SAND98-2829C

POTENTIAL DISADVANTAGES OF MICROTECHNOLOGY FOR FUTURE HIGH CONSEQUENCE SAFETY APPLICATIONS

Perry E. D'Antonio, J. Arlin Cooper, Stanley D. Spray, Michele Caldwell, and John M. Covan

Sandia National Laboratories*
Albuquerque, NM 87185-0490

ABSTRACT

Microtechnologies (e.g., microelectronics, and micromachines) are useful and promising for many applications. However, since the small size and specialized materials of electronics in general and microtechnologies in particular appear to make them sensitive to many normal and abnormal environments, and since complete characterization of the newer technologies is lacking, they must be used with extreme caution in high consequence safety applications. Based on what is now known, we believe that they should not be proposed for high consequence safety applications, particularly for nuclear weapons detonation safety.

* Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

INTRODUCTION

The development of new microtechnologies such as nanoelectronics and micromachines is exhilarating, and one is inclined to expect that applications may be plentiful. However, for some applications, including those involving high consequence operations, there are dangers in the use of both new and conventional electronics and microtechnologies that may not be immediately obvious. As independent assessors, the authors investigate this concern. For example, technologies that are extremely sensitive to electrical, electromagnetic, radiation, and contamination environments must be used with great caution where their functionality can affect safe operation.

This paper first acknowledges the attributes of some of the existing and new technologies that are being developed and outlines the reasons that their application in high consequence safety systems is so frequently proposed [1]. A general coordinated approach to safety assessment is outlined, and this approach is then applied to microtechnologies (solid-state microelectronics and micromachines).

MICROTECHNOLOGY CONTRIBUTIONS TO SYSTEM PERFORMANCE

Among the important potential contributions offered by microelectronics and micromachines are for any given system function to be performed, reductions in volume, weight, power consumption, and cost, along with increases in operating speed are realizable. Some implementations also provide enhanced reliability in some operating environments, and mass production capability may be enhanced for mature technologies. Along with this has come reduced sensitivity to some operating environments (e.g., shock, vibration, acceleration). Unfortunately, there is also increased sensitivity to many other environments. This problem will be addressed in a subsequent section.

System designers justifiably want to utilize the considerable advantages of the new technologies. A system that can be made smaller, cheaper, faster, more reliable, and more producible is obviously attractive. Many implementations involving the new technologies have increased immunity to limited environments. For example, most electronic wristwatches are now more immune to vibration and shock; and are more reliable than mechanical watches. But in severe environments, caution is warranted. For example, heat can make electronics non-functional and cold can make electronic displays non-functional. A general concern involves the possibility that the advantages might be overpowered by the disadvantages in some applications.

INDEPENDENT SAFETY ASSESSMENT

Systems engineering is intended to assure that systems provide the optimal benefits of meeting customer satisfaction, which may include meeting cost, reliability, and performance objectives, and not endangering safety. However, the main training and focus of system engineers is on meeting stated requirements (which sometimes bow to what is doable, not what is really desirable). Safety assessors are trained in failure

DISCLAIMER

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

analysis (how things fail and the consequences of failure), and are responsible for looking beyond the requirements to look for safety "cliffs" and extreme situations (e.g., emphasizing the "tails" of probability distributions). A prime consideration is that the independent assessors have a considerable understanding of the system design considerations. A concise expression of this is that there must be *knowledgeable independence*.

For these reasons, independent safety assessment is important in the development of new technologies that may be intended to have roles in safety applications. The added values of such assessments are that a different set of "eyes" can be brought to bear, looking for phenomena that may have been missed, personnel who are familiar with failure analysis can be utilized, an "audit trail" of assessment results can be made, and the assessment can be uniform (applicable to all technologies). It is important that the independent assessment process be flexible enough to allow new product development and application (where appropriate), and the assessment must be balanced, looking for positives as well as negatives.

An outline of the recommended engineering development process is shown in Fig. 1. This is the model we examine in independent assessment [2]. An essential "umbrella" that permeates all of the indicated activities (in addition to an unbiased independent assessment posture) is a strong safety "culture." Safety culture, a bottom-to-top organizational attitude about responsibility for safety, is absolutely necessary. The commitment to safety must be evident at all levels of the organization. The culture assures that assessments are reported to and taken seriously by the highest management levels and are truly independent (the assessors feel no management pressure to compromise safety principles or seek popular decisions). Safety culture is helped by management awareness and buy-in at the earliest stages of projects so that managers will recognize consequences and understand responsibilities. They must be a willing to make unpopular decisions when necessary. There must be openness and communication in all directions. There must be a respect for others' opinions and willingness to debate. In a good culture, designers welcome and even seek out independent assessment views. All of these contributions cannot be achieved without considerable effort.

