Appliances and Software: The Importance of the Buyer's Warranty and the Developer's Liability in Promoting the Use of Formal Methods

Daniel M. Berry

Computer Science Department, University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
dberry@csg.uwaterloo.ca
http://www.cs.technion.ac.il/~dberry

Formal Methods Not Being Used

Formal methodologists continue to bemoan the failure of practicing software engineers (SEs) to employ formal methods (FMs) in their daily software (SW) development work.

Early attempts by formal methodologists to convince SEs to use FMs focused on benefits to SW quality that would accrue if FMs were used in SW development.

Despite Benefits

Surely, once a SW practitioner understood the benefits, he or she would start to use FMs enthusiastically.

To fail to do so would be illogical!

Illogical or not, SEs by and large, ignored FMs.

Forced Use

When forced to use FMs, they resist and sometimes actively subvert the application of FMs to do meaningless busy work.

When the project fails, due to the subversion, they gleefully blame the FMs for the failure.

Successful Experiments

Successful experimental applications of FMs to real projects failed to convince most SEs of the effectiveness of FMs.

Perception is that project team got lucky or had other strengths going for it or ...

that the project had abnormal special security or safety needs that could not be handled with ordinary methods.

Making FMs More Attractive

Formal methodologists began exploring ways to make FMs more attractive.

Making FMs More Attractive

Most of these were technical solutions aimed at making

- the formal language,
- the method,
- the tools, etc.

- more palatable,
- more easily used,
- more powerful,
- more automatic,
- less ambitious,
- more realistic,
- more incremental, and
- even more fun.

Making FMs More Attractive

Each paper about one of these new approaches

- bemoans the lack of general use of FMs,
- diagnoses the lack as the result of some particular problem in the use of FMs, and
- offers a new approach that avoids, mitigates, or solves the identified problem.

FMs Still Not Being Used

However, none of these has had any real effect on the extent to which FMs are used.

Others try educational, sociological, and managerial approaches.

They too have failed to produce the desired bandwagon.

Even Non-FMs Not Being Used

For example, *SW inspection*

Lots of empirical evidence of inspection's effectiveness at finding faults before execution

It's considerably more effective than traditional testing.

Sadly, many organizations are reluctant to commit the 15% more resources it costs, giving very creative excuses for not using inspection, even when they know its effectiveness.

Other Engineering Disciplines

When we look at other engineering disciplines, we see that they all have their FMs.

Civil Engineering

Civil engineering has mathematical models of load and stress.

These allow calculating from only the paper design for a bridge, whether the proposed bridge will support the required weight, and then some.

Electrical Engineering

Electrical engineering has mathematical models of circuitry.

These allow calculating from only a circuit diagram, whether the proposed circuit will behave as required, will not overheat, etc.

Other Engineers

We see that engineers in these disciplines routinely apply their FMs with

- no complaints of being overburdened with useless work,
- no complaints of their creativity being stifled, and
- no complaints of having to use the dull, dreaded *mathematics* in another field.

The Questions

1. What makes the engineers in the other, more traditional engineerings, apply their FMs routinely, and

2. Can whatever does the trick in these other engineerings be used to get SEs to use SW engineering (SEing) FMs in their daily SW development?

Goal of Talk

Explore the quality of different engineering products, some electromechanical, some electronic, and some SW.

Note key differences in the warranties offered with these products and the liabilities borne by their developers.

Perhaps these differences account for the differences in the willingness of the various engineers to apply their engineerings' FMs.

I will be speculating without proof!

Recent Purchases of Appliances and SW

In the last two years (as of November, 1999), I have bought four appliances and four pieces of SW.

I am still using all the appliances.

I have yet to get the two of the programs running; of these, one is gathering dust on my shelf and one has been returned for a refund.

The other two programs are working.

The Four Appliances

1. Sharp Carousel Microwave Oven
2. RCA Color Television
3. Toshiba Video Cassette Recorder
4. Hoover Futura Vacuum Cleaner

The Four Programs

1. Adobe Illustrator 7.0

2. Adobe Acrobat Exchange 3.0

3. Microsoft Office ’97

4. Languageforce Deluxe Universal Translator

These 4 programs are developed for sale to the mass market and are different from *bespoke* SW developed by one producer under a specific negotiated contract for a specific client.

