Integration of Probabilistic Reasoning and Technology Assessment to Evaluate the Susceptibility of Electronic Systems by High Power Electromagnetics

Edward T. Toton[1], Ira Kohlberg[2], Michael Frankel[3]

[1]Toton Incorporated, 11417 Hollow Timber Court, Reston, VA USA, e-mail: etoton@comcast.net

[2]Kohlberg Associates, Inc., 11308 South Shore Road, Reston, VA USA, e-mail: ira.kohlberg@gmail.com

[3]Astra Analytics, LLC, 900 Clintwood Drive, Silver Spring, MD USA, e-mail: michael.frankel@AstraAnalytics.net

Abstract

A major challenge facing the information systems community in dealing with the susceptibility and vulnerability of integrated systems is to develop an investment strategy that address the threat of terrorist-employed High Power Electromagnetic weapons. The assessment of risk is attractive for guiding decisions in the evaluation of low risk – high consequence events. To what extent can a formal methodology be developed when there are uncertainties and risks in complex systems and when subjective assumptions must be made in the evaluation process? This paper addresses quantification of risk for electronic systems when these are susceptible to widespread electromagnetic effects.

1. Introduction

Many modern civilian and military systems take well over a decade to become operational and deployable. Within this period there can be dramatic changes in technology and in the political climate, many of which can't be predicted. A system concept that looks exceptionally promising today may find little application by the time it's built. Making the right decisions over a decade-plus time period is extraordinarily difficult. This is particularly true in dealing with the development of High Power Electromagnetic devices and defending systems against these weapons. We need to develop a methodology for making the best decisions based upon constantly changing conditions. This is somewhat like aviation planning and execution problem, i.e., we need to plan a course based on the best available forecast conditions, yet plan for unexpected developments that can change the course to the destination, or perhaps even change the destination. What should be our approach? First, we must recognize that we are dealing with uncertain events that fundamentally require a probabilistic perspective. With a probabilistic point of view we must recognize that there are three essential components: technology, i.e., technology elements chosen to provide system functionality through potential HPEM threats, evidence, i.e., any data that may be available to give confidence that system components and functions may be able to survive potential EMP threats, and a methodological framework for providing quantification of survivability and confidence in survivability estimates.

2. Methodology

Risk is frequently proposed as a useful metric as the basis for an investment strategy. We might plan the development of HPEM resistant electrical infrastructures, for example, and the discipline of a formal quantification of risk could reveal weaknesses that suggest hardening strategies. Simply put, where the risk is high, greater investment should be made. But the term *risk* can be used in a number of different ways, and it is useful to understand the different meanings. In general conversation one might hear the question "What is the risk of one being involved in a fatal automobile accident?" Here risk is used in the sense of a probability; one can easily substitute *probability* for *risk* in this question without change of meaning. Inherent in this meaning is a temporal factor. The question implicitly includes a phrase such as "in the next year" or "in the next trip." Many Americans regarded the risk of a second, catastrophic terrorist attack in the United States immediately after September 11 very high and, no doubt, they would have raised their estimates if a period of five years from the date of the first attack were to be considered.

The estimation of risk of damage from terrorist or rogue nation employment of HPEM weapons requires a methodology that recognizes that little data are available for complex systems for exposure to HPEM waveforms and that virtually no data exist for HPEM interactions with known systems. Such a methodology must therefore rely on an understanding of the architecture, the physical interconnection of components, and of how electromagnetic energy

infuses and interacts with such systems. Since much uncertainty exists in any characterizations of these interactions, and since the data are sparse to non-existent, it is apparent that a probabilistic methodology that incorporates expert opinion as well as data as they become available has the required characteristics.

A methodology that offers such characteristics was first developed under sponsorship by the Nuclear Regulatory Commission in response to a congressional mandate to assess the risk of catastrophic failure of the domestic nuclear reactor power plant. This resulted in the publication of the report *Reactor Safety Study*, otherwise known as the Rasmussen Report [1]. The elements of the methodology include the construction of fault trees that reveal the logical interconnectedness of the hardware components that support the functions of the power plant (inclusive of containment of nuclear material), the assignment of failure probabilities to each of the hardware components identified in the fault trees, and the mathematical evaluation of the overall probabilities of failure based on these elements.

Those practiced in the discipline of probabilistic risk assessment have turned to those tools to characterize the exposure of US assets to intentional terrorist disruption. The formal application of the probabilistic risk assessment methodology provides a framework for producing numerical estimates of the probabilities of failure or, in the case of terrorist attack, the probabilities of success on the part of terrorists or success of detection and mitigation on the part of asset protection systems. An example of the latter is found in a recent paper (*A Risk Assessment Methodology for Intentional Chemical and Biological Contamination of Distribution Systems*) which presents a conceptual model: "Structured as an event tree representing potential contamination entry points at various places in the supply chain, decisions related to where and how resources should be allocated to deterrence, detection and response can be evaluated" [2].

