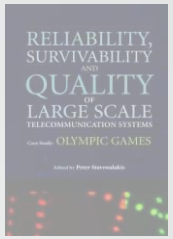


Survivability of critical networks:

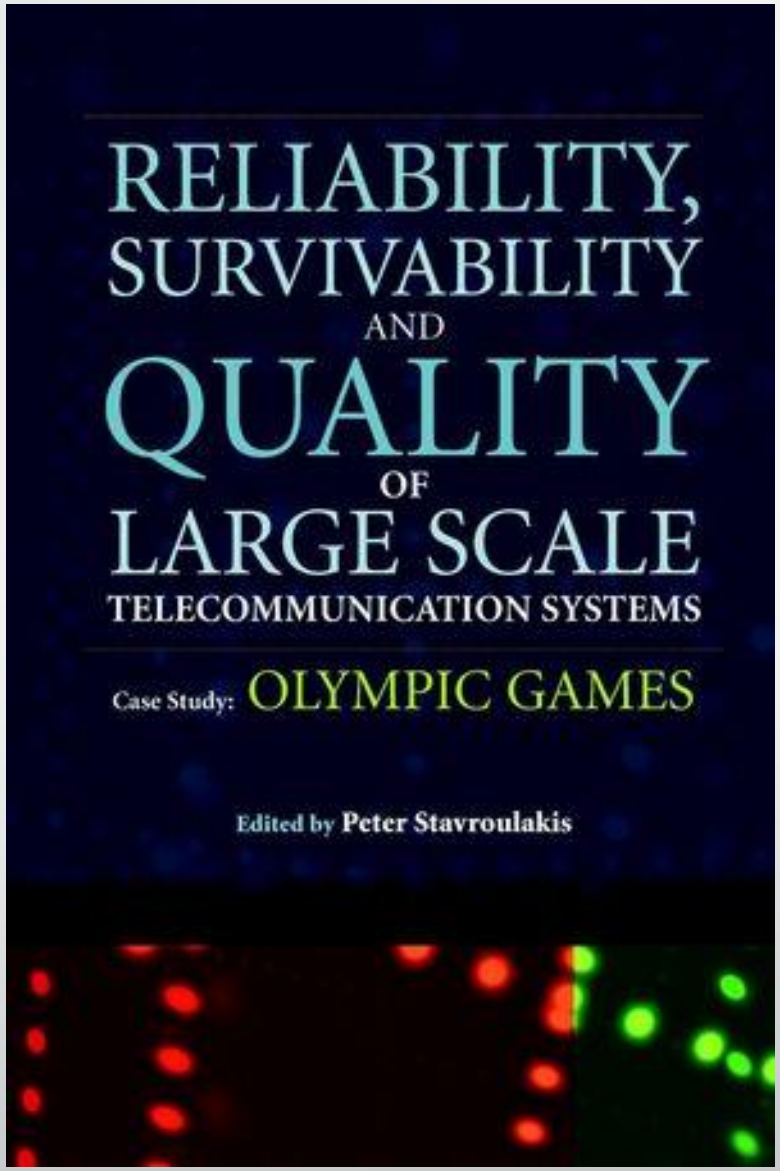
Case study Fiber Optical Networks

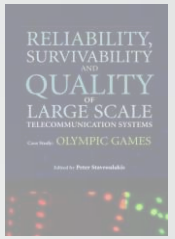
by

Professor Peter Stavroulakis

pete_tsi@yahoo.gr

- **References**
- 1)Peter Stavroulakis,Book, Reliability,Survivability and Quality of Large Scale Telecom Systems,John Wiley,2003
- 2)Peter Stavroulakis, Book, Chaos Applications in Telecommunications, Taylor Francis, 2006
- 3) A comparative Analysis of Network Dependability,Fault-tolerace, Reliability, Security,and Survivability, IEEE Surveys and Tutorials,Vol.11, No. 2,2009
- 4)Mable P. Fok et.al, Optical Layer Security in Fiber –Optic Networks, IEEE Transactions on Information Forensic and Security,Vol.6,No 3, September, 2011
-

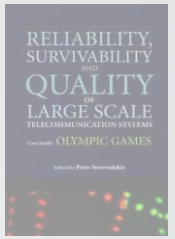

RELIABILITY,
SURVIVABILITY
AND
QUALITY
OF
LARGE SCALE
TELECOMMUNICATION SYSTEMS
Case Study: OLYMPIC GAMES
Edited by Peter Stavroulakis



Necessity of survivability study

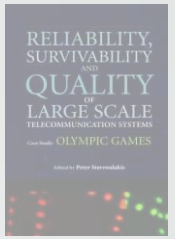
- The 19th Century was the Century of the Industrial Revolution
- The 20th Century was the Century of the Electronics Revolution
- The 21st Century is the Century of the Information Revolution

- Increase of world standards of living and security depends on how we use information



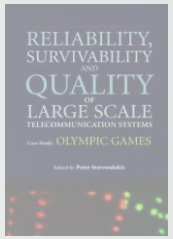
Information Revolution

- The information revolution is driven by the technological advancement in software, microelectronics, storage and very soon by nanotechnology.
- Technological advancement however did not keep in pace with the requirements of critical network systems and left some gaps in the fault tolerance, availability, reliability, security areas.
- Can Survivability help cover these gaps??



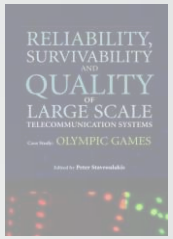
Definition of Survivability

- We define survivability as **the capability of a system to fulfill its mission (provide essential services) , in a timely manner, in the presence of attacks, failures, or accidents.** We use the term system in the broadest possible sense, including networks and large-scale unbounded systems.
- The term **mission** refers to a set of very high-level requirements or goals. Missions are not limited to military settings since any successful organization or project must have a vision of minimum objectives which need be necessarily realized .



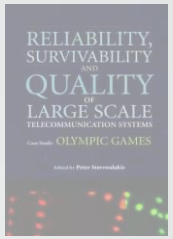
Information Revolution vs Technological Advancement

- Technological advancement however did not keep in pace with the requirements of critical network systems and left some gaps in the **fault tolerance, availability, reliability, security** areas
- Survivability is becoming a major study tool towards the effective and practical coverage of these gaps



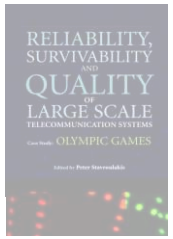
Is Survivability an autonomous tool ?

- As technology involved within the framework of the information revolution these information transferring systems such as **Fiber Networks** started offering services and capture every facet of life such as health, education, business, finance, commerce, energy, social media and even military (Electronic ,Information and Cyber warfare) and thus more and more the need arose to protect this information and in some cases even at any cost.



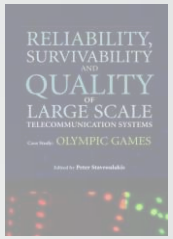
Could survivability help closing the gap ?

- Dependency on large scale high risk unbounded network systems, and growing sophistication of system intruders, the focus has been on how to ensure network system survivability to continue to provide essential critical services in a timely manner even after successful intrusion and compromise .
- Requirements of survivable systems must include features such as intrusion **resistance, recognition and recovery** which are called Survivability strategies.



Classification of survivability strategies

Survivability Aspect	Taxonomies of Strategies
Resistance	• traditional security, including encryption and covert channels • diversity and maximized differences in individual nodes • analytic redundancy and voting • specialization, division of labor, trust, and information • continuous validation of trust • exhibited stochastic properties and random behavior
Recognition	• analytic redundancy and testing (including failures in software, encryption, and trust) • intrusion monitoring and suspicious activities • system behavior and integrity monitoring
Recovery	• physical and information redundancy • non-local copies of information resources • preparation, readiness, contingency planning, and response teams
Adaptation and Evolution	• general or specific changes to resist, recognize, or recover from new vulnerabilities that are discovered • broadcast of warnings to other nodes • broadcast of adaptation and evolution strategies • deterrence through retaliation or punishment



Survivability vs other systems attributes

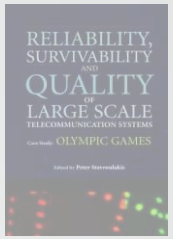
Availability
Reliability
Fault tolerance
Security

Quality
accessibility

Accountability
reusability
predictability
Interchangeability
adaptability
Interoperability
dependability

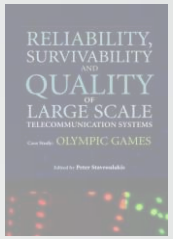
maintainability
recoverability
Compatibility

testability
upgradability
scalability



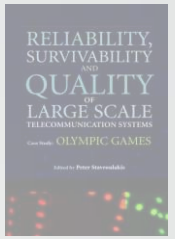
Could survivability be quantified ?

- Survivability must provide essential services but a measurable level of performance must exist in order to maintain an **acceptable and quantifiable** level of functioning of these essential services.
- Survivability necessarily depends on the attributes of **Availability, Reliability, Fault Tolerance and Security** which are only measured probabilistically and the same is true for Survivability.



Necessity for survivability quantification

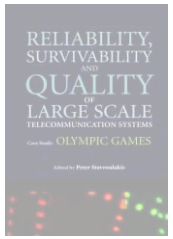
- It is therefore necessary to develop innovative methods and implementation strategies which can translate to quantifiable system performance according to the survivability requirements(completion of mission under attack)
- These survivability measures/metrics could allow us in turn to estimate **deterministic/subjective** measures for **quality of service** as it is proven that survivability is a subsystem of quality.



