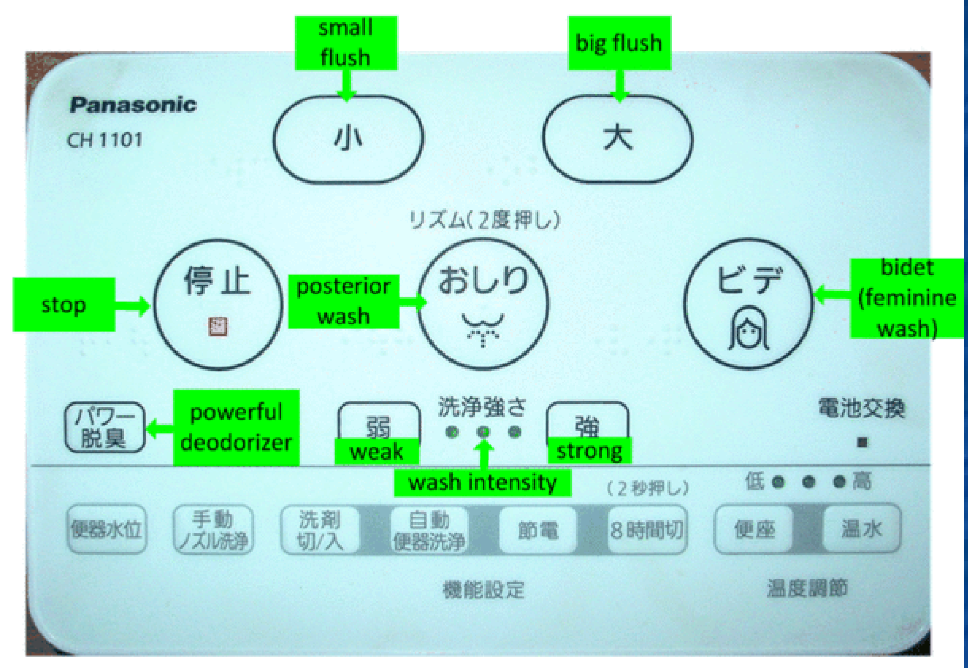
The Way Ahead in Software Engineering

...or, replacing artists with disciplined grownups.

Jack Ganssle

Embedded Systems

Other Embedded Systems



“When the software really has to work, use Ada.”

State of the Art

The current state of the art in embedded firmware: is it ED-12C? 61508? 50128?

Is it dominated by Ada? SPARK?

What about Correctness by Construction?

How to Start a Holy War

The *only* correct way to position braces:

```
void function(){
}
```

How to Start a Holy War

The *only* correct way to position braces:

```
void function()
{
}
```

How to Start a Holy War

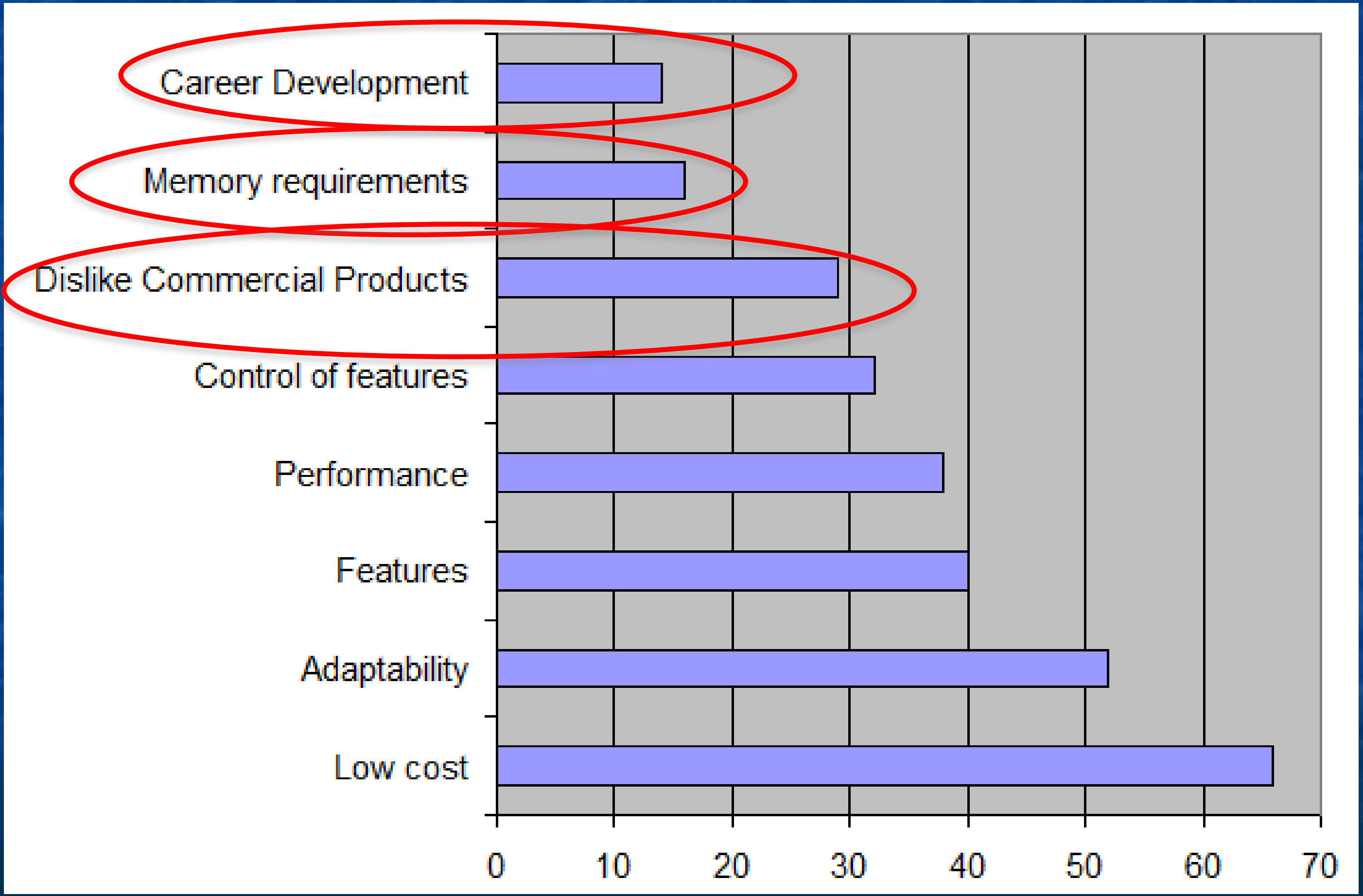
The *only* correct way to position braces:

```
void function()
  {
  }
```

How to Start a Holy War

Or, knock Linux

Why Did You Select Linux?

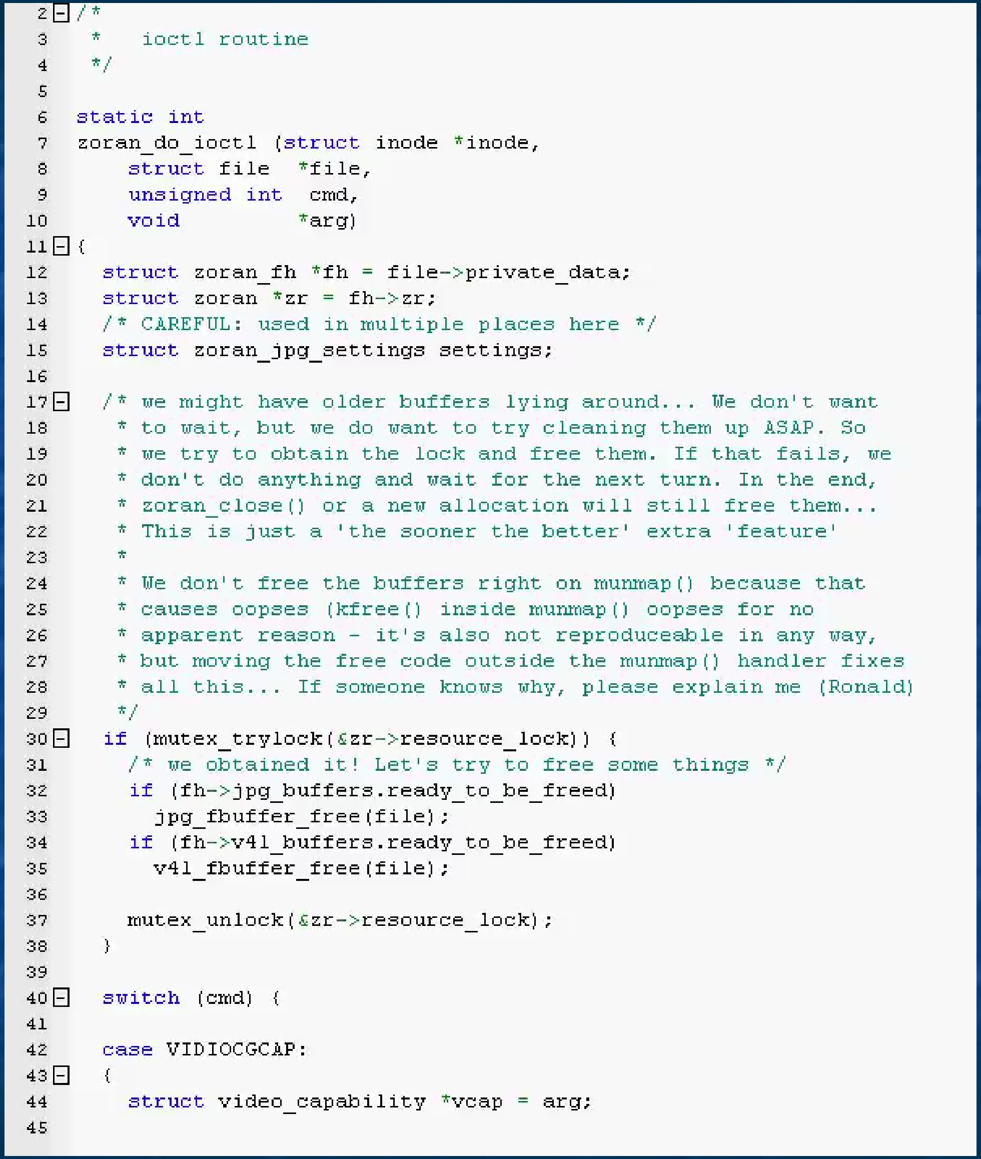


Linux: 161k functions

average complexity=4.94

750 functions: over 50
150 functions : over 100!

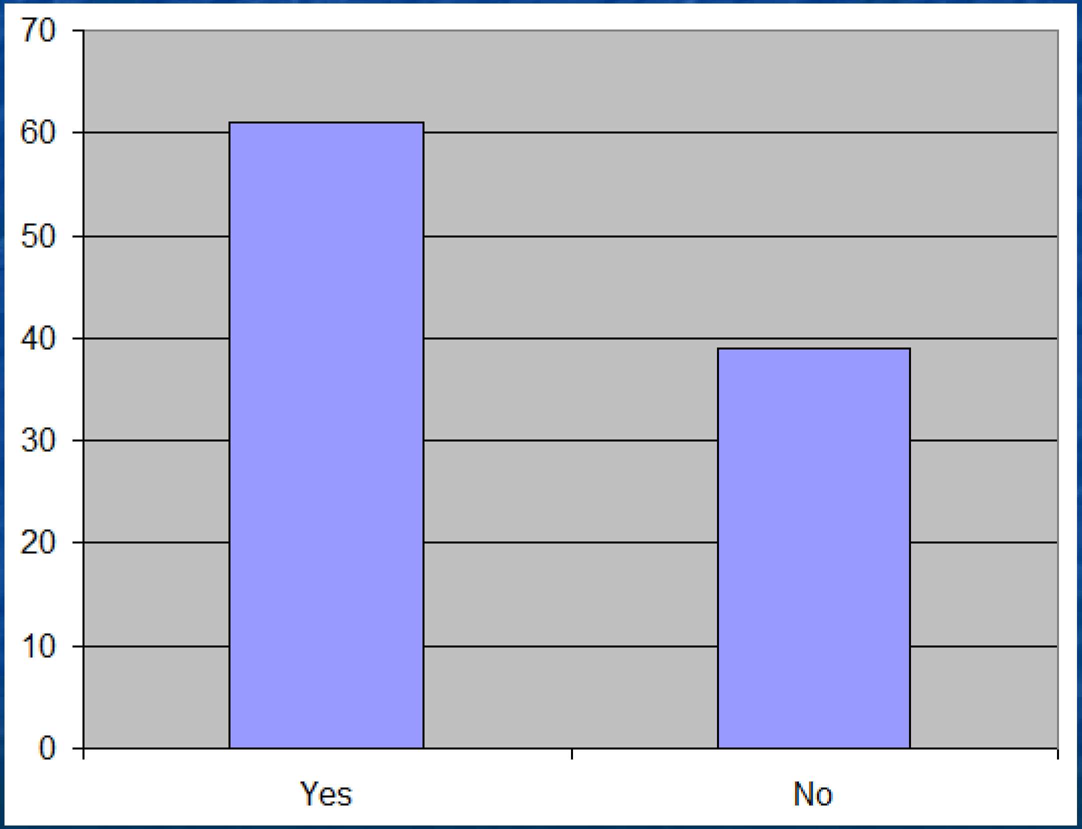
2261 LOC, complexity=352
86 comment lines



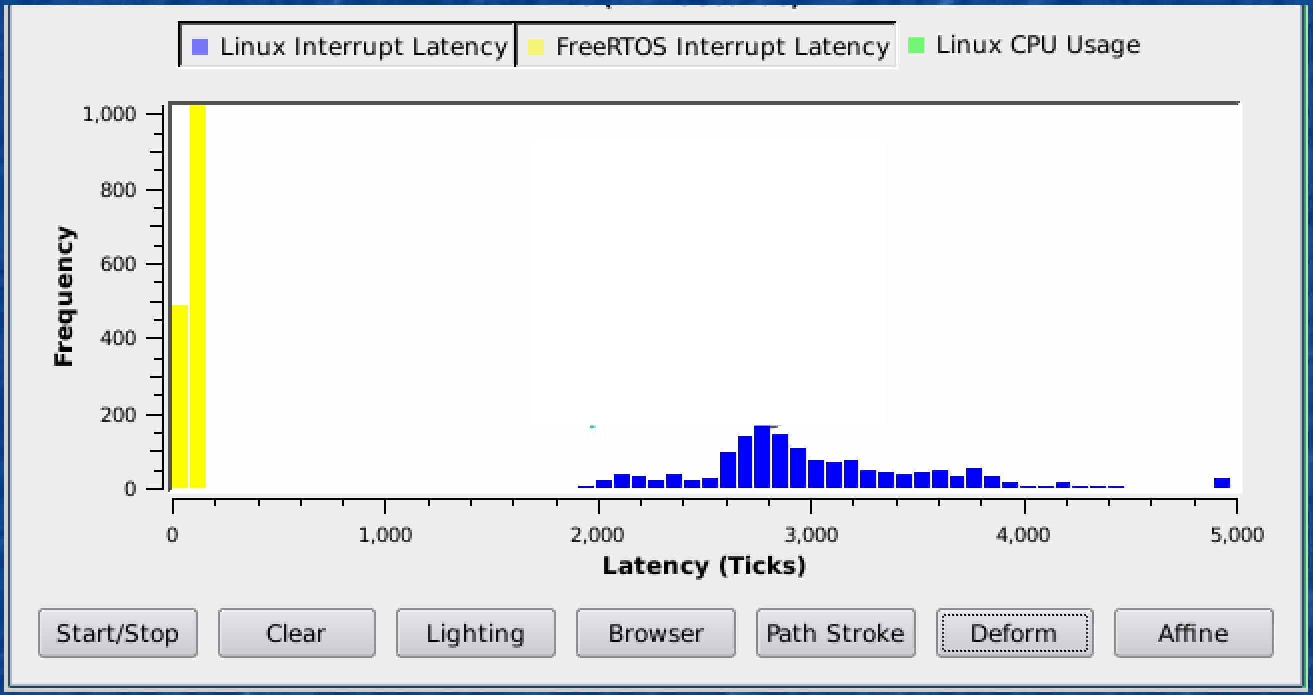
```
/*
 *   ioctl routine
 */

static int
zoran_do_ioctl (struct inode *inode,
    struct file  *file,
    unsigned int  cmd,
    void         *arg)
{
  struct zoran_fh *fh = file->private_data;
  struct zoran *zr = fh->zr;
  /* CAREFUL: used in multiple places here */
  struct zoran_jpg_settings settings;

  /* we might have older buffers lying around... We don't want
   * to wait, but we do want to try cleaning them up ASAP. So
   * we try to obtain the lock and free them. If that fails, we
   * don't do anything and wait for the next turn. In the end,
   * zoran_close() or a new allocation will still free them...
   * This is just a 'the sooner the better' extra 'feature'
   *
   * We don't free the buffers right on munmap() because that
   * causes oopses (kfree() inside munmap() oopses for no
   * apparent reason - it's also not reproduceable in any way,
   * but moving the free code outside the munmap() handler fixes
   * all this... If someone knows why, please explain me (Ronald)
   */
  if (mutex_trylock(&zr->resource_lock)) {
    /* we obtained it! Let's try to free some things */
    if (fh->jpg_buffers.ready_to_be_freed)
      jpg_fbuffer_free(file);
    if (fh->v4l_buffers.ready_to_be_freed)
      v4l_fbuffer_free(file);

    mutex_unlock(&zr->resource_lock);
  }

  switch (cmd) {

  case VIDIOCGCAP:
  {
    struct video_capability *vcap = arg;

```

Do You Have Hard Real-Time Requirements?

