enisa

European Network
and Information
Security Agency

Enabling and managing end-to-end resilience

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created as a response to security issues of the European Union. The Agency's mission is essential to achieving a high and effective level of network and information security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of network and information security for the benefit of citizens, consumers, business and public sector organisations in the European Union. ENISA is a centre of expertise for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between European institutions, the Member States and industry players.

Contact details

For enquiries about this study, please use the following contact details:
European Network and Information Security Agency
Technical Competence Department
Email: sta@enisa.europa.eu
Internet: http://www.enisa.europa.eu/act/it/eid

Acknowledgements

This study was carried out in close collaboration with a group of experts in the field.

Supervision:

- Sławomir Górniak

Other ENISA staff involved:

- Demosthenes Ikonomou
- Rodica Tirtea

The contributions of the experts below are gratefully acknowledged:

- Scott Cadzow – Cadzow Communications
- Henryk Gierszal – ITTI
- David Sutton – Telefónica O2 UK
- Paul Theron – Thales Information Systems Security
- Claire Vishik – Intel

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies, unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Table of Contents

Executive Summary

This document is structured in a manner that allows the reader to understand the definition of resilience and end-to-end resilience. The report identifies the contributors to end-to-end resilience and gives guidance on how to enable and manage end-to-end resilience.

The primary scope of this report is public networks and services.

End-to-end resilience is achieved from the planned combination of prevention, protection, response and recovery arrangements, whether technical, organisational or social. It is required:

- To cope with incidents from very minor up to extreme impacts
- To cope with situations that can be handled through everyday incident response procedures up to crises too complex to be handled in a day-to-day procedural manner

A number of statements can be made that characterise a resilient system:

- A resilient system is reliable

  - **corollary:** a reliable system may be used as the foundation of a resilient system but a reliable system will not always be resilient

- A resilient infrastructure features high availability that is an effect of all components
- A resilient system should provide for business continuity and management of unforeseen or unexpected risks
- A resilient system should offer a security level adequate to the information being transmitted
- End-to-end resilience requires resilience in all components of the infrastructure

The good practices identified in this document should be enforced as a first measure to achieve resilience.

1 – Case studies – resilience requirements in action

This section describes some of the challenges facing network and service providers, illustrating the need for resilience and including a selection of past events and failures that have resulted in serious consequences for the affected networks and their customers.

Abnormal but legitimate traffic load

On 7th July 2005, four improvised explosive devices (IEDs) were detonated by terrorist suicide bombers during the morning rush hour in central London. Three of these were on underground trains, the fourth on a double-decker bus – 52 people were killed and hundreds were injured. The public thirst for information regarding friends and family was enormous and immediate, and within minutes the load observed on GSM mobile networks was much greater than the norm for the time of day. This soon caused congestion in the radio layer that eventually began to filter back into the interconnected fixed-line networks.

Remedial action was quickly taken, but it took some time to establish the optimal way of solving the problem and both voice and data services were severely disrupted for three hours. After the event, one network operator reported that voice calls in the greater London area had been 60% greater than normal, and that text messaging had been 20% greater than normal across the whole of the UK.

One of the mobile operators in Poland introduced a new service allowing individual customers to make calls within the network free of charge every Friday between 16:00 and 20:00. After one month, the offer was withdrawn because it caused the congestion of the network in all big cities, leading to dropped calls that affected individual as well as business customers.

Accidents and human mistakes

Some failures occur as a result of deliberate actions and may be referred to as acts of terrorism or vandalism, if from an external source, or as sabotage, if from an internal source. However, many failures occur as a result of non-malicious interactions by people and nature.

> In the north-eastern United States in the summer of 2003, a combination of technical failures and human error resulted in more than 50 million people being without power
>
> In September 2003, the failure of a power link between Switzerland and Italy caused a power outage affecting 56 million people
>
> In March 2010, contractors working on a 150 mm water main in west London failed to secure the pipe properly and several millions of litres flooded the basement of a nearby telephone exchange that contained the power systems supplying the whole building. Tens of thousands of customers were deprived of all service until power could be restored, initially from external standby generators
>
> In 2000, a power disruption at Chicago Board of Trade caused a delay in processing of transactions that were worth $20 billion

Large-scale disasters

Large-scale disasters such as tsunamis, floods, ice storms and hurricanes invariably affect the power and electronic communications infrastructures when they strike.

> The tsunami that struck south east Asia in December 2004, resulting in the deaths of more than 200,000 people, destroyed the communications infrastructure across a wide region, impeding the rescue and recovery
>
> In August 2005, Hurricane Katrina caused massive destruction in the south-eastern United States and disrupted communications on many networks over an extended period. This demonstrated that even the more developed societies are not immune to the effects of nature
>
> In November 2006, a power line across the River Ems (Germany and The Netherlands) was disconnected to allow a large vessel to pass according to a pre-arranged plan. However, the disconnection took place earlier than expected, with the result that a cascade failure occurred and overall some 10 million households across Belgium, Germany, Italy, Portugal, Spain, and eastern Europe may have been affected.
>
> A four-day failure of the power network in the USA and Canada in 2003 led to losses of $10 billion.

For the telecommunication sector, an average loss due to outage of the power grid amounts $1 to $10 per kW, while the average loss of outage for a mobile operator is equal to $41,000/hour.

Malicious attacks

While many malicious attacks originate with criminal organisations, some are believed to be the direct result of information warfare between nation states, as well as from the more general hacking community.

Many malicious attacks could have far-reaching consequences that, apart from causing damage to critical network infrastructure, could damage or destroy end-point systems and services.

Typical of the exploits undertaken are ‘Distributed Denial-of-Service’ (DDoS) attacks that may be targeted at individual organisations or even nation states.

> In April 2007, following the Estonian government’s stated intention to relocate a former Soviet war memorial, a DDoS attack was launched against both public and private web sites within Estonia, allegedly from within Russia. This resulted in Estonia completely disconnecting its external Internet connection in order to stop the effects of the attacks
>
> During the 2009 Iranian election protests, foreign activists seeking to help the opposition engaged in DDoS attacks against Iran's government. The official website of the Iranian government (ahmedinejad.ir) was rendered inaccessible on several occasions.
>
> In the weeks leading up to the five-day 2008 South Ossetia war, a DDoS attack directed at Georgian government sites containing the message: "win+love+in+Rusia" effectively overloaded and shut down multiple Georgian servers. Websites targeted included that of of the Georgian president, Mikhail Saakashvili, which was rendered inoperable for 24 hours, and the National Bank of Georgia.

Failures at lower layers

In March 2004, a fire broke out in a tunnel beneath Manchester in the United Kingdom, causing serious damage to hundreds of copper and optical fibre cables providing both telecommunications and Internet connectivity. Customers of several service providers lost connectivity for several days until all the cables could be re-jointed.

In January 2008, cable breaks in the eastern Mediterranean caused major disruption in Internet connectivity to Egypt and India, with lesser disruptions to another nine middle-eastern countries and affecting more than 20 million Internet users. The cause of the breaks has never been positively identified, but has been assumed to be as the result of damage to the cable on the sea floor, caused either by a ship's anchor, or by abrasion resulting from tidal movements of the sea bed.

2 – e2e resilience concept

2.1 Introduction

End-to-end resilience involves aspects beyond, and in addition to, technology. This point of view is founded upon the premise that resilience is needed when operators lose control of the course of things, i.e. when incidents render incident response procedures ineffective and destabilise the management. Thus resilience management and design has to consider the end-users, the context in which they use the system, the technology of the system, the structure of the organisation and the organisation's ability to be resilient, and ultimately the ability of the society in which the system operates to be in a position to be ready for and to manage the conditions that require resilience.

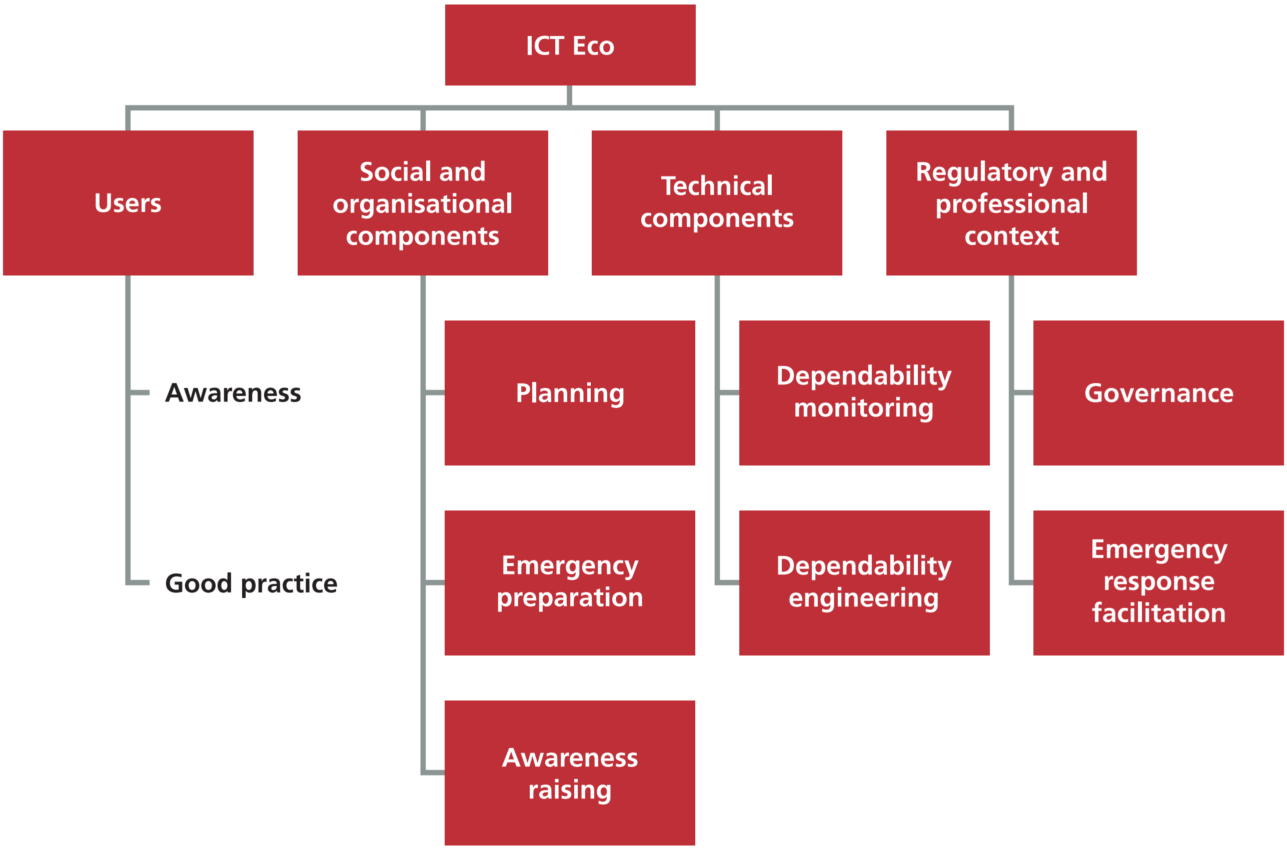


Figure 1: Factors in the resilience of an ICT system

When considering end-to-end resilience, a number of key points have to be borne in mind. These include some commonly understood aspects and a few that are rather less well considered:

End-to-end service implies:

- mouth to ear for voice services;

- user to on-line service or user to user for data services;

- broadcaster to subscriber for broadcast services.

End-to-end design should also imply and take into consideration:

- Interfaces from one technology to another (e.g. PSTN to PLMN);

- Interfaces or borders from one country to another;

NOTE: There is a need to acknowledge that both users and operators are geographically spread, thus introducing the need to take into account different legislative and regulatory frameworks and also different social and cultural frameworks to manage the response to events where resilience comes into play.

- from one kind of critical infrastructure to another;

- from private network to private network through public networks.

- In a combined environment containing highly secure and general components

NOTE: Organisations, both privately and publicly owned, may need to work together to manage resilience in both planning and in response.

2.2 Definition

2.2.1 From a technical to a more encompassing definition

The concentration of many services on to a shared infrastructure places a considerable strain on any system that has originally been designed with a more limited set of services in mind, but later adopted to run multiple services that were not originally envisioned. This has been the case for some telephone networks, which have evolved to become the backbone of the networks that are now required to deliver voice, video and data from person to person and from machine to machine in any combination. Where reliability and resilience could once have been managed on the basis of a given number of 3 minute voice calls per subscriber per day, with predictable busy hours and hot spots, the need for modern telecommunications networks to offer reliable and resilient service to all of the ICT services demanded by consumers, business, and, increasingly, the machines and sensors that need to communicate to support the societies of the 21st century, requires a re-examination of the means to achieve resilience.

In addition to resilience of communication, many of today's transactions that society relies upon are of a client-server nature, with the service being as important as the communication network that provides access to it. From a resilience perspective, this makes design, engineering, and preparedness more difficult, since the back-end service is often run by a different operator from the network provider(s), or the parties responsible for maintaining the customer premises equipment. Examples of these types of services include conferencing and collaboration services, on-line trading and settlement services, medical data repositories, and the emerging cloud computing services.

ENISA has defined resilience as "*The ability of a system to provide & maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation.*" This can be contrasted with a definition of resilience where stress is applied to the system "*The ability of an entity, system, network or service to resist the effects of a disruptive event, or to recover from the effects of a disruptive event to a normal or near-normal state*". The former does not address stress and recovery and may be considered as closer to reliability and thus using this as the definition for this report could lead to a focus on an inappropriate set of measures to give assurance of resilience. Reliability is addressed in the security domain by the Availability parts of the CIA paradigm and by existing Quality of Service (QoS) and Grade of Service (GoS) metrics. Therefore it is important to distinguish resilience, and the means to design for resilience, from the techniques and technologies to achieve reliability.

A more organisational definition from [PTH], established for the purpose of the study contract JLS/2008/D1/018 ANAC No 30-CE-0263198/00-49, the purpose of which was to conduct a study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and the Internet, is that ***Resilience*** is the aptitude of an organisation to keep its systems and services running under an emergency situation, to maintain the highest possible level of performance, to resume a nominal mode of functioning as quickly and easily as possible should performance have decreased, and to draw the lessons from the experience once the crisis is over. It stems from four ***resilience processes***, organised within response plans and implemented in times of crisis:

getting-by = the set of actions taken to maintain activity at the highest possible level of performance despite an emergency

resisting = the set of actions taken to withstand the destructive pressure of circumstances in order to maintain an ability to perform

recovering = the set of actions taken to resume a nominal course of activity and development once adverse circumstances are behind

rebounding = the set of actions taken once the crisis is over

- to learn from experience new capabilities, technologies and processes that will help to better prevent and protect against, respond to and recover from extreme adversity

- to help partner organisations caught in emergency situations to handle them

- possibly to adapt the organisation to new or expected patterns of its environment.

Resilience management is a learnt and prepared aptitude. It cannot be improvised at incident response time. Preparation yields the capabilities a telecommunication organisation and its systems need in order to be resilient. Preparation falls into two distinct phases, both of which have to be given equal weight:

Planning and preparation, for which preparation activities create

- The set of capabilities, tools, procedures and processes to prepare a network and other infrastructure components to withstand stress (this should encompass all the design techniques for reliability).

Response and recovery, for which preparation activities create

- The set of capabilities, tools, procedures and processes that act to recognise a stress event and to recover the network and other infrastructure and organisational components to their previous state.

2.2.2 From resilience to end-to-end resilience

The study of end-to-end resilience requires examination of all the aspects of delivering a service across the entire set of functional assets in the path, from source to sink.

Heterogeneous networks are the norm in modern networks, e.g. a single end-to-end connection may be made from the source device through an Ethernet LAN, to a star connected digital subscriber line, a cloud or grid managed network, to an SDH ISDN network and thence to a 3G PLMN and UMTS connection or WiMAX subscriber loop to the sink device. Each element (network or technology) may offer a different level of security and reliability. The aim of studying and defining end-to-end resilience is to be able to ensure that stresses (in the form of failure, for example) at any single point in the combination required to deliver end-to-end service are recoverable, without damage to the provision of the end-to-end service.

The components and characteristics of any end-to-end service comprise at least the following four distinct areas:
The source device or Customer Premises Equipment (CPE)

- Comprises a continuum of capability from a (dumb) standard telephone handset, through smartphone and tablet computer to a fully featured processor-based device such as a desktop or laptop computer. As the CPE evolves away from a standard telephone handset, it will contain four essential components – an Operating System (OS), a User Interface (UI), an Input/Output mechanism (IO) and an Application (App).

- Such devices tend not to be resilient by design, although some may be ruggedised (making the distinction between the adjectives 'resilient' and 'robust' to describe an item — i.e., resilient to physical stress), and the user will generally accept the occasional failure of such a device and not expect a fully resilient service from it. With COTS products responsible for more and more elements of critical infrastructure, and with low power devices entering common processes, end-to-end resilience becomes more complex, and it continues to be necessary to define and improve resilient architectures at all levels.

The network

- The network will contain many elements – switches, routers and the like, and due to the way in which network protocols operate, the physical network which provides service to the user at the beginning of a session may be at least in part made up of different individual components from that present at the end of the user's session.

- The implication of this is that the whole of the network must be designed to be resilient, regardless of which (or whose) elements service passes through during the session. Each part of the network must contain no single points of failure.

- However, it is commonly accepted that levels of resilience decrease as one moves further from the core of the network, which is invariably highly resilient, to the extremities of the network (such as home ADSL routers for example), which are generally much less or not at all resilient. Even a base station in a mobile network is seen as a very low resilience component, whose influence on the overall resilience of mobile operator's infrastructure is negligible.

The sink or endpoint

- This could be a fully featured processor-based device such as a server, or more likely a number of servers such as load-balancers, web servers, database servers and authentication servers, which work together to provide the service.

- It could also comprise another Customer Premises Equipment (CPE) device in the case of point-to-point services, or be a combination of server and CPE equipment for hybrid services.

- Each of these contains several essential components, such as an Operating System (OS), a User Interface (UI), an Input/Output mechanism (IO) and Applications (Apps), and while the individual components may not be resilient, service resilience is achieved by ensuring that there is an adequate combination of server types to allow for service to continue in the event of individual server failure and to ensure that there is adequate capacity in the service platform to permit efficient operation at times of peak usage. The service platform should contain no single points of failure. Today, more complex architectures including virtualisation and distributed data sources are common.

The supporting services which enable the service to operate

- These will be present across the network and the sink (and some cases the source), and will comprise the physical accommodation of the network equipment or servers, power, cooling, security, management, human resources and so on.

As the network and the sinks (endpoints) will often be providing many services to many users, it follows that these must also be highly resilient and contain no single points of failure.

2.2.3 Complexity of modern ICT ecosystems

Resilience and reliability continue to be measured separately for single components of the ICT ecosystem, while modern computing infrastructures have evolved into complex combinations of heterogeneous systems and devices that are cooperating to complete everyday processes. If one element in this complex computing environment lacks resilience and fails, or doesn't perform adequately, the integrity of the whole process is negatively affected. Figure 2 below illustrates a typical complexity for a process and the varying levels of resilience in today's ICT ecosystems. In order to ensure end-to-end resilience as defined in this paper, we need to study the complexity of the networking, communication and computing environment and understand the approaches that will increase end-to-end resilience, as opposed to resilience of the elements of the ICT ecosystem.

We also need to address the issue of composition: while the resilience of each element of the ecosystem is necessary, a better understanding of the effects of interoperation of diverse components on the resilience of the ecosystem is also important. The effect of the interoperation of the components is not well understood and needs additional investment in new research methodologies.

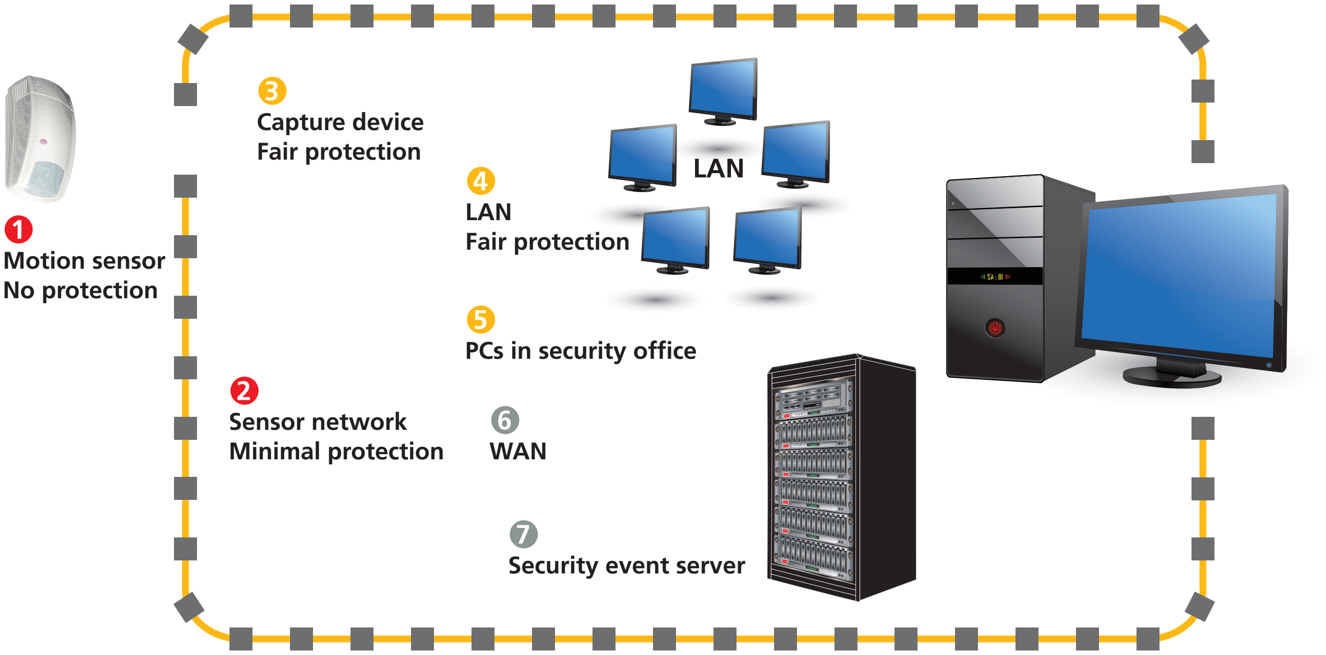


Figure 2: Example of a complex ICT ecosystem

2.2.4 Evolution of end-to-end resilience concepts

In the recent past, end-to-end resilience referred to the state of communications networks and was aimed at ensuring that the networks connecting endpoints were resilient in accordance with pre-defined metrics. The growing interdependences between components of ICT ecosystems gradually changed the approach by including other elements of the computing environment into the picture of resilience, as was noted above.

