IEEE COMMUNICATIONS SOCIETY

STUDY GROUP
FOR
SECURITY, RELIABILITY, AND PERFORMANCE
FOR SOFTWARE DEFINED AND VIRTUALIZED ECOSYSTEMS
(SRPSDVE)

Classification of Internet, Cloud and SDN/NFV Service Outages: Observations and Possible Options/Approaches

April 8, 2015

Spilios Makris , PhD, CBCP
Palindrome Technologies

Outline

- Introduction
- Some Observations
- Examples of Network/Service Outage Classifications
  - PSTN and VoIP based Service Outages
  - Internet and Cloud Service Outages
- Classification/Categorization Issues
- Examples of Pictorial Representation of Outages
- Possible Options/Approaches in analyzing SDN/NFV outages
- Proposed PAR text for the formation of an IEEE Reliability Working Group
- Q&A

Some Observations - 1

- There is no official U.S. government database to report Cloud Service outages similar to the FCC's Network Outage Reporting System (NORS)* for outages reported by the telecom service providers
- "…Even though large scale Internet incidents have been reported in the media, and some papers include a brief list of several such failures, a taxonomy of key Internet failures showing the cause, duration, range, and effect does not exist…" **

* NORS: http://transition.fcc.gov/pshs/services/cip/nors/nors.html

** Source: Christian Doerr & Fernando A. Kuipers "All Quiet on the Internet Front?" IEEE Communications Magazine, October 2014, Vol. 52, No. 10

FCC: Federal Communications Commission

IEEE COMMUNICATIONS SOCIETY

IEEE

Some Observations - 2

- There is no standardized classification methodology (e.g., Root Cause, Direct Cause, Contributing Factors) for Cloud Service outages similar to the:
  - ATIS Standard* prepared by the Network Reliability Steering Committee (NRSC) promoting the use of a new classification system in the FCC's Network Outage Reporting System (NORS)
  - FCC's latest NORS User Manual**.

ATIS: Alliance for Telecommunications Industry Solutions

* Source: ATIS Standard Outage Classification, ATIS-0100012.2013, April 2013

** Source: FCC's Network Outage Reporting System (NORS) User Manual, Version 9, Nov. 22, 2013

Some Observations - 3

- A Google search with the key words “worst cloud outages” may give you part of the story* but the root cause analysis mentioned in such analyses is subjective and based on an incomplete list of root cause categories

* Source:
http://www.infoworld.com/article/2606921/cloud-computing/133109-The-worst-cloud-outages-of-2013-part-2.html
http://www.infoworld.com/article/2622201/cloud-computing/the-10-worst-cloud-outages--and-what-we-can-learn-from-them-.html

** Source: Christian Doerr & Fernando A. Kuipers *“All Quiet on the Internet Front?”* IEEE Communications Magazine, October 2014, Vol. 52, No. 10

Examples of Service/Network Outage Classifications

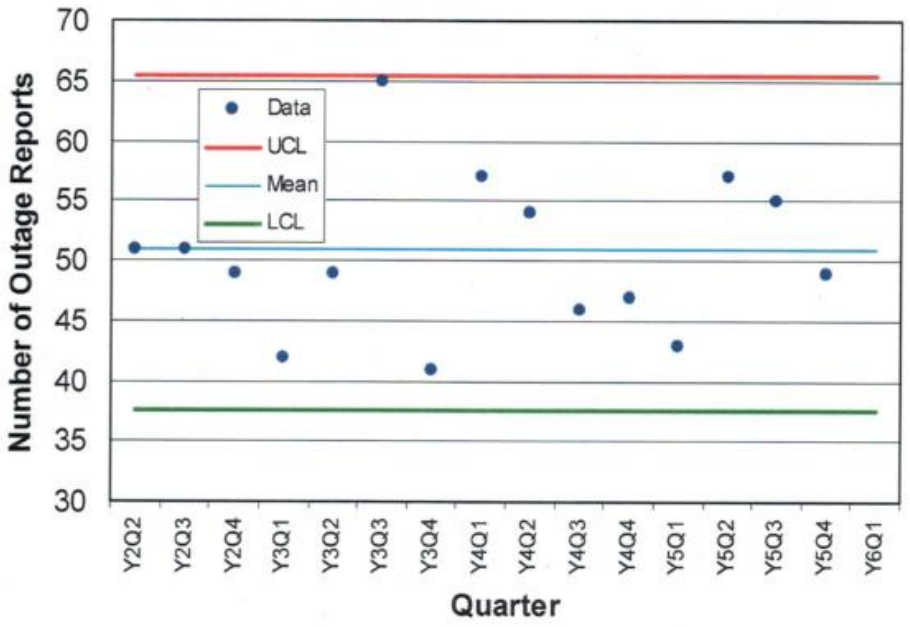
- FCC NORS
- ATIS NRSC
- TL 9000 (by the QuEST Forum)
- Ofcom (**Of**fice of **Com**munications, Britain)
- ENISA (European Network and Information Security Agency)
- National Telecom Regulatory Authorities (TRAs)
- Literature/Publications
  - IEEE Papers
  - InfoWorld Articles
- Etc.

