ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 6, No. 4, 259-277 (2021)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Software Development Lifecycle for Survivable Mobile Telecommunication Systems

Mykoniati Maria*, Lambrinoudakis Costas

Department of Digital Systems, University of Piraeus, Piraeus, 18532, Greece

ARTICLE INFO

Article history:
Received: 21 March, 2021
Accepted: 19 July, 2021
Online: 03 August, 2021

Keywords:
Telecommunication Systems
Software Development Lifecycle
Survivability

ABSTRACT

Survivability of systems is a very important system property and consists major concern for organizations and companies. Survivable systems should maintain their critical services functional in a timely manner. There are several approaches, proposed in the literature, on how to develop survivable telecommunication systems, but the majority is based on node outages or path failures, missing the main scope of survivability which is service failure. The contribution of this paper is that it presents a SDLC (Software Development Life Cycle) for developing survivable mobile telecommunication systems. Additionally, the main characteristic of a mobile telecommunication system is that it consists of different types of nodes (ex. MME, SGSN, etc.) that are connected to systems (ex. 5G, 4G, 3G, 2G etc.) and thus form an intersystem that provides services to end users. This interconnection and interoperability of network nodes is of high complexity constituting a threat to system survivability. Thus, another contribution of the current research work is that it provides a systematic approach for handling this complexity.

1. Introduction

Availability and continuity of critical IT infrastructures is a matter of concern in many of scientific fields like security, robustness, fault tolerance etc. In fact, the unavailability and failure of such infrastructures causes severe financial losses to many organizations.

Survival of IT infrastructures, like information systems or network systems is a matter of concern for any company that develops and maintains network systems. That means that such systems should continue to support the critical services even during attacks, failures or accidents. A definition of survivability is: "survivability is the capability of a system to fulfil its mission, in a timely manner, in the presence of threats such as attacks or large-scale natural disasters" [1], with security, robustness, fault-tolerance and recovery of systems to be among survivability's main disciplines.

It is important to highlight that survivability focusses on the survival of the mission of the system and not of the system itself. This is the core principle of survivability.

There is much research on survivability measures and approaches that should be adopted by a system to be survivable. But how can we be sure that a system is survivable? What are those capabilities that should be tested in order for a system to be characterized as survivable and against which threats? Additionally, what are the interconnections and interoperability threats that should be considered when survivability of large complex system of systems, like mobile telecommunication systems, is examined and how could these be analysed at everyday work when building such systems?

Through literature review, a detailed research on survivability approaches is presented highlighting that most of them address survivability of telecommunication networks by handling node or path outages. However, survivability should be based on service failure and not on system failure. In fact, even if the entire network is performing as expected, there could be failures in services for many other reasons. For example, a software bug could result in a specific service failure, or delays caused by excessive load in specific network nodes could result in random service failures. Another reason could be that robustness requirements are not considered during system design. A very representative example is the handling of collision scenarios, where two messages requesting a service arrive at the same node simultaneously. Robust system design could resolve this conflict.

To conclude, the contributions of the current paper are:

- The solution proposed by the current paper is Survivability by Design, meaning that survivability should be part of the software development lifecycle (SDLC) of the telecommunication system. The idea comes [2] which is a

*Corresponding Author: Mykoniati Maria, mmykoniati@gmail.com

paper titled as "Life-Cycle Models for Survivable Systems", that proposes survivability to be part of the SDLC phases and describes how this could be achieved. This is the theory that the current research is based on to describe how survivable telecommunication systems shall be developed.

- Another contribution of the current paper is that it addresses the risk of service failures arising from the increased complexity of interconnection and interoperability of mobile telecommunication network nodes. This is a major concern since most of the times development teams tend to focus only on the node under development, when new features are to be developed, without taking into consideration requirements or threats coming from connectivity with the other nodes. More specifically, even if the entire system is tested end-to-end, when a mobile telecommunication network node is operating in the provider's environment, it may be connected to nodes developed by other companies. The behaviour of that node is unpredictable, and this should be considered during SDLC phases, by setting appropriate survivability requirements and design practices, and by testing without ignoring specific failure scenarios.

During the next chapter, survivability as a term is examined in order to present the main principles and requirements of survivability. Following this literature review, the general framework in the form of a software development lifecycle (SDLC) is presented. Finally, the paper closes with overall conclusions.

2. Literature Review

2.1. Survivability as a term

As described in [1], survivability is the ability of a system to maintain its critical services that serve system's mission in a timely manner in case of attacks, failures or disasters. As a result, survivability itself is a system property that the system should emerge and should be considered as a requirement during the design phase and not as an ad-on characteristic [2]. Additionally, since the focus is on critical services and system mission, survivability should be considered as a different set of characteristics for each system, based on system's scope. For example, for a telecommunication network, survivability as a requirement may include, define and implement mechanisms that would allow the system to feature robustness, fault-tolerance, interoperability, restorability, security, safety, resilience, dependability etc, for its critical services in order to provide uninterrupted communication to end users. For an e-shop, usability or secure transactions would also be key principles for the survival of the mission of the system. There is much research on gathering these characteristics to a general set for systems' design, with the most representative one being the research described in [2]. They argue that for any system survivability is succeeded if it has the ability to provide Resistance, Recognition and Recovery (3Rs) from attacks or failures. In extend the system should provide Adaptation and Evolution by improving system survivability and increasing its resistance by knowledge gained from previous attacks or failures.

Threat for the survivability of a system, according to [3], is anything that may prevent the system from providing its essential services under the "minimum acceptable level of service", or affecting the provision of its essential services for more time than the one predefined as acceptable. As a result, the threat against a system's survivability is unknown and not always predictable through a risk analysis. Therefore, it is critical for survivability to gather, analyse and deal with the impact threat incident may cause, rather than focussing on predicting all possible threats. For instance, from the "survivability point of view", it is more important to focus on how a network node would behave under a Denial of Service attack and how it could recover rather than identifying measures that would prevent this attack.

2.2. Survivable Systems

Having defined survivability, a brief description of different approaches that have been adopted for designing and implementing a system that satisfies the survivability requirements follows.

Starting with the Survivability Analysis Framework (SAF) [4], survivability is considered as a set of peoples' capabilities, a set of actions and of technology working together to achieve operational effectiveness. The focus is on interoperability of organizational components and how to cope with complexity arising from this interoperability in order to analyse potential failure conditions, likelihood of error conditions, impact of occurrences, or recovery strategies. This analysis yields requirements for the design and implementation of the system.

The second approach considers survivability as part of the system's development life cycle. It is described by research [2] and claims that "survivability goals and methods must be addressed for each action of the life-cycle", as survivability should be integrated into the primary development phase of system and not treated as an add-on property of an already implemented system. Starting with requirements specification, the system should be able to monitor itself in order to recognise attacks or failures, resist and recover from attacks and failures and reconfigure to adapt to attacks and failures. Additionally, after mission definition, essential services of system should be depicted, and the system should be designed in such a way so that to maintain these services when it is under attack or failure. Continuing with requirements, intrusion requirements should be defined, in order for the performance of the system under attack or failure to be defined, in order to ensure that acceptable levels of quality of service are always reached. What is important here is that intrusion scenarios are considered as usage scenarios to be handled. The testing of these requirements should include three attack phases, the penetration phase, where the intruder attempts to gain access to the system, the exploration phase, where the intruder has gained access and is exploring the integral system organization and capabilities to find possible exploitation targets, and the exploitation phase where the intruder performs attacks against system facilities. According to these phases, survivability strategies for resistance, recognition, recovery, adaptation and evolution must be enforced. By considering these requirements, the system may be designed and implemented as survivable.

