ETSI GR F5G 010 V1.1.1 (2022-04)

Fifth Generation Fixed Network (F5G); Security; Threat Vulnerability Risk Analysis and countermeasure recommendations for F5G

Disclaimer

The present document has been produced and approved by the Fifth Generation Fixed Network (F5G) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGR/F5G-0010Security

Keywords

F5G, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights 4

Foreword 4

Modal verbs terminology 4

1 Scope 5

2 References 5
2.1 Normative references 5
2.2 Informative references 5

3 Definition of terms, symbols and abbreviations 6
3.1 Terms 6
3.2 Symbols 7
3.3 Abbreviations 7

4 Introduction to security review of F5G 8
4.1 F5G purpose and architecture review 8
4.2 F5G specificities 8
4.3 Network topology, network functions, and reference points 10
4.4 F5G security boundary and security objectives 11
4.5 F5G stakeholder model 12
4.6 Motivation and capability of attackers 13

5 F5G threat analysis 14
5.1 Summary of analysis 14
5.2 Trust in F5G 17
5.3 Physical attacks 19
5.4 Attacker profiles 19
5.5 Assets in the underlay plane 20
5.6 Assets in the service plane 20
5.7 Assets in the network management plane 21
5.8 Underlay plane threat analysis 21
5.9 Service plane threat analysis 23
5.10 MCA plane threat analysis 24

6 F5G mitigation strategies 24
6.1 Method and approach 24
6.2 Architectural mitigation strategies 25
6.3 Protocol mitigation strategies 25
6.4 Policy mitigation strategies 25
6.5 Other mitigations 25
6.6 Specific actions against identified risks 26

7 Cost benefit analysis for mitigations application 26
7.1 Summary of method and calculation 26
7.2 Sample calculation 27

Annex A: Risk assessment and CBA worksheets 28

Annex B: Bibliography 29

History 30

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Fifth Generation Fixed Network (F5G).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document identifies security threats to F5G and recommends mitigation strategies against them where F5G is defined by its purpose and use cases [i.1] and its architecture [i.3]. The present document adopts the TVRA method defined in ETSI TS 102 165-1 [i.5].

NOTE 1: The identified mitigation strategies in the present document are outlined with respect to the risk analysis contained in the present document and are indicative in nature (i.e. are not fully specified). Some mitigations that are identified may require non-technical measures as part of the strategy and the present document identifies them.

NOTE 2: The worksheets from ETSI TS 102 165-1 [i.5] and cited in clauses 5, 6 and 7 are provided as an electronic attachment to the present document (see Annex A).

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR F5G 002: "Fifth Generation Fixed Network (F5G); F5G Use Cases Release #1".

[i.2] ETSI GR F5G 001: "Fifth Generation Fixed Network (F5G); F5G Generation Definition Release #1".

[i.3] ETSI GS F5G 004: "Fifth Generation Fixed Network (F5G); F5G Network Architecture".

[i.4] Common Vulnerability Enumeration (CVE®) list.

NOTE: Available at www.cve.org.

[i.5] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.6] Shannon Claude: "Communication Theory of Secrecy Systems". Bell System Technical Journal. 28 (4): 662. doi:10.1002/j.1538-7305.1949.tb00928.x.

[i.7] Kerckhoffs Auguste (January 1883): "La cryptographie militaire" [Military cryptography]. Journal des sciences militaires [Military Science Journal].

[i.8] M. Zafar Iqbal, H. Fathallah and N. Belhadj: "Optical fiber tapping: Methods and precautions", 8th International Conference on High-capacity Optical Networks and Emerging Technologies, 2011, pp. 164-168, doi: 10.1109/HONET.2011.6149809.

[i.9] Recommendation ITU-T X.800: "Security Architecture for Open Systems Interconnection for CCITT Applications".

[i.10] ISO 7498-2: "Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture".

NOTE: ISO 7498-2 and ITU-T X.800 contain the same text.

[i.11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR).

[i.12] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

[i.13] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Radio Equipment Directive (RED)).

[i.14] European Treaty Series No. 185: "Convention on Cybercrime".

[i.15] ETSI GR NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[i.16] Recommendation ITU-T G.800: "Digital networks - General aspects. Unified functional architecture of transport networks".

[i.17] Recommendation ITU-T G.873.1: "Digital networks - Optical transport networks. Optical transport network: Linear protection".

[i.18] Recommendation IUT-T G.873.2: "Digital networks - Optical transport networks: ODUk shared ring protection".

[i.19] Recommendation ITU-T G.873.3: "Digital networks - Optical transport networks: Optical transport network - Shared mesh protection".

[i.20] National Vulnerability Database (NVD).

NOTE: Available at https://nvd.nist.gov.

[i.21] UK Computer Misuse Act 1990.

NOTE: Available at https://www.legislation.gov.uk/ukpga/1990/18/contents.

[i.22] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation Criteria for IT security - Part 2: Security functional components".

NOTE: Often referred to by the shorthand term "Common Criteria".

[i.23] TR-069: "CPE WAN Management Protocol".

NOTE: Available from https://www.broadband-forum.org/technical/download/TR-069_Amendment-6.pdf.

[i.24] IEC 60529: "Degrees of protection provided by enclosures (IP Code)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR F5G 00 [i.1], ETSI GR F5G 001 [i.2], ETSI GS F5G 004 [i.3] and the following apply:

botnet: network of connected computing devices infected with malicious software and controlled as a group without the owners' knowledge

data packet jitter: absolute difference in arrival time between the fastest and the slowest data packet or voice frame with respect to end-to-end latency

EXAMPLE: An end-to-end connection has a transfer time determined in part by the physics of transmission and in part by the variable processing time required to perform analysis of headers. The variation in the transfer time between fastest and slowest is the jitter and is commonly absorbed in buffering across the network. Thus, if a packet can take between 100 ms and 1 500 ms to arrive it is often prudent to impose a buffer that is slightly longer than the maximum transit time and to feed data out of the buffer at a constant rate for the receiving application. The existence of a buffer adds a point of attack to the system by adding the buffer as a system asset.

end-to-end latency: time it takes to transfer a given piece of information from a source to a destination, measured at the application level, from the moment it is transmitted by the source to the moment it is received at the destination

trust: confidence in the integrity of an entity for reliance on that entity to fulfil specific responsibilities

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR F5G 002 [i.1], ETSI GR F5G 001 [i.2], ETSI GS F5G 004 [i.3] and the following apply:

AggN	Aggregation Network
AI	Artificial Intelligence
AN	Access Network
BNG	Broadband Network Gateway
CE	Customer Equipment
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CVE	Common Vulnerability Enumeration
DC	Data Centre
EU	European Union
E-CPE	Edge CPE
FFC	Full Fibre Connection
GRE	Guaranteed Reliable Experience
LAN	Local Area Network
M&C	Management and Control
NVD	National Vulnerability Database
OLT	Optical Line Terminal
ONU	Optical Network Unit
ONT	Optical Network Terminal
OSI	Open Systems Interconnection
OTN	Optical Transport Network
PE	Provider Edge-Router
PPPoE	Point to Point Protocol over Ethernet
QoE	Quality of Experience
RG	Residential Gateway
SAP	Service Access Point
SMP	Service Mapping Point
SPP	Service Processing Point
VXLAN	Virtual Extensible LAN

4 Introduction to security review of F5G

4.1 F5G purpose and architecture review

The F5G network architecture is developed based on evolution of the current generation and deployment of fixed networks and focusses on the provision of more fibre connections, addressed using the term Full Fibre Connection (FFC), with high quality user experience, addressed using the term Guaranteed Reliable Experience (GRE). Thus for the purposes of the present document the core of the analysis is with respect to FCC.

The examination of use cases in ETSI GR F5G 002 [i.1] to drive the core set of F5G requirements identify a need for more data throughput and more control of uncertainties in that throughput. Thus, objectives including maximizing availability, minimizing end-to-end latency and minimizing data packet jitter (variation in packet arrival time), are all stated either explicitly or implicitly.

EXAMPLE: High end-to-end latency has a negative impact on real time operations across a network. High data packet jitter rates (variation in packet arrival time) require buffering of data to "smooth" the data delivery to applications.

Figure 4.2-1 from ETSI GS F5G 004 [i.3] describes the planar architecture and that is mapped, in part, to user expectations described in ETSI GR F5G 002 [i.1]. The intent of F5G is to enable more bits per second to the customer by exploiting Optical Transport Network (OTN) technologies and advances in local wireless networking, e.g. WiFi-6, resulting in each of FCC and GRE. The physical nature of all optical fibre transmission is that it is immune to ElectroMagnetic Interference (EMI), and the content of communication on the fibre is therefore not observable without direct access to the fibre. If, in addition, full optical switching is used there are no electrical signals directly in the signal/data path. It is known that optical fibres can be "tapped" and [i.8] summarizes a number of means of doing so. In some implementations switching of optical links includes devices that are susceptible to EMI and this is considered in the analysis.

NOTE 1: Whilst there may be elements of the customer premises network that maintain conventional copper wire based technology such technologies are not in the innovation sphere of F5G and are not directly addressed in the present document.

The managed security of optical networks is broadly addressed by the following services as defined by the OSI 7-layer security model (see Table 2 of Recommendation ITU-T X.800 [i.9] and its mirror ISO 7498-2 [i.10]):

- At layer 1: Connection confidentiality, Traffic flow confidentiality.
- At layer 2: Connection confidentiality, Connectionless confidentiality.
- At layer 3: Peer entity authentication, Data origin authentication, Access control service, Connection confidentiality, Connectionless confidentiality, Traffic flow confidentiality, Connection integrity without recovery, Connectionless integrity.

In addition the models of protection of the physical layer defined in Recommendations ITU-T G.873 series [i.17], [i.18] and [i.19] are taken into account that address some aspects of resilience in network provision (i.e. address the availability aspects of the CIA paradigm).