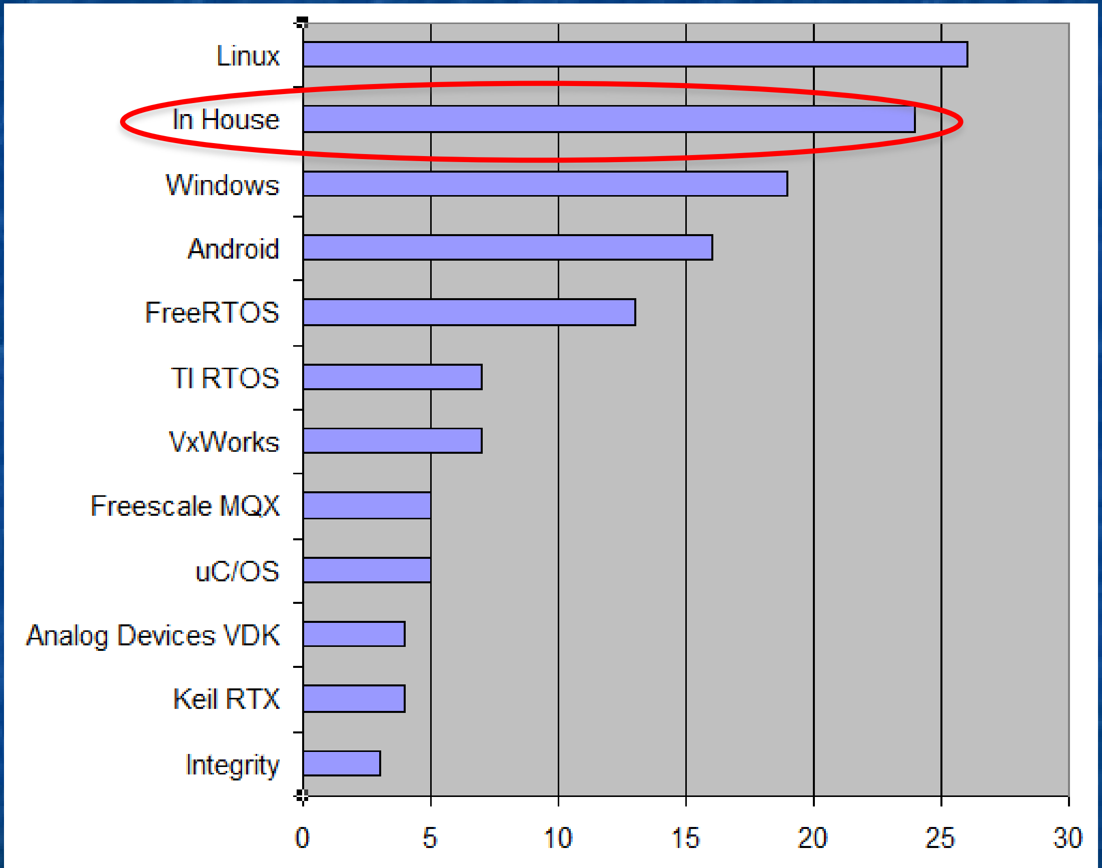
Percent



Linux vs RTOS

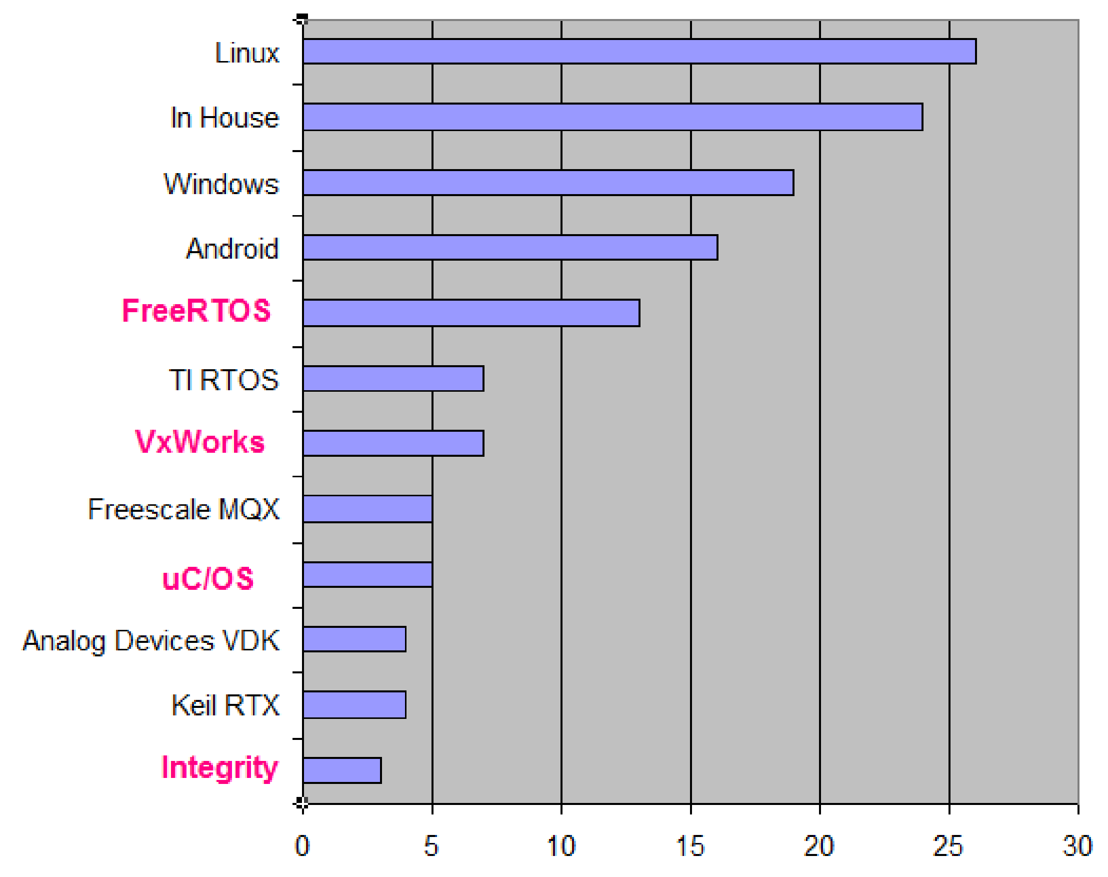


RTOS You're Using



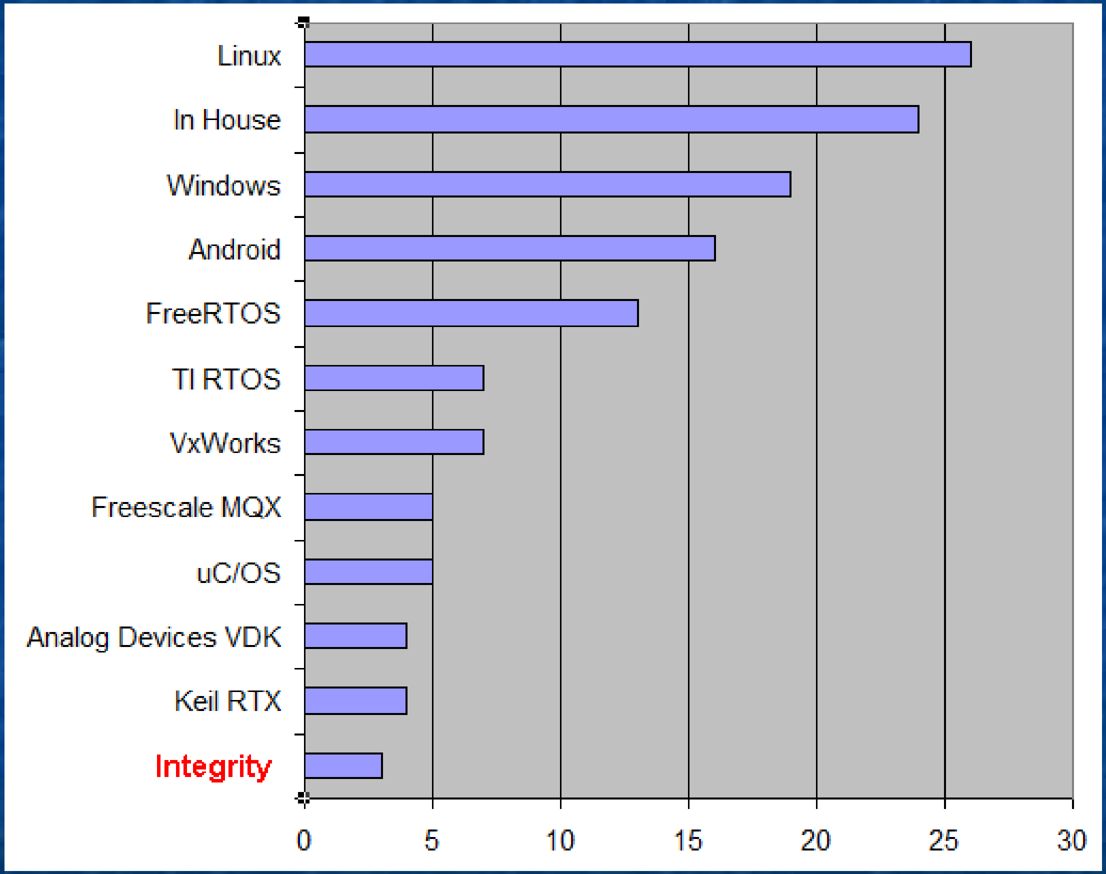
% Using the indicated RTOS

Is it a Proven RTOS?



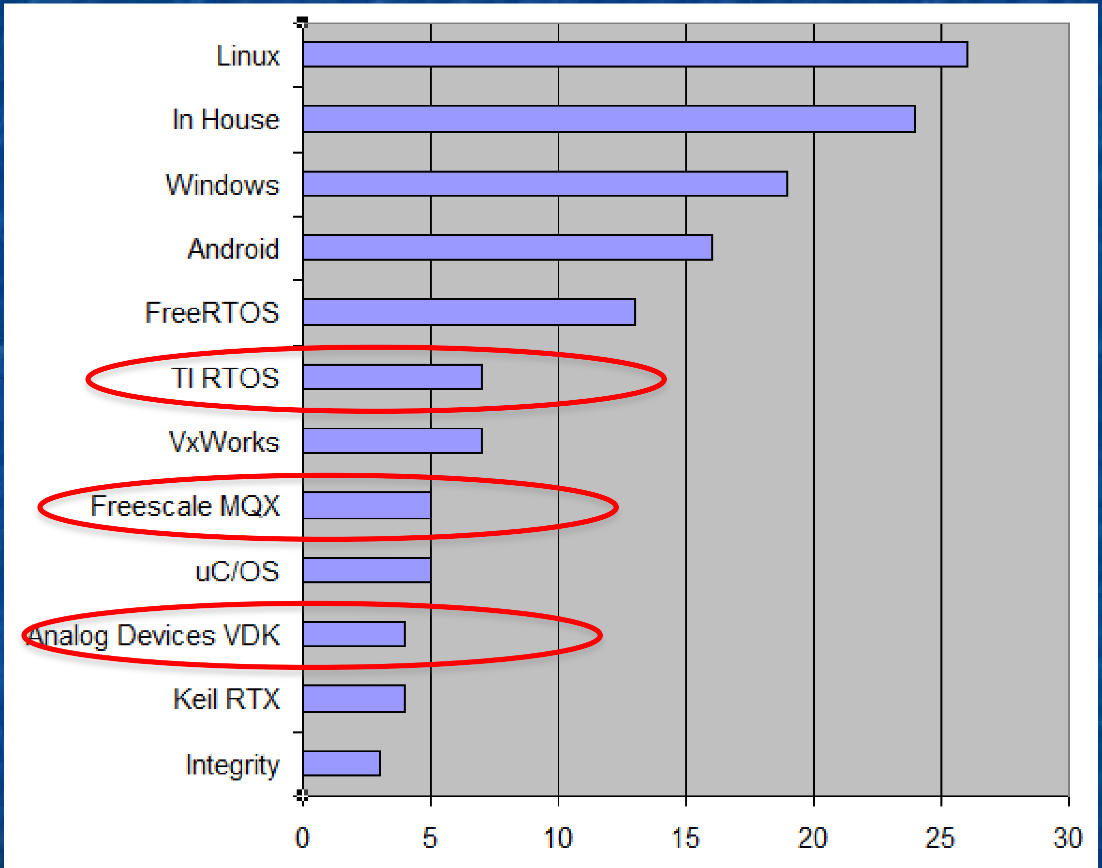
% Using the indicated RTOS

Security? EAL 5 or Higher



% Using the indicated RTOS

Vendor Lock-in?



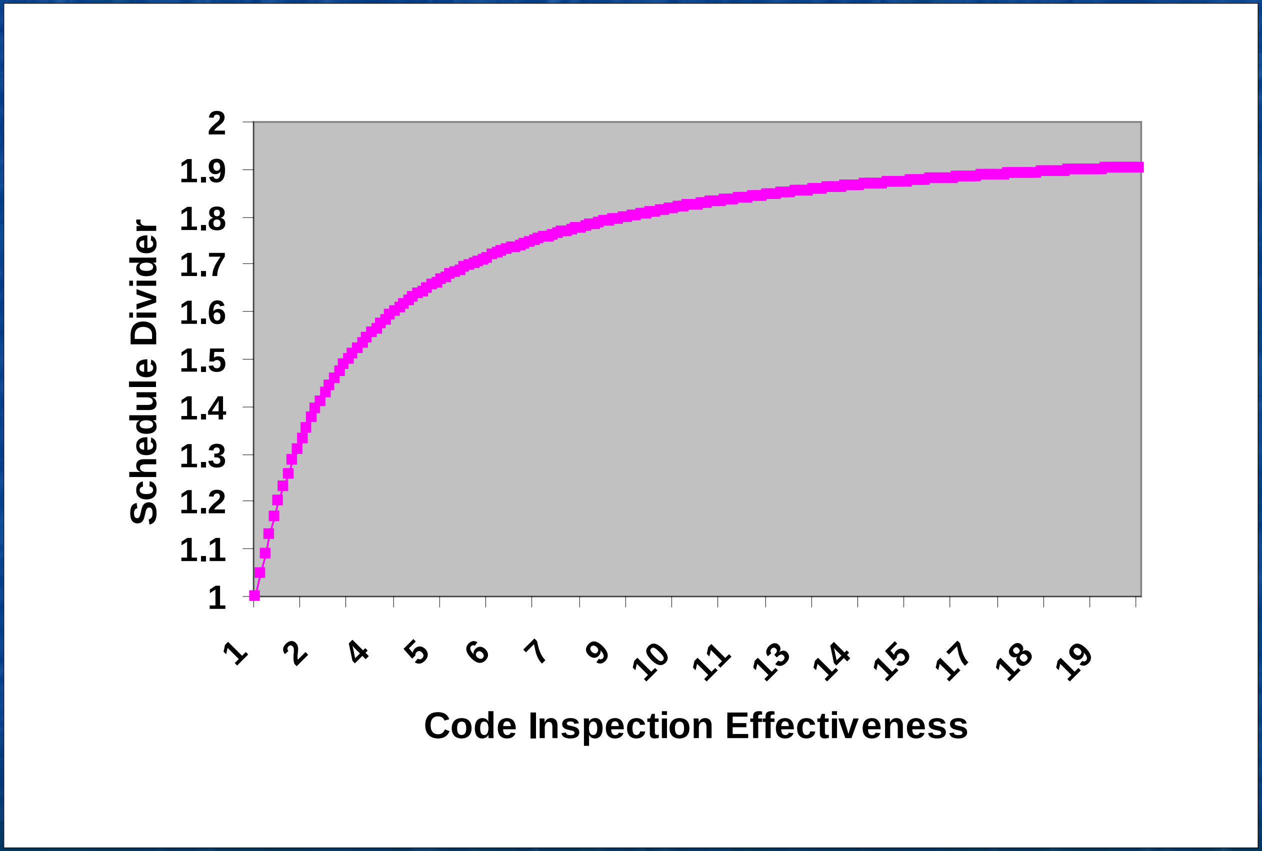
% Using the indicated RTOS

Code Inspections

- HP: 1 defect/4 hrs test, vs. 4.4/hr via inspection
- Russell: inspections 20x faster than testing
- IBM removes 82% of defects *before* testing!
- JPL: inspections 10 to 34x cheaper than test

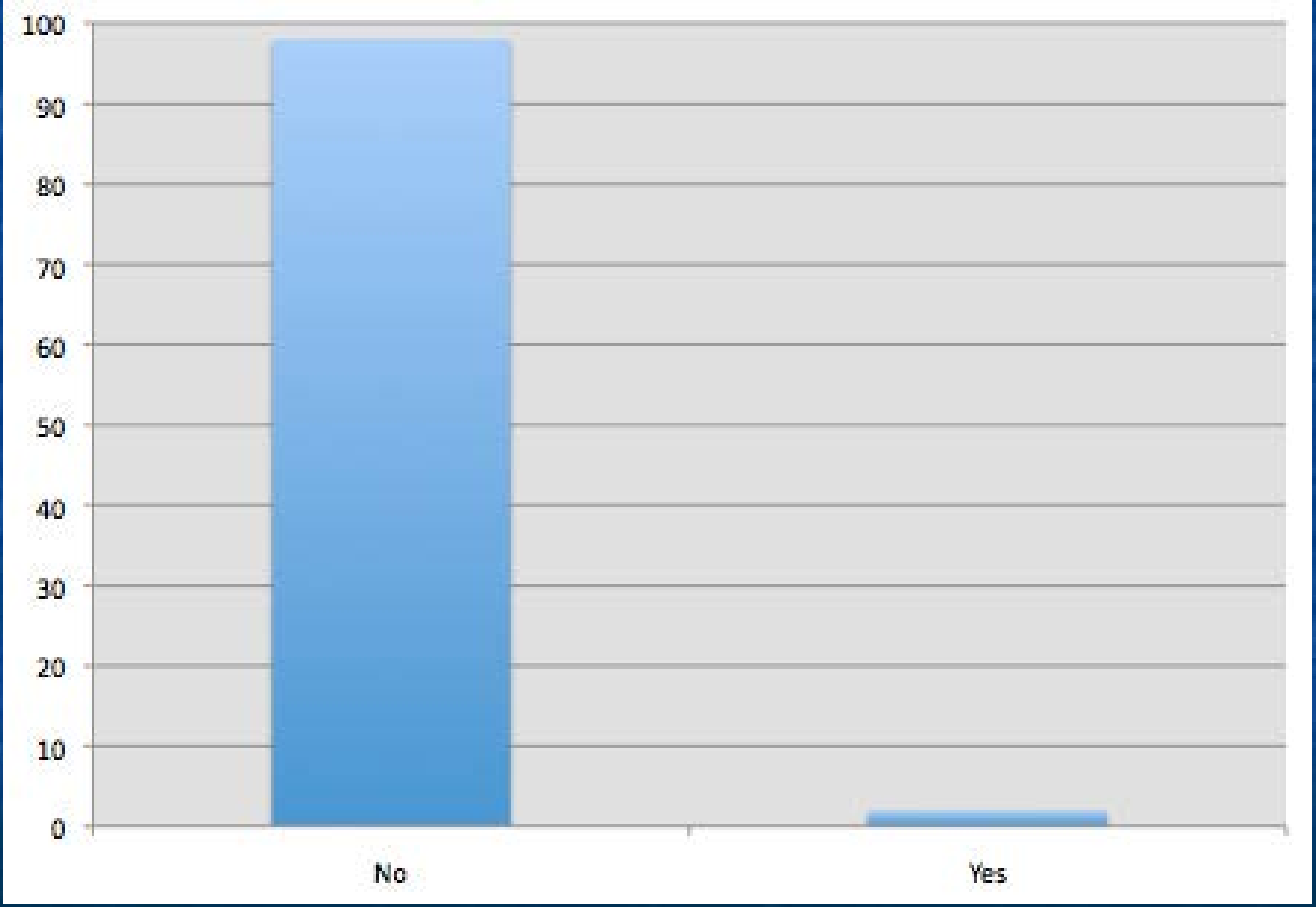
HP: In 22 projects testing only tested 1/2 the code
Glass: Testing exercises 55% of the code

Schedule Vs CI Effectiveness



Do You Routinely Use Inspections?