The first process step shown in the figure is to develop or identify system objectives. In this paper, we will focus on safety objectives. For high consequence systems, these objectives are to remain assuredly safe in all normal (specified operation) and abnormal (outside specified operation) environments. For systems that already exist, these objectives may be stated as desired improvements—like the goal of reducing the aircraft accident rate by 80% in 10 years. For nuclear weapons, our objective is to manage energy release – contain the potential energy during peacetime and release the (nuclear) energy when and only when desired.

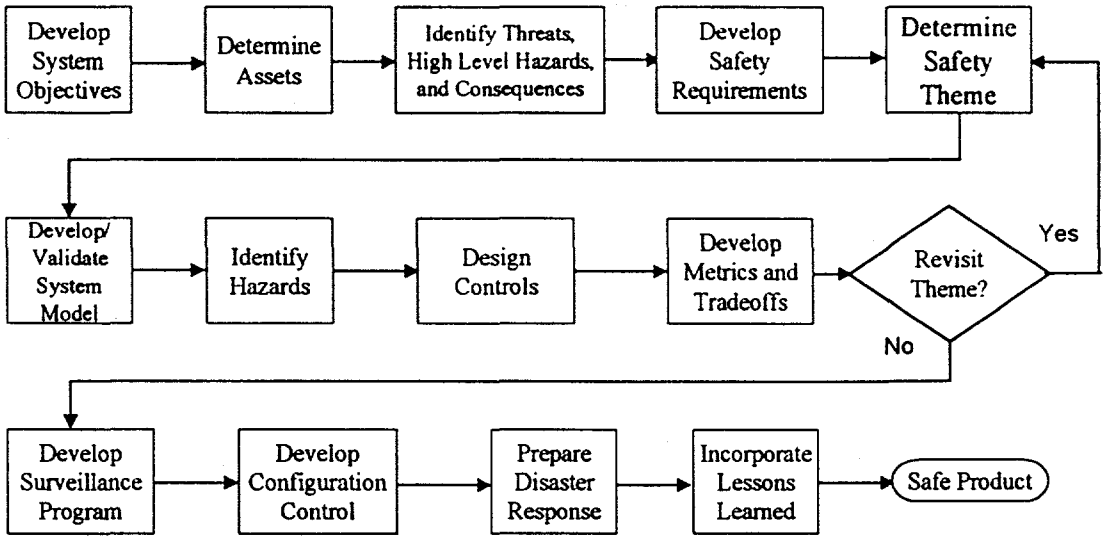

Figure 1. High Consequence System Safety Engineering Process

There are two types of assets to protect—those within the system and those outside the immediate system. The latter assets may include human well being, environmental protection, monetary assets, company reputation, and even organizational survival. The former are utilized to achieve the system objectives.

The "threats" are entities that might degrade assets (e.g., crush, lightning, EMR, radiation, temperature, aging). The high-level hazards are the general ways in which threats can degrade assets leading to undesired consequences. The consequences are used to evaluate adequacy of controls. The safety requirements recognize the consequences while establishing metrics for protecting the assets when not in use and for utilizing the assets to meet system objectives when and only when desired. For nuclear weapons, this step provides detailed requirements for energy management, since reducing threat energy (e.g., potential, kinetic, thermal) to a safe level, whether applied directly, through physical degradation, or human action, is always a safety goal.

Determining the "safety theme" [3] means identifying an overarching strategy for meeting the safety requirements and concentrating the implementation in a minimal set of "safety-critical" controls. For example, the nuclear detonation safety theme has been to isolate weapon detonators from electrical energy through physical barriers that shield against direct or electromagnetic electrical penetration. Since this isolation may be compromised in severe abnormal environments, some "inoperability" features (system assets critical to detonation that become irreversibly incapacitated due to "first principles" physical response) are co-located with the barriers so that they are subject to the same environmental threats. In this way, the "value" of assets is permanently removed in the desired way. The strategy is that no active measures need be taken to guarantee a fail-safe response.

In order for such a protected system to be used (e.g., an intended weapon detonation to take place), a "stronglink" gateway through the barrier is provided, such that the gateway can only be opened by an engineered "unique signal" [4]; not compromised by spurious signals that may be present in an accident.