Survivability Design and Implementation Strategies

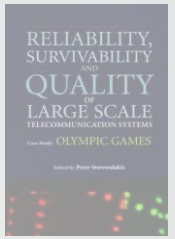
Survivability design of critical system functions in unbounded networks is based on the assumption that.

- Any individual node of the network can be compromised
- Survivability does not require that any **particular** physical component of the network be preserved
- Only the essential services of the network as a whole must survive at the end.



Passive vs Active survivability

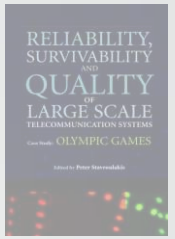
	Passive Survivability	Active Survivability
Philosophy	Survivability is something that a system *has*	Survivability is something that a system *does*
Characteristics	proactive, resistant, robust	reactive, flexible, adaptive
Design Principles	hardness, stealth, redundancy, diversity	regenerate, evolve, relocate, retaliate
Forecasting	Presupposes knowledge of disturbance environment	Acknowledges uncertainty in projection of future disturbances
Architecture	Closed (static)	Open (dynamic)
Design Focus	Defensive barriers at system-level to resist disturbances	Architectural agility to avoid, deter, and recover from disturbances
Failures	Causal chain (often linear)	Tight couplings, functional resonance (nonlinear)
Relevant Disciplines	Component reliability, safety engineering, risk analysis, domain-specific technologies	Real options, organizational theory, process design, domain-specific technologies



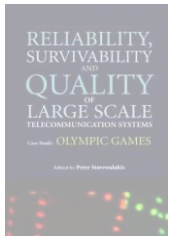
Comparative Analysis of Survivability Components

- Survivability as a general multidimensional concept, can lead to a survivable network system which will have the capability to fulfill its mission in a timely manner, and in the presence of attacks malicious or not , failures, or accidents of any kind.
- The components of this concept are : **Availability, Reliability, Fault Tolerance, Security**. Outages are defined as the unplanned interruptions of service for any reason and are equivalent to unavailability . [3]

Comparative analysis availability (1)



- Availability specifies the degree to which a network system is in a specified operable and committable state at the start of a mission, when the mission is called for at an unknown and random time For example, a system that is capable of being used on the average continuously 100 hours per week (168 hours) would have an availability of 100/168 , 20%.
-



Mathematical Analysis

Availability

The most simple representation for **availability** is as a ratio of the expected value of the uptime of a system to the aggregate of the expected values of up and down time, or

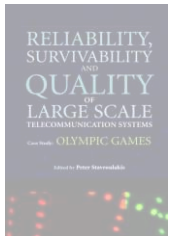
$$A = \frac{E[\text{Uptime}]}{E[\text{Uptime}] + E[\text{Downtime}]}$$

If we define the status function $X(t)$ as

$$X(t) = \begin{cases} 1, & \text{sys functions at time } t \\ 0, & \text{otherwise} \end{cases}$$

therefore, the availability $A(t)$ at time $t>0$ is represented by

$$A(t) = \Pr[X(t) = 1] = E[X(t)].$$



Mathematical Analysis (1)

Availability

Average availability must be defined on an interval of the real line. If we consider an arbitrary constant $c > 0$, then average availability is represented as

$$A_c = \frac{1}{c}\int_0^c A(t)\,dt.$$

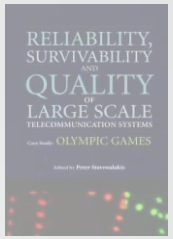
Limiting (or steady-state) availability is represented by

$$A = \lim_{c\to\infty} A_c.$$

Limiting average availability is also defined on an interval $[0, c]$ as,

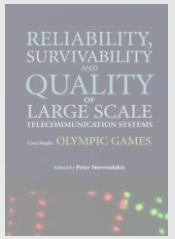
$$A_\infty = \lim_{c\to\infty} A_c = \lim_{c\to\infty} \frac{1}{c}\int_0^c A(t)\,dt, \quad c > 0.$$

Availability is the probability that an item will be in an operable and commitable state at the start of a mission when the mission is called for at a random time, and is generally defined as uptime divided by total time (uptime plus downtime).



Comparative Analysis (2)
Fault Tolerance

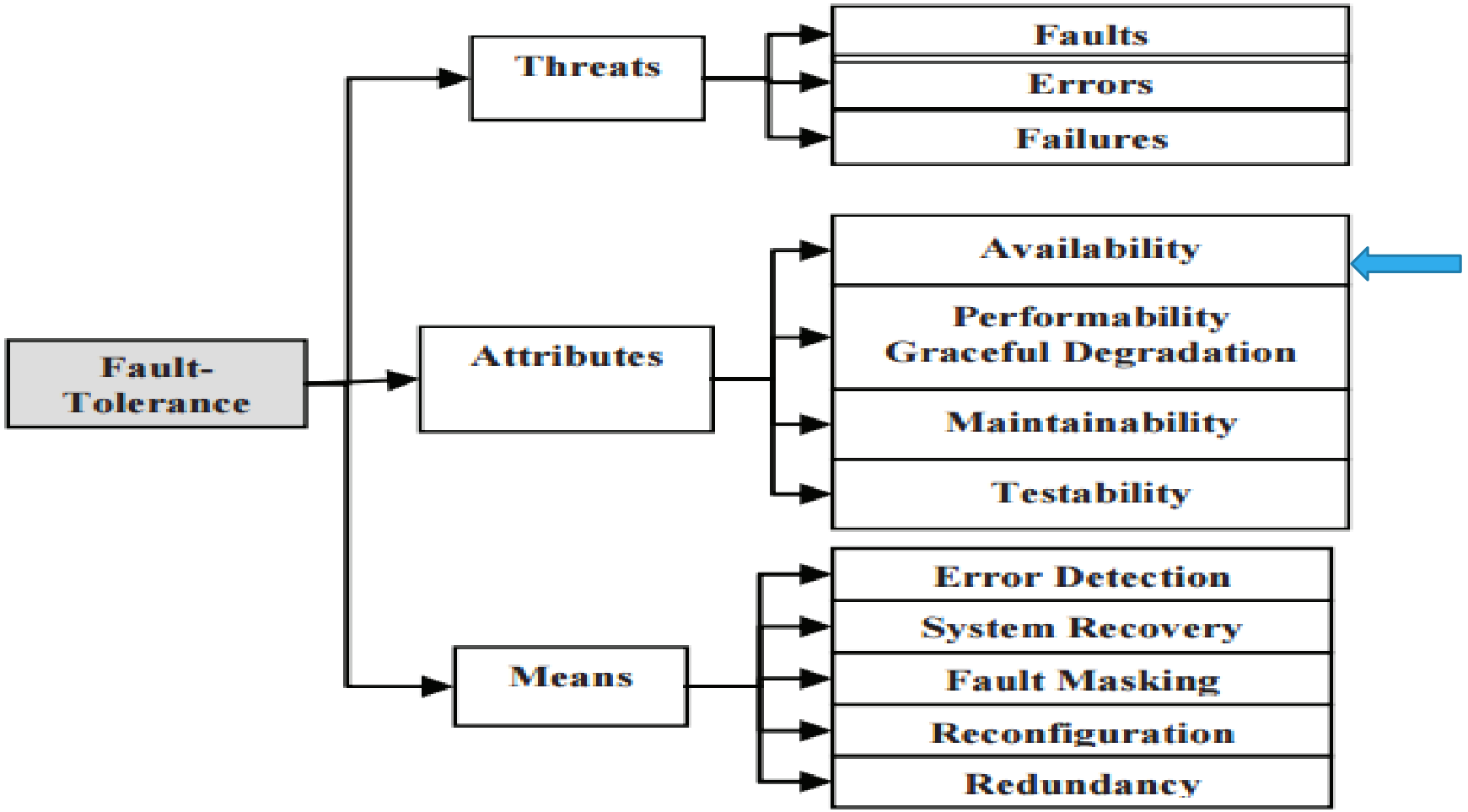
- Fault Tolerance is the ability of a network system to continue normal operation despite the presence of hardware or software faults.
- There exist fundamental terms in fault tolerant design which are fault ,error , failure and a cause- effect relationship that exists between them.
- There are various techniques for achieving fault tolerance design. In general, it is realized by **error detection** mechanisms followed by the appropriate **system recovery**. **Fault masking** is another technique to tolerate faults. Other techniques include detecting, locating, diagnosing , and confining faults as well as **reconfiguring** the network system to remove the faulty component.

