WP 6: Develop a User Guide and/or Implementation Guide for leveraging the cyber security reference architecture in any given domain, application or use case for digitals systems, solutions and/or infrastructures.*
* *WP 7: Creating an Inventory of the Standards in and around the Cyber Security paradigm.*
* *WP 8: Mapping the identified relevant standards with the different Models, Blocks and/or Layers of the Cyber Security Reference Architecture. Another approach for mapping the Standards could be around classification based on Security Concerns, domains, use cases, applications etc…*
* *NOTE: However, an exhaustive Standards Inventory without any structured mapping shall not be helpful to the ecosystem stakeholders for identifying the appropriate standards for their respective needs.*
* *WP 9: Identifying the GAPS in Standards available and required.*
	+ *Classifying them into System Standards and/or Products/Domain, applications, services specific Standards.*
	+ *Identifying the most appropriate SDOs for developing them by themselves or jointly with ITU-T SG 17.*
* *WP 10: Developing a comprehensive Compliance Testing Framework & Schemas for setting up TRUST Centres.*

ITU Study Groups shall benefit by using a common harmonized and standardized approach to describe the collected Security Concerns with their respective context so as to arrive at appropriate security requirement. The output of this work item shall contribute in developing a comprehensive Cyber Security Reference Architectures, as well as integrate Cyber Security in a structured manner in various digital systems, solutions, infrastructures & Networks Architectures.

1. **Proposal**

This contribution proposes to review this proposal, to obtain feedback, amend it accordingly and establish this new work item with A.13 justification in Annex A and baseline text in Annex B.

Annex A

A.13 justification for proposed Draft new Technical Report ITU-T TR.cs-sc “Collection of Security Concern to support X.cs-ra Cyber Security Reference Architecture”

|  |  |  |  |
| --- | --- | --- | --- |
| **Question:** | Q1/17 | **Proposed new ITU-T Technical Report** | Geneva, 20 February – 1 March 2024  |
| **Reference and title:** | Draft new Technical Report on “Collection of Security Concerns to support X.cs-ra "Cyber Security Reference Architecture” |
| **Base text:** | Annex B of this Contribution | **Timing:** | 2025-Q4 |
| **Editor(s):** |

|  |
| --- |
| Pushpendra Kumar SinghMinistry of Communications India, email. Pushpendraks.its@gov.in  |
| Preetika SinghMinistry of Communications India, email. preetika.singh87@gov.in |
| N. Kishor NarangNarnix Technolabs Pvt. Ltd.India email. kishor@narnix.com |

 | **Approval process:** | Agreement  |
| **Scope** (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):This Technical Report provides a structured “Collection of Security Concerns s with their contexts in use cases of Digital Systems, Solutions, Infrastructures and Networks for extracting the Security Requirements to help develop a comprehensive and Granular Cyber Security Reference Architecture as proposed in X.cs-ra. |
| (It shall develop a common harmonized and standardized approach & Template to describe diverse use cases for their respective context, security concerns & requirements. The output of this work item shall be highly crucial in developing a comprehensive Cyber Security Reference Architectures by analyzing the collected Use Cases in appropriate context, as well as integrate Cyber Security in a structured manner in various digital systems, solutions, infrastructures & Networks Architectures.) |
| **Summary** (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work): |
| The integration of TCP/IP technology with traditional protocols , for all activities has converted/transformed the digital Systems & Digital Infrastructures and Networks into a interconnection of Operations Technology(OT) part of the network and information Technology (IT) Part of the network. Security risks and concerns are managed differently in IT and OT networks. Security in IT is primarily focused on protecting data confidentiality, ensuring that sensitive information is accessible only to authorized users. OT security, however, prioritizes the safety and availability of industrial systems and processes. The integrity and continuous operation of physical equipment are paramount in OT, given that a failure can result in significant safety and financial implications.The wireless connectivity, or wireline connectivity, the authentication of the customers/subscriber, the actual routing/switching of the communication signals etc. is facilitated through the Operations Technology based network. The subscriber acquisition, charge/subscription management, deletion etc. are facilitated through IT part of the service provider’s network. The Security concerns of the OT part and the IT part are to be taken together so as to devise strategy & Mitigation measures toward building a secure and resilient digital Service Provider’s network. The Security concerns or threats are interchangeably used but have slightly different connotations and contexts to the OT part and IT part of the Service provider’s network , hence need not necessarily be the same. A Collection of the same for both with the appropriate context shall help in identifying the security requirements, and the stakeholders to be addressed through the Cyber Security Reference Architecture as proposed in X.cs-ra. This work item mainly covers the collection of Security concerns with the contexts of use case to derive the appropriate security requirements. The output of this Technical Report shall play an important role in developing a comprehensive Cyber Security Reference Architectures by analyzing the collected Security concerns and breaking down them into the generic concerns applicable to any network be it based on IT, or OT or both IT&OT.  |
| **Relations to ITU-T Recommendations or to other standards** (approved or under development)**:** |
| 1. ITU-T X.arch-design
2. ITU-T X.800
3. ITU-T Z.150
4. ISO/IEC/IEEE 42010
5. ISO/IEC/IEEE 42020
6. ISO/IEC/IEEE 42030
7. IEC SRD 63188
8. ISO 15704
9. ISO/IEC/IEEE 15288
10. ISO/IEC/IEEE 12207
11. ISO/IEC 31000 Family
12. ISO/IEC 27000
13. IEC 62559-1, -2, -3 & -4.
 |
| **Liaisons with other study groups or with other standards bodies:** |
| 1. ISO/IEC JTC1/SC27
2. ISO/IEC JTC1/WG13
3. ….
 |
| **Supporting members that are committing to contributing actively to the work item:** |
| Ministry of Communications (India) |