The third approach is presented in [5], and it is based on analysing the different states of quality of service, that the system may fall into during a failure, and on estimating the probability of

the essential services being available during the failure. After changes to the environment or attacks to the system, the system may degrade to the next quality of service level. When failure is restored, the system may return to the higher QoS level. Acceptable QoS levels for the system and transitions between them, may be modelled with the use of a transition matrix.

Another approach for providing survivability is the one proposed by [6]. Contrary to the security approaches that try to prevent an attacker to gain access, the assumption here is that the attacker has gained access and the objective is to try to find ways to prevent him from interfering with systems' critical services. Methods of prevention are based on frustrating the attacker to believe that he or she has gained access to essential services.

A fifth approach is presented in [7] known as the WILLOW architecture. It is a proposal that focuses on proactive and reactive reconfiguration of a system in order to achieve survivability for its services. During proactive reconfiguration, it is possible to add, remove and replace components and interconnections of the system, as well as to adjust their mode of operation. This is called posturing and is used to minimize the system's vulnerabilities that can be exploited by various threats. For instance, such a reconfiguration may be to turn-off non-essential services and networking links as well as to strengthen the cryptographic keys if a virus has infected the system. The reactive configuration does the same actions, aiming to restore a system from damage or intrusions, in specific time intervals. In fact, as proposed, the most appropriate approach for reacting is fault tolerance. An example, of reactive reconfiguration against an attack or damage is the activation of applications' copies.

A similar approach of reconfiguring the system and switching to different level of quality of service is also provided in [8], where the authors claim that QoS and survivability are firmly connected. As a result, if QoS is to be measured, reconfiguration approaches may be triggered under certain measurements to provide survivability for the system. Firstly, as "survivable system", may be characterized, any system that may repair itself or degrade in such a way that will provide as much functionality as possible. This may be done if the system is able to switch between alternatives of acceptable predefined levels of functionality. Secondly, a survivable system is a system that may adapt threats in its environment and environmental changes and reallocate essential processing to most robust resources. All these may be achieved through dynamic reconfiguration. Such reconfiguration may be "process/host restart, migration of objects to alternate hosts, replication, transparent rebinding of clients and servers, use of service alternatives, and approximate services". [8] These reconfigurations may be based on several metrics like "available battery power, varying communication bandwidth, available memory or faults in software components" [8] and must be done in predetermined time and based on QoS service levels. Then a survivable system must provide a minimum level of QoS under changing environments. For that purpose, the best-suited elements are to be chosen at each time, based on these QoS factors.

2.3. Evaluation of System Survivability

According to related literature, evaluation of systems' survivability, is mainly based on defining different acceptance levels of system performance and on evaluating the impact by measuring the key properties like number of outages, time needed for system recovery etc. Though, these evaluation models are mostly based on node failures or link failures, but they are not giving the whole idea about the quality of service the system provides to end users. As a result, they seem to be based on system availability and continuity and not on critical services or system's mission availability. Of course, system's availability is of vital importance for supporting system's mission and providing end to end functionality. So, system availability should be part of any survivability analysis and evaluation plan. Thus, the purpose of this paper is to provide an entire evaluation framework of all survivability aspects and not only providing system - centric evaluation methods. As a result, many of these evaluation models could be very useful to pinpoint any possible network failures and include these in a test suite that would test if the system could recover from them or if it could function as expected while the system is suffering from these failures. But it is very important to provide guidance for testing or evaluating systems' survivability from the requirements specification step of a SDLC, up to the release of new product.

Starting with [9], the authors use a Markov model to map the possibility of a failure. They base survivability measurements on the frequency of failure events, on the duration of outages and on the impact of failure. Since the research is conducted through a case study with wireless networks, as a failure is considered node failure, power faults and link failures. A similar approach is proposed by [10], where the authors are using a semi-Markov survivability evaluation model for intrusion tolerant database systems. As key attributes for quantification of a database's survivability, integrity and availability are proposed. Much focus is paid on system's functionality under failure and how system performs against these attributes.

To continue with quantification of system's survivability, the author in [11], proposed network condition metrics which are density (based on topology and its changes), mobility (speed of node, predictability etc.), channel (bit error rate, capacity distribution etc.), node resources (memory, computing power etc.), network traffic (QoS, packet size, distribution etc.), derived properties (degree of connectivity, queueing delay, propagation delay etc.). In addition to those metrics, service requirements are also defined. Again, every adverse event, transits system's performance to another state which is quantified by these measurements (based on network and service performance) in order to be marked as acceptable or not. Another approach based again on a Markov model is being presented in [12]. It is focused on call losses of a telecommunication switching system because of various system failures like hardware/software faults, human errors, impairment damage from adverse environments etc. As key survivability metrics, system performance, availability and performability are used and the measurements proposed are measurements that can be used to describe system survivability such as the number of functional units, the number of connected nodes, the maximum traffic capacity, blocking probability, throughput/goodput, and the service restoration time.

To continue with evaluation methods, in [13], authors propose a testing survivability framework, focusing again on the recovery part of the survivability attributes. They firstly present the idea of 5-step phases of survivability of a system under failure, normal

phase, resistance phase, destroyed phase, recovery phase and adaptation phase. Then they propose a scheme for representing the different stages of system performance against time during these phases. For quantification of network performance, two factors are proposed to be used, the Node Connectivity Factor (NCF) and the Link Connectivity Factor (LCF). Practically though, they try to focus on the availability of an end-to-end activity for the end user which is what really matters. This is why their research focuses on source-destination pairs "SD-pairs", to describe connectivity and service quality "SD-quality" and test these factors by applying different failures in order to calculate SD Recovery time for each pair. Finally, NRD metric is calculated to give an overall idea about the entire system's survivability.

Another very important research on evaluation of survivability has been conducted by authors in [14]. The framework proposed, is based on developing a general measurement model, which may be specified based on specific domain requirements, a network survivability testing model, which is based on testing network performance against survivability metrics during different steps of system performance (resistance, destroy, recovery), and the network survivability evaluation, which includes measurement of the entire system's survivability based on different metrics, evaluation models or algorithms. The method concludes to a mechanism which if applied to the system under test, may provide all possible combinations of test schemes to test failures of a network and to measure them in order to extract conclusions on the overall system's survivability.

In [15] the authors propose measuring survivability through four attributes, Process-Weighted Average Availability (PWAA), Process-Weighted Average Controllability (PWAC), Process-Weighted Average Robustness (PWAR), Process -Weighted Average Adaptability (PWAD). These depict the state of the system through survivability life cycle, which is normal state, resistance state, destroy state, recovery state and adaptation phase.

Finally, another important approach for quantifying survivability is coming from authors in [16], who propose to base quantification, on system's reaction to specific attacks and vulnerabilities modelled by attack graph. The attack graph represents the nodes that the attacker may exploit, while the way chosen to transverse these nodes in order to cover all possible system functionality states is forward-search, breadth-first and depth-limited.

To conclude, what may be observed is that most approaches on quantifying survivability are based on measuring availability and robustness characteristics of the system. Though, survivability is a more complex attribute that the system as a whole should emerge and should be based on the ability of the system to continue serving critical services. As a result, the approach proposed in this paper for evaluating survivability, is a testing framework focussing on testing services available against systems failures, attacks or accidents.

2.4. Survivability and Telecommunication Systems

Before concentrating on the proposed SDLC for mobile telecommunication systems, we conclude the current literature review with a brief presentation of a few representative approaches for designing and implementing a survivable telecommunication system. It becomes clear that all these approaches are focussing on outages and path failures and not on service failures as survivability preserves.