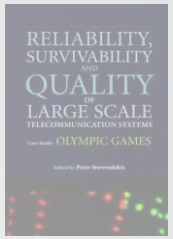


Comparative Analysis
Fault Tolerance

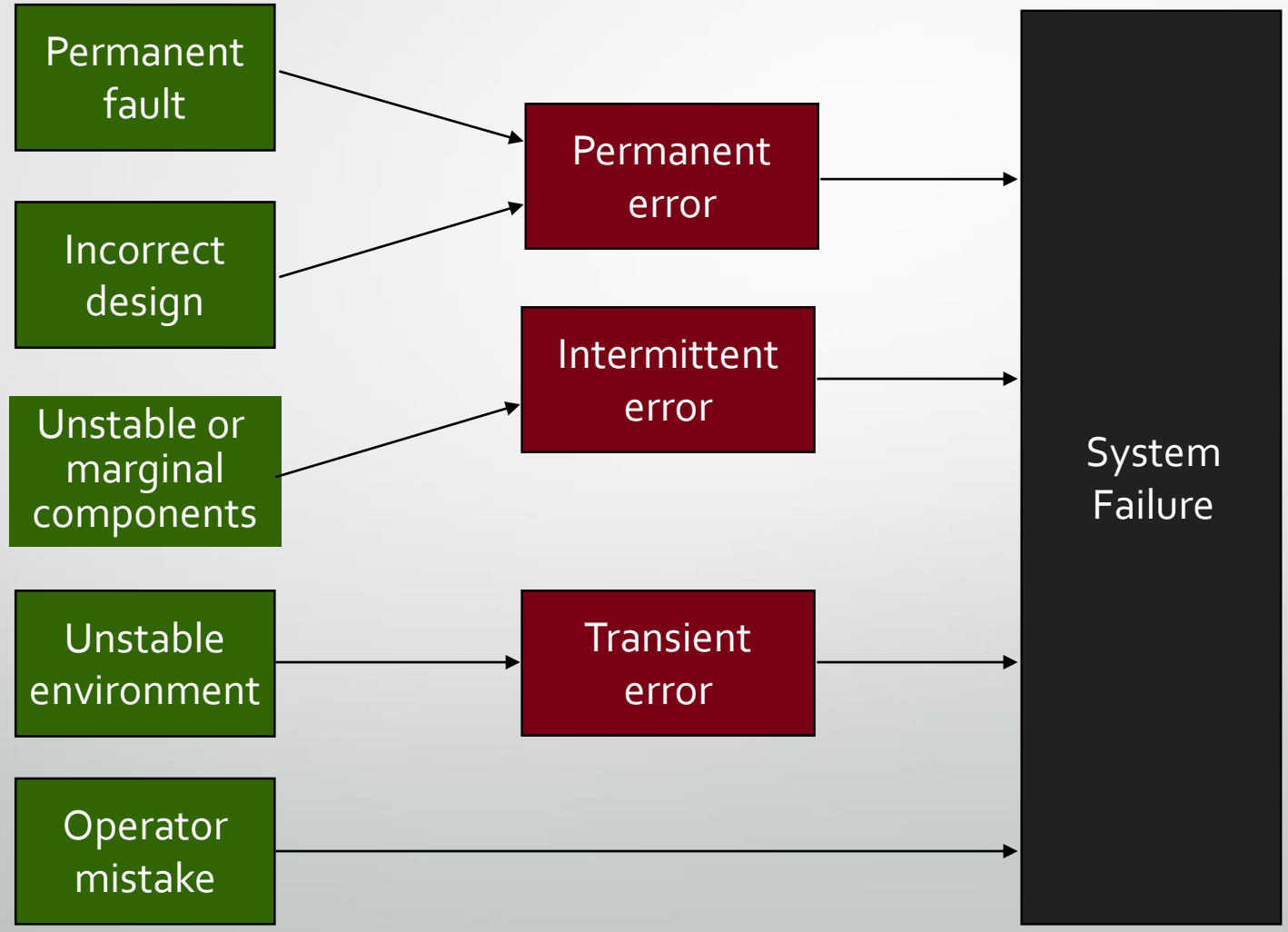
- Fault tolerance must have certain appropriate attributes to achieve its goal.
- **Reconfiguration** is the process of eliminating a faulty entity from a system and restoring the system to some operational condition or state. When using the reconfiguration process, the designer must be concerned with the **fault detection, fault location, fault containment, and fault recovery.**
- One way to satisfy the requirements on a fault tolerant system to operate correctly even after some failures of its elements is to introduce **redundancy** for some of its elements even though it may not be necessary in some cases.

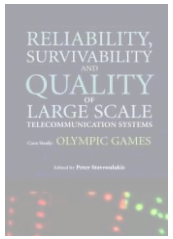
Comparative Analysis
Fault Tolerance



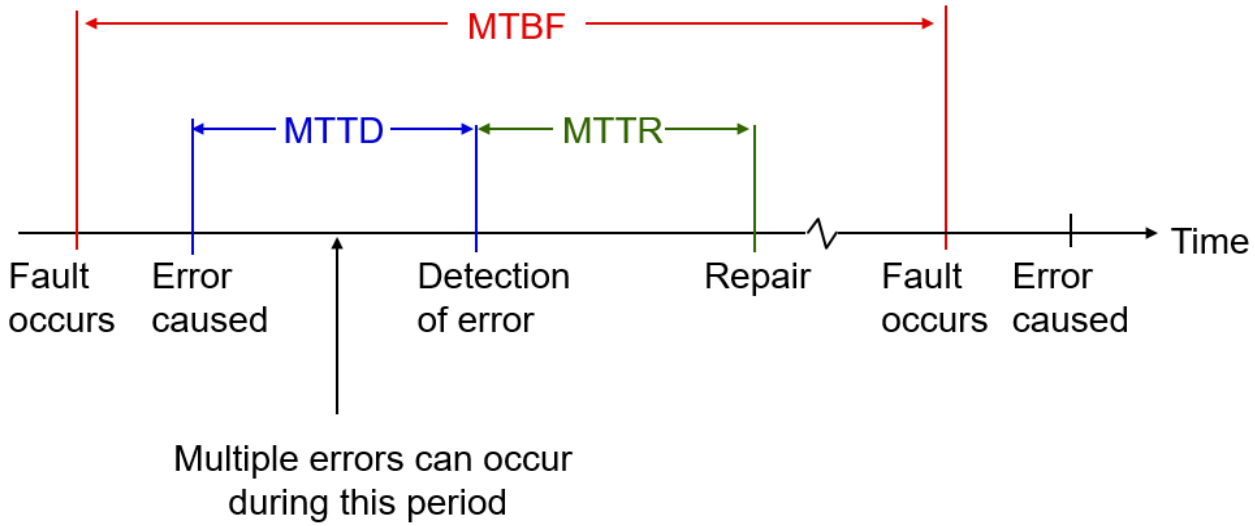


Fault Classification





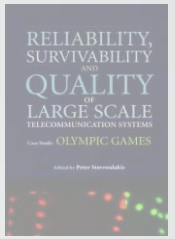
Fault tolerant Measure (MTBF)



MTBF

Mean time between failures

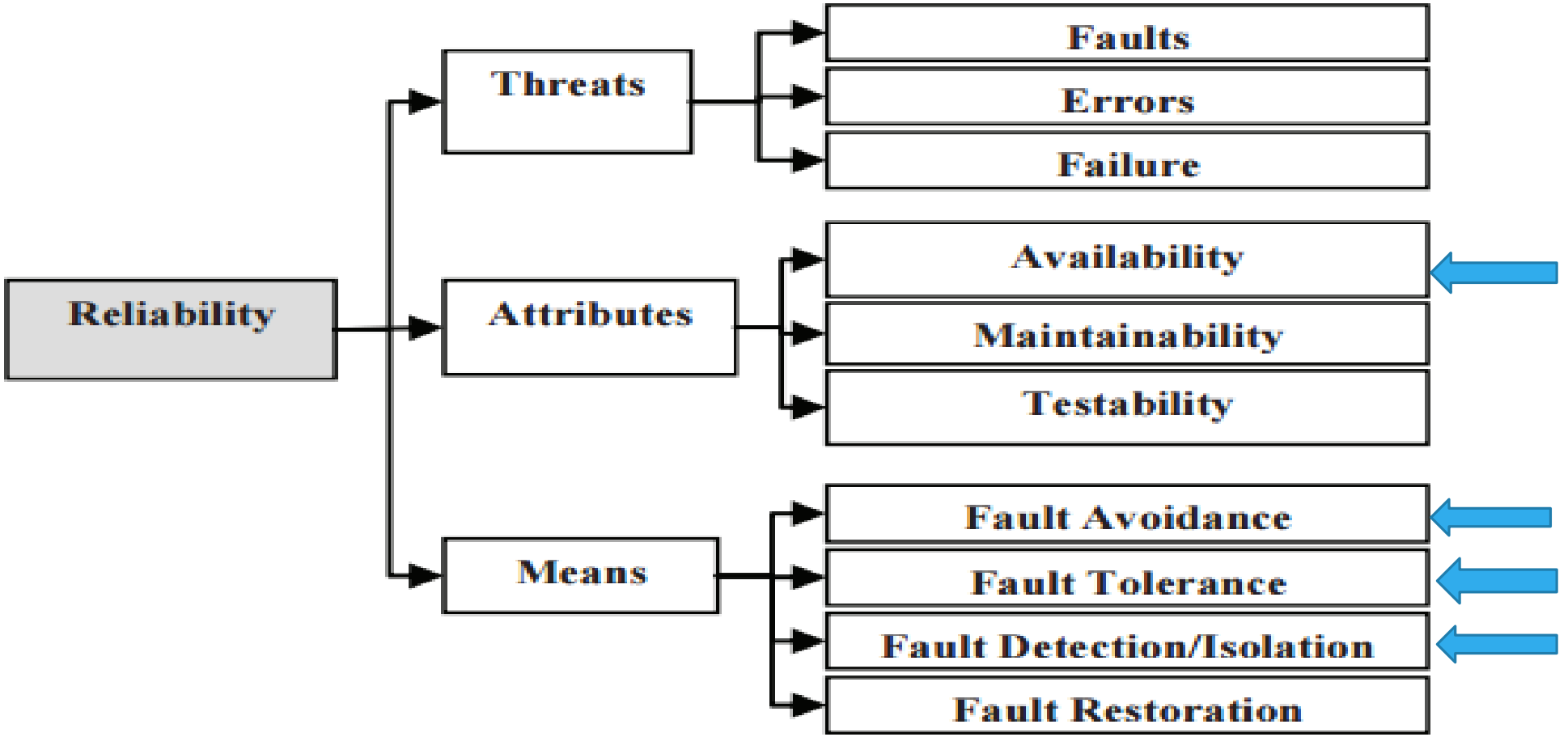
$$\mathrm{MTBF} = \int_0^\infty R(t)dt$$

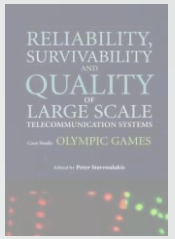


Comparative Analysis Reliability (3)

- Unlike fault tolerance , reliability can be used as a well-defined mathematical function, specifically, as the ability of a network system or component to perform its required functions under stated conditions for a specific period of time .
- The measure that can be obtained via this mathematical analysis is a probabilistic measure denoting the conditional probability that the system will perform its intended function without failure at time t provided it was operational at time t=o.
- In other words, it defines the measure of continuity of acceptable service.