Editor’s Note:

i) The definition of Security concerns and security threats are very similar and in many a literature are interchangeably used, however we may have to define Security concern to differentiate it from security threat, as no uniform definition exist for the same.

Annex B

Initial proposed Baseline text

ITU-T TR.cs-sc

Technical Report on Collection of security concerns for developing Cyber Security Reference Architecture

Summary

Strong security controls and practices are foundational elements for building and maintaining stakeholder trust. Security experts no longer can afford to assume that walling off the network would provide the security required to maintain system integrity and customer trust. Recognizing the impact of security breaches on customer trust, enterprises are striving to develop new comprehensive, scalable, and futureproof strategies to protect enterprise systems and data which will in turn will aid in developing a comprehensive granular cyber security reference architecture.

Security concerns collection is one of the foundational pillars for developing any Reference Architecture, because the comprehensive and granular understanding about the security concerns provides us the target for defining the cyber security Reference architecture. The Security concerns along with the use cases become the objective of protecting through the reference architecture.

Keywords

Security, Cyber Security, Cyber Resilience, Architecture, Reference Architecture, Security Concerns, Security threats, Vulnerabilities, Attack Surface, Digital Systems, Digital Infrastructure, Use Cases, Use Case Methodology, Use Case Analysis, Operational Technology, Information Technology

# Scope

This Technical Report provides a structured “Collection of security concerns with the contexts ” of Digital Systems, Solutions, Infrastructures and Networks for extracting the Security Requirements to help develop a comprehensive and Granular Cyber Security Reference Architecture as proposed in X.cs-ra.

(It shall develop a common harmonized and standardized approach & Template to describe diverse security concerns in their respective context & requirements. The output of Technical Report shall be highly crucial in developing a comprehensive Cyber Security Reference Architectures by analyzing the collected security concerns in their context, as well as integrate Cyber Security in a structured manner in various digital systems, solutions, infrastructures & Networks Architectures.)

# References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

ITU-T X.1814] Recommendation ITU-T X.1814 (09/2022), *Security guidelines for IMT-2020 communication systems*

[ITU-T X.1205] Recommendation ITU-T X.1205 (04/2008), *Overview of Cybersecurity*

[ITU-T X.1601] Recommendation ITU-T X.1601 (10/2015), *Security framework for cloud computing*

[ITU-T X.1044] Recommendation ITU-T X.1044 (10/2019), *Security requirements of network virtualization*

[ITU-T X.1038] Recommendation ITU-T X.1038 (10/2016), *Security requirements and reference architecture for software-defined networking*

[ITU-T X.1371] Recommendation ITU-T X.1371 (05/2020), *Security threats to connected vehicles*

[ITU-T X.1453] Recommendation ITU-T X.1453 (01/2022), *Security threats and requirements for video management systems*

# Definitions

<Check in the ITU-T terms and definitions database at [www.itu.int/go/terminology-database](http://www.itu.int/go/terminology-database) whether the term has already been defined in another Recommendation. It would be more consistent to refer to such a definition rather than to redefine the term>