2.2.5 Software Reliability

Software reliability engineering has developed engineering techniques for measuring software reliability and developing reliable software systems. Software reliability has been an active discipline for 35 years and is now undergoing assessments to improve future approaches. Fault prevention, fault removal, fault tolerance, and future fault forecasting are some of the important areas in this discipline. Software reliability modelling has been especially active in the last several years, and may point us to useful techniques to develop metrics to address the issue of composite reliability.

Software engineering promotes reliable, available, safe and secure software produced on the basis of complete and coherent requirements using different models for software development. Therefore software engineering is supported by requirement engineering and influences system engineering that takes software and hardware as well as overall ICT ecosystem issues into account. Software development processes deployed by system engineering aims at producing dependable software with minimum number of iterations in debugging, integration or implementation.

Software quality and software development lifecycle management process maturity have been areas for on-going investment in the industry. The scope of activities includes focus on better software development tools that prevent common faults from being introduced, formal software development process, environment, and professional sign-off, testing and verification tools, technics, and methods, and software update and patch management and planning.

Another approach adjacent to software reliability has become popular in response to the complexity and quick evolution of today's computing environments. It is focusing on equipping software with self-management and self-adaptation mechanisms capable of ensuring continued operations in changing conditions. It is done by such ideas as plug-and-play, on-the-fly, overall manageability as well as not blocking OS kernel.

Hardware has developed multiple capabilities to support resilience that are not always supported in software. Greater integration of the capabilities of all the elements of the computing environment are necessary to increase end-to-end resilience.

2.2.6 Hardware and Device Reliability

Reliability and performance have been the core engineering principles for hardware components of various levels of hardware devices, but continued efforts are needed to implement greater resilience at the device level and ensure mutual use of reliability and fault tolerance features available in hardware and software. In recent years, interesting proposals have been articulated by researchers like energy efficiency and fault tolerance using algorithmic resilience to translate into highly efficient hardware implementations. Cross-layer resilient system architectures are being studied, to ensure consistent levels of resilience in high performance low power systems.

NOTE: There is a close relation between improvements in device reliability with energy efficiency and eco-solutions within the ICT sector.

2.2.7 Data Dependability

Data resilience remains a serious problem that needs to be addressed to register progress in end-to-end resilience studies. Many different devices and networks participate in capturing, transmitting, and sharing data, and this contributes to the complexity of the issue. Much of the critical data is collected via sensor networks that are notoriously error prone and unreliable. Consequently, a lot of research is in place to define viable algorithms to improve data resilience in sensor networks; some work is also under way to improve sensor resilience and resilience of sensor and ad-hoc networks. At the same time, data resilience is an important subject of studies focusing on critical infrastructures, such as smart grids, and related data. Topics connected with the growth of distributed data storage environments are very important and may have a defining role in end-to-end resilience.

2.2.8 Organisational Resilience

The organisational resilience is an additional dimension of holistic strategic approach used by operators and service providers as well as their customers to achieve the resilience of infrastructure by dedicated management of unforeseen or unexpected hazards. The resiliency at the enterprise layer concerns different aspect of the organisation as well as its business background including process workflow, technologies or facilities (Figure 3). As a result the organisation gains a new capacity to deal with different, even sudden and extreme shocks. This level of resilience requires a change of mind in an organisation's culture and behaviour (Figure 5).

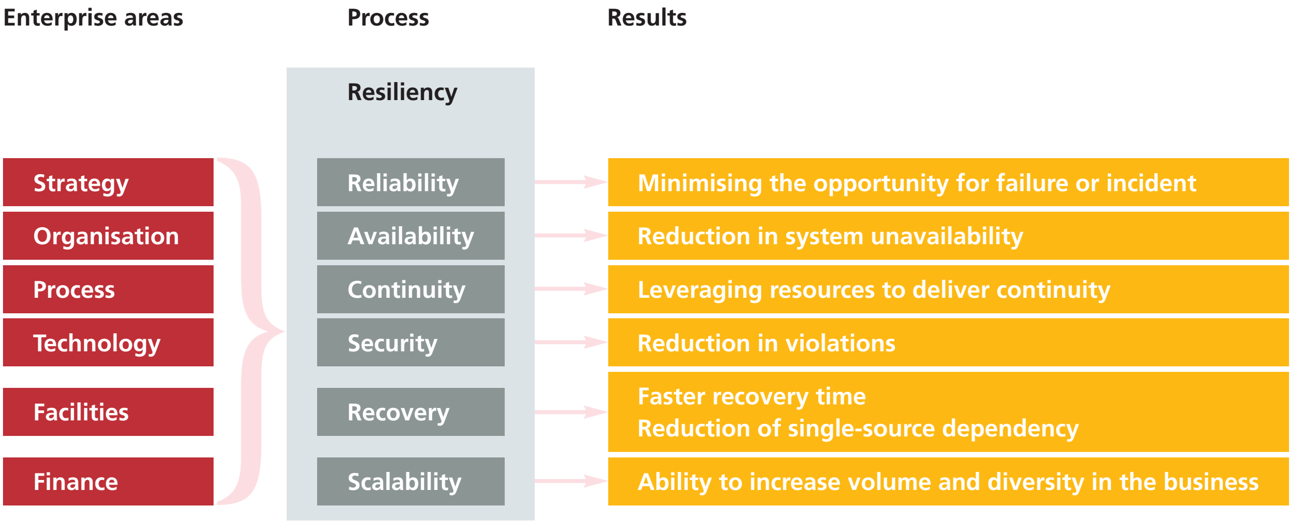

Enterprise areas
Process
Results
Resiliency
Strategy
Organisation
Process
Technology
Facilities
Finance
Reliability
Availability
Continuity
Security
Recovery
Scalability
Minimising the opportunity for failure or incident
Reduction in system unavailability
Leveraging resources to deliver continuity
Reduction in violations
Faster recovery time
Reduction of single-source dependency
Ability to increase volume and diversity in the business

Figure 3: Organisation overall resiliency and business outcomes

2.3 Statements about Resilient Systems

A number of statements can be made that characterise a resilient system:

A resilient system is reliable (**corollary**: a reliable system may be used as the foundation of a resilient system but a reliable system will not always be resilient).

A resilient infrastructure features high availability that is an effect of all components.

A resilient system guarantees business continuity and management of unforeseen or unexpected risks.

A resilient system should offer a security level adequate to information being transmitted.

Such a comprehensive approach should comprise co-ordinated activities to direct and control an organisation with regard to its major risks and to build a common understanding of resiliency. The complete process should:

create value for the organisation

be an integral part of its processes, including decision-making

explicitly address uncertainty and major emergencies / crises across the organisation

be systematic and structured

be based on the best available information (e.g. ISO 31000, BS25999, …)

be tailored to the organisation's needs and possibilities

take into account human factors

be transparent and inclusive

be dynamic, iterative and responsive to change in a managed way to deliver continuous improvement.

3 – Resilience in Telecommunications Networks

3.1 A Dynamic Model of Resilience Engineering

A telecommunications system is under stress from a number of factors and each of these factors have to be identified and their impact on system stress assessed in order to select appropriate technologies to provide a resilient network.

ANALOGY: In the selection of materials for a product the ability of the material to withstand attack by heat, light, impact, tension and compression is taken into account and materials are chosen to best withstand the combination of forces placed on the product. End-to-end resilience has to similarly take into account the set of forces acting on the system and to build a system using components, architectures and connections that are able to best resist the set of forces without changing the primary function of the system.

A model for resilience engineering is proposed below in Figure 4 that shows the interaction between four main disciplines of risk management and the respective topics / objects they aim at handling in a loop of continuous improvement, lessons being learned from one discipline feeding progress in the others.

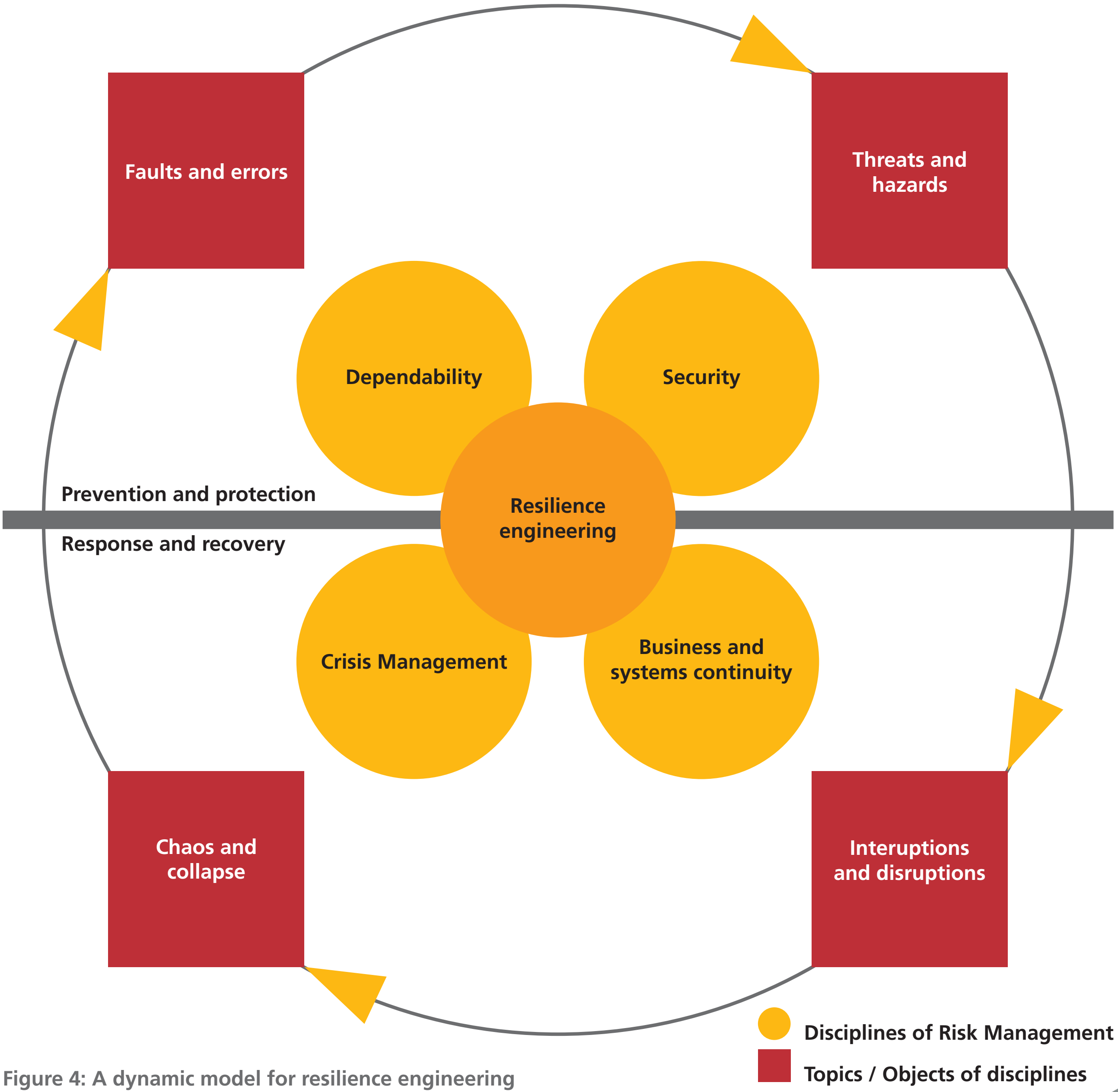

Faults and errors
Threats and hazards
Dependability
Security
Prevention and protection
Resilience engineering
Response and recovery
Crisis Management
Business and systems continuity
Chaos and collapse
Interuptions and disruptions
● Disciplines of Risk Management
■ Topics / Objects of disciplines

Figure 4: A dynamic model for resilience engineering

3.2 Basic Features of Resilient Telecom Infrastructures

The biggest source of stress on a telecommunications network is the offered load by end-, and interconnection-, points. Load can be roughly split into signalling and media with the path through the network being different for each as are other characteristics such as bandwidth, response time and hold time.
The capacity of the network to meet the load is the source of some stresses as insufficient capacity may exist in areas where maximum capacity is required, leaving "hotspots" in the system that are highly stressed whilst others are under no stress at all.

NOTE: Hotspots may exist geographically and temporally, for example many sports fans use their phones during the half time interval thus creating "exceptional" loads at (say) 3:45 on a Saturday afternoon in the area of Old Trafford (Manchester).

The resilience of telecommunications networks then is based around both connectivity and capacity, and is inscribed within an organisational and social context.

A resilient telecommunications network therefore should have:

No single point of failure

- It must address all areas of network equipment such as switches, routers, etc. and transmission interconnections between these elements, both on a local area and wide area basis.

In-built failover

- The failure of an element brings about a changeover to a standby working element; or load sharing, such that the failure of a single element within a group of similar elements does not cause degradation of service. As with network elements, the transmission interconnections between them must also operate on a failover or load-sharing basis.

Sufficient capacity

- In both network elements and transmission interconnections (both signalling and media) so as to allow for known peak demand plus a degree of 'headroom' which will allow for unexpected peaks in traffic beyond the norm.

Resilient ancillary services

- Such as DNS servers and other ancillary network elements that enable the transmission of network traffic as opposed to those network elements that actually carry network traffic.

Resilient network monitoring and management systems,

- that allow network engineers to identify and rectify problems in an efficient manner. This also implies a degree of resilience of the network monitoring and management centres that house these systems.

Resilience from the support infrastructure

- in terms of network engineering staff who plan and implement changes and who identify and correct problems, and of call centre staff who handle fault calls from users or customers and pass these onto the network engineering staff for fault diagnosis and repair.

- including the physical locations in which network equipment is housed, the power supplies which keep the equipment in operation, the cooling systems which maintain suitable environmental levels, and the physical and electronic security systems which ensure that network equipment is safe from physical or electronic attack either from within or outside the organisation.

- When the event vanishes or may be overcome with a counteraction measure the system should be restored to normal operation as soon as possible. The manual or automatic self-healing actions result in reducing interruption of services provided to consumers and in helping service providers more effectively manage the delivery infrastructure.

Resiliency from an operational culture in which policies, procedures and vigilance (Figure 5) usually encompass:

- Compliance — the ability to meet regulatory requirements, including those for transparency and data availability

- Continuity and recovery — the ability to keep the business processes up and running and to support customers and business partners while managing unexpected events

- Security and privacy — the ability to protect the business, information and customer data from external attack or internal breaches

- Scalability — the ability to adjust systems as business changes and grows.

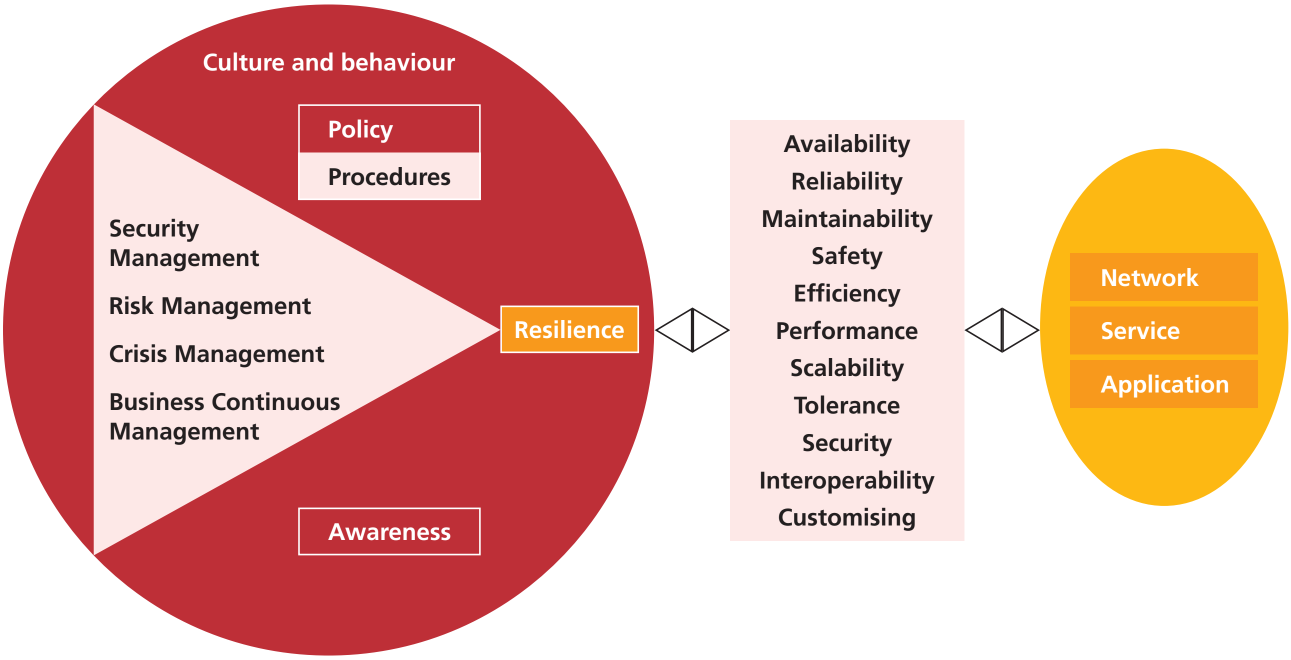


Figure 5: Elements of resilience engineering

4 – Network Resilience from a Technical Standpoint

Network resilience is strictly related to the network autonomy, dependability and connectivity. In addition a resilient network infrastructure has to provide security, availability, maintenance of performance, and business continuity.

The replication of hardware and software components may enhance reliability to ensure continuation of service in the event of a failure. A number of architectures, technologies, procedures and processes already exist to address this:

Resilient and scalable platforms can serve special connectivity requirements including:

- highly scalable and service-rich server farm switching;
- high bandwidth, ultra low latency server fabric switching;
- highly scalable, multiprotocol intelligent storage switching; and,
- high bandwidth, long distance data centre interconnect.

Storage Area Networks (SAN) — resilient architecture ensures efficient storage and consistent data replication and mirroring.

A resilient, integrated business continuance network infrastructure is to protect data, rapidly recover applications, and ensure continuous user access in the event of a disruption. Different techniques can ensure data resilience, application resilience and user access resilience. Data resilience can be obtained due to high-capacity, low-latency nodes, networks and interconnections. Application resilience can be enhanced by removing single point of server failure or distributing application environments among several remote locations. User access resilience is obtained by the use of Virtual Private Networks (VPN) or proxy solutions that allow network and site selection.

High availability networks must be considered as one of the ICT elements for building multiservice networks that ensure well internetworking, granular levels of Quality of Service (QoS), policy-based management as well as directory enabled networking. This is accelerated with the emergence of multiservice or converged networks supporting data, voice and video applications over a common IP-based packet infrastructure. The concept of all IP networking simplifies developing such networks but on the other hand it imposes a series of designing constraints that have to be met in order to make them resilient. In the multiservice model data networks will evolve to become a single network infrastructure based primarily on the IP protocol and capable of supporting traditional data applications plus a wide range of real-time and on-demand, multimedia communications services and applications. As more and more services are consolidated on a single infrastructure, the availability of the network becomes critical for operators.

The process of network design is very challenging for telecom operators, especially for those that operate in the "green field." The obvious constraints that have to be taken into account include availability of financial resources and time to launch of services. Moreover, operators have to consider the geographical coverage of the network, population density and demand, as well as the transmission capacity of the whole network. To achieve a trade-off between these, often contradictory, objectives they have to carefully plan the overall length of the transmission network and the number of households that will become consumers of different services like POTS, access to Internet, Web TV, Voice over IP, etc.

The starting point for selection of a technical model for planning e2e resilient network is to determine the architecture of the logical network. In this regard, it is recommended to use a hierarchical network composed of three layers:

backbone network,
distribution network,
access network.

This allows for functional division of the layers depending on the tasks they perform throughout the network. Each layer is composed of:

passive components — premises for backbone nodes, together with the necessary infrastructure to ensure secure and reliable functioning of active components; cable pipes and cable ducting system; optical fibre cables; passive accessories for fibre optics radio links; and,

active components — active devices that aggregate and transmit traffic from lower layers.

A hierarchical approach is crucial for a future operator of the network infrastructure, because it significantly simplifies traffic management in the network, reduces the time needed to determine failures and the range of an outage (thus decreasing costs of supervision, monitoring and maintenance of the whole transmission system).

In IP networks the network resiliency features should span Layer 2 and Layer 3 boundaries and should be deployed throughout the three-tiered Backbone/Distribution/Access design model. Very high network availability can be achieved by controlling the overall network failure rate that can be minimized by configuring an appropriate degree of device-level redundancy to increase hardware Mean Time Between Failures (MTBF). The degree of load sharing that can be achieved in high availability network design significantly reduces the cost burden of provisioning network redundancy and makes fault tolerance a more attractive design alternative. With a performance distributed across primary and secondary devices, a level of the redundancy may be improved.

Resilient networks should be designed bearing in mind at least the following issues: availability, fault tolerance at the node level and redundancy at the topology level.