Case Study

These eight personal experiences amount to a case study giving anecdotal evidence in support of a popular perception that consumer SW is of considerably poorer quality than consumer appliances.

Can Anything Be Done?

After these experiences, I started to wonder what can be done to improve the use of quality assurance methods in the development of consumer SW.

Technology Exists

Methods and technology do exist to do a better job with SW.

However, they are not being used in the rush to get SW out to the market.

SW Released Too Early

SW is being released before it is ready.

SW is going out for sale to consumers before it is certain that it will run and with the documentation woefully inadequate and even incorrect.

Fixing broken SW does not work; and next release has its own new bugs.

SW Service is Lousy

Manufacturers seem unprepared and even unwilling to service their shoddy merchandise.

Might even be that the merchandise is so shoddy that the service people are overwhelmed and the shoddy service is a direct result of this overload.

Rush to Market

A major reason SW is released before its ready is the pressure to be the first on the market.

Whoever is first usually gets and keeps a vast majority of the market.*

The second to the market usually gets very little of the market and fails as a business, *unless* its product is perceived as at least an order of magnitude better than that of the first.

---

*The exception that proves the rule is Macintosh OS vs. MS Windows.

Incentives

High incentive to release early.

Since customers accept s--t, very little incentive to delay to improve product.

More on this later.

Appliances Work & Are Serviced Well

Appliances for sale generally work with no trouble and continue to work

When they need service, the manufacturers stand behind the product and service the products in a reasonable time.

Once serviced, the problems seem to be solved.

Differences Between SW and Appliance Productions

What are the differences between appliances and SW that might account for this observed difference in quality?

SW More Complex

Certainly SW is more complex and has more states than do vacuum cleaners.

However, a television and a video cassette recorder are systems of moderate complexity matching that of many programs.

These machines probably implement some of their functionality with a computer and SW.

SW Environments More Varied

The environment on which SW runs is more varied than that on which appliances run.

SW must run on a variety of CPUs and operating systems and flavors thereof.

Appliance environments are far simpler, consisting of an electrical outlet and the television signals coming through a cable wire or over the air.

However

In my case, all my computers had very standard configurations.

I do all my real work on a Sun workstation.

I bought PCs strictly for use of the MS Office programs not available on the Sun.

I left the PCs in the original, presumably standard configuration.

I would expect the SW to have been tested for running on my configuration.

In My Opinion

I offer the following as my opinion.

I have no real proof of my belief.

One Key Difference—Warranties

One key difference is the difference in the warranty that comes with appliances and with SW.

An appliance is forced by law in most locales in the U.S. and Canada to have a warranty of fitness for its purpose.

That is, the product is guaranteed to function as what it *is*.

If I buy a television set, the manufacturer guarantees that it functions as a television set and ...

as a television set as understood by the man in the street.

One Key Difference, Cont’d

Mass-produced SW traditionally comes with a shrinkwrapped license that says that the manufacturer warrants almost nothing about the behavior of the SW.

The manufacturer does warrant the medium on which one buys the SW, the diskettes or the CD ROM.

One Key Difference, Cont'd

In other words, the manufacturer refuses to guarantee

- that Illustrator program actually allows the user to draw pictures,
- that Word actually formats documents,
- that PowerPoint actually makes slide shows, and
- that Universal Translator actually translates.

One Key Difference, Cont’d

The SW manufacturers refuse to make these guarantees, because they are not required to by law, as are appliance manufacturers.

Also, customers let the SW manufacturers get away with it.

What manufacturers are not required to do, they do not do, and the customers suffer.

Another Key Difference—Liabilities

Another key difference is the difference in liability borne by the producers of appliances and SW.

Appliance manufacturers are liable for damages caused by correctly used or malfunctioning appliances.

Another Key Difference, Cont'd

SW producers disclaim almost all liability in their shrinkwrapped licenses, accepting liability only up to the cost of the SW (i.e., a refund).