FCC Outage Classification

Source: FCC's Network Outage Reporting System (NORS)* for outages reported by the telecom service providers

Section 7: “Descriptions of Root Cause, Direct Cause and Contributing Factors”

Control Chart



UCL: Upper Control Limit
LCL: Lower control Limit

*NORS: http://transition.fcc.gov/pshs/services/cip/nors/nors.html

ATIS NRSC – Classification of Equipment in Outage Classification and Analysis

1. Circuit Switch
2. Packet Switch
3. Network Signaling Elements
4. Network Service Elements
5. Network Security Elements
6. Transport Equipment
7. Transmission Systems & Media
8. Wireless Transmission
9. System Supporting
10. Common Systems
11. Enterprise/Customer Service

ATIS: Alliance for Telecommunications Industry Solutions
NRSC: Network Reliability Steering Committee
* Source: ATIS Technical Report, *Categorization of Equipment Deployed within Communications Networks for Use in Outage Classification and Analysis, ATIS-0100015.2007, October 2007*

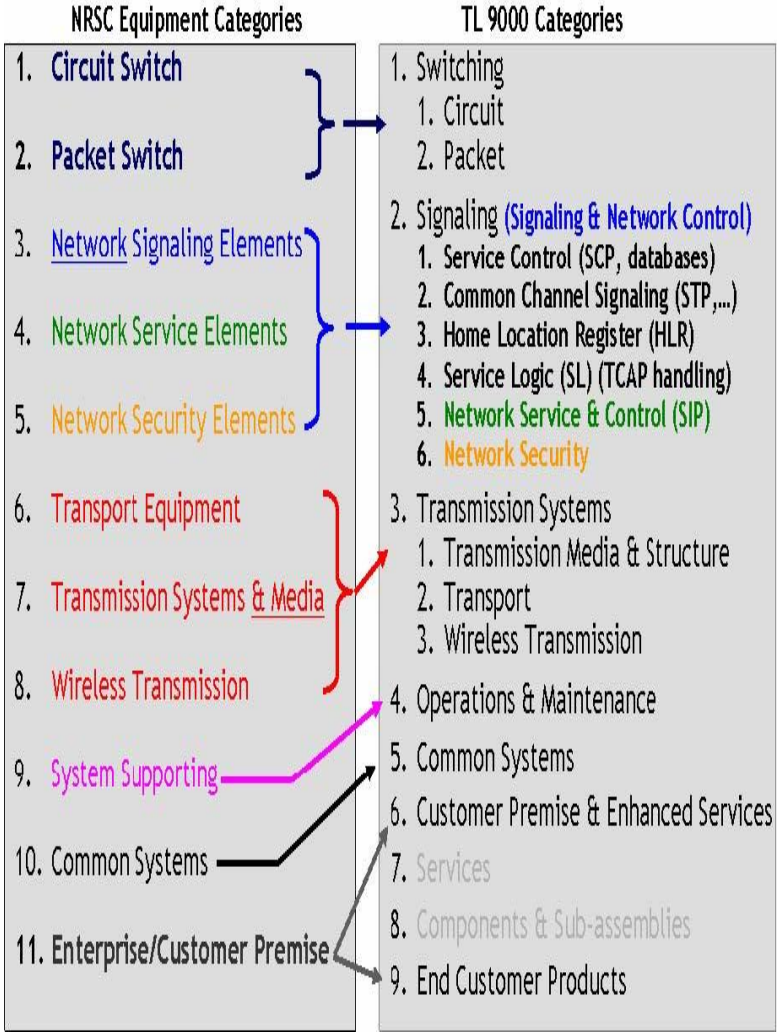
QuEST Forum*:
TL-9000** Classification of Equipment Outages

1. Switching
2. Signaling
3. Transmission Systems
4. Operations & Maintenance
5. Common Systems
6. Customer Premise & Enhanced Services
7. Services
8. Components & Sub-assemblies
9. End Customer Products