One approach to building highly available networks is to use extremely fault tolerant network devices throughout the network. To achieve high availability end-to-end, the fault tolerance of each device is optimized. This is achieved by providing redundant backup within the device for each of its key components. However if a network is designed with highly fault tolerant devices, but with multiple single points of failure, the additional economic burden of highly fault tolerant devices may produce little measurable benefit in terms of the overall network system availability. Another way to build highly available networks is to provide most of the reliability through redundancy in the network topology rather than within the network devices. The advantages are:

The network elements providing redundancy need not be co-located with the primary network elements. This reduces the probability that problems with the physical environment will interrupt service.

Problems with software bugs/upgrades or configuration errors/changes can often be dealt with separately in the primary and secondary forwarding paths without completely interrupting service. Therefore, network-level redundancy can also reduce the impact of non-hardware failure mechanisms.

With the redundancy provided by the network, each network device no longer needs to be configured in standalone fault tolerance. Device-level fault tolerance can be concentrated in the backbone and distribution layers of the network where a hardware failure would be expected to affect a larger number of users. By partially relaxing the requirements for device-level fault tolerance, the cost per network device is reduced, to some degree offsetting the requirement for more devices.

With appropriate resiliency features, plus careful design and configuration, the traffic load between the respective layers of the network topology (e.g., access layer to distribution layer) can be shared between the primary and secondary forwarding paths. Therefore, network-level redundancy can also provide increased aggregate performance and capacity, which in turn helps to reduce the incremental cost of a redundant network.

Redundant networks can be configured to automatically fail-over from primary to secondary facilities without operator intervention. The duration of service interruption is equal to the time it takes for fail-over to occur. Fail-over times as low as a few seconds are possible.

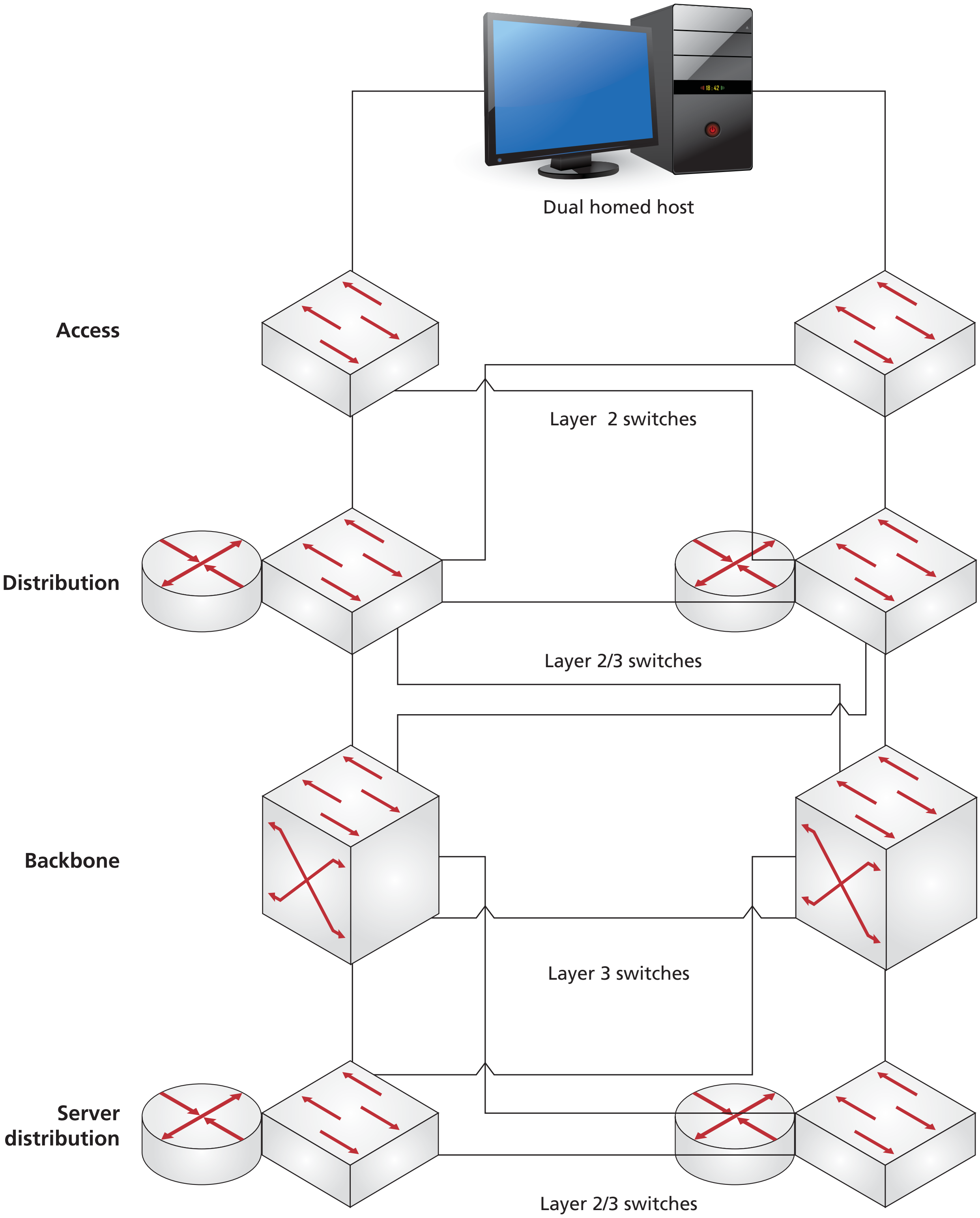


Figure 6: Redundant network with no single points of failure

Building a resilient infrastructure includes recovery, hardening, redundancy, accessibility, diversification and autonomy. Three first issues are mainly defensive. Resiliency is not a simply protection measure but a comprehensive and robust strategy to gain overall advantages for the network and its customers. That is why three other issues offer proactive operation. While fault-tolerance in the network means that the system or application must keep itself running in spite of component failures, the resilience is a comprehensive issue ensuring that the system with applications works to keep them running in spite of failures.

4.1 Effects of Network Convergence on Resilience

As already mentioned a resilient system should take overall ICT ecosystem into account. Using cross-layer solutions it is possible to improve the resulting resiliency and in fact to offer a variety of services in converged networks. It is especially important when modern heterogeneous CS/PS and wire-line/-less networks are deployed. For example in resilient networks high-available switching nodes should be installed that allow the protection of CS and PS switching. The convergent networks involve a large scope of network components that can be managed and controlled with different applications. The overlapping management systems having many plug-ins can support overall resiliency controlling all mechanisms used in components to ensure dependability. Such approach may need to implement a middleware to translate controlling signals exchanged among hardware elements.

4.2 System Architecture

4.2.1 Intrinsically Resilient Architectures

Resilient, highly reliable architecture eliminates single points of failure by automatically rerouting traffic to find new routes and, finally, to prevent downtime. The ring topologies, tree, star or mesh are the dominant approaches that have a different level of resiliency, reliability and availability. An advantage of the ring topology is its superior resiliency. Even the protected tree topology is protected against failures of equipment, but provides no path redundancy. In the star topology its resilience is mainly a function of the central node and links between central node and end nodes. Thus there is none inherent protection. The mesh topology demonstrates good resilience. However, it is practically excluded due to cost burden, although it is widely use in radio networks. The ring provides superior availability, due to inherent diversity of pathways. Service failures occur only when both paths fail. Thus, to achieve the same e2e availability in a tree and a ring, the ring links can be designed for a lower availability than the tree links.

In the backbone typically ring or mesh topology is applied (Figure 7).

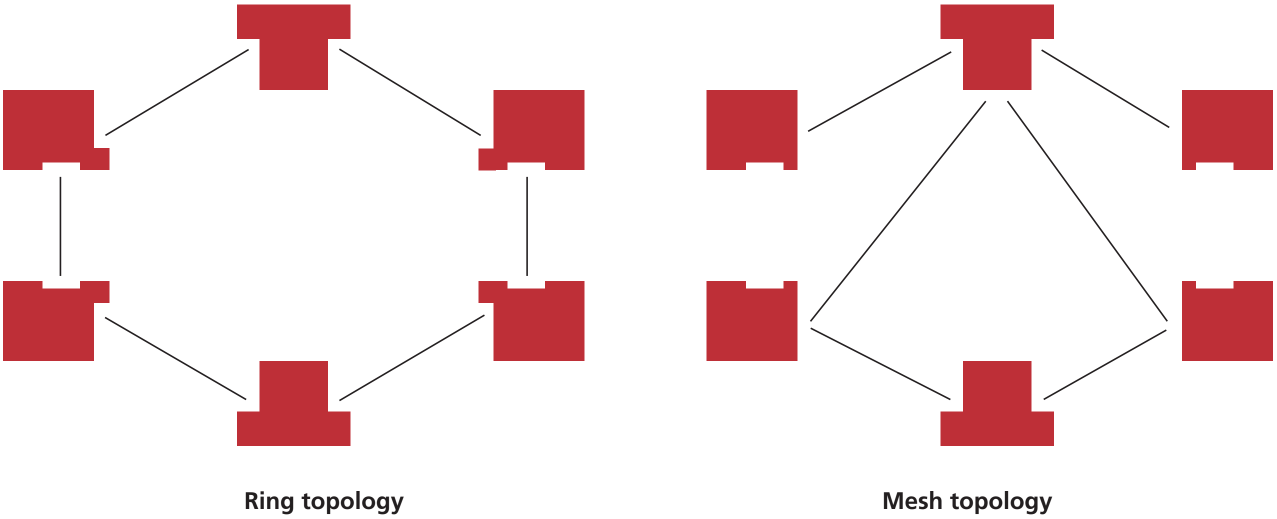


Figure 7: Accepted topologies for backbone layer

The ring topology can be easily extended to multi-ring topology. Using two cross connections a network with 2 rings can be obtained (Figure 8). The investment costs of the resulting architecture are greater but its reliability and traffic balancing is better.

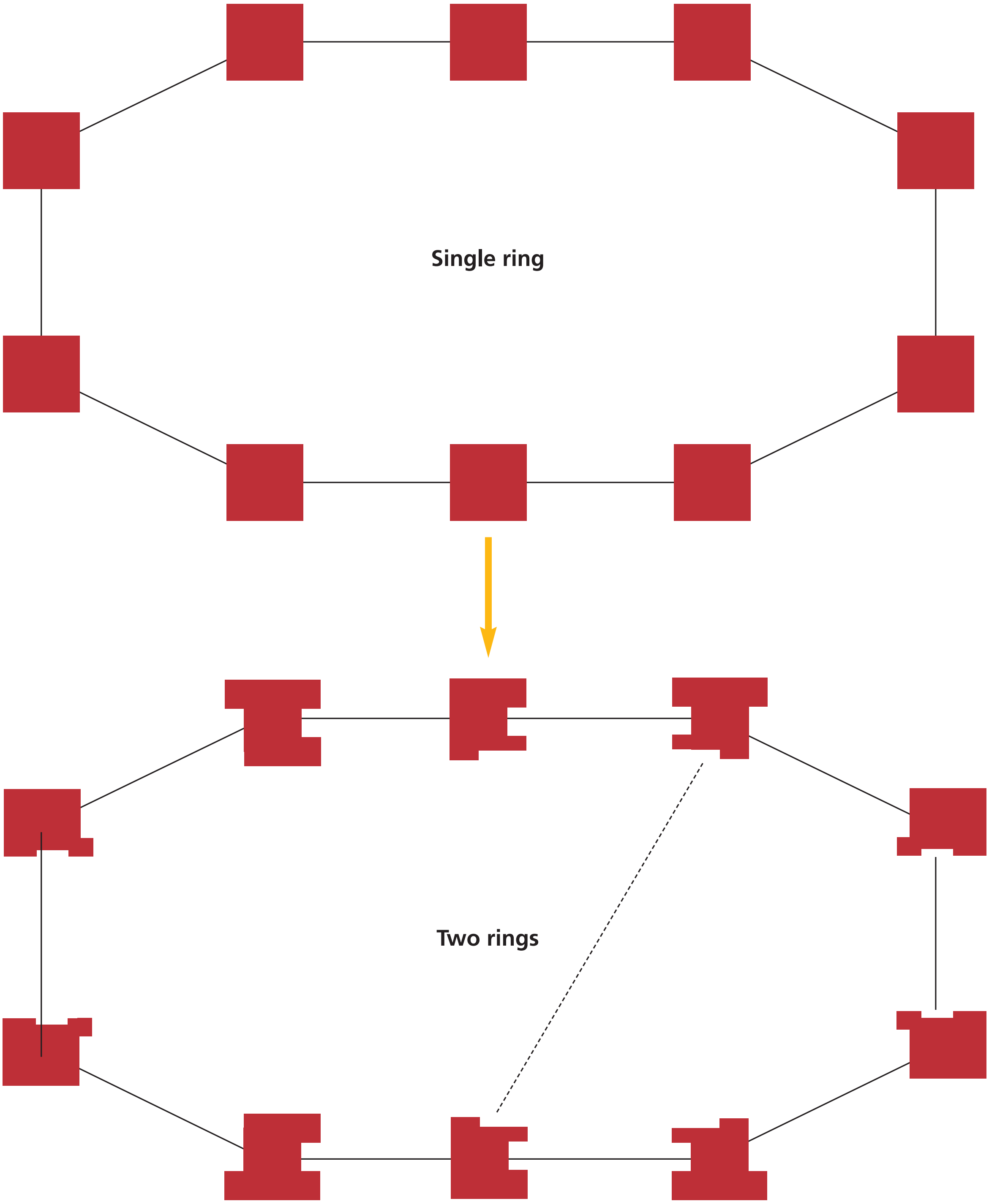


Figure 8: Example of extension of the single ring into a multi-ring topology

For the distribution layer ring, star or tree topology can be used. Advantages and disadvantages of these topologies are summarized in Table 1.

Topology	Advantages	Disadvantages
Ring	moderate building costs high reliability easy to extend from the single ring to a multi-ring topology	limited capabilities for traffic shaping — traffic can be routed only to the neighbouring nodes
Star	simple configuration failure of one end node does not influence the others	no capability of traffic shaping failure of the central nodes leads to downtime of whole network reduced efficiency in planning pathways without link redundancy
Tree	easy to extend adding new branches and nodes simple reconfiguration of the network failure of one node (except the central one) influences only the nodes located beneath in the tree structure easy to implement the hierarchy of the network capability to create nodes for traffic aggregation quite good efficiency in planning pathways	limited capabilities for traffic shaping failure of the central nodes leads to downtime of whole network without link redundancy failure of one link leads to downtime of some part of the network

Table 1: Advantages and disadvantages of topologies for distribution layer

Concluding the analysis of distribution layer topologies, it seems that the optimal solution is a tree topology. It simplifies network planning, reduces the number of links and enables the creation of easily managed and configured network. In addition, depending on operator's needs a volume of local traffic from access networks can be closed within selected leaves of the tree graph, which reduces the traffic load of the central node.

4.2.1.1 Ring

In the design process it is necessary to make a proposal of the most efficient topology for each layer, taking into account their roles in the network. It seems that the most recommended network topology is a ring topology. This solution is a trade-off between CAPEX and reliability. Analysing this solution in terms of performance and reliability of the backbone network, we come to the conclusion that the cost of building of the network in the ring topology is much lower than that in the mesh topology. This is due to the lack of necessity to make multiple cross-connections between nodes. Another saving is due to fewer optical interfaces used in transmission devices of the backbone network.

The ring provides a high level of reliability. Even when the transmission medium is broken at any point or a failure of node occurs, it allows for uninterrupted operation of the network. Damage to the transmission medium does not cause breakdown of the whole network, and the ring is converted to become a bus topology. A failure of the node results in unavailability of only the lower layer of the distribution network connected to this node.

One problem in building a network in the ring topology is smaller ability to manage traffic in comparison to the mesh topology. Traffic between nodes that are not direct neighbours must be routed through intermediate nodes. In case of the mesh topology there exists a possibility of direct routing of the traffic between all nodes. However, taking into account the current state of development of transmission technologies, it can be concluded that this limitation is negligible. Optimization of network traffic can be achieved through configuration of the transport layer in which virtual cross-connections using Dense Wavelength Division Multiplexing (DWDM) optical channels may be set up. In this way, the network that has the physical ring topology can be logically configured to have the mesh topology.

Another way to reduce that limitation and additionally to increase the reliability of the network is to build one or several cross-connections that will divide a single ring into two or more smaller ones. Such modification should be determined on the basis of demographic and geographic factors, cost, expected traffic volume and operator's strategies in terms of network development and level of its reliability.

4.2.1.2 Decentralized Architectures

The point of most architectural and design decisions is whether to build a centralized or decentralized architecture. Centralized systems can be purchased as Commercial Off-The-Shelf (COTS), are built with a pair of high availability components, are technically simple to use and provide the capabilities of the vertical scaling. The result is that well-designed centralized systems provide very high reliability and availability. However they can lead to catastrophic failures due to configuration errors because they usually have a synchronized configuration and any configuration error in one is propagated immediately to the other. Moreover the centralized approach has limits in scaling.

On the other hand, decentralized systems are scaled horizontally and are technically complex to operate. Distributed systems tend to be very resilient to the failure of a single unit because configurations are not shared. The failure of a unit does not affect neighbouring units. At most, the overall capacity is affected.

Compared to other distributed environments (e.g. clusters), complexity of grids derives from decentralized management and heterogeneity of resource components (e.g. hardware, software and utilization). These features lead to variations in grid availability, which depends on resource and network failure rates, administrative policies and fluctuations in system load. Obviously, run-time fluctuations of system availability can affect executed applications. That is why fault tolerance solutions in the grid infrastructure ought to be employed to reduce the influence of time-critical or time-consuming jobs, and the delay and loss that degrade overall system performance and are not accepted by customers. One of them is G2MPLS protocol [Gi08] dedicated for grid network services that aim at provisioning network and grid components in a single step. This protocol may ensure resiliency of network connections.

For server facilities or data centres, plans should be prepared for a backup process or an alternate site. A redundant processing site supplies the best level of resiliency. The less resilient alternatives include a host, warm or cold site. In large telecommunication networks, operators can also own mobile site.

4.2.1.3 Mesh

Resilient mesh networks are designed with multiple redundant communications pathways to ensure that there are no single points of failure. Mesh architecture is more resilient than single architecture even with hierarchy since there are multiple trust points. Recovery is also simpler in a mesh architecture than in a hierarchical one.
In the resilient, self-healing mesh architecture, each node monitors the environment to detect any network degradation or failures and to optimize the network configuration. If a problem occurs with a node, the mesh reconfigures itself to keep the network running. When the node is back online, the network reconfigures to its optimum configuration. Good mesh solutions allow nodes to self-organize into a redundant and resilient mesh topology which results in a high-availability architecture maximizing performance by controlling the environment conditions.

Wireless highly resilient mesh architectures can switch among different frequency bands to overcome any problems in one of them. It also helps ensure that interference on any one frequency band can be avoided. Dynamic channel selection, adaptive noise immunity, MIMO transmission and other advanced RF resource management techniques provide added resiliency.

4.2.1.4 Collaborative Strategies

Collaborative algorithms should be able to cope with the environment in order to manage nodes efficiently and respond dynamically to changes in task and network requirements, which permits the easy creation of ad hoc networks. They are capable using self-organising network infrastructures to adapt to any network incidents, e.g., node failure or connection degradation. Collaboration schemes can improve routing resilience while maintaining predictable latencies and low communication overhead. This approach allows building network-centric solutions.

4.2.1.5 Ad-Hoc

In a Mobile Ad-hoc NETwork (MANET), wireless devices communicate by sending packets on behalf of other devices. MANETs are particularly useful when a fixed infrastructure (e.g., a base station or access point) is impossible to deploy due to environment or time constraints, or when existing infrastructure is inadequate for the given tasks. The reliability, availability and security aspects of MANETs depend on many protocols that are responsible for smart routing, self configuration, self healing, ciphering or data aggregation.

Wireless Mesh Networks (WMN) are a type of MANET. Nodes maintain the mesh connectivity and hold minimal mobility, multiple wireless interfaces and resource constraints. Wireless Sensor Networks (WSN) are a type of WMN that are used for data collection, environmental monitoring and many other applications involving distributed interactions. Many of these applications involve a distributed system of sensors for measuring the environment and then aggregating the collected data to form an overall summary data set. The concept of self-organization is also used in the context of Sensor and Actor NETworks (SANET).

4.2.1.6 Delay Tolerant Networking

Delay-Tolerant Network (DTN) architectures are used for environments characterized by very long delay paths and frequent network partitions. Such circumstance may occur in mobile networks with limited power and extreme environments lacking "always-on" infrastructure due to e.g. inadequate planning of the radio coverage. DTN architectures overcome connectivity problems, long and variable delays, asymmetric data rates and high error rates using store-and-forward message switching. The DTN architecture may deliver the interoperable communications between and among networks with poor and different performance characteristics. So it is possible to get a more robust network architecture. DTN is an "overlay" architecture. It means that DTN is a network of regional networks. DTN protocols operate above the existing protocol stacks of regional networks. DTN can work with IP protocol. The intrinsic TCP resilience against disruptions based on retransmission can be enhanced with a DTN architecture [CFL10].

4.2.1.7 Cloud Networking

Some level of resilience can be reached using a cloud networking concept. Cloud networking improves data centre networks in terms of throughput and resilience. Cloud-based environments are mainly dedicated for web based applications. Clouds require a scalable network infrastructure with high throughput links for applications and a high level of network availability because a network failure can affect many nodes. Designing cloud networking should take the following issues into account: scalability, law latency, guaranteed performance, self-healing resilience and management [Ari09]. Cloud topology depends on user’s constraints of economics, performance and reliability (Figure 9). Nodes are connected to an access leaf via single port or dual-homed connection. Leaf switches are then connected to load-sharing backbone switches. Cloud architecture can be based on layer 2 or layer 3 switches.