A theoretical system model, overlaid by a lessons learned model, allows study of the implementation of the safety theme. Although it is tempting to model the system before this process step, it is generally much more productive to wait until the foundation of the previous steps is in place to ensure the important parameters are included and then validated in the model. In conjunction with the system model, specific hazards are identified and tested against "safety-critical" controls (design features intended solely or principally for safety and on which safety depend). Using the system model, metrics are developed to test the system against its safety requirements, and to weigh possible tradeoffs (although in the nuclear weapons program, nuclear detonation safety has the highest priority among competing tradeoffs). If the theme is judged robust at this point, the remainder of the process is established (surveillance, disaster response, and incorporation of lessons learned).

There are several key contributors to this process. One of the techniques that have been developed is to emphasize "first principles" (basics laws of physics and chemistry) in assessing expected behavior. Because these principles are not subjective and do not depend on probabilistic estimates, there is higher confidence in and justification for analysis and testing. Also, the safety assessments are more widely understood and accepted. The intent is to assess based on safety-critical controls that can be assured and to depend as little as possible on statistical expectations.

When new technologies are proposed to replace existing technologies, it is useful to consider advantages and disadvantages of both technologies from the viewpoint that each new technology developed may have features that are advantageous to safety, but also may have disadvantages. Also, new technologies may be susceptible to a larger threat population.

A GENERAL SAFETY ASSESSMENT OF MICROELECTRONICS AND MICROMACHINES

The small size of microtechnology and nanotechnology provides opportunities to not only decrease size and cost, but also to increase reliability and producibility. However, one of the salient observations regarding these technologies is that *different* vulnerabilities to abnormal environments (and in some cases normal

environments) are typically introduced[1]. The concern is that microtechnology is more sensitive to energy due to small size, and thereby makes energy management less assured.

The High Stakes

In nuclear detonation safety, the assets to be protected are the detonation-critical components. On a broader scale, the assets are national or even global (welfare and health of people, national defense posture) and therefore are of prime national importance. Great care is required to assure that no accident, situation, or unforeseen circumstance can cause an inadvertent nuclear detonation. This combination of extremely high value assets and severe environments makes our national safety requirements very stringent (the probability of an inadvertent nuclear detonation must be less than one in a million, *given* any credible abnormal environment or combination of environments[2]).

Increases in the Threat Space

The list of hazards that can result from normal and abnormal environments appears to be much larger for solid state components than for the electromechanical components that are currently used in nuclear weapons safety systems. For example, solid state components are generally more vulnerable to electrical effects, radiation, temperature, gases, contamination, and chemicals, all of which could insult a weapon system during its lifetime. Whether microelectronics or micromachines, the salient issue is ability of these components that are sensitive to small amounts of energy to protect against large amounts of energy.

The Concern with Sensitivity

A general observation is that the more sensitive the components in a protected region, the harder it is to isolate from compatible energy sources and the harder it is to design appropriate isolation/inoperability protection features. Although there is no readily identified level of concern, a primary consideration is: **"How sensitive is *too* sensitive?"**

[1] Electronics in general is not excluded from this assessment.

[2] A partial list of environments includes shock, vibration, acceleration, crush, puncture, extreme heat/cold, water, chemicals, gases, lightning, EMR, EMI, EMP, ESD, magnetic coupling, radiation, vacuum, contaminating particles, and aging effects, all caused by human action or natural effects.

A Judgment

This judgment is qualitative, and it is important to note that few applicable tests or analytical studies on the myriad of sensitivity questions involved have been conducted to date. However, based on current information, we assert that:

Since microtechnology has not and probably cannot be demonstrated to respond in a predictable way to energy management, there appears to be a considerably higher safety risk of using these components as high consequence system safety controls, particularly because of their sensitivity to a large number of potential environmental threats.

SUMMARY

The apparent non-safety advantages of miniaturized solid state components must be weighed against their less obvious, but highly vital safety risk. For many normal environment situations (e.g., information management), and possibly for some abnormal environment systems whose safety performance is considered low consequence, these devices may be useful. **For high consequence systems, especially those that must remain safe in abnormal environments, the safety risk does not appear to warrant their use.**

REFERENCES

1 "A Manufacturing Method for Multi-Layer Polysilicon Surface-Micromachining Technology," J. Sniegowski and S. Rodgers, GOMAC, March 1997

2. "Structured Design and Assessment of Safety Systems Based on Principles," S. Spray and A. Cooper, PSAM 4, September 1998

3. "A Study of Using Electronics for Nuclear Weapons Detonation Safety," M. Caldwell and P. D'Antonio, AIAA-98-3465

4. "The Unique Signal Concept for Detonation Safety in Nuclear Weapons," S. Spray and A. Cooper, Sandia National Laboratories SAND91-1269, June 1993