

# The Principles of System Survivability

**Alexandra DRAGOMIR**

University Politehnica of Bucharest

a\_dragomir@hotmail.com

## Abstract

*Nowadays, the society is growing increasingly dependent upon large-scale, highly distributed systems that operate in unbounded network environments. Unbounded networks, such as the Internet, have no central administrative control and no unified security policy. The number and nature of the nodes connected to such networks cannot be fully known. Despite the best efforts of security practitioners, no amount of system hardening can assure that a system that is connected to an unbounded network will be invulnerable to attack. Furthermore, organizations and individuals alike want their technology to survive attacks, failures, and accidents, but the technology in computer systems, software, and network infrastructure components changes frequently and is vulnerable to disruption. The discipline of survivability can help ensure that such systems can deliver essential services and maintain essential properties such as integrity, confidentiality, and performance, despite the presence of intrusions.*

**Keywords:** information system, survivability, SKiP

## References

- [1]. Ellison, Robert J. 2002. "Survivable Network Systems: An Emerging Discipline." Technical Report.
- [2]. [http://www.cert.org/info\\_assurance/principles.html](http://www.cert.org/info_assurance/principles.html).
- [3]. <http://www.sosresearch.org/>.
- [4]. Longstaff T. 2001 "A Case Study in Survivable Network System Analysis".
- [5]. Nancy, Mead R. 2005 "Security Quality Requirements Engineering Methodology".
- [6]. Ellison, Robert J. 2004 "Security, Survivability and Architectural Design Tactics" Technical Report.
- [7]. Lawrence, Rogers R. 2004. "Survivable Functional Units: Balancing an Enterprise's Mission and Technology".
- [8]. Nancy, Mead R. 2010 "Survivable Network Analysis".
- [9]. <http://en.wikipedia.org/wiki/Survivability>.
- [10]. <http://www.cert.org/research/papers.html>.