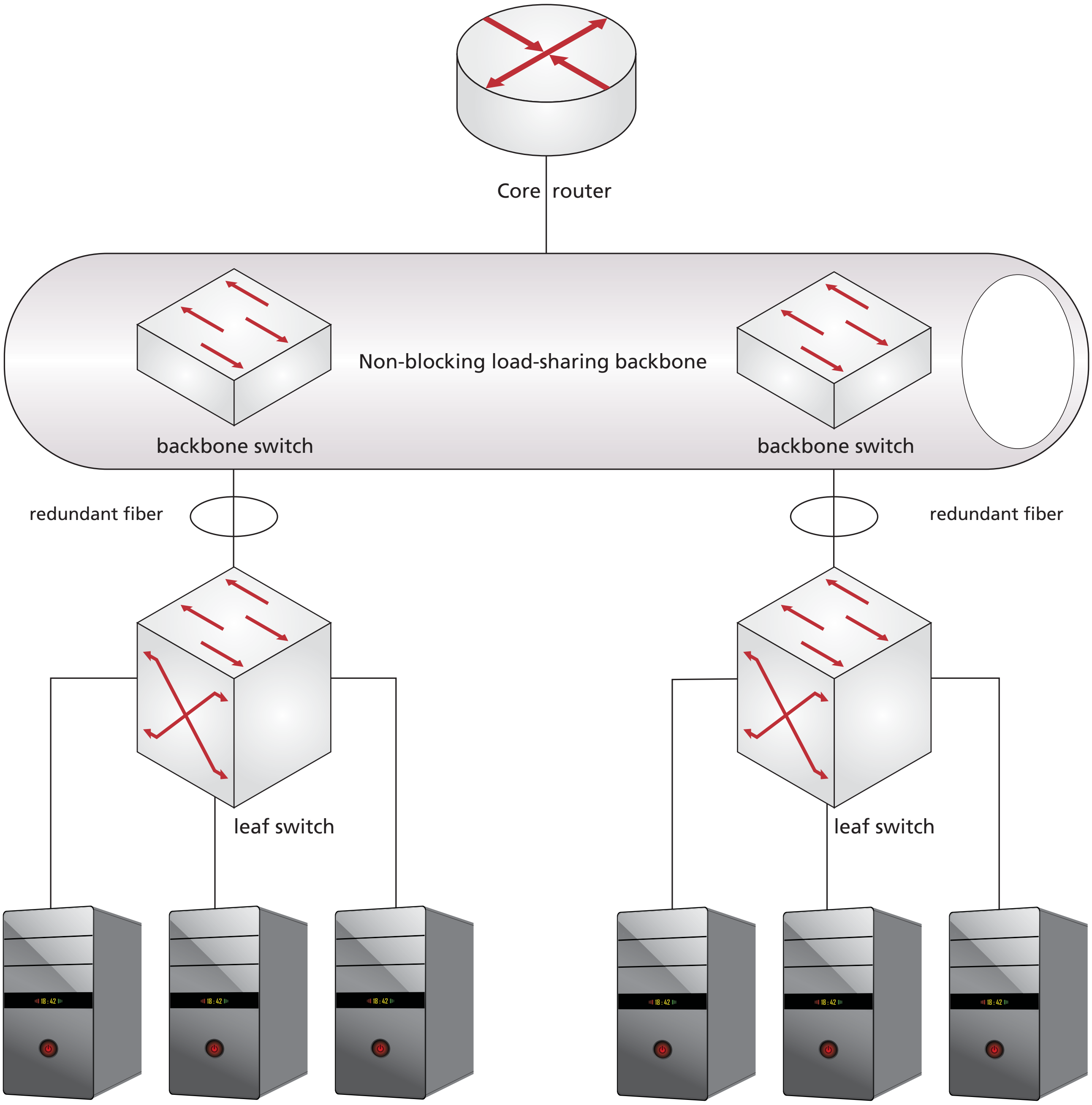


Figure 9: Cloud topology

4.2.1.8 Interoperability/Interworking within Interconnect

Interworking scenarios among different node solutions is desirable. Use cases must at least consider traffic and routing isolation, security, QoS, access and management aspects. This requirement is essential of network migration, to ensure service continuity among sites belonging to different portions of the network. For a resilient network interconnect distributed bridge and distributed port models may be deployed. Interconnect solutions should support multi-vendor interoperability. Multiple technologies or infrastructure suppliers will have a negative impact on interoperability, resilience and availability.

4.2.1.9 Service Oriented Architecture

Resiliency defined as the continued availability and performance of a service despite negative changes in its environment is vital in a Service-Oriented Architecture (SOA). An SOA infrastructure must ensure that a service is highly available regardless of unpredictable conditions, such as sudden and significant degradation of network latency, increase in database response times, or degradation of dependant services. SOA lets increasing productivity, efficiency and business resilience, reduce costs and improve IT alignment with business priorities. SOA allows creating architecture that is more flexible, responsive and easy to align with the needs of customers. Each transaction in an SOA application may concern many separate web services. SOA can be built based on a middleware solution that integrates services throughout a network architecture. In order to support SOA applications a flexible, adaptive and agile network infrastructure called Service-Oriented Network (SON) is used.

Using NoTA service oriented architecture and Smart M3 information sharing services an interoperability of cognitive radio modems, embedded systems, and other smart objects may be achieved. NoTA is a modular service level architecture which can use multiple PHY+MAC layer technologies. It can also be described as a generic network layer for any physical transports enabling extremely heterogeneous, portable and highly scalable networks. NoTA can be used for inter and intra-device communications as it abstracts the physical transport from the services using NoTA. Smart M3 is a semantic information level interoperability architecture for smart environments. It is used for sharing semantic information between devices and services much in the same manner as in the semantic web. Smart M3 is use case, device, domain and vendor independent system in which the smart applications share information conforming to a common ontology. Smart M3 is a publish-subscribe architecture with shared local databases enabling physical space mash-up applications.

Due to such complete approach an improvement in operation and efficiency of systems can be reached by enabling the information sharing between the devices and objects in the environment. Cognitive radio modems and other communication devices could benefit from the information from other embedded and communication systems in making better decisions. Used frequencies, transmission powers, number of devices in operation area, expected communication capacity needs, and positions and locations of devices are examples of such information. The NoTA allows creating modular and horizontal system architectures while Smart M3 semantic information sharing services allows simple and flexible interoperability agreements between device and system providers and reduces to complexity and cost of devices. Inclusion of NoTA and Smart M3 techniques would enable efficient cooperation of devices, even if they were using different radio access interfaces, e.g., in a heterogeneous environment.

4.2.1.10 Middleware Architectures – Dynamic Environments

Middleware architecture should be flexible and extensible to operate with different applications in different network configurations. Other features include communication architecture, interoperability, dynamic issues and dependability aspects. Network middleware is responsible interconnecting components in a distributed system. This concept is a basis to service-oriented network architecture. It uses a dynamic service discovery and composition to handle the dynamism and diversity in the environments. Robust middleware architecture should take into account services e.g. at link layer and performs optimization of connectivity with the help of decision making support provided by application requirements and network conditions. Good middleware approaches are application-focus and reusable. Middleware is often referred as the information exchange infrastructure. It can ease and facilitate the construction of distributed systems. Different middleware technologies deployed in components of large scale distributed systems can be integrated using object-oriented or data-oriented approaches. Fully distributed and highly resilient SOA may be based on Peer-to-Peer (P2P) agent-based middleware.

4.3 Intrinsically Resilient Technologies

A well-designed resilience scheme has to consider the various resiliency requirements of traffic flows, resulting in a more cost-effective network design as well as traffic engineering [Pho08]. Resilience mechanisms can be classified according to the different requirements requested by various applications. Of course it is impossible to guarantee 100% resilience to all types of traffic flows, because it is practically unnecessary, cost inefficient and wasteful in terms of resource utilization. A more efficient resilience scheme should provide different levels of network survivability to different traffic flows according to the respective Service Level Specifications (SLS) in order to maximize the network utilization.

Two recovery schemes can be identified. The first recovery approach recovers the affected services in the lowest possible layer. The survivability is provided as close as possible to the origin layer of the failure. In this method, every survivable layer reserves some resources for the recovery purposes. In the second multilayer recovery approach recovering disturbed traffic is done close to the origin of the failure, independent of the layer.

IP-layer recovery offers both proactive protection and reactive restoration. After detection each router independently replaces all paths corrupted by the failed link(s) with new path(s). Protection at the network layer is not inherently supported by the IP protocol suite. It can be however provided by MPLS protocol that offers fast recovery but consumes additional resources. Protection switching labels may be distributed along paths that are disjoint to the primary path. Additional resilient level is offered by IPv6 that allows end-user services to create multi-domain VPN/OPN networks with unicast, multicast or broadcast services.

Link state information required for routing includes link capacity, total link flow and the network topology. The network topology can be supported by classical routing protocols (e.g. SPF). The link capacity and the total flow capacity on links require extensions to traffic engineering (e.g. extended version of SPF). If there are anycast flows information on the location of the replica servers are also needed. An extension to the existing QoS architectures — Resilience-Differentiated QoS (RD-QoS) proposed in [AK02] — allows integrating the signalling of resilience requirements with QoS signalling. Applications inform the network edge about their resilience requirements together with their QoS requirements. The signalling message influence resource management and traffic handling. RSVP-TE and the CR-LDP protocols are also extended to include resilience classes in the signalling message [HJB06].

There are two methods for survivability: dynamic restoration and pre-designed protection. In dynamic restoration, the backup path discovery procedure is initiated after a primary path fails. On the other hand, in pre-designed protection, a backup path is calculated and reserved at the time of establishing the primary path. If a backup path cannot be found under current network conditions, the connection request is blocked. The pre-designed protection method can offer the shorter restoration times and the 100% restoration guarantee as compared to the dynamic restoration method.

Several principles for QoS guarantee can be identified: (i) marking of packets is needed to distinguish between different classes; (ii) isolation of one class to the other is required; (iii) resources should be used as efficient as possible; (iv) Call Admission Control mechanism has to be implemented. QoS metrics for presenting e2e service/application requirements are delay, jitter, loss rate and throughput. The QoS requirements of a user are grouped into a QoS profile. This QoS profile is then used to establish an appropriate bearer service.

Bandwidth management mechanisms include:

Traffic shaping:

- Token bucket
- Leaky bucket
- TCP rate control

Scheduling algorithms:

- Weighted Fair Queuing (WFQ)
- Class-Based Weighted Fair Queuing (CBWFQ)
- Low Latency Queuing (LLQ)
- Priority Queuing (PQ)
- Weighted Round Robin (WRR)
- Deficit Weighted Round Robin (DWRR)
- Hierarchical Fair Service Curve (HFSC)

Congestion avoidance:

- Random Early Detection (RED), Weighted Random Early Detection (WRED)
- Policing, i.e., marking or dropping the packet in excess of the committed traffic rate and burst size
- Explicit congestion notification
- Buffer tuning

QoS in IP networks can be provided using many techniques. They are DiffServ or IntServ models; RSVP, RSVP TE or MPLS protocols as well as IEEE 802.1p, IEEE 802.1Q or IEEE 802.11e standards.

For resiliency of routing in the domain of stability one can deploy:

- fast reroute and link bundling with fast recovery — it allows traffic to continue to be transmitted along an alternate path until the routing protocols converge on a new topology;

- BGP next-hop indirection — due to grouping BGP routes that use the same next-hop together this approach makes forwarding changes as a group;

- fast link failure detection — the time to detect a failure is reduced through the application of direct notification to routing-protocol processes;

- continuous forwarding upon routing changes — when a router receives an update that causes traffic to use a different route or next-hop, the router should not drop packets during this change.

It is estimated that stateful protocol protection can eliminate about 60% of routing convergence events [Bre04]. Routing scalability can be however achieved through a combination of network architectures/topologies and more powerful router-processing capabilities. Failures in fibre optics can be easily detected using such mechanisms as:

- UniDirectional Link Detection (UDLD) that detects and disables unidirectional links on fiber optic interfaces;

- Digital Diagnostic Monitoring (DDM) that diagnose fiber connections in real-time for early detection of optical signal deterioration;

- Bidirectional Forwarding Detection (BFD) that allows fast failure detection and reduced re-convergence times in a routed environment.

Resiliency and highly availability of ring topology can be achieved using:

- Ethernet Ring Protection (ITU T G.8032) designed for loop protection and fast convergence times in ring topologies;

- different Spanning Tree Protocol (STP) (IEEE 802.1D): Ring Rapid Spanning Tree Protocol (RRSTP), Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s), Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w).

Cooperative RRM framework can make joint optimization. Such QoS-balanced system allows different functional entities to form synergies and multiple access networks to interact. QoS differentiation can be based on transmitting content that is especially adequate for video streams.

An important requirement in a resilient network is to provide differentiated survivability services to different types of traffic. It allows higher priority demands to allocate higher network availability. The resiliency can be achieved by load balancing the network traffic between the tiers.

In the network infrastructure the system-level intelligence such as policy-based management, policy-based provisioning, adaptive threat defence, enhanced application optimization or fraud detection should be deployed. The system and protocol configuration procedures should be dynamic and automatic to the highest degree possible. Due to it the application can manage network transport services using higher-layer controls. Policy-based management seems the best platform to achieve these control features. A policy-based management system is useful if it allows high level description of abstract policy. It should also enable such policy to be refined and eventually mapped into an appropriate configuration for controlling devices in the managed system. Such system ought to enable flexible and modular composition of policies as well as to support distributed management e.g. with policy agents. It also manages dynamic networks with self-x features and scalable hierarchy of policy agents. Such approach ensures resilient network services, automatic correction network faults, reconfiguration of network components as needed, and optimization of network performance. Furthermore, policy protocols support an outsourcing [RFC2748] as well as a provisioning [RFC3084] model of operation. A further unification of these models is also possible using a dynamically configurable, highly flexible information exchange pattern based on recorded events [COPS]. Consequently, policy-based management can provide the integrated management of the service provision process and network operation in heterogeneous infrastructures.

Several types of resilient circuit configurations can be set up [BT10]:

i. single circuit with diversely routed primary and secondary fibre paths between nodes,

ii. primary and secondary diversely routed circuits,

iii. two configurations of type ii.

Resilient routing within a customer's premises can accompany each configuration.

In-built resilience solutions use different protection schemes. They can be dedicated 1+1 protection (simultaneously transmission on both primary and backup paths) or shared 1:1 protection (transmission is on the primary path and it is switched to the backup path if failure occurs). In the latter scheme, the backup path can be used to carry low-priority traffic during normal operation. Shared protection scheme can be extended to M:N protection where M primary paths may share N backup paths. Network pathways can be classified with different resilience objectives. Class 1 is fully protected by 1+1 or 1:1 dedicated protection. Class 2 is recovered by shared protection. Class 3 may provide restoration using the spare capacity left after recovery of Class 1 and Class 2.

Other solutions for resiliency can involve:

dual-home link support for link protection,

Virtual Router Redundancy Protocol (VRRP) to provide highly available routed environments,

redundant and hot-swappable power supplies as well as transceivers modules for uninterruptible availability,

dual image and dual configuration file storage for back-up.

To ensure the resiliency different priorities can be defined: i) high priority protected paths, ii) unprotected paths and iii) low priority pre-empted paths. For high priority protected path both primary and backup paths are identified before working path is set up. In the case of unprotected path when a failures appears a dynamic restoration mechanism is initiated to identify the back path but without any guarantees. Unprotected low priority pre-empted path is released if a failure occurs.

To deal with the increasing complexity of systems and uncertainty of their environments, networking has turned to self x concept that can be read as self-reconfiguration, self-optimising, self-diagnosing, self-healing, self-protecting, self-organization, self-forming, self-adaptivity or self-management. Self x leverages wireline and wireless systems and provides transmission resiliency resulting in an autonomous behaviour. The self x features and facilities relate to both hardware and software. All such solutions work with feedback loops that probe the whole infrastructure.

The resilience in radio networks can be guarantee not only by MANET architecture or collaborative strategies, but also by cognitive concept of radio transmission. Cognitive Radio Networks (CRN) are highly adaptable and resilient to maintain connectivity between nodes.

4.4 Network Management

To ensure that all steps are taken to provide maximum network resilience and reliability, designers and managers of the network should establish and implement corporate standards and requirements in consideration of the best practices of the communications industry (e.g., ETSI, ITU, NRIC Best Practices, TMN, ITIL, COBIT, etc.). Some of these steps are listed below.

4.4.1 Designing the Network

During the design phase of network building, several steps should be taken to ensure its proper manageability. These are at least: dimensioning, monitoring, security, reliability/availability (e.g. via physical and logical architecture/topology design) and quality of service.

Network operators should design and implement procedures for traffic monitoring, trending and forecasting so that capacity management issues may be addressed. This helps expanding the network and ensuring that it provides the necessary capacity. When the network capacity is too narrow its throughput is reduced, when too broad – funds are wasted.

Network designers should establish a process, during design or implementation of any network element or management system, to identify potentially vulnerable, network-accessible services (such as Network Time Protocol (NTP), Remote Procedure Calls (RPC), finger, rsh-type commands, etc.) and either disable, if unneeded, or provide additional external network protection, such as proxy servers, firewalls, or router filter lists, if such services are required for a business purpose. Also, network operators should implement architectures that partition networks and applications using means such as firewalls, De-Militarized Zones (DMZ), or Virtual Private Networks (VPN) so that contamination or damage to one asset does not disrupt or destroy other assets. In particular, where feasible, it is suggested that the user traffic networks, network management infrastructure networks, customer transaction system networks, and enterprise communication/business operations networks should be separated and partitioned from one another. Additionally, in critical networks for Operations, Administration, Management, and Provisioning (OAM&P) switched network hubs should be used, so that devices in promiscuous mode are less likely to be able to see/spoof all of the traffic on that network segment. If needed management centres should be multiplied and geographically split. They should be redundant processing sites or hot sites.

4.4.2 Operating the Network

Network operators should regularly scan infrastructure for vulnerabilities/exploitable conditions. They should measure EMS (Element Management System), NMS (Network Management System) and OSS (Operational Support System) performance, and comparing them to a benchmark or applicable requirements would help to verify that performance objectives and expectations (e.g., internal performance criteria, system vendor specifications) are being met. When available, a management system capability could be utilized (e.g., CORBA, SNMP) providing a single interface with access to alarms and monitoring information from all critical network elements.

Network operators and service providers should remotely monitor and manage the emergency network components using network management controls, where available, to quickly restore emergency/alarm service and provide priority repair during network failure events.

To prevent the loss of data, network operators should develop documentation for the restoration of power for areas of critical infrastructure including such things as contact information, escalation procedures, restoration steps and alternate means of communication. This documentation should be maintained both on-site and at centralized control centres.

Considering the software layer of the network, operators should maintain software version deployment records, as appropriate. They should understand the operating systems and applications deployed on their network and keep abreast of vulnerabilities, exploits, etc. Maintaining a patching process, to repair eventual vulnerabilities and exploits is also crucial.

Another way to prevent exploits is to authenticate, authorize, attribute, and log all management actions on critical infrastructure elements and management systems. This especially applies to management actions involving security resources such as passwords, encryption keys, access control lists, time-out values, etc. This however boils down to the security management in communication networks. To keep up with the technological progress of various networks, managers should incorporate methodologies that continually improve network or equipment performance defining processes met e.g. ISO standard.

4.4.3 Access Control Management

Network operators should develop an enforceable password policy, which considers different types of users, requiring users to protect, as applicable, either:

a) the passwords they are given/create or

b) their credentials for two-factor authentication.

This should be based on the principles of least-privilege (the minimum access needed to perform the job) and separation of duties (certain users perform certain tasks). To achieve this, a process should be determined, to discover which users require access to a specific device or application.

Operators should create an enforceable policy that considers different types of users and requires the use of passwords or stronger authentication methods. Where passwords can be used to enhance needed access controls, they should be sufficiently long and complex to defy brute-force guessing and deter password cracking. Everyone considered should change passwords on a periodic basis. Regular audits on passwords should be performed, including privileged passwords, on system and network devices. If available, features across the user base that force password changes should be activated.

Passwords should be stored in encrypted form, using industry-accepted algorithms and key lengths for encryption (for this and every other purpose), such as 3DES or AES.

Physical protection of the vulnerable network elements should also be provided. In particular, facilities/areas that are used to house certificates and/or encryption key management systems, information or operations should be provided with proper physical protection.

4.5 Basics of Risk Management for E2E Resilience

Risk Management, in relation to resilience, aims at :

- identifying major threats and risks
- evaluating those risks
- monitoring these threats and risks
- developing ad hoc defences and response measures
- managing a programme of continuous improvement
- establishing a risk management system
- embedding risk management within corporate management processes and functions.

Risk evaluation relies upon two major activities:

- incident likelihood assessment
- impact analysis

Typically, asset-focused approach is used in risk management for Critical Infrastructures and is described in the remainder of this chapter. However, for information services, another approach that may be more scalable in large installations, is working with critical functions the information service / infrastructure provides and then applying top-down model for identifying critical assets and performing threat modelling. Several approaches exist that help in modelling risk in complex infrastructures including scenarios (starting with threat actors and identifying specific scenarios, vulnerabilities, and consequences from there), threat trees (starting with undesirable consequences and identifying vulnerabilities and threats that could effect them).

4.5.1 Incident Likelihood Assessment

The process of risk management begins with identifying the assets concerned, which may commonly be thought of in terms of operational hardware and software, but which could also include intellectual property, organisational units and processes, and services provided. Each asset should be clearly identified and an asset owner should be allocated to ensure that some responsible person within the organisation is accountable for its entire life cycle.

For each asset considered, a series of possible threats may materialise into major incidents that may cause its loss or unavailability.

For each threat, the organisation should make an assessment of the potential likelihood of the threat occurring – again it may be possible to make a quantitative assessment in terms of percentage of probability, or it may be more feasible to use qualitative measures, examples of which are shown below:

Very high.
- This level of likelihood can be used where the threat or hazard is on the brink of happening and becoming a business disrupting issue, 81% to 100% probability.