In [17], the authors investigate the impact of possible failure scenarios and possible survivability strategies to contend with spatial and temporal network behaviour in mobile cellular networks. The failures for this paper are restricted to loss of BS, BSC-MSC or VLR. In [18], the authors analyse architectural principles for achieving minimization of services loss and service restoration through certain disaster recovery plans. The failure scenarios that are considered are central office switch fires, earthquakes, flooding, large-scale power outages, signalling network outages, fiber cuts, and terrorism. The result of these scenarios are outages to network devices for which the paper introduces a four-phase methodology to handle such cases. Another approach for providing survivability to Universal Mobile Telecommunication Systems (UMTS) networks is based on Markov chains, semi-Markov process, reliability block diagrams and Markov reward models [19].

What we may observe from these approaches is that the designs proposed are based on fault tolerance techniques and on how to mitigate the failure of network nodes. There are many other approaches in literature that indicate various techniques to handle the impact of the failure of a node or a link. Though, survivability is far more than that. Survivability should be part of every step of the SDLC. The current research focuses on providing survivability requirements for mobile telecommunication systems that should be taken into consideration during the requirements elicitation phase of the SDLC, and on how to validate the satisfaction of these requirements during the testing or development phases.

To sum up this literature review on survivability as a term and on approaches for providing survivability to a system the following requirements should be adopted:

- Survivability is a mission driven attribute which means that the mission of the system is what should survive at the end, and not the system itself. Additionally, the majority of approaches discriminate and mark system services at essential and non-essential services with the essential services being the ones that should survive, and perform at an acceptable level of QoS, when a system is under attack or failure.
- Threat against survivability is any failure that may affect its critical services. So, the system should be able to react to any failure even if the root cause is unknown.
- A system must be designed as survivable and for this to be succeeded, survivability requirements, based each time on system's nature, must be defined during requirements specification of every development life cycle. These requirements may be organized to 3Rs (recognition, resistance, recovery and adaptation methodology) Additionally, survivability requirements should be considered during all stages of system's development lifecycle and as part of the everyday work.
- For a system to be compliant with survivability requirements specification, a monitoring system that monitors and evaluates system's survivability is of vital importance. Additionally, if a monitoring system is available, the state of the system may be

known each time and preventive or corrective actions, like re-configuration or other system's self-healing processes, may be applied for providing survivability to the system, even when unplanned threats are realised.

- Finally, testing and evaluation of system's survivability should contain investigation of intrusion scenarios and failure incidents in order survivability requirements to be raised. This could be very useful if test driven development methodologies are used.

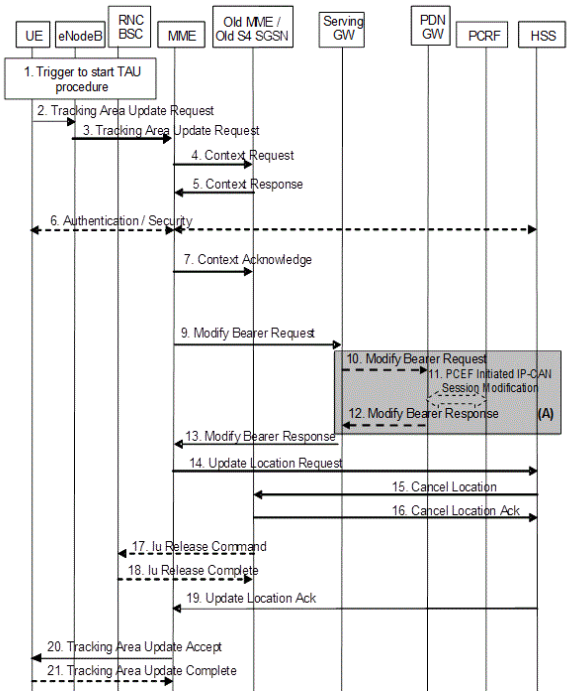
2.5. Mobile Telecommunication Systems

Before closing literature review, we will present some information on mobile telecommunication networks. Nowadays mobile telecommunication networks consist of a combination of 2G, 3G 4G and 5G mobile networks. Each network consists of the radio access network and the core network, which is finally connected to various networks like internet, IP Multimedia Subsystem (IMS) etc, to serve system's main mission which is to facilitate voice and data communications. Among network nodes, the communication in control-plane layer and user-plane layer is being established through specific interfaces.

Each of these systems has several nodes connected to each other. The particularity of mobile systems compared to other systems, like the internet, is that all services need an exchange of messages between a set of nodes to be established and performed. This significantly increases the risk of failure since problems may occur at any time during the exchange of the aforementioned messages. An example of such a message flow and possible failures that may occur, can be found in [20] or in the 3rd Generation Partnership Project (3GPP) standards. To continue with this logic, the network nodes that are connected to realize a service may be part of the same or a different network. For example, in 3G to 4G intersystem Tracking Area Update service, the nodes that may participate are from 4G, network nodes eNodeB, Mobility Management Entity (MME), Packet Gateway (P-GW), Serving Gateway (S-GW), Home Subscriber Server (HSS) and radio network controller (RNC), and Serving GPRS Support Node (SGSN) network nodes from the 3G network. This scenario is depicted in figure (1) bellow. Additionally, nodes may be manufactured from different organizations, a fact that increases the risk of interoperability failures. As a result, with various nodes interconnected, new networks are formed adding new system and survivability requirements that must be considered through the development of any new feature. The whole picture of a mobile network is shown in figure (2) bellow. This figure depicts the interconnection between 2G, 3G and 4G mobile networks through relevant interfaces. Though, the 5G network and the way it is connected with the rest of the mobile networks is missing. For this purpose, we utilize another picture from [21] that depicts the connection of the 5G network with the 4G network. This is figure 3 below.

The view of such interconnected systems adopted by the current work for all stages of the software development lifecycle is a multi-layered logic with the following levels:

- **Node level**: Any node of a mobile telecommunication network for which a new functionality or feature is to be developed. For example, MME should be considered to perform in node level.
- **System Level**: 2G, 3G, 4G and 5G, or any other that follow, are considered as systems. Nodes forming a system could be part of different PLMN operators. Any development task for a service that includes network nodes from the same system should be considered in system level.
- **Intersystem Level**: The entire telecommunication system may be considered as an intersystem. Nodes forming a network for serving an inter-system scenario may be considered as an intersystem. For example, in the scenario below, an Intersystem Tracking Area Update is depicted. The scenario includes nodes from 3G and 4G systems.



].

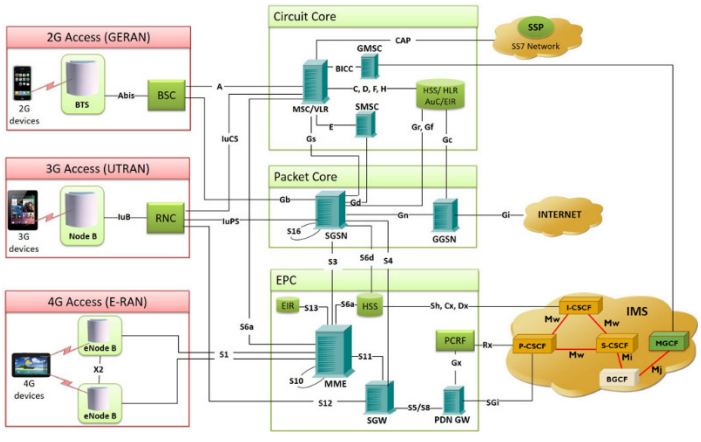


Figure 2: Common telecommunication network – The whole image (http://www.gl.com/telecom-test-solutions/communications-networking-2G-3G-4G-lab.html)

What is also important is that nodes supporting system or intersystem scenarios could even be part of different public switched telephone network (PLMN) operators. This means that when developing a new feature, the behaviour of nodes should not be considered as "known". Any possibility of receiving an unexpected message should be taken into consideration and the system should be able to resist to such a threat and recover from failure.