[To be updated…]

## Terms defined elsewhere.

<Normally, terms defined elsewhere will simply refer to the defining document. In certain cases, it may be desirable to quote the definition to allow for a stand-alone document. Before defining a new term, verify whether it has already been defined in the official ITU terminology database, at [www.itu.i.nt/go/terms](http://www.itu.i.nt/go/terms). >

This TR uses the following terms defined elsewhere:

**3.1.1 < Resilience >**

**Resilience is the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation.**

**At the network (topology) level, resilience amounts to preserving loss, jitter, and latency as successfully as possible for a given service — all these Quality of Service (QoS) metrics can be compromised if failures/attacks occur and there is a lack of resilience mechanisms to remediate/mitigate them>** [Reference]: <optional quoted definition>.

**3.1.2 <Term 2>** [Reference]: <optional quoted definition>.

[To be updated…]

## Terms defined in this Technical Recommendation.

This Recommendation defines the following terms:

### Security Concern: Security Concern is a novel security metric introduced to assess the security of business processes in the context of relevant threat scenarios. It is a function of threat and vulnerability. It quantitatively measures the "concern" due to various attributes of the security of a business process, considering the threat scenario and asset sensitivity. It is a function of threat and vulnerability of an asset.

### Security Threat : Security Threat refers to any type of malicious activity or attack that could potentially cause harm or damage to an organization, its data or its personnel. Security threats may refer to physical threats, such as theft or vandalism, as well as digital threats, such as malware or ransomware.

### IT Asset: IT Asset is any item, physical or virtual, that adds value to any information processing activity performed by the entity. IT Assets can be considered as Hardware IT Assets, Software IT Assets, Information IT Assets, and Service IT Assets. Thus, an information technology (IT) asset is any piece of information, software or hardware or service, that an organization uses in the course of its business activities. Hardware assets include physical computing equipment like physical servers in data centres, desktop computers, mobile devices, laptops, keyboards, and printers. Software assets, on the other hand, include applications for which licenses are typically issued per user or machine, as well as software systems and databases built using open-source resources. Service Assets would include IT related services, like ISP, Annual Maintenance Contracts (AMC) of various other IT Assets, and also cloud-based assets, such as Software-as-a-Service (SaaS) applications.

# Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CS-RA Cyber Security Reference Architecture

IT Information Technology

OT Operational Technologies

IoT Internet of Things

NT Network Technologies

DLT Distributed Ledger Technologies

AI Artificial Intelligence

CRM Customer Relationship Management

…..

# Conventions

This Technical Report applies the following verbal forms for the expression of provisions:

<None>

# Introduction

Cyber risk threat vectors have evolved rapidly, and attacks have become increasingly sophisticated, deliberate, and unrelenting in nature. In the digital era security, resilience and trust are complex issues fraught with myriad existential threats to the enterprise and infrastructure.

The new paradigm of Smart Grid, Smart Building, Smart Home, Smart City, Smart Manufacturing already complicated by the ‘Internet of Things’ & Internet of ‘Everything’ made further complex by the Artificial Intelligence, Machine Learning, Distributed Ledger Technology & Quantum Computing, make it truly complex to develop & embed comprehensive Security, Privacy and Trustworthiness attributes in the products, systems and solutions for any use case or application.

The recent evolution of cutting-edge technologies and digitalization compounded by the Covid 19, changing geopolitical situations, and increasing cyber-attacks bring a whole new set of challenges for the Security and Security Evaluation Methodologies for complex nature & architectures of diverse Digital (Information and Communication Technology) Systems.

Mobile communications provide a means for people to communicate with one another over long distance. With the growth of technology to the Fifth Generation (5G) technology or commonly known as International Mobile Telecommunications-2020 (IMT-2020) with the development work on 6G or IMT-2030,complexity along with dependence to several critical services has also been increased. With 5G capability to support a wide range of services, it is crucial for the 5G network and devices to be secured from external attacks and threats, as they can create serious effects. Mitigation controls for these threats and attacks should be in place to ensure that the network is available all the time, in addition to preventing espionages and sensitive data breach.

The pace of digitalisation has been very rapid over the past few years. The adoption of the TCP/IP technology with the telecommunication technology has revolutionised the telecom service spectrum. The internet connectivity through the telecom networks and its adoption for facilitating various types of voice, video & data based services has extended the use much beyond the regular use of ICT equipment like computers and mobile phones. This in turn is fuelling the development of cyber-physical or ‘smart’ systems. This coverage comprising of the virtual and real expanse has enlarged the attack surface with threat of remote exploitation of Operational Technology (OT) networks and systems, such as Telecom Switching system, power grids, air traffic control systems, port operation systems, railway signalling systems, industrial plants etc.