At higher layers the full suite of services described in Recommendation ITU-X.800 [i.9] apply. For the purposes of the present document only the lower layers of the OSI model are considered and only with respect to achieving FCC and GRE. The threat model addresses attacks against the Confidentiality, Integrity and Availability (CIA) of the assets in the system. Specific stakeholders are considered as targets of the attack on the system.

NOTE 2: The term availability in the CIA paradigm is intended to address many aspects of assuring the service or network is available to the right person at the right time thus includes aspects of identification, authentication and authorization.

4.2 F5G specificities

As indicated in clause 4.1 the purpose of F5G is to promote FCC and GRE. The architecture manages this by conceptualizing the network into 3 planes as shown in Figure 4.2-1.

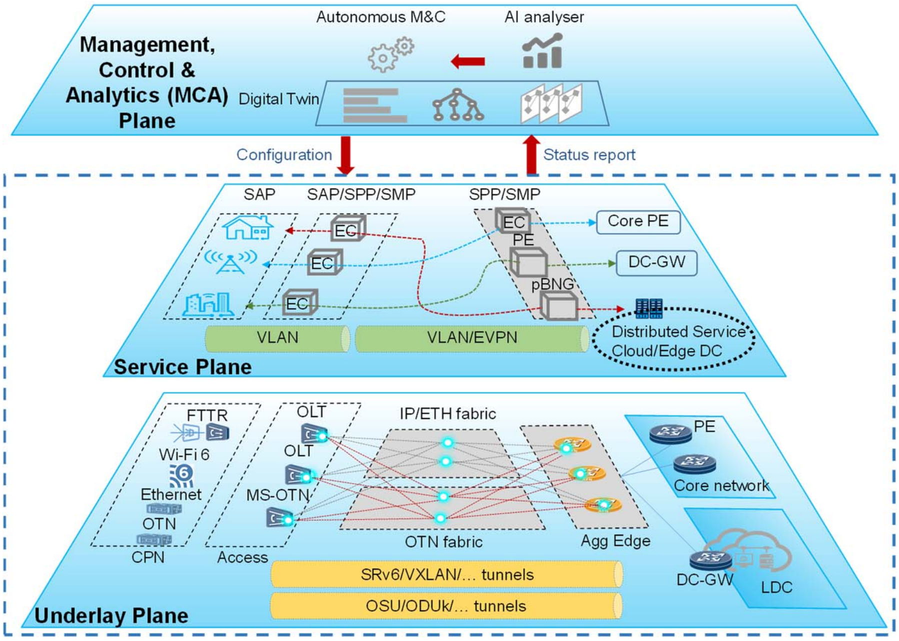


Figure 4.2-1: F5G network architecture

The F5G network architecture as shown in Figure 4.2-1 is comprised of 3 planes, an Underlay Plane, a Service Plane and a Management, Control & Analytics Plane (MCA Plane) with the following defining characteristics:

- Underlay Plane:
  - Carries the physical bits optically or electrically (OTN switches and Ethernet/IP switches and routers).
  - The Underlay Plane is comprised of physical network devices within 4 network segments:
    - Customer Premises Network (CPN);
    - Access Network (AN);
    - Aggregation Network;
    - Core Network.
  - Transmission technologies of the Underlay Plane are bounded (i.e. there are technology boundaries between network segments, which may be complemented by administrative boundaries in the Underlay Plane).

NOTE 1: Only the underlay plane can be defined as optical in nature, all other planes act on data and signalling without any fixed physical representation.

NOTE 2: Boundaries may be realized as interfaces in some instances and may implement some of the physical resilience measures identified in each of Recommendation ITU-G.800 [i.16] and in Recommendation ITU-T G.873 series [i.17], [i.18] and [i.19].

- Service Plane:
  - This plane provides service connections for customer and broadband service and is decoupled from the Underlay Plane. Service connections on the Service Plane can be dynamically created when triggered by protocols, e.g. Point to Point Protocol over Ethernet (PPPoE), or configured from the Management, Control & Analytics (MCA) Plane.

- Management, Control & Analytics Plane (MCA Plane):
    - The MCA Plane is in charge of management, control and performance analysis of the complete network. It is comprised of three logical components:
        - **Digital Twin**: models the network and defines resources, configuration and running models by real time analysis of network data to provide a real time model of the status and configuration of the network, which is the input for autonomous operation and artificial intelligence analysis (analysis is performed on the Digital Twin, not on the running model).
        - **Autonomous Management and Control** which is the main function for network configuration, service deployment, and network operation and includes the Intent Engine (a variant of natural language processing to derive intent from the user interface) and Autonomous Engine (enables MCA without direct human intervention).
        - **AI analyser**: analysis network data, identifies, locates and predicts network failures, provides management tools for QoE and analysing tools for network performance. It includes the Analysing Engine (realizes identification and analysis of network failures and drives close loop control of Autonomous Engine) and the AI Engine (performs data analysis and reasoning, in order to realize prediction of network failure and usage, and also failure identification and analysis).

The layering concept of Figure 4.2-1 is consistent with the OSI model of layering and the wider concept of information hiding using layers (or planes). One of the roles or purposes of the OSI model is to ensure that if a technology in the lower layers is evolved, e.g. the adoption of photons on optical transmission as opposed to electrons over copper wire transmission, the services that can be offered do not need to be changed.

EXAMPLE: A web service operates in the same way irrespective of the communication technology used from the client equipment to the core network (notwithstanding that a service designer may make presentation specialisations for the client device's screen, audio or user interface).

4.3 Network topology, network functions, and reference points

The F5G network provides connectivity, and high-speed, and high-quality, network services for subscribers. Figure 4.3-1 shows the F5G network topology with reference points T/T', U/U', V/Vo and A10/A10' which is a simplified version of the figure from ETSI GS F5G 004 [i.3].

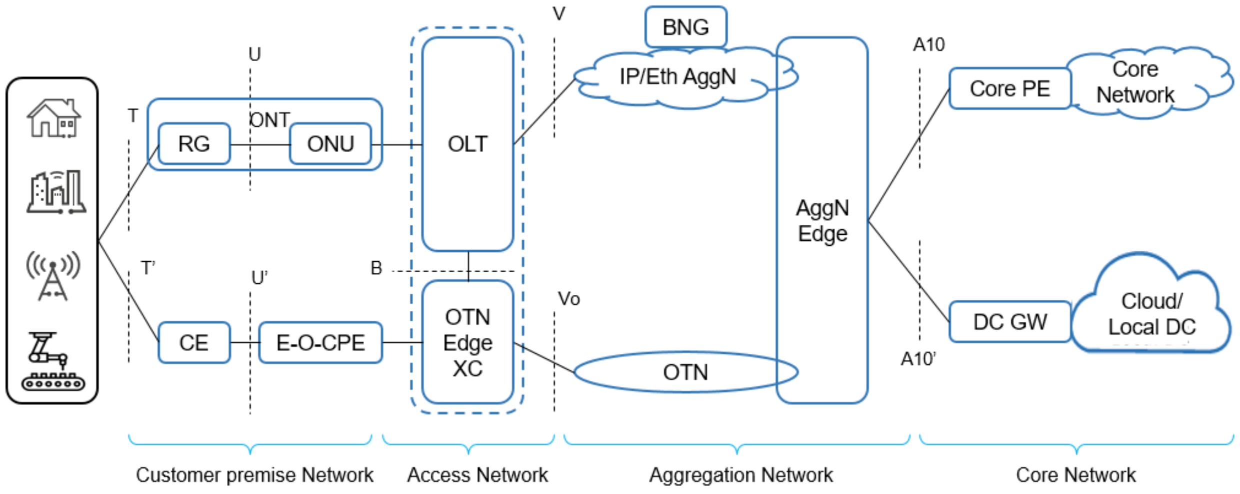


Figure 4.3-1: F5G network topology

In the case of premium private line, an OTN edge Customer Premises Equipment (O-E-CPE) represents the device that communicates with the OTN edge cross-connect on the network side, it is also the aggregation device for enterprise data. The enterprise network labelled Customer Equipment in Figure 4.3-1 and the Access Network is demarcated by the U' interface. The Optical Line Terminal (OLT) module in Figure 4.3-1 represents the data plane function of OLT and OTN edge cross-connect, the control and management function of OLT is not shown.

A Broadband Network Gateway (BNG) is a typical device in IP/Ethernet based Aggregation Network, which may be directly connected to an OLT or via an IP/Ethernet Aggregation network. A BNG may be implemented as a pool of devices although the pool represents a single function from the point of the present document. In some networks, there may be an IP aggregation network between the BNG and the Core Network. Besides typical IP/Ethernet aggregation network, OTN is also a possible option as complementary to typical IP/Ethernet aggregation. The OTN edge cross-connect aggregates the Access OTN traffic and will be a node on the OTN Aggregation Network. The Aggregation Network Edge represents the handover device between Aggregation Network and Core Network. It needs to identify and direct the traffic in both directions.

For the core network, considering local Data Centre (DC) and cloud service are getting more and more popular, it is an extension that expands the legacy core network. Even though the core network is not in the scope of the present document, the interfaces between Aggregation Network and Core Network need to be specified in the present document:

- The T interface is the handover point between adaptation box / E-CPE and the customer devices.
- The T' interface is the handover point between the CE and the enterprise devices.
- The V interface is the legacy IP/Ethernet based handover points between the Access Network and the Aggregation Network.

NOTE 1: It is anticipated that this interface will be improved in order to support new services.

- The B interface is the handover point between the OLT and the OTN edge cross connect.
- The Vo interface is the handover point between Access Network and OTN based Aggregation Network.

NOTE 2: For different services, the system may be configured to allow the OLT to handover the traffic via the V interface or the Vo interface.

- The A10 interface is the handover point between the Aggregation Network and the Core Network.

NOTE 3: In order to support new use cases in F5G, the A10 interface will be enhanced. The A10 interface is primarily Ethernet based, however, depending on reach, OTN may be used as the Ethernet transparent transport layer.