Thus, SW developers do not have to be as careful with their mass-market products as appliance manufacturers do.

Warranties

We examine the warranties supplied with the SW products and the appliances.

SW Warranties

Adobe’s and Microsoft’s End User License Agreement (EULA) are almost identical. Therefore, only one is quoted here.

Adobe’s EULA says:

5. Limited Warranty. Adobe warrants to you that the Software will perform substantially in accordance with the Documentation ...

... for the ninety (90) day period following your receipt of the Software.

[missing details dealing with fonts that are translated to other formats; the warranty does not apply to these other formats.]

To make a warranty claim, you must return the Software to the location where you obtained it along with a copy of your sales receipt within such ninety (90) day period. If the Software does not perform substantially in accordance with the Documentation, the entire and exclusive liability and remedy shall be limited to either, at Adobe’s option, the replacement of the Software or the return of the license fee you paid for the Software.

ADOBE AND ITS SUPPLIERS DO NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE OR DOCUMENTATION. THE FORGOING STATES THE SOLE AND EXCLUSIVE REMEDIES FOR ADOBE'S OR ITS SUPPLIER'S BREACH OF WARRANTY. EXCEPT FOR THE FORGOING LIMITED WARRANTY, ADOBE AND ITS SUPPLIERS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, AS TO NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE.

Some states or jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, so the above limitations may not apply to you. To the extent permissible, any implied warranties are limited to ninety (90) days. This warranty gives you specific legal rights. You may have other rights which vary from state to state or jurisdiction to jurisdiction. For further warranty information, please contact Adobe’s Customer Support Department.

This package contains software (‘‘Software’’) and related explanatory written materials (‘‘Documentation’’).

Substantial Compliance

Adobe Illustrator 7.0 and Microsoft Office ’97 come with reasonably good, descriptive manuals describing some typical scenarios the users might wish to do.

Therefore, it might appear that the SW is being warranted to behave as the manual says it does.

However, the warranty specifies only *substantial* compliance with the written documentation, not complete compliance.

Substantial Compliance, Cont'd

Who decides how much compliance is substantial enough?

In addition, it might be that the SW can do *all* the scenarios that are described in the manual, as these were the test cases.

Certainly the developer had to get these examples running to get the pictures of the screen that are shown in the manual.

However, the SW does nothing more general, because the manual describes *all* the test cases.

Substantial Compliance, Cont’d

In other words, the documentation means only what it says and not what the average reader generalizes it to say.

Substantial Compliance, Cont'd

The only written material I find in many packages these days is a manual describing only installation.

Given the typical EULA as described above, perhaps the producer is warranting only that the installation, and not necessarily the program, will perform substantially, but not necessarily completely, in accordance with the documentation provided.

Substantial Compliance, Cont'd

Of course, there is the help system providing documentation, but if the SW does not run, and the help system does not work, does that mean that the SW is effectively not documented or that if the user cannot get to the documentation, any behavior is allowed for the SW because it is undefined in the documentation?

SW Warranty Next to Useless

Clearly, the warranty accompanying SW is next to useless except for getting one’s money back if the SW does not work.

Appliance Warranties

The warranty of the Hoover vacuum cleaner says:

Full One Year Warranty (Domestic Use)

Your HOOVER® appliance is warranted in normal household use, in accordance with the Owner's Manual against original defects in material and workmanship ...

... for a period of one full year from date of purchase. This warranty provides, at no cost to you, all labor and parts to place this appliance in correct operating condition during the warranted period.

This warranty applies when the appliance is purchased in the United States including its territories and possessions, or in Canada, or from a U. S. Military Exchange. Appliances purchased elsewhere are covered by a limited one year warranty that covers the cost of parts only.

This warranty does not apply if the appliance is used in a commercial or rental application.

Warranty service can only [sic] be obtained by presenting the appliance to one of the following authorized warranty service outlets. Proof of purchase will be required before service is rendered.