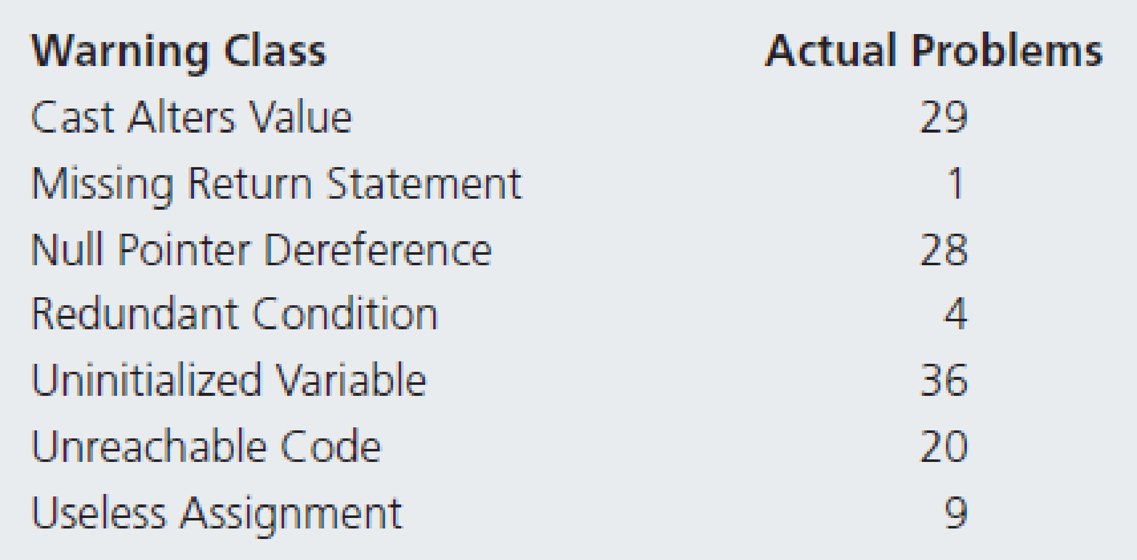
Percent



Static Analyzers

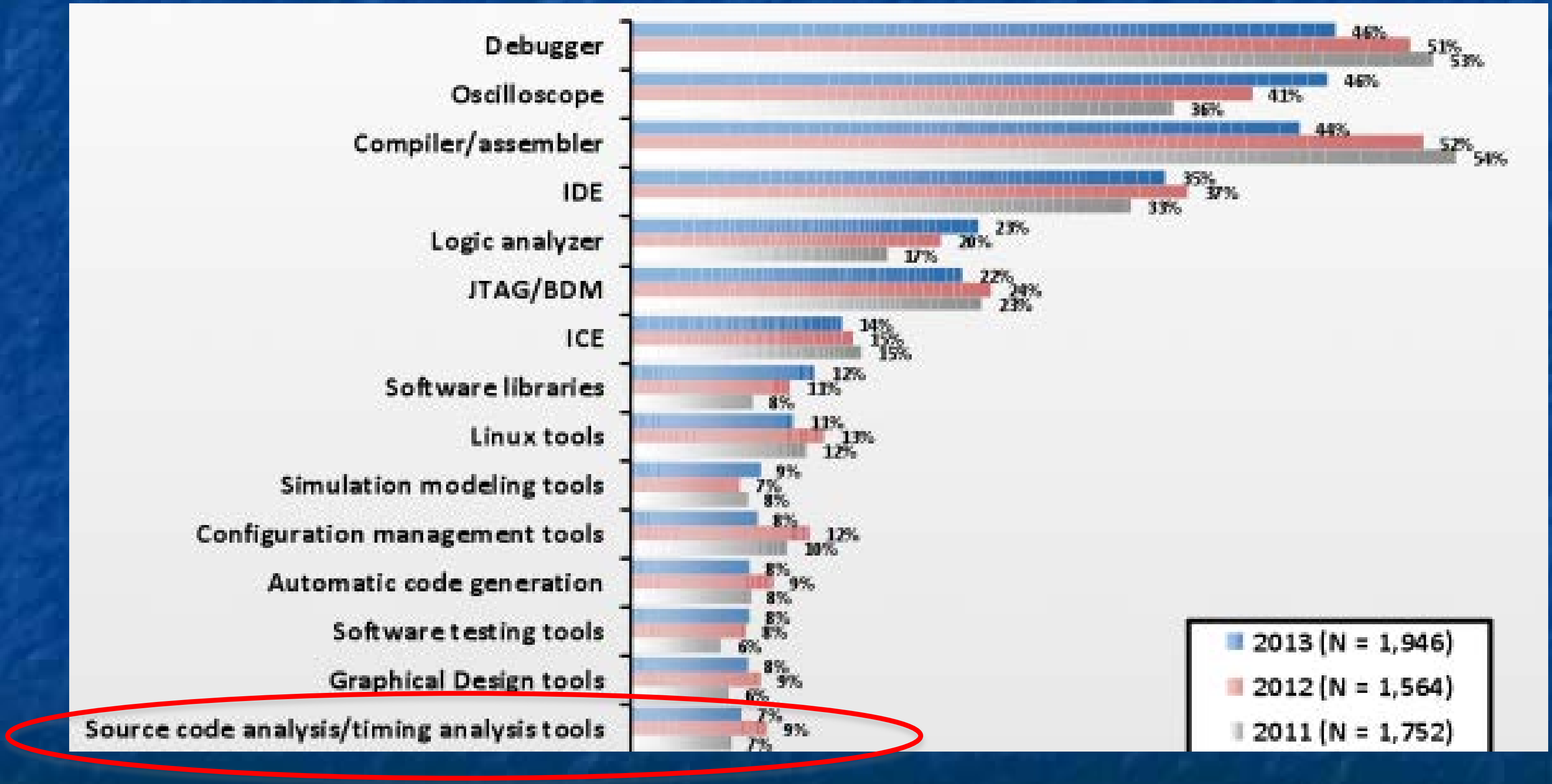
- Polyspace
- Klocwork
- Coverity
- Grammatech
- Green Hills

On one infusion pump with 200KLOC:

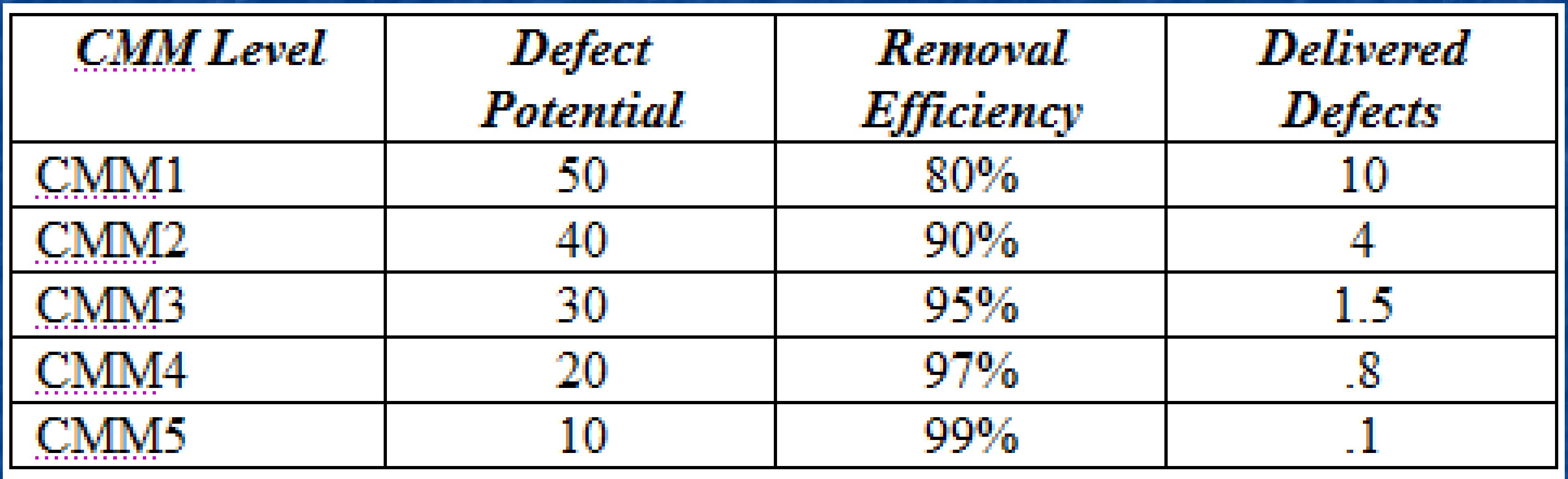


Warning Class	Actual Problems
Cast Alters Value	29
Missing Return Statement	1
Null Pointer Dereference	28
Redundant Condition	4
Uninitialized Variable	36
Unreachable Code	20
Useless Assignment	9

Static Analyzers



CMM: Typical Shipped Defects

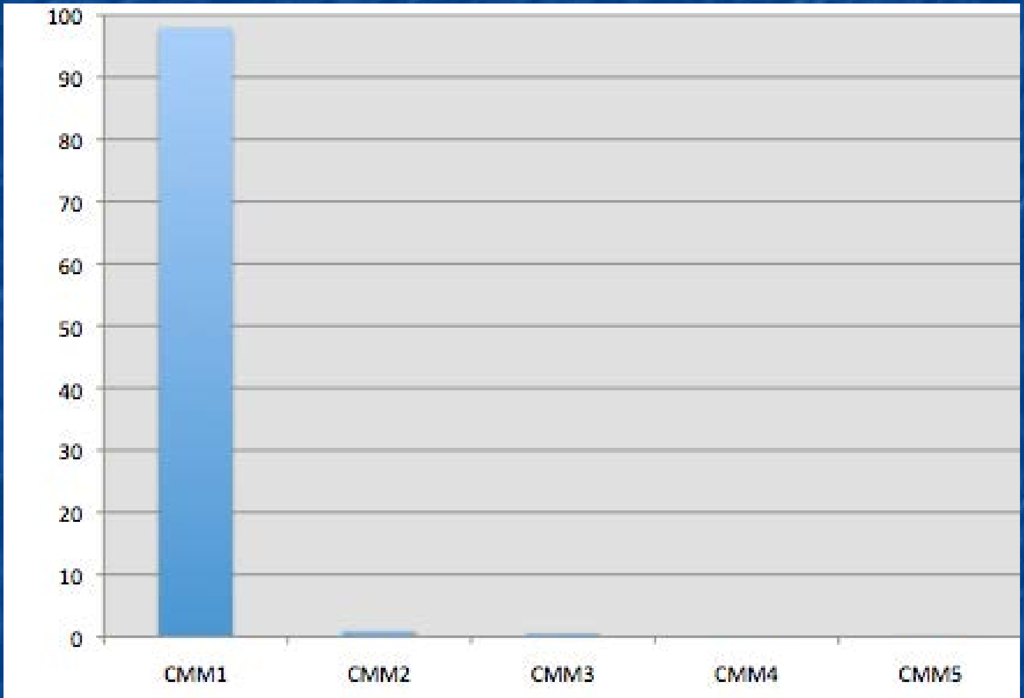


CMM Level	*Defect Potential*	*Removal Efficiency*	*Delivered Defects*
CMM1	50	80%	10
CMM2	40	90%	4
CMM3	30	95%	1.5
CMM4	20	97%	.8
CMM5	10	99%	.1

The Cost to Produce Good Code

	SIL1	SIL2	SIL3	SIL4
CMM1	1.00	1.15	1.28	1.70
CMM2	0.94	1.08	1.20	1.60
CMM3	0.74	0.85	0.95	1.26
CMM4	0.56	0.65	0.72	0.95

Use of CMM



Use of PSP – about 0%

Design in Years Past

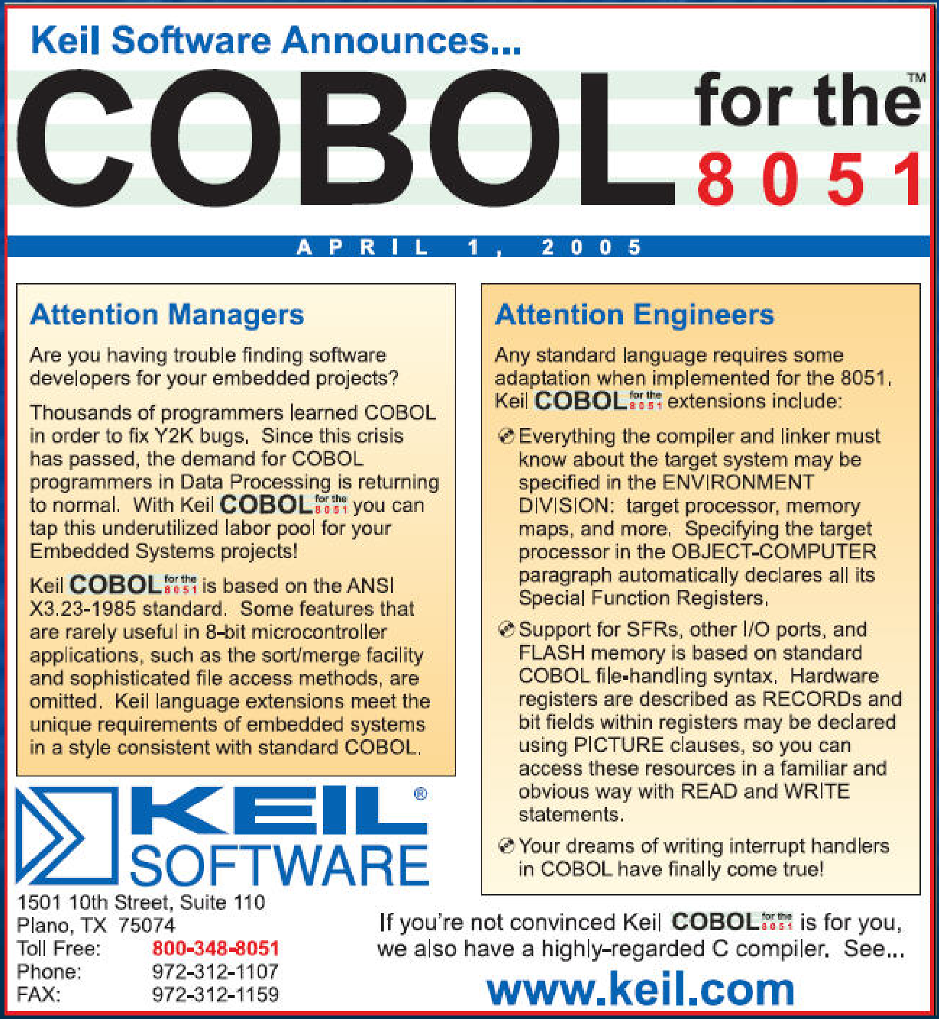
- “If you think good architecture is expensive, try bad architecture.” - *Brian Foote and Joseph Yoder*
- "Good design adds value faster than it adds cost." - *Thomas Gale*
- “I believe that good design is magical and not to be lightly tinkered with. The difference between a great design and a lousy one is in the meshing of the thousand details that either fit or don't.”
  - *Ted Nelson*

Design Today

- “Get a few people together and spend a few minutes sketching out the design. Ten minutes is ideal – half an hour should be the most time you spend to do this. After that, the best thing to do is to let the code participate in the design session – move to the machine and start typing in code.” - Ron Jeffries

- “The larger the scale, the more you must rely on emergence.” - Kent Beck

Language Choices



Keil Software Announces...

COBOL for the 8051™

APRIL 1, 2005

Attention Managers

Are you having trouble finding software developers for your embedded projects?

Thousands of programmers learned COBOL in order to fix Y2K bugs. Since this crisis has passed, the demand for COBOL programmers in Data Processing is returning to normal. With Keil **COBOL** for the 8051 you can tap this underutilized labor pool for your Embedded Systems projects!

Keil **COBOL** for the 8051 is based on the ANSI X3.23-1985 standard. Some features that are rarely useful in 8-bit microcontroller applications, such as the sort/merge facility and sophisticated file access methods, are omitted. Keil language extensions meet the unique requirements of embedded systems in a style consistent with standard COBOL.