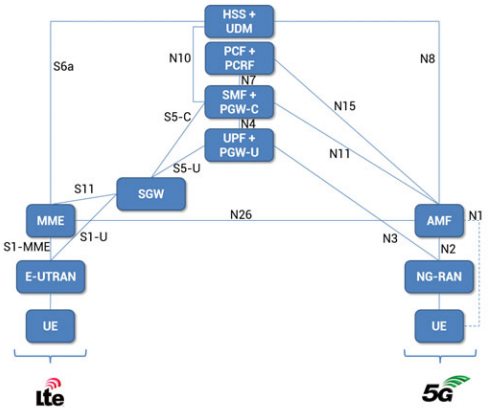


Figure 3: Common telecommunication network – 5G system added to the whole image (https://www.rfglobalnet.com/doc/g-core-network-architecture-network-functions-and-interworking-0001)

3. SDLC of Survivable Telecommunication Systems

Nowadays, systems development is mostly based on iterative models, or spiral models, in order to support continuous delivery of new functionality with certain predefined criteria. At the end of all iterations, an updated system, or a new release, is tested against its overall functionality in order to be delivered to the telecommunication operators.

Current research aims to improve this process by considering the survivability of critical services as the main requirement of the system under development. The main idea is to consider the whole (inter)system as a deliverable of any new release, instead of just focussing on a small part of the network. In this way, all survivability requirements at all system levels are considered and tested. The contribution of the current research is that it provides a complete proposal on how to handle survivability requirements and quality assurance of developed telecommunication system based on these requirements. The requirements are categorized to those related to service and those related to network since without it the system will not be available to perform any service. Additionally, the methodology proposed takes into consideration any arising requirement from the complicated interconnections of the telecommunication subsystems. All these requirements are gathered and grouped into 3Rs categories as described in literature; recognition, resistance, recovery and adaptation. In other words, requirements are enriched to include the whole network's survivability requirements. The result of not taking into consideration system and node inter-operability is a very important increase on the number of defects. Additionally, the testing methodology proposed by the current paper, considers all possible service failure scenarios and possible impact of any new functionality to the legacy code for critical services already developed.

The inputs to the aforementioned methodology are new features that will be developed or/and possible defects. When a new feature or a defect is planned to be developed, a new SDLC starts.

According to related literature, any methodology for designing survivable systems should start by defining the system's mission and the critical services that serve that mission. These should be documented and dealt with as requirements to any new functionality.

For mobile systems, critical are all services related to voice or data transmission from user perspective, and charging services from operator's perspective. This is also depicted in table (1) below, with service level requirements. So, for example, a voice bearer may be considered as critical service. A handover to such a bearer is critical also.

After definition of the mission and critical services that should survive, the general software development lifecycle (SDLC), is modified and used, with respect to special characteristics of the developed system, in such a way that at the end of the cycle the delivered (inter)system to emerge survivability. The SDLC that is proposed is depicted in figure (4).

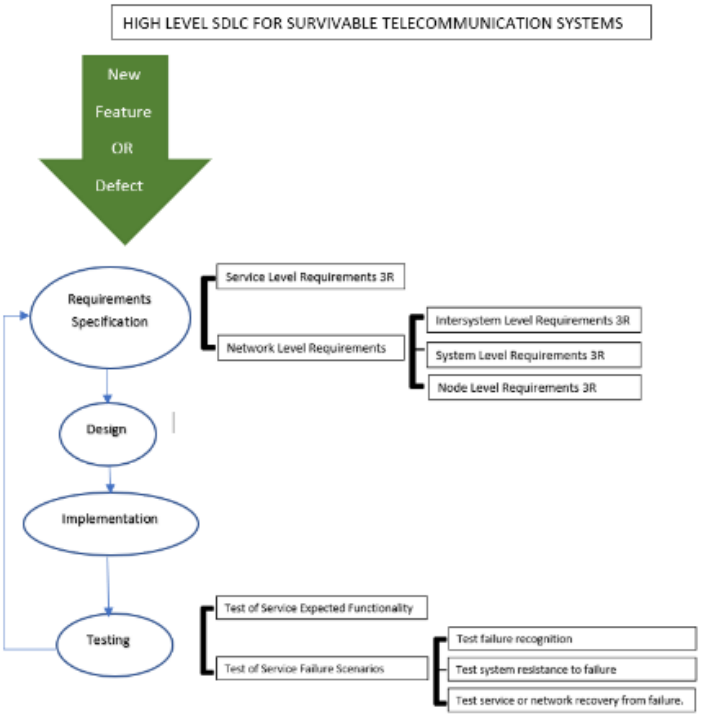


Figure 4: SDLC of Survivable Telecommunication Systems.

3.1. Requirement's specification

Requirements for extending the system's functionality are predefined and described in 3GPP documents. Survivability requirements should be based on a risk analysis study and detailed examination of the potential threats. As already explained, threats against survivability of the system are those that can directly affect the critical services of the system. This is the most effective way to protect critical services as such a service should survive even if the root cause of the failure is unknown. Thus, requirements are grouped to service level requirements that are related to services and network level requirements that are related to network

availability in order to support the operation of the services. For each group, requirements related to 3Rs (recognition, resistance, recovery, adaptation) methodology are presented.

In the tables below, high-level requirements related to survivability and defined by 3GPP are depicted. All these requirements are related to survivability and should be considered additionally to any requirement related to a new functionality or to any maintenance task. Additionally, any requirement that is an outcome of our research may also be depicted in service level survivability requirements table under columns titled "Our contribution". These requirements are related to **failure recognition** and **resistance** and are presented to previous papers [20], [22] related with survivability on telecommunication systems. Furthermore, the error handling requirements proposed from the current paper may be summarized to the following ones:

1. The system should be able to resist to failures related with **loss of messages**.

2. The system should be able to react to messages **arriving later or earlier** than expected. This should not have any impact to the service or to any other following services.

3. The system should be able to resist to failures related with **duplicate messages** sent to the nodes.

4. Any new functionality should be considered as a **threat to the critical services** already developed and any possible failure should be handled.

5. "**Hanging processes**" should also be considered as possible causes of failure.

Table 1: Service Level Requirements

3GPP Title	**3GPP Doc Num**	**3GPP Service Survivability Requirements related to failure Recognition**
UMTS Terrestrial Radio Access (UTRA) system	2101-301	*"*Set of attributes to describe UMTS bearer service (**delay variation tolerance, maximum transfer delay, maximum bit error rate**) information transfer rate attributes **(peak bit rate, mean bit rate, occupancy)**."* [23] *"*Performance: inherent transmission delay and level of traffic blocking"* [23]
Performance Management (PM)	32401	*"Data gathered through telecommunication management system are gathered to support performance evaluation on:* *- **Quality of Service** (e.g. delays during call set-up, packet throughput, etc) QoS can indicate the network performance expected to be experienced by the user."* [24]
Found across multiple 3GPP documents		
Error Causes **Please refer to certain interface 3GPP document for more details**		Specific error causes may be returned to the request message each time indicating a certain failure. For example, in GPRS Tunnelling Protocol (GTP) messages error cause "Mandatory IE incorrect" may be returned. From this the root cause of failure may be depicted and corrected by development team in case it can be corrected. Otherwise, there may be causes like "network failure" with root cause some failure to the network where all connections of the node with the node that returned this value, should be deleted.
Our contribution		
"Self-Diagnosis Framework for Mobile Network Services" [20]		Using the management reference mode of 32.101 we have proposed a self-diagnosis framework that may recognize and report different kinds of failure of service flow between nodes. Using this framework, the root cause of failure may also be depicted. Failures that have been analyzed are any possible failures that may occur when a message of a flow leaves a node to reach the neighboring node. The contribution of the paper is that focuses on diagnosis of service failure and not of system failure opposed to other proposals and to telecommunication management standard.
3GPP Title	**3GPP Doc Num**	**3GPP Service Survivability Requirements related to failure Resistance**
UMTS	2101-301	*"Handover should be transparent. In case of speech call loss of information may be tolerated but handover should be quick to **avoid connection break.** In case of data service temporary break is tolerable but not loss of information. Handover between terrestrial environments should be seamless within the same network"* [23]
		"Handovers should not increase the load on the fixed network significantly" [23]