In his book *Normal Accidents* [3] Perrow discusses in enjoyable detail the forensics of a large number of catastrophic accidents ranging from airline transport accidents to nuclear reactor accidents. In the case of the nuclear accident at Three Mile Island Perrow discusses the factors leading to a core meltdown in which human factors led to the overriding of automatic safety systems with little time for recovery. That is, the "tightness" of the interactions in the complex operating and safety systems produced a system that could deteriorate rapidly with little time available for human thought and prudent intervention to take place (the problem with pressurized boiling water reactors is that there is only a window of about 30 seconds before there is a catastrophic loss of coolant, should the cooling system be breached). But a far more important lesson can be taken from this accident. In the pre-accident risk assessment for meltdown, the analysts never contemplated the possibility of the formation of a hydrogen bubble at the top of the reactor core vessel. The hydrogen bubble that did in fact form in the Three Mile Island reactor core vessel forced coolant down and uncovered the reactor core itself, leading to the meltdown. That is to say, the probabilistic risk assessment methodology was formal, comprehensive, and quantitative, yet its predicted results overlooked a fundamental reaction mode that was realized in the accident. This is a fundamental problem in studies that are inherently survivability oriented such as that of Three Mile Island (and other nuclear power-plant reactors) and domestic infrastructure risks. That is to say, any quantified risk assessment inherently generates risk values that are *underestimates* of the true probability of failure of the systems in question, owing to overlooked and unknown risk factors.

The assessment of risk continues to be an attractive endeavor to guide decisions in the evaluation of low risk – high consequence events. The question before us is to what extent a formal quantification methodology can be developed when there are uncertainties in the description of complex systems, unknowns in the risks, however small, and when subjective assumptions must be made in the evaluation process. The effort suggested here is a first step in developing a methodology that could provide some quantification of risk, an understanding in a general sense of how risk might be reduced in complex systems, and a traceable formal process that provides a basis for defensible evaluations of risk.

Probabilistic risk assessment is inherently Bayesian in its structure and philosophy. Where data are plentiful, probabilities are virtually independent of expert opinion; where data are sparse, expert opinion must be relied upon in order to produce quantified estimates of risk. But it must be recognized that there is little other choice when addressing catastrophic risks when no such events have been observed. As with the nuclear power industry before Three Mile Island, risk projection had to be based entirely on the understanding of reactor systems and component-level failure probabilities, some of which could be quantified by fault testing. For future projections of infrastructure survivability under HPEM attack, much reliance must be similarly placed on the response of technology components and on the system architecture.

3. Technology

Here we mean all those technologies that are currently integrated into infrastructures such as a power grid or telecommunications systems, and those that could be adopted to reduce the risk of catastrophic failure. The critical infrastructures on which the functioning of modern society is dependent are susceptible to disruption, degradation, or destruction by HPEM upset and damage of electronic components. In power grids the critically important relays that protect the very long-lead replacement time circuit elements, such as the very high voltage transformers, are increasingly of digital electronic design and susceptible to HPEM damage. A worrisome scenario envisions a series of simultaneous attacks on geographically separated elements of the electric grid by such electromagnetic weapons which may produce a cascading failure of large sections of the grid. The data centers and operational control centers that enable the accounting and daily flow of trillions of dollars through our financial and banking systems are enabled by computers and other electronic elements that are intrinsically susceptible to EMP environments. Similarly, transportation control centers as well as switches that control railroad track function all contain digital electronic systems susceptible to HPEM energies. Thus a terrorist in possession of such a means would find himself in a very target rich environment.

The electric power grid depends on unhardened Supervisory Control and Data Systems (SCADAs) monitoring systems to detect and respond to problems. These modern SCADAs are increasingly deployed within every nook and cranny of our modern electronic based critical infrastructures. Their function is to automatically monitor and remotely control the operation of geographically far flung systems such as the electric power grid, the pumps on our oil and gas pipelines, or our national telecommunications infrastructure. These ubiquitous control units confer great economic benefit and enormous operational agility, but are essentially unhardened computers – electronically quite similar to the personal computers found on every desk - which have been demonstrated to be highly sensitive to HPEM radiation. In the 1980s catastrophic failure of a SCADA system controlling flow in a natural gas pipeline located one mile from the naval depot of Den Helder in the Netherlands caused a large gas explosion in a 36" diameter pipeline. This failure was caused by electromagnetic interference traced to an L-band naval radar coupling into the wires of the SCADA system. Radio frequency energy caused the SCADA system to open and close at the radar scan frequency, a relay that was, in turn, controlling the position of a large gas flow-control valve. The resulting changes in valve position created pressure waves that traveled down the pipeline and eventually caused the pipeline to fail. A similar gas pipeline explosion in Bellingham Washington was also traced to the failure of SCADA control. In an incident ultimately traced to the operation of a Navy AN/SPS-49 radar system 25 miles off the coast of San Diego, the radar induced failure of a SCADA system controlling the opening and closing of water and gas flow valves led to the subsequent letter of complaint by the San Diego County Water Authority to the Federal Communications Commission, warning of a potential "catastrophic failure" of the aqueduct system. The potential consequences of a failure of this 825 million gallon per day flow rate system ranged from "spilling vents at thousands of gallons per minute to aqueduct rupture with ensuing disruption of service, severe flooding, and related damage to private and public property."