Attention Engineers

Any standard language requires some adaptation when implemented for the 8051. Keil **COBOL** for the 8051 extensions include:

- Everything the compiler and linker must know about the target system may be specified in the ENVIRONMENT DIVISION: target processor, memory maps, and more. Specifying the target processor in the OBJECT-COMPUTER paragraph automatically declares all its Special Function Registers.
- Support for SFRs, other I/O ports, and FLASH memory is based on standard COBOL file-handling syntax. Hardware registers are described as RECORDs and bit fields within registers may be declared using PICTURE clauses, so you can access these resources in a familiar and obvious way with READ and WRITE statements.
- Your dreams of writing interrupt handlers in COBOL have finally come true!

KEIL® SOFTWARE

1501 10th Street, Suite 110
Plano, TX 75074

Toll Free:	800-348-8051
Phone:	972-312-1107
FAX:	972-312-1159

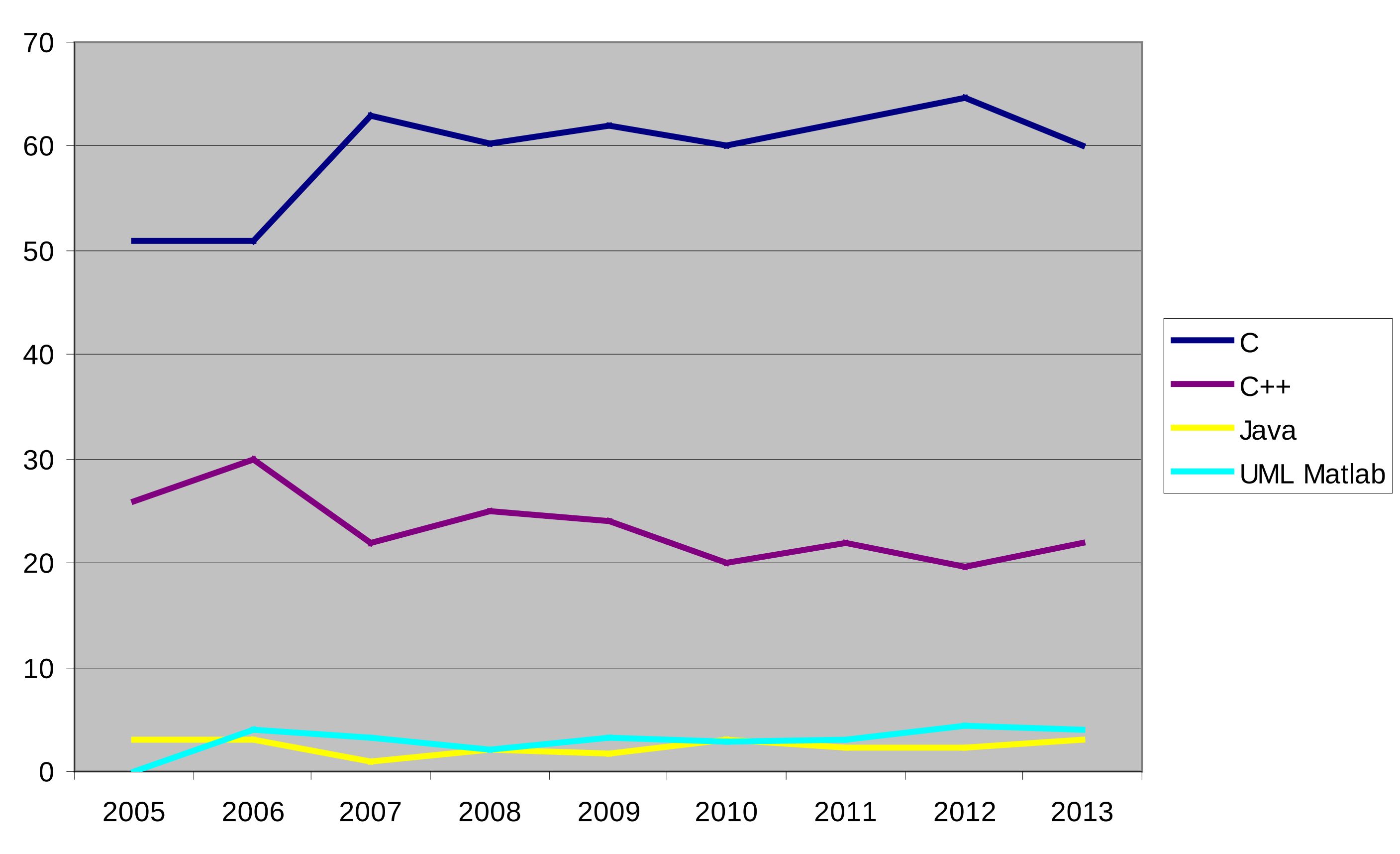
If you're not convinced Keil **COBOL** for the 8051 is for you, we also have a highly-regarded C compiler. See...

www.keil.com

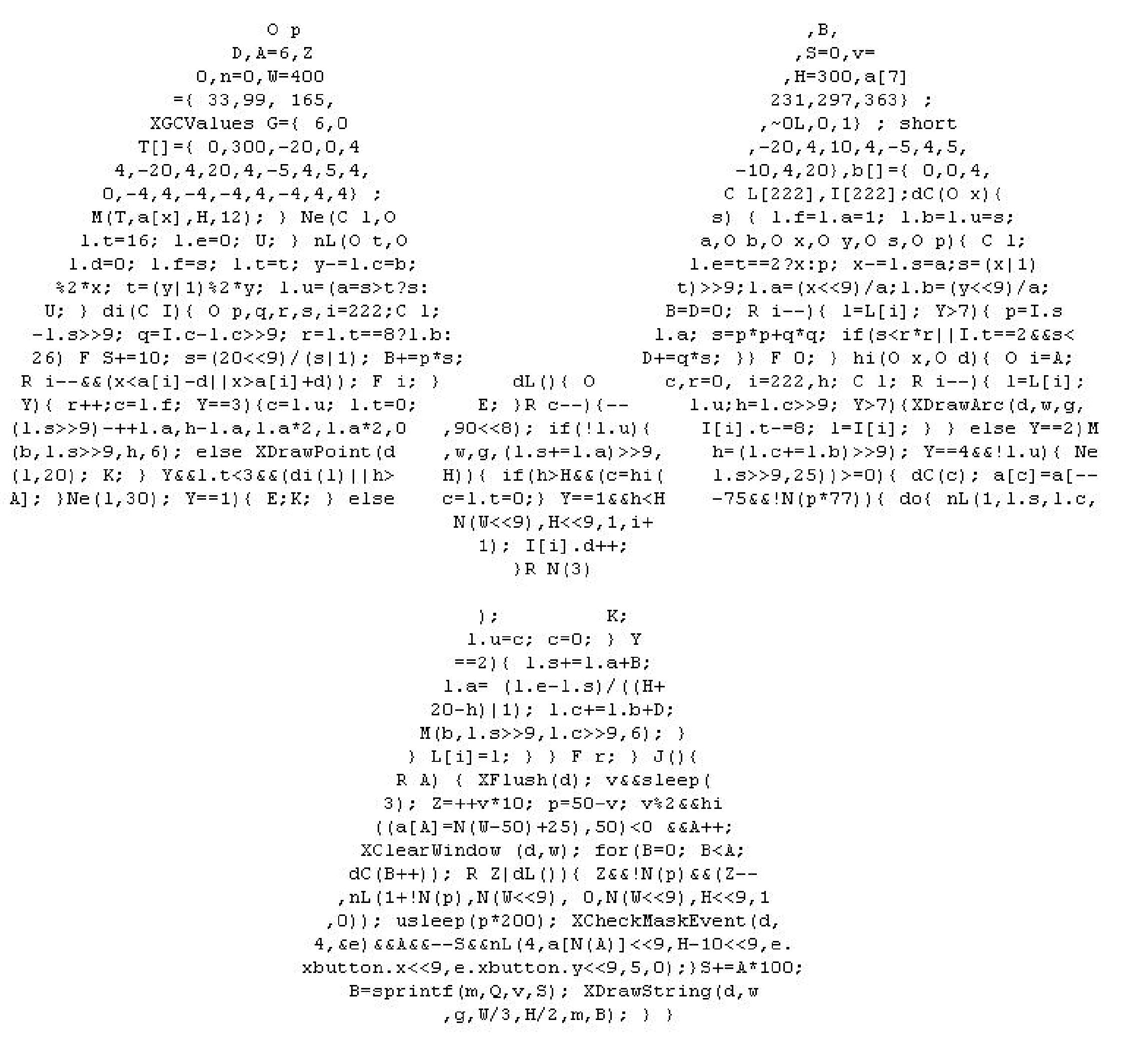
Bug Rates

C/C++ (typical)	50 - 100 bugs/KLOC
Ada (typical)	5 - 10
SPARK	pretty much none

Primary Language Used



C Wins



```
                      O p                                           ,B,
                   D,A=6,Z                                         ,S=0,v=
                0,n=0,W=400                                       ,H=300,a[7]
              ={ 33,99, 165,                                     231,297,363} ;
            XGCValues G={ 6,0                                   ,~0L,0,1} ; short
           T[]={ 0,300,-20,0,4                                 ,-20,4,10,4,-5,4,5,
         4,-20,4,20,4,-5,4,5,4,                               -10,4,20},b[]={ 0,0,4,
        0,-4,4,-4,-4,4,-4,4,4} ;                             C L[222],I[222];dC(O x){
       M(T,a[x],H,12); } Ne(C l,O                           s) { l.f=l.a=1; l.b=l.u=s;
      l.t=16; l.e=0; U; } nL(O t,O                         a,O b,O x,O y,O s,O p){ C l;
     l.d=0; l.f=s; l.t=t; y-=l.c=b;                       l.e=t==2?x:p; x-=l.s=a;s=(x|1)
    %2*x; t=(y|1)%2*y; l.u=(a=s>t?s:                     t)>>9;l.a=(x<<9)/a;l.b=(y<<9)/a;
   U; } di(C I){ O p,q,r,s,i=222;C l;                   B=D=0; R i--){ l=L[i]; Y>7){ p=I.s
  -l.s>>9; q=I.c-l.c>>9; r=l.t==8?l.b:                 l.a; s=p*p+q*q; if(s<r*r||I.t==2&&s<
  26) F S+=10; s=(20<<9)/(s|1); B+=p*s;               D+=q*s; }} F 0; } hi(O x,O d){ O i=A;
 R i--&&(x<a[i]-d||x>a[i]+d)); F i; }      dL(){ O      c,r=0, i=222,h; C l; R i--){ l=L[i];
 Y){ r++;c=l.f; Y==3){c=l.u; l.t=0;     E; }R c--){--     l.u;h=l.c>>9; Y>7){XDrawArc(d,w,g,
(l.s>>9)-++l.a,h-l.a,l.a*2,l.a*2,0   ,90<<8); if(!l.u){    I[i].t-=8; l=I[i]; } } else Y==2)M
(b,l.s>>9,h,6); else XDrawPoint(d    ,w,g,(l.s+=l.a)>>9,    h=(l.c+=l.b)>>9); Y==4&&!l.u){ Ne
(l,20); K; } Y&&l.t<3&&(di(l)||h>    H)){ if(h>H&&(c=hi(    l.s>>9,25))>=0){ dC(c); a[c]=a[--
A]; }Ne(l,30); Y==1){ E;K; } else    c=l.t=0;} Y==1&&h<H    -75&&!N(p*77)){ do{ nL(1,l.s,l.c,
                                      N(W<<9),H<<9,1,i+
                                        1); I[i].d++;
                                           }R N(3)

                                        );         K;
                                       l.u=c; c=0; } Y
                                      ==2){ l.s+=l.a+B;
                                     l.a= (l.e-l.s)/((H+
                                    20-h)|1); l.c+=l.b+D;
                                   M(b,l.s>>9,l.c>>9,6); }
                                  } L[i]=l; } } F r; } J(){
                                 R A) { XFlush(d); v&&sleep(
                                3); Z=++v*10; p=50-v; v%2&&hi
                               ((a[A]=N(W-50)+25),50)<0 &&A++;
                              XClearWindow (d,w); for(B=0; B<A;
                             dC(B++)); R Z|dL()){ Z&&!N(p)&&(Z--
                            ,nL(1+!N(p),N(W<<9), 0,N(W<<9),H<<9,1
                           ,0)); usleep(p*200); XCheckMaskEvent(d,
                          4,&e)&&A&&--S&&nL(4,a[N(A)]<<9,H-10<<9,e.
                         xbutton.x<<9,e.xbutton.y<<9,5,0);}S+=A*100;
                             B=sprintf(m,Q,v,S); XDrawString(d,w
                                     ,g,W/3,H/2,m,B); } }
```

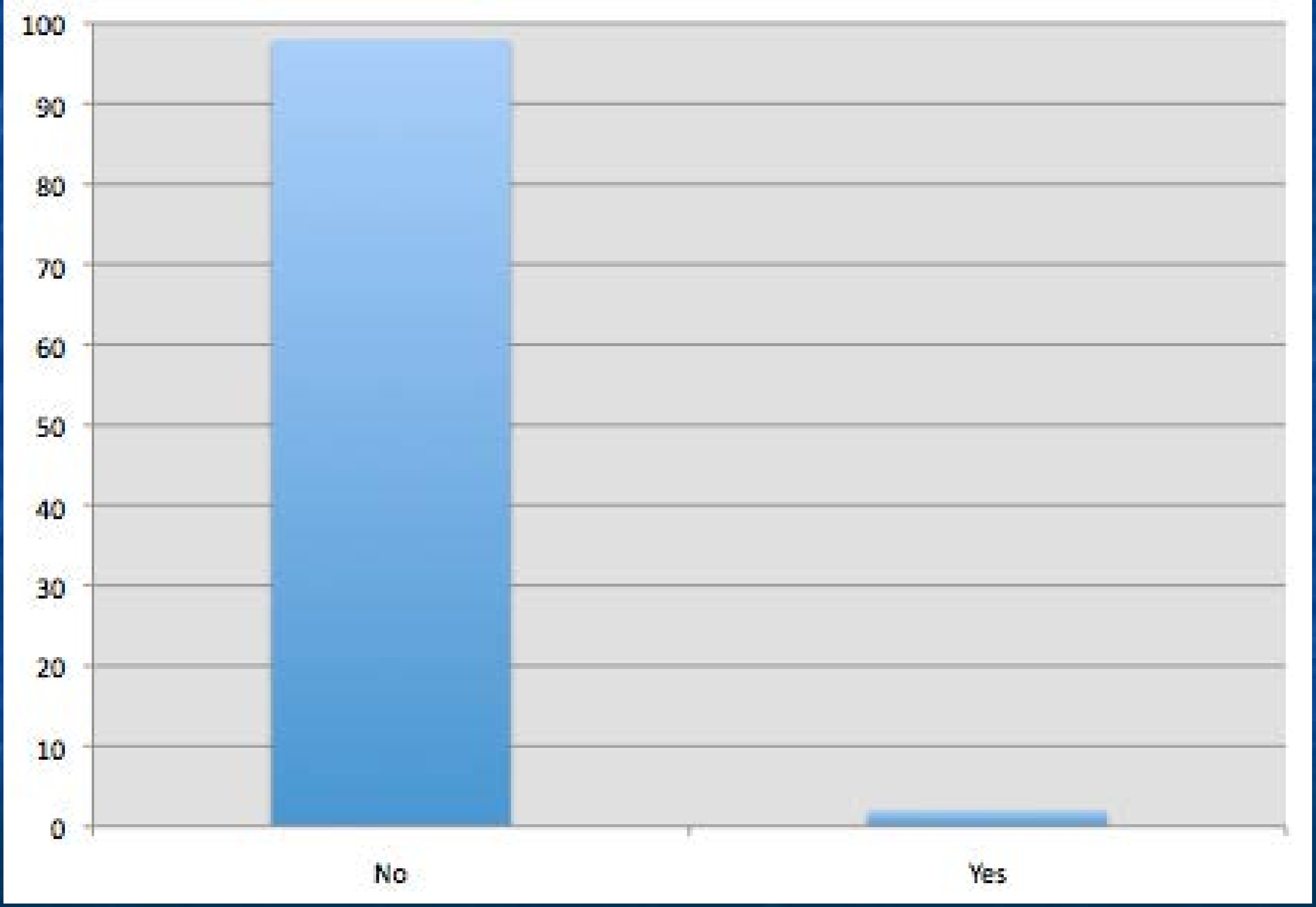
Incomprehensible C

```
*********************variable = 0;
```

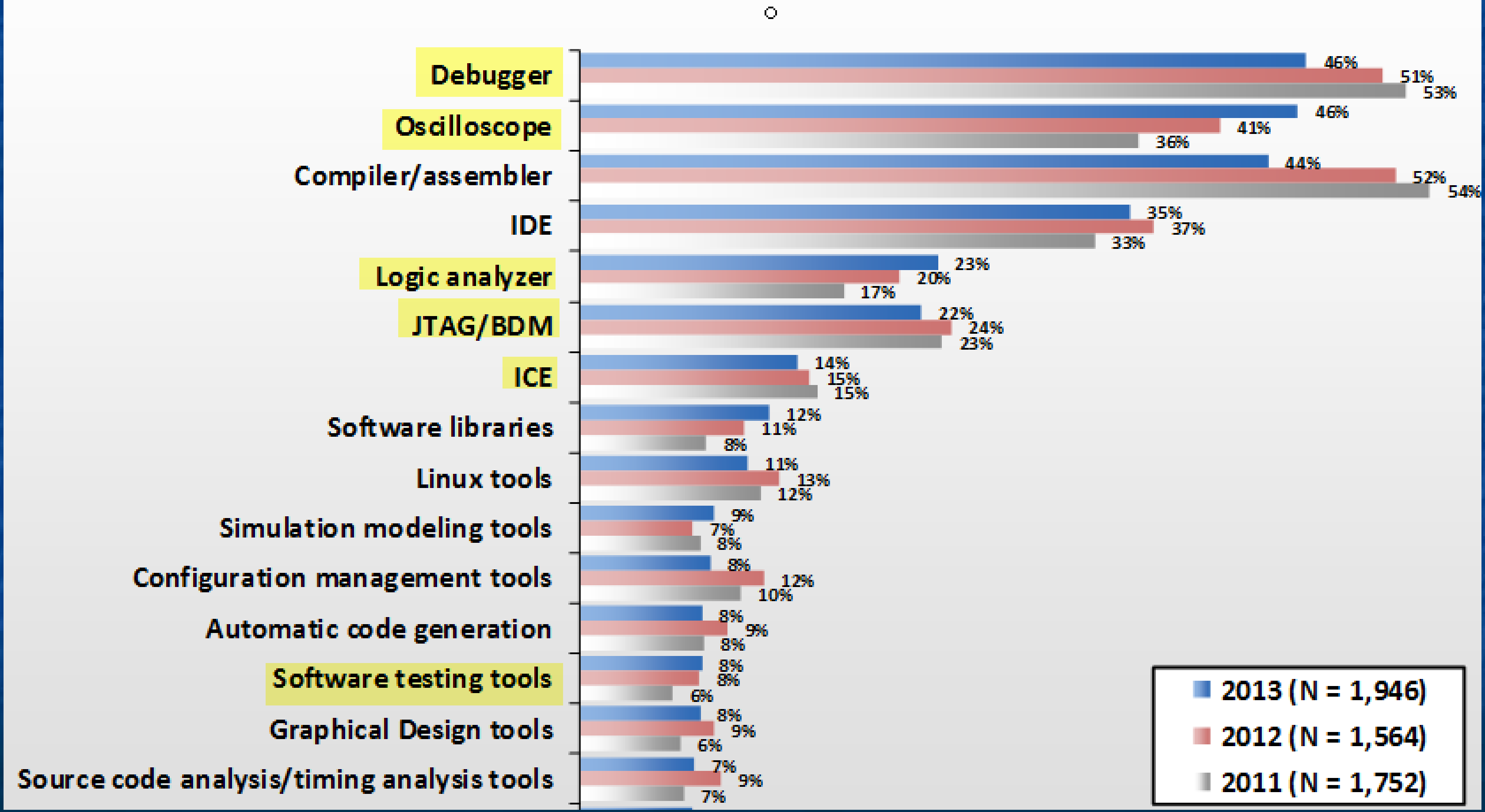
“int” means... what?