1. Hoover Factory Service Centers.

2. Hoover Authorized Warranty Service Dealers (Depots).

[details on servicing omitted]

This warranty does not cover pick up delivery, or house calls; however, if you mail your appliance to a Hoover Factory Service Center for warranty service, transportation will be paid one way.

While this warranty gives you specific legal rights, you may also have other rights which vary from state to state.

Full Warranty for Appliances

The contrast is striking. For the vacuum cleaner, I got a full, unlimited warranty, and I did not need it.

Moreover, I still have a fully functioning vacuum cleaner.

Limited Warranty for SW

For Illustrator, I got a limited warranty, and needed a full warranty, as the limited warranty did not provide a useful remedy.

A new copy would behave as the one I had and my money back would leave me with no Illustrator.

Another Appliance Warranty

For Sharp microwave ovens:

SHARP LIMITED WARRANTY

Consumer Electronics Products
Congratulations on your purchase!

Sharp Electronics of Canada Ltd. (hereinafter called ‘‘Sharp’’) gives the following express warranty to the first consumer purchaser for this Sharp brand product, when shipped in its original container and sold or distributed in Canada by Sharp or by an Authorized Sharp Dealer:

Sharp warrants that this product is free, under normal use and maintenance, from any defects in material and workmanship. If any such defects should be found in this product within the applicable warranty period, Sharp shall, at it’s [sic] option, repair or replace the product as specified herein.

This warranty shall not apply to; [sic]

(a) Any defects caused or repairs required as a result of abusive operation, negligence, accident [sic] improper installation or inappropriate use as outlined in the owner's manual;

(b) Any Sharp product tampered with, modified, adjusted or repaired by any party other than Sharp, Sharp's Authorized Service Centres or Sharp's Authorized Servicing Dealers;

(c) Damage caused or repairs required as a result of the use with items not specified or approved by Sharp, including but not limited to, head cleaning tapes and chemical cleaning agents.

(d) Any replacement of accessories, glassware, consumable or peripheral items required through normal use of the product, such as earphones, remote controls, AC adaptors, batteries, temperature probe, stylus, trays, filters, etc.

(e) Any cosmetic damage to the surface or exterior that has been defaced or caused by normal wear and tear.

(f) Any damage caused by external or environmental conditions such as liquid spillage or power line voltage, etc.

(g) Any product received without appropriate model and serial number identification and/or CSR markings.

(h) Any consumer products used for rental or commercial purposes.

Should this Sharp product fail to operate during the warranty period, service may be obtained upon delivery of the Sharp product together with proof of purchase to an Authorized Sharp Service Center or an Authorized Sharp Servicing Dealer.

[details on servicing omitted]

This warranty constitutes the entire express warranty granted by Sharp and no other dealer, service center or their agent or employee is authorized to extend, enlarge or transfer this warranty on behalf of Sharp.

WARRANTY PERIODS

...

Microwave Oven	2 years (magnetron 3 additional years part warranty only)

...

Full Warranty

Basically, for appliances, manufacturers warrant that there are no defects, that the appliance behaves as it is specified, and that they will make the appliance run if the customer finds a defect within the warranty period.

I believe that ...

If laws were changed forcing SW manufacturers to guarantee fitness for purpose or functionality, their procedures would change so that SW is released only after the same kind of quality control that appliances are subjected to.

Liability

We examine the liabilities borne by the producers of the SW products and the appliances.

Appliance Liability

Appliance manufacturers are held liable for damages caused by their appliances, e.g., if an appliance blows up, catches fire, etc.

If it can be shown that the manufacturer failed to apply accepted quality control procedures for the engineering disciplines involved in the manufacture, the manufacturer can be judged willfully negligent and can be assessed punitive damages.

Appliance Liability, Cont’d

Consequently, an appliance manufacturer applies whatever methods are available for predicting behavior and assuring quality of its products, including testing and modeling.

It also arranges for independent verification and validation (IV&V), for example, by the Underwriters’ Laboratory, as part of the process of determining the cost of its liability insurance.

Appliance Liability, Cont’d

The Hoover vacuum cleaner warranty has *no* limitation of liability whatsoever. The Sharp microwave oven warranty has a limitation of liability.