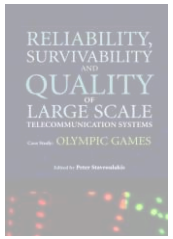
Comparative Analysis 2
Reliability





Comparative Analysis 1
Reliability

- There are four important features that must be introduced and implemented at the starting phase of the design to achieve reliable and available network systems, namely: fault-avoidance , fault -tolerance , fault –detection/isolation, and fault -restoration. This is the reason why fault –tolerance is a prerequisite to reliability and the attributes used on specifying fault tolerance such as maintainability and testability are also attributes of reliability as seen in the previous schematic.

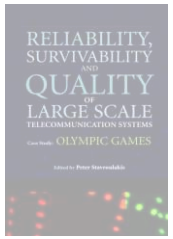


Reliability Mathematical Formulation

- Reliability is defined as the probability that a device will perform its intended function during a specified period of time under stated conditions. Mathematically, this may be expressed as,

$$R(t) = Pr\{T > t\} = \int_t^\infty f(x)\,dx,$$

where f(x) is the failure probability density function and t is the length of the period of time (which is assumed to start from time zero t=o)



Reliability measures

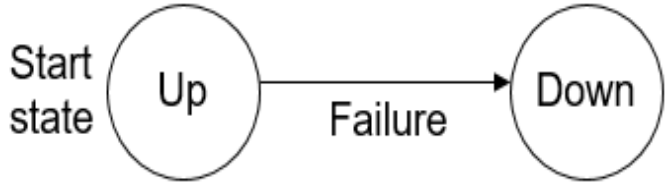
Reliability: $R(t)$

Probability that system remains in the "Good" state through the interval $[0, t]$

$$R(t + dt) = R(t)\,[1 - z(t)\,dt]$$

Hazard function

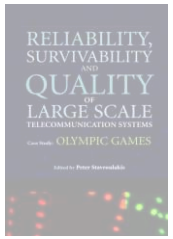
Two-state nonrepairable system



$R(t) = 1 - F(t)$ ---------- CDF of the system lifetime, or its unreliability

Constant hazard function $z(t) = \lambda \Rightarrow R(t) = e^{-\lambda t}$
(system failure rate is independent of its age)

Exponential reliability law



System reliability

The mean number of failures in time $[0, t]$ can be computed as

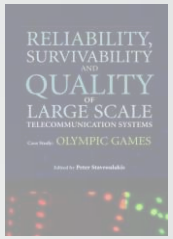
$$E[k] = \sum_{k=0}^{\infty} k \frac{e^{-m(t)}[m(t)]^k}{k!} = m(t)$$

Thus, reliability of a single component is

$$R(t) = e^{-m(t)}$$

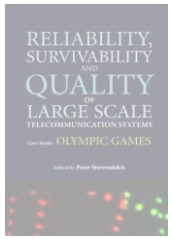
and of a system consisting of n non-redundant components as

$$R_{sys}(t) = \prod_{i=1}^{n} R_i(t)$$



Comparative Analysis
Relationship between Reliability and Availability

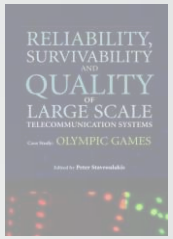
- . It is obvious that Reliability is related to Availability concept but there is a substantial difference .
- Reliability refers to failure free operation during an interval whereas
- Availability refers to a failure free operation at a given instant of time which is usually the time the network system is accessed to provide the required service.
- Thus we can say that reliability is availability at an instant and that is the reason they have entirely different measures.



Relationship reliability and fault tolerance

The reliability function, also known as the survival function, provides the probability that a system will be operational for at least a given time, t. provides the probability that a system will be operational at any given time in the future, given a mean time between failures, MTBF, and mean time to repair, MTTR.

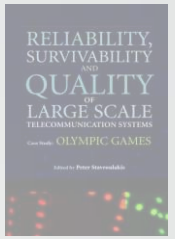
$$R(t) = 1 - F(t) = e^{-t/MTBF}$$



Comparative Analysis security (4)

- Security has a lot of meanings but when it is referred to critical network systems and in general to information security it becomes predominant and must be explained.
- The concept of security is closely related to the confidentiality , integrity, authenticity, non –repudiation, availability. These characteristics must be maintained despite attempted compromises, preventing timely responses to threats (military applications) and thus reducing the consequences of unforeseen threats.
- Up to recent times, security was only used as an add-on feature and not as an essential design component but nowadays where the network systems are used to offer essential services as well (military, banking, commerce, health/telemedicine, energy e.t.c), it has become an essential design component.

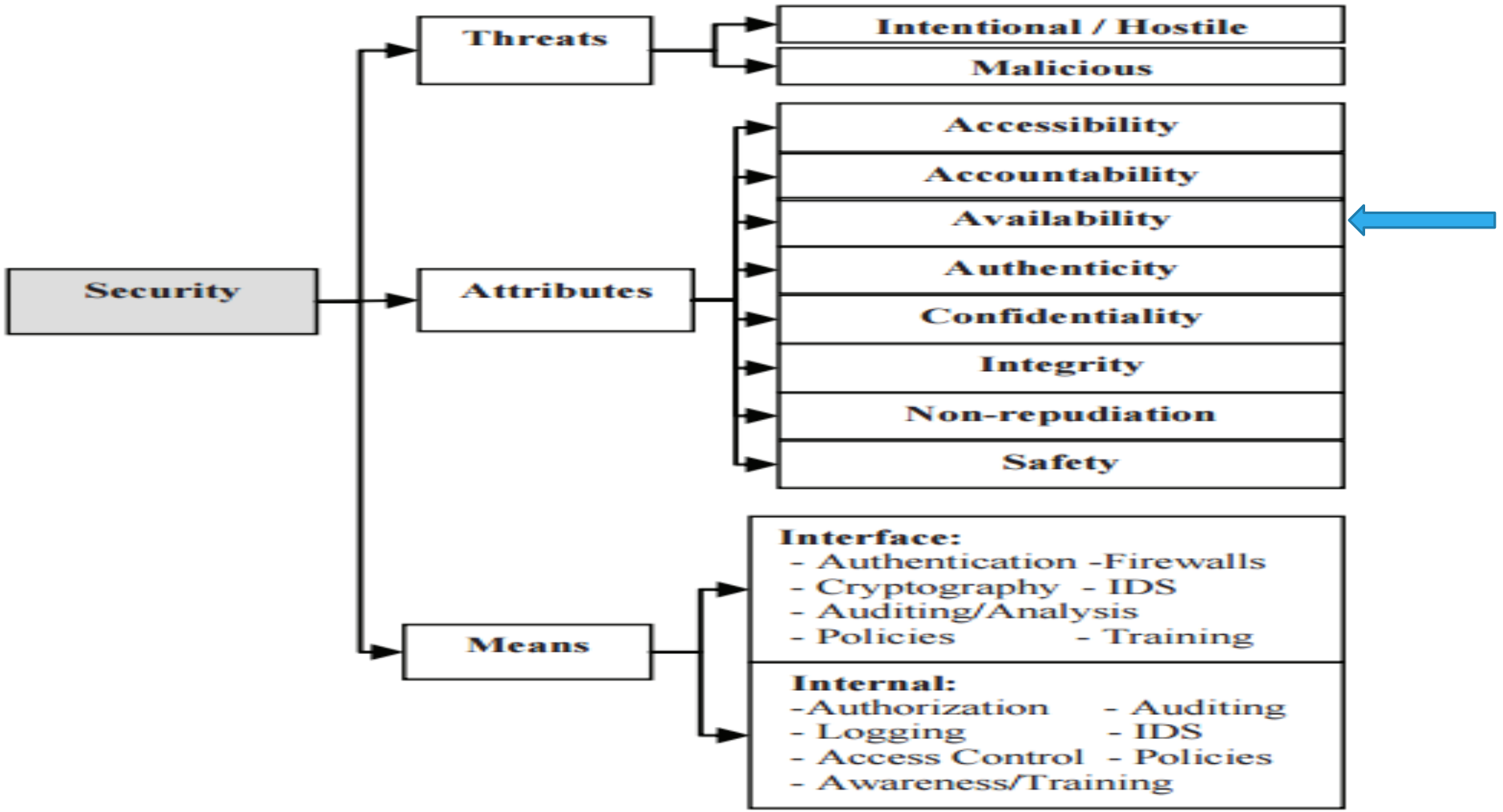
Comparative Analysis 1 security

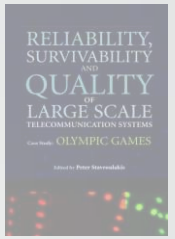


Control mechanisms are implemented in order to prevent, detect, tolerate, and respond timely to security attacks. This is done using theoretical and practical approaches such as cryptography , access control, authentication, firewalls, risk assessments, policies, auditing, and intrusion detection and intrusion prevention systems as well as raising the human awareness and training.