* http://www.questforum.org/index.htm

** http://www.tl9000.org/

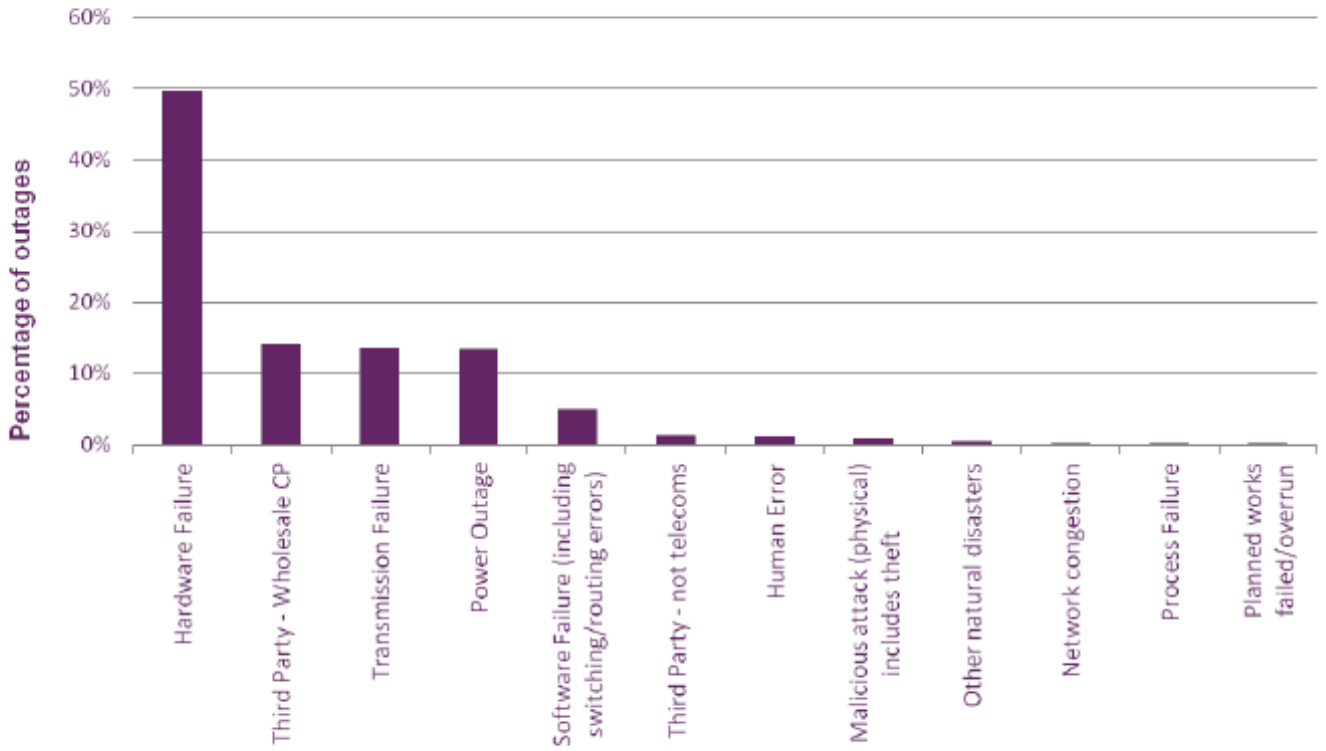
Mapping of NRSC and TL 9000 Categories



Source: ATIS Technical Report, *Categorization of Equipment Deployed within Communications Networks for Use in Outage Classification and Analysis, ATIS-0100015.2007, October 2007*

Ofcom Outage Classification
Root Causes

Figure 49 – Root causes of incidents reported to Ofcom (Oct 2012 – Aug 2013)



Source: Ofcom/Operators

http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/infrastructure-report/IRU_2013.pdf

Ofcom Outage Classification
Detailed Causes

Figure 12 shows the detailed causes of incidents.