Do You Use a Standard?

Percent



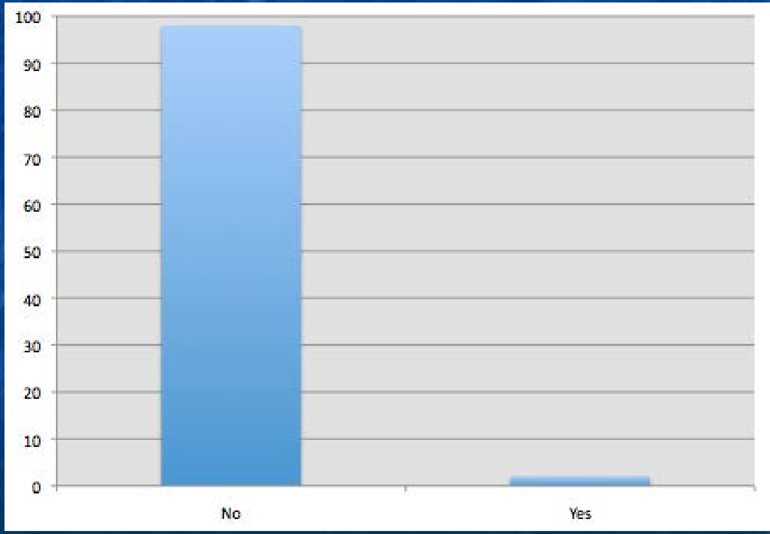
Most Important Tools



Biggest cause of slipped schedules:

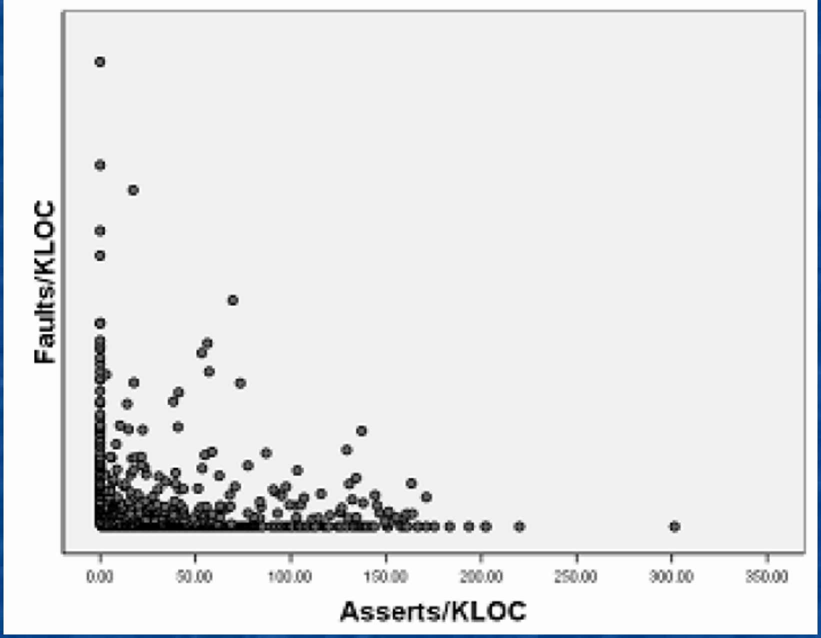
Bugs!

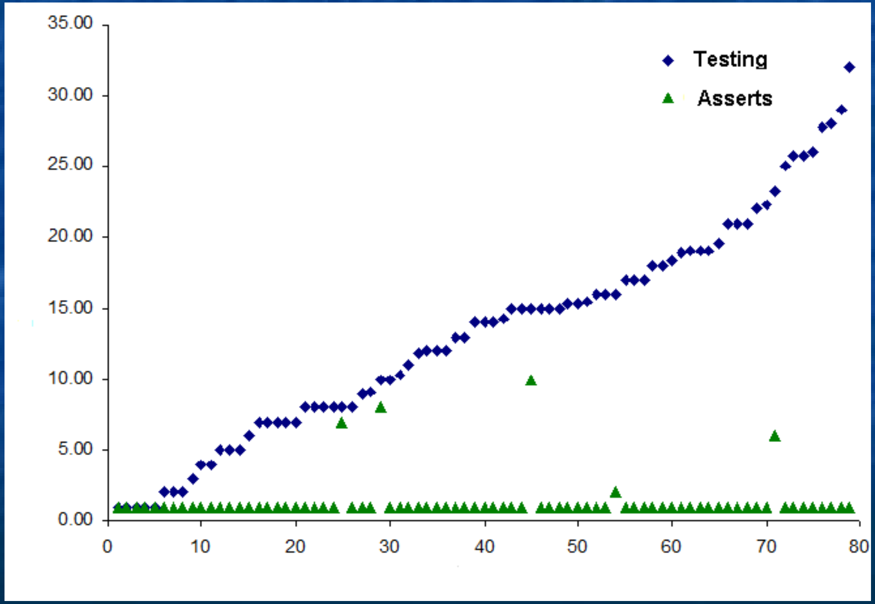
C/C++	50 - 100 bugs/KLOC
Ada	5 - 10
SPARK	pretty much none



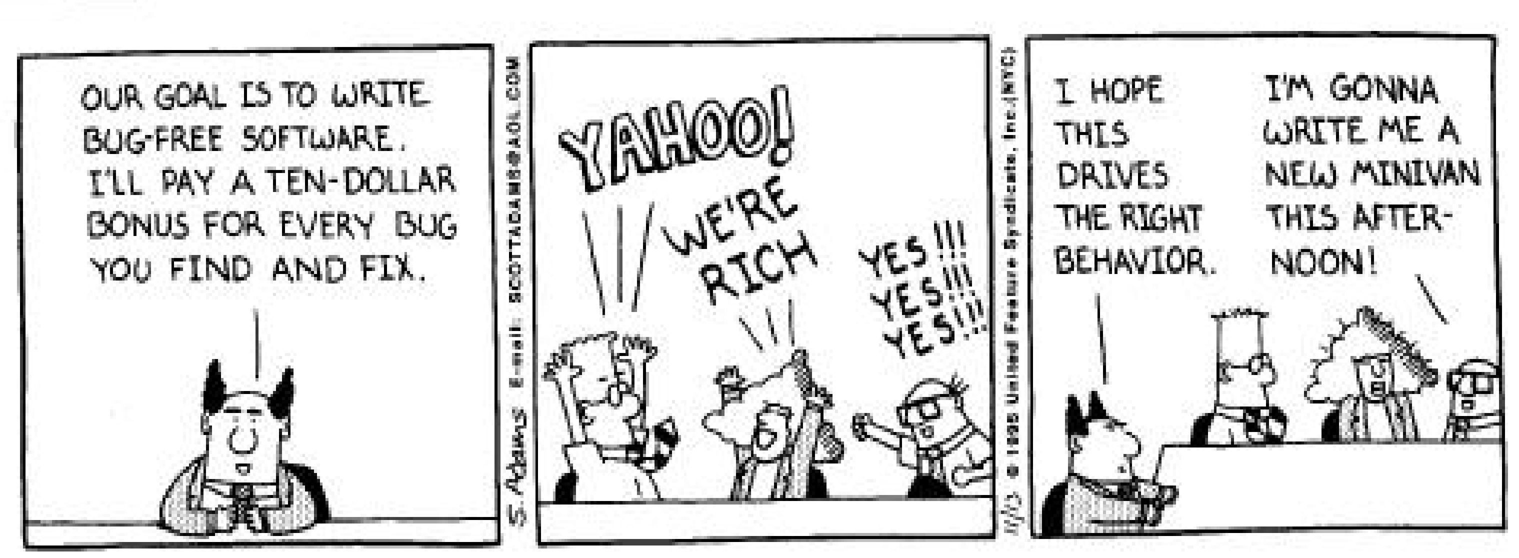
Use of inspections

Assertions vs. Bugs





Metrics?


OUR GOAL IS TO WRITE BUG-FREE SOFTWARE. I'LL PAY A TEN-DOLLAR BONUS FOR EVERY BUG YOU FIND AND FIX.
S. Adams E-mail: SCOTTADAMS@AOL.COM
YAHOO!
WE'RE RICH
YES!!! YES!!! YES!!!
© 1995 United Feature Syndicate, Inc.(NYC)
I HOPE THIS DRIVES THE RIGHT BEHAVIOR.
I'M GONNA WRITE ME A NEW MINIVAN THIS AFTER-NOON!

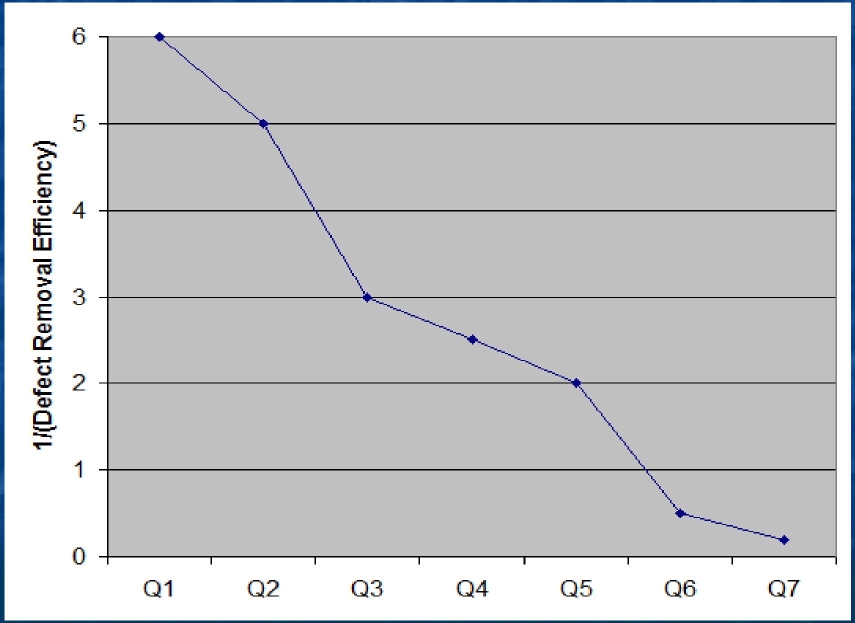
Bug Metrics

Bug source	**Malpractice**	**CMM3**
Requirements	15/50%	4/85%
Design	22/50%	6/97%
Coding	25/80%	10/99%
Documents	10/70%	4/98%
Bad fixes	8/50%	1/95%
TOTAL INJECTED	80	25
SHIPPED	50	1

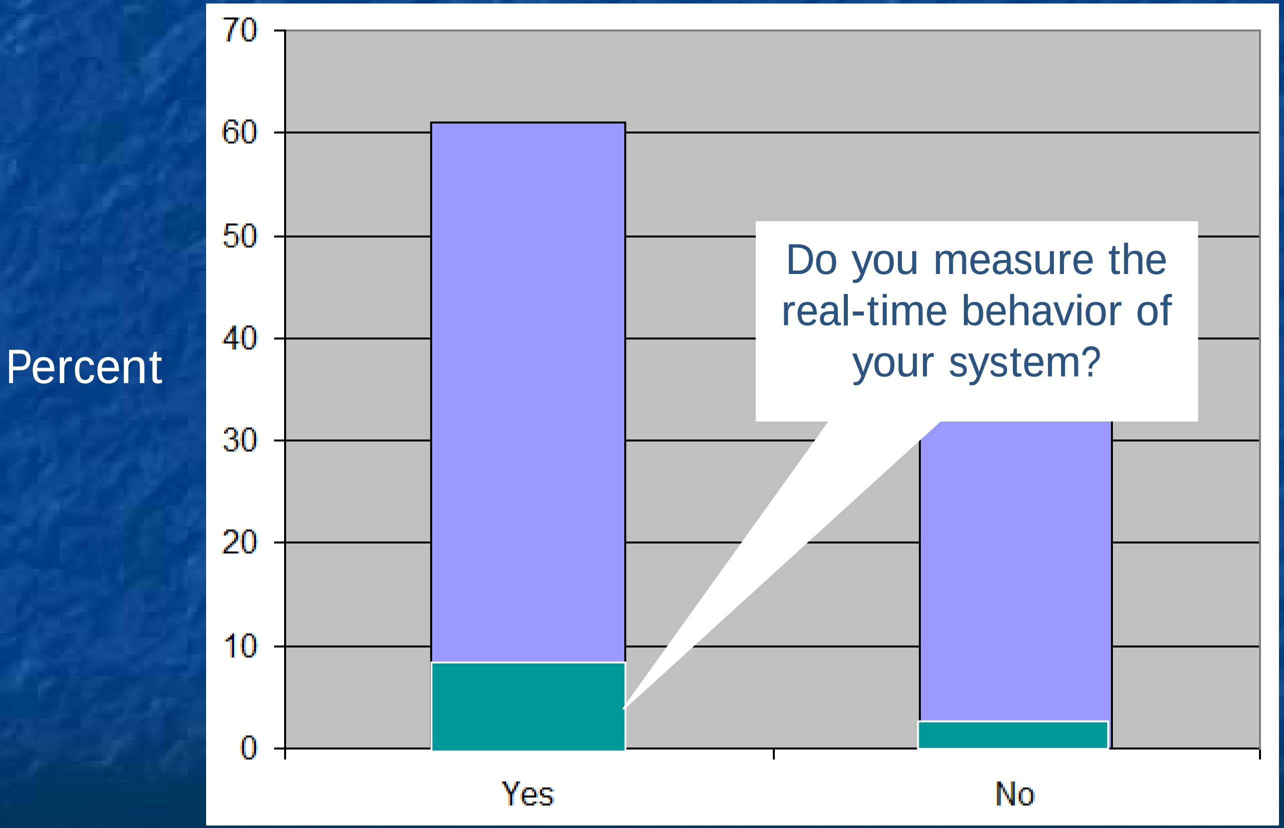
Defect Removal Efficiency

"When these measures were introduced into large corporations such as IBM and ITT, in less than four years the volumes of delivered defects had declined by more than 50%; maintenance costs were reduced by more than 40%; development schedules were shortened by more than 15%. There are no other measurements that can yield such positive benefits in such a short time span." - Capers Jones

Percent of bugs shipped



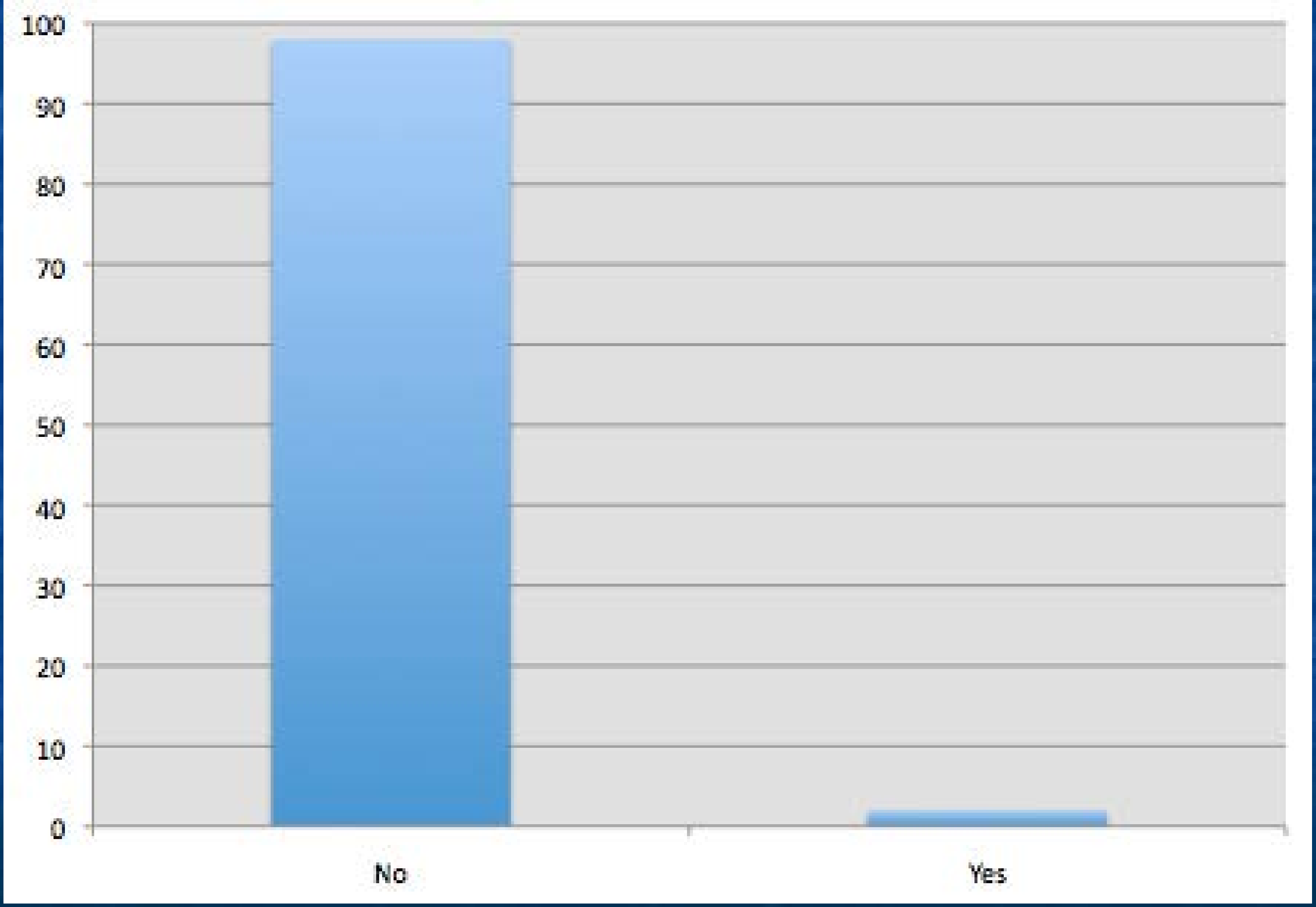
Hard Real-Time Requirements



Do you measure the real-time behavior of your system?

