

# Defending Complex Systems Against External Attacks

Gregory Levitin

*The Israel Electric Corporation Ltd., Haifa, Israel  
levitin@iec.co.il*

**Keywords:** defense, attack, game, protection, separation, redundancy, false target

Defending against intentional attacks is fundamentally different from protecting against accidents or natural cataclysms. Adaptive strategy allows the attacker to target the most sensitive parts of a system. Choosing the time, place, and means of attacks, the attacker has always an advantage over the defender. Therefore, the optimal policy for allocating resources among possible defensive investments should take into account the attacker's strategy. The defense measures include separation of system elements, their protection, deploying separated redundant elements as well as false targets.

A survivable system is one that is able to complete its mission in a timely manner, even if significant portions are incapacitated by attack or accident. This definition presumes two important things. First, both the impact of external factors (attacks), and internal causes (failures), affect system survivability. Therefore it is important to take into account the influence of the availability of system elements on the entire system survivability. Second, a system can have different states corresponding to different combinations of failed or damaged elements composing the system. Each state can be characterized by a system performance rate, which is the quantitative measure of a system's ability to perform its task. For example, the performance rates of a power generating unit, production line, and communication channel represent generating capacity, productivity, and bandwidth respectively. The system success is defined as its ability to meet a demand (desired performance rate).

This paper presents a review of recent research [1-10] based on combining risk and survivability analysis with game theory and aimed at optimizing the defense against unintentional and intentional attacks.

## References

1. Intelligence and impact contests in systems with redundancy, false targets, and partial protection, G. Levitin, K. Hausken. *Reliability Engineering & System Safety* 94 (12), pp. 1927-1941 (2009).
2. Intelligence and impact contests in systems with fake targets, G. Levitin, K. Hausken. *Defense and Security Analysis* 25, pp. 157-173 (2009).
3. Protection vs. false targets in series systems, K. Hausken, G. Levitin. *Reliability Engineering & System Safety* 94, pp. 973-981 (2009).
4. Redundancy vs. protection vs. false targets for systems under attack. G. Levitin, K. Hausken. *IEEE Transactions on Reliability* 58 (1), pp. 58-68 (2009).
5. Minmax defense strategy for complex multi-state systems. K. Hausken, G. Levitin. *Reliability Engineering & System Safety* 94, pp. 577-587 (2009).
6. False targets vs. redundancy in homogeneous parallel systems. G. Levitin, K. Hausken, *Reliability Engineering & System Safety* 94, pp. 588-595 (2009).
7. False targets efficiency in defense strategy. G. Levitin, K. Hausken, *European Journal of Operational Research* 194, pp. 155-162, (2009).
8. Protection vs. redundancy in homogeneous parallel systems. G. Levitin, K. Hausken, *Reliability Engineering & System Safety* 93, pp. 1444-1451, (2008).
9. Optimal defense strategy against intentional attacks, G. Levitin, *IEEE Transactions on Reliability*, 56(1), 148-157 (2007)
10. Survivability of systems under multiple factor impact, E. Korczak, G. Levitin, *Reliability Engineering & System Safety*, 92(2), pp. 269-274 (2007).