		"The level of security should not be affected by handovers" [23]
		"Bearer services cannot be handed over between two environments if they are not supported in both. However, handover to an alternative bearer ***offering reduced capabilities*** *should be possible where this is supported by the service in use. The radio interface should have the capability to provide for handover and roaming between networks run by different operators"* [23]
Services and System Aspects;	22 101	*"Any handover required to maintain an active service while a user is mobile within the coverage area of a given network, shall be seamless from the user's perspective."* [25]
		"The 3GPP system shall be able to provide ***continuity between CS voice services*** *and the full duplex speech component of IMS multimedia telephony service with no negative impact upon the user's experience of the voice service. The same should be true for IMS Services."* [25]
		"The system shall support either *- transparent relay of the IP signaling and traffic;* *- service aware interconnection"* [25]
3G security; Security threats and requirements	21 133	*"Service Integrity: "It shall be possible to protect against unauthorized modification of user traffic"* *Service availability: It shall be possible to prevent intruders from restricting the availability of services by logical means"* [26]
Security Objectives and Principles	33 120	*"Security Objectives:* *1. to ensure that the security features standardized are compatible with world-wide availability* *2. to ensure that the security features are adequately standardized to ensure world-wide interoperability and* *roaming between different serving networks;"* [27]
Security architecture	33 401	The standard presents: *"- user identities confidentiality: MSIN, the IMEI, and the IMEISV should be confidentiality protected* *- user data signaling confidentiality: All S1 and X2 messages carried between RN and eNB shall be confidentiality-protected. Synchronization of the input parameters for integrity protection shall be ensured for the protocols involved in the integrity protection.* *- Integrity protection, and replay protection, shall be provided to NAS and RRC-signaling.* *- authentication and key agreement procedure between the mobile device and the core network,* *- security interworking of mobile networks (EUTRAN-UTRAN-GERAN)"* [28]
Technical Specification Group Services and System Aspects;	23 401	*"Authentication: NAS security mode control procedure is to take an EPS security context into use, and initialize and start NAS signaling security between the UE and the MME with the corresponding EPS NAS keys and EPS security algorithms"* [21]
5G; Security architecture and procedures for 5G System	33.501	The standard presents: *"- network access security: enable a UE to authenticate and access services via the network securely, including the 3GPP access and on-3GPP access, and in particularly, to protect against attacks on the (radio) interfaces* *-network domain security secure exchange of signaling and user plane data between networks.* *- User domain security: user access to mobile equipment.* *- Application domain security: enable applications in the user domain and in the provider domain to exchange messages securely"* [29]
		As it is presented to the current standard part of network life-cycle includes: *"the PLMN network is being adjusted to meet the long-term requirements of the network operator and the customer, e.g. with regard to performance, capacity and customer satisfaction through the enhancement of the network or equipment up-grade"* [29]
Found across multiple 3GPP documents		

Error Handiling		Some error causes indicate failures that can be handled in order to avoid dropping the service. Sometimes these handlings may be found across 3GPP documents or there may be implementation specific approaches that each organization implements during development of the device. To the example above "Mandatory IE incorrect" if we assume that the mandatory IE that is not correct is bearer ID. And the message causing this error is an answer to a previous message, then we may conclude which is the correct bearer id and ignore the error instead of dropping the service. The same may happen with network errors if we use relocation through selection functions to relocate the service that may be dropped in case it is critical (voice bearer for example)
Collision Handling		Collision is the case where two messages requesting a service arrive at a network and at the same time or one request arrives before the whole process of messages of the previous one has been completed. Then a handing of these requests should take place. This handling may be for example to serve both requests by a priority sequence, or to drop one of the two. For example, in case a request arrives for a UE that is already in process of a handover there is no meaning in processing it since the UE will leave from current Tracking area. Though there are cases that the service should continue to the Tracking area the UE will move to.
Our conrtibution		
"Fault Prediction Model for Node Selection Function of Mobile Networks" [22]		Our proposal regarding service resistance to failure is the fault prediction model proposed. This model takes into consideration DPMO (Defects per million opportunities) value which is a value that may be used to evaluate the operational performance of a node against 6sigma value. Then this value is used as a parameter in selection algorithm of mobile systems. This function is used to select a node which will be used to successfully complete a service flow.
Error Handiling		Apart from error causes defined by 3GPP documents and robust measurements that should be developed in order such cases to be handled, here we introduce some other error handline requirements: 1. The system should be able to resist to failures related to loss of messages. The failure should be ignored if this is possible. For example, if an acknowledgement message has not arrived, the service could be considered as established to avoid dropping it. If it could not be ignored, then the system should consider if there is a failure of neighboring node. In this case, the node should inform network management system and release any connection associated with this node. 2. The system should be able to react to messages arriving later or earlier than expected. This should not have any impact to the service or to any other following services. 3. The system should be able to resist to failures related with duplicate messages sent to the nodes. 4. Any new functionality should be considered as a threat to the **critical services** already developed and any possible failure should be handled.
Hanging Processes		As "hanging processes" we mean a service that fails, and leaves resources reserved causing failure to future services. For example, if a PDN Connection fails to be released and it is found as "already established" when a new PDN Connection is requested. This PDN Connection may be a critical service like voice bearer.
3GPP Title	**3GPP Doc Num**	**3GPP Service Survivability Requirements related to service Recovery from failure and adaptation.**
Restoration procedures	23 007	*"The data stored in location registers are automatically updated in normal operation; the main information stored in a location register defines the location of each mobile station and the subscriber data required to handle traffic for each mobile subscriber. The loss or corruption of these data will seriously degrade the service offered to mobile subscribers; it is therefore necessary to define procedures to limit the effects of failure of a location register, and to restore the location register data automatically"* [30]

Services and Systems Aspects;	22 101	*"The voice call continuity user's experience shall be such that, to the greatest degree possible, a consistency of service is provided regardless of the underlying communication infrastructure and technology"* [25]
UMTS	2101-301	*"Flexibility: Negotiation of bearer service attributes (bearer type, bit rate, delay, BER, up/down link symmetry, protection including none or unequal protection), parallel bearer services (service mix), real-time / non-real-time communication modes, adaptation of bearer service bit rate"* [23]
		"UTRA should adapt flexibly into changes and should have the capability to serve a variety of traffic densities (up to very high densities) and a variety of traffic mixes in an economical way." [23]
		"Flexibility and dynamic reconfiguration: minimum set of bearer capabilities, operating modes and features to ensure that inter-operability is always possible; continuity of operation during dynamic updating of terminal capabilities." [23]
Self-Organizing Networks (SON); Self-healing concepts and requirements	32541	*"In the case of software faults, the recovery actions may be :* *a) system initializations (at different levels),* *b) reload of a backup of software,* *c) activation of a fallback software load,* *d) download of a software unit,* *e) reconfiguration, etc.* *In the case of hardware faults, the recovery actions depend on the existence and type of redundant (i.e. back-up) resources."* [31] *'[If the faulty resource has no redundancy, the recovery actions may be:* *a) Isolate and remove the faulty resource from service so that it does not disturb other working resources;* *b) Remove the physical and functional resources (if any) from the service, which are dependent on the faulty one. This prevents the propagation of the fault effects to other fault-free resources;* *c) State management related activities for the faulty resource and other affected/dependent resources;* *d) Reset the faulty resource;"* [31] *e) Other reconfiguration actions, etc.* *"If the faulty resource has redundancy, the recovery action shall be changeover, which includes the action a), c) and d) above and a specific recovery sequence. The detail of the specific recovery sequence is out of the scope of the present document"* [31]