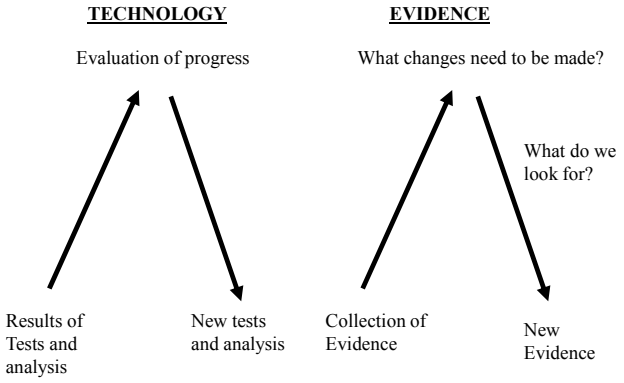
The discipline of the probabilistic risk assessment methodology requires the assembly of a systems-level representation of the probability of continued operation with assignments of probabilities of failure for each of the subsystems and their components to adverse HPEM environments. The overall probability of failure or survivability can be estimated through numerous mathematical strategies for complex systems. More importantly, however, is the awareness obtained of the interdependency of components and subsystems that may be strongly coupled, in the words of Perrow, as revealed in the conditional probabilities that are assigned by analysts in the absence of direct evidence, or resulting from subsystem studies in the form of data. Where strong coupling is detected, efforts can be applied to effect reduced coupling by systems architecture or hardware re-engineering.

4. Technology and Evidence

Little systems level evidence exists for widespread infrastructure failure from EMP attacks, and certainly none due to terrorist attack. On the other hand, there have been power grid failures resulting from coronal mass ejection (CME) events that produce the long-term HPEM effect of inducing large currents in long power transmission cables that have triggered shutdowns in the Northeast corridor of the United States. Such events suggest the possibility of failure of high voltage transformers by driving them into saturation. And, of course, there have been no widespread failures due to EMP or HPEM induced failures in SCADA systems, for example. This sparse data base allows us, nonetheless, to refine expert opinion in the overall evaluation of risk of catastrophic failure from HPEM attacks.

A significant feature of the probabilistic formalism is that the end result, indicating whether a system alteration or replacement should be adopted gives meaningful and quantifiable weight to the evidence factor. The process of development of system hardware configurations should come about iteratively, whereby each stage of design can be tested mathematically or in a small scale setting to develop data about system survivability. Lessons learned then result in modifications of the system design. The roles of Technology and Evidence are shown in the figure below.

TECHNOLOGY AND EVIDENCE



One aspect of the problem of system-level susceptibility is the extensive interconnectedness of infrastructures such as the power grid control system and telecommunications. A possible strategy for modeling such complex systems is to investigate the degree to which such system architectures are amenable to systems describable with the tools of percolation theory. If mappings can be identified between complex infrastructure architectures and fundamental abstract interconnected systems, then general conclusions of the susceptibility to catastrophic collapse can be inferred from percolation theorems. The assignment of probability to interconnectedness and tightness of coupling could then yield insight into the degree of dependence to which susceptibility of infrastructures may depend on details of subsystem hardware and system configuration.

5. Conclusion

The probabilistic methodology discussed here provides a likely starting point for developing predictions of the survivability of complex infrastructure systems susceptibility to HPEM attacks. It features the organized and traceable collection of system design, subsystem and component level hardware configurations, and it allows prediction of the response of such systems to postulated attacks. Understanding the interaction of elements of these architectures can lead to the identification of weaknesses that contribute to overall system collapse; this leads to the identification of what hardening strategies might be implemented such as specific hardware modifications and architecture changes. Furthermore, the complexity of such large systems suggest the possibility of representation of these as realizations of abstract architectures for which the power of percolation theory can be brought to bear. In all of this, we are faced with making predictions when the data base is sparse, expert opinion is essential, and data, as they are collected, can refine our predictive capability. A demonstration of this methodology will appear in a subsequent paper.

5. References

1. US Nuclear Regulatory Commission, *Reactor Safety Study*, Main Report (October 1975).

2. Spradley, Leah, Abkowitz, Mark, and Clarke, James, "A Risk Assessment Methodology for Intentional Chemical and Biological Contamination of Distribution Systems" *JHSEM*: Vol. 3 [2006], No. 3, Article 2.

3. Perrow, Charles, *Normal Accidents,* Princeton University Press, 1999.