- The A10' interface is the handover point between the Aggregation Network and the Cloud or local DC.

For the purposes of the present document the system is bounded by the scope of each reference point and each reference point is assessed independently, and then in combination, to determine the overall system risk. The end-points of F5G are assessed as:

- Reference point T: user access point at which user's devices is identified, authenticated and connected to the Internet Services Provider (ISP) network.
- Reference point A10: the edge of ISP network where user's data is transmitted to the core network.
- Reference point A10': the edge of ISP network where user's data is transmitted to the local DC's.

The F5G network provides the following service to subscribers:

- Provide the access point for user's devices to connect to the carrier's network and from there to the services offered by the carrier, including access to the public Internet.
- Provide high-capacity, high-speed and high-quality, data aggregation and transporting services.

4.4 F5G security boundary and security objectives

As a working example of F5G the following scenarios apply:

- User's device connects to the Residential Gateway (RG) at reference point T, connects to the Optical Network Unit (ONU) at reference point U, connects either to IP/Eth AggN at reference point V or to OTN at reference point Vo, connects to the Core Network or Cloud/Local DC at reference point A10 or A10'.

- RG and ONU co-exist in the Customer Premise Network (reference point T faces user's devices, reference point U faces the Access network).

NOTE 1: The RG and ONU can be integrated as a single device named ONT or Home Gateway.

- OLT and OTN Edge XC co-exist in the Access network (reference point V faces the IP/Eth AggN and reference point Vo faces the OTN).

Each interconnecting device or service should only connect to peers with known and verifiable identifiers and thus build a trusted framework of network entities.

Dividing the security problem into a set of domains is a common approach and is offered below. It should be applied with care as there is a danger to consider domains in isolation and to forget, or to overlook, the inter-connectivity of these domains, and the use of one domain to attack another. It is also recognized that security design requires compartmentation such that a problem in one domain (compartment) can be isolated such that it does not impact another compartment (domain). Another design guideline is to simplify assumptions regarding the attacker, summarized by both Kerckhoff and Shannon:

- **Kerckhoff's principle [**i.7**]**: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

- **Shannon's restatement [**i.6**]**: "the enemy knows the system", i.e. "one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them".

The security objectives of each network domain in CIA(AA) paradigm are summarized below:

NOTE 2: The conventional Confidentiality, Integrity, Availability paradigm (the CIA paradigm) has been extended for greater clarification in ETSI TS 102 165-1 [i.5] as the CIAAA paradigm by the expansion of the "Availability" element to explicitly draw out the concepts of Authenticity (as a pre-requisite in access control) and Accountability (as a pre-requisite in integrity).

Table 4.4-1 provides a mapping of the security objectives and the threats defined in ETSI TS 102 165-1 [i.5].

Table 4.4-1: Threats to security objective types (from ETSI TS 102 165-1)

Threat	Objective type				
	Confidentiality	Integrity	Availability	Authenticity	Accountability
Interception (eavesdropping)	X				
Unauthorized access	X	X		X	X
Masquerade	X	X		X	X
Forgery		X	X	X	X
Loss or corruption of information		X	X		
Repudiation		X		X	X
Denial of service			X		

4.5 F5G stakeholder model

In order to assess the potential attacks it is essential to identify the stakeholders in the technology and services. A perfunctory analysis suggests the stakeholders include the manufacturers of equipment used in the F5G installations, the operators of services, the regulators of service, the direct customers or users of F5G (i.e. those offering traffic to the network), and indirect stakeholders who require access to knowledge, data or content of the network. The specific set of stakeholders is use case specific but for the purposes of the present document the simplified list above is used.

Several regulatory frameworks apply to any installation of F5G based systems and this includes the following (this list is indicative and no claim is made for its completeness in any market):

- General Data Protection Regulation (GDPR) defined in Regulation (EU) 2016/679 [i.11] and equivalent regulations in non-EU markets.

- Network Information Systems directive (NIS) defined in Directive (EU) 2016/1148 [i.12] and equivalent regulations in non-EU markets.

NOTE: There is, at the time of writing, a development to update and strengthen the NIS Directive Directive (EU) 2016/1148 [i.12] in order to further improve the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole in both the field of cybersecurity and critical infrastructure protection. Where possible the present document has addressed developments anticipated to be part of the updated NIS Directive.

- The Radio Equipment Directive (RED) defined in European Treaty Series No. 185 [i.13] and equivalent regulations in non-EU markets where radio equipment is used.
- Right to repair legislation may apply to ensure that CPE can be repaired and maintained independently of the original manufacturer and supply chain (this adds new entities into the trust model for F5G).
- Regional and national regulation concerning the safety of equipment.
- Regional and national regulation concerning the disposal of equipment at end of life (see also GDPR).

With respect to NIS Directive (EU) 2016/1148 [i.12] the F5G network will support both Operators of Essential Services and Digital Service Providers subject to any strengthening of the requirements the NIS directive will contain after revision.

In addition in many markets there is a broad requirement to enable lawful access to data and content of networks and specific obligations fall onto operators to ensure that their networks and services are appropriately enabled.

EXAMPLE: The European Treaty No. 185 [i.14] applies for members of Council of Europe.

4.6 Motivation and capability of attackers

Motivation of the attacker is difficult to accurately assess prior to an attack. However, in determining the level of protection that is required it is essential to consider motivations in order to address the forms of attack that need to be protected against. Motivation is addressed in some detail in clause 6.6.4 of ETSI TS 102 165-1 [i.5] and in Annex B of ETSI TS 102 165-1 [i.5]. For the purposes of the present document the attacker is assumed to have at least Medium motivation level to the attack, and to have at least limited capability.

NOTE 1: In ETSI TS 102 165-1 [i.5] the definition of medium motivation level considers that the threat agent will attempt to attack the system on a frequent basis and will be unlikely to be deterred by the existence of non-system deterrents. In addition, the same source defines a limited capability to indicate that the threat agent has modest capabilities and resources.

NOTE 2: With respect to motivation the role of insider attack is not addressed by the present document, rather the attackers (threat agents) are assumed to be external to the system.

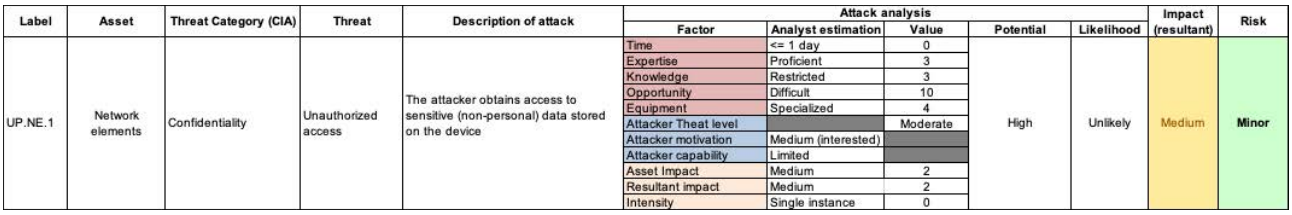
NOTE 3: The role of insider attack is often complex to analyse as an attacker may enrol an "insider" to perform part of the attack without that insider being aware of their role, however it remains as an external attack as the recruited "insider" is not the attacker, but rather a tool of the attacker.

NOTE 4: A non-system deterrent may include prosecution under things such as the Computer Misuse Act [i.21].

The assessment of an attacker's motivation and capability allows an estimation of threat level which for the purposes of the present document is classified as at least Moderate with potential to be either Severe or Critical.

An example of the impact of motivation on risk is shown in Tables 4.6-1 and 4.6-2. In Table 4.6-1 the motivation is set as "Medium+Limited" resulting in a Major risk, but increasing the motivation to "High+Significant" as shown in Table 4.6-2 results in a Critical risk. The assertion being that a more motivated attacker will take more time to ensure the attack is carried out hence more difficult to defend against, irrespective of the remainder of the analysis.

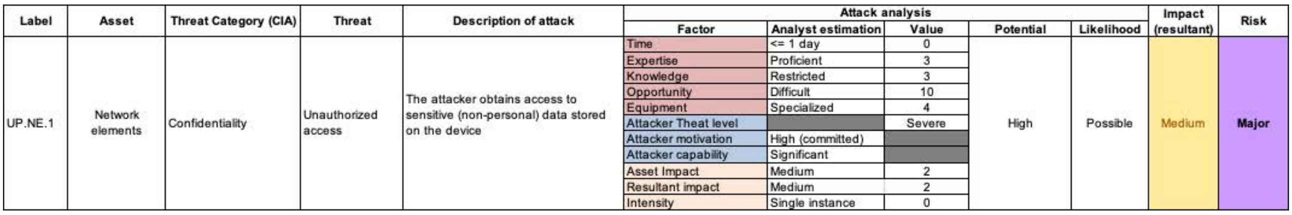
Table 4.6-1: Risk of an unauthorised access attack at CPE with Medium motivation and Limited capability



Label	Asset	Threat Category (CIA)	Threat	Description of attack	Attack analysis					Impact	Risk
					Factor	Analyst estimation	Value	Potential	Likelihood	(resultant)	
UP.NE.1	Network elements	Confidentiality	Unauthorized access	The attacker obtains access to sensitive (non-personal) data stored on the device	Time	<= 1 day	0	High	Unlikely	Medium	Minor
					Expertise	Proficient	3				
					Knowledge	Restricted	3				
					Opportunity	Difficult	10				
					Equipment	Specialized	4				
					Attacker Theat level		Moderate				
					Attacker motivation	Medium (interested)					
					Attacker capability	Limited					
					Asset Impact	Medium	2				
					Resultant impact	Medium	2				
					Intensity	Single instance	0				

A modification in assessment of motivation moves risk from Major (in Table 4.6-1) to Critical (in Table 4.6-2).