The necessary attributes of security are shown in the following schematic and be examined as a component of survivability

Comparative Analysis 2 security

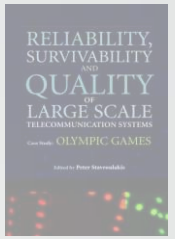




Comparative Analysis (5)
Survivability

Survivability as a concept has its origin in the military context and mainly the military air force and nuclear reactors. It is now used for network systems as it regards the offering and the delivering of critical services and includes the element of time as we have seen before

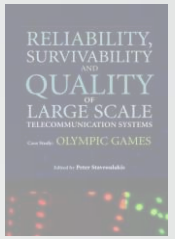
Under survivability, services should have the capacity to recognize and resist attacks, recover from them and adapt in the presence of them in order to diminish the effectiveness of future attacks.



Comparative Analysis Survivability

- Since critical network systems in question may provide non-essential services as well, it is necessary to have a clear understanding and immediate identification and response to essential services under attack.
- The survivability strategy must then be set up in four steps: protection, detection, response, and recovery. If the attack is catastrophic, survivability attributes must be able to keep the system operational long enough for at least the essential services before break down.

Comparative Analysis Survivability

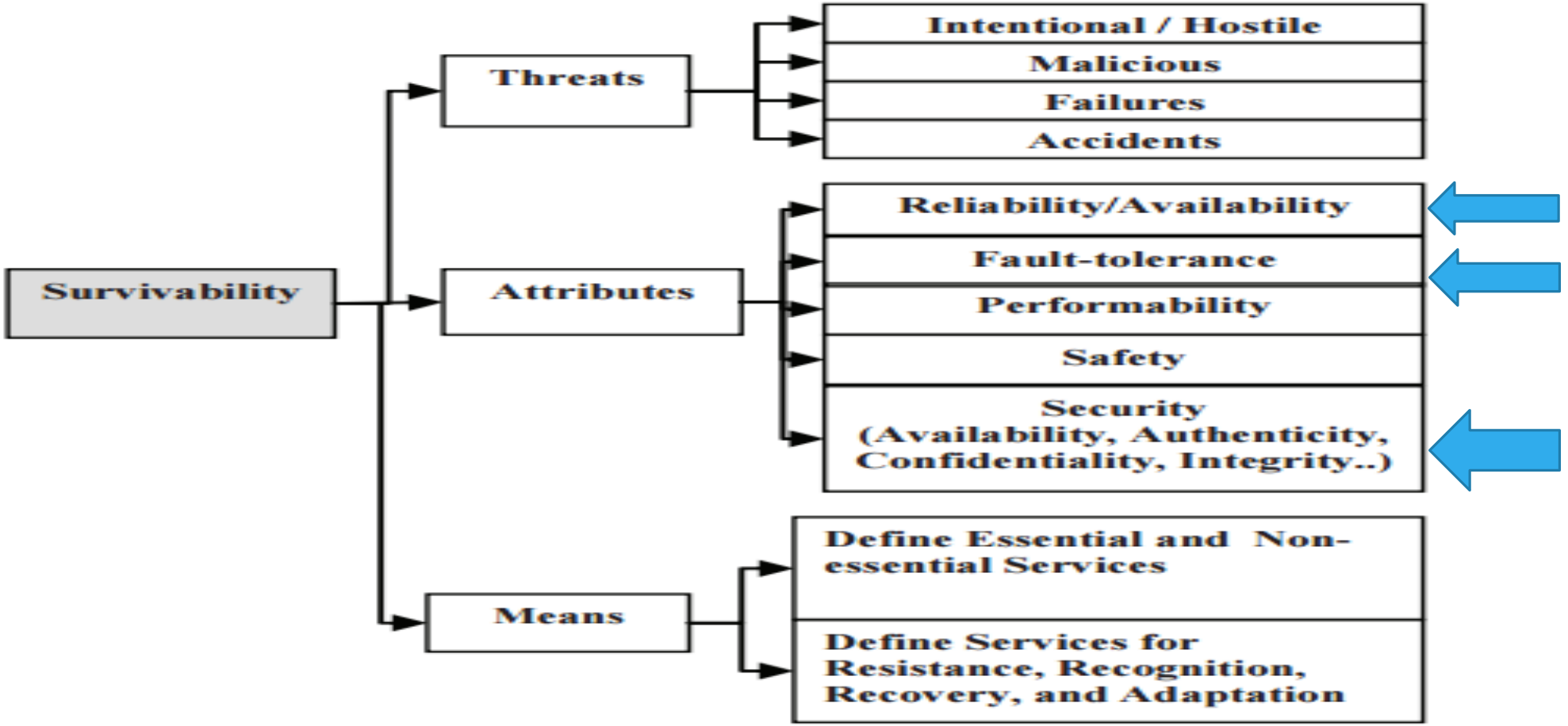


It has been obvious so far that the properties of these four concepts which cooperatively as needed in each application that lead to survivability must be interdependent and non overlapping as far as their attributes .

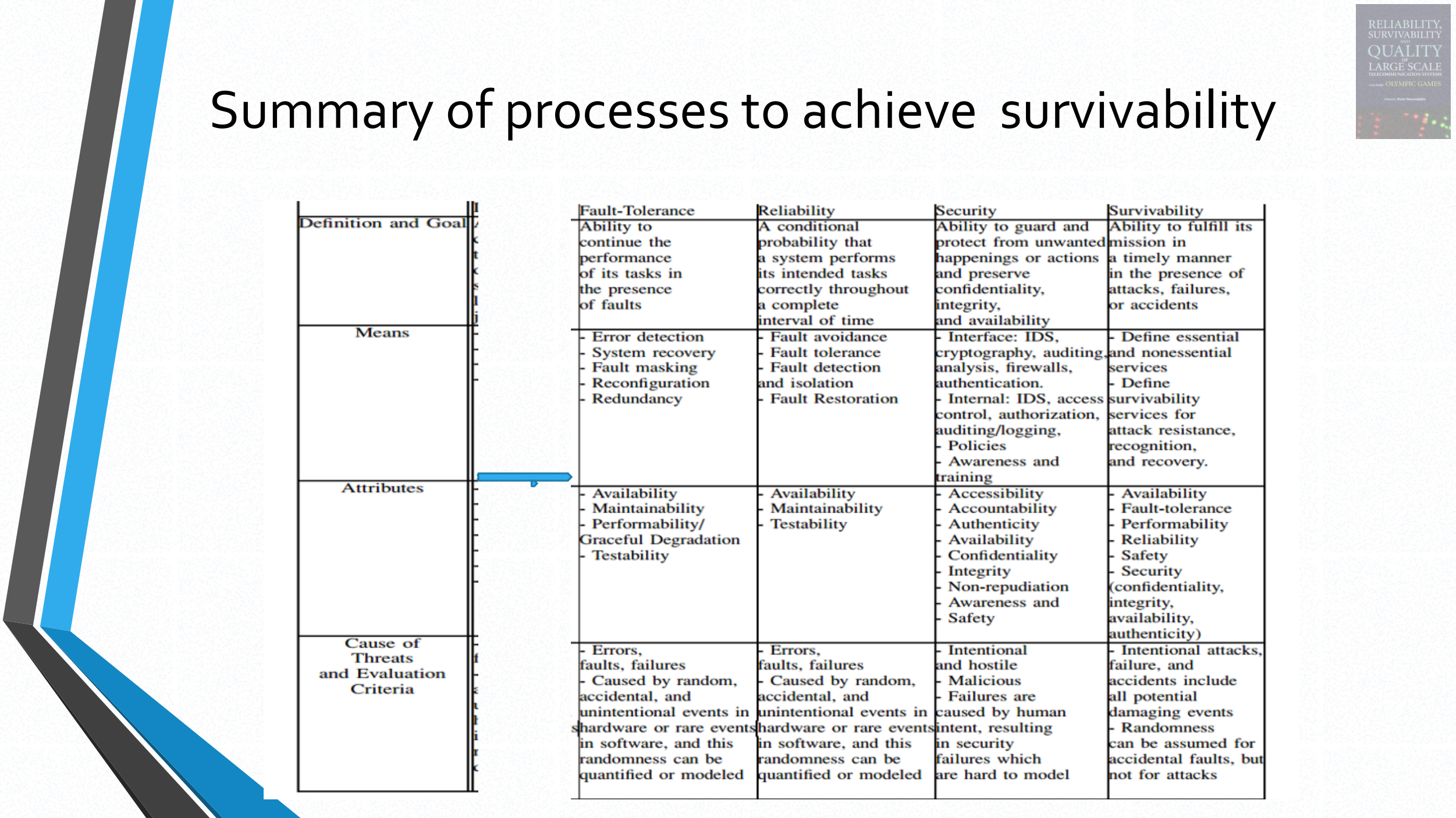
Some are explicit while others are implicit, whereas survivability is considered the all-encompassing concept and a such it is armed with extra capabilities, as see in the schematic that follows, to be able to perform such critical tasks.

The definitions of these concepts are constructed in such a way in order to indicate these subtle differences.