High.
- This level of likelihood can be used where the threat or hazard is more likely to occur than not, 61% to 80% probability.

Medium.
- This level of likelihood can be used where the threat or hazard is just as likely to occur as not, 41% to 60% probability.

Low.
- This level of likelihood can be used where the threat or hazard is still significant, but more likely not to occur than to occur, 21% to 40% probability.

Very low.
- This level of likelihood can be used where the threat or hazard is unlikely to occur, 1% to 20% probability.

As manifold threats may lead to a huge variety of possible incidents, likelihood assessment may turn into an overwhelming task. To keep it feasible and pertinent, some choices may be made by risk managers. For instance, it may be easier to group threats by type, such as abnormal traffic load, accidents and human error, large-scale disasters, malicious attacks, weather-related and failures at lower layers. Alternatively, it may be easier to consider only a type of incidents (on the basis of similar features or impacts) and to ignore the multitude of their possible causes on the basis that whatever causes an incident, the latter may occur and what matters is to probabilise its occurrence.

Beside, likelihood may reveal impossible to assess. In that case, it is wise to assess threat exposure, replacing the above metrics by a level of exposure or frequence of exposure. Variants of exposure analysis can rely upon or be pondered by an analysis of the visibility of an asset, the attraction the asset exercises on criminal or terrorist attackers, its vulnerabilities, the ease of an attack, the state and efficiency of existing detection / alarm / defence measures.

4.5.2 Impact Analysis

Should a major incident occur, the impact value of loss of the asset should be determined. This can (when applied to network elements for example) be quantified in terms of the asset's capital value, but should also include the loss of revenue resulting from the non-availability of the asset. Damage to the organisation's brand and reputation may also be evaluated. Domino effects and reciprocal interdependencies though can make this kind of analyses very difficult. In the event that it is not possible to quantify the impact, then more subjective (qualitative) measures should be used, examples of which are shown below:

Enterprise Threatening.
- The business would be irrevocably threatened without the availability of this function. The impact of loss would cause irreparable damage to revenue streams, market position or customer service capability.

Critical.
- A major impact on a specific element of the business where the damage to markets or customers would be severe, but where the organisation would remain viable as an enterprise. The impact would be very noticeable to customers and likely to have financial consequences.

Serious.
- A significant impact on one or more business elements that will require remedial action. In most cases, the impact would be noticed by customers, and likely to be high in financial terms to rectify the problem.

Minor.
- The impact of loss is likely to be localised and affect less critical business processes. It may or may not be noticed externally but some action would be required to rectify the problem. The financial impact is likely to be low and of a less tangible nature.

Trivial.
- No noticeable impact on operations. Can usually be dealt with under 'business as usual' conditions.

4.5.3 Risk Matrix

Once the Impact and Likelihood have been assessed, a Risk Matrix should be drawn up and each identified risk should be plotted on a risk matrix by impact against likelihood, as illustrated in Table 2.

Impact	Enterprise threatening	🟧	🟧	🟥	🟥	🟥
	Critical	🟧	🟧	🟧	🟥	🟥
	Serious	▨	🟧	🟧	🟧	🟥
	Minor	▨	▨	🟧	🟧	🟧
	Major	▨	▨	▨	🟧	🟧
		Very high	High	Medium	Low	Very low
				Likelihood		

Table 2: Risk Matrix

IThose risks which are categorised as High must be dealt with immediately; those which are categorised as Medium should be addressed when possible, and those which are categorised as Low may be left until last.

4.5.3 Risk Treatment

All risks shall be treated to the best possible extent. The means of treatment shall take one of the following forms of the "4T" Model:

Terminate / Avoid.

- The risk may be avoided by not undertaking or halting the activity that creates the risk. This may be the case with risks that cannot be controlled and that cannot be insured nor transferred.

Transfer.

- The risk may be transferred to another party (e.g. insurance or financial provisions). Ownership of the risk however remains with the organisation itself.

Treat / Mitigate.

- The risk is mitigated in some way by imposing controls to alter either its impact or its likelihood. This may involve innovative alternative solutions and/or capital investment in additional components of the service to raise it to a higher level of resilience.

Tolerate / Accept.

- If the level of risk falls within the risk appetite of the organisation, it may be accepted and reviewed at regular intervals to ensure that it remains low.

5 – Causes and Location of Failure

5.1 Network Elements

For the purposes of this discussion, a network element is described as any hardware device (which will also inevitably contain some form of operating system and one or more software applications) used within the end-to-end network. This can include (but is not limited to) routers, switches, base stations and cross-connecting equipment.

The failure of a single network element can, if the network is incorrectly configured, cause a complete failure of the service.

Types of problem that can have a negative impact on network elements include:

- Hardware failure – although many network elements provided at 'carrier class' are designed to operate on the basis of 'five nines' (i.e. 99.999% availability), failures can and do occur.

- Software and/or firmware failure – as with network hardware, the software and firmware that operates within it is designed to operate at a minimum of five nines availability but again, even with rigorous testing failures will occasionally occur. One important aspect of this type of failure is that if a particular software or firmware release has been rolled out across an entire network, there is the risk of a 'common mode' failure which implies that other network elements containing the same levels of software and firmware could suffer from the same fault. Further still, there is the added risk of a 'cascade failure', in which the same fault impacts all similar elements in a network that then all fail either simultaneously, or in rapid succession.

- Incorrect configuration – this is largely brought about by human error, in that the network design is either poorly carried out, or that the design is mis-keyed when making configuration changes.

- Electronic attack the symptoms of this are generally similar to the incorrect configuration problem described above, but in this case are as a direct result of a deliberate attempt to disrupt network operations. Electronic attacks are generally assumed to be from an external source, but there is a real danger of attacks taking place from within the organisation.

- Network synchronisation – it is vital that the synchronisation of elements within and between networks is maintained to a high level of accuracy. Typically, network operators use a synchronisation source that will guarantee accuracy and stability to one part in 1011, and is typically sourced from so-called 'Stratum 1' devices, for example the 2 Mb/s synchronisation signal widely used in the UK is recovered from GPS sources. Nevertheless, a single source for synchronisation (despite the fact that it may be presented at many network nodes simultaneously) remains a single point of failure, and although GPS is considered to be highly reliable, it has been shown that relatively low-power transmitters can interfere with GPS signals, and could cause inter- and intra-network synchronisation issues.

- Theft and vandalism – while the threat of theft is comparatively low, there have been a number of pre-planned robberies targeted directly at network operators, and high-value equipment has been stolen to order. Vandalism is generally not a major problem, but the results of it can be serious.

- Loss of power supply – without a constant, reliable, stable source of power, network equipment cannot deliver a reliable service.

- Over-heating – all network equipment generates heat during operation, and this heat must be removed from the operating environment by means of air conditioning, the failure of which can have serious effects.

It should be noted that the above descriptions also apply to the equipment that provides the network interconnections described below.

5.2 Network Interconnections

Some form of local-area or wide-area transmission link interconnects all network elements. This may be based on copper or fibre optic cable technology, or increasingly on wireless technologies. As with network elements, the failure of a single network interconnection can, if the network is incorrectly configured, cause a complete failure of the service.

Types of problem that can have a negative impact on network transmission include:

- Cable faults – older copper cables can be susceptible to faults as a result of either movement of the ground around the cable or by the ingress of moisture. Connection faults such as 'dry joints' in which the soldered connections lose their integrity are also a frequent cause of copper cable faults. More recent fibre optic cable technology suffers from similar faults in that movement of the ground around cables can cause fractures; terminations can become dirty, attenuating the flow of light through the fibre, and also mis-handling by technicians can cause breaks at the critical joints or splices in the fibre.

- Cable theft and vandalism – this is an increasingly serious problem for many critical infrastructure sectors – energy companies, water and sewerage companies, road and rail transport companies are affected as well as fixed, mobile and broadband network operators. Thieves are largely opportunistic, and will attempt to steal cable regardless of type, which results in fibre optic cable being cut as well as copper cable. Generally once thieves realise that it is fibre, they leave it in the ground, as it is almost worthless to them. The net result however is the same, as the break must still be repaired.

5.3 Functional Service Architecture

In addition to failures in individual components and network infrastructure a network service can fail due to defects or exceptions at the architectural level resulting from unforeseen or unhandled interactions between network elements and/or the network itself. Some examples include:

- Protocol-level implementation differences among key network elements
- Ineffective handling of intermittent network faults
- Unhandled exceptions in distributed service architecture
- Interoperability issues between different versions of hardware and software
- Insufficient integration testing of the solution
- Insufficient regression testing after service component upgrades or configuration changes

5.4 Supporting Infrastructure

All network elements and interconnections require the support of a number of distinct services in order to operate normally. These include the buildings or structures in which they are housed, power supplies, air conditioning, electronic security and network monitoring and management. Again, the failure of any or all of these supporting services can, if not appropriately provided cause a complete failure of the service.

Types of problem that can have a negative impact on supporting infrastructure include:

Building and compound security

- the environment in which network elements are housed is a key point of vulnerability, and if unprotected leaves the equipment vulnerable to theft and vandalism while also in some cases leaving opportunity for access for direct electronic attack.

Power

- One of the most critical components of the overall service is the power which supplies the infrastructure. Some countries (and indeed some areas within countries) are at greater risk of power failure than others, and even in those areas where power is thought to be reliable, unexpected events (such as floods and poorly executed civil engineering works) can cause significant issues. Indeed, severe weather is a major hazard to several types of critical infrastructure, and despite advances in meteorology, prediction of sudden-onset severe weather events remains a challenge.

Cooling

- The need to remove excess heat from equipment areas is of paramount importance. Much of the more recently-developed networking equipment is able to handle temperatures at which many humans are less comfortable, and there is a move towards to maintaining equipment room temperatures at around 25° C which results in lower cooling costs. However, if the temperature climbs above 30° C for more than a short amount of time, failures will inevitably occur, and long-term damage to the equipment is likely to result.

Electronic security

- While the physical security of an equipment site is important, the electronic security that underpins this has equal importance. This includes environmental security including moisture detection, fire detection (and suppression), building access control, and network security including network firewalls preventing access to the uninvited while allowing authorised staff to access equipment both physically and electronically.

Network monitoring and management

- Virtually all network equipment nowadays is able to communicate with operational support systems using the Simple Network Management Protocol (SNMP) or similar, and Network Operations Centres (NOCs) will monitor network elements and collate alarms which will either provide an indication of failure or of reduced operational effectiveness, or will provide an indication of problems which are building up. The next stage on from this is the taking of corrective action – network management. It is equally important that these network monitoring and management facilities are also resilient to failure of essential services.

5.5 Network Demand

All forms of network, fixed or mobile, must be planned both prior to initial installation and continually while in operation. Part of the planning process is to ensure not only that adequate capacity is provided, but also that there is sufficient additional capacity within the network to permit the handling of above-normal levels of traffic such as happen when a major sporting event (e.g. the World Cup) takes place.

Failure to plan for such eventualities can often result in traffic congestion, the consequences of which can be long lasting. Additionally, as 'normal' traffic levels grow organically, it is vital that ongoing capacity planning is carried out to ensure that supply always exceeds likely demand, plus a pre-defined amount of 'headroom' that caters for both planned and unplanned events.

5.6 Human Error

Human error is still one of the most common reasons for failure in network services. Countless cases of network and service failures can be cited that are attributable to misconfiguration, negligence, lack of coordination, lack of training, ambiguous or non-existent procedures, and social engineering. This challenge highlights the acute need for comprehensive preparedness as means of achieving high level of operational resilience.

5.7 Malicious Attacks

Malicious attacks can be carried out on different network components: nodes, links, servers, software, etc. using wireline/wireless access, malware, diskette, USB stick or even WWW pages. New techniques of cyber attack overcome those typical ways of attacks in Internet. In 2010 Bushehr nuclear power in Iran was targeted by a computer worm that had infected industrial computers in isolated LAN through contaminated private software of the power plant's employees. In this attack, Stuxnet virus infected Windows machines via USB keys. Moreover, it exploited several previously unknown and unpatched vulnerabilities in Windows, known as zero-day exploits.

The measures to counteract such attacks comprise firewall, IDS/IPS as well as anti-virus and anti-malware software.

6 – Good practices

6.1 Emergency Preparedness for Resilience

In order to be resilient so as to assure sustainability of operations, competitiveness and performance, organizations must prepare for major incidents.

The key benefits from preparedness are:

Increased provisioning reliability

Improved network and operational resilience

More effective and quicker recovery

Reduced cost of consequences

Increased stakeholder confidence.

But what does it take to get ready for emergencies? And first of all, what is an emergency?

6.1.1 From Minor Incidents to Crises

Incidents usually range from very minor events punctuating the daily operation of an organisation, up to catastrophes that usually destroy everything.

In a first approach, we could define a "***Minor Incident***" as:

a failure or error resulting either from human action or from natural or technical causes

that affects the organisation temporarily

that can be fixed following ad hoc set procedures

within a short frame of time and with impacts, whether direct or indirect, considered negligible as they do not affect customers nor users.

We could also define a "***Major Incident***" as:

an interruption, disruption, failure or error resulting either from human action or from natural or technical causes

that affects the organisation or its customers and users temporarily

that can be fixed with the help of ad hoc incident management arrangements, procedures and resource

within a frame of time and with impacts, whether direct or indirect, standing within specified limits beyond which they would become intolerable.

6.1.2 The Two Ways of Dealing with Incidents

Whereas minor incidents are usually dealt with by resorting on incident response procedures designed as part of safety or security analyses, major incidents, usually interruptions or significant disruptions of processes, are dealt with by way of a Business Continuity Plan, Contingency Plan or Disaster Recovery Plan (depending on the terms used in a given environment).

Their resolution is reputed to be fairly straightforward: an incident scenario has been studied in "peace times", a response plan has been defined to address it, and to deal with interruptions or significant disruptions that cause more trouble and require coordinated efforts from a variety of teams and actors an incident management team is organised who will supervise and drive recovery operations. That is the sense of the prescriptions found in standards BS25999-1:2006 and ISO PAS22399:2007, respectively on Business Continuity Management and Incident Preparedness and Operational Continuity Management.

But what experience shows, and what existing definitions say, is that there may also be situations in which "*things run out of control*". This means that the A-Z of the prescribed response procedure or plan reveals insufficient in the face of complex circumstances, unexpected combinations or repetitions or durations of incidents, that try the capabilities of the organisation beyond the specified limits mentioned earlier.

They require adaptive and creative solutions to deal with problems for which no pre-defined procedure or plan exists, or if there are such plans or procedures they are not adequate. They also require a "***shift in the commandment paradigm***", from a procedure-based response to a tactical reasoning-based decision-making process. When the treatment of major incidents requires such a shift in the way command and control are exercised, the organisation faces a "***shock***" that sparks the experience of a "***crisis***".

6.1.3 Crises and the Incident Severity Scale

In the context of Critical Information Infrastructures, we shall define a "***crisis***" as a destabilisation of a socio-technical system due to a loss of control of the course of events, caused by a "***shock***" characterised by:

Surprise: meaning that events or impacts were not prevented nor detected

Defencelessness: the lack or inadequacy of existing response plans or procedures

Criticality: the perception of a threat on given assets as fatal, extreme, overwhelming, global, major, unbearable,…

A crisis stems from a shock and requires a shift in the commandment paradigm to counter the destabilisation it causes.

To provide a definition of the notion of "***Emergency***" that can be independent from the particulars of an adverse situation, we proposed the European Commission the principle of an "***Incident Severity Scale***" based on two variables:

the downstream "***impact***" of the incident:

- ***Negligible***: Customers or users, or downstream systems or organisations are not affected
- ***Tolerable***: Customers or users, or downstream systems or organisations are affected within specified limits
- ***Untolerable***: Customers or users, or downstream systems or organisations are affected beyond specified limits

the "***mode of control***" – commandment – required to handle the situation:

- ***ranging from "Procedured defence" to "Supervised Incident management"***: responders follow prescribed procedures; when incidents become major, they need an Incident Management Team to coordinate the execution of the plans and procedures required to recover from the situation at hand

- ***ranging from "Creative adaptation" to "Tactical reasoning"***: when incidents are rather minor, responders may adapt, cut through or just ignore prescribed procedures to resolve them, based on their skills or knowledge; when incidents are rather major or extreme, responders need one or more Crisis Management Teams, within a Chain of Command, to make strategic and tactical decisions to handle situations at hand and (re)gain initiative over circumstances.

Those two variables help segregating everyday incidents from crises.

The Incident Severity Scale proposes six levels of incidents that are shown in Table 3.

#	Level	Impact	Mode of control
0	Minor Events	Negligible	ranging from "Procedured defence" to "Supervised Incident management"
1	Minor Incidents	Negligible	ranging from "Creative adaptation" to "Tactical reasoning"
2	Major Incidents	Tolerable	ranging from "Procedured defence" to "Supervised Incident management"
3	Severe Incidents	Untolerable	ranging from "Procedured defence" to "Supervised Incident management"
4	Severe Shocks	Tolerable	ranging from "Creative adaptation" to "Tactical reasoning"
5	Extreme Shocks	Untolerable	ranging from "Creative adaptation" to "Tactical reasoning"

Table 3: Characteristics of the 6 levels of severity in the Incident Severity Scale

The following chart (Figure 10) shows where the shift in the commandment paradigm occurs and details the modes of response that can be mobilised at each level.

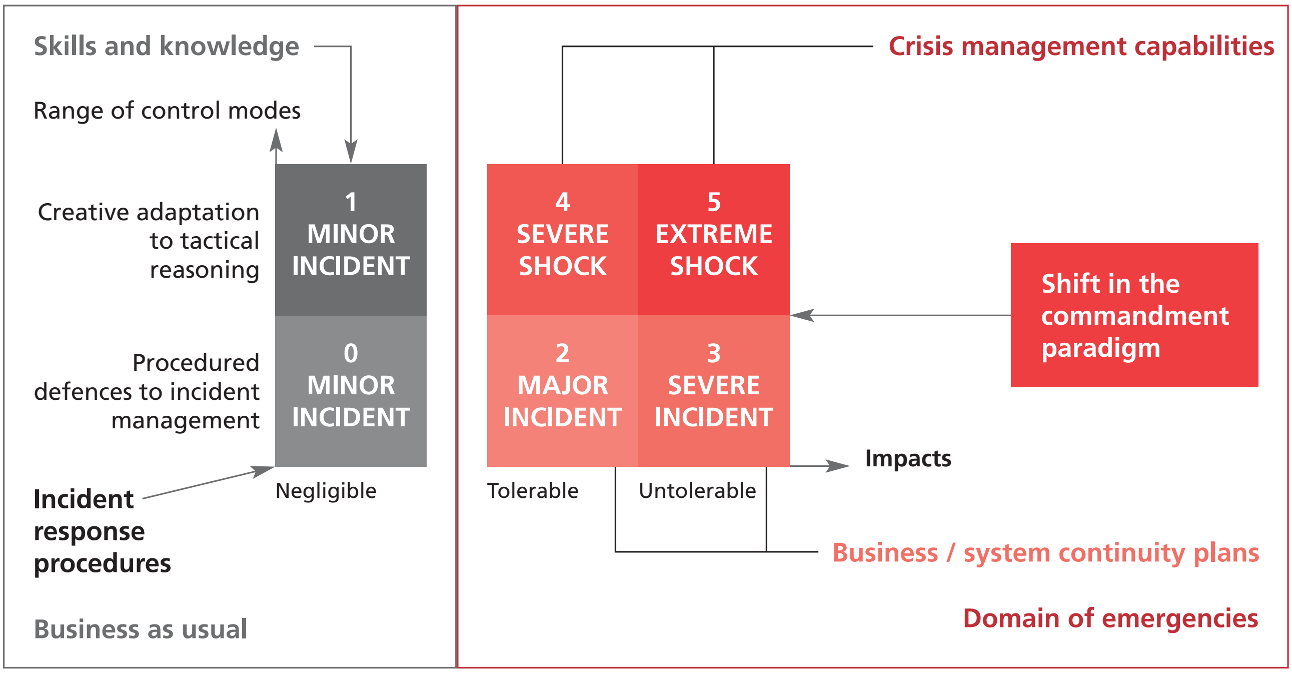


Figure 10: The Incident Severity Scale and the domain of Emergencies

Based on the Incident Severity Scale, an "***Emergency***" can be defined as a "situation in which a socio-technical system has to cope with a situation ranging from a major incident up to an extreme shock" (levels 2 to 5). Some events, usually ***interruptions*** or only significant ***disruptions***, can be handled by running Business or System Continuity Plans: they stand in the [2,3] range.

A "***Crisis***", in particular, is a situation in the [4,5] range.

Resilience is an organisation's aptitude to handle crises successfully. To understand how organisations can be resilient under critical circumstances, one needs first to understand the dynamics of such a crisis situation.

6.1.4 The Collapse Ladder and the various Response Modes

Studies performed in the field of socio-ecological systems' resilience for instance, as well as case studies of socio-technical systems show that a socio-technical system confronted with a crisis experience a more or less progressive collapse, i.e. the loss of:

- control over the course of events: their initiative over adverse circumstances
- control over their own course of action: their very capacity to act upon events
- control over their vital functions: key processes and resources needed for acting.

