ITAR CONSTRAINTS ON FREE TECHNICAL INTERCHANGE

The letter from R.S. Chang, in Computer’s October issue, regarding the cost of conferences made me think about what other constraints might prevent US engineers from attending conferences.

In my line of work, conferences once were a meaningful place to share and discuss our findings and experience and to improve our knowledge through interaction with our peers. Our large unnamed aerospace company used to gladly pay exorbitant fees and travel expenses to send us forth with meaningful papers. We US engineers used to write about mission data processing, failure tolerance, new algorithms, new protocols, high-assurance software, the strange architectures we work with, and so on, but our output has all but dried up in recent years.

As I scan the many conferences in my field, it is notable that the majority of useful recently published technical papers originate either from academic sources or from overseas. Today when we US engineers publish, mandatory compliance with the International Traffic in Arms Regulations (ITAR) invariably means that the information that survives censorship is generic. The information “exported” cannot by law improve test methods, cannot reveal “nonpublic” design or implementation details or “nonpublic” use of open source software, cannot discuss algorithms that are not in the “public domain,” and cannot improve anyone’s process. The term nonpublic requires multiple paragraphs of legal definition.

My US peers and I encounter many interesting topics in our projects that no longer find their way to conferences. To publish, or even have a conversation about, any of those details would require an export license from the State Department, an expensive process requiring a minimum of three months, and impossible from the standpoint that every person to whom I might “export” my information would need to be a signatory to the license agreement.

In short, those of us who are not associated with an academic institution and with the cover of a PhD (ITAR does not restrict “academic freedom”), or those of us who are not “foreign persons,” are essentially prohibited from improving the state of the art in our field.

Clyde Helms
chelms@socal.rr.com

SURVEILLANCE AS A SERVICE?

In reading “Dynamic Privacy in Public Surveillance” (S. Moncrieff, S. Venkatesh, and G.A.W. West, Sept. 2009, pp. 22-28), I was particularly interested in the description of East London residents who seemed to be more attracted to viewing public surveillance footage than to watching popular TV programs, which resulted in increased reporting of crime. I would be interested in information about the reporting statistics, specifically in relation to the time of day and age of viewers who have volunteered. (I suppose that during working hours, retirees are those who might be of help in doing surveillance.)

Although there are differences between viewing surveillance footage from public places (streets, bus stations, or the like) and from semiprivate spaces (like corridors in buildings with separate private apartments or small offices), it might be interesting to know if the residents of apartment buildings would be willing to share some of their free time by viewing the activities of visitors in the building’s hallways.

As an example, my household recently was burglarized while we were away during the working hours. Despite having two locks on the apartment door and another on the building’s main entrance doors, the thieves entered my apartment without being noticed by a single neighbor from the 32 apartments in our eight-floor building. Afterwards, some ideas about installing video surveillance of the main entrance were offered because another apartment on the next floor was also burglarized on the same day.

Despite all those plans, I wonder if an average homemaker or a retiree would be motivated to spend some time watching the corridors instead of viewing the endless soap operas on TV. If the answer is negative, the issue is whether the installation of a CCTV system would be cost-effective, especially in cases where the persons in charge of controlling such systems operate other businesses during the day. I have also heard about some CCTV surveillance systems being offline (say, without enough tape, hard-disk space, or whatever) just in those moments when incidents occurred. With that in mind, I wonder if we should educate our fellow neighbors to activate their brains to be online too, not relying solely on technology with enough backup storage.

In addition, it would be interesting to see some comments or articles related to distributing home surveillance footage over existing cable TV installations and the positive or negative experience with using such systems for collective safety.

Miroslav Skoric
skoric@computer.org

The authors respond:

There are several useful resources regarding the Shoreditch digital...
bridge program, the most significant being the RAE report “Dilemmas of Privacy and Surveillance Challenges of Technological Change” (www.raeng.org.uk/news/publications/list/reports/dilemmas_of_privacy_and_surveillance_report.pdf). Residents in Shoreditch were given access to a digital TV channel that enabled them to monitor local surveillance cameras. The following source was used regarding the popularity of access to surveillance in comparison to TV programs: www.theregister.co.uk/2007/11/11/home_tv_cctv_link. Information concerning the effectiveness of providing access to surveillance in reporting incidents is detailed in the Parliamentary Office of Science and Technology Postnote, 321 (www.parliament.uk/documents/upload/postpn321.pdf).