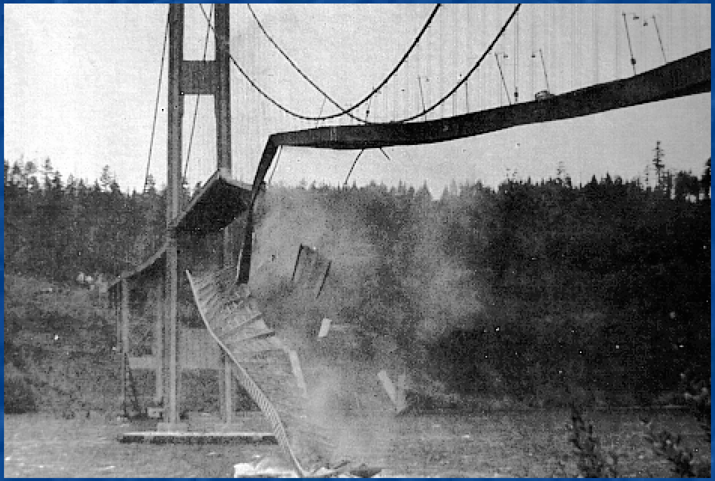
Do You Measure Anything?

Percent



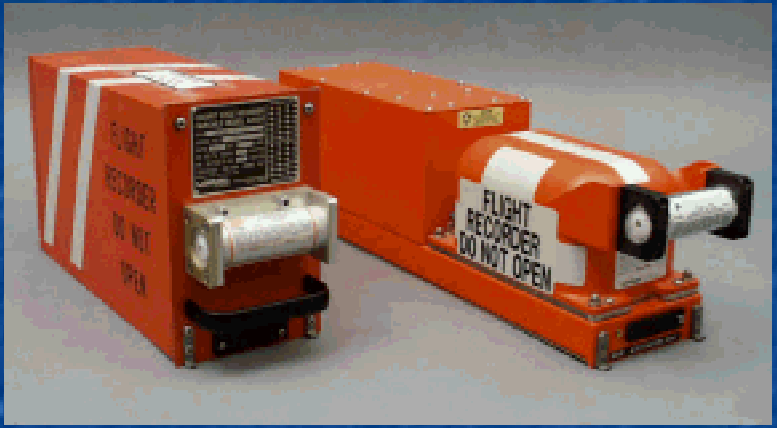
Are We Professionals?

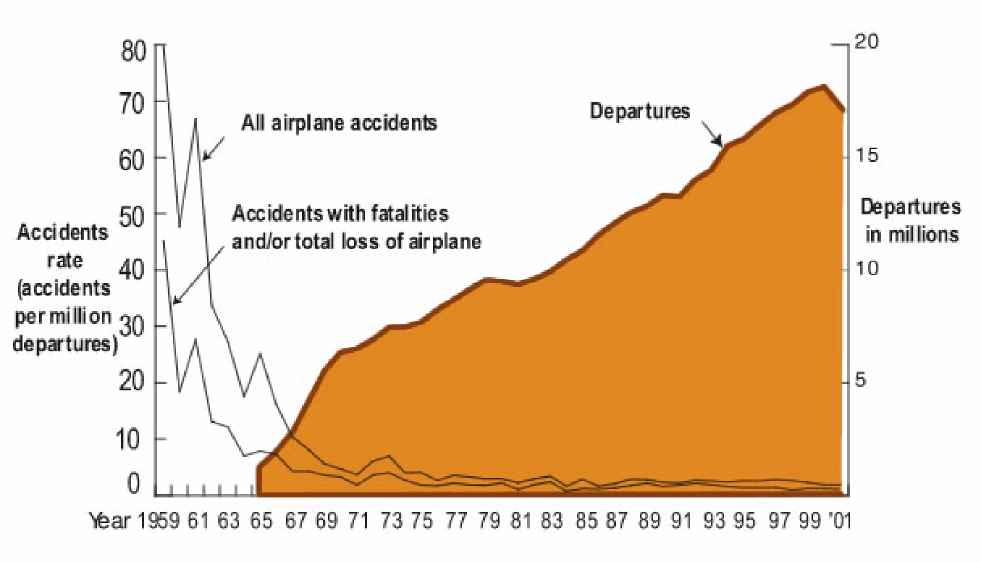
How Does Engineering Become Engineering?



- Montrose Bridge, Scotland 1838
- Menai Strait Bridge, Wales, 1839
- Basse-Chaine Bridge, 1850
- Roche-Bernard Bridge, France
- Wheeling Suspension Bridge, 1854
- Niagara-Lewiston Bridge, 1864
- Niagara-Clifton Bridge, 1889

How Does Engineering Become Engineering?





How Does Engineering Become Engineering?

Iroquois Fire

Triangle Shirtwaist fire

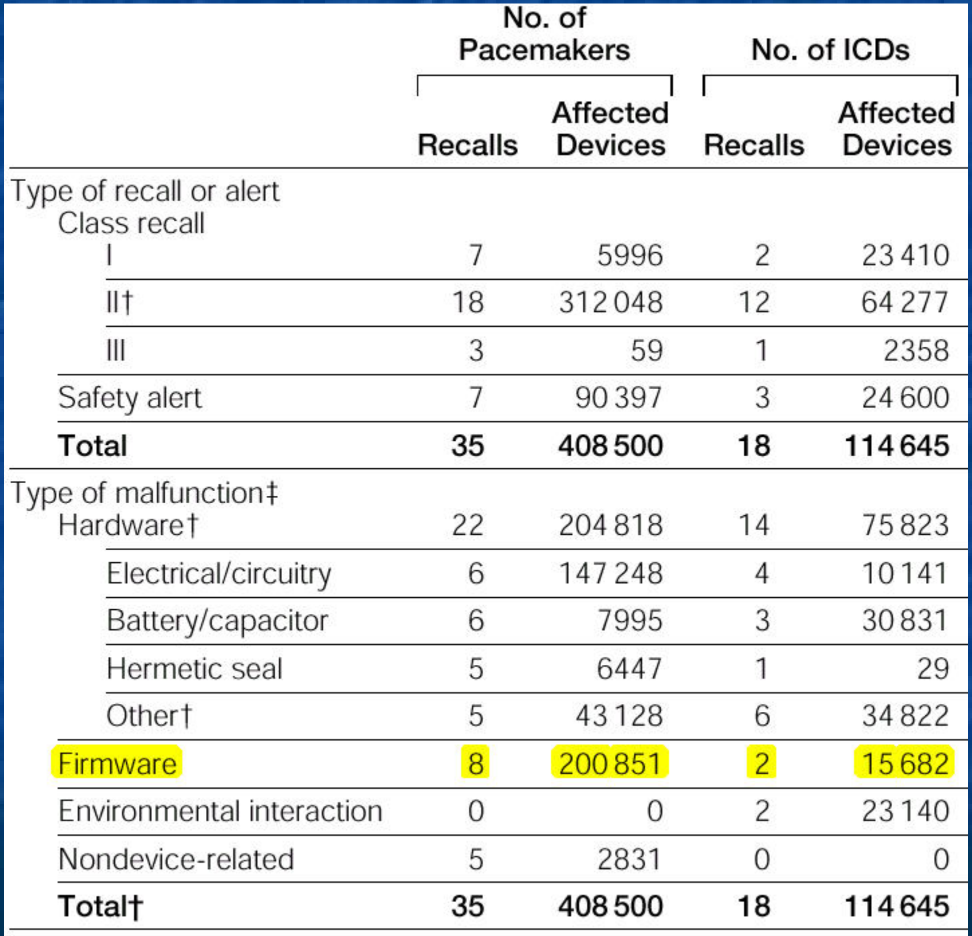
MGM fire

Iroquois Fire Report

“The fire department seemed to be under the impression that they were required only to fight flames and appeared surprised that their department was expected by the public to take every precaution to prevent fire from starting.”

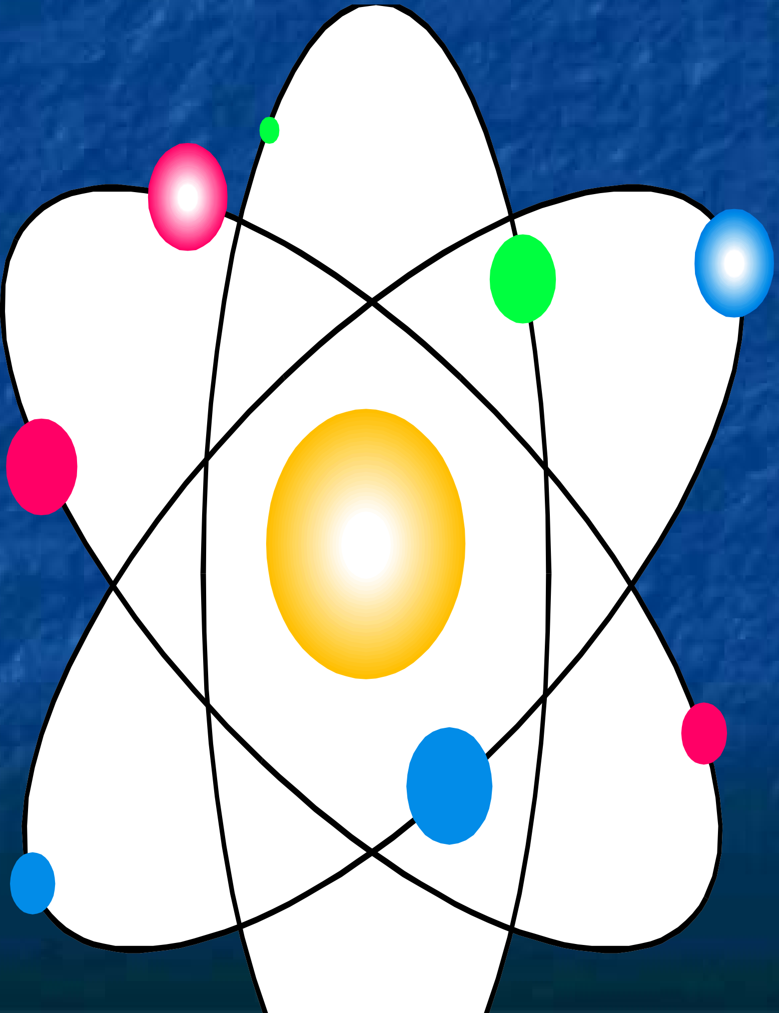
Recalls

Recalls Are Getting Worse



	No. of Pacemakers		No. of ICDs	
	Recalls	Affected Devices	Recalls	Affected Devices
Type of recall or alert				
Class recall				
I	7	5996	2	23 410
II†	18	312 048	12	64 277
III	3	59	1	2358
Safety alert	7	90 397	3	24 600
Total	**35**	**408 500**	**18**	**114 645**
Type of malfunction‡				
Hardware†	22	204 818	14	75 823
Electrical/circuitry	6	147 248	4	10 141
Battery/capacitor	6	7995	3	30 831
Hermetic seal	5	6447	1	29
Other†	5	43 128	6	34 822
Firmware	8	200 851	2	15 682
Environmental interaction	0	0	2	23 140
Nondevice-related	5	2831	0	0
Total†	**35**	**408 500**	**18**	**114 645**

Testing Failures

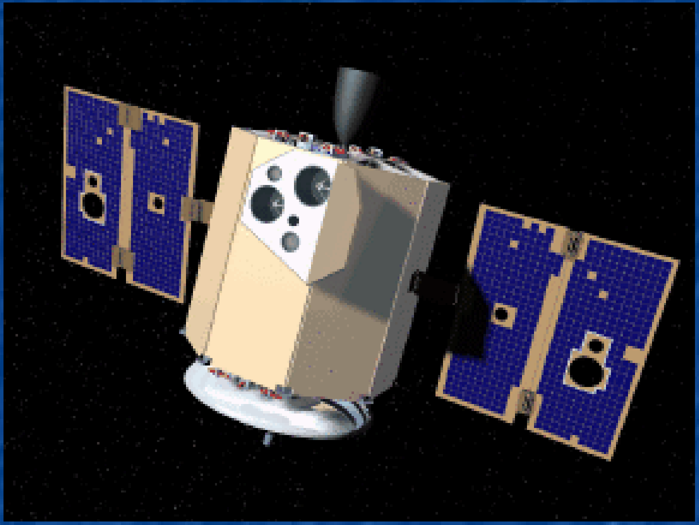


Testing Failures

“Although there was limited long duration testing whose purpose was to identify system memory consumption of this type, no problems were detected because the system was not exercised in the same way that it would later be used in flight.”

Testing Failures

We Can’t Learn From Disaster

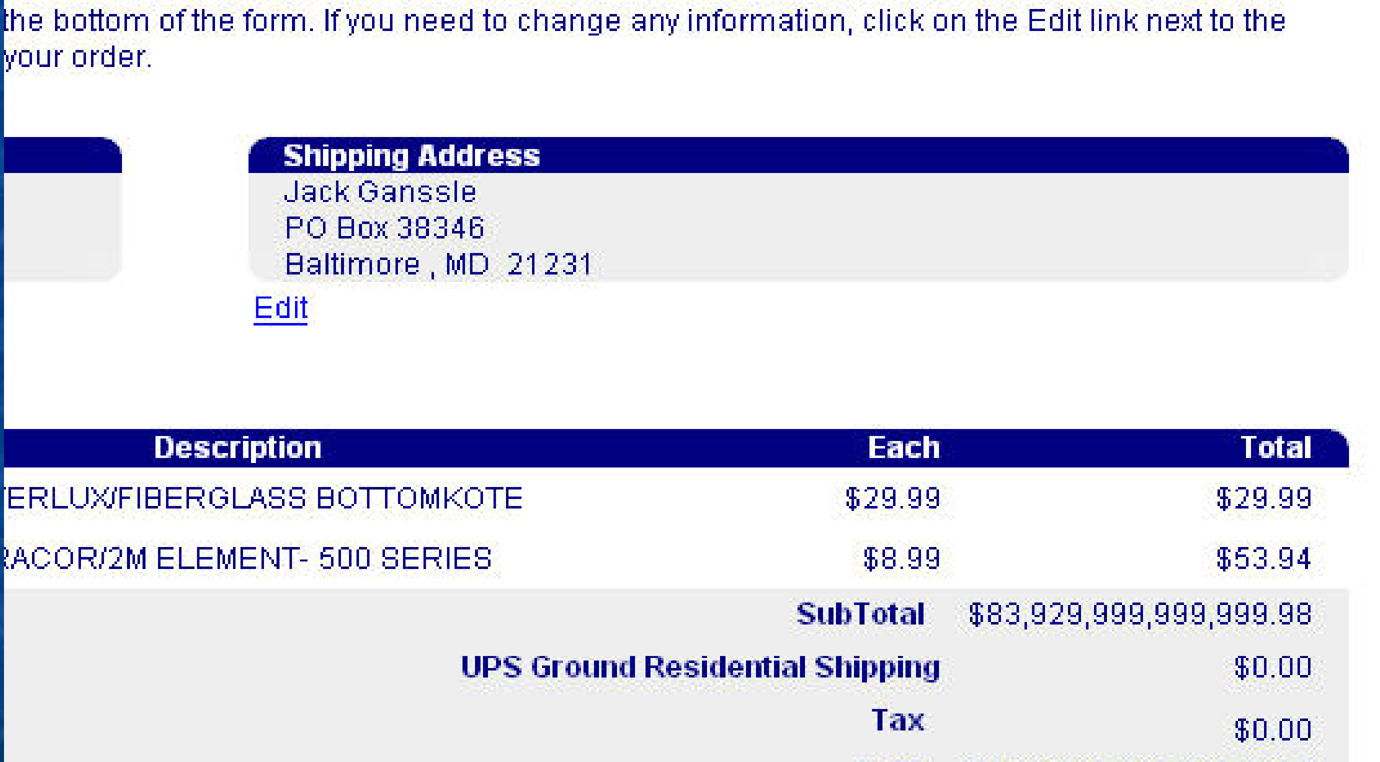


We Can’t Learn From Disaster

Uwatec dive computer

Challenger

Incredibly Sloppy Programming



the bottom of the form. If you need to change any information, click on the Edit link next to the
your order.