As the "***Collapse Ladder***" shows below in Figure 11, once taken aback by surprise, an organisation has to struggle in order:

- to avoid falling down the steps of the collapse ladder
- to keep acting on its missions
- to resume nominal operations as quickly as possible

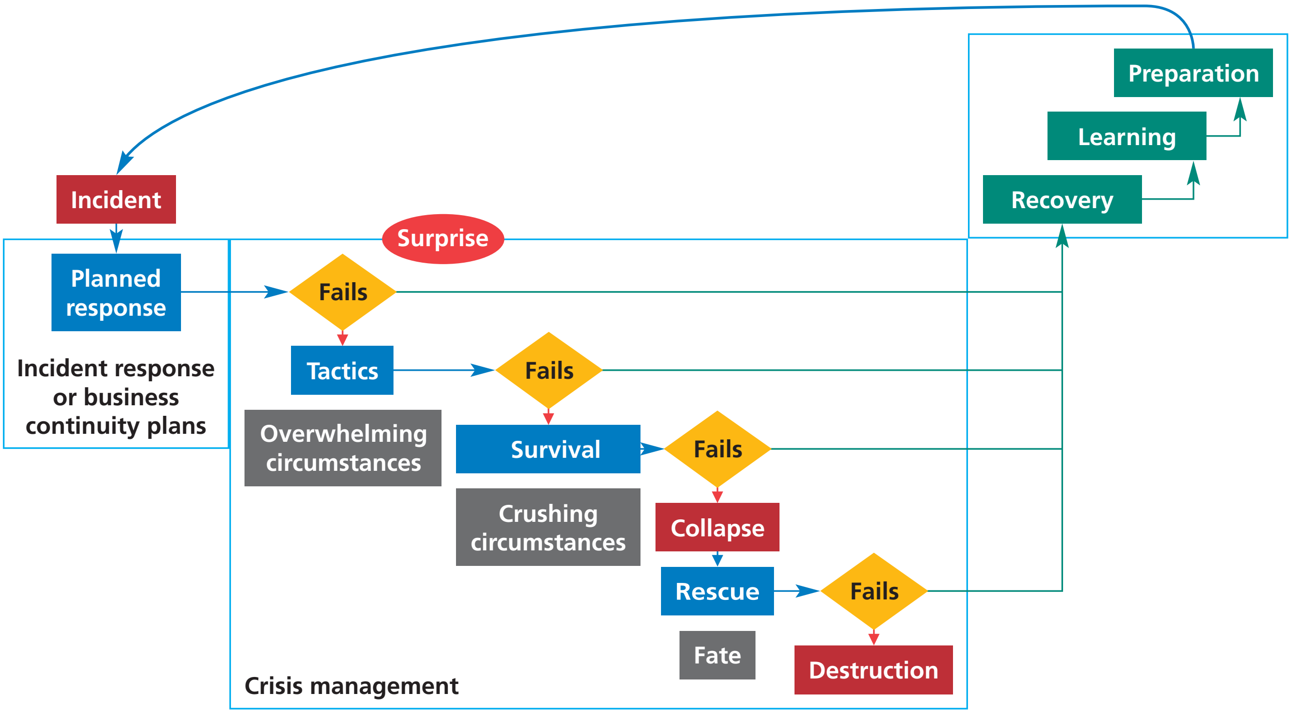


Figure 11: The Collapse Ladder

As long as the organisation controls the course of events, through its business continuity plans for instance, the organisation's "level of collapse" is nil, say 0.

Should it lose control of the *course of events* because it is surprised (by some unexpected combination of events, typically an emergency situation), the organisation's crisis manager must find ways to "navigate" through and around circumstances in order to keep the organisation performing missions and resisting their destructive pressures, and its level of collapse would be measured as 1.

If it is overwhelmed by circumstances and loses its grip on its own *course of action*, the organisation, whose vital functions are still intact but its margins of manoeuvre reduced to virtually nothing, can only place itself in a position of survival and wait for the storm to pass. Its collapse level would then be 2.

But then, if surviving reveals to be difficult and the organisation nearly loses its *vital functions*, like a body whose breath or blood circulation falls to a dangerous minimum, and cannot anymore act, it has to be rescued from the outside. Its level of collapse reaches 3.

Fate can, at that point, be totally adverse, rescue may itself fail, and the organisation is swept away and destroyed. Collapse is total, at level 4.

Response plans change from one level to the next below:

- **Level 0** requires ***Incident Response Procedures***, or in the worst of cases ***Business / System Continuity Plans*** addressing business processes for ICT and other technical systems.
- **Level 1** requires ***Crisis Management Arrangements***, encompassing Tactical Reasoning Guidelines and a number of Emergency response arrangements elaborated in "peace times".
- **Level 2** requires ***Business / Process Survival Plans***, which take account of the fact that margins of manoeuvre are reduced to a very minimum.
- **Level 3** requires ***Business / Process Rescue Plans***, designed for those external operators who are called in to save the agonising organisation or systems.
- There is no plan for **level 4**, except for the sheer liquidation of the organisation.
- The **Recovery Stage** requires itself specific arrangements.
- Similarly the **Learning** and **Preparation** stages, which fully fall into the realm of Emergency Preparation, require arrangements of another type.

Each level, in a given context, can be characterised by **indicators** useful for a crisis manager to assess the level of collapse reached (i.e. to maintain a satisfactory level of situation awareness and capacity to make informed tactical decisions), and therefore to trigger the appropriate type of response arrangements:

- On level 0, all systems, agents and relations between any of them works fine
- On level 1, typically some systems or organisational units stop functioning
- Below, more and more key systems and units are disrupted or come to a halt.

6.1.5 Emergency Preparation

An organisation shall define:

- **Emergency Preparedness** as the state of development of, and readiness to respond to each potential level of collapse of a telecommunication infrastructure.
- **Emergency Preparation** as the process leading to emergency preparedness, which builds on the lessons learned from the experience of real emergencies and milder incidents, and from exercises; its goal is to continuously improve **Emergency Response Measures**.

A basic Emergency Preparation framework is presented in Annex B.

6.2 Planning for Resilience

The resilience of a service should be agreed at the service definition stage of its delivery project. This should lay out the foundation for a Service Level Agreement (SLA) which will state the requirements for the successful provision and ongoing operation of the service.

A number of organisations use the Platinum/Gold/Silver/Bronze model, in which such key attributes as availability, grade of service and quality of service are agreed and documented before any solution design takes place.

This has an added benefit in that organisations who wish to differentiate levels of service (e.g. residential versus Corporate customer accounts) may wish to do so using availability as a metric, and allows those customers who require a higher grade of service to purchase that at a premium.

However, there some areas where a universal level of service is expected – for example it is not only a general expectation, but also a mandatory requirement that the general public have unrestricted access to the Emergency Services access number 112 (and 999 in the UK). On the other hand, an organisation may wish to allow general access to a service during normal business hours while permitting out-of-hours access just to premium customers. These factors must be considered when designing and planning the end-to-end service, and the level of resilience that the service must provide will be a key component of that decision-making process.

6.3 Response to Service-Affecting (or Potentially Service-Affecting) Incidents

While it is vital that the appropriate level of resilience is planned into a service, it is equally important that there are plans in place to ensure that the resilience works in practice and that the organisation providing the service can continue to do so successfully under failure conditions.

Equally important is the way in which an organisation responds to a service-affecting (or a potentially service-affecting) incident, as the automatic response mechanisms which allow continuity of service may only allow for a certain degree of failure – a second or subsequent failure of the same or a similar type could well have a real impact on service, and the organisation must have plans both for resumption to normal operations and have defined, documented and tested incident response processes to ensure swift and effective recovery.

6.4 Basic Technical Measures

In general measures should be presented in line with the risk treatment approach outlined in 5.5.3.

There is a tendency to think that avoiding single points of failure (the N-1 scenario) is the solution to providing resilient service, but this may in fact fall well short of the mark. In order to provide a fully resilient end-to-end service, network designers and planners should examine the ‘N-2’scenario in which one failure follows another. However, to implement a network design based on this approach would probably be overly expensive, and so a risk-based approach is suggested in which the likelihood of failure is assessed (or measured) for each element of the proposed network, and the design is adjusted to provide resilience for N-2 situations where the risk is greater, leaving resilience at N-1 levels where the risk is less severe.

NOTE: Alternative approaches centred on "critical points of disruption" have been discussed and may be further developed within industry to develop resilient systems.

To ensure overall resilience of telecommunication infrastructures and services, a number of technical measures have to be taken, as early as design time. Some of them are reminded below.

6.4.1 Network Elements

Hardware failure – most ‘carrier-class’ equipment is designed to operate at no less that 99.999% (five nines) availability.

Overall, the objective in design of ‘core’ networks must be to avoid single points of failure. However, there is a view that the subsequent failure of a second (similar) element is a case that should also be considered and this is sometimes referred to as the N-2 scenario. While redundancy of a single element might be considered to provide ‘Standard’ resilience, the redundancy required to cover the N-2 scenario might be considered to be ‘Premium’ resilience. The decision as to which level should be selected is of course for the service provider to determine, and must be balanced against the criticality of the service and the cost of providing such a high level of resilience.

Elements within the core network should always have both a high level of internal redundancy (e.g. active and standby central processing elements with automatic failover), as well as there being multiple elements at each key location so that there is always sufficient switching or routing capability to carry traffic in the event of failure. Further to this, good practice also dictates that the building infrastructure should also not present a single point of failure, and therefore no network design should rely on all the equipment (however resilient) being in one physical location.

Beyond the core, in the part of the network sometimes referred to as the 'access' network, the objective should still be to ensure there are no single points of failure as far as possible. However, it is recognised that at some point this becomes impractical from both an economic and complexity point of view, and the extremities of the network may well contain single points of failure, the loss of which would impact a relatively small number of customers.

The key point here is that the further away from the core of the network, the greater the risk appetite, and network providers must make an objective decision about the threshold at which they are willing to accept the risk of failure rather than to mitigate it – the suggested levels of resilience is shown in Figure 12 below.

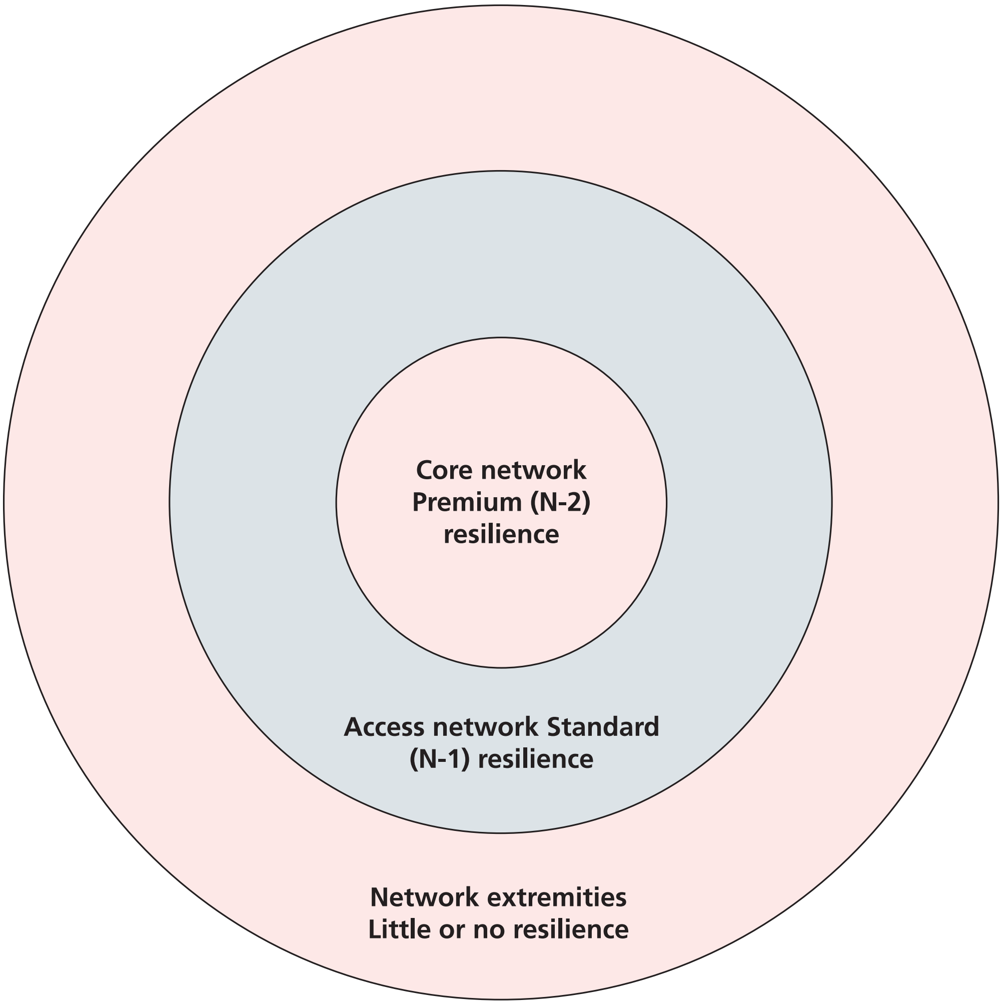


Figure 12: Resilience levels shown increasing towards the network core

Testing – hardware failures can be reduced by employing a robust testing and change management environment. All new hardware should be tested in three distinct ways — firstly at a system or element level in which the functional characteristics of the new hardware are verified in a stand-alone environment, and secondly in a wider (but controlled) environment which includes other interconnected network elements. This second area of testing ensure that there is compatibility between both similar and dissimilar network elements and may include elements of the similar kind. The final area of testing is the introduction of one element only of the new hardware into the main network. Only after a successful period of trouble-free operation can the hardware then be rolled out across the remainder of the network.

Change management is also vital in ensuring that rogue hardware does not enter the main network and cause failures. The change management process must ensure that both of the first two areas of testing have been carried out prior to deployment in the live network. There must be provision within the change management process for a graceful back out in the event that the installation itself fails, or that service-affecting incidents arise following such introduction.

6.4.2 Software and Firmware Failure

Mature software development process is the first step in preventing software or firmware failure. Key elements of an effective process / governance system include:

- Formal requirements definition, review, and management
- Formal design review and sign-off process
- Software development employing tools and controls that provide traceability of changes, integrate code review, and implement automated checks for common failure sources
- Testing and verification at multiple stages in the development process
- Deployment and support process that provides means to minimize impacts of faults and distribute patches and updates in an efficient manner

Once software or software updates are distributed to production environment similar formal process must be applied to field testing the software, staged deployment, and back-out planning.

Testing – software failures can be reduced by employing a robust testing and change management environment. All new software and firmware should be tested in three distinct ways – firstly at a system or element level in which the functional characteristics of the new revision or release are verified in a stand-alone environment, and secondly in a wider (but controlled) environment which includes other interconnected network elements. This second area of testing ensure that there is compatibility between both similar and dissimilar network elements and may include elements of the same kind which are at a lower revision or release level. The final area of testing is the introduction of the new revision or release into the main network on one element only. Only after a successful period of trouble-free operation can the release then be rolled out across other network elements.

As with network elements themselves, change management is the other major part of ensuring that rogue software does not enter the main network and cause failures. The change management process must ensure that both of the first two areas of testing have been carried out prior to deployment on a single element in the live network. There must be provision within the change management process for a graceful back out in the event that the installation itself fails, or that service-affecting incidents arise following such introduction.

Furthermore if appropriate, network operators and service providers should deploy security and reliability related software updates (e.g., patches, maintenance releases, dot releases) when available between major software releases. Prior to deployment, appropriate testing should be conducted to ensure that such software updates are ready for deployment in live networks. Equipment Suppliers should include such software updates in the next generic release and relevant previous generic releases.

6.4.3 Configuration

The correct configuration of network elements is a key factor in ensuring that network operations are maintained in a stable manner. In general, the configuration data is supplied by the design and planning teams and should be in a format which allows the data builders to create simple script files which are run at pre-determined times – usually out-of-hours.

The implication of this is three-fold:

- The configuration data itself must have a high degree of confidence – the design and planning teams must check carefully the data supplied against other 'standard' builds, and ensure that it aligns with data used in the testing environment.
- The data builders must ensure that all data is check carefully once it has been transferred to script form to ensure that there are no fundamental data entry errors, and that each change script has a matching back-out script which can be run in the event of problems with the change and which are not easily corrected at run time.
- Change management must validate the change request, ensure that there is a suitable back-out script, and monitor running of the change to ensure that it takes place within the allotted change window and that it is deemed to have been successful.

Implementation of a high availability network requires consideration of the following issues:

Definition and measurement of availability;

Fault management and diagnosis – it assists in preventing the same type of failures, however it requires a well-instrumented network in order to prepare e.g. event correlation;

Device-level hardware reliability – fault tolerance is a key factor to minimize hardware influence on the overall failure rate. The level of fault tolerance of devices should be suited to the availability metric related to network hardware;

Operational best practices – they are applied to both hardware, software and auxiliary equipment because they can reduce the overall failure rate;

Network-level redundancy – designer's attention to the network-level redundancy should be focused where it can have the greatest impact on the overall availability metric;

Network design and tuning – it can maximize the resiliency and availability of network devices;

Load balancing across redundant network devices – it is important because load sharing can reduce cost of dual network elements and redundant links;

Server fault tolerance – it is crucial for service availability.

6.4.4 Electronic Attack

Malicious attacks on network infrastructure can take place both from outside the organisation, but equally from within. For this reason, it is vital that security controls on staff are both rigorous and appropriate.

Staff with legitimate access to network elements (e.g. for configuration, monitoring or fault resolution purposes) should have clearly defined access rights that allow them to perform their role, but nothing besides. Access rights management should be carried out by a separate team within the organisation, thus allowing proper segregation of duties. All attempts to access network elements (successful as well as unsuccessful) should be recorded for audit purposes, and the audit trails should be reviewed periodically.

In order to reduce the likelihood of external attacks, additional security safeguards in the form of firewalls should be placed between the Internet and the internal network infrastructure – in many cases network operators deploy two sets of firewalls, one between the Internet and a so-called De-Militarised Zone (DMZ), and another between the DMZ and the main network infrastructure. This approach permits a more secure access to the main network infrastructure by staff and systems that are remote from it.

Furthermore network operators, service providers as well as equipment suppliers should carefully control and monitor the network availability of sensitive security information for critical infrastructure by:

periodic review public and internal website, file storage sites HTTP and FTP sites contents for strategic network information including but not limited to critical site locations, access codes;

documenting sanitizing processes and procedures required before uploading onto public internet or FTP site.

6.4.5 Network Synchronisation and Timing

A critical feature of networks is the requirement to ensure that they are synchronised with one another. Failures in synchronisation result in a poor quality of service, and in extreme situations can result in lost voice calls and multiple re-transmission attempts for data.

The timing signals which allow networks to synchronise can be provided in two ways – firstly by providing a reliable timing source for the network equipment to use (e.g. the 2 MHz. signal recovered from the Global Positioning by Satellite System (GPS) or a known ground-based Stratum 1 clock which is then used to provide timing into the transmitted data stream), or secondly by recovering the timing from the received data stream.

In either case, the reliability of this timing signal must be extremely high – accurate to at least one part in 1011, and the entire network must be configured to ensure that the timing across all network elements is consistent, otherwise the network will suffer from ‘clock-slip’ which will result in the type of service degradations referred to above. It is also important to avoid the risk of clock ‘loops’, in which a network element recovers its timing signal from received data and uses this to provide timing to the transmitted data, while the network element at the other end of the link does exactly the same.

Network timing should always have reliable secondary and tertiary clocking sources in addition to a reliable primary source.

6.4.6 Theft and Vandalism

While the threat of theft and vandalism cannot be controlled, it should be possible both to reduce the likelihood by reducing vulnerabilities. Good physical security is the first step in this process (see later section), but other factors can assist in reducing the vulnerability of an equipment site or data centre.

Removing corporate identification from the building itself means that its nature and purpose may be less obvious to casual inspection.

Ensuring that staff do not wear building passes outside the premises will have a similar effect, and security warning notices to both staff and visitors will encourage this practice.

Company literature and promotional material should not reflect the location of critical network equipment sites and data centres.

6.4.7 Network Interconnections

As with network elements, the resilience of network interconnections must be commensurate with the level of risk, so those interconnections within and between core network elements must always be highly resilient. This implies not only that multiple transmission circuits are provided, but also that the physical routing of circuits between network elements is both diverse and separate. Both cable faults and cable theft and vandalism are catered for by employing diversity and separacy.

By ‘diverse’ we mean that the circuits travel between their end points by totally different physical routes, and by ‘separate’ we mean that they do not converge at any point (except the end points) by a fixed distance. 30 metres is often taken to be a suitable separation between circuits, but network providers should make their own judgement as to what is acceptable – again from the perspective of risk.