Table 2: Network Level Requirements

3GPP Title	**3GPP Doc Num**	**3GPP Network Survivability Requirements related to failure Recognition**		
		Node Level	**System Level**	**Intersystem Level**
Telecommunication management; Principles and high-level requirements	32.101	*"Telecommunication management system consists of an architectural framework or management reference model, that is used to collect measurements for management functions. Some of which are related to survivability like performance management, fraud management, fault management, security management, etc. With the use of performance measurements, configuration of system due to load needs may be executed. Additionally, for fault management, alarms or events may also imply a needed re-configuration for avoiding failures. Failure may be detected; isolated and root cause may be depicted."* [32]		

Performance Management (PM)	32401	*"Data sent at node level are gathered through telecommunication management system to support performance evaluation on:* *- traffic levels within the network, including the level of both the user traffic and the signaling traffic* *- verification of the network configuration: evaluation of effectiveness of changes of network plan related to traffic levels.* *- resource access measurements* *- resource availability (e.g. the recording of begin and end times of service unavailability)*" [24]	*"Network Operators are informed of PM - related events through alarms and may act accordingly."* [24]	
Fault Management;	32.111-1	"*If the faulty resource has no redundancy, the recovery actions shall be:* *- Generate and forward appropriate notifications to inform the **OS** about all the changes performed*." [33]		
3GPP Title	**3GPP Doc Num**	**3GPP Network Survivability Requirements related to system Recovery from failure and adaptation**		
		Node Level	**System Level**	**Intersystem Level**
Restoration procedures	23 007	*"The data stored in location registers are automatically updated in normal operation; the main information stored in a location register defines the location of each mobile station and the subscriber data required to handle traffic for each mobile subscriber. The loss or corruption of these data will seriously degrade the service offered to mobile subscribers; it is therefore necessary to define procedures to limit the effects of failure of a location register, and to restore the location register data automatically. The document describes data restoration procedures for VLR, HLR, HSS, GGSN, SGSN, MME. Triggering point is receiving a request for unknown IMSI in cases when the failing node has not detected the failure or receiving a message with restoration indicator set to not confirmed. These indicators show data corruption and procedure for restoring of these data through message exchange follows."* [30]		
		"Node restart. If a node restarts it sends a reset indicator to the neighboring nodes. Upon receiving such an indicator, the neighboring node shall inform its neighbors about the failure and release and re-initiate any PDN connection associated with failing node." [30]		

Fault Management	**32.111-1**	*"After a fault has been detected and the replaceable faulty units have been identified, some management functions are necessary in order to perform system recovery and/or restoration, either automatically by the NE and/or the EM, or manually by the operator. If the faulty resource has no redundancy, the recovery actions shall be:* *a) Isolate and remove from service the faulty resource so that it cannot disturb other working resources;* *b) Remove from service the physical and functional resources (if any) which are dependent on the faulty one. This prevents the propagation of the fault effects to other fault-free resources;* *c) State management related activities for the faulty resource and other affected/dependent resources."* [33]		
Self-Organizing Networks (SON); Self-healing concepts and requirements	32541	*"In the case of **software faults**, the recovery actions may be :* *a) system initializations (at different levels),* *b) reload of a backup of software,* *c) activation of a fallback software load,* *d) download of a software unit,* *e) reconfiguration, etc.* *In the case of **hardware faults**, the same as line of fault management above plus this:* *a) **Reset** the faulty resource;* *b) Other reconfiguration actions**, etc.* *If the faulty resource has redundancy, the recovery action shall be changeover.* ***Here we see that reconfiguration is something proposed by 3GPP but not a "must have" attribute."* [31]		

3GPP Title	**3GPP Doc Num**	**3GPP Network Survivability Requirements related to failure Resistance**		
		Node Level	**System Level**	**Intersystem Level**
(UMTS); protocol description and error handling	25.921	*"The error handling shall be specified in the protocol for the cases when the requirement for presence or absence of an IE indicated by the condition is not followed."* [34]		
Technical Specification Group Services and System Aspects;	23401	*"SGW-MME / SGW-PGW* ***GTP-C Load Control*** *feature is an optional feature which allows a GTP control plane node to send its Load Control Information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing GW selection procedure"* [21]	***"APN level load control*** *may be supported and activated in the network. If this feature is activated, the PDN GW may convey the Load Control Information at APN level (reflecting the operating status of the resources at the APN level), besides at node level."* [21]	
		"SGW-MME / SGW-PGW ***GTP-C Overload Contro****l feature is an optional feature. Nodes using GTP control plane signaling may support communication of Overload Control Information in order to mitigate overload situation for the overloaded node through actions taken by the peer node(s)"* [21]	***"NAS Level Congestion control****: The MME may detect the NAS signaling congestion associated with the APN and start and stop performing the APN based congestion control based on criteria: (max number of EPS bearers and EPS bearer activation per APN, one or multiple PDN GWs of an APN are not reachable or indicated congestion to the MME, Maximum rate of MM signaling requests associated with the devices with a particular subscribed APN, Setting in network management)"* [21]	
		"MME-Enb The ***MME Load Balancing*** *functionality permits UEs that are entering into an MME Pool Area to be directed to an appropriate MME in a manner that achieves load balancing between MMEs".* [21]	*"PDN* ***GW control of overload*** *by rejection of PDN connection requests from UE."* [21]	
		"*MME-Enb The* ***MME Load Re-balancing*** *functionality permits UEs that are registered on an MME (within an MME Pool Area) to be moved to another MME*" [21]		

		"MME *The MME shall contain mechanisms for avoiding and handling overload situations"* [21]		
		"SGW-MME ***Throttling of Downlink Data Notification*** *Requests. MME may restrict the signaling load that its SGWs are generating on it, if configured to do so."* [21]		
		"MME-UE *UE Level* ***NAS congestion****: The MME may detect the NAS signaling congestion associated with the UEs belonging to a particular group. The MME may start and stop performing the group specific NAS level congestion control based on criteria (maximum rate of MM and SM signaling requests associated with the devices of a particular group, Setting in network management)"* [21]		
Configuration Management (CM);	32.600	*"Configuration Management (CM), in general, provides the operator with the ability to assure correct and effective operation of the PLMN network as it evolves. CM actions have the objective to control and monitor the actual configuration on the Network Elements (NEs) and network resources, and they may be initiated by the operator or by functions in the Operations Systems (OSs) or NEs. CM actions may be requested as part of an implementation program (e.g. additions and deletions), as part of an optimization program (e.g. modifications), and to* ***maintain the overall Quality of Service (QoS)****. The CM actions are initiated either as single actions on single NEs of the PLMN network, or as part of a complex procedure involving actions on many resources/objects in one or several NEs."* [35]		

3.2. Design and Implementation

After requirements specification, design and implementation phases follow which are not worth analysing further since they are organization specific. **Robust and secure code design** techniques should be part of this phase. Additionally, **risks related to survivability** should be part of risk assessment which is usually conducted through the design phase.