The multiplicity of technologies and their convergence in many new and emerging markets, however, particularly those involving large-scale infrastructure demand a top-down approach to standardization starting at the system or system-architecture rather than at the product level. Therefore, the systemic approach in standardization work can define and strengthen the systems approach throughout the technical community to ensure that highly complex market sectors can be properly addressed and supported.

This work item mainly covers the collection of Security concerns with their contexts in use cases and then deriving out appropriate security requirements. The output of this Technical Report shall play an important role in developing a comprehensive Cyber Security Reference Architectures by analyzing the collected Security concerns and breaking down them into the generic concerns applicable to any network be it based on IT, or OT or both IT & OT.

# Collection of Security concerns for an IMT-2020 services network

Nowadays along with Information technology (IT), Operational technology (OT) also plays an important role for not only Networks, but also devices, systems, and users. It is important to understand the difference between IT and OT to identify the security concerns pertaining to both of them.

## Information technology (IT) is the use of any computers, storage, networking and other physical devices, infrastructure, and processes to create, process, store, secure and exchange all forms of electronic data. Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events. IT focuses on managing electronic data, while OT is centered on controlling physical processes and equipment. IT is essential for business operations and decision-making and involves the use of computers and software to gather, store, process, share data securely. OT employs hardware and software to monitor and control industrial operations, ensuring efficiency and safety in sectors like manufacturing, Rail Transport, Ports, Air Traffic Control, Telecommunications, energy etc. The key differences between IT and OT are as per following:

1. IT focuses on managing and processing data, ensuring its availability, confidentiality, and integrity. It deals with the storage, retrieval, and transmission of data, ensuring that information is accessible and secure. OT is dedicated to controlling and monitoring physical processes and equipment, playing a crucial role in critical infrastructure. It ensures that machinery and processes operate effectively and safely.
2. IT operates in a general computing environment, managing devices like computers, servers, and smartphones. It involves standard operating systems and is centered around data-centric tasks. OT operates in industrial environments, managing specialized equipment and processes. It uses customized, often proprietary systems/protocols tailored to specific operational needs.
3. IT systems are regularly updated to patch vulnerabilities and enhance performance, with established schedules for updates. OT systems, conversely, aren’t typically updated as frequently. Interruptions for updates in the OT environment can halt production, so patches are applied during specific maintenance windows to avoid disrupting ongoing operations.
4. IT is inherently connected, facilitating data exchange and communication over networks, including the internet. OT has traditionally been isolated, with systems not designed for external connectivity. However, the advent of Industrial Internet of Things (IIoT) is bridging this gap, integrating OT systems with broader networks for enhanced data analytics and operational efficiency.
5. IT deals with a variety of data types, including transactional, voice, and bulky data, focusing on the broad business needs of data storage, processing, and communication. OT, in contrast, is centered around real-time data processing to monitor and control physical devices and processes. The immediacy and specificity of data use in OT are critical to ensuring operational efficiency and safety.
6. OT devices are also known for their durability. They are designed to withstand harsh conditions like heat, moisture, and vibration, making them suitable for industrial environments. This is in stark contrast to IT devices, which are not built to endure such challenging conditions. OT device design ensures effective integration with industrial machinery and processes.
7. OT and IT network infrastructure have similar elements, like switches, routers, and wireless technology. However, there are key differences in terms of form factor, network interface, protocols.

Viii The integration of Information Technology (IT) and Operational Technology (OT) is a transformative progression in the technological landscape, marking the intersection of digital and physical systems. Due to the advent and proliferation of technologies like the Industrial Internet of Things (IioT), big data analytics, Industry 4.0 etc systems are having a unified, interconnected operational model where insights and data are shared across the two domains, fostering enhanced efficiency, data accuracy, and operational performance. Real-time data from OT systems is fed into IT for in-depth analytics and insights. The integration of the digital and physical world offers organizations a holistic, 360-degree view of operations.