Table 4.6-2: Risk of an unauthorized access attack at CPE with High motivation and Significant capability



Label	Asset	Threat Category (CIA)	Threat	Description of attack	Attack analysis					Impact	Risk
					Factor	Analyst estimation	Value	Potential	Likelihood	(resultant)	
UP.NE.1	Network elements	Confidentiality	Unauthorized access	The attacker obtains access to sensitive (non-personal) data stored on the device	Time	<= 1 day	0	High	Possible	Medium	Major
					Expertise	Proficient	3				
					Knowledge	Restricted	3				
					Opportunity	Difficult	10				
					Equipment	Specialized	4				
					Attacker Theat level		Severe				
					Attacker motivation	High (committed)					
					Attacker capability	Significant					
					Asset Impact	Medium	2				
					Resultant impact	Medium	2				
					Intensity	Single instance	0				

The architecture of F5G includes aspects of Customer Premises Equipment (CPE) and if an insider attack is excluded the attacker has to be suitably motivated to be able to access the CPE. Thus in the example offered in Table 4.6-1 the less motivated and capable attacker is assumed to be dissuaded from the attack by not being willing to make an attempt to physically access the device, whereas a more motivated attacker is not dissuaded and raises the risk of the same attack from Minor to Major.

See also Annex A which refers to the core analysis tools/worksheets used in the derivation of the figures given in Tables 4.6-1 and 4.6-2.

5 F5G threat analysis

5.1 Summary of analysis

The analysis is presented in the format of analysing attacks from the CIA paradigm against specific physical assets and logical assets in the F5G architecture outlined in Figure 4.2-1 of clause 4.2.

The normal conduct of an analysis is recursive and should begin with no assumptions regarding countermeasures, or what is to be included by default. As a result of the first round of analysis where major and critical risks are identified and strategies to mitigate them proposed the analysis should be repeated in order to identify the new residual risk. This process should then be repeated, recursively, until the residual risk identified is within reasonable and manageable bounds.

NOTE 1: There is zero likelihood of a zero risk environment and some level of residual and background risk has to be accepted.

NOTE 2: For the purposes of the present document this is first pass analysis and identifies some significant results that are intended for the purpose of optimizing the development of future standards.

It is recognized that each user of a network places their own value on the data or content they distribute across the F5G enabled network. Insofar as is possible the analysis presented in the present document does not consider any relative values of user data but treats any manipulation of user data as high impact with respect to the user. There is a broad assumption that the level of impact as viewed by the infrastructure rises across these data domains in a manner consistent with that described in ETSI TS 102 165-1 [i.5] and shown in Table 5.1-1. In the present document the impact also considers the number of devices or users affected by a specific threat, therefore an attack that impacts only one subscriber line from many thousands of lines can be considered as low impact from the viewpoint of the infrastructure. If however multiple users are impacted by the loss of a single connection this should be considered in the impact. In some instances this may require joint liability for threat management on both CPE and Core network provisions.

NOTE 3: The present document's purpose is to identify network side provisions to mitigate against attacks on the network, thus attacks against a single customer are not considered in depth other than to mitigate as far as possible the use of network resources in propagating an attack against a single customer.

NOTE 4: Each stakeholder is expected to undertake a business risk analysis to identify the impact of attacks on their systems, thus if the CPE/CPN connection is essential for the support of systems and processes where the loss of a single point of connectivity has High impact the stakeholder is expected to take steps to ensure resilience of connectivity.

Table 5.1-1: Asset impact (from ETSI TS 102 165-1 [i.5])

Impact	Explanation	Value
Low	The concerned party is not harmed very strongly; the possible damage is low.	1
Medium	The threat addresses the interests of providers/subscribers and cannot be neglected.	2
High	A basis of business is threatened and severe damage might occur in this context.	3

In determining risk the second factor taken into consideration is the likelihood of an attack. The method given in ETSI TS 102 165-1 [i.5] assesses likelihood (see Table 5.1-2) across a number of metrics based on the capability of the attacker (see Table 5.1-3).

Table 5.1-2: Occurrence likelihood (from ETSI TS 102 165-1 [i.5])

Value	Likelihood of occurrence	Explanation
1 (note 1)	Very unlikely	According to up-to-date knowledge, there are no means of solving the technical difficulties to state the threat (see note 2) irrespective of the motivation or resources available to the attacker.
1	Unlikely	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat or the motivation for an attacker is very low.
2	Possible	The technical requirements necessary to state this threat are not high and could be solved without significant effort; furthermore, there is a reasonable motivation for an attacker to perform the threat.
3	Likely	There are no sufficient mechanisms installed to counteract this threat and the motivation for an attacker is quite high.
3 (note 1)	Very likely	As for very likely but the threat is considered more imminent.
NOTE 1: The values assigned to "Very unlikely" and "Unlikely" are identical, similarly the values assigned to "Likely and "Very likely" are identical. The rationale is that they represent extreme poles but in each case do not equate to risk escalation. NOTE 2: The term "state the threat" refers to having all the facilities available to mount the attack which includes being able to fully describe and rationalize it.		

The metrics for calculating an attacker's capability are shown in Table 5.1-3. The weightings in Table 5.1-3 are described in ETSI TS 102 165-1 [i.5] and are broadly relative weightings.

Table 5.1-3: Attack potential metrics from ETSI TS 102 165-1 [i.5] (table extended)

Factor	Range	Value (see note 4)
Time (elapsed time)	≤ 1 day	0
	≤ 1 week	1
	≤ 2 weeks	2
	≤ 1 month	4
	≤ 2 months	7
	≤ 3 months	10
	≤ 4 months	13
	≤ 5 months	15
	≤ 6 months	17
	> 6 months (see note 1)	19
Expertise	**Layman** 'Laymen are unknowledgeable compared to experts or proficient persons, with no particular expertise'	0
	Proficient 'Proficient persons are knowledgeable in that they are familiar with the security behaviour of the product or system type'	3
	Expert 'Experts are familiar with the underlying algorithms, protocols, hardware, structures, security behaviour, principles and concepts of security employed, techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc. implemented in the product or system type'	6
	Multiple experts 'As for expert but addressing the case where multiple experts are brought together to work as a team'	8
Knowledge	**Public** 'Public information concerning the asset (e.g. as gained from the Internet)'	0
	Restricted 'Restricted information concerning the asset (e.g. knowledge that is controlled within the developer organization and shared with other organizations under a non-disclosure agreement)'	3
	Sensitive 'Sensitive information about the asset (e.g. knowledge that is shared between discreet teams within the developer organization, access to which is constrained only to members of the specified teams)'	7
	Critical 'Critical information about the asset (e.g. knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking)'	11
Opportunity	**Unnecessary/ unlimited access** 'the attack does not need any kind of opportunity to be realized'	0
	Easy 'access is required for less than a day or that the number of asset samples required to perform the attack is less than ten'	1
	Moderate 'access is required for less than a month or that the number of asset samples required to perform the attack is less than fifty'	4
	Difficult 'access is required for at least a month or that the number of asset samples required to perform the attack is less than one hundred'	10
	None (see note 2) 'the opportunity window is not sufficient to perform the attack (the length for which the asset to be exploited is available or is sensitive is less than the opportunity length needed to perform the attack - for example, if the asset key is changed each week and the attack needs two weeks)'	999

Factor	Range	Value (see note 4)
Equipment	**Standard** 'Standard equipment is readily available to the attacker, either for the identification of a vulnerability or for an attack. This equipment may be a part of the asset itself (e.g. a debugger in an operating system), or can be readily obtained (e.g. Internet downloads, protocol analyser or simple attack scripts)'	0
	Specialized (see note 3) 'Specialized equipment is not readily available to the attacker, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g. power analysis tools, use of hundreds of PCs linked across the Internet would fall into this category), or development of more extensive attack scripts or programs'	4
	Bespoke 'Bespoke equipment is not readily available to the public as it may need to be specially produced (e.g. very sophisticated software), or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive'	7
	Multiple bespoke 'extends the definition of bespoke equipment to address where multiple instances of equipment are used by the attacker, e.g. addressing the recruitment of multiple devices in establishing a botnet'	9
NOTE 1: A successful attack requires in excess of 6 months. NOTE 2: None means that the window of opportunity is not sufficient to perform the attack. NOTE 3: If clearly different groups of specialized equipment are required for distinct steps of an attack, this should be rated as bespoke. NOTE 4: The weightings are relative indices and outlined in Common Criteria ISO/IEC 15408-2 [i.22] and are described in the TVRA method, ETSI TS 102 165-1 [i.5].		

In adopting the TVRA method [i.5], the vulnerability rating and attack potential values are mapped to the likelihood of attack as shown in Table 5.1-4.

Table 5.1-4: Mapping of vulnerability rating to likelihood of attack

Vulnerability rating	Attack potential values	Likelihood of attack
Basic	0 to 13	Likely
Moderate	14 to 19	Possible
High	> 20	Unlikely

TVRA method calculated the risk of identified threats using estimated values for the likelihood of occurrence (values 1 to 3) and impact (values 1 to 3) of threat to the system. As shown in Table 5.1-5, three levels of risk are defined as the product of each of impact and likelihood: Minor risks are mapped to where the risk is calculated as 1 or 2, Major risks are mapped to where the risk is calculated as 3 or 4. and Critical risks are mapped to where the risk is calculated as 6 or 9. Urgent and priority countermeasures should be specified for threats ranked as critical. Major risk should also be handled with attention. Minor risk can be handled optionally.

Table 5.1-5: Risk assessment

Likelihood	Impact		
	Low (1)	**Medium (2)**	**High (3)**
Unlikely (1)	Minor (1)	Minor (2)	Major(3)
Possible (2)	Minor (2)	Major (4)	Critical (6)
Likely (3)	Major (3)	Critical (6)	Critical (9)

The traffic light presentation in Table 5.1-5 offers critical risks as red (for danger), yellow/amber (for warning), and green (for ok to go with caution).