Comparative Analysis 2 Survivability

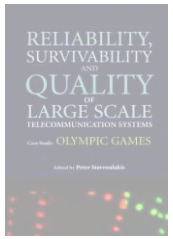


Summary of processes to achieve survivability

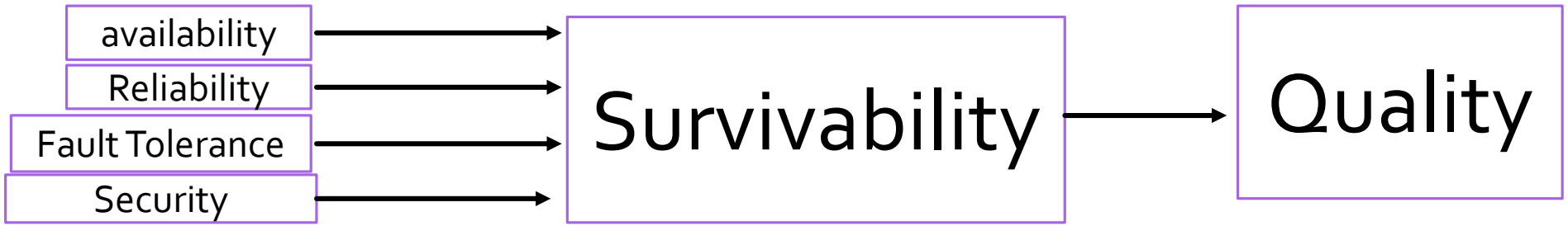


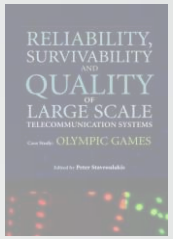
	Fault-Tolerance	Reliability	Security	Survivability
Definition and Goal	Ability to continue the performance of its tasks in the presence of faults	A conditional probability that a system performs its intended tasks correctly throughout a complete interval of time	Ability to guard and protect from unwanted happenings or actions and preserve confidentiality, integrity, and availability	Ability to fulfill its mission in a timely manner in the presence of attacks, failures, or accidents
Means	- Error detection - System recovery - Fault masking - Reconfiguration - Redundancy	- Fault avoidance - Fault tolerance - Fault detection and isolation - Fault Restoration	- Interface: IDS, cryptography, auditing, analysis, firewalls, authentication. - Internal: IDS, access control, authorization, auditing/logging, - Policies - Awareness and training	- Define essential and nonessential services - Define survivability services for attack resistance, recognition, and recovery.
Attributes	- Availability - Maintainability - Performability/ Graceful Degradation - Testability	- Availability - Maintainability - Testability	- Accessibility - Accountability - Authenticity - Availability - Confidentiality - Integrity - Non-repudiation - Awareness and - Safety	- Availability - Fault-tolerance - Performability - Reliability - Safety - Security (confidentiality, integrity, availability, authenticity)
Cause of Threats and Evaluation Criteria	- Errors, faults, failures - Caused by random, accidental, and unintentional events in hardware or rare events in software, and this randomness can be quantified or modeled	- Errors, faults, failures - Caused by random, accidental, and unintentional events in hardware or rare events in software, and this randomness can be quantified or modeled	- Intentional and hostile - Malicious - Failures are caused by human intent, resulting in security failures which are hard to model	- Intentional attacks, failure, and accidents include all potential damaging events - Randomness can be assumed for accidental faults, but not for attacks

Survivability must in general lead to overall quality



- To protect information depending on the goal of the transmitting agent and the network system used, various safety mechanisms must be developed to deal with the concept of Availability, Reliability , Fault tolerance/outage, Security because we have shown they constitutes attributes of the Survivability and all together lead to **Quality of Service** which finally is deterministically and quantitatively measurable.