Telecommunications network have been traditionally isolated and have been working in silos which has undergone significant change by integration of TCP/IP technology with telecommunication technology. With the increase in the complexity of technologies from 2G to 5G, fixed line to NGN, a lot of IT has found its place in the networks. There are many factors which have led to various use cases within which IT based components have been deployed. These factors may include, but are not limited to, Complexity of services and product portfolio, Tariffs, and value-added services (VAS) leading to deployment of CRM, order management, provisioning, and billing etc. . While traditional services such as voicemail and short-messaging services are mainly network-based and require minimal IT involvement, newer services such as mobile email, download portals, unified messaging, social networking platforms, application stores , online billing etc. are infinitely more IT-intensive. Technological advances such as fixed-mobile convergence, video-on-demand, mobile email, and femtocells pose a challenge for IT as their implementation normally requires new IT systems, or significant modifications to existing IT. All these new developments being facilitated through intermixing of IT & OT in Telecommunication Service provider’s networks requires an understanding of the security concern of the complete network.

## Security Concern in IMT-2020 systems:

The security concerns may arise due to well-known threats from software vulnerabilities, configuration mistakes and flooding attacks, threats from infrastructure sharing, threats from the network level, such as threats related to SDN, NFV, network slicing and cloud computing or applications services. There might be security concerns among users due to a fear of unknown technology which is very true for the IMT-2020 being in nascent stages of deployment across the world.

### Generic Security Concern:

1. There is a always a fear of loss of service due to Denial-of-service (DoS) attack which may make a network resource unavailable to its intended users by temporarily or indefinitely interfering with or disrupting the network service by flooding it with a massive number of requests. There may be a Distributed denial-of-service (DDoS) attack where multiple systems target a single system with a DoS attack, orchestrating a synchronized DoS attack to a single target for overwhelming the system’s resources thus leading to loss in service capability.
2. The is a a perception that Data breach, leak, theft, destruction, and manipulation of information may happen due to unauthenticated/unauthorized access to the systems and/or network, leading to the theft of PII and possible publication of personal data/biometric/medical data, organization confidential information or government/state-related information.
3. There is always a concern about illegal interception in the form of Eavesdropping wherein the intruder seeks to tamper with the application and communication layers of the various IMT-2020 network elements (SDN controller, network function, edge node, virtualization orchestrator).
4. Exploitation of software and hardware vulnerabilities by a malicious attacker may lead to derive an advantage due to unknown (to the vendor and user) software or hardware flaws or known but unpatched flaws to perform an attack. It also includes the exploitation of other known vulnerabilities related to previous generations of mobile telecommunications.
5. Deliberate or inadvertent Malicious code or software in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.
6. Compromised supply chain, vendor, service providers and untrustworthy personnel from third parties involved during supply, installation, product testing, maintenance, configuration and operation may enable insertion into the product , a concealed hardware, malicious software and software flaws. It may also facilitate remote access to the systems unknown to the Service Providers.
7. The flaws in security, management and operational procedures may be exploited by the malicious elements.
8. Abuse of authentication may be possible due to a theft of user credentials, brute force of user accounts, password cracking, masking user identity and impairing IoT grouping authentication as techniques used may lead to malicious elements accessing the IMT-2020 systems remotely.
9. Identity spoofing may affect any unprotected system leading to the control of the network functions to trigger several other types of attack (instigate network flows, divert traffic, etc.).

### Security concerns in user equipment:

1. Loading of Malicious software may lead to an attacker getting access to commercial sensitive information or PII in the User equipment.
2. A user equipment may be converted to a botnet through remote loading of malicious software. The botnet converted user equipment may further be controlled to automatically launch a variety of attacks (e.g., DoS/D-DoS) on IMT-2020 systems.
3. There is probability of an unauthorized access to and destruction, disclosure or modification of user and signaling data
4. The Tampering with subscription credentials may lead to compromise of authentication, confidentiality & integrity of communications.