To the extent the law permits, Sharp disclaims any and all liability for direct or indirect damages or losses or for any incidental, special or consequential damages or loss of profits resulting from a defect in material or workmanship relating to the product, including damages from loss of time or use of this Sharp product. Correction of defects, in the manner and period of time described herein, constitute complete fulfillment of all obligations and responsibilities of Sharp to the purchaser with respect to the product and shall constitute full satisfaction of all claims, whether based on contract, negligence, strict liability or otherwise.

Sharp Limitation Not Legal

In many places, the law does not permit Sharp to disclaim all liability, particularly of damages or loss caused by a functioning or malfunctioning product.

In other words, if a correctly used microwave oven explodes, Sharp is liable for the damages and loss caused by the explosion.

Note that the “to the extent the law permits” is a recognition of this fact.

SW Liability — None

SW developers suffer no such liability.

There are few laws specifying their liability.

Furthermore, they usually write into their shrinkwrap, mass market licenses a disclaimer for liability for damages beyond the cost of the SW itself.

Adobe’s EULA shouts out a very strong limitation on liability; Microsoft’s EULA has a very similar shouted limitation on liability.

6. Limitation of Liability. IN NO EVENT WILL ADOBE OR ITS SUPPLIERS BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL, OR SPECIAL DAMAGES, INCLUDING ANY LOST PROFITS OR LOST SAVINGS, EVEN IF ADOBE REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY THIRD PARTY. Some states or jurisdictions do not allow the exclusion or limitation of incidental, consequential or special damages, so the above limitation may not apply to you.

Limitation Not Illegal

In most jurisdictions, the producer has no liability whatsoever for any damages caused by the SW's inability to do its function or for any damage done by malfunctioning SW.

Consumers accept

1. the useless warranty and the limitation of liability and
2. the poor quality SW

They keep paying for upgrades, which are often little more than corrections of flaws in a product that they already paid for.

I believe that ...

If laws were changed forcing liability on SW developers, their procedures would change to use all available methods for assuring quality, including inspections, testing, IV&V, and even FMs.

They will do anything to stave off a claim of willful negligence in the event of damages from the execution of their SW.

Mass-Market vs. Bespoke Software

All this is about consumer SW developed at a producer's own expense and risk for the mass market.

For bespoke SW, esp. systems with high reliability and safety concerns, e.g., in aircraft, automobiles, telecommunications, and process control, ...

the producer warrants the product and is subject to liability ...

as a result of the contract negotiated face to face between the client and producer.

Negotiating Power in Bespoke SW

For bespoke SW, the client has power to force the producer to warrant the product and accept liability.

The client can always go to another producer.

Negotiating Power in Consumer SW

In consumer market, in which there is no face-to-face negotiation of a contract, a contract warranting nothing and limiting the producer's liability is foisted on the consumer through the shrink-wrap mechanism.

For a given function, there is often only one product that runs on a customer's system or that all those interacting with the customer can use.

Thus, the customer is forced to accept this product and its license.

Negotiating Power in Consumer SW, Cont'd

The producers have power to force consumers to accept an agreement that strongly favors the producers.

This imbalance of power is probably the reason that consumers accept poor quality SW and the unfavorable terms of the shrinkwrap consumer SW license.

Wrap Up

Consider a letter by Justus Pendleton of Somerville, MA to *IEEE Computer*, January 1999:

> There is a fitness-for-use disclaimer in virtually all software that usually says something to the effect ‘‘this [information, computer program] is being provided with all faults, and the entire risk as to satisfactory quality, performance, accuracy, and effort is with the user.’’.

Pendleton's Letter, Cont'd

> The buyer of shrinkware as to either take the vendor's word that the software is fit to use or subject it to black-box testing (the results of which cannot be published without the vendor's explicit and prior permission), which is arguably more difficult that a thorough inspection of source code.
> ...
> These are the same vendors that tell us the next version, which is due out next month sometime, will fix all the problems we are having.

QA Methods and Warranties and Liabilities

In a number of engineering disciplines, there are systematic and sometimes formal procedures for verification and validation that are to be followed while the product is in design stage.