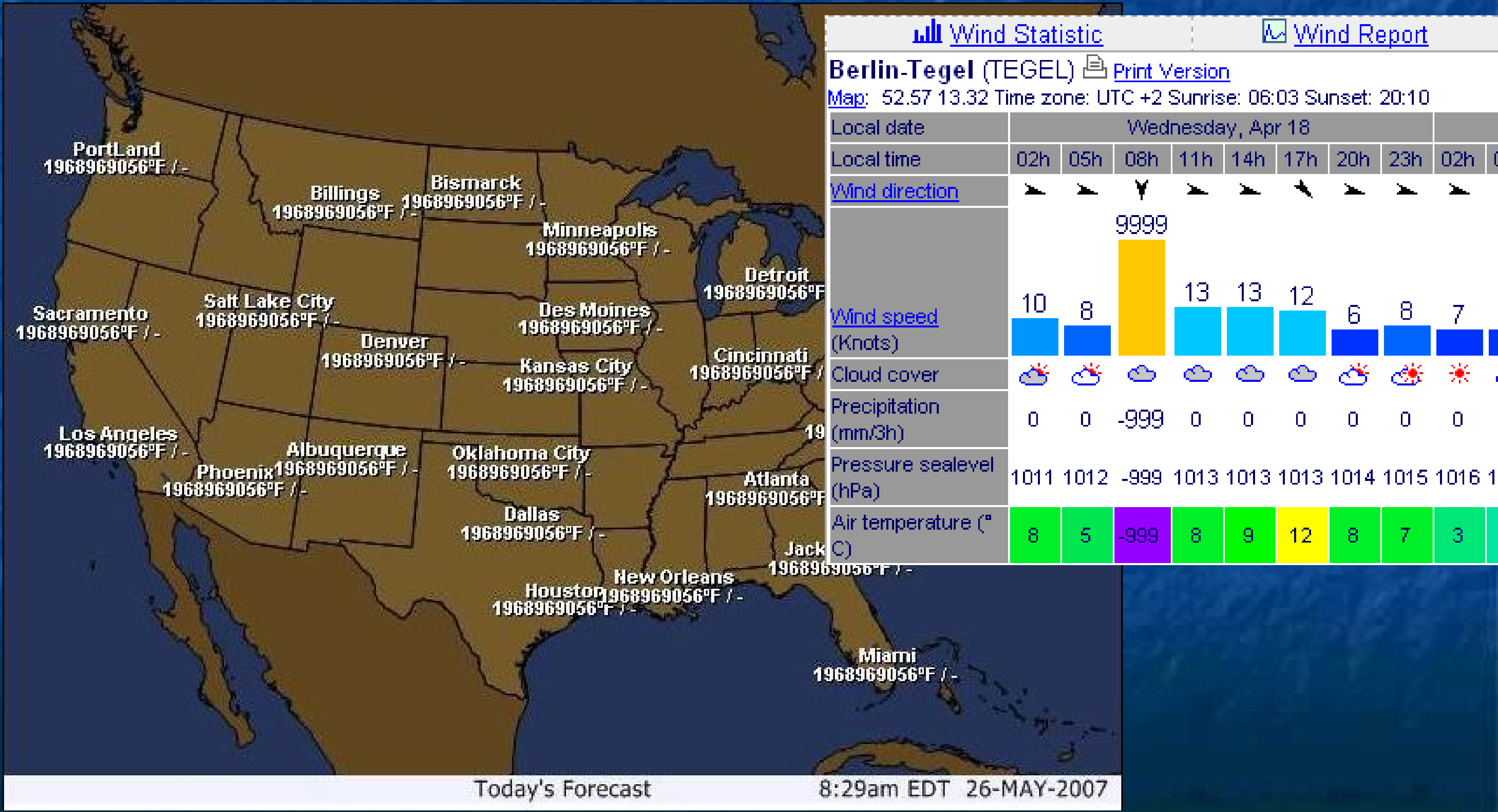
Shipping Address

Jack Ganssle
PO Box 38346
Baltimore , MD 21231

Edit

Description	Each	Total
ERLUX/FIBERGLASS BOTTOMKOTE	$29.99	$29.99
ACOR/2M ELEMENT- 500 SERIES	$8.99	$53.94
	SubTotal	$83,929,999,999,999.98
	UPS Ground Residential Shipping	$0.00
	Tax	$0.00

Incredibly Sloppy Programming



Today's Forecast 8:29am EDT 26-MAY-2007

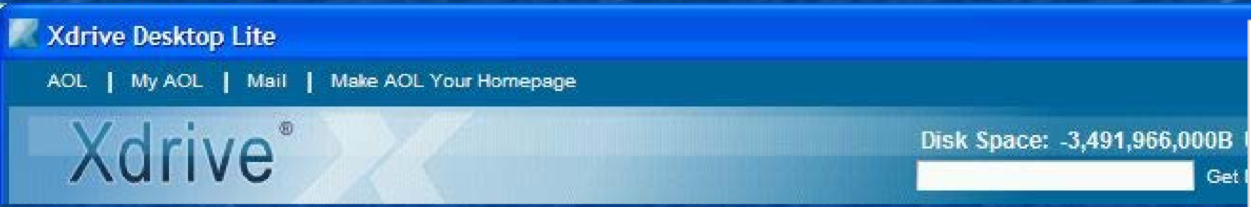
Wind Statistic | Wind Report

Berlin-Tegel (TEGEL) Print Version

Map: 52.57 13.32 Time zone: UTC +2 Sunrise: 06:03 Sunset: 20:10

Local date	Wednesday, Apr 18								
Local time	02h	05h	08h	11h	14h	17h	20h	23h	02h
Wind direction									
Wind speed (Knots)	10	8	9999	13	13	12	6	8	7
Cloud cover	⛅	⛅	☁	☁	☁	☁	⛅	⛅	☀
Precipitation (mm/3h)	0	0	-999	0	0	0	0	0	0
Pressure sealevel (hPa)	1011	1012	-999	1013	1013	1013	1014	1015	1016
Air temperature (° C)	8	5	-999	8	9	12	8	7	3

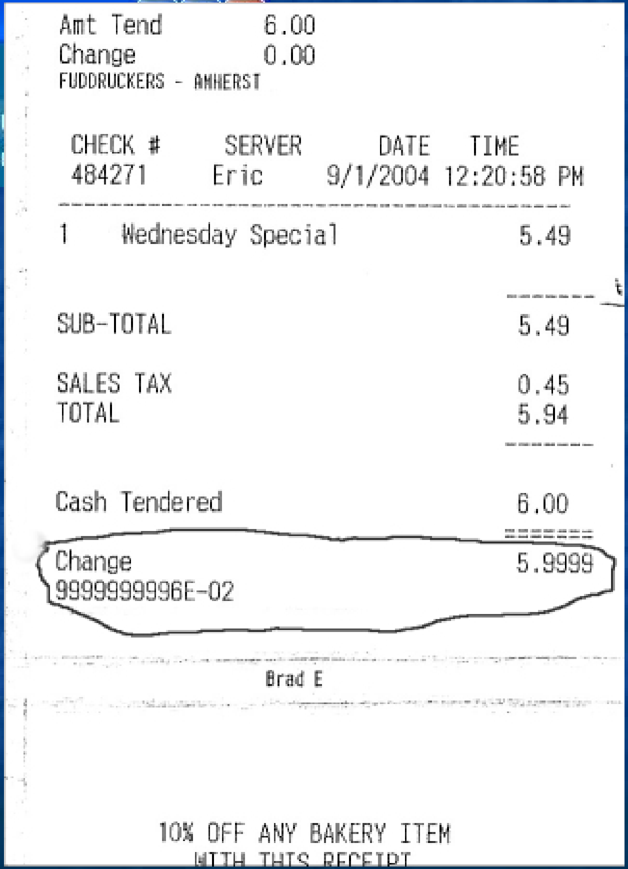
Incredibly Sloppy Programming


Xdrive Desktop Lite

AOL | My AOL | Mail | Make AOL Your Homepage

Xdrive®

Disk Space: -3,491,966,000B


Amt Tend 6.00
Change 0.00
FUDDRUCKERS - AMHERST

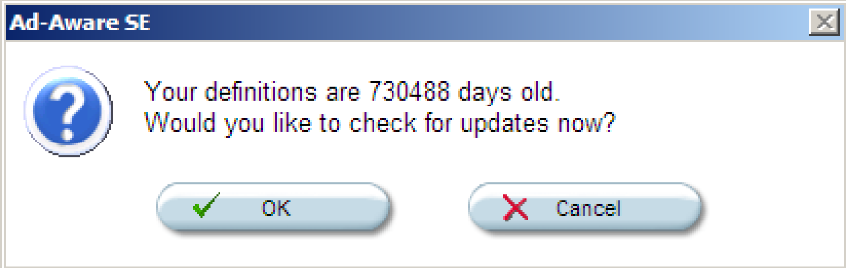
CHECK #	SERVER	DATE	TIME
484271	Eric	9/1/2004	12:20:58 PM

1 Wednesday Special	5.49
SUB-TOTAL	5.49
SALES TAX	0.45
TOTAL	5.94
Cash Tendered	6.00
Change	5.9999

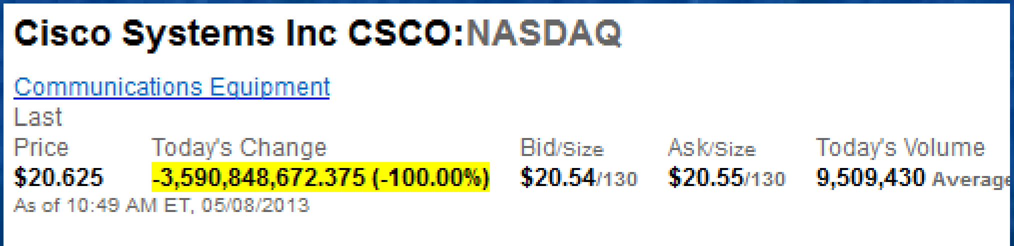
9999999996E-02

Brad E

10% OFF ANY BAKERY ITEM
WITH THIS RECEIPT


Ad-Aware SE

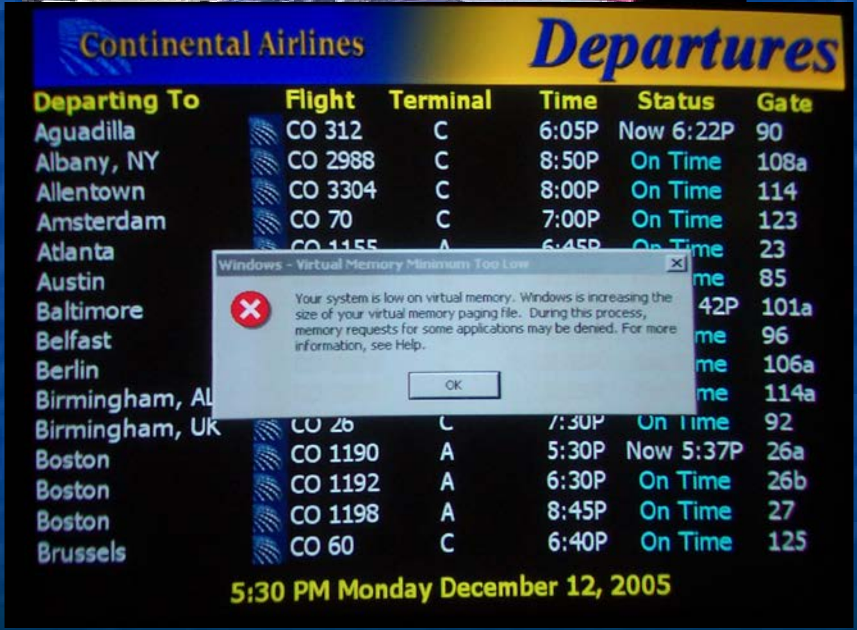
Your definitions are 730488 days old.
Would you like to check for updates now?


Cisco Systems Inc CSCO:NASDAQ

Communications Equipment

Last Price	Today's Change	Bid/Size	Ask/Size	Today's Volume
$20.625	-3,590,848,672.375 (-100.00%)	$20.54/130	$20.55/130	9,509,430 Average

As of 10:49 AM ET, 05/08/2013



Continental Airlines

Departures

Departing To	Flight	Terminal	Time	Status	Gate
Aguadilla	CO 312	C	6:05P	Now 6:22P	90
Albany, NY	CO 2988	C	8:50P	On Time	108a
Allentown	CO 3304	C	8:00P	On Time	114
Amsterdam	CO 70	C	7:00P	On Time	123
Atlanta	CO 1155	A	6:45P	On Time	23
Austin				me	85
Baltimore				42P	101a
Belfast				me	96
Berlin				me	106a
Birmingham, AL				me	114a
Birmingham, UK	CO 26	C	7:30P	On Time	92
Boston	CO 1190	A	5:30P	Now 5:37P	26a
Boston	CO 1192	A	6:30P	On Time	26b
Boston	CO 1198	A	8:45P	On Time	27
Brussels	CO 60	C	6:40P	On Time	125

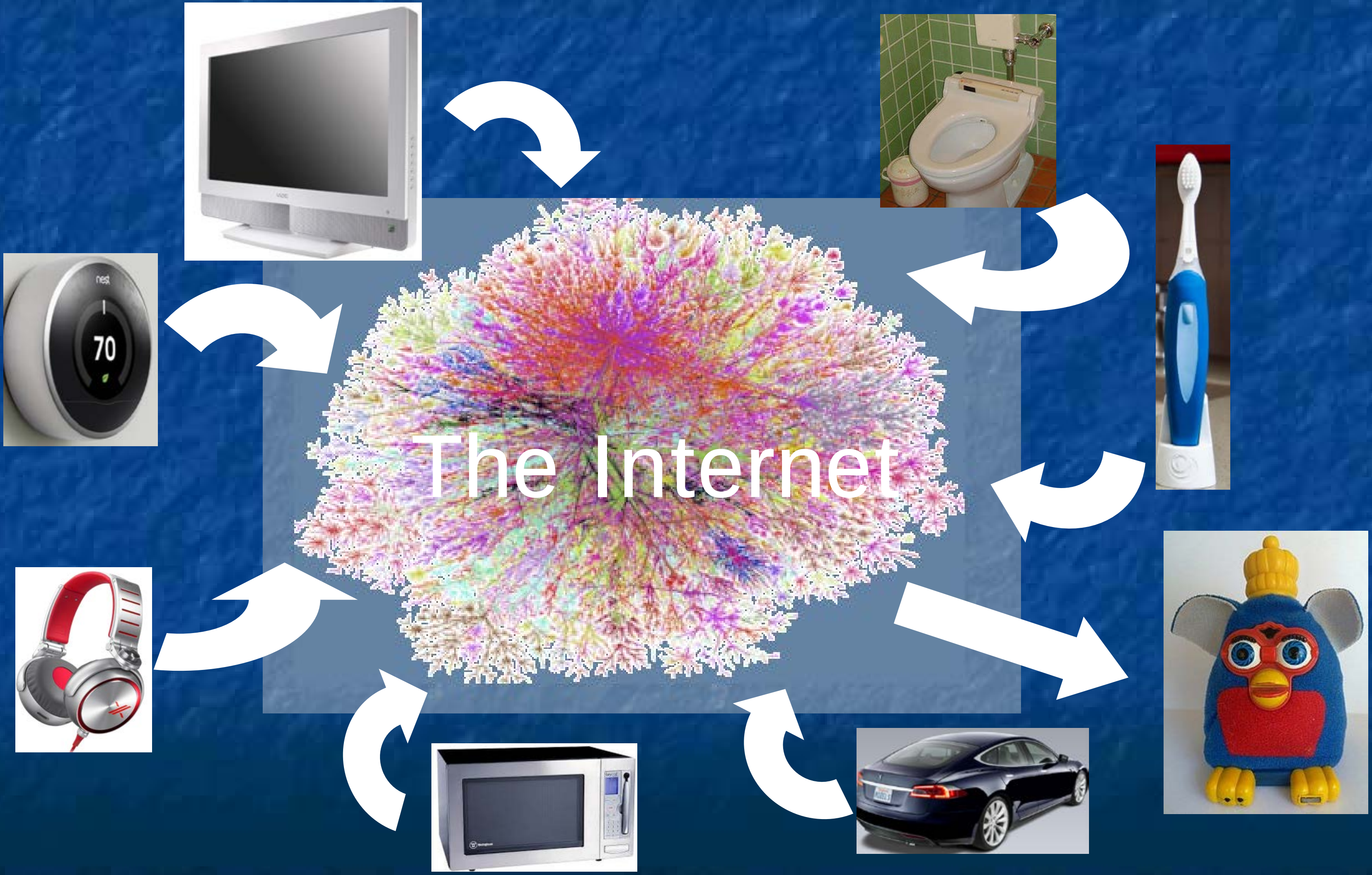
Windows - Virtual Memory Minimum Too Low

Your system is low on virtual memory. Windows is increasing the size of your virtual memory paging file. During this process, memory requests for some applications may be denied. For more information, see Help.