### Security Concerns in Radio Access Network:

1. There is a likelihood of a traffic surge due to an event or emergency which might lead to services becoming unavailable to the users or emergency responders.
2. The interface running the SS7, or the Radius/diameter may be intercepted illegally leading to Key leakage between the user and the operator. Similarly the illegal interception on signaling links between the operators may also lead to the leakage of inter-operator key/identifiers for authentication and authorizations.
3. There is a likelihood of the compromise of user plane integrity leading to insertion of malicious data into the mobile connection.
4. There is a likelihood of a false BTS/Malicious BTS deployment and hijacking the sessions to learn the authentication key. Without this authentication step, the key tier cannot achieve one of its design goals, that is, to protect customers from faulty base stations.
5. There is a likelihood of malicious elements exploiting the buffer status reports of access network components such as base stations to obtain information such as packet scheduling, load balancing and admission control algorithms to achieve their malicious intents.
6. Message injection by malicious elements after hijacking the sessions over the user plane or control plane links can launch DoS attacks on IMT-2020 networks. An attacker can also inject control protocol data units (C-PDUs) into the system during wake-up time to perform DoS attacks on newly arriving UE.
7. The physical size of base stations has been sharply reduced and they have been placed in indoor locations such as shopping malls, public places, stadiums, and hospitals making them more vulnerable as compared to the macro base stations used in pre-IMT-2020 networks. Moreover, the increase in the number of base stations will increase the potential vulnerabilities in IMT-2020 networks.

### Security concerns in core network:

1. The improper implementation of transport layer security (TLS)/secure sockets layer (SSL) may lead to exploitation of vulnerability attacks such as TCP/SYN DDoS, RC4 biases in TLS, browser exploits against SSL/TLS attacks etc.
2. An attacker can analyze SDN traffic and manually collect network information such as the Infrastructure Protocol and key network elements of the SDN controller.
3. The incorrect configuration may lead to Malicious diversion of traffic from network elements of the data plane. E.g. The compromise of isolation between radio slices in any active node or when the enforcement of access to a slice in the edge equipment is either bypassed or misconfigured may enable diversion of traffic from one network zone o another.
4. Misuse of audit tools may lead to unauthorized information disclosure which might be misused by malicious elements.
5. The Leak of long-term key for user authentication/authorization data by an disgruntled insider is a concern.
6. Exploitation of misconfigured or poorly configured systems/networks
7. An unauthorized network function or function embedding a trojan, which is introduced to the network by an insider (to the MNO) or a vendor could be made a part of SBA leading to making available malicious APIs to be exploited by external malicious actors.
8. Spoofing of management identity may lead to exchange of unauthorized messages over the service-based interface (SBI).

### Security concerns in network slicing

1. **< to be collected>**

### Security concerns in multiaccess edge computing (MEC):

1. **< to be collected>**

### Security concerns in network function virtualization:

1. **< to be collected>**

### Security concerns in cloud computing

1. **< to be collected>**

Bibliography

* The Concept of Reference Architectures: Gerrit Muller et all <https://www.researchgate.net/publication/220432603_The_Concept_of_Reference_Architectures>
* ISO 15704 – Enterprise Modelling and Architecture - Requirements for enterprise-reference architectures and methodologies
* ISO/IEC/IEEE 15288 – System and Software engineering – System Life Cycle Process
* ISO/IEC 12207 - System and Software engineering - Software Lifecycle Process
* ISO/IEC/IEEE 42010 – Software, systems and enterprise - Architecture Description
* ISO/IEC/IEEE 42020 – Software, systems and enterprise - Architecture Processes
* ISO/IEC/IEEE 42030 - Software, systems and enterprise - Architecture Evaluation Framework
* ISO 25000 - SQuaRE (System and Software Quality Requirements and Evaluation)
* ISO/IEC 25010 - System and software quality models:
* ISO 31000:2018 - Risk management — Guidelines
* IEC 31010:2019 - Risk management — Risk assessment techniques
* ISO 26000 – Social Responsibility
* ISO/IEC 27000 - Information technology — Security techniques — Information security management systems — Requirements
* ISO/IEC TS 5723:2022 - Trustworthiness Vocabulary
* ISO/IEC 21840:2019 - Systems and software engineering — Guidelines for the utilization of ISO/IEC/IEEE 15288 in the context of system of systems (SoS)
* ISO/IEC 30147 Internet of Things (IoT) – Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 systems engineering processes.
* ISO/IEC AWI 30149 - Internet of Things (IoT) - Trustworthiness Principles
* ISO/IEC TR 24028 Overview of AI Trustworthiness
* BS 10754 Series - Systems Trustworthiness
* ISO/IEC 25000 Family – Systems & Software Quality Requirements
* ISO/IEC 15026 Series – Systems & Software Assurance
* ISO/IEC 38500 Family - Governance of IT
* ISO/IEC 31000 Family – Risk Management
* ISO 31700 – Privacy by Design for Consumer Goods & Services
* ISO/IEC 20000 Series - IT Service Management
* ISO/IEC 33000 Family - Process assessment

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_