Electrical & Civil Engineers & Architects

Electrical engineers routinely apply mathematical models of electronics to determine if their designs will function correctly and will meet safety requirements.

Civil engineers and architects routinely apply mathematical models of structures to verify that the structures they are designing will support the load to which they will be subjected and that they will withstand the environmental forces that may push on them.

Why do QA?

The reason that these engineers routinely apply their quality assurance (QA) procedures is that ...

if they do not and the product does not work as it is supposed to, their employers may be inundated by customer complaints, may suffer massive returns with refunds, and may, in the worst case, be sued for damages.

Why do QA?

The employers may then take disciplinary and, in some cases, job action against the engineers responsible for the malfunctioning product.

Also, if these engineers do not apply their QA procedures and the product causes damages, the failure to apply the QA procedures in the construction of the product may subject the manufacturer to a negligence claim and punitive damages beyond the just the base cost of the damages.

Establish QA Procedures

In these engineering disciplines, the manufacturers establish procedures to be followed during design, development, and manufacturing.

These procedures include a variety of tests, ranging

- from inspection of documents,
- through actual usage of prototypes of and samples of the developed products,
- to exercising mathematical models.

Establish QA Procedures, Cont’d

The manufacturers require employees to follow these procedures and to document that they have followed the procedures.

The documentation may be subpoenaed in a damages lawsuit.

Failure to follow these procedures subjects the offending employee to disciplinary action and, in some cases, job termination.

QA Procedures vs. Negligence

These procedures and penalties for failure to follow the procedures is the manufacturer’s best defense against a negligence claim.

Physicians

The professional requirements for a medical doctor or physician are instructive.

A physician is held to *the standard of care* (SoC) in his or her community.

Failure to provide at least the current SoC may subject the physician to a negligence complaint and to malpractice action.

Definition of The SoC

The definition of the SoC varies and depends on

1. what is taught at medical school,

2. the results of recent medical research, and

3. what the physicians in the community regularly do, given the resources available.

Definition of The SoC, Cont'd

The community SoC is determined case-by-case in malpractice cases from the testimony of expert witnesses, usually other physicians.

In medicine, the SoC for a community is a baseline and may not be all that close to the state of the medical art.

The SoC consists of what the doctors in the community consider to have been demonstrated as effective treatment, modulo the facilities and resources available to carry it out.

Definition of The SoC, Cont’d

It is not required for a physician to apply the latest treatments, which may be only experimental

But, it is not an acceptable defense in a malpractice suit to say that the applied out-of-date treatment is what the physician learned in medical school.

Definition of The SoC, Cont’d

The physician is required to keep up to date and learn demonstrably effective new treatments against diseases in his or her specialty.

The SoC for a community evolves continually with new treatments established by research as effective.

Negligence

Anyone with a duty to be careful in a treatment is considered negligent and is liable for damages if

- he or she has not applied the accepted SoC,
- the care causes damages, and
- there was no independent, intervening cause of the damages.

The SoC is higher for a relevant professional than for others.

Negligence & Professional Malpractice

For a non-physician, the SoC for medical treatment is what the reasonable person-in-the-street would do in the circumstances.

For the professional physician, not to apply the community's SoC for physicians is considered malpractice.

New Treatments

In medicine, the SoC does not require using not-yet-widely used treatments and, in fact, may require *not* using them, especially if they are as yet unproved.

However, in other areas, one might be expected to use a new technology even it is not yet widely used.

In such a case, the SoC drives adoption of new techniques.

New Technology

There was a famous case from the 1920s or 1930s in which the operators of a tugboat, the *T. J. Hooper*, were held liable for the boat's sinking in a storm because there was no radio on board with which to listen to weather reports.

The operators were held liable even though, at the time, most boats did not have radios.

This case spurred the adoption of radios as standard equipment on board boats.

Loss of Exclusion of Warranty and Liability

What will happen if warranty and liability limitations for SW producers are brought in line with those of other manufactured products, and SW produces become as accountable for product quality as other manufacturers.

Please allow me to speculate.