5.2 Trust in F5G

Trust relationships in F5G are considered as part of the connectivity relationships in F5G. In the context of F5G security an understanding of trust is required in order to identify when and how a relationship or transaction between F5G entities can be relied upon.

NOTE: Trust relationships are only one of many aspects of the connectivity relationships in F5G, trust is often reinforced using cryptographic security mechanisms with the key management trust relationship being particularly critical.

Trust measures can combine a variety of security assurance elements that include identity, attribution, attestation and non-repudiation. In F5G the following objectives for trust apply:

- Establish guidance for F5G trust in platform, software, policies, processes, practices and interoperability.
- Define areas of consideration where technologies, practices and processes have novel requirements to be addressed in F5G systems and operations.
- Supply guidance for the operational environment that supports and interfaces with F5G systems and operations, but avoid redefining any security considerations that are not specific to F5G.
- The ability to specify and enforce detailed trust relationships for and between virtualisation resources for End-to-End Trust Lifecycle Management.

The assignment of trust in F5G is the decision that an entity A should trust entity B in one or more particular contexts. Key criteria for assigning trust are:

- the identity of the entity to be trusted;
- the contexts within which the trust should be constrained.

In F5G, across planes and internally to each plane, are a number of transitive trust relationships that have to be addressed in order to give assurance of the overall integrity of the F5G network. The security relationships of F5G, in addition to countering risks and attacks on the system, are used to reinforce trust relationships. Recognizing that many of the relationships in F5G will be transitive the overall trust model is likely to embrace one or more models of delegated trust:

- Delegated trust:
  - entity A is unable to evaluate the appropriate level of trust for a relationship with another entity B, thus entity A may choose to delegate the decision to another entity C.
- Collaborative trust:
  - two entities (entities A and C) work together to decide whether to trust another (entity B) - the final goal may be for both entity A and entity C to have a trust relationship with entity B.
- Transitive trust:
  - entity A trusts entity B because entity C trusts it.

A more complete description of the role of trust in networks is found in ETSI GR NFV-SEC-003 [i.15].

Within the F5G model trust should be constrained within each plane, and for very specific relationships between planes. Thus each of the underplay plane, the service plane and the management plane should represent a single trust domain. A trust manager, or root of trust should exist within each plane from which both transitive trust and delegated trust relationships can be assured.

There is a close relationship between trust and both virtual and physical relationships. Thus CPE/CPN, being physically isolated from the bulk of the planes should initially be treated as less trusted.

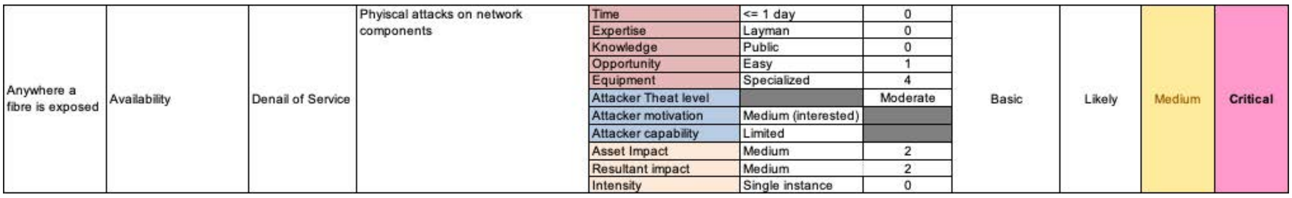
In a complete definition of countermeasures, following on from the content of the present document, the trust relationships should be explicitly identified for each countermeasure.

5.3 Physical attacks

NOTE: This is added for completeness only as the attacks described are not unique to F5G.

The F5G network is composed of a number of physical elements including fibre, routers, computing elements, switches, and so on. Many attacks on the physical components are non-malicious and may involve simple accidents (e.g. disconnecting leads by tripping over an exposed lead), natural phenomena (e.g. flooding or lightning strike), 3rd party incidents (e.g. construction works cutting a cable), animal problems (e.g. rodents destroying cable). It is expected that reasonable provisions are taken against physical attack. Such measures should routinely include using armoured cable, armoured cable runs, the use of Uninterruptable Power Supplies (UPS) to counter power outages, using enclosures with higher ratings against dust and water contamination (e.g. IPX6 and higher), and using reasonable means to isolate critical equipment from unauthorized access (e.g. by using dedicated equipment rooms in CPE/CPN installations).

Table 5.3-1: Risk calculation for physical attacks on F5G equipment



Anywhere a fibre is exposed	Availability	Denail of Service	Phyiscal attacks on network components	Time	<= 1 day	0	Basic	Likely	Medium	**Critical**
				Expertise	Layman	0				
				Knowledge	Public	0				
				Opportunity	Easy	1				
				Equipment	Specialized	4				
				Attacker Theat level		Moderate				
				Attacker motivation	Medium (interested)					
				Attacker capability	Limited					
				Asset Impact	Medium	2				
				Resultant impact	Medium	2				
				Intensity	Single instance	0				

The risk calculation as shown in Table 5.3-1 highlight that the risk to the system is critical from physical attack as although the impact is often only medium (it affects a limited set of users) the likelihood without adequate measures in place is "Likely" (there may be instances where the likelihood is changed to "Highly Likely" but the risk remains Critical). (See also Annex A which refers to the core analysis tools/worksheets used in the derivation of the figures given in Table 5.3-1.)

In assessing the risk of physical attack there is often no need for particularly specialized equipment or for particularly detailed knowledge of the system. An errant employee could incapacitate a corporate network by simply pulling power plugs from the wall, or by disconnecting an optical feed cable. A more angry or less controlled physical attack is just as likely. As indicated above physical attacks may be as a result of poor design of cables or ducts, of failure to consider the impact of rain or other sources of flooding. The majority of physical attacks are mitigated by methods that are often not classified as security techniques, and rarely as ICT security techniques hence outside of the primary scope of the present document, however it is recommended that reasonable physical security should be addressed in installation in order that any higher order security mechanisms such as those of any cryptographic nature are not impacted.

5.4 Attacker profiles

One purpose of the present analysis is to determine any distinguishing features of F5G when compared to any other networking technology that suggests the existence of attack modes that are unique to F5G. In this respect attacks at the higher layers of the OSI stack, primarily those in the service plane and the MCA plane, are likely to share a number of common characteristics with conventional networks, in addition attacks against virtualisation or AI analysis in the service and MCA planes are not considered to be unique to F5G or to optical underlay networks. In looking to the attacker-victim relationship there are a number of victim forms:

- Individuals lying in the CPN/CPE domain.
- ISPs accessed through the core network and accessible at any of the open interfaces between the CPN/CPE and the core network.
- The core network provider, accessible at any of the open interfaces of the F5G system and both directly and indirectly by data manipulation.
- Interconnected networks by manipulation of the traffic management at the Management Control and Analysis Plane.
- Data in any form is a target of attack.

The aims of the attacker are assessed by consideration of the violation of the principles of the CIA paradigm.

5.5 Assets in the underlay plane

The underlay plane consists of optical and ETH/IP packet components.

NOTE 1: There are a number of documents from ETSI and IETF that address vulnerabilities and attacks on IP and IP based systems and networks (including IP as infrastructure) that can be readily found using any internet search engine, in addition a large number of implementation vulnerabilities are catalogued in resources including the CVE list (www.cve.org) [i.4] and the US based National Vulnerability Database (NVD) [i.20].

- User data (and content)

NOTE 2: For users it is necessary to address both user specific signalling data, i.e. data that informs the network, and user specific data content, i.e. data owned by, or which the user has privileged access to, and to which the network does not have the same level of access.

- Network elements:
  - Includes O-E-CPE, ONU, OLT, OTN Edge-XC, IP/Eth and OTN fabric, and AggN Edge equipment as shown in Figure 4.3-1
- Signalling assets including:
  - Core network service signalling:
    - Signalling or control data exchanged between the CPN and the CN equipment.
  - Customer premises network service signalling:
    - Signalling or control data exchanged between the CPE and CPN equipment.

5.6 Assets in the service plane

In a simple analysis such as that given in the present document the service plane of F5G shares commonality with many other network technologies. Where the service plane is offering many conventional IP services such as the Domain Name Service (DNS) and its associated name to address resolution any threats to such services is not unique to F5G.

The service plane consists of the software providing accessing, switching and routing services range from layer-1 to layer-3 of the OSI stack as they apply to the particularities of the underlay plane.

- Access service:
  - Provides connection services.
- Data processing service:
  - Processes service data and enabling efficient data forwarding and routing.

In addition to the service assets each service above offers a Service Access Point (SAP) in common with the OSI model giving access to a Service Processing Point (SPP) within the service itself.

As noted above for the present document there is no detail consideration of the service plane. A more detailed analysis should however be completed when countermeasures are defined as the OSI model will use the service plane to drive security functions of the underlay plane. As has been stated in clause 4 the abstraction, information hiding, and compartmentalisation offered by the OSI model is a fundamental element of providing a secure framework. The service plane is a consumer of performance information data from the underlay plane and with further collaboration from the MCA plane is used to ensure that the underlay plane can maintain the promise of GRE with FCC at the heart of F5G. Attacks against the service plane, in like manner to attacks against the MCA plane (see clause 5.7), may result in harm to the underlay plane but application of the OSI approach similarly suggests that the optical nature of the underlay plane is masked from the service plane.

5.7 Assets in the network management plane

The MCA plane consists of Management and Control (M&C) software, digital twin and AI analyser providing efficient and intelligent network management and maintaining services in layer-7 (application layer) of the OSI stack as they apply to the particularities of the underlay plane and the associated service plane (see clause 5.6).

From a security perspective access at the management plane is likely to map to access to critical operational controls, the impact of any attack at the management level is likely to be high (i.e. as in Table 5.1-1 "A basis of business is threatened and severe damage might occur in this context"). The shared or common nature of the MCA plane to non-optical networks means that whilst the MCA plane will be attacked the peculiarities of the optical nature of the underlay plane has negligible influence on the MCA plane.