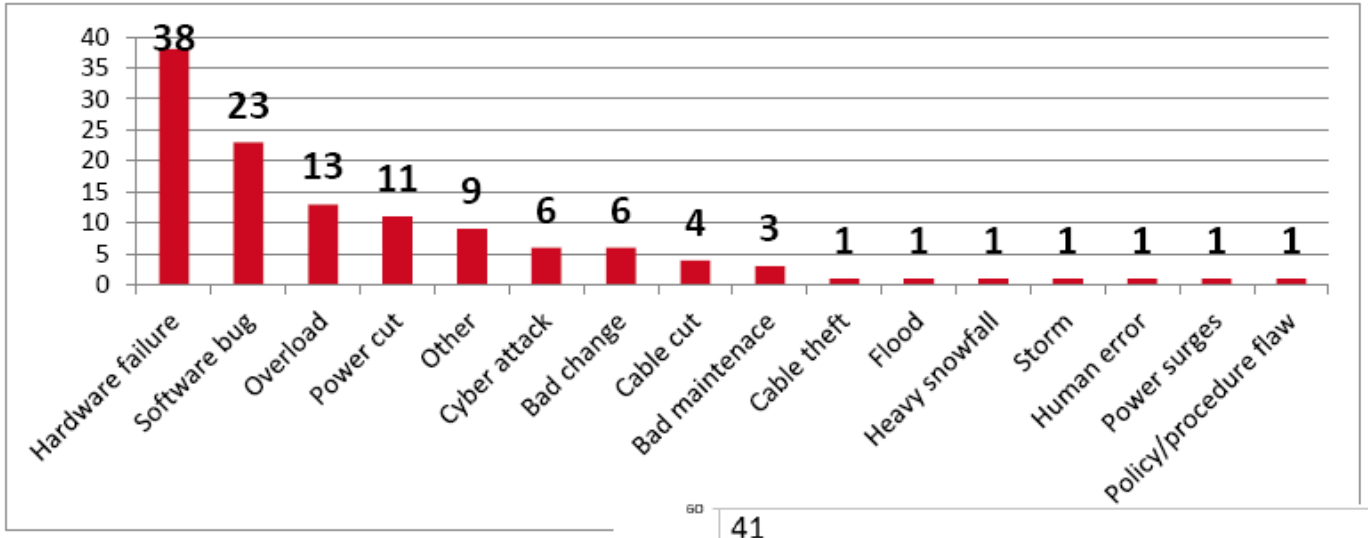
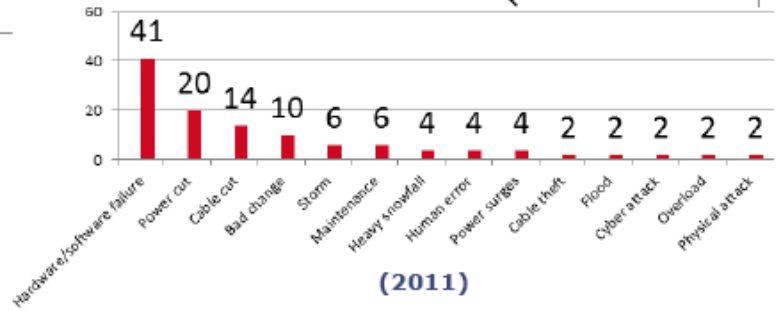


Figure 12 Detailed causes of reported incidents

(2012)



http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/infrastructure-report/IRU_2013.pdf

ENISA Outage Classification

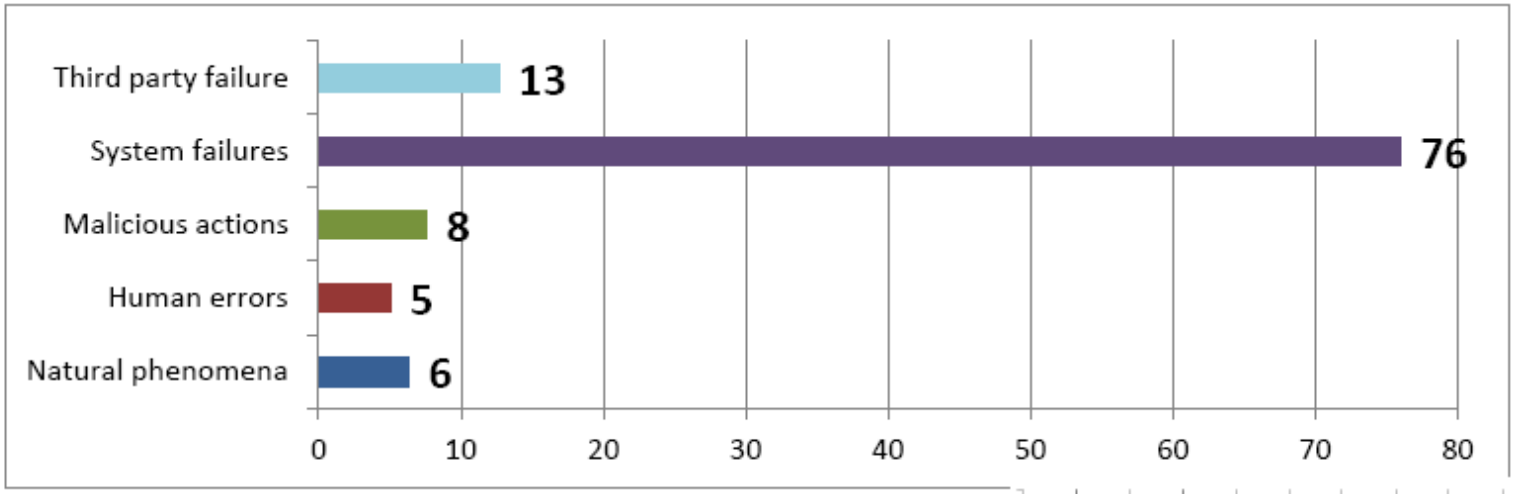
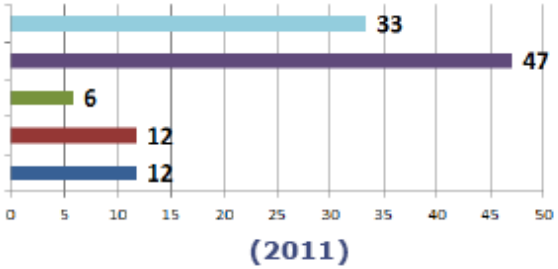


Figure 9 Incidents per root cause category (percentage).

(2012)



http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012-1/annual-incident-reports-2012

Example 1: Internet Service Outages (2007-2013)*

This Study** was based on:

- Interviews with:
  - Regional Internet Service Providers (ISPs)
  - National Research & Educational Network Operators (NRENs)
  - National Incumbent Operators
  - Multi-national networks
- Research
  - Literary searches in academic and trade articles
  - News websites
  - Blogs, fora, and operator mailing lists about Internet incidents

* Period: June 2007 – December 2013

** Source: Christian Doerr & Fernando A. Kuipers *"All Quiet on the Internet Front?"* IEEE Communications Magazine, October 2014, Vol. 52, No. 10 (The authors are with Dreft University of Technology)

IEEE COMMUNICATIONS SOCIETY

IEEE

Example 1: Internet Service Outages (2007-2013) (Continued)

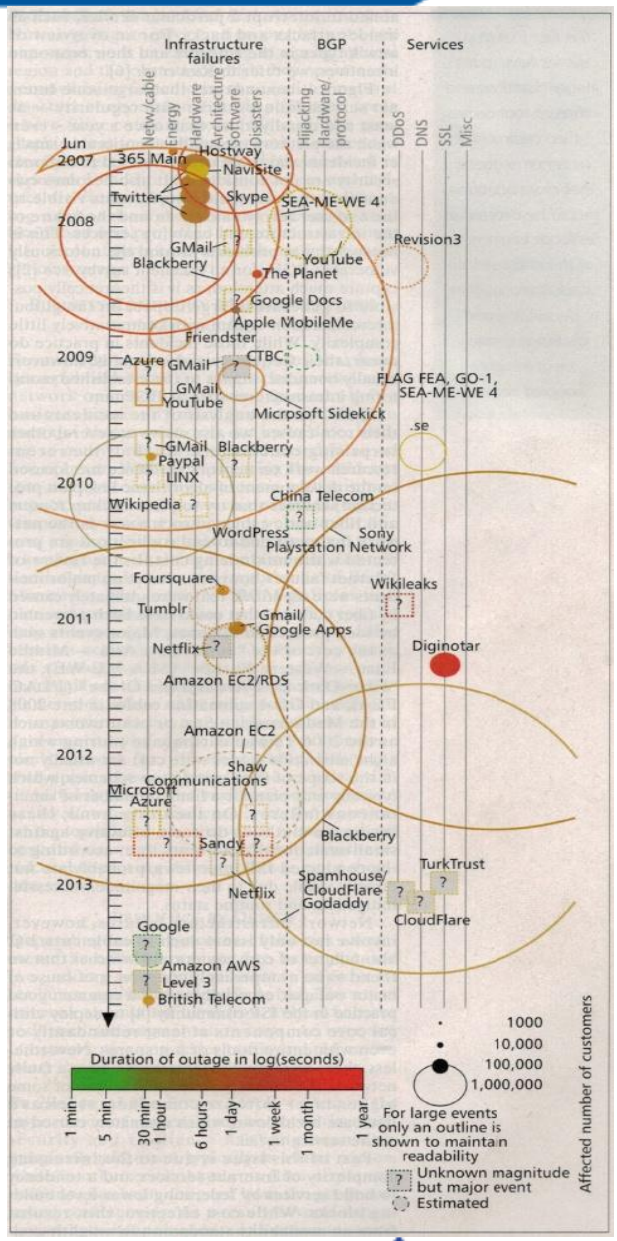
The Study:

- Investigated a broad scale of major (54) Internet failures and analyzed their root cause, frequency, duration, and societal impact
- Categorized/classified the Internet outages as following:
  1. Infrastructure failures
     - Network/cable, Energy, Hardware, Architecture, Software, and Disasters
  2. Border Gateway Control (BGC)
     - Hijacking, Hardware/Protocol
  3. Services
     - DDoS, DNS, SSL, and Miscellaneous (e.g., insider attacks, hacks, etc.)

DDoS: Distributed Denial of Service
DNS: Domain Name Service
SSL: Secure Socket Layer

Example 1: Internet Service Outages (2007-2013) (Continued)

Pictorial Representation of Outages



Example 2: Cloud Service Outages in 2014 (till August 2014)*

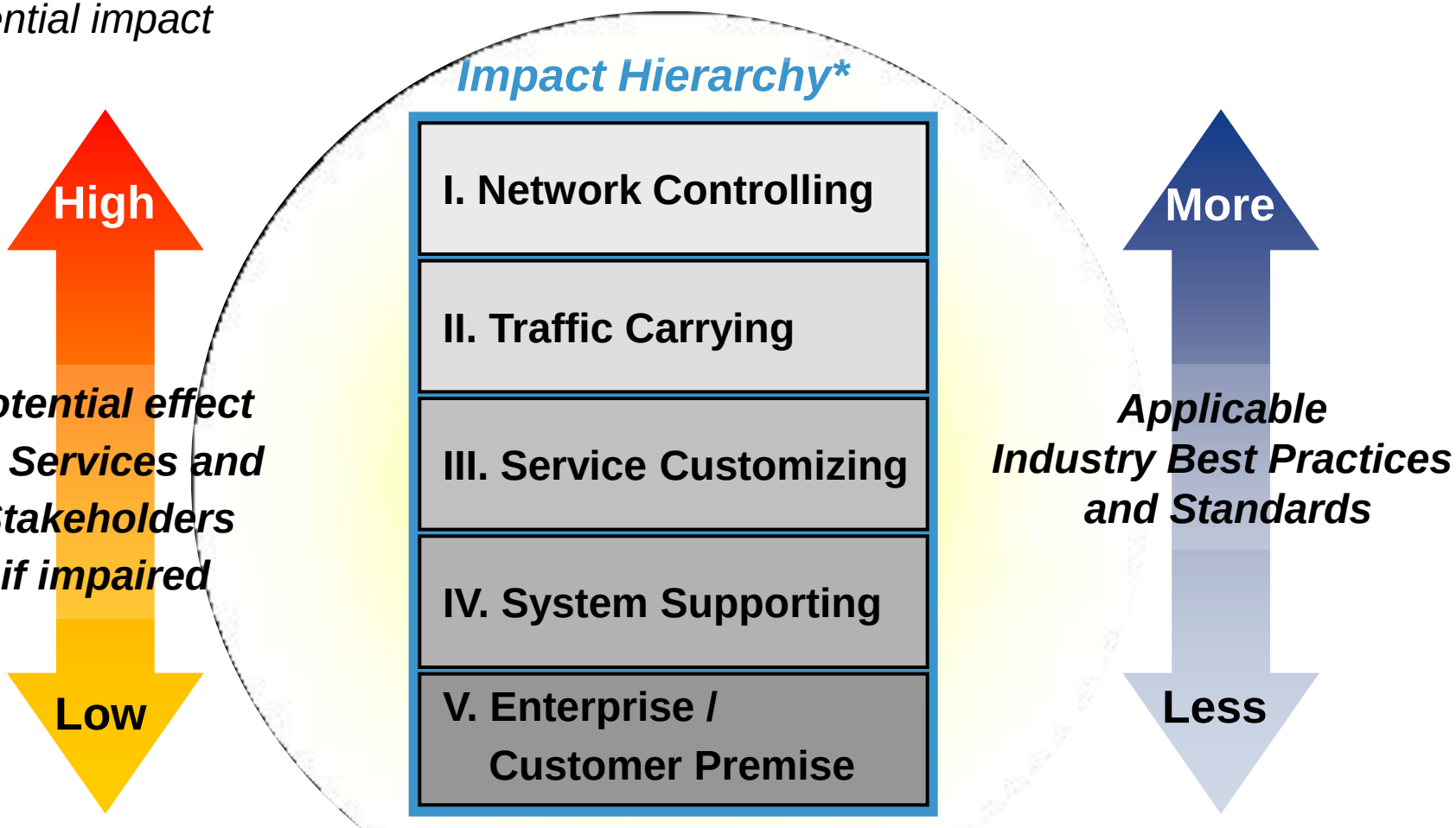
- An article* at the InfoWorld listed the worst Cloud outages in 2014 (till August). Based on high-level information, the cause for the12 listed outages may be attributed to:
  - 3 Denial of Service
  - 2 Improper Procedure
  - 2 “Undefined”
  - 1 Script Error
  - 1 Software Bug
  - 1 Fire
  - 1 “Routing Issue”

Is this ad-hoc root cause analysis, based on incomplete information, a satisfactory way to learn lessons from the cloud service outages?

* Source: J. R. Raphael, "*The worst cloud outages of 2014 (so far)”* InfoWorld, August 25, 2014
http://www.infoworld.com/article/2606209/cloud-computing/162288-The-worst-cloud-outages-of-2014-so-far.html

Impact: Equipment Categorization Framework

A simple concept drives each of the interests: apply rigor in proportion to the potential impact



* Source: The "Impact Hierarchy" was introduced by Alcatel-Lucent Bell Labs Network Reliability & Security Office (NRSO)

IEEE COMMUNICATIONS SOCIETY

IEEE

Etymology Issue Regarding the Naming of a New IEEE Working Group

- Before deciding about the proposing a Working Group name, some care is required in interpreting the literature regarding:
  - reliability
  - resiliency
  - survivability, and
  - vulnerability

  because these terms are sometimes used interchangeably with no warning (see next viewgraphs)

Terms Contrasted: Reliability & Resiliency*

- "….The primary difference is that *resiliency* applies to the functions or services performed by the network, whereas *reliability* is usually used to describe the failure and repair behavior of network elements.
- Network resiliency is an attempt to describe how the reliability of services or applications that run on the network changes when certain parts of the network experience reductions in capacity (possibly stemming from equipment failures, natural disasters, deliberate attacks, etc.).
- Therefore, reliability is an important primitive concept in the construction of network resiliency measures, and such measures incorporate the change in reliability (broadly interpreted) as network conditions change. …"

***** Source: Michael Tortorella, "Design for Network Resiliency", *Wiley Encyclopedia of Operations Research and Management Sciences*, 2010 John Wiley & Sons, Inc.

Terms Contrasted: Resiliency & Survivability*

- "….The related notion of *survivability* has been studied primarily in the telecommunications context .
- The earliest approaches to *survivability* were mainly concerned with the provision of geographically diverse alternate routes so that traffic, which would normally be carried on facilities that could be lost due to natural disaster or deliberate attack, would continue to reach its destination.
- While the amount of traffic that is successfully rerouted and carried is a key indicator of network resiliency, *survivability* studies did not necessarily explicitly incorporate measures of how much traffic would be successfully rerouted.
- Later studies began to incorporate such considerations , and thereby resemble more comprehensive *resiliency* studies…"

***** Source: Michael Tortorella, "Design for Network Resiliency", *Wiley Encyclopedia of Operations Research and Management Sciences*, 2010 John Wiley & Sons, Inc.

Terms Contrasted: Resiliency & Vulnerability*

- "….In a sense, network resiliency is a more complete description of network operation under degraded conditions than network vulnerability.
- For example, certain network elements may be vulnerable to damage to a greater degree than other network elements, but if the consequences of damage to the former are minor in terms of, say, added congestion or other disruptions of the flow in the network, and the service consequences of this flow disruption are also minor, then the network may still be resilient even though vulnerable.
- General considerations aside, network vulnerability would have to be defined precisely, and in quantitative terms, in order to make valid comparisons.
- Any such definition has not yet received wide acceptance..."

***** Source: Michael Tortorella, "Design for Network Resiliency", *Wiley Encyclopedia of Operations Research and Management Sciences*, 2010 John Wiley & Sons, Inc.

Decisions for the SRPSDVE SG to Make

- Should we ask for the formation of IEEE Working Groups?
  If yes, for which one(s)?
  - Reliability, Security, Performance
- Ensure that complementary work is pursued at the IEEE and ETSI SDN/NFV Working Groups as well as other Standards Developing Organizations (SDOs) regarding SDN/NFV/Cloud Computing
- Review the draft PAR(s) and gain a consensus from the SRPSDVE Study Group
- Present the Study Group's recommendation(s) to the IEEE ComSoc Board for their consideration and final decision on the formation or not of new Working Group(s)

Possible Options/Approaches - 1

A future IEEE Reliability Working Group may:

1. Capitalize on the knowledge and lessons learned from previous telecom outage classification and analysis efforts and tailor a suitable scheme for the outages in software defined and virtualized ecosystems (e.g., Cloud Computing, SDN/NFV, NGSON)

In other words…., move from the current ad-hoc (e.g., "InfoWorld") analysis to an *IEEE standardized categorization and analysis methodology* for such outage data

Possible Options/Approaches - 2

2. Establish a voluntary outage reporting database for outages in software defined and virtualized ecosystems (e.g., Cloud Computing, SDN/NFV, NGSON) where, besides the industry, IEEE members around the world may contribute information from:
   - Literary searches in academic and trade articles
   - News websites
   - Blogs, fora, and operator mailing lists about outage incidents

In other words…., provide a source of publicly available outage data for research and periodic reports regarding the "state of the software-defined and virtualized ecosystems" avoiding the need for FCC-mandated reporting of such outages

Possible Options/Approaches - 3

4. Level of Resilience
   - N+1, or N+x
5. Level of Service Availability (e.g., five 9's vs. three 9's)
   - Cost vs. Need for Reliability
6. Use Cases
   - Data Center vs. Mobile
7. Key Performance Indicators (KPIs)
8. Hot Swap
   - E.g., Protocol for Hot Swap of two SDN Controllers
9. Balance in Provision of Reliability
   - Hardware vs. Software
10. Layered vs. Cross-layered

IEEE COMMUNICATIONS SOCIETY

*Source: Mohammad Asad Chaudhry, SRPSDVE Study Group Vice Chair, Univ. of Toronto

IEEE

Possible Options/Approaches - 4

11. Standard requirements for service reliability attributes
    - Accessibility
    - Continuity
    - Release
12. Standard reliability models for SDN/NFV architectures
    - Stochastic Petri net models
        - Failovers
        - Timing
13. Establishment of explicit, quantitative links between service reliability attributes and reliability/behavior of SDN/NFV infrastructures

*Source: Mike Tortorella, Rutgers University

Proposed PAR Text for an IEEE Reliability Working Group Issue Statement based on this Presentation's Topic 1

Issue Statement/Business Need:

Because the availability of communications services is vital for social-economic stability and public safety, the study of the reliability of the emerging software-defined and virtualized ecosystems (e.g., Cloud Computing, SDN/NFV, NGSON) can be very valuable. Since service providers are looking to use network functions virtualization to build dynamic, virtualized networks with application and content awareness they are changing the traditional equipment classification schemes by introducing virtual machines, hypervisors, etc. from many different suppliers. Various systems for classifying network equipment and direct/route causes of service outages currently exist for the communications industry. However, most do not account for advances in SDN/NFV-based network architectures, the new types of systems (e.g., Hypervisor) and failure modes (e.g., OpenFlow protocol). The industry would benefit from an updated standard equipment categorization system and an updated standard classification scheme for direct/route causes used in outage analysis.

Proposed PAR Text for an IEEE Reliability Working Group Issue Statement based on this Presentation's Topic 1

Suggested Solution:

A future IEEE Reliability Working Group should create a standard that offers a categorization of the:

(i) Equipment used in both legacy, converged and emerging technologies networks, and
(ii) Direct/rouse outage causes that would be used in outage classification and analysis of the virtualized networks and associated services.

Proposed PAR Text for an IEEE Reliability Working Group Issue Statement based on this Presentation's Topic 2

Issue Statement/Business Need:

Because there is no official U.S. government database to voluntary report outages occurred in virtualized networks (i.e., similar to the FCC's Network Outage Reporting System – NORS - for outages reported by the telecom service providers), capturing such outages in an IEEE database, would be:

i. Of particular value to the industry for writing Best Practices based on lessons learned , and
ii. Conducive to reliability analysis of virtualized networks from a root/direct cause analysis perspective

Proposed PAR Text for an IEEE Reliability Working Group Issue Statement based on this Presentation's Topic 2

Suggested Solution:

A future IEEE Reliability Working Group should promulgate a voluntary reporting of outages occurred in virtualized networks to be captured in an IEEE database. Besides the industry, IEEE members from around the world may contribute outage information from:

- Literary searches in academic and trade articles
- News websites
- Blogs, fora, and operator mailing lists about outage incidents