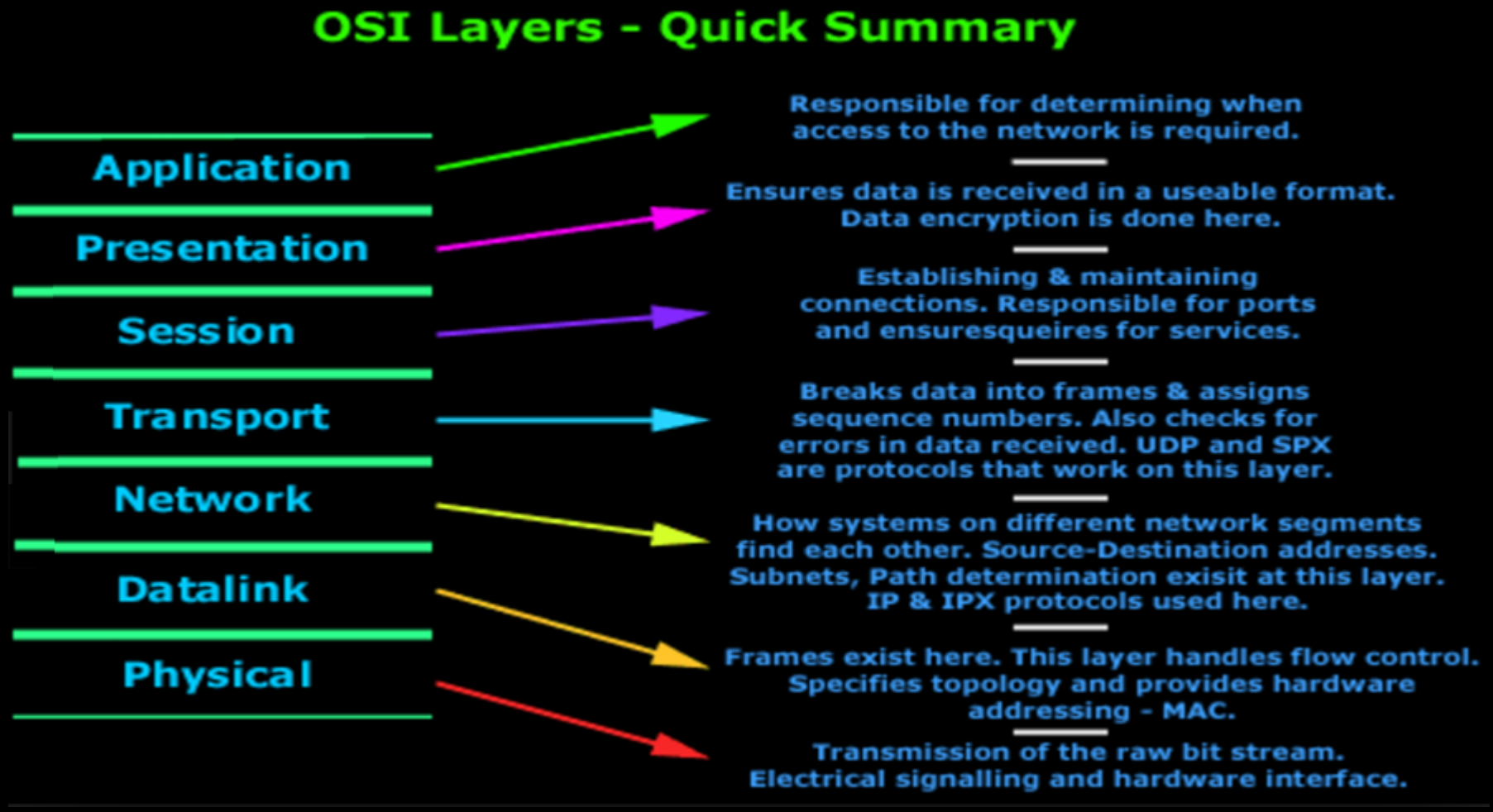




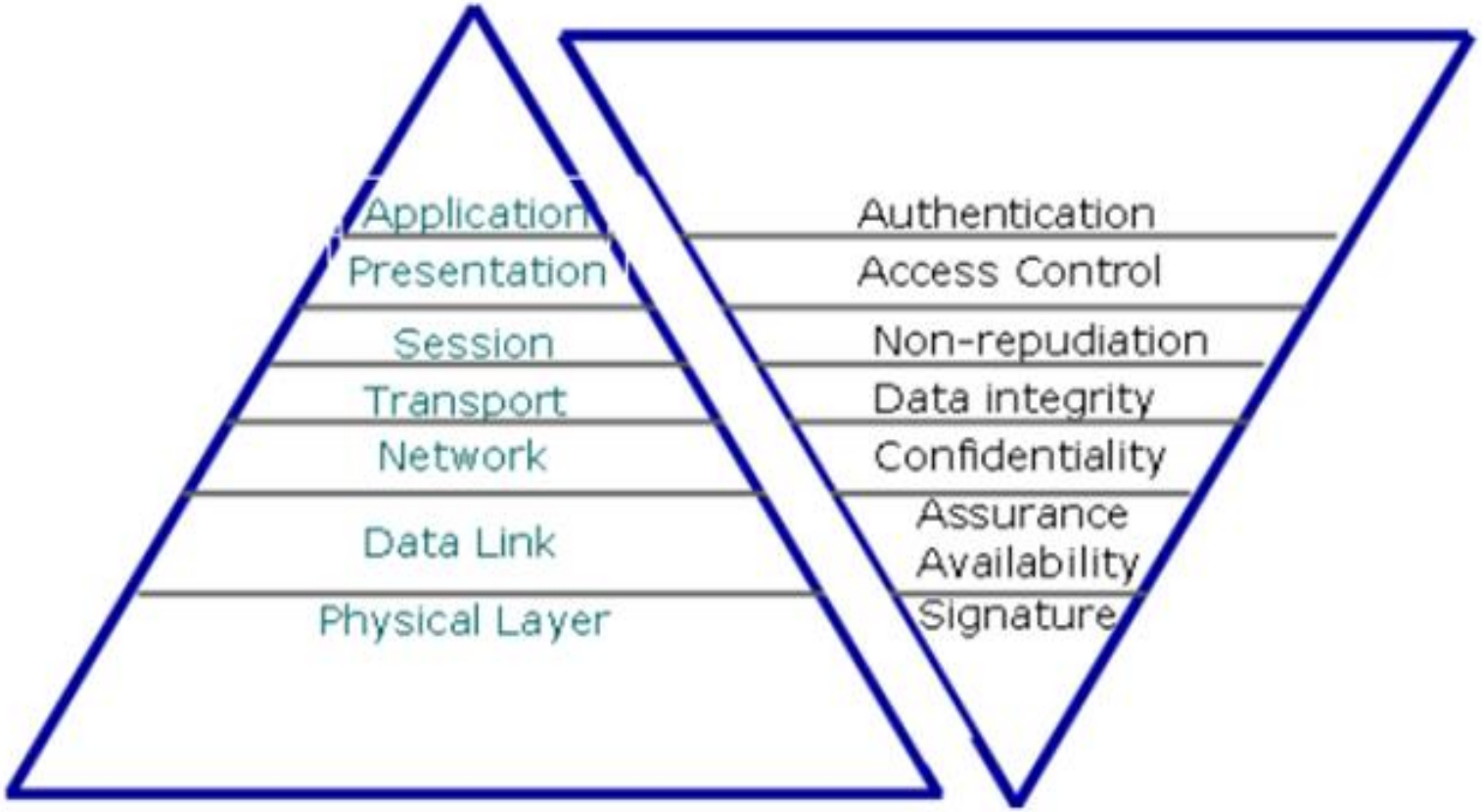
Survivability Quantification

- It has been believed that by studying the components of Survivability and implementing each component to realize perfectly its partial goal in a quantitative manner, we can achieve survivability quantification.
- It has, however, been proven that we are missing an important dimension.
- The system in question itself is broken up into components/layers
- We refer to a seven layer model and thus for network survivability all its layers must be survivable.

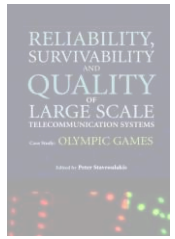
OSI MODEL


OSI Layers - Quick Summary
Application
Presentation
Session
Transport
Network
Datalink
Physical
Responsible for determining when access to the network is required.
Ensures data is received in a useable format. Data encryption is done here.
Establishing & maintaining connections. Responsible for ports and ensuresqueires for services.
Breaks data into frames & assigns sequence numbers. Also checks for errors in data received. UDP and SPX are protocols that work on this layer.
How systems on different network segments find each other. Source-Destination addresses. Subnets, Path determination exisit at this layer. IP & IPX protocols used here.
Frames exist here. This layer handles flow control. Specifies topology and provides hardware addressing - MAC.
Transmission of the raw bit stream. Electrical signalling and hardware interface.

OSI Model
Requirements for each layer



OSI Model



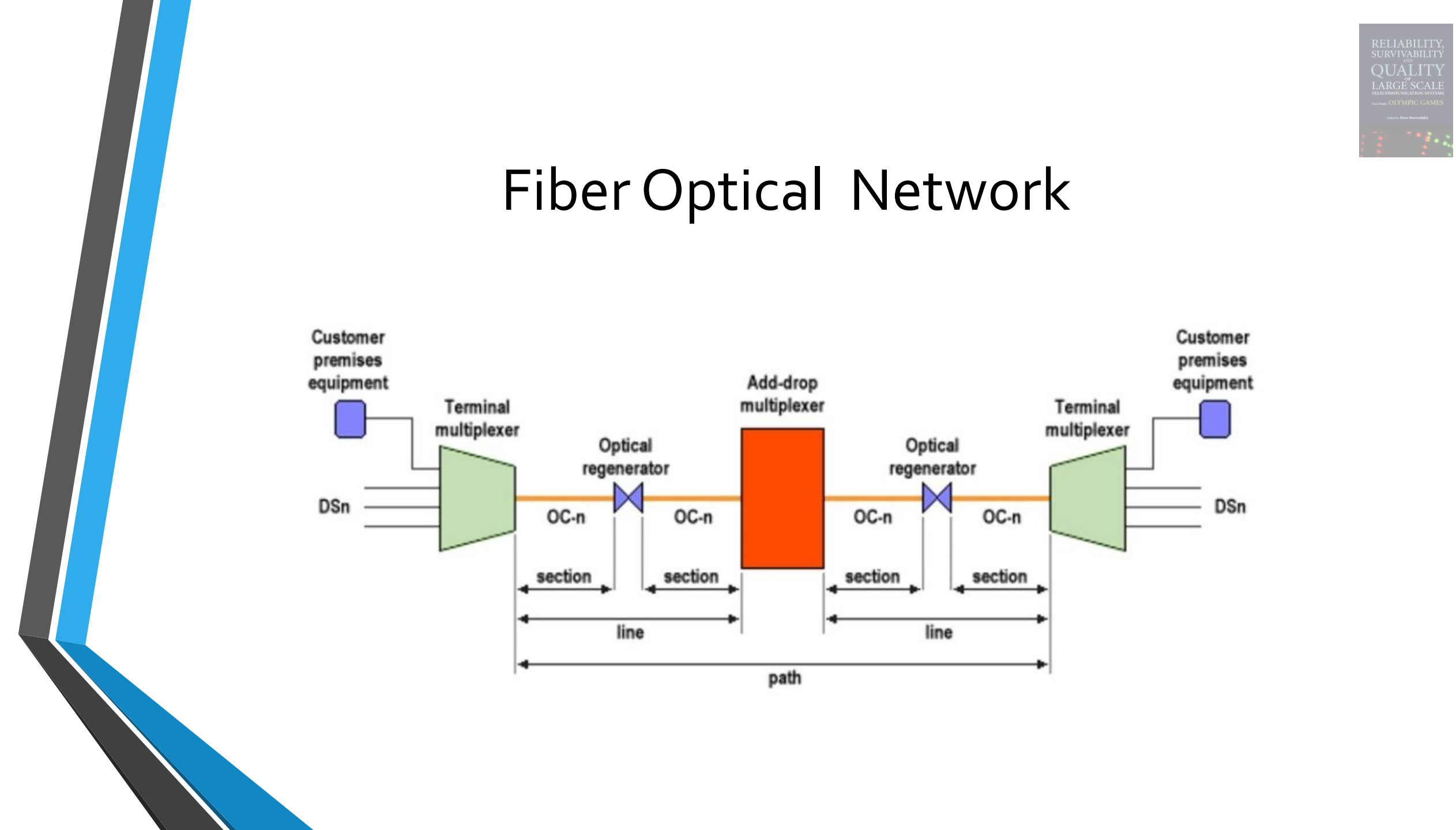
Reduced OSI Model

Application Layer/ Mission

Survivability requirements through its components of availability, fault tolerance, reliability and security cover the other layers 6-2

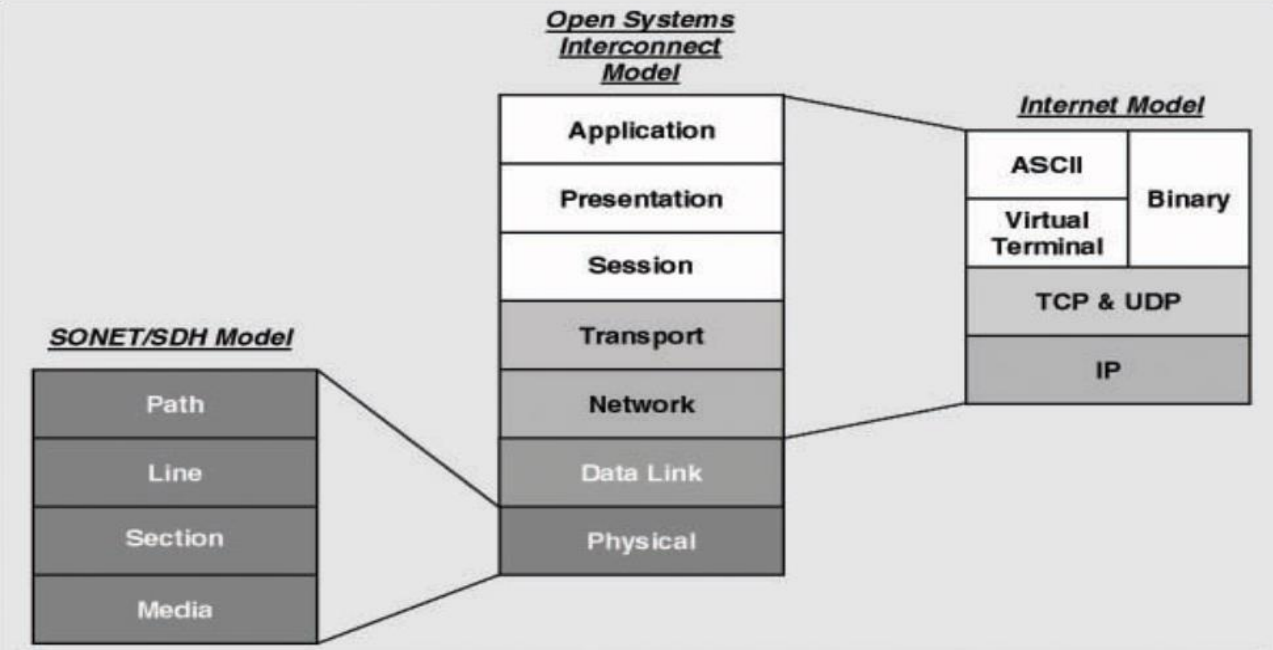
Presentation	Access Control
Session	Non-repudiation
Transport	Data integrity
Network	Confidentiality
Datalink	Availability