I believe that ...

SoCs for SW Production

SW producers will have to start applying community and professionally accepted SoCs, both

- to produce more reliable SW and
- to serve as a defense against liability should products cause damages despite the care.

They will need to establish procedures that must be followed during specification, design, development, and deployment.

SoCs for SW Production, Cont'd

These procedures will include a variety of tests, ranging

- from inspection of documents,
- through uses of prototypes and production code in runs against test data,
- to formal model checking and verification.

SW producers will require their SEs to follow these procedures and to document that they have done so.

Finally, they will provide for disciplinary action and even job termination for failure to follow these procedures.

CMM and ISO

Similar procedures are established by many SW producers in order to obtain CMM or ISO 9000 certification.

These artificially imposed procedures have no observable direct positive impact and seem to mire a project in process.

Many employees doubt the effectiveness of the procedures and may even subvert their imposition.

CMM and ISO, Cont’d

Many SW manufacturers have no chance for or interest in government contracts.

They simply do not bother with certification at all.

CMM and ISO, Cont'd

Loss of warranty and liability limitation will force all SW producers to adopt systematic QA procedures, possibly those suggested by CMM or ISO.

In addition, the effect of failure to follow the procedures will be felt more directly and swiftly, in the form of job and legal actions, thus encouraging better compliance by employees.

Rush to Market

Recall how the rush to market gives a high incentive to premature release of SW.

The loss of warranty and liability limitation changes the economics of early release.

Early release may increase exposure to warranty and liability claims, which can be very costly.

Rush to Market, Slowed Down

Thus, there would be a higher incentive to slowing down to release higher quality SW.

It would become a tradeoff of exposure to warranty and liability claims versus loss of market.

SoCs for SW Development, Cont'd

These procedures will become the accepted SoC against which all work will be compared, particularly if the work has led to a substandard product or one which has caused damages.

Of course, in SW development, the SoC will vary depending on the product.

Higher SoCs for Some SW Development

The more critical the product, the higher the SoC for its development.

For SW driving a system on which lives depend, the SoC will be considerably higher than for SW driving a recreational game.

Higher SoCs for Some SW Development, Cont'd

For some life-critical systems, the SoC would likely include FMs such as model checking and possibly even formal verification.

For a program to play solitaire, the SoC would be considerably lower, probably including only inspection and basic testing.

Origins of SoCs for SW Development

The SoC for SW development will depend on

1. what is taught in SEing degree programs,

2. the results of recent SEing research, and

3. what SEs in the community regularly do, given the resources available and the domain of the SW.

New Techniques

Quite likely SEing will be judged to be a field in which new techniques, not yet widely adopted, will be expected to be used when the situation warrants it.

FMs

Where are FMs in all of this?

- FMs are taught in SEing degree programs.
- FMs are explored in SEing research.
- FMs are used in the most critical projects.
- Finally, FMs, while not widely adopted, have been shown to be of benefit in development of critical SW.

SoCs & FMs

Therefore, it seems clear that FMs will be part of the SoC for some SW developments and that the exposure of SW producers to liability will drive them to adopt FMs for the development of critical SW, and possibly, of some less than critical SW.

The SEing Profession

There is a move to make SEing a full-fledged engineering profession.

Just as the practitioners of other professions, engineering, medicine, or others, are expected to apply the profession's SoC in their work or face malpractice action, so will the SE be expected to apply SEing's SoC.

Engineer’s Responsibility

An engineer’s responsibilities include making sure products he or she produces are *fit for use*, ...

contrary to what current SW warranties claim.

FMs Become Compulsory?

If this SoC includes FMs, SEs would be compelled to apply FMs in appropriate circumstances.

The SE who does not apply this SoC would find himself out of a job or facing legal malpractice action.

Company vs. Engineer Liability

Normally, the company that produces a product is liable for the product

The individual employees are not.

However, an individual licensed engineer assumes liability for those products whose fitness he or she has guaranteed with his or her signature.

Scary Liability

This individual liability is scary and probably accounts for resistance of many current SW developers, who call themselves “SEs”, to licensing of SEs under standard engineering charters.