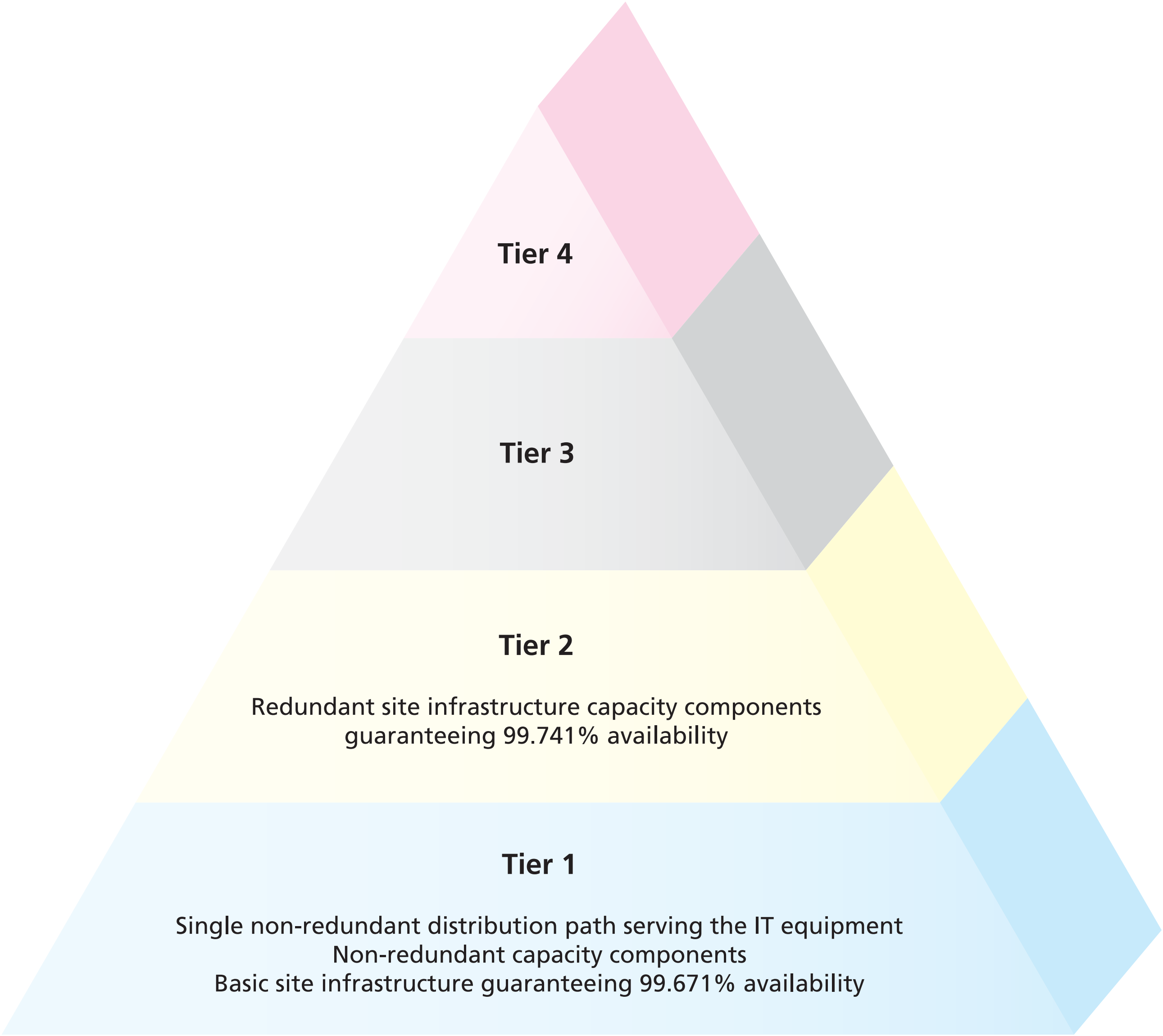
This need was highlighted in the UK in 2004, when a fire occurred in a cable tunnel beneath Manchester. Most of the circuits were provided over resilient cables (both copper and fibre optic), but separation was provided by running the cables down opposite sides of the tunnel. When the fire broke out, both sets of cables were damaged.

It is clear also that any regeneration equipment used in network interconnections must follow the principles described in the ‘network elements’ section above.

Summarizing network operators, service providers and equipment suppliers should implement minimum network management controls in order to promote reliability of the interconnected network

6.4.8 Supporting Infrastructure

Standards already exist for the resilience of data centres, which define the data centre’s ability to withstand disruptive events. While the standards specifically refer to data centres, other types of equipment location such as networking equipment sites can use the same principles to define their capability. Such data centres can be classified in the following way:


Tier 4
Tier 3
Tier 2
Redundant site infrastructure capacity components
guaranteeing 99.741% availability
Tier 1
Single non-redundant distribution path serving the IT equipment
Non-redundant capacity components
Basic site infrastructure guaranteeing 99.671% availability

NOTE: Each succeeding tier encapsulates the requirements of the preceding tier

Tier 3: Multiple independent distribution paths serving the IT equipment
All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture
Concurrently maintainable site infrastructure guaranteeing 99.982% availability

Tier 4: All cooling equipment is independently dual-powered, including chillers and Heating, Ventilating and Air Conditioning (HVAC) systems
Fault tolerant site infrastructure with electrical power storage and distribution facilities guaranteeing 99.995% availability

Figure 13: Classification scheme for data centres
(from The Uptime Institute (http://www.uptimeinstitute.org) [Uptime])

All aspects of a data centre's capability are defined in a number of similar standards:

The Telecommunications Infrastructure Standard for Data Centers TIA-942 which deals with all aspects of data centre provision

Information technology — Generic cabling systems for data centres ISO/IEC 24764:2010 which, as the title suggests applies to the internal structured cabling systems

Information technology. Generic cabling systems. Data centres BS EN 50173-5:2007 which also, as the title suggests applies to the internal structured cabling systems.

6.4.9 Building and Compound Security

The equipment housed in a building – be it a data centre or network equipment site has two distinct areas of value – the first is inherent in the equipment itself – this has already been discussed earlier, and secondly in the value of the services it provides.

It is vital then that the equipment is protected from external intrusion, and the following recommendations will form part of an overall building security plan:

Equipment sites and data centres should preferably be located in areas where there is little or no risk of damage by natural hazards, e.g. flood, earthquake, landslip, etc.

Equipment sites and data centres should preferably be located in areas where crime rates are low

Planting in garden areas outside equipment sites and data centres should be properly maintained

An external perimeter palisade fence which will deter most vandals and thieves

Electronically-controlled external access gates which form part of the perimeter defence – one or more will be required for access by staff, while another somewhat larger gate will be required for equipment deliveries

Electronically- controlled external access doors into the building itself – again, one or more will be required for access by staff, while another somewhat larger gate will be required for equipment deliveries

Solid external wall construction, with a corridor between the external walls and the internal structure

A robust internal structure which houses the data centre or network equipment site systems

Provision for standby generation and fuel storage – usually in a separate external compound within the outer perimeter, but occasionally on an upper floor of the building

Provision for power switching, UPS systems (usually outside the main equipment areas) and power distribution (usually within the main equipment areas)

Provision for telecommunications cable access – invariably using at least two points of entry at opposite sides of the building, and taking separate routes back to their source (see Sec. 6.4.7 Network Interconnections above)

Provision of suitable cooling systems (see later Section 6.4.11). The main chilling units will generally be located inside or just outside the main equipment space, while condensing units will normally be located in a separate external compound within the outer perimeter, but occasionally on an upper floor of the building

A resilient electronic access control system that can permit or deny access to all areas of the site. This will also include voice communication capability with the security guard so that authorised visitors can be admitted. Such a system must be provided with a resilient power supply. Details of personnel using the access system should be recorded by the system itself

A Closed-Circuit Television (CCTV) surveillance capability with cameras able to view all external parts of the site including gates into the perimeter and doors into the building itself. Cameras may be fixed for those locations that can be adequately covered by them, or Pan, Tilt and Zoom (PTZ) cameras where more detailed monitoring is required. The recording and monitoring systems connected to the cameras may be sufficiently sophisticated to permit recording of abnormal events while not recording when nothing moves within a defined zone. Recording tapes or computer files should be kept as long as feasible, but not less than 31 days. Such a system must be provided with a resilient power supply.

Access to data centers or other sensitive rooms should be secured with electronic and construction solutions, including authentication methods. Interior controls include: doors (e.g. double doors lets avoid piggybacking), windows, security guards, walls, locks and access control. The last control can be based on:

something you know (password, PIN number),

something you have (USB token, smart cards, magnetic strip cards),

something you are (different biometric systems: palm scan, hand geometry, iris recognition, retina pattern, fingerprint, facial scan or voice recognition).

6.4.10 Power

It is fairly obvious that without power, networks cannot function at all. However, there are seven other types of power-related issue which can cause problems with both network and IT equipment, and which need to be addressed:

Power failure: defined as a total loss of input voltage.

Surge: defined as a momentary or sustained increase in the mains voltage.

Sag: defined as a momentary or sustained reduction in input voltage.

Spike: defined as a brief high voltage excursion.

Noise: defined as a high frequency transient or oscillation, usually injected into the line by nearby equipment.

Frequency instability: defined as temporary changes in the mains frequency.

Harmonic distortion: defined as a departure from the ideal sinusoidal waveform expected on the line.

Most equipment at the network's core is designed to operate on direct current power supplies, where the power system cleans up the incoming mains supply and provides a constant -48 volts to the equipment, usually with a battery back-up which will maintain power during a power failure.

More recently however, and especially in the case of data centre equipment (servers, etc.) the equipment is mains-powered, and some form of Uninterruptible Power Supply (UPS) will be necessary in order to carry out this process. A UPS may come in a number of forms, but generally will have the ability to maintain both alternating and direct current supplies to equipment with the option of standby generation in the event of incoming mains failure.

Standby generation should always be provided to power at least the demand of a full network equipment centre or data centre (with suitable headroom for expansion), and may optionally introduce N+1 or N+2 capability to ensure that the failure of one or more generators does not affect service.

Likewise, stores of fuel (normally diesel, but occasionally Liquid Propane Gas called also LPG) should also be provided in suitably secure areas, as diesel especially is attractive to thieves. Arrangements should also be in place with fuel suppliers to provide replenishment of stocks at short notice.

Network operators should provide back-up power (e.g., some combination of batteries, generator, fuel cells) at cell sites and remote equipment locations, consistent with the site-specific constraints, criticality of the site, the expected load and reliability of primary power. They ought to ensure that fuses and breakers meet quality Level III reliability per Technical Reference (SR-332), Reliability Prediction Procedure for Electronic Equipment.

Network planning should also consider placing all power and network equipment in a location to increase reliability in case of disaster (e.g., floods, broken water mains, fuel spillage). In storm surge areas, consider placing all power related equipment above the highest predicted or recorded storm surge levels. The use of networked electronic access control systems that apply appropriate security and reliability principles for critical systems (e.g., cyber security) should also be considered.

6.4.11 Cooling

All equipment generates heat when operational, and in order to ensure the correct operation of the equipment, this must be maintained within recommended limits. There are a number of ways in which this can be achieved.

The most common is by the use of forced-air cooling in which air chilled to a low temperature is blown into equipment areas (often through holes cut specifically beneath racks in a raised floor environment), and the warm air is extracted and passed through air handling units which chill and recycle the air.

An alternative method, often used in mainframe computer environments is by the use of water or chemical (such as Freon) cooling, which is more efficient, but also more costly. As server blade densities are increasing, this method is becoming more widely accepted for servers and network equipment areas.

In either case, it is vital that the cooling equipment itself is also powered by resilient power systems, and that the N+1 or N+2 capability is exploited to ensure that the failure of a single cooling unit does not cause service failure. For example in the 1+1 configuration it is allowed that the redundant cooling unit has a lower cooling power that ensures to keep temperature acceptable low but higher than recommended one. In an alternative approach only sum of cooling powers of both units can provide recommended temperature. If one of the units breaks down, the other can handle only accepted but higher range of cooling temperatures.

6.4.12 Electronic Systems Security

In addition to the electronic access control system that permits or denies entry to areas of the building, attention should be paid to system access control. Personnel authorised to connect into systems, servers and network equipment must be properly authorised to do so, their accesses should be monitored and passwords should be required to be changed on a regular basis.

Root access to systems should be disabled, and where details of root access passwords are required to be kept on site, there should be in a secure location such as a fire safe.

Network operators, service providers and equipment suppliers should also ensure that staff is given awareness training on security policies, standards, procedures, and general best practices. Moreover awareness training should cover the threats to the confidentiality, integrity, and availability of data including social engineering. Training as part of new employee orientation should be supplemented with regular refreshers to all staff.

6.4.13 Network Monitoring and Management

All network equipment and systems should be linked to suitable network monitoring systems that will permit alarm generation on failure or when conditions go outside those parameters set. Where possible, network equipment and systems should be able to be configured remotely, which will reduce the need for visits within the equipment site or data centre itself.

Network monitoring and management centres should themselves be resilient to failure by having two geographically separate locations, preferably up to Tier 2 standard.

6.4.14 Network Demand

Network demand increases in two distinct ways – organically, as more customers use the service or use more services, and in peaks, when sudden and usually unexpected events cause a surge in use. If these are not considered, services can be seriously affected, both in their ability to permit new connections, and in their ability to handle the volume of traffic in progress – congestion.

Good practice dictates that network and service planners should take both of these into account, and should include a pre-determined level of headroom into all connectivity and service capability.

6.4.15 Fire and Water Detection and Fire Control Systems

Two major threats that can have a serious impact on network equipment sites and data centres are flooding (or at least water leakage from cooling systems) and fire. Either can render the equipment – and occasionally the building itself – completely useless, and so both should be continuously monitored and managed.

Water ingress or leakage can be detected by installing sensor wires beneath raised flooring systems, causing an alarm to be generated, or on more sophisticated systems, allowing the exact location to be pin-pointed.

Fire detection systems have long been available, the most effective being known as VESDA® or Very Early-warning Smoke Detection Apparatus, in which the atmosphere below raised flooring and at ceiling height is sampled for the presence of smoke particles, and an alarm is generated if two or more detectors are triggered.

Four types of sprinkler systems can be identified:

dry pipe — there is no standing water

wet pipe — system is ready to be activated

preaction — it is a combination of two systems above

deluge — a large volume of water is released after triggering.

VESDA systems are generally linked to a system of extinguishing chemical that will deprive the affected area of oxygen by lowering its relative proportion in the atmosphere to less than 15%, below which combustion cannot take place. A number of gases are currently commercially available, such as Argonite® and Inergen®.

Furthermore network operators, service providers and equipment suppliers should use cables with adequate reliability and cable signal integrity. Such properties as flammability, strain relief and signal loss should be considered. If non-standard cables are used because of an emergency restoration, they should be marked as temporary and should be replaced with standard cables as soon as practical.

Summarizing network planning process should identify essential staff within their organizations that are critical to disaster recovery efforts. Planning should address the availability of these individuals and provide for backup staff.

6.4.16 General Housekeeping Recommendations

Recommendations can be defined as:

Equipment cabinets should be kept locked at all times except when engineering personnel are carrying out legitimate work within them

Equipment areas should be kept clean and tidy – free of surplus equipment and packaging (which can also be a fire hazard)

Security policies should be set up and regularly reviewed, especially with regard to the admittance of visitors.

6.5 Measuring Resilience

Annex C provides some tips that can help the reader to create metrix aimed at measuring various dimensions of telecom systems' resilience and dependability.

Work is still in progress at the ENISA at the present time on this topic.

Annex A: References

[AK02] A. Autenrieth, A. Kirstädter, "Engineering End-to-end IP Resilience using Resilience- Differentiated QoS", IEEE Communications Magazine, Vol. 40, No. 1, January 2002

[AQ07] Syed Zubair Ahmad, Mohammad Abdul Qadir, "Terminal Mobility Services in the Middleware Environment", IEEE/ACS International Conference on Computer Systems and Applications, pp. 332-335, 2007

[Ari09] Cloud Networking Whitepaper, Arista, 2009

[CFL10] Carlo Caini, Rosario Firrincieli and Marco Livini, "DTN Bundle Layer over TCP: Retransmission Algorithms in the Presence of Channel Disruptions", Journal of Communications, Vol. 5, No. 2, February 2010

[Cisco06] Cisco Data Center Network Architecture and Solutions Overview, 2006

[Clo09] Up, Out, Centralized, and Decentralized, Cloudscaling, 2009

[DHNH03] Stefan Dulman, Lodewijk v. Hoesel, Tim Nieberg, Paul Havinga, "Collaborative communication protocols for wireless sensor networks", 2003

[Do03] Song Dong, "Resilience Provisioning Mechanisms for IP-Centric Optical Networks", Department of Electronic Engineering, Queen Mary University of London, November 2003

[Do99] B. T. Doshi, "Optical Network Design and Restoration", Bell Labs Tech. J., pp. 58- 84, 1999.

[Fa02] Kevin Fall, "A Message-Switched Architecture for Challenged Internets", Intel, 2002

[Fa03] Kevin Fall, "A Delay-Tolerant Network Architecture for Challenged Internets", Intel, 2003

[FW03] "Delay-Tolerant Networks (DTNs)", Forrest Warthman, 2003

[Gi08] Nicola Giulli, "Control Plane capabilities and challenges for NGN and Grids", TNC, 2008

[GMKL09] Henryk Gierszal, Joanna Modławska, Dominik Kasprzak, Krzysztof Liszy ski, Tomasz Pia cik, "Algorithms for Designing of Optimized Fixed Broadband Networks", Mathematica Balkanica, New Series, Vol. 23, 2009, Fasc. 3 4, pp. 249 270

[Had10] Stephen Haddock, "Resilient Network Interconnect using Distributed Link Aggregation", IEEE 802, 2010

[HJB06] Huang He, Wang Jin, Yang Bo, "Multi-Class MPLS Resilience Mechanism Supporting Traffic Engineering", Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), 2006

[IG00] R. Iraschko, W. Grover, "A Highly Efficient Path-Restoration Protocol for Management of Optical Network Transport Integrity", IEEE J. Sel. Areas Comm., Vol. 18, pp. 779-794, 2000

[Jo07] Rajive Joshi, "Data-Oriented Architecture: A Loosely-Coupled Real-Time SOA", Real-Time Innovations, 2007

[KKY03] D. Katz, K. Kompella, D. Yeung, "Traffic engineering (TE) extensions to OSPF version 2", RFC 3630, 2003

[KL00] M. Kodialam, T. V. Lakshman, "Dynamic Routing of Bandwidth Guaranteed Tunnels with Restoration", in Proceeding of IEEE conference on Computer Communication, pp. 902-911, 2000

[LHSS08] Michele N. Lima, Helber W. da Silva, Aldri L. dos Santos, Guy Pujolle, "An Architecture for Survivable Mesh Networking", IEEE GLOBECOM proceedings, 2008

[LKLK07] Choonhwa Lee, Sunghoon Ko, Seungjae Lee, Wonjun Lee, Sumi Helal, "Context-Aware Service Composition for Mobile Network Environments", J. Indulska et al. (Eds.), Springer, pp. 941-952, 2007

[McCL99] Rolf McClellan and Nick Lippis, "Network-Level Redundancy/Resilience for High-Availability Campus LANs with Cisco Systems' Catalyst Family of Switches", ZDTag, 1999

[McG09] Eileen McGrath, "3GPP2 Vision for 2009 and Beyond, 3GPP2", April 2009

[NRIC] NRIC.org

[Pho08] "Resilient Grid Networks", Phosphorus, 2008

[ResNet] ResiliNets Wiki: wiki.ittc.ku.edu/resilinets

[RM99] S. Ramamurthy, B. Mukherjee, "Survivable WDM Mesh Networks, Part II-Restoration", in Proceeding of IEEE Conference on Communications, pp. 2023-2030, 1999

[RM99b] S. Ramamurthy, B. Mukherjee, "Survivable WDM Mesh Networks, Part I – Protection", in Proceedings of IEEE Conference on Computer and Communication Societies, pp. 744-751, 1999

[RX06] Duncan Russell, Jie Xu, University of Leeds "Service Oriented Architecture For Network Enabled Capability", School of Computing, 2006

[SL04] H. Smit, T. Li, "ISIS extensions for traffic engineering", RFC3784, 2004

[SLRJ07] Andrzej Szymanski, Artur Lason, Jacek Rzasa, and Andrzej Jajszczyk, "Grade-of-Service-Based Routing in Optical Networks", IEEE Communications Magazine, February 2007

[Wag04] David Wagner, "Resilient Aggregation in Sensor Networks", ACM, 2004

[ZD02] H. Zhang, A. Durresi, "Differentiated Multi-layer Survivability in IP/WDM Networks", in Proceedings of IEEE/IFIP Symposium on Network Operations and Management, pp. 681–694, 2002

[Zeu09] "Building a Service Oriented Network", Zeus Technology, 2009

[OK10] Eng Hwee Ong, Jamil Y. Khan Cooperative radio resource management framework for future IP-based multiple radio access technologies environment, Computer Networks, Volume 54, Issue 7, 17 May 2010, pp. 1083-1107

[WP05] Haibo Wang and Devendra Prasad, End-2-End QoS Provisioning in UMTS networks, 12 January 2005

[He99] Urs Hengartner, Intserv, Diffserv, RSVP, CMU, 1999

[TP07] Nicolas Tizon, Béatrice Pesquet-Popescu, Content Based QoS Differentiation for Video Streaming in a wireless environment, 15th European Signal Processing Conference (EUSIPCO 2007), Pozna , Poland, September 3-7, 2007

[MBG10] M. Cassasa Mont, A. Baldwin, C. Goh, POWER Prototype: Towards Integrated Policy-Based Management, Frontier Journal, Volume 7, Number 5, May 2010

[RFC2748]. RFC 2748, The Common Open Policy Service (COPS) protocol, www.ietf.org

[RFC3084] RFC 3084, COPS usage for policy provisioning, www.ietf.org

[COPS]. Internet Draft, COPS-PR for outsourcing in UMTS: UMTS Go PIB, www.ietf.org

[GHAM02] V. Gazis, N. Houssos, A. Alonistioti, L. Merakos, Evolving perspectives of 4th generation mobile communication systems, The 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2002

[XC09] Chunsheng Xin, Xiaojun Cao, A cognitive radio network architecture without control channel, Proceedings of the 28th IEEE conference on Global telecommunications, pp. 796-801, 2009

[BT10] Ethernet Resilience, Customer Guide, openreach BT, 2010

[LBHS08] Octavian Lascu, Shawn Bodily, Matti Harvala, Anil K Singh, DoYoung Song, Frans Van Den Berg, IBM AIX Continuous Availability Features, IBM, 2008

[Ba02] Robin Bailey, Service costing for a resilient network business, Analysis Mason, 2002

[GFC02] Gregg Goble, Howard Fields, Richard Cocchiara, Resilient infrastructure: Improving your business resilience, IBM, 2002

[DepEne09] Smart Grid System Report, U.S. Department of Energy, July 2009

[RaRM10] resilienceandriskmanagement.com, 2010

[IBM05] Operational resilience, IBM, 2005

[DNV10] www.dnv.com, 2010

[ASIS10] www.asisonline.org, ASIS International, 2010

[TISN10] Critical Infrastructure Program for Modelling and Analysis, TISN, www.tisn.gov.au, 2010

[AU10] Critical Infrastructure Resilience Strategy, Australian Government, 2010

[Uptime] The Uptime Institute (http://www.uptimeinstitute.org)

[Endsley] Endsley M R (1988) Design and evaluation for situation awareness enhancement. Proceedings of the Human Factors Society 32nd annual meeting. Santa Monica, CA: Human Factors Society, 1988, pp. 97–101

[Klein] Klein G (1997) The Recognition-Primed Decision (RPD) Model: Looking Back, Looking Forward. In Zsambok C E and Klein G A (Eds) Naturalistic Decision Making. Mahwah, New Jersey. Lawrence Erlbaum Associates

[PTH] Theron P. (2009) Resilience, Incident Reporting and Exercises. Measuring Resilience – the Next Challenge. ENISA Quarterly Review Vol. 5, No. 4, December 2009

[BSI25999] BSI 25999: "Part 1, the Code of Practice, provides BCM best practice recommendations. Please note that this is a guidance document only", "Part 2, the Specification, provides the requirements for a Business Continuity Management System (BCMS) based on BCM best practice. This is the part of the standard that you can use to demonstrate compliance via an auditing and certification process."