3.3. Testing or Evaluation of System's Survivability

To continue, the testing phase of the proposed SDLC is presented. Testing is the way to evaluate a system's survivability. Testing phase should also follow the same model and test cases should be designed for node, system and intersystem level. In this way the whole system will be tested each time. Additionally, test cases should include tests against services' correct functionality, and they should be extended to also test any resistance, recognition or recovery survivability requirement to all testing levels (node, system, intersystem). For this to be achieved test-driven development is the most appropriate approach. Modern SDLC approaches are test-driven which is what is also proposed for the current SDLC.

Test-driven means that the tests are designed according to the requirements and are constructed even before the development of new features or maintenance tasks like bug fixing. Additionally, through this work we propose another approach that is related to test-driven development and has to do with failure impact evaluation. In other words, testing may be also used to evaluate the impact of any failure to critical services, and having this information available, new tasks may be extracted for the next iteration cycle regarding failure recognition, resistance or recovery. So, in this case tests are indeed driving the development and are a tool to discover many issues that may occur from any combination of services. So, any time a new service is to be

developed or updated, testing any possible combination of it with critical services will reveal any threats to critical services from the newly inserted code.

Impact analysis could be applied in any iteration of SDLC providing new requirements related to survivability requirements. Tests related to impact analysis may be:

1. Executing critical services before and after newly developed or modified service.

2. Executing critical services after failure of newly developed or modified service.

3. Executing critical services in collision with newly developed or modified service.

Additionally, another proposal is to test all survivability requirements for each new or modified functionality. So apart from just testing failure scenarios, recognition of failure and recovery from failure or resistance to failure should be also tested in order testing procedure to be considered complete.

All tests related to survivability evaluation and corresponding test approaches that could be used, are depicted in the following table (4) below. Test scenarios are also related to corresponding threat to survivability and impact of realization of this theat. Finally, any test case should be added to regression testing in order to ensure that future changes will not affect the existing functionality.

Table 3: Evaluation of Survivability Requirements through testing.

Survivability Threats		**Root Cause of Failure**	**Failure Impact in Node Level**	**Test Scenarios**	**Testing Methods**	**Examples from 4G network**
3GPP Fault Management; 32.111-1 Categories of faults for which an NE (network element) may	**Hardware failures**, i.e. the malfunction of some physical resource within a NE.	Device damage	Messages sent from one node to neighboring node may not be answered.	Testing of scenario where device is forced out - no information of the event to management system. The NE should be able to track the issue and report to management system. The impact from this failure to service under development and the restoration time should be defined.	Functional testing	Unplug of the device.
				Testing of scenario where device fails and sends alarm to management system. Service under development should be released or served by alternative resources after system re-configuration.	Functional testing	Enforcement of the NE to send a failure alarm to the management system
		CPU / Memory Overload		Testing of scenarios that		

raise alarms are:		System missconfiguration	Messages sent from one node to neighboring node may not be answered or answered with delay.	the message is not answered from neighboring NE in all phases of service establishment and test requirements related to handing of this situation.	Functional testing Unit or Module Testing Static Analysis,	Test scenarios where message is not answered.
			Faulty messages may arrive to NEs.	Testing of scenarios that the message arrives with wrong configuration information.	Functional testing Unit or Module testing Static Analysis Fuzzy-testing Fault-injection testing	Test message with wrong information about MMEs capability of supporting IOT devices.
	Software problems, e.g. software bugs, database inconsistencies	Any S/W bug that results in wrong functionality of service or non-compliance with standards	Service rejection or faulty service establishment.	Test-driven development with tests that are designed due to 3GPP standards requirements.	Functional testing Unit or Module Testing Static Analysis Fault-injection testing	Test all scenarios that reflect 3GPP requirements.
		S/W Bug lead to hanging processes	Future service requests may be rejected.	Enforce processes to be hanged and see if system reacts according to requirements. Test critical services impact if attempted.	Functional testing Unit or Module Testing Static Analysis,	Test if after deletion of a voice bearer it can re-established.
3GPP Fault Management; 32.111-1		Missing of robustness measurements like handling collision scenarios or handling of wrong Information Elements in messages	Service rejection or faulty service establishment.	Testing of all possible collision combination, especially with critical services, and test scenarios during which messages have wrong IEs that could be	Functional testing Unit or Module Testing Static Analysis,	PDN connection consists of a series of messages. A test case could include the modification of bearer id to a wrong one and see

				handled by robustness measurements.		if system is robust enough to handle this error.
		S/W bug that may lead to unanswered messages	Service rejection.	Testing of scenarios where messages of process under development are not answered.	Functional testing Unit or Module Testing Static Analysis,	A test case could be the PDN establishment and testing if service is properly rejected.
				Test the impact to critical services. Test cases with critical services already established and the above scenario following should be tested. The opposite is also valid scenario and should be tested. In this case failures from hanging processes will also be tested.	Functional testing Unit or Module Testing Static Analysis,	Testing of the above scenario after and before voice bearer handover.
		S/W bug that may lead to message sent twice	Service may be re-established if there is no mechanism for ignoring repeated messages	Testing of scenarios where messages of service under development are sent twice.	Functional testing Unit or Module Testing Static Analysis,	A test case could be sending PDN request twice for the same bearer.
	Functional faults, i.e. a failure of some functional resource in a NE and no hardware component can be found responsible for the problem.	Any other failure that may lead to service unavailability	Service Failure	Any related test	Functional testing Unit or Module Testing Static Analysis,	Any related test

	Loss of some or all of the NE's specified capability due to overload situations.	System Overload of requests	Messages sent from one node to neighboring node may not be answered or answered with delay.	Testing of service impact after increasing system load. Testing service impact after increasing load of service.	Stress testing Load testing Stability testing	Try to establish a voice bearer in a loaded system and an overloaded system. And try to see the impact to the system and voice bearer when system is loaded by voice bearer requests.
	Communication failures between two NEs, or between NE and OS, or between two OSs.	S/W failures, H/W failure, Overload situations, Path / Link failures, Network timing issues.	Messages sent from one node to neighboring node may not be answered or answered with delay.	Testing of scenarios of scenarios that the message is not answered from neighboring NE in all phases of service establishment and test requirements related to handing of this situation.	Functional testing Unit or Module Testing Static Analysis,	Testing of scenarios of scenarios that the message is not answered from neighboring NE.
Security Testing	Any security threat should be considered and tested. Details on security testing will not be provided to current document.					
Failure Recognition	In all possible errors, network management system should be tested. Network management system should be informed about any kind failure and should be able to trigger system resistance or recovery mechanisms. So, any NE that is under development should be tested against this functionality also.					
System Recovery	In all possible failure scenarios, recovery mechanisms following should also be tested.					

4. Conclusions and Future Work

To sum up, during the current paper, a development framework of a survivable mobile telecommunication system, based on system's mission and critical services, has been presented and proposed. This framework was based on the available survivability approaches through literature review with its main contribution to be that it provides a solution that is more focussed on interconnection and interoperation of systems forming larger intersystem. By this any survivability requirement from any level of service is considered through everyday development work and the focus is not only based on correct system functionality. Additionally, by this any interoperability and interconnection requirements and threats related to survivability may be examined through development life cycle.

Contrary to other approaches for evaluation of survivability, the one proposed is a more practical guide for testing the critical services of systems and evaluating measurements correlated to survivability of (inter)system, end to end from the requirements specification phase of the system and it does not only focus on node or link failure as most of proposals of literature review. This approach has been adopted because survivability is a built-on and not an add-on characteristic.