An engineer can lose his or her profession and face severe legal consequences if a product he or she develops and guarantees fails.

Conclusion

Once product warranty and liability applies to SW products, a producer of SW will be compelled not to release SW until it can guarantee that it behaves as it is supposed to, for fear of consequences such as

- a flood or complaints,
- having to refund lots of buyers,
- having to recall the product,
- having to stand behind a faulty product, and
- possibly even paying damages if the product causes damage as a result of not behaving as it is supposed to.

Establish Procedures

I believe that ...

To meet the required level of quality, SW producers will be force to establish systematic QA procedures.

They will be forced to put teeth into the procedures in order to force employees, the SEs, to comply with these procedures.

Establish Procedures, Cont’d

The SEs will face disciplinary action and possible termination for failure to follow the procedures.

The procedures will likely include FMs for certain classes of critical systems.

SW Like Appliances?

Perhaps one day, commercial SW will be as reliable as commercial appliances are today.

While appliances are not perfect, ...

they are a whole lot more reliable than SW.

I could live with SW being as good as my microwave oven!

Added in Proof

As I was preparing this paper for submission, an extremely relevant article authored by Joseph Menn, a *Times* staff writer, appeared in the newspapers on 4 February 2000.

It also appeared in the WWW at

http://www.latimes.com/business/updates/lat_rights000204.ht

The article at the web site is titled “Software Makers Aim to Dilute Consumer Rights” with a subtitle of “Technology: Companies push legislation at state level that would dramatically alter contract law in their favor.”

Microsoft Corp. and other powerful software companies are quietly pushing state legislation across the nation that would dramatically reduce consumer rights for individuals and businesses who buy or lease software and database information.

The push comes as software companies are beefing up their lobbying effort to pass favorable laws while their industry is at peak popularity among politicians who want to keep their local economies booming, consumer groups say.

“[This] is an example of newly powerful software giants using the promise of high-tech jobs to push through legislation that restricts consumer and business-customer rights,” said James Tierney, former Maine attorney general, who opposes the effort.

The tech bills spring from a proposal with an arcane name, the Uniform Computer Information Transactions Act (UCITA). Should states pass this legislation, the impact on consumers would be dramatic:

....

But in dozens of ways, large and small, the bills tip the balance of power toward software companies, according to law professors, consumer groups, more than 20 state attorneys general and some corporate software buyers that are beginning to organize an opposition to the UCITA campaign.

If these UCITA-sponsored bills pass, “it will dramatically change the law,” said Herschel Elkins, head of the California attorney general’s consumer department. He said the legislation would put buyers into a legal corner with little way out. “It’s pay first, find out what you bought later,” he said. “The refund right disappears when you click twice on ‘I agree.’ ”

...

“It’s very difficult to understand,” [Temple University law professor Amy] Boss said of the bill. Under the legislation, customers who install software in their computers have already lost some of their basic rights, she said. The tech bill “gives the consumer no way to disagree with the terms,” she said.

Microsoft’s [Rick] Miller declined to discuss some of the complex bill’s provisions. Other supporters of the legislation said its critics misunderstand the effect of the measure.

Wow!

It can be even worse than I thought.

Recall that the public seems to accept SW producers' claims of no warranty and no liability.

However, it is not clear that the courts would accept these claims if enough members of the public were to sue.

The courts would likely apply standards for normal consumer products, ...

simply because judges and juries do not understand SW.

Effect of UCITA

UCITA, however, would override any such court decision by explicitly legislating the provisions of most shrink-wrapped SW licenses:

NO warranty and NO liability.

Acknowledgments

I thank Connie Heitmeyer and Dino Mandrioli for bibliographical references and comments and suggestions that led to improvements in the paper.

I thank David Kay for an e-mail discussion about SoCs for medical doctors.

I thank Egon Boerger, Martin Feather, and three anonymous reviewers for their sharp criticisms of a previous version of this paper. These criticisms led to a major revision of the paper.

I was supported in parts by a University of Waterloo Startup Grant and by NSERC grant NSERC-RGPIN227055-00.