While giving the access to CCTV proved successful in Shoreditch, the functionality was left out when extending the digital bridge concept to other areas due to privacy concerns. This creates an opening for the extension of privacy in public surveillance. If privacy measures were enacted prior to public access, the infringement on privacy would be reduced. Further, by accessing public surveillance cameras, people would become more aware of the level of monitoring within their local area. This relates to the importance of reciprocity, as outlined in the RAE report cited above.

As to the efficacy of supplying surveillance footage to the public, it would appear that watching such footage might prove popular. Consider, for example, the popularity, and effectiveness, of the scheme in the digital bridge project. There are also several websites around the world that offer access to webcam and surveillance footage. Such sites appear to be popular, as gauged by the notoriety of the recent iSpy iPhone application, which gives access to such cameras via the phone. Finally, if curiosity or civic duty are lacking as motivation, a company called Internet Eyes is offering financial incentives for watching surveillance footage and reporting potential crimes.

**MATHEMATICAL KNOWLEDGE AND PRACTICE**

In his message titled “Defining Computer Engineering” (Letters, Nov. 2009, p.6-7), Harry Gilbert conjectures that we really don’t need mathematics for “computer engineering” (presumably, he means software engineering or computer programming). This is true; trial and error, design patterns, and other ad hoc nonmathematical approaches can get the job done partially and inefficiently. But, ad hoc approaches are rapidly becoming economically disadvantageous, and such approaches have no place in modern safety-critical systems. Properly applied, mathematical knowledge and practices can make the process thorough and efficient.

“Brain-numbing bureaucratic functions … get it all signed, and you are done” is not engineering; it is ignorantly misusing and abusing the classical systems engineering design control process. Correctly implemented, that process is iterative and one of the earliest agile methods. It clarifies what we want to build (design inputs or requirements), how we are going to build it (design outputs or specifications), and once built, it (1) verifies if we built it how we said and (2) validates if we built what we said. It can be on 3 × 5 cards or on a monstrous database, as long as all are clear about the “whats” and “hows.”

Engineers certainly do “intuitive” and they also do cockpits. Human factors engineering (HFE), one of four subdisciplines of industrial engineering, depends heavily on work in biology, psychology, and sociology. What seems intuitive to you is probably not intuitive to all of us. This well-known hubris is a classic example of ignoring the body of HFE knowledge. And, yes, HFE also relies on mathematics and statistics.

The software development community’s successes and failures on mathematics and statistics. Properly applied, mathematical knowledge and practices can make the process thorough and efficient.

“What CAN AGILE DO?”

I urge all readers of Computer who are involved with software to also read IEEE Software. If they had been doing that, they could recall that some time ago, Barry Boehm showed that nonfunctional requirements (NFRs) were key to success, and how a bad specification of NFRs leads to failure.

One way to guarantee bad NFRs is to just let them happen as a by-product of slinging code instead of being logically determined in advance with a tradeoff analysis that considers the entire system.

This should be self-evident, so it is a puzzlement why anyone would claim that agile can do everything and that those who argue against it reflect thinking of decades ago. If old thinking is correct and new ideas are nonsense, then that is a compliment. I doubt the agile guys meant that though.

Just because somebody used agile successfully once does not mean that it is the right solution for all problems. I grant that there are small
problems where agile is useful. But we still need to determine the actual transition point between methods good for instantiating small, simple, preceded, linear, scalable problems and those needed for large, complex, unprecedented, nonlinear, unique problems. We need to know where that transition point is and why it occurs so we do not mess up with larger projects because we used a faulty approach that could not succeed.

Boehm showed that bad NFRs doom a project to failure. So, can any agile proponent tell us how the proper NFRs can be determined, if at all, except through long, expensive trial and error, if agile methods are used? NFRs need to be determined by a systems architect before a software architecture has been created, and certainly before any coding starts, unless the cost of failure is so small that the expense of planning cannot be ignored.

When the unintended consequences have already unleashed the alligators on your swamp-draining efforts, it is too late. Wasn’t that a problem with the waterfall model that agile was supposed to avoid?

William Adams
williamadams@ieee.org

Imagine a teenager excited about technology

Every innovative, life-changing idea comes from someone’s imagination.

The IEEE Foundation provides resources to advance education, innovation and preservation. Make a gift—and imagine the difference you can make.

Donate today at www.ieeefoundation.org or through your IEEE dues renewal.

We welcome your letters. Send them to letters@computer.org. Letters are subject to editing for style, clarity, and length.