To sum up, the major outcomes of the current research are:

- The current research improves the traditional SDLC process, by enriching requirements analysis and testing phases with approaches related to survivability. The resulting proposed methodology is the Survivability Software Development Lifecycle presented in Chapter 3 that may be applied to telecommunication systems.
- The current research provides a systematic approach for handling the complexity arising from the interconnection of different network nodes of a telecommunication system.

Finally, as future work, we are planning to apply the proposed methodology in order gather and analyse metrics related to overall system survivability.

Conflict of Interest

The authors declare no conflict of interest

Acknowledgment

This work has been partly supported by the University of Piraeus Research Center.

References

[1] R.J. Ellison, D.A. Fisher, R.C. Linger, H.F. Lipson, T.A. Longstaff, N.R. Mead, "Survivable network systems: An emerging discipline", Carnegie Mellon University Digital Library, 1997, doi:10.21236/ada341963

[2] R.C. Linger, et al., "Life-Cycle models for survivable systems", Carnegie Mellon University Digital Library, 2002, doi: 10.1184/R1/6575138.v1

[3] V. R. Westmark, "A definition for information system survivability", in 37th Annual Hawaii International Conference on System Sciences, 10-19, 2004 doi: 10.1109/HICSS.2004.1265710.

[4] R.J. Ellison, "Survivability analysis framework", Carnegie Mellon University Digital Library. 2010, doi: 10.1184/R1/6584474.v1

[5] J. C. Knight, E. A. Strunk and K. J. Sullivan, "Towards a rigorous definition of information system survivability" in DARPA Information Survivability Conference and Exposition, 78-89, 2003, doi: 10.1109/DISCEX.2003.1194874.

[6] P. Pal, "Survival by defense – enabling" , in 2001 workshop on New security paradigms, 71–78, 2001, doi: 10.1145/508171.508183

[7] J. Knight, Dennis Heimbigner , Alexander Wolf, Antoinio Carzaniga, Jonathan Hill, Premkumar Devanbu, Michael Gertz, "The WILLOW survivability architecture", in Fourth Information Survivability Workshop, 2001, doi: 10.1.1.96.5316

[8] W. Li, L. Shu and Y. Feng, "A Dynamic Survivability reconfiguration framework based on QoS", in 2009 International Conference on Advanced Computer Control, 103-106, 2009, doi: 10.1109/ICACC.2009.107.

[9] D. Chen et al., "Network survivability performance evaluation: a quantitative approach with applications in wireless ad-hoc networks", in 5th International Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems, 61-68, 2002, doi: 10.1145/570758.570769.

[10] A. H. Wang, S. Yan and P. Liu, "A semi-Markov survivability evaluation model for intrusion tolerant database systems," in 2010 International Conference on Availability, Reliability and Security, 104-111, 2010, doi: 10.1109/ARES.2010.90..

[11] A.J. Mohammad, "Towards quantifying metrics for resilient and survivable networks", in 14th IEEE International Conference on Network Protocols (ICNP 2006), 2006, doi: 10.1.1.1.6900

[12] L.Y. Trivedi, "A general framework for network survivability quantification.", in 12th GI/ITG Conference on Measuring, Modeling, and Evaluation of Computer and Communication Systems, 369-378, 2004, doi: 10.1.1.94.3404

[13] M. Liang et al., "A novel method for survivability test based on end nodes in large scale network", KSII Transactions On Internet Ans Information Systems 9(2), 620-636, 2015, doi:10.3837/tiis.2015.02.008.

[14] C. Wang et al., "A general framework for network survivability testing and evaluation", Journal of Networks **6**(6), 831-841, 2004, doi: 10.4304/jnw.6.6.831-841

[15] M. Liang et al., "Research on survivability metrics based on survivable process of network system", in 4th international conference on security of information and networks, 247-250, 2011, doi: 10.1145/2070425.2070470 .

[16] L. Zhang, W. Wang, L. Guo, W. Yang and Y. Yang, "A survivability quantitative analysis model for network system based on attack graph", in 2007 International Conference on Machine Learning and Cybernetics, 3211-3216, 2007, doi: 10.1109/ICMLC.2007.4370701.

[17] D.W. Tipper et al., "Survivability analysis for mobile cellular networks", in Communication Networks and Distributed Systems Modeling and Simulation Conference, 2731-2738, 2002, doi: 10.1.1.361.411

[18] M. C. Baker, C. A. Witschorik, J. C. Tuch, W. Hagey-Espie and V. B. Mendiratta, "Architectures and disaster recovery strategies for survivable telecommunications services", Bell Labs Technical Journal, **9**(2), 125-145, 2004, doi: 10.1002/bltj.20030.

[19] S. Dharmaraja, V. Jindal and U. Varshney, "Reliability and survivability analysis for UMTS networks: an analytical approach", IEEE Transactions on Network and Service Management, **5**(3), 132-142, 2008, doi: 10.1109/TNSM.2009.031101. 8

[20] M. Mykoniati et al., "Self-Diagnosis framework for mobile network services", JACN, **7**(2), 2019, doi: 10.18178/JACN.2019.7.2.268

[21] "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", Version 16, Technical specification 3GPP org The Mobile Broadband Standard 23401, 2021.

[22] M. Mykoniati et al., Lambrinoudakis, "Fault prediction model for node selection function of mobile networks", in 9th International Conference on Information Communication and Management ICICM 2019, 153-159, 2019, doi: doi.org/10.1145/3357419.3357452.

[23] "Requirements for the UMTS Terrestrial Radio Access (UTRA) system", Version 3.0.1, Technical specification 3GPP org The Mobile Broadband Standard, 21.01U, 1997

[24] "Telecommunication management;Performance Management (PM);Concept and requirements", Version 16.0.0., Technical specification 3GPP org The Mobile Broadband Standard 32401, 2020

[25] "Service aspects; Service principle", Version 18.1.1, Technical specification 3GPP org The Mobile Broadband Standard 22101, 2021

[26] "3G security; Security threats and requirements", Version 4.1.0, Technical specification 3GPP org The Mobile Broadband Standard 21133, 2002

[27] "Security objectives and principles", Version 4.0.0, Technical specification 3GPP org The Mobile Broadband Standard 33120, 2001

[28] "System Architecture Evolution (SAE); Security architecture", Version 16.3.0, Technical specification 3GPP org The Mobile Broadband Standard 33.401, 2020

[29] "Security architecture and procedures for 5G System", Version 17.2.0, Technical specification 3GPP org The Mobile Broadband Standard 33.501, 2021

[30] "Restoration procedures", Version 17.1.0, Technical specification 3GPP org The Mobile Broadband Standard 23.007, 2021

[31] "Telecommunication management; Self-Organizing Networks (SON); Self-healing concepts and requirements", Version 16.0.0, Technical specification 3GPP org The Mobile Broadband Standard 23.541, 2020

[32] "Telecommunication management; Principles and high level requirements", Version 16.0.0, Technical specification 3GPP org The Mobile Broadband Standard 32101, 2020

[33] "Telecommunication management; Fault Management; Part 1: 3G fault management requirements", Version 16.0.0, Technical specification 3GPP org The Mobile Broadband Standard 32111-1, 2020

[34] "Guidelines and principles for protocol description and error handling", Version 7.0.0, Technical specification 3GPP org The Mobile Broadband Standard 25.921, 2007

[35] "Telecommunication management; Configuration Management (CM); Concept and high-level requirements", Version 16.0.0, Technical specification 3GPP org The Mobile Broadband Standard 32600, 2020