NOTE: Digital twin and AI analyser are AI-based functions of the F5G network. The security of AI is being addressed by work items from ETSI ISG SAI and readers are referred to there for details of general AI security threats. The threat analysis of the MCA plane in the present document addresses the non-AI aspects of the M&C service inside the MCA plane.

- M&C services including:
    - local M&C service accessed using commonly available protocols and services (e.g. SSH, Telnet, FTP, Web service at LAN side);
    - remote M&C service accessed using commonly available protocols and services (e.g. CPE WAN Management Protocol (CWMP) defined in TR-069 [i.23], SNMP, NETCONF, Web service at WAN side).

In like manner to the assessment of the Service Plane (see clause 5.6) the As noted above for the present document there is no detailed consideration of the MCA plane. A more detailed analysis is for further study.

5.8 Underlay plane threat analysis

User data transmitted over the F5G network is treated as user content and includes voice, video and other internet-based application content such as e-mail, and e-commerce transactions.

An attacker able to access the content of user communication may be in a position to cause harm to the user. The extent of harm is dependent on the exact nature of the content. In addition, both the network provider and the end-points for receiving user data can be required to comply with specific legal obligations to protect the user content.

EXAMPLE 1: In Europe the network and service provider have obligations under GDPR [i.11] to protect user data from exploitation.

Attackers are considered motivated to access user data and content for a number of reasons.

EXAMPLE 2: Data that informs the network of the identity of the user, or that associates a service to a user, may be attacked with a view to masquerade as that user, or to inhibit the user from accessing the network (denial of service), or to direct malicious content to the user.

EXAMPLE 3: Attacks on data content may be conducted with an intent to steal user-owned or generated content, or to manipulate user-owned data assets.

The threat analysis, as noted in clauses 4 and 5 of the present document, addresses the CIA paradigm and threats to it. In the F5G, concentrating on the underlay plane, there are multiple points of attack open to the attacker. Thus all of the assets described in clause 5.5 are considered to have vulnerabilities.

NOTE: The model given in ETSI TS 102 165-1 [i.5] applies wherein a **threat** is enacted by a **threat agent**, and may lead to an **unwanted incident** breaking certain pre-defined security objectives established for F5G, and in addition a **vulnerability** is modelled as a **weakness** that can be exploited by one or more **threats.**

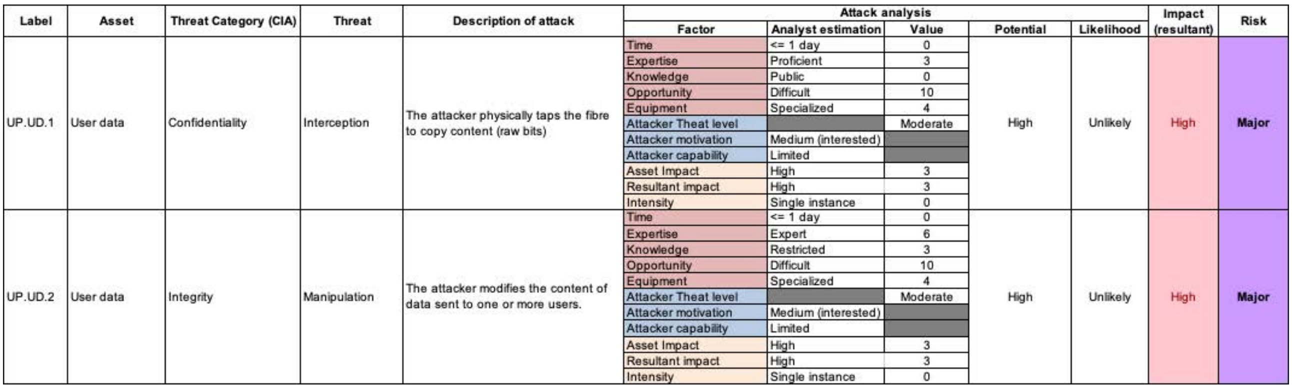
The core model of attacks is as follows:

- every connection is open to interception (breach of confidentiality);
- every processing point is open to a data manipulation attack (breach of integrity);

- every connection between peers is open to one of the peers not being who/what is expected but masquerading as legitimate entity (breach of availability).

A more detailed threat analysis to user data in the Underlay Plane is elaborated in Table 5.8-1 (see also Annex A which refers to the core analysis tools/worksheets used in the derivation of the figures given in Table 5.8-1).

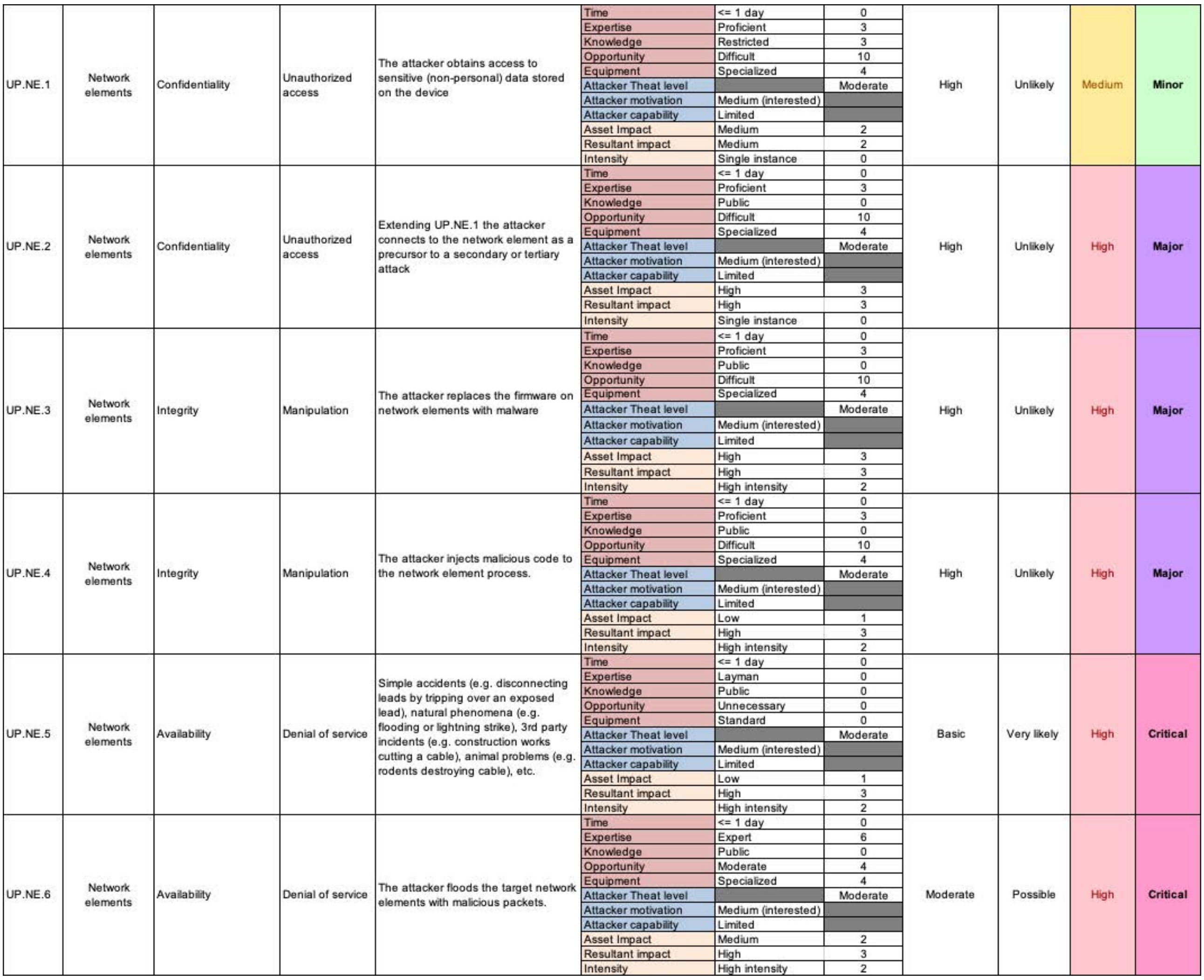
Table 5.8-1: User plane quantitative threat assessment (user data)



Label	Asset	Threat Category (CIA)	Threat	Description of attack	Attack analysis					Impact (resultant)	Risk
					Factor	Analyst estimation	Value	Potential	Likelihood		
UP.UD.1	User data	Confidentiality	Interception	The attacker physically taps the fibre to copy content (raw bits)	Time	<= 1 day	0	High	Unlikely	High	Major
					Expertise	Proficient	3				
					Knowledge	Public	0				
					Opportunity	Difficult	10				
					Equipment	Specialized	4				
					Attacker Theat level		Moderate				
					Attacker motivation	Medium (interested)					
					Attacker capability	Limited					
					Asset Impact	High	3				
					Resultant impact	High	3				
					Intensity	Single instance	0				
UP.UD.2	User data	Integrity	Manipulation	The attacker modifies the content of data sent to one or more users.	Time	<= 1 day	0	High	Unlikely	High	Major
					Expertise	Expert	6				
					Knowledge	Restricted	3				
					Opportunity	Difficult	10				
					Equipment	Specialized	4				
					Attacker Theat level		Moderate				
					Attacker motivation	Medium (interested)					
					Attacker capability	Limited					
					Asset Impact	High	3				
					Resultant impact	High	3				
					Intensity	Single instance	0				

For UP.UD.1 the mechanisms for tapping are described in [i.8]. The attack requires a significant degree of expertise or skill to gain physical access to a fibre that is generally contained in an armoured cable, and the tapping equipment, whilst relatively common, is specialized. Similarly in assessing the attack likelihood for UP.UD.2 the attacker needs to be able to selectively identify the content of a user-level message, remove it in order to replace it, and to modify it. In each case the attack is classified as resulting in a Major risk to the overall system and thus should be seen as a priority to counter. In each case the asset impact is classified as high as the User Data element is directly related to the user and in this instance the impact to the user is assessed, rather than the impact to the wider network. The Underlay Plane is the fundamental physical network plane, which is comprised of physical elements including fibre, routers, computing elements, switches, and so on. An attacker is expected to exploit vulnerabilities in hardware and software to obtain system control or crash the system of the network element for purposes including building a botnet, or causing network failure. In addition the physical security issues illustrated in clause 5.3 apply. A quantitative threat analysis using the method of ETSI TS 102 165-1 [i.5] to network elements from Underlay Plane is elaborated in Table 5.8-2 (see also Annex A which refers to the core analysis tools/worksheets used in the derivation of the figures given in Table 5.8-2).