Physical layer/ Infrastructure

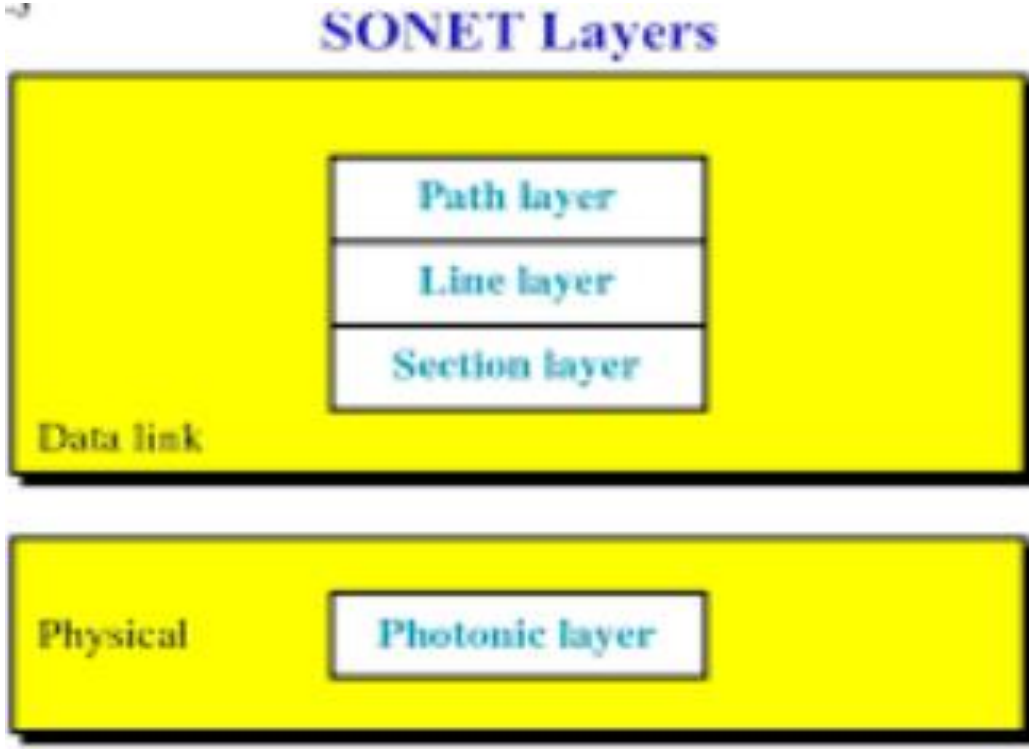


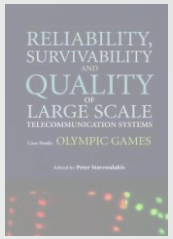
Fiber Optical Network

Fiber Optical Network Layers compared to OSI Model



Fiber Optical Network Layers





Physical layer of Fiber Optical Networks Threats and Means

Threats : Tapping and **Intrusion** of any kind

Physical Layer Intrusion Prevention Systems: desired traits

Automatic identification and characterization of the following distinct optical event types:

Optical Signal Injections & Eavesdropping

Cable Breaks

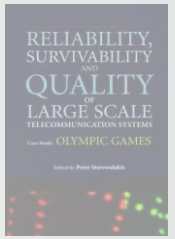
Transients

Receiver Overloads (Jamming)

Low Optical Signal Levels

Data Signal Loss

Identify Causes of Power-off Conditions

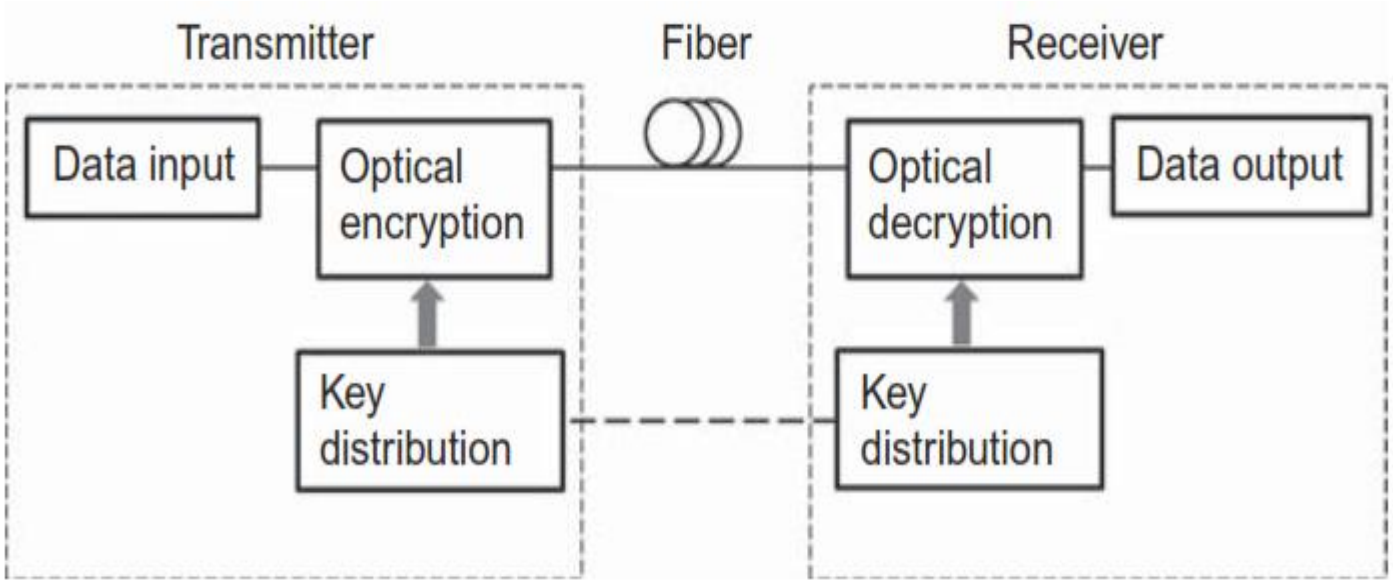


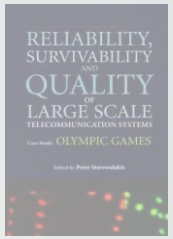
Contribution to overall Network Availability

- Fiber Optical Networks on the seven layer model correspond to the first three layers physical , data link, and network. It also depends what part of the entire Network they represent in any application.
- Jamming is the biggest threat to Availability.
- Stenography can be used to protect availability when the signal is carried by the Amplified Spontaneous Emission (ASE) noise which covers the entire transmission band.
- Chaos based communications can be used as an anti-jamming technique as well

Confidentiality

- Optical Encryption and Optical coding(WCDM)can effectively protect **Confidentiality** especially in areas requesting strong security and processing speed.

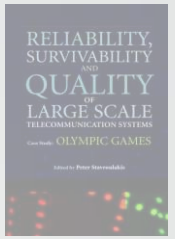




Encryption methods

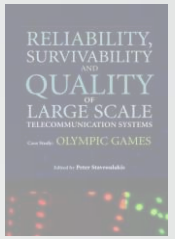
- CDMA in conjunction with XOR logic operations

  which contributes to confidentiality and authentication
- Cross Polarization modulation
- Cross Gain Modulation
- Cross Phase Modulation



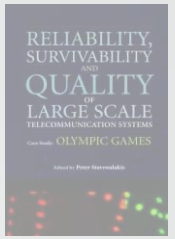
Security

- Fiber Optical Network channel capacity, data rate, and processing speed provide creates the platform for even upper layer security utilizing
  - All optical signal processing
  - Optical key distribution
  - Optical stenography
  - Electromagnetic immunity
  - Chaos based communications for transmitting confidential data with a high degree of robustness
  - Fault tolerance through redundancy .



Survivability Capabilities of Fiber Optical Systems

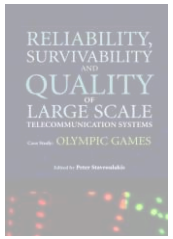
- We observe that Fiber Optical Systems even though they constitute only three layers of the OSI seven layer model, they contribute after careful analysis and proper design to a large extent to all attributes of Survivability
- 1) Availability
- 2) Fault tolerance
- 3) Reliability
- 4) Security
-



Survivability Quantification

- The solution that has been found was to map the attributes of the survivability components to each layer of the network under study and determine the survivability metrics of each layer as a probabilistic measure meeting a certain threshold which will then be used to find the overall survivability metric.

Availability and reliability for physical layer



AVAILABILITY
Ability to perform well
at any instant during a period
RELIABILITY
Probability will perform well at time
t when it was operative at t=0

SIGNAL PROCESSING
Parameters estimated via
accelerating testing
MTTB, MTTF,MTTR
Failure rate
Repair rate

1)Development of a **availability** markov model using failure and repair of each node[1]
2) Reliability mathematical formulation

MEASURES
Availability
MTTB +MTTR
Reliability
Function

References
1) Survivability Quantification: An Analytical Modeling Approach, Gi/ITG conference, Dresden Germany, 2004
Y. Liu and K.Trivedi