OK

5:30 PM Monday December 12, 2005

The Internet of Things



Iroquois Fire Report

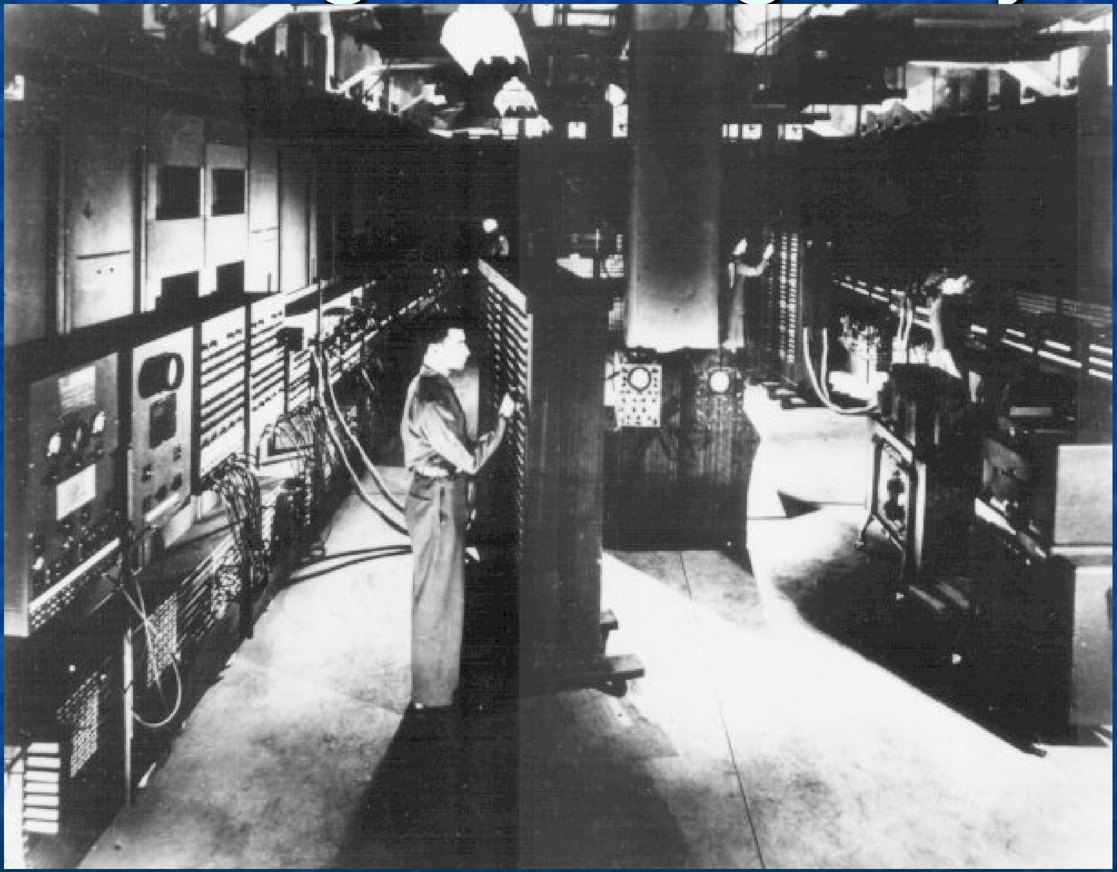
"The fire department seemed to be under the impression that they were required only to fight flames and appeared surprised that their department was expected by the public to take every precaution to prevent fire from starting."

Software Failure Report

“The Fire Department [software community] seemed to be under the impression that they were required only to fight flames (bugs) and appeared surprised that their department was expected by the public to take every precaution (inspections, careful design, encapsulation, etc) to prevent fire (bugs) from starting.”

Great Engineering Projects

Great Engineering Projects



Great Engineering Projects

Great Engineering Projects

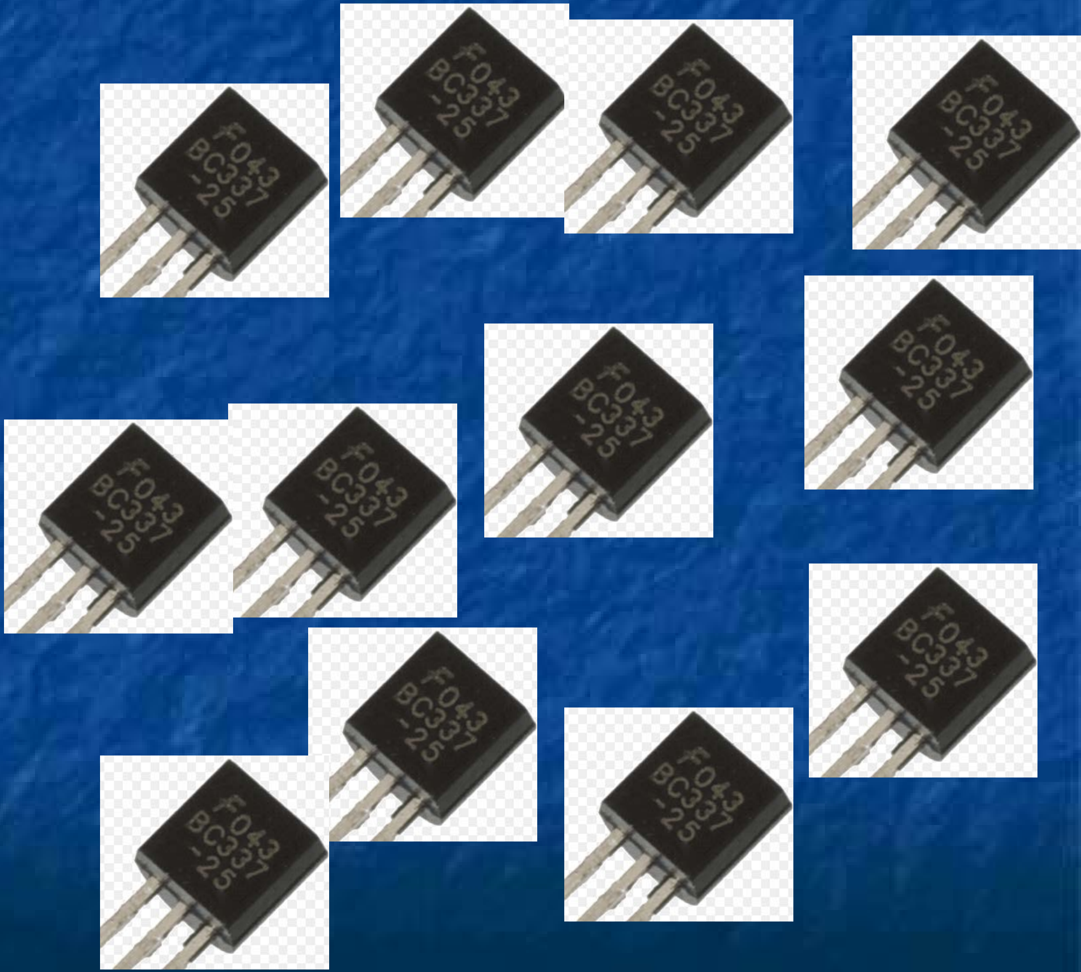
X 173

Great Engineering Projects

Great Engineering Projects

Great Engineering Projects

Or:

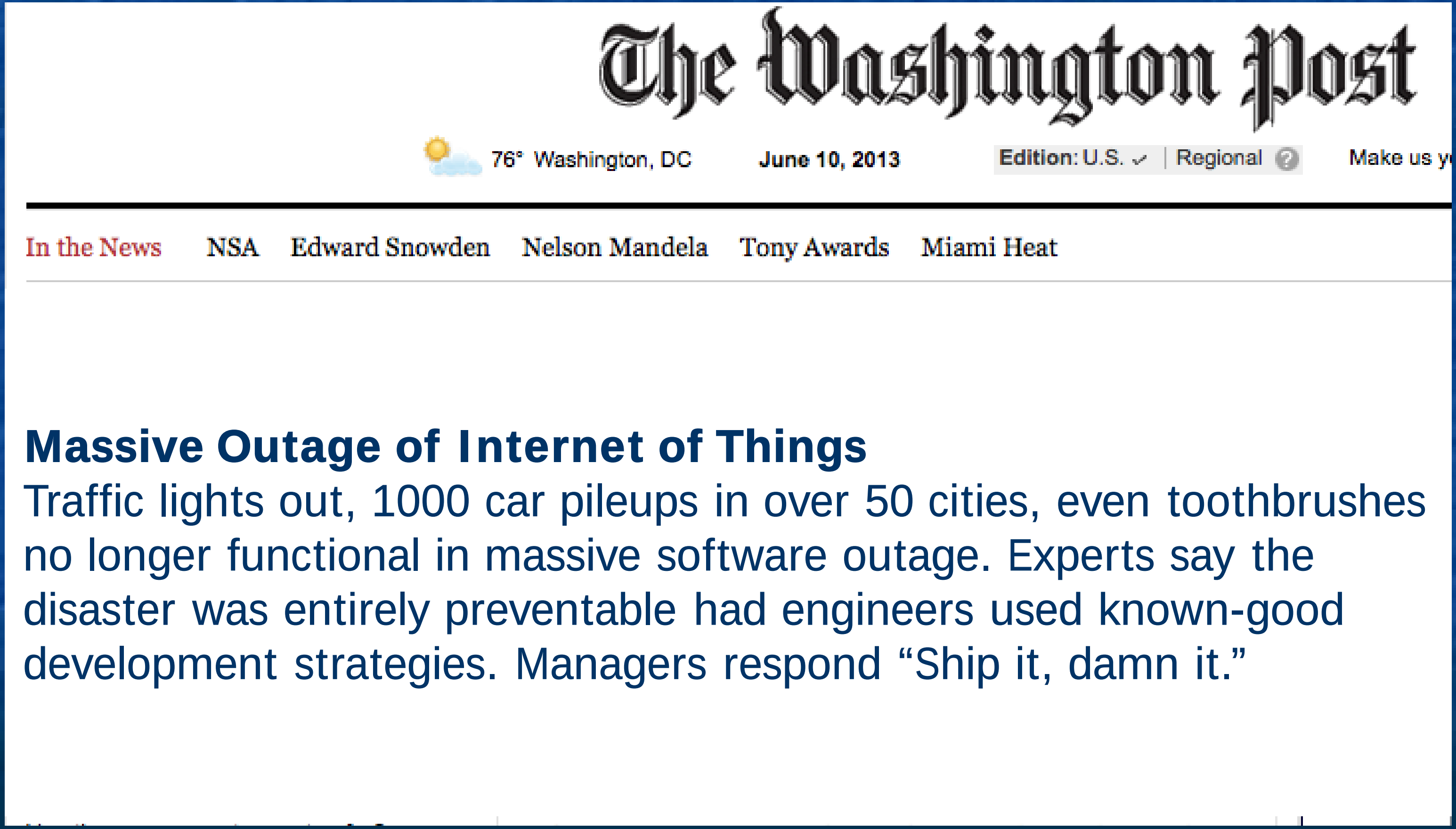


The Way Ahead

The Way Ahead

The Way Ahead

Litigation



The Washington Post

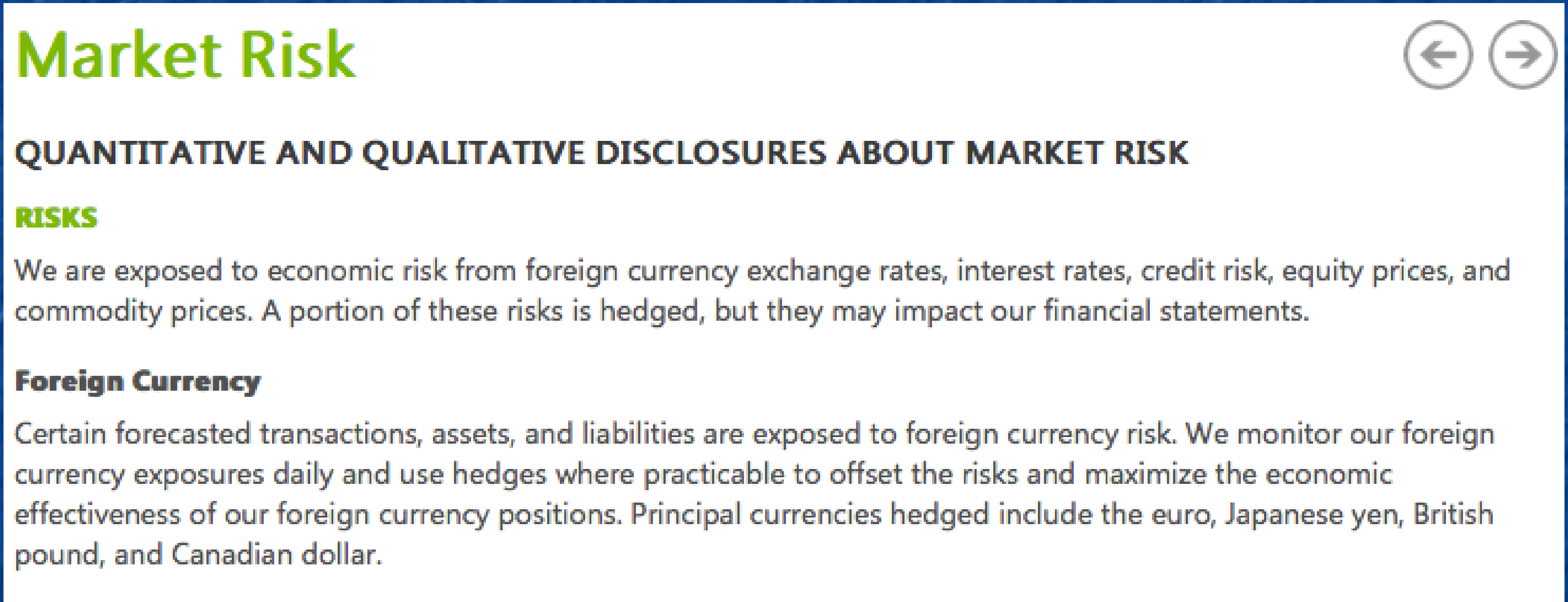
76° Washington, DC June 10, 2013 Edition: U.S. ✓ | Regional ? Make us y

Massive Outage of Internet of Things

Traffic lights out, 1000 car pileups in over 50 cities, even toothbrushes no longer functional in massive software outage. Experts say the disaster was entirely preventable had engineers used known-good development strategies. Managers respond “Ship it, damn it.”

The Way Ahead

Wall Street



Market Risk

QUANTITATIVE AND QUALITATIVE DISCLOSURES ABOUT MARKET RISK

RISKS

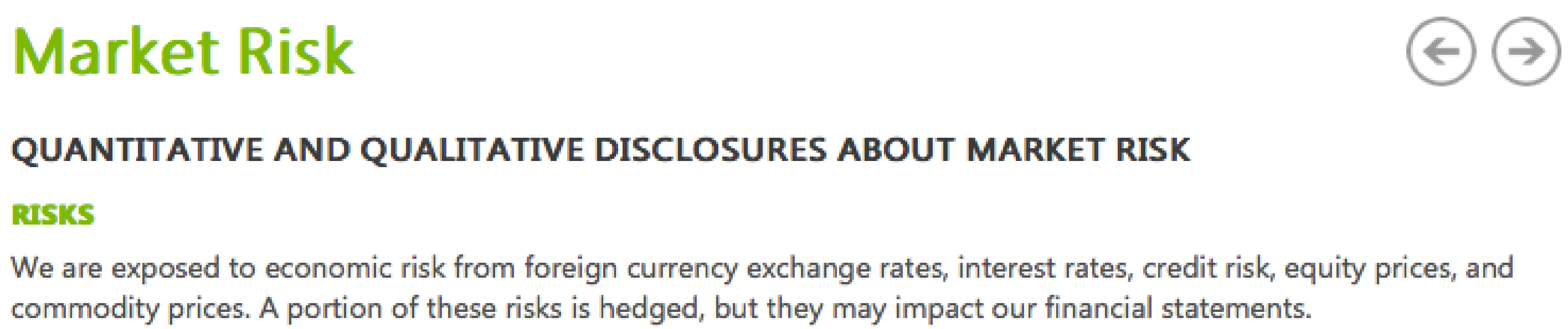
We are exposed to economic risk from foreign currency exchange rates, interest rates, credit risk, equity prices, and commodity prices. A portion of these risks is hedged, but they may impact our financial statements.

Foreign Currency

Certain forecasted transactions, assets, and liabilities are exposed to foreign currency risk. We monitor our foreign currency exposures daily and use hedges where practicable to offset the risks and maximize the economic effectiveness of our foreign currency positions. Principal currencies hedged include the euro, Japanese yen, British pound, and Canadian dollar.

The Way Ahead

Wall Street



Market Risk

QUANTITATIVE AND QUALITATIVE DISCLOSURES ABOUT MARKET RISK

RISKS

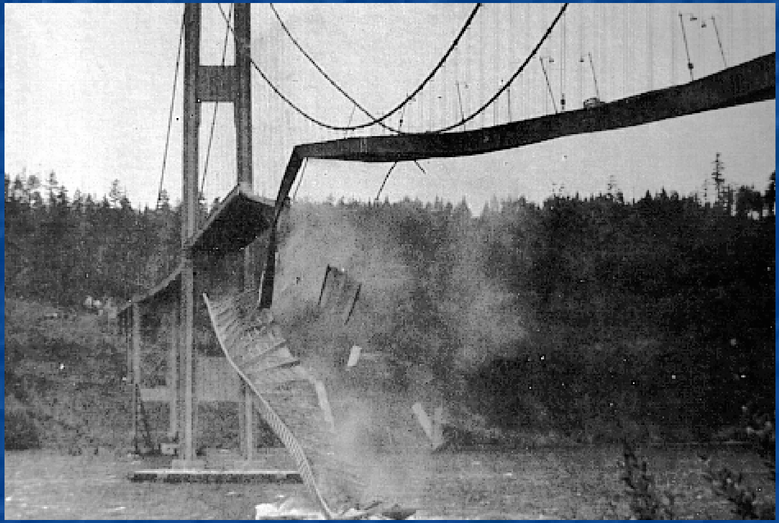
We are exposed to economic risk from foreign currency exchange rates, interest rates, credit risk, equity prices, and commodity prices. A portion of these risks is hedged, but they may impact our financial statements.

Software Engineering

We have elected to use development strategies known to lead to high bug rates, massive returns, and in some cases injury and/or death. These issues don’t concern us at all, but it’s reasonable to expect massive impacts to future financials.

The Way Ahead

Regulation (by catastrophe)



The Way Ahead

Education

- This is not software engineering:

```
long timer_read(void)
{
  unsigned int low, high;
  push_interrupt_state;
  disable_interrupts;
  low=inword(hardware_register);
  high=timer_hi;
  if(timer_overflow){++high;
     low=inword(hardware_register);}
  pop_interrupt_state;
  return (((ulong)high)<<16 + (ulong)low);
}
```

The Way Ahead

Strong management

- An absolute quality mindset.
- Complete intolerance of “artistes”
- Disciplined use of careful strategies that may not be considered “fun”.

ANY
QUESTIONS