Table 5.8-2: User plane quantitative threat assessment (network elements)



UP.NE.1	Network elements	Confidentiality	Unauthorized access	The attacker obtains access to sensitive (non-personal) data stored on the device	Time	<= 1 day	0	High	Unlikely	Medium	Minor
					Expertise	Proficient	3				
					Knowledge	Restricted	3				
					Opportunity	Difficult	10				
					Equipment	Specialized	4				
					Attacker Theat level		Moderate				
					Attacker motivation	Medium (interested)					
					Attacker capability	Limited					
					Asset Impact	Medium	2				
					Resultant impact	Medium	2				
					Intensity	Single instance	0				
UP.NE.2	Network elements	Confidentiality	Unauthorized access	Extending UP.NE.1 the attacker connects to the network element as a precursor to a secondary or tertiary attack	Time	<= 1 day	0	High	Unlikely	High	Major
					Expertise	Proficient	3				
					Knowledge	Public	0				
					Opportunity	Difficult	10				
					Equipment	Specialized	4				
					Attacker Theat level		Moderate				
					Attacker motivation	Medium (interested)					
					Attacker capability	Limited					
					Asset Impact	High	3				
					Resultant impact	High	3				
					Intensity	Single instance	0				
UP.NE.3	Network elements	Integrity	Manipulation	The attacker replaces the firmware on network elements with malware	Time	<= 1 day	0	High	Unlikely	High	Major
					Expertise	Proficient	3				
					Knowledge	Public	0				
					Opportunity	Difficult	10				
					Equipment	Specialized	4				
					Attacker Theat level		Moderate				
					Attacker motivation	Medium (interested)					
					Attacker capability	Limited					
					Asset Impact	High	3				
					Resultant impact	High	3				
					Intensity	High intensity	2				
UP.NE.4	Network elements	Integrity	Manipulation	The attacker injects malicious code to the network element process.	Time	<= 1 day	0	High	Unlikely	High	Major
					Expertise	Proficient	3				
					Knowledge	Public	0				
					Opportunity	Difficult	10				
					Equipment	Specialized	4				
					Attacker Theat level		Moderate				
					Attacker motivation	Medium (interested)					
					Attacker capability	Limited					
					Asset Impact	Low	1				
					Resultant impact	High	3				
					Intensity	High intensity	2				
UP.NE.5	Network elements	Availability	Denial of service	Simple accidents (e.g. disconnecting leads by tripping over an exposed lead), natural phenomena (e.g. flooding or lightning strike), 3rd party incidents (e.g. construction works cutting a cable), animal problems (e.g. rodents destroying cable), etc.	Time	<= 1 day	0	Basic	Very likely	High	Critical
					Expertise	Layman	0				
					Knowledge	Public	0				
					Opportunity	Unnecessary	0				
					Equipment	Standard	0				
					Attacker Theat level		Moderate				
					Attacker motivation	Medium (interested)					
					Attacker capability	Limited					
					Asset Impact	Low	1				
					Resultant impact	High	3				
					Intensity	High intensity	2				
UP.NE.6	Network elements	Availability	Denial of service	The attacker floods the target network elements with malicious packets.	Time	<= 1 day	0	Moderate	Possible	High	Critical
					Expertise	Expert	6				
					Knowledge	Public	0				
					Opportunity	Moderate	4				
					Equipment	Specialized	4				
					Attacker Theat level		Moderate				
					Attacker motivation	Medium (interested)					
					Attacker capability	Limited					
					Asset Impact	Medium	2				
					Resultant impact	High	3				
					Intensity	High intensity	2				

In the analysis of attacks against network elements the attacks that lead to critical risk are anticipated to be relatively straightforward to implement (hence the likelihood assessments of Very Likely (UP.NE.5) and Possible (UP.NE.6)). In assessing attacks for UP.NE.5 it is assumed that some of the "accidental" attack types will cover a wide geographic region and therefore act as a low impact attack on multiple fronts. In attacks UP.NE.4 and UP.NE.3 there is a requirement that the attacker knows detailed knowledge of the system or device operation in order to install software with a malicious payload.

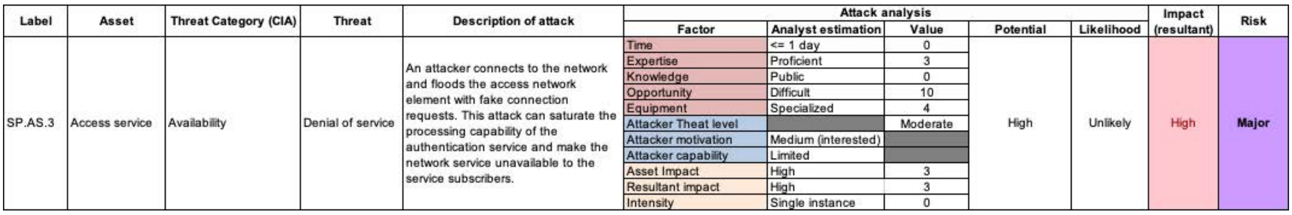
5.9 Service plane threat analysis

The service plane offers services that are largely common to most telecommunications service providers. Whilst there may be some specializations of the service plane for the particularities of the underlay plane the bulk of attacks in the service plane address the layered provision of countermeasures from the service plane to the underlay plane. In this regard whilst it is reasonable to assume that a point of attack will be the authentication protocols, identity management and key management entities, it is premature to determine the risk whilst those services are speculative (i.e. the countermeasures of authentication, identity management and associated key management are not defined).

In a similar manner to the paragraph above, the management of service plane specific data services that enable signal data processing, traffic steering and network slicing, are not clearly differentiated between an optical network and any other network format. However whist it is reasonable to suggest that a motivated attacker will exploit the vulnerabilities in data processing there are many general studies for this that are widely available. The detail analysis of the F5G peculiarities with respect to services over the underlay plane are for further study.

Table 5.9-1 offers an example of the form of attack and resulting risk that may apply to the service plane (see also Annex A which refers to the core analysis tools/worksheets used in the derivation of the figures given in Table 5.9-1).

Table 5.9-1: Example analysis of attack at the service plane to initiate denial of service



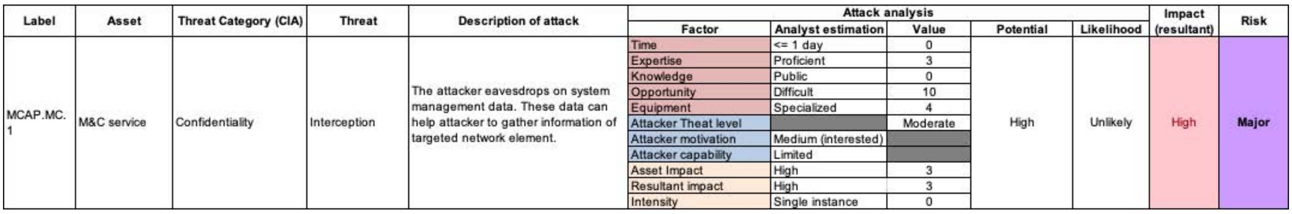
Label	Asset	Threat Category (CIA)	Threat	Description of attack	Attack analysis					Impact (resultant)	Risk
					Factor	Analyst estimation	Value	Potential	Likelihood		
SP.AS.3	Access service	Availability	Denial of service	An attacker connects to the network and floods the access network element with fake connection requests. This attack can saturate the processing capability of the authentication service and make the network service unavailable to the service subscribers.	Time	<= 1 day	0	High	Unlikely	High	Major
					Expertise	Proficient	3				
					Knowledge	Public	0				
					Opportunity	Difficult	10				
					Equipment	Specialized	4				
					Attacker Theat level		Moderate				
					Attacker motivation	Medium (interested)					
					Attacker capability	Limited					
					Asset Impact	High	3				
					Resultant impact	High	3				
					Intensity	Single instance	0				

5.10 MCA plane threat analysis

The management and control service hosts a suite of functions for network configuration, service deployment and network operation. Any attack at the MCA is likely to impact multiple users and almost by default can be assumed to be of at least medium impact with many attacks reaching high impact. Whilst it would be normal to assume that all functions in the MCA plane are only open to authorized and authenticated parties the starting point of analysis assumes that such provisions, even if normally required, are not provisioned. The purpose is to identify where to place the countermeasures and not to make simplifying assumptions, as any simplifying assumption is also a risk. Therefore for the present document, acting as a base analysis, the threats to the MCA plane are not fully explored pending further determination of the countermeasures to threats identified in the underlay plane.

In like manner to the service plane Table 5.10-1 offers an example of the risk assessment for an attack against the MCA plane (see also Annex A which refers to the core analysis tools/worksheets used in the derivation of the figures given in Table 5.10-1).