[ISO22399] ISO/PAS 22399:2007: "Societal security - Guideline for incident preparedness and operational continuity management"

Annex B: The Emergency Preparation Process (EPP)

The **Emergency Preparation Process** (EPP) is a holistic, flexible and all-hazards framework aimed at organising progress in Emergency Preparedness at the EU, Member State and Stakeholder levels of the Telecommunication sector. It is based on three key Pillars:

A **Governance** Pillar: the Emergency Preparedness Governance Model (EPGM)

An **Achievement** Pillar: the Emergency Response Framework (ERFW)

A **Process** Pillar: the Emergency Preparation Framework (EPFW)

NOTE: The Process itself provides only the key principles and measures around which to prepare for Emergencies; it is not linked to any particular type of crises; it is the strategies and plans established under the framework that will address the particular types of emergencies that Member States and Stakeholders will wish to prepare for.

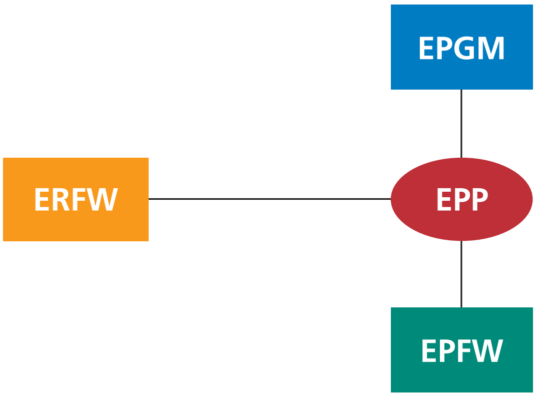


Figure 14: The three Pillars of the EPP

B.1 Three Pillars and Their Elements

Each pillar is composed of **elements** described as follows:

- Its function and structure
- The guidelines that will help to produce it.
- Its key delivery

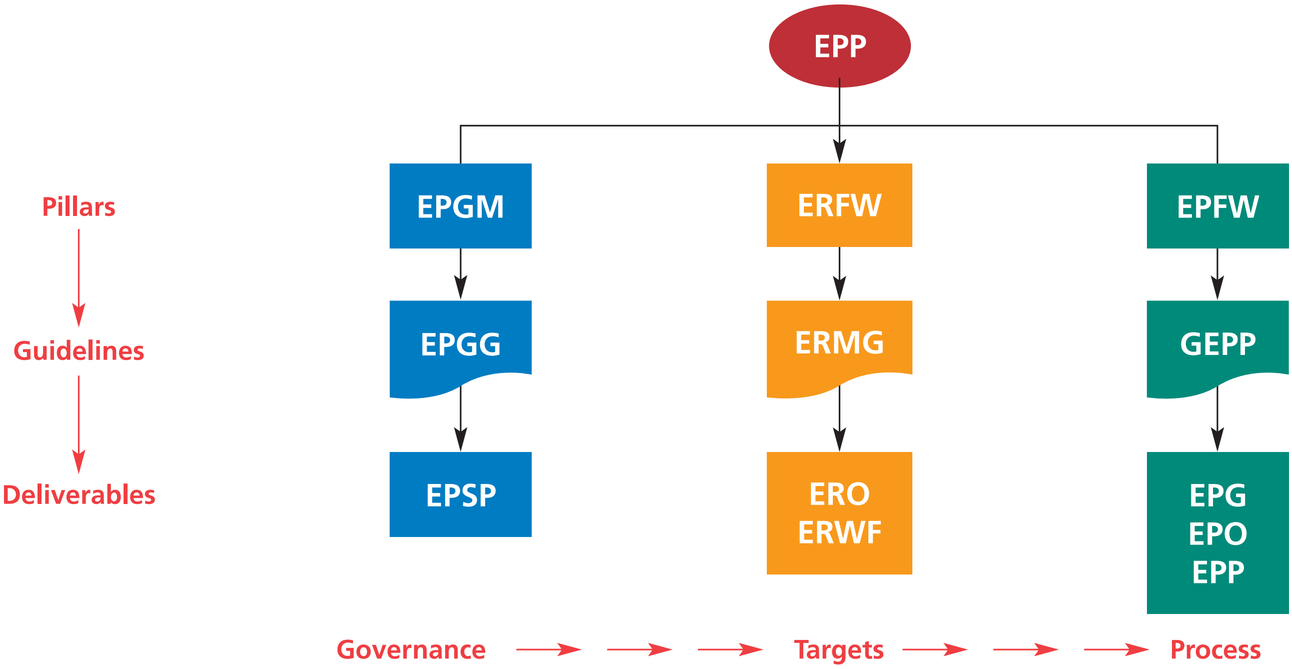


Figure 15: The structure of the 3 Pillars of the Emergency Preparation Process

B.1.1 The Emergency Preparation Governance Model (EPGM)

B.1.1.1 Function and Structure

As the Governance Pillar of the Emergency Preparation Process (EPP), the **Emergency Preparedness Governance Model** (EPGM) is the minimal requirement that will help to define the objectives, priorities and rules organising periodically and smoothly (when needed) the improvement of Emergency Preparedness.

It rests on two elements:

- The periodic definition of an **Emergency Preparation Strategic Plan** (EPSP)
- **Emergency Preparedness Governance Guidelines** (EPGG).

B.1.1.2 Key Delivery

B.1.1.2.1 The Emergency Preparation Strategic Plan (EPSP)

The **Emergency Preparation Strategic Plan** (EPSP) sets the Objectives, Priorities and Rules organising the progress of Emergency Preparedness, periodically, for a given period of time.

B.1.1.3 Guidelines that Will Help to Produce It

Emergency Preparedness Governance Guidelines (EPGG) provide the method to elaborate an Emergency Preparation Strategic Plan.

B.1.2 The Emergency Response Framework (ERFW)

B.1.2.1 Function and structure

As the Achievement Pillar of the Emergency Preparation Process (EPP), the **Emergency Response Framework** (ERFW) is the minimal requirement for a common understanding of Emergency Response arrangements and for their development.

It rests on three elements:

- An **Emergency Response Organisation** (ERO)
- An **Emergency Response Workflow** (ERWF)
- **Emergency Response Methodological Guidelines** (ERMG).

B.1.2.2 Key deliveries

B.1.2.2.1 The Emergency Response Organisation (ERO)

The **Emergency Response Organisation** (ERO) is the set of Phases, Activities and Resilience Capabilities that need to be designed and implemented in advance in order to respond to Emergencies (Emergency Preparedness is the state of development and readiness of these elements).

Emergency Response **Phases** include:

- **Early Warning**: this phase is activated only when early signs of a potential Emergency are perceived; this can be a hurricane alert or weak signals of the preparation of a cyber-attack

- **Response and Mitigation**: this phase is always, a minima, activated as soon as the incident has occurred; its common function is to perform reconnaissance, to rescue and evacuate people and what should be spared, to contain the incident within boundaries as limited as feasible, and to prepare for the next phase

NOTE: It is during these first two phases that organisations and systems may collapse (see the Collapse Ladder in Figure 11).

- **Stabilisation and Continuity**: this phase allows the restoration of some life to the system after conditions have been stabilised and made sustainable for a degraded mode activity

- **Recovery**: this phase is activated once adverse circumstances have passed or are about pass and conditions for resuming activity to its nominal level are met

- **Aftershock**: that phase is the post-crisis follow-up phase, as important and often much longer and sometimes more costly than the previous phases, possibly generating frustration to the point of sparking psychosocial crises.

Emergency Response **Activities** allow response to emerging situations during those **Phases** and include:

- **Situation Awareness** (SA): based on recent work by Endsley [Endsley], they include situation data acquisition, situation interpretation and sharing, and projection of the situation (through simulation and models)

- **Decision-making** (DM): very much studied in tactical command posts [Klein], they include plan drafting and sharing, plan evaluation, plan selection, plan communication, vigilance setting

- **Action** (AC): that is the execution part of the situation response cycle, in which actors – and activators – do and report on what they do, and actors or sensors alarm command posts on changes in the situation.

B.1.2.2.2 The Emergency Response Workflow (ERWF)

The **Emergency Response Workflow** (ERWF) is the cooperative process and information system needed within the Emergency Response Organisation to cooperate in crisis times. Schematically, an Emergency response Workflow usually includes the following elements:

- **Alarm and mobilisation procedures**: to take early warnings or sudden signs of an incident into account, to pass the alarm on to systems or people in charge, to evaluate the situation and confirm an Emergency situation, to mobilise teams, systems and logistic resources needed to handle the Emergency
- **Emergency response procedures**: to handle circumstances according to the intensity of the crisis
- **Coordination processes**: to keep actors acting together toward the same plans
- **Data management processes**: to keep records of what is going on
- **Reporting processes**: to keep upper levels of command and other concerned stakeholders informed
- **Debriefing and Lesson Learning processes**: to generate future progress.

B.1.2.3 Guidelines that Will Help to Produce Them

The **Emergency Response Methodological Guidelines** (ERMG) should cover in a consistent manner:

- Explications and recommendations to implement an Emergency Response Organisation
- Explications and recommendations to implement an Emergency Response Workflow.

Such guidelines should be defined within a Forum of the appropriate level (European seems best suited in order to harmonise practices and reach a better shared understanding of the why's and how's of Emergency Preparation).

B.1.3 The Emergency Preparation Framework (EPFW)

B.1.3.1 Function and Structure

As the Process Pillar of the Emergency Preparation Process (EPP), the Emergency Preparation Framework (EPFW) is the minimal requirement for the organisation of Emergency Preparation. It rests on four elements:

- An **Emergency Preparation Organisation** (EPO)
- An **Emergency Preparation Process** (EPP)
- Ad hoc periodic **Emergency Preparation Programmes** (EPG)
- **Guidelines** for the establishment of **Emergency Preparation Programmes** (GEPP).

B.1.3.2 Key Deliveries

B.1.3.2.1 The Emergency Preparation Organisation (EPO)

The **Emergency Preparation Organisation** (EPO) includes the Collaborative Mechanisms needed:

- To develop the governance of Emergency Preparation
- To establish, coordinate and execute Emergency Preparation orientations, plans and actions required
- To share lessons drawn from experience, key pieces of information and good practices.

B.1.3.2.2 The Emergency Preparation Process (EPP)

The **Emergency Preparation Process** (EPP) needed to constantly improve Emergency Preparedness:

- Is based on the principle of a Plan-Do-Check-Act (PDCA) loop
- Should be defined broadly so as to allow Member States and Stakeholders to implement it with consideration for their particular circumstances and level of maturity
- Is in line with current good practices advocated in Business Continuity Standards [BSI29999], [ISO22399]

It is structured around the following Emergency Preparation Activities:

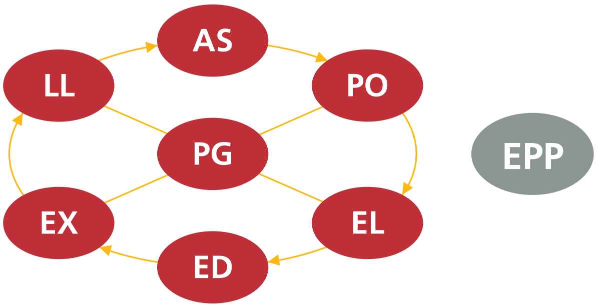


Figure 16: The Emergency Preparation Process

- (Re)**Assessment** (AS): of existing practices vs. reassessed needs, legislation and goals
- **Policy Definition** (PO): rules, priorities and plans framing Emergency Preparation efforts
- **Elaboration** (EL): of both Emergency Response and Emergency Preparation Measures
- **Education and Dissemination** (ED): targetting stakeholders and citizens, and Awareness raising
- **Exercising and Testing** (EX): in-house or multi-organisation tests of systems and plans
- **Lessons Learning** (LL): Feedback from both real crises and exercises, and Monitoring
- **Programme Management** (PG): to keep the Continuous Improvement Cycle in line with needs.

B.1.3.2.3 Emergency Preparation Programmes (EPG)

Ad hoc **Emergency Preparation Programmes** (EPG) should be defined periodically and implemented by each actor concerned as agreed in order to:

- Enhance continuously the Emergency Preparation Organisation and the Emergency Preparation Process themselves
- Develop and enhance Emergency Response Measures needed to respond to Emergencies
- Follow-up the execution of the programme and allow to assess progress made in that respect.

Emergency Preparation Programmes (EPG) should define Emergency Preparation projects to be undertaken by stakeholders or groups of stakeholders, of one or more countries in order to improve either the Emergency Preparation Organisation or Process, or the Emergency Response Organisation or Workflow.

They could also establish Emergency Preparation **KPI's** (Key Performance Indicators) to assess the progress made with regard to the implementation of the Emergency Preparation Plans, Programmes and projects. Those programmes should be defined within the appropriate level of Forum:

- Based on minimal requirements
- In collaboration between stakeholders involved.

B.1.3.3 Guidelines that Will Help to Produce Them

Guidelines for the establishment of **Emergency Preparation Programmes** (GEPP) should cover, in a consistent approach:

- Explications and recommendations to establish Emergency Preparation Programmes
- Explications and recommendations for setting-up an efficient Emergency Preparation Organisation
- Explications and recommendations for running an efficient Emergency Preparation Process
- Explications and recommendations for assessing the progress of the Emergency Preparation Process.

Such guidelines should be defined at the appropriate level of the organisation.

B.2 How Would the Elements of the Concept Work Together?

The general principle that articulates its elements is that **Emergencies** require the preparation of Emergency Response Capabilities / Measures (**Emergency Preparedness**), and their delivery requires in turn **Emergency Preparation** Activities. **Guidelines** help to implement that virtuous circle. The following chart depicts the dynamics of the Concept:

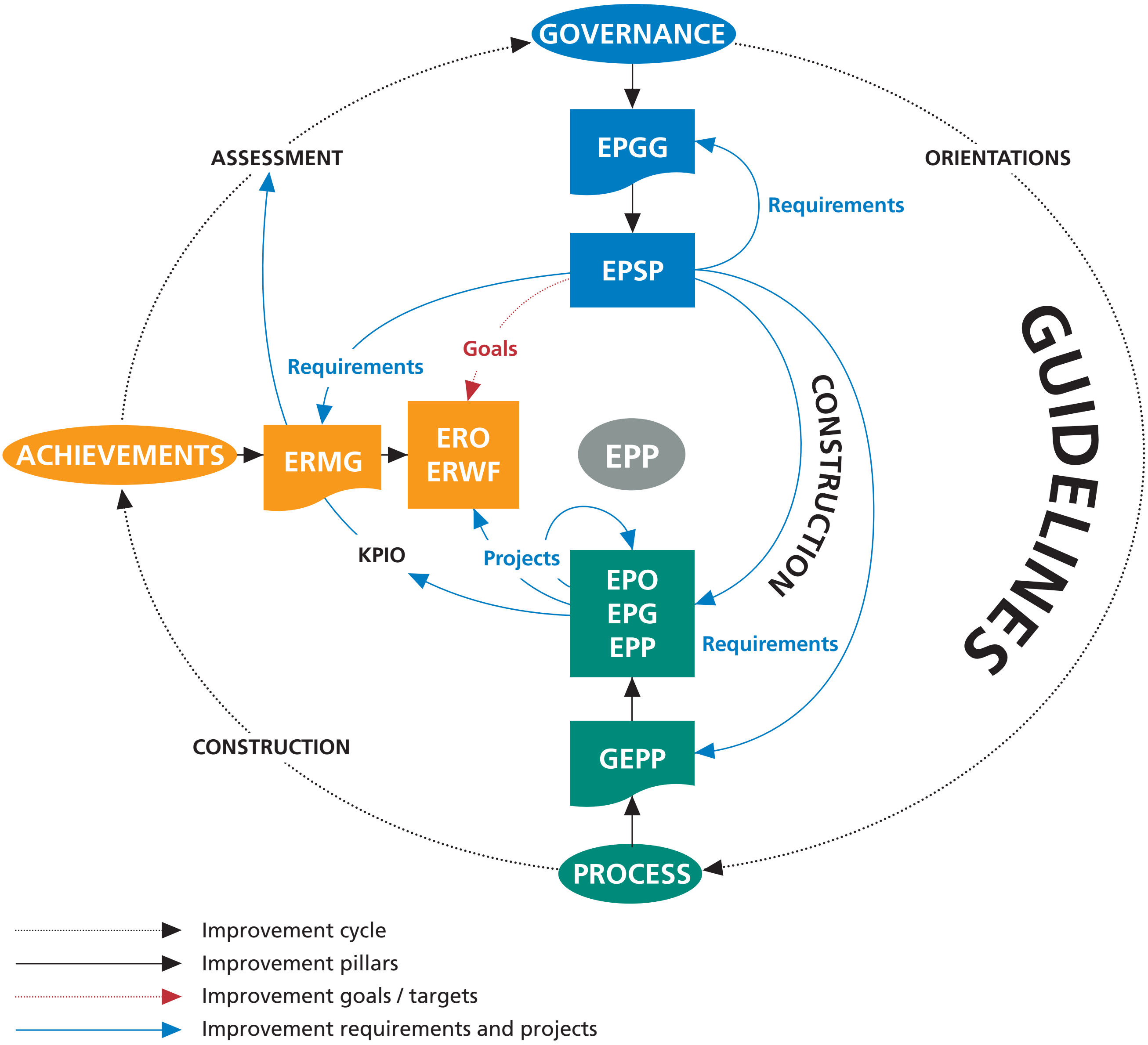


Figure 17: The dynamics of the Emergency Preparation Process

Governance will frame the process according to prior achievements and periodic reassessments. The process will in turn deliver the achievements expected by governance.

Annex C: Abbreviations

3DES	Triple Data Encryption Standard
3G	3rd Generation
AAA	Authentication, Authorisation and Accounting
AES	Advanced Encryption Standard
App	Application
ADSL	Asymmetric Digital Subscriber Loop
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BS	British Standards
CAPEX	Capital Expenditure
CBWFQ	Class-Based Weighted Fair Queuing
CCTV	Closed-Circuit Television
CIA	Confidentiality Integrity Availability
CR-LDP	Constraint-based Routing Label Distribution Protocol
CRN	Cognitive Radio Network
CS	Circuit Switching
COBIT	Control Objectives for Information and related Technology
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off-The-Shelf
CPE	Customer Premises Equipment
DDM	Digital Diagnostic Monitoring
DDoS	Distributed Denial-of-Service
DiffServ	Differentiated Service
DMZ	De-Militarized Zone
DTN	Delay-Tolerant Network
DWDM	Dense Wavelength Division Multiplexing
DWRR	Deficit Weighted Round Robin
e2e	end-to-end
EN	European Standard
ENISA	European Network and Information Security Agency
EMS	Element Management System
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
G2MPLS	Grid General MPLS
GoS	Grade of Service
GPS	Global Positioning System
GSM	Global System for Mobile communication
HFSC	Hierarchical Fair Service Curve
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilating and Air Conditioning
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronic Engineers
IntServ	Integrated Service
IO	Input/Output
IP	Internet Protocol
IPS	Intrusion Prevention System
ISDN	Integrated Service Digital Network
ISO	Organisation Internationale de Normalisation / International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LAN	Local Area Network
LLQ	Low Latency Queuing
LPG	Liquid Petroleum Gas

MAC	Medium Access Control
MANET	Mobile Ad-hoc NETwork
MIMO	Multiple Input Multiple Output
MPLS	Multiprotocol Label Switching
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Between Failures
NMS	Network Management System
NOC	Network Operations Centre
NoTA	Network on Terminal Architecture
NRIC	Network Reliability & Interoperability Council
NTP	Network Time Protocol
OAM&P	Operations, Administration, Management, and Provisioning
OPN	Optical Private Network
OS	Operating System
OSS	Operational Support System
PHY	Physical
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
POTS	Plain Old Telephony Service
PQ	Priority Queuing
PS	Packet Switching
PSTN	Public Switch Telephony Network
PTZ	Pan, Tilt and Zoom
QoE	Quality of Experience
QoS	Quality of Service
RPC	Remote Procedure Call
RD	Resilience-Differentiated
RED	Random Early Detection
RF	Radio Frequency
RRSTP	Ring Rapid STP
RSTP	Rapid STP
RSVP-TE	Resource Reservation Protocol - Traffic Engineering
SAN	Storage Area Network
SANET	Sensor and Actor NETworks
SDH	Synchronous Digital Hierarchy
SLA	Service-Level Agreement
SLS	Service Level Specification
SNMP	Simple Network Management Protocol
SPF	Shortest Path First
SOA	Service-Oriented Architecture
SON	Service-Oriented Network
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
TMN	Telecommunications Management Network
TV	Television
UDLD	UniDirectional Link Detection
UI	User Interface
UMTS	Universal Mobile Telephony System
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
W3C	World Wide Web Consortium
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WMN	Wireless Mesh Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin
WSN	Wireless Sensor Network

enisa
European Network
and Information
Security Agency

PO Box 1309   71001 Heraklion   Greece
Tel: +30 2810 391 280   Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu