系统可生存性研究综述*)

赖积保　王慧强　王　健
(哈尔滨工程大学计算机科学与技术学院　哈尔滨 150001)

摘　要　系统可生存性是信息安全的新研究方向，是对传统安全观念的突破和创新。本文首先给出了开展系统可生存性研究的必要性以及系统可生存性若干定义；基于此，结合可生存性的评测和增强技术研究，从计算系统可生存性、网络可生存性、服务可生存性以及软件可生存性4个角度，综述了可生存性的研究现状，并进行了国内外对比分析；随后探讨了可生存系统的设计与实现问题，最后描述了系统可生存性的发展趋势。

关键词　计算系统可生存性，网络可生存性，服务可生存性，软件可生存性，可生存系统

Survey of Information System Survivability

LAI Ji-Bao　WANG Hui-Qiang　WANG Jian
(College Computer Science & Technology, Harbin Engineering University, Harbin 150001)

Abstract　Information system survivability is a new research direction in information security. It is also a new idea compared to traditional security theory. Firstly, the necessities of developing information system survivability are given. The definition of system survivability is introduced. Then, related with research on evaluation techniques and enhancement techniques of survivability, the summarization of studying situation in the world is presented from computer system survivability, network survivability, service survivability and software survivability. And researches in and abroad are compared. Finally, the design and implementation of survivable system are discussed. The future development of system survivability is described.

Keywords　Comuting system survivability, Network survivability, Service survivability, Software survivability, Survivable system

1　引言

可生存性研究源于军事领域。在计算机领域中，随着日趋严重的网络以及信息系统安全问题的出现，研究人员和机构已经开始意识到开展网络及信息系统的可生存性研究势在必行。Barnes[1]等人于1993年正式提出了计算机领域内的可生存性概念。

尽管关于可生存性的研究已经开展了十几年，但目前尚无一致认可的定义。但CMU/SEI研究小组给出的定义最具影响力，即指在遭受攻击、故障或意外事故时，系统能够及时完成其关键任务的能力[2]。从定义可知，系统可生存能力主要体现在系统遭受到成功入侵、关键部分遭到损害甚至摧毁时，系统依然能完成其关键任务，并能及时恢复被损坏的服务，也即系统可生存性强调的是任务、服务，而不是系统中某些具体的所谓关键部分。

2　可生存性研究现状及分析

在文[3]中并未给出可生存性研究现状综述，着重探讨了可生存系统的设计方法；文[4]采用统计分析方法概述了目前该领域的论文分布情况，也并未给出研究现状详细综述，主要工作侧重于总结可生存性定义要素、测定标准、实现技术，深入探讨可生存系统SSA(Survivable System Analysis)分析方法，对比可生存性的两种不同实现方法。而本文在上述工作的基础上，从计算系统可生存性、网络可生存性、服务可生存性以及软件可生存性四个角度进一步详细综述可生存性研究现状，如图1所示，涵盖了可生存性的体系结构、系统模型、系统分析与设计、增强技术、系统评价与测试等。

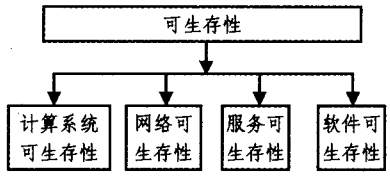

图1　目前可生存性研究分类

2.1　国内外研究现状

自Barnes[1]等人于1993年首次提出信息系统的“生存性”概念开始，1996年DARPA/ITO的项目“信息生存”在Howard Shrobe领导下开展，随后几年SEI/CERT共同举办了四次(1997-2002)信息生存研究会ISW(Information Survivability Workshop)，在1999年生存性作为商业/风险管理的观点第一次被引入到美国计算机学会新的安全范例研究组(ACM New Security Paradigms Workshop)。文[5]中涉及的“关键基础设施保护的信息可生存性”项目给出了生存体系结构方面的研究。Semir Daskapan[6]等人将移动代理技术应用到SNS中，研究智能移动代理如何增强系统的可生存性。国内方面，陈左宁[7]在研究大规模计算机系统可信性技术时，指

*)基金项目：高等学校博士学科点专项科研基金项目(20050217007)。**赖积保**　博士研究生，研究方向为计算机网络、信息安全；**王慧强**　教授，博士，研究方向为可靠性理论、计算机网络；**王　健**　博士研究生，研究方向为信息安全。

出系统可生存性的关键技术，欲通过建立系统可生存模型，实现以自我配置、自我恢复、自我优化以及自我保护为特征的自主计算。林闯[8]在提出可信网络概念的基础上，分析了安全性、可生存性和可控性之间的联系。文[9]提出了利用多样化动态漂移技术来达到生存性的系统框架设计。王慧强[10]提出了开展面向关键任务的分布式信息系统可生存性研究，建立了基于PST的分布式信息系统可生存性模型，并给出了相应的评估方法。973项目[11]中的"海量信息的协同性和可生存性的理论与实践研究"，在其六项主要研究内容中有四项与可生存性有关，依次为：①实时流媒体协同可生存的海量信息系统的试验和验证平台；②可生存的海量信息系统设计理论；③海量信息系统生存性分析方法及软件可生存性增强技术；④海量信息系统可生存性策略和测评方法研究。

服务可生存性用于刻画系统在异常条件下继续提供关键服务的能力。国外在这方面研究主要是针对光纤网络、无线网络等领域来展开的，尤其是在光纤网络的服务可生存性方面研究取得了较大的成果。文[12]在分析了无线网络所面临的问题后，结合各层协议的特点，提出了一种基于策略的动态自愈恢复机制，实现无线网络的服务可生存性。A Keromytise[13]等人提出了多层协作的可生存性框架结构——SABER，提供一种实现服务可生存性的整体方案。文[14]中提出采用动态资源定价策略(dynamic resource pricing strategies)缓解各种DDoS攻击，并改善服务可生存性。国内研究主要围绕各种应用系统中的服务可生存性定量分析及改进方法来展开，目前还处于探索阶段。文[15]在给出服务可生存性大小比较的充要条件基础上，定义了系统服务间的依赖关系，借助于传统与或树概念，将服务用与或结构表示来分析服务的生存性，探索出一种服务可生存性的定量表达方法。在文[16]中分析了ATM网络中各种服务不同的生存重要性基础上，引入了故障恢复过程中的资源剥夺，并改进了预先的空闲容量规划，形成了新的生存性资源管理机制。在文[17]中作者设计了一个基于NTP的附加协议SANP，并着重讨论了恶意攻击下的服务生存性问题。

软件可生存性用于刻画软件在异常情况下继续完成关键任务的能力。在这方面的研究国外主要是围绕着结构、测试方法、增强技术等方面开展的。David Wells[18]等人研究新的软件机制确保系统可生存性，提出了基于OSA的软件结构，并采用适应性和易构建(ease of construction)对基于OSA应用进行描述。Anup K. Ghosh[19]等人在分析了软件可生存性研究的必要性基础上，指出传统软件测试方法的不足，提出了基于故障注入的"off-nominal"测试方法，旨在增强软件的可生存能力。在文[20]中，作者提出了采用快速软件组件迁移的方法实现软件可生存性。国内复旦大学的协同信息与系统实验室[21]目前承担的"海量信息系统可生存性分析方法及软件可生存性增强技术"项目，以提高软件的可生存性为核心目标，研究相应的模型、结构、分析方法和增强技术。主要研究内容包括：①建立无界网络环境中SOA软件系统的生存力统计学模型和无锁(服务)副本控制模型；②研究满足高可生存性要求的、基于服务的软件构架，以及软件结构对软件部署的影响；③研究出现算法，对邻近可视(服务)任务进行分析，包括对入侵、故障、事故和性能的监测；④通过调整软件服务部署、采用自迁移技术和副本技术，提高软件的可生存性。与此同时，在2006年国家自然科学基金委员会信息科学部与微软亚洲研究院联合资助项目中，拟对"软件可生存性策略设计方法以及可生存软件的规范理论、需求分析和设计方法[22]"给与资助。

在增强系统可生存性研究方面，国外主要是从系统设计的角度来考虑的。CMU/SEI的CERT/CC[2,23]将系统划分成不能攻破的安全核和可恢复部分，然后针对一定的攻击模式，给出相应的抵抗、识别和恢复策略。文[24]中介绍了可生存性系统设计的螺旋模型，该模型基于传统软件工程中的瀑布模型和螺旋模型，并加入了可信系统的一些概念。文[25]提出用异构网络来增强网络生存能力的解决方案，探索系统地增加网络的异构性而不牺牲互操作性，文中提出了多样化空间、多样化距离以及不全等的网络元素之间互助时功能的弥补等问题。宾州大学的Luenam P[26]等人介绍了一种在原系统中加入入侵检测和响应技术来增强系统可生存性能力的方法，并根据这种方法设计了入侵容忍数据库系统ITDR(Intrusion Tolerant Database System)。国内主要是在现有系统设计基础上，从性能优化角度来研究。文[27]提出了系统信息冗余分散的二部图模型，通过分析点覆盖集与可存活性之间的联系，改善了冗余系统的可存活性。文[28]提出了以多样化分布式动态备份技术和随机漂移机制为手段的生存能力增强技术模型。上述国内外研究方法可以不同程度地增加系统的实时检测和响应能力、重配置能力或冗余能力来提高系统的可生存能力。但是在这些解决方案中，对攻击、异常的检测、评估以及重新配置的执行，都需要人为介入，存在不同程度的时延。针对可生存系统的自适应响应、恢复和演化能力的增强还没有涉及。

在系统可生存性评测方面，目前还未有统一的标准，也尚未取得突破性进展。其中，比较有代表性的是CMU/SEI的CERT/CC研究中心提出的SSA方法[5,29]，但它是一种定性的分析方法，未能提出一个可靠的综合各性能评估的数学模型，因而难以对网络系统的生存能力做出准确的评价和比较。卡耐基·梅隆大学的Soumyo D. Moitra[30]等研究如何对系统的可生存性进行量化分析，并开发一套仿真模型，用来评估各种网络防御机制的开销和网络遭受攻击后预期的生存能力之间的权衡。文[31]以银行电子支付服务的生存性分析为例，基于故障场景图(fault scenario graph)，即一种改进的故障树进行分析，由于场景图的数量众多使得这种方法难以用于复杂系统。文[32]提出了基于问题空间转换思路，将系统生存性分析转换为图的某种典型问题求解的方法框架。上述系统生存性的定性分析，往往对具体的系统生存能力判断不够准确；定量评估都是研究者按照自己的理解和思路给出的评估框架，缺乏统一、公认的标准，且主要针对的是系统局部或特定系统，还没有形成一套系统的方法。

2.2 国内外研究对比

国外在系统可生存性方面的研究起步比较早，尤其是美国，针对关键基础设施(包括电力网、传输、电信、医疗、银行、金融及国防等系统)的可生存性问题开展了专门、系统的研究，并取得了一些阶段性的成果，如系统可生存性的SSA分析方法、体系结构、增强技术等方面[2,5,23~26,29~32]，这为进一步开展研究工作奠定了坚实的基础。此外，欧洲可靠性组织EDI也开始致力于关键基础设施的保护和可生存性领域的研究。

就国内研究现状而言，尚属起步阶段。无论从技术还是资源方面，与美国相比还存在很大差距。但目前系统可生存性研究已受到足够的重视。2005年国家自然科学基金委员

会分别对“计算系统可生存性理论及其关键技术研究”和“网络可生存性研究”[33]进行了资助。与此同时,“网络可生存性和可信可控的安全服务研究[34]”作为2005年度973计划的重要支持方向予以支持。2006年,在国家自然科学基金委员会信息科学部与微软亚洲研究院联合资助项目[22]中,拟开展软件可生存性方面的研究。基于此,研究人员在可生存性的分析与需求定义、可生存性定性定量分析方法以及可生存性增强技术等方面[7~10,15~17,27~28]取得了一定的成果,这为进一步开展该领域的研究奠定了基础。

纵观国内外研究,可生存性研究目前主要还是处在理论研究阶段,并且在不断地吸收容错、入侵容忍、健壮性等研究思路。

3 可生存系统分析

构建合理高效的可生存系统必须从系统需求分析着手,全面客观分析所涉及到的问题,并逐一进行解决,才能最终实现满足需求的可生存系统。

3.1 可生存系统需求分析

可生存系统需求分析是设计和实现可生存系统的前提和基础。可生存系统需求受系统使用范围、重要程度、服务停止或中断造成的后果严重程度不同的影响,一般包括有系统功能需求、软件质量需求和可生存性需求,具体可细分为以下五种需求[29,35]:

(1)系统/可生存性需求。系统需求侧重关注系统必须提供的基本功能,也包括效率、性能、可靠性等非功能性需求;可生存性需求则主要包括识别抵抗入侵、系统的自愈恢复以及自适应等需求。

(2)使用/入侵需求。系统服务的入侵使用和合法使用都是基于使用模式的,而使用模式的基础就是使用需求。

(3)开发需求。可生存系统的开发和测试要求非常严格。一旦出现软件错误或功能设计不当,都会给入侵者提供可乘之机,因此规范合理的开发需求对于实现可生存系统也是至关重要的。

(4)操作需求。可生存性操作需求通过系统操作和管理需求定义,主要包括可生存性策略定义和传递、系统实时监控、入侵报警与响应、系统自适应等功能。

(5)演化需求。系统演化需求主要受用户功能需求变动及入侵攻击策略演变的影响。尤其对于入侵攻击,要求可生存系统的演化速度快于入侵者知识的提高。

可生存系统的核心是维持关键服务,而为了维持这些关键服务,可生存性系统必须具备四个关键特性:抵抗能力、识别能力、可恢复性、自适应性。

3.2 可生存系统设计方法

可生存系统设计主要有两种思路:一是设计全新具有可生存能力的系统,将可生存性需求作为系统设计的必要先决条件,贯穿于系统开发设计的整个生命周期。常用方法有SSA分析方法[5,24,29]。二是在原有系统基础上,加入可生存性增强技术,实现系统可生存性。常用技术有冗余异构技术、完整性验证技术、自主配置技术以及入侵容忍技术等。对于第一种设计思路而言,目前还处于理论研究阶段,而且成本非常高;而对于第二种思路而言,可操作性较强,且成本较低。

4 可生存性研究趋势

系统可生存性作为信息安全领域的一个新研究方向,有很大的发展潜力。在理清国内外的相关研究基础上,结合分析研究,将其发展趋势简单归纳如下:

(1)统一对可生存性的各种理解和认识,形成一致的定义和描述;

(2)制订可生存性需求分析过程、方法和描述等标准,形成系统化、工程化的可生存性需求分析和开发过程;

(3)制订统一的测定标准,为可生存性研究提供标准化的测定依据;

(4)改进和完善已有理论框架,建立可生存系统的体系结构,形成高效的可生存性系统开发方法和实施过程;

(5)建立一个适当的模拟环境,用于可生存性模拟测试分析,改进和完善系统的可生存能力;

(6)采用理论指导实践的办法,建立实际的可生存系统。

总之,可生存性研究将朝着系统化、标准化、应用化方向发展。

结论 开展系统可生存性研究对于提高大规模系统的可生存能力具有重要的现实意义。本文通过综述计算机系统可生存性、网络可生存性、服务可生存性以及软件可生存性,旨在把握国内外研究动态,明确不同层次实现可生存性所涉及的理论问题及关键技术,为进一步开展研究奠定基础。

参 考 文 献

1 Hollway B A, Neumman P G. Survivable computer-communication systems: The problem and working group recommendations [R]Washington: US Army Research Laboratory, 1993

2 Fisher J, Linger R. Survivability: protecting your critical systems [J]. IEEE Journal of Internet Computing, 1999, 3(6): 55~63

3 张永,方滨兴,等. 网络可生存性研究概述[J]. 计算机工程与应用,2005, 41(7): 119~121

4 张鸿志,张玉清,等. 网络可生存性研究进展[J]. 计算机工程,2005,31(20): 3~5

5 Srikitja A, et al. On Providing Survivable QoS Services in the Next Generation Internet[R]. Supported in Part by NSF Grant NCR9506652 and DARPA under Agreement No. 1730602-97-1-0257

6 Daskapan S, Vree W G. Self-organizing trust principle for survivable systems[C]. IASTED International Conference on Artificial and Computational Intelligence, Tokyo, Japan, 2002. 7~12

7 陈左宁. 大规模计算机系统可信性技术的研究[J]. 高性能计算技术,2004, 6: i001~i004

8 林闯,彭雪海. 可信网络研究[J]. 计算机学报,2005, 28(5): 751~758

9 黄遵国,卢锡城,胡华平. 生存能力技术及其实现案例研究[J]. 通信学报,2004, 25(7): 137~145

10 Wang H Q, Liu D X, et al. A holistic approach to survivable distributed information system for critical applications[C]. In: The Proc. of ISPA'2005, Nanjing, China, Published in Springer's Lecture Notes in Computer Science, LNCS 3758. 2005. 713~724

11 关于国家重点基础研究发展计划973计划[EB/OL]. http://www. 973. gov. cn/mana/contfile/web/234/20051271353429a. doc, 2005.

12 Kant L, Chen W. Service survivability in wireless networks via multi-layer self-healing [C]. In: Wireless Communications and Networking Conference, 2005 IEEE Volume 4, 2005. 2446~2452

13 Keromytis A, et al. A Holistic Approach to Service Survivability [C]. In: Proceedings of the 2003 ACM workshop on Survivable and self-regenerative systems • : in association with 10th ACM Conference on Computer and Communications Security, 2003. 11~20

14 Mankins D, Krishnan R, et al. Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing[C]. In: Proceedings of the 17th Annual Computer Security Applications Conference, 2001. 411~421

15 郭渊博,马建峰. 分布式系统中服务可生存性的定量分析[J]. 同济大学学报:自然科学版,2002, 30(10): 1190~1193

16 王东霞,窦文华,周兴铭. 保证关键服务生存性的ATM网络资源管理[J]. 计算机研究与发展,2000, 37(1): 50~54

(下转第275页)

系统，开发过程是不完整的、未经确认的。可以预期的将来，如果能有标准的构件质量定义，生产者复用和消费者复用的过程才是可以分割的。

5.2.4 本评估模型同 IEEE1517、CMMI、RCM、RMM、OOSPICE 等评估模型的联系

本模型建立过程中，参考了 RCM、RMM 以及 OOSPICE 的基于复用程度的评估方法及其对部分级别的定义。在过程方面同 IEEE1517 的软件复用开发过程存在共同之处——符合综合复用等级的复用指导过程；同 IEEE1517 的完整复用过程之间，存在内涵等同的对应关系。该模型同 CMMI 之间无直接关系，但建议应用本模型的企业首先实施 CMMI，来提升企业的软件开发能力，然后再实施模型来提升软件复用能力。

总结和展望 本文以软件复用能力评估和改进相关的工业实践和研究情况为基础，提出了一种面向过程改进的系统的软件复用能力评估框架。该框架为企业面向复用的开发过程提供了一种阶段式的评估框架，通过能力等级和关键过程域的划分，帮组企业识别和改进自身的软件复用开发能力。

对该模型来说，主要的问题就是尚未对关键过程域展开进一步细化，包括如何识别过程域满足的条件、过程域的主要表现方法以及部分过程域的可选内容。这部分是下一阶段工作的主要内容研究之一。

模型的另一个问题是缺乏对实际软件企业的复用能力改进指导的示例性研究，下一阶段的研究工作也包括这部分的内容。

在本文的研究过程中，结合国家 863 计划项目（特征驱动的领域分析、体系结构建模技术及支持工具研究）进行了电子行业标准——企业构件化能力成熟度模型的制定，该标准的申请工作已经基本完成。

参 考 文 献

1 CMMI Product Team. Capability Maturity Model Integration. CMMISM for Software Engineering. Staged Representation. 2002. 8

2 Stallinger F, Dorling A, Rout T, et al. Software Process Improvement for Component-based Software Engineering: An Introduction to the OOSPICE Project. In: the 28 th Euromicro Conference (EUROMICRO 02). 2002

3 Davis T. The Reuse Capability Model: A Basis for Improving an Organization Reuse Capability. IEEE, 1993

4 Mili H, Mili F, Mili A. Reusing Software: Issues and Research Directions. IEEE Transactions on Software Engineering, 1995(6)

5 Institute of Electrical and Electronics Engineers Inc. (ISO/IEC 12207) Standard for Information Technology: Software Life Cycle Processes. United States of America, 1998. 3

6 Institute of Electrical and Electronics Engineers Inc(IEEE 1517). IEEE Standard for Information Technology: Software Life Cycle Processes - Reuse Processes. United States of America. 2004. 3

7 Morisio M, Ezran M, Tully C. Success and Failure Factors in Software Reuse. IEEE Transactions on Software Engineering, 2002(4)

8 Morisio M, Ezran M, Tully C. Comments on "More Success and Failure Factors in Software Reuse". IEEE Transactions on Software Engineering, 2003(5)

9 Ezran M, Morisio M, Tully C. Failure and Success Factors in Reuse Programs: a Synthesis of Industrial Experiences. ICSE 19991

10 Koltun P, Hudson A. A Reuse Maturity Model

11 Zahran S. Software Process Improvement: Practical Guidelines for Business Success. Pearson Education, 1998

12 Menzies T, Di Stefano J S. More Success and Failure Factors in Software Reuse. IEEE Transactions on Software Engineering, 2003(5)

13 BiggerstafS T J. Reuse Technologies and Their Niches. ICSE 1999 1

14 Frakes W, Terry C. Software Reuse: Metrics and Models. ACM Computing Surveys, 1996(6)

15 Frakes W B, Kang K. Software Reuse Research: Status and Future. IEEE Transactions on Software Engineering, 2005(7)

（上接第 239 页）

17 包秀国，蒋宗礼，等. NTP 自主配置的自组织途径[J]. 计算机学报，2005，28(5)：759～766

18 Wells D, et al. Software Survivability[C]. In: Proc. DARPA Information Survivability Conf. and Exposition (DISCEX), IEEE Computer Soc. Press, Los Alamitos, Calif., Jan. 2000, 2: 241～255

19 Ghosh A K, Voas J M. Inoculating Software for Survivability [C]. Communications of the ACM, 1999, 42(7): 38～44

20 Choi B K, Rho S, Bettati R. Fast software component migration for applications survivability in distributed real-time systems[C]. Object-Oriented Real-Time Distributed Computing. In: Proceedings. Seventh IEEE International Symposium on, 2004. 269～276

21 协同信息与系统实验室. 海量信息系统可生存性分析方法及软件可生存性增强技术[EB/OL]. http://cscw. fudan. edu. cn/main_project. htm, 2006

22 国家自然科学基金委员会与微软亚洲研究院联合资助项目[EB/OL]. http://www. nsfc. gov. cn/nsfc/cen/xmzn/2006xmzn/06lh/102. htm, 2006

23 Knight J C, Sullivan K J, et al. Survivability architectures: issues and approaches[C]. DARPA Information Survivability Conference and Exposition, 2000. DISCEX'00. ProceedingsVolume 2, Jan. 2000. 157～171

24 Linger R C, Lipson H F, et al. Life-Cycle Models for Survivable Systems[R]. Sledge TECHNICAL REPORTCMU/SEI -2002-TR-026

25 Zhang YG, Vin H, et al. Heterogeneous Networking: A New Survivability Paradigm[C], NSPW'01. Cloudcroft, New Mexico, USA, 2001. 33～39

26 Luenam P, Liu Peng. The design of an adaptive intrusion tolerant database system[C]. Foundations of Intrusion Tolerant Systems, 2003 Organically Assured and Survivable Information Systems, 2003. 14～21

27 李之棠，舒承椿. 基于信息冗余分散的两种系统可存活性模型[J]. 计算机研究与发展，2002，39(7)：769～774

28 包秀国，胡铭曾，张宏莉. 两种网络安全管理系统的生存性定量分析方法[J]. 通信学报，2004，25(9)：34～41

29 Ellison R, Fisher D, et al. Survivable Network System Analysis: A Case Study[J]. Software, IEEE, 1999, 16(4): 70～77

30 Moitra S D, Konda S L. A Simulation Model for Managing Survivability of Networked Information Systems[R]: [CMU/SEI -2000-TR-020]. 2000

31 Jha S, Wing J M. Survivability Analysis of Networked Systems [C]. In: Proceedings of the 23rd International Conference on Software Engineering (ICSE), 2001. 307～317

32 Kring W. A Graph Based Model for Survivability Applications [EB/OL]. http://www. cs. uidaho. edu/krings/publications. html. 2006

33 徐琳，刘志勇，等. 国家自然科学基金委员会信息科学部计算机科学处 2005 年度基金申请与资助概况[J]. 软件学报，2005，16(11)：2021～2028

34 邵立勤. "十一五"期间国家科技发展重点方向[EB/OL]. http://sche. dlut. edu. cn/news/ download/fazhanfangxiang. doc, 2006

35 Ellison R, David A, et al. Survivable Network System: An Emerging Discipline [EB/OL]. http://www. sei. cmu. edu/publications/documents/, 1999