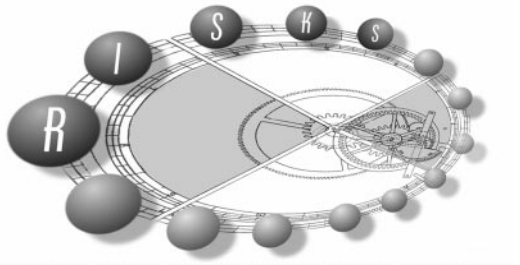
Inside



Harold W. Lawson

Infrastructure Risk Reduction

The FBI and U.S. Attorney General Janet Reno recently announced plans to establish a National Infrastructure Protection Center. Critical processing and communication structures are to be protected against hackers and criminals. Given today's IT infrastructure complexity, I'm sure that attaining reasonable effectiveness will require an enormous personnel and equipment investment.

In addition to dealing with malicious acts, infrastructure reliability and availability is vital. The recent Alan Greenspan disclosure of a New York bank computer failure a few years ago makes me shudder. The Federal Reserve bailed the bank out with a $20 billion loan. Greenspan admitted that if the loan could not have been supplied, or if other banks simultaneously had the same problem, the entire banking system could have become unstable. Such information outages are probably common, but, as with this case, covered up to avoid public panic.

How far away are we from major catastrophes? What would happen if, due to outages, international companies start defaulting on debt payments resulting in business failures? International information outages could make power and telecommunication outages seem like small inconveniences.

These and many other related risk questions lead me to conclude that a concerted effort aimed at infrastructure risk must come to the absolute top of national and international political and commercial agendas.

While there are many sources of risk, there is an undeniable relationship between risks and complexity. Thus, a major part of risk mitigation must be aimed at reducing complexity.

Today's computer-communication-based system structures are layered with unnecessary complexity. This unnecessary complexity is partially, but significantly, due to the mapping of application functions through levels of languages and middlewares onto poor or inappropriate platforms of system software and hardware.

Mainstream microprocessors require large quantities of complex software to be useful. This is not a new situation. Even the earlier mainstream IBM 360/370 series suffered in this regard. There is a significant semantic gap between useful higher levels of problem solving (via programming languages) and the instruction repertories of these machines.

That current RISC and CISC processors are poor hosts for higher level languages perpetuates the motivation to widely deploy lower levels of programming, including C and C++. This adds unnecessary complexity, the cost and risk of which is borne many times over in developing and especially in maintaining the growing mountain of software.

In my opinion, complexity and risk reduction must focus on restructuring of the hardware and system software infrastructure components. Restructuring must address programming languages, suitable system software functions, and, most importantly, well-defined (verifiable) execution machines for the languages and functions. Further, robust security mechanisms must be integrated into the infrastructure backbone. The restructuring must result in publicly available standards that are strictly enforced via independent certification agencies.

The vital IT infrastructure cannot continue to be based upon products that are *caveat emptor*. Enforced standards do not eliminate the competitive nature of supplying infrastructure components; nor do they hinder creativity in introducing a virtually unlimited number of value-added products. Standards increase the market potential for good products. For safety-critical, computer-based systems in areas such as nuclear energy, aviation, and medical instruments, certification against standards is applied. However, even for these critical embedded systems, there is a need for tougher standards as well as complexity reduction via appropriate architectural structuring of hardware and system software.

Given the fact that today's suppliers of critical infrastructure components swear themselves free from product responsibility, an insurance-related enforcement solution may be appropriate, analogous to the Underwriters Laboratory certification of electrical products. Before infrastructure products are put on the market, they must be certified against standards in order to limit (but not eliminate) supplier product responsibility and instill public confidence.

It is time to stop quibbling over trivial issues such as Internet browsers. When catastrophes occur, browsers will seem like small potatoes. Today, we can do fantastic things with electronic circuitry. We must tame this potential and do the right things aimed at reducing infrastructure risk. It is time to take the bull by the horns and find a political and commercial path leading to infrastructure restructuring and enforceable standards. C

HAROLD W. (BUD) LAWSON *(bud@lawson.se) is an independent consultant in Stockholm. He is an ACM and IEEE Fellow.*

PAUL WATSON