Table 5.10-1: Example analysis of attack at the MCA plane to initiate future attacks



Label	Asset	Threat Category (CIA)	Threat	Description of attack	Attack analysis					Impact (resultant)	Risk
					Factor	Analyst estimation	Value	Potential	Likelihood		
MCAP.MC.1	M&C service	Confidentiality	Interception	The attacker eavesdrops on system management data. These data can help attacker to gather information of targeted network element.	Time	<= 1 day	0	High	Unlikely	High	Major
					Expertise	Proficient	3				
					Knowledge	Public	0				
					Opportunity	Difficult	10				
					Equipment	Specialized	4				
					Attacker Theat level		Moderate				
					Attacker motivation	Medium (interested)					
					Attacker capability	Limited					
					Asset Impact	High	3				
					Resultant impact	High	3				
					Intensity	Single instance	0				

6 F5G mitigation strategies

6.1 Method and approach

The purpose of this clause is to provide high level recommendations of countermeasures to counter the risks from the threats identified in clause 5 of the present document. In very simple terms a countermeasure is formed in a triplet of {threat, security-dimension, countermeasure}. Many countermeasures often have to be combined. In order to enable an encryption countermeasure it is necessary to identify cryptographic keying strategy, an identity strategy (to ensure that the key is delivered to the correct entity), a re-keying strategy, and a scoping strategy (i.e. the end points of the encryption measure).

EXAMPLE: To counter threats to confidentiality the following triple {interception, confidentiality, encryption} is formed.

In general countermeasures are distributed and support a relationship, or more precisely a security association. A security association, in addition to the triplets described above, identify the following:

- the relying party;
- the dependent party;
- any independent related party or parties;
- the nature of the relationship;
- the lifetime of the relationship.

A security association can be defined using architecture, protocol or policy.

6.2 Architectural mitigation strategies

NOTE: An architectural mitigation is the separation into security domains. This means having distinct security policies for each of the planes.

As stressed in the core of the present document, the F5G architecture is divided into distinct planes. This forms part of the mitigation strategy and is extended by use of managed trust zones in each plane and between each plane. If any trust zone is compromised the overall trust in the F5G facility is only minimally impacted.

6.3 Protocol mitigation strategies

Every protocol used in the F5G should ensure that the parties to the protocol are able to be identified and their authority to perform actions confirmed. On the understanding that systems are initialized on the basis of zero trust appropriate measures to build trust per protocol and per set of stakeholders per protocol should be applied. This is closely integrated to the architecture and to the policy mitigations.

6.4 Policy mitigation strategies

In the context of F5G policy mitigation strategies should be developed to give confidence in the supply chain. Included in the supply chain should be considerations of staff training and selection, staff vetting for roles associated to critical network elements, and similar. The impact of standardisation on such non-technical policy roles is minimal although some guidance documents are offered in Annex B.

6.5 Other mitigations

As indicated in clause 5.3 there are a series of attacks against the physical infrastructure. Many mitigations against physical attack require application of in-depth design and engineering. Some of the basic forms of mitigation are outlined in clause 5.3 and are repeated here and expanded upon.

As indicated in clause 5.3 measure to contain risk arising from physical damage and accidental damage include the use of armoured cable and armoured cable runs, which are addressed in a number of standards including those from ISO/IEC and summarized in Annex A, the use of Uninterruptable Power Supplies (UPS) to counter power outages, using enclosures with higher ratings against dust and water contamination (e.g. IPX6 and higher, see IEC 60529 [i.24]), and using reasonable means to isolate critical equipment from unauthorized access (e.g. by using dedicated equipment rooms in CPE/CPN installations).

Where a dedicated computer room for assets in the M&C plane, and in the service plane, is used some of the considerations as below apply.

- Location:
  - Not located in rooms with external walls with ability to isolate physical access to the facility.

- Air conditioning:
    - Required to enable a thermally controlled, and humidity controlled, environment, with clean room like conditions to minimize risks from dust and other foreign object intrusions.
- Fire protection:
    - Detection and protection facilities should be "dry" and non-conductive to both extinguish the fire but to also ensure survivability of equipment.
- Future-proofing:
    - Demand will grow thus the facility will require additional capacity (all dimensions) at some point and this has to be considered in the design.
- Redundancy:
    - Whilst existing standards for optical fibre use allow for redundancy at the transmission level additional redundancy has to be considered for power supply, cooling and fire control.

6.6 Specific actions against identified risks

In preceding clauses a number of threats have been subject to quantitative risk analysis. The measures in Table 6.6-1 are considered for each of the attacks outlined in clause 5.8.

Table 6.6-1: Mitigations against quantified risk assessments

Threat	Risk	Recommended countermeasures
UP.UD.001, tapping of cable	Major	Data encryption and detection of the existence of tap devices.
UP.UD.002, data modification at source	Major	Integrity proof and verification of data content.
UP.NE.001, access to data on device	Major	Access control (including aspects of identity management) and intruder detection systems.
UP.NE.002, access to data on device	Critical	Access control (including aspects of identity management) and intruder detection systems. System integrity mechanisms to detect changes in software.
UP.NE.003, modification of system firm ware	Critical	System integrity mechanisms to detect changes in software. Secure boot (may include remote attestation of system images).
UP.NE.004, modification of system software with malicious code	Critical	System integrity mechanisms to detect changes in software. Secure boot (may include remote attestation of system images).
UP.NE.005, denial of service (physical attack)	Critical	Redundancy protection (e.g. measures in Recommendations ITU-T G.873 series [i.17], [i.18] and [i.19]). In addition the measures identified in clauses 5.3 and 6.5 apply.
UP.NE.006, denial of service (packet flooding)	Critical	Management plane and service plane coordinated traffic analysis and throttling or redirection measures.

7 Cost benefit analysis for mitigations application

7.1 Summary of method and calculation

NOTE: The Cost Benefit Analysis (CBA) provided in the present document is used to give an initial analysis of the recommendations of clause 6 and should be repeated in any follow up document.

The calculation method and the metrics for the cost benefit analysis of the application of countermeasures is defined in ETSI TS 102 165-1 [i.5]. The analysis has been applied to the core countermeasure strategies given in the present document.

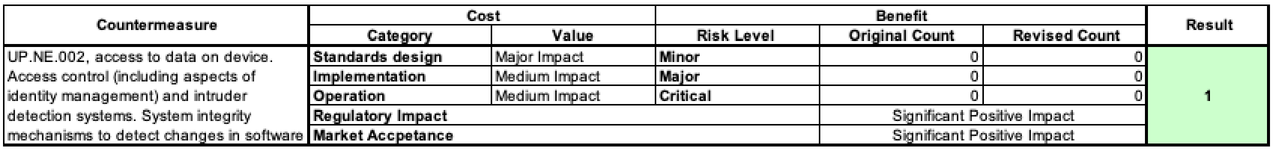
- Standards design:
    - Introducing countermeasures to a standard under development or an existing standard (published) may impose changes affecting the time schedule and resulting in additional effort and cost.

- Implementation:
    - Adding countermeasures to standards may affect its adoption and implementation in the targeted user community. This is an important aspect of standards adoption and crucial for countermeasure cost-benefit analysis.
- Operation:
    - Countermeasures may impact the ongoing operation of standardized products or systems once they have been deployed into an operational environment.
- Regulatory impact:
    - Regulatory impacts concern the influence that the countermeasure may have on ensuring regulatory compliance. The impact on regulation is assessed as very favourable as the supply chain is now bound together with a set of cryptographic proofs of delivery and assignment. Assuming the burden of Implementation and Operation are overcome this is the primary rationale for adoption of the methods given in the present document.
- Market acceptance:
    - Adoption of a standard into industrial products and its acceptance by the targeted user community determine the success of a standard. Therefore, countermeasures with negative predicted effect on market acceptance should be carefully analysed.

7.2 Sample calculation

The following calculation assesses the CBA for application of countermeasures against threat UP.NE.002, access to data on device (see also Annex A which refers to the core analysis tools/worksheets used in the derivation of the figures given in Table 7.2-1).

Table 7.2-1: CBA analysis for application of countermeasures to UP.NE.002



Countermeasure	Cost		Benefit			Result
	Category	Value	Risk Level	Original Count	Revised Count	
UP.NE.002, access to data on device. Access control (including aspects of identity management) and intruder detection systems. System integrity mechanisms to detect changes in software	**Standards design**	Major Impact	**Minor**	0	0	1
	Implementation	Medium Impact	**Major**	0	0	
	Operation	Medium Impact	**Critical**	0	0	
	Regulatory Impact			Significant Positive Impact		
	Market Accpetance			Significant Positive Impact		

The application of the countermeasures to UP.NE.002 will, when addressed across the F5G ecosystem, provide measures that also address many of the other threats identified in clause 5.8. The assessment of significant positive impact for each of regulatory impact and market acceptance is with regards to the CSA, the NIS Directive, and to GDPR, and the increased trust and reputation that often comes from the necessary attention to detail required to ensure conformance to such regulatory tools. The offset is that more technical precision is necessary in the standards domain and in each of implementation and operation. In very simple terms there is more complexity in the system and more specialized knowledge is required to implement and manage it. In addition, whilst the countermeasures are applied against threats in the underlay plane, the overall management of the threat requires coordination across all 3 planes of the F5G architecture. The data required to successfully detect intrusion (by software in this instance) is likely to be only visible at higher planes or layers than where the actual intrusion is happening hence the major impact on standards as this has to be coordinated across many different documents.

Annex A:
Risk assessment and CBA worksheets

The risk assessment worksheet used in calculating the risk in the main body of the present document, and the CBA worksheet, are contained in gr_f5g010v010101p0.zip which accompanies the present document.

Annex B: Bibliography

Security Policy

- ETSI TS 103 742: "Cybersecurity for a Communications Network".
- ETSI TR 103 838: "Guide to Coordinated Vulnerability Disclosure".
- ETSI TR 103 305-1: "Critical Security Controls".
- ETSI TS 103 523-5: "Enterprise Network Security".
- BBF TR101: "Migration to Ethernet-Based Broadband Aggregation".
- Recommendation ITU-T G.987.3: "10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification".
- Recommendation ITU-T G.871/Y.1301: "Digital networks - Optical transport networks: Framework for optical transport network Recommendations".

History

Document history		
V1.1.1	April 2022	Publication